ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

DISEÑO DEL SISTEMA DE TELEFONÍA IP PARA EL MUNICIPIO DE AMBATO

MARCELO SOLÍS

Sangolquí – Ecuador

2008

CERTIFICACIÓN

Por medio de la presente certificamos que el proyecto de grado para la obtención del título en ingeniería electrónica denominado: "**DISEÑO DEL SISTEMA DE TELEFONÍA IP PARA EL MUNICIPIO DE AMBATO"** fue desarrollado en su totalidad por el señor LUIS MARCELO SOLÍS SÁNCHEZ.

Atentamente,

Ing. Gonzalo Olmedo	Ing. Román Lara
DIRECTOR	CODIRECTOR

RESUMEN

El presente estudio, tiene por objeto desarrollar un sistema de Telefonía IP para el Municipio de Ambato, que permita explotar los beneficios que ofrece esta nueva tecnología así como brindar lineamientos para futuros diseños de este tipo, con la finalidad de determinar si la red de datos actual con la que cuenta la Municipalidad, presenta las condiciones adecuadas para soportar servicios convergentes de voz y datos se realizo un completo análisis cualitativo y cuantitativo, del mismo modo se examino la red telefónica para investigar y obtener los requerimientos, esto derivó en la recomendación de un rediseño de la red, que agregue mecanismos para control y provisión de Calidad de Servicio, seguidamente y sobre una plataforma eficazmente funcional ahora si es posible, seleccionar el sistema de Telefonía IP más adecuado para este caso específico, el cual ofrecerá redundancia en el procesamiento de llamadas lo que implica una alta disponibilidad, además de mensajería de voz unificada, que en su conjunto brindarán una plataforma de comunicación eficiente que facilitará e impulsará el trabajo diario de los funcionarios municipales, además de reducir en por lo menos un 14% los costos en llamadas locales de toda la organización.

DEDICATORIA

Este al igual que todos los triunfos que he alcanzado y alcanzaré en mi vida se los dedico a mi madre, pues es mi fuente de infinita inspiración, con su ejemplar, modo de afrontar las adversidades de la vida así como de regocijarse en los momentos de alegría me ha ensañado las lecciones más sabias que han forjado mi personalidad y me han convertido en un hombre de provecho para mi familia y la sociedad.

Ahora que su corazón desborda de alegría al cosechar las semillas de su esfuerzo diario, reflejado en la consecución de mi profesión, lo cual no es más que una pequeña retribución a todo ese sacrificio, realmente no existen palabras que puedan exteriorizar el sentimiento de agradecimiento eterno que profeso, por haberme apoyado siempre.

También quiero extender esta dedicatoria a mi queridos hermanos, pues apoyados en ellos los caminos de la vida siempre serán mucho más llevaderos, a la vez a Diego mi hermano menor, espero inculcar en ti, el compromiso de brindarle a tu madre la satisfacción total de ver a todos sus hijos como exitosos profesionales.

AGRADECIMIENTO

Reitero mi agradecimiento a todos los excelentes profesores, que durante toda mi carrera universitaria en la Escuela Politécnica del Ejercito, me han preparado exitosamente para afrontar los retos profesionales, que el mundo actual exige.

Agradezco y resalto el apoyo que recibí por parte de los funcionarios del Ilustre Municipio de Ambato, sobre todo del Departamento de Sistemas dirigido por el Ing. Xavier Francisco López, quien junto a su selecto grupo de colaboradores, me brindaron total apertura para poder desarrollar mi proyecto de grado, demostrando siempre un elevado espíritu de colaboración digno de destacar, agradezco también a mi buen amigo Marco Castillo, quien colaboró desinteresada y pro-activamente brindando asistencia en el desarrollo del monitoreo de la red.

PROLOGO

La Ilustre municipalidad de Ambato, con el afán de ofrecer un mejor servicio a la ciudadanía, esta empeñada en un proceso de mejoramiento tecnológico, que le permita explotar las ventajas de las tecnologías de la Información y Comunicación TIC´s, que se han convertido en un conjunto de herramientas, soportes y canales para el tratamiento y acceso a la información; siguiendo con esta directiva, a través del presente estudio se busca diseñar un sistema de comunicaciones de voz que reemplace al actual, el mismo que funciona sobre una plataforma totalmente analógica e independiente de la de datos y presenta algunas falencias en la Matriz.

La Telefonía IP, consiste en utilizar tecnología de redes IP para transmitir llamadas de voz. La ventaja obvia es que permite ahorrar costos, puesto que enviar llamadas de voz en paquetes de datos a través de la red es más eficiente y económico que realizar llamadas a través de una red de telefonía tradicional.

Inicialmente para el desarrollo de este estudio y la obtención de requerimientos se realizó un completo levantamiento de campo en la Matriz de la Ilustre Municipalidad de Ambato y sus dependencias que por compartir un enlace WAN están dentro del alcance del presente estudio estas son: Las Comisarias, El Departamento de Cultura, El Hospital Municipal, La Unidad de Tránsito, El Mercado Mayorista, El Camal Municipal, y Las Bodegas; con la finalidad de determinar aspectos como el estado actual de la red tanto de datos, como, telefónica, permitiéndonos establecer aspectos como; la estructura de la red WAN, las LAN´s de cada dependencia, el tipo de cableado o medios de comunicación, los equipos que soportan dicha red, las topologías de red, las PBX telefónicas, el número de usuarios de telefonía a satisfacer y cantidad de hosts. Así como diagnosticar el comportamiento funcional de la red para determinar si los servicios de voz pueden converger con los de datos que actualmente circulan por la misma.

Al determinar las limitaciones funcionales de los equipos de red con que actualmente se cuenta, se recomienda una reestructuración de la red introduciendo en ella características, estándares y funcionalidades que permitan ubicar los parámetros de QoS dentro de los rangos recomendables para el tráfico de voz.

INDICE DE CONTENIDO

CAPÍTULO I:

INTRODUCCIÓN A LA TELEFONÍA Y REDES IP

CAPITULO II:

LA TELEFONÍA IP, SUS PROTOCOLOS Y APLICACIONES

CAPÍTULO III:

ANALISIS DE LA RED EXISTENTE Y OBTENCIÓN DE REQUERIMIENTOS

CAPÍTULO IV:

RECOMENDACIONES PARA EL REDISEÑO DE LA RED DE DATOS

CAPÍTULO V:

DISEÑO DEL SISTEMA DE TELEFONÍA IP PARA EL MUNICIPIO DE AMBATO

CAPÍTULO VI:

CONCLUSIONES Y RECOMENDACIONES

INDICE DE TABLAS

CAPÍTULO I:

INTRODUCCIÓN A LA TELEFONÍA Y REDES IP

CAPITULO II:

LA TELEFONÍA IP, SUS PROTOCOLOS Y APLICACIONES

CAPÍTULO III:

ANALISIS DE LA RED EXISTENTE Y OBTENCIÓN DE REQUERIMIENTOS

CAPÍTULO IV:

RECOMENDACIONES PARA EL REDISEÑO DE LA RED DE DATOS

CAPÍTULO V:

DISEÑO DEL SISTEMA DE TELEFONÍA IP PARA EL MUNICIPIO DE AMBATO

INDICE DE FIGURAS

CAPÍTULO I:

INTRODUCCIÓN A LA TELEFONÍA Y REDES IP

CAPITULO II:

LA TELEFONÍA IP, SUS PROTOCOLOS Y APLICACIONES

CAPÍTULO III:

ANALISIS DE LA RED EXISTENTE Y OBTENCIÓN DE REQUERIMIENTOS

CAPÍTULO IV:

RECOMENDACIONES PARA EL REDISEÑO DE LA RED DE DATOS

CAPÍTULO V:

DISEÑO DEL SISTEMA DE TELEFONÍA IP PARA EL MUNICIPIO DE AMBATO

GLOSARIO

-A-

ACL	Access control list
ADPCM	Adaptive Differential Pulse Code Modulation
AP	Access point
ARP	Address Resolution Protocol
ATA	Cisco Analog Telephone Adapter
ATM	Asynchronous Transfer Mode

-B-

BGP	Border Gateway Protocol
bps	Bits per second
BRI	Basic Rate Interface

-C-

CAC	Call Admisión control
CAS	Channel Associated Signaling
CBWFQ	Class-Based Weighted Fair Queuing
CCS	Common channel signaling
CDP	Cisco Discovery Protocol
CDR	Call detail record
CIR	Committed information rate
CM	Cisco Unified Communications Manager
CME	Cisco Unified Communications Manager Express
CO	Central office
CoS	Class of service
CUE	Cisco Unity Express

-D-

DHCP	Dynamic Host Configuration Protocol
DID	Direct inward dial
DNS	Domain Name System
DoS	Denial of service
DSCP	Differentiated Services Code Point
DSP	Digital signal processor
DTMF	Dual tone multifrequency

-E-

E&M	Receive and transmit, or ear and mouth
EC	Echo cancellation
EIGRP	Enhanced Interior Gateway Routing Protocol

-F-

FIFO	First-in, first-out
FR	Frame Relay
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station

-G-

GSM	Global System for Mobile Communication
GUI	Graphical user interface

-H-

HTTP	Hyper-Text Transfer Protocol
HTTPS	Secure HTTP
Hz	Hertz

-I-

IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IMAP	Internet Message Access Protocol
IntServ	Integrated Services
IntServ/DiffServ	Integrated Services/Differentiated Services
IP	Internet Protocol
IPSec	IP Security
ISO	International Standards Organization
ITU	International Telecommunication Union
IVR	Interactive voice response

-K-

kbps	Kilobits per second

-L-

LAN	Local area network
LBR	Low bit-rate
LCD	Liquid Cristal display
LDAP	Lightweight Directory Access Protocol
LLQ	Low-latency queuing

-M-

MAC	Media Access Control
MAN	Metropolitan area network
Mbps	Megabits per second
MGCP	Media Gateway Control Protocol

MIB	Management Information Base
MIPS	Millions of instructions per second
MPLS	Multiprotocol Label Switching
ms	Millisecond
Mw	Milli-Watt

-N-

NAT	Network Address Translation
NIC	Network interface card

-O-

OSPF	Open Shortest Path First

-P-

PBX	Private branch exchange
PC	Personal computer
PCM	Pulse code modulation
PoE	Power over Ethernet
pps	Packets per second
PQ	Priority Queue
PRI	Primary Rate Interface
PSTN	Public switched telephone network
PVC	Permanent virtual circuit

-Q-

QoS	Quality of Service

-R-

RF	Radio frequency
RIP	Routing Information Protocol
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
RTT	Round-trip time

-S-

SCCP	Skinny Client Control Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SRST	Survivable Remote Site Telephony
SRTP	Secure Real-Time Transport Protocol
SS7	Signaling System 7
STP	Spanning Tree Protocol

-T-

TCP	Transmission Control Protocol
TDM	Time-division multiplexing
TFTP	Trivial File Transfer Protocol
ToS	Type of service
TTL	Time to live

-U-

UAC	User agent client
UAS	User agent server
UDP	User Datagram Protocol
UPS	Uninterrupted power supply
USB	Universal Serial Bus
UTP	Unshielded twisted pair

-V-

VAD	Voice activity detection
VIC	Voice interface card
VLAN	Virtual local area network
VoIP	Voice over IP
VPN	Virtual private network

-W-

WAN	Wide area network
WFQ	Weighted fair queuing
WLAN	Wireless local area network

CAPÍTULO I:

1. INTRODUCCIÓN A LA TELEFONÍA Y REDES IP

1.1. LA TELEFONÍA CONVENCIONAL

Los constantes progresos tecnológicos, especialmente en el campo de las telecomunicaciones, obligan al profesional e incluso al usuario final, a mantenerse actualizado en cuanto a las diversas opciones que actualmente pueden satisfacer las necesidades de comunicación. Sin embargo, para enfocar a la tecnología más reciente, vale la pena mirar hacia atrás; el conocer los antecedentes de la telefonía actual ayudará a entender de mejor manera el cómo y el porqué de la misma. En otras palabras, se deberá comprender cómo las necesidades que fueron satisfechas de una u otra manera con antiguas tecnologías e infraestructuras, con sus limitaciones, obligaron a buscar nuevas soluciones tecnológicas. Es por eso que el presente apartado busca explicar el funcionamiento de las redes de telefonía convencional, lo cual encierra la comprensión de varios conceptos, y la familiarización con muchos de los términos que se usan en Telefonía.

1.1.1. TIPOS DE SISTEMAS DE TELEFONÍA [1]

Actualmente, los sistemas de telefonía se dividen en tres grupos, según el tipo de usuario:

- Sistemas de uso residencial
- Sistemas empresariales
- Sistemas *Centrex* externos

a) Sistemas de uso residencial [1]

Se trata de los sistemas telefónicos más simples, que como su nombre lo indica, trata de las instalaciones telefónicas que llegan a los hogares, tal como se muestra en la figura 1.1. Los sistemas telefónicos suelen dividirse en niveles funcionales, que son: la red de acceso, la red de transporte, la red de distribución y la red de transmisión. La red de acceso se refiere principalmente al *loop* del abonado que va desde la roseta ubicada en el domicilio hasta el cajetín telefónico o punto de terminación; la red de transporte es todo el cableado que se aglomera en los armarios telefónicos con cientos de pares. La red de distribución es la agrupación de todos los pares telefónicos de los armarios y es la que finalmente llega a la oficina central. Por último se conoce como red de transmisión al conjunto de líneas troncales a través de las cuales se conectan las oficinas centrales. Los dispositivos que controlan el funcionamiento de la red de transmisión son dispositivos de gran capacidad conocidos como *switches* de voz, construidos solo por ciertos fabricantes.

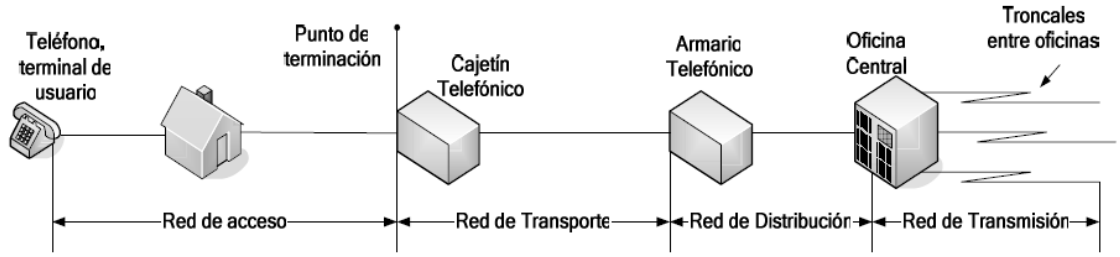


Figura. 1.1. Niveles funcionales de un Sistema Telefónico Residencial

b) Sistemas empresariales [1] [2]

Debido a las necesidades especiales de telecomunicación y de funcionamiento (alta productividad personal, gran número de usuarios, minimización de costos y ahorro de recursos) que requieren las organizaciones a mediana y gran escala, se vio la necesidad de crear sistemas telefónicos que se adapten a las mismas. Esto en razón de que los sistemas telefónicos suelen variar de acuerdo a la necesidad que buscan suplir, existiendo además grandes diferencias entre uno y otro.

Gracias a que los emplazamientos se encuentran conectados entre sí a través de enlaces dedicados, no es necesario interactuar con la RTC (Red Telefónica Conmutada) para la comunicación interna de la empresa, ahorrando con ello costos. Para comunicarse

con el exterior se tiene al menos en un emplazamiento una línea hacia la red telefónica conmutada e incluso cada una de las sucursales generalmente está provista de un teléfono exclusivo con línea directa a la RTC, de manera que un fallo en el sistema empresarial no deje a la empresa incomunicada en su totalidad.

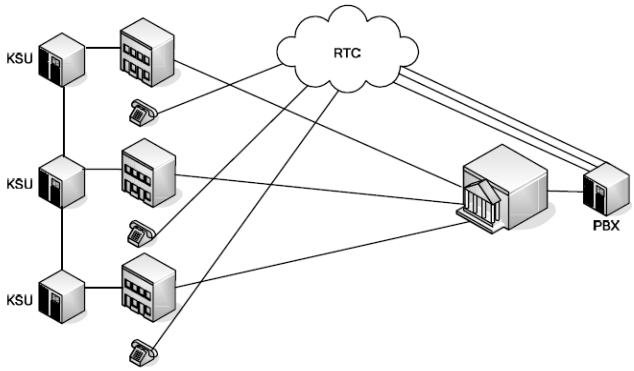


Figura. 1.2. Sistema Telefónico Empresarial típico para una entidad de varias sucursales o emplazamientos [1]

Los elementos que forman parte de sistemas telefónicos empresariales se describen a continuación:

Teléfonos de tipo empresarial: son teléfonos propietarios, por lo que el sistema telefónico empresarial debe tener terminales del mismo fabricante; esto con excepción de los teléfonos analógicos o convencionales, debido a que la diferencia entre proveedores se refiere principalmente a señalización digital.

Dispositivos analógicos: son todos los dispositivos que necesitan una línea analógica o POTS (Servicio Telefónico Analógico Convencional) para funcionar; debido a que las PBX (*Private Branch Exchange*, Central Privada) trabajan digitalmente, éstas permiten la conexión de puertos especiales para este tipo de aplicaciones. Un fax o un módem analógico son ejemplos de este tipo de dispositivos.

Key System Unit (KSU) tradicionales e híbridos: un KSU es un concentrador de líneas telefónicas, no realiza conmutación, lo que quiere decir que tal tarea se halla aún en manos de la Oficina Central (CO), sin embargo provee algo de control sobre los servicios de valor agregado.

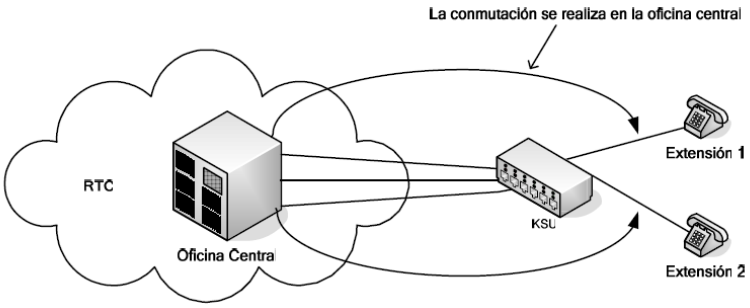


Figura. 1.3. KSU tradicional [2]

Los KSU tradicionales no soportan troncales digitales, utilizan troncales analógicas del tipo *loop – start*. En el caso de las KSU híbridas, su operación es bastante cercana a la de una PBX (soporte para troncal digital, marcación directa interna DID) sin embargo su capacidad para manejar un gran número de líneas sigue siendo inferior.

Centrales privadas (PBX): la PBX o PABX (*Private Automatic Branch Exchange*), es un conmutador o *switch* telefónico capaz de enrutar las llamadas que entran y salen de la empresa. En el caso de tener llamadas internas o entre extensiones, la PBX conmuta por sí misma la llamada evitando el uso de circuitos de la RTC; solo cuando la llamada saliente tiene como destino un terminal ajeno a la empresa utiliza una de las líneas externas.

Físicamente la PBX consta de un gabinete que puede ser instalado de forma independiente o sobre un RACK, en el cual se insertan tarjetas electrónicas, cada una con funcionalidad propia; es decir existe una tarjeta de CPU (*Central Processing Unit*, Unidad Central de Procesamiento), otra para teléfonos empresariales, otra para terminales convencionales, otra más para troncales, cancelación de eco, etc. La mayoría de estas tarjetas se diseñan para manipulación en "caliente" (*Hot Swapping*), es decir no es necesario apagar la PBX para extraer o colocar la tarjeta, permitiendo que la comunicación dentro de la empresa no caiga totalmente.

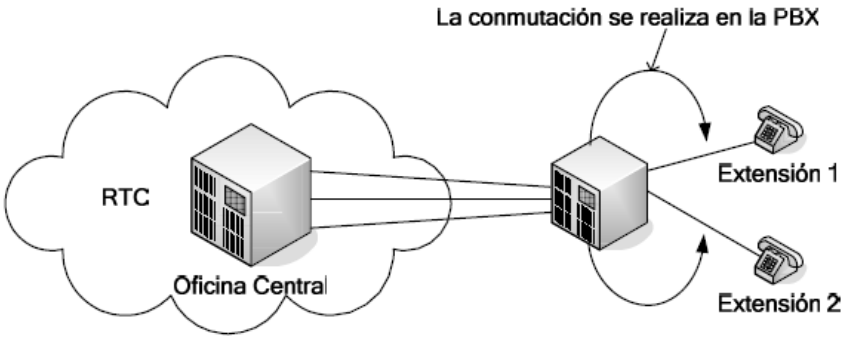


Figura. 1.4. Central telefónica privada PBX [2]

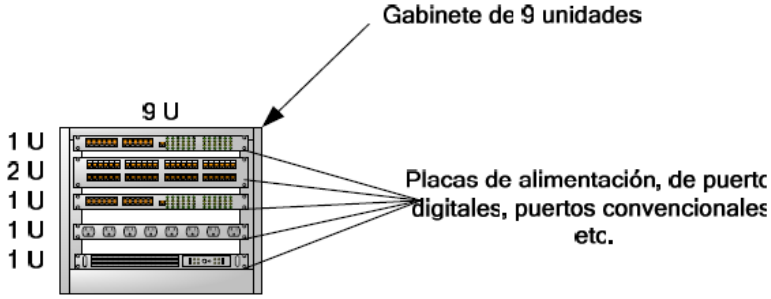


Figura. 1.5. Disposición física de una PBX [1]

Distribuidores automáticos de llamada (ACD): un ACD es simplemente un tipo especial de PBX; una de sus aplicaciones más importantes es en *Call Centers* o en soporte de ventas. En dichos establecimientos las llamadas que se reciben se distribuyen entre los agentes (operadores calificados en atención) de acuerdo a un conjunto de reglas previamente acordado. La recepción de llamadas puede jerarquizarse de distintos modos, por ejemplo se puede direccionar una comunicación al agente que ha pasado más tiempo sin recibir una llamada, o aquel que tiene más experiencia o según el horario de trabajo que éste cumple.

DNIS (*Dialing Number Identification Service*) y ANI (*Automatic Number Identification*): proveen respectivamente, la identificación del número del abonado llamante y un número de identificación del cliente dentro de la organización, asociado a su línea telefónica. Ambos son dos fuentes importantes de que el ACD hace uso para la obtención de datos del cliente, a través de los mismos se pueden distribuir las llamadas al agente correcto; sin embargo no es el único método.

A través de un ACD una organización puede tener más troncales que agentes atendiendo las líneas, esto gracias a un simple mecanismo de cola que mantiene; tal mecanismo puede configurarse para priorizar los clientes que deben ser atendidos primero. En la mayoría de centrales privadas actuales el ACD es más bien un software bien definido a través del cual la misma PBX puede realizar todas estas funcionalidades.

Unidades de respuesta de voz interactiva (IVR): son dispositivos que pueden integrarse a la PBX. Un mensaje grabado desde la central privada hacia el usuario inicia la comunicación, pudiendo éste contestar a través del teclado numérico; de todas maneras siempre se da la opción de esperar para acceder a una operadora.

Un IVR no solamente funciona para tomar datos para el ACD, es también capaz de satisfacer consultas sencillas, lo que se traduce en reducción del tráfico hacia los agentes lo cual se refleja en la productividad; en este caso los IVR deberán siempre trabajar en conjunto con bases de datos de las cuales descargan la información a tiempo real, que el cliente pide a través del teclado. Estados de cuenta, saldos, e información en general son situaciones de explotación de los IVR.

Correo de voz y sistemas de atención automática: el correo de voz generalmente es un dispositivo autónomo, el cual es capaz de receptar y reproducir mensajes para todos los usuarios que mantienen una cuenta de correo.

Cada vez que una extensión no responde, el sistema redirige la comunicación al buzón de voz correspondiente, el cual tiene un mensaje grabado personalizado de recepción de mensajes; esto ocurre siempre y cuando tal función se halle habilitada a través de una conexión serie SMDI (*Simplified Message Desk Interface*). En caso contrario el sistema utiliza el asistente automático de correo de voz, en donde a través del IVR, el usuario que llama ingresa un número clave del buzón de voz al que quiere acceder y lo utiliza de manera normal. Terminado el proceso el asistente da la opción de dejar un mensaje grabado en otro buzón o abandonar el sistema.

c) Sistemas *Centrex* externos [1]

Un sistema *Centrex* es un servicio que ofrece el operador telefónico local, de manera que simula una pequeña central privada agrupando varias líneas a las cuales entrega funcionalidades avanzadas como re-direccionamiento de llamadas, conferencia, marcación

abreviada, etc. Se podría decir que el *Centrex* es un punto intermedio entre una PBX y un sistema residencial, pues su uso es frecuente en empresas que no desean realizar grandes gastos en sistemas telefónicos privados pero necesitan algunas de sus funcionalidades. Cabe aclarar que en un *Centrex* la conmutación se hace dentro de la CO y por tanto una llamada entre extensiones es tarificada como una llamada local. La escalabilidad de un sistema *Centrex* es aceptable dentro de un rango; en el caso de empresas pequeñas e incluso medianas el obtener nuevas líneas del sistema *Centrex* es una operación bastante fácil gracias a las grandes capacidades del conmutador telefónico de la CO. Sin embargo para un número grande de usuarios el cableado vendría a ser un inconveniente grave, recuérdese que cada extensión es un par telefónico entre la empresa y la CO.

Finalmente los terminales de una *Centrex* son del tipo convencional y generalmente carecen de visualizadores, por esto las funcionalidades avanzadas se representan a través de tonos especiales que envía el conmutador.

1.1.2. CIRCUITOS TRONCALES [1] [3]

Los circuitos troncales se utilizan en la conexión entre emplazamientos de una empresa; toman también este nombre las líneas que llegan desde el proveedor de servicio telefónico local. Este último puede proveer troncales analógicas o troncales digitales con canales de voz multiplexados en el tiempo (TDM) como un T1 o E1 de 24 y 30 canales de voz respectivamente. Las PBX suelen contar con tarjetas de troncales digitales E1/T1 a las que fácilmente se puede conectar las líneas que vienen del proveedor, en caso de no disponer de estas tarjetas se puede usar un banco de canales de manera que cada canal multiplexado de la troncal digital simule un DS0 (*Digital signal – Level* 0, 64 kbits/s) independiente que pueda dar conectividad a un puerto analógico del *switch* de voz.

El proveedor puede abastecer distintos tipos de troncales (depende del país), cuyas características se tratan a continuación de manera general.

a) Línea con tono de marcación [1]

Se trata de un par de hilos que proporcionan conectividad analógica; es la típica conexión residencial asociada a un número único asignado por el proveedor. En ambiente empresarial este tipo de troncal toma el nombre de *loop-start* (por el tipo de señalización que utiliza esta troncal analógica) si está conectado a una PBX.

b) Troncales bidireccionales [1]

Las troncales bidireccionales o troncales de combinación se conectan a una PBX. La señalización que utilizan (*ground – start*) está diseñada para evitar un problema conocido como "*glare*", el cual ocurre cuando las llamadas salientes y entrantes coinciden; el usuario que llama logra la conexión pero no tiene comunicación, en tanto que el llamante ignora que ya está comunicado y trata de tomar línea.

Por lo general las líneas bidireccionales se ocupan solo para llamadas salientes, debido a la existencia de las líneas DID (Marcación directa interna), es por eso que las troncales bidireccionales se ocupan como DOD (Marcación directa externa).

c) Troncales DID [1]

La troncal de marcación interna directa permite la comunicación entre los empleados de una empresa sin necesidad de utilizar circuitos del proveedor. Para que un usuario exterior acceda a una empresa que no está utilizando troncales DID, éste marcará el número principal de la empresa y después la extensión asignada al empleado con el que desea comunicarse; si la empresa utiliza DID y posee un bloque de números reservados, la parte que llama marcará solo los dígitos asignados al bloque y la extensión del empleado.

Pero la función de DID no se detiene ahí, se pueden además asignar bloques de números en mayor número que las líneas existentes, por ejemplo con 24 troncales DID se podría dar un número propio hacia el exterior para 100 empleados, a diferencia de una troncal básica en la cual la línea física está relacionada con un número único.

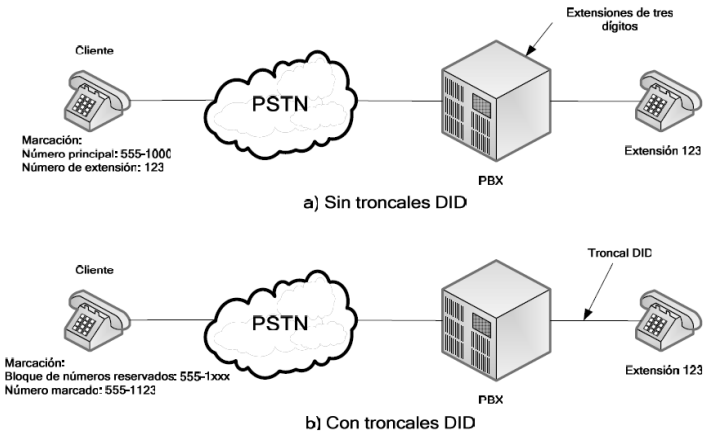


Figura. 1.6. Troncales DID en un sistema telefónico empresarial [1]

La desventaja de DID es que solo atiende llamadas internas, de todas formas es en este punto donde entra la funcionalidad de las líneas DOD.

d) Líneas punto a punto [1]

Las líneas punto a punto o *tie lines* son líneas dedicadas que pueden usarse en voz y datos. En el caso de la voz estas líneas suelen usarse en formato de tramas D4 y codificación de línea AMI (*Alternate Mark Inversion*), o también con formato de trama ESF (*Extended Super-Framing*) y codificación de línea B8ZS si la PBX considerada lo soporta. Por lo general se usa *tie lines* entre PBX, con señalización E&M para establecimiento y desconexión de la llamada.

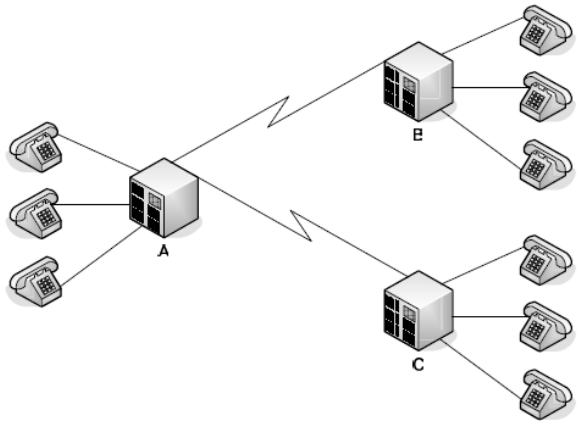


Figura. 1.7. Red con troncales punto a punto [1]

En la figura 1.7 se muestra una red con troncales punto a punto; en este caso un usuario en el emplazamiento B que desee entablar comunicación con un miembro del emplazamiento C debe atravesar dos líneas punto a punto, el proceso que se debe llevar a cabo es parecido al enrutamiento en una red de datos en donde cada número marcado se refiere a un salto en la red. En este caso el usuario en B marca un número de código de acceso al troncal (TAC) de manera que obtiene acceso a la troncal del emplazamiento A; la PBX de A entrega tono de marcación y se podrá llamar a las extensiones en dicho emplazamiento.

El proceso de tomar la línea punto a punto y efectuar las llamadas a extensiones desde el emplazamiento remoto se conoce como *tail-end hop-off* o *toll bypass*.

e) Troncales digitales RDSI (Red Digital De Servicios Integrados) [4]

Las líneas RDSI son conexiones realizadas por medio de líneas telefónicas para transmitir señales digitales en lugar de analógicas.

La RDSI cuenta con canales B y D para transmisión de datos. La información en los canales tipo B, operan en modo de conmutación de circuitos, una vez que ha sido establecida la llamada, se transmite de un modo totalmente transparente, lo cual eventualmente permitiría emplear cualquier conjunto de protocolos como SNA, PPP, TCP/IP, etc.

El canal de control de la llamada, o canal D, también denominado de señalización, permite, el establecimiento, monitorización y control de la conexión RDSI, y es el responsable de generar incluso los timbres de llamada. Está definido por la recomendación UIT-T Q.931.

Acceso Básico o BRI.- Acceso simultáneo a 2 canales B de 64 kbps, para voz o datos y un canal D de 16 kbps, para la realización de la llamada y otros tipos de señalización entre dispositivos de la red. En conjunto, se denomina 2B+D, o I.420, que es la recomendación UIT-T que define el acceso básico. El conjunto proporciona 144 kbps.

Acceso Primario o PRI.- Acceso simultáneo a 30 canales tipo B de 64 kbps, para voz y datos. Un canal de 64 kbps, o canal D, para la realización de la llamada y la señalización entre dispositivos de la red. En conjunto, se referencia como 30B+D o I.421, que es la recomendación UIT-T que define el acceso primario y el conjunto proporciona 1.984 kbps.

Por tanto, las interfaces BRI y PRI tienen la siguiente estructura:

Tabla. 1.1. Estructura de las interfaces BRI y PRI

INTERFAZ	ESTRUCTURA	VELOCIDAD TOTAL	VELOCIDAD DISPONIBLE
BRI	2B + D16	192 Kbps.	144 Kbps.
PRI	23B + D64	1.544 Kbps.	1.536 Kbps.
	30B + D64	2.048 Kbps.	1.984 Kbps.

1.2 REDES DE INFORMACION

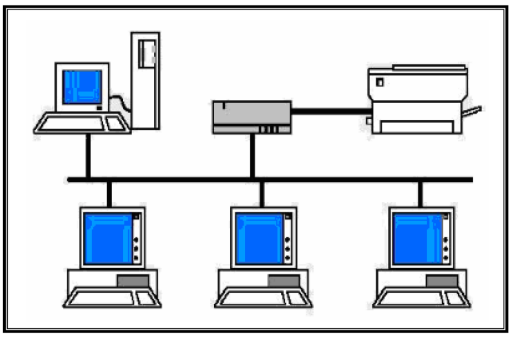


Figura. 1.8. Ejemplo de red sencilla

Una red es un sistema que conecta equipos independientes entre sí para compartir información: voz, datos, video así como también recursos: hardware y software; facilitando la administración y el soporte.

1.2.1 TIPOS DE REDES

Según la Cobertura

Las redes se clasifican en: LAN, MAN, WAN, INTERNET.

a. LAN (Red de Área Local)

Son redes privadas de cobertura pequeña, limitada a una extensión de entre diez metros a un kilómetro, generalmente se las utiliza en oficinas dentro de una edificación o un conjunto de edificaciones que estén contiguos. Es un sistema de interconexión con conectividad total entre estaciones, cobertura pequeña y variadas velocidades de transmisión.

Las principales tecnologías usadas en una LAN son: Ethernet, Token Bus, Token Ring, y FDDI.

b. MAN (Red de Área Metropolitana)

Es un sistema de interconexión de equipos informáticos distribuidos en una zona privada o pública, con una cobertura que va desde un kilómetro a diez kilómetros, esta

extensión suele abarcar una ciudad. Este tipo de redes se utilizan normalmente para interconectar redes de área local.

Una MAN privada sería un gran departamento o administración con edificios distribuidos por la ciudad, transportando todo el tráfico de voz y datos entre edificios por medio de su propia MAN y encaminando la información externa por medio de los operadores públicos.

Una MAN pública es la infraestructura que un operador de telecomunicaciones instala en una ciudad con el fin de ofrecer servicios de banda ancha a sus clientes localizados en esta área geográfica.

Las principales tecnologías usadas en una MAN son: FDDI, DQDB, SMDS y ATM.

c. WAN (Red de Área Extendida)

Es un sistema de interconexión de equipos informáticos geográficamente distantes, con una cobertura que va desde diez kilómetros a diez mil kilómetros El sistema de conexión normalmente involucra a redes públicas de transmisión de datos.

Las principales tecnologías usadas en una WAN son: Frame Relay, ATM.

d. Internet

Es una red WAN mundial o súper WAN que está formada por un conjunto de redes interconectadas a nivel mundial que usan ciertos protocolos comunes para proporcionar servicios y puede estar desarrollada sobre diferentes software y hardware.

Según la Tecnología de Transmisión

a. Redes de *Broadcast*

Aquellas redes en las que la transmisión de datos se realiza por un sólo canal de comunicación compartido por todas las máquinas de la red. Cualquier paquete de datos enviado por una máquina cualesquiera es recibido por las máquinas restantes de la red.

b. Redes Punto a Punto

Aquellas en las que existen muchas conexiones entre parejas individuales de máquinas. En una red punto a punto, los dispositivos en red actúan como pares entre sí. La información puede pasar por una o más máquinas intermedias para ir del origen hacia su destino.

Según el Tipo de Transferencia de Datos que soportan

a. Redes de Transmisión Simplex

Son aquellas redes en las que los datos sólo pueden viajar en un sentido.

b. Redes *Half-Duplex*

Aquellas en las que los datos pueden viajar en ambos sentidos, pero sólo puede haber transferencia en un sentido a la vez.

c. Redes *Full-Duplex*

Aquellas en las que los datos pueden viajar en ambos sentidos a la vez.

Redes Inalámbricas

Son redes cuyos medios físicos no son cables de ningún tipo. Están basadas en la transmisión de datos mediante ondas de radio de diferentes rangos tales como microondas terrestres, microondas satelitales y ondas infrarrojas o milimétricas.

1.2.2 TÉCNICAS DE ACCESO AL MEDIO

Se pueden distinguir a las siguientes técnicas para la resolución de conflictos:

a. Acceso Múltiple con Detección de Portadora y Detección de Colisiones [5]

Las redes Ethernet / IEEE 802.3, utiliza CSMA/CD (*Carrier Sense Multiple Access / Collision Detection*) como método de acceso al medio, es decir antes de que una estación desee transmitir una trama escucha que el canal se encuentre libre, caso contrario, ejecuta el algoritmo de retroceso binario, el cual establece ranuras iguales al peor tiempo de ida y

vuelta de propagación (para una red de 100 Mbits/s es de 5.12 us), al detectar que el canal está ocupado, la estación espera 2k-1 ranuras de tiempo antes de transmitir, siendo k el número de colisiones.

Gracias a que el algoritmo de retroceso binario es autoadaptivo, es decir, al aumentar el tráfico en una red aumenta la probabilidad de colisiones, el algoritmo introduce un retardo creciente en la estaciones emisoras antes de transmitir nuevamente, con la consiguiente disminución de tráfico. Para evitar introducir retardos excesivos, el número de ranuras de tiempo deja de aumentar tras diez colisiones. A partir de ese instante se intenta transmitir la trama seis veces más. De no ser así se descarta la trama y se notifica el fallo a nivel de capa red.

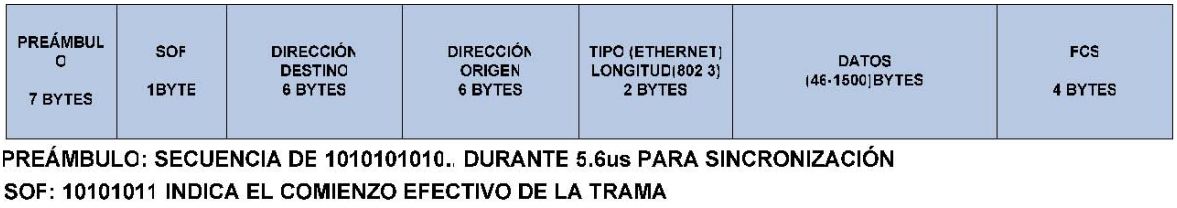


Figura. 1.9. Trama Ethernet [5]

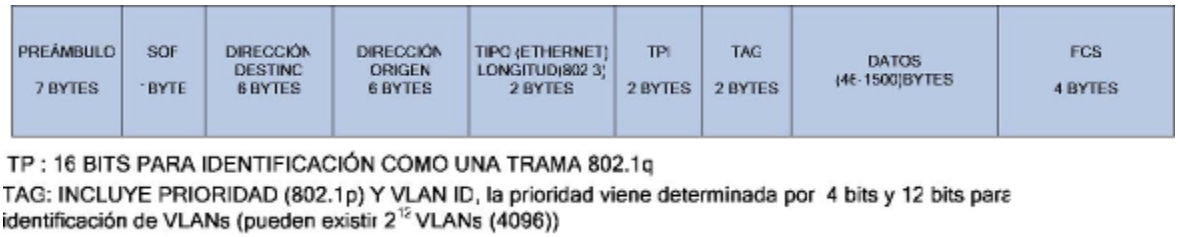


Figura. 1.10. Trama 802.1q [5]

En la mayoría de implementaciones de VoIP, se crea una VLAN dedicada para el servicio de voz. La ventaja radica en aislar el tráfico de la red de los clientes IP, en especial del tráfico de *broadcast*, puesto que los terminales IP dejan de transmitir momentáneamente para escuchar dicha petición, con lo cual la calidad de voz se ve afectada. La implementación de VLANs consta como un método para mejorar la calidad de servicio (QoS) de la VoIP. Cuando se trabaja con VLAN hay que tomar en cuenta que se transmiten 4 bytes más de la trama normal de Ethernet, dicho aumento no repercute considerablemente en el rendimiento de la red.

b. Acceso Múltiple con Detección de Portadora y Evita Colisiones

CSMA/CA, es una técnica que se usa en las redes inalámbricas, en esta técnica si un equipo quiere transmitir escucha el canal, si esta libre transmite y si el canal está ocupado espera un intervalo de tiempo aleatorio envía un pedido de reserva de canal para evitar la colisión de los datos.

c. Paso de Testigo

Bus con Paso de Testigo

Las redes Token Bus IEEE 802.4 se basan en esta técnica. Se utiliza principalmente en aplicaciones industriales con redes de topología física bus y consiste en un token o testigo que pasa de estación en estación en forma cíclica, es decir forma un anillo lógico. Cuando una estación tiene el token, tiene el derecho exclusivo del bus para transmitir o recibir datos por un tiempo determinado y luego pasa el token a otra estación, previamente designada. Las otras estaciones no pueden transmitir sin el token, sólo pueden escuchar y esperar su turno.

Anillo con Paso del Testigo

Las redes con topología física en anillo se basan en esta técnica. Se usa en redes de área local con o sin prioridad, el token pasa de estación en estación en forma cíclica, inicialmente en estado desocupado.

Cada estación cuando tiene el token (en este momento la estación controla el anillo), si quiere transmitir cambia su estado a ocupado y agrega los datos, caso contrario pasa el token a la estación siguiente.

Cuando el token pasa de nuevo por la estación que transmitió, la estación saca datos, pone en desocupado al token y lo regresa a la red.

1.2.3 ESTRUCTURA DEL MODELO ISO/OSI

El modelo ISO/OSI está compuesto por siete capas o niveles, cada uno de los cuales presta servicios a un nivel superior denominado usuario. Así, el nivel 3 es usuario del nivel 2, el nivel 4 es usuario del nivel 3, etc.

CAPAS DEL MODELO ISO/OSI

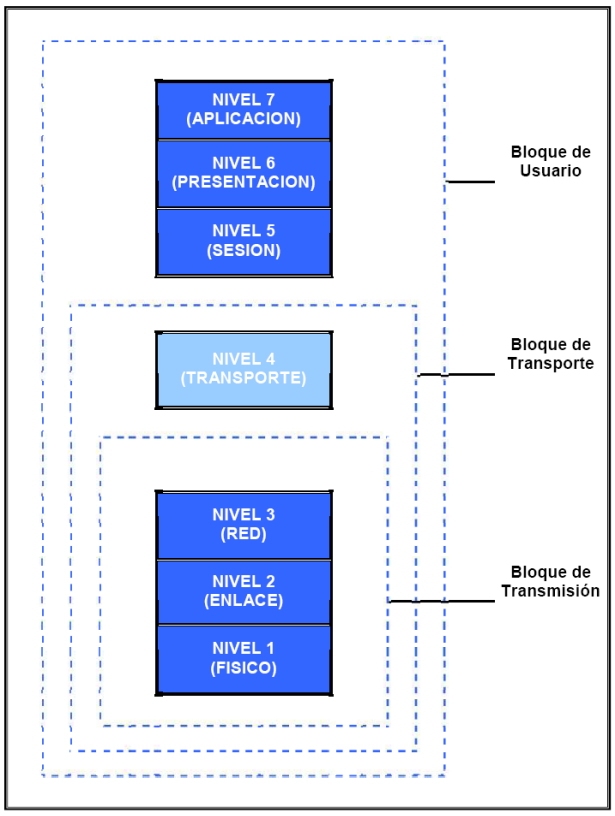


Figura. 1.11. Modelo ISO/OSI

a. Nivel 7: Aplicación

En esta capa se ejecutan las aplicaciones que proporcionan los servicios al usuario, diferenciando las funciones del sistema como transferencia, manipulación de archivos, acceso a terminales, correo electrónico, etc.

De las funciones del usuario que normalmente interactúa con este nivel de aplicación a través de programas, tales como las aplicaciones informáticas como por ejemplo, tratamiento de los archivos recibidos, etc.

b. Nivel 6: Presentación

Se encarga de las funciones de interpretación y presentación de la estructura de la información recibida. En este nivel se realiza la conversión entre distintos alfabetos de comunicaciones, de esa manera sí las máquinas presentan formatos incompatibles, esta capa se encarga de adaptar los datos.

Las funciones del nivel 7 y las del nivel 6 son en cierta forma complementarias.

c. Nivel 5: Sesión

Está relacionado con la gestión de las distintas actividades que pueden tener lugar durante la comunicación.

Regula el diálogo entre los distintos participantes en una comunicación e inserta puntos de pruebas que permiten la comprobación de la transmisión.

d. Nivel 4: Transporte

Es la capa encargada de efectuar el transporte de los datos desde la máquina origen hasta la máquina destino, proporcionando los medios para establecer una comunicación transparente a los niveles superiores.

Este nivel actúa como un puente entre los tres niveles inferiores orientados a las comunicaciones y los tres niveles superiores orientados al procesamiento, garantizando una entrega confiable de la información entre origen y destino encargándose de que se mantenga su secuencia, almacenándolos si el sistema no puede dar respuesta con la suficiente velocidad.

e. Nivel 3: Red

Este nivel define el enrutamiento y el envío de paquetes entre distintas redes, se encarga de conmutar, enrutar y controlar la congestión de los paquetes de información en la subred eligiendo el camino que va a seguir, a fin de que la comunicación tenga lugar.

f. Nivel 2: Enlace

Su función consiste en una comunicación entre los terminales de nivel de enlace y garantiza a los niveles superiores una comunicación libre de errores.

g. Nivel 1: Físico

En él se especifican las características físicas de los medios de comunicación para garantizar los servicios requeridos por los niveles superiores.

Es el único que tiene especificaciones de hardware.

1.3 FAMILIA DE PROTOCOLOS DE INTERNET [6]

La Familia de protocolos de internet es un conjunto de protocolos de red en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se la denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular HTTP (*HyperText Transfer Protocol*), que es el que se utiliza para acceder a las páginas web, además de otros como el ARP (*Address Resolution Protocol*) para la resolución de direcciones, el FTP (*File Transfer Protocol*) para transferencia de archivos, y el SMTP (*Simple Mail Transfer Protocol*) y el POP (*Post Office Protocol*) para correo electrónico, TELNET para acceder a equipos remotos, entre otros.

El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN). TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa del departamento de defensa.

La familia de protocolos de internet puede describirse por analogía con el modelo OSI, que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. En una pila de protocolos, cada nivel soluciona una serie de problemas relacionados con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

El modelo de Internet fue diseñado como la solución a un problema práctico de ingeniería. El modelo OSI, en cambio, fue propuesto como una aproximación teórica y también como una primera fase en la evolución de las redes de ordenadores. Por lo tanto, el modelo OSI es más fácil de entender, pero el modelo TCP/IP es el que realmente se usa.

Sirve de ayuda entender el modelo OSI antes de conocer TCP/IP, ya que se aplican los mismos principios, pero son más fáciles de entender en el modelo OSI.

El 1 de enero de 2008 el Protocolo TCP/IP cumplió 25 años.

1.3.1. ESTRUCTURA DEL MODELO TCP/IP

Hay algunas discusiones sobre cómo encaja el modelo TCP/IP dentro del modelo OSI. Como TCP/IP y modelo OSI no están delimitados con precisión no hay una respuesta que sea la correcta.

El modelo TCP/IP no está lo suficientemente dotado en los niveles inferiores como para detallar la auténtica estratificación en niveles: necesitaría tener una capa extra (el nivel de Red) entre los niveles de transporte e internet. Protocolos específicos de un tipo concreto de red, que se sitúan por encima del marco de hardware básico, pertenecen al nivel de red, pero sin serlo. Ejemplos de estos protocolos son el ARP (Protocolo de resolución de direcciones) y el STP (*Spanning Tree Protocol*). De todas formas, estos son protocolos locales, y trabajan por debajo de las capas de Internet. Cierto es que situar ambos grupos (sin mencionar los protocolos que forman parte del nivel de Internet pero se sitúan por encima de los protocolos de Internet, como ICMP) todos en la misma capa puede producir confusión, pero el modelo OSI no llega a ese nivel de complejidad para ser más útil como modelo de referencia.

Normalmente, los tres niveles superiores del modelo OSI (Aplicación, Presentación y Sesión) son considerados simplemente como el nivel de aplicación en el conjunto TCP/IP. Como TCP/IP no tiene un nivel de sesión unificado sobre el que los niveles superiores se sostengan, estas funciones son típicamente desempeñadas (o ignoradas) por las aplicaciones de usuario. La diferencia más notable entre los modelos de TCP/IP y OSI es el nivel de Aplicación, en TCP/IP se integran algunos niveles del modelo OSI en su nivel de Aplicación. Una interpretación simplificada de la pila TCP/IP se muestra debajo:

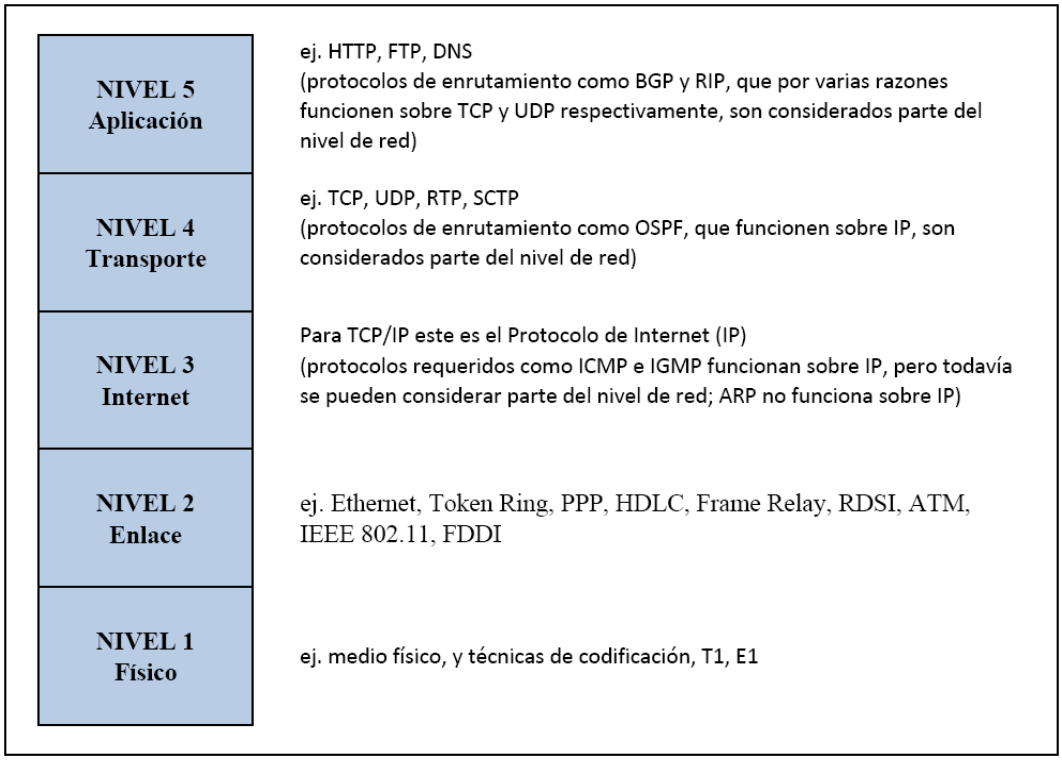


Figura. 1.12. Modelo TCP/IP

El nivel Físico

El nivel físico describe las características físicas de la comunicación, como las convenciones sobre la naturaleza del medio usado para la comunicación (como las comunicaciones por cable, fibra óptica o radio), y todo lo relativo a los detalles como los conectores, código de canales y modulación, potencias de señal, longitudes de onda, sincronización y temporización y distancias máximas..

El nivel de Enlace de datos

El nivel de enlace de datos especifica cómo son transportados los paquetes sobre el nivel físico, incluyendo los delimitadores (patrones de bits concretos que marcan el comienzo y el fin de cada trama). Ethernet, por ejemplo, incluye campos en la cabecera de la trama que especifican que máquina o máquinas de la red son las destinatarias de la trama. Ejemplos de protocolos de nivel de enlace de datos son Ethernet, Wireless Ethernet, SLIP, Token Ring y ATM.

PPP es un poco más complejo y originalmente fue diseñado como un protocolo separado que funcionaba sobre otro nivel de enlace, HDLC/SDLC.

Este nivel es a veces subdividido en Control de enlace lógico (*Logical Link Control*) y Control de acceso al medio (Media Access Control).

El nivel de Internet

Como fue definido originalmente, el nivel de red soluciona el problema de conseguir transportar paquetes a través de una red sencilla. Ejemplos de protocolos son X.25 y Host/IMP Protocol de ARPANET.

Con la llegada del concepto de Internet, nuevas funcionalidades fueron añadidas a este nivel, basadas en el intercambio de datos entre una red origen y una red destino. Generalmente esto incluye un enrutamiento de paquetes a través de una red de redes, conocida como Internet.

En la familia de protocolos de Internet, IP realiza las tareas básicas para conseguir transportar datos desde un origen a un destino. IP puede pasar los datos a una serie de protocolos superiores; cada uno de esos protocolos es identificado con un único "Número de protocolo IP". ICMP e IGMP son los protocolos 1 y 2, respectivamente.

Algunos de los protocolos por encima de IP como ICMP (usado para transmitir información de diagnóstico sobre transmisiones IP) e IGMP (usado para dirigir tráfico *multicast*) van en niveles superiores a IP pero realizan funciones del nivel de red e ilustran una incompatibilidad entre los modelos de Internet y OSI. Todos los protocolos de enrutamiento, como BGP, OSPF, y RIP son realmente también parte del nivel de red, aunque ellos parecen pertenecer a niveles más altos en la pila.

El nivel de Transporte

Los protocolos del nivel de transporte pueden solucionar problemas como la fiabilidad ("¿alcanzan los datos su destino?") y la seguridad de que los datos llegan en el orden correcto. En el conjunto de protocolos TCP/IP, los protocolos de transporte también determinan a qué aplicación van destinados los datos.

Los protocolos de enrutamiento dinámico que técnicamente encajan en el conjunto de protocolos TCP/IP (ya que funcionan sobre IP) son generalmente considerados parte del nivel de red; un ejemplo es OSPF (protocolo IP número 89).

TCP (protocolo IP número 6) es un mecanismo de transporte fiable y orientado a conexión, que proporciona un flujo fiable de bytes, que asegura que los datos llegan completos, sin daños y en orden. TCP realiza continuamente medidas sobre el estado de la red para evitar sobrecargarla con demasiado tráfico. Además, TCP trata de enviar todos los datos correctamente en la secuencia especificada. Esta es una de las principales diferencias con UDP, y puede convertirse en una desventaja en flujos en tiempo real (muy sensibles a la variación del retardo) o aplicaciones de enrutamiento con porcentajes altos de pérdida en el nivel de internet.

Más reciente es SCTP, también un mecanismo fiable y orientado a conexión. Está relacionado con la orientación a byte, y proporciona múltiples sub-flujos multiplexados sobre la misma conexión. También proporciona soporte de *multihoming*, donde una conexión puede ser representada por múltiples direcciones IP (representando múltiples interfaces físicas), así si hay una falla la conexión no se interrumpe. Fue desarrollado inicialmente para aplicaciones telefónicas (para transportar SS7 sobre IP), pero también fue usado para otras aplicaciones.

RTP es un protocolo de datagramas que ha sido diseñado para datos en tiempo real como el *streaming* de audio y video que se monta sobre UDP.

El nivel de Aplicación

El nivel de aplicación es el nivel que los programas más comunes utilizan para comunicarse a través de una red con otros programas. Los procesos que acontecen en este nivel son aplicaciones específicas que pasan los datos al nivel de aplicación en el formato que internamente use el programa y es codificado de acuerdo con un protocolo estándar.

Algunos programas específicos se considera que se ejecutan en este nivel. Proporcionan servicios que directamente trabajan con las aplicaciones de usuario. Estos programas y sus correspondientes protocolos incluyen a HTTP (*HyperText Transfer Protocol*), FTP (Transferencia de archivos), SMTP (correo electrónico), SSH (*login* remoto seguro), DNS (Resolución de nombres de dominio) y a muchos otros.

Una vez que los datos de la aplicación han sido codificados en un protocolo estándar del nivel de aplicación son pasados hacia abajo al siguiente nivel de la pila de protocolos TCP/IP.

En el nivel de transporte, las aplicaciones normalmente hacen uso de TCP y UDP, y son habitualmente asociados a un número de puerto bien conocido (*well-known port*). Los puertos fueron asignados originalmente por la IANA.

1.3.2 EL PROTOCOLO IP [4]

Los datagramas IP están formados por palabras de 32 bits, distribuidos en una cabecera y un campo de datos.

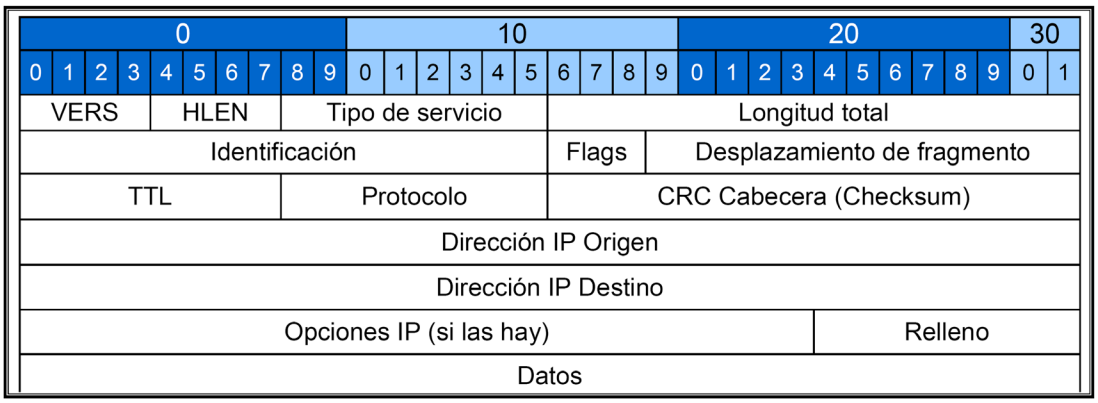


Figura. 1.13. Datagrama IP

Campos del Datagrama IP

a. Versión (VERS): Campo de 4 bits, indica la versión del protocolo IP que se utilizó para crear el datagrama.

b. Cabecera (HLEN): Campo de 4 bits, indica la longitud de la cabecera expresada en múltiplos de 32 bits.

c. Tipo de Servicio (*Type Of Service*): Los 8 bits de este campo se dividen a su vez en:

- Prioridad (3 bits): Un valor de 0 indica baja prioridad y un valor de 7 prioridad máxima.

- Los siguientes cuatro bits indican cómo se prefiere que se transmita el mensaje. Y el bit restante no tiene uso, y queda reservado.

-Bit D (*Delay*): Solicita retardos cortos (enviar rápido).

- Bit T (*Throughput*): Solicita un alto rendimiento (enviar mucho en el menor tiempo posible).

- Bit R (*Reliability*): Solicita que se minimice la probabilidad de que el datagrama se pierda o resulte dañado (enviar bien).

- Bit C (*Cost*): Solicita que el tratamiento que debe recibir el paquete debe ser de mínimo costo.

Tabla. 1.2. Clases de Servicio ToS

Bits (0-2) del byte ToS	Precedencia IP	Bits (3-6) del byte ToS	Tipo de Servicio
111	Control de red	0000	Todo Normal
110	Encaminamiento	1000	Minimizar Retardo
101	Crítico	0100	Maximizar Troughput
100	Muy Urgente	0010	Maximizar Fiabilidad
011	Urgente	0001	Minimizar costes
101	Inmediato		
001	Prioridad		
000	Normal		

d. Longitud Total: Campo de 16 bits, indica la longitud total del datagrama expresada en bytes. Como el campo tiene 16 bits, la máxima longitud posible de un datagrama será de 65535 bytes.

e. Identificación: Campo de 16 bits, indica el número de secuencia que junto con la dirección origen, dirección destino y el protocolo utilizado. Éste identifica de manera única un datagrama en toda la red. Si se trata de un datagrama fragmentado, llevará la misma identificación que el resto de fragmentos.

f. Banderas o Identificadores: Sólo 2 bits de los 3 bits disponibles están actualmente utilizados.

- Bit DF Datagrama fragmentado: Indica si un datagrama puede ser fragmentado DF=0 y si DF=1 no puede ser fragmentado.

- Bit MF Más fragmentos: Indica que no es el último datagrama si MF=1 y si MF=0 es el último datagrama.

g. Desplazamiento de Fragmentación: Campo de 13 bits, indica el lugar en el cual se insertará el fragmento actual dentro del datagrama.

h. Tiempo de Vida o TTL: Campo de 8 bits, indica el número máximo de segundos que puede estar un datagrama en la red de redes. El máximo valor es 255 segundos. Cada vez que el datagrama atraviesa un *router* se resta 1 a este número. Cuando llegue a 0, el datagrama se descarta y se devuelve un mensaje ICMP de tipo "tiempo excedido".

i. Protocolo: Indica el código numérico oficial de un protocolo en que debe entregarse el paquete a las capas superiores.

Algunos códigos se muestran en la siguiente tabla:

Tabla. 1.3. Códigos Numéricos de Protocolos

PROTOCOLO	CÓDIGO
Reservado	0
ICMP	1
IGMP	2
IP encapsulado	4
TCP	6
UDP	17
OSPF	89

j. Cabecera CRC: Campo de 16 bits, permite detectar errores sólo para la cabecera del datagrama. La verificación de errores de los datos corresponde a las capas superiores.

k. Dirección Origen: Campo de 32 bits, contiene la dirección IP del origen.

l. Dirección Destino: Campo de 32 bits, contiene la dirección IP del destino.

m. Opciones IP: Este campo no es obligatorio y especifica las distintas opciones solicitadas por el usuario que envía los datos (generalmente para pruebas de red y depuración).

n. Relleno: Si las opciones IP (en caso de existir) no ocupan un múltiplo de 32 bits, se completa con bits adicionales hasta alcanzar el siguiente múltiplo de 32 bits.

FRAGMENTACIÓN [4]

El tamaño de un datagrama IP se especifica en un campo de dos bytes en la cabecera, por lo que su valor máximo es de 65535 bytes, pero muy pocos protocolos o tecnologías a nivel de enlace admiten enviar tramas de semejante tamaño. Normalmente el nivel de enlace no fragmenta, por lo que tendrá que ser IP el que adapte el tamaño de los datagramas para que quepan en las tramas del nivel de enlace; por tanto en la práctica el tamaño máximo del datagrama viene determinado por el tamaño máximo de trama característico de la red utilizada. Este tamaño máximo de datagrama se conoce como MTU (*Maximum Transfer Unit*). La tabla 1.4 muestra algunos ejemplos de valores de MTU característicos de las redes más habituales.

Tabla. 1.4. Valor de MTU para los protocolos más comunes a nivel de enlace

Protocolo a nivel de enlace	MTU (bytes)
PPP (valor por defecto)	1500
PPP (bajo retardo)	296
SLIP	1006 (límite original)
X.25	1600 (RFC 1356)
Frame relay	1600 normalmente (depende de la red)
SMDS	9235
Ethernet DIX	1500
Ethernet LLC-SNAP	1492
IEEE 802.4/802.2	8166
Token Ring 16 Mb/s	17940 (token holding time 8 ms)
Token Ring 4 Mb/s	4440 (token holding time 8 ms)
FDDI	4352
Hyperchannel	65535
Classical IP over ATM	9180

Podemos distinguir dos situaciones en las que se produce fragmentación. La primera, que podemos denominar fragmentación en ruta, se produce cuando un datagrama es creado por un host en una red con un valor determinado de MTU y en su camino hacia el host de destino ha de pasar por otra red con una MTU menor. Por ejemplo un datagrama creado en una *Toquen Ring* con MTU de 4440 bytes dirigido a una Ethernet con MTU de 1500 bytes.

En estos casos el *router* que hace la transición a la red de MTU menor ha de fragmentar los datagramas para que no excedan el tamaño de la nueva red.

La segunda, que podemos llamar fragmentación en origen, se produce como consecuencia del diseño de la aplicación. Por ejemplo muchas implementaciones de NFS generan datagramas de 8 kbytes de datos (8212 bytes con la cabecera IP). Un host en una red Ethernet que utilice NFS tendrá que fragmentar cada datagrama en seis fragmentos antes de enviarlo, aun cuando el host de origen y destino se encuentren ambos en el mismo concentrador de Ethernet.

DIRECCIONAMIENTO IPv4 [4]

Cada computador se conecta a la red mediante su correspondiente dirección.

Esta dirección es un número de 32 bits que debe ser único para cada host y enrutador, normalmente suele representarse como cuatro cifras de 8 bits separadas por puntos.

Por lo tanto la combinación es única no existen dos máquinas que tengan la misma dirección IP.

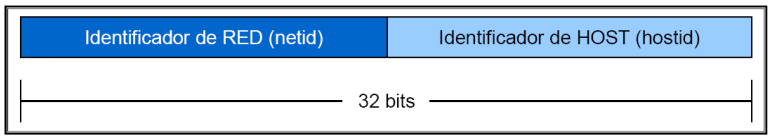


Figura. 1.14. Dirección IPv4

Clases

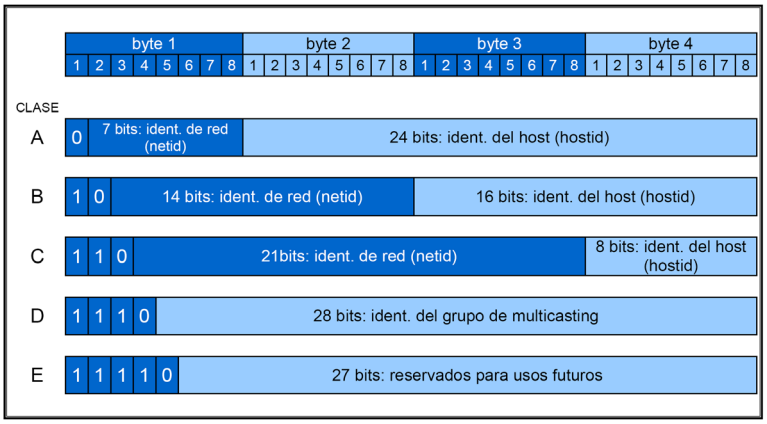


Figura. 1.15. Clases de direcciones

a. Clase A

Estas direcciones utilizan el primer byte para identificar la red, tienen un valor desde 1 hasta 126 (no es posible utilizar los valores 0 y 127 por tener un significado especial), quedando los otros tres bytes disponibles para cada uno de los hosts. Esto significa que podrán existir más de dieciséis millones de computadores en cada una de las redes de esta clase.

Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que sólo puede haber 126 redes de este tamaño.

b. Clase B

En estas direcciones el identificador de la red se obtiene de los dos primeros bytes, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del host permitiendo, por consiguiente, un número máximo de 64516 computadores.

c. Clase C

Estas direcciones utilizan los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 computadores en cada red.

d. Clase D

Las direcciones de Clase D se usan con fines de multidifusión, cuando se quiere una difusión general a más de un dispositivo.

El rango es desde 224.0.0.0 hasta 239.255.235.255.

e. Clase E

Las direcciones de clase E (aunque su utilización será futura) comprenden el rango desde 240.0.0.0 hasta el 247.255.255.255.

La asignación de direcciones válidas de Internet la realizan los NICs (NIC = *Network Information Center*). Al principio había un NIC para toda la Internet pero luego se crearon NICs regionales. Actualmente existen los tres siguientes:

América: www.internic.net

Europa: www.ripe.net

Asia y Pacífico: www.apnic.net

Estos NICs asignan direcciones IP a los proveedores de Internet y a las grandes organizaciones. Los proveedores a su vez asignan direcciones a las organizaciones de menor tamaño y a sus usuarios.

Direcciones Especiales

El número 0 está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red NetID para máquinas que aún no conocen el número de red a la que se encuentran conectadas, en la identificación de host HostID para máquinas que aún no conocen su número de host dentro de la red, o en ambos casos.

El número 127 no puede utilizarse en NetID porque está reservado para funciones de *loopback* 127.0.0.0 es una red clase A, que se reserva para prueba de retorno de lazo y tiene un significado especial que generalmente apunta a la misma máquina o *localhost* que verifica el enlace de comunicaciones.

El número 255 se reserva para el *broadcast*. El *broadcast* es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red.

SUBREDES [7]

Supongamos que una empresa dispone de varias oficinas, cada una con una red local, todas ellas interconectadas entre sí, y que desea unirlas mediante el protocolo TCP/IP; una de dichas oficinas (la principal) dispone además de una conexión a Internet. Supongamos también cada oficina tiene suficiente con 254 direcciones de hosts. En principio sería posible asignar una red clase C diferente para cada oficina, pero esto supone solicitar al

NIC una red para cada oficina que se conecte, y al ser cada una independiente de las demás la gestión se complica; por ejemplo sería preciso anunciar en Internet la ruta para cada nueva red para que la oficina correspondiente fuera accesible. Dado que cada red sería en principio independiente de las demás no habría una forma sencilla de agrupar las redes de la organización.

Hay un mecanismo que permite dividir una red IP en trozos o subredes, de forma que la empresa de nuestro ejemplo podría solicitar una clase B y asignar fragmentos de dicha red a cada oficina a medida que se fueran incorporando a la red. Esto equivale a crear un nivel jerárquico intermedio entre la red y el host, permitiendo así grados variables de agrupación según el nivel en el que nos encontramos. Supongamos que a la empresa de nuestro ejemplo se le asigna una red clase B, la 156.134.0.0; de los 16 bits que en principio corresponden al host podría reservar los primeros 8 para la subred y dejar los 8 siguientes para el host, con lo que dispondrá de 256 subredes de 256 direcciones cada una. Desde fuera la red de la empresa seguirá siendo 156.134.0.0, ya que la estructura de subred no será visible.

Las subredes se añadieron a la Internet en 1982; con ello se consiguió una mayor flexibilidad en el reparto de direcciones dentro de una red.

SUPERREDES: *ROUTING CLASSLESS* (CIDR) [7]

El rápido crecimiento de la Internet está creando varios problemas, el más importante de los cuales es el agotamiento del espacio de direcciones IP. La causa de esto ha sido en parte la excesiva disparidad de tamaños entre las diferentes clases de redes. Hace ya mucho tiempo que han dejado de asignarse redes clase A, debido a su escaso número y tamaño excesivo. Las organizaciones tenían pues que elegir entre solicitar una clase B o una clase C. En muchos casos una clase B era excesiva, pero una C resultaba insuficiente, por lo que la mayoría de las organizaciones optaban por solicitar una clase B, aunque a menudo no necesitaban tantas direcciones. A la vista del rápido agotamiento de redes clase B debido a este motivo se pensó en crear grupos de clases C, de forma que las organizaciones pudieran optar por niveles intermedios entre las redes B y C, más adecuados a sus necesidades; por ejemplo una organización que necesite 2048 direcciones puede hoy en día solicitar un grupo de ocho redes clase C. De esta forma se reduce el problema de escasez de direcciones, pero se crea un problema nuevo: el crecimiento de las tablas de rutas. Antes,

cuando a una organización que se conectaba a Internet se le asignaba una red esto suponía una nueva entrada en las tablas de rutas de Internet, pero al dar grupos de clases C se requiere una entrada diferente para cada red asignada. Esto habría provocado un crecimiento exponencial en las tablas de rutas de los *routers* que forman el '*backbone'*, cuyas capacidades se encuentran ya bastante cerca del límite de la tecnología.

El gran tamaño de las tablas de rutas de Internet se debe también al mecanismo de asignación de direcciones que se ha seguido, que durante mucho tiempo ha sido estrictamente cronológico. Al no haber una correspondencia entre la ubicación geográfica de una organización o el proveedor que la conecta a Internet y su rango de direcciones no es posible resumir o 'sumarizar' las tablas de rutas; la información se ha de incluir enumerando una a una todas las redes existentes. Esto se podría resolver con una organización jerárquica de direcciones de acuerdo con criterios geográficos, como ocurre por ejemplo en el direccionamiento de la red telefónica que identifica a cada país con prefijo, cada región dentro de un país con un subprefijo, y así sucesivamente.

Actualmente hay más de 100.000 redes registradas en la Internet. Además del costo en memoria RAM que supone el mantener tablas extremadamente grandes en los *routers*, los algoritmos de búsqueda se complican y no funcionan adecuadamente con esas tablas, ya que fueron diseñados pensando en tablas con muchas menos entradas. A principios de los 90 el crecimiento de la Internet se estaba produciendo a un ritmo tal que el número de redes conectadas se duplicaba cada 9 meses, mientras que la tecnología sólo permite duplicar la capacidad y potencia de los *routers* cada 18 meses. En esta situación la explosión de las tablas de *routing* se estaba convirtiendo en un problema aún más grave que la escasez de direcciones. Según cálculos hechos por la IETF en 1993 de seguir produciéndose el crecimiento al mismo ritmo en el número de redes y rutas la Internet se habría colapsado hacia 1998.

Los dos problemas antes descritos, desperdicio del espacio de direcciones debido a la rigidez en la asignación de rangos (redes clase B o C) y crecimiento de las tablas de rutas, se resolvieron conjuntamente en 1993 con la adopción de un sistema denominado CIDR (*Classless InterDomain Routing*) descrito en los RFCs 1466, 1518 y 1519 que consiste en dos medidas complementarias.

La primera medida consiste en establecer una jerarquía en la asignación de direcciones. En vez de utilizar un criterio puramente cronológico, que desde el punto de vista geográfico o de topología de la red equivale a una asignación aleatoria, los rangos se asignan por continentes. Inicialmente se realizó la asignación de una parte del espacio de clase C de la siguiente manera:

Multi regional:	192.0.0.0 - 193.255.255.255
Europa:	194.0.0.0 - 195.255.255.255
Otros:	196.0.0.0 - 197.255.255.255
Noteamérica:	198.0.0.0 - 199.255.255.255
Centro y Sudamérica:	200.0.0.0 - 201.255.255.255
Anillo Pacífico:	202.0.0.0 - 203.255.255.255
Otros:	204.0.0.0 - 205.255.255.255
Otros:	206.0.0.0 - 207.255.255.255

Algunos de estos grupos se han ampliado posteriormente con nuevos rangos. A su vez cada proveedor Internet solicita rangos propios al NIC que le corresponde según el continente donde se encuentra. Con esta distribución regional de los números es en principio posible agrupar las entradas en las tablas de rutas; por ejemplo un *router* en Japón podría tener una sola entrada en sus tablas indicando que todos los paquetes dirigidos a las redes 194.0.0.0 hasta 195.255.255.0 se envíen a la interfaz por la cual accede a Europa, evitando así las 131.072 entradas que normalmente harían falta para este rango de direcciones.

Una consecuencia curiosa de la asignación de rangos de direcciones por proveedor es que si una empresa cambia de proveedor normalmente tendrá que 'devolver' al primero sus direcciones, y solicitar direcciones al nuevo proveedor; por supuesto tendrá que modificar la configuración de todas las máquinas que tuviera utilizando direcciones del primero.

Para que la sumarización de rutas (o agrupamiento de redes clase C) sea posible es preciso introducir una ligera modificación en el software de los *routers*, ya que en principio el software no considera el rango 194.0.0.0–195.255.255.255 como una sola red sino como 131.072 redes clase C. Para resolver este problema se ha extendido el concepto

de subred en sentido contrario, es decir la máscara no solo puede crecer hacia la derecha para dividir una red en subredes sino que puede menguar hacia la izquierda para agrupar varias redes en una mayor (de ahí la denominación de 'superredes'). Dicho de otra forma, la parte red de la dirección vendrá especificada por la longitud de la máscara únicamente, no teniendo ya ningún significado la clasificación tradicional en clases A, B y C de acuerdo con el valor de los primeros bits; solo se repita dicho significado en el caso de las clases D (*multicast*) y E (reservado). Dicha supresión de las clases tradicionales es lo que da nombre a esta técnica conocida como enrutamiento entre dominios sin clases o CIDR (*Classless InterDomain Routing*).

La segunda medida adoptada por CIDR es en realidad un complemento de la anterior. Consiste sencillamente en dar a cada organización (bien directamente o a través de su proveedor correspondiente) la posibilidad de solicitar rangos de direcciones ajustado a sus necesidades previstas, dándole siempre un rango contiguo y que tenga una máscara de red común; por ejemplo un rango de 2048 direcciones se daría asignando los primeros 21 bits de la dirección y podría estar formado por ejemplo por el rango que va del 194.0.8.0 al 194.0.15.255.

DIRECCIONAMIENTO IP V6 [8]

IPv6 es la versión 6 del Protocolo de Internet (*Internet Protocol*), un estándar en desarrollo del nivel de red encargado de dirigir y encaminar los paquetes a través de una red.

IPv6 está destinado a sustituir al estándar IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. Pero el nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionando a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes. Al día de hoy se calcula que las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas.

IPv4 soporta 4.294.967.296 (2^{32}) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos para cada coche, teléfono, PDA, etcétera; mientras que IPv6 soporta:

340.282.366.920.938.463.463.374.607.431.768.211.456 (2^{128} ó 340 sextillones) direcciones cerca de $3{,}4 \times 10^{20}$ (340 trillones) direcciones por cada pulgada cuadrada ($6{,}7 \times 10^{17}$ ó 670 mil billones direcciones/mm^2) de la superficie de La Tierra.

Adoptado por el IETF en 1994 (cuando era llamado "IP *Next Generation*" o IPng), IPv6 cuenta con un pequeño porcentaje de las direcciones públicas de Internet, que todavía están dominadas por IPv4. La adopción de IPv6 ha sido frenada por la traducción de direcciones de red (NAT), que alivia parcialmente el problema de la falta de direcciones IP. Pero NAT hace difícil o imposible el uso de algunas aplicaciones P2P, como son la voz sobre IP (VoIP) y juegos multiusuario. Además, NAT rompe con la idea originaria de Internet donde todos pueden conectarse con todos. Actualmente, el gran catalizador de IPv6 es la capacidad de ofrecer nuevos servicios, como la movilidad, Calidad de Servicio (QoS), privacidad, etc. El gobierno de los Estados Unidos ha ordenado el despliegue de IPv6 por todas sus agencias federales para el año 2008.

Se espera que IPv4 se siga soportando hasta por lo menos el 2011, dado que hay muchos dispositivos heredados que no se migrarán a IPv6 nunca y que seguirán siendo utilizados por mucho tiempo.

IPv6 es la segunda versión del Protocolo de Internet que se ha adoptado para uso general. También hubo un IPv5, pero no fue un sucesor de IPv4; mejor dicho, fue un protocolo experimental orientado al flujo de *streaming* que intentaba soportar voz, video y audio.

El cambio más drástico de IPv4 a IPv6 es la longitud de las direcciones de red. Las direcciones IPv6, definidas en el RFC 2373 y RFC 2374, son de 128 bits; esto corresponde a 32 dígitos hexadecimales, que se utilizan normalmente para escribir las direcciones IPv6, como se describe en la siguiente sección.

En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

Notación para las direcciones IPv6

Las direcciones IPv6, de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales.

Por ejemplo,

```
2001:0db8:85a3:08d3:1319:8a2e:0370:7334
```

Es una dirección IPv6 válida.

Si un grupo de cuatro dígitos es nulo (es decir, toma el valor "0000"), puede ser comprimido. Por ejemplo,

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

Es la misma dirección que

```
2001:0db8:85a3::1319:8a2e:0370:7344
```

1.3.3 PROTOCOLOS DE CONTROL [7]

Antes hemos dicho que todo el tráfico de Internet está formado por datagramas IP. Normalmente los datagramas transportan TPDUs (*Transport Protocol Data Unit*) de TCP o UDP, que son los dos protocolos de transporte utilizados en Internet. Todas las aplicaciones de interés para el usuario de Internet (correo electrónico, transferencia de ficheros, videoconferencia, etc.) generan tráfico TCP o UDP. Sin embargo cuando vimos en la estructura de la cabecera de un datagrama el valor del campo protocolo observamos que existen muchos posibles significados del contenido de un datagrama IP, aparte de los 'normales' que serían TCP y UDP. Algunos de los datos que pueden transportarse en datagramas IP son mensajes de protocolos de control de Internet como los que veremos en este apartado. Los protocolos de control son una parte necesaria para el correcto funcionamiento de la red. Aquí describiremos los más utilizados que son ICMP, ARP, RARP, BOOTP y DHCP.

a) ICMP (Internet Control Message Protocol)

En el funcionamiento normal de una red se dan a veces situaciones extraordinarias que requieren enviar avisos especiales. Por ejemplo, si un datagrama con el bit DF (*Don't Fragment*) puesto a 1 no puede pasar por una determinada red el *router* donde se produce el problema debe devolver un mensaje al host emisor indicándole lo sucedido. El mecanismo para reportar todos estos incidentes en Internet es el protocolo conocido como ICMP, que veremos a continuación. Aquí solo describiremos brevemente los más importantes, para una descripción detallada de todos ellos se puede consultar el RFC 792.

Conviene recordar que los mensajes ICMP viajan por la red como datagramas IP (con el valor 1 en el campo 'protocolo'), sujetos en los *routers* a las mismas reglas que cualquier otro datagrama. Los mensajes ICMP son generados por el host o router que detecta el problema o situación extraordinaria y dirigidos al host o *router* que aparece en el campo dirección origen del datagrama que causó el problema. Para facilitar la identificación del datagrama por parte del host emisor la mayoría de los mensajes ICMP incluyen, además del código de error correspondiente, la cabecera y los primeros ocho bytes de datos del datagrama original.

A continuación describiremos los mensajes ICMP más importantes:

DESTINATION UNREACHABLE. Este mensaje se produce cuando no se puede entregar el datagrama en su destino por diversas situaciones, entre las que destacaremos a modo de ejemplo las dos siguientes: a) cuando un *router* se encuentra con un datagrama que tiene puesto a 1 el bit DF (*Don't Fragment*) y que no cabe en la MTU de la red por la que ha de enviarlo, y b) cuando un *router* no encuentra en sus tablas ninguna ruta por la que pueda llegar a la dirección para la que va dirigido un datagrama. Obsérvese que cuando un *router* tiene configurada ruta por defecto nunca enviará mensajes ICMP *Destination Unreachable* por este segundo motivo.

SOURCE QUENCH. Este mensaje se creó para permitir a los *routers* solicitar una reducción en el tráfico generado por los hosts en caso de congestión, por lo que actuaban como paquetes de asfixia. En la práctica se ha visto que el uso de este tipo de mensajes agrava los problemas en caso de congestión, por lo que la recomendación actual es que los *routers* no deben generar paquetes SOURCE QUENCH en ningún caso.

ECHO REQUEST y ECHO REPLY: se usan para detectar si un destino determinado está operativo. Al recibir el mensaje el destino debe responder con el comando ICMP ECHO REPLY. El comando ping, muy utilizado en Internet para pruebas de accesibilidad, utiliza este comando. En la mayoría de las implementaciones de ping es posible especificar el tamaño del datagrama a enviar, y también la frecuencia de los envíos, con lo que se puede utilizar para generar un tráfico en la red de forma controlada. El comando ping suministra información del tiempo de ida y vuelta y porcentaje de datagramas perdidos, por lo que permite tener una idea bastante aproximada del estado de la red.

TIME EXCEEDED se envía al emisor cuando un paquete es descartado porque su TTL ha llegado a cero. Esto puede se síntoma de que se ha producido algún bucle en la red, o que el valor del TTL utilizado es demasiado bajo para el diámetro de la red. Hay un programa muy utilizado para diagnóstico de redes, denominado *traceroute*[1], que averigua la ruta a un destino determinado enviando paquetes con TTL de 1, 2, 3, y así sucesivamente. A partir de los mensajes ICMP TIME EXCEEDED recibidos el programa puede deducir la ruta completa hasta el destino especificado. *Traceroute* mide además el tiempo de ida y vuelta en cada caso, y para dar una información estadísticamente más significativa normalmente envía tres paquetes para cada valor de TTL y muestra los tiempos de ida y vuelta de cada uno, dando así información no sólo de la ruta seguida sino de los retardos en cada parte del trayecto.

REDIRECT se utiliza para alertar al host emisor cuando se sospecha que un paquete se está encaminando incorrectamente. Por ejemplo este mensaje lo utilizan los *routers* cuando reciben de un host datagramas que van dirigidos a otro host que se encuentra en la misma LAN.

b) Resolución de direcciones: ARP

Cuando se utilizan líneas punto a punto en una red la interfaz física fija el siguiente nodo al que se dirige el datagrama, ya que para cada enlace existe un único destinatario posible. En cambio cuando se utiliza una red multiacceso (por ejemplo RDSI, ATM o una LAN cualquiera) la tecnología utilizada para enviar los datagramas permite llegar por la misma interfaz física a más de un destinatario. En este caso es necesario algún mecanismo que permita saber a cuál de todos los destinos posibles se dirigen los paquetes. Todas las

[1] Este programa está disponible en UNIX con su propio nombre y en Windows con el nombre *tracert*.

redes multiacceso disponen de un sistema de direccionamiento propio, por ejemplo en una RDSI las direcciones serían los números de teléfono RDSI con los que queremos conectar, en una LAN serían las direcciones MAC de las estaciones, etc. En todos estos casos es el nivel de red el encargado de realizar la correspondencia entre la dirección en la tecnología multiacceso correspondiente y la dirección de red, correspondencia que se conoce como resolución de direcciones.

Existen múltiples mecanismos posibles para realizar la resolución de direcciones. De ellos comentaremos aquí algunos de los más utilizados.

Tabla estática mantenida manualmente en cada nodo. En este caso se tiene en cada nodo de la red multiacceso la tabla completa de equivalencia de direcciones. Esta técnica se utilizaba en las primeras redes locales y se utiliza actualmente en RDSI, X.25, Frame Relay y también en ATM en algunos casos. El principal problema que tiene es la necesidad de actualizar las tablas en todos los nodos de la red cada vez que se produce alguna modificación en la tabla de direcciones.

Tabla dinámica mantenida de forma automática en un servidor de la red conocido por todos. Cuando un nodo quiere enviar un mensaje a un destino determinado indica al servidor la dirección de red que busca y éste le devuelve la dirección de la red multiacceso correspondiente.

Establecer un mecanismo trivial por el que se pueda deducir la dirección de la red multiacceso a partir de la dirección de red. De esta forma cualquier nodo puede derivar la dirección de la red multiacceso a partir de la dirección de red. Este mecanismo se emplea por ejemplo en DECNET que construye la dirección MAC añadiendo a la dirección de red un prefijo determinado y conocido por todos los nodos. Para que esto sea posible no se utiliza la dirección global grabada en la tarjeta de red y se recurre al uso de direcciones MAC locales (las fijadas por software, que tienen a 1 el segundo bit) para poder imponer la dirección MAC a partir de la dirección de red. Este mecanismo no puede ser utilizado simultáneamente por más de un protocolo de red ya que se produciría conflicto entre las direcciones MAC requeridas por los diversos protocolos.

Utilizar un mensaje *broadcast* para lanzar a la red una pregunta solicitando respuesta del nodo en la red multiacceso que posee la dirección de red buscada. Esta técnica da

máxima flexibilidad ya que los equipos no necesitan registrarse y no hay un servidor centralizado del que dependa el funcionamiento de la red. Sin embargo solo es factible en redes de naturaleza *broadcast*, como las redes locales. El principal inconveniente de esta solución es el uso de paquetes *broadcast* que produce una degradación del rendimiento de toda la red[2]. Esta técnica es la utilizada en IP sobre redes locales de todo tipo. De modo que cada ordenador de la red local mantiene en memoria una tabla denominada ARP cache con las parejas de direcciones MAC-IP utilizadas recientemente.

c) Resolución inversa de direcciones

A veces se plantea el problema inverso a ARP, es decir hallar la dirección IP a partir de una determinada dirección LAN. Por ejemplo cuando se arranca una estación de trabajo '*diskless*', es decir sin disco, ésta ha de cargar su sistema operativo desde otro ordenador normalmente situado en la misma red local, pero desconoce todo lo relativo a su configuración de red, incluida la dirección IP; lo único que la estación conoce en principio es su dirección MAC, que se encuentra escrita en su tarjeta de red local.

RARP.- Para estas situaciones se inventó RARP (*Reverse Address Resolution Protocol*), que funciona de la siguiente manera: la estación *diskless* envía un mensaje *broadcast* en el que indica su dirección MAC y solicita que alguien le informe de cuál es la dirección IP que le corresponde. En la red habrá un servidor RARP encargado de atender este tipo de peticiones que consultará sus tablas y devolverá la dirección IP correspondiente.

RARP utiliza el mismo formato de mensaje que ARP. La única diferencia es que utiliza los códigos de operación 3 y 4 para la pregunta y respuesta RARP, respectivamente. Además en vez de utilizar el *Ethertype* x0806 emplea el x8035; esto permite a los hosts que no soportan el protocolo RARP descartar estos mensajes rápidamente, sin tener que analizar su contenido.

BOOTP.- RARP aporta funcionalidades interesantes pero tiene algunas limitaciones importantes. Como la consulta se realiza mediante un mensaje *broadcast* el servidor RARP ha de estar en la misma LAN que el cliente; por tanto es necesario prever un servidor

[2] El tráfico broadcast es altamente perjudicial para el rendimiento por dos razones: no es aislado por los conmutadores y además tiene que ser recibido y procesado por todas las estaciones de la red, ya que en principio les incumbe. En una red de gran tamaño con mucho tráfico broadcast el consumo en ciclos de CPU debido a este motivo puede llegar a ser considerable.

RARP en cada LAN, ya que los mensajes broadcast a nivel MAC no atraviesan los *routers*. Otra limitación es el hecho de que el protocolo RARP solo prevé el envío de la dirección IP, cuando sería interesante aprovechar el mensaje para informar al cliente de todo el conjunto de parámetros relacionados con la configuración de la red (la máscara, el router por defecto, etc.). Para superar estas limitaciones de *RARP* se inventó el protocolo BOOTP (BOOTstrap Protocol).

DHCP.- Tanto RARP como BOOTP requieren una asignación estática biunívoca entre direcciones MAC y direcciones IP; hacen falta tantas direcciones IP como ordenadores vayan a utilizar el protocolo TCP/IP. Existen situaciones en las que esto no es conveniente, por ejemplo:

Una empresa con 500 ordenadores quiere conectarse a la Internet, de forma que cualquiera de ellos pueda salir al exterior; para esto dispone de una clase C; se calcula que nunca habrá más de 200 ordenadores simultáneamente conectados a la Internet, por lo que en principio una red clase C sería suficiente, pero la necesidad de asignar una dirección IP a cada ordenador requiere disponer de 500 direcciones IP si se quiere ofrecer conectividad a todos ellos.

En una universidad se dispone de una sala para la conexión a Internet de los ordenadores portátiles de los alumnos. No se conocen las direcciones MAC de los ordenadores que se utilizarán ni cuantos serán, lo único que se sabe es que no habrá en ningún momento más de 50 conectados simultáneamente ya que esta es la capacidad de la sala.

Evidentemente en estas situaciones es necesario un mecanismo más flexible de asignación de direcciones IP que el ofrecido por BOOTP.

Para resolver estos problemas el IETF diseñó en 1993 el protocolo DHCP (Dynamic Host Configuration Protocol), que es similar a BOOTP pero es más versátil en los mecanismos de asignación de direcciones IP. En DHCP los clientes pueden recibir sus direcciones por uno de los tres mecanismos siguientes:

Asignación indefinida y estática. En este caso la dirección es fijada por el administrador. Este equivale a BOOTP.

Asignación automática. La asignación es también estática pero la elección de la dirección IP correspondiente es tomada por el servidor DHCP la primera vez que el equipo le solicita su dirección.

Asignación dinámica. En este caso el cliente recibe la dirección IP del servidor durante un tiempo limitado. Pasado ese tiempo el cliente debe renovar su solicitud o de lo contrario la concesión expirará. De esta forma una misma dirección puede ser reutilizada por diferentes máquinas en momentos diferentes. Esta modalidad es también conocida como 'alquiler de direcciones'.

La mayor flexibilidad de DHCP le ha convertido en el protocolo preferido para la configuración remota de ordenadores en redes locales. Con DHCP se mejora notablemente la seguridad y fiabilidad de una red; también se simplifican las labores de administración de la misma.

Un inconveniente de la asignación dinámica de direcciones es que si se desea rastrear un problema y, como es lo normal, sólo se dispone de la dirección IP resulta más difícil (a veces imposible) averiguar que ordenador o usuario ha sido el causante del problema. Otro problema es la asociación de direcciones y nombres en el DNS; con la asignación dinámica diferentes máquinas pueden recibir el mismo nombre en diferentes momentos.

RARP se describe en el RFC 903. BOOTP se describe en los RFC 951, 1497 y 1542. DHCP se describe en el RFC 1541.

1.3.4 PROTOCOLOS DE ENRUTAMIENTO [7]

La Internet está formada por multitud de redes interconectadas, pertenecientes a diversas empresas y organizaciones. Todas estas redes interconectadas comparten a nivel de red el protocolo IP. Al margen de esta interoperabilidad existen dos aspectos fundamentales en los que las redes pueden diferir entre si:

El protocolo de routing utilizado: existen como veremos multitud de protocolos de routing diferentes, unos basados en el algoritmo del vector distancia y otros en el del estado del enlace; incluso utilizando el mismo algoritmo se pueden emplean protocolos diferentes. Aun utilizando el mismo algoritmo y protocolo de routing dos proveedores

diferentes normalmente no querrán que sus routers intercambien entre sí la misma información de routing que intercambian internamente.

La política de intercambio de tráfico: un proveedor puede tener acuerdos bilaterales o multilaterales para intercambiar tráfico con otros, pero normalmente no estará dispuesto a ser utilizado como vía de tránsito para el tráfico entre dos proveedores si esto no está expresamente recogido en los acuerdos, aun cuando desde el punto de vista de topología de la red pueda ser ese el camino más corto entre ambas.

SISTEMA AUTÓNOMO

Entendemos por Sistema Autónomo (AS, *Autonomous System*) la subred que es administrada o gestionada por una autoridad común, que tiene un protocolo de *routing* homogéneo mediante el cual intercambia información en toda la subred y que posee una política común para el intercambio de tráfico con otras redes o sistemas autónomos.

Normalmente cada ISP (*Internet Service Provider*) constituye su propio sistema autónomo. Los sistemas autónomos reciben números de dos bytes que se registran en el IANA de forma análoga a las direcciones IP.

De la misma forma que existen unos rangos de direcciones IP reservados para redes privadas existe un rango de números de sistemas autónomos reservados para sistemas autónomos privados, que son los que van del 64512 al 65535.

Así pues, como mínimo en la Internet se dan dos niveles jerárquicos de routing, el que se realiza dentro de un sistema autónomo (AS) y el que se efectúa entre sistemas autónomos. Al primero lo denominamos routing interno, o routing en el interior de la pasarela (pasarela es una antigua denominación de router). Al routing entre sistemas autónomos lo denominamos routing externo, o también routing exterior a la pasarela. Dado que los requerimientos en uno y otro caso son muy diferentes, se utilizan protocolos de routing distintos. Los protocolos de routing dentro del sistema autónomo se denominan IGP (Interior Gateway Protocol), mientras que los utilizados entre sistemas autónomos se llaman EGP (Exterior Gateway Protocol).

