ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

DISEÑO DEL SISTEMA DE MEJORAMIENTO DE SEGURIDAD Y ADMINISTRACIÓN DE TRÁFICO PARA EL ISP (INTERNET SERVICE PROVIDER) “READYNET”

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

MERY ELIZABETH GONZÁLEZ TELLO

DIRECTOR: MSC. ALEX RODRÍGUEZ T.
CODIRECTOR: ING. FLAVIO CEPEDA

QUITO, MAYO 2006

DECLARACIÓN

Yo, Mery Elízabeth González Tello, declaro 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.

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

_____

Mery Elízabeth González Tello

CONTENIDO

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

RESUMEN

El presente proyecto de titulación tiene como objetivo primordial presentar una solución en dos áreas del ISP “READYNET”, las cuales son: el sistema de mejoramiento de seguridad, mediante el establecimiento de políticas y procedimientos de seguridad e introducción de tecnologías que permitan cumplir con un esquema riguroso, y el manejo de tráfico de usuarios en base a un sistema de administración de ancho de banda que permite establecer políticas de control a nivel de aplicación.

Se ha realizado este proyecto en cinco capítulos que van de la siguiente manera: el primer capítulo presenta una introducción a la seguridad en redes de forma general, para luego particularizar el caso en la red de un proveedor de servicios de Internet; además, contiene un estudio de la calidad de servicio en Internet desde el punto de vista de funcionalidad de la red y la percepción de usuario.

El segundo capítulo recopila información de la situación actual del ISP, en infraestructura, acceso al *backbone* principal de Internet, tipos de usuarios, los mecanismos implementados en el ámbito de seguridad y administración de tráfico.

El diseño propuesto, se detalla en el capítulo tres, y está enfocado a proponer políticas y procedimientos de seguridad, para posteriormente proponer un esquema de red con implantación de tecnologías que ofrezca seguridad en profundidad. Además, se presentan las ventajas de trabajar bajo el esquema de un sistema de administración de ancho de banda con políticas de control de tráfico, y por último se consideran acuerdos de niveles de servicio que deberían ser incorporados en la promoción de productos.

En el capítulo cuatro se analizan viabilidades técnicas y económicas del proyecto y un estudio de tarifas en el Ecuador. Para finalizar, se presentan conclusiones y recomendaciones que el ISP deberá considerar para la implantación del diseño propuesto en este proyecto.

PRESENTACIÓN

El servicio de acceso a Internet, desde el punto de vista del usuario, es una herramienta para acceder a una gama de servicios, como correo electrónico, navegación *Web*, videoconferencia, etc. Sin embargo estos servicios pueden servir de soporte a otros servicios como son: educación en línea, recreación, negocios electrónicos; en definitiva, una red multiservicio.

Esto lleva a ver la seguridad en redes como algo primordial dentro de una empresa, y con mayor razón en el ambiente de un proveedor de servicios. En base a lo expuesto en este proyecto, el diseño de mejoras al sistema de seguridad ya establecido en la red del ISP es de vital importancia, principalmente por que se enfoca a proteger las plataformas de servicio que están directamente involucradas con el usuario.

Además, extiende la seguridad a dos frentes como son: brindar una de las primeras líneas de defensa perimetral a la red del usuario, y proteger además al Internet de los usuarios del ISP.

El esquema de administración de ancho de banda propuesto en este proyecto permite asignar recursos en base a políticas de control de tráfico; además se enfoca en ofrecer un producto más competitivo en base a canales compartidos y control de aplicaciones que utilizan gran cantidad de ancho de banda, sin afectar la rentabilidad de negocio desde el punto de vista del ISP.

Dado que se pretende ofertar calidad en el servicio ofrecido, garantizando ancho de banda para aplicaciones críticas, el ISP podrá competir en el mercado por la variedad de productos que podrá ofertar.

La información que se presenta aquí, ayudará al lector a comprender de mejor manera el ambiente de un ISP que manejaría como pilares la seguridad en su red y la administración de tráfico, principalmente a nivel de aplicación.

CAPÍTULO 1

INTRODUCCIÓN

1.1 GENERALIDADES SOBRE SEGURIDAD DE REDES [1]

1.1.1 OBJETIVO E IMPORTANCIA DE LA SEGURIDAD DE REDES

La seguridad en redes tiene como objetivo controlar el acceso al conjunto de elementos que conforman la red, y a la vez, a los servicios que estos ofrecen.

La seguridad de la red, es de vital importancia, ya que las organizaciones deben estar concientes de lo que pueden lograr con la implementación. Algunas de las razones por las que la seguridad en redes y computadores es importante, son: proteger los recursos de la organización, ganar una ventaja competitiva, cumplir con requerimientos y responsabilidades en el ámbito de regulación de la organización.

La tendencia actual es convertir a las redes públicas principalmente la Internet en redes multiservicio, se ha generado un notable incremento de la confianza en las redes públicas para manejar información personal, financiera y otra información restringida, esto agrava el problema de la seguridad pues el protocolo de Internet no fue diseñado para ser seguro en sí mismo, no existen estándares de seguridad aprobados incorporados en las comunicaciones TCP/IP, dejándolas abiertas a potenciales usuarios maliciosos y procesos en la red.

Los desarrollos modernos han hecho de las comunicaciones en Internet más seguras, pero todavía hay muchos incidentes que capturan la atención y alertan al usuario del hecho de que nada es completamente seguro, por ende la seguridad en redes más que nunca debe ser considerada como prioridad para una organización.

1.1.2 BASES DE LA SEGURIDAD EN REDES

Las bases fundamentales de la seguridad en redes son: prevención, detección y respuesta.

La prevención se enfoca en varias estrategias y herramientas para advertir la ocurrencia de una brecha de seguridad en la red, comprendiendo todos sus estamentos.

La detección permite saber que componentes de la red está siendo atacado, y la forma en que se produce el ataque.

Una vez producido el ataque, es necesaria una respuesta al mismo, para asegurar la integridad de la red, y, de ser posible, identificar al responsable.

1.1.3 INFRAESTRUCTURA DE SEGURIDAD [2]

1.1.3.1 Políticas de seguridad, estándares y directrices

La política de seguridad, define las reglas que todos los participantes deberían observar. La política, entonces, debe estar respaldada por estándares y directrices, los cuales determinan para todos los estamentos las maneras en la que se podrá acceder o distribuir los recursos y medios de información. Las mejores prácticas incluyen algunos aspectos, entre otros la seguridad física, seguridad de la red, seguridad a niveles de aplicación y el acceso desde o hacia redes externas.

1.1.3.2 Responsabilidades y roles organizacionales

Cada entidad en la red juega un rol importante en el establecimiento y mantenimiento de la seguridad, por lo tanto, se deben asignar responsabilidades, que de no ser cumplidas, acarrearán problemas en los estamentos base de la seguridad de la red.

1.1.3.3 Objetivos básicos de seguridad para la infraestructura de red.

1.1.3.3.1 Seguridad de servidores

Los servidores constituyen el corazón de la red, por lo tanto el objetivo de seguridad incluye el sistema operativo, la estructura de archivos, las cuentas de administración, cuentas de usuario y procesos del servidor.

1.1.3.3.2 Seguridad en la red

Este objetivo comprende lo siguiente: dispositivos de red**,** (enrutadores*, switchs*, etc), lo que deviene en los siguientes procesos: configuración y convenios de seguridad, etc. Por ejemplo los enrutadores pueden tener mecanismos de acceso como RADIUS (*Remote Authentication and Dial-In User Service*) o TACACS (*Terminal Access Controller Access Control System*), los cuales van a rastrear formas y tiempos de acceso a la red.

1.1.3.3.3 Seguridad a nivel de aplicación

En este nivel existen varios tipos de aplicaciones, como por ejemplo.

- Aplicaciones *Web*: es necesario seguir estándares base, como el uso de CGIs (*Common Gateway Interface*), que pueden ayudar a evitar vulnerabilidades de algunos programas en servidores *Web*.

- Respaldo de Datos: es crucial, y los mismo pueden estar en: servidores de aplicación, servidores de bases de datos, o en unidades de red. Se debe considerar la frecuencia y niveles de respaldo.

- Configuración del sistema: se tomará en cuenta los frecuentes cambios que existen en los sistemas, dispositivos de red, y aplicaciones, para actualizar las versiones de *software*, y configuraciones de las mismas.

1.1.3.4 Administración de Riesgos

Este objetivo incluye valoración, cuantificación y prevención de riesgos. La valoración de riesgos deberá considerar las fuentes de amenaza, forma de acceso a la información y los costos de proteger la red de esta potencial amenaza.

1.1.3.5 Respuesta ante Incidentes

Se define incidente como “un evento adverso en un sistema de información y/o una red, o la amenaza de la ocurrencia de semejante evento”[1], un incidente abarca eventos como: ataques con código malicioso, accesos no autorizados o imprevistos, utilización de servicios no autorizados, ruptura del servicio, uso inapropiado, espionaje o engaño. La organización deberá planificar respuestas y coordinarlas, para no originar pérdida de datos o ruptura del servicio, cuando se trate de identificar la fuente del incidente.

Se tienen dos tipos de respuestas, las cuales dependerán del tipo de sistema o servicio afectado, primero reprimir inmediatamente el evento y posterior a esto seguir al perpetrador aceptando los riesgos de los sistemas o redes.

Los aspectos a considerarse en el plan de respuesta a incidentes son: objetivos y metas del plan, procesos para identificar el incidente y alcance del mismo, procesos para notificación, directivas para el manejo del incidente, documentación y análisis del incidente, y procesos para manejar preguntas por parte de clientes y medios de comunicación si se diera el caso.

1.1.3.6 Entrenamiento al Usuario

Es extremadamente importante que cada usuario conozca el rol y las responsabilidades que tiene ante la implementación de seguridad. Esto se logra a través de una adecuada capacitación.

---

[1] Definición dada por FCIRT (*The Federal Computer Incident Response Team*).

1.1.3.7 Monitoreo continuo y mecanismos de retroacción

Cada día las organizaciones están expuestas a nuevas amenazas, por lo que es necesario tener procesos continuos de aseguramiento, (ver figura 1-1). Estos procesos pueden ser: implementar nuevas herramientas, instalar parches o actualizaciones y programas de entrenamiento regular, aplicación de nuevas políticas, entre otras.

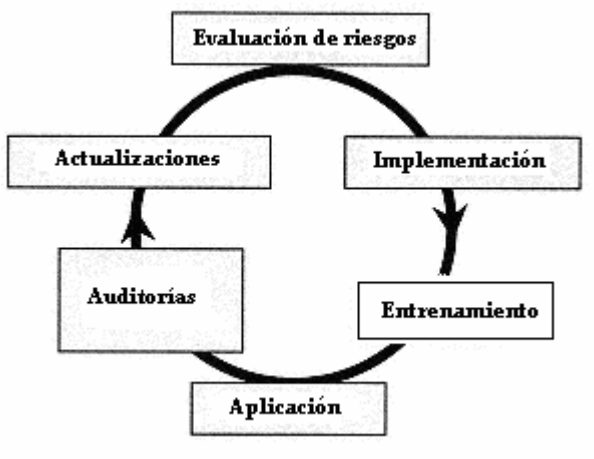


Figura 1- 1: Proceso continúo de administración de riesgos [1].

1.1.4 PRINCIPIOS IMPORTANTES DE LA SEGURIDAD EN REDES [1] [2]

La seguridad en redes gira en torno a los siguientes principios fundamentales que son: confidencialidad, integridad, disponibilidad y autenticación.

1.1.4.1 Confidencialidad

Está relacionada con la prevención de divulgaciones no autorizadas de información. Las publicaciones pueden ser intencionales, esto por ejemplo se da cuando se rompe un código que esta cifrando la información y se logra leer el contenido, también son no intencionales cuando debido a la incompetencia o descuido al manejar la información se accede a la misma.

1.1.4.2 Integridad

Se entiende como la veracidad de la información, datos, o transmisiones. Estos pueden ser alterados accidentalmente, sin autorización, o sin control. Las principales metas de la integridad son: prevenir la modificación de la información por usuarios no autorizados, o la modificación de la información no autorizada o no intencional de usuarios autorizados, y preservar la consistencia interna y externa de la información.

1.1.4.3 Disponibilidad

Garantiza que usuarios autorizados al sistema pueden acceder a la información en dicho sistema y en la red, a tiempo y sin interrupciones, y que; si llegara a ocurrir una interrupción al sistema, éste se recupere de forma rápida y completa.

1.1.4.4 Autenticación

La autenticación afirma la identidad de un usuario, es importante tanto si se trabaja sobre la red o se accede hacia una red.

Cuando se está trabajando sobre la red se plantean dos preguntas [3]: ¿Con quién me estoy comunicando? Y ¿Por qué pienso que la persona o entidad es quien dice ser? Si no se tiene una buena respuesta a la segunda pregunta, hay la posibilidad de que se haya errado en la primera.

Cuando se accede hacia una red se manejan tres esquemas:

- *Algo que se conoce*: se usan claves, códigos o secuencias, la idea es que si se conoce la clave o código, la identidad es quien dice ser, y por ende se le otorga acceso a la red. Es el más utilizado, pero no es seguro ya que es fácil de engañar.

- *Algo que se tiene*: se requiere una llave, distintivo, o tarjeta de identificación, es decir algún dispositivo que provea acceso. La idea de éste esquema es que sólo las personas autorizadas deberán tener este distintivo, el inconveniente se presenta cuando el mismo se pierde o es sustraído.

- *Algo que se es*: este esquema se basa en características físicas, se usa por ejemplo: análisis del iris, huellas dactilares, muestras de voz, etc. Es más seguro y difícil de engañar.

1.1.5 SEGURIDAD DE LA INFORMACIÓN [3]

Es el resultado de garantizar: confidencialidad, integridad, disponibilidad y autenticación.

1.1.5.1 Confidencialidad de la información

La seguridad de la información se relaciona con la confidencialidad, porque garantiza que usuarios no autorizados queden impedidos de interceptar, copiar o replicar la información. Para esto se usa técnicas de encripción, obteniendo como resultado privacidad de los datos al ser transmitidos. Las técnicas de encripción son: encripción de clave secreta, se usa la misma llave para encriptar y desencriptar datos; y encripción de clave pública, se usan diferentes claves, para encriptar (públicas) y desencriptar (privada) datos.

1.1.5.2 Integridad de la información

La integridad es necesaria para garantizar que existe la suficiente veracidad de la información, es decir, que la información no sea alterada o modificada. Se tiene dos maneras para establecer integridad de los datos:

- Criptografía *checksum*: se usa para detectar algún cambio de los datos cuando son transmitidos.

- Funciones *hashing*: el texto plano genera un valor *hash* este valor será único.

1.1.5.3 Disponibilidad de la información

La disponibilidad de la información es importante, porque los usuarios deberán acceder a los datos cuando ellos lo estimen necesario.

1.1.5.4 Autenticación de la información

La autenticación determinará si el usuario tendrá acceso a la información. Existen varios esquemas de autenticación que proveen diferentes niveles de seguridad.

Otros aspectos a considerar en la seguridad de la información son:

- Adecuada seguridad física
- Contratar el personal apropiado
- Establecimientos de políticas y procedimientos de protección ante incidentes, accidentes, incompetencia y desastres naturales
- Monitoreo de la red
- Desarrollo de aplicaciones seguras

Se debe recordar que la mayoría de ataques a la seguridad en una organización son internos, por lo que las políticas internas serán de vital importancia. Las políticas y procedimientos de protección abarcarán lo siguiente:

- Respaldos, control en las configuraciones, control en los medios de almacenamiento de la información
- Recuperación ante desastres y planes de contingencia
- Integridad en los datos

La seguridad no es absoluta, por lo que siempre se podrá mejorar. Como organización, se debe hacer un análisis costo – beneficio, que abarca costos de seguridad y a veces el costo de lo asegurado.

