# ESCUELA POLITÉCNICA NACIONAL

## FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

## REDISEÑO DE LA RED DEL ISP READYNET CIA. LTDA., PROCEDIMIENTO PARA CONVERTIR AL ISP EN UN SISTEMA AUTÓNOMO

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

**FERNANDO ANDRÉS MOYA LEIMBERG**
**fercho_aml@yahoo.es**

**DIRECTOR: M.Sc. MARÍA SOLEDAD JIMÉNEZ**
**maria.jimenez@epn.edu.ec**

**Quito, Septiembre 2009**

# DECLARACIÓN

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

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

Fernando Andrés Moya Leimberg

# CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Fernando Andrés Moya Leimberg, bajo mi supervisión.

María Soledad Jiménez, M.Sc.
DIRECTOR DE PROYECTO

# AGRADECIMIENTO

Principalmente a Dios por darme los medios para seguir creciendo como ser humano; a mis padres, por su esfuerzo, dedicación y amor, la base fundamental para lograr este objetivo.

A mi hermano, por su amistad, apoyo y aguante desde el momento en el que llegó a este mundo.

A la mujer que amo, por su paciencia, amor y ejemplo.

A los verdaderos amigos y sus respectivas familias que siempre me abrieron las puertas para tratarme como un miembro más, en los buenos, pero sobre todo, en los malos momentos. Y aún cuando no frecuentemos, el sentimiento sigue palpitante hacia todos ustedes.

Al resto de mi familia, que fueron parte de los medios que Dios me entregó para culminar la carrera universitaria. En especial a mis abuelitos y tíos.

A Mireya, Soledad, Carlos, Alex, Sabrina, César y Paúl, por su amistad, apertura y confianza en ReadyNet Cia. Ltda.

No puedo decir que el 100% de los profesores que tuve aportaron para mi desarrollo profesional, pero si puedo hablar de muchos que influyeron e inyectaron no solo conocimientos, sino valores, en especial María Soledad Jiménez, Pablo Hidalgo, Iván Bernal y Soraya Sinche.

Sinceramente,

Fernando Andrés Moya Leimberg

# DEDICATORIA

Este trabajo está dedicado a ese ser que acabó de llegar a mi vida, Esteban Javier, mi sobrino.

Para “Papi Julio”, por su eterna presencia en mi vida y corazón.

A Fernando Moya Rueda y Mónica Leimberg Sarmiento, por su legado de conocimientos, valores y porque si no hubieran sido mis padres, posiblemente no estaría escribiendo estas palabras.

Para Ibeth Dávila, por sus cualidades y defectos, el motor de todo lo que vivo.

Fernando Andrés Moya Leimberg

# CONTENIDO

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# RESUMEN

El mercado de los servicios de valor agregado de Internet en el Ecuador, se encuentra totalmente concentrado en ciudades como Quito y Guayaquil, forzando a los proveedores de servicios de Internet en dichas regiones a una mejora constante.

El presente proyecto analiza la red del ISP ReadyNet Cia. Ltda, propone el rediseño de la red de borde, acceso y distribución del ISP y especifica el procedimiento necesario para que el ISP se registre en el Internet como Sistema Autónomo.

Los distintos objetivos del presente proyecto, se desarrollan en cuatro capítulos que presentan los siguientes contenidos:

El primer capítulo describe de manera eficiente y con la mayor discreción posible la situación actual de la red del ISP.

El segundo capítulo especifica definiciones y protocolos de enrutamiento utilizados en un Sistema Autónomo, que permitirán realizar una selección de parámetros que influyan en un nuevo diseño físico y lógico de la red del ISP.

El tercer capítulo presenta algunas alternativas de diseño para que cada uno de los módulos de red, crezcan sin problemas, en base a un dimensionamiento para los próximos 5 años.

El cuarto capítulo define el procedimiento que el ISP debe seguir para anunciar sus redes y servicios como Sistema Autónomo, para la implementación del diseño y para la migración de redes y servicios en caso de que decida obtener un prefijo IP del RIR (*Regional Internet Registries*), correspondiente.

El proyecto finaliza presentando conclusiones obtenidas en el desarrollo del mismo y presentando recomendaciones relacionadas.

# PRESENTACIÓN

El campo de acción y mercado objetivo de los proveedores de servicios de Internet en el Ecuador ha cambiado drásticamente en los últimos años. La tendencia latinoamericana de accesos al Internet de usuarios finales de algunos cientos de miles de bits por segundo, obliga a los operadores de red a buscar prever el impacto de dichos cambios en sus redes.

A nivel mundial, hace no menos de 10 años, un ISP como parte de la aprobación de su funcionamiento en el Internet debía adquirir recursos como un Número de Sistema Autónomo y bloques de direcciones IPv4, recursos que deben ser controlados actualmente dado el inminente agotamiento de los bloques de direcciones IPv4.

Los ISPs deben tener cierta independencia a la hora de seleccionar su salida al Internet, ya sea por costos o facilidad, dicha independencia se logra únicamente siendo una entidad que publique la forma de alcanzar sus redes IP de manera autónoma y única, sin la dependencia o el temor de que cuando se desea cambiar de proveedor, tiene que recurrir a trabajos tediosos de migración de todo el esquema de direccionamiento de sus clientes y de los servicios que el ISP publique en el Internet.

El diseño presentado en este proyecto, permitirá al ISP tomar decisiones a corto plazo que influyan directamente en su capacidad de brindar nuevos servicios y en soportar un tránsito eficiente de paquetes IP dentro de su red y fuera de su red. Dicho diseño se basó en proyecciones anuales de acuerdo al comportamiento del mercado en los últimos años y a la participación del ISP en el mercado con el que cerró el 2008.

El proceso de la migración de redes y servicios del ISP se presenta en este proyecto especificando responsables, tiempos, duraciones y una ruta crítica para el cumplimiento de las tareas asignadas.

# CAPÍTULO 1

# 1 ANÁLISIS DE LA SITUACIÓN ACTUAL DEL ISP

## 1.1 INTRODUCCIÓN

Readynet Cia. Ltda. tiene ya casi 10 años (octubre 2000) en el mercado de los prestadores de servicio de Internet. Cuenta actualmente con un aproximado de 300 usuarios de acceso telefónico de marcado, y 300 usuarios de banda ancha con accesos DSL (*Digital Subscriber Line*) y de radio, maneja dos salidas de Internet para la totalidad de sus usuarios y la granja de servidores. Está a cargo de 9 prefijos de direcciones IP con subredes de máscara de 24 bits cuyos dueños son los sistemas autónomos registrados de los proveedores de Internet que brindan el acceso internacional al ISP.

En el año 2007 las estadísticas mostraban 270 usuarios de acceso banda ancha (entre DSL y radio). Aún cuando el número de clientes no ha crecido, el mercado y la masificación de otros proveedores como CNT (Corporación Nacional de Telecomunicaciones), Suratel, y la creciente demanda de accesos brindados por los operadores de telefonía celular, obligaron prácticamente a duplicar la capacidad de acceso de los clientes por lo que la capacidad inicial de equipos y en algunos casos de servidores fue quedando obsoleta para toda la carga de tráfico generado desde el usuario final. Este aumento es normal, ya que en otros países de América Latina, como Chile, Brasil y Argentina, los accesos brindados al usuario final son de capacidades de cientos de miles de bits por segundo.[1]

Se espera que para los próximos años, Ecuador esté en esa misma situación a precios mucho más accesibles con respecto a los actuales.

[1] Datos obtenidos de usuarios de países como Chile, Argentina y Brasil. Donde en Chile operadores como VTR ofrecen 4Mbps a 45 USD. En Argentina, Coopsur, ofrece 2 Mbps a 26,73 USD y en Brasil, el operador Speedy, ofrece 1 Mbps a 35 USD. xpertin18@managerzone.com; marucha2004@managerzone.com; rj_moraes@managerzone.com

## 1.2 DESCRIPCIÓN DE LA RED DE BORDE[33][34]

El ISP cuenta con dos accesos que delimitan el dominio o injerencia en administración técnica de los enlaces. Uno al que se llamará PROVEEDOR A, y otro al que se llamará PROVEEDOR B. Ambos proveedores brindan un acceso a su backbone a través de fibra óptica, y la capacidad contratada actualmente en ambos proveedores cuenta con cerca de 17 Mbps. La Figura 1.1 muestra un detalle de la red de borde actual del ISP.

### 1.2.1 PROVEEDOR DE BORDE A

El PROVEEDOR A entrega un anillo redundante de Fibra para que en caso de que exista una ruptura de ese enlace, automáticamente suba el otro hilo que tiene circuitos distintos. Tanto los conversores de fibra como el switch son de propiedad del proveedor y está conectado al router de Borde A que actualmente maneja 3 redes IP con máscara de 24 bits, donde se tiene contratada una capacidad de 7 Mbps. El router de borde A, propiedad de ReadyNet, maneja dos interfaces Ethernet, uno para la conexión al proveedor y otro para la red de distribución, por ende la capacidad en cada uno de los enlaces no puede superar los 10 Mbps teóricos del estándar IEEE 802.3i (10BaseT)[1].

El router de borde A (Cisco 2611), tiene un procesador MPC860 con 28672/4096 Kbytes de memoria, 2 interfaces Ethernet/IEEE 802.3, 2 interfaces Seriales, 32 Kbytes de memoria no volátil, 8192 Kbytes de memoria flash y un sistema operativo (C2600-I-M-12.2.26) que ofrece, entre otras, las siguientes características:

- Configuración básica y especial de ambientes de Autenticación, Autorización y Registro AAA (*Authentication, Authorization, Accounting*).
- Listas de acceso ACL (*Access Lists*).

[1] IEEE (*Institute of Electrical and Electronic Engineer*), es una entidad encargada de estandarización de protocolos en las ramas de la Ingeniería Eléctrica y Electrónica, famosa por los estándares de la familia 802, definidos para ambientes LAN.

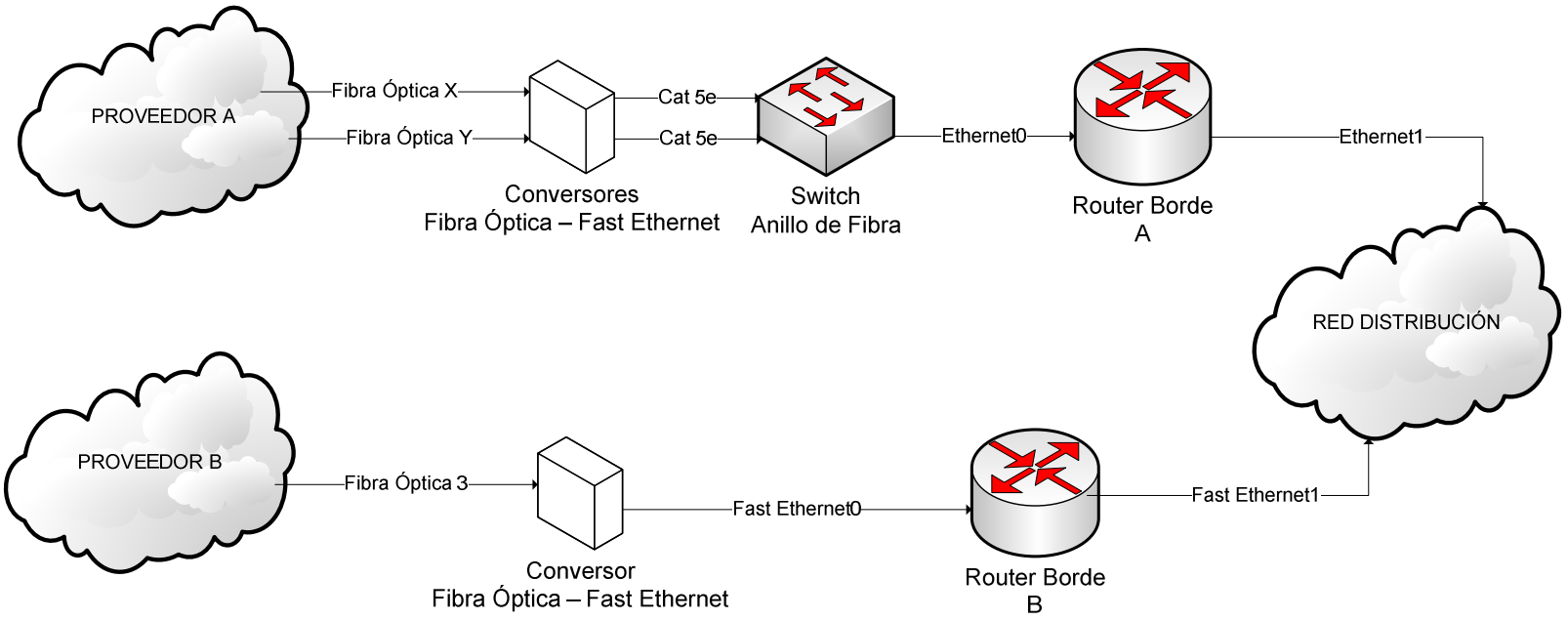


Figura 1.1 Esquema de la Red de Borde, Elementos Activos

Donde: *Fibra Óptica x* y *Fibra Óptica y* son entregadas por el Proveedor A para el anillo redundante en la salida internacional.

*Fibra Óptica 3*, es el tercer hilo de fibra de los 6 hilos tendidos por el Proveedor B donde solo 4 están fusionados.

- Protocolo de Resolución de Nombres ARP (*Address Resolution Protocol*).
- Auto instalación de interfaces LAN con DHCP (*Dynamic Host Configuration Protocol*).
- Protocolo de Salida de Borde BGP (*Border Gateway Protocol*).
- BGP4 con soporte de múltiples caminos, filtro de prefijos y mapas internos.
- Señalización de E1 por canales tipo CAS (*Channel Associated Signaling*).
- IEEE 802.1p.
- Búsqueda de caracteres en línea de comandos.
- Listas de acceso comentables.
- Soporte para Políticas de Servicio Abiertas y Comunes COPS (*Common Open Policy Service*) para el Protocolo de Reservación de Recursos RSVP (*Resource ReSerVation Protocol*).
- Cliente DHCP.
- Cliente DHCP de un proxy.
- Soporte del agente de relay para interfaces no enumerados.
- Servidor DHCP.
- Marcado bajo demanda y autenticación.
- Enrutamiento X.25 basado en Sistema de Resolución de Nombres DNS (*Domain Name System*).
- Protocolo de enrutamiento de salida exterior EGP (*Exterior Gateway Protocol*).
- Protocolo de enrutamiento de salida interior mejorado EIGRP (*Enhanced Interior Gateway Routing Protocol*).
- Encapsulación y conmutación del protocolo Frame Relay.
- Encapsulación de enrutamiento genérico GRE (*Generic Routing Encapsulation*).
- Conformador Genérico de Tráfico GTS (*Generic Traffic Shapping*).
- Mitad Router Mitad Bridge para CPP (*Combinet Packet Protocol*) y PPP (*Point to Point Protocol*).
- Seguridad HTTP (*Hyper Text Transfer Protocol*).
- IGMP (*Internet Group Management Protocol*) versión 1 y 3.

- Protocolo de Enrutamiento de Salida Interior IGRP (*Interior Gateway Routing Protocol*).
- Enrutamiento IP.
- Definición de parámetros SLA (*Service Level Agreements*).
- Protocolo de la Red Digital de Servicios Integrados ISDN (*Integrated Services Digital Network*).
- PPP multienlace.
- Protocolo OSPF (*Open Shortest Path First*).
- Protocolos PAP (*Password Authentication Protocol*) y CHAP (*Challenge Handshake Authentication Protocol*).
- PPP sobre ATM (*Asynchronous Transfer Mode*).
- PPP sobre Frame Relay.
- Soporte para RADIUS (*Remote Access Dial-In User Service*).
- SNMP (*Simple Network Management Protocol*) hasta la tercera versión.
- Protocolo de Árbol Contenedor STP (*Spanning Tree Protocol*).
- Registro de uso de listas de acceso.
- TACACS+ (*Terminal Access Controller Access Control System*).
- Bridging transparente.
- Servicio de plantillas de interfaces virtuales.
- Perfiles virtuales.
- Protocolo X.25 y sus características principales.

### 1.2.2 PROVEEDOR DE BORDE B

El PROVEEDOR B entrega a través de uno de los cuatro hilos de fibra óptica fusionadas (Fibra Óptica 3) conectado a un conversor de medios que permite utilizar la capacidad de 10 Mbps, contratada con dicho proveedor en la interfaz Fast Ethernet del router de Borde B. La otra interfaz del Router de Borde B, propiedad del proveedor B y administrado por el ISP, maneja 6 redes IP con máscara de 24 bits y se conecta a la red de distribución con una capacidad máxima de 100 Mbps teóricos del estándar IEEE 802.3u (100BaseTX).

El router de borde B (Cisco 1841), tiene un procesador de 114688/16384 Kbytes de memoria, 2 interfaces FastEthernet, 191 Kbytes de memoria no volátil, 31360 Kbytes de memoria flash y un sistema operativo (C1841-IPBASE-M-12.4.1c) que ofrece entre otras, las siguientes características:

- Configuración básica y especial de ambientes de Autenticación, Autorización y Registro (AAA).
- Listas de acceso (ACL).
- Protocolo de Resolución de Nombres (ARP).
- Auto instalación de interfaces LAN con DHCP.
- Señalización de E1 por canales tipo CAS.
- IEEE 802.1p.
- Búsqueda de caracteres en línea de comandos.
- Listas de acceso que permiten comentarios.
- Soporte para Políticas de Servicio Abiertas y Comunes (COPS) para el Protocolo de Reservación de Recursos (RSVP).
- Cliente DHCP.
- Cliente DHCP de un proxy.
- Soporte del agente de relay para interfaces no enumerados.
- Servidor DHCP.
- Marcado bajo demanda y autenticación.
- Enrutamiento X.25 basado en DNS.
- Señalización E1 R2.
- Protocolo de enrutamiento de salida exterior (EGP).
- Protocolo de enrutamiento de salida interior mejorado (EIGRP).
- El protocolo Frame Relay, su encapsulación y conmutación.
- Encapsulación de enrutamiento genérico (GRE).
- Conformador Genérico de Tráfico (GTS).
- Mitad Router Mitad Bridge para CPP y PPP.
- Seguridad HTTP.
- IGMP versión 1 y 3.
- Protocolo de Enrutamiento de Salida Interior (IGRP).

- Enrutamiento IP.
- Definición de parámetros SLA.
- Protocolo ISDN.
- PPP multienlace.
- Protocolo OSPF.
- Protocolos PAP y CHAP.
- PPP sobre ATM.
- PPP sobre Frame Relay.
- RADIUS.
- SNMP hasta la tercera versión.
- Protocolo Spanning Tree (STP).
- Registro de uso de listas de acceso.
- TACACS+
- Bridging transparente.
- Servicio de plantillas de interfaces virtuales.
- Perfiles virtuales.
- Protocolo X.25 y sus características principales.

## 1.3 DESCRIPCIÓN DE LA RED DE ACCESO [32][33][34]

El ISP cuenta con 3 proveedores de última milla, para un total de 6 accesos al usuario final. Estos proveedores se denominarán PROVEEDOR C, D y E.

El PROVEEDOR D y el PROVEEDOR E permiten llegar al usuario final con enlaces inalámbricos, el acceso a cada uno de los usuarios finales depende de los nodos disponibles de los proveedores, en algunos casos usando tecnología del estándar IEEE 802.11g para exteriores, en otros casos usando IEEE 802.16f.

El PROVEEDOR C llega con tres tipos de acceso, el primero es a través de la red ATM que poseen y el otro se da a través de un acceso MetroEthernet, que actualmente transporta clientes en capa 3 y a través del router de borde del

proveedor B, segmentando los enlaces a través de etiquetas IEEE 802.1q. El tercer acceso es a través de dos PBX que reciben los accesos de marcado telefónico.

La Figura 1.2 describe los elementos activos que forman parte de la red de acceso del ISP.

### 1.3.1 PROVEEDOR DE ACCESO C

El PROVEEDOR C de acceso, vendría a ser el mismo que el PROVEEDOR B de borde, compartiendo el tercer hilo de fibra de una bandeja de 6 hilos de los cuales 3 están fusionados u operativos y llegan hasta el ISP. El acceso ATM de este ruteador, usa dos hilos de fibra (1 y 2), y permite llegar hacia cada cliente a través de parámetros básicos ATM (PVC, VPI/VCI)[1] en subinterfaces creados dentro del ruteador, propiedad del ISP con una tarjeta T3/E3, conectado a la red de distribución a través de un puerto Ethernet, pudiendo en un futuro convertirse en un cuello de botella, ya que los 45 Mbps de capacidad total de los clientes que podrían llegar a través del par de hilos de fibra desde el proveedor C, superan totalmente los 10 Mbps teóricos de dicha tarjeta.

El router ATM de acceso C (Cisco 7206VXR-NPE400-Rev.A), tiene un procesador de 350 MHz, de 491520K/32768 Kbytes de memoria, 8 interfaces Ethernet, 125 Kbytes de memoria no volátil, dos ranuras de disco, con capacidad de 20480 Kbytes y 46976 Kbytes cada uno, con una memoria flash interna de 4096 Kbytes y un sistema operativo (C7200-AEK9-M.12.4.11T) que ofrece entre otras, las siguientes características:

- Configuración básica y especial de ambientes de Autenticación, Autorización y Registro (AAA).

  .

[1] PVC (*Permanent Virtual Channel*) es un parámetro que indica el camino o mapa a seguir para cerrar un circuito ATM entre dos puntos, para lo cual necesita identificador del camino virtual VPI (*Virtual Path Identifier*) y el identificador del canal virtual VCI (*Virtual Channel Identifier*)

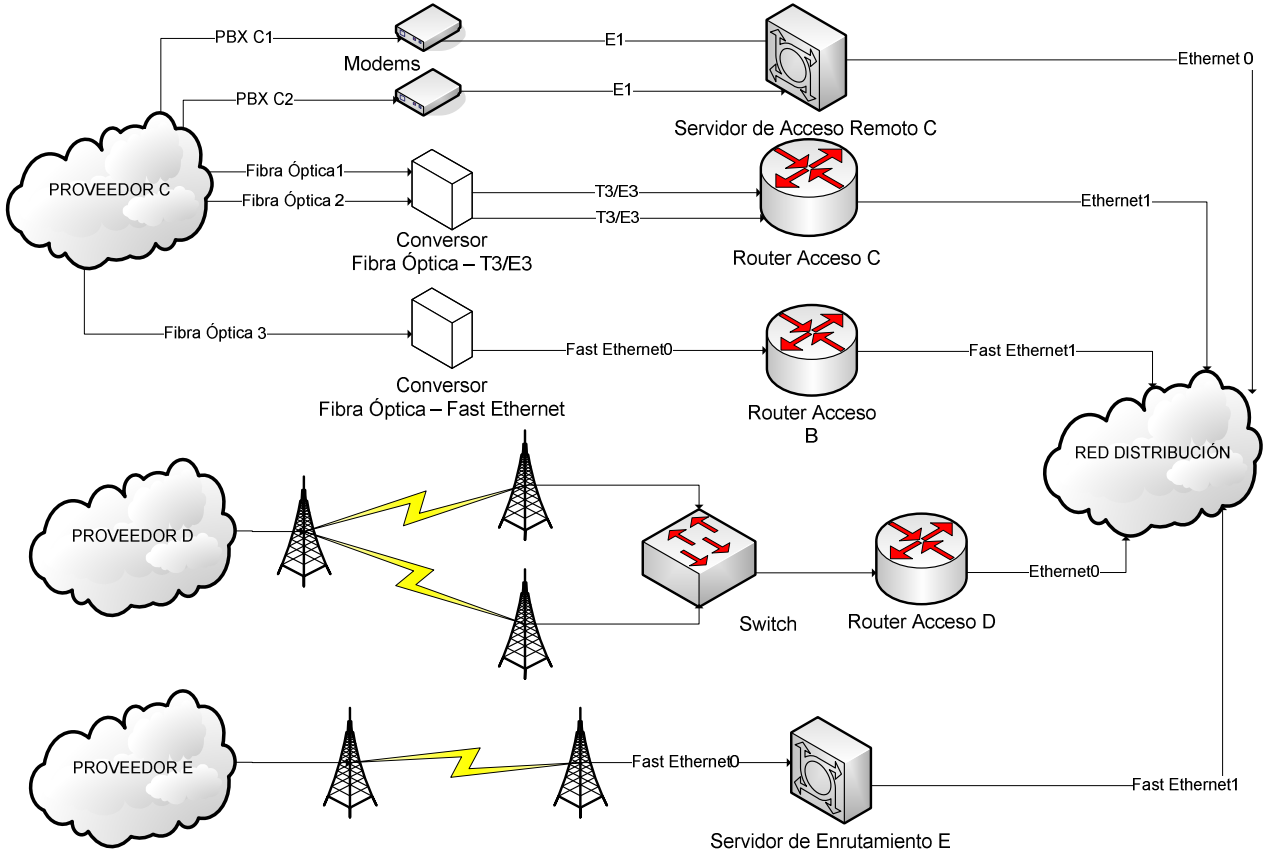


Figura 1.2 Esquema de la Red de Acceso, Elementos Activos

- Capacidad para deshabilitar parámetros de autenticación para entidades pares IPSec
- Protocolo de Salida de Borde BGP.
- Registro de causas de desconexión de redes privadas virtuales de acceso por marcado VPDN (*Virtual Private Dial In Network*).
- BGP4 con soporte de Múltiples Caminos, filtro de prefijos y mapas internos.
- Listas de acceso ACL.
- Conformador de Tráfico Adaptivo ATS (*Adaptive Traffic Shaping*) en Frame Relay para congestión de Interfaces.
- Protocolo de Resolución de Nombres (ARP).
- Estándar de Cifrado Avanzado AES (*Advanced Encryption Standard*).
- Cualquier tipo de transporte sobre MPLS (*Multi Protocol Label Switching*) para Ethernet, ATM tipo AAL5, Frame Relay, HDLC, PPP.
- Auto instalación de interfaces LAN con DHCP.
- Protocolo de Salida de Borde BGP y varios parámetros útiles.
- Señalización de E1 por canales tipo CAS.
- Manipulación de Certificados Digitales.
- IEEE 802.1p.
- Búsqueda de caracteres en línea de comandos.
- Listas de acceso comentables.
- Soporte para Políticas de Servicio Abiertas y Comunes (COPS) para el Protocolo de Reservación de Recursos (RSVP).
- Cliente DHCP.
- Cliente DHCP de un proxy.
- Soporte del agente de relay para interfaces no enumerados.
- Servidor DHCP.
- Marcado bajo demanda y autenticación.
- Enrutamiento X.25 basado en DNS.
- Señalización E1 R2.
- Protocolo de enrutamiento de salida exterior (EGP).
- Protocolo de enrutamiento de salida interior mejorado (EIGRP).
- El protocolo Frame Relay, su encapsulación y conmutación.

- Encapsulación de enrutamiento genérico GRE.
- Conformador de Tráfico Genérico GTS.
- Mitad Router Mitad Bridge para CPP y PPP.
- Seguridad HTTP.
- IGMP versión 1 y 3.
- Protocolo de Enrutamiento de Salida Interior (IGRP).
- Enrutamiento IP.
- Definición de parámetros SLA.
- Protocolo ISDN.
- PPP multienlace.
- Protocolo OSPF.
- Protocolos PAP y CHAP.
- PPP sobre ATM.
- PPP sobre Frame Relay.
- RADIUS.
- SNMP hasta la tercera versión.
- Protocolo STP.
- Registro de uso de listas de acceso.
- TACACS+.
- Bridging transparente.
- Servicio de plantillas[1] de interfaces virtuales.
- Perfiles virtuales.
- Protocolo X.25 y sus características principales.
- Opciones de firewall y de sistema de detección de intrusos.
- Soporte de H.323 y SIP.
- Soporte para túneles basados en 802.1q y soporte de VLANs (*Virtual LAN*) cuando existen puertos FastEthernet.
- Protocolo de intercambio de claves de Internet (IKE) y características funcionales.
- Soporte IS-IS.

[1] Una plantilla, es una estructura que permite separar la forma o estructura de los interfaces, del contenido de cada interfaz.

- Soporte IPv6.
- Soporte Mobile IP.
- Soporte MPLS.
- Soporte NAT.
- Soporte PPPoE.
- Soporte de parámetros de calidad de servicio.
- Implementación de Shell Seguro (SSH) versión 2 y de Copias Seguras (SCP).
- Soporte de enrutamiento y reenvío virtuales VRF (*Virtual Routing and Forwarding*).
- Soporte de balanceo de carga a servidores en distintos interfaces.

Por otro lado ambas PBX permiten a través de dos módems recibir solicitudes de acceso de marcado telefónico, que con ayuda de un servidor RADIUS se establece un máximo de 60 conversaciones simultáneas (2 E1). El servidor de acceso remoto C y los módems son propiedad del ISP.

### 1.3.2 PROVEEDOR DE ACCESO D

El PROVEEDOR D permite tener redundancia a través de dos enlaces apuntando a distintos nodos, de manera que si el enlace principal cae, automáticamente suba el otro enlace. Ambos enlaces trabajan en la banda libre de los 5.8 GHz. Tanto el router de acceso D como las antenas y el switch de redundancia son de propiedad del PROVEEDOR D. En el momento en que el total de enlaces de última milla supere los 22 Mbps de capacidad instalada por el proveedor en ambos enlaces, existiría un cuello de botella en el paso a la red de distribución, ya que el interfaz con el cual se conecta dicho equipo cumple únicamente con la norma IEEE 802.3i. [1]

[1] Los 22 Mbps fueron demostrados en la fase de puesta en marcha de ambos enlaces durante el último cambio de equipos en febrero del 2008 por parte del Proveedor D, según el acta de entrega de dichos equipos.

Dado que el router de acceso D es de propiedad del proveedor, no se puede obtener mayor detalle de las características del hardware y software del equipo, solo se conoce la marca, y se puede conocer muy poco sobre el mismo.

### 1.3.3 PROVEEDOR DE ACCESO E

El PROVEEDOR E, llega directamente a través de una enlace inalámbrico en la banda de los 5.8 GHz. hacia una PC que maneja funciones de enrutamiento y que permiten la comunicación con el proveedor y la red de borde con tarjetas FastEthernet. Tanto las antenas como el servidor de comunicaciones son de propiedad del PROVEEDOR E.

De igual manera por ser propiedad del proveedor E, no se tienen características adicionales de hardware y software del servidor de acceso E.

