TRABAJO ESPECIAL DE GRADO

INTRODUCCIÓN DEL CONCEPTO SOFTSWITCH EN UN OPERADOR DE LARGA DISTANCIA

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. Santana A., Johnatan A.
para optar al título de
Ingeniero Electricista

Caracas, 2007

TRABAJO ESPECIAL DE GRADO

INTRODUCCIÓN DEL CONCEPTO SOFTSWITCH EN UN OPERADOR DE LARGA DISTANCIA

Prof. Guía: Ing. Carlos Fuenmayor
Tutor Industrial: Ing. Fidel Salgueiro

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. Santana A., Johnatan A.
para optar al título de
Ingeniero Electricista

Caracas, 2007

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELECTRICA
DEPARTAMENTO DE COMUNICACIONES

CONSTANCIA DE APROBACIÓN

Caracas, 12 de diciembre de 2007

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Johnatan A, Santana A., titulado:

"INTRODUCCIÓN DEL CONCEPTO SOFTSWITCH EN UN OPERADOR DE LARGA DISTANCIA"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Maria Lejed
Jurado

Prof. Franklin Martínez
Jurado

Prof. Carlos Fuenmayor
Prof. Guía

Edificio Escuela de Ingeniería Eléctrica, piso 1, oficina 201, Ciudad Universitaria, Los Chaguaramos, Caracas 1051, D.F.
TELÉFONOS. (VOZ) +58 212 6053300 (FAX) +58 212 6053105
Mail: eie-com@elecrisc.ing.ucv.ve

DEDICATORIA

Quiero dedicar este trabajo de grado primero que todo a Dios, por acompañarme en momentos de logros y dificultades, además, por guiarme en el trayecto hacia la conquista de mis metas. Esto es por ti.

A mis Padres, que con su esfuerzo me han hecho quien soy y me han ayudado en todos mis proyectos y decisiones. Mil Gracias.

A Laura, Cathy y Josy que con su apoyo y paciencia me han ayudado a enfrentar el reto de esta difícil carrera.

A los Ingenieros Carlos Fuenmayor y Fidel Salgueiro, que me han guiado en el desarrollo de este proyecto y en general a todos los profesores, que impartiendo sus conocimientos me han hecho llegar hasta aquí.

A todas aquellas otras personas que de alguna u otra forma estuvieron presentes a lo largo de este camino.

Santana A., Johnatan A.

INTRODUCCIÓN DEL CONCEPTO SOFTSWITCH EN UN OPERADOR DE LARGA DISTANCIA

Profesor Guía: Carlos Fuenmayor. Tutor Industrial: Ing. Fidel Salgueiro. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: 123.com.ve. Trabajo de Grado. 2007. 118h.

Palabras Claves: Telefonía TDM; *Switch* Telefónico; Migración; Telefonía IP; Redes de próxima generación; *Softswitch*; Protocolo de pruebas.

Resumen. El presente trabajo de grado consiste en desarrollar especificaciones técnicas para la sustitución de una central telefónica ANS Ericsson por un *switch* de paquetes "*Softswitch* Nextone MSX" Clase 4, en la plataforma de Entel Venezuela *Core* La Urbina, hoy 123.com.ve. Con esto se busca atender los nuevos requerimientos de los clientes en cuanto a servicios de voz, datos, video y generar reducción de costos en transporte, traduciéndose en mejores tarifas para el cliente final, manteniendo o mejorando la calidad de servicio que se presta. A su vez con la actualización y la reducción de tarifas se busca proveer de la mejor y más actual tecnología a clientes actuales, futuros y a los sectores más desfavorecidos. Para la realización de este proyecto, primero se estudiará la plataforma de red actual de la Empresa y se realizará un levantamiento de información (base de estudio para la sustitución de la central telefónica), acompañado esto por el desarrollo de un protocolo de pruebas necesario para cumplir con las exigencias de la Empresa y recomendaciones internacionales referentes a servicios de voz sobre redes de próxima generación. Finalmente, se procederá a desarrollar un modelo de Ingeniería conveniente para la futura inserción del *Softswitch Clase 4 Nextone*, utilizando los protocolos de control y transporte apropiados, incluyendo una metodología técnica necesaria para la migración de las rutas LDI TDM-S y LDN TDM-S a rutas IP a través del *Softswitch*.

ÍNDICE GENERAL

Pág.

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ACRÓNIMOS

AAA	***Authentication, Authorization, Accounting***
ACELP	***Algebraic Code Excited Linear Prediction***
ACR	***Absolute Category Rating***
ADPCM	***Adaptative Differential Pulse Code Modulation***
ALT	***Autonomous Line Terminating Unit***
ANI	***Automatic Identification Number***
ANS	***Access Node Switch***
ARQ	***Admission Request***
ASCII	***American Standard Code Information Interchange***
BNC	***Bayonet Neill-Concelman***
CAS	***Channel Associated Signalling***
CBR	***Constrained Based Routing***
CCSS7	***Common Channel Signalling System 7***
CDC	***Centros de Comunicaciones***
CDR	***Call Detail Report***
CS-ACELP	***Conjugate Structure Algebraic Code Excited Linear Prediction***
CSB	***Circuit Switch Block***
CSMA/CD	***Carrier Sense Multiple Access with Collision Detection***
CTU	***Clock and Tone Unit***
DMZ	***Demilitarized Zones***
DNS	***Domain Name System***
DoS	***Denial of Service***
DRQ	***Disengage Request***
DSU	***Data Service Unit***
DTMF	***Dual-Tone Multifrequency***
EBCDIC	***Extended Binary Coded Decimal Interchange Code***
ENUM	***Telephone Number Mapping***
ERL	***Echo Return Lost***
FDM	***Frequency Division Multiplexing***
FEC	***Forwarding Equivalent Class***
FTP	***File Transfer Protocol***
FWSM	***Firewall Security System***
GIF	***Graphics Interchange Format***
GLBP	***Gateway Load Balancing Protocol***
HSRP	***Hot Stand By Router Protocol***
HSSI	***High Speed Serial Interface***
HTTP	***Hypertext Transfer Protocol***
IHL	***Internet Header Length***
IMS	***IP Multimedia Subsystem***
IMX	***IP Multimedia Exchange***
IP	***Internet Protocol***

IPv4	***Internet Protocol version 4***
IPv6	***Internet Protocol version 6***
ISDN	***Integrated Services Digital Network***
ISDN-PRI	***ISDN-Primary Rate Interface***
ISO	***International Standards Organization***
ISP	***Internet Service Provider***
IVR	***Interactive Voice Response***
JPEG	***Joint Photographics Experts Group***
LAN	***Local Area Network***
LDI	***Larga Distancia Internacional***
LDN	***Larga Distancia Nacional***
LRQ	***Location Request***
LSP	***Label Switched Path***
LSR	***Label Switched Router***
MAC	***Media Access Control***
MCU	***Multipoint Control Unit***
MDF	***Main Distribution Frame***
MOS	***Mean Option SCore***
MPEG	***Moving Pictures Experts Group***
MPLS	***Multi Protocol Label Switching***
MP-MLQ	***Multipulse Maximun Likelihood Quantization***
MSX	***Multiprotocol Session Exchange***
NAT	***Network Address Translation***
NGN	***Next Generation Networks***
NIC	***Network Interface Card***
OSI	***Open System Interconnection***
PABX	***Private Automatic Branch Exchange***
PAMS	***Perceptual Analysis Measurement System***
PAT	***Port Address Translation***
PCM	***Pulse Code Modulation***
PDH	***Plesiochronous Digital Hierarchy***
PDV	***Post Delay Variance***
PESQ	***Perceptual Evaluation of Speech Quality***
PHB	***Per Hop Behavior***
PRI	***Primary Rate Interface***
PSB	***Packet Switch Block***
PSQM	***Perceptual Speech Quality Measurement***
PSTN	***Public Switched Telephone Network***
PSU	***Power Supply Unit***
QoS	***Quality of Service***
QoV	***Quality of Voice***
RADIUS	***Remote Authentication Dial In User Service***
RAS	***Registration Admission Status***
RFC	***Request for Comments***
RRQ	***Registration Request***

RSM	***Real time Session Management***
RSVP	***Resource Reservation Protocol***
RTCP	***Real Time Control Protocol***
RTP	***Real Time Protocol***
SBC	***Session Border Controller***
SCP	***Service Control Point***
SCP	***Session Control Protocol***
SDH	***Synchronous Digital Hierarchy***
SDP	***Session Description Protocol***
SHU	***System Handling Unit***
SIP	***Session Initiation Protocol***
SL	***Signalling Links***
SLA	***Service Level Agreements***
SNMP	***Simple Mail Transfer Protocol***
SP	***Signalling Point***
SSP	***Service Switching Point***
STM	***Synchronous Transport Module***
STP	***Signal Transfer Point***
TCP	***Transmission Control Protocol***
TDM	***Time Division Multiplexing***
TDMS	***Synchronous Time Division Multiplexing***
ToS	***Type of Service***
TTL	***Time to Live***
UA	***User Agent***
UAC	***User Agent Client***
UAS	***User Agent Server***
UDP	***User Datagram Protocol***
URQ	***Unregister Request***
VAD	***Voice Activity Detection***
VAU	***Voice Announcement Unit***
VLAN	***Virtual Local Area Network***
VoD	***Video on Demand***
VoIP	***Voice over Internet Protocol***
VPN	***Virtual Private Network***
WAN	***Wide Area Network***
ZIP	***Zone Information Protocol***

SIGLAS

3GPP	*3rd Generation Partnership Project*
ANSI	*American National Standards Institute*
ARPA	*Advanced Research Program Agency*
ARPANET	*Advanced Research Program Agency Network*
AT&T	*American Telephone and Telegraph*
CANTV	*Compañía Anónima Teléfonos de Venezuela*
CONATEL	*Comisión Nacional de Telecomunicaciones*
EE.UU	*Estados Unidos*
ENTEL	*Empresa Nacional de Telecomunicaciones*
ETECSA	*Empresa de Telecomunicaciones de Cuba, S.A.*
ETSI	*European Telecommunications Standards Institute*
ICANN	*Internet Corporation for Assigned Names and Numbers*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IPCC	*International Packet Communications Consortium*
ISC	*International Softswitch Consortium*
ITU	*Internacional Telecommunication Union*
ITU-T	*ITU- Telecommunication Standardization Sector*
LANautilus	*Latin American Nautilus*

INTRODUCCIÓN

La imprescindible necesidad de comunicación que ha tenido el ser humano desde hace más de un siglo hizo que científicos de la época desarrollaran sistemas que pudieran dar solución a esas necesidades. En 1847 Alexander Graham Bell concluyó teóricamente que se podía transmitir el habla a través de un alambre, haciendo variar una corriente eléctrica de la misma forma que lo hace el aire al variar su densidad dada la producción de sonidos. Entre 1854 y 1860 Antonio Meucci diseñó y construyó el primer aparato telefónico. En 1876 le fue aprobada la patente del teléfono eléctrico a Graham Bell; tres días después se llevo a cabo la primera conversación a través de un sistema telefónico. Hoy en día, y a partir de Junio de 2.002 el Congreso de los Estados Unidos aprobó la resolución 269 donde se reconoce a Antonio Meucci como el inventor del teléfono.

En 1878, la ciudad de New Heaven en Connecticut fue la primera en tener una central telefónica comercial y contaba con 20 abonados, cuyo par de hilos de transmisión terminaban en un conector que era manejado por un operador de la Central, el cual realizaba la conmutación de manera manual introduciendo una clavija en el puerto del abonado llamante para preguntar el número destino donde quería conectarse, hecho esto, insertaba la clavija en el puerto del destinatario y se establecía la conexión. Ya en 1880, 54 mil estadounidenses contaban con servicio telefónico.

Por otro lado, los primeros sistemas de conmutación automáticos se denominaron “de paso” ó “paso a paso”. En estos sistemas electromecánicos, la mayoría de los equipos de conmutación tienen sus propios circuitos de control, los cuales están bajo el control del abonado que llama, posteriormente un conmutador

localiza la línea y la conecta a otro conmutador selector, que a su vez localiza la línea destino y establece la conexión de la llamada.

Poco a poco las centrales telefónicas fueron evolucionando de manera conjunta con la electrónica, actualmente son administradas a través de computadoras; dichas centrales permiten ofrecer servicios complementarios a los habituales en estas redes.

Cabe destacar que estas redes telefónicas estaban basadas en conmutación de circuitos; para que exista una conmutación de circuito, se requiere una conexión física previa al establecimiento del enlace y durante todo el tiempo que este perdure, esto conlleva a cierta ineficiencia dado a que este circuito no puede ser utilizado mientras se mantenga la conexión.

Dado al amplio crecimiento en los suscriptores de dichas redes, la distribución de los recursos se hace cada vez más crítica. Debido a esto y gracias a la evolución de tecnologías y protocolos como el IP (Internet Protocol), basado en conmutación de paquetes[1], se ha logrado un mejor rendimiento de dichos recursos a un costo más bajo.

La tendencia actual en las telecomunicaciones se inclina hacia la integración de todo tipo de servicios en una sola infraestructura de red basada en conmutación de

---

[1] *Conmutación de paquetes: utilizada en redes de datos, voz y video; el mensaje se divide en pequeños paquetes, estos paquetes son enviados por distintos caminos a su destino, lo que permite que la utilización del medio de transmisión se haga de manera compartida. Disponible en: http://mit.ocw.universia.net/15.565J/NR/rdonlyres/Sloan-School-of-Management/15-565JIntegrating-eSystems---Global-Information-SystemsSpring20/8C978DE3-B3CB-446A-8480-928C78A9460F/0/lecture08.pdf*

paquetes. Estas redes deben ofrecer un nivel de calidad de servicio, capacidad, fiabilidad y seguridad equivalente al de las redes telefónicas públicas conmutadas.

Para darle solución al desarrollo de estas redes, han aparecido en el mercado numerosos equipos, técnicas, tecnologías y protocolos que permiten la creación de modelos de redes capaces de cubrir dichas necesidades. Estos modelos son conocidos como modelos de Red de Próxima Generación NGN (Next Generation Networks).

Buscando atender los nuevos requerimientos de los clientes en cuanto a servicios de voz, datos, video y adicionalmente generar reducción de costos en transporte, traduciéndose esto en mejores tarifas para el cliente final, manteniendo o mejorando a su vez la calidad de servicio que se presta, Entel Venezuela, Empresa proveedora de tránsito para servicios de voz y operador de larga distancia, tanto nacional como internacional, requiere actualizar su plataforma, reducir costos operativos, aumentar su competitividad, mejorar la calidad de servicio de sus clientes y aumentar su capacidad de crecimiento.

Es importante destacar que la Empresa Entel Venezuela actualmente lleva por nombre 123.com.ve, ya que en enero de 2007 surge una oportunidad de negocio donde es adquirida por un grupo de Empresarios venezolanos, y a partir de ahí se replantea la visión de negocio llevando esto a un cambio necesario de infraestructura y actualización de su plataforma tecnológica para dar soporte a la demanda de clientes y crecer como Empresa de telecomunicaciones integradora de servicios.

Es por esto, que a través de la Vice-Presidencia de Ingeniería y Operaciones se decide desarrollar un modelo de red NGN mediante la inserción de tecnología *Softswitch* en sustitución de la central telefónica actual. Con la actualización y la reducción de tarifas se busca proveer de la mejor y más actual tecnología no solo a los clientes actuales y futuros, sino llegar también a los sectores más desfavorecidos,

política que fomenta el gobierno actual a través de sus proyectos sociales y dando cumplimiento a la constitución del servicio universal.

Tomando en cuenta que la tecnología NGN y sus valores agregados están en el comienzo de su auge, se abre un abanico de oportunidades para la Empresa, permitiéndole dar un paso adelante sobre sus competidores y convertirse en uno de los pioneros en Venezuela y America Latina en ofrecer este tipo de servicios.

El presente trabajo especial de grado consiste en desarrollar especificaciones técnicas para la sustitución de una central telefónica ANS (Access Node *Switch*) Ericsson clase 4 por un *switch* de paquetes "*Softswitch* Nextone MSX (Multiprotocol Session Exchange)" Clase 4, en la plataforma de 123.com.ve *Core* La Urbina. En tal sentido, se plantean los siguientes objetivos:

1. Estudiar la plataforma de red actual, así como el levantamiento de información que sirva como base para el estudio de la sustitución de la central telefónica.

2. Desarrollar el modelo de Ingeniería más conveniente para la futura inserción del *Softswitch Clase 4 Nextone*, utilizando los protocolos de control y transporte apropiados.

3. Desarrollar el protocolo de pruebas necesario para cumplir las exigencias de las normas ITU (International Telecommunication Union) e IETF (Internet Engineering Task Force), así como las de la Vice-Presidencia de Ingeniería y Operaciones, referentes a servicios de voz sobre redes de próxima generación.

4. Establecer la metodología técnica necesaria para la migración de las rutas LDI (Larga Distancia Internacional) TDM-S (Synchronous Time Division

Multiplexing) y LDN (Larga Distancia Nacional) TDM-S, a rutas IP, a través del *Softswitch* contemplando desde el levantamiento de información de la plataforma actual hasta el establecimiento de la metodología técnica para la migración de las rutas TDM a rutas IP.

A partir del desarrollo de los objetivos anteriores se podrá determinar ¿Cómo introducir el concepto *Softswitch* en un operador de larga distancia?

Partiendo de lo referido anteriormente, es de gran importancia el aporte que puede significar este trabajo especial de grado, tomando en cuenta que no solo podrá ser utilizado por la Empresa sino por cualquier Empresa de servicios nacional o internacional, adaptándolo a sus necesidades; así como pudiese ser utilizado como base para desarrollar o apoyar futuros estudios o proyectos relacionados con el tema.

CAPÍTULO I

MARCO REFERENCIAL

1.1 Redes de conmutación de circuitos

La conmutación de circuitos es la técnica más utilizada en redes de telefonía pública; en principio, se desarrolló para el tráfico de señales de voz analógicas y señales de voz digitales, pero también es capaz de gestionar tráfico de datos de manera poco eficiente. En estas redes se establece un canal dedicado para cada conexión que ocurra entre dos terminales, en donde se reservan los recursos de transmisión y conmutación de la red, el tiempo que dure dicha conexión.

En general, la transmisión se realiza a través de un conjunto de nodos, los cuales pueden estar conectados a otros nodos o directamente a equipos terminales o de abonado. La existencia de un canal dedicado entre estaciones, se da como consecuencia de la conexión sucesiva entre distintos nodos de la red, donde en cada enlace físico se dedica un canal lógico para el establecimiento de la conexión. Los enlaces entre nodos se multiplexan en FDM (Frequency Division Multiplexing) ó en TDM (Time Division Multiplexing), siendo este último el de mayor interés en este trabajo.

Una red telefónica pública de telecomunicaciones está formada por los siguientes elementos de red: (a) Equipos de abonados: son los dispositivos de usuario que se conectan a la red como un teléfono, computador, fax, entre otros. (b) Bucle de abonado: constituye el enlace entre la red y el abonado, está formado por un par de cables trenzados. (c) Centrales telefónicas: son los nodos de conmutación de la red.

(d) Líneas principales: formados por los enlaces entre centrales; transportan tráfico multiplexado en FDM o TDM sincrónico.

En la Figura 1 se muestra un esquema general de la arquitectura de una red telefónica pública:

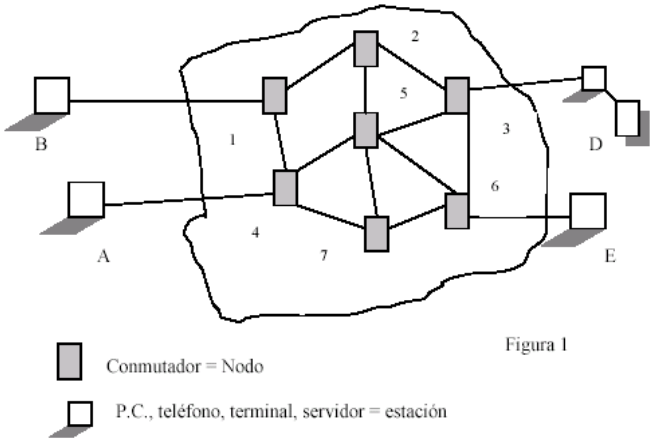


Figura 1. Esquema general de la arquitectura de una red telefónica pública

Fuente: http://www.it.uniovi.es/docencia/Telecomunicaciones/arss/material/arssTema5-Conmutacioncircuitos.pdf. [1]

La conmutación de circuitos implica tres fases: (a) Establecimiento de un circuito extremo a extremo: en la Figura 1 el nodo A envía una solicitud al nodo 4 pidiéndole una conexión con la estación E. El nodo 4 debe encontrar una ruta hacia el nodo 6 dependiendo de su tabla de enrutamiento y costo del enlace. Una vez que decide que es el nodo 5, éste toma un canal libre del enlace; el nodo 5 procede de manera similar hacia el nodo 6 y se le envía un mensaje solicitándole conexión al terminal E. (b) Envío de información: bien sea analógica o digital siguiendo el camino preestablecido en el enlace. (c) Desconexión: sucede posterior a la transferencia de información; ésta se finaliza cuando alguno de los terminales da la orden de hacerlo. El mensaje de desconexión se envía a cada uno de los nodos involucrados para que procedan con la liberación de recursos.

1.1.1 Multiplexación por división en el tiempo TDM

Este sistema de multiplexación para transmisiones digitales, se encarga de dividir el tiempo de transmisión en intervalos denominados “time slots”, los cuales son asignados a distintos canales de entrada siguiendo una ley preestablecida para esto; lo que permite recibir los canales de entrada en el receptor. A la salida, se tendrá un régimen binario que será la suma de todas las entradas ordenadas de manera estructural; este proceso se repite de manera constante en el tiempo, y a esta estructura se le denomina “trama”. El sistema TDM sincrónico es un esquema de multiplexación en donde el tiempo es obtenido desde un reloj que controla tanto el multiplexor como el canal fuente.

En la Figura 2 se muestra la creación de una trama de 2º orden jerárquico a partir de los datos provenientes de 3 canales:

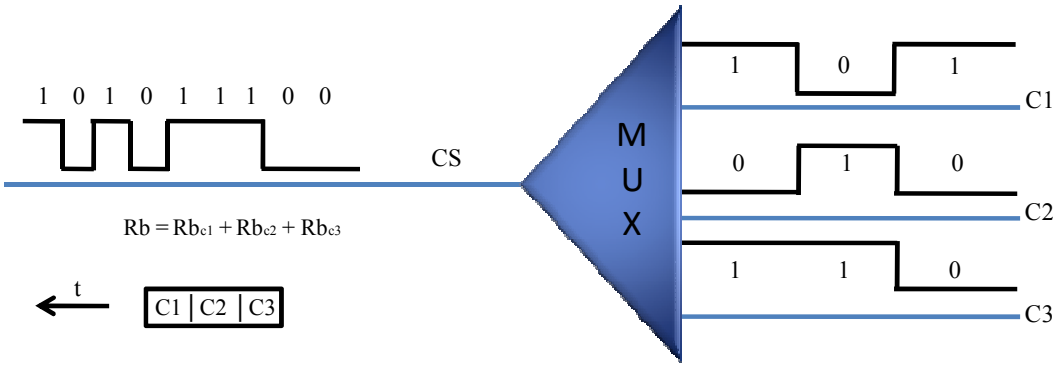


Figura 2. Creación de una trama

Fuente: Estepa, R. EN: http://trajano.us.es/~rafa/ARSS/apuntes/tema6.pdf. Digitalización de la Red Telefónica : R.D.S.I. [2]

La ITU, estableció diferentes jerarquías de multiplexación digital; una de ellas es la Jerarquía Digital Plesiócrona ó PDH (Plesiochronous Digital Hierarchy), todas controladas por equipos multiplexores con relojes de alta precisión; el primer nivel de la jerarquización está formado por un grupo primario, definido en la

recomendación G.732 para Europa, la cual agrupa 30 canales para tráfico a 64 Kb/s cada uno y dos canales de servicio, uno para uso de señalización y sincronización de multitrama y otro para sincronismo de trama y alarmas, ambos a la misma velocidad. La velocidad de transmisión del grupo básico es de 2048 Kb/s utilizando entrelazado de palabras de 8 bits, este grupo primario se le denomina E1.

A partir del E1, y utilizando entrelazado de palabras de 4 bits se forman las jerarquías superiores E2, E3, E4 y E5, las cuales llevarán 120, 480, 1920 y 7680 canales de voz respectivamente, disponiendo éstas de espacios reservados para la justificación debido a la diferencia entre los relojes que componen las señales de entrada a la trama

En la Figura 3 se muestra la estructura de una trama E1:

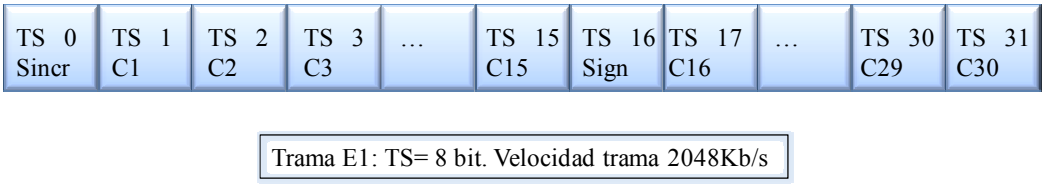


Figura 3. Trama E1.

Fuente:Ing. Héctor Figueroa. Estructura de Trama. En: www.desi.iteso.mx/telecom/comunicaciones_1/informacion/comunicacioin_digital_basica.ppt [3]

Con el uso masivo que ha tenido la fibra óptica, las velocidades de transmisión han aumentado considerablemente; dado a esto surgió una nueva jerarquía de multiplexación digital llamada SDH (Synchronous Digital Hierarchy). El nivel básico en la jerarquía SDH es el STM-1 (Synchronous Transport Module) de 155 Mb/s que es capaz de incorporar tributarios plesiócronos PDH dentro de su espacio de carga, lo que permite la convivencia entre ambas jerarquizaciones. Para los niveles superiores STM-4, STM-16, STM-32 y STM-64, la velocidad se multiplica por 4 en cada salto.

1.1.2 Señalización por canal común CCSS7 (Common Channel Signalling System 7)

Es un estándar global de telecomunicaciones creado por la UIT, el cual define los procedimientos y protocolos sobre cómo los elementos de las redes PSTN[2] (Public *Switch*ed Telephone Network) intercambian información sobre una red de señalización digital para realizar enrutamientos y control de llamadas tanto en redes alámbricas como inalámbricas. Entre los usos principales de la red CCSS7 y sus protocolos están: conexión, manejo y desconexión de llamadas y servicios de *roaming* global, entre otros. Adicional a esto, se encuentra relacionado el concepto de Red Inteligente, el cual consiste en la evolución de las redes de telefonía básica, introduciendo una nueva arquitectura de red mediante la inserción de nuevos nodos que cumplen funciones especializadas y adicionales a las que ya se cumplen en estos sistemas, que permitan un manejo eficiente de un volumen considerable de datos, junto con tecnologías de la información y modernas técnicas de manejo de bases de datos. Éstas redes permiten ofrecer servicios de tarificación especial como los números 800 y 900, reenvío de llamadas, identificación de llamadas, conferencia, llamada en espera, desvío de llamadas y servicios de redes privadas virtuales. Los elementos que conforman la red de señalización CCSS7 son:

a) **Enlaces de señalización SL (Signalling Links):** constituyen los canales bidireccionales donde se intercambian los mensajes CCSS7 entre los elementos de red a 64Kbps. La señalización ocurre fuera de banda en canales dedicados independientes de los canales de voz, esto permite una conexión

---

[2] *PSTN (Public Switched Telephone Network). Colección mundial de redes telefónicas publicas interconectadas orientadas a voz.*
Mas información en: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214316,00.html

más rápida de las llamadas, utilización más eficiente de los canales de voz y facilidad en el control de la red en general. [3]

a) **Puntos de señalización SP (Signalling Point):** los puntos de señalización utilizan una tabla de enrutamiento para seleccionar el camino de señalización apropiado para cada mensaje. Cada punto de señalización es identificado con un único código; estos códigos están presentes en cada mensaje de señalización para identificar la fuente y el destino de cada mensaje. Un tipo de punto de señalización es el STP (Signal Transfer Point), en el cual se transfieren los mensajes de señalización al enlace de señalización correcto de acuerdo a la tabla de enrutamiento que estos poseen.

Los nodos que permiten ofrecer servicios de Red Inteligentes son nombrados a continuación:

a) **SSP (Service *Switch*ing Point):** constituyen los puntos donde se originan, terminan o transitan llamadas.
b) **STP (Signal Transfer Point): SCP (Service Control Point):** envían una respuesta al nodo SSP con información del código de enrutamiento que está asociado al número discado. [3]

En la Figura 4, se muestra el esquema de una red típica de señalización CCSS7, para aplicaciones de Red Inteligente:

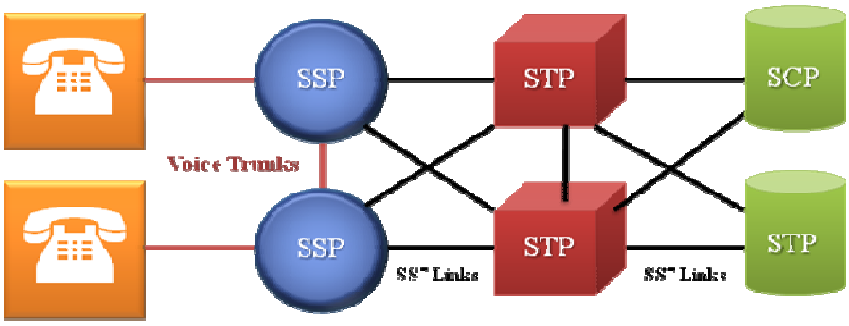


Figura 4. Esquema de Red CCSS7 para aplicaciones de Red Inteligente.

Fuente: http: //www.pt.com [4]

1.2 Redes de conmutación de paquetes

En la conmutación de paquetes, la transmisión de información es estructurada o dividida en pequeñas unidades denominadas paquetes o datagramas; cada uno de estos paquetes es transmitido de manera individual a través de la red siguiendo cualquier ruta disponible hacia el destino, en donde estos son ensamblados según una secuencia preestablecida para obtener el mensaje original. El enrutamiento de estos paquetes no se realiza por una ruta fija, su camino depende de la congestión que tengan los nodos entre el origen y el destino; esto permite que el medio no se utilice para una única transmisión. A todo lo anterior se le conoce como Técnica de Datagramas.

Informaciones como el origen, el destino, número de paquetes que conforman la información, la secuencia, el chequeo de errores, entre otros, son almacenadas en una parte del paquete denominada "cabecera ó *header*" y la información de usuario final en el "espacio de carga o *payload*".

Otra manera de llevar a cabo la conmutación de paquetes, es a través de la denominada Técnica de Circuitos Virtuales utilizada en redes orientadas a conexión, en donde se envía un paquete de control antes de los paquetes que contienen los datos; este paquete se comporta como si fuera una petición de llamada, y establece un

camino lógico de nodo en nodo, donde posteriormente se enviarán todos los paquetes con la información. Este sistema es similar al de conmutación de circuitos, pero con la salvedad de que cada nodo es capaz de mantener varios circuitos virtuales a la vez.

1.2.1 Modelo de referencia ISO (International Standards Organization) - OSI (Open System Interconnection)

La Organización Internacional de Estandarización (ISO por sus siglas en inglés) crea en 1984 una norma universal para protocolos de comunicación en respuesta a la necesidad de interconectar e inter operar redes disímiles; este concepto introdujo a un modelo referencial de sistemas abiertos, denominado OSI.

