ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

PLANIFICACIÓN DE UN PROVEEDOR DE SERVICIOS DE INTERNET Y DISEÑO DE SU SISTEMA DE SEGURIDAD

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

MARÍA SOLEDAD CAICEDO JARAMILLO
FERNANDO ISAÍAS YÁNEZ ANDAGANA

DIRECTOR: ING. PABLO HIDALGO

QUITO, FEBRERO DE 2002

DECLARACIÓN

Nosotros, María Soledad Caicedo Jaramillo y Fernando Isaías Yánez Andagana, declaramos que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley, Reglamento de Propiedad Intelectual y por la normatividad institucional vigente.

María Soledad Caicedo J.

Fernando Isaías Yánez A.

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por la Srta. María Soledad Caicedo Jaramillo y el Sr. Fernando Isaías Yánez Andagana, bajo mi supervisión.

Ing. Pablo Hidalgo

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Nuestro más sincero agradecimiento a todas aquellas personas e instituciones que nos brindaron su apoyo para poder llevar a cabo este proyecto. Nuestro especial agradecimiento al Ing. Pablo Hidalgo por su acertada dirección y colaboración.

DEDICATORIA

A la persona que ha hecho posible la culminación de mis metas y sueños con gran entrega y dedicación: mi madre, para ella todo mi cariño.

María Soledad

4.4. Protección de la infraestructura del ISP. Problemas y soluciones 170
4.4.1. Seguridad de las plataformas de servicio (servidores)... 175
4.4.1.1. Seguridad del servidor *Web* 178
4.4.1.2. Seguridad del servidor de Nombres de Dominio (DNS) 185
4.4.1.3. Seguridad del servidor de Transferencia de Archivos (FTP) 186
4.4.1.4. Seguridad del servidor de Correo Electrónico 187
4.4.2. Seguridad de los *routers* 189
4.5. Protección del *software* del ISP. Problemas y soluciones 193
4.6. Protección de los datos 197
4.7. Políticas de seguridad del ISP 202
Bibliografía Capítulo IV **207**

CAPÍTULO V. SISTEMA DE TARIFACIÓN

5.1. Plan de negocios del ISP 208
5.2. Identificación de los costos del ISP 210
5.2.1. Costos referenciales de los equipos y enlaces que conforman el ISP 212
5.2.2. Perfil de costos del ISP 220
5.3. Estructuras y modelos de cálculo de tarifas 222
5.3.1. Parámetros que intervienen en la tarifación 222
5.3.1.1. Acceso 223
5.3.1.2. Tiempo 224
5.3.1.3. Volumen 225
5.3.1.4. Distancia 226
5.3.1.5. Calidad de servicio 227
5.3.2. Primer modelo de cálculo de tarifas basado en tiempo.. 227
5.3.2.1. Cálculo de los costos anuales para usuarios *dial-up* y corporativos 228
5.3.2.2. Cálculo de las tarifas basadas en tiempo 231

5.3.2.3. Análisis Beneficio/Costo 233
5.3.3. Segundo modelo de cálculo de tarifas basado en volumen 234
5.3.3.1. Cálculo de los costos por GB para usuarios *dial-up* y corporativos 234
5.3.3.2. Cálculo de las tarifas basadas en volumen 239
5.3.3.3. Análisis Beneficio/Costo 241
Bibliografía Capítulo V 242

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES 240

6.1. Conclusiones 243
6.2. Recomendaciones 246

ANEXOS

A. Cálculo de los retardos A-1
B. Características de equipos y *software* B-1
C. Proyecciones anuales de costos e ingresos del ISP C-1
D. Lista de Siglas D-1

REFERENCIAS BIBLIOGRÁFICAS R-1

RESUMEN

Internet se ha constituido en una herramienta indispensable en el ámbito tecnológico, de negocios, social y en el de las comunicaciones. Internet es un mercado en crecimiento en nuestro país y Quito es una de las ciudades que concentra mayor actividad económica y población del Ecuador lo que la convierte en un sitio estratégico para el desarrollo e implementación de un ISP, siendo el objetivo primordial diseñar un plan para el manejo y administración de las seguridades así como el diseño en sí de la infraestructura de la red de un ISP de mediano tamaño.

Capítulo I

En este capítulo se revisa la estructura jerárquica de los ISPs (*Internet Service Provider*; Proveedor de Servicios de Internet), la secuencia de conectividad entre ISPs y usuarios finales. Se analiza tanto la infraestructura interna de la red estudiando varias opciones de diseño, como los elementos que la conforman y los puntos de acceso o PoPs (*Points of Presence;* Puntos de Presencia), además, trata acerca de las formas cómo el cliente accede a la red del proveedor. Todos estos puntos en sí constituyen las herramientas que ayudarán a realizar un apropiado diseño de la infraestructura del ISP que será abordada en el capítulo III.

Capítulo II

Hace una revisión de los protocolos de enrutamiento interior que un ISP puede adoptar; en cuanto al protocolo de enrutamiento exterior, se analiza BGP (*Border Gateway Protocol*; Protocolo de Pasarela Fronterizo) y los varios ambientes de conexión del ISP. Esta información contribuirá a afirmar los conceptos y principios de los protocolos de enrutamiento, de manera que el administrador de red pueda diseñar e implementar estrategias de enrutamiento en la red del ISP. La segunda mitad de este capítulo, aborda los varios tipos de routers y su papel en la red del ISP, concluyendo con los entornos de enrutamiento.

Capítulo III

Este capítulo incluye aspectos involucrados en el diseño de la infraestructura de un ISP para la ciudad de Quito como son: proyección del número de usuarios, qué servicios se van a ofrecer a dichos usuarios, cálculo del número de líneas telefónicas, dimensionamiento de la capacidad de los servidores y tecnologías de acceso. Todos estos principios se trasladan dentro del diseño de ingeniería para la red del ISP, minimizando los costos operacionales a largo plazo y maximizando la capacidad de servicio. Finalmente, se analizan los diferentes mecanismos de QoS (*Quality of Service;* Calidad de servicio) para ofrecer servicios de mayor calidad a los usuarios e incrementar la eficacia de la red, estableciendo distintas clases de servicio.

Capítulo IV

Este capítulo cubre temas como son: técnicas de prevención, análisis y control de las vulnerabilidades relacionadas con la integridad y disponibilidad de los equipos que forman parte de la infraestructura de la red del ISP así como temas relacionados con la confidencialidad de los datos del usuario. Además trata acerca de las políticas de seguridad las misma que minimizan los riesgos, y la forma cómo establecer estrategias para responder y recuperarse ante posibles incidentes de seguridad. Todo esto para mejorar el nivel de seguridad de los clientes, de manera que la imagen de la empresa no se vea deteriorada ante los usuarios.

Capítulo V

Como la red del ISP debe estar operativa las 24 horas del día los 7 días de la semana, se necesitan equipos fiables que además permitan el crecimiento del ISP, esto es lo que trata parte del Capítulo V (características de los equipos utilizados). A partir del presupuesto referencial de dichos equipos, enlaces, costos por personal que tiene que invertir el ISP en su implementación, etc., se procede a realizar el cálculo de las tarifas mensuales tanto para usuarios *dial-up* como para usuarios corporativos basados en el sistema de tarifación por tiempo y por volumen.

Finalmente, en el capítulo VI se presentan conclusiones y recomendaciones del presente plan de proyecto.

PRESENTACIÓN

Este proyecto de titulación provee el material esencial para quienes deseen iniciar un ISP, para lo cual se ha incluido una serie de pasos útiles y métodos que pueden ayudar a la introducción de un nuevo Proveedor de Servicios de Internet en el mercado.

Este trabajo va dirigido a aquellos quienes operan un ISP o trabajan dentro de la industria del ISP. El material de este proyecto debe darles a conocer las oportunidades que tiene este negocio así como también las presiones que un ISP tiene que afrontar ahora y en el futuro. Para los administradores de un ISP, este proyecto pretende indicar porqué se debe combinar equilibradamente el aspecto tecnológico con el aspecto de negocios.

El desarrollo de este proyecto ha sido una experiencia de gran aprendizaje en la que se han documentado los puntos esenciales de la operación de un ISP, de esta manera se pueda comprender el porqué del rápido crecimiento del Internet y sus cambios constantes. Por tal razón este trabajo también va dirigido a todos quienes deseen comprender la naturaleza de dichos cambios, riesgos y oportunidades de este negocio: ingenieros en telecomunicaciones, ingenieros en redes, ingenieros en sistemas, estudiantes de ingeniería y público en general con conocimientos básicos de redes de información.

El empeño de este trabajo ha sido direccionado a entender el entorno de operación de un ISP adecuándolo a nuestro país, de manera que sea factible implementar en el Ecuador un ISP de éxito tanto para la empresa como para sus clientes.

1

DESCRIPCIÓN Y ESTRUCTURA FUNCIONAL DE UN ISP

3.5.5 Capacidad de disco del servidor *Caché*..... 125
3.5.6 Capacidad de disco del servidor FTP..... 126
3.5.7 Capacidad de disco del servidor DNS..... 126
3.5.8 Capacidad de disco del servidor de Tarifación y Facturación..... 127
3.6 Características técnicas de los equipos..... 127
3.6.1 Servidor *Web Caching*..... 127
3.6.2 Servidor Radius..... 129
3.6.3 Servidor de *Mail* y DNS..... 130
3.6.4 Servidor *Web Hosting* y FTP..... 131
3.6.5 Servidor de Tarifación y Facturación..... 132
3.6.6 Servidor de Administración..... 133
3.6.7 *Firewall* 133
3.6.8 *Router* de Acceso Corporativo..... 134
3.6.9 *Router* Principal..... 136
3.6.10 NAS..... 137
3.6.11 *Switch* 138
3.7 Selección de los protocolos de enrutamiento..... 139
3.8 Redundancia, simetría y equilibrado de carga de la red..... 142
3.9 Calidad de Servicio (QoS)..... 152
3.9.1 Medidas de calidad..... 153
3.9.2 Mecanismos para introducir QoS en Internet..... 155
3.9.2.1. Modelo de Servicios Integrados. 156
3.9.2.2. Moldelo de Servicios Diferenciados. 157
3.9.2.3. MPLS. 158
3.9.3 QoS de ATM..... 158
3.9.4 QoS de *Frame Relay* 159
Bibliografía Capítulo III..... **161**

CAPÍTULO IV. DISEÑO DEL SISTEMA DE SEGURIDADES DEL ISP

4.1. Introducción a la seguridad en Internet..... 163
4.2. Plan de seguridad del ISP..... 164
4.3. Naturaleza de los incidentes de seguridad..... 168

DEDICATORIA

La creación de este proyecto ha sido toda una experiencia y hay muchas personas a las que quiero dedicar este trabajo: mis padres, hermanos, cuñadas

DEDICATORIA

La creación de este proyecto ha sido toda una experiencia y hay muchas personas a las que quiero dedicar este trabajo: mis padres, hermanos, cuñadas, tíos, sobrinos y a mi compañera de tesis por su paciencia y comprensión. Gracias a todos los demás que han ayudado a hacer que este proyecto vea la luz.

Fernando

CONTENIDO

PLANIFICACIÓN DE UN PROVEEDOR DE SERVICIOS DE INTERNET Y DISEÑO DE SU SISTEMA DE SEGURIDAD

R. RESUMEN XIII
P. PRESENTACIÓN XVI

CAPÍTULO I. DESCRIPCIÓN Y ESTRUCTURA FUNCIONAL DE UN ISP

1.1. El Internet 1
1.1.1. TCP / IP 2
1.1.2. Organismos que gestionan el Internet 4
1.2. Definición de ISP 5
1.2.1. Estructura jerárquica de los ISPs 6
1.3. Arquitectura del ISP 9
1.3.1. Acceso a Internet 10
1.3.2. Red del ISP 10
1.3.2.1. Topologías de la Red del ISP 10
1.3.2.1.1. Topología en Estrella 11
1.3.2.1.2. Topología en Lazo 12
1.3.2.1.3. Topología en Malla 13
1.3.2.1.4. *Dial Backup* 13
1.3.2.2. Elementos de la Red del ISP 14
1.3.2.3. Puntos de Presencia (PoPs) 15
1.3.3. Red de Acceso al Cliente 17
1.3.3.1. Cliente Corporativo 17
1.3.3.1.1. Cliente *single-homed* 19
1.3.3.1.2. Cliente multiconectado 19
1.3.3.1.3. Cliente *multi-homed* 20
1.3.3.2. Cliente *dial-up* 21
1.4. Tipos de ISPs 24

1.4.1. El ISP local o ISP de acceso 25
1.4.1.1. Oficinas Locales 26
1.4.1.2. Oficina Central 26
1.4.2. El ISP Regional 27
1.4.2.1. Oficinas Regionales y Locales 28
1.4.3. El ISP Nacional e Internacional 29
1.4.3.1. El ISP Integrado 30
1.4.3.2. El ISP de Acceso *Outsourced* 30
1.4.3.3. El ISP Multimodo 31
Bibliografía Capítulo I 32

CAPÍTULO II. PROTOCOLOS DE ENRUTAMIENTO EN UN ISP

2.1. Introducción 33
2.2. Estudio de los Protocolos de Enrutamiento 38
2.2.1. Función de los Protocolos de Enrutamiento 38
2.2.2. Protocolos de Enrutamiento Interior 39
2.2.2.1. RIP 40
2.2.2.2. RIP v2 43
2.2.2.3. IGRP 45
2.2.2.4. EIGRP 51
2.2.2.5. OSPF 56
2.2.3. Protocolos de Enrutamiento Exterior 63
2.2.3.1. BGP-4 63
2.3. Descripciones generales de un *router* 71
2.4. *Routers* del ISP 74
2.4.1. *Router* propiedad del cliente 74
2.4.2. Servidor de Acceso de Red (NAS) 75
2.4.3. *Router* de Acceso del Cliente 77
2.4.4. *Router* principal (*Core Router*) 78
2.5. Entornos de enrutamiento 79
2.5.1. Enrutamiento al Cliente 79
2.5.2. Enrutamiento Interior 83

2.5.3. Enrutamiento Exterior..... 83
Bibliografía Capítulo II..... 85

CAPÍTULO III. PLANIFICACIÓN Y DIMENSIONAMIENTO DEL ISP

3.1. Atributos que debe cumplir un ISP..... 87
3.2. Identificación de los objetivos del ISP..... 89
3.2.1. Viabilidad de mercado en la ciudad de Quito..... 89
3.2.2. Proyección de usuarios *dial-up* y corporativos..... 92
3.2.2.1. Proyección de usuarios *dial-up*..... 92
3.2.2.2. Proyección de usuarios corporativos..... 93
3.2.3. Planificación de los servicios que se ofrecerán a los usuarios del ISP..... 95
3.3. Conectividad hacia el cliente..... 105
3.3.1. Tecnologías de acceso..... 105
3.3.1.1. Conexiones de línea telefónica..... 105
3.3.1.2. Líneas arrendadas..... 105
3.3.1.3. RDSI..... 106
3.3.1.4. XDSL..... 107
3.3.1.5. *Frame Relay*..... 108
3.3.1.6. ATM..... 109
3.3.1.7. Modems-Cable..... 111
3.3.2. Dimensionamiento del número de líneas telefónicas para usuarios *dial-up*..... 111
3.4. Conectividad a Internet..... 114
3.4.1. Dimensionamiento del ancho de banda satelital..... 114
3.4.2. Cálculo de los retardos en la descarga de páginas *Web* 117
3.4.3. Interacción con otros ISPs..... 118
3.4.3.1 NAP de las Américas..... 121
3.4.3.2 NAP Ecuador..... 121
3.5 Dimensionamiento de la capacidad de los servidores..... 122
3.5.3 Capacidad de disco del servidor de *Mail*..... 123
3.5.4 Capacidad de disco del servidor de *Web Hosting*.... 124

CAPÍTULO 1

DESCRIPCIÓN Y ESTRUCTURA FUNCIONAL DE UN ISP

1.1. EL INTERNET

Internet es un conjunto de miles de redes interconectadas que se comunican entre sí utilizando el *stack* de protocolos TCP/IP (*Transmission Control Protocol / Internet Protocol*; Protocolo de Control de Transmisión / Protocolo Internet). Los protocolos TCP/IP son las normas que posibilitan la interconexión de ordenadores de diferentes fabricantes utilizando todo tipo de tecnología (Ethernet, líneas telefónicas conmutadas o dedicadas, *Frame Relay*, etc). Estas redes son muy diferentes, tanto en el número y en el tipo de máquinas conectadas así como en los sistemas operativos soportados.

Hoy en día, los servicios más usados en Internet son: Correo Electrónico, *World Wide Web,* FTP (*File Transfer Prrotocol;* Protocolo de Transferencia de Archivos), Grupos de Noticias, IRC (*Internet Relay Chat*), Servicios de voz, etc.

Internet funciona con el modelo ***"cliente/servidor",*** lo que significa que en esta red hay ordenadores servidores que dan una información concreta en el momento que se solicite, y por otro lado están los ordenadores que piden dicha información, los cuales representan los clientes de la red.

En el mundo de hoy, cada vez más, la información constituye la base de la riqueza y del poder, constituyéndose no sólo una revolución desde el punto de vista tecnológico, sino que también representa una revolución social que está cambiando las mentalidades aumentando las posibilidades de desarrollo de los individuos y de los pueblos.

1.1.1. TCP / IP

Cuando un ordenador quiere enviar a otro un fichero de datos, lo primero que hace es segmentar en paquetes pequeños y posteriormente enviar cada paquete de forma independiente; cada paquete elige el camino dependiendo de factores tales como saturación de las rutas o posibles congestiones. Cada paquete de información contiene la dirección del ordenador de destino, y la dirección del remitente, por si hay que recibir respuesta. Los equipos que conectan las diferentes redes que deciden por donde es mejor enviar un paquete según el destino, son los *routers* o direccionadores que se revisarán en el Capítulo II.

Como TCP/IP funciona en base a paquetes, siempre queda abierta la posibilidad de volver a solicitar el paquete perdido, y completar la información sin necesidad de volver a transferir todo el conjunto de datos.

La familia de protocolos TCP/IP está formada por más de 100 normas o protocolos que no dependen de ningún fabricante y son estándar. Cada uno de los protocolos se especializa en dar una solución a algún aspecto específico en la comunicación de datos entre equipos informáticos diversos, a través de medios diversos y con fines diversos. Así por ejemplo, existen protocolos que definen la forma de funcionar aplicaciones concretas como correo electrónico (SMTP; *Simple Mail Transfer Protocol*; Protocolo de Transferencias de *E-mail*), FTP.

Los dos protocolos más importantes son los que dan nombre a toda la familia: IP y TCP, los mismos que a continuación se revisarán sin ahondar en estos tópicos.

El protocolo IP.- No tiene en cuenta la fiabilidad de los datos, su ordenación, ni otras necesidades de las redes. Simplemente proporciona un esquema de direccionamiento y un mecanismo para fragmentar paquetes y transmitirlos a lo largo de redes que permitan tamaños de trama muy reducidos. Además IP es un protocolo no orientado a la conexión, es decir no intercambia información de control para establecer una conexión extremo a extremo antes de transmitir los datos.

El protocolo IP incluye información en cada paquete, para que los dispositivos (Ej. *routers*) puedan seleccionar la ruta que deberán seguir los datos, donde cada paquete de información se procesa por separado. Es posible que además se incluya con los datos alguna otra información útil, como información de seguridad y marcas temporales. Ej. TTL[a] (*Time to Live*; Tiempo de vida).

El protocolo IP se encarga de gestionar la fragmentación de paquetes cuando ve que es necesario, añadiéndoles a cada uno información sobre el origen y el destino en cada uno de los nuevos paquetes creados, además de la información necesaria para que el receptor pueda ensamblar los paquetes fragmentados y formar la secuencia original. Es posible que haya datos que se envíen con una marca de "no fragmentar", en cuyo caso los descartará.

El protocolo TCP.- Proporciona un servicio de datos confiable, es decir contiene detección y corrección de errores de extremo a extremo. TCP es responsable de la recuperación de datos en caso de que los paquetes se reciban de forma no secuencial, o si se produce algún tipo de corrupción durante la entrega, para lo cual TCP requiere de una confirmación denominada ACK, de la máquina de destino, una vez que haya recibido satisfactoriamente los datos. En caso de no recibir un ACK adecuado en un determinado intervalo de tiempo se retransmitirá el paquete, esto provoca a veces duplicación de paquetes en caso de que la red esté congestionada. Sin embargo, el receptor utiliza el número de secuencia de los paquetes para determinar si son duplicados, en cuyo caso los descartará.

TCP permite además que el receptor especifique la cantidad de datos que desea que le envíen, evitando así que el emisor envíe datos ciegamente esperando su confirmación.

[a] El campo TTL dentro de los paquetes IP es un contador que se utiliza para limitar el tiempo de vida de dichos paquetes. Cuando dicho contador llega a cero, el paquete IP se destruye.

1.1.2. ORGANISMOS QUE GESTIONAN EL INTERNET

Las principales organizaciones y grupos de trabajo que gestionan de una forma descentralizada Internet son los siguientes:

La ISOC (*Internet Society*, http://www.isoc.org/) que es una organización profesional sin ánimo de lucro para la cooperación y coordinación en la evolución de Internet. Está formada por asociaciones individuales y organizaciones (agencias gubernamentales, operadores de red, empresas, fundaciones, etc.). Publica un boletín trimestral (*On The Net*) y convoca una conferencia anual (INET, http://www.isoc.org/inet98/).

IANA (*Internet Assigned Numbers Authority,* http://www.iana.org) es la responsable de todos los "parámetros únicos" de Internet: protocolos, direcciones IP, nombres de dominio, etc. Está localizada en la USC (*University of Southern California*) (http://www.usc.edu/ y http://www.isi.edu/).

IETF (Internet Engineering Task Force, http://www.ietf.org/) es una comunidad abierta e internacional de operadores de red, diseñadores, investigadores, etc. preocupados por el diseño, arquitectura y evolución de Internet. Está organizada en 8 áreas divididas en Grupos de Trabajo.

El IAB (*Internet Architecture Board*, http://www.iab.org/) es el grupo asesor técnico de ISOC, formado por voluntarios, responsable de la edición y publicación de RFCs (*Request for Comments*), de la gestión de apelaciones por definiciones o uso de protocolos, etc. Además selecciona a los miembros del IESG y es responsable de supervisar las actividades de la IETF.

El IESG (*Internet Engineering Steering Group*, http://www.ietf.org/iesg.html) está formado por los 8 directores de área del IETF, especialistas en los siguientes campos: Aplicaciones, Internet, Protocolo IP, Gestión de Red, Requisitos de Operaciones, *Routing*, Seguridad y Servicios de Usuario.

Los estándares Internet se basan en las famosas RFCs (*Request for Comments*, http://www.rfc-editor.org/) que definen los protocolos y servicios de uso en la red. La propuesta y discusión de RFCs los realizan los grupos de trabajo de la IETF en colaboración con IANA y el IAB. Para entender un poco el mundo complejo de la definición de estándares en Internet se puede consultar la URL http://www.ietf.org/overview.html.

El organismo encargado de los nuevos desarrollos relativos al WWW es el *World Wide Web Consortium* (W3C) que se encuentran en el MIT (*Massachusets Institute of Technology*, http://www.mit.edu/) en Estados Unidos. La única participación europea en el proyecto es el INRIA francés (http://www.inria.fr/) y el CERN en Suiza (http://www.cern.ch/), donde se desarrolló el WWW. Muchos de los protocolos y desarrollos descritos se pueden encontrar con mucho más detalle en el servidor del W3C (http://www.w3c.org/).

Antes de entrar en detalle sobre la estructura jerárquica de los ISPs se definirá lo que es un ISP.

1.2. DEFINICIÓN DE ISP

Un ISP es una empresa que da servicios de conexión a la red Internet a usuarios del público en general (empresas públicas y privadas o clientes residenciales) a cambio de una tarifa determinada.

A través de un ISP los usuarios pueden tener acceso a la amplia gama de servicios que se encuentran disponibles en Internet. Además, el proveedor puede ofrecer servicios propios como por ejemplo: servicios de *mail*, hospedaje de páginas *Web*, *forums* de debate, etc.

El corazón de un ISP está conformado por los servidores que desempeñan las funciones necesarias para proveer el servicio a sus clientes. Los servidores son los dispositivos más importantes de Internet, pues son los que contienen la

información con la que cuenta la red. Éstos son máquinas que generalmente están disponibles las 24 horas del día durante los 365 días del año.

1.2.1. ESTRUCTURA JERÁRQUICA DE LOS ISPs

Los servicios de la Internet lo proporcionan los proveedores o ISPs. Cada ISP tiene su red propia que cubre una determinada zona geográfica según el tipo y tamaño del mismo: una ciudad, un país, un continente, etc. De acuerdo con ello, existe una organización jerárquica de ISPs, en la que el nivel superior lo ocupan los proveedores de troncales (*carriers*), aquellos que tienen redes de extensión (inter)continental y que son los que proporcionan el tránsito de la información de los ISPs de segundo nivel.

Los ISPs de segundo nivel suelen operar en un país o región, normalmente proporcionan acceso a clientes corporativos y a su vez "revenden" tránsito a ISPs menores, aquellos que suelen tener como clientes a usuarios residenciales o enfocan su negocio a servicios de valor añadido (correo electrónico, W*eb hosting*, etc.).

En la figura 1.1 se representa esquemáticamente esta organización jerárquica y la interconexión entre los distintos proveedores.

Los proveedores de nivel superior (ISP n1) unen sus redes en los nodos globales para el intercambio de tráfico, los NAP (*Network Access Point;* Punto de Acceso a la Red) en EE.UU. y los GIX (*Global Internet eXchange;* Intercambio de Internet Global) en otros lugares. Actualmente hay 5 NAPs en EE.UU. y 5 GIX en Europa. Los ISPs n1 pueden intercambiar el tráfico entre sus redes en los nodos globales correspondientes mediante acuerdos específicos, multilaterales o bilaterales. Esto es lo que representa la citada figura en el anillo superior. Los nodos de interconexión son básicamente un medio de transmisión de alta velocidad al que los ISPs conectan sus *routers* para implementar el intercambio de tráfico de acuerdo con la normativa acordada.

Así mismo, puede haber ISPs que intercambien el tráfico directamente entre sus redes sin pasar por los nodos de interconexión. En la figura 1.1 se pueden ver algunos casos.

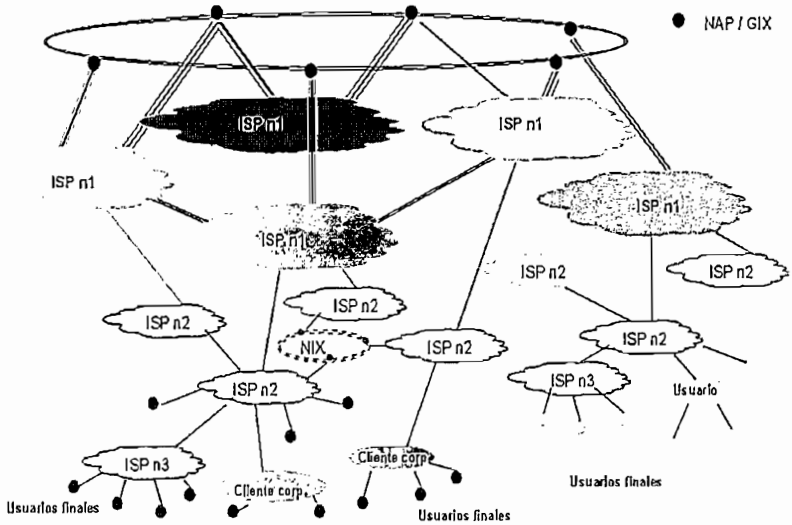


Fig.1.1. Estructura jerárquica de los ISPs [5]

En el nivel inferior se ven los ISPs n2, que "compran" tránsito a uno o varios ISPs n1. A su vez, "revenden" acceso a otros clientes, que bien pueden ser clientes finales (normalmente corporativos) o bien ISP n3, que son los que dan el servicio a usuarios finales.

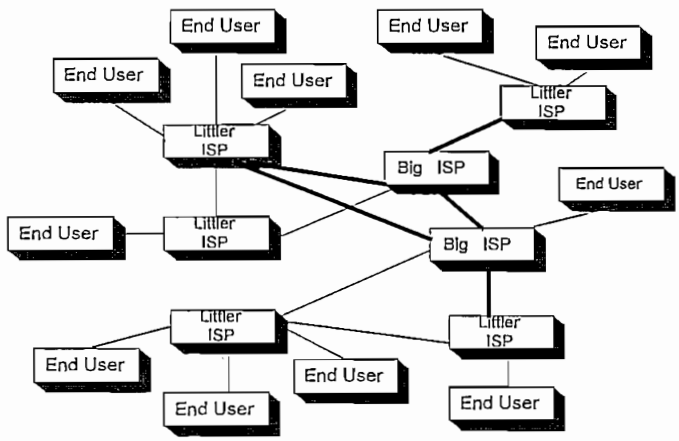
El tráfico entre ISPs n2 se puede intercambiar, evidentemente, a través de los ISPs n1 correspondientes; sin embargo, dado que esto conlleva el uso de enlaces internacionales, más caros, lo habitual es que los ISPs n2 unan sus redes en nodos de interconexión locales, normalmente a nivel de un país, en lo que se conoce como nodos neutros de interconexión (NIX), tal como se representa en la figura 1.1.

El funcionamiento de los NIX es similar al de los GIX y NAP. La idea es facilitar un medio común para conectar las redes en cuestión y llegar a los correspondientes acuerdos entre proveedores para el intercambio de tráfico. Es posible, asimismo, intercambiar el tráfico directamente, sin necesidad de ir a los NIX, dependiendo del interés de los ISPs en proporcionar una *buena conectividad*

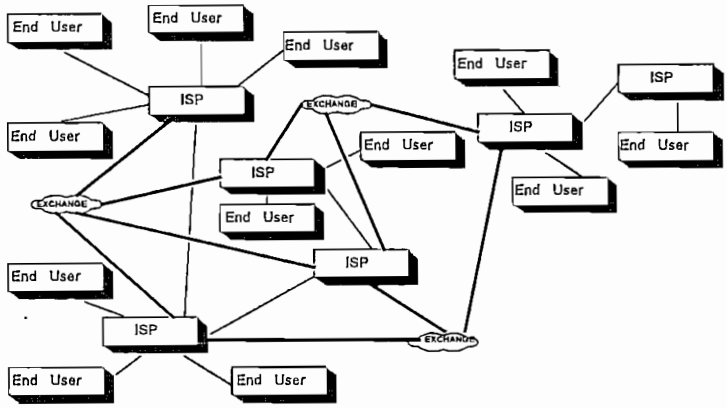
global a sus clientes.

En una estructura idealizada, la secuencia de conectividad entre usuarios finales e ISPs sería: ISP n1, ISP n2, ISP n3 y usuarios finales como se indica en la figura anterior, pero en realidad esto no es así, debido a que cada proveedor de servicios trata de acaparar algún sector de mercado (usuarios finales), de manera que no se puede realizar una distinción clara entre ISPs mayoristas y minoristas como se ve en la figura 1.2(a).

La conectividad no es verdaderamente proveedor a proveedor sino que incluye varias formas de puntos de intercambio en los cuales múltiples proveedores pueden intercambiar tráfico. Los ISPs interactúan en disposiciones: bilaterales como conexiones 1:1 y multilaterales que son típicamente abordados en los puntos de intercambio. En la figura 1.2(b), se puede visualizar mejor la actual arquitectura del Internet, en la cual se incluye la conectividad entre ISPs y usuarios finales, la mezcla de ISPs minoristas y mayoristas, así como la existencia de puntos de intercambio en varios lugares dentro del Internet.



(a) Vista no jerárquica



(b) Vista actual

Fig.1.2. Estructura de Internet [1]

1.3. ARQUITECTURA DEL ISP

Se puede dividir la arquitectura de un ISP en tres amplias áreas con el objeto de facilitar su estudio y diseño:

- Acceso a Internet
- Red del ISP
- Red de acceso al cliente

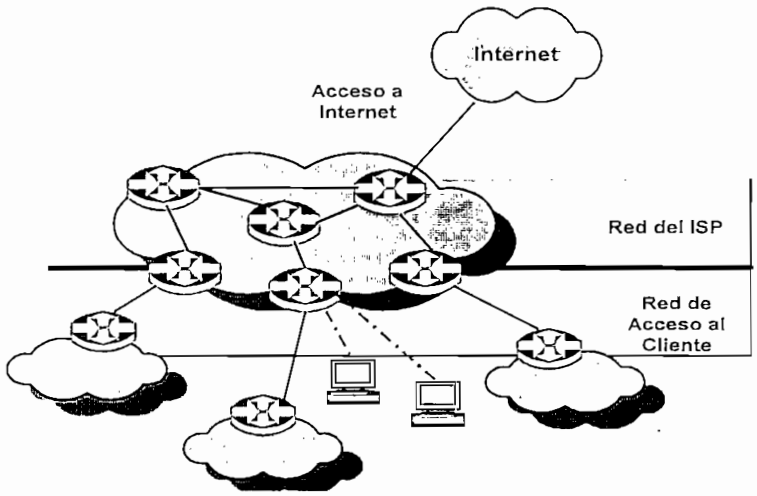


Fig.1.3. Arquitectura del ISP [1]

1.3.1. ACCESO A INTERNET

Para proveer servicios de acceso a Internet, obviamente, la red del ISP necesita estar conectada a Internet. Dicha conexión es a través de uno o más enlaces WAN a ISPs de niveles superiores, estos proveedores son usualmente llamados proveedores de *backbone* o proveedores *upstream*. En el caso de ISPs más grandes, éstos pueden estar directamente conectados al *backbone* de Internet mediante enlaces dedicados arrendados.

Usualmente, un ISP pequeño inicia con un único proveedor de *backbone* y un solo enlace WAN, pero como el número de usuarios crece, se presenta la necesidad de enlaces y proveedores de respaldo.

El enlace WAN debe ser una conexión permanente, típicamente una línea arrendada T1/E1 con PPP (*Point to Point Protocol*; Protocolo Punto a Punto), circuitos X.25, *Frame Relay,* ISDN (*Integrated Services Digital Network*; Red Digital de Servicios Integrados), ATM (*Asynchronous Transfer Mode*; Modo de Transferencia Asincrónico), etc, o enlaces satelitales, todos éstos deben ser adecuadamente dimensionados para soportar todo el tráfico externo generado por los usuarios.

Con la finalidad de escoger una tecnología de transmisión adecuada, se debe tener en cuenta aspectos importantes de cada una de ellas como son: velocidad de transmisión, retardo de propagación, tasa de error en la transmisión, etc dentro de las restricciones de costos. No existe una norma específica para tal selección, cada ISP escogerá su propia posición en términos de precio y rendimiento.

1.3.2. RED DEL ISP

1.3.2.1. Topologías de la Red del ISP

La topología interna de un ISP es un factor muy importante a la *hora de realizar*

un diseño, por esta razón, a continuación se detallarán las posible topologías de dicha red.

1.3.2.1.1. Topología en Estrella

La topología más simple de todas es la llamada topología en estrella o conocida también como jerárquica. Esta topología tiene un punto central que actúa como el corazón de la red y circuitos radiales que conectan distintos puntos de la misma red. Una topología en estrella puede sufrir de ciertos problemas ya que si el corazón de la red falla, entonces la red entera falla y si el enlace entre un punto remoto y el central falla, la localización remota quedará aislada. El objetivo de un ISP es brindar una eficiente capacidad de transporte de datos, y la topología en estrella puede presentar una combinación de máxima capacidad a un costo mínimo junto con lo que puede ser un nivel aceptable de riesgo operacional.

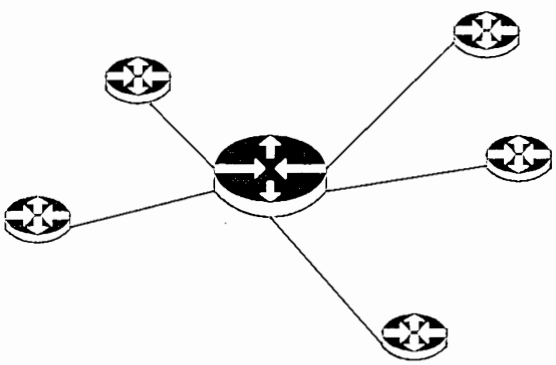


Fig.1.4. Topología estrella

Un mejoramiento a esta topología es la topología de estrella en cascada, en la cual un *backbone* con topología en estrella alimenta a una concentración de puntos que son a su vez parte de una topología en estrella más pequeña. Tales topologías tienen la ventaja de reducir los costos de los circuitos para proveer acceso a un conjunto de puntos antes de proveer acceso al punto central de la estrella mayor lo cual encarecería el costo. Sin embargo, con esta topología no se consiguen aislar los problemas mencionados anteriormente, es decir, si un

enlace falla, el servicio no estará disponible durante el tiempo de duración de la falla.

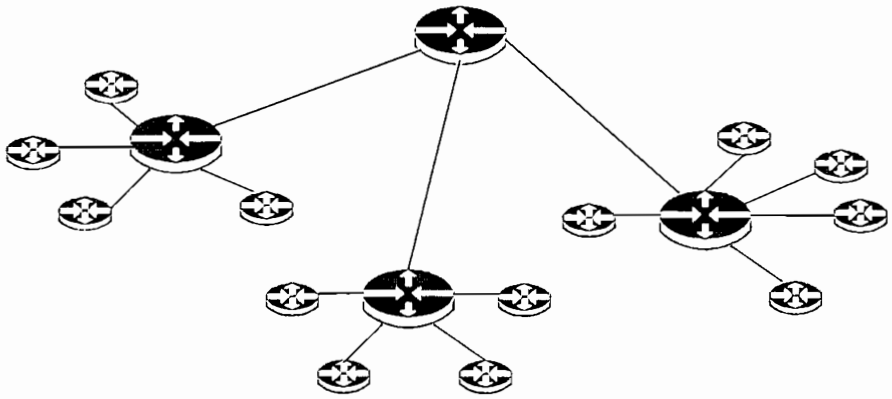


Fig.1.5. Topología estrella en cascada

1.3.2.1.2. Topología en Lazo

Una solución a los problemas que presenta la topología en estrella es usar una configuración en la que el *backbone* del ISP tenga una configuración en lazo, en la cual cada punto de la red es conectado con otros dos puntos, resultando de esta manera una conectividad en forma de anillo. Un anillo tiene la ventaja de ser más flexible ante las fallas de un único enlace ya que el algoritmo de enrutamiento que es utilizado por esta configuración reestablecerá la conectividad. Sin embargo, una topología en lazo no es siempre una solución efectiva de costos dado que, los puntos regionales más pequeños y potencialmente más lejanos pueden requerir de dos circuitos de acceso de alta capacidad para administrar la carga que transita por el *backbone*, imponiendo de esta manera un financiamiento innecesario.

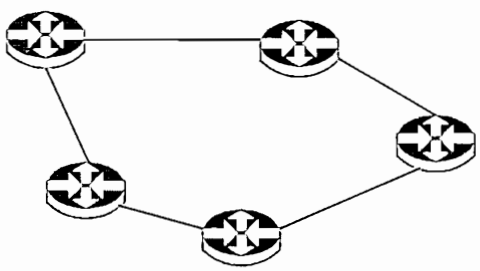


Fig.1.6. Topología en lazo

1.3.2.1.3. Topología en Malla

Una topología alternativa es una conectividad en malla. Una malla enlaza cada punto de la red con dos o más puntos remotos distintos. De esta forma, si un enlace en la red falla, la conectividad con dicho punto no se pierde ya que existen caminos alternativos; y si una localización entera de la red falla y es necesario aislar este punto, ninguna otra localización es aislada como efecto secundario. Las topologías malladas son más costosas que las topologías jerárquicas pero pueden soportar mayores flujos de tráfico que una topología de lazo.

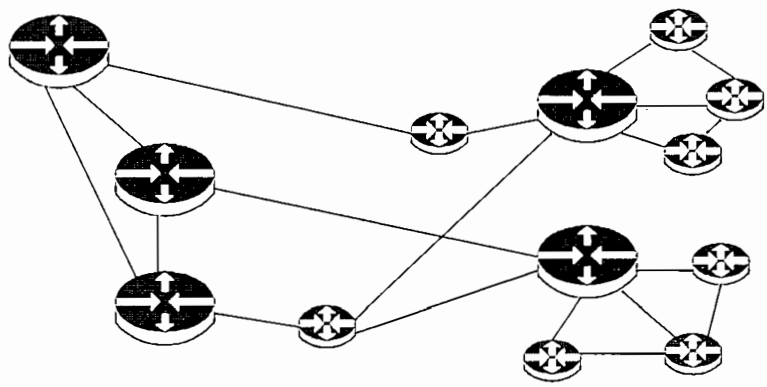


Fig.1.7. Topología en malla

1.3.2.1.4. Dial Backup

Otra topología alternativa es una topología dispersa complementada con un circuito de respaldo *dial* o *dial backup*. Cuando un enlace falla, los *routers* pueden ser configurados para establecer dinámicamente un circuito temporal que actuará como un puente sobre el punto de falla. Esto puede ser posible usando servicios X.25, ISDN, circuitos virtuales conmutados dentro de *Frame Relay*, ATM o circuitos de módems establecidos a través de la PSTN. Se deben instaurar ciertas directivas para asegurar que esto opere de forma adecuada:

Primero, la capacidad del circuito de respaldo dinámico o *backup* deberá ser de la misma magnitud del circuito original. Usar un circuito de *backup* que no pueda soportar el nivel de tráfico impuesto causaría serios problemas de congestión.

Segundo, la activación del circuito de *backup* deberá ser correctamente amortiguada ya que debido a ciertas condiciones externas, el circuito podría oscilar entre los estados de "disponible" y "no disponible" dentro de un período de décimas de segundo hasta decenas de segundos.

1.3.2.2. Elementos de la Red del ISP

Como se explicará más adelante, un ISP local esta conformado por una oficina central y oficinas locales. La red de un ISP central[a] consta básicamente de tres redes locales: una LAN conformada por las plataformas de servicio (servidores de aplicación), una LAN compuesta por las plataformas de administración de los servicios (servidores de administración) y otra LAN en la cual se encuentran los dispositivos de acceso. Esto se puede ver en la figura 1.8.

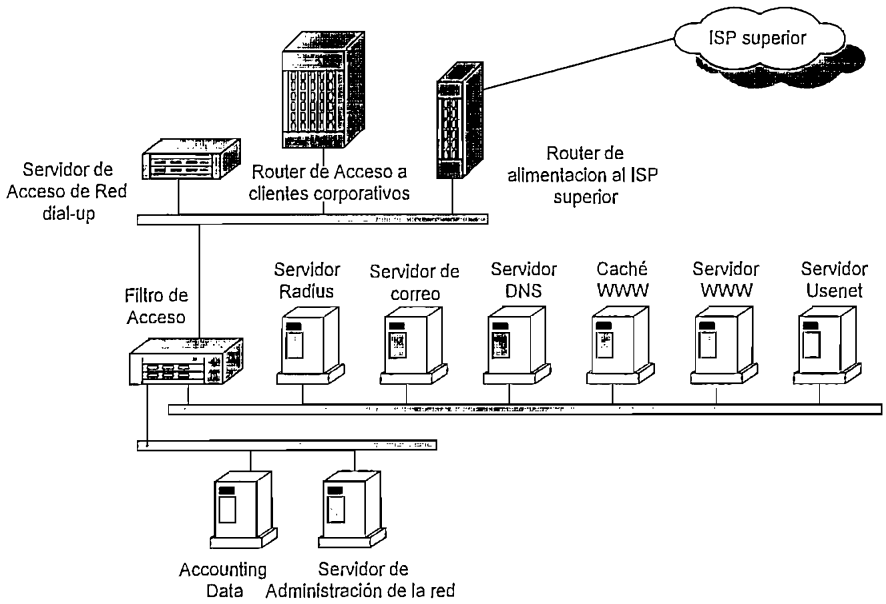


Fig.1.8. Red del ISP central [1]

La razón para la existencia de estas tres redes es separar las funciones de servicio y las funciones administrativas de los componentes de acceso al cliente como una medida de seguridad. Aunque este método no es una completa política de seguridad, esta segregación de tráfico dentro de tres dominios es un excelente primer paso en la construcción de un medio de seguridad útil y robusto, como se

[a] ISP central es el sitio donde se encuentran concentrados la mayoría de equipos del ISP, no son los PoPs.

verá en el capítulo IV.

En la red LAN conformada por los dispositivos de acceso se puede encontrar los siguientes *routers*: el *router* principal, encargado del flujo de los datagramas IP entre el ISP y la red Internet; el *router* de acceso a clientes corporativos; y el servidor de acceso de red (NAS), encargado de proveer conectividad a los usuarios *dial-up*. Las características y funciones de estos *routers* serán analizados con más detalle en el capítulo II.

A través de la red conformada por los servidores se puede tener acceso a servicios de correo electrónico, *hosting* DNS, *cachés proxy* WWW, *hosting* WWW para páginas de los clientes y un servicio de *browser Usenet.*

En la red de administración, se incluye un sistema de autenticación, manejo del perfil del cliente, sistemas de contabilidad y facturación.

Los requerimientos de *hardware* de los servidores de un ISP serán analizados en el capítulo III.

1.3.2.3. Puntos de Presencia (PoPs)

El diseño de la red del ISP también abarca el diseño de los puntos de presencia o PoPs. Un PoP es básicamente la misma red del ISP central que se ha extendido debido a la demanda de los usuarios.

Por medio del PoP, un ISP puede estar presente en otras áreas geográficas para *proveer acceso dial-up* a los usuarios utilizando para ésto números telefónicos locales o para proveer servicio a clientes corporativos. En un PoP, algunos de los servidores (tales como autenticación, *Web, mail*) no necesariamente deben estar presentes ya que se puede acceder a estos servicios desde el ISP central.

Todos los servicios que brinda un PoP pueden ser comprimidos dentro de una

única plataforma de *hardware*, sin embargo esto no es muy común ya que a pesar de minimizar costos, crea un punto de falla altamente crítico. El método más común es usar un conjunto de plataformas dedicadas con cada una de ellas realizando una tarea especializada.

Dentro de un PoP es conveniente disponer de dos clases de *routers*: *routers* de acceso y *routers* internos. En general, en los *routers* internos de un PoP terminan los enlaces de transmisión internos y en los *routers* de acceso terminan los circuitos de los clientes.

Los ***routers de acceso*** deben soportar servicios de acceso compartido de alta densidad tales como ISDN y otros servicios de transmisión tales como *Frame Relay*, ATM, o servicios de transmisión punto a punto para los clientes dedicados.

Adicionalmente, un PoP puede incluir un conjunto de Servidores de Acceso a la Red (NAS; *Network Access Servers*) los mismos que usan un banco de módems o servicios de acceso de velocidad primaria ISDN[a] y módems digitales para los clientes intermitentes. Otros servicios de acceso más especializados pueden ser incluidos en la arquitectura del PoP, como por ejemplo: unidades de terminación de la Línea Digital de Abonado (DSL, *Digital Subscriber Line*), Multiplexor de Acceso DSL (DSLAM, DSL *Access Multiplexor*) y unidades de terminación para un sistema de datos de cable híbrido fibra/coaxial (HFC; *Hybrid Fiber-Coaxial*).

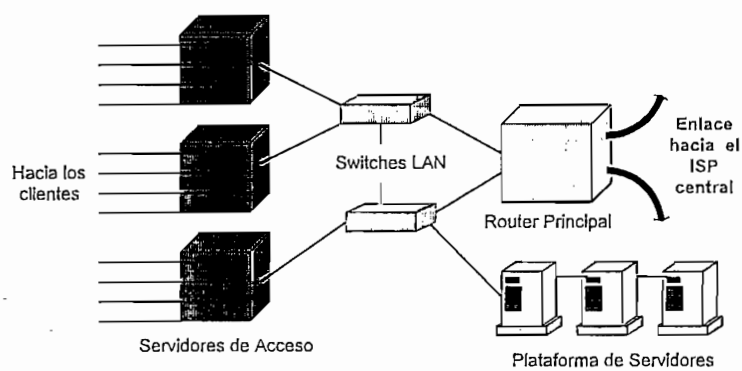


Fig.1.9. Estructura de un PoP [1]

[a] Para mayor detalle acerca de ISDN, referirse a la sección 3.3.1.3.

Los ***routers internos*** son típicamente diseñados para ofrecer máxima disponibilidad y máximo rendimiento y usan una configuración de densidad de puerto más baja, es decir, tienen menos número de puertos por *router*.

El elemento que sirve de enlace entre los *routers* de acceso y los *routers* internos es una ***red local.*** Aunque un *hub* Ethernet puede ser suficiente para PoPs de baja densidad de tráfico, muchos centros ahora utilizan múltiples *switches* conmutados basados en *switches Fast* Ethernet de 100 Mbps.

1.3.3. RED DE ACCESO AL CLIENTE

Existen dos maneras para acceder a la red del ISP, la decisión de cual modelo utilizar en cualquier caso particular está determinado ampliamente por la naturaleza del cliente.

Si el cliente es una entidad corporativa, un campus universitario, una agencia gubernamental, o similar, entonces el cliente es caracterizado como un cliente corporativo.

Si el cliente es un sistema único, tal como una PC residencial o una PC de una oficina pequeña, y la conexión es sobre demanda, entonces el modelo de acceso es *dial-up*. Este cliente es caracterizado como un cliente que accede por *dial.*

1.3.3.1. Cliente Corporativo

Estos son clientes de negocios que desean conectar sus redes a Internet a través de un ISP. Un ISP más pequeño (como un PoP) también puede ser un cliente corporativo.

Se debe tener claro la demarcación de la frontera entre el ISP y el cliente, pues con un claro conocimiento de las responsabilidades respectivas de equipos y

servicios se obtiene una operación efectiva pues de lo contrario se tendrá confusión operacional e inconsistencias.

La estructura típica de conectividad para las redes del cliente y del ISP se indica en la figura 1.10 y está compuesta de tres elementos:

- El *router* fronterizo del cliente
- Un circuito de transmisión
- El *router* de acceso del ISP, comúnmente referido como un *router* PoP.

El ***router fronterizo del cliente*** típicamente está en el lado del cliente e interconecta a la red local del cliente; se encarga de funciones específicas del cliente, incluyendo funciones de *firewall* y filtros de tráfico para permitir algún nivel de seguridad en el lado del cliente.

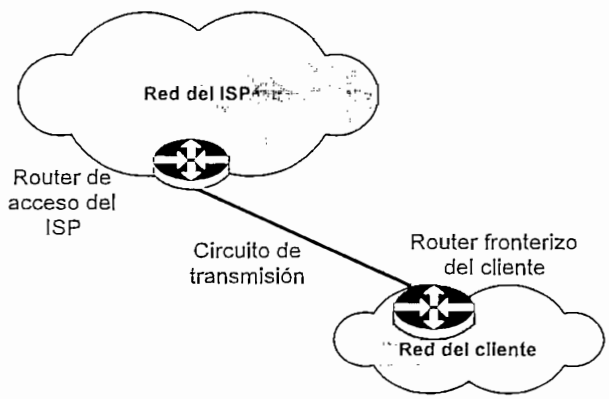


Fig.1.10. Arquitectura de la red de acceso al cliente corporativo[1]

El ***circuito de transmisión*** es un circuito dedicado, que puede ser arrendado desde el *carrier* o puede ser alguno de los circuitos conmutados, tal como un circuito ISDN, un circuito virtual *Frame Relay* o un circuito virtual ATM.

El ***router POP*** típicamente se encarga de las funciones de control de ruteo de red y tiene la responsabilidad de administrar el acceso de la red del cliente. El *router* POP es el punto donde los filtros de ruta están instalados *para garantizar* la

integridad en la notificación de rutas. Además se encarga del control de tráfico que entra o sale de la red, monitoreo y contabilidad, porque es la frontera lógica del campo de administración del ISP.

Un cliente corporativo puede conectarse a uno o varios ISPs de acuerdo a tres modelos de enlace cliente/ISP, éstos son: *single-homed*, multiconectado y *multi-homed.*

1.3.3.1.1. Cliente single-homed

Es el cliente de red quien se conecta exclusivamente a un ISP utilizando un puerto de acceso dedicado. Esta conexión puede ser de varias formas tales como circuitos arrendados, enlaces de radio, cable privado, etc. Este modelo de conexión se ilustra en la figura.1.11.

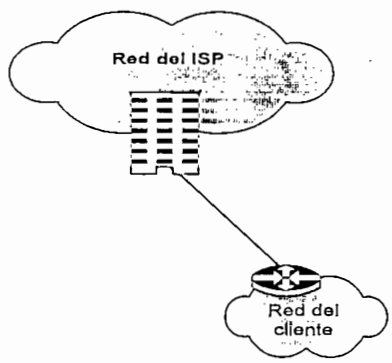


Fig.1.11. Cliente single - homed [1]

1.3.3.1.2. Cliente multiconectado

La arquitectura para la conexión de clientes *single-homed* puede ser reproducida cuando el cliente se conecta al mismo ISP usando más de una conexión. El resultado de esta configuración es un caso de *salida cercana,* donde el tráfico transita de una red a otra utilizando el punto accesible más cercano (ver figura 1.12).

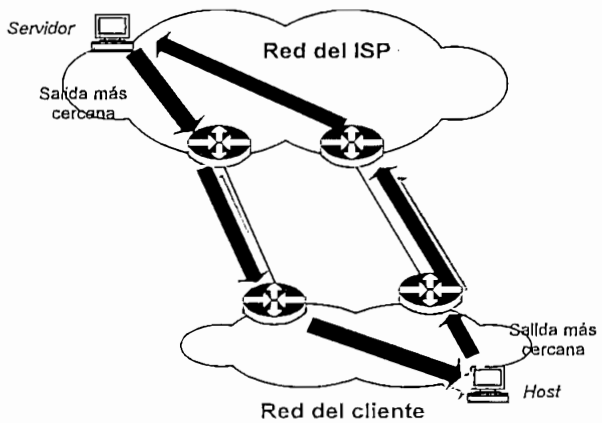


Fig.1.12. Cliente multiconectado [1]

Este modelo puede presentar un flujo de carga asimétrico, donde la información puede tomar un camino de regreso diferente al camino de ida entre el *host* del cliente y el ISP.

Este tipo de conexión pretende incrementar la robustez y confiabilidad de la conexión externa mediante el uso enlaces de *backup*.

1.3.3.1.3. Cliente multi-homed

Otro tipo de conexión que el cliente opta por realizar, es cuando él decide conectarse con múltiples proveedores de servicios de Internet, ya sea para mejorar la fiabilidad de la conectividad externa o la equiparación de políticas y requerimientos de seguridad, esta configuración se indica en la figura1.13.

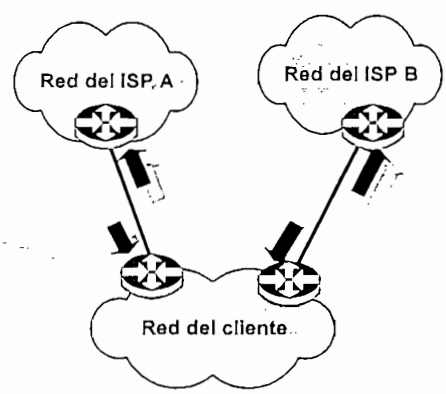


Fig.1.13. Cliente multi-homed [1]

1.3.3.2. Cliente *dial-up*

El segundo modelo de acceso a la red del ISP es mediante acceso *dial-up*, el cual involucra una computadora personal, un módem y el uso de una línea telefónica de la PSTN (*Public Switched Telephone Network*; Red Telefónica Pública Conmutada) para alcanzar el servidor de acceso de red (NAS) del ISP. Este término es pretendido para cubrir escenarios como acceso *dial* de redes LAN, acceso ISDN, y otros mecanismos de acceso dinámico donde la conexión entre el cliente y el ISP es sobre demanda antes que permanente.

Típicamente este tipo de clientes se conectan a Internet para tener acceso a páginas *Web* y servicio de *mail*. Como regla general, estos clientes se conectan en horas fuera de oficina o fines de semana.

Los elementos de soporte del ISP para clientes de acceso *dial-up* son:

- Unidades NAS
- Sistemas de soporte de autenticación
- Servidores de correo y *Web* para soporte de funciones de usuario.

Esta configuración se indica en la figura 1.14.

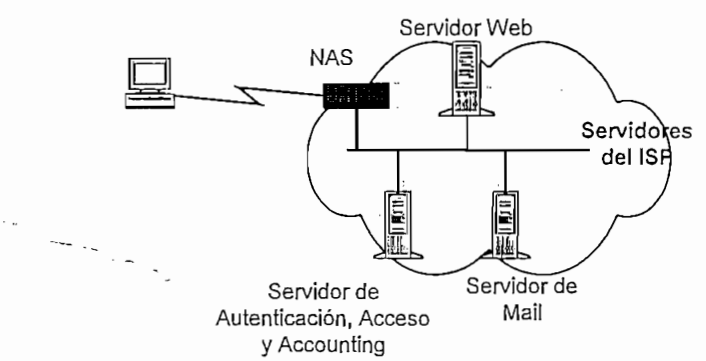


Fig.1.14. Sistemas de soporte de acceso del cliente dial – up[1]

Unidades NAS

Una ***unidad NAS*** (*Network Access Server*; Servidor de Acceso de Red) es el equipo que responde las llamadas y provee conectividad PPP a los usuarios *dial-up*. Un NAS es un dispositivo combinado que consisten de un banco de módems y un servidor de acceso.

El banco de módems está configurado en un grupo rotatorio a fin de que una llamada de acceso analógica seleccione el siguiente módem disponible para establecer la conexión. Entonces, el módem del cliente y el módem NAS se sincronizan y la PC del cliente se conecta al puerto serial del servidor de acceso.

Si la llamada entrante es una llamada digital ISDN, ésta es directamente conmutada al servidor de acceso sin necesidad de pasar por el banco de módems.

En ambos casos cuando la llamada es sincronizada, la sesión PPP (protocolo punto a punto) transmite una dirección IP asignada dinámicamente al sistema del cliente para usar en el puerto serial, y cuando éste es configurado la sesión PPP registra el modo de transferencia de datos.

Sistemas de Soporte de Autenticación

Por ***autenticación*** se entiende la necesidad de permitir o no el acceso de un usuario remoto a los recursos de la red del ISP. Una autenticación requiere la existencia de una base de datos donde están registrados los usuarios: sus datos personales y los recursos a los cuales tiene acceso. Esta base de datos puede ser local en el servidor de acceso o situado en otro lugar, en un servidor de red denominado Servidor de Autenticación. La comunicación entre el Servidor de Acceso Remoto y el Servidor de Autenticación se da a través de los protocolos definidos específicamente para esta función. Los establecidos en la comunidad Internet son: TACACS y RADIUS.

RADIUS (*Remote Authentication Dial-In User Service*) es un protocolo que

permite a un Servidor de Acceso Remoto hacer la autenticación de un usuario a través de un Servidor de Autenticación. Además de la autenticación, suministra información referente a la actividad del usuario.

El RADIUS constituye un sistema de seguridad previsto para implementaciones de acceso remoto. En la actualidad su mayor aplicación se da con los Proveedores de Servicios (ISP) para validar a usuarios que desean ganar el acceso a Internet. Tanto *routers* y Servidores de Acceso Remoto tienen soporte Radius, y se han convertido en una característica importante cuando se considera la selección de un equipo de conectividad. Una de las características del Radius es su seguridad.

Los paquetes de información son autenticados a través de una clave secreta, que nunca es enviada por la red, cualquier *password* es transferido encriptado entre el cliente y el Servidor Radius. El Radius adopta el modelo cliente/servidor para una operación: la parte cliente del Radius reside en el servidor de acceso y la parte *server* en el Servidor Radius que pueden tener como plataforma operativa UNIX o Windows NT (típicamente).

Los pedidos de autorización de acceso, recibidos por el Servidor Radius, son enviados por el servidor de acceso al recibir llamadas de usuarios remotos. A través de un banco de datos, los pedidos son aceptados o no, y la contabilización[a] puede ser iniciada. Se puede comprender mejor esta dinámica describiendo las fases de su operación.

Fase 1: Autenticación: El servidor de acceso envía un pedido de acceso al Servidor Radius y espera:

Aceptado: Continua con la fase 2 (descrita a continuación).

Rechazo: Permite nuevo intento o cancela la tentativa de acceso.

[a] Contabilización es el registro de uso de los recursos por parte de los usuarios, sea para cobranzas o fines estadísticos. Por ejemplo, la información que más se utiliza es el tiempo que el usuario está conectado. También se puede obtener: número de accesos, total de paquetes o bytes recibidos/transmitidos, etc.

Desafío: Envía mensaje, en el cual el usuario deberá enviar una respuesta esperada. Si el servidor valida esta respuesta envía un "*Aceptado*".

Fase 2: Contabilidad: El Servidor de Acceso Remoto envía un "pedido de contabilizar ", luego de la autenticación, y otro inmediatamente después de la desconexión , señalando el fin de la contabilización.

Sistemas de soporte de acceso

El principal ***sistema de soporte*** para usuarios *dial-up* es el correo electrónico, en el cual el ISP debe operar un *host send-mail* para permitir la recopilación de mensajes en representación del usuario y operar un *host PoP/IMAP mail* para permitir al usuario descargar los mensajes almacenados.

Los servicios de soporte también incluyen servicios de Dominio de Nombre, servicios *Web hosting*, y servicios de acceso *Usenet* como el núcleo de la carpeta de servicios, aunque esto varía entre ISPs. Adicionalmente servidores caché *Web proxy*, servidores IRC y servidores FTP podrían ser parte de la carpeta de servicios. En un ISP de pequeño o mediano tamaño todos estos servicios pueden ser colocados en un único *host*, pero para ISPs más grandes, estos servicios deben estar albergados en múltiples servidores operando en paralelo para servir a los clientes.

1.4. TIPOS DE ISPs

Los ISPs varían ampliamente de tamaño y de acuerdo a esta característica se puede encontrar en el mercado ISPs pequeños conformados por un único PoP hasta ISPs de alcance internacional cuyos PoPs estén distribuidos en todo el mundo.

De acuerdo al alcance de cada ISP, se los puede clasificar de la siguiente manera:

- ISP Local o ISP de Acceso
- ISP Regional
- ISP Nacional e Internacional

1.4.1. El ISP LOCAL O ISP DE ACCESO

Un ISP local o de acceso es un ISP pequeño que puede cubrir un área determinada de una ciudad o parte de ella. Generalmente se encuentra conectado a un ISP Regional, Nacional o Internacional para acceder al *backbone* de Internet y proveer acceso a sus clientes. Un ISP local puede ser visto como el PoP de un ISP de nivel superior.

Este tipo de ISPs normalmente concentran su servicio dentro del mercado de acceso *dial*, ofreciendo acceso a Internet dentro del sector residencial y pequeñas empresas.

Un ISP local está conformado por una ***oficina central*** y ninguna, una o varias ***oficinas locales*** dependiendo del tamaño del ISP.

La figura 1.15 ilustra un ISP local que usa una simple topología de estrella como parte del diseño.

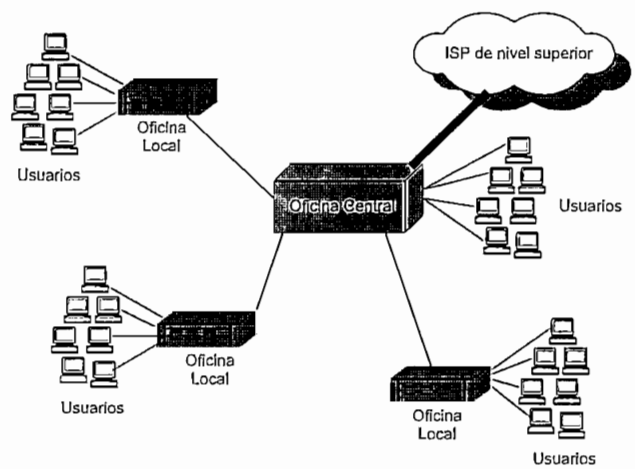


Fig.1.15. El ISP de acceso[1]

1.4.1.1. Oficinas Locales

Las oficinas locales o PoPs desempeñan dos funciones importantes que son: terminación de llamadas *dial* entrantes de los clientes y terminación del circuito proveniente de la oficina central.

Es recomendable utilizar servicios de acceso de velocidad primaria ISDN para terminación de servicios de acceso *dial*. Esta decisión de utilizar tecnología ISDN permite la eliminación del banco de módems y un grupo rotativo asociado de números de acceso PSTN, simplificando grandemente la tarea de administración operacional y permitiendo ahorrar en gastos operacionales.

El circuito de datos que va hacia la oficina central no tiene requerimientos particulares, de tal manera que la selección de tecnología de portadora está típicamente basada en minimizar el precio del ancho de banda y operar con un nivel aceptable de disponibilidad y confiabilidad.

La relación entre la capacidad del circuito que va hacia la oficina central y el número de puertos de acceso *dial* de los clientes es una decisión de precio/calidad que debe ser tomada por el ISP, de la misma forma que el número de puertos de acceso *dial* por número de clientes que han contraído el servicio.

1.4.1.2. Oficina Central

Así como un *hub* de tráfico, la oficina central opera como un centro de servicio y administración para el cliente de la red, de manera que aquí se encuentran todos los servidores y *routers* que conforman el corazón del ISP.

En la oficina central se encuentra un *router* de acceso a las oficinas locales encargado de terminar los circuitos provenientes de las oficinas locales y proveer enrutamiento del tráfico entre ellas, el *router* principal encargado de proveer conectividad externa y servidores de acceso a la red (NAS) para los clientes *dial*.

Todos los servicios ofrecidos por el ISP local pueden encontrarse operativos a través de distintos servidores o, en el caso ISPs de acceso muy pequeños, se puede utilizar un único *host* para albergar todos estos servicios.

Los servicios que típicamente se ofrecen aquí son: servicios de correo electrónico, *hosting* DNS, cachés *proxy* WWW, *hosting* WWW para páginas de los clientes y un servicio de *browser Usenet*. En el lado de administración, se incluye un sistema de autenticación, manejo del perfil del cliente, sistemas de contabilidad y facturación.

1.4.2. EL ISP REGIONAL

Un ISP Regional puede ser definido como aquel que tiene sus PoPs difundidos en determinadas zonas y que además de proveer acceso *dial* debe tener la capacidad de ofrecer acceso permanente a sus clientes, lo cual generalmente demanda velocidades de acceso y calidad de servicio más altas. Se encuentra conectado a un ISP Nacional o Internacional o, en algunos casos, se encuentran directamente conectados a una compañía de telecomunicaciones que le brinde acceso directo al *backbone* de Internet.

La arquitectura de un ISP regional es típicamente más compleja que la de una simple estrella o una estrella jerárquica, debido al requerimiento de incrementar la robustez de los servicios que ofrece la red. Adicionalmente, la topología de la red se ve influenciada por el requerimiento de ofrecer una escala más grande de servicios.

La función de la oficina central está ahora distribuida en dos o más oficinas centrales, como un medio de distribución de carga y respaldo mutuo para mejorar la disponibilidad del servicio. Las oficinas centrales están interconectadas mediante un circuito primario y adicionalmente posee algunos caminos de respaldo, nuevamente, esto es un medio de garantizar disponibilidad máxima de los servicios.

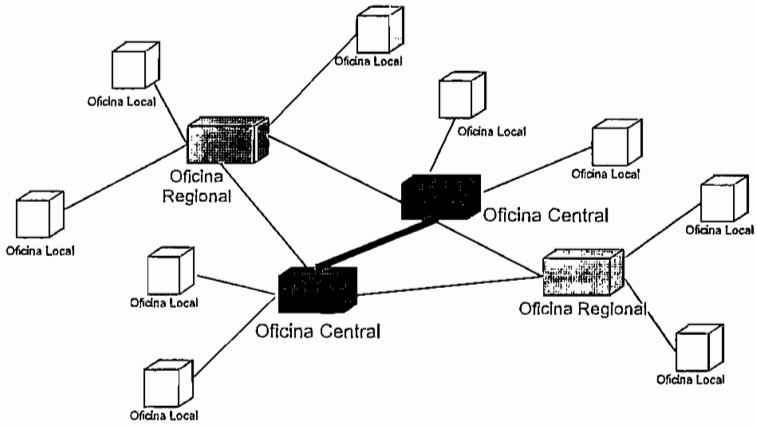


Fig.1.16. ISP Regional [1]

1.4.2.1. Oficinas Regionales y Locales

En este diseño se introduce un nuevo componente que es una oficina regional. Los circuitos de las oficinas locales terminan en la oficinas regionales dentro de un *router hub* el cual conmuta este tráfico hacia las oficinas centrales. Las oficinas regionales están compuestas de *routers*, unidades de acceso a la red, y un conjunto básico de servidores locales los cuales a su vez están enlazados hacia los servidores principales de la oficina central.