### 1.3.4 CAPACIDAD DE LOS ENLACES

Las capacidades totales actuales de los clientes de acuerdo a los equipos de acceso donde se conectan se pueden ver en la Tabla 1.1 , que muestra también la capacidad máxima de cada interfaz en cada equipo de acceso:

| PROVEEDOR | | Capacidad Efectiva | Capacidad Máxima del Enlace |
|---|---|---|---|
| C | ATM | 40 Mbps | 44736 Mbps |
| | Metro Ethernet | 8 Mbps | 100 Mbps |
| | DIAL UP PBX1 | 2048 Mbps[1] | 2048 Mbps |
| | DIAL UP PBX2 | 2048 Mbps | 2048 Mbps |
| D | | 3328 Mbps | 22 Mbps |
| E | | 1792 Mbps | 22 Mbps |

Tabla 1.1 Capacidad de los enlaces de última milla. [34]

[1] Al tratarse de dos líneas de acceso telefónico, estamos hablando de que la capacidad máxima de cada enlace según el estándar PCM (*Pulse Code Modulation*) para América es de treinta canales de voz más dos canales de control, dado que por el método de multiplexación en el tiempo, cada canal puede llevar 64 Kbps, la capacidad total de cada PBX es de 2048 Mbps.

Tanto el proveedor D como el proveedor E, garantizan que la totalidad de los enlaces de ultima milla funcionará adecuadamente, mientras no se supere la capacidad de 22 Mbps, de manera que se puede crecer en clientes, sin ningún inconveniente, hasta completar dicho valor. Estos valores fueron determinados según pruebas realizadas previo funcionamiento de los mismos.

La distribución de planes contratados actualmente por los abonados, clientes de ReadyNet Cia.Ltda, junto con la capacidad total requerida para salir hacia el Internet, se muestran en la Tabla 1.2.

| **Planes Contratados** | | |
|---|---|---|
| **Velocidad [Kbps]** | **Cantidad Abonados** | **Capacidad Requerida [Kbps]** |
| 128/64 | 168 | 21504 |
| 256/128 | 56 | 14336 |
| 512/256 | 8 | 4096 |
| 1024/512 | 8 | 8192 |
| 64/64 | 48 | 3072 |
| 128/128 | 8 | 1024 |
| 256/256 | 4 | 1024 |
| dial up | 300 | 4096 |
| **Total** | **600** | **57344** |

Tabla 1.2 Número de abonados, por plan contratado, capacidad requerida [32]

Del total de 57344 Kbps teóricos requeridos de salida de Internet, se debe tomar en cuenta la compartición de los servicios. Donde la distribución con el nivel de compartición de los clientes según el Departamento Comercial del ISP, y la capacidad requerida por nivel de compartición de acuerdo a la capacidad total contratada en últimas millas, se muestra en la Tabla 1.3.

Donde un gran total de 16384 Kbps son necesarios para satisfacer los niveles de acuerdo de nivel de servicio (SLA) contratado por los clientes actualmente.

| Distribución de Planes Contratados Según Nivel de Compartición | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Velocidad [Kbps] | Total Abonados | Número de Abonados 8:1 | Capacidad Requerida Plan 8:1 [Kbps] | Número de Abonados 4:1 | Capacidad Requerida Plan 4:1 [Kbps] | Número de Abonados 2:1 | Capacidad Requerida Plan 2:1 [Kbps] | Número de Abonados 1:1 | Capacidad Requerida Plan 1:1 [Kbps] |
| 128/64 | 168 | 60 | 1024 | 56 | 1792 | 42 | 2688 | 10 | 1280 |
| 256/128 | 56 | 17 | 768 | 24 | 1536 | 10 | 1280 | 5 | 1280 |
| 512/256 | 10 | 8 | 512 | 0 | 0 | 2 | 512 | 0 | 0 |
| 1024/512 | 8 | 4 | 1024 | 4 | 1024 | 0 | 0 | 0 | 0 |
| 64/64 | 46 | 16 | 128 | 16 | 256 | 8 | 256 | 6 | 384 |
| 128/128 | 8 | 3 | 128 | 4 | 128 | 0 | 0 | 1 | 128 |
| 256/256 | 4 | 0 | 0 | 4 | 256 | 0 | 0 | 0 | 0 |
| TOTAL | 300 | 108 | 3584 | 108 | 4992 | 62 | 4736 | 22 | 3072 |
| **Capacidad de Internet Requerida [Kbps]** | | | | | | | | | **16384** |

Tabla 1.3 Total de Capacidad de Internet requerida según planes de compartición de clientes. [32]

## 1.4 DESCRIPCIÓN DE LA RED DE DISTRIBUCIÓN [31][33][34][35]

La red de distribución actualmente permite la conexión entre la red de borde y la red de acceso, así como la conexión con los equipos que brindan los servicios básicos de DNS (*Domain Name System*), HTTP, SMTP (*Simple Mail Transfer Protocol*), POP (*Post Office Protocol*) e IMAP (*Internet Messages Access Protocol*).

La Figura 1.3 muestra la forma en la que se conectan actualmente los equipos activos en la red de distribución.

### 1.4.1 SWITCH A

El switch A (Cisco Catalyst WS-C2950-24), es un switch administrable de 24 puertos Fast Ethernet donde están conectadas directamente las redes de borde, acceso y la red interna que está conectada a través del switch B que es el switch terminal de una cascada de switches existentes y que no son administrables. El switch A cuenta con una memoria no volátil de 16 MB y 8 MB de flash, y un sistema operativo (C2950-I6Q4L2-M.12.1.13.EA1) que ofrece entre otras, las siguientes características:

- Tasa de conmutación en cobre de hasta 6.6 Mpps.

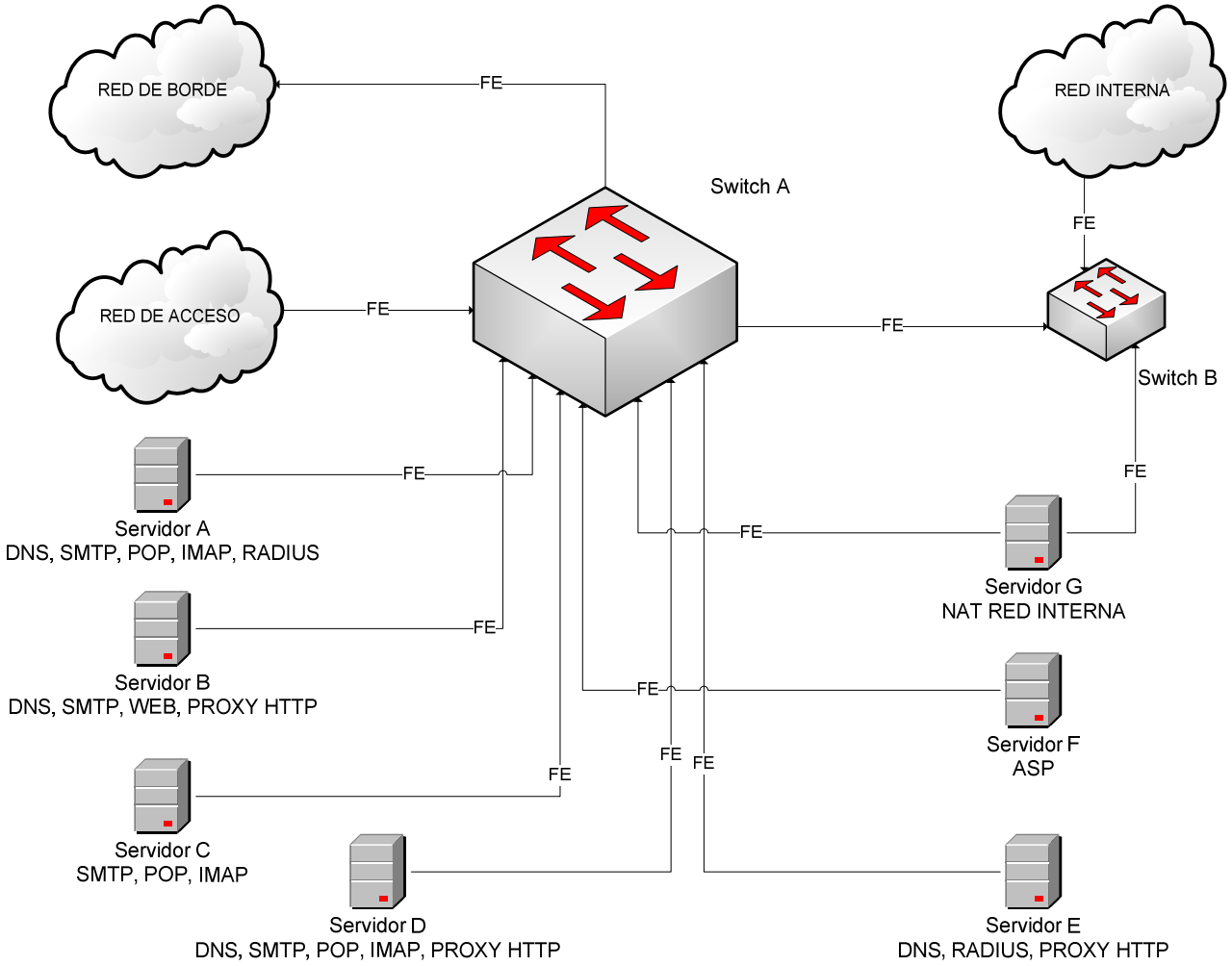


Figura 1.3 Esquema de la Red de Distribución, Equipos Activos

- 32 MB de buffer de memoria compartida para todos los puertos.
- SNMP, versión 1, 2c y 3.
- IEEE 802.1d STP.
- Priorización de clases de servicio IEEE 802.1p.
- IEEE 802.1q VLAN.
- IEEE 802.3i,3u 10BaseT, y 100BaseTX.
- Puerto de Consola de Administración.
- Auto negociación de puertos.
- Soporte para IEEE 802.1x, 1w, 1s.

### 1.4.2 SERVIDOR A

El servidor A es un equipo con 256 MB en memoria RAM, procesador de 733 MHz, y 50 GB de disco, funcionando con un sistema operativo basado en Linux de kernel 2.4. Por obvias razones de hardware, este equipo está siendo ya sacado de producción en servicios como SMTP, POP e IMAP y seguirá funcionando como DNS principal en el esquema de direccionamiento correspondiente al proveedor de borde A y como servidor de autenticación para los usuarios de acceso telefónico RADIUS.

### 1.4.3 SERVIDOR B

El servidor B es un equipo con 512 MB en memoria RAM, con doble procesador de 2.4 GHz. y un disco de 100 GB, funcionando con un sistema operativo basado en Linux de kernel 2.4. Funcionando perfectamente en la actualidad como servidor web de algunos dominios de clientes del ISP y como servidor de contenido para los clientes cuyo esquema de direccionamiento corresponde al del proveedor A. Así como también trabaja como servidor DNS secundario de esa red.

### 1.4.4 SERVIDOR C

El servidor C es un equipo con 2 GB en memoria RAM, con doble procesador de 3 GHz. y un disco duro de 250 GB, funcionando con un sistema operativo basado en Linux de kernel 2.6. Equipo por el cual se ha migrado el procesamiento de correo electrónico del 90% de los dominios que antes se encontraban apuntando al servidor A. Este equipo ejecuta una aplicación antispam y antivirus que permite filtrar y controlar los correos basura de los clientes y los protege además contra amenazas de virus constantes. Este servidor pertenece también al esquema de direccionamiento correspondiente al proveedor A.

### 1.4.5 SERVIDOR D

El servidor D es un equipo con 3 GB en memoria RAM, con doble procesador de 2.5 GHz. y un disco duro de 320 GB, funcionando con un sistema operativo basado en Linux de kernel 2.6. Este equipo funciona como servidor DNS principal de los clientes con esquema de direccionamiento del proveedor B, funciona como servidor de cache de páginas web, así como también se encarga del procesamiento de correo electrónico y filtro de SPAM y virus de la mayoría de los dominios asociados a ese esquema de direccionamiento. Este equipo fue cambiado, ya que antes tenía otras características de hardware.

### 1.4.6 SERVIDOR E

El servidor E es un equipo con 512 MB en memoria RAM, con doble procesador de 2.4 GHz. y un disco duro de 120 GB, funcionando actualmente con un sistema operativo basado en Linux de kernel 2.6. Antiguamente éste era el servidor D, luego de la respectiva migración, funciona como servidor DNS secundario de clientes con esquema de direccionamiento del proveedor B, y como servidor de autenticación para enlaces PPPoE (*Point to Point Protocol Over Ethernet*). Estos

enlaces PPPoE, serán implementados, luego de las pruebas respectivas con el proveedor de acceso C.

### 1.4.7 SERVIDOR F

El servidor F es un equipo de 2 GB en memoria RAM, con doble procesador de 3.0 GHz. y un disco duro de 250 GB, funcionando con un sistema operativo de la familia de servidores de Microsoft. Este equipo permite publicar páginas de servidor activo (ASP) propietarias de Microsoft, por lo que es necesario usar dicho sistema operativo, y es utilizado para clientes que manejan este tipo de desarrollo en aplicaciones web.

### 1.4.8 SERVIDOR G

El servidor G es un equipo con 256 MB en memoria RAM, con procesador de 1.8 GHZ y un disco duro de 60 GB, funcionando con un sistema operativo basado en Linux de kernel 2.4. Este equipo realiza funciones de NAT para la red interna de del ISP, y soporta una base de datos del sistema de facturación y contabilidad de la empresa. En pocas palabras, permite al Departamentos Financiero y Comercial, navegar en el Internet, y al Departamento Técnico, el monitoreo y administración de todos los enlaces y servicios del ISP.

### 1.4.9 CAPACIDAD DE SERVIDORES

El consumo de capacidad promedio para cada servidor en 24 horas, está disponible en la Tabla 1.4. Los datos fueron obtenidos de los gráficos de la Herramienta MRTG disponible en ReadyNet Cia. Ltda.

| Media de Tráfico en 24 horas | |
|---|---|
| Servidor | Capacidad Usada [Kbps] |
| A | 400 |
| B | 400 |
| C | 256 |
| D | 400 |
| E | 230 |
| F | 128 |
| G | 784 |
| TOTAL | 2598 |

Tabla 1.4 Media de Tráfico por servidor en 24 horas. [36]

Tomando en cuenta que se puede tener 8 subredes /27, 16 subredes /28, 32 subredes /29 o 64 subredes /30 por prefijo /24, en la Tabla 1.5 se muestra el plan de direccionamiento del ISP por cada prefijo /24 asignado al ISP:

| | Red /24 | Subdivisión | Bloques | Asignados |
|---|---|---|---|---|
| | 2 | 16 | /27 | 11 |
| | 1 | 16 | /28 | 10 |
| | 1 | 32 | /29 | 25 |
| | 5 | 320 | /30 | 260 |
| TOTAL | 9 | 384 | | 306 |

Tabla 1.5 Plan de Direccionamiento IPv4 del ISP. [37]

Esto implica que bajo la división en subredes realizada, se pueden asignar un total de 384 subredes, ya sea para clientes o para equipos activos. Las 6 subredes asignadas adicionalmente de las 300 para abonados banda ancha con los que cuenta el ISP están distribuidas en 3 para equipos activos y 3 para acceso telefónico de marcado. Se nota claramente que no se optimiza la distribución de direcciones IP y que tranquilamente se podría usar menos bloques IPv4.

La distribución actual de las 9 redes IP con prefijo /24 entregadas actualmente al ISP por módulo de red se encuentra en la Tabla 1.6.

| Sección de Red | Número de redes | Prefijo IP |
|---|---|---|
| Acceso | 9 | /27 |
| | 9 | /28 |
| | 25 | /29 |
| | 260 | /30 |
| Borde | 2 | /27 |
| | 1 | /28 |

Tabla 1.6 Distribución de Prefijos por Red.

La red /28 en la red de borde, fue introducida por una inicial conexión con cobre con el proveedor de borde B, que luego fue reemplazada por la conexión de fibra actual y la correspondiente separación de un bloque /27 del esquema de direccionamiento del proveedor B. Sin embargo, se mantuvo este esquema porque ambos DNSs pertenecen a ese rango de direcciones, y son autoritativos[1] para muchos dominios de clientes.

## 1.5 REQUERIMIENTOS DEL ISP

### 1.5.1 ANTECEDENTES [10]

A inicios del 2007 algunos de los prefijos anunciados por el Sistema Autónomo del Proveedor B cayeron en una lista negra internacional europea llamada UCEPROTECT®. En general, la gran mayoría de listas negras en tiempo real RBL (*Real time Black Lists*), pretenden terminar con prácticas abusivas de SPAM (Correo Electrónico Basura o No deseado) en el Internet. Sin embargo, la RBL de UCEPROTECT®, definitivamente implementa un proceso eficiente en contra de proveedores de Internet y operadores de red que no toman las debidas precauciones y acciones necesarias para detener el SPAM en el Internet. Su método de funcionamiento tiene 3 niveles que se encuentran detallados en su correspondiente página web [10]:

[1] En el esquema jerárquico del Sistema DNS, es necesario especificar al menos dos servidores que mantengan información sobre las zonas de un dominio. Ambos servidores se conocen como servidores autoritativos del dominio.

- El primer nivel, lista o muestra una dirección IP que ha sido detectada por trampas ubicadas en distintos servidores de correo en el Internet. Una vez que una dirección IP ha sido ubicada en esta lista, deberán pasar 7 días desde el último registro en las trampas de SPAM de no recibir ningún otro correo para que automáticamente salga de listas, caso contrario, seguirá en la lista.
- El segundo nivel, se activa cuando al menos 5 direcciones IP de un prefijo /24 han sido listadas.
- El tercer nivel, se activa cuando al menos 10 prefijos /24 o 102 direcciones IP registradas por el Sistema Autónomo están enlistadas, haciendo que todo el Sistema Autónomo sea enlistado. El número puede variar de acuerdo a la cantidad de prefijos que tenga el Sistema Autónomo.

ReadyNet Cia. Ltda., aportó únicamente con 6 direcciones IP para que todo el número de SA del proveedor B sea enlistado; en ese entonces el ISP tenía asignado 4 prefijos /24, y la única solución que encontró el proveedor B fue la de cambiar 2 de los prefijos del ISP en un plazo de 15 días, y así con todos los clientes de dicho proveedor afectados, para dejar de publicar los prefijos en su borde y “eliminar el problema”.

Ventajosamente el Departamento Técnico demostró que esa no era una solución, sino que se debe exigir la implementación de mecanismos que permitan proteger el puerto 25 TCP, tanto en usuarios residenciales como en usuarios corporativos, que no tienen por qué usar ese puerto en el Internet y que generalmente por un virus son usados como generadores de SPAM.

Al pasar los 7 días, los prefijos de ReadyNet, estaban limpios, y se pudo detener la migración, sin embargo, los costos operativos del ISP para dichos cambios, fueron altos en esa semana.

Problema que no se hubiera presentado, si la administración de enrutamiento y prefijos IP, fueran de propiedad de ReadyNet Cia. Ltda., ya que no se hubiera

visto inmiscuido en un problema de seguridad por negligencia administrativa técnica del proveedor de borde B.

### 1.5.2 REQUERIMIENTOS

Aún cuando en el presente proyecto se habla de una distinción física de las Redes de Borde, Acceso y Distribución del ISP, no existe una separación lógica entre la Red de Borde y Distribución ni mucho menos una distinción de la red interna del ISP con la red de monitoreo y control de operación de la red.

El ISP requiere alternativas que permitan integrar dispositivos que brinden nuevos valores agregados a los clientes y una plataforma de red escalable en tipos de acceso y su salida al Internet.

La red debería ser segmentada de manera lógica y física, la autonomía del enrutamiento de sus clientes, y servicios de igual manera. El depender de los proveedores de salida internacional por la administración de los bloques IPv4 asignados, ata de manos decisiones que muchas veces deben ser tomadas en cuestión de horas, tanto a nivel financiero, como a nivel técnico.

El Departamento Técnico del ISP tiene que ingeniarse formas de enrutar la salida al Internet de sus clientes dependiendo de la última milla y de la salida internacional. Muchas veces las soluciones se presentan especificando mapas de enrutamiento en los distintos equipos de acceso.

Los servicios que se encuentran con esquemas de direccionamiento del proveedor A y que reciben una solicitud de clientes del ISP con esquema de direccionamiento del proveedor B necesariamente salen de la red del ISP consumiendo capacidad de Internet que puede ser usada en otras actividades o clientes. De igual manera cuando se invierten las cosas y los servicios con esquema de direccionamiento del proveedor B reciben solicitudes desde clientes con esquema de direccionamiento del proveedor A. Incluso cuando servicios de

clientes desean ser accedidos a través de otros clientes y el esquema de direccionamiento pertenece a un proveedor distinto (A o B), aún cuando se encuentran dentro del mismo equipo de acceso, salen al Internet y regresan.

Como se determinó en la sección 1.3, los equipos de acceso D y E, no son de propiedad del ISP, y el enrutamiento de dichos clientes, implica archivos de configuración en los routers de borde excesivamente grandes, complejos y que consumen gran cantidad de los recursos disponibles en los equipos activos.

Todo esto, remarca la necesidad de ReadyNet Cia. Ltda. a nivel técnico, previa aprobación del departamento de Adquisiciones y Financiero de la empresa lo siguiente:

- Un cambio de la topología física de la red que permita crecer sin problemas al ISP en clientes y capacidad de Internet por al menos 5 años.
- Registrar recursos de Internet que eviten dependencia de los proveedores de salida Internacional.
- Un cambio de la topología lógica de la red que permita implementar mecanismos eficientes de enrutamiento y de acceso a los servicios actuales del ISP, entregando escalabilidad y una fácil integración de nuevos servicios sobre la plataforma de red.

# CAPÍTULO 2

# 2 DEFINICIÓN DE REQUISITOS PARA SER SISTEMA AUTÓNOMO

## 2.1 DEFINICIONES

El presente capítulo se desarrolla bajo la base de los estándares de Internet publicados en los RFCs (*Request For Comment*) que van a permitir entender el desarrollo de los siguientes capítulos del presente proyecto.

Todos los documentos referenciados como RFC y pertinentes a lo largo del presente documento, se encuentran en el Anexo A.

### 2.1.1 SISTEMA AUTÓNOMO [1][2][5]23][30]

Un Sistema Autónomo (SA) es la unidad de políticas de enrutamiento en el mundo moderno del enrutamiento externo y que es aplicable en protocolos como EGP (*Exterior Gateway Protocol*), BGP (*Border Gateway Protocol*), e IDRP (*Inter Domain Routing Protocol*). La definición clásica dice que un Sistema Autónomo es un conjunto de routers bajo una administración técnica única, utilizando un protocolo de salida interior IGP (*Interior Gateway Protocol*) junto con métricas comunes para enrutar paquetes dentro del Sistema Autónomo, y un protocolo de salida exterior para enrutar paquetes hacia otros SAs.

Dentro del RFC 1930, "*Guidelines for creation, selection, and registration of an Autonomous System (AS)*", se define también al término prefijo, que en el mundo actual de Internet, permite que un bloque de redes IP puedan ser citadas con un prefijo y una máscara del tamaño que abarque a dichas redes en el límite de la potencia de dos. Por ejemplo, el grupo de direcciones reservadas por el

IANA (*Internet Assigned Numbers Authority*), del rango clase B que van desde la red 172.16.0.0/16 hasta la red 172.31.0.0/16 (16 redes clase B), se las puede determinar con el siguiente prefijo: 172.16.0.0/12.

En general el término prefijo es un equivalente a un bloque CIDR (*Classless Inter Domain Routing*), y en pocas palabras puede ser pensado como un grupo de una o más redes A, B, o C.

El uso del término Sistema Autónomo resalta en su definición el hecho de que aún cuando se utilicen múltiples IGPs y múltiples métricas, la administración de un Sistema Autónomo muestra a otros SAs, que tiene un plan de enrutamiento interior coherente y presenta una imagen consistente de qué redes son alcanzadas a través de dicho SA.

En resumen, un Sistema Autónomo es un grupo de uno o más prefijos IP anunciados a través de uno o más operadores de red que tienen una, única y claramente definida, política de enrutamiento.

En el RFC 1930 también se define a una política de enrutamiento como el conjunto de decisiones tomadas en el Internet hoy en día para enrutar tráfico IP, es decir, el objetivo de una política de enrutamiento es el intercambio de información de enrutamiento entre SAs.

Un Sistema Autónomo tiene un identificador único asociado, conocido como Número de Sistema Autónomo, o ASN por sus siglas en inglés. Dicho número es utilizado, no solo para identificar al Sistema autónomo, sino para el intercambio de información de enrutamiento exterior (entre SAs vecinos).

El término Sistema Autónomo a veces es confundido o mal utilizado como una manera conveniente de agrupar un conjunto de prefijos usados bajo el mismo control técnico administrativo, aún cuando dentro de ese grupo de prefijos existen varias políticas diferentes de enrutamiento. Sin excepción alguna, un SA debe tener una única política de enrutamiento.

Se espera que la información del enrutamiento de un SA hacia otro, sea simétrica, es decir, tanto el anuncio como la aceptación de las políticas de un SA debería ser recíproco con otro, ya que no sería útil una conexión de aplicaciones en una sola dirección. Sin embargo, en topologías de red complejas, el tráfico de una red anunciada por un SA hacia otra red anunciada por otro SA, no necesariamente toma el mismo camino o la misma ruta para alcanzar redes publicadas en cada SA, dando lugar a lo que se conoce como enrutamiento asimétrico. Este enrutamiento asimétrico, no es malo, pero puede generar problemas en capas superiores, como TCP, y debería ser usado con precaución y sólo cuando sea necesario.

## 2.2 PROTOCOLOS DE ENRUTAMIENTO[4][16][30]

Dado que muchas de las definiciones obligan a verificar y entender ciertos protocolos de salida interior y exterior, el presente proyecto, pretende describirlos de acuerdo a los más comunes y usados ampliamente en el mundo de las rutas y caminos de Internet, con la finalidad de entender los mecanismos, métricas y parámetros que utiliza un IGP o un EGP para escoger un camino para los paquetes IP dentro de una topología lógica y física de la red de un ISP.

### 2.2.1 BGP (*BORDER GATEWAY PROTOCOL*) [1][2][6][7][8][22]

Es un protocolo de enrutamiento entre Sistemas Autónomos. La función principal de un sistema que “habla” BGP es el intercambio de información de accesibilidad con otros sistemas BGP. Esta información de accesibilidad incluye la información de la lista de SAs por las que atraviesa dicha información. Esta información es suficiente para construir una imagen de conectividad de SAs para dicho acceso, desde donde se puedan eliminar lazos de enrutamiento y, a nivel de SA, algunas políticas de decisión puedan ser ejecutadas.

BGP se convirtió en un estándar de Internet en 1989 y fue definido originalmente en el RFC 1105, la versión actual es BGP4, adoptada en 1995 y definida en el RFC4721, que deja obsoleto al RFC 1771.

Este protocolo ha sido probado en escalabilidad, estabilidad y provee mecanismos necesarios para soportar políticas de enrutamiento complejas. Es por eso que en la actualidad, cuando se habla de BGP, implícitamente se habla de BGP4, ya que hoy en día nadie usa versiones anteriores, y muy pocos fabricantes soportan dichas versiones. Es un protocolo que puede trabajar adecuadamente al tener múltiples conexiones hacia dominios de enrutamiento no relacionados y con amplia utilización en el Internet y Sistemas Autónomos del mundo.

Provee un conjunto de mecanismo para el soporte de Enrutamiento Entre Dominios sin Clase CIDR. Estos mecanismos incluyen el soporte de anunciar un conjunto de destinos como prefijo IP, eliminando el concepto de clase de red que trajo el antiguo BGP. De igual manera presenta mecanismos que permiten agregación de rutas, así como agregación de caminos de SAs.

La información intercambiada a través de BGP soporta únicamente el paradigma de reenvío de paquetes basado en el destino, que asume que una ruta envía un paquete tomando en cuenta solo la dirección de destino llevada en la cabecera del paquete IP. Esto, por otro lado, refleja el conjunto de políticas de decisión que pueden o no ser aplicadas usando BGP.

Cuando se usa BGP entre Sistemas Autónomos, el protocolo es referido como BGP Externo o EBGP (*Exterior BGP*). Cuando el proveedor de servicios usa BGP para el intercambio de rutas dentro del SA, el protocolo es referido como BGP Interior o IBGP (*Interior BGP*).

BGP utiliza varios parámetros para definir políticas de enrutamiento y mantener un ambiente de enrutamiento estable, estos parámetros son llamados atributos.

Adicionalmente a estos atributos, BGP utiliza CIDR, que al dejar obsoleta la idea de redes IP de cierta clase (A,B,C,D,E), permite anunciar prefijos más pequeños que abarca más redes de cualquier clase, reduciendo significativamente el tamaño de las tablas de enrutamiento.

Los vecinos BGP intercambian la totalidad de información de enrutamiento cuando una conexión TCP entre vecinos es establecida. Cuando se encuentran cambios en las tablas de enrutamiento, los routers BGP envían a sus vecinos únicamente dichos cambios, ya que BGP no utiliza un envío periódico de actualizaciones de enrutamiento, y además porque anuncian el mejor camino para alcanzar una red.

#### 2.2.1.1 Atributos BGP

Las rutas aprendidas a través de BGP asocian algunas propiedades para determinar el mejor camino cuando existen múltiples caminos para un destino en particular, estas propiedades son conocidas como atributos. Es necesario entender cómo estos atributos influyen en la selección de un camino para el diseño de redes robustas. Los atributos son:

- Peso
- Preferencia Local
- Discriminador Multi Salida
- Origen
- Camino_SA
- Siguiente Salto
- Comunidad

#### *2.2.1.1.1 Peso*

Es un atributo local para un router con valores enteros desde de 0 a 65535. Este atributo no es anunciado a routers vecinos. Si el router aprende más de una ruta para el mismo destino, la ruta con el mayor peso será preferida. Este atributo es propietario del fabricante de equipos Cisco ®.

#### *2.2.1.1.2 Preferencia Local*

Este atributo es utilizado para escoger un punto de salida desde el Sistema Autónomo local. Es un valor entero positivo de cuatro octetos y en algunos fabricantes tiene el valor por defecto de 100 (Cisco), pero distinto al atributo peso, el atributo de preferencia local es propagado a través de todo el SA. Si existieran múltiples puntos de salida desde un SA, el atributo de preferencia local es utilizado para seleccionar el punto de salida para una ruta en específico, utilizando el más alto de los valores de preferencia local entre dos anuncios para la misma red.

#### *2.2.1.1.3 Discriminador de Multi Salida MED (Multi Exit Discriminator)*

El MED o atributo métrica es utilizado como una sugerencia hacia un SA externo con respecto a la ruta preferida dentro de un SA que está publicando la métrica. El término sugerencia es utilizado porque un SA externo que reciba las MEDs puede estar utilizando otros atributos BGP para la selección del camino. Consiste en un valor entero positivo de cuatro octetos, y un router selecciona la ruta anunciada o publicada con el valor de métrica o MED más bajo.