PROTOCOLOS DE ROUTING INTERNO (IGP)

En la Internet se usan actualmente diversos protocolos de routing interno. Estos pueden agruparse en protocolos de vector distancia entre los que destacamos RIP, RIPv2, IGRP y EIGRP, y protocolos del estado del enlace de los que los más importantes son IS-IS y OSPF. Los describiremos brevemente, centrándonos en el caso de OSPF que es el más importante por su mayor uso y sofisticación.

a) RIP y RIPv2

RIP (Routing Information Protocol) es uno de los protocolos de routing más antiguos y deriva del protocolo de routing de XNS (Xerox Network Systems); RIP sufre los problemas típicos de los algoritmos basados en el vector distancia, tales como la cuenta a infinito, etc. Además RIP arrastra otros problemas que son consecuencia de ser un protocolo de routing muy antiguo, como son:

- Métricas basadas exclusivamente en número de saltos
- No soporta subredes ni máscaras de tamaño variable (si en RIPv2).
- No permite usar múltiples rutas simultáneamente.

Se genera una gran cantidad de información de routing que se intercambia cada 30 segundos. Con el paso del tiempo los routers tienden a sincronizarse de forma que todos acaban enviando los paquetes a la vez; esto provoca congestión y parones en la red durante el momento en que se intercambia la información de routing.

Algunos de estos problemas aumentan a medida que crece el tamaño de los sistemas autónomos, por lo que en la práctica no es aconsejable usar RIP en ninguna red que tenga mas de 5 a 10 routers. A pesar de todos sus inconvenientes RIP aún se utiliza en algunas partes de Internet. Existen dos versiones de RIP: la versión 1, que se definió en el RFC 1058 y se publicó en 1983 (aunque se empezó a utilizar mucho antes) se ha declarado histórica, es decir su uso está desaconsejado. En vista de la popularidad de RIP y de los muchos problemas que presentaba en 1993 se publicó RIP versión 2, que intentaba resolver al menos algunos de ellos (RFC 1388).

b) IGRP y EIGRP

A pesar de sus inconvenientes, el routing por vector distancia tiene algunos serios partidarios. Quizá el más importante sea la empresa Cisco, actualmente el principal fabricante de routers en el mundo. En 1988, cuando el único protocolo de routing estandarizado y ampliamente utilizado era RIP, Cisco optó por crear un protocolo de routing propio denominado IGRP (Interior Gateway Routing Protocol) para resolver algunos de los problemas que presentaba RIP. IGRP está basado también en el vector distancia. Cisco siguió (y sigue) apostando por los protocolos de routing basados en el vector distancia ya que en 1993 produjo un nuevo protocolo denominado EIGRP (Enhanced IGRP) que introducía mejoras importantes respecto a IGRP, pero basado también en el vector distancia. Hay que resaltar que tanto IGRP como EIGRP son protocolos propietarios, y no hay implementaciones de ellos para equipos de otros fabricantes, por lo que el uso de estos protocolos requiere que todos los routers del sistema autónomo correspondiente sean de Cisco. Los routers Cisco también pueden funcionar con protocolos estándar, tales como RIP OSPF e IS-IS.

c) OSPF

La respuesta del IETF a los problemas de RIP fue OSPF (Open Shortest Path First), protocolo de routing basado en el estado del enlace. OSPF fue desarrollado entre 1988 y 1990, y en 1991 ya se había producido OSPF versión 2. OSPF esta basado en IS-IS y muchos de los conceptos que maneja son comunes a ambos protocolos. Es un estándar Internet y es el protocolo actualmente recomendado por el IAB para sustituir a RIP. Su complejidad es notablemente superior, mientras que la descripción de RIP ocupa menos de 20 páginas la especificación de OSPF emplea más de 200. La especificación vigente de OSPF está en el RFC 2328.

Entre las características más notables de OSPF podemos destacar las siguientes:

- Es un algoritmo dinámico autoadaptativo, que reacciona a los cambios de manera automática y rápida.

- Soporta una diversidad de parámetros para el cálculo de la métrica, tales como capacidad (ancho de banda), retardo, etc.

- Realiza balance de carga si existe más de una ruta hacia un destino dado.

- Establece mecanismos de validación de los mensajes de routing, para evitar que un usuario malintencionado envíe mensajes engañosos a un router.

- Soporta rutas de red, de subred y de host.

- Se contempla la circunstancia en la que dos routers se comuniquen directamente entre sí sin que haya una línea directa entre ellos, por ejemplo cuando están conectados a través de un túnel.

OSPF permite dos niveles de jerarquía creando lo que se denominan áreas dentro de un sistema autónomo. De esta forma un router sólo necesita conocer la topología e información de routing correspondiente a su área, con lo que la cantidad de información de routing se reduce. En redes complejas esta es una característica muy valiosa.

Los algoritmos de routing por el estado del enlace se aplican dentro de cada área. En todo Sistema Autónomo (AS) hay al menos un área, el área 0 denominada backbone. Un router puede pertenecer simultáneamente a dos o mas áreas, en cuyo caso debe disponer de la información de routing y ejecutar los cálculos correspondientes a todas ellas. Al menos un router de cada área debe estar además en el backbone, para conectar dicha área con el resto del Sistema Autónomo. Dos áreas sólo pueden hablar entre sí a través del backbone.

En OSPF se contemplan cuatro clases de routers:

- Routers backbone; son los que se encuentran en el área 0 ó backbone.

- Routers internos; los que pertenecen únicamente a un área.

- Routers frontera de área; son los que están en mas de un área, y por tanto las interconectan (una de las áreas interconectadas siempre es necesariamente el backbone).

- Routers frontera de Sistema Autónomo; son los que intercambian tráfico con routers de otros Sistemas Autónomos. Estos routers pueden estar en el backbone o en cualquier otra área.

d) IS-IS

El protocolo de routing IS-IS (Intermediate System-Intermediate System) está basado en el algoritmo del estado del enlace; además IS-IS permite hacer routing integrado, es decir calcular las rutas una vez y aplicarlas para todos los protocolos utilizados, permitiendo así auténtico routing. Soporta hasta ocho niveles jerárquicos, para reducir así la cantidad de información de routing intercambiada. IS-IS fue diseñado para el protocolo DECNET (de Digital) y adoptado después por ISO como protocolo de routing para el protocolo de red CLNP[3]. Una variante de IS-IS se utiliza en Netware de Novell.

IS-IS también se utiliza en algunas zonas de la Internet. El protocolo IS-IS se especifica en el RFC 1142.

IS-IS no es un estándar Internet, aunque se especifica en el RFC 1142. Actualmente es el protocolo utilizado en las redes grandes, por ejemplo la gran mayoría de las redes de los ISPs utilizan IS-IS en lugar de OSPF.

PROTOCOLOS DE ROUTING EXTERNO (EGP)

Todos los protocolos de routing hasta ahora descritos se emplean dentro de sistemas autónomos. Normalmente un sistema autónomo corresponde a una subred que tiene una entidad común desde el punto de vista administrativo y de gestión, puede ser por ejemplo la red de una gran empresa, de un proveedor de servicios Internet o la red académca de un país. En estos casos se supone que el protocolo de routing ha de buscar la ruta óptima atendiendo únicamente al criterio de minimizar la 'distancia' medida en términos de la métrica elegida para la red.

La selección de rutas para el tráfico entre sistemas autónomos plantea un problema diferente, ya que la cuestión no se reduce a la selección de la ruta óptima sino que se debe atender a criterios externos que obedezcan a razones de tipo político, económico, administrativo, etc. (recordemos que se trata de decidir el routing entre redes que pertenecen a organizaciones diferentes). Un ejemplo típico de este tipo de restricciones es

[3] CLNP (ConnectionLess Network Protocol) es un protocolo desarrollado por ISO a imagen y semejanza de IP. Su mayor diferencia estriba en el uso de direcciones OSI de 20 bytes en vez de lasde 4 bytes de IP.

el caso en que la ruta óptima entre dos sistemas autónomos, X e Y, pasa por un tercero Z que no desea que su red sea utilizada como vía de tránsito. Para dar cabida a la utilización de criterios externos en el cálculo de las rutas entre sistemas autónomos se utilizan en este caso otro tipo de protocolos de routing, denominados protocolos de routing externo.

Hasta 1990 se utilizaba como protocolo de routing externo en la Internet el denominado EGP (Exterior Gateway Protocol), diseñado entre 1982 y 1984. Como era de esperar EGP no fue capaz de soportar la enorme evolución que sufrió Internet y como ya era habitual el IETF desarrolló un nuevo protocolo de routing externo, denominado BGP (Border Gateway Protocol). La primera especificación de BGP apareció en 1989; desde entonces el IETF ha producido cuatro versiones de BGP; las especificaciones actualmente vigentes de BGP-4 se encuentran en el RFC 1771.

Los routers que utilizan BGP (pertenecientes a diferentes ASes) forman entre ellos una red e intercambian información de routing para calcular las rutas óptimas; se utiliza el vector distancia, pero para evitar el problema de la cuenta a infinito la información intercambiada incluye, además de los routers accesibles y el costo, la ruta completa utilizada para llegar a cada posible destino; de esta forma el router que recibe la información puede descartar las rutas que pasan por él mismo que son las que podrían dar lugar al problema de la cuenta a infinito. La especificación de la ruta completa permite también a los routers revisar si dicha ruta es conforme con las políticas que se hayan especificado en cuanto a tránsito por otros sistemas autónomos.

BGP permite introducir manualmente restricciones o reglas de tipo 'político'; éstas se traducen en que cualquier ruta que viola la regla recibe automáticamente una distancia de infinito.

Para simplificar la gestión de los Sistemas Autónomos se crean Confederaciones de Sistemas Autónomos; una confederación es vista como un único Sistema Autónomo desde el exterior. Esto equivale a introducir en el protocolo de routing externo dos niveles jerárquicos, con lo que se reduce la información de routing de forma análoga a lo que ocurría con las áreas de OSPF dentro de un Sistema Autónomo.

1.3.5 PROTOCOLOS DE TRANSPORTE

a) TCP (TRANSMISSION CONTROL PROTOCOL) [9]

Es uno de los protocolos fundamentales en Internet. Muchos programas dentro de una red de datos compuesta por ordenadores pueden usar TCP para crear conexiones entre ellos a través de las cuales enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP y SSH.

Funciones de TCP

En la pila de protocolos TCP/IP, TCP es la capa intermedia entre el protocolo de internet (IP) y la aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe: libre de errores, sin pérdidas y con seguridad.

Formato de los Segmentos TCP

En el nivel de transporte, los paquetes de bits que constituyen las unidades de datos de protocolo o PDU (protocol data unit) se llaman segmentos. El formato de los segmentos TCP se muestra en el siguiente esquema:

+	Bits 0 - 3	4 - 7	8 - 15	16 - 31
0	Puerto Origen			Puerto Destino
32	Número de Secuencia			
64	Número de Acuse de Recibo (ACK)			
96	longitud cabecera TCP	Reservado	Flags	Ventana
128	Suma de Verificación (Checksum)			Puntero Urgente
160	Opciones + Relleno (opcional)			
224	Datos			

Figura. 1.16. Formato de los segmentos de TCP

Las aplicaciones envían flujos de bytes a la capa TCP para ser enviados a la red. TCP divide el flujo de bytes llegado de la aplicación en segmentos de tamaño apropiado (normalmente esta limitación viene impuesta por la unidad máxima de transferencia MTU) y le añade sus cabeceras. Entonces, TCP pasa el segmento resultante a la capa IP, donde a través de la red, llega a la capa TCP de la entidad destino. TCP comprueba que ningún segmento se ha perdido dando a cada uno un número de secuencia, que es también usado para asegurarse de que los paquetes han llegado a la entidad destino en el orden correcto. TCP devuelve un asentimiento por bytes que han sido recibidos correctamente; un temporizador en la entidad origen del envío causará un timeout si el asentimiento no es recibido en un tiempo razonable, y el (presuntamente desaparecido) paquete será entonces retransmitido. TCP revisa que no haya bytes dañados durante el envío usando un checksum; es calculado por el emisor en cada paquete antes de ser enviado, y comprobado por el receptor.

El campo Flags utiliza 8 bits para activar o desactivar cada una de las siguientes funciones: URG, ACK, PSH, Flag RST, SYN y FIN. Mirar versión en inglés.

Funcionamiento del protocolo en detalle

Las conexiones TCP se componen de tres etapas: establecimiento de conexión, transferencia de datos y fin de la conexión. Para establecer la conexión se usa el

procedimiento llamado negociación en tres pasos (3-way handshake). Una negociación en cuatro pasos (4-way handshake) es usada para la desconexión. Durante el establecimiento de la conexión, algunos parámetros como el número de secuencia son configurados para asegurar la entrega ordenada de los datos y la robustez de la comunicación.

- **Establecimiento de la conexión (negociación en tres pasos)**

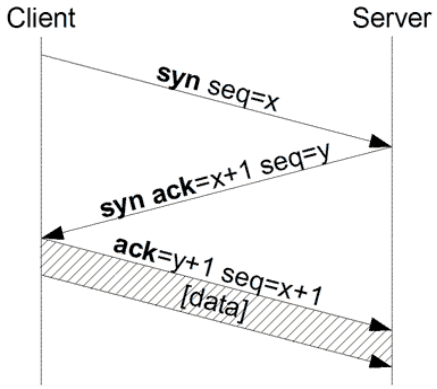


Figura. 1.17. Negociación en tres pasos o Three-way handshake

Aunque es posible que un par de entidades finales comiencen una conexión entre ellas simultáneamente, normalmente una de ellas abre un socket en un determinado puerto tcp y se queda a la escucha de nuevas conexiones. Es común referirse a esto como apertura pasiva, y determina el lado servidor de una conexión. El lado cliente de una conexión realiza una apertura activa de un puerto enviando un segmento SYN inicial al servidor como parte de la negociación en tres pasos. El lado servidor respondería a la petición SYN válida con un paquete SYN/ACK. Finalmente, el cliente debería responderle al servidor con un ACK, completando así la negociación en tres pasos (SYN, SYN/ACK y ACK) y la fase de establecimiento de conexión.

Es interesante notar que existe un número de secuencia generado por cada lado, ayudando de este modo a que no se puedan establecer conexiones falseadas (spoofing).

- **Transferencia de datos**

Durante la etapa de transferencia de datos, una serie de mecanismos claves determinan la fiabilidad y robustez del protocolo. Entre ellos están incluidos el uso del número de secuencia para ordenar los segmentos TCP recibidos y detectar paquetes

duplicados, checksums para detectar errores, y asentimientos y temporizadores para detectar pérdidas y retrasos.

Durante el establecimiento de conexión TCP, los números iniciales de secuencia son intercambiados entre las dos entidades TCP. Estos números de secuencia son usados para identificar los datos dentro del flujo de bytes, y poder identificar (y contar) los bytes de los datos de la aplicación. Siempre hay un par de números de secuencia incluidos en todo segmento TCP, referidos al número de secuencia y al número de asentimiento. Un emisor TCP se refiere a su propio número de secuencia cuando habla de número de secuencia, mientras que con el número de asentimiento se refiere al número de secuencia del receptor. Para mantener la fiabilidad, un receptor asiente los segmentos TCP indicando que ha recibido una parte del flujo continuo de bytes. Una mejora de TCP, llamada asentimiento selectivo (SACK, selective acknowledgement) permite a un receptor TCP asentir los datos que se han recibido de tal forma que el remitente solo retransmita los segmentos de datos que faltan.

- **Fin de la conexión**

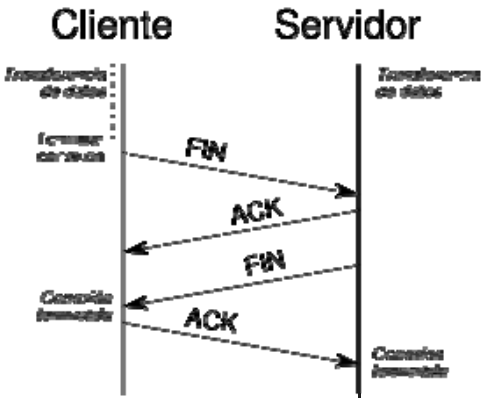


Figura. 1.18. Cierre de una conexión según el estándar

La fase de finalización de la conexión usa una negociación en cuatro pasos (four-way handshake), terminando la conexión desde cada lado independientemente. Cuando uno de los dos extremos de la conexión desea parar su "mitad" de conexión transmite un paquete FIN, que el otro interlocutor asentirá con un ACK. Por tanto, una desconexión típica requiere un par de segmentos FIN y ACK desde cada lado de la conexión.

Una conexión puede estar "medio abierta" en el caso de que uno de los lados la finalice pero el otro no. El lado que ha dado por finalizada la conexión no puede envíar más datos pero la otra parte si podrá.

b) UDP (USER DATAGRAM PROTOCOL) [10]

User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

En la familia de protocolos de Internet UDP proporciona una sencilla interfaz entre la capa de red y la capa de aplicación. UDP no otorga garantías para la entrega de sus mensajes y el origen UDP no retiene estados de los mensajes UDP que han sido enviados a la red. UDP sólo añade multiplexado de aplicación y suma de verificación de la cabecera y payload. Cualquier tipo de garantías para la transmisión de la información, deben ser implementadas en capas superiores.

+	Bits 0 - 15	16 - 31
0	Puerto origen	Puerto destino
32	Longitud del Mensaje	Suma de verificación
64	Datos	

Figura. 1.19. Formato de los segmentos de TCP

La cabecera UDP consta de 4 campos de los cuales 2 son opcionales (con fondo rojo en la Fig). Los campos de los puertos fuente y destino son campos de 16 bits que identifican el proceso de origen y recepción. Ya que UDP carece de un servidor de estado

y el origen UDP no solicita respuestas, el puerto origen es opcional. En caso de no ser utilizado, el puerto origen debe ser puesto a cero. A los campos del puerto origen le sigue un campo obligatorio que indica el tamaño en bytes del datagrama UDP incluidos los datos. El valor mínimo es de 8 bytes. El campo de la cabecera restante es un checksum de 16 bit que abarca la cabecera, los datos y una pseudo-cabecera con las IP origen y destino, el protocolo, la longitud del datagrama y 0's hasta completar un múltiplo de 16. pero no los datos. El checksum también es opcional, aunque generalmente se utiliza en la práctica.

Se utiliza cuando se necesita transmitir voz o vídeo y resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

Puertos

Los puertos sirven para identificar a las aplicaciones emisoras y receptoras. Cada lado de la conexión tiene asociado un número de puerto (de 16 bits sin signo, con lo que existen 65536 puertos posibles) asignado por la aplicación emisora o receptora. Los puertos son clasificados en tres categorías: bien conocidos, registrados y dinámicos/privados. Los puertos bien conocidos son asignados por la Internet Assigned Numbers Authority (IANA), van del 0 al 1023 y son usados normalmente por el sistema o por procesos con privilegios. Las aplicaciones que usan este tipo de puertos son ejecutadas como servidores y se quedan a la escucha de conexiones. Algunos ejemplos son: FTP (21), SSH (22), Telnet (23), SMTP (25) y HTTP (80). Los puertos registrados son normalmente empleados por las aplicaciones de usuario de forma temporal cuando conectan con los servidores, pero también pueden representar servicios que hayan sido registrados por un tercero (rango de puertos registrados: 1024 al 49151). Los puertos dinámicos/privados también pueden ser usados por las aplicaciones de usuario, pero este caso es menos común.

1.4 CALIDAD DE LA VOZ [11]

En una llamada telefónica por IP, la voz se digitaliza, se comprime y se envía en paquetes de datos IP. Estos paquetes se envían a través de Internet o una Intranet a la persona con la que estamos hablando. Cuando alcanzan su destino éstos paquetes son ensamblados de nuevo, descomprimidos y convertidos en la señal de voz original.

Al comprimir la voz su calidad va disminuyendo debido a la pérdida de información que se produce en el proceso, por consiguiente mayores compresiones implican mayores pérdidas de información con mayor degradación de la voz.

Los sistemas de VoIP utilizan algún algoritmo de compresión de audio llamado codec, siendo responsable tanto de codificar (convertir el sonido analógico recibido por el micrófono en forma digital) y decodificar (convertir el sonido codificado en su forma analógica y enviarla). Algunos codecs trabajan mejor para conexiones en bandas angostas, otros son optimizados para conexiones en diferentes velocidades.

1.4.1 ATRIBUTOS DE LA CODIFICACIÓN [11]

La codificación de la voz se refiere al proceso de reducir la velocidad binaria de la representación digital del habla para la transmisión o almacenamiento, mientras se mantenga una calidad de habla que sea aceptable para la aplicación.

De esta manera cuando se consideran codificadores de voz es importante revisar todos los atributos. Cada uno de estos atributos está estrechamente relacionados. Por ejemplo, los codificadores de baja velocidad binaria tienden a tener mas retardo que los codificadores de alta velocidad binaria. Ellos también pueden requerir alta complejidad para implementarlos y frecuentemente poseen baja calidad en comparación con los codificadores de alta velocidad binaria.

a) Velocidad binaria.

Debido a que los codificadores de voz están compartiendo el canal de comunicación con otros datos, el pico de velocidad binario deberá ser tan bajo como sea posible para no provocar un uso inapropiado de dicho canal. Muchos codificadores de voz operan en una velocidad binaria fija independiente de las características de la señal de entrada. Dado a que los codificadores de voz multimedios comparten el canal con otras formas de datos, es mejor hacer el codificador de velocidad variable. Para aplicaciones de voz y datos simultáneos un buen compromiso es crear un esquema de compresión de los silencios como parte del estándar de codificación.

Una solución común es usar velocidad fija para habla activa y baja velocidad para ruido de fondo.

La compresión de silencio se basa en dos algoritmos principales:

- El primero es un detector activo de voz (VAD), el cual determina si la señal de entrada es habla o algún tipo de ruido de fondo. Si la señal es considerada como habla, ésta es codificada totalmente a velocidad binaria fija. Si la señal detectada es considerada como ruido, ésta es codificada a baja velocidad binaria;

- El segundo algoritmo, generación de ruido confortable (CNG), es invocado en el receptor para reconstruir la característica principal del ruido de fondo. El nombre de ruido confortable es usado ya que oído prefiere un ruido de bajo nivel que un silencio total.

Obviamente la composición del VAD es vital para la obtención de la calidad del habla. Si el habla ocurre demasiado frecuente, la potencial ganancia de la compresión de silencio no será lograda.

Sin embargo para altos ruidos de fondo puede ser difícil distinguir entre el habla y ruido. Si el VAD falla para reconocer la presencia del habla, entonces el comienzo del habla puede ser cortado.

Afectando seriamente la inteligibilidad del habla codificada. Por lo tanto el esquema de ruido confortable debe ser diseñado de tal manera que el codificador y el decodificador están sincronizados, aun si no hay bits transmitidos durante algún intervalo. Esto permite lentas transiciones entre intervalos de habla activos y no activos.

b) Retardo de codificacion.

La tecnología actual puede ser calificada como buena, pero en ningún caso comparable a la telefonía tradicional. Se debe considerar que la voz es sensible a retardos. Sin embargo la mejora en los algoritmos de compresión, está generando una disminución en los tiempos de retardo.

El retardo de un sistema de codificación de habla usualmente consiste de tres importantes componentes. La mayoría de los codificadores de baja velocidad binaria

procesan una trama de datos a la vez. Los parámetros del habla son actualizados y luego transmitidos para cada trama.

Adicionalmente, para analizar los datos apropiadamente es necesario analizar el comportamiento de los datos y de la trama. Además, antes de que el habla sea analizada es necesario almacenar una trama de datos. El retardo resultante debido a los procesos anteriores se denomina retardo algorítmico, siendo el único componente del retardo que no puede ser reducido cambiando la implementación. La segunda mayor contribución viene del tiempo que toma al codificador analizar el habla y al decodificador reconstruir la señal de habla

Este es conocido como retardo de procesamiento, el cual depende de la velocidad de hardware utilizado para implementar el codificador.

La suma del retardo algorítmico y el de procesamiento es denominado retardo de codificación del codec.

El tercer componente es el retardo de comunicación, siendo el tiempo que toma una trama entera de datos ser transmitida del codificador al decodificador. La suma de los tres retardos, se denomina retardo en un sentido del sistema, debiendo ser menor que 200 mseg. Si hay presencia de eco, el máximo de retardo del sistema tolerable es de solo 25 mseg, esto muestra porque el uso del supresor de eco se hace necesario.

c) Medición de calidad.

La necesidad de sistemas de medición, comenzó en los años 1950 con el desarrollo del sistema de comunicación análogo. Estas técnicas fueron esenciales en la optimización de diseños de sistemas de codificación. Los constantes avances en este campo de estudio han llevado a concluir que existen diferentes métodos o formas para medir dicha calidad de servicio, clasificándose la mayoría métodos subjetivos y objetivos.

Los métodos subjetivos de medición de calidad entregan una herramienta adecuada para este tipo de codificadores, pero producto del elevado costo de las evaluaciones, debido a los requerimientos necesarios para llevar a cabo este tipo de pruebas, hacen complicada su utilización La forma de comparar las distintas metodologías a nivel de calidad, dependerá del tipo de codificación que se trate.

- Métodos subjetivos.

Estos métodos están basados en la opinión de grupos de personas sobre la calidad de frases codificadas. Las personas son entrenadas auditivamente, para posteriormente en laboratorios con equipos altamente especializados realizar las pruebas.

Algunos de los métodos subjetivos buscan medir la inteligibilidad de los codificadores. Para ello, utilizando palabras que se pronuncien parecidas se evalúa a los codificadores. Ejemplo de este tipo de sistemas de medida son MRT (Modified Rhyme Test) y DRT (Diagnostic Rhyme Test). Sin embargo, la inteligibilidad es sólo una parte en la calidad de voz, por lo que estos sistemas de medidas son incompletos, si el objetivo es medir la calidad.

Otro tipo de metodología utilizada es entrenar a los evaluadores con señales de referencia, para evitar diferencias de criterios. Alguno de estos sistemas de medida son: MOS (Mean Opinión Score), PAR (Paired Acceptability Rating) y ACR.

De los cuales el test MOS o "puntuación en base a la opinión promedio", es el más importante y el más utilizado. Esta escala de medida está fijada por el estándar P.800 de la ITU-T.

En estas encuestas, se colocan grupos de personas a realizar evaluaciones sobre la calidad de la voz percibida, escuchando la voz reconstruida con los diferentes métodos de compresión, utilizando puntuaciones que varían en una escala de cinco valores (Excelente = 5, Buena = 4, Regular = 3, Mediocre = 2, Mala = 1) y se ponderan para obtener una taza de puntuación media.

Una de las características interesantes de destacar, es que este método es aplicable a un amplio rango de distorsiones. La desventaja que presenta el sistema de medida MOS es que los resultados pueden variar por factores como la selección de los evaluadores, las instrucciones dadas, el equipamiento utilizado, el orden en que se realiza la prueba, etc.

- Métodos objetivos.

A diferencia, los métodos objetivos de medición de calidad para señales de voz se basan en comparaciones matemáticas entre la señal original y codificada. La mayoría de

estos métodos utilizan medidas de distancia para cuantizar la diferencia entre la señal distorsionada y la original. Una de las ventajas de este tipo de prueba es que permite obtener un valor cuantitativo de la calidad que no depende de factores externos, como en el caso de las medidas de calidad subjetivas. Es decir, cada vez que se realice la medición se obtendrá el mismo valor. Esto permite medir variaciones pequeñas en la calidad producidos por modificaciones poco significativas en los codificadores. Si se quisiera medir estas variaciones con métodos objetivos, se tendría que utilizar un gran número de evaluadores para tener un resultado significativo estadísticamente

Los métodos más elementales de este tipo de codificadores son el SNR y la razón señal a ruido segmentada (Segmental Signal to Noise Ratio, SEGSNR), los cuales miden la razón entre la potencia de la señal y la potencia del ruido.

Una de las recomendaciones más utilizadas, basada en este método, podría bien ser el que fija la ITU-T como estándar, el P.862, que proporciona un modelo psico-acústico, denominado PESQ (Perceptual Speech Quality Measure).

El método PESQ presenta mayor exactitud que cualquier otro modelo en promedio, es altamente robusto y da predicciones exactas de calidad para un amplio rango de condiciones. Es ideal para medir efecto de pérdida de paquete, jitter, ruido ambiental y errores en transmisión de canal en codificadores como G.711, G.726, G.728, G729 y G723.1. El resultado entregado por el estándar PESQ es normalizado a una escala similar al sistema MOS en el rango 0.5 y 4.5, sin embargo en la mayoría de los casos el rango de salida varia entre 1.0 y 4.5, rango normal para valores MOS encontrados en los experimentos de calidad subjetivos.

En consecuencia, el problema inherente a estos los métodos subjetivos, es el tiempo necesario para realizarlos, el costo y que no pueden ser usados para monitorear la calidad en períodos largos de tiempo. Esto ha hecho a los métodos objetivos atractivos para estimar la calidad percibida en redes de comunicaciones.

1.4.2 CODIFICACIÓN DE LA VOZ [11]

La codificación de la voz, que comprende la digitalización y la compresión de la voz, puede ser realizada mediante tres técnicas principales: por codificación de forma de onda,

por codificación basada en modelos matemáticos sobre la producción de la voz y por último, en modelos híbridos que combinan ambas técnicas.

Los codificadores de forma de onda se basan en la codificación de la señal a partir de las muestras de la señal, reproduciendo una aproximación de la señal original a través de una serie de muestras reconstruidas que tratan de acercarse lo más posible a las muestras originales de la señal.

Entre estos tipos de codificadores tenemos el PCM y el ADPCM. Dichos codificadores se basan en el teorema de Nyquist, que señala que una señal puede ser reconstruida si se muestrea a por lo menos el doble de su frecuencia máxima.

Los codificadores basados en modelos matemáticos no trabajan con muestras de la voz, como los codificadores de forma de onda, sino que utilizan segmentos de voz de corta duración (de 10 a 40 mseg). Por cada segmento de voz se calcula un conjunto de parámetros que lo caracteriza, convirtiendo dichos parámetros en un conjunto de bits. Estos codificadores se basan en el modelaje matemático del tracto vocal.

El tercer método de codificación es el híbrido, que como su nombre lo indica es una combinación de los dos anteriores.

A continuación analizaremos un poco en detalle estos codificadores.

a) PCM (modulación de impulsos codificados) o MIC.

PCM (*Pulse Code Modulation*), modulación por pulsos codificados, se desarrolló en los años 60 y fue estandarizado por la ITU bajo el nombre de Recomendación G.711, esta es una codificación de forma de onda que se basa en un proceso de tres pasos: muestreo, cuantificación y codificación.

- Muestreo.

El teorema de Nyquist señala que si una señal es muestreada a por lo menos el doble de la frecuencia máxima de la misma, la señal puede ser reconstruida fielmente a partir de estas muestras.

Como la señal de voz está contenida fundamentalmente dentro de una banda de frecuencias entre 300 y 3400 Hz la misma se filtra para que no exista prácticamente ninguna componente de frecuencia por encima de 4 KHz, procediéndose, después de este filtraje a tomar 8000 muestras por segundo (2 x 4 KHz).

El resultado del proceso de muestreo es una serie de pulsos con una amplitud igual al valor de cada muestra (PAM, Pulse Amplitud Modulation, modulación por amplitud de pulsos).

- Cuantificación.

La idea fundamental de PCM es la de convertir una señal analógica a su equivalente digital, sin embargo, el proceso de muestreo nos da una serie de pulsos cuya amplitud se encuentra en una gama infinita de valores. Para asignar una secuencia binaria diferente a cada valor de una señal que presenta una gama infinita de valores, se requeriría un código de longitud infinita.

La idea del proceso de cuantificación es la de relacionar esa gama infinita de valores a una serie de valores discretos, de forma tal de minimizar el número de valores discretos requeridos (minimizando la longitud del código), sin sacrificar de forma apreciable la calidad de la señal reconstruida, sin embargo la señal reconstruida no será exactamente igual a la señal original. A esta diferencia se le denomina error de cuantificación.

En el proceso de cuantificación se trata de disminuir dicho error, es por ello que dicho proceso no es uniforme. Es decir, los valores discretos no se encuentran equidistantes entre sí. En la gama de valores pertenecientes a las amplitudes más bajas se asigna un mayor número de valores discretos. A medida que se acerca a la gama de valores de amplitudes más altas, el número de valores discretos asignados disminuye.

Esto debido a que existe mucha mayor probabilidad de que las muestras de las señales de voz se encuentren en la gama de las amplitudes menores, por lo que se hace todavía más importante minimizar el error de cuantificación para estas amplitudes.

En América del Norte y en Japón se utiliza una cuantificación donde las muestras están espaciadas logarítmicamente, denominada ley μ. En Europa y en América del Sur se utiliza principalmente una cuantificación también logarítmica, denominada ley A.

- Codificación.

En el proceso de codificación, a cada valor discreto de la muestra se le asigna un código único de 8 bits (con lo cual podemos representar 256 valores discretos diferentes).

De todo esto tenemos que, siguiendo el teorema de Nyquist, transmitimos 8000 muestras por segundo (4 KHz x 2), y dado que cada muestra está constituida por 8 bits, para transportar una señal de voz, requerimos un canal de 64 kbps (8000 m/s x 8b/m = 64000 b/s).

b) Modulación diferencial adaptativa por pulsos codificados (ADPCM).

En ADPCM (*Adaptive Differential Pulse Code Modulation*), a diferencia del PCM, no se codifica cada una de las muestras, sino que se codifica la diferencia entre la predicción de la muestra y la muestra original. Dado el alto grado de correlación entre las muestras, se pueden realizar predicciones cercanas a los valores de las muestras, por lo que se requiere enviar menos bits para indicar cuál es el error de la predicción (diferencia entre la predicción y la muestra real) que el número de bits que se requiere para enviar la muestra en su totalidad.

Con ADPCM se muestrea la señal de voz 8000 veces por segundo (como en PCM), pero dado que se envía solamente el error de predicción, solamente se requiere transmitir 4 bits de información en lugar de los 8 que se requerirían para enviar la información de la muestra en su totalidad. Con esto se logra disminuir la velocidad de transmisión en la mitad (32 kbps, 8000 muestras por segundo x 4bits por muestra) con respecto al PCM.

El ADPCM fue estandarizada por la ITU a mediados de los años ochenta bajo la recomendación G.721. En 1988 surgieron extensiones al G.721 (la G.723) que permiten reducir la velocidad de bits en el canal cuando la red presenta congestión. Con esta extensión se puede ajustar los bits por muestra a 3 y a 5, obteniéndose velocidades de 24 kbps y 40 kbps, respectivamente.

En 1990 surgió una nueva versión de ADPCM (G.726) la cual es capaz de ajustar la velocidad de bits, cambiando el número de bits por muestra de 2 hasta 5, obteniéndose velocidades entre 16 kbps y 40 kbps.

A diferencia del PCM, donde todas las muestras son independientes unas de otras, para estos algoritmos de ADPCM la predicción de la muestra presente depende de las muestras precedentes. De esta manera, si al utilizar PCM se pierde una muestra de la señal, la calidad de la señal se ve afectada solamente por la pérdida de esa muestra, sin embargo, si se utiliza ADPCM la pérdida de una muestra afecta la predicción de las muestras siguientes, teniendo esto un mayor impacto en la calidad de la señal.

De PCM, se deriva el algoritmo Embedded ADPCM, definido en la recomendación G.727, el cual, provee una capacidad para asignar el ancho de banda de una manera mucho más flexible, sin requerir ningún tipo de negociación.

Por estas razones, se hace muy importante que todos los bits generados en el transmisor lleguen correctamente al receptor de forma tal de mantener la predicción de ambos equipos sincronizada.

c) Codificación predictiva lineal (LPC).

Los métodos de codificación de forma de onda discutidos previamente se basan en la representación de la señal de voz en el dominio del tiempo. LPC (*Linear Predictive Coding*) analiza la señal en el dominio de la frecuencia.

En gamas de milisegundos, las señales de voz no varían significativamente y esta característica es lo que permite la posibilidad de sintetizar la voz. Con este tipo de codificación, en lugar de digitalizarse la señal analógica, se digitaliza los parámetros del modelo de voz y el nivel de excitación pertenecientes a una gama pequeña de tiempo (alrededor de 20 mseg) enviando esta información al decodificador.

Básicamente, LPC divide la señal de voz en segmentos temporales de alrededor de 20 mseg. (lo que equivaldría a 160 muestras PCM). Para cada segmento el codificador calcula el filtro que ha de utilizarse para modelar el tracto vocal (a partir de la ecuación lineal y de los valores de las muestras) y le envía los parámetros que caracterizan a este filtro al decodificador. Adicionalmente le envía los parámetros que caracterizan al formante (vibración de las cuerdas vocales) presente en ese lapso de tiempo en que se está analizando la señal (frecuencia e intensidad). Con esta información el decodificador puede reconstruir la señal fuente, la cual hace pasar por el filtro, obteniéndose la voz sintetizada.

Actualmente se puede codificar la voz con LPC a velocidades entre 2.4 y 4.8 kbps con una señal de voz reconstruida con una calidad razonable. Desafortunadamente, ciertos sonidos no se pueden reproducir fielmente con este método. La representación del tracto vocal por una serie de tubos acústicos concatenados no permite representar los sonidos nasales, los cuales, requieren una representación matemática mucho más compleja.

Adicionalmente, el modelaje del tracto vocal también conlleva a que la señal reconstruida difiera de la real, debido a las diferencias entre el modelo y el tracto vocal real.

La principal ventaja de la utilización del LPC es su capacidad de producir voz inteligible a muy bajas velocidades (entre 2,4 y 4,8 kbps). Sin embargo, al utilizar este tipo de codificación generalmente se hace imposible reconocer, a partir de la voz sintetizada, a la persona que la origina.

La razón de esto es que las características del tracto vocal varían enormemente de persona a persona, lo cual hace el modelaje sumamente difícil. Adicionalmente, cuanto más complejo se haga el modelaje, se requieren más bits para representarlo, y por tanto las velocidades de transmisión aumentan, no viéndose justificadas la complejidad del modelo con la velocidad de transmisión obtenida.

Por otro lado, LPC basa su funcionamiento en dos tipos de sonidos: con voz y sin voz, por lo que no puede representar los otros tipos de sonidos existentes, resultando esto en la producción de una voz artificial.

Estas razones hacen que la calidad de la voz sea muy inferior a la obtenida a través de las técnicas de PCM y ADPCM.

d) Codificación por excitación lineal predictiva (CELP).

CELP (Code Excited Linear Prediction) es una técnica híbrida de codificación, donde se combinan la codificación por forma de onda y la codificación por modelaje de la voz.

La idea es tratar de obtener las ventajas de ambas técnicas. A través de la codificación por forma de onda se logra reconstruir la señal con un grado de fidelidad alto

(pero utilizando un ancho de banda significativo). Por otro lado, con la codificación por modelaje logro transmitir la señal de voz utilizando un ancho de banda muy pequeño (pero con una calidad muy inferior).

Como vimos anteriormente, LPC basa su algoritmo en los sonidos con voz y los sonidos sin voz, para lo cual elimina los componentes de la voz que no se encuentran dentro de estas dos clases.

La información eliminada se denomina residuo de la voz y contiene información importante que puede permitir la reconstrucción mucho más fiel de la voz.

CELP utiliza un modelo del tracto vocal muy similar al utilizado por LPC y la diferencia fundamental se basa en que, adicionalmente, CELP utiliza un libro de códigos que contiene una tabla con las señales residuo típicas. En operación, el codificador compara el residuo con todas las entradas en el libro de códigos, eligiendo la que más se parece y enviando el código de la misma. El receptor recibe el código, y elige el residuo relacionado con el mismo, el cual utiliza para excitar el filtro. De aquí el nombre de predicción lineal con excitación por código.

De esta manera, CELP, además de enviar los parámetros que modelan el tracto vocal, la intensidad de la excitación, y la frecuencia de la formante (sonidos con voz), también envía el código que permite obtener una aproximación al residuo de la señal de voz.

En el decodificador, tanto la señal del generador de excitación (con los valores de intensidad y frecuencia indicados por el codificador) como la señal reconstruida del residuo (obtenida a partir del libro de códigos y del código enviado por el codificador) se pasa a través del filtro que modela el tracto vocal (construido a través de los parámetros enviados por el codificador), obteniéndose así la reconstrucción de la voz.

Con esta codificación se logra obtener una calidad mucho mayor a la obtenida con LPC sin sacrificar mucho ancho de banda adicional (velocidades entre 4.8 y 16 kbps).

e) Codificación CS-ACELP.

La codificación CS-ACELP (Conjugate Structure Algebraic Code Excited Linear Prediction, predicción por excitación lineal de código algebraico de estructura conjugada)

fue estandarizada por la ITU en Noviembre de 1995 bajo la recomendación G.729. Con la utilización de esta recomendación se codifica la voz a 8 kbps.

Esta codificación opera con segmentos de voz de 10 mseg, correspondientes a 80 muestras PCM. Cada 10 mseg se analiza la señal de voz y se extrae los parámetros del modelo CELP.

La característica principal de CS-ACELP es que las entradas del libro de códigos ya no vienen dadas por un conjunto de valores que caracterizan las formas de onda de los residuos, sino que dichas formas de onda son representadas por un conjunto de ecuaciones algebraicas.

Los procesadores de señales digitales manipulan con mucha mayor facilidad las formas de onda de los residuos cuando estos son representados como funciones matemáticas que cuando estas son representadas por un conjunto de valores.

CS-ACELP utiliza dos libros de códigos, uno fijo y otro adaptable. El libro fijo contiene formas de onda preestablecidas, las cuales no varían. En el libro adaptable, las formas de onda se van adaptando a las señales reconstruidas, permitiendo con esto que la reconstrucción de la voz se vaya ajustando a las características de la misma, obteniéndose con esto una mayor fidelidad.

Como vimos antes, G.729 utiliza segmentos de voz de 10 mseg. Adicionalmente, el cálculo de los coeficientes del filtro se basa no solamente en las muestras tomadas durante esos 10 mseg, sino que también toma en consideración las muestras de los 5 mseg siguientes, teniéndose con esto un retardo del algoritmo de 15 mseg.

f) Codificación LD-CELP.

LD-CELP (Low Delay CELP, CELP de bajo retardo) fue estandarizado por la ITU en 1992 bajo la recomendación G.728.

Con esta codificación ya no se transmite los parámetros del filtro, la frecuencia y amplitud de la excitación y el código del residuo, sino que se transmite el código de la excitación. Realmente, se transmite aquél código que, al pasarlo por un filtro adaptable, genera la señal más similar a la señal de entrada (el menor error). En el decodificador, los

parámetros que caracterizan al filtro son calculados a partir de los segmentos previos de voz reconstruida.

Esta codificación opera con segmentos de voz de 0,625 mseg, correspondientes a 5 muestras PCM. Por cada segmento de voz, el codificador analiza entre los 1024 vectores de su libro de códigos para encontrar la forma de onda del mismo que más se aproxime a la excitación de entrada (el que minimiza el error medio cuadrático compensado en frecuencia con respecto a la señal de entrada).

Los 10 bits correspondientes al vector del libro de código seleccionado son enviados al decodificador.

De esta manera, cada 0,625 mseg el codificador envía 10 bits, lo que da una velocidad de 16 kbps.

En la práctica, 7 bits son utilizados para representar 128 formas de onda patrón y los otros bits se utilizan para indicar la amplitud de la señal. Sabiendo que una señal analógica puede poseer una variedad infinita de valores la selección entre 1024 posibilidades se ve muy débil, y realmente lo sería si esta selección fuera estática. Sin embargo, esta selección no es estática, como en ninguna de las codificaciones CELP. Justamente la reputación de altamente compleja que posee la codificación CELP viene dada de la actualización constante de los libros de código y de los filtros, a partir del pasado reciente de la señal de entrada.

Esta codificación presenta un retardo de algoritmo de apenas 0,625 mseg, el cual es bastante bajo sobre todo si se lo compara con el de la recomendación G.729, el cual posee un retardo de algoritmo de 15 mseg. (Un retardo 24 veces mayor).

Al acumular solamente 5 muestras PCM para procesar el segmento de voz (en lugar de 80 para G.729) se logra tiempos de acumulación mucho menores que reducen el retardo del algoritmo, y, adicionalmente, resultan bloques de información más pequeños que se procesan de una manera mucho más rápida.

1.4.3 RESUMEN DE CODIFICADORES [12]

En la siguiente tabla se resumen las características de los diferentes tipos de codificadores:

Tabla. 1.5. Resumen de códecs

	G.711	G.721	G.726	G.727	G.728	G.729	G.723.1	GSM FR
Tipo de codificación	PCM	ADPCM	ADPCM	ADPCM	LD-CELP	CS-ACELP	MP-MLQ / ACELP	RPE-LTP
Tasa binaria (kbit/s)	64	32	16/24/32/40	16/24/32/40	16	8	6,4/5,3	13
Complejidad (MIPS)	0,1	10	12	12	33	22	16/18	2,5
Retardo codificador (ms)	0,125	0,125	0,625	0,125	0,125	15	37,5	20
Calidad (MOS)	4,2	4,0	4,0	4,0	4,0	4,0	3,9/3,7	3,6-3-8

1.5. CALIDAD DE SERVICIO (QOS) [11]

La provisión de QoS garantizada por parte de las redes de comunicación en un ámbito global es actualmente uno de los campos de investigación en activo, principalmente debido a la creciente importancia de aplicaciones telemáticas (destacando entre ellas a la ToIP), que precisan de esa garantía para su correcto funcionamiento.

El auge de la ToIP es algo evidente y la principal razón es el reaprovechamiento de los recursos y la disminución en el costo de llamadas a través de Internet. Sin embargo, si de algo adolece todavía la ToIP es de la calidad de los sistemas telefónicos tradicionales. Los problemas de esta calidad son muchas veces inherentes a la utilización de la red (Internet y su velocidad y ancho de banda) y podrán irse solventando en el futuro. Mientras tanto, cuanto mejor conozcamos los problemas que se producen y sus posibles soluciones mayor calidad disfrutaremos.

1.5.1. CONCEPTO DE QOS [11]

Se entiende por “Calidad de Servicio”, a la capacidad de una red para sostener un comportamiento adecuado de tráfico que transita por ella, cumpliendo a su vez con los requerimientos de ciertos parámetros relevantes para el usuario final. Esto puede entenderse también como el cumplimiento de un conjunto de requisitos estipulados en un contrato (SLA: *Service Level Agreement*, acuerdo de nivel de servicio) entre un ISP y sus clientes.

Al contar con QoS, es posible asegurar una correcta entrega de la información necesaria o crítica, para ámbitos empresariales o institucionales, dando preferencia a aplicaciones de desempeño crítico, donde se comparten simultáneamente los recursos de la red con otras aplicaciones no críticas.

1.5.2 SERVICIO *BEST-EFFOR* [11]

Las redes IP fueron diseñadas para el transporte óptimo del tráfico de datos, por lo que la QoS requerida en las mismas se basó únicamente en la integridad de los datos, esto es, no pérdida de contenido y ni secuencialidad de los mismos. En este sentido IP fue concebido, es decir, para "mover" por la red, de forma óptima y segura, tráfico sin requerimientos de tiempo real.

Para esto el servicio que brinda IPv4 es del tipo "*Best Effort*", es decir, cuando la red hace todo lo posible para intentar entregar el paquete a su destino, no existiendo garantía de que esto ocurra. Por otra parte, el tráfico de audio y vídeo no solo requiere ser transferido por las redes IP de forma íntegra, sino que además requiere ser transferido en el tiempo adecuado, al "ritmo" adecuado, en correspondencia con la cadencia que es generado.

El nacimiento de IPv6 viene a resolver las limitaciones de IPv4, además de integrar nuevas características que permitan entregar seguridad y confiabilidad en la transmisión de la información.

Soporte de QoS que incorporan los protocolos IPv4 e IPv6.

Los protocolos IPv4 e IPv6 siguen la estrategia de asignación de prioridades definiendo campos incluidos en las cabeceras que permiten diferenciar tráfico. Estos protocolos, sin embargo, no pueden ofrecer por sí solos una QoS extremo a extremo. Para que esto sea posible necesitan apoyarse en alguno de los modelos y mecanismos propuestos por la IETF como:

• Servicios Integrados (IntServ) y RSVP (Resource ReserVation Protocol). Sigue una estrategia de reserva de recursos. Antes de que se transmitan los datos, las aplicaciones deben primero establecer caminos y reservar recursos. RSVP es el protocolo que usa IntServ para establecer los caminos y reservar los recursos necesarios.

• Servicios Diferenciados (DiffServ ó DS). Sigue una estrategia de asignación de prioridades.

Los paquetes se marcan de distintas formas para crear varias clases de paquetes. Los paquetes de diferente clase recibirán servicios distintos.

• MPLS (MultiProtocol Label Switching). Es un nuevo esquema de encaminamiento y conmutación que integra los niveles de red y enlace sin discontinuidades. Se presenta como sustituto de IP sobre ATM ó IP/ATM. A los paquetes se les asignan etiquetas al ingresar en un dominio con capacidad de MPLS. La posterior clasificación, encaminado, y servicios aplicados a los paquetes se basarán en las etiquetas.

1.5.3. REQUERIMIENTOS PARA GARANTIZAR QOS [11]

Cuando una aplicación recurre a una o varias redes de datos, la calidad de servicio resultante de extremo a extremo entre las dos máquinas que ejecutan la aplicación en cuestión dependerá de la calidad de servicio garantizada por todas las redes que intervienen. Por este motivo, la calidad de servicio es criticada muy a menudo. Basta con que una sola red ofrezca una calidad de servicio inferior a la aceptable para que se vea afectada la calidad de extremo a extremo.

Por este motivo, cuando las empresas emplean la red Internet para interconectar máquinas distantes para sus aplicaciones estratégicas, con frecuencia eligen los servicios de proveedores de red privada virtual (VPN). Este tipo de proveedor establece, mediante ingeniería especializada, la configuración de señalización por encima de la red Internet, mediante una red virtual que garantiza propiedades de calidad de servicios aceptables entre todos los puntos de acceso de la empresa, con inclusión de algunos puntos de acceso dinámicos para los usuarios distantes. Por supuesto que una VPN sólo podrá establecerse mediante la reservación de recursos en todas las redes fijas que la apoyen; por consiguiente, un servicio de este tipo tendrá un costo más elevado y está previsto actualmente sólo para clientes empresariales.

En una comunicación extremo a extremo, para garantizar la QoS se requiere de la interacción de un conjunto de elementos, los cuales se describen a continuación:

• Aplicaciones. Aquí la aplicación debe de manejar la señalización necesaria para hacer la negociación de parámetros con la red.

• Intranet. La red IP implementada por la propia empresa. Suele constar de varias redes LAN (Ethernet conmutada, ATM, etc.) que se interconectan mediante redes WAN tipo Frame-Relay/ATM, líneas punto a punto, RDSI para el acceso remoto, etc. En este escenario se tiene bajo control prácticamente todos los parámetros de la red, resultando ideal para el transporte de la red.

• Red IP pública. Los operadores ofrecen a las empresas la conectividad necesaria para interactuar sus redes de área local en lo que al tráfico IP se refiere. Considerándose como algo similar a Internet, pero con una mayor QoS, y con importantes mejoras en seguridad.

• Internet. El estado actual no permite un uso profesional para el tráfico de voz.

a) QOS en la transmisión de paquetes de VoIP sobre LAN.

Una de las principales desventajas para cualquier tráfico crítico respecto del tiempo y en particular los paquetes de VoIP en una LAN, es que los protocolos más utilizados en el nivel de enlace, Ethernet y Token Ring, trabajan con un tamaño de paquete variable. El equipamiento desarrollado para VoIP brinda sólo conectividad Ethernet, con un ancho de banda de transmisión (BW) de 10 Mbps. El tamaño de la carga útil del paquete varía entre 46 y 1500 bytes y el encabezado ocupa entre 14 y 20 bytes. Por ejemplo, si tenemos un paquete con una carga útil de 64 bytes, y un encabezado de 20 bytes, la tasa de paquetes Ethernet es de 14880 pps (10000000 bps/ [(64 bytes +20 bytes) x 8 bits/Bytes]).

Por lo tanto, la utilización del ancho de banda y la tasa de paquetes pueden o no coincidir debido a la variación del tamaño de los paquetes. La utilización se incrementa debido a la variación de dos factores, aumento de la cantidad de paquetes y/o el tamaño de la carga útil de los mismos.

En Ethernet la disponibilidad de ancho de banda es dependiente del número de colisiones, en forma exponencial debido a la forma de trabajo del mecanismo CSMA/CD de la norma Ethernet 802.3

Para cumplir con los requerimientos de QoS para ToIP la utilización del ancho de banda no debe superar el 25 % o su equivalencia en porcentaje de colisiones que no debe superar el 45 %.

El estándar 802.1p provee el método para especificar los requerimientos de retardo y prioridades sobre una red LAN Ethernet y Token Ring.

Normalmente la QoS de LAN va asociada a la QoS a nivel de red, haciendo una equivalencia de prioridades 802.1p a tipos de servicio IntServ o DiffServ (más fácil con Diffserv).

b) QOS en la transmisión de paquetes de VoIP sobre WAN.

De acuerdo a resultados empíricos, la calidad de la voz comienza a degradarse en un enlace WAN, cuando el retardo supera los 150 ms. Debemos considerar no solo el ancho de banda que ocupa el tráfico de VoIP sino también el tráfico de datos propiamente dicho. En enlaces de baja capacidad, es decir menores a 512 kbps se puede llegar a degradar la voz en forma notable cuando se transmiten los paquetes de VoIP que compiten con paquetes de datos o con otros paquetes de VoIP.

Esto ocurre cuando no hay una política correctamente aplicada de QoS. Hay soluciones propietarias, como LFI (*Link Fragmentation Interleave*) utilizadas en enlaces de baja velocidad. Funcionan segmentando y entrelazando todos los paquetes para evitar la competencia con los pequeños paquetes de VoIP.

c) PROBLEMAS DE QOS EN LAS FRONTERAS.

El tráfico intercambiado entre redes ISP se convierte en el denominado tráfico "fuera de red", el cual plantea una serie de problemas de QoS.

Los principales problemas de QoS existentes fuera de la red pueden resumirse del siguiente modo:

• Cuando las redes de interconexión utilizan equipos de distintos vendedores y esos equipos no incluyen productos industriales plenamente normalizados, suelen surgir ciertos problemas que inciden en la QoS. Así, por ejemplo, se pierden estructuras del diseño de redes que mejoran la calidad de servicio, y no se utilizan sistemas de gestión normalizados.

• Cada uno de los acuerdos de nivel de servicio (SLA) ofrecidos por los proveedores de tránsito es específico. Las propiedades estadísticas de las redes ISP son distintas y, además, no son fácilmente comparables, ya que existen diferencias en cuanto al modo de recopilar los datos.

• Algunas veces, las especificaciones del servicio de VBR del ATM (empleado para el tráfico de Internet) varían de una red a otra, por lo que la QoS no se mantiene cuando el tráfico cruza las fronteras.

• Los equipos con dos o más años de antigüedad no suelen proporcionar las mismas capacidades de QoS que las ofrecidas por equipos más nuevos.

De lo anterior se desprende que la degradación de la calidad de servicio es muy frecuente en los extremos.

Por otra parte, existen motivos para sospechar que las posibles soluciones a estos problemas de QoS pueden verse aplazadas debido a un problema de coordinación. Todas las redes que manejan los datagramas enviados entre anfitriones comunicantes ("equipos terminales", en términos de RTPC) deben ser capaces de conservar los parámetros de QoS que proporciona la red de origen para que dichos parámetros puedan ser actualizados entre los anfitriones o las partes que establecen la comunicación. En otras palabras, si una de las redes del ISP encargadas de proporcionar la comunicación confiere a su parte de la red una calidad de servicio inferior a la ofrecida por otras redes, la QoS del flujo se verá reducida en consecuencia.

En este contexto, las redes individuales pueden mostrarse renuentes a invertir en una QoS superior si no existe alguna forma de coordinar esta mejora con las demás partes de la cadena.

1.5.4. DIFICULTADES TÉCNICAS, PARÁMETROS DE QOS [11]

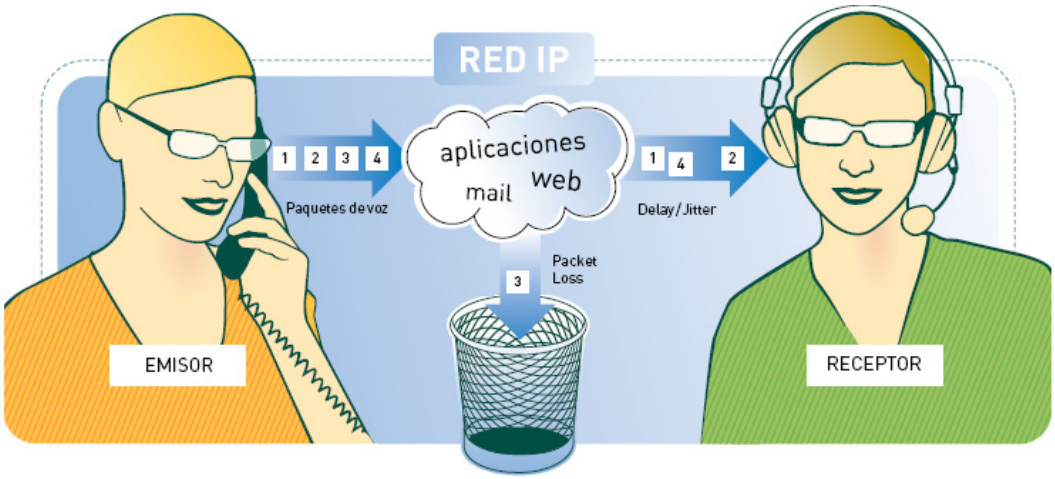


Figura. 1.20. Representación de los parámetros QoS [13]

El elemento que más afecta a la calidad de las llamadas de ToIP es el diseño, implementación y uso de la red en la que tienen lugar estas llamadas. Una llamada típicamente se originará en un CPE (Customer Pre-mises Equipment) o "equipo en las premisas del cliente", circulará primero a través de la LAN del cliente, circulará posteriormente a través de un enlace WAN, la red del proveedor de servicios y vuelta a otra red LAN y, por último, el CPE del extremo remoto. Los equipos CPE y los enlaces WAN son los más vulnerables a factores degradantes.

La entrega de señales de voz, vídeo y fax desde un punto a otro no se puede considerar realizada con un éxito total a menos que la calidad de las señales transmitidas satisfaga al receptor.

Entre los factores que afectan a la calidad se encuentran los siguientes:

a) RETARDO.

El retardo de extremo a extremo (a veces denominado "latencia") es el tiempo entre la generación de un sonido en un extremo de una llamada y su recepción en el otro extremo. El retardo incluye el tiempo que toma codificar el sonido como señal digital, la travesía de la señala por la red, y la regeneración de la señal como sonido en el extremo de recepción. El retardo causa dos deterioros diferentes. Primero, al aumentar el retardo, el

eco se vuelve más evidente. Segundo, cuando el retardo es lo suficientemente prolongado, perturba la dinámica de la conversación, dificultando la comunicación.

Se ha determinado que el retardo máximo que la voz puede sufrir en una conversación es de 250 mseg, y que un retardo mayor de este valor se torna sumamente desagradable, ocasionando que los integrantes de la conversación traten de hablar simultáneamente. De esta manera, cuando uno de los usuarios escucha que el otro no está hablando, entonces comienza a hablar, pero debido al retardo, el otro usuario no lo escucha de manera inmediata, por lo que puede comenzar a hablar también, lo cual ocasiona que las voces de los usuarios se solapen constantemente, haciendo muy difícil que la conversación se desarrolle normalmente. El solapamiento de las voces es detectado por los integrantes de la conversación un tiempo después de que comenzaron a hablar, siendo este tiempo igual al retardo sufrido por la voz. Cuanto mayor sea este retardo, mayor será el tiempo que se tarde en detectar que se está hablando simultáneamente, resultando las colisiones de las voces más desagradables y difíciles de controlar. Cuando el retardo es menor a 250 mseg, el efecto causado por las colisiones es tolerable y la conversación se puede desarrollar normalmente. A continuación se muestran los valores (véase la Recomendación UIT-T G.114) que indican las clases de calidad e interactividad de acuerdo con el retardo de transmisión en una conversación telefónica.

Tabla. 1.6. Clases de calidad del UIT-T según el retardo de transmisión

Clase N°	Retardo por cada sentido	Observaciones
1	De 0 a 150 ms	Aceptable para la mayoría de las conversaciones; sólo algunas funciones altamente interactivas pueden experimentar degradación.
2	De 150 a 300 ms	Aceptable para las llamadas de baja interactividad (satélite con 250 ms por salto).
3	De 300 a 700 ms	Prácticamente una llamada semidúplex.
4	Más de 700 ms	Inútil, a menos que los llamantes estén habituados a conversar en semidúplex (como en el ejército).

Para las transmisiones de vídeo, el retardo debe también mantenerse dentro de un límite tolerable de alrededor de 3 segundos. Para lograr retardos no mayores de un límite superior se emplean métodos de segmentación y de asignación de prioridades.

A los paquetes de voz y vídeo se le asignan prioridades mayores que a los paquetes de datos. Con este esquema, los paquetes de datos son almacenados hasta que los paquetes de mayor prioridad (voz y vídeo) son transmitidos.

- **Retardo de compresión.**

Este retardo ya fue analizado en el apartado 1.4.1 Atributos a la codificación.

- **Retardo de empaquetamiento de la información.**

Como se vio anteriormente, la duración de los segmentos de voz que procesa el algoritmo de compresión depende del algoritmo que se está utilizando.

G.728 utiliza segmentos de voz de 0,625 mseg. y la velocidad del algoritmo es de 16 kbps. De esta manera se tiene que el segmento de voz es representado por 10 bits (0625mseg. x 16 kbps). Si solo estos 10 bits se empaquetan en una trama IP se tiene un overhead (sobre carga) muy grande, y por lo tanto un desperdicio importante de ancho de banda.

Usualmente, se reúnen varios segmentos de voz en un solo paquete de información, con la finalidad de disminuir el overhead en la comunicación. Esto tiene como contraparte un mayor retardo. Así, si se reúnen 40 segmentos G.728 de voz, el overhead pasa a ser 11% pero el retardo de empaquetamiento pasa a ser de 25 mseg. (0,625 mseg x 40).

- **Retardos por serialización.**

Este retardo es el tiempo que tarda el paquete en ser transmitido en su totalidad hacia la WAN cuando el mismo ya se encuentra de primero en la "cola" de transmisión del CPE. Cuanto más grande es el paquete mayor será el tiempo para que este sea transmitido en su totalidad hacia la WAN y cuanto menor sea la velocidad del enlace también será mayor el retardo de serialización (retardo de serialización = tamaño del paquete / velocidad del enlace).

- **Retardo de espera en cola.**

Cuando se requiere transmitir un paquete de información, pero otro paquete se está transmitiendo en ese momento, hay que esperar a que termine la transmisión del mismo

antes de proceder a transmitir el otro paquete. El tiempo que transcurre debido a esta espera de que el otro paquete se transmita se denomina retardo de espera en cola.

La forma de minimizar este retardo, consiste en segmentar los paquetes de datos. Así, un paquete de 1500 bytes puede ser segmentado en, digamos, 15 paquetes de 100 bytes. De esta manera, ya no tendríamos un paquete de 1500 bytes en cola, sino que tendríamos 15 paquetes de 100 bytes en cola. Ahora bien, dado que el paquete de voz tiene prioridad sobre los de datos, éste deberá esperar a lo sumo, a que un solo paquete de datos se transmita.

- **Retardo de propagación.**

El retardo de propagación está relacionado con la transmisión de una señal a una distancia considerable. Por ejemplo, una línea de fibras ópticas a larga distancia impone un retardo de propagación de unos 5 μseg. por kilómetro.

- **Retardo en el buffer.**

Para que los paquetes de información puedan ser reproducidos de manera constante en el receptor, se hace necesario almacenar una determinada cantidad de los mismos, y luego reproducirlos de manera constante, lo cual implica un retardo.

La idea básica es que este tiempo de almacenamiento de un paquete sea tal que, en los momentos en que la red experimente una carga pesada, los paquetes almacenados en buffer no se agoten y se pueda seguir suministrando los mismos de una manera relativamente constante.

- **Retardos de descompresión.**

Hace refieren al tiempo que se tarda en descomprimir la voz (o video). Estos tiempos dependen de la complejidad de descomprimir el algoritmo utilizado y del hardware utilizado para ello. Para descomprimir la voz usualmente no se toma tiempos mayores a 4 mseg. Por lo que no resultan tan significativos como los anteriores, por lo que no se analizaran detalladamente.

b) VARIACIÓN DEL RETARDO (JITTER).

Otro factor de importancia en la transmisión de voz, es el ocasionado por las variaciones de retardos existente entre los paquetes. Por su filosofía de funcionamiento, la información que viaja a través de las redes de paquetes experimenta retardos variables de tiempo para llegar a su destino.

Estas variaciones de retardo se deben a que el ancho de banda se utiliza bajo demanda y de manera compartida, por lo que cuando se requiere mayor uso de ancho de banda, los retardos de transmisión son mayores que cuando se requiere menor ancho de banda.

El jitter entre el punto inicial y final de la comunicación debiera ser inferior a 50 mseg. Si el valor es menor a 50 mseg el jitter puede ser compensado de manera apropiada. En caso contrario debiera ser minimizado.

Para controlar este fenómeno, la solución más ampliamente adoptada es la utilización del "jitter buffer". El jitter buffer consiste básicamente en asignar una pequeña cola o almacén para ir recibiendo los paquetes y sirviéndolos con un pequeño retraso, permitiendo así a las tramas más lentas arrivar a tiempo para ser ubicadas en la secuencia correcta. Si algún paquete no está en el buffer (se perdió o no ha llegado todavía) cuando sea necesario se decarta. Normalmente en los teléfonos IP (hardware y software) se pueden modificar los buffers. Un aumento del buffer implica menos perdida de paquetes pero más retraso. Una disminución implica menos retardo pero más pérdida de paquetes.

Dada estas condiciones, se debe encontrar un tamaño óptimo del buffer que permita controlar el jitter sin aumentar el retardo a niveles excesivos. Algunos equipos comerciales lo ajustan dinámicamente de acuerdo con la variabilidad de la red.

Si la red de datos está bien construida y se toman las precauciones apropiadas, la variabilidad del retardo es normalmente un problema menor y el buffer de jitter no contribuye significativamente al retraso total de extremo a extremo. Es aquí, donde las timestamps de RTP juegan un papel importante, al ayudar a determinar qué el jitter, si lo hubiera, existe dentro de la red.

c) DETERIORO POR EL ECO Y SU CONTROL.

El eco en la red es el resultado del acoplamiento entre el trayecto de transmisión y el de recepción, que hace que el habla saliente vuelva a la persona que la originó. Por lo general, este problema aparece en el contexto de las comunicaciones de PC a teléfono, de teléfono a PC o de teléfono a teléfono, y es causado por los componentes electrónicos de las partes analógicas del sistema que reflejan una parte de la señal procesada. Este eco es problema cuando el retardo completo (ida y vuelta) en la red es mayor que 50 mseg.

Este umbral es subjetivo y varía persona a persona. Un valor de retardo mas allá de 65 mseg será percibido como un verdadero eco (el hablante oirá su propia voz después de haber hablado), entre 30 y 65 mseg el retardo le añadirá a la voz un sonido que se conoce como “túnel” y un valor de retardo por debajo de 30 mseg el efecto es imperceptible.

En las comunicaciones telefónicas, existen dos tipos de eco. Uno tiene alto nivel y poco retardo y se produce en el circuito híbrido de 2 a 4 hilos local; mientras que otro es de bajo nivel y gran retardo y se produce en el circuito separador híbrido remoto.

La intensidad de un eco depende de dos factores: la amplitud de la señal que produce el eco y el tiempo que le toma para volver a la persona que habla. La amplitud es una función de la intensidad del acoplamiento entre los canales de transmisión y de recepción. Es caracterizada como “pérdida del trayecto del eco”, que es la diferencia en nivel (en dB) entre el habla de entrada original y la señal que hace eco. Para una pérdida del trayecto del eco determinada (es decir, un nivel constante), cuanto más prolongado sea el período entre el habla original y el eco que vuelve, más fuerte o perceptible, parecerá el eco

Existen dos posibles soluciones para evitar este efecto tan molesto.

- **Canceladores de eco.**

El control del eco es necesario en la interfaz entre una red de paquetes y una red con conmutación de circuitos en donde pueda haber híbridos. Para ello, se establece la recomendación G.168 de la ITU-T, que define el desempeño de los canceladores de eco.

Los canceladores de eco aprenden como el circuito que tienen conectado refleja la señal proveniente de la WAN. Estos equipos observan y ajustan el filtro adaptable para

reproducir esta reflexión, mejorando así la pérdida del trayecto del eco hasta en 26 – 30 dB. Los ajustes se realizan en menos de medio segundo después de comenzada la conexión.

Los ajustes realizados por el cancelador de eco incluyen el cálculo tanto del retardo de la reflexión como de su amplitud proveniente de los diferentes puntos del circuito: del híbrido del CPE, del teléfono y de cualquier otro punto que genere reflexiones (cambio de calibre de cables, "bridged taps", etc.).

De esta manera, el cancelador de eco aprende las características del circuito que tiene conectado y como ocurre el retorno del eco: la relación amplitud, frecuencia y retardo. Entonces almacena una copia de la señal transmitida, le aplica la respuesta que aprendió, y le substrae a la señal que recibe la señal almacenada, cancelando con esto el eco. Cualquier residuo del eco es removido usando un procesador no lineal, que elimina todas las señales por debajo de cierto umbral.

- **Supresores de eco.**

Para ofrecer un servicio de ToIP, las pasarelas tendrán que procesar el eco generado por la transferencia de dos a cuatro hilos (desadaptación de impedancias), de lo contrario, no será posible utilizar el servicio con equipos analógicos clásicos. Como solución, se están instalando compensadores de eco de alta calidad en la pasarela de la red.

Conocido también como conmutador vocal (ITU-T G.165/168), detecta una señal en el trayecto entrante o saliente, y conmuta la atenuación en el otro trayecto para reducir el nivel de cualquier señal de retorno. Esta técnica de supresión puede usarse en teléfonos con parlantes, audífonos, y microteléfonos inalámbricos, en los que es común el acoplamiento acústico. La conmutación vocal es una función más simple que la compensación de eco, pero es menos transparente a la dinámica de la conversación, y puede sumar sus propios deterioros a la señal de habla.

SUPRESIÓN DE SILENCIO Y RUIDOS.

Es una gran ventaja del empaquetamiento de la voz ya que no se generan paquetes a trasmitir durante pausas en medio de las frases, o silencio de una persona mientras la otra está hablando. Se debe establecer diferencia entre habla y silencio, el no transmitir

paquetes de silencio y la generación de los silencios correspondiente al otro extremo. Con este parámetro activado, se consigue que la transmisión de paquetes (uso de ancho de banda) se reduzca a las situaciones en que los agentes están hablando. El resto del tiempo, cuando no existe voz a transmitir, se libera el ancho de banda.

Considerando este aspecto, se puede afirmar que el tamaño medio de un paquete de voz durante una conversación es de 8 kbps.

De esta forma, aunque realmente el caudal en datos de la voz codificada no requiere grandes anchos de banda, se puede decir que una conversación full-duplex consume máximo 22kbps. Durante una conversación normal por teléfono, sólo en pequeños intervalos ambos locutores hablan simultáneamente, la tecnología actual provee un sistema conocido como supresión de datos en silencio, el cual no envía datos si no hay sonido.

d) PERDIDAS DE PAQUETES.

A menos que la red esté precisamente adaptada a la carga de tráfico de pico, existe una cantidad de paquetes que a veces no llegan a su destino. Esos paquetes perdidos producen lagunas en las comunicaciones vocales, que pueden causar chasquidos, silenciamiento, o un habla ininteligible.

Generalmente, hay dos maneras de perder paquetes. Pueden perderse en nodos de la red a causa de un desborde en la memoria intermedia, o porque un encaminador congestionado los descarta deliberadamente para reducir la congestión. Estos paquetes realmente se pierden, y nunca llegarán a destino. Las interrupciones en la red debidas a dispositivos fuera de servicio o a cortes de las fibras ópticas también pueden causar la pérdida de paquetes. Esos eventos pueden causar grandes pérdidas de paquetes, que se distribuirán entre los diferentes canales virtuales que la red esté cursando en ese momento.

Segundo, los paquetes pueden retrasarse si toman una ruta más larga o pasan tiempo en la cola de un dispositivo, causando una variabilidad en la hora de llegada al extremo receptor. La memoria intermedia de fluctuaciones (jitter buffer) se usa para reducir la variabilidad, reteniendo los paquetes para la entrada al descodificador. La demora introducida por dicha memoria intermedia se sintoniza con la variación prevista del retardo de la red. Esa demora determina el tiempo máximo que un paquete puede tomar para llegar todavía a tiempo para ser descodificado. Los paquetes que lleguen después del retardo

prescrito pierden su turno, y prácticamente se pierden, ya que la operación de la voz no puede aguardar a que aparezcan los paquetes tardíos. La tasa de pérdida de paquetes dependerá de la calidad de las líneas utilizadas y del dimensionamiento de la red. Para que la calidad vocal sea aceptable, dicha tasa de pérdida de paquetes ha de ser menor que el 5 % en WAN y el 2 % en LAN.

El fax no incorpora procedimientos de recuperación de errores, sin embargo muchos errores no son notorios ante el ojo humano y la degradación no molesta.

En el caso del habla, si la voz es comprimida, la pérdida de información se convierte en un gran problema, ya que puede ocurrir que varios fonemas se pierdan y de ocurrir varias perdidas puede resultar en la degradación de la calidad de la voz. Cada paquete IP contiene entre 40 y 80 ms. de voz, que corresponde a la duración de unidades fundamentales de voz, como son los fonemas: cuando se pierde un paquete, se pierde un fonema. Aunque el cerebro humano es capaz de reconstruir algunos fonemas perdidos, demasiadas pérdidas pueden generar una señal ininteligible.

Medidas para evitar paquetes perdidos y datos faltantes.

- Protocolos QoS.

La ejecución de protocolos de QoS en la red facilita la transmisión de paquetes vocales en las diversas pasarelas y encaminadores, reduciendo las fluctuaciones y la pérdida resultante de paquetes.

La eficacia de esto es mayor si la red está cursando una proporción considerable de tráfico de datos. Si la red cursa una proporción elevada de tráfico vocal, podrá todavía haber demoras de colas en los encaminadores, con el consiguiente aumento de las fluctuaciones y las pérdidas de paquetes.

- Control de admisión de llamadas.

En las redes con una alta proporción de tráfico vocal, el control de admisión de llamadas puede prevenir la congestión limitando el número de llamadas activas a través de diversos nodos de la red. Esto es análogo a la “señal rápida de ocupado” en la red con conmutación de circuitos. Cuando no hay control de admisión de llamadas y el número de

llamadas aumenta por encima de la utilización recomendada, la calidad de las llamadas en la red declina a medida que aumentan el retardo, la fluctuación y la pérdida de paquetes.

- Memoria intermedia adaptable de fluctuaciones.

Cuando un paquete vocal llega a destino, es retenido en la memoria intermedia de fluctuaciones hasta que el descodificador está listo para el paquete. Los paquetes tardíos son descartados. Un aumento en la tasa de pérdida de paquetes en el descodificador puede significar que hay más paquetes que llegan tarde. Se puede usar un algoritmo adaptable para ajustar el retardo de la memoria intermedia de fluctuaciones según aumenta y disminuye la tasa de pérdida de paquetes. La memoria intermedia es ajustada durante los períodos de silencio, de manera que el desplazamiento temporal de la señal es transparente para los usuarios.

- Envío de datos duplicados.

El envío de datos redundantes también corrige la pérdida de paquetes vocales. Para emplear esta solución, la información de un paquete es copiada al paquete siguiente de la secuencia, y se usa si el paquete original se pierde o se retrasa. Con algunos codecs, tales como el G.729, incluso los datos incompletos pueden ser útiles para reparar la laguna. Como la descodificación de los datos duplicados debe aguardar la llegada de otro paquete si se pierde el original, este método de supresión de pérdidas agrega un retraso más.

- Tasa de pérdida de paquetes.

Esta variable mide el comportamiento del enlace para detectar congestión. Como se ha mencionado inicialmente, IP es un protocolo de transporte basado en el paradigma del mejor esfuerzo “Best Effort”, que no garantiza que un paquete que es transportado por una red IP llegue finalmente a su destino. Es estos términos, la tasa de pérdida de paquetes mide cuantitativamente este factor.

Usualmente en un enlace usado como subred de interconexión no deben observarse pérdidas mayores al 1% salvo que el circuito este congestionado o que existan problemas a nivel de transmisión Física, o que los nodos (routers) extremos estén sobrecargados.

Para medir la pérdida de paquetes se usa también ICMP (Internet Control Message Protocol), enviando un número finito de paquetes, y contabilizando el número de paquetes recibidos desde la interfase remota. Estos resultados son posteriormente presentados en forma gráfica. Al igual que la latencia, la tasa de pérdida de paquetes es una variable muy importante a considerar en el análisis de aplicaciones de VoIP, y en las aplicaciones relacionadas con la distribución de audio y video en tiempo real, sobre redes de datos.

e) REQUERIMIENTOS DE ANCHO DE BANDA.

Una llamada telefónica ocupa un ancho de banda de unos 32 kb. Este ancho de banda debe estar disponible para que la comunicación sea fluida. Si la línea de datos se satura repentinamente, puede deteriorarse la calidad o incluso cortarse la llamada. Además puede ser determinante el tiempo de latencia, para evitar el efecto de retardo en la conversación, este efecto no será perceptible si la latencia es inferior a 50 ms, pero si es superior, puede hacerse molesto. Un remedio a estos problemas consiste en contratar con nuestro proveedor de comunicaciones lo que se denomina “calidad de servicio, QoS”, que garantiza que siempre hay un determinado ancho de banda disponible para la telefonía.

Cabe recordar que conforme el ancho de banda disminuye, la calidad de sonido se degrada en mayor grado. Es por ello que la elección de la codificación que vaya a implementarse en la red deberá tomar en cuenta esta consideración.

Tabla. 1.7. Anchos de banda de codecs

Codec de Audio	Ancho de banda comprimido	Ancho de banda paquetizado	Ancho de banda en Ethernet
G723	6,3 Kbps	17 Kbps	27,2 Kbps
G729	8 Kbps	24 Kbps	28,8 Kbps
G711	64 Kbps	74,6 Kbps	84,7 Kbps
FAX	4,8 Kbps	12,8 Kbps	20,4 Kbps

Habitualmente en un entorno LAN, donde se utiliza tecnología Switch a 10 o 100Mbps, se elige la compresión G711 con un ancho de banda de 84,7kbps. ya que se obtiene mayor calidad y se dispone suficiente ancho de banda. En cambio en el entorno WAN donde el ancho de banda sea más escaso y costoso, se elige la compresión G723 con un ancho de banda de 27,2kbps.

El ancho de banda puede reducirse 30 a 40% cuando se utiliza detección de silencios (VAD).

Y en las líneas WAN, los Routers pueden utilizar la compresión de cabeceras IP (cRTP) para reducir las cabeceras de 40 a 24 bytes, pudiendo reducir hasta 16,41kbps en el caso del G723.

1.6. CONTROL DE CONGESTIÓN [11]

Existen varios niveles en los cuales se puede proveer de calidad de servicio en una red IP. Uno de ellos es el de contar con una estrategia de manejo de los paquetes en caso de congestión, o el evitar que la red alcance este estado, descartando paquetes a medida que estos ingresan a la red.

El "manejo de congestión" es un término general usado para nombrar los distintos tipos de estrategia de encolamiento que se utilizan para manejar situaciones donde la demanda de ancho de banda solicitada por las aplicaciones excede el ancho de banda total de la red, controlando la inyección de tráfico a la red, para que ciertos flujos tengan prioridad sobre otros.

1.6.1. MECANISMOS DE PREVISIÓN DE LA CONGESTIÓN [11]

a) RED (RANDOM EARLY DETECTION).

RED es un mecanismo de gestión activa de cola que trata de evitar la congestión eliminando paquetes aleatoriamente. El descarte de un simple paquete es suficiente para indicar que existe congestión a los protocolos de nivel de transporte del cliente, ya que cuando se descarta un paquete, el nodo envía un aviso implícito a la fuente TCP que lo envió indicándole que el paquete descartado sufrió congestión en algún punto del camino hacia el destino TCP. Como respuesta a este aviso implícito, la fuente TCP reducirá su ritmo de transmisión (volviendo a un comienzo lento ó recuperación rápida cuando desaparezca la congestión) de modo que la cola del nodo no se sature.

Las ventajas que aporta la gestión activa de cola RED son entre otras:

• Identifica los estados tempranos de congestión y responde descartando aleatoriamente paquetes. Si la congestión continua creciendo, RED descarta paquetes de

forma más agresiva para prevenir que la cola alcance el 100 por ciento de su capacidad, lo cual resultaría en una pérdida total de servicio. Esto permite a RED mantener un cierto nivel máximo de tamaño medio de cola incluso con los protocolos de transporte no cooperativos.

• Gracias a que RED no espera hasta que la cola esté completamente llena para comenzar a descartar paquetes, la cola puede aceptar ráfagas de tráfico y no descartar todos los paquetes de la ráfaga. Así, RED es apropiado para TCP porque no descarta grupos de paquetes de una única sesión TCP ayudando así a evitar la sincronización global de TCP.

• Permite mantener la cantidad de tráfico en la cola a nivel moderado. Ni demasiado bajo, lo que causaría que el ancho de banda estuviese infrautilizado, ni con valores cercanos a la capacidad máxima, donde el excesivo descarte de paquetes provocaría que una gran cantidad de sesiones TCP redujera sus tasas de transmisión, llevando a una pobre utilización del ancho de banda. Así, RED permite mantener el nivel de tráfico en cola de modo que se pueda obtener la mejor utilización del ancho de banda.

Las limitaciones de la gestión activa RED son:

• Puede ser muy difícil de configurar para obtener un funcionamiento predecible.

• RED no es apropiado para flujos no TCP tales como ICMP (*Internet Control Message Protocol*) ó UDP (*User Datagram Protocol*), ya que estos no detectan el descarte de paquetes y continuarían transmitiendo al mismo ritmo, perdiendo gran cantidad de paquetes debido a la congestión de la red.

• Existen algunos problemas en el uso e implementación de RED. Uno de ellos es que no tiene en cuenta las prioridades de los flujos a la hora de descartar, de modo que puede darse el caso de que se descarten paquetes de más prioridad mientras se estén sirviendo los de baja prioridad.

Este sistema podría utilizarse para gestionar una cola para tráfico Best Effort, ya que todos los flujos tendrán igual prioridad y el problema de RED de no distinguir prioridades no sería un inconveniente en este caso.

b) WRED (WEIGHTED RANDOM EARLY DETECTION).

Es una extensión de RED en la que se permite mantener un algoritmo RED diferente para cada tipo de tráfico dentro de la cola, teniendo en cuenta la prioridad de éstos.

Trabaja monitoreando la carga de tráfico en algunas partes de las redes y descarta paquetes en forma random si la congestión aumenta. Está diseñada para aplicaciones TCP debido a la posibilidad de retransmisión. Esta pérdida en la red obliga a TCP a un control de flujo reduciendo la ventana e incrementándola luego en forma paulatina. Un proceso de descarte generalizado, en cambio, produce la retransmisión en "olas" y reduce la eficiencia de la red.

La versión ponderada WRED realiza el drop de paquetes de forma que no afecta al tráfico de tipo RSVP. Una versión superior debería considerar el tráfico de aplicación.

1.6.2. MECANISMOS DE GESTIÓN DE LA CONGESTIÓN [11]

a) FIFO (First In First Out).

Es el tipo más simple de encolamiento, se basa en el siguiente concepto: el primer paquete en entrar a la interfaz, es el primero en salir. Es adecuado para interfaces de alta velocidad, sin embargo no para bajas, ya que FIFO es capaz de manejar cantidades limitadas de ráfagas de datos. Si llegan más paquetes cuando la cola está llena, éstos son descartados. No tiene mecanismos de diferenciación de paquetes, tratando a todos los flujos por igual, ya que el retardo medio de cola aumenta para todos los flujos a medida que la cogestión aumenta. Esto hace es especialmente perjudicial para las aplicaciones de tiempo real que sufrirán mayores retardos, jitters y pérdidas.

Otra característica, durante los periodos de congestión, el encolamiento FIFO beneficia a los flujos UDP sobre los TCP. Cuando se produce una pérdida de paquete debido a la congestión, las aplicaciones basadas en TCP reducen su tasa de transmisión, pero las aplicaciones basadas en UDP continúan transmitiendo paquetes al mismo ritmo que antes sin percatarse de la pérdida de paquetes.

b) FQ (Fair Queuing).

Generalmente conocida como WFQ (*Weighted Fair Queueing*), es un método automatizado que provee una justa asignación de ancho de banda para todo el tráfico de la red, utilizado habitualmente para enlaces de velocidades menores a 2048 [Mbps]. WFQ ordena el tráfico en flujos, utilizando una combinación de parámetros. Por ejemplo, para una conversación TCP/IP, se utiliza como filtro el protocolo IP, dirección IP fuente, dirección IP destino, puerto de origen, etc. Una vez distinguidos estos flujos, el enrutador determina cuáles son de uso intensivo o sensibles al retardo, priorizándolos y asegurando que los flujos de alto volumen sean empujados al final de la cola, y los volúmenes bajos, sensibles al retardo, sean empujados al principio de la cola. WFQ es apropiado en situaciones donde se desea proveer un tiempo de respuesta consistente ante usuarios que generen altas y bajas cargas en la red, ya que WFQ se adapta a las condiciones cambiantes del tráfico en la red.

Sin embargo, la carga que significa para el procesador en los equipos de enrutamiento, hace de esta metodología poco escalable, al requerir recursos adicionales en la clasificación y manipulación dinámica de las colas.

c) PQ (Priority Queuing).

El Encolamiento de Prioridad (PQ), consiste en un conjunto de colas, clasificadas desde alta a baja prioridad. Cada paquete es asignado a una de estas colas, las cuales son servidas en estricto orden de prioridad. Las colas de mayor prioridad son siempre atendidas primero, luego la siguiente de menor prioridad, y así. Si una cola de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente. Este mecanismo se ajusta a condiciones donde existe un tráfico importante, pero puede causar la total falta de atención de colas de menor prioridad (starvation).

d) CQ (Custom Queuing).

Para evadir la rigidez de PQ, se opta por utilizar Encolamiento Personalizado (CQ). Permite al administrador priorizar el tráfico sin los efectos laterales de inanición de las colas de baja prioridad, especificando el número de paquetes o bytes que deben ser atendidos para cada cola. Se pueden crear hasta 16 colas para categorizar el tráfico, donde

cada cola es atendida al estilo Round-Robin. CQ ofrece un mecanismo más refinado de encolamiento, pero no asegura una prioridad absoluta como PQ. Se utiliza CQ para proveer a tráficos particulares de un ancho de banda garantizado en un punto de posible congestión, asegurando para este tráfico una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles.

e) CBWFQ (Class Based WFQ).

WFQ tiene algunas limitaciones de escalamiento, ya que la implementación del algoritmo se ve afectada a medida que el tráfico por enlace aumenta; colapsa debido a la cantidad numerosa de flujos que analizar. CBWFQ fue desarrollada para evitar estas limitaciones, tomando el algoritmo de WFQ y expandiéndolo, permitiendo la creación de clases definidas por el usuario, que permiten un mayor control sobre las colas tráfico y asignación del ancho de banda.

Algunas veces es necesario garantizar una determinada tasa de transmisión para cierto tipo de tráfico, lo cual no es posible mediante WFQ, pero si con CBWFQ. Las clases que son posibles implementar con CBWFQ pueden ser determinadas según protocolo, ACL, valor DSCP, o interfaz de ingreso. Cada clase posee una cola separada, y todos los paquetes que cumplen el criterio definido para una clase en particular son asignados a dicha cola. Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados. Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. Se puede configurar específicamente el ancho de banda y límite de paquetes máximos (o profundidad de cola) para cada clase. El peso asignado a la cola de la clase es determinado mediante el ancho de banda asignado a dicha clase.

f) LLQ (Low Latency Queuing).

El Encolamiento de Baja Latencia (LLQ) es una mezcla entre PQ y CBWFQ. Es actualmente el método de encolamiento recomendado para ToIP, que también trabajará apropiadamente con tráfico de videoconferencias. LLQ consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas.

Si existe tráfico en la cola de prioridad, ésta es atendida antes que las otras colas de prioridad personalizadas. Si la cola de prioridad no está encolando paquetes, se procede a atender las otras colas según su prioridad. Debido a este comportamiento es necesario configurar un ancho de banda límite reservado para la cola de prioridad, evitando la inanición del resto de las colas. La cola de prioridad que posee LLQ provee de un máximo retardo garantizado para los paquetes entrantes en esta cola, el cual es calculado como el tamaño del MTU dividido po la velocidad de enlace.

1.7 GESTION DEL ANCHO DE BANDA

Para la gestión del ancho de banda existen los siguientes mecanismos de señalización con QoS:

- Servicios Integrados (IntServ).
- Servicios Diferenciados (DiffServ o DS).
- MPLS (Multi Protocol Label Switching).

1.7.1 SERVICIOS INTEGRADOS (IntServ) [11]

La arquitectura de Internet de IntServ, parte de las premisas de seguir utilizando el protocolo IP y de ofrecer servicio tanto “mejor esfuerzo” como servicios de tiempo real. La idea fundamental de esta arquitectura radica en que las aplicaciones se ven como un flujo dentro de la Internet y por cada flujo se deberá crear un estado (soft state) en cada uno de los enrutadores. En estos estados se realiza la reserva de los recursos necesarios para ofrecer QoS a las aplicaciones.

IntServ, se basa en el protocolo RSVP (Resource ReSerVation Protocol, RFC 1633), que implica una reserva de recursos en la red para cada flujo de información de usuario, así como el mantenimiento en la red (en los routers) de un estado para cada flujo, esto es, mantenimiento de la “reserva” (tablas de estados de reserva). Esto conduce a un considerable tráfico de señalización y ocupación de recursos en cada router para cada flujo, con la consiguiente complejidad en el hardware, al margen del aporte que esta señalización hace a la congestión de la red. No es una solución escalable, no es una solución adecuada

para grandes entornos como Internet, aunque si lo es para entornos más limitados y también para redes de acceso al backbone.

El modelo de Servicios Integrados esta implementado por 4 componentes:

a) Control de admisión: El control de admisión implementa el algoritmo de decisión para determinar si se puede admitir un nuevo flujo sin afectar a los que ya estaban asignados. Se invoca en cada nodo para hacer una decisión de aceptación/rechazo local para cada terminal que solicita un servicio de tiempo real a lo largo de un camino de la red. El algoritmo de admisión tiene que ser consistente con el modelo de servicio, y forma parte lógicamente del control de tráfico. El control de admisión se confunde a menudo con la política de admisión, que es una función que se realiza paquete a paquete en los "bordes" de la red para asegurar que un terminal no viola las características de tráfico comprometidas. La política de admisión se considerada como parte del organizador de paquetes.

b) Clasificador: Clasifica los paquetes dentro de alguna clase. La elección de una determinada clase puede estar basada en los contenidos de la cabecera y/o en algún número de clasificación adicional añadido en cada paquete. Una clase puede corresponder a una amplia gama de flujos, por ejemplo, todos los flujos de vídeo o todos los flujos provenientes de una determinada organización. Por otro lado, una clase puede contener un solo flujo. Una clase es una abstracción que puede ser local a cada uno de los encaminadores; el mismo paquete puede ser clasificado de forma diferente en diferentes encaminadores a lo largo del camino.

c) Organizador de paquetes: El organizador de paquetes gestiona el envío de diferentes secuencias de paquetes usando un conjunto de colas y otros mecanismos como temporizadores. Uno de los organizadores más utilizados en el modelo de Servicios Integrados es el WFQ, aunque para las partes de la red que se sabe que están siempre poco cargadas se usan mecanismos más sencillos como las colas FIFO.

d) Protocolo de reserva de recursos: Se utiliza para crear y mantener estados específicos de flujo en los terminales y en los encaminadores presentes en el camino de un flujo y debe estar implementado en todos ellos. Aunque en las especificaciones del

protocolo no se cierra la posibilidad de usar otros protocolos, el recomendado por la comunidad internacional es el RSVP.

TIPOS DE SERVICIOS DEFINIDOS EN IntServ.

Los tres tipos de servicios que se han aprobado hasta ahora en el Modelo de Servicios Integrados son:

• Servicio de mejor esfuerzo ó Best Effort: Es el servicio que se le suele asignar al tráfico de las aplicaciones elásticas. La red no promete nada, pero trata de entregar los paquetes tan pronto como sea posible. En cada momento, la velocidad de transferencia depende del ancho de banda disponible en la red. Todos los flujos de tiempo-real que no hayan hecho una reserva de recursos también se transmiten con el servicio de mejor-esfuerzo.

• Servicio Garantizado (GS): Es usado por las aplicaciones rígidas intolerantes. Proporciona un límite firme en el retardo y la ausencia de pérdida de paquetes para un flujo que se ajuste a sus especificaciones de tráfico. El servicio garantizado no intenta minimizar el jitter, tan solo controla el retardo máximo de las colas de espera. Las aplicaciones de tiempo real, una vez conocido este retardo máximo, fijan su punto de reproducción de forma que todos los paquetes lleguen a tiempo. El retardo instantáneo para la mayoría de los paquetes será mucho menor que el retardo garantizado, por lo que los paquetes deben almacenarse en el receptor antes de ser reproducidos.

• Servicio de Carga Controlada (CL): diseñado para las aplicaciones adaptativas y tolerantes. No se dan garantías cuantitativas, simplemente se asegura que el servicio en condiciones de sobrecarga es aproximadamente tan bueno como el servicio de “mejor esfuerzo” en redes ligeramente cargadas. Una fuente de datos proporciona a la red las especificaciones del tráfico que va a generar. La red asegura que habrá suficientes recursos disponibles para ese flujo, siempre y cuando el flujo siga ajustándose a las especificaciones dadas. El servicio dado a los paquetes que se ajustan a las especificaciones se caracteriza por retardos pequeños y escasas pérdidas de paquetes. Los retardos de colas no son significativamente más grandes que el tiempo que se tarda en vaciar una ráfaga de tamaño máximo a la velocidad demandada. Puede haber pérdidas de paquetes ocasionales debidas

a efectos estadísticos, pero la tasa de pérdidas total no debe exceder demasiado la tasa de errores de paquetes básica del medio de transmisión.

RSVP (RESOURCE RESERVATION PROTOCOL).

RSVP es un protocolo que se desarrolla entre los usuarios y la red, y entre los diferentes nodos (routers) de la red que soportan este protocolo. Consiste en hacer "reservas" de recursos e n dichos nodos para cada flujo de información de usuario, con la consecuente ocupación de los mismos. Esto requiere, lógicamente, intercambio de mensajes RSVP entre dichos entes funcionales, así como "mantener" estados de reserva en cada nodo RSVP. De manera que tanto la solicitud de las reservas, como el mantenimiento de éstas durante la comunicación, y la posterior cancelación, implica el intercambio de mensajes de señalización, lo que representa un tráfico considerable cuando de entornos como Internet se trata.

Las características más importantes del RSVP son:

• El RSVP hace reservas para aplicaciones: unicast y multicast, adaptándose dinámicamente las alteraciones de los miembros de un grupo o de rutas.

• El RSVP es simplex, solo reserva recursos para flujos unidireccionales. Para tener reserva bidireccional se debe solicitar dos consultas RSVD de ambos sentidos.