El diseño interior de la oficina central es similar al diseño de la oficina central del ISP local, aunque aquí es mucho mejor utilizar plataformas de servicio (servidores) individuales para cada servicio y no un único *host* como alternativa. La diferencia básica entre la oficina regional y la oficina central es que en esta última se encuentran todos los servicios que ofrece el ISP a sus clientes mientras que en la oficina regional no necesariamente se deben encontrar todos los servidores, se puede tener acceso a éstos a través de la oficina central.

La oficina local es similar en diseño y función a la oficina local del ISP de acceso. En esta arquitectura, la oficina local está diseñada tanto para satisfacer requerimientos de clientes conectados permanentemente con bajo ancho de banda como requerimientos de clientes de acceso *dial*.
Una unidad adicional es necesaria en esta arquitectura: el *router* de acceso que

es utilizado para terminar conexiones permanentes de los clientes. Estos servicios normalmente incluirán alguna forma de servicio de acceso de n x 64 Kbps, servicio *Frame Relay*, y otros servicios de portadora de velocidad baja a media.

El diseño de la oficina local puede extenderse desde un simple NAS hasta un conjunto de unidades, como se indica en la figura 1.17.

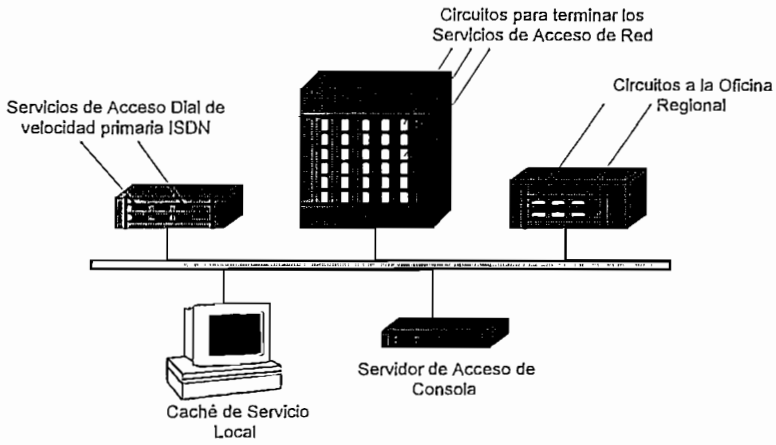


Fig.1.17. La oficina local del ISP Regional [1]

1.4.3. El ISP NACIONAL E INTERNACIONAL

Tanto los ISPs Nacionales como Internacionales arriendan circuitos de alta velocidad a las compañías de telecomunicaciones para de esta forma conectar sus PoPs y tener acceso a los NAPs donde ellos pueden intercambiar rutas y tráfico.

Un ISP Nacional tiene sus PoPs difundidos a lo largo de un país, mientras que un ISP Internacional está presente en varios países llegando inclusive a constituirse en ISPs de alcance mundial.

Estos ISPs son empresas a gran escala que pueden ser clasificados como se indica a continuación:

1.4.3.1. El ISP Integrado

Una primera clasificación de ISPs internacionales es aquella que pretende continuar con el crecimiento del ISP regional con la idea de ser una red con un corazón interior de alta velocidad conectado a un grupo de oficinas centrales. Estas oficinas centrales alimentan a un determinado número de oficinas regionales y a su vez éstas alimentan a varias oficinas locales. Esta metodología se indica en la figura 1.18.

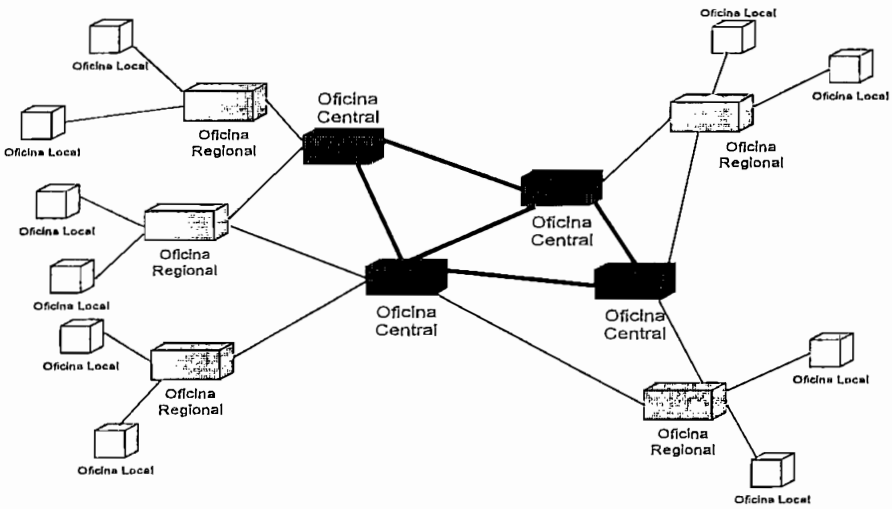


Fig.1.18. El gran ISP Integrado [1]

1.4.3.2. El ISP de Acceso *Outsourced*

Outsourcing o tercerización es transferir a terceros proveedores aquellas actividades que no son la columna vertebral del negocio. Básicamente, ésta es una modalidad mediante la cual determinadas organizaciones, grupos o personas ajenas a una compañía son contratadas para hacerse cargo de "una parte del negocio" o de un determinado servicio con el fin de agilizarlo, optimizar su calidad y/o reducir sus costos.

Dentro del contexto ISP, un proveedor de acceso a gran escala del tipo *outsourced* utiliza un grupo de proveedores locales rentados para brindar servicios de acceso local a los clientes y entonces transportar el tráfico a través de la red de los proveedores locales rentados. Este método permite al ISP extenderse hacia más áreas marginales de pequeña penetración en el mercado mediante la compartición de infraestructura de acceso. En este tipo de diseño el ISP de acceso *outsorced* opera la oficina central y el corazón de la red, pero no el acceso mediante las oficinas locales y regionales lo cual lo hace el proveedor de acceso contratado.

1.4.3.3. El ISP Multimodo

Algunos proveedores de telefonía han visto como un mecanismo para mantenerse dentro del mercado ofrecer servicios de comunicaciones relacionados con Internet, tales como llamadas telefónicas de larga distancia, telefonía móvil, etc.

Algunas empresas telefónicas actualmente proveen servicios de mayor amplitud, ofreciendo paquetes completos de servicios de acceso a Internet utilizado su propia infraestructura como medio de transporte de la información, de esta manera ofrecen un amplio rango de servicios de acceso y cobertura a gran escala.

BIBLIOGRAFÍA CAPÍTULO 1

[1] "*ISP Survival Guide. Strategies for Running a Competitive ISP*"; Geoff Huston; Primera Edición; John Wiley & Sons, Inc; 1999; EE.UU.

[2] "Edición Especial TCP/IP"; John Ray; Prentice Hall; 1999; Madrid.

[3] "TCP/IP. Principios Básicos; Protocolos y Arquitectura"; Douglas E. Comer; Tercera Edición; Prentice Hall; 1996; México.

[4] "*Internet Routing Architectures*"; Sam Halabi y Danny McPherson; Segunda Edición; Cisco Press; Indianapolis; 2000

[5] http://www.aui.es/

Biblioteca. Libros. Servicios en Internet con garantías de calidad

[6] http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg242133.pdf

The Technical Side of Being an Internet Service Provider.

[7] http://www.isa.uniovi.es/docencia/redes/tema6.pdf

El Protocolo TCP/IP

[8] http://www.itpapers.com

ISP

[9] http://gsyc.inf.uc3m.es/~jjmunoz/ro/992000/98ip.pdf

Redes de Ordenadores

[10] http://www.amazing.com.internet.htm

The Internet Provider (FAQ)

[11] http://www.cis.ohio-state.edu/htbin/rdc/rfc0791.html

Protocolo Internet

[12] http://www.cis.ohio-state.edu/htbin/rdc/rfc0793.html

Transmission Control Protocol

[13] http://www.arrakis.es/~val/curs/SERV/INET/TECNIC.htm

Funcionamiento de Internet

2

PROTOCOLOS DE ENRUTAMIENTO EN UN ISP

CAPÍTULO II

PROTOCOLOS DE ENRUTAMIENTO EN UN ISP

2.1. INTRODUCCIÓN

Se denomina enrutamiento al proceso de elegir el mejor camino por el cual viajará un paquete, y *router* al dispositivo encargado de realizar esta decisión.

Como se dijo anteriormente, Internet es un conjunto de redes físicas interconectadas mediante *routers*. Cada *router* está unido a dos o más redes físicas, y los *hosts* en cambio, frecuentemente, suelen estar conectados a una sola red física. Tanto los *routers* como los *hosts* participan en el proceso de enrutamiento IP.

Existen dos tipos de enrutamiento: enrutamiento estático y enrutamiento dinámico.

En el ***enrutamiento estático***, el *router* almacena sus tablas de enrutamiento en forma estática, es decir, almacena tablas fijas cuyas rutas están basadas en la información de la topología de la red no obtenida en tiempo real, sino ingresada por el administrador del equipo; de esta manera el *router* no necesita intercambiar información de ruteo con los *routers* vecinos y por lo tanto no requiere para su funcionamiento un protocolo de enrutamiento. La desventaja de un algoritmo de enrutamiento estático es que éste no se ajusta a situaciones cambiantes en la red como por ejemplo: fallo de una conexión física, saturación, etc. X.25 utiliza este tipo de enrutamiento.

En el ***enrutamiento dinámico***, el *router* configura automáticamente las tablas de enrutamiento en base a la información en tiempo real que los *routers* reciben de los protocolos de enrutamiento. Es decir, un protocolo de enrutamiento es aquel que permite a los *routers* crear tablas de rutas mediante el continuo intercambio

de información acerca del estado de la red para lo cual el *router* utiliza protocolos de ruteo como por ejemplo IP o UDP. Esta información, conocida como información de ruteo notifica a los *routers* acerca de parámetros variables de la red como congestión, prioridad, distancia, etc.

Una red IP como Internet utiliza enrutamiento dinámico, lo cual implica un doble nivel de complejidad ya que necesita de algoritmos para generar las tablas de enrutamiento y protocolos de ruteo encargados de distribuir dichas tablas a los distintos destinos.

Internet utiliza el protocolo IP como protocolo de ruteo, es decir IP se encarga de rutear los datagramas hasta su destino final. Para que IP pueda rutear un datagrama, hace uso de las tablas de enrutamiento, las mismas que son creadas en base a los algoritmos de enrutamiento. Un algoritmo de enrutamiento es implementado por los protocolos de enrutamiento.

Los protocolos de enrutamiento se basan principalmente en dos tipos de algoritmos de enrutamiento: algoritmo vector distancia y algoritmo de estado de enlace. El estudio de estos algoritmos se lo realizará a continuación.

Algoritmo Vector Distancia

Este algoritmo también es conocido como algoritmo de Bellman-Ford y fue el algoritmo original de Arpanet. Se lo aplica en diversos protocolos de enrutamiento como RIP (*Routing Internet Protocol*; Protocolo de Enrutamiento Interior) e inclusive en protocolos propietarios como IGRP (*Interior Gateway Routing Protocol*; Protocolo de Enrutamiento de Pasarela Interior) y EIGRP (*Enhanced Interior Gateway Routing Protocol*; Protocolo de Enrutamiento de Pasarela Interior Mejorado) de Cisco, aunque estos dos últimos hacen una combinación del algoritmo vector distancia y estado de enlace.

El término vector distancia se basa en que la información de enrutamiento se envía dentro de mensajes constituidos por listas de pares (*a,b*), *donde a* es el

vector o destino y *b* es la distancia (o métrica) ya sea en saltos o retardo.

A continuación se describe el funcionamiento del algoritmo vector distancia:

1. Inicialmente, cada *router* genera una tabla de enrutamiento local que contiene información de cada una de las interfaces locales a las cuales tiene conectadas directamente redes y entonces asigna un valor de distancia igual a 0.
2. Esta tabla es difundida a cada uno de los *routers* adyacentes, para lo cual utiliza la dirección de la interfaz local como la fuente (origen) del *broadcast*.
3. El receptor de la tabla incrementa el valor de la distancia de la tabla recibida en 1 (ya que las redes están ahora a 1 *router* más de distancia).
4. La información entrante es entonces comparada con la información almacenada para cada dirección de red. Un *router* que ha recibido una nueva tabla de enrutamiento, actualizará sus tablas si:

    - La métrica recibida es más baja que el anterior valor almacenado.
    - En la tabla recibida se encuentra un destino que el *router* local no conocía.
    - La distancia de un *router* A a un destino desde un *router* B pasando por A ha cambiado.

5. Si una ruta no ha sido actualizada en un período determinado de tiempo, ésta es removida de la tabla.
6. Nuevamente la tabla es difundida a cada *router* adyacente, de la misma forma que en el paso 2, y el algoritmo continúa el proceso ya descrito.

Este tipo de algoritmo es muy fácil de implementar, pero tiene algunas desventajas como las que se mencionan a continuación.

Cuando las rutas cambian rápidamente, es decir, aparece una nueva o cae otra, la nueva información de enrutamiento se propaga lentamente. Esto puede ocasionar que mientras dicha información se está propagando, algunos *routers* tengan información de enrutamiento incorrecta, este problema se conoce como ***convergencia lenta,*** la cual ocasiona el ***conteo al infinito***.

Para comprender el problema de conteo al infinito, supongamos que la conexión entre un *router* A y una de sus redes directamente conectadas falla. A entonces actualizará su tabla para hacer la distancia igual a infinito. En la siguiente difusión A anunciará su tabla con costo elevado (infinito) para dicho destino, al recibir esta información, el router B entenderá que este destino es inalcanzable a través de A. Sin embargo, si B logra difundir sus rutas antes que lo haga A, A recibirá esta información no actualizada y se ejecutará el algoritmo vector distancia, es decir: A notará que B a enviado una ruta con un valor (o costo) más bajo y actualizará su tabla sumándole 1. En el siguiente ciclo, A difundirá nuevamente sus tablas a B y éste sumará 1 nuevamente a las rutas recibidas y las agregará a sus tablas y así sucesivamente hasta el infinito.

Algoritmo Estado de Enlace

Este algoritmo también es conocido con el nombre SPF (*Shortest Path First*; Primero la ruta más corta) y es una alternativa para solucionar los problemas que presenta el algoritmo vector distancia.

El algoritmo de estado de enlace divide a un conjunto de redes físicas en un número determinado de áreas.

Todos los *routers* dentro de un área deben tener bases de datos idénticas. La topología de un área se representa mediante una base de datos denominada LSD (*Link State Database*; Base de datos del Estado de Enlace) que es una descripción de todos los enlaces de los *routers* del área. La base de datos de cada *router* describe la topología completa del dominio, es decir, qué *router* se conectan a qué redes. Cada *router* usa su base de datos para computar el

conjunto de caminos mínimos a todos los destinos que contiene su tabla.

La operación básica de un protocolo de estado de enlace es relativamente simple:

1. Cada *router* aprende la identidad de todos los *routers* adyacentes y calcula el costo del enlace a cada uno de ellos. El costo de un enlace puede utilizar diferentes métricas como retardo, distancia física, ancho de banda, etc.
2. Con esta información, el *router* construye un mensaje que contiene la identidad y costo del enlace de cada vecino. Este mensaje es llamado LSP (*Link State Packet*; Paquete de Estado de Enlace) en el protocolo IS-IS o LSA (*Link State Advertisement*; Notificación del Estado de Enlace) en OSPF.
3. El LSA inunda el dominio o área del *router.*
4. Cada *router* del dominio guarda la más reciente LSA de cada uno de los otros *routers.*
5. Cada *router* ahora tiene una descripción completa de la topología actual del área a la que pertenece y puede ahora computar las rutas más cortas a cada destino dentro de la misma.
6. Conociendo la ruta más corta a cada destino, el *router* crea una tabla de enrutamiento para cada tipo de métrica que utilice.

Un datagrama que deba atravesar varias áreas, será manejado en forma independiente dentro de cada área, pero siempre utilizará la ruta más corta a través de ellas.

A diferencia del algoritmo vector distancia, éste envía actualizaciones solamente cada vez que se den cambios en la red y converge rápidamente ante eventos inesperados. La información que se intercambia es acerca del estado del enlace más no los contenidos de las tablas de enrutamiento, por esta razón los algoritmos de estado de enlace utilizan un menor número de recursos de red. El algoritmo estado de enlace encuentra el camino más corto en base a parámetros como la velocidad y capacidad de las líneas por lo que requiere un elevado

cálculo computacional en cada *router*. Todos los *routers* poseen la misma tabla, la cual describe la topología del área a la que pertenecen.

2.2. ESTUDIO DE LOS PROTOCOLOS DE ENRUTAMIENTO

Antes de estudiar en detalle cada uno de los protocolos de enrutamiento, se definirá de forma general el papel de estos protocolos.

2.2.1. FUNCIÓN DE LOS PROTOCOLOS DE ENRUTAMIENTO

Para permitir a cada una de las redes que conforman Internet intercambiar su información de enrutamiento y para definir sus políticas de intercambio de tráfico se ha creado el concepto de *Sistema Autónomo* (AS, *Autonomous System*). Un Sistema Autónomo es visto como una colección de subredes interconectadas mediante un conjunto de *routers* y que es administrado por una autoridad administrativa común, que tiene un protocolo de enrutamiento homogéneo para el intercambio de información y que posee una política común de intercambio de tráfico con otros sistemas autónomos.

Normalmente cada ISP constituye su propio sistema autónomo.

De esta manera, dentro de Internet se dan dos niveles jerárquicos de enrutamiento: aquel que se realiza dentro de un sistema autónomo AS conocido como ***enrutamiento interno*** y aquel que se realiza entre sistemas autónomos conocido como ***enrutamiento externo***.

Los protocolos de enrutamiento que se utilizan en el primer caso se denominan protocolos de enrutamiento internos o IGP (*Interior Gateway Protocol*; Protocolo de Pasarela Interior), y los protocolos utilizados en el segundo caso se denominan protocolos de enrutamiento externos o EGP (*Exterior Gateway Protocolo*; Protocolo de Pasarela Exterior).

Un ***protocolo de enrutamiento interior*** es aquel cuya tarea principal es descubrir la actual topología de la red sobre la cual está operando, luego debe distribuir esta información entre los *routers* del Sistema Autónomo al cual pertenece y entonces calcular las rutas óptimas para el traslado de los paquetes a través de la red en base a diversos factores o ***métricas*** como son: costo, distancia, congestión, etc. Esta información luego es cargada en las tablas de enrutamiento. Los protocolos de enrutamiento por consiguiente deben responder rápidamente a los cambios que se den en la topología interna de un AS tales como: adición de nuevos circuitos o *routers*, eliminación de componentes, etc.

Un ***protocolo de enrutamiento exterior*** no pretende dar a conocer la topología interna de un AS a otro, todo lo contrario. La intención de un protocolo de enrutamiento exterior es permitir el intercambio de información de enrutamiento entre varios Sistemas Autónomos sin dar a conocer explícitamente los caminos internos utilizados. Un EGP, más que encontrar la ruta óptima, realiza enrutamiento obedeciendo a razones de tipo económico, administrativo, político, etc; ya que lo que pretende este tipo de protocolos es el intercambio de información entre redes que pertenecen a organizaciones diferentes. Durante mucho tiempo el EGP ha sido el protocolo utilizado a la hora de realizar enrutamiento exterior; actualmente el BGP elimina muchas de las restricciones y limitaciones del EGP y por consiguiente está creciendo rápidamente.

Un *router* IP no está obligado a operar un único protocolo de enrutamiento, y múltiples protocolos de enrutamiento pueden estar activos al mismo tiempo. No importa cuantos procesos de enrutamiento se estén ejecutando simultáneamente, el *router* mantiene una única tabla de enrutamiento IP para tomar decisiones de conmutación.

2.2.2. PROTOCOLOS DE ENRUTAMIENTO INTERIOR

Entre los protocolos de enrutamiento interior se puede mencionar a los siguientes: RIP, HELLO, que utilizan el algoritmo vector distancia, IGRP y EIGRP utilizan una

combinación del algoritmo vector distancia y estado de enlace, y OSPF e IS-IS que utilizan el algoritmo estado de enlace. El protocolo HELLO, es un protocolo importante en la historia de Internet que utiliza el algoritmo vector distancia con una métrica basada en los retardos, sin embargo por ser un protocolo obsoleto no se lo tratará en este proyecto de titulación.

2.2.2.1. RIP

RIP (*Routing Information Protocol*, Protocolo de Información de Enrutamiento) es uno de los protocolos de enrutamiento más antiguo y más simple, derivado del protocolo de enrutamiento de XNS (*Xerox Network Systems*, Sistemas de Red de Xerox).

RIP utiliza UDP (*User Datagram Protocol*; Protocolo de Datagramas de Usuario) como protocolo de transporte o ruteo.

RIP, clasifica a todas las máquinas participantes (*hosts* y *routers*) como: activas y pasivas. Los *routers* son los ***elementos activos*** encargados de anunciar sus rutas tanto a *hosts* como a *routers*, y los *hosts* son los ***elementos pasivos*** que solamente actualizan sus tablas en base a los anuncios de los *routers*. De esta manera, solamente un *router* puede correr RIP de modo activo, y un *host* correrá RIP de modo pasivo.

RIP utiliza una métrica de ***conteo de saltos*** para medir la distancia hacia un destino. El número de saltos a lo largo de una trayectoria se refiere al número de *routers* que un datagrama atravesará a lo largo de su camino hasta llegar a su destino.

Para que un *router* pueda anunciar sus rutas a sus vecinos, debe enviar mensajes con información tomada de sus tablas de enrutamiento actualizadas. Estos mensajes están formados por varios pares (*a,b*), donde: *a* es la dirección IP de la red destino y *b* un número entero que indica el número de saltos hacia esta red.

Los mensajes RIP se envían en datagramas UDP dirigidos al puerto 520 y utilizan 20 octetos por ruta (sin contar los 20 de IP y los 8 de UDP), es decir, cada mensaje puede tener un máximo de 25 pares o rutas y conserva una longitud no superior a los 512 bytes por mensaje.

Un *router* que habla RIP, difunde sus mensajes periódicamente (cada 30 segundos) vía *broadcast* a todos sus vecinos (tanto activos como pasivos) para que éstos actualicen sus tablas. Este proceso se lleva a cabo según el algoritmo vector distancia descrito anteriormente.

Sin embargo, cuando un *router* falla o un enlace cae, RIP debe ser capaz de invalidar dichas rutas de las tablas (paso 5 del algoritmo vector distancia), para lo cual este protocolo define un intervalo de tiempo de 180 segundos entre *broadcasts* (el envío de los mensajes con información de enrutamiento se realiza cada 30 segundos) al cabo del cual, si no se ha recibido anuncios de rutas del *router* emisor, se invalidan todas las rutas que fueron recibidas de dicho *router*.

Uno de los defectos de RIP es que satura la red con *broadcast* innecesario; además, la métrica que utiliza no toma en cuenta otros aspectos importantes como: capacidad de las distintas redes, confiabilidad, carga, etc., de esta manera la selección de la ruta que tenga menor número de saltos, no necesariamente es la más corta ni la más rápida.

RIP además no presta ningún tipo de servicio para garantizar que las actualizaciones de las tablas provengan de *routers* autorizados, por lo que este protocolo se torna inseguro.

Otro de los principales problemas de RIP es el mismo del que sufren todos los protocolos que utilizan el algoritmo vector distancia, éste es la convergencia lenta que ya fue explicado. RIP ha establecido un conteo de saltos igual a 16 como equivalente a infinito que significa que la red es inalcanzable, así se mejora el problema de convergencia lenta pero no se lo elimina. Por esta razón RIP es

inadecuado para grandes redes ya que este protocolo limitaría el diámetro de una red a menos de 16 saltos.

Para resolver el problema de conteo a infinito, RIP utiliza varias técnicas como: *triggered updates* (actualizaciones activadas), *hold down* (mantener abajo), *split horizont update* (actualización de horizonte separado) y *poisoned reverse* (antídoto).

Triggered updates obliga a un router a que envíe un mensaje de actualización inmediatamente después de haber detectado la remoción de alguna ruta debido a la falla de un *router* o de un enlace, en lugar de esperar el próximo período de difusión. Con esta técnica se consigue disminuir el tiempo en que un *router* es vulnerable.

Cuando los *routers* vecinos reciben estos mensajes de actualización, inmediatamente ellos envían nuevas actualizaciones a sus vecinos anunciando que la ruta ya no es utilizable, de manera que se dispara una ola de actualizaciones. *Triggered updates* sería suficiente si se garantizara que esta ola de actualizaciones alcanzará a todos los *routers* inmediatamente. Sin embargo existen dos problemas: primero, los paquetes de actualización pueden sufrir algún daño en el trayecto y segundo, esta técnica no sucede instantáneamente. De manera que es posible que un *router* que no ha recibido todavía las actualizaciones, emita su tabla de enrutamiento causando la reinserción de una ruta incorrecta.

La técnica conocida como ***hold down*** intenta resolver este problema obligando a los *routers* participantes a ignorar información acerca de una ruta durante un tiempo fijo luego de la recepción de un mensaje que afirma que dicha ruta es inaccesible. Este período de tiempo se establece en 60 segundos para RIP. La *idea* es esperar lo suficiente como para asegurar que todas la máquinas reciban las malas noticias y no acepten un mensaje erróneo.

La técnica ***split horizont update*** registra la interfaz por la cual ha recibido una

determinada ruta y no difunde información sobre dicha ruta a través de la misma interfaz. *Split horizont* previene la formación de lazos entre *routers* adyacentes.

Poisoned reverse evita la formación de grandes lazos y trabaja de la siguiente manera. Una vez que una ruta ha desaparecido, el *router* anuncia la ruta conservando la entrada de información por varios períodos de actualizaciones pero incluye un costo infinito en la difusión.

2.2.2.2. RIP v2

RIPv2 (*Routing Information Protocolo version* 2; Protocolo de Información de Enrutamiento versión 2) es una versión actualizada de RIP v1 diseñada para aliviar sus limitaciones, siendo al mismo tiempo muy compatible con su predecesor.

RIP v2 añade soporte para direcciones de red sin clase, para lo cual hace uso de uno de los campos que no fueron utilizados en el formato del paquete de RIP para transportar una máscara de red y una dirección del siguiente salto por cada entrada de red. Esto permite a RIP v2 transportar rutas sin clase para de esta manera poder trabajar adecuadamente en un entorno de direcciones sin clase.

Aunque RIP v2 utiliza el algoritmo básico de RIP v1, adopta características nuevas muy importantes como las siguientes:

Identificador de rutas externas: Permite difundir información sobre rutas adquiridas con otros protocolos de enrutamiento sin alterarla. Su objetivo principal es separar rutas internas (rutas de la red que utiliza RIP) de rutas externas que utilizan otros protocolos de enrutamiento como EGP o BGP.

Máscaras de Subred: Permite trabajar con rutas de subredes, solucionando de esta manera el gran problema de RIP v1 que no disponía de esta característica.

Dirección del siguiente salto: En cada ruta de un mensaje RIP se especifica además del número de saltos para llegar a la IP destino (como se hace en RIP v1) la dirección IP del siguiente *router* al que pueden ser enviados los paquetes, en lugar de utilizar el *router* que genera el mensaje.

Autenticación: Aporta mecanismos para que un router solo acepte mensajes RIP tras una autenticación de una clave con el objetivo de aumentar la seguridad de acceso a los *routers*.

***Multicasting*:** Los paquetes de RIP v2 no son enviados a la dirección de *broadcast* como en RIP v1 sino que se envían a una dirección IP en concreto de clase *multicast*. Solo los *routers* activos con RIP v2 hacen caso de lo recibido por esta dirección *multicast*, es decir, funciona como si se tratara de un *broadcast* selectivo.

Un mensaje RIP v2 generado por un *router* dado, contiene una dirección IP del destino de red o máquina que se puede alcanzar desde el *router*, su correspondiente máscara de subred, la dirección IP del siguiente salto o *router* al que deberían enviarse los paquetes y al número de saltos necesario para alcanzar el destino (métrica).

Cuando se inicia el proceso de actualización de la tabla de rutas en un *router* con RIP v2 instalado, se envían *solicitudes RIP* por todas las interfaces activas reclamando entradas de rutas de los *routers* adyacentes. Los *routers* que las reciben envían la información de sus correspondientes tablas de enrutamiento mediante mensajes RIP de respuesta. Además, en cada *router* con RIP, cada 30 segundos, una parte o la totalidad de la tabla de encaminamiento es enviada a los *routers* adyacentes a través de la dirección *multicast* de RIP v2 o al otro lado de una conexión punto a punto.

Cuando un *router* que acepta mensajes RIP v2 por la dirección de *multicast* recibe un mensaje, examina sus rutas para comprobar si debe actualizar su tabla. Si aparece una ruta referente a un destino que no conoce, o que permite alcanzar un

destino del cual ya se tenía ruta dinámica, aunque a través de un mayor número de saltos que usando como *gateway* el *router* del cual proviene el paquete RIP, procede a actualizar su tabla.

Ni RIP v1 ni RIP v2 son adecuados para ser utilizados como IGPs en un sistema autónomo en el cual el número de saltos es mayor que 16. Los protocolos que utilizan el algoritmo estado de enlace como OSPF o IS-IS proporcionan una solución de enrutamiento más adecuada para redes mucho más largas.

2.2.2.3. IGRP

A inicios de los años 80, la selección de un protocolo de enrutamiento interior fue efectivamente centrada en RIP, pero las redes fueron creciendo y las limitaciones de este protocolo se hicieron presentes. IGRP (*Interior Gateway Routing Protocol*; Protocolo de Enrutamiento de Pasarela Interior) es un protocolo de enrutamiento interior desarrollado por *Cisco Systems*, principal fabricante de *routers* del mundo, como respuesta al requerimiento de un protocolo de mayor capacidad de enrutamiento.

Existen características en las implementaciones de Cisco que permiten que IGRP sea usado como un EGP en algunas circunstancias; sin embargo, en este capítulo se lo analizará como IGP.

Al igual que RIP, IGRP es un protocolo que permite a los *routers* construir su propia tabla de enrutamiento mediante el uso del algoritmo vector distancia. IGRP utiliza este algoritmo modificado principalmente en tres aspectos :

1. En lugar de utilizar una única métrica, utiliza un vector de métricas (o conjunto de métricas) para caracterizar el camino.
2. En lugar de seleccionar un único camino con la mejor métrica, el tráfico puede ser dividido y enviado entre varios caminos cuya métrica cae dentro de los rangos especificados, para lo cual IGRP introduce el concepto de

varianza que se lo verá más adelante.

3. Muchas características son introducidas para proveer estabilidad en situaciones donde la topología está cambiando. Estas características pretenden prevenir la formación de lazos y el efecto de la cuenta al infinito que son los problemas que ocasiona el uso del algoritmo vector distancia. Éstas son: *hold downs, triggered updates, split horizont y poisoning.*

Vector de métricas

IGRP utiliza un vector compuesto por las siguientes métricas: retardo, ancho de banda, confiabilidad y ocupación del canal (carga).

Retardo es el tiempo que toma un paquete en llegar a su destino asumiendo una red descargada, es decir, es la suma de todos los retardos de los enlaces que conforman el camino; por supuesto, existe retardo adicional cuando la red está cargada. El ancho de banda de la ruta es simplemente el mínimo ancho de banda de entre todos los enlaces que conforman el camino. La confiabilidad indica la tasa de error y es la fracción de paquetes que llegarán a su destino sin daño. La ocupación del canal indica que cantidad del ancho de banda está actualmente en uso, la cual varía de acuerdo a la carga.

Hay que notar que el ancho de banda y el retardo, están en función de la tecnología de la red y pueden ser configurados por el operador; en cambio la confiabilidad y la ocupación del canal son valores que varían con el tiempo y deben ser recalculados periódicamente por el router.

Basado en la información de todas estas métricas, IGRP calcula una sola métrica combinada para caracterizar una ruta. Esta nueva métrica combina el efecto de todas la métricas anteriormente mencionadas en un único número que representa la *bondad* del camino. Un *router* calcula este valor haciendo uso de la siguiente ecuación:

$$Métrica = \left[\left(\frac{K1}{Be}\right) + K2 \times D\right] \times R$$

Ec 1. Ecuación para el cálculo de la métrica combinada en IGRP[1]

Donde: K1, K2= constantes
Be= ancho de banda efectivo
D= retardo
R= confiabilidad

Las constantes K1 y K2 indican la prioridad (*weight*; peso) asignados al ancho de banda y al retardo respectivamente. Esta prioridad dependerá del tipo de servicio; por ejemplo, el tráfico en tiempo real normalmente tendrá un *weight* más elevado para el retardo.

El ancho de banda efectivo Be está dado por:

$$Be = (\textit{ancho de banda del camino sin carga}) * (1 - \textit{ocupación del canal})$$

El ancho de banda del camino sin carga es el ancho de banda inverso en Kbps escalado por un factor de 10^7. La ocupación del canal es el porcentaje del canal que se encuentra con carga y está dada como una fracción de 255, es decir 255 corresponde al 100%.

El retardo D está expresado en decenas de microsegundos. Esto abarca retardos dentro del rango de 10 µs a 168 segundos[2].

La confiabilidad R es el porcentaje de los datos transmitidos que son exitosamente recibidos en el siguiente salto y también está expresada como una fracción de 255.

IGRP provee un amplio rango para estas métricas; por ejemplo: confiabilidad y carga pueden tomar valores entre 1 y 255, el ancho de banda puede tomar

valores que reflejan velocidad desde 1200 bps hasta 10 Gbps, mientras el retardo puede tomar valores desde 1 hasta 2^{24} que son valores expresados en decenas de microsegundos.

En base a esta métrica combinada, IGRP selecciona la mejor ruta para un paquete, ésta será aquella que tenga la métrica combinada más pequeña.

Varianza

IGRP incluye el concepto de varianza o balanceamiento de carga, lo cual permite que el tráfico sea dividido entre rutas de diferentes métricas.

Cuando la varianza V es igual a 1, IGRP envía el tráfico únicamente por la mejor ruta, es decir, aquella de mínima métrica; sin embargo, si dos rutas tienen igual valor de métrica, el tráfico será dividido equitativamente.

Incrementando el valor de la varianza se permite que el tráfico sea dividido entre la mejor ruta y otras que sean aproximadamente buenas y que se encuentren dentro de un determinado rango. Por ejemplo, para una varianza V=1, si una ruta *A* tiene una métrica de 20 y una ruta *B* tiene una métrica de 40, IGRP seleccionará la mejor ruta, es decir, M=20. Con varianza V=2, se incrementa la mínima métrica a 40 (V * M), lo cual significa que ahora el *router* puede seleccionar no solo la ruta con menor métrica para enviar paquetes sino todas aquellas rutas cuyas métricas estén en el rango comprendido entre M y V*M (en este caso, entre 20 y 40). Esto significa que IGRP repartirá su tráfico entre las rutas anteriores de la siguiente manera:

- Para la ruta A: 40/20 = 2
- Para la ruta B: 40/40 = 1

Es decir, por la ruta A se enviará el doble de paquetes que por la ruta B. Si el resultado de la relación anterior no fuera un número entero, IGRP lo aproximará al entero más cercano.

Sin embargo, existen algunos problemas con el concepto de varianza; por esta razón en la publicación 8.2 de Cisco, esta característica no es implementada, es decir, este valor está permanentemente seteado a 1.

Cuando un *router* desea enviar un paquete a un destino, compara la métrica combinada remota del siguiente salto con su métrica combinada local, si la métrica remota es menor que la métrica local, entonces envía el paquete. Una ruta cuya métrica combinada remota es más grande que su métrica combinada local es una ruta cuyo siguiente salto está muy alejado del destino. Este tipo de rutas son conocidos como rutas *upstream.* Utilizando este método, nunca se escogerá una ruta *upstream* para enviar un paquete; sin embargo, cuando se utiliza un valor de varianza mayor que 1, es posible que algunas de las rutas utilizadas sean *upstream.*

Características de estabilidad

Estas características son diseñadas para impedir que los *routers* seleccionen rutas erróneas para enviar sus paquetes, lo cual puede suceder cuando una ruta llega a ser inutilizable debido a una falla del *router* o de la red.

En principio, los *routers* adyacentes detectan la falla. Ellos entonces envían actualizaciones de enrutamiento que indican que la antigua ruta es inutilizable. Sin embargo, es posible que estas actualizaciones no alcancen algunas partes de la red completamente o que se demoren en alcanzar ciertos *routers*. Un *router* que todavía cree que la vieja ruta es buena puede continuar enviando esta información, de esta manera reingresará la ruta fallida al sistema.

Para evitar estos problemas, IGRP utiliza 4 técnicas: *hold downs, triggered updates, split horizont* y *poisoning*. Estas técnicas ya fueron analizadas en la sección 2.2.2.1.

La publicación 8.2 de Cisco, provee la opción de deshabilitar *hold downs* ya que presenta la desventaja de generar un retardo en la adopción de una nueva ruta

cuando una vieja ruta ha fallado. Con los parámetros por *default,* puede tomar varios minutos antes que un *router* adopte una nueva ruta después de un cambio.

A fin de evitar el conteo a infinito que podría causar la remoción de esta técnica, se utiliza una versión más fuerte de *poisoning*, la cual está basada en un conteo de saltos. Si el conteo de saltos para una ruta determinada incrementa, la ruta será removida. Este procedimiento obviamente removerá rutas que todavía sean válidas; si esto sucede, éstas serán reinstaladas en el siguiente mensaje de actualización y causarán un *triggered updates* que reinstalará la ruta en el sistema.

Otras características

Existe otra información adicional que no es parte del vector de métricas pero es mantenida en las tablas de enrutamiento a fin de caracterizar a una ruta, ésta es: el conteo de saltos y MTU (*Maximum Transmissión Unit*; Unidad de Transmisión Máxima) de cada red.

El conteo de saltos es simplemente el número de *routers* que un paquete tendrá que atravesar hasta llegar a su destino. MTU es el máximo tamaño del paquete que puede viajar a través de todo el camino hasta su destino sin necesidad de ser fragmentado, es decir, es el mínimo de todos los MTUs de todas las redes involucradas en el camino.

Adicionalmente a estas entradas, el algoritmo de enrutamiento requiere que sean configurados valores de otros parámetros importantes como: *timers*, valor de la varianza, y si la técnica de *hold down* está habilitada o no.

En IGRP existen 4 constantes de tiempo (*timers*) que son valores críticos en el control de propagación de las tablas de rutas y expiración de las mismas. Estos timers son: *Broadcast Time*, *Invalid Time*, *Hold Time* y *Flush Time*. Estas constantes de tiempo pueden ser seteadas por el administrador del sistema o usar sus valores por *default*.

En IGRP, los *routers* difunden periódicamente su tabla de enrutamiento (a intervalos regulares de tiempo) mediante *broadcast* a todos sus *routers* vecinos. A diferencia de RIP, IGRP utiliza un intervalo de 90 segundos llamado *Broadcast Time* para enviar mensajes de actualización de las tablas.

IGRP trabaja con un parámetro denominado *Invalid Time*, el cual especifica cuánto tiempo un *router* podría permanecer sin recibir mensajes de actualización sobre una específica ruta antes de declararla inválida. Este tiempo es 3 veces el tiempo de *broadcast*.

Una vez que una ruta ha sido invalidada, transcurre un período de tiempo denominado *Flush Time,* al final del cual esta ruta es removida de la tabla de enrutamiento. Su valor es 7 veces el tiempo de *broadcast*.

Cuando un destino ha llegado a ser inaccesible, dicho destino pasa al estado *hold down*. Durante este estado ninguna nueva ruta será aceptada para este destino. El *Hold Time* indica cuánto tiempo este estado debe durar. El valor por defecto es 3 veces el tiempo de *broadcast* más 10 segundos.

La diferencia entre *invalid time* y *flush time* es que una vez que el *invalid time* invalida una ruta hacia un destino, esta ruta permanece en la base de datos con el objeto de implementar *hold down. Flush time* indica cuánto tiempo debería pasar antes de que una ruta deba ser eliminada de la tabla de enrutamiento.

2.2.2.4. EIGRP

Conviene destacar que tanto IGRP como EIGRP son protocolos propietarios de Cisco, y no hay implementaciones para equipos de otros fabricantes, por lo que el uso de estos protocolos requiere que todos los *routers* del sistema autónomo correspondiente sean de Cisco. Los *routers* Cisco también pueden funcionar con protocolos estándar, tales como RIP y OSPF.

EIGRP (*Enhanced Interior Gateway Routing Protocol;* Protocolo de Enrutamiento de Pasarela Interior Mejorado) introduce mejoras importantes a IGRP pero sigue utilizando el algoritmo vector distancia.

Al igual que IGRP, este protocolo utiliza balanceamiento de carga para rutas de igual costo y el concepto de varianza para dividir el tráfico entre caminos de diferentes costos.

En EIGRP, los *routers* deben descubrir si sus vecinos están operativos o si son inalcanzables. Para ello, los *routers* envían paquetes *hello* cada 5 segundos en enlaces con alto ancho de banda (medios *broadcast* como: *Token Ring*, FDDI, etc) y cada 60 segundos en enlaces multipunto de bajo ancho de banda (circuitos virtuales conmutados, enlaces BRI de ISDN, etc). Mientras los paquetes *hello* son recibidos, un *router* puede determinar si su vecino está operativo y entonces puede intercambiar información de enrutamiento.

Para distribuir dicha información de enrutamiento a través de una red, EIGRP envía mensajes de actualización no periódicos (paquetes *update*), es decir, IGRP solamente envía actualizaciones cuando alguna ruta ha cambiado. Cuando estos cambios ocurren, EIGRP no envía dentro de sus mensajes de actualización toda la tabla de rutas como lo hace RIP e IGRP sino solamente aquellas rutas que han sufrido algún cambio. Esta es una razón por la que se dice que EIGRP hace bajo uso de los recursos de red.

Un *router* corriendo un típico protocolo de enrutamiento que utiliza el algoritmo vector distancia (como RIP), recibe la tabla de enrutamiento de un *router* vecino, compara estas rutas con las rutas locales y actualiza sus tablas solamente si la métrica recibida es más baja que la métrica almacenada; caso contrario la ruta recibida es eliminada. EIGRP, en lugar de descartar estas notificaciones, las guarda y construye una segunda tabla denominada tabla topológica. Este método garantiza que los tiempos de convergencia sean mucho más cortos, ya que cuando un enlace falla, EIGRP solamente buscará en su tabla topológica un camino alterno que pueda transportar el tráfico hacia el mismo destino y la

instalará en su tabla de enrutamiento. Esto no ocurre con RIP, ya que cuando un enlace falla, se tiene que esperar un nuevo período de 90 segundos y hasta 120 segundos para que un *router* pueda encontrar una nueva ruta.

La tabla topológica contiene la información necesaria para construir un conjunto de vectores (destinos) y distancias (métricas) para cada una de las redes accesibles, esta información incluye: mínimo ancho de banda *ab* (seleccionado de entre todos los tramos que conforman el camino hacia un destino), retardo total *d* (suma de los retardos de cada uno de los tramos que conforman el camino hacia un destino), confiabilidad y carga de la ruta, mínimo MTU, distancia factible (*feasible distance*) y distancia reportada (*reported distance*). Estos dos últimos términos serán explicados más adelante.

EIGRP escala el ancho de banda *ab* y el retardo *d* de la siguiente manera:

$$AB = \frac{10^7}{ab} * 256$$

$$D = d * 256$$

Las unidades para el mínimo ancho de banda *ab* están dadas en Kbps y las unidades del retardo total *d* están dadas en decenas de microsegundos.

EIGRP utiliza estos valores escalados para computar el valor de la métrica haciendo uso de la siguiente fórmula:

$$Métrica = \left[K_1 * AB + \frac{K_2 * AB}{256 - L} + K_3 * D \right] * \left[\frac{K_5}{R + K_4} \right]$$

Ec.2 . Ecuación para el cálculo de la métrica en EIGRP [3]

Donde: K =constantes
AB= ancho de banda escalado
L =carga

D =retardo escalado

R =confiabilidad

Los valores por defecto para las constantes K son: K1=1, K2=0, K3=1 y K4=0. Cuando K5=0 el término de confiabilidad no es incluído, de manera que la fórmula simplificada para calcular la métrica de una ruta sería:

$$Métrica = \left(\frac{10^7}{ab} + d \right) * 256$$

Ec.3. Ecuación simplificada [3]

Algoritmo DUAL

El algoritmo DUAL (*Diffusing Update Algorithm*; Algoritmo de Difusión de Actualización) utiliza el concepto de distancia factible y distancia reportada para seleccionar rutas cortas y eficientes (libres de lazos) llamadas sucesores factibles que serán luego insertadas en la tabla de enrutamiento.

Si un *router* tiene varias posibilidades de rutas para llegar a un mismo destino, escoge aquella ruta que tenga la mejor métrica, es decir, aquella de menor métrica y envía por allí el tráfico. La mejor métrica es denominada distancia factible (*feasible distance*).

La distancia reportada (*reported distance*) como su nombre lo indica, es la métrica reportada por un vecino a un determinado *router*.

Un sucesor factible (*feasible sucesor*) es una ruta cuya distancia reportada es menor que la distancia factible. Como se dijo anteriormente, EIGRP no descarta la información recibida de sus vecinos, más bien la almacena para de entre este conjunto de rutas escoger los sucesores factibles.

La cantidad de tiempo que un *router* considerará a un vecino como operativo es denominada *hold time*. Si dentro de este intervalo, un *router* no recibe paquetes

hello de un determinado vecino, se declarará al enlace inválido. El valor por defecto para este intervalo de tiempo es típicamente tres veces el intervalo *hello*, es decir, 15 segundos para enlaces de alto ancho de banda y 180 segundos para enlaces de bajo ancho de banda.

Una vez que ha expirado el *hold time*, el algoritmo DUAL chequea si existen sucesores factibles que puedan reemplazar al enlace principal, si hay sucesores factibles envía inmediatamente el tráfico a través de alguno de ellos, acortando de esta manera el tiempo de convergencia.

Si un *router* siempre tiene sucesores factibles permanece entonces en el estado *Pasivo*, pero si no los tiene pasa al estado *Activo* y empieza el recómputo de una nueva ruta a fin de determinar un sucesor. El tiempo que toma el recómputo de la nueva ruta afecta el tiempo de convergencia.

Cuando un *router* ha pasado al estado *Activo,* es decir no tiene sucesores factibles, pero tiene *routers* vecinos a través de los cuales puede llegar a su destino, el *router* envía paquetes *multicast* denominados *query* a sus vecinos a fin de averiguar si existe una ruta alternativa para alcanzar su destino. Una vez que un vecino ha recibido un *query* busca la información solicitada en su tabla topológica. Si existe tal información, envía un paquete *unicast* dirigido exclusivamente al *router* que originó el *query* informándole que sí existe un sucesor factible, este paquete es llamado *reply*. Tanto los paquetes *query* como los *reply* son transmitidos de forma confiable, es decir, son confirmados mediante ACKs.

Si no existe la información solicitada, el vecino que recibió el *query* envía a su vez otros paquetes *query* a sus vecinos (excepto al inicial originador del *query*). De esta manera el *router* puede encontrar un nuevo sucesor o declarar ese destino como inaccesible.

En resumen se podría decir que entre las mejoras que EIGRP ofrece con respecto a IGRP y RIP están las siguientes:

- Cuando sucede algún cambio en la topología de la red, solamente dichos cambios son propagados, ya no la tabla completa, esto reduce la carga del protocolo de enrutamiento.
- Los tiempos de convergencia para los cambios en la topología de la red son mucho más rápidos; en algunos casos la convergencia puede ser casi instantánea.
- EIGRP hace uso de un algoritmo DUAL (*Diffusing Update Algorithm*; Algoritmo de Difusión de Actualización), para calcular la ruta más corta a un destino dentro de una red evitando la formación de lazos.

2.2.2.5. OSPF

El término OSPF (*Open Shortest Path First*; Primero la Ruta más corta Disponible) se usa para referirse a la versión 2 de dicho protocolo, ya que OSPF v1 es ya obsoleto. Se trata de un estándar abierto y público, por lo que cualquier persona lo puede implementar sin pagar licencia por su uso.

Este es un protocolo de enrutamiento interior que utiliza el algoritmo estado de enlace para hacer una descripción completa del estado de cada enlace que tiene un *router* con sus vecinos. Esta descripción del enlace incluye parámetros muy importantes como son la dirección IP de la interfaz del vecino y su máscara, el tipo de red a la cual está conectado, su costo y un tiempo de vida o período de convergencia. El conjunto de todos estos estados forman la base de datos de los *routers*.

OSPF es un protocolo autoadaptativo, es decir, reacciona de manera automática y rápida ante los cambios que se suscitan en un sistema autónomo tales como fallas en las interfaces del *router*, caída de un enlace, etc, calculando nuevas rutas después de un período de convergencia. Este período de convergencia es corto e involucra un mínimo de tráfico de enrutamiento.

OSPF divide a un sistema autónomo en áreas. Un área es un conjunto de redes

contiguas y *host* agrupados mediante *routers*. La topología de un área permanece oculta (es invisible) para el resto de áreas del AS de manera que un *router* solo necesita conocer la topología e información de enrutamiento correspondiente a su área, esto significa que cada área tiene su propia base de datos topológica.

El objetivo de dividir un AS en varias áreas es minimizar el volumen de tráfico de enrutamiento requerido para gestionar la base de datos de un AS y por lo tanto minimizar los requerimientos de memoria de un *router* y el tiempo de cálculo de las rutas.

En OSPF se contemplan cuatro clases de *routers*:

***Routers* internos.-** Son aquellos cuyas interfaces pertenecen única y exclusivamente a un área. Cada uno de estos *routers* tienen una base de datos idéntica correspondiente al área a la cual pertenecen.

***Routers* frontera de área** (ABR; *Area Border Router*).- Son aquellos *routers* cuyas interfaces están en más de un área y por tanto las interconectan. Tienen una copia de la base de datos de cada área a la que están conectados. Siempre forma parte del *backbone* y son los responsables de la propagación de la información de enrutamiento inter-áreas entre las áreas que conectan.

***Routers* frontera de AS** (ASBR; *Autonomous System Border Router*).- Son aquellos que intercambian tráfico de enrutamiento con *routers* de otros ASs. Todos los *routers* de un sistema autónomo conocen el camino a todos los *routers* frontera de AS. Un *router* del tipo ASBR puede ser un *router* frontera de área ABR o un *router* interno.

***Routers* del Backbone.-** Son aquellos que tienen una interfaz conectada al *backbone* como los ABRs. Sin embargo, no todos los *routers* del *backbone* tiene que ser ABRs.

El enrutamiento dentro de un AS se da en dos niveles: enrutamiento intra-área (si el origen y destino del paquete están en la misma área) y enrutamiento inter-área (si el origen y el destino de un paquete están en distintas áreas).

En todo sistema autónomo hay al menos un área que se conoce con el nombre de *área 0* o *backbone.* El *backbone* está conformado por el conjunto de redes que no pertenecen a ninguna área, por los *routers* conectados a estas redes y por los *routers* que pertenecen a múltiples áreas a la vez (ABRs). Los elementos que conforman el *backbone* deben ser contiguos; en caso que esto no suceda, el administrador del sistema debe instaurar la conectividad mediante la configuración de enlaces virtuales. Los enlaces virtuales también pertenecen al *backbone*. El *backbone* tiene las mismas propiedades de un área, es decir, su topología es invisible al resto de áreas.

El *backbone* es el responsable del enrutamiento inter-áreas, es decir, todas las áreas que desean intercambiar información de enrutamiento entre ellas deben mantener conectividad con éste para lo cual deben tener al menos un *router* en el *backbone*.

Cuando un paquete tiene que viajar entre dos áreas, el camino que éste seguirá puede ser dividido en tres partes: un camino intra-área desde el origen hasta el *router* frontera de área, el camino del *backbone* y otro camino intra-área hasta el destino.

Cada *router* frontera de área está conectado al *backbone*. Cada ABR resume la topología de sus áreas enlazadas y las distribuye a través del *backbone* a otros ABRs, de esta manera, un ABR tiene una información topológica completa de todos los ABRs del sistema autónomo. A partir de esta información el *router* calcula las rutas a todos los destinos que no están contenidos en sus áreas enlazadas.

OSPF soporta varios tipos de redes físicas:

Redes punto a punto.- Son redes que enlaza un único par de *routers*. Un línea serial de 56 Kbps, es un ejemplo de red punto a punto.

Redes de *broadcast*.- Son redes físicas que soporta la conexión de múltiples *routers* con la capacidad de direccionar mensajes a todos los *routers* que la conforman. Se asume que cada par de *routers* de una red es capaz de comunicarse directamente. Por ejemplo: redes *Ethernet*, *Token Ring*, FDDI, redes de radio, etc.

Redes no *broadcast*.- Son redes físicas que soportan la conexión de múltiples *routers* pero no tienen la capacidad de hacer *broadcast*. X.25 es un ejemplo de red no *broadcast*.

Tanto las redes *broadcast* como las redes no *broadcast* son llamadas redes multiacceso.

Toda red multiacceso con al menos dos *routers* conectados tiene un *router* designado (DR; *Designated Router*) y un BDR (*Backup Designated Router*; *Router* Designado de Respaldo).

El *router* designado DR es el *router* encargado de formar adyacencias con los otros *routers* de la red, es decir, éste será quien determine qué *routers* llegarán a ser adyacentes.

Adyacencia es una nueva relación formada entre *routers* vecinos seleccionados con el fin de intercambiar información de enrutamiento para iniciar la base de datos topológica de la red. Solamente los *routers* adyacentes pueden intercambiar información de enrutamiento. No todos los pares de vecinos se vuelven adyacentes. El DR además, se hace adyacente a todos los *routers* pertenecientes a la red.

El BDR (*Backup Designated Router*; *Router* Designado de Respaldo), es un *router* de respaldo, el cual pasa a ser DR cuando el actual falla por cualquier

motivo.

Además de formar adyacencia, el *router* designado DR, es el único que puede enviar mensajes LSA (*Link State Advertisement*; Notificación del estado del enlace) a los otros *routers* de la red. Estos mensajes contienen información acerca de la identidad y costo del enlace de cada vecino. El conjunto de LSAs de todos los *routers* y redes forman la base de datos topológica del área.

A partir de esta base de datos, cada *router* construye un *shortest-path tree* (árbol mínimo de ruta) para lo cual el *router* ejecuta el algoritmo de Dijkstra, siendo dicho *router* la raíz del árbol. En la siguiente figura se muestra una red y su respectivo árbol mínimo de ruta siendo el *router* A la raíz. El árbol da la ruta a cualquier *host* o red de destino dentro del área lo cual será utilizado posteriormente para la construcción de la tabla de enrutamiento.

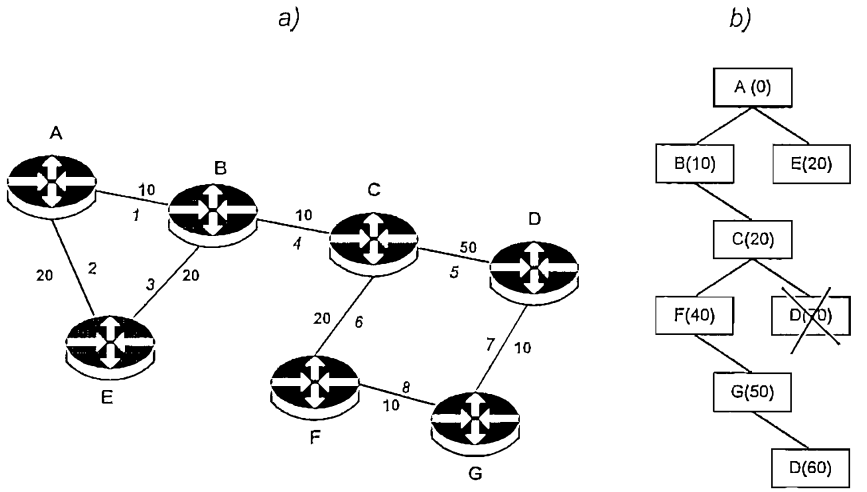


Fig. 2.1. a) Red OSPF b) Árbol con raíz en el router A [4]

OSPF utiliza el campo TOS (*Type of Service*; Tipo de Servicio) de los datagramas IP para calcular un conjunto de rutas separadas para cada TOS. Esto significa que para cada destino pueden existir múltiples rutas, una para cada TOS (retardo, confiabilidad, rendimiento, costo y seguridad). Con esta información OSPF calcula la ruta óptima para cada TOS por separado (así se tendrá la ruta óptima para mínimo retardo, máxima confiabilidad, etc). Cuando los costos de las interfaces varían basadas en TOS, se calcula un árbol de ruta mínimo para cada TOS. Sin embargo, con la finalidad de conservar espacio en las tablas de

enrutamiento, un *router* OSPF puede ser configurado para ignorar el campo TOS. En este caso el *router* calcula las rutas para TOS=0.

Si para un destino dado existe más de una ruta disponible con igual costo, OSPF proporciona balanceamiento de la carga, es decir, el tráfico es distribuido igualmente entre dichas rutas.

Una tabla de enrutamiento contiene entradas para cada destino (*host*, subred, red). Para cada destino existe información para uno o más tipos de servicio (TOS).

OSPF trabaja con cinco clases de paquetes: *Hello,* Descripción de la Base de Datos (DD; *Database Description)*, Solicitud del Estado del Enlace (LSR; *Link State Request)*, Actualización del Estado del Enlace (LSU, *Link State Update)* y Acuse de Recibo de Estado de Enlace (*Link State Acknowledge)*.

Cuando los *routers* OSPF se activan, envían y reciben paquetes *hello* periódicamente por todas sus interfaces, los mismos que son utilizados para descubrir a sus vecinos, mantener relaciones con ellos y de esta manera asegurarse que sus líneas permanecen operativas. Un *router* anuncia constantemente el estado de su enlace, por lo que la ausencia de un anuncio reciente indica a los vecinos del *router* que no está activo. Luego, el *router* intentará formar adyacencias con algunos de su vecinos recientemente adquiridos.

Los paquetes de Descripción de la Base de Datos y Solicitud del Estado del Enlace son utilizados en la formación de adyacencias.

Los *routers* intercambian paquetes de Descripción de la Base de Datos para iniciar sus bases de datos. Durante este proceso los dos *routers* forman un relación maestro/esclavo, en la cual el *router* que sirve como maestro envía paquetes DD (*pollings* o sondeos) mientras que el otro *router* que actúa como esclavo reconoce dichos paquetes y envía DDs como respuesta; este proceso se

denomina DEP (*Database Exchange Process;* Proceso de Intercambio de las Bases de Datos). Cada paquete de Descripción de la Base de Datos contiene una lista (posiblemente parcial) de notificaciones de estado de enlace o LSAs pertenecientes a la base de datos del *router*, por esta razón múltiples paquetes pueden ser necesarios para una descripción completa de la base de datos.

Luego de haber intercambiado paquetes de Descripción de la Base de Datos, el *router* puede descubrir que alguna parte de su base de datos está fuera de fecha. Los paquetes de Solicitud del Estado del Enlace son utilizados para solicitar que se le envíe información más actualizada de mensajes específicos desde la base de datos del vecino. De la misma forma que los paquetes DD, se puede requerir más de un mensaje de solicitud. El envío de paquetes de Solicitud del Estado del Enlace es el último paso en la formación de adyacencias.

Los paquetes de Actualización del Estado del Enlace son aquellos que implementan *flooding*[a] para asegurar que cada LSA se pase entre *routers* adyacentes para alcanzar a cada *router* del área. Cada paquete de Actualización del Estado del Enlace transporta un conjunto de LSAs un salto más allá de su origen. Muchos LSAs pueden estar incluidos en un único paquete de actualización.

Cuando en una red *broadcast* hay varios *routers* resulta ineficiente que cada uno intercambie paquetes de Actualización del Estado del Enlace con todos los demás ya que mucha de la información sería redundante. En este caso, OSPF prevé que uno de ellos pueda ser un *router* designado DR, siendo éste el único que intercambiará información con todos los demás para de esta manera optimizar el proceso de *flooding.*

Con el propósito de hacer el procedimiento de *flooding* confiable, se notifica la llegada de los paquetes de actualización a través de Acuses de Recibo del Estado

[a] *Flooding* o Inundación, es el proceso mediante el cual se envían paquetes por todas las interfaces excepto por las que se ha recibido.

del Enlace. Múltiples LSAs pueden ser confirmados con un único acuse de recibo.

Los paquetes de enrutamiento del protocolo OSPF, a excepción de los paquetes *hello* solamente son enviados una vez que se han formado adyacencias.

OSPF establece mecanismos de autenticación de los paquetes de enrutamiento, para evitar que un usuario malintencionado envíe mensajes engañosos a un *router*. Esto significa que solamente *routers* confiables pueden participar en el enrutamiento dentro de un sistema autónomo. Una variedad de esquemas de autenticación pueden ser usados, pero solo un único esquema de autenticación puede ser configurado para cada área.

2.2.3. PROTOCOLOS DE ENRUTAMIENTO EXTERIOR

Entre los protocolos de enrutamiento exterior existentes se puede mencionar: EGP-2 y BGP. Actualmente BGP-4 es el más difundido y por tal razón será objeto de estudio en este capítulo.

2.2.3.1. BGP-4

Es un protocolo de enrutamiento exterior y está diseñado para ser utilizado entre múltiples sistemas autónomos. BGP no impone restricciones a la topología fundamental de Internet. Además BGP asume que existe un protocolo de enrutamiento interno en los sistemas autónomos para los cuales él presta servicio, sin embargo, no asume nada acerca de cuáles son o qué hacen esos protocolos.

Antes de entrar en detalle es necesario clasificar los sistemas autónomos (AS) en tres tipos:

- *AS Terminal (Stub Terminal).-* Es un AS que tiene solo una conexión hacia otro AS, este tipo solo transporta tráfico local.
- *AS Multiconectado (Multihomed AS).-* Es un AS que tiene conexiones a varios AS pero por ningún motivo transporta tráfico en tránsito.
- *AS de Tránsito (Transit AS).-* Es un AS que tiene conexiones con varios AS y transporta tanto tráfico local como tráfico en tránsito.

La función primaria de los sistemas BGP es intercambiar la información sobre rutas de redes con otros sistemas BGP, tal Información es suficiente para construir grafos de conectividad entre los sistemas autónomos. Así mismo BGP provee nuevos conjuntos de mecanismos para el soporte de clases de inter-dominios enrutados, este mecanismo incluye el soporte para publicar prefijos de direcciones IP y eliminar el concepto de clases de red dentro de BGP.

Hay cuatro versiones de BGP, BGP-1 y BGP-2 descritos en los RFCs [1105] y [1163] están obsoletos. Para que exista interoperatividad entre BGP-3 y BGP-4, BGP define un mecanismo para que dos BGPs negocien una versión que ambos entiendan, utilizando el mensaje OPEN.

Para evitar los bucles, BGP-4 utiliza vectores camino (*path vectors*) como evolución de los vectores distancia:

- Cada red accesible se anuncia junto con la lista de AS que hay desde el *router* que la anuncia hasta esa red.
- Cuando se recibe un anuncio, si el AS del que lo recibe ya está en la lista del trayecto, se rechaza dicha ruta.

Con respecto al algoritmo utilizado por BGP no puede ser clasificado ni como un algoritmo de vector distancia puro ni como un algoritmo de estado de enlace puro dado que:

- El atributo *AS_path* (campo del paquete *update*) permite la reconstrucción de largas porciones de la topología lo que lo hace similar al algoritmo de

estado de enlace.

- Intercambiando solo las rutas utilizadas entre los pares, lo hace similar al algoritmo de vector distancia.

BGP soporta dos tipo de sesiones entre *routers* vecinos, la interna y la externa. La interna es llamada comúnmente iBGP, corre entre *routers* que se encuentren en un mismo sistema autónomo. Mientras que la externa eBGP, corre entre *routers* localizados en sistemas autónomos distintos.

A diferencia de OSPF, BGP es un protocolo situado sobre el nivel de transporte, es decir, los paquetes BGP son transmitidos encapsulados dentro de paquetes TCP. Esto permite asumir que el intercambio de información se realiza de forma confiable. Existen cuatro tipos de paquetes BGP a citar: *open*, *update*, *notification* y *keepalive*.

Para adquirir un vecino, un *router* establece primero una conexión TCP, para ello utiliza un ***mensaje open*** el cual identifica al AS (sistema autónomo) al que pertenece el emisor y suministra la dirección IP del *router*, si se rechaza al vecino se cierra la conexión.

Un ***mensaje update*** facilita dos tipos de información:

- Información sobre una ruta particular a través del conjunto de redes. Dicha ruta se incorpora a la base de datos de cada *router* que la recibe.
- Una lista de rutas que fueron previamente anunciadas por este *router*, y que ahora han sido eliminadas.

Estos dos tipos de información pueden ser proporcionadas simultáneamente en un único paquete, es decir, cada *router* mantiene una base de datos con las *subredes* que puede alcanzar y la ruta completa (preferida) para hacerlo. Siempre que se modifica esta base de datos, el dispositivo de encaminamiento notifica por medio de paquetes *update* (realiza difusión) a todos los demás dispositivos de encaminamiento que implementan BGP.

El ***mensaje notification*** es enviado por un *router* R_1 al *router* R_2 para explicar por qué rechaza la conexión a R_2.

El cuarto y último es el ***mensaje keepalive.*** Sirve para confirmar un mensaje *open* y confirmar periódicamente la relación de vecindad. Los mensajes *keepalive* se envían cada 60 seg. por defecto, las sesiones BGP usan un valor de *hold time* (tiempo de retención)[a] seteado comúnmente a 180 seg., es decir, seteado a un valor tres veces del intervalo *keepalive.* En una configuración sin mensajes *update*, BGP consume un ancho de banda de 3 bits/seg.

Inmediatamente después de la conexión inicial BGP, los parlantes BGP[b] intercambian un conjunto completo de información de enrutamiento, luego BGP utiliza actualizaciones incrementales para intercambiar solo las variaciones de información.

En BGP las ***rutas*** son definidas como una unidad de información para un destino y con atributos de camino para ese destino, es decir, está compuesta por la dirección IP y su prefijo así como el número de ASs para llegar al destino. Las rutas son anunciadas entre elementos BGP a través de mensajes *update* y luego son almacenadas en RIB (*Routing Information Bases*; Bases de información de Encaminamiento).

Cuando un elemento BGP resuelve anunciar una ruta, él debe adicionar o modificar los atributos de camino para la ruta antes de anunciarla. Existen también atributos para notificar que una ruta ya no está disponible:

- A través del campo *withdrawn routes* del mensaje *update.*
- A través de una ruta de sustitución.
- Cuando una conexión ha caído, el *router* elimina todas las rutas que pasan por el BGP remoto.

---

[a] Tiempo que tiene que esperar el receptor antes de asumir que el emisor ha caído al no recibir mensajes *keepalive o update.*

[b] BGP *speaker* (BGPs) es un sistema que ejecuta BGP.

El vector camino contiene una lista de los sistemas autónomos del trayecto. En la figura 2.2, AS1 origina la ruta para la red 10.1.0.0/17 para lo cual tiene que anexar el vector camino local (AS1) a los anuncios de ruta enviados a AS2 y AS3. AS2 anuncia la ruta para la red 10.1.0.0/17 pero con vector camino de (AS2,AS1) y así hasta llegar al destino, lo mismo realiza AS3. Ahora AS5 debe realizar una decisión sobre cual de los dos vectores caminos (AS4, AS2,AS1) o (AS3,AS1) aceptar; este proceso de selección de ruta se tratará más adelante.

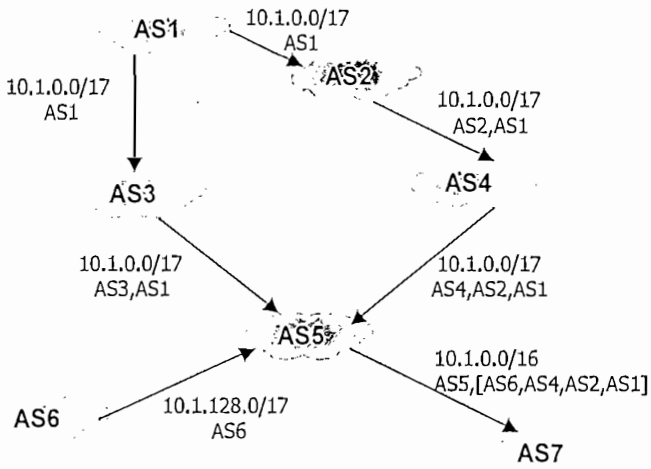


Fig. 2.2. Interacción de múltiples ASs.