#### *2.2.1.1.4 Origen*

Este atributo, indica cómo BGP aprendió una ruta en particular. Este atributo puede tener uno de los siguientes valores posibles:

- IGP – la ruta es interior para el SA que la originó. Este valor es fijado cuando se ingresa la ruta a BGP a través de la línea de comandos desde el mismo router.
- EGP – la ruta es aprendida a través de un protocolo de salida de borde externo (EBGP).
- Incompleta – el origen de la ruta es desconocido o aprendida de distinta manera, un origen incompleto ocurre cuando una ruta es redistribuida dentro de BGP.

#### *2.2.1.1.5 Camino_SA*

Cuando una publicación de una ruta pasa a través de un sistema autónomo, el ASN es añadido a una lista ordenada de ASNs por los cuales el anuncio de una red ha atravesado. Por ejemplo, un router que tiene como ASN el 1 y que está conectado directamente a dos sistemas autónomos con ASNs, 2 y 3 respectivamente, publica un prefijo con el atributo camino_SA igual a {1}; en el momento en que el ASN2 quiera anunciar ese mismo prefijo, lo hará con el valor de camino_SA {2,1}, y de igual manera el ASN3, con el valor {3,1}; cuando esa ruta sea recibida nuevamente por el ASN1, la descartará, así como con cualquier publicación de ruta, donde el atributo camino_SA contenga su número de sistema autónomo. Éste es el mecanismo que BGP utiliza para detectar lazos de enrutamiento.

#### *2.2.1.1.6 Siguiente Salto*

Este atributo es usado por los entes EBGP, y es la dirección IP que es utilizada para alcanzar una ruta publicada. Para las entidades pares EBGP, la dirección IP del siguiente salto es la dirección IP de la conexión entre entidades pares. Para entidades IBGP, la dirección del siguiente salto EBGP se mantiene dentro del SA. Si la información propagada dentro de un mismo SA no mantiene la información

del siguiente salto, las rutas son descartadas, por eso es importante tener un IGP ejecutándose dentro del SA que propague la información de enrutamiento del siguiente salto.

#### *2.2.1.1.7 Comunidad*

El atributo de comunidad, provee una manera de agrupar destinos, llamados comunidades, para las cuales se puede aplicar decisiones de enrutamiento (aceptación, preferencia y redistribución). En algunos fabricantes, los mapas de enrutamiento pueden ser usados para especificar el atributo comunidad. Los atributos predefinidos son los siguientes:

- No-exportar – no publicar esta ruta a las entidades pares EBGP.
- No-publicar – no publicar esta ruta a ninguna entidad par.
- Internet – Anunciar o publicar esta ruta a la comunidad de Internet, todos los routers en la red pertenecen a esta comunidad.

Por ende un router que anuncia un prefijo con el atributo no-exportar, anunciará dicho prefijo al Sistema Autónomo vecino, y éste a su vez, a todos los routers dentro del SA, pero no la pasarán o publicarán hacia un tercer SA conectado directamente al segundo SA.

Si un router anuncia un prefijo con el atributo no-publicar, nunca saldrá dicho prefijo publicado hacia cualquier otro SA.

Si un router anuncia un prefijo con el atributo igual a Internet, no existen límites en la publicación de dicho prefijo a través de los sistemas autónomos.

#### 2.2.1.2 Selección del Camino BGP

BGP posiblemente recibirá muchas publicaciones para la misma ruta desde múltiples orígenes. BGP selecciona únicamente un camino como el mejor camino. Cuando un camino es seleccionado, BGP ubica este camino en la tabla de enrutamiento IP y la propaga hacia sus vecinos. BGP utiliza los siguientes criterios, en el orden presentado para seleccionar un camino para un destino:

- Si el camino especifica un siguiente salto inaccesible, elimina la actualización.
- Prefiere la ruta con el mayor peso.
- Si el peso es el mismo, prefiere el camino con la mayor preferencia local.
- Si las preferencias locales son las mismas, prefieren el camino que fue originado por BGP ejecutándose en el router que realiza la selección.
- Si no se originó ninguna ruta, prefiere la ruta que tiene el camino_SA más pequeño.
- Si todos los caminos tienen la misma longitud de camino_SA, prefieren el camino con el tipo de origen más bajo (donde el origen IGP es más bajo que el origen EGP, y el origen EGP es más bajo que un origen incompleto).
- Si los códigos de origen son los mismos, se prefiere la ruta con el atributo MED más bajo.
- Si los caminos tienen el mismo valor del atributo MED, prefieren un camino externo sobre un camino interno.
- Si los caminos siguen siendo iguales, prefieren el camino a través del vecino IGP más cercano.
- Se prefiere el camino con la dirección IP más baja, especificada en el ID del router por BGP.

### 2.2.2 RIP (*ROUTING INFORMATION PROTOCOL*)[4][14][16][17][18][19]

Es un protocolo de enrutamiento de salida interior (IGP). En un principio desarrollado para su ejecución en sistemas Unix, estandarizado por el RFC 1058

en 1988. La versión actual es la versión 2, especificada inicialmente por el RFC1388 que añade el soporte para máscaras de subred de longitud variable VLSM (*Variable Length Subnet Mask*), pero que no se enfocó en otras debilidades de la primera versión. El RFC 2453 deja obsoleto a los RFC 1723[1] y 1388, siendo la última actualización de la versión 2 de RIP. Con la llegada de IPv6, RIP fue adaptado y renombrado como RIPng (*RIP Next Generation*) en el RFC 2080 y 2081.

RIP ha sido clasificado como un protocolo de vector distancia, es decir, utiliza la distancia, medida en el número de saltos de enrutamiento, para determinar el camino óptimo de un paquete. Cada uno de los routers que trabajan con RIP, envía publicaciones de red hacia otros routers cada 30 segundos, y cada uno de los receptores de dichas publicaciones aumenta el contador de saltos en uno. Si la publicación fue recibida desde múltiples ruteadores, el camino con el menor número de saltos es el escogido. En caso de que la ruta preferida hacia un destino no esté disponible, la ruta con el siguiente menor número de saltos es utilizada. El máximo número de saltos permitidos por RIP es de 15, limitando también el tamaño de las redes que RIP puede soportar.

El proceso de convergencia (proceso para determinar una ruta alternativa cuando la ruta preferida para alcanzar un destino no está disponible) en RIP es el mayor problema, ya que fue diseñado para esperar la pérdida de seis actualizaciones seguidas, con un total de 180 segundos antes de considerar una ruta inalcanzable. Luego de lo cual espera a una nueva publicación de otra ruta disponible antes de actualizar la tabla de enrutamiento hacia una nueva ruta. Esto significa que al menos 3 minutos pasarán antes de que una ruta alterna sea usada, tiempo suficiente para que la mayoría de usuarios noten un desfase y para que la mayoría de aplicaciones expiren.

El otro problema fundamental con RIP es que ignora la velocidad de los enlaces involucrados al escoger una ruta. Si por ejemplo un camino está conformado por una serie de enlaces FastEthernet y cuya métrica devuelta es un salto mayor a la

[1] El RFC 1723 es la primera actualización de la segunda versión de RIP, publicado en noviembre de 1994.

de un único enlace Ethernet, el camino de la Ethernet será escogido como el óptimo.

La versión original de RIP no podía usar VLSM, limitando totalmente el espacio de direccionamiento IP posible. RIP versión 2, soluciona ese problema al publicar también la máscara de la red a anunciar.

RIP implementa mecanismos de límite de horizonte, envenenamiento de rutas y tiempos de espera para prevenir la propagación de información de enrutamiento errada.

Es un protocolo basado en UDP ejecutándose en capa transporte del modelo OSI (*Open System Interconnection*), en el puerto 520. Inicialmente se tenía una autenticación en texto plano para asegurar actualizaciones de rutas, luego en el RFC 2082, se definió una autenticación MD5.

En un esfuerzo de evitar levantar equipos que no participan en el protocolo de enrutamiento, RIP actualiza rutas en un multicast en la IP 224.0.0.9, ya que inicialmente utilizaba broadcast, y no cuenta con un mecanismo que detecte lazos de enrutamiento.

La facilidad de implementar RIP lo ha marcado para su uso en redes y en sistemas autónomos pequeños que no tienen suficientes caminos redundantes para manejar la sobrecarga de un protocolo más sofisticado.

RIPng realiza cambios muy pequeños para su utilización con redes IPv6, como los implícitos por el tamaño de los prefijos IPv6, manteniendo parámetros como el número de saltos, temporizadores, proceso de convergencia y el proceso de selección del mejor camino hacia un destino IPv6. Usa el puerto UDP 521 y deshabilita la autenticación ya que IPv6 maneja sus propios mecanismos.

### 2.2.3 OSPF (*OPEN SHORTEST PATH FIRST*) [3][4][9][15][16][20][30]

Es un protocolo de enrutamiento desarrollado para redes IP por el grupo de trabajo IGP del IETF (*Internet Engineering Task Force*). Este grupo de trabajo diseñó un IGP basado en el algoritmo del Primer Camino más Corto, o SPF (*Shortest Path First*).

Tiene dos características fundamentales, primero que es un protocolo abierto, por lo que sus especificaciones son de dominio público, y se las encuentra en el RFC 2328, publicado en abril de 1998, dejando obsoleto a versiones anteriores de la misma versión 2 del protocolo. Con la llegada de IPv6, se describe también una versión de OSPF (Versión 3) en el RFC 5340 de julio del 2008 y que deja obsoleta la primera versión con soporte de IPv6 de diciembre de 1999. La segunda característica es que es un protocolo basado en el algoritmo SPF, conocido también como algoritmo de Dijkstra, que es la persona que creó dicho algoritmo.

OSPF es un protocolo de estado de enlace que llama a todos los routers dentro de su área jerárquica para que envíen publicaciones del estado de enlace o LSA (*Link State Advertisement*). Dichas LSAs contienen información de interfaces, métricas usadas, y otras variables. Luego de recolectar toda la información de estado de enlace, los routers OSPF usan dicha información dentro del algoritmo SPF para calcular el camino más corto hacia cada nodo de la red.

OSPF puede operar de manera jerárquica. La entidad más grande dentro de la jerarquía es un Sistema Autónomo, aún cuando es conocido como protocolo de enrutamiento interior para un SA, es capaz de recibir y enviar rutas desde y hacia otros SAs.

Un Sistema Autónomo puede ser divido en un número de áreas, que son grupos de redes contiguas donde operan equipos. Routers con varios interfaces pueden participar en múltiples áreas; estos routers, que son llamados routers de borde de área ABR (*Area Border Router*), mantienen bases de datos topológicas separadas para cada área.

Una base de datos topológica es un gráfico resumido de las redes en relación a los routers. Esta base de datos topológica, contiene la colección de LSAs recibidos de todos los routers en la misma área. Dado que los routers dentro de la misma área comparten la misma información, tendrán bases de datos topológicas iguales.

El término dominio, a veces se usa para describir una porción de red en la cual todos los routers tienen bases de datos topológicas similares. El término dominio vendría a ser un SA.

La topología de un área es invisible a entidades fuera de dicha área. Al mantener las topologías de área separadas, OSPF pasa menos tráfico de enrutamiento que el tráfico que pasaría si no fuera segmentado.

La segmentación en áreas crea dos tipos de enrutamiento OSPF, dependiendo de si el origen y el destino están en áreas distintas o en la misma área. El enrutamiento intra-área se presenta cuando el origen y el destino se encuentran dentro de la misma área, el enrutamiento inter-área, ocurre cuando el destino y el origen están en áreas distintas.

Un backbone OSPF es el responsable de distribuir información de enrutamiento entre áreas, además consiste en todos los routers de borde de área, las redes que no están totalmente contenidas en ningún área, y los routers adjuntos.

El backbone en sí, es un área OSPF, de manera que todos los routers de backbone utilizan los mismos procedimientos y algoritmos para mantener la información de enrutamiento dentro del backbone, como en cualquier área a la que el router pertenecería. La topología del backbone es invisible a todos los routers intra-área, así como lo son las topologías individuales de cada área para el backbone.

Las áreas pueden ser definidas de manera que el backbone no esté contiguo. En este caso, la conectividad con el backbone debe ser establecida a través de enlaces virtuales. Estos enlaces virtuales son configurados entre cualquier router de backbone que comparte un enlace con un área que no pertenezca al backbone y que funcione como si fuera un enlace directo entre ellos.
Un router de borde de un sistema autónomo que ejecuta OSPF, aprende sobre rutas exteriores a través de protocolos de salida exterior (EGP) como BGP, o a través de información de la configuración directa en el equipo.

El algoritmo de enrutamiento SPF es la base de las operaciones de OSPF. Cuando un router SPF es encendido, inicializa sus estructuras de datos de protocolo de enrutamiento y luego espera indicaciones de protocolos de capas inferiores indicando que sus interfaces están funcionales.

Luego de que un router asegura que sus interfaces están funcionando, utiliza el protocolo de saludo OSPF (*Hello Protocol*) para solicitar a sus vecinos, que son routers con interfaces conectados en una red en común. El router envía y recibe paquetes *Hello* hacia y desde sus vecinos. Adicionalmente, los paquetes Hello actúan como paquetes de advertencia de vida (*keepalive*) para indicar a otros ruteadores que aún están operativos o funcionales.

En redes de múltiples accesos (redes que manejan más de dos routers), el protocolo Hello elige un router designado DR (*Designated Router*) y un router designado de respaldo BDR (*Backup Designated Router*). Entre otras cosas, el router designado es el responsable de generar LSAs para la totalidad de la red múltiples accesos. El tener un router designado, permite la reducción del tráfico de red y del tamaño de la base de datos topológica.

Cuando las bases de datos de estado de enlace de dos routers vecinos están sincronizadas, se dice que los routers son adyacentes.  En redes de múltiples accesos, el router designado determina qué routers serán adyacentes. Las bases de datos topológicas son sincronizadas entre pares de routers adyacentes.

Cada router designado envía periódicamente un LSA para alimentar de información a una adyacencia de un router o para informar a otros cuándo el estado de un router ha cambiado. Al comparar las adyacencias establecidas con estados de enlace, un router defectuoso puede ser detectado rápidamente, y la topología de la red puede ser alterada apropiadamente. De la base de datos topológica generada a partir de las LSAs, cada router calcula un árbol de camino más corto, con dicho router como la raíz del árbol. Luego dicho árbol del camino más corto, resulta en una tabla de enrutamiento.

Todos los paquetes OSPF comienzan con una cabecera de 24 bytes, como se muestra en la Tabla 2.1.

| Tamaño En Bytes | 1 | 1 | 2 | 4 | 4 | 2 | 2 | 8 | Variable |
|---|---|---|---|---|---|---|---|---|---|
| Nombre del Campo | Número De Versión | Tipo | Longitud Del Paquete | ID de Router | ID De Área | Suma de Verificación | Tipo de Autenticación | Autenticación | Datos |

Tabla 2.1 Paquete OSPF. Fuente RFC 2328

El número de versión, identifica la versión de OSPF utilizada, que puede ser 2 o 3.

El tipo, identifica si se trata de uno de los siguientes paquetes:

- Hello – Establece y mantiene relaciones con routers vecinos.
- Descripción de base de datos – Describe el contenido de una base de datos topológica. Estos mensajes son intercambiados cuando una adyacencia es inicializada.
- Solicitud de estado de enlace – Solicita partes de una base de datos topológica de routers vecinos. Estos mensajes son intercambiados luego de que un router descubre (al examinar los paquetes de descripción de base de datos) las partes de su base de datos topológica que no está actualizada.

- Actualización de estado de enlace – Es la respuesta a un paquete de solicitud de estado de enlace. Estos mensajes también son utilizados para la dispersión regular de LSAs. Algunos LSAs pueden ser incluidos dentro un único paquete de actualización de estado de enlace.
- Reconocimiento de estado de enlace – Son una notificación de la llegada de un paquete de actualización de estado de enlace.

El campo de longitud del paquete, es el tamaño total del paquete OSPF, incluyendo la cabecera y está especificada en bytes.

El ID de router, identifica el origen del paquete.

El ID de Área, identifica el área a la cual pertenece el paquete. Todos los paquetes OSPF están asociados a una única área.

La Suma de verificación, permite revisar que el contenido de todo el paquete esté libre de errores luego de su tránsito en la red.

El campo tipo de autenticación, puede ser cualquiera de los siguientes valores:

- 0, que significa que ninguna autenticación es utilizada.
- 1, que significa que se usa una simple contraseña.
- 2, que significa que se usa una autenticación cifrada, cualquier otro valor, es reservado para su definición por IANA.

El tipo de autenticación puede ser configurable por interfaz o por área, y en la versión 3 de OSPF la autenticación es deshabilitada ya que en IPv6 ésta se la deja en manos de la capa de Internet.

El campo autenticación, consiste en la información de autenticación en sí, es decir que si el tipo fue 0, el campo está vacío, si el tipo es 1, viaja la contraseña, si el campo tipo es 2, se añaden 3 campos adicionales al paquete OSPF que son:

- ID de llave, que permite identificar la llave precompartida y el algoritmo de cifrado a utilizar.
- Longitud de la información de cifrado añadida al paquete OSPF.
- Número de Secuencia Criptográfica.

Los datos, son la información encapsulada de capas superiores.
Algunas características adicionales de OSPF incluyen enrutamiento de múltiple camino, enrutamiento basado en capa superior o solicitudes de tipo de servicio TOS (*Type Of Service*).

También soporta más de una métrica. Si se usa únicamente una métrica, esta métrica sería considerada arbitrariamente, y TOS no estaría soportado. Si se usa más de una métrica, TOS estaría opcionalmente soportado a través del uso de una métrica separada (por ende una tabla de enrutamiento separada) para cada una de las ocho combinaciones creadas por los tres bits IP de TOS (retardo, velocidad efectiva y confiabilidad). OSPF calculará las rutas hacia todos los destinos dependiendo de la designación TOS.

El añadir la máscara de subred con cada publicación, habilita también VLSM; una red IP puede ser subdividida entonces en varias subredes de varios tamaños, permitiendo a los administradores de red flexibilidad adicional.

### 2.2.4 PROTOCOLOS DE ENRUTAMIENTO OSI [1][2][13][14][16][21]

La Organización de Estandarización Internacional, ISO (*International Organization for Standardization)*, ha desarrollado un completo conjunto de protocolos de enrutamiento para su uso en el modelo de Interconexión de Sistemas Abiertos, OSI (*Open System Interconnection*). Estos protocolos incluyen al protocolo de Sistema Intermedio – a – Sistema Intermedio, IS-IS (*Intermediate System to Intermediate System*), al protocolo de Sistema Final – a – Sistema Intermedio, ES-IS (*End System to Intermediate System*), y al Protocolo de Enrutamiento Inter Dominio, IDRP.

IS-IS fue originalmente desarrollado para enrutar redes que manejan el protocolo de red independiente de la conexión de la ISO, CLNP (*Connection Less Network Protocol*). Sin embargo, una versión posterior fue desarrollada para soportar tanto redes CLNP como redes IP, esta versión es referida como IS-IS Integrado, o IS-IS Dual.

La estandarización de IS-IS está descrita en el estándar ISO 10589, la ISO 9542 define ES-IS, y la ISO 10747 define IDRP.

El mundo de las redes OSI maneja cierta terminología, como Sistema Final (ES), que se refiere a un nodo de red que no realiza enrutamiento, o Sistema Intermedio (IS), que se refiere a un router. Estos términos foman la base de los protocolos OSI. El protocolo ES-IS permite a los ESs y a los ISs descubrirse unos a otros. El protocolo IS-IS provee el enrutamiento entre ISs.

Otros términos importantes de las redes OSI incluyen: área, dominio, enrutamiento de nivel 1 y enrutamiento de nivel 2. Un área es un grupo de redes contiguas y hosts adjuntos a dichas redes que han sido especificados como área por un administrador de red u operador de red. Un dominio es una colección de áreas conectadas. Los dominios de enrutamiento proveen la total conectividad a todos los sistemas finales dentro de cada dominio. El enrutamiento de nivel 1 es un enrutamiento dentro de un área o nivel 1, mientras que el enrutamiento de nivel 2, es el enrutamiento entre áreas dentro de un dominio o nivel 2.

#### 2.2.4.1 Sistema Final – A – Sistema Intermedio (ES-IS)

Este protocolo define cómo cada sistema final e intermedio aprende acerca de cada uno, en un proceso llamado configuración. Este proceso de configuración debe suceder antes que el enrutamiento entre sistemas finales (ESs) ocurra.

ES-IS es más un protocolo de descubrimiento que un protocolo de enrutamiento. Distingue entre tres tipos de subredes: subredes punto a punto (enlaces WAN seriales), subredes de broadcast (enlaces Ethernet o IEEE 802.3), y subredes de topología general (X.25).

El proceso de configuración ES-IS es el descubrimiento de otros ES o IS de manera que el enrutamiento entre ESs pueda tener lugar. La información de la configuración ES-IS es transmitida a intervalos regulares de tiempo a través de dos tipos de mensajes: mensajes de saludo ES (ESH) y mensajes de saludo IS (ISH). Los ESH son generados por los ESs, y son enviados a cada IS dentro de la subred. Los ISHs son generados por los ISs y son enviados a todos los ESs dentro de la subred. Estos mensajes de saludo (*hello*) inicialmente son destinados a comunicar las direcciones de red y subred de los sistemas que los originaron.

Donde es posible, ES-IS intenta enviar información de configuración simultáneamente a varios sistemas. En redes de broadcast, los mensajes de saludo ES-IS son enviados a todos los ISs a través de direcciones de multicast especiales que designan todos los sistemas finales. Cuando se opera en una topología de subred general, ES-IS no transmite información de configuración dado el alto costo de las transmisiones multicast.

El protocolo de configuración ES-IS comunica tanto la información de direcciones de capa red del modelo OSI y las direcciones de subred OSI. Las direcciones de capa red OSI identifican tanto el punto de acceso al servicio de red NSAP (*Network Service Access Point*), que es el interfaz entre las capas OSI 3 y 4, como el título de entidad de red NET (*Network Entity Title*), que es una entidad en capa de red en un IS del modelo OSI.

Las direcciones de subred, o direcciones de punto de fijación de la subred SNPAs (*Sub Network Point of Attachment*) son los puntos donde un ES o IS es conectado físicamente a la subred. La dirección SNPA identifica únicamente a cada sistema conectado a la subred. En una red Ethernet, por ejemplo, la dirección SNPA es la dirección de control de acceso al medio conformada por 48 bits, o dirección MAC

(*Media Access Control*). Resumiendo, la información de configuración transmitida por el protocolo ES-IS es la de los mapas NSAP a SNPA o NET a SNPA.

#### 2.2.4.2 Sistema Intermedio – A – Sistema Intermedio (IS-IS)

Es un protocolo de enrutamiento de estado de enlace jerárquico, que inunda a la red con información de estado de enlace para construir una imagen completa y consistente de la topología de red. Para simplificar el diseño y operación de un router, IS-IS distingue entre ISs de nivel 1 y de nivel 2. Los ISs de nivel 1 se comunican con otros ISs de nivel 1 dentro de la misma área. Los ISs de nivel 2 enrutan entre áreas de nivel 1 y forman un backbone de enrutamiento intra dominio. El enrutamiento jerárquico simplifica el diseño del backbone, ya que ISs de nivel 1 necesitan conocer únicamente cómo llegar al IS más cercano de nivel 2. El protocolo de enrutamiento en el backbone puede cambiar sin necesidad de impactar al protocolo de enrutamiento intra-área.

Cada ES vive dentro de un área en particular. El enrutamiento OSI comienza cuando un ES descubre un IS cercano al escuchar paquetes ISH. Cuando un ES desea enviar un paquete a otro ES, envía el paquete a uno de los ISs que se encuentre conectado a su red. El router entonces busca la dirección de destino y envía el paquete a través de la mejor ruta. Si el ES destino se encuentra dentro de la misma subred, el IS local lo conocerá por haber escuchado el mensaje ESH de dicho ES y le reenviará el paquete adecuadamente. Este IS puede enviar un mensaje de redirección (RD) hacia el origen del paquete para indicarle que una ruta directa está disponible. Si la dirección de destino es un ES dentro de otra subred en la misma área, el IS conocerá la ruta correcta y reenviará el paquete apropiadamente. Si la dirección destino es un ES en otra área, el IS de nivel 1 envía el paquete al IS de nivel 2 más cercano. Dentro del área de destino, los ISs reenvían paquetes a través del mejor camino hasta que el ES de destino es alcanzado.

Los mensajes de actualización de estado de enlace ayudan a los ISs a aprender más acerca de la topología de red. Primero, cada IS genera una actualización especificando los ISs y ESs a los cuales está conectado, así como las métricas asociadas. Dicha actualización luego es enviada a todos los ISs vecinos, que reenvían dicha información a sus vecinos, y así sucesivamente. Los números de secuencia terminan la inundación y distinguen actualizaciones antiguas de las nuevas. Cada IS puede construir una topología completa de la red, usando estas actualizaciones. Cuando la topología cambia, nuevas actualizaciones son enviadas.

IS-IS utiliza una única métrica por defecto con un máximo valor de camino de 1024. La métrica es arbitraria y típicamente asignada por el administrador de la red. Cualquier enlace único puede tener un valor de 64, y los enlaces de caminos son calculados sumando valores de enlace.

Los valores máximos de la métrica fueron configurados a ese nivel para proveer la facilidad de soportar varios tipos de enlaces mientras que al mismo tiempo se asegura que el algoritmo del camino más corto utilizado para el cálculo de rutas sea razonablemente eficiente.

IS-IS define tres métricas o costos adicionales y opcionales: retardo, gasto y error. La métrica de costo del retardo refleja el valor del retardo en un enlace. La métrica de costo de gasto refleja el costo de las comunicaciones asociado al uso de un enlace. La métrica de costo de error refleja la tasa de errores del enlace.

IS-IS mantiene un mapa de estas cuatro métricas (camino, retardo, gasto y error) para la opción de calidad de servicio (QoS) dentro de la cabecera CLNP y usa este mapa para el cálculo de rutas a través de la red.

IS-IS Integrado o Dual, es la versión del protocolo de enrutamiento IS-IS que usa un único algoritmo de enrutamiento para soportar más protocolos de capa red que tan solo CLNP. Algunos campos fueron añadidos a los paquetes IS-IS para permitir el soporte de capas de red adicionales. Estos campos informan a los

routers sobre la accesibilidad de direcciones de red desde otro conjunto de protocolos y otra información requerida por un conjunto de protocolos en específico.

#### 2.2.4.3 Protocolo de Enrutamiento Inter Dominio (IDRP)

Este protocolo OSI específica cómo se comunican routers con otros routers en dominios diferentes. IDRP fue diseñado para operar con CLNP, ES-IS e IS-IS.

IDRP presenta varios términos específicos del ambiente, entre los cuales se puede enumerar: un sistema intermedio de borde BIS (*Border Intermediate System*), dominio de enrutamiento RD (*Routing Domain*), identificador de dominio de enrutamiento RDI (*Routing Domain Identifier*), una base de información de enrutamiento RIB (*Routing Information Base*), y una confederación.

Un BIS es un IS que participa en enrutamiento inter dominios, y como tal, utiliza IDRP. Un RD es un conjunto de ESs e ISs que operan bajo el mismo conjunto de reglas administrativas y que comparte un plan de enrutamiento en común. Un RDI es un identificador único de un RD. Una RIB es una base de datos de enrutamiento utilizada por IDRP y que es construida por cada BIS en base a la información recibida dentro de un RD o desde otros BISs. Una RIB contiene el conjunto de rutas escogidas para ser usadas por un BIS en particular. Una confederación es un grupo de RDs que se muestran a otros RDs fuera de la confederación, como un único RD. La topología de una confederación no es visible para otros RDs fuera de la confederación. Las confederaciones deben ser anidadas unas dentro de otras y ayudan a reducir el tráfico de la red actuando como firewalls inter redes.

Una ruta IDRP es una secuencia de RDIs, algunos de los cuales pueden ser confederaciones. Cada BIS es configurado para conocer el RD y la confederación a la que pertenece. Un BIS aprende acerca de otros BISs, RDs y confederaciones a través de intercambios de información con cada vecino. Al usar enrutamiento

vector distancia, las rutas hacia un camino en particular se van acumulando exteriormente desde el destino. Únicamente las rutas que cumplan con las políticas locales de los BIS y que han sido seleccionadas para ser usadas serán pasadas a otros BISs. El recálculo de rutas es parcial y ocurre cuando uno de los eventos siguientes sucede: una actualización de enrutamiento incremental con nuevas rutas es recibido, un BIS vecino cae, o un BIS vecino sube.

IDRP basado en BGP, y maneja las siguientes características:

- Soporte para calidad de servicio (QoS) CLNP.
- Eliminación de lazos al mantener todos los dominios de enrutamiento por una ruta.
- Reducción de información y procesamiento de ruta al usar confederaciones, la compresión de información de caminos de dominios de enrutamiento, entre otras.
- Confiabilidad al utilizar un protocolo de transporte confiable incorporado.
- Seguridad al utilizar firmas criptográficas en una base por paquete.
- Servidores de rutas.

## 2.3 READYNET COMO SISTEMA AUTÓNOMO [5][23][24]

### 2.3.1 CONSIDERACIONES

El usar un Número de Sistema Autónomo por el hecho de querer ser Sistema Autónomo, no es una buena idea. La situación ideal sería tener un único prefijo anunciado que contenga varios prefijos por cada SA, es decir en el peor de los casos, un SA debería anunciar una red de cualquier clase IPv4 en su totalidad.

Este hecho de intentar llegar a lo ideal implica alguna práctica de reingeniería para poder aplicar las guías para la creación y asignación de un SA que enuncia el RFC 1930 y que probablemente será la única manera de implementar una política de enrutamiento deseada.

Algunas implementaciones utilizan un número de SA como una manera de etiquetar procesos de enrutamiento internos y externos. Dicha etiqueta no necesariamente es única, a menos que la información de enrutamiento sea intercambiada con otros SAs.

### 2.3.2 CRITERIOS DE DECISIÓN

Un SA debe ser utilizado para el intercambio de información de enrutamiento externa con otros SAs, a través de un protocolo de enrutamiento exterior. El protocolo recomendado es el protocolo de salida de borde, BPG.

En general, se debe acomodar tantos prefijos como sea posible dentro de un SA dado, entregando o publicando dichos prefijos con la misma política de enrutamiento.

Un SA es únicamente necesario cuando se tiene una política de enrutamiento distinta a la de las políticas de los SAs vecinos. En este caso la política de enrutamiento se refiere a cómo el resto del Internet toma decisiones de enrutamiento basada en la información de un SA.

