

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

**DISEÑO DE UN ISP SOBRE ADSL PARA PRESTAR EL SERVICIO
DE INTERNET Y SERVICIOS AGREGADOS DE VOZ (VOIP) Y
DATOS, Y ESTUDIO DE FACTIBILIDAD DE IMPLEMENTACIÓN
DEL ISP PARA LA CIUDAD DE PUERTO AYORA EN LA ISLA
SANTA CRUZ (GALÁPAGOS)**

**PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN
ELECTRÓNICA Y TELECOMUNICACIONES**

JORGE DANIEL UQUILLAS LASSO

ldudany@hotmail.com

DIRECTOR: Dr. LUIS CORRALES

lcorrales@epn.edu.ec

Quito, Marzo 2010

DECLARACIÓN

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

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

Jorge Daniel Uquillas Lasso

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Jorge Daniel Uquillas Lasso, bajo mi supervisión.

Doc. Luis Corrales

AGRADECIMIENTO

Le agradezco a mi madre Ruth Magdalena, por apoyarme durante toda mi educación; a Dios por cada día de vida para seguir adelante.

A mi abuela Gioconda por ser tan cariñosa, paciente, por las veces que me daba ánimo y fuerzas para seguir, por ayudarme y siempre estar pendiente de mí.

A mis tíos Luis y Jorge por su apoyo incondicional y su fe constante mostrada hacia mi persona.

A los amigos y amigas con quienes hemos compartido muchas cosas más que sólo las respectivas a nuestra formación profesional, gracias por todo lo vivido en la Escuela Politécnica Nacional y fuera de ella.

Mis más sinceros agradecimientos al Doctor Luis Corrales por su tiempo, acertada dirección, paciencia y colaboración para poder cumplir con este proyecto de titulación.

A los Ingenieros quienes han apoyado las iniciativas y han puesto su granito de arena en los proyectos de los estudiantes.

A Susana Paola por creer en mí a pesar de haberle fallado un par de veces durante la elaboración de este proyecto, siempre me apoyo y nunca me dejo caer.

A todos mis familiares quienes de una u otra manera me presionaban para que siguiera adelante con este proyecto y nunca desfallecer.

DEDICATORIA

Esta tesis se la dedico a toda mi familia pues gracias a ellos lo he podido conseguir; mi abuela Gioconda, mi madre Ruth, mis hermanos Sebastián, Andrea, Pablo y Valeria, tíos, tías, primos, primas.

A Susana Paola.

CONTENIDO

CAPÍTULO 1 ESTUDIO DEL ENTORNO DE IMPLEMENTACIÓN Y DE CONCEPTOS BÁSICOS SOBRE UN ISP Y ADSL	8
1.1 INTRODUCCIÓN.....	8
1.2 DESCRIPCIÓN Y SERVICIOS BÁSICOS DE UN ISP	9
1.3 SERVICIOS QUE OFRECE UN ISP	11
1.3.1 SERVICIOS BÁSICOS.....	11
1.3.1.1 Servicio de Nombre de Dominio (DNS, Domain Name Service)	11
1.3.1.2 Protocolo de Configuración Dinámica de Host (DHCP, Dynamic Host Configuration Protocol)	12
1.3.1.3 Protocolo Simple de Transferencia de Correo (SNMP, Simple Mail Transfer Protocol)	13
1.3.2 SERVICIOS PARA USUARIO FINAL	13
1.3.2.1 Protocolo de Transferencia de Archivos (FTP, File Transfer Protocol)	14
1.3.2.2 Servicio de Correo Electrónico.....	14
1.3.2.3 Servicio Web	15
1.3.2.4 Servicio Telnet.....	16
1.3.2.5 Servicio Web Hosting.....	17
1.3.2.6 Servicio Proxy-Caché	17
1.3.2.7 Servicio de Charla a través de Internet (IRC, Internet Relay Chat)	18
1.3.2.8 Servicio de Voz.....	18
1.3.2.9 Servicio de Video sobre IP	19
1.3.2.9.1 Video broadcast sobre IP.....	20
1.3.2.9.2 Video bajo demanda sobre IP (VoD)	20
1.3.2.9.3 Videoconferencia	20
1.4 SEGURIDADES EN UN ISP.....	21
1.5 ESTUDIO DE LA TECNOLOGÍA ADSL	22
1.5.1 TRANSMISIÓN DE DATOS Y VOZ SOBRE PAR TRENZADO.....	23
1.5.1.1 ADSL.....	24
1.5.1.2 SDSL.....	25
1.5.1.3 HDSL.....	25

1.5.1.4 HDSL-2.....	26
1.5.1.5 G.SHDSL.....	26
1.5.1.6 VDSL.....	26
1.5.2 ORIGEN Y ESTANDARIZACIÓN DE ADSL	28
1.5.3 MODELO DE REFERENCIA PARA EL SISTEMA ADSL.....	30
1.5.4 ARQUITECTURA GENERAL Y FUNCIONAMIENTO DE UNA RED CON ACCESO ADSL.....	32
1.5.5 CODIFICACIÓN DE LÍNEA UTILIZADA EN ADSL.....	34
1.5.5.1 Modulación DMT	34
1.5.5.2 Modulación CAP	36
REFERENCIAS BIBLIOGRÁFICAS.....	37
CAPÍTULO 2 DISEÑO DEL ISP	40
2.1 ESTRUCTURA BÁSICA DEL ISP	40
2.2 REQUERIMIENTOS BÁSICOS DEL DISEÑO	41
2.2.1 DISPONIBILIDAD DE LA RED	42
2.2.2 EFICIENCIA DE LA RED	42
2.3 DETERMINACIÓN DEL ÁREA GEOGRÁFICA.....	44
2.4 DIMENSIONAMIENTO DEL ISP	46
2.4.1 PROYECCIÓN DE LA DEMANDA	48
2.5 INFRAESTRUCTURA DEL ISP	53
2.5.1 RED TRONCAL	53
2.5.2 DISEÑO DE LA RED DEL ISP	54
2.5.2.1 Capa núcleo	55
2.5.2.2 Capa de distribución	55
2.5.2.2.1 VLAN de servidores de administración	56
2.5.2.2.2 VLAN de servidores de aplicación.....	56
2.5.2.2.3 VLAN de dispositivos de acceso	57
2.5.2.2.4 VLAN de dispositivos de conectividad externa.....	57
2.5.2.3 Capa de acceso.....	57
2.5.3 RED DE DISTRIBUCIÓN	57
2.5.4 RED DE ACCESO AL CLIENTE.....	58

2.6 INTEGRIDAD DEL SISTEMA	58
2.6.1 ADMINISTRACIÓN DE USUARIOS Y DEL SISTEMA	58
2.6.2 POLÍTICAS DE SEGURIDAD	59
2.7 CALIDAD DE SERVICIO PARA UN ISP	60
2.7.1 PARÁMETROS DE CALIDAD DE SERVICIO	61
2.7.2 PROCEDIMIENTOS DE CALIDAD DE SERVICIO	62
2.7.2.1 Colas basadas en clases (CBQ)	62
2.7.2.2 Colas equitativas ponderadas (WFQ)	63
2.7.2.3 Tasa de acceso entregado.....	63
2.7.2.4 Descarte aleatorio anticipado.....	64
2.8 ARQUITECTURAS EXISTENTES de QoS	65
2.9 ARQUITECTURA DE SERVICIOS INTEGRADOS (INTSERV)...	65
2.9.1 COMPONENTES DE LA ARQUITECTURA DE SERVICIOS INTEGRADOS	67
2.9.1.1 Control de admisión.....	67
2.9.1.1.1 <i>Funciones básicas:</i>	67
2.9.1.1.2 <i>Aproximaciones para el control de admisión:</i>	68
2.9.1.2 Clasificador de paquetes	69
2.9.1.2.1 <i>Procesamiento de los paquetes en los ruteadores:</i>	69
2.9.1.3 Planificador de paquetes	70
2.9.1.4 Protocolo de reserva	70
2.9.1.4.1 <i>Operación del protocolo RSV</i>	71
2.10 ARQUITECTURA DE SERVICIOS DIFERENCIADOS	
(DIFFSERV)	73
2.11 SELECCIÓN DEL MODELO DE CALIDAD DE SERVICIO....	77
REFERENCIAS BIBLIOGRÁFICAS.....	80
CAPITULO 3 DETERMINACIÓN DE EQUIPOS PARA EL	
ISP	82
3.1 INTRODUCCIÓN.....	82
3.2 REQUERIMIENTO DE LOS EQUIPOS.....	83
3.2.1 RUTEADOR PRINCIPAL.....	83

3.2.2 CONCENTRADOR DE ACCESO O DSLAM	85
3.2.3 MODEM ADSL	86
3.2.4 CONMUTADORES.....	87
3.2.5 CORTAFUEGOS	88
3.2.6 SERVIDORES	89
3.2.6.1 GNU/Linux	91
3.2.6.2 Distribuciones de Linux.....	91
3.2.6.3 CentOS 5.0.....	93
3.2.6.4 Servidor de correo electrónico.....	93
3.2.6.5 Servidor Web	96
3.2.6.6 Servidor FTP.....	97
3.2.6.7 Servidor Caché.....	98
3.2.6.8 Servidor DNS.....	99
3.2.6.9 Servidor administración.....	100
3.3 DIRECCIONAMIENTO IP.....	101
3.4 SELECCIÓN DE EQUIPOS	103
3.4.1 RUTEADOR PRINCIPAL.....	103
3.4.2 CONMUTADORES.....	106
3.4.3 DSLAM	109
3.4.4 MODEM.....	111
3.5 SOFTWARE PARA MONITOREO Y ADMINISTRACIÓN.....	111
3.5.1 MRTG	112
3.5.2 CACTI.....	112
3.6 SEGURIDADES DEL ISP.....	113
REFERENCIAS BIBLIOGRÁFICAS.....	117
CAPÍTULO 4 ESTUDIO DE LA DEMANDA Y COSTOS DE IMPLEMENTACIÓN	119
4.1 ANÁLISIS DE COSTOS.....	119
4.1.1 ESTUDIO DE MERCADO.....	119
4.1.2 ANÁLISIS COSTO – BENEFICIO	121

4.1.2.1	Costos de la implementación inicial	121
4.1.2.1.1	<i>Servidores</i>	121
4.1.2.1.2	<i>Equipamiento adicional</i>	123
4.1.2.1.3	<i>Costo inicial del equipamiento del ISP</i>	123
4.1.2.1.4	<i>Costo de la Implementación inicial del ISP</i>	125
4.1.2.2	Costos anuales del ISP	125
4.1.2.2.1	<i>Acceso a Internet</i>	125
4.1.2.2.2	<i>Sueldos y Salarios</i>	126
4.1.2.2.3	<i>Servicios básicos</i>	127
4.1.2.2.4	<i>Costos última milla</i>	127
4.1.2.3	Equipos	128
4.1.2.3.1	<i>Módems</i>	128
4.1.2.4	Ingresos del ISP	129
4.1.2.5	Total de ingresos y egresos del ISP	130
4.1.3	EVALUACIÓN DEL PROYECTO	131
4.1.3.1	Flujo neto	131
4.1.4	INDICADORES DE RENTABILIDAD	132
4.1.4.1	Tiempo De Recuperación De La Inversión	132
4.1.4.2	Valor actual neto	132
4.1.4.3	Tasa interna de retorno, TIR	133
	REFERENCIAS BIBLIOGRÁFICAS	135
	CAPITULO 5 CONCLUSIONES Y RECOMENDACIONES	136
5.1	CONCLUSIONES	136
5.2	RECOMENDACIONES	141
	ANEXOS	145

RESUMEN

El presente proyecto tiene como objetivo realizar el diseño de un Proveedor de Servicio de Internet para la población de Pto. Ayora en la Isla Sta. Cruz Galápagos, utilizando tecnología ADSL, e integrando el servicio de voz (VoIP) y datos y el análisis de factibilidad para su posible implementación.

En el primer capítulo se presenta una breve introducción del posible Proveedor de Servicios de Internet en la población de Pto. Ayora, la arquitectura del ISP, servicios que este ofrece, funcionamiento y seguridades.

Se profundiza en la tecnología ADSL en la cual está basada la implementación del ISP, la transmisión de datos sobre el par trenzado, las diferentes tecnologías relacionadas con ADSL, sus orígenes, revisión del modelo de referencia y las codificaciones que este utiliza.

En el segundo capítulo se abarca todo lo relacionado con el diseño del ISP, se definen requerimientos que este debe tener, se define una arquitectura básica para el ISP, se determina el área geográfica y se realiza el dimensionamiento del mismo. Se habla de la infraestructura que el ISP debe tener, utilizando un modelo de referencia sobre el cual se profundiza el diseño. Además se presenta la selección del modelo de Calidad de Servicio más adecuado para el ISP; y finalmente se presenta el diseño que podría ser implementado.

En el tercer capítulo se presentan algunas opciones de diferentes marcas para la selección de los equipos que pudieran instalarse en el caso de implementación del proyecto. Se detalla el direccionamiento IP que podría ser usado en el proyecto y se presentan configuraciones recomendadas para los equipos. Se finaliza el capítulo presentando opciones para la parte de seguridad del ISP.

En el cuarto capítulo se realiza un análisis de costos de la posible implementación del proyecto, utilizando herramientas financieras como es el caso del Valor Actual Neto y la Tasa Interna de Retorno.

Para finalizar, en el quinto capítulo se realizan las conclusiones y recomendaciones que del presente proyecto se obtienen.

CAPÍTULO 1

ESTUDIO DEL ENTORNO DE IMPLEMENTACIÓN Y DE CONCEPTOS BÁSICOS SOBRE UN ISP Y ADSL

Este proyecto tiene como objetivo diseñar un ISP usando la tecnología ADSL para la ciudad de Puerto Ayora en la Isla Santa Cruz (Galápagos) y ofrecer el servicio de Internet, servicios agregados de voz (VoIP) y datos a los habitantes y empresas del sector. Así mismo realizar un estudio de factibilidad de implementación del ISP diseñado.

A continuación se presenta la teoría necesaria para la realización del presente proyecto. Entre los tópicos se trata todo lo relacionado a un ISP como: servicios, red del ISP, seguridades, etc. Adicionalmente se trata lo relacionado a la tecnología ADSL conceptos básicos e implementación del mismo.

1.1 INTRODUCCIÓN

Si bien un ISP en general tiene como función entregar a los usuarios el servicio de acceso al Internet, este debe orientarse a las necesidades de los mismos, en este caso en particular, a la población de Puerto Ayora en la isla de Santa Cruz Galápagos.

Debido a la gran demanda de la población de comunicarse con el resto del mundo, el Internet se convierte en una herramienta clave para acercarlos al mundo externo. Cada persona o usuario tiene sus propias necesidades, pero en el caso de la población de Galápagos esta es de particular importancia, por lo que es necesario definir una excelente estrategia para cubrir dichas necesidades.

Una de las necesidades más apremiantes en dicha población es la relacionada a las comunicaciones, ya que por su peculiar ubicación geográfica se ve en la

necesidad de enlazarse de alguna manera con las personas del continente. La mejor manera de satisfacer esta necesidad es usar una herramienta que permite no solo la transmisión de datos, sino también de voz y video. Es por este motivo que se ha pensado en un ISP en las Islas, capaz de manejar parámetros de Calidad de Servicio que garantice un desempeño adecuado.

Los ISPs llegan a los usuarios por diferentes medios como por ejemplo línea telefónica, modem de alta velocidad, enlaces de radio, etc. Cada vez se implementan nuevos métodos de acceso. En el presente trabajo se utilizará el par trenzado por diversos factores, entre ellos se puede citar, su disponibilidad y su costo.

Los elementos principales de un ISP son los dispositivos llamados servidores, que están permanentemente disponibles, pues desempeñan funciones esenciales para proveer el servicio a los clientes y poseen la información que requiere la red.

1.2 DESCRIPCIÓN Y SERVICIOS BÁSICOS DE UN ISP [1]

Un Proveedor de Servicios de Internet es un punto intermedio entre el usuario y el Internet. Puede estar unido directamente a un NAP (Network Access Point - Punto de Acceso a la Red) o a otro ISP más grande mediante ruteadores, y para llegar a los clientes hace uso de líneas telefónicas, modems de alta velocidad, enlaces de radio, etc., de su propiedad, o subordinados a otras empresas dedicadas a brindar acceso de última milla hacia los usuarios.

Los ISPs no solo comercializan el servicio de conexión a Internet, sino que son responsables del adecuado funcionamiento de la conexión, y de brindar servicios mediante sus servidores. Para diseñar un ISP se puede considerar el modelo jerárquico de redes, el cual separa la red de computadores en módulos autónomos con funcionalidades bien diferenciadas para facilitar la resolución de problemas.

Las capas del modelo Jerárquico de Redes son las siguientes:

Capa de Núcleo. Esta capa constituye la parte principal o el backbone de la red. Debe poseer gran velocidad de conmutación de paquetes.

Capa de Distribución. Esta capa administra las políticas de conexión. Su objetivo principal es definir claramente los límites de las capas. Aquí se da la manipulación de paquetes en base a políticas de conectividad.

Capa de Acceso. Esta capa provee el acceso dentro de la red a los usuarios finales locales. Puede emplear filtros o listas de acceso para optimizar la atención a ciertos usuarios.

La estructura de un ISP empleando los tres niveles jerárquicos de interconexión, se indica en la Figura 1.1.

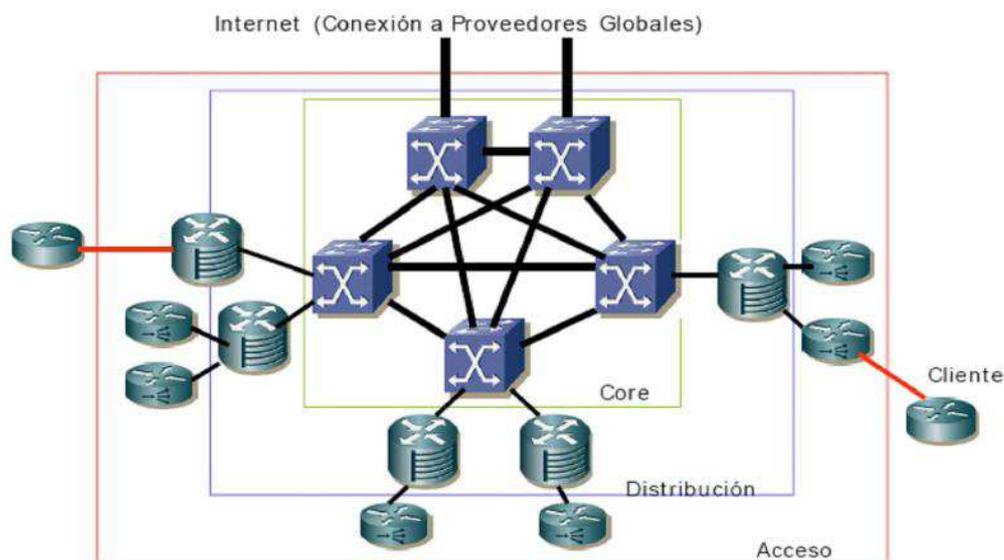


Figura 1.1 Capas del Modelo Jerárquico para un ISP [2]

Dentro de esta infraestructura, un ISP debe contar con los elementos para brindar un excelente servicio, esto es fiabilidad, estabilidad, escalabilidad, accesibilidad, entre otros. Esto se puede lograr por medio de servidores orientados a cada servicio. A continuación se detallan los servicios ofrecidos por medio de los servidores de un ISP.

1.3 SERVICIOS QUE OFRECE UN ISP [3], [4]

El Internet se caracteriza por brindar una gran variedad de servicios a los usuarios.

Los ISPs brindan este tipo de servicios dependiendo del usuario a quien van dirigidos, no es lo mismo un usuario *corporativo* que un usuario *residencial*. Un usuario corporativo tiene requerimientos más complejos en cuanto a seguridad, disponibilidad y garantía.

Los servicios proporcionados por el ISP, sirven para tareas específicas y pueden clasificarse de la siguiente en:

- Servicios básicos
- Servicios para usuario final

1.3.1 SERVICIOS BÁSICOS

Son aquellos que soportan a las demás aplicaciones. Suelen utilizarse para actividades de administración y monitoreo de la red. Algunos se resumen a continuación:

1.3.1.1 Servicio de Nombre de Dominio (DNS, Domain Name Service) [22], [5]

Este se encarga de la traducción entre nombres de dominio y direcciones IP mediante una base de datos distribuida y jerárquica que almacena dicha información. DNS permite que las personas utilicen nombres de dominio, porque son mucho más fáciles de recordar que números.

DNS puede asociar distintos tipos de información a cada nombre aunque el uso más común es la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. Por ejemplo

transforma `www.google.com` a `64.233.187.99`. Así, cuando se llama a un servidor por su nombre de dominio, un servidor DNS lo traduce a su dirección IP.

A la etiqueta ubicada más a la derecha se la llama *dominio de nivel superior*. Cada una de las etiquetas a la izquierda especifica un subdominio o subdivisión. Cada subdivisión admite hasta 127 niveles, y una etiqueta puede tener hasta 63 caracteres, mientras la longitud total del nombre del dominio no exceda 255 caracteres. La parte más a la izquierda del dominio expone el hostname y el resto especifica la manera de crear una ruta lógica a la información requerida.

1.3.1.2 Protocolo de Configuración Dinámica de Host (DHCP, Dynamic Host Configuration Protocol)

DHCP es un protocolo en el que un servidor va asignando direcciones IP dinámicas a equipos clientes habilitados para DHCP. Así se reduce la complejidad de la administración de configuraciones de red. DHCP permite supervisar y distribuir de forma centralizada las direcciones IP, además de asignar automáticamente y enviar una nueva IP si el computador es conectado en un lugar diferente de la red.

Sin DHCP las direcciones IP deben configurarse manualmente en cada computador. Existen tres métodos de asignación de direcciones IP mediante DHCP:

Asignación manual: Se basa en una tabla con direcciones MAC, solo se asigna la dirección IP a los equipos cuya MAC consta en la tabla.

Asignación automática: Una dirección IP libre que pertenece a un rango dado, es asignada permanentemente a la computadora que la requiere.

Asignación dinámica: Al iniciar cada computador solicita una dirección IP al servidor, el mismo que le asigna una por un tiempo determinado por el administrador de la red.

1.3.1.3 Protocolo Simple de Transferencia de Correo (SMTP, Simple Mail Transfer Protocol) [6]

SMTP es un estándar basado en el modelo cliente servidor, para intercambiar correo electrónico entre computadores de manera confiable y eficiente. Este protocolo define el formato de los mensajes pero no la forma en que éstos se almacenan o la frecuencia de envío.

La entrega del mensaje se inicia al transferir el mensaje a un servidor SMTP dedicado. SMTP utiliza el nombre de dominio de la dirección de correo electrónico del destino para iniciar la comunicación con un DNS, que devuelve el nombre de host del servidor SMTP de destino para ese dominio. El servidor SMTP origen se comunica directamente con el servidor SMTP de destino por el puerto 25 de TCP.

Cuando el nombre de usuario de la dirección de correo electrónico del destinatario concuerda con una cuenta de usuario autorizada en el servidor de destino, el mensaje se transfiere a dicho servidor, y se espera que el destinatario recoja el mensaje mediante un programa cliente.

Si el servidor SMTP origen no puede comunicarse directamente con el servidor de destino, SMTP puede transferir mensajes a otros servidores SMTP intermedios para retransmisión, éstos reciben el mensaje original y lo entregan a otro servidor de retransmisión hasta llegar al destino o hasta que termine el tiempo de espera designado.

1.3.2 SERVICIOS PARA USUARIO FINAL

Estos servicios son utilizados por el usuario final, algunas de las más conocidas se detallan a continuación:

1.3.2.1 Protocolo de Transferencia de Archivos (FTP, File Transfer Protocol) [7]

El servicio FTP es un mecanismo simple para intercambiar archivos entre computadores dentro de la red. Permite acceder a un servidor FTP a través de un nombre de usuario y contraseña para ver, descargar, borrar, renombrar, mover y copiar archivos en el servidor. También permite enviar archivos desde un computador local hacia el servidor o de un servidor a otro.

Es necesario un servidor FTP y un cliente FTP. Cuando los servidores son de libre acceso se trata de FTP anónimo, en estos casos generalmente se puede descargar archivos desde el servidor más no enviar.

FTP dispone de un sistema de corrección de errores para garantizar la integridad de los datos. Es utilizado para el transporte de páginas HTML desde el computador de desarrollo hacia el servidor Web y descargar programas desde los servidores FTP en Internet. Se pueden utilizar clientes FTP desde la línea de comando o interfaces gráficas. La mayoría de páginas Web a nivel mundial son colocadas en sus servidores mediante el uso de este protocolo.

Por defecto FTP utiliza el puerto 20 para el flujo de datos entre cliente servidor y el puerto 21 para control de flujo, es decir para enviar órdenes del cliente al servidor.

1.3.2.2 Servicio de Correo Electrónico [8]

El servicio de correo electrónico (e-mail) es una de las aplicaciones más utilizadas a nivel de Internet. Permite enviar y recibir mensajes entre usuarios de la red, a través de medios electrónicos, incluso adjuntando archivos de cualquier índole. Es muy útil comparado con el correo tradicional, ya que es más económico y más rápido. Los ISPs entregan una o más cuentas a sus clientes pero también debe limitar el tamaño de los correos electrónicos y el tiempo que los almacenará para optimizar recursos.

Este servicio utiliza los protocolos SMTP para transferir los correos electrónicos de modo confiable y eficiente; y POP3 (Protocolo de Oficina Postal Versión 3) o IMAP4 (Protocolo de Acceso de Mensajes de Internet Versión 4) que permiten el acceso a los buzones de correo por parte de los usuarios.

El intercambio de correo electrónico entre distintos sitios lo realizan los Agentes de Transferencia de Mensajes (MTA, Message Transfer Agent), que son agentes de software que transfieren los mensajes desde un computador a otro. El cliente destino puede estar desconectado cuando llega el correo. Cuando un usuario envía un mensaje especificando la dirección del destinatario, el mensaje queda almacenado en el servidor hasta que el usuario destino abre su cuenta y solicita los mensajes.

1.3.2.3 Servicio Web [9]

Un servicio Web es un conjunto de protocolos y estándares que sirven para intercambiar datos entre distintas aplicaciones de software, desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma.

Los servicios Web son equivalentes a cualquier aplicación que corre en un equipo local, pero la información necesaria para alguna tarea es enviada al servidor y el resultado se devuelve al usuario, ambos en la forma de contenido Web.

Se requiere de un navegador Web para acceder a este servicio, extraer documentos o páginas Web y visualizarlos. Los documentos pueden contener información en formato de texto plano, imágenes, sonidos, animaciones, etc., y el usuario puede seguir los hiperenlaces de una página a otros documentos, o enviar información al servidor.

WWW (World Wide Web) tiene su inicio en 1989 en el Centro Europeo de Investigación Nuclear (CERN). Nació con la intención de difundir de manera uniforme y simple, contenidos científicos a través de la red. Un sistema de hipertexto enlazaría todos los documentos entre sí para que el lector pudiera

revisar las referencias de un artículo mientras lo fuera leyendo. El gran avance de la “www” admite hoy incluso servicios en tiempo real como webcasts, radio Web y webcams en directo. Su funcionalidad se basa en tres estándares:

- **URL (Localizador Uniforme de Recursos).** Detalla la asociación de la información con una "dirección" única en donde encontrarla. Está compuesto de tres partes. Método de acceso, nombre de host y ruta de acceso.
- **HTTP (Protocolo de Transferencia de Hipertexto).** Especifica la manera en que el navegador y el servidor intercambian información en forma de solicitudes y respuestas.
- **HTML (Lenguaje de Marcación de Hipertexto).** Lenguaje de marcación diseñado para estructurar textos y presentarlos en forma de hipertexto que es el formato estándar de las páginas Web.

El Consorcio World Wide Web (W3C) es el organismo que regula los estándares Web, y asegura el acceso universal a la información.

1.3.2.4 Servicio Telnet ^[10], ^[11]

Este servicio utiliza el protocolo TELNET (Terminal Virtual), que se ejecuta sobre TCP en el puerto 23. Telnet es el nombre de un protocolo y del programa informático que implementa el cliente para tener acceso remoto a un equipo por medio de la red, creando un canal virtual de comunicaciones como si se estuviera utilizando un terminal de consola o una de sus terminales físicas.

Telnet es una herramienta muy útil para arreglar fallas o consultar datos a distancia. No puede acceder cualquier persona, ya que por seguridad se utilizan nombres de usuario y contraseñas, aunque viajen por la red sin cifrado. Por esta razón apareció SSH, que es una versión cifrada de Telnet pero emplea mecanismos de autenticación de usuario más seguros. Un cliente telnet es un programa de emulación de terminal para teleproceso adaptado al sistema de

Internet, es decir, al protocolo TCP/IP. Una vez establecida la conexión, los comandos a utilizar son los mismos que se usarían frente a un computador remoto. Si por algún motivo Telnet no logra realizar conexión, mostrará un mensaje diciendo que el host es desconocido.

1.3.2.5 Servicio Web Hosting [12]

Este servicio consiste en alquilar a los usuarios un espacio en el disco del servidor Web del ISP para alojar sus páginas Web, html, php, etc., para su publicación. El servicio de Web Hosting permite a las empresas tener presencia en Internet de forma fácil y económica ya que los costos del cliente se reducen al compartir el costo de hardware, aplicaciones, licencias, sistemas operativos y mantenimiento con los demás sitios Web alojados en el servidor.