Supóngase que AS5 ha escogido la ruta 10.1.0.0/17 con el vector camino (AS4, AS2,AS1). Para anunciar las rutas que contiene AS5 a AS7, AS5 procede a agregar la ruta 10.1.0.0/17 con el vector camino (AS4, AS2,AS1) con la ruta 10.1.128.0/17 originada en AS6 con camino AS6, dando como resultado una ruta 10.1.0.0/16 con el vector camino (AS5,[AS6,AS4,AS2,AS1]).

En el caso de que un anuncio contenga un vector camino con el mismo valor de AS del que lo recibe, entonces el *router* sabe que se ha dado lugar a un lazo y procede a borrar el anuncio.

Métricas de BGP

La métrica de BGP es una unidad arbitraria que especifica el *grado de preferencia*

de un camino particular. BGP utiliza el número de saltos de ASs como una métrica por defecto desde la fuente al destino AS, sin embargo, esto no siempre resulta óptimo y se utilizan métricas que son asignadas por el administrador de la red. Los grados de preferencia pueden basarse en diversos criterios tales como si es el enlace estable, rápido y confiable y otros factores como lo económico, seguridad, etc.

BGP trabaja con dos tipos de tablas: la tabla principal de rutas y la tabla BGP. La tabla de rutas contiene las mejores rutas a través de las cuales se puede alcanzar las redes aprendidas a través de un protocolo de enrutamiento interior, mientras que la tabla BGP posee solo las rutas recibidas vía BGP, con la existencia de estas dos tablas es posible tener caminos duplicados para alcanzar la misma red.

Lo anterior no quiere decir que si una ruta está en la tabla principal de rutas pueda ser anunciada vía BGP, ya que las tablas se encuentran lógicamente separadas. Igualmente es posible que las rutas estáticas en el *router* sean publicadas. Una de las características de BGP es que todas la rutas recibidas de un vecino con número de AS diferente al conocido (un par extremo), es informada a otros pares externos (pares eBGP) e internos (iBGP).

Proceso de selección de ruta

La base de este proceso es seleccionar la dirección de red más específica (prefijo más largo) que corresponde a la dirección destino. En el ejemplo anterior si AS7 tuviese además una conexión con AS4 entonces escogería la ruta 10.1.0.0/17 con vector camino (AS4, AS2,AS1). En el caso de que los anuncios tengan el mismo prefijo pero con diferentes vectores camino, BGP elige el camino con el menor número de saltos AS de tránsito, un ejemplo se puede ver cuando AS5 recibe dos rutas con el mismo prefijo pero con diferentes vectores camino para lo cual AS5 elige la ruta con vector camino (AS3,AS1).

Sin embargo, existen métodos que se pueden usar para alterar este proceso de selección, algunos de los métodos se listan a continuación:

Filtrado *AS path*.- En la figura 2.3, según el proceso de selección, AS3 escogería el camino (AS1,AS2) para llegar a AS2. Para direccionar el tráfico por AS5, es decir, alterando el proceso de selección se procede a filtrar los caminos entrantes de la forma (AS1,AS2), de manera que se acepte todas las rutas con vectores camino diferentes al anterior.

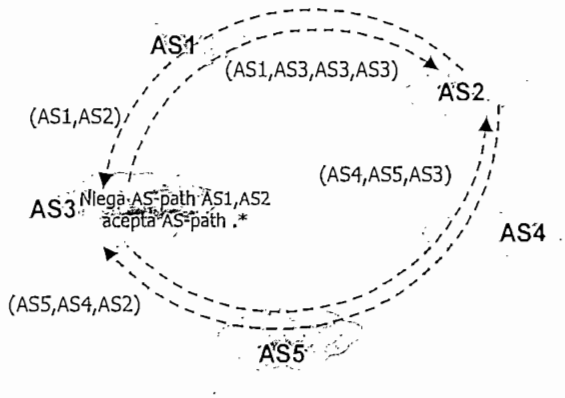


Fig. 2.3. Filtrado y alargamiento AS-path [4]

Alargamiento *AS path*.- En el caso anterior el flujo de tráfico en la dirección opuesta puede no obedecer la misma política, puesto que AS2 elegirá AS1 como tránsito para alcanzar AS3. Para que AS2 modifique esta selección AS3 inserta peticiones adicionales del AS originante en el vector camino (en este caso AS3 inserta dos peticiones de AS3 dando como resultado el vector camino (AS1,AS3,AS3,AS3)), de esta manera se consigue que AS2 seleccione el camino más largo (AS4,AS5,AS3). Este mecanismo se usa para definir caminos de respaldo.

El problema que se presenta en este mecanismo es que si algún AS de tránsito también implementa alargamiento de los caminos AS, el AS origen no se dará por enterado de esta situación de manera AS2 seguirá eligiendo AS1 como tránsito.

Inyección de rutas específicas.- Este método radica en anunciar una ruta adicional de mayor prefijo en el camino que se quiere tener como principal. En la figura 2.4 (a) AS3 anuncia la dirección de red 10.0.0.0/8 a AS2 para que use el camino (AS1,AS3) como respaldo y anuncia las rutas 10.0.0.0/8 y 10.128.0.0/9 a

AS5 para que AS2 use el camino (AS4,AS5,AS3) como primario ya que AS2 elegirá el camino más largo debido a la existencia de rutas más específicas dentro de la tabla de enrutamiento.

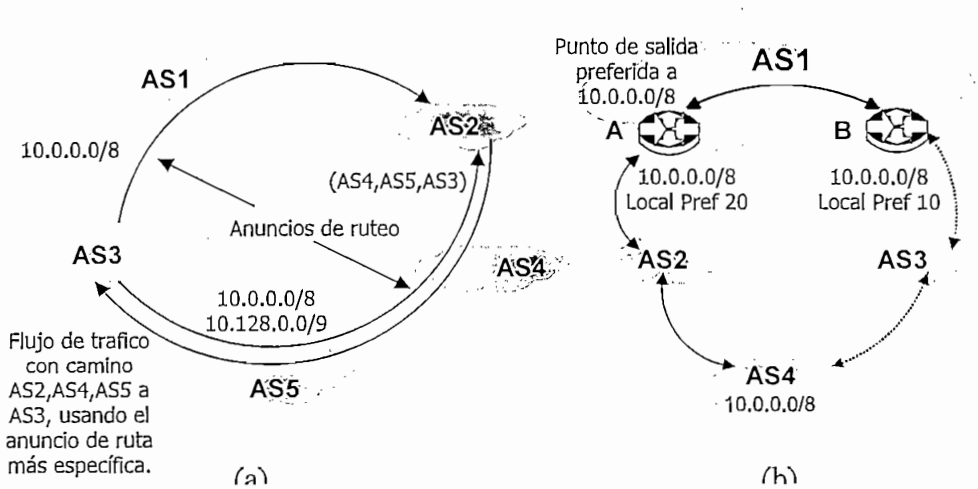


Fig. 2.4. (a) Selección de ruta específica y (b) Preferencia local BGP [4]

Preferencia local BGP.- Es un atributo de camino local el cual indica la preferencia que tiene una ruta, este atributo es implementado solo por *routers* que mantienen sesiones iBGP; ésta es una manera de garantizar de que estas preferencias sean divulgadas por todos *routers* BGP dentro del AS. En la figura 2.4 (b) AS1 elige a AS2 como tránsito para la ruta 10.0.0.0/8 regulando el atributo de preferencia local a 20 en el *router* límite A y a 10 en el *router* límite B, es decir, elige el camino saliente con mayor valor de atributo.

Atributo MED (*Multi-Exit Discriminator;* Discriminador de Múltiples Salidas).- Es un atributo de exportación que mediante la asignación de un valor para cada camino le permite al administrador de red informar a ASs adyacentes de un camino de entrada preferida al AS cuando múltiples conexiones existen entre los dos ASs, así como también balancear la carga del tráfico entrante. Por ejemplo, el tráfico entrante direccionado a las redes 10.0.1.0/24 y 10.0.2.0/24 en el mismo AS utilizarán los caminos A y B respectivamente mediante la asignación de valores MED. El proceso de selección utilizará la ruta con valor MED más bajo.

2.3. DESCRIPCIONES GENERALES DE UN *ROUTER*

Como se ha visto, uno de los principales componentes dentro de un ISP son los *routers*. Los routers son dispositivos de conmutación de paquetes diseñados para interconectar redes o segmentar una red con la finalidad de limitar el tráfico. Los *routers* son sistemas que determinan cuál es el camino más adecuado para que viaje un paquete de datos hasta llegar a su destino final, es decir, elige qué camino es el más conveniente de entre muchas opciones que pueden existir dentro de una infraestructura de cableados y enlaces digitales de Internet.

Existen dos tipos de *routers*: internos y externos. Los ***routers internos*** o dispositivos de propósito general, son tarjetas inteligentes que se instalan dentro de un DTE de la red (generalmente el servidor) y consisten en una plataforma con un único procesador y una memoria con un *software* de enrutamiento para manejar un conjunto de dispositivos de interfaz. Los ***routers externos*** son equipos especializados de alto rendimiento compuestos por una plataforma de alta capacidad con múltiples procesadores de propósito especial dedicados a las tareas de enrutamiento.

La selección de uno u otro *router* radica en la escalabilidad de la red, ya que los requerimientos de un *software* de enrutamiento no podrán ser alojados en una plataforma con un único procesador si se trata de una red muy grande.

Un *router* trabaja a nivel de capa 3 (capa red) dentro del modelo OSI. Los servicios que ofrece la capa red pueden ser orientados a conexión o no orientados a conexión, por esta razón, se pueden clasificar a los *routers* como *routers* orientados a conexión y *routers* no orientados a conexión.

Un ***router que trabaja con servicios orientados a conexión*** como los servicios que presta ATM o X.25, debe primero establecer la conexión en forma explícita, es decir, debe establecer un circuito virtual o VC por donde viajarán todos los paquetes de información en estricto orden y luego, de la misma manera debe liberar la conexión. Estos paquetes no necesitan llevar la dirección destino pero

sí la dirección del circuito virtual. Cada *router* deberá constantemente tomar nota de los circuitos virtuales existentes y con esta información formar una tabla en la que se indique la interfaz de entrada y de salida para cada circuito virtual que pase por dicho *router*. Un *router* de este tipo tiene la desventaja de ser vulnerable a fallos, ya que si éste queda fuera de servicio, desaparecerán todos los circuitos virtuales que pasen por él en ese momento y los *hosts* involucrados dejarán de comunicar y se perderá la información, aunque se puede establecer otro circuito virtual por otro camino alternativo. Una ventaja de este *router* es que puede trabajar con cabeceras pequeñas y además evitar los problemas ocasionados por la duplicación de paquetes retardados; además, es fácil realizar un control de congestión y asegurar un QoS (calidad de servicio).

Un ***router que trabaja con servicios no orientados a conexión*** como los servicios que presta una red IP, debe mantener una tabla de enrutamiento en la que se indique la interfaz por la que se deben encaminar los paquetes o datagramas en función de su destino. Cada datagrama debe llevar la dirección de su destino y cada uno debe averiguar la ruta por sí mismo, razón por la que aquí no se garantiza el orden de llegada de los paquetes. Una de las ventajas es que si un *router* de la red queda fuera de servicio, solamente se perderán los datagramas que en ese momento estuvieran en proceso dentro del *router* ya que el resto de *routers* de la red buscarán caminos alternativos para poder comunicarse. Una desventaja de este tipo de *routers* es que utiliza cabeceras grandes y además no se puede realizar un control de congestión ni ofrecer una QoS.

Funciones de un Router

Una de las principales funciones de un router es la creación de las tablas de enrutamiento (ya sea estáticamente o dinámicamente), de esta manera el *router* realiza la decisión de envío del paquete basado en la dirección destino.

Otra de las funciones de la capa red en un *router* es seleccionar la ruta por la cual se enviará un paquete. Cuando el *router* trabaja con datagramas, esta selección se la hace para cada uno de los paquetes que conforman el mensaje original;

pero si el *router* trabaja con circuitos virtuales, la selección de la ruta se la hace solamente en el momento del establecimiento de cada nuevo circuito.

Cuando un datagrama llega a un *host*, el *software* compara si la dirección de destino de dicho datagrama es igual a la dirección IP del *host*, si esto sucede se acepta el paquete y se lo pasa al *software* del protocolo de alto nivel para que sea procesado, caso contrario se descarta el datagrama.

Cuando un datagrama llega a un *router*, el *software* compara si la dirección de destino del datagrama es igual a la dirección IP del *router*, si esto sucede se acepta el paquete para ser procesado internamente del mismo modo que lo hace un *host*. Generalmente, los únicos paquetes que son direccionados a un *router* son aquellos que se utilizan para probar la conectividad del enlace o los que llevan comandos de control del *router*.

Si la dirección destino de un paquete que llega a un *router* no tiene la misma dirección IP del *router*, significa que dicho paquete tendrá que seguir viajando a través de la red hasta alcanzar su destino. En este caso, cada vez que un datagrama llegue a un *router*, éste será almacenado hasta que el paquete anterior haya sido procesado, luego el *software* IP extrae el datagrama encapsulado, selecciona la dirección del siguiente salto en base a la tabla de enrutamiento y de nuevo encapsula el datagrama en una o varias tramas (fragmentación) que le permita viajar a lo largo de la red física hasta alcanzar su destino. Si la dirección destino de un datagrama no aparece en la tabla de enrutamiento, las rutinas de enrutamiento direccionan este datagrama hacia un *router* específico llamado ***router por omisión*** o ***router por default,*** el cual tratará de encontrar el siguiente salto del paquete.

Las direcciones IP tienen una estructura jerárquica, es decir, una parte de la dirección IP corresponde a la red y la otra al *host* dentro de la red. Cuando un *router* recibe un datagrama por cualquiera de sus interfaces, compara la parte de red de la dirección con las entradas contenidas en sus tablas (que normalmente solo contienen direcciones de red, no de *host*) y envía el datagrama por la interfaz

correspondiente. Es decir, para tomar decisiones de enrutamiento de manera eficiente y para mantener reducido el tamaño de las tablas de enrutamiento, dichas tablas guardan información sobre direcciones de redes destino y no direcciones de *host* individuales.

Otras funciones importantes que desempeña un *router* son:

- Proporcionar seguridad a través de sofisticados filtros de paquetes en ambientes LAN y WAN, lo que permite al *router* la construcción de un *firewall* para brindar seguridad y control de acceso.
- Integrar diferentes tecnologías de enlace de datos, tales como *Ethernet*, *Fast Ethernet*, *Token Ring*, FDDI, ATM, etc.

2.4. *ROUTERS* DEL ISP

Los *routers* que se pueden encontrar dentro de la Infraestructura del Proveedor de Servicios de Internet son:

2.4.1. *ROUTER* PROPIEDAD DEL CLIENTE

Cuando el cliente es una red de área local (LAN), la manera como éste accede al ISP es mediante un *router* CPE (*Customer Premises Equipment;* Equipo Propiedad del Cliente). El *router* CPE puede contener lo siguiente:

- Una interfaz local Ethernet (o un pequeño *hub* Ethernet multipuerto).
- Una interfaz de velocidad básica (BRI) ISDN.
- Memoria de configuración no volátil, que permite a la unidad operar correctamente en el estado encendido.

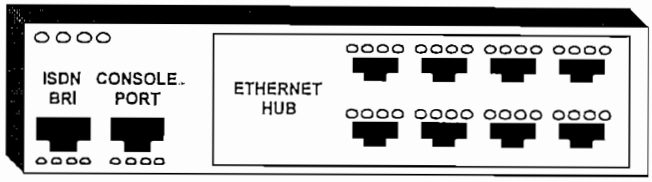


Fig. 2.5. Ejemplo de Router CPE[4] .

Estas unidades usan una configuración *dial* bajo demanda a fin de que la llamada sea establecida por el ISP, además pueden usar múltiples canales B en una configuración de multienlace PPP.

El *router* CPE puede incluir funciones de servidor DHCP (*Dinamic Host Configuration Protocol;* Protocolo de Configuración Dinámica de *Host*), para permitir la configuración dinámica local de *host*, capacidad de traducción de direcciones *firewall*, así como definir varias formas de filtros de paquetes. El *router* CPE puede ser usado para generar una notificación local de ruta por defecto en la LAN y puede usar RIP para esta tarea. Así como también el *router* CPE puede notificar los prefijos de red local al ISP, aunque la configuración más típica usaría notificaciones de rutas configuradas estáticamente al extremo del proveedor de servicio.

2.4.2. SERVIDOR DE ACCESO DE RED (NAS)

El NAS es una unidad usada para terminar las llamadas entrantes de la PSTN (Red Telefónica Pública Conmutada) e ISDN (Red Digital de Servicios Integrados). La unidad consta típicamente de lo siguiente:

- Un determinado número de interfaces de velocidad primaria (PRI) ISDN.
- Una interfaz *Ethernet* 10/100.
- Uno o más puertos de acceso de control administrativo (una configuración multipuerto usaría un puerto para acceso local y un segundo para acceso remoto).

El servidor de acceso remoto (NAS) realiza lo siguiente:

- ***Acepta llamadas entrantes PSTN o ISDN***, en el caso de las llamadas entrantes PSTN, la unidad conmuta la llamada a un módem analógico. Las llamadas ISDN puede ser directamente manejadas sin necesidad de ser conmutadas hacia el procesador de señal, como se mencionó en el capítulo I.
- ***Usa un mecanismo de autenticación asociado, tal como RADIUS o una variante de TACACS***, este mecanismo permite una estructura de administración de cuenta centralizada para validar al usuario y opcionalmente detallar un perfil que puede ser cargado al NAS para equiparar los requerimientos del usuario, tal perfil puede ser la configuración de una red *dial* privada virtual.
- ***Se aloja normalmente en un ambiente especializado***, la tolerancia ambiental no es un factor crítico, pero es útil tener algún nivel de resistencia ambiental.
- ***La memoria y la capacidad del procesador son factores críticos***, los servidores de acceso *dial* tienden a ser el "cuello de botella" para los servicios de Internet y en consecuencia es aquí el punto donde el rendimiento se vuelve crítico. La unidad debe tener suficientes *buffers* de memoria para atender el número de puertos de acceso configurados. Entre las cosas que debe realizar un NAS, se incluye la administración del *buffer*, selección de paquetes a ser descartados y medidas de administración de rendimiento operacional como son: una espera adecuada de los paquetes, descarte previo y notificación de congestión explícita.
- ***Debe soportar acceso PPP y multienlace PPP***, esto es necesario en el inicio de la sesión y en el modelo de administración dinámica de llamadas.

El NAS puede administrar, a más de las llamadas entrantes de *hosts* individuales, las llamadas de redes, en este caso el perfil de autenticación puede detallar los prefijos de red a ser asociados con la llamada, el cual debe ser cargado dentro del NAS por el administrador como rutas estáticas. El servidor de acceso remoto

protege la red local de los problemas de seguridad presentes en el Internet, los filtros son configurados por el administrador de la red para asegurar que solo se permita el paso del tráfico autorizado entre la red local e Internet.

El servidor de acceso remoto y el equipo remoto, deben emplear un protocolo compatible siendo el más usado el PPP (*Point to Point Protocol*; o Protocolo Punto a Punto), y en segundo plano el SLIP (*Serial Line Interface Protocol*; o Protocolo de Interconexión de Líneas Serie).

El NAS puede entregar diferentes tipos o calidades de servicios a los usuarios, por medio de la administración del ancho de banda, basándose en la política y la identidad del usuario.

La arquitectura típica del NAS es un chasis con un *motherboard* que contiene un procesador y puertos de red local y de control, además posee módulos que contienen puertos de acceso ISDN y arreglos de módems digitales. El NAS debe soportar el protocolo de enrutamiento interior usado por el ISP.

2.4.3. *ROUTER* DE ACCESO DEL CLIENTE

Aunque el NAS se usa para terminar las llamadas de acceso *dial*, el *router* de acceso del cliente se usa para terminar varias formas de circuitos de acceso permanente. El *router* de acceso del cliente debe ser capaz de manejar una diversidad de tecnologías de conexiones físicas como se verá a continuación:

Los medios sincronizados (circuitos DDS[a], T1, T3, E1, E3, o más), usualmente terminan en una interfaz dedicada en el *router* de acceso, donde la característica de esta familia de circuitos es garantizar que ningún dato se pierda dentro del medio de comunicación. El factor de densidad de tales interfaces es un factor crítico en la elección del *router*.

[a] Servicio de Datos Digitales.

Otro mecanismo de comunicación es mediante medios compartidos conmutados, donde los circuitos virtuales *end-to-end* son configurados a través de la conmutación, tales medios de comunicación incluyen PVCs (Circuitos Virtuales Permanentes) Frame Relay y PVCs ATM, la característica de esta familia es que se puede dar pérdida de datos debido a la falta de sincronización *end-to-end* de la velocidad del flujo de datos. Dentro del *router* una sola terminación física es compartida a través de un número de PVCs que son representados dentro del *router* como una interfaz lógica.

La arquitectura típica de este *router* es un chasis con un conjunto de procesadores e interfaces, permitiendo una gran densidad de conexiones de acceso.

Este *router* forma la frontera de la red del proveedor de servicio, siendo capaz de soportar una gran cantidad de tráfico y proveer un amplio rango de opciones de enrutamiento. Además la unidad debe ser capaz de aplicar un conjunto de herramientas administrativas incluyendo perfiles de: QoS, accesibilidad, enrutamiento y contabilidad.

2.4.4. *ROUTER* PRINCIPAL (*CORE ROUTER*)

Este *router* presenta un perfil diferente en términos de requerimientos operacionales, éste provee una plataforma estable que protege la integridad del *backbone* principal de la red, garantizando que los sistemas de transmisión principal sean capaces de resistir la presión de grandes volúmenes de paquetes conmutados por segundo entre un pequeño número de puertos locales y circuitos de enlace de gran volumen.

El *router* principal necesita por tanto de un alto nivel de funcionalidad para soportar la arquitectura de enrutamiento escogida, memoria suficiente, y capacidad de procesamiento para encargarse de la conmutación de paquetes de gran velocidad, por lo que su inversión es un gasto importante dentro del ISP.

Una arquitectura potencial usa un chasis común para ambos *routers*: el principal y el de acceso del cliente, mientras el *router* de acceso posee una gran densidad de interfaces, el *router* principal posee un pequeño número de interfaces de alta velocidad para soportar la red principal.

Las interfaces del *router* principal deben soportar medios de transmisión de alta velocidad, para lo cual los requerimientos de velocidad en la conmutación de paquetes están en el orden algunas decenas de Gbps.

2.5. ENTORNOS DE ENRUTAMIENTO

El corazón del entorno operacional de un ISP es el sistema de enrutamiento. El sistema de enrutamiento es el elemento crítico para proveer conectividad a un ISP tanto con sus clientes como con su proveedor de acceso a Internet *upstream*. La selección y configuración de un adecuado protocolo de enrutamiento es una tarea crítica que asegura no solamente la estabilidad de la red local sino también la operación estable de las redes adyacentes.

Aquí deben ser tomados en cuenta tres aspectos importantes relacionados con el enrutamiento: enrutamiento al cliente, enrutamiento interior dentro de un AS, y enrutamiento exterior hacia otros sistemas autónomos.

2.5.1. ENRUTAMIENTO AL CLIENTE

Existen varios mecanismos de conexiones hacia el cliente, consecuentemente, a continuación se examinará la interfaz de enrutamiento para cada uno de estos mecanismos:

El Host Dial-Up

Cuando un cliente *dial-up* desea conectarse a Internet, realiza una llamada telefónica a uno de los números provistos por su ISP, la llamada *dial* es

respondida por el módem del NAS, se realiza la correspondiente autenticación, y en la fase de conexión se asigna una única dirección IP al *host* que realizó la llamada, esto es realizado como parte de la operación del protocolo PPP. Un cliente *dial-up* utiliza una dirección IP asignada dinámicamente desde un *poll* de direcciones que han sido estáticamente configuradas en el Servidor de Acceso de Red (NAS). Esta dirección es entonces notificada a toda la red del ISP a través del IGP.

Cuando un cliente desea operar servicios tales como publicación de páginas Web o descarga de archivos FTP desde una dirección constante, se asigna una dirección constante al cliente cada vez que éste se conecte a la red.

La Red Dial-Up

El modelo de un único *host* utilizando conectividad dinámica *dial-up* está siendo complementado con un modelo de conectividad dinámica *dial-up* de una pequeña red o sistemas de *host*. En este modelo, el NAS debe ser capaz de notificar una ruta a la red del cliente cada vez que se establezca una conexión . Una forma de realizar esto es asociar una dirección fija a la conexión *dial-up* y entonces configurar el NAS con una ruta estática a la red del cliente que usa la dirección *dial-up* asignada como el destino de la ruta.

El Cliente Corporativo

Esta es una forma común de conexión en la cual el cliente del servicio de red es otra red y cuya conexión al ISP utiliza una línea arrendada o una forma similar de conexión permanente.

El ***cliente single-homed,*** como se mencionó en el Capítulo I, es aquel que utiliza una única conexión al ISP para satisfacer sus requerimientos de conectividad exterior.

Desde el punto de vista de enrutamiento, esta configuración utiliza rutas estáticas

en ambos lados de la conexión. Dentro de la red del cliente, éste genera una ruta por defecto en el *router* fronterizo, esta ruta corresponde a aquella que le permitirá la conexión con la interfaz del *router* del ISP. La red del cliente es notificada de esta ruta a través de la red local utilizando el protocolo de enrutamiento interior seleccionado. Dentro de la red del ISP, el ISP asigna una ruta estática al cliente y le dedica un puerto de acceso (al cual le asocia una sola dirección IP del conjunto de rutas estáticas que se encuentran configuradas en el interior del *router* de acceso que es el encargado de terminar la conexión del cliente dedicado). El ISP tiene la responsabilidad de notificar las rutas de los clientes al resto de clientes de dicho ISP. De esta forma, la información a cerca de las direcciones de las redes de los clientes es notificada al proveedor del servicio, y éste pasa al cliente información acerca de la accesibilidad de las otras redes a través de la interfaz del proveedor.

En términos de protocolos, la interfaz del cliente es una interfaz de enrutamiento a través de la cual se debe pasar información de enrutamiento en ambas direcciones mediante el uso de un protocolo de enrutamiento. RIP es un protocolo que puede desarrollar esta tarea ya que uno de sus atributos es la simplicidad de configuración y operación. RIPv2 es una versión mejorada de RIP, el cual permite el uso de máscaras de direcciones a fin de que pueda ser utilizado eficazmente dentro de un entorno de enrutamiento sin clase. Otras alternativas también incluyen el uso de EIGRP u OSPF.

Todos los protocolos que se utilizan en esta configuración son protocolos de enrutamiento internos, debido a que aquí no se pretende dar a conocer la topología interna de la red del cliente al ISP o viceversa, más bien lo que se desea es mantener la accesibilidad a la red, razón por lo cual es conveniente mantener rutas estáticas para soportar esta forma de interfaz del cliente.

El ***cliente multiconectado***, es el mismo cliente single-homed, solamente que en lugar de tener una única conexión al ISP tiene *varias*.

En esta configuración se prefiere utilizar protocolos de enrutamiento *exterior* ya

que el uso de un IGP no se considera una solución estable y BGP-4 es una buena elección. Aquí, el cliente usa sesiones *peering* iBGP para interconectar todos los *routers* fronterizos de su red y usa sesiones *peering* eBGP para conectar dicho puntos a los respectivos *routers* del ISP.

El ***cliente multi-homed*** es aquel que está conectado a varios proveedores de servicio. Los motivos para realizar esto son muy variados; por ejemplo, muchos clientes desean mejorar la *confiabilidad* de la conectividad de Internet, ya que si la conectividad de un proveedor falla, se tiene otro proveedor.

La asimetría de flujo de tráfico de una conexión multi-proveedor no ayuda cuando se intenta diagnosticar fallas operacionales e inestabilidad de la conectividad del cliente, siendo esto un resultado potencial de dicho arreglo.

El protocolo BGP ayudará aquí, usando una configuración en la cual el cliente es un AS *multi-homed.* El cliente tiene dos sesiones eBGP una para cada ISP y anuncia sus rutas a cada ISP con un camino AS que hace referencia a su AS local. Si múltiples *routers* fronterizos exteriores son usados, ellos necesitarán estar interconectados mediante sesiones iBGP.

Para la salida de tráfico, la red del cliente tiene varias opciones. El cliente puede usar una ruta por defecto primaria dirigida a un proveedor e introducir (o importar) un conjunto de rutas desde otros proveedores, junto con el uso de una jerarquía de rutas por defecto para asegurar que la conectividad externa permanezca disponible durante las pausas del enlace de egreso primario. Si el cliente desea tomar una decisión sobre cuál proveedor usar para un gran conjunto de *routers*, el cliente puede recibir un conjunto completo de entradas de enrutamiento desde cada proveedor y entonces aplicar consideraciones de política local para seleccionar caminos para cada destino. Para tráfico entrante, el cliente puede usar varias técnicas BGP para describir preferencias de camino para tráfico entrante.

El uso de BGP en esta conexión ahora introduce un acoplamiento de los entornos

de enrutamiento del cliente y el proveedor del servicio, y el proveedor de servicio ahora debe usar un mecanismo diferente para limitar la interacción de enrutamiento a un conjunto administrativo de rutas y atributos de ruta. El típico mecanismo es pasar todas las rutas anunciadas a través de un filtro de entrada, para asegurar que la red del cliente anuncie solamente esos destinos de red que han sido notificados como pertenecientes al cliente.

El ***cliente de tránsito*** es aquel que siendo cliente de un ISP sirve de proveedor o intermediario a terceros clientes. El cliente de tránsito puede ser un cliente *single-homed*, *multi-homed* o multiconectado. Para que un ISP pueda conectarse con el cliente de tránsito debe establecer una sesión eBGP con dicho cliente.

2.5.2. ENRUTAMIENTO INTERIOR

La selección de un IGP adecuado para trabajar dentro de un sistema autónomo tal como un ISP, es fuertemente influenciado por la arquitectura interior de la red, su tamaño y la forma en la cual son implementadas las políticas de enrutamiento.

De esta manera, RIP no es aconsejable en redes cuya topología es muy compleja ya que la métrica de 16 limita el diámetro de la red a no más de 15 saltos. La elección de un protocolo propietario como IGRP o EIGRP puede implicar algunas restricciones con respecto al equipo de enrutamiento usado por el ISP.

2.5.3. ENRUTAMIENTO EXTERIOR

En este entorno, un ISP debe utilizar un EGP que le permita intercambiar información de enrutamiento con otras entidades como su proveedor de servicios *upstream* o clientes quienes han contratado al ISP para proveer servicios de conectividad.

El enrutamiento para redes exteriores es similar a las consideraciones de

enrutamiento que se aplican a las redes del cliente de tránsito, por lo tanto el protocolo más utilizado en este entorno es BGP-4.

BIBLIOGRAFÍA CAPÍTULO 2

[1] http://www.cisco.com/warp/public/103/5.html#4

An Introduction to IGRP. Summary of IGRP

[2] http://www.cisco.com/warp/public/103/5.html#4

An Introduction to IGRP. Update

[3] http://www.cisco.com/warp/public/103/eigrp1.html

Enhanced Interior Gateway Routing Protocol. EIGRP Metrics.

[4] "*ISP Survival Guide. Strategies for Running a Competitive ISP*"; Geoff Huston; Primera Edición; John Wiley & Sons, Inc.; 1999; EEUU.

[5] "Edición Especial TCP/IP"; John Ray; Primera Edición ;Prentice Hall; 1999; Madrid-España

[6] *"Internet Routing Architectures"*; Sam Halabi y Danny McPherson; Segunda Edición; Cisco Press; 2000; Indianapolis-EE.UU.

[7] "TCP/IP. Principios Básicos, Protocolos y Arquitectura"; Douglas E. Comer; Tercera Edición; Prentice Hall; 1996, México.

[8] http://www.faqs.org/rfcs/rfc1721.html

RFC1721. RIP versión 2 PROTOCOL ANALISIS

[9] http://www.itpapers.com

ISP

[10] http://it.aut.alcala.es/josema/rc_teleco/OSPF.pdf

Protocolos de enrutamiento

[11] http://www.die.udec.cl/~redes/apuntes/myapuntes.pdf

Apuntes de redes de datos

[12] http://www.dis.eafit.edu.co/areas/telematica/online/introredes/arqRedes.pdf

Redes y Protocolos de comunicaciones

[13] http://www.scit.wlv.ac.uk/jphb/comms/iproute.html

Encaminamiento en Internet

[14] http://www.cis.ohio-state.edu/htbin/rdc/rfc1771.html

A Border Gateway Protocol 4 (BGP-4)

[15] http://www.cis.ohio-state.edu/htbin/rdc/rfc1772.html

Application of the Border Gateway Protocol in the Internet

[16] http://www.cis.ohio-state.edu/htbin/rdc/rfc1773.html

Experience with the BGP-4 protocol

[17] http://www.cis.ohio-state.edu/htbin/rdc/rfc1774.html

BGP-4 Protocol Analysis

[18] http://www.dcc.uchile.cl/~jpiquer/Extension/Postitulo/45.html

Protocolos de enrutamiento

[19] http://lovecraft.die.udec.cl/~jorge/apuntes/node1.html

Protocolos de ruteo exterior

[20] http://gsyc.escet.urjc.es/docencia/asignaturas/redes-I/transparencias/routing/text0.htm

Encaminamiento en Internet

[21] http://www.ldc.usb.ve/~redes/Temas/Tema.20/index.html

Protocolos de ruteo exterior

[22] http://www.cicei.ulpgc.es/gsi/tut_tcpip/3376fm.html

Protocolos de encaminamiento interior

[23] http://www.it.uc3m.es/~prometeo/rsc/apuntes/index.html

Encaminamiento

[24] www.faqs.org/rfcs/rfc1583.html

RFC1583. OSPF versión 2

[25] http://itaut.alcala.es/josema/rc_teleco/OSPF.pdf

Protocolos de encaminamiento

[26] http://www.cisco.com/warp/public/103/eigrp-toc.html

Enhanced Interior Gateway Routing Protocol

[27] http://www.cisco.com/warp/public/103/index.shtml

IGRP/EIGRP *Technical Tips*

3

PLANIFICACIÓN Y DIMENSIONAMIENTO DEL ISP

CAPÍTULO III

PLANIFICACIÓN Y DIMENSIONAMIENTO DEL ISP

3.1. ATRIBUTOS QUE DEBE CUMPLIR UN ISP

Es necesario conocer los atributos más importantes que debe cumplir un ISP ya que éstos deberán ser posteriormente aplicados dentro del diseño de ingeniería de dicha red. La estrategia de diseño de un ISP es integrar las consideraciones que a continuación se describirán dentro de un modelo global de costos y capacidad. Dichos atributos son:

Simplicidad

El aspecto más crítico que debe cumplir un ISP es la simplicidad estructural, es decir, el ISP debe imponer el mínimo de restricciones a sus clientes, permitiendo que éstos se interconecten fácilmente al ISP. La simplicidad de diseño también permite al proveedor adaptarse a cambios tanto tecnológicos como de requerimientos de servicio que podrían ser demandados por el cliente en el futuro.

Factibilidad técnica

Factibilidad técnica significa que, una arquitectura de red debe contar con tecnología de vanguardia y disponer de recursos suficientes para adquirir tal tecnología, caso contrario la red podría quedar obsoleta en corto tiempo y no se podrá ajustar a los objetivos de servicio futuros. Además, los clientes esperan fiabilidad en un servicio de comunicaciones y ésta debe ser provista por el ISP usando dispositivos y sistemas *fiables* que ya hayan sido probados en tales entornos.

Relevancia

La arquitectura de un ISP deberá ser diseñada para resolver los problemas actuales del cliente final más no para imponer una metodología diferente que obligue a los clientes a utilizar nuevos servicios y protocolos e incurrir en costos

adicionales para emigrar su entorno de servicio simplemente para equilibrar su tecnología con la del ISP.

Escalabilidad

A lo ancho del mundo, el mercado de servicios de Internet crece entre el 5% al 20% mensual. Ese nivel de crecimiento corresponde a situaciones en las cuales las redes duplican su tamaño en un período de entre 6 a 20 meses. Por tanto la arquitectura de red escogida debe ser capaz de escalar en tamaño de modo significativo[1].

Este tipo de crecimiento es quizá el obstáculo más significativo para cualquier arquitectura de Internet. *Escalar* se hace necesario cuando el número de clientes que se conectan crece continuamente y cuando crece la cantidad de tráfico a ser transportado.

En estos casos se debe considerar cómo la arquitectura se expande para manejar más clientes, más lugares, y volúmenes más grandes de tráfico y en qué punto la arquitectura elegida alcanza su límite de expansión.

Redundancia

La redundancia juega un papel importante en el desempeño del proveedor del servicio de Internet. Es conveniente que un ISP cuente con redundancia tanto de sus dispositivos como de sus enlaces (mantener una capacidad adicional del ancho de banda total es una buena opción) ya que una falla en cualquiera de los recursos de la red del ISP provocará la suspensión del servicio a los clientes.

Confiabilidad

Diseñar un sistema confiable involucra varios aspectos ya mencionados como: la redundancia, factibilidad técnica, etc. Adicionalmente, un cliente califica a un ISP como confiable si éste dispone de un eficiente servicio de asistencia al cliente (soporte técnico), mantiene copias de seguridad del sistema con relativa frecuencia y ofrece un buen sistema de seguridad que mantenga la confiabilidad de las transacciones.

Viabilidad financiera

Quien implemente un ISP debe contar con suficiente capital para soportar períodos de pérdida financiera para de esta manera no optar por las desapariciones, fusiones o adquisiciones de ISPs.

3.2. IDENTIFICACIÓN DE LOS OBJETIVOS DEL ISP

Uno de los objetivos más importantes de un ISP es decidir cuál es el área de cobertura geográfica que se desea servir, para lo cual es conveniente realizar un análisis de viabilidad de mercado de la zona seleccionada. Además, se debe tener en cuenta quiénes podrían ser los clientes potenciales del ISP, cómo se planea que crezca el proveedor, la clase de servicios que se ofrecerán y las perspectivas de escalabilidad de dicho ISP, todo esto sin dejar de lado el aspecto económico.

Internet es un mercado en crecimiento en nuestro país y Quito es una de las ciudades que concentra mayor actividad económica y población del Ecuador lo que la convierte en un sitio estratégico para el desarrollo e implementación de un ISP, siendo el objetivo primordial diseñar un plan para el manejo y administración de las seguridades así como el diseño en sí de la infraestructura de la red de un ISP de mediano tamaño.

3.2.1. VIABILIDAD DE MERCADO EN LA CIUDAD DE QUITO

Un análisis de viabilidad de mercado permite tener una idea de la demanda de un determinado servicio dentro de la región geográfica a la cual se desea servir y permite cuantificar el tamaño de dicho mercado en base al número de competidores significativos en la región. Una vez hecho esto se decidirá si es factible o no la implantación del negocio.

En esta sección se hará el cálculo de la viabilidad de mercado de un ISP para la

ciudad de Quito, el mismo que permitirá obtener el número de clientes tanto *dial-up* como corporativos con los que podría contar cada proveedor si todos éstos fueran iguales.

$$Número\ de\ usuarios = \frac{(Posibles\ usuarios\ de\ Internet * Tasa\ de\ Penetración\ de\ Acceso\ de\ Internet)}{Número\ total\ de\ competidores}$$

Ec. 3.1. Fórmula para el cálculo de la viabilidad de mercado [6]

Posibles usuarios de Internet

Según la última proyección de población realizada por el INEC (Instituto Nacional de Estadísticas y Censos) para el período comprendido entre 1990 y 2000, se obtuvo que en la ciudad de Quito existe una población de 1'645.631 habitantes concentrados en el área urbana para el año 2000[7]. Se sabe además que a nivel nacional, el número de personas que tienen computadoras personales por cada 100 habitantes corresponde al 2%[8] de manera que:

$$Posibles\ usuarios\ dial = 1'645.631 habitantes * 2 \frac{personas\ con\ PCs}{100\ habitantes}$$

$$Posibles\ usuarios\ dial = 32913\ personas\ que\ potencialmente\ podrían\ usar\ Internet$$

En Quito existen 8500 empresas (dato proporcionado por CEDATOS, actualizado al 2001) de las cuales se considera que un 85% tienen redes de computadoras, de manera que:

$$Posibles\ usuarios\ corporativos = 8500\ empresas * 0.85$$

$$Posibles\ usuarios\ corporativos = 7225\ empresas\ que\ potencialmente\ podrían\ usar\ Internet$$

Hay que considerar que de este valor, la mayor parte de empresas se encuentran concentradas en la ciudad de Quito.

Tasa de Penetración de Acceso de Internet

Se define la tasa de penetración en el servicio de Internet como el número de personas que tienen Internet por cada 100 habitantes de aquellos que poseen computadoras personales. Se estima que la tasa de penetración en Quito al año 2001 es del 30% (dato proporcionado por la Superintendencia de Telecomunicaciones).

Número total de competidores

A nivel nacional existen 35 proveedores autorizados distribuidos a lo largo del país[9], de los cuales 30 de ellos prestan servicios a la ciudad de Quito[10]. Para este cálculo, el número total de competidores en la ciudad de Quito no puede ser tomado como 30, ya que no todos estos ISPs son iguales y por lo tanto no tienen el mismo número de usuarios. En Quito existen 4 proveedores mayores que abarcan el mercado, éstos son: Andinanet, Ecuanet, Impsatel (Impsat, Interactive) y Satnet, los otros son proveedores pequeños que por el número de usuarios que tienen equivalen a 2 proveedores grandes; de esta manera, se tienen 7 ISPs de tamaño similar incluido el ISP del diseño.

Cálculo de la viabilidad de mercado

$$Número\ de\ usuarios = \frac{(32913\ personas + 7225\ empresas) * 30\%}{7}$$

$$Número\ de\ usuarios = (1411\ personas + 310\ empresas)\ por\ competidor$$

Este resultado significa que existe posibilidad de éxito en la implementación del ISP ya que el número de usuarios obtenido refleja que existe demanda del servicio. Además, existe una clara tendencia de crecimiento de la tasa de penetración de acceso a Internet lo cual hace que cada vez más personas y empresas requieran el servicio.

3.2.2. PROYECCIÓN DE USUARIOS *DIAL-UP* Y CORPORATIVOS

El siguiente objetivo del ISP es planear como será su crecimiento para un determinado período de tiempo. Esto es necesario ya que permitirá tener una visión del incremento de los equipos y enlaces y por lo tanto del capital que se deberá invertir a mediano plazo.

3.2.2.1. Proyección de usuarios *dial-up*

Los siguientes datos (obtenidos directamente de la Superintendencia de Telecomunicaciones) muestran el crecimiento promedio del número de usuarios *dial-up* de los ISPs más grandes en la ciudad de Quito:

OPERADORA	Ene-00	Feb-00	Mar-00	Abr-00	May-00	Jun-00	Jul-00	Ago-00	Sep-00	Oct-00
Andinanet	1271	2150	2330	3023	3739	4091	5210	5662	6127	6870
Ecuanet	1235	3028	3906	4214	4163	4084	4005	3837	4034	4013
Impsatel	3932	3759	3759	4048	4130	4243	4472	4722	4797	4900
Satnet	6266	7711	7702	6329	6340	6114	6056	5918	6000	6056
Valor Promedio	3176	4162	4424	4404	4593	4633	4936	5035	5240	5460

Tabla 3.1. Crecimiento de los usuarios dial-up en Quito

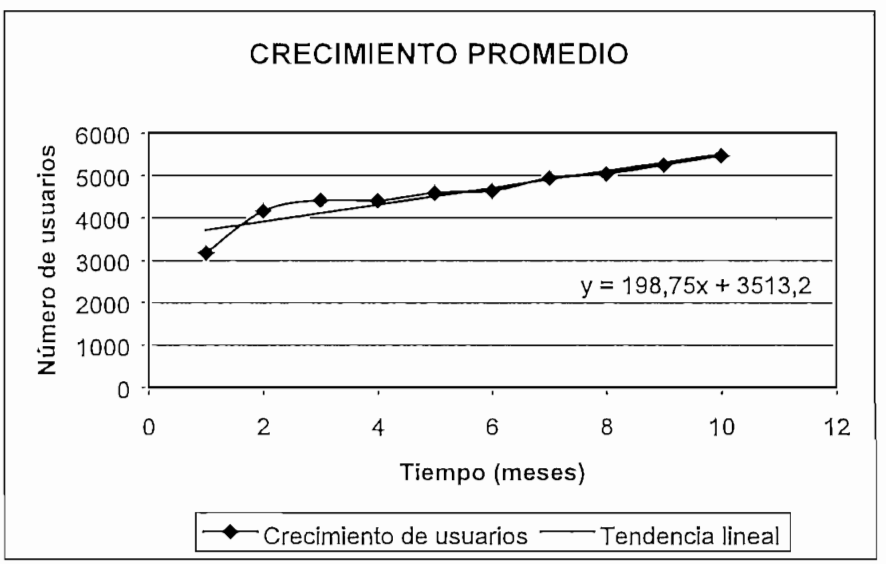


Fig. 3.1. Crecimiento promedio de los usuarios dial-up en Quito

Como se puede observar, la línea de tendencia de crecimiento de usuarios *dial-up* en Quito corresponde a una función lineal. Considerando que se conservará dicha tendencia (misma pendiente de la recta) y que al final de los 3 primeros meses de operación del ISP se contará con 300[a] usuarios *dial-up*, se obtiene la ecuación: $y = 198.75 * x - 296.25$, donde y es el número de usuarios *dial-up* y x es el tiempo en meses. Esta ecuación será utilizada para obtener la proyección de usuarios para los siguientes cuatro años a partir del 2002:

	Inicio	AÑO 1	AÑO 2	AÑO 3	AÑO 4
Usuarios esperados	300	2089	4474	6859	9244

Tabla 3.2. Planificación de crecimiento de usuarios dial-up para el ISP de diseño

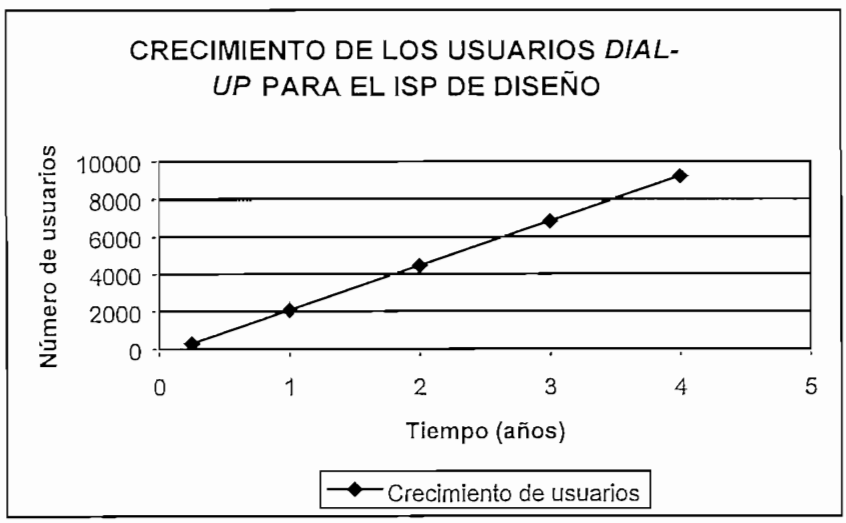


Fig. 3.2. Planificación de crecimiento de usuarios dial-up para el ISP de diseño

3.2.2.2. Proyección de usuarios corporativos

Los siguientes datos muestran el crecimiento promedio del número de usuarios corporativos de dos de los ISPs más grandes en la ciudad de Quito:

[a] Dato sugerido por el personal técnico de Satnet.

OPERADORA	Ene-00	Feb-00	Mar-00	Abr-00	May-00	Jun-00	Jul-00	Ago-00	Sep-00	Oct-00
Andinanet	10	20	30	38	52	59	70	80	90	100
Satnet	100	115	125	131	133	133	136	138	134	148
Valor Promedio	55	68	78	84	93	96	103	109	112	124

Tabla 3.3. Crecimiento de los usuarios corporativos en Quito

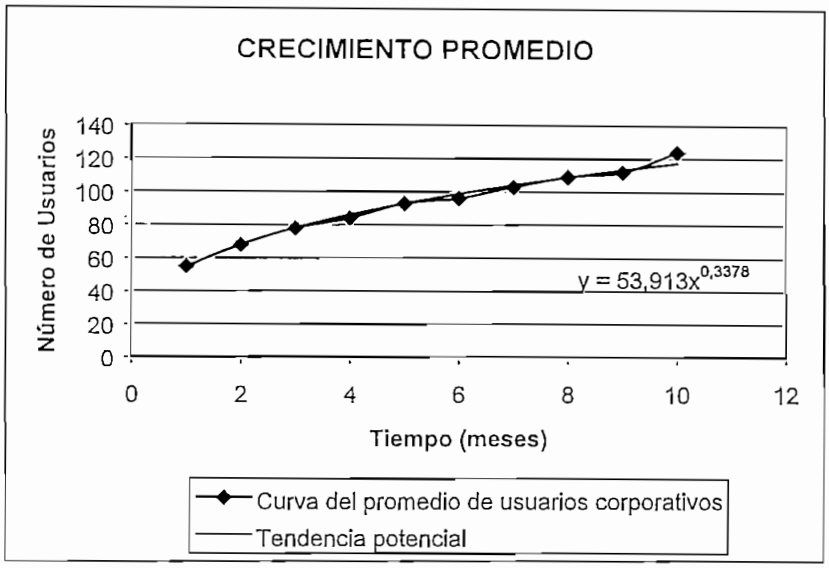


Fig. 3.3. Crecimiento promedio de los usuarios corporativos en Quito

Como se puede observar, la línea de tendencia de crecimiento de usuarios corporativos en Quito corresponde a una función de la forma $y = ax^b$. De la ecuación de esta curva y considerando que se conservará dicha tendencia, se obtiene la proyección para los siguientes cuatro años (a partir del 2002):

	AÑO 1	AÑO 2	AÑO 3	AÑO 4
Usuarios Proyectados	189	200	215	230

Tabla 3.4. Proyección del crecimiento de usuarios corporativos para 2 de los ISPs que abarcan el mercado en Qutio

Al final del año 2005, los ISPs que abarcan el mercado en la ciudad de Quito, contarán con un promedio de 230 usuarios corporativos por ISP. Uno de los objetivos del ISP que se diseña en el presente trabajo es llegar a tener más de

230 usuarios corporativos, por lo que se planifica que el ISP del diseño deberá crecer de la forma que se indica a continuación:

	Inicio	AÑO 1	AÑO 2	AÑO 3	AÑO 4
Usuarios esperados[a]	30	120	190	250	300

Tabla 3.5. Planificación de crecimiento de usuarios corporativos para el ISP de diseño

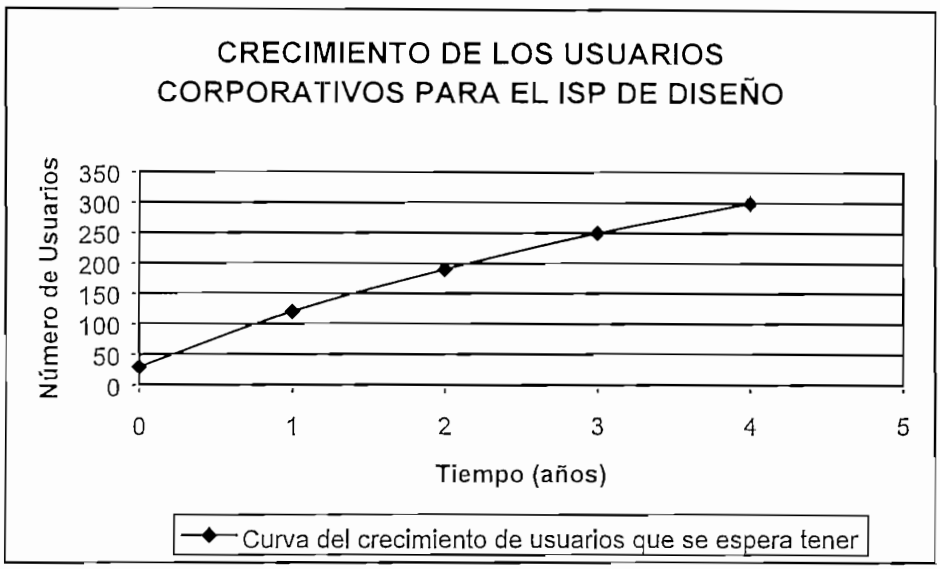


Fig. 3.4. Planificación de crecimiento de usuarios corporativos para el ISP de diseño

3.2.3. PLANIFICACIÓN DE LOS SERVICIOS QUE SE OFRECERÁN A LOS USUARIOS DEL ISP

En los primeros años de desarrollo del Internet, un ISP operaba en forma similar a la de un *carrier*. El ISP arrendaba capacidad de portadora y entonces revendía esta capacidad como un servicio de acceso a Internet, en este caso un ISP solamente servía de intermediario entre el cliente y la nube Internet. Este perfil de servicio del ISP ha evolucionado considerablemente en la década pasada, y ahora un perfil típico incluye un conjunto de elementos de servicio de valor agregado como: servicio de *mail,* servicio de resolución de nombres, servicio

[a] Distribución de usuarios sugerida por Satnet.

Web, servicio *Usenet*, FTP y otros que un ISP puede considerar como parte de la oferta de servicios a sus clientes.

Para la planificación de los servicios que ofrecerá un ISP, se deben considerar los siguientes puntos de vista:

Visión del Cliente

Para los clientes, el ISP tiene básicamente dos funcionalidades:

- Ofrecer conectividad a Internet, de manera que el usuario pueda utilizar todos los servicios que le ofrece la red.
- Servicios de Internet, el ISP debe garantizar al cliente la disponibilidad de sus servicios. Se hace especial hincapié en dos servicios que son masivamente empleados por los usuarios, éstos son: correo electrónico y WWW. Un tercer servicio de uso masivo es el de transferencia de archivos (FTP).

Para que un cliente pueda conectarse al ISP debe disponer del *software* necesario tal como: Windows98/NT, Mac OS, Linux, entre otros, los cuales incluyen un conjunto de aplicaciones necesarias para establecer la conexión, esto incluye el *stack* de protocolos TCP/IP.

El *software* de conexión en combinación con los navegadores que implementan *Web*: *Microsoft Internet Explorer* o *Netscape Communicator* permiten a los usuarios el acceso a Internet y a sus servicios. Ambos navegadores implementan HTML (*Web*), NNTP (noticias), FTP (transferencia de archivos) y SMTP/POP3 (correo), con esto los usuarios están conectados a Internet y pueden obtener otras aplicaciones desde la red.

Visión del Proveedor

La visión del proveedor es mucho más compleja, pues es él quien se encarga de entregar la conectividad a sus clientes. Un ISP pequeño, que es cliente de un ISP

mayor, puede delegar parte de este problema de conexión a Internet al ISP mayor. Por otro lado, el ISP ofrece servicios de Internet que son implementados en sus servidores, los mismos que forman la red interna del ISP.

Todo ISP debe velar por dos objetivos que son:

1. Debe mantener alta disponibilidad de conectividad con la Internet y sus clientes.
2. Debe mantener alta disponibilidad en la prestación de los servicios básicos.

Todos los otros servicios que el cliente desee pueden obtenerse una vez dentro de Internet utilizando los recursos que ya existen (*Hotmail*, buscadores como Altavista, *Web Hosting* gratuito, etc).

Para la planificación de los servicios que ofrecerá un ISP a sus clientes se debe considerar desde la población objetivo, es decir, los requerimientos planteados por los clientes hasta el nivel de servicios que ofrece la competencia. Es importante destacar que en el corazón de los servicios se encuentra el de resolución de nombres (DNS), pues permite la traducción de nombres a direcciones IP y viceversa, ésta es una función vital en el ambiente Internet y es un servicio que no puede faltar en un ISP.

Este ISP comenzará brindando a sus usuarios los siguientes servicios básicos: *E-mail, Web hosting y* FTP debido a su gran demanda y popularidad. A medida que los requerimientos crezcan (en base a la demanda de los clientes), se tendrán que hacer mejoras al portafolio de servicios del ISP; de esta manera, el ISP del diseño deberá ofrecer nuevos servicios como: *Usenet*, servicios de voz sobre IP, generación dinámica de páginas *Web*, comercio electrónico y otros servicios que pronto llegarán al país, tal como: Internet *call waiting* y *click to dial;* éstos dos últimos serán explicados con más detalle en la sección 3.2.3.1.

Para soportar todas estas aplicaciones se debe implementar adicionalmente los siguientes servicios: servicio de resolución de nombres (DNS), servicio de

autenticación de usuarios (Radius) y, servicios de facturación y tarifación de los clientes. Un servidor caché es altamente aconsejable para racionalizar el uso del ancho de banda.

Descripción de los Servicios

A continuación se dará una breve explicación de cada uno de los siguientes servicios: *E-mail, Web*, FTP, *Usenet, Telnet, Web Hosting*, DNS, *Proxy-Caché, Chat,* Servicios de voz, *Call Waiting, Click to Dial*.

Servicio de E-mail

El correo electrónico es uno de los servicios de mayor uso a través de Internet. Permite enviar mensajes de un usuario a otro en la red, con la posibilidad de adjuntar archivos, lo que lo transforma en un *servicio de encomiendas electrónicas* aumentando enormemente sus potencialidades.

Los proveedores de Internet dan una o dos cuentas de correo a sus clientes cuando solicitan una conexión a la red. De este modo, si una persona puede conectarse a Internet, puede enviar y recibir correo electrónico.

El sistema de correo de Internet , se basa en los protocolos SMTP (*Simple Mail Transfer Protocol;* Protocolo Simple de Transferencia de Correo) y POP3 (*Post Office Protocol versión 3*) o IMAP4 (*Internet Message Access Protocol versión 4;* Protocolo de Acceso de Mensajes de Internet). De estos tres protocolos el primero se encarga del envío y recepción del correo y cualquiera de los restantes permiten a los usuarios el acceso a los buzones de correo.

Desde el punto de vista del ISP, se deben incluir en las expectativas del cliente un conjunto de condiciones bajo las cuales el servicio de *mail* será operado. No es aconsejable que un ISP acepte la responsabilidad de mantener una cantidad arbitraria de *mails* de sus usuarios y durante un período indefinido de tiempo ya que existe gran incertidumbre acerca de los requerimientos de recursos y niveles

de carga que necesitará un cliente, por esta razón, un ISP no puede permitirse ofrecer un servicio de *mail* de alta calidad.

Una forma muy común de control es permitir que los *mails* sean almacenados solamente por cierto período de tiempo hasta que el proveedor los remueva. Un límite puede ser también la cantidad de *mails* almacenados en el servidor en términos de capacidad de memoria. El ISP puede hacer una distinción entre los *mails* que han sido leídos y los que no, implementando un pequeño período de retención de los *mails* que ya han sido leídos, luego del cual éstos serán borrados automáticamente del servidor.

Servicio Web

El servicio WWW fue desarrollado en el Centro Europeo de Investigación Nuclear (CERN). Su intención original era poder difundir de manera uniforme y simple contenidos a través de la red de modo que los científicos pudieran compartir su información, para lo cual se creó un mecanismo de Localización Uniforme de Recursos (URL).

Actualmente, el servicio más conocido y atractivo de Internet es el WWW (*World Wide Web*) el cual ofrece opciones para búsqueda de información independiente de cual sea su fuente y del lugar donde se encuentre. Ofrece transferencia de texto, imágenes, sonidos, animaciones, etc, por lo que se puede decir que el servicio WWW es la parte multimedia de Internet.

A este servicio se puede acceder mediante un *browser* o navegador como *Netscape Navigator* o *Microsoft Internet Explorer.* El *browser* es una aplicación que permite visualizar documentos escritos según el formato HTML (*Hyper Text Mark-up Language;* Lenguaje de Marcas de Hipertexto) que es el lenguaje de programación ideado para publicación de páginas Web. El servicio Web opera en base al protocolo HTTP.

Servicio de Transferencia de Archivos

El FTP es el protocolo que permite la transferencia de ficheros de datos entre dos ordenadores en una red TCP/IP. Estos ficheros pueden ser textos, imágenes, sonidos, programas, etc. Además, permite a un usuario borrar, renombrar, mover y copiar archivos en el servidor.

FTP requiere que un determinado usuario se identifique a través de un nombre de usuario y un *password*. Un usuario común puede utilizar el nombre de usuario *Anonymous* para tener acceso a un conjunto de archivos de uso público en un servidor FTP.

FTP dispone de una interfaz de usuario que permite: iniciar una sesión FTP, seleccionar directorios y archivos a transferirse, especificar el formato de presentación en el que un archivo debe ser transferido, llevar a cabo la transferencia de un archivo y finalizar la sesión.

Servicio de Noticias

Usenet News es el servicio más apropiado para intercambiar artículos a nivel mundial acerca de un determinado tema y de esta manera entablar foros de discusión. Consiste de un conjunto de grupos de noticias (*newsgroups*) que son clasificados dentro de jerarquía de similar interés en su contenido, y a su vez estas se dividen en subjerarquías. La lista principal de jerarquías está disponible en la Web en: http://home.magmacom.com/leisen/master_list.html.

Existen cerca de 500 jerarquías oficiales, pero las 8 más grandes son: *Usenet computer, Usenet discussions about humanities, Usenet miscellaneous, Usenet news, Usenet recreational, Usenet science, Usenet social issues* y *Usenet talk newsgroups.*

Un usuario de este servicio debe suscribirse a uno o varios de estos grupos de noticias para poder participar en los foros de discusión. *Browsers* como *Netscape Navigator* o *Internet Explorer* proveen soporte para *Usenet* y pueden acceder a

cualquier grupo de noticias que se escoja. Los artículos o mensajes que se envían a los grupos de noticias se hacen públicos y cualquier persona puede leerlos y enviar una contestación. En algunos casos estos foros de discusión tienen un moderador que filtra, edita y envía los mensajes.

Cada servidor de noticias, mantiene una copia del grupo de noticias y envía una copia de cada uno a los servidores de noticias vecinos, de esta manera se propagan las noticias.

NNTP (*Network News Transfer Protocol*; Protocolo de Transferencia de Noticias de Red), es el encargado de enviar, distribuir y recuperar mensajes de un servidor de noticias *Usenet*.

Servicio Telnet

Este servicio es llevado a cabo mediante el protocolo Telnet (terminal de red) para emular un terminal remoto virtual de una computadora.

Telnet permite a un cliente acceder remotamente a recursos en cualquier otra máquina en la red conocida como servidor Telnet evitando de esta manera la duplicación de recursos. Éstos pueden ser discos duros, manejo de archivos, ejecución de aplicaciones, acceso a datos, impresión de documentos en el lado remoto, etc. Para llevar a cabo esta compartición de recursos, la máquina remota deberá tener cargado un *software* de servidor Telnet.

El acceso remoto, antes considerado como privilegio de las redes corporativas, forma hoy parte de la planificación de cualquier red, esto se debe a que cada vez más personas trabajan a distancia.

Servicio de Web Hosting

Consiste en proveer al cliente del servicio un espacio para albergar sus páginas *Web* en un servidor denominado *Web Host* para su posterior publicación en la

WWW.

Este tipo de servicio puede ser gratuito o contratado. Los *Web Host* gratuitos limitan la capacidad del espacio a máximo 5 MB (típicamente) mientras que con los servicios contratados se pueden conseguir espacios entre 25, 100 MB o más[11]. La decisión de cual de estos servicios de *Web hosting* utilizar dependerá en gran escala de la imagen que el cliente desea tener en Internet (comercial, profesional, entretenimiento, etc). Si se desea capacidad de comercio electrónico u otros beneficios tales como operar con tarjetas de crédito a través de Internet, la solución óptima serán los servicios contratados.

Servicio de resolución de nombres

Las aplicaciones orientadas a los servicios de Internet no hacen referencia a las direcciones binarias (o decimales) de las máquinas que componen la red. En lugar de esto, los programas utilizan cadenas de caracteres ASCII (o nombres). Sin embargo, Internet solo maneja direcciones binarias, por lo que se necesita algún mecanismo que convierta los nombres en direcciones de red.

El DNS (*Domain Name Service; Servicio de Nombres de Dominio*) está constituido por una base de datos jerárquica y distribuida, que es usada por las aplicaciones TCP/IP para establecer la asociación entre los nombres de *host* y sus direcciones IP. Se dice que es *distribuida* puesto que no tiene nodos que contengan la información de nombres de toda la red Internet, sino que existe un sistema corporativo entre los servidores. El protocolo DNS permite a los clientes y servidores comunicarse entre ellos y de este modo compartir la información.

Para utilizar el DNS, la aplicación invoca a un *resolutor de direcciones* y le entrega como parámetro el nombre del *host*. El resolutor a su vez, envía la consulta al DNS local, el cual le retorna la dirección IP del *host*. Por último el resolutor entrega la dirección IP solicitada a la aplicación llamadora.

La estructura de la base de datos del DNS es jerárquica en forma de árbol. A

partir de la raíz de la base de datos se ramifican y se crean nodos de alto nivel, los cuales a su vez se subdividen. Cada nodo en el árbol de la base de datos del DNS, junto con todos sus nodos hijo es llamado un dominio.

Un dominio es una colección de nodos relacionados de alguna manera, como estar en una misma red o estar en una misma organización o país.

Dependiendo de la localización en la jerarquía, un dominio puede ser de primero, segundo o tercer nivel. Pueden existir otros dominios pero no son frecuentes. Los dominios de primer nivel pueden ser: dominios genéricos (edu, com, org, net, mil, gov, int, etc) y dominios geográficos o de país (ec, mx, es, ar, etc).

Servicio Proxy-Caché

Cuando un cliente solicita una página *Web* o archivo vía FTP, el servidor *Proxy-Caché* actúa de intermediario y solicita dicha página o archivo al destino final y se la reenvía al cliente. Este servidor mantiene una copia local y temporal en su memoria principal y/o secundaria de todas las páginas y archivos que han sido solicitados. Luego, frente a solicitudes repetidas de páginas o archivos, el servidor *Proxy-Caché* envía la que tiene en la memoria principal o secundaria. De este modo se puede mejorar los tiempos de respuesta en situaciones donde existe un enlace lento para acceder a los destinos fuera de la red, frente a enlaces locales rápidos.

Medidas de perfiles de tráfico de ISPs, indican que cerca del 70% del tráfico de un ISP es tráfico *Web*. Un análisis de demanda indica que el nivel típico de repetición de peticiones puede llegar a ser mayor que el 50% de todo el tráfico Web. Si el servidor Caché puede almacenar más del 50% del tráfico Web total, el ISP reduce los requerimientos de volumen de tráfico externo en aproximadamente el 17%[1].

El uso de un servidor *Proxy-Caché*, beneficia al cliente ya que se da un incremento de velocidad en la entrega de páginas *Web* debido a que el caché

está generalmente más cerca del cliente de lo que está la fuente original de la página *Web* solicitada, por lo tanto el tiempo de descarga desde el servidor caché es más rápido.

Servicio de Chat

El servicio IRC nos permite entablar una conversación en tiempo real con una o varias personas por medio de texto. También permite el envío de imágenes u otro tipo de ficheros mientras se dialoga.

Un uso más profesional del *chat* se puede realizar en redes locales corporativas a través de las herramientas que acompañan a los navegadores como *Netmeeting* de *Microsoft*. Estos programas pueden permitir además de un simple *chat*, aplicaciones de trabajo compartido, permitiendo la visualización de programas de forma simultánea en los ordenadores que están "charlando". Programas en el mercado como el ICQ de *Mirabilis* permiten un uso más sofisticado del *chat* puesto que notifica a los usuarios registrados en el servidor cuando determinado usuario se encuentra conectado.

Servicios de voz

Son las últimas aplicaciones que han aparecido para Internet. Permite establecer una conexión con voz entre dos personas conectadas a Internet desde cualquier parte del mundo sin tener que pagar el costo de una llamada internacional. Algunos de estos servicios incorporan no solo voz, sino también imagen. A esto se conoce como videoconferencias.

Otros servicios que se podrán ofrecer en el futuro son: *Internet call waiting, click to dial*, entre otros. *Internet call waiting* es un nuevo servicio que permitirá a los usuarios *dial-up* contestar llamadas telefónicas entrantes mientras navegan por Internet. *Click to dial* permitirá a los usuarios que navegan por el *Web* hacer una llamada telefónica mediante un *click* en el URL.

3.3. CONECTIVIDAD HACIA EL CLIENTE

3.3.1. TECNOLOGÍAS DE ACCESO

Existe una amplia variedad de tecnologías de acceso para conectar un ISP a sus clientes, éstas varían desde líneas *dial-up* hasta líneas arrendadas (líneas dedicadas), ISDN, *Frame Relay*, ATM, etc.

Debido a que existen varias opciones, a continuación se describirán en forma breve las tecnologías de acceso más comúnmente utilizadas.

3.3.1.1. Conexiones de línea telefónica

Es uno de los métodos más utilizados para conectarse a Internet (individualmente), consiste en utilizar un módem para marcar en un servidor de red. Estas líneas permiten velocidades desde 33.6 Kbps (V.34) hasta 56 Kbps (V.90) en los módems actuales.