1.1.6 MODELOS DE SEGURIDAD [3]

1.1.6.1 Seguridad por oscuridad

El concepto detrás de este modelo es que si no se conoce de la existencia de una red o un sistema, entonces no es susceptible de ser atacado. El problema de este esquema es que una vez descubierta la red, será completamente vulnerable.

1.1.6.2 Perímetro de defensa

Se basa en protegerse de ataques externos, para lo cual se simula una especie de cerco. Se utiliza por ejemplo enrutadores de borde, o se aísla la red por medio de un *firewall*. El problema de este modelo es que supone ataques internos nulos, por ende no protege los sistemas en contra de ataques dentro de la organización.

1.1.6.3 Defensa en profundidad

Es un modelo más robusto. No depende de un solo mecanismo, cada sistema es una isla que se defiende a sí misma. La seguridad interna no se ve comprometida si se cometen errores en otros sistemas.

1.1.7 ATAQUES COMUNES [1]

Los ataques en contra de recursos de red son comunes en el mundo actual dependiente de la Internet. Están comprometidos directamente con la confidencialidad, integridad, y disponibilidad de las redes y sus recursos. Se tienen las siguientes categorías:

- Modificación: Alteración de la información no autorizada.

- Repudio: Negar que un evento o transacción ocurra.
- Negación de servicio: acciones que dejan recursos y servicios de la red no disponibles cuando estos son requeridos.
- Acceso: accesos no autorizados a recursos o información de la red.

1.1.7.1 Ataques de negación de servicio

Este tipo de ataque acapara los recursos del sistema de manera que no pueda responder al servicio requerido. En este caso, se pueden inundar con peticiones al servidor las cuales no son completadas, o se envían una gran cantidad de archivos que el disco duro del sistema queda exhausto. Los siguientes son ejemplos de ataques de negación de servicios.

- Desbordamiento de *buffer*[1]: un proceso recibe más datos de los esperados.

- Ataque SYN: se inunda con peticiones que luego no son contestadas cuando el sistema responde a estas peticiones, pues simplemente el que generó las peticiones las hizo para que el servidor se mantenga ocupado.

- *Smurf*: este ataque usa engaños IP e ICMP para saturar una tarjeta de red con tráfico. Falsifica un paquete ICMP ECHO_REQUEST a la dirección de *broadcast* con lo que todas las máquinas responden a esta dirección falsificada, y por saturación la dejan fuera.

1.1.7.2 *Backdoor*

En este tipo de ataque se usan *módems dial-up* o conexiones externas asincrónicas, lo cual permite tener acceso evitando mecanismos de control. Esto por ejemplo sucede cuando usuarios de la red se conectan a la misma mediante *módems*, los cuales usualmente acceden a la red sin pasar por sistemas de *firewall*.

[1] Como ejemplo esta el "*Ping* de la muerte", el cual es un intento de saturar un servidor por ejemplo con una cantidad casi infinita de ping hacia el mismo.

1.1.7.3 *Spoofing*

El *spoofing* se basa en engañar al sistema para convencerlo que está tratando con alguien conocido, una de las formas de ejecutarlo es enviando paquetes con una dirección IP conocida, de tal forma que el sistema reconoce que está dentro del rango permitido, y deja pasar el paquete.

Otro ejemplo tiene que ver con la manipulación del DNS al lograr cambiar la forma de transformar el URL en una IP, diferente que redirecciona al usuario directamente al *hacker*.

1.1.7.4 *Man-in-the-middle*

El atacante hace un intercambio de claves de tal forma que el receptor ahora tenga la clave del atacante y viceversa; entonces, cuando alguien envía un mensaje encriptado para el receptor, ignoran que en realidad está usando la clave del atacante, por lo que este puede leer el mensaje, incluso modificarlo, y luego enviarlo al verdadero receptor.

1.1.7.5 *Replay*

Esto ocurre cuando un atacante intercepta y guarda mensajes viejos, posteriormente los envía esperando algún tiempo, actuando como si fuera uno de las entidades que se estaban comunicando.

1.1.7.6 *TCP/Hijacking*

Un atacante secuestra una sesión entre un cliente verdadero y un servidor de red, el atacante sustituye su dirección IP por la del cliente verdadero, y continúa el diálogo con el servidor, el cual piensa que sigue comunicándose con el cliente.

1.1.7.7 Ataques por fragmentación

Este ataque busca burlar las seguridades de un *firewall* de filtrado de paquetes, al fragmentar el paquete de tal forma que el primer paquete contenga todos los datos de la cabecera, el resto de fragmentos no serán filtrados por el *firewall* y por ende pasarán.

1.1.7.8 Claves débiles

Algunos algoritmos criptográficos tienen claves más débiles que otras, es decir no son seguras, por ende no deberían ser usadas, ya que pueden ser descubiertas fácilmente. Un ejemplo es el algoritmo DES que de 2^{56} posibles claves, 16 son no seguras.

1.1.7.9 Ataques matemáticos

Se usan las matemáticas para romper claves o algoritmos criptográficos.

1.1.7.10 Ingeniería Social

Se usan técnicas sociales tales como hacer llamadas fingiendo ser usuarios del sistema para obtener información de claves, números de PIN, entre otros datos para ser usados en accesos a sistemas de información.

1.1.7.11 Escaneo de puertos

Usualmente es un tipo de *software* que se usa para determinar que *hosts* están activos, para posteriormente obtener información de puertos abiertos[1] y atacar los mismos.

[1] Es aquel que permite comunicarse con otro equipo que este solicitando comunicación.

1.1.7.12 *Dumpster diving*

Se refiere a la adquisición de información que fue descartada por un individuo u organización. En muchos casos, se bota a la papelera información de claves de acceso, números telefónicos, esquemas de la organización, que otras personas pueden recogerlos y hacer uso de los mismos.

1.1.7.13 *Password guessing*

Las claves son los mecanismos más usados para autentificar usuarios en un sistema de información. El error común de los usuarios es apuntar las claves en lugares visibles, donde pueden ser accedidos por posibles atacantes, otra opción es que las claves viajan sin encripción por la red y con *sniffers* pueden ser interceptadas. En este ataque se usa la fuerza bruta, y ataque por diccionario[1].

1.1.7.14 Explotación de *software*

Las vulnerabilidades propias del *software* (comúnmente sistema operativo) son usadas para generar accesos no autorizados a los recursos y datos del sistema.

1.1.7.15 Uso de sistemas no apropiados

Esta actividad relaciona al uso de recursos y computadoras comerciales para asuntos no comerciales o personales, éste es un ataque contra los recursos de una organización usándolos para propósitos desautorizados.

1.1.7.16 *Eavesdropping*

Ocurre a través de la intercepción de tráfico de la red, esto se da especialmente cuando en la red se incorpora componentes inalámbricos y dispositivos de acceso remoto.

[1] Se usa un diccionario común de claves incluso con el mismo tipo de encripción para tratar de acceder al sistema.

1.1.7.17 *War driving*

Mediante recursos de accesos inalámbricos, se pone el adaptador en modo promiscuo[1], y con la ayuda de *software* localizar nodos de la red.

1.1.7.18 Ataques a números de secuencia TCP

El atacante hace que el objeto a ser atacado piense que está conectado a un *host* verdadero, y secuestra la sesión. Esta sesión es usada para posteriores ataques a otros *hosts*.

1.1.7.19 *War dialing*

Mediante llamadas consecutivas a números telefónicos, el *hacker* busca *módems* conectados para obtener acceso a un sistema.

1.1.8 MECANISMOS DE SEGURIDAD PARA EL MODELO TCP/IP [12]

Se analizarán mecanismos de seguridad para las diferentes capas del modelo TCP/IP y las correspondientes tecnologías.

1.1.8.1 Capa de Acceso a la Red

Corresponde a capa física y capa enlace en el modelo ISO/OSI, si se habla de encripción a nivel de capa física podría resultar en degradación de la calidad de servicio, tomando en cuenta que no todos los datos son confidenciales.

En la capa enlace se presentan protocolos como, ATM (*Asynchronous Transfer Mode*), PPP (*Point-to-Point Protocol*), L2TP (*Layer Two Tunneling Protocol*), por mencionar algunos.

[1] Modo en el que se pone el adaptador para que en una red compartida capture todos los paquetes, incluyendo los paquetes destinados a otras computadoras.

1.1.8.1.1 Servicios de seguridad ATM (Asynchronous Transfer Mode – Modo de transferencia Asincrónico)

En ATM se encuentran diferenciados los servicios de seguridad para la transferencia de datos entre usuarios, el intercambio de señales de control y datos de administración[1], teniendo una gran gama de servicios para los primeros y servicios limitados para los segundos.

Los servicios de seguridad son provistos y negociados por un agente de seguridad (SA – *Security Agent*).

Para el plano de usuario se tienen los siguientes servicios:

- Autenticación de entidades y negociación de atributos de seguridad: se ejecuta durante el establecimiento de la conexión, una conexión segura establecida entre dos SAs, se denomina asociación de seguridad. Se definen dos protocolos: *handshake* de dos vías, y *handshake* de tres vías[2], que proveen autenticación unilateral o recíproca, el protocolo de tres vías además provee intercambio de certificados y negociación de servicios de seguridad.

- Intercambio de llaves: usualmente se usa el protocolo de intercambio de llaves *Diffie-Helmann*.

- Confidencialidad de datos: se aplica en la capa ATM, protege el *payload* de una celda ATM, encriptándolo.

- Integridad y autenticación de datos origen: se aplica en la capa AAL, y los parámetros para garantizar integridad se determinan al momento de establecer la conexión.

[1] ***User plane***.- transfiere datos de usuario junto con alguna información de control (control de flujo y errores).
Control plane.- transmiten mensajes que tratan funciones de control de llamadas, control de conexiones.
Management plane.- funciones de coordinación y administración.
[2] Estándares ISO/IEC (9594-8 y 11770-2), tratan en el objetivo de administración de claves y los mecanismos que se usan.

- Control de acceso: se ejecuta por canal virtual base, y se decide si se acepta o rechaza una petición de conexión en base a niveles de control de acceso, los cuales definen los atributos de seguridad del recurso protegido.

Se puede formar incluso una VPN sobre ATM usando las características propias de la tecnología como son las interfaces UNI (*User-Network Interface*) y NNI (*Network-Network Interface*). La figura 1-2 muestra como un agente de seguridad ATM puede proveer servicios de seguridad para uno o más sistemas finales o redes que estén detrás de una interfaz NNI.

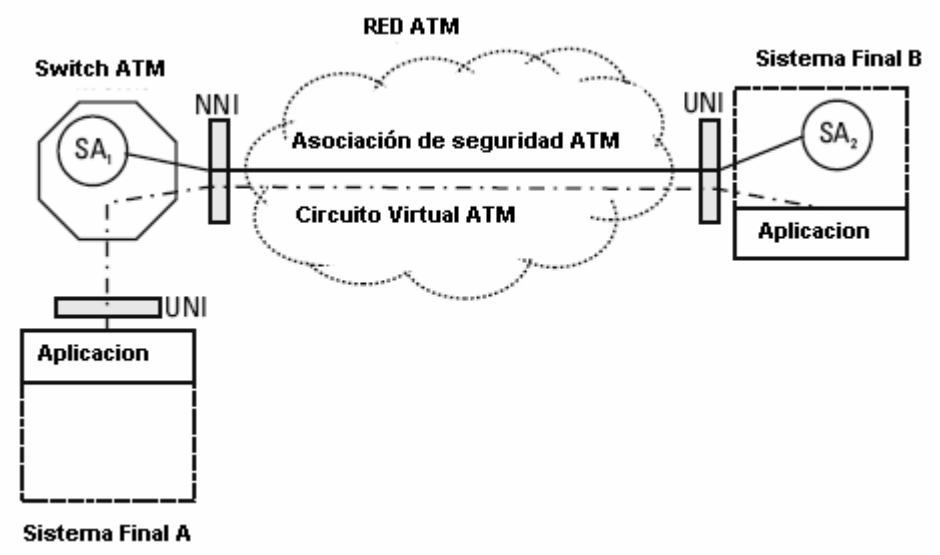


Figura 1- 2: Red Privada Virtual ATM [2]

1.1.8.1.2 Seguridad en el Protocolo PPP (Point-to-Point)

Este protocolo va a permitir transmitir datagramas multiprotocolo sobre un enlace serial, cumpliendo con las siguientes fases: *link dead*, establecimiento del enlace, autenticación, protocolo de capa red y finalización del enlace.

La autenticación provista por PPP aplica únicamente al establecimiento de la conexión, posterior a esto la información viaja sin protección. Y se utiliza los siguientes protocolos para autenticar:

PAP (*Password Authentication Protocol*): es un protocolo de autenticación débil porque las claves son enviadas sin protección. Usa una identidad para el usuario (ID) de usuario y una clave. Tampoco provee protección de tramas enviadas luego de la fase de autenticación.

CHAP (*Challenge-Handshake Authentication Protocol*): el cliente y el servidor comparten una clave secreta tal como en encripción simétrica. Cuando se inicia la sesión PPP, el servidor envía un requerimiento al cliente con tres parámetros: nombre del servidor, una identificación y un número aleatorio; en el siguiente paso el cliente calcula un valor *hash* usando MD5 (usa ID del servidor, número aleatorio y clave privada) y envía este valor acompañado de ID del usuario y ID del servidor, finalmente el servidor hace el cálculo del valor *hash,* y sí coincide se logra la autenticación. Tampoco ofrece protección de tramas enviadas luego del proceso de autenticación.

EAP (*Extensible Authentication Protocol*): en este protocolo, dentro de los campos que contiene el paquete, está el campo **TYPE,** en el cual se especifica el mecanismo de autenticación que se usará. Se tiene los siguientes valores:

- *Type* = 3 Usa MD5 similar a CHAP
- *Type* = 4 *One-Time password*[1]
- *Type* = 5 *Token card* genérico
- *Type* = no conocido, para EAP-TLS[2]

ECP (*Encryption Control Protocol*): provee confidencialidad de datos enviados en un datagrama *PPP*, no inicia sino hasta después de la fase de autenticación. Antes de ser trasmitidos los datos, se negocia el algoritmo de encripción y sus parámetros.

[1] *One time password*.- se utiliza una "semilla" aleatoria y un número de secuencia del *password*. El cliente generador de OTP ingresa el valor aleatorio y la "passphrase" en una función hash.
[2] Este mecanismo se explica en el *RFC* 2716.

1.1.8.1.3 L2TP (Layer Two Tunneling Protocol)

Este protocolo transporta en un túnel el tráfico PPP sobre una variedad de redes (IP, ATM), opera a nivel de capa 2, por lo que corresponde a una implementación de tipo nodo a nodo, estos nodos deben ser compatibles. Se forma un túnel hasta el servidor L2TP desde la red del cliente o ISP. Soporta autenticación como es CHAP, PAP o MS-CHAP.

1.1.8.2 Capa Internet

Los principales mecanismos de seguridad para la capa Internet son: sistemas de *firewall* basados en filtros de paquetes, IPSec, detección de intrusos.

1.1.8.2.1 Filtros de paquetes

Los filtros de paquetes permiten o bloquean el paso de paquetes, usualmente en la etapa de enrutamiento. Los primeros *firewalls* fueron enrutadores con la capacidad de filtrar tráfico en base a un campo en la cabecera IP. El filtrado se puede hacer en enrutadores, *bridges*, o a nivel de *host*.

- *Filtros basados en la dirección IP*: éstos operan con direcciones IP fuente y destino, trabajan a nivel de direcciones de red y subred, se pueden crear reglas de filtrado con la capacidad de permitir o negar acceso. Se debe considerar que cuando un paquete llega busca la primera regla que cumpla y la ejecuta, las demás posteriores no las considera. Es necesario que bajo éste esquema se trabaje con una herramienta que revise consistencia de las reglas de filtrado.