El modelo de referencia OSI está conformado por siete niveles o capas los cuáles se pueden observar en la siguiente Figura:

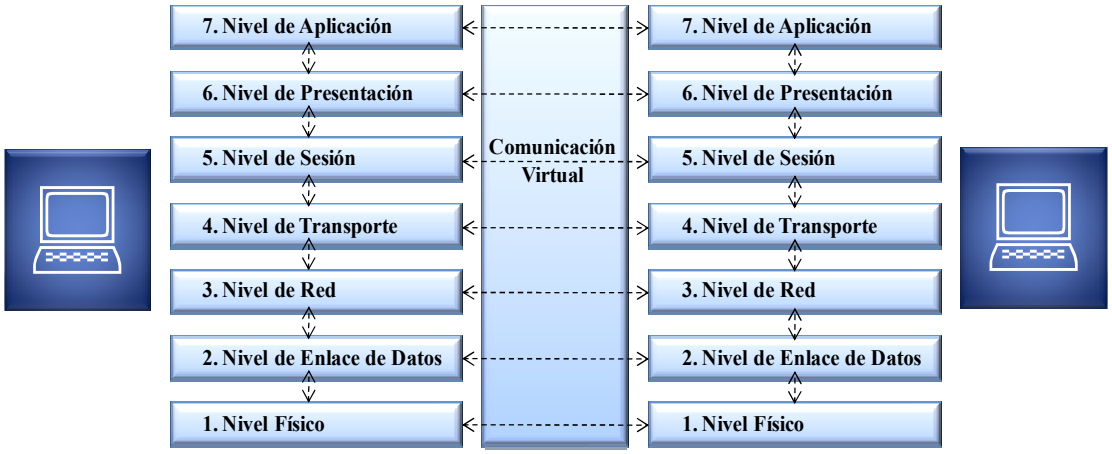


Figura 5. Modelo de referencia OSI

Fuente: http://fmc.axarnet.es/redes/tema_05.htm. [5]

a) **Nivel físico:** es el primer nivel del modelo OSI, en éste se reglamentan todas las características físicas, eléctricas y mecánicas. Esta capa es la encargada directa de la transmisión y recepción de bits a lo largo del canal de

comunicaciones, sea este satelital, por microondas, radio enlaces, cable de cobre, fibra óptica, entre otros. Por otra parte, en éste se encuentran todos aquellos dispositivos activos y pasivos que permiten la comunicación como concentradores, conmutadores, equipos de modulación, aparatos terminales, etc. Cabe destacar que el nivel físico es el encargado de adecuar los datos provenientes de la capa de enlace, en señales adecuadas para transmitir en un determinado medio.

b) **Nivel de enlace:** el nivel de enlace es el encargado de proporcionar la comunicación nodo a nodo en una red, para ello, éste proporciona las direcciones que permiten entregar los datos a los nodos correctos y a su vez traducir los mensajes provenientes de las capas superiores en bits que puedan ser transmitidos por la capa física. Estos bits los agrupa en tramas que contienen información de indicadores de inicio, dirección de origen y destino, información de control, datos e información sobre el control y detección de errores. El nivel de enlace es también encargado de gestionar y coordinar la manera en como se comparte el medio de transmisión.

c) **Nivel de red:** es el nivel encargado de proporcionar el esquema de direccionamiento que los mensajes siguen desde la fuente hasta el destino a través de encaminadores ó ruteadores (*routers*) intermedios. Éste debe ser capaz de manejar el establecimiento, mantenimiento y terminación de conexiones; así como evitar la congestión, y ser el responsable de realizar saltos de subred en caso de ser necesario. Esta capa es totalmente independiente de la capa física.

d) **Nivel de transporte:** es la que se encarga de controlar el flujo de datos entre los nodos involucrados en la comunicación; por otra parte, recibe los mensajes de la capa superior (Sesión) y los fragmenta con la responsabilidad de reensamblarlos en el orden exacto en el receptor, y así obtener el mensaje original. Estos mensajes fragmentados son entregados a la capa de red para ser enviados a su destino. La capa de transporte está relacionada con la optimización del uso de servicios de la red y con la calidad de servicio

requerida para un tipo de servicio específico, todo esto mediante el uso de los protocolos adecuados. Además, establece la transparencia de datos y asegura la confiabilidad de entrega de información entre sistemas.

e) **Nivel de sesión:** El nivel de sesión establece, maneja y termina las sesiones de comunicación. Las sesiones de comunicaciones consisten en peticiones y respuestas de servicios que ocurren entre aplicaciones localizadas en diferentes dispositivos de red. Estas peticiones y servicios son coordinadas por protocolos implementados en esta capa. Entre los protocolos más usados se encuentran: ZIP (Zone Information Protocol), AppleTalk (coordina la referencia de nombres a dispositivos), SCP (Session Control Protocol), entre otros.

f) **Nivel de presentación:** La capa de presentación provee a la red de funciones de codificación y conversión que son utilizadas por la capa superior de aplicación. Éstas funciones aseguran que la información enviada por la capa de aplicación de un sistema pueda ser entendida por otro. Algunos ejemplos de éstas son formatos comunes de representación de datos, formatos de conversión de caracteres, esquemas de compresión, encriptación, entre algunos otros. De igual manera, diferentes tipos de representación de texto y data como el código ASCII (American Standard Code Information Interchange), EBCDIC (Extended Binary Coded Decimal Interchange Code), Unicode; estándares para video como MPEG (Moving Pictures Experts Group), formatos de imágenes GIF (Graphics Interchange Format), JPEG (Joint Photographics Experts Group) y otros más, son muy utilizados en esta capa.

g) **Nivel de aplicación:** la capa de aplicación es considerada la más cercana al usuario final, y es la que representa o caracteriza el modo en que los usuarios interactúan con el ambiente OSI. Dicho nivel provee la interfaz al entorno de comunicaciones, el cual es usado por los procesos de aplicaciones. En resumen, es el encargado de comunicar los parámetros de los procesos de aplicaciones. Algunas otras funciones de la capa de aplicación son:

transferencia de información, identificación de los equipos que hacen uso de estas aplicaciones (por nombre, dirección o algún otro parámetro), sincronización entre aplicaciones, determinación de la calidad de servicio, acordar quiénes son los responsable por la integridad de la *data* y por la recuperación de errores, determinación de los recursos disponibles para la comunicación, disponibilidad de los terminales al momento de la comunicación, etc. Varios ejemplos de implementaciones de la capa de aplicación son: Telnet[3], FTP[4] (File Transfer Protocol) y SNMP[5] (Simple Mail Transfer Protocol). Un buen ejemplo de la aplicación del modelo OSI es el basamento dado al sistema de señalización CCSS7 para el desarrollo de dicho protocolo.

---

[3] Telnet. Protocolo de red utilizado para acceder en modo terminal a otro equipo terminal para su control.
[4] FTP. Protocolo con funcionamiento en las redes TCP con funcionamiento en la capa de aplicación que se utiliza para el intercambio de archivos entre equipos.
[5] SNMP. Parte de la suite de protocolos TCP/IP, trabaja en la capa de aplicación y es usado para manejar información de administración de las rede,s como por ejemplo el monitoreo.

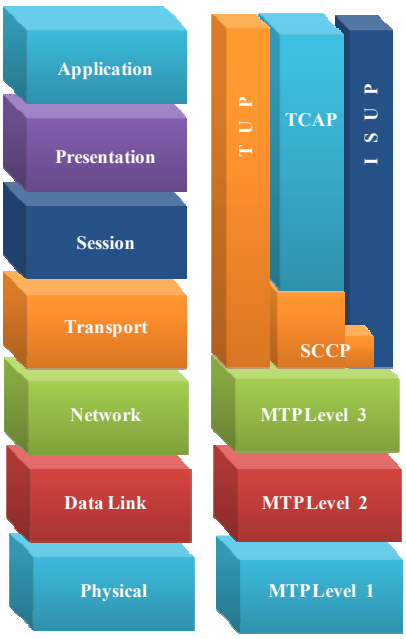


Figura 6. El modelo de referencia OSI y protocolo CCSS7.

Fuente: http: //www.pt.com [4]

1.2.2 Modelo TCP (Transmission Control Protocol) / IP

Este modelo surge a partir de los años 70 tras el financiamiento del Departamento de Defensa de los EE.UU (Estados Unidos) a través de ARPA (Advanced Research Projects Agency); la red informática de ARPA, denominada ARPANET (Advanced Research Projects Agency Network), estaba constituida por redes que interconectaban varias universidades, laboratorios y centros de investigación en Estados Unidos; esta red dio comienzo a lo que hoy se conoce como Internet.

"El TCP/IP no es un único protocolo, sino que es en realidad un conjunto de protocolos que cubren los distintos niveles del modelo OSI"[6]. [1]. Los protocolos más importantes que lo conforman son el TCP y el IP, el conjunto TCP/IP está formado por cuatro niveles o capas:

a) **Capa de aplicación:** constituye todos los protocolos de alto nivel como el SMTP, Telnet, FTP y HTTP[7] (HyperText Transfer Protocol), así como la representación, codificación, control de sesión y correcta paquetización de datos para ser presentados al nivel inferior. Esta capa corresponde con las capas de aplicación, presentación y sesión del modelo OSI.
b) **Capa de transporte:** nivel que da base a transmisiones de datos confiables, con control de flujo y detección de errores. Utiliza TCP como protocolo principal y coincide con la capa de transporte del modelo OSI.
c) **Capa de Internet:** esta capa se encarga de identificar si cada datagrama debe ser procesado de manera local o si debe ser transmitido; asignando para esto la ruta adecuada dependiendo de la información contenida en la cabecera del mensaje. Corresponde al tercer nivel del modelo OSI ó de Red, y el protocolo principal utilizado es el IP.
d) **Capa de acceso de red:** su principal función consiste en encapsular los datagramas en tramas y mapear las direcciones IP en direcciones físicas; todo esto con el fin de realizar el enlace para la transferencia de información. Este nivel cumple con las funciones de la capa 1 y 2 (Físico y Enlace) del modelo OSI.

---

[6] *Disponible en: http://r_marca.pe.tripod.com/pagina1.htm*
[7] *HTTP. Protocolo que se encarga del control de acceso y respuestas de contenidos provenientes de entornos web.*

En la Figura7 se muestra el modelo TCP/IP y su relación con el modelo OSI:

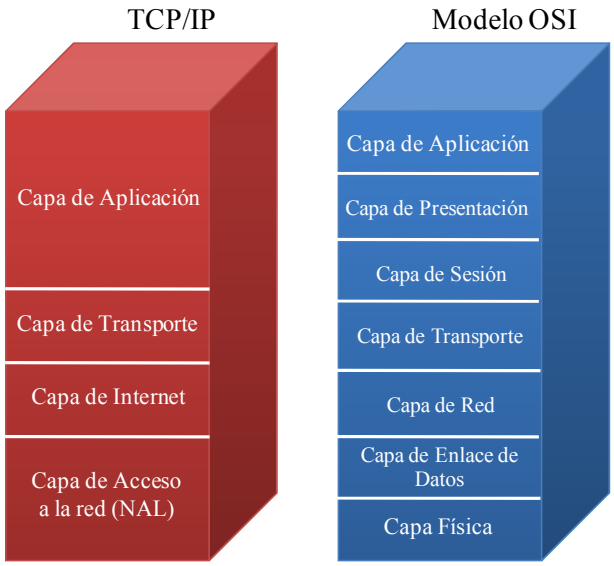


Figura 7. TCP/IP y el modelo OSI

Fuente: http: //www.textosciientificos.com/redes/tcp-ip/comparación-modelo-osi [6]

1.2.3 El Protocolo de Internet

IP es un protocolo de capa de red, el cual contiene información de direccionamiento y alguna información de control que permite el enrutamiento de los paquetes. Este protocolo fue diseñado para ser usado en redes que utilizan conmutación de paquetes; el mismo se encuentra documentado en la RFC 791 (Request For Comments) de la IETF[8]. IP proporciona todas las funciones necesarias para el envío de un paquete desde el origen a su destino, pero sin embargo no garantiza el envío de mensaje de extremo a extremo ó *end to end*. Para contrarrestar

[8] *IETF: Internet Engineering Task Force es una amplia y abierta comunidad internacional de diseñadores, operadores, vendedores e investigadores vinculados con el desarrollo de Internet y de la arquitectura de redes.*

dicha limitante, IP se vale de los servicios que ofrecen los protocolos de nivel de enlace para así proporcionar diferentes tipos de garantía y de calidades de servicio.

Mediante el uso de enrutadores o *routers*, el protocolo IP tiene entre sus funciones, encaminar de manera eficiente los paquetes de acuerdo a la dirección de destino y otros campos ubicados en la cabecera de los mismos. Otra función importante es la de fragmentar y reensamblar los paquetes IP dependiendo si el tipo de red requiere o no que éstos sean más pequeños.

El protocolo IP presta su servicio utilizando la información de los siguientes campos de cabecera:

a) **Versión:** utilizando 4 bits, este sector identifica la versión del protocolo utilizado para transmitir el mensaje, por ejemplo si es IPv4[9] ó IPv6[10].
b) **IHL (Internet Header Length):** en este campo se indica la longitud de la cabecera del datagrama en palabras de 32 bits.
c) **ToS (Type of Service):** indica los parámetros para el tipo de servicio requerido, dichos parámetros pueden ser utilizados por las redes para definir cómo debe ser tratado el paquete en su transporte; además en este campo se asigna el nivel de importancia del datagrama, esto para dar prioridades al momento del enrutamiento.

---

[9] IPv4: Es la primera versión del protocolo de internet que está actualmente en uso; tiene capacidad para algo más de 4 mil millones de direcciones, las cuales no serán suficientes para las necesidades del futuro.
Mas información en: http://www.arin.net/media/fact_sheets/Spanish/IPv4_IPv6_spanish.pdf
[10] IPv6: Lanzado en 1999, se presenta como el substituto de la versión 4, soporta una cantidad muy superior de direcciones en comparación a su antecesor. Creado con el fin de dar solución a tecnologías futuras, incluido en esto el uso de dispositivos móviles. Mas información en: http://www.arin.net/media/fact_sheets/Spanish/IPv4_IPv6_spanish.pdf

d) **Longitud total:** donde se especifica el número total de octetos que conforman el datagrama. Posee un campo máximo de representación de 16 bits o 65.535 octetos.
e) **Identificación:** contiene un valor que identifica el datagrama; con el uso de este campo se posibilita el reensamblaje en el destino de los distintos fragmentos que conforman el mensaje.
f) **Banderas (Flags):** consiste de un campo de 3 bits, en los cuales los dos menos significativos son bits de control de la fragmentación, uno que indica cómo el paquete puede ser fragmentado y el otro indica si el datagrama contiene fragmentos adicionales; el último bit no está en uso.
g) **Posición del fragmento:** indica la posición relativa del fragmento respecto al inicio de la data en el datagrama original, lo cual permite al destino la correcta reconstrucción del mismo.
h) **TTL (Time to Live) ó Tiempo de Vida:** es un campo de temporización utilizado para seguir el tiempo de vida de un datagrama, cuando este decrementa hasta cero tras el paso por nodos, el paquete es descartado.
i) **Protocolo:** indica qué protocolo de capa superior recibe los paquetes luego de todo el procesamiento IP
j) **Suma de control de cabecera:** contiene una suma de comprobación de los datos de la cabecera, esto permite conocer si la información ha sido recibida correctamente.
k) **Dirección fuente:** identifica mediante 32 bits el nodo que envía el mensaje.
l) **Dirección destino:** especifica con un campo de 32 bits el nodo receptor.
m) **Opciones:** campo que no es de uso obligatorio; puede ser utilizado con propósitos de encaminamiento, seguridad, entre otros.
n) **Relleno (Padding):** utilizado para rellenar con ceros el encabezado IP, asegurando que éste sea siempre múltiplo de 32 bits.

En la Figura 8 se muestra la estructura de una cabecera IPv4:

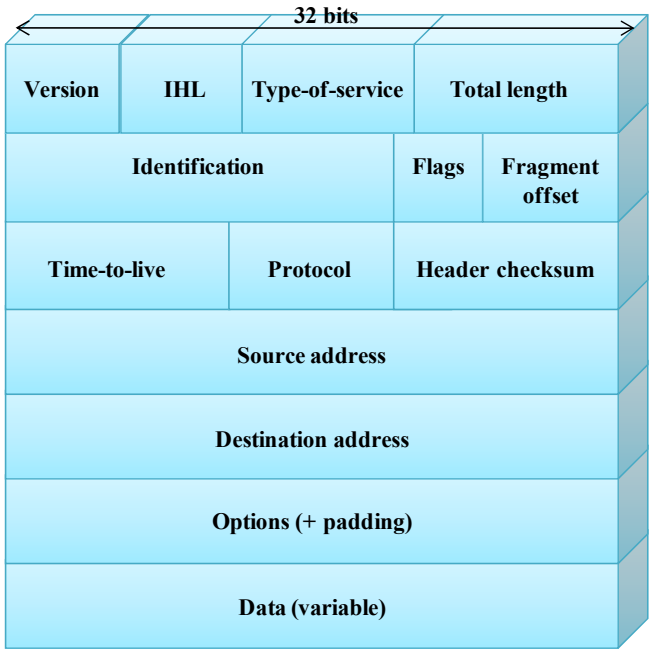


Figura 8. Cabecera IPv4

Fuente: Huidobro, José Manuel – Martínez, David. Tecnología VoIP y Telefonía IP. (Libro). España, 2006. p. 160. [7]

La dirección de Internet ó dirección IP es la encargada de identificar tanto al equipo terminal como a la red a la que pertenece; esto con el fin de distinguir a todos los equipos que se encuentren en diversas redes. Para tal fin, la ICANN (Internet Corporation for Assigned Names and Numbers) asigna direcciones según tres clases diferentes basadas en los tamaños de las mismas. Éstas son:

a) **Clase A:** utilizada en redes muy grandes, generalmente por gobiernos en todo el mundo y grandes corporaciones. En esta clase el primer octeto es utilizado para identificar la red, el primer bit es siempre cero y sólo se permite direccionar a 126 de las 128 redes posibles (las direcciones 0.0.0.0 y 127.0.0.0 están reservadas). Los tres últimos octetos permiten direccionar a

16.777.214 nodos (los tres últimos octetos a 255 y a 0 están reservados de igual forma). Se les conoce también como /8 (barra ocho).

b) **Clase B:** utilizadas en mayor parte en medianas Empresas; esta clase utiliza los dos primeros octetos para identificar la red, en donde el primer bit es asignado a 1 y el segundo a 0; con esto existen 16.384 posibles redes y 65.536 nodos distintos por red. Se dice que esta clase contiene un aproximado del 25% de los números de direcciones posibles del sistema IPv4. También conocidas como /16 (barra dieciséis).

c) **Clase C:** en esta clase se engloban al resto de los solicitantes de direcciones. Los tres primeros octetos son usados para identificar la red, con valor fijo de 110 para el primero, segundo y tercer bit respectivamente. Ofrece 2.097.152 direcciones de red y 254 direcciones de hosts para cada red. Se les denomina también /24 (barra veinticuatro).

En la Figura 9 se observa la estructura de las clases de direcciones:

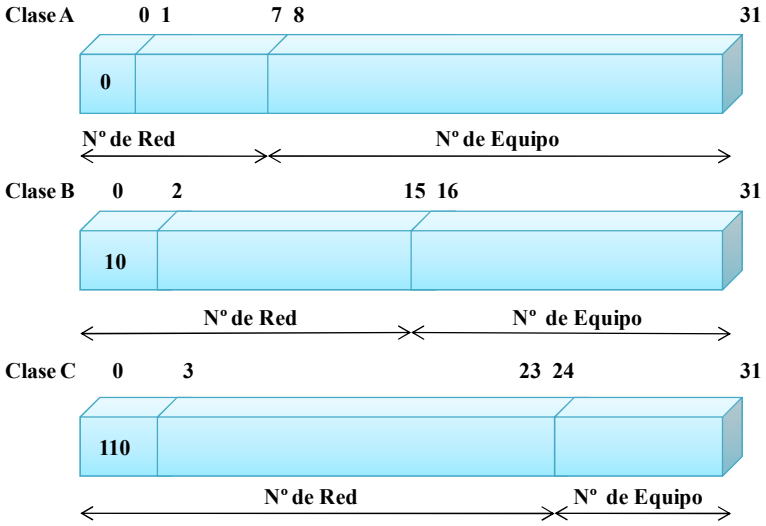


Figura 9. Clases de direcciones IP

Fuente: Huidobro, José Manuel – Martínez, David. Tecnología VoIP y Telefonía IP. (Libro). España, 2006. p. 160. [7]

Tabla 1. Representación decimal de las direcciones IP de cada clase

Direcciones IPv4	Dirección Mínima de Red	Dirección Máxima de Red	Direcciones de Red Posibles	Direcciones de Host Posibles
Clase A	1.xxx.xxx.xxx	126.xxx.xxx.xxx	126	16.777.216
Clase B	128.0.xxx.xxx	191.255.xxx.xxx	16.384	65.536
Clase C	192.0.0.xxx	223.255.255.xxx	2.097.152	254

Para efectos de direccionamiento, son muy usados hoy en día los conceptos de subredes y súper redes.

1.2.4 Redes LAN (Local Area Network)/WAN (Wide Area Network)

Las redes LAN o Redes de Área Local se definen como redes de comunicaciones de alta velocidad que utilizan un medio compartido para interconectar dispositivos y aplicaciones, que permitan el intercambio de información entre distancias relativamente pequeñas, usualmente no mayores a 3 Km para medios eléctricos y menores a los 200 Km para medios ópticos.

Las redes LAN utilizan tecnología de difusión (broadcast) para transmitir datos mayormente a través de medios compartidos a velocidades comprendidas entre 1 Mbps y 10 Gbps, utilizando para esto diferentes tipos de cableados entre los cuales se pueden conseguir los cables coaxiales, de par trenzado y de fibra óptica.

Otro tipo de redes son las de Área Extensa o WAN, las cuales son concebidas como redes que interconectan subredes y/o equipos de redes que se encuentran a largas distancias, bien sean países o continentes. Dada esta característica, las redes WAN suelen ser de uso público o redes públicas, que a diferencia de las redes LAN, no son de uso exclusivo de una organización o empresa,

sino que al contrario, son utilizadas para interconectar diferentes organizaciones y usuarios pertenecientes a distintas redes alrededor del mundo.

Por otra parte, las redes WAN se caracterizan por transmitir voz, datos y video a menor velocidad que las LAN pero con un volumen de tráfico mucho mayor, dado a que éstas cursan datos provenientes de numerosas redes.

1.2.4.1 Estandarización de redes LAN

Gran parte de las redes LAN han sido estandarizadas por la IEEE (Institute of Electrical and Electronic Engineers) mediante un grupo de trabajo denominado 802; estos grupos de trabajo son los encargados de la investigación de nuevas técnicas y protocolos aplicables a las redes, donde son discutidos para su posible estandarización.

De los estándares asociados al grupo 802, son relevantes para esta investigación el 802.3u, 802.3z y el 802.1Q correspondientes a redes FastEthernet GigaEthernet y Redes de Área Local Virtuales ó VLAN respectivamente.

En general, las redes Ethernet conforman la tecnología LAN más utilizada actualmente por su ventaja de poder transmitir tráfico esporádico y pesado a velocidades elevadas. Éstas utilizan como método de acceso el denominado Método CSMA/CD (Carrier Sense Multiple Access with Collision Detection) ó Acceso Múltiple con Detección de Portadora y Detección de Colisiones; este método consiste en que todos los equipos de red son capaces de acceder al mismo medio, sólo que el envío de información se realiza de a uno por vez, es decir, sólo puede existir un único emisor para cada instante de tiempo, lo que evita posibles colisiones de paquetes en la red. Las redes Ethernet se pueden diferenciar según su velocidad de transmisión en: 10Base5, 10Base2 y 10BaseT, definiendo el tipo de cableado, distancias y topologías a usar en cada estándar.

Por otra parte, las redes Ethernet están basadas en topología de Broadcast, en donde cada equipo es capaz de ver todas las tramas encontradas en la red, así no sean éstos el punto de destino de una determinada información; el descarte de estos paquetes se realiza con la verificación de dirección destino en la cabecera del datagrama.

La construcción de las tramas Ethernet sucede a través de un proceso llamado encapsulamiento, en donde cada capa por donde pasan estos paquetes va añadiendo cabeceras y datos adicionales que permiten rastrear y administrar éstos a lo largo de toda la red de manera que lleguen de forma satisfactoria a su destino.

La Figura 10 muestra un proceso de encapsulamiento en una red Ethernet:

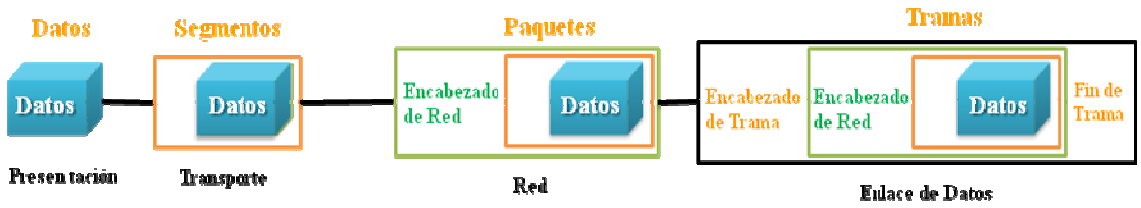


Figura 10. Encapsulamiento en una red Ethernet

Fuente: Quiroz M, Rafael. Evaluación de factibilidad para la migración de la plataforma actual hacia telefonía IP en la Red del BCV. Trabajo de Grado. Caracas, 2006. [8]

1.2.4.1.1 Redes FastEthernet

Las redes FastEthernet están soportadas bajo el estándar 802.3u y ofrecen un incremento de velocidad de hasta 10 veces más que la especificación 10BaseT (hasta 100Mbps), manteniendo los mismos esquemas de funcionamiento, como resolución

de direcciones MAC (Media Access Control)[11], formatos de tramas, entre otros; estas similitudes permiten el uso de aplicaciones y herramientas de manejo de redes 10BaseT sobre redes FastEthernet.

1.2.4.1.2 Redes Gigabit Ethernet ó GigaEthernet

El estándar que soporta las redes GigaEthernet ó 802.3z fue aprobado por la IEEE en el año 1998, pensado para ser el estándar predominante en núcleos de redes de alta velocidad; su desarrollo está basado de igual manera en el protocolo Ethernet, pero es capaz de proveer velocidades de hasta 1000Mbps ó 1Gbps; esto fue logrado gracias al cambio en las interfaces físicas, pero a su vez manteniendo todas las características de las redes Ethernet como acceso CSMA/CD, formatos de tramas y todo el resto de compatibilidades involucradas con el estándar Ethernet. Este desafío se resolvió uniendo a dos tecnologías, IEEE 802.3 y ANSI (American National Standards Institute)[12] X3T11 para canales de fibra óptica.

---

[11] Dirección MAC (Media Access Control): es un valor único de identificación asociado a un adaptador de red, suele llamarse dirección de hardware o dirección física. Está representada por doce dígitos hexadecimales ordenados de la forma AA:AA:AA:AA:AA:AA .
Más información en: http://compnetworking.about.com/od/networkprotocolsip/l/aa062202a.htm
[12] ANSI. American National Standards Institute. Organización sin fines de lucro que supervisa el desarrollo de estándares para productos, servicios y sistemas en los Estados Unidos. De igual forma coordina la compatibilidad de estos estándares con el resto del mundo. Más información en: http://es.wikipedia.org/wiki/ANSI

La siguiente Figura representa un Protocolo Gigabit Ethernet:

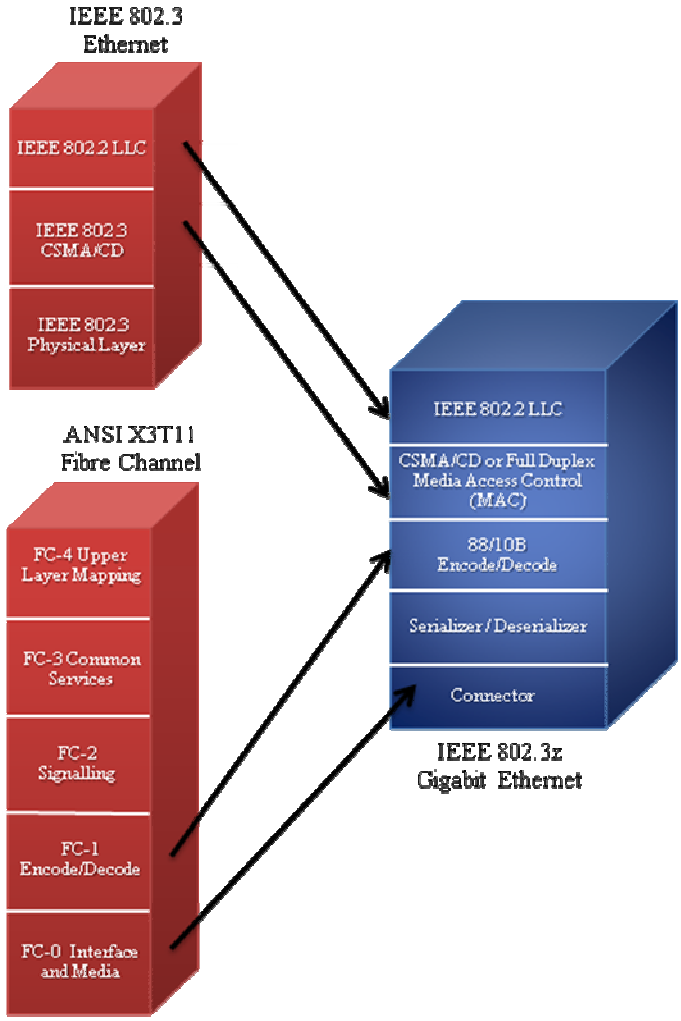


Figura 11. Protocolo Gigabit Ethernet

Fuente: http://donatello.icesi.edu.co/~redesi/exposiciones/Ethernet_SesionNo_TELEMATICA.pdf. Presentación en Línea. [9]

1.2.4.1.3 Redes LAN Virtuales ó VLAN (Virtual Local Area Network)

Las redes de Área Local LAN fueron originalmente definidas como una red de computadores localizados en la misma área; hoy en día estas redes son definidas como un simple dominio de difusión ó *broadcast*, esto significa que si un usuario transmite una información, esta puede ser recibida por el resto de usuarios de la LAN. Muchas veces esto no suele ser tan ventajoso dado a que no todo el tráfico es útil a todas las estaciones de la red, provocan retrasos y colisiones de tráfico.

Para solventar dichos problemas, surge el concepto de Redes de Área Local Virtuales, el cual consiste en hacer que redes de computadores conectadas en un mismo *switch* sean lógicamente independientes, es decir, divide en diferentes dominios de *broadcast* a un *switch* con la intención de crear dominios más pequeños que no se afecten unos a otros con mensajes de *broadcast* y permitan un funcionamiento más eficiente.

La flexibilidad obtenida de este estándar respaldado por la IEEE mediante su grupo de trabajo 802.1Q, data en que es posible tener equipos geográficamente apartados (zonas distantes, edificios, entre otros), y aún así que éstos pertenezcan al mismo segmento de red, situación útil si se quieren crear grupos virtuales de aplicaciones, trabajando con un rendimiento mayor y con una capacidad de administración considerablemente más sencilla.

Las VLAN trabajan en la capa de enlace del modelo OSI y el transporte de sus datos suele hacerse en enlaces troncalizados (trunking) capaces de transmitir tráfico de diferentes VLAN, los cuales son identificados y diferenciados (voz, datos o video) con etiquetas en sus mensajes; estas troncales suelen ser enlaces de *switch* a *switch* o de *switch* a encaminador ó *router*.

1.3 Telefonía IP y VoIP (Voice over IP)

Desde la década pasada la industria de las telecomunicaciones ha sido testigo de impresionantes cambios en la manera como las personas y las organizaciones se comunican. Muchos de estos cambios son consecuencia del crecimiento explosivo de Internet y de aplicaciones basadas en el Protocolo de Internet IP.

Es claro para las Empresas de telecomunicaciones actuales que el tráfico de voz y los servicios serán una de las mayores aplicaciones que sacarán gran provecho de IP y sus ventajas, esto basado en una serie de nuevas tecnologías conocidas como voz sobre IP, VoIP ó telefonía IP.

Es en los años 90 cuando organizaciones como la ITU, la IETF y la IEEE comenzaron a establecer una serie de parámetros y recomendaciones para la transmisión de voz a través de redes IP, con lo cual pretendían estandarizar los protocolos y las tecnologías a implementar para asegurar la fácil y segura interconexión de productos de distintos fabricantes para el correcto funcionamiento de las redes que involucran servicios de VoIP.

La VoIP no es más que el transporte vía Internet de servicios como voz, facsímil y aplicaciones de mensajería en lugar del transporte tradicional de éstos a través de redes telefónicas tradicionales (PSTN); en esta tecnología se encuentran involucrados procesos como la conversión de señales de voz analógicas en formatos de voz digital, así como la compresión y traducción de señales en paquetes IP para su transmisión sobre Internet. El objetivo principal que persigue la telefonía sobre Internet es la de proveer un servicio rentable y de alta calidad, similar a la que espera un usuario de una red telefónica tradicional.

1.3.1 Protocolos de VoIP

1.3.1.1 Protocolos de digitalización de voz

Como es sabido, los primeros sistemas telefónicos transmitían la voz mediante señales analógicas. Tras la evolución de la electrónica y de los circuitos integrados, la digitalización de voz se convirtió en un paso importante para solventar muchos de los problemas que tenían los primeros sistemas de voz, como control y señalización complejos, falta de encriptación, baja tolerancia a ruido, entre otros. Las técnicas de muestreo, cuantificación y codificación hicieron posible la digitalización de la voz mediante un esquema de modulación muy utilizado en entornos telefónicos como lo es la Modulación por Codificación de Pulsos ó PCM (Pulse Code Modulation)[13].

La codificación, entendida como el proceso completo de digitalización y compresión de la voz es lograda a través de un módulo codificador/decodificador (codec) que además de realizar la compresión analógica/digital, comprime la secuencia de bits y proporciona la cancelación de eco. Esta codificación puede ser realizada mediante tres técnicas principales: por codificación de forma de onda, por codificación basada en modelos matemáticos (algoritmos) sobre la producción de voz, y por modelos que combinen ambas técnicas. El ahorro del ancho de banda es una de las principales razones por la que se busca realizar este tipo de codificaciones de la voz para ser transmitidas sobre redes digitales como las basadas en IP. Los codecs tendrán a su salida una secuencia de bits que se empaquetan en paquetes IP,

---

[13] PCM. Esquema de modulación que representa de manera digital una señal análoga, donde la magnitud de dicha señal es muestreada regularmente en intervalos uniformes, para luego ser cuantificada en una serie de símbolos binarios, generalmente cada muestra de voz es representada por 8 bits y muestreada a 8000 muestras/seg para conforman un flujo de información de 64 kbps. Disponible en: http://www.cisco.com/warp/public/788/signalling/waveform_coding.pdf

los cuales son transportados por la red IP hacia el destino, el cual debe estar preparado con los mismos estándares para realizar el proceso inverso, y así lograr una comunicación inteligible. Hay que considerar que a mayor sea la compresión usada, menor es la calidad de la voz lograda; además se tendrá un mayor consumo de recursos de procesamiento en los equipos involucrados.

La ITU cubre entre sus protocolos, los correspondientes a codificación de voz, agrupados éstos en las recomendaciones G.7xx. En la Tabla 2 se muestran los códec comúnmente usados en telefonía.