Debido a la naturaleza analógica de las líneas telefónicas, los módems no pueden conectarse a velocidades mayores debido al ruido de la línea. También existe una limitación en el intervalo de frecuencias que se pueden llevar en una línea telefónica, limitando de esta manera la cantidad de datos que se pueden transmitir.

3.3.1.2. Líneas arrendadas

Las líneas arrendadas conocidas también como líneas o circuitos dedicados son la solución más simple y más utilizada para conectar un ISP a sus usuarios corporativos. Están formadas por un enlace punto a punto de forma permanente entre los *routers* que se desea unir.

Normalmente, no es posible contratar una línea dedicada de una velocidad arbitraria, existen velocidades prefijadas que son las que suelen ofrecer las compañías de telecomunicaciones, los valores estándares más comunes son: 56 Kbps, 64 Kbps, fraccional T1, T1 (1,536 Mbps, contiene 24 líneas T1 fraccionales de 64 Kbps, el término T1 es usado en USA, Australia y otras partes del mundo), E1 (2,048 Mbps, contiene 32 canales de 64 Kbps, estándar usado en Europa, Sudamérica y otras partes del mundo), E3 (34,368 Mbps, contiene 480 canales de 64 Kbps), T3 (44,736 Mbps, es equivalente a 28 circuitos T1, es decir 896 canales; es una línea arrendada de alta velocidad)

El precio de una línea dedicada es una cuota fija mensual que depende de la velocidad y de la distancia entre los puntos que se une. En las líneas dedicadas, la capacidad contratada está reservada en forma permanente a través de todo el trayecto.

3.3.1.3. RDSI

RDSI o ISDN (*Integrated Services Digital Network;* Red Digital de Servicios Integrados), está formada por enlaces digitales hasta el bucle de abonado, por lo que el circuito se constituye de forma digital de extremo a extremo. Esta es una red de conmutación de circuitos que pretende la óptima utilización de las líneas dedicadas ya que la conexión extremo a extremo solo se establece durante el tiempo necesario.

ISDN es una tecnología que elimina el problema analógico de la línea telefónica (ruido e interferencia) y proporciona canales digitales de datos de 64 Kbps. Contempla dos tipos de acceso al servicio:

El ***acceso básico*** denominado BRI (*Basic Rate Interface*; Interfaz de Velocidad Básica) o acceso 2B+D (2 canales digitales de 64 Kbps llamados canales B y 1 canal de 16 Kbps llamado canal D) y está orientado a usuarios domésticos o pequeñas oficinas; y el ***acceso primario*** también denominado PRI (*Primary Rate*

Interface; Interfaz de Velocidad Primaria) formado por 30B+D (en Europa) y 23B+D en USA y Japón, aquí todos los canales son de 64 Kbps. El acceso primario está pensado para grandes oficinas o centros proveedores de servicios

Un ISP puede ofrecer acceso RDSI a sus usuarios (que normalmente utilizarán un BRI) y en lugar de instalar múltiples accesos básicos instalar un acceso primario que le permitirá atender simultáneamente hasta 30 clientes o menos si decide permitir que los clientes que lo deseen utilicen 2 canales.

Las conexiones o llamadas RDSI se pagan con el mismo criterio que el de la red analógica y con los mismos ámbitos (local, regional, nacional, internacional).

3.3.1.4. xDSL

Recientemente han aparecido en el mercado una serie de tecnologías orientadas a obtener el máximo rendimiento posible del par de hilos de cobre que une al abonado con su central telefónica, ofreciendo al usuario la posibilidad de transmitir datos a velocidades del orden de megabits por segundo, una de estas tecnologías es ADSL, de la familia xDSL.

DSL (*Digital Suscriber Line;* Línea Digital de Abonado), utiliza el bucle de abonado para transmitir información digitalmente, pudiendo transmitir señales con un ancho de banda mayor, utilizando la parte alta del espectro del bucle de abonado por encima de los 4 Khz, separando tanto en la central como en los equipos de usuario los dos espectros para encaminarlos hacia distintos equipos. Cabe destacar que la cantidad de bits que pueden transmitirse dependen de la calidad del cable y de su longitud, es decir, a mayor longitud admisible y/o mejor calidad de cable, mayor capacidad.
A continuación, en la tabla 3.6 se exponen los tipos más importantes de las tecnologías DSL:

Tecnología DSL	Velocidad Upstream	Velocidad Downstream	Tipo de Tráfico	Distancia Máxima	Estanda-rización
ADSL[a]	16 a 640 Kbps	1.5 a 8 Mbps	Asimétrico	2-3 Km	Si
HDSL[b]	1.544-2.048 Mbps	1.544-2.048 Mbps	Simétrico	3-4 Km	Si
SDSL[c]	1.544-2.048 Mbps	1.544-2.048 Mbps	Simétrico	6-5 Km	No
VDSL[d]	1.6 a 19.2 Mbps dependiendo de la distancia	12.9 Mbps a 1.372 Km 55.2 Mbps a 0.305 Km	Simétrico o Asimétrico	300 m a 1 Km	En desarrollo

Tabla 3.6. Tecnologías xDSL [2]

Es conveniente resaltar la tecnología ***ADSL*** ya que ésta se está introduciendo lentamente en nuestro país y pretende ser el sustituto del módem tradicional, emplea la banda 30-138 Khz para el canal ascendente y 138-1104 Khz para el descendente. ADSL utiliza la técnica DMT (*Discrete Multi Tone;* Múltiples tonos discretos) que divide el rango en múltiples canales estrechos (de 4.3 Khz cada uno) y maneja cada canal de forma independiente. ADSL es un tipo de conexión punto a punto en la que el usuario no tiene que compartir su ancho de banda con ningún otro usuario. ADSL permite transmitir de forma simultánea voz y datos sobre la misma línea telefónica.

3.3.1.5. Frame Relay

Frame Relay ha evolucionado como alternativa a las redes de líneas dedicadas punto a punto, hacia una tecnología multiservicio capaz de transportar distintos tipos de datos y tráfico en tiempo real en una única conexión. *Frame Relay* es una tecnología basada en la conmutación de paquetes, usada a través de la interfaz entre los dispositivos de usuario (Ej. *routers*, máquinas *host*) y equipos de red (Ej. nodos de intercambio).

FR deja en manos de los equipos finales toda la labor de acuse de recibo,

[a] *Asymmetrical Digital Subscriber Line*; Línea Digital de Abonado Asimétrica.
[b] *High-bit-rate Digital Subscriber Line*; Línea Digital de Abonado de Alta Velocidad de Bit.
[c] *Symmetric Digital Subscriber Lline*; Línea Digital de Abonado Simétrica.
[d] *Very High-bit-rate Digital Subscriber Line*; Línea Digital de Abonado de muy alta Velocidad de Bit.

retransmisión de tramas erróneas y control de flujo, y no en cada nodo como lo hace X.25. FR incluye un algoritmo de chequeo cíclico redundante (CRC) para detectar los bits dañados (así el dato puede ser descartado), pero no incluye ningún mecanismo de protocolo para corregir los datos erróneos.

A diferencia de X.25, *Frame Relay* no tiene control de flujo ni genera acuses de recibo de los paquetes ya que esta tarea la deja a los niveles superiores en los equipos finales. Proporciona mecanismos simples de notificación de congestión para permitir a una red informar a un dispositivo de usuario que los recursos de red están cerca de un estado de congestión.

La tecnología FR basa su utilización en dos tipos de circuitos: circuitos virtuales conmutados SVCs y circuitos virtuales permanentes PVCs. FR define dos tipos de parámetros: la velocidad de información comprometida CIR, que representa la velocidad de transmisión unidireccional mínima garantizada en un PVC para un período de tiempo; y la velocidad de información en exceso EIR que define el margen de tolerancia, es decir, cuanto se va a dejar pasar del CIR contratado, si se intenta sobrepasar este parámetro el conmutador FR empezará a descartar tramas.

Las redes *Frame Relay* ofrecen una conexión local económica, escalable y altamente fiable entre el punto de presencia del ISP (POP) y el cliente. Los ISPs pueden beneficiarse de la capacidad de *Frame Relay* de manejar tráfico a ráfagas (*burst traffic*) para ofrecer un servicio básico a un precio establecido, y permitir tráfico en exceso si hay capacidad disponible.

3.3.1.6. ATM

La tecnología ATM (*Asynchronous Transfer Mode;* Modo de Transferencia Asíncrono), puede verse como una evolución de FR con la diferencia de que los paquetes ATM (denominados celdas) tienen una longitud fija de 53 bytes (5 de

cabecera y 48 de datos) frente al tamaño variable y mucho mayor de las tramas FR, simplificando el procesamiento en los nodos intermedios.

Al igual que en X.25 o FR, una red ATM se constituye mediante conmutadores ATM normalmente interconectados por líneas dedicadas, y equipos de usuario conectados a los conmutadores. Mientras que X.25 y FR utilizan velocidades de 64 Kbps y 2 Mbps respectivamente, en ATM las velocidades pueden llegar a 155.52 Mbps, 622.08 Mbps o incluso superiores.

Es una tecnología orientada a conexión pudiendo establecer circuitos virtuales permanentes o conmutados, garantizando de este modo que todas las celdas lleguen a su destino en el mismo orden en que salieron; sin embargo no se garantiza que lleguen todas las celdas, en situaciones de severa congestión se considera aceptable que haya una pérdida muy reducida de celdas.

ATM se basa en la creación de circuitos virtuales unidireccionales, de manera que para establecer un canal virtual *full duplex* crean dos circuitos con el mismo identificador lógico. ATM satisface de mejor manera a los usuarios brindando los siguientes servicios:

Clase	Descripción	Ejemplo
CBR	Constant Bit Rate	Enlace T1
RT-VBR	Variable Bit Rate, Real Time	Videoconferencia
NRT-VBR	Variable Bit Rate, Non Real Time	Correo con multimedia
ABR	Available Bit Rate	Navegar en WWW
UBR	Unspecified Bit Rate	FTP

Tabla 3.7. Clases de servicio [12]

CBR es útil para ofrecer los servicios que típicamente resuelve el sistema telefónico, aunque no hay control de errores, ni congestión ni ningún otro procesamiento extra. RT-VBR garantiza que la aplicación obtendrá el ancho de banda requerido y es útil en servicios de tiempo real como las videoconferencias y el despliegue de presentaciones tipo filme. NRT-VBR es igual que el anterior, excepto que el protocolo puede tener un retraso en la entrega *tal como en el*

servicio de correo electrónico. ABR está enfocado a ofrecer un ancho de banda base y si la aplicación requiere más entonces hará su mejor esfuerzo para incrementarla. UBR no promete ningún ancho de banda base ni control de flujo ni chequeo de errores, lo cual es útil para enviar paquetes IP y no incrementar la sobrecarga en el nivel de transporte. Si la red está congestionada, los paquetes son descartados sin avisar, pero si hay ancho de banda sobrante, se entregan la mayor cantidad de paquetes posibles.

3.3.1.7. Modems-cable

Fue diseñado para utilizar la ya existente infraestructura de televisión por cable fibra y coaxial, el cual fue optimizado para transmitir *broadcast* unidireccional. La capacidad del proveedor de servicios típico es 2 Mbps *downstream* y 64 Kbps *upstream*, siendo su ancho de banda compartido entre los múltiples usuarios de servicio en cada momento. La disponibilidad de esta tecnología está actualmente limitada en el país porque sus normas aún no se encuentran definidas.

3.3.2. DIMENSIONAMIENTO DEL NÚMERO DE LÍNEAS TELEFÓNICAS PARA USUARIOS *DIAL-UP*

Cuando se dimensiona el número de líneas telefónicas de un ISP, el objetivo es tener el mínimo número de líneas pero que puedan proveer adecuado acceso a todos los clientes. Como una referencia, a continuación se presenta una tabla que resume lo que puede suceder cuando se utiliza cualquiera de las siguientes relaciones usuario/línea:

Relación usuarios/línea	Calidad del Servicio
10:1	En este nivel de servicio, generalmente no se tendrán señales de ocupado excepto por breves períodos de tiempo en las horas pico.
12:1	Los usuarios encuentran la línea ocupada por menos de 2 minutos y aún consideran el servicio como bueno.
15:1	Con esta relación se pueden encontrar períodos de ocupación de 10 minutos o más, regularmente en la noche y los usuarios empiezan a quejarse del servicio.
18:1	Los usuarios empiezan a desertar del servicio ya que ellos no se pueden conectar por horas.
20:1 o más	Con esta relación un ISP llega a tener serios problemas. La mayoría de los clientes se sentirán descontentos y abandonarán el servicio.

Tabla 3.8. Calidad de servicio de acuerdo a la relación usuarios/línea [13]

Como regla, 10 usuarios por línea (10:1) es la relación sugerida para conexiones *dial-up* convencionales[13]. Sin embargo, no se puede decir exactamente cual es la relación de transformación usuario a línea correcta que se debería operar, ya que ésta puede variar debido a diversos factores como el tamaño del ISP y los servicios que éste desea proveer a sus usuarios. Existe una aproximación de cómo calcular esta relación[14] para lo cual se necesita conocer lo siguiente:

- El tiempo promedio en que los usuarios permanecen conectados.
- Cuántas veces entran o salen de Internet en un determinado día.
- Cuál es el período pico de uso que registra el ISP.

Las relaciones de transformación usuario/línea asumen que no todas las llamadas de los usuarios entran al mismo tiempo y suponen que todos los puertos son usados completamente durante todo el período pico, considerando el tiempo pico como el peor de los casos a fin de prevenir que los usuarios encuentren señales de ocupado. Para asegurarse que existan pocas señales de ocupado como sea posible, se necesita tener una relación de transformación usuario a línea ligeramente baja.

En la gráfica siguiente, obtenida mediante SNMP (*Simple Network Management Protocol*; Protocolo para la Administración Simple de una Red) por un ISP real en la ciudad de Quito el 3 de agosto del 2001, se observa la curva de tráfico de la cual se obtiene un intervalo de tiempo pico promedio de 6 horas (11:30 a 13:45h y desde las 15:00 a 18:45h).

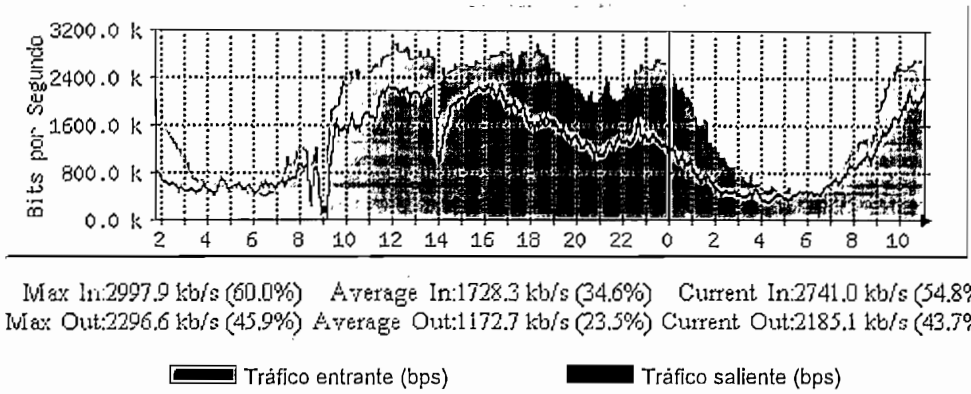


Fig. 3.5 Tráfico de entrada y salida de un ISP en el NAP de Access [9]

Además, el número de veces que un usuario entra o sale de Internet es de 3 veces en el día durante un tiempo total de 90 minutos (dato proporcionado por el ISP de la gráfica), por lo tanto, el tiempo promedio que los usuarios permanecen conectados es de 30 min. (90 min. / 3). Como el período pico es de 6 horas, se calcula que a lo largo de este período podrían llegar a conectarse hasta 12 personas, estableciendo sesiones de 30 minutos cada una.

$$\frac{1\ usuario}{30\ min.} * \frac{60\ min.}{1\ hora} * 6\ horas\ en\ el\ período\ pico = 12\ usuarios$$

dando una relación de 12:1 usuarios/línea, es decir, un módem puede manejar hasta 12 usuarios.

El número de líneas telefónicas necesarias puede ser calculado a partir de la siguiente expresión:

$$\#\ líneas\ telefónicas = \#\ usuarios\ dial-up * \frac{1\ línea}{12\ usuarios}$$

Ec. 3.2. Fórmula para el cálculo del número de líneas telefónicas

Proyección

Con el número de usuarios esperados que se obtuvo anteriormente y con la relación 12:1 se puede obtener el número de líneas telefónicas (E1s) que se adquirirán conforme crezca el ISP.

PROYECCIONES	Inicio	AÑO 1	AÑO 2	AÑO 3	AÑO 4
# Clientes Dial-up	300	2089	4474	6859	9244
Líneas telefónicas	25	174	373	572	770
E1s	1	6	13	19	26

Tabla 3.9. Proyección del número de líneas telefónicas

3.4. CONECTIVIDAD A LA INTERNET

Para proveer servicios de acceso a Internet, obviamente, la red del ISP necesita estar conectada a Internet. Dicha conexión es a través de uno o más enlaces WAN (generalmente a través del enlace satelital) a ISPs de niveles superiores, estos proveedores son usualmente llamados proveedores de *backbone* o proveedores *upstream*.

3.4.1. DIMENSIONAMIENTO DEL ANCHO DE BANDA SATELITAL

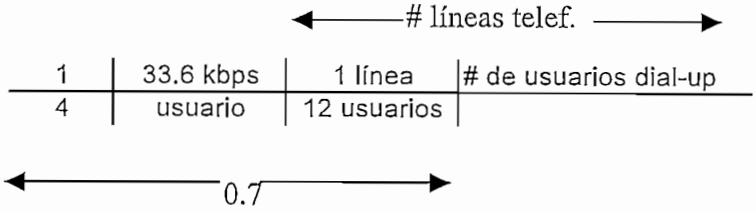
El ancho de banda satelital será calculado mediante la relación usuarios/línea, el *throughput* promedio y la calidad de servicio que se va a brindar a los usuarios tanto *dial-up* como corporativos.

AB para usuarios dial-up:

Calidad de servicio = 4:1[a]

Throughput promedio = 33.6 Kbps por usuario

Relación usuarios/línea = 12:1

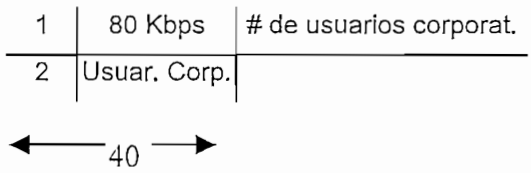


$$AB_{DIAL-UP} = 0.7 * \#\ de\ usuarios\ dial-up$$

AB para usuarios corporativos:

Ancho de banda promedio = 80 Kbps por usuario corporativo (64 Kbps de bajada + 16 Kbps de subida).

Calidad de servicio = 2:1[a]



$$AB_{CORPORATIVO} = 40 * \#\ usuarios\ corporativos$$

Por lo tanto, la fórmula para el cálculo del ancho de banda queda resumida de la siguiente manera:

$$AB = 0.7 * \#\ usuarios\ dial + 40 * \#\ usuarios\ corporativos$$

Ec. 3.3. Ecuación para el cálculo del ancho de banda

[a] Calidad recomendada por un ISP real en la ciudad de Quito. Este valor significa que en el peor de los casos (horas pico), un cliente *dial-up* no va a tener una velocidad de 33.6 Kbps, sino la cuarta parte de este valor.

[a] Calidad recomendada por un ISP real en la ciudad de Quito. Lo óptimo sería ofrecer al cliente una relación de 1:1 ya que éste está pagando por su ancho de banda; sin embargo, los ISPs aprovechan que el cliente no ocupa el 100% de su ancho de banda y que su utilización es estadística para ofrecer menor calidad de servicio. En el país, algunos proveedores inclusive ofrecen calidad de servicio muy por debajo de lo aconsejable (3:1, 4:1 o aún de 5:1) lo cual ocasiona la degradación del servicio y la consecuente inconformidad del cliente.

Se pretende que el ISP del diseño se conecte al NAP Ecuador donde intercambiará tráfico con otros ISPs en la ciudad de Quito, evitando que el tráfico nacional circule a través del enlace satelital. Según técnicos ecuatorianos, con la creación del NAP Ecuador, el tráfico de datos hacia el exterior disminuirá hasta un 30%[3], como se explica más adelante.

Para el enlace satelital, un ISP requiere un ancho de banda de bajada mayor que el ancho de banda de subida, ya que la mayor parte de clientes "bajan" información de Internet. La relación recomendada que será utilizada por este ISP en la ciudad de Quito es de 4:1[1], es decir: $AB_{BAJADA} = 4 * AB_{SUBIDA}$. Por consiguiente:

$$AB = AB_{SUBIDA} + AB_{BAJADA} = AB_{SUBIDA} + 4 * AB_{SUBIDA} = 5 * AB_{SUBIDA}$$

Proyección

En la tabla 3.10. se indican los resultados de los cálculos realizados para el ancho de banda satelital conforme crezca el ISP:

			Kbps				
	# USUARIOS		AB	NAP	SATELITE	AB BAJADA	AB SUBIDA
	Dial-up	Corporat.	0.7*# dial+40*# corp.	0.3*AB	0.7*AB	4*Absub	
Inicio	300	30	1410	423	987	789,6	197,4
AÑO 1	2089	120	6262	1879	4384	3506,9	876,7
AÑO 2	4474	190	10732	3220	7512	6009,8	1502,5
AÑO 3	6859	250	14801	4440	10361	8288,7	2072,2
AÑO 4	9244	300	18471	5541	12930	10343,6	2585,9

Tabla 3.10. Proyecciones del ancho de banda satelital

Para evitar congestión y la posibilidad de degradar el servicio, hay que realizar un buen diseño del ancho de banda con suficiente anticipación, monitoreando su uso de forma permanente. Si el tráfico aumenta por encima del valor umbral recomendado que es del 70% durante una semana o con picos de más del 90% durante 5 minutos, es señal de que la demanda está por encima de la capacidad disponible, lo que indica que hay que aumentar el ancho de banda o poner

nuevos enlaces. Algo similar ocurre cuando se detecta una pérdida de paquetes superior a un cierto umbral (mayor al 2%) durante períodos de 5 minutos, es señal de escasez de capacidad[1].

3.4.2. CÁLCULO DE LOS RETARDOS EN LA DESCARGA DE PÁGINAS *WEB*[4]

En esta sección se expondrán los resultados de los cálculos para determinar los retardos en descargar páginas *Web* de Internet. Estos retardos son calculados con el objetivo de determinar qué tan eficiente es el ISP del diseño.

Para dichos cálculos se han utilizado los valores obtenidos en el diseño del ISP como son: número de líneas telefónicas, capacidad satelital, etc.

En la tabla 3.11. se indica el retardo total en segundos para "bajar" páginas de 50 KB para valores de N (tamaño del segmento máximo de la ventana de congestión) de 512, 1024 y 2048 bytes, y para bajar páginas de 100 y 1000 KB desde la red Internet a través del ISP diseñado en este proyecto.

X [KB]	N [bytes]	Ret. Total f(SD) [seg]	Ret. Total (seg)
50	512	17.65 + 478400/SD	31,96
	1024	16.50 + 456800/SD	30,17
	2048	15.65 + 445200/SD	28,97
100	512	32.13 + 931200/SD	60,00
1000	512	288.44 + 9068800/SD	559,77

Tabla 3.11. Resultado de los cálculos para retardos de descargas de páginas Web

En conclusión, para que un usuario descargue una página de un determinado tamaño, a medida que aumenta el tamaño del segmento máximo disminuye el retardo, mientras que para un mismo valor de N a medida que aumenta el tamaño del archivo a descargar también aumenta el retardo.

Para mayor información del cálculo de retardos, referirse al Anexo A.

4

DISEÑO DEL SISTEMA DE SEGURIDAD DEL ISP

3.4.3. INTERACCIÓN CON OTROS ISPs

Ya que Internet es una colección de redes interconectadas que interactúan entre sí, un ISP no puede operar aisladamente. Cada proveedor no debe solamente coexistir con otros ISPs, debe además operar en cooperación con ellos. Esta relación de dependencia entre ISPs es debido a que los clientes esperan poder conectarse con usuarios de otros ISPs y en cualquier parte del mundo. El cliente de un ISP no contrata un servicio que limite su conectividad.

Ningún proveedor de Internet ofrece acceso a todos los puntos del mundo, por tal razón, cada ISP debe confiar en otros proveedores para completar su conectividad y tener cobertura universal.

Es difícil hacer una clara distinción entre ISPs clientes e ISPs proveedores de servicio. Un ISP que revende conectividad a Internet, opera en ambos sentidos: tanto como cliente y como proveedor, lo cual es muy común en Internet. Por ejemplo: una red de un campus puede ser cliente de uno o más proveedores de servicio y a la vez puede ser proveedor de servicio a los usuarios del campus.

Efectivamente, la mayoría de redes en Internet tienen un doble papel de cliente y proveedor. Consecuentemente el entorno de conexión entre ISPs no sigue un modelo en el cual se pueda hacer una clara distinción entre proveedores mayoristas y minoristas. Existe una gran cantidad de ISPs orientados a la reventa, cada uno puede operar tanto como proveedor mayorista (que vende acceso a otros ISPs) y como minorista (que compra acceso a ISPs *upstream*).

Interacción Física: Intercambios y NAPs

Dentro de Internet, es conveniente asegurar que el camino físico que debe atravesar un paquete hasta su destino sea el más corto y el más rápido posible. La distancia más corta entre un transmisor y un receptor requiere un presupuesto más bajo: *más cerca es más barato.* En cambio, un enlace más rápido minimizará el retardo entre el receptor y el emisor permitiendo que las

comunicaciones sean más eficientes: *más cerca es más rápido y más rápido es más eficiente.*

Un modelo jerárquico es una estructura en la cual el tráfico entre dos ISPs locales debe forzosamente ir a un ISP regional, luego a un ISP nacional y finalmente a un ISP de tránsito para luego recorrer el mismo camino en sentido descendente hasta alcanzar al ISP local destino, como se indica en la figura 3.6. Esta forma de interconexión de ISPs es ineficiente ya que un paquete tiene que recorrer caminos largos, costosos y con grandes retardos. Estos costos se verán reflejados en el precio que los usuarios finales tendrán que pagar por el acceso a Internet.

En un mercado altamente competitivo como lo es Internet, existen fuertes presiones que obligan a los proveedores a interconectar sus redes para reducir los costos. Por ejemplo, los ISPs locales bajarían sus costos si interconectan sus redes con las de otros ISPs locales para permitir el intercambio de tráfico local, evitando de esta manera el pago de los costos de tránsito a los respectivos proveedores de tránsito.

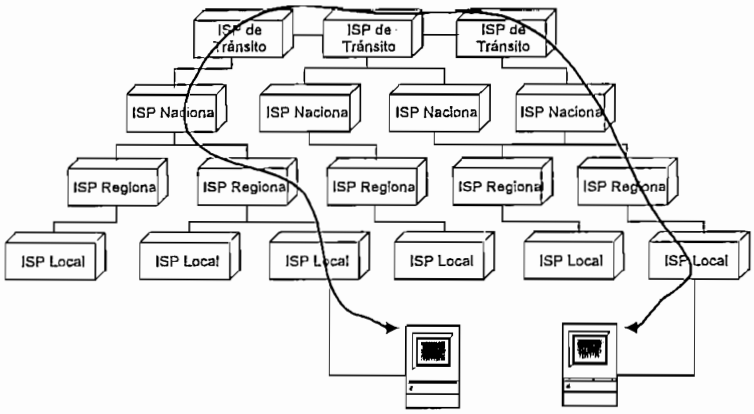


Fig.3.6. Estructura jerárquica de la Internet [1]

Aunque es posible construir una estructura basada en conexiones bilaterales punto a punto (es decir, todos los IPSs interconectando sus redes en una estructura en malla), este método no ofrecería buenas propiedades de escalabilidad ya que entre N proveedores que deseen interconectarse se necesitarían $N/2*(N-1)$ circuitos. Para simplificar la estructura anterior, cada

proveedor se conecta a un punto de intercambio de tráfico utilizando un solo circuito y entonces lleva a cabo interconexiones con otros ISPs conectados a este mismo punto. De esta manera, si N proveedores desean interconectarse necesitarán solamente N circuitos punto a punto.

Un NAP (*Network Acces Point*; Punto de Acceso a la Red) es un punto al cual se conectan los proveedores de Internet para intercambiar tráfico y rutas a través de acuerdos de interconexión. El acuerdo de intercambio de información entre dos o más ISPs en un NAP es llamado *peering*. En un acuerdo de *peering*, dos ISPs intercambian tráfico de Internet que se origina y va destinado a sus respectivas redes. Un acuerdo *peering* es llevado a cabo entre ISPs de similar tamaño ya que la cantidad de tráfico que se intercambie entre ellos será también similar y el trato entre uno y otro es igualitario.

Un acuerdo *peering* puede ser bilateral o multilateral. Es bilateral si solamente dos ISPs acuerdan intercambiar tráfico y rutas. Es multilateral cuando se realiza *peering* con varios ISPs a la vez.

Los NAP pueden ser clasificados de acuerdo a su tecnología y a su cobertura. De acuerdo a su tecnología un NAP puede ser: un *router*, una red LAN o WAN, o un *switch* de alta velocidad. De acuerdo a la cobertura, éstos pueden ser clasificados en NAPs centrales, regionales, nacionales y locales.

Los cuatro NAPs centrales originales fueron establecidos en los Estados Unidos en: San Francisco (operado por *Pacific Bell*), Chicago (operado por *Ameritech*), New Jersey (operado por *Spring*), y en Washington DC (operado por *Metropolitan Fiber Systems*).

Además de éstos, varios NAPs han surgido alrededor del mundo como una solución para reducir los costos de ancho de banda que se necesitan de un proveedor de los Estados Unidos y además para mejorar la calidad del servicio; entre éstos, se mencionarán los recientemente inaugurados: ***NAP de las Américas*** y el ***NAP Ecuador***

3.4.3.1. NAP de las Américas

Entró en funcionamiento el 21 de junio del 2001. Con sede en la ciudad de Miami, este NAP conectará Latinoamérica con Norteamérica y Europa. Este es el quinto NAP mundial de nivel 1 (NAP central), es un *TerreNAPsm DataCenter*, propiedad de *Terremark Worlwide* y operado por la misma (empresa líder mundial en el suministro de infraestructura para Internet).

Hasta la fecha, 29 clientes, cuyo número va en aumento, han firmado contratos por varios años para generar ganancias con el fin de alojar sus equipos de mayor importancia en el NAP y actualmente ya pueden empezar el envío de tráfico[3].

3.4.3.2. NAP Ecuador

Empezó a operar el 4 de julio del 2001. Ubicado en la ciudad de Quito, este NAP local además de mejorar la velocidad de transmisión, logrará descongestionar la red internacional y abaratará los costos satelitales en un 20%, ya que según los técnicos, el tráfico de datos hacia el exterior bajará hasta un 30%. A futuro, éste método permitirá enviar datos directamente hacia otros países de Latinoamérica, es decir, si un usuario debe enviar información a Colombia, es preferible hacerlo de forma directa sin que dicha información deba pasar primero por los Estados Unidos[3].

El NAP Ecuador permitirá dirigir la información a su destino de manera que se acorten las distancias, es decir, si un usuario de Internet vive en Quito y debe enviar un e-mail a otro en la misma ciudad, no deberá hacer el camino por el satélite. El NAP recibirá estos datos y en función del usuario final, seleccionará los datos para ser enviados localmente.

En la actualidad no todos los ISPs se encuentran conectados a este NAP, pero tendrán que converger a este sistema porque reduce los costos satelitales y optimiza las comunicaciones a nivel interno. Las empresas proveedoras de

Internet conectadas al NAP Ec son:

Fig 3.7. ISPs conectados al NAP Ecuador[9]

Este NAP ofrecerá grandes beneficios al usuario final, ya que esto le significa un mejor tiempo de respuesta en el acceso al contenido de las páginas Web que residen en el país, así como un ágil envío y recepción de sus correos.

3.5. DIMENSIONAMIENTO DE LA CAPACIDAD DE LOS SERVIDORES

Un servidor es una combinación de *hardware* y *software* diseñado para recibir peticiones y enviar respuestas, por tal razón, es necesario realizar una buena combinación entre plataformas de *hardware* y sistema operativo.

Un parámetro de *hardware* muy importante y cuyo dimensionamiento se lo realizará a continuación es la ***capacidad del disco duro***. Los requerimientos del espacio de almacenamiento de los servidores es determinado por la cantidad de información inicial que se almacenará en el servidor y por un valor adicional para poder crecer o la posibilidad de aumentar discos duros.

A continuación, se dimensionará la capacidad de disco duro que necesitarán los distintos servidores, estos valores serán los parámetros mínimos con los que se deberá contar de inicio para poder satisfacer las necesidades de los usuarios del ISP durante el primer año.

3.5.1. CAPACIDAD DE DISCO DEL SERVIDOR DE *E-MAIL*

Para dimensionar la capacidad de disco duro del servidor de e-mail se deben tener en cuenta dos parámetros importantes: el número de usuarios *dial-up* que tendrán cuentas de correo y el espacio de disco que se asignará a cada cliente para albergar sus mensajes.

Los usuarios corporativos generalmente tienen sus propios servidores de *mail* con su propio dominio; sin embargo, se considera conveniente agregar un valor adicional a esta capacidad de disco (3 GB[a]), ya que existe la posibilidad de que las pequeñas empresas, clientes del ISP, requieran también espacio de disco para albergar sus mensajes de correo.

Normalmente, un proveedor asigna a sus usuarios un espacio de 5 a 15 MB por cuenta. Para este diseño, se asignará 10 MB por cuenta siendo éste un valor promedio de los anteriormente mencionados. De esta manera, se tiene el siguiente cálculo[15]:

$$Capacidad\ de\ disco = \#\ usuarios \times espacio\ por\ usuario + espacio\ adicional$$

[a] Capacidad recomendada por el personal técnico de Andinanet.

$$Capacidad\ de\ disco = 2089\ usuarios \times 10\ MB + 3\ GB$$

$$Capacidad\ de\ disco = 24\ GB$$

3.5.2. CAPACIDAD DE DISCO DEL SERVIDOR *WEB HOSTING*

El servicio de *Web Hosting*, normalmente es utilizado por los clientes corporativos ya que son éstos quienes desean tener presencia en Internet a través de su propia página *Web*. Hay que recalcar que las grandes empresas son propietarias de sus servidores de *Web Hosting* y correo electrónico, por esta razón no necesitarán de este servicio por parte del ISP. Sin embargo, según experiencias en nuestro país, se conoce que quienes utilizan el servicio de *Web Hosting* son en su mayoría las pequeñas empresas debido a que éstas no poseen un servidor propio.

Como se indicó en la sección 3.2.1 el número de empresas existentes en la ciudad de Quito es de 8500. Según datos obtenidos de la Superintendencia de Compañías, el número de pequeñas empresas existentes en Quito es de 4270, valor que corresponde al 50.23%. Conociendo que el ISP de diseño pretende tener 120 usuarios corporativos al final del primer año, el número de posibles usuarios (pequeñas empresas) correspondería al 50.23% de 120 usuarios corporativos, dando un resultado de 60 usuarios.

Tomando en cuenta lo dicho anteriormente, la capacidad de disco del servidor *Web Hosting* puede ser determinada tomando en cuenta dos parámetros: el tamaño del espacio que generalmente se asigna a un usuario de este servicio (50 MB[a]) y el número de posibles clientes. De esta manera, se tiene el siguiente cálculo:

$$Capacidad\ de\ disco = \#\ posibles\ usuarios \times espacio\ por\ usuario$$

$$Capacidad\ de\ disco = 60\ usuarios \times 50\ MB$$

$$Capacidad\ de\ disco = 3\ GB$$

[a] Capacidad recomendada por el personal técnico de Andinanet.

3.5.3. CAPACIDAD DE DISCO DEL SERVIDOR CACHÉ

Para dimensionar la capacidad del disco duro del servidor caché se deben tomar en cuenta los siguientes parámetros: ancho de banda al final de primer año (o del período para el cual se desea hacer el cálculo), período pico de uso del enlace y máxima cantidad de información transmitida en un día.

Durante el intervalo pico se genera la mayor cantidad de tráfico y por ende la mayor cantidad de páginas *Web* serán almacenadas en el servidor caché en este tiempo. Para los períodos restantes del día, se registrarán tanto peticiones repetidas de las páginas *Web* ya almacenadas como también nuevas solicitudes. El servidor caché retirará de su disco ciertas páginas que no han sido solicitadas en un intervalo de tiempo configurable en el servidor proporcionando espacio para almacenar las nuevas páginas solicitadas el resto del día.

Teniendo en cuenta estos criterios y considerando que el ancho de banda satelital requerido al final del primer año es 6262 Kbps y que el período pico es de 6 horas al día se tiene el siguiente cálculo:

$$Cantidad\ de\ inf.transmitida = 6262\frac{Kb}{seg}\times 60\frac{seg}{min}\times 60\frac{min}{hora}\times 6\frac{horas\ pico}{día}$$

$$Cantidad\ de\ inf.\ transmitida = 135.3\ Gb = 16.5\ GB$$

Este es el tráfico que el ISP generaría durante el período pico en un día. Como se indicó en la sección 3.2.3, cerca del 70% del tráfico es tráfico Web y según el análisis de demanda, el nivel típico de repetición de peticiones puede llegar a ser mayor que el 50% de todo el tráfico Web, de manera que:

$$Capacidad\ de\ disco = Cantidad\ de\ inf\ transmitida \times 0.7 \times 0.5$$

$$Capacidad\ de\ disco = 16.5\ GB \times 0.7 \times 0.5$$

$$Capacidad\ de\ disco = 5.8\ GB$$

3.5.4. CAPACIDAD DE DISCO DEL SERVIDOR FTP

Según técnicos de Andinanet en la ciudad de Quito y basados en experiencias reales, se sugiere que este servidor debe ser de capacidad similar a la del servidor *Web hosting*, ya que es aquí donde se encuentran almacenados los programas que el ISP ofrece para que sus clientes los descarguen, es decir, la capacidad requerida será:

$$Capacidad\ de\ disco = 3\ GB$$

3.5.5. CAPACIDAD DE DISCO DEL SERVIDOR DNS

La capacidad de disco para este servidor será obtenida a partir de valores sugeridos por ISPs con amplia experiencia en este campo (Impsat). Ellos recomiendan que el disco duro de este servidor debe tener una partición de 4 GB para almacenar el sistema operativo y 9 GB para el almacenamiento de archivos DNS.

$$Capacidad\ de\ disco = 13\ GB$$

Una forma de determinar la capacidad de este servidor, según el personal técnico de Andinatel y basándose en la práctica, se lo calcula como el 30% de la capacidad de disco del servidor de *E-mail* más 4 GB para el sistema operativo.

$$Capacidad\ de\ disco = 30\% * 24\ GB + 4\ GB$$
$$Capacidad\ de\ disco = 11.2\ GB$$

Esta capacidad se asemeja a la sugerida por los otros proveedores.

En cuanto al servidor secundario, éste debe tener la misma capacidad del servidor DNS primario, de manera que cuando caiga el primario éste funcionará como servidor de respaldo.

3.5.6. CAPACIDAD DE DISCO DEL SERVIDOR DE TARIFACIÓN Y FACTURACIÓN

La capacidad de disco de este servidor dependerá casi en su totalidad del software de facturación que se utilice. Normalmente, este *software* es diseñado por una empresa especializada en base a requerimientos específicos de cada ISP, por esta razón se recomienda adquirir el *hardware* una vez que se conozca el tamaño del *software* de facturación.

La capacidad de los servidores de tarifación y facturación en los ISPs visitados (Andinanet, Satnet, Impsat) tienen un valor promedio de 36 GB.

3.6. CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS

A continuación se detallarán las características técnicas mínimas que debe satisfacer el equipo que conformará el ISP. Se comenzará describiendo los requerimientos de los servidores para luego continuar con los dispositivos de comunicaciones como son: servidores de acceso, *routers* y *switches*. Al final de cada dispositivo se citarán sugerencias de los equipos que cumplen con dichas características técnicas y se resaltará en letra cursiva los equipos que serán utilizados en el diseño.

Las opciones de *software* para los distintos servidores con respecto al sistema operativo son detalladas en el anexo C.

3.6.1. SERVIDOR *WEB CACHING*

Antes de entrar en detalle sobre las características técnica que debe cumplir el servidor caché, se mencionarán algunos puntos que se deben tener en cuenta a la hora de ubicar un servidor *Web Caching* en el ISP con el objeto de obtener el máximo beneficio.

En vista que el servidor *Web Caching* almacena todos los datos que van dirigidos al puerto TCP/IP número 80 (puerto WWW), es conveniente ubicar este servidor en el mismo segmento de red del *router* principal del ISP. Esta ubicación estratégica se debe a que este servidor trabaja junto con el *router* principal, es decir se complementan, de manera que así acortan el tiempo de procesamiento de la información haciendo más rápido el servicio a los usuarios.

Si el ISP se ha extendido a otras áreas geográficas mediante POPs (ya que una de las metas del ISP es llegar a ser uno de nivel nacional) y si éste necesita incrementar el número de servidores caché para formar una *granja de servidores,* se recomienda colocar un único servidor caché en cada PoP y varios servidores caché en los *routers* de la oficina principal a excepción del *router* que se conecta al Internet.

Esta nueva estrategia es fuertemente recomendada ya que si se colocara la granja de servidores caché en el mismo segmento de red del *router* principal de la oficina central como se indicó anteriormente, el segmento de red que contiene estos servidores experimentará un significativo incremento de tráfico ocasionando "cuellos de botella".

El servidor *Web Caching* a seleccionar debe cumplir con las siguientes características técnicas:

- Disponer de una interfaz 10/100 Fast Ethernet.
- Velocidad del procesador: 500 Mhz mínimo.
- SRAM mínimo: 256 MB.
- Almacenamiento: 9.1 GB (Ultra SCSI) expandible hasta 18 GB.
- Soporte HTTP 1.0, 1.1.
- Memoria flash de 16 GB.
- Alimentación eléctrica a 110V / 60 Hz.
- Cables eléctricos y de datos.
- Soporte de jerarquías ICP.
- Garantía técnica: 2 años contra defectos de fabricación.

- *Software* a utilizar: IOS de Cisco con el protocolo WCCP v2 (Web Cache Communication Protocol; Protocolo de Comunicación del Caché Web) .

Sugerencias

Entre otros, los productos que cumplen con las características anteriores son: *Content Engine 560 de Content Delivery Network Products de Cisco*, 3Com SuperStack 3 Webcache 3000: Número de parte 3C16116, CacheFlow: Server Accelerator 725.

3.6.2. SERVIDOR RADIUS

El servidor RADIUS que se debe adquirir deberá realizar las funciones de autenticación, autorización y *accouting* (contabilidad) de los usuarios: AAA, para lo cual debe soportar los protocolos RADIUS y TACACS+.

Los requisitos mínimos de *hardware* y *software* que debe cumplir este servidor son los siguientes:

- 1 Interfaz 10/100 Fast Ethernet.
- Procesador Pentium III mínimo, con velocidad de 300 MHz o más rápido.
- Memoria RAM de 128 MB o 256 MB recomendada para Windows NT Server.
- Al menos 150 MB de espacio de disco libre. (Si se está corriendo la base de datos en la misma máquina, se requiere más espacio de disco).
- Resolución mínima de la pantalla de 256 colores en 800*600 líneas.
- Debe operar sobre el sistema operativo Windows NT 4.0 o Windows 2000.
- Compatibilidad con el NAS utilizado para el acceso de usuarios *dial-up* y con el *firewall.*
- Capacidad para actualizar las versiones de los *software* utilizados.
- Soporte para los principales protocolos de autenticación: Radius, ASCII / PAP, CHAP, MS-CHAP, Generic LDAP, Microsoft MCIS, etc.
- Opciones para réplicas de la base de datos (*Database Replication*) y

servicios de *backup*, para hacer el entorno AAA más tolerante ante fallas.

- *Software* a utilizar: *Steel Belted* Radius

Sugerencias

Se recomienda utilizar cualquiera de los siguientes equipos: *Cisco Secure Access Control Server* o Steel Belted RADIUS de Funk.

3.6.3. SERVIDOR DE *E-MAIL* Y DNS

El servidor de *E-Mail* y el servidor DNS pueden ser combinados en un único servidor[16], pero si se planea ubicarlos en máquinas diferentes, entonces cada uno de ellos deberá cumplir con las siguientes especificaciones:

Servidor de E-Mail

Un servidor de *E-Mail*, a veces referido como un *messaging server,* deberá cumplir con las siguientes requisitos mínimos:

- 1 Interfaz 10/100 Fast Ethernet.
- Procesador: 500 MHz mínimo.
- Se necesitará mínimo 24 GB libres una vez instalado el *software* correspondiente, para lo cual se adquirirá un disco duro SCSI de 36 GB.
- Memoria RAM: 512 MB.
- Capacidad de expansión de hasta 5 discos duros.
- Características para la detección de virus, segregación de *mails* dudosos y manejo de *spams*.
- Soporte para protocolos SMTP, ESMTP, POP3, IMAP4, MIME.
- Soporte para encriptación de mensaje mediante SSL o RSA.
- *Software* a utilizar: *Sendmail*

Servidor DNS

Se resumen a continuación las características que debe reunir este servidor:

- 1 Interfaz 10/100 Fast Ethernet.
- Velocidad del procesador: 500 Mhz mínimo.
- SRAM: 512 MB mínimo.
- Capacidad de disco: 18 GB SCSI expandible hasta 2 discos duros.
- 1 puerto paralelo, 2 seriales, 1 puerto para teclado.
- Memoria caché externa de 2 MB mínimo.
- CD-ROM 52x.
- *Software* a utilizar: BIND

Si se decide utilizar un solo servidor para *E-Mail* y DNS, como es el caso de este diseño, el servidor deberán cumplir las siguientes características:

- Disponer de dos interfaces 10/100 Base-TX.
- Velocidad del procesador: 800 MHz mínimo.
- SRAM mínimo: 1024 MB.
- Capacidad de disco: 36 GB SCSI.
- Caché externa de 2 MB mínimo.
- Capacidad de expansión para 5 discos duros *hot swap* (*scalable clustering*)
- CD-ROM 52x.

Sugerencias

Servidor Altos 1200 de Acer, Servidor Sun Blade 100 de Sun Microsystem, Servidor Compaq Proliant ML370 de Compaq, entre los principales.

3.6.4. SERVIDOR *WEB HOSTING* Y FTP

Al igual que los servidores de *E-mail* y DNS, los servidores de *Web Hosting* y FTP también pueden ser combinados en un solo servidor que cumpla con los

siguientes requerimientos:

- Disponer de dos interfaces 10/100 Base-TX.
- Velocidad del procesador: 800 MHz mínimo.
- SRAM mínimo: 1024 MB.
- Almacenamiento: 8 GB SCSI expandible hasta 36 GB.
- Caché externa de 2 MB mínimo.
- Capacidad para 5 discos duros *hot swap* (*scalable clustering*).
- CD-ROM
- Software a utilizar: Apache para el servidor *Web*
  War FTP *Daemon* para el servidor FTP

Sugerencias

Servidor Altos 1200 de Acer, Servidor Sun Blade 100 de Sun Microsystem, Servidor Compaq Proliant ML370 de Compaq.

3.6.5. SERVIDOR DE TARIFACIÓN Y FACTURACIÓN

Las características del equipo de tarifación y facturación se detallan a continuación:

- Procesador Intel Pentium III.
- Velocidad del procesador: 1 GHz.
- Memoria SDRAM 128 MB expandible a 4 GB.
- Disco duro SCSI de 36 GB.
- CD-ROM 48X.
- Red 10/100.
- 2 bahías *hot swap*.
- Fuente de poder de 110V.
- El *software* para este servidor debe ser diseñado por una empresa especializada en base a requerimientos específicos de cada ISP.

Sugerencia

Servidor Altos 1200 LP de Acer.

3.6.6. SERVIDOR DE ADMINISTRACIÓN

Este servidor no requiere de características especiales y simplemente puede ser una PC normal, entonces la PC a adquirir podrá tener las siguientes características:

- Procesador Intel Pentium III de 1 GHz .
- 128 MB SDRAM.
- Disco duro de 40 GB.
- Bus del sistema de 100 MHz.
- Tarjeta de red 10/100 Mbps.
- Monitor MV540 de 15".
- 8 MB de memoria para video AGP.
- MODEM 56K ITU V.90.
- Teclado y *mouse*.
- *Software* a utilizar: Cisco Works 2000

Sugerencias

Sun Blade 100 de Sun Microsystem, o una PC cualquiera.

3.6.7. *FIREWALL*

El *firewall* será el dispositivo encargado de brindar seguridad a la red del ISP, asegurando que los usuarios válidos accedan a los recursos de la red que ellos necesitan, para esto deberá presentar las siguientes características:

- Equipo modular con 4 interfaces LAN 10/100 Fast Ethernet y capacidad de expansión de los puertos del 50%, que inicialmente le permitirán

conectarse a las cuatro redes LAN que se tendrá.

- *Throughput* de 1.7 Gbps como mínimo.
- Debe soportar un número ilimitado de conexiones simultáneas.
- Procesador de 120 MHz.
- Memoria RAM de 32 MB con capacidad de expansión al 100%.
- Memoria *flash* de 16 MB.
- Ofrecer herramientas de protección contra ataques comunes como son:
  - IP *Spoofing*
  - *Denial of Service Attack* (Negación del servicio).
- Ofrecer capacidades de contenido seguro como son:
  - Opciones de filtrado URL, para bloquear el acceso a sitios *Web* inapropiados.
  - Soluciones antivirus, para *e-mail*, *file attachments* y *applets* Java maliciosos.
- Soporte para los siguientes métodos de autenticación de usuario: RADIUS, TACACS.
- Opciones para soportar VPNs
- El protocolo soportado para VPNs será IPSec.
- Proveer capacidades de NAT.
- Alimentación de 100-240 VAC a 50-60 Hz.

Sugerencias

Se recomienda el *Firewall Secure PIX 515UR de Cisco* o el FireWall-1 de CheckPoint Technologies.

3.6.8. *ROUTER* DE ACCESO CORPORATIVO

Generalmente, un *router* de acceso ofrece servicios de conectividad tanto para usuarios *dial-up* como para usuarios corporativos; es decir, el *router* corporativo puede realizar también la función de NAS. Un ISP debe tomar la decisión de utilizar un solo dispositivo para realizar ambas funciones o adquirir dispositivos diferentes para cada una de ellas.

Un *router* de acceso realizando ambas funciones, normalmente no puede escalar en grandes proporciones, por tal razón, un ISP con gran proyección de crecimiento de usuarios no deberá optar por un solo *router*.

En el presente diseño, se utilizará un NAS y un *router* de acceso corporativo en distintos dispositivos. Por lo tanto, el *router* corporativo deberá cumplir con lo siguiente:

- 2 puertos 10/100 Fast Ethernet con conector RJ-45.
- 1 puerto WAN sincrónico de 2 Mbps con cable V.35 DTE. La interfaz V.35 debe disponer de un conector M34 macho (Winchester macho).
- 8 puertos seriales sync/async (hasta 115,2 Kbps asinc. o 128 Kbps sinc.) tipo V.35 DTE. La interfaz V.35 debe disponer de un conector M34 macho (Winchester macho).
- Un puerto de consola RS-232.
- Soporte de protocolos: al menos *Frame Relay*, PPP, X.25, TCP / IP, RIP, OSPF.
- Memoria DRAM mínimo 64 MB con capacidad de expansión en 100%.
- Memoria *flash* que permita el almacenamiento del sistema operativo del *router* con todos los protocolos solicitados.
- Capacidad de expansión de 4 puertos WAN de 2 Mbps.
- Alimentación 110V AC, 60 Hz.
- Manuales del equipo.
- Cables eléctricos y de datos.
- Garantía de dos años en los equipos.

En caso de que éste desempeñe también funciones de NAS debe cumplir con las siguientes características adicionales:

- 1 puerto canalizado E1 / ISDN PRI
- 30 módems digitales de 56K
- Soporte de protocolos para módem V.90, V.33, V.34, V.32bis.

- Señalización R2 soportada

Sugerencias

Los productos para el *router* corporativo que cumplen con lo mencionado anteriormente son: *Router Cisco 3640*, Livingstone/Lucent Po.

3.6.9. *ROUTER* PRINCIPAL

Adicionalmente a las propiedades listadas en el *router* corporativo, este *router* debe proveer conectividad WAN de alta densidad y conectividad LAN de mediana a alta densidad.

Las características que debe tener este *router* son las siguientes:

- 2 puertos 10/100 Fast Ethernet con conector RJ-45
- 2 puertos WAN sincrónico de 2 Mbps con cable V.35 DTE. El interfaz V.35 debe disponer de un conector M34 macho (Winchester macho)
- Un puerto de consola RS-232
- Soporte de protocolos: al menos *Frame Relay*, PPP, X.25, TCP / IP, RIP, OSPF y BGP.
- Memoria DRAM mínimo 64 MB con capacidad de expansión en 100%.
- Memoria *flash* que permita el almacenamiento del sistema operativo del *router* con todos los protocolos solicitados.
- Capacidad de expansión de 8 puertos WAN de 2 Mbps.
- Alimentación 110V AC, 60 Hz.
- Manuales del equipo.
- Cables eléctricos y de datos.
- Garantía de dos años en los equipos.

Sugerencias

Se recomiendan los siguientes productos: *Router Cisco 3640*, Livingstone/Lucent Po.

3.6.10. NAS (*NETWORK ACCESS SERVER*)

El NAS es el dispositivo que se utilizará para conectar a los usuarios *dial-up* a la red del ISP y de esta manera podrán acceder a los servicios que ofrece el ISP e Internet.

Tomando en cuenta que se planea dar servicio a 2089 usuarios *dial-up* al final del primer año y que se utilizará una relación de 12:1, se deberá seleccionar un equipo que cumpla con las siguientes características técnicas mínimas para poder cumplir con los objetivos propuestos:

- 6 enlaces E1/PRI, para poder conectar a los usuarios *dial-up* del primer año.
- Equipo modular, con el objeto de poder incrementar el número de configuraciones E1/PRI hasta 26. Dependiendo del máximo número de puertos del NAS, será necesario tener uno o más servidores de acceso para poder ofrecer servicio a todos los clientes.
- 1 interfaz 10/100 Fast Ethernet, para conectar el NAS con el *switch*.
- Interfaces adicionales: Puerto de consola, para acceso administrativo local.
  Puerto auxiliar, para acceso administrativo remoto.
- Velocidad del procesador de 150 Mhz mínimo.
- Memoria *flash* de 16 MB mínimo.
- *Dynamic* RAM (DRAM) de 32 MB, con capacidad de expansión de al menos el 100%.
- Software IP.
- Soporte para el protocolo PPP.
- Capacidad para permitir autenticación mediante los protocolos PAP/CHAP.
- Soporte para el protocolo de enrutamiento interior utilizado por el ISP: OSPF o RIP.
- Procesadores duales y fuentes de alimentación duales, como un medio de redundancia.
- Facilidades de administración.

- Soporte para señalización R2.
- Soporte para VPNs.
- Soporte V.92 para futuro

Sugerencias

Se recomiendan los siguientes equipos, ya que éstos satisfacen los parámetros descritos anteriormente: *AS5400 Universal Access Server de Cisco*, MAX 6000 y PM-3 de Lucent, TCH HiPer de 3Com.

3.6.11. *SWITCH*

Este dispositivo se lo utiliza para conectar entre sí todos los dispositivos de la red del ISP. El *switch* a utilizarse debe satisfacer las siguientes especificaciones técnicas:

- *Throughput* de ruteo por encima de 5 Mpps.
- *Backplane* por encima de 8 Gbps.
- Direcciones MAC por encima de 18000 MAC *address.*
- 16 puertos 10/100 Base-TX *autosensing* con capacidad de expansión.
- Todos los puertos deben ser *half / full duplex.*
- Memoria: DRAM al menos 64 MB. Debe poseer memoria RAM *flash* para actualizaciones de *software.*
- Alimentación 110V AC, 60 Hz
- Capacidad de ser administrado local y remotamente mediante puerto de consola, Telnet, SNMP (MIB-II), RMON.
- Soporte IEEE 802.3x, 802.3u, 802.3z.
- Soporte protocolos: IP, RIP v1 y v2, OSPF.
- Calidad de servicio: 802.1q, 802.1p.
- Soporte de VLANs, al menos 4 VLANs.

Sugerencias

Los *switches* que entran en esta clasificación son: Cabletron X-PEDITION™ SS-2-B128 Switch Router, *Extreme Summit 24*, Cisco Catalyst 2948G-L3.

Nota: La infraestructura del ISP de diseño se indica en la figura 3.8.

3.7. SELECCIÓN DE LOS PROTOCOLOS DE ENRUTAMIENTO

Para elegir el protocolo de enrutamiento interior de un ISP se debe considerar las características específicas que tiene cada IGP (*Interior Gateway Protocol*; Protocolo de Pasarela Interior), así como también la implementación elegida por el ISP. A continuación se verán los criterios más utilizados para comparar los protocolos de enrutamiento:

Velocidad de respuesta.- Es el tiempo necesario para que un cambio de topología se propague a través de la red, y para que las tablas de enrutamiento se estabilicen en un nuevo estado, el del camino más corto. Esta medida de *performance* es muy importante, ya que en un ambiente dinámico la velocidad de respuesta debe ser mayor que la velocidad de cambio de la topología de la red, ya que de lo contrario no se dará la convergencia.

Cantidad de paquetes de control transmitidos.- Es la cantidad de información que debe transmitirse a través de la red para propagar un cambio en la topología y actualizaciones de la tabla de enrutamiento. Cuanto más grande sea la cantidad de paquetes de control, mayor será el *overhead* y la posibilidad de provocar congestión debido a la transmisión de información de enrutamiento y topológica.

Complejidad computacional.- Los algoritmos requieren una cierta cantidad de cálculo en cada nodo para procesar los paquetes de control, realizar los cálculos para obtener los caminos más cortos y actualizar las tablas de enrutamiento.

INFRAESTRUCTURA DEL ISP DE DISEÑO

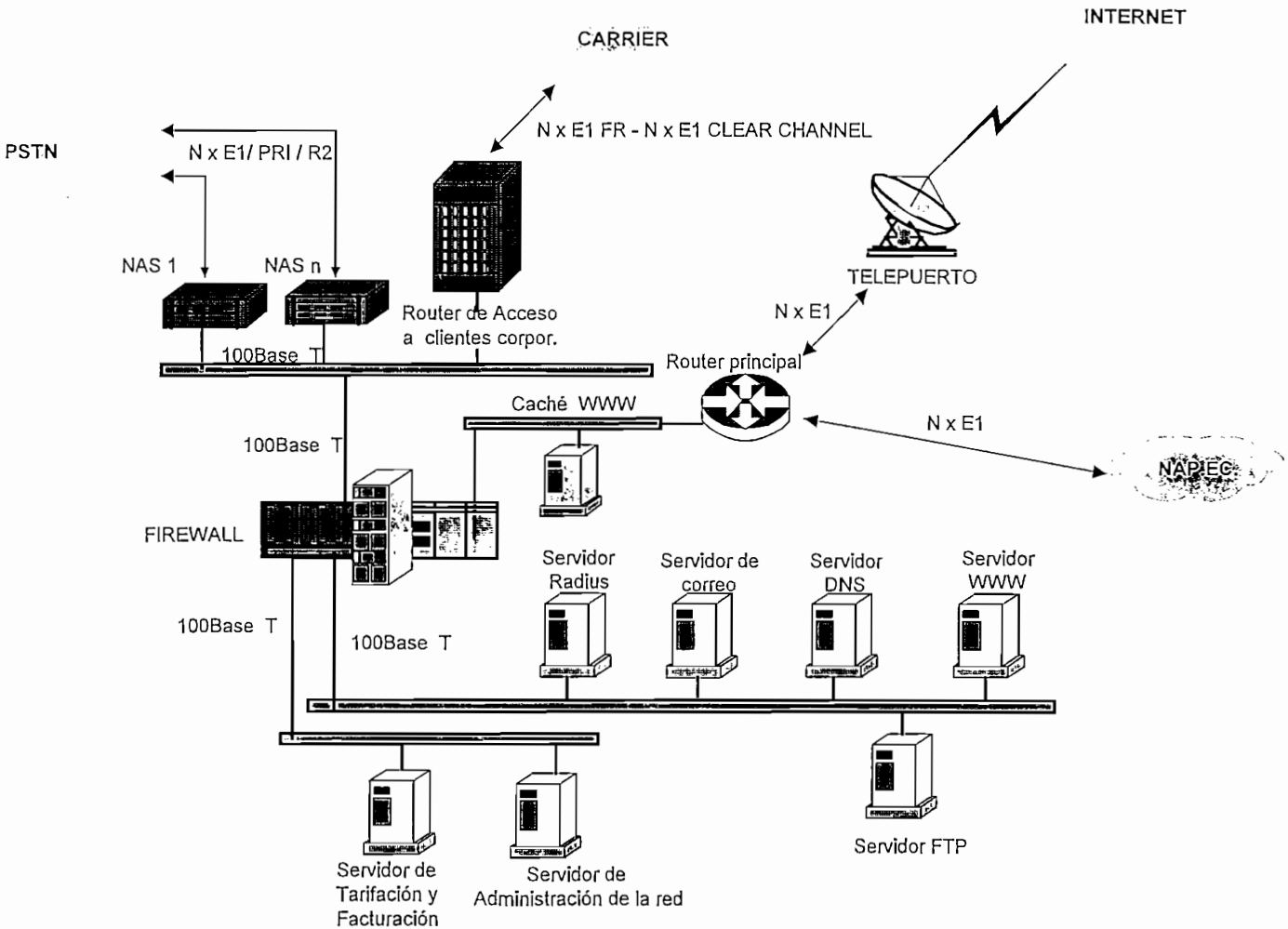


Fig.3.8. Infraestructura del ISP de diseño

Tamaño de los paquetes de control.- Es la cantidad de información que se transmite en cada paquete de control.

Requerimientos de memoria para mantener las tablas de enrutamiento.- En este punto es importante considerar cuánta información se requiere para el funcionamiento correcto del algoritmo. La cantidad de tablas, el tamaño de éstas y su factor de crecimiento con respecto a la cantidad de nodos en la red y también con respecto a la cantidad de enlaces de la red.

Existencia de ciclos.- La no existencia de ciclos asegura que un paquete no volverá a nodos por los que ya pasó en el periodo de convergencia del algoritmo, es decir cuando las tablas de enrutamiento están en proceso de cambio.

Tomando en cuenta los parámetros descritos anteriormente, a continuación se realizará un cuadro comparativo entre los protocolos de enrutamiento interior:

PROTOCOLO	RIP	OSPF	IGRP	EIGRP
Tipo	Vector Distancia	Estado de Enlace	Vector Distancia	Vector Distancia
Tiempo de convergencia	Lento	Rápido	Lento	Rápido
Consumo Ancho de Banda	Alto	Bajo	Alto	Bajo
Consumo de recursos	Bajo	Alto	Bajo	Bajo
Soporte de múltiples caminos	No	No		Si
Estabilidad	No	Si	Si	Si
Propietario	No	No	Si	Si

Tabla 3.12. Cuadro comparativo de los protocolos más utilizados[17]

Es bueno sin embargo que los protocolos de enrutamiento dinámicos puedan ser complementados con el enrutamiento estático, tales como las rutas por defecto. De esta forma se sabe que se podrá enrutar todos los mensajes que llegan. Sin embargo las rutas por defecto siempre tienen el riesgo de provocar "agujeros negros", ya que si se producen cambios topológicos que hacen que estas rutas se vuelvan inválidas, es raro que el algoritmo se entere a tiempo para dejar de utilizarlas, pues depende para ello del administrador de la red.

En lo que respecta al protocolo de enrutamiento exterior se utilizará el protocolo BGP-4 para conectar el ISP al Internet por las características mencionadas en el

capítulo II.

3.8. REDUNDANCIA, SIMETRÍA Y EQUILIBRADO DE LA CARGA DE LA RED

Tanto las empresas conectadas a los ISPs como los ISPs, requieren de un mecanismo de control para el tráfico entrante y saliente. A continuación se abordan los temas claves en la implementación de conexiones a Internet de alto rendimiento:

La ***Redundancia*** proporciona rutas alternativas en caso de fallo de uno de los enlaces, para conseguirlo el AS debe tener múltiples conexiones a uno o más AS.

La ***Simetría*** significa que tanto el tráfico entrante como el saliente deben hacerlo por el mismo punto en el AS.

El ***Equilibrado*** de la carga divide el tráfico sobre múltiples enlaces de forma óptima no significando una distribución por igual de la carga. Otro aspecto a tomar en cuenta es que tanto el tráfico entrante como el saliente deben ser considerados como dos entidades diferentes, ya que una configuración para el tráfico entrante no afecta al tráfico saliente.

A continuación se hará un breve análisis de los valores predeterminados para entender los tipos de escenarios sin entrar en un estudio profundo ya que no es el objetivo de este proyecto.

Valores Predeterminados(0/0).- Son una herramienta que minimiza el número de rutas que tiene que aprender un *router*, constituyéndose en una ruta en la tabla de reenvío IP utilizada en caso de que la información de una ruta específica para un destino sea desconocida. El tráfico hacia destinos desconocidos por el *router* se envía hacia dicha conexión de salida; además mediante la preferencia local se da grados de preferencia a los valores predeterminados, es decir, uno puede ser

utilizado como primario y los otros como respaldo en caso de que el primario ya no sea válido. Los valores predeterminados son aprendidos tanto dinámicamente vía BGP o IGP como estáticamente en la que el administrador establece la ruta 0/0 apuntando a: la dirección IP del *gateway* del próximo salto, una interfaz de *router* específica, o un número de red.

ESCENARIOS ESPECÍFICOS: REDUNDANCIA, SIMETRÍA Y EQUILIBRADO DE LA CARGA

Los escenarios específicos que se detallarán a continuación indican las alternativas de conexión entre el ISP y los clientes corporativos. Existen cinco escenarios: escenario con conexión única, escenario con múltiples conexiones a un solo proveedor, escenario con múltiples conexiones a proveedores diferentes, escenario de clientes del mismo proveedor con un enlace de respaldo y escenario de clientes de proveedores distintos con un enlace de respaldo.

ESCENARIO 1: CONEXIÓN ÚNICA

En este escenario los clientes se conectan al Internet mediante una única conexión sin enlace de respaldo, escenario inapropiado para aplicaciones que necesitan niveles altos de fiabilidad.

Fig. 3.9 Escenario con conexión única [2]

Generalmente, los clientes configuran los valores predeterminados para llegar al proveedor, y el proveedor utiliza enrutamiento estático para llegar al cliente, de esta manera el *router* del cliente no necesita aprender las rutas de Internet. Además, por poseer un único punto de entrada y de salida la simetría de carga se cumple.

ESCENARIO 2: MÚLTIPLES CONEXIONES A UN SOLO PROVEEDOR

En los siguientes tipos de escenarios, los atributos vistos en el capítulo II acerca de BGP son necesarios para comprender como realizar la simetría y equilibrado de carga. Este escenario se divide en varios escenarios a la vez los mismos que se tratan a continuación:

Sólo valor predeterminado, un enlace primario y uno de respaldo.- Aquí el cliente tiene varias conexiones al ISP, en la cual el cliente puede configurar valores predeterminados al ISP en ambas conexiones con distintos niveles de preferencia, para usar un enlace como primario y otro como respaldo en caso de fallo del primario. En la figura 3.10, para conseguir que el tráfico saliente utilice el enlace Y como primario, el cliente puede configurar:

- Valores predeterminados estáticos con distancias[a] diferentes (una distancia menor para el enlace Y y una distancia mayor para el enlace X).
- Valores predeterminados dinámicos y utilizar la preferencia local para preferir una ruta sobre otra (una preferencia local mayor para el enlace Y).

Por otra parte, para que el tráfico entrante utilice el enlace Y, el cliente debe enviar valores predeterminados hacia el ISP con una métrica menor para el enlace Y (Ej. MED) y una métrica mayor para el enlace X, de manera que la entrada y salida de datos sea por el enlace Y. En caso de que el cliente no envíe los valores de métricas, el tráfico fluirá a través de la salida más cercana del proveedor hacia el cliente (si el tráfico hacia el cliente esta más cerca de X, entrará a través de X).

[a] La distancia significa el grado de preferencia de una ruta estática en caso de que haya múltiples entradas para la misma red. Rutas con distancias más cortas son preferibles a las rutas con una distancia más larga.