- *Filtros basados en dirección IP y números de puerto*: aunque difícil pero no imposible, se puede permitir o negar accesos a servicios como FTP o TELNET. Es necesario conocer las direcciones IP y los servicios a los que podrán acceder para crear las reglas de filtrado.

Las desventajas del filtrado de paquetes es que reduce el desempeño del enrutador, hay problemas con la fragmentación IP[1], problemas con FTP, problemas con TCP[2]

1.1.8.2.2 Seguridad IP (IPSec)

Es un conjunto de protocolos para soportar intercambio seguro de paquetes a nivel de capa IP.

Los modos soportados son: IPSec en modo transparente, donde se solo encripta los datos, e IPSec en modo túnel, donde se encripta el paquete completo. Las partes fundamentales de este esquema son:

- Protocolos de seguridad:

  - *Authentication Header (AH).-* provee autenticación del origen de los paquetes y chequea integridad (soporta MD5 o SHA).

  - *Encapsulation Security Payload (ESP).-* provee confidencialidad al tráfico de datos, se encripta el paquete original incluyendo la cabecera (soporta DES, 3DES o cualquier esquema de encripción simétrica). Provee protección parcial contra análisis de tráfico (solo en modo túnel).

Es posible usar los dos en conjunto para establecer una conexión segura, por ejemplo en una VPN, se usa AH entre un *host* y un *gateway* de seguridad, mientras que ESP se lo usa entre *gateways* de seguridad[3].

- Manejo de claves:

Soportan diferentes sistemas de administración de claves como *Kerberos*, el protocolo por defecto es IKE (*Internet Key Exchange*), la principal función de IKE

[1] Solo el primer fragmento es revisado ya que ahí se encuentra el número de puerto y la bandera *TCP ACK*.
[2] Ataque TCP SYN Flooding, y predicción del número de secuencia TCP.
[3] Un *gateway* de seguridad es aquel que se encuentra en la parte perimetral de la red.

es el establecimiento y mantenimiento de asociaciones de seguridad, combina las características de ISAKMP y OAKLEY[1]. Entre los principales cometidos están:

- Servicio de seguridad de parámetros para la asociación de seguridad.
- Autenticación primaria para el inicio de comunicación entre las entidades participantes.
- Método para generar claves para los servicios de autenticación y encripción.
- Manejo de claves.

❖ Asociaciones de seguridad:

Son conexiones de red unidireccionales que aplican ciertos servicios de seguridad para el tráfico trasportado por ellas. El ISAKMP (*Internet Security Association and Key Management Protocol*) maneja la negociación (parámetros de seguridad), modificación y eliminación de asociaciones de seguridad.

1.1.8.2.3 Detección de Intrusos

El rol fundamental de este sistema es identificar preferentemente en tiempo real una intrusión, uso no autorizado, mal manejo o abuso de un sistema computacional o de red, ya sea que se efectúe internamente o externamente. Se definen políticas de seguridad como: los servicios a ser permitidos dentro del segmento de red monitoreada, o que *hosts* serán accedidos por redes externas, o las actividades a ser monitoreadas. Existen sistemas de detección de intrusos, que se clasifican de la siguiente manera:

❖ En función de la datos a analizar

- *Basados en host (HIDS)*: se concentra en proteger el sistema operativo, se tiene verificadores de integridad del sistema, monitores de registros y

[1] Estos protocolos se describen en el *RFC* 2409

sistemas de decepción entre otros. Usualmente la técnica de atacar un *host* es escuchar o romper una clave.

- *Basados en red (NIDS)*: protege la infraestructura de comunicación, no es necesario ubicarlos en toda la red, se eligen segmentos críticos.

❖ En función de la técnica de análisis usada

- *Detección de anomalías*: se busca en un sistema lo que es normal, para poder detectar lo que no lo es, es un sistema muy complejo ya que requiere un aprendizaje automático.

- *Detección de usos indebidos*: se busca lo anormal de un sistema para atacarlo directamente, el problema es que solo detecta conocidos.

Otra de las clasificaciones es tiempo real vs periódicos, que permiten monitoreo permanente en el caso de tiempo real, los periódicos buscan más bien vulnerabilidades. También existen centralizados vs distribuidos donde el IDS y la lógica del mismo están implementados en un único sistema.

1.1.8.3 Capa Transporte

Los mecanismos aplicados a esta capa establecen un túnel de seguridad o asociaciones en beneficio de otros protocolos y aplicaciones.

1.1.8.3.1 TCP Wrapper

Es una herramienta para monitorear y controlar el tráfico generado tanto por TCP como UDP, no requiere modificaciones en el sistema para funcionar, provee un débil control de acceso, sus decisiones las basa en direcciones IP, usualmente genera *logs* donde se encuentran datos como: nombre del *server host*, nombre del servicio solicitado, y nombre del *host* del cual vino el requerimiento.

1.1.8.3.2 Gateways de Circuito

Son conocidos como *relays* de capa transporte, copian los datos que se trasmiten desde un *host* a un *gateway* de seguridad, entre un *gateway* y un *host* externo y viceversa. Usualmente son utilizados como mecanismos de *firewall*.

- *SOCKS* versión 5: soporta aplicaciones cliente-servidor basados en TCP y además aplicaciones UDP, superando con esto a *SOCKS* versión 4, provee un *proxy*[1] a nivel de capa sesión, no importa la aplicación que cruce sobre este dado que no es un *proxy* de aplicación. Cuando interactúan un cliente y un servidor *SOCKS* negocian métodos de autenticación, luego intercambian parámetros de la misma.

1.1.8.4 Capa Aplicación

A nivel de capa aplicación existen ciertos mecanismos de *firewall* como son los *gateways* de aplicación y filtros de contenido, se maneja también control de acceso y autorización.

1.1.8.4.1 Gateways de Aplicación

Generalmente se los conoce como *proxies*, y tienen como función ser intermediario, entre cliente y servidor: para el cliente que hace la petición, el *proxy* actúa como servidor, pero para el servidor, el *proxy* hace las veces de cliente, receptando las respuestas a la peticiones hechas por el cliente que se encuentra al otro extremo. Se evita generar un gran conjunto de reglas basadas en filtrado de paquetes.

1.1.8.4.2 Filtros de Contenido

Analizan el tráfico en base a la semántica del nivel de aplicación, por ejemplo, puede buscar virus y bloquear la aplicación si se encuentran, analizan adjuntos en

[1] Proxy, hace referencia a un programa o dispositivo que realiza una acción en representación de otro.

correos electrónicos, pueden bloquear *applets* o *scripts* de Java. Se debe considerar que degradarán el *throughput* desde o hacia la red.

1.1.8.4.3 Control de acceso y Autorización

Si el cliente logra autenticarse con el servidor, es necesario que éste le otorgue la autorización para esta conexión, para esto muchos servidores usan RADIUS o TACACS para autenticar y autorizar.

En el caso de RADIUS, por ejemplo, el cliente se conecta a través de un servidor denominado NAS (*Network Access Server*), el cual es cliente de un servidor RADIUS que administra una base de datos, donde se encuentra la información sobre la autenticación de usuario y el control de acceso. Entre los mecanismos de autenticación basados en claves están PAP, CHAP, o UNIX *login*.

1.1.8.4.4 Seguridad en el sistema operativo

La mayoría de sistemas operativos son complejos, por lo que es imposible garantizar seguridad total. Uno de los problemas en varios sistemas son los permisos de super usuario ya que tiene todo tipo de acceso a todos los recursos del sistema, si cualquier individuo llega a obtener permisos como súper usuario entonces no habrá forma de proteger el sistema.

En un sistema operativo seguro se maneja lo que se conoce como monitor de referencia, mediante el cual se refuerza la política de seguridad; éste es el que tendrá acceso a la base de datos donde están los controles de acceso, en algunos casos estos datos son encriptados y solo el monitor tiene la llave para desencriptar dicha información. Una de las maneras de proteger los sistemas operativos es tener detectores de intrusos basados en *host*.

1.1.8.5 Mecanismos complementarios

1.1.8.5.1 Integridad de datos

Se usan funciones *hash*, que son algoritmos que se aplican a los mensajes y generan un valor único de longitud constante dependiendo del algoritmo aplicado por ejemplo en SHA-1 es de 160 *bits*. Esta función debe ser fácil de calcular en una dirección, no debe ocurrir lo mismo en sentido contrario. Las funciones *hash* más conocidas son: MD4, MD5, SHA-1, RIPEMD.

1.1.8.5.2 Encripción

Garantiza confidencialidad de los datos. Consiste en usar métodos para transformar información legible en un formato ilegible, se usará generalmente una clave dentro del algoritmo. Hay dos tipos de criptosistemas: simétricos (clave secreta), asimétricos (clave pública).

1.1.8.5.3 Firma Digital

Permite autenticar, utiliza una combinación de funciones *hashing* y criptografía asimétrica. Primero se calcula el valor *hash* del mensaje, el cual se encripta con la clave privada del transmisor. Al llegar el mensaje al destinatario, este desencripta con la clave pública del transmisor el valor *hash*, verificando de esta manera la integridad del mensaje. Se verifica la identidad del que envía porque solo si se encriptó con la clave privada del transmisor se puede desencriptar con la clave pública del mismo.

1.1.8.5.4 Certificados Digitales

Es un método para ligar una entidad a una clave pública. El certificado está firmado digitalmente por la autoridad certificadora[1] de modo que la autoridad debe

[1] Es una entidad pública o privada que busca llenar las necesidades de confiabilidad especialmente en comercio electrónico.

ser bien conocida, y su clave pública también de modo que no haya necesidad de autentificar la firma digital de la misma.

1.1.8.5.5 Control de Acceso

Está diseñado para mitigar accesos que pueden relacionarse con vulnerabilidades que pueden ser explotadas por amenazas en la red. En la mayoría de los casos la autenticación no es suficiente, ya que los accesos difieren de un usuario a otro, no todos tienen los mismos accesos a recursos. Se tiene control de acceso por:

- *Identidad*.- envuelve criterios de autorización basados en atributos individuales. Con esto se regula accesos a recursos, mas no a la información que se puede encontrar en los mismos.

- *Reglas*.- se basan en un número pequeño de atributos generales o clases. Todos los objetos del sistema tendrán diferentes niveles de seguridad. Este tipo de acceso es frecuentemente referido como control de acceso obligatorio o control de flujo de información.

- *Rol*.- se asigna a un tipo de sujeto que cumple con un rol dentro de la organización, especialmente donde los cambios de personal son constantes.

Hay modelos para control de accesos, entre otros están: discrecional, mandatario y no discrecional.[1]

[1] **Discrecional.-** se basa en tener una lista de acceso, donde se tiene: usuario, objeto a ser accedido, y los privilegios de acceso al mismo.
Mandatario.- trata de emparejar las autorizaciones dadas al usuario y la sensibilidad del objeto a ser accedido, se usa con el control de acceso basado en reglas.
No Discrecional.- se basa en accesos por el rol de individuo, responsabilidades u obligaciones en la organización.

1.1.8.5.6 Padding de tráfico

Protege contra análisis de tráfico no autorizado. Un atacante puede sacar conclusiones basadas en la presencia, ausencia, cantidad o frecuencia de datos intercambiado, en consecuencia, se puede brindar seguridad ya sea generando datos al azar, enviándolo encriptado sobre la red o introduciendo tráfico espurio junto con los datos válidos para que no se pueda conocer si se está enviando información o la cantidad de datos útiles que se están enviando.

1.1.8.5.7 Firewalls

Actúan como puertas entre dos redes, provee el aislamiento necesario entre la red interna y la externa. Debe permitir el paso de tráfico autorizado, a más de ser inmune a cualquier penetración o intrusión.

1.2 VISIÓN GENERAL SOBRE SERVICIOS OFRECIDOS POR UN ISP [4]

1.2.1 ISP (*INTERNET SERVICE PROVIDER*)

Es una compañía que vende servicios de acceso a Internet al público en general. Hay varias maneras que un proveedor puede conectarse al Internet; normalmente un proveedor se conectará con algún tipo de línea de telecomunicación con un *throughput* mucho más alto que cualquier individuo que necesite acceso individualmente o pueda permitirse el lujo de un acceso dedicado. Este *throughput* y costo son entonces “compartidos” por todos los suscriptores. Ofrece servicios de red como alojamiento de páginas *Web*, servicios de correo electrónico, servicio FTP entre otros. Son conocidos tanto por sus servicios, como por su inseguridad; y es que realmente no es fácil compaginar una amplia oferta de servicios con una buena seguridad.

1.2.2 ACCESO WEB

El acceso *Web* en la actualidad es muy popular. Los servicios *Web* corren sobre dos protocolos: HTTP (usando los puertos TCP: 80, 81, 8080, y otros) y HTTPS (usualmente usando el puerto TCP 443). Este servicio ofrece opciones para búsqueda de información, transferencia de texto, imágenes, sonidos, etc. El servicio WWW *(World Wide Web)* fue desarrollado por el centro Europeo de Investigación Nuclear (*CERN*).

Mucha gente confunde las funciones y orígenes de la WEB con, *Netscape*, *Microsoft Internet Explorer*, HTTP y HTML, siendo necesario exponer un resumen de las funciones de dichos términos.

La *Web*.- es la colección de servidores HTTP en el Internet.

HTTP (*Hypertext Transfer Protocol*).- es el principal protocolo en el que se fundamenta la *Web*, este permite acceso a archivos que están a disposición en la misma. Los archivos pueden estar en diferentes formatos como: texto, gráficos, audio, video, etc. El formato usado para los enlaces entre archivos en la *Web* es HTML. Se lo usa para comunicarse con otros protocolos como:

- *Simple Mail Transfer Protocol* (SMTP)
- *Network News Transfer Protocol* (NNTP)
- *File Transfer Protocol* (FTP)
- *Post Office Protocol* (POP)
- *Wide Area Information Servers* (WAIS)
- *Gopher servers*

HTML (*HyperText Mark-up Language*).- se lo conoce como el lenguaje estándar para crear paginas *Web*, permite especificar enlaces hacia otros servidores y archivos.

Web Browsers.- permiten leer documentos vía HTTP y otros protocolos. Los más conocidos son *Mozila, Firefox* y *Microsoft Internet Explorer,* aunque existen cientos de otros *web browsers*.

URLs (*Uniform Resourse Locators*).- Las URLs HTTP son las más usadas, y tienen dos trabajos principales: identificar cual servidor web mantiene el recurso, e identificar cual de los recursos de ese servidor es requerido.

1.2.3 SERVICIO DE CORREO ELECTRÓNICO [4]

Es uno de los más populares servicios de red, permite enviar mensajes con la posibilidad de adjuntar archivos, llegando a ser un servicio de encomiendas electrónicas, sin olvidar que se diseñó para transmitir una limitada cantidad de datos.

Se basa en los protocolos SMTP (*Simple Mail Transfer Protocol*) y POP3 (*Post Office Protocol version 3*) o IMAP4 (*Internet Message Access Protocol versión 4*), SMTP se encarga del envío y recepción de correo, mientras que para el acceso a los buzones de correo se utiliza POP3 e IMAP4.

Existen en el mercado paquetes de software usados para el transporte de correo como son: *Sendmail*, *Microsoft Exchange*, *Lotus Domino*, *Postfix, etc*.

1.2.4 SERVICIO DE TRANSFERENCIA DE ARCHIVOS

Este servicio permite transferir archivos de mayor tamaño que los adjuntos que se envía mediante correo electrónico. El protocolo usado es FTP (*File Transfer Protocol*), es soportado tanto por servidores en Internet como en plataformas de cliente. Un servidor FTP puede ser usado para actualizaciones de programas cliente o tan solo si se desea compartir datos con otros usuarios vía FTP.