1.3.2.6 Servicio Proxy-Caché [13], [14]

El servicio Proxy-Caché es utilizado por algunos navegadores para tener un acceso indirecto a otros servidores Web o FTP con el objetivo de incrementar la velocidad de acceso a Internet. El Servidor Caché almacena una copia local y temporal en su memoria de todas las páginas y archivos solicitados por los usuarios, evitando las conexiones directas con los servidores remotos. Cuando un cliente Proxy solicita una página Web, el servidor Proxy- Caché busca en su base de datos para ver si posee una copia de la página solicitada. Si es así, la envía directamente al usuario, sin buscarla en Internet; es decir, actúa como un intermediario. Caso contrario, irá a la fuente original a solicitarla y se tardará lo mismo que si no hubiera proxy. Pero la siguiente vez que alguien solicite esa información, el acceso será más rápido.

Así se mejoran los tiempos de respuesta en enlaces lentos, para acceder a destinos fuera de la red, frente a enlaces locales rápidos. Una vez configurado el acceso a www mediante un servidor Proxy-Caché, todos los accesos se realizarán a través de éste de forma transparente al usuario.

1.3.2.7 Servicio de Charla a través de Internet (IRC, Internet Relay Chat) [15], [16]

El Servicio IRC permite intercambiar mensajes escritos en tiempo real, con decenas de usuarios alrededor del mundo en una misma conversación. Se basa en la técnica cliente/servidor y utiliza TCP para el transporte de los datos, generalmente el puerto utilizado es el 6667.

Para acceder a este servicio se requiere de un programa cliente como interfaz entre el usuario y el programa servidor. El programa servidor está en el equipo remoto y su dirección debe configurarse en el programa cliente. A cada lugar virtual se lo llama “canal” y es allí donde los usuarios comparten opiniones acerca de un tema específico. Existe un gran número de canales, cada uno con un nombre relativo al tema en discusión. Es posible conectarse a varios canales o mantener una conversación privada con otro usuario conectado.

1.3.2.8 Servicio de Voz [17], [18], [19]

Este servicio consiste en aprovechar la infraestructura de Internet para la transmisión de voz, mediante la utilización del protocolo IP.

El gran crecimiento de las redes IP en Internet, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real y nuevos estándares de Calidad de Servicio, han creado el entorno adecuado para la transmisión de voz sobre IP.

Con la integración de tecnologías que permiten convergencia de redes de voz y datos en los mismos ruteadores que controlan el tráfico a través de Internet, la “telefonía IP” se ha convertido en “comunicación IP”, unificando telefonía, correo de voz, e-mail, servicios de datos, aplicaciones empresariales y videoconferencia, a través de un teléfono IP.

La transmisión de voz es diferente a la de datos, pues requiere de conceptos de telefonía, redes, ingeniería de tráfico y calidad de servicio. Un sistema de voz

sobre IP debe realizar tres operaciones básicas: digitalización de la voz, conversión de la señal en paquetes IP y enrutamiento de los paquetes.

Se pueden generar tres tipos de llamadas: computador-computador, computador-teléfono y teléfono-teléfono a través de IP. Los procedimientos de señalización de voz sobre IP son muy importantes ya que establecen, mantienen, administran y proveen Calidad de Servicio al transmitir voz en paquetes. Los estándares utilizados se conocen como H.323 y se emplean en la señalización y transmisión de voz en tiempo real, video y datos, dentro de una red de paquetes.

Para el servicio de VoIP utilizan protocolos que garanticen Calidad de Servicio y no utilicen retransmisiones, dando prioridad a la voz sobre los datos, y controlando el número máximo de saltos y los demás factores que aumentan el retardo de transmisión.

1.3.2.9 Servicio de Video sobre IP [20], [21]

En la actualidad, la utilización de las redes para la transmisión de vídeo ha tenido un crecimiento masivo, ya que el Internet se utiliza para muchos fines como ver películas, descargar videos, clases remotas, televisión, etc. Estas aplicaciones demandan gran ancho de banda, lo que contribuye a la presencia de problemas como cuellos de botella, lentitud en la reproducción de imágenes, errores de transmisión y pérdidas de datos.

A pesar de que las señales de video son de naturaleza analógica, se puede transmitir las también de forma digital teniendo grandes ventajas como mayor fiabilidad, mecanismos de detección de errores, inmunidad a interferencias y ruido, mejor codificación y encriptado, etc. Los avances en la tecnología han permitido capturar, digitalizar, secuenciar y transmitir señales compuestas de video y voz sobre Internet. La señal procesada y comprimida se almacena en un servidor de video para luego enviarla a través de la red. La compresión del vídeo generalmente involucra pérdida de información y disminución de calidad. El vídeo

comprimido es más sensible a los errores ya que un error puede hacer ilegible la imagen.

Existen tres tipos de Video sobre IP:

1.3.2.9.1 Video broadcast sobre IP

Consiste en la transmisión de un archivo con contenido de vídeo, hacia ciertos puntos de la red. La transmisión es unidireccional; es decir, los puntos de destino son visualizadores pasivos y no tienen ningún tipo de control en la sesión. Los videos pueden ser en tiempo real o pregrabados.

El Video broadcast se origina en el servidor y puede ser Unicast. Generalmente la configuración Multicast se implementa en ambientes corporativos para capacitación o presentaciones, y en centros de educación para difundir material didáctico.

1.3.2.9.2 Video bajo demanda sobre IP (VoD)

VoD sobre IP (Video on Demand over IP), es un servicio que permite a un usuario seleccionar y ver contenido de video almacenado en un servidor de una red. Es diferente de Video broadcast, porque se trata de un video interactivo, en donde el usuario puede visualizar en tiempo real, iniciar y suspender un vídeo almacenado en un servidor central de vídeo. Entre sus aplicaciones se encuentran: capacitación, aprendizaje, entretenimiento y cualquier área donde el usuario precise visualizar los archivos según su itinerario.

1.3.2.9.3 Videoconferencia

El servicio Videoconferencia (VC) sobre IP combina transmisiones full dúplex tanto de video como de audio, permitiendo que usuarios ubicados en distintos puntos geográficos puedan verse y escucharse como si estuvieran en el mismo lugar. El abaratamiento y disponibilidad de los equipos y servicios de

videoconferencia han ocasionado que esta industria sea de gran crecimiento en el mercado de teleconferencias. Se puede tener videoconferencia punto - punto o punto - multipunto.

No se debe confundir la Videoconferencia con la "televisión interactiva" que consiste en la interacción entre una persona y un programa educativo grabado con anterioridad, pero que no requiere de la transmisión de video.

Las normas H323 permiten Videoconferencia sobre IP. La conferencia puede iniciarse desde cualquier computador que disponga de cámara y micrófono. Entre las aplicaciones más conocidas se encuentra: e-learning, telemedicina, reuniones corporativas, capacitación. Para tener un buen funcionamiento de video en tiempo real en Internet, se debe implementar mecanismos de priorización de tráfico de vídeo y voz (Calidad de Servicio). Se debe utilizar el bit llamado Tipo de Servicio (TOS, Type of Service) que se encuentra en el encabezado IP. La Calidad de Servicio consiste en parámetros que proporcionan un buen desempeño de la red frente a tráfico sensible al retardo o a errores de transmisión.

A continuación se analiza como los futuros clientes o usuarios acceden a estos servicios; es decir, la última milla o bucle local.

1.4 SEGURIDADES EN UN ISP [²²], [²³]

El Internet es un entorno en el que tanto el ISP como sus clientes pueden ser objeto de cualquier tipo de infiltración. A pesar de que no existe seguridad absoluta, es imprescindible dotar al ISP de mecanismos de contención para impedir que intrusos destruyan o contaminen la red. Estos mecanismos no solo deben evitar problemas sino ser capaces también de resolverlos en el caso de que se presenten.

Se debe realizar una planificación de la seguridad, para lo cual es necesario identificar lo que se quiere proteger, determinar las posibles amenazas, implementar las medidas necesarias y revisar continuamente el proceso.

En un ISP es importante proteger el hardware, el software y la información. Es necesario proporcionar seguridad física a los elementos del ISP. Separar el tráfico en varias redes puede ayudar también a brindar seguridad. Es también importante controlar cualquier tipo de ataque mediante el cortafuegos.

1.5 ESTUDIO DE LA TECNOLOGÍA ADSL

Gracias a los estudios realizados sobre el par trenzado de cobre hoy en día, se puede sacar un mayor provecho del mismo para poder prestar varios servicios, tales como Internet, voz y datos. El tender una red de cobre en una gran área requiere un minucioso estudio del lugar, no solo en el aspecto físico sino también en el aspecto económico del mismo.

Con el pasar de los años y el auge del Internet, este servicio se ha convertido hoy en día en algo indispensable, ya sea para comunicación con alguien del exterior o simplemente leer una noticia. Pero en nuestro país este servicio tiene un costo elevado y no todos tienen acceso al mismo.

La última milla o bucle local influye en el costo del servicio del Internet, así, el usar par trenzado en lugar de cable coaxial o fibra óptica, ayuda mucho para abaratar los costos en los usuarios y de la empresa misma.

Uno de los factores más influyentes en las empresas proveedoras de servicios en escoger al par trenzado como medio de transmisión, está en el hecho del costo beneficio que el mismo puede llegar a producir, con una mínima inversión en comparación de si se utilizara coaxial o fibra.

MEDIO DE TRANSMISIÓN	ANCHO DE BANDA	DISTANCIAS MEDIAS	CAPACIDAD MÁXIMA	REPETIDORES	ATENUACIÓN
PAR TRENZADO	4 MHz	100 m 65 MHz	4 Mbps	2 a 10 Km	3 a 30 dB/Km 1 KHz a 1 MHz
CABLE COAXIAL	350 MHz	500	500 Mbps	1 a 10 Km	3 a 30 dB/Km 1 MHz a 1 GHz
FIBRA OPTICA	2 GHz	2 km (Multi.) 100 km (Mono.)	2 Gbps	10 a 100 Km	0.2 a 3 dB/Km 1 THz a 1000 THz

Tabla 1.1 Comparación entre algunos medios de transmisión. [24], [25], [26]

De lo expuesto anteriormente se justifica el hecho de que los ISPs (Internet Service Provider) y compañías fabricantes de equipos de telecomunicaciones se hayan interesado en desarrollar tecnologías para mejorar el rendimiento de los cables de cobre, y usarla en el futuro.

1.5.1 TRANSMISIÓN DE DATOS Y VOZ SOBRE PAR TRENZADO. [24]

En un principio el par trenzado se empleó en las redes de telefonía; es decir, para la transmisión de la voz. Posteriormente y gracias a los desarrollos en el área de procesamiento digital de señales y semiconductores se logró transmitir por un mismo canal voz y datos, obteniendo velocidades de hasta 56,6 Kbps con los módems V.90. Las señales de datos transmitidas por estos módems son tratadas como señales de voz, de ahí su sencillez y bajos costos para los proveedores y usuarios. La velocidad de transmisión sobre este medio está relacionada directamente con la longitud del mismo, así, a distancias de 25 Km se tendría velocidades de 9,6 Kbps

La tecnología **xDSL (x Digital Subscriber Line-Línea Digital de Abonado)** provee soporte para la transmisión de servicios de banda ancha sobre la red existente de

cobre. Sin embargo, se puede utilizar dicha tecnología para usarla fundamentalmente en el servicio de Internet, y no como fue en un principio para brindar servicio de voz.

El término xDSL abarca un gran número de tecnologías similares que compiten entre sí para acoplarse a las necesidades de los usuarios, entre los cuales se puede mencionar ADSL, SDSL, HDSL, HDSL-2, G.SHDSL, IDSL y VDSL.

1.5.1.1 ADSL [24], [27]

La tecnología DSL asimétrica fue introducida en un principio para proveer servicios de video bajo demanda (VoD video-on-demand) a los usuarios residenciales. Después el VoD fue abandonado y el uso del Internet se volvió el objetivo de ADSL el cual fue desarrollado para tasas de datos altas y asimétricas, ideal para la carga de contenidos multimedia del Internet. Ofrece rangos de tasa de datos en dirección de bajada que varían desde 1 a 8 Mbit/s y de subida desde 16 a 800 kbit/s. La distancia de operación puede ser por arriba de los 5 km dependiendo de la calidad del cable. Los módems ADSL son estandarizados para ser de tasa adaptiva, así es posible adaptar la tasa de los datos según las condiciones de la línea. Para los usuarios residenciales una cualidad del ADSL es que este puede ser usado simultáneamente sobre el mismo par de cobre existente del POTS (Plain Old Telephone Service - Servicio telefónico ordinario antiguo). Entonces los llamados POTS splitters son requeridos para separar las señales POTS y ADSL.

ADSL utiliza dos esquemas de codificación; el primero llamado CAP (Carrierless Amplitude Modulation – Modulación de amplitud sin portadora) y el otro DMT (Discrete Multitone Technology – Tecnología de multitono discreto). DMT fue elegido por la ITU-T como el primer estándar para ADSL (G.992.1 and G.992.2), todos sus sucesores como ADSL2 y ADSL2+ son basados en este tipo de codificación.

1.5.1.2 SDSL [24], [27]

La Línea Digital de Subscriptor Simétrica (SDSL) es una versión de tasa-adaptiva de HDSL, y como HDSL es simétrico permite una tasa de transferencia de bajada igual desde una oficina central del NSP (Network Service Provider) hacia el lugar del consumidor, así como de subida desde el subscriptor hacia la oficina central. SDSL soporta datos solo en una línea simple y no soporta llamadas analógicas. SDSL usa el código de línea 2B1Q y puede transmitir arriba de 1.54 Mbps hacia y desde el subscriptor, o puede ser configurado para ofrecer rangos variables de tasas de bit arriba de 1.45 Mbps

Debido a que el tráfico es simétrico, la transferencia de archivos, el web hosting, y aplicaciones de aprendizaje a distancia pueden ser implementados efectivamente con SDSL.

1.5.1.3 HDSL [24], [27]

Originalmente desarrollado por Bellcore, las tecnologías DSL de altas tasas de bit (HDSL)/T1/E1 han sido estandarizados por la ANSI en los Estados Unidos y por la ETSI en Europa. El estándar de la ANSI cubre transmisiones T1 sobre dos pares, con una tasa de 784 Kbps en cada par trenzado. Existen estándares para ambos sistemas de la ETSI, para un sistema E1 de dos pares, con cada par llevando 1168 Kbps, y un sistema E1 de tres pares, con 784 Kbps en cada par trenzado.

HDSL se ha hecho popular ya que es una mejor vía de proveer T1 o E1 sobre líneas de cobre de par trenzado que la tan usada técnica conocida como Alternative Mark Inversion (AMI) - Inversión de Señal Alternativa. HDSL usa menor ancho de banda y no requiere repetidores arriba de los rangos CSA (9000 pies para 26 AWG y 12000 pies para 24 AWG) [28]. Usando una ecualización de línea adaptiva y modulación 2B1Q, HDSL transmite 1.544 Mbps o 2.048 Mbps. La instalación de un sistema HDSL es más barato que un sistema AMI y con relación al tiempo es menor, debido a la instalación de repetidores entre el subscriptor y el

CO (Central Office – Oficina Central). Así dependiendo de la longitud de la línea el costo de los repetidores para un sistema AMI aumenta con la misma.

HDSL tiene desventajas, primero no provee existencia para la voz analógica porque este usa la banda de la voz. Segundo ADSL alcanza mejores velocidades que HDSL porque la asimetría de ADSL deliberadamente mantiene la interferencia (crosstalk) a un final de la línea. Sistemas simétricos como HDSL tienen interferencia (crosstalk) en ambos finales.

1.5.1.4 HDSL-2 [24], [27]

HDSL-2 es un estándar emergente y una alternativa prometedora para HDSL. La intención es de ofrecer un servicio simétrico a velocidades T1 usando un par simple de cable antes que dos pares. Este requerirá modulación más agresiva, distancias cortas (alrededor de 10.000 pies), y mejores líneas telefónicas.

La ventaja más grande de HDSL-2, la cual fue desarrollada para servir como estándar, por el cual equipos de diferentes marcas pueden interoperar, es que este fue designado para no interferir con otros servicios. Sin embargo, HDSL-2 es solo tasa full, ofreciendo servicios solo hasta 1.5 Mbps

1.5.1.5 G.SHDSL [24], [27]

G.SHDSL es un estándar basado en una versión de tasa múltiple de HDSL-2 y ofrece servicio simétrico. La multi tasa de HDSL-2 es parte del problema 2 del estándar conocido como G.SHDSL, y es ratificado por la ITU. G.SHDSL se construye sobre los beneficios de HDSL-2 ofreciendo tasas simétricas de 2.3 Mbps

1.5.1.6 VDSL [24], [27]

VDSL trasmite datos de alta velocidad sobre cortos alcances de la línea telefónica de par trenzado, con rangos de velocidad dependiendo de la longitud actual de la

línea. La tasa máxima de bajada bajo consideración es entre 51 y 55 Mbps, sobre líneas arriba de los 1000 pies (300 mts) de longitud. Tasas de bajada tan menores como 13 Mbps sobre distancias cercanas a los 4000 pies (1500 mts) son comunes también. Tasas de subida en modelos recientes serian asimétricos, tal como ADSL, con velocidades desde 1.6 a 2.3 Mbps. Ambos canales de datos serán separados en frecuencia desde las bandas usadas por el servicio telefónico básico y la Red Digital de Servicios Integrados (ISDN), habilitando a los proveedores de servicio para que cubran VDSL en los servicios existentes. Actualmente, los canales de alta velocidad son también separados en frecuencia. Como las necesidades surgen para canales de subida de alta velocidad o para tasas simétricas, los sistemas VDSL quizá necesiten usar cancelación de eco.

Tipo de DSL	Velocidad Descendente (Mbps)	Velocidad Ascendente (Mbps)	Distancia de la línea (m)	Aplicación
ADSL	1.544 to 6.1	0.928	3600	Usado para Internet y acceso Web, video conferencia, video bajo demanda VoD, acceso remoto a una LAN
ADSL G.lite	1.5	0.512	5400	Similar a ADSL
HDSL	1.544 en 2 pares y 2.048 en 3 pares	1.544 en 2 pares y 2.048 en 3 pares	3600	Servicio de E1/T1 entre un servidor y la empresa telefónica o una compañía WAN,
SDSL	1.544	1.544	3000	Lo mismo que HDSL pero requiere solo una línea de par trenzado.
SHDSL	2.312 en 1 par y 4.624 en 2 pares	2.312 en 1 par y 4.624 en 2 pares	1800	Para aplicaciones de negocios, alojamiento de la página web, ftp o otro tipo de servidores

VDSL	de 12.9 a 52.8 y de 1.6 a 2.3	de 1.5 a 2.3	de 300 a 1000	Redes ATM, fibra para el vecindario.
-------------	----------------------------------	--------------	---------------	---

Tabla 1.2 Características principales de las tecnologías xDSL [²⁹], [³⁰]

De todas las tecnologías antes mencionadas se da prioridad a ADSL ya que es la que se utiliza en este proyecto.

1.5.2 ORIGEN Y ESTANDARIZACIÓN DE ADSL [24]

Esta tecnología tiene sus inicios en 1989, con un investigador de la empresa Bellcore llamado Joe Lechleider. Posteriormente, ANSI toma la iniciativa de normalizarla, asignando el número T1.413 al grupo de trabajo encargado de dicha estandarización con su primer trabajo publicado en 1995.

El estándar ANSI T1.413 se encuentra dentro de los estudios sobre interfaces entre redes y la instalación de usuario como: Asymmetric Digital Subscriber Line Metallic Interfaz, en términos de su interacción y características eléctricas. Este estándar incluye descripción de: Cancelación de eco, códigos utilizados para modulación, sincronización en el transporte, latencia dual, transporte en modo síncronico y asíncronico y modo de entramado con cabecera reducida entre otros.

La segunda versión de este estándar se publicó en el año 1998 con el nombre de ANSI T1E1.4

Actualmente se tiene grupos de trabajo sobre ADSL en las principales organizaciones de estándares en telecomunicaciones; así, se puede nombrar a la Unión Internacional de Telecomunicaciones UT con los grupos de trabajo:

- **G.991.1** Estándar introductorio para enlaces xDSL.
- **G.992.1 o G.dmt** Estándar ADSL de velocidad completa (hasta 8 Mbps).
- **G.992.2 o G.lite** Estándar ADSL de velocidad limitada (hasta 1.5 Mbps).

- **G.994.1 o G.hs** Estándar sobre manejo de señalización para identificar. Capacidad y negociación de los modos de operación para xDSL.
- **G.995.1 o G.ref** Estándar sobre referencias.
- **G.996.1 o G.test** Estándar que define un modelo de red y procedimientos para realizar pruebas en módems xDSL.
- **G.997.1 o G.cam** Estándar que identifica los requerimientos del canal de control para operación y mantenimiento de módems xDSL.

Existen también grupos de estudio para estandarización de ADSL en el ETSI (Instituto Europeo de Estándares de Telecomunicaciones), uno de estos es el ETR 328 Transmisión y Multiplicación – ADSL, Requerimientos y Características.

Además dentro del Consejo de digitalización Audio-Visual-DAVIC existe una especificación denominada DAVIC1.0 especificación 7 que contiene información sobre Redes de acceso utilizando ADSL abordando en la:

Parte 2.- Modelo del sistema de referencia y escenarios,

Parte 4.- Arquitecturas de sistemas de entrega, y

Parte 8.- Protocolos de capa baja e interfaces físicos.

El ATM Forum incluye a la tecnología ADSL como posible alternativa para el interfaz físico entre la red de acceso ATM y los usuarios finales.

Existe además un grupo denominado UAWG Grupo Mundial para un estándar ADSL Universal que también está trabajando en recomendaciones al respecto de esta tecnología.

En la actualidad, el DSL Forum (antes ADSL Forum), es la asociación que agrupa a distintos fabricantes de ADSL y se encarga de la estandarización de esta nueva tecnología. El DSL Forum se formó a finales de 1994, sus actividades son de orden técnico y comercial, y trata de recopilar todos los informes de todos los grupos de estandarización mencionados anteriormente, más los criterios de los

fabricantes y operadores de telecomunicaciones para ofrecer un estándar universal de ADSL.

1.5.3 MODELO DE REFERENCIA PARA EL SISTEMA ADSL [24], [31]

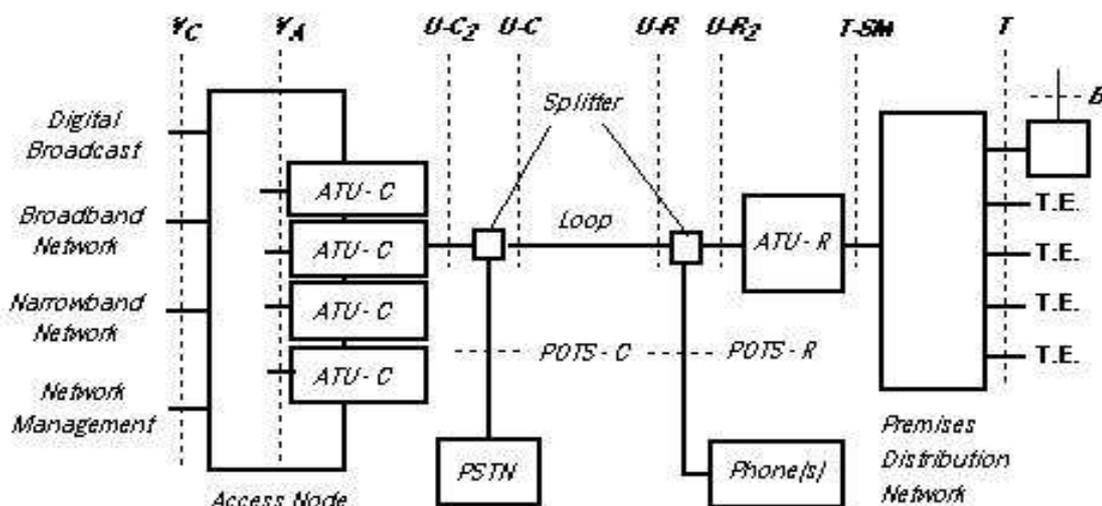


Figura 1.2 Modelo de Referencia del Sistema ADSL publicado por DSL Forum [31]

A continuación la definición de los componentes de la Figura 1.2:

- **ATU-C:** ADSL Transceiver Unit - Central Office. Unidad de Transmisión/Recepción ADSL en la Oficina Central, que puede estar incluida dentro del nodo de acceso.
- **ATU-R:** ADSL Transceiver Unit - Remote. Unidad de Transmisión/Recepción ADSL (módem ADSL) Remoto del cliente o suscriptor, que puede estar incluida dentro del módulo de servicio.
- **Access Node:** Nodo de Acceso. Punto de concentración para datos de banda ancha y banda angosta. Puede colocarse tanto en la oficina central o en un sitio remoto.
- **B:** Entrada auxiliar de datos (por ejemplo, de un satélite) al módulo de servicio (por ejemplo, un Set Top Box).
- **Broadcast:** Entrada de datos de banda ancha en modo simple (típicamente broadcast video).

- **Broadband Network:** Red de Banda Ancha. Sistema de conmutación para tasas de transmisión de datos por encima de 1.5/2.0 Mbps
- **Loop:** Lazo o Bucle: la línea telefónica o par trenzado de cobre. Los lazos pueden variar en distancia, diámetro, antigüedad y características de transmisión dependiendo de la red.
- **Narrowband Network:** Red de Banda Angosta. Sistema de conmutación para tasas de transmisión de datos iguales o por debajo de 1.5/2.0 Mbps
- **POTS:** Servicio Tradicional de Telefonía (Plain Old Telephone Service).
- **POTS-C:** Interfaz entre la PSTN y el filtro POTS en la parte final de la red.
- **POTS-R:** Interfaz entre los teléfonos y el filtro POTS en el lado del cliente.
- **PDN:** Red de Distribución del Cliente (Premises Distribution Network). Sistema para interconectar ATU-R con los módulos de servicio. Puede ser interconexión punto a punto o multipunto; para este último caso, la topología puede ser bus o estrella.
- **PSTN:** Red de Telefonía Pública Conmutada (Public Switched Telephone Network).
- **SM:** Módulo de servicio (Service Module). Realiza funciones de adaptación de terminales. Algunos ejemplos son las interfaces de PC, ruteadores LAN o Set Top Boxes.
- **Splitter:** Filtro que separa las señales de alta frecuencia de ADSL de las señales de baja frecuencia de POTS, localizado tanto en la parte de la oficina central como en la parte del cliente. El filtro puede estar integrado dentro de los ATU o físicamente separado de ellos.
- **T-SM:** Interfaz entre la ATU-R y la PDN. Puede estar integrada dentro de un módulo de servicio. Ejemplos son conexiones T1/E1 y conexión Ethernet.
- **T:** Interfaz entre la PDN y los módulos de servicio. Esta interfaz puede desaparecer a nivel físico cuando un aATU-R está integrada a un módulo de servicio.
- **U-C:** Interfaz entre el lazo y el filtro POTS en el lado de la red.
- **U-C2:** Interfaz entre el filtro POTS y ATU-C.
- **U-R:** Interfaz entre el lazo y el filtro POTS en el lado del cliente
- **U-R₂:** Interfaz entre POTS y ATU-R

- **VA:** Interfaz lógica entre ATU-C y el nodo de acceso. Esta interfaz puede contener STM (Synchronous Transfer Mode), ATM (Asynchronous Transfer Mode), o ambos modos de transferencia.
- **VC:** Interfaz entre el nodo de acceso y la red. Para el segmento de banda ancha de esta interfaz pueden utilizarse conmutación STM, conmutación ATM o conexiones de línea tipo privada.

1.5.4 ARQUITECTURA GENERAL Y FUNCIONAMIENTO DE UNA RED CON ACCESO ADSL. [24]

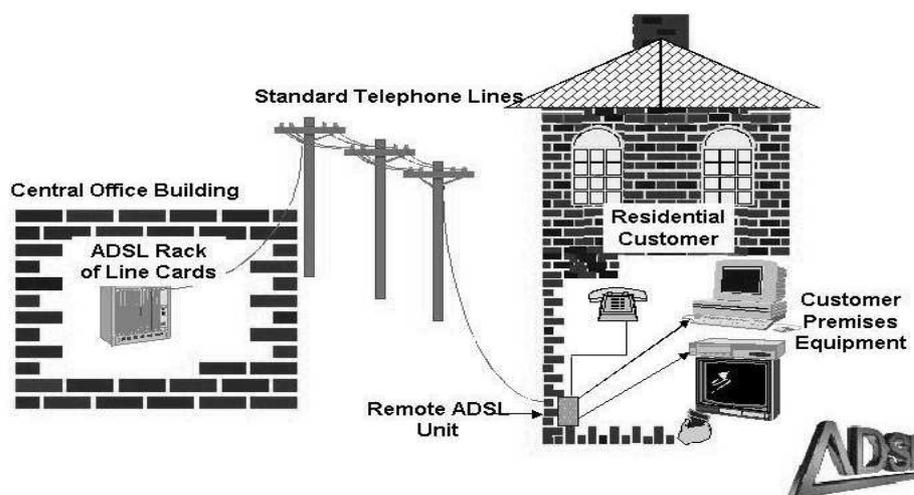


Figura 1.3 Estructura de una red de acceso ADSL [32]

Según muestra la Figura 1.3 se observa que del lado del usuario se debe tener la unidad remota ADSL, que no es más que el conjunto de un filtro (splitter) y un modem ADSL, los cuales por medio de interfaces se conectan a un aparato telefónico convencional, una computadora personal, un decodificador, etc. Esta unidad a su vez debe tener su opuesto en la central local, en la que existirá una tarjeta de línea, la cual contiene filtros y módems. Las señales se transmiten a través de la red de cobre a instalarse para este servicio o la ya instalada para telefonía.