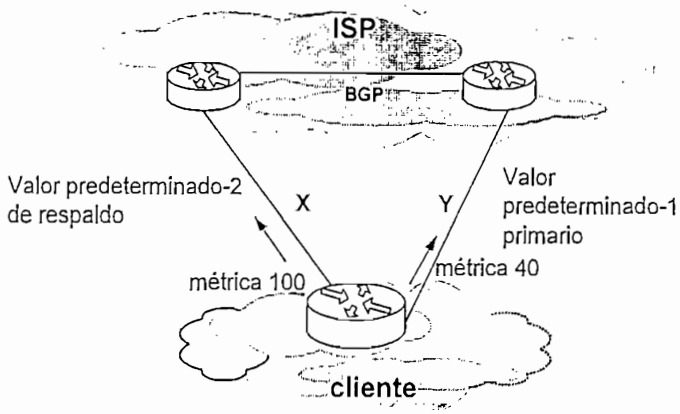


Fig. 3.10 Escenario básico de múlticonexiones a un único ISP[2]

Tanto para el tráfico entrante y saliente existe ausencia de equilibrado de la carga, debido a que entra en funcionamiento uno de los enlaces a la vez.

Valor predeterminado, el primario y el de respaldo además de enrutamiento parcial.- A diferencia del escenario anterior, éste acepta enrutamiento parcial[a] del ISP, pudiendo el cliente elegir el punto de salida mediante la configuración de preferencias locales, un ejemplo se ilustra en la figura 3.11:

- Para enviar tráfico por un determinado enlace el cliente debe asignar preferencias a *las direcciones aprendidas por un determinado enlace*, por ejemplo se asigna una preferencia local *m* para las direcciones C2 y C3 y una preferencia local *n* para el resto de direcciones *(m>n)*, mientras que para las direcciones C4 y C5 se asigna una preferencia local *p* y para el resto de direcciones una preferencia local *q* (*p>q*). De esta manera, el cliente preferirá el enlace X para las direcciones C2 y C3 si y solo si (*m>q*) y preferirá el enlace Y para las direcciones C4 y C5 si y solo si (*p>n*). Para clientes distintos a C2, C3, C4 y C5 se preferirá el enlace Y si y solo si *q>n*. Otra forma de realizar el proceso de enrutamiento es por medio del envío de métricas por parte del ISP al cliente mediante atributo MED. Se podría obtener resultados óptimos combinando ambos enfoques.

[a] Se lo realiza en base a rutas parciales que habitualmente son las rutas locales del proveedor y sus rutas de clientes.

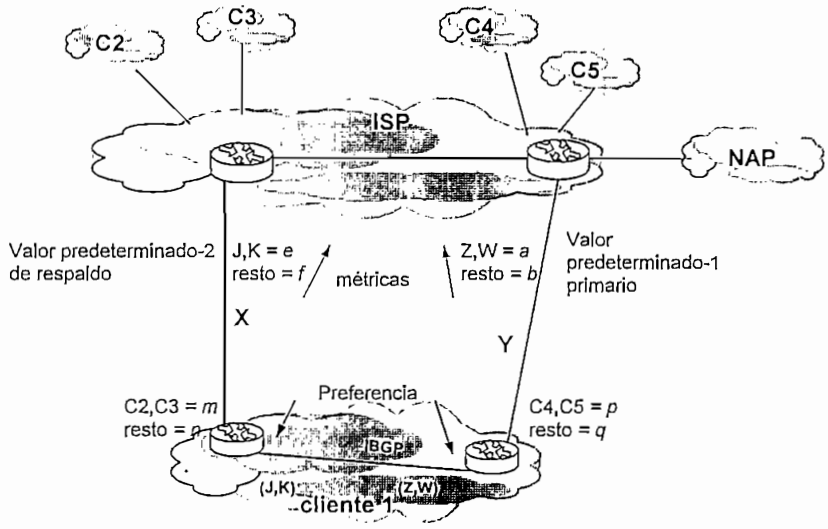


Fig. 3.11 Escenario de proveedor único con enrutamiento parcial [2]

- Para el tráfico entrante algunos ISP distribuirán el tráfico hacia el cliente mediante el enlace más próximo, o el cliente puede enviar la asignación de métricas (Ej: MED) para los enlaces al ISP para que realice el reenvío de tráfico en base a las métricas. En el ejemplo, el cliente asigna una métrica *a* para las direcciones Z y W y una métrica *b* para el resto de direcciones ($a<b$). Similarmente asigna una métrica *e* para las direcciones J y K y una métrica *f* para el resto de direcciones ($e<f$). De manera que el tráfico destinado a Z y W fluya por el enlace Y si y solo si $a<f$, y el tráfico para J y K fluya por el enlace X si y solo si $e<b$, mientras que para clientes distintos a J, K, Z y W el ISP seleccionará el enlace Y si y solo si $b<f$.

Para el tráfico destinado a las todas las demás redes del Internet el usuario debe configurar valores predeterminados por los enlaces y hacer uso de la preferencia local para seleccionar un enlace como primario y el otro como respaldo, de manera que todas las demás redes puedan ser alcanzadas siguiendo el valor predeterminado.

Valor predeterminado, el primario y el de respaldo además de enrutamiento completo y parcial.- Utiliza las mismas técnicas mencionadas anteriormente, la preferencia local y la métrica para controlar el tráfico saliente y entrante

respectivamente, pudiendo obtener rutas completas para un enlace o todos los enlaces y valores predeterminados o rutas parciales para los demás enlaces al ISP.

ESCENARIO 3: MÚLTIPLES CONEXIONES A PROVEEDORES DIFERENTES

Existen tres tipos de escenarios incluidos en éste, los mismos que se revisarán a continuación:

Sólo valor predeterminado, primario y de respaldo.- Este es un escenario similar al anterior pero con la diferencia de que el cliente se encuentra conectado a dos o más ISP, pudiendo el cliente puede configurar valores predeterminados a los ISPs con distintos niveles de preferencia para seleccionar un enlace u otro. El método utilizado por los clientes es apuntar los valores predeterminados a una red que ambos proveedores tengan en común y hacer uso de la preferencia local para seleccionar un enlace como primario y el otro como respaldo. En caso de que no se configure de esta manera, si el enlace entre el ISP2 y el NAP se cayera, el cliente todavía enviaría tráfico hacia el ISP2 en lugar de redirigirlo hacia otro valor predeterminado.

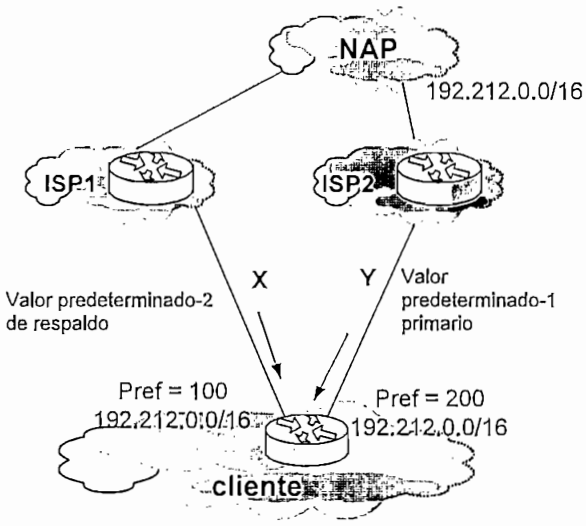


Fig. 3.12 Conexiones múltiples a ISP diferentes [2]

Valor predeterminado, primario y de respaldo además de enrutamiento parcial.- El cliente puede aceptar el enrutamiento parcial de uno o de varios ISPs, siendo el tráfico con destino a las direcciones de los ISPs que proveen enrutamiento parcial dirigido por el enlace que los conectan directamente (es decir por el enlace Y y por el enlace X) ya que es la ruta más corta, siendo necesario de que el cliente configure o apunte hacia un ISP un valor predeterminado, de manera que todas las demás rutas puedan ser alcanzadas siguiendo el valor predeterminado. En el caso de que se configuren más de un valor predeterminado se debe hacer uso de la preferencia local para preferir un enlace, ver figura 3.13.

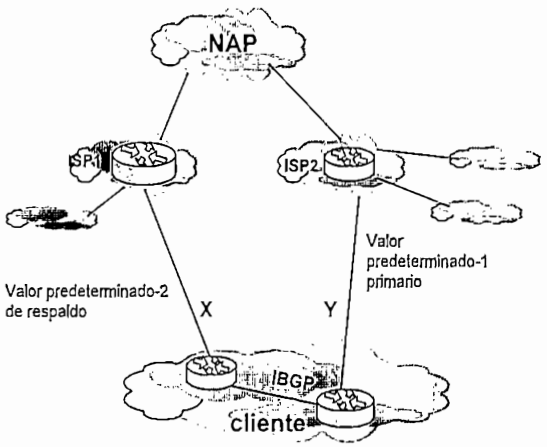


Fig. 3.13 Conexiones múltiples a ISP diferentes con enrutamiento parcial [2]

Valor predeterminado, primario y de respaldo además de enrutamiento completo y parcial.- En el entorno del ISP es necesario la aceptación de rutas completas de uno o varios ISP superiores y utilizar la preferencia local para decidir a que redes se puede acceder y a través de que ISP, basándose en función del sistema autónomo, prefijo, etc.

Otra solución podría ser aceptar el enrutamiento completo de un ISP (por ejemplo ISP2), y el enrutamiento parcial para los otros ISPs (por ejemplo ISP1, siendo importante además de que se apunte el valor predeterminado al ISP1). Dicho en otras palabras, el tráfico dirigido para las direcciones del ISP1 se utilizará el enlace X porque es la ruta más corta, mientras que para las demás rutas se utiliza el enlace Y ya que por el enlace X se obtiene rutas parciales.

Este tipo de configuración es importante ya que si se cae el enlace Y todas las rutas además de las redes locales del ISP1 son alcanzadas utilizando el enlace X porque el valor predeterminado esta apuntando hacia ese ISP. En el caso de que se cayera el enlace X todas las rutas son alcanzadas por el enlace Y porque se acepta enrutamiento completo.

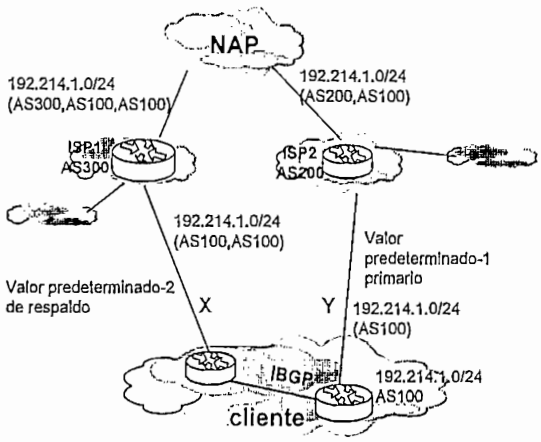


Fig. 3.14 Conexiones múltiples a ISP diferentes con enrutamiento completo [2]

En cuanto al tráfico entrante a los escenarios anteriores se ve afectado en cómo el cliente publica sus redes a los proveedores; para afectar dinámicamente al comportamiento de los proveedores, el cliente puede manipular la decisión de enrutamiento incrementando la longitud de ruta con el número de AS del cliente, consiguiendo los ISPs los mismos prefijos con longitudes de rutas distintas y seleccionarán la ruta con longitud más corta (en el ejemplo (AS300, AS100, AS100) frente a (AS200, AS100) se escogerá la ruta última para el flujo de tráfico entrante) ver figura 3.14.

ESCENARIO 4: CLIENTES DEL MISMO PROVEEDOR CON UN ENLACE DE RESPALDO

Son clientes conectados a un mismo ISP que mantienen un enlace entre ellos para utilizarlo como un enlace de respaldo cuando falle el enlace a Internet,

actuando uno de ellos como un AS de tránsito para el otro cliente, o lo utilizan como primario para el tráfico interior entre ellos.

- *En el caso de que se utilice como respaldo* (ver figura 3.15)*:* si AS2 está obteniendo un enrutamiento predeterminado, parcial, completo o una combinación de éstos, AS2 tendrá que establecer una preferencia local mayor para las rutas procedentes del ISP que para las de AS3, lo que garantiza que el tráfico saliente utilice el enlace hacia el ISP y no el enlace de respaldo, proceso similar debe hacer AS3.

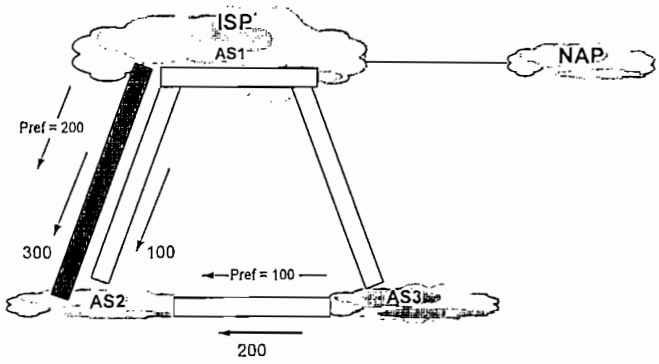


Fig. 3.15 Clientes del mismo proveedor con un enlace de respaldo [2]

- *En el caso de que se utilice como enlace primario:*, AS2 debe establecer una preferencia local mayor para todas las direcciones no originadas por AS3, lo que garantiza que todo tráfico dirigido a redes distintas de AS3 salga por el enlace con el ISP. Mientras que las preferencias locales para las direcciones originadas por AS3 y enviadas a través del ISP deben ser menores que las enviadas directamente por el enlace entre ellos, lo que garantiza que el tráfico salga por AS3 cuando se envíen datos a las redes de AS3. Cuando falle el enlace de AS2 con el ISP, AS3 servirá como tránsito por parte de AS2. En cuanto al tráfico entrante procedente de Internet utilizará la ruta más corta ISP-AS2 y el tráfico procedente de AS3 utilizará el enlace AS2-AS3. Proceso similar se debe aplicar en AS3.

ESCENARIO 5: CLIENTES DE PROVEEDORES DISTINTOS CON UN ENLACE DE RESPALDO

Es un caso muy raro visto en el Ecuador con clientes que poseen AS independientes con conexión a diferentes ISP y que hayan acordado utilizar un enlace de respaldo entre ellos en caso de falla del enlace con un ISP; esto se puede apreciar en la figura 3.16, para lo cual el cliente1 debe publicar las redes del cliente 2 al ISP1, y el cliente 2 publica las redes del cliente1 al ISP2, claro además de las rutas locales del cliente. El método preferido por los ISP es el método de la manipulación de la ruta de AS estableciendo sus políticas en función del número de AS, en el ejemplo se configurará el enrutamiento y la política desde el punto de vista del ISP1 las mismas que se realizarán en función de la ruta más corta al AS.

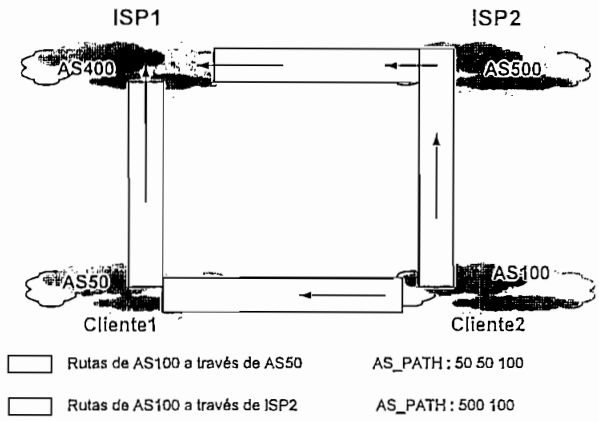


Fig. 3.16 Clientes de varios ISP con un enlace de respaldo

En condiciones normales, ISP1 tendrá longitudes equivalentes al cliente 2 [a través del cliente1 (AS50, AS100) y a través de ISP2 (AS500, AS100)], para influir en esta decisión el cliente1 debe incrementar la longitud de la ruta (con su propio número de AS) cuando se publiquen las rutas del cliente 2 al ISP1 lo que provocará que el ISP1 utilice el enlace con ISP2 para alcanzar al cliente 2, ya que la nueva ruta a través del cliente1 será (AS50, AS50, AS100).

En conclusión, aplicando lo visto anteriormente en el ISP del diseño, conforme éste vaya necesitando más ancho de banda, debe no solo contratar los servicios de un solo proveedor *upstream*, si no que debe hacerlo con varios ISPs para asegurar su conectividad global. Mediante la conectividad con varios de ellos se

puede realizar balanceo de carga así como redundancia en caso de fallo de uno de éstos.

Para obtener una mayor área de cobertura en el país, también será necesaria la contratación de varios *carriers* para proveer conectividad a los usuarios corporativos, lo cual es uno de los objetivos del ISP de diseño.

3.9. CALIDAD DE SERVICIO

El concepto de Calidad de Servicio (QoS) se aplica en tres ámbitos dentro del entorno Internet:

- Operadores de redes de telecomunicaciones
- ISP
- Usuario de Internet

Para los operadores de redes de telecomunicaciones, calidad de servicio es:

- Evitar situaciones de congestión en los nodos de la red.
- Proporcionar mecanismos para clasificar el tráfico.
- Asignar prioridades en función de los contratos de tráfico con los clientes.

Para el ISP, calidad de servicio es:

- Dimensionar los recursos de red de forma óptima en función del número de suscriptores.
- Ofrecer a un determinado conjunto de usuarios un grado de servicio acordado aún en casos de congestión.
- Actuar de forma rápida y eficiente frente a las incidencias que se produzcan con los clientes.

Para los Usuarios de Internet, calidad de servicio es:

- Obtener un acceso más fiable, ágil y sencillo que le permita sacar el máximo partido de las ventajas que ofrecen las tecnologías de la información.

En forma general se puede decir que QoS es la capacidad de una red o de un elemento dado de la misma para asegurar con un grado de fiabilidad preestablecido que los requisitos de tráfico en términos de perfil y ancho de banda para un flujo de información dado sean cumplidos.

Históricamente, el Internet ha ofrecido un único nivel de servicio el "*best effort*", en el cual todos los paquetes de datos son tratados por igual en la red y su entrega se la realiza de la mejor forma posible. Sin embargo, el Internet mismo no ofrece un único nivel de QoS.

Los factores determinantes de QoS en términos cualitativos están directamente relacionados con la respuesta percibida por los usuarios finales cuando acceden a la red y por el grado de satisfacción de los mismos, ya que si la respuesta de la red no es buena es porque hay deficiencias de ingeniería y de diseño. En términos cuantitativos, la calidad de servicio se refleja por una serie de parámetros que se pueden medir y ajustar convenientemente para proporcionar un grado de servicio satisfactorio; estos parámetros son: el retardo, la fluctuación del mismo (*jitter*), el ancho de banda y la fiabilidad.

Para proveer un buen servicio a Internet se deben considerar los siguientes elementos: el usuario, la línea de transmisión, la red de acceso de los usuarios, la infraestructura del proveedor ISP, los operadores ISP internacionales y los servidores de información.

3.9.1. MEDIDAS DE CALIDAD

Son los parámetros que permiten evaluar la calidad de servicio en un ISP y son

los siguientes:

Parámetros medibles en el servicio de red:

1. **Medidas de rendimiento.-** Se suele establecer sobre dos objetivos principales: los servicios propios incluyendo el equipamiento básico de red (DNS, *routers*, etc.) y los servicios externos más utilizados por los usuarios (servidores *web, e-mail*, ftp). Se realizan dos tipos de medidas para evaluar el rendimiento de un ISP: el número de datagramas perdidos y el tiempo de respuesta de las peticiones que sirven para evaluar respectivamente las pérdidas de información y los retardos que se producen en las comunicaciones que se realizan.

2. **Medidas de fiabilidad.-** Estas medidas van encaminadas a evaluar los aspectos referidos al servicio de la propia red y a la de los servidores del propio proveedor, éstas son: accesibilidad al servicio, disponibilidad del servicio, duración de la indisponibilidad y tiempo entre indisponibilidades.

Parámetros medibles en el servicio de atención al cliente:

El usuario es el más indicado para notificar si el funcionamiento del ISP es el correcto entre otras cosas porque es él, quien está conectándose permanentemente. El servicio de atención a clientes bien utilizado por los ISPs puede ser una herramienta clave en la medida de la calidad de su servicio. Dichos parámetros son: disponibilidad de servicio, tiempo medio de respuesta frente a cada tipo de problema.

Las medidas de QoS pueden ayudar a la detección de problemas en el servicio de red, siendo necesario introducirse en un proceso de mejora continua. De esta forma se dará solución a los problemas que vayan surgiendo, ya que cada vez más el QoS es un factor fundamental diferenciador tomado en cuenta por los usuarios a la hora de elegir un ISP.

Las herramientas para implementar un entorno de QoS efectivo son configuraciones en los *routers* de la red que se detallan a continuación:

- Señalar los enlaces de transmisión de más bajo nivel para usar un criterio diferente de transmisión al proveer servicio y cumplir con los perfiles de servicio contratados.
- Alterar el algoritmo de selección del siguiente salto a fin de seleccionar un camino cuyas características concuerden con los niveles de servicio deseado.
- Alterar el retardo de encolamiento de los *routers* y algoritmo de descarte de paquetes.

3.9.2. MECANISMOS PARA INTRODUCIR QoS EN INTERNET

Antes de detallar los mecanismos para introducir QoS en Internet, se revisarán algunos aspectos que se deberán tener en cuenta para tal propósito.

- Se debe dimensionar la red tomando en cuenta las horas pico, ya que es ahí donde se va a producir carga máxima. En el caso de dimensionar los puertos de acceso se deben tomar en cuenta las características de tráfico del usuario y el uso del puerto del *pool* de módems basándose en el tiempo del día y día de la semana.

- Para minimizar el retardo de la red se debe contar con un sistema de encolamiento que intente localizar tráfico a fin de preferir los caminos de distancia mínima. Para minimizar el *jitter*, el sistema de encaminamiento debe mantenerse tan estable como sea posible.

- En términos de fiabilidad, la red debe usar *routers* que tengan altos niveles de disponibilidad y estabilidad y que los medios de transmisión tengan un BER (*Bit Error Rate*; Tasa de Bits Errados) muy bajo, mientras que el ancho de banda debe ser diseñado para minimizar el nivel de pérdida de

paquetes inducido por congestión. La arquitectura de red debe examinar los cálculos de rendimiento de horas de ocupación para que la red no entre en una condición de congestión extrema en las horas pico.

La IETF, ha propuesto varios modelos o mecanismos para satisfacer la demanda de QoS, siendo los más conocidos el modelo de servicios integrados RSVP (*Resource Reservation Protocol*; Protocolo de reservación de recursos), el modelo DS de servicios diferenciados, la técnica MPLS (*Multiprotocol Label Switching*; Conmutación de etiquetas multiprotocolo), la ingeniería de tráfico y el enrutamiento sujeto a restricciones.

3.9.2.1. Modelo de Servicios Integrados

Su funcionamiento se basa en la reserva de recursos sobre los *routers* para poder garantizar los parámetros de calidad negociados. RSVP permite que un sistema reserve una cantidad predeterminada de ancho de banda en una ruta de acceso específica de la red, lo que elimina la posibilidad de escasez de ancho de banda.

Para reservar flujo, el cliente y el servidor deben tener recursos asignados de cada elemento de hardware de red que participe en la transmisión. Para iniciar el proceso de reserva, el cliente envía un mensaje *path* al receptor, y a medida que cada elemento de hardware de red lo recibe se agrega a si mismo a la lista (con el fin de que paquetes posteriores de la misma sesión sigan la misma ruta), reenviándose el paquete hasta llegar al receptor. Como respuesta, el receptor envía un mensaje *resv* (de reserva) que utilizará la misma ruta del mensaje *path*, ya que cada salto está enumerado en el mensaje. A medida que cada elemento reenvía el mensaje *resv*, comprueba que dispone del ancho de banda solicitado y lo reserva en ese momento, y si no es así envía un mensaje de error.

El emisor reenvía automáticamente un mensaje *path* de forma periódica (cada 30 seg.) para adaptarse a los estados cambiantes de la red. En caso de que la estación receptora no reciba ningún mensaje *path* en un intervalo predeterminado

de tiempo (90 seg.), se elimina la reserva. Una vez finalizada la sesión, la estación que interrumpe la conexión enviará un mensaje *path tear*.

3.9.2.2. Modelo de servicios diferenciados

Esta técnica utiliza el campo de tipo de servicio (TOS) del protocolo Ipv4, para indicar qué tipo de exigencia por parte de la red requieren los datos que viajan en el paquete, en base a este campo se propone diferente tratamiento para los flujos de paquetes que contengan un tipo de servicio u otro.

Para que un usuario reciba este servicio del ISP debe acordar de antemano un nivel de servicio (SLA, *Service Level Agreement*). Un SLA especifica los tipos de servicio soportados así como la cantidad de tráfico permitido para cada tipo de servicio.

Un SLA puede ser estático, es decir, los usuarios podrán transmitir/recibir información en cualquier momento, mientras que en los SLA dinámicos utilizarán un protocolo de señalización (Ej. RSVP) para solicitar servicios y recursos bajo demanda, antes de la transmisión.

Los usuarios marcan los paquetes de forma individual para indicar el tipo de servicio que desean recibir o bien son los *routers* de frontera los encargados de utilizar este campo al ingresar un paquete a un dominio de servicios diferenciados. Ello obliga a negociar y establecer los mismos criterios que permitan definir SLAs adecuados para cada servicio utilizado por las aplicaciones.

Una vez en la red, los paquetes son clasificados e inspeccionados (esta tarea se la realiza únicamente en los puntos de entrada de los dominios). Cuando un paquete entra a otro dominio el campo TOS será modificado en función del nuevo SLA existente entre ambos dominios.

3.9.2.3. MPLS

Es un esquema de retransmisión que asigna etiquetas a los paquetes en función de prioridad de despacho. Un *router* con capacidad MPLS examina solo la etiqueta correspondiente para decidir cómo llevar a cabo el reenvío del paquete.

Los paquetes son clasificados y encaminados una vez que entran en un dominio MPLS, a través de un *router* LSR (*Label Switching Router*, *Router* de Conmutación de Etiquetas), el cual introduce una cabecera MPLS. Cuando el LSR recibe un paquete que ya dispone de cabecera MPLS, utilizará la etiqueta como índice para consultar la tabla de encaminamiento.

Finalmente, ***la ingeniería de tráfico*** está constituida por un conjunto de técnicas que tienen como objetivo organizar los procesos mediante los cuales los paquetes fluyen sobre la red. Mientras que el ***enrutamiento bajo restricciones*** tiene en cuenta el ancho de banda disponible o el retraso predecible en la red.

3.9.3. QoS DE ATM

ATM es una tecnología que fue diseñada desde el inicio pensando en el QoS. El QoS que presenta ATM se divide en las siguientes clases:

- CBR (*Constant Bit Rate*; Tasa de Bits constante), se caracteriza por flujos continuos de bits a una tasa constante de bajo ancho de banda y es altamente sensible al retardo e intolerante a pérdidas de paquetes, Ej. enlace T1.
- RT-VBR (*Real Time Variable Bit Rate*; Tasa de Bit Variable en Tiempo Real), garantiza que la aplicación obtendrá el ancho de banda requerido y es útil en servicios de tiempo real como las videoconferencias y el despliegue de presentaciones tipo filme.
- NRT-VBT (*Non Real Time Variable Bit Rate*; Tasa de Bit Variable en Tiempo No Real), es igual que el anterior, excepto que el protocolo puede

tener un retraso en la entrega tal como en el servicio de correo electrónico.

- ABR (*Available Bit Rate*; Tasa de Bit Disponible), está enfocado a ofrecer un ancho de banda base y si la aplicación requiere más entonces hará su mejor esfuerzo para incrementarla, Ej. navegar en WWW.
- UBR (*Unspecified Bit Rate*; Tasa de Bit no especificada), es un servicio *best-effort* en que si la red está congestionada, los paquetes son descartados sin avisar, pero si hay ancho de banda sobrante, se entregan la mayor cantidad de paquetes posibles.

La calidad de servicio se define con parámetros de envío de celdas por un lado y en la entrega de las mismas por el otro.

Para establecer un control de calidad en los servicios, se han definido una serie de parámetros que el cliente y el proveedor pueden negociar de acuerdo a la tabla 3.13:

Parámetro	Definición	Significado
PCR	*Peek Cell Rate*	Razón máxima de envío de celdas
SCR	*Sustained Cell Rate*	Razón promedio de envío a largo plazo
MCR	*Minimum Cell Rate*	Razón mínima aceptable de envío
CDVT	*Cell Delay Variation Tolerance*	Razón máxima aceptable de retraso
CLR	*Cell Loss Ratio*	Fracción de celdas tardías o perdidas
CTD	*Cell Transfer Delay*	Retraso promedio máximo en la entrega
CDV	*Cell Delay Variation*	Varianza en la entrega de celdas
CER	*Cell Error Rate*	Fracción de celdas entregadas con error
SECBR	*Severely-Errored Cell Block Ratio*	Fracción de bloques con celdas erróneas
CMR	*Cell Misinsertion Rate*	Fracción de celdas entregadas en otra parte

Tabla 3.13. Parámetros de QoS de ATM[17]

3.9.4. QoS DE *FRAME RELAY*

Es posible contratar para cada conexión una calidad de servicio distinta. Dicha calidad está definida mediante ciertos parámetros:

- CIR (*Committed Information Rate*; Tasa de Información Comprometida) (bps), es el caudal medio garantizado que la red se compromete a dar en

una conexión durante un intervalo de tiempo definido (Tc). Es un parámetro asociado a cada sentido de la transmisión de cada circuito virtual.

- Tc (*Committed measurement interval*; Intervalo de Observación), parámetro del algoritmo para calcular el CIR.
- C*Tc, máximo volumen de información que se podría cursar en Tc (lo que posibilita el canal), este parámetro es lo primero que contrata el abonado.

Además el usuario debe ajustarse a los parámetros Bc[a] y Be[b] que se ha negociado con el ISP. Cuando las tramas superan Bc, la red activa el bit DE para indicar que estas tramas deberían ser descartadas, si es necesario. El usuario también puede marcar este bit para indicar la importancia relativa de la trama respecto a otras.

Cualquiera que sea la plataforma, topología o tamaño de la red, es imprescindible hacer uso de las herramientas de control existentes, analizar con detalle las herramientas de administración más adecuadas de la topología a utilizar, inclusive se puede requerir combinaciones de ellas implementando IP sobre ATM o *Frame Relay*, para llevar a cabo una buena planeación y administración del ancho de banda. Siempre se debe recordar que todo se traduce en costos de operación y productividad, por lo que diseñar, implementar, y mantener una red con alto desempeño se traducirá en ganancias para todos: empresa, operador y sobre todo "el usuario final".

---

[a] Bc (*Committed burst size*), es el volumen de información comprometida durante un Tc que el ISP se compromete a transmitir.

[b] Be (volumen de información en exceso),información cursada durante el intervalo Tc que exceda de Bc+Be no se sabe si llegará o no a su destino.

BIBLIOGRAFÍA CAPÍTULO III

[1] "*ISP Survival Guide. Strategies for Running a Competitive ISP*"; Geoff Huston; Primera Edición; John Wiley & Sons, Inc; 1999; EE.UU.

[2] "*Internet Routing Architectures*"; Sam Halabi y Danny McPherson; Segunda Edición; Cisco Press; Indianapolis; 2000

[3] "Revista *Computerworld* Ecuador"; agosto del 2001.

[4] "XVIII Jornadas Anales Ingeniería Eléctrica y Electrónica"; Ing. Alexis Barreto; Diseño Matemático de un ISP; Junio 2000; Quito-Ecuador.

[5] "Edición Especial TCP/IP"; John Ray; Prentice Hall; 1999; Madrid.

[6] http://www.isp-planet.com/business/getting_into_isp1.html

Getting Into the ISP Business

[7] http://www.inec.gov.ec/

Instituto Nacional de Estadísticas y Censos

[8] http://www.opinamos.com

Estadísticas e Investigación de Mercado Digital en Latinoamérica.

[9] http://www.aeprovi.org.ec

Estado actual de Internet.

[10] http://www.supertel.gov.ec

Estadísticas. Valor Agregado: Acceso a Internet

[11] http://www1.ecua.net.ec/servicios/web/index.html

Servicios de *Web Sites*

[12] http://www.arrakis.es/~val/curs/SERV/INET/TECNIC.htm

Funcionamiento de Internet

[13] http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg242133.pdf

The Technical Side of Being an Internet Service Provider.

[14] http://www.isp-planet.com/business/pricing1b.html

What is the right ratio?

[15] http://www.dcc.uchile.cl/~raparede/cuerpo.v1.00.pdf

Diseño e Implementación de Experiencias Docentes para un Sitio Proveedor de Servicios de Internet.

[16] http://ispltd.com/howdo/eq.html

How to Become an ISP. Servers and Other Equipment.

[17] http://www.cs.virginia.edu/~knabe/iic3512/apuntes.html.
ATM
[18] http://it.aut.alcala.es/antonio/CD/Tema8.pdf
QoS
[19] http://mmm.upc.es/moliver/TELECOM2000Oral29up.pdf
QoS.
[20] http://www.icontec.org.co/basesdatos/nor_software/ntc4536.pdf
Tecnología de la Información. QoS. Estructura.
[21] http://www1.avaya.com/enterprise/whitepapers/deliveringqos.pdf
Delivering Internet Access Quality of Service.
[22] http://www.index.mis.net/kanti/6.html
Choosing a location and connection.
[23] http://www.index.mis.net/kanti/5.html
Assessing your Market Presence.
[24] http://www.index.mis.net/kanti/4.html
Assessing your Market Presence.
[23] http://www.index.mis.net/kanti/3.html
Bussines Opportunities on the Net.

CAPÍTULO IV

DISEÑO DEL SISTEMA DE SEGURIDAD DEL ISP

4.1. INTRODUCCIÓN A LA SEGURIDAD EN INTERNET

Se define como seguridad a la protección que se brinda a una red contra el comportamiento inesperado. El Internet es un entorno hostil en el cual un ISP y sus clientes pueden ser el blanco de varios incidentes que comprometen la seguridad de la red, éstos pueden ir desde intentos de infiltración a la red hasta una simple contaminación de virus; por tal razón, se hace necesario tomar medida de seguridad.

En Internet existen millones de puntos vulnerables los cuales permiten que se lleven a cabo ataques con mucho éxito. En gran parte, los atacantes son oportunistas y utilizan la vía más fácil y conveniente. Utilizan las vulnerabilidades mejor conocidas mediante el uso de herramientas de ataque muy conocidas y ampliamente difundidas. Se aprovechan de aquellas organizaciones que no aplican adecuadas medidas de seguridad para resolver sus problemas, realizando ataques de forma indiscriminada.

En Internet no existe seguridad absoluta, pero esto no es causa suficiente para dejar de utilizarlo o para no tomar ninguna medida de seguridad. La seguridad en este entorno es una cuestión de grados. Entre más medidas se utilicen, más se reduce el riesgo. La meta de un sistema de seguridad, además de reducir el riesgo al mínimo, debe ser tomar medidas adicionales, de manera que, si un incidente de seguridad llegara a ocurrir, sea posible una rápida recuperación.

Para responder adecuadamente ante los incidentes de seguridad, es necesario tomar ciertas consideraciones de seguridad, formular políticas sobre cómo minimizar los riesgos de tales incidentes y planear cómo responder cuando ellos ocurren.

Este capítulo provee una revisión de los temas de seguridad y riesgos a los que puede verse expuesto un ISP cuando conecta su red a Internet, así como de las tecnologías disponibles para afrontar tales riesgos.

4.2. PLAN DE SEGURIDAD DEL ISP

Un ISP necesita formular un plan de seguridad para la red y sus servidores como un conjunto de mecanismos de defensa para impedir que se desarrollen exitosamente ataques a la seguridad de la red. Por esta razón se sugiere seguir los siguientes pasos como una guía en la elaboración de un adecuado proceso de seguridad:

- Identificar qué se está tratando de proteger
- Determinar de qué se está tratando de proteger
- Determinar cuan probable es que se susciten amenazas a la seguridad
- Implementar medidas que protejan los bienes del ISP en forma efectiva sin descuidar el costo de tales medidas de seguridad
- Revisar el proceso continuamente y hacer mejoras cada vez que una debilidad sea encontrada.

Un ISP debe proteger principalmente tres aspectos de la red: el *hardware,* el *software* y la información. A continuación se listará aquello que podría verse afectado debido a un problema de seguridad.

Hardware.- Con respecto al *hardware.* existen varias áreas en la red del ISP donde se deben aplicar medidas de seguridad, éstas son: seguridad de las plataformas de servicio (HTTP, FTP, Telnet, etc) y seguridad de los *routers*; esto incluye: CPUs, teclados, terminales, impresoras, *disk drives*, computadoras personales, líneas de comunicación, etc.

Software.- Se debe proteger: programas fuente, programas objeto, programas de diagnóstico, sistema operativo, programas de comunicación, etc.

Información.- Se debe proteger toda aquella información importante para el ISP y para el cliente, como por ejemplo: *backups,* bases de datos, información que está siendo transmitida a lo largo de los medios de comunicación, etc.

Una vez que se ha identificado lo que se va a proteger, es necesario identificar las amenazas a las que está expuesta la red, se debe tener presente que los riesgos más comunes contra la seguridad son: amenazas internas, amenazas externas, intrusos (*hackers*), virus, etc. Este tema se tratará con mas detalle en la siguiente sección.

Actualmente, debido al tremendo potencial del comercio electrónico sobre Internet, cualquier usuario del ISP debe ser considerado como un potencial intruso, lo cual hace que la probabilidad con la que se suscitan ataques contra la seguridad sea muy elevada. En estos días, la mejor política de seguridad es "no confiar en nadie".

Las medidas que se deben implementar para proteger al ISP deben ser tomadas en base a un análisis de costos, ya que el costo de la protección debe ser siempre menor que el costo total de lo que se está protegiendo. Adoptar medidas de seguridad no debe hacer tan cara la tarea de operar el servicio de manera que sea imposible competir dentro del mercado. Un incidente de seguridad no solo acarrea un costo adicional de recuperación sino que también incluye el costo asociado con la reputación y la confiabilidad del ISP frente a sus clientes.

Se deben revisar las seguridades periódicamente, y cada vez que una falla sea encontrada ésta debe ser combatida. Se recomienda adoptar nuevos mecanismos de seguridad cada vez que uno nuevo esté disponible en el mercado. Sin embargo, se debe tener la precaución que éstos hayan sido previamente probados y adoptarlos una vez comprobada su eficacia en esta tarea.

Respuesta ante incidentes de seguridad

Es prudente para el ISP no solamente preparar y ejecutar un plan de seguridad sino que además debe planear cómo va a responder ante episodios de intrusión. Una respuesta oportuna y eficiente es necesaria para asegurar que no se comprometan los bienes del ISP y que el sistema no sea usado como un trampolín para posteriores ataques a otros sistemas dentro de la red del ISP o dentro de las redes de los clientes, para asegurar que los datos esenciales no sean corrompidos y que la integridad en las operaciones del ISP no sean comprometidas.

Planear una respuesta ante incidentes de seguridad involucra una serie de objetivos como son: identificar qué ha sucedido, tomar medidas para solucionar el problema, establecer cómo prevenir que la misma vulnerabilidad sea explotada y prevenir ataques posteriores. El siguiente paso es actualizar las políticas del ISP reforzando las debilidades existentes dentro de este proceso y como último punto, se debe presentar la evidencia del incidente a las agencias respectivas como por ejemplo el CERT[a] (*Computer Emergency Response Team*; Equipo de Respuesta para Emergencias Informáticas), trabajar con ellas y determinar la identidad del atacante.

Los incidentes de seguridad deben ser reportados al ISP, tanto sus clientes como ISPs *peers* y grupos de respuesta de seguridad de Internet deben ser concientes de esta responsabilidad y reportar cualquier intento de violación de la seguridad que puedan detectar. Cuando un incidente es reportado, la tarea principal es verificar que tal reporte es relevante para el ISP. Un ISP frecuentemente recibe reportes de seguridad falsos por lo que se hace necesario confirmar el evento antes de proceder.

Una vez confirmado un incidente de seguridad, el segundo paso es iniciar un mecanismo de defensa el cual debe realizar actividades prioritarias. Como

---

[a] El CERT es un centro con amplia experiencia en seguridad de Internet operado por la universidad de Carnegie Mellon. Está encargado de estudiar las vulnerabilidades en la seguridad de Internet, manejar incidentes de seguridad informática, publicar alertas de seguridad, desarrollar información y proveer de entrenamiento para ayudar a mejorar la seguridad de un sitio.

siempre, la seguridad humana debe ser la principal actividad de seguridad. Un segundo nivel de prioridad debe ser proteger la confidencialidad de los datos, en el caso del ISP, estos datos frecuentemente están relacionados con información de tarjetas de crédito y otras formas de datos de los clientes. El siguiente nivel de prioridad es proteger la integridad de las plataformas de servicios (servidores).

Teniendo en cuenta estas prioridades, las respuesta ante incidentes típicamente siguen una secuencia de actividades. El objetivo inicial es identificar el alcance del incidente. Comúnmente un ISP utiliza plataformas de *hardware* y *software* uniformes en todos sus sistemas; en este caso, la vulnerabilidad explotada en un sistema puede ser compartida y explotada en otros sistemas, de manera que, cuando un sistema violado es identificado, el cuarto nivel de prioridad debe ser identificar las amenazas a la seguridad humana, datos sensitivos, recursos del sistema y si las plataformas de servicio deben continuar en operación o ser aisladas de la red. Si el alcance del ataque se extiende a otros sitios es muy prudente notificar a estos sitios acerca de la naturaleza del incidente.

El siguiente paso es contener el incidente y remover la vulnerabilidad. Para contener el incidente puede ser necesario cerrar los sistemas afectados y posteriormente el sistema debe ser revisado para identificar y remover la vulnerabilidad (virus, archivos ocultos, *software* de caballos de Troya, etc). La evidencia de la intrusión debe mantenerse segura para ser analizada más tarde ya que ésta ayudará en la determinación del intruso y en la investigación del incidente.

El siguiente paso es recobrar el estado normal del sistema. En muchas ocasiones y debido a la incertidumbre del punto donde sucedió el ataque, es conveniente recurrir al proveedor del producto a fin de asegurar que un sistema limpio sea cargado nuevamente en las plataformas.

4.3. NATURALEZA DE LOS INCIDENTES DE SEGURIDAD

Para saber de qué se va a proteger a la red del ISP y cómo protegerlo, es conveniente hacer una revisión de los principales problemas que pueden amenazar la seguridad del proveedor de servicios. Identificar las amenazas, servirá para que el ISP pueda prevenir robos, fraude, espionaje, vandalismo, extorsión o terrorismo.

El rango de incidentes que pueden suscitarse en un ISP van desde una infiltración accidental hasta un ataque malicioso, algunas afectan el *hardware* y otras el *software*. Entre los incidentes más comunes se pueden mencionar los siguientes:

Amenazas Internas.- Ya que muchos de los ataques a la red del ISP son internos, es conveniente tomar precauciones en lo referente al acceso físico de los equipos. Es importante que los recursos de la red se encuentren en medios adecuados que le permitan ser protegido del desgaste causado por el medio ambiente, de robos, de sabotajes causados ya sea por personas extrañas o por los propios empleados del ISP, o de otros factores tales como inundaciones, incendios, etc que pueden causar la destrucción de los recursos.

El *software* es otro factor que se debe proteger. Las amenazas internas contra este elemento pueden ser: supresión de programas, robo de un programa por uno de sus usuarios, corrupción de un programa causado por una falla en el *hardware*, o por intrusos que disfrazan su identidad con el fin de ingresar en la red.

Amenazas externas.- Las amenazas externas a la seguridad son las que traen mayores problemas. Un ataque externo es normalmente llevado a cabo utilizando alguna de las vulnerabilidades existentes en Internet.

El método más común de ataque a un sistema es mediante la obtención de un *password* de acceso mediante programas llamados *password crackers* para entonces sacar ventaja de los puntos vulnerables de una plataforma específica y de esta manera tomar el control de tal plataforma. Aunque esta actividad todavía

toma lugar en Internet con alarmante frecuencia, se están dando también otras formas de ataques a la seguridad, como son:

- Explotación de los huecos de seguridad existentes en los sistemas operativos como Unix y Windows NT.
- Explotación de los desperfectos en los protocolos.
- Uso de ICMP para lanzar el ataque mediante negación del servicio (*denial of service)*.
- Abuso de los servidores FTP anónimos
- Explotación de las debilidades en los servidores Web y servidores de E-mail.
- Uso de direcciones IP de origen engañoso (*spoofing*[a]).
- Uso de *sniffers*[b] para tener acceso a *passwords* y datos.

Existen muchas formas de ataques mediante negación del servicio (*denial of service*). Por ejemplo, una negación de servicio puede ser ocasionada debido a un incidente físico como la ruptura de un cable o por un incidente de tipo lógico como un error en las tablas de enrutamiento, pero una de las formas más utilizadas de negación de servicio es mediante inundación sincrónica (*SYN Flood*). Mediante este tipo de negación de servicio, una conexión TCP es iniciada por un cliente quien envía un paquete de *request* a un servidor y normalmente el servidor enviará un paquete *syn/ack* al cliente. El cliente entonces enviará un paquete *ack* al servidor y se iniciará la transferencia. Cuando la dirección IP del cliente es inalcanzable (ya que el cliente a enviado una dirección IP falsa), el servidor no puede completar la conexión. Cuando el servidor recibe cientos o miles de paquetes *request* el servidor es incapaz de servir a los clientes y niega el servicio a todos.

Cuando un intruso ha irrumpido exitosamente en el sistema, generalmente ellos

---

[a] *Spoofing* es el proceso de reemplazar partes de la cabecera TCP/IP con información ficticia para engañar al *firewall* o proxy haciéndoles creer que los datagramas que llegan son de origen confiable.

[b] Los *sniffers* pueden ser *hardware* o *software*, son fácilmente disponibles y pueden ser usados para monitorear el tráfico de la red. Los *sniffers* para *hardware* son utilizados en el cable físico de la red y los *sniffers* para *software* pueden correr desde una *workstation* enlazada a la red y aún sobre un enlace *dial-up*.

crean un *back door* por donde fácilmente podrán volver a ingresar. Cuando se ha detectado que un intruso ha ingresado al sistema de la red, es conveniente buscar los posibles *back doors* que éste abrió en el sistema. Para anular dichos *back doors*, lo que se debe hacer es reformatear el disco duro del servidor afectado y reinstalar el sistema operativo.

Amenazas debido a virus.- Los virus son una de las amenazas más comunes a la seguridad de los sistemas de computación. Los virus son programas hostiles que crean copias de sí mismos y los anexa a otros programas. Estos pueden ser de todo tipo, van desde aquellos que son inofensivos hasta aquellos que destruyen todos los datos a su alcance tanto en la máquina local como en la red. Erradicar un virus de un sistema computacional puede llegar a ser una actividad que tome mucho tiempo y puede ser muy difícil.

Adicionalmente a los virus, existen otros problemas que afectan al *software* de una red como por ejemplo los caballos de Troya y los gusanos (*worms*). Un gusano es similar a un virus, la diferencia es que éste envía copias de sí mismo a otras máquinas y allí se ejecutan como programas independientes. Los caballos de Troya, en cambio, son programas que tienen una función destructiva oculta bajo la apariencia de ser un programa con una función específica.

4.4. PROTECCIÓN DE LA INFRAESTRUCTURA DEL ISP. PROBLEMAS Y SOLUCIONES

Seguridad Física

Uno de los principales puntos a proteger es el acceso físico de los equipos que conforman la red del ISP ya sea de accidentes o ataques intencionales. Para ello se recomienda que elementos tales como: servidores, *routers*, *switches*, armarios de distribución, módems y demás elementos se encuentren en un ambiente protegido y de acceso restringido, ya que uno de los más importantes ataques a la red son internos.

En este capítulo no se desarrollará un plan completo de seguridad física, pero a continuación se darán algunas recomendaciones que serán de utilidad:

- Hacer un inventario de los bienes que posee el ISP
- Asegurarse de instalar protecciones adecuadas contra incendios, humedad, polvo, ruido eléctrico, rayos, inundaciones, vibraciones, etc.
- Proporcionar ventilación adecuada.
- No permitir el ingreso de comida al área donde se encuentran los equipos del ISP.
- Proteger los cables de red contra destrucción, escucha o intercepción.
- Tener a mano una lista de números de teléfono, números de cuenta de todos los proveedores de equipos y *software*, información de contratos de servicio e información para comunicarse con los empleados más importantes.

Separación de los servicios

Otra manera de proteger a la red del ISP es mediante la separación de los servicios. Como se indicó en el capítulo I, un excelente primer paso en la construcción de un útil y robusto medio de seguridad es la segregación del tráfico en varias redes. Para el ISP diseñado en el capítulo III, la razón por la cual se han separado los servicios en tres redes distintas se debe a que el ISP ofrece servicios con distintos niveles de necesidad de acceso, en otras palabras:

- La red de administración del ISP debe ser de accesibilidad restringida a los usuarios del proveedor y del público en general y de fácil acceso al administrador de la red.
- La red de servicios requiere más accesibilidad por parte de los usuarios del ISP ya que aquí se encuentran los servidores de aplicación, y
- La red de acceso debe permitir a los usuarios *dial-up* y corporativos conectarse a Internet sin ningún tipo de restricción.

Control de ataques mediante dispositivos adecuados

Los ataques externos a la red de un ISP pueden ser controlados por medio de dispositivos tales como los *firewalls.* Los *firewalls* son parte de la estrategia global de seguridad de un ISP, lo cual no significa que ésta deba ser la única medida de seguridad, un *firewall* debe emplearse para obtener seguridad adicional en conjunto con otros tipos controles internos.

Un *firewall* provee un medio de protección a una red interna, en este caso la red del ISP, de accesos no autorizados a intrusos a través de Internet, es decir, permite pasar conexiones específicas mientras bloquea otras. Es usado para ayudar a implementar políticas de seguridad ya que actúa como una barrera entre una red segura (ISP) y una red insegura como lo es Internet.

Un *firewall* permite que los usuarios del ISP accedan a los servidores Web de Internet y que intercambien *mail* con otros usuarios en Internet de manera confiable. Además evita que la información acerca de la red del ISP, como las direcciones IP, sean expuestas a los usuarios de Internet.

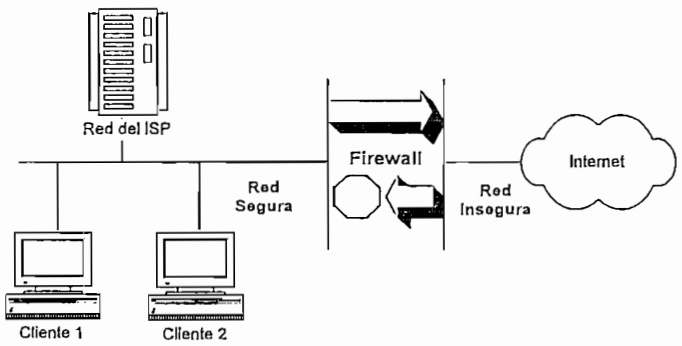


Fig. 4.1. Protección de una red interna con un Firewall [1]

Un *firewall* no es siempre un único dispositivo en una caja, generalmente, éste es construido en base a uno o más productos de *software* que corren en uno o más *hosts* que pueden ser sistemas de propósito general o *routers.*

Las principales tecnologías implementadas con un *firewall* son:

- Filtro de paquetes para limitar el tráfico
- Servidores Proxy o servidores SOCKS[a] para romper conexiones TCP/IP
- Servicios de nombre de dominio para proteger la información de la red.

Un ***filtro de paquetes IP*** es una buena forma de selectividad de tráfico ya que compara un paquete con un conjunto de reglas previamente configuradas que dicen qué paquetes son permitidos; es decir, los filtros de paquetes chequean la cabecera del paquete para determinar si debe ser enviado o descartado. Un filtro de paquetes es completamente transparente al usuario.

La mayoría de *routers* tienen alguna clase de tecnología de filtro de paquetes a nivel de cada red, aunque éstos no son realmente un *firewall*, pueden proveer suficiente protección en algunas circunstancias. Por ejemplo, un servidor Web conectado a Internet es un servidor público que debe ser fácilmente accesible por los usuarios de manera que aislarlo no sería una buena forma de protección. En este caso, utilizar un filtro de paquetes en un *router* es probablemente todo lo que se necesitaría para proveer alguna protección a este servidor.

Es conveniente que una red sea segmentada en dos partes: una red segura o interna y el perímetro de la red. En la red interna se encuentran todos los usuarios internos y servidores a los cuales un usuario externo no debe tener acceso (servidores encargados del control y administración de la red). En el perímetro de la red en cambio, se encuentran los servidores que pueden ser accesados a través de Internet (servidor *Web*, de correo, etc). Se hace esta división de redes ya que un solo *router* no puede proveer suficiente protección a la red interna.

Un ***servidor Proxy*** es una aplicación TCP o UDP. Su propósito es recibir peticiones de los clientes y reenviarlas a un servidor, y luego reenviar las respuestas desde el servidor hasta el cliente.

---

[a] *Socks* es la forma corta de la palabra *sockets*. Un *socket* es una combinación de un número de puerto TCP o UDP y una dirección IP

El objetivo más importante de un servidor Proxy es romper la conexión TCP/IP, es decir, los clientes no se conectan directamente a los servidores. El servidor solamente ve la dirección IP del servidor Proxy más no la del cliente. Esto es útil para mantener en privado la información de la red interna del ISP.

Los clientes necesitan conocer la dirección del servidor Proxy para enviar las peticiones en lugar de enviarlas al servidor con el cual desean comunicarse. Por otro lado, los servidores no tienen conocimiento que un servidor Proxy está siendo utilizado. Lo malo de los servidores Proxy es que se necesita uno para cada aplicación, es decir, un programa por cada aplicación como *Telnet*, FTP, HTTP, etc.

Un servidor Proxy, en lugar de controlar qué paquetes son admitidos y cuáles no, realiza una rigurosa autenticación de los usuarios en base a contraseñas y nombres de usuario.

El propósito de un ***servidor Socks*** es el mismo que un servidor Proxy, o sea, rompe la conexión TCP/IP y esconde la información interna de la red del ISP. La diferencia entre ambos es que un servidor *Socks* en lugar de manejar un solo tipo de protocolo de aplicación, maneja todos: HTTP, FTP, Telnet, etc., de esta manera se reduce la necesidad de tener servidores Proxy individuales a tener un solo servidor *Socks*.

Para usar un servidor *Socks*, el cliente debe soportar el protocolo *Socks*. Algunas aplicaciones tales como los *browsers* Web soportan *Socks*. Hay algunos sistemas tales como OS/2 que soportan *Socks* en su *stack* de protocolos TCP/IP a fin de que todas las aplicaciones del cliente puedan usar un servidor *Socks*.

Cuando se construye un *firewall*, se usa el ***servicio de Nombres de Dominio*** para que los usuarios internos puedan localizar las direcciones IP de todos los sistemas: internos y públicos, mientras que los usuarios en el Internet pueden solamente localizar direcciones IP de los servidores del ISP.

Se necesitan dos servicios de Nombres de Dominio, uno para nombres internos y otro para nombres externos. El servicio de Nombres de Dominio Interno envía peticiones de resolución de nombres al servicio de Nombres de Dominio Externo si no conoce el nombre del *host*. El servicio de Nombres de Dominio Externo es configurado para enviar peticiones a los servidores de nombre en el Internet si no conoce el nombre del *host*. Esto permite a los usuarios internos acceder a *hosts* en el Internet

Los usuarios en el Internet envían peticiones al servicio de Nombres de Dominio Externo para localizar a los servidores del ISP, pero éste no envía peticiones al servicio de Nombre de Dominio interno.

4.4.1. SEGURIDAD DE LAS PLATAFORMAS DE SERVICIO (SERVIDORES)

Para cada uno los servicios que ofrece el ISP se deben adoptar medidas de seguridad para prevenir el acceso desautorizado, la modificación de su base de datos, entre otras cosas.

En la Internet, los servicios más populares son los que tienen la mayor probabilidad de ser atacados y esto trae consigo grandes problemas tanto a los clientes como al ISP ya que se degrada la imagen del proveedor de servicios de Internet para con los clientes actuales y para clientes futuros.

Las plataformas de servicio individuales (servidores) deben ser configuradas de modo que solo respondan ante peticiones dirigidas a un puerto de servicio determinado. Por ejemplo, un servidor de *mail* debe responder solamente ante peticiones entrantes al puerto 25, un servidor DNS al puerto 53, etc.

Como se mencionó en el capítulo I en la sección 1.4.2.2, en la medida de lo posible, los servidores deben ser colocados en una *red de servicio dedicada* distinta de la *red de acceso al cliente* (*routers*) y de la *red NOC* (*Network Operation Center*, Centro de Operación de la Red) como se indica en la figura 4.2.

El acceso a la red de servidores debe ser por medio de un *router* de entrada, el cual realiza las funciones de un *firewall de filtro de paquetes.* El objeto de tal configuración es:

- El *firewall* debe permitir el acceso a los paquetes de los usuarios dirigidos a los puertos de los servidores.
- El *firewall* debe permitir el *acceso* al administrador de la red desde el centro de operaciones de la red NOC con fines de control y administración.
- Pero, debe impedir el acceso de los usuarios al centro de operación de la red.

Esta arquitectura es llamada *out-of-band* debido a que todas las funciones de administración y control son realizadas en una red de administración separada físicamente de la red de servicio. Sin embargo, esta separación en distintas redes implica un costo adicional para el ISP.

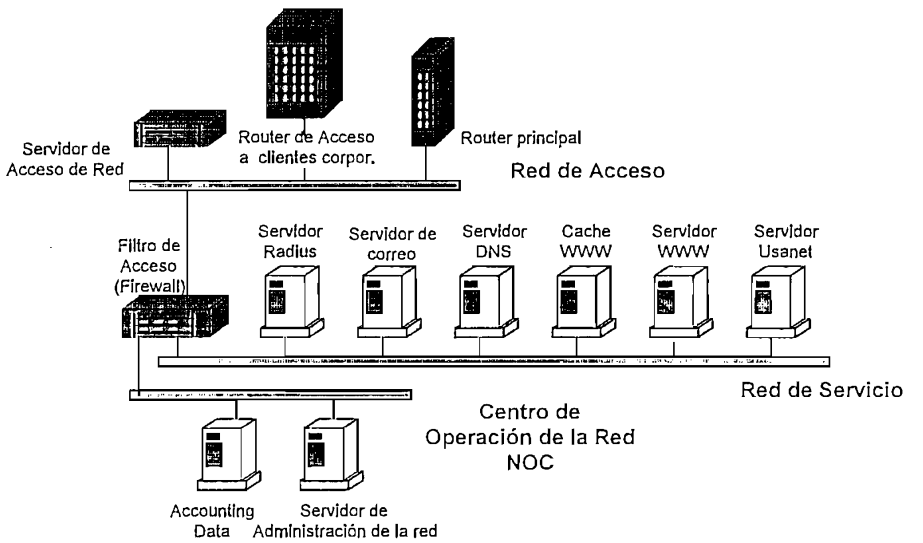


Fig. 4.2. Seguridad de las plataformas de servicio [2]

La segunda parte de seguridad para los servidores es asegurar cada uno de ellos individualmente. Cada aplicación tal como HTTP, FTP, DNS, etc., ofrecen diferentes alternativas para limitar el acceso y hacer seguro su uso. En este punto, se destacarán los principales mecanismos de seguridad para los servidores:

- Usar *wrappers*, los cuales son filtros configurados para permitir ciertos tipos de conexiones y negar el acceso a otros intentos de conexión.
- Utilizar plataformas de *software* actualizadas.
- Registrar todos los eventos de acceso al servidor como un medio de detectar intentos de infiltración.
- Mantener una copia segura del *software* del sistema para asegurar una rápida recuperación del servidor.
- Si se mantiene en el servidor información delicada, usar encriptación de datos para minimizar daños en caso de intrusos.
- Cambiar regularmente los *passwords* de acceso a los servidores.
- Ejecutar varios comandos de monitorización a diferentes horas del día puede hacer más difícil el acceso a personas no autorizadas.
- Evitar errores en la configuración de los servidores para no permitir a algún usuario ejecutar programas propios en la máquina del servidor, lo que puede comprometer la seguridad del sistema.
- No ejecutar nunca un comando del sistema cuyos parámetros sea información enviada por el cliente y no esté chequeada.
- Restringir el acceso a la información, es decir, qué información está disponible para qué personas.
- Verificar la compatibilidad entre *software* y *hardware*.

Para minimizar las caídas del sistema del ISP es conveniente adoptar arquitecturas tales como *mirroring* o *clustering.*

Mirroring o duplicación de servidores en tiempo real es llevada a cabo mediante un conjunto de servidores espejo (duplicación del primero) en el que cualquier dato que se escribe en el primero se escribe inmediatamente en el segundo. Si falla la unidad primaria por alguna razón, el disco secundario entra en acción, sustituyendo al primario sin interrumpir el funcionamiento.

Otra arquitectura es el ***clustering*** que consiste en un conjunto de discos interconectados que se comportan como un único disco virtual, con la diferencia del aumento de *performance* y de las características de redundancia; una

implementación más sencilla de un *cluster* es con dos servidores en la que si uno se cae el otro toma la responsabilidad justo en el punto del proceso donde se produjo el fallo. Los clientes notarán una demora de unos segundos mientras se regeneran los datos, superado ese momento el funcionamiento será el normal.

A continuación se detallan las consideraciones de seguridad para los servidores que sufren la mayor cantidad de ataques actualmente en el Internet:

4.4.1.1. Seguridad del Servidor Web

El Word Wide Web es el servicio con mayor crecimiento en el Internet y por lo tanto se está convirtiendo en uno de los puntos más vulnerables a los ataques, razón por la cual requiere especial atención.

El WWW es el blanco preferido de *hackers* y *crackers* quienes lanzan sus ataques ya sea por razones ideológicas, financieras o simplemente como actos vandálicos. Los servidores Web son la cara que una organización presenta al público, al violar servidores Web se puede dañar la reputación de una empresa, perder dinero e inclusive los atacantes pueden utilizarlo para iniciar desde allí otros ataques al resto de servidores o *routers* del ISP o contra otras organizaciones y usuarios.

Muchos servidores Web están ligados con el comercio electrónico y por lo tanto con dinero, de manera que estos servidores se han convertido en el depósito de información financiera confidencial y por lo tanto en un punto con muy alta probabilidad de violación de sus seguridades.

La solución a éstos y otros problemas es, por un lado, comprender sus limitaciones y por otro, adoptar medidas para estructurar un servidor Web seguro. La seguridad de un servidor Web abarca varios aspectos. Para los proveedores de *software*, un servidor Web seguro es aquel que provee ciertos protocolos criptográficos. Para los usuarios, un servidor Web seguro es aquel que guarda su

información confidencial sin riesgo alguno. Para la empresa que lo administra, un servidor Web seguro es aquel que resiste a ataques de todo tipo.

Para un ISP, un servidor Web seguro, debe ser esto y más, debe ser un servidor confiable que posea un espejo que lo respalde ante eventuales fallas de *software* o *hardware*, debe ser un servidor con posibilidad de escalar para brindar buen servicio aún con grandes cantidades de tráfico.

Un primer paso de seguridad para el servidor Web es seleccionar su posición con respecto al *firewall*. A continuación se verá este punto.

¿Cómo colocar el servidor Web en relación con el firewall?

Existen varias posibilidades a cerca de donde colocar el servidor Web con respecto al *firewall:*

1. El servidor Web puede estar colocado fuera del *firewall*, de manera que si un *cracker* logra violar la seguridad de este servidor no podrá proseguir tan fácilmente con otros ataques hacia la red del ISP ya que tendrá que vencer otro obstáculo: el *firewall*. La desventaja de esta ubicación es que el servidor Web no recibe la protección del *firewall*. Ver figura 4.3.

2. El servidor Web puede estar colocado detrás del *firewall,* de manera que los usuarios externos no utilicen otros servicios de Internet, como *Telnet* o FTP. En este caso es necesario configurar el *firewall* para que permita pasar transacciones en el puerto 80 (puerto WWW).

3. La última opción es colocar dos *firewalls*: uno para proteger la red del ISP y otro para proteger el servidor Web.

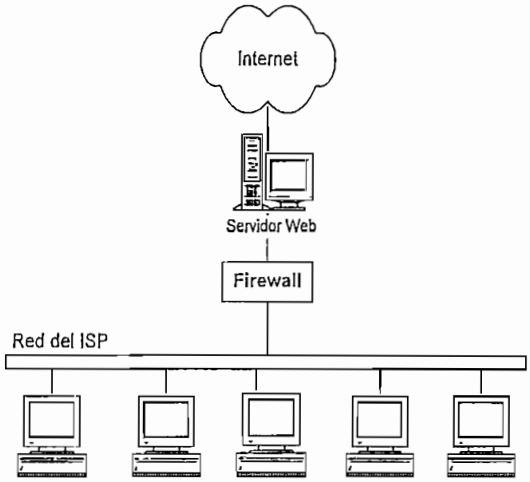


Fig.4.3. Servidor Web fuera del firewall [1]

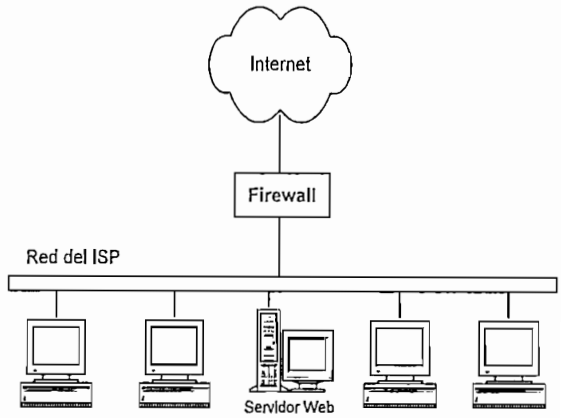


Fig.4.4. Servidor Web tras el firewall [1]

Control de acceso al Servidor Web

Controlar el acceso de personas no autorizadas es otra manera de asegurar un servidor Web y su contenido. Un ISP puede controlar el acceso a cierto tipo de información que se encuentra en su servidor y a la cual no desea que *todos* tengan acceso. Este método es aplicado cuando, por ejemplo, un servidor contiene información exclusiva para los empleados de una determinada empresa, cuando existe información que debe estar disponible solo para quienes hayan pagado una cuota de inscripción o firmado acuerdos de confidencialidad, etc.

Un servidor Web incluye varias formas mediante las cuales se puede controlar el acceso a su información, las más utilizadas son las siguientes:

- **Restricción del acceso mediante URL secretos**

Esta es la forma más sencilla de restringir el acceso a usuarios no autorizados, pero este método no es recomendado para asegurar información muy importante. Consiste en guardar la información en sitios ocultos del servidor Web, en este caso solo los interesados tendrán la dirección de la información oculta. Sin embargo este método no es considerado muy seguro ya que la

página podría ser fácilmente encontrada mediante las "arañas" del Web[a]. La página secreta será descubierta cuando una araña acceda a una página Web cualquiera que tiene un *link* hacia la página que se deseaba ocultar.

- **Restricción en base a la dirección**

Consiste en denegar el acceso en base a las direcciones IP de las máquinas o en base a su dominio de DNS. Las restricciones basadas en la dirección son transparentes al usuario, es decir, si un usuario utiliza una máquina autorizada éste puede tener acceso al servidor Web sin ninguna restricción. La desventaja que tiene este método es que un atacante puede atravesar esta barrera enviando paquetes con direcciones IP de origen engañoso (*spoofing*). También es posible implementar este tipo de restricción utilizando un *firewall* que bloquee las conexiones http de usuarios a los cuales se quiere restringir el acceso.

- **Restricción con base en la identidad**

Este método consiste en restringir la entrada a un servidor Web mediante el nombre del usuario y su clave que es la que lo autentica. El problema con este método es que es muy común que los usuarios compartan u olviden sus claves con facilidad. Para solucionar este problema se están buscando otras opciones, una de ellas es utilizar una *prenda física* para obtener el acceso. Las prendas físicas son computadoras de bolsillo (como por ejemplo: *Secure ID* o la *SecureNet Key*) que permiten utilizar una clave de acceso distinta cada vez que se ingresa a un sitio remoto, de esta manera, como el atacante no posee la prenda entonces no posee la clave de acceso.

Programación mediante CGI

Un servidor Web, además de transmitir archivos, puede ejecutar programas en

[a] Las arañas del Web son programas que escudriñan la páginas Web de un servidor y agregan palabras clave de cada una de estas páginas a una base de datos central. Ej.: Servidores Lycos y Altavista.

tiempo real como respuesta a la petición de un *browser*, dichos programas son conocidos como CGI (*Common Gateway Interface*; Interfaz de Pasarela Común). Un CGI, por ejemplo, puede ser un programa que haga consultas a bases de datos y luego muestre el resultado (motores de búsqueda) o programas que permitan a los usuarios de Internet conversar con otros usuarios, contadores, etc. En general, un CGI es un programa que recibe datos, los evalúa, los procesa y envía el resultado en forma de página de respuesta. El propósito de un CGI es agregar dinamicidad e interactividad a una página Web.