Tabla 2. Codecs comunes en telefonía

Codec	**Ancho de Banda (Khz)**	**Intervalo muestra(ms)**	**Aplicación**
G.711 (PCM)	64	10	Telefonía
G.721 (ADPCM*)	32	10	
G.723.1 (MP-MLQ*)	6,3	30	Telefonía Internet
G.723.1 (ACELP*)	5,3	30	Telefonía Internet
G.726 (ADPCM*)	32	5	Telefonía
G.729 (CS-ACELP*)	8	10	Telefonía

**ADPCM (Adaptive Differential Pulse Code Modulation), MP-MLQ (Multipulse Maximum Likelihood Quantization), ACELP (Algebraic Code Excited Linear Prediction), CS-ACELP (Conjugate Structure Algebraic Code Excited Linear Prediction)*

1.3.1.2 RTP (Real Time Protocol)

Estándar que define las comunicaciones de audio y video en tiempo real que son cursadas a través de redes IP, lo que lleva a entender que es un protocolo adaptado a soportar la existencia de pérdidas, retardos y a la variación dinámica de las condiciones por las que pasa toda red de esta naturaleza. Da funciones de transporte extremo a extremo, además de ofrecer servicios como identificación de la información transportada, numeraciones de secuencia, marcas temporales, entre otras.

Los paquetes RTP constan de una cabecera, la cual contiene información para poder rearmar el flujo de bits generado por el códec emisor y otra parte de carga útil donde va el propio flujo de bits. La Figura 12 muestra la estructura de una cabecera RTP.

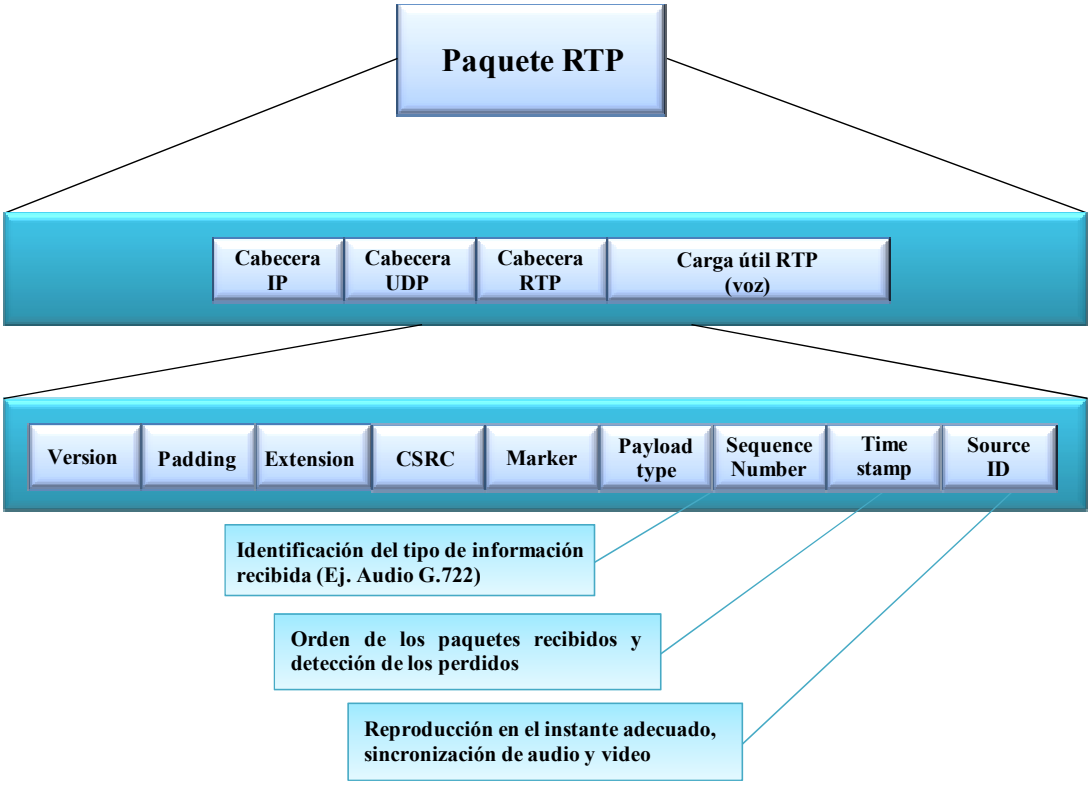


Figura 12. Estructura de la cabecera RTP

Fuente: Huidobro, José Manuel – Martínez, David. Tecnología VoIP y Telefonía IP. (Libro). España, 2006. p. 146. [7]

1.3.1.3 H.323

El estándar H.323 es un estándar (ITU-T) que permite la transmisión de audio, video y datos a tiempo real a través de redes basadas en transmisión de paquetes, sus aplicaciones se extienden a áreas como consumidores, Empresas y aplicaciones de entretenimiento. Está pensado para dar solución a necesidades de

comunicaciones de servicios multimedia a través de redes LAN y WAN. Este estándar está especificado por el grupo de estudio 16 de la ITU-T (ITU Telecommunication Standardization Sector) y engloba a otros protocolos especificados más adelante.

El estándar hace uso de elementos de red como terminales, gateways, gatekeepers y MCU (Multipoint Control Unit), este último empleado en comunicaciones simultáneas de más de dos usuarios, donde los flujos de audio y video son distribuidos entre los participantes de la multiconferencia.

H.323 está conformado por una suite de protocolos de la ITU, éstos y sus funcionalidades son presentados en la Tabla 3:

Tabla 3. Protocolos usados en H.323

Protocolos	Característica
H.225 Q.931	Manejo de inicialización y fin de llamadas. Paquetización, sincronización e inicio de llamadas mediante mensajes de señalización Q.931
H.225 RAS*	Registro, Admisión y Status de terminales en gatekeepers H.323
H.235	Autentificación y otras opciones de seguridad
H.245	Negociación de capacidades y manejo de canales lógicos
RTP	Comunicación de audio y video en tiempo real.
RTCP*	Control de mensajes relacionados con calidad de servicio, además de información como identificación, sincronización, y control de sesión
H.261/263	Codificación de video
G.7xx	Codificación de audio
T.120	Control de conferencias punto-punto, punto-multipunto

*RAS (Registration, Admission, Status), RTCP (Real Time Control Protocol)

La Figura 13 muestra la arquitectura de una red H.323:

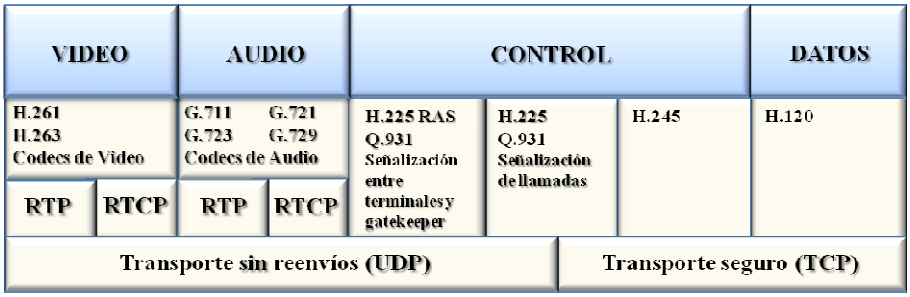


Figura 13. Arquitectura de red H.323

Fuente: Quiroz M, Rafael. Evaluación de factibilidad para la migración de la plataforma actual hacia telefonía IP en la Red del BCV. Trabajo de Grado. Caracas, 2006. [8]

1.3.1.4 SIP (Session Initiation Protocol). Protocolo de Inicio de Sesiones

Estándar publicado por la IETF en el año 1.999 como alternativa a H.323 bajo la RFC 3261, está caracterizado como un protocolo de control de la capa de aplicación el cual define cómo establecer, modificar o finalizar sesiones entre dos o más extremos sin importar el tipo de sesión que sea.

En contraste a H.323, en SIP sólo se definen los elementos que participan en un entorno SIP y el sistema de mensajes que intercambian. Los mensajes en SIP están basados en HTTP y son empleados en funciones de registro, además se usan para establecer qué direcciones IP y puertos TCP y UDP (User Datagram Protocol)[14] serán los encargados de intercambiar información. Esta puede ser la característica por la

[14] *UDP. User Datagram Protocol. Protocolo base de IP, permite el intercambio de datagramas entre aplicaciones en una red con minima utilización de protocolos. No garantiza que los paquetes lleguen en orden, duplicados ó se pierdan. Utilizado comúnmente por servicios que no requieren garantía de entrega ni calidad de servicio. Mas informacion en: http://www.faqs.org/rfcs/rfc768.html*

cual SIP se perfila como el protocolo por excelencia para desarrollar aplicaciones como telefonía y videoconferencia sobre redes IP. Otros de los protocolos utilizados en SIP, al igual que en H.323, son UDP y RTP para el transporte, H.26x para la compresión de video y G.7xx para la compresión de voz.

Otra gran ventaja es el basamento de SIP en el modelo de Internet y el uso del código de texto ASCII al igual que el de HTTP; el direccionamiento se hace de manera similar al del correo electrónico -*User@host*-, pudiendo ser *User* un nombre o un número telefónico.

SIP utiliza una arquitectura del tipo cliente/servidor, es decir, un cliente manda una solicitud, el servidor la procesa y envía una respuesta a dicho solicitante. Es considerada de igual manera una arquitectura descentralizada (peer-to-peer) donde gran parte de la inteligencia reside en los equipos terminales. Por otra parte, el estándar es capaz de distinguir los elementos que lo conforman; estos elementos son:

Los elementos que conforman una arquitectura SIP son:

a) **Agentes de usuario ó UA(User Agent):** corresponde a los equipos terminales de donde se originan las peticiones para inicio o culminación de llamadas, están formados por los UAC (User Agent Client) que inician las sesiones SIP y los UAS (User Agent Server) responsables de aceptar las peticiones recibidas. Ejemplos claros de UA son un teléfono IP y un softphone (Software que simula un teléfono tradicional).
b) **Servidor proxy:** entidad intermedia que puede actuar como servidor o como cliente, debido a que se encarga de servir las peticiones internamente o redireccionarlas hacia otros servidores dependiendo a donde se dirija dicha petición.

c) **Servidor de localización:** es el encargado de dar información constante de la localización de usuarios en la red, de manera que éstas lleguen al destino correcto en un instante de tiempo.
d) **Servidor de redirección:** es el encargado de responder a la resolución de nombres de usuario (mapeo de direcciones). A diferencia de los servidores proxy, los de redirección no inician peticiones SIP, ni son capaces de aceptar o terminar llamadas.
e) **Servidor de registro:** acepta las peticiones de registro de los UAC, y almacena la información de ellos en una base de datos de localización.

Todas las peticiones, excepto la ACK (Acknowledge), tienen asociadas una respuesta del servidor, dicha respuesta tiene asociado un código numérico indicando el resultado de la petición, códigos tomados de *http*. La Tabla 4 muestra las peticiones y respuestas con sus respectivas funciones.

Tabla 4. Peticiones y respuestas SIP

Peticiones SIP	***Funciones***
INVITE	Mensaje de invitación enviado por el llamante
ACK	Respuesta del agente llamante ante mensaje de aceptación de llamada por parte del destino
BYE	Terminación de sesión
CANCEL	Cancelación de petición pendiente
REGISTER	Empleado por usuarios para el registro de su dirección de contacto actual
OPTIONS	Para hacer consulta de capacidades, por ej. Codecs
INFO	Información fuera de banda como DTMF
Respuestas SIP	***Funciones***
1xx	Mensajes de Información
2xx	Éxito
3xx	Mensaje de desvío
4xx	Error en la petición
5xx	Error de servidor
6xx	Error generalizado

En la siguiente Figura se muestra la manera cómo se ejecuta una llamada en SIP, mostrando los mensajes de petición y respuesta de cada UA y de los servidores normalmente involucrados.

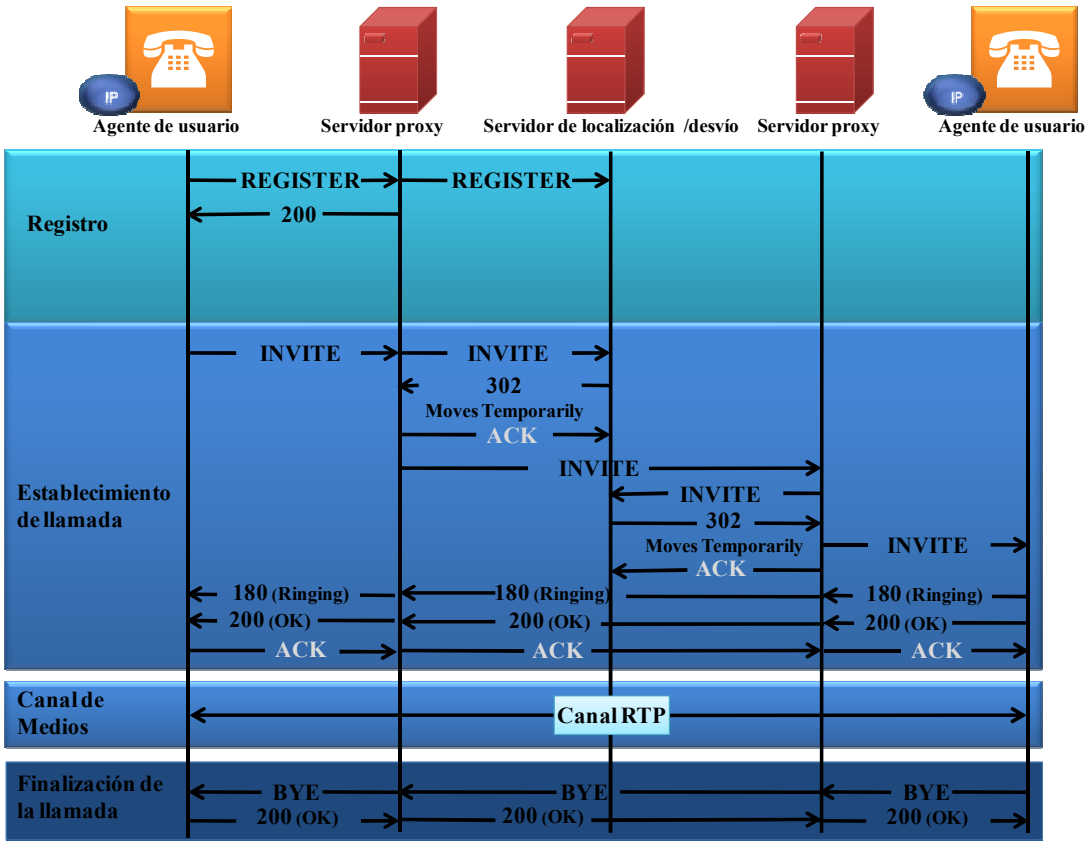


Figura 14. Llamada haciendo uso de SIP

Fuente: Huidobro, José Manuel – Martínez, David. Tecnología VoIP y Telefonía IP. (Libro). España, 2006. p. 160. [7]

De la figura anterior se pueden resumir los siguientes pasos básicos necesarios para llevar a cabo una llamada en SIP:

a) Registro, iniciación y localización del usuario.
b) Descripción del tipo de sesión a establecer.
c) Aceptación de la petición.
d) Establecimiento de la llamada.

e) Comunicación.
f) Terminación de la llamada.

1.3.2 Elementos de una red de VoIP

La posibilidad de codificar y encapsular la voz para luego enrutar estos paquetes es la base de toda red capaz de soportar servicios de voz sobre IP. Para que esto se lleve a cabo sin contratiempos, es necesario que dicha red contenga algunos elementos básicos que permitan el funcionamiento de la misma y se adapte a las exigencias que esta tecnología requiere. Algunos de los elementos a explicar no son indispensables para el establecimiento de llamadas VoIP, pero son de relevancia para esta investigación.

1.3.2.1 Infraestructura IP

Los primeros elementos básicos a considerar en toda red IP son:

a) **Estaciones de Trabajo:** es la interfaz directa donde se ejecutan las aplicaciones mediante las cuales los usuarios transmiten y reciben información, los computadores a pesar de estar conectados a una red tienen capacidad de funcionar de manera independiente sin compartir datos con otros equipos.
b) **Tarjeta de Interfaz de Red:** es un dispositivo electrónico colocado en los computadores mediante el cual el equipo es capaz de comunicarse con el resto de la red, se les conoce también como NIC (Network Interface Card).
c) **Servidor:** se refiere a una aplicación de software cuya finalidad consiste en proveer de servicio a estaciones remotas llamadas clientes. La naturaleza de estos servicios es muy variada, va desde el aprovisionamiento de archivos a los clientes hasta compartir recursos como impresoras, unidades de lectura,

entre otros. El termino servidor comúnmente se usa para referirse también al equipo físico en donde funciona este software.

d) **Concentradores ó Hubs:** equipo que permite centralizar el cableado de red, este dispositivo tiene la característica de repetir los datos en cada uno de sus puertos de manera que cada red o equipo conectado a éstos tiene acceso a los mismos. La topología emergente de estos hubs es de tipo estrella.
e) **Bridges:** estos dispositivos se encargan de conectar diferentes segmentos de red, los mismos trabajan en la capa de enlace del modelo OSI; son capaces de interconectar diferentes LAN para hacer que parezcan una sola.
f) ***Routers*:** la función principal de los *routers* es la de interconectar subredes lógicamente separadas, además define el camino más eficiente que un paquete debe seguir a través de diferentes redes, así como reenviar los datos al siguiente dispositivo presente en el camino. Éstos dispositivos trabajan en la capa de red del modelo OSI y tienen la ventaja de poder conectar redes basadas en diferentes topologías lógicas, por ejemplo Token Ring y Ethernet.

1.3.2.2 Gateways

Son también conocidos como Pasarelas, estos dispositivos son los encargados de unir diferentes tipos de redes y están ubicados en los bordes de salida de cada red, es decir, son usados como nodos de entrada hacia otra red y viceversa.

Los Gateways pueden ser implementados completamente en software, completamente en hardware o como una combinación de ambos. Dependiendo de su aplicación, los gateways son capaces de operar a cualquier nivel del modelo OSI, desde protocolos de aplicación hasta protocolos de señalización; es por esto que se consideran unidades muy versátiles. Son dispositivos que resultan sumamente útiles en entornos de redes de datos que adicionalmente involucren telefonía; estos son

capaces de actuar como unidades de traducción entre redes de telefonía PSTN y redes basadas en IP, como por ejemplo redes de próxima generación NGN.

1.3.2.3 Gatekeepers

Los Gatekeepers están encargados de las tareas de control de una determinada zona de red; un gatekeeper provee de una serie de servicios a entidades registradas, entre los cuales están la gestión, la autenticación, administración del ancho de banda y la traducción de direcciones IP en números telefónicos. Son considerados el componente más importante de una red basada en el protocolo H.323.

1.3.3 Concepto *Softswitch* y SBC (Session Border Controller)

La evolución de las redes basadas en conmutación de paquetes a través del Protocolo de Internet y la gran flexibilidad que éstas ofrecen, han llevado a los proveedores de servicio de telefonía, cuya infraestructura está basada mayormente en redes de conmutación de circuitos, a la búsqueda de conectar a sus clientes a través de redes convergentes basadas en el concepto de red de próxima generación NGN, con la fiabilidad, conveniencia y funcionalidad de las redes telefónicas tradicionales; aunado a esto, tener la capacidad de ofrecer servicios de voz, datos y video de calidad a un costo más reducido a través de una misma infraestructura de red.

La tecnología *Softswitch* surge en gran parte para dar soluciones a estas necesidades, ésta será la encargada de ofrecer lo mejor de las redes telefónicas tradicionales y el Internet. *Softswitch* es un nombre genérico dado a la nueva evolución en la manera cómo se realiza la conmutación telefónica. Como su nombre lo indica, este nuevo esquema de conmutación se basa en software para emular las tareas que cumplen los *Switches* telefónicos tradicionales, y ofrecer a su vez toda la innovación en servicios multimedia que el desarrollo de software y las redes IP son capaces de proporcionar. El software es capaz de desempeñar funciones de control de

llamada, enrutamientos, facturación y contabilidad (billing and accounting) además de ofrecer servicios de administración de operaciones. Esto denota la capacidad de los *Softswitch* de realizar las operaciones que hacen redes clase 5 para conectar abonados, interconectar múltiples centrales tandem o clase 4 y servir de centrales de larga distancia ó clase 3, de la misma forma que lo hacen las centrales actuales.

El concepto de *Softswitch* puede consistir en uno o varios componentes, esto es debido al abanico de tecnologías y equipos ofrecidos en el mercado actual, en donde las funciones pueden residir en un solo sistema o expandirse a través de varios de ellos. El concepto de *Softswitch* está basado en los siguientes componentes básicos, según el ISC (International *Softswitch* Consortium), hoy IPCC (International Packet Communications Consortium).

a) **Controlador de Gateway:** referida anteriormente como Call Agent, definido como el centro operativo del *Softswitch*; controla el procesamiento de llamadas a través de otros entes sobre los cuales ejerce control como lo son el Media Gateway y el Signalling Gateway. Es conocido también como *Softswitch*.
b) **Media Gateway:** es el mediador entre la red PSTN y el entorno IP; encargado de dar apertura a los canales de voz, y de aplicar los codecs respectivos a dicha comunicación.
c) **Signalling Gateway:** traduce los mensajes de señalización entre la red PSTN y la IP, los cuales permiten la conexión, establecimiento y desconexión de sesiones. Por ejemplo, es capaz de hacer la traslación de una llamada generada en la PSTN con el uso de señalización CCSS7, la cual debe ser terminada en una red basada en VoIP, bajo protocolo SIP.
d) **Servidor de *Media*:** encargado de ofrecer funcionalidades adicionales de audio al sistema de *Softswitch*, puede proveer por ejemplo de sistemas de IVR (Interactive Voice Response) que ofrezcan valores agregados a la solución.

e) **Servidor de aplicaciones (Feature Server):** ofrece la interfaz de operación y es el encargado de controlar los datos provenientes de los componentes de *Softswitch* para generar aplicaciones de utilidad para la gestión del sistema como servicios localizados, uso de recursos, facturación, alarmas, entre otras.

Algunas de las características y ventajas de la implementación de tecnología *Softswitch* son las siguientes:

a) Capacidad de coexistir con redes tradicionales, lo cual permite el desarrollo de implementaciones híbridas en momentos de migración de infraestructuras.
b) Amplio espectro de servicios soportados: voz, fax, video, datos y nuevos servicios desarrollados bajo protocolos de internet.
c) Bajo costo de desarrollo. Los equipos basados en tecnología *Softswitch* son evidentemente más económicos que lo *Switches* tradicionales, al estar basados en arquitecturas estándares de computadores.
d) Permite una mejor utilización de recursos, lo que se traduce en mejores ingresos para los proveedores de servicio y operadores.
e) Ofrece mayor facilidad de gestión de red y unificación de mensajes.

La última tecnología en equipos de *Softswitch* trae como implementación lo que se conoce como controlador de sesiones de borde ó SBC (Session Border Controller), de igual forma ocurre con equipos que tienen como principal función la de SBC e incorporan soluciones de *Softswitch* integradas. Los SBC son dispositivos que manejan sesiones de voz y multimedia en los bordes de las redes IP, principalmente son los encargados de controlar las dos partes de una llamada sobre IP: señalización y *media*. La versatilidad de los SBC reside en el hecho de poderlos conectar en el borde entre el acceso y la red *Core* ó entre dos redes *Core* en el caso de interconexión.

Otra función importante de los SBC es la de proveer servicios SIP a través de NAT (Network Address Translation) y *Firewalls* localizados en los predios del cliente o entre redes, adicionalmente, proteger al módulo de *Softswitch* de ataques de señalización identificando el trafico malicioso antes de que alcance el *Core* de la red.

En cuanto a calidad de servicio, los SBC ocupan una posición única en cuanto al control de la calidad de la comunicación del usuario final y refuerzo de los niveles de servicio prestado SLA (Service Level Agreements) mediante los sistemas de control de admisión, los cuales pueden monitorear el número de llamadas y el uso de ancho de banda, de manera de preservar la calidad de las llamadas establecidas. Permite manejar únicamente la señalización de las llamadas, dejando el flujo de información directamente entre dispositivos de clientes, lo que se traduce en un ahorro significativo de ancho de banda en la red.

1.3.4 Calidad de Voz ó QoV (Quality of Voice)

La calidad de voz es un concepto un tanto subjetivo; desde el punto de vista del usuario, ésta se basa en qué tan bien o con qué tanta calidad son capaces de escucharse los interlocutores en una conversación telefónica, en este caso específico, a través de una red de voz sobre paquetes.

Existen varios factores por los cuales la calidad de voz puede verse afectada, estos son:

a) **Disponibilidad:** la disponibilidad de un sistema es la probabilidad de que éste se encuentre en condiciones de funcionamiento; en cuanto mayor es la disponibilidad, mayor es esa probabilidad. Las redes telefónicas tradicionales presentan valores de disponibilidad muy elevados, del orden de 99,999%, cifra equivalente a unos 5 minutos indisponible al año. Las redes de datos no alcanzan estos valores de disponibilidad, bien sea por errores de

los usuarios o por errores de software; la manera de combatir esta situación es creando tolerancia a fallos mediante la colocación de equipos redundantes en las zonas más críticas de la red, así como haciendo uso de sistemas ininterrumpidos de energía.

b) **Jitter:** Como es sabido, en redes IP no es posible asegurar que todos los paquetes sigan una misma dirección, de hecho, lo más probable es que no lo hagan; en consecuencia, cada paquete atravesará un numero de nodos distinto para llegar al destino, y por ende lo alcanzarán con un retardo diferente. Esta variabilidad del retardo es lo que se conoce como Jitter. Para absorber esta variación, se utilizan buffers de supresión de jitter, los cuales almacenan los paquetes el tiempo suficiente para que los paquetes que han llegado fuera de secuencia puedan reordenarse para su correcta reproducción; el tamaño del buffer depende de manera proporcional a la magnitud del jitter. Sin embargo, la supresión de jitter puede generar a su vez, pérdida en la calidad de voz, lo que conlleva a encontrar un compromiso entre su tamaño, el retardo y las pérdidas.

c) **Pérdida de paquete (Packet Loss):** se refiere al descarte de paquetes que realizan los nodos de la red debido a la congestión de éstos. El efecto de estas pérdidas causa que la señal no pueda ser reconstruida con exactitud en el destino, consecuencia que es más notable a medida que la tasa de compresión del códec sea mayor. Para esto se desarrollaron tres técnicas: la de corrección de errores, en las cuales se inserta entre los paquetes información redundante; distribución de errores, con la cual se hacen aleatorias las pérdidas para dispersar el efecto, y la recuperación de errores, que consiste en la sustitución de un paquete perdido por un silencio, un ruido blanco o un paquete tratado con una técnica de predicción haciendo uso de los paquetes anteriores y posteriores a la pérdida.

d) **Retardo (Latency):** está definida por el tiempo que toma una señal de voz en transmitirse desde el origen hasta el destino; la alteración de este tiempo de propagación de la señal afecta la secuencia natural de una conversación

(escucha/respuesta), lo que puede hacer a dicha conversación ininteligible. La recomendación G.144 de la ITU-T establece un umbral de retardo entre los 150 ms y los 200 ms para que éste sea aceptable. Para redes satelitales se utilizan umbrales de unos 400 ms dado a la naturaleza de dicha comunicación, dejando valores por encima de éste como inaceptables.

e) **Eco:** este efecto se produce cuando el emisor escucha su propia voz junto con la del otro interlocutor o en ausencia de ella, este fenómeno es muy común tanto en redes tradicionales como en redes de conmutación de paquetes, y ocurre debido a la reflexión que sufre la señal tras el paso de ésta por dispositivos presentes en la red y al acoplamiento de los mismos. Es importante destacar que el eco es producido únicamente en los segmentos analógicos de la red (como en el bucle de abonado). Además del retardo del eco, el cual debe ser de alrededor de 16 ms, también es importante su amplitud; la magnitud de la señal reflejada recibe el nombre de ERL (Echo Return Loss) y se define como:

$$ERL = AmplitudSeñalOriginal - AmpitudEco \qquad (1)$$

La recomendación ITU-T G.168 establece valores de 56 dB ó superiores como aceptables.

f) **Ancho de Banda del Medio:** se entiende por ancho de banda como a la cantidad máxima de información que una red es capaz de transportar en cada unidad de tiempo, sin degradación. El primer factor que toda red de voz sobre paquetes debe asegurar para una calidad adecuada es poseer un ancho de banda suficiente para dar curso a dichas comunicaciones. Un sobredimensionamiento de ancho de banda para la red de VoIP puede evitar que las pérdidas, el jitter o el retardo tenga un impacto considerable, lo que no quiere decir, que esto resuelva de manera definitiva el problema de calidad. Para esto se recurren a estudios exhaustivos de todos los factores que influyen en la calidad de voz y a la aplicación de técnicas como la

codificación y la supresión de silencios; éste último encargado de suprimir las ausencias de voz de las conversaciones (que abarcan casi el 60% de las mismas), y sustituirlos por paquetes correspondientes a otras conversaciones, haciendo más eficiente el uso de ancho de banda.

1.3.4.1 Medidas de la calidad de voz

Los métodos y técnicas existentes para medir la calidad de voz son muy variados; existen dos tipos de métodos que se emplean para medir este parámetro, el método intrusivo consiste en enviar una llamada de prueba a través de la red; posteriormente la señal transmitida se compara con la recibida para evaluar la degradación que se produce al pasar por la red. Este tipo de técnicas no son aplicables en tiempo real, o lo que es lo mismo, tienen que realizarse sin ningún tipo de tráfico en la red, lo cual no resulta rentable para una Empresa en producción. Entre los sistemas intrusivos de medición se encuentran los pertenecientes a los estándares PAMS (Perceptual Analysis Measurement System), PESQ (Perceptual Evaluation of Speech Quality) (ITU- P.862) y PSQM (Perceptual Speech Quality Measurement) (ITU- P.862).

Otro tipo de métodos de medición son los no intrusivos, estos son practicables en tiempo real, lo cual es conveniente en ambientes en producción. El sistemas de escala MOS (Mean Opinion Score), es un ejemplo de éste tipo de métodos.

1.3.4.1.1 Escalas MOS

Este método se encuentra estandarizado bajo la recomendación P.800 de la ITU-T, han venido siendo utilizadas desde 1993 y se trata de un conjunto de técnicas subjetivas de medida de la calidad de voz que reciben el nombre de test ACR (Absolute Category Rating) que consisten en reunir una muestra de usuarios a los que

se les pide opinión sobre algún aspecto concreto de un sistema de transmisión de voz; los test ACR no disponen de una señal de referencia para las medidas, al igual de lo que le sucede al usuario al no tener como comparar la voz recibida con la original. Para obtener estas escalas, es necesario construir valores basados en una escala absoluta, para ello se presenta a los usuarios, ejemplos predefinidos que proporcionan una base a la hora de evaluar. Los aspectos que se miden con la escala son: la calidad de voz y el esfuerzo requerido para entender el significado de un mensaje.

En la Tabla 5 y 6 se presentan la escala MOS para medir la calidad de voz y el esfuerzo.

Tabla 5. Escala MOS para medición de calidad de voz

Calidad	***Puntuación***
Mala	1
Pobre	2
Aceptable	3
Buena	4
Excelente	5

Tabla 6. Escala MOS para la medición de esfuerzo

Esfuerzo	***Puntuación***
Inentendible	1
Esfuerzo considerable	2
Esfuerzo moderado	3
Sin esfuerzo apreciable	4
Sin ningún esfuerzo	5

De igual forma, existe una calidad de voz asociada a los Codecs más utilizados en telefonía sobre redes de paquetes, esta escala se muestra en la Tabla 7:

Tabla 7. Escala MOS para codecs comunes

Codec	*Puntuación*	*Velocidad*
G.711	4,4	64 kbps
G.723.1	3,9	6,3 kbps
G.726	3,8	32 kbps
G.729	3,7	8 kbps

1.3.5 Calidad de Servicio ó QoS (Quality of Service)

La calidad de servicio se refiere a la capacidad de la red de transportar tráfico dado sus características de pérdidas, *jitter*, retardo, ancho de banda, entre otros; estas características forman parte de lo que se denomina su perfil de tráfico. Dada las diferentes fuentes generadoras de información (teléfonos, servidores, PC, video, etc.), las técnicas de calidad de servicio deben proporcionar unas prestaciones adecuadas para cada fuente de tráfico de acuerdo a su perfil. Una vez identificada la fuente de tráfico, se gestiona el ancho de banda y se controlan las situaciones de congestión en la red dando prioridad a las fuentes de tráfico más restrictivas, como por ejemplo, las que generan tráfico de voz.

A principios de los 90, la IETF en su RFC 1633 estandarizó dos arquitecturas que ofrecen calidad de servicio, la de servicios integrados ó IntServ la cual está basada en el protocolo RSVP (Resource Reservation Protocol)[15] y se encarga de garantizar buenos valores de ancho de banda y retardo en todos los nodos presentes en la comunicación entre el origen y el destino. Esta solución requería que cada nodo soportara dicho protocolo, lo cual resulta difícil debido a las coexistencias de equipos de diferente procedencia. La otra arquitectura es la de servicios

[15] *RSVP. Protocolo de control de red que permite que aplicaciones de Internet obtengan diferentes calidades de servicio en sus flujos de datos, y así adecuarse a las distintas necesidades que requiere cada servicio. Se encuentra documentada en la RFC 2205 de la IETF. Disponible en: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rsvp.htm*

diferenciados ó DifServ, la cual describe el tratamiento que debe darse a los paquetes en cada nodo de la red. En este caso, la QoS se gestiona en cada nodo ó salto, lo que se denomina PHB (Per Hop Behavior), dejando a los fabricantes de equipos la libertad de gestión, siempre y cuando se cumpla la interoperabilidad de dispositivos.