El RFC 1930 muestra algunos ejemplos para orientar a la toma de decisión de ser o no Sistema Autónomo.

Cuando se tiene un sitio único con un único prefijo, un SA no es necesario, el prefijo debe ser ubicado en el SA del proveedor de Internet, ya que esa ubicación o sitio, tiene exactamente la misma política que el resto de sitios de clientes del ISP, por lo que no es necesario realizar un distinción en la información de enrutamiento. Dejando totalmente clara la idea de que el uso de un ASN es la representación de una política de enrutamiento en lugar de algún tipo de formalismo administrativo. Aún cuando puede darse el raro caso de que un sitio en especial quiera deslindar su política de enrutamiento de las del resto de sitios del SA del ISP.

Cuando se tiene un único sitio, pero con múltiples prefijos, bajo los mismos antecedentes y con el mismo criterio, un SA no es necesario.

Cuando se tiene un sitio con varios proveedores, o sitios multi-homed, quiere decir un grupo de prefijos que se conecta a más de un proveedor de servicios, y que obviamente no implica un sitio multi-homed ejecutando un protocolo IGP para propósitos de residencia. En este caso, un SA es requerido, los prefijos deberán ser parte de un único SA, distinto de los SAs de sus proveedores de servicio, permitiendo al cliente la posibilidad de tener una representación diferente de política y preferencia entre los distintos proveedores. Se puede decir que éste es el único caso donde un operador de red debería crear y registrar su propio número de SA (ASN), asegurándose de tener las posibilidades de ejecutar los protocolos de enrutamiento adecuados, como por ejemplo, BGP4.

Otros factores que pueden influir en la decisión, son la topología y el planeamiento a futuro. En ambos casos, la recomendación es tomar en cuenta definiciones y conceptos antes de tomar la decisión de registrar un SA, ya que los números son finitos, y en la historia, generalmente dicha decisión era tomada por ser parte del proceso de un operador para estar conectado a Internet.

### 2.3.3 CONSIDERACIONES IGP

Varios fabricantes de routers, requieren un identificador para etiquetar los procesos del protocolo IGP. Sin embargo, esta etiqueta no necesita ser única a nivel global, ya que en la práctica, esta información no es vista por protocolos de enrutamiento exterior.

Si se tiene un protocolo de enrutamiento exterior, es perfectamente razonable que se use el ASN como etiqueta IGP; si no es el caso, es aceptable escoger un número del rango privado de ASNs disponible.

El hecho de ejecutar un protocolo de enrutamiento interno, tampoco justifica el hecho de registrar un número de SA.

Con la llegada de BGP4, es necesario utilizar un protocolo IGP que pueda manejar rutas de redes sin clase, por ejemplo OSPF o IS-IS.

El espacio de números de SA es de capacidad limitada, ya que está definido actualmente como un número entero de 16 bits, y por ende limitado a 65535 números únicos de SA. En marzo del 2006 existían 5100 ASNs asignados, pero menos de 600 enrutados en el Internet. Dicho crecimiento debe ser monitoreado continuamente, sin embargo, si los criterios anunciados previamente son seguidos a la perfección, entonces no existirá peligro de un agotamiento de ASNs. Se espera que el protocolo IDRP sea desarrollado como estándar de Internet, antes de que esto suceda, ya que IDRP no posee un número tope en el tamaño de un RDI.

### 2.3.4 REGISTRO DE ASN

Un número de sistema autónomo único (ASN) es asignado a cada SA para ser usado en el enrutamiento BGP. Estos números son asignados por el IANA y los Registrantes Regionales de Internet RIR (*Regional Internet Registries*), las mismas autoridades que asignan direcciones IP, reservando los números privados de ASN desde 64512 hasta 65535.

Actualmente los Números de Sistema Autónomo, ASN, son enteros de 16 bits, pero un desarrollo de un número de 32 bits se ha iniciado, por el posible agotamiento del rango de 16 bits para el año 2010. En el RFC 4893 se describen algunas extensiones nuevas de BGP para migrar los ASNs como una entidad de 4 octetos.

Los Registrantes Regionales de Internet son organizaciones que se encargan de la asignación o registro de recursos de números de Internet en una región en

particular del mundo, estos recursos incluyen direcciones IP (IPv4 e IPv6) y números de sistemas autónomos (ASN). Actualmente existen 5 RIR en operación:

- ARIN (Registro Americano para Números de Internet), para América del Norte y parte del Caribe.
- RIPE NCC (Centro de Coordinación de Red de RIPE) para Europa, Medio Oriente y Asia Central.
- APNIC (Centro de Información de Red Asia-Pacifico) para Asia y la región del pacífico.
- LACNIC (Registro de Direcciones de Internet para Latino América y el Caribe) como el nombre lo indica para América Latina y parte de la región del Caribe.
- AfriNIC (Centro de Información de Red Africano) para toda África.

### 2.3.5 ANÁLISIS COSTO BENEFICIO

La presente sección, pretende analizar la relación costo junto con beneficio que implica registrar recursos de Internet por parte de ReadyNet Cia. Ltda., tanto desde el punto de vista del ISP, como desde el punto de vista de los clientes del ISP.

#### 2.3.5.1 Costo Beneficio desde el Punto de Vista del ISP

El costo de registrar y mantener los números de recursos de Internet por el ISP puede representar un gasto considerable en un inicio, pero en el futuro, con la llegada de IPv6 al Ecuador, se facilitará notablemente la adquisición y enrutamiento de ambos protocolos en su red.

Es más se podría aprovechar, el hecho de que actualmente LACNIC, el RIR correspondiente, no cobra ningún rubro por el hecho de registrar un bloque IPv6 y

que ReadyNet pueda ser pionero en el Ecuador del uso y explotación de dicho recurso de Internet.

El beneficio impacta directamente a nivel financiero y gerencial en el ISP, ya que puede buscar alternativas de proveedores de salida internacional con mejores precios, sin que dicho cambio a nivel técnico, impacte o incomode a clientes, ni recurra en gastos operativos de movilización y configuración de servicios primordiales, como implementar servidores DNS que se usen en la nueva salida al Internet. De igual manera optimizando recursos como la capacidad de internet contratada actualmente a los proveedores de borde, que se ocupa cuando se desea acceder a servicios con esquema de direccionamiento del otro proveedor como si no fueran parte de una misma red.

Todos estos cambios lógicos, deberán ir de la mano con cambios físicos en la red de ReadyNet Cia. Ltda., que permitan explotar el cambio administrativo de la operación de la red.

#### 2.3.5.2 Costo Beneficio desde el Punto de Vista de Clientes

A nivel de clientes, el beneficio será a largo plazo, cuando se pueda ver beneficiado con servicios de valor agregado a los tradicionales, utilizando su mismo canal.

Prácticamente los servicios básicos que entrega el ISP actualmente son:

- El servicio de resolución de nombres DNS, registro y publicación de zonas de dominios de clientes.
- El servicio de acceso y alojamiento de páginas web, HTTP y HTTPS.
- El servicio de recepción (POP, IMAP) y envío de correos, bajo los dominios de clientes o bajo los dominios de ReadyNet Cia. Ltda., junto con filtros de SPAM y virus en los respectivos servidores.

- El servicio de alojamiento de servidores, que permite que los clientes mantengan su servidor en el cuarto de equipos del ISP, para su conexión a Internet.

Sin embargo, con los cambios adecuados dentro de la red del ISP y con el registro de recursos de Internet, se podría agregar fácilmente equipos que puedan brindar servicios de manera eficiente como:

- Difusión constante de audio.
- Difusión constante de video.
- Telefonía IP.
- Video Conferencia Centralizada.

El ISP sin ser Sistema Autónomo puede brindar estos servicios, pero la inversión sería mayor ya que tendrían que ser implementados uno por cada proveedor de borde, para evitar más saltos de los necesarios cuando se accede con distintos esquemas de direccionamiento y el uso innecesario de capacidad de Internet en cada proveedor de borde.

Dichos servicios podrían ser gratis en un inicio y luego a un costo notablemente accesible. Por último, cualquier cambio del enrutamiento de las direcciones IP de los clientes, será totalmente transparente, y dependerá únicamente de la última milla contratada.

# CAPÍTULO 3

# 3 DIMENSIONAMIENTO Y REDISEÑO DE LA RED

## 3.1 DIMENSIONAMIENTO DE LA RED [12][32][33]

### 3.1.1 DIMENSIONAMIENTO DE USUARIOS

La Tabla 3.1, muestra la cantidad de abonados de Internet a nivel nacional en los últimos 7 años, definiendo como abonado a toda persona natural o jurídica que suscribe un contrato de adhesión y contrata el servicio de Internet con un Proveedor de Servicios de Internet, según la SENATEL (Secretaría Nacional de Telecomunicaciones) con datos al 31 de Octubre del 2008.

| Abonados de Internet a Nivel Nacional | | | |
|---|---|---|---|
| Año | Conmutado[1] | No Conmutado[2] | Total |
| 2001 | 83007 | 2623 | 85630 |
| 2002 | 94164 | 6499 | 100663 |
| 2003 | 102787 | 4563 | 107350 |
| 2004 | 108169 | 11599 | 119768 |
| 2005 | 110540 | 26786 | 137326 |
| 2006 | 141814 | 65463 | 207277 |
| 2007 | 187981 | 88733 | 276714 |
| oct-08 | 180788 | 142352 | 323140 |

Tabla 3.1 Abonados de Internet a Nivel Nacional – Fuente SENATEL 10/2008

De estos datos, se puede calcular una tasa de crecimiento de abonados en los últimos años, dando una tasa de crecimiento del 21,66% promedio en el número de abonados de Internet en los últimos 7 años. Los cálculos fueron realizados

[1] Abonados Conmutados son aquellos que usan los canales de voz de la Red Telefónica Pública para su acceso al Internet.
[2] Abonados No Conmutados son aquellos que no usan los canales de voz de la Red Telefónica Pública, por ende, la última milla puede ser xDSL, radio, coaxial, etc.

utilizando el porcentaje de abonados nuevos en el siguiente año, de acuerdo al diferencial de crecimiento. Estos datos, se muestran en la Tabla 3.2.

| Año | % |
|---|---|
| 2002 | 17,56 |
| 2003 | 6,64 |
| 2004 | 11,57 |
| 2005 | 14,66 |
| 2006 | 50,94 |
| 2007 | 33,50 |
| 2008 | 16,78 |

Tabla 3.2 Tasa de Crecimiento de Abonados de Internet a nivel nacional 2002-2008

Sin embargo, el tomar un promedio de dichos años con muestras tan desiguales, como las muestras de los años 2006 y el 2003, simplemente daría datos erróneos. Por lo que es necesario descartar dichas muestras ya que son muestras atípicas. Nuevamente al hacer el cálculo de la tasa promedio de crecimiento de abonados por año, eliminando esos dos valores, se tendría un crecimiento de un 18,81 % anual. La Figura 3.1, muestra la línea de tendencia del crecimiento de abonados de Internet a nivel nacional desde el año 2002 hasta el año 2008.

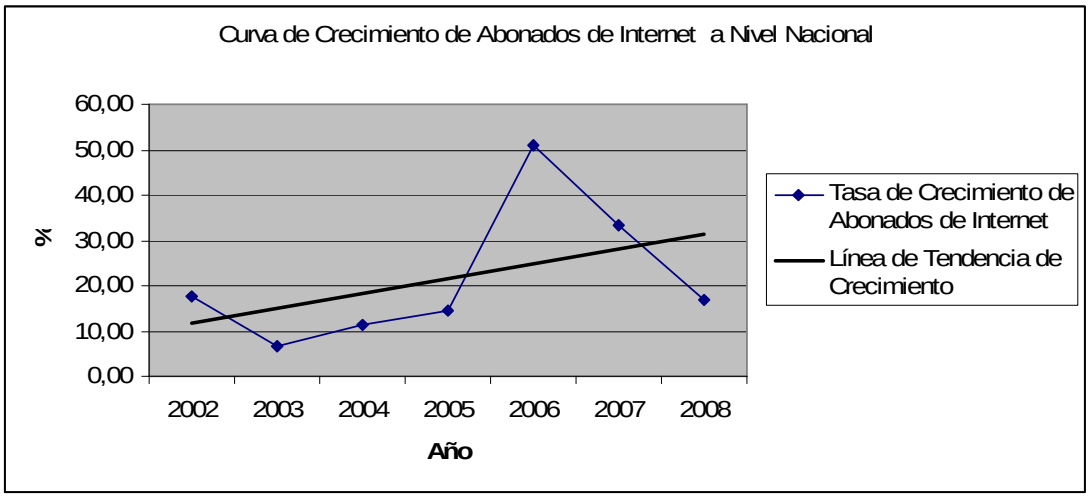


Figura 3.1 Curva de Crecimiento de Abonados de Internet a Nivel Nacional[1]

[1] Utilizando la herramienta de línea de tendencia de Microsoft Excel 2007 ®, que es un análisis de regresión de una serie de datos, se buscó la regresión que se ajuste a los datos ingresados con cada una de las regresiones posibles (exponencial, lineal, logarítmica, polinómica y potencial), dando todas las gráficas una tendencia lineal. Esta herramienta usa el método de ajuste de mínimos cuadrados para las regresiones.

De tal manera que al utilizar los datos de la Tabla 3.1 y el promedio de crecimiento anual, se podría generar una tabla proyectada a 5 años del número nacional de abonados de Internet. Se proyecta a 5 años, para tener valores iniciales en el redimensionamiento de las distintas redes del ISP y porque es el tiempo aproximado en el que la tecnología llega a cumplir su ciclo de vida, o se vuelve caduca. El crecimiento de abonados a nivel nacional, se presenta en la Tabla 3.3.

| Año | Total Abonados |
|---|---|
| 2008 | 323140 |
| 2009 | 383930 |
| 2010 | 456155 |
| 2011 | 541968 |
| 2012 | 643924 |
| 2013 | 765060 |

Tabla 3.3 Abonados de Internet a Nivel Nacional, proyectado a 5 años

Por otro lado, SENATEL proporciona también la densidad de Internet a nivel nacional, con datos hasta la última muestra tomada en Octubre del 2008. Siendo dicha densidad determinada por el número de abonados existentes por cada 100 habitantes del país. Esta información es únicamente informativa, y se muestra en la Tabla 3.4.

| Densidad de Internet | | |
|---|---|---|
| Año | Población | Densidad |
| 2001 | 12’479924 | 0,69% |
| 2002 | 12’660728 | 0,80% |
| 2003 | 12’842578 | 0,84% |
| 2004 | 13’026891 | 0,92% |
| 2005 | 13’215089 | 1,04% |
| 2006 | 13’408270 | 1,55% |
| 2007 | 13’605485 | 2,03% |
| oct-08 | 13’788350 | 2,34% |

Tabla 3.4 Densidad de Internet desde el 2001 – Fuente SENATEL

De la Tabla 3.4 se puede realizar un cálculo de la tasa de crecimiento de población en el Ecuador en los últimos años. Esta tasa anual de crecimiento, se

encuentra en la Tabla 3.5. No se toman datos del Instituto Nacional de Estadísticas y Censos INEC, ya que SENATEL los usa en la Tabla 3.4. A partir de dichos datos es posible calcular una tasa promedio anual del crecimiento de la población, que resulta en un 1.43 %. La Tabla 3.4 y la Tabla 3.5 permitirán proyectar la población en el Ecuador en 5 años, dato que se muestra en la Tabla 3.6.

| Año | % |
|---|---|
| 2002 | 1,45 |
| 2003 | 1,44 |
| 2004 | 1,44 |
| 2005 | 1,44 |
| 2006 | 1,46 |
| 2007 | 1,47 |
| 2008 | 1,34 |

Tabla 3.5 Tasa anual de crecimiento de Población en el Ecuador

| Año | Población |
|---|---|
| 2008 | 13’788350 |
| 2009 | 13’985705 |
| 2010 | 14’185885 |
| 2011 | 14’388930 |
| 2012 | 14’594881 |
| 2013 | 14’803780 |

Tabla 3.6 Población del Ecuador Proyectada a 5 años.

Para determinar la proyección de la densidad de Internet anual, se toman los datos de la Tabla 3.3 y de la Tabla 3.6 y se los ingresa en la Ecuación 3.1:

$$\eta = \frac{Aa}{Pa/100}$$

Ecuación 3.1 Cálculo Densidad de Internet por Año

Donde:

*η:* es la densidad de Internet por año.

*Aa:* es la cantidad de abonados de Internet a nivel nacional por año.

*Pa:* es la población proyectada por año.

Con lo que se puede generar una nueva tabla de la densidad de Internet proyectada por año, a nivel nacional, en los próximos 5 años. La misma que se muestra en la Tabla 3.7.

| Densidad de Internet Proyectada | | |
|---|---|---|
| Año | Población | Densidad % |
| 2008 | 13.788.350 | 2,34 |
| 2009 | 13.985.705 | 2,75 |
| 2010 | 14.185.885 | 3,22 |
| 2011 | 14.388.930 | 3,77 |
| 2012 | 14.594.881 | 4,41 |
| 2013 | 14.803.780 | 5,17 |

Tabla 3.7 Densidad de Internet Proyectada a 5 años.

Al igual que la población, dicha densidad tiene como primer valor el del año 2008.

Tomando en cuenta la cantidad de abonados con los que ReadyNet cuenta actualmente en el mercado, se podría proyectar la cantidad de abonados para los próximos 5 años, de acuerdo al porcentaje de participación en el número de abonados totales de Internet. Bajo la premisa que ReadyNet Cia. Ltda. cerró el año 2008 con 600 abonados, entre usuarios de marcado telefónico y acceso banda ancha, se puede determinar que el porcentaje de abonados del total del mercado para el ISP es el 0,1856%.

Se puede hacer esto porque los datos entregados a SENATEL trimestralmente por todos los ISPs del país, incluyen los datos de ReadyNet, evitando la revisión de históricos de ReadyNet, que no existen en un documento formal en la empresa.

Asumiendo que el porcentaje especificado de la participación en el mercado a nivel nacional se mantendría, se puede determinar una proyección de abonados para los próximos 5 años, tomando como punto de partida, el año 2008 recién

cerrado. Donde se espera que los clientes conmutados pasen a ser usuarios de banda ancha con una estrategia de ventas. La Tabla 3.8 muestra esta información, que posteriormente será utilizada para el dimensionamiento de la red de acceso y borde del ISP.

| Año | Total Nacional | Total ReadyNet |
|---|---|---|
| 2008 | 323140 | 600 |
| 2009 | 383930 | 713 |
| 2010 | 456155 | 847 |
| 2011 | 541968 | 1006 |
| 2012 | 643924 | 1196 |
| 2013 | 765060 | 1421 |

Tabla 3.8 Proyección del Total de Abonados de Internet por Año.

Aún cuando es verdad que la tendencia de los usuarios de acceso telefónico es a disminuir, también es verdad que no por eso van a dejar de contratar un acceso no conmutado que cueste lo mismo y que le brinde mayor velocidad para utilizar servicios de Internet.

### 3.1.2 REDIMENSIONAMIENTO DE LA RED DE ACCESO

Utilizando los valores de la Tabla 1.2 y desglosándola en servicios, solo con la idea de que el 50%[1] de los clientes duplicarían su capacidad durante los primeros meses del 2009, algo inevitable por el comportamiento del mercado de Internet en el Ecuador actualmente, se llega a la Tabla 3.9.

Con ese movimiento estratégico comercial para mantener clientes, sin tomar en cuenta el crecimiento esperado a finales del 2009, la capacidad total del Acceso ATM del proveedor C sería sobrepasada. Y la totalidad inicial a proyectar del ISP para el 2009 sería únicamente la suma de las troncales de última milla sin las

[1] Aproximadamente la mitad de los abonados, son abonados residenciales del ISP, pero por la influencia de la estrategia de mercado de empresas como CNT o Suratel a inicios del 2009, que es la de duplicar la capacidad de sus abonados, y bajo la visión de que es mejor duplicar capacidades de última milla, aumentando el nivel de compartición, que reducir el valor facturado por abonado. Se toma el 50% de cada plan.

PBX, ya que esos accesos no tienden a crecer, sino a reducirse. Teniendo un valor inicial de 79872 Kbps en la capacidad de acceso total en los puntos que pueden crecer.

| | Planes Contratados | | | | |
|---|---|---|---|---|---|
| Proveedor de Acceso | Capacidad [Kbps] | Cantidad Abonados 2008 | Cantidad Abonados Inicios 2009 | Capacidad Requerida [Kbps] | Total Requerido por Acceso [Kbps] |
| C ATM | 128/64 | 168 | 84 | 10752 | 55808 |
| | 256/128 | 56 | 112 | 28672 | |
| | 512/256 | 8 | 32 | 16384 | |
| C Metro Ethernet | 1024/512 | 8 | 8 | 8192 | 16384 |
| | 2048/1024 | | 4 | 8192 | |
| D y E | 64/64 | 48 | 24 | 1536 | 7680 |
| | 128/128 | 8 | 28 | 3584 | |
| | 256/256 | 4 | 6 | 1536 | |
| | 512/512 | | 2 | 1024 | |
| C PBX | Marcado Telefónico | 300 | 300 | 4096 | 4096 |
| | | | | | 83968 |

Tabla 3.9 Capacidad Base Total de Acceso por Punto de Acceso Estimado a Inicios del 2009.

Por lo tanto, el porcentaje de capacidad de acceso total en cada punto de acceso, para el inicio del 2009 sería el especificado en la Tabla 3.10. Donde se excluye a las troncales PBX, ya que difícilmente incrementen el número de usuarios de acceso de marcado telefónico como para proyectarlos en su totalidad.

| Proveedor de Acceso | Total Requerido por Acceso [Kbps] | Porcentaje % |
|---|---|---|
| C ATM | 55808 | 69,87 |
| C Metro Ethernet | 16384 | 20,51 |
| D y E | 7680 | 9,62 |

Tabla 3.10 Porcentaje de la Capacidad Total de Acceso por Punto de Acceso.

Según la proyección del número de abonados para el 2013, ReadyNet Cia.Ltda., debería contar con una totalidad de 1421 abonados. Tomando en cuenta que según normas internacionales un acceso a Internet es considerado como de banda ancha al superar los 256 Kbps, todos los planes que estén bajo los 256 Kbps deberían desaparecer, al igual que los clientes conmutados, sin embargo, la intención del ISP es que desaparezcan las conexiones, más no los abonados.

La totalidad de la capacidad de acceso por año, se puede calcular utilizando el porcentaje de crecimiento promedio anual de abonados del 0.1856%, arrancando con el valor inicial del 2009 obtenido de la Tabla 3.9 y realizando un redondeo a un valor múltiplo de 8. Esta información se muestra en la Tabla 3.11.

| Año | Capacidad de Acceso Requerida [Kbps] | Redondeo [Kbps] |
|---|---|---|
| 2009 | 81,354 | 81,368 |
| 2010 | 82,864 | 82,872 |
| 2011 | 84,402 | 84,408 |
| 2012 | 85,969 | 85,976 |
| 2013 | 87,564 | 87,576 |

Tabla 3.11 Proyección a 5 años de la Capacidad de Acceso Total.

Aplicando los porcentajes de cada proveedor de acceso de la Tabla 3.10, cuya tendencia debería mantenerse, ya que siempre un enlace de radio va a ser más caro que una última milla de cobre, se obtendrían los valores proyectados por año de la capacidad de acceso requerida en cada proveedor, mostrados en la Tabla 3.12.

| Proveedor de Acceso | Porcentaje | Capacidad de Acceso Requerida por Año [Kbps] | | | | |
|---|---|---|---|---|---|---|
| | | 2009 | 2010 | 2011 | 2012 | 2013 |
| C ATM | 69,87 | 56853 | 57904 | 58977 | 60073 | 61191 |
| C Metro Ethernet | 20,51 | 16691 | 16999 | 17314 | 17636 | 17964 |
| D y E | 9,62 | 7824 | 7968 | 8116 | 8267 | 8421 |

Tabla 3.12 Capacidad de Acceso Proyectada por Proveedor.

### 3.1.3 REDIMENSIONAMIENTO DE LA RED DE BORDE

De acuerdo a los planes de compartición de la Tabla 1.3, se puede realizar una proyección de usuarios por plan que brinda el ISP, valores que variarán por el movimiento estratégico de que la mitad de los usuarios van a aumentar su capacidad (Tabla 3.9). La cantidad de usuarios por plan a inicios del 2009 se muestran en la Tabla 3.13.

| Abonados por Plan de Compartición Estimados Iniciales del 2009 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Velocidad [Kbps] | Abonados 8:1 | **Abonados 8:1 Inicios 2009** | Abonados 4:1 | **Abonados 4:1 Inicios 2009** | Abonados 2:1 | **Abonados 2:1 Inicios 2009** | Abonados 1:1 | **Abonados 1:1 Inicios 2009** |
| 128/64 | 60 | **30** | 56 | **28** | 42 | **21** | 10 | **5** |
| 256/128 | 17 | **38** | 24 | **40** | 10 | **26** | 5 | **8** |
| 512/256 | 8 | **12** | 0 | **12** | 2 | **6** | 0 | **2** |
| 1024/512 | 4 | **6** | 4 | **2** | 0 | **1** | 0 | **0** |
| 2048/1024 | 0 | **2** | 0 | **2** | 0 | **0** | 0 | **0** |
| 64/64 | 16 | **8** | 16 | **8** | 8 | **4** | 6 | **4** |
| 128/128 | 3 | **9** | 4 | **10** | 0 | **4** | 1 | **3** |
| 256/256 | 0 | **2** | 4 | **4** | 0 | **0** | 0 | **0** |
| 5125/512 | 0 | **1** | 0 | **2** | 0 | **0** | 0 | **0** |
| TOTAL | 108 | **108** | 108 | **108** | 62 | **62** | 22 | **22** |

Tabla 3.13 Abonados por Plan de Compartición Estimados a Inicios del 2009.

Con los valores de la Tabla 3.13 se puede determinar una nueva capacidad de salida internacional, utilizando el mismo criterio con el que se obtuvieron los datos de la Tabla 1.3. Dicha información está disponible en la Tabla 3.14.

| Velocidad [Kbps] | Abonados 8:1 Inicios 2009 | Grupos 8:1 | Capacidad Requerida [Kbps] | Abonados 4:1 Inicios 2009 | Grupos 4:1 | Capacidad Requerida [Kbps] | Abonados 2:1 Inicios 2009 | Grupos 2:1 | Capacidad Requerida [Kbps] | Abonados 1:1 Inicios 2009 | Capacidad Requerida [Kbps] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 128/64 | 30 | 4 | 512 | 28 | 7 | 896 | 21 | 11 | 1408 | 5 | 640 |
| 256/128 | 38 | 5 | 1280 | 40 | 10 | 2560 | 26 | 13 | 3328 | 8 | 2048 |
| 512/256 | 12 | 2 | 1024 | 12 | 3 | 1536 | 6 | 3 | 1536 | 2 | 1024 |
| 1024/512 | 6 | 1 | 1024 | 2 | 1 | 1024 | 1 | 1 | 1024 | 0 | 0 |
| 2048/1024 | 2 | 1 | 2048 | 2 | 1 | 2048 | 0 | 0 | 0 | 0 | 0 |
| 64/64 | 8 | 1 | 64 | 8 | 2 | 128 | 4 | 2 | 128 | 4 | 256 |
| 128/128 | 9 | 2 | 256 | 10 | 3 | 384 | 4 | 2 | 256 | 3 | 384 |
| 256/256 | 2 | 1 | 256 | 4 | 1 | 256 | 0 | 0 | 0 | 0 | 0 |
| 5125/512 | 1 | 1 | 512 | 2 | 1 | 512 | 0 | 0 | 0 | 0 | 0 |
| TOTAL | 108 | | 6976 | 108 | | 9344 | 62 | | 7680 | 22 | 4352 |
| Capacidad de Salida Internacional Requerida Estimada a Inicios del 2009 | | | | | | | | | | | 28352 |

Tabla 3.14 Capacidad de Internet Requerida Estimada a Inicios del 2009

El valor de 28352 Kbps requeridos a contratar en la Red de Borde tiene dos implicaciones:

- El interfaz del router del proveedor A no soporta más de 10 Mbps.
- Los 18 Mbps excedentes pueden ir en el proveedor B, pero no todos los clientes que incrementen su capacidad, van necesariamente a estar con un esquema de direccionamiento del proveedor B.

Utilizando el porcentaje de presencia de abonados por red de acceso de la Tabla 3.12, junto con los valores obtenidos en la Tabla 3.8, se puede distribuir la

proyección de abonados en los próximos 5 años, en cada red de acceso; información disponible en la
Tabla **3.15**.

| Proveedor de Acceso | Año 2009 | Año 2010 | Año 2011 | Año 2012 | Año 2013 |
|---|---|---|---|---|---|
| C ATM | 498 | 592 | 703 | 836 | 993 |
| C Metro Ethernet | 146 | 174 | 206 | 246 | 291 |
| D y E | 69 | 81 | 97 | 114 | 137 |
| TOTAL | 713 | 847 | 1006 | 1196 | 1421 |

Tabla 3.15 Distribución de la Proyección de Abonados por Proveedor de Acceso

Se puede obtener de igual manera un porcentaje de usuarios por plan contratado, para luego poder aplicar dicho porcentaje en la proyección de abonados por tipo de acceso y obtener un estimado a 5 años. La Tabla 3.16 muestra el porcentaje de usuarios por proveedor de acceso.

| | Porcentajes de Usuarios por Plan Contratado en Cada Acceso | | | | |
|---|---|---|---|---|---|
| | Capacidad [Kbps] | % Abonados 8:1 | % Abonados 4:1 | % Abonados 2:1 | % Abonados 1:1 |
| C ATM | 128/64 | 13,2 | 12,3 | 9,2 | 2,2 |
| | 256/128 | 16,7 | 17,5 | 11,4 | 3,5 |
| | 512/256 | 5,3 | 5,3 | 2,6 | 0,9 |
| C Metro Ethernet | 1024/512 | 46,2 | 15,4 | 7,7 | 0,0 |
| | 2048/1024 | 15,4 | 15,4 | 0,0 | 0,0 |
| D y E | 64/64 | 13,6 | 13,6 | 6,8 | 6,8 |
| | 128/128 | 15,3 | 16,9 | 6,8 | 5,1 |
| | 256/256 | 3,4 | 6,8 | 0,0 | 0,0 |
| | 5125/512 | 1,7 | 3,4 | 0,0 | 0,0 |

Tabla 3.16 Porcentaje de Usuarios por Plan Contratado Estimado a Inicios del 2009

Con los datos de las Tabla 3.15 y Tabla 3.16, se realizará un estimado por cada año de la capacidad de Internet por plan de servicios existentes en el ISP. Un ejemplo del procedimiento es realizado para el año 2009 en la **¡Error! No se encuentra el origen de la referencia.**. Dicha estimación muestra que para fines del 2009, sólo para satisfacer la demanda de clientes y mantener el SLA contratado por los mismos, se necesitará de una capacidad internacional de 83392 Kbps.

| **Capacidad [Kbps]** | Abonados 8:1 | Grupos 8:1 | **Capacidad Proyectada [Kbps]** | Abonados 4:1 | Grupos 4:1 | **Capacidad Proyectada [Kbps]** | Abonados 2:1 | Grupos 2:1 | **Capacidad Proyectada [Kbps]** | Abonados 1:1 | **Capacidad Proyectada [Kbps]** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **128/64** | 66 | 9 | **1152** | 61 | 16 | **2048** | 46 | 23 | **2944** | 11 | **1408** |
| **256/128** | 83 | 11 | **2816** | 87 | 22 | **5632** | 57 | 29 | **7424** | 18 | **4608** |
| **512/256** | 26 | 4 | **2048** | 26 | 7 | **3584** | 13 | 7 | **3584** | 4 | **2048** |
| **1024/512** | 68 | 9 | **9216** | 23 | 6 | **6144** | 11 | 6 | **6144** | 0 | **0** |
| **2048/1024** | 22 | 3 | **6144** | 22 | 6 | **12288** | 0 | 0 | **0** | 0 | **0** |
| **64/64** | 9 | 2 | **128** | 9 | 3 | **192** | 5 | 3 | **192** | 5 | **320** |
| **128/128** | 10 | 2 | **256** | 12 | 3 | **384** | 5 | 3 | **384** | 4 | **512** |
| **256/256** | 2 | 1 | **256** | 5 | 2 | **512** | 0 | 0 | **0** | 0 | **0** |
| **512/512** | 1 | 1 | **512** | 2 | 1 | **512** | 0 | 0 | **0** | 0 | **0** |
| **Totales** | 287 | | **22528** | 247 | | **31296** | 137 | | **20672** | 42 | **8896** |
| **Capacidad Total Proyectada a Finales del 2009** | | | | | | | | | | | **83392** |

Tabla 3.17 Estimado de la Capacidad Total Proyectada a Finales del 2009.