• El que inicia y mantiene las reservas en RSVP son los receptores llamados (*receiverinitiated*).

• El estado de las reservas es "leve" (soft-sate), o sea después de un intervalo de tiempo la reserva se vence, para lo cual todos lo receptores constantemente deben actualizar la solicitud de reservas para mantener el canal de comunicación.

• El RSVP no es un protocolo de enrutamiento, sino que usa la ruta escogida por cualquier protocolo de enrutamiento de uso actual o de uso futuro.

• El RSVP transporta y mantiene información sobre el control de tráfico y control de políticas que son tratados por otros módulos.

• El RSVP ofrece varios estilos de reserva, para adaptarse a una gran variedad de aplicaciones y usos.

• Los routers que no implementan RSVP pueden funcionar perfectamente en las transmisiones de la red.

• El RSVP soporta IPv4 e IPv6.

RSVP se ha diseñado para permitir a los emisores, receptores y routers de las sesiones de comunicación (tanto multicast como unicast) comunicarse con el resto para establecer una ruta que pueda soportar la calidad de servicio requerida. La calidad de servicio viene especificado en un flowspec.

1.7.2. SERVICIOS DIFERENCIADOS (DiffServ o DS) [11]

A diferencia de la arquitectura de servicios integrados, en donde es necesario hacer una reservación del canal, de manera análoga al servicio telefónico, y en donde existe una señalización para mantener la reservación, en la arquitectura de servicios diferenciados, los paquetes son clasificados únicamente en el dispositivo de acceso a la red, y ya dentro de la red, el tipo de procesamiento que reciban los paquetes va a depender del contenido del encabezado.

Los servicios diferenciados (DS) proporcionan mecanismos de calidad de servicio para reducir la carga en dispositivos de la red a través de un mapeo entre flujos de tráfico y niveles de servicio. Los paquetes que pertenecen a una determinada clase se marcan con un código específico (DSCP – DiffServ CodePoint). Este código es todo lo que necesitamos para identificar una clase de tráfico. La diferenciación de servicios se logra mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, hecho conocido como PHB (Per Hop Behavior).

De esta manera a través de DS se asignan prioridades a los diferentes paquetes que son enviados a la red. Los nodos intermedios (routers) tendrán que analizar estos paquetes y tratarlos según sus necesidades. Esta es la razón principal por la que DS ofrece mejores características de escalabilidad que IntServ. Dentro del grupo de trabajo de DiffServ de la IETF, se define en el campo DS (Differentiated Services) donde se especificarán las prioridades de los paquetes. En el subcampo DSCP (Differentiated Service CodePoint) se

especifica la prioridad de cada paquete. Estos campos son validos tanto para IPv4 como IPv6.

ARQUITECTURA.

La arquitectura DiffServ es la propuesta del IETF para solucionar problemas asociados a IntServ. La solución consiste básicamente en agrupar los flujos de tráfico IP en agregados, dentro de los cuales, los paquetes de un agregado serán tratados de la misma forma en cada nodo.

Este tratamiento realizado salto a salto se denomina Per-hop behavior (PHB), que se corresponden con distintos niveles de:

• Prioridad de servicio. Determina que paquete se atiende en primer lugar de todos los que están esperando a ser transmitidos por el enlace.

• Prioridad de descarte. En el interior de los nodos los paquetes son almacenados en buffers de tamaño finito. Como consecuencia de esto, cuando se agota su capacidad hay que proceder al descarte de uno o más paquetes. La prioridad de descarte permite cuales son los paquetes que se van a descartar cuando se produzca esta situación.

Cada grupo PHB al que pertenecen paquetes se codifica en un campo de su cabecera llamado en DS y su valor determina el tratamiento que se le debe dar a ese paquete en cada tramo de la red.

PER HOP BEHAVIORS (PHB).

La RFC 2475 define PHB como el comportamiento de “fordwaring” observable externamente aplicado en un nodo DiffServ hacia un DiffServ Behavior Aggregate (BA).

Con la capacidad del sistema de marcar paquetes de acuerdo al parámetro DSCP, los conjuntos de paquetes con el mismo DSCP y enviados en una determinada dirección pueden agruparse en un BA. Paquetes provenientes de fuentes múltiples o diversas aplicaciones, por tanto, pueden pertenecer al mismo BA.

En otras palabras, un PHB se refiere a la planificación del paquete, el encolamiento, la política, de un nodo en cualquier paquete dado perteneciente a un BA.

Existen cuatro estándares disponibles de PHBs especificados para ser usados dentro de una red de servicios diferenciados:

• Default PHB (PHB por defecto o Best Effort, RFC 2474);

• Class-Selector PHB (PHB selector de clases, RFC 2474);

• Assured Forwarding PHB (PHB tránsito asegurado, RFC 2597);

• Expedited Forwarding PHB (PHB tránsito expedito, RFC 2598).

La IETF se ha centrado en la especificación de estos dos últimos tipos de PHBs, dadas sus características.

CLASIFICADORES.

El clasificador tiene como función el clasificar el tráfico entrante de acuerdo con los perfiles de los clientes y reenviar los flujos al gestor correspondiente AF, EF ó BE.

Para ello, el clasificador toma un flujo de tráfico simple como entrada y le aplica una serie de filtros. Cada filtro representa un determinado perfil de cliente y tendrá un gestor de servicios asociado. A la salida de cada filtro tendremos un flujo de tráfico formado por los paquetes que hayan pasado el filtro. Este flujo se enviará al gestor de servicios que tenga asociado el filtro.

Un filtro consiste en un conjunto de condiciones sobre los valores que componen el paquete que se consideren claves para su clasificación.

Dos de los clasificadores más usados son el Clasificador BA (Behaviour Aggegate) para los nodos interiores y el Clasificador Multi-Field ó MF para los nodos frontera.

a) Clasificador BA.

Este tipo de clasificador, usa solamente los DSCP de la cabecera IP de los paquetes para determinar el flujo de salida lógico hacia el cual el paquete debería ser dirigido.

Cada filtro BA estará configurado con un valor DSCP y solo dejará pasar los paquetes marcados con este DSCP.

b) Clasificador MF.

Los clasificadores MF clasifican paquetes basándose en uno o más campos del paquete (entre los que puede estar el DSCP). Un tipo común de clasificador MF es el llamado '6-tuple' que clasifica basándose en 6 campos de las cabeceras IP y TCP o UDP (dirección destino, dirección origen, protocolo IP, puerto origen, puerto destino, y DSCP). Los clasificadores MF pueden clasificar también basándose en otros campos como las direcciones MAC, etiquetas VLAN, campos de clases de tráfico de capa de enlace o campos de protocolos de capas más altas, pero el '6-tuple' es el más usado.

NODOS DS.

En la arquitectura definida por Diffserv aparecen nodos extremos DS de entrada y salida, así como nodos DS internos. Este conjunto de nodos definen el dominio Diffserv y presenta un tipo de políticas y grupos de comportamiento por salto (PHB) que determinarán el tratamiento de los paquetes en la red.

Veamos a continuación las diferentes funciones que deben realizar los nodos DS:

a) Nodos extremos DS.

Será necesario realizar diferentes funciones como el acondicionamiento de tráfico entre los dominios Diffserv interconectados. De esta manera debe clasificar y establecer las condiciones de ingreso de los flujos de tráfico en función de: dirección IP y puerto (origen y destino), protocolo de transporte y DSCP, este clasificador se conoce como MF (Multi-Field Classifier). Una vez que los paquetes han sido marcados adecuadamente, los nodos internos deberán seleccionar el PHB definido para cada flujo de datos.

Los nodos DS de entrada serán responsables de asegurar que el tráfico de entrada cumple los requisitos de algún TCA (Traffic Conditioning Agreement), que es un derivado del SLA, entre los dominios interconectados. Por otro lado los nodos DS de salida deberán realizar funciones de acondicionamiento de tráfico o TC (Traffic Conformation) sobre el tráfico transferido al otro dominio DS conectado.

b) Nodos internos DS.

Podrá realizar limitadas funciones de TC, tales como remarcado de DSCP. Los nodos DS internos solo se conectan a nodos internos o a nodos externos de su propio dominio. A diferencia de los nodos externos para la selección del PHB solo ser tendrá en cuenta el campo DSCP, conocido como clasificador BA (Behavior Aggregate Classifier).

ANÁLISIS DE LOS ROUTERS DS.

Una red de Servicios Diferenciados es un dominio que comprende un conjunto de dispositivos. Este dominio puede tener acceso otros elementos de red fuera de él.

Los tipos de routers en redes DS se clasifican así:

• First Hop Router: es el router más próximo al host emisor de paquetes. Los flujos de paquetes son clasificados y marcados acorde a la etiqueta SLA (Service Level Agreement). Es responsable de que el tráfico esté acorde con el ancho de banda del perfil.

• Ingrees Router: se sitúan en los puntos de entrada al backbone DiffServ (dominio DS), efectuando la clasificación de los paquetes en base al campo DS o en base a múltiples campos de la cabecera de éstos.

• Egress Router: se ubican en los puntos de salida de redes DiffServ (dominio DS), controlando el tráfico. Efectúan la clasificación de paquetes en base solo al campo DS de las cabeceras.

• Interior router: tienen la misión de "sumar" flujos, realizar la clasificación DS y reenvío de paquetes. Se sitúan dentro del backbone DS (dominio DS).

1.7.3 MPLS (MULTI PROTOCOL LABEL SWITCHING) [11]

El protocolo de conmutación por etiquetas multiprotocolo (MPLS) surgió en los últimos años de la década de los 90 como una arquitectura que debiera permitir mejorar la performance de las redes IP. Sin embargo, actualmente su interés radica en sus aplicaciones a redes privadas virtuales, a Ingeniería de Tráfico y a QoS sobre IP.

El principal objetivo que se persigue con MPLS es conseguir una red IP que trabaje directamente sobre tecnologías de transporte de datos (sin capas intermedias que reduzcan el rendimiento) y donde la calidad de servicio y la gestión de tráfico se proporcionen a través de tecnologías de capa IP, es decir, pretende tener las ventajas que ofrecía ATM evitando sus desventajas.

Gracias a ello, los usuarios empresariales pueden obtener el recorte de costos que ofrece una infraestructura de red compartida y beneficiarse simultáneamente de un tráfico con unos niveles garantizados de latencia, pérdidas de paquetes y fluctuación de fase (jitter), algo crucial para aplicaciones en tiempo real como la ToIP.

Cisco Systems ha sido una empresa pionera al proporcionar una solución pre-estandarizada MPLS a la conmutación por etiquetas. Así también respondiendo a esta necesidad de los clientes, Telmex (empresa de servicios IP) ofrece su servicio de Ancho de Banda por Demanda, que saca partido a las capacidades de administración de su plataforma de conectividad IP MPLS, para entregar a sus clientes de Redes Corporativas los anchos de banda diferenciados que se ajusten a la temporalidad de sus requerimientos específicos.

NODOS LSRs y LERs.

La arquitectura de una red MPLS está definida en el RFC 3031. Los dispositivos que participan en los mecanismos del protocolo MPLS pueden ser clasificados en enrutadores de etiqueta de borde o Label Edge Routers (LERs), y en ruteadores de conmutación de etiquetas o Label Switching Routers (LSRs).

• Un LSR es un dispositivo ruteador de alta velocidad, que dentro del núcleo de una red MPLS, participa en el establecimiento de las LSPs, usando el protocolo de señalización apropiado y una conmutación de alta velocidad aplicado al tráfico de datos, que se basa en las trayectorias establecidas.

• Un LER es un dispositivo que opera en el borde de una red de acceso hacia una red MPLS. Un LER soporta múltiples puertos conectados a diferentes tipos de redes (por ejemplo, frame relay, ATM, Ethernet); y se encarga, en el ingreso de establecer una LSP para el trafico en uso y de evitar este trafico hacia la red MPLS, usando el protocolo de señalización de etiquetas, y en egreso de distribuir de nuevo el trafico hacia la red de

acceso que corresponda. El LER juega un papel muy importante en la asignación y remoción de etiquetas que se aplica al tráfico que entra y sale de una red MPLS.

FEC.

Una clase de envío equivalente o Forwarding Equivalence Class (FEC), es una representación de un grupo de paquetes que comparten los mismos requerimientos para su transporte; todos los paquetes de este gripo tienen el mismo trato en la ruta hacia su destino. Al contrario de lo que pasa en el tradicional envío de paquetes en IP, en MPLS, la asignación de un paquete a una FEC en particular se realiza solo una vez, en el momento en el que paquete entra a la red.

La definición de una FEC se basa en los requerimientos de servicio que posea un conjunto de paquetes dado, o simplemente por el prefijo de una dirección IP. Cada LSR construye una tabla para especificar que paquete debe ser enviado; esta tabla, llanada base de información de etiquetas (LIB), se construye con uniones FEC/etiqueta.

FUNCIONAMIENTO BÁSICO DE MPLS.

Una MPLS consiste de un conjunto de LSR que tienen la capacidad de conmutar y rutear paquetes en base a la etiqueta que se ha añadido a cada paquete. Cada etiqueta define un flujo de paquetes entre dos puntos finales. Cada flujo es diferente y es llamado FEC, así como también cada flujo tiene un camino específico a través de los LSR de la red, es por eso que se dice que la tecnología MPLS es “orientada a conexión”. Cada FEC, además de la ruta de los paquetes contiene una serie de caracteres que define los requerimientos de QoS del flujo. Los routers de la red MPLS no necesitan examinar ni procesar el encabezado IP, solo es necesario reenviar cada paquete dependiendo el valor de su etiqueta. Esta es una de las ventajas que tiene los routers MPLS sobre los routers IP, en donde el proceso de reenvió es más complejo.

En un router IP cada vez que se recibe un paquete se analiza su encabezado IP para compararlo con la tabla de enrutamiento (routing table) y ver cual es el siguiente salto (next hop). El hecho de examinar estos paquetes en cada uno de los puntos de tránsito que deberán recorrer para llegar a su destino final significa un mayor tiempo de procesamiento en cada nodo y por lo tanto, una mayor duración en el recorrido.

FORMATO CABECERA MPLS.

La cabecera MPLS se compone de los campos Etiqueta MPLS, EXP ó experimental (antes conocido como CoS.), S ó Stack que se usa para apilar etiquetas de forma jerárquica y TTL (Time To Live), que sustenta la funcionalidad estándar TTL de las redes IP.

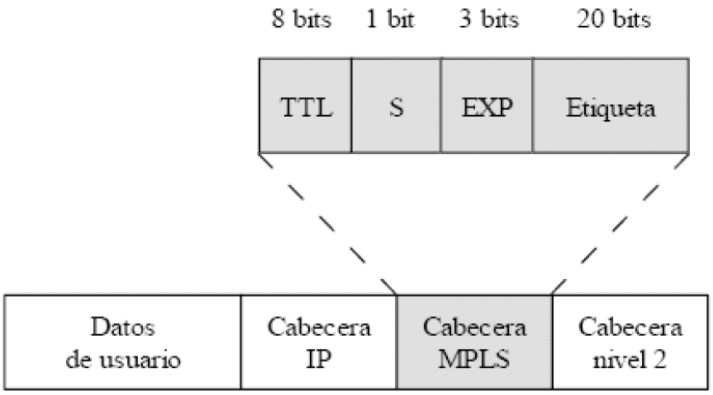


Figura. 1.21. Cabecera MPLS

La cabecera MPLS está conformada por 32 bits, divididos como se muestra en la figura anterior, y contiene los siguientes elementos:

• Valor de la etiqueta: Etiqueta de 20 bits con valor local.

• Experimental (EXP): Son los 3 bits siguientes reservados para uso experimental. Se podría especificar en estos bits el PHB del salto.

• Pila (S o Stack): Es el bit de posición de pila:

Cuando es "1"denota que es la entrada más antigua en la pila.

Cuando es "0" denota que es cualquier otra entrada.

• Tiempo de vida (TTL o Time To Live): Es un campo de 8 bits, y se utilizan para codificar el valor del conteo de saltos (IPv6) o de tiempo de vida (IPv4).

MECANISMOS DE SEÑALIZACIÓN.

• Petición de Etiquetas (label request): usando este mecanismo, un LSR hace una petición de etiqueta a su vecino downstream, de manera que la pueda unir a una FEC específica. Este mecanismo puede ser empleado por toda la cadena de LSRs hasta el LER de egreso.

• Mapeo de Etiquetas (label mapping): en respuesta a una petición de etiqueta, un LSR downstream entonces manda (mapea) una etiqueta el LSR upstream correspondiente, usando este mecanismo de mapeo.

PROTOCOLO DE SELECCIÓN DE RUTAS.

Una de las funcionalidades que tiene MPLS, principalmente en la transmisión de video, es que asegura que siempre habrá recursos disponibles para mantener el canal de transferencia fluido; cuando se cumplen los requisitos de QoS. Esto es muy importante en videoconferencias multipunto, en donde se asegura ancho de banda suficiente para el video y se acota un retardo máximo para la voz. Para hacer esto se necesitan dos cosas:

• Ruteo con QoS para determinar la métrica, los mas recomendados son:

- Ruteo de Salto a Salto (Hop by Hop routing).
- Ruteo Explicito (Explicit routing).

• Algoritmo de Ruteo basado en restricciones (Constraint-based routing algorythm), que permita reservar recursos para cada petición, los tres principales recomendados por la IETF son:

- LDP (Label Distribution Protocol, RFC 3036);
- RSVP–TE (ReSource reserVation Protocol – Traffic Engineering, RFC 3473);
- y el CR–LDP (Constraint-Based Routing – Label Distribution Protocol, RFC 3472).

Dependiendo de como se establezcan los LSP se pueden presentar diversas opciones: Si se utiliza la aproximación “hop by hop” (o “salto a salto”) para el establecimiento de los LSP la IETF ha recomendado (no obligatorio) el uso del protocolo LDP para la asignación de etiquetas, en este caso también se pueden utilizar los protocolos RSVP–TE y CR–LDP. Si la estrategia utilizada es la “downstream unsolicited” donde el LER de salida distribuye las etiquetas que deben ser utilizadas para alcanzar un determinado destino, la única opción disponible es LDP.

Cuando la estrategia es “downstream on demand” iniciada por el LER de entrada y no se desea seguir el camino calculado paso a paso, sino que se desea utilizar el que permita definir una ruta explicita, las opciones actualmente disponibles son CR–LDP y RSVP–TE.

1.7.4 COMBINACIONES DE DIFERENTES TÉCNICAS DE QOS [11]

Las tecnologías de QoS explicadas anteriormente en la práctica no se van a utilizar de forma excluyente y de hecho están diseñadas para ser utilizadas de forma conjunta con otras tecnologías para dar soporte a la QoS extremo a extremo.

La mayoría de las especificaciones de cómo se interrelacionan las diferentes tecnologías de calidad de servicio no están todavía estandarizadas, pero se han previsto varias arquitecturas para soportar calidad de servicio extremo a extremo.

IntServ/DiffServ.

Esta arquitectura propone usar una combinación de los modelos DiffServ e IntServ de forma estratégica para obtener un rendimiento óptimo de ambas en el entorno en que se usen. Para ello se propone que las aplicaciones se conecten a redes periféricas IntServ para solicitar, reservar y transferir los requerimientos de QoS, donde la clasificación MF y el control de tráfico por flujo son soportados.

Entre las redes periféricas IntServ se ubicaría la red DiffServ, por donde fluirán grandes volúmenes de tráficos, soportando control de tráfico agregado (control de tráfico basado en la clasificación BA, análisis del DSCP).

MPLS/IntServ.

Existe el propósito de usar un objeto en RSVP para predeterminar el camino a tomar por parte de las sesiones RSVP con etiquetas. Estas sesiones usan las conexiones establecidas por los encaminadores MLPS. Incluso sin este objeto es posible que MPLS asigne etiquetas con arreglo a las especificaciones de RSVP. En cualquier caso, la consecuencia es una simplificación del funcionamiento de IntServ en los encaminadores MPLS.

MPLS/DiffServ.

Como cabría esperar, dada la similitud entre MPLS y DiffServ, la traslación del tráfico DiffServ a conexiones MPLS resuelven gran parte de los problemas de QoS en las redes IP. DiffServ se apoya del campo Tipo de Servicio (ToS) clasificando los tráficos en diferentes clases en los nodos de ingreso al dominio DiffServ. MPLS realiza en cierta manera una clasificación similar a DiffServ, sólo que éste los clasifica y agrupa en FEC para garantizar QoS. Ambos emplean etiquetas, en DiffServ son conocidas como DiffServ Code Point (DSCP) y etiqueta MPLS en ésta última.

La etiqueta MPLS determina la ruta que un paquete tomará, lo cual permite optimizar el ruteo dentro de una red. Además es factible aplicar la Ingeniería de Tráfico, la cual garantiza la asignación de circuitos virtuales con ciertas garantías de ancho de banda para igual número de etiquetas que lo requieran. Por otro lado, el valor DSCP determina el comportamiento de los nodos de acuerdo a esquemas de colas (Queuing).

En la gran mayoría de estas arquitecturas mixtas, se plantean esquemas para mejorar el desempeño que ofrece MPLS, DiffServ e IntServ, no obstante ello, es necesario realizar un estudio y simulaciones previas de los posibles tráficos a soportar, de tal manera que se pueda seleccionar el mejor esquema. El seleccionar erróneamente uno de estos esquemas, podría ser la causa principal de bajo desempeño en nuestras aplicaciones sensibles a retardo.

CAPÍTULO II:

2. LA TELEFONÍA IP, SUS PROTOCOLOS Y APLICACIONES

2.1. LA TELEFONÍA IP [1][11]

El rápido desarrollo de las redes de datos (LAN, WAN e Internet), hizo interesante la posibilidad de transmitir voz, puesto que las llamadas realizadas en este entorno son independientes de la distancia y comúnmente del tiempo de conexión, a diferencia de la tarificación utilizada en la telefonía convencional. La voz sobre IP permite transmitir voz sobre redes IP empleando conmutación por paquetes, lo que permite el uso eficiente del canal de transmisión en contraste con la conmutación de circuitos empleada en la RTC (Red Telefónica Conmutada).

La Voz sobre IP es una tecnología conocida en Internet con MSN Hotmail, MSN Yahoo y similares.

La "Telefonía IP" es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP utilizando un PC, gateways teléfonos estándares, etc. En general, servicios de comunicación: voz, fax, aplicaciones de mensajes de voz, etc, que son transportadas vía redes IP y tienen la capacidad de conectarse con la red telefónica conmutada.

Por lo tanto la conclusión es clara: la telefonía IP ToIP es mucho más que voz sobre IP VoIP; es integrar servicios que tradicionalmente se ofrecían en PBX con la ubicuidad de

Internet (o redes IP) y la cantidad de servicios posibles, convergentes y, en cierta manera, revolucionarios.

De este modo se facilita el diseño de redes integradas de voz y datos convergentes. Una de las mayores limitaciones en telefonía sobre IP se encuentra en la transmisión de voz de alta calidad, como la prestada en telefonía convencional. El problema radica en que las redes conmutadas de paquetes no fueron concebidas para tráfico en tiempo real. A pesar de estos problemas en redes privadas la calidad de voz es aceptable, debido a que se puede: limitar los tiempos de transmisión a través de algún sistema de prioridad sobre el resto de datos en la red, y estableciendo el número de enrutadores por donde el mensaje de voz debe atravesar antes de llegar a su destino.

En la Internet, puesto que no se puede priorizar los datos de voz frente a otros y que debe atravesar un sinnúmero de nodos es evidente que su calidad será inferior a la prestada en RTC, pero existen empresas que prestan este servicio a bajos costos y previo acuerdos de calidad. Es de esperar que las grandes empresas de telecomunicaciones implementen QoS en sus redes de datos y de esta manera proveer telefonía IP sin tener que sacrificar la calidad de voz.

2.1.1 ARQUITECTURA DE ToIP [14] [15]

En el caso de una empresa, tradicionalmente existían dos tipos de cableado, tanto para datos como para voz, sin existir relación entre ellos. En ToIP se integra el servicio de voz a través de la red de datos, puesto que, una conversación se transporta en forma de paquetes de datos, basándose en el protocolo IP, pudiendo tener diferentes caminos entre origen y destino mientras la comunicación dure. Esto significa que los recursos de la red pueden ser destinados para otros tipos de conexiones al mismo tiempo, como por ejemplo Internet.

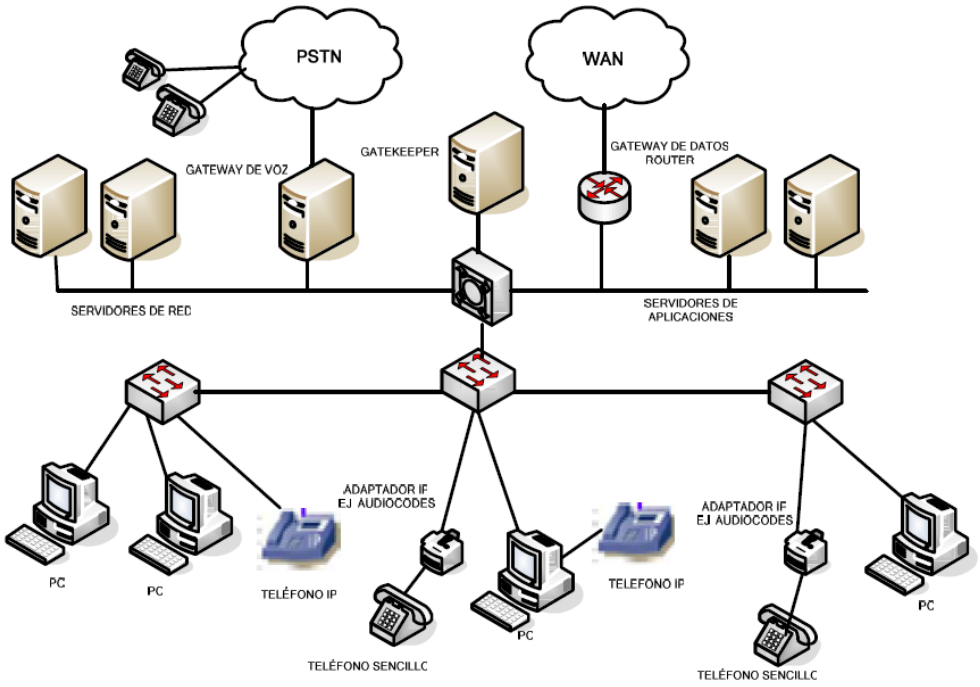


Figura. 2.1. Arquitectura de un Sistema telefónico IP

Como se observa en la figura 2.1 existen dos Gateway, uno para datos y el otro para voz; el primero se refiere a la puerta de enlace para los datos y el segundo permite interactuar, a la red de datos con la RTC.

Los elementos que se muestran corresponden a los del estándar H.323 y SIP que son los protocolos para señalización y establecimiento de las llamadas.

Claro está que mediante servidores no es la única manera de implementar la voz sobre IP, en otros casos los routers integran los Gateways de voz, datos y gatekeeper (realiza funciones de administración de llamada). En la actualidad, puede coexistir la telefonía tradicional e IP, es decir, se pueden tener abonados digitales, analógicos e IP. Este tipo de alternativa se la conoce como una red telefónica híbrida y se la implementa a través de una central telefónica privada IP (IP-PBX). Los elementos mostrados en la figura 2.2, también conforman este tipo de estructura, puesto que los Gateways y gatekeeper se encuentran integrados en la central IP, la cual se conecta a la red de datos; los terminales IP, analógicos y digitales por lo general son propietarios de la marca de la central telefónica IP.

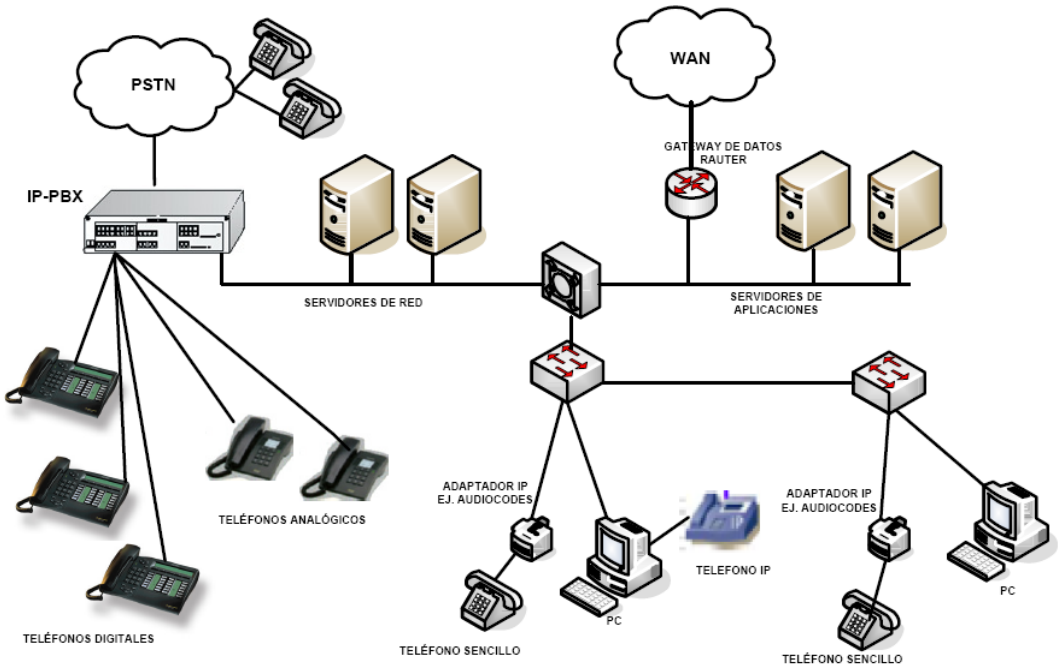


Figura. 2.2. Sistema de telefonía híbrida

Un sistema de telefonía IP en general se compone de:

Gateway y Gatekeeper.- El Gateway permite la interoperabilidad de la red de datos y de la red telefónica conmutada. El gatekeeper que puede ser opcional, realiza funciones de administración de llamadas, traducción de direcciones, control de admisión y ancho de banda.

Terminales.- Pueden ser teléfonos IP. Los terminales no IP se los puede usar conjuntamente con algún tipo de adaptador IP, o como en el caso de la PC con un programa que emule un terminal H.323 o SIP.

Redes de datos LAN/WAN.- Las redes LAN permite el tráfico de voz IP en una misma red, mientras que la red WAN permiten la interconectividad de sitios remotos a través de trunking IP.

Protocolos.- Los protocolos asociados a voz sobre IP se los puede dividir en tres grupos: protocolos de señalización, transporte IP y de soporte. Todos estos protocolos operan desde la capa sesión hasta la capa aplicación.

Todos estos aspectos relacionados con la telefonía IP se ampliarán en el próximo capítulo.

2.2 PROTOCOLOS DE TELEFONÍA IP [11]

En los últimos años, los protocolos de señalización para el servicio de transmisión de voz han experimentado una fuerte evolución junto con la tendencia a trasportar dicho tráfico desde las redes de conmutación de circuitos hacia las redes de conmutación de paquetes. Esta tendencia queda reflejada con la fuerte evolución de estándares en este ámbito y la aparición de productos en el mercado que cubren las necesidades de los operadores, grandes empresas y PYMES.

Para soportar el servicio de ToIP se requiere, además de los protocolos para el transporte de la información de usuario en tiempo real, también de la correspondiente señalización, es decir, de los protocolos necesarios que garanticen el establecimiento, mantenimiento - modificación y terminación de las llamadas de voz sobre las redes IP, lo que quiere decir que es necesario la señalización de control de las llamadas, todo el control de la comunicación, como pueden ser:

• Negociar el tipo de codificador a utilizar

• Negociar los parámetros de empaquetado de la voz (y video);

• Intercambio de número de puertos a través de los que se llevará a cabo la comunicación...etc.

El flujo de la información de usuario y el flujo de la señalización siguen trayectorias diferentes en su paso por las redes IP. La voz (información de usuario) y la señalización no presentan los mismos requerimientos de transporte por la red. La voz tiene que ser tratada con demora y jitter mínimos, pues pierde valor con el tiempo, dados sus requerimientos de tiempo real, y en cambio la señalización no requiere de esto último. Es decir, el tráfico de información de usuario es tratado por la red IP de manera diferente a como lo hace con el tráfico de señalización.

Con respecto a lo señalado anteriormente, se han desarrollado diferentes soluciones para la problemática de la señalización de control de llamada en sistemas de VoIP.

Evidenciando cada modelo, con la arquitectura funcional y protocolos que lo caracterizan respectivamente.

Los protocolos de señalización utilizados son de diversos tipos, siendo transportados sobre los protocolos TCP/IP o UDP/IP:

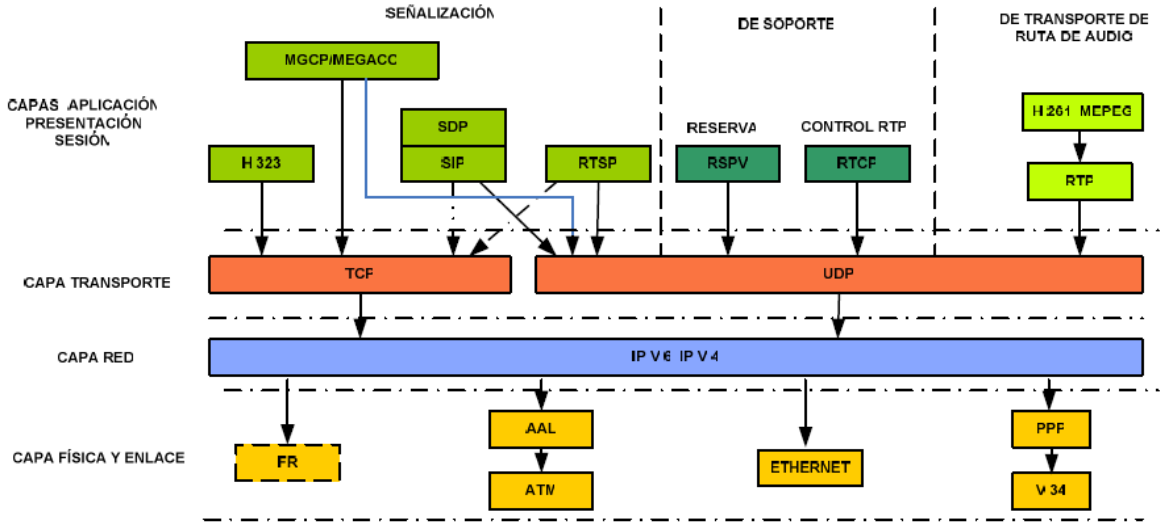


Figura. 2.3. Arquitectura de protocolos de telefonía IP [14]

• El ITU-T H.323 es una cobertura para diversos protocolos H.225, H.245 y RAS que se soportan en TCP y UDP. Siendo el primero aplicado para acciones dentro de una Intranet, cuya finalidad amplia, apoya la conferencia multimedios audio y vídeo, el establecimiento y control de llamadas, la gestión de anchura de banda y las interfaces entre diferentes arquitecturas de red.

• El protocolo mixto MEGACO (nombre asignado por la ITU-T) o H.248 (nombre asignado por la IETF), el cual define un protocolo que controla pasarelas de medios que pueden hacer pasar tráfico vocal, vídeo, facsímil y de datos entre las redes RTPC y las basadas en el IP.

• EL IETF define los protocolos SIP/SAP/SDP para el control hacia las redes privadas. El protocolo de señalización SIP es propuesto como alternativa a la recomendación H.323, su funcionalidad es proporcionar conferencia, telefonía y detección de presencia, notificación de eventos y mensajería instantánea.

• La señal vocal se transmite sobre el protocolo de tiempo real RTP (con el control RTPC) y con transporte sobre UDP. El protocolo de reservación de ancho de banda RSVP puede ser de utilidad en conexiones unidireccionales.

• La señalización SS7 se utiliza hacia la red pública PSTN. De forma que se disponen de los protocolos ISUP/SCCP/TCAP que se transmiten sobre MTP en la PSTN y sobre TCP/IP en la red de paquetes. El protocolo Q.931 (derivado de ISDN) se utiliza para establecer la llamada en H.323.

2.3 PROTOCOLO DE TRANSPORTE EN TIEMPO REAL (RTP) [1]

- Distingue los emisores múltiples de un flujo multidifusión RTP.
- Identifica los tipos de medios.
- Conserva la relación de temporización entre flujos.
- Permite detectar paquetes perdidos.

Cada paquete RTP consiste en un cabezal y los datos de voz. El cabezal contiene números de secuencia, marcas de tiempo, y monitoreo de entrega.

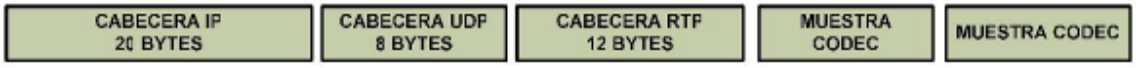


Figura. 2.4. Paquete RTP [1]

La figura 2.5 muestra la cabecera RTP (12 bytes), mientras que en la tabla 2.1 se describe la función de cada uno de los campos que la conforman.

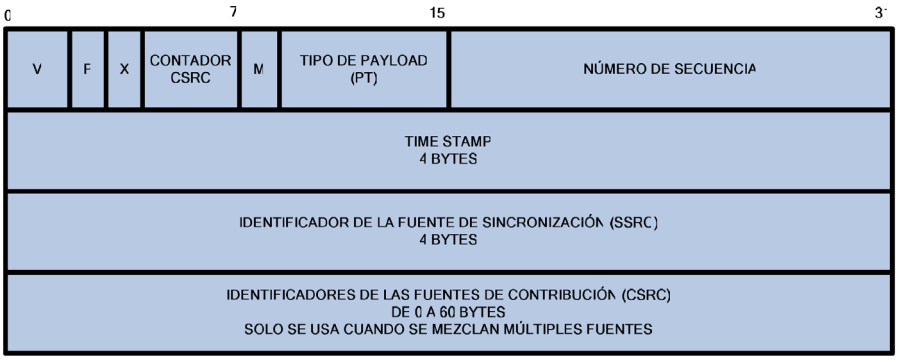


Figura. 2.5. Cabecera RTP [1]

Tabla. 2.1. Campos de la cabecera RTP [1]

Campo de la cabecera	Función
Versión (V)*	Especifica la versión de RTP
Padding (P)*	Indica si existe o no bytes de relleno para los algoritmos de cifrado de bloques fijos
Extensión (X)*	Indica si una cabecera de longitud variable sigue a la cabecera fija de 12 bytes
Contador CSRC (CC)*	Indica el número de campos de la cabecera de longitud variable
Market (M)*	Depende de la aplicación. Para VoIP determina el inicio de una ráfaga de voz.
Tipo de Payload (PT)*	Identifica los diferentes codecs de audio para VoIP
Número de secuencia*	Permite al receptor detectar los paquetes perdidos, comienza en un número aleatorio y aumenta en 1 con cada paquete.
Time Stamp*	Permite corregir el tiempo de temporización de la sobrecarga, aumenta en 1 con cada muestra del codec.
Identificador de la* fuente de sincronización (SSRC)	Único identificador aleatorio para cada emisor en una multidifusión RTP.
Identificadores de las fuentes de contribución (CSRC)	Fuentes de contribución para VoIP, indican todos los SSCR en intervienen en una conferencia

***Campos pertenecientes a la cabecera fija 12 bytes**

Al inicio de cada sesión RTP, se asigna aleatoriamente un número SSRC a cada emisor, el cual identifica al mismo dentro de un flujo de medios simple. Cuando se tiene varios flujos, como por ejemplo a través de un puente de conferencia VoIP o MCU (unidad de conferencia multidifusión), en el campo SSRC, se envía el número SSRC propio de la MCU, mientras que en el campo opcional CSRC, se envía los SSCR de los emisores pertenecientes a esa MCU.

El campo Contador CSRC (CC) de 4 bits, indica el número de campos que siguen a la cabecera fija de 12 bytes, lo que quiere decir que se puede identificar un máximo de 16 emisores simultáneamente. Puesto que en una conversación cada parte habla por lo menos dos segundos cada vez, los campo SSCR o CSRC permanecerían constantes, alrededor de unos 50 a 100 paquetes, lo que permite utilizar compresión en la cabecera RTP y así ahorrar el consumo del ancho de banda.

El bit M indica el comienzo de una conversación entrecortada seguida de un silencio, el cual tiene estrecha relación con la operación del búfer de fluctuación playout (búfer donde se almacena la VoIP para ser receptada y transmitida). Cuando se pierde la

sincronización entre codificador del emisor y decodificador del receptor, el playout del receptor se puede llenar demasiado lento o rápido. Con la ayuda de VAD (detección de la actividad de la voz), se puede ajustar el búfer playout ya sea quitando tiempo a una pausa para procesar muestras adicionales del búfer lleno o añadiendo tiempo a una pausa para las tramas que llenen un búfer vacío. De esta forma el bit M=1 indica que acaba de terminar un periodo de silencio y se puede ajustar los búferes playout, con M=0 es más complejo ajustar el búfer, ya que se debe manipular las interacciones con el codec.

El Time Stamp, permite a la fuente de medios determinar la temporización precisa que debería usar un receptor cuando reproduce los paquetes sucesivos en el flujo de medios; es decir se podrá sincronizar un flujo de audio con los labios en movimiento de una imagen, pero no es posible relacionar la información de temporización con los eventos en tiempo real. RTCP permite relacionar dicha información con los eventos en tiempo real a través del protocolo del tiempo de la red, NTP (Network Time Protocol).

2.4 PROTOCOLO DE CONTROL EN TIEMPO REAL (RTCP) [1]

RTCP aparece en el RFC (Request For Comment) 1889 como parte del RTP, administrando los procesos relacionados con una conferencia RTP multidifusión. En una conversación VoIP punto a punto, permite retroalimentar QoS desde el receptor al emisor en cada dirección.

La cantidad de paquetes enviados por RTCP son inversamente proporcionales al número de usuarios que interviene en una conferencia, tal y como muestra la figura 2.6. RTCP limita el control del ancho de banda mientras aumenta el número de participantes.

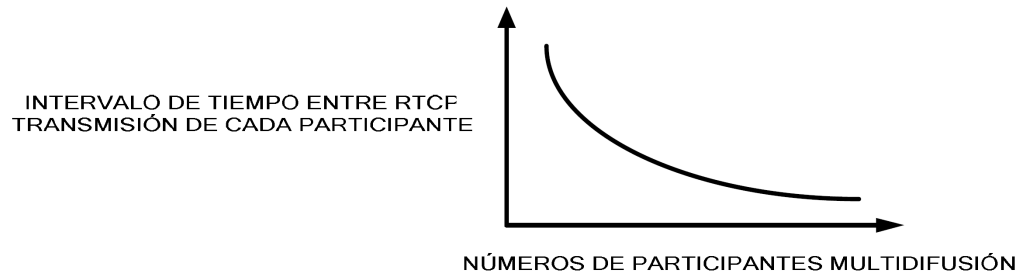


Figura. 2.6. Comportamiento del tráfico RTCP [1]

El paquete RTCP sólo contiene la información necesaria para el control de transporte y no transporta ningún contenido. Está compuesto por un encabezamiento de conjunto, similar al de los paquetes RTP que transportan el contenido, seguido de otros elementos que dependen del tipo de paquete RTCP.

RTCP realiza diferentes tareas, relacionados con cada uno de los paquetes que posee, como lo son:

-Informe del emisor (SR) y del receptor (RR)

-Descripción de la fuente (SDES)

-Desconexión (BYE)

-Específica de la aplicación (APP)

Los orígenes de los flujos de medios RTP transmiten informes del emisor (SR), a todos los participantes de la multidifusión, mientras que los participantes transmiten informes del receptor (RR). Tanto los SR como RR contienen información del receptor, pero SR adiciona información del emisor. Puesto que en VoIP, ambas partes son emisoras, los puntos finales crearán SR. De esta forma cada parte sabrá la calidad del transporte analizando el informe de receptor de cada paquete SR.

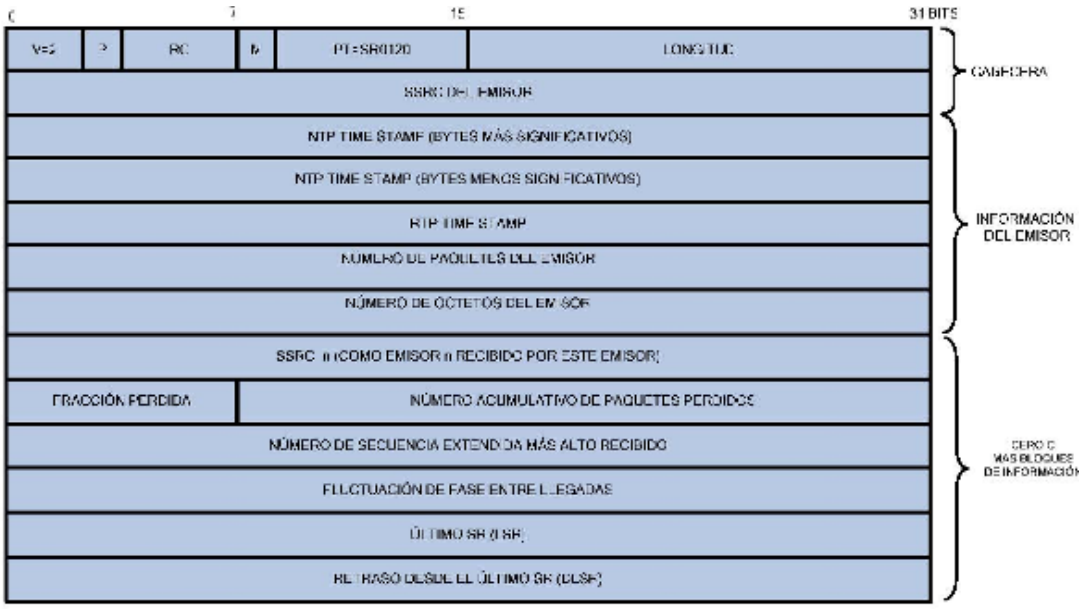


Figura. 2.7. Cabecera del paquete SC de protocolo RTP [1]

Tabla. 2.2. Campos de la Cabecera SR RTCP [1]

Campo de la cabecera	Función
Versión (V)	Especifica la versión de RTP
Padding (P)	Indica si existe o no bytes de relleno
Contador de reportes de recepción (RC)	Indica el número de bloques de informes de recepción que siguen a la información del emisor
Market (M)	Depende de la aplicación. Para VoIP determina el inicio de una ráfaga de voz.
Tipo de paquete (PT)	Identifica al paquete como un SR RTCP con PT=200 SR y PT=201 RR
Longitud	Longitud del informe RTCP del emisor
SSRC	Identificador del origen de envío del emisor
NTP Time Stamp	Permite que el paquete sea transmitido en tiempo real.
RTP Time Stamp	Permite que los datos Time Stamp RTP sean correlativos con el tiempo real vía NTP
Número de paquetes del emisor	Número total de paquetes enviados en el flujo de medios RTP
Número de octetos del emisor	Total de bytes enviados en el flujo de medios RTP
SSRC_n SSRC	Identificación SSRC del emisor de quien se aplica el informe de recepción
Fracción perdida	Número de paquetes RTP, dividido entre los paquetes RTP enviados. (Desde el último SR/RR).
Número acumulativo de paquetes perdidos	Número de paquetes RTP perdidos desde el comienzo de la sesión
Número de secuencia extendida más alto recibido.	Número de secuencia más alto recibido del emisor.
Fluctuación de fases entre llegadas (J)	Diferencia entre paquetes del emisor y receptor.
Último SR	Fecha y hora en el último paquete SR recibido del emisor
Retraso desde el último SR	Diferencia de tiempo entre recibir el último SR y enviar este informe de

La figura 2.7 muestra la cabecera del paquete SR del protocolo RTCP, mientras que la tabla 2.2 expone la descripción de los campos de la cabecera.

A más de que RTCP ofrezca medios de retroalimentación QoS de los receptores, permite conocer si su calidad de recepción coincide con otros receptores, o si los

problemas locales pueden influir negativamente en la calidad de recepción. En resumen los emisores pueden aprender las siguientes estadísticas de la red:

− Tiempo de ida y vuelta (RTT), que es la diferencia de cuando se envía un SR a los receptores y cuando se recibe un RR de éstos.

− Tasa de paquetes perdidos.

− Fluctuación de fase.

La descripción de origen (SDES), proporciona información de cada emisor de medios RTP en una sesión multidifusión. Generalmente cada host envía un elemento SDES sencillo, relacionado con su propia identificación SSRC. Para el caso de una MCU envía varios bloques de Elementos SDES (campo de la cabecera SDES, ver figura 1.33), cada uno con diferente CSRC dentro de un paquete SDES RTCP.

La figura 2.8, muestra el formato de la cabecera del paquete SDES, en el cual se observa el campo llamado "Elementos SDES", del cual hace uso los dispositivos mezcladores como el MCU para transmitir flujos multidifusión, tales elementos se muestran en la tabla 2.3.

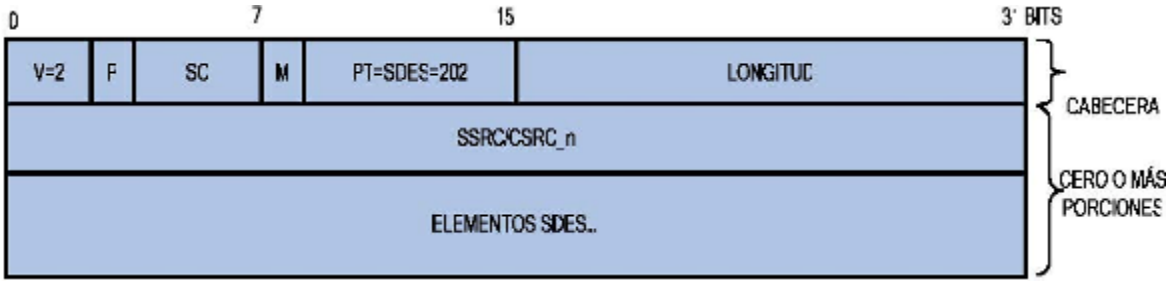


Figura. 2.8. Cabecera del paquete SDES del protocolo RTCP [1]

Tabla. 2.3. Elementos SDES que pueden transmitirse [1]

Campo de la cabecera	Función
CNAME	<usuario>@<nombre_host > refleja el host de la aplicación
NAME	Nombre real, contrario a un ID de login
EMAIL	Dirección de mail del emisor
PHONE	Número de teléfono del emisor , en formato E.164 completo
LOC	Localización geográfica del emisor
TOOL	El nombre y versión de una entidad generada por una aplicación
NOTE	Texto de forma libre para mensajes transitorios
PRIV	De propósito experimentales o de aplicaciones específicas

Cuando un participante desea retirarse de una sesión RTP, envía paquetes de desconexión BYE para conocer el número de usuarios activos; la importancia radica en que la cantidad de tráfico RTCP, depende del número total de participantes. La figura 2.9 muestra el formato del paquete BYE.

Figura. 2.9. Paquete BYE del protocolo RTCP [1]

Los paquetes RTCP de aplicación específica (APP), capacitan al protocolo para la experimentación y las extensiones, sin la necesidad de nuevos paquetes. La figura 2.10 muestra el paquete APP.

Figura. 2.10. Paquete APP del protocolo RTCP [1]

Existe la posibilidad de que los paquetes RTCP, puedan agruparse para formar un paquete compuesto o también llamado metapaquete, que será transportado en una sobrecarga UDP, de manera que éstos contribuyan a reducir el coste UDP/IP asociado a los datos RTCP.

2.5 PROTOCOLO DE SEÑALIZACIÓN: H.323 [1] [15]

En 1996 la ITU (International Telecommunications Union) definió el estándar H.323, como el indicado para el transporte de voz datos y video en redes LAN basadas en IP, a más de incluir la especificación T.120 de conferencia de datos.

H.323 está basada en los protocolos RTP y RTCP para el manejo de señalización de audio y video. Las recomendaciones de la ITU que aparecen en la tabla 2.4 son parte integrante de las especificaciones de señalización H.323.

Tabla. 2.4. Recomendaciones de la ITU que soportan la señalización H.323 [1]

Recomendación de la ITU	Descripción
H.225.0	Protocolo de señalización de llamada y empaquetamiento de flujos de medios para sistemas de comunicación multimedia basados en paquetes.
H.235	Seguridad y cifrados de los terminales multimedia de la serie H.
H.245	Protocolo de control de comunicación multimedia.
H.450.x	Servicios complementarios de H.323.
Series T.120	Protocolo de datos para conferencia multimedia.

Tabla. 2.5. Formato de medios apoyados por la ITU para H.323 [1]

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

En cuanto a la operación de H.323, se debe conocer primero los componentes que intervienen en el sistema, para luego hablar del direccionamiento y de los protocolos que lo conforman.

2.5.1 COMPONENTES DE H.323 [1] [15]

H.323 define los siguientes componentes:

− Gateway

− Terminal

− Gatekeeper

− Unidad de control multipuerto, MCU

a) Gateway

Proporciona internetworking con tecnologías que no son H.323 como H.320 o redes telefónicas convencionales. Está formado por el "Media Gateway" MG y el "Media Gateway Controller" MGC, los cuales comúnmente se encuentran integrados en el Gateway.

El MGC se encarga de la señalización, establecimiento de la llamada y otras funciones no relacionadas con el medio. El MG se encarga del manejo de los medios.

b) Terminales

Son puntos finales del cliente de la LAN. Todos los terminales H.323 tienen que apoyarse en H.245 para el uso de los canales, Q.931 para el establecimiento de la llamada, RAS (Register Admission Status) para la admisión de llamadas, RTP, (Real-time Transport Protocol) y UDP para la transmisión de los paquetes. Los terminales H.323 pueden también incluir protocolos de comunicación de datos T.120 utilizados para fax y la ayuda de MCU para aplicaciones de videoconferencia.

c) Gatekeeper

Controla una zona H.323, regula los puntos finales que pueden iniciar o recibir llamadas. Los gatekeepers no son un requisito obligatorio en redes H.323 pero cuando están, realizan las siguientes funciones:

Address Translation Network, Conversión de dirección de red (NAT): Traducción de una dirección del alias a la dirección de transporte. Se hace esto usando la tabla de traducción que es actualizada con los mensajes del registro.

Admissions Control, Control de Admisión: El Gatekeeper puede conceder o negar el acceso basado en la autorización de la llamada, las direcciones de fuente, direcciones de destino, etc.

Call signaling, Señalización de llamada: el gatekeeper puede ordenar, aprender y conocer los puntos finales para conectar la llamada.

Call Authorization, Autorización de llamadas: el gatekeeper junto con el Gateway pueden restringir las llamadas a ciertos números dentro de la red y, si es necesario, hacer la marcación más versátil, por ejemplo en casos de llamadas de emergencias.

Cabe mencionar que los servicios antes mencionados son proporcionados solo a los puntos finales inscritos a un gatekeeper en particular.

d) MCU

La unidad de control multipuerto es requerida para la gestión de multi-conferencias, y está formada por dos partes fundamentales, de un Multipoint Controller (MC), que gestiona el control de los canales de los medios, y opcionalmente un Multipoint Processor (MP), que maneja los medios, ya sea, mezclando flujos, conmutación o cualquier otro procesamiento.

Para el diseño de la red de VoIP, el servicio de conferencia multidifusión, dependerá de los equipos empleados. Generalmente en una IP-PBX, los terminales tienen propiedades para mezclar los flujos de audio procedente de cada fuente, interpretar los formatos de audio y entregar al usuario un flujo de audio sencillo de entender, por lo que se suele usar una conferencia multidifusión descentralizada, y donde la central solo tiene integrada una MC puesto que parte del trabajo del MP es realizado en cada terminal.

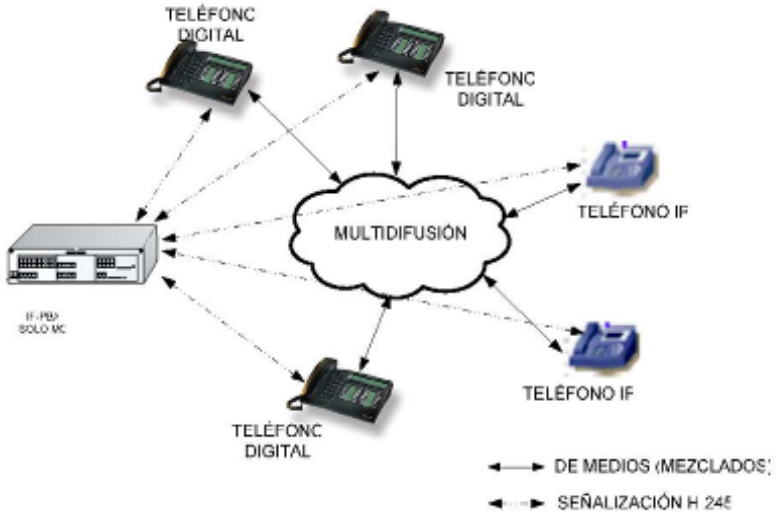


Figura. 2.11. Conferencia multidifusión descentralizada [1]

Para otros tipos de alternativas como servidores, se debe implementar una MCU, la cual contendrá el MC y MP. En estos casos en particular se puede tener conferencias multidifusión centralizadas y conferencias unidifusión centralizadas. En las primeras, se establecen sesiones de medios a través de la MC y el MP mezcla los flujos de medios para luego entregarlos al grupo de multidifusión, que es recibida por cada participante en la conferencia. En la unidifusión sucede de igual forma, pero el MP entrega el flujo de medios mezclados a cada uno de los participantes de la conferencia.

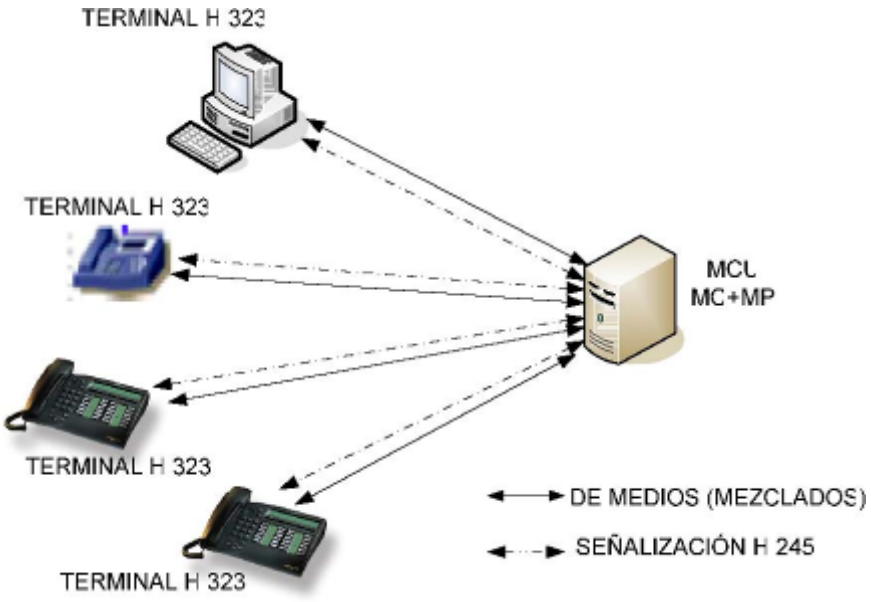


Figura. 2.12. Conferencia unidifusión centralizada [1]

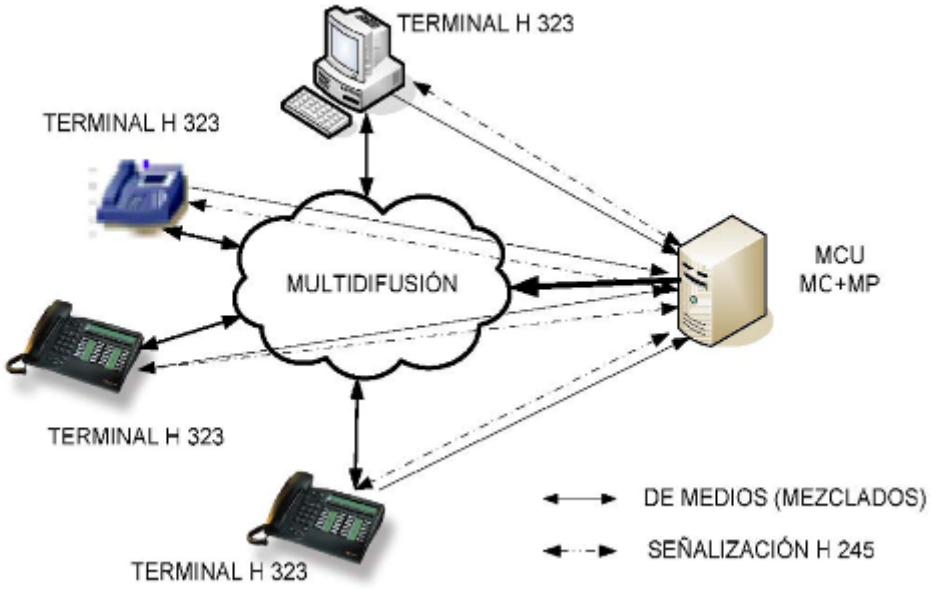


Figura. 2.13. Conferencia multidifusión centralizada [1]

2.5.2. DIRECCIONAMIENTO [1]

H.323 emplea un esquema de nombres y direccionamiento independiente de la tecnología subyacente de la red. El establecimiento de una comunicación en una red H.323, requiere del conocimiento de su dirección de red y un identificador de punto de acceso al servicio de transporte y direcciones (TSAP). Para redes IP la dirección de red es la dirección IP y el TSAP es el número de puerto UDP o TCP.

Puesto que la dirección de red y las TSAP son difíciles de recordar H.323 se vale de alias para identificar los puntos finales y conferencias multiparte. Éstos pueden tener varias formas como:

-Cadenas alfanuméricas: luis, luis@host.com, etc.

-Direcciones E.164: 1-02-3451058, 21,215, etc.

Existen diferentes TSAP para las diferentes comunicaciones llevadas en VoIP. Por ejemplo para descubrir el gatekeeper dentro de la red se envían paquetes GRQ con TSAP 1718 UDP, para comunicaciones RAS del gatekeeper se usa el TSAP 1719 UDP, para el

control de llamada H.225 1720 TCP, en cuanto al control de medios H.245 son el mismo que para H.225 puesto que los TSAP de H.245 se negocian sobre el canal de control de llamada.

2.5.3 PROTOCOLOS [1]

El protocolo H.323 ofrece servicios de comunicación multiparte, multimedia y de tiempo real sobre una red IP existente. Los servicios de H.323 se forman dentro de las aplicaciones de usuario que incluyen los principales servicios de audio y servicios opcionales de video y datos compartidos.

Cabe mencionar algunos de los protocolos más importantes usados para establecer una llamada a través de una red H.323. El canal de control de llamada H.225 puede estar enrutado directamente o a través de uno o varios gatekeepers, todo depende de la funcionalidad que se le desee dar a la red de VoIP, puesto que al enrutarlo a través de un gatekeeper se adicionará servicios como: Proxy, seguridad, conferencias, etc.

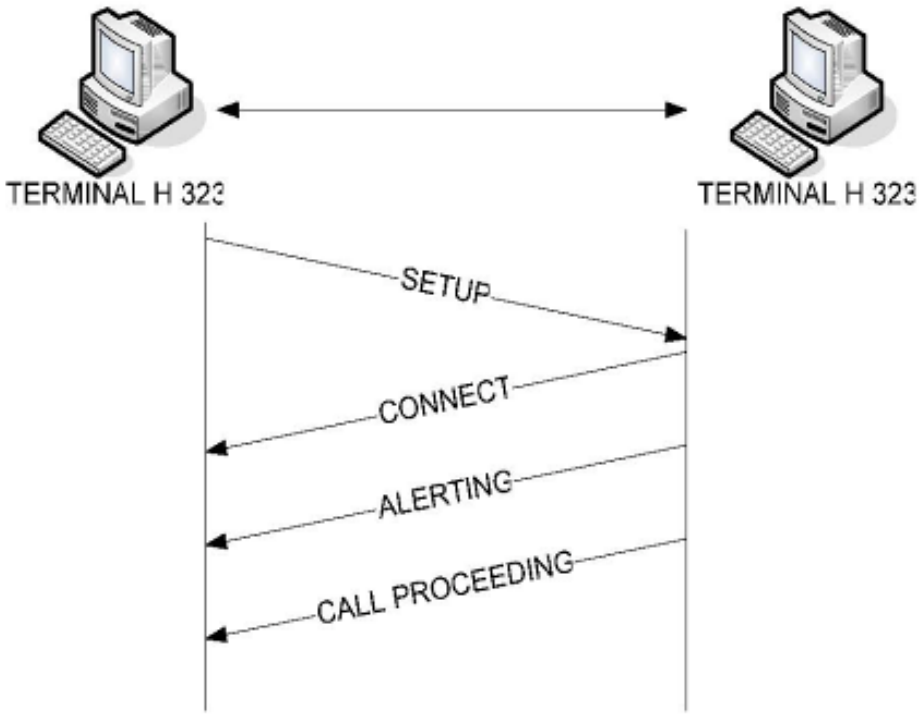


Figura. 2.14. Control de llamada H.225 directo entre puntos finales [1]

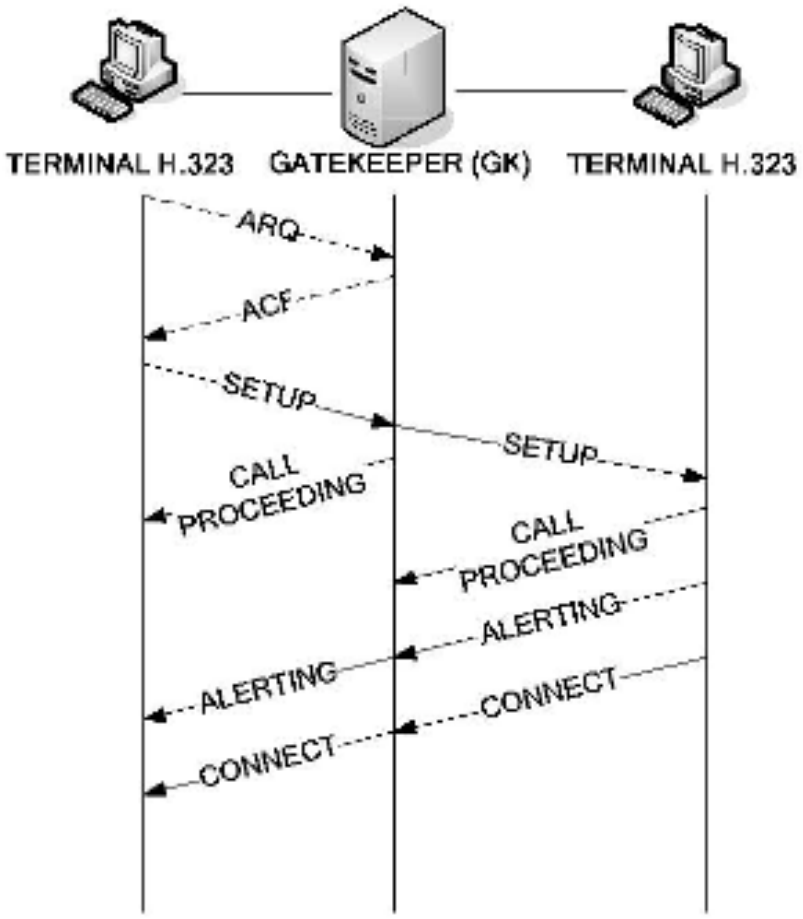


Figura. 2.15. Control de llamada H.225 enrutado mediante un gatekeeper [1]

El canal de control de medios H.245 se establece dinámicamente sobre una conexión TCP fiable. La mayoría de peticiones más interesantes de H.245 son secuencias de solicitud respuesta o solicitud-respuesta-indicación. La clase de un comando permite a un punto final pedir transacciones durante la llamada y realizar funciones de mantenimiento.

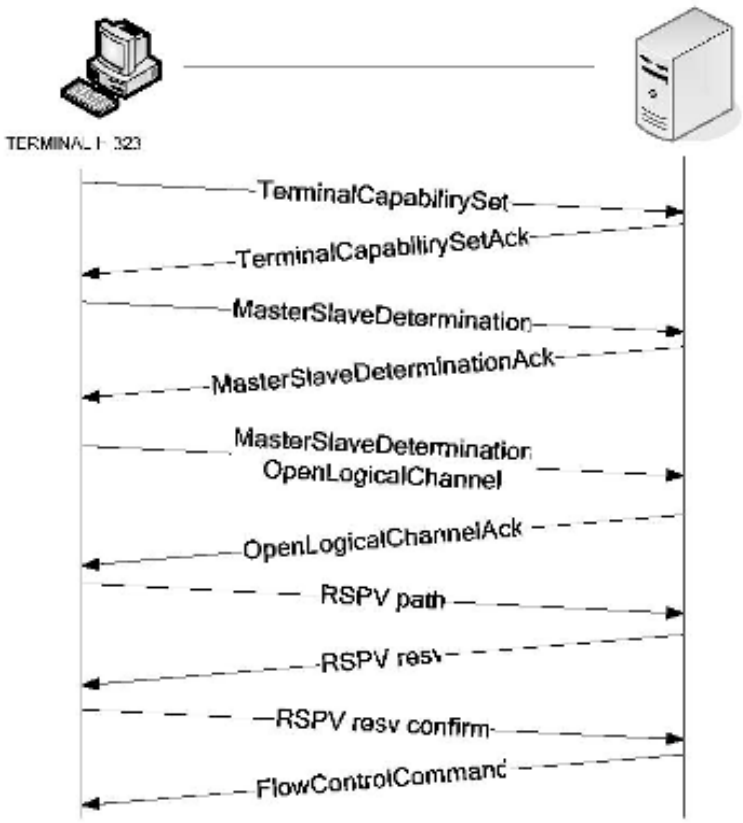


Figura. 2.16. Establecimiento del control de medio H.245 [1]

Inicialmente H.323v1 se diseñó para una estructura LAN, no se consideraba la posibilidad de los retrasos en la transmisión entre las entidades de señalización, lo cual era un problema cuando se lo implementaba a través de una red WAN.

H.323v2 presenta un nuevo modelo de negociación con los medios para solucionar el problema de la ruta de audio, y hacer a H.323 más resistente a los retrasos en la red.

En H.323v2 se realiza un by-pass al proceso de negociación de medios H.245 normal para agilitar la conexión. Además los mensajes H.245 se pueden manejar mediante H.225, o se puede establecer una sesión TCP separada para el canal H.245.

2.5.4 ESTABLECIMIENTO DE LLAMADA H.323 ENTRE DOS TERMINALES [16]

Para el establecimiento de una llamada en una red H.323, se deben cumplir ciertas fases que implican el establecimiento, mantenimiento y desconexión de una llamada.

A continuación se describen las fases que deben cumplir dos terminales H.323 mientras se efectúa una comunicación de voz.

Primera fase: Inicio de llamada

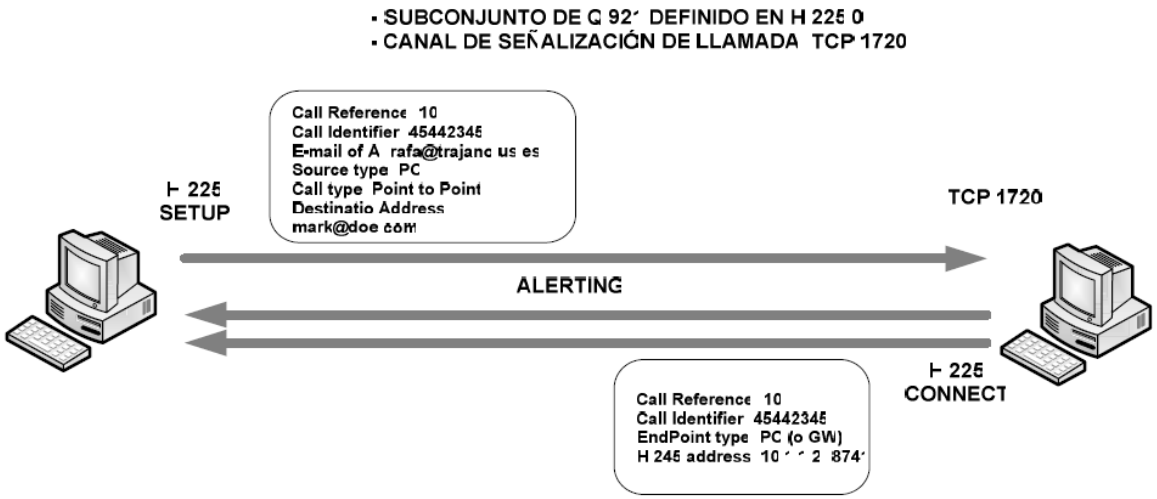


Figura. 2.17. Inicio de llamada

Segunda fase: Establecimiento del canal de control

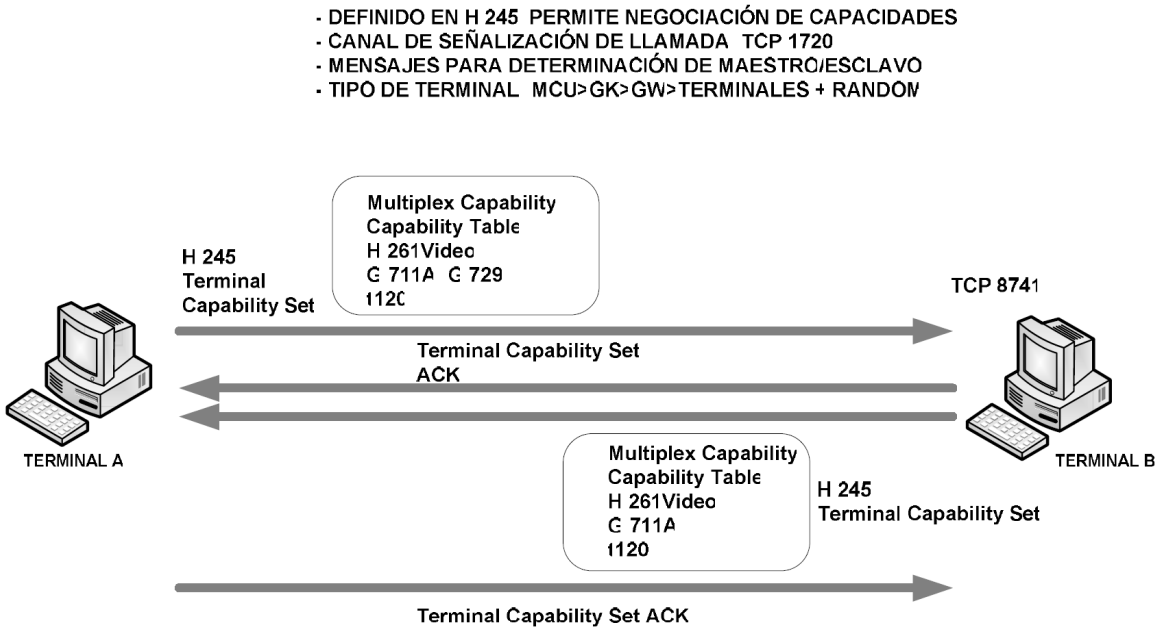


Figura. 2.18. Establecimiento de llamada

Tercera fase: Comienzo de la llamada

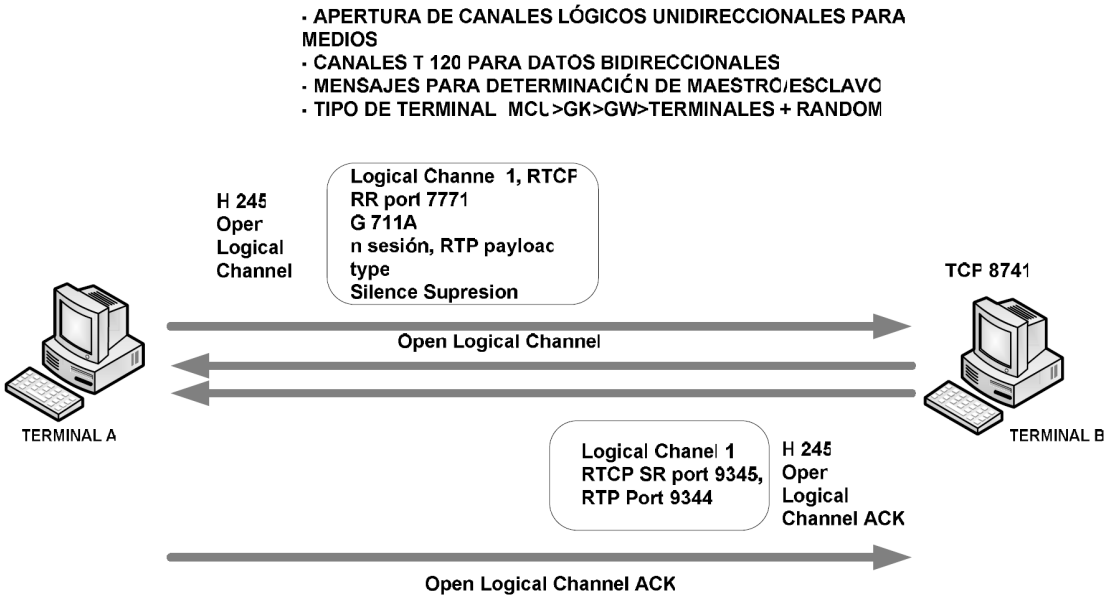


Figura. 2.19. Comienzo de llamada

Cuarta fase: Diálogo

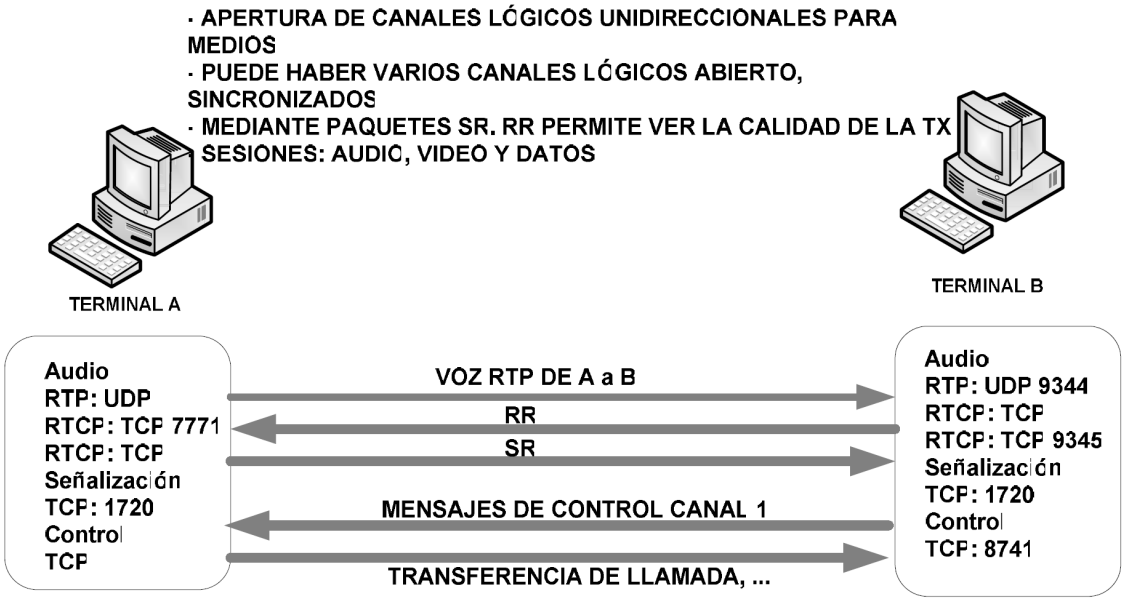


Figura. 2.20. Diálogo

Quinta fase: Finalización de la llamada

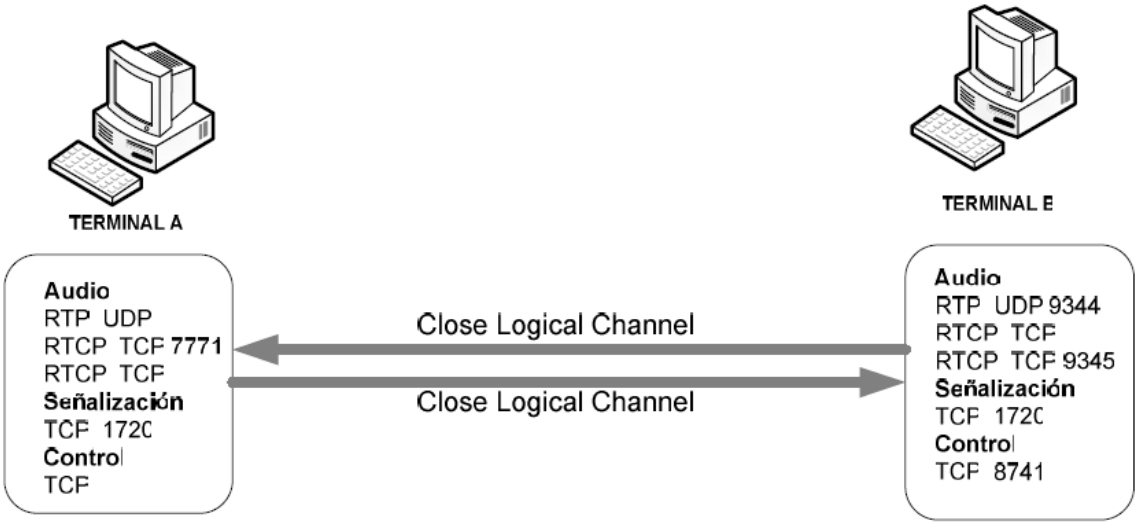


Figura. 2.21. Finalización de la llamada

Se lo puede hacer de diferentes maneras, una de ellas es una secuencia que se describe a continuación:

• Enviar: Close Logical Channel por cada canal abierto

• Recibir ACK de los anteriores

• Enviar H.245 End Session Command

• Recibir lo mismo para cerrar el canal H.245

• Enviar: H.225.0 Release Complete

2.6. PROTOCOLO DE SEÑALIZACIÓN: SIP [11]

El protocolo SIP (Session Initiation Portocol), ó protocolo de iniciación de sesión, es un protocolo de señalización que se utiliza para establecer, modificar y terminar llamadas vocales y sesiones multimedios, a través de redes IP (redes intranet y/o Internet), como también con usuarios de las redes telefónicas por intermedio de gateways.

Para comunicaciones multimedia interactúa (especificaciones IETF), conjuntamente con otros protocolos como RTP/RTCP y SDP, pero su funcionalidad no depende de ninguno de éstos. El protocolo RTP se usa para transportar los datos de voz en tiempo real (igual que para el protocolo H.323), mientras que el protocolo SDP se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc.

Se trata de un protocolo cliente-servidor similar en cuanto a sintaxis y semántica al protocolo HTTP que se utiliza en la web. Los cometidos de cliente y servidor son funcionales, es decir, un cliente puede comportarse como servidor y viceversa. Para establecer una llamada, el cliente envía peticiones SIP al servidor y éste las recibe y avisa al usuario o ejecuta un programa para determinar la respuesta.

Además por su naturaleza, al ser un protocolo 'peer-to-peer', admite que en el control de la llamada puedan intervenir terceros agentes o aplicaciones, capaces de modificar los mensajes SIP que se intercambian entre los extremos de una comunicación, habilitando a través de dichas aplicaciones funciones como el desvío de llamadas entrantes en base a ciertas reglas o la transferencia de sesiones de video conferencia al ordenador personal entre otras.

El SIP define tres tipos de servidores: registradores, intermediarios y retransmisores. Un servidor registrador recibe los registros de clientes sobre su ubicación, lo que ulteriormente ayuda a localizarlos para terminar las llamadas. Un servidor intermediario reenvía las peticiones del cliente a su destino final o a otro u otros servidores SIP. Un servidor retransmisor, retransmite los usuarios para que prueben otro servidor SIP que se encuentra en el siguiente tramo en la dirección del destino.

2.6.1. ARQUITECTURA SIP [11]

SIP utiliza una arquitectura del tipo "Cliente-Servidor", y tiene los siguientes componentes:

• Terminales SIP (SIP User Agents);

• Servidores SIP (Registrar, Proxy, Redirect, Location);

• Pasarelas SIP (Gateways)

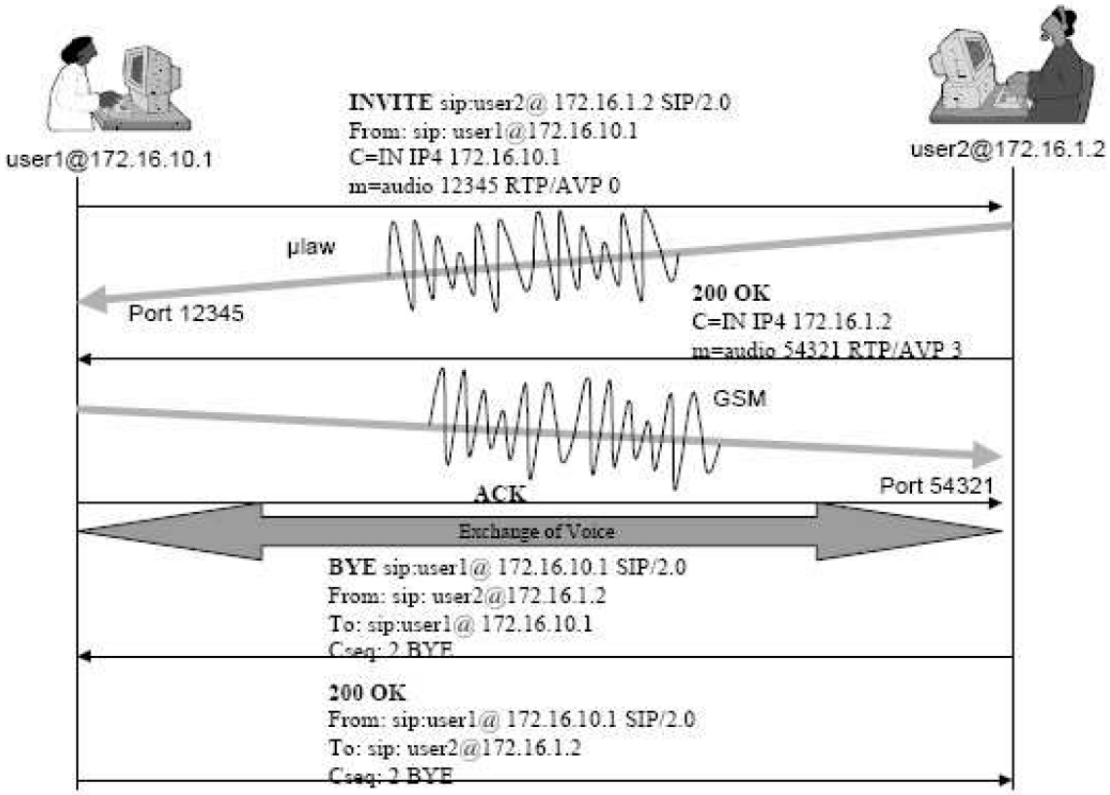


Figura. 2.22. Ejemplo de llamada SIP [11]

a) Terminales SIP.

Al igual que los H.323 son teléfonos multimedia IP (terminales SIP). Estos teléfonos pueden ser aplicaciones informáticas, que utilizan las capacidades multimedia del PC (parlantes y micrófono), o terminales físicos de similar aspecto a cualquier teléfono o videoteléfono.

Los terminales SIP, llamados “SIP User Agents”, pueden iniciar y recibir “sesiones” SIP.

Cada terminal dispone de un “User Agent Client” (UAC) y un “User Agent Server” (UAS). Los UAC son los encargados de iniciar requerimientos SIP hacia otros terminales.

Los UAS son quienes escuchan y atienden los requerimientos remotos. Implementado el transporte tanto sobre TCP como sobre UDP.

Estos se identifican a través de su "dirección SIP". El direccionamiento en SIP utiliza el formato de URL (Uniform Resource Locater) de Internet: sip:nombre@dominio.

Los establecimientos de comunicaciones SIP se realizan mediante el intercambio de mensajes (SIP INVITE) con formato similar al http, del tipo "Request" – "Response". El componente UAC envía un "Request" invitando a una conversación a su contraparte. El componente UAS del destino recibe el "Request", y lo contesta con el correspondiente "Response". Un ejemplo de llamada SIP se muestra en la Figura 2.22.

El funcionamiento requiere que el usuario al iniciar la sesión se registre con su dirección SIP, un identificador similar a los utilizados en correo electrónico (el formato es user@domain), y su actual dirección IP en el registrar. En este caso, es el registrar el que mantiene la base de datos con las direcciones SIP-URI asociadas a cada dirección IP.

El establecimiento de llamada requiere el envío de un mensaje SIP INVITE destinado al proxy, quien tras contactar con distintos servidores reenvía la petición al usuario destinatario quien puede aceptar o rechazar la llamada.

b) Servidores SIP.

Los UAC y UAS pueden, por si solos y sin los servidores de red, ser capaces de soportar una comunicación básica (entre endpoints). No obstante, la potencialidad de SIP se aprovecha con el empleo de los servidores de red. Los servidores de red se clasifican, desde un punto de vista lógico, de la manera siguiente:

• Servidores de redirección.

Procesan mensajes INVITE, que son solicitudes SIP, y retornan la dirección (o direcciones) de la parte llamada, esto es, el SIP – URL (Uniform Resource Locator) de la parte llamada, o cómo contactar con ella (respuesta 3xx). De lo contrario rechaza la llamada, enviando una respuesta de error (error de cliente 4xx o error de servidor 5xx). Desarrollan una funcionalidad similar al Gatekeeper H.323, cuando se emplea el modelo de llamada directo.

• Servidores proxy.

Se ocupan de reenviar las solicitudes y respuestas SIP para el establecimiento y liberación de llamadas de VoIP, con los medios necesarios para garantizar que los mensajes de señalización SIP de ida y vuelta sigan la misma ruta.

Un servidor proxy puede re-enviar solicitudes hasta el destino final sin efectuar cambio alguno en ellas, o cambiar alguno de sus parámetros si se requiere, por ejemplo, en el caso de las cabeceras "Via""Record Route".

Desarrollan el "routing" de los mensajes de solicitudes y respuestas SIP. Pueden ser "stateful" o "stateless". Los servidores proxy stateful retienen información de la llamada durante el tiempo que dure el establecimiento de ésta, no así los servidores proxy stateless, los que procesan un mensaje SIP y entonces "olvidan" todo lo referente a la llamada hasta que vuelven a recibir otro mensaje SIP asociado a la misma. Esto se refiere al "estado" de la llamada, sin embargo, pueden mantener un "estado" para una simple transacción SIP, lo que es denominado "minimal state". La implementación stateless provee buena escalabilidad, pues los servidores no requieren mantener información referente al estado de la llamada una vez que la transacción ha sido procesada.

Además, esta solución es muy robusta dado que el servidor no necesita "recordar" nada en relación con una llamada. Sin embargo, no todas las funcionalidades pueden ser implementadas en un servidor proxy stateless, por ejemplo, las funcionalidades relativas a la contabilización y facturación de las llamadas puede requerir funcionalidades proxy stateful, de manera que se le pueda "seguir el rastro" a todos los mensajes y estados de una comunicación.

• Servidores de registro.

Es un servidor que registra las direcciones SIP (SIP – URL) y sus direcciones IP asociadas, es decir, garantizan el "mapping" entre direcciones SIP y direcciones IP. Típicamente están localizados con servidores proxy o servidores de redirección.

Acepta solo mensajes de solicitud REGISTER, posibilitando el registro correspondiente a la localización actual de los usuarios, esto es, "seguir el rastro" de los usuarios, pues por diferentes razones (conexión vía ISP, usuarios móviles, conexión vía

LAN con DHCP) las direcciones IP de éstos puede cambiar. También se les denomina servidores de localización (Location Server), pues son utilizados por los servidores proxy y de redirección para obtener información respecto a la localización o localizaciones posibles de la parte llamada.

Ahora bien, en rigor, los Location Server (LS) no son servidores SIP, ni entidades SIP, si no bases de datos, que pueden formar parte de arquitecturas de comunicaciones que utilicen SIP. Entre un LS y un servidor SIP no se utiliza el protocolo SIP, por ejemplo, en ocasiones se emplea entre éstos el protocolo LDAP (Lightweight Directory Access Protocol).

La información registrada en los servidores de registro, esto es, el registro del mapping de direcciones SIP correspondiente a un usuario, no es permanente, requiere ser "refrescado" periódicamente, de lo contrario, vencido un "time out" (por defecto, una hora), el registro correspondiente será borrado. Este valor por defecto del "time out" puede ser modificado según valor que se especifique en la cabecera "Expires" de un mensaje de solicitud REGISTER. En consecuencia, para mantener la información de registro, el terminal (o el usuario) necesita refrescarlo periódicamente.

Igualmente, un registro vigente puede ser cancelado y/o renovado por el usuario. Usualmente, un servidor de red SIP implementa una combinación de los diferentes tipos de servidores SIP ya comentados: servidor proxy + servidor de registro y/o servidor de redirección + servidor de registro.

En cualquier caso deben implementar el transporte sobre TCP y UDP.

c) Gateway SIP.

Al igual que en H.323, existen pasarelas SIP hacia la PSTN y también hacia H.323. Los gateways son responsables de adaptar el audio, video y los datos, así como también la señalización, entre los formatos propios de SIP y otras redes de telecomunicación, de manera transparente para los usuarios. En redes dónde no es necesario tener comunicación con terminales externos a la propia red, no es necesario disponer de gateways.

2.6.2. MENSAJERÍA SIP [11]

Los mensajes SIP, Request-Response (solicitudes-respuestas) de http, emplean el formato de mensaje genérico establecido en la RFC 822, esto es: una línea de inicio, uno o más campos de cabeceras (header), una línea vacía (indica final del campo de cabeceras) y finalmente el cuerpo del mensaje (opcional).

REQUEST SIP.

Los usuarios SIP disponen de direcciones de correo electrónico similares a los URL SIP (análogos a los de http). El formato de los mensajes de solicitud es como sigue: <Función><URL><SIP-Version> Ej: INVITE sip:pepe@fing.com SIP/2.0 En la figura siguiente se muestra el formato general de los mensajes de solicitud o métodos.

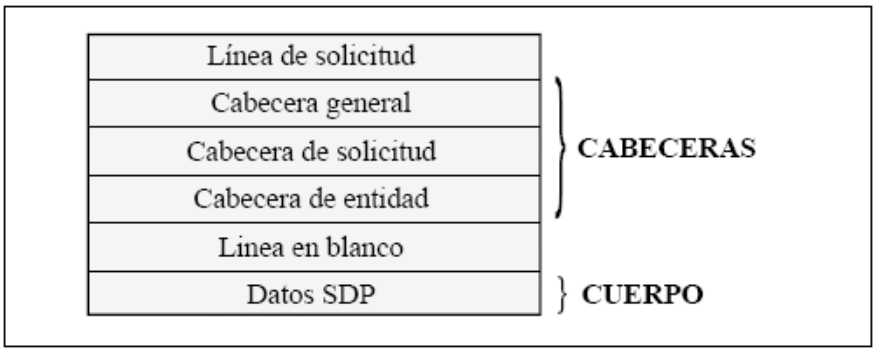


Figura. 2.23. Formato general de los mensajes de solicitud SIP

Estos URL pueden indicar que el usuario pertenece a un dominio (sip:usuario@dominio), a un determinado computador (sip:usuario@computador), a una dirección IP de un computador determinado (sip:usuario@dirección_IP), o incluso a un número de teléfono (número E.164) accesible a través de una pasarela IP/RTPC (sip:número_teléfono@pasarela).

SIP- Versión da cuenta de la versión del protocolo SIP en uso, y se incluye tanto en mensajes de solicitud (métodos) como en mensajes de respuesta (códigos de estado).

Para ello se han definido 6 métodos para estos tipos de mensajes, los cuales son descritos a continuación:

• INVITE: invita a un usuario, o servicio, a participar en una sesión. El cuerpo del mensaje contiene, generalmente, una descripción de la sesión.