Como un programa CGI es un ejecutable, esto equivale a dejar al mundo ejecutar un programa en nuestro sistema lo cual compromete seriamente la seguridad del servidor. Uno de los métodos más comunes de ataque a un servidor Web es haciendo uso de los CGI. Un atacante puede engañar a estos programas externos para hacer algo que no debe o simplemente puede cargar sus propios programas externos en el servidor Web para luego ejecutarlos y de esta manera ganar el acceso al servidor para luego modificar, robar o suprimir archivos importantes. Por tal razón, existen una serie de precauciones de seguridad que son necesarias implementar cuando se usan programas CGI.

Debido a que es difícil tener certeza acerca de la seguridad de los programas CGI, lo que se puede hacer en este caso para evitar que un atacante engañe a un programa CGI es proporcionar un ambiente seguro donde se puedan ejecutar los *scripts* y programas CGI de manera que no consigan salirse de este ambiente limitado. La función *chroot* permite restringir el acceso a un directorio, en otras palabras, otorga a un proceso un mundo privado del cual no puede escapar.

Un atacante puede cargar sus propios programas externos haciendo uso del servicio FTP anónimo para luego hacerlo ejecutar por el servidor Web. Esto puede suceder: cuando ambos servidores se encuentran en la misma máquina, cuando los dos servidores pueden tener acceso a las mismas áreas del sistema de archivos, y cuando existe un directorio de escritura en alguna parte de estas áreas donde los clientes puedan cargar sus programas mediante FTP. En este

caso, el atacante podrá cargar su propio CGI o *script*[a] mediante FTP para luego ejecutarlo mediante HTTP. Para evitar que los atacantes carguen programas hostiles CGI, lo que se debe hacer es limitar las áreas del sistema de archivos a las que accede cada servidor, esto es posible también utilizando la función *chroot*.

En otras palabras, la función *chroot()* es de gran utilidad ya que mediante ella solo se da acceso a una sección específica de la jerarquía del sistema de archivos dentro del servidor Web.

Software de bloqueo y censura en el Web

De la misma manera que el Internet ha servido como un medio para compartir recursos, ideas y gran cantidad de información entre personas de cualquier parte del mundo, en éste se puede también encontrar información inapropiada sobre sexo, drogas, fórmulas para la fabricación de bombas, discusiones acerca de política que pueden desestabilizar regímenes y un sin número de temas que requieren algún tipo de control. Por tal motivo, la seguridad del cliente debe ser también un punto importante para el ISP.

En el Internet existen productos de *software* especializados cuyo objetivo es bloquear el acceso a un sitio Web que contenga material pornográfico el cual no debería ser visto por un niño o un adolescente. Siendo esta una de las principales preocupaciones que un padre tiene con respecto al contenido del Web, un ISP debe aconsejar el uso de tales productos a los padres que no desean que sus hijos vean este tipo de páginas. Otro motivo para que el proveedor aconseje el uso de dichos *software* es que de esta manera se reduciría notablemente el tráfico innecesario en la red del ISP.

Los *software* de bloqueo trabajan con varias técnicas para cumplir sus propósito. Entre ellas tenemos las siguientes:

---

[a] Algunos programas de comunicación vienen cargados con la función *script* que, en pocas palabras, consiste en una función que digita automáticamente informaciones como por ejemplo; el nombre de usuario, el *password* y cualquier otra cosa que sea necesaria para establecer un inicio de sesión.

- *Listas de exclusión de sitios*, la empresa que distribuye el *software* crea una lista de sitios que deben ser filtrados debido a su contenido. Esta lista inicial es distribuida con el *software* de bloqueo y luego se venden las listas actualizadas con base en suscripciones.
- *Bloqueo de palabras clave de nombres de sitio y páginas,* el *software* de censura bloquea todas las páginas que contengas palabras específicas.
- *Bloqueo de información transmitida,* el *software* de bloqueo puede ser configurado de manera que no se pueda enviar a Internet cierto tipo de información como números telefónicos, nombres, números de tarjetas de crédito, etc.

Algunos ejemplos de *software* de bloqueo disponibles en el Internet son: *SurfWatch* (http://www.surfwatch.com), *Net Nanny* (http://www.netnanny.com), *CYBERsitter* (http://www.solidoak.com), *CYBERtimer* (es un programa para Windows 95 que es parte de la familia de productos CYBERsitter), *Cyber Patrol* (http://www.cyberpatrol.com). Estos *software* puede ser directamente controlado por el usuario final o por el proveedor de acceso.

La tarea de mantener actualizada la base de datos de estas páginas no es tan simple para las empresas proveedoras de *software* de bloqueo ya que estos sitios cambian rápidamente o disfrazan su identidad con nombres de dominio aparentemente inofensivos. Otro problema de los *software* de censura es que accidentalmente se pueden bloquear páginas con contenido inofensivo o quizá haya personas que logren eludir este *software* simplemente inicializando el disco duro e instalando nuevamente el sistema operativo.

Resumen de recomendaciones para el servidor WWW

- Es aconsejable y en la medida de lo posible ejecutar un servidor Web en un host dedicado.
- Verificar la identidad del usuario al servidor
- El servidor WWW debe ser cuidadosamente configurado, controlando

quienes tienes acceso y a qué se tiene acceso. Se debe poner especial atención en las formas en que se podría cargar un programa, ya sea mediante FTP o correo, para luego hacerlo ejecutar mediante HTTP.

- Permitir a los clientes cargas sus programas CGI en el servidor Web dentro de áreas dedicadas para tal propósito. Generalmente, el directorio */cgi-bin* es el directorio que contiene los *scripts* y programas CGI.
- Administrar cuidadosamente el uso de programas CGI provistos por los usuarios y probarlos antes de correr tales programas en el servidor.
- Llevar bitácoras y auditar información sobre las transacciones con propósitos de facturación, resolución de conflictos, no reclamo e investigación de uso incorrecto.

4.4.1.2. Seguridad del Servidor de Nombres de Dominio (DNS)

Los servidores DNS contienen información de una parte de las computadoras de Internet (sobre determinadas subredes) teniendo capacidad de consultar información a otros servidores DNS para responder a las solicitudes referentes a *host* sobre los que no tienen autoridad. Para mantener la información actualizada en el DNS cada elemento de la base de datos tiene un tiempo de vida al cabo del cual si no se consigue una actualización se procederá a borrar dicha información.

Entre los problemas de seguridad que se presentan en este tipo de servicio es que los servidores DNS pueden obtener información falsa de un atacante y luego responder a solicitudes con esta información debido a una falta de comprobación entre el servidor solicitante y el servidor al que le preguntaron.

Aunque la mayoría de las resoluciones de nombres de *host* se efectúan de forma transparente, un atacante puede re-rutear el tráfico, destruir sus protecciones de seguridad y obtener otro tipo de información publicada sobre un *host* que se encuentre en los servidores DNS (adicional a la información que traduce el nombre de *host* a dirección IP y la información que traduce la dirección IP a

nombre de *host*) como su registro MX[a], HINFO (*Host Information; Información de Host)*[b], etc. Este almacenamiento constituye un riesgo para la seguridad, ya que los atacantes pueden preguntar al servidor de nombres y determinar los sistemas operativos más vulnerables, para realizar ataques contra los *host*. Una medida de seguridad sería implementar mecanismos de filtrado de paquetes y configurar DNS para que los registros HINFO no sean visibles al mundo exterior o no utilizarlos.

BIND, el servidor de DNS más utilizado en Internet, tiene algunos fallos de seguridad que comprometen la estabilidad del servicio de nombres a escala mundial, entre estos problemas se tiene: *bug NXT*, *bug solinger*, *bug fdmax*, *bug sig*, *bug naptr*, *bug maxdname*, para lo cual se recomienda actualizar los servidores BIND inmediatamente.

4.4.1.3. Seguridad del Servidor de Transferencia de Archivos (FTP)

Otro tipo de servicio que merece consideración especial es el FTP, ya que un servidor FTP mal configurado puede permitir que intrusos copien, reemplacen y borren archivos, razón por la que se requiere una correcta configuración. Se debe en la medida de lo posible, residir los servidores FTP en su propio *host*, ya que varios servicios corriendo en una misma máquina pueden interactuar de manera catastrófica. Algunos ISPs eligen colocar el FTP en los servidores de Web, debido a que los dos protocolos comparten las mismas consideraciones de seguridad, siendo en la práctica no recomendable ya que un intruso puede depositar un archivo en el área de FTP anónimo y causar que el servidor de HTTP lo ejecute.

Al proporcionar servicio FTP anónimo, el reto es asegurar que dicho servidor ponga disponible sólo la información que se desea y no dar acceso a otra

[a] *Mail Exchanger* (intercambiador de correo) que permite que los mensajes dirigidos a un determinado nombre de host se puedan redirigir a un nombre diferente. Por ejemplo, mediante MX se puede redirigir el correo enviado a epn.com hacia mail.epn.com.

[b] Se emplea para almacenar información sobre el *hardware* y configuración del sistema operativo de un determinado *host*.

información en la máquina a un extraño, debiendo proteger el área de escritura de manera que no se pueda utilizarla para transferir archivos entre otros lugares.

Cuando un atacante halla un sitio nuevo, por lo general crea un sitio oculto con nombre ".. " en el que guarda sus archivos e imágenes. El uso de las áreas de FTP anónimo consume recursos del ISP sea espacio en el disco duro o ancho de banda en la red sobretodo en el enlace a Internet, como consecuencia de este ataque se puede llegar a la negación de servicio.

Una forma de limitar la vulnerabilidad del FTP anónimo es desactivar la creación de directorios y ciertos archivos que posean nombres extraños (por ejemplo que empiecen con ".") mediante archivos de configuración. Este método no evita que un atacante deposite sus archivos pero sí hace más difícil que oculten cosas.

Otro método es crear subdirectorios secretos de escritura de manera que los usuarios puedan depositar archivos sólo si saben el nombre secreto tipo contraseña. Los atacantes no pueden verlos, no saben que hay un lugar para sus archivos.

El TFTP no soporta el mismo rango de funciones que FTP y no tiene seguridad por lo que se lo debe evitar tanto como sea posible. Este servicio se lo debe considerar sólo para uso interno y debe ser configurado en una manera restringida para que el servidor tenga acceso a un conjunto de archivos predeterminados, siendo el uso más conocido el bajar archivos de configuración a los routers. El TFTP debe residir en un *host* que soporte FTP externos.

4.4.1.4. Seguridad del Servidor de Correo Electrónico

El servidor SMTP más común en UNIX es Sendmail propiedad que lo hace un blanco tentador para los atacantes. Una de las razones por las cuales Sendmail tiene problemas de seguridad es que es un programa muy complejo, realiza varias funciones y necesita privilegios de *root* desventaja que un atacante puede

explotar. Para evitar estas desventajas se requeriría que Sendmail se rediseñara de manera importante y se volviera a implementar, reto que nadie lo ha realizado aún.

Los problemas más comunes en el servicio de correo electrónico son ataques de negación de servicio, caballos de Troya, desbordamiento de *buffer*, etc. Los problemas de seguridad de Sendmail han sido analizados ampliamente, mientras que la de los otros programas no, lo que no garantiza que éstos sean más seguros que Sendmail. Como solución a estos problemas se han realizado parches para cada *software* lo cual ha eliminado o reducido la mayor parte de ellos.

El ejemplo más famoso es el *bug* de Sendmail que puede permitir a un *craker* robar una *shell root*, utilizándolo para borrar archivos, crear nuevas cuentas, copiar el fichero de *password*, etc.

Otro problema que se presenta en los servidores de *e-mail* son los SPAM que son correos no solicitados que inundan el Internet con tantas copias del mismo mensaje llegando a personas que no desean recibirlo, lo que involucra pérdida de recursos en la red del ISP. Como medida de seguridad, se debe adoptar filtrado de mensajes por parte del servidor de correo electrónico.

Para evitar abusos en los mensajes de *e-mail* se debe recurrir al cifrado de dichos mensajes siendo la opción más utilizada en estos momentos el *software* PGP (*Pretty Good Privacy*[a]). El problema con estos programas es que para usarlos tienen que estar instalados tanto en el lado del emisor como en el del receptor. Otra alternativa simple consiste en enviar los mensajes en formato ZIP con *password*, pero no es lo más seguro ya que el *password* va incluido de algún modo dentro del mensaje, pero da una protección suficiente contra los intrusos casuales y no técnicos.

---

[a] Es un programa de utilidad para criptografiar los mensajes de e-mail, transformándolos en mensajes de código. Una vez criptografiado un mensaje con PGP, nadie podrá leerlo a menos que sea el destinatario.

Una medida eficaz de protección es suscribirse a listas de correo para poder tener lo antes posible información con detalle acerca de problemas y/o parches y actuar en cuanto esté disponible.

4.4.2. SEGURIDAD DE LOS *ROUTERS*

Uno de los principales ataques llevados a cabo en una red es el ataque a los *routers*, lo cual origina el cese del envío de paquetes o el envío de paquetes a destinos incorrectos provocado por la inserción de falsos paquetes de actualización de enrutamiento.

El requisito básico para tener una buena seguridad de los *routers* es tener un diseño de enrutamiento robusto. Es una actividad de alto riesgo realizar acuerdos *peering* sin tomar antes algunas precauciones básicas:

- Hasta donde sea posible, el enrutamiento *peering* debe ser evitado. En su lugar es mejor utilizar rutas estáticas ya que de esta manera se reduce notablemente el riesgo de promulgación de información falsa de enrutamiento filtrada a través de los clientes.
- Cuando el *peering* es completamente necesario, es recomendable utilizar un protocolo de enrutamiento exterior robusto. Actualmente, BGP-4 es una buena elección.
- Muchas formas de ataque a los *routers* usan direcciones de origen inventadas o engañosas en los paquetes con el fin de esconder la identidad y localización del atacante. Para evitar promulgación de información de enrutamiento falsa, es recomendable pasar todas las rutas aprendidas a través de *filtros de paquetes de ingreso.* Estos filtros descartan los paquetes cuyas direcciones de origen no corresponden al conjunto de rutas notificadas desde el puerto de red asociado.
- Es recomendable que el ISP utilice un registro de enrutamiento para

registrar sus políticas de enrutamiento y además sugerir a sus *peers* BGP[a] hacer lo mismo.

De esta forma, la información de enrutamiento pasada a través de una sesión *peering* deberá adaptarse a un conjunto de políticas de enrutamiento, minimizando el riesgo de corrupción de la información de enrutamiento. La identidad de los *peers* de enrutamiento también debe ser protegida, ya que un mecanismo de ataque es disfrazar la identidad de un *peer* de enrutamiento fiable.

Un ataque a un *router* puede causar un despacho (*forwarding*) incorrecto, mediante una desconfiguración, inyección de información de enrutamiento falsa, o de "*flood attack*" en la que un *router* es bombardeado con paquetes causando que baje el rendimiento del *router.*

Otro problema es el de "*spoofing*" que mediante actualizaciones de ruteo falsas causará que los paquetes sean enrutados a un *host* y luego re-enrutados a sus destinos correctos, de manera que un intruso puede monitorear los datos en los paquetes e incluso modificarlos. La solución ante este tipo de amenaza es proteger los mensajes de actualización de enrutamiento (paquetes *update*) mediante:

- El uso de campos de autenticación dentro de los paquetes *update*
- El uso de encriptación de los paquetes de actualización del protocolo de enrutamiento escogido.

La inestabilidad de las rutas es otro problema que puede estar directa o indirectamente relacionados con los *routers* y que a continuación se detalla:

Inestabilidades de las rutas

Varios defectos de diseño y problemas ya sea de la red del ISP o del *router* contribuyen a la desaparición y reaparición de rutas intermitentemente. A

[a] *Peers* BGP son dos sistemas que hablan BGP.

continuación se explican algunas de las causas de la inestabilidad de las rutas así como las técnicas para reducirlas:

- Inestabilidad del Protocolo de *Gateway* Interior (IGP).- La inserción de IGP en BGP mediante redistribución[a] puede causar fuga de información no deseada (direcciones privadas o direcciones internas ilegales, es decir, direcciones no registradas que son utilizadas dentro del AS) hacia BGP, una solución sería la inserción estática de información en BGP. En el caso de que una ruta o varias estén constantemente arriba y abajo provoca que la estabilidad de Internet se afecte negativamente, debido a la gran cantidad de tráfico de enrutamiento generado que puede consumir todo el ancho de banda del enlace y sobreutilizar la CPU de los routers. Mediante el mecanismo de *route dampening*[b] se puede solucionar este problema.

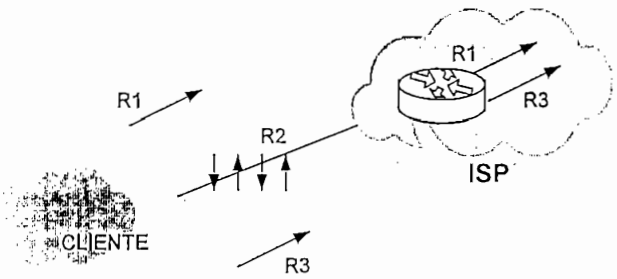


Fig. 4.5. Route dampening en un entorno ISP[3]

En la figura 4.5 se ilustra el mecanismo *route dampening* en un entorno ISP, donde la ruta R2 del cliente está fluctuando; al momento que el ISP ejecute *route dampening* R2 será penalizado y eliminado de acuerdo a su nivel de fluctuación, ya que las fluctuaciones de R2 crea gran gasto en los *routers* fronterizos e interiores. Mientras tanto las rutas R1 y R3 son transportadas a través de IBGP y/o IGP dependiendo de cómo el administrador está insertando las rutas.

---

[a] Es el proceso por el cual se importan rutas de un protocolo de enrutamiento a otro.

[b] Penaliza y concluye la publicación de rutas fluctuantes (durante minutos incluso horas hasta que se estabilice), dependiendo del grado de inestabilidad. Cada vez que una ruta efectúe una fluctuación, se le impone una penalización (valor numérico incrementado) y cuando dicha penalización alcanza un umbral predefinido en un intervalo de tiempo se suprime la ruta.

- ***Hardware* defectuoso.-** Producido por interfaces, sistemas o enlaces defectuosos. Este tipo de fallas están fuera del control del ISP, por lo que la redundancia del sistema y del enlace se constituyen en herramientas importantes para reducir la pérdida de conectividad debida a fallos.

- **Potencia de CPU insuficiente.-** A medida que crecen las actualizaciones de enrutamiento y sesiones de *peering* que administra el *router*, se requiere mayor potencia de CPU. Al comenzar la construcción de tablas BGP después del establecimiento de sesiones BGP, un procesador de sistema puede pasar más del 90%[3] de su tiempo procesando actualizaciones. Cosa similar ocurre cuando los enlaces se vuelven inestables, la CPU se encuentra bastante ocupada gestionando actualizaciones, provocando la caída de sesiones BGP y por consiguiente la inestabilidad.

- **Memoria insuficiente.-** Un *router* puede dejar de funcionar en el momento en el que alcanza su límite de memoria, problema que causaría la pérdida de todas las rutas conocidas; la mayoría de los proveedores han actualizado sus sistemas a 256 MB[3] de memoria para la tabla de enrutamiento. En la actualidad, las tablas de enrutamiento de BGP incluyen más de 75000 rutas, número que se incrementa cada mes.

- **Actualizaciones de red y mantenimiento de rutina.-** Se refiere a las actualizaciones de nuevas versiones de *software* o *hardware*, adición de enlaces (más ancho de banda), etc, que mediante una buena planificación y simulación de la red son las claves para conseguir actualizaciones satisfactorias. Por ejemplo, los cambios en la red se deben primero simular en entornos que no son de producción.

- **Error humano.-** Son cometidos por los administradores que realizan cambios sin tener en cuenta las posibles repercusiones que pueden acarrear, para lo cual ellos deben anticiparse ante los posibles problemas

que podrían surgir; por ejemplo, deben desarrollar un plan de copia de seguridad para volver a la antigua configuración si la nueva no funciona.

- **Congestión del enlace.-** La caída de un enlace provoca que otro enlace adopte el tráfico del enlace caído. Pese a que el enlace pueda o no soportar la carga adicional, se ve involucrado otro aspecto: la potencia del *router*, éste podría no ser capaz de administrar la carga adicional, lo cual se ve reflejado en la degradación del rendimiento para el usuario final.

4.5. PROTECCIÓN DEL *SOFTWARE* DEL ISP. PROBLEMAS Y SOLUCIONES

Compra inicial del software

El primer paso que hay que dar frente a la seguridad del *software* de un ISP es la compra inicial del mismo. Se debe adquirir un *software* de proveedores con conocida reputación y que respondan en forma oportuna ante reportes de fallas en la seguridad o con respecto al desempeño de sus productos.

Antes de adquirir un *software*, se deben tener ciertas precauciones. El comprador de *software* debe asegurarse que dicho producto haya sido previamente probado y evaluado y debe solicitar la documentación en la cual consten los resultados de dichas pruebas operacionales. Debe además solicitar una cláusula escrita mediante la cual el proveedor de *software* se comprometa a responder ante eventuales fallas de su producto, sin embargo, ningún desarrollador de *software* correrá con los gastos correspondientes a las pérdidas totales que su producto pueda ocasionar, su responsabilidad se limitará al costo del medio físico en el que se distribuye el producto. Es importante también solicitar una cláusula escrita en la cual se aclare cómo el proveedor de *software* notificará a sus clientes acerca de fallas de seguridad recién corregidas.

Normalmente, estas notificaciones son realizadas a los clientes mediante FIRST[a] (*Forum of Incident Response and Security Teams*; Foros de Equipos de Respuesta a Incidentes y Seguridad)

Seguridad del Sistema Operativo

El siguiente paso con respecto a seguridad del *software* es estar conciente de las inseguridades que presentan los sistemas operativos que se están utilizando y de esta manera realizar planes de seguridad para afrontar tales fallas.

Windows y Windows NT han sido el blanco de los más recientes ataques de piratería. Debido a la fama que está adquiriendo Windows NT, está siendo constantemente bombardeado y más gente está tratando de romper sus seguridades. Desafortunadamente, una vez que se descubre una debilidad en un sistema operativo, ésta se difunde rápidamente por Internet y es aprovechada por los atacantes para realizar intrusiones a cualquier organización o compañía.

Una forma de mantener segura la red del ISP es mantenerse informado de los problemas del sistema operativo (cualquiera que sea el sistema operativo que se utilice) y mantenerlo actualizado para lo cual lo mejor es visitar constantemente el sitio Web del proveedor del sistema operativo. Microsoft es muy rápido en desarrollar parches (*Service Packs*) para los errores descubiertos, estos parches o actualizaciones contienen las soluciones para los problemas de seguridad detectados.

Existen muchos recursos en línea en los cuales se puede hallar información detallada acerca de los errores y soluciones de algunos sistemas operativos, uno de ellos es http://www.rootshell.com/. De igual manera, se pueden descargar actualizaciones de Linux desde http://www.redhat.com.

---

[a] FIRST es una asociación constituida por organizaciones privadas, de gobierno, comerciales, académicas, etc. para intercambiar información y coordinar actividades de respuesta ante incidentes de seguridad. FIRST provee un medio para la comunicación de alertas sobre nuevas amenazas potenciales a la seguridad, incluye investigación y facilita la compartición de información relacionada con seguridad, herramientas y técnicas. Actualmente FIRST cuenta con más de 100 miembros alrededor del mundo, los cuales se reúnen en un foro (2 o 3 veces al año) para intercambiar ideas y soluciones.

Linux ha heredado algunos de los problemas de Unix (errores en *Sendmail*, por ejemplo) y adicionalmente añade algunos errores propios. Continuamente se descubren nuevos errores en el núcleo de Linux, los cuales son generalmente peligrosos porque el interrumpir las operaciones en dicho nivel da lugar a errores serios del sistema como colapso o pérdida de los servicios de red.

Instalar un parche para Linux es mucho más complicado de lo que lo es para Windows ya que a menudo se debe aplicar el parche al código fuente del núcleo, recompilar y reinstalar el núcleo. La compañía RedHat mantiene disponible en línea los parches de estas fallas de seguridad.

La conclusión es mantener actualizados los sistemas operativos. Los usuarios NT y usuarios UNIX deben prestar especial atención a los errores que vayan apareciendo en los sistemas operativos ya que una manera de hacer frente a las intrusiones es conocer antes lo que los atacantes podrían utilizar en su beneficio.

Reconocimiento de actividades no autorizadas

Existen herramientas dentro de los sistemas operativos o herramientas públicamente disponibles que permiten detectar la mayoría de accesos no autorizados a un sistema de computación mediante monitoreo. El monitoreo debe ser un proceso regular mediante el cual se pueda vigilar el sistema para detectar violaciones a la seguridad o algún suceso inusual en la red.

La mayoría de sistemas operativos almacenan numerosos bits de información en los *log files*[a]; es una buena medida de seguridad chequear constantemente estos archivos para detectar a cualquier usuario no autorizado. Cuando se realiza la inspección de los *log files*, se puede seguir cualquiera de los siguientes procedimientos o inclusive todos:

- La mayoría de usuarios, típicamente se conectan a Internet a la misma hora del día. Una conexión fuera del tiempo normal podría significar la

[a] *Log files* son archivos en los cuales se registran las actividades de un ordenador.

presencia de un intruso. Por lo tanto, es conveniente constantemente comparar las listas de usuarios que están en ese momento *logged in* con las historias de *login* pasados de los usuarios.

- Un ISP mantiene registros de *accounting* con propósitos de facturación, estos registros pueden ser utilizados para determinar modelos de uso, es decir, un registro inusual de *accounting* (como por ejemplo, uso excesivo del servicio) podría indicar uso no autorizado del sistema.
- Algunos sistemas operativos tales como UNIX ofrecen ciertas herramientas de utilidad tal como *syslog.* Esta herramienta permite detectar cuándo un *password* es ingresado incorrectamente varias veces durante un período corto de tiempo, lo cual hace suponer que alguien está intentando adivinar la clave.

Detectar a tiempo intentos de acceso no autorizado al sistema del ISP mediante monitoreo es una forma de proteger el *software* y a la vez proteger la integridad del usuario del ISP ya que mediante este método se puede detectar no solamente a intrusos que buscan causar daño al sistema sino también a aquellos quienes "piratean" la cuenta de algún usuario del ISP.

Monitorear un sistema es una tarea constante que es realizada por el administrador del sistema quien debe ejecutar periódicamente comandos de monitoreo. Es recomendable que esta acción no se la realice en horas fijas del día ya que si un intruso conoce las horas en la que se realiza el monitoreo de la red, simplemente esperará para entrar y atacar.

Las acciones que se deben tomar cuando se detecta acceso no autorizado a la red deben ser claramente delineadas en las políticas de seguridad del ISP que se verán más adelante.

Respaldos o Backups

Un respaldo o *backup* es una copia de los datos escrita en algún medio de almacenamiento duradero. El objetivo de realizar *backups* es proteger los datos

en caso de fallas de los equipos, borrado accidental de archivos, poder restaurar archivos modificados por un atacante mediante la comparación de los archivos dañados con los de respaldo.

Los archivos de respaldo sin embargo, no están exentos de problemas por lo que conviene verificar que los datos de respaldo sean correctos para poder emplearse en el restauración de un sistema. Adicionalmente, se considera prudente encriptar los *backups* ya que en el caso de que un atacante tenga acceso al sistema de respaldo no resulten comprometidos los datos. Deben hacerse respaldos del sistema regularmente y éstos deben guardarse en sitios seguros y protegidos a fin de proteger la información que contienen.

4.6. PROTECCIÓN DE LOS DATOS

Uno de los puntos más vulnerables de una red frente a ataques de intrusos, es la captura de información durante su transferencia. Las transacciones comerciales a través de Internet requieren una comunicación segura. Modificar un mensaje de manera que ningún intruso lea su contenido, es una buena manera de proteger la información en caso que ésta sea interceptada durante su transmisión.

El objetivo de la seguridad de la información es asegurar la continuidad de las transacciones y minimizar el daño que se puede producir, previniendo y minimizando el impacto de incidentes de seguridad.

Encriptación

La encriptación (o codificación) es el método por el cual la información puede ser protegida a través de programas encargados de *cifrarla*, *firmarla*, y cerrarla para que sólo pueda ser abierta nuevamente por quien tenga la *clave* apropiada para poder recuperar el mensaje (desencriptación), agregándose además métodos para validar la integridad de la información recibida, o sea, para confirmar que la información no haya sido modificada en el camino.

Varios son los aspectos que hay que manejar en el proceso de transferencia de un documento y que define una comunicación segura:

1. **Autenticidad:** consiste en la seguridad de que las personas que intervienen en el proceso de comunicación son las que dicen ser. ¿Cómo está seguro B de que en verdad es A el que se lo ha enviado y no otra persona?. El método más usado para proporcionar autenticidad es la firma digital que más adelante se lo tratará.
2. **Confidencialidad:** se trata de la seguridad de que los datos que contiene el documento permanezca oculto a los ojos de terceras personas durante su viaje. Ataques posibles a la confidencialidad pueden ser la captura del documento en su viaje de A a B y el uso indebido de los datos del documento o la mala gestión y almacenamiento de éstos por parte de B. La confidencialidad se logra generalmente mediante métodos criptográficos.
3. **Integridad:** consiste en la seguridad de que los datos del documento no sufran modificación a lo largo de su viaje. Esto significa que se querrá proveer algo de seguridad como la integridad de la información del sistema. Una manera de realizar esto es producir el *checksum* de un archivo no alterado y periódicamente chequear que el archivo no se alteró.
4. **No repudio:** se trata de que una vez enviado un documento por A, éste no pueda negar haber sido el autor de dicho envío.

El ***cifrado*** es el proceso mediante el cual se disfraza la información utilizando reglas matemáticas. Para que los datos estén seguros, los sistemas de cifrado utilizan una *clave*[a], que a veces se genera aleatoriamente y otras veces es seleccionada por el usuario. Para obtener los datos en su forma original el receptor debe conocer la clave. Indudablemente, cuanto más complicado sea el mecanismo de cifrado y cuanto más larga sea la clave, más difícil será romper el sistema y obtener el mensaje original para un extraño.

---

[a] Se utiliza como parte del proceso de cifrado, siendo los datos cifrados los únicos para esa clave en particular. Los sistemas que permiten al usuario a elegir sus claves suelen ser poco confiables, ya que las claves pueden no ser del tamaño adecuado.

Para que una función pueda ser considerada de codificación debe ser biyectiva por lo que debe cumplir:

1. Elementos diferentes deben tener imágenes diferentes, es decir, no puede haber dos palabras que tengan la misma transformación en el código.
2. Todos los elementos deben tener imagen, es decir, no puede haber palabras que no tengan su transformación en el código.
3. No puede haber palabras del código que no se correspondan con alguna palabra de la fuente.

A continuación se hace una breve revisión de los algoritmos criptográficos más utilizados: algoritmos de llaves simétricas, algoritmos de llave pública y sistemas mixtos.

- Los *algoritmos de llaves simétricas* utilizan la misma llave para encriptar y desencriptar un mensaje. Ejemplos de este tipo de algoritmo son: DES (*Data Encryption Standard*; Estándar de Encriptación de Datos), DESX, *Blowfish*, IDEA (*Internacional Data Encryption Algorithm*; Algoritmo Internacional de Encriptación de Datos), etc. En criptosistemas[a] de clave secreta se logra la confidencialidad manteniendo secreta la clave de descifrado. La integridad se logra manteniendo secreta la clave de cifrado. Por lo tanto, el secreto y la autenticidad de los mensajes se obtienen al mismo tiempo. Las principales desventajas son la distribución de las claves, el peligro de que muchas personas deban conocer la misma clave y la dificultad de almacenar y proteger muchas claves diferentes.

- En los *algoritmos de llave pública* el usuario puede cifrar sus mensajes de dos formas:

    a) Usando la clave pública del receptor; en este caso, sólo el receptor en posesión de la clave privada podrá descifrar el

[a] Es un sistema que permite cifrar y descifrar la información, logrando con ello la integridad y confidencialidad de los datos.

mensaje asegurándose la confidencialidad, y

b) Usando su propia clave privada; en esta situación, cualquier usuario en conocimiento de la clave pública del emisor, podrá descifrar el mensaje comprobando la integridad del mensaje y la autenticidad del emisor.

La llave pública puede ser divulgada sin poner en peligro la confidencialidad del mensaje; como punto importante no se puede obtener la clave pública a partir de la privada y viceversa, lo cual constituye una ventaja para transmitir los datos cifrados y la clave a través de la red sin tener que preocuparse de que dichas claves sean interceptadas. Ejemplos de estos algoritmos son: RSA (*Rivest, Shamir and Adleman* son sus autores), DSS (*Digital Signature Standard*; Estándar de Firmas Digitales), etc. En criptosistemas de clave pública se logra la confidencialidad al descifrar el receptor el mensaje cifrado con su clave privada. La integridad se logra al cifrar el emisor el mensaje con su clave privada. Por lo tanto, el secreto y la autenticidad de los mensajes se logra en general por separado.

- En la actualidad se están implementando *sistemas criptográficos mixtos* en los que se utiliza la llave pública del receptor para encriptar una clave simétrica que se usará en el proceso de comunicación encriptada. De esta forma se aprovechan las desventajas de ambos sistemas, utilizando el sistema asimétrico para el envío de la clave sensible y el simétrico (con mayor velocidad de proceso) para el envío masivo de datos.

La fortaleza de los criptosistemas simétricos o de clave secreta descansa en la imposibilidad de calcular la clave. Mientras en los de clave pública la fortaleza descansa en la imposibilidad computacional de deducir la clave privada a partir de una clave pública.

La ***firma digital*** es el conjunto de datos que permiten identificar al remitente. Se añade a una unidad de datos para protegerlos contra la falsificación, permitiendo al receptor probar el origen y la integridad de los mismos. La firma digital suele

usarse para autentificar mensajes, para validar compras por Internet, para realizar transferencias de fondos bancarios y para otras transacciones de negocios. A un mensaje resumido mediante una *función hash*[a] (MD2, MD4, MD5, SHA-1,etc.) y encriptado con una llave privada es lo que en la vida real se denomina firma digital. La firma digital ha llegado a constituirse en una prueba indudable de autoría del envío de un documento electrónico, semejante a la firma tradicional de puño y letra.

Los sistemas criptográficos más utilizados en la actualidad se dividen en dos categorías:

- Programas y protocolos utilizados para encriptar mensajes de correo electrónico o archivos guardados en computadoras para darles mayor protección como: PGP (*Pretty Good Privacy*; Privacía Bastante Segura), S/MIME (*Secure/Multipurpose Internet Mail Extensions*; Extensiones Multipropósito de Correo de Internet Seguro); y,
- Protocolos de red utilizados para proporcionar confidencialidad, autenticación, integridad y no repudio[b] como: SSL (*Secure Sockets Layer*; Nivel de Conexiones Seguras), Kerberos, SET (*Secure Electronic Transactions*; Transacciones Electrónicas Seguras), CyberCash, etc.

La encriptación de datos es muy necesaria en aplicaciones tales como:

- Compras a través de Internet, en el cual un usuario puede seleccionar una tarjeta de crédito como un método de pago. En este caso, la aplicación invoca un servicio criptográfico de pago seguro: el sistema de Transacción Electrónica Segura SET. Las funciones criptográficas usadas tienen que

[a] Son funciones matemáticas que comprimen el documento a enviar en un único bloque de longitud fija, bloque cuyo contenido es ilegible y no tiene ningún sentido real. El proceso es el siguiente: el emisor aplica una función *hash* conocida al documento, obteniendo un resumen *hash* del mismo para luego encriptarlo con la clave privada del emisor. Consecutivamente se envía el documento original plano y el resumen *hash* encriptado. El receptor por su parte aplica la función *hash* al resumen sin encriptar y desencripta el resumen encriptado con la llave pública del emisor, si ambos resúmenes coinciden se comprueba la autoría del emisor, caso contrario, el documento fue interceptado y modificado o no es de quien dice ser, por lo que conlleva al rechazo del mismo.

[b] Es decir, mediante la encriptación se crean recibos, de forma que el autor de un mensaje no pueda negar falsamente su envío.

ser invocadas transparentemente entre las partes para lo cual utiliza el protocolo PPN (*Protocol for Payment Negotiation*; Protocolo para la negociación de Pagos).

- Actividades bancarias, en las cuales se deben tomar medidas de seguridad apropiadas para proteger los bienes financieros del cliente y de la institución financiera.
- Distribución de contenido seguro, para evitar la proliferación de copias ilegales y de esta manera proteger los derechos del autor. Los *cryptolope containers* son una solución de IBM que consiste en un sofisticado paquete electrónico que mantiene una versión encriptada de un documento de texto o un artículo electrónico como música, *film*, *software*, gráficos y productos multimedia. Estos *containers* pueden ser abiertos usando solamente llaves criptográficas que son provistas a los usuarios quienes han comprado el contenido.

4.7. POLÍTICAS DE SEGURIDAD DEL ISP

Una política de seguridad es el establecimiento formal de reglas mediante las cuales los usuarios de un ISP tienen acceso a los recursos del proveedor. Una política de seguridad ayuda al ISP a responder ante incidentes de seguridad, permitiéndole minimizar los riesgos, manejar los incidentes en forma rápida, eficiente y efectiva para reducir el potencial impacto de un ataque.

La creación de las políticas de seguridad debe ser un esfuerzo conjunto entre el personal técnico de la empresa y entre quienes tienen el poder para hacerlas cumplir. Entre las personas que deben estar involucradas en el desarrollo de tales políticas se mencionan las siguientes: administradores de la red, *staff* técnico, administradores de grandes grupos en la organización, representantes de los grupos de usuarios afectados, asesor legal, etc. Dentro de este conjunto de personas, los *managers* tienen el presupuesto y la autoridad para llevar a cabo las decisiones tomadas, el *staff* técnico son las personas que saben lo que se debe o no hacer y la consulta legal sabe todos los aspectos legales acerca de las

distintas opciones se que podrían tomar.

Las políticas de seguridad deben abarcar varias áreas de actividad del ISP:

- Una política de seguridad debe proveer instrucciones relacionadas a la *evaluación de la tecnología del servicio* para asegurar que el equipo no comprometa el entorno de seguridad actual.
- Una política de seguridad debe hacer constar la posición del ISP con respecto a la *privacidad de datos*.
- En forma similar, dicha política debe definir el proceso de *acceso de datos* y en qué formatos.
- En general, la mayoría de ISPs adoptan una política similar a la de un *carrier*, en la cual el ISP no realiza inspección o alteración de ninguna clase sobre el contenido de los datos del cliente ni tampoco acepta ninguna obligación acerca del tipo de información que transita por su red, es decir, el cliente es el responsable del contenido de dichos datos.
- El ISP debe especificar dentro de sus políticas de seguridad el proceso mediante el cual reportará incidentes de seguridad, aclarando las *responsabilidades del ISP y la del cliente* en tales situaciones.

Una política de seguridad debe permitir al ISP que su *staff* responda eficientemente ante los incidentes de seguridad sin comprometer la confidencialidad del cliente y sin exponer al ISP ni al cliente a aceptar obligaciones injustificadas. Un ISP debe obtener asesoría legal sobre sus políticas para asegurarse que sus objetivos estén adecuadamente direccionados desde el punto de vista legal.

Además, una política de seguridad debe hacer constar claramente las circunstancias bajo las cuales el administrador del sistema podría inspeccionar los datos del cliente y las obligaciones del administrador respecto a la divulgación de esta información.

Las políticas de seguridad deben impactar directamente en el diseño del contrato

de servicio entre el ISP y sus clientes. Se debe asegurar que el contrato incluya el compromiso del cliente para utilizar los servicios del ISP en forma responsable y legal. El contrato debe incluir especificaciones prohibitivas con respecto a lo siguiente:

- El abuso en la utilización del servicio
- Acciones que desestabilicen el servicio del ISP o terceros.
- Introducción ilegal a otras cuentas o servicios.
- Acceso o alteración de datos de terceros sin el consentimiento de la parte involucrada.

El contrato de servicio debe cubrir aspectos acerca del comportamiento destructivo o criminal tales como. Intentos de intrusión, ataques de negación del servicio (*denial of service*), abuso del sistema de *E-mail* o *Usenet* a través del envío de grandes volúmenes de mensajes no solicitados. Hasta donde sea posible, el contrato debe otorgar al ISP la capacidad de cancelar el contrato de servicio al cliente si se llegara a detectar el abuso de alguno de los puntos mencionados anteriormente. Finalmente, el contrato debe hacer constar claramente las sanciones al cliente como una consecuencia de llevar a cabo tales actividades.

Resumen del sistema de seguridad del ISP de diseño

1. La primera medida de seguridad que se ha adoptado como parte del diseño del ISP es la separación de los servicios en redes distintas para ofrecer diferentes niveles de acceso a los servicios del ISP, para esto se utilizará el *switch Extreme Summit* 24 de *Extreme Networks*.

2. Se controlará los posibles ataques al ISP utilizando el *firewall* PIX 515UR de Cisco, ya que éste es un dispositivo de alto rendimiento, proporciona suficiente potencia para más de 100000 conexiones simultáneas, permite

hacer de una red un DMZ (*Demilitarized Zone*; Zona Desmilitarizada) protegido, realizar filtrado URL y detección de virus.

3. Se asegurará el servidor *Web* colocándolo tras el *firewall* de manera que este servidor se vea beneficiado de las características de seguridad que ofrece dicho elemento.

4. Se adquirirán discos duros de respaldo para todos los servidores como medida de protección de la información del ISP. En la medida de lo posible, estos discos duros deberán ser SCSI.

5. Se asegurarán todos los servidores con el *software* antivirus *Norton Security* 2002 edición profesional de la compañía Symantec ya que protege de las amenazas de virus, defiende de infiltraciones de *hackeres*, intercepta automáticamente conexiones sospechosas, entre otras.

6. Una vez implementado el proveedor de servicios, se deberán seguir todos o varios de los criterios mencionados en este capítulo para mejorar los niveles de seguridad. Por ejemplo:

    - Configurar cada uno de los servidores de manera que respondan ante peticiones dirigidas a un determinado puerto de servicio.
    - Asegurar cada uno de los servidores individualmente haciendo uso de las diferentes herramientas que éstos ofrecen.
    - Configurar los *routers* adecuadamente mediante la implementación de filtros de paquetes.
    - Mantener actualizado el *software* de todos los equipos.
    - Monitorear constantemente la red.
    - Incluir normas de uso de los servicios del ISP en el contrato de los usuarios. Este contrato debe incluir:

        1. El compromiso del cliente para utilizar los servicios del proveedor en forma responsable y legal.

2. El compromiso del ISP de mantener la privacidad de los datos del cliente. Sin embargo, el proveedor debe aclarar en qué casos éste podría inspeccionar los datos del usuario y aún cancelar el contrato de servicio si fuera necesario.

BIBLIOGRAFÍA CAPÍTULO IV

[1] "Seguridad y Comercio en el Web, Riesgos, Tecnologías y Estrategias"; Simson Garsinkel y Gene Spafford; Traducción de la primera edición; McGraw-Hill Interamericana editores; 1999; México.

[2] "*ISP Survival Guide. Strategies for Running a Competitive ISP*"; Geoff Huston; Primera Edición; John Wiley & Son,Inc.; 1999; EE.UU.

[3] "*Internet Routing Architectures*"; Sam Halabi y Danny McPherson; Segunda Edición; Cisco Press; 2000; Indianapolis-EE.UU.

[4] http://personales.ciudad.com.ar/technical_support/intranet-nt.PDF
Seguridad de acceso

[5] http://www.consorci.net/difusio/seguridad_perimetral.pdf
Seguridad de los sistemas informáticos

[6] http://www.firstvpn.com/papers/misc/DSLSecurity.pdf
Fundamentos de la seguridad en redes

[7] http://atencion.faces.ula.ve/pagseguridad/web/tutoriales/pdf/firewallspresentacion.pdf
Seguridad

[8] http://www.unam-cert.unam.mx/herramientas.html
Área de seguridad en cómputo

[9] http://www.terra.es/personal6/morenocerro2/seguridad/cripto/cripto_12.html
Criptografía

5

SISTEMA DE TARIFACIÓN

CAPÍTULO V

SISTEMA DE TARIFACIÓN

Cuando la Agencia de Proyectos de Investigación Avanzada de Defensa de Estados Unidos (DARPA) se interesó en establecer una red de comunicación de paquetes para proveer comunicaciones robustas entre instituciones de investigación civiles y militares, la posición inicial de esta agencia fue la de establecer una red dedicada a la investigación y al desarrollo, consecuentemente ningún sistema de tarifación fue impuesto a los clientes finales de dicha red. Dado que el servicio era libre de costo para los usuarios, la red empezó a crecer a pasos acelerados, razón para que este modelo de operación no fuera un modelo sustentable a largo plazo; y, establecer una forma de tarifación para proveer los servicios de la red, fue un paso inevitable.

5.1. PLAN DE NEGOCIOS DEL ISP

Si bien es cierto que el aspecto técnico es un elemento esencial para el buen funcionamiento de un proveedor de servicios de Internet, esto no es suficiente para asegurar el éxito de la empresa. Desde el punto de vista comercial se hace necesario realizar una adecuada planeación del negocio.

El objetivo del plan de negocios no es definir un plan de operaciones detallado que debe ser seguido minuciosamente. Un plan de negocios debe dar a conocer la viabilidad de la empresa mediante una investigación de mercado en las áreas en las que se desea operar e identificar sus riesgos. En un plan de negocios se debe realizar una descripción de los eventos de manera cronológica con el fin de indicar el progreso de la empresa. Obviamente, un plan de negocios no es un documento que debe ser realizado una sola vez, éste debe ser revisado periódicamente y debe reflejar el estado actual de la empresa.

El plan de negocios del ISP debe contener los resultado deseados para la empresa, es decir, un plan de negocios es una presunción de un futuro muy probable el cual debe maximizar las oportunidades de la empresa y minimizar los riesgos financieros.

A continuación se indicarán 5 pasos importantes para estructurar adecuadamente un sólido plan de negocios para un ISP.

PASO 1.- Identificar los objetivos

Identificar los objetivos del ISP es un aspecto muy importante ya que permitirá a la empresa construir un plan de negocios que pueda llevar a cabo tales objetivos. La identificación de objetivos del ISP debe reflejar las motivaciones por las que se desean ingresar al mercado.

PASO 2.- Dimensionar el mercado

Dimensionar el mercado es investigar el tamaño potencial del mercado dentro de las áreas que serán el objetivo de operación con el propósito de conocer los niveles actuales de demanda para el servicio. En este punto se estimará la proporción del mercado el cual probablemente será ganado por el ISP. Este dimensionamiento provee un punto de referencia de los niveles inmediatos de oportunidad de la empresa dentro del mercado compartido. El proceso debe además estimar el crecimiento de la demanda a lo largo de un período de tiempo examinado en el plan de negocios.

PASO 3.- Identificar los costos

El siguiente paso en un plan de negocios es identificar los costos. Este punto permitirá al ISP analizar en forma detallada todos los rubros que se deben cubrir para iniciar la empresa y aquellos que irán apareciendo conforme pase el tiempo. Una adecuada identificación de costos proporciona una idea del capital que se requerirá para implantar el negocio y luego mantenerlo dentro del mercado competitivo.

PASO 4.- Determinar una estructura de tarifación

La siguiente tarea dentro del proceso de planear el negocio es determinar una estructura de precios o tarifación, la cual debe asegurar el posicionamiento competitivo de los servicios del ISP dentro del mercado. En este punto se debe examinar la amplia diversidad de estrategias de tarifación que existen y escoger aquella que más se adapte al ISP y a su entorno.

PASO 5.- Desarrollar un plan de negocios completo

Una vez realizados los pasos 1, 2, 3 y 4 del plan de negocios, el ISP cuenta con suficiente material para desarrollar un plan de negocios completo. En este punto se deben traducir las proyecciones del número de clientes en requerimientos de recursos del ISP (puertos de módem, líneas de acceso, requerimientos de ancho de banda, equipo, etc) y posteriormente estas cifras deben ser traducidas a costos por año.

Por supuesto, en este punto del plan de negocios se debe incluir un modelo de ingresos en el cual se debe hacer constar cuál es la estructura de tarifación mediante la cual el ISP cobrará a sus clientes e indicar los ingresos por año que el ISP planea recibir.

Con estos dos puntos (costos e ingresos) desarrollados adecuadamente se debe proceder a determinar las posibles ganancias que el ISP percibirá y cuándo iniciará el proceso de empezar a recuperar el capital invertido.

NOTA.- Hasta el momento, en este proyecto de titulación se han desarrollado los pasos 1 y 2 del plan de negocios del ISP, en las secciones posteriores se analizarán con más detalle los siguientes pasos y se harán los cálculos correspondientes para el ISP del diseño.

5.2. IDENTIFICACIÓN DE LOS COSTOS DEL ISP

Para la operación de un ISP se pueden clasificar los costos en tres categorías:

costos de operación del servicio (costos operativos), costos de ventas y *marketing,* y costos administrativos.

Dentro de los ***costos de operación del servicio*** se incluyen los costos de propiedad de los equipos (servidores de aplicación, servidores de acceso de red, etc.), costos de los enlaces, costos por mantenimiento de equipos y costos por personal técnico.

El costo de los enlaces y comunicaciones incluye los costos de acceso *dial*, costo del enlace satelital, pago de las cuotas mensuales de dichos enlaces y costos de instalación.

Los costos operativos pueden ser clasificados en: costos eventuales y costos recurrentes. Los costos eventuales son aquellos que se realizan una sola vez al inicio de la empresa y aquellos que se dan de vez en cuando. Los costos recurrentes son costos fijos que se los realiza mensualmente como: pagos por enlaces, mantenimiento de equipos, sueldos, etc.

Los ***costos de marketing*** son aquellos que han sido dedicados a promocionar la empresa y sus servicios. En el Ecuador, los niveles de penetración de Internet son muy bajos (aunque con creciente demanda), por esta razón se requerirá de un adecuado *marketing* que sirva de estímulo a los posibles clientes.

La actividad de *marketing* para un ISP se ha convertido en un componente crítico para su plan de negocios. Para un ISP esta área ha llegado a ser una inversión obligatoria ya que es el medio mediante el cual el proveedor se abastece de nuevos clientes dando a conocer los beneficios de los servicios que éste ofrece.

Dentro de los ***costos administrativos*** o ***costos fijos*** se encuentran los costos de soporte del personal administrativo, arriendo del local, luz y gastos extras. Estos costos normalmente son una proporción constante de todos los costos del ISP y pueden ser estimados con suficiente exactitud.

5.2.1. COSTOS REFERENCIALES DE LOS EQUIPOS Y ENLACES QUE CONFORMAN EL ISP

Los precios referenciales que se muestran a continuación son precios vigentes en el mercado, obtenidos de empresas serias con puntos de distribución en la ciudad de Quito. Estos precios pueden variar dependiendo de la marca de los equipos o de la empresa donde se los adquiera, por lo tanto, la inversión inicial puede verse modificada considerablemente.

Las listas de precios que se detallan a continuación reflejará la inversión inicial que debe realizar el ISP durante el primer año en lo que respecta a equipos, para los siguientes años se deberá ir adquiriendo nuevos equipos o en su defecto comprar tarjetas de red, memorias, procesadores, discos duros, etc, para ir incorporándolas en los equipos y así ofrecer una buena calidad de servicio y satisfacer la demanda de los usuarios.

Costos referenciales de los equipos [a]

ITEM	DESCRIPCIÓN	PRECIO UNIT.	CANT.	PRECIO TOT.
1	*Router* equipado con: 2 puertos 10/100 Base TX. 240 módems analógicos y 8 E1/PRI canalizado Cable octal de 8 E1 con conectores RJ-45 hembra Soporte de acceso VPN Señalización R2 soportada	$ 73.670,00	1	$ 73.670,00
SUBTOTAL				**$ 73.670,00**

Tabla 5.1. Servidor de Acceso de Red (NAS)

[a] Ninguno de estos precios incluye IVA.

ITEM	DESCRIPCIÓN	PRECIO UNIT.	CANT.	PRECIO TOT.
1	*Router* equipado con: 2 puertos 10/100 Base TX. 1 módulo Ethernet de dos puertos y ranura de dos tarjetas WAN 1 módulo de red serie asincrónico/ sincrónico de ocho puertos 1 tarjetas de interfaz WAN serie con dos puertos Diez Cables V.35MT de tres metros	$ 17.900,00	1	$ 17.900,00
SUBTOTAL				**$ 17.900,00**

Tabla 5.2. Router Corporativo

ITEM	DESCRIPCIÓN	PRECIO UNIT.	CANT.	PRECIO TOT.
1	*Router* equipado con: 2 puertos 10/100 Base TX. 1 módulo Ethernet de dos puertos y ranura de dos tarjetas WAN 2 tarjetas de interfaz WAN serie con dos puertos Cuatro Cables V.35MT de tres metros	$ 14.300,00	1	$ 14.300,00
SUBTOTAL				**$ 14.300,00**

Tabla 5.3. Ruteador principal

ITEM	DESCRIPCIÓN	PRECIO UNIT.	CANT.	PRECIO TOT.
1	Servidor equipado con. RAM: 128 MB Procesador: 350 MHz Disco: 150 MB de memoria de disco libre	**$ 5.597,00**	1	**$ 5.597,00**
SUBTOTAL				**$ 5.597,00**

Tabla 5.4. Servidor Radius

ITEM	DESCRIPCIÓN	PRECIO UNIT.	CANT.	PRECIO TOT.
1	Servidores equipados con: SRAM: 1280 MB Procesador: 1 GHz Unidad de CD-ROM 48X interno Disco: 36,4 GB Ultra SCSI 10.000 rpm expandible hasta 6DD internos hot swap con capacidad hasta 145,6GB Interfaz de red Fast Ethernet 10/100 Mbps Dos fuentes de poder redundantes Teclado, mouse Monitor a color 15" de alta resolución Sistema operativo con soporte Garantía: 3 años de soporte en partes más soporte técnico	$ 6.917,12	2	**$ 13.834,24**
SUBTOTAL				**$ 13.834,24**

Tabla 5.5. Servidores de aplicación

ITEM	DESCRIPCIÓN	PRECIO UNIT	CANT	PRECIO TOT.
1	Servidor equipado con: SRAM: 128 MB Procesador: 1 GHz Unidad de CD-ROM 48X interno Disco Duro de 40 GB Tarjeta de red 10/100 Mbps Módem 56K ITU V.90 Teclado, mouse Monitor a color 15" de alta resolución Garantía: 3 años de soporte en partes	$ 1.396,64	1	$ 1.396,64
2	Impresora Lexmark Z52	$ 161,00	1	$ 161,00
3	Regulador Magom 1000 con protector de Fax módem	$ 28,00	1	$ 28,00
SUBTOTAL				**$ 1.585,64**

Tabla 5.6. Servidor de Administración

ITEM	DESCRIPCIÓN	PRECIO UNIT	CANT	PRECIO TOT.
1	1 Content Engine 560 Software Caché	$ 12.400,00	1	$ 12.400,00
SUBTOTAL				**$ 12.400,00**

Tabla 5.7. Servidor Caché WWW

ITEM	DESCRIPCIÓN	PRECIO UNIT	CANT	PRECIO TOT.
1	Servidor equipado con: RAM: 128 MB expandible a 4GB hasta 2 procesadores Intel PIII 1 GHz Disco: SCSI de 36 GB 2 bahías hot swap Tarjeta de red 10/100 Mbps CD-ROM 48X	$ 3.500,00	1	$ 3.500,00
SUBTOTAL				**$ 3.500,00**

Tabla 5.8. Servidor de tarifación y facturación

ITEM	DESCRIPCIÓN	PRECIO UNIT	CANT	PRECIO TOT.
1	*Switch* equipado con: 16 puertos 10/100 Base TX. Desempeño en capa tres.	$ 6.495,00	1	$ 6.495,00
2	*Rack* Mount Kit	$ 250,00	1	$ 250,00
SUBTOTAL				**$ 6.745,00**

Tabla 5.9. Switch

ITEM	DESCRIPCIÓN	PRECIO UNIT	CANT	PRECIO TOT.
1	*Firewall* equipado con: Software restringido 4 puertos 10/100 Base TX Licencia para encriptación de 56 bits DES Ipsec	$ 14.000,00	1	$ 14.000,00
SUBTOTAL				**$ 14.000,00**

Tabla 5.10. Firewall

ITEM	DESCRIPCIÓN	PRECIO UNIT	CANT	PRECIO TOT.
1	UPS con banco de baterías de 1 hora de soporte	$ 2.500,00	1	$ 2.500,00
SUBTOTAL				**$ 2.500,00**

Tabla 5.11. UPS

ITEM	DESCRIPCIÓN	PRECIO UNIT	CANT	PRECIO TOT.
1	*Rack* 48"	$ 107,00	1	$ 107,00
2	Organizador doble	$ 15,00	4	$ 60,00
3	Organizador vertical	$ 38,00	2	$ 72,00
4	Bandeja 2 posiciones	$ 14,00	5	$ 70,00
5	Soporte de pared	$ 30,00	1	$ 30,00
SUBTOTAL				**$ 343,00**

Tabla 5.12. Implementos Adicionales

ITEM	DESCRIPCIÓN	PRECIO UNIT	CANT	PRECIO TOT.
1	9,1 GB pluggable ultra3 SCSI 10000 rpm universal	$ 386,40	1	$ 386,40
2	18,2 GB pluggable ultra3 SCSI 10000 rpm universal	$ 514,08	1	$ 514,08
3	512 MB Reg SDRAM DIMM 133	$ 571,20	1	$ 571,20
4	Pentium III 1 GHz Processor Option Kit	$ 927,36	1	$ 927,36
5	Monitor de 15"	$ 207,20	1	$ 207,20
6	NM-1HSSI	$ 5.000,00	1	$ 5.000,00
SUBTOTAL				**$ 7.606,24**

Tabla 5.13. Opciones

Resumen de los costos referenciales de los equipos

ITEM	DESCRIPCIÓN	PRECIO UNIT	CANT	PRECIO TOT.
1	*Switch*	$ 6.745,00	1	$ 6.745,00
2	*Router* corporativo	$ 17.900,00	1	$ 17.900,00
3	*Router* principal	$ 14.300,00	1	$ 14.300,00
4	*Access Server* (NAS)	$ 73.670,00	1	$ 73.670,00
5	Servidor caché WWW	$ 12.400,00	1	$ 12.400,00
6	Servidor Radius	$ 5.597,00	1	$ 5.597,00
7	Servidores	$ 6.917,12	2	$ 13.834,24
8	Servidor de tarifación y facturación	$ 3.500,00	1	$ 3.500,00
9	Servidor de administración	$ 1.585,64	1	$ 1.585,64
10	*Firewall*	$ 14.000,00	1	$ 14.000,00
11	UPS	$ 2.500,00	1	$ 2.500,00
12	*Rack* de 48"	$ 343,00	1	$ 343,00
TOTAL (USD)				**$ 166.374,88**

Tabla 5.14. Resumen de costos de equipos

Costos referenciales de los enlaces

Los costos de los enlaces satelitales y los enlaces con el (los) *carrier*(s) que proporcionan conectividad de última milla (Suratel, Integraldata, Andinatel, Teleholding, etc.) varían dependiendo de la capacidad del enlace requerido. Los costos que se indican en las siguientes tablas son los costos vigentes en el mercado para diferentes capacidades.

A continuación se listan los costos referenciales de los enlaces satelitales y los costos de los enlaces de última milla para tres diferentes tecnologías de acceso: TDM, *Clear Channel* y *Frame Relay*. Estos costos no incluyen impuestos.

Enlace Satelital

DESCRIPCION	Velocidad	Instalación	Costo
	Kbps	USD	USD/mes
Servicio de acceso dedicado a Internet	1024	3500	18400
	2048	3500	22900

Tabla 5.15. Costos referenciales del enlace satelital [a]

TDM

	TIPO DE ENLACE					
	NACIONAL				INTERNACIONAL	
Velocidad	Local	Provincial	Regional	Nacional	Colombia	Otros
Kbps	USD				USD	
9,6	76	160	320	380		
19,2	92	192	388	456		
32,0	120	256	494	608		
64,0	148	320	614	760	2.500	4.100
128,0	236	512	988	1.216	4.000	6.560
256,0	440	960	1.834	2.280	7.500	12.300
384,0	592	1.280	2.430	3.040	10.000	16.400
512,0	739	1.600	3.028	3.800	12.500	19.400
1.024,0	888	1.920	3.640	4.560	15.000	25.000
2.048,0	1.600	3.424	6.460	8.160	26.750	40.000
Instalación	250	400	400	500	1500	1500

Tabla 5.16. Costos refrenciales de TDM [b]

[a] Datos proporcionados por Grupo Bravco.
[b] Datos proporcionados por Impsat

Frame Relay

	VELOCIDAD	Bc	CIR	Be	INSTALACION	COSTO
QOS	Kbps	Kb	Kbps	Kb	USD	USD
PREMIUM	256	256	256	0	1400	800
	256	128	128	128	1400	750
	256	256	128	64	1400	720
	256	128	64	128	1400	680
BASICO	256	256	256	0	1200	710
	256	128	128	128	1200	670
	256	256	128	64	1200	650
	256	256	128	32	800	600
PREMIUM	192	192	192	0	600	700
	192	192	96	192	600	680
	192	96	96	96	600	650
	192	192	96	48	600	600
BASICO	192	192	192	0	500	550
	192	96	96	96	500	520
	192	192	96	48	500	490
	192	192	96	32	400	450
PREMIUM	128	128	128	0	450	550
	128	128	64	128	450	530
	128	64	64	64	450	520
	128	128	64	32	450	500
CIRCUITO	128	128	128	0	400	370
	128	64	64	64	400	350
	128	128	64	32	400	300
	128	128	64	16	300	255
CIRCUITO	64	64	64	0	300	270
	64	32	32	32	300	265
	64	64	32	16	300	250
	64	64	32	8	200	210
CIRCUITO	32	32	32	0	300	245
	32	16	16	16	300	240
	32	32	16	8	300	230
	32	32	16	4	200	200
CIRCUITO	19,2	19,2	19,2	0	300	210
	19,2	9,6	9,6	9,6	300	205
	19,2	19,2	9,6	4	300	190
	19,2	19,2	9,6	0	200	185

Tabla 5.17. Costos referenciales de Frame Relay [a]

[a] Datos proporcionados por Suratel.

Clear Channel

	QOS: PREMIUM		QOS: BASICO	
Velocidad	Instalación	Costo	Instalación	Costo
Kbps	USD	USD	USD	USD
19,2	500	350	350	250
32	600	350	400	300
64	600	600	400	320
128	600	650	400	400
192	800	700	600	500
256	800	800	600	600
384	800	900	600	700
512	2.000	1000	1000	750
1.024	3.000	1300	1500	1000

Tabla 5.18. Costos referenciales de Clear Channel [a]

Costos referenciales del software

Los costos del *software* que se utilizará en cada uno de los servidores del ISP, se indican a continuación en la tabla 5.19. Estos costos han sido obtenidos de varias referencias electrónicas actualizadas.

SOFTWARE			
	Software	Plataforma	Precio (USD)
E-mail	*Sendmail*	Linux	Gratuito
Web	Apache	Linux	Gratuito
FTP	*War* FTP *Daemon*	*Windows 2000*	Gratuito
DNS	BIND	Linux	Gratuito
Autenticación	*Steel Belted* RADIUS	*Windows 2000*	3112
Tarifac. Y Facturac.		*Windows 2000*	18000[b]
Administración	Cisco *Works* 2000	*Windows 2000*	2000
Firewall	*Watchguard* FB-II		2600
Software Antivirus			400
Windows 2000			973
COSTO TOTAL DEL *SOFTWARE* (USD)			27085

Tabla 5.19. Costos referenciales del software

[a] Datos proporcionados por Impsat.

5.2.2. PERFIL DE COSTOS DEL ISP

La clasificación de costos que se han visto hasta el momento resume la naturaleza de los costos del ISP dentro de la estructura de un plan de negocios. El balance de éstos variará para ciertos perfiles de ISPs y para varias áreas alrededor del mundo. De esta manera, se tiene que para un ISP dentro de Norte América los costos de los enlaces (enlace al ISP *upstream* y costos de las líneas arredadas) no dominan el plan de negocios; en su lugar, los costos de *marketing* y ventas tienen un papel significativo dentro del perfil de negocios global.

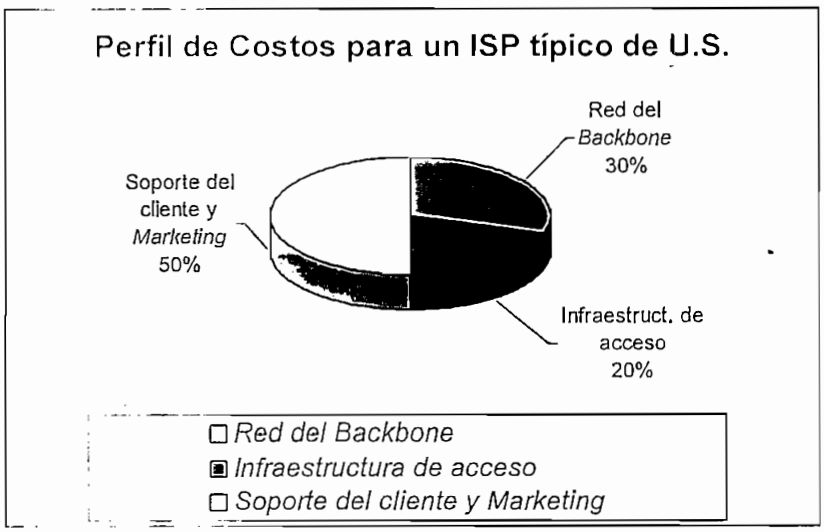


Fig. 5.1. Perfil de costos para un ISP en U.S[1].

Este perfil de costos varía para un ISP que no está dentro del área geográfica de los Estados Unidos. Para este caso es muy común que los costos de los enlaces superen el 60%[1] del gasto total del proveedor, dependiendo por supuesto de la localización del proveedor y de las tarifas de los *carriers* dentro de la región del ISP.

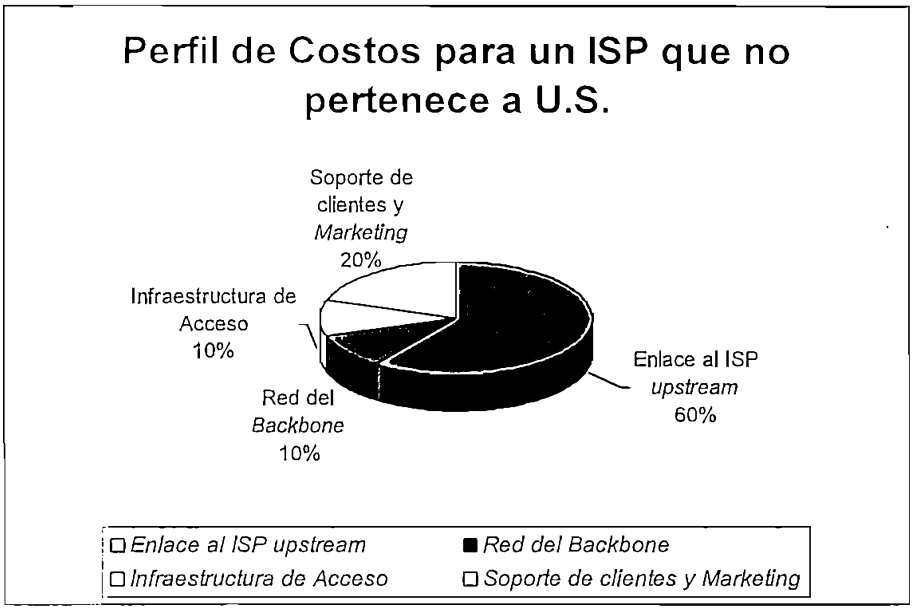


Fig. 5.2. Perfil de costos para un ISP fuera del área de los U.S[1].

Para el ISP de diseño, el costo por enlaces corresponde al 38%, lo cual confirma que éste es el rubro que más impacto causa dentro de la economía de un ISP que no pertenece a los Estados Unidos. El costo por equipos es también un gasto importante (24%) que se lo realiza una sola vez al inicio del funcionamiento del proveedor. Se requiere además adecuado mantenimiento, personal especializado y otros rubros administrativos (arriendo, luz, etc.) lo cual significa aproximadamente un 18% del costo total. El *marketing* también es un rubro muy importante ya que gran parte de la acogida que tiene un ISP dentro del mercado de Internet, depende de cuan buena sea la publicidad del mismo. Un ISP puede destinar el 20% de sus costos totales para tal objetivo[a]. Ver figura 5.3.