Si se procede de igual manera, para cada uno de los años proyectados, se obtiene un resumen de la capacidad proyectada a 5 años, información disponible en la Tabla 3.18.

| Año | Capacidad [Kbps] |
|---|---|
| 2009 | 83392 |
| 2010 | 97088 |
| 2011 | 112256 |
| 2012 | 136384 |
| 2013 | 161280 |

Tabla 3.18 Dimensionamiento de Capacidad Requerida por Clientes del ISP Proyectado a 5 años.

Todo esto, asumiendo que los planes de servicio que el ISP vende, se mantienen y crecerán según lo estimado.

### 3.1.4 REDIMENSIONAMIENTO DE LA RED DE DISTRIBUCIÓN

La última sección a considerar, es la de la capacidad necesaria para los servidores dentro de la empresa. La misma que puede ser proyectada con el mismo índice que el de las últimas millas, junto con los valores de la Tabla 1.4 y que se presenta en la Tabla 3.19.

Esta consideración se la realiza porque prácticamente todos los servidores que brindan servicios que consumen alta cantidad de recursos de hardware, son

nuevos y el procesamiento de tráfico hacia el Internet no es constante en los valores indicados.

| | Capacidad Promedio Diaria Proyectada Al Año [Kbps] | | | | | |
|---|---|---|---|---|---|---|
| Servidor / Año | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
| A | 400 | 407 | 415 | 423 | 431 | 439 |
| B | 400 | 407 | 415 | 423 | 431 | 439 |
| C | 256 | 261 | 266 | 271 | 276 | 281 |
| D | 400 | 407 | 415 | 423 | 431 | 439 |
| E | 230 | 234 | 239 | 243 | 248 | 252 |
| F | 128 | 130 | 133 | 135 | 138 | 140 |
| G | 784 | 799 | 813 | 828 | 844 | 860 |
| TOTAL | 2598 | 2646 | 2695 | 2745 | 2796 | 2848 |

Tabla 3.19 Capacidad de Internet para Servidores Requerida Proyectada a 5 años.

En el caso que fuera necesario y siempre bajo la marcha, se podría requerir de un equipo adicional cuyo tráfico estaría considerado dentro del crecimiento del tráfico del servidor G, que no debería incrementar, a menos que aumente el personal de la empresa.

En la actualidad, con 600 abonados, se tienen en existencia alrededor de 1800 cuentas de correo, distribuidas entre cada uno de los servidores SMTP, lo que da un promedio de 3 cuentas de correo por abonado, manteniendo este índice en los clientes proyectados para los próximos 5 años de la Tabla 3.8, se obtendrán los datos de la Tabla 3.20.

| Año | Total Abonados ReadyNet | Total Cuentas De Correo Proyectadas |
|---|---|---|
| 2008 | 600 | 1800 |
| 2009 | 713 | 2139 |
| 2010 | 847 | 2541 |
| 2011 | 1006 | 3019 |
| 2012 | 1196 | 3587 |
| 2013 | 1421 | 4262 |

Tabla 3.20 Total de Cuentas de Correo Electrónico Proyectadas por Abonado por Año.

Se usó una relación directa, porque así como existen abonados que tienen una sola cuenta de correo o que no la tienen porque usan correos gratuitos, existen abonados que tienen entre 14 a 25 cuentas. Estos datos, serán tomados en cuenta para el diseño correspondiente de la red de distribución que impacta directamente en la red de borde.

## 3.2 REDISEÑO DE LA RED[1][2][4][33][34][35]

Dada la necesidad de una separación física de la red de distribución, de la red de borde y de la red de acceso, las siguientes secciones presentarán varias alternativas que van a variar tanto económica como técnicamente, según la situación actual del ISP y el redimensionamiento especificado en la sección 3.1.

Recalcando la idea de que dichas secciones enfocarán únicamente en la topología física de la red. Los cambios en la topología lógica y asignación de direcciones vendrán luego de la selección de la mejor opción que acople la idea de registrar números de Internet por parte del ISP y como parte del proceso de migración de redes y servicios de la empresa.

### 3.2.1 REDISEÑO DE LA RED DE BORDE

Actualmente la capacidad contratada tanto al proveedor A como al proveedor B, no supera la velocidad máxima de los interfaces al exterior en cada uno de los routers de borde disponibles. La Tabla 3.21, muestra la capacidad de conexión e interfaces disponibles en los routers de borde de cada proveedor:

| | Interfaz | Capacidad Contratada [Mbps] | Capacidad Interfaz de Borde [Mbps] |
|---|---|---|---|
| Proveedor A | Ethernet/IEEE802.3i | 7 | 10 |
| Proveedor B | FastEthernet/IEEE802.3u | 10 | 100 |

Tabla 3.21 Capacidad Equipos de Borde

De lo que se puede notar, el interfaz del proveedor A está por llegar a su máxima capacidad, pudiendo tener inconvenientes en el crecimiento de la capacidad contratada en dicho proveedor.

Adicionalmente es importante recordar que el sistema operativo del router de borde B, no soporta protocolos de enrutamiento exterior o de borde.

Tanto el proveedor A, como el proveedor B, pueden ofrecer la publicación de un prefijo y número de Sistema Autónomo con BGP. Según el RFC 1930, ReadyNet Cia. Ltda., califica como *multi-homed* o ISP con dos salidas internacionales, por ende puede registrar un ASN.

Actualmente el plan de distribución de direcciones IP del ISP hace que maneje 9 prefijos /24 de los Sistemas Autónomos de los proveedores A y B de manera ineficiente; sin embargo, con un plan de reasignación y la debida justificación, el ISP podría solicitar un prefijo /21 u 8 redes máscara /24, y mantenerse con ese prefijo al menos los próximos 5 años.

Bajo la definición de un Sistema Autónomo, es necesario escoger un protocolo de enrutamiento de salida exterior, un protocolo o protocolos de enrutamiento de salida interior y métricas que definan políticas de enrutamiento adecuadas.

Inicialmente las características de software del router de borde A, serían suficientes para comenzar a “conversar” en el protocolo EGP que “habla” dicho proveedor; sin embargo, las características de procesamiento, memoria e interfaces de conexión no son las adecuadas para soportar un crecimiento y balanceo al estimado en los próximos 5 años.

Por otro lado el router de borde B, únicamente necesitaría actualizar el sistema operativo con el que está trabajando actualmente y aumentar la memoria no volátil del equipo.

#### 3.2.1.1 Primera Solución de Red de Borde

La primera alternativa, sería cambiar el router de borde A ya que sus interfaces no soportarían el dimensionamiento a 5 años presentado. Por otro lado, se debería actualizar el sistema operativo del router de borde B ya que no soporta ningún protocolo de salida exterior. Se debe considerar que el router de borde B, no es de propiedad de ReadyNet Cia. Ltda, sino que está en las instalaciones de la empresa, y es únicamente administrado por el personal técnico del ISP. Esta solución se muestra en la Figura 3.2.

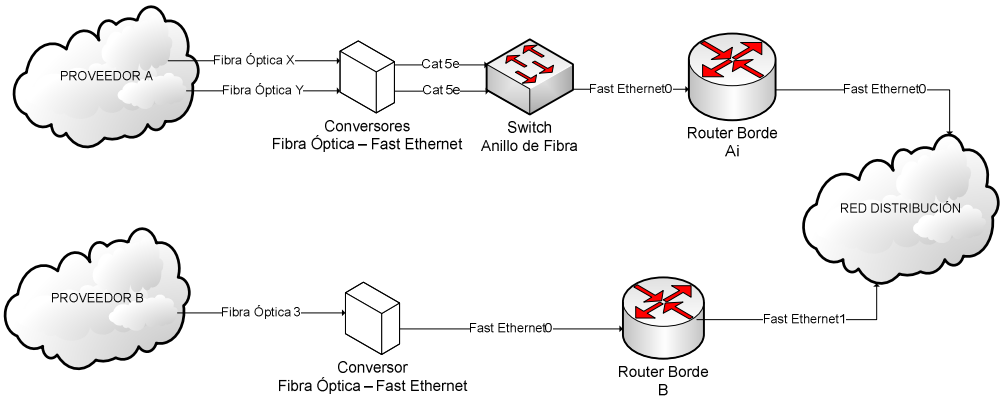


Figura 3.2 Primera Alternativa de Diseño de Red de Borde

Donde el router Ai sería un nuevo equipo con dos tarjetas FastEthernet, una tarjeta de memoria no volátil y procesador que recomiende el fabricante para soportar un sistema operativo con al menos las siguientes características:

- Soporte BGP4 y todas sus extensiones.
- Soporte IDRP OSI.
- Soporte de Listas de Acceso.
- Soporte IS-IS de OSI.
- Soporte de Cifrado en el Acceso Remoto a línea de comandos SSHv2 (*Secure SHell 2*).
- Soporte de OSPF.
- Autocompletado de caracteres en línea de comandos.
- Soporte de Etiquetas IEEE 802.1q.

- Soporte de GTS (*Generic Traffic Shaping)*.
- Definición de parámetros SLA.
- Soporte de firewall y sistema detección de intrusos IDS (*Intrusion Detection System*).
- Soporte SNMP, versiones 1,2 y 3.
- Soporte STP.

El nuevo sistema operativo del Router B, debería soportar al menos las mismas características definidas para el Router Ai.

#### 3.2.1.2 Segunda Solución de Red de Borde

La segunda alternativa sería cambiar ambos routers de borde, devolviendo al proveedor B el equipo y consiguiendo dos equipos que tengan al menos 2 interfaces FastEthernet, con una memoria volátil, procesador y espacio suficiente para almacenar y cargar un sistema operativo que cumpla con las siguientes características:

- Soporte BGP4 y todas sus extensiones.
- Soporte IDRP OSI.
- Soporte de Listas de Acceso.
- Soporte de Cifrado en el acceso remoto (SSHv2).
- Soporte IS-IS OSI.
- Soporte de OSPF.
- Autocompletado de caracteres en línea de comandos.
- Soporte de Etiquetas IEEE 802.1q.
- Soporte de GTS.
- Definición de parámetros SLA.
- Soporte de firewall y sistema detección de intrusos (IDS).
- Soporte SNMP, versiones 1,2 y 3.
- Soporte STP.

La segunda alternativa para la red de borde, es la que se muestra en la Figura 3.3

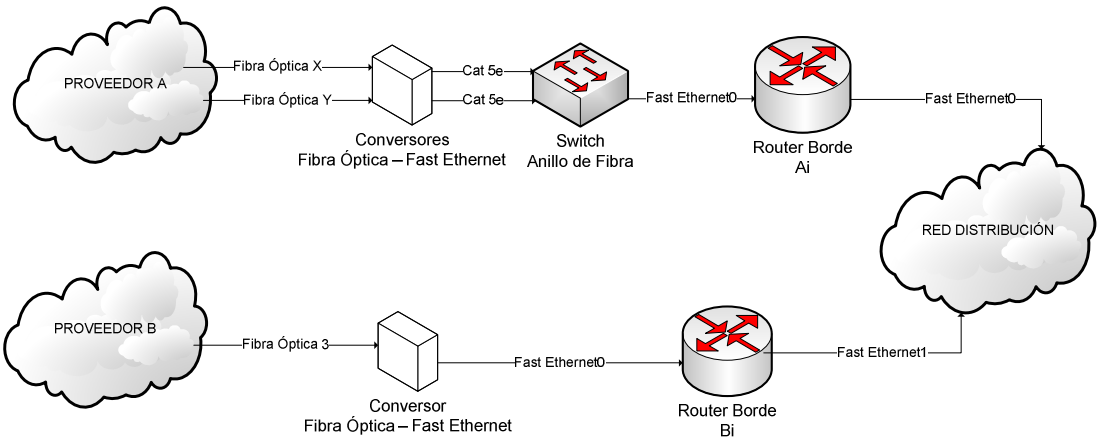


Figura 3.3 Segunda Alternativa de Diseño de Red de Borde

Donde Bi y Ai son los routers con las características especificadas.

### 3.2.1.3 Tercera Solución de Red de Borde

La tercera alternativa, es comprar un solo equipo con los mismos requerimientos de las anteriores soluciones, a diferencia de las interfaces FastEthernet, en lugar de ser 2, serían 3, ya que se eliminaría uno de los routers de borde, es decir; una tarjeta para la conexión con la red de distribución, otra tarjeta para la salida con el proveedor A y la última para la conexión con el proveedor de borde B.

Esta tercera alternativa involucraría el uso de un switch de 8 puertos (Switch de Borde) que maneje etiquetas IEEE 802.1q, que pueda administrar y separar la etiqueta de la salida del proveedor A, la etiqueta de la salida del proveedor B y la etiqueta del acceso Metro Ethernet del proveedor C, que en dicha instancia, compartirían el mismo equipo. Adicionalmente el switch deberá tener una tasa de conmutación de paquetes mayor a 5 Mpps.

El router indicado se denominará Router de Borde Bii y, el switch mencionado, será ubicado como Switch de Borde, tal como se ve en la Figura 3.4.

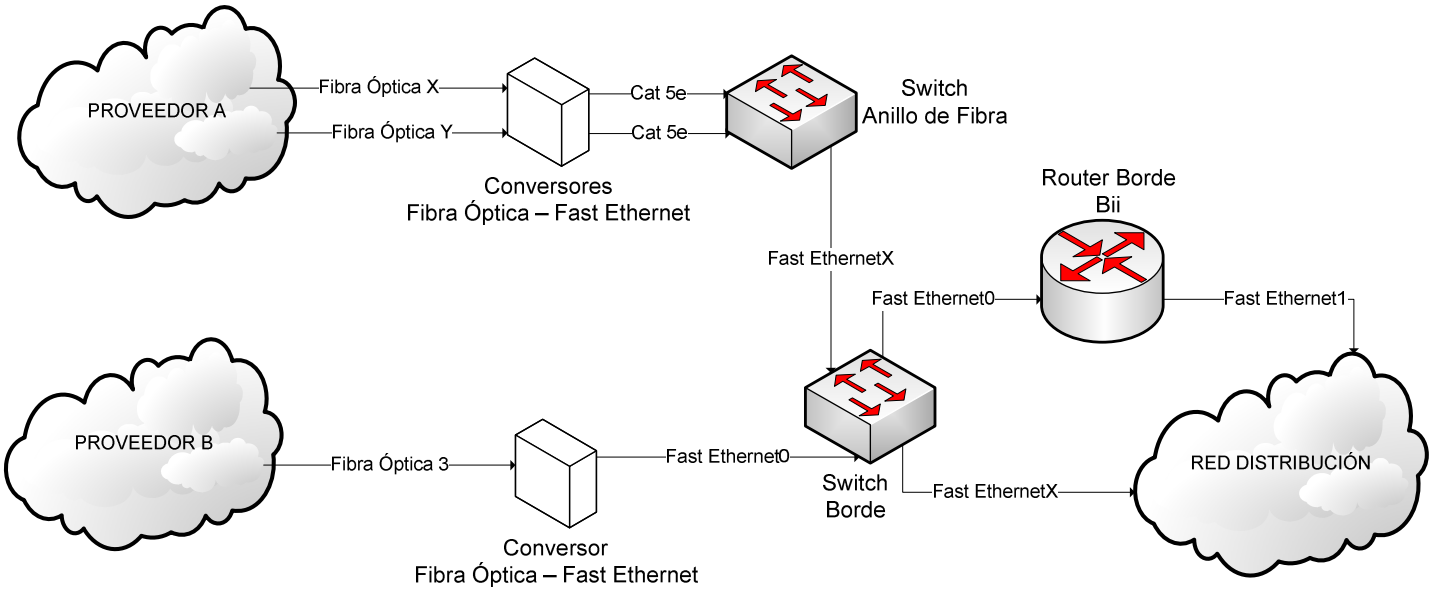


Figura 3.4 Tercera Alternativa de Diseño de Red de Borde

Las características del Router de Borde Bii de memoria, procesador y espacio, serían las recomendadas por el fabricante de manera que el equipo pueda soportar un sistema operativo con las siguientes características mínimas:

- Soporte BGP4 y todas sus extensiones.
- Soporte IDRP OSI.
- Soporte de Listas de acceso.
- Soporte de Cifrado en el acceso remoto (SSHv2).
- Soporte IS-IS OSI.
- Soporte de OSPF.
- Autocompletado de caracteres en línea de comandos.
- Soporte de Etiquetas IEEE 802.1q.
- Soporte de GTS.
- Definición de parámetros SLA.
- Soporte de firewall y sistema de detección de intrusos (IDS).
- Soporte SNMP, versiones 1,2 y 3.
- Soporte STP.

#### 3.2.1.4 Cuarta Solución de Red de Borde

La cuarta alternativa sería tener como al inicio, dos routers de borde más una tarjeta Fast Ethernet adicional cada uno, con dos switches (Switch de Borde B y C) como el de la tercera alternativa, pero que además soporten el protocolo STP.

Esta solución tendrá un impacto directo en la red de distribución, donde también sería necesario verificar que el switch de la actual red de distribución, soporte etiquetas IEEE 802.1q y STP.

Además, surge la necesidad de un switch (Switch de Borde A) para la recepción de la fibra óptica 3 del proveedor B, que permita discriminar el tráfico de borde y acceso que entrega el hilo de fibra fusionado desde el proveedor B.

Entregando un esquema redundante que se muestra en la Figura 3.5 donde el Router Aii y el Router Biii, nuevamente serían equipos con características recomendadas por el fabricante de procesador, memoria no volátil y espacio disponible para cargar un sistema operativo con al menos las siguientes características:

- Soporte BGP4 y todas sus extensiones.
- Soporte IDRP OSI.
- Soporte de Listas de acceso.
- Soporte de Cifrado en el acceso remoto (SSHv2).
- Soporte IS-IS OSI.
- Soporte de OSPF.
- Autocompletado de caracteres en línea de comandos.
- Soporte de Etiquetas IEEE 802.1q.
- Soporte de GTS.
- Definición de parámetros SLA.
- Soporte de firewall y sistema de detección de intrusos (IDS).
- Soporte SNMP, versiones 1,2 y 3.
- Soporte STP.

Los Switches de Borde A, B y C, deberían ser únicamente de 8 puertos; con la característica de que si el Switch B deja de funcionar, automáticamente suba el Switch C, o viceversa, gracias a la configuración de STP.

Adicionalmente sería necesario un Router que permita manejar el acceso Metro Ethernet, sin embargo, las características del equipo serán basadas en las consideraciones de la sección 3.2.2.

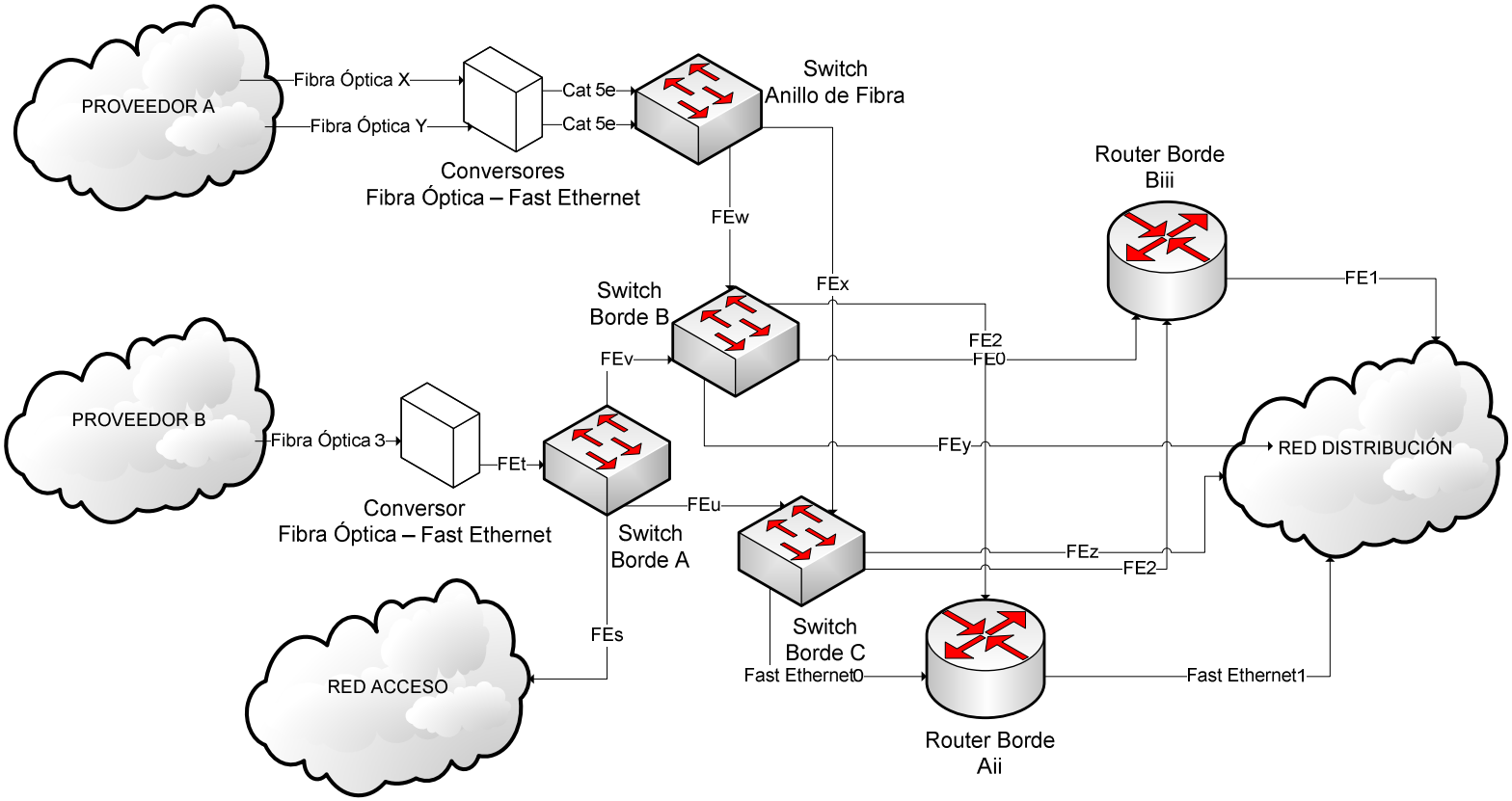


Figura 3.5 Cuarta Alternativa de Diseño de Red de Borde.

### 3.2.2 REDISEÑO DE LA RED DE ACCESO

Según la Tabla 3.9, al final del presente año, la capacidad del acceso a través del router de acceso C, habría de sobrepasar el valor teórico soportado por el interfaz ATM/DS3. Y por otro lado, el equipo conecta una interfaz Ethernet hacia la red de distribución, una solución temporal es equilibrar la capacidad por 3 interfaces de los 8 interfaces Ethernet que tiene el equipo.

El primer cambio a realizar en el Router de Acceso C es incorporar un módulo FastEthernet. El segundo cambio urgente, sería acordar con el proveedor de acceso C, la fusión de los dos hilos de fibra que están sin fusionar del grupo de los 6 tendidos por parte del proveedor de Acceso C hacia el ISP; de manera que se pueda conectar otra tarjeta ATM/DS3, en un proyecto a final de año. Mientras tanto se tiene la versatilidad de crecer en la troncal Metro Ethernet, que de igual manera, se debería buscar a futuro la forma de eliminar dicha conexión lógica y hacer una conexión física hacia otro router.

Con el router de acceso D, sería necesario cambiar la tarjeta Ethernet que actualmente conecta al equipo con la red de distribución, por una FastEthernet, aunque; de igual manera, dicho equipo es propiedad del proveedor D, por lo que el cambio lo realizaría personal técnico de dicho proveedor, previa coordinación con el ISP. Negociaciones con el proveedor deberían agilitar un cambio de equipo, o en su defecto, ReadyNet Cia. Ltda. deberá comprar un equipo.

La misma situación sería necesaria con el servidor de acceso E, se deberá negociar con el proveedor de acceso, para que instale un router, o en su defecto ReadyNet Cia. Ltda., adquiera uno.

#### 3.2.2.1 Primera Solución de Red de Acceso

Entonces, la primera solución involucra únicamente cambios de módulos de tarjetas Ethernet por FastEthernet para la conexión hacia la red de distribución de

los routers de Acceso C y D, confirmando que el sistema operativo del ruteador de acceso D soporte al menos OSPF e IS-IS y exigiendo al proveedor de acceso E, que implemente el protocolo IGP seleccionado en su servidor.

Adicionalmente, la fusión de 2 hilos de fibra, junto con la adquisición de una tarjeta ATM/DS3 para otra troncal en el router de Acceso C. Más la migración o cambio de interfaz por otro hilo de fibra del acceso Metro Ethernet que llegue hacia un router adicional que se llamará Cm, que tenga dos tarjetas FastEthernet y que soporte etiquetas IEEE802.1q, más OSPF e IS-IS para implementar IGP. Quedando la red de acceso como lo muestra la Figura 3.6.

#### 3.2.2.2 Segunda Solución de Red de Acceso

La segunda solución, involucra el cambio del módulo de la tarjeta de 8 puertos Ethernet por una tarjeta FastEthernet y la adquisición de una tarjeta ATM/DS3 para el router de acceso C. Adicionalmente se deberá negociar con el proveedor de acceso C para la habilitación de dicha troncal al fusionar 2 hilos de fibra.

Se sugiere migrar el acceso Metro Ethernet a otro router que sería llamado Router Cm, bien sea, utilizando otro hilo de fibra o simplemente separando la etiqueta de la salida internacional de la etiqueta del acceso Metro Ethernet con la ayuda de un switch en la red de borde, como el mencionado en las secciones 3.2.1.3 y 3.2.1.4.

Adicionalmente se debería comprar dos routers para cambiar al ruteador de acceso D y al servidor de acceso E, que se llamarán Router de Acceso Di y Router de Acceso Ei.

Dichos routers deben tener dos tarjetas FastEthernet, con características sugeridas por el fabricante de memoria no volátil, procesador y capacidad de almacenar configuraciones y cargar un sistema operativo que soporte al menos:

- Listas de acceso.

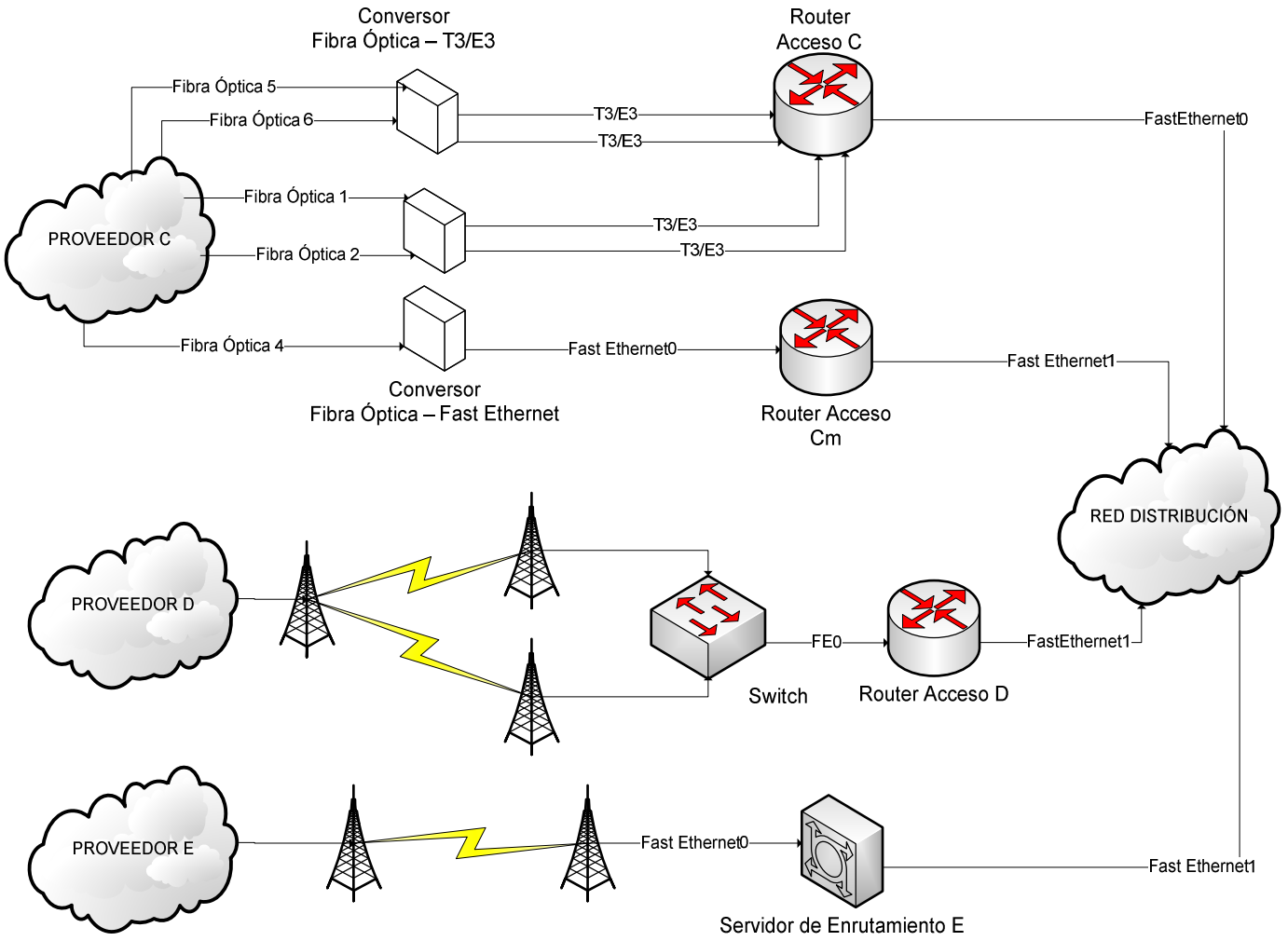


Figura 3.6 Primera Alternativa de Diseño de Red de Acceso

- Cifrado en el acceso remoto (SSHv2).
- IS-IS OSI.
- OSPF.
- Autocompletado de caracteres en línea de comandos.
- Etiquetas IEEE 802.1q.
- GTS.
- Definición de parámetros SLA.
- SNMP, versiones 1,2 y 3.
- STP.