Las técnicas de calidad de servicio han ido aumentando su sofisticación de manera de adaptarse a las más actuales técnicas de conmutación, como es el caso de MPLS (Multiprotocol Label Switching), el cual permite ofrecer una alta calidad de servicio sobre redes privadas virtuales VPN (Virtual Private Network)[16].

1.3.6 MPLS

Recogida en la IETF bajo su RFC 3031, es una nueva técnica de conmutación de alta velocidad. La misma, permite insertar a los paquetes que llegan a un nodo (por ejemplo un *router*) una etiqueta en su cabecera que los identifica como FEC (Forwarding Equivalent Class), esto con el fin de que los paquetes sean tratados de la misma manera y no se procesen sus cabeceras completas, lo que supone un tiempo de procesamiento y consumo de recursos menor, esto es posible gracias a que MPLS incluye una nueva etiqueta donde se incluye toda la información necesaria para el enrutamiento.

Los nodos que soportan MPLS, llamados LSR (Label *Switch*ed *Router*), comprueban qué etiqueta corresponde a la subred a la que pertenece el destino, y marca el paquete con dicha etiqueta antes de enviarlo al siguiente LSR, de manera

---

[16] VPN (Virtual Private Networks). Redes Privadas Virtuales: permiten el uso de la infraestructura de telecomunicaciones pública para el establecimiento de redes privadas, las cuales mediante técnicas de túneles virtuales (tunneling) y encriptación, ofrecen la seguridad y el aislamiento de las redes privadas . Información disponible en: http://www.vpnc.org/vpn-technologies.html

que todos los siguientes nodos LSR ignoren la cabecera IP y analicen únicamente la cabecera MPLS. El camino que forma este conjunto de etiquetas (de LSR a LSR) recibe el nombre de LSP (Label *Switch*ed Path), una vez llegue el paquete al final del camino, la etiqueta es sustituida por una de enrutamiento tradicional.

La solución que ofrece MPLS al problema de QoS, se resuelve asignando a un LSP específico, recursos necesarios en cada LSR y en cada enlace que forma parte del LSP para cada tipo de tráfico. Para esto se calculan las rutas óptimas mediante un enrutamiento basado en CBR (Constrained Based Routing) según parámetros concretos de QoS como retardo, jitter, pérdidas y otros. Este tipo de soluciones permiten controlar el dimensionamiento y la planificación de redes, concepto que se conoce como ingeniería de tráfico.

En la Figura 15 se muestra una estructura de cabecera genérica de 32 bits de MPLS:

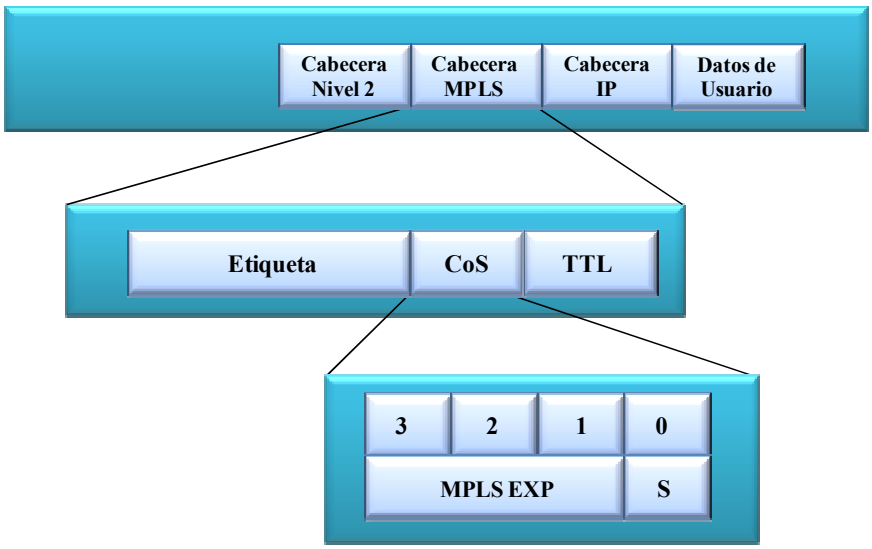


Figura 15. Cabecera MPLS

Fuente: Huidobro, José Manuel – Martínez, David. Tecnología VoIP y Telefonía IP. (Libro). España, 2006. p. 160. [7]

CAPÍTULO II

RED ACTUAL DE LA EMPRESA: 123.COM.VE

Para realizar el modelo para la inserción del *Softswitch* en la red de la Empresa es imprescindible hacer el estudio de la plataforma y de los equipos que la conforman. Para esto, se llevó a cabo una revisión en la sala de operaciones de manera de levantar la información para la realización de un esquema general que permita describir de una manera concreta el funcionamiento y la estructura de la red de 123.com.ve.

2.1 Red de telefonía TDM

123.com.ve presta servicio de tráfico telefónico por medio de rutas establecidas para tráfico nacional e internacional a través de convenios de interconexión con empresas importantes de telecomunicaciones del país y del mundo. La red de conmutación de la Empresa está basada en conmutación de circuitos y el servicio es prestado a través de enlaces dedicados E1 con los distintos operadores tanto para originación como para terminación de llamadas.

2.1.1 Elementos de la red de telefonía TDM

Los elementos de la red de telefonía TDM son:

2.1.1.1 Central Ericsson ANS

La red de conmutación de la Empresa está soportada por la tecnología del *switch* telefónico público Ericsson ANS clase 4, el cual se conecta con diferentes *Switches* de otros operadores alrededor del país y a nivel internacional para ofrecer el servicio telefónico.

El equipo es de arquitectura modular y permite realizar la conmutación de tráfico telefónico hacia o desde la red de telefonía pública PSTN. Es capaz de soportar 88 enlaces digitales E1 de 2 Mbits y tiene una capacidad de atender hasta 3000 suscriptores, prestando su servicio mediante el uso de protocolos de señalización por canal común CCSS7, ISDN-PRI[17] (Integrated Services Digital Network-Primary Rate Interface) ó por canal asociado R2[18].

El equipo es totalmente escalable, permitiendo que cada enlace digital se conecte a través de ranuras de tarjetas que soportan hasta 4 E1, lo que permite un crecimiento de hardware y software acorde a las necesidades de la red. Adicionalmente, el equipo cuenta con soporte para servicios de redes inteligentes,

---

[17] *ISDN PRI. Estándar de telecomunicaciones utilizado en la Red Digital de Servicios Integrados para llevar múltiples transmisiones de voz y de datos a partir de 30 canales de 64 Kbps llamados "B" (de Bearer Channel) y un canal que puede ser de 16Kbps ó 64 Kbps usado comúnmente para señalización denominado D (Delta Cahnnel). En: http://public.swbell.net/ISDN/overview.html*

[18] *R2. Tipo de señalización por canal asociado CAS (por su siglas en inglés) desarrollada en los años 60, la cual es usada todavía en países de Europa, Latinoamérica, Australia y Asia. Sus especificaciones se encuentran en las recomendaciones de la ITU-T Q.400 a la Q.490. Información extraída de: http://www.cisco.com/warp/public/788/signalling/e1_r2_sig.html*

sistemas de acceso de lista blanca (White lists), sistemas de enrutamiento de llamadas por costo (Less cost routing), soporte de sistemas de mediación para facturación y sistemas para operación y mantenimiento.

La arquitectura del *switch* Ericsson ANS está basada en los siguientes módulos básicos:

a) **Unidad SHU (System Handling Unit):** constituye la tarjeta principal del ANS; contiene elementos de datos vitales para el arranque del sistema, ofrece control sobre el hardware, proporciona la interfaz de conexión con el sistema de manejo de la Central a través de una conexión serial a 9,6 kbps y es la encargada de controlar el flujo de alarmas del sistema.
b) **Unidad DSU (Data Service Unit):** unidad encargada de procesamiento central, contiene el software de configuración del sistema; además se encuentran en ella los archivos y respaldos del equipo.
c) **Unidad CSU (Central Signal Processing Unit):** unidad encargada del procesamiento de señales digitales, de la generación de tonos multifrecuenciales DTMF y de Conferencia.
d) **Unidad CSB (Circuit *Switch* Block) y PSB (Packet *Switch* Block):** la CSB es la encargada de manejar las interfaces digitales de conexión de los circuitos PCM de 2 Mbits (E1) y la PSB se encarga de la conmutación interna de paquetes.
e) **Unidad CTU (Clock and Tone Unit):** unidad encargada de generar la señal de reloj interna y los tonos para los suscriptores.
f) **Unidad PSU (Power Supply Unit):** se encarga de convertir la alimentación DC entrante, en tensiones estables de 5V y 12V utilizadas por toda la tarjetería del equipo. Provee de igual forma de los voltajes para repique y para señales de pulsos utilizados en mediciones.
g) **Unidad VAU (Voice Announcement Unit):** unidad donde se cargan los mensajes de voz, soporta hasta 20 minutos de anuncios y contiene 40 mensajes pregrabados.

h) **Unidad ALT (Autonomous Line Terminating Unit):** unidades encargadas de la terminación de enlaces PCM de 2 Mbits, soporta distintos tipos de señalización, por ejemplo CCSS7, R2 y CAS (Channel Associated Signalling).

2.1.1.2 Central telefónica Corporativa Ericsson MD110

El servicio de conmutación telefónico interno de la Empresa es abastecido por la solución PABX (Private Automatic Branch Exchange) MD110 de Ericsson; el cual cuenta con arquitectura modular, lo que permite adicionar gabinetes de comunicaciones para ampliaciones del sistema. El sistema MD110 de la Empresa cuenta con un gabinete de comunicaciones que contiene una interfaz troncal E1 (el cual es usado para la conexión con el *switch* ANS para abastecerse de servicio telefónico) y 2 troncales analógicos; así como también tiene una capacidad de 60 extensiones digitales y 30 extensiones analógicas. Utiliza protocolos de señalización R2 y CCSS7; además, soporta servicios de redes inteligentes, *call centers*, sistemas de IVR, conferencia, desvío de llamadas y llamada en espera; adicionalmente, es capaz de ofrecer soporte para algunos servicios de telefonía IP a través del protocolo H.323, previa adquisición de los módulos correspondientes.

2.1.2 Descripción de la red de telefonía TDM

La red de telefonía TDM está formada por rutas para tráfico LDN (Larga Distancia Nacional) y para tráfico LDI (Larga Distancia Internacional). Estas rutas han sido establecidas tras convenios de interconexión con importantes Empresas de telecomunicaciones del país como lo son CANTV (Compañía Anónima Teléfonos de Venezuela), Movilnet, Movistar, Digitel y Net Uno, así como con Empresas internacionales como AT&T (American Telephone and Telegraph), Entel Chile (Empresa Nacional de Telecomunicaciones), Telecom Italia, Americatel y ETECSA (Empresa de Telecomunicaciones de Cuba Sociedad Anónima).

CONATEL (Comisión Nacional de Telecomunicaciones), órgano regulador de las telecomunicaciones en Venezuela, estableció mediante el artículo 218 de la Ley Orgánica de Telecomunicaciones, que todo tráfico entre conectantes a nivel nacional debe ser en telefonía básica tradicional TDM y a través del uso de señalización por canal común CCSS7, de esta forma, toda la red de interconexión nacional se encuentra bajo este formato.

La red nacional es tipo estrella, siendo el nodo principal el *switch* público Ericsson ANS; esta red permite cubrir ciudades como Caracas, Valencia, Maracay, Barquisimeto, Maracaibo, San Cristóbal, Puerto La Cruz y Puerto Ordaz con enlaces E1 directos; el resto de las ciudades es cubierto por saltos de conmutación provistos principalmente por las Empresas CANTV y Movistar. En las siguientes Figuras y Tablas se muestra información acerca de la red de interconexión con las distintas operadoras, dando detalle de puntos de señalización, puntos de interconexión, número de enlaces digitales E1 e identificación del enlace dentro del *switch* Ericsson ANS de 123.com.ve.

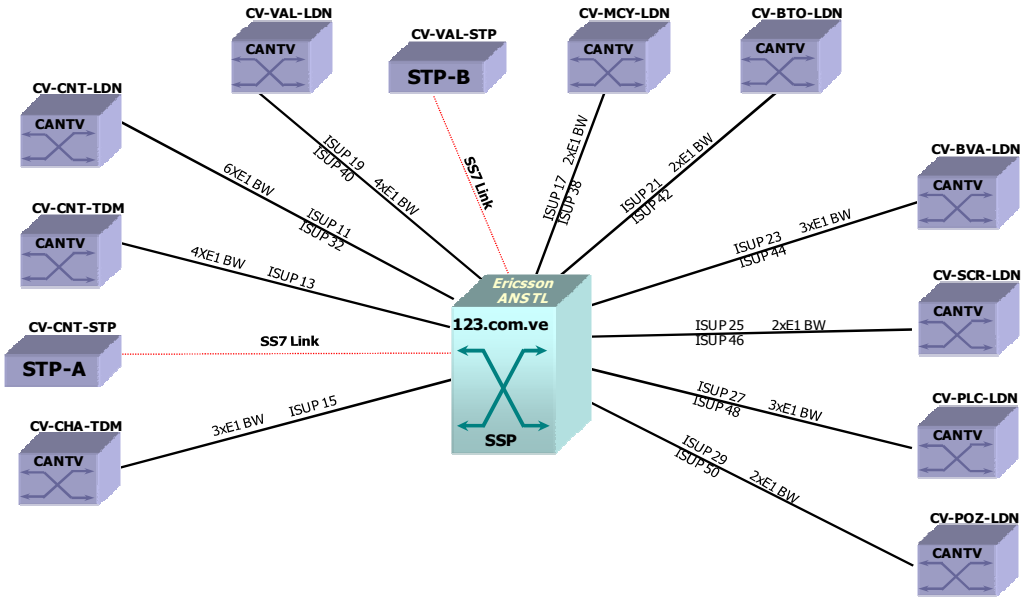


Figura 16. Red de interconexión nacional con CANTV

Fuente: Entel Venezuela. Vicepresidencia de Ingeniería y Operaciones. [11]

Tabla 8. Descripción red de interconexión nacional con CANTV

Ruta	*Identificación Grupo Troncal*	*Enlaces E1*
CANTV CNT LDN	CV-CNT-LDN	6 E1
CANTV CNT TANDEM	CV-CNT-TDM	4 E1
CANTV CNT STP	CV-CNT-STP	Pto. de señalización CCSS7
CANTV CHACAO TANDEM	CV-CHA-TDM	3 E1
CANTV VALENCIA LDN	CV-VAL-LDN	4 E1
CANTV VALENCIA STP	CV-VAL-STP	Pto. de señalización CCSS7
CANTV MARACAY LDN	CV-MCY-LDN	2 E1
CANTV BARQUISIMETO LDN	CV-BTO-LDN	2 E1
CANTV BELLA VISTA LDN	CV-BVA-LDN	3 E1
CANTV SAN CRISTOBAL LDN	CV-SCR-LDN	2 E1
CANTV PTO. LA CRUZ LDN	CV-PLC-LDN	3 E1
CANTV PTO. ORDAZ LDN	CV-POZ-LDN	2 E1

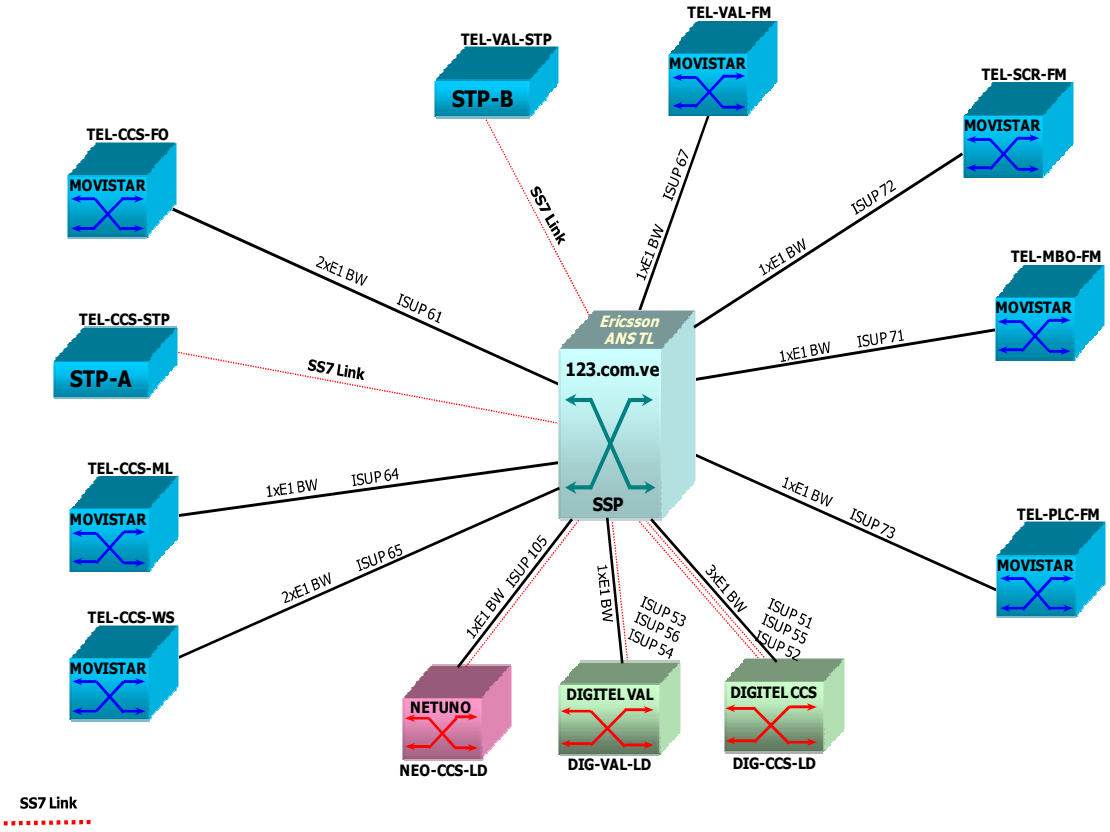


Figura 17. Red de interconexión nacional con Movistar, Digitel y Net Uno

Fuente: Entel Venezuela. Vicepresidencia de Ingeniería y Operaciones. [11]

Tabla 9. Descripción de la red de interconexión nacional con Movistar, Digitel y NetUno.

Ruta	***Identificación Grupo Troncal***	***Enlaces E1***
MOVISTAR CARACAS	TEL-CCS-FO	2 E1
MOVISTAR CARACAS STP	TEL-CCS-STP	Pto. de señalización CCSS7
MOVISTAR CARACAS ML	TEL-CCS-ML	1 E1
MOVISTAR CARACAS WS	TEL-CCS-WS	2 E1
MOVISTAR VALENCIA STP	TEL-VAL-STP	Pto. de señalización CCSS7
MOVISTAR VALENCIA FM	TEL-VAL-FM	1 E1
MOVISTAR SAN CRISTOBAL FM	TEL-SCR-FM	1 E1
MOVISTAR MARACAIBO FM	TEL-MBO-FM	1 E1
MOVISTAR PTO. LA CRUZ FM	TEL-PLC-FM	1 E1
NET UNO CARACAS LD	NEO-CCS-LD	1 E1
DIGITEL CARACAS LD	DIG-CCS-LD	3 E1
DIGITEL VALENCIA LD	DIG-VAL-LD	1 E1

El transporte hacia estos *switches* destinos es dado bien por la empresa con la que está provista la conexión (como es el caso de CANTV a nivel nacional) ó a través de la red de fibra óptica interurbana de La Electricidad de Caracas, C.A. para la conexión con Movistar, Digitel y Net Uno en Caracas; dichas empresas son las encargadas del transporte de tráfico en sus redes a nivel nacional.

El transporte de la red que soporta el tráfico LDI, se lleva acabo a través de un anillo de fibra óptica, el cual se encuentra arrendado a la Empresa Global Crossing; este enlace es de jerarquía SDH STM-4 de 622 Mbps, del cual se encuentra arrendado un enlace tributario DS-3 ó T3 de 45 Mbps canalizado en 21 enlaces E1 de 2 Mbps. En los predios de Global Crossing, parten dos enlaces STM-1 de 155 Mbps, cada uno con un arrendamiento de un tributario DS-3; uno de ellos es la conexión hacia Americatel en Nueva York – EE.UU y el otro corresponde a la conexión con Entel en Santiago de Chile.

De la conexión con Americatel en Nueva York, parten conexiones cruzadas (cross-conexiones) de enlaces digitales E1, de los cuales 2 E1 van hacia la empresa

AT&T, 2 E1 hacia la empresa Telecom Italia y 5 E1 quedan en la empresa Americatel, cada uno de éstos con sus canales de señalización CCSS7 respectivos. De la conexión con Entel Chile, los cinco enlaces E1 son utilizados para las rutas provistas con la empresa chilena, así como también para el tráfico que tiene como destino la Empresa de telecomunicaciones Cubana ETECSA.

Todos estos enlaces son transportados a través de la fibra submarina de LANautilus (Latin American Nautilus) con ubicación en el Tele Housing de Global Crossing en Caracas hacia los destinos antes mencionados. Estas conexiones fueron realizadas con el fin de transportar todo el tráfico internacional de manera de cumplir con el plan de negocios que tenía Entel Venezuela, ahora 123.com.ve. La Figura 18 muestra la topología lógica de la interconexión internacional.

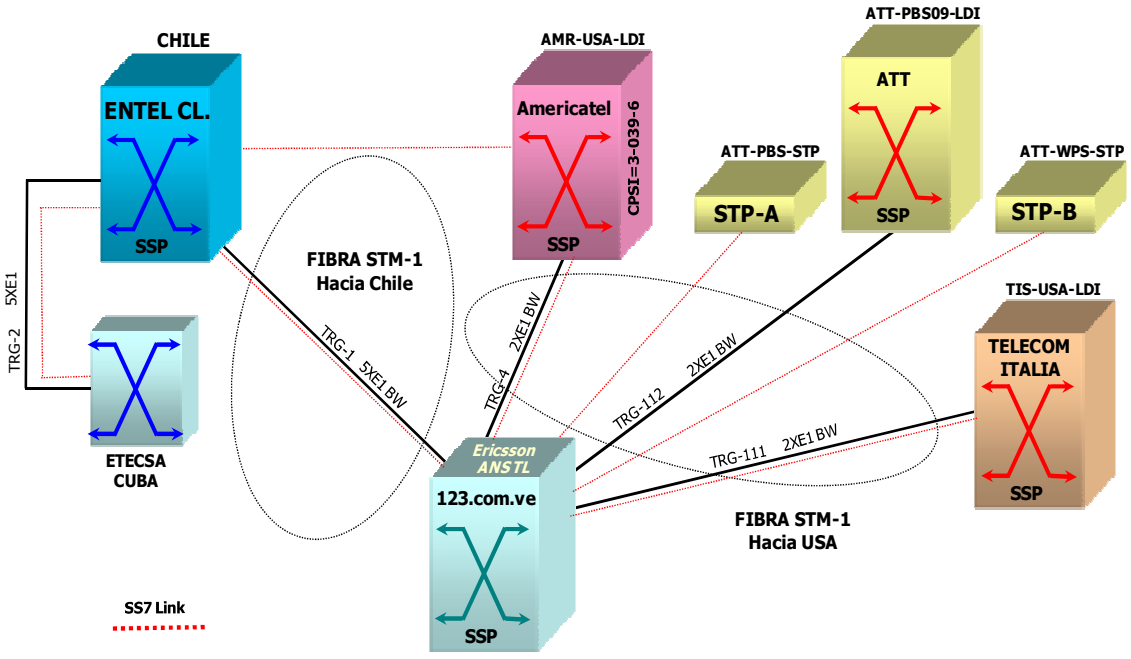


Figura 18. Red de interconexión internacional

Fuente: Entel Venezuela. Vicepresidencia de Ingeniería y Operaciones. [11]

Tabla 10. Descripción de la red de interconexión internacional

Ruta	***Identificación Grupo Troncal***	***Enlaces E1***
ENTEL CHILE	ENT-CHL-LDI	5 E1
AMERICATEL USA LDI	AMR-USA-LDI	2 E1
AT&T STP A	ATT-PBS-STP	Pto. de señalización CCSS7
AT&T STP B	ATT-WPS-STP	Pto. de señalización CCSS7
AT&T LDI	ATT-PBS09-LDI	2 E1
TELECOM ITALIA LDI	TIS-USA-LDI	2 E1

El principal integrante de la red de transmisión internacional es el multiplexor Marconi MSH41C, el cual se encuentra replicado tanto en las instalaciones de 123.com.ve, como en el *Tele Housing* de Global Crossing, los cuales forman un anillo STM-4 protegido con redundancia 1+1 para éstos y para ambos enlaces STM-1 hacia EE.UU y Chile. Este equipo permite la conexión de enlaces de fibra de corto y largo alcance cumpliendo con las normas ITU-T G.957, G.958, G.781, G.782, G.783, G.784, G.826, y la conexión de interfaces eléctricas según la norma G.703. En la Figura 19 se muestra un esquema de la red de transmisión internacional:

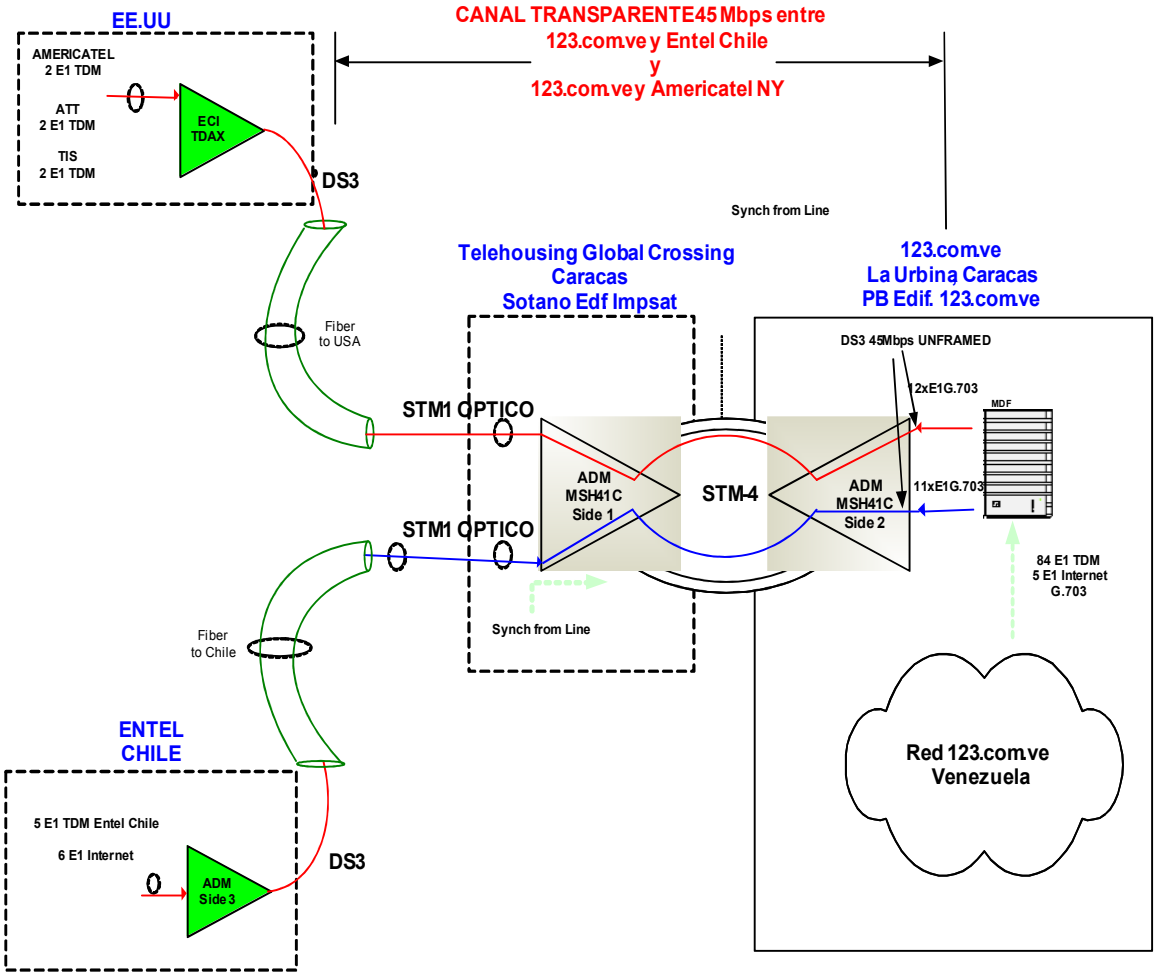


Figura 19. Red de transmisión internacional

Fuente: Entel Venezuela. Vicepresidencia de Ingeniería y Operaciones. [11]

2.2 Red Ethernet de la Empresa

La red Ethernet de la Empresa soporta los servicios internos corporativos y públicos de voz y datos, ésta se encuentra estructurada en VLANs, las cuales permiten dar servicios como correo, aplicaciones, seguridad, Internet, entre otros; así como soportar a las plataformas de servicios ofrecidas por la Empresa, que en conjunto con la red de telefonía TDM, permiten brindar servicios de telefonía de larga distancia prepagada y presuscrita, además de control de tarificación a CDC

(Centros de Comunicaciones). Adicionalmente la red Ethernet provee algunos servicios de telefonía IP ya existentes como es la terminación de llamadas en la red TDM de carriers nacionales como Net Uno e internacionales como LD Telecom, New Zealand Telecom, Telco 214, GRT Com, entre otros. La plataforma física de la red está estructurada de la siguiente manera:

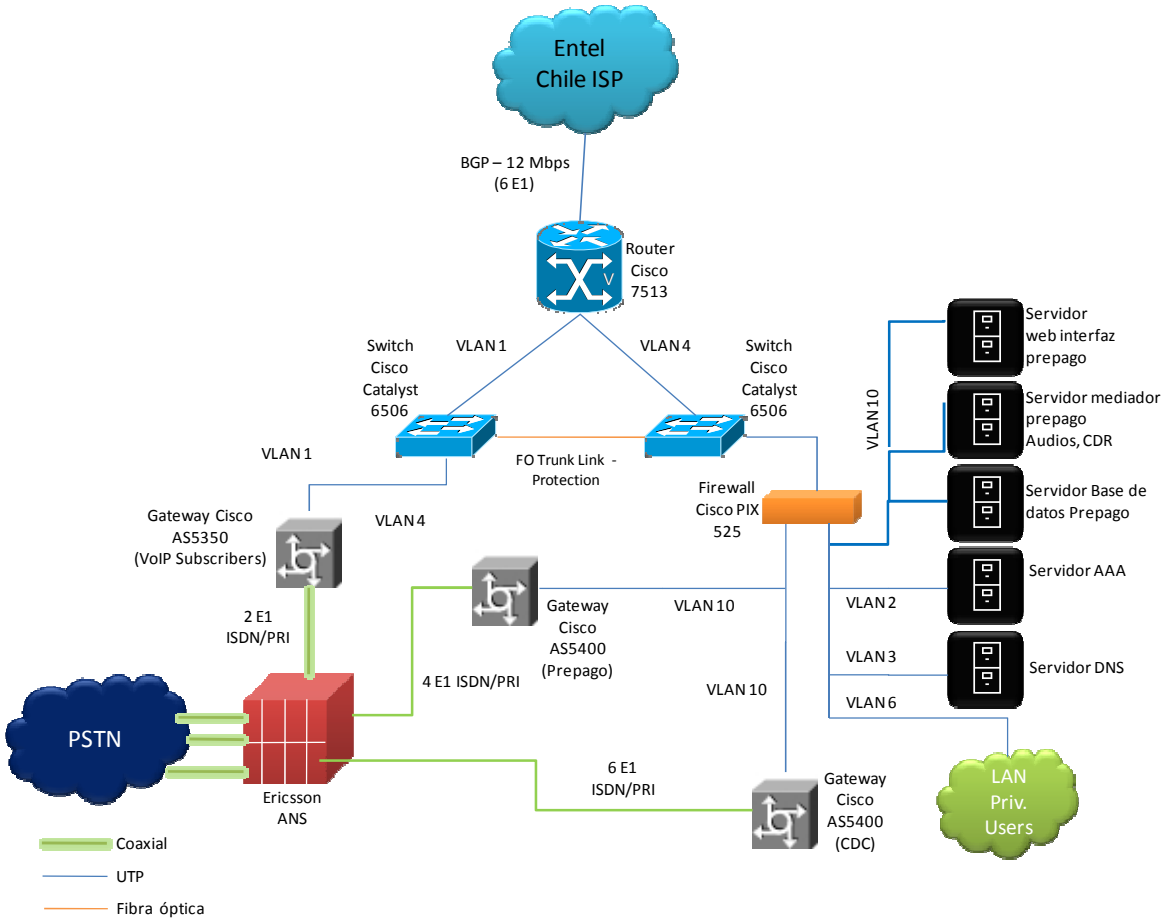


Figura 20. Plataforma física de la red Ethernet en el *Core* La Urbina

Fuente: Figura propia.

Se puede observar en la Figura 20, que la red está soportada sobre un *backbone* redundante constituido por un enlace troncal de fibra óptica entre dos *Switches* Cisco Catalyst 6506, esto permite que un *switch* se encargue de toda la carga de tráfico en caso de falla de uno de éstos; esta misma configuración permite el

balanceo de carga, de manera que todo el tráfico de la red se divide entre estos dos s*witches* mientras estén activos. En dichos *switches* 6506 se encuentran configuradas las VLANs, las cuales permiten aislar los servicios de la red según sus funciones y posición física de los equipos.