Se permite al usuario borrar, renombrar, mover y copiar archivos en el servidor. Para acceder al servicio se requiere de un usuario y contraseña, aunque se tiene

la opción de usuario anónimo, con el cual podrá acceder un usuario común a los archivos de uso público. Los puertos usados son: puerto 21, para recibir y procesar comandos FTP, puerto 20 usado para enviar datos desde el servidor hacia el cliente.

1.2.5 SERVICIO DE ACCESO REMOTO

En muchas situaciones hay la necesidad de acceder a computadores que no están físicamente frente al usuario, ya sea por comodidad o porque las circunstancias lo ameritan, para este tipo de accesos se tienen los siguientes modos: acceso por medio de un terminal o acceso por interfaz gráfica.

1.2.5.1 Acceso remoto por terminal y comandos de ejecución

1.2.5.1.1 Servicio Telnet

El protocolo *Telnet* (puerto 23) permite utilizar una máquina como terminal virtual de otra a través de la red y acceder a los recursos que estén a disposición, de forma que se crea un canal virtual de comunicaciones. Para el acceso se utilizan usuario y contraseña. Para la compartición de recursos debe existir un *software* cargado en la máquina remota que haga las veces de servidor *telnet*.

1.2.5.1.2 Servicio SSH

Provee acceso encriptado tanto para plataformas UNIX como WIN32, para administración de archivos.

1.2.5.2 Acceso remoto con interfaz gráfica [5]

El acceso mediante interfaz gráfica permite visualizar directamente los contenidos del terminal accesado remotamente. *Microsoft* permite acceder remotamente a través de interfaz gráfica como parte de servidores *Windows* 2000 mediante un paquete llamado *Terminal Services*. También está disponible para *Windows NT* 4

con una edición especial de *Terminal Server* del sistema operativo. *Terminal Services y Terminal Server* usan un protocolo desarrollado por *Microsoft* llamado *Remote Desktop Protocol* (RDP), que permite la comunicación entre servidores y clientes usualmente por el puerto 3389.

Una variedad de protocolos propietarios son usados para acceso mediante interfaz gráfica, el más competente y más extendido es *Independent Computing Architecture* (ICA) desarrollado por *Citrix*.

1.2.6 SERVICIO DNS (DOMAIN NAME SYSTEM) [1]

Diferentes protocolos usan los servicios de nombre de dominio, el principal es el DNS, que está compuesto de servidores de nombre*, resolvers, y* sus protocolos de comunicación, todos juntos crean el servicio de directorio distribuido de Internet, que es capaz de convertir *hostnames* a direcciones IP, dado que las aplicaciones de Internet no hacen referencia a las direcciones binarias sino a cadenas de caracteres ASCII. Incluso es más fácil recordar nombres denominados dominios, como *google.com* que una dirección IP, 216.239.39.99. Los dominios son registrados por las organizaciones a través de proveedores como son: *Network Solutions y Register.com.* La resolución de nombre a dirección IP se denomina *forward* DNS *lookup,* el usuario envía un DNS *query* o una consulta al servidor DNS, el cual le va responder si tiene información, con la IP correspondiente, como se muestra en la figura 1-3.

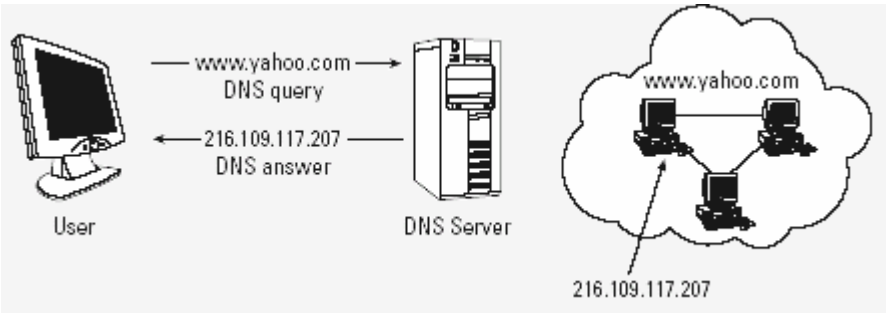


Figura 1- 3: *forward DNS lookup* [3]

El DNS permite a cada sitio guardar información sobre sus propios *hosts* y buscar información de otros sitios. Si bien el DNS no es un servicio a nivel de usuario, es la base para otros protocolos que necesitan del mismo como: SMTP, FTP, Telnet.

1.2.7 SERVICIO DE NOTICIAS [4]

1.2.7.1 Noticias *Usenet*

Es un servidor que está compuesto por miles de grupos de noticias (*newsgroups*), razón por la cual es el servicio más importante para intercambio de artículos de diferentes tópicos a nivel mundial. Los usuarios podrán leer estos artículos y también aportar si lo desean (el servicio *Usenet* es ahora propiedad de *Google*).

Los servidores de noticias guardan su artículo y también envían una copia a los servidores vecinos que podrían estar interesados, así se realiza la propagación de noticias.

Los grupos de noticias están clasificados por jerarquías de intereses similares, entre las más importantes tenemos:

- *USENET computer newsgroups*
- *USENET discussions about Humanities*
- *USENET miscellaneous newsgroups*
- *USENET news*
- *USENET recreational newsgroups*
- *USENET science newsgroups*
- *USENET social issues newsgroups*
- *USENET talk newsgroups.*

1.2.7.2 NNTP (*Network News Transport Protocol*)

El Protocolo de transferencia de noticias a través de la red (NNTP) es un protocolo TCP/IP basado en cadenas de texto que se envían de forma

bidireccional a través de canales TCP ASCII de siete bits. El protocolo NNTP es propiedad de IETF y se define en RFC 977. NNTP se denomina habitualmente Protocolo de noticias de Internet, porque contiene las reglas utilizadas para transportar artículos de noticias de un equipo a otro.

1.2.8 SERVICIO DE *HOSTING* [4]

Provee al cliente la posibilidad de alojar sus páginas *Web* en un servidor destinado a publicar páginas *Web*. La capacidad será contratada por el cliente, pero dependerá de las políticas que tenga el proveedor del servicio.

1.2.9 SERVICIO *PROXY – CACHÉ* [4]

Es un servicio muy importante, permite disminuir tiempos de respuesta ante una petición de una página *Web* solicitada o un archivo vía FTP. La idea de un *proxy – caché* es actuar como intermediario, el cliente solicita la página, pero como el *proxy* actúa de intermediario, la respuesta llega a él y éste le reenvía al cliente, pero también guarda una copia local de esta página o archivo, para que, cuando haya un pedido posterior a la misma página, la descarga sea más rápida.

Dado que el tráfico P2P (*Peer to Peer* - descargas de música, videos, etc), tiende a saturar enlaces, algunos ISPs están optando por *cachés* P2P.

1.2.10 SERVICIO DE CONFERENCIA EN TIEMPO REAL [4]

Existen diferentes servicios de conferencia en tiempo real disponibles en Internet entre otros están: *talk*, *web chat*, *rooms, y* varios servicios provistos sobre *Multicast Backbone (*MBONE*).* Todos estos servicios permiten a las personas interactuar con otras. Por ejemplo, los servicios de correo y noticias no necesitan que los participantes estén en ese momento en línea, en cambio, en los servicios de conferencia en tiempo real como su nombre lo indica, los usuarios deben estar en línea.

1.2.10.1 *Internet relay chat* (IRC)

Fue creado en Finlandia en 1988, y permite a usuarios de todo el mundo obtener conversaciones vía texto en línea y en tiempo real. Los usuarios acceden mediante clientes IRC, o vía *Telnet* a lugares donde se tienen clientes IRC públicos. Los servidores IRC manejan cientos y algunas veces miles de canales para unir usuarios. Comparado con *talk,* donde se limita para un par de usuarios, IRC permite que varios usuarios participen en un canal IRC.

1.2.10.2 MBONE

Es la fuente de un nuevo conjunto de servicios en Internet, enfocados a expandir los servicios de conferencia en tiempo real, que va más allá de servicios basados en texto o IRC. Se lo usa para enviar video en tiempo real, conferencias técnicas y programas por Internet.

Cada día el servicio de *chat* avanza permitiendo a los usuarios enviar y recibir archivos, mantener conversaciones y en resumen expandir el universo social del usuario.

1.2.11 SERVICIO DE VOZ [4]

Permite a dos personas en cualquier lugar del mundo a través del Internet tener una conexión por voz, sin tener que pagar por una conexión internacional. En la actualidad, los protocolos usados para transmisión por voz, permiten tener un conjunto de características muy buenas, acompañada de escalabilidad y estandarización.

1.2.12 SERVICIO DE TIEMPO [4]

NTP (*Network Time Protocol*): es un protocolo de Internet que fija el reloj en un sistema con gran precisión, tiene clientes en diversos sistemas operativos como: *Unix*, *Windows NT*, y *MacOS*. Es importante tener una referencia externa en

cuanto a tiempo, porque puede suceder que todos los equipos se encuentren con un error de tiempo, afectando por ejemplo a *logs* de donde se obtiene información de sucesos ocurridos en el sistema.

1.3 SEGURIDADES PARA ISPs [6]

Los problemas de seguridad para los ISPs, son mucho más amplios que cualquier otra red, no es fácil compaginar una amplia oferta de servicios con una buena seguridad. Los ISPs viven justamente de permitir accesos a Internet incluso a sus propios servidores, entonces no podrán aplicar políticas estrictas de seguridad en su sistema. Un claro ejemplo es si un ISP no permite acceso FTP a los clientes que deseen alojar sus páginas *Web* y les obliga a usar un protocolo de transferencia de archivos que aplique criptografía, lo más probable es que muchos de esos clientes abandonen y se vayan a la competencia.

La seguridad de los ISPs sufre el problema típico en cualquier entorno; es decir, se está trabajando con algo intangible. Si se realiza una inversión para incrementar la seguridad quizás las mejoras obtenidas nunca las pueda notar el usuario. La mayor parte de los clientes de un ISP prefieren una conexión un poco más rápida frente a una conexión o unos servicios más seguros.

Se pide mucho de un ISP, como por ejemplo: efectividad en costos, además de un alto rendimiento en la conectividad a Internet, y si a esto se añade seguridad, entonces se notará que las medidas para dicha seguridad podrán afectar en la operación de la red del ISP. Los ISPs son blancos para ataques con código malicioso, actos criminales, etc. A más de protegerse a sí mismos tienen que proteger a sus usuarios y minimizar los riesgos de que sus usuarios lleguen a afectar de alguna manera a la misma Internet.

1.3.1 OBJETIVOS EN EL ÁMBITO DE SEGURIDAD PARA UN ISP [6]

- Protegerse a sí mismo.
- Ayudar a proteger a sus usuarios.

- Proteger al Internet de sus usuarios.

La figura 1-4, muestra claramente que estos objetivos deberán cumplirse, para alcanzar niveles aceptables de seguridad, ya que el ISP se encuentra expuesto a diversos ataques por usuarios grandes, medianos y pequeños, a más de tener la red externa que es la Internet.

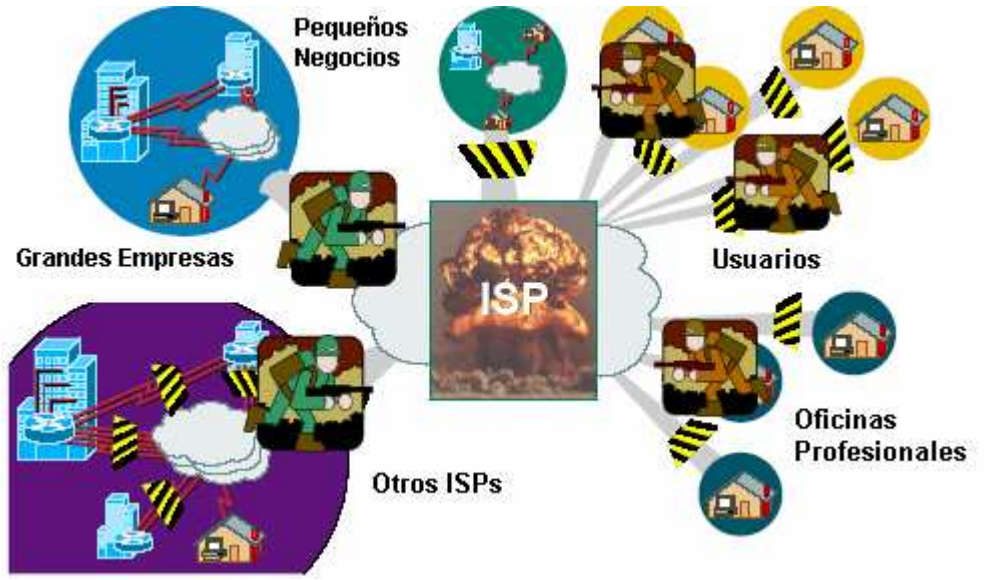


Figura 1- 4: Nuevos entornos de batalla para un ISP [4]

1.3.2 MODELO DE ASEGURAMIENTO CONTINUO [6]

Implementar seguridad no es algo opcional en un ISP, es algo de vital importancia, por lo que el modelo de aseguramiento continúo (ver figura 1-5) aplicado a diversas redes es aplicable con más razón aquí.

Entre las diversas opciones a implementar, el ISP deberá cumplir con los cinco pasos esenciales de este modelo que se detallan a continuación:

Figura 1- 5: Modelo de Aseguramiento Continuo [4]

1.3.2.1 Establecer e implementar políticas de seguridad

Las políticas de seguridad y los procedimientos definen niveles aceptables de seguridad, en primer lugar se tienen las políticas que definen los activos a proteger, es decir las entidades y los motivos a proteger, describe la seguridad en términos generales, son declaraciones de las metas a ser alcanzadas por los procedimientos. Los procedimientos incluyen los detalles es decir, quién, como y cuando se ejecutarán.

1.3.2.2 Asegurarse

Son mecanismos que el ISP deberá implementar para asegurarse; entre los principales se tiene: encripción, autenticación, controles de acceso, auditorias, *firewalls* y *patching*.

1.3.2.3 Monitorear y responder

Monitorear es una actividad continua, preferentemente debe hacerse en tiempo real. Reporta eventos de seguridad que podrían ser peligros para la red y sus recursos. Entre los objetos monitoreados están: tráfico de la red LAN, y hacia o

desde Internet, protocolos LAN, inventario de los dispositivos de red, etc. Mecanismos de detección de intrusos, se usan como complemento de monitoreo.

1.3.2.4 Pruebas

Se las conoce también como *ethical hacking*, en este caso, lo que se trata de descubrir es que tipo de defensa tiene actualmente el ISP, que debilidades presenta la red y los recursos de la misma. Se utilizan medios que usan los atacantes, la diferencia es que el objetivo es obtener información para mejorar la red; entre los datos que se pueden obtener están:

- Reacción del sistema ante un ataque
- Calidad y fortaleza de las defensas
- Información susceptible a ataques

Entre los métodos más comunes para probar los problemas que puede tener la red se tiene los siguientes:

1.3.2.4.1 Prueba de penetración interna

Trata de obtener conexión no autorizada y acceder a la red, determinar la arquitectura de la misma identificando, por ejemplo sistemas operativos de dispositivos, vulnerabilidades del mismo, evaluar la respuesta de cualquier sistema de detección de intrusos, determinar si hay objetos no autorizados conectados a la red.

1.3.2.4.2 Prueba de penetración externa

La meta es acceder de manera no autorizada hacia la red interna, obtener información de la misma, ya sea información en tránsito o que se encuentra almacenada en recursos de la red interna, sirve para probar el sistema de detección de intrusos externo, y el *firewall*.

1.3.2.4.3 Prueba con conocimiento completo de la red

Se asume que el atacante tiene excesivo conocimiento de la red por lo que tendrá éxito en la penetración a la red.

1.3.2.4.4 Prueba con conocimiento de las vulnerabilidades

Puede incluir ataques directos a las vulnerabilidades conocidas.