[a] Referirse a la tabla 5.32 de este capítulo.

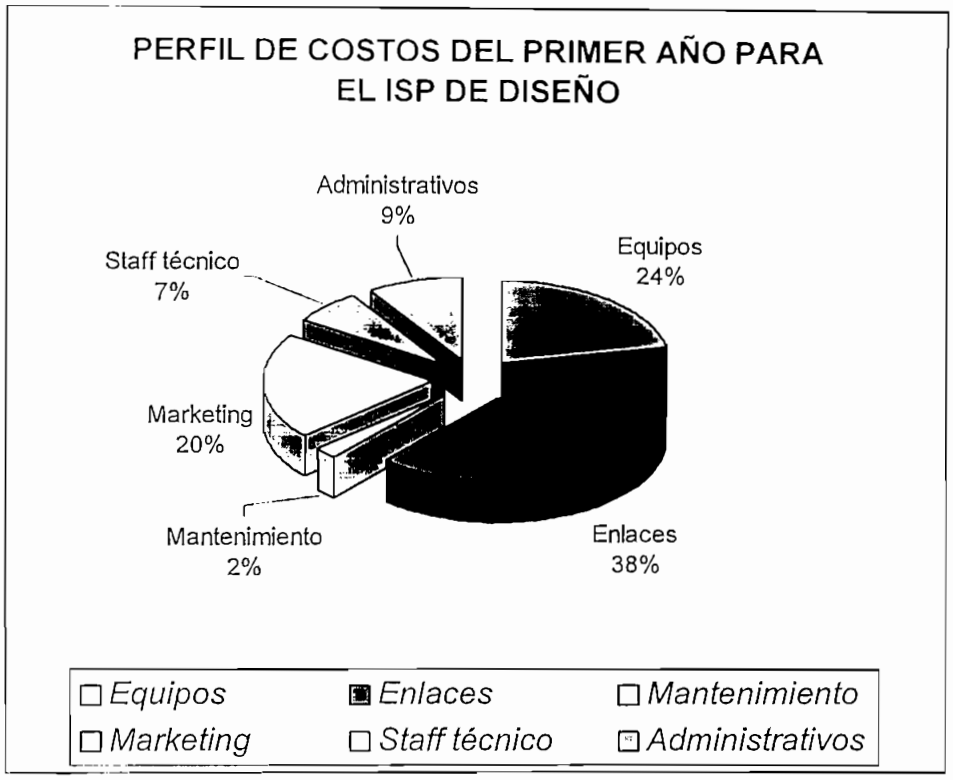


Fig. 5.3. Distribución de costos durante el primer año de funcionamiento del ISP

5.3. ESTRUCTURAS Y MODELOS DE CÁLCULO DE TARIFAS

Tarifar es poner precio a un determinado servicio basándose en diferentes aspectos con fines de comercialización. Existe una variedad de estructuras de tarifación las cuales incluyen cobros por hora, cobros por velocidad fija, cobros basados en volumen y muchas otras formas que permiten tarifar el servicio. Por supuesto, la principal característica dentro de un mercado de consumo es la competitividad del servicio, lo cual debe verse reflejado en la estructura de tarifación del ISP.

5.3.1. PARÁMETROS QUE INTERVIENEN EN LA TARIFACIÓN

Para un ISP, existen cinco aspectos principales para llevar a cabo la tarifación de los clientes, éstos son: ancho de banda adquirido (acceso), duración del acceso

(tiempo), cantidad de datos transmitidos (volumen), distancia y calidad del servicio (QoS). Casi cualquier estructura de tarifación de acceso puede ser expresada como una combinación que involucre algunos o todos estos parámetros.

5.3.1.1. Acceso

La habilidad para acceder a Internet está restringida por los aspectos técnicos del acceso. La principal métrica de los circuitos de acceso es el ancho de banda. El ancho de banda de acceso indica la velocidad pico del flujo de datos que el cliente puede pasar dentro de la red así como el máximo volumen de datos que se puede pasar a y desde la red del ISP en cualquier período de tiempo.

La tarifación basada en acceso, si es utilizada por el ISP como el único parámetro para conexiones permanentes, resulta en una estructura de tarifa plana, es decir, el cliente paga mensualmente la misma tarifa independientemente del tiempo de conexión o volumen de datos.

Desde la perspectiva del cliente, la ventaja de tal estructura de tarifación es que el cliente corporativo puede disfrutar del servicio e incluir este costo fijo dentro de su presupuesto de gastos. Además, el cliente corporativo puede extender el acceso a Internet a lo largo de su red corporativa sin ningún requerimiento externo que imponga control en el acceso. De esta manera, el cliente corporativo tendrá siempre una conexión permanente dedicada lo cual le permitirá albergar plataformas de servicio de Internet dentro de su empresa para extender su alcance y por lo tanto su actividad de negocios dentro del Internet sin incurrir en cobros imprevisibles por el servicio. Para un cliente corporativo tales atributos de la tarifación por acceso constituyen un incentivo muy poderoso.

Considerando las ventajas de la estructura de tarifación basada en acceso y tarifa plana, es éste el modelo de tarifación más ampliamente utilizado en la industria del ISP para clientes corporativos.

Desde el punto de vista del proveedor, existen algunas debilidades dentro de este modelo de tarifación lo cual representa una desventaja para el ISP, ya que si los clientes incrementan considerablemente su volumen de datos, el proveedor deberá transportar más datos al mismo precio y con el riesgo de ocasionar un incremento en los niveles de congestión.

La desventaja de la tarifa plana es que no provee ningún control para el uso racional y cuidadoso de los recursos de la red del ISP pudiéndose dar un exceso de uso del servicio y la consecuente saturación de los puertos en el caso del acceso *dial-up.* La ventaja en cambio es que en una estructura de tarifa plana, el cliente paga por adelantado lo cual reduce el riesgo de pérdidas del ISP.

5.3.1.2. Tiempo

Existen dos dimensiones para la estructura de tarifación por tiempo: la primera consiste en una estructura de tarifación para clientes conectados permanentemente basada en la hora del día en la que usan el servicio (horas pico u horas bajas), y la segunda para clientes *dial-up* dependiendo de la hora del día y duración del acceso. La primera estructura es aplicable cuando se considera tarifación por volumen y será vista en la sección 5.3.1.3., el servicio de acceso dial será examinado a continuación.

La tarifación basada en la duración del acceso (o tiempo consumido) y la hora del día del acceso es un método ampliamente utilizado por los ISPs para la facturación de usuarios *dial-up.* La forma en que se cobra al cliente es por hora, en cada acceso se contabiliza el tiempo de consumo y al final de cada período de facturación se calcula el tiempo total de acceso. Tarifar basándose en la hora del día del acceso ocasiona que el cliente incremente el número de horas de conexión durante el período de tiempo considerado como bajo lo cual se ve reflejado como un incremento de ingresos para el ISP.

La desventaja de utilizar esta estructura de tarifación pura es que los clientes pueden buscar otros ISPs a fin de optimizar sus costos en un mercado altamente competitivo como lo es Internet. Para evitar esto, un proveedor de Internet debe combinar este método con una tarifa plana; es decir, un cliente *dial-up* pagará una cuota mensual por un determinado número de horas y tendrá que pagar cargos adicionales por horas extras de conexión o conexiones fuera del horario establecido.

5.3.1.3. Volumen

El riesgo de implementar una estructura de tarifa fija, como se vio anteriormente, es que el ISP puede ver incrementados sus niveles de tráfico sin que esto implique el incremento de sus ingresos. El consecuente dilema para el ISP es si éste debe mantener su capacidad y sufrir el incremento de los niveles de congestión y la consecuente caída de la calidad de servicio o aumentar su capacidad y sufrir un decremento en sus ganancias debido al incremento de gastos sin recibir ingresos a cambio.

En tal situación, una alternativa es utilizar un estructura de tarifación en la cual si los clientes aumentan su volumen de tráfico, el ISP incrementa sus ingresos. De esta forma, el ISP puede aumentar su capacidad de red y consecuentemente mantener sus niveles de calidad de servicio.

Si la tarifación se realiza en base al volumen de tráfico que pasa a través de la red del ISP, esto no incentiva a los proveedores de contenido (que envían información a través de la red del ISP cuando un cliente lo solicita), ya que ellos estarían pagando por transportar información hacia el receptor. Además, el proveedor de contenido estaría pagando al ISP por transportar sus datos a través de su red independientemente de si estos datos son entregados o no al cliente que los solicitó, por tal razón, los paquetes descartados dentro de la red del ISP no deben generar ingresos al proveedor de servicios. La alternativa ante este problema es facturar al cliente en base a la cantidad de tráfico que éste recibe *más no a la*

cantidad de tráfico que envía ya que gran parte de la información que pasa por la red del ISP es generada como resultado de un requerimiento del receptor que es quien está utilizando aplicaciones tales como: *Web*, *downloads* ftp, recepciones de audio y vídeo, etc.

Generalmente, la tarifación por volumen es combinada con la hora del día en la que se realiza la recepción de datos, es decir un cliente pagará menos cuando reciba grandes volúmenes de información en horas que no sean las horas pico, de esta manera el ISP logra equilibrar el tráfico a lo largo del día.

5.3.1.4. Distancia

Este método ha sido ampliamente difundido por las empresas telefónicas donde el costo de una llamada está relacionado con la distancia entre las dos partes, la duración de la misma y la hora del día en que se la realiza. Tal estructura de tarifación ya ha penetrado en el Internet pero no es muy utilizada.

La desventaja de este método de tarifación es que los cambios en los estados de enrutamiento de la red pueden redireccionar el tráfico a través de caminos más largos para llegar a su destino incrementando la distancia recorrida y perjudicando al cliente. Lo contrario sucede con la red telefónica, aquí los usuarios están concientes que la distancia existente entre dos puntos siempre será la misma.

La ventaja es que con este método se introduce el uso de las tarifas diferenciadas entre tráfico local e internacional. Por ejemplo, el tráfico entregado a un cliente desde un servidor *Web Caching* local tendrá una tarifa más baja, de esta manera el cliente se ve incentivado a generar tráfico local utilizando el caché local en lugar de generar tráfico internacional mediante el uso de sitios *Web* dispersos en el mundo y de este modo pagar menos. El ISP también disminuirá los costos que implica el enlace satelital.

5.3.1.5. Calidad de Servicio

Con este tipo de tarifación, el ISP deberá ofrecer a sus clientes una amplia variedad de calidad de servicio QoS utilizando tarifas diferenciadas dependiendo de la calidad de servicio que el cliente desea recibir. Un ISP puede brindar QoS a un cliente marcando todos sus paquetes con una indicación de prioridad elevada, media o normal y tarifar de acuerdo a dicha prioridad.

5.3.2. PRIMER MODELO DE CÁLCULO DE TARIFAS BASADO EN TIEMPO

Un ISP debe ser capaz de soportar un período de pérdida durante los primeros meses e inclusive durante los primeros años después de haber iniciado su operación. Esto se debe a que durante el primer año, el ISP adquiere los equipos y enlaces necesarios para la red siendo éste un costo muy significativo tomando en cuenta que todavía no ha adquirido suficientes clientes para equilibrar tales gastos.

Para la mayoría de ISPs existen dos principales categorías de servicio que necesitan ser tarifadas y a partir de las cuales se espera recuperar el capital invertido, éstas son: servicio de acceso *dial-up* y servicio de acceso corporativo. Un proveedor de servicios de Internet debe introducirse en el mercado con precios competitivos y que a la vez le permitan recuperar la inversión manteniendo el equilibrio entre gastos y ganancias.

Los cálculos de costos que se realizarán a continuación serán utilizados posteriormente en el cálculo de las tarifas. Estos costos serán obtenidos para cuatro años de funcionamiento del ISP con el objetivo de determinar el tiempo requerido para recuperar el capital invertido. Los costos de mantenimiento anuales serán calculados como el 10%[1] del costo de adquisición del equipo.

5.3.2.1. Cálculo de los costos anuales para usuarios *dial-up* y corporativos

Para calcular el costo por año que representa al ISP mantener a los usuarios *dial-up* (USD/año), se debe tener en cuenta que existen equipos y enlaces exclusivos de los usuarios *dial-up* cuyos costos (costos parciales) no tienen que ser compartidos con los usuarios corporativos, éstos son: NAS y enlaces E1s de Andinatel. En la tabla 5.20 se indican dichos costos:

COSTOS PARCIALES (*DIAL-UP*) (USD)					
Costos	ITEMS	AÑO 1	AÑO 2[a]	AÑO 3	AÑO 4
Eventuales	NAS [b]	82510	43100	73670	43000
	Instalación E1s[c]	1500			
Recurrentes	E1s [d]	32000	84960	127008	162130
Subtotal (USD/año)		**116010**	**128060**	**200678**	**205130**

Tabla 5.20. Costos parciales anuales por usuarios dial-up

También existen equipos y enlaces exclusivos de los usuarios corporativos cuyos costos no tienen que ser compartidos con los usuarios *dial-up*, éstos son: *router* corporativo y enlaces *Frame Relay*. En la tabla 5.21 se indican dichos costos:

COSTOS PARCIALES (CORPORATIVOS)					
Costos	ITEMS	AÑO 1	AÑO 2	AÑO 3	AÑO 4
Eventuales	*Router* corp	20048	1600		3600
	Instalación FR	2500			
Recurrentes	FR [e]	21184	30586	36191	40316
Subtotal (USD/año)		**43732**	**32186**	**36191**	**43916**

Tabla 5.21. Costos parciales anuales por usuarios corporativos

Los usuarios deberán pagar el 10% [1] del costo total de sus equipos por concepto de mantenimiento.

---

[a] Referirse a la tabla C-1 para los costos de los equipos adicionales a partir del año 2.
[b] Se incluye el 12% del IVA a los costos de los equipos presentados en la tabla 5.14.
[c] Dato proporcionado por el personal técnico de Andinanet.
[d] Referirse a las tablas C-2 a C-5 del Anexo C.
[e] Referirse a las tablas C-6 a C-9 del Anexo C.

COSTOS POR MANTENIMIENTO (Equipos exclusivos)				
	AÑO 1	AÑO 2	AÑO 3	AÑO 4
Costo NAS (*dial-up*)	82510	43100	73670	43000
% Mantenimiento anual	10	10	10	10
Costo por mant. NAS (USD/año)	**8251**	**12561**	**19928**	**24228**
Costo *router* (corporativo)	20048	1600	0	3600
% Mantenimiento anual	10	10	10	10
Costo por mant. *router* corp. (USD/año)	**2005**	**2165**	**2165**	**2525**

Tabla 5.22. Mantenimiento anual por equipos exclusivos para usuarios dial-up y corporativos

Existen elementos cuyo uso y costos deben ser compartidos con los clientes corporativos, éstos son: servidores, *router* principal, *firewall*, *switch*, UPS, *rack*, *software*, ancho de banda satelital, enlaces al NAP, etc. A continuación se indican los costos globales (o compartidos) detallados anualmente.

COSTOS GLOBALES DE EQUIPOS (*DIAL-UP* + CORPORATIVOS) (USD)					
Costos	ITEMS	AÑO 1	AÑO 2	AÑO 3	AÑO 4
Costos Eventuales	Servidores	41347	738	1197	1197
	Router Principal	16016	4100	4100	3600
	Firewall	15680			
	Switch	7554			
	UPS	2800			
	Rack de 48"	384			
	Software[a]	27085			
	Discos duros de respaldo	1197	738	1197	1197
	Instalación de enlaces(Satelit+NAP)	7000			
Costos Recurrentes	AB Satelital	271800	385020	435780	458460
	AB al NAP	14800	18904	21571	23512
Costo Global Total (USD/año)		**405663**	**409500**	**463845**	**487966**

Tabla 5.23. Costos globales

Tomando en cuenta que no se puede repartir equitativamente los costo anuales por equipos y enlaces compartidos entre clientes corporativos y *dial-up*, es necesario calcular una relación la cual indique la relación de costos entre dichos usuarios.

Esta relación es el coeficiente que existe entre el ancho de banda satelital ocupado por los clientes corporativos y el ancho de banda satelital ocupado por

[a] Referirse a la tabla 5.19

los usuarios *dial-up* como se indica en la tabla 5.24, ya que los costos se repartirán también de la misma manera.

AB = 0.7*#*dial-up* + 40*#corp.	AÑO 1	AÑO 2	AÑO 3	AÑO 4
# Usuarios *dial-up*	2089	4474	6859	9244
# Usuarios corporativos	120	190	250	300
AB satelital Total (Kbps)	6262,3	10731,8	14801,3	18470,8
AB satelital para *dial-up* (Kbps)	1462,3	3131,8	4801,3	6470,8
AB satelital para corp. (Kbps)	4800	7600	10000	12000
RELACIÓN	3,28	2,43	2,08	1,85

Tabla 5.24. Relación de costos usuarios corporativos/usuarios dial-up

Con estas relaciones anuales se procede a distribuir los costos globales anuales entre usuarios corporativos y usuarios *dial-up* como se indica a continuación:

Costo Global *Dial-up* (USD/año)	94726	119502	150464	170947
Costo Global Corp. (USD/año)	310937	289998	313381	317019

Tabla 5.25. Distribución de costos globales entre usuarios dial-up y corporativos

El costo por mantenimiento será obtenido como el 10% del costo de adquisición del equipo más el costo por mantenimiento del equipo en el año (s) anterior (es). El costo por mantenimiento del *software* indica el porcentaje que se pagará a la empresa distribuidora de dichos programas con el objeto de mantenerlo actualizado y en óptimas condiciones. Los gastos por mantenimiento también serán distribuidos en base a la misma relación de costos de la tabla 5.24.

COSTOS POR MANTENIMIENTO (Elementos compartidos)				
	AÑO 1	AÑO 2	AÑO 3	AÑO 4
Costo equipos (costos globales)	84978	5576	6494	5994
Mantenimiento anual de los equipos compartidos	10%	10%	10%	10%
Costo total por mantenimiento equipos	8498	9055	9705	10304
Costo por mant. equipos *dial-up* (USD/año)	**1984**	**2643**	**3148**	**3610**
Costo por mant. equipos corpor. (USD/año)	**6514**	**6413**	**6557**	**6694**
Costo *software*	27085			
Mantenimiento anual *software* [a]	10%	10%	10%	10%
Costo total por mantenimiento *software*	2708	2708	2708	2708
Costo por mant. *software dial-up* (USD/año)	**632**	**790**	**879**	**949**
Costo por mant. *software* corpor. (USD/año)	**2076**	**1918**	**1830**	**1760**

Tabla 5.26. Distribución de costos por mantenimiento entre usuarios dial-up y corporativos

[a] Valor recomendado por el personal técnico de Impsat

Dentro de los costos que se deben tener en cuenta para el cálculo de tarifas también se incluyen los costos por *marketing* y por sueldos del *staff* técnico. La distribución de estos costos se las hace equitativamente ya que éstos son independientes del tipo de usuarios.

COSTOS POR *MARKETING*				
	AÑO 1	AÑO 2	AÑO 3	AÑO 4
Costo Mensual [a]	15000	12000	10000	10000
Costo Annual	180000	144000	120000	120000
Marketing dial-up (USD/año)	**90000**	**72000**	**60000**	**60000**
Marketing corpor. (USD/año)	**90000**	**72000**	**60000**	**60000**

Tabla 5.27. Distribución de costos por marketing entre usuarios dial-up y corporativos

COSTOS POR PERSONAL TÉCNICO				
	AÑO 1	AÑO 2	AÑO 3	AÑO 4
Personal técnico	5	10	15	20
Aumento de sueldos [3]		10%	10%	10%
Sueldo mensual (USD)	1000	1100	1210	1331
Costo anual por sueldos (USD)	60000	132000	217800	319440
Costo para usuarios *dial-up* (USD/año)	**30000**	**66000**	**108900**	**159720**
Costo para usuarios corpor. (USD/año)	**30000**	**66000**	**108900**	**159720**

Tabla 5.28. Distribución de costos por sueldo del personal técnico entre usuarios dial-up y corporativos

5.3.2.2. Cálculo de las tarifas basadas en tiempo

Como se mencionó en la sección 5.2, en un ISP se distinguen tres tipos de costos: operativos, de *marketing* y administrativos. Los costos operativos son el resultado de la suma de los costos de propiedad de los equipos, enlaces, mantenimiento y personal técnico. Los costos de *marketing* son los mismos de la tabla 5.27 y los costos administrativos constituyen el 10%[b] de los costos operativos y de *marketing*. Las tablas 5.29 y 5.30 que se presentan a continuación, resumen los costos para clientes *dial-up* y corporativos respectivamente, costos por usuario por mes y el costo promedio.

[a] Valor recomendado por el departamento de ventas y *marketing* de Impsat.
[b] Valor recomendado por el departamento administrativo de Impsat.

RESUMEN COSTOS PARA USUARIOS *DIAL-UP*				
	AÑO 1	AÑO 2	AÑO 3	AÑO 4
Costos operativos	251604	329556	483997	564583
Costos *Marketing*	90000	72000	60000	60000
Costos administrativos	41343	43612	53651	60811
COSTO TOTAL (USD)	382947	445168	597648	685394
# Usuarios	2089	4474	6859	9244
Costo/usuario/mes	15	8	7	6
Costo Promedio (USD)	9,25			

Tabla 5.29. Resumen de costos y costo promedio para usuarios dial-up

RESUMEN COSTOS PARA USUARIOS CORPORATIVO				
	AÑO 1	AÑO 2	AÑO 3	AÑO 4
Costos operativos	395264	398679	469024	531634
Costos *Marketing*	90000	72000	60000	60000
Costos administrativos	41343	43612	53651	60811
COSTO TOTAL (USD)	526607	514291	582675	652445
# Usuarios	120	190	250	300
Costo/usuario/mes	366	226	194	181
Costo promedio (USD)	241.68			

Tabla 5.30. Resumen de costos y costo promedio para usuarios corporativos

De esta manera se obtiene lo que cuesta a un ISP mantener mensualmente a un usuario *dial-up* y a un corporativo. Con el objetivo de ofrecer precios competitivos y obtener ganancias, las tarifas para estos dos tipos de clientes serán calculadas de la siguiente manera:

$$\text{Tarifa} = \text{Costo promedio} + \%\ \text{Rentabilidad} * \text{Costo promedio}$$

TARIFAS	
% Rentabilidad *dial-up* [a]	20%
% Rentabilidad corporativos	15%
***Dial-up* (USD/mes)**	**11**
Corporativos (USD/mes)	**278**

Tabla 5.31. Tarifas basadas en tiempo

El ISP de diseño ofrecerá un único plan de acceso a Internet con tarifa plana y acceso ilimitado, para lo cual cobrará a sus usuarios *dial-up* 11 USD/mes y 278 USD/mes para usuarios corporativos por un acceso de 64 Kbps.

[a] Porcentajes de rentabilidad recomendados por el personal técnico de Impsat

5.3.2.3. Análisis Beneficio/Costo

Para estimar a partir de cuando se espera que el ISP empiece a obtener ganancias tarifando a sus clientes con el modelo de tarifa plana basada en tiempo se debe realizar un análisis beneficio/costo. Cuando este valor es mayor que la unidad, significa que las ganancias son mayores a los costos, es entonces cuando el ISP empieza a recuperar el capital invertido.

A continuación se indican dos tablas, en la primera constan los egresos por año que se prevé va a realizar el ISP. En la segunda tabla se encuentran los ingresos por año que espera recibir el ISP, éstos están basado en el número de clientes y los valores de las tarifas mensuales anteriormente descritas.

Si se desea información más detallada a cerca de los cálculos de ingresos, referirse al Anexo C.

EGRESOS DEL ISP (USD/AÑO)					
		AÑO 1	AÑO 2	AÑO 3	AÑO 4
OPERACIÓN	Equipo (+ *Software*)	214621	50276	80164	52594
	Enlaces	350784	519469	620550	684418
	Mantenimiento	21462	26490	34506	39766
	Staff técnico	60000	132000	217800	319440
MARKETING	*Marketing*	180000	144000	120000	120000
ADMINISTRATIVO	Arriendo, luz, extras	82687	87223	107302	121622
TOTAL EGRESOS		909554	959458	1180322	1337839

Tabla 5.32. Resumen de egresos anuales del ISP del diseño

INGRESOS DEL ISP (USD/AÑO)				
	AÑO 1	AÑO 2	AÑO 3	AÑO 4
DIAL-UP	134328	450446	768196	1085946
CORPORATIVOS	217900	532798	742360	924406
TOTAL INGRESOS	352227	983244	1510556	2010353

Tabla 5.33. Resumen de ingresos anuales del ISP del diseño

En la tabla 5.34 se muestra la relación beneficio/costo y las ganancias por año que se esperan percibir para que el ISP pueda mantenerse en el mercado y además se indica el valor del TIR para determinar la factibilidad del proyecto.

CASH FLOW				
	AÑO 1	AÑO 2	AÑO 3	AÑO 4
INGRESOS	352227	983244	1510556	2010353
EGRESOS	909554	959458	1180322	1337839
INGRESOS-EGRESOS	-557327	23786	330234	672514
BENEFICIO/COSTO	0,39	1,02	1,28	1,50
TIR[a]	27%			

Tabla 5.34. Relación beneficio/costo y TIR

Se espera que al final del segundo año el ISP del diseño empiece a recuperar la inversión facturando a sus clientes con tarifa plana basada en tiempo y que el rendimiento (tasa de interés) que ganará el dinero que permanece invertido en este proyecto sea del 27%. Tomando en cuenta que la tasa activa del mercado a enero del 2002 es del 18%[4], se concluye que el proyecto es factible.

5.3.3 SEGUNDO MODELO DE CALCULO DE TARIFAS BASADO EN VOLUMEN

Para determinar la tarifa por volumen, se debe realizar el cálculo del costo que representaría al ISP transportar 1 GB para lo cual se debe tomar en cuenta los costos de todos los elementos que intervienen en dicho trasporte como son: equipos y enlaces. Otro aspecto a considerar es que en el enlace internacional la ocupación del mismo es del 60%[1], valor que será utilizado para calcular el volumen de datos a transportar.

5.3.3.1. Cálculo de los costos por GB para usuarios dial-up y corporativos

Para comenzar con el cálculo se hace imprescindible conocer la cantidad de tráfico mensual promedio que transmiten tanto un usuario *dial-up* como un corporativo. Los valores a utilizar son 1462.3 y 4800 Kbits/seg que corresponden a los anchos de banda calculados para el primer año tanto para los usuarios *dial-*

[a]La tasa interna de retorno (TIR) es definida como aquella tasa de descuento que iguala a cero los flujos netos de fondos en términos de valor presente.

up como corporativos respectivamente obtenidos con las ecuaciones 0.7*# usuarios *dial* y 40*# usuarios corporativos.

Para un usuario *dial-up*:

$$\frac{1462.3\ \text{Kbits}}{1\ \text{seg}} \cdot \frac{1000\ \text{bits}}{1\ \text{Kbit}} \cdot \frac{1\ \text{byte}}{8\ \text{bits}} \cdot \frac{1\ \text{KB}}{1024\ \text{bytes}} \cdot \frac{1\ \text{GB}}{1E6\ \text{KB}} \cdot \frac{3600\ \text{seg}}{1\ \text{h}} \cdot \frac{24\ \text{h}}{1\ \text{día}} \cdot \frac{30\ \text{días}}{1\ \text{mes}} \cdot \frac{0.6}{2089\ \text{usua}} = 0.133\ \text{GB/usu/mes}$$

Para un usuario corporativo:

$$\frac{4800\ \text{Kbits}}{1\ \text{seg}} \cdot \frac{1000\ \text{bits}}{1\ \text{Kbit}} \cdot \frac{1\ \text{byte}}{8\ \text{bits}} \cdot \frac{1\ \text{KB}}{1024\ \text{bytes}} \cdot \frac{1\ \text{GB}}{1E6\ \text{KB}} \cdot \frac{3600\ \text{seg}}{1\ \text{h}} \cdot \frac{24\ \text{h}}{1\ \text{día}} \cdot \frac{30\ \text{días}}{1\ \text{mes}} \cdot \frac{0.6}{120\ \text{usua}} = 7.59\ \text{GB/usu/mes}$$

Con estos datos se procede a calcular la cantidad de tráfico cursado tanto por los usuarios *dial-up* como por los corporativos durante el primer año.

PRIMER AÑO						
MES	# usuar. Dial-up	GB/usu/mes	*Dial* GB/mes	# corpor	GB/usu/mes	Corp. GB/mes
1	50	0.133	6.64	4	7.594	30.38
2	102		13.55	15		113.91
3	300		39.87	30		227.81
4	499		66.31	40		303.75
5	698		92.76	52		394.88
6	897		119.20	60		455.63
7	1095		145.52	72		546.75
8	1294		171.96	83		630.28
9	1493		198.41	92		698.63
10	1692		224.85	104		789.75
11	1890		251.16	112		850.50
12	2089		277.61	120		911.25
VOLUMEN ANUAL (GB/año)			1607.84			5953.50
VOLUMEN ANUAL TOTAL (GB/año)			7561.34			

Tabla 5.35. Trafico esperado cursado por los usuarios dial-up y corporativos durante el primer año

Para el resto de años se sigue un procedimiento similar, a continuación se presenta una tabla de resumen:

RESUMEN DE LA CANTIDAD DE TRAFICO			
	VOLUMEN *Dial*	VOLUMEN Corp.	VOLUMEN TOTAL
AÑO 1	1607.84	5953.5	7561.34
AÑO 2	5391.64	14557.22	19948.86
AÑO 3	9194.97	20282.91	29477.88
AÑO 4	12998.3	25256.81	38255.11

Tabla 5.36. Resumen anual del tráfico cursado por los usuarios

Todos los costos relacionados con enlaces y equipos que comparten ambos tipos de usuarios se los coloca en una sola tabla denominada tabla de costos globales de equipos.

$$\text{Costo global (USD/GB)} = \frac{\text{Costo global (USD/año)}}{\text{Volumen TOTAL (GB/año)}}$$

Este valor corresponde al costo por GB que debe aportar un usuario *dial* o corporativo ya que ambos lo comparten, pagando más los usuarios que cursen mayor cantidad de tráfico.

COSTOS GLOBALES DE EQUIPOS (*DIAL-UP* + CORPORATIVOS) (USD)					
Costos	**ITEMS**	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**
Costos Eventuales	Servidores	41347	738	1197	1197
	Router Principal	16016	4100	4100	3600
	Firewall	15680			
	Switch	7554			
	UPS	2800			
	Rack de 48"	384			
	Software	27085			
	Discos duros de respaldo	1197	738	1197	1197
	Instalación de enlaces(Satelit+NAP)	7000			
Costos Recurrentes	AB Satelital	271800	385020	435780	458460
	AB al NAP	14800	18904	21571	23512
Costo Global Total (USD/año)		**405663**	**409500**	**463845**	**487966**
Costo Global *Dial-up* (USD/GB)		53.65	20.53	15.74	12.76
Costo Global Corp. (USD/GB)		53.65	20.53	15.74	12.76

Tabla 5.37. Costos globales y distribución de costos

Los costos referentes a enlaces y equipos particulares para un determinado usuario son utilizados para determinar el costo parcial, el mismo que hace uso de la siguiente fórmula:

$$\textit{DIAL-UP}\text{ Costo parcial (USD/GB)} = \frac{\textit{DIAL-UP}\text{ Costo parcial (USD/año)}}{\text{Volumen de tráfico }\textit{dial}\text{ (GB/año)}}$$

Para el costo parcial corporativo (USD/GB) se utiliza una fórmula similar.

COSTOS PARCIALES (*DIAL-UP*) (USD)					
Costos	**ITEMS**	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**
Eventuales	NAS	82510	43.100.00	73670	43.000.00
	Instalación E1s	1500			
Recurrentes	E1s	32000	84960	127008	162129.6
Subtotal (USD/año)		**116010**	**128060**	**200678**	**205129.6**
Subtotal (USD/GB)		72.15	23.75	21.82	15.78

Tabla 5.38. Costos parciales anuales para usuarios dial-up

COSTOS PARCIALES (CORPORATIVOS)					
Costos	**ITEMS**	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**
Eventuales	*Router* corp	20048	1600	0	3600
	Instalación FR	2500			
Recurrentes	FR	21184	30586	36191	40316
Subtotal (USD/año)		**43732**	**32185.6**	**36190.8**	**43916.4**
Subtotal (USD/GB)		7.35	2.21	1.78	1.74

Tabla 5.39. Costos parciales anuales para usuarios corporativos

Como se mencionó anteriormente el costo por mantenimiento corresponde al 10% del costo de los equipos y dependiendo del volumen de tráfico se calcula el costo de mantenimiento por GB, así:

$$\textit{DIAL-UP}\text{ Costo manteni. Equipos compar. (USD/GB)} = \frac{\text{Costo manteni. Equipos comp. (USD/año)}}{\text{Volumen TOTAL de tráfico (GB/año)}}$$

$$\textit{DIAL-UP}\text{ Costo manteni. }\textit{Softw.}\text{ compar. (USD/GB)} = \frac{\text{Costo manteni. }\textit{Softw. comp.}\text{ (USD/año)}}{\text{Volumen TOTAL de tráfico (GB/año)}}$$

DIAL-UP Costo manteni. NAS (USD/GB) = $\frac{\text{Costo manteni. NAS. (USD/año)}}{\text{Volumen de tráfico } DIAL \text{ (GB/año)}}$

Corp. Costo manteni. *Router* corp. (USD/GB) = $\frac{\text{Costo manteni. } Router \text{ corp. (USD/año)}}{\text{Volumen de tráfico corp. (GB/año)}}$

A continuación se presenta un cuadro de resumen con los costos por mantenimiento de los equipos utilizados tanto para usuarios *dial* como corporativos.

COSTOS POR MANTENIMIENTO					
		AÑO 1	AÑO 2	AÑO 3	AÑO 4
Eq. Compart.	Costo equipos (costos globales)	84978	5576	6494	5994
	% Mantenimiento anual	10	10	10	10
	Costo por mantenimiento equipos	8498	9055	9705	10304
	Costo por mant. Equipos *dial-up*	1.12	0.45	0.33	0.27
	Costo por mant. Equipos corporativos	1.12	0.45	0.33	0.27
Soft. Comp.	Costo total *software*	27085			
	% Mantenimiento *software*	10	10	10	10
	Costo por mantenimiento *software*	2708.5	2708.5	2708.5	2708.5
	Costo por mant. Equipos *dial-up*	0.36	0.14	0.09	0.07
	Costo por mant. Equipos corporativos	0.36	0.14	0.09	0.07
Eq. *Dial-up*	Costo total equipos *dial-up* (NAS)	82510	43100	73670	43000
	10% Mantenimiento anual	8251	12561	19928	24228
	Costo por mant. Equipos *dial-up*	5.13	2.33	2.17	1.86
Eq. Corpor.	Costo total equipos corporativos CORP.	20048	1600	0	3600
	10% Mantenimiento anual	2005	2165	2165	2525
	Costo por mant. Equipos corporativos	0.34	0.15	0.11	0.10
Costo por mantenimiento total:					
Dial-up (USD/GB)		6.61	2.92	2.59	2.20
Corporat.(USD/GB)		1.82	0.74	0.53	0.44

Tabla 5.40. Distribución de costos por mantenimiento entre usuarios dial-up y corporativos

Así por ejemplo, para obtener el costo por mantenimiento para usuarios corporativos, se deben sumar los costos de mantenimiento por equipos y *software* compartidos y el mantenimiento del *router* corporativo (indicados en la misma tabla), dando un total de 1.82 USD/ GB (1.12+0.36+0.34).

Para calcular los costos por *marketing*, personal técnico y administrativo se utilizan las fórmulas que a continuación se presentan, considerando que el costo administrativo representa el 10% de los costos operativos y de *marketing*, además estos costos (USD/año) deben ser equitativos para los dos tipos de usuarios ya que van enfocados para ambos sectores y no para uno en particular .

$$\text{Corp. Costo } \textit{marketing} \text{ (USD/GB)} = \frac{[\text{Costo } \textit{marketing} \text{ (USD/año)}]/2}{\text{Volumen de tráfico corp. (GB/año)}}$$

$$\text{Corp. Costo personal técn. (USD/GB)} = \frac{[\text{Costo personal Tecn. (USD/año)}]/2}{\text{Volumen de tráfico corp. (GB/año)}}$$

$$\text{Corp. Costo administrativo (USD/GB)} = \frac{[\text{Costo administrativo (USD/año)}]/2}{\text{Volumen de tráfico corp. (GB/año)}}$$

COSTOS VARIOS				
	AÑO 1	**AÑO 2**	**AÑO 3**	**AÑO 4**
Costo Mensual	15000	12000	10000	10000
Costo Anual	180000	144000	120000	120000
***Marketing Dial-up* (USD/GB)**	55.98	13.35	6.53	4.62
***Marketing* Corpor. (USD/GB)**	15.12	4.95	2.96	2.38
Personal técnico	5	10	15	20
Compensación costo de vida		10%	10%	10%
Sueldo mensual (USD)	1000	1100	1210	1331
Costo anual por sueldos (USD)	60000	132000	217800	319440
Costo para usuarios *dial-up* (USD/GB)	18.66	12.24	11.84	12.29
Costo para usuarios corporat. (USD/GB)	5.04	4.53	5.37	6.32
Costos admimistrativos (USD)	82686.80	87223.50	107302.02	121621.72
Costos admimistrativos *dial-up*(USD/GB)	25.71	8.09	5.83	4.68
Costos admimistrativos corp.(USD/GB)	6.94	3.00	2.65	2.41

Tabla 5.41. Distribución de costos por marketing, staff técnico y costos administrativos entre usuarios dial-up y corporativos

5.3.3.2. Cálculo de las tarifas basadas en volumen

La tabla 5.42 presenta un resumen de resultados de los costos por *marketing*, personal técnico y administrativos para los cuatro años.

A continuación se presenta un resumen de costos por GB para usuarios *dial-up* y corporativos en base a los resultados que se obtuvieron anteriormente.

USUARIO	RESUMEN COSTOS (USD/GB)				
		AÑO 1	AÑO 2	AÑO 3	AÑO 4
DIAL-UP	Costos operativos/GB	151.07	59.44	51.99	43.03
	Costos *Marketing/GB*	55.98	13.35	6.53	4.62
	Costos Administri./*GB*	25.71	8.09	5.83	4.68
	Costo TOTAL/GB	**232.76**	**80.88**	**64.35**	**52.33**
CORPOR.	Costos operativos/GB	67.85	28.01	23.42	21.26
	Costos *Marketing/GB*	15.12	4.95	2.96	2.38
	Costos Administri./*GB*	6.94	3.00	2.65	2.41
	Costo TOTAL/GB	**89.91**	**35.96**	**29.03**	**26.05**

Tabla 5.42. Resumen de costos por tipo de usuario

El porcentaje de rentabilidad será tomado como el 15%[a] del costo neto por GB en el sector de las telecomunicaciones, siendo por tanto la tarifa a cobrar de:

$$\text{Tarifa} = \text{Costo neto} + \%\text{Rentabilidad} * \text{Costo neto}$$

Ahora, la tarea se centra en encontrar la tarifa adecuada para los usuarios *dial-up* y corporativos de manera que el TIR se mantenga dentro del intervalo del 20% al 30% que sugieren los expertos. Para un TIR del 23% se procede a encontrar los valores de tarifa correspondientes para un usuario *dial* y corporativo.

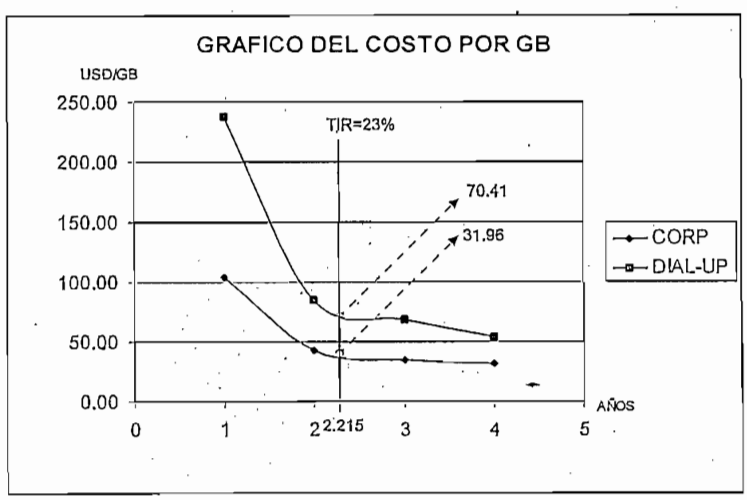


Fig. 5.4. Gráfico del costo por GB

[a] Valor recomendado por el personal técnico de Impsat.

Mediante la ayuda del cálculo computacional se encontró que estos valores son 70.41 USD/GB y 31.96 USD/GB para un usuario *dial-up* y corporativo respectivamente, de manera que la tarifa a cobrar por GB es la siguiente:

TARIFAS	
% Rentabilidad	15%
Dial-up (USD/GB)	80.97
Corporatiovos (USD/GB)	36.75

Tabla 5.43. Tarifas basadas en volumen

5.3.3.3. Análisis Beneficio/Costo

En base a los clientes proyectados por el ISP de diseño y con la tarifa que se espera cobrar se muestra la relación beneficio/costo así como las ganancias a percibir por año.

CASH FLOW				
	AÑO 1	AÑO 2	AÑO 3	AÑO 4
INGRESOS	349004	971605	1490008	1980781
EGRESOS	909555	959458	1180322	1337839
BENEFICIO/COSTO	0.38	1.01	1.26	1.48
GANANCIA=ING-EGR	-560550	12147	309686	642942
TIR	23%			

Tabla 5.44. Relación beneficio/costo y TIR

El método de tarifación por volumen tiene ventajas y desventajas frente al modelo de tarifación por tiempo. Si un usuario aumenta el tráfico cursado, el ISP recibirá mayores ingresos, los mismos que posteriormente pueden ser invertidos para adquirir mayor capacidad y no degradar la calidad de servicio, sin embargo, si un usuario transmite menos de la capacidad promedio calculada, el ISP correrá el riesgo de fracasar. En el método de facturación por volumen en cambio, el ISP cobra por adelantado, independientemente de si el usuario transmite o no información siendo ésta es una forma de garantizar la entrada de ingresos al proveedor.

BIBLIOGRAFÍA CAPÍTULO V

[1] "*ISP Survival Guide. Strategies for Running a Competitive ISP*"; Geoff Huston; Primera Edición; John Wiley & Sons, Inc; 1999; EE.UU.

[2] http://isp-planet.com/business/requiem.html

Pricing your Internet Service

[3] http://www.ccq.org.ec/servicio/asesora/aum.htm

Acuerdo No.0007-Sobre el aumento de sueldos

[4] http://www.ccq.org.ec/ecuador/Indica/18.htm

Indicadores económicos. Tasas de interés.

6

CONCLUSIONES Y RECOMENDACIONES

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

El proyecto de tesis desarrollado a lo largo de este trabajo constituye una guía básica que provee la metodología y los procedimientos a seguir para la implementación de la infraestructura de un Proveedor de Servicios de Internet y de su sistema de seguridades. Debido a que Internet es un mercado en crecimiento en nuestro país y Quito es una de las ciudades que concentra gran cantidad de negocios, oficinas, empresas, industrias, instituciones educativas, estudiantes y personas que requieren servicios de Internet fuera de sus sitios de trabajo, esta ciudad se convierte en un área con grandes oportunidades de éxito para la implantación de un ISP.

Es importante que un ISP sepa elegir adecuadamente los enlaces internacionales que necesita para asegurar su conectividad global, incluso contratando el servicio con varios operadores diferentes.

Tanto los equipos de comunicación como los equipos de aplicación a adquirir por el proveedor deben ser fáciles de instalar, configurar y administrar para hacer el trabajo más rápido y más económico. Estos equipos deben ser capaces de adaptarse a cambios en la red para poder satisfacer requerimientos de escalabilidad, alta disponibilidad y factibilidad de administración.

Cuando el ISP observe que un servidor es muy visitado por los clientes, el servicio puede verse degradado por la falta de capacidad del equipo para atender tantas peticiones. Para poder mejorar esa respuesta, se dan varias soluciones entre las que se encuentran: duplicidad del servicio entre varios servidores, mejora de servidores en capacidad de proceso, etc. Conforme el ISP vaya creciendo es

recomendable distribuir los servicios que se ofrecen en servidores independientes para mejorar los tiempos de respuesta de las solicitudes de los usuarios.

Como se puede ver existen varios y diversos métodos para implementar seguridad en la red del ISP, pero ninguno por sí sólo puede brindar la suficiente seguridad, sino que es la combinación de todos los elementos vistos junto con una acertada planeación de políticas de seguridad. Aunque una estrategia de seguridad puede ahorrar mucho tiempo a la organización y proporcionar importantes recomendaciones de lo que se debe hacer, la seguridad es una parte integrante del ciclo de vida de los sistemas, por lo que se debe revisarse y probarse con periodicidad.

Es importante documentar el ataque una vez que se ha producido, documentación que debe contemplar todos los aspectos que se conozcan del mismo, entre los que se incluyen el daño que ha causado, puntos vulnerables y las debilidades que se explotaron durante el ataque, la cantidad de tiempo de producción perdido y los procedimientos para reparar el daño. Dicha documentación ayudará a modificar las estrategias proactivas para evitar ataques futuros o mermar los daños.

La seguridad por si misma hace más difícil el acceso a un sistema al tener que proveer seguros adicionales que los usuarios deben pasar, mientras que al disminuir la cantidad de seguridad aumenta la posibilidad de intrusión, por lo que se debe trabajar en el punto en el cual la compañía trabaja más eficientemente, a éste punto se lo denomina punto de equilibrio.

Determinar una estructura de precios para establecer el modelo de tarifación de un ISP significa considerar una variedad de factores como son: aceptación en el mercado, facilidad de implementación, exactitud en la medición de los parámetros, escalabilidad y viabilidad competitiva.

Para un ISP en el cual dominan los costos de los enlaces (como el proveedor del diseño), es conveniente establecer una estructura de tarifación que permita al ISP

generar ingresos de acuerdo al consumo del cliente (mientras más se consume más se paga), de esta manera el ISP contaría con los recursos para invertir tales ingresos en la compra de más capacidad para no degradar el servicio. Sin embargo, en un mercado de consumo donde del factor discriminante es el precio, se ha hecho muy común la estructura de tarifa plana sin tomar en cuenta que cuando la red se congestiona por exceso de tráfico el ISP no podrá aumentar su capacidad ya que no contará con los suficientes recursos para hacerlo.

En la actualidad los usuarios de Internet en Ecuador empiezan a tomar conciencia de la importancia que tiene el saber elegir adecuadamente un ISP, un usuario ya no solo se fija en el precio, sino también en el servicio que obtienen de su ISP en cuanto a la capacidad del mismo de ofrecer una buena conectividad que se vea reflejada en la reducción de tiempos de acceso a los servicios finales del usuario. Para ello el ISP debe proporcionar un conjunto de herramientas por medio de mecanismos de QoS para que el administrador las utilice para controlar el uso de recursos de red en forma eficaz.

Por lo tanto, un ISP es una empresa de negocios y como tal está expuesta a muchos riegos que pueden afectar su estabilidad. Uno de los aspectos claves para tener éxito dentro de este entorno es saber combinar correctamente el aspecto tecnológico, económico y por supuesto los recursos humanos con los que se debe contar. Un adecuado conocimiento del mercado en el que se desenvuelve el ISP permitirá identificar las oportunidades de éxito del proveedor antes de emprender el negocio. Efectivamente, un proveedor de servicios de Internet debe ser una empresa que tome en consideración muchos aspectos para garantizar su permanencia dentro de un mercado altamente competitivo como lo es Internet.

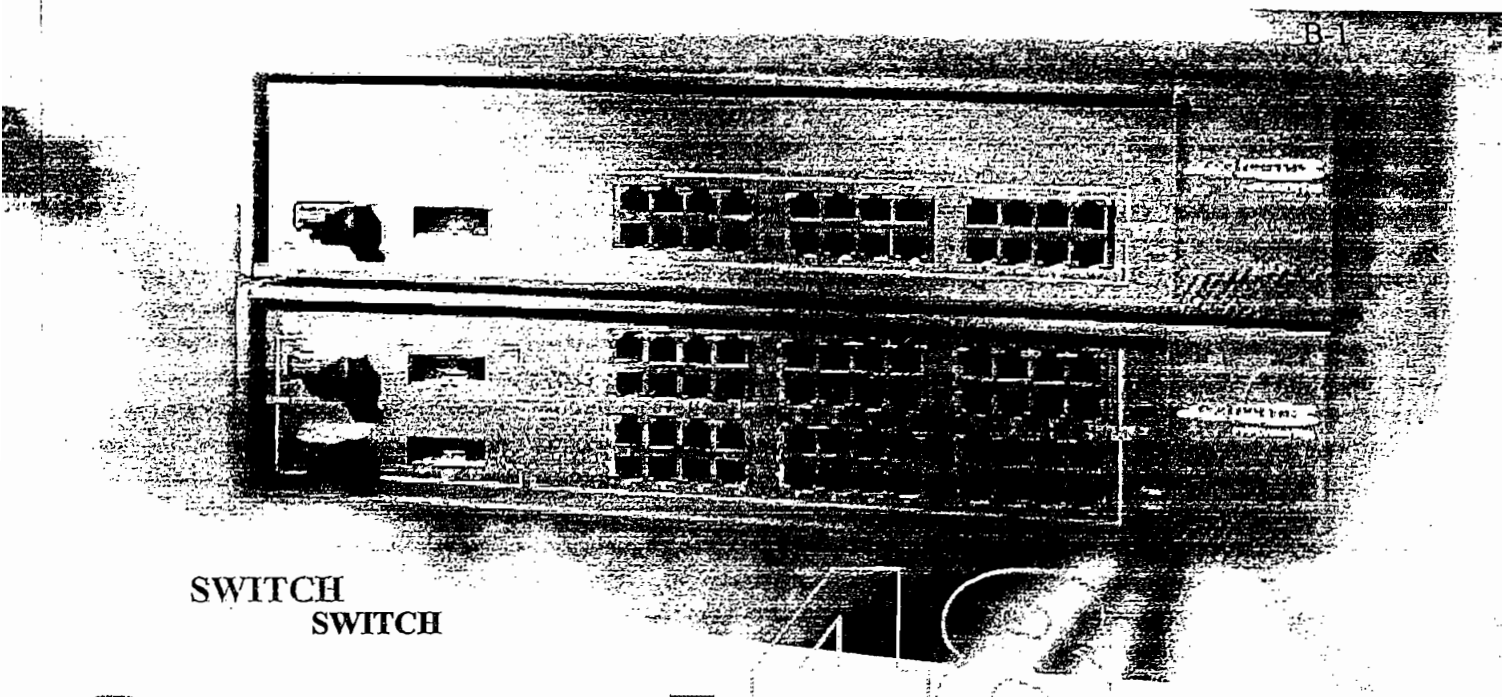
6.2. RECOMENDACIONES

Para que el ISP de diseño se convierta en una empresa de éxito, es necesario que brinde servicios propios adicionales como son: chat, Usenet, Internet call waiting, click to dial, servicios de banda ancha, .etc. Para los dos primeros servicios es necesario hacer el dimensionamiento de las capacidades de los discos duros. En cuanto al servicio de banda ancha, se debe hacer un estudio de mercado para conocer quienes van a ser los potenciales clientes y realizar el diseño en base a dicho estudio.

Como trabajo complementario, se recomienda realizar el diseño de un ISP inalámbrico con un estudio previo en el área para conocer si es factible o no la implementación de este servicio y si tendrá acogida o no de acuerdo a su tarifa correspondiente.

Siendo la seguridad del ISP un aspecto muy importante, se recomienda ampliar este punto y tratar en más detalle las formas de asegurar la infraestructura de la red del ISP y la forma cómo el proveedor debe ayudar a sus clientes a proteger sus redes de posibles ataques.

Finalmente, se recomienda a los organismos encargados de la regulación de las telecomunicaciones, realizar un análisis acerca del método del cobro de las tarifas de Internet en el país. Es conveniente realizar un estudio cuyo objetivo sea determinar cuán factible es implementar una estructura de facturación basada en volumen para los clientes del ISP en el Ecuador.



SWITCH
SWITCH

Summit48 and Summit24

The Summit48 and Summit24 provide 10/100 Mbps aggregation in service provider data centers, server farms, metropolitan area networks, multi-tenant buildings, and wiring closets. They integrated seamlessly into networks while delivering high port density, wire-speed performance and low cost of ownership.

Summit48 With 48 switched 10/100 Mbps auto-negotiating Ethernet ports and two full-duplex GBIC-based 1000BASE-SX, LX or LX-70 Gigabit Ethernet ports, Summit48 has a 17.5 Gbps non-blocking switch fabric and a forwarding rate of 10.1 million packets per second. Summit48 comes with wire-speed Layer 2 and wire-speed basic Layer 3 switching using static routing or RIP V1/V2 routing protocols. For easy scalability, the Summit48 upgrades to full Layer 3 switching with a simple upgrade key. The full Layer 3 switching includes support for protocols such as OSPF, DVMRP, PIM and IPX routing of multiple encapsulation types.

Summit24 With 24 switched 10/100 Mbps auto-negotiating Ethernet ports and one full-duplex GBIC-based 1000BASE-SX, LX or LX-70 Gigabit Ethernet port, Summit24 has an 8.5 Gbps non-blocking switch fabric and a forwarding rate of 5.1 million packets per second. Summit24 comes with wire-speed Layer 2 and wire-speed basic Layer 3 switching using static routing or RIP V1/V2 routing protocols. For easy scalability, the Summit24 upgrades to full Layer 3 switching with a simple upgrade key. The full Layer 3 switching includes support for protocols such as OSPF, DVMRP, PIM and IPX routing of multiple encapsulation types.

Pre-installed on every Extreme Networks switch, the ExtremeWare™ software suite combines industry-standard protocols to ensure interoperability with legacy switches and routers, plus Policy-Based Quality of Service (QoS) for bandwidth management and traffic.

- **Gigabit Ethernet links to the network core and high-density 10/100 Mbps ports to the edge**
- **Non-blocking switch fabric bandwidth with wire-speed switch performance**
- **Start with basic Layer 3 switching and wire-speed Layer 2 switching**
- **Scale up to full Layer 3— using advanced IP Routing Protocols and IPX Routing— with a simple upgrade key**
- **Policy-Based QoS, including bandwidth management, prioritization and congestion control**
- **Fault-tolerant: multiple load-sharing trunks, multiple spanning trees and optional redundant power supply**
- **Extensive management through HTTP, SNMP, RMON and command line interface**

Summit24 Specifications

General

True QoS via ExtremeWare and Policy-Based Quality of Service
Full or half duplex operation
Multiple spanning tree support
Multiple load-sharing trunks
Up to 128,000 Layer 2 addresses
Up to 64,000 Layer 3 addresses
4 MB buffering

Summit48
48 10/100BASE-X ports
Two GBIC-based 1000BASE-SX ports

Summit24
24 10/100BASE-TX ports
One GBIC-based active 1000BASE-X ports

Protocols and Standards

IEEE 802.3z 1000BASE-X
IEEE 802.3ab 1000BASE-T
IEEE 802.3x Flow control
IEEE 802.3ad Link aggregation
IEEE 802.1D-1998 (includes 802.1p)
IEEE 802.1Q VLAN Tagging
RFC 768 UDP
RFC 783 TFTP
RFC 791 IP
RFC 792 ICMP
RFC 826 ARP
RFC 854 Telnet
RFC 1058 RIP
RFC 1122 Host Requirements
RFC 1256 Router Discover Protocol
RFC 1519 CIDR
RFC 1542 BootP
RFC 1723 RIP v2
RFC 1812 IP Router Requirement
RFC 2068 HTTP
RFC 2178 OSPF
RFC 2131 BootP/DHCP Relay
RFC 2236
DVMRP v3
PIM

Performance

Summit48
17.5 Gbps non-blocking bandwidth
Route/filter/forward 10.1 million pps

Summit24
8.5 Gbps non-blocking bandwidth
Route/filter/forward 5.1 million pps

Management and Security

RFC 1157 SNMP v1/v2c
RFC 1213 MIB II
RFC 1354 IP forwarding table MIB
RFC 1493 Bridge MIB
RFC 1573 Evolution of Interface
RFC 1643 Ethernet MIB
RFC 1724 RIP v2 MIB
RFC 1757 Four groups of RMON
RFC 2021 RMON Probe Configuration
RFC 2037 Entity MIB
RFC 2138 RADIUS
RFC 2239 802.3 MAU MIB
ExtremeWare Enterprise MIB
HTML and Telnet Management

Physical and Environmental

Dimensions:
Summit48 & Summit24
(H) 3.5 in x (W) 17.32 in x (D) 17.42 in
(H) 8.90 cm x (W) 44.0 cm x (D) 44.25 cm
Weight:
Summit48
18 lbs (8.17 kg)
Summit24
17 lbs (7.65 kg)
Operating Temperature: 0° C to 40° C
Storage Temperature: -10° C to 70° C
Humidity: 10% to 95% non-condensing
Power: 90-250 VAC, 47-63 Hz, 2.5 A max
Includes hardware for mounting in a standard 19-inch rack
Heat Dissipation:
341-2 BTU/hr (118 Watts)
MTBF = 50,000 hours

Regulatory Compliance

FCC Part 15 Class A
ICES-0003 Class A
VCCI Class 1
EN55022 Class A
CISPR 22 Class A
EN55024

Environmental

EN60068 to Extreme IEC68 schedule

Reliability

Minimum 50000 hrs MTBF to Mil HDBK 217F Notice I, Parts Stresss Method

Acoustic

58 dB/pW Weighted Sound Power Level to ENC27779 and EN29295

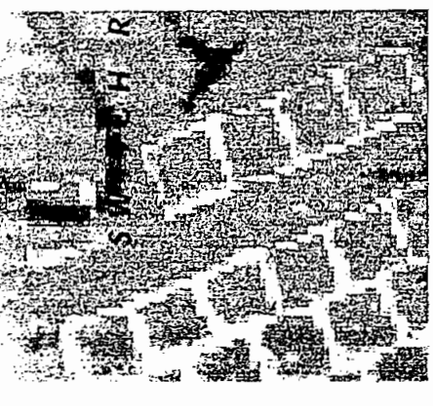
Summit24 and Summit48 Ordering Information

Order Number	Description
13010	24 10/100BASE-TX ports, 2 unpopulated GBIC based 1000BASE-X port (1 active and 1 redundant) with Basic Layer 3 switching software
13020	24 10/100BASE-TX ports, 2 unpopulated GBIC based 1000BASE-X port (1 active and 1 redundant) with Full Layer 3 switching software
15010	48 10/100BASE-TX ports, 4 unpopulated GBIC based 1000BASE-X port (2 active and 2 redundant) with Basic Layer 3 switching software
15020	48 10/100BASE-TX ports, 4 unpopulated GBIC based 1000BASE-X port (2 active and 2 redundant) with Full Layer 3 switching software
10027	Optional upgrade key from Basic to Full Layer 3 switching software for Summit24
10029	Optional upgrade key from Basic to Full Layer 3 switching software for Summit48
10011	SX GBIC Module (275 meters)
10013	LX GBIC Module (10 kms)
10016	LX-70 GBIC Module (70 kms)
10901	Redundant Power Supply system for Summit24 or Summit48 (supports 2 switches)

For more product information from Extreme Networks, please call 1-888-257-3000.3585 Monroe Street Santa Clara, CA 95051-1450 Phone 408.579.2800 Fax 408.579.3000
Email info@extremenetworks.com Web www.extremenetworks.com

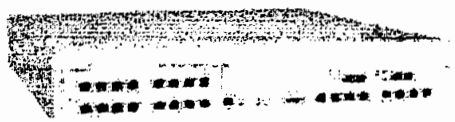
©2000 Extreme Networks, Inc. All rights reserved. Extreme Networks and BlackDiamond are registered trademarks of Extreme Networks, Inc. in certain jurisdictions. ExtremeWare, ExtremeWare Vista, ExtremeWorks, ExtremeAssist, ExtremeAssist1, ExtremeAssist2, PartnerAssist, Extreme Standby Router Protocol, ESRP, SmartTraps, Summit, Summit1, Summit4, Summit4/FX, Summit7i, Summit24, Summit48, Summit Virtual Chassis, SummitLink, SummitGbX, SummitRPS, Velocity, the BlackDiamond logo and the Extreme Networks logo are trademarks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. The Extreme Turbodrive logo is a service mark of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. All other registered trademarks, tradenarks and service marks are property of their respective owners. Specifications are subject to change without notice.

LDS-S48-24-101



In addition to performance, the X-Pedition 2000 provides pinpoint application control and superior routing capacity. The X-Pedition 2000 is standards-based and provides seamless interoperability with previous generations of networking equipment. Finally, the X-Pedition 2000 features full Layer 2 switching, full-function routing, and Layer 4 application switching. Layer 4 application switching provides pinpoint control of network traffic through extensive security, port-level accounting and comprehensive quality of service (QoS)—all at the application level, and all without sacrificing wire-speed performance.

Specifications



Physical

Dimensions	7.1cm (2.8") H x 43.2cm (17") W x 47cm (18.5") D
Weight	9 kg (20 lb)

Environmental

Operating Temperature	5° C to 40° C (41° F to 104° F)
Relative Humidity	15% to 90% (non-condensing)

Ordering Information

Part No.	*Description*
SSR-2-B128	X- Pedition 2000 desktop switch router in a fixed configuration with 16 10/100 TX ports. Includes redundant power supplies, X- Pedition Router Services software and CoreWatch device management software
SSR-2-PKG128	10/100Base-TX module for the X-Pedition 2000 with 24 10/1000 ports and a 2-port 1000Base-SX expansion module
SSR-2-LX-AA	1000Base-LX expansion module for the X-Pedition 2000, 2 ports
SSR-2-SX-AA	1000Base-SX expansion module for the X-Pedition 2000, 2 ports
SSR-2-FX-AA	100Base-FX expansion module for the X-Pedition 2000, 8 ports with MT-RJ connectors
SSR-2-TX-AA	10/100Base-TX expansion module for the X-Pedition 2000, 8 ports

Product Configuration

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠

CISCO 3640 (ROUTER CORPORATIVO)

Cisco 3600 4-slot Modular Router-AC with IP Software

Product	Description	Quant
CISCO3640	Cisco 3600 4-slot Modular Router-AC with IP Software	1
CAB-AC	Power Cord, 110V	1
S364AP-12102T	Cisco 3640 Series IOS ENTERPRICE PLUS	1
MEM3600-8U16FS	8-to-16MB Flash Factory Upgrade for the Cisco 3600	1
MEM3640-32U64D	32-to-64 MB DRAM Factory Upgrade for the Cisco 3640	1
NM-2W	2 WAN Card Slot Network Module (no LAN)	1
WIC-1T	1- Port Serial WAN Interface Card	1
NM-8A/S	8- Port Async/Sync Serial Network Module	1
CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet	9
CON-OSP-3640	Cisco 3640 On-Site Premium Maintenance	1

Total LeadTime: 15 days Total Price: $ 17900

Product Leadtime and Pricing information is not final until your order has been accepted and processed by Cisco. By saving this configuration and retrieving it in the Ordering Tool, your organization can be assured Pricing and Leadtimes will stay updated to the point of submission (receipt). For orders being shipped through our Euopean logistics Center (ELC), please add 4 business days to the stated leadtime for shipping/processing time between manufacturing and the ELC.

Cisco Systems, Inc.
170 West Tasman Drive.
San Jose, CA 95134-1706
Phone: 11 408 526-4000
Fax: 11 408 526-4100

CISCO SYSTEMS

Product Configuration

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠

CISCO 3640 (ROUTER,PRINCIPAL)

Cisco 3600 4-slot Modular Router-AC with IP Software

Product	Description	Quant
CISCO3640	Cisco 3600 4-slot Modular Router-AC with IP Software	1
CAB-AC	Power Cord, 110V	1
S364AP-12201	Cisco 3640 Series IOS IP PLUS	1
MEM3600-8U16FS	8-to-16MB Flash Factory Upgrade for the Cisco 3600	1
MEM3640-32U64D	32-to-64 MB DRAM Factory Upgrade for the Cisco 3640	1
NM-1FE2W	1 10/100 Ethernet 2 WAN Card Slot Network Module	1
WIC-1T	1-Port Serial WAN Interface Card	1
NM-1HSSI	Single port HSSI Network Module for 3660, 3640 and 3620	1
CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet	1
CON-OSP-3640	Cisco 3640 On-Site Premium Maintenance	1

Total LeadTime: 15 days Total Price: $ 14300

Product Leadtime and Pricing information is not final until your order has been accepted and processed by Cisco. By saving this configuration and retrieving it in the Ordering Tool, your organization can be assured Pricing and Leadtimes will stay updated to the point of submission (receipt). For orders being shipped through our European logistics Center (ELC), please add 4 business days to the stated leadtime for shipping/processing time between manufacturing and the ELC.

Cisco Systems, Inc.
170 West Tasman Drive,
San Jose, CA 95134-1706
Phone: +1 408 526-4000
Fax: +1 408 536-4100

Product Configuration

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠

CISCO 3640 (ROUTER CORPORATIVO+NAS)

Cisco 3600 4-slot Modular Router-AC with IP Software

Product	Description	Quant
CISCO3640	Cisco 3600 4-slot Modular Router-AC with IP Software	1
CAB-AC	Power Cord, 110V	1
S364AP-12201	Cisco 3640 Series IOS IP PLUS	1
MEM3600-8U16FS	8-to-16MB Flash Factory Upgrade for the Cisco 3600	1
MEM3640-32U64D	32-to-64 MB DRAM Factory Upgrade for the Cisco 3640	1
NM-1FE2W	1 10/100 Ethernet 2 WAN Card Slot Network Module	1
WIC-1T	1- Port Serial WAN Interface Card	1
NM-HDV-2E1-60	Dual-Port 60 Channel E1 Voice/Fax Network Module	1
NM-16AM	16 Port Analog Modem Network Module	1
CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet	1
CAB-E1-BNC-3M	E1 Cable, BNC E1, 75ohm/Unbalanced, 3 Meters	1
CON-OSP-3640	Cisco 3640 On-Site Premium Maintenance	1

Total LeadTime: 15 days Total Price: null 0.00

Product Leadtime and Pricing information is not final until your order has been accepted and processed by Cisco. By saving this configuration and retrieving it in the Ordering Tool, your organization can be assured Pricing and Leadtimes will stay updated to the point of submission (receipt). For orders being shipped through our European logistics Center (ELC), please add 4 business days to the stated leadtime for shipping/processing time between manufacturing and the ELC.

Cisco Systems, Inc.
170 West Tasman Drive.
San Jose, CA 95134-1706
Phone: +1 408 526-4000
Fax: +1 408 526-4100

CISCO SYSTEMS

Configuration Summary

CISCO SYSTEMS

AS5400
AS5400 CHASSIS WITH MB,3 DFC CARRIER CARDS

You have successfully completed your configuration.

Click the Edit Configuration button to edit your configuration.