En la Tabla 11, se muestra la distribución de VLANs de la Empresa:

Tabla 11. Distribución de VLANs

VLAN	***Descripción***
VLAN 1	VLAN principal *Core*, Clientes VoIP
VLAN 2	VLAN seguridad y servidores AAA
VLAN 3	Servidores de internet, DNS
VLAN 4	VLAN respaldo *Core*
VLAN 6	Red Usuarios
VLAN 10	Servidores IVR, Billing, Base de datos

Los *switches* de núcleo ó *Core* Cisco Catalyst 6506 son de arquitectura modular y totalmente escalables; los *switches* de la Empresa cuentan con una ranura de 48 puertos eléctricos en interfaz RJ-45 de 100Mbps, que surten de servicio a todos los equipos de *Core* de la red e interconectan al conjunto de *switches* de piso que dan soporte de red a los usuarios de la LAN interna. Adicionalmente, cuentan con un puerto de fibra óptica cada uno de 1 Gbps que sirven de enlace de troncal entre ellos para la redundancia y el balanceo de carga.

Las tareas de enrutamiento (capa 3) se realizan a través del *Router* Cisco 7513, el cual es de igual forma de arquitectura modular y escalable. Este equipo se encarga de enviar los paquetes IP al destino correcto dentro de la red. Dicho *router* es capaz de manejar listas de acceso (Access Lists) que brindan seguridad contra posibles ataques a la red. El *Router* Cisco 7513 contiene dos interfaces RJ-45 de 100 Mbps, 8 interfaces seriales RJ-48 y un módulo HSSI (High Speed Serial Interface) propietario de Cisco, este es conectado a un multiplexor que permite separar el canal

de 12 Mbps en 6 E1 que son insertados al multiplexor SDH para su transporte a la red internacional, de esta manera se surte de conexión a internet a la red LAN.

El servicio de Internet de la Empresa es provisto por Entel Chile (ISP) mediante el enlace de 12 Mbps mencionado anteriormente. Los bloques de direcciones IP públicas de la Empresa son propiedad de Entel Chile, estas direcciones son usadas, entre otras cosas, para el acceso a través del Gateway Cisco AS5350 de las conexiones entrantes de VoIP provenientes de Internet que terminan en la red TDM.

La solución de gateways Cisco AS5350 y AS5400 (mostrados en la Figura 20), sirven de interfaz entre la red LAN y la red TDM; estos equipos cuentan con una capacidad de 8 E1 y se conectan al *switch* Ericsson ANS mediante interfaces ISDN (Integrated Services Digital Network)/PRI (Primary Rate Interface) para la conexión de dichos E1.

El AS5350 es el encargado de recibir el tráfico de telefonía IP en protocolo H.323 proveniente de Net Uno y de otros operadores internacionales; es el que se encarga de hacer la terminación de dicho tráfico en la red TDM mediante 2 enlaces E1.

Los dos equipos AS5400 de la red, realizan dos funciones importantes: el primero de ellos, realiza funciones de IVR para la plataforma de tarjetas telefónicas de larga distancia prepagadas en conjunto con los servidores de mediación y base de datos pertenecientes a la misma VLAN (VLAN 10). El gateway se encarga de extraer los audios y el árbol de instrucciones de la plataforma del servidor de mediación, utilizando para esto un canal de voz de uno de los E1 provenientes del ANS. Posteriormente se autentica el pin de la tarjeta prepago en el servidor AAA (Authentication, Authorization, Accounting) y se utiliza en conjunto el servidor de base de datos para obtener información como categoría de la tarjeta (tipo de

producto), saldo disponible, entre otros. Una vez realizada esta comprobación, el gateway apertura un canal adicional de vuelta donde se enlaza al cliente con el destino mediante el *switch* Ericsson. Los reportes de las llamadas realizadas en la plataforma ó CDR (Call Detail Report) son el resultado de la unión de los CDRs provenientes del ANS y los CDR generados por el servidor de mediación de la plataforma prepago; esta tarea se realiza en el mismo servidor de mediación. Los reportes de tráfico, CDRs y el control de la plataforma se observan mediante la interfaz provista desde el servidor web de la plataforma. Como es notable, para el establecimiento de una llamada a través de la plataforma prepago, se requiere del uso de dos circuitos de voz de los 4 E1 conectados entre el gateway y el ANS.

El otro gateway AS5400, también perteneciente a la VLAN 10, cumple funciones de apertura de los canales de voz para llamadas provenientes de CDC a nivel nacional. Cuando los CDC cursan una llamada a través del sistema, se abre un circuito de voz de uno de los 6 E1 disponibles para la plataforma y su número telefónico de identificación ó ANI (Automatic Identification Number) es validado en el servidor AAA. El gateway ejecuta un programa ó *script* descargado del servidor de mediación, el cual consiste en la generación de un tono (de vuelta hacia los CDC) al momento en que el abonado llamado contesta; al ocurrir esto, el gateway apertura un canal adicional para conectar al cliente con el destino. El tono recibido por los CDC es utilizado por éstos para el proceso de facturación a sus clientes. Se utilizan de igual manera dos circuitos de voz por llamada conectada.

La solución Firewall de Cisco PIX serie 500 (mostrado en la Figura 20), provee de seguridad a la red LAN de usuarios, aislándolos por completo de la red de *Core* a través de lo que se conoce como zonas desmilitarizadas o DMZ (Demilitarized Zones), esto con el fin de que ningún virus o ataque que se origine en la red de usuarios, afecte a los equipos de *Core* y servidores.

CAPÍTULO III

MODELO DE INGENIERÍA PROPUESTO

3.1 Requerimiento de la Empresa

De manera de reducir costos operativos y facilitar la gestión de la plataforma de la Empresa a través de una única red, 123.com.ve plantea la migración de sus servicios de telefonía tradicional TDM a una basada en el Protocolo de Internet, esto gracias a la confiabilidad que ha venido ganando el hardware IP y a la mejora de las redes de transporte de fibra óptica sobre la cual se sustenta Internet. Esto le permite a la Empresa cumplir su meta de ofrecer servicios integrados de telecomunicaciones a través de la más reciente tecnología, y ofrecerle a sus clientes actuales y futuros servicios confiables y a costos altamente competitivos.

La migración de toda la plataforma requiere de una solución de ingeniería que permita cumplir con éxito el objetivo sin impactar el servicio actual con el que cuentan sus clientes, ni su calidad, es por esto, que el modelo que se propone requerirá de la convivencia de ambas tecnologías para la transmisión de voz (TDM e IP) hasta que finalmente se logre la incorporación total de la tecnología de VoIP. Esta solución mixta requiere la utilización de Media Gateways que permitan la conversión entre el mundo TDM y el IP.

Para asegurar el correcto funcionamiento de la red de telefonía, es necesario comprobar el dimensionamiento de la misma, tanto en canales utilizados como en ancho de banda; para esto se realizará un estudio del tráfico actual de la red.

3.2 Estudio de tráfico de la red

De manera de garantizar la calidad del servicio de telefonía LDN y LDI soportado por la plataforma actual TDM, realizar un estudio del tráfico que la red de la Empresa soporta hoy en día es de gran utilidad, sobre todo si se considera dicho estudio para cualquiera de estos dos escenarios: (a) Escenario mixto (TDM e IP), con el cual se puede corroborar el estado de ocupación de los actuales circuitos y ayuda al dimensionamiento de canales entre los dispositivos TDM e IP (Media Gateways), y (b) Escenario Full IP, donde se puede deducir qué tanto ancho de banda debe soportar la red para manejar los servicios IP con una buena calidad (QoS).

Los datos que se encuentran en la Tabla 12 recopilan las estadísticas de reportes de tráfico de la Vice Presidencia de Ingeniería y Operaciones de 123.com.ve, tomando como referencia el valor pico máximo en Erlang[19] traficados en los últimos tres meses para cada ruta; como se mencionó anteriormente, estos datos permitirán comprobar el estado de las rutas actuales y dimensionar el ancho de banda necesario para soportar dicho tráfico.

---

[19] Erlang, A.K. ingeniero danés originador de la ingeniería de tráfico y la teoría de colas en telefonía. Su nombre lo lleva una unidad adimensional (Erlang) usada para medir el uso de un canal de comunicaciones por unidad de tiempo; el 100% de uso es referido como 1 Erlang. Disponible en: http://en.wikipedia.org/wiki/Erlang_unit

Tabla 12. Erlangs pico por ruta

Ruta	*Identificación Grupo Troncal*	*Enlaces E1 Actuales*	*Erlang pico*
ENTEL CHILE	ENT-CHL-LDI	5 E1	140,63
AMERICATEL USA LDI	AMR-USA-LDI	2 E1	68,65
AT&T LDI	ATT-PBS09-LDI	2 E1	58,92
TELECOM ITALIA LDI	TIS-USA-LDI	2 E1	36,65
CANTV CNT LDN	CV-CNT-LDN	6 E1	172,62
CANTV CNT TANDEM	CV-CNT-TDM	4 E1	41,4
CANTV CHACAO TANDEM	CV-CHA-TDM	3 E1	48,3
CANTV VALENCIA LDN	CV-VAL-LDN	4 E1	96,89
CANTV MARACAY LDN	CV-MCY-LDN	2 E1	54,57
CANTV BARQUISIMETO LDN	CV-BTO-LDN	2 E1	51,56
CANTV BELLA VISTA LDN	CV-BVA-LDN	3 E1	51,51
CANTV SAN CRISTOBAL LDN	CV-SCR-LDN	2 E1	45,06
CANTV PTO. LA CRUZ LDN	CV-PLC-LDN	3 E1	53,37
CANTV PTO. ORDAZ LDN	CV-POZ-LDN	2 E1	32,13
MOVISTAR CARACAS	TEL-CCS-FO	2 E1	92,57
MOVISTAR CARACAS ML	TEL-CCS-ML	1 E1	9,31
MOVISTAR CARACAS WS	TEL-CCS-WS	2 E1	31,42
MOVISTAR VALENCIA FM	TEL-VAL-FM	1 E1	29,02
MOVISTAR SAN CRISTOBAL FM	TEL-SCR-FM	1 E1	9,59
MOVISTAR MARACAIBO FM	TEL-MBO-FM	1 E1	24,12
MOVISTAR PTO. LA CRUZ FM	TEL-PLC-FM	1 E1	17,44
NET UNO CARACAS LD	NEO-CCS-LD	1 E1	28,50
DIGITEL CARACAS LD	DIG-CCS-LD	3 E1	66,07
DIGITEL VALENCIA LD	DIG-VAL-LD	1 E1	23,33

De los datos de la tabla anterior, es posible realizar el estudio de tráfico para comprobar el estado de los enlaces actuales. Para dicho estudio se utilizará el modelo de Erlang B, el cual supone que la cantidad de fuentes ó suscriptores del servicio son infinitos, y que las llamadas que son bloqueadas se eliminan inmediatamente.

Mediante la utilización de la Tabla existente para el modelo, la cual se encuentra en el Anexo 1, es posible hallar el número correcto de canales para dimensionar el sistema acorde al tráfico presentado, tomando como parámetro de grado de servicio el valor de 0,01, el cual indica que una de cada cien llamadas puede ser bloqueada. Los valores de dicha tabla son obtenidos a partir de iteraciones sucesivas haciendo uso de las fórmulas del modelo de Erlang B, las cuales se presentan como ecuación (2), (3) y (4) a continuación:

$$B(N,A) = \frac{\frac{A^N}{N!}}{\sum_{i=0}^{N} \frac{A^i}{i!}} \qquad (2)$$

$$B(0,A) = 1 \qquad (3)$$

$$B(N,A) = \frac{AB(N-1,A)}{N + AB(N-1,A)} \qquad (4)$$

En donde:

N = número de recursos disponibles, como circuitos.
A = tráfico total ofrecido en Erlangs.
B = probabilidad de bloqueo.

El resultado de estos cálculos es presentado en la Tabla 13:

Tabla 13. Cálculo de canales y enlaces necesarios

Ruta	*Número de Canales Necesarios*	*Enlaces E1 necesarios*
ENTEL CHILE	183	6,1 E1
AMERICATEL USA LDI	100	3,3 E1
AT&T LDI	88	2,9 E1
TELECOM ITALIA LDI	60	2 E1
CANTV CNT LDN	219	7,3 E1
CANTV CNT TANDEM	67	2,2 E1
CANTV CHACAO TANDEM	75	2,5 E1
CANTV VALENCIA LDN	133	4,4 E1
CANTV MARACAY LDN	83	2,7 E1
CANTV BARQUISIMETO LDN	79	2,6 E1
CANTV BELLA VISTA LDN	79	2,6 E1
CANTV SAN CRISTOBAL LDN	71	2,3 E1
CANTV PTO. LA CRUZ LDN	81	2,7 E1
CANTV PTO. ORDAZ LDN	55	1,8 E1
MOVISTAR CARACAS	128	4,2 E1
MOVISTAR CARACAS ML	23	0,7 E1
MOVISTAR CARACAS WS	54	1,8 E1
MOVISTAR VALENCIA FM	51	1,7 E1
MOVISTAR SAN CRISTOBAL FM	24	0,8 E1
MOVISTAR MARACAIBO FM	44	1,4 E1
MOVISTAR PTO. LA CRUZ FM	35	1,1 E1
NET UNO CARACAS LD	50	1,6 E1
DIGITEL CARACAS LD	97	3,2 E1
DIGITEL VALENCIA LD	43	1,4 E1

Comparando las Tablas 12 y 13, se puede notar la evidente congestión que presentan algunas de las rutas en la actualidad, situación que adicionalmente subsana la futura migración de éstas a rutas IP.

Para dimensionar la red en valores de ancho de banda que permitan el manejo del tráfico requerido, es necesario saber en primer lugar cuál es el codec a

utilizar para el servicio; el recomendado es el G.729 con 20ms de tiempo entre paquetes, esto dado a su buena relación compresión/calidad de voz. Adicionalmente, hay que considerar las sobrecargas en bytes que adicionan cada protocolo que se involucra en una trama para el servicio de VoIP. Sabiendo que el transporte de este servicio se hará sobre una red Ethernet, la sobrecarga introducida por la cabecera y la cola Ethernet es de 14 bytes y 4 bytes. De igual manera, la cabecera para los protocolos IP, UDP y RTP son 20 bytes, 8 bytes y 12 bytes respectivamente. Si se considera el uso de la técnica MPLS, se añaden 4 bytes adicionales a la trama.

Los valores en bytes de la carga útil se pueden calcular con la ecuación (5):

$$Payload(bytes) = \frac{CodecSpeed(bps)xDatagramDelay(ms)}{8\frac{bits}{byte}x1000\frac{ms}{s}} \qquad (6)$$

Utilizando como codec el G.729, cuyos valores son:

$$Codec\_Speed = 8000$$
$$Datagram\_Delay = 20ms$$

Da como resultado 20 bytes para la carga útil de voz.

Con la ecuación (7) es posible calcular el ancho de banda necesario por llamada (ocupación de canal), tomando en cuenta toda la sobrecarga que introducen los protocolos antes mencionados, el cual será:

$$BW(kbps) = \frac{FrameSize(bytes)x8\frac{bits}{byte}}{DatagramDelay(ms)} \qquad (7)$$

$$Frame\_Size(bytes) = (14+4+20+8+12+20+4)bytes = 92bytes \qquad (8)$$

De aquí se obtiene que el valor de ancho de banda medido en kbps necesario por canal para transmitir sólo los paquetes de voz es de 36,8 Kbps; este valor permite hacer el cálculo necesario en ancho de banda para cada ruta. Dado a los niveles de congestión, se tomarán los valores de canales que reduzcan el porcentaje de ocupación de las mismas. Los resultados calculados se muestran en la Tabla 14:

Tabla 14. Ancho de banda requerido por ruta

Ruta	***Número de Canales Propuestos***	***Ancho de Banda (Kbps)***
ENTEL CHILE	210	7728
AMERICATEL USA LDI	120	4416
AT&T LDI	90	3312
TELECOM ITALIA LDI	60	2208
CANTV CNT LDN	240	8832
CANTV CNT TANDEM	90	3312
CANTV CHACAO TANDEM	90	3312
CANTV VALENCIA LDN	150	5520
CANTV MARACAY LDN	90	3312
CANTV BARQUISIMETO LDN	90	3312
CANTV BELLA VISTA LDN	90	3312
CANTV SAN CRISTOBAL LDN	90	3312
CANTV PTO. LA CRUZ LDN	90	3312
CANTV PTO. ORDAZ LDN	60	2208
MOVISTAR CARACAS	150	5520
MOVISTAR CARACAS ML	30	1104
MOVISTAR CARACAS WS	60	2208
MOVISTAR VALENCIA FM	60	2208
MOVISTAR SAN CRISTOBAL FM	30	1104
MOVISTAR MARACAIBO FM	60	2208
MOVISTAR PTO. LA CRUZ FM	60	2208
NET UNO CARACAS LD	60	2208
DIGITEL CARACAS LD	120	4416
DIGITEL VALENCIA LD	60	2208

El total de ancho de banda para cursar el tráfico actual es de 82800 Kbps ó lo que es igual 82.8 Mbps, donde 17.6 Mbps corresponden al tráfico internacional y 65,1 Mbps al tráfico nacional, los cuales serán aumentados bajo demanda a medida que el tráfico de voz incremente acorde al paso del tiempo. Adicionalmente, pueden ser usadas técnicas para la supresión de silencios como la VAD (Voice Activity Detection) la cual reduce el ancho de banda usado en un 50%, pero se recomienda su uso sólo si se hace estrictamente necesario, ya que aumenta los tiempos de retardo, lo que puede convertirse en disminución de la calidad de la voz.

Los datos resultantes por rutas, demuestran que una red de *Core* basada en los estándares GigaEthernet (1 Gbps) y FastEthernet (100 Mbps) deberá sin inconvenientes manejar estas cantidades de ancho de banda; además deberá encontrarse correctamente dimensionada la red de transporte para que estas cifras de ancho de banda puedan ser manejadas por dichos enlaces.

Es importante destacar que el valor arrojado por los resultados del estudio, deberá ser reservado en la planificación de ancho de banda para los servicios de voz de la Empresa; otros servicios agregados como datos y video deberán ser calculados adicionalmente de manera de obtener el ancho de banda total requerido.

3.3 Solución de SBC y *Softswitch Nextone Clase 4*

Nextone ofrece una solución de manejo inteligente de sesiones, dando a los operadores una conectividad segura y escalable entre diversas redes IP. El sistema está constituido por 4 dispositivos principales: (a) El Nextone SBC, quien hace las veces de Session Border Controller asegurando conexiones bilaterales, (b) El Nextone

MSX, el cual es la plataforma para la interconexión de redes SIP y H.323, (c) El Nextone IMX (IP Multimedia Exchange), para la interconexión de redes VoIP e IMS[20] (IP Multimedia Subsystem) y (d) El Nextone RSM (Real Time Session Management), el cual se encarga de controlar de manera centralizada los dispositivos de borde de red antes mencionados.

El sistema es capaz de asegurar la red de VoIP contra ataques tradicionales de Internet como los de DoS, proveer del control de acceso a la red, proporcionar traducción de direcciones IP privadas a públicas ó IP privadas a privadas, usando NAT en tiempo real y posee suplementariamente métodos de regulación de consumo de ancho de banda entre redes y de ocultamiento de topologías (topology hidding).

La solución *Softswitch* de Nextone es capaz de realizar gran parte de las funciones de un *Softswitch*; posee un sistema de enrutamiento dinámico, permitiendo a los operadores establecer rutas según calidad, tarifas y disponibilidad, esto mediante lo que se conoce como caza de llamadas ó *call hunting*, además de realizar funciones de traducción de Codecs (transcoding). El sistema cuenta con un cliente ENUM (Telephone Number Mapping) que permite unificar el sistema de numeración tradicional propuesto por la norma E.164 de la ITU-T y el sistema de direccionamiento de internet DNS[21] (Domain Name System) lo que hace que sea

---

[20] IMS (IP Multimedia Subsystem). Estándar que define una arquitectura genérica para ofrecer servicios de VoIP y servicios multimedia, especificada por el grupo para proyectos en conjunto de tercera generación 3GPP (3rd Generation Partnership Project) y avalada por organizaciones como ETSI (European Telecommunications Standards Institute). El estándar soporta múltiple sistemas de acceso como GSM, WCDMA, CDMA2000 y WLAN. Disponible en: http://www.ericsson.com/products/hp/Ericsson_IMS__IP_Multimedia_Subsystem__pa.shtml

[21] DNS (Domain Name System). Es un servicio de directorio distribuido de internet. Es usado generalmente para traducir nombres de dominios en direcciones IP y adicionalmente para el control de entrega de correos electrónicos. Permite la búsqueda y apertura de manera rápida de sitios web. Disponible en: http://www.dns.net/dnsrd/

capaz de determinar si una llamada debe ser enrutada a una red IP ó a la PSTN. La arquitectura es manejada de manera centralizada por el módulo RSM, el cual obtiene del MSX los datos de cada llamada ó CDR, los cuales constan a su vez de más de 90 campos que describen la localización de los equipos terminales (endpoints), los datos intercambiados para el inicio de la sesión, duración y tarifa de la sesión, información de diagnóstico y mediciones de calidad.

Nextone ofrece un alto rendimiento basando su sistema en una arquitectura que separa las interfaces de señalización de las de *media*; esto permite total flexibilidad en la señalización y la sustentación del rendimiento y de la calidad de las llamadas cuando el sistema se encuentre frente a ataques externos. El equipamiento cuenta con configuración física redundante para los módulos MSX, y a su vez cada equipo cuenta con dos interfaces GigabitEthernet para señalización (privada y pública) y dos interfaces del mismo tipo para la media (privada y pública); adicionalmente cuenta con interfaces de 100 Mbps eléctricas para comunicación y control. La solución es totalmente escalable, permitiendo licenciamiento desde 500 hasta 30.000 sesiones concurrentes, lo que ofrece un alto volumen de tráfico.

Algunas características relevantes y protocolos soportados se presentan a continuación en la Tabla 15:

Tabla 15. Características y protocolos soportados por la solución de *Softswitch*

H.323	**H.323 versión 4** **H.225 RAS:** • **Registro por E.164 , H.323 ID** • **Soporte para grupos troncales origen o destino** • **Mensajes RAS (LRQ,RRQ,ARQ,DRQ,URQ)*** • **Registro de *endpoints* estáticos** **H.245 *tunneling*** **T.38 Fax Relay (UDP)** **Seguridad H.235**
SIP	SIP *Proxy* SIP *Back-to-Back User Agent* SIP *Redirect Server* SIP/H.323 *Interworking* RFC 3261 SIP RFC SDP (Session Description Protocol) RFC 1889 RTP RFC 2833 DTMF, Tonos y Señales Telefónicas SIP T.38 Fax Relay SIP *Session Timers* Autenticación SIP soportado en RADIUS (Remote Authentication Dial In User Service) Soporte de RFCs: 2976,2069,2138,2139,3264,3323,3325,3326,2617,3262,3372,3265,3515,3842
Enrutamiento Multiprotocolo y Control de Admisión de Llamadas	Enrutamiento de llamada basado en Tiempo del dia ó Tipo de servicio *Call Hunting* según prioridad, capacidad, o configuración por códigos ISDN ó SIP Enrutamiento basado en capacidades (Max. De llamadas, Max de llamadas por min, Límite de tarifa) Traducción de números discados Traducción de ANI Bloqueo de llamadas Enrutamiento basado en grupos troncales Generación de CDR con más de 90 campos
Enrutamiento y Procesamiento de Media	Procesamiento y enrutamiento selectivo de media Traduccion NAT y traducción de puerto PAT (Port Address Translation.) NAT transversal para uso con redes de banda ancha *Firewall* dinámico para control de media y control de acceso Codec y DTMF (Dual-tone Multifrequency) transcoding

**LRQ (Location Request), RRQ (Registration Request), ARQ (Admission Request), DSQ (Disengage Request), URQ (Unregister Request).*

3.4 Actualización de equipos de *Core*

La necesidad de la Empresa de ofrecer servicios integrados de telecomunicaciones basados en redes IP y de soportar una arquitectura temporal de tipo mixta (TDM-IP), trae como consecuencia la implementación de tecnología *Softswitch* y la inserción de un número importante de Media Gateways para cubrir las rutas TDM en IP, unido a esto, el manejo de ancho de banda y el aumento en procesamiento al incorporar los servicios de voz, datos y video en la red IP, conllevan a un alto consumo de interfaces y de capacidad de procesamiento que la red Ethernet actual no posee. Para cubrir estas necesidades y mantener la calidad de servicio, se propone la sustitución de los equipos actuales por un conjunto de *routers* y *switches* de *Core* que ofrezcan tanto solución a lo planteado como mejoras, en cuanto a rendimiento, calidad y seguridad. Cabe destacar que por petición de la Vice Presidencia de Ingeniería y Operaciones de la Empresa los productos a ser adquiridos deben ser de la marca Cisco Systems.

Tomando en cuenta lo anterior señalado, los equipos *routers* propuestos para el *Core* constan de dos chasis del modelo 7609; estos equipos tienen la capacidad de manejar servicios IP/MPLS de alto rendimiento con una capacidad de procesamiento de hasta 720 Gbps y con una variedad amplia de interfaces que van hasta velocidades máximas de 10Gbps; incorpora de igual manera servicios de admisión y control para sesiones de video y VoD (Video on Demand). Cada uno de estos chasis cuentan con 2 fuentes de poder redundantes de 4000W a -48V DC, una tarjeta supervisora Cisco *Route Switch Processor* 720 (RSP720-3C), la cual tiene una capacidad máxima de procesamiento de 720Gbps repartida entre sus nueves ranuras o slots; cuenta de igual forma con 4 puertos GigabitEthernet ópticos (4X1GE) para la conexión entre *router* y *Switches* y un módulo de interfaz STM-1 canalizado (OC-3/STM-1) para ser conectado directamente al multiplexor SDH Marconi. (Más especificaciones del *router* 7609 en el Anexo 2).

Los equipos de *switches* propuestos son los pertenecientes a la nueva gama Catalyst 6509-E, los cuales cuentan con una capacidad de procesamiento semejante a la familia de *routers* propuestos, esto debido al uso de la misma tarjeta procesadora (RSP720-3C); los *switches* cuentan con características para el soporte de servicios como: *tunneling* 802.1Q, Ethernet sobre MPLS, QoS en capa 2 y capa 3 e incorporación de interfaces de hasta 10Gbps. Adicionalmente cuentan con una tarjeta de 48 puertos de interfaz eléctrica RJ-45 GigaEthernet autosensora de 10/100/1000 Mbps (WS-X6148V-GE-TX) y una tarjeta de 24 puertos ópticos GigabitEthernet (WS-6724-SFP). Una adición importante a los *switches* es la incorporación de módulos FWSM (Firewall Security System), los cuales hacen uso del procesamiento de 720 Gbps de la tarjeta procesadora; estos módulos proveen de protección contra ataques DoS y virtualización de hasta 250 Firewalls. Este módulo incorpora las funcionalidades de la serie Cisco PIX actual de la Empresa, pero con la ventaja de mayor procesamiento, de manera de impactar en mucho menor grado el retraso de los paquetes dado su paso por el mismo. (Más especificaciones del *Switch* Catalyst 6509-E en el Anexo 3).

En la Figura 22 se podrá notar la manera en la que el equipamiento propuesto se conectará a la red.

3.5 Esquema propuesto transitorio de red y reestructuración de VLANs

El esquema de la red estará soportado en un *backbone* redundante conformado por dos *routers* Cisco 7609 y dos *Switches* Cisco Catalyst 6509-E, antes mencionados. La conexión entre *routers* se hará utilizando uno de los puertos GigabitEthernet dispuestos en cada uno, de manera que sea el enlace que permita la redundancia y el balanceo de carga entre ellos. La conexión de *routers* a *switches* se realizará mediante el uso de uno de los cuatro puertos GigabitEthernet en cada *router*, los cuales se conectarán a cada *switch* a través de la tarjeta de 24 puertos ópticos dispuestos en ellos; otro puerto adicional de los 24 existentes se utilizará para la

conexión entre *switches*. Este conjunto de conexiones entre los enrutadores y los *switches* permitirán crear un anillo redundante MPLS que ofrezca una conmutación de alta velocidad y prioridad de tráfico que garantice QoS a los servicios de VoIP.

La conexión del *Softswitch* Nextone estará soportada por el *backbone* redundante conformado por los dos *Switches* Cisco Catalyst 6509-E y los dos *routers* Cisco 7609. A esta redundancia se le agrega la propia de la solución de *Softswitch* a través de los dos módulos de enrutamiento MSX, uno en modo activo y otro en modo *stand-by*. La conexión de los puertos entre el Nextone y cada *switch* Catalyst se realizará mediante conectores de fibra de tipo LC en ambos extremos; cabe destacar que son necesarios 4 conexiones de este tipo por equipo MSX, las cuales son: señalización privada, *media* privada, señalización pública y media pública, cada una con una dirección IP asignada; las interfaces privadas son las que comunican directamente con los equipos de *core*, por ejemplo *gateways*; mediante las interfaces públicas se recibe o envía el tráfico hacia otros operadores. A esto debe sumarse una interfaz eléctrica RJ-45 para gestión y monitoreo del equipo, y otra en la misma interfaz para la redundancia o *fail-over* entre ambos MSX. Para el módulo RSM se requiere una interfaz RJ-45 para la gestión del mismo y para la comunicación con los módulos MSX.

La Figura 21 muestra en detalle la conexión entre el Softswicth Nextone y los *Switches* Cisco Catalyst.

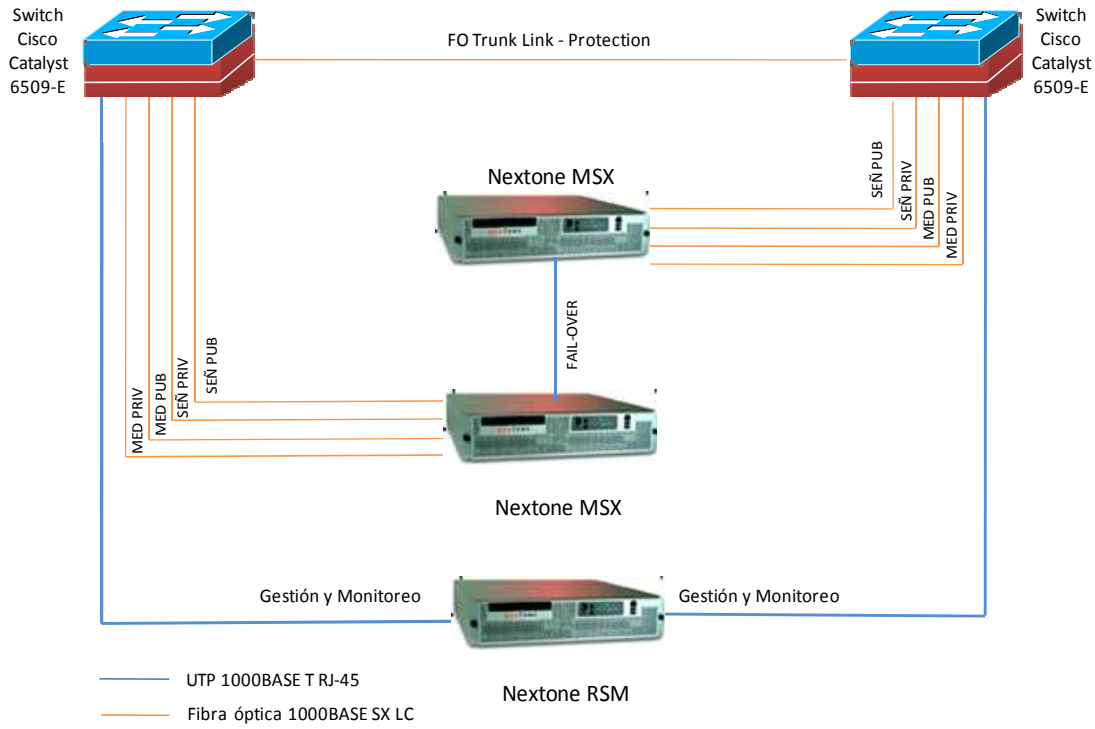


Figura 21. Conexión *Softswitch* Nextone – *Switches* Cisco Catalyst 6509-E

Fuente: Figura propia.

Con el fin de cumplir con una primera fase de migración donde se involucren la solución TDM con la solución IP, un equipo Media Gateway es requerido para la conexión entre el *switch* TDM ANS y el equipo Nextone, el cual será el encargado de realizar la traducción entre ambos equipos. En este Media Gateway, perteneciente a la familia de Access Server 5400 de Cisco, se configurarán las rutas (*dial- peers*) que permitirán la comunicación, haciendo uso del protocolo SIP en su versión 2, lo cual se llevará a cabo mediante interfaces eléctricas RJ-45 conectadas a ambos *Switches* de *Core*, de manera de crear redundancia y balanceo de carga haciendo uso de los protocolos propietarios de Cisco HSRP (Hot Stand By *Router* Protocol) y GLBP (Gateway Load Balancing Protocol). En principio se

realizará la migración de todas las rutas TDM internacionales a IP, dado a que la mayoría de empresas de telecomunicaciones (*carriers*) internacionales manejan su trafico LDI sobre redes de telefonía IP y adicionalmente por ahorro de costos, tomando en cuenta esto y partiendo del número de canales propuestos en el estudio antes realizado, para la conexión internacional se requerirán algo más de 12 E1, por lo que sería conveniente el uso de un Media Gateway de 16 canales, configuración más cercana al valor estimado con anterioridad (este número se basa en especificaciones de equipos Media Gateway Cisco).