• ACK: confirma que el cliente solicitante ha recibido una respuesta final desde un servidor a una solicitud INVITE, reconociendo la respuesta como adecuada. Solo para reconocer solicitudes INVITE, y no otros mensajes de solicitud.

• OPTIONS: posibilita "descubrir" las capacidades del receptor, las cuales pueden ser configuradas entre agentes o mediante un server SIP.

• BYE: finaliza una llamada, o una solicitud de llamada. Puede ser enviado por el agente llamante o por el agente llamado.

• CANCEL: cancela una solicitud pendiente, pero no afecta una solicitud ya completada. Este método finaliza una solicitud de llamada incompleta.

• REGISTER: se utiliza este método como un servicio de localización que registra la localización actual de un usuario. Los métodos que no sean soportados por servidores, Proxy o de redirección, son tratados por éstos como si se tratase de un método OPTION, y en consecuencia reenviados. Y por otro lado los métodos que no sean soportados por los servidores UAS o Registrar, provocan el mensaje de respuesta 501, "no implementado".

RESPONSE SIP.

Después que se recibe e interpreta un mensaje de solicitud SIP, el receptor del mismo (servidor SIP) responde con un mensaje (o varios) de respuesta (código de estado) El formato de los mensajes de respuesta es como sigue: <SIP-Version> < Status-Code> <Reason> Ej: SIP/2.0 404 Not Found

En la figura que se muestra a continuación, representa el formato general de los mensajes de respuesta.

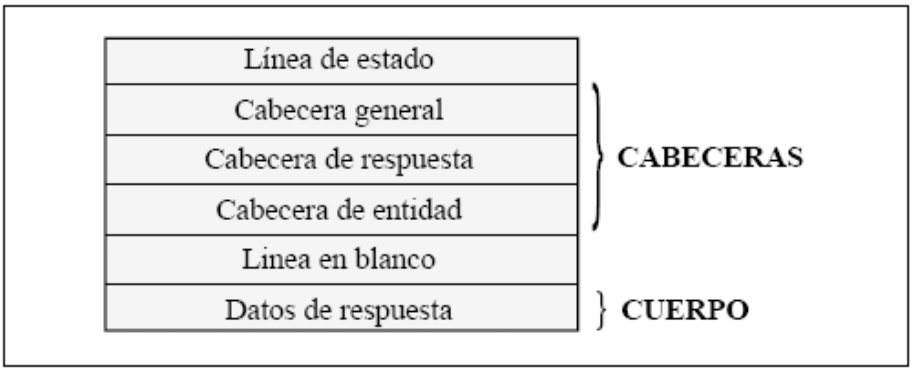


Figura. 2.24. Formato general de los mensajes de respuesta SIP

El formato, comprende la versión del protocolo SIP, un código de tres enteros los cuales son interpretados por máquinas, indicando el resultado de comprender y satisfacer o no una solicitud. Y finalmente una explicación textual (Reason-Phrase) muy breve del Status Code (códigos de respuesta), para ser interpretada por las personas. Encontrando seis diferentes tipos de Códigos de respuesta:

• 1xx: Informativo. Solicitud recibida, se continua para procesar la solicitud. (Ej: 180 Ringing)

• 2xx: Solicitud exitosa. La solicitud (acción) fue recibida de forma adecuada, comprendida y aceptada. (Ej: 200 OK)

• 3xx: Redireccionado. Más acciones deben ser consideradas para completar la solicitud. (Ej: 302 Moved Temporarily)

• 4xx: Error de cliente. La solicitud contiene mal la sintaxis o no puede ser resuelta en este servidor. (Ej: 404 Not Found)

• 5xx: Error de servidor. El servidor ha errado en la resolución de una solicitud aparentemente válida. (Ej: 501 Not Implemented)

• 6xx: Fallo global. La solicitud no puede ser resuelta en servidor alguno. (Ej: 600 Busy Everywhere) Destacando de lo dicho anteriormente que los mensajes respuestas 2xx, 3xx, 4xx, 5xx y 6xx son “respuestas finales”, y terminan la transacción SIP. En cambio, los mensajes de respuestas 1xx`s son “respuestas provisionales”, y no terminan la transacción SIP.

ENCABEZADO.

Las cabeceras SIP son similares a las cabeceras utilizadas en el protocolo HTTP (Hyper Text Transfer Protocol), tanto en la sintaxis como en la semántica. Se utilizan para transportar información necesaria a las entidades (SIP).

Determinadas cabeceras están presentes en todos los mensajes, otras no, solo en algunos. Igualmente, una aplicación que contenga el protocolo SIP no requiere necesariamente tener que comprender todas las cabeceras, aunque si es deseable. En el mismo sentido, si un participante SIP no entiende una cabecera, la ignora. Las cabeceras no especificadas deben ser ignoradas por los servidores. Detallándose los siguientes campos más significativos

• Vía: Indica el transporte usado para el envío e identifica la ruta del request, por ello cada proxy añade una línea a este campo.

• *From*: Indica la dirección del origen de la petición.

• *To*: Indica la dirección del destinatario de la petición.

• *Call-Id*: Identificador único para cada llamada y contiene la dirección del host. Debe ser igual para todos los mensajes dentro de una transacción.

• Cseq: Se inicia con un número aleatorio e identifica de forma secuencial cada petición.

Contact: Contiene una (o más) dirección que pueden ser usada para contactar con el usuario.

• User Agent: Contiene el cliente agente que realiza la comunicación.

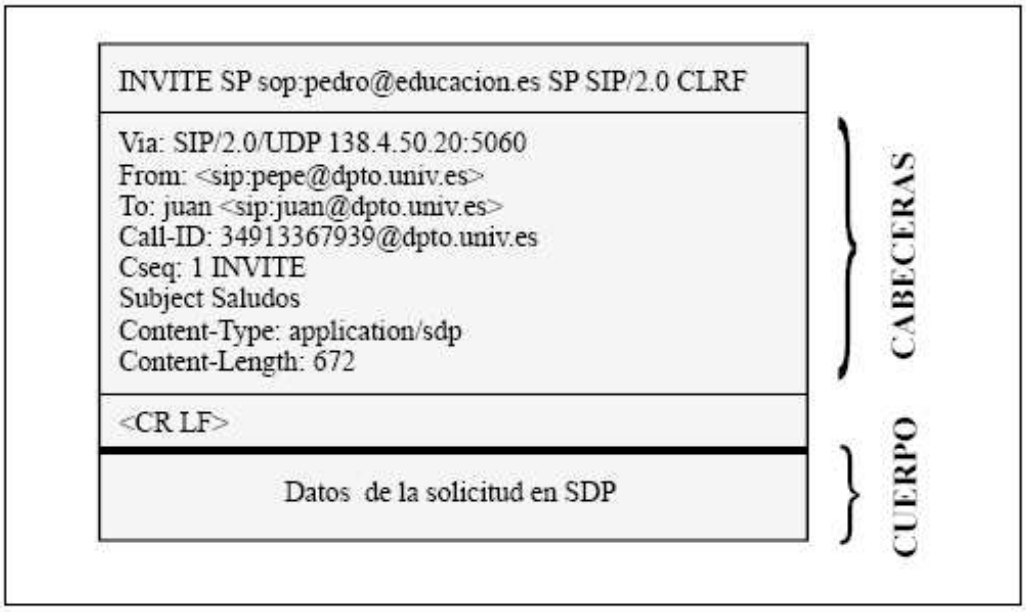


Figura. 2.25. Ejemplo de un mensaje de solicitud SIP

Generalmente, el orden en que aparecen las cabeceras no tiene mayor importancia, siempre que se cumpla que las cabeceras del tipo "salto a salto" (hop-by-hop) deben aparecer antes que cualquier cabecera del tipo "extremo a extremo" (end-to-end). Las primeras pueden ser modificadas o añadidas por los servidores proxy, en cambio las segundas deben ser transmitidas por éstos sin modificación alguna.

Una implementación mínima de SIP bebe cumplir, en relación con los elementos funcionales clientes y servidores, lo siguiente: A nivel de Clientes: deben ser capaces de generar las solicitudes INVITE y ACK, así como las cabeceras Call-Id, Content-Length, Content-Type, Cseq, Require, From y To. También deben "entender" el protocolo SDP y ser capaces de reconocer las clases 1 hasta la 6 de los status code.

Y como Servidores: deben "entender" las solicitudes INVITE, ACK, OPTIONS y BYE. De tratarse de servidores proxy, también la solicitud CANCEL. También deben ser capaces de generar de manera apropiada las cabeceras Call-Id, Content-Lenght, Content-Type, CSeq, Expires, From, Max- Forwards, Require, To y Via.

2.6.3. DIRECCIONAMIENTO SIP [11]

Una de las funciones de los servidores SIP es la localización de los usuarios y resolución de nombres. Normalmente, el agente de usuario no conoce la dirección IP del destinatario de la llamada, sino su e-mail.

Las entidades SIP identifican a un usuario con las SIP URI (Uniform Resource Identifiers) definido en el RFC 2396. Una SIP URI tiene un formato similar al del e-mail, consta de un usuario y un dominio delimitado por una @, como muestra los siguientes casos:

usuario@dominio, donde dominio es un nombre de dominio completo.

usuario@equipo, donde equipo es el nombre de la máquina.

usuario@dirección_ip, donde dirección_ip es la dirección IP del dispositivo.

número_teléfono@gateway, donde el gateway permite acceder al número de teléfono a través de la red telefónica pública.

La solución de identificación de SIP, también puede ser basada en el DNS (descrito en el RFC 3263), donde se describen los procedimientos DNS utilizados por los clientes para traducir una SIP URI en una dirección IP, puerta y protocolo de transporte utilizado, o por los servidores para retornar una respuesta al cliente en caso de que la petición falle.

2.6.4. DESCRIPCIÓN DE SDP (*SESSION DESCRIPTION PROTOCOL*) [11]

El protocolo de descripción de sesión (SDP, RFC 2327), se utiliza para describir sesiones multicast en tiempo real, siendo útil para invitaciones, anuncios, y cualquier otra forma de inicio de sesiones.

La propuesta original de SDP fue diseñada para anunciar información necesaria para los participantes y para aplicaciones de multicast MBONE (Multicast Backbone). Actualmente, su uso está extendido para el anuncio y la negociación de las capacidades de una sesión multimedia en Internet. Puesto que SDP es un protocolo de descripción, los mensajes SDP se pueden transportar mediante distintos protocolos con SIP, SAP, RTSP, correo electrónico con aplicaciones MIME o protocolos como HTTP. Como el SIP, el SDP

utiliza la codificación del texto. Un mensaje del SDP se compone de una serie de líneas, denominados campos, dónde los nombres son abreviados por una sola letra, y está en una orden requerida para simplificar el análisis. El SDP no fue diseñado para ser fácilmente extensible. La única manera de ampliar o de agregar nuevas capacidades al SDP es definir un nuevo atributo. Sin embargo, los atributos desconocidos pueden ser ignorados. En la tabla siguiente podemos observar todos los campos.

Tabla. 2.6. Descripción de la sesión

Tipo	Descripción	Obligatorio
V	Versión del protocolo	o
o	Identificador	o
S	Nombre de sesión	o
I	Información de la sesión	o
U	URI de la descripción	*
e	Dirección de correo	*
p	Número de teléfono	*
C	Información de conexión	*
b	Ancho de banda	*
Z	Tiempo de corrección	*
K	Clave de encriptación	*
a	Atributos	*
T	Tiempo de sesión(Start y stop)	o
R	Tiempo de repetición	*
m	Información del protocolo de transporte(media)	o

2.6.5. FASES DE UNA LLAMADA SIP [11]

En una llamada SIP hay varias transacciones SIP, cuya transacción se realiza mediante un intercambio de mensajes entre un cliente y un servidor. Consta de varias peticiones y respuestas y para agruparlas en la misma transacción esta el parámetro CSeq.

Inicialmente las dos primeras transacciones corresponden al registro de los usuarios. Los usuarios deben registrarse para poder ser encontrados por otros usuarios. En este caso, los terminales envían una petición REGISTER, donde los campos from y to corresponden al usuario registrado. El servidor Proxy, que actúa como Register, consulta si el usuario puede ser autenticado y envía un mensaje de OK en caso positivo.

La siguiente transacción corresponde a un establecimiento de sesión Esta sesión consiste en una petición INVITE del usario a proxy. Inmediatamente, el proxy envía un TRYING 100 para parar las retransmisiones y reenvía la petición al usuario B. El usuario

B envía un Ringing 180 cuando el teléfono empieza a sonar y también es reenviado por el proxy hacia el usuario A. Por ultimo, el OK 200 corresponde a aceptar la llamada (el usuario B descuelga).

Posteriormente en el momento que la llamada está establecida, pasa a funcionar el protocolo de transporte RTP con los parámetros (puertos, direcciones, codecs, etc.) establecidos en la negociación mediante el protocolo SDP.

La última transacción corresponde a una finalización de sesión. Esta finalización se lleva a cabo con una única petición BYE enviada al Proxy, y posteriormente reenviada al usuario B. Este usuario contesta con un OK 200 para confirmar que se ha recibido el mensaje final correctamente.

2.7. PROTOCOLODE SEÑALIZACIÓN: MEGACO y MGCP [11]

H.323 y SIP se desarrollaron teniendo como objetivo el desarrollo de terminales que estuvieran directamente conectados a la red IP e intercambiaran tráfico de voz directamente entre sí o bien con terminales tradicionales (conectados a redes conmutadas) mediante el uso de pasarelas. El objetivo inicial de MEGACO fue la utilización de redes de paquetes como backbone para la transmisión de tráfico de voz originado por redes tradicionales. Los operadores tradicionales fueron uno de los que mayor interés han mostrado en esta propuesta, pensando en integrar progresivamente sus redes de telefonía basadas en conmutación de circuitos y sus redes de datos basadas en conmutación de paquetes en una red homogénea que transportará ambos tipos de tráfico (voz y datos) y que fuera transparente a los usuarios finales. MEGACO (Media Gateway Control)/H.248 elaborado de manera conjunta por IETF/ITU-T, resuelve este problema dividiendo las pasarelas en tres entidades diferentes:

2.7.1. ENTIDADES [11]

a) Pasarelas de medios (Media Gateways - MG).

Son básicamente matrices de conmutación con puertos TDM y puertos de datos, con capacidad de traducir señal TDM a paquetes IP y con funcionalidades VoIP y RAS. Según su función específica o su ubicación, los media gateways se pueden clasificar en:

MG's residenciales (entre teléfonos y red IP);

MG's troncales (entre redes PSTN y red IP);

MG's de acceso (entre PBX's y red IP).

b) Pasarelas de señalización (Signalling Gateways - SG).

En este caso, este elemento realiza la traducción de la señalización SS7 a los protocolos de gestión de la sesión (H.323/SIP), cuyos mensajes procesa el softswitch. En ocasiones su funcionalidad la realiza directamente el media gateway o los controladores de sesión (Softswitches- SS).

c) Controlador de Medios (Media Gateway Controller - MGC).

Proporciona la señalización H.323 o SIP y realiza el mapping entre la señalización de redes tradicionales y las redes de paquetes. En un escenario habitual los tres elementos están físicamente separados de modo que pueden proporcionar ventajas como la concentración de muchos MG (conectados a usuarios finales) en algunos MGC controlados por un SG. La figura a continuación muestra la arquitectura de MEGACO:

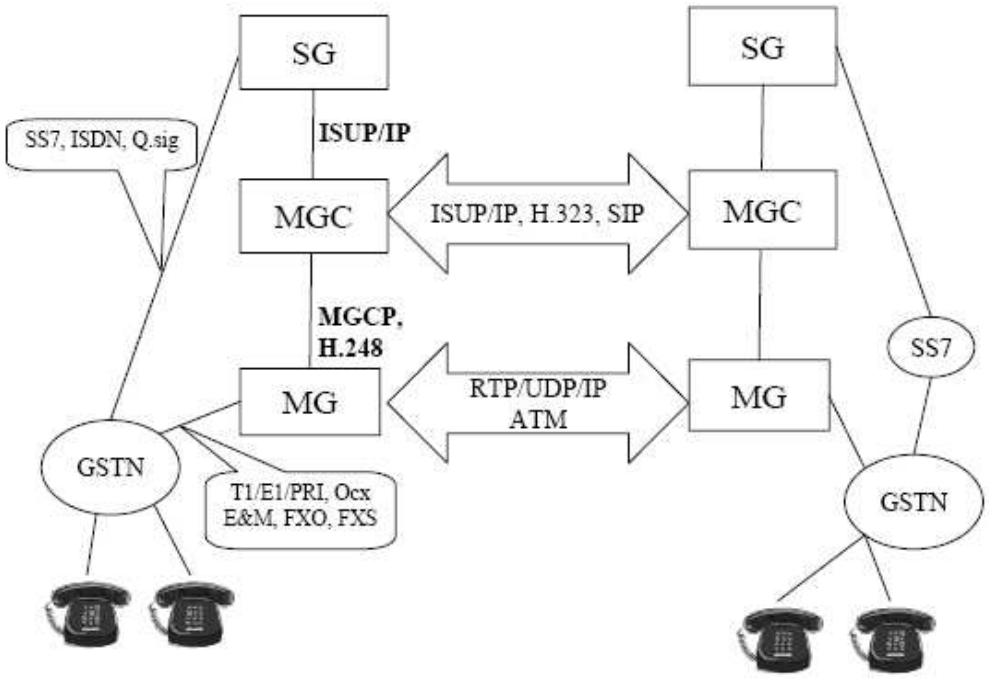


Figura. 2.26. Arquitectura de MEGACO

La conexión entre endpoints (teléfonos, software, etc.), a través de las redes IP se desarrolla bajo el control de los MGC y el MG que corresponda. Toda la información generada por los endpoints se maneja por el MGC, aunque el MG puede desarrollar también este tipo de tareas.

2.7.2. PROTOCOLO MGCP (MEDIA GATEWAY CONTROLLER PROTOCOL) [11]

Éste es un protocolo que permite comunicar al controlador de gateway MGC (también conocido como Call Agent) con las gateway de telefonía GW (hacia la PABX o PSTN). Se trata de un protocolo de arquitectura *master/slave* (maestro/esclavo), donde el MGC informa las acciones a seguir al GW. Los mensajes MGCP viajan sobre UDP/IP, por la misma red de transporte IP con seguridad IPsec.

El formato de trabajo genera una inteligencia externa a la red (concentrada en el MGC) y donde la red de conmutación está formada por los router de la red IP. El GW solo realiza funciones de conversión vocal (analógica o de velocidad digital) y genera un camino RTP entre extremos. La sesión de MGCP puede ser punto-a-punto o multipunto. Entrega a GW la dirección IP, el port de UDP y los perfiles de RPT; siguiendo los lineamientos del protocolo SDP. Los comandos disponibles en MGCP son:

• *Notifications Request*, indica al GW de eventos, como ser la señalización DTMF en el extremo.

• *Notification Command*, confirma las acciones del comando *NotificationsRequest*.

• *Create Connection*, usado para crear una conexión que se inicia en el GW.

• *Modify Connection*, usado para cambiar los parámetros de la conexión existente.

• *Delete Connection*, usado para cancelar la conexión existente.

• *AuditEndpoint*, usado para requerir el estado del extremo al GW.

• *AuditConnection*, usado para requerir el estado de la conexión.

• *RestartInProgress*, usado por el GW para notificar que un grupo de conexiones se encuentran en falla o reinicio.

• *EndpointConfiguration*, usado para indicar al GW las características de codificación esperadas en el extremo final.

Obsérvese que los comandos *AuditEndpoint* y *AuditConnection* permiten obtener información que posteriormente forman parte de la MIB y pueden consultadas mediante el protocolo SNMP por el sistema de Management.

Como respuesta al comando *DeleteConnection* el GW envía una serie de informaciones obtenidas desde el protocolo RTP: número de paquetes y de Bytes emitidos; número de paquetes y Bytes recibidos; número de paquetes perdidos; jitter promedio en mseg, retardo de la transmisión.

2.8. COMPONENTES DEL SISTEMA DE TELEFONÍA IP [11]

Las necesidades de equipamiento que implica cada una de las modalidades de funcionamiento varían. Cuando la comunicación es entre ordenadores, únicamente es necesario que dispongan deciertos elementos (tarjetas de sonido, micrófono y altavoz, software de comunicación). Sin embargo,el problema es mucho mayor cuando en uno o en los dos extremos de la comunicación existe un terminal telefónico. En estos casos se hace necesario el uso de ciertos equipos, conocidos como pasarelas.

De lo anterior, los principales son:

2.8.1. TERMINALES DE USUARIO [11]

Pueden encontrarse clientes que desean utilizar sus teléfonos convencionales y aquellos que cambian hacia una ToIP integrada con su LAN. Cuando un cliente desea instalar un servicio integrado de telefonía y datos, la red LAN es donde se conectan los terminales, los elementos de interconexión al exterior (router, proxy o gateway) y el gatekeeper GK local. El servicio de ToIP puede ofrecerse sin necesidad de una LAN, por ejemplo mediante líneas analógicas que se conectan a la vieja PABX del usuario.

En el caso de utilizar la LAN, los terminales se comunican en forma bidireccional en tiempo real. Se utilizan software en la PC (SoftPhone) o teléfonos dedicados (IP-Phone).

De esta forma el mismo terminal de cableado estructurado se utiliza para ambos componentes del escritorio (el teléfono y la PC). Para el caso de utilizar la vieja PABX, se requiere instalar un Gateway de usuario FXS o E1.

2.8.2. GATEWAY [11]

El Gateway es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red IP con la red telefónica analógica. Podemos considerar al Gateway como una caja que por un lado tiene un interface LAN y por el otro dispone de uno o varios de los siguientes interfaces:

- FXS. Para conexión a enlaces o a teléfonos analógicos.
- FXO. Para conexión a líneas de la red telefónica.
- E&M. Para enlaces de audio de 4 hilos.
- BRI. Acceso básico RDSI.
- PRI. Acceso primario RDSI.
- G703/G.704. (E&M digital) Conexión especifica a un conmutador a 2 Mbps.

La primera de las interfaces es llamada FXS (estación de intercambio remota o "*foreing exchange station*"), la cual se conecta directamente a teléfonos ó faxes. La interface FXO (oficina de intercambio remota o "*foreign exchange office*") se conecta a un PBX y proporciona accesos externos mientras que la interface E&M (interface de un dispositivo VOIP) se conecta a las líneas troncales de un PBX. Varios gateways de VoIP también ofrecen interfaces de tipo E&M.

Dentro de este contexto, el núcleo del sistema propuesto por Cisco, que es “Cisco Call Manager Express (CME), el cual consiste en un software que se instala en los routers Cisco (con soporte para voz), ejerce dentro de una multitud de servicios, la de pasarela del sistema de telefonía IP con las centralitas PBX tradicionales.

Esta es una solución ideal para empresas con necesidades inferiores a 100 usuarios. Y en caso que las necesidades de la empresa sean mayores es aconsejable utilizar CM (Cisco Call Manager).

2.8.3 IP-PBX (INTERNET PROTOCOL-PUBLIC BRANCH EXCHANGE) [11]

Debido a que la ventaja de las IP-PBX es poder conectar un grupo de gente con otros grupos en locaciones remotas, está destinada a utilizarse en empresas u organizaciones con buen tráfico de larga distancia o en sucursales de empresas internacionales.

Una central IP-PBX es un conmutador telefónico que maneja todas las comunicaciones externas e internas por ToIP. De esta manera todos las extensiones manejadas por este equipo terminan en teléfonos IP, teléfonos comunes con ATA, u otros servidores SIP.

Otras funciones de una IP-PBX son:

• voice mail personalizado.

• ACD (*automatic call distribution*): coloca los llamados en colas y los rutea a los grupos. Si dentro de un grupo una extensión esta ocupada, el llamado es ruteado a la próxima extensión libre de ese grupo.

• IVR (*interactive voice response*): reconoce sonidos y automáticamente ejecuta una acción. Ejemplos: ayuda al ACD a reconocer los tonos de discado; interactúa con base de datos (ejemplo clásico es obtener el saldo de la cuenta bancaria por teléfono).

• Dial plan: muy importantes en centrales IP-PBX, permite automáticamente permitir/ bloquear/ reemplazar dígitos / anteponer dígitos a números discados desde las extensiones. El dial plan permite rutear llamados locales al gateway para salir a línea convencional. El dial plan es totalmente configurable.

• Todas las funciones de las centrales telefónicas convencionales

Las funciones anteriores hacen que el IP-PBX sea optimo para ser utilizado como *Call Center* ubicados en lugares remotos.

2.8.4. SERVIDORES [11]

El servidor provee el manejo y funciones administrativas para soportar el enrutamiento de llamadas a través de la red. En un sistema basado en H.323, el servidor es conocido como un Gatekeeper. En un sistema SIP, el servidor es un servidor SIP. En un sistema basado en MGCP o MEGACO, el servidor es un *Call Agent* (Agente de llamadas).

El gatekeeper actúa en conjunción con varios gateways, y se encarga de realizar tareas de autenticación de usuarios, control de ancho de banda, encaminamiento IP, siendo el cerebro de la red de telefonía IP.

Los servidores SIP actúan generalmente como varios tipos de servidores de forma simultánea (servidores de redirección, de registro y proxys). Gracias a una infraestructura de servidores SIP, es posible gestionar las llamadas de forma distribuida entre equipos personales, equipos de proveedores de servicios y pasarelas corporativas, con la consiguiente flexibilidad y control por parte del usuario, que puede mantener la privacidad de sus datos personales en todo momento.

El *Call Agent* puede actuar como punto de origen y terminación para protocolos SCN (ISUP/SS7, Q.931/DSS1). Casi toda la "inteligencia" recae en los MGC's y una pequeña parte en los G's. Por lo tanto es adecuado cuando los terminales disponen de poca inteligencia como son los teléfonos convencionales.

Dentro de la arquitectura, además encontramos los Servidores *Backend*, que corresponde a la serie de aplicaciones de *backoffice* que constituyen el corazón del sistema operativo de un proveedor de servicios. Poseen las bases de datos inteligentes y redundantes que almacenan información crítica que intercambian con los gatekeepers durante las fases de inicio y término de las llamadas. En el entorno de una oficina central, resulta vital preservar la integridad de las bases de datos de *backend*. La solución ofrece un enfoque único que garantiza la resistencia de los servidores de *backend* y la seguridad de sus bases de datos. Los servidores SQL (*Structured Query Language*) de Microsoft están integrados dentro de la arquitectura del sistema de *backend* y administran las bases de datos SQL para las funciones de autentificación, mapeo de directorios, contabilidad y determinación de tarifas. Este nivel de la arquitectura fue optimizado a fin de responder a las necesidades exclusivas de seguridad y disponibilidad de los proveedores de servicios.

Para implementaciones a menor escala, el sistema ofrece flexibilidad para consolidar las bases de datos en un solo servidor robusto o en la plataforma de un gatekeeper.

2.8.5. ADAPTADOR ANÁLOGO PARA EL TELÉFONO (ATA) [11]

Un *Analog Telephone Adaptor* es un dispositivo para conectar un teléfono estándar a un computador o a una red para que el usuario pueda hacer llamadas telefónicas por la Internet.

Llamadas de larga distancia basadas en la Internet son substancialmente más baratas que las llamadas transmitidas sobre el sistema telefónico tradicional, y los ATA's son generalmente más baratos que teléfonos especializados para ToIP que se conectan al puerto USB de un computador.

Hay varios tipos de adaptadores análogos para el teléfono. Todos los ATA's crean una conexión física entre un teléfono y un computador o un dispositivo de red. Algunos efectúan conversión de análogo a digital y conectan directamente a un servidor VoIP, mientras que otros utilizan software para cualquiera o las dos tareas.

2.8.6. LAS NUBES IP Y PSTN [11]

Los Router conforman la "nube" IP. Son los componentes que distribuidos en la red IP permiten el enrutamiento de los paquetes entre Gateways (reemplazan a los centros de conmutación de las PSTN). La PSTN (*Public Switched Telephone Network*) conforma la "nube" de telefonía convencional con conmutación de circuitos.

2.8.7. OPERADORES [11]

Para acceder a Internet, es necesario contratar el servicio correspondiente a un Proveedor de Servicio Internet (ISP). El ISP, por su parte, recurre generalmente a una Compañía Telefónica Local (para el caso de usuarios residenciales), para que ésta suministre la conexión física con el computador del usuario, que se establece mediante una llamada telefónica convencional (acceso conmutado a Internet), o mediante un equipo

adicional que deja libre a la línea telefónica y crea una vía separada para Internet (acceso de banda ancha a Internet). Para el caso de usuarios privados o “corporativos”, no se requiere de este último, debido a que la conexión física consiste en una red diseñada por la propia empresa.

Además de los dos tipos de operadores recién mencionados (ISP y Compañía Telefónica Local), en Internet existe un tercer tipo de operadores conocido como Proveedor de Aplicaciones sobre Internet (ASP), tales como Yahoo, E-Bay, Hotmail o Skype, que venden o regalan sus respectivos servicios a los usuarios de Internet. Por ejemplo, RedVoiss S.A. es un “ASP” cuyo rubro principal es la prestación de servicios de ToIP. Conocidos también como ITSP, *Internet Telephony Service Provider*.

Para expandir el servicio de ToIP (internacional), se requiere de acuerdos entre varios ITSP. Para ello, hay que tener en cuenta los conceptos de "*clearinghouse*" e “interoperatividad”.

Los servicios de *clearinghouse* son ofrecidos por proveedores de servicios de interconexión entre varios ISTP, denominados “Proveedores de Servicios de *Clearinghouse*” (CSP), a través de los cuales, un ISTP puede generar mayores ingresos económicos, intercambiando minutos de tráfico con otros ITSP. Una vez firmado un acuerdo con un CSP, el ITSP puede terminar minutos generados desde sus clientes, más allá de su propia red de gateways y, por consiguiente, también puede terminar el tráfico generado por otros ITSP en su propia red de gateways.

Los CSP facilitan a un ITSP la ardua y costosa tarea de llegar a un acuerdo individual y bilateral con otros ITSP para terminar las llamadas en los gateways remotos de cada ISTP. Por lo tanto, el ITSP sólo tiene que negociar con el CSP, que manejará el encaminamiento de llamadas, administración de la red, autorización de llamadas y liquidación económica del acuerdo. Ejemplos de CSP son ITXC, AT&T y Arbinet.

También al margen de un CSP, los ITSP pueden intercambiar minutos de tráfico con otros ITSP. Para ello, es muy importante considerar el equipamiento necesario para ToIP. Este debe ser compatible con los estándares del mercado y, por lo tanto, asegurar una completa interoperatividad con los productos existentes.

2.9. SEGURIDAD DE LOS SERVICIOS DE TELEFONÍA IP [11]

Como la ToIP consiste, en definitiva, en datos que viajan por la red, en cuanto a seguridad tiene los mismos riesgos que el resto de los datos que viajan por ella pero también puede tener la misma protección.

La "seguridad" de los servicios telefónicos por IP requiere por lo menos de confidencialidad y disponibilidad. Actualmente hay varios tipos de ataques (DoS, *Eavesdropping, hijack*) que son producidos por deficiencias en el protocolo TCP/IP. Los dispositivos de redes, los servidores y sus sistemas operativos, los protocolos, los teléfonos y su software, todos son vulnerables.

Dado lo anterior, la minimización de los riesgos de confidencialidad, disponibilidad, Integridad y la posibilidad de lograr algún grado de autenticación se logra por medio de la "Encriptación", que es el mecanismo más óptimo para prevenir ataques. Se puede llevar adelante por medio de:

• VPN (Virtual Private Network);

• IPsec (Internet Protocol Security);

• SRTP (Secure Real-time Transport Protocol);

Y adicionalmente, se pueden emplear:

• Firewall; y

• Tecnología IDS/IPS (Intrusion Detection/Protection Systems).

2.9.1. VPN (VIRTUAL PRIVATE NETWORK) [11]

Una VPN o "red privada virtual" es una tecnología en la que se establecen canales seguros de comunicación que ofrecen protección a los datos transmitidos mediante el uso de algoritmos de encriptación y/o autentificación criptográfica. Una VPN es virtual porque no es físicamente una red distinta, es privada porque la información que transita por los túneles es encriptada para brindar confidencialidad, y es una red porque consiste de

computadoras y enlaces de comunicación, pudiendo incluir enrutadores, switches y gateways de seguridad.

Esta tecnología punto a punto, es ampliamente adoptada en ambientes de transacciones financieras, y/o redes que requieren confidencialidad permanente, tanto en redes privadas como entre proveedores de Servicio de Internet y sus clientes. En el mercado existe una gran variedad de soluciones VPN, la figura siguiente se ilustra un ejemplo de interconexión de oficinas sucursales de un corporativo, interconectadas vía VPN usando la Internet como dorsal de su red. Cada oficina tiene un gateway de seguridad que provee una interfaz con Internet y la red interna del corporativo. Los gateways de seguridad se configuran para definir las políticas de control de acceso para cada oficina.

Las VPNs tienen cierto nicho de aplicación, en ambientes punto a punto que requieren canales seguros de forma permanente (telefonía IP, por ejemplo).

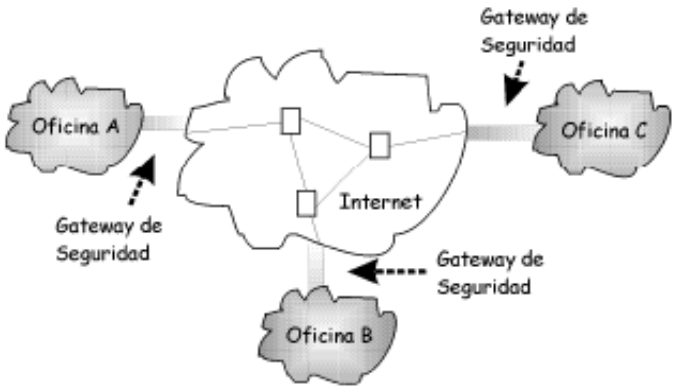


Figura. 2.27. Ejemplo. VPN interconectando las oficinas A, B, y C, utilizando Internet.

Por ello, los servicios de seguridad de IPSec (*Internet Protocol Security*) son ampliamente utilizados para la implementación de VPNs, así como también, otra solución para la confidencialidad e integridad del tráfico, es MPLS (*Multi Protocol Label Switching*). Las VPN basadas en IPSec y MPLS representan el siguiente nivel de la tecnología WAN, permitiendo la creación de redes multiservicio capaces de transportar cualquier tipo de tráfico.

2.9.2. IPSec (INTERNET PROTOCOL SECURITY) [11]

IPSec o "protocolo de seguridad IP" es un conjunto de extensiones al protocolo IP. Es un estándar de la IETF (Internet Engineering Task Force) definido en el RFC 2401,

diseñado para proveer seguridad interoperable de alta calidad basada en criptografía, tanto para IPv4 como para IPv6. Provee servicios de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa de Red, de tal forma que su funcionamiento es completamente transparente al nivel de aplicaciones, y es mucho más poderoso. IPSec provee un mecanismo estándar, robusto y con posibilidades de expansión, para proveer seguridad al protocolo IP y protocolos de capas superiores.

Es considerado una excelente opción para implementar VPN (*Virtual Private Networks*), de hecho se le conoce también como el protocolo VPN. Soporta dos modos de encripción: *Transport* y *Tunnel*. El "modo *Transport*" encripta solamente la porción de datos (carga) de cada paquete, pero no toca el encabezado. En cambio, el "modo *Tunnel*", más seguro, encripta tanto el encabezado como la carga del paquete. Del lado del receptor, un equipo compatible con IPSec decodifica cada paquete.

Para que funcione el IPsec, los dispositivos emisores y receptores tienen que compartir una clave pública. Esto se logra mediante un protocolo conocido como Internet *Security Association and Key Management Protocol/Oakley* (ISAKMP/Oakley), el cual le permite obtener al receptor una clave pública y autenticar al emisor usando certificados digitales.

2.9.3. SRTP (SECURE REAL-TIME TRANSPORT PROTOCOL) [11]

Igualmente, para la protección de la conversación puede lograrse utilizando, el protocolo SRTP (Secure Real-time Transport Protocol), definido por la RFC 3711. Es una extensión del perfil de RTP (Real-time Transport Protocol), que incorpora confidencialidad encriptando el campo de voz del paquete, así como un mecanismo para comprobar la integridad del mensaje, es decir que no haya sido alterado en lo más mínimo y protección de reenvío para flujos (audio y/o video).

2.9.4. FIREWALL [11]

Es un sistema o grupo de sistemas que refuerzan la seguridad en las redes corporativas o proveedores de servicios con protocolos IP. El firewall determina los servicios que pueden ser accedidos desde el exterior de la red (desde la conexión a Internet). Todo el tráfico debe pasar por el firewall para ser inspeccionado.

El módulo de firewall instalado como un software sobre el router o servidor de acceso permite realizar las siguientes funciones:

• Control de acceso. Es el principal objetivo del firewall. Crea un perímetro de defensa diseñado para proteger las reservas corporativas. Acepta, rechaza y controla el flujo de paquetes basado en identificadores de capa 3 o aplicaciones. El principio de funcionamiento es: "todas las conexiones son denegadas a menos que estén expresamente autorizadas".

• Logging. Es el inicio de las conexiones entrantes y salientes. El uso de un sistema proxy y cache incrementa la velocidad de respuesta de estas operaciones.

• Traslación de direcciones. Permite realizar las funciones de NAT (*Network Address Translator*) asegura la supervisión de la información de entrada y salida. El NAT permite aliviar la escasez de direcciones IP y eliminar la necesidad de renumeración cuando se realiza un cambio de ISP.

• Autentificación. El proceso de autentificación involucra a 3 componentes: el servidor, el agente y el cliente.

• Reportes. El firewall ofrece un punto conveniente para monitorear (*Audit and log*) y generar alarmas.

El firewall genera dos áreas en una red: el área pública con facilidad de acceso desde el exterior (para visita de Web, por ejemplo) y el área interna, detrás del firewall que se encuentra protegida contra la penetración no deseada. El perímetro de defensa se denomina zona desmilitarizada DMZ (*De-Militarized Zone*) y puede ser accedida por un cliente externo. El firewall puede trabajar sobre un server o sobre un router. La ventaja es que se concentra esta acción en un centro de la red consolidado en lugar de estar distribuido en cada host. Esta acción es más útil cuando es llevada a cabo por el router de entrada a la red. Por otro lado, ofrece un punto óptimo para instalar el Web y FTP Server.

Al comunicarnos con usuarios externos a la red LAN, en ToIP, es casi seguro que estos firewalls no permitirán establecer la comunicación. Esto es porque los protocolos SIP y RTP son nuevos, y la mayoría de los firewalls no permiten tráfico SIP y RTP.

Algunas formas de resolver problemas de firewall son:

• Permitir en el firewall tráfico SIP y RTP abriendo el puerto 5060 para paquetes TCP y UDP.

• Abrir un rango de puertos UDP para RPTP. Configurando los PC de la red para que utilicen el rango de puertos que se configuró.

• Deshabilitar el NAT.

• Reemplazar el firewall por versiones que permitan el protocolo SIP.

Acotar los puertos TCP/UDP de un teléfono IP (hardware), resulta sencillo al ser un equipo dedicado, pero en los clientes software el rango de puertos es dinámico ya que hay múltiples aplicaciones sobre el mismo equipo utilizando recursos de red.

En la práctica, en el caso de utilizar un firewalls "*packet filtering*", se deben indicar todos los puertos que serán utilizados, ya que la función que realiza es la de simple filtrado de paquetes según reglas. En cambio cuando se dispone de un firewalls "*stateful inspection*" se puede simplificar el problema. Este tipo de firewalls es capaz de analizar y mantener las conversaciones, identificando protocolos como H.323 o SIP. Donde en este caso no sería necesario definir todos los puertos utilizados dinámicamente ya que el propio firewalls los puede obtener al analizar el cuerpo de los mensajes y establecimiento de llamadas.

2.9.5. TECNOLOGÍA IDS/IPS (INTRUSION DETECTION/PROTECTION SYSTEMS) [11]

La implementación de esta tecnología es otra de las opciones a la problemática de seguridad de los elementos que intervienen en los servicios de ToIP.

El sistema de detección/protección de intrusos (IDS/IPS) es un programa usado para detectar y/o prevenir accesos desautorizados a un PC o a una red. Están basados en una arquitectura para detección y prevención, en tiempo real, de intrusos de redes. Integra técnicas de análisis de firmas, anomalías del trafico de red e intentos de *Denial of Service* (DoS), permitiendo la detección y prevención precisa e inteligente de ataques en alta velocidad.

El Sistema de Detección de Intrusos o IDS (*Intrusion Detection System*) detecta y registra los ataques comunes y otras actividades sospechosas, por toro lado como Sistema de Prevención de Intrusos o IPS (*Intrusion Prevention Systems*) controla los paquetes de datos de entrada o salida en busca de transferencias de datos o métodos de transferencia sospechosos y reacciona de forma activa evitado este tipo de amenaza.

2.10. ESCENARIOS DE IMPLEMENTACIÓN DE TELEFONÍA IP

2.10.1. APLICACIONES EN EL ÁMBITO PRIVADO [12]

Muchas empresas han implementado redes de voz sobre paquetes para integrar en sus redes corporativas el tráfico de voz y datos. Estas redes son de tecnologías variadas, pero aquellas basadas en el protocolo IP son las más numerosas y nos concentraremos, entonces, en ellas.

Las aplicaciones más comunes son las empresariales y entre estas se destacan:

• La interconexión PBX tradicionales mediante la red IP.

• La utilización de IP-PBX, es decir aquellas que nativamente utilizan protocolos de transporte y señalización de voz sobre IP.

El plan de convergencia consiste en una serie de pasos para lograr la integración de los servicios de ToIP en empresas donde actualmente se encuentran un amplio parque de centralitas (PBX) como se muestra en la figura.

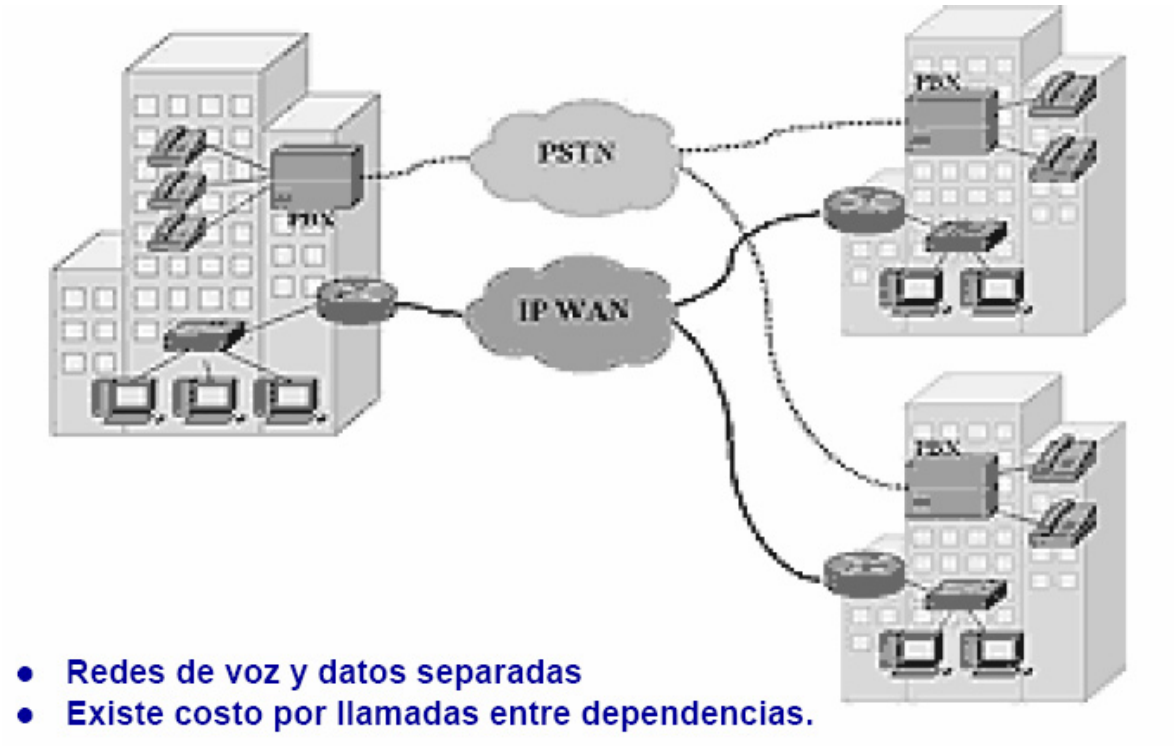


Figura. 2.28. Camino a la convergencia estado actual [12]

En este caso el cliente dispone de equipos tradicionales (centralitas y teléfonos analógicos o RDSI, etc.).

Dicha convergencia puede ser gradual, cuyo fin es eliminar la comunicación a través de la PSTN entre dependencias corporativas y obtener una red de ToIP totalmente pura.

Las PBX se conectan a través de un gateways de voz, que transporta punto a punto tanto la señalización interna de las PBX como los canales vocales, y además conecta las redes de datos que pudieran existir en cada sucursal. El transporte de estas informaciones puede hacerse utilizando la red IP que se utilizaba para la interconexión de las redes de datos. Este puede ser una red privada de la empresa en cuestión (empresas grandes), una VPN contratada a un operador público o una red privada virtual a través de Internet (pequeñas empresas). En este último caso la empresa debe tomar las precauciones de seguridad requeridas para el intercambio de información por Internet, por ejemplo encriptando la información mediante el uso del protocolo IPSec (IP Security) como se muestra a continuación en la figura.

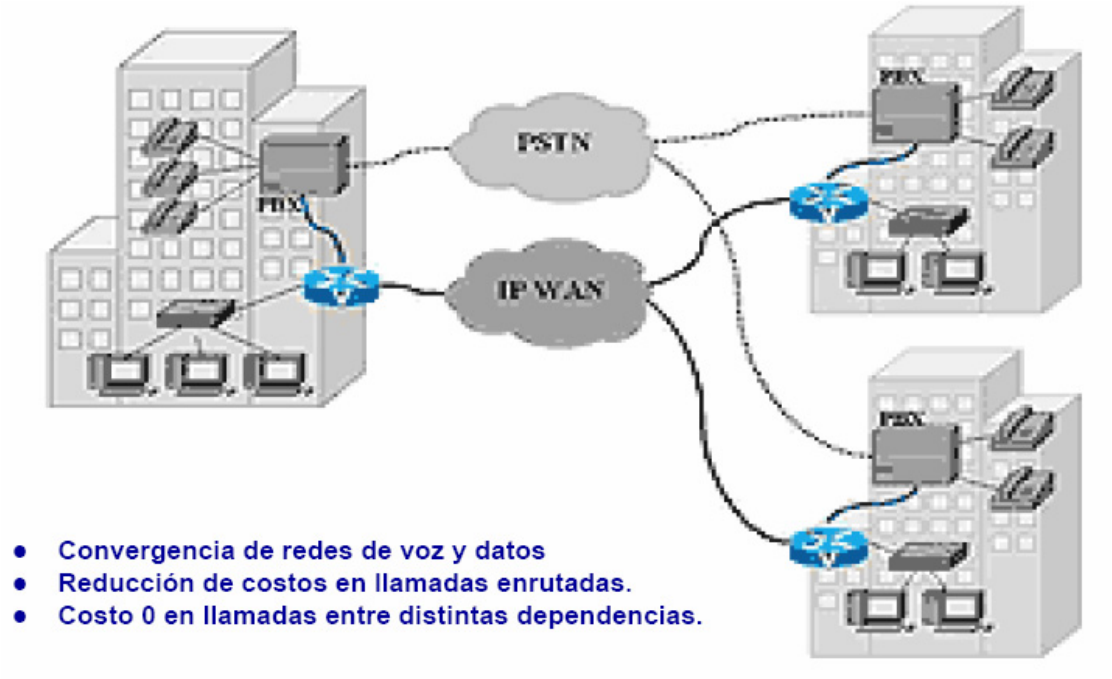


Figura. 2.29. Camino a la convergencia primer paso [12]

El siguiente paso es añadir una central IP-PBX que se encargue de la administración de los servicios de telefonía corporativos, y se proyecte a remplazar las antiguas centrales PBX que están ubicadas en cada sucursal.

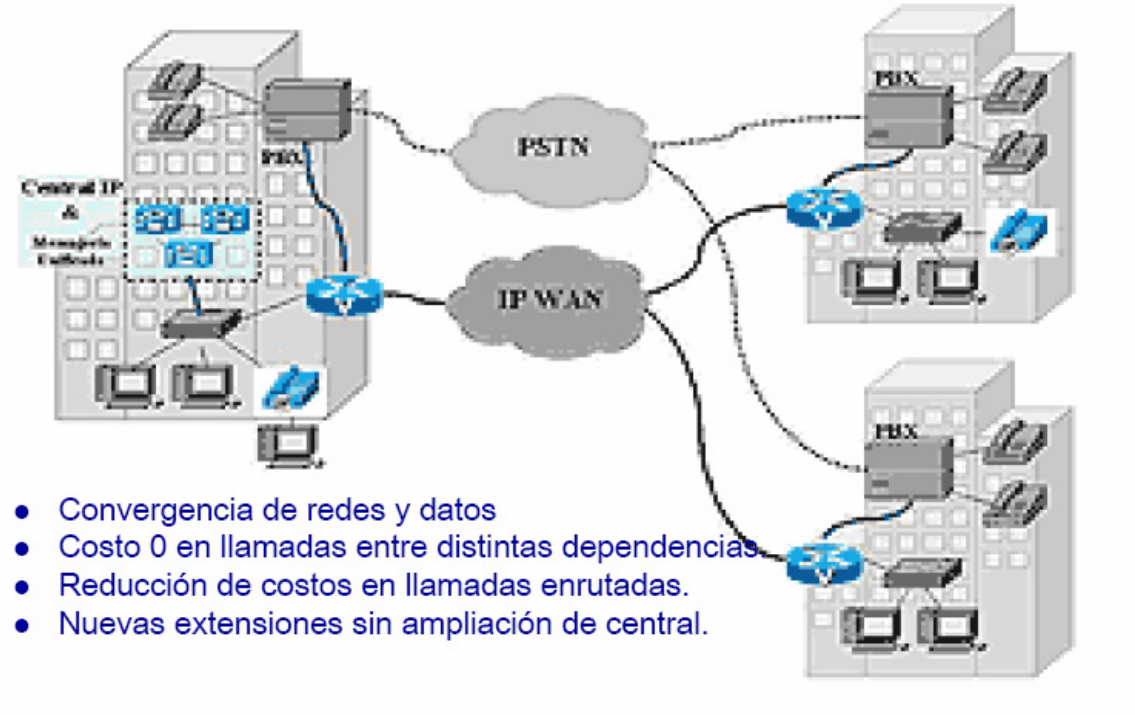


Figura. 2.30. Camino a la convergencia segundo paso

Finalmente se busca obtener una red completamente convergente que consta de una IP-PBX centralizada en la oficina principal y encargada de la administración y provisión de servicios a todas las sucursales, permitiendo que las mismas se comuniquen a través de la red de datos de una manera totalmente transparente y con un costo cero sin necesidad de recurrir a los servicios de la PSTN, los cuales serán requeridos solamente para comunicaciones hacia el exterior de la organización.

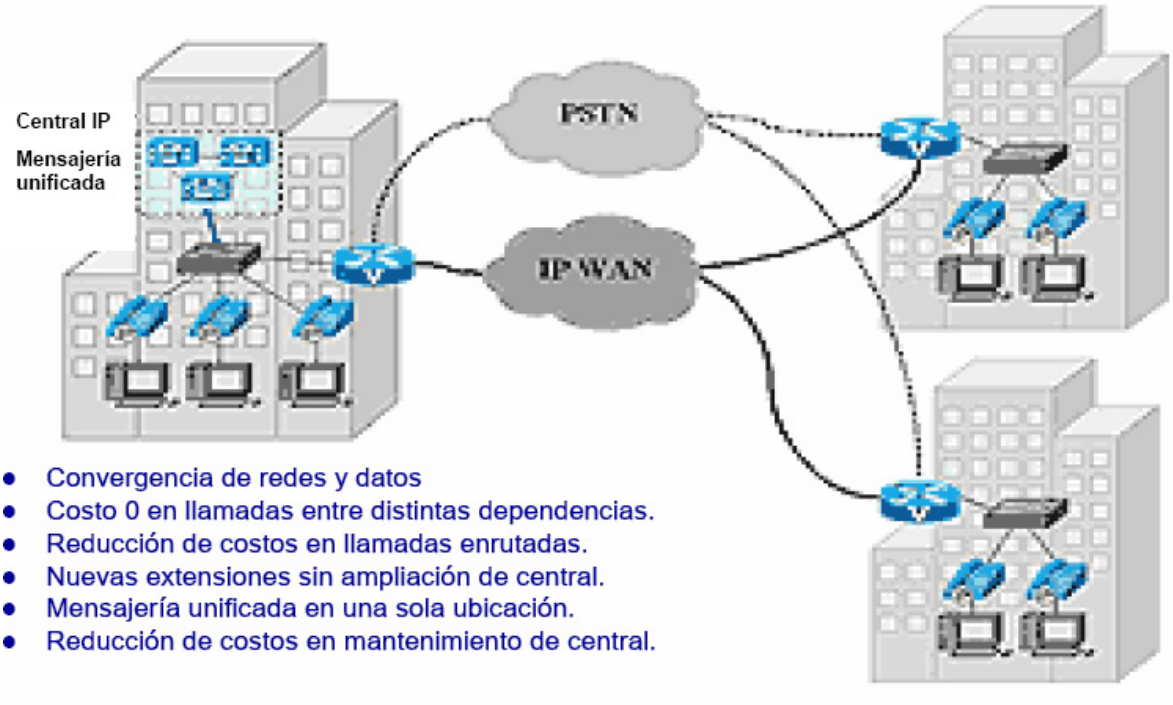


Figura. 2.31. Red totalmente convergente

2.10.2. APLICACIONES EN EL ÁMBITO PÚBLICO [11]

En el caso anterior existe la limitación que solo se pueden realizar llamadas entre las sucursales. Ahora de lo que se trata es el realizar llamadas al exterior utilizando la red IP interna.

El elemento esencial para poder interconectar la red IP a la PSTN es el “gateways”, que hace de interfaz entre la red IP y la red telefónica. El escenario más común es la combinación del acceso a la red pública, para poder acceder a terminales externos y la red privada para poder acceder a terminales de la propia red, es decir de la misma empresa.

La siguiente figura esquematiza la arquitectura de las “redes de nueva generación” (NGN - Next Generation Networks).

Según la ITU, la NGN se define como una red basada en paquetes capaz de ofrecer servicios de telecomunicaciones y hacer uso de múltiples tecnologías de transporte de banda ancha y QoS (Quality of Service/Calidad de Servicio), en la cual las funciones relacionadas con el servicio son independientes de las tecnologías subyacentes de transporte.

Estas redes NGN proporcionan servicios de ToIP privada, como también servicios de ToIP local pública.

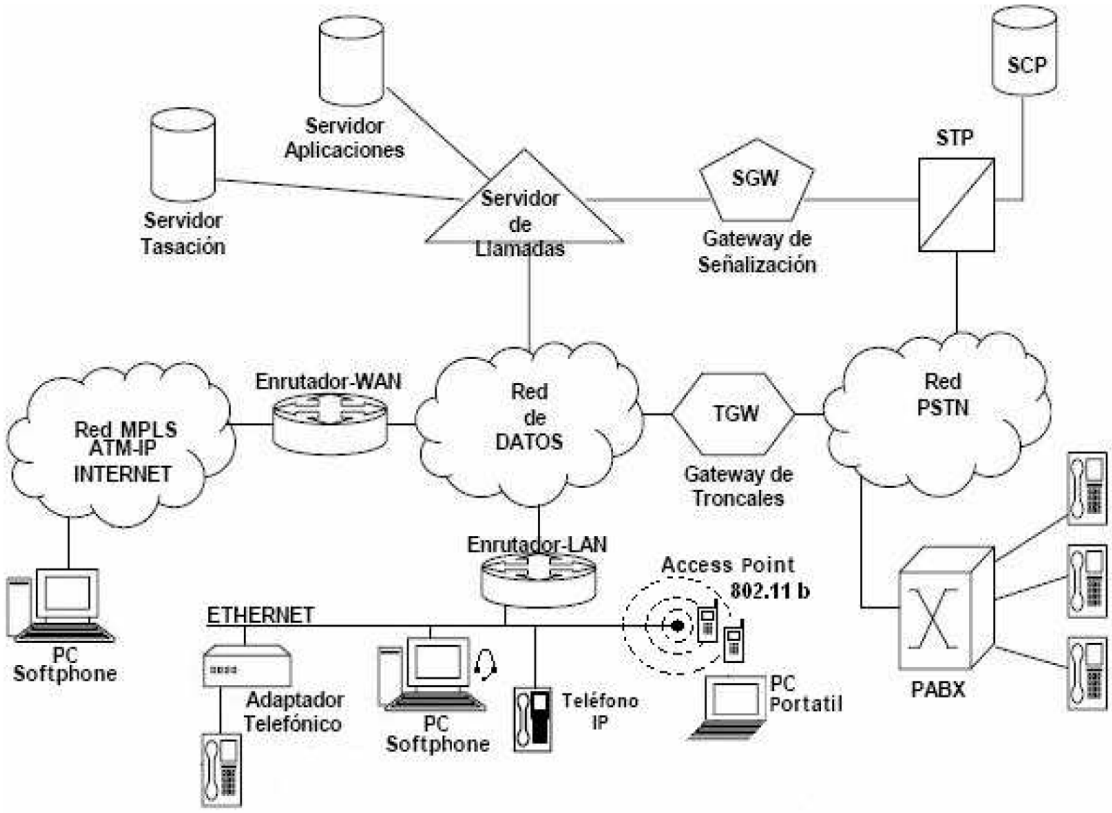


Figura. 2.32. Arquitectura de redes públicas de nueva generación [11]

Esta arquitectura permite la operación con la red de conmutación de circuitos. El Servidor de Llamadas es el corazón del sistema y su función es la de procesar los mensajes de señalización de ambas redes y hacer el interfuncionamiento necesario. Este bloque que se esquematiza como una única caja en realidad es un conjunto de componentes tales como Media Gateway Controllers que son los encargados de interactuar al nivel de señalización con la PSTN y servidores de VoIP, como por ejemplo “SIP Servers” o “Gatekeeper” (SIP o H.323), que encaminan los mensajes de señalización y procesan las llamadas dentro de la red IP. La conversión de la voz de circuitos a paquetes y viceversa es realizada por los

Media Gateways (Trunking Gateways) controlados por los Media Gateway Controllers del Servidor de Llamadas. El Signalling Gateway realiza las adaptaciones necesarias para transportar los mensajes de señalización número 7 sobre la red IP.

La red de ToIP irá avanzando hacia el abonado a través de Access Gateways que son dispositivos que controlan un gran número de líneas de telefonía tradicional y las convierten a VoIP controlados por los Servidores de Llamadas de clase 5 (Media Gateway Controllers de clase 5). Más cerca del cliente, e incluso en sus domicilios se ubican los IAD (Integrated Access Devices) estos realizan la conversión de la voz y la señalización de abonado a los protocolos de VoIP. También puede haber usuarios que directamente se conecten a la red IP a través de teléfonos IP (fijos-móviles).

A diferencia de los terminales IP "fijos", los terminales "móviles", se basan en el estándar para Redes Locales Inalámbricas (WLAN) 802.11b que permite entregar una solución práctica para redes inalámbricas de múltiples proveedores, y para igual número de aplicaciones. Disfrutando de las mismas facilidades y funcionalidad que el resto de los usuarios con terminales fijas. Para garantizar la seguridad de estas redes inalámbricas, existen varias alternativas, por ejemplo, los protocolos WEP (Wired Equivalency Protocol), o "Privacidad Equivalente al Alámbrico" y el WPA (Wi-Fi Application Protocol), o "Acceso Protegido Wi-Fi", que se encargan de autenticación, integridad y confidencialidad, proporcionados por los propios dispositivos inalámbricos, o IPsec (túneles).

Los servicios de voz (y multimedia) avanzados se dan a través de plataformas de servicio generalmente dedicadas a un determinado servicio que presentarán interfaces de programación estándar de manera que pueda utilizarse un entorno de creación de servicios también estándar que permita a terceras partes desarrollar servicios independientes de la plataforma "hardware" y sus fabricantes.

El advenimiento de las NGN, es una realidad en el desarrollo de las telecomunicaciones, condicionada por un grupo de circunstancias tecnológicas y de mercado. Las características de esta red, de hacer converger las redes de datos, voz y video, llaman la atención a operadores, fabricantes y usuarios por las ventajas que introduce desde el punto de vista tecnológico, social y económico.

Por ejemplo, la infraestructura de ToIP de Cisco Systems permite ofrecer multitud de servicios sobre una única plataforma, como: ToIP, VoIP, acceso a Internet, VPNs que permitan la interconexión entre las sedes de una empresa o el acceso a la LAN corporativa a tele-trabajadores.

CAPÍTULO III:

3. ANALISIS DE LA RED EXISTENTE Y OBTENCIÓN DE REQUERIMIENTOS

3.1. DESCRIPCIÓN DE LAS EDIFICACIONES DEL IMA

3.1.1. DESCRIPCIÓN DEL EDIFICIO MATRIZ

La infraestructura física de la matriz de la Ilustre Municipalidad de Ambato está conformada por un edificio estilo colonial antiguo, de 4 plantas ubicado en las calles Bolívar y Castillo, este edificio cuenta con un cuarto de telecomunicaciones y sus pisos están distribuidos de la siguiente manera:

Figura. 3.1. Edificio Matriz

Planta Baja

Atención al Cliente, Tesorería, Archivo, Plan Estratégico, Proveeduría, Laboratorio de suelos.

Primer Piso Alto

Dirección de Sistemas, Coordinación de Alcaldía, Sala de comisiones Consejales, Alcaldía, Dirección Administrativa, Comunicación Institucional, Secretaria General

Segundo Piso Alto

Asesoría Jurídica, Dirección Financiera, Renta, Contabilidad, Avalúos y Catastros, Planificación.

Tercer Piso Alto

Dirección de obras públicas.

Figura. 3.2. Distribución del edificio matriz

3.1.2. DESCRIPCIÓN DE LOS DEPARTAMENTOS EXTERNOS

Exteriormente el Municipio cuenta con varios departamentos y dependencias que están a cargo de su administración a continuación se detallaran los departamentos que por estar interconectados a través de la red WAN estarán dentro del alcance del presente estudio:

BODEGA MUNICIPAL

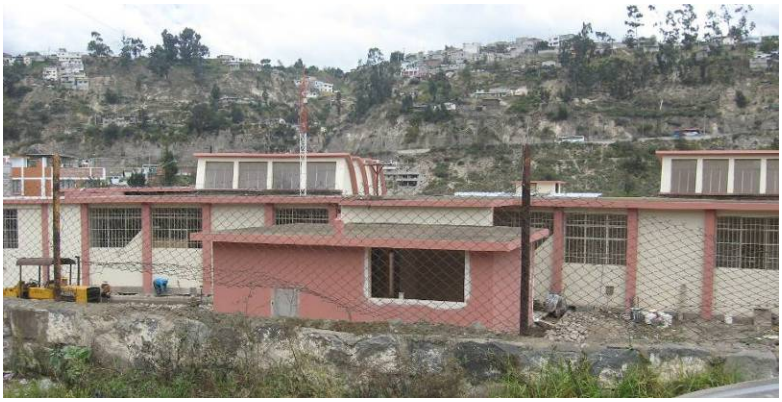


Figura. 3.3. Bodega Municipal

La Bodega Municipal está ubicada en las instalaciones del antiguo camal, aquí se realizan tareas de Administración, Control de Inventarios, y las bodegas en sí.

MERCADO MAYORISTA

Figura. 3.4. Mercado Mayorista

El Mercado Mayorista está ubicado en la avenida Bolivariana, aquí se realiza el acopio de los productos de primera necesidad de la ciudad, consta de las instalaciones necesarias para dicho fin y de un edificio administrativo.

DEPARTAMENTO DE CULTURA

Figura. 3.5. Departamento de Cultura

El departamento de Cultura, se encuentra ubicado en el monumento a la primera imprenta en Pinllo, en esta dependencia se realizan y gestionan las tareas concernientes al ámbito cultural de la cuidad.

UNIDAD MUNICIPAL DE TRANSITO

Figura. 3.6. Unidad Municipal de Transito

La unidad municipal de tránsito se encuentra ubicado en la ciudadela España, esta unidad es la encargada de la administración del tránsito en la cuidad, así como del terminal terrestre de la ciudad.

EDIFICIO DE LAS COMISARIAS

Figura. 3.7. Edificio de las Comisarias

El edificio de las comisarias está ubicado en la Av los Chasquis, aquí están distribuidas las diferentes comisarías que el municipio requiere para el manejo administrativo de la cuidad.

HOSPITAL MUNICIPAL

Figura. 3.8. Edificio del Hospital Municipal

El edificio del hospital municipal está ubicado en la ciudadela Letamendi, en esta dependencia se realizan las tereas necesarias para proveer de servicios de salud a la colectividad.

CAMAL MUNICIPAL

Figura. 3.9. Edificio del Camal Municipal

El nuevo camal municipal está ubicado en el parque industrial, sus instalaciones fueron construidas para satisfacer las necesidades específicas que requieren para las tareas de faenamiento de ganado.

En el anexo A encontramos una ilustración de la ubicación geográfica de todas las dependencias municipales, utilizando el servicio de *Google Earth.*

3.2. LEVANTAMIENTO DE LA RED DE DATOS IMA

A continuación se analizará la estructura y el funcionamiento de la red de datos existente en el IMA, con la cual sus usuarios comparten datos, documentos y otros servicios que brinda dicha red, actualmente es utilizada exclusivamente para la transmisión de datos y es totalmente independiente de la red telefónica.

En la descripción de la red se profundizará en el análisis del edificio matriz, pues, por razones presupuestarias, para la implementación del presente proyecto se ha considerado un plan de migración que contemple, un cambio total a telefonía IP en la matriz eliminando completamente su actual central telefónica analógica, mientras que en las otras dependencias se mantendrán sus respectivas centrales telefónicas analógicas, y su infraestructura como son los terminales y cableado, las mismas que serán enlazadas al sistema IP a través de pasarelas, para lograr la integración de las mismas, y por ende los beneficios propios de la telefonía IP.

3.2.1. RED DE DATOS DEL EDIFICIO MATRIZ

La ilustre municipalidad de Ambato como se describió en el apartado 3.1.1 está conformada por una planta baja y tres plantas altas, cada una de ellas posee un cableado horizontal de datos y uno de voz independientes ambos están tendidos con cable UTP CAT5e, la red de datos su comunica a través de un *backbone* vertical de fibra óptica que desemboca en la primera planta alta en la dirección de sistemas, donde se concentran los servidores y demás elementos de dicha red, la red de voz por su parte posee un *backbone* vertical con cableado UTP CAT 5e, que sale desde cada una de las plantas para converger en el rack principal en la dirección de sistemas. En la siguiente figura se muestra el diagrama unifilar del sistema de cableado estructurado del Municipio. Cabe destacar que el cableado no está certificado.

El tipo de topología empleada en la red del IMA es estrella.

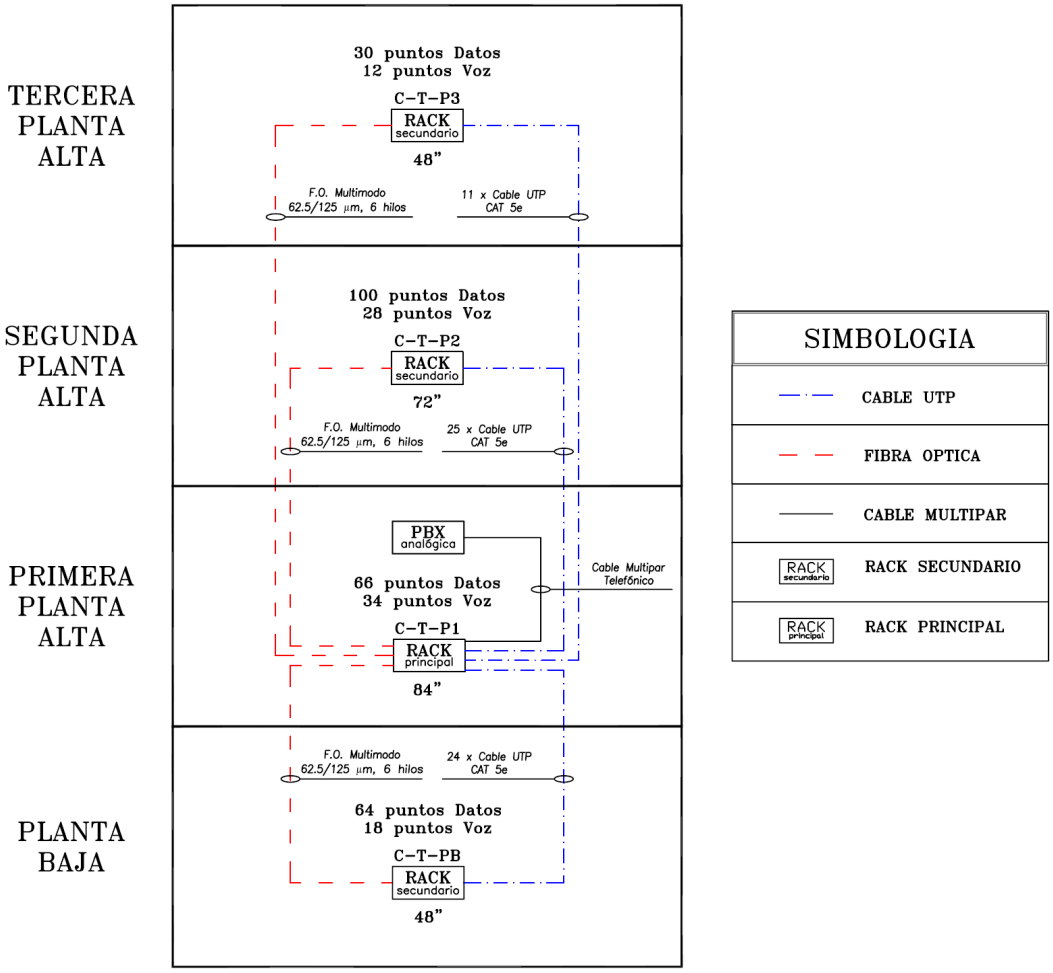


Figura. 3.10. Diagrama Unifilar de la Matriz

RACK PRINCIPAL C-T-P1 EN EL CUARTO DE EQUIPOS DE COMUNICACIONES DE LA PRIMERA PLANTA ALTA

El cuarto de equipos del edificio matriz está ubicado en la dirección de sistemas en la primera planta alta, aquí se encuentra el rack principal de comunicaciones, los servidores, además es donde converge el *backbone* de la red, los enlaces con el ISP, también es donde se ubica la central telefónica analógica.

En la figura 3.11 se observa el cuarto de equipos mientras que en la figura 3.12 encontramos el rack principal de comunicaciones.

Figura. 3.11. Cuarto de Comunicaciones

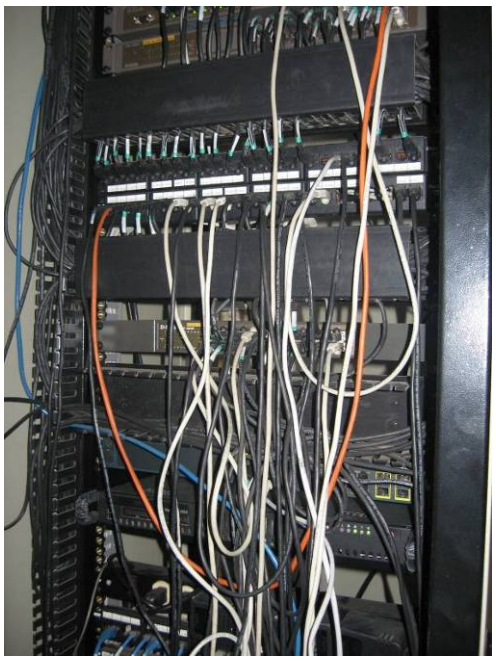


Figura. 3.12. Rack Principal C-T-P1 en Sistemas

Al rack principal de comunicaciones llega el cableado UTP CAT 5e de los 66 puntos de datos y 34 puntos de voz que se encuentran distribuidos en toda la primera planta alta como se muestra en el anexo C, además aquí converge el *backbone* vertical de datos de las tres plantas restantes cada una de las cuales llega con cable de fibra óptica multimodo 62.5/125 μm de 6 hilos; brindando una capacidad de tres enlaces por cada cable, de los cuales actualmente solo se utiliza uno. También encontramos el *backbone* de voz que llega desde todos los pisos a través de cables UTP CAT 5e que atraviesan verticalmente la edificación, para poder conectarse con la central telefónica analógica.

En este rack encontramos los siguientes equipos activos:

- Un *switch* marca D-Link DES-3226 el mismo que actúa como el *core* de la red de datos de la matriz, posee 24 puertos Fast Ethernet 10/100Mbps BASE-TX, aquí se conectan los servidores, los 3 enlaces de fibra óptica de cada una de las plantas del edificio, los mismos que antes de llegar a conectarse a los puertos 1, 2, 3, atraviesan por conversores marca D-Link DMC-300SC que realizan la transformación de interfaz óptica a eléctrica, la conexión a internet luego de atravesar por un servidor proxy llega al puerto 6, además en el puerto 20 está conectado el *switch* D-Link DES-1024R de este rack, los puertos restantes sirven para brindar acceso a puntos de datos de esta planta. Actualmente están utilizados 21 de los 24 puertos disponibles.

- Un *switch* marca D-Link DES-1024R, al cual se conecta en cascada por el puerto 24 el *switch* marca D-Link DES-1024D, además brinda acceso a los puntos de datos de la red, posee 24 puertos *Fast Ethernet* 10/100Mbps BASE-TX. Actualmente se utiliza la totalidad de los puertos disponibles en este equipo.

- Un *switch* marca D-Link DES-1024D, al cual se conecta en cascada por el puerto 22 el *switch* marca CISCO 2960, además brinda acceso a los puntos de datos de la red, posee 24 puertos *Fast Ethernet* 10/100Mbps BASE-TX. Actualmente se utiliza la totalidad de los puertos disponibles en este equipo.

- Un *switch* marca CISCO 2960 que fue recientemente anexado a la red, brinda acceso a los puntos de datos de la red, posee 24 puertos *Fast Ethernet*

10/100Mbps BASE-TX, 2 puertos Gigabit Combo Cobre/SFP. Actualmente se utilizan solo 10 puertos *Fast Ethernet*, quedando disponibles el resto de puertos incluyendo los dos de puertos Gigabit.

RACK SECUNDARIO C-T-PB DE LA PLANTA BAJA EN TESORERÍA

A este rack secundario de comunicaciones llega el cableado UTP CAT 5e de los 64puntos de datos y 18 puntos de voz que se encuentran distribuidos en toda la planta baja acorde al anexo B, de aquí sale *backbone* vertical de datos que llega al rack de comunicaciones principal con cable de fibra óptica multimodo 62.5/125 μm de 6 hilos; brindando una capacidad de transmisión para tres enlaces de los cuales actualmente se utiliza solo uno, también encontramos el *backbone* de voz que alcanza el rack principal a través de cables UTP CAT 5e que atraviesan verticalmente la edificación, para poder conectarse con la central telefónica analógica.

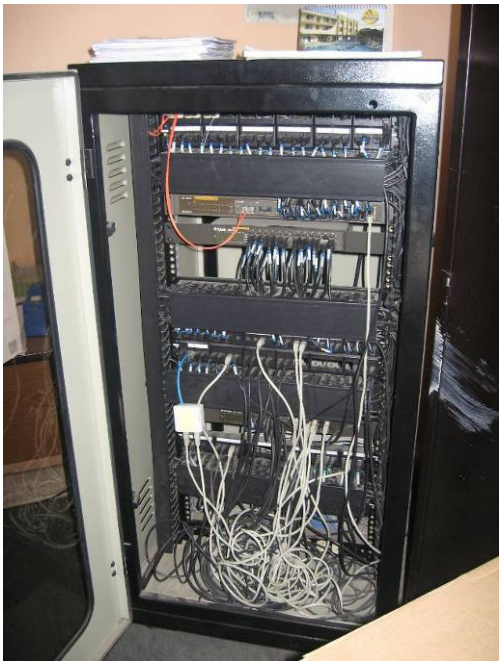


Figura. 3.13. Rack C-T-PB Secundario en Tesorería

En este rack encontramos los siguientes equipos activos:

- Un *switch* marca D-Link DES-1024R con el módulo DES-102F que provee de dos puertos 100BASE-FX de fibra óptica multimodo, de los cuales solo se usa uno para conectarse con el *core* de la red en el rack principal, posee 24 puertos *Fast Ethernet* 10/100Mbps BASE-TX a los cuales se conectan

los otros dos *switches* de este rack y sirven también para brindar acceso a los puntos de datos de esta planta. Actualmente se utilizan 21 de los 24 puertos disponibles en este equipo.

- Dos *switches* marca D-Link DES-1024D, mismos que brinda acceso a los puntos de datos de esta planta, poseen 24 puertos *Fast Ethernet* 10/100Mbps BASE-TX cada uno. Actualmente se utilizan 23 y 18 puertos de los 24 disponibles en cada uno.

RACK SECUNDARIO C-T-P2 DE LA SEGUNDA PLANTA ALTA EN CONTABILIDAD

A este rack secundario de comunicaciones llega el cableado UTP CAT 5e de los 100 puntos de datos y 28 puntos de voz que se encuentran distribuidos en toda la segunda planta alta acorde al anexo D, de aquí sale *backbone* vertical de datos que llega al rack de comunicaciones principal con cable de fibra óptica multimodo 62.5/125 μm de 6 hilos; brindando una capacidad de transmisión para tres enlaces de los cuales actualmente se utiliza solo uno, también encontramos el *backbone* de voz que alcanza el rack principal a través de cables UTP CAT 5e que atraviesan verticalmente la edificación, para poder conectarse con la central telefónica analógica.

Figura. 3.14. Rack Secundario C-T-P2 en Contabilidad

En este rack encontramos los siguientes equipos activos:

- Un *switch* marca D-Link DES-1024R con el módulo DES-102F que provee de dos puertos 100BASE-FX de fibra óptica multimodo, de los cuales solo se usa uno para conectarse con el *core* de la red en el rack principal, posee 24 puertos *Fast Ethernet* 10/100Mbps BASE-TX a los cuales se conectan los otros cuatro *switches* de este rack y sirven también para brindar acceso a los puntos de datos de esta planta. Actualmente se utilizan la totalidad de los puertos disponibles en este equipo.

- Tres *switches* marca D-Link DES-1024D, mismos que brinda acceso a los puntos de datos de esta planta, poseen 24 puertos *Fast Ethernet* 10/100Mbps BASE-TX cada uno. Actualmente se utilizan todos los puertos disponibles de estos equipos.

- Un *switch* marca D-Link DES-3226L, mismo que brinda acceso a los puntos de datos de esta planta, posee 24 puertos *Fast Ethernet* 10/100Mbps BASE-TX y 2 puertos Gigabit Combo Cobre/SFP. Actualmente se utilizan todos los puertos disponibles en este equipo excepto los dos puertos Gigabit.

RACK SECUNDARIO C-T-P3 DE LA TERCERA PLANTA ALTA EN OBRAS PÚBLICAS

A este rack secundario de comunicaciones llega el cableado UTP CAT 5e de los 30 puntos de datos y 12 puntos de voz que se encuentran distribuidos en toda la tercera planta alta acorde al anexo E, aquí por ser la planta más alta y por lo tanto más próxima a la terraza encontramos la conexión de la antena que enlaza a la matriz con la WAN municipal, además de aquí sale *backbone* vertical de datos que llega al rack de comunicaciones principal con cable de fibra óptica multimodo 62.5/125 μm de 6 hilos; brindando una capacidad de transmisión para tres enlaces de los cuales actualmente se utiliza solo uno, también encontramos el *backbone* de voz que alcanza el rack principal a través de cables UTP CAT 5e que atraviesan verticalmente la edificación, para poder conectarse con la central telefónica analógica.

Figura. 3.15. Rack Secundario C-T-P3 en Obras Públicas

En este rack encontramos los siguientes equipos activos:

- Un *switch* marca D-Link DES-1024R con el módulo DES-102F que provee de dos puertos 100BASE-FX de fibra óptica multimodo, de los cuales solo se usa uno para conectarse con el *core* de la red en el rack principal, posee 24 puertos *Fast Ethernet* 10/100Mbps BASE-TX a los cuales se conectan, el otro *switch* de este rack, la antena que conecta q la matriz con la WAN municipal y sirven también para brindar acceso a los puntos de datos de esta planta. Actualmente se utilizan 21 de los 24 puertos disponibles en este equipo.

- Un *switch* marca D-Link DES-1024D, mismo que brinda acceso a los puntos de datos de esta planta, poseen 24 puertos *Fast Ethernet* 10/100Mbps BASE-TX. Actualmente se utilizan 14 de los 24 puertos disponibles en este equipo.

DIAGRAMA LOGICO DE LA RED

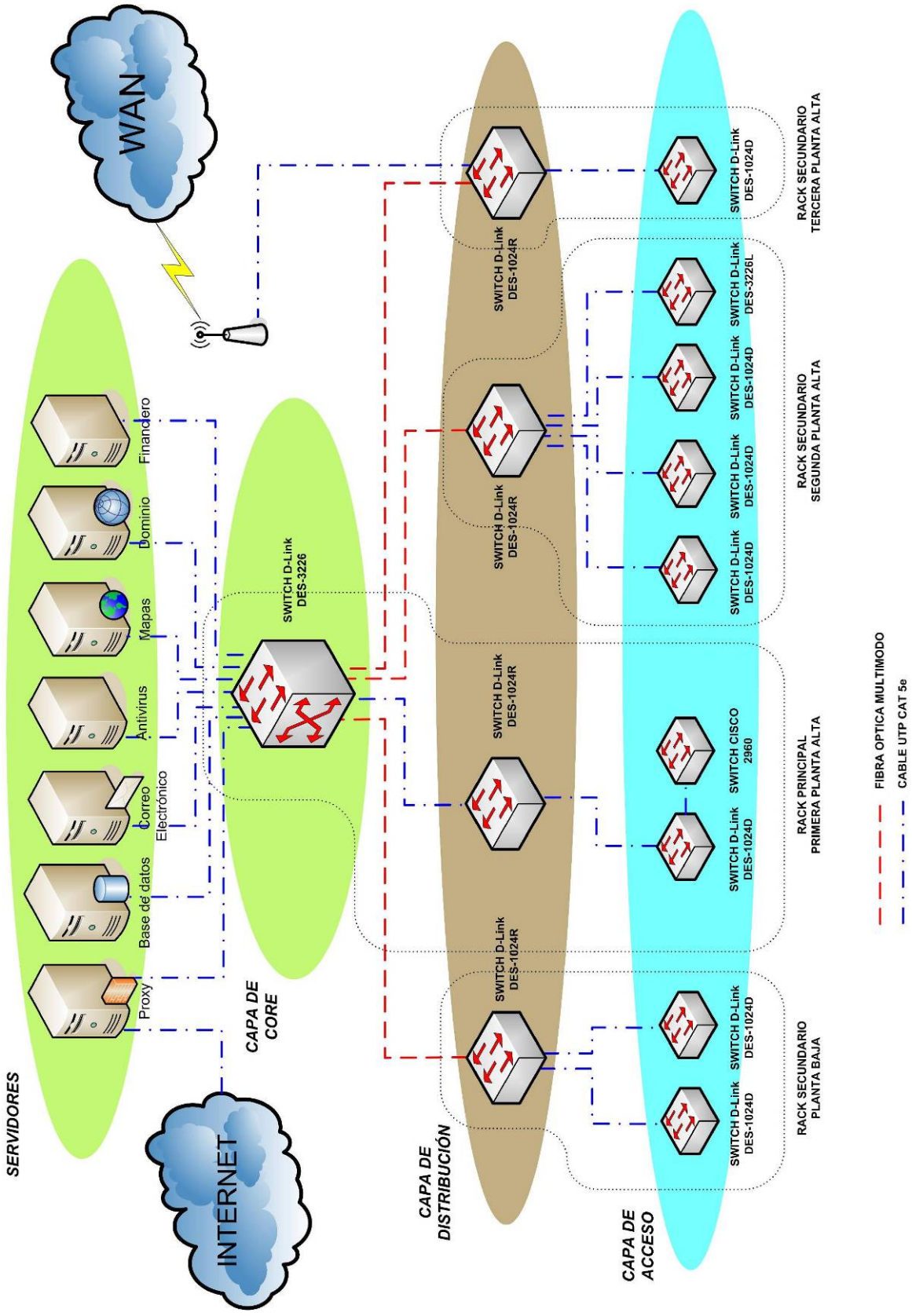


Figura. 3.16. Diagrama Lógico de la red de datos del edificio matriz

CARACTERÍSTICAS DE LOS *SWITCHES* DEL EDIFICIO MATRIZ

Tabla. 3.1. Características del switch D-Link DES-3226

Tipo	Switch administrable de capa 2
Velocidad de conmutación de paquetes	148,810 pps por puerto Fast Ethernet 1,488,100 pps por puerto Gigabit
Velocidad de backplane	8.8 Gbps
RAM Buffer	8MB
MAC soportadas	8K
Método de transmisión	Store-and-forward
Soporte Multicast	IGMP Snooping
Maneja hasta 255 VLANs	(Protocolo 802.1q)
Monitoreable	SNMP, RMON (4 grupos Alarmas, Eventos, Estadísticas, e Historia), MIB II
Spanning Tree Protocol	(802.1D)
Control de flujo	Protocolo 802.3X
QoS	(802.1p), 4 colas
Número de puertos:	24 puertos 10/100 Mbps 1 slot disponible para puertos de fibra óptica

Tabla. 3.2. Características del switch D-Link DES-3226L

Tipo	Switch administrable de capa 2
Velocidad de conmutación de paquetes	148,810 pps por puerto Fast Ethernet 1,488,100 pps por puerto Gigabit
Velocidad de backplane	8.8 Gbps
RAM Buffer	8MB
MAC soportadas	8K
Método de transmisión	Store-and-forward
Soporte Multicast	IGMP Snooping
Maneja hasta 255 VLANs	(Protocolo 802.1q)
Manejo de enlaces	802.3ad
Monitoreable	SNMP v1/v2/v3, RMON (4 grupos Alarmas, Eventos, Estadísticas, e Historia), MIB II
Spanning Tree Protocol	(802.1D/802.1s/802.1w)
Control de flujo	Protocolo 802.3X
QoS	(802.1p/DSCP/IP precedence), 4 colas
Número de puertos:	24 puertos 10/100 Mbps 2 Combo Gigabit Copper/(permite instalar SFP Ports)

Tabla. 3.3. Características del switch D-Link DES-1024R

Tipo	Switch no administrable de capa 2
Velocidad de conmutación de paquetes	148,810 pps por puerto Fast Ethernet
Velocidad de backplane	5.2 Gbps
RAM Buffer	256KB por 8 puertos
MAC soportadas	8K
Método de transmisión	Store-and-forward
Control de flujo	Protocolo 802.3X
Número de puertos:	24 puertos 10/100 Mbps 2 puertos 100BASE-FX de fibra óptica

Tabla. 3.4. Características del switch D-Link DES-1024D

Tipo	Switch no administrable de capa 2
Velocidad de conmutación de paquetes	148,809 pps por puerto Fast Ethernet
Velocidad de backplane	4.8 Gbps
RAM Buffer	160KB
MAC soportadas	8K
Método de transmisión	Store-and-forward
Control de flujo	802.3X
QoS	(802.1p), 2 colas
Número de puertos:	24 puertos 10/100 Mbps

Tabla. 3.5. Características del switch CISCO 2960

Tipo	Switch administrable de capa 2
Velocidad de conmutación de paquetes	148,810 pps por puerto Fast Ethernet 1,488,100 pps por puerto Gigabit
Velocidad de backplane	16 Gbps
RAM Buffer	64MB
MAC soportadas	8K
Método de transmisión	Store-and-forward
Soporte Multicast	255 IGMP groups
ACLs de nivel	2 y 3.
Maneja hasta 255 VLANs	(Protocolo 802.1q) (VLAN trunking protocol VTP)
Manejo de enlaces	Trunking

Monitoreable	SNMP v1/v2/v3, RMON (4 grupos Alarmas, Eventos, Estadísticas, e Historia), MIB II
Spanning Tree Protocol	(802.1D/802.1s/802.1w)
Control de flujo	802.1x
QoS	(802.1p/DSCP/IP precedence, dirección IP de fuente y destino, dirección MAC de fuente y destino, o puerto TCP o UDP de capa 4) 4 colas
Número de puertos:	24 puertos 10/100 Mbps 2 Combo Gigabit de cobre/(permite instalar SFP Ports)

3.2.2. RED DE DATOS DE LA BODEGA MUNICIPAL

La bodega municipal, posee una pequeña red de datos debido a la naturaleza de sus operaciones, no posee muchas oficinas y por tanto estaciones de trabajo, en la figura que se muestra a continuación se observa el área de oficinas de la bodega, que está ubicada en una sola planta.

Figura. 3.17. Área de oficinas de la bodega municipal

La red de datos está conformada por un *switch* marca: D-Link modelo: DES-1008D de ocho puertos 10/100 BASE-TX el cual se conecta a la antena que enlaza la bodega a la red WAN municipal, y a su vez se conecta en cascada con un *hub* marca: 3COM modelo: Office Connect Dual Speed Hub 8, con 8 puertos 10/100 BASE-TX, de los cuales se utilizan 3 para ofrecer conectividad a los equipos de trabajo distribuidos, utilizando un cableado UTP CAT 5e.

Figura. 3.18. Equipos de red de las bodegas

3.2.3. RED DE DATOS DEL MERCADO MAYORISTA

El mercado mayorista, posee una pequeña red de datos pues el área de oficinas no es muy extensa y está ubicada en una edificación de una sola planta como se muestra en las siguientes figuras.

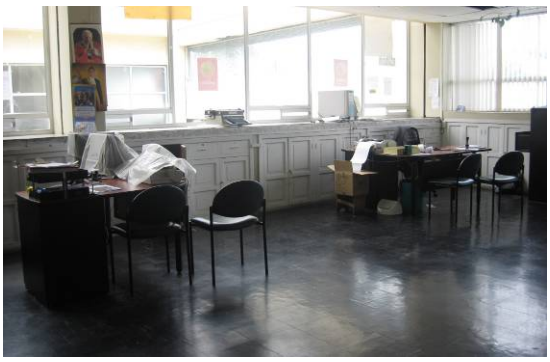


Figura. 3.19. Oficinas del mercado mayorista I

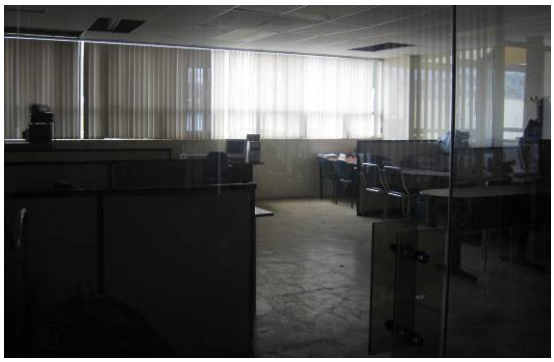


Figura. 3.20. Oficinas del mercado mayorista II

La red de datos está conformada por un *hub* marca 3COM *Office Connect Dual Speed Hub* 8, con 8 puertos, el cual se conecta a la antena que enlaza al mercado mayorista a la red WAN municipal, y a su vez brinda acceso a 7 equipos distribuidos en los puestos de trabajo conectados a través de cableado UTP CAT 5e.

Figura. 3.21. Equipo de red en el mercado mayorista

3.2.4. RED DE DATOS EN EL DEPARTAMENTO DE CULTURA

El departamento de cultura, posee una pequeña red de datos para brindar conectividad al área de oficinas ubicada en la primera planta alta de una edificación ubicada en un conocido monumento e ícono de la ciudad, como se muestra a continuación en las siguientes figuras.

Figura. 3.22. Oficinas del departamento de cultura I

Figura. 3.23. Oficinas del departamento de cultura II

La red de datos está conformada por un switch marca 3COM baseline switch 2024 (3C16471), al cual se conecta la antena que enlaza este departamento a la red WAN municipal, y a su vez brinda acceso a 14 puntos de red cableados con UTP CAT 5e que se encuentran distribuidos entre las oficinas que brindan conectividad a 8 equipos y una impresora de red, en la siguiente figura observamos el pequeño rack de datos.

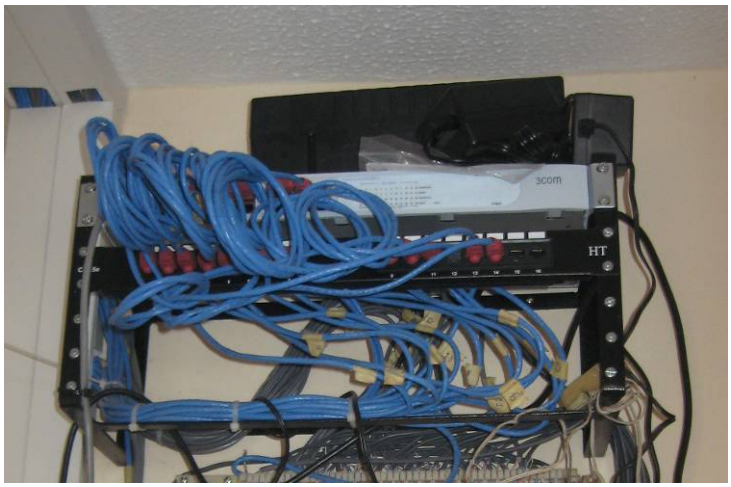


Figura. 3.24. Equipo de datos del departamento de cultura

3.2.5. RED DE DATOS EN LA UNIDAD MUNICIPAL DE TRANSITO

La unidad municipal de tránsito está ubicada en una edificación de dos plantas, de áreas poco extensas, como se muestra a continuación en las siguientes figuras.

Figura. 3.25. Oficinas de la unidad de tránsito planta baja

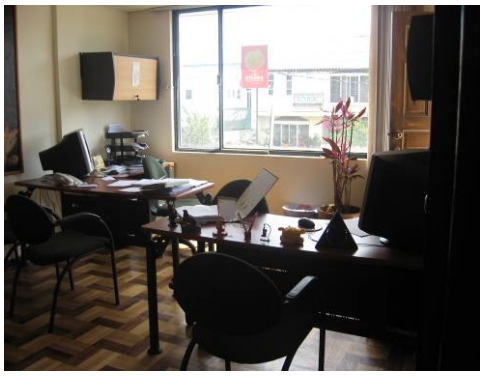


Figura. 3.26. Oficinas de la unidad de tránsito planta alta

La red de datos está conformada por un switch marca D-Link DES-1008D en la primera planta baja que brinda acceso en esta planta a 7 puntos de red a través de cable UTP CAT 5e, uno de los puertos de este equipo se conecta con otro *switch* de las mismas características ubicado en la planta alta que brinda acceso a seis puntos de red en esta planta a través de cable UTP CAT 5e, el puerto restante de este equipo se conecta a la antena de la WAN municipal. Además en esta dependencia existe un servidor con la aplicación del sistema de la unidad de tránsito y transporte. En las siguientes figuras se observan los equipos de red.

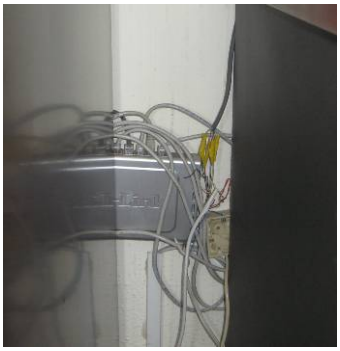


Figura. 3.27. Equipo de datos de la unidad de tránsito planta baja

Figura. 3.28. Equipo de datos de la unidad de tránsito planta alta

3.2.6. RED DE DATOS DE LAS COMISARIAS

Las comisarias están ubicadas en un edificio con una planta baja y dos altas en la planta baja existen ventanillas de cobro, y en las dos plantas altas se desenvuelven las actividades propias de esta dependencia municipal, estas áreas no son muy extensas como se observa en las figuras.