La tecnología ADSL permite utilizar el viejo par de cobre instalado para el servicio de telefonía fija, y así obtener un servicio permanente de transmisión de datos a alta velocidad. Varios años se consideró que la red telefónica era inadecuada para realizar la transmisión de datos a alta velocidad, pero en realidad no es así,

ya que el ancho de banda usado por la red telefónica es de 3.1 KHz. (300 a 3400 Hz); lo cual indica que se tiene todo un rango de frecuencias inutilizado, no por la limitación del cable sino más bien por la tecnología a utilizar. ADSL utiliza el resto de frecuencias disponibles, esto es, de 4KHz a 2.2 Mhz. Una ventaja de la tecnología ADSL es que permite conversar por teléfono y transmitir datos simultáneamente, gracias a los filtros que discriminan la zona de frecuencia alta de la zona de frecuencia baja, a estos se los conoce como splitters.

ADSL utiliza tres canales para la comunicación, un canal de alta velocidad simplex en el sentido red – usuario, un canal dúplex de menor velocidad y un canal ordinario telefónico; estos tres canales se transmiten sobre un único par de cobre. El canal de alta velocidad transmite de 1.5 a 9 Mbps, mientras que en el canal duplex está entre 16 kbps y 640 kbps, dependiendo de la calidad y longitud del cable.

Por el lado de la central el servicio de voz analógico se dirige hacia el conmutador de voz con ayuda de otro filtro. El bucle local ADSL finaliza ahora en un nodo de acceso (un tipo de multiplexor de acceso DSL o DSLAM), este multiplexa varias líneas ADSL. Al otro lado del nodo de acceso se pueden mantener enlaces a enrutadores TCP/IP o conmutadores ATM. Estos conmutadores o enrutadores permiten a los usuarios acceder a los servicios de su elección, entre los cuales se tiene Internet, Proveedores de Contenido (Información, Noticias, Bibliotecas, etc.), video bajo demanda VoD, Redes Corporativas para teletrabajo, etc. Estos servicios pueden ser implementados sobre TCP/IP o sobre ATM, porque ADSL soporta ambos.

Como ADSL desvía el tráfico de datos y de voz hacia redes diferentes, esto reduce la congestión en los conmutadores de voz y las troncales, causadas por los servicios de datos. Después de pasar por el multiplexor los enlaces ADSL se agruparían para llegar a un DACS (Digital Access and Crossconnect System – Acceso Digital a Sistemas de Conexión Cruzada), el cual llevaría los datos por un enlace troncal (un E3 a 34 Mbps) a un ruteador de borde, el mismo que se

conectaría con un ISP o un NAP; la suma total del ancho de banda de todos los enlaces ADSL no debe superar los 34 Mbps.

Otra alternativa es que el nodo de acceso podría conectarse directamente a un enrutador IP o a un switch ATM; el tráfico se acumula en el nodo de acceso para pasar a través de la conexión física y luego siguiendo el mismo procedimiento para llegar al proveedor de servicio. Esto tiene sentido cuando el proveedor ADSL a su vez es Carrier de Datos de Banda Ancha.

Para el caso de este proyecto se opta por la primera opción ya que por la ubicación geográfica es más fácil conectarse a un ISP grande que ya funcione en la Isla.

1.5.5 CODIFICACIÓN DE LÍNEA UTILIZADA EN ADSL [24], [29], [31]

Como se indico anteriormente existen dos técnicas de modulación para ADSL: CAP y DMT. A continuación se detallan estas dos.

1.5.5.1 Modulación DMT

La idea básica de DMT es de separar el ancho de banda disponible de 1.104 MHz en un número grande de subcanales o múltiples portadoras (256 subcanales o tonos), cada uno ocupa 4.3125 KHz de ancho de banda y se utiliza una técnica de modulación en cuadratura conocida como QAM (Quadrature Amplitude Modulation – Modulación de Amplitud en Cuadratura). Con esto cada tono puede transportar hasta 15 bits de información, dependiendo de la relación señal a ruido existente en cada tono.

El primer tono o sub-canal se utiliza para los servicios de telefonía de voz tradicional (POTS), mientras que los tonos entre el rango de frecuencias de 4.3125 KHz a 25.875 KHz (tonos del 2 al 6) se utilizan para evitar la interferencia entre POTS y ADSL. Los tonos del 7 al 32 ubicados entre 25.768 KHz y 138 KHz se utilizan para la transferencia de datos en la dirección de subida (*upstream*), y

tonos del 33 al 256 ubicados entre 138 KHz y 1.104 MHz son utilizados para la transferencia de datos en la dirección de bajada (*downstream*). Estas frecuencias están estandarizadas por la ANSI (*American National Standards Institute*) bajo ANSI T1.413. La Figura 1.4 muestra un esquema de FDM (*Frequency Division Multiplexing*) para el ancho de banda disponible en un cable par trenzado y que hace posible la coexistencia entre POTS (*Plain Old Telephone Service*) o PSTN, ISDN y la tecnología ADSL. La Figura 1.5 muestra la asignación de tonos de frecuencia o sub-canales para la modulación DMT.

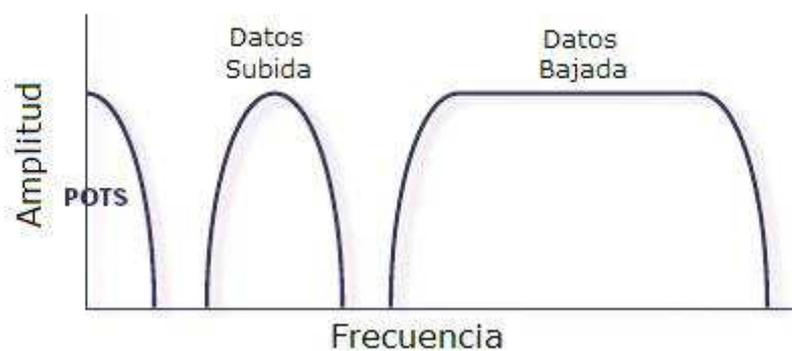


Figura 1.4 FDM para un cable par trenzado [31]

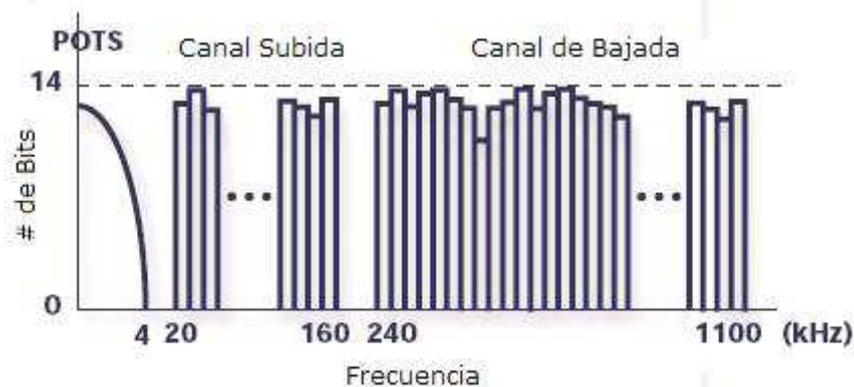


Figura 1.5 Asignación de sub-canales o tonos para modulación DMT [31]

Así mismo, existe otra técnica para asignar las bandas de frecuencias, conocida como cancelación de eco. Esta permite un traslape del canal de bajada con el canal de subida, lo que provoca que los canales sean independientes permitiendo un incremento en la tasa de transmisión de bajada. Aun así esta técnica no es muy utilizada debido a su costo con respecto a la tasa de transmisión de subida,

la cual disminuye considerablemente respecto a la de bajada, y es mucho más compleja de implementar. Es por estas razones que se prefiere usar FDM.

1.5.5.2 Modulación CAP

Como se indicó antes, la modulación CAP fue en un principio la utilizada en la tecnología DSL, con el pasar del tiempo y la mejora en la tecnología esta fue reemplazada por la modulación DMT, la cual es la que se usa en la actualidad. CAP es un código bastante similar a QAM (Modulación de Amplitud en Cuadratura). Una definición simple sería que CAP es QAM sin portadora. Debido a que la portadora no transmite información y usa una gran parte de la potencia transmitida, es común no enviar ninguna portadora y reconstruirla electrónicamente en el destino.

QAM establece constelaciones basándose en dos valores de la señal recibida: la amplitud y la diferencia de fase. Esto es, cualquier punto especificado por una amplitud y una diferencia de fase, representan una secuencia de bits concreta. En este tipo de modulación es común observar diagramas de constelación para visualizar los diferentes estados que va tomando la señal.

CAP usa todo el ancho de banda disponible a excepción de los 4kHz que utiliza la voz analógica para enviar todos los bits, no existen subportadoras ni subcanales como en DMT.

Una vez presentados los conceptos referentes al ISP y de la tecnología ADSL se procederá en el siguiente capítulo a la realización del diseño para el presente proyecto, teniendo en cuenta todo lo expuesto en el presente capítulo.

CAPÍTULO 2

DISEÑO DEL ISP

El objetivo principal de este capítulo es el de realizar el diseño del ISP tomando en cuenta factores como: disponibilidad, eficiencia de la red, calidad de servicio y un esquema de la posible área de cobertura del mismo. Así mismo, se realizará el dimensionamiento de la red, la infraestructura, el análisis para la selección de equipos, y se indicará las posibles soluciones para la parte de seguridad del ISP.

Un factor adicional y clave para el diseño del ISP en Pto. Ayora es el lugar en el cual se ubicarán los equipos y el área de cobertura del mismo. La empresa EQUYSUM tiene arrendado espacio para sus equipos en uno de los nodos de CONECEL en Pto. Ayora, el cual está ubicado en el centro comercial de la población, esto facilitará la adquisición de clientes y empresas que se encuentran alrededor del mismo.

La población de Pto. Ayora recibe constantemente un ingreso proveniente del Turismo, ya que se encuentra en un lugar estratégico de las Islas Galápagos. Entonces, se puede asumir como principales usuarios a las personas que poseen o quieren implementar un café Internet.

Se inicia el diseño con un diagrama de la red tomando en consideración los equipos que se utilizan comúnmente en un ISP basado en la tecnología ADSL.

2.1 ESTRUCTURA BÁSICA DEL ISP

Si bien la función básica de un ISP es prestar el servicio de Internet, en la actualidad esto no es suficiente para atraer clientes. Un ISP debe ofrecer atractivos servicios como: capacidad para almacenar y recobrar correo electrónico, visualizar y hospedar (hosting) páginas Web, transmisión de datos de

forma segura (VPNs), etc. Basado en estos conceptos se puede realizar un diagrama de la arquitectura inicial del ISP, para luego adecuarlo según necesidades concretas y el alcance que tendrá el mismo.

A continuación, la Figura 2.1 muestra un esquema básico del ISP basado en la tecnología que usara y los servicios que prestará.

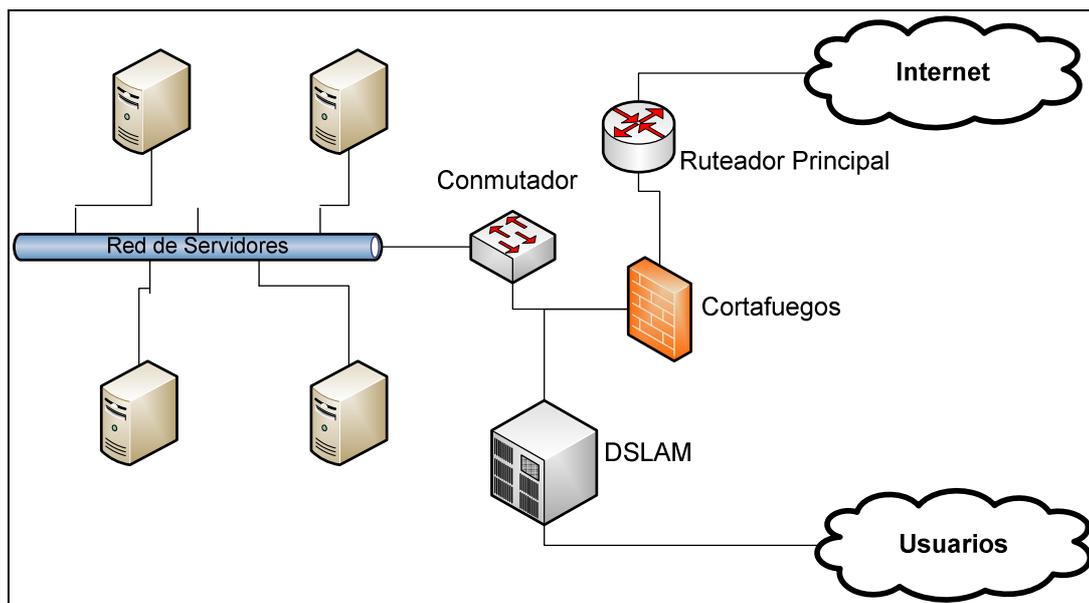


Figura 2.1 Arquitectura básica del ISP

2.2 REQUERIMIENTOS BÁSICOS DEL DISEÑO

Establecer los requerimientos del diseño es fundamental para una correcta planificación de la red, ya que permite equiparar las diferentes opciones y escoger aquellas que satisfagan de mejor manera dichos requerimientos. Antes de ocuparse de la parte de Calidad de Servicio se deben garantizar los siguientes aspectos ya antes mencionados:

- Disponibilidad de red
- Eficiencia en la transmisión de información.

2.2.1 DISPONIBILIDAD DE LA RED [3], [4]

La disponibilidad de la red puede definirse como: “el porcentaje de tiempo que la red funciona con la calidad requerida, respecto al tiempo total”. En la medición de la disponibilidad de la red se debe involucrar a todos los equipos activos de la misma.

El entorno empresarial demanda una disponibilidad de 24x7 (24 horas al día, 7 días a la semana durante todo el año), alto rendimiento y altos niveles de fiabilidad de sus sistemas. Para los usuarios la disponibilidad es muy importante. A través de las redes viaja información empresarial y se ejecutan servicios comerciales fundamentales, lo que implica la necesidad de contar con redes robustas.

Las interrupciones del servicio (planificadas o no), pueden tener grandes repercusiones no solo para el cliente sino para el proveedor, debido a que afectan la productividad de la compañía, las ventas y la calidad del servicio ofrecido. La calidad en el servicio de voz y video, es un factor crítico para lograr una óptima comunicación entre distintas aéreas, clientes y proveedores; en caso de una caída o degradación del sistema, el impacto podría reflejarse en pérdida de negocio, cobranzas o multas.

Se puede aumentar al máximo la disponibilidad de servicio mediante un diseño que funcione con una disponibilidad del 99.99% gracias al respaldo que el nodo de CONECEL provee a los equipos que se instalan en el.

2.2.2 EFICIENCIA DE LA RED [44], [33]

La eficiencia de la red de un ISP está relacionada con su desempeño, tanto desde el punto de vista del proveedor como del cliente, principalmente en aplicaciones críticas como voz y video. Una red eficiente debe garantizar un desempeño óptimo tanto para transmisión de datos como para las aplicaciones de gran demanda de ancho de banda.

Para garantizar una alta disponibilidad de la red y eficiencia en la transmisión de la información, es necesario tomar en cuenta los siguientes requisitos:

- Alta capacidad, escalabilidad.
- Mecanismos de redundancia, prevención, detección y recuperación rápida de la red frente a posibles fallas, y reducción al mínimo del impacto sobre el servicio.
- Simplicidad estructural, facilidades de instalación, gestión, administración, configuración, control y monitoreo.
- Conectividad segura, tanto interna como externa.
- Seguridad e integridad de los datos, para proteger información confidencial.
- Provisión de Calidad de Servicio y Niveles de Servicio contratados al ISP.
- Topologías adecuadas de red
- Costos razonables para el proveedor y accesibles para los clientes.
- Servicio técnico inmediato y especializado.

Para la eficiencia en aplicaciones como voz y video se requiere la utilización de políticas de Calidad de Servicio. En la Tabla 2.1 se presentan los requerimientos de calidad de servicio de las distintas aplicaciones y que servirán de referencia para la fase de diseño.

APLICACIÓN	CONFIABILIDAD	RETARDO	FLUCTUACIÓN	ANCHO DE BANDA
Correo Electrónico	Alta	Bajo	Baja	Bajo
Transferencia de Archivos	Alta	Bajo	Baja	Medio
Acceso a Web	Alta	Medio	Baja	Medio
Inicio de Sesión Remoto	Alta	Medio	Media	Bajo
Audio bajo demanda	Baja	Bajo	Alta	Medio
Video bajo demanda	Baja	Bajo	Alta	Alto
Telefonía	Baja	Alto	Alta	Bajo
Videoconferencia	Baja	Alto	Alta	Alto

Tabla 2.1 Requerimientos de Calidad de Servicio para las distintas aplicaciones [44]

2.3 DETERMINACIÓN DEL ÁREA GEOGRÁFICA [44]

En los últimos tiempos las Islas Galápagos en general han incrementado su turismo y por ende su actividad económica. Entre las principales islas está la de Sta. Cruz la cual es un sitio de gran afluencia turística por su ubicación estratégica con respecto a las demás islas. Su población a aumentado con el pasar de los tiempos hasta alrededor de 11262 habitantes en toda la isla, y en Puerto Ayora es de 9208 habitantes según el INEC [34].

Así mismo, las islas reciben un total aproximado de 80000 turistas al año [35], lo cual da impulso a la realización del presente proyecto, específicamente para la zona central de Puerto Ayora en la Isla de Sta. Cruz, ya que en esta zona se encuentra gran cantidad de empresas y domicilios que constituyen clientes potenciales del ISP.

En la Figura 2.2 se muestra el área geográfica que buscaría cubrir el ISP.



Figura 2.2. Área geográfica del ISP

La zona mencionada es de alrededor de 1 Km. de largo y 1 Km. de ancho. Es importante tomar en cuenta que se trata de una zona urbana, donde se puede encontrar posibles clientes tanto corporativos como residenciales. El hecho de recibir una gran cantidad de turistas ha hecho que la población oriente sus negocios a prestar servicios orientados a los mismos como es el caso de cybers-cafés o café-internets, los cuales posibilitan la comunicación de larga distancia de los turistas con sus familiares y amigos.

Como se muestra en la Figura 2.2 la zona de cobertura tiene una topografía regular, esto ayuda para el tendido de cables, colocación de mangas de empalme y cajas de distribución sin problemas. La empresa EQUYSUM realizó un tendido de cable multipar para uso propio, no específicamente para el uso del ISP, y en la Figura 2.3 se muestra la distribución de dicho tendido.

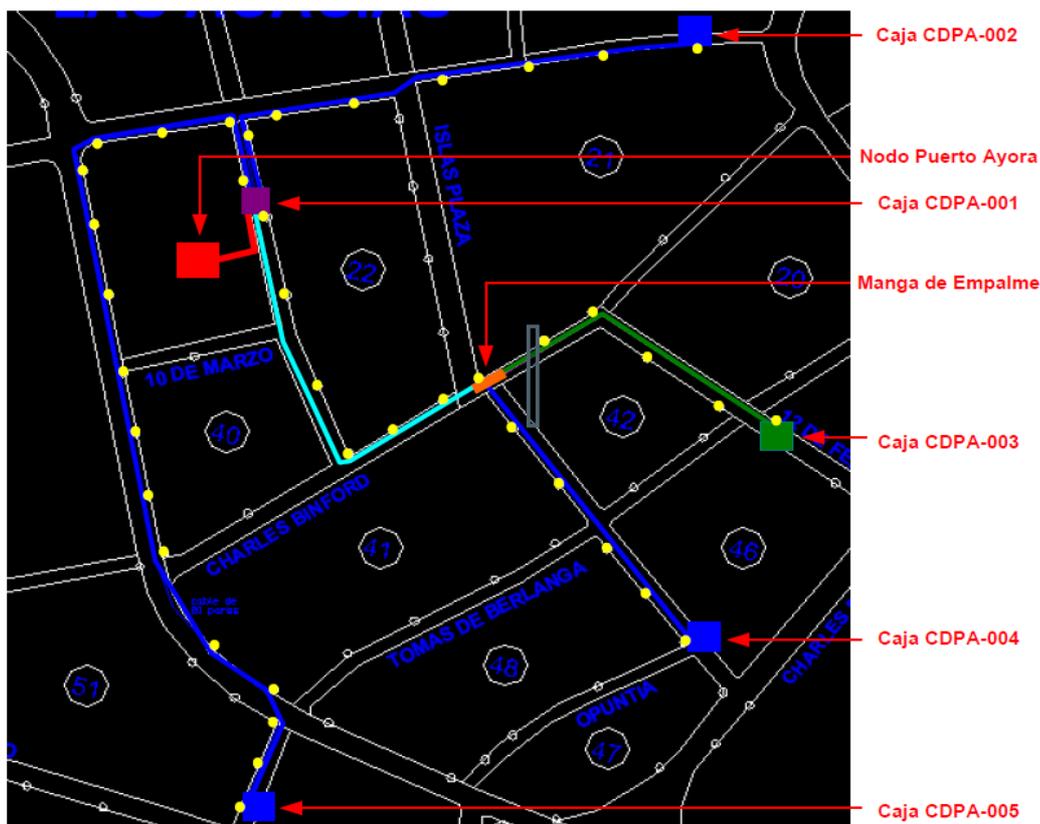


Figura 2.3 Distribución cable multipar.

Si bien esta instalación no estaba orientada al ISP sino para prestar servicios de datos en la isla, se la puede utilizar para el diseño de la red de acceso del ISP de este proyecto.

2.4 DIMENSIONAMIENTO DEL ISP [42], [44] [36], [37]

El dimensionamiento del ISP es un aspecto muy importante respecto a la Calidad de Servicio percibida por los usuarios finales. Es necesario realizar un cálculo del número de posibles clientes del sistema y la capacidad máxima a corto plazo para escoger equipos que soporten dichos requerimientos.

Para obtener una estimación del número de posibles clientes se tomó como referencia los datos publicados en la página web de la Superintendencia de

Telecomunicaciones actualizados a Septiembre del 2008, que se detallan en la Tabla 2.2.

AÑO	CUENTAS CONMUTADAS	CUENTAS DEDICADAS	CUENTAS TOTALES
2002	94164	6499	100663
2003	102787	4563	107350
2004	108169	11599	119768
2005	101934	26786	128720
2006	141814	65463	207277
2007	224999	85946	310945
2008	173681	116913	290594

Tabla 2.2 Número de cuentas de Internet a nivel nacional [³⁸]

A pesar de que en el último año se ha tenido un decrecimiento en las cuentas totales, el número de cuentas de Internet va creciendo cada año. La Tabla 2.3 corresponde a la tasa de crecimiento anual de las cuentas de Internet a nivel nacional. Para obtener una mejor proyección de las posibles cuentas en los próximos años se toma en cuenta la tasa de crecimiento del total de cuentas.

Ejemplo de cálculo:

Año 2002 – 2003

$$\text{Tasa de crecimiento} = \frac{(107350 - 100663) * 100}{100663}$$

Tasa de crecimiento = 6.6

AÑO	CUENTAS CONMUTADAS %	CUENTAS DEDICADAS %	CUENTAS TOTALES %
2002 – 2003	9,16	-29,80	6.6
2003 – 2004	5,24	154,20	11.6
2004 – 2005	-5,76	130,93	7.5
2005 – 2006	39,12	144,40	61
2006 – 2007	58,66	31,29	50
2007 – 2008	-22,80	36,03	-6.5
Tasa de crecimiento anual promedio	13,93	77,84	21.7

Tabla 2.3 Tasa de crecimiento promedio de cuentas de Internet a nivel nacional

2.4.1 PROYECCIÓN DE LA DEMANDA [42], [44]

Mediante datos obtenidos de la Página Web de la Superintendencia de Telecomunicaciones a Marzo del 2009, se logró estimar el número de cuentas de Internet en la isla de Sta. Cruz. Según los datos presentados del INEC la población de Pto. Ayora ocupa aproximadamente el 80% de la población de la isla, es por esto que se toma dicho porcentaje para los cálculos. La Tabla 2.4 indica la cantidad de cuentas en Galápagos y la isla de Sta. Cruz concretamente en la población de Pto. Ayora.

LUGAR	CUENTAS CONMUTADAS	CUENTAS DEDICADAS	CUENTAS TOTALES
GALÁPAGOS	300	457	757
ISLA STA. CRUZ	91	148	239
PTO. AYORA	73	118	191

Tabla 2.4 Número aproximado de cuentas de Internet en Pto. Ayora.

Para la proyección de la demanda en la población de Pto. Ayora se utilizó los datos de la Tabla 2.4 y una tasa de crecimiento exponencial, cuya fórmula es la siguiente: [44]

$$P_T = P_o * (1 + C)^T$$

Ecuación 2.1

P_T = Número de usuarios potenciales dentro de T años.

P_o = Número de usuarios potenciales del servicio.

T = Número de años.

C = Tasa de crecimiento acumulativa anual promedio

En la Tabla 2.3 se indica que la tasa de crecimiento promedio de cuentas dedicadas es de 77,8% y de cuentas conmutadas es de 13,9%. Se utilizarán estos valores para el cálculo de la demanda a cuatro años, por tratarse de un proyecto a corto plazo. La Tabla 2.5 indica los valores obtenidos para la demanda de cuentas de Internet.

AÑO	DEMANDA Cuentas CONMUTADAS	DEMANDA Cuentas DEDICADAS	DEMANDA Cuentas TOTALES
Primero	83	210	293
Segundo	95	373	468
Tercero	108	664	772
Cuarto	123	1180	1303

Tabla 2.5 Demanda aproximada de cuentas de Internet en Pto. Ayora

Como en la población de Pto. Ayora existen algunos ISP, se puede decir que se ha cubierto gran parte de la demanda actual, por lo que la diferencia entre la proyección del primer año y los datos actualizados a Septiembre del 2008 según la Superintendencia de Telecomunicaciones, dará un valor aproximado de los potenciales clientes. En la Tabla 2.6 se presenta el número de posibles nuevas cuentas de Internet en cuatro años.

AÑO	DEMANDA CUENTAS CONMUTADAS	DEMANDA CUENTAS DEDICADAS	DEMANDA CUENTAS TOTALES	POSIBLES CUENTAS CONMUTADAS	POSIBLES CUENTAS DEDICADAS	POSIBLES CUENTAS TOTALES
Primero	83	210	293	8	62	54
Segundo	95	373	468	4	225	229
Tercero	108	664	772	17	516	533
Cuarto	123	1180	1303	32	1180	1212

Tabla 2.6 Posibles nuevas cuentas de Internet en Pto. Ayora

En la Tabla 2.7 se detalla el porcentaje de demanda de cuentas fijado como objetivo del ISP por año, que obviamente es menor al de los ISP que ya poseen un sector de mercado.

AÑO	%	CLIENTES CONMUTADOS	CLIENTES DEDICADOS	CLIENTES TOTALES
Primero	0.45	4	28	24
Segundo	0.55	2	124	126
Tercero	0.65	11	335	346
Cuarto	0.75	24	885	909

Tabla 2.7 Proyección de Clientes dentro de cuatro años para el presente diseño

El enfoque más importante del presente diseño son los Clientes Dedicados, ya que a través de este tipo de enlaces se puede explotar el servicio de valor agregado de VoIP, y adicionalmente contar con el servicio de Cuentas Conmutadas. Esto hará que el ISP pueda compensar el número de usuarios por posibles disminuciones de Clientes Dedicados, y ser un puente que ligue a los clientes en posibles nuevos demandantes de Cuentas Dedicadas.

Una vez determinado el número de cuentas y usuarios potenciales del servicio, es necesario realizar una estimación del tráfico que cursará por la red ya que el dimensionamiento de la red es indispensable para ofrecer un servicio de calidad, tanto en las aplicaciones del servicio de Internet como en el de VoIP.

Para el cálculo del ancho de banda necesario se tomó como mínimo un ancho de banda de 128/64 Kbps para usuarios dedicados, ya que para utilizar la aplicación de VoIP o la transmisión de video se requiere por lo menos dicha capacidad.

Mediante datos recomendados por un ISP de Quito en la Tabla 2.8, en porcentajes de la demanda actual, se determinó una estimación del número de cuentas por la capacidad de su enlace.