La compatibilidad entre el *switch* ANS y los Media Gateways Cisco se logra mediante el uso del protocolo de señalización ISDN-PRI; las conexiones serán realizadas a través de las interfaces PRI de los AS 5400; esta interfaz consta de un peine de conectores RJ-.45 cuyos terminales extremos se encuentran bajo la norma G.703 de la ITU-T en formato de conector tipo BNC (Bayonet Neill-Concelman), el cual es muy usado en aplicaciones de telefonía, video y comunicaciones de radio frecuencia. Los puertos E1 del *switch* Ericsson se deberán cablear directamente en el distribuidor principal MDF (Main Distribution Frame) donde son conectados mediante conexiones cruzadas (cross-conexiones) con los puertos donde se encuentran los E1 provenientes del Media Gateway Cisco de manera de completar la conexión ANS – Media Gateway – Nextone. De igual forma, la conexión entre la central que surte de servicio telefónico corporativo interno Ericsson MD110 y el *Softswitch*, se realizará mediante el *switch* público ANS haciendo uso del E1 ya operativo entre ambas y la conexión del ANS al Nextone antes comentada; la única distinción radica en que la señalización usada entre el ambos *Switches* TDM es del tipo R2, protocolo que también es manejado por la serie AS5400 de Cisco.

Dada la característica de libre marcación y suscripción de las plataformas Prepago y CDC respectivamente, es importante notar que el origen de estas llamadas es proveniente de la red PSTN, por lo que la conexión de estas arquitecturas deben seguirse manejando de la misma manera para la originación (ANS-Media Gateway)

cuando se trata de terminación nacional; para terminaciones internacionales, ambos Media Gateways deberán ser conectados a través de los *Switches* Catalyst al *Softswitch* Nextone.

De manera de ofrecer buenos niveles de QoS para los servicios de voz y datos, es aconsejable mantener estos tráficos por separado; para esto la configuración de VLANs en los *Switches* de *Core*, deberá designar qué puertos del mismo corresponden a cada VLAN, así se asegura que cada equipo esté conectado al segmento para el cual están designados según el tipo de servicio que prestan; dicha distribución se propone de la siguiente manera:

a) **VLAN 1:** será la encargada de transportar los datos que son transmitidos o recibidos por los servidores que prestan servicios de seguridad, autenticación, mediación y facturación del *Core* de la red; de igual manera se incluirán los servidores que dan soporte a la red de usuarios en cuanto a aplicaciones y archivos. Esta VLAN se encontrará separada del corazón de la red como función de aislamiento de topología y control de acceso de los usuarios al *Core*. La solución de Firewall PIX de Cisco cumplirá con estas funciones a través de DMZs.
b) **VLAN 2:** corresponde a la VLAN para los servicios de voz; dará soporte de red a todos los equipos que conforman la plataforma de telefonía IP de la Empresa y donde se configurarán los accesos a los puertos que requieren los protocolos de VoIP y transporte IP que son necesarios para las conexiones de voz. Éstos estarán protegidos por la solución de Firewall Cisco que se integra dentro de los *Switches* Catalyst propuestos dado al alto rendimiento en procesamiento del módulo, parámetro de gran importancia si no se quiere añadir más retardo del esperado en los servicios de voz.
c) **VLAN 3:** asociada al segmento donde se encontrarán las sub redes de usuarios de la Empresa y donde se encontrarán estaciones de trabajo y

sistemas de impresión. La VLAN se encontrará protegida por un segundo Firewall PIX Cisco, permitiendo el control de acceso hacia las otras VLANs.

d) **VLAN 4:** corresponde a la VLAN que soportará los servicios de gestión, monitoreo y respaldo; a su vez contendrá todos los servidores que apoyan los sistemas antes mencionados, lográndose a través de la configuración de las interfaces correspondientes de los equipos de comunicaciones y servidores críticos como: gestión del Nextone, del *switch* ANS, sistemas de monitoreo de red, respaldo de bases de datos, entre otros. Esta VLAN por separado permite que las funciones que ella cumple no se vean afectadas por fallas parciales o segmentos de la red.

De manera de esquematizar la solución transitoria, donde se involucren el *Softswitch* Nextone y la Central Ericsson ANS (TDM-S e IP), se hace útil proponer un esquema de red contemplando los tipos de cableados a utilizar, distribución de VLANs e interfaces. Por facilidad, se han colocado las conexiones entre el *Softswitch* Nextone y los *Switches* 6509-E de manera unifilar. En la Figura 22 se presenta dicho esquema:

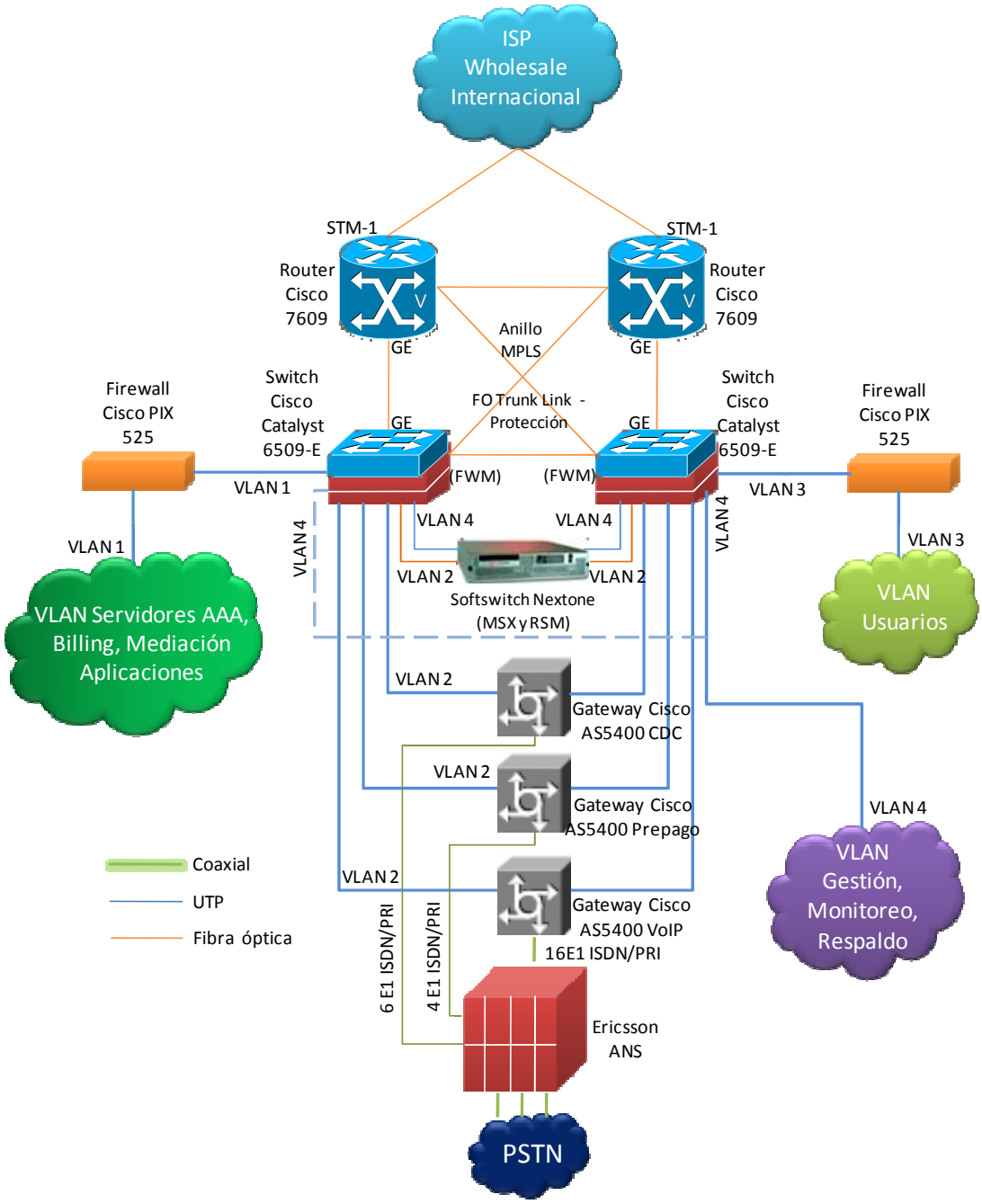


Figura 22. Esquema transitorio de red propuesto

Fuente: Figura propia.

3.6 Redimensionamiento de la Red de Transporte

Tras la disminución del ancho de banda requerido para el tráfico de las rutas de telefonía, como consecuencia de la migración a telefonía IP, se hace necesario el redimensionamiento de la red de transporte, esto debido a la reducción de costos que conlleva y al aporte que da a la culminación de la migración total de los servicios de voz. Básicamente el redimensionamiento se aplicará tanto a la red de transporte nacional como a la internacional.

3.6.1 Redimensionamiento de la Red de Transporte Nacional

De manera de cumplir con la migración total de la infraestructura de telefonía TDM y de reducir los costos en transporte, se propone la migración a IP de la red de transporte nacional buscando reducir el número de enlaces que son requeridos para cada localidad. Con basamento en el estudio que se realizó en este Capítulo, es posible obtener el dimensionamiento de los enlaces requeridos para cubrir el tráfico de la plataforma en IP. Dado a que la Comisión Nacional de Telecomunicaciones establece en norma, donde el tráfico entre operadores debe realizarse utilizando protocolos de señalización por canal común CCSS7, la terminación en las rutas de los operadores nacionales seguirá siendo por los momentos en TDM. Para que el transporte de ese tráfico sea recibido en el *Softswitch*, éste debe convertirse en IP, lo que requiere un estudio de ingeniería por localidad que dé solución a lo planteado. Para resolver el problema, deberá instalarse un equipo de Media Gateway en los predios del operador, para que éste sea el que convierta a IP el tráfico presente en ese nodo. Para esto debe entregarse un "Proyecto de Coubicación" al operador respectivo. La Coubicación permitirá el trasporte de los paquetes IP a través de los enlaces, de manera que sean recibidos por el *switch* de *Core* y éstos sean entregados al *Softswitch*. Los E1 provenientes de los distribuidores del operador se encuentran normados bajo G.703 con conectores del tipo BNC y/o Mini BNC, éstos deben ser conectados a un panel en donde son cross-conectado con el equipo de

Media Gateway. Las tres interfaces del Media Gateway (Señalización, Media y Gestión) serán conectadas a un *switch* colocado en la coubicación de donde se extraerá la interfaz de conexión de salida para el transporte de los paquetes hasta el *switch* Catalyst en el *Core*, el cual a su vez entregará el tráfico al *Softswitch*.

En la Figura 23 se muestra una arquitectura general de los proyectos de coubicaciones en los operadores nacionales.

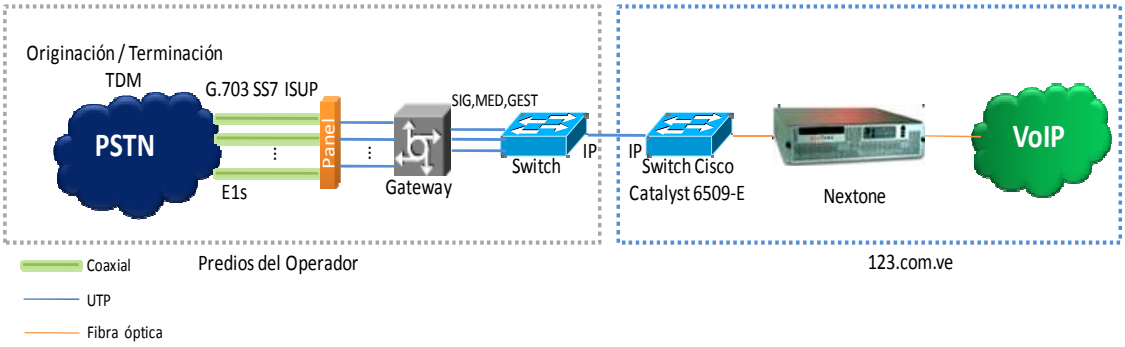


Figura 23. Arquitectura general para los proyectos de Coubicaciones

Fuente: Figura propia.

3.6.2 Redimensionamiento de la red de transporte internacional

Como se mencionó en el Capítulo II, la red de transporte internacional está conformada por 3 enlaces DS-3 de 45 Mbps divididos cada uno en 21 E1s; el primero de ellos pertenece a las conexiones entre los multiplexores SDH Marconi de la Empresa, el cual deberá transportar todo el tráfico de la red internacional; los otros dos enlaces pertenecen, uno a la conexión hacia EE.UU donde se encuentran conectadas las rutas con AT&T, Americatel y Telecom Italia, y el otro enlaza las rutas con Entel Chile, donde se hallan entre otras rutas, la conexión hacia Cuba.

Tomando como referencia el estudio realizado para las rutas, y en específico para las internacionales, puede observarse que para el enlace con EEUU (rutas de AT&T, Americatel y Telecom Italia) serán suficientes 9 Mbps en la actualidad, y el enlace hacia Entel deberá transportar 12 Mbps para el servicio de Internet y unos 7 Mbps para las rutas enlazadas hacia Chile y Cuba. Por lo que el DS-3 entre Global Crossing y la Empresa cargará con 28 Mbps aproximadamente.

Observando estos valores, es evidente la reducción de ancho de banda lograda con la migración de las rutas a IP; este nuevo escenario abre las puertas a la posibilidad de reducir el ancho de banda para el transporte internacional, sobre todo en los dos enlaces DS-3 hacia los operadores (EEUU y Chile); lo cual se traduce en reducción de costos; siempre teniendo en cuenta de dejar un ancho de banda holgado de guarda para servicios agregados, y que a su vez permita el crecimiento según la demanda de tráfico en la red.

3.7 Esquema propuesto definitivo de Red

Tras el redimensionamiento de la Red de Transporte de la Empresa, se hace posible la migración de la totalidad de las rutas a VoIP; las rutas LDI, a través de la conexión directa en IP con los operadores internacionales, y las rutas LDN, haciendo uso de los proyectos diseñados para las coubicaciones y la arquitectura planteada para éstos. De esta forma, es posible lograr un escenario totalmente IP, tanto en conmutación como en transporte; en donde el servicio de voz quede totalmente centralizado en el *Softswitch Clase 4 Nextone*, otorgando facilidad de gestión, calidad de servicio y ahorros de ancho de banda. En la Figura 24, se muestra el esquema definitivo de la red, donde se ha sustituido por completo al switch TDM-S Ericsson ANS, se han eliminado los gateways utilizados para la conexión Nextone – ANS y se han sustituido los gateways que soportaban aplicaciones de IVR para la plataforma prepago y de CDCs, por servidores de aplicaciones capaces de realizar dichas funciones.

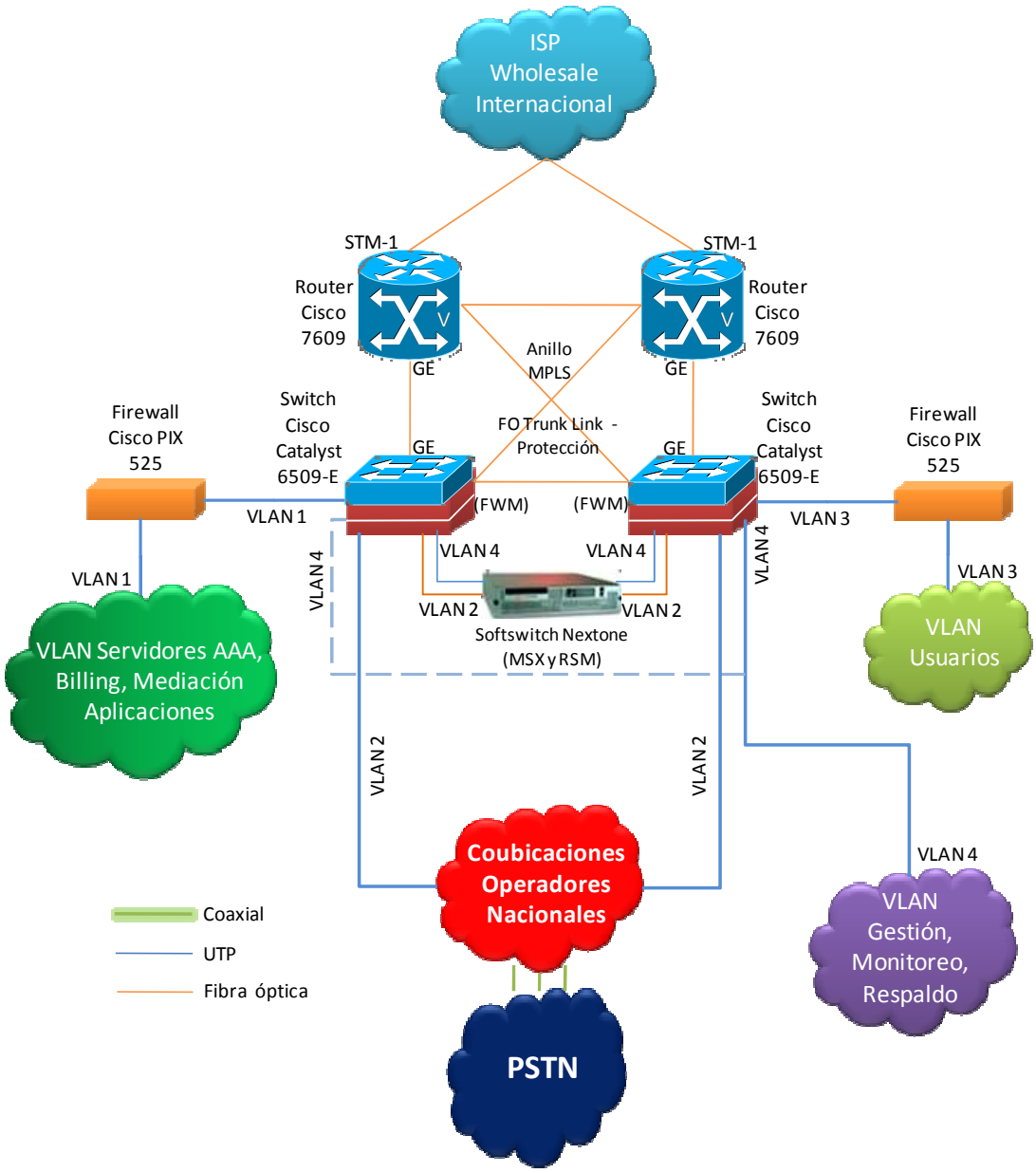


Figura 24. Esquema definitivo de red propuesto

Fuente: Figura propia.

CAPÍTULO IV

PROTOCOLO DE PRUEBAS

En ambientes de redes de telecomunicaciones públicas, la conversión de conmutación de circuitos digitales a redes de conmutación de paquetes, pasa por un proceso de reestructuración de arquitectura, de la calidad de servicio y del manejo de red. Aparte de esto, un aspecto de gran importancia en la implementación de modelos de NGN, es la prueba de compatibilidad entre equipos y la coexistencia de nuevos servicios con los ya implementados.

La futura introducción de la solución de *Softswitch* de Nextone en la red, acarrea una serie de cambios tecnológicos importantes, que permiten a la Empresa ofrecer servicios de vanguardia, así como el ahorro de costos y el beneficio operativo que esta solución ofrece. Dada la importancia y el alto costo de la implementación, la inserción del *Softswitch* debe estar respaldada por una serie de parámetros que aseguren la perfecta interoperabilidad y el cumplimiento de todas las especificaciones, estándares y garantías que el sistema provee.

Para el cumplimiento de esta tarea, es necesario diseñar una serie de procedimientos y pruebas acordes con las recomendaciones, estándares internacionales y expectativas de la Empresa para con el nuevo modelo.

El protocolo de pruebas a desarrollar para la futura inserción del equipo, está íntimamente relacionado a las funcionalidades, características y capacidades que ofrece el mismo, de manera de lograr un resultado que se adapte a la realidad de la futura arquitectura de red. Dicho protocolo puede encontrarse en el Anexo 4.

A continuación se presenta un esquema general del ambiente de pruebas para la aplicación del protocolo:

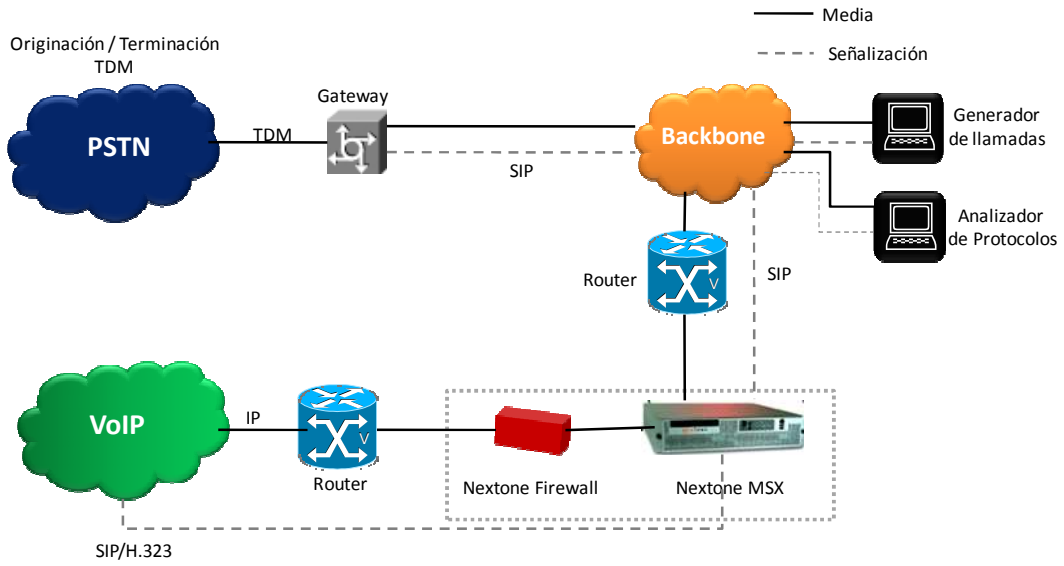


Figura 25. Esquema general del ambiente de pruebas

Fuente: Figura propia.

4.1 Modelo de protocolo de pruebas

El modelo propuesto para protocolo de pruebas, consta de las siguientes pruebas:

4.1.1 Pruebas de estrés

La calidad de transmisión de la red depende de su diseño y tamaño; ambos factores afectan el número de llamadas VoIP que ésta puede manejar. La mejor manera de determinar la capacidad de llamadas VoIP que la red puede soportar es mediante pruebas de estrés que simulen dichas llamadas. Estas pruebas deben ser programadas con las configuraciones máximas permitidas por el equipo; esto permite verificar el comportamiento del sistema bajo diferentes patrones de carga y estrés.

Las pruebas de estrés presentadas a continuación tienen como objetivo verificar la robustez y seguridad de la solución, generando una amplia gama de ataques potenciales diseñados para degradar o suprimir los servicios de VoIP. Éstas son:

4.1.1.1 Prueba de mensajes de inundación SIP (SIP Flood Tests)

Consiste en realizar un flujo de llamadas de ataque para generar estrés, utilizando mensajes de invitación, registro y respuesta proveniente de millares de direcciones y puertos generados al azar. Esta prueba requiere que el equipo esté conectado a la red en operación normal y puede llevarse a cabo con la utilización de una herramienta de estrés (software o hardware) que simule un escenario con millares de ataques y direcciones aleatorias. Los objetivos principales que se persiguen al aplicar esta prueba son: verificar la correcta formación y formato de mensajes SIP según los comentarios extraídos de la RFC 3261 de la IETF, comprobar la normal ejecución de secuencias de llamadas SIP, y adicionalmente hacer que el sistema sea capaz de protegerse así mismo y al Proxy Server contra ataques externos.

4.1.1.2 Prueba de tortura SIP (SIP Torture Test)

Esta prueba se lleva a cabo formando mensajes SIP de invitación y registro modificados o mal formados con diferentes campos, cabeceras y direcciones. Estos mensajes SIP mal formados pueden generarse mediante equipos o software de simulación; para esto puede tomarse como referencia la generación de mensajes de tortura según la IETF en su RFC 4475. Es necesario como condición para realizar la prueba, que el equipo esté conectado a la red, y que esté funcionando en condiciones normales de operación.

Es recomendable que la prueba se haga enviando simultáneamente millones de mensajes cortos mal formados, y que a la vez se hagan cursar por el equipo gran

cantidad de llamadas de manera de verificar si éstas son afectadas; esto para simular un ataque malicioso cuando el equipo este cursando tráfico en condiciones normales.

4.1.1.3 Prueba de ataques RTP y negación de servicio DoS (Denial of Service)

Consiste en generar ataques de mensajes RTP fraudulentos, de manera de obtener gran cantidad de mensajes de negación siguiendo la norma RFC 3550 de la IETF; esta tarea es realizada por un software o hardware de simulación que genere millones de intentos desde direcciones y puertos aleatorios. Con los CDR creados por el equipo deberá ser posible identificar problemas de calidad de servicio en llamadas que son cursadas en el momento de la prueba.

4.2 Pruebas de reporte de alarmas

Las pruebas de alarmas consisten en verificar la generación de éstas, tras acciones que puedan ocurrir en condiciones de operación, de manera que puedan ser vistas por el/los operadores, es decir, que en condiciones de funcionamiento normal del equipo, se recomienda provocar alarmas y verificar que pueden ser observadas en cada estación de trabajo y monitoreo a través de las ventanas de alarmas del sistema. La prueba se regirá según los tipos de alarmas que el equipo sea capaz de generar.

Los tipos de alarmas a ser chequeados se presentan en la Tabla 16. Estas alarmas pueden ser provocadas por el simulador realizando llamadas sucesivas ó por acciones manuales que permitan la activación de las mismas; como por ejemplo una caída total o parcial realizada mediante la activación o desactivación intencional de módulos del equipo.

Tabla 16. Tipos de alarmas generales

Tipo de Alarma	*Descripción*
Desconexión Local	Se activa encaso de que un fallo interno cause una desconexión del sistema
Promedio de completación de llamadas	Porcentaje de llamadas exitosas sobre el número total de llamadas recibidas o realizadas. Se activa cuando el valor es mayor, menor o iguala un umbral definido.
Limite de minutos	Se activa cuando el total de minutos consumidos es igual, excede o es menor a un valor predefinido (prepago)
Límite por tarifa	Es activada cuando el valor acumulado en moneda (por tráfico tarificado) excede el valor umbral establecido.
Promedio de duración de llamadas	Se enciende cuando el valor promedio de duración de las llamadas coincide con uno preestablecido. Puede ser usado cuando el valor es muy corto (5 seg o menos), indicativo de un posible problema
Retraso Post Marcado	Se activa cuando el tiempo de espera después de marcar coincide o excede un valor pre configurado, posible indicativo de problemas en la red.
Alta pérdida de paquetes	Tiene que ver con los valores de *Packet Loss* extraídos de los CDR, es activada según el valor limite configurado.
Variación de retardo de paquetes o Jitter	Referida al valor de jitter medidos en las llamadas. Es activada al ser inferior o superior del valor pre establecido.

4.3 Pruebas de seguridad y *Log Management*

Las pruebas de seguridad y *Log Management* permiten en esencia comprobar la vulnerabilidad del equipo ante situaciones o acciones que pongan en riesgo la integridad del mismo y de la red en general. Las pruebas correspondientes a seguridad y *log management* son:

4.3.1 Pruebas de seguridad e ingreso de usuarios

Estas pruebas consisten en comprobar si el sistema es capaz de permitir o rechazar el ingreso de usuarios, así como sus niveles de autoridad una vez que hayan ingresado en el sistema. Las mismas deben ser llevadas a cabo una vez que el equipo se encuentre instalado y operando; además deben encontrarse creados los perfiles de acceso. Las pruebas a realizar para comprobar la correcta funcionalidad son:

a) Intentar ingresar al sistema de operación y mantenimiento sin nombre de usuario y contraseña, como usuario válido pero contraseña errada o sin contraseña alguna. El sistema debe automáticamente rechazar el ingreso.
b) Intentar ingresar con un usuario permisado, es decir, con nombre de usuario y contraseña, ambos válidos; se espera que el sistema le dé ingreso normalmente.
c) Asegurar los niveles de seguridad de un usuario una vez se encuentre en el sistema según su perfil de acceso. Un usuario de administración del equipo debe crear un perfil con ciertas restricciones; el usuario creado debe ingresar y realizar una acción o ejecución de comandos para los cuales no se encuentra autorizado. Se espera que el sistema rechace toda acción no autorizada.
d) Tratar de ingresar al sistema desde la red de Internet mediante direcciones de IP (privadas o públicas) no autorizadas; el sistema debe rechazar los intentos de ingreso.

4.3.2 Pruebas de seguridad y auditoría

El sistema debe garantizar que se generen los reportes de auditoría donde se muestre entre otras cosas: (a) Nombre de usuario, (b) Datos como fecha, hora, dirección de acceso, entre otros, (c) Cambios efectuados, bien sean en configuraciones de sistema, cambios de rutas y tasaciones. Para esto, el equipo debe

encontrarse en normal operación y que un usuario registrado provoque cambios en el equipo de manera que éstos puedan ser monitoreados en el reporte o Log del sistema.

4.4 Pruebas de fiabilidad

Las pruebas de fiabilidad permiten comprobar la robustez de la solución tanto en software como en hardware, de manera de comprobar si el equipo es capaz de resistir caídas del sistema, bien sea por fallo interno, desconexión y daño de interfaces ó por la supresión de servicio de energía. Para comprobar esto, las pruebas a realizar están descritas a continuación:

a) Provocar el reinicio tanto de los servidores de *switch*, como de los servidores de interfaz y gestión; esto con el fin de comprobar que el equipo es capaz de regenerar el servicio, control y monitoreo sin ninguna dificultad y sin la intervención de operador alguno.
b) Desconexión de las interfaces físicas (puertos) de los equipos, con el fin de simular fallas en las tarjetas de interfaz o corte de comunicaciones por falla del medio, ruptura u otros. Del sistema se espera la activación de la redundancia en caso de existencia, y la generación de las alarmas correspondientes.
c) Quitar toda alimentación de los equipos, de manera de simular una caída por fallo de alimentación. Esta prueba puede realizarse suprimiendo el servicio eléctrico a todos los equipos o a uno en particular, así puede confirmarse la funcionalidad de redundancia en caso de existir. Los resultados esperados deben ser un reinicio del servicio exitoso o la activación de un sistema de respaldo de energía, que evite la supresión del servicio de comunicaciones.

4.5 Pruebas de calidad de servicio (QoS)

A este nivel se busca medir indicadores de rendimiento de parámetros relacionados con la calidad de servicio de acuerdo a niveles establecidos en estándares internacionales.

4.5.1 Pruebas de Jitter ó PDV (Post Delay Variance)

Estas pruebas permiten medir en la red si el retardo relativo de todos los paquetes que llegan al destino es tal que la calidad de servicio no se vea afectada. El valor debe estar contenido en los recomendados por la norma Y.1541 de la ITU-T para el rendimiento de servicios basados en IP. Para esto, se deben generar llamadas con el protocolo y códec a utilizar, de manera de obtener los valores de Jitter asociados a la red de VoIP bajo prueba.

4.5.2 Pruebas de retardo

Para la medición del retardo presente en la red, se debe generar un flujo de llamadas de manera de obtener el valor de retardo de las mismas, el valor medido se recomienda que esté comprendido entre los dados por los estándar G.144 y Y.1541 de la ITU-T para no afectar la calidad de servicio del sistema. Para la realización de la prueba, el equipo debe estar en funcionamiento normal, es recomendable que el número de llamadas sea alto de manera de comprobar de igual forma si la operación bajo alta carga afecta estos valores.

4.5.3 Pruebas de pérdidas de paquetes (Packet Loss)

Con el equipo configurado y en normal funcionamiento, consiste en medir el valor de pérdida de paquetes tras el curso considerable de tráfico telefónico, de manera de comprobar que dicho valor se encuentre en los valores recomendados por

la norma Y.1540 de la ITU-T referente al rendimiento de servicios basados en IP, y que no afecte la calidad de servicio esperada por la Empresa y el usuario.

4.5.4 Pruebas de MOS

Como anteriormente se ha comentado, la característica subjetiva del valor de MOS conlleva a que la prueba sea realizada no a través de medios técnicos sino directamente a los usuarios del sistema telefónico. Es por esto, que la prueba se recomienda sea aplicada a sujetos de la Empresa. Aprovechando que la red de telefonía será en primera instancia de carácter mixto (TDM e IP), el ambiente es propicio para que se lleven a cabo dichas pruebas. Los sujetos preparados para las pruebas deberán realizar llamadas utilizando terminales dispuestos para tal fin conectados a la red tradicional de telefonía; seguidamente realizar llamadas a los mismos destinos haciendo utilización de terminales conectados a la red de VoIP, esto con el fin de aplicarle encuestas que contengan los parámetros de evaluación de calidad de voz y esfuerzo dispuestos en la recomendación P.800 de la ITU-T.

4.6 Pruebas adicionales

Para cumplir con los requerimientos internos de la Empresa, las pruebas de funcionalidades son útiles para soportar la actividad y el funcionamiento diario de ésta y asegurar la buena y segura operación de la plataforma. Las pruebas adicionales propuestas son:

4.6.1 Prueba de respaldo

Para esta prueba se deben generar respaldos de distintos datos y configuraciones del sistema; los respaldos más críticos e importantes comprenden los reportes de llamadas ó CDR y configuraciones críticas de red, firewall, configuraciones de los agentes de *switch* y de gestión del equipo, parámetros de

sistema operativo, *logs* y *scripts*. Paso seguido, se debe confirmar el respaldo de los parámetros antes mencionados en las localidades preestablecidas para esto.