Figura. 3.29. Comisarias en la planta baja

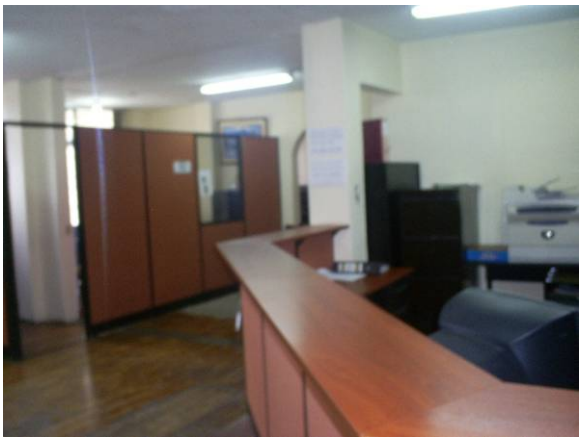


Figura. 3.30. Comisarias primera planta alta

Figura. 3.31. Oficinas Comisarias segunda planta

La red de datos está centralizada en un pequeño rack ubicado en la primera planta alta conformada por un *switch* marca 3COM baseline 2024, de 24 puertos los cuales están completamente utilizados y sirven para conectarse a la antena de la WAN municipal, brindar acceso a los puntos de red y conectar en cascada a dos switches marca CNet CNSH-1600 de 16 puertos cada uno, de los cuales se utilizan 15 y 7 puertos en cada uno de ellos. De modo que existen 40 puntos de red distribuidos entre las áreas de trabajo de esta dependencia.

Figura. 3.32. Equipos de datos en las comisarias

3.2.7. RED DE DATOS DEL HOSPITAL MUNICIPAL

El hospital municipal está ubicado en una edificación diseñada para brindar los servicios de salud para lo cual fue creado es por ello que las áreas más extensas son utilizadas para habitaciones, quirófanos, consultorios médicos, etc por lo tanto la red de

datos no es muy grande, la misma está conformada por dos switch D-Link DES-1008D de 8 puertos, uno de los cuales se conecta a la antena que enlaza esta dependencia a la red WAN Municpal y se conecta en cascada al otro switch de similares características y a un *switch* marca 3COM baseline 2026 de 24 puertos, el mismo que brinda acceso a 21 puntos de red distribuidos en toda la edificación. A continuación podemos observar el rack de comunicaciones de esta dependencia municipal.

Figura. 3.33. Equipos de datos en el hospital

3.2.8. RED DE DATOS DEL CAMAL MUNICIPAL

El camal municipal está ubicado en una edificación diseñada para desarrollar las operaciones propias del faenamiento de ganado para el consumo humano es por ello que las áreas más extensas son para dicho fin, mientras que las oficinas ocupan una pequeña planta, por lo tanto la red de datos no es muy grande, la misma está conformada por un *hub* 3COM *Office Connect Dual Speed* 16, de 16 puertos, el cual se conecta a la antena de la WAN municipal y brinda acceso a los 8 puntos de datos de esta dependencia que posee 6 equipos de trabajo. No se observan imágenes de esta dependencia pues no se permitió tomar fotografías de las instalaciones.

CARACTERÍSTICAS DE LOS SWITCHES DE OTRAS DEPENDENCIAS

Tabla. 3.6. Características del switch 3COM 2024

Tipo	Switch no administrable de capa 2
Velocidad de conmutación de paquetes	148,809 pps por puerto Fast Ethernet
Velocidad de backplane	4.8 Gbps

RAM Buffer	160KB
MAC soportadas	4K
Método de transmisión	Store-and-forward
Control de flujo	802.3X
Spanning tree protocol	802.1D
Número de puertos:	24 puertos 10/100 Mbps

Tabla. 3.7. Características del switch D-Link DES-1008D

Tipo	Switch no administrable de capa 2
Velocidad de conmutación de paquetes	148,800 pps por puerto Fast Ethernet
Velocidad de backplane	1.6 Gbps
RAM Buffer	64KB
MAC soportadas	1K
Método de transmisión	Store-and-forward
Número de puertos:	8 puertos 10/100 Mbps

Tabla. 3.8. Características del switch CNet 1600

Tipo	Switch no administrable de capa 2
Velocidad de conmutación de paquetes	148,810 pps por puerto Fast Ethernet
Velocidad de backplane	3.2 Gbps
RAM Buffer	160KB
MAC soportadas	4K
Método de transmisión	Store-and-forward
ManejaVLANs	(Protocolo 802.1Q) dos para configuración de "Home VLAN"
Manejo de enlaces	cuatro para configuración de Troncales
QoS	802.1p
Número de puertos:	16 puertos 10/100 Mbps

3.2.9. RED DE DATOS WAN MUNICIPAL

La red WAN municipal, utiliza tecnología inalámbrica para enlazar las 7 dependencias municipales que actualmente están conectadas a través de este medio, la solución implementada para este fin, utiliza equipos de la marca Trango Broadband, como se muestra en la siguiente figura.

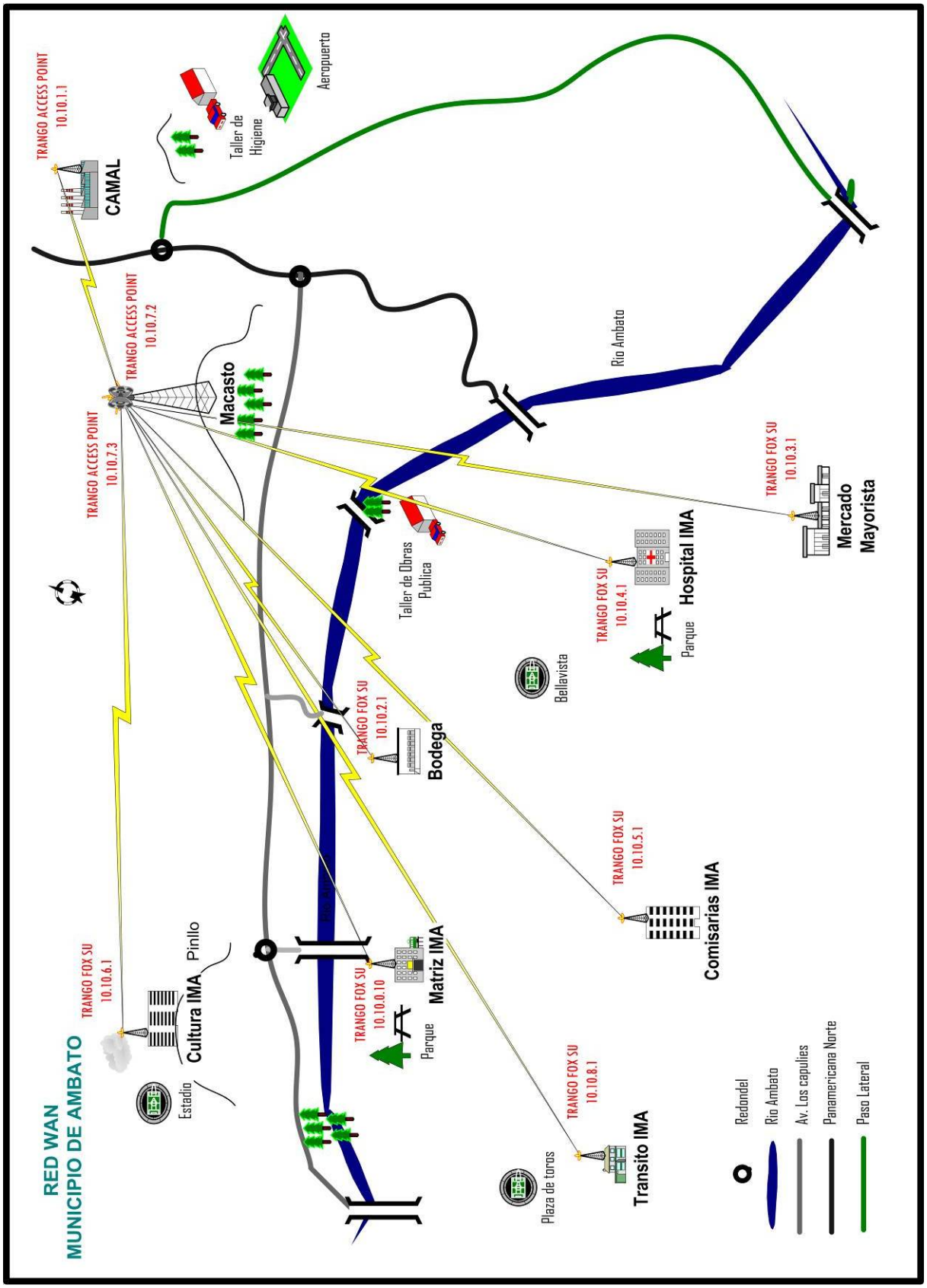


Figura. 3.34. Esquema de la red WAN

La arquitectura de esta solución es de tipo punto a multipunto, y consiste en dos tipos de equipos: Puntos de acceso (AP) y Unidades de suscriptor (SU). El AP está clasificado como un puente multipunto de capa 2 en una configuración tipo estrella inalámbrica, provee servicio inalámbrico de banda ancha en formato Ethernet a un máximo de 512 SU de acuerdo a un algoritmo adaptativo de interrogación dinámica denominado "*SMARTPolling*" que es propietario de esta marca de equipos, que son autenticadas usando un método de seguridad a nivel MAC, además no existe limitación en el número de direcciones IP o equipos que físicamente un SU individual puede tener conectado a él.

Se pueden colocar múltiples AP´s con un máximo de 22, en la misma celda, con el fin de incrementar la velocidad de datos disponible a cada SU.

Tanto AP´s como SU´s pueden ser fácilmente configuradas y administradas a través de interfaces seriales o Ethernet mediante un navegador web, se alimentan a través de PoE para facilitar su instalación.

Figura. 3.35. Antena de unidad de suscriptor

Algoritmo *SmartPolling*

Gracias a este algoritmo el AP maneja múltiples conexiones con SU´s compartiendo eficientemente su velocidad de datos disponible de 10Mbps, para administrar el ancho de banda el algoritmo, se sirve de ciertos parámetros provistos por el administrador del sistema. El AP interroga a cada SU en forma circular *"round robin format"* para determinar si él SU tiene datos para transferir. El SU solo transmite el flujo de datos de subida, hacia el AP cuando este lo autoriza a través de una "concesión de transmisión". El SU escucha y analiza cada paquete del flujo de datos de bajada desde el AP, e identifica los paquetes que son dirigidos a él.

Para que un SU se comunique con un AP, el administrador del sistema debe primero añadir la dirección MAC y el ID de este SU a la base de datos en el AP. Otros parámetros considerados por el algoritmo son *Committed Information Rate* (CIR), *Maximum Information Rate* (MIR), y la configuración de prioridad.

Cuando un SU se inicializa, este escanea todos los canales que constan en su tabla de escaneo en búsqueda de un AP con la misma ID que este enviando "concesiones de transmisión". Entonces el SU detiene el escaneo, se bloquea en este canal y transmite al AP usando la máxima potencia RF. Antes de que el AP pueda añadir este SU a la lista de interrogación, este debe autenticar al SU verificando la dirección MAC y corriendo ciertas operaciones con el SU.

3.2.10. FUNCIONAMIENTO OPERACIONAL DE LA RED ACTUAL

DESCRIPCIÓN DE LOS SERVIDORES DE LA RED

En la Ilustre Municipalidad de Ambato existen 8 servidores, de los cuales 7 se encuentran en la matriz en el departamento de sistemas y uno de ellos se encuentra en la unidad de tránsito, y proveen servicio a las distintas aplicaciones de red. Estos servidores tienen Sistemas Operativos que soportan una gran cantidad de operaciones, sus características son:

Tabla. 3.9. Características del servidor de base de datos

CARACTERÍSTICAS	DESCRIPCIÓN
Marca	HP
Modelo	DL380G5 Quad-Core
Memoria	
RAM	4 Gigabytes
Disco Duro	144 GB en array
Sistema Operativo	Linux Red Hat 4
Servicios	Base de Datos
Aplicaciones	Oracle 10g
Dirección IP	10.10.0.3

Tabla. 3.10. Características del servidor de correo electrónico

CARACTERÍSTICAS	DESCRIPCIÓN
Marca	Intel
Modelo	Hudson
Memoria	
RAM	1 Gigabyte
Disco Duro	20 GB 20 GB
Sistema Operativo	Linux Red Hat 2.4
Servicios	Correo Electrónico
Aplicaciones	Lotus Notes 6.5
Dirección IP	10.10.0.1

Tabla. 3.11. Características del servidor de antivirus

CARACTERÍSTICAS	DESCRIPCIÓN
Marca	Intel
Modelo	Hudson
Memoria	
RAM	1 Gigabyte
Disco Duro	20 GB
Sistema Operativo	Windows 2000
Servicios	Antivirus
Aplicaciones	Mcafee Antivirus versión 8.5 Mcafee Malware 2.0
Dirección IP	10.10.0.8

Tabla. 3.12. Características del servidor de mapas

CARACTERÍSTICAS	DESCRIPCIÓN
Marca	HP
Modelo	ML530
Memoria	
RAM	2 Gigabytes
Disco Duro	72 GB 72 GB 72 GB
Sistema Operativo	Linux Red Hat 2.4
Servicios	Mapas
Aplicaciones	ARC GIS 8.3
Dirección IP	10.10.0.7

Tabla. 3.13. Características del servidor de dominio principal

CARACTERÍSTICAS	DESCRIPCIÓN
Marca	HP
Modelo	ML570
Memoria	
RAM	2 Gigabytes
Disco Duro	72 GB 72 GB 72 GB
Sistema Operativo	Windows 2003
Servicios	Controlador de Dominio Principal
Aplicaciones	Cabildo (Manejo de predios y tesorería) DocFlow (Seguimiento de Trámites) VIF (Compras e Inventarios de Bodega)
Dirección IP	10.10.0.6

Tabla. 3.14. Características del servidor de servicios financieros

CARACTERÍSTICAS	DESCRIPCIÓN
Marca	HP
Modelo	ML350
Memoria	
RAM	2 Gigabytes
Disco Duro	72 GB 144 GB
Sistema Operativo	Windows 2003
Servicios	Financieros Controlador de Dominio
Aplicaciones	SIGEF (Sistema de Información Financiera del Estado) Oracle 9.0
Dirección IP	10.10.0.5

Tabla. 3.15. Características del servidor de la unidad de tránsito

CARACTERÍSTICAS	DESCRIPCIÓN
Marca	HP
Modelo	ML350
Memoria	
RAM	2 Gigabytes
Disco Duro	72 GB 144 GB
Sistema Operativo	Windows 2003
Servicios	Transporte Respaldo Remoto

	Controlador de Dominio
Aplicaciones	Oracle 9.0 Sistema de la Unidad de Tránsito y Transporte
Dirección IP	10.10.8.5

Tabla. 3.16. Características del servidor Proxy

CARACTERÍSTICAS	DESCRIPCIÓN
Marca	HighTelecomm
Memoria	
RAM	2 Gigabytes
Disco Duro	160 Gigabytes
Sistema Operativo	Linux
Servicios	Firewall Spam Web Server
Aplicaciones	HT Firewall HT Spam HT Web Server
Dirección IP	10.10.0.2

DIRECCIONAMIENTO

La asignación de direcciones IP a las redes locales de cada una de las dependencias de la red municipal, se basan en una máscara de subred de longitud fija, de modo que todos los equipos sin importar si estos están geográficamente distribuidos se ven entre sí como una sola red de área local, en la cual no se encuentran implementadas VLAN´s principalmente por la ausencia de *switches* administrables.

Al utilizar en el software, Colasosft Capsa la herramienta MAC scanner se obtiene un listado de las direcciones IP, con sus correspondientes MAC, nombre de equipo y fabricante de la tarjeta de red, como se puede observar en el anexo F, de allí podemos resumir.

Tabla. 3.17. Número y direccionamiento de equipo conectados a la red

Direcciones IP escaneadas en la red municipal		
RED	**SUBRED**	**NÚMERO DE HOSTS**
10.10.0.0/16	10.10.0.0/16	123
10.10.0.0/16	10.10.1.0/16	72
10.10.0.0/16	10.10.3.0/16	7

10.10.0.0/16	10.10.4.0/16	10
10.10.0.0/16	10.10.5.0/16	31
10.10.0.0/16	10.10.6.0/16	15
10.10.0.0/16	10.10.7.0/16	2
10.10.0.0/16	10.10.8.0/16	15
10.10.0.0/16	10.10.9.0/16	3
10.10.0.0/16	10.10.10.0/16	2
10.10.0.0/16	10.10.11.0/16	1
10.10.0.0/16	10.10.12.0/16	1
10.10.0.0/16	10.10.44.0/16	1
10.10.0.0/16	10.10.199.0/16	3
	TOTAL	**286**

En la siguiente tabla se muestran las direcciones reservadas para las unidades de suscriptores ubicadas en cada dependencia así como para los Access point ubicados en Macasto y en el camal, que en su conjunto forman la red WAN Municipal, como se observó en la Fig 3.35.

Tabla. 3.18. Direcciones IP de la red WAN

Direcciones IP de la red WAN			
DEPENDENCIA	**EQUIPO**	**DIRECCIÓN**	**MÁSCARA**
MATRIZ	M5800S-FSU-D	10.10.0.10	255.255.0.0
CAMAL	Access5800 AP	10.10.1.1	255.255.0.0
BODEGAS	M5800S-FSU-D	10.10.2.1	255.255.0.0
MERCADO MAYORISTA	M5800S-FSU-D	10.10.3.1	255.255.0.0
HOSPITAL	M5800S-FSU-D	10.10.4.1	255.255.0.0
COMISARIAS	M5800S-FSU-D	10.10.5.1	255.255.0.0
CULTURA	M5800S-FSU-D	10.10.6.1	255.255.0.0
MACASTO-CAMAL	Access5800 AP	10.10.7.2	255.255.0.0
MACASTO-PRINCIPAL	Access5800 AP	10.10.7.3	255.255.0.0
TRÁNSITO	M5800S-FSU-D	10.10.8.1	255.255.0.0

Observando los nombres de los equipos del anexo F del MAC scanner, determinamos a que dependencia corresponde cada equipo, notándose que no existe la correspondencia total entre el direccionamiento lógico y la ubicación física que los equipos deberían tener, siendo así que por ejemplo a la subred 10.10.1.0/24 deberían estar asociados los equipos del camal de acuerdo a la tabla 3.18, sin embargo en esta subred encontramos también equipos de la matriz, existen también pocos equipos en las subredes 10.10.9.0/24, 10.10.10.0/24, 10.10.11.0/24, 10.10.12.0/24, 10.10.44.0/24, que están fuera

del esquema de direccionamiento, y los equipos de la subred 10.10.199.0/24, que es la que se seleccionó para los equipos encargados de hacer el monitoreo de la red.

A continuación se muestra un resumen del número de equipos que posee cada dependencia, sin considerar los equipos usados temporalmente para el monitoreo de la red y los *Access Point* en Macasto.

Tabla. 3.19. Número de Hosts por dependencia

Número de hosts en cada dependencia	
DEPENDENCIA	**# HOSTS**
MATRIZ	194
CAMAL	6
BODEGAS	3
MERCADO MAYORISTA	7
HOSPITAL	10
COMISARIAS	31
CULTURA	15
TRÁNSITO	15
TOTAL	**281**

3.3. LEVANTAMIENTO DE LA RED TELEFÓNICA IMA

La red telefónica de la Ilustre Municipalidad de Ambato utiliza tecnología analógica y como lo veremos a continuación no todas las dependencias cuentan con una central telefónica, algunas de ellas solamente poseen líneas análogas que se conectan directamente a la red de Andinatel.

3.3.1. RED TELEFÓNICA DEL EDIFICIO MATRIZ

El edificio matriz cuenta con una central telefónica analógica marca: PANASONIC modelo: KX-T96100, y conformada por las siguientes tarjetas:

- 3 PLC

- 1 HLC

- 4 SLC

- 2 LCOT

Figura. 3.36. Central telefónica Edificio Matriz

Debido a la expansión que ha tenido el Municipio en los últimos años ha existido un incremento en la demanda de servicios telefónicos con la finalidad de atender las necesidades que han ido surgiendo con el pasar del tiempo, dicho fenómeno ha desencadenado una saturación en la capacidad de la central telefónica, que no fue dimensionada para atender el crecimiento que actualmente existe, o esto se suma la escases de repuestos para este equipo pues al ser antiguo esta ya descontinuado, y ha provocado graves inconvenientes en circunstancias cuando se ha quemado alguna de las tarjetas, pues se debe buscar repuestos en equipos similares que han sido dados de baja, lo cual implica mucha pérdida de tiempo, y la consecuente pérdida de servicios de comunicación telefónica en el Municipio actualmente de las 64 extensiones que proporcionan las tarjetas destinadas a este fin 3 de estos puertos han dejado de funcionar, las 61 extensiones restantes están operativas y tienen asignados los números del 100 al 153, 160, 161, 163 al 167. Y brindan servicio a los departamentos que se muestran la siguiente tabla.

Tabla. 3.20. Tabla de distribución de la central telefónica de la matriz

DEPARTAMENTOS	UBICACION	NUMERO	EXT	ATRIBUTO
TRONCAL	INFORMACION	2820311	100	LIBRE
		2813051		
		2826315		
ALCALDIA	ALCALDE		105	LIBRE
	SECRETARIA		103 - 104	LIBRE
	COORD. ALCALDIA		122	LIBRE
	PLAN ESTRATEGICO		137 - 149	LOCAL - PROV
	VICEPRESIDENCIA DE CONCEJO		165	LOCAL
	SECRETARIA VICE		152	PROV

	ALCALDIA			
SECRE. GENERAL	DIRECCION	2820178	123	LIBRE
	FAX		148	PROV
	SECRETARIA		101	LIBRE
	PRO-SECRETARIA		102	LIBRE
	ARCHIVO		143	LOCAL
	SALA COMISIONES	2421953	151	LOCAL
	COMUNICACION INSTITUCIONAL		107	LIBRE
	SECRETARIA COMUNICACION		138	LIBRE
ADMINISTRATIVO	DIRECTOR	2829501	124	LIBRE
	SECRETARIA		144	PROV
	ORGANIZ METODOS		120	LIBRE
ASESORIA JURIDICA	DIRECCION	2421346	114	LIBRE
	SECRETARIA		113	LOCAL
	ABOGADO JEFE		106	LOCAL
AUDITORIA	SECRETARIA		145	PROV
AVALUOS	DIRECCION	2828683	140	PROV
	SECRETARIA		139	PROV
	CATASTRO ECONO.		141	PROV
	CARTOGRAFIA		142	PROV
BIBLIOTECA			153	LOCAL
FINANCIERO	DIRECTOR	2823058	115	PROV
	SECRETARIA		116	PROV
	PRESUPUESTO		150	PROV
	RENTAS		117	LOCAL
	CONTABILIDAD		133 - 134	LOCAL
	PROVEEDURIA		135	PROV
	TESORERIA		126 - 125	LIBRE
OBRAS PUBLICAS	DIRECTOR	2826296	110	PROV
	SECRETARIA		160 -161- 127	LOCAL-PROV-LOCAL
	ARCHIVO		146	LOCAL
	FISCAL. CONSTRUC		128	LOCAL
	FISCAL.VIAS		129	LOCAL
	PARROQUIAS Y CONSTRUCCIONES		163	LOCAL
	LABORATORIO		136	LOCAL
	OBRAS CIVILES		164	LOCAL
PATRONATO	PRESIDENTA		166	LOCAL
PLANIFICACION	DIRECTOR	2822949	112	PROV
	SECRETARIA		111	PROV
	PLAN DESARROLLO		130	LOCAL
	PROG. Y PROYECTOS		131	LOCAL
	CONTROL URBANO		132	LOCAL
RECURSOS HUMANOS	DIRECTOR	2822785	119	PROV
	SECRETARIA		118 - 147	PROV-LOCAL
INFORMATICA	DIRECTOR		109	PROV
	SECRETARIA	2821024	108	PROV
	DESARROLLO		167	PROV
SERVICIOS PÚBLICOS	SECRETARIA		109	PROV

En la tabla se pueden observar los números asignados por Andinatel a las 13 troncales analógicas que ingresan por la PBX y están asociadas a los departamentos que se muestran en la tabla, además por la creciente necesidad de comunicaciones anteriormente mencionada ha sido necesario instalar extensiones que no pasan por la central telefónica y se conectan directamente desde la acometida entregada por Andinatel hasta los puestos de trabajo, estas líneas analógicas suman 10 y se reflejan en la siguiente tabla.

Tabla. 3.21. Líneas conectadas directamente a la matriz

DEPARTAMENTOS	UBICACION	NUMERO
ALCALDIA	SECRETARIA	2421951
	FAX	2829977
	VICEPRESIDENCIA DE CONCEJO	2820380
SECRE. GENERAL	COMUNICACION INSTITUCIONAL	2820056
FINANCIERO	PROVEEDURIA	2822491
		2424310
	TESORERIA	2822819
		2425513
PATRONATO	PRESIDENTA	2820094
INFORMATICA	DIRECTOR	2422302

3.3.2. RED TELEFÓNICA DE LA BODEGA MUNICIPAL

La bodega municipal no con cuenta con una infraestructura telefónica solamente posee una línea analógica que la provee Andinatel, y del cual se conectan en paralelo dos teléfonos que se encuentran en el área de oficinas.

Tabla. 3.22. Línea conectada directamente a la Bodega Municipal

DEPARTAMENTO	NÚMERO
BODEGA MUNICIPAL	2424196

3.3.3. RED TELEFÓNICA DEL MERCADO MAYORISTA

El mercado mayorista no con cuenta con una infraestructura telefónica solamente posee una línea analógica que la provee Andinatel, y del cual se conectan en paralelo varios teléfonos que se encuentran en el área de oficinas.

Tabla. 3.23. Línea conectada directamente al Mercado Mayorista

DEPARTAMENTO	NÚMERO
MERCADO MAYORISTA	2853930

3.3.4. RED TELEFÓNICA EN EL DEPARTAMENTO DE CULTURA

El departamento de cultura posee una central telefónica marca: SIEMENS modelo: HiPath 1120, que tiene capacidad de manejar 6 líneas análogas y 16 extensiones, a continuación se observa este equipo.

Figura. 3.37. Central telefónica Departamento de Cultura

En la siguiente tabla se muestra la distribución de extensiones y troncales que maneja esta central.

Tabla. 3.24. Tabla de distribución de la central telefónica de cultura

DEPARTAMENTOS	UBICACION	NUMERO	EXT	
CULTURA	SECRETARIA	2426652		8 Extensiones en total
	DIRECCION			
	PROMOCION CULTURAL			
DESARROLLO SOCIAL	TURISMO		21	
	DIRECCION	2425922	25	
	DESARROLLO INDIGENA		24	

3.3.5. RED TELEFÓNICA EN LA UNIDAD MUNICIPAL DE TRANSITO

La unidad de transito municipal tiene una central telefónica marca: PANASONIC modelo: TES824, con una capacidad de 3 a 8 (con tarjetas de expansión) líneas externas y de 8 a 24 (con tarjetas de expansión) extensiones a continuación podemos observar este equipo.

Figura. 3.38. Central telefónica Unidad de Tránsito

En la siguiente tabla se muestran las 2 troncales que maneja esta central, que dan servicio a 6 extensiones.

Tabla. 3.25. Tabla de distribución de la central telefónica de tránsito

DEPARTAMENTOS	UBICACION	NUMERO	EXT
UNIDAD DE TRANSITO	SECRETARIA	2843154	6 extensiones
	FAX	2843464	

3.3.6. RED TELEFÓNICA DE LAS COMISARIAS

El edificio de las comisarías no posee una estructura telefónica solamente líneas análogas directamente conectadas desde la acometida entregada por Andinatel hasta los puestos de trabajo, de modo que cada planta cuenta con una línea a excepción de la planta donde se encuentran servicios públicos que cuenta con dos líneas, a las mismas que a su vez se conectan extensiones en paralelo, distribuidas en cada una de las plantas.

Tabla. 3.26. Líneas conectadas directamente a las comisarías

DEPARTAMENTOS	UBICACION	NUMERO
COMISARIAS	TESORERIA	2841248
HIGIENE	SECRETARÍA	2844825
AVALUOS	CATASTRO FISICO	2840533
	INQUILINATO	2846391
SERVICIOS PÚBLICOS	SECRETARIA	2841384

3.3.7. RED TELEFÓNICA DEL HOSPITAL MUNICIPAL

El hospital municipal cuenta con una central telefónica analógica marca: PANASONIC modelo: KX-TDA100, y conformada por las siguientes tarjetas, que como se puede observar en la figura ocupan todos los slots disponibles:

- 3 Tarjetas de extensiones de teléfono regular de 16 puertos

- 1 Tarjeta de extensiones digitales de 16 puertos

- 1 Tarjeta de líneas analógicas de 4 puertos (LCOT 4)

Figura. 3.39. Central telefónica Hospital Municipal

En la siguiente tabla se muestra la distribución de extensiones y troncales que maneja esta central.

Tabla. 3.27. Tabla de distribución de la central telefónica del Hospital Municipal

DEPARTAMENTOS	UBICACION	NUMERO	EXT	
HOSPITAL MUNICIPAL	TRONCALES	2415637		41 Extensiones en total
		2849047		
		2416840		
	GERENCIA		101	
	SECRETARIA		100	
	EMERGENCIA		128	
	ENFERMERIA		129	
	FARMACIA		136	
	LABORATORIO		138	
	PEDIATRIA		133	
	TRABAJADOR SOCIAL		110	

3.3.8. RED TELEFÓNICA DEL CAMAL MUNICIPAL

El camal municipal cuenta con una central telefónica analógica marca: PANASONIC modelo: KX-TEM824 con una capacidad de 6 a 8 (con tarjetas de expansión) líneas externas y de 16 a 24 (con tarjetas de expansión) extensiones, a continuación podemos observar este equipo.

Figura. 3.40. Central telefónica Camal Municipal

En la siguiente tabla se muestra la distribución de extensiones y troncales que maneja esta central.

Tabla. 3.28. Tabla de distribución de la central telefónica del Camal Municipal

DEPARTAMENTOS	UBICACION	NUMERO	EXT
CAMAL	INFORMACION	2855857	
		2855859	
	SECRETARIA		11
	ADMINISTRACION		12
	MANTENIMIENTO		13
	CONTABILIDAD		14
	FAX		21

3.4. ANÁLISIS DE TRÁFICO DE DATOS

Las tareas de monitoreo de tráfico se las realizó sobre los enlaces principales de la red, que son los que se muestran en la siguiente figura, donde encontramos un esquema de dicho monitoreo, para lo cual se integro a un nuevo PC a la red donde se instalaron las aplicaciones necesarias para dicho fin, este equipo cuenta con dos tarjetas de red conectadas a los puertos disponibles 22 y 23 del switch administrable D-Link 3226 con las direcciones 10.10.199.2 y 10.10.199.3, respectivamente, este switch que se encontraba con las configuraciones por defecto, se le direccionó con 10.10.199.1.

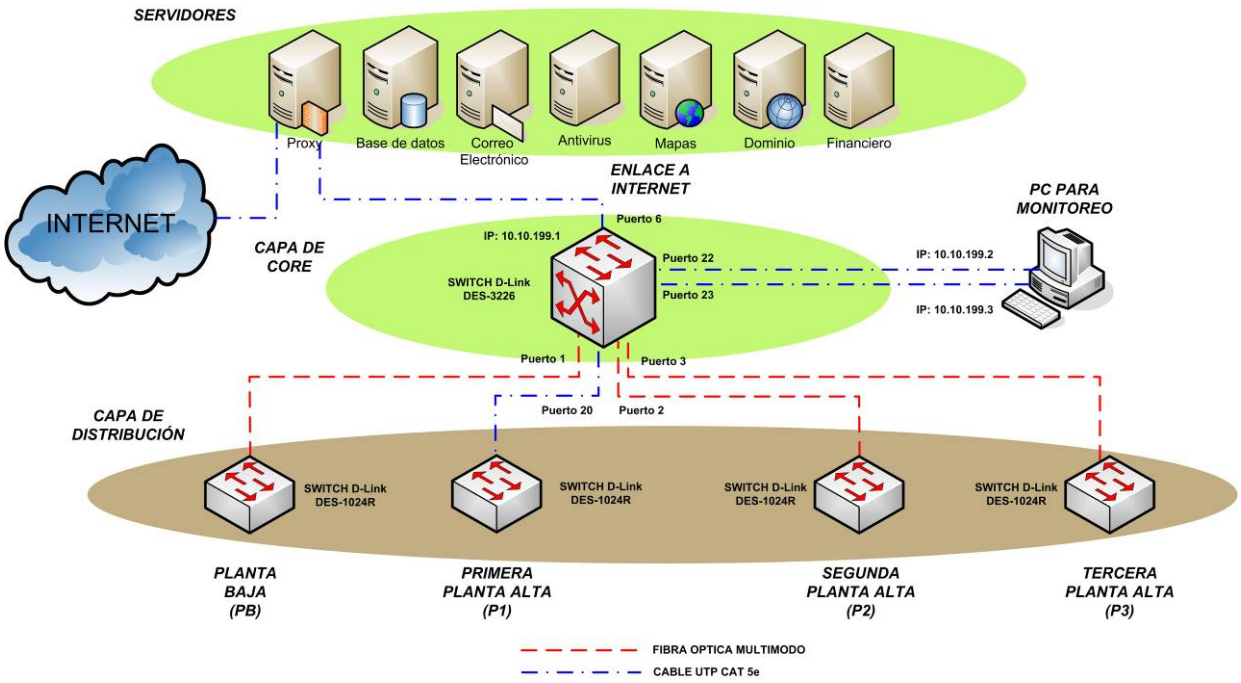


Figura. 3.41. Esquema de monitoreo

3.4.1. ANÁLISIS CUANTITATIVO DE TRÁFICO DE DATOS

El monitoreo de tráfico se realizó aprovechando el servicio de SNMP (*Simple Network Management Protocol*), el cual se levanto y configuró en el *switch* D-Link 3226 de la matriz que es el core de la red; para lo cual se utilizó el software PRTG V6.1.1.855 (*Paessler Router Traffic Grapher*) en el PC destinado al monitoreo con la tarjeta de red de dirección 10.10.199.2 conectada al puerto 22, y mediante la dirección de administración del dispositivo 10.10.199.1 y la comunidad SNMP configurada como "*prívate*" a la que pertenecen dichos elementos de red. Las mediciones de niveles de tráfico fueron tomadas la segunda semana de Julio del 2008 en los puertos que sirven como enlace hacia el backbone vertical para conectar los otros pisos y en la conexión hacia internet, a continuación se detallan los enlaces monitoreados:

- Tráfico de entrada y salida de la planta baja, (puerto 1).

- Tráfico de entrada y salida de la primera planta alta, (puerto 20).

- Tráfico de entrada y salida de la segunda planta alta, (puerto 2).

- Tráfico de entrada y salida de la tercera planta alta, (puerto 3).

- Tráfico de entrada y salida de la conexión a internet, (puerto 6).

A continuación se observan las gráficas de tráfico de cada uno de los enlaces mencionados, dichas gráficas corresponden el día 10 de Julio como se puede notar, y en correspondencia al horario de trabajo de jornada única que lleva a cabo el municipio se puede ver que la actividad comienza a las 8 am y decrece a las 4 pm.

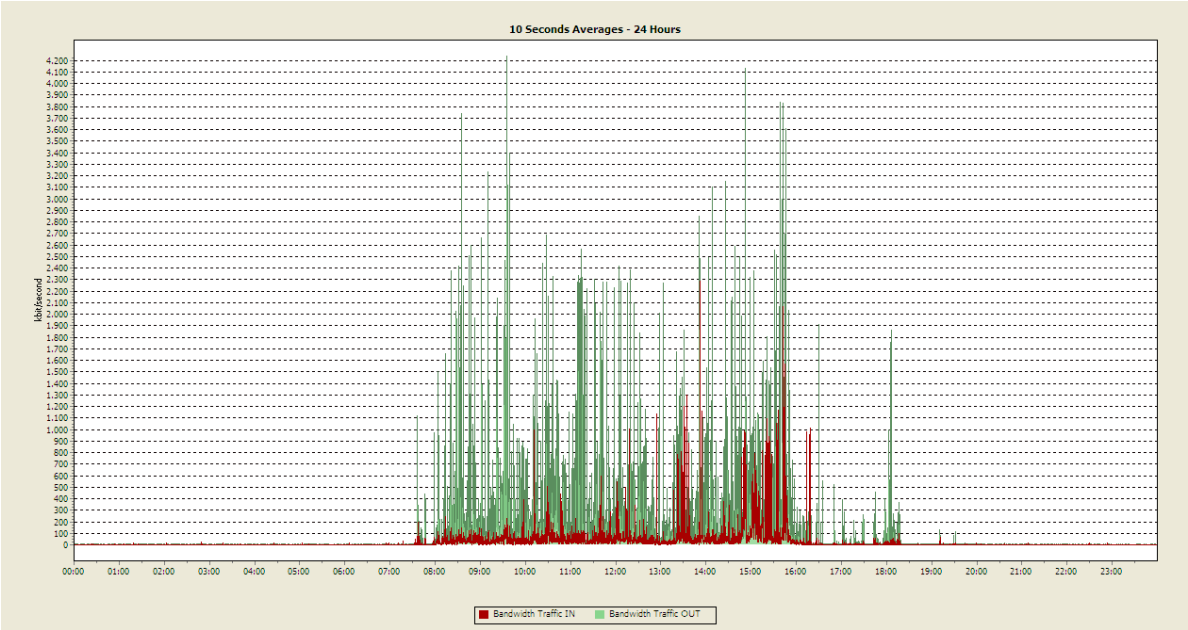


Figura. 3.42. Tráfico de la Planta Baja

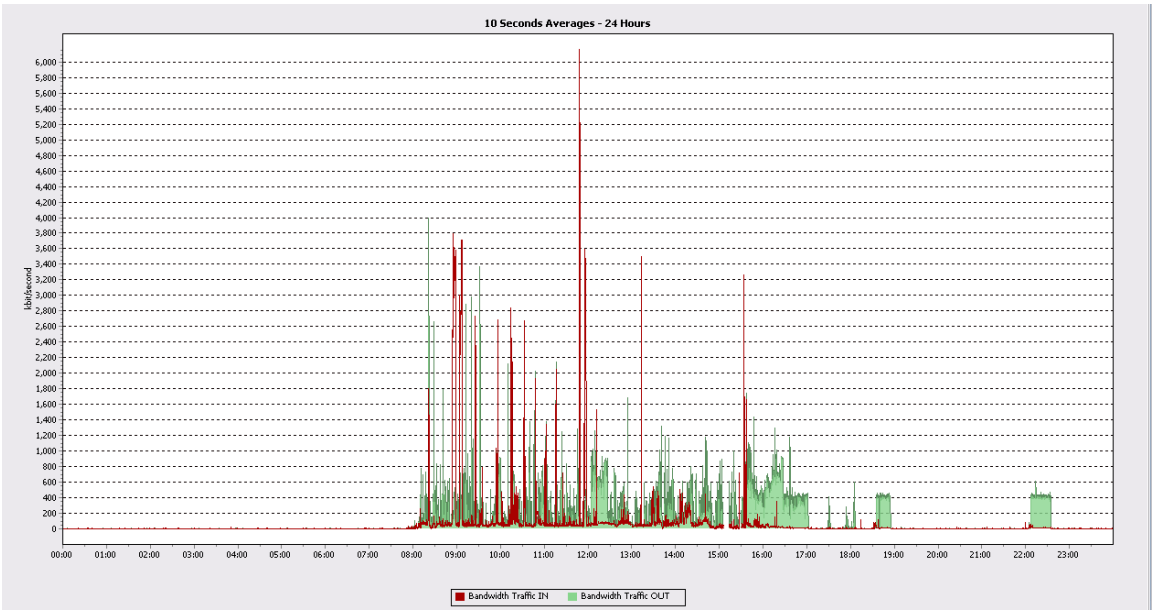


Figura. 3.43. Tráfico de la Primera Planta Alta

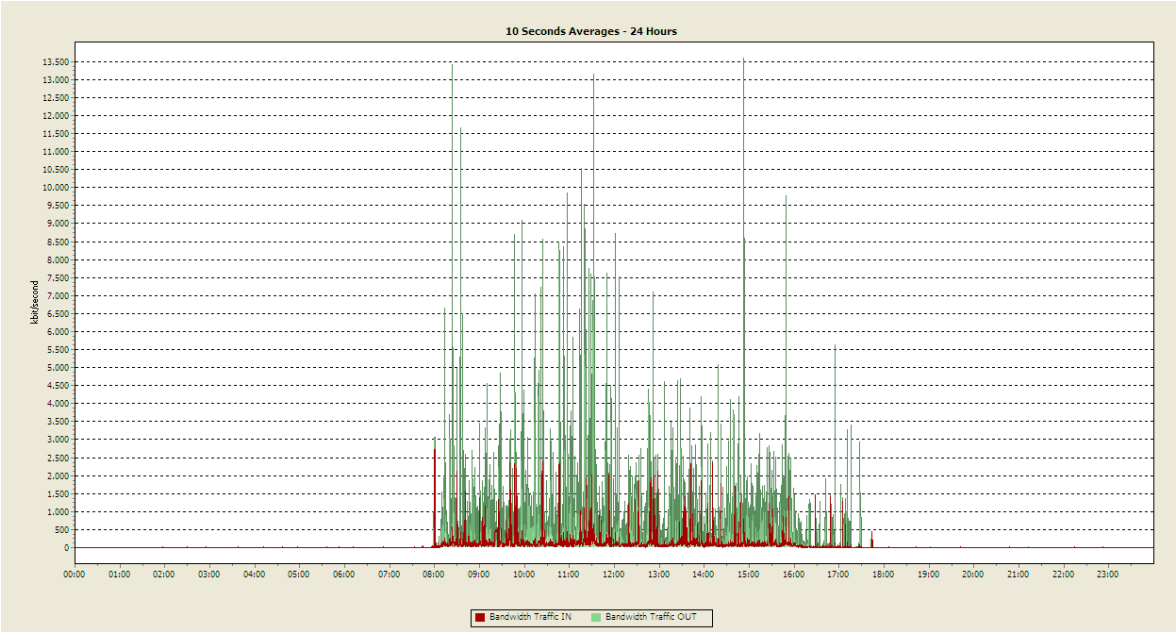


Figura. 3.44. Tráfico de la Segunda Planta Alta

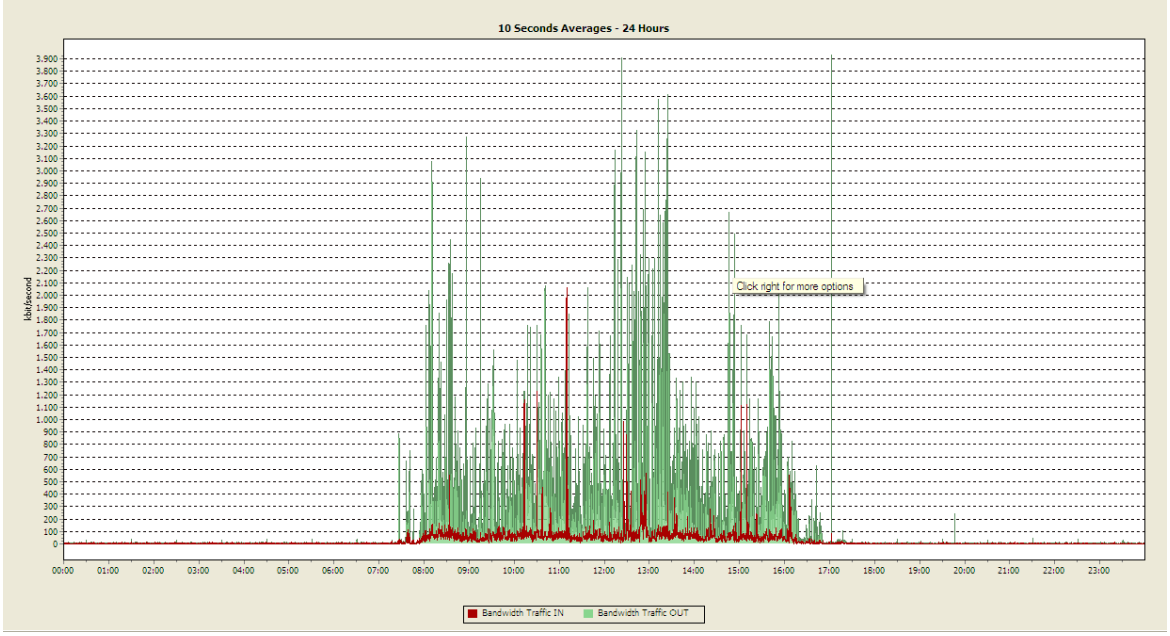


Figura. 3.45. Tráfico de la Tercera Planta Alta

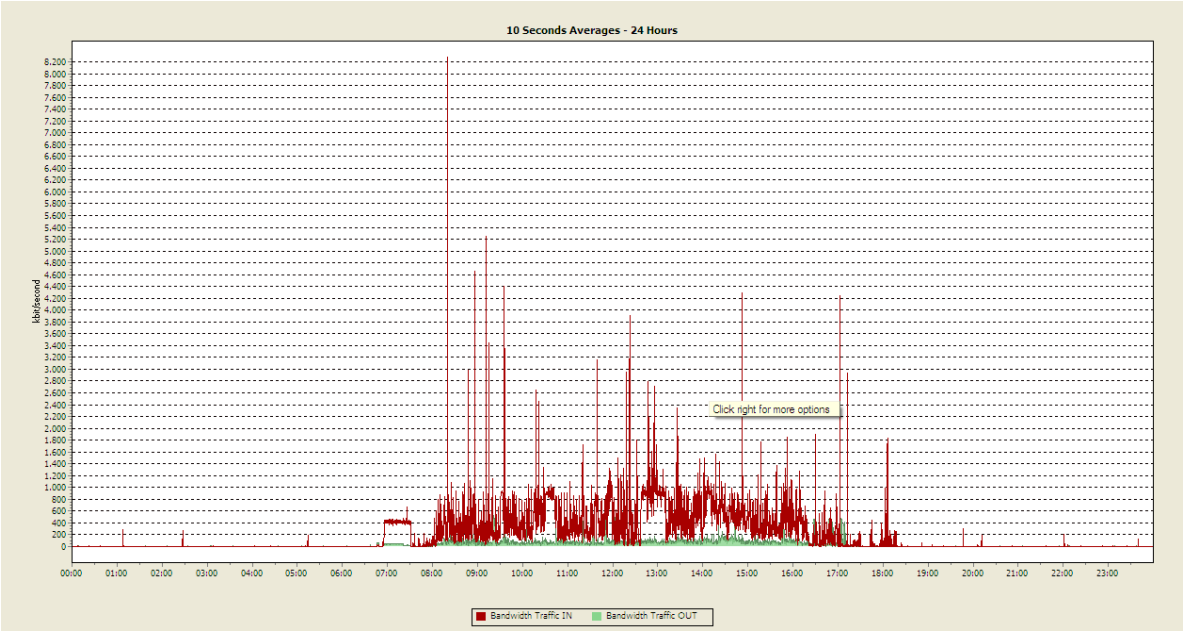


Figura. 3.46. Tráfico del enlace a Internet

En la tabla y gráfica que sigue a continuación se resume la sumatoria de kbytes que han pasado por cada enlace, así como la velocidad pico y promedio (calculada en el intervalo del horario de laborable) con la que dichos kbytes han circulado por la red.

Tabla. 3.29. Resumen de tráfico cuantitativo

PLANTA/ INTERNET	TRÁFICO ENTRANTE			TRÁFICO SALIENTE			SUMATORIA		
	kbyte (Sumatoria)	kbit/s (Max)	kbit/s (Promedio)	kbyte (Sumatoria)	kbit/s (Max)	kbit/s (Promedio)	kbyte (Sumatoria)	kbit/s (Max)	kbit/s (Promedio)
PB	269,184	2,285	77	1,090,167	4,238	310	1,359,351	6,523	387
P1	618,208	6,154	176	925,690	4,035	264	1,543,898	10,189	440
P2	584,142	2,725	166	3,311,452	13,597	943	3,895,594	16,322	1,109
P3	363,872	3,687	105	2,310,550	5,943	663	2,674,422	9,630	768
INTERNET	1,762,722	8,280	502	278,739	489	79	2,041,461	8,769	581

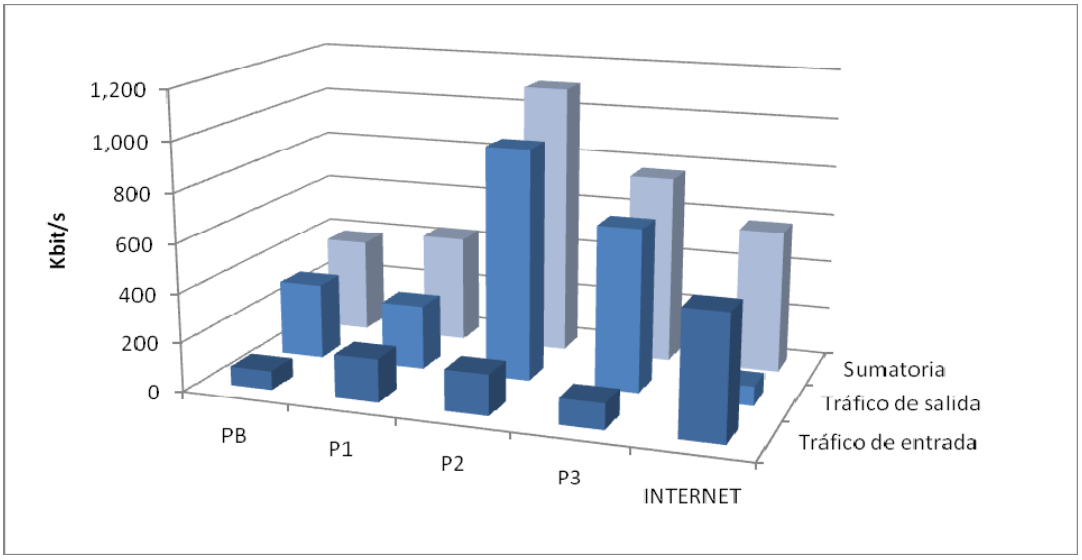


Figura. 3.47. Gráfica comparativa de tráfico promedio

3.4.2. ANÁLISIS CUALITATIVO DE TRÁFICO DE DATOS

A través del servicio SNMP se pudo conocer cuantitativamente el tráfico que se encontraba circulando por el switch en los enlaces de interés, sin embargo, adicionalmente a esta información es importante conocer cualitativamente el tipo de tráfico que atraviesa la red, para ello, se usó el sniffer TracePlus V2.07, para este fin se programó el switch de core habilitando un puerto SPAN (*Switched Port Analyzer*). El puerto SPAN refleja el tráfico de datos que circula por un puerto denominado fuente (puertos de los enlaces a monitorear), a otro denominado destino, que para nuestro caso fue el puerto 23, al cual se conectó el host destinado al monitoreo que se comunica con el puerto SPAN a través de la tarjeta de red que posee la dirección 10.10.199.3, en dicho host se instaló el sniffer. Con la ayuda de estas herramientas, se logro monitorear los 5 enlaces antes descritos, durante la tercera semana de Julio, cada enlace fue monitoreado durante un día, en el lapso del horario laborable, es decir de 8 am hasta las 4 pm.

A continuación se muestran los resultados para cada enlace:

PLANTA BAJA

Tabla. 3.30. Tipo de Tráfico de la PB

TAMAÑO	# PAQUETES
PACKETS	5,160,758
BYTES	1,468,762,141

UNICAST	4,809,955
BROADCAST	321,853
MULTICAST	28,951

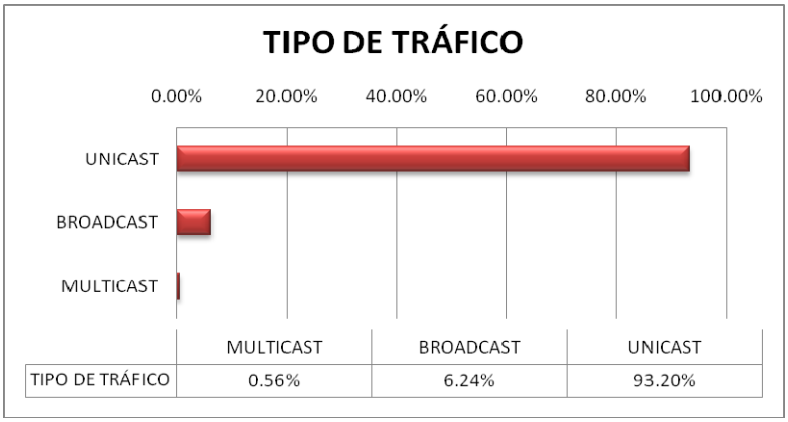


Figura. 3.48. Distribución del tipo de tráfico de la PB

Tabla. 3.31. Distribución de paquetes por tamaño de la PB

TAMAÑO	# PAQUETES
0-64 bytes	1,558,356
65-127 bytes	1,881,050
128-255 bytes	791,367
256-511 bytes	198,705
512-1023 bytes	94,707
> 1024 bytes	636,574
TOTAL	**5,160,759**

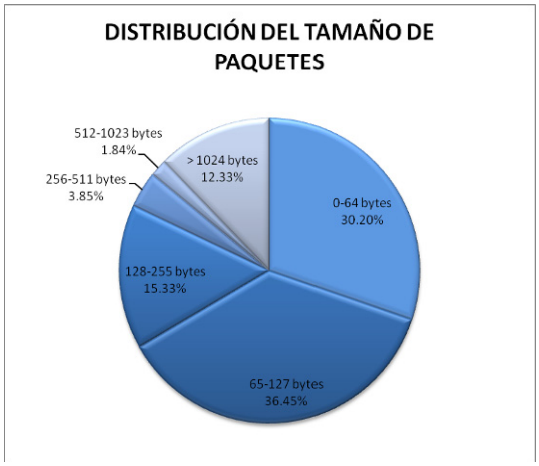


Figura. 3.49. Distribución de paquetes por tamaño de la PB

Tabla. 3.32. Distribución de protocolos de la PB

PROTOCOLO	# PAQUETES
IP	**4,875,184**
TCP	4,760,289
UDP	104,525
ICMP	7,676
IGMP	2,695
ARP	**241,392**
IPX	**21,633**
Apple Talk	**21,539**
NetBEUI	**612**
TOTAL	**285,176**

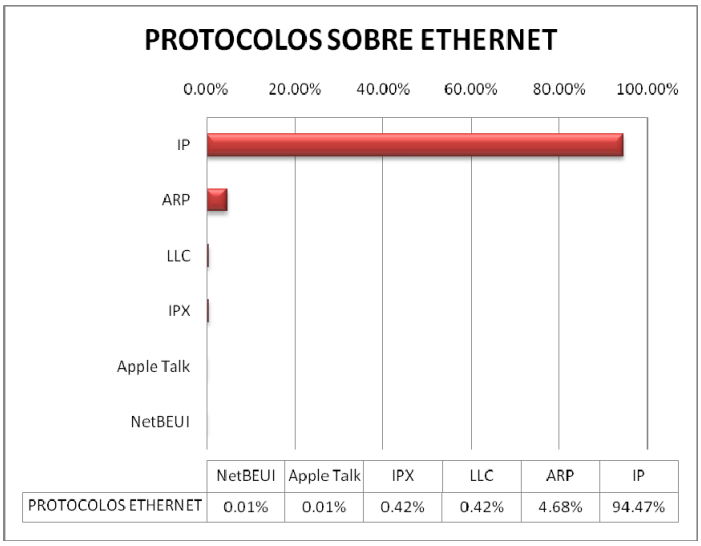


Figura. 3.50. Distribución de protocolos sobre Ethernet de la PB

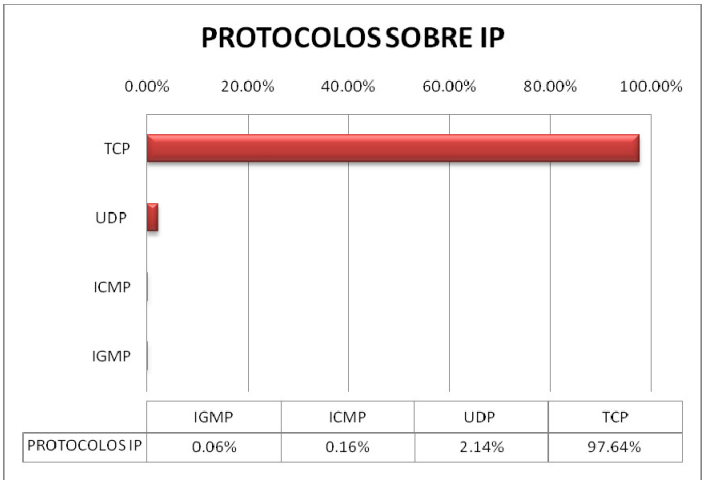


Figura. 3.51. Distribución de protocolos sobre IP de la PB

Tabla. 3.33. Distribución de protocolos de aplicación de la PB

PROTOCOLO	# PAQUETES
OTROS	4,339,803
NetBIOS Session	369,019
HTTP	86,411
NetBIOS Name	27,166
BOOTP	14,807
DNS	13,473
NetBIOS Datagram	9,512
SNMP	4,301
HTTPS	238
NFS	85
TOTAL	**4,864,815**

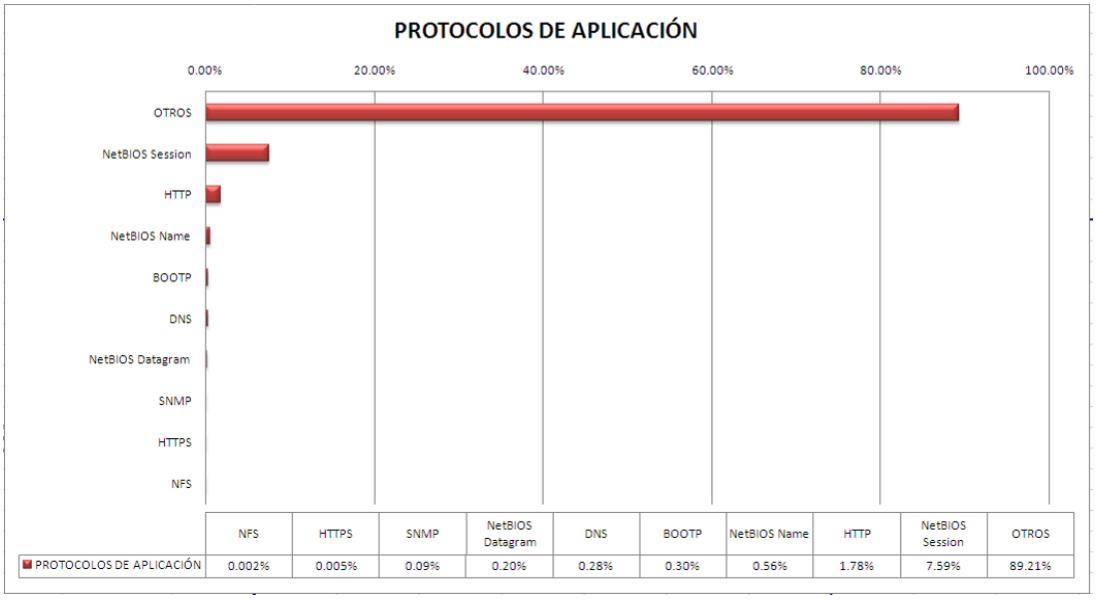


Figura. 3.52. Distribución de protocolos de aplicación de la PB

PRIMERA PLANTA ALTA

Tabla. 3.34. Tipo de Tráfico de la P1

TAMAÑO	# PAQUETES
PACKETS	2,930,000
BYTES	1,935,851,480
UNICAST	2,569,416
BROADCAST	324,000
MULTICAST	36,584

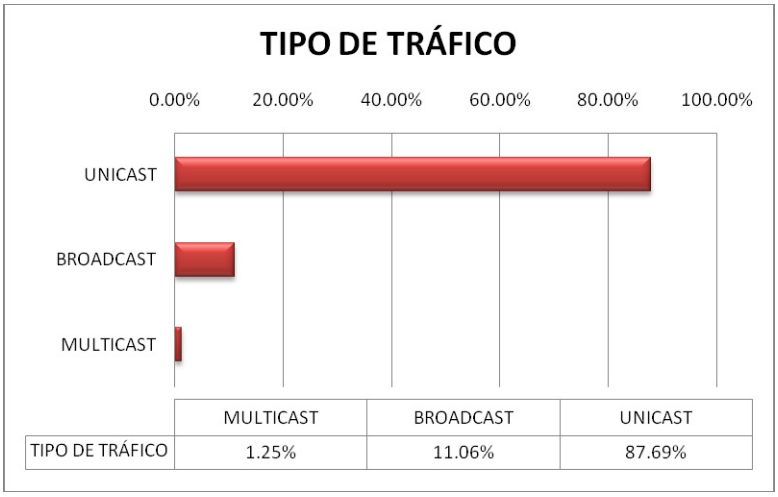


Figura. 3.53. Distribución del tipo de tráfico de la P1

Tabla. 3.35. Distribución de paquetes por tamaño de la P1

TAMAÑO	# PAQUETES
0-64 bytes	1,105,024
65-127 bytes	330,696
128-255 bytes	189,368
256-511 bytes	87,024
512-1023 bytes	74,800
> 1024 bytes	1,143,088
TOTAL	**2,930,000**

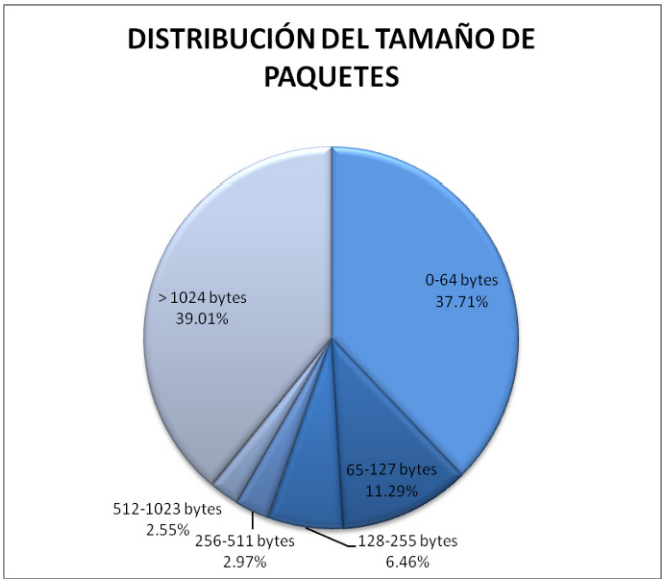


Figura. 3.54. Distribución de paquetes por tamaño de la P1

Tabla. 3.36. Distribución de protocolos de la P1

PROTOCOLO	# PAQUETES
IP	**2,626,024**
TCP	2,502,440
UDP	104,120
ICMP	15,544
OTROS	2,960
IGMP	960
ARP	**251,592**
LLC	**32,872**
IPX	**19,024**
NetBEUI	**376**
TOTAL	**303,864**

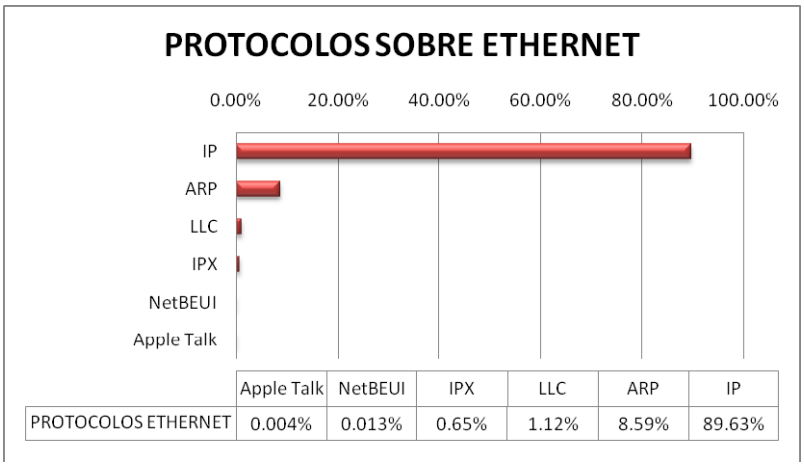


Figura. 3.55. Distribución de protocolos sobre Ethernet de la P1

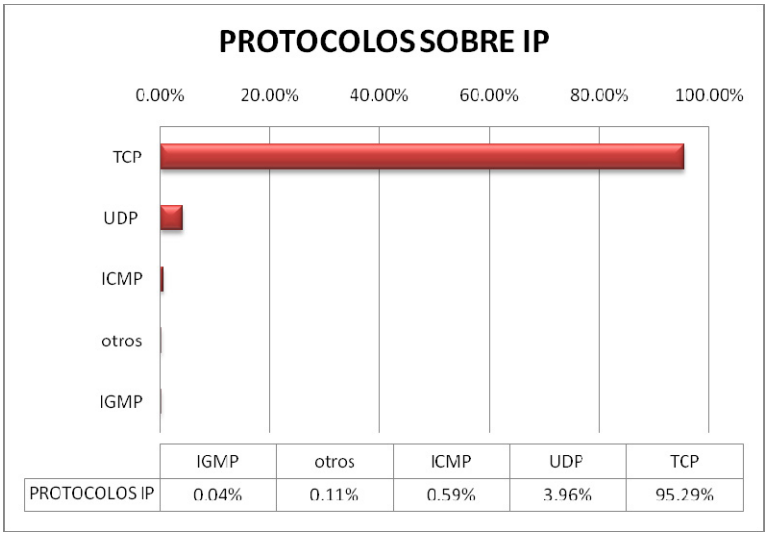


Figura. 3.56. Distribución de protocolos sobre IP de la P1

Tabla. 3.37. Distribución de protocolos de aplicación de la P1

PROTOCOLO	# PAQUETES
OTROS	1,610,096
NetBIOS Session	922,408
NetBIOS Name	25,928
DNS	16,440
BOOTP	12,632
SNMP	10,384
NetBIOS Datagram	8,672
TOTAL	**2,606,560**

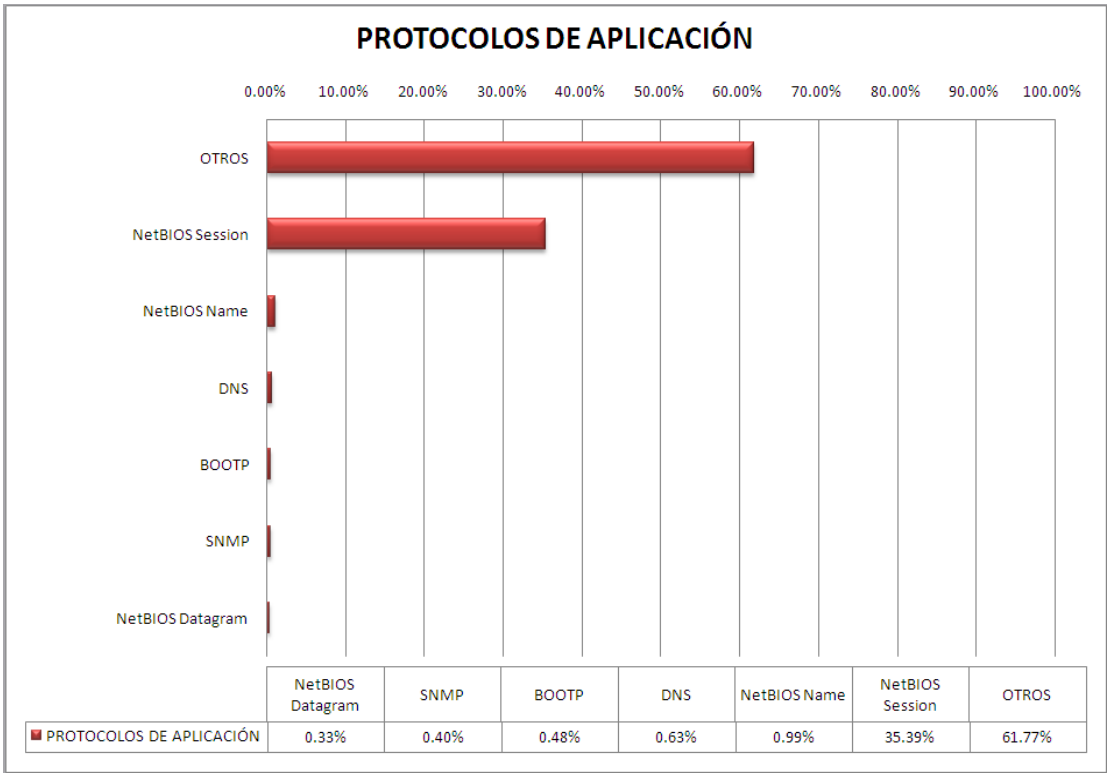


Figura. 3.57. Distribución de protocolos de aplicación de la P1

SEGUNDA PLANTA ALTA

Tabla. 3.38. Tipo de Tráfico de la P2

TAMAÑO	# PAQUETES
PACKETS	8,258,459
BYTES	3,909,638,502
UNICAST	7,937,523
BROADCAST	293,359
MULTICAST	27,577

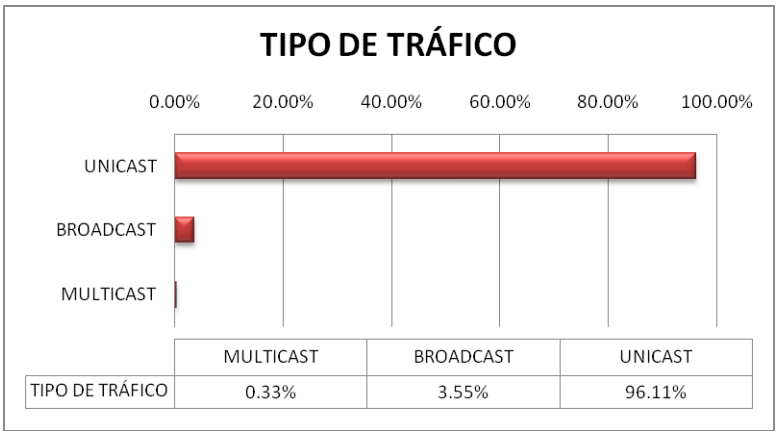


Figura. 3.58. Distribución del tipo de tráfico de la P2

Tabla. 3.39. Distribución de paquetes por tamaño de la P2

TAMAÑO	# PAQUETES
0-64 bytes	2,092,750
65-127 bytes	1,713,800
128-255 bytes	1,709,807
256-511 bytes	456,654
512-1023 bytes	265,595
> 1024 bytes	2,019,853
TOTAL	**8,258,459**

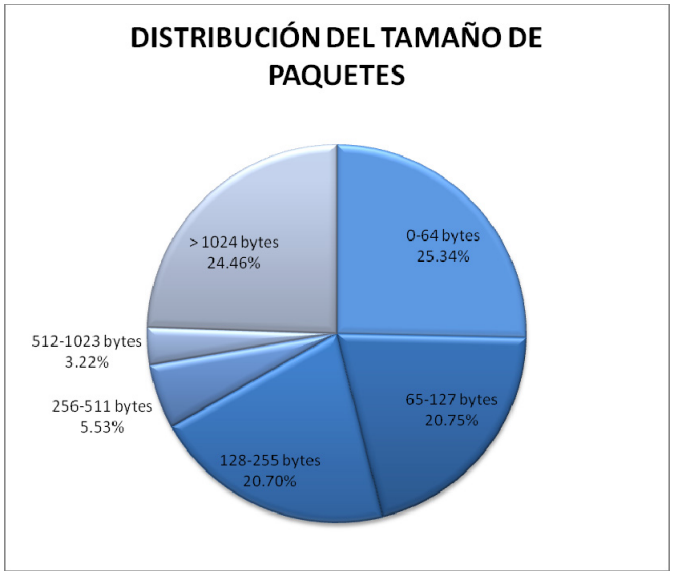


Figura. 3.59. Distribución de paquetes por tamaño de la P2

Tabla. 3.40. Distribución de protocolos de la P2

PROTOCOLO	# PAQUETES
IP	**7,989,861**
TCP	7,814,598
UDP	153,010
ICMP	19,943
IGMP	2,310
ARP	**219,692**
IPX	**25,619**
LLC	**23,144**
NetBEUI	**143**
TOTAL	**268,598**

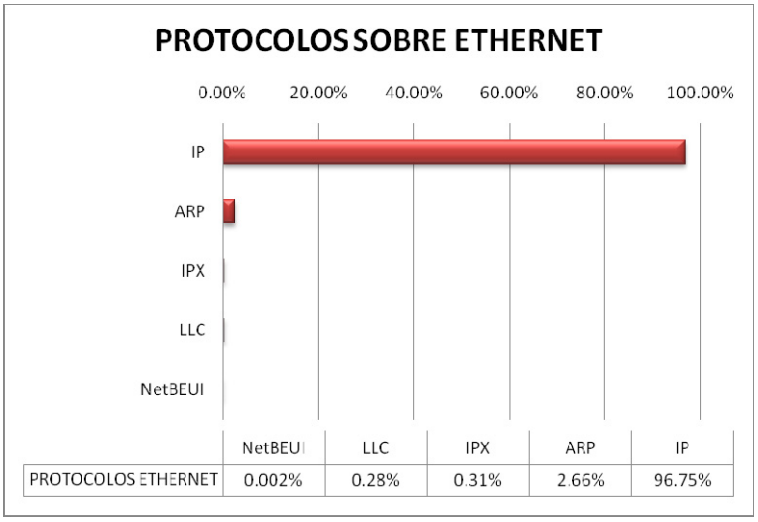


Figura. 3.60. Distribución de protocolos sobre Ethernet de la P2

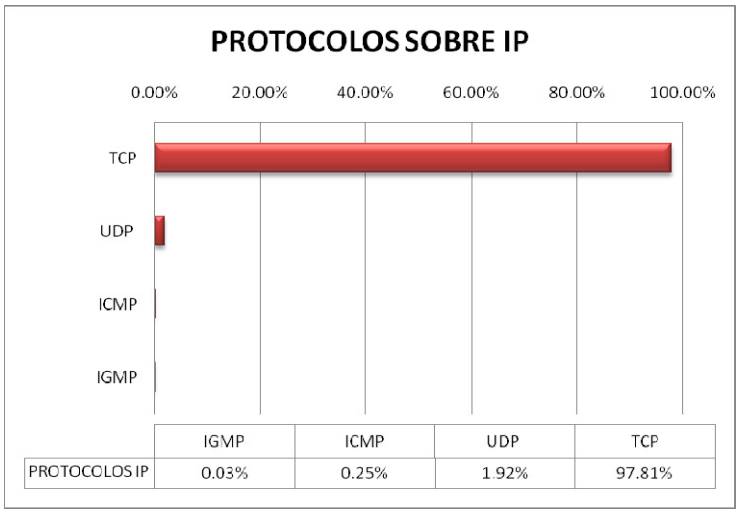


Figura. 3.61. Distribución de protocolos sobre IP de la P2

Tabla. 3.41. Distribución de protocolos de aplicación de la P2

PROTOCOLO	# PAQUETES
OTROS	6,473,863
NetBIOS Session	1,321,683
HTTP	55,715
DNS	34,826
NetBIOS Name	30,657
SNMP	21,010
BOOTP	16,742
NetBIOS Datagram	11,011
HTTPS	1,804
FTP	297
TOTAL	**7,967,608**

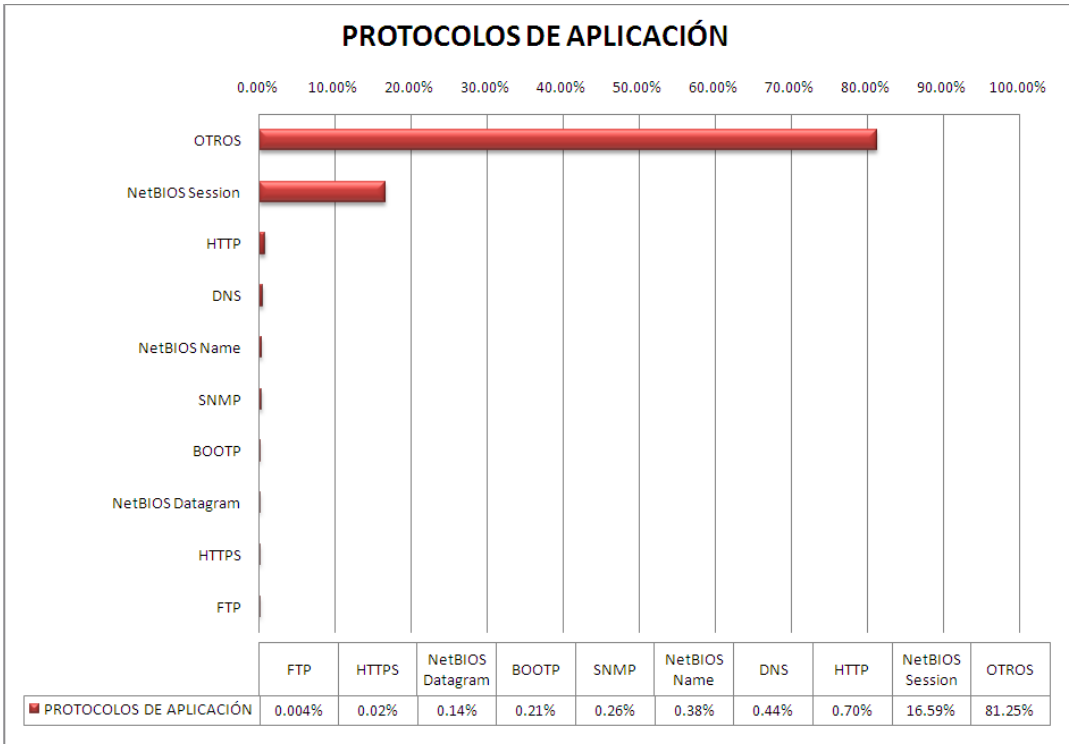


Figura. 3.62. Distribución de protocolos de aplicación de la P2

TERCERA PLANTA ALTA

Tabla. 3.42. Tipo de Tráfico de la P3

TAMAÑO	# PAQUETES
PACKETS	4,525,189
BYTES	1,942,992,971
UNICAST	4,064,445
BROADCAST	424,687
MULTICAST	36,057

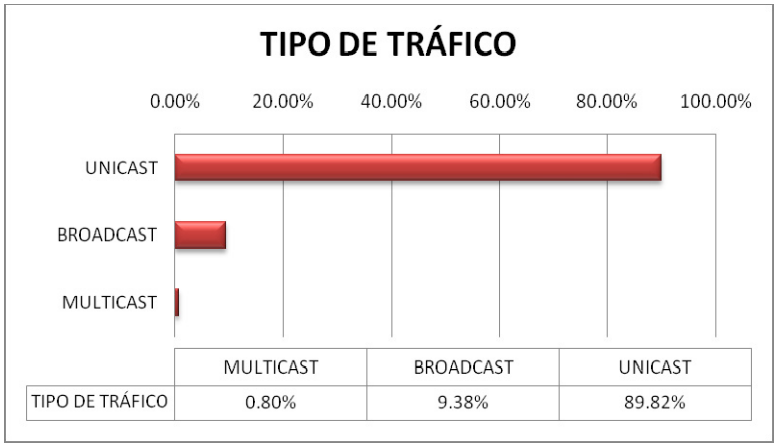


Figura. 3.63. Distribución del tipo de tráfico de la P3

Tabla. 3.43. Distribución de paquetes por tamaño de la P3

TAMAÑO	# PAQUETES
0-64 bytes	1,527,022
65-127 bytes	815,296
128-255 bytes	832,973
256-511 bytes	251,705
512-1023 bytes	114,913
> 1024 bytes	983,280
TOTAL	**4,525,189**

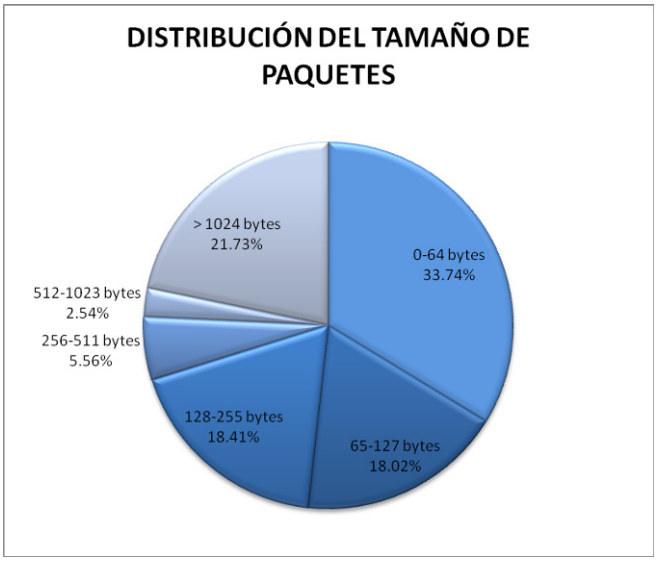


Figura. 3.64. Distribución de paquetes por tamaño de la P3

Tabla. 3.44. Distribución de protocolos de la P3

PROTOCOLO	# PAQUETES
IP	**4,148,075**
TCP	3,881,528
UDP	195,361
ICMP	64,933
OTROS	3,764
IGMP	2,489
ARP	**309,621**
IPX	**41,290**
LLC	**21,899**
Apple Talk	**3,376**
NetBEUI	**928**
TOTAL	**377,114**

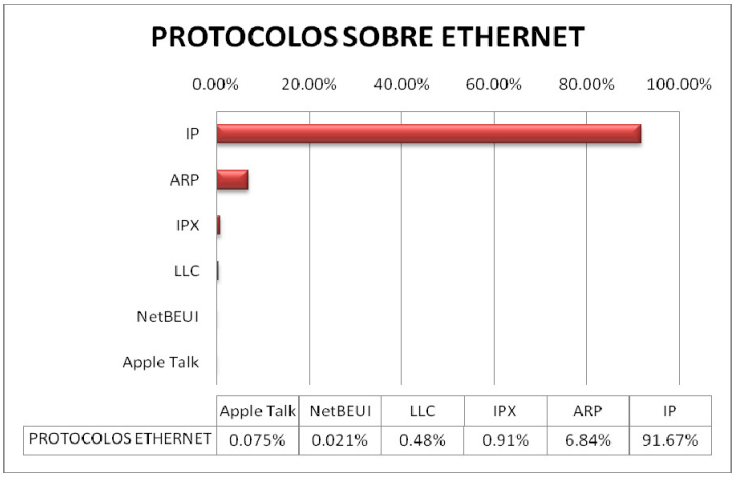


Figura. 3.65. Distribución de protocolos sobre Ethernet de la P3

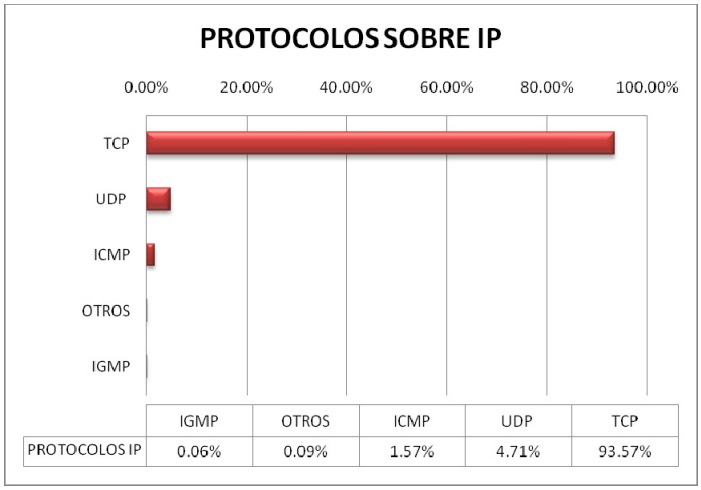


Figura. 3.66. Distribución de protocolos sobre IP de la P3

Tabla. 3.45. Distribución de protocolos de aplicación de la P3

PROTOCOLO	# PAQUETES
OTROS	3,602,018
NetBIOS Session	339,446
NetBIOS Name	54,488
DNS	37,944
BOOTP	15,739
NetBIOS Datagram	14,117
SNMP	13,138
TOTAL	**4,076,890**

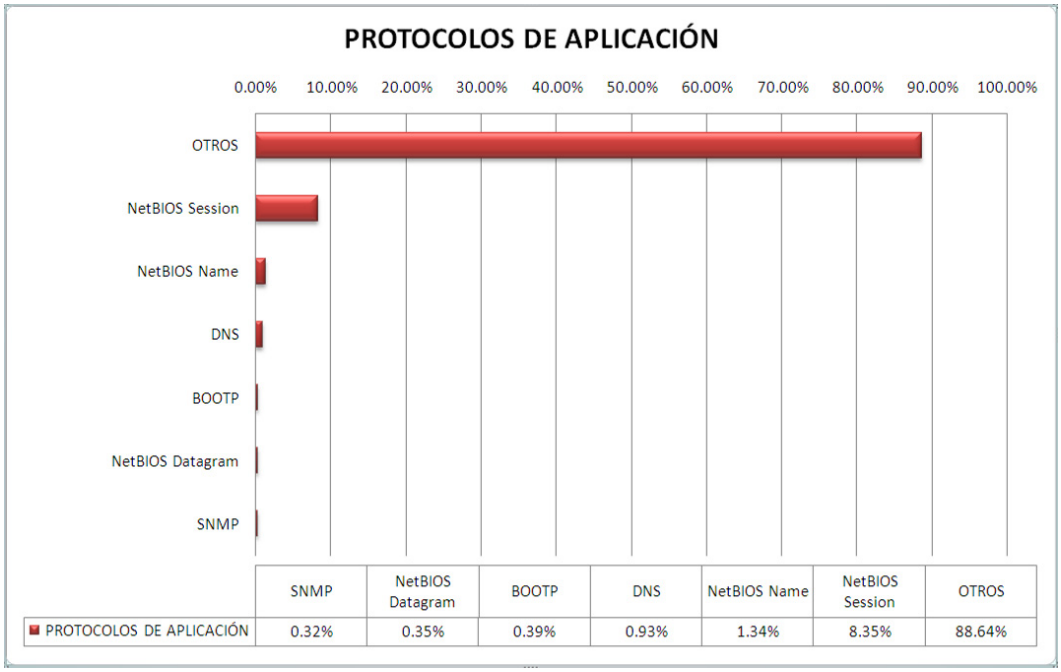


Figura. 3.67. Distribución de protocolos de aplicación de la P3

ENLACE A INTERNET

Tabla. 3.46. Tipo de Tráfico de INTERNET

TAMAÑO	# PAQUETES
PACKETS	3,908,035
BYTES	2,288,523,178
UNICAST	3,448,003
BROADCAST	428,458
MULTICAST	31,574

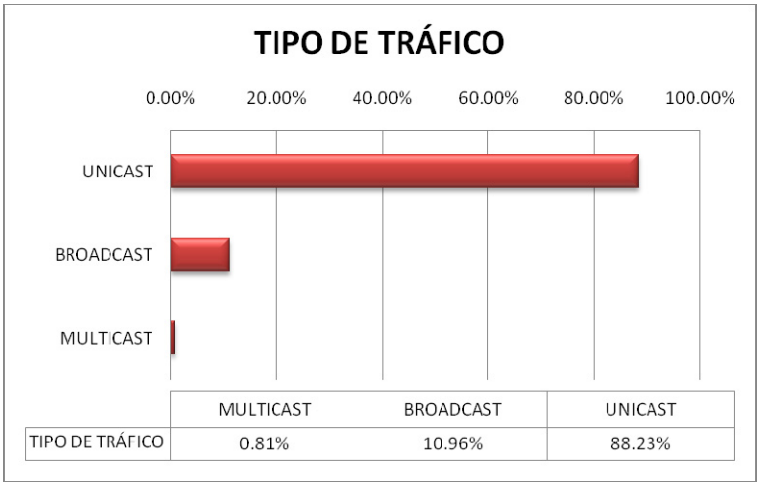


Figura. 3.68. Distribución del tipo de tráfico de INTERNET

Tabla. 3.47. Distribución de paquetes por tamaño de INTERNET

TAMAÑO	# PAQUETES
0-64 bytes	1,931,750
65-127 bytes	275,443
128-255 bytes	67,334
256-511 bytes	195,926
512-1023 bytes	110,506
> 1024 bytes	1,327,075
TOTAL	**3,908,034**

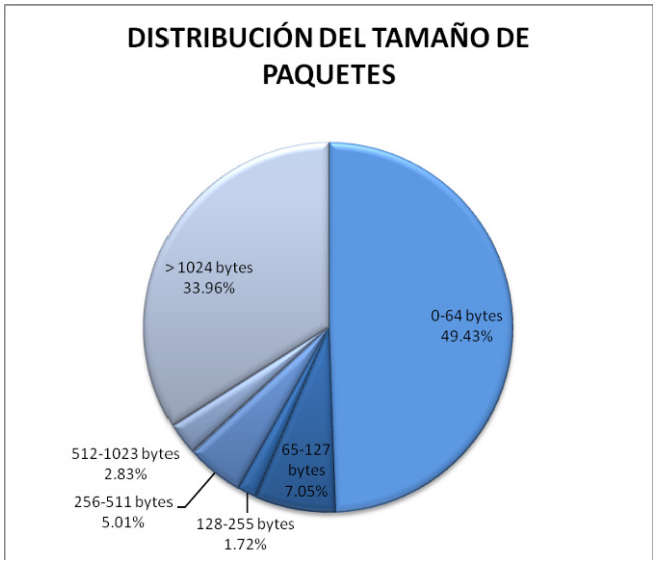


Figura. 3.69. Distribución de paquetes por tamaño de INTERNET

Tabla. 3.48. Distribución de protocolos de INTERNET

PROTOCOLO	# PAQUETES
IP	**3,535,286**
TCP	3,337,642
UDP	187,392
OTROS	4,282
ICMP	4,109
IGMP	1,862
ARP	**322,829**
LLC	**24,931**
IPX	**24,365**
NetBEUI	**490**
Apple Talk	**134**
TOTAL	**372,749**

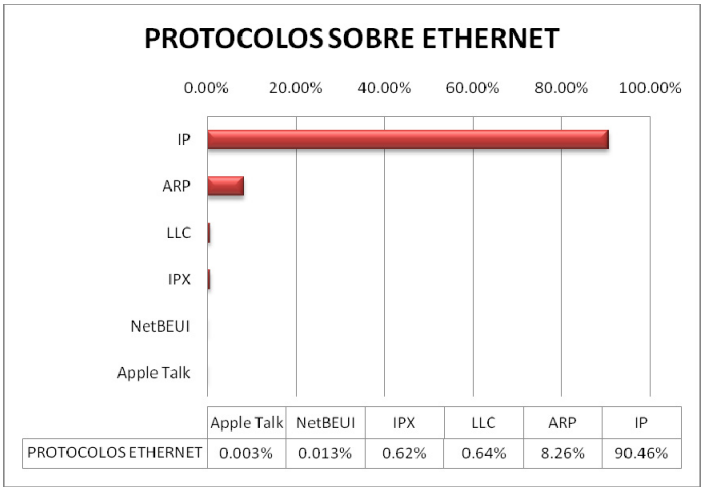


Figura. 3.70. Distribución de protocolos sobre Ethernet de INTERNET

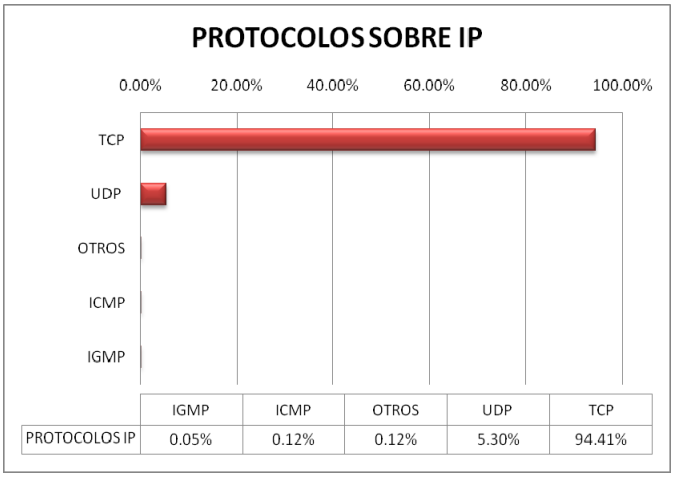


Figura. 3.71. Distribución de protocolos sobre IP de INTERNET

Tabla. 3.49. Distribución de protocolos de aplicación de INTERNET

PROTOCOLO	# PAQUETES
OTROS	3,364,522
DNS	56,986
NetBIOS Name	45,984
HTTP	28,944
NetBIOS Datagram	14,496
BOOTP	13,920
SNMP	96
NetBIOS Session	86
TOTAL	**3,525,034**

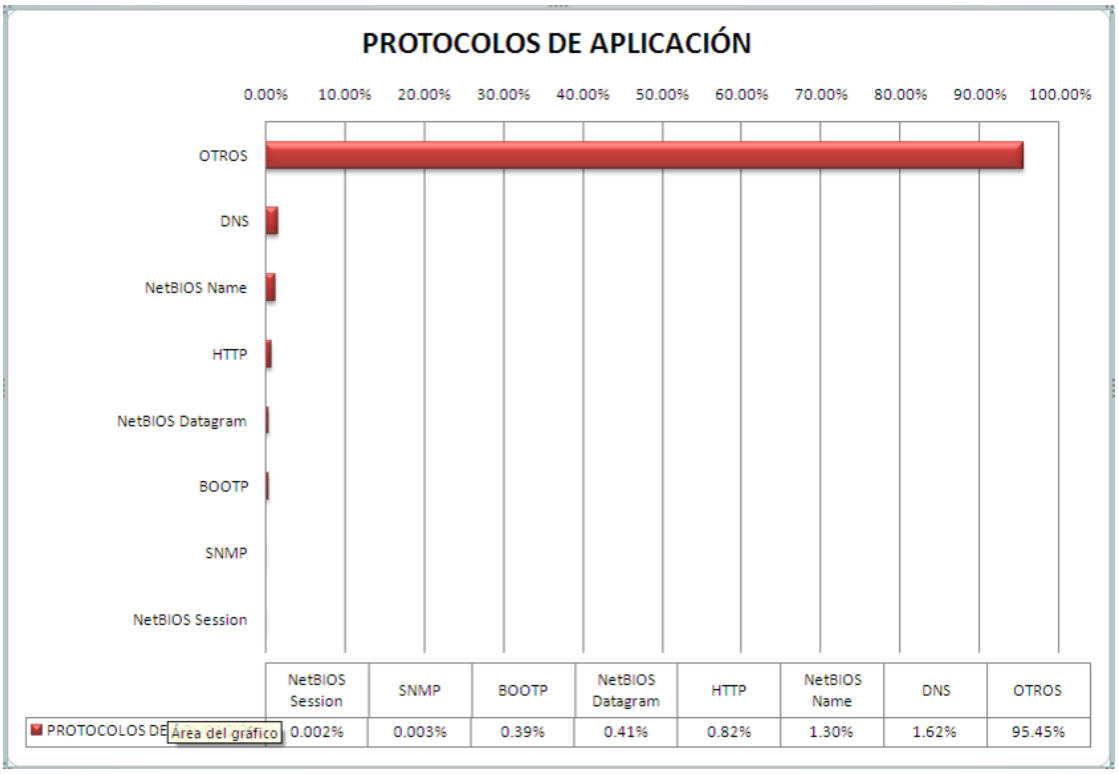


Figura. 3.72. Distribución de protocolos de aplicación de INTERNET

3.4.3. ANÁLISIS DE LATENCIA EN LA RED WAN

Finalmente y aprovechando los sensores de latencia que el software PRTG provee, en el PC destinado al monitoreo y con la tarjeta de red asociada a dicha aplicación, se puso en marcha sensores para cada una de las dependencias que componen la WAN Municipal,

estos sensores utilizan la herramienta ping, para enviar continuamente peticiones e ir almacenando los intervalos de tiempo que tardan las respuestas en llegar, dichos tiempos son los retardos que le toman a un paquete en viajar ida y vuelta entre dos puntos a través de la red, a continuación se detallan las antenas de las red WAN a las cuales se configuraron sensores de latencia.