PORCENTAJE DE CUENTAS DEDICADAS SEGÚN LA CAPACIDAD CONTRATADA		
%	VELOCIDAD DE BAJADA DL [Kbps]	VELOCIDAD DE SUBIDA UL [Kbps]
75	128	64
20	256	128
5	512	256

Tabla 2.8 Porcentaje de cuentas dedicadas según la capacidad contratada

Una vez determinado el número de cuentas y usuarios potenciales que debe cubrir el ISP del presente diseño, es necesario determinar el ancho de banda mínimo con el que debe contar el ISP para soportar el tráfico producido por los clientes, proporcionar un servicio de calidad, y así garantizar que la aplicación de VoIP se entregue en las mejores condiciones, que es el objetivo del presente diseño, y así lograr que un mayor número de clientes adquieran el valor agregado. La Tabla 2.8 indica que la mayor concentración de usuarios se encuentra en enlaces de 128kbps; y considerando una simultaneidad del 20%, se tienen los valores mínimos de ancho de banda requeridos en la Tabla 2.9 y 2.10

ANCHO DE BANDA PARA CUENTAS CONMUTADAS				
AÑO	Número de clientes	Velocidad de bajada [Kbps]	Velocidad de subida [Kbps]	Ancho de banda total
Primero	4	90	45	135
Segundo	2	53	26	79
Tercero	11	282	141	423
Cuarto	24	615	307	922

Tabla 2.9 Ancho de Banda requerido por cuentas conmutadas

ANCHO DE BANDA PARA CUENTAS DEDICADAS				
AÑO	Número de clientes	Velocidad de bajada [Kbps]	Velocidad de subida [Kbps]	Ancho de banda total
Primero	28	713	356	1069
Segundo	124	3171	1585	4756
Tercero	335	8582	4291	12872
Cuarto	885	22663	11332	33995

Tabla 2.10 Ancho de Banda requerido por cuentas dedicadas

La Tabla 2.11 presenta el total de cuentas conmutadas y dedicadas con el respectivo ancho de banda por año.

ANCHO DE BANDA TOTAL						
AÑO	Número de clientes conmutados	Número de clientes dedicados	Ancho de banda conmutado	Ancho de banda dedicado	Total de clientes	Ancho de banda total
Primero	4	28	135	1069	32	1204
Segundo	2	124	79	4756	126	4836
Tercero	11	335	423	12872	346	13296
Cuarto	24	885	922	33995	909	34917

Tabla 2.11 Ancho de Banda total

2.5 INFRAESTRUCTURA DEL ISP [39]

Entre las características más importantes que debe cumplir un ISP está la simplicidad en su estructura, que permita a los clientes una fácil interconexión sin pasar por demasiados puntos, y permita que el proveedor pueda adaptarse con facilidad a cambios tecnológicos y estructurales. Para el diseño se divide la arquitectura del ISP en las siguientes partes:

- Red Troncal.
- Red del ISP.
- Red de Distribución.
- Red de acceso.

2.5.1 RED TRONCAL

Para brindar el servicio de Internet es necesario que un ISP se conecte al Internet, por medio de uno o varios enlaces WAN. Existen algunas tecnologías utilizadas para cumplir este objetivo, tales como una conexión satelital, conexión mediante fibra óptica o enlaces WAN de alta velocidad, como por ejemplo ATM. Esta conexión se la realiza mediante el ruteador principal que debe soportar la tecnología a utilizarse.

Además de la conexión externa es necesario considerar una conexión al Punto de Acceso de Red Ecuador (NAP.EC, Network Access Point of Ecuador). Se entiende por NAP.EC, una infraestructura que soporta el tráfico que se genera y se dirige a Ecuador. Entre sus datos principales se tiene que la administración de este nodo está en manos de la AEPROVI (Asociación de Empresas Proveedoras de Servicios de Internet, Valor Agregado, Portadores y Tecnologías de la Información). Este tipo de conexiones se conoce con el nombre de “peering” cuyo objetivo es el de disminuir tráfico hacia el exterior. Los ISPs más importantes del país cuentan con una conexión al NAP.EC.

Mediante datos de la página del CONATEL se puede observar que el tráfico que soporta el NAP.EC que cuenta con uno en Quito y uno en Guayaquil es muy alto, además del costo extremo que representa, por lo que para el presente diseño se considera que la mejor opción para el acceso al Internet (tránsito al backbone de Internet) sea en un principio a través de un enlace WAN de alta velocidad, ofrecido por empresas como Telconet, y que además tiene cobertura en Galápagos. Telconet cuenta con las siguientes características: [40]

- Canales de acceso directo hasta el NAP de las Américas
- Latencia: 112 ms. hacia portales como Yahoo o Google
- Confiabilidad: BER 10E-12
- Concentración 1:1 garantizada
- Respaldo satelital automático.
- SLA (Service Level Agreement):
 - Disponibilidad del 99.8%
 - Pérdida de paquetes prácticamente nula
 - Latencias al backbone de USA de 120 ms. (promedio)
 - Tiempo Promedio para Reparar (MTTR, Mean Time To Repair) de dos horas

Telconet se conecta al NAP.EC y al NAP internacional en Miami, posee redundancia de plataforma y de interconexión internacional, lo que asegura un desempeño óptimo con altos estándares internacionales. [40]

2.5.2 DISEÑO DE LA RED DEL ISP

Para el diseño de la red del ISP es conveniente utilizar el modelo jerárquico de redes que consta de las capas de núcleo, distribución y acceso.

2.5.2.1 Capa núcleo [41]

La capa núcleo debe ofrecer la conexión más rápida posible entre los puntos de distribución. Para este diseño la capa núcleo está conformado por el ruteador principal que provee la conectividad entre el exterior y la red interna del ISP.

Para el caso de este proyecto dicho ruteador no necesita implementar protocolos de enrutamiento complejos como sería el caso de BGP, ya que el ruteador solo recibirá las IPS públicas y realizara el NAT (*Network Address Translation - Traducción de Dirección de Red*) correspondiente. Así mismo no se necesita de protocolos de enrutamiento internos como son: RIPv2, OSPF, IGRP, EIGRP, ya que se utilizarán rutas estáticas para encaminar los datos a su destino. Estas decisiones conllevan a los siguientes aspectos:

- No se aumenta la carga en la CPU del ruteador.
- No consume ancho de banda en los enlaces entre ruteadores.
- Se requiere de un conocimiento pleno de la red por parte de los administradores.
- Si surgen nuevas rutas, deben ser agregadas por parte del administrador.
- Las rutas estáticas son más seguras

En primera instancia se puede pensar que este tipo de red es de gran tamaño pero para este caso específico se trata de una red no muy compleja debido al poco tamaño físico que tendría la red entre otras cosas.

2.5.2.2 Capa de distribución [39], [41]

La capa de distribución ofrece conectividad basada en VLANs. Para el presente diseño, es necesario que un conmutador maneje VLANS básicamente y provea de conectividad a los equipos. La función de este conmutador es muy importante ya que aquí se realiza la separación en las diferentes LAN virtuales, que

conforman la red del ISP. Se puede dividir a la red interna del ISP en las siguientes VLANs:

- VLAN de servidores de administración
- VLAN de servidores de aplicación
- VLAN de dispositivos de conectividad externa
- VLAN de dispositivos de acceso

2.5.2.2.1 VLAN de servidores de administración

En esta VLAN se encuentran los puertos conectados al servidor de administración y monitoreo.

2.5.2.2.2 VLAN de servidores de aplicación

Un ISP debe poseer una serie de servidores de aplicación para proveer de diferentes servicios a sus usuarios. Los servidores que conforman la red son: Correo electrónico, FTP, DNS1, DNS2, y Alojamiento Web. En esta VLAN se encuentran los puertos conectados a cada uno de los servidores mencionados anteriormente.

2.5.2.2.3 VLAN de dispositivos de acceso

En esta VLAN se encuentra el puerto conectado hacia el DSLAM de acceso corporativo o residencial.

2.5.2.2.4 VLAN de dispositivos de conectividad externa

En esta VLAN se encuentra el puerto conectado al cortafuegos, que a su vez se conecta al ruteador principal, y el puerto conectado al servidor cache. El servidor cache se coloca en este segmento debido a que la www (World Wide Web) es

uno de los servicios más solicitados por parte de los usuarios, y en esta ubicación se obtiene un ahorro significativo de ancho de banda. [10]

2.5.2.3 Capa de acceso

En la capa de acceso de la LAN se encuentran los dispositivos que integran las cuatro VLANs del diseño. La capa de acceso consiste en el punto de entrada de los usuarios finales del ISP. En el presente diseño está conformada por el DSLAM de acceso corporativo y residencial, cuyas interfaces se conectan a los módems de los usuarios. En esta capa se encuentra también la granja de servidores del ISP, dentro de su respectiva VLAN. El DSLAM de acceso corporativo y residencial puede o no soportar QoS, ya que se lo puede realizar a nivel del ruteador principal.

2.5.3 RED DE DISTRIBUCIÓN

La red de distribución se encarga de agregar las conexiones de los clientes en los PoPs del ISP. Para la concentración de tráfico se utiliza la tecnología ADSL, mediante enlaces punto-punto que agregan el tráfico de los módems ADSL. Los módems van conectados al DSLAM y este a los conmutadores. El DSLAM debe disponer de funcionalidades de enrutamiento, políticas de control de tráfico y Calidad de Servicio, para así disminuir el procesamiento en el ruteador principal.

2.5.4 RED DE ACCESO AL CLIENTE

La última milla para este proyecto se la realiza por medio de líneas de par trenzado los cuales parten de cajas de distribución (CD) ubicadas estratégicamente para abarcar una mayor extensión del área de estudio. Por medio de un estudio realizado por la empresa EQUYSUM se obtiene la distribución de las cajas antes mencionadas, las mismas que estaban orientadas para prestar otros servicios.

La red consta además de cable multipar y de mangas de empalme las cuales interconectan las cajas hacia el nodo principal de distribución de la red de acceso al cliente.

2.6 INTEGRIDAD DEL SISTEMA [42]

Todo ISP debe velar por dos objetivos básicos, conservar la conectividad entre la Internet y sus clientes, y mantener alta disponibilidad en la prestación de los servicios. Adicionalmente debe velar por la integridad de los datos de los usuarios, lo cual se consigue mediante servicios que estén protegidos contra rompimientos de seguridad y fallas de software usando un Firewall que proteja al ISP de la intrusión desde el Internet y usuarios propios del ISP.

2.6.1 ADMINISTRACIÓN DE USUARIOS Y DEL SISTEMA [42]

Un ISP debe tener estrategias muy bien pensadas para administrar sus redes y sus usuarios, y debe tener en cuenta el crecimiento que este tendrá al ofrecer un servicio de alto nivel a los mismos.

Es por esta razón que un ISP suele estructurarse en dos zonas importantes, una dedicada a los servicios, y la otra dedicada a la administración. La zona de los servicios es la más frágil, desde el punto de vista de seguridad, ya que está expuesta a todos los usuarios de Internet. Por otro lado, la zona de administración debe ser la más protegida, y evitar ataques de cualquier tipo.

2.6.2 POLÍTICAS DE SEGURIDAD [43], [44]

El objetivo principal de un ISP es prestar el servicio de Internet a todos sus usuarios, esto hace que el ISP pueda estar en constantes ataques desde el Internet y desde sus usuarios; por lo tanto, se deben tener todos los equipos del ISP protegidos, pero de tal manera tal que sea transparente para los usuarios. Los principales objetivos de seguridad para un ISP serían entonces:

- Protegerse a sí mismos de: amenazas internas, amenazas desde sus usuarios (clientes), y amenazas desde los usuarios de Internet.
- Ayudar a que sus usuarios se protejan de las amenazas de Internet.
- Disminuir los riesgos y amenazas hacia Internet que se pueden presentar por el acceso de los clientes del ISP.

Para proporcionar seguridad a un ISP se debe tomar en cuenta el aspecto físico y lógico de protección de sus equipos y servicios. La seguridad se la puede tomar en cinco fases que son:

1. *Preparación*. La cual incluye todo el trabajo que se requiere para preparar el sistema, probar herramientas, establecer procedimientos y capacitar al personal técnico.
2. *Clasificación*. En el caso de que ocurra un evento que se presume riesgoso para la seguridad, se deberá identificar el tipo de ataque y el daño que puede causar.
3. *Registro hacia atrás (Traceback)*. Significa buscar el origen del ataque con las herramientas identificadas en la fase 1.
4. *Reacción*. Que implica tomar medidas para contrarrestar el ataque.
5. *Post Mortem*. Se refiere a las acciones que se realizarán después del ataque.

De las fases mencionadas se hará un enfoque inicial en la fase 1, la cual es primordial para el diseño de la seguridad del ISP. Ciertos aspectos de la calidad de servicio también entran en la parte de seguridad, y se debe buscar equipos adecuados para la prestación de este servicio.

2.7 CALIDAD DE SERVICIO PARA UN ISP [42]

Se puede definir la calidad de servicio (QoS) como “la capacidad que tiene un sistema de asegurar, con un grado de fiabilidad preestablecido, que se cumplan los requisitos de tráfico, en términos de perfil y ancho de banda, para un flujo de información dado.”^[45]

Para un ISP el significado de calidad de servicio (QoS) se relaciona con el dimensionamiento de recursos de manera óptima en función del número de usuarios y de la disponibilidad de los servicios entregados por el ISP.

La calidad de servicio (QoS) es un concepto relativo; esto es, depende desde la perspectiva que se lo mire. En el caso del ISP se debe considerar desde el punto de vista de los usuarios, los proveedores (carriers) y el administrador de la red. Para los usuarios la calidad de servicio se reflejaría como rapidez, fiabilidad, rendimiento y disponibilidad.

2.7.1 PARÁMETROS DE CALIDAD DE SERVICIO

La calidad de servicio se la puede medir de dos formas, la una cualitativa y la otra cuantitativa. La primera está relacionada con la percepción que experimenta el usuario al acceder a la red. Cuantitativamente hay varios factores para medir la calidad de servicio, y así poder ajustarla para prestar un servicio de calidad.

Estos factores son:

- a) **Retardo.-** Para aplicaciones que usan TCP, cuanto mayor sea el retardo, mayor es el esfuerzo del protocolo por funcionar eficazmente. Mientras que para aplicaciones que utilizan UDP (como voz y video), el aumento del retardo hace que la red sea incapaz de funcionar adecuadamente.
- b) **Jitter.-** Es una variación del retardo existente en el tráfico entre extremos, y es causado principalmente por congestión en la red. En aplicaciones que usan TCP provoca ineficiencia para restablecer un flujo de datos determinado luego de superar umbrales prefijados (timeouts). Mientras que en aplicaciones

que usan UDP, se entregan señales distorsionadas que dificultan mantener sesiones de telefonía IP o teleconferencias.

- c) **Ancho de banda.**- La máxima velocidad de transferencia de datos entre dos extremos de la red, en donde el límite está dado por la capacidad de su infraestructura física y el patrón de los flujos de datos que se originan en los nodos al ir entre origen y destino, compartiendo enlaces en una determinada ruta.
- d) **Fiabilidad.**- Es una propiedad del sistema que se caracteriza por el tiempo de funcionamiento sin fallas. La falta de fiabilidad produce una red de baja calidad. En una red se puede cuantificar la fiabilidad determinando la tasa media de errores. Para aplicaciones basadas en TCP se corrigen los errores de fiabilidad mediante retransmisiones, mientras que para aplicaciones que usan UDP, la falta de fiabilidad provoca distorsión en la información recibida ya que no hay retransmisiones.

2.7.2 PROCEDIMIENTOS DE CALIDAD DE SERVICIO

Las herramientas de QoS son variadas y actúan sobre diferentes niveles (enlace, red, transporte, etc.) dependiendo de los problemas específicos que se quieran resolver, así se tiene:

- a) Colas Basadas en Clases (CBQ).
- b) Colas Equitativas Ponderadas.
- c) Tasa de acceso Entregada

2.7.2.1 Colas basadas en clases (CBQ)

Este mecanismo consiste en clasificar el tráfico en clases, y dependiendo de la clase se asigna una cola de salida. El algoritmo CBQ determina el conjunto de colas a utilizar, la clase de tráfico que se almacena, y la cantidad de tráfico que se pone en cada cola en cada turno de servicio.

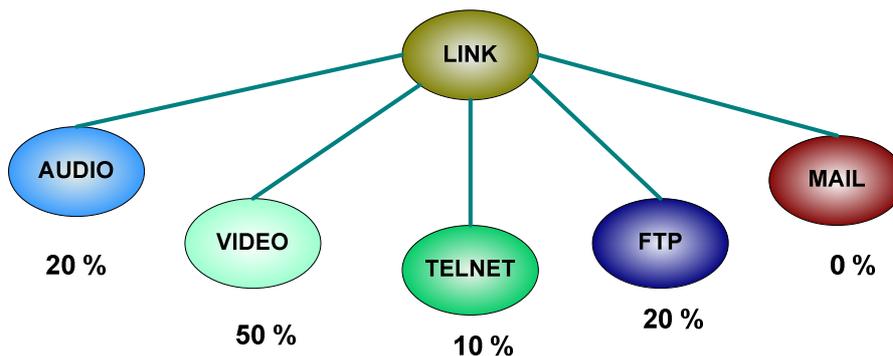


Figura 2.4 Compartición de enlace CBQ

Tal como se indica en la Figura 2.4, a cada clase de tráfico se le asigna un porcentaje de ancho de banda que va a utilizar en forma estática y dinámica.

El algoritmo cuenta con los siguientes mecanismos:

- a) **Clasificador.-** Asigna paquetes entrantes a las clases.
- b) **Estimador.-** Estima el ancho de banda que necesita cada clase.
- c) **Planificador de compartición de enlace.-** Marca paquetes para definir como se ha de compartir el enlace.
- d) **Planificador general.-** Decide entre utilizar FCFS (first-come, first-served) por prioridad y Round Robin (forma cíclica) entre los paquetes del mismo nivel de prioridad.

2.7.2.2 Colas equitativas ponderadas (WFQ)

Procedimiento que garantiza un cierto ancho de banda basado en un reparto equitativo de ancho de banda, donde el tráfico de poco volumen es tratado como prioritario para reducir el tiempo en el que se encuentra en la red, mientras que al tráfico de gran volumen se reparte ancho de banda proporcionalmente. En definitiva, WFQ determina un mecanismo en el que el flujo de tráfico mayor no tiene que interrumpir el flujo de tráfico menor.

2.7.2.3 Tasa de acceso entregado

Se refiere a mecanismos que garantizan ancho de banda, pudiendo ser:

- a) **Clasificación de paquetes.-** Distribuye el tráfico en niveles de prioridad o clase de servicio (CoS), y utiliza políticas de acceso, dirección IP origen y destino, etc. Clasifica los paquetes en función de su importancia, definida en los bits de procedencia IP del campo TIPO de SERVICIO en la cabecera IP.

- b) **Limitación de la tasa de transmisión.-** Limita la velocidad máxima de transferencia de tráfico. Se basa en políticas que toman ciertas acciones según el tráfico conforme exceda o no la tasa límite preestablecida, pudiendo dejarlo pasar mientras se descarta el resto de paquetes o, a su vez, ser transmitidos con prioridad más baja, y en el peor de los casos descartarlo por completo.

Para realizar este tipo de clasificación se establecen tres parámetros importantes:

- 1) **Equiparación de tráfico.** Identificación del tráfico bajo criterios tales como: Tráfico IP, Precedencia IP, Grupos de QoS, Dirección MAC.

- 2) **Medición de tráfico.** Es decir, determinar si el tráfico excede o no la tasa de transmisión establecida, dependiendo de los límites establecidos con anterioridad.

- 3) **Políticas de acción.** Tal como sugiere se toman acciones que se ejecutan sobre el tráfico.

- 4) **Acciones a ejecutar.** Las acciones que se toman son:
 - 4.1) Transmitir el paquete.
 - 4.2) Fijar precedencia y transmitir

- 4.3) Descartar el paquete.
- 4.4) Fijar Precedencia y Continuar.
- 4.5) Fijar el nivel de QoS y transmitir
- 4.6) Fijar el nivel de QoS y Continuar

2.7.2.4 Descarte aleatorio anticipado

Se basa en el control del tamaño de la cola, indicando a los sistemas finales cuando deben dejar de enviar paquetes. Se establece un límite normal y un límite excedido.

Con el primero, cuando el tráfico excede el límite normal, la red descarta aleatoriamente paquetes adaptando la tasa a la que la red pueda soportar. Si no se supera la congestión mediante este mecanismo y el tráfico alcanza el límite excedido se produce un descarte indiscriminado de paquetes

2.8 ARQUITECTURAS EXISTENTES de QoS [42], [44]

Se analizarán dos arquitecturas de QoS:

- a) Arquitectura de Servicios Integrados (IntServ)
- b) Arquitectura de Servicios Diferenciados (Diffserv)

2.9 ARQUITECTURA DE SERVICIOS INTEGRADOS (INTSERV)

La arquitectura de servicios integrados (IntServ) se enfoca en asignar un ancho de banda y recursos específicos a flujos individuales de paquetes de extremo a extremo (los flujos son identificados por las direcciones de origen y destino). Esto significa que cada flujo puede pedir a la red niveles específicos de servicios y se aceptará o negará tal petición basándose en disponibilidad de recursos y garantías provistas a otros flujos, antes que las aplicaciones empiecen a operar. Los posibles niveles de calidad de servicio que las aplicaciones pueden solicitar necesitan de:

- a) Definiciones de niveles de calidad de servicio y los parámetros que las especifican.
- b) Un protocolo de reserva de recursos implementado en los nodos extremos y en los elementos intermedios de la red.

En la arquitectura IntServ se definen tres tipos o niveles de calidad de servicio:

- a) **Servicio Garantizado.**- Garantiza un caudal mínimo y un retardo máximo; es decir, asegura a las aplicaciones un tiempo máximo garantizado de transmisión de extremo a extremo, mientras el tráfico se mantenga dentro de las especificaciones acordadas y dependiendo de las características del medio físico. Cada ruteador del trayecto debe ofrecer las garantías solicitadas. Las claves del servicio son:
 - 1. Garantizar la calidad del servicio en términos de capacidad o tasa de datos.
 - 2. Establecer un retardo de cola máximo, que se añade al retardo de propagación.
 - 3. Asegurar que no haya pérdidas en las colas.
- b) **Servicio de carga controlada.**- Ofrece una calidad que se compare a la de una red de datagramas con poca carga (mejor esfuerzo). Utiliza control de admisión para seguir proporcionando el servicio, incluso en caso de congestión. Las claves de este servicio son:
 - 1. Asemejarse al servicio de mejor esfuerzo en condiciones de bajo nivel de carga.
 - 2. No establecer un límite máximo específico en el retardo de cola.
 - 3. Garantizar que la mayoría de los paquetes se entreguen con éxito.

c) **Servicio de mejor esfuerzo.**- Se trata de un servicio sin garantía. Sus claves son:

1. No existe negación al ingreso para cualquier tipo de tráfico en la red
2. Todo el tráfico es tratado de la misma manera.
3. Todo tráfico será transmitido de la mejor manera posible dándole los recursos disponibles.

2.9.1 COMPONENTES DE LA ARQUITECTURA DE SERVICIOS INTEGRADOS.

Los componentes de ésta arquitectura son los siguientes:

1. Control de admisión.
2. Clasificador de paquetes.
3. Planificador de paquetes.
4. Protocolo de reserva.

2.9.1.1 Control de admisión

Para ofrecer recursos garantizados para los flujos reservados, una red debe monitorear el uso de sus recursos. De este monitoreo debe decidir negar solicitudes de reserva cuando no hay suficientes recursos disponibles en la red, esa es la tarea principal del agente de control de admisión.

Antes que una solicitud de reserva pueda ser aceptada, esta debe pasar una prueba de control de admisión.

2.9.1.1.1 Funciones básicas:

Se manejan las siguientes funciones básicas

1. Determinar si una reserva puede ser establecida basándose en políticas de control de admisión.

2. La segunda función es monitorear y medir los recursos disponibles en la red.

2.9.1.1.2 Aproximaciones para el control de admisión:

Se tienen las siguientes aproximaciones:

1. Aproximación basada en parámetros.- Usa un conjunto de parámetros para caracterizar los flujos de tráfico en forma precisa. Se calcula los recursos requeridos en base a estos parámetros.
2. Aproximación basada en medidas.- No se mantiene una caracterización del tráfico. La red mide la carga de tráfico real y usa esto para el control de admisión. Es de naturaleza probabilística y no puede ser usada para proveer garantías fijas en acuerdos de recursos.

Cuando hay un gran número de flujos, se puede mejorar la utilización de la red mediante multiplexación estadística. Se han propuesto diferentes métodos para decidir si un flujo puede ser admitido o no en la red. Algunos algoritmos propuestos son:

1. **Suma simple.**- Es la aproximación más simple, además de conservadora. Asegura que los anchos de banda solicitados para todos los flujos no excedan la capacidad del enlace.
2. **Suma medida.**- Se usa la carga medida de los flujos existentes en vez del ancho de banda solicitado por ellos. Toma en cuenta que la carga de tráfico real es más baja que la suma de todos los anchos de banda requeridos.
3. **Región de aceptación.**- Este algoritmo maximiza los incrementos en la utilización versus las pérdidas de los paquetes. La región de aceptación para

un tipo de tráfico puede ser calculada dados los modelos estadísticas de las fuentes de tráfico.

4. **Ancho de banda equivalente.**- Es otra aproximación basada en un modelo estadístico. El ancho de banda equivalente para un conjunto de flujos se define como el ancho de banda tal que los requerimientos estacionarios de ancho de banda del conjunto de flujos, excede este valor con una probabilidad de por lo menos p .

2.9.1.2 Clasificador de paquetes.

Es un componente del control de tráfico que clasifica en clases de servicio los paquetes entrantes. Los principales responsables de realizar este control son los ruteadores de la red. A continuación se detallan los pasos que se siguen:

2.9.1.2.1 Procesamiento de los paquetes en los ruteadores:

Deben examinar cada paquete entrante y decidir si cada uno de los paquetes pertenece a uno de los flujos RSVP reservados. La identificación de cada flujo IP se lo hace mediante 5 campos de la cabecera del paquete.

- a) Dirección Fuente.
- b) Dirección destino.
- c) Identificación del protocolo.
- d) Puerto fuente.
- e) Puerto destino

Para identificar si cada paquete corresponde a un flujo RSVP específico, el motor de identificación debe comparar los 5 campos de la cabecera del paquete entrante con los 5 campos de todos los flujos en la tabla de reserva. Si hay coincidencia el paquete es enviado al identificador de paquetes junto con el estado de reserva asociado al flujo.

2.9.1.3 Planificador de paquetes.

Este componente dirige el envío de diferentes paquetes utilizando un conjunto de colas. Es el último paso en la reserva de recursos de la arquitectura de servicios integrados como se observa en la Figura 2.5.

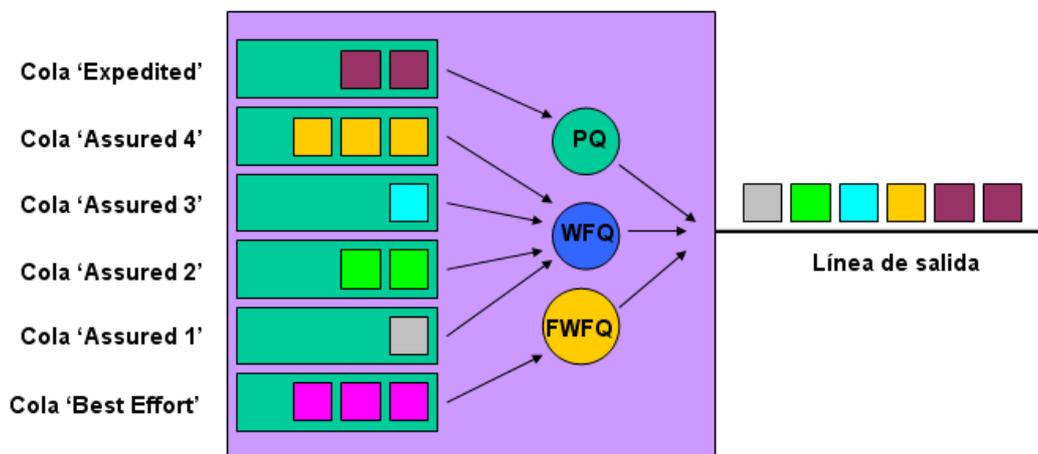


Figura 2.5 Planificador de paquetes

Es el proceso responsable de la asignación de los recursos, y afecta en forma directa a los retardos que experimentan los paquetes e indirectamente a cualquier paquete que se pierde cuando el buffer se llena. Utiliza el algoritmo WFQ (colas equitativas ponderadas).

2.9.1.4 Protocolo de reserva.

RSVP (Protocolo de Reserva de Recursos) es un protocolo de señalización que hace reservas de recursos para aplicaciones, y así garantizar QoS entre nodos extremos y los encaminadores de la ruta seguida por cada flujo. Es considerado un protocolo de señalización porque las reservas de recursos son negociadas por comunicación entre las estaciones finales, además de ser considerado como un protocolo de señalización fuera de banda, ya que los paquetes RSVP se envían en paralelo con otros paquetes y no van junto al flujo de datos transmitidos.

RSVP es un protocolo de control para Internet que reside en la capa 4 del modelo OSI (capa de transporte). Es similar a protocolos de control tales como: ICMP (Protocolo de control de mensajes de internet) e IGMP (Protocolo de administración de grupos de internet) pero diferente a protocolos de transporte o enrutamiento. Está diseñado para funcionar sobre cualquier protocolo de enrutamiento (OSPF, EIGRP, BGP) en forma unicast o multicast.

RSVP reserva recursos para el flujo de datos a través de la red. Estos flujos con reserva son referidos a sesiones. Una sesión RSVP se define por la terna:

- Dirección Destino.- Es la dirección IP destino de los paquetes, la cual puede ser unicast o multicast.
- ID del Protocolo IP.- Es el identificador del protocolo IP.
- Puerto destino.- Es un parámetro opcional que indica el puerto de servicio en el destino.