4.6.2 Pruebas de configuración

Consiste en comprobar la capacidad de configuración del equipo respecto a protocolos y dispositivos (End Points) SIP y H.323 como SIP Gateways, H.323 Gateways, H.323 Gatekeepers, IP Phones, entre otros; adicionalmente realizar y comprobar la creación de rutas y características asociadas a éstas como destinos, el mejor costo por ruta (Less Cost Routing), limitaciones en cantidad de llamadas y realizar configuraciones generales respecto a módulos de configuración de parámetros de red, agentes del sistema, servicios, personalizaciones, seguridad y firewall, parámetros de acceso, auditorias, reportes y alarmas, todo para comprobar y verificar las funcionalidades ofrecidas por la solución.

4.6.3 Pruebas de facturación y *Billing*

Consiste en realizar la configuración de tarifas y tasaciones a rutas de pruebas, de manera de generar un tráfico a través de dichas rutas y comprobar su efectiva tarificación en el sistema gestor; adicionalmente, verificar que los datos sean almacenados de manera correcta en el servidor de *billing* de la Empresa y que éste refleje los datos exactos arrojados por los CDR que genera la solución; estos permitirán culminar la prueba de facturación de manera exitosa.

CAPITULO V

METODOLOGÍA TÉCNICA PARA LA MIGRACIÓN DE LAS RUTAS TDM A IP

En este capítulo se hace referencia a la metodología técnica propuesta para migrar una red basada en telefonía TDM hacia una basada en telefonía IP, dando un enfoque general de los pasos que se recomiendan seguir a cualquier Empresa operadora de larga distancia que tenga la necesidad de realizar una migración de este tipo.

5.1 Levantamiento de información

El primer paso a seguir en la metodología propuesta para la migración, consiste en recopilar todas las especificaciones técnicas que permitan tener una visión clara de la red. Las especificaciones más importantes a considerar son descritas a continuación:

a) **Red:** es importante conocer en la red de telefonía, la distribución de los nodos, de forma de identificar los puntos de enrutamiento, señalización y tráfico de voz, así como también el punto de donde se obtiene el sincronismo del sistema. Adicionalmente, resulta relevante el poder identificar las topologías pertenecientes a la red Ethernet y a la red de telefonía conmutada por circuitos. Lo anterior permite entender el trabajo que realiza la red en cada uno de sus nodos en cuanto al camino que siguen las señales y cómo son procesadas para cumplir con todas las funciones de comunicación para la cual fue diseñada.

b) **Equipos:** reconocer y recaudar información técnica acerca de los equipos presentes en la red TDM, entre los cuales se pueden encontrar tanto *switches* telefónicos públicos, que prestan servicio de conexión a usuarios o nodos externos a la red, como s*witches* telefónicos privados, para el servicio telefónico interno de la Empresa; este reconocimiento y recaudación de información técnica se hace con la finalidad de identificar qué clase de función cumplen los *switches* en la red, por ejemplo si son clase 4 y atienden como abonados a otras centrales ó clase 5, si tienen por abonados a usuarios finales del servicio. Se debe reconocer y recaudar información también de otros equipos como fuentes de tiempo y canceladores de eco, los cuales se encargan de establecer el sincronismo de la red y proporcionar sistemas de mejora de la voz respectivamente. De igual forma, obtener las especificaciones del equipamiento involucrado en la red IP existente como *routers*, *switches*, gateways, bridges, firewalls y servidores que permitan conocer las funciones y funcionalidades que ofrecen; esto con el fin de estudiar las capacidades y funciones que puedan ser usadas en la nueva plataforma a desarrollar.

c) **Protocolos e interfaces:** recaudar información detallada de cada protocolo de transporte y control utilizado para la red TDM y la IP. Para telefonía, se pueden utilizar los protocolos referentes a digitalización de la voz, sincronismo, señalización y transporte, mientras que para la red IP, se pueden utilizar los protocolos asociados a transporte IP, seguridad, métodos de compresión, encapsulamiento y control. Adicionalmente, se debe realizar un levantamiento de información exhaustivo referente a las interfaces usadas para comunicación y control entre los equipos, así como de la naturaleza de las señales que manejan (ópticas o eléctricas) y el estándar o protocolo que son capaces de manejar; esto permitirá establecer capacidades y parámetros de interoperabilidad que serán de utilidad al momento de incorporar nuevos dispositivos.

d) **Rutas:** con este punto se busca obtener la información del enrutamiento de los servicios telefónicos de la Empresa, de manera de conocer los nodos, tanto internos como externos, involucrados en dichas rutas. Esta información permite conocer los medios utilizados, las configuraciones y los caminos que sigue un tráfico a través de la red interna y de transporte para alcanzar su destino, así como los protocolos referentes a señalización y transporte; de igual forma, se busca conocer las interfaces utilizadas para entregar o recibir el tráfico en cada nodo y por consecuencia tener a disposición documentación que facilite la ingeniería para la futura migración de estas rutas a redes basadas en conmutación de paquetes.

5.2 Ingeniería propuesta

Una vez obtenida toda la información necesaria acerca de todos los equipos, protocolos, interfaces y capacidades, así como el conocimiento acerca del funcionamiento de la red, el segundo paso es desarrollar un modelo de ingeniería acorde a las necesidades y capacidades de la Empresa, teniendo como objetivo redimensionar en equipamiento y capacidades toda la arquitectura actual, para así permitirle ofrecer nuevos servicios, reducir los costos y hacer la red más eficiente.

Estos puntos se pueden resumir de la siguiente manera:

a) **Estudio de la red:** de forma de conocer el comportamiento y el estado actual de la red (TDM e IP) en cuanto al uso de sus capacidades, es importante realizar un estudio del tráfico presente en ella, tanto para ocupación del sistema telefónico y de la red de transporte, como para la red Ethernet. Para esto, se debe recurrir al uso de técnicas de medición de tráfico telefónico como las creadas por el científico A.K. Erlang, de manera que esto sirva como base para el estudio del dimensionamiento en ancho de banda de la red IP que soportará dichos servicios. El estudio permitirá

dimensionar los equipos de la red del *Core* encargados de manejar el tráfico de la misma, de igual forma guiará la manera de cómo debe ajustarse la red de transporte a fin de ofrecer una buena calidad de servicio.

b) **Elección de equipos:** si se requiere de alguna actualización o implementación de equipamiento que se ajuste a las nuevas tecnologías, debe hacerse un análisis de los equipos a elegir, según sus especificaciones técnicas en cuanto a capacidades, protocolos utilizados, rendimiento, gestión y seguridad, tomando como base el estudio realizado de la plataforma actual y las necesidades de la Empresa que deben ser cubiertas. Es importante hacer énfasis en el estudio de las interfaces de comunicación, dado que esto es base fundamental para la correcta interoperabilidad con los equipos existentes. Por otro lado, se recomiendan los equipos con arquitecturas escalables, que permitan dar solución a los primeros requerimientos, pero puedan actualizarse en capacidades a medida que aumenta la demanda de la red, de manera de realizar una migración costo-eficiente.

c) **Reestructuración de la red:** al ser una red única multiservicios, se hace necesario estructurarla de manera que el tráfico de datos no afecte al servicio de voz, con el fin de ofrecer una calidad comparable al sistema telefónico actual. La conexión del *Softswitch* debe estar basada en la recomendación del fabricante en cuanto a interfaces y topología utilizada para la inserción del mismo a la red, es recomendable que éste sea soportado por una arquitectura redundante que ofrezca robustez a la solución.

d) **Redimensionamiento de la red de transporte:** al implementar soluciones de red basadas en VoIP, una disminución del ancho de banda requerido en transporte se hace evidente; con esta disminución es necesario redimensionar la red de manera de reducir los costos que acarrea el transporte de tráfico telefónico. Para reestructurar la red de transporte nacional, se hace necesario realizar planes de coubicación, para los cuales debe hacerse un desarrollo previo que especifique las necesidades, objetivos y alcance del proyecto; así como los equipos a utilizar, estudios de energía, especificaciones de

cableado y planta física requerida para llevar a cabo el desarrollo del proyecto. El dimensionamiento de la red internacional se realiza básicamente reduciendo el ancho de banda requerido para realizar el transporte de tráfico LDI de la red.

5.3 Protocolos de pruebas

Para asegurar una correcta implementación de la solución de VoIP, garantizar la interoperabilidad, el correcto funcionamiento de los equipos y asegurar que el equipamiento adquirido (luego del análisis realizado para elegir la solución que más se adapta a los requerimientos técnicos de la Empresa) cumpla con todas las especificaciones y capacidades que ofrece, es recomendable desarrollar e implementar un protocolo de pruebas que dé soporte a lo anteriormente señalado y en un escenario que se ajuste en lo posible al ambiente más cercano al de producción que tendrá la solución.

El protocolo debe aplicarse a la mayor cantidad de aspectos que puedan afectar de manera directa el funcionamiento de la red, como pruebas de fiabilidad de los equipos, las cuales permiten comprobar el funcionamiento del hardware y la redundancia de éste, pruebas de estrés y de ataque de negación de servicio, con las que se pueden llevar los equipos al límite y simular una situación de alta carga o ataques al equipo y pruebas de calidad de servicio como niveles de *jitter*, *delay*, *packet loss* y MOS. De igual forma son de importancia pruebas de gestión como creación y generación de alarmas, configuración y respaldo.

5.4 Migración de las rutas LDN y LDI TDM a IP

Con la finalidad de culminar el proyecto de manera satisfactoria, una vez finalizada la implementación del equipamiento, es necesario realizar la migración de las rutas presentes en el sistema de telefonía TDM. Con el uso del estudio realizado en el levantamiento de información, se hace posible diseñar un plan de migración que sea ejecutado de manera gradual y transparente de forma que impacte lo menor posible y no produzca paradas del servicio.

En el caso de operadores de larga distancia nacional e internacional, el plan debe llevarse a cabo según la facilidad que tiene dicho operador de realizar modificaciones en las interconexiones, por ejemplo, para el caso de la Empresa 123.com.ve, resulta más sencillo comenzar por la migración de las rutas LDI, dado a que la mayoría de los grandes suplidores internacionales de servicio telefónico tienen la capacidad hoy en día de interconectarse mediante el uso de protocolo de Internet, añadiéndose a esto las regulaciones que en materia de telecomunicaciones se tienen en el extranjero. Para las rutas LDN, el panorama se presenta de una manera distinta; el transporte puede realizarse en IP pero las interconexiones deben manejarse bajo sistemas de telefonía TDM, esto debido a temas regulatorios que obligan a las empresas de telecomunicaciones regirse de esta manera.

Partiendo del hecho de que se ha realizado completamente el dimensionamiento en ancho de banda del *Core* y de los enlaces de transporte de manera de soportar con calidad de servicio el tráfico telefónico a cursar, la migración de las rutas se puede completar siguiendo los siguientes pasos:

a) Implementar la solución de ingeniería para Coubicaciones en el caso de rutas LDN o en su defecto de la interconexión internacional en IP para las rutas LDI.
b) Identificar la ruta a migrar.

c) Obtener todos los datos del estudio previamente realizado, tomando en cuenta los equipos por donde cursa el tráfico, señalización utilizada, protocolos, capacidades, estado y dimensionamiento de las rutas.

d) Realizar la configuración de las rutas en el equipo *Softswitch*, la cual debe contener: autorización de equipos terminales (endpoints), protocolos, parámetros a utilizar (codecs, técnicas de seguridad, compresión, control y gestión), destinos u orígenes permitidos y tarificación.

e) Completar llamadas de prueba que permitan corroborar el funcionamiento de la señalización, el enrutamiento y la calidad de servicio.

f) Colocar en producción la nueva ruta y realizar el monitoreo respectivo de todos los parámetros referentes a calidad.

g) Cerrar las rutas TDM de manera de poder desincorporarlas gradualmente.

En la Figura 26 se muestra gráficamente un esquema metodológico para la migración de la plataforma de telefonía TDM a IP.

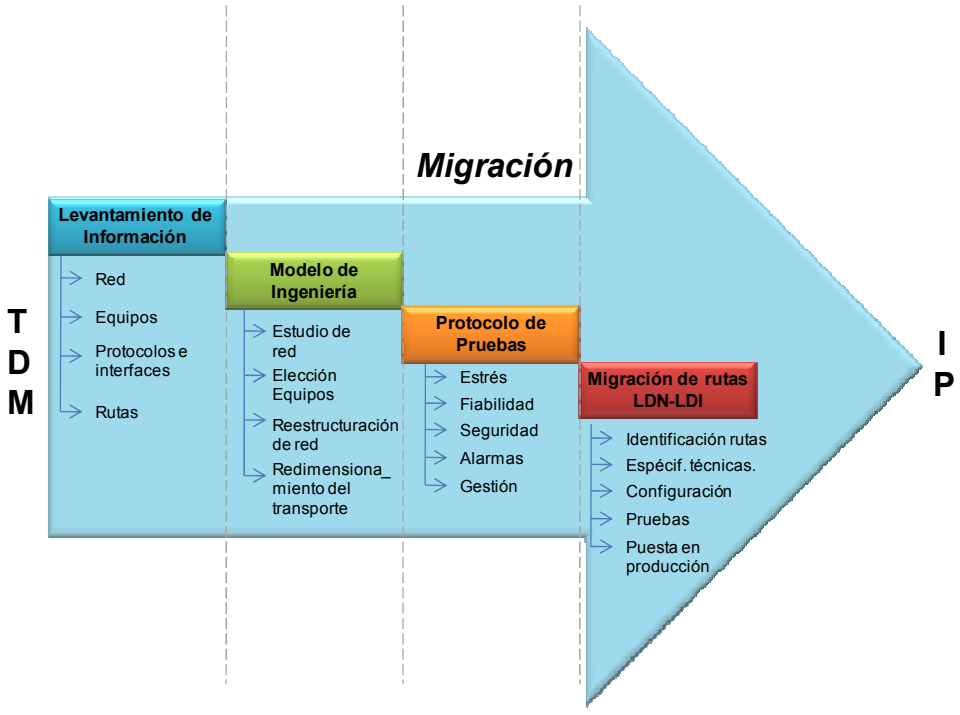


Figura 26. Esquema metodológico para la migración TDM-IP

Fuente: Figura propia.

CONCLUSIONES

a) En definitiva, las normas y recomendaciones que desde sus inicios han sido creadas para el mundo conmutación de circuitos TDM tienen la característica de ser estándares rígidos y poco flexibles, en cambio, para sistemas de datos éstas están basadas en sistemas abiertos, creados por grupos de trabajo de manera consensuada, lo que le otorga la capacidad de ser más flexibles. Es por esto, que la interacción entre las tecnologías TDM-S e IP resultan tan complejas, sobre todo cuando se habla del tema de interfaces de conexión. Tomando en cuenta lo referido, se puede afirmar que se hace menos complicado el desarrollo y la implementación de una arquitectura para soporte de multiservicios en IP desde cero, que atravesar una etapa de migración donde se involucren ambos mundos, dado a que esto genera problemas técnicos y cortes de servicio.

b) Es importante contar con una red NGN en la Empresa que permita ofrecer servicios integrales de telecomunicaciones mediante una infraestructura de red distribuida que reduzca los costos de entrada al mercado dramáticamente, aumente la flexibilidad e incorpore tecnologías de voz por conmutación de circuitos, voz por conmutación de paquetes y adicionalmente sea capaz de manejar servicios de video y sistemas IMS.

c) Se deben utilizar los protocolos SIP ó H323 para dar soluciones de comunicaciones multimedia a través de redes IP, permitiendo facilidad de gestión, control y reparación de fallas debido a su poco complejo esquema de señalización y basamento en el formato de mensajes de Internet.

d) Dentro de los sistemas de *Switches* de la red, es importante contar con técnicas de calidad de servicio y de alto rendimiento en el manejo de paquetes como MPLS, dado a sus capacidades de prioritización del tráfico de voz en conjunto con la implementación de arquitecturas DiffServ.

e) Es primordial el uso del estándar 802.1Q mediante la configuración en los *Switches* de VLANs separadas para voz y para datos que aporten al conjunto una alta calidad de servicio, alto rendimiento y facilidad de administración.
f) Se puede utilizar el proceso de migración de TDM a IP, como medida de solución a la congestión de tráfico que puedan presentar las redes de telefonía tradicional, utilizando para esto la compresión de voz en IP mediante el uso de los codecs que mejor se adapten a los requerimientos de calidad de voz y compresión exigidos.
g) Se hace significativa la realización de un cálculo cuidadoso y exhaustivo en cuanto al correcto dimensionamiento de ancho de banda, debido a que sobre esto se contratan las capacidades de transporte, las cuales son altamente costosas. De igual forma lo es aplicar un estudio detenido a las interfaces utilizadas, que en conjunto con los protocolos, garantizan la interoperabilidad de los equipos en implementaciones mixtas, sobre todo si se tiene en cuenta que los equipos de traducción TDM/IP pueden resultar tan costosos como la solución de los equipos que sean planteados para la actualización completa a IP.
h) Es importante contar con un servicio de monitoreo centralizado y constante que permita visualizar el comportamiento de la red de voz, de manera de ampliar si es necesario el ancho de banda disponible para cada ruta y así evitar alcanzar las cifras de congestión presentadas en el estudio del tráfico.

RECOMENDACIONES

a) Desarrollar una metodología que incluya un cronograma técnico que tome en cuenta el estudio de la plataforma actual, la ingeniería de tráfico, el estudio de soluciones, los tiempos de prueba e implementación, ya que el período de diseño, proceso licitatorio y de procura de equipamiento puede extenderse ampliamente afectando la implementación a tiempo de todo el proyecto.
b) Para realizar la sustitución del *switch* TDM por la tecnología de *Softswitch*, se deben tener totalmente implementados los equipos propuestos para el *Core*, de manera de contar con una arquitectura escalable que permita mantenerlos actualizados y den soporte a la Empresa con tecnologías recientes que impulsen nuevas soluciones en comunicaciones. De igual forma, se recomienda actualizar el software de los equipos existentes, lo que permite obtener soporte de algunas de las últimas tecnologías y aplicaciones que se adapten al nuevo equipamiento y exigencias.
c) Es recomendable llevar a cabo el protocolo de pruebas planteado, mediante el cual se puede obtener una muy buena aproximación del comportamiento del equipo en situaciones de producción, lo cual permite establecer planes de gestión y contingencia acorde a los resultados.
d) Tratar en la manera de lo posible que las interconexiones se hagan utilizando telefonía IP, dado a la facilidad de conexión, configuración, gestión y a la reducción de costos implicados.
e) Realizar pruebas futuras con nuevos protocolos y tecnologías, como servicios de video y multimedia en IP, de manera de ir adaptando la plataforma NGN para que permita ofrecer soluciones convergentes.

REFERENCIAS BIBLIOGRÁFICAS

[1] Universidad de Oviedo. *Redes de Conmutación de Circuitos.* **EN:** *http://www.it.uniovi.es/docencia/Telecomunicaciones/arss/material/arssTema5-Conmutacioncircuitos.pdf*.- Trabajo de investigación en Línea, (s/f). [Consulta: 2007, Junio].

[2] Estepa, R. *Digitalización de la Red telefónica RDSI.* **EN:** *http://trajano.us.es/~rafa/ARSS/apuntes/tema6.pdf.* Notas en Línea, (Diciembre 2004). [Consulta: 2007, Junio].

[3] Ing. Héctor Figueroa. *Estructura de Trama.* **EN:** *www.desi.iteso.mx/telecom/comunicaciones_1/informacion/comunicacioin_digital_basica.ppt* . Presentación en Línea. (s/f). [Consulta: 2007, Junio].

[4] Performance Technologies. *Tutorial on Signaling System 7 (CCSS7).* **EN:** *http: //www.pt.com*.- Tutorial en Línea, (2000-2003). [Consulta: 2007, Julio].

[5] Axarnet. *Redes.* **EN:** http://fmc.axarnet.es/redes/tema_05.htm. Tema en Línea, (s/f). [Consulta: 2007, Junio].

[6] TextosCientíficos.com. *TCP/IP y el modelo OSI.* **EN:** *http: //www.textosciientificos.com/redes/tcp-ip/comparación-modelo-osi.* Trabajo de investigación en Línea, (s/f). [Consulta: 2007, Junio].

[7] Huidobro, José Manuel – Martínez, David. *Tecnología VoIP y Telefonía IP*. (Libro). España, 2006. p. 131.

[8] Quiróz, Rafael. Evaluación de Factibilidad para la migración de la plataforma telefónica actual hacia telefonía IP en la red del BCV (Trabajo de Grado). Caracas: UCV, 2006.

[9] Ing. Alvaro Pachón. *Ethernet.* Universidad Icesi. **EN:** *http://donatello.icesi.edu.co/~redesi/exposiciones/Ethernet_SesionNo_TELEMATICA.pdf*. Presentación en Línea. Marzo 2003. [Consulta: 2007, Junio].

[10] Marca, Ricardo. *La Arquitectura de TCP/IP* - **EN:** *http://r_marca.pe.tripod.com/pagina1.htm*.- Trabajo de Investigación en Línea, (2000). [Consulta: 2007, Junio].

[11] Entel Venezuela. Ing. Giancarlo Saponaro. *Red ISP General.* Diapositivas – Vicepresidencia de Ingeniería y Operaciones. Caracas, 2002.

BIBLIOGRAFÍA

Cisco Systems. Internet Protocols EN: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip.htm#wp4145. Cisco Documentation. (2006). [Consulta: 2007, Julio].

Data Network Resource. *Voice.* **EN:** *http://www.rhyshaden.com/voice.htm* - Paper en Línea. (s/f). [Consulta: 2007, Julio].

Domínguez, Juan José. *La Red Telefónica* - **EN:** *https://www.icai.ve/publicación/anales_get.php?id=909* – Revista en Línea, (s/f). [Consulta: 2007, Julio].

Entel Venezuela. Ing. Giancarlo Saponaro. *Red ISP General.* Diapositivas – Vicepresidencia de Ingeniería y Operaciones. Caracas, 2002.

Entrevista realizada al equipo de operaciones de 123.com.ve, Agosto 2007.

Entrevista realizada al Ing. Fidel Salgueiro, Vicepresidente de Ingeniería y Operaciones de 123.com.ve, Agosto 2007.

Ericsson. *Ericsson ANS Operations & Maintenance*.. Manual. 1999.

Ericsson. *MD110 PBX. System Description.* Manual. 1999.

Escalona, Javier. *Estudio de Factibilidad Técnica y Económica para la Implantación de Telefonía IP en las Subestaciones de la Electricidad de Caracas, C.A.* Trabajo de Grado. UCV, Caracas, 2007.

Guenul, Omar. *Redes*. Trabajo de Investigación. Entel, Chile: 2000.
IETF. RFC: 3261 / 4475 / 3550. **EN:** *http://www.ietf.org.* Recomendaciones en Línea. (2006/2007). [Consulta: 2007, Junio-Septiembre].

International Engineering Consortium. *Fundamentals of Telecommunication.* **EN:** *http://www.iec.org* - Web ProForum Tutorials. (s/f). [Consulta: 2007, Agosto].

International Engineering Consortium. *Interworking Switched Circuit and Voice-over-IP Networks Tutorial.* **EN:** *http://www.iec.org* - Web ProForum Tutorials. (s/f). [Consulta: 2007, Agosto].

International Engineering Consortium. *Next-Generation Networks.* **EN:** *http://www.iec.org* - Web ProForum Tutorials. (s/f). [Consulta: 2007, Agosto].

International Engineering Consortium. *The Coming of True Convergence: Why Service Providers Can Finally Turn Out the Lights on the Old Public Switched Telephone Network (PSTN).* **EN:** *http://www.iec.org* - Web ProForum Tutorials. (s/f). [Consulta: 2007, Agosto].

International Engineering Consortium. *Voice Quality (VQ) in Converging Telephony and IP Networks*. **EN:** *http://www.iec.org* - Web ProForum Tutorials. (s/f). [Consulta: 2007, Agosto].

ITU-T. Recommendations: G.144 / G.729 / P.800 / Q.3900 / Y.1541. **EN:** *http://www.itu.int/rec.* Recomendaciones en Línea. (2006/2007). [Consulta: 2007, Junio-Septiembre].

Quiróz, Rafael. Evaluación de Factibilidad para la migración de la plataforma telefónica actual hacia telefonía IP en la red del BCV (Trabajo de Grado). Caracas: UCV, 2006.

Red de Entel Venezuela. Manuales y documentos de la Vicepresidencia de Ingeniería y Operaciones. Caracas: 2002-2003.

ANEXO 1

(Tabla modelo Erlang B)

Tabla Erlang B 0.01%

Canales	T.Erl	Canales	T. Erl	Canales	T. Erl	Canales	T. Erl	Canales	T. Erl
1	0	45	25	89	60	133	97.3	177	135.7
2	0	46	25.8	90	60.9	134	98.2	178	136.6
3	0	47	26.5	91	61.7	135	99	179	137.5
4	0.2	48	27.3	92	62.5	136	99.9	180	138.4
5	0.4	49	28	93	63.4	137	100.8	181	139.3
6	0.7	50	28.8	94	64.2	138	101.6	182	140.1
7	1	51	29.6	95	65	139	102.5	183	141
8	1.4	52	30.3	96	65.9	140	103.4	184	141.9
9	1.8	53	31.1	97	66.7	141	104.2	185	142.8
10	2.2	54	31.9	98	67.5	142	105.1	186	143.7
11	2.7	55	32.7	99	68.4	143	106	187	144.6
12	3.2	56	33.4	100	69.2	144	106.8	188	145.4
13	3.7	57	34.2	101	70	145	107.7	189	146.3
14	4.2	58	35	102	70.9	146	108.6	190	147.2
15	4.7	59	35.8	103	71.7	147	109.4	191	148.1
16	5.3	60	36.6	104	72.6	148	110.3	192	149
17	5.9	61	37.4	105	73.4	149	111.2	193	149.9
18	6.4	62	38.1	106	74.3	150	112	194	150.8
19	7	63	38.9	107	75.1	151	112.9	195	151.7
20	7.6	64	39.7	108	75.9	152	113.8	196	152.5
21	8.3	65	40.5	109	76.8	153	114.7	197	153.4
22	8.9	66	41.3	110	77.6	154	115.5	198	154.3
23	9.5	67	42.1	111	78.5	155	116.4	199	155.2
24	10.2	68	42.9	112	79.3	156	117.3	200	156.1
25	10.8	69	43.7	113	80.2	157	118.1	201	157
26	11.5	70	44.5	114	81	158	119	202	157.9
27	12.2	71	45.3	115	81.9	159	119.9	203	158.8
28	12.8	72	46.1	116	82.7	160	120.8	204	159.7
29	13.5	73	46.9	117	83.6	161	121.6	205	160.6
30	14.2	74	47.7	118	84.4	162	122.5	206	161.5
31	14.9	75	48.6	119	85.3	163	123.4	207	162.3
32	15.6	76	49.4	120	86.1	164	124.3	208	163.2
33	16.3	77	50.2	121	87	165	125.2	209	164.1
34	17	78	51	122	87.9	166	126	210	165
35	17.7	79	51.8	123	88.7	167	126.9	211	165.9
36	18.4	80	52.6	124	89.6	168	127.8	212	166.8
37	19.1	81	53.4	125	90.4	169	128.7	213	167.7
38	19.9	82	54.3	126	91.3	170	129.6	214	168.6
39	20.6	83	55.1	127	92.1	171	130.4	215	169.5
40	21.3	84	55.9	128	93	172	131.3	216	170.4
41	22.1	85	56.7	129	93.9	173	132.2	217	171.3
42	22.8	86	57.6	130	94.7	174	133.1	218	172.2
43	23.5	87	58.4	131	95.6	175	134	219	173.1
44	24.3	88	59.2	132	96.4	176	134.8		

Tabla modelo Erlang B.

Disponible en http://personal.telefonica.terra.es/web/vr/erlang/mtaula.htm

ANEXO 2

Características mas relevantes del Cisco Serie 7600

Cisco 7609 *Router*

The Cisco® 7609 *Router* is a high-performance *router* deployed at the network edge, where performance, IP services, redundancy, and fault resiliency are critical. It enables Carrier Ethernet service providers to deploy an advanced network infrastructure that supports a range of IP video and triple-play (voice, video, and data) system applications in both the residential and business services markets. The Cisco 7609 enables enterprises to deploy advanced WAN and metropolitan-area network (MAN) networking solutions necessary to succeed in demanding, high-traffic environments.

Providing the foundation for a powerful combination of speed and services, the 9-slot Cisco 7609 *Router* is an outstanding choice for multiple applications. Whether deployed as a high-speed WAN aggregator, as a device for peering, as a residential broadband services aggregator, or as a device for Metro Ethernet aggregation and uplink, the Cisco 7609 meets requirements for redundancy, high availability, and rack density. In the point-of-presence (POP) service provider edge or the metropolitan network edge, the Cisco 7609 sets new standards as part of the industry-leading Cisco 7600 Series *Routers*.

With a forwarding rate of up to 400-Mpps distributed and 720-Gbps total throughput, the Cisco 7609 provides performance and reliability with options for redundant route processors and power supplies. The inclusion of two Gigabit Ethernet ports on the Cisco Catalyst® 6500 Series Supervisor Engine 720 with the Multilayer *Switch* Feature Card 3 (MSFC-3) or the new Cisco Route *Switch* Processor 720 (RSP 720) with the MSFC-4 used in the Cisco 7609 eliminates the need for a line-card slot for uplink ports. The result of this design is more efficient use of available line-card slots and increased deployment flexibility. Four Gigabit Ethernet ports are available for use in dual-route processor configurations.

Shared port adaptors (SPA) on the SPA interface processors (SIPs) are available on the Cisco 7600 Series with interface speeds ranging from OC-3 to OC-192 and from Fast Ethernet to 10 Gigabit Ethernet. The Cisco 7600 Series can also use the Cisco 7600 Series/Catalyst 6500 Series Enhanced FlexWAN Module to take advantage of most Cisco 7200 and 7500 Port Adapters for terminating DS-0 to OC-3 speeds. By using the Cisco Catalyst 6000 Series of Ethernet line cards in conjunction with the SIP-based SPAs and the enhanced FlexWAN module, the Cisco 7600 provides a multitude of options to scale WAN connectivity from DS-0 to OC-192 and LAN connectivity from 10-Mbps Ethernet through 10 Gigabit Ethernet.

The Cisco 7609 chassis accommodates a broad selection of line cards supporting numerous applications, including:

- SPAs and SIPs (Cisco 7600 Series SPA Interface Processor-200 [SIP-200], SIP-400, and SIP-600):
  - –Channelized T1/E1, Channelized T3, and Channelized OC-3/STM-1
  - –OC-3/STM-1, OC-12/STM-4, OC-48/STM-16 Packet over SONET/SDH (PoS), and OC-192/STM-64 PoS
  - –OC-3/STM-1 ATM, OC-12/STM-4 ATM, and OC-48/STM-16 ATM
  - –Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet
- Enhanced FlexWAN module: Supporting Cisco 7200 and 7500 WAN port adapters from DS-0 to OC-3 for channelized and ATM interfaces and also Fast Ethernet port adapters
- High-density Ethernet services modules: 10/100 Mbps, Gigabit Ethernet, and 10-Gigabit Ethernet
- Services modules: IP Security (IPsec), firewall, distributed denial of service, intrusion detection systems, network analysis, and content witching commonly used, for example, in the Cisco Mobile Exchange solution
- Supervisor support: Cisco Catalyst 6500 Supervisor Engine 32 (WS-SUP32-GE-3B and WS-SUP32-10GE-3B), Cisco Catalyst 6500 Supervisor Engine 720 (WS-SUP720-3B and WS-

SUP720-3BXL), and the new Cisco Route *Switch* Processor 720 (RSP720-3C and RSP720-3CXL)

The Cisco 7609 incorporates many service provider and high-end enterprise carrier-class requirements. Line cards are vertically mounted for efficient cooling with front-to-back airflow. High availability is an inherent facet in the form of redundant power supplies and redundant fan-tray modules. Standard or extended cable-tray inserts provide unrestricted management of either fiber and coaxial or multiple conductor types with up to 48 10/100 cables per slot. Two chassis can be installed per 7-foot rack.

Applications

The flexible Cisco 7609 *Router* is ideal for addressing high-performance applications such as:

- High-end customer premises equipment (CPE)
- Leased line
- IP/Multiprotocol Label *Switch*ing (MPLS) provider edge
- Metro Ethernet access
- Enterprise WAN aggregation
- Mobile Radio Access Network (RAN) aggregation
- Residential subscriber aggregation

Feature Summary

Cisco 7609 Chassis Features

- 21RU (36.75 in. [93.3 cm]) high, up to 2 chassis per 7-foot rack
- Nine configurable interface slots
- Route processor, *switch* fabric, and power supply protection capability: 1 + 1
- Tiered-speed fan design (standard): 1 + 1
- Cable management tray options for fiber and coaxial and dense 10/100 cable configurations
- Single-side connection management for both interface and power terminations
- Front-to-back airflow

Cisco 7609 System Features

- Total throughput: 720 Gbps
- Up to 400-Mpps distributed forward rate (requires distributed forwarding cards [DFCs])

Cisco 7609 Technical Specifications

- Nine-slot chassis
- Network Equipment Building Standards (NEBS) Level 3 compliance
- Minimum route processor requirement; one Cisco Catalyst 6500 Series Supervisor Engine 2 with Multilayer *Switch* Feature Card 2 (MFSC-2)
- Dimensions (H x W x D): 36.75 x 17.2 x 20.7 in. (93.3 x 43.1 x 53.3 cm)
- Power requirements:
  - –-208 to 240 VAC (recommended)
  - –-48 to -60 VDC (4000 WAC supplies require 30A input circuits)
- Weight: 121 lb (54.9 kg; chassis only); 270 lb (122.5 kg; full configuration)
- Mean time between failure (MTBF): 7 years for system configuration
- Environmental conditions:
  - –Operating temperature: 32 to 104°F (0 to 40°C)
  - –Storage temperature: -4 to 149°F (-20 to 65°C)
  - –Relative humidity, operating: 10 to 85%, noncondensing
  - –Relative humidity, storage: 5 to 95%, noncondensing
  - –Operating altitude: -500 to 6500 ft
- Minimum software release: Cisco IOS® Software Release 12.1(13) E1.