La Figura 3.7 muestra cómo quedaría la segunda opción.

Cabe recalcar que aún cuando se tomó en cuenta dentro del crecimiento total de abonados, las cuentas de acceso telefónico de marcado, el crecimiento proyectado a 5 años no justifica la adquisición de un RAS, ni la contratación de otra troncal de 30 canales simultáneos; la idea sería que esos usuarios pasen a ser clientes banda ancha y mantener la troncal de acceso telefónico para que en caso de que un cliente pierda el servicio por problemas de última milla, pueda utilizar un usuario y contraseña, junto con su línea telefónica como respaldo.

El cambio de abonados conmutados a no conmutados debe ser el resultado de una estrategia de ventas  por parte del Departamento Comercial del ISP.

#### 3.2.2.3 Tercera Solución de Red de Acceso

La tercera solución, involucra añadir un router más robusto con cuatro interfaces FastEthernet, que realice las veces de router de borde en el área de la red de acceso y maneje todo el enrutamiento hacia la red de distribución y la red de borde desde todos los accesos disponibles en el ISP.

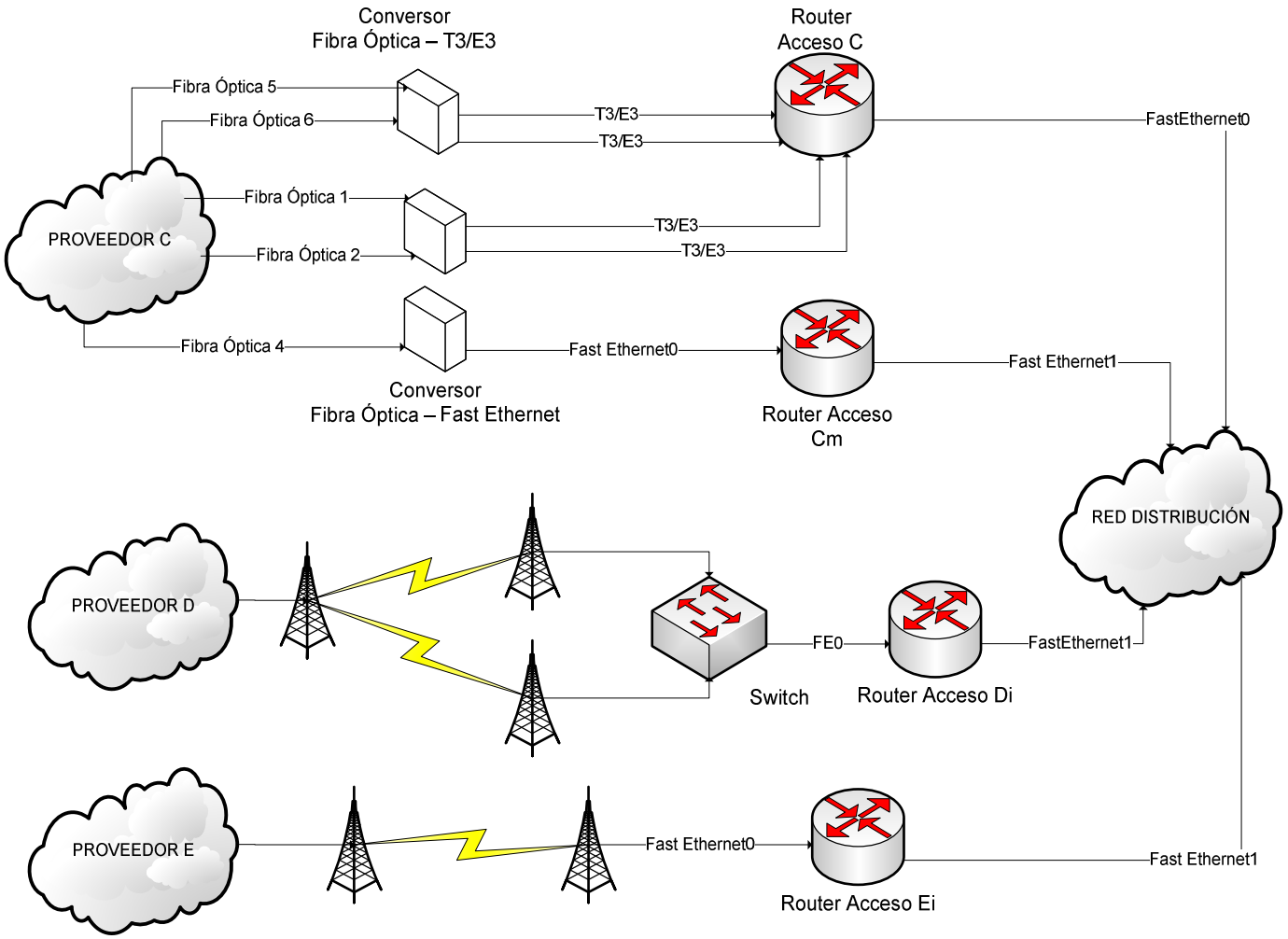


Figura 3.7 Segunda Alternativa de Diseño de Red de Acceso.

Se deja fuera al RAS del proveedor C, ya que es necesaria una directa conexión con el servidor de autenticación.

Con este router del área de acceso, se evita inundar de tráfico de enrutamiento a la red de distribución por tener varios equipos en el área núcleo de la red o distribución. Dicho equipo sería llamado Router de Acceso Borde.

De igual manera, para hacer el esquema redundante, sería necesario dos switches de 24 puertos, separados por VLANs que soporten STP y que a todos los routers de acceso (Cm, Di, Ei) de la segunda solución, se les incorpore una tarjeta FastEthernet adicional para la conexión hacia los dos switches, que se denominarán Switch de Acceso A y Switch de Acceso B.

Estos switches de acceso tendrán características de procesamiento, memoria y sistema operativo, iguales a las de los requeridos para la red de borde, tal como se muestra en la Figura 3.8.

El Router de Acceso Borde deberá tener características recomendadas por el fabricante de procesador, memoria no volátil y capacidad de almacenamiento para mantener y cargar un sistema operativo que soporte, al menos, las siguientes características:

- Soporte de Listas de acceso.
- Soporte de Cifrado en el acceso remoto (SSHv2).
- Soporte IS-IS OSI.
- Soporte de OSPF.
- Autocompletado de caracteres en línea de comandos.
- Soporte de Etiquetas IEEE 802.1q.
- Soporte de GTS.
- Definición de parámetros SLA.

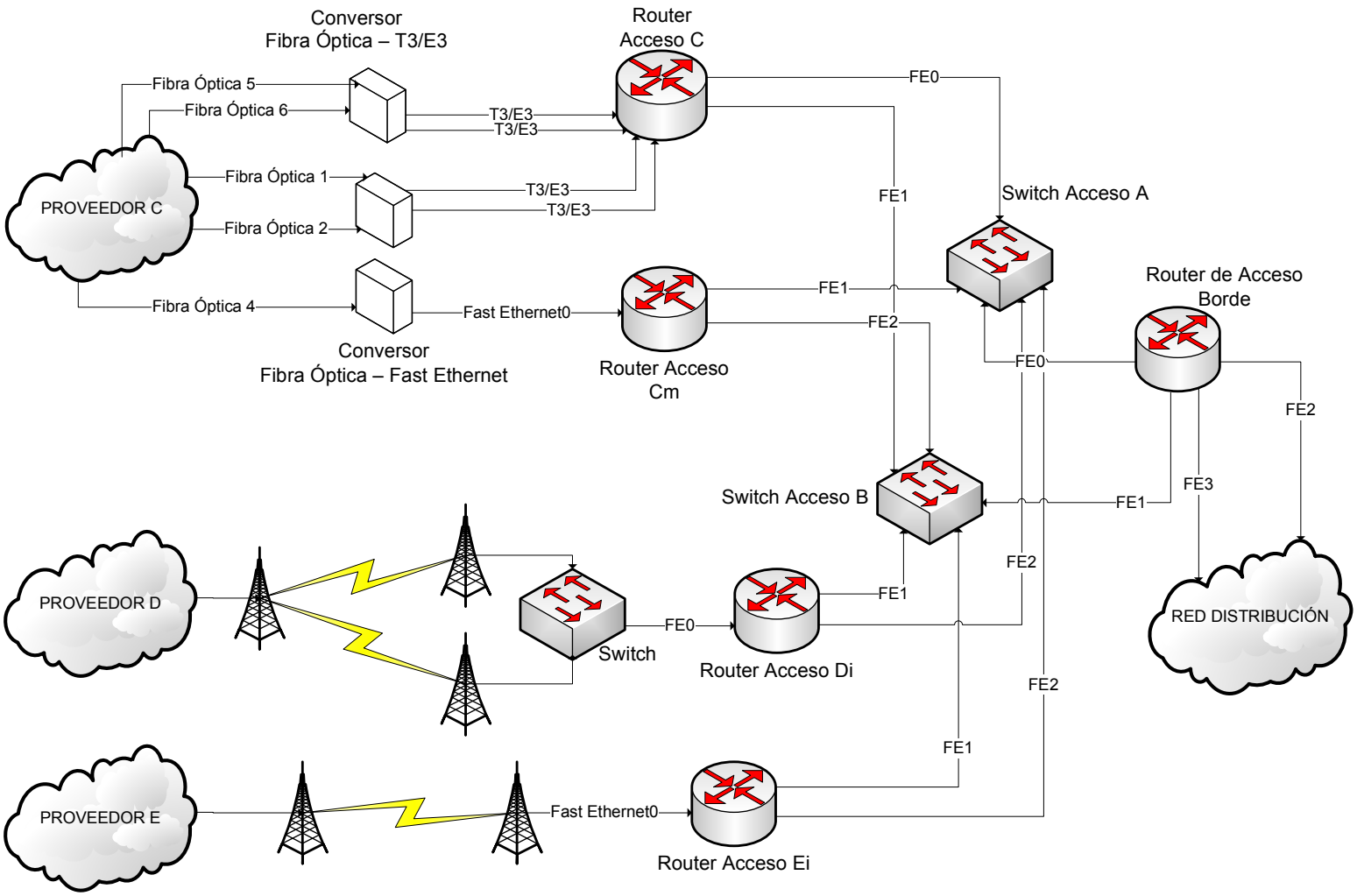


Figura 3.8 Tercera Alternativa de Diseño de Red de Acceso

- Soporte de firewall y sistema detección de intrusos (IDS).
- Soporte SNMP, versiones 1,2 y 3.
- Soporte STP.

### 3.2.3 REDISEÑO DE LA RED DE DISTRIBUCIÓN

En esta sección de la red, la situación es un tanto más complicada; ya que se debe mantener una eficiente comunicación entre la red de acceso, la red de borde, la red interna y separar la red de monitoreo y soporte.

#### 3.2.3.1 Primera Solución de Red de Distribución

La primera solución sería cambiar el switch principal de 24 puertos, por uno de 48 puertos, que siga siendo administrable y que supere las características de buffer de almacenamiento y de conmutación de paquetes del Switch A. Este nuevo switch tendría el nombre de Switch Ai. Reubicando el Switch A de 24 puertos, para la tercera alternativa de la red de borde. La Figura 3.9 muestra la primera solución.

Se aumenta el número de puertos porque eso permitiría la conexión de otros equipos para servicios adicionales como por ejemplo voz o televisión, ya que actualmente, según la Figura 1.3 todos los equipos activos están concentrados en el Switch A, que no tiene lugar para conectar un solo equipo activo adicional.

#### 3.2.3.2 Segunda Solución de Red de Distribución

La segunda solución de igual manera sería cambiar el switch de 24 puertos, por otro de 24 puertos con el resto de características iguales a las del switch especificado para la primera solución (excepto obviamente en el número de puertos) y que se llamará Switch Aii.

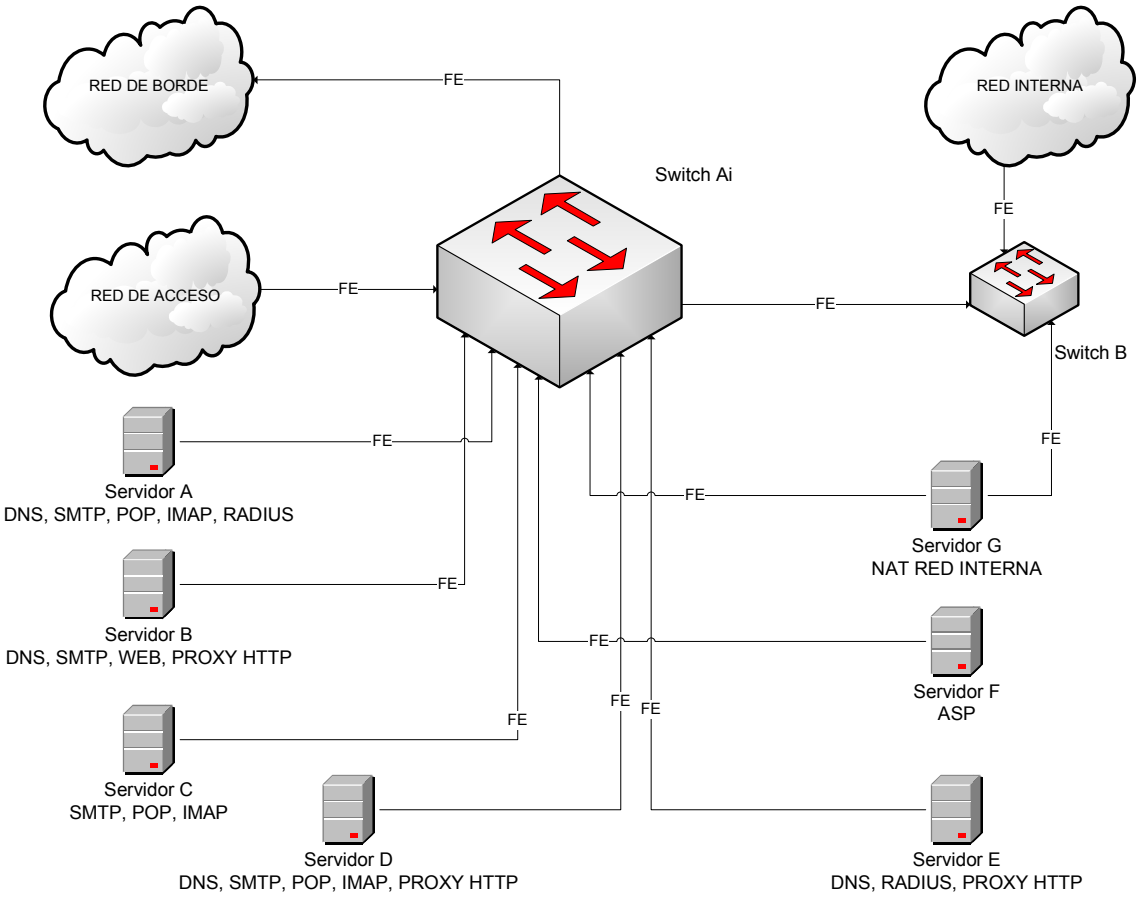


Figura 3.9 Primera Alternativa de Diseño de la Red de Distribución

Reutilizando el switch A de 24 puertos, para la granja de servidores y ubicando un router con 2 interfaces Fast Ethernet; y, características recomendadas por el fabricante de memoria no volátil, procesador y suficiente capacidad para almacenar y ejecutar un sistema operativo con soporte para:

- Listas de acceso.
- Cifrado en el acceso remoto (SSHv2).
- IS-IS OSI.
- OSPF.
- Firewall e IDS.
- Autocompletado de caracteres en línea de comandos.
- Etiquetas IEEE 802.1q.
- GTS.
- Definición de parámetros SLA.
- SNMP, versiones 1,2 y 3.
- STP.
- NAT y PAT (*Port Address Traslation*).

Este router será llamado Router de Servidores.

Adicionalmente, un cambio del servidor G por un router con características similares a las del Router de Servidores, que permita manejar el tráfico o área de la red interna y de monitoreo con el IGP escogido. Este router será nominado como Router de Red Interna.

La segunda solución es la mostrada en la Figura 3.10.

#### 3.2.3.3 Tercera Solución de Red de Distribución

La tercera solución es el esquema técnicamente recomendado, sin embargo; puede involucrar una gran inversión y cambios en los tres módulos de la Red del ISP.

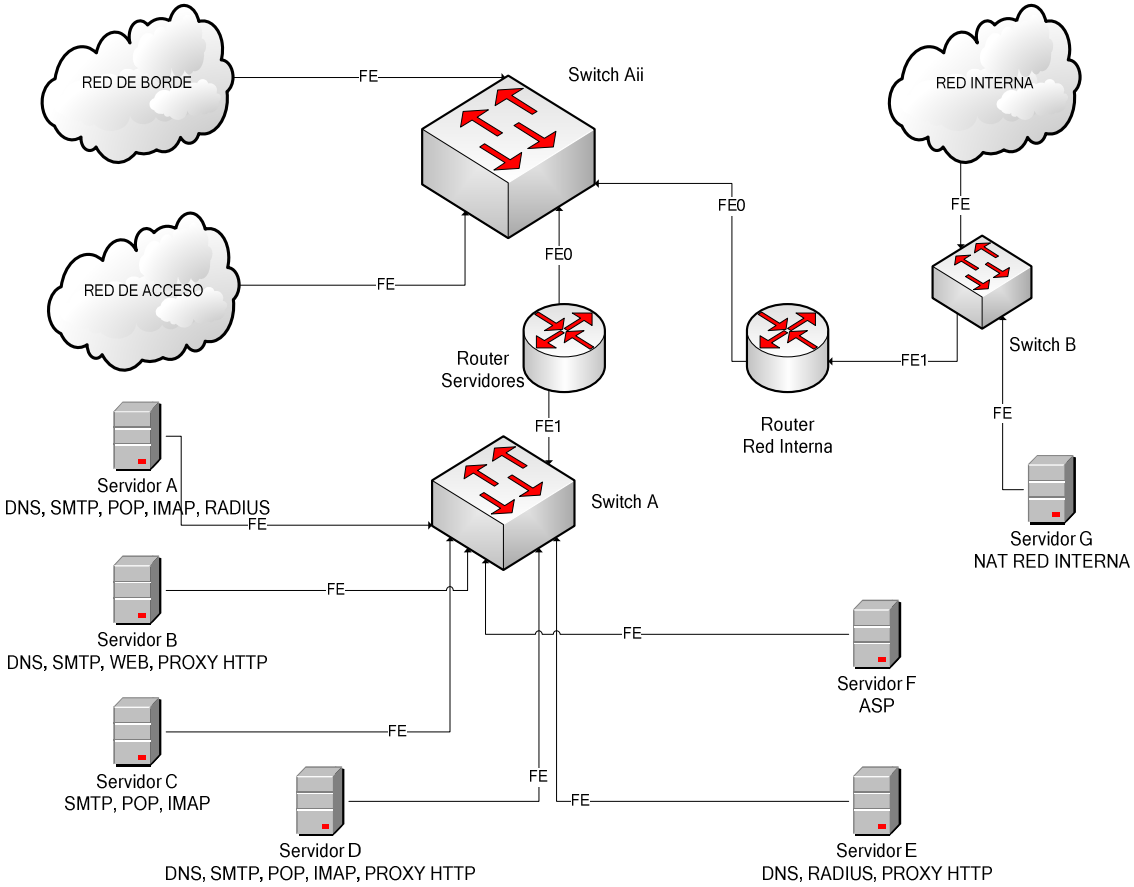


Figura 3.10 Segunda Alternativa de Diseño de Red de Distribución

El esquema es redundante e involucra dos switchs de 24 puertos en la red de distribución (Switch Aii, Aiii) y la necesidad de que tanto los routers de Acceso, como los de Borde y los recientes routers aumentados de la segunda solución, tengan un puerto adicional FastEthernet, más la característica de que todos los equipos activos deben soportar en su sistema operativo el protocolo STP.

La tercera solución es la que se muestra en la Figura 3.11.

## 3.3 SELECCIÓN DE LA MEJOR OPCIÓN[1][2]

No cabe duda, que las alternativas entregadas en las secciones anteriores son soluciones que varían desde la más económica hasta la más cara y son soluciones que avanzan desde una solución temporal, hasta una solución a largo plazo.

Lastimosamente, no depende del Departamento Técnico de ReadyNet la selección de una de las soluciones presentadas para cada módulo de la red, sino del Departamento de Adquisiciones, que junto con la Gerencia Técnica y el Departamento Financiero; revisarán costos de cada solución presentada y las debidas cotizaciones recibidas por parte de su único proveedor de equipos.

Sin embargo, la presente sección pretende definir los requerimientos y adquisiciones mínimas de cada solución para la toma de decisiones en la empresa, junto con un valor estimado y referencial por cada solución. Los equipos que pueden cumplir con los requerimientos solicitados, junto con los sistemas operativos disponibles, se encuentran en el Anexo B, ya que el ISP decide siempre en base a las alternativas que su proveedor de equipos le presenta y que son específicamente de una marca, *Cisco Systems, Inc*. Se presentarán 3 equipos de *Cisco Systems, Inc.*, que pueden cumplir con lo requerido en cada red.

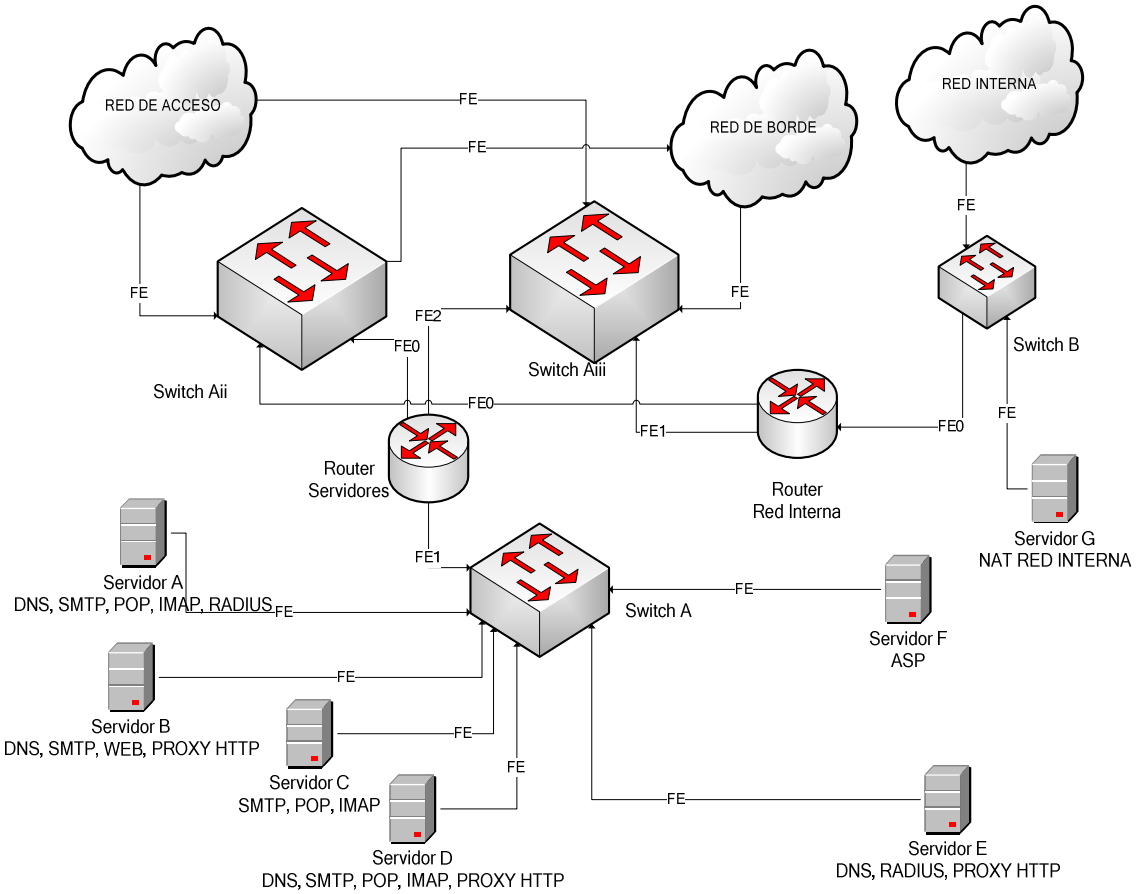


Figura 3.11 Tercera Alternativa de Diseño de la Red de Distribución

### 3.3.1 SELECCIÓN DE LA RED DE BORDE [38][39][40][41][42][43][44]

La Tabla 3.22, emite un resumen del equipamiento requerido en cada solución detallada en el presente proyecto para la red de Borde, junto con un costo estimado referencial de los equipos que pueden cumplir con lo requerido, según el dimensionamiento y rediseño de la red.

De igual manera, dicha tabla aclara que las soluciones fueron mencionadas, desde la más barata pero menos eficiente, hasta la más cara pero compleja y eficiente.

| Solución | Equipos Activos | Puertos FastEthernet | Costo Referencial [USD] |
|---|---|---|---|
| **Primera** | **Router de Borde Ai** | **2** | **$4.100 - $19.300** |
| Segunda | Router de Borde Ai | 2 | $4.100 - $19.300 |
| | Router de Borde Bi | 2 | $4.100 - $19.300 |
| **Costo Total Referencial Segunda Solución** | | | **$8.200 – $38.600** |
| Tercera | Router de Borde Bii | 3 | $14.100 - $21.500 |
| | Switch de Borde | 8 | $1.200 - $8.990 |
| **Costo Total Referencial Tercera Solución** | | | **$15.300 – $30.490** |
| Cuarta | Router de Borde Aii | 3 | $5.100 - $21.500 |
| | Router de borde Biii | 3 | $5.100 - $21.500 |
| | Switch de BordeA | 8 | $1.200 - $8.990 |
| | Switch de Borde B | 8 | $1.200 - $8.990 |
| | Switch de Borde C | 8 | $1.200 - $8.990 |
| **Costo Total Referencial Cuarta Solución** | | | **$17.700 – $82.480** |

Tabla 3.22 Equipos y Costos Referenciales del Rediseño de la Red de Borde.[1]

Los equipos que cumplen con los requerimientos de los Routers de Borde Ai, Aii, Bi,Bii, serían los siguientes:

- Cisco 2851
- Cisco 3845
- Cisco 7206VXR (NPE-G1)

[1] El amplio rango de costos referenciales se debe a que los equipos activos se pueden conseguir nuevos, usados o incluso reensamblados. De igual manera con los módulos de red adicionales.

Los equipos que cumplen con los requerimientos de los Routers de Borde Aii y Bii, serían los mismos mencionados, sin embargo; el costo referencial aumenta por la adquisición de los módulos FastEthernet.

Los equipos que cumplen con los requerimientos para el Router de Borde Bii, serían los siguientes:

- Cisco 7301
- Cisco 7507
- Cisco 7513

Los equipos que cumplen con las características requeridas para los Switches de Borde, A, B, y C, serían los siguientes:

- Cisco Catalyst 3560-8PC
- Cisco Catalyst 3750G-16TD[1]

Tomando en cuenta que el presente proyecto, pretende brindar soluciones que permitan explotar el hecho de registrar recursos de Internet y comunicar de manera eficiente los distintos sectores de la red, la solución escogida será la cuarta. Vale la pena especificar que las características de cada uno de los equipos mencionados se encuentran en el Anexo B.

### 3.3.2 SELECCIÓN DE LA RED DE ACCESO[38][39][40][41][42][43][44]

En la Tabla 3.23, se presenta un resumen de equipos activos y partes requeridas en las distintas soluciones de la red de Acceso, que identifican a las soluciones desde la más barata y menos eficiente, hasta la más cara y eficiente.

Los números de parte correspondientes al módulo de la tarjeta Fast Ethernet y de la tarjeta ATM/DS3, son para un router *Cisco 7206VXR (NPE-400)*.

[1] El switch es de 16 puertos, porque no existe una solución de 8 puertos en esa serie de switches.

| Solución | Partes | Equipo Activo | Puertos FastEthernet | Costo Referencial [USD] |
|---|---|---|---|---|
| Primera | Tarjeta FastEthernet para Router C | | | $250 |
| | Tarjeta ATM/DS3 para Router C | | | $1.900 |
| | | Router Cm | 2 | $4.100 -$19.300 |
| **Costo Total Referencial Primera Solución** | | | | **$6.250 – $21.450** |
| Segunda | Tarjeta FastEthernet para Router C | | | $250 |
| | Tarjeta ATM/DS3 para Router C | | | $1.900 |
| | | Router Cm | 2 | $4.100 -$19.300 |
| | | Router Di | 2 | $4.100 -$19.300 |
| | | Router Ei | 2 | $4.100 -$19.300 |
| **Costo Total Referencial Segunda Solución** | | | | **$14.450 - $60.050** |
| Tercera | 2 Tarjetas FastEthernet para Router C | | | $500 |
| | Tarjeta ATM/DS3 para Router C | | | $1.900 |
| | | Router de Acceso Borde | 4 | $5700 - $22.100 |
| | | Router Cm | 3 | $5.100 - $21.500 |
| | | Router Di | 3 | $5.100 - $21.500 |
| | | Router Ei | 3 | $5.100 - $21.500 |
| | | Switch de Acceso A | 24 | $3400 - $5.500 |
| | | Switch de Acceso B | 24 | $3400 - $5.500 |
| **Costo Total Referencial Tercera Solución** | | | | **$30200 - $99.400** |

Tabla 3.23 Partes, Equipo Activo y Costos Referenciales del Rediseño de la Red de Acceso.