- Antena de Comisaría (10.10.5.1).

- Antena de Tránsito (10.10.8.1).

- Antena de Cultura (10.10.6.1).

- Antena del Hospital (10.10.4.1).

- Antena de Bodegas (10.10.2.1).

- Antena del Mercado Mayorista (10.10.3.1).

- Antena del Camal (10.10.7.2).

A continuación se observan las gráficas de los sensores de latencia de cada una de las dependencias mencionados, dichas gráficas corresponden al día 10 de Julio como se puede notar, los retardos comienzan a bajar en el intervalo de horas laborables, pues las antenas al estar atendiendo el tráfico de datos que se genera entre dependencias, están continuamente registradas con el Access point, los cual no ocurre en horas de inactividad de la red, pues cada antena debe registrarse con el Access Point, para estar incluido en la lista de *polling* del algoritmo que corre este equipo para conceder acceso al medio para la transmisión, motivo por el cual cada antena debe primero registrarse y luego enviar el ping lo cual dispara los tiempos de retardo.

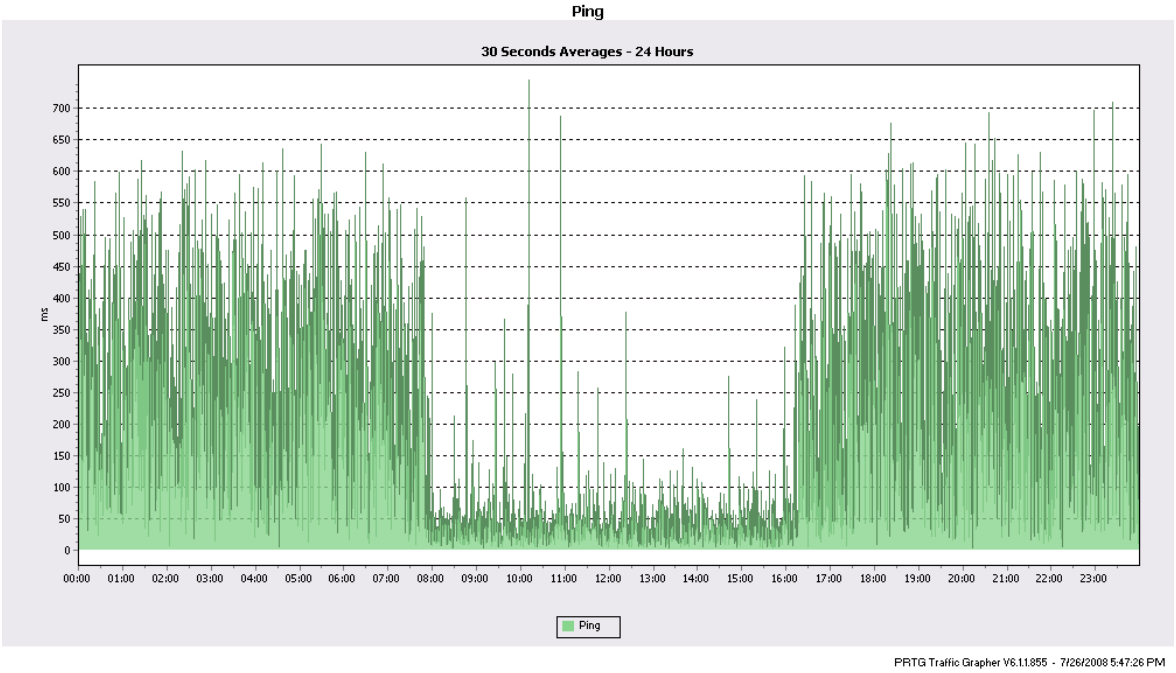


Figura. 3.73. Retardo de las Comisarías

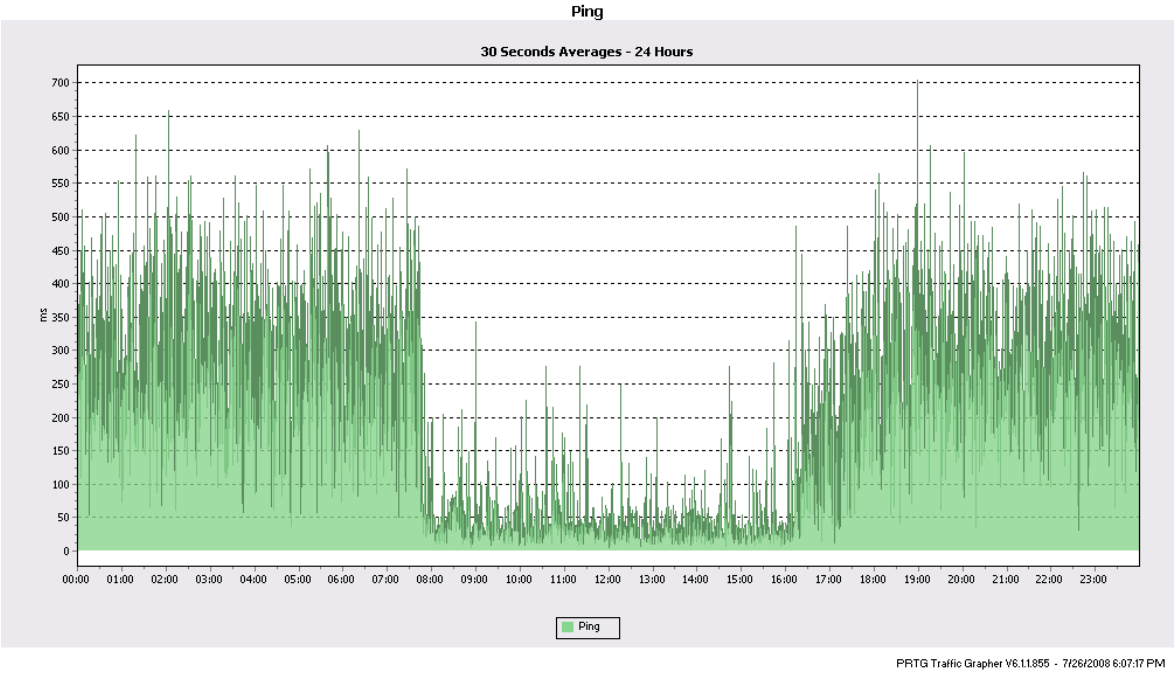


Figura. 3.74. Retardo de Tránsito

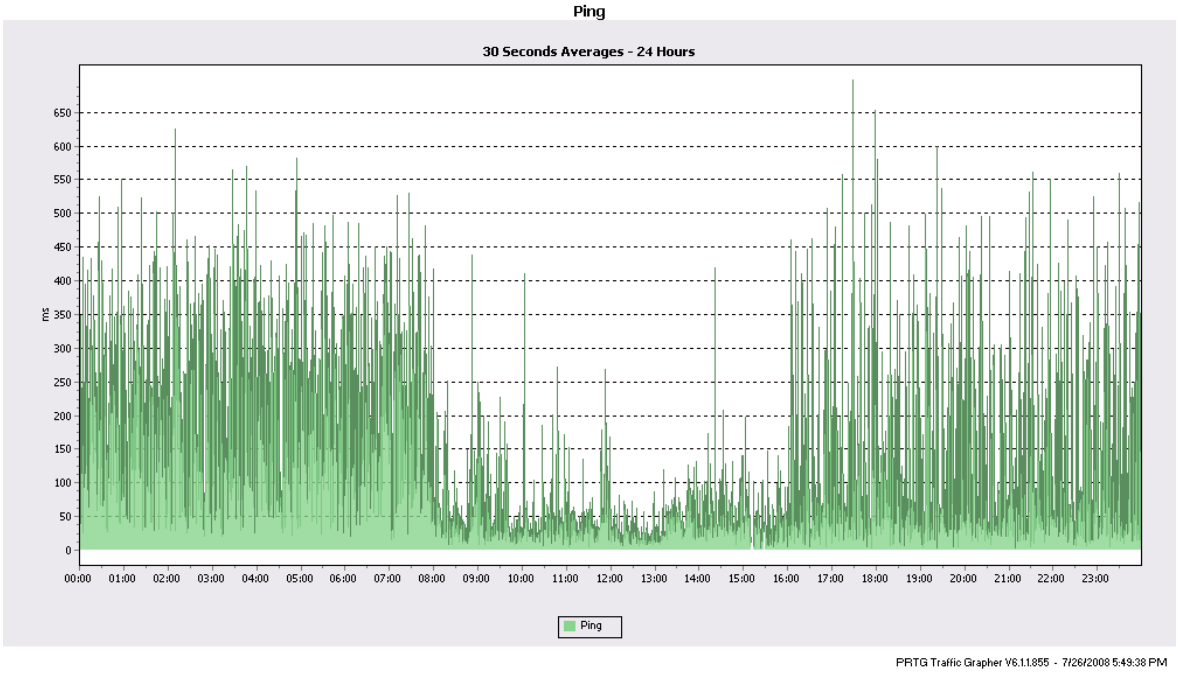


Figura. 3.75. Retardo de Cultura

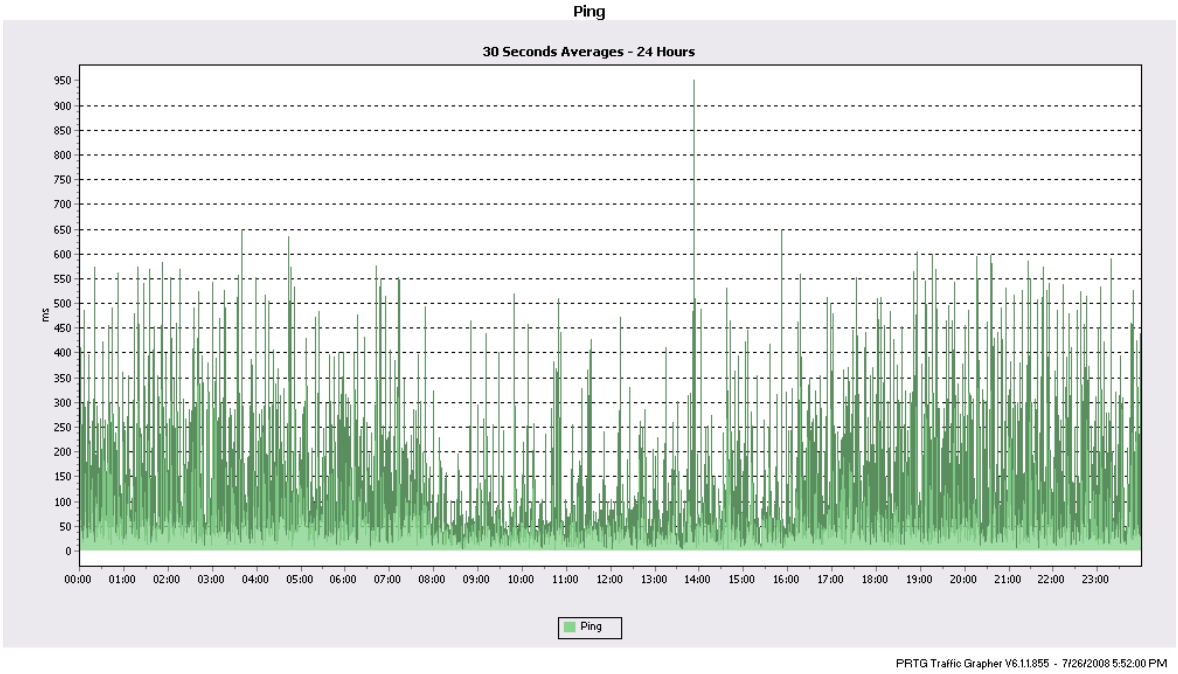


Figura. 3.76. Retardo de Hospital

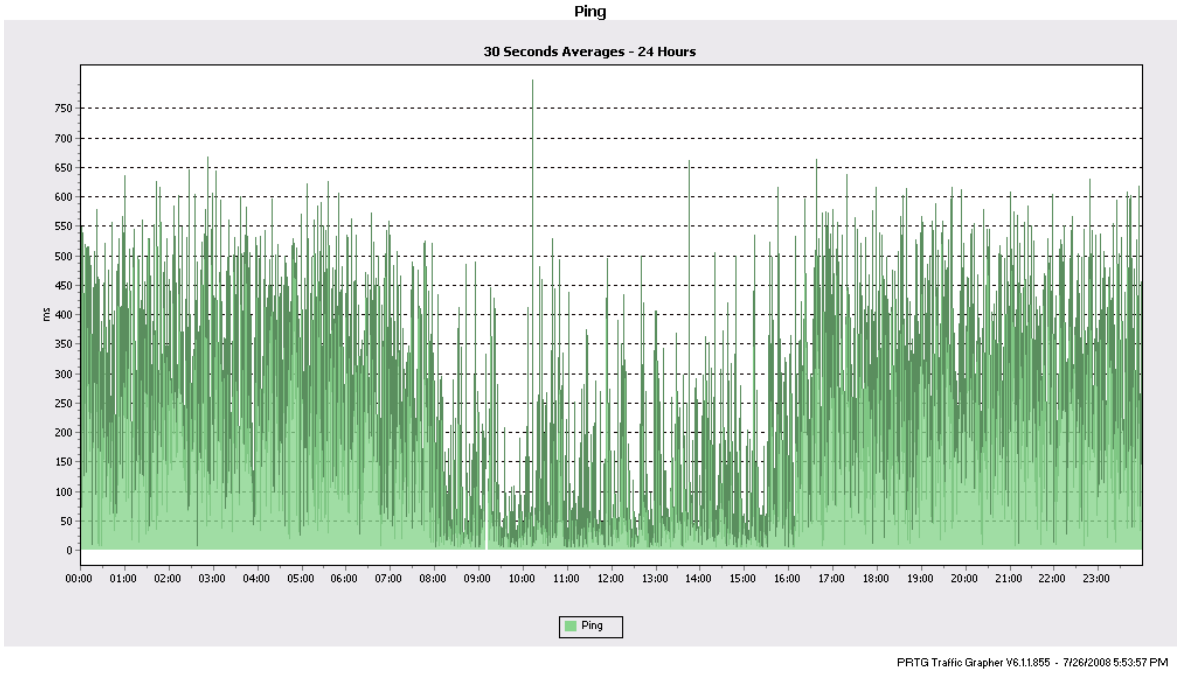


Figura. 3.77. Retardo de Bodega

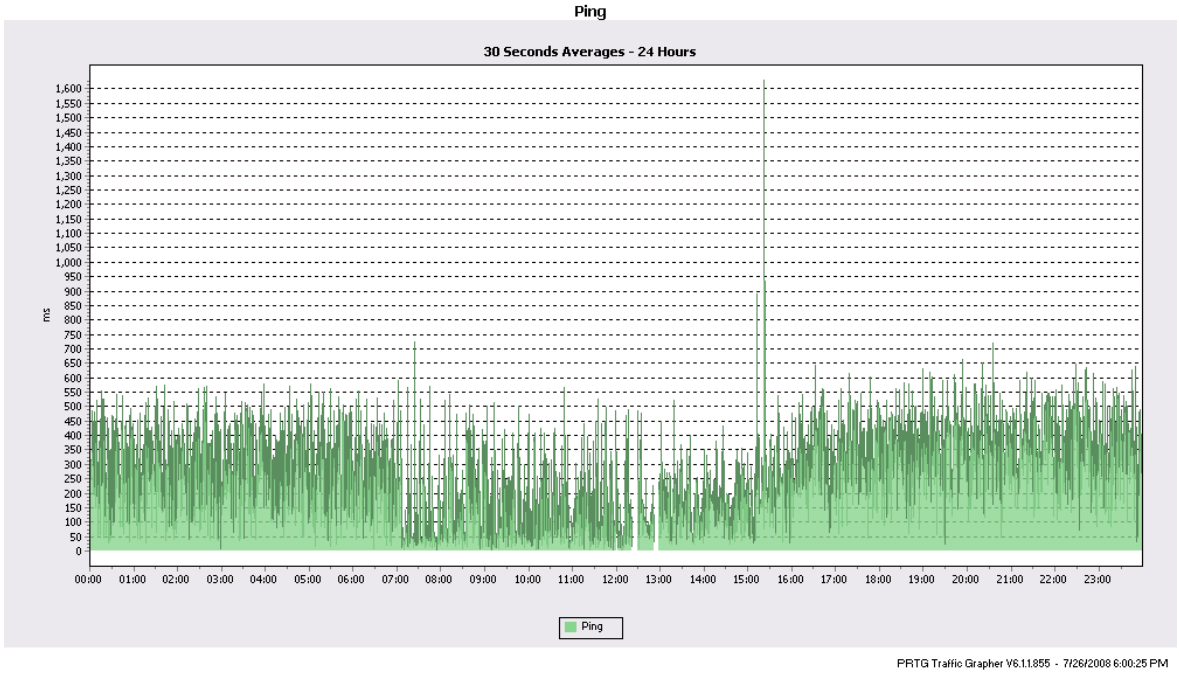


Figura. 3.78. Retardo del Mercado Mayorista

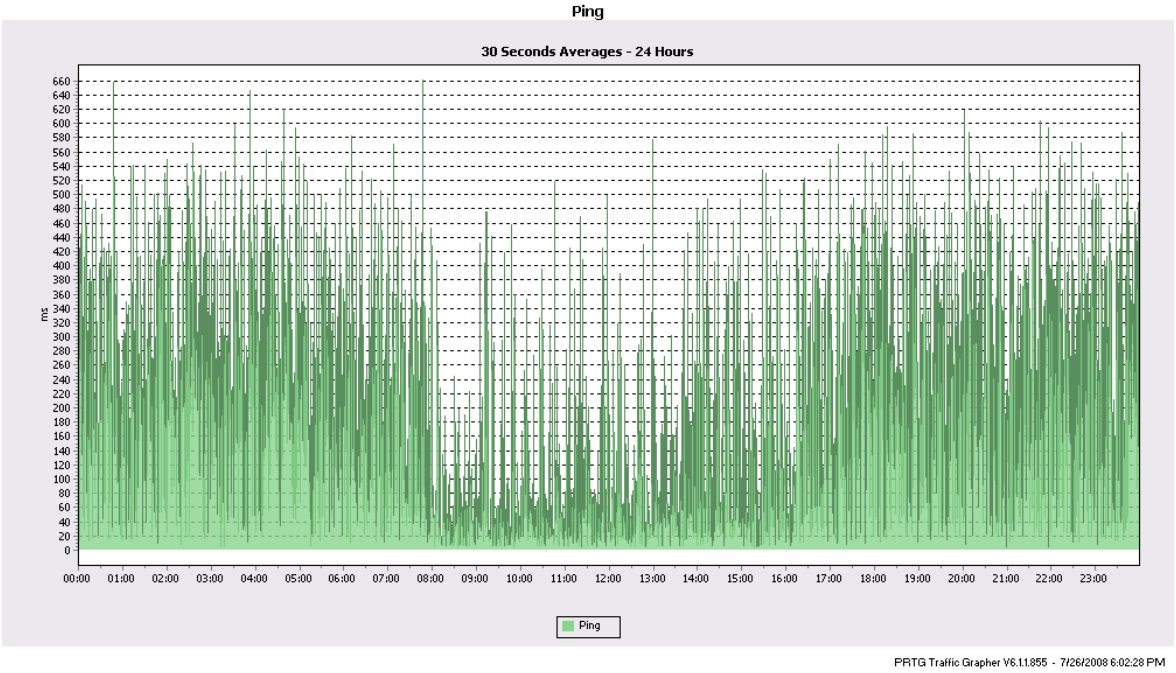


Figura. 3.79. Retardo del Camal

En la tabla y gráfica siguientes se resume los retardos de ida y vuelta (RTT) máximos y promedios considerados dentro del intervalo de horas laborables para cada dependencia, para nuestro análisis es importante conocer el retardo en sentido unidireccional, sin embargo es muy complicado determinar dicha variable, sin embargo una división entre dos del valor RTT nos puede dar una aproximación bastante buena.

Tabla. 3.50. Resumen de retardos de la red WAN Municipal

DEPENDENCIA	RETARDO DE IDA Y VUELTA (RTT)		RETARDO UNIDIRECCIONAL (RTT/2)	
	MAX (ms)	PROMEDIO (ms)	MAX (ms)	PROMEDIO (ms)
COMISARIAS	745.00	45.49	372.50	22.75
TRÁNSITO	348.00	44.49	174.00	22.25
CULTURA	447.00	49.93	223.50	24.97
HOSPITAL	948.00	76.22	474.00	38.11
BODEGAS	782.00	97.67	391.00	48.84
MAYORISTA	1641.00	162.68	820.50	81.34
CAMAL	578.00	93.35	289.00	46.68

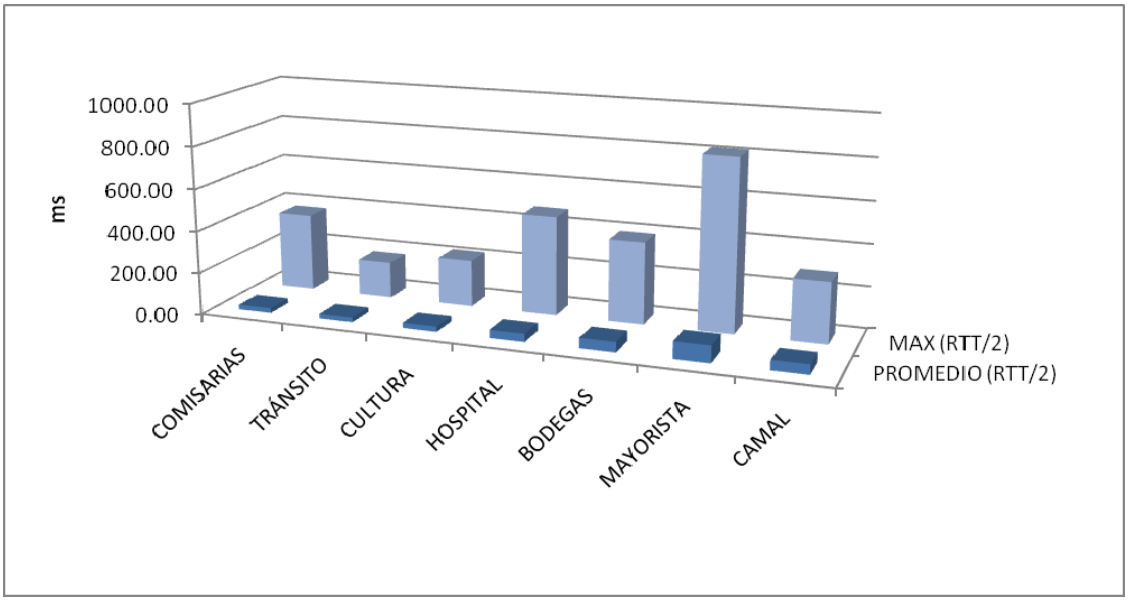


Figura. 3.80. Gráfica comparativa de latencia

Del monitoreo realizado a la red de datos de la matriz del Municipio podemos desprender, que el tráfico visto desde el punto de vista cuantitativo que cruza por los enlaces principales, está en todos los casos por debajo del 1% de la capacidad de dichos enlaces, por lo tanto no existe problemas de elevada congestión, lo cual resulta altamente beneficioso al momento de instalar un nuevo servicio que utilizará esta red como medio de comunicación para brindar el servicio de telefonía, sin embargo desde el punto de vista cualitativo, podemos observar que en la mayoría de los casos el tráfico broadcast comienza a ser elevado, especialmente por el protocolo ARP de resolución de direcciones, y con el incremento considerable de equipos en la red, que se producirá al introducir teléfonos IP, es previsible que este se incremente aun más, pues cada equipo de la red genera este tipo de tráfico para descubrir a otros que se encuentren dentro de ella, por lo tanto se torna importante plantear estrategias que se orienten a disminuir el impacto de este tráfico en la red, implementando VLAN's, que reducen virtualmente el tamaño de grandes redes locales a subredes más pequeñas, brindando un mecanismo efectivo para solventar este problema.

Un aspecto positivo a resaltar es la distribución en el tamaño de los paquetes, como podemos observar la mayoría de los paquetes que atraviesan la red están entre 0 y 127

bytes, es decir en gran parte son de corta duración lo cual es un aliciente para asegurar que los paquetes de voz en las colas de los switches, no tengan retardos muy grandes, en los casos cuando el equipo estuvo previamente a la llegada de un paquete de voz transmitiendo uno de datos y debe necesariamente esperar que aquella transmisión termine para dar prioridad al paquete de telefonía que tuvo que retardarse mientras esto ocurre, al ser este tiempo reducido se ayuda a asegurar la QoS. Un comportamiento que cambiará al introducir un sistema de telefonía IP en la red es el incremento de tráfico UDP el cual actualmente es bastante reducido lo cual implica un predominio de tráfico TCP, sin que esto tenga implicaciones importantes en el desempeño global de la red.

En el análisis de latencia de la red WAN, podemos ver que los tiempos de retardo son aceptables, pues tomando como referencia la Tabla 1.6. Clases de calidad del UIT-T según el retardo de transmisión, hasta 150ms es aceptable y de acuerdo al monitoreo ninguna de las dependencias de la municipalidad supera este límite en promedio en sentido unidireccional. Sin embargo es imperiosamente recomendable revisar el radioenlace que conecta al mercado mayorista, pues evidentemente este enlace sale de los parámetros típicos mostrados en esta red lo cual brinda un claro indicio de una posible falla en dicho sistema, además durante todos los días que duró el monitoreo de tráfico se determino claramente una baja disponibilidad en este enlace, observándose extendidos períodos de tiempo en los que dicha antena no respondió a las peticiones algunos de hasta 10 minutos.

3.5. ANÁLISIS DE TRÁFICO DE VOZ

Para el presente análisis, se recurrió al uso de la herramienta SMDR (Station Message Detail Recording), que provee la central telefónica analógica Panasonic KX-T96100, la cual está equipada con un puerto serial con conector DB-25, que estaba diseñado para conectarse a una impresora serial, que se encargaba de imprimir el detalle de los registros que la central enviaba a través de dicho puerto, para nuestro análisis en lugar de imprimir dichos registros, los capturamos digitalmente a través del hyperterminal, pues los registros son enviados como bits a través del puerto serial en formato ASCII. Estos registros contienen información de la fecha y hora de llamada, así como del la fuente y el destino de la misma y su duración, cuando la llamada es entrante se registra como “INCOMING”. Básicamente el análisis de tráfico telefónico se realiza para hallar la hora

del día de mayor ocupación del sistema, también conocida como hora pico; la intensidad de tráfico telefónico generado en esta hora es muy importante al momento de dimensionar la red telefónica.

El período de monitoreo considerado fue de la segunda a la tercera semana de Mayo, desde las 8 am hasta las 6 pm, considerando que en el mes de mayo el municipio aun no estaba en horario de jornada única, observándose claramente un período de inactividad de 1pm 2:30pm en el horario de almuerzo.

A través de los datos obtenidos en 14150 registros de las dos semanas laborables monitoreadas, podemos observar los siguientes resultados, en cuanto al tipo de tráfico generado.

Tabla. 3.51. Resumen del tipo de tráfico de voz

TIPO DE TRÁFICO TELEFÓNICO			DUARACIÓN [s]
ENTRANTE			531821
SALIENTE			562377
	PSTN		486389
		LOCAL	327425
		CELULAR	78846
		REGIONAL	67082
		NACIONAL	9821
		1700	2205
		1800	1010
	DEPENDENCIAS		75988
		COMISARIAS	25225
		CULTURA	18610
		BODEGAS	9874
		TRANSITO	9029
		HOSPITAL	8618
		CAMAL	2804
		MERCADO	1828

Figura. 3.81. Gráfica de tráfico de voz por dirección

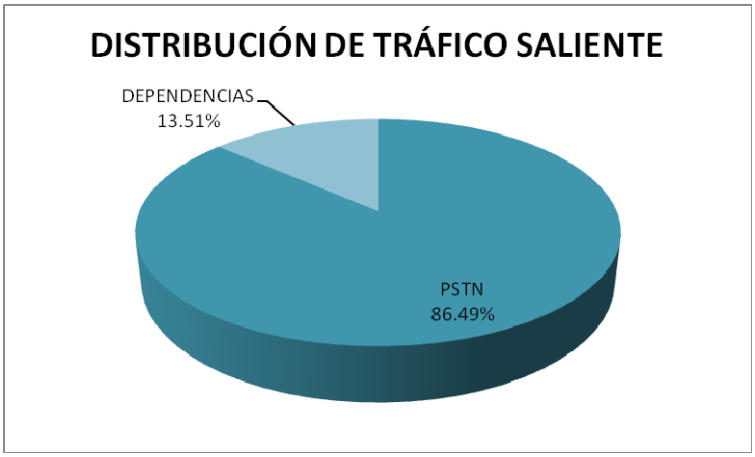


Figura. 3.82. Gráfica de la distribución del tráfico de voz saliente

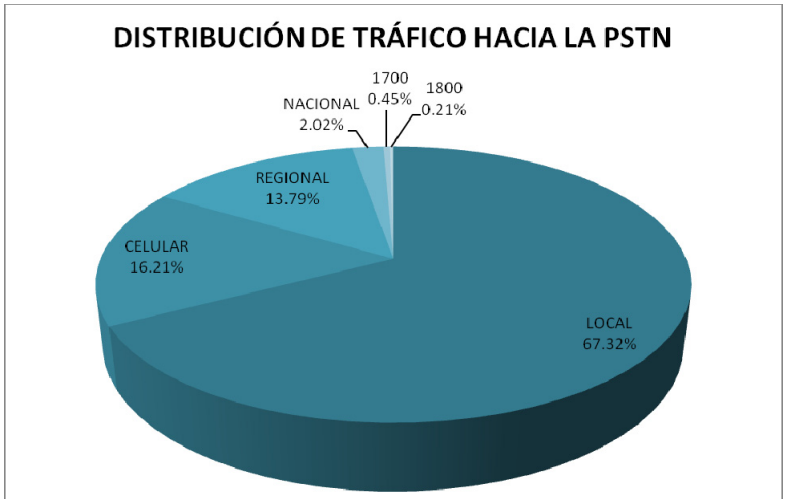


Figura. 3.83. Gráfica de la distribución del tráfico de voz saliente hacia la PSTN

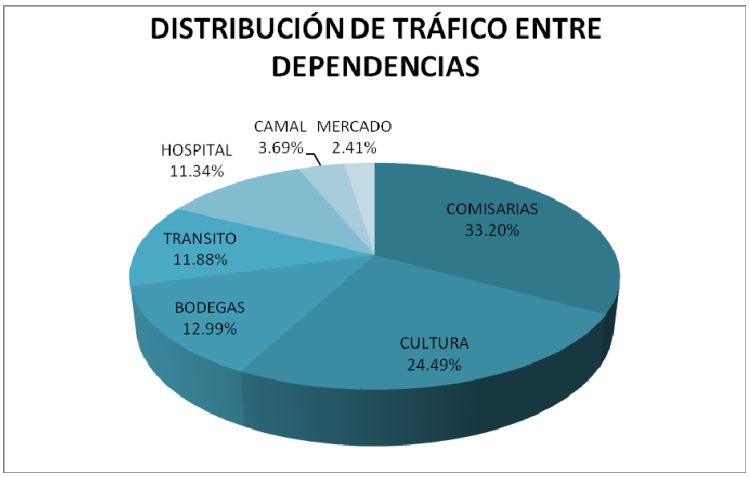


Figura. 3.84. Gráfica de la distribución del tráfico de voz saliente entre dependencias municipales

Básicamente el análisis de tráfico telefónico se realiza para hallar la hora del día de mayor ocupación del sistema, también conocida como hora pico; la intensidad de tráfico telefónico generado en esta hora es muy importante al momento de dimensionar la red telefónica, esta hora pico nos permitirá evaluar el número de troncales que el sistema requiere para operar satisfactoriamente. Es importante señalar que debemos evaluar no solo el número de troncales necesarias para comunicarse con la red pública conmutada, sino también entre dependencias, pues la nueva arquitectura telefónica permitirá direccionar las llamadas entre dependencias por la red de datos interna del municipio y no por la red pública conmutada como hasta ahora se venía haciendo.

Para evaluar el tráfico entre dependencias debemos considerar que porción de tráfico tanto entrante como saliente corresponde a este grupo, esto no presenta inconveniente para el tráfico saliente, pues como se muestra en la Fig. 3.84, dicha distribución está completamente determinada, el problema suscita con el tráfico entrante del cual solo se conoce su totalidad, más no una distribución detallada. Dados estos antecedentes vamos a proceder a realizar una estimación sobre el tráfico entrante, como se determinó anteriormente el 13.51% de tráfico saliente corresponde a llamadas a otras dependencias, partiendo de la premisa de que el municipio ofrece servicios centralizados el tráfico de voz entre dependencias debe ser más intenso de afuera hacia dentro, que en sentido contrario, por ello se estimará el 16% del tráfico entrante como aquel que viene dirigido de otras dependencias, este 16% se lo distribuirá entre dependencias de manera exactamente igual a lo mostrado en la Fig. 3.84. De este modo las llamadas entrantes quedan distribuidas de la siguiente manera:

Tabla. 3.52. Estimación de llamadas entrantes

ESTIMACIÓN DE LLAMADAS ENTRANTES	
EXTERIOR	**84.00%**
ENTE DEPENDENCIAS	**16.00%**
COMISARIAS	5.31%
CULTURA	3.92%
BODEGAS	2.08%
TRANSITO	1.90%
HOSPITAL	1.81%
CAMAL	0.59%
MERCADO	0.38%

A través del análisis y organización de los datos se obtiene la intensidad de tráfico (A) de cada hora; este parámetro tiene como unidad el Erlang que equivale a una llamada de una hora de duración, considerada en una hora de referencia, (A) se puede calcular de dos formas:

$$A = To/3600s$$

$$A = C.T$$

Donde:

A: Es la intensidad de tráfico en Erlangs.

To: Es el tiempo de ocupación total en segundos.

C: Es el número de llamadas por segundo, obtenido de la división de las llamadas monitoreadas durante una hora.

T: Es el tiempo medio de llamada, proviene de la división de To para el número de llamadas.

En las siguientes tablas se muestra la clasificación de todas las llamadas generadas durante el periodo de monitoreo para cada dependencias y hacia la PSTN (desde el 5 hasta el 16 de Mayo del 2008 en horarios y días laborables).

Tabla. 3.53. Intensidad de tráfico telefónico hacia y desde el exterior

	PSTN									
	DIAS									
Horas	**Lunes 5**	**Martes 6**	**Miercls 7**	**Jueves 8**	**Viernes 9**	**Lunes 12**	**Martes 13**	**Miercls 14**	**Jueves 15**	**Viernes 16**
8	1.09081	2.03257	2.43808	1.78403	2.39377	1.14720	1.61908	2.10012	2.14247	2.07012
9	2.59284	3.56453	3.75882	3.84716	2.63892	2.91851	3.66438	3.47698	2.67853	3.20633
10	3.60959	2.96639	4.28481	4.27363	2.59584	3.38166	3.73078	3.64893	3.20296	3.28086
11	2.36494	2.88622	2.79517	3.67922	1.64799	2.93607	2.32958	3.29267	3.35190	3.21231
12	3.23432	2.72124	2.43806	2.20818	2.15473	2.74741	3.77776	2.67942	2.84402	2.29393
13	0.29142	0.06229	0.14429	0.30720	0.37993	0.33778	2.44533	2.67328	3.02102	1.55372
14	1.66183	1.37783	1.52253	0.85424	1.40832	0.84157	3.54464	2.33279	2.49742	3.62740
15	3.24389	4.60511	4.02746	4.48481	3.73587	3.57507	3.80651	3.08219	2.89789	3.56860
16	3.25398	3.21111	3.20822	3.14064	3.30253	2.70118	1.89379	1.40139	1.66959	1.46839
17	2.77627	1.64583	2.83053	2.59463	2.00473	1.94621	1.09057	0.35871	0.31812	0.46916
18	1.16158	0.81816	1.03656	0.99853	0.03673	0.80868	0.42448	0.37002	0.04802	0.24088

Tabla. 3.54. Intensidad de tráfico telefónico hacia y desde las comisarias

	COMISARÍAS									
	DIAS									
Horas	**Lunes 5**	**Martes 6**	**Miercls 7**	**Jueves 8**	**Viernes 9**	**Lunes 12**	**Martes 13**	**Miercls 14**	**Jueves 15**	**Viernes 16**
8	0.05257	0.13260	0.14212	0.16501	0.17142	0.07950	0.24279	0.20298	0.14638	0.05925
9	0.12392	0.28493	0.44123	0.16069	0.25565	0.20522	0.17537	0.28412	0.17876	0.18222
10	0.29175	0.12756	0.14892	0.23067	0.10389	0.13970	0.13601	0.16291	0.14114	0.24780
11	0.09639	0.32587	0.19756	0.33306	0.05848	0.13218	0.12887	0.32395	0.29228	0.15788
12	0.10514	0.22129	0.14806	0.16773	0.10409	0.09814	0.11424	0.15350	0.19204	0.06453
13	0.00617	0.00238	0.00761	0.00609	0.00832	0.00590	0.06598	0.11840	0.06611	0.05174
14	0.04079	0.04581	0.11286	0.03160	0.03938	0.03811	0.16771	0.07751	0.11881	0.09141
15	0.18253	0.31830	0.17924	0.24156	0.18820	0.27088	0.14877	0.15982	0.22326	0.13122
16	0.16713	0.08188	0.24138	0.43483	0.14153	0.17095	0.11212	0.04538	0.04394	0.03327
17	0.19839	0.10007	0.16700	0.23778	0.08823	0.18291	0.01079	0.01666	0.01381	0.01467
18	0.04757	0.01887	0.01534	0.02372	0.00201	0.02008	0.00137	0.00276	0.00195	0.00257

Tabla. 3.55. Intensidad de tráfico telefónico hacia y desde cultura

	CULTURA									
	DIAS									
Horas	Lunes 5	Martes 6	Miercls 7	Jueves 8	Viernes 9	Lunes 12	Martes 13	Miercls 14	Jueves 15	Viernes 16
8	0.08934	0.06205	0.12937	0.16719	0.16598	0.09797	0.17149	0.09376	0.07208	0.33927
9	0.20227	0.12268	0.13605	0.12539	0.12714	0.09892	0.12871	0.37153	0.18329	0.23406
10	0.05990	0.09211	0.26231	0.14562	0.06537	0.10973	0.13763	0.10312	0.09600	0.24257
11	0.05328	0.27311	0.07772	0.07788	0.09454	0.05960	0.19647	0.13932	0.10510	0.10647
12	0.06405	0.08020	0.08641	0.04997	0.07654	0.05581	0.05375	0.12706	0.12238	0.06261
13	0.00455	0.00175	0.00562	0.00450	0.00614	0.00435	0.03679	0.07159	0.07367	0.08449
14	0.15454	0.10602	0.04006	0.04248	0.09738	0.08749	0.17037	0.04714	0.15708	0.06744
15	0.34034	0.11576	0.15540	0.20208	0.12020	0.19276	0.21177	0.16194	0.18695	0.12542
16	0.07426	0.07985	0.09160	0.09342	0.10442	0.07468	0.04132	0.03102	0.03241	0.02455
17	0.08037	0.06839	0.05783	0.05390	0.05014	0.05256	0.00796	0.01229	0.01019	0.01082
18	0.02587	0.01392	0.01132	0.01750	0.00148	0.01481	0.00101	0.00204	0.00144	0.00189

Tabla. 3.56. Intensidad de tráfico telefónico hacia y desde las bodegas

	BODEGAS									
	DIAS									
Horas	Lunes 5	Martes 6	Miercl. 7	Jueves 8	Viernes 9	Lunes 12	Martes 13	Miercl 14	Jueves 15	Viernes 16
8	0.02058	0.09172	0.09844	0.05963	0.02720	0.03362	0.05186	0.02911	0.01968	0.03764
9	0.03024	0.06892	0.04108	0.06478	0.14172	0.07723	0.13662	0.09698	0.03987	0.03664
10	0.03178	0.03840	0.07816	0.10549	0.03469	0.07552	0.05947	0.16112	0.04416	0.05840
11	0.05466	0.04632	0.05512	0.04132	0.06650	0.04385	0.07845	0.05004	0.22792	0.03984
12	0.04509	0.05292	0.07230	0.02651	0.04491	0.02961	0.05685	0.07576	0.03059	0.04526
13	0.00241	0.00093	0.00298	0.00239	0.00326	0.00231	0.01952	0.03705	0.05995	0.01580
14	0.01597	0.01793	0.03008	0.01237	0.01541	0.02216	0.17847	0.02501	0.13705	0.03578
15	0.09934	0.06142	0.16984	0.22915	0.12044	0.19779	0.07538	0.04451	0.10581	0.16803
16	0.06108	0.04372	0.14471	0.03984	0.05540	0.05462	0.02192	0.01646	0.03637	0.01302
17	0.04264	0.01992	0.03068	0.02860	0.02660	0.02789	0.00422	0.00652	0.00541	0.00574
18	0.01373	0.00739	0.00601	0.00929	0.00079	0.00786	0.00054	0.00108	0.00076	0.00100

Tabla. 3.57. Intensidad de tráfico telefónico hacia y desde tránsito

	TRÁNSITO									
	DIAS									
Horas	Lunes 5	Martes 6	Miercls 7	Jueves 8	Viernes 9	Lunes 12	Martes 13	Miercls 14	Jueves 15	Viernes 16
8	0.01882	0.01326	0.02422	0.10290	0.18403	0.01195	0.02104	0.11134	0.03716	0.02121
9	0.04848	0.06966	0.03757	0.04628	0.05669	0.03969	0.06596	0.21147	0.12853	0.03351
10	0.02906	0.04845	0.05415	0.05353	0.08922	0.05001	0.06651	0.13981	0.04038	0.06673
11	0.02585	0.03372	0.18882	0.03779	0.02649	0.05142	0.11760	0.21520	0.03671	0.03643
12	0.03107	0.02045	0.03182	0.02424	0.03040	0.05069	0.02608	0.08133	0.02797	0.02310
13	0.00221	0.00085	0.00272	0.00218	0.00298	0.00211	0.03452	0.01991	0.01849	0.01444
14	0.01460	0.01640	0.01633	0.09742	0.01409	0.01579	0.18100	0.02287	0.02473	0.03272
15	0.03749	0.09033	0.23318	0.05465	0.05832	0.04217	0.04903	0.19153	0.03728	0.04697
16	0.02969	0.02931	0.04444	0.22337	0.05066	0.05179	0.02005	0.01505	0.01573	0.01691
17	0.03899	0.01822	0.02806	0.09004	0.02432	0.02550	0.00386	0.00596	0.00494	0.00525
18	0.01255	0.00675	0.00549	0.00849	0.00072	0.00747	0.00049	0.00099	0.00070	0.00092

Tabla. 3.58. Intensidad de tráfico telefónico hacia y desde el hospital

	HOSPITAL									
	DIAS									
Horas	Lunes 5	Martes 6	Miercls 7	Jueves 8	Viernes 9	Lunes 12	Martes 13	Miercls 14	Jueves 15	Viernes 16
8	0.01796	0.01266	0.27012	0.02610	0.02374	0.06613	0.01690	0.07041	0.01717	0.12108
9	0.07750	0.05479	0.03586	0.09168	0.06658	0.02304	0.03220	0.03348	0.02776	0.03198
10	0.02774	0.25630	0.06332	0.05415	0.03027	0.07051	0.03299	0.04171	0.11548	0.07819
11	0.02467	0.18163	0.06432	0.08273	0.11637	0.02760	0.02846	0.04368	0.08115	0.03477
12	0.02966	0.01952	0.03037	0.02620	0.06124	0.05140	0.02489	0.05734	0.07948	0.02205
13	0.00211	0.00081	0.00260	0.00208	0.00284	0.00202	0.01704	0.01900	0.01765	0.05934
14	0.01394	0.01565	0.01559	0.01080	0.04568	0.00552	0.03091	0.03378	0.15610	0.03123
15	0.03579	0.05361	0.07639	0.07966	0.26566	0.05164	0.07355	0.09885	0.03319	0.22233
16	0.02834	0.07798	0.04908	0.03477	0.04835	0.03458	0.01913	0.01437	0.01501	0.04109
17	0.03722	0.01739	0.02678	0.02496	0.02322	0.02434	0.00368	0.00569	0.00472	0.00501
18	0.01198	0.00645	0.00524	0.00811	0.00069	0.00686	0.00047	0.00094	0.00067	0.00088

Tabla. 3.59. Intensidad de tráfico telefónico hacia y desde el camal

	CAMAL									
	DIAS									
Horas	**Lunes 5**	**Martes 6**	**Miercls 7**	**Jueves 8**	**Viernes 9**	**Lunes 12**	**Martes 13**	**Miercls 14**	**Jueves 15**	**Viernes 16**
8	0.00584	0.05051	0.00752	0.00849	0.00772	0.00371	0.00550	0.09882	0.01087	0.00659
9	0.00859	0.00861	0.01167	0.01437	0.01208	0.00750	0.01048	0.01089	0.05070	0.01041
10	0.00903	0.01091	0.01328	0.13147	0.00985	0.01553	0.01073	0.01357	0.06032	0.01658
11	0.00803	0.01047	0.01171	0.01173	0.00650	0.02454	0.01982	0.01421	0.01140	0.03576
12	0.00965	0.00635	0.00988	0.00864	0.00944	0.11202	0.00810	0.06187	0.00869	0.00717
13	0.00069	0.00026	0.00085	0.00068	0.00092	0.00066	0.00554	0.00618	0.07880	0.00449
14	0.00453	0.00509	0.00507	0.00351	0.00438	0.00180	0.01006	0.01516	0.05129	0.01016
15	0.01164	0.01744	0.01329	0.01697	0.01811	0.01310	0.01462	0.01264	0.01080	0.01459
16	0.00922	0.02160	0.03408	0.01131	0.01573	0.01125	0.00623	0.00467	0.00488	0.00370
17	0.01211	0.00566	0.00871	0.00812	0.00755	0.00792	0.00120	0.00185	0.00154	0.00163
18	0.00390	0.00210	0.00171	0.00264	0.00022	0.00223	0.00015	0.00031	0.00022	0.00029

Tabla. 3.60. Intensidad de tráfico telefónico hacia y desde el mercado mayorista

	MERCADO MAYORISTA									
	DIAS									
Horas	**Lunes 5**	**Martes 6**	**Miercls 7**	**Jueves 8**	**Viernes 9**	**Lunes 12**	**Martes 13**	**Miercls 14**	**Jueves 15**	**Viernes 16**
8	0.00381	0.00268	0.05046	0.06915	0.00503	0.00242	0.00358	0.04622	0.00364	0.00429
9	0.00560	0.00561	0.05094	0.08527	0.00788	0.00489	0.00683	0.02377	0.00589	0.00678
10	0.02422	0.00711	0.00866	0.04084	0.00642	0.01012	0.01672	0.00885	0.00817	0.01081
11	0.00523	0.00683	0.00763	0.00765	0.00424	0.01308	0.00604	0.00926	0.00743	0.00738
12	0.07268	0.00414	0.00644	0.02241	0.00615	0.00548	0.00528	0.02678	0.00566	0.00468
13	0.00045	0.00017	0.00055	0.00044	0.00060	0.00043	0.00361	0.00403	0.00374	0.00292
14	0.00296	0.00332	0.00331	0.01423	0.00285	0.00117	0.01767	0.00463	0.00501	0.00662
15	0.00759	0.01137	0.00866	0.01106	0.01181	0.00854	0.00953	0.00824	0.00704	0.00951
16	0.00601	0.00593	0.00900	0.00738	0.01026	0.00734	0.00406	0.00305	0.00318	0.00241
17	0.00789	0.00369	0.00568	0.00529	0.00492	0.00516	0.00078	0.00121	0.00100	0.00106
18	0.00254	0.00137	0.00111	0.00172	0.00015	0.00146	0.00010	0.00020	0.00014	0.00019

El número de circuitos a usarse se determina a través de las tablas de Erlang B (el tipo de tabla viene determinada por la función de distribución de llamadas considerada, en este caso gaussiana), las cuales para una intensidad de tráfico y un grado de servicio

(posibilidad de que una llamada falle debido a congestión del sistema, tradicionalmente 1% en telefonía) dados, proporciona el número de circuitos óptimo.

Con un grado de servicio (GoS) de 1%, el valor más alto de intensidad de tráfico en la hora pico y basados en la tabla de Erlang B, el número de circuitos recomendado se muestra en la siguiente table (ver anexo G; tablas de Erlang B).

Tabla. 3.61. Resumen de análisis de Intensidad de tráfico telefónico

DESTINO	INTENSIDAD DE TRÁFICO EN HORA PICO	NÚMERO DE CIRCUITOS
PSTN	4.6054	11
COMISARIAS	0.44123	3
CULTURA	0.37153	3
HOSPITAL	0.27012	3
TRANSITO	0.23318	3
BODEGAS	0.22915	3
CAMAL	0.13147	2
MERCADO MAYORISTA	0.08527	2

Finalmente cabe aclarar que este análisis considera sólo el tráfico concerniente a la central y deja de lado las 10 líneas directas que funcionan independientemente de la central telefónica.

3.6. OBTENCIÓN DE REQUERIMIENTOS

Con objeto de brindar servicio de voz y datos de manera eficiente a los usuarios de una red, el análisis y obtención de requerimientos es un proceso fundamental. Dependiendo de la organización considerada, las características, necesidades y limitaciones de los usuarios son diferentes, por lo que el diseño de la red siempre debe adaptarse a las mismas.

Para la red municipal el dimensionamiento se lo realizará partiendo de la premisa de un programa de migración gradual hacia telefonía IP, esto principalmente debido a

limitaciones económicas que no posibilitan un cambio total hacia esta tecnología, sin embargo el presente estudio expondrá un sistema que permita al municipio continuar con la migración a medida que las partidas presupuestarias sigan siendo asignadas para dicho efecto, sin encontrar bloqueos técnicos en dicha expansión.

El plan de migración implicará reemplazar completamente la central analógica actualmente existente en la matriz, la cual ha venido provocando muchas molestias, pues por su extendido tiempo de operación sus componentes de hardware comienzan a fallar, y siendo este un equipo descontinuado se dificulta la adquisición de repuestos, además su capacidad de expansión ha llegado a su límite. Por estas razones se instalará una nueva central con tecnología IP en la matriz que además servirá como elemento integrador del sistema para unificar las otras dependencias municipales; en las instalaciones de la matriz se reemplazarán y añadirán cuando sea el caso, las extensiones análogas por extensiones IP, a excepción de considerarse necesario mantener interfaces análogas como máquinas de fax, en cuyo caso será necesario añadir adaptadores análogos a IP en nuestra central.

De este modo en la primera fase de a más del cambio a la nueva central IP en la matriz, se proveerán de extensiones remotas a las dependencias de Comisarias, Mercado Mayorista y Tránsito, que por el momento no cuentan con una infraestructura telefónica, por otro lado las dependencias Hospital, Cultura, Tránsito y Camal, que poseen sus propias centrales telefónicas análogas serán anexadas al sistema a través de troncales IP y un conversor análogo IP en cada dependencia que realizará la transformación necesaria para poderse conectar a las interfaces para troncales análogas disponibles de cada una de dichas centrales.

Para la Ilustre Municipalidad de Ambato desde donde se ejercen las funciones de gobierno seccional de la cuidad, se buscará determinar los parámetros a utilizarse para la obtención de requerimientos, tales como:

- Determinación de usuarios que acceden al servicio telefónico
- Número de troncales
- Selección de Codec

3.6.1. DETERMINACIÓN DE USUARIOS QUE ACCEDEN AL SERVICIO TELEFÓNICO

Determinación de usuarios que acceden al servicio telefónico de la Matriz

El sistema telefónico actual no presta servicio a la mayoría de usuarios de la matriz, considerándose como usuarios, las personas que aquí trabajan y pasan la mayor parte del día en la misma, por lo cual necesitan acceder al servicio telefónico.

Actualmente la central telefónica, con las 61extensiones activas no brinda cobertura a todos los usuarios, razón por la cual, el número de extensiones destinadas para dar el acceso al servicio telefónico, se realizará en base al número de ambientes físicos en cada una de las oficinas y departamentos que funcionan en el edificio matriz.

Se consideran ambientes físicos las oficinas, módulos de trabajo, y salas de reuniones; para cada uno se dispondrá de una extensión, independientemente del número de personas que trabajen en dicho ambiente. Sin embargo dependiendo de la situación del lugar, la asignación de extensiones cambiará, existiendo sitios o ambientes sin extensión propia por ser poco necesario o por tener un acceso al servicio en las proximidades inmediatas.

A continuación en las Tablas 3.62, 3.63, 3.64, 3.65, exponen la nueva distribución que tendría la red telefónica de la matriz.

Para localizar los puntos de red cada departamento en las diferentes plantas de la Matriz del Municipaio hacer referencia a los Anexos B, C, D, E.

Tabla. 3.62. Requerimientos de la planta baja

PRIMERA PLANTA BAJA					
DEPARTAMENTO	**Ambientes Físicos**	**Extensiones propuestas**	**Pts de red**	**Función**	**Equipo**
ARCHIVO	3	2	VZ-14 VZ-15	Archivo Secretaría	IP-E IP-N
PLAN ESTRATÉGICO	3	3	VZ-16 VZ-17 VZ-18	Director Secretaría P. Estratégico	IP-E IP-N IP-N
PROVEEDURÍA	2	2	VZ-09 VZ-10	Proveedora Secretaría	IP-E IP-N
TALLERES OO.PP.	3	1	VZ-8	Taller OO.PP.	IP-N
TESORERÍA	8	7	VZ-02	Tesorero	IP-E

			VZ-03 DT-02 VZ-01 DT-62 DT-19 DT20	Secretaría Tesorería 1 Tesorería 2 Tesorería 3 Tesorería 4 Tesorería 5	IP-N IP-N IP-N IP-N IP-N IP-N
SIMERT	1	1	NUEVO	SIMERT	IP-N
BALCÓN DE SERVICIOS	4	4	DT33 DT29 DT28 DT24	B. Servicios 1 B. Servicios 2 B. Servicios 3 B. Servicios 4	IP-N IP-N IP-N IP-N
INFORMACIÓN	1	2	DT-60 VZ-11	Información Fax Información	OP. FX
PATRONATO MUNICIPAL	2	2	VZ-05 VZ-04	Patronato Secretaría	IP-E IP-N
SALA DE REUNIONES	1	1	VZ-06	Sala de reuniones	IP-N
SALA DE COMISIONES	4	2	VZ-07 NUEVO	Sala de comisi. 1 Sala de comisi. 2	IP-N CF.
SALA DE CONS. CANTONAL	1	1	DT-56	Sala de Consejo	CF
TOTALES	**33**	**28**			

Tabla. 3.63. Requerimientos de la primera planta alta

PRIMERA PLANTA ALTA					
DEPARTAMENTO	**Ambientes Físicos**	**Extensiones propuestas**	**Pts de red**	**Función**	**Equipo**
VICEALCALDÍA	3	3	VZ-07 VZ-08 VZ-09	Vicealcalde Secretaría 1 Secretaría 2	IP-E IP-N IP-N
INFORMÁTICA	4	3	VZ-12 VZ-10 VZ-28	Director Secretaría Desarrollo	IP-E IP-N IP-N
ALCALDÍA	2	2	VZ-15 VZ-14	Alcalde Fax-Alcaldía	IP-E FX
COORDINACIÓN ALCALDÍA	1	1	VZ-29	Coord. Alcaldía	IP-E
SECRETARÍA ALCALDÍA	3	3	VZ-27 VZ-17 VZ-18	Secretario Alc. Secretaría Alc. 1 Secretaría Alc. 2	IP-E IP-N IP-N
SALA DE PRENSA Y TRABAJO	2	1	VZ-19	Sala de Prensa	IP-N
SECRETARÍA GENERAL	1	1	VZ-21	Secretario General	IP-N
PRO- SECRETARÍA	5	4	VZ-26 VZ-25 VZ-23 VZ-22	Pro secretario Pro secretaría 1 Pro secretaría 2 Fax Pro secretaría	IP-E IP-N IP-N FX
AUDITORÍA	2	2	VZ-01 VZ-02	Auditor Auditoría 1	IP-E IP-N
RR.HH.	4	3	VZ-04 VZ-05 VZ-06	Director RR.HH. 1 RR.HH. 2	IP-E IP-N IP-N
UNIDAD DE COMUNICACIÓN INSTITUCIONAL	3	3	VZ-32 VZ-33 VZ-34	Director Comun. Inst. 1 Comun. Inst. 2	IP-E IP-N IP-N

DIRECCION ADMINISTRATIVA	2	2	VZ-30 VZ-31	Director Administrat. 1	IP-E IP-N
TOTALES	**32**	**28**			

Tabla. 3.64. Requerimientos de la segunda planta alta

SEGUNDA PLANTA ALTA					
DEPARTAMENTO	**Ambientes Físicos**	**Extensiones propuestas**	**Pts de red**	**Función**	**Equipo**
ASESORIA JURÍDICA	6	5	VZ-01 VZ-02 VZ-03 VZ-04 VZ-05	Director Secretaría Abogado Jefe Jurídico 2 Jurídico 3	IP-E IP-N IP-N IP-N IP-N
DIRECCIÓN FINANCIERA	3	3	VZ-06 VZ-08 VZ-07	Director Secretaria Financiero 1	IP-E IP-N IP-N
UNIDAD DE PRESUPUESTOS	5	2	VZ-09 VZ-27	Director Secretario	IP-E IP-N
RENTAS	4	3	VZ-10 VZ-11 VZ-12	Rentas Secretario Rentas 1	IP-E IP-N IP-N
AVALÚOS Y CATASTROS	4	3	VZ-15 VZ-13 VZ-14	Director Secretario Avalúos 1	IP-E IP-N IP-N
SERVICIOS PÚBLICOS	3	2	DT-42 DT-46	Servicios 1 Servicios 2	IP-N IP-N
CARTOGRAFÍA	2	1	VZ-16	Cartografía	IP-N
PLANIFICACIÓN 1	4	3	VZ-19 VZ-18 VZ-17	Director Secretaría Fax Planificación	IP-E IP-N FX
CONTROL URBANO	4	3	VZ-20 VZ-21 VZ-22	Director Secretaría Control U. 1	IP-E IP-N IP-N
CONTABILIDAD	4	2	VZ-27 VZ-28	Contador Secretaría	IP-E IP-N
PLANIFICACIÓN 2	4	4	VZ-26 VZ-24 VZ-25 VZ-26	Progrs. y Proycts. Planificación 2 Planificación 3 Planificación 4	IP-E IP-N IP-N IP-N
TOTALES	**43**	**31**			

Tabla. 3.65. Requerimientos de la tercera planta alta

TERCERA PLANTA ALTA					
DEPARTAMENTO	**Ambientes Físicos**	**Extensiones propuestas**	**Pts de red**	**Función**	**Equipo**
OBRAS PÚBLICAS	14	12	VZ-05 VZ-04 VZ-12 VZ-08 VZ-09	Director Secretaria Archivo Vías Parroquias	IP-E IP-N IP-N IP-N IP-N

			VZ-02	Fax OO.PP.	FX
			VZ-06	OO.PP. 1	IP-N
			VZ-07	OO.PP. 2	IP-N
			VZ-08	OO.PP. 3	IP-N
			VZ-11	OO.PP. 4	IP-N
			VZ-10	OO.PP. 5	IP-N
			VZ-01	OO.PP. 6	IP-N
TOTALES	**14**	**12**			

El criterio de distribución de extensiones por ambiente permite el fácil acceso al servicio telefónico de todas las personas (*al no haber divisiones físicas todos los usuarios pueden realizar o responder llamadas a través de la extensión en igualdad de condiciones*) que trabajan en el sitio, de esta forma se brinda comunicación de voz a un mayor número de usuarios con menos extensiones, optimizándose el uso del sistema en general.

A continuación se resumen los requerimientos de telefonía para la matriz.

Tabla. 3.66. Resumen de requerimientos para la matriz

PLANTA	Teléfonos IP normales	Teléfonos IP ejecutivos	FAX	IP Conferencia	Operadora	TOTAL
PB	19	5	1	2	1	28
P1	16	10	2	0	0	28
P2	21	9	1	0	0	31
P3	10	1	1	0	0	12
TOTAL	66	25	5	2	1	99

Del mismo modo resumimos los puntos de red necesarios en cada planta, para brindar servicio a las extensiones designadas.

Tabla. 3.67. Resumen de puntos de red para las nuevas extensiones de la matriz

PLANTA	PUNTOS DE VOZ	PUNTOS DE DATOS	PUNTOS NUEVOS	TOTAL
PB	16	10	2	28
P1	28	0	0	28
P2	29	2	0	31
P3	12	0	0	12
TOTAL	85	12	2	99

Como podemos observar la mayor parte de los puntos de red utilizan aquellos designados en el cableado estructurado como puntos de voz “VZ-XX”, que actualmente se encuentran disponibles en algunos casos y en otros brindando servicio a las extensiones

analógicas, que serán removidas, por lo cual no presentan inconvenientes para la nueva implementación, sin embargo se requiere utilizar 12 puntos de datos designados en el cableado estructurado como "DT-XX", que están actualmente siendo utilizados, además de dos nuevos puntos de voz que se requieren en la planta baja, en el departamento de SIMERT, y en la sala de comisiones, estos requerimientos serán solventados en el rediseño de la red.

Determinación de usuarios que acceden al servicio telefónico de las Comisarías

El edificio de las comisarías como se explicó anteriormente no cuenta con una infraestructura telefónica, simplemente cuenta con 5 líneas analógicas conectadas directamente desde la acometida de Andinatel hasta los puestos de trabajo distribuidos en su planta baja y dos plantas altas, por lo tanto no presta servicio a la mayoría de usuarios.

Por este motivo se plantea integrar a esta dependencia la siguiente cantidad de extensiones IP distribuidas entre las diferentes plantas así.

Tabla. 3.68. Requerimientos de las comisarías

PLANTA	Ambientes Físicos	Extensiones propuestas	Función	Equipo
PLANTA BAJA	6	5	Atención al Público	IP-E IP-N IP-N IP-N IP-N
PRIMERA PLANTA ALTA	9	7	Servicios Públicos	IP-E IP-E IP-N IP-N IP-N IP-N FX
SEGUNDA PLANTA ALTA	8	6	Dirección de Higiene	IP-E IP-N IP-N IP-N IP-N IP-N
TOTALES	**23**	**18**		

A continuación se resumen los requerimientos de telefonía para las comisarías.

Tabla. 3.69. Resumen de requerimientos para las comisarías

PLANTA	Teléfonos IP normales	Teléfonos IP ejecutivos	FAX	TOTAL
PB	4	1	0	5
P1	4	2	1	7
P2	5	1	0	6
TOTAL	13	4	1	18

Los puntos de red en este edificio solamente están distribuidos para datos, los teléfonos IP se conectarán a dichos puntos y deberán tener dos puertos para permitir conectar en el otro puerto el host asociado, a cada puesto de trabajo, que sea equipado con telefonía, además deberá dejarse una de las líneas analógicas de Andinatel para que se pueda conectar una máquina de fax, y para que sirva también como backup en caso de que la red WAN no funcione.

Determinación de usuarios que acceden al servicio telefónico del Mercado Mayorista

El edificio administrativo del mercado mayorista cuenta solamente con 1 líneas analógicas desde la acometida de Andinatel y conectada en paralelo hasta algunos de los puestos de trabajo distribuidos en su única planta.

Por este motivo se plantea integrar a esta dependencia la siguiente cantidad de extensiones IP.

Tabla. 3.70. Requerimientos del mercado mayorista

DEPENDENCIA	Ambientes Físicos	Extensiones propuestas	Función	Equipo
Mercado Mayorista	6	6	Mercado Mayorista	IP-E IP-N IP-N IP-N IP-N FX
TOTALES	**6**	**6**		

Debido a que solamente existe cableado para datos en este edificio, los teléfonos IP deberán estar equipados con dos puertos para permitir conectar en el otro puerto el host asociado, a cada puesto de trabajo, que sea equipado con telefonía, además deberá dejarse

la línea analógica de Andinatel para que se pueda conectar una máquina de fax, y para que sirva también como backup en caso de que la red WAN no funcione.

Determinación de usuarios que acceden al servicio telefónico de las Bodegas

El edificio administrativo de las bodegas municipales cuenta solamente con 1 líneas analógicas desde la acometida de Andinatel y conectada en paralelo hasta algunos de los puestos de trabajo distribuidos en su única planta.

Por este motivo se plantea integrar a esta dependencia la siguiente cantidad de extensiones IP.

Tabla. 3.71. Requerimientos de las bodegas

DEPENDENCIA	Ambientes Físicos	Extensiones propuestas	Función	Equipo
Bodegas	4	3	Bodegas	IP-E IP-N FX
TOTALES	**4**	**3**		

Debido a que solamente existe cableado para datos en este edificio, los teléfonos IP deberán estar equipados con dos puertos para permitir conectar en el otro puerto el host asociado, a cada puesto de trabajo, que sea equipado con telefonía, además deberá dejarse la línea analógica de Andinatel para que se pueda conectar una máquina de fax, y para que sirva también como backup en caso de que la red WAN no funcione.

A continuación se presentan los requerimientos totales de extensiones, de la matriz y comisarias, bodegas y mercado mayorista.

Tabla. 3.72. Resumen total de requerimientos

DEPENDENCIA	Teléfonos IP normales	Teléfonos IP ejecutivos	FAX	IP Conferencia	Operadora	TOTAL
MATRIZ	66	25	5	2	1	99
COMISARÍAS	13	4	1	0	0	18
MERCADO MAYORISTA	4	1	1	0	0	6
BODEGAS	1	1	1	0	0	3
TOTAL	84	31	8	2	1	126
TOTAL DE EXTENSIONES QUE DEBE MANEJAR LA NUEVA CENTRAL						123

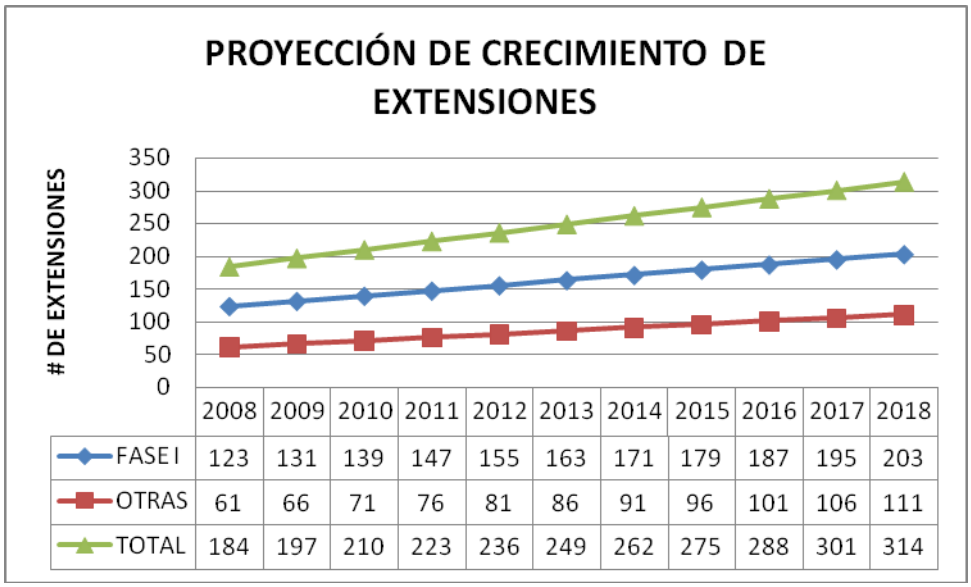
Hay que destacar que las tres máquinas de fax que no están en la matriz, no serán conectadas a la nueva central IP sino que se comunicarán a través de las troncales analógicas de Andinatel, por lo cual la nueva central IP deberá manejar 123 extensiones.

Proyecciones Futuras

Es importante dimensionar las expectativas futuras de crecimiento, pues de este modo al momento de especificar la nueva central nos aseguraremos que la misma este en capacidad de solventar las necesidades que pueden surgir con el paso del tiempo, esta proyección se la realiza considerando una primera fase que es la que cubre el presente estudio y fases posteriores que se pueden dar a futuro para completar un camino hacia la convergencia total a telefonía IP.

De acuerdo a datos obtenidos de registros anuales de la central telefónica, el incremento de extensiones en la matriz se comporta de forma lineal, obteniendo un aumento constante anual de 5 extensiones, a ello aumentaremos 3 extensiones por las dependencias anexadas a la nueva central en la primera fase que serán comisarias, mercado mayorista y bodegas, de este modo el nuevo sistema telefónico estará en capacidad de manejar 123 extensiones y llegará a requerir de 203 extensiones en el año 2018.

Para las dependencias que actualmente poseen una central telefónica analógica, se proyectará reemplazarlas por extensiones remotas IP que estarán anexadas a la nueva central telefónica, por ello es importante considerar dicho cambio actualmente el hospital posee 41 extensiones, cultura 8, tránsito 6 y camal 6, es decir actualmente se requerirían 61 extensiones, y se proyectará un incremento de 5 extensiones anuales entre todos los departamentos, con lo cual al 2018 se requerirá de 111 extensiones, lo dicho se muestra a continuación en la siguiente figura.



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
FASE I	123	131	139	147	155	163	171	179	187	195	203
OTRAS	61	66	71	76	81	86	91	96	101	106	111
TOTAL	184	197	210	223	236	249	262	275	288	301	314

Figura. 3.85. Proyección de crecimiento anual de extensiones

3.6.2. DETERMINACIÓN DEL NÚMERO DE TRONCALES

Número de troncales para interacción con las redes públicas

A través del análisis de tráfico telefónico se obtuvo que para las 61 extensiones actuales del servicio, la intensidad de tráfico pico obtenida para comunicarse desde y hacia la PSTN fue de 4,6054 Erlangs. Considerando que el comportamiento de los nuevos usuarios sea similar al de los actuales, se puede admitir una variación lineal de la intensidad de tráfico en función del número de beneficiarios del servicio; considerado esto se obtiene las proyecciones de tráfico para las 123 extensiones propuestas:

$$A_1 = U_f \ A_0 / U_a$$

Donde:

- A_1= Intensidad de tráfico proyectada
- A_0= Intensidad de tráfico actual
- U_f = Usuarios finales
- U_a = Usuarios actuales

La siguiente tabla, muestra las troncales analógicas necesarias para la implementación de la Fase I, mediante el análisis de Erlang B con un grado de servicio del 1%, en base a la intensidad de tráfico proyectado a través de la ecuación lineal expuesta.

Tabla. 3.73. Proyección de líneas troncales analógicas para la fase I

U_a = 61 extensiones, A_0=4,6054 Erlangs, GoS = 1%			
Situación	**# de extensiones [Uf]**	**Intensidad de tráfico $A_1 = U_f A_0 / U_a$**	**Número de troncales Analógicas requeridas**
2008	123	9.2863	17
2013	163	12.3062	21
2018	203	15.3262	25

A continuación observaremos la misma proyección considerando una implementación completa que se realizaría en fases posteriores.

Tabla. 3.74. Proyección de líneas troncales analógicas para fases futuras

U_a = 61 extensiones, A_0=4,6054 Erlangs, GoS = 1%			
Situación	**# de extensiones [Uf]**	**Intensidad de tráfico $A_1 = U_f A_0 / U_a$**	**Número de troncales Analógicas requeridas**
2008	184	13.8917	23
2013	249	18.7991	29
2018	314	23.7065	34

Inicialmente el sistema requerirá de 17 troncales, en el caso de disponer de troncales analógicas en su totalidad, implicaría adicionar hardware para la conexión de cada uno de los pares telefónicos al sistema; por estas razones y por proyecciones de crecimiento, que concebirán un sistema totalmente centralizado, eliminando las centrales analógicas de las otras dependencias y por ende las líneas troncales asociadas a ellas, de modo que todo el tráfico hacia la PSTN se curse por la nueva central telefónica IP que estará en la matriz, lo cual sumará considerablemente el número de troncales necesarias para dicho fin. Es por ello que las troncales necesarias para el acceso hacia la PSTN serán del tipo digital, siendo las alternativas prestadas por Andinatel, las siguientes (exceptuando el acceso básico BRI ($2B + D$) por brindar solo dos canales de comunicación).

- Un acceso PRI ($30B + D$) con señalización ISDN (*Recomendación Q.931*) disponiendo de 100 números telefónicos por acceso primario y 30 llamadas simultáneas en total.

- Un E1 con señalización R2, disponiendo de 100 números telefónicos por E1 y 30 llamadas simultáneas en total.

El uso de enlaces digitales, permite flexibilidad del uso de troncales y servicios suplementarios prestados por los mismos. Cuando se realiza o se contesta una llamada a través de un acceso E1 ya sea con R2 o ISDN, la comunicación utiliza un canal de los 30 disponibles, permitiendo 29 comunicaciones más, de salida o entrada mediante cualquiera de los 100 números telefónicos. Al igual que con troncales analógicas es permitido crear grupos de enlace, solo que en este caso se asocia canales del E1 en lugar de troncales.

El E1 permite tener un máximo de 30 comunicaciones simultáneas a través de un solo número telefónico generalmente el de cabecera *(primer número en la serie de los 100 entregados)*, gracias a que cada una de las llamadas ocupa un canal distinto del enlace. Esta opción es aprovechada para la asignación de líneas de entrada para una operadora, ya que puede atender un número definido de llamadas a través de un solo número telefónico; claro está que la cantidad de llamadas a ser atendidas también depende de los recursos de *hardware* del teléfono operadora.

El E1 por defecto tiene la opción de realizar DID (*Discado Interno Directo*), es decir se puede conmutar un canal del E1 directamente a una extensión telefónica asociada a uno de los 100 números telefónicos. En síntesis, cuando se llame a un número telefónico programado con DID, timbrará directamente en la extensión designada sin pasar por la operadora. La configuración de esta opción es exclusiva en los equipos del cliente.

Tabla. 3.75. Costo de línea de acceso a la PSTN

Concepto	Inscripción (USD)	Pensión Básica(USD)
RDSI Primario (ISDN-PRI)	$ 2250	$ 225
E1-R2	$ 4000	$ 500
RDSI Básico (ISDN-BRI)	$ 150	$ 15
Línea urbana comercial	$60	$12,06

La tabla 3.75 describe los costos por inscripción y pensiones básicas mensuales de las opciones consideradas para las troncales, tanto el acceso ISDN-PRI como el E1-R2 prestan las mismas funcionalidades; sin embargo su costo varía considerablemente debido a que los E1-R2 funcionan bajo la red antigua de Andinatel siendo su mantenimiento oneroso, mientras que RDSI está diseñada para integrar voz, datos y video utilizando la

infraestructura telefónica. Por tales motivos el enlace hacia la PSTN se realizará a través de un acceso PRI.

Número de canales de voz IP para interacción entre dependencias

En el presente análisis se busca determinar los canales de voz IP, que cursarán a través de la red WAN desde otras dependencias hasta la matriz y viceversa, para lo cual usaremos el análisis de tráfico telefónico, que determinó la intensidad de tráfico pico obtenida para comunicarse desde y hacia otras dependencias por las 61 extensiones con las que cuenta la matriz actualmente lo cual se refleja en la Tabla 3.61. Para ello se usará el mismo criterio aplicado para determinar el número de troncales que interactúan con la PSTN.

Tabla. 3.76. Intensidad de tráfico de voz entre dependencias

Ua = 61 extensiones, Uf=99 extensiones, GoS = 1%		
Dependencia	**Intensidad de tráfico para 61 ext [Ao]**	**Intensidad de tráfico 99 ext $A_1 = U_f A_0 / U_a$**
COMISARIAS	0.44123	0.71609
CULTURA	0.37153	0.60297
HOSPITAL	0.27012	0.43839
TRANSITO	0.23318	0.37843
BODEGAS	0.22915	0.37189
CAMAL	0.13147	0.21336
MERCADO MAYORISTA	0.08527	0.13838

Es necesario también analizar que por el cambio de arquitectura que sufrirá la red voz, el tráfico hacia la PSTN que generen las Comisarías, Mercado Mayorista y Bodegas, deberá primero ser transportado vía IP hasta la matriz donde se ubicará la nueva central que se encargará finalmente de conectar dicha comunicación con la PSTN, esto implica la ocupación de un canal IP durante todo el tiempo que dure la comunicación entre la matriz y la dependencia desde donde se generó dicho tráfico. Para ello utilizaremos como referencia el comportamiento de tráfico hacia la PSTN de la matriz.

Tabla. 3.77. Intensidad de tráfico de voz de otras dependencias hacia la PSTN

U_a = 61 extensiones, A_0=4,6054 Erlangs, GoS = 1%		
Dependencia	**# de extensiones [Uf]**	**Intensidad de tráfico $A_1 = U_f A_0 / U_a$**
COMISARIAS	17	1.28347
MERCADO MAYORISTA	5	0.37749
BODEGAS	2	0.15099

Una vez determinadas las intensidades de tráfico para cada dependencia, las sumamos para obtener los canales de voz IP, que circularán por la WAN.

Tabla. 3.78. Número de canales de voz IP sobre la WAN

GoS = 1%		
Dependencia	**Intensidad de tráfico total**	**Número De Canales De Voz IP**
COMISARIAS	1.99956	7
CULTURA	0.60297	4
HOSPITAL	0.43839	3
TRANSITO	0.37844	3
BODEGAS	0.52289	4
CAMAL	0.21337	3
MERCADO MAYORISTA	0.51588	4

3.6.3. SELECCIÓN DEL CÓDEC

Los equipos de un sistema telefónico IP, independientemente de la tecnología empleada en el diseño de la red integrada de voz y datos, usan por defecto el codec G.711 para telefonía IP en un entorno LAN que es en el cual trabajarán las extensiones internas de la matriz, proporcionando la más alta calidad de voz. Los codecs de menor tasa de bits son empleados generalmente para conexiones WAN donde el ancho de banda es limitado y se requiere de compresión, estos codecs tomar importancia cuando se analicen las troncales IP y extensiones remotas que conectarán las otras dependencias y se comunicaran a través de la red WAN municipal.

En el entorno de una red integrada de voz y datos, la selección del codec es un parámetro de importancia pues posee alta influencia en la calidad que presenta el sistema

de ToIP hacia el usuario final; como se pudo analizar en el capítulo 1, tomando como referencia la Tabla 1.5 Resumen de codecs y la Tabla 1.7 Anchos de banda de codecs vamos a seleccionar el códec G.711 para comunicaciones internas en la matriz, y el códec G.729 para comunicaciones que atraviesan la WAN. A continuación se resumen las características de los codecs seleccionados.

Tabla. 3.79. Codificadores seleccionados

Códec	Tipo de codificación	Tasa binaria	Complejidad (MIPS)	Retardo codificador (ms)	Calidad (MOS)	Ancho de Banda en Ethernet
G.711	PCM	64 kbps	0.1	0.125	4.2	87.7 kbps
G.729	CS-ACELP	8 kbps	22	15	4.0	28.8 kbps

CAPÍTULO IV:

4. RECOMENDACIONES PARA EL REDISEÑO DE LA RED DE DATOS

Las consideraciones de diseño se enfocarán a concebir una red integrada que sirva como medio de comunicación a través del cual circulen eficientemente los flujos de voz y datos asegurando calidad de servicio y disponibilidad sobre dicho medio, lo cual, permitirá facilitar las tareas diarias de los funcionarios municipales.

4.1. SERVICIOS PROPUESTOS PARA LA RED DE COMUNICACIONES

De acuerdo a los alcances planteados para la red de comunicaciones Municipal, el diseño que se realizará brindará los siguientes servicios con los que deberá contar cada una de las secciones que forman parte de su infraestructura:

- Servicios de transmisión de datos
- Telefonía sobre IP

4.1.1. SERVICIOS DE TRANSMISIÓN DE DATOS

La transmisión de datos no es nada más que el intercambio de información entre dispositivos como documentos o bases de datos y recursos físicos, como impresoras o unidades de disco, a través de algún medio físico de transmisión.

4.1.2. TELEFONÍA SOBRE IP

Telefonía sobre el Protocolo de Internet, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP. Esto significa que

se envía la señal de voz en forma digital en paquetes en lugar de enviarla en forma de circuitos como una compañía telefónica convencional o PSTN.

El tráfico de Telefonía sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo redes de área local (LAN).

Las características más importantes de ToIP, y que a diferencia de los servicios de comunicación de voz convencionales son las siguientes:

• Las llamadas telefónicas entre dependencias pueden ser automáticamente enrutadas a teléfonos IP, sin importar en donde estén geográficamente conectados a la red, lo cual implica una reducción de costos en las planillas telefónicas pues no se requiere atravesar la PSTN.

• Optimiza el uso de la capacidad del canal disponible.

• El tamaño de los equipos disminuye en relación al equipamiento TDM, debido a que los equipos IP requieren de un solo puerto para enviar y recibir las comunicaciones de varias extensiones IP, en tanto que los equipos TDM requieren reservar un número de puertos para las extensiones telefónicas.

• Coexiste con los demás servicios que se presentan simultáneamente en la misma red; para lo cual, los equipos deben manejar priorización de tráfico y calidad de servicio.

• Los teléfonos IP pueden integrarse con otros servicios disponibles en Internet, incluyendo videoconferencias, intercambio de datos y mensajes con otros servicios en paralelo con la conversación, audio conferencias, administración de libros de direcciones e intercambio de información.

• En las llamadas a través de la PSTN se consume ancho de banda, inclusive en los momentos de silencio de la conversación; en la telefonía IP, la voz es procesada de tal manera que se puede detectar los momentos de silencio, para de ésta forma no procesarlos ni transmitirlos, optimizando así el uso del ancho de banda.

4.2. DIMENSIONAMIENTO DE TRÁFICO

Para realizar el dimensionamiento de tráfico de la red municipal, se tomará en cuenta los siguientes criterios:

• Dimensionamiento del tráfico por estación de trabajo

• Dimensionamiento del tráfico de voz

4.2.1. DIMENSIONAMIENTO DEL TRÁFICO POR ESTACIÓN DE TRABAJO

Para dimensionar el tráfico de las estaciones de trabajo de la red, tomaremos en cuenta los datos del monitoreo realizado en el capítulo 3, en la Tabla 3.29. observamos el flujo de tráfico de los principales enlaces, a continuación vamos a determinar el tráfico individual de cada estación en función de la cantidad de hosts de cada planta, hay que considerar que el enlace de la planta 3, no solo contiene el flujo de dicha planta sino que además transporta el tráfico de la WAN pues la antena de la misma está conectada en esta planta, por esta razón se debe desglosar este valor, para ello se realizara una estimación del tráfico de las estaciones de trabajo de esta planta como promedio de las otras plantas y la diferencia constituirá entonces el tráfico WAN.

Tabla. 4.1. Dimensionamiento de tráfico por host

		Tráfico total kbps			Tráfico por host kbps		
Enlace	**Host's**	**In**	**Out**	**Total**	**In**	**Out**	**Total**
PB	42	77	310	387	1.83	7.38	9.21
P1	46	176	264	440	3.83	5.74	9.57
P2	83	166	943	1,109	2.00	11.36	13.36
P3	23	59	188	246	2.55	8.16	10.71
WAN	87	46	475	522	0.53	5.46	6.00
Internet	281	502	79	581	1.79	0.28	2.07

4.2.2. DIMENSIONAMIENTO DEL TRÁFICO DE VOZ

Procedemos a calcular el ancho de banda necesario para cada planta de la matriz, utilizando los requerimientos obtenidos en el capítulo III, y de acuerdo a la Tabla. 3.66.

Resumen de requerimientos para la matriz así como a la Tabla. 3.79. Codificadores seleccionados, tenemos lo siguiente:

Tabla. 4.2. Dimensionamiento del tráfico de voz en la matriz

U_a = 61 extensiones, A_0=4,6054 Erlangs, GoS = 1%					
PLANTA	**Extensiones IP**	**Intensidad de tráfico $A_1 = U_f$ A_0 / U_a**	**Canales De Voz IP**	**Ancho de banda (kbps)**	**Total (kbps)**
PB	27	2.0385	7	87.7	614
P1	260	1.9630	7	87.7	614
P2	30	2.2650	7	87.7	614
P3	11	0.8305	5	87.7	439

De la misma forma dimensionamos el tráfico de voz en la red WAN, para cada una de las dependencias municipales, utilizando los requerimientos obtenidos en el capítulo III, y de acuerdo a la Tabla. 3.78. Número de canales de voz IP sobre la WAN, y a la Tabla. 3.79. Codificadores seleccionados.

Tabla. 4.3. Dimensionamiento del tráfico de voz entre dependencias

GoS = 1%				
Dependencia	**Intensidad de tráfico total**	**Canales De Voz IP**	**Ancho de banda (kbps)**	**Total (kbps)**
COMISARIAS	1.99956	7	28.8	202
CULTURA	0.60297	4	28.8	115
HOSPITAL	0.43839	3	28.8	86
TRANSITO	0.37844	3	28.8	86
BODEGAS	0.52289	4	28.8	115
CAMAL	0.21337	3	28.8	86
MERCADO MAYORISTA	0.51588	4	28.8	115
				805

A continuación resumimos el tráfico total que tendrá cada enlace tanto en la matriz como en la WAN municipal.

Tabla. 4.4. Resumen dimensionamiento de tráfico

Enlace	Datos (kbps)	Voz (kbps)	Total (kbps)
PB	387	614	1,001
P1	440	614	1,054
P2	1,109	614	1,723

P3	246	439	685
WAN	522	805	1,327

4.3. DIRECCIONAMIENTO IP

Una dirección IP es el número que identifica de manera lógica y jerárquica la interfaz de un dispositivo dentro de una red que utilice el protocolo IP. La misma puede ser configurada de manera dinámica o fija.

4.3.1. IP FIJA

Una dirección IP fija, es una IP la cual es asignada por el usuario.

Esto permite al usuario montar servidores web, correo, FTP, etc. y dirigir un nombre de dominio a esta IP sin tener que mantener actualizado el servidor DNS cada vez que cambie la IP, como ocurre con las IPs dinámicas.

4.3.2. IP DINÁMICA

Una dirección IP dinámica es una IP la cual es asignada mediante un servidor DHCP (*Dynamic Host Configuration Protocol*) al usuario. La IP que se obtiene, tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.

La asignación de Direcciones IP, dependiendo de la implementación concreta, del servidor DHCP, puede darse por cualquiera de los siguientes métodos:

Manualmente: cuando el servidor tiene a su disposición una tabla que empareja direcciones MAC con direcciones IP, creadas manualmente por el administrador de la red. Sólo clientes con una dirección MAC válida recibirán una dirección IP del servidor.

Automáticamente: donde el servidor DHCP asigna permanentemente una dirección IP libre, tomada de un rango prefijado por el administrador, a cualquier cliente que solicite una.

Dinámicamente: el único método que permite la reutilización de direcciones IP. El administrador de la red asigna un rango de direcciones IP para el DHCP y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

4.3.3. RECOMENDACIÓN DE DIRECCIONAMIENTO

La asignación de direcciones IP se las seguirá realizando a través del servidor DCHP, con el que cuenta la matriz municipal cuya dirección es 10.10.0.6., sin embargo en la nueva implementación se incluirá este servicio para las dependencias municipales que están fuera de la matriz, esto a excepción de los servidores, dirección de administración de equipos de red y aquellos elementos que necesariamente deben tener una asignación de dirección fija.

Con la finalidad de disminuir el impacto en el cambio de direccionamiento se recomienda mantener el esquema sobre una red CLASE A bajo la dirección 10.0.0.0, y con las subredes que se muestran en la siguiente tabla:

Tabla. 4.5. Recomendaciones de direccionamiento

Dependencia	# de Hosts	# de ToIP	Total	Subred	Rango de Direcciones	# Max Dir. IP
MATRIZ	194	0	194	Subnet: 10.10.0.0 Mask: 255.255.254.0	Desde: 10.10.0.1 Hasta: 10.10.1.254	510
TELEFONIA MATRIZ	0	94	94	Subnet: 10.10.2.0 Mask: 255.255.255.0	Desde: 10.10.2.1 Hasta: 10.10.3.254	254
MERCADO MAYORISTA	7	5	12	Subnet: 10.10.3.0 Mask: 255.255.255.0	Desde: 10.10.3.1 Hasta: 10.10.3.254	254
HOSPITAL	10	1	11	Subnet: 10.10.4.0 Mask: 255.255.255.0	Desde: 10.10.4.1 Hasta: 10.10.4.254	254
COMISARIAS	31	17	48	Subnet: 10.10.5.0 Mask: 255.255.255.0	Desde: 10.10.5.1 Hasta: 10.10.5.254	254
CULTURA	15	1	16	Subnet: 10.10.6.0 Mask: 255.255.255.0	Desde: 10.10.6.1 Hasta: 10.10.6.254	254
TRÁNSITO	15	1	16	Subnet: 10.10.8.0 Mask: 255.255.255.0	Desde: 10.10.8.1 Hasta: 10.10.8.254	254
CAMAL	6	1	7	Subnet: 10.10.9.0 Mask: 255.255.255.0	Desde: 10.10.9.1 Hasta: 10.10.9.254	254
BODEGAS	3	2	5	Subnet: 10.10.10.0 Mask: 255.255.255.0	Desde: 10.10.10.1 Hasta: 10.10.2.254	254

De este modo solo se limita a reemplazar la máscara de subred, en comparación al esquema anterior, a excepción del caso del Camal que tenia asociada la subred 10.10.1.0/16, ahora se le asignará la subred 10.10.9.0/24, en similar situación estarían las Bodegas que tenían asignada la subred 10.10.2.0/16, ahora se le asignará la subred 10.10.10.0/24

A continuación se muestra el direccionamiento que seguirá siendo fijo, para la administración de las antenas de la red WAN para cada dependencia.

Tabla. 4.6. Direcciones IP de la red WAN

Dependencia	Equipo	Dirección	Máscara
MATRIZ	M5800S-FSU-D	10.10.0.33	255.255.255.224
MERCADO MAYORISTA	M5800S-FSU-D	10.10.3.1	255.255.255.128
HOSPITAL	M5800S-FSU-D	10.10.4.1	255.255.255.128
COMISARIAS	M5800S-FSU-D	10.10.5.1	255.255.255.128
CULTURA	M5800S-FSU-D	10.10.6.1	255.255.255.128
MACASTO-CAMAL	Access5800 AP	10.10.7.2	255.255.255.0
MACASTO-PRINCIPAL	Access5800 AP	10.10.7.3	255.255.255.0
TRÁNSITO	M5800S-FSU-D	10.10.8.1	255.255.255.128
CAMAL	Access5800 AP	10.10.9.1	255.255.255.128
BODEGAS	M5800S-FSU-D	10.10.10.1	255.255.255.128

El direccionamiento para los servidores debe mantenerse de manera estática, debido a las obvias dificultades que se producirían si continuamente sus direcciones IP cambiaran aleatoriamente por el servidor DHCP.

Tabla. 4.7. Direcciones IP de los servidores y Gateway de voz

Servidor	Dirección	Máscara	Gateway
Correo Electrónico	10.10.0.1	255.255.255.224	10.10.0.11
Internet	10.10.0.2	255.255.255.224	----------
Base de Datos	10.10.0.3	255.255.255.224	10.10.0.11
Telefonía IP	10.10.0.4	255.255.255.224	10.10.0.11
Servicios financieros	10.10.0.5	255.255.255.224	10.10.0.11
Dominio y DCHP	10.10.0.6	255.255.255.224	10.10.0.11
Mapas	10.10.0.7	255.255.255.224	10.10.0.11
Antivirus	10.10.0.8	255.255.255.224	10.10.0.11
Gateway de Voz	10.10.0.9	255.255.255.224	10.10.0.11
Unidad de Tránsito	10.10.8.5	255.255.255.128	10.10.8.2

Como podemos observar el cambio que sufrirán los servidores será su máscara de red, además observamos dos elementos adicionales el servidor de telefonía IP y el Gateway de voz que serán los elementos centrales del sistema de telefonía.

4.4. SEGMENTACIÓN DE LA RED

Una VLAN (Virtual LAN, "Red de Área Local Virtual") es una red de computadoras lógicamente independiente. Varias VLAN´s pueden coexistir en un único *switch* físico. Una VLAN consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo cable, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLAN´s mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLAN´s surge cuando se traslada físicamente una computadora a otra ubicación; puede permanecer en la misma VLAN sin necesidad de ninguna reconfiguración del hardware.

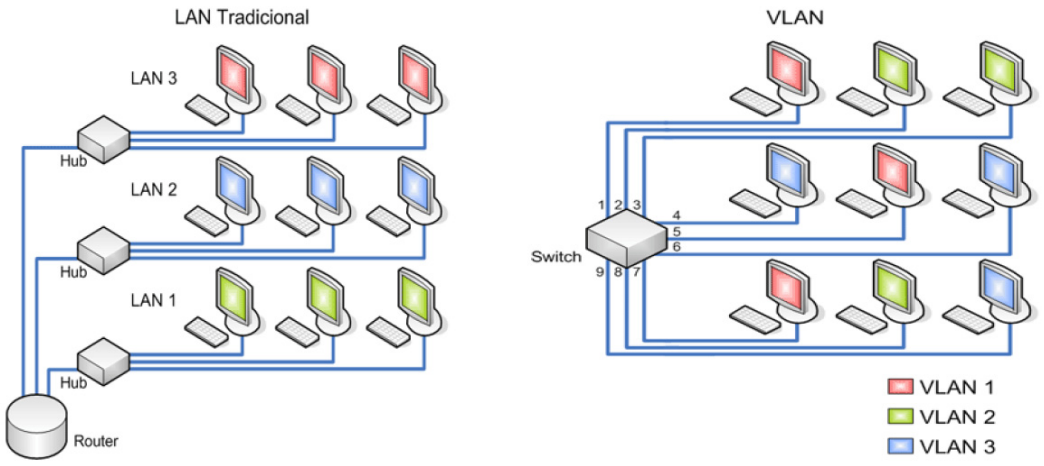


Figura. 4.1. Establecimiento de redes VLAN

El funcionamiento e implementación de las VLAN´s está definido en el estándar IEEE 802.1Q, donde se define que para llevar a cabo ésta comunicación se requerirá de un dispositivo dentro de la LAN, capaz de entender los formatos de los paquetes con que están formadas las VLAN´s. Para poder realizar la comunicación entre equipos asociados a diferentes VLAN´s, se requiere de un equipo de capa 3, mejor conocido como router.

Con los *switches* se crean pequeños dominios, llamados segmentos, conectando un pequeño *Hub* de grupo de trabajo a un puerto de *switch* o bien se aplica micro

segmentación, la cual se realiza conectando cada estación de trabajo y cada servidor directamente a puertos de *switch* teniendo una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

Una de las ventajas que se pueden notar en las VLAN´s es la reducción en el trafico de la red ya que solo se transmiten los paquetes a los dispositivos que estén incluidos dentro del dominio de cada VLAN, una mejor utilización del ancho de banda y confidencialidad respecto a personas ajenas a la VLAN, alta performance, reducción de latencia y facilidad para armar grupos de trabajo.

La comunicación que se hace entre switches para interconectar VLANs utiliza un proceso llamado *Trunking*.

4.4.1. VLAN´s ESTÁTICAS

Los puertos del *switch* están ya pre asignados a las estaciones de trabajo.

Por puerto

Se configura por una cantidad "n" de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN.

Ventajas:

• Facilidad de movimientos y cambios.

• Micro segmentación y reducción del dominio de *Broadcast*.

• Multiprotocolo: la definición de la VLAN es independiente del o los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados, incluso permitiendo el uso de protocolos dinámicos.