2.9.1.4.1 Operación del protocolo RSVP

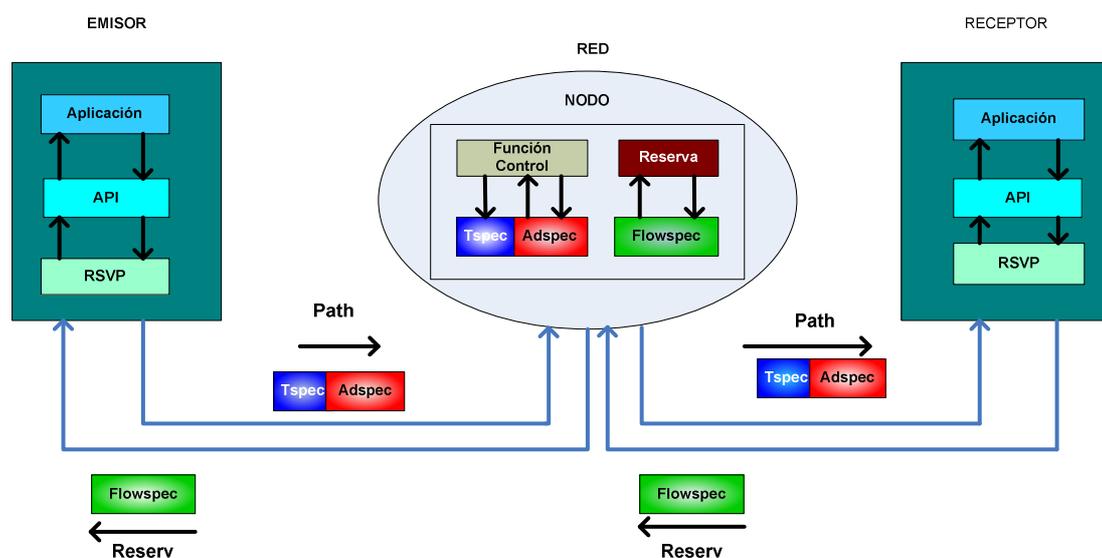


Figura 2.6 Operación Protocolo RSVP

Los pasos que se representan en la Figura 2.6 son descritos a continuación:

1. La aplicación del sistema emisor solicita una sesión RSVP.
2. Se genera un mensaje de ruta (path) a lo largo de las rutas dadas por el protocolo de encaminamiento.
3. En cada nodo se evalúa el mensaje de ruta, almacenando el estado de ruta.
4. El mensaje de ruta llega al sistema receptor.
5. Se genera la solicitud de reserva, que se encamina utilizando el estado de la ruta.
6. Cuando un nodo recibe un mensaje de reserva lo pasa a los componentes de la arquitectura IntServ, los cuales realizan pruebas y ante cualquier falla se rechaza la solicitud de reserva y el nodo envía un mensaje de error de reserva al receptor. Caso contrario, el nodo activa el clasificador y planificador de paquetes, y se envía el mensaje de reserva al siguiente nodo.

El mensaje de reserva se propaga a los emisores correspondientes, estos mensajes crean el estado de reserva en cada nodo de la ruta. El mensaje de reserva se propaga por la red hasta encontrar una reserva igual o superior, si el receptor solicita una confirmación de la reserva entonces el nodo enviará el mensaje de confirmación de reserva al receptor.

2.10 ARQUITECTURA DE SERVICIOS DIFERENCIADOS (DIFFSERV) [42], [46]

DiffServ se basa en la idea de que la información sobre la calidad de servicio se escribe en los datagramas y no en los ruteadores.

La arquitectura de servicios diferenciados (DiffServ) posibilita una discriminación de servicios escalable en Internet y redes IP. Utiliza los conceptos básicos de enrutamiento en reenvío (forwarding) y control.

Este reenvío se caracteriza por un comportamiento por salto (PHB, Per Hop Behavior) que caracteriza el tratamiento diferenciado que recibe un paquete individual. Los PHB se realizan en cada nodo para proporcionar un tratamiento diferenciado.

Los ruteadores tienen diferentes roles, los de frontera (ruteador en el punto final de dominio) clasifican a los usuarios en diferentes clases para disminuir la cantidad de información de estado, así los ruteadores del núcleo pueden contar con un número manejable de clases de usuario, Las clases pueden ser determinadas mediante el uso del campo DSCP (DiffServ Code Point) en la cabecera IP.

Todo esto se hace porque la cantidad de tráfico en el núcleo de la red no permite mecanismos complejos de QoS, ya que estos deben ser ejecutados en la red periférica donde el volumen de tráfico es menor.

Al utilizar el modelo DiffServ se obtienen varias ventajas. Los ruteadores operan más rápido, ya que se limita la complejidad de la clasificación y el encolado. Se minimizan el tráfico de señalización y el almacenamiento. Los ruteadores internos sólo están interesados en el comportamiento por salto, marcado en la cabecera del paquete. Esta arquitectura permite a DiffServ rendir mucho mejor en ambientes de bajo ancho de banda, y provee de un mayor potencial que una arquitectura IntServ. La Figura 2.7 muestra la arquitectura de la cabecera IPV4 con Diffserv.



Figura 2.7 Cabecera IPv4 con DiffServ

Para escribir la información sobre la calidad de servicio para cada datagrama se utiliza un campo de un byte en la cabecera denominado DS (ver Figura 2.8). El campo DS se estructura de la siguiente forma:

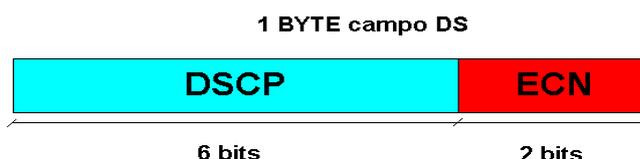


Figura 2.8 Campo DS

El subcampo ECN se utiliza para la notificación de situaciones de congestión, En cuanto al subcampo DSCP permite definir en principio hasta $2^6 = 64$ (codepoints) posibles categorías de tráfico. Aunque en la práctica no se utilizan todos los valores de DSCP se dividen en los tres grupos siguientes:

CODEPOINTS	POSIBLES VALORES	USO
x x x y y 0	32	Estándar
x x x x 1 1	16	Local / experimental
x x x x 0 1	16	Reservado

Tabla 2.11 Codepoints

De esta manera se tienen 32 posibles categorías de datagramas, correspondientes a los 5 primeros bits del campo DS.

En la Tabla 2.12 se proponen los diferentes tipos de servicios, y las características que DiffServ ofrece.

Servicio	Características
'Expedited Forwarding' o 'Premium'	<ul style="list-style-type: none"> • Es el que da más garantías. Equivale a una línea dedicada • Garantiza Caudal, tasa de pérdidas, retardo y jitter • Valor 101110 en DSCP
'Assured Forwarding'	<ul style="list-style-type: none"> • Asegura un trato preferente, pero sin fijar garantías. • Se definen cuatro clases y en cada una tres niveles de descarte de paquetes
'Best Effort' con prioridad	<ul style="list-style-type: none"> • Sin garantías, pero obtendrá trato preferente frente a 'best effort sin prioridad'
'Best Effort' sin prioridad	<ul style="list-style-type: none"> • Ninguna garantía, obtiene solo las migajas

Tabla 2.12 Características de DiffServ

El servicio Expedited Forwarding (EF) es aproximadamente equivalente al Servicio Garantizado de IntServ, mientras que el Assured Forwarding corresponde más o menos al Servicio de Carga Controlada de IntServ.

El servicio EF asegura un trato preferente pero no garantiza, caudales, retardos etc. Además se definen cuatro clases de servicio AF para asegurar este trato, pudiéndose asignar una cantidad de recursos (ancho de banda y espacio en buffer) diferente a cada una. Además, cada clase define tres categorías de descarte de paquetes (alta, media y baja). A continuación se presenta la Tabla 2.13 con los codepoints del servicio AF.

	Precedencia de descarte		
	Dd		
Clase	Baja	Media	Alta
ccc	01	10	11
4 100	10001	10010	10011
3 011	01101	01110	01111
2 010	01001	01010	01011
1 001	00101	00110	00111

Tabla 2.13 CodePoints utilizados en el servicio Assured Forwarding

En el servicio AF el usuario puede contratar con el ISP un caudal para una clase determinada, así de esta manera se podrá aplicar “traffic policing” sobre el tráfico del usuario. Algunos ISPs ofrecen servicios denominados ‘olímpicos’ con categorías denominadas tiempo-real, negocios y normal. Generalmente estos servicios se basan en las diversas clases del servicio Assured Forwarding.

En la Figura 2.9 se observa la forma como DiffServ se implementa en los ruteadores.



Figura 2.9 Implementación DiffServ en los ruteadores

2.11 SELECCIÓN DEL MODELO DE CALIDAD DE SERVICIO [42]

Después de realizar un análisis de las dos principales arquitecturas existentes para la implementación de la calidad de servicio, se puede determinar que DiffServ es la arquitectura que más garantiza que un flujo de datagramas, entre extremos finales, que conlleven aplicaciones de alta demanda de ancho de banda, puedan circular en la red y cumplan su función de transmitir el flujo de datagramas con calidad para el extremo final.

Adicionalmente, DiffServ tiene ventajas sobre IntServ, sobre todo cuando hay congestión en la red, debido a que IntServ basa su servicio en el envío de la información en datagramas extra que, aunque garantizan una buena calidad de servicio, influyen para congestionar la red, mientras que DiffServ envía información de calidad de servicio en los propios datagramas IP.

A continuación se realiza la Tabla 2.14 con la correspondiente comparación entre los servicios de ofrecen las arquitecturas analizadas.

	IntServ	DiffServ
Forma de la diferenciación del servicio	Flujos individuales	Agregado de flujo
Estado en los ruteadores	Por flujo	Por agregado
Base de la clasificación de tráfico	Algunos campos de cabecera	El campo DSCP
Tipo de diferenciación de servicio	Garantías determinísticas y estadísticas	Aseguramiento absoluto o relativo
Control de admisión	Requerido	Requerido solo para diferenciación absoluta
Protocolo de señalización	Requerido (RSVP)	No requerido para esquemas relativos; esquemas absolutos necesitan reservaciones semi-estáticas o un agente broker
Coordinación para la diferenciación del	Extremo a extremo	Local (por salto)

servicio		
Alcance de diferenciación de servicio	Ruta unicast o multicast	Cualquier lugar de la red o rutas específicas
Escalabilidad	Limitada por el número de flujos	Limitado por el número de clases de servicio
Contabilidad de la red	Basado en las características del flujo y requerimientos QoS	Basado en el uso de clases
Manejo de red	Similar a la de los circuitos conmutados	Similar a la existentes en redes IP
Despliegue interdominio	Acuerdos multilaterales	Acuerdos bilaterales

Tabla 2.14 Comparación Arquitecturas Calidad de Servicios

Una vez realizado el análisis y escogida la arquitectura a implementar, en este caso DiffSerf, se debe tener en cuenta que los equipos tengan este tipo de servicio.

Finalmente se presenta la arquitectura final de la red del ISP en la Figura 2.10, que resume todo lo realizado hasta aquí. En esencia la red consta de dos VLANs para facilitar su administración.

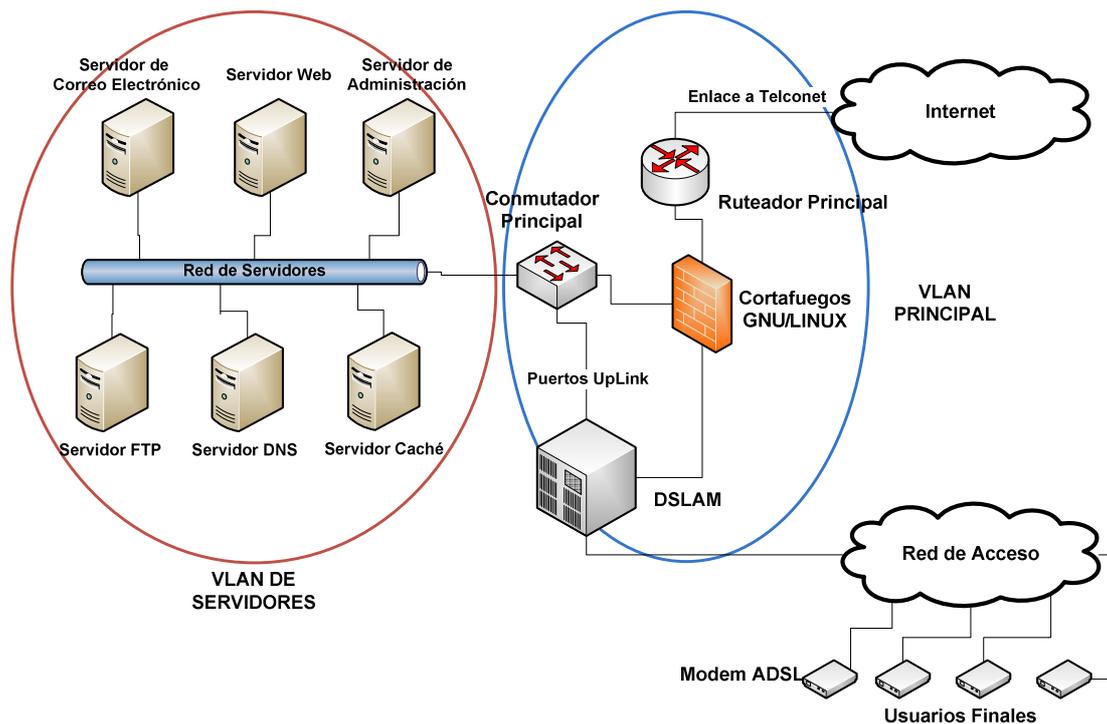


Figura 2.10 Arquitectura Final del ISP

En este capítulo se cubrieron aspectos fundamentales para el diseño del ISP. Así se puede dar por terminado este capítulo, a continuación se realizara la selección de los equipos que se utilizarán en el ISP.

CAPÍTULO 3.

DETERMINACIÓN DE EQUIPOS PARA EL ISP.

3.1 INTRODUCCIÓN

Este capítulo tiene como objetivo determinar los equipos necesarios para prestar el servicio de Internet, así como de los equipos que se requieran para prestar servicios adicionales de VoIP o transmisión de datos.

Se tomará en cuenta la arquitectura propuesta en el Capítulo 2 referente al diagrama básico del ISP.

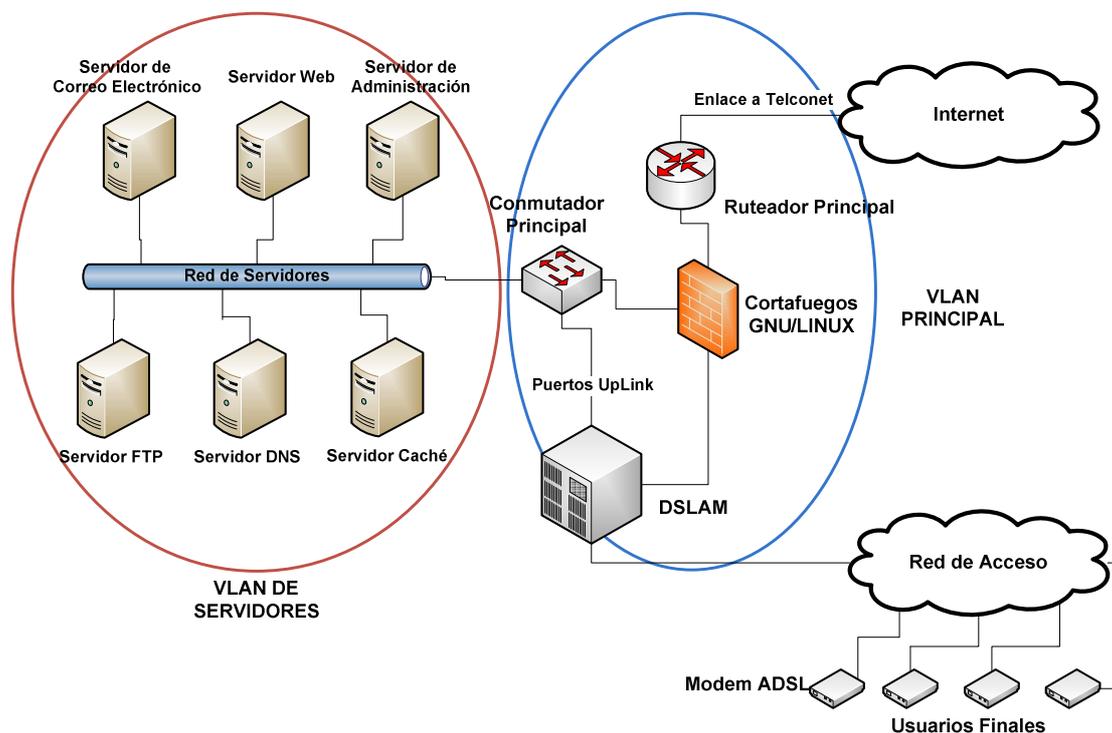


Figura 3.1 Arquitectura Final del ISP

La Figura 3.1 da una guía para realizar el análisis de los equipos que se usaran en el ISP.

3.2 REQUERIMIENTO DE LOS EQUIPOS [47], [48], [49]

Tomando en cuenta que la empresa EQUYSUM es una empresa mediana, y la población de Pto. Ayora no es de gran extensión, los equipos no deben ser grandes ni costosos, sino deben cumplir con los requerimientos básicos propuestos en el diseño.

3.2.1 RUTEADOR PRINCIPAL

El ruteador principal permite tanto la conectividad externa, como la conectividad hacia la red interna del ISP. A continuación se detallan las características técnicas mínimas que debe tener el ruteador principal:

- Conectividad LAN (10/100/1000baseTX, 10/100baseTX)
- Conectividad WAN (ATM, ISDN BRI/PRI, T1/E1, T3/E3, Serial Asíncrono)
- Multiservicio (voz, datos y video)
- Modular
- Puerto de consola asíncrono EIA-232, RJ-45
- Puerto auxiliar
- Puertos Fijos Ethernet 10/100/1000 base T, RJ-45
- Ranuras para módulos WAN/LAN
- Listas de control de acceso (ACLs, Access Control List)
- Traducción de direcciones de red (NAT, Network Address Translation)
- ATM, PPP, HDLC. Ethernet, VPN
- TCP/IP; RIP-1, RIP-2, OSPF, BGP4;
- DiffServ (Servicios Diferenciados)
- IEEE 802.1Q VLAN (20 VLANs)
- Telnet, SNMP, TFTP, VTP

La mayoría de las características expuestas anteriormente son consecuencia del estudio realizado sobre calidad de servicio, y otros de requerimientos básicos que debe tener un ruteador principal. También se debe tomar en cuenta que el ISP de

la empresa EQUYSUM se conectará a un ISP más grande o carrier para brindar el servicio de Internet, así se tiene como requerimiento básico que el ruteador maneje un protocolo de borde como es BGP; adicionalmente, influye en los requerimientos de interfaces físicos que debería tener el ruteador principal, ya que el ISP o carrier de mayor tamaño entrega sus servicios por algunos medios de transmisión como: fibra óptica, Ethernet o conexión serial. Para el caso en estudio, el carrier Telconet entregará su conexión por medio de un puerto Ethernet en uno de sus switches de interconexión de la población de Puerto Ayora.

Por otra parte, Telconet entrega un pool de direcciones IP públicas las cuales deben ser traducidas hacia los servidores y equipos del ISP, es por esto que es necesario que el ruteador maneje NAT. Esto conlleva a tener en cuenta que los equipos estarían expuestos a los ataques provenientes del exterior e inclusive de sus propios usuarios y exige implementar métodos de seguridad como un Cortafuegos o Firewall y listas de acceso o ACLs, los cuales ayudan con la selectividad de tráfico y de conexiones a los equipos.

Otro punto importante es que el ruteador debe manejar VLANs, ya que se explicó en el diseño que se las usará para separar redes y distinguirlas con mayor facilidad, lo cual ayudará al administrador de la red a identificar fácilmente problemas que puedan presentarse en el ISP.

3.2.2 CONCENTRADOR DE ACCESO O DSLAM ^[50]

El DSLAM se puede decir que es uno de los equipos indispensables para el funcionamiento de la tecnología ADSL, este contiene todas las conexiones ADSL de los usuarios. Así mismo, este debe poseer ciertas características básicas:

- Puertos de Uplink (10/100/1000)
- Puertos de acceso ADSL
- Ranuras de expansión para nuevos usuarios
- Puerto de consola asíncrono EIA-232, RJ-45

- Puerto auxiliar
- IEEE 802.1Q VLAN
- Telnet, SNMP, TFTP, VTP

Un DSLAM es transparente para los servicios que se quieren implementar como por ejemplo VoIP, aunque existen DSLAM-IP que se usan para este tipo de servicios, los mismos que se pueden manejar a nivel de ruteadores. Los puertos de Uplink permiten diferenciar un ancho de banda de otro; esto es, configurar en cada puerto de Uplink un cierto ancho de banda para facilitar la configuración de un acceso nuevo o nuevo usuario.

Los puertos ADSL en un DSLAM o ATU-C (explicados en el Capítulo 1) son indispensables para la conexión con los módems o ATU-R de los usuarios, básicamente estarían relacionados con el número de usuarios que este soporta. Dependiendo del modelo, marca y capacidad de un DSLAM estos puertos tienen un número mínimo de usuarios. Adicionalmente se deben tener ranuras de expansión para nuevas tarjetas o puertos ADSL según vaya creciendo la red de acceso.

Los usuarios en un DSLAM se diferencian uno de otro de dos maneras: la primera es por medio de VLANs y la segunda es por medio de circuitos virtuales. Estos circuitos son configurados en un DSLAM con ciertos parámetros dependiendo del servicio que se entregará, y luego son asignados a una VLAN para realizar el transporte de los datos de manera ordenada.

3.2.3 MODEM ADSL

El modem es la segunda parte más importante de la tecnología ADSL, en conjunto con el DSLAM forman la red de acceso al cliente. Hay una gran variedad de módems para la tecnología ADSL, pero uno de otro no difiere mucho. En el país se encuentran marcas como HUAWEI, FIBERHOME, BVT, XAVI, etc. Entre las características básicas de los módems ADSL están las siguientes:

- Puerto de conexión Ethernet o USB
- Soporte para ADSL2, ADSL2+
- Soporte para Bridge o Router
- Rango de transmisión máximo de 5 kmts.
- Velocidad de transmisión de bajada mayor a 24 Mbps y de subida mayor a 1 Mbps.

Los puertos de conexión indispensables para que el usuario tenga el acceso al Internet a través de los módems.

Como se explicó en el Capítulo 1 existen varias tecnologías ADSL, entre las principales y más utilizadas son la ADSL2 y ADSL2+.

Hay veces en que un usuario desea compartir su acceso a Internet con más PCs dentro de su área, la parte de Router ayuda para este propósito, en cambio la parte de Bridge o puente se aplica para usuarios con un único acceso al Internet. Pero cabe recalcar que estas no son las únicas aplicaciones de estos modos que tiene el modem.

El alcance o rango máximo de transmisión de los módems no solo depende de sí mismo, sino también del estado de la línea de transmisión, en el caso de este proyecto es del par trenzado. Las características del cable ayudan a una transmisión sin errores.

Otra característica muy importante en un modem es la velocidad a la que pueden llegar a transmitir, según el estándar que se haya configurado en el mismo; para el caso de ADSL2 es de 12 Mbps de bajada y 2 Mbps de subida y para ADSL2+ las velocidades son de 24 Mbps y 2 Mbps respectivamente.

3.2.4 CONMUTADORES

Los conmutadores permiten conectar entre si los dispositivos de la red, así mismo permiten manejar las VLANs provenientes del DSLAM que ayudan a diferenciar un cliente de otro. Se debe usar un conmutador de similares características para

tener redundancia. A continuación se detallan las características técnicas mínimas que debería tener el conmutador:

- 24 puertos Ethernet 10/100base TX autosensing, RJ45
- Puertos Uplink 1000base TX fijo
- Nivel de conmutación: 2 y 3
- Puerto de consola RJ-45asincrono EIA-232 y 1 puerto auxiliar
- Velocidad de Conmutación de paquetes de 3.6 Mbps
- Soporte 20 VLANs y direcciones MAC sobre 10K
- Telnet, SNMP
- STP (Spanning-Tree Protocol, IEEE 802.1D)
- Telnet, SNMP, TFTP, VTP
- Puertos half / full duplex.
- Manejo de enlaces Trunking.
- ACLs L2- L3
- MTBF: 200000 horas, para asegurar gran disponibilidad

Los conmutadores tienen muchos requerimientos mínimos porque por ellos pasa la mayor parte del tráfico proveniente del exterior como del interior, y deben procesar de manera rápida y precisa la información. Como aspecto fundamental que debe tener un conmutador para este proyecto es que pueda manejar VLANs ya que como se indicó anteriormente los usuarios se diferencian uno de otro por medio de estas.

Los o el puerto de Uplink de un conmutador ayuda a la rapidez con la que este procesa la información que recibe. Generalmente este puerto está conectado al ruteador y así agilizar el procesamiento de la información.

El protocolo Spanning Tree ayuda a evitar los bucles que se generan cuando se está utilizando redundancia o cuando existen varios caminos para llegar a un mismo lugar. Por ende este protocolo es fundamental para el equipo que se vaya a instalar.

3.2.5 CORTAFUEGOS

El Cortafuegos puede ser: dispositivos de hardware, aplicaciones de software o una combinación de ambos. Se colocan generalmente en el punto de conexión de la red interna con la red exterior. Para el presente diseño se optará por un dispositivo de software debido a que estos dispositivos son apropiados para empresas pequeñas o medianas, proporcionan protección para varios equipos, son independientes de los demás dispositivos. Para este caso concreto, se usará un servidor Linux, por su fiabilidad y fácil instalación y configuración del mismo. A continuación se detallan las características técnicas mínimas que debe tener el Cortafuegos:

- Número ilimitado de usuarios
- Rendimiento de 600 Mbps. y 200 de Mbps. de tráfico 3DES/AES VPN
- 2500 sesiones de usuario VPN SSL, 300.000 conexiones simultáneas
- 10000 conexiones por segundo
- 512GB de RAM
- 2 puertos Ethernet 10/100/1000BaseT (RJ-45)
- Puertos USB 2.0
- 20 VLANs (802.1q), Soporte IPsec
- Anti-X (antivirus, antispyware, bloqueo de archivos, antispam, antipishing, y filtrado URL)

3.2.6 SERVIDORES [49], [51], [52]

La diferencia principal entre los servidores y los computadores radica en el rendimiento. Los sistemas operativos de los servidores deben ser capaces de permitir el acceso a múltiples usuarios y la realización de múltiples tareas. Un servidor debe ser fiable, por esta razón es importante contar con fuentes de alimentación redundantes o un buen respaldo de energía como un banco de baterías. Las necesidades específicas de rendimiento, escalabilidad y fiabilidad

determinan el tipo de plataforma de servidor que se debe adquirir y su modo de utilización.

Un servidor se caracteriza por tener un hardware de alta capacidad, como es el caso de discos duros con gran capacidad de almacenamiento debido a la gran cantidad de información que manejan. Así mismo, deben poseer un software diferente al de un computador personal ya que sus sistemas operativos están orientados a tareas propias de servidores, tales como base de datos, correo, DNS, etc.

Los servidores también permiten autenticar usuarios y brindar acceso a recursos compartidos. Para tener un rendimiento aceptable es necesario utilizar varios servidores separados de manera que cada servidor este a cargo de cierta tarea o tareas necesarias en la red.

Los servidores requieren de un Sistema Operativo de Red (NOS, Network Operative System), capaz de brindar las funciones y servicios necesarios en un ambiente de red. Existen varios NOS, entre los cuales se puede destacar Linux, UNIX, MacOS y las versiones NT, 2000 y XP de Windows. UNIX y Linux pueden funcionar en estaciones de trabajo pero es muy común instalarlos en computadores de alto nivel. En el presente diseño se optara por Linux, por las siguientes ventajas:

- Es un Sistema Operativo de categoría "Open Source"; es decir, de código abierto y libre de licencia. Sin embargo, deben tomarse en cuenta costos de capacitación e investigación de soluciones.
- Las versiones actuales de Linux presentan un entorno gráfico muy amigable y aplicaciones maduras y funcionales.
- Linux es mucho menos susceptible a ser infectado por un virus (alrededor de 50 virus documentados [53]). Cuando un virus llega a Linux no puede ejecutarse, porque no posee permisos, y si los tuviera, no puede activar

ningún servicio porque no es dueño del “demonio” que lo ejecuta. El sistema aloja el virus pero no lo ejecuta.

- Linux fue diseñado para funcionar continuamente sin necesidad de reiniciar las maquinas debido a que muchas tareas se realizan durante la noche o en periodos tranquilos, lo que resulta en mayor disponibilidad durante los periodos de mayor ocupación del sistema y un uso más balanceado del hardware.
- Linux es seguro y versátil. Su seguridad está basada en UNIX, que se caracteriza por ser un sistema robusto y de calidad, aun así es necesaria la utilización de un cortafuegos.
- El sistema operativo y las aplicaciones de Linux tienen un tiempo de depuración muy corto, ya que miles de personas alrededor del mundo las arreglan constante y rápidamente. (alrededor de dos horas entre la detección y corrección del error)
- Existe una gran gama de distribuciones que sea adaptan a diferentes requerimientos, todas contienen el mismo conjunto de paquetes básicos.