1.3.2.5 Administrar y mejorar

Una vez obtenidos los resultados de las diversas pruebas, o a su vez, si se ha tenido ya un incidente, el ISP deberá mirar si los procesos, procedimientos, herramientas, técnicas y configuraciones pueden ser mejorados.

1.3.3 ATAQUES COMUNES A ISPs [6]

Similar a cualquier red, los ISPs sufren ataques, en esta sección se mencionan tres tipos de ataques:

1.3.3.1 Reconocimiento

El posible atacante, mira a través de herramientas o comandos, el tráfico de la red; puede usar *sniffers*, *scripts* construidos para ese propósito, etc. El objetivo final es acceder a información importante o descubrir vulnerabilidades del sistema.

1.3.3.2 Acceso

Manipulación de datos sin autorización, en base a mecanismos para descubrir usuarios y contraseñas para entonces acceder al sistema.

1.3.3.3 Negación de servicio

El atacante podrá sobrecargar recursos de la red, y así dejar sin acceso a cierto servicio.

1.3.4 RESPUESTA ANTE INCIDENTES DE SEGURIDAD [7]

Se mencionan las siguientes fases:

1.3.4.1 Preparación [8]

Se deberán crear grupos de respuesta ante incidentes, conocedores de políticas y procedimientos creados para este fin. Para tal fin, se pueden construir canales de comunicación entre otros ISPs, así como también con los usuarios de la red del proveedor de servicios. Deberán existir canales de comunicación entre proveedores de *hardware* y *software* del ISP. Si hay herramientas automáticas para manejar incidentes y permiten conocer el enemigo, se deberá estar muy bien familiarizado con ellas. Si fuere posible, conocer al enemigo y las armas que podría usar.

1.3.4.2 Identificación [9]

Es necesario un monitoreo constante, lo que permitiría tener una idea clara sobre el comportamiento de tráfico, para fácilmente detectar conductas anómalas. Es recomendable usar herramientas que entreguen información sobre: utilización del CPU, estabilidad de la ruta, *Netflow*, etc. La necesidad de ser pro-activo es importante, se debe notificar a los clientes sobre fallas antes que ellos lo hagan hacia el ISP.

1.3.4.3 Clasificación

Implica comprender el tipo de ataque y la cantidad de daño que está causando. En base a todos los datos recogidos, se puede medir el riesgo que puede

ocasionar el ataque. El problema surge si no se conoce las características del ataque, entonces la reacción podría agravar el problema. Las técnicas que se usan con frecuencia son: clasificación mediante ACL y *Sink Hole*[1].

1.3.4.4 Traceback

Tiene como meta identificar el sitio donde se origina el ataque, ya sea éste interno o externo. Una vez identificado el ataque es necesario un rastreo del mismo, para esto existen los siguientes mecanismos: *hop by hop*[2] y *jump to ingress*[3].

1.3.4.5 Reacción

Significa ejecutar algún mecanismo para responder y mitigar el ataque, o incluso se puede escoger no hacer nada. Entre los mecanismos que ejecutan algunos ISPs para ayudar a usuarios que están siendo atacados es desechar los paquetes que provienen de una lista de direcciones origen, o limitar la velocidad de los enlaces. Entre las técnicas usadas están: ACL, CAR (*Committed Access Rate*), *Sink Holes*.

1.3.4.6 Post Mortem [10]

Este punto consiste en analizar que es lo que precisamente sucedió (análisis de la causa raíz), y si se puede construir algún tipo de resistencia, si el ataque ocurriese otra vez. Es importante revisar procesos, procedimientos, herramientas, técnicas y configuraciones para mejorarlas. Se deberá informar a los clientes cuando el problema esté solucionado.

---

[1] Similar a un *Honey Pot* (una trampa o *host* para engañar al atacante).
[2] Es un rastreo ruteador por ruteador, entre las limitaciones que tiene es la velocidad.
[3] Usa *NetFlow* en el router de ingreso para descubrir el ataque. *NetFlow* es una tecnología que permite entregar un conjunto de servicios para aplicaciones IP, los más conocidos son: contabilidad del tráfico en la red, planeamiento de la red, seguridad, monitoreo de ataques de negación de servicio, y monitoreo de la red. Provee información vital de usuarios y aplicaciones en la red.

1.3.5 SEGURIDAD EN LA INFRAESTRUCTURA DEL ISP [3] [6]

1.3.5.1 Generalidades de seguridad física del ISP

Aunque es un área olvidada en la mayoría de redes, es fundamental porque usualmente los ataques a sistemas o recursos de una red son internos, entonces es más fácil acceder, por ejemplo, a una copia del sistema por vulnerabilidades físicas, que buscar vulnerabilidades en el *software*. Este proyecto no intenta diseñar un nivel aceptable de seguridad física del ISP, por lo que se mencionan las siguientes pautas generales a seguir:

- Controles de accesos físicos, alarmas, etc, para protección del cuarto de equipos.

- Los desastres naturales es otro factor a considerar, incluso no es necesario un desastre si se habla de tormentas eléctricas, las cuales suelen originar descargas que llegan a través de líneas telefónicas, líneas de acceso a usuarios, y el sistema eléctrico; por este motivo, se deberá considerar el uso de voltaje regulado, protectores de línea, y un correcto sistema de puesta a tierra.

- Deberán haber sistemas de control de incendios, temperatura, humedad, en donde sean necesarios.

- Dado que suelen ocurrir cortes de energía, es indispensable el uso de UPSs[1], para garantizar la continuidad del servicio, aún en la ausencia de energía eléctrica habitual.

1.3.5.2 Seguridad en la red del ISP

Un ISP prototipo tiene una red como se muestra en la figura 1-6, con tráfico entrante de usuarios u otros ISPs, y saliente desde el ISP hacia los mismos, lo

[1] Dispositivo de respaldo de energía.

que lleva a pensar en mecanismos para asegurar la red del ISP, como son: *route filtering*, *packet filtering*, y *rate limits*.

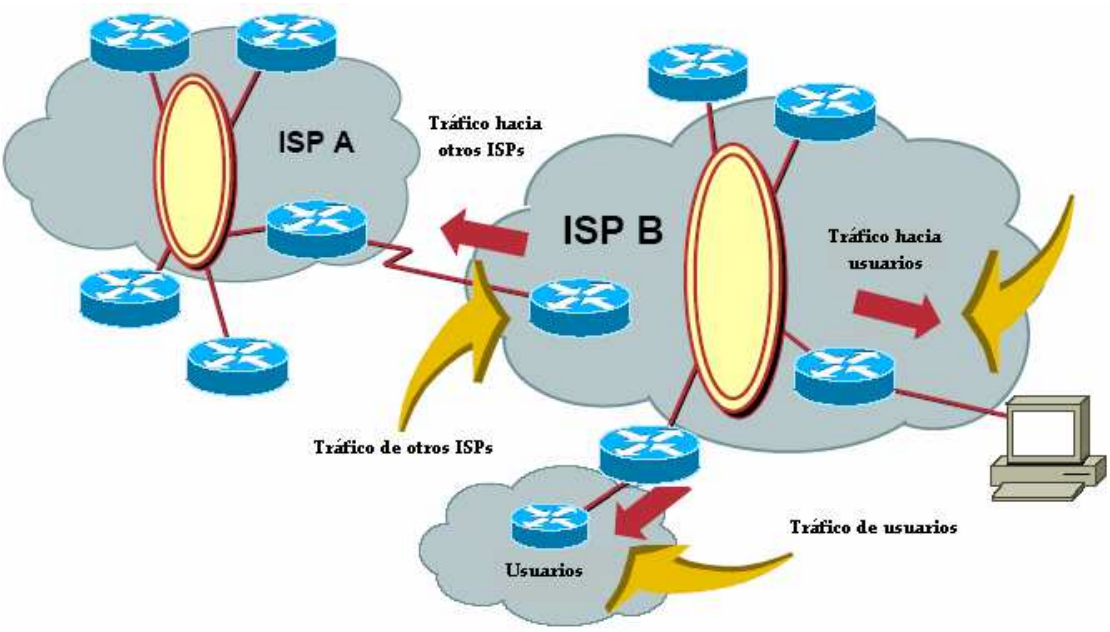


Figura 1- 6: Tráfico hacia o desde un ISP [4]

1.3.5.2.1 Route filtering

Hay rutas que no deberían estar dirigidas a Internet, y que son las pertenecientes al rango de direcciones privadas o aquellas listadas en el RFC 1918, las que incluyen las siguientes: 10.x.x.x/8, 172.16.x.x/12, 192.168.x.x/16, de la red de retorno o *loopback* 127.0.0.0/8, direcciones reservadas, como las de auto configuración DHCP 169.254.0.0/16, *default* y *broadcast* 0.0.0.0/8, 0.0.0.0/32, y 192.0.2.0/24, 224.0.0.0/4, 240.0.0.0/4 *TEST-NET*.

El protocolo de enrutamiento debería tener filtros aplicados para que estas rutas no sean anunciadas o propagadas a través de la Internet. Hay técnicas que permiten deshacerse de tráfico que puede sobrecargar la red, como son: *Black Hole Filtering, Black Hole Shunt, Sink Hole.*

1.3.5.2.2 Packet filtering

Este mecanismo intenta defender en lo posible tres componentes de la red del ISP: la red de acceso de clientes, la red del ISP en sí, y la red hacia la Internet. Por ejemplo, se estipula que los usuarios del ISP no deberán enviar paquetes con una dirección origen, que no sea la que está asignada a ellos.

Las técnicas para filtrado de paquetes son: listas de acceso estáticas aplicadas al borde de la red, listas de acceso dinámicas con perfiles AAA, y *unicast* RPF.

- *Listas de acceso estáticas*: serán creadas para limitar o negar el acceso desde o hacia la Internet, de redes no autorizadas.

- *Filtro en el enrutador de borde*: en el *upstream* del enrutador se permitirá tráfico saliente, de direcciones origen que estén destinadas a la red del ISP, las demás redes deberán ser bloqueadas. El tráfico entrante, en cambio, será permitido para cualquier red, excepto las direcciones pertenecientes al *backbone* del ISP. Esto también es aplicable si se tienen enrutadores de acceso para clientes. (Ver figura 1-7).

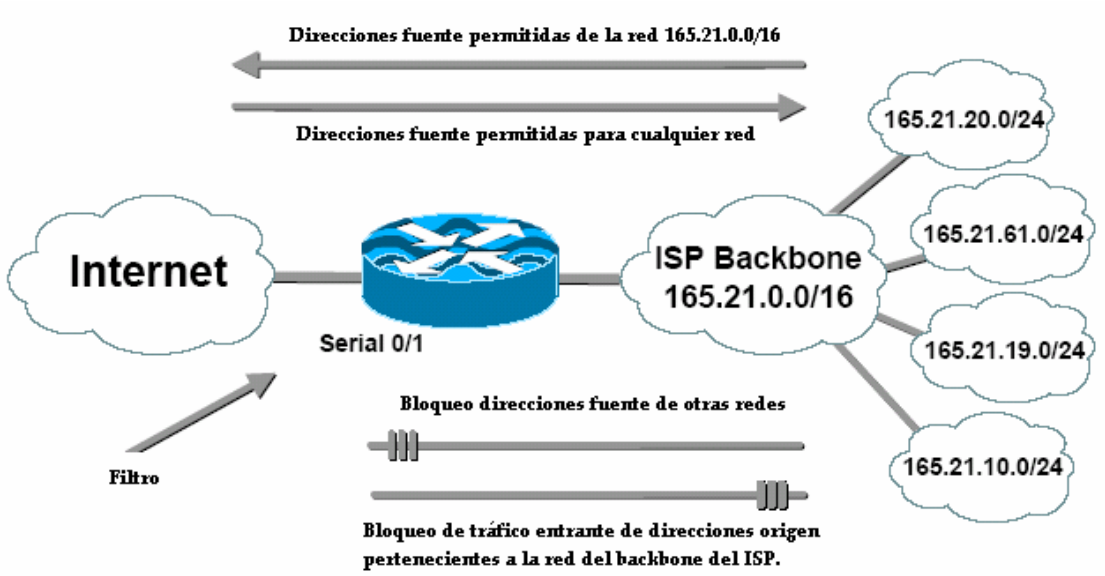


Figura 1- 7: ACLs para enrutadores [4]

- *Listas de acceso dinámicas*: se trabaja usualmente con usuarios *dial-up*, las listas de acceso están almacenadas en un servidor AAA, el cual entregará información sobre accesos de determinado usuario. Soporta el uso de mecanismos de autenticación como RADIUS y TACACS.

- *Reverse path forwarding*: los paquetes IP origen son chequeados para verificar que la ruta de regreso hacia la fuente u origen no sea a través de la misma interfaz, si no hay cumplimiento de esto los paquetes son descartados. En principio se diseñó para enrutadores de acceso hacia el ISP, pero nuevas mejoras permiten que se trabaje a nivel de acceso del ISP, con el proveedor del mismo.

1.3.5.2.3 Rate limits

Diseñado para controlar ráfagas de tráfico, provocado por ejemplo por un ataque de negación de servicio, la forma de trabajar es desechando paquetes antes de ser procesados, el administrador de la red podrá limitar tráfico de fuentes o destinos específicos.

Otro mecanismo para asegurar la red del ISP, es segmentarla, destinando accesos y privilegios a los servicios, dependiendo la ubicación del usuario.

1.3.5.3 Seguridad en servidores [1]

Para estas plataformas de servicio, la protección, es de vital importancia ya que son blanco fácil de los atacantes por los siguientes motivos:

- El gran volumen de datos críticos que contienen.

- Si el atacante logra obtener acceso a un servidor, probablemente logre alcanzar a una estación de trabajo.

- Los servidores son fáciles de encontrar ya que están expuestos por la gama de servicios que ofrecen.

Existen varias consideraciones de seguridad a tomar en cuenta al momento de adquirir una de estas plataformas, por ejemplo el *software* instalado en los mismos, debe estar desarrollado con altos niveles de seguridad, pocas vulnerabilidades, para así reducir costos por trabajos de administración del mismo.

1.3.5.3.1 Operación segura de servidores

Para operar de manera segura servidores de la red del ISP, hay que tomar en cuenta los siguientes aspectos:

- *Controlando la configuración del servidor*: hay tres consideraciones básicas en este tema: asegurar físicamente el sistema (sólo personal autorizado podrá acceder físicamente), minimizar el riesgo, mediante la eliminación de servicios levantados innecesariamente (separar servicios), y respaldos del sistema para mitigar los riesgos y daños que pueden surgir si se diera un ataque. Las configuraciones deben ser hechas de tal manera que minimicen el riesgo de sufrir un ataque, y por lo tanto no se debe dejar cosas configuradas por defecto. El sistema operativo y las aplicaciones deberán ser permanentemente actualizados.

- *Controlando accesos y usuarios*: es necesario establecer control de acceso a los datos, por parte de los usuarios. El principio básico aquí es que ya sean usuarios o desarrolladores no deberán tener ningún tipo de acceso extra, sino sólo el necesario para ejecutar sus aplicaciones o servicios específicos. Será necesario tener algún tipo de autenticación, por ejemplo mediante contraseñas las cuales serán almacenadas pero en forma encriptada. Como característica importante debe tener la habilidad de controlar el acceso de varias formas de programas ejecutables.

- *Monitoreo, auditoría, y logging*: es un aspecto crítico y de vital importancia para detectar ataques y responder inmediatamente a los mismos. *Logging* es el mecanismo que tiene el servidor para grabar eventos, y posterior a esto, reconstruir un ataque o incidente. El monitoreo es una revisión continua de los *logs* del sistema, además de otro tipo de información del mismo. Auditoría es el proceso mediante el cual se verifica que el *logging* y el monitoreo se están ejecutando de acuerdo a un plan o procedimiento.

1.3.5.4 Seguridad en los enrutadores [11]

Los enrutadores juegan un papel muy importante en las redes, razón por la cual a más de brindar protección al enrutador, se ayuda a proteger a la red que sirve.