Desventajas:

• Administración: un movimiento en las estaciones de trabajo hace necesaria la reconfiguración del puerto del *switch* al que está conectado el usuario, lo cual se puede facilitar combinando con mecanismos de LAN Dinámicas.

Por dirección MAC

Los miembros de la VLAN están especificados en una tabla por su dirección MAC

Ventajas:

• Facilidad de movimientos: no es necesario en caso de que una terminal de trabajo cambie de lugar la reconfiguración del *switch*.

• Multiprotocolo.

• Se puede tener miembros en múltiples VLAN´s.

Desventajas:

• Problemas de rendimiento y control de *Broadcast*: el tráfico de paquetes de tipo *Multicast* y *Broadcast* se propagan por todas las VLANs.

• Complejidad en la administración: en un principio, todos los usuarios deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo. También se puede emplear soluciones de DVLAN.

Por protocolo

Asigna a un protocolo una VLAN. El *switch* se encarga de dependiendo el protocolo por el cual venga la trama, derivarlo a la VLAN correspondiente.

Ventajas:

• Segmentación por protocolo.

• Asignación dinámica.

Desventajas:

• Problemas de rendimiento y control de *Broadcast*: por las búsquedas en tablas de pertenencia se pierde rendimiento en la VLAN.

• No soporta protocolos de nivel 2 ni dinámicos.

Por direcciones IP

Está basado en el encabezado de la capa 3 del modelo OSI. Las direcciones IP a los servidores de VLAN configurados. No actúa como *router*, sino para hacer un mapeo de que direcciones IP están autorizadas a entrar en la red VLAN. No realiza otros procesos con la dirección IP.

Ventajas:

• Facilidad en los cambios de estaciones de trabajo: cada estación de trabajo al tener asignada una dirección IP en forma estática no necesita que se reconfigure el *switch*.

Desventajas:

• El tamaño de los paquetes enviados es menor que en el caso de utilizar direcciones MAC.

• Pérdida de tiempo en la lectura de las tablas.

• Complejidad en la administración: en un principio, todos los usuarios deben configurar de forma manual las direcciones MAC de cada una de las estaciones de trabajo.

Por nombre de usuario

Se basan en la autenticación del usuario y no por las direcciones MAC de los dispositivos.

Ventajas:

• Facilidad de movimiento de los integrantes de la VLAN.

• Multiprotocolo.

Desventajas:

• En corporaciones muy dinámicas la administración de las tablas de usuarios.

4.4.2. VLAN´s DINÁMICAS (DVLAN)

Las VLAN dinámicas son puertos del *switch* que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de éstas VLAN´s se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN el *switch* chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas, y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN. El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones, cuando se cambian de lugar las estaciones de trabajo o se agregan, y también notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

4.4.3. VENTAJAS DE LAS VLANs

Las VLAN proporcionan las siguientes ventajas:

• Reducen los costes administrativos relacionados con la resolución de los problemas asociados con los traslados, adiciones y cambios

• Proporcionan una actividad de difusión controlada.

• Proporcionan seguridad de grupo de trabajo y de red.

• Las VLAN´s ofrecen un mecanismo efectivo para controlar cambios en la reorganización de los usuarios y reducir en gran parte el costo asociado con las reconfiguraciones de *switches* y *routers*. Los usuarios en una VLAN pueden compartir el mismo espacio de dirección de red (es decir, la subred IP), sin importar su ubicación.

• Las VLANs representan un importante progreso con respecto a las técnicas basadas en LAN que se usan en los centros del cableado, porque necesitan menos cambios en el cableado, configuración y depuración. La configuración del *router* queda intacta. Cuando simplemente se debe desplazar a un usuario de una ubicación a otra, esto no crea modificaciones en la configuración del *router*, si el usuario permanece en la misma VLAN.

• Las VLAN´s son un mecanismo efectivo para extender los firewalls desde los *routers* a la estructura de los *switches* y proteger la red contra problemas de *broadcast* potencialmente peligrosos. El tráfico de *broadcast* dentro de una VLAN no se transmite fuera de la VLAN. Por el contrario, los puertos adyacentes no reciben ningún tráfico de *broadcast* generado desde otras VLAN´s. Éste tipo de configuración reduce sustancialmente el tráfico total de *broadcast*, libera el ancho de banda para el tráfico real de usuarios, y reduce la vulnerabilidad general de la red a las tormentas de *broadcast*.

• Cuanto menor sea el grupo de VLAN, menor será la cantidad de usuarios afectados por la actividad de tráfico de *broadcast* dentro del grupo de VLAN. También se pueden asignar VLANs basadas en el tipo de aplicación y la cantidad de *broadcasts* de aplicaciones. Se pueden colocar usuarios que comparten una aplicación que produce *broadcasts* en el mismo grupo de VLAN y distribuir la aplicación a través del campus.

4.4.4. RECOMENDACIONES DE SEGMENTACIÓN

A nivel de capa acceso se maneja la asociación de VLAN, en la cual se realizará la configuración para que los puertos de un mismo *switch* pertenezcan a diferentes VLANs. La comunicación entre diferentes VLANs emplea conmutación de capa 3 (enrutamiento), esta característica será provista por la capa de *core* (nivel superior al de distribución). La recomendación para el Ilustre Municipio de Ambato sería trabajar con VLAN mediante "Asignación de puertos" ya que este tipo de VLAN funciona bien en las redes en las que el movimiento se encuentra controlado y administrado, como es el caso de esta organización.

La red que cuenta con un servidor DHCP, que facilitará la inserción de nuevas estaciones de trabajo. En este caso, el servidor DHCP asignará a una nueva estación una dirección IP libre, de acuerdo al grupo de usuario al que vaya a corresponder dicha estación.

Para facilitar la administración de usuarios y permisos en la red se va a establecer un dominio en cada VLAN, que en su conjunto formaran las denominadas zonas dentro de la red, las cuales están conformadas por: PCs, impresoras, teléfonos y *access points* del dominio correspondiente.

La subred de la matriz a diseñarse estará dividida en las VLANs independientes, indicadas en la siguiente tabla, donde también se pueden observar las unidades operativas que se anexarán a cada grupo y las plantas de la edificación en las que estas funcionan, esto de acuerdo a los Anexos B, C, D, E, se establece una VLAN independiente para la granja de servidores por motivos de seguridad, debido a que los servidores son puntos críticos para posibles ataques.

Tabla. 4.8. VLAN's de la nueva red en la matriz

DOMINIO	VLAN	UNIDAD OPERATIVA	PLANTA
ADMINISTRATIVO	ADMIMA	ARCHIVO	PB
		PATRONATO MUNICIPAL	PB
		ALCALDÍA	P1
		AUDITORÍA	P1
		COORDINACIÓN ALCALDÍA	P1
		DIRECCION ADMINISTRATIVA	P1
		INFORMÁTICA	P1
		PRO- SECRETARÍA	P1
		RR.HH.	P1
		SECRETARÍA ALCALDÍA	P1
		SECRETARÍA GENERAL	P1
		VICEALCALDÍA	P1
		COM. INSTITUCIONAL	P1
		ASESORIA JURÍDICA	P2
FINANCIERO	FINIMA	PROVEEDURÍA	PB
		TESORERÍA	PB
		AVALÚOS Y CATASTROS	P2
		CONTABILIDAD	P2
		DIRECCIÓN FINANCIERA	P2
		RENTAS	P2
		UNIDAD DE PRESUPUESTOS	P2
OOPP	OOPPIMA	TALLERES OO.PP.	PB
		OBRAS PÚBLICAS	P3
PLANIFICACION	PLANIMA	PLAN ESTRATÉGICO	PB
		CARTOGRAFÍA	P2
		CONTROL URBANO	P2
		PLANIFICACIÓN	P2

SERVICIOS	SERIMA	BALCÓN DE SERVICIOS	PB
		INFORMACIÓN	PB
		SALA DE COMISIONES	PB
		SALA DE CONS. CANTONAL	PB
		SALA DE REUNIONES	PB
		SIMERT	PB
		SALA DE PRENSA Y TRABAJO	P1
		SALÓN DE LA CIUDAD	P1
		SALÓN EX ALCALDES	P1
		SERVICIOS PÚBLICOS	P2
TELEFONÍA IP	TOIPIMA	TODAS	TODAS
ADMINISTRACION DE RED	NETIMA	TODAS	TODAS

Para las redes de las otras dependencias debido a sus dimensiones se considera solamente dos segmentos, uno para voz y otro para datos. Para facilitar la administración de la red, se asignará un rango de direcciones a cada VLAN; de esta manera cuando una estación se conecte a la red el servidor DHCP, apoyado por la funcionalidad DHCP *relay,* con la que deberá contar el *switch* de *core,* podrá determinar en que VLAN está el equipo que realiza la solicitud, y de este modo asignarle una dirección libre dentro del rango correspondiente a dicho grupo. Esta asignación de rangos se observa en las siguientes tablas para cada dependencia municipal.

Tabla. 4.9. Direccionamiento para cada VLAN de la Matriz

VLAN	Subred	Rango de Direcciones	Default Gateway	# Max Dir. IP
SRVIMA	Subnet: 10.10.0.0 Mask: 255.255.255.224	Desde: 10.10.0.1 Hasta: 10.10.0.30	10.10.0.11	30
NETIMA	Subnet: 10.10.0.32 Mask: 255.255.255.224	Desde: 10.10.0.33 Hasta: 10.10.0.62	10.10.0.33	30
PLANIMA	Subnet: 10.10.0.64 Mask: 255.255.255.192	Desde: 10.10.0.65 Hasta: 10.10.0.126	10.10.0.65	62
OOPPIMA	Subnet: 10.10.0.128 Mask: 255.255.255.192	Desde: 10.10.0.129 Hasta: 10.10.0.190	10.10.0.129	62
SERIMA	Subnet: 10.10.0.192 Mask: 255.255.255.192	Desde: 10.10.0.193 Hasta: 10.10.0.254	10.10.0.193	62
FINIMA	Subnet: 10.10.1.0 Mask: 255.255.255.128	Desde: 10.10.1.1 Hasta: 10.10.1.126	10.10.1.1	126
ADMIMA	Subnet: 10.10.1.128 Mask: 255.255.255.128	Desde: 10.10.1.129 Hasta: 10.10.1.254	10.10.1.129	126
TOIPIMA	Subnet: 10.10.2.0 Mask: 255.255.255.0	Desde: 10.10.2.1 Hasta: 10.10.2.254	10.10.2.1	254

Tabla. 4.10. Direccionamiento para cada VLAN de las Comisarías

VLAN	Subred	Rango de Direcciones	Default Gateway	# Max Dir. IP
DTCMSR	Subnet: 10.10.5.0 Mask: 255.255.255.128	Desde: 10.10.5.1 Hasta: 10.10.5.126	10.10.5.2	126
TOIPCMSR	Subnet: 10.10.5.128 Mask: 255.255.255.128	Desde: 10.10.5.129 Hasta: 10.10.5.254	10.10.5.129	126

Tabla. 4.11. Direccionamiento para cada VLAN de Cultura

VLAN	Subred	Rango de Direcciones	Default Gateway	# Max Dir. IP
DTCLTR	Subnet: 10.10.6.0 Mask: 255.255.255.128	Desde: 10.10.6.1 Hasta: 10.10.6.126	10.10.6.2	126
TOIPCLTR	Subnet: 10.10.6.128 Mask: 255.255.255.128	Desde: 10.10.6.129 Hasta: 10.10.6.254	10.10.6.129	126

Tabla. 4.12. Direccionamiento para cada VLAN de Tránsito

VLAN	Subred	Rango de Direcciones	Default Gateway	# Max Dir. IP
DTUMT	Subnet: 10.10.8.0 Mask: 255.255.255.128	Desde: 10.10.8.1 Hasta: 10.10.8.126	10.10.8.2	126
TOIPUMT	Subnet: 10.10.8.128 Mask: 255.255.255.128	Desde: 10.10.8.129 Hasta: 10.10.8.254	10.10.8.129	126

Tabla. 4.13. Direccionamiento para cada VLAN del Hospital

VLAN	Subred	Rango de Direcciones	Default Gateway	# Max Dir. IP
DTHSPTL	Subnet: 10.10.4.0 Mask: 255.255.255.128	Desde: 10.10.4.1 Hasta: 10.10.4.126	10.10.4.2	126
TOIPHSPTL	Subnet: 10.10.4.128 Mask: 255.255.255.128	Desde: 10.10.4.129 Hasta: 10.10.4.254	10.10.4.129	126

Tabla. 4.14. Direccionamiento para cada VLAN del Mercado Mayorista

VLAN	Subred	Rango de Direcciones	Default Gateway	# Max Dir. IP
DTMMY	Subnet: 10.10.3.0 Mask: 255.255.255.128	Desde: 10.10.3.1 Hasta: 10.10.3.126	10.10.3.2	126
TOIPMMY	Subnet: 10.10.3.128 Mask: 255.255.255.128	Desde: 10.10.3.129 Hasta: 10.10.3.254	10.10.3.129	126

Tabla. 4.15. Direccionamiento para cada VLAN del Camal

VLAN	Subred	Rango de Direcciones	Default Gateway	# Max Dir. IP
DTCML	Subnet: 10.10.9.0 Mask: 255.255.255.128	Desde: 10.10.9.1 Hasta: 10.10.9.126	10.10.9.2	126
TOIPCML	Subnet: 10.10.9.128 Mask: 255.255.255.128	Desde: 10.10.9.129 Hasta: 10.10.9.254	10.10.9.129	126

Tabla. 4.16. Direccionamiento para cada VLAN de las Bodegas

VLAN	Subred	Rango de Direcciones	Default Gateway	# Max Dir. IP
DTBDG	Subnet: 10.10.10.0 Mask: 255.255.255.128	Desde: 10.10.10.1 Hasta: 10.10.10.126	10.10.10.2	126
TOIPBDG	Subnet: 10.10.10.128 Mask: 255.255.255.128	Desde: 10.10.10.129 Hasta: 10.10.10.254	10.10.10.129	126

4.5. INTERCONEXIÓN DE REDES

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar que características posean. Esto se logra mediante protocolos de encaminamiento.

En el nuevo diseño planteado, se modificará la filosofía de la red municipal en su conjunto, pues inicialmente existía una sola subred la 10.10.0.0/16 a la cual estaban anexadas todas las dependencias, al tener un solo dominio de *broadcast*, la red era poco eficiente y se desperdiciaban los recursos especialmente los de la WAN, que constituye el cuello de botella de modo que el tráfico *broadcast* y *multicast* cruzaba por toda la red

innecesariamente, por esta razón el nuevo diseño plantea implementar una subred independiente para cada dependencia y además de ello segmentación VLAN en cada una de estas subredes, de este modo los dominios de *broadcast* se reducirán considerablemente y las diferentes redes serán más eficientes en su desempeño, con lo cual solventamos este inconveniente; sin embargo esta nueva filosofía como tal no permite que las diferentes redes o diferentes VLAN's se comuniquen entre sí, para satisfacer este requerimiento es necesario introducir un equipo que trabaje en la capa 3 del modelo OSI, es decir en la capa de red, los equipos que cumplen con esta condición actualmente son los *routers* y *switches* de capa 3, la ilustre municipalidad de Ambato cuenta con un switch de capa 3, marca Cisco, modelo 3560, que fue adquirido específicamente para el rediseño de la red, previo a la implementación de la nueva central telefónica de tecnología IP, este equipo vendría a satisfacer la necesidad de interconexión de redes y VLAN's y estaría ubicado en el borde de la matriz, donde esta se comunica con la WAN, estando así conectada al resto de redes.

En este equipo se deben configurar sus puertos con las direcciones de los *default Gateway* que se muestran en las tablas de direccionamiento para cada VLAN, de este modo un puerto tendrá varias direcciones, de acurdo a las redes que estén físicamente asociadas a dicho puerto, así este *switch* internamente conocerá por qué puerto puede alcanzar a cada una de las redes y VLAN's. De entre todos los protocolos de encaminamiento que fueron analizados en el capítulo I, se requerirá solamente de rutas estáticas, la ruta estática que se deberá añadir es para la conexión a Internet que se realiza a través del servidor destinado para este fin y deberá ser la siguiente: a 0.0.0.0 0.0.0.0 por 10.10.0.2, de este modo cuando el equipo no encuentre dentro de la red municipal a un dirección IP de destino enviará el paquete por la interfaz indicada en esta ruta estática.

4.6. GESTIÓN DE RED

Las redes y los sistemas de procesamiento distribuido son de una importancia crítica y creciente en los negocios, gobierno y otras instituciones. Dentro de una institución, la tendencia es hacia redes más grandes, más complejas y dando soporte a más aplicaciones y a más usuarios.

Una red grande no se puede instalar y gestionar sólo con el esfuerzo humano. La complejidad de un sistema tal, impone el uso de herramientas automáticas de gestión de red. La urgencia de la necesidad de esas herramientas se incrementa, y también está en

auge la dificultad de suministrar dichas herramientas, si la red incluye equipos de múltiples distribuidores. En respuesta, se han desarrollado normalizaciones para tratar la gestión de red, y que cubren los servicios, los protocolos y la base de información de gestión.

4.6.1. SNMP (Simple Network Management Protocol)

El protocolo *Simple Network Management Protocol* (SNMP) permite gestionar redes TCP/IP y está basado en SGMP que permite manejar los *routers* en Internet.

Actualmente SNMP está soportado en muchos sistemas distintos tales como puentes, PC's, estaciones de trabajo, encaminadores, terminales, servidores, concentradores, y tarjetas avanzadas *ethernet*, *token ring* y FDDI.

SNMP se basa en un sistema de petición-respuesta. La autoridad gestora no es la red como sistema sino una o varias estaciones distinguidas (NMS).

La arquitectura SNMP consta de los siguientes componentes:

• Gestores (NMS's)

• Agentes (nodos administrados)

• MIB (base de datos con información)

• SMI (administración de la base de datos)

• Protocolos (órdenes)

4.6.2. RMON (Remote Monitoring)

RMON es un estándar que define objetos de control, permitiendo que se capture la información en tiempo real a través de la red entera. El estándar de RMON es una definición para Ethernet.

El MIB de RMON proporciona un método estándar para vigilar las operaciones básicas de Ethernet. RMON también proporciona un mecanismo para notificar cambios en el comportamiento de la red.

Se puede utilizar RMON para analizar y para vigilar datos del tráfico de la red dentro de segmentos alejados de la LAN. Esto permite que se detecte, aísle, diagnostique, y señale problemas potenciales y reales de la red antes de que se extiendan a las situaciones de crisis.

RMON permite que se instale las historias automáticas que se recoge durante todo el tiempo, proporcionando datos en la estadística básica como por ejemplo la utilización o colisiones. RMON automatiza ésta colección de datos y proporciona a otros datos del proceso las hojas de operación (*planning*), el proceso es más fácil y el resultado más exacto.

4.6.3. RECOMIENDACIONES PARA LA GESTIÓN DE LA RED

Para la gestión de la red se recomienda implementar en la estación de trabajo del encargado de la administración de la misma, en el departamento de sistemas de forma permanentemente la herramienta utilizada para el monitoreo, el software PRTG, que trabaja con el protocolo SNMP, y permite la recolección almacenamiento de históricos y análisis de las principales variables de la red, además permite monitorear permanentemente los retardos de los enlaces WAN parámetro que es de gran utilidad especialmente para las aplicaciones de voz, también nos brinda una visión de la disponibilidad de la red. Adicionalmente resultaría de gran utilidad contar con la herramienta *Colasoft Capsa* que es un *sniffer*, y a través de la configuración de *port mirroring* de los *switches* administrables permite conocer cualitativamente el tráfico que esta fluyendo a través de la red, de este modo se puede diagnosticar de mejor manera los problemas que pueden surgir, así como también permite identificar tráfico indeseable o utilidades de internet que no son productivas para el desarrollo del trabajo municipal y más bien, producen un consumo innecesario de ancho de banda.

4.7. MODELO DE RED

La realización de un diseño de red debe abarcar características de confiabilidad, escalabilidad y facilidad de administración, así que una solución jerárquica nos proporciona un enfoque sistemático para lograr estos objetivos.

El modelo jerárquico se caracteriza por ser modular (adaptabilidad a cambios permitiendo aumentar el tamaño de la red), de simple implementación, facilidad de

administración y gestión (estructura comprensible), y capacidad de redundancia. Adicionalmente, permite el aislamiento de fallas, de tal manera que evita que un equipo defectuoso influya en el rendimiento de toda la red, limitando el daño a su correspondiente segmento, lo que simplifica su detección.

El modelo jerárquico está conformado por tres capas: Acceso, Distribución y *Core*.

4.7.1. CAPA DE ACCESO

Punto en el cual se conectan los usuarios finales de la red (estaciones de trabajo, impresoras, puntos de acceso inalámbrico, teléfonos IP, retroproyectores), los cuales pueden pertenecen a múltiples grupos de trabajo. Su función principal es permitir el flujo de tráfico generado por los usuarios que demandan el acceso a los servicios de red, aquí se definen también las VLAN's. Posteriormente este flujo será desviado a la siguiente capa del modelo: la capa de distribución.

El número de switches de acceso dependerán del número de puntos de red presentes en cada una de las plantas del edificio.

4.7.2. CAPA DE DISTRIBUCIÓN

Punto intermedio entre la capa de acceso y la de *core*. Proporciona conectividad basada en una determinada política, ya que establece cuándo y cómo los paquetes pueden acceder a los servicios de la red.

La capa de distribución determina la ruta más rápida (enrutamiento de capa 3), para que la petición de un usuario pueda ser enviada al servidor y posteriormente a la capa de *core*. En la capa de distribución se realizará la segmentación de la red en múltiples dominios de *broadcast*, la definición de subredes y la implementación de directivas de control de acceso y de seguridad.

4.7.3. CAPA DE CORE

Es el núcleo de alta velocidad de la red, de ahí su nombre. Facilita la transferencia de datos entre las capas de distribución interconectadas, es tolerante a errores, el equipamiento se caracteriza por su alto grado de confiabilidad y se requiere la detección de cualquier

característica que pueda afectar el rendimiento de esta capa en una de distribución o de acceso.

Al *switch* de core se conectarán todos los *switches* de distribución y los del grupo de servidores. La siguiente figura, muestra el modelo jerárquico de red.

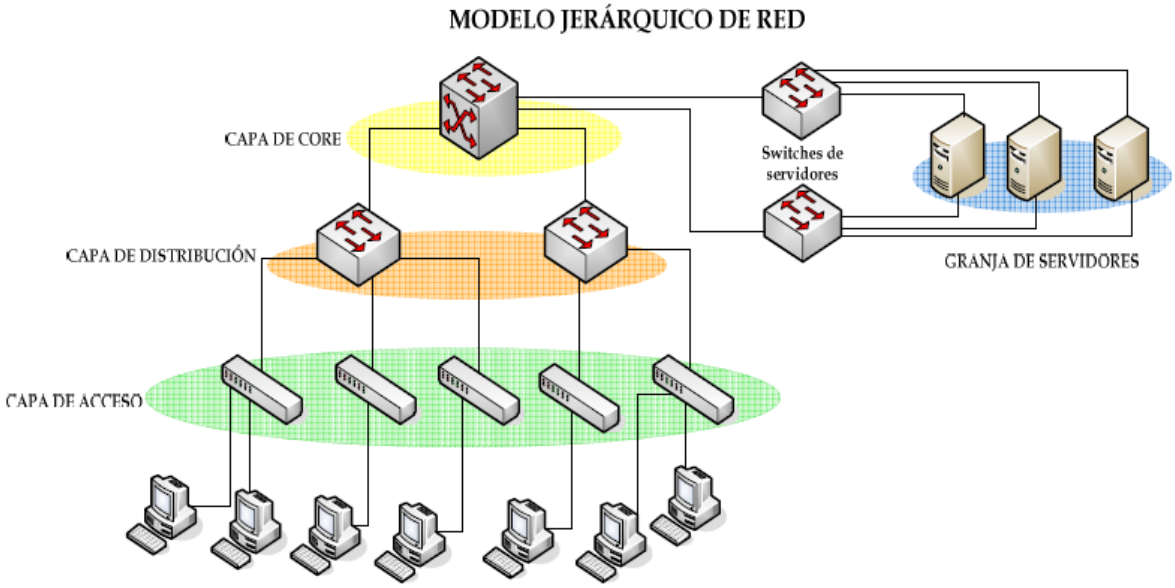


Figura. 4.2. Modelo jerárquico de red

Debido, a que nuestra red no es muy extensa, se fusionarán en una, la capa de distribución, y la capa de *core*, esto sin embargo no limita la escalabilidad de la red pues a medida que esta vaya creciendo se puede implementar una capa de *core* independiente, cuando las necesidades así lo ameriten.

4.8. SELECCIÓN DE LA TECNOLOGÍA DE RED

Debido a que las nuevas redes de datos están orientadas al manejo de aplicaciones de alta velocidad y carga de procesamiento (multimedia, videoconferencia, procesamiento de datos e imágenes, VoIP, etc.), se requiere un mayor ancho de banda para cubrir dichas demandas.

La tecnología LAN más difundida es Ethernet, por lo cual se seleccionó las siguientes tecnologías Ethernet.

- Fast Ethernet. Se empleará esta tecnología para la parte del cableado horizontal, comprendida desde las estaciones de trabajo hacia los switches de accesos, debido a que el tráfico estimado por usuario no se acerca a los 100 Mbps, ni en los valores picos. Así mismo, una gran cantidad de aplicaciones que se manejarán a este nivel son soportadas por dicha tecnología (multimedia, videoconferencia, VoIP, etc.).

- Gigabit Ethernet. Se empleará para el cableado vertical y una parte del cableado horizontal, cuando se requiera interconexión entre switches. Dichos enlaces (tanto para el cableado horizontal como vertical), requerirán de altas velocidades de transmisión, especialmente en los instantes picos de tráfico.

La siguiente figura muestra el tipo de tecnología empleado en cada conexión.

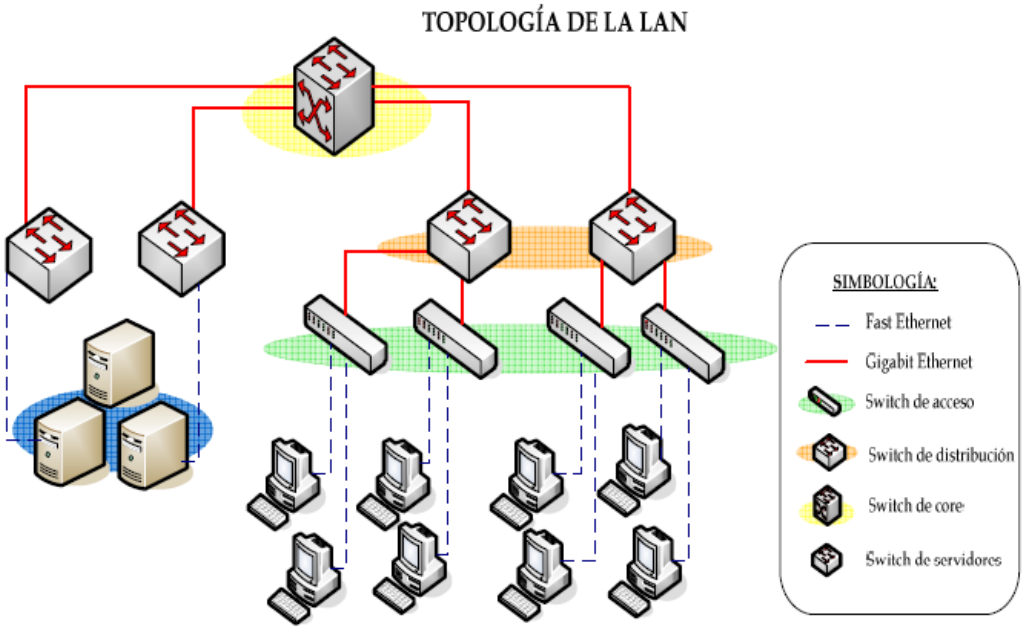


Figura. 4.3. Tecnologías LAN empleadas

4.9. CRITERIOS PARA ELECCIÓN DE EQUIPOS

Los criterios para la elección de equipos se basarán como mínimo en el cumplimiento de los siguientes requerimientos técnicos:

• El equipo deberá soportar voltajes entre 100 y 240 VAC.

• Los equipos escogidos deberán pertenecer a familias tecnológicas altas, de tal manera que no se descontinúen durante los próximos cinco años como mínimo.

• Capacidad de soportar cable categoría 6 para la parte LAN y enlaces Gigabit para fibra óptica multimodo, en los casos en que sea necesario.

• Presentar puertos Ethernet 10Base-T/100Base-TX con conectores RJ-45 para los puertos de acceso, y puertos Ethernet 10Base-T/100Base-TX/1000Base-T con conectores RJ-45 o ranuras para la instalación de tarjetas 1000Base-SX, 1000Base-LX y 1000Base-ZX, para los puertos de *uplink.*

• Tener la capacidad de trabajar como *switch* de capa 3 en el caso así requerido, de tal forma que pueda enrutar VLANS que se crean dentro de la red, debido a que un switch capa 2 mantiene las VLANS separadas, detección de fallas, modificación, seguridad de red y controles QoS, este *switch* debe soportar como mínimo el protocolo de encaminamiento RIP, y manejar rutas estáticas. Deberá brindar apoyo IPv6. Y cumplir con la funcionalidad de *DHCP relay agent*.

• Disponibilidad ininterrumpida: se refiere a que si una de las unidades falla, el resto de unidades continuarán con el tráfico de envío y manteniendo la operación.

• Seguridad de la red: los *switches* adquiridos deben poseer características de seguridad para conectividad y control de acceso, incluyendo ACL, autenticación, seguridad *port-level*, servicios con 802.1x, de ésta forma se ayudará a prevenir ataques externos, que constituyen las principales preocupaciones en el mundo actual de los negocios.

• Soporte de tecnología *Power over Ethernet* (PoE), la cual permite que los dispositivos Ethernet como teléfonos IP, reciban alimentación y datos a través del cableado de la LAN existente. El estándar PoE IEEE802.3af, es el primer estándar internacional de distribución de alimentación a través de una LAN Ethernet.

• Los *switches* deben soportar los siguientes protocolos, como mínimo:

- 802.1p/Q (soporte de QoS y VLAN's)
- TCP (*Transmission Control Protocol*)

- UDP (*User Datagram Protocol*),
- SNMP (*Simple Network Management Protocol*)
- RMON (*Remote Monitoring*)
- STP (*Spanning Tree Protocol*): es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología esté libre de lazos. STP es transparente a las estaciones de usuario.
- IGMP (*Internet Grouping Management Protocol*): protocolo que permite a los hosts comunicar su interés; o no, en pertenecer a grupos multicast, dinámicamente.

  Este interés se comunica a *los routers multicast* que usarán la información para construir o podar árboles de distribución *multicast* y usarlos en algún algoritmo de encaminamiento *multicast*.

  Los mensajes IGMP van encapsulados dentro de datagramas IP.
- Finalmente debe dar cumplimiento de manera general a las normas IEEE 802.3 y IEEE 802.1

4.10. RECOMENDACIONES PARA EL DISEÑO DE LA RED PASIVA

En cuanto a la red pasiva los requerimientos se limitan a incrementar el cableado para los nuevos puntos de datos descritos en la tabla 3.67, pues en la matriz se utilizará el cableado de voz existente en la mayoría de los casos, y en algunos de ellos se compartirá el cableado de datos. Para las otras dependencias se utilizará el cableado de datos que llega a las estaciones de trabajo y ahora transportarán conjuntamente el tráfico de voz y de datos.

Se recomienda certificar el cableado la red municipal, pues actualmente, no se ha realizado esta tarea que es de gran importancia para asegurar la eficiencia del mismo.

4.10.1. DISTRIBUCIÓN DE PUNTOS DE RED

Los nuevos puntos de red serán ubicados en la planta baja en los departamentos SIMERT y Sala de comisiones claramente identificados en el anexo B, en las siguientes figuras se muestra la distribución de estos puntos, que serán identificados como DT65, DT66, DT67, VZ19, VZ20.

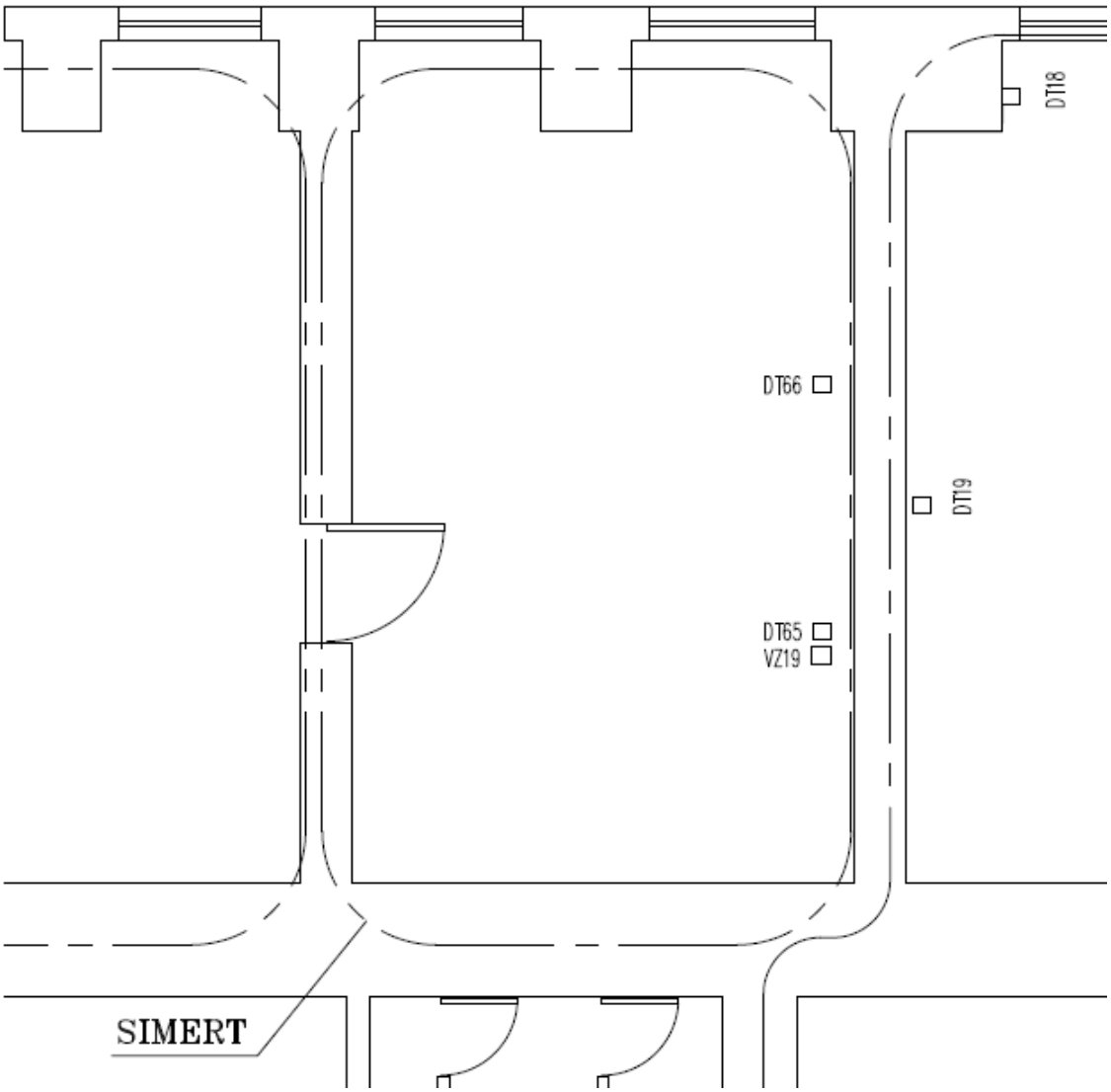


Figura. 4.4. Nuevos puntos de red en SIMERT

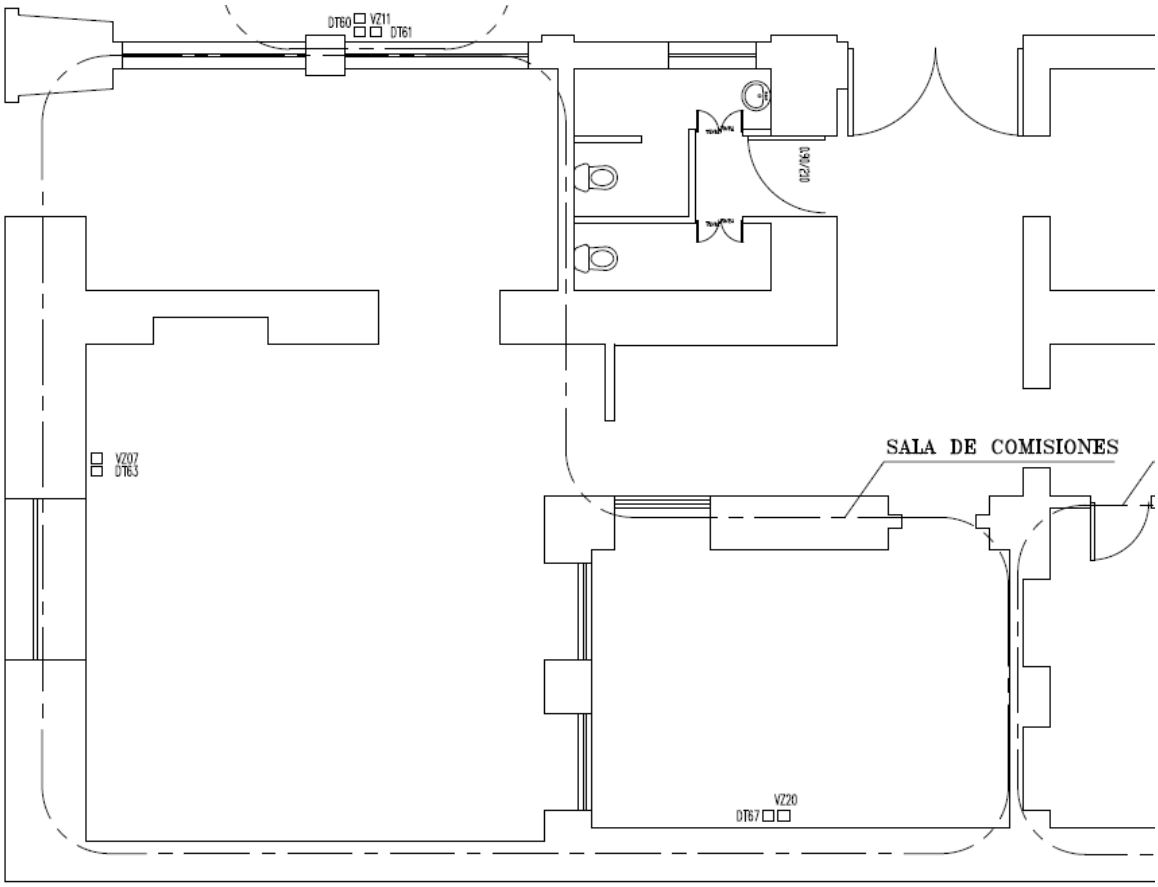


Figura. 4.5. Nuevos puntos de red en Sala de Comisiones

4.10.2. MATERIALES PARA LOS NUEVOS PUNTOS DE RED

Los nuevos puntos de red, requerirán de cable UTP CAT5e, tramos de ductería para llevarlos desde las estaciones de trabajo hasta, la canaleta más cercana que conduce los cables hasta el rack de la planta baja.

A continuación se listan los materiales necesarios:

Tabla. 4.17. Materiales para la red pasiva

Marerial	Cantidad
Cable UTP CAT 5e	260 m
Patch Cords UTP CAT 5e	96
Certificación de cableado	
Ductería	

4.11. RECOMENDACIONES PARA EL DISEÑO DE LA RED ACTIVA

Los equipos de red con los que cuenta actualmente la Ilustre Municipalidad de Ambato, son en su gran mayoría no administrables y poseen solamente las características básicas de conmutación, por lo tanto no presentan las facilidades técnicas para implementar la red descrita en este capítulo a excepción de dos *switches* marca D-LINK DES-3226, DES-3226L y CISCO 2960, además de los equipos descritos en el capítulo 3, se cuenta con un *switch* CISCO 3560 nuevo, de capa 3 el cual está listo y disponible para entrar en operación, con estos antecedentes y considerando que el elemento central de la red rediseñada es el *switch* de capa 3, los equipos que se seleccionarán serán de la marca CISCO, y cumplirán los requerimientos mencionados en este capítulo.

En el esquema presentado observamos, el escenario sobre el cual, podremos implementar la nueva central telefónica IP, en la misma se consideran *switches* CISCO 520 de capa 2 para el acceso que poseen 24 puertos *Fast Ethernet* con PoE (*Power over Ethernet*), lo cual facilitará la instalación de los equipos telefónicos, estos puertos deberán ser asociados con sus respectivas VLAN's, de acuerdo a la tabla 4.8, además estos switches poseen dos puertos uplink *Gigabit Ethernet*, los cuales sirven para interconectarse con el resto de la red, estos puertos deben ser configurados como troncales, es decir por ellos pueden fluir paquetes de todas las VLAN's, se debe habilitar el protocolo *Spanning Tree,* pues debido a los enlaces redundantes que tiene cada *switch* se debe evitar a través de este protocolo el problema de bucles cerrados, evitando así que los paquetes se queden circulando infinitamente por dichos bucles.

En la capa de distribución, realmente no se realizan las funciones que se le debe asignar a esta capa de acuerdo con el modelo jerárquico, como ya se analizó en el apartado 4.7., sin embargo, estos *switches* servirán para interconectar equipos que se encuentran sobre la misma VLAN, pero en diferente *switch* de acceso, y concentrarán todos los enlaces principales y redundantes que interconectan la red, para este fin poseen 24 puertos (*Fast Ethernet* en la planta 3 y *Gigabit Ethernet* en las otras plantas), y dos (planta 3) o cuatro (resto de plantas), puertos de *uplink Gigabit Ethernet*, se debe habilitar el protocolo *Spanning Tree* en estos equipos, los puertos que quedan disponibles se pueden utilizar para brindar acceso, en cuyo caso deberán ser asociados a sus correspondientes VLAN's,

mientras que aquellos que sirvan para interconectar *switches* deberán ser configurados como troncales.

En la capa de *core*, y de acuerdo a las recomendaciones del fabricante de equipos CISCO para redes no muy extensas, se agrupan las funciones de la capa de *core* en sí, y las de la capa de distribución, brindando interconexión entre VLAN´s y entre redes lo cual fue descrito en el apartado 4.5., también se provee la funcionalidad de DHCP relay, para que el servidor pueda asignar la dirección dinámicamente, a todos los equipos, aunque estos se encuentren fuera de su red lógica.

Es condición indispensable que en toda la red se aplique QoS, brindando mayor prioridad a los paquetes destinados al tráfico de voz.

A continuación se resume la cantidad de puertos disponibles para acceso en cada planta.

Tabla. 4.18. Resumen de puertos para acceso en la matriz

	REQUERIMIENTOS				DISPONIBLES
Planta	**Acceso Datos**	**Acceso Voz/Datos**	**Acceso Voz**	**Total**	**Para Acceso**
PB	50	10	15	75	88
P1	63	0	26	89	106
P2	98	2	28	128	132
P3	30	0	11	41	48

A continuación se muestra el diagrama de la nueva red, que se recomienda implementar para obtener un medio de comunicación convergente, que permita el flujo ordenado y eficiente del tráfico de voz y datos, asegurando calidad de servicio, y dejando la puerta abierta para que a futuro la red sea fácilmente escalable.

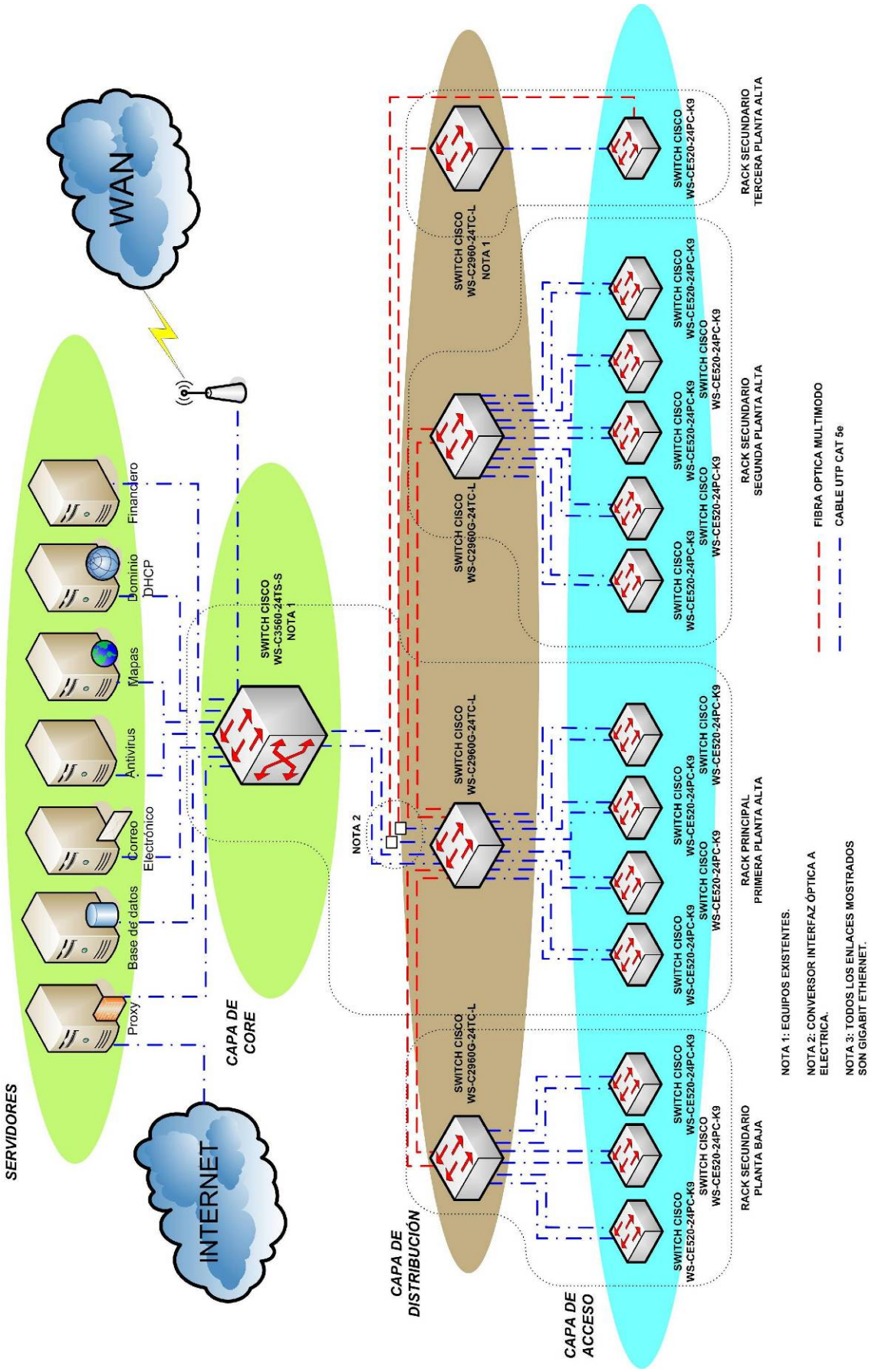


Figura. 4.6. Red rediseñada de la matriz

Para las dependencias municipales restantes, debido a no disponer de *switches* que cumplan con los requerimientos y estándares necesarios para asegurar el buen funcionamiento del nuevo sistema y en algunos casos los equipos de red son solamente *hubs*, se hace indispensable un cambio total de estos dispositivos, hay que tomar en cuenta que los dos *switches*, que cumplen con las características básicas y venían operando en la matriz serán reubicados, estos son los D-LINK DES-3226 y DES-3226L.

Como podemos observar en el esquema básicamente por poseer redes pequeñas las dependencias municipales requieren solamente de acceso y conexión a la red WAN, lo cual se proveerá a través de los *switches* CISCO 520, que se encargarán de segmentar la red en VLAN's de acuerdo a lo expuesto en el apartado 4.4.4., para lo cual se deberá configurar sus puertos, aquellos que sirvan para enlazarse al resto de la red deberán ser configurados como troncales y en el caso de comisarias donde se utilizan enlacen redundantes, es necesario habilitar el protocolo *Spannig Tree*. Se debe configurar necesariamente QoS en toda la red brindando una mayor prioridad al tráfico de voz, lo cual asegurará que los paquetes de voz puedan ser transportados preferentemente sobre la WAN, que constituye el cuello de botella de nuestra red, por lo tanto esta configuración es vital para lograr atravesar de manera eficiente esta parte de la red.

A continuación se resume la cantidad de puertos de acceso disponibles, en cada dependencia.

Tabla. 4.19. Resumen de puertos para acceso en las dependencias

	REQUERIMIENTOS				DISPONIBLES
Planta	**Acceso Datos**	**Acceso Voz/Datos**	**Acceso Voz**	**Total**	**Para Acceso**
Bodegas	3	0	2	5	24
Camal	8	0	1	9	24
Mercado Mayorista	7	0	5	12	24
Cultura	14	0	2	15	25
Tránsito	13	0	2	14	25
Comisarías	23	17	0	40	48
Hospital	21	0	2	22	25

En el siguiente esquema se se muestra la red rediseñada.

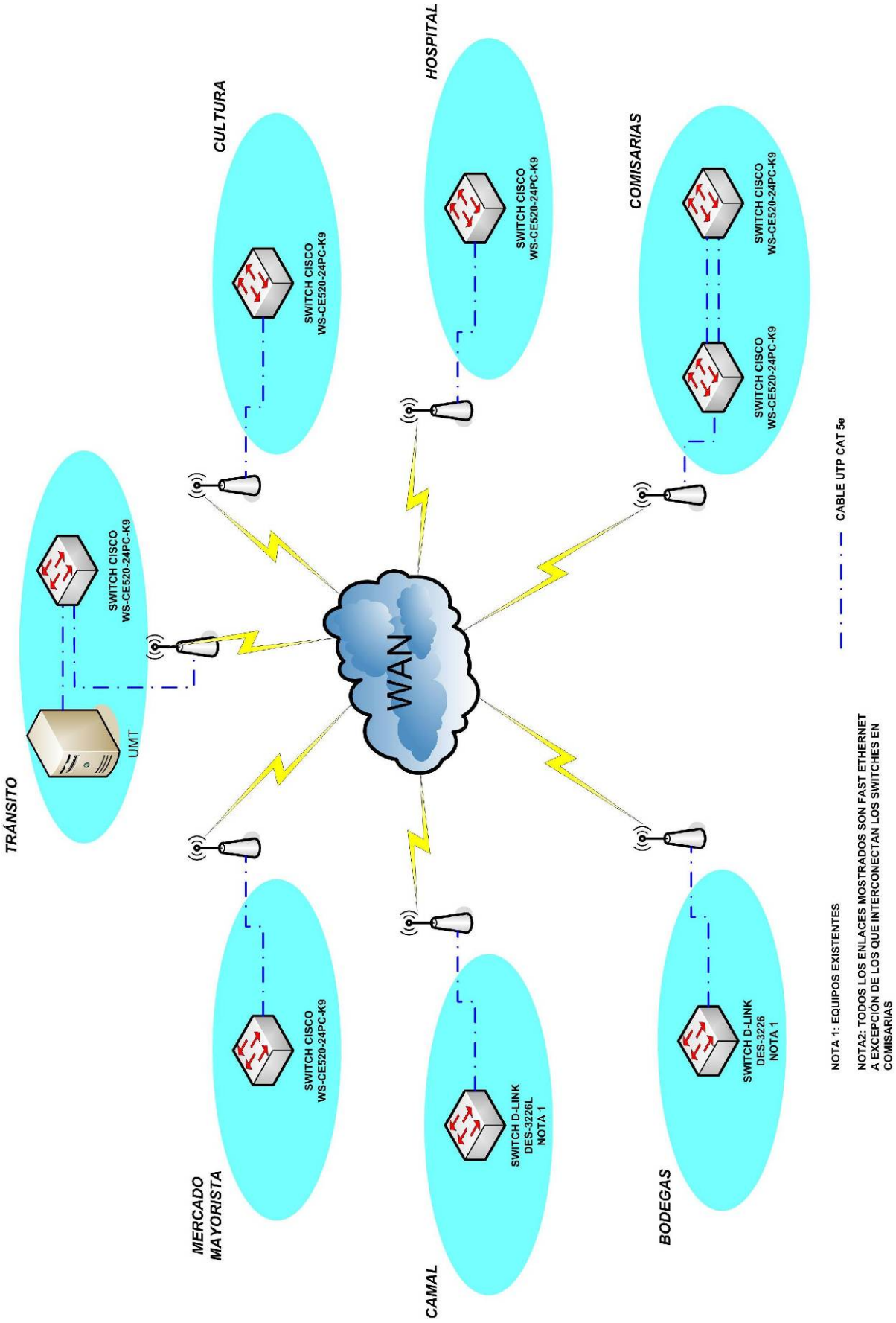


Figura. 4.7. Red rediseñada de las dependencias municipales

4.11.1. EQUIPOS PARA EL REDISEÑO DE LA RED

De lo expuesto en el rediseño de la red y tomando en consideración los equipos reutilizables se resume a continuación los requerimientos en cuanto a equipos de red respecta.

Tabla. 4.20. Requerimientos de equipos para le red rediseñada

Equipos	Cantidad
Switch CISCO WS-C2960G-24TC-L	3
Switch CISCO WS-CE520-24PC-K9	21
Transceiver CISCO GLC-SX-MM	9
Transceiver Externo	2

CAPÍTULO V:

5. DISEÑO DEL SISTEMA DE TELEFONÍA IP PARA EL MUNICIPIO DE AMBATO

Para el diseño de telefonía IP, se buscará especificar un sistema, que permita migrar hacia la convergencia, para poder aprovechar la red de datos rediseñada y direccionar el tráfico de voz a través de la WAN Municipal, para aprovechando todas estas infraestructuras lograr reducir los costos de telefonía y brindar herramientas de comunicación que impulsen y faciliten el desarrollo de las actividades diarias de todos los colaboradores de la Ilustre Municipalidad de Ambato.

5.1. MIGRACIÓN A TELEFONÍA IP

Como se analizó en el capítulo 3, actualmente la Ilustre Municipalidad de Ambato, cuenta con una red de datos y una telefónica totalmente independiente entre sí, además el sistema telefónico análogo de la matriz está saturado y presenta daños difíciles de reparar pues los repuestos son difíciles de conseguir por ser un producto descontinuado.

Por este motivo se concebirá el diseño de una red de telefonía IP, que aproveche la infraestructura de datos y reemplace al obsoleto sistema de la matriz, para las dependencias que actualmente no cuentan con una infraestructura de datos también se implementará una solución completamente IP, sin embargo para las dependencias que cuentan una infraestructura analógica que funcione correctamente como es el caso de los departamentos

Municipales de Cultura, Hospital, Tránsito y Camal, se mantendrá y anexará la misma al nuevo sistema de telefonía IP.

Este proceso de migración se considera con la finalidad de reducir el impacto de la inversión inicial, sin embargo se contempla que en un futuro cercano se consiga un sistema de telefonía completamente IP, por este motivo el sistema seleccionado debe estar en completa capacidad de satisfacer las necesidades al momento de esta primera implementación, y de toda la red municipal en un futuro.

5.2. SOLUCIONES DE TELEFONÍA IP EN EL MERCADO

5.2.1. SOLUCIÓN MEDIANTE NETWORKING

La tendencia actual en comunicaciones es la convergencia, es decir, la integración a todo nivel de servicios y recursos; basados en esta corriente las empresas dedicadas a telecomunicaciones (Siemens y Alcatel, por ejemplo) se han aproximado al campo de los datos, así como las empresas que trabajan en la creación y diseño de redes de computadoras (Cisco y 3COM, por ejemplo) han buscado la integración de la voz entre sus servicios. Producto de esto último es el aparecimiento de diversas clases de dispositivos, aparatos, protocolos, convenciones y programas que permiten utilizar una red de datos para la transmisión de voz. Se admiten, por supuesto condiciones previas por cumplirse, entre éstas el control del retardo y el limitar la pérdida de paquetes; situaciones superables en el caso de datos pero críticas para la voz.

DESCRIPCIÓN TECNOLÓGICA

Una red de datos que soporta voz es a todo nivel, un conjunto de interfaces estandarizados, lo que hace que el sistema sea más flexible y deje de ser centralizado puesto que las funciones del sistema telefónico pueden distribuirse en toda la red. Es así que dentro de una red de datos ya establecida donde se busca implementar voz, se consideran los elementos fundamentales de la siguiente figura.

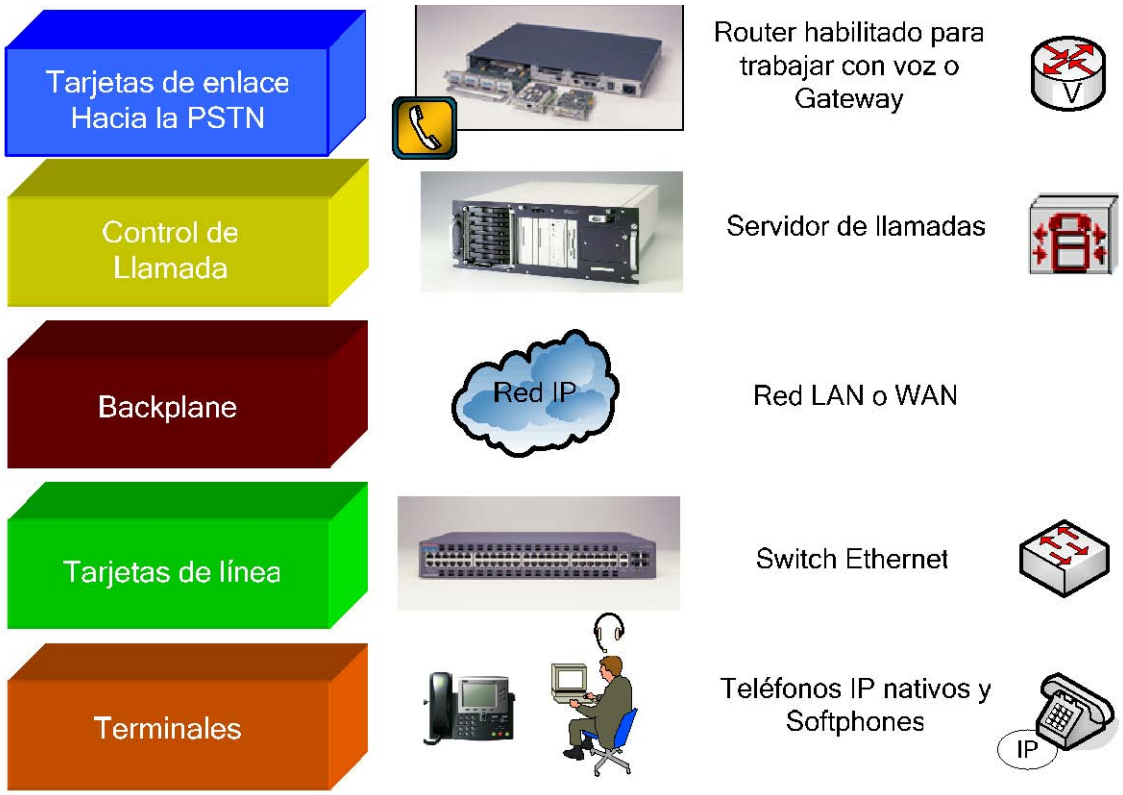


Figura. 5.1. Elementos de la Telefonía IP

Los terminales IP (independientemente del tipo) se conectan a puntos de datos provistos por tarjetas de línea instaladas en *switches*; el conjunto de *switches* están conectados entre sí a través de una Red IP privada (comunicación a nivel local) o pública (en situaciones remotas) y la operación del conjunto está comandada por el Servidor de Llamadas (*Call Server*). Para interactuar con la PSTN se utilizan los *routers* de voz o *Gateways*. Es decir el *Call Server* y el *Gateway* son los principales elementos para obtener telefonía IP sobre la red de datos y se tratan en detalle a continuación.

Servidor de llamadas.-Se encarga de las tareas de gestión propias de una PBX tradicional; es decir maneja el control, admisión, establecimiento, desconexión, tarificación de las llamadas, generación de música de espera, servicios de agenda electrónica, etc.

Un conjunto interconectado de servidores de comunicación se le conoce como "*cluster*" de manera que un servidor principal y un servidor de respaldo forman de por sí un *cluster* básico; dependiendo de la complejidad del sistema y el número de usuarios el *cluster* adquiere un mayor número de servidores. Ciertas funciones suplementarias que

ejercía un solo servidor como publicación de actualizaciones (informes a toda la red de cambios de configuración y grabación de detalles de llamada realizada), descargas TFTP (archivos de configuración, códigos de uso o tonos de timbrado), música en espera (MoH) o servidor de conferencias pueden delegarse a servidores anexados para un fin único debido al tamaño que adquieren esas tareas junto con el incremento de la red.

Los diversos servidores que forman el *cluster* pueden repartirse en diversos puntos de la red LAN o WAN manteniendo la operatividad única del *cluster* a través de enlaces *intra-cluster*; esta técnica llamada "*clustering*" permite evitar que los servidores compartan puntos de falla comunes.

La programación de los servidores se puede hacer vía consola y por vía WEB, tanto a un servidor en particular como a todo el *cluster*.

Dependiendo del entorno de la empresa, es posible utilizar un "modelo de procesamiento de llamada" centralizado o distribuido (común para cualquier tipo de tecnología empleada: IP-PBX y servidores). En el primero el *cluster* está ubicado en las oficinas principales de la empresa y uno o más *Gateways* (de existir sucursales) se ubican en la matriz y las locaciones remotas de la red, en este caso las operaciones de gestión de llamada y los canales de procesamiento de señal digital se ubican en un punto físico único ya sea mediante un solo *Call Server* o un *cluster*.

El modelo de procesamiento distribuido ubica un *Call Server* o un *cluster* en cada sitio remoto y la comunicación entre las locaciones se hace a través de un red IP WAN por donde se envía únicamente tráfico de voz; cabe aclarar que es necesaria la intervención de un *gatekeeper* que gestione la interacción de los *Gateways* al darse llamadas entre las oficinas remotas.

A través del servidor de llamadas es posible la implementación de VoIP en el entorno LAN, sin la necesidad de otro dispositivo como el *Gateway*, este último permite la interoperabilidad con redes externas como la PSTN. Los principales elementos con los que interactúa un servidor de comunicaciones se citan a continuación:

- Teléfono IP o Softphone
- Gateway de voz

- Servidor de voice mail, Fax Server
- Troncales Intra-cluster
- Recursos para conferencia (Hardware y software)

Gateway de voz.-Principalmente maneja extensiones analógicas (a través de puertos FXS), actúa como un interfaz con la red telefónica pública y PBX tradicionales. Realiza ciertas funciones suplementarias como la detección/recepción de tonos DTMF, generación de timbrado, soporte para funciones avanzadas de llamada e incluso encriptación de la voz para comunicaciones seguras. El hardware utilizado como Gateway suele ser un *router* o conjunto de *routers* de servicios integrados cuyas múltiples tareas (enrutamiento, brindar calidad de servicio, seguridad, etc.) hacen necesario que el dispositivo deba tener amplias capacidades tanto en lo referente al procesador como a la memoria, ya que en éste elemento se realiza la convergencia datos-voz.

Los fabricantes suelen aplicar varios protocolos en lo referente a control del *Gateway*, en este caso se puede nombrar MGCP (*Media Gateway Control Protocol*) y H.323.

Cabe aclarar que el estándar H.323 cuenta con dos versiones; la primera no permitía ofrecer servicios de llamada como espera o transferencia, por lo que los fabricantes estaban obligados a anexar banderas a los paquetes RTP de manera que estos servicios se implementen (Cisco limitaba su campo de acción solo a codecs G.711). Sin embargo al ser estas convenciones propias de los fabricantes existían problemas al querer interconectar redes de diversas marcas.

En el caso de H.323v2, se crearon ciertos parámetros en el paquete H.323 como "abrir y cerrar el canal lógico" (*open/close logical channel*) que permitían alterar ciertos procesos relacionados con la negociación de llamada. Por esta razón el incremento de la cabecera por parte de los fabricantes se hacía innecesario y ya se podían usar varias funcionalidades de llamada, incluso la posibilidad de escoger el tipo de *codec* a usarse en la conversación y solucionar la interconexión de redes de diferentes fabricantes.

La configuración de los *Gateways* no se realiza de forma gráfica, es decir, se lo hace mediante CLI (*Command Line Interface*, en el caso de Cisco) o menú selectivo (por

ejemplo 3COM), introduciendo cierta complejidad en su configuración y administración; además no es aconsejable con estos tipos de *Gateways* tener un gran número de usuarios o troncales analógicas, ya que por cada uno es necesario líneas de configuración, consumiendo recursos del CPU.

Terminales.-Es posible tener varios tipos de terminales como: H.323, SIP, Skinny (propietario de Cisco), o todos; depende de la señalización provista por el Servidor de Llamadas.

La administración general del sistema se la realiza a través del Servidor de llamadas, previa configuración en los respectivos *Gateways*.

El hecho de implementar una solución de voz mediante elementos de Networking como Cisco permite: optimizar la red integrada al tener compatibilidad con la mayoría de protocolos empleados en la red de datos, reutilizar elementos como el *router* trabajando como *Gateway* de voz y datos, además de tener un sistema único de administración de los equipos que conforman la red integrada (en el caso de poseer equipos de un solo fabricante).

5.2.2. SOLUCIÓN HÍBRIDA (IP¬PBX)

Una central telefónica híbrida básicamente es aquella que puede soportar terminales de usuario de diversas naturalezas, sean éstos analógicos, digitales, inalámbricos o IP, conservando su funcionamiento modular. La tecnología y ciertos protocolos de señalización con los que trabajan este tipo de IP-PBX son propietarios del fabricante. Las tareas de configuración, gestión, mantenimiento y monitoreo se hacen a través de software de aplicación (comúnmente bajo OS Windows y Linux) o por terminales de usuario diseñadas para el efecto.

Este tipo de equipo, son desarrollados por empresas especializadas en telecomunicaciones, razón por la cual no presentan un open source (código abierto) para manipular su sistema operativo. La aplicación radica en saber maximizar las funciones que el fabricante pone en consideración en su equipo.

Una central híbrida cumple con todas las capacidades tradicionales de una PBX (y funciones avanzadas creadas por el fabricante); opera a través de tarjetas de función independiente que se interconectan entre sí a través de un back-panel, el cual puede funcionar de manera centralizada (gabinete único) o en arquitectura distribuida (varios gabinetes interconectados).

DESCRIPCIÓN TECNOLÓGICA

Los principales componentes de una central telefónica híbrida se enumeran a continuación:

- Un sistema central de control (*Call Server*)
- Tarjetas, interfaces, radio bases o cualquier dispositivo que permita conectividad a troncales analógicas y digitales de las redes públicas y a los terminales de usuario de todo tipo, conocido este conjunto como "*Media Gateway*,". El Media Gateway puede funcionar como parte de un gabinete principal o de forma remota interactuando con el sistema central de control.
- Terminales.-Teléfonos analógicos, digitales, inalámbricos, terminales IP (H.323 o SIP), softphones.

El sistema central de control o servidor de llamadas ("Call Server, CS").- Es un programa que actúa prácticamente como el cerebro de la central telefónica. A través del sistema central de control se puede: configurar los atributos, propiedades y limitaciones de cada elemento del sistema, agrupar extensiones, permitir o no salida de llamadas, horarios de atención, desvíos automáticos de llamada, etc.

El *Call Server* recibe la información de eventos y estado del sistema vía IP (a través del *Media Gateway*) y toma decisiones según la programación efectuada por el administrador, luego envía estas órdenes por el mismo enlace al Media Gateway para su ejecución. Tanto el Call Server como el Media Gateway pueden compartir o no un solo gabinete; generalmente para redes grandes de voz el *Call Server* es un equipo separado (servidor), del cual se aprovecha su alto rendimiento y capacidad de almacenamiento (por ejemplo: guías de voz, buzones de mensajería, reportes, etc.)

Las tareas básicas del sistema central de control pueden resumirse en:

Administración y gestión de llamada. Aplicaciones enfocadas al usuario: modo hotel, modo negocio, Call Centers, etc. Para VoIP: Servidor DHCP y gatekeeper.

El hardware que puede contener al Call Server puede ser una tarjeta diseñada para el efecto que va montada en un slot normal de un gabinete de la PBX o un computador, que toma el nombre de servidor de aplicaciones; la primera opción es la más común pues facilita la conexión con el *Media Gateway*. Cabe recalcar que la conexión que se utiliza entre el *Call Server* y otros dispositivos (*Media Gateway*) se hace generalmente a través de enlaces IP o enlaces dedicados (E1).

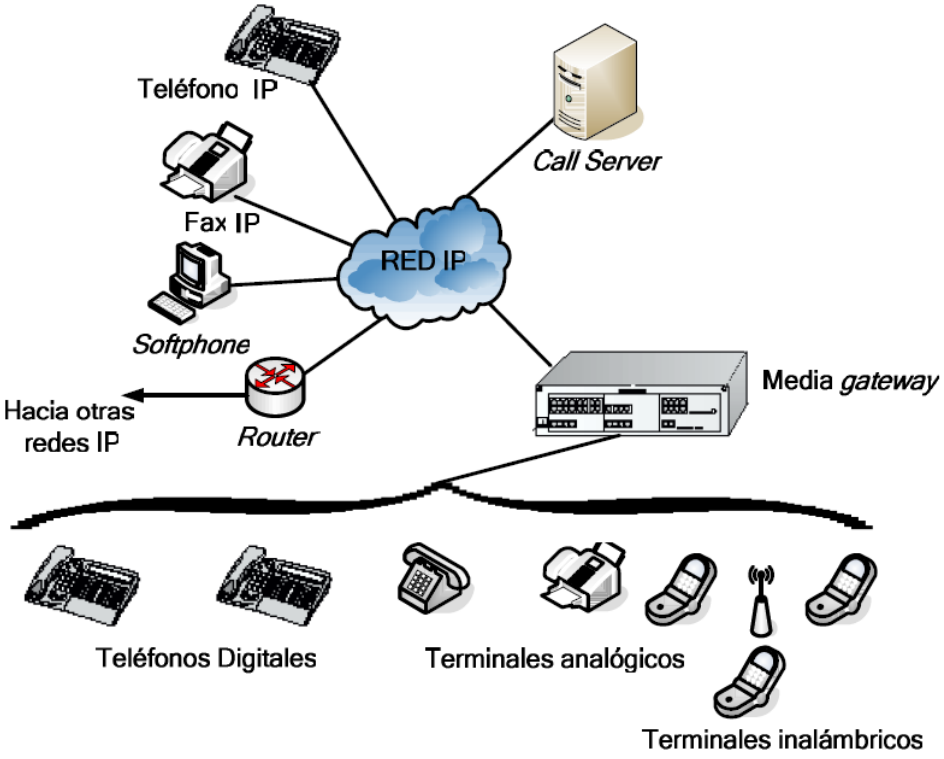


Figura. 5.2. Sistema telefónico básico con Central Híbrida

La figura podemos observar la arquitectura básica en la que están conectados un *Call Server* y un *Media Gateway*, comunicados a través de una red IP, entendiéndose por red IP una red de datos de área local.

Cabe mencionar que el *Call Server* no puede trabajar por sí solo, necesita del Media Gateway para monitorear el sistema y ejecutar sus instrucciones; es decir no es posible

implementar VoIP en la LAN únicamente a través del *Call Server* como en el caso del Servidor de Llamadas en la tecnología de networking (por ejemplo: Cisco, 3COM, etc.).

El Media Gateway (MG).- Actúa como interfaz entre los usuarios finales y las redes públicas tanto analógicas como digitales. Cada tarjeta tiene una tarea bien definida y se conecta con las demás a través del back-panel del gabinete que contiene al conjunto de tarjetas; las aplicaciones y necesidades del sistema es proporcional al número de tarjetas así como al tamaño del gabinete. Ciertos sistemas pueden necesitar extensiones o incluso nuevos gabinetes para cumplir con las exigencias de la red de voz.

El *Media Gateway* ejecuta las instrucciones del *Call Server* y permite la conexión con la PSTN. Principalmente realiza las funciones de DSP (Procesamiento Digital de Señales), implementadas a través de tarjetas hijas (llamadas DSP, las cuales son pequeños módulos que se montan sobre tarjetas normales de la PBX), fabricadas exclusivamente para este propósito, prestando alto rendimiento al sistema. Aplicaciones especificas, como guías de voz, mensajes de operadora, RAS (Sistema de acceso remoto), etc. al igual que los DSP generalmente se encuentran en estas tarjetas.

Actualmente, las centrales híbridas soportan conexión con las siguientes redes públicas:

- Redes digitales: ISDN, E1/T1, *tie lines* (líneas dedicadas, 64 kbits/s).
- Redes analógicas: Generalmente *loop-start* y *ground-start* sin embargo. algunos fabricantes ocupan líneas E&M (principalmente para conexión entre PBXs).

Dependiendo de las necesidades de la organización, varios *Gateways* pueden operar de manera remota bajo un solo sistema central de control. La conexión es básicamente igual que en el caso de trabajar en un ambiente local; sin embargo en estas conexiones el intercambio de información entre el *Call Server* y los *Media Gateway* remotos debe atravesar una red WAN. A continuación se describe el entorno descrito.

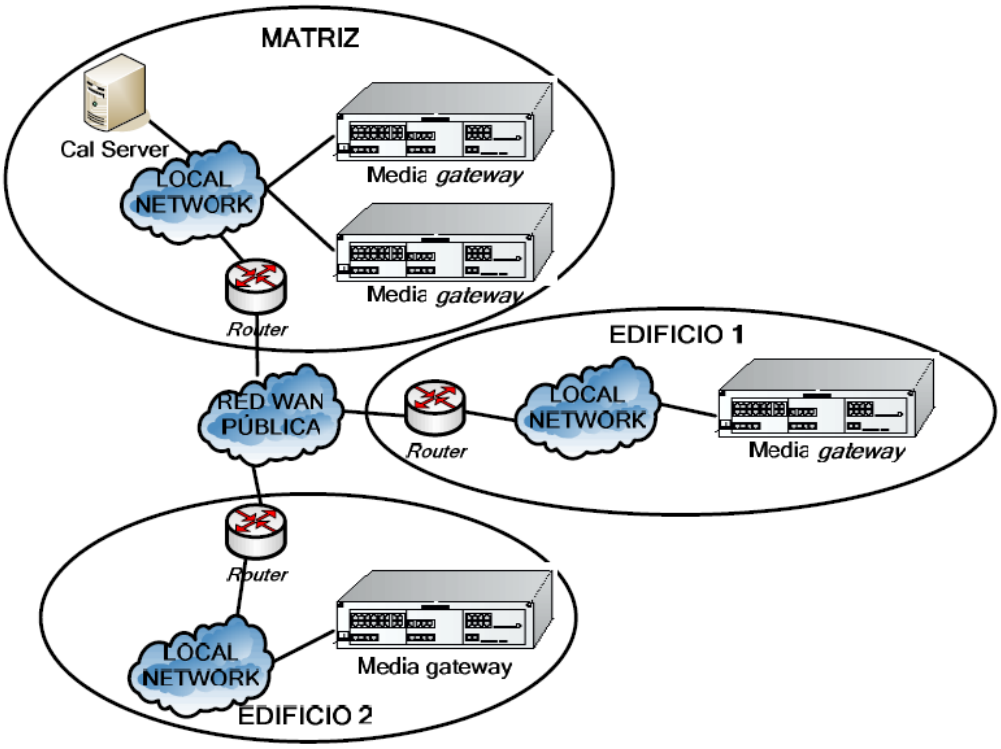


Figura. 5.3. Arquitectura de un Call Server y Media Gateway remotos

Terminales.- Los terminales telefónicos IP y digitales de las centrales híbridas trabajan con protocolos propietarios; es decir una PBX de este tipo trabaja solo con teléfonos del mismo fabricante. Esto inicialmente puede contar con varios puntos negativos, sin embargo permite al constructor proveer aplicaciones exclusivas al usuario. Finalmente muchos fabricantes suelen incluir instaladores de *softphones* propietarios; la dirección IP para los terminales puede obtenerse dinámicamente del *Call Server* si éste está trabajando como un servidor DHCP.

5.2.3. SOLUCIÓN MEDIANTE SERVIDORES

Un servidor de comunicaciones PC-PBX es un sistema telefónico cuya arquitectura física o hardware está basada en la tecnología de un computador personal. Las diferentes funcionalidades de la PC-PBX se implementan a través de diversas tarjetas de expansión PCI (*Peripheral Component Interface*); el control del sistema telefónico y su configuración se realiza por medio de aplicaciones instaladas en el procesador.

DESCRIPCIÓN TECNOLÓGICA

Existen diversas empresas que ocupan este enfoque tecnológico para entregar soluciones de voz. Las tarjetas utilizadas tienen funcionalidades muy similares a las descritas en las IP-PBX y el número de las mismas por servidor depende de varios factores como: el número de usuarios, capacidades del servidor (principalmente el procesador, la fuente de energía, la memoria RAM y el disco duro), aplicaciones y servicios que presta la tarjeta.

La elección de la Unidad Central de Proceso (CPU) depende de su velocidad (proporcional al número de abonados; por ejemplo, un sistema pequeño de hasta 10 usuarios puede trabajar con un procesador de 700 MHz), y la capacidad de su Unidad de Punto Flotante (FPU); esto último debido a que todos los pasos que conlleva la ejecución de una conferencia se representan como procesos matemáticos cuya prontitud se traduce en eficacia del sistema.

La memoria del procesador es dividida y utilizada por las tarjetas en procesos propios, como por ejemplo información sobre enrutamiento, gestión y control de llamada, tarificación, etc. Finalmente el uso del disco duro se incrementa según las aplicaciones del sistema, en el mismo se graban los archivos de sonido (.wav), éstos pueden ser los mensajes utilizados en el IVR, música de espera o incluso grabación de las conversaciones.

Los conectores PCI no son iguales y la diferencia radica en dos aspectos, el voltaje (3,3 y 5V) y el número de bits de trabajo (32 y 64 bits). Si bien generalmente los *motherboards* de los servidores vienen con conectores para ambos voltajes, algunos suelen incluir solamente versiones de 5V. La figura 1.29 muestra los conectores anteriormente descritos

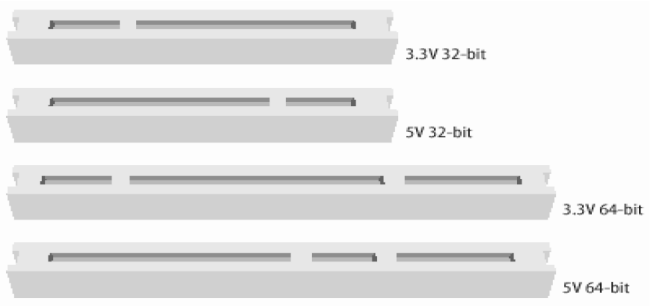


Figura. 5.4. Identificación visual de slots PCI52

En cuanto al sistema operativo bajo el cual trabaja el servidor existen opciones tanto bajo Windows como Linux, en el caso de Windows las PC-PBX suelen implementarse como aplicaciones propietarias del fabricante. En el caso de Linux se utiliza Asterisk, un software abierto que emula una central telefónica permitiendo ocupar todas o al menos la mayoría de las capacidades de las centrales comerciales, incluso incrementando las capacidades del servidor a través de programas externos.

Un servidor de comunicaciones puede conectarse a:

- Línea analógica convencional (POTS)
- TDM (Time division Multiplexing)
- Línea digital RDSI
- Accesos primarios RDSI (E1/T1)
- Canal de voz sobre IP
- Redes heterogéneas (PBX tradicionales)

Debido a esto el servidor trabaja tanto con terminales IP (lo más recomendado) como con terminales analógicos (teléfonos o fax) que pueden conectarse directamente a puertos analógicos de las tarjetas o utilizar un adaptador.

Las tarjetas utilizadas en los servidores de comunicación se pueden dividir en dos grupos principales que se describen a continuación.

Tarjetas de voz: Dentro de las tarjetas de voz se pueden agrupar a todas aquellas que entregan conectividad hacia la red telefónica del proveedor local PSTN a través de puertos analógicos y que además son capaces de realizar funciones de gestión de la voz (digitalización, compresión, grabación y reproducción de la conversación principalmente) y control del establecimiento, transcurso y terminación de llamada (generador de tonos de timbrado, espera, ocupado, llamando, etc. y receptores/generadores de tonos digitales de multi¬frecuencia, DTMF), así como la conectividad física hacia las extensiones (de tipo analógico, a través de conectores RJ-11).

Dependiendo de la aplicación estas tarjetas suelen construirse de forma exclusiva para recibir troncales (o puertos FXO) o solo para entregar extensiones (puertos FXS); sin embargo ciertas tarjetas misceláneas o "mix" entregan tanto puertos troncales como para extensiones.

La distancia que puede existir entre la central y el terminal del usuario son relativamente grandes, alrededor de 1 Km. Normalmente; sin embargo a través de tarjetas especiales, que utilizan fuentes de alimentación extra, para compensar la disipación de energía en la señal de voz esta distancia puede incrementarse a 5 Km. o más. Esto permite dar servicio a edificios de una misma organización como por ejemplo un campus o un hospital con el mismo servidor y el mismo plan de numeración.

En el caso de requerirse un gran número de extensiones analógicas, los servidores utilizan bancos de canales o *switches* de extensión, los cuales permiten que un circuito digital (T1/E1, por ejemplo) sea demultiplexado en varios circuitos analógicos y viceversa; dicho de otra forma un banco de canales permite conectar un teléfono analógico a un sistema a través de líneas digitales como un E1. La siguiente figura muestra la función de un *switch* de extensión.

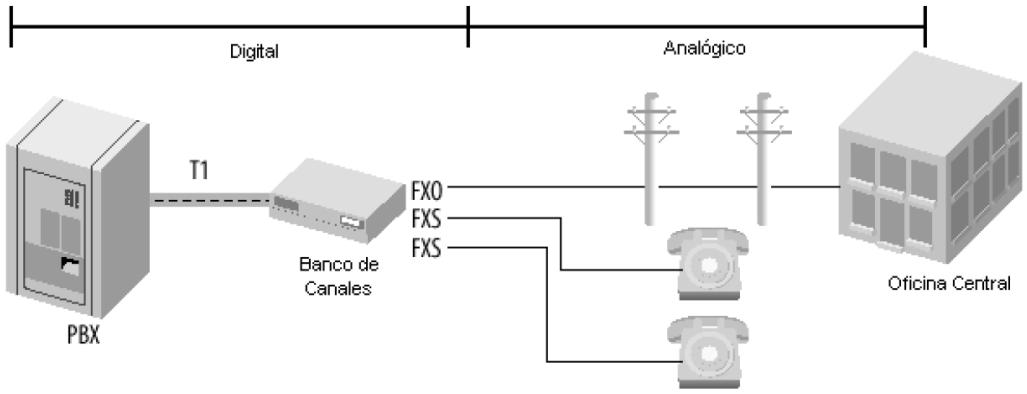


Figura. 5.5. Switch de extensión

Tarjetas para acceso digital: Cuando se requieren soluciones medias y de alta demanda o si se requiere conectividad digital, las tarjetas de acceso digital son la solución. El protocolo base para estas tarjetas es el ITU-T Q.931 (Especificación de la capa 3 de la interfaz usuario-red de la ISDN para el control de la llamada básica, acceso PRI y BRI); sin embargo suelen incluir soporte para otros protocolos como E1 y T1. Estas tarjetas

actúan como interfaces entre el proveedor de canales digital y la PC-PBX, y esta última con otros dispositivos (por ejemplo, un banco de canales o un servidor remoto).

Para hacer posible la ToIP basta con tener una conexión a la red de datos, El PC-PBX soporta el protocolo de inicio de sesión (SIP), H.323 (protocolo de comunicación de multimedia) y en el caso de las PC-PBX que utilizan Asterisk el protocolo propietario de *trunking* para intercambio de información cifrada entre servidores conocido como IAX (*Inter Asterisk Exchange*), así como los estándares de voz más comunes:

- Para digitalización y compresión de la voz: G.711 (Modulación por codificación de pulsos, PCM) y G.729 (Predicción algebraica conjugada de código lineal, CS-ACELP).

- Para cancelación de eco (necesaria para la interacción con la PSTN): G.165 (Protocolo de eliminación automática de eco) y G.168 (compensadores de eco en redes digitales).

- Para soporte de fax sobre IP (FoIP): se utiliza el protocolo T.38 (Facsímile sobre PSTN a 14400 bits/s) o ciertos fabricantes adjuntan tarjetas exclusivas con puertos analógicos para facsímiles.

Varios son los tipos de terminales IP posibles con servidores: teléfonos IP nativos, terminales que se conectan directamente a la red, teléfonos analógicos con adaptadores para paquetizar su señal y los softphones; también es posible tener terminales analógicos conectados a puertos FXS del servidor.

5.3. SELECCIÓN DE LA SOLUCIÓN

Para el diseño de la nueva red de telefonía se considerará como base las soluciones tecnológicas provistas por Cisco Systems, debido tanto a la configuración propuesta para el rediseño de la red de datos (la marca de los dispositivos, el modelo de capas y los protocolos con que trabaja) como a la amplia difusión y fiabilidad de esta marca a nivel global como local.

Los pasos considerados para completar el esquema del nuevo sistema telefónico son los siguientes:

- Selección del modelo de procesamiento de llamada y tamaño del cluster
- Selección del Call Server (CallManager para Cisco).
- Métodos de redundancia
- Selección de la plataforma del Gateway
- Mensajería Unificada
- Terminales
- Ubicación de los equipos dentro de la red datos
- Costos

5.3.1. SELECCIÓN DEL MODELO DE PROCESAMIENTO DE LLAMADA Y TAMAÑO DEL CLUSTER

El modelo de procesamiento a utilizarse para este diseño es del tipo centralizado; el utilizar varios *cluster* dentro de la red Municipal es innecesario (por el número de usuarios, y por estar distribuidos principalmente en la matriz) y significaría un aumento de costo importante. Al existir un *cluster* único ubicado en un punto de la red, éste será fácilmente monitoreable y gestionará todo el sistema.

Con esta solución se puede prever a futuro el uso de Gateways independientes de voz para enlazar las dependencias con mayor densidad de usuarios a la WAN, lo cual habilitaría un control remoto; esta condición de los equipos se conoce en Cisco como SRST (*Survivable Remote Site Telephony*) característica propia de ciertos Gateway de voz que permiten incluso que el mismo actúe como CallManager de redundancia en caso de caída del enlace o del Call Server.

Inicialmente se buscará determinar el número de servidores necesarios para soportar la cantidad total de extensiones requeridas, a través de la determinación del tamaño del cluster.

5.3.2. MÉTODOS DE REDUNDANCIA

La solución de Cisco, para telefonía permite implementar redundancia, elevando de este modo, altamente la disponibilidad del sistema, en un esquema redundante, es necesario implementar un servidor *Publisher*, que es el encargado de mantener y administrar la base de datos de las configuraciones de los usuarios que acceden al servicio, además de publicarla hacia todos los *Suscriber* anexados al *cluster*, este último tipo de servidor, es el encargado de brindar procesamiento a las llamadas dentro de sistema, como podemos observar en la siguiente figura encontramos los diferentes tipos de configuraciones redundantes, su selección depende del número de usuarios, estas van desde las que comparten un mismo servidor para *Publisher* y *Suscriber backup*, hasta las que poseen un servidor para *Publisher* dedicado, con *Suscribers* en configuraciones redundantes 1:1 y 2:1.

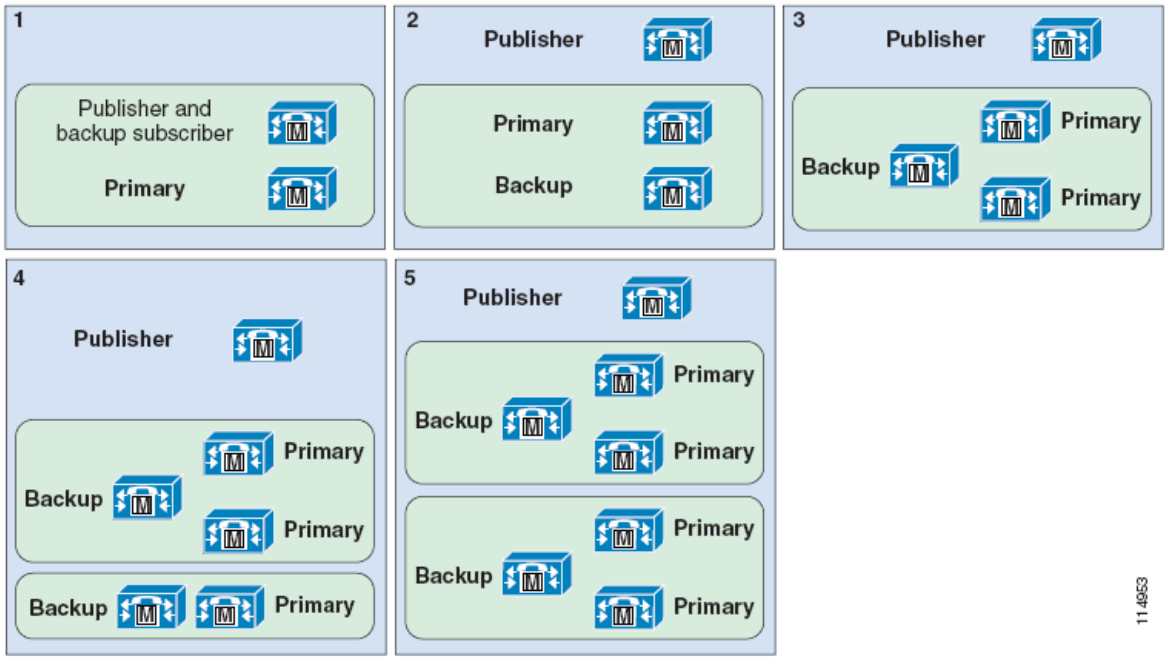


Figura. 5.6. Configuraciones redundantes.

Para cubrir las necesidades específicas del Municipio de Ambato (123 extensiones), es recomendable el uso de tres servidores un *Publisher*, un *Suscriber* principal y uno de redundancia; sin embargo por el número de usuarios se puede integrar las funciones del servidor *Publisher/TFTP* con el *Suscriber* de *backup*, con lo cual se obtendría un *cluster* de solo dos servidores (los servidores dedicados para actualizaciones o descargas TFTP suelen recomendarse para sistemas con 1250 usuarios en adelante). Además cabe aclarar

que el sistema puede partir con el servidor principal sin necesidad de implementar el *cluster* completo, por lo cual el otro servidor se lo considerará como opcional.

Esta implementación de redundancia se hará a través de un servidor en Stand By de iguales características y programación que el *Suscriber* principal, de este modo se logra mayor eficiencia y disponibilidad del sistema de telefonía.

5.3.3 SELECCIÓN DEL SERVIDOR

Una vez determinado el tamaño del *cluster* se debe definir qué tipo de servidores conformarán el mismo (dependiendo de la capacidad del sistema y de la frecuencia de llamadas). Los servidores vienen clasificados según sus características y límites de hardware; tomando en cuenta especialmente procesamiento y capacidad de almacenamiento de datos. La siguiente tabla muestra la clasificación que da Cisco a sus servidores.

Tabla. 5.1. Tipos de servidores

Tipo de servidor	Modelo de Servidor Cisco	Características
Servidor Standard (no alta disponibilidad)	MCS 7815, MCS 7816, o equivalente	• Un procesador • Una fuente de poder • No soporta disco duro RAID SATA
Servidor Standard de Alta disponibilidad	MCS 7825 o equivalente	• Un procesador • Una fuente de poder • Controlador SATA con soporte RAID 0/1
Servidor de Alto rendimiento	MCS 7835, MCS 7845, o equivalente	• Múltiples procesadores • Múltiples fuentes de poder • Múltiples controladores SCSI (SAS) con RAID 1

Siendo el *CallManager* un punto crítico para el funcionamiento del sistema de voz, es recomendable proveer al servidor con soporte de SCSI RAID y UPS, de manera de poder gestionar los datos del sistema en más de un disco duro y proveer mecanismos de redundancia en caso de fallas de energía, respectivamente.

Las características de un "Servidor de alto rendimiento" se usan en sistemas de requerimientos extensos tanto a nivel de funcionalidad como de número de usuarios (10,000); este tipo de servidor sería subutilizado en el sistema propuesto, de manera que un "Servidor estándar de alta disponibilidad" es el indicado para el Municipio de Ambato.

El *CallManager* lleva registros de todos los dispositivos de la red e interactúa de diferente forma con los mismos, de manera que el trabajar con un teléfono IP no es lo mismo que gestionar un enlace PRI, o en otras palabras cada dispositivo ocupa recursos de procesamiento y memoria del servidor según su necesidad; dicho esto cada servidor soporta un número máximo de teléfonos IP y un número máximo de dispositivos, lo que se indica en la siguiente tabla.

Tabla. 5.2. Dimensionamiento del Servidor[4]

Plataforma del Servidor	Máximo # de Usuarios [1]	Servidor de alta disponibilidad	Servidor de alto rendimiento
Cisco MCS 7845	7500	Yes	Yes
Cisco MCS 7835	2500	Yes	No
Cisco MCS 7825	1000	Yes	No
Cisco MCS 7815 or MCS 7816 [2]	300[3]	No	No

1. Una plataforma de servidor que no es de alta disponibilidad puede soportar un número máximo de 500 teléfonos IP en una instalación no redundante.
2. Los servidores MCS 7815 y MCS 7816 soportan solamente redundancia 1+1 (máximo 2 servidores), y no pueden ser miembros de un cluster que contenga otros servidores.
3. El servidor MCS 7815 soporta un máximo de 500 usuarios.

El servidor seleccionado es el MCS-7825 por ser el que más se ajusta a los requerimientos propuestos. Y la versión del *Call Manager* a utilizarse será la 7.0 que es la última que ha liberado Cisco para esta solución, a continuación se muestran las características del servidor seleccionado.

Tabla. 5.3. Características del servidor MCS7825

Componente	Valor
Numero de parte:	MCS7825I3-K9-CMC1
Pre cargado:	Cisco Unified Communications Manager 7.0
OS:	Incluido
Procesador:	Single Intel Dual Core 3050 2.13 GHz
Memoria:	2-GB (dos 1-GB) PC2-5300 *error-correcting-code* (ECC) *double-data-rate* 2 (DDR2)
Discos duros:	Dos 160-GB SATA 2.5-inch *cold-swap drives* configurados usando *Redundant Array of Independent Disks* (RAID) 1
Administración remota:	IBM *Remote Supervisor Adapter* (RSA) II *Slimline*: Soportado pero no incluido

[4]Fuente: Cisco Unified Communications Solution Reference Network Design (SRND)

5.3.4. SELECCIÓN DE LA PLATAFORMA DEL GATEWAY

Cuatro ítems agrupan los requerimientos que utiliza Cisco para selección del Gateway:

Requerimientos de capa núcleo

Se refiere a un conjunto de capacidades que todo Gateway en un entorno de telefonía IP debe cubrir, como son:

- Manejo DTMF (*Dual Tone MultiFrequency*).- Específicamente el Gateway debe ser capaz de separar los paquetes de voz de los dígitos DTMF y enviar estos últimos como señalización a través del canal de control considerado para el Gateway (H.323, o MGCP), en lugar de que estos dígitos sean transmitidos junto con la conversación; esta técnica conocida como señalización fuera de banda es recomendada si se utilizan *codecs* de baja tasa de bit (redes WAN) debido al peligro de pérdida o distorsión de señal que tienen los tonos DTMF en estos escenarios.

- Soporte para servicios suplementarios.- Los servicios suplementarios se refieren básicamente a funciones básicas de telefonía, tales como: espera, transferencia y conferencias.