3.2.6.1 GNU/Linux [⁵³]

Linux está basado en Kernel, con arquitectura UNIX y existe desde 1992. Su desarrollo ha sido auspiciado por la fundación GNU. Por esta razón comúnmente se habla de GNU/Linux o simplemente Linux. Se caracteriza por su estabilidad y seguridad. El sistema operativo en sí, se llama Kernel y constituye el eje de un sistema informático. Existen varias versiones, la versión 2.4 está completamente probada y en utilización, la versión 2.6 incluye varias mejoras en el soporte de dispositivos físicos como microprocesadores de alto desempeño, puertos USB, etc.). Generalmente el usuario no interactúa directamente con el Kernel, sino con las aplicaciones, mientras que el Kernel interactúa con las aplicaciones y con los componentes de hardware.

Existen diferentes versiones de GNU/Linux que se las conoce como distribuciones de Linux, las cuales se diferencian una de otra no por el Kernel que usan sino por las aplicaciones propietarias de cada uno.

3.2.6.2 Distribuciones de Linux

Una distribución de Linux es una combinación de una versión de Kernel, con un conjunto de aplicaciones orientadas a una tarea específica. Una distribución se asocia generalmente a un distribuidor; es decir, a la entidad que lo desarrolla y distribuye. Cada entidad tiene sus políticas de distribución que se encuentran relacionadas directamente a los objetivos de dicha organización. Formalmente el término Linux debería referirse solamente al Kernel. Existe un gran número de distribuciones entre las cuales se puede mencionar: Red Hat, Mandrake, Debian, Suse, Knoppix, Fedora, CentOS, entre otras.

Cada una de estas distribuciones posee características básicas similares pero diferente orientación. La gran mayoría de distribuciones poseen la misma versión del Kernel y un conjunto similar de aplicaciones. Incluso ciertas distribuciones son derivadas de otras distribuciones como Mandrake y CentOS que se derivan de Red Hat, o Knoppix y Ubuntu que son derivadas de Debian. Entre las diferencias más importantes entre las distribuciones de Linux se puede destacar las siguientes:

- **Soporte y capacitación.** Muchos distribuidores obtienen sus ganancias mediante la oferta de soporte técnico y la capacitación en el uso de sus productos, o comercializando distribuciones certificadas con garantía.
- **Aplicaciones de instalación y configuración.** Los distribuidores más grandes de Linux han desarrollado un conjunto de aplicaciones de instalación y configuración que facilitan la administración del sistema operativo, esto ha ocasionado que ciertas distribuciones sean más populares que otras.

- **Orientación a tareas específicas.** Algunas distribuciones están orientadas a una tarea específica y contienen aplicaciones reconfiguradas para facilitar el proceso de instalación de dichas tareas.

En vista de que las distintas distribuciones están basadas en el mismo Kernel y las mismas aplicaciones, lo que realmente interviene en el presente diseño radica en escoger una distribución adecuada para las necesidades de un Proveedor de Servicios de Internet. La distribución elegida es CentOS (Community Enterprise Operating System), que está enfocada para el uso en servidores y es un clon a nivel binario de la distribución RHEL (Red Hat Enterprise Linux), compilado por voluntarios a partir del código fuente liberado por Red Hat.

3.2.6.3 CentOS 5.0 [⁵⁴], [⁵⁵]

CentOS 5.0 está basado Red Hat 5, y utiliza el Kernel 2.6.18. CentOS soporta prácticamente las mismas arquitecturas que el original RHEL 5, como se detalla a continuación:

- i386: Esta arquitectura soporta procesadores: AMD (K6, K7, Thunderbird, Athlon, Athlon XP, Sempron), Pentium (Classic, Pro, II, III, 4, Celeron, M, Xeon), VIA (C3, Eden, Luke, C7).
- x86_64: soporta procesadores: AMD 64 (Athlon 64, Opteron) and Intel Pentium (Xeon EM64T).
- Hardware recomendado: Memoria RAM: 64 MB (mínimo) y espacio en Disco Duro de 512 MB (mínimo) - 2 GB (recomendado).

3.2.6.4 Servidor de correo electrónico [48], [⁵⁶], [⁵⁷]

Un servidor de correo electrónico en Linux garantiza la independencia del ISP en cuanto a servicios gratuitos como Hotmail o Yahoo sin necesidad de la adquisición de ningún software. Para el presente diseño se utilizará el software

Sendmail. Sendmail es un agente de transporte de correo electrónico (MTA, Mail Transfer Agent) que se caracteriza por su seguridad, eficiencia, facilidad de configuración y administración, compatibilidad con otros sistemas de correo.

La capacidad de disco duro del servidor de correo electrónico está relacionada directamente con el número de posibles clientes que soliciten una cuenta de correo. A cada uno se le asigna cierta cantidad de memoria para almacenar sus mensajes.

Como no todos los clientes solicitan una cuenta de correo (los clientes corporativos generalmente poseen sus propios servidores y pocos clientes residenciales solicitan una cuenta), se asumirá que el 50% de los clientes solicitan cuenta de correo. El espacio de memoria disponible para almacenamiento de mensajes en cada cuenta será de 25 MB. En la Tabla 3.1 se indica el cálculo de la capacidad requerida para el servidor de correo.

AÑO	CLIENTES	CAPACIDAD EN DISCO
Primer año	32	2GB (S.O) +725 MB=2.8GB
Segundo año	126	3.8GB
Tercer año	346	5.4GB
Cuarto año	909	7.5GB

Tabla 3.1 Capacidad requerida para el servidor de correo

Para tener alta seguridad en el filtrado de correo, tanto entrante como saliente, es conveniente instalar también en el servidor de correo electrónico, un antivirus y un antispam para Linux. Para el caso de este proyecto se usa conjuntamente con Sendmail, el antivirus Clamav y el antispam MailScanner. Este servidor realiza las siguientes funciones:

- **Escaneado de tráfico de correo mejorado.** Escaneo de correo entrante y saliente, escaneo por "asunto", "cuerpo" y "adjunto", utilizando un mínimo de recursos del sistema.
- **Prevención sobre el filtrado de información.** Filtro de contenido (acciones frente a mensajes con virus), definición de parámetros de actuación en función de patrón establecido y protección antispam contra envíos masivos.
- **Filtro AntiSpam.** Bloquea correo que proviene de ciertas direcciones predefinidas, consulta en tiempo real de listas de direcciones consideradas como Spam y realiza análisis de cabecera, asunto y cuerpo para determinar contenido considerado como Spam.

A continuación se detallan las características técnicas mínimas del Servidor de correo electrónico:

- Certificación de Soporte RHEL 5 (Red Hat Enterprise Linux Version 5), categoría servidor
- Procesador Intel Dual Core 3.0GHz, 1333Mz FSB
- 512 de RAM con capacidad de expansión del 100%
- 2 GB libres en disco para software y 2.8 GB para almacenamiento de mensajes
- Disco duro SAS (Serial Attached SCSI; SCSI: Small Computer System Interface), con la capacidad de expansión de dos discos duros hot swap.
- Memoria cache externa L2 de 2MB.
- Software: Sendmail
- Puertos USB
- Antivirus y antispam: Clamav y MailScanner
- 2 puertos Ethernet 10/100 baseTX, RJ45.
- Puerto para teclado, monitor y ratón
- Unidad de CD-ROM 24x o superior

3.2.6.5 Servidor Web [48], [56], [57]

El servicio Web provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, video, o cualquier contenido accesible vía Web.

En el presente diseño se utiliza el software Apache 2.2 con PHP 5.2.11, que constituye un servidor web en Linux, potente y flexible. Para el cálculo de la capacidad de disco del servidor, a cada usuario se le asigna un espacio referencial de 125MB.

Las empresas grandes suelen tener sus propios servidores, por lo que no todos los clientes dedicados contrataran este servicio, sin embargo en el cálculo se tomará en cuenta el 100% de clientes, para poder ofrecer capacidades de alojamiento mayores a 125MB.

AÑO	CLIENTES	CAPACIDAD EN DISCO
Primer año	32	2GB (S.O) +2.7GB = 4.7GB
Segundo año	126	8.9GB
Tercer año	346	14.7GB
Cuarto año	909	22.9GB

Tabla 3.2 Capacidad requerida para el servidor web

A continuación se detallan las características técnicas mínimas del Servidor Web.

- Certificación de Soporte RHEL 5, categoría servidor
- Procesador Intel Dual Core 3.0 GHz, 1333Mz FSB
- 512MB de RAM con capacidad de expansión del 100%
- 2 GB libres en disco para software y 4.7GB para alojamiento web

- Disco duro SAS, capacidad de expansión requerida hasta el cuarto año
- Memoria cache externa L2 de 2MB.
- Puertos USB
- Software: Apache 2.2 con PHP 5.2.11
- 2 puertos Ethernet 10/100 baseTX, RJ45.
- Puerto para teclado, monitor y ratón
- Unidad de CD-ROM 24x o superior

3.2.6.6 Servidor FTP [48], [56], [57]

El Servidor FTP requiere de una unidad de disco considerable, gran velocidad y altas prestaciones. En el presente diseño se utilizará el Sistema Operativo Linux, con el software ProFTPD. ProFTPD es un servidor FTP probado, escalable y de buen desempeño que se caracteriza por su seguridad, simplicidad y facilidad de configuración. Es importante también instalar un antivirus en el servidor FTP para protección de los archivos.

Se considerará una capacidad del servidor FTP similar a la capacidad del servidor web, debido a que aquí se almacenarán los programas disponibles en el ISP para la descarga por parte de los clientes [48]. A continuación se detallan las características técnicas mínimas del servidor FTP:

- Certificación de Soporte RHEL 5, categoría servidor
- Procesador Intel Dual Core 3.0 GHz, 1333Mz FSB
- 512 de RAM con capacidad de expansión del 100%
- 2 GB libres en disco para software y 30 GB para programas disponibles
- Disco duro SAS, capacidad de expansión de 2 discos duros hot swap
- Memoria cache externa L2 de 2MB.
- Software: Proftpd
- Puertos USB
- 2 puertos 10/100 baseTX, RJ45.
- Puerto para teclado, monitor y ratón

- Unidad de CD-ROM 24x o superior

3.2.6.7 Servidor Caché [48], [56], [57]

El objetivo del servidor cache es acelerar el suministro de información a los usuarios de la WWW. La mayor cantidad de páginas web son visitadas durante el periodo pico de utilización de la red, generando la mayoría del tráfico. Durante este periodo el Servidor Cache almacena las páginas visitadas; por esta razón, durante otros periodos del día se registrarán peticiones tanto nuevas como repetidas.

Cada cierto tiempo el servidor cache borra de su memoria las páginas no solicitadas para poder almacenar las nuevas peticiones. Se utilizará el software Squid ya que soporta HTTP y FTP, posee un mecanismo avanzado de autenticación y control de acceso. Para mejorar el desempeño de la red, el Servidor Cache estará ubicado en el mismo segmento que el ruteador principal.

En el cálculo de la capacidad del servidor cache se considerará un periodo pico de 8 horas al día, que es el número de horas laborales en el Ecuador, 70% de tráfico web y un nivel de repetición de peticiones del 50%, valores recomendados en [48].

Cantidad de información transmitida: Ancho de banda [Kb/s] * 8[h/día] * [3600s/1 h]

Capacidad de disco \approx Cantidad de información transmitida * 0.7 * 0.5

AÑO	ANCHO DE BANDA [Kbps]	CAPACIDAD EN DISCO
Primer año	1204	2GB (S.O) + 8.9GB = 10.9GB
Segundo año	4836	24.4GB
Tercer año	13296	43.6GB
Cuarto año	34917	70.3GB

Tabla 3.3 Capacidad requerida para el servidor caché

A continuación se detallan las características técnicas mínimas del servidor cache:

- Certificación de Soporte RHEL 5, categoría servidor
- Procesador Intel Dual Core 3.0 GHz, 1333Mz FSB
- 512 de RAM con capacidad de expansión del 100%
- 2 GB en disco para software y 11 GB para almacenamiento de páginas web
- Disco duro SAS, capacidad de expansión requerida hasta el cuarto año
- Memoria cache externa L2 de 2MB.
- Software: Squid
- Puertos USB
- 2 puertos Ethernet 10/100 baseTX, RJ45.
- Puerto para teclado, monitor y ratón
- Unidad de CD-ROM 24x o superior

3.2.6.8 Servidor DNS [54], [56], [57]

El servidor DNS es encargado de recibir y resolver peticiones relacionadas con el sistema de nombres. Un servidor DNS traduce un nombre de dominio en una dirección IP, asigna nombres a las maquinas de una red y trabaja con nombres de dominio en lugar de IPs. Como mínimo, el disco duro del servidor DNS debe tener la capacidad mínima para almacenar el Sistema Operativo y alrededor de 9 GB para almacenar archivos DNS, valor recomendado en [48]. En este diseño se optará por el Software BIND (Berkeley Internet Name Domain), que es una implementación del protocolo DNS que provee mejores componentes del sistema DNS como un Sistema de Nombre de Dominio, una librería de resolución de nombres y herramientas para verificar la correcta operación del servidor DNS.

BIND es utilizado en la mayoría de servidores DNS de Internet y provee una arquitectura estable y robusta. A continuación se detallan las características técnicas mínimas del servidor DNS:

- Certificación de Soporte RHEL 5, categoría servidor
- Procesador Intel Dual Core 3.0 GHz, 1333Mz FSB
- 512 de RAM con capacidad de expansión del 100%
- 2 GB libres en disco para software y 9 GB para almacenamiento DNS
- Disco duro SAS, capacidad de expansión de dos discos duros hot swap
- Memoria cache externa L2 de 2MB.
- Software: Bind 9.4.1
- Puertos USB
- 2 puertos Ethernet 10/100 Base TX.
- Puerto para teclado, monitor y ratón
- Unidad de CD-ROM 24x o superior

Es importante tomar en cuenta la adquisición de un Servidor DNS de respaldo con la misma capacidad del servidor principal.

3.2.6.9 Servidor administración [48]

El servidor de administración almacena el software de administración y monitoreo del ISP, por lo cual sus características están sujetas a los requerimientos específicos de dichos programas. El software de gestión de red debe contar con una interfaz grafica que permita:

- Graficar y administrar la red y sus componentes
- Monitorear el tráfico de la red
- Administrar la red (equipos de la red VLANs, enlaces, etc.)
- Detectar y corregir fallos.
- Seguir el estado y funcionamiento de la red.
- Configurar/reconfigurar la red.
- Características de Calidad de Servicio
- Generar alarmas y reportes de tráfico y uso de la red

El servidor de administración puede instalarse en un computador personal normal, pero siempre un servidor será más robusto. A continuación se presentan las características técnicas mínimas del servidor de administración:

- Certificación de Soporte RHEL 5, categoría servidor
- Procesador Intel Dual Core 3.0 GHz, 1333Mz FSB
- 2 GB de RAM, 80 GB en disco, para que almacenar Software.
- Disco duro SAS, capacidad de expansión de dos discos duros hot swap
- Memoria cache externa L2 de 2MB.
- 2 puertos Ethernet 10/100 base TX, RJ45.
- Puertos USB
- Puerto para teclado, monitor y ratón
- Unidad de CD-ROM 24x o superior
- Unidad de respaldo de datos

3.3 DIRECCIONAMIENTO IP

Esta sección está orientada a realizar una propuesta de direccionamiento para los equipos, y facilitar las configuraciones y administración de los mismos.

Como se mencionó al final del Capítulo 2, por facilidad de administración del ISP se dividió la red en dos VLANs. La primera que constará de los siguientes equipos: ruteador principal, conmutador principal, DSLAM y cortafuegos. La segunda tendrá todos los equipos relacionados con los servidores.

Para la primera VLAN se tomará una subred privada para 8 equipos, es decir, se toma un factor de crecimiento de la red. Así la subred con las IPs para cada equipo quedaría:

Ruteador principal = 192.168.200.1 255.255.255.248

Conmutador principal = 192.168.200.2 255.255.255.248

DSLAM = 192.168.200.3 255.255.255.248

Cortafuegos = 192.168.200.4 255.255.255.248

Quedando libres 2 IPs disponibles dentro de la subred para futuros equipos que se puedan agregar.

En el caso de la segunda VLAN se tomara una subred privada para 16 equipos, de igual manera se toma un factor de crecimiento de la red. Así la subred con las IPs para cada equipo quedaría:

Servidor de administración = 192.168.300.2 255.255.255.240

Servidor DNS = 192.168.300.3 255.255.255.240

Servidor de Correo Electrónico = 192.168.300.4 255.255.255.240

Servidor FTP = 192.168.300.5 255.255.255.240

Servidor Caché = 192.168.300.6 255.255.255.240

Servidor Web = 192.168.300.7 255.255.255.240

Quedando libres 9 IPs disponibles dentro de la subred para futuros requerimientos.

Para el caso de direccionamiento de los clientes se lo asignara de acuerdo a la VLAN que se configure para el mismo, por ejemplo: si la VLAN es la 3 la dirección asignada al cliente en el ruteador seria 192.168.3.1 255.255.255.252.

3.4 SELECCIÓN DE EQUIPOS

A continuación se presentan diferentes opciones en cuanto a equipos, que cumplen los principales requisitos del diseño para elegir aquellos que se acoplen de la mejor manera al mismo. Se tomarán en cuenta equipos que se encuentran en el mercado y sean accesibles para la empresa.

Todo equipo debe ser elegido de tal modo que se minimice o que no se generen aspectos negativos en términos económicos y de calidad en el servicio para el usuario final y para el ISP en general.

3.4.1 RUTEADOR PRINCIPAL ^[58], ^[59], ^[60]

Para el presente proyecto se tomó en cuenta que los equipos que se comparan son orientados a empresas medianas y con un presupuesto que no es comparable al de empresas de gran tamaño.

En la Tabla 3.4 se presentan tres opciones de equipos para ruteador principal, y se indican los requerimientos del diseño que



CARACTERÍSTICAS			
Imagen			
Modelo	1841	5232	DI-2621
Conectividad LAN (10/100/1000 baseTX, 10/100baseTX)	√	√	√
Conectividad WAN (ATM, ISDN BRI/PRI, T1/E1, T3/E3, Serial Asíncrono)	√	√	√
Multiservicio (voz, datos y video)	√	√	√
DRAM de 256 MB default (expansión hasta 1GB)	√	√	x
Flash de 64 MB default (expansión hasta 256 MB)	√	x	x
Modular	√	√	√
Puertos USB	√	x	x
1 puerto de consola RJ-45asíncrono EIA-232	√	√	√
1 puerto auxiliar	√	√	√
2 puertos Fijos Ethernet 10/100/1000 base TX, RJ-45	√	√	√
4 Ranuras para módulos WAN/LAN	√	√	√
IPv6	√	x	x
ACLs	√	√	√
NAT	√	√	√
ATM, PPP, HDLC. Ethernet	√	√	√
TCP/IP; RIP-1, RIP-2, OSPF, BGP4	√	√	√
DiffServ (Servicios Diferenciados)	√	√	√
VPN	√	√	√
Algoritmo de Cifrado AES, DES y Triple DES	√	√	x
IEEE 802.1Q VLAN (20 VLANs)	√	√	√
Telnet, SNMP	√	√	√
Fuente de poder dual	x	x	x
Alimentación 110 V AC, 60 Hz.	√	√	√

Tabla 3.4 Comparación entre equipos para ruteador principal

Como se puede observar en la Tabla 3.4, los tres modelos de ruteadores cumplen con la mayoría de requerimientos, pero DI-2621 no soporta algunos requerimientos al igual que el ruteador 3com 5232, además no soportan IPv6. Además estos dos modelos no soportan VoIP, otra característica necesaria; mientras el ruteador Cisco 1841 cumple con todos los requerimientos, por lo que es el modelo escogido para este diseño.

A continuación se presenta en la Tabla 3.5 una configuración recomendada para el ruteador principal de este proyecto:

COMANDOS	UTILIZACIÓN
<ul style="list-style-type: none"> • policy-map 64 • class class-default • shape average 64000 	Comandos utilizados para control de ancho de banda
<ul style="list-style-type: none"> • interface FastEthernet0/0.1 • encapsulation dot1Q 1 native • ip address 192.168.200.1 255.255.255.248 • ip access-group 101 in • ip nat inside 	Configuración del la IP del ruteador en la VLAN principal dentro de un subinterfaz
<ul style="list-style-type: none"> • interface FastEthernet0/0.2 • description SERVIDORES • encapsulation dot1Q 2 • ip address 192.168.300.1 255.255.255.240 • ip access-group 101 in • ip nat inside 	Configuración del la IP de los servidores en la VLAN secundaria dentro de una subinterfaz
<ul style="list-style-type: none"> • interface FastEthernet0/0.3 • description CLIENTE • bandwidth 64 • encapsulation dot1Q 3 • ip address 192.168.3.1 255.255.255.0 • ip access-group 101 in • ip nat inside • service-policy output 64 	Configuración del la IP de un cliente y su VLAN correspondiente dentro de una subinterfaz. Control de ancho de banda y control de acceso por ACL

<ul style="list-style-type: none"> • interface FastEthernet0/1 • bandwidth 1024 • ip address 200.93.212.114 255.255.255.252 • ip nat outside 	Configuración de la IP Pública dentro de un interfaz del ruteador con su respectivo ancho de banda
<ul style="list-style-type: none"> • ip route 0.0.0.0 0.0.0.0 200.93.212.113 • ip route 192.168.0.0 255.255.255.0 192.168.21.2 • ip route 200.93.212.126 255.255.255.255 FastEthernet0/0.18 name CCCQ 	Rutas estáticas para acceder al Internet, a una red de algún usuario y algún servidor de un usuario que usa IP pública.
<ul style="list-style-type: none"> • ip nat pool PUBLICA 200.93.212.114 200.93.212.114 prefix-length 30 • ip nat inside source list 1 pool PUBLICA overload • ip nat inside source static tcp 192.168.200.2 80 200.93.212.114 8888 extendable 	Configuración del NAT dinámico con una IP pública del pool entregado, y configuración de NAT para administrar el conmutador principal por medio del navegador de Internet.
<ul style="list-style-type: none"> • access-list 1 permit 192.168.0.0 0.0.255.255 • access-list 101 permit tcp 192.168.15.0 0.0.0.255 any eq smtp • access-list 101 deny tcp any any eq smtp • access-list 101 permit ip any any 	Configuración de ACLs para control de acceso de los clientes y control para correo electrónico.
<ul style="list-style-type: none"> • snmp-server community equsumsnmp RO 	Configuración del protocolo SNMP para administración de la red.

Tabla 3.5 Comandos de configuración sugeridos para el ruteador principal.

3.4.2 CONMUTADORES [58], [59], [60]

Para este proyecto los puntos claves en la elección de los conmutadores está en la parte de si manejan VLANs y si poseen protocolos básicos de conmutación como Spanning Tree. A continuación se presenta la Tabla 3.6 con los posibles conmutadores:

CARACTERÍSTICAS	CISCO	3COM	DLINK
IMAGEN			
MODELO	Express 500-24TT	4500G - 24	DES-1228
24 puertos FastEthernet 10/100base TX autosensing, RJ45	√	√	√
1 Puerto UL 1000base TX fijo	√	√	√
Nivel de conmutación: 2 y 3	√	√	√
DRAM de 16 MB Memoria	√	√	√
Flash de 8 MB	√	√	√
Backplane sobre 4.8 Gbps., Full Duplex	√	√	√
1 Puerto de consola RJ-45 Asíncrono EIA 232	√	√	√
1 puerto auxiliar	√	√	√
Velocidad de conmutación de paquetes de 3.6 Mbps	√	√	√
Soporte VLANs y direcciones MAC sobre 8K	√	√	√
Telnet, SNMP, TFTP, VTP	√	√	√
STP (Spanning-Tree Protocol, IEEE 802.1D)	√	√	√
DiffServ (Servicios Diferenciados)	√	√	√
Puertos half/full dúplex	√	√	√
Manejo de enlaces Trunking			
IPv6	√	√	√
ACLs L2-L3	√	√	√
IEEE 802.1x	√	√	√
Alimentación de energía redundante, 120/230V AC (50/60 Hz)	√	√	√
MTBF: 300000 horas, para asegurar gran disponibilidad	√	√	√

Tabla 3.6 Comparación entre equipos para conmutador principal

Como se puede observar no hay diferencia entre los conmutadores propuestos. Por motivos de fácil accesibilidad al equipo y fiabilidad de la marca se escoge el conmutador CISCO Express 500-24TT. Un dato curioso de este equipo es el de que se puede administrar por medio de un navegador de Internet como IExplorer.

Las siguientes Figuras muestran una configuración recomendada para el conmutador principal:

Express Setup

Configuración de red

Interfaz de administración (VLAN): default - 1

Modo de asignación IP: Estático DHCP

Dirección IP: 192 . 168 . 200 . 2 Máscara de subred: 255.255.248.0

Puerta de enlace predeterminada: 192 . 168 . 200 . 1

Figura 3.2 Configuración de la IP y VLAN del conmutador principal

Puerto	Perfil	VLAN nativa	VLAN de acceso
Fa1	Desktop		default - 1
Fa2	Router	default - 1	
Fa3	Switch	default - 1	
Fa4	Switch	default - 1	
Fa5	Switch	default - 1	
Fa6	Switch	default - 1	
Fa7	Desktop		2-2
Fa8	Desktop		2-2
Fa9	Desktop		2-2

Figura 3.3 Configuración los puertos del conmutador y asignación de VLANs

Administrador de Dispositivos Serie Catalyst Express 500 - Switch Idioma:

Actualizar Imprimir Smartports Actualizar software Leyenda Ayuda

Tiempo de funcionamiento: 3 semanas, 2 días, 14 horas, 37 minutos Próxima actualización:

Visualizar: Estado

Catalyst Express 500 SERIES

Mueva el cursor sobre los puertos para obtener más información.

Contenidos

- Dashboard
- Configurar
 - Smartports
 - Configuración del puer
 - Express Setup
 - VLANs**
 - SNMP
 - EtherChannels
 - Usuarios y contraseña
 - Reiniciar / Restaurar
- Monitorizar
 - Diagnóstico
 - Actualizar software
 - Network Assistant

VLAN: Crear

Nombre VLAN: 25

ID VLAN: 25

Listo Cancelar

Figura 3.4 Creación de una nueva VLAN

The screenshot shows the Catalyst Express 500 Switch configuration interface. The top bar displays the title 'Administrador de Dispositivos Serie Catalyst Express 500 - Switch' and the language 'Idioma: Es'. Below the title bar, there are icons for 'Actualizar', 'Imprimir', 'Smartports', 'Actualizar software', 'Leyenda', and 'Ayuda'. The status bar indicates 'Tiempo de funcionamiento: 3 semanas, 2 días, 14 horas, 35 minutos' and 'Próxima actualización en 1'. A visual representation of the switch hardware is shown with a 'Visualizar: Estado' dropdown and a note: 'Mueva el cursor sobre los puertos para obtener más información.' The main content area is titled 'VLAN' and contains a table with the following data:

Nombre	ID	Borrar
22	22	<input type="checkbox"/>
23	23	<input type="checkbox"/>
24	24	<input type="checkbox"/>
3	3	<input type="checkbox"/>
4	4	<input type="checkbox"/>

Buttons for 'Crear', 'Avanzado', 'Enviar', and 'Cancelar' are visible at the bottom of the interface.

Figura 3.5 Listado de las VLANs del conmutador principal

3.4.3 DSLAM

Como se dijo anteriormente, este es uno de los equipos indispensables para el funcionamiento de ADSL. En el país no existen muchos proveedores de estos equipos. Actualmente quien lidera el mercado en este tipo de equipos es la empresa HUAWEI. Es por este motivo que se escoge uno de sus equipos para el diseño de este proyecto.

Se debe seleccionar un equipo para una pequeña a mediana empresa como es el caso de la empresa EQUYSUM. Con estos antecedentes se selecciono el equipo de la serie SmartAX MA5300. Las características técnicas del equipo se presentan en el Anexo 1

A continuación se presenta en la Tabla 3.7 una configuración recomendada para el DSLAM

COMANDO	UTILIZACIÓN
<ul style="list-style-type: none"> • interface vlanif1 • description HUAWEI, MA5600 Series, Vlanif1 Interface • ip address 192.168.200.3 255.255.255.448 	Configuración de la IP del DSLAM y su VLAN correspondiente.
<ul style="list-style-type: none"> • adsl line-profile quickadd 128 basic-para all trellis 1 bitswap 1 1 channel interleaved 16 6 adapt fixed snr 6 0 31 6 0 31 rate 128 128 128 128 name ADSL LINE PROFILE 128 	Configuración de un perfil para clientes de 128 kbps de ancho de banda
<ul style="list-style-type: none"> • vlan 2 to 27 mux • port vlan 4 0/7 3 • port vlan 2 0/7 4 • port vlan 5 to 13 0/7 4 	Configuración de las VLANs y asignación de las mismas de acuerdo al tipo de compartición.
<ul style="list-style-type: none"> • port desc 0/6/3 description PRUEBAS-EQY • activate 3 profile-index 128 • service-port vlan 6 adsl 0/6/3 vpi 8 vci 35 rx-cttr 0 tx-cttr 0 	Configuración de un puerto ADSL y asignación a un perfil predefinido y asignación de la VLAN correspondiente.
<ul style="list-style-type: none"> • ip route-static 0.0.0.0 0.0.0.0 192.168.200.1 • snmp-agent sys-info version v1 v2c 	Configuración de la ruta por defecto para accede al Internet y activación del protocolo SNMP para el servidor de administración
<ul style="list-style-type: none"> • line-rate 256 port 0/7/3 • line-rate 512 port 0/7/4 	Configuración de los puertos de UPLINK y su ancho de banda de acuerdo a la compartición que se maneja.