1.3.5.4.1 Seguridad física

El lugar donde se encuentra el enrutador, debe tener las siguientes características: libre de interferencia electrostática o magnética, control de temperatura y humedad, fuente de poder ininterrumpida, considerando que existen ataques de negación de servicio debe estar configurado con el máximo de memoria posible, los accesos físicos al cuarto donde se encuentra el enrutador deberán ser autorizados.

1.3.5.4.2 Sistema operativo

El sistema operativo en un enrutador es un componente de vital importancia, dependiendo de las necesidades de la red, se escogerá la versión de *software* más fiable, recordando que la última versión probablemente no exista para el tipo de *hardware* que se dispone, entonces lo recomendable es usar la versión disponible más estable.

1.3.5.4.3 Adecuada configuración

Similar a muchos sistemas, los enrutadores vienen configurados con algunas características por defecto, que no son necesarias, y por ende los atacantes pueden usarlas para recolectar datos, razón por la cual deben ser deshabilitadas en la configuración personalizada del ISP.

1.3.6 SEGURIDAD EN SERVICIOS DEL ISP [12]

1.3.6.1 Seguridad *Web*

1.3.6.1.1 Problemas de seguridad en el protocolo HTTP

HTTP trabaja encima del protocolo de transporte TCP (*Transmission Control Protocol*), opera a través de un modelo simple de petición - respuesta. El cliente o *browser Web,* inicia la sesión usando un método de petición (GET*,* HEAD*,* POST*,* PUT*,* DELETE*, etc*), un objeto de petición (URI)[1], cero o más cabeceras, cero o más entidades en el cuerpo del mensaje. Los servidores *Web* procesan y manejan la petición hecha y retornan al cliente la respuesta más apropiada.

- *Seguridad en transacciones Web*: Al igual que todo sistema a ser asegurado, los mensajes HTTP deben llenar los siguientes requerimientos de seguridad: autentificación del mensaje origen, integridad del mensaje, confidencialidad, no repudio del mensaje origen.

Los peligros a los que está expuesto son los siguientes: información sensible llevada en las cabeceras, *spoofing* de la dirección IP, fuga de información importante, si la existencia del recurso o su URI son confidenciales, se podría encriptar.

[1] Request – URI: Es el objeto de interés es decir el que será procesado en el servidor *Web*.

Por las pocas seguridades que ofrecen los mecanismos de autenticación en cuanto a los mensajes transmitidos, se tienen otros mecanismos después de autenticar:

- Protocolos para asegurar el canal (SSL o TLS)
- Protocolo de encapsulamiento seguro de identidades (PGP, S/MIME)
- Extensiones de HTTP (S-HTTP, PEP)

La solución basada en canales seguros no garantiza en contra de problemas de seguridad relacionados con negación de eventos, la razón es que para garantizar que no se niegue un evento, el cuerpo del mensaje deberá contener una firma digital, la cual va en el cuerpo del mensaje, no en el flujo de datos. La principal ventaja de un canal seguro es que pueden añadirse de forma transparente a HTTP, y protege el mensaje completamente (línea de inicio, cabeceras, y cuerpo del mensaje). La forma de asegurar HTTP por medio de SSL se conoce como HTTPS.

Al usar PGP y S/MIME los mensajes son encriptados y posteriormente transportados dentro de mensajes HTTP, como entidades dentro del cuerpo del mensaje, en este caso HTTP es usado como protocolo de transporte para mensajes ya protegidos. El servidor y el cliente pueden generar y comprender los formatos utilizados para encripción. Con esta solución no se protegen las líneas de inicio o cabeceras. Además como estos formatos de encripción no forman parte del protocolo, HTTP no ofrece mecanismos para negociar mecanismos de seguridad.

Las ventajas de usar extensiones HTTP es que comprenden la semántica de mensajes HTTP, son protocolos orientados a mensaje que trabajan a nivel de aplicación, por ende es posible negociar opciones de seguridad a nivel de HTTP.

1.3.6.1.2 Problemas y mecanismos de seguridad en el servidor Web

Los servidores *Web*, son accedidos por desconocidos, frecuentemente usuarios anónimos, por lo que no pueden protegerse a sí mismos con mecanismos de autenticación de clientes, más bien usan mecanismos de control de acceso, por lo que deberían tomar especial cuidado en la información activa que está usualmente almacenada en bases de datos, y en algunos casos requiere protección de derechos de autor. Otro factor a tomar en cuenta lo constituyen los mecanismos que tiene un cliente para ejecutar comandos en el servidor (CGIs), pudiendo ser deshabilitados completamente, o tener un rango limitado.

El contenido activo en un sitio *Web* está compuesto por ejecutables en el lado del servidor, y ejecutables en el lado del cliente. Esta parte se centra en el lado del servidor.

- *Programas externos*: usualmente se permite por medio de programas externos que una página sea cambiada mediante el uso del *browser*. Entre estos se tiene el uso de CGI *scripts*, o también *Active Server Pages* (ASP, usadas para crear páginas dinámicas). Los problemas que vienen relacionados con este tipo de programas es que provienen de diferentes fuentes y son escritos en múltiples lenguajes, por lo que no es raro encontrar tres o cuatro capas de programas para una simple página, entonces si se tienen problemas de seguridad, el sistema en sí es vulnerable.

- *Scripts CGIs*: CGI (*Common Gateway Interface*), fue la primera interfaz diseñada para proveer a los desarrolladores la capacidad para producir contenido dinámico en sus sitios *Web*, como ejemplo se tiene: sitios de registro, páginas *Web* basadas en foros de *chat*, búsquedas de información en línea en bases de datos, etc. En definitiva, lo que va permitir un CGI es la comunicación entre un servidor *Web,* y un programa escrito en algún lenguaje de programación.

Aunque los *scripts* CGIs usualmente están en un directorio específico, y separados físicamente de archivos del sistema, errores de configuración pueden conducir a permitir accesos de usuarios malintencionados.

Los *Scripts* CGI pueden ser programados de forma más segura usando *wrappers,* que en algunos casos actúan buscando hoyos de seguridad en el *script*, o ejecuta el *script* en un ambiente restringido, limitando accesos a archivos del sistema, CPU, disco, y otros recursos del sistema.

- *Servlets:* los *servlets* son a los servidores, lo que las *applets* para los buscadores *Web*, representan un tipo de código móvil, por ende deberá cumplir con todos los requerimientos de seguridad dispuestos para código móvil. Los *servlets* pueden ser usados para extender las funcionalidades de un servidor *Web*, y manejar peticiones HTTP.

- *Accesos a Bases de datos*: los controles de acceso usualmente en una red con acceso a bases de datos, serán a través de redes desmilitarizadas (DMZs)[1], dependiendo de las políticas de seguridad. No es posible diseñar una base de datos que sea completamente segura, y a la vez cumpla requerimientos de tiempo real, ya que a mayor seguridad mayor será el retardo que presente.

❖ *Ataques comunes a servidores web*

Un servidor *Web* es objeto de ataque por su gran valor y su alta probabilidad de vulnerabilidades.

Account Harvesting: significa apoderarse de información de cuentas legítimas, para luego tener acceso al sistema. Suele ser uno de los primeros pasos de un atacante.

[1] Es un segmento de red con niveles mínimos de seguidad.

Directorios listados: un error común de los administradores de sitios *Web* es permitir un listado de directorios por defecto, cualquier página nombrada *index.html* o *index.htm* dentro de un directorio podría ser desplegada, si se diera el caso que un archivo no exista, y si está permitido el listado de directorio.

Búsqueda investigativa: la idea de este ataque es buscar piezas de información publicadas en la Internet, tales como direcciones de correo electrónico, que en muchos de los casos conducen a varias direcciones de donde se puede obtener un único nombre de usuario, la tendencia de los administradores *Web* es proveer demasiada información en sus sitios, dando municiones al atacante para atacar los mismos.

Autorización defectuosa: errores en autorización pueden conducir a un *account harvesting,* o peor aún, a personificación.

Otros:

- Ataques de negación de servicio
- Ataques de desbordamiento de *buffers*, ejecutando comandos arbitrariamente

❖ *Mecanismos de seguridad:*

Consideraciones:

- Configurar cuidadosamente la seguridad y características de control de acceso de usuarios.
- Correr el servidor como un usuario no privilegiado
- Usar permisos del sistema de archivos para asegurar que el servidor no pueda leer archivos a los cuales no tiene acceso.
- Minimizar la cantidad de información sensible en la máquina.
- Limitar el número de personas que pueden publicar datos en los sitios *web*.

Minimizar riesgos con el uso de programas externos:

- Instalar programas externos solo después de considerar las implicaciones de seguridad de los mismos.
- Ejecutarlos lo menos posible.
- Correrlos con permisos mínimos.
- Desarrollar configuraciones especiales para programas externos en *bastion hosts*[1].

1.3.6.1.3 Seguridad en el cliente Web

Al igual que los servidores *Web* los clientes *Web* tendrán varios problemas como: inseguridad en el envío de información, vulnerabilidad en visores externos, y vulnerabilidad en sistemas de extensión.

- *Inseguridad al envío de información*: los *web browsers* pasan información confidencial sin protección, como son nombres de usuario y claves. Otro de los peligros son los *cookies*, que son pequeños rastros que deja un sitio de Internet, contendrá información que será recordada en el próximo inicio de sesión de dicho sitio; dado que viajan a través de la red sin encripción, no se los usará para transacciones críticas, como envío de números de tarjetas de crédito. Ciertos *browsers* no soportan *cookies,* o solo aceptan algunos como medida de seguridad.

- *Vulnerabilidades con visores externos*: el servidor provee datos en diferentes formatos, por lo que es necesario visores, entre ellos pueden ser los denominados descompresores, por ejemplo *plug-ins* que ayudan a visualizar algún tipo de información.

Entre las implicaciones de seguridad se tiene: vulnerabilidades inherentes de programas externos, de los cuales el atacante podría tomar ventaja, y nuevos

[1] Un *bastion host* es el sistema principal que da frente al Internet, se encuentra entre la red externa y la red interna.

programas o nuevos argumentos para programas existentes, podrían usarse para que el usuario cambie la configuración local.

- *Vulnerabilidades en sistemas de extensión*: los sistemas de extensión permiten mediante páginas Web, descargas de programas que se ejecutan en el *browser* para dar mayores ventajas que las que se obtiene por visores externos, sin embargo mayores capacidades hacen del lenguaje más peligroso, un ejemplo de esto es que el usuario busca por el nombre de la herramienta, y si la encuentra simplemente la ejecuta, sin saber que el atacante pudo haberla usado como carnada para ejecutar otro código malicioso.

❖ *Ataques comunes al cliente Web*

- *Web spoofing*: el atacante crea una convincente pero falsa copia de un sitio *Web* visitado por el usuario, logrando visualizar todo el tráfico entre cliente y la *Web*.

- *Violaciones de privacidad*: usualmente son causadas por: contenido ejecutable o código móvil, *cookies*, *logs*. Como ejemplo si un cliente descarga una página *web*, lo común es que se guarde información del cliente como la dirección IP, la petición URI y otro tipo de información en *logs,* que posteriormente pueden ser usados para violar la privacidad del usuario.

❖ *Mecanismos de seguridad*

Se deberá combinar una instalación cuidadosa, configuración en el lado del cliente, programas auxiliares que busquen hoyos de seguridad y educación del usuario.

Entre las mayores ayudas estarán los filtros de contenido, se podrá filtrar todo lo que es peligroso, pero se corre el riesgo de nuevos ataques.

Existen las técnicas de *anonymizing*, que buscan ocultar la identidad tanto del que envía como del que recibe, otros mecanismos de *anonymizing* como *onion routing* o *crowds* generalmente proveen un proxy de filtrado que remueve *cookies*, y algunos otros medios por los que un servidor podría identificar a un cliente.

1.3.6.1.4 Seguridad en código móvil

Se conoce como código móvil al contenido ejecutable dinámicamente descargable, se transmite a través de una red de comunicaciones, y se ejecuta al llegar al *host* de destino. Está presente en clientes *web* (*Java Applets*, Controles *ActiveX*, Agentes Móviles) y servidores *web* (Agentes Móviles, *Servlets*).

Entre los ataques comunes ocasionados por código móvil, están aquellos en que se lleven *applets* maliciosos, provocando ataques de negación de servicio, invasión de privacidad o molestias (despliegues de sonidos no requeridos o imágenes obscenas). Otros son los *applets* hostiles que provocan serios ataques, como son modificaciones del sistema, causando daños significativos o irreparables.

- *Mecanismos de Seguridad*

Los sistemas de código móvil tienen dos aspectos fundamentales para el problema de seguridad, la mayoría de ellos intentan impedir que los programas hagan algo peligroso, o por lo menos de hacer algo peligroso sin preguntarle primero. Como ejemplo está *JavaScript,* que no permite que se escriban archivos en disco sin el consentimiento del usuario, en el caso de controles *ActiveX* usan firmas digitales usando *authenticode*[1].

Otro mecanismo es el denominado *stack inspection*, técnica usada por la mayoría de proveedores de *browsers* para permitir o negar accesos. Este mecanismo de

[1] Tecnología de firma digital de Microsoft que usa certificados de clave pública.

stack inspection es conocido por ejemplo en el *browser* de *Netscape* como *capabilities*, y en *Internet Explorer* como *permission scoping*.

Como recomendación, muchas organizaciones deshabilitan todo tipo de contenido ejecutable, o implementan filtros de contenido en *gateways* de seguridad.

1.3.6.2 Seguridad en correo electrónico

El correo electrónico es uno de los servicios más cruciales, tal y como lo es la comunicación vía teléfono, por lo tanto las medidas de seguridad a tomarse son de vital importancia. Los aspectos asociados con la seguridad de correo electrónico, tienen relación con el emisor, el receptor, el medio y el efecto que puede ocasionar en la red.

1.3.6.2.1 *Seguridad en protocolos de correo electrónico* [5]

SMTP (*Simple Mail Transfer Potocol*) maneja el intercambio de correo electrónico entre servidores de correo a través del Internet. En SMTP uno de los problemas de seguridad es que pasa el tráfico a través de la red sin encripción**.** Para solventar estos inconvenientes, se hablará posteriormente de protocolos para asegurar el correo electrónico, los mismos que protegen el cuerpo del mensaje, pero estas técnicas no protegen las cabeceras del mismo, por lo que se puede correr SMTP sobre SSL o TLS.

Algunas recomendaciones para el uso de SMTP son:

- Uso de las características de almacenaje y envió normales de SMTP para enviar todo el tráfico de correo a través de un *bastion host*.

- Usar filtrado de paquetes para restringir conexiones SMTP desde *host* externos hacia el *bastion host*, y desde el *bastion host* hacia servidores internos.

- Autenticación SMTP[1].

POP (*Post Office Protocol*) es un protocolo cliente – servidor que maneja la entrega de correo al usuario, desde su casillero de correo en el servidor. Las principales implicaciones de seguridad son:

- El envío de contraseñas POP sin protección sobre la red.

- La mayoría de contraseñas POP, son iguales a los nombres de usuario POP.

- Los problemas de privacidad ya que pueden estar siendo monitoreadas las sesiones POP.

Hay algunos procesos que se están considerando como es el uso de POP sobre SSL, aquí se encripta en sí la conexión, el problema es que requiere el uso de otro puerto para POP sobre SSL[2]. Otro aspecto es el uso de *proxys* comerciales que soporten POP. Para autenticación se tiene el uso de *Kerberos* llamado KPOP y APOP (*Authenticated Post Office Protocol*).

IMAP (*Internet Message Access Protocol*) usado para recuperar correos desde un servidor remoto hacia el cliente de correo en el lado del usuario, tiene mayor flexibilidad que POP, soporta múltiples casilleros para cada usuario. Las implicaciones de seguridad son: envío de contraseñas sin protección a través de la red, algunos servidores permiten el uso de contraseñas no reusables, pero no todos permiten este mecanismo de seguridad. También hay pocos servidores que soportan IMAP sobre TLS.