- Soporte para Fax/módem.- Permite utilizar fax en un entorno IP; la imagen del fax se convierte de una señal analógica a datos digitales para transmitirse por la red de conmutación de paquetes.

- Soporte para redundancia de *CallManager*.- El Gateway debe tener la capacidad de seleccionar de forma transparente el servidor de respaldo una vez que el principal falla.

Protocolos del Gateway

Cisco Unified CM, Liberación 3.1 y posteriores soporta los siguientes protocolos:

• H.323

• *Media Gateway Control Protocol* (MGCP)

Cisco Unified CM Liberación 4.0 y posteriores soporta además:

• *Session Initiation Protocol* (SIP) en el lado de las troncales.

La implementación de las troncales SIP ha sido ampliada en el Cisco Unified CM liberación del 5.0 hasta la 7.x para soportar más funcionalidades.

La selección del protocol depende de los requierimientos específicos de cada implementación. Para la configuración del Gateway MGCP, es preferido sobre H.323 o SIP debido a su simplicidad. De otro modo H.323 o SIP es preferido sobre MGCP, debido a la robustez de las interfaces soportadas. *Simplified Message Desk Interface* (SMDI) es un estandar para integración de sistemas de mensajes de voz a PBX. Conectándose a un sistema de correo de voz vía SMDI y usando una interfaz FXS o digital T1 PRI se requiere el protocolo SCCP o MGCP debido a que los dispositivos H.323 o SIP no identifican la línea específica usada de un grupo determinado de puertos.

Debido a la mayor funcionalidad que brinda el protocolo H.323 y en vista a que nuestra implementación no posee dispositivos para mensajes de voz que trabajen con SMDI, el protocolo seleccionado será H.323.

Capacidades específicas del Gateway

Las capacidades específicas del Gateway se refieren básicamente al conjunto de interfaces con que trabajará el dispositivo. La tabla 5.5. muestra el número máximo de interfaces analógicos y digitales que pueden adicionarse a través de módulos o tarjetas a las diferentes plataformas de Gateways de voz de Cisco.

De acuerdo a esta tabla debemos cubrir los requerimientos de interfaces del Gateway de voz analizados anteriormente, (5 puertos FXO y 1 interfaces PRI como mínimo).

Además para definir cuál de estas plataformas se ajusta de mejor forma al sistema telefónico propuesto se compara el número de llamadas simultáneas que cada una de ellas puede soportar.

La siguiente tabla muestra el número de llamadas simultáneas (sin exceder el 75% de uso del CPU) para las diversas plataformas de Gateway Cisco considerando el modo de "Límite hacia la red WAN", y el uso o no de comunicación segura (SRTP, Secure Real-Time Transport Protocol).

Tabla. 5.4. Número de llamadas simultáneas por plataforma de Gateway Cisco

	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851	Cisco 3825	Cisco 3845
Sin encriptar	32	48	88	150	290	330
SRTP	32	41	80	130	240	280

Un Gateway de voz Cisco puede utilizarse en tres modos, las cuales se resumen a continuación:

- Standalone.- Se consideran solamente enlaces del tipo *Gigabit ethernet* (entorno LAN) y además se asume que por el Gateway solo existe tráfico de voz, siendo innecesarias políticas de QoS.

- Límite hacia la red WAN.- Se consideran enlaces del tipo T1/E1; se añaden algunas políticas de calidad de servicio, pues se considera que por el Gateway fluye también tráfico de datos.

- Límite hacia la red WAN con compresión de la cabecera RTP (CRTP) incluye el funcionamiento del Gateway de voz en modo límite hacia la red WAN, con la modificación de que se añade una compresión de la cabecera RTP para compensar las demoras en el enlace WAN.

En el diseño desarrollado, el Gateway trabajará en el modo "Límite hacia la WAN" por el tipo de enlaces E1/T1 que se piensa manejar; dejando abierta la posibilidad de manejar tráfico de datos a través de estos enlaces.

Tabla. 5.5. Número máximo de interfaces por Gateway

	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851	Cisco 2691	Cisco 3825	Cisco 3845
FXS	16	28	52	52	12	52	88
FXO	16	24	36	36	8	36	56
E&M	8	12	12	12	4	16	24
DID	8	24	32	32	8	32	48
Puertos BRI	4	20	20	20	4	20	32
Puertos T1/E1	1	12	12	12	6	16	24
Canales T1	24	288	288	288	144	384	576
Canales E1	30	360	360	360	180	480	720

Finalmente se puede determinar que la plataforma para el Gateway de voz más indicada para el proyecto, de entre las que ofrece Cisco es el Gateway 2811, el cual soporta el protocolo H.323, siendo posible utilizar interfaces *Gigabit Ethernet*, FXS, FXO ; además de los *codecs* estandarizados más comunes en la telefonía IP.

El Gateway 2811 tiene capacidad para 24 puertos FXO y 12 enlaces T1/E1, soporta hasta 48 llamadas simultáneas hacia la PSTN (inicialmente el número máximo de llamadas considerado en el diseño es de 17 simultáneas), u 41 en el caso de utilizar encriptación. Soporta redundancia de servidores y SRST en el caso de utilizarse en sitios remotos.

5.3.5. MENSAJERÍA UNIFICADA

Cisco considera tres soluciones para el uso de mensajería unificada, que se definen a continuación:

• *Cisco Unity*: Esta es una solución altamente escalable que cubre las necesidades de organizaciones bastante amplias y provee, opciones de mensajería unificada de voz e integración, que trabaja con Microsoft Exchange y Domino Lotus.

• *Cisco Unity Connection:* Esta opción mensajería integrada, reconocimiento de voz, y reglas de transferencia de llamadas dentro de un sistema fácil de administrar para organizaciones medianas.

• *Cisco Unity Express:* Esta opción inicialmente está pensada para sistemas de número de usuarios medio y bajo (120 usuarios máximo), pero es utilizada también para aplicaciones distribuidas de correo de voz y operadora automática. En un entorno oficina principal-sucursales, en lugar de manejar un sistema centralizado, cada una de las oficinas remotas utiliza su propio Cisco Unity Express, estando éstos conectados entre sí (a través de una red WAN) formando un sistema de funcionamiento en conjunto. Esto suele implementarse en especial cuando se carece de un enlace WAN de ancho de banda suficiente para transmitir los mensajes desde un servidor centralizado o la confiabilidad del enlace oficina principal – sucursal no es lo suficientemente alta; en este tipo de ambiente los mensajes son descargados desde el Cisco Unity Express local.

En el caso de servidores de voicemail de otros fabricantes Cisco ofrece el interfaz SMDI (*Simplified Message Desk Interface*), que permite la conexión de un servidor de correo de voz estándar con el sistema de voz IP.

En el caso del Municipio, al no existir un sistema de mensajería de voz y peor aún un servidor con estos fines, no será necesario establecer procesos de migración de buzones de voz o interfaces para interactuar con el sistema actual. Se debe en cambio seleccionar el equipo de mensajería que más se ajuste a las necesidades del Municipio, considerando las siguientes topologías para implementación de mensajería:

- Mensajería de lugar único (*Single-Site Messaging*).- Este modelo se aplica principalmente en redes LAN o entornos (como un campus) en los cuales es necesario el uso de enlaces MAN de alta velocidad; en todo caso la característica principal de este modelo es la ausencia de clientes remotos.

- Mensajería Centralizada (*Centralized Messaging*).- De igual manera que el modelo anterior los componentes y equipos para la implementación de mensajería están en el mismo lugar, sin embargo en este modelo los usuarios pueden ubicarse de manera local o remota

- Mensajería Distribuida (*Distributed Messaging*).- Básicamente son varios sistemas de mensajería *single-site* con un *backbone* de mensajería común. Cada sitio tiene su sistema de mensajería completo y con todos los componentes necesarios para cubrir las exigencias de todos los usuarios y los mensajes viajan de un sitio a otro a través del *backbone* de mensajería con políticas propias de enrutamiento. Este tipo de modelo está diseñado para uso en entornos de gran número de usuarios y grandes distancias entre las oficinas de la organización.

El modelo de mensajería que se ajusta a la Municipalidad de Ambato, es el modelo de "mensajería centralizado" que utilizará un solo servidor cargado con *Unity Connection* (el *Unity Express,* soporta hasta 120 usuarios estando al límite para nuestro caso dificultando la escalabilidad) que brindará mensajería de voz unificada para todos los usuarios y permitirá el acceso a beneficiarios remotos (a diferencia del *single-site messaging*).

A continuación se definen las características de hardware del equipo en el cual funcionará el *Cisco Unity Connection*; para este fin Cisco permite el uso de tres plataformas las cuales se describen en la siguiente tabla.

Tabla. 5.6. Plataformas del Cisco Unity Connection

Características	Plataforma 1	Plataforma 2	Plataforma 3
Plataforma del hardware	MCS7825H3-K9-UCB1/ MCS7825I3-K9-UCB1	MCS7835H2-K9-UCB1/MCS7835I2-K9-UCB1	MCS7845H2-K9-UCB1/ MCS7845I2-K9-UCB1
Número total de puertos disponibles	24	48	72
Número total de usuarios disponibles	1000	3000	7500
Número total de contactos disponibles en el directorio corporativo	10000	10000	10000

Ya que se considera el mismo número de extensiones propuestas para el uso de mensajería unificada (123), de acuerdo a la tabla la "plataforma 1" es la que se ajusta a los mencionados requerimientos, el equipo que se implementará será MCS7825I3-K9-UCB1, de iguales características de hardware al descrito para el *Call Manager*.

5.3.6. TERMINALES

La selección del terminal indicado para un sistema telefónico se basa principalmente en las necesidades del usuario, no solamente respecto a los servicios y funcionalidades que éste utilizará del sistema sino también de su comportamiento, es decir la cantidad de tráfico que comúnmente genera el beneficiario telefónico.

Otros parámetros que suelen tomarse en cuenta es la jerarquía de las autoridades de la organización, las necesidades de comunicación que tiene un empleado para cumplir con su trabajo y el estado actual del cableado (puntos de red disponibles).

Considerando las circunstancias antes mencionadas, el terminal seleccionado para el usuario normal del nuevo sistema será el teléfono Cisco IP 7912G. Por ende el nuevo sistema partiría con 84 terminales 7912G, como se analizó en el capítulo III.

Los 31 terminales IP ejecutivos serán teléfonos IP Cisco 7960G, ya que son los dispositivos de mejor desempeño en la categoría de rango medio y entregan gran cantidad de funcionalidades.

Para los 2 teléfonos IP para conferencias se seleccionó el equipo Cisco 7936, por sus prestaciones y diseño especialmente concebido para permitir la cómoda interacción de los interlocutores en salas de reuniones.

La consola de operadora, *Cisco Unified CallManager Attendant Console*, desde la versión de *Call Manager* 4.1, viene incluida con el servidor. Requiere un PC cliente, para lo cual, se utilizara el mismo equipo que actualmente se encuentra en la isla de información.

Las máquinas de fax serán reutilizadas.

Finalmente para interconectar las centrales telefónicas analógicas que se mantendrán en las dependencias de Cultura, Hospital, Tránsito y el Camal, se lo hará por medio de adaptadores telefónicos (ATAs) conectados a dichas PBX.

En la siguiente tabla se expone los terminales usados en el diseño del sistema telefónico.

Tabla. 5.7. Terminales del nuevo sistema telefónico

Equipos	Características
 Teléfono IP Normal CISCO 7912G	• Acceso para una sola línea y teclas de función. • Soporta aplicaciones XML hacia la pantalla (Menús). • Acceso a una líneas telefónicas • Switch Ethernet integrado 10/100 Base T conexión vía RJ-45 hacia la LAN. • Indicador de llamada y mensaje de espera. • PoE (Power over Ethernet) plus • Soporta codecs G.711 y G.729 • Soporta estándar SIP
 Teléfono IP Ejecutivo CISCO 7960G	• Diseñado para trabajadores de oficina con altas cargas de tráfico de voz. • Acceso a dos líneas telefónicas (o combinación de líneas y funcionalidades de llamada) • Soporta aplicaciones XML hacia la pantalla (Menús). • Switch Ethernet integrado 10/100 Base T conexión vía RJ-45 hacia la LAN. • Indicador de llamada y mensaje de espera. • PoE (Power over Ethernet) plus • Soporta codecs G.711 y G.729 • Soporta estándar SIP
 Teléfono IP para conferencias CISCO 7936	• Diseñado para conferencias e ideal para salas diseñadas para reuniones de trabajo. • 360º de cobertura de la sala. • Conexión 10/100 Base T vía RJ-45 hacia la LAN. • Acceso a una líneas telefónicas • Soporta codecs G.711 y G.729
 Adaptador analógico CISCO ATA188	• Dos puertos FXS • 1 RJ-45 10/100 BaseT uplink • 1 RJ-45 10/100 BaseT data port • Soporta codecs G.711 y G.729

5.4. ESQUEMA DE LA SOLUCIÓN

La topología general del diseño se visualiza en las siguientes figuras, tanto para la matriz como para el resto de dependencias, el *cluster* estará formado por dos servidores, MCS-7825/I3 con software Cisco *CallManager* 7.0, el uno como Suscriber principal y el otro como Publisher y Suscriber de respaldo que además tiene funciones de descargas TFTP.

Los servidores se conectarán al switch de core, el Gateway de voz 2811 se enlaza con uno de sus puertos fijos al switch de core y también se conecta con la WAN Municipal convirtiéndose en el límite de la red de la matriz, al Gateway se conecta también el enlace E1/PRI de la PSTN, y los puertos analógicos para fax.

El Servidor de Mensajería Unificada Cisco Unity funciona sobre la plataforma MCS-7825/I2 y se ubica de manera centralizada en el mismo switch de core.

En las dependencias municipales que conservarán sus centrales análogas se utilizarán los adaptadores analógicos para poder anexarlas al sistema de telefonía IP.

La capacidad del sistema propuesto puede cubrir hasta 12 puertos E1 y hasta 1000 usuarios de manera que las proyecciones consideradas están cubiertas y superadas, la anexión de estas capacidades y servicios avanzados se facilita gracias a la capacidad del *CallManager* y a la modularidad del Gateway, respectivamente, que pese a inicialmente no brindar toda la capacidad antes mencionada puede ir creciendo de acuerdo a las necesidades emergentes.

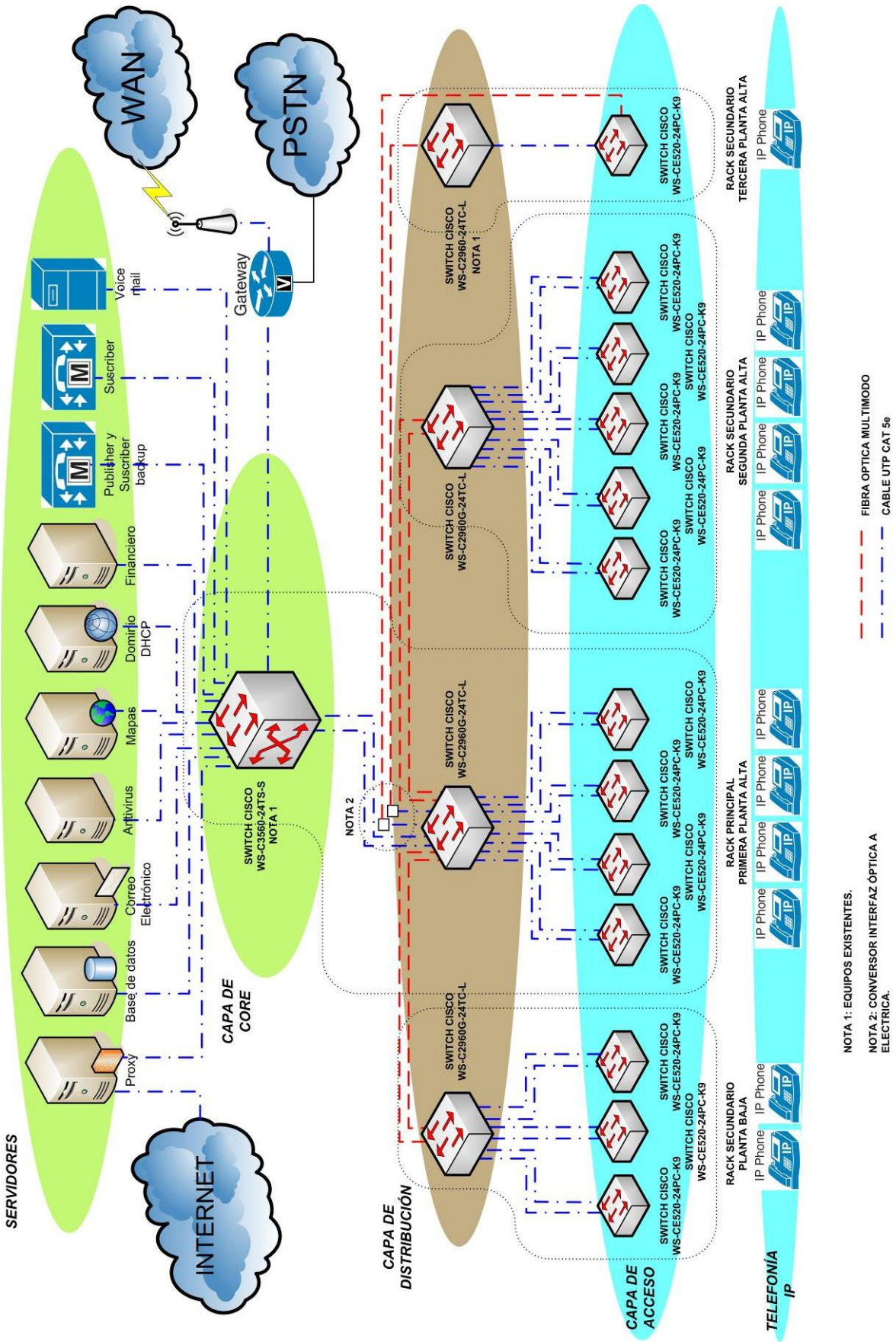


Figura. 5.7. Esquema de la solución de ToIP en la matriz.

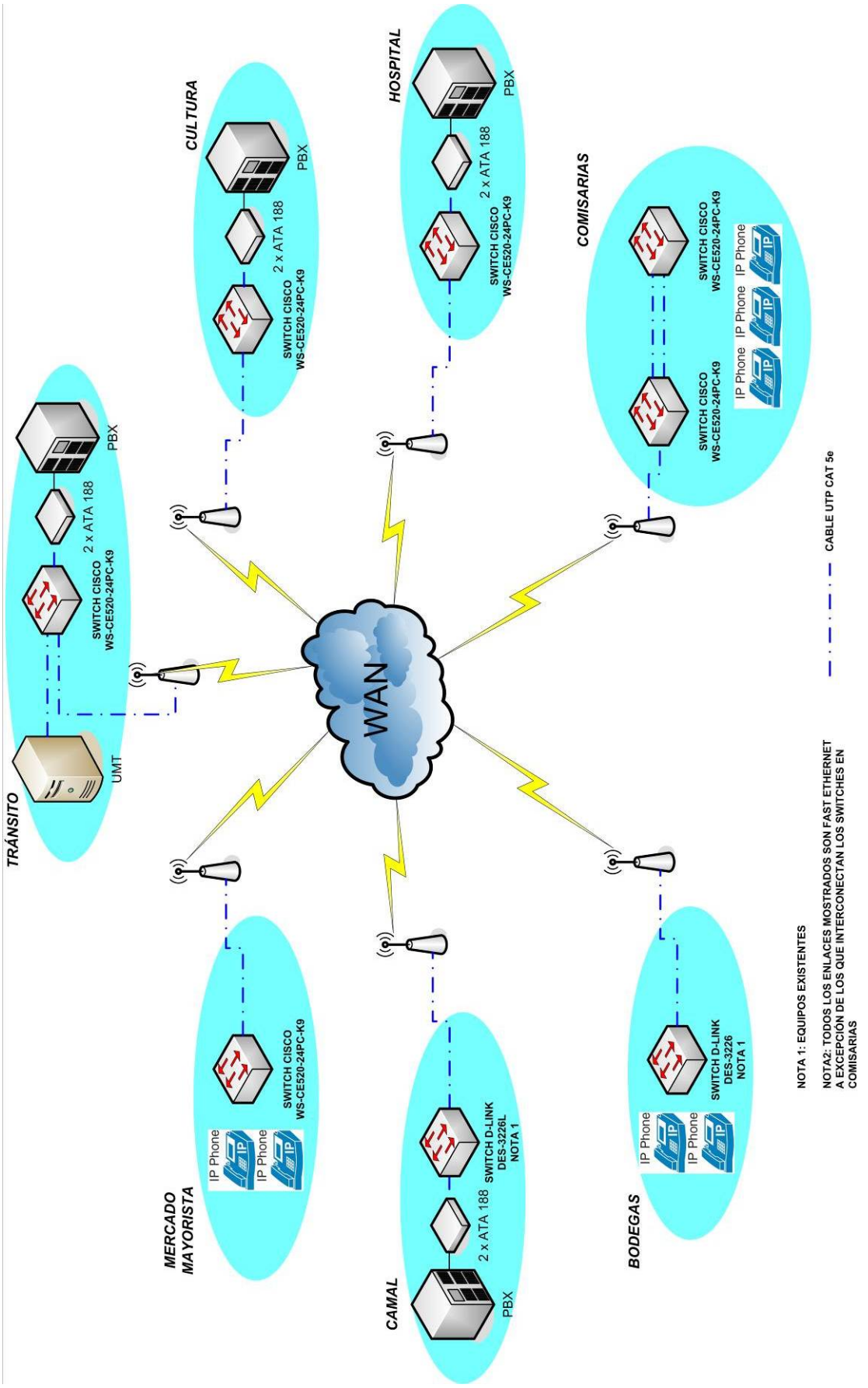


Figura. 5.8. Esquema de la solución de ToIP en las dependencias municipales.

5.5. COSTOS DE LA IMPLEMENTACIÓN

En cuanto a los costos de la implementación vamos a analizar primero los costos que generará el rediseño de la red, que se desarrolló en el capítulo anterior, en la siguiente tabla, se muestran dichos valores.

Tabla. 5.8. Costos para el rediseño de la red de datos[5]

DESCRIPCIÓN	CANT.	P.UNIT	P.TOTAL
RED ACTIVA			$69.348,68
Switch CISCO: WS-C2960G-24TC-L	3	$2.973,19	$8.919,58
Switch CISCO: WS-CE520-24PC-K9	21	$2.627,10	$55.169,10
GE SFP LC connector SX transceiver: GLC-SX-MM	9	$500,00	$4.500,00
External Transceiver D-Link 1000Base-T: DMC700SC	2	$380,00	$760,00
RED PASIVA			$2.373,60
Cable UTP CAT 5e (m)	260	$0,36	$93,60
Patch Cords UTP CAT 5e	96	$5,00	$480,00
Certificación de cableado estructurado	1	$1.500,00	$1.500,00
Ductería para nuevos puntos de red	1	$300,00	$300,00
		TOTAL	**$71.722,28**

Para interacción del *CallManager* con los terminales, Cisco define licencias llamadas "*CallManager Device License - unit*" (CDLu), las cuales permiten la gestión y administración de los terminales por parte del *CallManager*. Dependiendo del terminal IP se necesita una o varias de estas licencias por terminal.

Para el terminal IP 7906G se necesita 2 CDLu. Para el *conference IP* 7936 y convertidores análogos ATA se necesita 3 CDLu. Para el terminal IP 7940G se necesita 4 CDLu. De acuerdo al número total de teléfonos IP se necesita el siguiente número de licencias:

CDLu total = (84 teléfonos 7906G) x 2 CDLu + (5 Teléfonos convencionales fax) x 3 CDLu + (4 adaptadores análogos ATA) x 3 CDLu + (31 teléfonos 7940G) x 4 CDLu

CDLu total = 319

[5] Fuente: Departamento de compras del consorcio SANTOS CMI

Puesto que las CDLu se liberan por paquetes de 10, 100 y 1000 unidades, se necesitan 3 paquetes de 100 CDLu y 2 paquetes de 10 CDLu, para cubrir las 430 CDLu requeridas para el funcionamiento del número de terminales propuestos.

En la siguiente tabla se muestran los costos de los dispositivos, licencias y accesorios considerados en el diseño del sistema de telefonía IP.

Tabla. 5.9. Costos para la implementación de ToIP[6]

DESCRIPCIÓN	CANT.	P.UNIT	P.TOTAL
CISCO CALLMANAGER			**$28.995,00**
HW/SW Server MCS7825-I3, CallManager 7.0 Appliance: MCS7825I3-K9-CMC1	1	$7.000,00	$7.000,00
License CallManager 7.0 7815 Appliance, 1000 seats: LIC-CM7.0-7825	1	$5.995,00	$5.995,00
CallManager Device License - 100 units: LIC-CM-DL-100	3	$5.000,00	$15.000,00
CallManager Device License - 10 units: LIC-CM-DL-10	2	$500,00	$1.000,00
CISCO CALLMANAGER BACK UP			**$12.995,00**
HW/SW Server MCS7825-I3, CallManager 7.0 Appliance: MCS7825I3-K9-CMC1	1	$7.000,00	$7.000,00
License CallManager 7.0 7815 Appliance, 1000 seats: LIC-CM7.0-7825	1	$5.995,00	$5.995,00
CISCO UNITY CONNECTION			**$15.770,00**
Server Cisco Unity Connection 7.0 7825 IBM: MCS7825I3-K9-UCB1	1	$7.000,00	$7.000,00
Unity Connection, 25 users, 24 ports: UNITYCN7-25USR	1	$2.400,00	$2.400,00
One Cisco Unity Connection User: UNITYCN7-VM-USR	98	$65,00	$6.370,00
TERMINALES			**$27.261,00**
Cisco Basic IP Phone: 7906G	84	$175,00	$14.700,00
Cisco Business IP Phone: 7940G	31	$265,00	$8.215,00
Cisco IP Conference Phone: 7936	2	$1.113,00	$2.226,00
Adaptador Análogo: ATA-188	4	$265,00	$2.120,00
GATEWAY DE VOZ CISCO 2811			**$10.295,00**
Cisco 2811 Voice Security Bundle, PVDM2-16, IOS Advanced IP Services, 64 MB Flash/256 MB: DRAM C2811-VSEC/K9	1	$4.195,00	$4.195,00
64-channel fax and voice DSP module: PVDM2-64	1	$3.200,00	$3.200,00
1-Port T1/E1 Voice/WAN with Drop & Insert: VWIC2-1MFT-T1/E1	1	$1.300,00	$1.300,00
4-port FXS or DID VIC: VIC-4FXS/DID	2	$800,00	$1.600,00
		TOTAL	**$95.316,00**

[6] Fuente: Departamento de compras del consorcio SANTOS CMI

CAPÍTULO VI:

6. CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- En la actualidad las organizaciones, se han visto en la necesidad de considerar la utilización de tecnologías para la información y comunicación con el fin de mejorar su desempeño institucional. En este contexto el uso de la Telefonía sobre IP es cada vez más común por las siguientes razones:

  - Explotación más eficiente de los medios de transmisión a través de la conmutación de paquetes.

  - Reducción en costos de mantenimiento al utilizar una única infraestructura de comunicación convergente, en la cual pueden coexistir armónicamente, múltiples servicios.

  - Ahorro en gastos de llamada en entornos matriz – sucursales, al no utilizar los circuitos de la PSTN. La utilización de ToIP en estos ambientes provee comunicaciones cuya tarificación es independiente de la distancia así como del tiempo de conexión.

- Del análisis de la red de datos de la Ilustre Municipalidad de Ambato se obtuvieron los siguientes resultados:

  - El sistema de cableado utiliza UTP Cat5e y fibra óptica multimodo, el mismo no está certificado.

- Los switches y en algunos casos hubs con los que actualmente cuenta la red, no facilitan la convergencia de servicios, pues un su gran mayoría son no administrables (a excepción de los 2 switches D-Link 3226), es decir no brindan funcionalidades de QoS, parámetro necesariamente requerido, para reducir los efectos nocivos que puede encontrar la voz en un entorno de conmutación de paquetes, como son: retardo, jitter, y perdida de paquetes.

- Debido a las limitaciones de los equipos de red, no se ha establecido ningún tipo de segmentación en la misma, por lo tanto esta forma un único y dilatado dominio de *broadcast*, que incluye a las 7 dependencias externas a la matriz, lo cual introduce un tráfico *broadcast* y *multicast* considerable sobre la red WAN Municipal, que constituye el cuello de botella de la red.

- El análisis de tráfico cuantitativo demostró que el promedio del mismo es bajo, ocupando en todos los casos como máximo 1,1 Mbps de la capacidad de los enlaces principales; el mayor volumen de tráfico corresponde a la segunda planta donde se concentra la mayor densidad de usuarios de la red. Sin embargo se presentan picos de tráfico de hasta 13,6 Mbps.

- El análisis de tráfico cualitativo confirmo el efecto causado por la falta de segmentación en la red, pues el tráfico *broadcast* y *multicast* sumados dan valores en algunos casos de hasta el 11,3%. Cabe destacar que la distribución del tamaño de paquetes que circula por la red, demostró que la mayoría de ellos están entre más de 0 hasta 127 bytes, lo cual es positivo, disminuyendo el retardo que sufre un paquete de voz, cuando debe esperar la finalización de la transmisión de uno de datos, que inicio este proceso antes del ingreso del de voz al buffer.

- Del análisis de retardo que se realizó sobre la red WAN se desprende que el enlace con el Mercado Mayorista presenta el valor promedio más alto con 81.34 ms, y pese a ser considerable, está dentro del rango menor a 150 ms necesario para asegurar la calidad de la voz. Este análisis

expuso también que algunos enlaces sobre todo el del mencionado Mercado Mayorista tienen problemas de disponibilidad, por lo cual es necesario, dar mantenimiento a esta infraestructura, direccionando correctamente las antenas o identificando obstáculos que impidan la eficiente propagación de la señal electromagnética.

- La red de datos requiere una reestructuración, que introduzca estándares y mecanismos, que permitan la convergencia de servicios sobre la misma.

➢ Del análisis de la red telefónica de la Ilustre Municipalidad de Ambato se obtuvieron los siguientes resultados:

- La Matriz, Hospital Municipal, Unidad de Tránsito, Camal y Departamento de Cultura, poseen infraestructuras telefónicas independientes que incluyen PBX analógicas, sin embargo el Mercado Mayorista, Bodegas y Comisarias, cuentan solamente con algunas líneas directamente conectadas a la acometida de Andinatel, en algunos casos con teléfonos conectados en paralelo como extensiones.

- El análisis del tráfico de voz determinó que el 13,51% de las llamadas salientes desde la matriz tienen como destino alguna de las dependencias municipales, siendo las Comisarias la que presenta mayor participación sobre dicho porcentaje. El resto de tráfico saliente se distribuye mayoritariamente en llamadas locales, y en menor proporción hacia celulares, regionales, nacionales y otros.

- El sistema telefónico actual no entrega servicio de voz a todos los usuarios de la Municipalidad, ya que a través del criterio de número de ambientes físicos se determinó que solo en la matriz se requiere un total de 99 extensiones, en contraste a las 61 con las que actualmente se cuenta. Esta situación se repite en las dependencias que no cuentan con una infraestructura telefónica.

- El sistema telefónico actual de la matriz tiene muchos años de funcionamiento por lo que presenta problemas de operación, escalabilidad, degradación del hardware, discontinuidad del modelo con la consecuente escases de repuestos y dificultad para prestar nuevos servicios y funcionalidades; por estas razones es una necesidad imperiosa implementar un sistema capaz de dar cobertura a toda la Municipalidad con servicios de llamada avanzados y todos los beneficios adicionales que brinda la Telefonía sobre IP.

- Se plantea un plan de migración hacia ToIP que contempla inicialmente, equipar por completo con esta tecnología a la Matriz, y a las dependencias que actualmente no cuentan con una infraestructura telefónica, como son Comisarías, Mercado Mayorista y Bodegas, para el resto de dependencias se considera implementar adaptadores análogos a IP, para enlazar las PBX, con las cuentan que actualmente, al sistema unificado de telefonía.

- El análisis de los datos recolectados en los registros históricos de llamadas determinó la intensidad de tráfico en la hora pico, y utilizando la fórmula Erlang B, con un GoS del 1% se determinó el requerimiento de 17 canales de voz para comunicarse con la PSTN, sin embargo se estima contratar un canal E1 que brinda 30 canales de voz, lo cual incrementa la disponibilidad y deja abierta la posibilidad de utilizar este enlace para transmitir datos, pues es una interfaz digital. Del mismo modo para cada una de las dependencias se determinó el número de canales de voz requeridos para comunicarse con la matriz, encontrándose necesarios un total de 28 canales que atravesarán la WAN para satisfacer la demanda en la hora pico.

➢ El codec seleccionado para el entorno LAN, es el G.711 que trabaja a 64 kbits/s, debido principalmente a la más alta calidad de voz, que este proporciona, siendo el ancho de banda un aspecto poco crítico (generalmente 100 Mbits/s en el ambiente LAN). Sin embargo para el tráfico de voz que atraviesa la WAN, se seleccionó el códec G.729 que trabaja a 8 kbps, y más la cabecera sobre Ethernet genera un tráfico de 28,8 kbps, considerando los

28 canales que cruzarán la WAN, se totaliza 0,805 Mbps, los cuales se deberán reservar de los 10 Mbps que provee dicho enlace. El fabricante Cisco recomienda reservar como mínimo el 33% del enlace para los servicios que tienen mayor prioridad que los denominados *best-effort,* por lo tanto tenemos la seguridad de trabajar dentro de los parámetros adecuados.

- La nueva red de datos contará con segmentación creando dominios de redes virtuales que a su vez están asociadas a una subred lógica independiente, para aislar el tráfico de voz del de datos, en el caso de la matriz el tráfico de datos se segmenta aún más en sub-dominios virtuales en función a usuarios que pertenecen a las mismas unidades operativas Municipales.

- Para permitir la interconexión entre redes se introduce un *switch* de capa 3 del modelo OSI, que tendrá la función de interconectar las diferentes subredes segmentadas, y distribuidas alrededor del Municipio.

- El *backbone* principal de la red de datos deberá manejar tecnología Gigabit Ethernet con redundancia en el enlace incrementando así la velocidad y disponibilidad de los servicios.

- La red rediseñada permite absoluta escalabilidad, proporcionando una plataforma tecnológica, cuya inversión y beneficios estarán completamente justificados.

- La solución tecnológica para telefonía seleccionada para la Municipalidad de Ambato es la de *networking*, denominada *Cisco Unified Communications Manager*, pues permite la asignación de servicios o procesamiento de llamadas a través de varios servidores, permitiendo brindar redundancia y escalabilidad, además de presentar una convergencia tecnológica ampliada, así como características y funcionalidades que son de gran ayuda para la administración del sistema como el control de admisión de llamadas que en nuestro caso específico ayudará a controlar que la red WAN no se sature, y por lo tanto no se afecten los servicios que la misma transporta.

- La municipalidad podrá contar con el servicio de mensajería de voz unificada a través de la interacción del servidor *Cisco Unity Connection,* con el sistema

de telefonía, incrementando aún más la capacidad de la plataforma de comunicaciones de voz.

- La implementación del SISTEMA DE TELEFONÍA IP, diseñado y propuesto en el presente estudio, permitirá reducir en por lo menos un 14% los costos que el Municipio venía cancelando por servicios de telefonía a Andinatel, sobre las llamadas locales, además de brindar una herramienta tecnológica de comunicación, altamente eficiente, que permitirá a los funcionarios Municipales mejorar su rendimiento y por lo tanto la atención a la ciudadanía de Ambato.

- Finalmente el sistema propuesto está en capacidad de crecer cuando lo requiera hasta en 12 enlaces E1 y 1000 usuarios, de manera que las proyecciones consideradas están cubiertas y superadas.

6.2 RECOMENDACIONES

- Por ningún motivo descartar el mantenimiento aconsejado para la red WAN previo a la implementación de los servicios de voz.

- Se recomienda realizar la certificación del cableado estructurado, para poder descartar problemas por voltajes inducidos y puesta a tierra, que provocaría interferencias en los datos y por lo tanto disminución de la calidad de voz prestada por el sistema.

- Seguir los lineamientos del rediseño de la red, eliminando los *switches* que no proveen QoS, y más aún los *hubs*, que introducen dominios de colisión en la red, reduciendo su eficiencia.

- No descartar la implementación del servidor redundante *Cisco Call Manager,* pues esto aumentará la disponibilidad del servicio, evitando dejar incomunicados a los funcionarios municipales.

- Adicionar los mecanismos de monitoreo de red, descritos en el capitulo IV, lo cual nos permitirá conocer en todo momento el estado de la red y brindar

soporte preventivo aplicando medidas correctivas a las posibles fallas que puedan surgir durante la operación de la misma.

- Cuando se finalice la implementación del sistema solicitar un informe técnico detallado, el cual facilitará las tareas de mantenimiento y solución de problemas durante la operación por parte del departamento de sistemas del Municipio.

- Todos los equipos que se adquieran deben contar con garantía mínima de 1 año.

- Es necesario seguir adelante con el plan de migración, procurando llegar a concebir un modelo de telefonía totalmente IP en todas las dependencias.

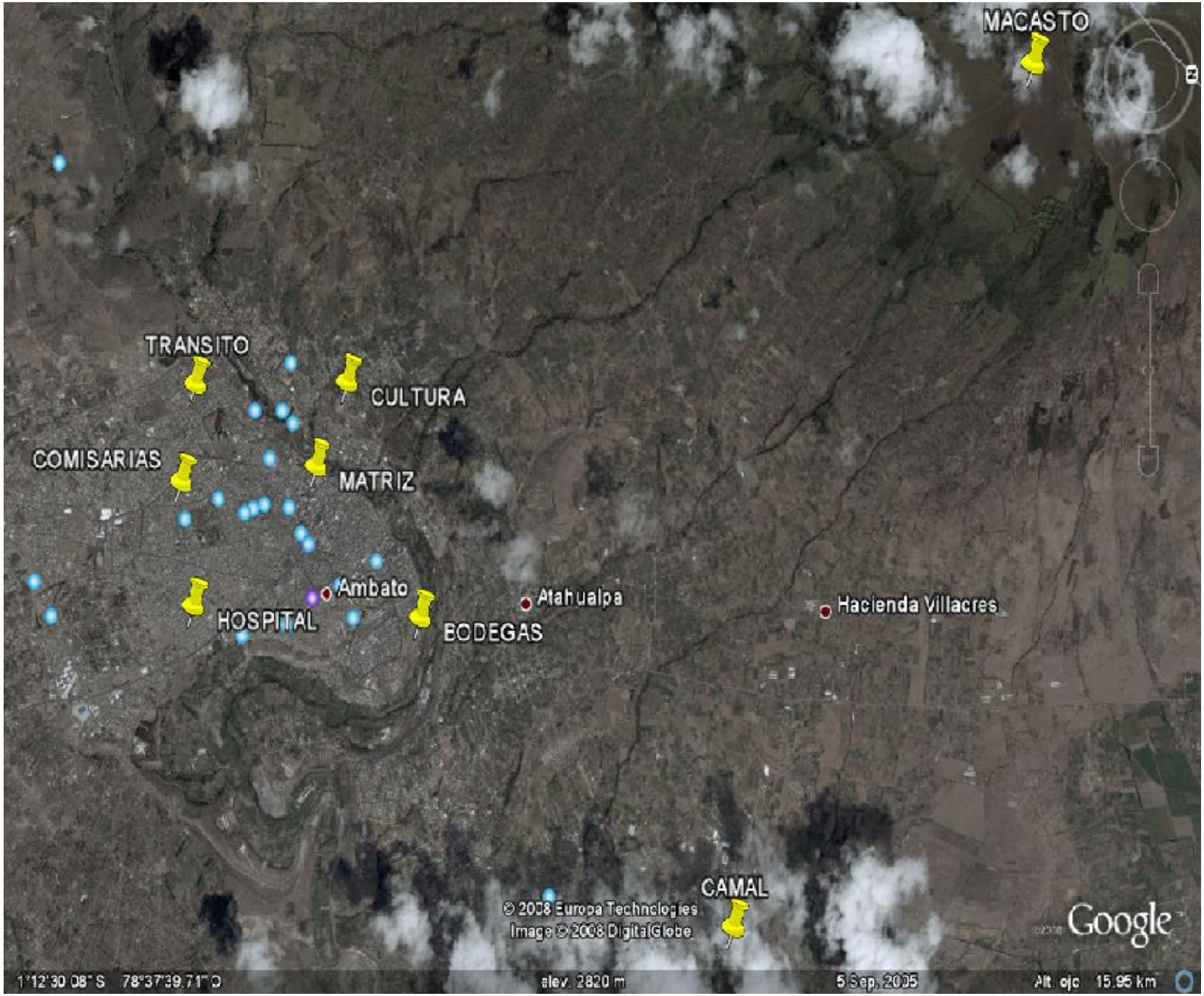
- En las dependencias donde la densidad de usuarios crezca considerablemente es recomendable, adicionar un router CISCO en el límite hacia la WAN, con la funcionalidad, SRST *Survivable Remote Site Telephony,* que permite brindar redundancia local, es decir cuando la red WAN cae y el *Call Manager* de la matriz, no puede atender las peticiones de los usuarios remotos, el *router* a través de las mencionada funcionalidad brinda procesamiento para los usuarios que se encuentran dentro de su red local.

- A medida que la red vaya creciendo y aumenten los requerimientos de la WAN, sería necesario implementar un enlace punto a punto desde Macasto (Ubicación central del enlace punto multipunto de la red WAN), hasta la Matriz, pues es hacia donde se dirige la mayor parte del tráfico.

ANEXOS

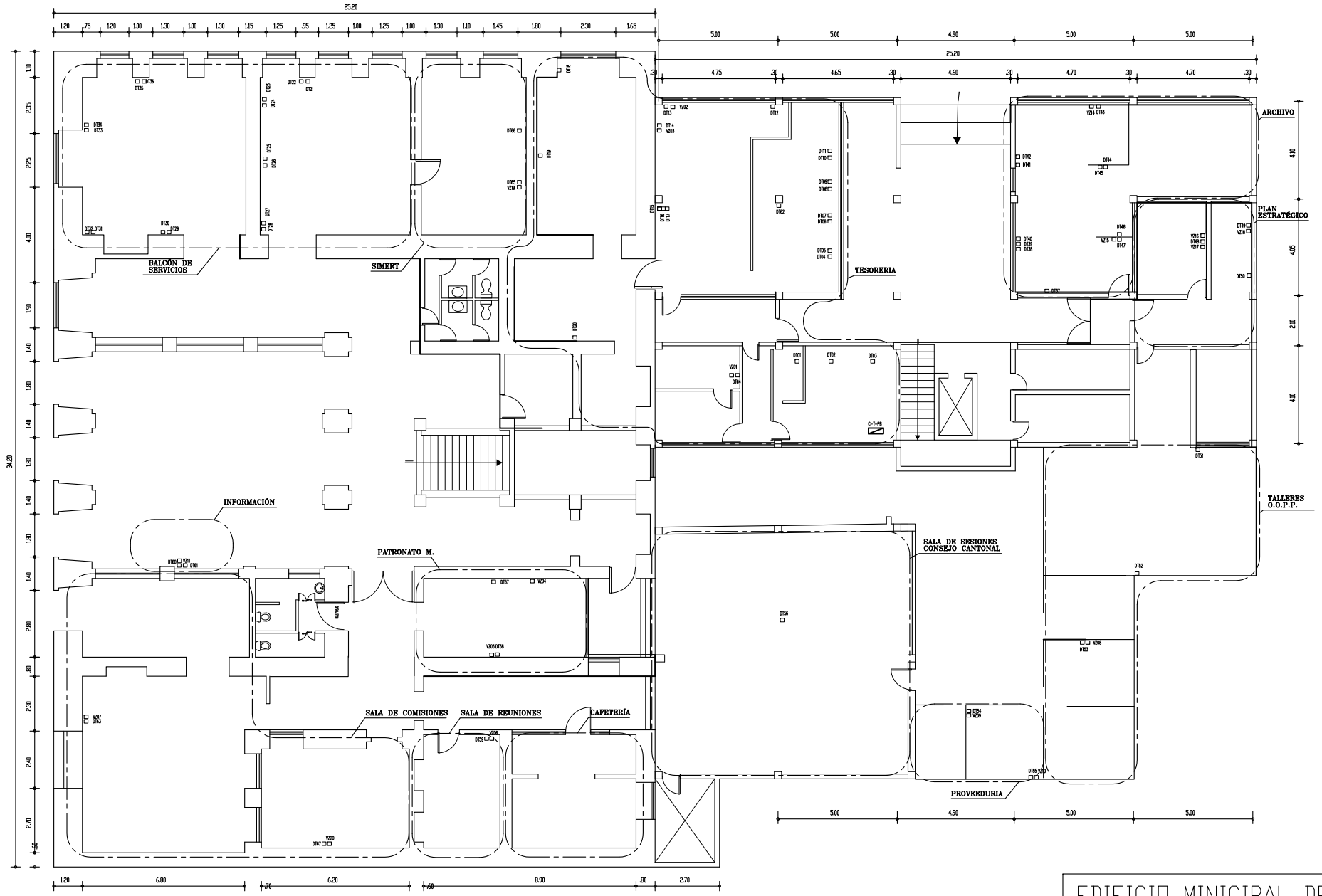
ANEXO A

UBICACIÓN GEOGRÁFICA DE LAS DEPENDENCIAS MUNICIPALES


MACASTO
TRANSITO
CULTURA
COMISARIAS
MATRIZ
Ambato
Atahualpa
Hacienda Villacres
HOSPITAL
BODEGAS
CAMAL
© 2008 Europa Technologies
Image © 2008 DigitalGlobe
Google
1°12'30.08" S 78°37'39.71" O
elev. 2820 m
5 Sep. 2005
Alt. ojo 15.95 km

ANEXO B

PLANOS DE UBICACIÓN DE PUNTOS DE VOZ Y DATOS PLANTA BAJA



PLANTA BAJA

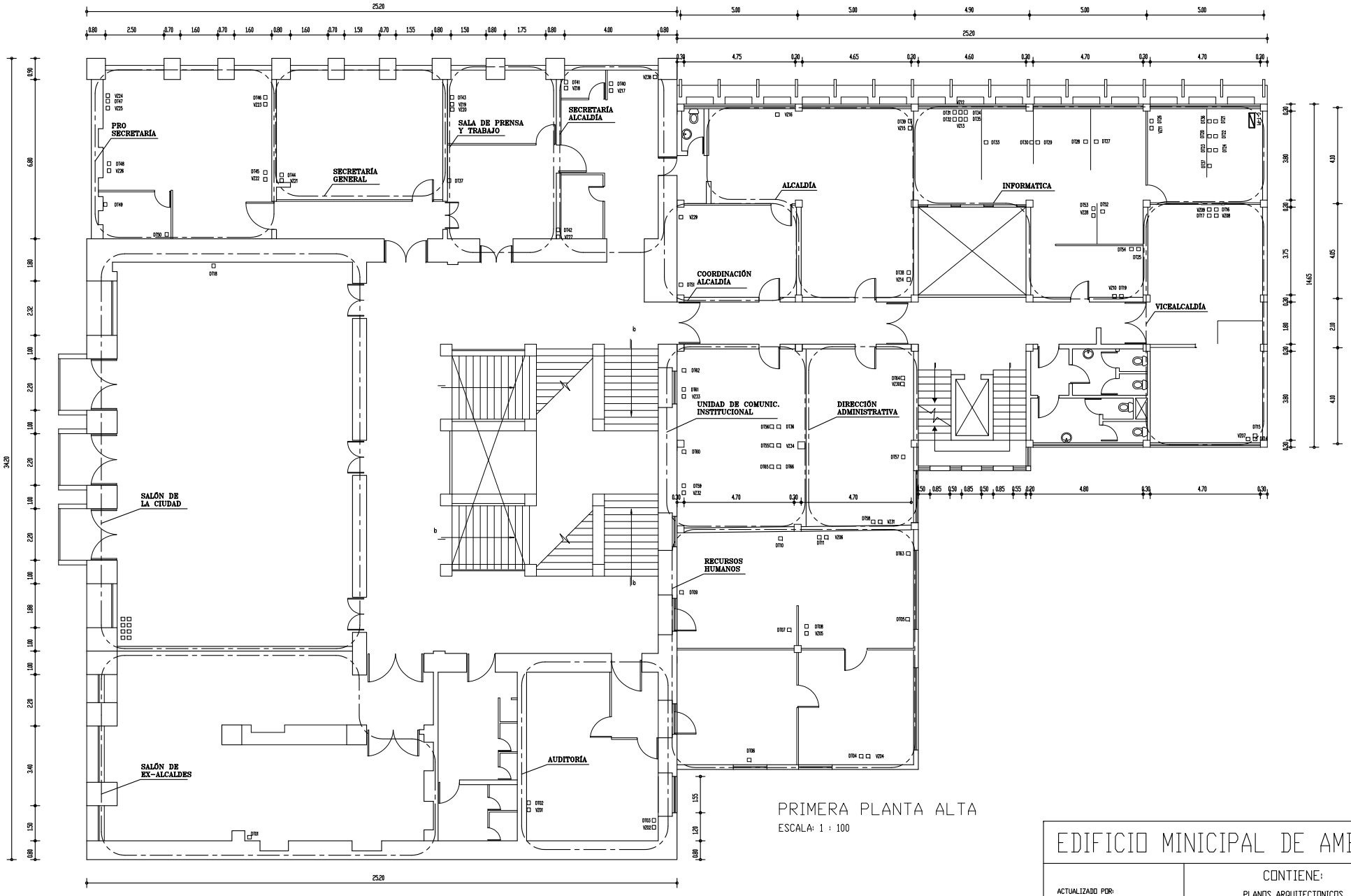
ESCALA: 1 : 100

EDIFICIO MINICIPAL DE AMBATO

ACTUALIZADO POR: MARCELO SOLÍS	CONTIENE: PLANOS ARQUITECTONICOS — PLANTA BAJA
DIRECCION: Calles Bolívar y Castillo	ESCALA: 1 : 100 — HOJA 1 DE 4

ANEXO C

PLANOS DE UBICACIÓN DE PUNTOS DE VOZ Y DATOS PRIMERA PLANTA ALTA



PRIMERA PLANTA ALTA

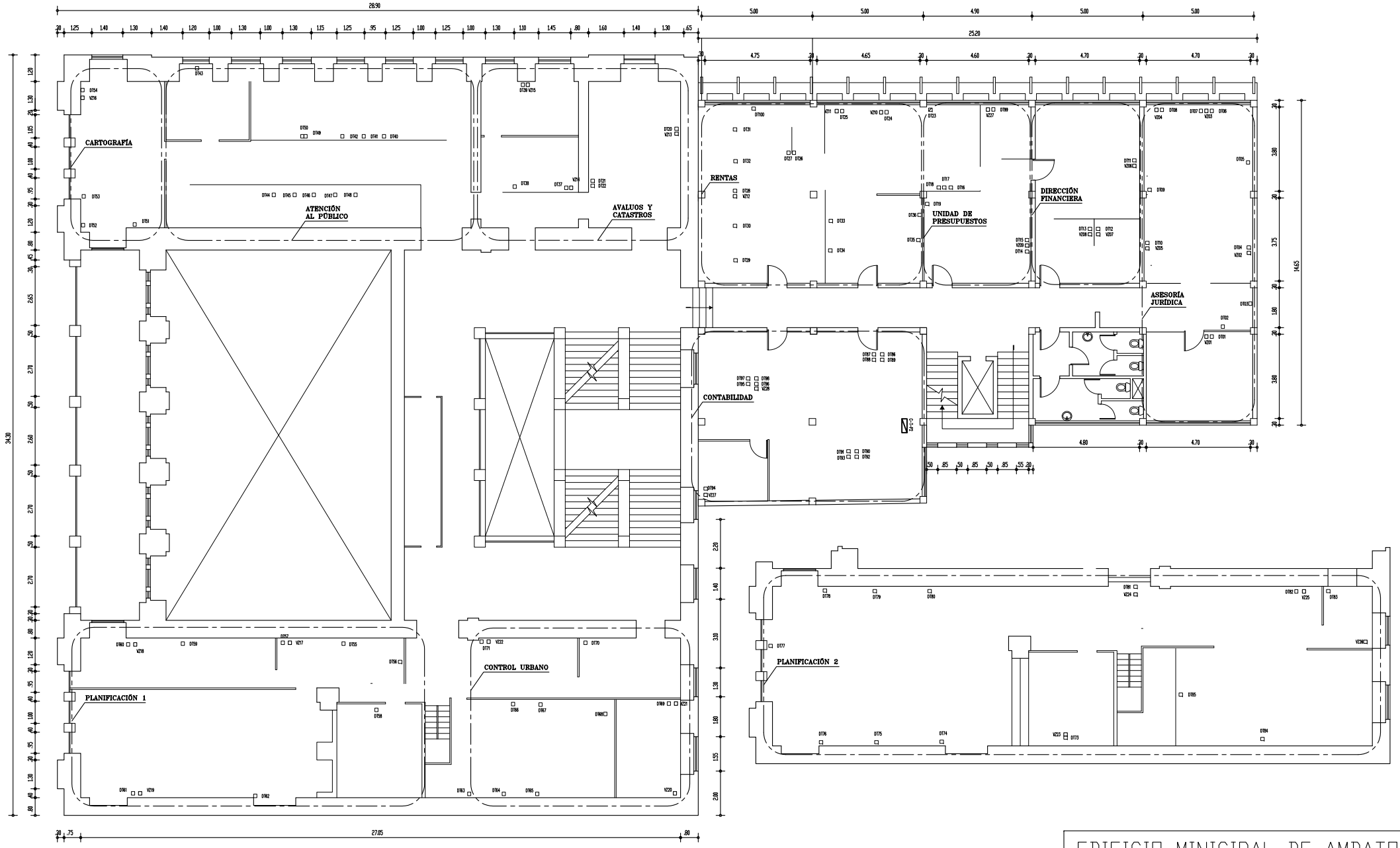
ESCALA: 1 : 100

EDIFICIO MINICIPAL DE AMBATO

ACTUALIZADO POR: MARCELO SOLÍS	CONTIENE: PLANOS ARQUITECTONICOS — PRIMERA PLANTA ALTA
DIRECCION: Calles Bolívar y Castillo	ESCALA: 1 : 100 — HOJA 2 DE 4

ANEXO D

PLANOS DE UBICACIÓN DE PUNTOS DE VOZ Y DATOS SEGUNDA PLANTA ALTA



SEGUNDA PLANTA ALTA

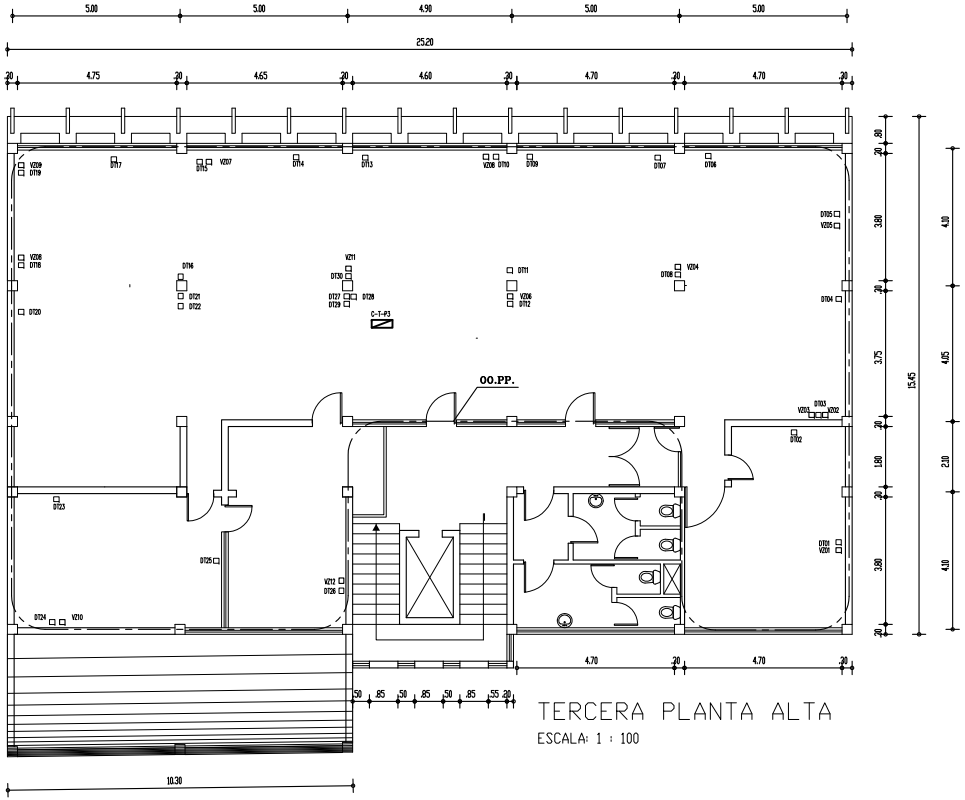
ESCALA: 1 : 100

EDIFICIO MINICIPAL DE AMBATO

ACTUALIZADO POR: MARCELO SOLÍS	CONTIENE: PLANOS ARQUITECTONICOS — SEGUNDA PLANTA ALTA
DIRECCION: Calles Bolivar y Castillo	ESCALA: 1 : 100 — HOJA 3 DE 4

ANEXO E

PLANOS DE UBICACIÓN DE PUNTOS DE VOZ Y DATOS TERCERA PLANTA ALTA



TERCERA PLANTA ALTA

ESCALA: 1 : 100

EDIFICIO MINICIPAL DE AMBATO

ACTUALIZADO POR: MARCELO SOLIS	CONTIENE: PLANOS ARQUITECTONICOS TERCERA PLANTA ALTA
DIRECCION: Calles Bolivar y Castillo	ESCALA: 1 : 100

HOJA 4 DE 4

ANEXO F

MAC SCANNER

IP Address	MAC Address	Host Name
10.10.0.1	00:D0:B7:B6:F5:F7	
10.10.0.2	00:30:48:83:5F:51	NS
10.10.0.3	00:19:BB:E6:01:52	IMSEDB
10.10.0.5	00:13:21:FD:52:47	IMSEFIN
10.10.0.6	00:0E:7F:24:5B:DC	APLICSERVER
10.10.0.7	00:0E:7F:24:79:5D	IMADB
10.10.0.8	00:D0:B7:B7:1C:8F	IMCAFEE
10.10.0.10	00:01:DE:13:D7:75	
10.10.0.11	00:01:E6:A1:E3:2F	
10.10.0.12	00:01:E6:A1:EA:0B	
10.10.0.13	00:17:08:8E:B2:76	NPI8EB276
10.10.0.14	00:01:E6:A1:E3:1C	
10.10.0.16	00:01:E6:A1:8A:9E	
10.10.0.17	00:01:E6:A1:E3:42	
10.10.0.18	00:01:E6:86:27:50	
10.10.0.21	00:01:E6:9C:32:D2	
10.10.0.25	00:19:5B:EB:1F:21	PS-JURI
10.10.0.26	00:01:E6:A1:EA:02	
10.10.0.28	00:13:21:26:04:C4	NPI2604C4
10.10.0.34	00:30:6E:C9:36:52	NPIC93652
10.10.0.41	00:13:21:CE:06:98	IM02FI55
10.10.0.44	00:14:38:93:61:4B	NPI93614B
10.10.0.45	00:04:75:E6:D7:B7	IM02PL02
10.10.0.51	00:18:E7:0D:1A:D1	IM00SC03
10.10.0.52	00:1B:11:18:1D:14	PS-BOD-P1
10.10.0.53	00:D0:09:A1:49:E4	IM01AD06
10.10.0.54	00:04:75:E6:D8:89	CALDERONFA
10.10.0.57	00:0E:7F:67:EE:8C	ARMIJOSL
10.10.0.61	00:04:75:E6:D8:85	BARBAD
10.10.0.62	00:0E:7F:FC:3A:9C	ALVAREZM
10.10.0.73	00:04:75:E6:DB:52	BONILLAG
10.10.0.75	00:04:75:E6:D8:A8	IM02AJ07
10.10.0.77	00:D0:09:A1:4F:E3	DIAZE
10.10.0.79	00:04:75:E6:DA:F4	AGUILARN
10.10.0.81	00:04:75:E6:DA:62	CAJAMAYORISTA
10.10.0.82	00:04:75:E6:DB:4C	IM00PE01
10.10.0.85	00:0E:7F:FC:39:69	BETANCOURTM
10.10.0.87	00:19:BB:E3:E2:0E	IM01SI04
10.10.0.88	00:04:75:E6:DC:55	IM01RH04
10.10.0.89	00:0E:7F:FC:38:29	CEPEDAT
10.10.0.91	00:04:75:E6:DB:5D	CHAGCHAM
10.10.0.92	00:19:BB:E3:DA:CB	PLANDESARROLLO
10.10.0.94	00:0E:7F:FC:38:69	IM03PL09
10.10.0.97	00:0E:7F:FC:39:94	
10.10.0.99	00:04:75:E6:D8:CA	DAVALOSL
10.10.0.100	00:0E:7F:67:F1:70	IM01AD08
10.10.0.101	00:04:75:E6:D8:C9	IM00AR00
10.10.0.102	00:0E:7F:67:F9:78	ENDARAW
10.10.0.103	00:0E:7F:67:EA:BD	ESCOBARF
10.10.0.104	00:04:75:E6:DC:53	IM03OP40
10.10.0.109	00:0E:7F:67:EB:22	FERNANDEZR
10.10.0.112	00:D0:09:A9:6B:0B	IM03OP27
10.10.0.113	00:04:75:E6:D8:A7	IM02FI02
10.10.0.114	00:04:75:E6:DB:D7	GAMBOAN
10.10.0.119	00:04:75:E6:DA:AB	GUERREROL
10.10.0.120	00:04:75:E6:DB:66	GUERREROM
10.10.0.121	00:0E:7F:67:F9:51	IM00SC02
10.10.0.124	00:0E:7F:67:EE:94	IM02AV03
10.10.0.126	00:04:75:E6:D7:D8	GUZMANR
10.10.0.128	00:19:BB:E3:DA:AD	IM01SI02
10.10.0.129	00:D0:09:99:F8:3F	IM00XX00
10.10.0.130	00:04:75:E6:DC:14	JIMENEZB
10.10.0.137	00:D0:09:A9:6B:40	IM03OP08
10.10.0.139	00:0D:61:16:65:11	IM01TE15
10.10.0.140	00:0E:7F:67:F9:0D	IM02AJ04
10.10.0.141	00:0E:7F:67:EE:97	IM02AV01
10.10.0.142	00:0E:7F:67:EA:B4	IM01AD04
10.10.0.143	00:0F:FE:43:24:77	IM01AD07
10.10.0.144	00:04:75:E6:DB:E2	LOPEZS
10.10.0.145	00:04:75:E6:DB:CC	
10.10.0.147	00:04:75:E6:D7:D7	IM02CB04
10.10.0.150	00:04:75:E6:DB:F8	MAYORGAJ

IP Address	MAC Address	Host Name
10.10.0.151	00:04:75:E6:DA:9F	IM01VP01
10.10.0.152	00:19:BB:E3:E2:6C	IM01SI07
10.10.0.153	00:0E:7F:67:EB:40	CANTUNAM
10.10.0.154	00:0E:7F:67:F9:04	MOLINAG
10.10.0.155	00:04:75:E6:DB:68	MONTALVOM
10.10.0.161	00:0E:7F:67:EB:14	MUÑOZP
10.10.0.163	00:0E:7F:67:EF:25	NARANJOS
10.10.0.164	00:04:75:E6:DC:0C	NAVASM
10.10.0.165	00:0E:7F:67:EE:86	NUNEZC
10.10.0.168	00:0E:7F:FC:39:D8	IM00LB01
10.10.0.169	00:04:75:E6:DB:CB	OVIEDOJO
10.10.0.171	00:04:75:E6:DB:48	PALATEM
10.10.0.174	00:04:75:E6:D8:87	IM02AJ09
10.10.0.175	00:0E:7F:68:0C:46	PEREZA
10.10.0.178	00:19:BB:4D:66:55	CLIRSEN13
10.10.0.181	00:04:75:E6:DB:30	REYESC
10.10.0.182	00:D0:09:A8:C8:0A	RIVADENEIRAM
10.10.0.183	00:04:75:E6:DA:9B	IM02AJ02
10.10.0.184	00:04:75:E6:DB:C7	RIVERAM
10.10.0.187	00:0E:7F:FC:38:35	RODRIGUEZM
10.10.0.189	00:0E:7F:67:EE:8F	ROSALESM
10.10.0.190	00:04:75:E6:DB:D8	RUIZJ
10.10.0.191	00:0E:7F:67:EE:99	SALINASM
10.10.0.192	00:04:75:E6:D8:88	MORETAJ
10.10.0.194	00:04:75:E6:DB:65	SANCHEZE
10.10.0.195	00:19:BB:E3:E2:64	IM00PV03
10.10.0.196	00:04:75:E6:D7:FA	SANCHEZM
10.10.0.197	00:04:75:E6:DB:64	IM00PL02
10.10.0.198	00:0E:7F:67:EE:FC	MESCOBAR
10.10.0.200	00:04:75:E6:DB:53	VASQUEZG
10.10.0.201	00:04:75:E6:D7:B9	IM01AD05
10.10.0.207	00:D0:09:A8:CA:9E	IM03OP17
10.10.0.208	00:0D:87:66:64:F1	TOUCHSCREEN
10.10.0.210	00:04:75:E6:DB:19	VALLEM
10.10.0.211	00:19:BB:E3:E2:B6	IM01RH07
10.10.0.212	00:19:BB:E3:E1:7F	IM02FI03
10.10.0.213	00:0F:FE:8A:61:C8	IM02AV11
10.10.0.215	00:04:75:E6:DA:B7	VELASTEGUII
10.10.0.218	00:0F:FE:33:B0:9E	IM04OP22
10.10.0.220	00:0E:7F:67:EE:91	IM03AV33
10.10.0.222	00:04:75:E6:DA:A0	YEPEZR
10.10.0.223	00:04:75:E6:DB:F4	ZURITAJ
10.10.0.225	00:19:BB:E3:E1:74	IM01SI21
10.10.0.227	00:0E:7F:FC:38:24	LEONV
10.10.0.228	00:04:75:E6:DB:69	LEONC
10.10.0.232	00:19:BB:E3:E2:8B	IM01CR02
10.10.0.234	00:04:75:E6:DB:E7	IM01UA04
10.10.0.240	00:15:60:98:32:E8	
10.10.0.242	00:04:75:E6:DA:7E	IM03PL17
10.10.0.244	00:19:BB:E3:E2:A2	IM02PR07
10.10.0.249	00:08:A1:41:0D:49	IM02FI05
10.10.1.12	00:13:21:24:31:E8	NPI2431E8
10.10.1.15	00:13:21:26:A2:E0	NPI26A2E0
10.10.1.16	08:00:37:46:97:45	FX-469745
10.10.1.17	08:00:37:46:97:9E	FX-46979E
10.10.1.18	00:13:21:25:EC:CB	NPI25ECCB
10.10.1.19	08:00:37:46:96:05	FX-469605
10.10.1.20	00:00:AA:7C:DF:BC	
10.10.1.25	00:19:5B:CA:57:6F	PS-CAMAL-1
10.10.1.33	00:E0:4D:33:0E:E1	CA01CA02
10.10.1.39	00:04:75:E6:D9:F8	CM01CM01
10.10.1.49	00:19:BB:E3:E1:FE	IM01AL03
10.10.1.51	00:04:75:E6:DB:50	IM00PA01
10.10.1.56	00:04:75:E6:DB:01	CM01CM04
10.10.1.62	00:0F:FE:33:2C:B3	IM00PE02
10.10.1.65	00:0F:FE:33:89:16	IM03OP05
10.10.1.68	00:0F:FE:31:99:16	IM01CR01
10.10.1.69	00:0F:FE:33:B0:F2	IM01RH02
10.10.1.70	00:0F:FE:31:62:34	IM03OP26
10.10.1.71	00:0F:FE:33:9F:D5	IM02PL06
10.10.1.73	00:0F:FE:33:B0:6A	IM03OP06
10.10.1.75	00:0F:FE:31:62:3D	IM03OP03

IP Address	MAC Address	Host Name
10.10.1.80	00:19:BB:E3:E2:91	IM01AL04
10.10.1.84	00:0F:FE:33:AE:A1	IM02PL01
10.10.1.87	00:0F:FE:31:99:3D	IM02PL12
10.10.1.98	00:13:21:CF:6B:19	IM02AJ20
10.10.1.99	00:0F:FE:31:63:3B	IM02AV17
10.10.1.100	00:0F:FE:33:88:B2	IM02AV18
10.10.1.101	00:13:21:CF:6B:38	IM01SI01
10.10.1.108	00:13:21:CE:05:B8	IM03PL15
10.10.1.109	00:13:21:CD:93:38	IM03PL44
10.10.1.110	00:13:21:D1:3C:48	IM01CR03
10.10.1.111	00:13:8F:1A:7E:22	CM01CM02
10.10.1.113	00:0E:7F:FC:38:00	IM01RH01
10.10.1.114	00:13:21:D1:3B:B6	IM01AD02
10.10.1.119	00:0F:FE:31:99:0C	IM04OP06
10.10.1.121	00:13:21:D0:3C:E8	IM02AJ06
10.10.1.122	00:0F:FE:31:63:28	IM01AI10
10.10.1.133	00:19:BB:E3:E1:4E	IM02PR04
10.10.1.134	00:04:75:E6:D7:CF	IM01PL01
10.10.1.135	00:19:BB:E3:E1:34	IM01SIX8
10.10.1.136	00:19:BB:E3:E2:43	IM01SIS1
10.10.1.141	00:19:BB:E3:E0:F9	IM02PR05
10.10.1.142	00:0F:FE:2B:11:EE	IM01RH00
10.10.1.147	00:19:BB:E3:E1:91	IM01SI05
10.10.1.148	00:0F:FE:2C:DD:CE	IM01RH03
10.10.1.151	00:0F:FE:43:24:19	IM01SG02
10.10.1.152	00:15:60:9B:17:79	IM00PV01
10.10.1.166	00:19:BB:E3:E2:38	IM02FI01
10.10.1.167	00:50:BA:77:FB:61	IM01SI11
10.10.1.171	00:0F:FE:3E:3B:DE	IM01RH11
10.10.1.173	00:16:76:2B:10:CF	IM03OP02
10.10.1.174	00:19:BB:E3:E2:7F	IM02CO01
10.10.1.179	00:0F:FE:2E:9D:9C	CM01CM03
10.10.1.183	00:16:35:66:8E:23	IM01CM05
10.10.1.188	00:0F:FE:2E:C8:F7	IM01AD10
10.10.1.189	00:0F:FE:43:22:29	IM00PV04
10.10.1.190	00:0F:FE:43:23:9A	IM01AU03
10.10.1.192	00:0F:FE:43:22:C1	
10.10.1.193	00:0F:FE:43:22:2F	IM02AJ11
10.10.1.196	00:0F:FE:43:24:11	IM02AJ10
10.10.1.197	00:0F:FE:43:21:B3	IM02AV85
10.10.1.198	00:0F:FE:43:23:91	IM01SG01
10.10.1.201	00:0F:FE:43:23:87	IM02AV10
10.10.1.202	00:0F:FE:41:80:37	IM02AV62
10.10.1.206	00:0F:FE:41:8A:91	IM02CO05
10.10.1.209	00:0F:FE:43:23:BE	IM03PL04
10.10.1.213	00:04:75:E6:DC:DF	VELAR
10.10.1.214	00:0F:FE:43:23:70	IM03PL07
10.10.1.238	00:1B:78:7F:C6:E6	IM01SI12
10.10.1.239	00:1B:78:40:77:7A	IM03PL10
10.10.1.241	00:0F:FE:31:99:F7	IM00SG01
10.10.1.254	00:04:75:E6:D8:33	IM01RH06
10.10.3.1	00:01:DE:13:D7:89	
10.10.3.46	00:19:BB:E3:E0:F9	
10.10.3.48	00:19:BB:E3:E1:67	
10.10.3.49	00:08:A1:5A:4A:28	
10.10.3.50	00:0F:FE:33:88:AD	MM01AD01
10.10.3.51	00:04:75:E6:DA:60	MM00SC01
10.10.3.241	00:19:E7:77:E4:C0	
10.10.4.1	00:01:DE:13:D7:92	
10.10.4.11	00:00:80:00:31:74	
10.10.4.12	00:19:5F:00:2B:54	
10.10.4.13	00:19:5F:00:2B:44	
10.10.4.14	00:19:5F:00:2B:64	
10.10.4.30	00:0E:7F:67:EE:8B	BD00BD02
10.10.4.31	00:04:75:E6:DB:C9	BD00BD03
10.10.4.32	00:0E:7F:67:D3:68	CAIZAV
10.10.4.40	00:19:D1:2F:DF:C1	
10.10.4.44	00:0F:FE:AA:41:BA	HOSE0301
10.10.5.1	00:01:DE:13:D7:77	
10.10.5.31	00:04:75:E6:DB:4F	CO00CO01
10.10.5.32	00:0F:FE:43:21:AC	CO00IN01
10.10.5.33	00:0D:88:F7:F2:23	TINITANAT

IP Address	MAC Address	Host Name
10.10.5.34	00:18:71:71:B8:D6	CO00IN03
10.10.5.36	00:18:71:72:BA:D3	CO00IN02
10.10.5.50	00:0E:7F:67:EE:93	CO02HI01
10.10.5.51	00:0F:FE:33:88:A7	CO02HI02
10.10.5.53	00:D0:09:A1:4E:77	CO02HI04
10.10.5.54	00:0F:FE:31:99:18	CO02HI05
10.10.5.55	00:0F:FE:33:B0:FC	CO02HI06
10.10.5.56	00:04:75:E6:D8:31	CO02HI07
10.10.5.57	00:04:75:E6:DB:D9	CO02HI08
10.10.5.58	00:0F:FE:43:22:87	CO02HI09
10.10.5.59	00:0F:FE:33:2C:93	CO02HI10
10.10.5.60	00:07:95:56:F4:90	CO02HI11
10.10.5.61	00:0F:3D:EB:2C:26	CO02HI12
10.10.5.62	00:08:A1:91:71:17	CO02HI23
10.10.5.63	00:19:BB:E3:E1:67	CO02H14
10.10.5.64	00:0E:7F:68:0C:2A	CO02HI15
10.10.5.71	00:0F:FE:33:AF:3B	CO02SP03
10.10.5.74	00:1B:78:B3:C0:45	CO02SP06
10.10.5.77	00:0F:FE:31:63:1B	CO01SP15
10.10.5.91	00:18:71:72:DB:15	CO03CF01
10.10.5.92	00:19:BB:4D:48:52	CLIRSEN12
10.10.5.94	00:18:71:72:B5:FE	CO03CF05
10.10.5.95	00:18:71:72:B8:01	CO03CF07
10.10.5.96	00:19:BB:E0:BC:F7	CO03CF06
10.10.5.97	00:19:BB:4E:33:EA	CO03CF04
10.10.5.133	00:18:71:72:DC:35	CO03AV01
10.10.5.177	00:0E:7F:67:EA:E8	CAJACOMISARIAS
10.10.6.1	00:01:DE:13:E0:4F	
10.10.6.10	00:12:79:81:7C:3C	NPI817C3C
10.10.6.20	00:1B:78:B3:C1:E1	AS00AS02
10.10.6.29	00:1B:78:83:44:D1	CU01CU02
10.10.6.33	00:0F:FE:2B:11:FB	UT01UT05
10.10.6.41	00:80:AD:74:95:A1	RUBIOM
10.10.6.43	00:D0:09:9A:7C:E6	AGUILARJ
10.10.6.81	00:0F:FE:31:62:33	CU00CU01
10.10.6.89	00:08:A1:5A:4A:28	VELARDEF
10.10.6.99	00:D0:09:A8:13:A3	IM01AD01
10.10.6.101	00:19:BB:4C:13:2B	AS01DI02
10.10.6.175	00:0F:FE:31:99:E0	CU00CU02
10.10.6.193	00:18:71:72:DC:94	IM01PREST
10.10.6.200	00:19:BB:E3:E1:34	IM01SIX8
10.10.6.245	00:13:48:00:1B:F0	
10.10.7.2	00:01:DE:13:E1:08	
10.10.7.42	00:14:D1:39:20:FE	
10.10.8.1	00:01:DE:13:DE:6E	
10.10.8.5	00:14:C2:3B:C6:0E	UMTSERVER
10.10.8.20	00:14:38:8B:F8:74	IMAUMT
10.10.8.40	00:0F:FE:31:5D:BC	AS00AS03
10.10.8.42	00:0F:FE:31:5F:C1	AS00AS01
10.10.8.46	00:04:75:E6:DB:77	ELIAS
10.10.8.50	00:0F:FE:2C:70:3D	UT00UT03
10.10.8.51	00:0F:FE:2C:70:46	UT00UT01
10.10.8.52	00:0F:FE:2B:11:A8	UT01UT03
10.10.8.53	00:0F:FE:2C:DD:F2	UT00UT02
10.10.8.55	00:0F:FE:2C:6E:53	UT00UT04
10.10.8.79	00:D0:09:A8:13:D6	ENRIQUE
10.10.8.111	00:19:BB:4E:33:9D	CLIRSEN11
10.10.8.115	00:19:BB:4E:33:84	CLIRSEN15
10.10.8.135	00:0E:7F:67:EE:84	SANCHEZJ
10.10.9.10	00:07:50:B5:DE:21	
10.10.9.40	00:0C:29:FD:EA:EA	DEMO-7ZYOH27OVC
10.10.9.52	00:1B:78:1D:3B:9B	
10.10.10.5	00:00:48:B3:65:A1	
10.10.10.34	00:12:79:81:6C:65	NPI816C65
10.10.11.11	00:D0:09:87:AD:0A	SISTEMAS
10.10.12.27	00:00:48:B3:60:5A	
10.10.44.128	00:13:21:CF:6B:1D	IM03OP55
10.10.199.1	00:05:5D:83:B7:94	
10.10.199.2	00:05:5D:77:E1:B3	DIEGO-4BA6ADFD1
10.10.199.3	00:02:E3:16:98:3C	DIEGO-4BA6ADFD1

ANEXO G

TABLAS DE ERLANG B

ERLANG B

GoS = 1%		GoS = 2%		GoS = 3%		GoS = 4%		GoS = 5%		GoS = 6%		GoS = 7%		GoS = 8%		GoS = 9%		GoS = 10%	
Tráfico Ofrecido	Cts	Tráfico Ofrecido	Cts	Tráfico Ofrecido	Cts	Tráfico Ofrecido	Cts	Tráfico Ofrecido	Cts	Tráfico Ofrecido	Cts	Tráfico Ofrecido	Cts	Tráfico Ofrecido	Cts	Tráfico Ofrecido	Cts	Tráfico Ofrecido	Cts
0	1	0	1	0	1	0	1	0.1	1	0.1	1	0.1	1	0.1	1	0.1	1	0.1	1
0.1	2	0.1	2	0.3	2	0.3	2	0.3	2	0.4	2	0.4	2	0.5	2	0.5	2	0.5	2
0.4	3	0.6	3	0.7	3	0.7	3	0.9	3	0.9	3	1	3	1	3	1.2	3	1.2	3
0.8	4	1.1	4	1.2	4	1.4	4	1.5	4	1.5	4	1.7	4	1.8	4	1.9	4	2	4
1.4	5	1.6	5	1.9	5	2	5	2.2	5	2.3	5	2.5	5	2.6	5	2.8	5	2.8	5
1.9	6	2.2	6	2.5	6	2.7	6	2.9	6	3.1	6	3.2	6	3.4	6	3.5	6	3.7	6
2.5	7	2.8	7	3.2	7	3.5	7	3.7	7	3.9	7	4.1	7	4.3	7	4.4	7	4.6	7
3.1	8	3.6	8	3.9	8	4.2	8	4.5	8	4.7	8	5	8	5.1	8	5.3	8	5.5	8
3.7	9	4.3	9	4.7	9	5.1	9	5.4	9	5.5	9	5.8	9	6	9	6.3	9	6.5	9
4.4	10	5	10	5.5	10	5.8	10	6.2	10	6.5	10	6.7	10	7	10	7.2	10	7.4	10
5.1	11	5.8	11	6.2	11	6.6	11	7.1	11	7.4	11	7.7	11	7.9	11	8.2	11	8.4	11
5.8	12	6.5	12	7.1	12	7.5	12	7.9	12	8.2	12	8.5	12	8.9	12	9.2	12	9.4	12
6.5	13	7.4	13	7.9	13	8.4	13	8.8	13	9.2	13	9.5	13	9.8	13	10.1	13	10.4	13
7.3	14	8.2	14	8.7	14	9.3	14	9.7	14	10	14	10.4	14	10.8	14	11.1	14	11.4	14
8.1	15	9	15	9.6	15	10.1	15	10.6	15	11	15	11.4	15	11.7	15	12.1	15	12.4	15
8.9	16	9.8	16	10.5	16	11	16	11.5	16	12	16	12.3	16	12.7	16	13	16	13.4	16
9.6	17	10.6	17	11.3	17	11.9	17	12.5	17	12.8	17	13.3	17	13.7	17	14.1	17	14.5	17
10.4	18	11.5	18	12.1	18	12.8	18	13.3	18	13.8	18	14.3	18	14.6	18	15.1	18	15.5	18
11.2	19	12.3	19	13.1	19	13.7	19	14.3	19	14.7	19	15.2	19	15.7	19	16.1	19	16.5	19
12	20	13.1	20	13.9	20	14.6	20	15.2	20	15.7	20	16.2	20	16.7	20	17.1	20	17.6	20
12.8	21	14	21	14.8	21	15.5	21	16.2	21	16.7	21	17.2	21	17.7	21	18.2	21	18.6	21
13.6	22	14.8	22	15.8	22	16.5	22	17.1	22	17.6	22	18.1	22	18.7	22	19.2	22	19.6	22
14.4	23	15.8	23	16.6	23	17.4	23	18.1	23	18.6	23	19.2	23	19.7	23	20.2	23	20.7	23
15.2	24	16.6	24	17.5	24	18.3	24	19	24	19.6	24	20.2	24	20.7	24	21.3	24	21.7	24
16.1	25	17.5	25	18.5	25	19.2	25	20	25	20.6	25	21.2	25	21.7	25	22.3	25	22.8	25
16.9	26	18.3	26	19.4	26	20.1	26	20.9	26	21.6	26	22.1	26	22.8	26	23.2	26	23.8	26
17.8	27	19.2	27	20.2	27	21.1	27	21.9	27	22.5	27	23.2	27	23.8	27	24.3	27	24.9	27
18.6	28	20.1	28	21.1	28	22	28	22.8	28	23.5	28	24.2	28	24.7	28	25.3	28	25.9	28
19.4	29	21	29	22.1	29	23	29	23.8	29	24.5	29	25.1	29	25.8	29	26.4	29	27	29
20.3	30	21.9	30	23	30	23.9	30	24.7	30	25.5	30	26.2	30	26.8	30	27.4	30	28.1	30
21.1	31	22.8	31	23.9	31	24.8	31	25.8	31	26.5	31	27.2	31	27.9	31	28.5	31	29.1	31
22	32	23.6	32	24.9	32	25.9	32	26.7	32	27.4	32	28.2	32	28.9	32	29.6	32	30.2	32
22.8	33	24.6	33	25.8	33	26.8	33	27.7	33	28.5	33	29.2	33	29.9	33	30.6	33	31.2	33
23.7	34	25.5	34	26.7	34	27.8	34	28.6	34	29.4	34	30.2	34	30.9	34	31.7	34	32.3	34
24.6	35	26.4	35	27.7	35	28.7	35	29.7	35	30.5	35	31.3	35	32	35	32.7	35	33.4	35
25.5	36	27.3	36	28.6	36	29.6	36	30.6	36	31.5	36	32.2	36	33	36	33.7	36	34.4	36
26.4	37	28.2	37	29.5	37	30.6	37	31.6	37	32.4	37	33.3	37	34.1	37	34.8	37	35.5	37
27.2	38	29.2	38	30.4	38	31.6	38	32.6	38	33.5	38	34.3	38	35	38	35.8	38	36.6	38
28.1	39	30.1	39	31.4	39	32.6	39	33.6	39	34.4	39	35.3	39	36.1	39	36.9	39	37.7	39
29	40	30.9	40	32.4	40	33.5	40	34.5	40	35.5	40	36.3	40	37.2	40	38	40	38.7	40
29.8	41	31.8	41	33.3	41	34.5	41	35.6	41	36.5	41	37.4	41	38.2	41	39	41	39.8	41
30.7	42	32.7	42	34.3	42	35.5	42	36.5	42	37.5	42	38.4	42	39.3	42	40.1	42	40.9	42
31.6	43	33.7	43	35.2	43	36.4	43	37.6	43	38.5	43	39.4	43	40.3	43	41.2	43	42	43
32.5	44	34.7	44	36.1	44	37.4	44	38.5	44	39.5	44	40.5	44	41.3	44	42.2	44	43	44
33.4	45	35.6	45	37.2	45	38.4	45	39.5	45	40.5	45	41.5	45	42.4	45	43.3	45	44.1	45
34.3	46	36.5	46	38.1	46	39.3	46	40.5	46	41.6	46	42.5	46	43.4	46	44.3	46	45.2	46
35.2	47	37.4	47	39	47	40.3	47	41.5	47	42.5	47	43.5	47	44.5	47	45.4	47	46.3	47
36.1	48	38.4	48	39.9	48	41.3	48	42.5	48	43.6	48	44.6	48	45.5	48	46.4	48	47.3	48
37	49	39.3	49	41	49	42.3	49	43.5	49	44.5	49	45.6	49	46.6	49	47.5	49	48.4	49
37.9	50	40.2	50	41.9	50	43.3	50	44.5	50	45.6	50	46.6	50	47.6	50	48.6	50	49.5	50
38.7	51	41.1	51	42.8	51	44.2	51	45.5	51	46.6	51	47.7	51	48.7	51	49.6	51	50.6	51
39.6	52	42	52	43.8	52	45.2	52	46.5	52	47.6	52	48.7	52	49.8	52	50.7	52	51.7	52
40.5	53	43	53	44.8	53	46.2	53	47.5	53	48.7	53	49.7	53	50.7	53	51.8	53	52.7	53
41.4	54	44	54	45.7	54	47.2	54	48.5	54	49.6	54	50.8	54	51.8	54	52.9	54	53.8	54
42.4	55	44.9	55	46.7	55	48.2	55	49.5	55	50.7	55	51.9	55	52.9	55	54	55	54.9	55
43.3	56	45.8	56	47.7	56	49.1	56	50.5	56	51.7	56	52.8	56	54	56	54.9	56	56	56
44.2	57	46.7	57	48.6	57	50.2	57	51.5	57	52.7	57	53.9	57	55	57	56	57	57.1	57
45.1	58	47.7	58	49.5	58	51.1	58	52.5	58	53.8	58	55	58	56	58	57.1	58	58.2	58
46	59	48.7	59	50.6	59	52.2	59	53.6	59	54.7	59	55.9	59	57.1	59	58.2	59	59.3	59
46.9	60	49.6	60	51.5	60	53.1	60	54.5	60	55.8	60	57	60	58.2	60	59.3	60	60.3	60
47.8	61	50.5	61	52.5	61	54.1	61	55.6	61	56.9	61	58.1	61	59.2	61	60.3	61	61.4	61
48.7	62	51.4	62	53.5	62	55.1	62	56.5	62	57.8	62	59	62	60.3	62	61.4	62	62.5	62
49.6	63	52.5	63	54.4	63	56.1	63	57.6	63	58.9	63	60.1	63	61.3	63	62.5	63	63.6	63
50.5	64	53.4	64	55.4	64	57.1	64	58.5	64	59.9	64	61.2	64	62.4	64	63.6	64	64.7	64
51.5	65	54.3	65	56.4	65	58.1	65	59.6	65	60.9	65	62.3	65	63.4	65	64.7	65	65.8	65
52.4	66	55.3	66	57.4	66	59	66	60.6	66	62	66	63.2	66	64.5	66	65.7	66	66.9	66
53.3	67	56.2	67	58.3	67	60.1	67	61.6	67	63	67	64.3	67	65.6	67	66.7	67	68	67
54.2	68	57.2	68	59.3	68	61	68	62.6	68	64	68	65.4	68	66.6	68	67.8	68	69	68
55.2	69	58.1	69	60.3	69	62.1	69	63.7	69	65	69	66.4	69	67.7	69	68.9	69	70.1	69
56.1	70	59.1	70	61.2	70	63	70	64.6	70	66.1	70	67.4	70	68.7	70	70	70	71.2	70
57	71	60	71	62.2	71	64	71	65.7	71	67.1	71	68.5	71	69.8	71	71.1	71	72.3	71
57.9	72	60.9	72	63.2	72	65	72	66.6	72	68.1	72	69.5	72	70.9	72	72.2	72	73.4	72
58.8	73	62	73	64.2	73	66	73	67.7	73	69.2	73	70.6	73	71.9	73	73.3	73	74.5	73
59.7	74	62.9	74	65.1	74	67.1	74	68.7	74	70.1	74	71.6	74	73	74	74.3	74	75.6	74
60.7	75	63.9	75	66.2	75	68	75	69.7	75	71.2	75	72.7	75	74	75	75.4	75	76.7	75
61.6	76	64.8	76	67.1	76	69	76	70.7	76	72.3	76	73.7	76	75.1	76	76.4	76	77.8	76
62.6	77	65.7	77	68.1	77	70	77	71.8	77	73.3	77	74.8	77	76.2	77	77.5	77	78.9	77
63.5	78	66.8	78	69	78	71	78	72.7	78	74.3	78	75.8	78	77.2	78	78.6	78	80	78
64.4	79	67.7	79	70.1	79	72	79	73.8	79	75.3	79	76.8	79	78.3	79	79.7	79	81	79
65.3	80	68.6	80	71	80	73	80	74.8	80	76.4	80	77.9	80	79.4	80	80.8	80	82.1	80
66.2	81	69.6	81	72	81	74	81	75.8	81	77.5	81	79	81	80.4	81	81.9	81	83.2	81
67.2	82	70.5	82	73	82	75	82	76.8	82	78.4	82	80	82	81.5	82	82.9	82	84.3	82
68.1	83	71.6	83	74	83	76	83	77.9	83	79.5	83	81	83	82.5	83	84	83	85.4	83
69	84	72.5	84	74.9	84	77.1	84	78.8	84	80.5	84	82.1	84	83.6	84	85.1	84	86.5	84
70	85	73.4	85	76	85	78	85	79.9	85	81.6	85	83.2	85	84.7	85	86.2	85	87.6	85
70.9	86	74.4	86	76.9	86	79	86	80.9	86	82.6	86	84.2	86	85.8	86	87.2	86	88.7	86
71.9	87	75.3	87	77.9	87	80	87	81.9	87	83.6	87	85.3	87	86.9	87	88.3	87	89.8	87
72.8	88	76.4	88	78.9	88	81	88	82.9	88	84.7	88	86.3	88	87.8	88	89.4	88	90.9	88
73.7	89	77.3	89	79.9	89	82.1	89	84	89	85.7	89	87.3	89	88.9	89	90.5	89	92	89
74.6	90	78.3	90	80.9	90	83	90	85	90	86.7	90	88.4	90	90	90	91.6	90	93.1	90
75.6	91	79.2	91	81.8	91	84	91	86	91	87.8	91	89.5	91	91.1	91	92.7	91	94.2	91
76.5	92	80.1	92	82.9	92	85.1	92	87	92	88.8	92	90.5	92	92.2	92	93.7	92	95.3	92
77.4	93	81.2	93	83.8	93	86	93	88.1	93	89.9	93	91.6	93	93.2	93	94.8	93	96.4	93
78.3	94	82.1	94	84.8	94	87.1	94	89	94	90.8	94	92.6	94	94.3	94	95.9	94	97.5	94
79.4	95	83.1	95	85.8	95	88.1	95	90.1	95	91.9	95	93.7	95	95.3	95	97	95	98.6	95
80.3	96	84	96	86.8	96	89	96	91.1	96	93	96	94.7	96	96.4	96	98	96	99.7	96
81.2	97	85	97	87.8	97	90.1	97	92.2	97	94	97	95.8	97	97.5	97	99.1	97	100.8	97
82.2	98	86	98	88.7	98	91.1	98	93.1	98	95.1	98	96.9	98	98.5	98	100.2	98	101.9	98
83.1	99	87	99	89.8	99	92.1	99	94.2	99	96	99	97.9	99	99.6	99	101.3	99	103	99
84	100	87.9	100	90.7	100	93.1	100	95.2	100	97.1	100	98.9	100	100.7	100	102.4	100	104	100

REFERENCIAS BIBLIOGRÁFICAS

[1] KEAGY, Scott, *Integración de redes de voz y datos*, tercera edición, Cisco Publication, Madrid, 2001.

[2] ALERIOS, *Telefonía IP en el entorno corporativo*, http://alerios.blogspot.com/2005_10_01_alerios_archive.html, Octubre 2005, Marzo 2008.

[3] RASGADO, Eduardo, *Teleinformática y Telefonía*, http://us.geocities.com/v.iniestra/apuntes/telefonia/, Marzo 2008.

[4] JÁCOME, Lorena, *Análisis y diseño de una red IP en las instalaciones del IMI con aplicación dirigida a la telefonía*, Quito, Septiembre 2007

[5] JOSCOWICZ, José, *Redes corporativas*, http://iie.fing.edu.uy/ense/asign/redcorp/material/2007/Presentacion%20Redes%20de%20Datos%202007%20(3%20laminas%20por%20pagina).pdf, Abril 2008

[6] Enciclopedia Libre, varios autores, *Familia de protocolos de Internet,* http://es.wikipedia.org/wiki/Familia_de_protocolos_de_Internet, Abril 2008

[7] FELICI, Santiago, *El Nivel De Red En Internet,* http://informatica.uv.es/it3guia/ARS/, Abril 2008

[8] Enciclopedia Libre, varios autores, *IPv6,* http://es.wikipedia.org/wiki/Ipv6, Abril 2008

[9] Enciclopedia Libre, varios autores, *Transmission Control Protocol,* http://es.wikipedia.org/wiki/Transmission_Control_Protocol, Abril 2008

[10] Enciclopedia Libre, varios autores, *UDP,* http://es.wikipedia.org/wiki/Udp, Abril 2008

[11] DELGADO, Cristian*, Análisis Y Evaluación De Parámetros Para Una Óptima Calidad De Servicio En Telefonía IP*, http://cybertesis.uach.cl/tesis/uach/2006/bmfcid3521a/doc/bmfcid3521a.pdf, Valdivia 2006, Abril 2008

[12] IBUJES, Juan, *Voz y Video Sobre el Protocolo de Internet*, Curso dictado en el CIEEPI, Noviembre 2007

[13] *Diagnóstico de red para voz IP,* www.teknos.cl , Abril 2008

[14] CASTAÑEDA, Rodolfo, *Protocolos Para Voz Sobre IP*, www.cudi.edu.mx/primavera_2005/presentaciones/rodolfo_castaneda.pdf, Abril 2008

[15] TRIVIÑO, Javier, *Voz Sobre IP,* Julio 2007, http://www.eslared.org.ve/walc2004/apc-aa/archivos-aa/1e60354f4717edb9fb793dbc5219499d/VoIp_practica.doc, Abril 2008

[16] UNIVERSIDAD DE OVIEDO, ÁREA DE INGENIERÍA TELEMÁTICA. Fundamentos de transmisión de datos, http://www.it.uniovi.es/old/material/cursos/InternetNG_EU_072006/voipcursoV3.pdf, Marzo 2008

FECHA DE ENTREGA:

LUIS MARCELO SOLÍS SÁNCHEZ

AUTOR

ING. GONZALO OLMEDO

COORDINADOR DE LA CARRERA DE INGENIERÍA ELECTRÓNICA, TELECOMUNICACIONES

AB. JORGE CARVAJAL R

SECRETARIO ACADÉMICO