Los equipos que cumplen con las características para el Router Cm, Di, Ei, y Router de Acceso de Borde, son los siguientes:

- Cisco 2851
- Cisco 3845
- Cisco 7206VXR (NPE-G1)

Para la tercera solución, se tomó en cuenta el costo de cada módulo Fast Ethernet Adicional en cada router de acceso.

Los equipos que cumplen con las características para los Switches de Acceso A y B, serían los siguientes:

- Catalyst 3560G-24TS/PS[1]
- Cisco Catalyst 3750G-24TS/WS[2]

Al igual que con la red de borde, para cumplir con el objetivo de explotar al máximo el registro de recursos de Internet y para tener una eficiente comunicación con el resto de módulos de la red, la solución escogida, será la tercera.

### 3.3.3 SELECCIÓN DE LA RED DE DISTRIBUCIÓN[38][39][40][41][42][43][44]

La Tabla 3.24, presenta un resumen del equipo activo y los requerimientos de cada solución mencionada en las secciones correspondientes del rediseño de la red de distribución y su costo referencial.

| Solución | Equipos Activos | Conmutación de Paquetes | Puertos FastEthernet | Costo Referencial [USD] |
|---|---|---|---|---|
| **Primera** | **Switch Ai** | **> 6,6Mpps** | **48** | **S5.800 – $17.100** |
| Segunda | Switch Aii | >6,6Mpps | 24 | $3.400 - $5.500 |
| | Router Servidores | | 2 | $4.100 -$19.300 |
| | Router Red Interna | | 2 | $4.100 -$19.300 |
| **Costo Total Referencial Segunda Solución** | | | | **$11.600 - $44.100** |
| Tercera | Switch Aii | >6.6Mpps | 24 | $3.400 - $5.500 |
| | Switch Aiii | >6.6Mpps | 24 | $3.400 - $5.500 |
| | Router Servidores | | 3 | $5.100 - $21.500 |
| | Router Red Interna | | 3 | $5.100 - $21.500 |
| **Costo Total Referencial Tercera Solución** | | | | **$17.000 - $54.000** |

Tabla 3.24 Equipos y Costos Referenciales del Rediseño de la Red de Distribución

[1] Son dos equipos de la misma serie, con características distintas.
[2] Son dos equipos de la misma serie, con características distintas.

Nuevamente se nota que el orden de las soluciones fue presentado desde la más barata y menos eficiente, hasta la más compleja y cara.

Los routers que cumplen con las características requeridas para el Router de Servidores y Router Red Interna, son los siguientes:

- Cisco 2851
- Cisco 3845
- Cisco 7206VXR (NPE-G1)

Los equipos que cumplen con las características requeridas para el Switch Ai, serían los siguientes:

- Cisco Catalyst 2975
- Cisco Catalyst 3560G-48TS/PS
- Cisco Catalyst 3750-48TS

Los equipos que se ajustan a lo requerido para los Switches Aii, y Aiii son los siguientes:

- Catalyst 3560G-24TS/PS[1]
- Cisco Catalyst 3750G-24TS/WS[2]

Dado que se logra una segmentación física de la red interna, con la red de servidores y el resto de módulos de la red, con la segunda y tercera solución; pero que solo se logra redundancia con la tercera solución y dado que es fundamental aprovechar el registro de recursos de Internet, la solución a escoger será la tercera.

Se tienen registros de la adquisición del Switch A que se incorporó a la Red de Distribución desde finales del año 2005, dado que el Switch que estaba operativo

[1] Son dos equipos de la misma serie, con características distintas
[2] Son dos equipos de la misma serie, con características distintas

colapsó por un daño en la fuente principal. En ese entonces, no se tenía otro equipo a la mano, ni existía un esquema redundante y hasta conseguir otro equipo que reemplace al anterior, los clientes estuvieron un día sin servicio. En ese año las pérdidas para el ISP fueron considerablemente fuertes, ya que se tuvieron que generar notas de crédito debido a la falla a una gran cantidad de clientes, tomando en cuenta que el costo de un enlace de 64 kbps era de cientos de dólares.

Actualmente, y en un futuro no muy lejano, la tendencia es que las actividades de comercio electrónico en el Ecuador aumenten. Muchas entidades bancarias y gubernamentales hoy en día ofrecen servicios en línea junto con la posibilidad de realizar transacciones e intercambio de información relevante; lo que implica que en temas de disponibilidad se puede ganar mercado con el usuario final y con una entidad de comercio electrónico. Pero si el ISP no toma las medidas adecuadas para brindar parámetros necesarios de disponibilidad de servicios y redundancia, se corre el riesgo de salir fácilmente del mercado.

# CAPÍTULO 4

# 4 PROCESO Y PLANIFICACIÓN DE LA MIGRACIÓN DE SERVICIOS Y CLIENTES

Para que el ISP a se convierta en Sistema Autónomo, la respectiva migración se debe especificar en un proceso, un procedimiento y una planificación; primero para obtener un ASN y adquirir los prefijos necesarios de direcciones IP, después para comenzar a funcionar en el Internet bajo dichos prefijos, y luego migrar la lógica de enrutamiento actual a las políticas definidas en el diseño.

Todos los procedimientos deben ser realizados de manera ordenada y de la forma más transparente posible para los clientes del ISP.

Todo el proceso macro, se puede dividir en tres subprocesos, junto con tareas, responsables, tiempos de respuesta y tiempos críticos. Los tres procesos son:

- Selección del Protocolo IGP a utilizar, definición de parámetros.
- Registro de ASN y un prefijo IP en el RIR correspondiente.
- Migración de Redes y Servicios de Clientes.

## 4.1 SELECCIÓN DEL PROTOCOLO IGP[3][11][16][20][21][23]

De los protocolos más utilizados, y en base a los requerimientos de diseño, se puede seleccionar IS-IS u OSPF, sobretodo, por el tema de escalabilidad; si llegase a ser necesario crecer, no se va a tener un limitante en el número de equipos que puedan formar parte del Sistema Autónomo o de un Dominio de Enrutamiento. En términos comparativos se dice que, según la jerarquía de cada modelo de referencia, un sistema autónomo y un dominio de enrutamiento son lo mismo.

Ambos protocolos han tenido un largo uso, desarrollo y mejoras en el soporte de los protocolos del stack TCP/IP. Muchos fabricantes los implementan y muchos portadores de datos a nivel mundial los usan ampliamente; sin embargo, el hecho de usar IS-IS prácticamente obliga a que el protocolo de enrutamiento de borde sea IDRP.

Tomando en cuenta que la ampliación de un ASN a un número de 32 bits es un hecho, que en Ecuador la totalidad de Sistemas Autónomos hablan BGP, y que ese es el protocolo de borde escogido, se podría utilizar OSPF como IGP; no se descartan protocolos como IGRP o EIGRP, sin embargo, eso sería limitar la interoperabilidad, al tener que usar únicamente equipos de un fabricante en específico.

### 4.1.1 DEFINICIÓN DE PARÁMETROS

En caso de que la primera opción de todos los diseños físicos de la red, sea la escogida por la parte Administrativa del ISP, probablemente por costos, no sería necesario un IGP, sino únicamente el protocolo de borde y pasar al siguiente proceso.

Sin embargo, todas las últimas soluciones brindadas en el diseño, implican redundancia, y permitirían la implementación de un IGP que separe adecuadamente las redes de acceso, borde y distribución del ISP. Como el IGP seleccionado fue OSPF, y la nueva topología de Red permitiría una plena distribución de la Red en áreas, ese sería el siguiente paso del proceso.

Dicha separación permitirá disminuir el tráfico de cada segmento de red y evitará tráfico innecesario o caminos extensos de los paquetes para llegar a un servicio brindado en el ISP que corresponda al esquema de direccionamiento distinto al del cliente que los originó.

#### 4.1.1.1 Distribución de Áreas.

Es necesario especificar el área de backbone, o área 0 (cero), el área de servidores, el área de monitoreo y el área de borde. Todo esto tomando en cuenta, las últimas soluciones escogidas para cada una de las secciones de la totalidad de la red del ISP. La segmentación lógica de la red en base a áreas se muestra en la Figura 4.1.

##### *4.1.1.1.1 Área 0*

Todos los interfaces de los router de borde Bii y Aii que tengan conexión con los switches Aii y Aiii, más los interfaces del router de acceso borde, router de servidores, router de red interna, y el RAS del proveedor C, conectados a dichos switches, pertenecerían a esta área.

##### *4.1.1.1.2 Área 1*

En resumen es el área que tendría como única salida al router de servidores y que maneja una LAN con todos los equipos conectados al switch A. Generalmente este tipo de áreas son conocidas como áreas stub, lo que significa que ningún tipo de enrutamiento externo distinto al inyectado por OSPF ingresa al área, y que para la comunicación con el mundo exterior se manejan únicamente rutas por defecto.

##### *4.1.1.1.3 Área 2*

Es la sección conformada únicamente por el router de la red interna, como router de borde de área (ABR), de igual manera un área stub, donde estará la red interna de ReadyNet Cia. Ltda nuevamente junto con la red de monitoreo, sin embargo, con módulos de red fácilmente alcanzables por el NOC del ISP.

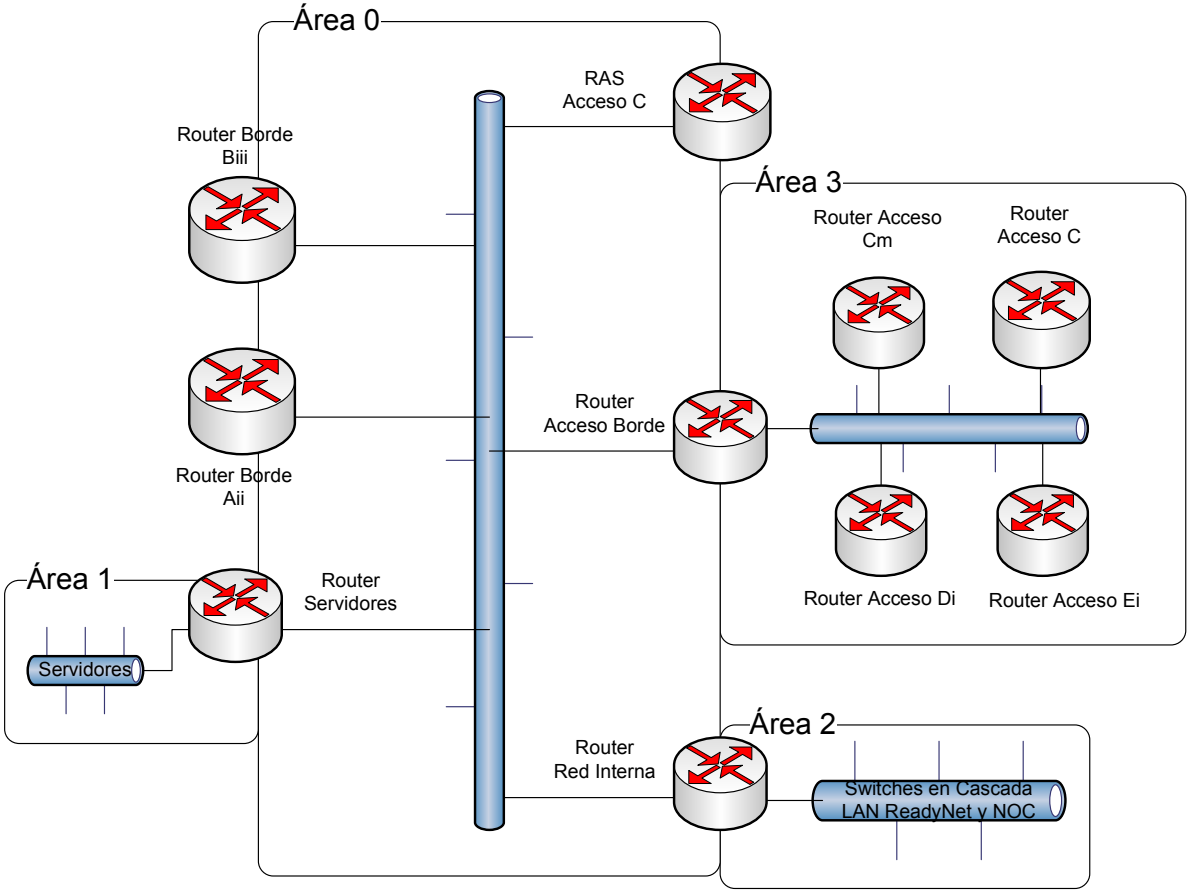


Figura 4.1 Esquema de Distribución de Áreas

*4.1.1.1.4 Área 3*

Contiene a todos los routers que permiten al usuario final conectarse con los servicios brindados por el ISP, en este caso, uno de los routers funcionará como router designado (DR) y otro como router designado de respaldo (BDR).

La selección es realizada cuando los routers arrancan su operación en base a paquetes Hello y son únicamente seleccionados en segmentos de red tipo difusión, como en este caso.

Parámetros configurados en cada router de acceso, como el identificador del router y la prioridad del mismo, definen ambos elementos del área, que no hacen más que evitar una inundación de publicaciones de redes exteriores e interiores al área por todos los routers del segmento, sino que todos los routers generan adyacencias con el DR y BDR para intercambiar LSAs solo en el caso de un cambio en la topología de la red.

### 4.1.1.2 Distribución de prefijos IP

Una vez que se tiene a la red del ISP claramente segmentada, es necesario especificar el esquema de direccionamiento IP del ISP. Lo más importante es tomar en cuenta el número de equipos conectados actualmente, más un crecimiento razonable en 5 años.

*4.1.1.2.1 Área 0*

Para el segmento de la red de borde se necesita 6 direcciones válidas al menos, 2 para la administración de cada switch de borde y al menos dos para cada router de borde. Asumiendo que el ISP podría tener un proveedor adicional para su salida internacional en pruebas, se podrían requerir dos direcciones IP más.

Una dirección IP para el router de borde del área 2, otra para el router de borde del área 1, una más para el router de acceso borde y una última para el RAS de acceso C. A esto hay que añadir dos direcciones IPs para los switches de la red de distribución.

Se tendría un total de 15 direcciones IP válidas disponibles en dicha área. Un prefijo con máscara /27 sería suficiente para el área 0, dejando libres otras 15 direcciones IP para pruebas o incluso, para agregar más equipos al backbone del ISP.

#### *4.1.1.2.2 Área 1*

En el área de servidores, se requiere una dirección IP para el router de servidores y una por cada uno de los servidores A,B,C,D, y F. Dando un total de 6 direcciones IPs para esta área. Sin embargo, cabe recordar que el ISP brinda el servicio de server hosting; asumiendo que se pueden tener más de 6 servidores de clientes alojados en el ISP (actualmente existen 2), se hablaría de 12 direcciones IP requeridas, por lo que un prefijo /28 sería necesario y suficiente para el área 1, dejando la posibilidad de aumentar hasta 30 equipos en dicha área, bien sean de servicios adicionales, o bien sean de otros clientes que necesiten que sus servidores estén conectados directamente al internet.

#### *4.1.1.2.3 Área 2*

El área de la red interna, definitivamente no necesita direccionamiento público, más que el considerado en el área 0. Con NAT (*Network Address Translation*) habilitado en el router y manejando dos esquemas de direccionamiento privados, uno para monitoreo y otro para el resto de departamentos de la empresa, se podría discriminar ambos sectores de la red interna del ISP.

*4.1.1.2.4 Área 3*

Éste es el segmento más trascendente dentro de la red, ya que directamente los clientes tendrán acceso al Internet y los servicios ofrecidos por el ISP a través de este segmento. Según la Tabla 1.6, los 9 prefijos utilizados actualmente no necesariamente reflejan un uso óptimo de las direcciones IP.

Tomando en cuenta que por abonado es necesaria una dirección IP pública, sea ésta dinámica o fija, junto con la Tabla 3.8 se puede decir que serían necesarios la cantidad de prefijos IP en la red de acceso, proyectado año a año que se muestra en la Tabla 4.1.

| Año | Total ReadyNet | Prefijo /24 Requerido |
|---|---|---|
| 2008 | 600 | 3 |
| 2009 | 713 | 3 |
| 2010 | 847 | 4 |
| 2011 | 1006 | 4 |
| 2012 | 1196 | 5 |
| 2013 | 1421 | 5 |

Tabla 4.1 Prefijos IPv4 Requeridos Proyectados a 5 años

Aún cuando, hay que tomar en cuenta que actualmente existen clientes con rangos de direcciones que abarcan más de una dirección pública, definitivamente el enrutamiento debe cambiar para justificar al RIR correspondiente los prefijos a solicitar.

Dando una totalidad de 4 prefijos /24 IPv4, requeridos para el funcionamiento lógico del ISP.

## 4.2 REGISTRO DE ASN Y DE UN PREFIJO IP [24][25][26][27][28][29]

El procedimiento de ambos recursos está claramente especificado en el sitio web de LACNIC, el RIR que corresponde a la ubicación de Ecuador.

El primer paso es conseguir tres identificadores de usuario, uno para el contacto técnico, otro para el contacto de facturación y el tercero para la organización que desea obtener bien sea un número ASN o un bloque IPv4 o IPv6. Estos usuarios, se los puede registrar en el sistema disponible en http://lacnic.net/cgi-bin/lacnic/idmng?lg=SP.

El segundo paso es llenar el formulario correspondiente, en primer lugar para el registro del ASN, dicho formulario está disponible en el sitio web de LACNIC, en el URL: http://lacnic.net/templates/asn-template-sp.txt .

LACNIC entregará un ASN cuando se cumpla con los siguientes requisitos:

- La organización debe ser multiproveedor y dichos proveedores deben ser dos o más Sistemas Autónomos independientes al momento de la solicitud, o tener programado convertirse en multiproveedor en menos de dos semanas a partir del momento de la solicitud.
- Enviar documentación que describa la política de enrutamiento de la organización solicitante, que debe ser única y distinta de aquella aplicada por el ASN al cual se conecta. Dicha documentación incluye al protocolo de enrutamiento exterior a utilizar, las direcciones que van a componer el SA y una detallada explicación de las razones por las cuales, la política de enrutamiento de la organización solicitante, es distinta a aquella a la de sus proveedores.

ReadyNet Cia. Ltda, posiblemente tendrá que utilizar los prefijos asignados por los proveedores de borde A y B en un inicio. LACNIC, ofrece un sistema de administración de recursos de Internet, donde maneja la información del sistema WHOIS donde se debe representar 3 puntos de contacto distintos:

- El contacto dueño (owner – contact) que representa al contacto administrativo de la organización a la que el ASN fue asignado.

- El contacto de enrutamiento (routing – contact), contacto que registra las políticas de enrutamiento adoptadas por el Sistema Autónomo.
- El contacto de abuso (abuse – contact), que es un contacto de seguridad o de reporte de problemas.

El tercer paso es registrar un bloque mínimo /21 (bloque de 8 /24), necesario y suficiente para el ISP. Llenando el formulario disponible en el sitio web de LACNIC bajo la URL: http://lacnic.net/templates/isp-v4-template-sp.txt

LACNIC no entrega más que dicho prefijo inicialmente, previo cumplimiento y verificación de los siguientes requisitos:

- Demostrar el uso o la necesidad inmediata de un /23 (4 bloques /24).
- Entregar un plan detallado de uso de un /22 a un año (8 bloques /24).
- Aceptar, regresar los bloques IP entregados por sus ISPs a no más tardar de 12 meses a partir de la distribución del /21.

Todo esto, porque el espacio de direcciones IPv4 públicas es limitado y entregado en un modelo de lento inicio, siempre basadas en una necesidad justificada actual y no en base a predicciones de número de clientes, estudios de mercado, etc.

Tanto el formulario de registro de un ASN y de un prefijo /21, deben ser enviados por correo electrónico a hostmaster@lacnic.net y deben ser parte del cuerpo del correo electrónico.

Una vez que la solicitud de un recurso de Internet ha sido aprobada, es necesario hacer un pago relacionado a cada recurso. Actualmente el costo de un ASN es de 1000 dólares americanos y no se factura monto adicional por mantenimiento de dicho recurso. La Tabla 4.2 muestra las categorías de los bloques IPv4 y sus precios, según el prefijo requerido en LACNIC:

| Categoría | Tamaño | Monto Inicial USD | Monto Renovación USD | Renovación anual (antes de 60 días del vencimiento de la factura) |
|---|---|---|---|---|
| Small/Micro | < /20 | 1.000 | 1.000 | 900 |
| Small | ≥ /20 = /19 | 2.100 | 2.100 | 1.890 |
| Medium | > /19 = /16 | 5.700 | 5.700 | 5.130 |
| Large | > /16 = /14 | 12.000 | 12.000 | 10.800 |
| Extra Large | > /14 = /11 | 23.500 | 23.500 | 21.150 |
| Mayor | > /11 | 35.000 | 35.000 | 31.500 |

Tabla 4.2 Costo de Servicios LACNIC – Fuente www.lacnic.net

## 4.3 MIGRACIÓN DE REDES Y SERVICIOS DE CLIENTES [30][31]

El punto crítico del salto de pasar a ser parte de dos Sistemas Autónomos distintos a ser uno solo, con una política de enrutamiento diferente a las de los proveedores actuales de salida a Internet de ReadyNet Cia. Ltda, es justamente eso, anunciar al Internet su existencia y comenzar a publicar sus servicios en el nuevo esquema.

Cabe recalcar, que este punto del proceso, arranca desde que el ISP logra registrar un prefijo /21 en LACNIC y se realiza la inversión necesaria para que un IGP corra dentro del SA de manera que maneje parámetros de escalabilidad y disponibilidad necesarios y suficientes para brindar un servicio de calidad, como los mencionados en el capítulo de diseño.

### 4.3.1 MIGRACIÓN FÍSICA DE LA RED

El primer paso de este proceso, es cambiar la topología física de la red en cada punto, con el esquema de direccionamiento actualmente asignado y manteniendo las políticas usadas hoy en día por el ISP.

Una vez que el esquema físico ha sido adoptado, se debe comenzar a manejar pruebas de IGP con el nuevo esquema de direccionamiento, verificando que no existan errores en las configuraciones. El enrutamiento estático es mantenido en conjunto con OSPF dentro del Sistema Autónomo. Las pruebas deberán tener una duración de al menos un mes.

### 4.3.2 MIGRACIÓN DE SERVICIOS

Por facilidad, cualquier aplicación que se ejecute sobre TCP/IP, antes de recordar una dirección IP, recuerda un nombre, por ende, la publicación de servicios está asociada directamente al sistema jerárquico de resolución de nombres DNS. Por lo que el siguiente paso es el cambio que involucra al sistema DNS.

Aprovechando que ReadyNet Cia. Ltda., maneja tres dominios principales y que los dos primeros están publicados en los servidores A y B, y que el tercero está definido en los servidores D y E; el procedimiento a realizar es usar el segundo dominio publicado en los servidores A y B, haciendo que consten como DNSs autoritativos de dicha zona el servidor A, el servidor D y un servidor temporal configurado como DNS, que pertenezca a las nuevas direcciones IP registradas por el ISP.

Procedimiento que deberá ser realizado en la tarde de un viernes para que pasado el mínimo tiempo de vida TTL (*Time To Live*) de los registros de recursos RR (*Resource Registries*) de las zonas del dominio se anuncien en Internet, y el día lunes siguiente no se tenga inconvenientes. Necesariamente un servidor de correo que pertenezca al nuevo rango, también será necesario, incluso, podría ser el mismo equipo.

Luego de que dicho dominio esté plenamente resuelto en el Internet bajo los nuevos recursos anunciados, se procede a ingresar al servidor temporal como servidor autoritativo de los otros dominios principales del ISP, previa configuración

de las zonas correspondientes y en todos y cada uno de los dominios de los clientes.

Esto se realizará previa comunicación a los clientes en donde no se tiene injerencia con el registrante de sus dominios para que añadan el DNS temporal recientemente creado. Otro boletín informativo debe ser enviado a los clientes, indicando las nuevas direcciones IP de los servidores DNS preferidos y alternativos a utilizar en cada una de las conexiones, más un instructivo de dónde cambiar dicha información en los equipos terminales de los clientes.

Se procede al cambio de los otros dos dominios principales simultáneamente, luego de 15 días de depurar cualquier inconveniente que el cambio en el primer dominio causare. Tiempo durante el cual, todas las zonas de reversa de las redes sean escritas coherentemente y se mantengan aún las zonas de reversa de las redes a devolver a cada proveedor de salida internacional.

Para hacer más explicativo este procedimiento, se afirmará que los tres dominios principales serán: a.TLD (*Top Level Domain* o Dominio de Alto Nivel), b.TLD, y c.TLD. Dado que prácticamente el dominio b.TLD no tiene más que 15 abonados de marcado telefónico asociados, el impacto sobre la totalidad de clientes se reduce.

Los RR asociados al dominio b.TLD serían:

- Servidor de nombres (NS) = ns1.b.TLD (nuevo recurso).
- Servidor de nombres (NS) = ns1.a.TLD.
- Servidor de nombres (NS) = ns1.c.TLD.
- Registro de Intercambio de Correo (MX) de b.TLD, con prioridad 0 = mail2.b.TLD.
- Registro de Intercambio de Correo MX de b.TLD, con prioridad 10 = antiguo registro del dominio.
- Registro A de ns1 = IP válida rango asignado al área 1.
- Registro A de mail2 = IP válida rango asignado al área 1.

El resto de registros, junto con el TTL del dominio, es necesario bajarlos a 24 horas para que el siguiente anuncio o cambio de dicho dominio, sea verificado en ese tiempo por servidores de caché u otros servidores de nombres en el Internet. Obviamente todas las cuentas de correo existentes en los dominios involucrados deben ser creadas en el servidor de correo temporal, para que durante la transición, no se pierda información, más que la involucrada directamente por el protocolo SMTP.

Luego, las zonas de los dominios a.TLD y c.TLD, únicamente tendrían tanto en el registrante del dominio, como en las zonas, un registro adicional de servidor de nombres NS (*Name Server*) con el nombre ns1.b.TLD. La información de las zonas de los dominios a.TLD y c.TLD, en el servidor ns1.b.TLD serían exactamente las mismas inicialmente. Así como en todas las zonas de los dominios de los clientes involucrados en la transición.

Al pasar los 15 días, todos los servidores dentro del Área 1, cambiarán su dirección IP a una de las nuevas asignadas, otra vez un viernes en la tarde o noche, y el resto de las zonas necesarias para los dominios a.TLD y c.TLD, únicamente cambiarán en los RR tipo A, apuntando a las nuevas direcciones asignadas siempre que dichos recursos impliquen un servicio como web, DNS, o correo.

El resto de registros A irán cambiando conforme vayan cambiando las redes de los clientes. De esta manera, el día lunes, no se perdería ninguna información porque al menos uno de los servidores registrados en todos los dominios, estaría disponible y manteniendo información correcta sobre todos los dominios de los clientes y dominios del ISP. El día lunes, los clientes que presenten problemas serán aquellos que no hayan leído la información enviada 15 días antes por el ISP.

El próximo paso, es eliminar el registro de intercambio de correo MX (*Mail eXchanger*) de respaldo de cada dominio principal del ISP, así como las reglas

que hicieron este respaldo de correo transparente para los usuarios en el servidor de correo de respaldo utilizado.

### 4.3.3 MIGRACIÓN DE CLIENTES

El resto del proceso, es un lazo, donde se irán cambiando paulatinamente uno a uno los dominios y clientes que manejen servicios dentro de sus redes y que estén publicados bajo su dominio, en un proceso muy parecido al seguido en el caso de los servicios del ISP.

Al ser cada cliente un caso especial, el personal técnico, deberá manejar de acuerdo a la magnitud de cada cliente, los viernes de cada semana, al menos 4 dominios modificados al nuevo esquema de direccionamiento.

Tomando en cuenta que existen 80 dominios publicados actualmente por el ISP, en 20 semanas la totalidad de los dominios estaría cambiada al nuevo esquema de direccionamiento.

Dado que actualmente se tiene 300 clientes banda ancha y eliminando los 80 que tienen dominio asociado, si se cambia el esquema de direccionamiento con 3 técnicos realizando 3 cambios diarios, sin tomar en cuenta los viernes que son para clientes con dominios, en 7 semanas, en el peor de los casos, los clientes que no tienen un dominio asociado, estarían cambiados al nuevo esquema de direccionamiento.

Después de este tiempo, el ISP deberá eliminar toda información de recursos asociados a los Sistemas Autónomos de sus proveedores, para cumplir con el compromiso con LACNIC, de retornar los prefijos IPv4 que actualmente administra.

De esta manera se llega al final del proceso, con lo que se convertiría a ReadyNet Cia. Ltda. en un Sistema Autónomo, con un nuevo esquema de red que permite separar de manera física y lógica los módulos de red.

## 4.4 DIAGRAMA DE FLUJO Y DE GANTT

Luego de que se detalló el proceso en cada uno de los puntos necesarios para la migración de redes y servicios del ISP hacia la nueva política de enrutamiento y el nuevo esquema de direccionamiento, se presenta un diagrama de flujo separando cada proceso, procedimiento y decisiones en la Figura 4.2.

El diagrama de Gantt presenta tareas, responsables y tiempos, más un gráfico de la ruta crítica del cumplimiento de todo el proyecto relacionado al presente capítulo. Este tipo de diagramas es utilizado en la gestión, evaluación y diseño de proyectos, ya sean estos tecnológicos o administrativos.

La fecha de inicio de la migración, depende directamente de las decisiones a nivel gerencial que se tomen.

La Figura 4.3 muestra el Diagrama de Gantt correspondiente a la migración de redes y servicios.