Tabla 3.7 Comandos de configuración sugeridos para el DSLAM

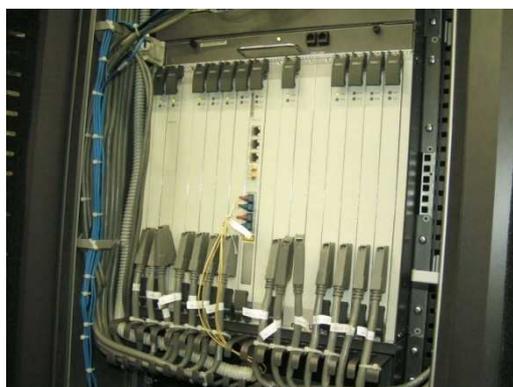


Figura 3.6 DSLAM para ADSL

3.4.4 MODEM

Como se dijo anteriormente, la segunda parte fundamental en una red ADSL es el modem de Internet, básicamente es el que recibe los datos del ISP y los entrega al usuario final. Para este proyecto se optó por la marca FIBERHOME, ya que es de fácil acceso y se la encuentra en el mercado actual con un costo moderado. Las características técnicas del equipo se presentan en el Anexo 2



Figura 3.7 Modem para ADSL

3.5 SOFTWARE PARA MONITOREO Y ADMINISTRACIÓN

Existe una variedad de opciones en cuanto al Software de monitoreo que se ejecuta sobre Linux o Windows, disponibles para descarga en Internet, como el MRTG. En cuanto al Software de administración, la mejor opción está ligada directamente a la decisión del administrador del ISP.

3.5.1 MRTG

MRTG (Multi Router Traffic Grapher) es una herramienta, escrita en Lenguaje C, que se utiliza para supervisar la carga de tráfico de interfaces de red. MRTG genera páginas HTML con gráficos que proveen una representación visual de dicho tráfico. MRTG utiliza SNMP (Simple Network Management Protocol) para recolectar los datos de tráfico de un determinado dispositivo (ruteadores o servidores), por tanto es requisito contar con al menos un sistema con SNMP funcionando y correctamente configurado.

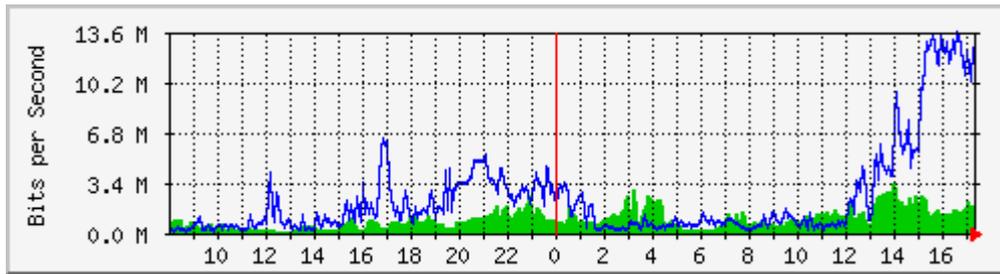


Figura 3.8 Resultado presentado por MRTG

3.5.2 CACTI

CACTI es una herramienta de usuario final basada en RRDtool (Round Robin Database tool) que trabaja conjuntamente con MRTG para presentar sus graficas. Al igual que MRTG utiliza SNMP para la recolección de datos de los equipos de la red. Esta herramienta, a diferencia de MRTG, muestra sus gráficas de manera más ordenada y presentable, si el caso fuera la de presentar informes frente a supervisores.

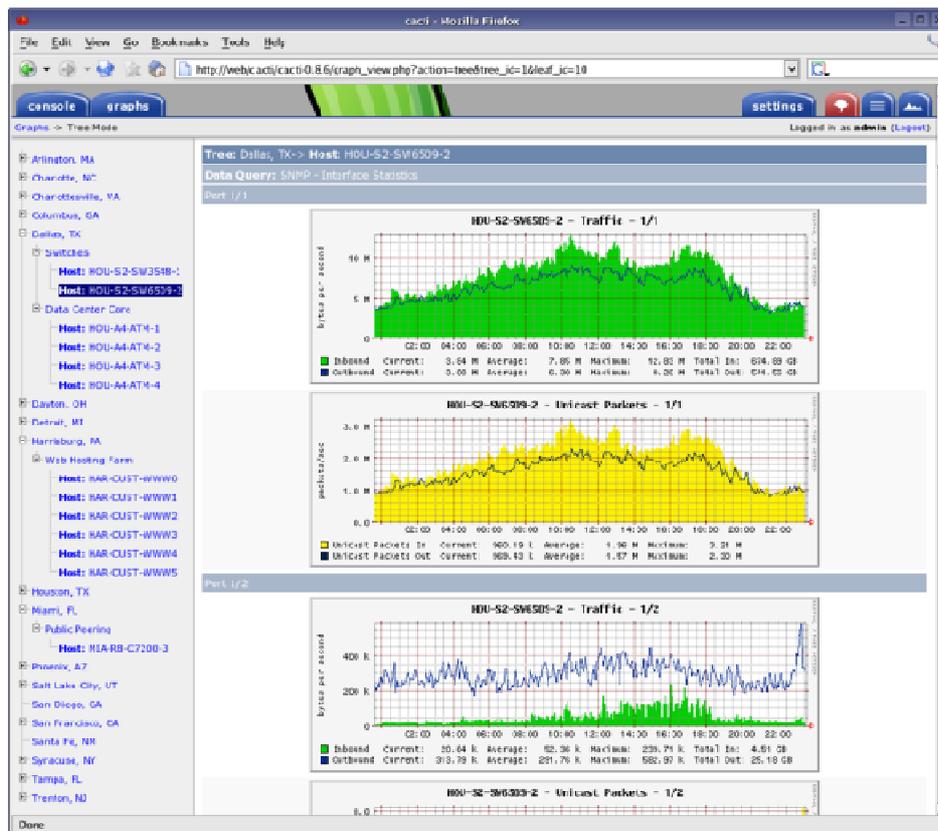


Figura 3.9 Resultados presentados por CACTI

Estas herramientas también se pueden utilizar para la parte de administración de la red. Algo importante sobre las mismas es que son software libre, pero esto no quita que su desempeño sea eficaz y con resultados favorables para sus usuarios.

3.6 SEGURIDADES DEL ISP

A pesar de todas las ventajas que brinda el Internet, conforme se realizan progresos aumentan también los riesgos de vulnerabilidades informáticas ante amenazas internas y externas que puedan comprometer la seguridad de la red.

Debido al gran crecimiento de los servicios de banda ancha, existe una infinidad de computadoras conectadas a Internet. La seguridad de las redes en ambientes residenciales no suele tomarse como una prioridad; sin embargo, en un ISP la seguridad es un aspecto fundamental, por lo que se deben analizar los problemas más relevantes y evitarlos o minimizarlos.

La mayoría de empresas ven a la seguridad de la red como una medida reactiva ante un problema dado, cuando lo ideal es tomarlo como una medida preventiva. Cuando se conoce de una vulnerabilidad, puede pasar demasiado tiempo hasta solucionarla y el impacto de una violación de seguridad puede tener graves consecuencias.

Entre los problemas más comunes de seguridad para redes en general, particularmente para un ISP, que es el diseño en cuestión, se puede mencionar:

- Intentos de robo de identidad como phishing y pharming.
- Infección de virus, spyware y software malicioso.
- Inundación de tráfico (Flooding), ICMP, UDP.
- IP de origen falso (Spoofing), muy difícil de detectar y filtrar.
- Negación del servicio (DoS, Deny of Service), que es un ataque que busca volver inaccesibles los recursos de la red a los usuarios autorizados.

- Negación del servicio distribuida (DDoS, Distributed Deny of Service), que consiste en direcciones distribuidas en un amplio rango de direccionamiento IP. DoS y DDoS pueden provocar la saturación de equipos y enlaces intermedios que perjudica a los usuarios. DDoS es muy difícil de filtrar sin agravar el problema.
- Ataques a los protocolos de enrutamiento interior y exterior. Si el protocolo de enrutamiento exterior (BGP) se cae, la red se vuelve inalcanzable. Esto se produce por que BGP corre sobre TCP y este último tiene sus propios problemas de seguridad.
- Ataques al DNS, que es utilizado por todas las aplicaciones y si no funciona causa muchos problemas.
- Ataques internos; es decir, los equipos de la red por parte de personal no autorizado.

A continuación se presentan posibles soluciones para seguridad de un ISP:

- Soluciones para seguridad en protocolos de enrutamiento interior:
 - Integridad del dominio de enrutamiento.
 - Correcta configuración en los interfaces correspondientes.
 - Autenticación con Código Hash.
 - Anillo antispoofing.
- Soluciones para seguridad en protocolos de enrutamiento exterior:
 - Incorporar mecanismos que revisen el campo TTL de los mensajes involucrados (RFC 3682).
 - Protección de sesiones BGP mediante Shared Key y MD5 (RFC 2385).
 - Filtrado de número de sistema autónomo (AS, Autonomous System) por prefijo.
- Soluciones para seguridad en DNS:
 - DNSSEC
 - ✓ Split DNS, que sirve para controlar las entradas al servidor.
 - ✓ Especializar las tareas de los servidores DNS.

- ✓ Protección de mensajes “Query Response” mediante firma de registros en una zona posterior y verificación de la firma por parte de quien la recibe.
- ✓ Implementar nuevos registros como RRSIG, DNSKEY, NSEC y DS.
- TSIG
 - ✓ Autenticación del origen e integridad de los mensajes.
 - ✓ Clave secreta compartida.
 - ✓ Código Hash.
- Envenenamiento del caché del DNS.
 - ✓ Limitación de acceso a la información y mecanismos de control.
 - ✓ Lista de acceso a los ruteadores y conmutadores.
 - ✓ Plan de soporte técnico para Linux que incluye visitas preventivas.

Una vez terminada la parte de selección de equipos, software y soluciones para el área de seguridad basta realizar el análisis económico del mismo y ver su factibilidad de implementación. El siguiente capítulo abarcara en general los aspectos económicos de este proyecto.

CAPÍTULO 4

ESTUDIO DE LA DEMANDA Y COSTOS DE IMPLEMENTACIÓN

En este capítulo se realiza un análisis económico de la futura implementación del ISP que se está diseñando en el presente proyecto, como se planteó en los objetivos. Con el fin de establecer el factor costo beneficio y en qué porcentaje la inversión resultará rentable o no. Se realizará el cálculo de la tasa interna de retorno, y se plantea el cálculo del valor actual neto. Una vez obtenidos los costos se determinará el punto de equilibrio de la inversión en base a las ecuaciones de costos e ingresos.

4.1 ANÁLISIS DE COSTOS

Aunque el aspecto técnico es importante a la hora de diseñar, no es suficiente para que la posible inversión tenga éxito, por esta razón es necesario una planificación adecuada.

Se trata a continuación factores importantes como son el estudio de mercado y el análisis de costo – beneficio.

4.1.1 ESTUDIO DE MERCADO

Para el diseño de la red es necesario tomar en cuenta el dimensionamiento del mercado que consiste en investigar su tamaño potencial dentro de las áreas de operación y de esta manera conocer la demanda existente.

En el Capítulo 2 se hizo una introducción de la forma como el Internet ha penetrado en el mercado ecuatoriano, de esos datos obtenidos se hizo el dimensionamiento del actual proyecto.

Las estadísticas de penetración del Internet en América Latina darán una visión más cercana de la penetración existente en el Ecuador.

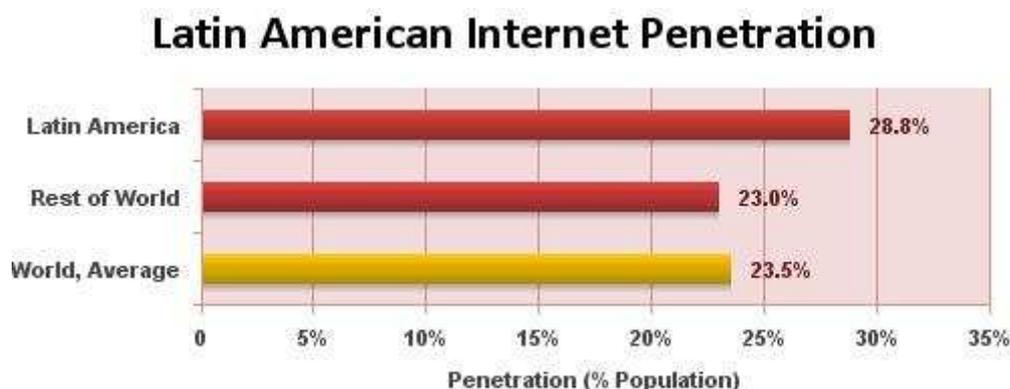


Figura 4.1: Penetración Internet América Latina [61]

Como se observa en la Figura 4.1, América Latina tiene un buen porcentaje de penetración a nivel mundial, un 28.8% comparada con el resto del mundo, que tiene un 23.0%. Esto indica que hay una demanda que va en aumento en América latina. Pero hay que establecer cuanto de este 28.8 % es el índice de penetración que pertenece al Ecuador.

Para este fin, la Tabla 4.1 muestra el índice de penetración correspondiente al Ecuador y se compara además con otros países que pertenecen al grupo andino.

Uso del Internet en Ecuador				
País	Población (datos 2007)	Usuarios Internet	Penetración (%)	Crecimiento (2000-2007)
Bolivia	9,775,246	1,000,000	10.2 %	733.3 %
Colombia	43,677,372	19,792,718	45.3 %	2,154.3 %
Ecuador	14,573,101	1,759,472	12.1 %	877.5 %
Perú	29,546,963	7,636,400	25.8 %	205.5 %
Venezuela	26,814,843	7,552,570	28.2 %	695.0 %

Tabla 4.1 Índice penetración Ecuador [61]

En la Tabla anterior se puede observar que el índice de penetración en el Ecuador es del 12.1%; además, en los últimos años el crecimiento de usuarios de Internet

ha ido aumentando y la principal concentración está en las ciudades grandes como Quito y Guayaquil.

De estos datos se puede concluir que el mercado existente está en constante crecimiento lo que justifica la implementación del presente proyecto.

4.1.2 ANÁLISIS COSTO – BENEFICIO

Para la posible implementación del proyecto es necesario identificar el capital necesario para la posible inversión. Para este fin se requiere de una adecuada información de costos.

Los precios del equipamiento, tanto de hardware así como de software, son referenciales y son susceptibles a variaciones debido a tiempo y cambio de tecnología.

4.1.2.1 Costos de la implementación inicial

4.1.2.1.1 Servidores

En la Tabla 4.2 se detallan aspectos importantes, así como características de la granja de servidores que se utilizan para el ISP.

EQUIPO	PRECIO UNITARIO
DNS1 y DNS2	
PC, Procesador Intel Dual Core E4600 2.4 GHZ, bus 800 MHZ, Motherboard Intel, DDR2 667 2GB, RAM, Cache 2MB L2 cache, Disco Duro 250 GB, RED 10/100/1000	\$ 915
Correo	
PC, Procesador Intel Dual Core E4600 2.4 GHZ, bus 800 MHZ, Motherboard Intel, DDR2 667 2GB, RAM, Cache 2MB L2 cache, Disco Duro 250 GB, RED 10/100/1000	\$ 915

FTP y Web	
PC, Procesador Intel Dual Core E4600 2.4 GHZ, bus 800 MHZ, Motherboard Intel, DDR2 667 2GB, RAM, Cache 2MB L2 cache, Disco Duro 250 GB, RED 10/100/1000	\$ 915
Cache	
PC, Procesador Intel Dual Core E4600 2.4 GHZ, bus 800 MHZ, Motherboard Intel, DDR2 667 2GB, RAM, Cache 2MB L2 cache, Disco Duro 250 GB, RED 10/100/1000	\$ 915
Administración	
PC, Procesador Intel Dual Core E4600 2.4 GHZ, bus 800 MHZ, Motherboard Intel, DDR2 667 2GB, RAM, Cache 2MB L2 cache, Disco Duro 250 GB, RED 10/100/1000	\$ 915
TOTAL	\$ 4575

Tabla 4.2 Costos de equipos para la granja de servidores

Los dispositivos detallados anteriormente en la Tabla 4.2 son los necesarios para la implementación del ISP, pero hay que tomar en cuenta que para proyecciones futuras se podría ofrecer mayores servicios e incluso un aumento en el número de clientes, por lo que habría que prever las características de ciertos equipos.

Por ejemplo, el servicio de VoIP, que anteriormente necesitaba equipos adicionales para su implementación, en la actualidad, equipos grandes como ruteadores que tienen ciertas características que permiten implementar este tipo de servicios sin necesidad de algún equipo adicional.

4.1.2.1.2 Equipamiento adicional

En la Tabla 4.3 se observa los distintos equipos que se necesitan adicionalmente a los servidores. Se cuenta con el ruteador principal, que es llamado ruteador de frontera o de borde, y además se tiene equipos como el DSLAM y también el conmutador principal.

EQUIPO	PRECIO UNITARIO
RUTEADOR PRINCIPAL	
Ruteador Cisco 1841	\$ 1.395
DSLAM	
SmartAX MA5603 + 64ADSL2+	\$ 6.301
CONMUTADOR	
Cisco Catalyst Express 500-24TT	\$ 795
TOTAL	\$ 8.491

Tabla 4.3 Equipamiento adicional para ISP

4.1.2.1.3 Costo inicial del equipamiento del ISP

En la Tabla 4.5 se estima el costo inicial que demandaría el equipamiento total del ISP.

COSTO INICIAL DEL EQUIPAMIENTO	
EQUIPAMIENTO	COSTO (USD)
Granja de Servidores	\$ 4.575
Equipamiento adicional	\$ 8.491
Subtotal	\$ 13.066
12 % IVA	\$ 2.817,552
Total	\$ 14.633,92

Tabla 4.5 Costo inicial ISP

Adicional a los costos de los equipos hay que tomar en cuenta aspectos como son costos de publicidad, costos de administración, y permisos de funcionamiento. Los costos de publicidad son una necesidad, son una inversión necesaria, de esta manera se maneja un abastecimiento de nuevos clientes para dar a conocer los beneficios y servicios que se ofrece.

A su vez, el costo del permiso de funcionamiento es un gasto que se realiza por una sola vez, para un cierto periodo de tiempo

En la Tabla 4.6 se detallan los costos relacionados con lo citado anteriormente

DESCRIPCIÓN	PRECIO TOTAL [USD]
Publicidad	\$ 2 000
Permiso por 10 años de funcionamiento como ISP (SENATEL)	\$ 500
Total	\$ 2 500

Tabla 4.6 Tabla de costos de Publicidad y Permisos

4.1.2.1.4 Costo de la Implementación inicial del ISP

IMPLEMENTACIÓN INICIAL DEL ISP	
Costo inicial del Equipamiento	\$ 14.633,92
Costo de Publicidad y Permisos	\$ 2 500
Total	\$ 17.133,92

Tabla 4.7 Tabla de costo de la Implementación Inicial

4.1.2.2 Costos anuales del ISP

Todos los costos analizados para el ISP incluyen el 12% de IVA

4.1.2.2.1 Acceso a Internet

Para el cálculo de este costo se debe recurrir a los datos obtenidos en el Capítulo 2 acerca del ancho de banda del total de clientes dedicados.

AÑO	Total de clientes	Ancho de banda total
Primero	28	1069
Segundo	124	4756
Tercero	335	12872
Cuarto	885	33995

Tabla 4.8 Ancho de Banda total

Para facilidad de los cálculos se redondearan los valores para hacer relaciones con E1s, así la tabla quedaría:

AÑO	Total de clientes	Ancho de banda total
Primero	28	1024
Segundo	124	5120
Tercero	335	13312
Cuarto	885	33792

Tabla 4.9 Ancho de Banda total

La Tabla 4.10 muestra el costo anual del ancho de banda de acuerdo a los precios entregados por Telconet sabiendo que el valor de 1E1 es de 3.570 dólares, así el costo de cada Kb sería 3,49 dólares.

AÑO	Total de clientes	Ancho de banda total	E1	E1 a contratar	Factor de descuento por volumen	Valor Ancho de banda
Primero	28	1024	1	1	4%	41.126,4
Segundo	124	5120	5	4	6%	161.078,4
Tercero	335	13312	13	8	8%	315.302,4
Cuarto	885	33792	33	20	10%	771.120,0

Tabla 4.10 Costo Anual Ancho de Banda

4.1.2.2.2 Sueldos y Salarios

A continuación la Tabla 4.11 muestra los costos que se presentaran por conceptos del personal que se requerirá en el ISP.

PERSONAL DEL ISP				
No EMPLEADOS	CARGO	SUELDO MENSUAL	TOTAL MENSUAL	TOTAL ANUAL
1	Gerente	1000	1000	12000
1	Ingeniero en Telecomunicaciones	700	700	8400
1	Ingeniero Con Certificación LPI	600	600	7200
1	Contador	500	500	6000
1	Secretaria	400	400	4800
2	Técnicos	350	700	8400
1	Conserje y Mensajero	300	300	3600
TOTAL				50.400

Tabla 4.11 Tabla de Sueldos y Salarios Anual

4.1.2.2.3 Servicios básicos

La Tabla 4.12 muestra los costos que se generarán aproximadamente por conceptos de servicios básicos necesitados en las oficinas del ISP.

COSTOS POR SERVICIOS BÁSICOS		
SERVICIOS	COSTO MENSUAL	COSTO ANUAL
Arriendo Local	500	6.000
Luz	30	360
Teléfono	20	240
Agua	10	120
Útiles de Oficina	15	180
TOTAL (USD)		6.900

Tabla 4.12 Tabla de costos de Servicios Básico Anual

4.1.2.2.4 Costos última milla

El costo de la última milla depende de los valores propuestos por la empresa EQUYSUM de acuerdo a la Tabla 4.13

Año	Ultima Milla	Usuarios	Totales
Primero	20	28	6.720
Segundo	20	124	29.760
Tercero	20	335	80.400
Cuarto	20	885	212.400

Tabla 4.13 Tabla de costos para Ultima Milla Anual

4.1.2.3 Equipos

Básicamente quien genera costos de equipos son los módems que se deben instalar en cada uno de los usuarios.

4.1.2.3.1 Módems

El costo de los Módems que se utilizarán por los posibles clientes del ISP está reflejado en la Tabla 4.14.

COSTO DE MÓDEMS						
Año	No de Clientes	No Equipos requeridos	Costo unitario	Costo Anual	Descuento Corporativo	TOTAL ANUAL
Primero	28	28	45	1.260	10%	1.134
Segundo	124	96	45	4.320	10%	3.888
Tercero	335	211	45	9.495	10%	8.545,5
Cuarto	885	550	45	24.750	10%	22.275

Tabla 4.14 Tabla de costos de Módems Anual

Finalmente la Tabla 4.15 presenta el total de egresos que podría tener el ISP.

Año	Acceso a Internet	Sueldos y salarios	Servicios básicos	Costo anual por ultima milla	Módems	TOTAL
Primero	41.126,4	54000	6.900	6.720	1.134	109.880,4
Segundo	161.078,4	54000	6.900	29.760	3.888	255.626,4
Tercero	315.302,4	54000	6.900	80.400	8.545,5	465.147,9
Cuarto	771.120	54000	6.900	212.400	22.275	1'066.695

Tabla 4.15 Tabla de Egresos del ISP Anual

4.1.2.4 Ingresos del ISP

Para calcular los ingresos del ISP se debe tomar un valor fijo mensual según el enlace que se desea contratar y un valor fijo por costo de instalación que paga una sola vez cada usuario.

El precio por cada Kb de ancho de banda que le cuesta a la empresa es 3,49 obtenido del valor total del E1 que cobra Telconet a este valor se lo multiplica 4 veces para así tener una ganancia; entonces, se tiene 0,8725. A este valor se le suma la ganancia que desea tener la empresa del 30%, así se tiene el valor de Kb multiplexado que es 1,13425 y el valor de cada Kb sin multiplexar sería 4,537. Este valor es el que la empresa debe cobrar por cada Kb.

Se debe sumar el costo calculado en las instalaciones debido a que no se lo saco mensualmente sino anualmente.

Para calcular el valor de ingreso se toma como base enlaces de 128Kbps y el valor multiplexado, y un costo de instalación que se cobra solo una vez al año.

INGRESOS DEL ISP				
AÑO	NÚMERO DE CLIENTES	PRECIO MENSUAL (USD)	COSTO INSTALACIÓN (USD)	INGRESO ANUAL
Primero	28	165,18	100	55.600,48
Segundo	96	165,18	100	190.387,36
Tercero	211	165,18	100	418.335,76
Cuarto	550	165,18	100	1'090.288

Tabla 4.16 Tabla de ingresos del ISP anual

4.1.2.5 Total de ingresos y egresos del ISP

El costo de la implementación inicial del ISP está sujeto a variaciones, por ejemplo depende de la variación de precios que se tenga al momento de la

implementación. Además, pueden existir elementos adicionales que no se han tomado en cuenta y que luego pudieran aparecer; por lo tanto, un incremento del 20% de la inversión inicial cubriría estos imprevistos.

La inversión inicial es entonces: $17.133,92 \times 1.2 = 20560,704$

AÑO	INVERSIÓN INICIAL	TOTAL INGRESOS ISP	TOTAL EGRESOS ISP
Inicio	20.560,704		
Primero		55600,48	109.880,4
Segundo		190387,36	255.626,4
Tercero		418335,76	465.147,9
Cuarto		1.090.288	1.066.695

Tabla 4.17 Tabla de Ingresos y egresos

4.1.3 EVALUACIÓN DEL PROYECTO [62]

En el desarrollo de este proyecto se ha visto la factibilidad técnica para implementarlo, pero la evaluación económica es también importante, para esto se ha buscado analizar los distintos factores que influyen en la realización de este proyecto.

4.1.3.1 Flujo neto

El flujo neto se lo considera como la utilidad que recibe la empresa por concepto de rendimiento, de instalación, ahorro de costo del servicio, entre los principales.

Aunque no es un esquema de presentación sistemática de los ingresos y egresos, estos se obtienen de los diferentes estudios que se realizan al formular un proyecto. El flujo neto funciona como una síntesis de todos los estudios realizados

en lo referente a ingresos y el entregar los servicios, así como los respectivos costos que genera la inversión.

A continuación se presenta la Tabla 4.18 con los flujos netos calculados a partir de los diferentes análisis que se ha hecho hasta el momento

AÑO	TOTAL INGRESOS ISP	TOTAL EGRESOS ISP	FLUJO NETO
Inicio		20.560,704	- 20.560,704
Primero	55600,48	109.880,4	-54279,92
Segundo	190387,36	255.626,4	-65239,04
Tercero	418335,76	465.147,9	-46812,14
Cuarto	1090288	1.066.695	23593

Tabla 4.18 Tabla de Flujo neto

4.1.4 INDICADORES DE RENTABILIDAD

Para poder evaluar si un proyecto es rentable realizarlo o no, hay que establecer Métodos de análisis económicos del proyecto.

Los métodos más comunes para el análisis costo beneficio incluyen los siguientes indicadores de rentabilidad:

- Tiempo de recuperación de la inversión.
- Valor presente neto.
- Tasa interna de retorno

4.1.4.1 Tiempo De Recuperación De La Inversión

El objetivo de este análisis es determinar en cuanto tiempo se recupera la inversión inicial. Para este fin se necesita datos de variables como el flujo neto y el tiempo en que se espera la recuperación.

4.1.4.2 Valor actual neto

El valor actual neto en una inversión se lo calcula a partir de una tasa de interés y una serie de pagos futuros e ingresos. Se suele utilizar para determinar cuan rentable es un proyecto o no. El objetivo es obtener un VAN mayor que cero en cuyo caso cualquier inversión es rentable.

Los criterios para establecer si un proyecto es rentable o no se presentan a continuación.

VAN > 0	Proyecto aceptado
VAN = 0	El proyecto es indiferente
VAN < 0	El proyecto debe ser rechazado

Para el cálculo del VAN se utiliza una tasa de rendimiento activa promedio de 10.6 %, según datos del Banco Central, con una vida útil de 4 años y el flujo neto de valores obtenidos en tablas anteriores.

$$VAN = -I_0 + \sum_{i=1}^4 \left[\frac{FlujoNeto_i}{(1+r)^i} \right]$$

$$VAN = -20.560,704 + \sum_{i=1}^4 \left[\frac{FN_i}{(1+0,10)^i} \right]$$

Donde:

I_0 = Inversión inicial.

FN = Flujo Neto

I = Vida útil

r = Tasa de interés.

$$VAN = 129.889,97$$

De los resultados se puede concluir que el proyecto es rentable, porque el VAN es mayor a cero.

4.1.4.3 Tasa interna de retorno, TIR

La tasa interna de retorno equivale a la tasa de interés producida por un proyecto de inversión con pagos e ingresos que ocurren en periodos regulares. La TIR es aquella tasa que hace que el valor actual neto sea igual a cero.

Cuando la TIR es mayor que la tasa de interés, el rendimiento que obtendría el inversionista realizando la inversión es mayor que el que obtendría en la mejor inversión alternativa, por lo tanto, conviene realizar la inversión.