[1] La información se detalla en el *RFC* 2554
[2] El puerto usado en este caso es 995.

1.3.6.2.2 Problemas de seguridad en correo electrónico

Los ataques comunes a correo electrónico se basan principalmente en los siguientes aspectos:

- Entrega y ejecución de código malicioso.
- Divulgación de información sensible o propietaria tanto en el tránsito como en el almacenaje.
- El proceso de identificación es un aspecto crítico para los usuarios de correo electrónico, la autenticación de la identidad que envía es un problema para el receptor.
- El servicio de correo electrónico estándar es vulnerable a: intersección, replicación, divulgación y modificación.
- Ataques denominados "*man-in-the-middle*", pueden ocasionar pérdida de privacidad e integridad del mensaje.
- Ataques de *replay,* con el fin de enviar nuevos correos posteriores al original, pero con la misma identidad del emisor.
- Servicios de correo electrónico basados en *Web*, son considerados muy inseguros, por las vulnerabilidades e incidentes reportados.

❖ *Correo electrónico basura*

Los problemas más frecuentes con los servidores de correo son: el conocido "*spam"* y los denominados correos comerciales no solicitados, los mismos que sobrecargan la red. Los servidores de correo deberán protegerse de extraños que pueden usar el servidor para enviar correos a terceras personas, a usuarios de la

red, e incluso los mismos usuarios de la red pueden ocasionar molestias a otras personas.

❖ *Ataques que involucran código malicioso*

Son ataques directos a equipos de usuario, usualmente vienen como archivos adjuntos, los cuales, al ser ejecutados, afectan directamente al sistema o aplicaciones que corren sobre el mismo. En diversas ocasiones estos archivos no llegan como un programa ejecutable, sino en texto plano, pero utilizan las herramientas de colaboración del cliente de correo, para ejecutarse.

1.3.6.2.3 Mecanismos de Seguridad

En los siguientes párrafos se examinará diferentes formas para hacer el correo electrónico más seguro. Entre otros se comentarán protocolos para asegurar correo, salvaguardar datos transmitidos, autenticación, y medidas de seguridad en herramientas de colaboración en clientes de correo electrónico.

❖ *Autenticación de correo electrónico*

La autenticación apropiada es un aspecto importante de seguridad para correo electrónico, incluso es considerada un aspecto de confidencialidad en el caso del receptor e integridad para el emisor.

Plain Login: el nombre de usuario y la contraseña se las convierte en una cadena codificada en base-64; dada esta transformación, el nombre de usuario y la contraseña no son legibles, sin embargo con un *sniffing* de paquetes sería fácil identificar el protocolo y el método de autenticación.

Login Authentication: similar a *plain login*, con la diferencia que son pasados separadamente el nombre de usuario y la contraseña. Igualmente fácil de extraer datos y decodificarlos.

APOP (*Authenticated Post Office Protocol*): encripta la contraseña del usuario durante una sesión POP, esto lo realiza mediante una llave secreta provista desde el cliente al servidor mucho antes de iniciada la sesión POP. La fortaleza de la encripción se basa en la complejidad de la llave secreta, y con qué frecuencia se usa la misma.

Las implicaciones de seguridad en este caso son: el nombre de usuario no es el mismo que la contraseña, pero se puede crear un archivo que conserve estas contraseñas; otro aspecto es que no todos los clientes soportan APOP; finalmente, la encripción no protege el mensaje en sí.

NTLM/SPA (*Secure Password Authentication*) [1]: protocolo propietario de Microsoft, esta autenticación es provista para servidores y clientes de correo para tráfico POP3, SMTP e IMAP.

Kerberos: es un protocolo de autenticación de red para aplicaciones cliente – servidor, usa criptografía de clave secreta. No intercambia contraseñas

1.3.6.2.4 Protocolos para correo electrónico seguro [3]

Hay varios estándares y productos para asegurar el correo electrónico, algunos de los cuales se mencionan a continuación:

PEM (*Private Enhanced Mail*): es un estándar que define el uso de encripción de clave pública para asegurar el correo electrónico para su transmisión por Internet; también provee autenticación. Este estándar se implementa a nivel de capa aplicación.

Los servicios de seguridad que ofrece PEM son: autenticación de origen (usando certificados digitales X.509), confidencialidad, integridad del mensaje, no repudio del origen cuando se utiliza gestión de clave con algoritmo de clave simétrica. PEM usa una organización jerárquica para autenticación y distribución de claves, la clave es válida si está firmada por una autoridad certificadora.

El problema para que este estándar no haya sido difundido es la falta de infraestructura jerárquica de autenticación y distribución de claves.

PGP (*Pretty Good Privacy*): es una aplicación usada para encriptar correo electrónico y archivos, la encripción usada es de clave pública para garantizar confidencialidad, usa firmas digitales para autenticar la identidad del emisor, la integridad del mensaje y evitar negación de eventos. Los algoritmos que usa son[1]:

- IDEA, para cifrar con sistema de clave secreta.
- RSA, para intercambio de claves y firma digital.
- MD5, para obtener la función *hash* de la firma digital.
- ZIP, para compresión, se comprime el mensaje en llano y la firma para almacenarlo o transmitirlo.
- Base-64, permite transmitir el mensaje a todo tipo de aplicaciones correo. Convierte los octetos en caracteres imprimibles.

Secure *MIME* (S/MIME): es un estándar propuesto por RSA, por ende usa el sistema de encripción RSA; para autenticación del emisor usa certificados digitales y firmas digitales. Para garantizar integridad del mensaje usa algoritmos *hash*, y para garantizar confidencialidad usa una combinación de encripción pública y privada.

MIME *Object Security Services* (MOSS): es derivado de PEM, depende de la existencia de claves públicas y privadas para soportar los servicios de seguridad. A través de firma digital y encripción provee autenticación del emisor, integridad del mensaje, y confidencialidad.

MSP (*Message Security Protocol*): es de uso militar, provee recibos firmados para evitar la negación de eventos y prueba de entrega.

[1] Los algoritmos mencionados son para la versión PGP 2.6.3i.

❖ *Recomendaciones en uso de clientes de correo*

- Mientras más facilidades ofrece el cliente de correo, más inseguro se torna, por ende es necesario configurarlo con restricciones para que se ejecute código adjunto.

- Actualizar las versiones tanto del cliente como del servidor de correo para evitar ataques directos a vulnerabilidades de los mismos.

- Herramientas o programas para revisión de correo con virus adjunto.

- Uso de *proxy* para correo electrónico, usualmente ubicado en una zona desmilitarizada.

- Respaldos frecuentes, minimizarán el impacto si llega a ocurrir un ataque.

1.3.6.3 Seguridad en servicio DNS [1]

El servicio DNS está compuesto de servidores de nombre, *resolvers*[1], y protocolos de comunicación. Juntos crean el servicio de directorio distribuido en Internet que es capaz de traducir entre direcciones IP y nombres de *hosts*. Los principales problemas de seguridad se relacionan con las transacciones (peticiones y respuestas) hechas por o hacia el servidor.

1.3.6.3.1 Ataques al servicio DNS

DNS *spoofing*: el atacante observa la petición hecha al servidor DNS e inmediatamente responde antes que el mismo, redirecciona la petición a otro *site*, llevando todo el tráfico hacia el atacante.

[1] Biblioteca de rutinas llamadas por procesos de red.

Cache poisoning: las entradas de datos han sido maliciosamente modificadas en el servidor, el usuario sin embargo sigue confiado que son verdaderas sus respuestas.

Preguntas maliciosas al DNS: los servidores DNS también son atacados con preguntas maliciosas (por ejemplo, nombres demasiado largos de *host*), ocasionando problemas con *buffer overflows*, incluso podrían ejecutar código hostil.

Errores de configuración: entre los problemas generados por estos errores, se tienen por ejemplo, ataques de negación de servicio, una muestra de esto se da cuando se modifica los registros, y cierta petición es redireccionada a otro rango de direcciones no existente, y si alguien trata de resolver el domino, el resultado será que no existe generando un ataque de DoS (*Denial of Sevice*).

Además, la gran cantidad de información que suelen tener los servidores DNS, puede ser aprovechada por los atacantes, ya que en la mayoría de los casos, contiene información de otros equipos de la red.

1.3.6.3.2 Mecanismos de seguridad

Para hablar de seguridad del DNS, no se puede asumir que el sistema es seguro, la seguridad implica que el sistema esté diseñado, y configurado apropiadamente.

Split DNS*:* divide la red en zonas alcanzables internamente o externamente, un servidor interno recibe las peticiones de usuarios, y éste a su vez envía a uno externo, que hace las peticiones en representación del interno, es una de las maneras de proteger contra vulnerabilidades de la aplicación como son *buffer overflows*.

Split-Split DNS*:* como se muestra en la figura 1-8, usa separación física, que es capaz de deshabilitar peticiones hechas desde la Internet hacia servidores de

nombre que sirven a la red interna, ofrece protección contra ataques como *cache poisoning*.

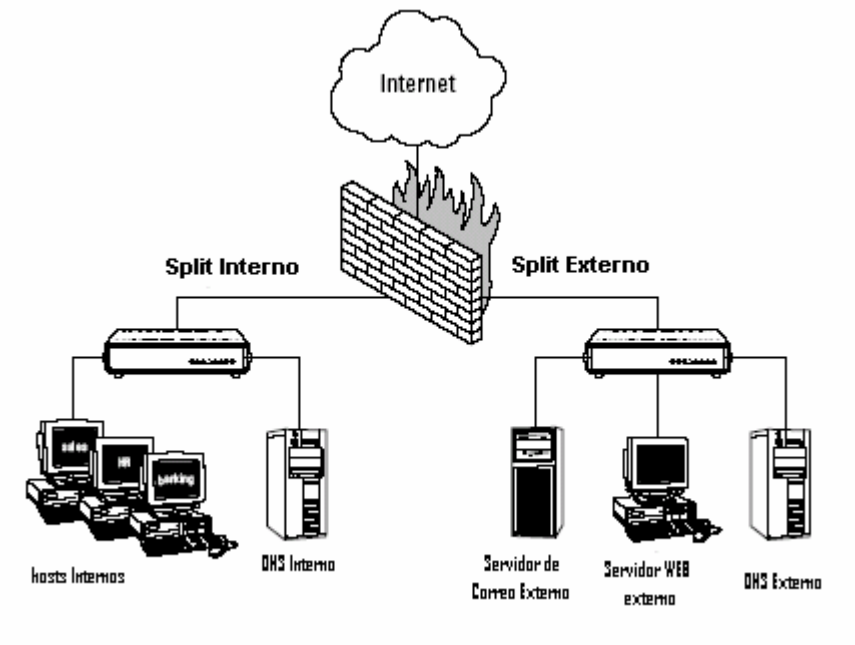


Figura 1- 8: *Split-Split* DNS [3]

Master Slave DNS: la necesidad de redundancia y balanceo de carga hace que varias redes incrementen el número de servidores de nombre, lo que hace que la administración de los mismos sea más compleja. La solución, es tener solo un servidor como maestro donde las configuraciones y actualizaciones hechas a éste obviamente se notificarán a los esclavos.

TSIG (*transaction signatures*)[1]: utiliza un secreto compartido, una función *hash* (HMAC-MD5) de una sola vía para autenticar mensajes tales como respuestas y actualizaciones. Las ventajas de esta opción es que es simple de configurar, lo suficientemente flexible como para asegurar mensajes DNS, zonas de transferencia y actualizaciones automáticas.

Firewall de filtrado de paquetes: se configura el *firewall* usualmente permitiendo tráfico selectivo entre *hosts* en la Internet y *host* internos. Incluso se puede configurar de tal manera que los servidores de nombre de la organización hagan peticiones a servidores en la Internet pero no viceversa.

[1] Este mecanismo se explica más detallado en el *RFC* 2845

Extensiones de seguridad DNS[1]: usa criptografía de clave pública, y permite a los administradores de la zona firmar digitalmente los datos de la misma.

Recomendaciones: entre las políticas a implantarse están; que tanto el sistema operativo como el software del servidor DNS, se mantengan con los parches y *releases* al día. Otra opción es un HIDS (detector de intrusos a nivel de *host*), instalado en el servidor, y monitoreo constante.

1.3.6.4 Seguridad en servicio de transferencia de archivos

FTP (*File Transfer Protocol*) es un estándar de facto para la transferencia de archivos sobre Internet, existen algunos protocolos especializados para aplicaciones donde FTP no es conveniente, por ejemplo, se tiene TFTP usado para transferir configuraciones de ciertos dispositivos.

1.3.6.4.1 Ataques al servicio de transferencia de archivos

- Ataques por fuerza bruta, para obtener usuario y contraseña de tal manera que permitan ganar acceso directo al servidor.

- Ataque FTP *bounce*: *port-scanning y exploit payload delivery,* busca puertos abiertos en *hosts* clientes de FTP, o sube datos que se encargarán de buscar vulnerabilidades en el servidor FTP, (ver figura 1-9).

Figura 1- 9: FTP *bounce* [5]

[1] Se menciona más detalladamente en el *RFC* 2535

- Ataques usando comandos FTP como PORT[1] y PASV[2] para evadir la protección de filtros *stateful*[3], engañan al *firewall* y envían datos a través de puertos altos que supuestamente están abiertos para enviar datos al cliente FTP.

- Manipulación de procesos, incluye ataques de desbordamiento de *buffer*.

1.3.6.4.2 Mecanismos de seguridad

- No proveer accesos *anonymous* FTP, especialmente acceso a directorios que puedan escribirse.

- Evitar el uso del servidor FTP para distribuir datos de otras personas.

- Evitar correr servicios públicos como *Web* o correo electrónico en el mismo servidor FTP.

- Si se ofrece acceso público al servidor FTP, se debe asegurar que el *firewall* esté con los últimos parches.

- Si se desea permitir un FTP entrante, se debe usar filtros de paquetes que solo permitan FTP entrante del *bastion host*.

- Si el cliente FTP maneja conexiones en modo pasivo, entonces se permite que *hosts* internos se contacten con servidores FTP externos, mediante filtrado de paquetes, esto es seguro sólo si el filtro de paquetes permite filtrar en el *bit* TCP ACK que solo permita conexiones TCP salientes de puertos sobre 1023, hacia puertos 1023.

[1] Comando que define un puerto alto dinámico para que el cliente *FTP* reciba los datos.
[2] Comando generado por el cliente, para que el servidor asigne el puerto por el que el servidor entregará datos al cliente *FTP*.
[3] Filtrado a nivel de capas superiores (aplicación)

- Se puede proveer acceso por filtrado de paquetes y *proxys*, soportando modo pasivo para filtrado de paquetes[1] y modo normal para *proxys*[2].

- Recomendar a los usuarios a usar *web browsers* como clientes FTP, con el fin de obtener características actualizadas sobre FTP.

1.3.6.5 Seguridad en Acceso Remoto

Entre las principales herramientas (protocolos y aplicaciones) para acceso remoto se tiene las siguientes: SSH, *Telnet*, *Microsoft Terminal Services*, entre otros. Los atacantes tratan de acceder al *host*, que permite acceso remoto, tratando de aprovechar hoyos de seguridad en el servicio.

1.3.6.5.1 Ataques al servicio de acceso remoto

Fuga de información, ya sea del usuario o sistema, manipulación de procesos (desbordamiento de *buffers*) y mecanismos como fuerza bruta, para obtener usuario y contraseña, de tal forma que ganen acceso directo al sistema.

- *Telnet*: el principal problema es la falta de seguridad al transmitir usuario y contraseña que van en texto plano. Entre los ataques comunes se tiene:

  - *Telnet Service Fingerprinting*, usualmente se usan herramientas como *telnetfp*, para obtener cierta información sobre el servicio que está corriendo.