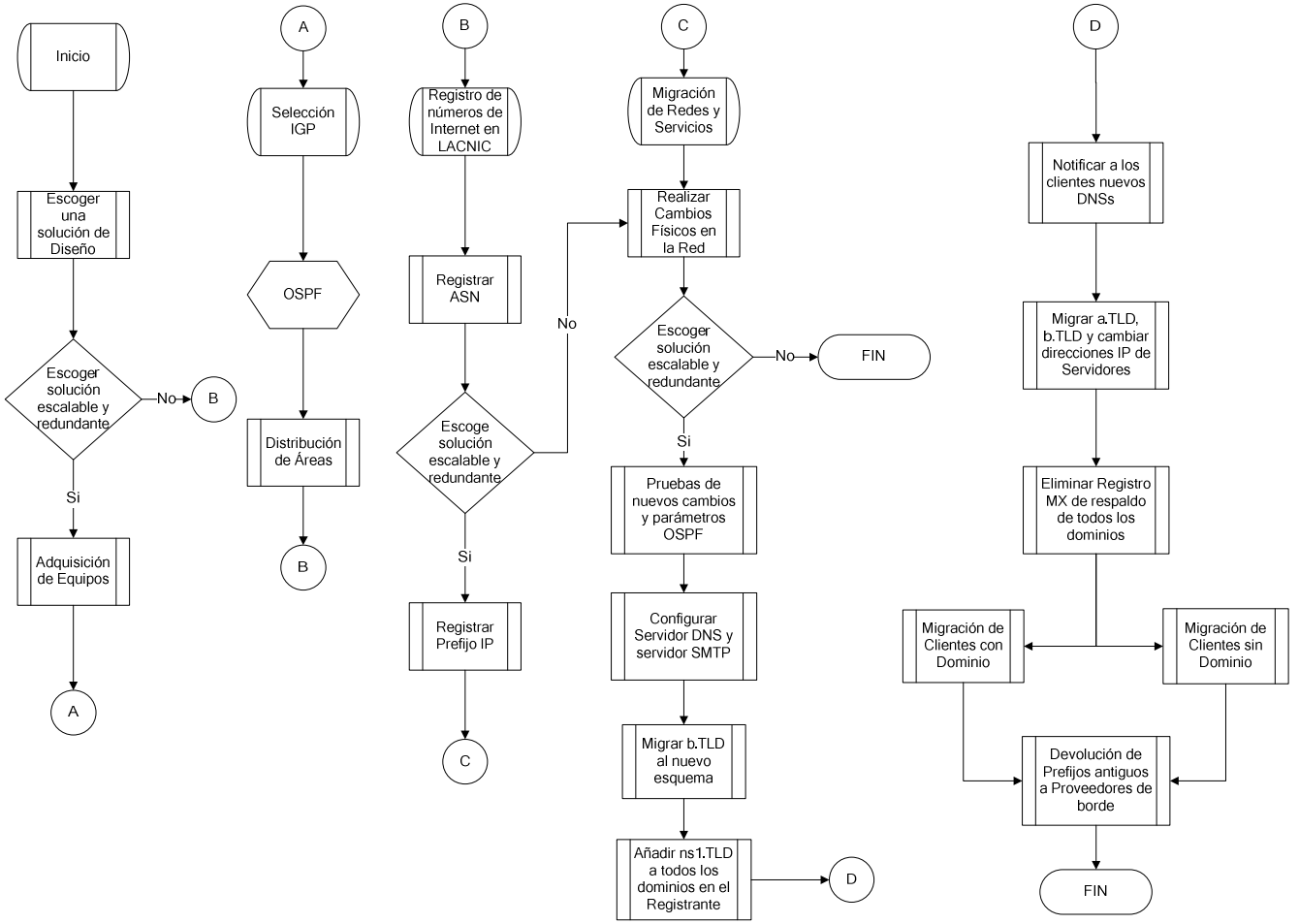


Figura 4.2 Diagrama de Flujo de Migración de Redes y Servicios

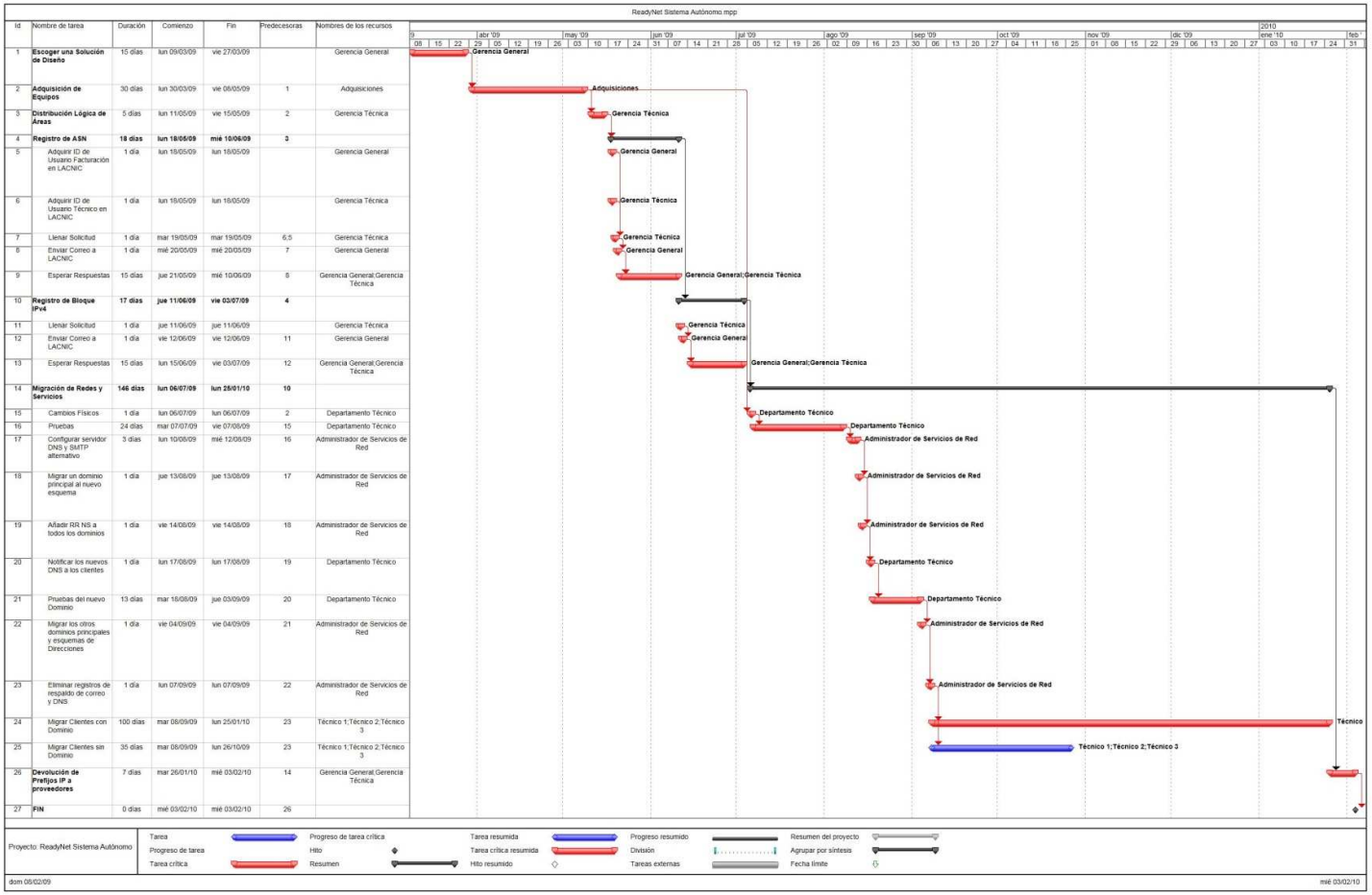


Figura 4.3 Diagrama de Gantt

# CAPÍTULO 5

# 5 CONCLUSIONES Y RECOMENDACIONES

## 5.1 CONCLUSIONES

- La política de enrutamiento actual del ISP es basada en rutas estáticas, por lo que para que los servicios disponibles en el ISP que pertenezcan a un esquema de direccionamiento IP de un proveedor de borde, puedan ser accedidos por clientes con esquema de direccionamiento IP distinto, deben salir de la red del ISP y volver a ingresar por el otro proveedor, aumentando tiempos de respuesta y congestionando los canales contratados.

- Tanto la Red de Borde, la Red de Distribución y la Red de Acceso del ISP, junto con los servidores y la red interna del ISP, se encuentran actualmente unidas por un único punto de falla, el switch principal. Los cambios propuestos en la topología física de la red, permitirán distinguir y asegurar las distintas áreas del proveedor, de manera que se comuniquen entre ellas en cualquier momento y bajo cualquier circunstancia.

- La distribución de los 9 bloques IP con máscara /24 administrados por el Departamento Técnico del proveedor es ineficiente desde el punto de vista de un RIR, en la gran mayoría de casos. El separar un bloque /30 por cada cliente involucra el desperdicio de 3 direcciones IP por abonado, pero se gana a nivel administrativo de los enlaces por el hecho de alcanzar los equipos terminales de los abonados desde cualquier lugar del Internet, ya que tienen dirección IP pública.

- El registro de un Número de Sistema Autónomo es justificable en un operador cuando el operador tiene al menos dos proveedores de conexión

a Internet, y cuando las políticas de enrutamiento de sus proveedores, difieren de la política del operador, que debe ser estrictamente única.

- La métrica utilizada por BGP para seleccionar un camino hacia un destino con varios caminos, es el resultado de la configuración de los atributos del protocolo:
    - Peso
    - Preferencia Local
    - Discriminador Multi Salida
    - Origen
    - Camino_SA
    - Siguiente Salto
    - Comunidad

  Tomando en cuenta que BGP utiliza el paradigma de reenvío de paquetes basado en el destino.

- Los protocolos de enrutamiento vector distancia, tienen un tiempo de convergencia de la red más alto que un protocolo de estado de enlace. Aún cuando existen protocolos híbridos que tienen características de ambos, en la selección de un IGP la convergencia es trascendental.

- OSPF es un protocolo de estado de enlace que permite separar un Sistema Autónomo en Áreas para evitar la inundación de LSAs a todos los routers del SA, reduciendo significativamente las tablas de enrutamiento en cada Área o la cantidad de bases de datos topológicas en el SA.

- Los protocolos de enrutamiento de la ISO utilizados en el modelo OSI, tienen su nacimiento con la idea de interconectar redes CLNP, aún cuando actualmente también soportan redes IP, su funcionalidad está basada en otros protocolos desarrollados para redes que no son IP, por ende, su utilización puede requerir mayores recursos de hardware en los enrutadores, algo innecesario dado que las redes CLNP prácticamente están desapareciendo.

- La capacidad del enlace ATM con el proveedor C, podría verse comprometida durante los primeros meses del año 2009, únicamente si el ISP decide duplicar la capacidad de acceso al Internet del 50 % de los abonados en dicha troncal.

- El nivel de compartición del servicio de Internet de los clientes del ISP, siempre influye en la decisión de adquirir o no capacidad a los proveedores de conexión a Internet del ISP; produciéndose una relación inversamente proporcional que establece que a mayor nivel de compartición de clientes, menor capacidad de conexión a Internet del ISP requerida y a menor nivel de compartición de clientes, mayor capacidad de conexión a Internet del ISP.

- La decisión de implementar las distintas alternativas de diseño propuestas en el presente proyecto, depende directamente de la capacidad económica de ReadyNet Cia. Ltda., de cómo vaya manejando su mercado objetivo en el mundo de los servicios de valor agregado de Internet en el Ecuador, pero sobre todo de las decisiones de inversión y gestión, en base a ambiciones del mercado, del Directorio Ejecutivo del ISP.

- La cuarta solución de diseño físico para la red de borde, la tercera solución de diseño físico para la red de acceso y la tercera solución de diseño físico para la red de distribución presentan esquemas redundantes y de alta disponibilidad para cada uno de los módulos de la red del ISP; aún cuando involucran mayor inversión, también involucran mejor servicio.

- La selección de OSPF como IGP, y la implementación del punto anterior como esquema físico general, permite entregar una solución lógica que alcanza los objetivos del presente proyecto de titulación.

- La división de Áreas OSPF presentadas en el presente proyecto de titulación, permite manejar tablas de enrutamiento eficientes dentro del futuro Sistema Autónomo de ReadyNet Cia. Ltda.; y, aún cuando puede

presentar puntos críticos de falla por tener un solo ABR por Área, su reemplazo temporal por otro equipo puede ser rápido y factible.

- La separación de Áreas OSPF, permite conectar fácilmente un servidor, o equipos activos necesarios para brindar servicios como Telefonía IP, o en general cualquier servicio de streaming directamente en el Área 1 y manejar parámetros de calidad de servicio entre los clientes y los nuevos servicios por los sistemas operativos solicitados en los ABRs y ARs.

- La proyección a 5 años de bloques de direcciones IPv4 a utilizar por ReadyNet Cia. Ltda. no sirve para la justificación a LACNIC de un prefijo mayor a un /21, por políticas propias de dicho RIR. Ventajosamente, es necesario y suficiente para la demanda estimada en el presente proyecto.

## 5.2 RECOMENDACIONES

- El ISP debería pensar en la posibilidad de buscar financiamiento o inyectar capital que le permita soportar su propia infraestructura de últimas millas, ya que actualmente en el mercado de los servicios de valor agregado de Internet en el Ecuador, no existe competencia de precios con aquellos que si poseen su infraestructura y que constantemente la actualizan y mejoran.

- De la totalidad de factores que pueden influir en la decisión de registrar un SA, se encuentran la topología y el planeamiento a futuro. En ambos casos, la recomendación es tomar en cuenta definiciones y conceptos antes de tomar la decisión de registrar un SA, ya que los números son finitos, y en la historia, generalmente dicha decisión era tomada por ser parte del proceso de un operador para estar conectado a Internet.

- Todas las primeras soluciones físicas de los distintos sectores de la red del ISP deben ser aplicadas al menos hasta mediados del año 2009 para no comprometer los parámetros de SLA firmados en los contratos de los abonados.

- Solicitar al Departamento Comercial, un método de convertir a los abonados de acceso de marcado telefónico en usuarios banda ancha, de manera de mantener dicha troncal como valor agregado para los abonados del ISP como respaldo en el caso de que su enlace banda ancha deje de estar disponible por cualquier razón.

- Es necesario que el Departamento Técnico del ISP investigue un método eficiente de entregar direcciones IPv4 dinámicas y fijas a sus abonados, de manera que la solicitud y justificación ante LACNIC lleve a un resultado favorable en la asignación tanto del ASN como del prefijo /21 que inicialmente entrega el RIR.

- Especificar un método de autenticación dentro del IGP seleccionado, para evitar la inyección de rutas erradas dentro del Sistema Autónomo. El método recomendado es el tipo 2.

- Redistribuir servicios en cada equipo disponible luego de la migración para separar funciones en cada uno de los servidores es necesario para no comprometer la disponibilidad de más de un servicio en el caso de fallas de un único equipo. Es decir, servidores DNS que solo realicen esa función, servidores antivirus y antispam que solo realicen esa función, servidores POP /IMAP que únicamente brinden dicho servicio, etc.

- La revisión de la capacidad eléctrica generada por los nuevos equipos, junto con la ubicación física de los mismos y el cableado estructurado del cuarto de equipos es recomendada como parte del proceso de migración.

- Una eficiente administración técnica de los bloques de direcciones IPv4, verificando constantemente cualquier tipo de abuso de los clientes es recomendada, ya que problemas con el puerto 25, por ejemplo, pueden comprometer la reputación en Internet del Sistema Autónomo, y la penalización del enrutamiento de los prefijos anunciados.

# BIBLIOGRAFÍA

Libros Consultados:


1. HECKMAN, Oliver, "***The Competitive Internet Service Provider: Network Architecture, Interconnection, Traffic Engineering and Network Design***", Jhon Wiley & Sons, 2006, Primera Edición, Inglaterra.

2. HUSTON, Geoff, "***ISP Survival Guide. Strategies for Running a Competitive ISP****",* John Wiley & Sons, 1999, Primera Edición, EEUU.

3. BERKOWITZ, Howard, "***OSPF Goodies for ISPs***", NANOG 17, 1999, Montreal.


Tesis consultadas:


4. ROJAS, Franklin; VASQUEZ Carlos, "***Diseño de un Proveedor de Servicio de Internet (ISP) con Tecnología Frame Relay, Integrando el Servicio de Voz Sobre IP Y Análisis de Factibilidad Para su Posible Implementación***". Proyecto de Titulación EPN, Quito, 2008.

5. PROAÑO Hugo, "***Sistemas Autónomos para Proveedores de Servicio de Internet***", Proyecto de Titulación EPN, Quito, 2001.


Páginas Web consultadas:


6. BGP, "*The Border Gateway Protocol Advanced Internet Routing Resources*", http://www.bgp4.as/security

7. BGP, "*The Border Gateway Protocol Advanced Internet Routing Resources*", http://www.bgp4.as/links

8. BGP, "*The Border Gateway Protocol Advanced Internet Routing Resources*", http://www.bgp4.as/presentations

9. "*What Are OSPF Areas and Virtual Links?*", ID de Documento CISCO: 13703, December 2005, http://www.cisco.com/warp/public/104/8.html

10. http://www.uceprotect.net/en/index.php

11. http://www.oreillynet.com/pub/a/network/2002/08/12/multihoming.html.

12. http://www.conatel.gov.ec/site_conatel/index.php?option=com_docman&task=doc_download&gid=1808&Itemid=Estadisticas_SVA_31DIC08.pdf

13. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214018,00.html.

14. http://www.networkcomputing.com/1021/1021ws2.html?ls=NCJS_1021bt.

15. http://www.join.uni-muenster.de/Dokumente/drafts/draft-bhatia-manral-diff-isis-ospf-01.txt.

16. http://www.networksorcery.com/enp/protocol/is-is.htm

17. RFC 1058, "*Routing Information Protocol*", http://www.ietf.org/rfc/rfc1058.txt

18. RFC 2453, "*RIP Version 2*", http://www.ietf.org/rfc/rfc2453.txt

19. RFC 2080, "*RIPng for IPv6*", http://www.ietf.org/rfc/rfc2080.txt

20. RFC 2328, "*OSPF version 2*", http://www.ietf.org/rfc/rfc2328.txt

21. RFC 1195, "*Use of OSI IS-IS for Routing in TCP/IP and Dual Enviroments*", http://www.ietf.org/rfc/rfc1195.txt

22. RFC 1771, BGP4, http://www.ietf.org/rfc/rfc1771.txt.

23. RFC 1930, "*Guidelines for creation, selection, and registration of an Autonomous System* (AS)", http://www.ietf.org/rfc/rfc1930.txt.

24. http://www.lacnic.net/sp/registro/index.html

25. http://www.lacnic.net/sp/registro/table.html

26. http://lacnic.net/templates/asn-template-sp.txt

27. http://lacnic.net/templates/isp-v4-template-sp.txt

28. http://lacnic.net/sp/politicas/manual3.html#2.3.2.17

29. http://lacnic.net/sp/politicas/manual4.html

Otras fuentes consultadas:

30. SMITH Philip, "***Cisco ISP Essentials***", Cisco Press, 2002, ISBN: 1-58705-041-2.

31. IBM, "***Linux Network Administration I: TCP/IP Services***", Copyright IBM Corp., 2003.

32. Plan de Servicios Contratados por Clientes de ReadyNet Cia. Ltda., Departamento Comercial, 2008

33. Plan de Servicios a la Venta de ReadyNet Cia. Ltda., Departamento Comercial, 2008

34. Históricos de Instalación de Proveedores de Última Milla de ReadyNet Cia. Ltda., Departamento Técnico, 2008

35. Registros de Hardware y Software de Equipo Activo y Servidores de ReadyNet Cia. Ltda.

36. Herramienta de Generación de Tráfico basada en software libre para recoger datos del tráfico de equipos activos de ReadyNet Cia. Ltda., Departamento Técnico, 2008.

37. Plan de Direccionamiento IP de ReadyNet Cia. Ltda., Departamento Técnico, 2008.

38. Data Sheet, Cisco 2800 Series Integrated Services Routers.

39. Data Sheet, Cisco 3800 Series Integrated Services Routers.

40. Data Sheet, Cisco 7200 VXR Series Routers Overview.

41. Data Sheet, Cisco 7301 Router.

42. Data Sheet, Cisco 7500 Series Router.

43. Data Sheet, Cisco Catalyst 3560 Series Switches.

44. Data Sheet, Cisco Catalyst 3750 Series Switches.

# GLOSARIO

**AAA.** (*Authorization, Authentication, Accounting*) Autorización, Autenticación y Registro, conjunto de herramientas, procedimientos y protocolos que permiten autorizar, autenticar y registrar la actividad de entidades que tienen acceso a un sistema.

**ABR.** (*Area Border Router)* Router de Borde de Área o que pertenece a más de un área en OSPF.

**ACL.** (*Access List*) Lista de Acceso

**AES.** (*Advanced Encryption Standard*). Protocolo de Cifrado Avanzado.

**ARP.** (*Address Resolution Protocol*) Protocolo de Resolución de Direcciones.

**ASN.** (*Autonomous System Number*) Número de Sistema Autónomo.

**ATM.** (*Asynchronous Transfer Mode*) Tecnología de red de área extensa de modo de transferencia asincrónica.

**ATS.** (*Adaptive Traffic Shaping*) Conformador de Tráfico Adaptivo.

**BACKBONE.** Núcleo o columna vertebral de una red que tiene varios segmentos.

**BGP.** (*Border Gateway Protocol*) Protocolo de Enrutamiento de Salida de Borde.

**BIS.** (*Border Intermediate System*) Sistema Intermedio de Borde en el Modelo OSI.

**BROADCAST.** Difusión a todo el segmento de una red que maneja un algoritmo de acceso al medio de transmisión.

**CAS.** (*Channel Associated Signaling*) Señalización asociada por canal utilizada en PCM para el transporte de 30 canales de voz en un E1.

**CHAP.** (*Challenge Handshake Authentication Protocol*) Mecanismo de Autenticación de PPP

**CIDR.** (*Classless Inter Domain Routing*) Enrutamiento entre dominios sin clase.

**CLNP.** (*ConnectionLess Network Protocol*) Protocolo de Red Independiente de conexión en el Modelo OSI.

**COPS.** (*Common Open Policy Service*)Servicio de Políticas Abiertas y Comunes.

**CPP.** (*Combinet Packet Protocol*) Protocolo de Paquetes Combinet.

**DHCP.** (*Dynamic Host Configuration Protocol*)Protocolo de Configuración IP de Asignación Dinámica.

**DNS.** (*Domain Name System*) Servicio jerárquico de Resolución de Nombres de Internet.

**EBGP.** (*Exterior BGP*) Protocolo de salida de borde exterior, BGP exterior.

**EGP.** (*Exterior Gateway Protocol*) Protocolo de salida exterior, ej. BGP IDRP.

**EIGRP.** (*Enhanced Interior Gateway Routing Protocol*) Protocolo de Enrutamiento de Salida Interior Mejorado, IGP propietario de CISCO Systems.

**ES-IS.** (*End System to Intermediate System*) Protocolo de Sistema Final a Sistema Intermedio en el Modelo ISO/OSI.

**ES.** (*End System*) Terminología OSI de Sistema Final.

**GRE.** (*Generic Routing Encapsulation*) Encapsulación de Enrutamiento Genérica.

**GTS.** (*Generic Traffic Shaping*) Conformador genérico de tráfico.

**HTTP.** (*Hyper Text Transfer Protocol*) Protocolo de Transferencia de Híper Texto.

**IANA.** (*Internet Assigned Numbers Authority*) Autoridad de Asignación de Números de Internet.

**IBGP.** (*Internal BGP*)Protocolo de salida de borde interior, BGP interior.

**IDRP.** (*Inter Domain Routing Protocol*) Protocolo de Enrutamiento Inter Dominio.

**IEEE.** (*Institute of Electrical and Electronics Engineer*) Instituto de Ingenieros Eléctricos y Electrónicos, con sede en EEUU que desarrolla estándares, famoso por la familia 802.

**IETF.** (*Internet Engineering Task Force*)Fuerza de Tareas de Ingeniería del Internet. Organización sin fines de lucro, grupo de diseñadores de red, fabricantes de equipos, operadores de red, e investigadores que se encarga de la evolución y operación del Internet.

**IGP.** (*Interior Gateway Protocol*) Protocolo de Salida Interior, permite manejar el tráfico dentro de un Sistema Autónomo.

**IGRP.** (*Interior Gateway Routing Protocol*) Protocolo de enrutamiento de Salida Interior, un IGP estandarizado, pero creado por CISCO SYSTEMS.

**IMAP.** (*Internet Messages Access Protocol*) Protocolo de Acceso a Mensajes de Internet, acceso a un buzón de correo.

**IP.** (*Internet Protocol*) Protocolo Internet. Existen dos versiones, la 4 y la 6.

**IS.** (*Intermediate System*)Terminología OSI de Sistema Final.

**ISDN.** (*Integrated Service Digital Network*) Red Digital de Servicios Integrados.

**ISP.** (*Internet Service Provider*) Proveedor de Servicios de Internet.

**IS-IS.** (*Intermediate System to Intermediate System*) Protocolo de Sistema Intermedio a Sistema Intermedio en el Modelo OSI.

**LACNIC.** (*Latin American and Caribbean Network Information Centre*) Entidad que permite el registro de recursos de Internet para América Latina y el Caribe.

**LAN.** (*Local Area Network*) Red de Área Local, según clasificación de las redes por alcance de cobertura geográfica.

**LSA.** (*Link State Advertisement*) Publicación de Estado de Enlace en OSPF.

**MAC.** (*Media Access Control*) Control de Acceso al Medio de transmisión.

**MED.** (*Multi Exit Discriminator*) Discriminador de Múltiple Salida, atributo BGP utilizado para calcular el mejor camino de un paquete.

**MPLS.** (*Multi Protocol Label Switching*) Protocolo de Conmutación de Etiquetas para múltiples protocolos, ampliamente utilizado hoy en día.

**NAT.** (*Network Address Translation*) Traslación de direcciones IP de un interfaz a otro. Generalmente utilizado cuando detrás de un router existe un esquema de direccionamiento IP privado.

**NOC.** (*Network Operations Center*) Centro de Operaciones de la Red, lugar físico y lógico que permite la administración de uno o varios segmentos de red.

**NSAP.** (*Network Service Access Point*) Punto de Acceso al Servicio de Red, relativo al modelo OSI para la comunicación de capa 3 con capa 4.

**OSI.** (*Open System Interconnection*) Interconexión de Sistemas Abiertos.

**OSPF.** (*Open Shortest Path First*) Protocolo del Primer Camino más Corto Abierto. Es un IGP de estado de enlace robusto y escalable.

**PAP.** (*Password Authentication Protocol*) Mecanismo de Autenticación de PPP.

**PAT.** (*Port Address Traslation*) Traslación de direcciones de red basada en puertos.

**PBX.** (*Private Branch Exchange*) Intercambio de Red Secundaria Privada, permite la comunicación con varios sitios simultáneamente, utilizando la red telefónica pública.

**PCM.** (*Pulse Code Modulation*) Modulación de Pulsos Codificados, procedimiento para convertir una señal analógica en bits y transportarlos por la red telefónica pública.

**POP.** (*Post Office Protocol*) Protocolo de Oficina Postal, que permite revisar a un usuario, su buzón de correo electrónico.

**PPP.** (*Point to Point Protocol*) Protocolo Punto a Punto. Ampliamente utilizado para establecer canales físicos o lógicos de topología punto a punto.

**RAS.** (*Remote Access Server*) Servidor de Acceso Remoto, combinación de hardware y software necesario para habilitar acceso remoto a un segmento de red.

**RD.** (*Routing Domain*) Dominio de Enrutamiento.

**RDI.** (*Routing Domain Identifier*) Identificador de Dominio de Enrutamiento.

**RFC.** (*Request For Comments*) Solicitud de Comentarios, documento que describe las mejores prácticas en el mundo del Internet.

**RIB.** (*Routing Information Base*) Base de Datos de Información de Enrutamiento.

**RIP.** (*Routing Information Protocol*)Protocolo de Información de enrutamiento, primer protocolo IGP y EGP utilizado en los inicios de Internet.

**RIR.** (*Regional Internet Registries*) Registrantes Regionales de Internet. Delegados de IANA a entregar y distribuir los recursos de Internet en regiones del tamaño de continentes.

**RR.** (*Resource Registries*) Registros de Recursos, utilizados por el sistema jerárquico de resolución de nombres DNS para especificar nombres o direcciones IP dentro de las zonas de un dominio.

**RSVP.** (*Resource ReSerVation Protocol*) Protocolo de Reservación de Recursos de Hardware en equipos activos.

**SA.** Sistema Autónomo**.**

**SCP.** (*Secure Shell Copy*) Protocolo de Copias Seguras entre equipos que se basa en SSH para la transferencia de archivos.

**SLA.** (*Service Level Agreement*) Acuerdo de Nivel de Servicio, parámetros ofrecidos, aceptados o requeridos por un abonado sobre un estado de una conexión, sea dicha conexión pública o privada.

**SMTP.** (*Simple Mail Transfer Protocol*)Protocolo de Transferencia de Correos Simple, permite el tránsito del correo electrónico en el Internet.

**SNMP.** (*Simple Network Management Protocol*)Protocolo de Administración de Red Simple, permite obtener información de equipos activos dentro de una red.

**SNPA.** (*Sub Network Point of Attachment*) Punto de acceso físico a la subred de comunicaciones en el Modelo OSI.

**SPF.** (*Shortest Path First*) Algoritmo del Primer Camino más Corto (DIJKSTRA)**.**

**SSH.** (*Secure Shell*) Protocolo que permite tener una línea de comandos con un equipo activo, cifrado o seguro.

**STP.** (*Spanning Tree Protocol*) Protocolo de conmutación de paquetes Spanning Tree, ampliamente utilizado en equipos activos de capa 2.

**TACACS+.** (*Terminal Access Controller Access Control System*) Sistema de Control de Acceso al Controlador de Acceso Terminal en la versión +.

**TCP.** (*Transfer Control Protocol*) Protocolo de Control de Transmisión, uno de los principales protocolos de Internet.

**TLD.** (*Top Level Domain*) Dominio de Alto Nivel, identificador utilizado en el sistema jerárquico de resolución de nombres DNS que se encuentra bajo el dominio raíz o punto (.) y que define el tipo de organización que usa un dominio.

**UDP.** (*User Datagram Protocol*) Protocolo de Datagrama de Usuario, otro de los principales protocolos de Internet.

**VLAN.** (*Virtual LAN*) Redes manejadas bajo el estándar IEEE 208.1q y permite tener varias redes separadas tanto el dominio de colisión como el dominio de difusión bajo el mismo equipo de interconexión.

**VLSM.** (*Variable Length Subnet Mask*) Máscaras de Subred de Longitud Variable.

**VPDN.** (*Virtual Private Dial In Network*). Tecnología de Red Utilizada en enrutadores CISCO para distintos accesos cifrados a través de un marcado previo.

**VPN.** (*Virtual Private Network*) Red Privada Virtual.

**VRF.** (*Virtual Routing and Forwarding*) Tecnología de enrutamiento y reenvío de VPNs utilizada en redes distintas que comparten un mismo equipo.

**WHOIS.** Aplicación basada en TCP/IP que permite identificar al registrante de recursos de Internet.

# ANEXOS