Si la TIR es menor que la tasa de interés, el proyecto debe rechazarse.

Cuando la TIR es igual a la tasa de interés, el inversionista es indiferente entre realizar la inversión o no.

TIR > i => realizar el proyecto

TIR < i => no realizar el proyecto

TIR = i => el inversionista es indiferente entre realizar el proyecto o no.

La tasa interna de retorno de los flujos de caja debe ocurrir en intervalos regulares tales como meses, semestres o años.

$$0 = -I_0 + \sum_{i=1}^4 \left[\frac{\text{FlujoNeto}_i}{(1+r)^i} \right]$$

$$0 = -20.560,704 + \sum_{i=1}^4 \left[\frac{FN_i}{(1+0,10)^i} \right]$$

Donde:

Io = Inversión inicial

FN= Flujo Neto

I = vida útil.

TIR = 16.8 %

Este valor es la máxima tasa de retorno que este proyecto proporciona; es decir, no se puede lograr una mayor rentabilidad a esa. Tomando en cuenta estándares empresariales, un proyecto puede ser realizable si se tiene un TIR mínimo de 5%.

Realizando los cálculos financieros expuestos anteriormente, se puede concluir que la implementación del proyecto planteado es realizable.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

De los resultados de este proyecto es posible obtener las conclusiones siguientes:

- El diseño de una red, en general, es algo que no se debe tomar a la ligera, ya que podría acarrear a futuro muchos problemas al administrador de la misma o peor aun problemas con los usuarios que mostraran inconformidad con el servicio prestado. Así podemos concluir que un proyecto debería tener un estudio exhaustivo de la tecnología a implementarse y de todo lo que conllevaría dicho diseño.
- De algunos análisis expuestos en el presente proyecto se puede concluir que aunque el índice de penetración de usuarios de Internet en el Ecuador no es tan alto, el mercado de empresas prestadoras de servicio se está saturando lo que implica que debe haber un mayor control en cuanto a la obtención de los

títulos habilitantes, todo con el objetivo de mejorar la calidad de la prestación de este servicio.

- ADSL es una tecnología que está en evolución constantemente debido a que su costo/beneficio es alto y sobre esta tecnología se pueden implementar varios servicios, no solo el de Internet. Estos criterios positivos influyen en un diseño ya que así se toma conciencia de que los equipos a elegirse deben contemplar no solo soluciones presentes si no a futuro y procurar estar a la par con el avance tecnológico y prestar un servicio de calidad.
- ADSL Con respecto a otras tecnologías, como por ejemplo la de cable modem, es una tecnología de bajo costo de implementación, debido a que los costos del cable, equipos, etc., han disminuido con el pasar de los años en nuestro país y en el resto del mundo. Se puede concluir entonces que para empresas que desean prestar servicios de Internet, voz y video una alternativa real económica sería la tecnología ADSL.
- Existen varios mecanismos para incorporar Calidad de Servicio en un ISP, pero la forma más apropiada depende de la tecnología desplegada y las características particulares de cada proveedor. De aquí que resulta esencial un análisis de los servicios ofrecidos, el requerimiento de los usuarios y la infraestructura desplegada antes de elegir el mecanismo más adecuado para adaptarlos al comportamiento real de la red.
- La incorporación de mecanismos de Calidad de Servicio en un ISP promete grandes ventajas no solo para el proveedor servicios sino para el usuario final. Al proveedor le permite optimizar la utilización de los recursos de la red mediante la diferenciación del tráfico según el tipo de usuarios y/o aplicaciones, y no se requieren cambios drásticos en la infraestructura de la red ya desplegada o un incremento significativo del ancho de banda. En cuanto al usuario final, la Calidad de Servicio se refleja en mejores características de rendimiento de la red y un alto grado de satisfacción del cliente.

- El turismo es un factor muy importante para este proyecto, ya que particularmente en la población de Pto. Ayora de la Isla Sta. Cruz, Galápagos es un punto de gran afluencia de turistas que de uno u otro modo necesitan comunicarse con sus lugares de origen. Esto hace que la implementación de un ISP en el área sea llamativo para cualquier empresa. De esto se puede concluir que para un estudio de tal magnitud, no solo influyen factores técnicos, sino también el factor social que, en este caso, es de mucho valor y de gran impacto.
- En la actualidad hay diversos servicios que se pueden prestar a través de un ISP como: Internet, voz y datos. El uso de VoIP soluciona muchos problemas de comunicación de larga distancia con respecto al costo de la misma. En el área de estudio se realizan llamadas constantes hacia el exterior, es por esto que la red debe poder soportar este tipo de tráfico y dar prioridad al mismo. Anteriormente se ofrecía el servicio de VoIP como parte de los servicios de un ISP y teniendo un servidor dedicado al mismo. En la actualidad, este servicio lo implementa el usuario final según su criterio, pero debe estar al tanto que dicho servicio está soportado por la empresa proveedora de servicios con la que tiene un contrato.
- En este proyecto la tecnología ADSL tiene otro tipo de instalación de la que se conoce comúnmente utilizando la red existente de par de cobre de líneas telefónicas. Para este proyecto se utiliza como ultima milla par trenzado para ofrecer servicio de Internet y servicios adicionales de VoIP y datos, a diferencia de la red PSTN que está orientada a ofrecer servicio de voz. Así la implementación de la red ADSL es más simple de lo común y se requieren menos equipos. Se puede concluir por lo mismo que el presente proyecto está enfocado a prestar el servicio de Internet utilizando tecnología ADSL para con una menor complejidad que la red típica que utiliza ADSL. Este proyecto es un ejemplo viable de arquitectura e implementación, pero no debe ser tomado como un estricto modelo de diseño, sino como una guía para entender los

múltiples factores y elementos que involucran el funcionamiento y operación de un proveedor de servicios de Internet.

- En cuanto a servidores, se ha dispuesto que más de una aplicación sean cubiertas por un mismo equipo, aunque siempre es mejor repartir las tareas en distintos equipos para evitar que colapse el sistema. El diseño con un análisis previo puede funcionar sin problemas, así de esta manera se reducen gastos iniciales en la posible implementación.
- Al diseñar una red, es importante comenzar con una sólida topología, la misma que ayudará a entender y visualizar de mejor manera las características generales que se involucran en una red, como: el esquema de direccionamiento, la dirección del flujo de tráfico de las aplicaciones, posibles problemas por congestión, permisos de acceso a usuarios y aplicaciones, etc. Se concluye que con una buena topología resultará más fácil caracterizar y entender a las aplicaciones que van a estar “corriendo” sobre la red y de esta manera poder dimensionarla correctamente. Hay que tomar muy en cuenta que no existe un modelo fijo para la infraestructura de la red, la topología puede variar de acuerdo a las necesidades de la misma.
- Las aplicaciones en tiempo real, como VoIP, tienen diferentes características y requerimientos con respecto a las aplicaciones de datos. Las aplicaciones de voz toleran pequeñas variaciones en el retardo, las mismas que afectan directamente a la entrega de los paquetes. La pérdida de paquetes y el jitter degradan la calidad de las transmisiones de voz, por lo tanto se debe aplicar QoS para evitar que la calidad de la voz se degrade. De esta manera la QoS ha encontrado la manera de optimizar una red proporcionando los algoritmos eficazmente para asegurar la entrega de la información y permitir que una red funcione eficientemente. QoS es la habilidad de poder seleccionar varios tipos de tráfico y tratarlos a cada uno dependiendo de sus necesidades. Por lo tanto, para un correcto diseño con QoS se debe poner mucha atención a los requerimientos de capa 2: Diffserv cumple con estas características.

- En cualquier infraestructura de red el cortafuegos es una parte fundamental de la seguridad. Actualmente existen cortafuegos de hardware con protección completa que a pesar de su alto costo resultan indispensables. Sin embargo la solución ofrecida por sistemas que utilizan software libre es tentadora para empresas pequeñas y medianas. Se deben combinar varios mecanismos de seguridad a lo largo de la infraestructura de un ISP, en especial al tratarse de un ISP que es muy susceptible a ataques malintencionados. Se puede concluir que una buena seguridad es aquella que combina hardware y software.
- Es notable que Linux continúa emergiendo como una fuente, al parecer inagotable, de soluciones para networking que permite reducción de costos y acceso a servicios indispensables para datos y comunicaciones. Los desarrollos que han alcanzado los grupos de código abierto posibilitarán que en el futuro empresas pequeñas y medianas puedan acceder a soluciones de calidad, flexibles, seguras y económicas.
- Se ha logrado el diseño del proveedor de servicios de Internet, con equipos de bajo presupuesto para la puesta en funcionamiento de los servicios de correo, DNS, caché, administración, FTP, WEB, etc.; todo gracias al manejo en la actualidad de software libre, que ha demostrado ser muy estable para este tipo de aplicaciones y que reduce costos comparado con equipos que necesitan licencia para su funcionamiento, por lo mismo se recomienda, si es posible, la utilización de servidores que se basen en GNU/Linux.
- El crecimiento de un ISP no tiene parámetros definidos, ya que es difícil acoplar los diversos factores de los que este depende tales como: publicidad, marketing, costos, y calidad de servicio. Existen datos que permiten concluir que ISPs que entran al mercado en poco tiempo han logrado obtener gran número de clientes, mientras que otros no ha tenido tal demanda. Sin embargo cualquier proyecto nuevo debe tener visión y misiones claras para obtener el éxito.

- Desarrollado el Capítulo 4, se concluye que la inversión que se debería realizar para la implementación de ISP es retribuable a mediano plazo, es decir que el proyecto cumple con los requerimientos financieros para su puesta en marcha.
- La evaluación de proyectos se complementa con la planeación. La evaluación verifica y la planeación prevee, la evaluación se puede realizar utilizando criterios de costo-beneficio, costo-eficiencia y costo-mínimo, dependiendo de la información que se posee y la facilidad para estimar los beneficios; el flujo de fondos es una herramienta que ayuda a identificar ingresos y costos, para poder establecer las necesidades de recursos o ganancias en una unidad de tiempo. En este proyecto para identificar la mejor alternativa se utilizó el criterio de costo-beneficio, ya que la única información que se obtuvo para evaluar el proyecto fueron los costos. Para el método de evaluación se utilizó el identificar financiero VAN “Valor Actual Neto”, que consiste en identificar todas las entradas de dinero en un periodo determinado, llevarlos a tiempo presente, y la suma de todo es un valor positivo, otro criterio usado fue el TIR “Tasa Interna de Retorno”, que es una tasa promedio a la cual se recuperara la inversión en un periodo dado.
- El modelo del diseño, el plan a ejecutar y la implementación de la red deben proporcionar ingresos económicos que justifiquen la inversión. El modelo es el punto de partida, y siempre debe estar sujeto a revisión constante. Ningún modelo fijo es apropiado para ninguna empresa. En algunas organizaciones la información es el producto, por lo que se invierte más en una infraestructura de red. Por lo tanto la parte económica, juega un papel muy importante en el diseño, para poder lograr en lo posible el mejor servicio al costo más bajo. Un administrador o un diseñador de red, debe enfocarse principalmente en los componentes que causan el incremento o disminución del costo del diseño; estos componentes generalmente son ancho de banda, calidad de servicio garantizada, disponibilidad, seguridad y administración. Una parte estratégica dentro del proceso de diseño de una red es tratar de medir la ganancia que involucra realizar una inversión como esta. Generalmente las empresas usan

esta herramienta como un componente financiero para tomar la decisión adecuada y medir la actuación de la empresa en el mercado.

- La parte económica no es la única razón para que las empresas realicen inversiones en hacer converger las redes de voz y datos. Otros motivos para invertir en una red son las aplicaciones. La integración de redes facilita la creación de nuevas aplicaciones que integran voz y datos.

5.2 RECOMENDACIONES

De la experiencia obtenida durante la realización de este trabajo se pueden obtener las recomendaciones que siguen:

- Para el caso de este proyecto el cual fue implementado por la empresa EQUYSUM y mi persona se tomaron en cuenta algunos aspectos importantes que se escapan al diseño de la parte técnica y económica, y estos son: la capacitación del personal técnico indispensable para un mejor manejo de tecnologías y, una buena atención al cliente, de esta manera se logran mejorar las expectativas de incremento en el número de usuarios y por ende obtener mejores ingresos. Conseguir distribuidores de equipos que sean conocidos o mejor aun de confianza, con esto se logra minimizar los roces por causa de devoluciones o aplicaciones de garantías; un estudio a futuro de crecimiento de la infraestructura, para de esta manera si llegará a necesitarse la migración no sea tan desprevenida, finalmente la posible implementación de un segundo ISP en la Isla San Cristóbal en Pto. Baquerizo Moreno
- Es recomendable al momento de realizar los respectivos contratos con los clientes, el ser claros en cuanto a la capacidad de los enlaces que van a recibir, aunque en el diseño se estableció en su mayoría a clientes con enlaces uno a uno, por diversas circunstancias habrá la necesidad de compartir el enlace, lo que significará que el cliente tendrá una percepción de que su enlace se ha desmejorado. Este aspecto de compartición se lo toma con el objetivo primordial de recuperar la inversión vendiendo más de lo que

se compra, pero eso si no se debe exagerar en este aspecto o será reflejado con la inconformidad del servicio en los usuarios.

- Aunque el diseño del ISP trata de asegurar que no haya inconvenientes a la hora de la implementación, se deben seguir el diseño como una guía y no intentar forzar aspectos que tal vez al momento de la implementación no sean los más adecuados y se debe actuar de acuerdo al tipo de necesidad que se requiera.
- A pesar que la arquitectura de servicios diferenciados es menos compleja que otros mecanismos de calidad de servicio, es muy recomendable realizar un análisis del tráfico de la red para asignar prioridades en forma adecuada y de esta manera priorizar recursos para transmisión de tráfico del “mejor esfuerzo”.
- El uso de VoIP por los clientes es una gran posibilidad para buscar mercado en el aspecto de capacitación sobre este tema, es decir se está hablando de un mercado complementario y así mejorar los ingresos de la empresa.
- Al momento de realizar los papeleos a la hora obtener el título habilitante por parte de la SENATEL, hay que tomar en cuenta que el contrato que se hace no es por tiempo indefinido sino que hay que renovarlo cada cierto tiempo, así se evitarán problemas futuros de posibles multas innecesarias o de clausuras, temporales.
- Un factor importante a especificar en el diseño de una red es la capacidad del canal, definida como la cantidad de información que puede fluir a través de una conexión de red en un periodo de tiempo dado. Este factor es esencial para entender el concepto de ancho de banda, y poder aplicarlo cuando se esté dimensionando una red en especial. Los aspectos más importantes a tomar en cuenta son:

1. Tomar en consideración el medio que se está usando para la construcción de la red, ya que el ancho de banda es limitado por las leyes físicas (dependiendo del material) y por la tecnología usada para colocar la información en el medio.
 2. Para la adquisición de equipos, o para el alquiler de enlaces, una buena comprensión del ancho de banda puede ahorrar a una empresa una significativa cantidad de dinero. Un administrador de red necesita tomar las decisiones correctas sobre el tipo de equipos y servicios a comprar.
 3. A medida que se implementan nuevas tecnologías e infraestructuras de red para proporcionar un mayor ancho de banda, se pueden crear nuevas aplicaciones para aprovechar estas capacidades y dar varios beneficios y servicios a los usuarios. Sin embargo, es importante que un administrador de red considere que este factor no es gratuito; debe ser tomado muy en cuenta al diseñar y administrar la red para tratar de optimizarla lo mayormente posible, sin perder el desempeño normal de la misma, y que además se mantenga la capacidad requerida para la voz, ya que si esta se ve afectada por la carga de datos, o es disminuida por ahorro de costos, la calidad de la voz se va a perder notablemente.
- El conjunto o granja de servidores se ha diseñado en su mayoría utilizando PCs, con características de última tecnología, sin embargo si a futuro la infraestructura del ISP crece considerablemente sería muy conveniente migrar estos servidores PCs a servidores de marca para optimizar y sobre todo evitar posibles fallas producto del sobredimensionamiento que se dé a los equipos actuales.
 - Se recomienda la creación de una materia relacionada con la Telefonía IP, y las soluciones más adecuadas entre estas la implementación de una central Asterisk o Elastix; pues, esta tecnología tiene la tendencia a convertirse en una nueva revolución de las telecomunicaciones a nivel mundial y nuestro

país está adoptando este camino con mucha rapidez y es una muy buena solución empresarial.

- Finalmente se recomienda que se cree una materia que profundice el estudio de tecnologías utilizadas para dar el servicio de Internet como: ADSL, cable modem, Wi-MAX, etc. Y así lograr que los futuros ingenieros puedan aportar fácilmente con sus ideas en empresas que prestan este tipo de servicios, las cuales abarcan un gran porcentaje en el ámbito de las telecomunicaciones.

REFERENCIAS BIBLIOGRÁFICAS

-
- [¹] PAREDES, Rodrigo, “Documento: Diseño e implementación de experiencias docentes para un sitio proveedor de servicios internet”, Universidad de Chile, 2000. <http://www.dcc.uchile.cl/~raparede/publ/00memDIE.pdf>
- [²] PÉREZ DE LEMA, Andoni, “Documento: Infraestructura de un ISP”, Consulta: Junio, 2009. <http://greco.dit.upm.es/~david/tar/trabajos2002/10-infraestructura-isp- andoniperez-res.pdf>
- [³] Anónimo, “Proveedor de Servicios de Internet”, Consulta: Junio, 2009. http://www.zator.com/Internet/A7_1.htm
- [⁴] Anónimo, “Cómo seleccionar un ISP”, COPCA Consulta: Octubre, 2006. <http://www.39ymas.com/empresa/informacion/Seleccionar%20un%20ISP/>
- [⁵] Anónimo, “El Servicio FTP”, Agosto, 2003. <http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node218.html>
- [⁶] CHING, Aaron, “Utilizar SMTP para los mensajes salientes”, Diciembre, 2000. <http://www.microsoft.com/latam/technet/articulos/200110/art04/default.asp>
- [⁷] GARCÍA Jesús; RAYA José Luis y RAYA Víctor, “Alta velocidad y calidad de servicio en redes IP”, Edición RA-MA, Cáp.16-20, Madrid, España, 2002
- [⁸] AGUIRRE, Bruno, “Correo electrónico (e-mail)”, Mayo, 1999. <http://www.monografias.com/trabajos/email/email.shtml>
- [⁹] RAMOS, Johnny, “Documento: Latencia en Internet”, 2004. <http://www.linux.org.pe/Ind/PLUG-LND-Latencia-JRamos.pdf>
- [¹⁰] Anónimo, “Telnet”, Consulta: Junio, 2009. http://www.zator.com/Internet/A8_7.htm
- [¹¹] Anónimo, “Netline WebHosting”, Consulta: Junio, 2009. <http://carro.netline.cl/carro/site/faq/#1>
- [¹²] Anónimo, “Funcionamiento del Servicio de proxy-caché”, Universidad Autónoma de Madrid, Agosto, 2002. <http://www.uam.es/servicios/ti/servicios/proxy/faq.html>
- [¹³] Anónimo, “Servicio Proxy/Caché”, Universidad de Murcia, Consulta: Junio, 2009. <http://www.um.es/si/proxy/>

[14] Anónimo, “Chat (IRC)”, Consulta: Junio, 2009.
<http://www.esi2.us.es/~mbilbao/ap24.htm>

[15] SPHYNX, “Tutorial de Servicios de IRC-Hispano (I)”, 2004. <http://www.ayuda-internet.net/tutoriales/manu-irchispano/manu-irchispano.html>

[16] PIETROSEMOLI, Ermanno, “Documento: VoIP”, Consulta: Junio, 2009.
<http://www.wilac.net/descargas/documentos/11ri.pdf>

[17] SIENRA, Luis, “Voz Sobre Redes de Cable: Un Modelo para Implementar VoIP en su Sistema”, 2001. <http://www.cinit.org.mx/articulo.php?idArticulo=2>

[18] MASSA, Xavier, “Documento: VoIP, una realidad”, Marzo, 2005.
<http://www.coit.es/publicaciones/bit/bit149/24-27.pdf>

[19] Anónimo, “Video sobre redes”, Consulta: Junio, 2009.
<http://www.monografias.com/trabajos10/vire/vire.shtml>

[20] CHARRO, Francisco; ERAZO, Paulina, “Estudio y diseño de una red LAN híbrida utilizando las tecnologías WiMax y WiFi para brindar servicios de video sobre IP e Internet de banda ancha incluyendo transmisión de voz y 119 datos en la Universidad Central de Ecuador”, EPN, Quito, Ecuador, Julio 2006.

[21] GUANÍN, Francisco; GUERRERO, Héctor, “Determinación de parámetros que intervienen en la Calidad de Servicio prestado por Proveedores de Servicio de Internet (ISP) nacionales y análisis del ISP más conveniente en relación costos-beneficios para el cliente”, Director: Ing. Erwin Barriga, EPN, Quito, Ecuador, Noviembre, 2005.

[22] CAICEDO María; YÁNEZ, Hernando, “Planificación de un Proveedor de Servicios de Internet y Diseño de su Sistema de Seguridad”, EPN, Quito, Ecuador, 2002.

[23] TOSCANO, Miguel; GUIJARRO, René, “Estudio y Diseño de un ISP para la EPN y de la conectividad entre la EPN y un nodo principal de Backbone de Internet”, Carrera de Ingeniería en Electrónica y Telecomunicaciones, Escuela Politécnica Nacional, Quito, Ecuador, Febrero, 2004.

[24] León del Salto, Roberto Javier, “Estudio de la tecnología ADSL (Línea Digital Asimétrica de abonado) para su implementación en la estructura de la red de Andinatel SA en la ciudad de Quito”, EPN, Quito, Ecuador, 2002.

[25] Anónimo, “Medios guiados y no guiados”, *Consulta: Junio, 2009*
<http://www.scribd.com/doc/5705604/MEDIOS-GUIADOS>

[26] Anónimo, “Cables de Transmisión”, *Consulta: Junio, 2009*. https://www.u-cursos.cl/ingenieria/2008/2/EL41B/1/material_alumnos/objeto/25679

[27] Anónimo, “Medios de transmisión más utilizados” *Consulta: Junio, 2009.*
<http://www.monografias.com/trabajos22/redes-transmision/redes-transmision.shtml>

[28] Anónimo, “*Digital Subscriber Line*”, *Consulta: Junio, 2009.*
http://www.cisco.com/en/US/docs/internetworking/technology/handbook/DSL_Dig_Subscr_Ln.pdf

[29] Anónimo, “DSL Advances”, *Consulta: Junio, 2009.*
<http://books.google.com.ec/books?id=VWaMdlq2w8QC&lpg=PA102&ots=rQmYun u6PO&dq=hdsl%20csa%20range&pg=PA102#v=onepage&q=hdsl%20csa%20range&f=false>

[30] Anónimo, “Tecnologías de acceso de banda ancha y su integración con ATM”, *Consulta: Junio, 2009.* <http://www.monografias.com/trabajos14/acceso-atm/acceso-atm.shtml>

[31] Anónimo, “Fast Guide to DSL”, *Consulta: Junio, 2009.*
http://whatis.techtarget.com/definition/0,,sid9_gci213915,00.html#adsl

[32] Alcudia, Alejandro, “Modelado y simulación de transmisión de datos en un ADSL transceiver utilizando LabVIEW”, *Consulta: Junio, 2009.*
http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/alcudia_lad/portada.html

[33] Anónimo, “Digital Subscriber Line (xDSL)”, *Consulta: Junio, 2009.*
<http://www.xilinx.com/esp/wired/optical/collateral/DSL.pdf>

[33] CISCO SYSTEMS, “Redes de Gran Disponibilidad”, *Consulta: Octubre, 2009.*
<http://www.cisco.com/global/LA/microsites/isr/espanol/redes.shtml>

[34] INEC “Censos de población y vivienda”, *Consulta: Octubre 2009.*
http://www.inec.gov.ec/web/guest/ecu_est/est_soc/cen_pob_viv

[35] “Habitantes de galápagos quieren más del turismo”, *Consulta: Octubre 2009.*
<http://www.elsiglodetorreon.com.mx/noticia/651.habitantes-de-galapagos-quieren-mas-del-turis.html>

[36] GUANÍN, Francisco; GUERRERO, Héctor, “Determinación de parámetros que intervienen en la Calidad de Servicio prestado por Proveedores de Servicio de Internet (ISP) nacionales y análisis del ISP más conveniente en relación costos-

beneficios para el cliente”, Director: Ing. Erwin Barriga, EPN, Quito, Ecuador, Noviembre, 2006

[³⁷] SUPTEL, “Estadísticas de acceso a Internet”. <http://www.supertel.gov.ec/>

[³⁸] CONATEL “Estadísticas Servicio de Valor Agregado (SVA)”, Consulta: Octubre 2009.

http://www.conatel.gov.ec/site_conatel/index.php?view=article&catid=41%3Aestadisticas&id=176%3Aservicios-de-valor-agregado&option=com_content&Itemid=167

[³⁹] CAICEDO María; YÁNEZ, Hernando, “Planificación de un Proveedor de Servicios de Internet y Diseño de su Sistema de Seguridad”, EPN, Quito, Ecuador, 2002.

[⁴⁰] TELCONET, “Servicios para carriers e ISP”, Consulta: Octubre, 2009.

<http://www.telconet.net/espanol/productos/carriers.php>

[⁴¹] CISCO SYSTEM, “CCNA, Modulo 4”, Consulta: Octubre 2009.

<http://www.cisco.com/web/learning/netacad/index.html>

[⁴²] ROJAS, Franklin; VÁSQUEZ, Carlos, “Diseño de un proveedor de servicio de internet (ISP) con tecnología Frame Relay, integrando el servicio de voz sobre IP y análisis de factibilidad para su posible implementación”, EPN, Quito, Ecuador, 2008.

[⁴³] BRAVO, Christian; CALLE, José, “Diseño de un ISP, basado en la tecnología Broadband Power Line Communications, para la Empresa Eléctrica Quito S.A.”, EPN, Quito, Ecuador, 2006

[⁴⁴] RACINES, Paola, “Diseño de un ISP considerando criterios de calidad de servicio para la transmisión de voz, datos y video utilizando el estándar IEEE

802.16 (WiMax) para cubrir el área norte de la ciudad de Quito”, EPN, Quito, Ecuador, 2007

[⁴⁵] Jesús García Tomás; Alta velocidad y calidad de servicio en Redes IP; Editorial Alfaomega; México 2002.

[⁴⁶] GARCÍA, Jesús, “Alta velocidad y calidad de servicio en redes IP”, EPN, Quito, Ecuador, Julio 2002.

[⁴⁷] RACINES, Paola, “Diseño de un ISP considerando criterios de calidad de servicio para la transmisión de voz, datos y video utilizando el estándar IEEE 802.16 (WiMax) para cubrir el área norte de la ciudad de Quito”, EPN, Quito, Ecuador, 2007

[⁴⁸] CAICEDO María; YÁNEZ, Hernando, “Planificación de un Proveedor de Servicios de Internet y Diseño de su Sistema de Seguridad”, EPN, Quito, Ecuador, 2002.

[⁴⁹] CISCO SYSTEM, “CCNA, Modulo 4”, Consulta: Octubre 2009.
<http://www.cisco.com/web/learning/netacad/index.html>

[⁵⁰] <http://www.monografias.com/trabajos65/equipo-dslam-smartax/equipo-dslam-smartax2.shtml>

[⁵¹] MONTOYA, Manuel, “15 mitos sobre GNU/Linux”, Octubre, 2009.
http://www.ecualug.org/?q=2005/05/23/15_mitos_sobre_gnu_linux

[⁵²] DELL, “Guía de redes, servidores y almacenamiento”, Consulta: Octubre, 2009
http://www1.la.dell.com/content/topics/global.aspx/solutions/es/network_learning_ctr?sv&l=es&s=biz&~section=003

[⁵³] DONOSO, Marco, “Linux Alternativas de Software libre para la gestión empresarial”, CEC-EPN, Consulta: Octubre, 2009

[⁵⁴] CENTOS, “The Community ENTERprise Operating System”, Consulta: Octubre, 2009. <http://www.centos.org>

[⁵⁵] REDHAT, “An Overview of Red Hat Enterprise Linux 5”, Consulta: Octubre, 2009. <http://www.redhat.com/rhel/>

[⁵⁶] TIMME, Falko, “The Perfect Setup - CentOS 5.0 (32-bit)” , Octubre, 2009
http://www.howtoforge.com/perfect_setup_centos5.0

[⁵⁷] Anónimo, “Instalación de Servidores Linux”, Linux para todos, Octubre, 2009.
<http://www.linuxparatodos.net/portal/staticpages/index.php?page=instalacionservidores>

[⁵⁸] CISCO, “Products & Services”, Consulta: Octubre, 2009.
<http://www.cisco.com/en/US/products/index.html>

[⁵⁹] 3COM, “Welcome to 3com Corporation”, Consulta: Octubre, 2009.
<http://www.3com.com/>

[⁶⁰] D-LINK, “Productos & Solutions”, Consulta: Octubre 2009.
<http://www.dlink.com/products/category.asp>

[⁶¹] <http://www.internetworldstats.com/stats.htm>, datos Diciembre 2009.

[⁶²] TOSCANO Miguel, GUIJARRO René, “Estudio y Diseño de un ISP para la EPN y de la Conectividad entre la EPN y un Nodo Principal del Backbone de Internet” Quito, Ecuador Febrero 2004.