Edit This Configuration

Global Price List Latin America Availability

Update Price

No Service

Hide Discounts

SERVIDOR DE ACCESO DE RED (NAS)

Product #	Description	Discount %	Quantity	Price	Lead Time
AS5400	AS5400 CHASSIS WITH MB,3 DFC CARRIER CARDS	0.00	1	30,000.00	15 days
AS54-AC-RPS	AS5400 Chassis-MB-Dual AC Power Supply	0.00	1	0.00	
CAB-AC	Power Cord,110V	0.00	2	0.00	
S54CP-12205	Cisco AS5400 Series IOS IP PLUS	0.00	1	0.00	
AS54-E1-216NP	216 NP Modems, 1 Octal E1/PRI DFC Card	0.00	1	43,000.00	
CAB-DFC-OCTAL-1MF	1 Meter 8 PRI DFC Cable - Female RJ45	0.00	1	300.00	
FR5X-ISDNONLY-LIC	AS5000 series IOS ISDN Only License Per Port	0.00	216	3,240.00	
FR5X-SS7-LIC	AS5000 series IOS SS7 License Per Port	0.00	216	1,728.00	
FR5X-ISDN2UP-LIC	AS5000 series ISDNOnly to UnivPort Upgrade License Per Port	0.00	1	15.00	

Total Lead Time:
15 days

Total Price: USD 78,283.00

Link to Pricing and Lead Time information

akros
Grupo Corporativo

SERVIDORES

Quito, 22 de Octubre del 2001

SATNET
Ing. FLAVIO CEPEDA
Presente.-

akros

SERVIDOR COMPAQ PROLIANT ML370

ITEM	Producto	Precio unitario	cantidad	total
1	ProLiant ML370 Model T01 P1000-256K	$2.832,00	1	$2.832,00
	One Intel Pentium III 1GHz processor with 256kB integrated cache (dual processor capability), 128-MB 133MHz registered ECC SDRAM DIMM memory standard (expandable to 4GB), six total slots (four 64-bit PCI and two 32-bit PCI), Compaq NC3163 PCI 10/100 WOL NIC (embedded), Integrated Dual Channel Wide Ultra3 SCSI Controller, support for four 1" non-hot-plug hard drives, plus two available 5.25-inch non-hot plug removable media bays, internal mass storage capacity of up to 145.6 GB, High Speed IDE CD-ROM Drive, Compaq Insight Manager, SmartStart and Automatic Server Recovery (ASR).			
2	36.4 GB Pluggable Ultra3 SCSI 10,000 rpm Uni	$738,00	1	$738,00
3	1GB Reg SDRAM DIMM 133	$1.525,00	1	$1.525,00
4	Tarjeta de Red 10/100 PCI	$22,00	1	$22,00
	OPCIONES			
5	9.1 GB Pluggable Ultra3 SCSI 10,000 rpm Univ	$345,00	1	$345,00
6	18.2 GB Pluggable Ultra3 SCSI 10,000 rpm Uni	$459,00	1	$459,00
7	512MB Reg SDRAM DIMM 133	$510,00	1	$510,00
8	Pentium III 1GHz Processor Option Kit (ML370	$828,00	1	$828,00
9	Compaq S510 15-Inch Color Monitor	$185,00	1	$185,00
			Precio	$7.444,00
			IVA	$893,28
			TOTAL	$8.337,28

INCLUYE 2 HORAS DE SERVICIO

Condiciones de la negociación

50% al realizar el pedido

50% contraentrega del producto

Tiempo de entrega:

Inmediato previa consulta de stock

Validez de la oferta:

15 días

Microsof
TOSHIBA
e-Flex

akros
Grupo Corporativo

Granatía: 3 años de soporte en partes, mano de obra en sitio para los servidores.
Tiempo de Respuesta: 20 días laborables luego derealizado el pedido.
Soporte Técnico: del Centro Autorizado de Servicios Compaq

Atentamente;

Tlga. MARISOL LOZANO R
AKROS
502334 ext. 205
CELULAR: 09715218

Microsoft
TOSHIBA
Fax

Su Pla e™ 1

El poder gráfico y de procesamiento de una estación de trabajo avanzada, a precio de PC

SERVIDORES

Sun Microsystems está cambiando las reglas de juego una vez más con la presentación de la nueva Sun Blade™ 100, la primera estación de trabajo de 64 bits a precio de PC. Con un rendimiento significativamente superior y aproximadamente a la mitad del costo– se espera que la Sun Blade™ 100 ofrezca a los clientes la continuación ideal de la Sun Ultra™ 5 2D, la estación de trabajo para gráficos en plataforma UNIX® más vendida del mundo.

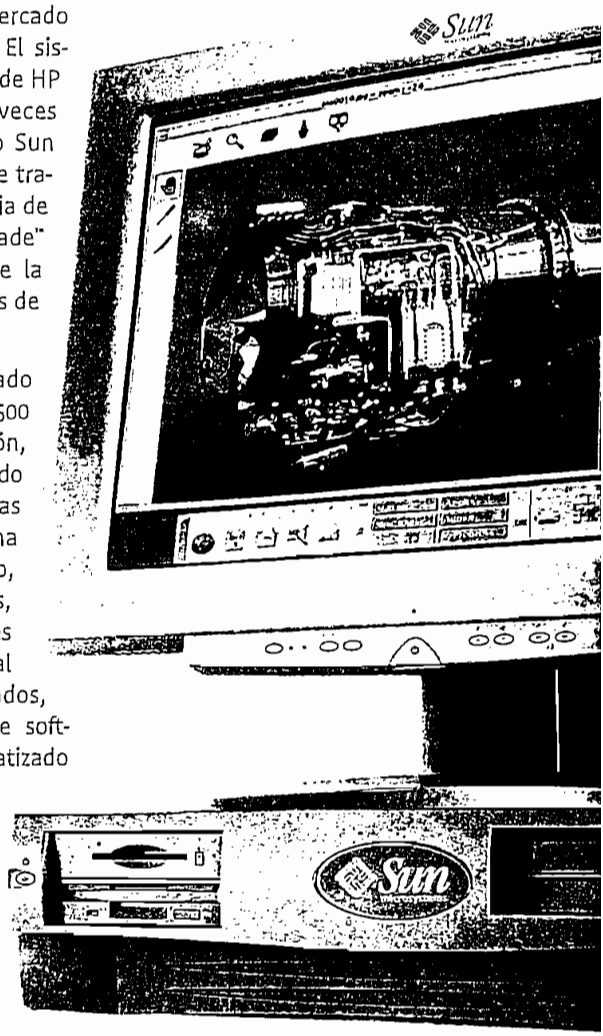
El anuncio de Sun Blade™ 100 coincide con la presentación de la nueva tarjeta de aceleración de gráficos Sun Expert3D-Lite™, el miembro más reciente de la línea Sun de equipos gráficos para profesionales. Juntas, ofrecen una funcionalidad total en 3D a las estaciones de trabajo de 64 bits y a un nuevo nivel de precio. Por otro lado, la recién anunciada tarjeta coprocesadora SunPCi™ II coloca íntegramente una PC de ambiente Windows dentro de la estación de trabajo Sun Blade™ 100. Un usuario puede ejecutar aplicaciones simultáneamente en Windows y en el Ambiente Operativo Solaris™ a velocidad nativa; de modo que no hay necesidad de tener dos computadoras en un escritorio. Esto le ahorra al usuario dinero y espacio.

"Sun marcó un hito en precio y rendimiento en 1998 con la estación de trabajo Sun Ultra 5, y ahora lo está haciendo de nuevo con la Sun Blade™ 100", declaró Fred Kohout, director de mercadeo del Grupo de Productos para Mercado Técnico, de Sun Microsystems. "Estamos atacando el mercado de las PC en su propio terreno con precio y rendimiento. No sólo estamos ofreciendo a los usuarios de UNIX una nueva y excelente estación de trabajo, sino que también les estamos dando a los usuarios de PC el incentivo que necesitan –un mejor precio– para que adopten nuestro Ambiente Operativo Solaris™ 8 de 64 bits, que es mucho más poderoso.

La nueva estación de trabajo Sun Blade™ 100 se adapta bien al mercado de rango bajo de la industria. El sistema de 64 bits más económico de HP cuesta aproximadamente 5 veces más que la estación de trabajo Sun Blade™ 100. Y cuando se trata de trabajo pesado, los 2 GB de memoria de la estación de trabajo Sun Blade™ 100 de 64 bits son el doble de la capacidad de la PC 220 de 32 bits de Dell.

Basada en el recién anunciado procesador UltraSPARC™ III de 500 MHz y 64 bits, de alta integración, Sun Blade™ 100 ofrece el sólido Ambiente Operativo Solaris™ 8 y las características propias de una avanzada estación de trabajo, incluyendo arquitectura de 64 bits, 2 GB de memoria y capacidades gráficas en 3D de nivel profesional para una gama de mercados, incluyendo los de desarrollo de software, diseño electrónico automatizado (EDA), servicios financieros, MCAD/MCAE (diseño mecánico asistido por computadora/ ingeniería mecánica asistida por computadora) de nivel básico, educación/investigación y creación de contenido digital.

"La estación de trabajo Sun Blade™ 100 con tarjeta gráfica Sun Expert3D-Lite™ abrirá nuevas puertas a mercados que anteriormente no podían permitirse el desarrollo en un ambiente UNIX®", afirma Kara Yokley, analista de investigación de estaciones de trabajo de IDC. "La estrategia de Sun Microsystems de ofrecer estaciones de trabajo UNIX® de 64 bits a precios de PC de 32 bits, ha frenado la migración de usuarios técnicos a Windows NT y ha ayudado a Sun a mantener su posición de líder en el mercado de UNIX®."



La única estación de trabajo que soporta tanto plataformas UNIX® como NT

Procesador intel Pentium III 866MHz
RAM: 128MB expandible a 512MB
Disco duro: 20GB
Video AGP 2X 8MB
CD ROM 48X
Sonido 3D
Red 10/100
Windows "Millenium Edition" en español
Lotus Smart Suite
Monitores de 14, 15 o 17"

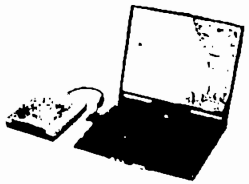
Procesador Intel Pentium III 933MHz
RAM: 128MB expandible a 512MB
Disco duro: 30GB
Video AGP 2X 8MB
Sonido 3D parlantes estéreo
CD ROM 48X
Fax modem 56k
Red 10/100
Teclado para Internet
Windows "Millenium Edition" en español
Lotus Smart Suite
Monitores de 14, 15 o 17"

Procesador Intel Pentium III 1GHz
RAM 256MB expandible a 512MB
Disco duro: 20GB
Video AGP 8MB
Sonido 3D y parlantes incorporados
CD Writer y DVD
Fax modem 56K
Red 10/100
Teclado para Internet
Windows "Millenium Edition" en español
Monitor LCD (Flat Panel) de 15"

Procesador Intel Pentium 4 de 1,5 GHz
Memoria RAM 128MB SDRAM expandible a 1GB
Disco duro 40GB
Video AGP 32MB
Sonido 3D parlantes estéreo y micrófono
CD Writer 12X10X32X
Fax modem 56K
Red 10/100
Teclado para Internet
Windows "Millenium Edition" en español
Lotus Smart Suite
Monitores de 14, 15 o 17"

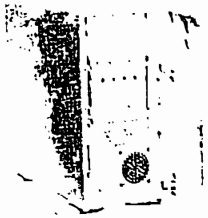
Procesador Intel Celeron 800MHz
Pantalla de 12,1" pasiva (DX) o activa (T)
RAM 32MB (200DX) o 64MB (200T)
Video AGP 4MB
Disco duro: 5GB
Fax modem interno 56K
CD ROM interno 24X
Parlantes y micrófono incorporados
Windows "Millenium Edition" en español

Ultralight
Procesador Intel Pentium III 650MHz
Pantalla de 13,3" activa
Video AGP 8MB
RAM 64MB
Disco duro: 10GB
CD ROM 24X y FDD externos
Fax modem interno
Red 10/100 interno
Parlantes y micrófono incorporados
Windows "Millenium Edition" en español

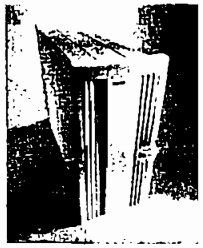


Ultralight
Procesador Intel Pentium III 700MHz
Pantalla de 13,3" activa
Video AGP 8MB
RAM 128MB
Disco duro: 10GB
DVD ROM 8X y FDD externos
Fax modem interno
Red 10/100 interno
Parlantes y micrófono incorporados
Windows "Millenium Edition" en español

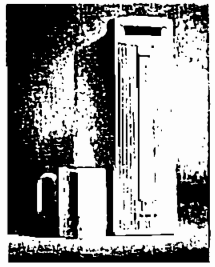
Procesador Intel Pentium III 700MHz
Pantalla de 13,3" activa
Video AGP 8MB
RAM 64MB
Disco duro: 10GB
CD ROM 24X y FDD internos
Fax modem interno
Red 10/100 interno
Parlantes y micrófono incorporados
Windows "Millenium Edition" en español



Hasta 2 procesadores Intel Pentium III 1 GHz
Memoria SDRAM ECC 128 MB expandible a 3GB
Discos duros Ultra 160SCSI de 9, 18 y 36GB
CD ROM 48X
Red 10/100
Instalación: EasyBuild 4.0
Administración: ASM Pro 4.3
BMC Board para detección de fallas
5 bahías hot swap
Hasta 2 fuentes de poder redundantes
$ 2550 + IVA



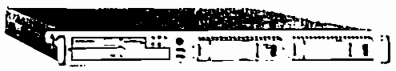
Hasta 2 procesadores Intel Pentium III 1GHz
Memoria SDRAM ECC 128 MB expandible a 4GB
Discos duros Ultra 160SCSI de 9, 18 y 36GB
CD ROM 48X
Red 10/100
Instalación: EasyBuild 4 0
Administracion: ASM Pro 4.3
BMC Board para detección de fallas
6 bahías hot swap
Hasta 2 fuentes de poder redundantes
$ 3370 + IVA



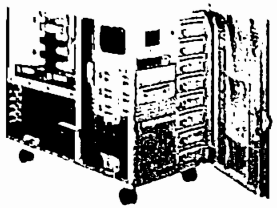
$ 1226 + IVA

Server Appliance con Servicios de Impresión,
Correo, Archivos, WEB, NAT, Proxy
Sistema Operativo Linux Preinstalado en DOC
Administración remota, no necesita teclado ni mouse
Red 10/100
Disco duro de 15GB IDE
Modem ADSL
Procesador Intel Celeron 566MHz 66MHz FSB
64MB RAM ECC ampliable a 512MB

SERVIDORES



Altura: 1 unidad Rack
Hasta 2 procesadores Intel Pentium III 1 GHz
Memoria SDRAM ECC 128 MB expandible a 4GB
Discos duros Ultra 160SCSI de 9, 18 y 36GB
CD ROM 48X
Red 10/100
Instalación: EasyBuild 4.0
Administración: ASM Pro 4.3
BMC Board para deteccion de fallas
2 bahías hot swap
1 fuente de poder



Hasta 4 procesadores Intel Pentium III Xeon
de 900MHz y 2MB cache
Memoria SDRAM ECC 512MB expandible a 16GB
Discos duros Ultra 160SCSI de 9, 18 y 36GB
CD ROM 48X
Red 10/100
Instalación: EasyBuild 4.0
Administración: ASM Pro 4.3
BMC Board para detección de fallas
8 bahías hot swap
Hasta 3 fuentes de poder redundant

Product Configuration

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠

CiscoSecure Access Control Server(SERVIDOR RADIUS)

Características	Description
Platform	PC with Windows NT Server 4.0 and Service Pack 6 or Windows 2000 Server; Pentium 350-MHz processor or faster; Screen resolution of 256 colors at 800x600 lines
RAM	128 MB required
Disk Drive	150 MB of disk space
Software Requirements	Any Cisco or third-party access/management solution configurable as a TACACS+ or RADIUS client

Total LeadTime: 15 days Total Price: $ 5597

Product Leadtime and Pricing information is not final until your order has been accepted and processed by Cisco. By saving this configuration and retrieving it in the Ordering Tool, your organization can be assured Pricing and Leadtimes will stay updated to the point of submission (receipt). For orders being shipped through our Euopean logistics Center (ELC), please add 4 business days to the stated leadtime for shipping/processing time between manufacturing and the ELC.

SERVIDOR CACHÉ

Fecha: 15 de Octubre de 2001

ITEM	No. PARTE	DESCRIPCION	CANT.	P.UNIT.	P.TOTAL
1	CE-560	Cache Web	1	$12,546.00	$12,546.00
		Cisco Systems Cisco Content Engine 560			
		Rendimiento HTTP: 20 Mbps			
		SDRAM: 512 MB			
		Cap. Máx. almacenamiento: 144GB			
		Alm. interno (Ultra2 SCSI) : 2 HD de 18GB			
		Compatibilidad con matriz de almacenamiento: Sí.			
		Interfaces de red: 2 puertos 10/100BASE-TX			
		Memoria Flash: 16GB			
	SF-560-CACHE-3.1.1	CE-560 sotware: Cache			
	CAB-AC	Cable de poder. 110VAC			
TOTAL US$ - C.I.F.:					$12,546.00

Son: Doce mil quinientos cuarenta y seis 00/100 dólares americanos

CONDICIONES COMERCIALES:
Precio: Precios C.I.F. descritos en dólares, no incluyen I.V.A.
Forma de pago: 60% a la orden de compra y 40% a la entrega de los equipos
Validez de la oferta: 30 días
Tiempo de entrega: 45 días a partir del pago del anticipo
Garantía Técnica: 1 año contra defectos de fábrica

Atentamente,
ComWare del Ecuador S.A.

Product Configuration

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠

FIREWALL

PIX 515 Chassis only

Product	Description	Quant
PIX-515	PIX 515 Chassis only	1
CAB-AC	Power Cord, 110V	1
PIX-VPN-3DES	PIX 3DES Software License Without Client Software	1
PIX-515UR-SW	PIX 515 Unrestricted Function software license	1
SF-PIX-6.0	PIX v6.0 Software for the PIX Chassis	1
PIX-4FE	PIX Four-port 10/100 Ethernet interface	1
CON-OSP-PIX515	Cisco 3640 On-Site Premium Maintenance	1

Total LeadTime: 15 days Total Price: $ 14000

Product Leadtime and Pricing information is not final until your order has been accepted and processed by Cisco. By saving this configuration and retrieving it in the Ordering Tool, your organization can be assured Pricing and Leadtimes will stay updated to the point of submission (receipt). For orders being shipped through our European logistics Center (ELC), please add 4 business days to the stated leadtime for shipping/processing time between manufacturing and the ELC.

GRUPO BRAVCO
ENLACE SATELITAL

Global One Connected

SERVICIO CORPORATIVO

Presentamos a continuación nuestra justificación económica diseñada especialmente a su requerimiento. Esta contiene:

- Acceso a Internet (a la velocidad requerida por el cliente)
- Servicio de última milla (através de un operador autorizado)

1.- SERVICIO DE ACCESO A INTERNET DEDICADO ILIMITADO

Este servicio Grupo BRAVCO lo ofrece a través de la red de Global One / Sprint la misma que provee de ventajas competitivas por sobre todos los proveedores de Internet del Ecuador (ver cuadro de ventajas).

- Acceso dedicado a 1024Kbps, para interconectar a SATNET con LA RED de Global One Sprint

1024Kbps

Description	*Speed (Kbps)*	*Inscription (USD)*	*Monthly Rate (USD)*
Servicio de acceso Internet dedicado al *backbone* Mundial de Global One.	1024	3.500.00	18.400.00
TOTAL USD	*1024*	3.500.00	*18,400.00*

2048Kbps

Description	*Speed (Kbps)*	*Inscription (USD)*	*Monthly Rate (USD)*
Servicio de acceso Internet dedicado al *backbone* Mundial de Global One.	2048	3.500.00	22.900.00
TOTAL USD	*2048*	3.500.00	22,900.00

Estos valores incluyen el acceso a internet, la última milla y los equipos terminales.

Servicio de la linea dedicada incluye:

- Servicio de 24 horas al día
- Casilleros de Correo Electrónico (*e_mail*)
- 16 IP reales
- 10 Mb de espacio en Servidor para *Web Hosting*
- Acceso al *World Wide Web* Ilimitado
- Acceso a Servidores FTP (transferencia de archivos)

	WINDOWS		
	WINDOWS 95/98	WINDOWS NT 4.0	WINDOWS 2000
SERVIDOR FTP	ArGoSoft Avirt Gateway Bison FTP Server Dragon Server Fictional Daemon FTP Serv-U FtpMax G6 FTP Server Ghetto FTP Server GuildFTPd Vermillion FTP Daemon War FTP Daemon WFTPD ZBServerPro aVirtMail Server CommuniGate Pro Dmail Server FTGate Mail Server Internet Anywhere	ArGoSoft Avirt Gateway Bison FTP Server Dragon Server Fictional Daemon FTP Serv-U FtpMax G6 FTP Server GuildFTPd Vermillion FTP Daemon War FTP Daemon WFTPD ZBServerPro aVirtMail Server CommuniGate Pro Dmail Server Eudora WorldMail Server FTGate Mail Server	ArGoSoft Avirt Gateway Bison FTP Server Dragon Server FTP Serv-U FtpMax G6 FTP Server WFTPD WS_FTP aVirtMail Server CommuniGate Pro iMail Server InterMail Post Office Internet Anywhere
SERVIDOR DE MAIL	Internet MailBridge MailMax MailSite mDaemon Merak Mercur NTMail Nu-Mail QuickMail Pro Rover SLmail VOPmail	iMail Server InterMail Post Office Internet Anywhere Internet MailBridge MailMax MailSite mDaemon Merak Mercur Microsoft Exchange Server NTMail Nu-Mail	MailMax MailSite mDaemon Merak Mercur NTMail Nu-Mail Slmail VOPmail
SERVIDOR DE NEWS	Cassandra DNEWS News Server nDaemon	CoffeLink News Server Netscape Collabra NewsChannel	DNEWS News Server
SERVIDOR TELNET	Ataman TCP Remote WinTD	Ataman TCP Remote Georgia SoftWorks Windows NT InterAccess TelnetD Server Slnet WinTD	Fictional Daemon Georgia SoftWorks InterAccess TelnetD Slnet
SERVIDOR WEB	Alibaba Apache Avenida Domino Go Webserver GoAhead WebServer iServer Jigsaw Lotus Domino Microsoft Personal Web Server OnmiHTTPd Pro Roxen Challenger Sambar Server Savant Server SimpleServer: WWW Tcl Web Server URL Live vqServer WebSite Pro	First Class Intranet Server iPlanet Web Server Microsoft Internet Information Ser. Microsoft Site Server Netscape Enterprise Server WebSite Pro WebSite Standard Xitami ZBServer * Además de estos servidores, se incluyen los que corren bajo Windows 95/98	IServer Microsoft Internet Informat. Savant Servertec Internet Server SimpleServer:WWW
SERVIDOR CHAT	Chat Space Conference Room Pow Wow Community Server	Chat Space Conference Room eRoom Meeting Point Place Ware Conferece Center Pow Wow Community Server Volano Chat Pro	Chat Space Conference Room ERoom Meeting Point

	UNI	SGI IR	IBM AIX	TRU64
SERVIDOR FTP	CommuniGate Pr InterMail Post Off Sendmail		CommunicaGate Pro Dmail Server InterMail Post Office Sendmail	
SERVIDOR DE MAIL	DNEWS News S InterNetNews Netscape Collabr		DNEWS News Server InterNetNews Netscape Collabra Server	
SERVIDOR WEB	AOLserver Apache Avenida Domino Go Webs iPlanet Web Serv iServer NCSA HTTPd Netscape Enterpi iPlanet Web Serv iServer NCSA HTTPd Netscape Enterpi Rapidsite Roxen Challenge Stronghold Tcl Web Server vqServer Xitami Zeus Web Server		AOLserver Apache Avenida Domino Go Webserver iPlanet Web Server iServer NCSA HTTPd Netscape Enterprise Server Netscape FastTrack Roxen Challenger Stronghold Tcl Web Server vqServer Xitami Zeus Web Server	
SERVIDOR CHAT	Conference Roor Volano Chat Pro		Volano Chat Pro	
SERVIDOR DE NEWS				
SERVIDOR TELNET				
SERVIDOR PROXY	Netscape Proxy S Squid Web Proxy		Netscape Proxy Server Squid Web Proxy Caché	

	B
SERVIDOR DE MAIL	CommuniGat DMail Server Sendmail
SERVIDOR DE NEWS	DNEWS New InterNetNews Netscape Co
SERVIDOR WEB	Apache iServer NCSA HTTP Stronghold Tcl Web Ser vqServer Xitami Zeus Web S
SERVIDOR CHAT	Lucid Chat Volano Chat
SERVIDOR PROXY	Squid Web I

	UNIX COMERCIAL					
	COMPAQ TRU64	IBM AIX	SGI IRIX	SOLARIS	SUN OS	ULTRIX
SERVIDOR DE MAIL	Sendmail	CommunicaGate Pro Dmail Server InterMail Post Office Sendmail	CommuniGate Pro InterMail Post Office Sendmail	CommuniGate Pro Dmail Server MailStudio 2000 Plus Netscape Messaging Server NT Mail InterMail Post Office Sendmail	Sendmail	Sendmail
SERVIDOR DE NEWS	InterNetNews	DNEWS News Server InterNetNews Netscape Collabra Server	DNEWS News Server InterNetNews Netscape Collabra Server	CoffeeLink News Server DNEWS News Server InterNetNews Netscape Collabra Server	DNEWS News Server InterNetNews	InterNetNews
SERVIDOR DE WEB	iPlanet Web Server Netscape Enterprise Server Netscape FastTrack Roxen Challenger Tcl Web Server vqServer Xitami	AOLserver Apache Avenida Domino Go Webserver iPlanet Web Server iServer NCSA HTTPd Netscape Enterprise Server Netscape FastTrack Roxen Challenger Stronghold Tcl Web Server vqServer Xitami Zeus Web Server	AOLserver Apache Avenida Domino Go Webserver iPlanet Web Server iServer NCSA HTTPd Netscape Enterprise Server iPlanet Web Server iServer NCSA HTTPd Netscape Enterprise Server Rapidsite Roxen Challenger Stronghold Tcl Web Server vqServer Xitami Zeus Web Server	AOLserver Apache Avenida Domino Go Webserver iPlanet Web Server iServer Jigsaw Lotus Domino NCSA HTTPd Netscape Enterprise Server Roxen Challenger Stronghold Tcl Web Server vqServer Xitami Zeus Web Server	Apache Avenida iServer NCSA HTTPd Stronghold Tcl Web Server vqServer Xitami	NCSA HTTPd Stronghold Tcl Web Server vqServer Xitami
SERVIDOR CHAT	Volano Chat Pro	Volano Chat Pro	Conference Room Volano Chat Pro	Lucid Chat Volano Chat Pro Conference Room Meeting Point Place Ware Conference Center	Volano Chat Pro	Volano Chat Pro
SERVIDOR PROXY	Squid Web Proxy Caché	Netscape Proxy Server Squid Web Proxy Caché	Netscape Proxy Server Squid Web Proxy Caché	Squid Web Proxy Caché CSM Proxy Server CSM Proxy Server Plus Netscape Proxy Server	Squid Web Proxy C.	Squid Web Proxy Caché

ANEXO C

$$4*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1}{SD} + RS\ seg + 4*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1\text{seg}.}{MD\text{ bits}} +$$

$$AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{4}{SD} + RS\ seg +$$

$$8*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1}{SD} + RS\ seg + 8*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1\text{seg}.}{MD\text{ bits}} +$$

$$AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{4}{SD} + RS\ seg +$$

$$16*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1}{SD} + RS\ seg + 16*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1\text{seg}.}{MD\text{ bits}} +$$

$$AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{4}{SD} + RS\ seg +$$

$$32*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1}{SD} + RS\ seg + 32*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1\text{seg}.}{MD\text{ bits}} +$$

$$AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{4}{SD} + RS\ seg +$$

$$37*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1}{SD} + RS\ seg + 37*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1\text{seg}.}{MD\text{ bits}} +$$

$$AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \Big|\ \frac{4}{SD} + RS\ seg$$

$$Ret.\ TOTAL = 7200.\ \frac{1}{MA} + 7200.\ \frac{4}{SD} + 449600.\ \frac{1}{SD} + 449600.\ \frac{1}{MD} + 4{,}05\ [seg]$$

Para una página de 50 KB y con N = 1024 bytes

$$\text{Ret. TOTAL} = (PH+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + (PH+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg} +$$

$$(1024+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1}{SD} + RS\text{ seg} + (512+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{seg.}}{MD\text{ bits}} +$$

$$AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg} +$$

$$2*(1024+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1}{SD} + RS\text{ seg} + 2*(1024+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{seg.}}{MD\text{ bits}} +$$

$$AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg} +$$

$$4*(1024+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1}{SD} + RS\text{ seg} + 4*(1024+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{seg.}}{MD\text{ bits}} +$$

$$AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg} +$$

$$8*(1024+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1}{SD} + RS\text{ seg} + 8*(1024+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{seg.}}{MD\text{ bits}} +$$

$$AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg} +$$

$$16*(1024+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1}{SD} + RS\text{ seg} + 16*(1024+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{seg.}}{MD\text{ bits}} +$$

$$AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg} +$$

$$19*(1024+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1}{SD} + RS\text{ seg} + 19*(1024+C)\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{seg.}}{MD\text{ bits}} +$$

$$AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes.}\ \frac{8\text{ bits.}}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg}$$

Ret. TOTAL= 6800. $\frac{1}{MA}$ + 6800. $\frac{4}{SD}$ + 429600. $\frac{1}{SD}$ + 429600. $\frac{1}{MD}$ + 3,51 [seg]

Para N = 2048 bytes el retardo total es el siguiente:

Ret. TOTAL= 6400. $\frac{1}{MA}$ + 6400. $\frac{4}{SD}$ + 419600. $\frac{1}{SD}$ + 419600. $\frac{1}{MD}$ + 2,97 [seg]

Para una página de 100 KB y con N = 512 bytes

Ret. TOTAL= (PH+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{ seg}}{MA\text{ bits}}$ + (PH+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{4}{SD}$ + RS seg +

(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1}{SD}$ + RS seg + (512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{seg.}}{MD\text{ bits}}$ +

AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{ seg}}{MA\text{ bits}}$ + AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{4}{SD}$ + RS seg +

2*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1}{SD}$ + RS seg + 2*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{seg.}}{MD\text{ bits}}$ +

AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{ seg}}{MA\text{ bits}}$ + AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{4}{SD}$ + RS seg +

4*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1}{SD}$ + RS seg + 4*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{seg.}}{MD\text{ bits}}$ +

AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{ seg}}{MA\text{ bits}}$ + AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{4}{SD}$ + RS seg +

8*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1}{SD}$ + RS seg + 8*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{seg.}}{MD\text{ bits}}$ +

AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{ seg}}{MA\text{ bits}}$ + AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{4}{SD}$ + RS seg +

16*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1}{SD}$ + RS seg + 16*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{seg.}}{MD\text{ bits}}$ +

1 byte | MA bits ... 1 byte | SD ... RS seg +

64*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1}{SD}$ + RS seg + 64*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{seg.}}{MD\text{ bits}}$ +

AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{ seg}}{MA\text{ bits}}$ + AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{4}{SD}$ + RS seg +

[64*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1}{SD}$ + RS seg + 64*(512+C) bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{seg.}}{MD\text{ bits}}$ +

AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{1\text{ seg}}{MA\text{ bits}}$ + AR bytes. $\frac{8\text{ bits.}}{1\text{ byte}} \mid \frac{4}{SD}$ + RS seg +

$$\frac{1\text{ byte}}{SD} \qquad \frac{1\text{ byte}}{MD\text{ bits}}$$

$$AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg} +$$

$$32*(512+0)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1}{SD} + RS\text{ seg} + 32*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1\text{seg}.}{MD\text{ bits}} +$$

$$AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg} +$$

$$64*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1}{SD} + RS\text{ seg} + 64*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1\text{seg}.}{MD\text{ bits}} +$$

$$AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg} +$$

$$\left[64*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1}{SD} + RS\text{ seg} + 64*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1\text{seg}.}{MD\text{ bits}} + \right.$$

$$AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg} +$$

$$9*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1}{SD} + RS\text{ seg} + 9*(512+C)\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1\text{seg}.}{MD\text{ bits}} +$$

$$\left. AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{1\text{ seg}}{MA\text{ bits}} + AR\text{ bytes}.\ \frac{8\text{ bits}.}{1\text{ byte}}\ \frac{4}{SD} + RS\text{ seg} \right]$$

$$\text{Ret. TOTAL} = 8000.\frac{1}{MA} + 8000.\frac{4}{SD} + 899200.\frac{1}{SD} + 899200.\frac{1}{MD} + 5{,}13\ [\text{seg}]$$

Para una página Web de 1MB el retardo es el siguiente:

$$\text{Ret. TOTAL} = 19200.\frac{1}{MA} + 19200.\frac{4}{SD} + 8992000.\frac{1}{SD} + 8992000.\frac{1}{MD} + 20{,}25\ [\text{seg}]$$

Datos:

MA =MD = 33600 bps

Capacidad del canal satelital *dial-up*: 1169.84 Kbps = 1169840 bps

Número de líneas telefónicas: 175

Número de pedidos simultáneos: 20%

En base a la capacidad del canal satelital ascendente se calcula el valor de SD mediante la siguiente fórmula:

*# líneas telefónicas * # pedidos simultáneos * SD = capacidad del canal satelital ascendente*

Donde: SD = 33424 bps

Resultados:

X [KB]	N [bytes]	Ret. Total f(SD) [seg]	Ret. Total (seg)
50	512	17.65 + 478400/SD	31,96
	1024	16.50 + 456800/SD	30,17
	2048	15.65 + 445200/SD	28,97
100	512	32.13 + 931200/SD	60,00
1000	512	288.44 + 9068800/SD	559,77

Tabla A.5. Resultado de los cálculos para retardos de descargas de páginas Web de 50, 1000 y 1000 KB

ANEXO B

ANEXOS

ANEXO A

CÁLCULO DE LOS RETARDOS

En esta sección se realizarán los cálculos para determinar los retardos en descargar una página Web de la red Internet. Antes de detallar el algoritmo de comienzo lento, necesario para dichos cálculos, se deben conocer las siguientes definiciones:

Ventana de Transmisión	VT	Es la cantidad de datos que se pueden transmitir antes de ser confirmados mediante un acuse de recibo. VT es igual al mínimo valor entre la ventana de congestión y ventana de recepción.
Ventana de Recepción	VR	Indica el número de bytes que el host destino puede recibir en la siguiente transmisión (después del acuse de recibo)
Ventana de Congestión	VC	Indica el tamaño máximo de bytes que la red podría procesar sin que existan problemas de congestión interna en la red. Dicha ventana se incrementa con el algoritmo de comienzo lento

Tabla A.1. Parámetros relacionados con el retraso en TCP

Algoritmo de Comienzo Lento

Una vez que una conexión TCP ha sido establecida, el *host* emisor inicia la transmisión con una ventana de congestión de la red igual al tamaño del máximo segmento en uso en dicha conexión. La ventana de congestión se va incrementando mediante la siguiente fórmula:

$$VC = Tamaño\ del\ máximo\ segmento \times 2^i$$

Siendo i= 0,1,2,3,4,.....

Una vez que se envía el primer segmento máximo, es decir i=0, la ventana de congestión de la red es igual al tamaño máximo del segmento, y si dicho segmento es acusado antes de que su contador expire, el valor de i seguirá aumentando en cada transmisión hasta que se produzca un *timeout* o hasta que se alcance el tamaño de la ventana de recepción.

Una vez expirado el contador antes de alcanzar el tamaño de VR, se fijará a VC el tamaño inmediatamente anterior al *timeout*, es decir, tamaño para el cual la red garantizó que no hubo congestión.

El tamaño de la ventana de congestión es una función del *threshold* que tiene un valor inicial de 64 KB. Al expirar el contador, el *threshold* se fija a la mitad del valor de la ventana de congestión determinada anteriormente. Luego de esto, la ventana de congestión se resetea al tamaño de un segmento máximo reiniciándose nuevamente el Algoritmo de Comienzo Lento con estos nuevos valores, de manera que la ventana de congestión crece exponencialmente hasta llegar al valor del *threshold* y a partir de aquí crecerá linealmente de segmento máximo en segmento máximo hasta que se alcance el valor de la ventana de recepción (la ventana de congestión permanecerá constante mientras no varíe el tamaño de la ventana de recepción) o hasta que un nuevo *timeout* ocurra y entonces se repite el proceso.

Cálculos

NOMENCLATURA		
MA	Velocidad de Tx del módem ascendente (usuario)	bps
MD	Velocidad de Tx del módem descendente (ISP)	bps
SA	Velocidad de Tx del enlace satelital ascendente (SA=SD/4)	bps
SD	Velocidad de Tx del enlace satelital descendente	bps
RS	Retardo del salto satelital (RS=0,27 seg)	seg
X	Tamaño del archivo a descargar	Bytes
N	Tamaño de un segmento máximo de la ventana de congestión	Bytes
M	Número de segmentos de N bytes en el archivo de X bytes	
C	Tamaño total de las cabeceras TCP, IP, enlace (C=50 bytes)	Bytes
PH	Tamaño del pedido (PH= 500 bytes)	Bytes
AR	Tamaño del acuse TCP ya incluidos los C bytes de cabeceras (AR=50B)	Bytes
VR	Tamaño de la ventana de recepción	Bytes
VC	Tamaño de la ventana de congestión	Bytes
VT	Tamaño de la ventana de transmisión	Bytes
TI	Número total de transmisiones necesarias para bajar el archivo	
NCL	Número de segmentos transmitidos en ventanas completas durante la ejecución del comienzo lento	
NE	Número de segmentos transmitidos en ventanas completas después de que se estabilizó VT en VR	
NF	Número de segmentos transmitidos en la última ventana de transmisión	

Tabla A.2. Nomenclatura a utilizar

Tx. N°.	N = 512 bytes		N = 1024 bytes		N = 2048 bytes	
	VC (bytes)	# segm. Tx	VC (bytes)	# segm. Tx	VC (bytes)	# segm. Tx
1	512	1	1024	1	2048	1
2	1024	2	2048	2	4096	2
3	2048	4	4096	4	8192	4
4	4096	8	8192	8	16384	8
5	8192	16	16384	16	32768	16
6	16384	32	32768	32		
7	32768	64				
8	65536	128				
9	131072	256				
Total segm. Tx.		511		63		31

Tabla A.3. Algoritmo de comienzo lento para distintos valores de N

A continuación se determinará el retardo en descargar páginas Web de 50 KB con N = 512, 1024, 2048 bytes; mientras que para páginas de 100 KB y 1 MB se utilizará N = 512 en base al ancho de banda calculado en la sección anterior. El tamaño de la ventana de recepción se fija en 32768 bytes. Para tal propósito se considerará un canal satelital libre de errores, red libre de congestión, retardos nulos en el procesamiento de *routers* y redes terrestres y en los *host* y no habrá fragmentación de datagramas.

Tx. N°.	N = 512 bytes		N = 1024 bytes		N = 2048 bytes	
	VC (bytes)	# segm. Tx	VC (bytes)	# segm. Tx	VC (bytes)	# segm. Tx
1	512	1	1024	1	2048	1
2	1024	2	2048	2	4096	2
3	2048	4	4096	4	8192	4
4	4096	8	8192	8	16384	8
5	8192	16	16384	16	32768	16
6	16384	32	32768	32		
7	32768	64				
8	65536	128				
9	131072	256				
Total segm. Tx.		511		63		31

Tabla A.3. Algoritmo de comienzo lento para distintos valores de N

X (KB)	N (bytes)	M (segm.)	VR (KB)	VR=VT	TI	NCL (segm.)	NE (segm.)	NF (segm.)
50	512	100	32	NO	7	63		37
	1024	50		NO	6	31		19
	2048	25		NO	5	15		10
100	512	200		SI	9	127	64	9
1000	512	2000		SI	37	127	29 X 64	17

Tabla A.4. Características de cada transferencia

Para descargar una página de 50 KB, será necesario transferir 100 segmentos de 512 bytes (M = 51200 bytes / 512 bytes). La tabla A.3. indica que durante la primera transmisión se ha recibido un segmento de 512 bytes, durante la segunda transmisión se han recibido dos segmentos de la misma longitud y así sucesivamente hasta la sexta transmisión, no alcanzándose el estado estable (VR=VT= 32768 bytes) porque si se continua con el algoritmo de comienzo lento en la séptima transmisión se recibirán 64 segmentos, más lo cual da un total de

127 segmentos transferidos, superándose el tamaño de la página Web a descargar. Hasta la sexta transferencia un cliente habrá recibido 63 segmentos, por lo tanto en la séptima transmisión se recibirán 37 segmentos para completar la descarga, como se indica en la tabla A.4. Procedimiento similar ocurre para N=1024 y 2048.

Para la descarga de una página Web de 100 KB, será necesario transferir 200 segmentos de 512 bytes (M = 102400 bytes / 512 bytes). La transferencia parte con el algoritmo de comienzo lento, cuando se alcanza el estado estable (7° transmisión) ya se han recibido un total de 127 segmentos (NCL), a partir de ahí se recibe sólo 1 paquete de 32768 bytes de datos (NE=64 segmentos). Por lo tanto en la última transferencia será necesario transferir 9 segmentos más para completar la descarga. Procedimiento similar ocurre para una página de 1 MB.

Haciendo uso de las tablas anteriores se procede a calcular el retardo total mediante la siguiente fórmula:

Retardo total = Ret. *loop* asc. + Ret. TX. sat. ascen. + Ret. prop. sat. ascen. +
+ Ret. TX. sat. desc. + Ret. prop. sat. desc. + Ret. *loop* desc.

Para una página de 50 KB y con N = 512 bytes

$$\text{Ret. TOTAL} = (\text{PH+C})\ \text{bytes} \cdot \frac{8\ \text{bits}}{1\ \text{byte}} \cdot \frac{1\ \text{seg}}{\text{MA bits}} + (\text{PH+C})\ \text{bytes} \cdot \frac{8\ \text{bits}}{1\ \text{byte}} \cdot \frac{4}{\text{SD}} + \text{RS seg} +$$

$$(512\text{+C})\ \text{bytes} \cdot \frac{8\ \text{bits}}{1\ \text{byte}} \cdot \frac{1}{\text{SD}} + \text{RS seg} + (512\text{+C})\ \text{bytes} \cdot \frac{8\ \text{bits}}{1\ \text{byte}} \cdot \frac{1\text{seg}}{\text{MD bits}} +$$

$$\text{AR bytes} \cdot \frac{8\ \text{bits}}{1\ \text{byte}} \cdot \frac{1\ \text{seg}}{\text{MA bits}} + \text{AR bytes} \cdot \frac{8\ \text{bits}}{1\ \text{byte}} \cdot \frac{4}{\text{SD}} + \text{RS seg} +$$

$$2\text{*}(512\text{+C})\ \text{bytes} \cdot \frac{8\ \text{bits}}{1\ \text{byte}} \cdot \frac{1}{\text{SD}} + \text{RS seg} + 2\text{*}(512\text{+C})\ \text{bytes} \cdot \frac{8\ \text{bits}}{1\ \text{byte}} \cdot \frac{1\text{seg}}{\text{MD bits}} +$$

$$\text{AR bytes} \cdot \frac{8\ \text{bits}}{1\ \text{byte}} \cdot \frac{1\ \text{seg}}{\text{MA bits}} + \text{AR bytes} \cdot \frac{8\ \text{bits}}{1\ \text{byte}} \cdot \frac{4}{\text{SD}} + \text{RS seg} +$$

Los costos para el primer año de funcionamiento del [illegible] adquisición de todos los equipos: *routers*, servidores, *firewall, switch*, etc, como se especifica en el capítulo V. A partir del segundo año en adelante, se irá adquiriendo tarjetas de red, memorias, discos duros, etc, que se irán incorporando en los equipos de la manera que se indica a continuación.

DESCRICIÓN	EQUIPO [a]	AÑO 1	AÑO 2	AÑO 3	AÑO 4
CAB-35MT	*Router* acceso corp.		200,00		200,00
Tarjeta WIC-2T			1.400,00		1.400,00
NM-WIC-2T					2.000,00
CAB-35MT	*Router* principal		100,00	100,00	200,00
NM-4T			4.000,00	4.000,00	
Tarjeta WIC-2T					1.400,00

PROYECCIONES ANUALES DE COSTOS E INGRESOS DEL ISP

PROYECCIÓN ANUAL DE LOS COSTOS DE LOS EQUIPOS

Los costos para el primer año de funcionamiento del ISP son los costos de adquisición de todos los equipos: *routers*, servidores, *firewall, switch*, etc, como se especifica en el capítulo V. A partir del segundo año en adelante, se irá adquiriendo tarjetas de red, memorias, discos duros, etc, que se irán incorporando en los equipos de la manera que se indica a continuación.

DESCRICIÓN	EQUIPO [a]	AÑO 1	AÑO 2	AÑO 3	AÑO 4
CAB-35MT	*Router* acceso corp.		200,00		200,00
Tarjeta WIC-2T			1.400,00		1.400,00
NM-WIC-2T					2.000,00
CAB-35MT	*Router* principal		100,00	100,00	200,00
NM-4T			4.000,00	4.000,00	
Tarjeta WIC-2T					1.400,00
NM-WIC-2T					2.000,00
CAB-35MT	NAS		100,00		200,00
Tarjeta de módems			43.000,00		43.000,00
Equipo NAS				73.670,00	
DD: SCSI 36.4 GB	Servidor 1 (*E-mail* y DNS)		738,00	738,00	738,00
DD: SCSI 18 GB	Servidor 2 (*Web Hosting* y FTP)			459,00	459,00
SUBTOTAL(USD)		166.374,88	49.538,00	78.967,00	51.597,00

Tabla C.1. Costos de elementos adicionales que se adquirirán anualmente

PROYECCIÓN ANUAL DE LOS COSTOS DE LOS ENLACES

A continuación se realizará una proyección anual de costos para todos los enlaces que necesita el ISP; estos son: enlaces para los clientes *dial-up*, enlaces para clientes corporativos, enlace al ISP *upstream* y enlaces al NAP Ecuador.

[a] Estos precios no incluyen IVA.

Para la proyección de enlaces se considerará que éstos tienden a bajar de precio en un 10%[a].

COSTO DE LOS E1s PARA USUARIOS *DIAL-UP*

Para el siguiente cálculo se ha considerado: el número de usuarios *dial-up* por mes que ha sido obtenido a partir de la ecuación: $y = 198.75 * x - 296.25$ como se explicó en el capítulo III. La relación usuario/línea se mantiene constante a lo largo del período considerado.

PRIMER AÑO						
MES	# usuar. dial-up	usuar/línea	Líneas telef.	# E1s	Costo de 1E1	Costo total
1	50	12	4	1	800	800
2	102	12	9	1	800	800
3	300	12	25	1	800	800
4	499	12	42	2	800	1600
5	698	12	58	2	800	1600
6	897	12	75	3	800	2400
7	1095	12	91	4	800	3200
8	1294	12	108	4	800	3200
9	1493	12	124	5	800	4000
10	1692	12	141	5	800	4000
11	1890	12	158	6	800	4800
12	2089	12	174	6	800	4800
Costo anual de E1s (USD/año)						32000

Tabla C.2. Detalle mensual de costos de enlaces E1s durante el primer año

SEGUNDO AÑO						
MES	# usuar. dial-up	usuar/línea	líneas telef.	# E1s	costo de 1E1	Costo total
13	2288	12	191	7	720	5040
14	2487	12	207	7	720	5040
15	2685	12	224	8	720	5760
16	2884	12	240	8	720	5760
17	3083	12	257	9	720	6480
18	3282	12	274	10	720	7200
19	3480	12	290	10	720	7200
20	3679	12	307	11	720	7920
21	3878	12	323	11	720	7920
22	4077	12	340	12	720	8640
23	4275	12	356	12	720	8640
24	4474	12	373	13	720	9360
Costo anual de E1s (USD/año)						84960

Tabla C.3. Detalle mensual de costos de enlaces E1s durante el segundo año

[a] Valor recomendado por el personal técnico de Impsat.

TERCER AÑO						
MES	# usuar. dial-up	usuar/línea	líneas telef.	# E1s	costo de 1E1	Costo total
25	4673	12	389	13	648	8424
26	4872	12	406	14	648	9072
27	5070	12	423	14	648	9072
28	5269	12	439	14	648	9072
29	5468	12	456	16	648	10368
30	5667	12	472	16	648	10368
31	5865	12	489	17	648	11016
32	6064	12	505	17	648	11016
33	6263	12	522	18	648	11664
34	6462	12	539	18	648	11664
35	6660	12	555	19	648	12312
36	6859	12	572	20	648	12960
Costo anual de E1s (USD/año)						127008

Tabla C.4. Detalle mensual de costos de enlaces E1s durante el tercer año

CUARTO AÑO						
MES	# usuar. dial-up	usuar/línea	líneas telef.	# E1s	costo de 1E1	Costo total
37	7058	12	588	20	583,2	11664
38	7257	12	605	21	583,2	12247
39	7455	12	621	21	583,2	12247
40	7654	12	638	22	583,2	12830
41	7853	12	654	22	583,2	12830
42	8052	12	671	23	583,2	13414
43	8250	12	688	23	583,2	13414
44	8449	12	704	24	583,2	13997
45	8648	12	721	25	583,2	14580
46	8847	12	737	25	583,2	14580
47	9045	12	754	26	583,2	15163
48	9244	12	770	26	583,2	15163
Costo anual de E1s (USD/año)						162130

Tabla C.5. Detalle mensual de costos de enlaces E1s durante el cuarto año

COSTO DE LA CONECTIVIDAD A LA NUBE *FRAME RELAY*

Para la conectividad de los usuarios corporativos a la nube *Frame Relay* se ha considerado una relación de 2:1, es decir, un enlace de 64 Kbps será compartido por dos clientes. En nuestro país, normalmente los ISP ofrecen una relación de 4:1 lo cual degrada el servicio afectando el QoS.

PRIMER AÑO					
MES	# corpor	AB al *carrier*	AB total (Kbps)	Capac. Presupuestada (Kbps)	Cost. Mens.
1	4	32	128	712	1109
2	15	32	480		1109
3	30	32	960		1109
4	40	32	1280		1109
5	52	32	1664	2136	1855
6	60	32	1920		1855
7	72	32	2304		1855
8	83	32	2656		1855
9	92	32	2944	3424	2332
10	104	32	3328		2332
11	112	32	3584		2332
12	120	32	3840		2332
Costo Anual (USD/año)					21184

Tabla C.6. Detalle mensual de costos de enlaces FR durante el primer año

SEGUNDO AÑO					
MES	# corpor	AB al *carrier*	AB total (Kbps)	Capac. Presupuestada (Kbps)	Cost. Mens.
13	128	32	4096	4392	2367
14	135	32	4320		2367
15	140	32	4480		2367
16	146	32	4672		2367
17	151	32	4832	5120	2549
18	158	32	5056		2549
19	162	32	5184		2549
20	169	32	5408		2549
21	173	32	5536	5824	2731
22	180	32	5760		2731
23	185	32	5920		2731
24	190	32	6080		2731
Costo Anual (USD/año)					30586

Tabla C.7. Detalle mensual de costos de enlaces FR durante el segundo año

TERCER AÑO					
MES	# corpor	AB al *carrier*	AB total (Kbps)	Capac. Presupuestada (Kbps)	Cost. Mens.
25	195	32	6240	6488	2874
26	200	32	6400		2874
27	206	32	6592		2874
28	210	32	6720		2874
29	215	32	6880	7120	3010
30	220	32	7040		3010
31	225	32	7200		3010
32	230	32	7360		3010
33	235	32	7520	7760	3164
34	240	32	7680		3164
35	245	32	7840		3164
36	250	32	8000		3164
Costo Anual (USD/año)					36191

Tabla C.8. Detalle mensual de costos de enlaces FR durante el tercer año

CUARTO AÑO					
MES	# corpor	AB al *carrier*	AB total (Kbps)	Capac. Presupuestada (Kbps)	Cost. Mens.
37	254	32	8128	8344	3264
38	259	32	8288		3264
39	262	32	8384		3264
40	268	32	8576		3264
41	270	32	8640	8856	3361
42	275	32	8800		3361
43	280	32	8960		3361
44	282	32	9024		3361
45	288	32	9216	9408	3454
46	291	32	9312		3454
47	297	32	9504		3454
48	300	32	9600		3454
Costo Anual (USD/año)					40316

Tabla C.9. Detalle mensual de costos de enlaces FR durante el cuarto año

COSTO DEL ANCHO DE BANDA SATELITAL

PRIMER AÑO			
MES	AB Requerido (Kbps)	AB Presupuest. (Kbps)	Cost. Mens.
1	137	1146	18400
2	470		18400
3	987		18400
4	1365		18400
5	1798		18400
6	2120		18400
7	2553	3501	26900
8	2958		26900
9	3308		26900
10	3741		26900
11	4062		26900
12	4384		26900
Costo Anual (USD/año)			271800

Tabla C.10. Detalle de costos del AB satelital para el primer año

SEGUNDO AÑO			
MES	AB REQUERIDO	AB Presupuest. (Kbps)	Cost. Mens.
13	4705	5369	30060
14	4999		30060
15	5236		30060
16	5501		30060
17	5739		30060
18	6032		30060
19	6241	6891	34110
20	6535		34110
21	6744		34110
22	7038		34110
23	7275		34110
24	7512		34110
Costo Anual (USD/año)			385020

Tabla C.11. Detalle de costos del AB satelital para el segundo año

TERCER AÑO			
MES	AB REQUERIDO	AB Presupuest. (Kbps)	Cost. Mens.
25	7750	8348	35460
26	7987		35460
27	8252		35460
28	8462		35460
29	8699		35460
30	8937		35460
31	9174	9767	37170
32	9411		37170
33	9649		37170
34	9886		37170
35	10123		37170
36	10361		37170
Costo Anual (USD/año)			435780

Tabla C.12. Detalle de costos del AB satelital para el tercer año

CUARTO AÑO			
MES	AB REQUERIDO	AB Presupuest. (Kbps)	Cost. Mens.
37	10570	11113	37890
38	10808		37890
39	10989		37890
40	11254		37890
41	11408		37890
42	11645		37890
43	11883	12397	38520
44	12036		38520
45	12302		38520
46	12483		38520
47	12748		38520
48	12930		38520
Costo Anual (USD/año)			458460

Tabla C.13. Detalle de costos del AB satelital para el cuarto año

COSTO DEL ENLACE AL NAP ECUADOR

Para el enlace al NAP Ecuador, se ha utilizado circuitos *Clear Channel*.

PRIMER AÑO			
Mes	**AB Calculado al NAP**	**AB Presupuest. (Kbps)**	**Cost. Mens.**
1	59	317	900
2	201		900
3	423		900
4	585		900
5	771	1010	1300
6	908		1300
7	1094		1300
8	1268		1300
9	1418	1660	1500
10	1603		1500
11	1741		1500
12	1879		1500
Costo Anual (USD/año)			**14800**

Tabla C.14. Detalle de costos del enlace al NAP para el primer año

SEGUNDO AÑO			
Mes	**AB Calculado al NAP**	**AB Presupuest. (Kbps)**	**Cost. Mens.**
13	2016	2190	1490
14	2142		1490
15	2244		1490
16	2358		1490
17	2459	2630	1582
18	2585		1582
19	2675		1582
20	2801		1582
21	2890	3061	1654
22	3016		1654
23	3118		1654
24	3220		1654
Costo Anual (USD/año)			**18904**

Tabla C.15. Detalle de costos del enlace al NAP para el segundo año

TERCER AÑO			
Mes	AB Calculado al NAP	AB Presupuest. (Kbps)	Cost. Mens.
25	3321	3477	1725
26	3423		1725
27	3537		1725
28	3626		1725
29	3728	3881	1820
30	3830		1820
31	3932		1820
32	4033		1820
33	4135	4288	1848
34	4237		1848
35	4339		1848
36	4440		1848
Costo Anual (USD/año)			21571

Tabla C.16. Detalle de costos del enlace al NAP para el tercer año

CUARTO AÑO			
Mes	AB Calculado al NAP	AB Presupuest. (Kbps)	Cost. Mens.
37	4530	4674	1910
38	4632		1910
39	4710		1910
40	4823		1910
41	4889	5033	1960
42	4991		1960
43	5093		1960
44	5158		1960
45	5272	5407	2008
46	5350		2008
47	5463		2008
48	5541		2008
Costo Anual (USD/año)			23512

Tabla C.17. Detalle de costos del enlace al NAP para el cuarto año

PROYECCIÓN ANUAL DE LOS INGRESOS DEL ISP

Los siguientes cálculos han sido realizados tomando como base las tarifas indicadas en el capítulo V, es decir, una tarifa plana de 11 USD mensuales por cada usuario *dial-up* y 278 USD mensuales por cada usuario corporativo.

INGRESOS POR USUARIOS *DIAL-UP*

PRIMER AÑO			
MES	# us. *dial-up*	Cuota (USD/mes)	Ingresos (USD)
1	50	11	555
2	102	11	1132
3	300	11	3331
4	499	11	5540
5	698	11	7749
6	897	11	9959
7	1095	11	12157
8	1294	11	14366
9	1493	11	16576
10	1692	11	18785
11	1890	11	20984
12	2089	11	23193
INGRESOS (USD)			134328

Tabla C.18. Ingresos por usuarios dial-up durante el primer año

SEGUNDO AÑO			
MES	# us. *dial-up*	Cuota (USD/mes)	Ingresos (USD)
13	2288	11	25402
14	2487	11	27612
15	2685	11	29810
16	2884	11	32019
17	3083	11	34229
18	3282	11	36438
19	3480	11	38636
20	3679	11	40846
21	3878	11	43055
22	4077	11	45264
23	4275	11	47463
24	4474	11	49672
INGRESOS (USD)			450446

Tabla C.19. Ingresos por usuarios dial-up durante el segundo año

TERCER AÑO			
MES	# us. *dial-up*	Cuota (USD/mes)	Ingresos (USD)
25	4673	11	51881
26	4872	11	54091
27	5070	11	56289
28	5269	11	58498
29	5468	11	60708
30	5667	11	62917
31	5865	11	65115
32	6064	11	67325
33	6263	11	69534
34	6462	11	71744
35	6660	11	73942
36	6859	11	76151
INGRESOS (USD)			**768196**

Tabla C.20. Ingresos por usuarios dial-up durante el tercer año

CUARTO AÑO			
MES	# us. *dial-up*	Cuota (USD/mes)	Ingresos (USD)
37	7058	11	78361
38	7257	11	80570
39	7455	11	82768
40	7654	11	84978
41	7853	11	87187
42	8052	11	89396
43	8250	11	91595
44	8449	11	93804
45	8648	11	96013
46	8847	11	98223
47	9045	11	100421
48	9244	11	102630
INGRESOS (USD)			**1085946**

Tabla C.21. Ingresos por usuarios dial-up durante el cuarto año

INGRESOS POR USUARIOS CORPORATIVOS

PRIMER AÑO			
MES	# us. corporat.	Cuota (USD/mes)	Ingresos (USD)
1	4	278	1112
2	15	278	4169
3	30	278	8338
4	40	278	11117
5	52	278	14453
6	60	278	16676
7	72	278	20011
8	83	278	23068
9	92	278	25570
10	104	278	28905
11	112	278	31129
12	120	278	33352
INGRESOS (USD)			217900

Tabla C.22. Ingresos por usuarios corporativos durante el primer año

SEGUNDO AÑO			
MES	# us. corporat.	Cuota (USD/mes)	Ingresos (USD)
13	128	278	35575
14	135	278	37521
15	140	278	38911
16	146	278	40578
17	151	278	41968
18	158	278	43913
19	162	278	45025
20	169	278	46971
21	173	278	48082
22	180	278	50028
23	185	278	51418
24	190	278	52807
INGRESOS (USD)			532798

Tabla C.23. Ingresos por usuarios corporativos durante el segundo año

TERCER AÑO			
MES	# us. corporat.	Cuota (USD/mes)	Ingresos (USD)
25	195	278	54197
26	200	278	55587
27	206	278	57254
28	210	278	58366
29	215	278	59756
30	220	278	61145
31	225	278	62535
32	230	278	63925
33	235	278	65314
34	240	278	66704
35	245	278	68094
36	250	278	69483
INGRESOS (USD)			742360

Tabla C.24. Ingresos por usuarios corporativos durante el tercer año

CUARTO AÑO			
MES	# us. corporat.	Cuota (USD/mes)	Ingresos (USD)
37	254	278	70595
38	259	278	71985
39	262	278	72819
40	268	278	74486
41	270	278	75042
42	275	278	76432
43	280	278	77821
44	282	278	78377
45	288	278	80045
46	291	278	80879
47	297	278	82546
48	300	278	83380
INGRESOS (USD)			924406

Tabla C.25. Ingresos por usuarios corporativos durante el cuarto año

ANEXO D

DSS: *Digital Signature Standard*; Estándar de Firmas Digitales

DUAL: *Diffusing Update Algorithm*; Algoritmo de Difusión de Actualización

EGP: *Exterior Gateway Protocolo*; Protocolo de Pasarela Exterior

EIGRP: *Enhanced Interior Gateway Routing Protocol*; Protocolo de Enrutamiento de Pasarela Interior Mejorado

FTP: *File Transfer Protocol;* Protocolo de Transferencia de Archivos

GIX: *Global Internet eXchange;* Intercambio de Internet Global

HTML: *Hyper Text Mark Lenguage*; Lenguaje de marcado de hipertexto

HDSL: *High-bit-rate Digital Subscriber Line*; Línea Digital de Abonado de Alta Velocidad de Bit

HINFO: *Host Information;* Información de *Host*

HTTP: Hyper Text Transport Protocol; Protocolo de transporte para hypertextos

IDEA: *Internacional Data Encryption Algorithm;* Algoritmo Internacional de Encriptación de Datos

IGP: *Interior Gateway Protocol*; Protocolo de Pasarela Interior.

IGRP: *Interior Gateway Routing Protocol*; Protocolo de Enrutamiento de Pasarela Interior

IMAP4: *Internet Message Access Protocol versión 4;* Protocolo de Acceso de Mensajes de Internet versión 4

ISDN: *Integrated Services Digital Network*; Red Digital de Servicios Integrados

ISP: *Internet Service Provider;* Proveedor de Servicios de Internet

LSA: *Link State Advertisement*; Notificación del Estado de Enlace

LSD: *Link State Database*; Base de datos del Estado de Enlace

LSP: *Link State Packet*; Paquete de Estado de Enlace

LSR: *Label Switching Router*, *Router* de Conmutación de Etiquetas

LSU: *Link State Update;* Actualización del Estado del Enlace

MPLS: *Multiprotocol Label Switching*; Conmutación de etiquetas multiprotocolo

MX: *Mail Exchanger*; Intercambiador de correo

NAP: *Network Access Point;* Punto de Acceso a la Red

NAS: *Network Access Servers*; Servidor de acceso de red

NNTP: *Network News Transfer Protocol*; Protocolo de Transferencia de Noticias de Red

NOC: *Network Operation Center*; Centro de Operación de la Red

NRT-VBR: *Real Time Variable Bit Rate*; Tasa de Bit.Variable en Tiempo no Real

OSPF: *Open Shortest Path First*; Primero la Ruta más corta Disponible

PAP: *Password Authentication Protocol;* Protocolo de verificación de contraseña

PGP: *Pretty Good Privacy*; Privacía Bastante Segura

PoP: *Point of Presence*; Punto de Presencia

PPN: *Protocol for Payment Negotiation*; Protocolo para la negociación de Pagos

PPP: *Point to Point Protocol*; Protocolo Punto a Punto

PRI: *Primary Rate Interface*; Interfaz de Velocidad Primaria

PSTN: *Public Switched Telephone Network*; Red Telefónica Pública Conmutada

QoS: *Quality of Service;* Calidad de servicio

RIB: *Routing Information Bases*; Bases de información de Encaminamiento

RIP: *Routing Internet Protocol*; Protocolo de Enrutamiento Interior

RIPv2: *Routing Information Protocolo version 2*; Protocolo de Información de Enrutamiento versión 2

RSVP: *Resource Reservation Protocol*; Protocolo de reservación de recursos

RT-VBR: *Real Time Variable Bit Rate*; Tasa de Bit Variable en Tiempo Real

S/MIME: *Secure/Multipurpose Internet Mail Extensions*; Extensiones Multipropósito de Correo de Internet Seguro

***SDSL**: Symmetric Digital Subscriber Lline*; Línea Digital de Abonado Simétrica

SET: *Secure Electronic Transactions*; Transacciones Electrónicas Seguras

SLA: *Service Level Agreement;* Contrato de nivel de servicio

SLIP: *Serial Line Interface Protocol*; Protocolo de Interconexión de Líneas Serie

SMTP: *Simple Mail Transfer Protocol*; Protocolo de Transferencias de correo

SNMP: *Simple Network Management Protocol*; Protocolo para la Administración Simple de una Red

SPF: *Shortest Path First*; Primero la ruta más corta

SSL: *Secure Sockets Layer*; Nivel de Conexiones Seguras

Tc: *Committed measurement interval*; Intervalo de Observación

TCP/IP: *Transmission Control Protocol / Internet Protocol*; Protocolo de Control de Transmisión / Protocolo Internet

TOS: *Tipe of Service*; Tipo de servicio

TTL: *Time to Live*; Tiempo de vida

UBR: *Unspecified Bit Rate*; Tasa de Bit no especificada

REFERENCIAS BIBLIOGRÁFICAS

- http://ispltd.com/howto/
  How to Become an ISP
- http://ispltd.com/howto/eq-latout.html
  How to Become an ISP
- http://isp-planet.com/business/requiem.html
  Requiem for an ISP.
- http://it.aut.alcala.es/antonio/CD/Tema8.pdf
  QoS
- http://it.aut.alcala.es/josema/rc_teleco/OSPF.pdf
  Protocolos de Enrutamiento
- http://lovecraft.die.udec.cl/~jorge/apuntes/node1.html
  Protocolos de Ruteo Exterior.
- http://mmm.upc.es/moliver/TELECOM2000Oral29up.pdf
  QoS.
- http://pisuerga.inf.ubu.es/jmsd/comunicaciones/C1/C1-8/C1-8.html#Las_claves_de_la_tecnologia_TCPIP
  TCP/IP
- http://ww3com.com/nsc/800606.html
  RDSI y Redes de Datos (de 3COM)
- http://www.abcdatos.com/tutoriales/comunicaciones.html
  Comunicaciones
- http://www.amazing.com.internet.htm
  The Internet Provider (FAQ)
- http://www.arrakis.es/~val/curs/SERV/INET/TECNIC.htm
  Funcionamiento de Internet
- http://www.canalti.com/magazine/1098/redescap1.cfm?id=1098/redescap1&clav=curso%20OR%20redes%20OR%20LAN%20OR%20WAN
  Curso de Redes.
- http://www.cicei.ulpgc.es/gsi/tut_tcpip/3376ch1.html
  Tutorial y Descripción Técnica de TCP/IP.
- http://www.cicei.ulpgc.es/gsi/tut_tcpip/3376fm.html
  Protocolos de Encaminamiento Interior.

- http://www.cis.ohio-state.edu/htbin/rdc/rfc0791.html
  Protocolo Internet
- http://www.cis.ohio-state.edu/htbin/rdc/rfc0793.html
  Transmission Control Protocol
- http://www.cis.ohio-state.edu/htbin/rdc/rfc1771.html
  Border Gateway Protocol (BGP-4)
- http://www.cis.ohio-state.edu/htbin/rdc/rfc1772.html
  Application of the Border Gateway Protocol in the Internet
- http://www.cis.ohio-state.edu/htbin/rdc/rfc1773.html
  Experience with the BGP- 4 Protocol
- http://www.cis.ohio-state.edu/htbin/rdc/rfc1774.html
  BGP-4 Protocol Analysis.
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm
  Internetworking Technology Overview.
- http://www.cisco.com/warp/public/103/eigrp-toc.html
  Enhanced Interior Gateway Routing Protocol.
- http://www.cisco.com/warp/public/103/index.shtml
  IGRP/EIGRP Technical Tips.
- http://www.cs.virginia.edu/~knabe/iic3512/apuntes_7.html
  Nivel de Red.
- http://www.cyclades.com/solutions/techtalk/techtalk01.htm
  What do I need to be an ISP?
- http://www.dcc.uchile.cl/~jpiquer/Extension/Postitulo/45.html
  Protocolos de Enrutamiento.
- http://www.die.udec.cl/~redes/apuntes/myapuntes.pdf
  Apuntes de Redes.de Datos
- http://www.dis.eafit.edu.co/areas/telematica/online/introredes/arqRedes.pdf
  Redes y Protocolos de Comunicaciones
- http://www.faqs.org/rfcs/rfc1583.html
  RFC 1583: OSPF versión 2.
- http://www.faqs.org/rfcs/rfc1721.html
  RFC 1721: RIP versión 2 *Protocol Analysis.*

- http://www.faqs.org/rfcs/rfc1771.html
  RFC 1771: *A Border Gateway Protocol 4* (BGP-4).
- http://www.icontec.org.co/basesdatos/nor_software/ntc4536.pdf
  Tecnología de la Información. QoS. Estructura.
- http://www.ldc.usb.ve/~redes/Topicos_de_Redes/node1.html
  Redes de Computadoras (CI-4831)
- http://www.index.mis.net/kanti/3.html
  Bussines Opportunities on the Net.
- http://www.index.mis.net/kanti/4.html
  Assessing your Market Presence.
- http://www.index.mis.net/kanti/6.html
  Choosing a location and connection.
- http://www.insflug.org/COMOs/conceptos-de-redes-COMO/conceptos-de-redes-COMO-1.html
  Conceptos de Redes
- http://www.internet.com/sections/isp.html
  Libro ISP-*Planet.*
- http://www.ipv6.ru/docs/EBSCO/fulltext26.htm
  Routing Toward the Future.
- http://www.isa.uniovi.es/docencia/redes/tema6.pdf
  El Protocolo TCP/IP
- http://www.it.uc3m.es/~prometeo/rsc/apuntes/index.html
  Encaminamiento.
- http://www.itpapers.com
  ISP
- http://www.jazztel.com/esp/rincon/pdf/capítulo4.pdf
  Tecnologías de Transmisión.
- http://www.lacnic.org/draft_politicas.pdf
  Políticas de Administración de Recursos.
- http://www.ldc.usb.ve/~redes/Temas/Tema.20/index.html
  Protocolos de Ruteo Exterior.