ANEXO 3

Características más relevantes del Cisco Catalyst Serie 6500

Table 1. Cisco Catalyst 6500 Series at a Glance

Feature	Cisco Catalyst 6500 Series
Chassis Configurations	• 3-slot • 6-slot • 9-slot • 9 vertical slots • 13-slot
Backplane Bandwidth	• 32-Gbps shared bus • 256-Gbps switch fabric • 720-Gbps switch fabric
Layer 3 Forwarding Performance	• Cisco Catalyst 6500 Supervisor Engine 1A Multilayer Switch Feature Card (MSFC2): 15 mpps • Catalyst 6500 Supervisor Engine 2 MSFC2: up to 210 mpps • Catalyst 6500 Supervisor Engine 32 MSFC2a: 15 mpps • Catalyst 6500 Supervisor Engine 720: up to 400 mpps
Operating System	• Cisco Catalyst OS • Cisco IOS Software • Hybrid configuration
Redundant Supervisor Engines	Yes, with stateful failover
Redundant Components	• Power supplies (1+1) • Switch fabric (1+1) • Replaceable clock • Replaceable fan tray
High-Availability Features	• Gateway Load Balancing Protocol • Hot Standby Router Protocol (HSRP) • Multimodule EtherChannel technology • Rapid Spanning Tree Protocol (RSTP) • Multiple Spanning Tree Protocol (MSTP) • Per-VLAN Rapid Spanning Tree • Rapid convergence Layer 3 protocols
Advanced Services Modules	• Content services gateway • CSM • Firewall module • IDS module • IP Security (IPSec) VPN module • Network analysis module • Persistent storage device • SSL module • Wireless LAN services module

Table 2. Cisco Catalyst 6500 Series Port Density Information, WAN Modules and Interfaces

Maximum System Port Densities (Including Supervisor Engine Ports)	**Catalyst 6503**	**Catalyst 6503-E**	**Catalyst 6506 and 6506-E**	**Catalyst 6509 and 6509-E**	**Catalyst 6509-NEB and 6509-NEB-A**	**Catalyst 6513**
10 Gigabit Ethernet (XENPAK)	2	8	20	32	32	20
Gigabit Ethernet (Small Form-Factor Pluggable [SFP] optics)	8	98	242	386	384	410
Gigabit Ethernet (gigabit interface converter [GBIC])	34	34	82	130	130	194
10/100/1000 Ethernet	97	97	241	385	385	577
10/100 Fast Ethernet	192	192	480	768	768	1152
100BASE-FX	96	96	240	384	384	576
FlexWAN (DS-0 to OC-3)	2 modules with 4 port adapters	2 modules with 4 port adapters	5 modules with 10 port adapters	8 modules with 16 port adapters	8 modules with 16 port adapters	12 modules with 24 port adapters
Integrated WAN Modules						
OC-3 POS ports	16	16	40	64	64	96
OC-12 POS ports	8	8	20	32	32	48
OC-12 ATM ports	4	4	10	16	16	24
OC-48 POS/Dynamic Packet Transport (DPT) ports	4 POS 2 DPT	4 POS 2 DPT	10 POS 5 DPT	16 POS 8 DPT	16 POS 8 DPT	24 POS 12 DPT
PSTN Interfaces						
Digital T1/E1 trunk ports	36	36	90	144	144	216

ANEXO 4

Next Generation Network (NGN) Test

Especificaciones

NEXTONE *MSX/RSM*

REGISTRO DE FIRMAS

Elaborado por

123.COM.VE: Johnatan Santana	**Proveedor**

Revisado por

123.COM.VE: Fidel Salgueiro	**Proveedor**

Aprobado por

123.COM.VE	**Proveedor**

LISTADO DE PRUEBAS

0. TEST ENVIROMENT

1. PRUEBAS DE ESTRÉS

1.1. Sip Flood Test

1.2. Sip Torture Test

1.3. RTP attack tests – RTP fraud and denial-of-service attack

2. ALARMAS

2.1. Funciones de Alarma 01

2.2. Funciones de Alarma 02

3. SEGURIDAD Y LOG MANAGEMENT

3.1. Funciones de Seguridad 01

3.2. Funciones de Seguridad 02

3.3 Funciones de Seguridad 03

3.4 Funciones de Seguridad 04

3.5 Funciones de Seguridad 05

3.6 Funciones de Seguridad 06

3.7 Funciones de Seguridad 07

3.8 Funciones de Seguridad 08

8.2 Prueba de Delay

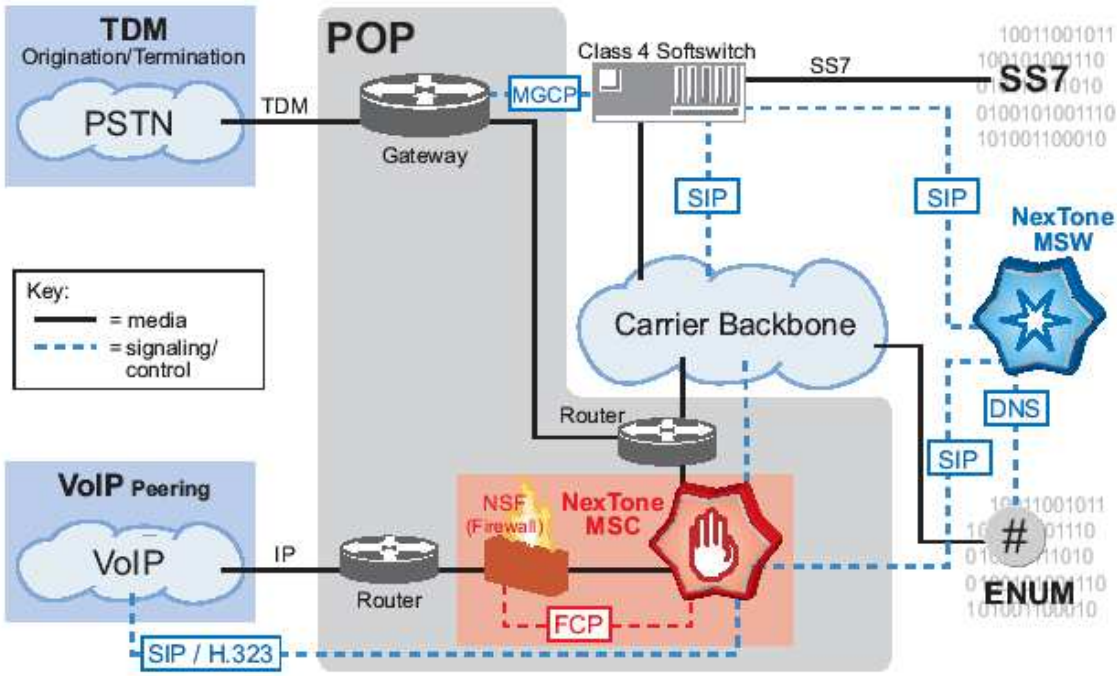
8.3 Prueba de Packet Lost

8.4 Prueba de Factor R

8.5 MOS

0. TEST ENVIROMENT

Figure 1. NexTone iServer (MSC and MSW)



PRUEBAS DE ESTRÉS DEL EQUIPO

1.1 SIP Flood Test

<table>
<tr><td colspan="2">Prueba número 01: Flujo de Llamadas</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: SIP Flood Test</td><td colspan="2">Sub Item: Ninguno</td></tr>
<tr><td colspan="4">Condiciones de la prueba: Consiste en generar un flujo llamadas de ataque para generar estrés utilizando mensajes de invitación, registro y respuesta según la RFC 3261, provenientes de millares de direcciones/puertos escogido al azar.</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba

Una herramienta de Stress (software o hardware) simulará un escenario de ataque con millares de ataques y direcciones escogidas al azar</td></tr>
<tr><td colspan="4">Resultados esperados,

Comprobar la correcta formación de secuencia de mensajes SIP, y adicionalmente que el equipo sea capaz de protegerse el mismo y al Proxy SIP contra ataque externos.</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Paso la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

Nota: El proveedor debe proporcionar una herramienta de estrés

1.2 Sip Torture Test

<table>
<tr><td colspan="2">Prueba número 02: Flujo de Llamadas</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: SIP torture tests</td><td colspan="2">Sub Item: Ninguno</td></tr>
<tr><td colspan="4">Condiciones de la prueba:

Utilizar los comentarios extraídos de la RFC 4475 del IETF (Internet Engineering Task Force), para generar 49 de los mensajes SIP mal formateados o inusualmente formateados</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba

Una herramienta de Stress simulara un escenario de ataque con millares de ataques y direcciones escogidas al azar</td></tr>
<tr><td colspan="4">Resultados esperados,

Que el equipo sea capaz de protegerse contra un flujo de mensajes pequeños o mal formados de SIP INVITE, REGISTER y OPTIONS a una rata de velocidad de 300,000 mensajes/segundo en un periodo de 12 horas continuas sin impactar las llamadas legitimas y registrando todas las llamadas a través del SIP proxy server.</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

1.3 RTP attack tests – RTP fraud and denial-of-service attack

<table>
<tr><td colspan="2">Prueba numero 03: Flujo de Llamadas</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: RTP attack tests – RTP fraud and denial-of-service attacks</td><td colspan="2">Sub Item: Ninguno</td></tr>
<tr><td colspan="4">Condiciones de la prueba:

Ataques de RTP (Real-Time Transpoort Protocol) de fraude y negación de servicio, comentario RFC 3550 del IETF</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba

Una herramienta de Stress simulara un escenario de ataque con millares de ataques y direcciones escogidas al azar</td></tr>
<tr><td colspan="4">Resultados esperados,

Latencia de señalización de solo 2 ms mientras el equipo este siendo atacado. Adicionalmente el jitter del RTP debe ser menos 1 ms – Mínimo valor medido por el equipo de prueba.</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

ALARMAS

2.1 Funciones de Alarma 01

<table>
<tr><td colspan="2">Prueba numero 01: Alarmas</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Reporte de Alarmas</td><td colspan="2">Sub Item: Generación de una Alarma cuando ocurre una falla</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba

Simular las condiciones en el equipo según tabla anexa, y verificar si éste registra la alarma correctamente. Garantizar que la alarma se presente en la ventana de alarma de monitoreo</td></tr>
<tr><td colspan="4">Resultados esperados,

Que la alarma se genere apropiadamente en la ventana de la estación de trabajo</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

Tabla de Alarmas

Alarm Type	Description
local disconnect	This alarm will trigger when an internal error causes a local disconnection.
Answer Seizure Ratio (ASR)	The Answer Seizure Ratio is the ratio of the number of successful calls over the total number of outgoing calls from a carrier's network.
Gateway Minutes	The number of prepaid customer minutes.
Dollar Amount	This alarm triggers when the cumulative dollar value of the traffic, carried by a certain endpoint, exceeds the configured threshold. This is similar to the "Gateway Minutes Alarm", but counts the dollar value of each call instead of the duration of the call.
Average Request Rate (ARR)	Average Request Rate is essentially ASR calculated within a subset of the total calls. ASR is the ratio of the normal calls (ISDN code = 16) to the total calls and ARR is the ratio of the normal calls (ISDN code = 16) to the total calls with a certain ISDN code values (ISDN code = configured values). The ISDN codes to be used in the ARR calculation is user specific and is configured in the user preferences. This alarm triggers when the ARR meets the configured threshold value within a certain duration.
Average Call Duration (ACD)	This alarm triggers when the average call duration meets the configured threshold value. For example, this alarm could be configured to trigger when the average call duration falls under, say, 5 seconds, indicating some problem in the operation.
Post Dial Delay (PDD)	This alarm is based on the PDD value measured on the call. This alarm will trigger id, in a configured window of time, the number of CDRs containing the given PDD exceeds a configured threshold. E.g., trigger an alarm if 5 CDRs in a 30 minute period contain PDD exceeding 300ms.

Alarm Type	Description
Average PDD	This alarm is based on the PDD value measured on the call. This alarm will trigger if, the average PDD of all calls in a configured window of time exceeds a configured threshold. E.g., trigger an alarm if the average PDD of the calls over a 30 minute period is greater than 400ms.
Low Voice Quality (LVQ)	This alarm is based on the R Factor value measured on the call. This alarm triggers if, in a configured window of time, the percentage of CDRs containing the given R Factor condition exceeds a configured threshold. Both the R Factor values from a CDR are considered in the alarm. For example, trigger an alarm if 5% of the calls over a 30 minute period have a R Factor value less than 65.
Average LVQ	This alarm is based on the R Factor value measured on the call. This alarm triggers if, the average R Factor of all calls in a configured window of time exceeds a configured threshold. The average is calculated using both the R Factor values in a CDR. For example, trigger an alarm if the average R Factor of the calls over a 30 minute period is less than 75.
High Packet Loss (HPL)	This alarm is based on the Packets Lost and Packets Received values in the CDRs. This alarm triggers if, in a configured window of time, the number of CDRs containing a packet loss (%) exceeds a configured threshold. Packet Loss from both sides of the call are considered in the alarm.
Average HPL	This alarm is based on the Packets Lost and Packets Received values in the CDRs. This alarm triggers if the average Packet Loss of all calls in a configured window of time exceeds a configured threshold. The average is calculated using values from both sides of a call.

Alarm Type	Description
Packet Delay Variance (PDV)	This alarm is based on the PDV (jitter) value measured on the call. This alarm will trigger if, in a configured window of time, the percentage of CDRs containing the given PDV exceeds a configured threshold. Both the PDV values from a CDR are considered in the alarm, e.g., trigger an alarm if 5% of the calls over a 30 minute period has a PDV (jitter) value greater than 30ms.
Average Packet Delay Variance (APDV)	This alarm is based on the PDV (jitter) value measured on the call. This alarm will trigger if, the average PDV of all calls in a configured window of time exceeds a configured threshold. The average is calculated using both the PDV values in a CDR, e.g., trigger an alarm if the average PDV (jitter) of the calls over a 30 minute period is greater than 25ms.

2.2 Funciones de Alarma 02

<table>
<tr><td colspan="2">Prueba numero 02: Alarmas</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Reporte de Alarmas</td><td colspan="2">Sub Item: Generación de una Alarma cuando hay una caída del sistema y el equipo se recupera automáticamente</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba

Simular una condición de caída del sistema, ver si el equipo la registra correctamente y se recupera satisfactoriamente. Garantizar que la alarma se presente en la ventana de alarma de monitoreo, cuando ocurre la caída y cuando se esta recuperando.</td></tr>
<tr><td colspan="4">Resultados esperados,

Que la alarma se genere apropiadamente en la ventana de la estación de trabajo y el equipo se recupere normalmente.</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

3 SEGURIDAD Y LOG MANAGEMENT

3.1 Funciones de seguridad

<table>
<tr><td colspan="2">Prueba numero 01: Funciones de seguridad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Seguridad y log management</td><td colspan="2">Sub Item: No permitir el ingreso de usuarios no autorizados</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba
1. Intentar ingresar en el sistema de operación y mantenimiento sin user name o password.
2. Intentar ingresar en el sistema de administración, operación y mantenimiento sin password.
3. Intentar ingresar en el sistema de administración, operación y mantenimiento como usuario no registrado.
4. Intentar romper la seguridad e ingresar de otras maneras.</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Ingreso Fallido.
2. Ingreso Fallido.
3. Ingreso Fallido.
4. Ingreso Fallido.</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

3.2 Funciones de seguridad

<table>
<tr><td colspan="2">Prueba numero 02: Funciones de seguridad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Seguridad y log management</td><td colspan="2">Sub Item: Asegurar el login con un user name y login debidamente autenticados</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
Ingresar correctamente con un usuario permisado</td></tr>
<tr><td colspan="4">Resultados esperados,
Ingreso Exitoso</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

3.3 Funciones de seguridad

<table>
<tr><td colspan="2">Prueba numero 03: Funciones de seguridad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Seguridad y log management</td><td colspan="2">Sub Item: Asegurar los niveles de autoridad de un usuario una vez logeado</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y los perfiles de acceso configurados</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Ingresar como Administrador del Sistema.
2. Listar comandos permitidos para éste tipo de operador.
3. Ingresar como operador e intentar eliminar una comando o ejecutar un comando para el cual no está autorizado.
4. Eliminar un comando como operador, recuperarlo como administrador del sistema e intentar ejecutarlo como operador.</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Ingreso Exitoso.
2. Operación Exitosa.
3. Rechazado debido a autoridad inadecuada.
4. Operación Exitosa y Comando Exitoso.</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Paso la prueba
Fallo la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

3.4 Funciones de seguridad

<table>
<tr><td colspan="2">Prueba numero 04: Funciones de seguridad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Seguridad y log management</td><td colspan="2">Sub Item: Operación desde distintos terminales</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba
1. El administrador del sistema ingresa desde un terminal de operación.
2. Ejecuta comandos para los cuales está autorizado como administrador del sistema.
3. Ingresar como operador en el terminal de operación.
4. Ejecutar comandos para los cuales está autorizado como operador.</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Ingreso Exitoso.
2. Operación Exitosa.
3. Ingreso Exitoso.
4. Operación Exitosa.</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Paso la prueba

Fallo la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

3.5 Funciones de seguridad

<table>
<tr><td colspan="2">Prueba numero 05: Funciones de seguridad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Seguridad y log management</td><td colspan="2">Sub Item: Tiempo de ejecución de comandos</td></tr>
<tr><td colspan="4">Condiciones de la prueba:

El equipo instalado, trabajando y los perfiles de acceso configurados</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba
1. El operador con autoridad prepara un set de comandos para ejecutarlos en una rutina.
2. Añade un tiempo de inicio de comando con una duración de 5 minutos y ejecuta el query de comandos.
3. En lo siguientes 5 minutos, se verifica que la lista de comandos se ejecutó.</td></tr>
<tr><td colspan="4">Resultados esperados,

1. Ingreso Exitoso.
2. Operación Exitosa.
3. Los comandos se ejecutan normalmente.</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Paso la prueba

Fallo la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

3.6 Funciones de seguridad

<table>
<tr><td colspan="2">Prueba numero 06: Funciones de seguridad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Seguridad y log management</td><td colspan="2">Sub Item: Chequeo en la restricción de parámetros de entrada</td></tr>
<tr><td colspan="4">Condiciones de la prueba:

El equipo instalado, trabajando y los perfiles de acceso configurados</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba
1. El operador con la autoridad de ingresar usuarios se loguea.
2. Introduce usuarios y usa la función de programar una llamada, modificar la tasación de un ruta, o reenrutar trafico sin autorización</td></tr>
<tr><td colspan="4">Resultados esperados,

1. Ingreso Exitoso.
2. La función falla. El sistema de RSM tiene una función para validar y chequear que estas funciones se hagan dentro de ciertos parámetros</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

3.7 Funciones de seguridad

<table>
<tr><td colspan="2">Prueba numero 07: Funciones de seguridad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Seguridad y log management</td><td colspan="2">Sub Item: Registros de login y logout</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y los perfiles de acceso configurados</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba
1. El administrador del sistema ingresa
2. Realiza un Query log y chequea los eventos de login y logout .</td></tr>
<tr><td colspan="4">Resultados esperados,

1. Ingreso Exitoso.
2. El registro es exitoso</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

3.8 Funciones de seguridad

<table>
<tr><td colspan="2">Prueba numero 08: Funciones de seguridad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Seguridad y log management</td><td colspan="2">Sub Item: Log query</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado y trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba
1. El administrador del sistema ingresa.
2. Se realiza un Log Query, por ejemplo se hace una operación de comando, que puede ser fallida o exitosa durante cierto intervalo de tiempo.</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Ingreso Exitoso.
2. El query es exitoso y arroja los resultados correctos</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

3.9 Funciones de seguridad

<table>
<tr><td colspan="2">Prueba numero 09: Funciones de seguridad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Seguridad y log management</td><td colspan="2">Sub Item: Acceso externo a la IP del equipo</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado y trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba
1. Acceder a la IP publica del equipo del Gestor RSM.
2. Intentar logearse 3 veces</td></tr>
<tr><td colspan="4">Resultados esperados,

1. Ingreso negado
2. Al tercer intento se debe generar un Trap de advertencia hacia un gestor de monitoreo establecido</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

4. CONFIGURACIONES

4.1 Configuración 01

Prueba numero 01: : Funciones de configuración	**Fecha:**
Item: Configuraciones de diferentes tipos de End Points	**Sub Item:** Configuración Generic IP Device
Condiciones de la prueba: El equipo instalado, trabajando y configurados los perfiles de acceso	
Condiciones para la prueba: Que el equipo esté conectado a la red, en condición de trabajo normal **Procedimiento de Prueba** Usando el iView configurar : • Registration ID (required) • Port number (required) • IP address (speciéying this makes the device a *static* endpoint) • Extension • Calling plan (see Chapter 12, *Calling Plans* on page 213). • Realm the endpoint resides in • iEdge Group (for CAC control) • Zone1 • Vendor • Subnet IP address • Subnet mask • User information (first name, last name, email address, location, country, comments, customer ID) • Whether configured as a gateway/proxy, and priority for routing calls • Call filtering specifications (allow calls, unlimited calls or maximum call limit) • Maximum call limit	

<table>
<tr><td colspan="4">• H.323 protocol parameters
• SIP protocol parameters
• Trunk group routing-related parameters
• Call Hunting options
• Media Routing options</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Configuraciones exitosas.</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

4.2 Configuración 02

<table>
<tr><td colspan="2">Prueba numero 02: : Funciones de configuración</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Configuración de diferentes tipos de End-Points</td><td colspan="2">Sub Item: H.323 Gateway/H.323 Gatekeeper/Sgatekeeper</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Configuración y prueba del H.323 Gateway/H.323 Gatekeeper/Sgatekeeper</td></tr>
<tr><td colspan="4">Resultados esperados
1. Configuración exitosa</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

4.3 Configuración 03

<table>
<tr><td colspan="2">Prueba numero 03: : Funciones de configuración</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Configuración de diferentes tipos de End-Points</td><td colspan="2">Sub Item: SIP Gateway/SIP Proxy</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba
1. Configurar el SIP Gateway/SIP Proxy.
2. Validar todas las respuestas SIP de acuerdo a la Norma RFC 3261</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Configuración exitosa
2. Respuestas de acuerdo a la norma</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

4.4 Configuración 04

<table>
<tr><td colspan="2">Prueba numero 04: Funciones de configuración</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Configuración de diferentes tipos de End-Points</td><td colspan="2">Sub Item: SoftSwitch/Enum Services</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Aprovisionar el ENUM Server en el MSX usando iView.
2. Agregar en la BD del NexTone MSX como Domain Name Server (DNS)</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Configuración exitosa</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

4.5 Configuración 05

<table>
<tr><td colspan="2">Prueba numero 05: : Funciones de configuración</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Configuración de diferentes tipos de End-Points</td><td colspan="2">Sub Item: User Account</td></tr>
<tr><td colspan="4">Condiciones de la prueba:

El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba

Usando iVIEW configurar:

1. Registration ID (required)
2. IP address
3. Extensión
4. Calling plan
5. Zone
6. Vendor
7. Subnet IP ardes
8. Subnet mask
9. User information (first name, last name, email address, location, country, comments)</td></tr>
<tr><td colspan="4">Resultados esperados,

1. Configuración exitosa</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

4.6 Configuración 06

<table>
<tr><td colspan="2">Prueba numero 06: : Funciones de configuración</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Configuración de diferentes tipos de End-Points</td><td colspan="2">Sub Item: MSX Global Setting</td></tr>
<tr><td colspan="4">Condiciones de la prueba:

El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
Configurar y revisar si ocurre automáticamente en el almacenamiento del MSX, usando server.cfg, la siguiente categoría de parámetros :
1. Billing and Call Detail Records (CDRs)
2. MSX server
3. SIP
4. H.323
5. Other (ENUM domain, allow all source numbers, default route on all gateways)
6. Firewall parameters (including NSF-NP)
7. Pools (formerly Firewall Control Entity, FCE)
8. MSX peering
9. MSX Database replication
10. Local Number Portability (LNP)
11. Quality of Service (QoS)</td></tr>
<tr><td colspan="4">Resultados esperados,

1. Configuración exitosa</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

5 Fiabilidad

5.1 Pruebas fiabilidad del equipo 01

<table>
<tr><td colspan="2">Prueba numero 01: Fiabilidad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Fiabilidad</td><td colspan="2">Sub Item: Prueba al MSX</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Resetear el servidor que contiene el MSX, verificar que el equipo levante sin dificultad</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Reinicio exitoso</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

5.2 Pruebas fiabilidad del equipo 02

<table>
<tr><td colspan="2">Prueba numero 02: Fiabilidad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Fiabilidad</td><td colspan="2">Sub Item: Prueba al RSM Agent Software</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Resetear el servidor que contiene el RSM, verificar que el equipo levante sin dificultad</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Reinicio exitoso</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

5.3 Pruebas fiabilidad del equipo 03

<table>
<tr><td colspan="2">Prueba numero 03: Fiabilidad</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Fiabilidad</td><td colspan="2">Sub Item: Pruebas desconexión de alimentación</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:

Que el equipo esté conectado a la red, en condición de trabajo normal

Procedimiento de Prueba
1. Quitar toda la alimentación de los equipos, para simular una caída del sistema por falla del Energia</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Reinicio exitoso de todos los componentes y de toda la configuración del sistema</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba

Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

6 SOPORTE SMNP

6.1 Generación de TRAPS

<table>
<tr><td colspan="2">Prueba numero 01: Soporte SMNP</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Soporte SMNP</td><td colspan="2">Sub Item: Generación de Traps</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Generar cada una de las fallas de la tabla anexa</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Generación de cada uno de los Traps</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

Tabla de Traps del sistema

Event Description	Cause	Recommended Response	SNMP Trap Objects and Example Values
Free space on a monitored partition is below threshold.	• Log rollover/trim functions have failed • Excessive core dump files generated • CDR file growth off-loaded.	Check the trap output to determine which partition is over limit. If CDR files are the cause, move old files to another partition or offline. See *Setting a Rule for Opening New CDR Log Files* on page 313 for more info on CDR files.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3022) 0:00:30.22 SNMPv2-MIB::snmpTrapOID.0 = OID: DISMAN-EVENT-MIB::mteTriggerFired DISMAN-EVENT-MIB::mteHotTrigger = STRING: dskTable DISMAN-EVENT-MIB::mteHotTargetName = STRING: DISMAN-EVENT-MIB::mteHotContextName = STRING: DISMAN-EVENT-MIB::mteHotOID = OID: UCD-SNMP-MIB::dskErrorFlag.1 DISMAN-EVENT-MIB::mteHotValue = INTEGER: 1 UCD-SNMP-MIB::dskPath.1 = STRING: / UCD-SNMP-MIB::dskErrorMsg.1 = STRING: /: less than 10% free (= 91%)
Ethernet link state has changed. *Note: Enabling this function may generate excessive traps in HA systems*	• Disconnected cable • HA system failover • Device at other end of link went down • Manual stop	If trap indicates that link state has changed to "down", check cabling and attached device for physical connection.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (6318) 0:01:03.18 SNMPv2-MIB::snmpTrapOID.0 = OID: DISMAN-EVENT-MIB::mteTriggerFired DISMAN-EVENT-MIB::mteHotTrigger = STRING: Generate linkUp DISMAN-EVENT-MIB::mteHotTargetName = STRING: DISMAN-EVENT-MIB::mteHotContextName = STRING: DISMAN-EVENT-MIB::mteHotOID = OID: IF-MIB::ifOperStatus.2 DISMAN-EVENT-MIB::mteHotValue = INTEGER: 1 IF-MIB::ifDescr.2 = STRING: e1000g0
Event Description	**Cause**	**Recommended Response**	**SNMP Trap Objects and Example Values**
Size of memory allocated to a running process has exceeded threshold.	Generally associated with a leak in the main call routing process (gis). *Note: Correct configuration depends on installation; see iServer release notes.*	Log on the system. Use ps command to locate the PID of the process. Analyze to determine cause of excessive memory, if possible. Kill or restart controlling application.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (11333) 0:01:53.33 SNMPv2-MIB::snmpTrapOID.0 = OID: DISMAN-EVENT-MIB::mteTriggerFired DISMAN-EVENT-MIB::mteHotTrigger = STRING: high process memory DISMAN-EVENT-MIB::mteHotTargetName = STRING: DISMAN-EVENT-MIB::mteHotContextName = STRING: DISMAN-EVENT-MIB::mteHotOID = OID: HOST-RESOURCES-MIB::hrSWRunPerfMem.245 DISMAN-EVENT-MIB::mteHotValue = INTEGER: 1328 HOST-RESOURCES-MIB::hrSWRunName.245 = STRING: "gis"
CPU load average has exceeded threshold	High incoming call volume, DOS attack	Check endpoints for call volume, check logs for invalid messages (DOS).	Note that on multiprocessor systems, threshold monitoring is based on an overall total of utilization for all processors in an iServer, rather than individual CPUs.
SNMP agent startup	Normal startup	None	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (20) 0:00:00.20 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::coldStart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
SNMP agent shutdown	Normal shutdown	None	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (620) 0:00:06.20 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown
SNMPv3 authentication failure	Unauthorized access or incorrect v3 configuration.	If authorized, verify username and password.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (4108) 0:00:41.08 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::authenticationFailure SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

7 GENERACIÒN DE ARCHIVOS DE BACKUP

7.1 Generación de Respaldos

<table>
<tr><td colspan="2">Prueba numero 01: Generación de Respaldos</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Generación de Respaldos</td><td colspan="2">Sub Item: Generación de Respaldos</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Generar respaldos de CDRs y de cada uno de los respaldos de la tabla anexa.</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Verificar que se genera el respaldo</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

Tabla de Respaldos

Category	Files
Machine operating system/network configuration	/etc/passwd /etc/shadow /etc/system
Networking	/etc/hosts /etc/netmasks /etc/nodename /etc/resolv.conf /etc/inet/ntp.conf /kernel/drv/e1000g.conf /etc/TIMEZONE crontab file (/var/spool/cron/crontabs/*)
Firewall	/etc/opt/ipf/ipf.conf /etc/opt/ipf/additional*
rsync and syslog	/etc/rsyncd.conf /etc/syslog.conf
iServer configuration	/usr/local/nextone/bin/server.cfg /usr/local/nextone/bin/pools.xml /usr/local/nextone/bin/iserverlc.xml /usr/local/nextone/bin/h323gk*val /usr/local/nextone/bin/codemap*
Configuration files used by scripts under crontab	/usr/local/nextone/etc/dbback.cfg /usr/local/nextone/etc/cdrtrim.cfg /usr/local/nextone/etc/logpp.conf /usr/local/nextone/etc/events.conf
iVMS (or NARS) Agent	/usr/local/narsagent/cdrstream*.xml /usr/local/narsagent/NARS.server.lc /usr/local/narsagent/nars.cfg /usr/local/narsagent/narslog.cfg
Output from cli db export	cli db export /opt/old-database gzip /opt/old-database
SNMP Configuration	/etc/snmp/conf/snmpd.conf
CDR formatting scripts	Scripts under /home/nextone/cdrs

8. CALIDAD DE SERVICIO

8.1 Prueba de Jitter

<table>
<tr><td colspan="2">Prueba numero 01: Prueba de Jitter, norma Y.1541 ITU</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Prueba de Jitter</td><td colspan="2">Sub Item: Ninguno</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Generar pruebas de Jitter</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Mediciones de Jitter acorde a la norma Y.1541 ITU</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

8.2 Prueba de Delay

<table>
<tr><td colspan="2">Prueba numero 02: Prueba de Delay, norma Y.1541 ITU</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Prueba de Delay</td><td colspan="2">Sub Item: Ninguno</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Generar pruebas de Delay</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Mediciones de Delay acorde a la norma Y.1541 ITU</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

8.3 Prueba de Packet Lost

<table>
<tr><td colspan="2">Prueba numero 03: Prueba de Packet Lost, norma Y.1540 ITU</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Prueba de Packet Lost</td><td colspan="2">Sub Item: Ninguno</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Generar pruebas de Packet Lost</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Mediciones de Packet Lost acorde a la norma Y.1540 ITU</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

8.4 Prueba de Factor R

<table>
<tr><td colspan="2">Prueba numero 04: Prueba de Factor R, norma G.107 UIT</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Prueba de Factor R</td><td colspan="2">Sub Item: Ninguno</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Generar pruebas de Factor R</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Mediciones de Factor R, por encima del 80% acorde a la norma G.107</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>

8.5 Prueba de MOS

<table>
<tr><td colspan="2">Prueba numero 05: Prueba de MOS, norma P.800 ITU</td><td colspan="2">Fecha:</td></tr>
<tr><td colspan="2">Item: Prueba de Factor R</td><td colspan="2">Sub Item: Ninguno</td></tr>
<tr><td colspan="4">Condiciones de la prueba:
El equipo instalado, trabajando y configurados los perfiles de acceso</td></tr>
<tr><td colspan="4">Condiciones para la prueba:
Que el equipo esté conectado a la red, en condición de trabajo normal
Procedimiento de Prueba
1. Generar pruebas de MOS</td></tr>
<tr><td colspan="4">Resultados esperados,
1. Mediciones de MOS, por encima del 3,5 acorde a la norma P.800</td></tr>
<tr><td colspan="3">Resultados de la prueba y conclusiones</td><td>Pasó la prueba
Falló la prueba</td></tr>
<tr><td>Por 123.COM.VE</td><td></td><td>Por el proveedor</td><td></td></tr>
</table>