  - *Telnet Brute-Force Password-Grinding*, este ataque obtiene usuarios y contraseñas para así acceder al equipo remoto. La mayoría de veces los administradores dejan los equipos con usuarios y contraseñas por defecto.

[1] Las conexiones se abrirán desde el interior, por el cliente.
[2] En este caso el cliente *FTP* estará protegido de conexiones *TCP* entrantes por el canal de datos ya que solo permitirá que estas ocurran desde el *proxy*.

- SSH: se crea para proveer acceso encriptado a *hosts* basados en *Unix*, existen también servidores para *Windows NT*. SSH, está extendido en casi todas las plataformas. Entre los ataques comunes se tiene:

  - SSH *Fingerprinting*, algunos administradores de red para protegerse de este ataque modifican el *banner ssh*, para presentar información falsa al atacante.

  - SSH *Brute-Force Password Grinding*, si bien *ssh* es muy resistente a este tipo de ataques, se han creado herramientas como *guess-who* desarrollada por *Sebastian Krahmer*.

  - Vulnerabilidades SSH, entre las conocidas están: SSH1 CRC32 *compensation vulnerability*, SSH1 CRC32 *compensation exploit*.

  - La capacidad de manejar *Port forwarding*[1], se convierte en un peligro ya que puede levantar conexiones externas a otros servicios, pasando por alto el *firewall*.

- Interfaces gráficas para acceso remoto: por ejemplo se tiene *Microsoft Remote Desktop Protocol*, conocido como servicio de terminal para *Microsoft*, entre los ataques que puede enfrentar son:

  - RDP *Brute-Force Password Grinding*, después de un escaneo de puertos y verificar que el servicio está arriba, el atacante usará por ejemplo la herramienta *tsgrinder*[2], creada por *Tim Mullen* para empezar a adivinar usuarios y contraseñas.

  - Vulnerabilidades RDP, entre las más conocidas tenemos: CVE-2000-1149 y CAN-2002-0863 [13].

[1] *Port Forwarding*: permite correr otros protocolos a través de una conexión ssh.
[2] http://www.hammerofgod.com

1.3.6.5.2 Mecanismos de seguridad

- Es preferible no usar *Telnet* para administración remota, si el sistema ofrece otras opciones.

- *Telnet* saliente, se lo usa de forma segura al aplicar filtrado de paquetes a través de un p*roxy*.

- Si el administrador o usuario sabe de la sensibilidad de los datos a cruzar por la sesión *Telnet*, usar alguna versión de *Telnet* encriptado.

- Permitir solo conexiones SSH entrantes hacia servidores que están bajo su control.

- Preferentemente tener la opción *port forwarding* deshabilitada.

- Se deberán permitir conexiones salientes de *ssh* para clientes que estén bajo control.

- Dado que las conexiones mediante RDP, son altamente inseguras es mejor usar VPNs para administración remota.

- Para evitar la mayoría de ataques por fuerza bruta para averiguar contraseñas, es necesario manejar una buena política de contraseñas.

- No correr *r-services* (*rsh*, *rexec*, or *rlogin*), ya que son altamente vulnerables a ataques de *spoofing*, la autenticación es muy débil a más de viajar en texto plano.

- En ambientes inseguros es mejor usar por ejemplo, servicios *Citrix* con encripción SSL, para prevenir ataques de *sniffing* y *hijacking*.

1.4 FUNDAMENTOS DE QOS (QUALITY OF SERVICE) EN INTERNET [14]

1.4.1 INTRODUCCIÓN

Calidad de servicio se define como la medida de rendimiento para un sistema de transmisión, que refleja su calidad de transmisión y disponibilidad de servicio.

La calidad de servicio va más allá de añadir mecanismos como: políticas de tráfico, clasificación y planificación, fundamentalmente significaba desarrollar nuevos servicios sobre Internet. Además el término calidad de servicio se lo ha usado ampliamente en la comunidad de *networking*, para definir un conjunto de características de desempeño como son: retardo, *jitter*, tasa de bits errados, pérdida de paquetes, etc.

Los diferentes requerimientos de diversas aplicaciones que cursan por la Internet, para lo cual no fue diseñada la misma[1], hacen que se susciten problemas como: confianza en el desempeño y diferenciación de servicio. Las aplicaciones en tiempo real, requieren niveles mínimos de recursos para poder operar efectivamente.

La diferenciación de servicios es de vital importancia, ya que la Internet trata a todos los paquetes de la misma manera, no se considera que los requerimientos van a variar, por ejemplo, ciertas aplicaciones como sistemas de telefonía IP y video conferencia necesitan más ancho de banda que aplicaciones que se han usado a lo largo de los años como son: WWW, FTP o *Telnet*. Se puede hacer una distinción entre estos dos esquemas, un ejemplo es que las primeras aplicaciones pueden soportar paquetes perdidos, pero son sensibles al retardo, lo que no ocurre con el segundo rango de aplicaciones que no toleran pérdidas de paquetes pero no son muy sensibles a retardos [15].

[1] "Sigue un modelo datagrama que no tiene la capacidad de administrar recursos y menos garantizar recursos a los usuarios" [16].

Calidad de servicio usualmente se refiere a proveer reserva de recursos y diferenciación de servicios, para esto se han desarrollado arquitecturas y mecanismos para cubrir dos necesidades básicas de la Internet que son: asignación de recursos y optimización del rendimiento.

1.4.2 ASIGNACIÓN DE RECURSOS [16]

La Internet no puede soportar todas las demandas de tráfico, por lo que los paquetes pueden ser retardados o desechados. Una red que soporta QoS toma un rol activo en el proceso de asignación de recursos, en donde se decide quién obtiene recursos y a la vez cuántos. Se mencionan dos arquitecturas desarrolladas para asignación de recursos son: Servicios Integrados y Servicios Diferenciados.

1.4.2.1 Servicios Integrados [14]

Se basa en reservación de recursos por flujo, la aplicación deberá hacer la reservación antes de comenzar a enviar datos a través de la red. Los pasos a seguirse son los siguientes:

- La aplicación debe particularizar la fuente del tráfico y los requerimientos del recurso.

- Después se usa un protocolo de enrutamiento para encontrar un camino basado en los requerimientos ya estipulados.

- El protocolo de reservación es el encargado de instalar el estado de la misma a lo largo del camino.

- En cada salto se verifica si existen los suficientes recursos para la nueva reservación.

- Una vez hecha la reservación se inicia la transferencia de los datos sobre el camino reservado.

La reservación de recursos se basa en la clasificación de paquetes y mecanismos de *scheduling*, aplicados a elementos de la red, como son los enrutadores. *Intserv* se diseñó para aplicaciones con requerimientos bajos en ancho de banda y bajo retardo.

1.4.2.1.1 Clasificación de aplicaciones

- *Aplicaciones Elásticas*: Son flexibles en los requerimientos de QoS, y pueden operar sobre un rango de ciertos parámetros como: *data rates*, limites de retardo y tasa de pérdida. Entre estas aplicaciones se encuentran *Telnet*, *ftp*, *Web browsing* y *Net news*.

- *Aplicaciones en tiempo real tolerantes*: aplicaciones como audio conferencia, video *streaming*, son muy sensibles al retardo, aunque soportarían retardo moderado extremo a extremo, requieren alto *throughput* y muy baja tasa de error.

- *Aplicaciones en tiempo real intolerantes*: este tipo de aplicaciones demandan mayores requerimientos de QoS. Necesitan precisión en ancho de banda, retardo y *jitter*, telefonía IP es un ejemplo de este tipo.

1.4.2.1.2 Clases de servicio

- *Servicio garantizado*: permite a la aplicación reservación de ancho de banda, suministra fronteras en *throughput*, además de topes máximos en retardos de paquetes, a través de un estricto control de admisión y *fair queuing scheduling*, entonces el paquete llegará con un retardo preestablecido, se calcula el retardo máximo en cada salto y es el que se garantiza. Se diseñó para aplicaciones en tiempo real intolerantes al retardo como telefonía IP, en redes bajo medio compartido es difícil implementar esta clase de servicio.

- *Servicio de control de carga*: la idea básica es proveer las mismas facilidades que presenta una red sin carga, este servicio se diseñó para aplicaciones en tiempo real tolerantes, que requieren una cantidad suficiente de ancho de banda y ocasionalmente toleran pérdidas y retardo. Estas aplicaciones se ejecutan bien cuando la red ligeramente se carga pero se degradan rápidamente si la red incrementa la carga. Como solo una cantidad limitada de ancho de banda es reservada, si hay paquetes adicionales, la entrega será usando la técnica del mejor esfuerzo.

1.4.2.1.3 Control de admisión

Implementa el algoritmo de decisión [17], que un enrutador o un *host* usan para determinar si la petición de un nuevo flujo de datos sobre la red es admitida sin causar desestabilización en el flujo de datos actual. Este control de admisión se hace localmente en cada nodo.

1.4.2.1.4 Identificación de flujos

Con el objeto de proveer diferentes grados de servicio, los paquetes pueden ser marcados con diferentes códigos para así recibir cierto tipo de tratamiento.

En IPv4 se hace por:

- Dirección IP de origen
- Puerto de origen
- Dirección IP de destino
- Puerto de destino
- Protocolo de transporte utilizado (TCP o UDP)

En IPv6 la identificación puede hacerse como en IPv4 o alternativamente usando el campo ‘etiqueta de flujo’ en vez de los números de puertos. Aún no hay ninguna implementación de RSVP que utilice la etiqueta de flujo.

1.4.2.1.5 Packet scheduling

Packet scheduling es responsable de asegurar que los flujos identificados por la clasificación de paquetes reciban las garantías de calidad de servicio negociadas, además de ejecutar una reserva equitativa de recursos. La manera más simple de ver esto es como un mecanismo de encolamiento de alto nivel.

- *Objetivos de scheduling:*

  - Compartición del ancho de banda
  - Compromiso con las garantías de ancho de banda (mínimo y máximo), pérdida de paquetes, y retardo.
  - Reducción de las variaciones del retardo.

- *Técnicas de scheduling:*

  - *First come first serve* (FCFS): los paquetes son encolados en un *buffer* común y despachados así como van llegando (ver figura 1-10), usar este esquema tiene mayores limitaciones para ofrecer QoS. No ofrece aislamiento de tráfico, y sin esto es muy difícil garantizar un tope en cuanto a retardo; lo mismo ocurre con el ancho de banda. También no hay distinción de paquetes, por ende no hay flujos diferentes que es una de las maneras de garantizar parámetros solicitados por las aplicaciones.

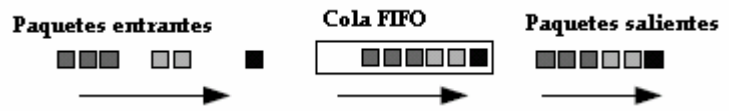


Figura 1- 10: *First come first serve* [6]

- *Encolamiento prioritario*: permite definir cuatro colas para el tráfico de la red, estas colas son: de prioridad alta, media, normal y baja. Si hay paquetes en la cola de alta prioridad, ésta es procesada hasta que quede vacía, independientemente del estado de las otras colas. Las tres primeras colas con prioridades deberán quedar vacías, para despachar un simple paquete que esté en la cola de baja prioridad, como lo muestra la figura 1-11.

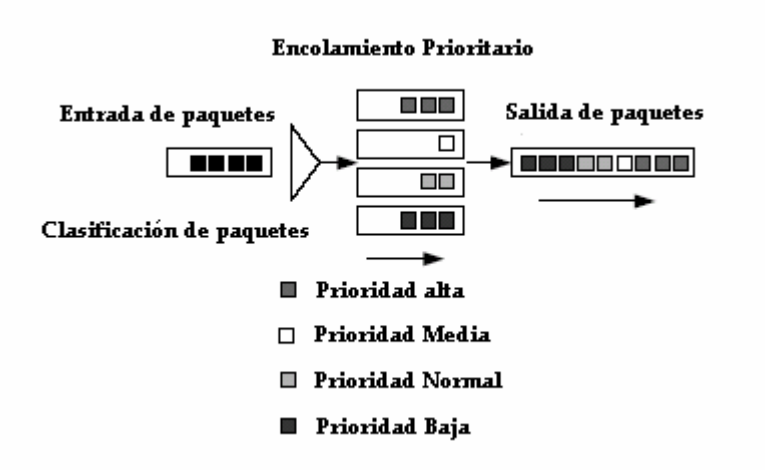


Figura 1- 11: Encolamiento prioritario [6]

- *Generalized Processor Sharing* (GPS)*:* asume que cada flujo se mantiene en una cola lógica separada, sirve una cantidad infinitesimal de cada cola, se le asocia además un peso y se la puede servir por su peso también. Si una cola está vacía entonces se toma estos recursos para servir a otra.

- *Round Robin* (RR)*:* es una implementación de GPS, un paquete reemplaza la cantidad infinitesimal mencionada, mantiene una cola por cada flujo, cada paquete entrante es puesto en una cola apropiada y se va tomando un paquete de cada cola, las colas vacías son saltadas y se continúa con la siguiente, sin embargo surge el problema de tener paquetes de distintos tamaños, como ocurre en Internet, entonces la cola de paquetes grandes es la que

se llevará la mayoría del ancho de banda, y aumentará el retardo para colas con paquetes pequeños.

- *Weighted Round Robin*: es una simple modificación de RR, aquí se sirve *n* paquetes por turno, *n* se ajusta para reservar una fracción específica de ancho de banda del enlace. A la cola se le asigna un peso, el número de paquetes servidos estará en función del peso y de la capacidad del enlace. El problema de paquetes con tamaño variable persiste.

- *Deficit Round Robin:* mejora a WRR, ya que puede servir a paquetes de diferentes tamaños; para esto utiliza una variable que será inicializada con un número de bits para servir en una cola, si el paquete es menor o igual al tamaño de la variable, entonces será servido, si es mayor se le deja para la siguiente ronda donde el valor de la variable aumentará.

- *Weighted Fair Queuing*: está diseñado para paquetes de tamaño variable, cada paquete es etiquetado con un valor identificativo, teóricamente es el tiempo en que el último *bit* sería transmitido. Cada vez que el enlace está disponible para enviar un paquete, aquel con el valor de etiqueta más bajo es el que será seleccionado.

1.4.2.1.6 Problemas de IntServ

- La razón principal fueron problemas de escalabilidad debidos a la necesidad de mantener información de estado en cada enrutador. Esto hace no viable usar RSVP en redes grandes, por ejemplo en el '*core'* de Internet.

- Los fabricantes de enrutadores no han desarrollado implementaciones eficientes de RSVP, debido al elevado costo que tiene implementar en hardware las funciones de mantenimiento de la información de estado.

- Los *overheads* que se obtienen al hacer una reservación por cada sesión definitivamente son demasiado altos.

- Para soportar reservación por flujo, implica que cada nodo en la red debe tener implementados mecanismos de clasificación y *scheduling*, estos mecanismos no estarían lo suficientemente disponibles para un gran número de flujos y a altas velocidades, como ocurre en Internet.

- Reservación de recursos requiere el soporte de *accounting* y acuerdos entre diferentes proveedores de servicios.

- Como recomendación para esta arquitectura, se la puede ejecutar en redes corporativas.

1.4.2.1.7 Protocolo de Reservación de Recursos

Reservation Setup Protocol (RSVP) fue estandarizado a causa de requerimientos de las aplicaciones para asegurar la reservación de recursos a lo largo de camino, por ende un protocolo de señalización es necesario.

RSVP lleva peticiones sobre reservación de recursos a través de la red como son: especificaciones de tráfico y QoS, disponibilidad de recursos en la red, etc. Trabaja en conjunto con mecanismos de encolamiento.

- *Características de RSVP* [14]

Entre las más importantes se tiene:

  - Protocolo simple: soporta una gran cantidad de métodos de comunicación.

- Independiente del protocolo de enrutamiento: hace uso de protocolos ya existentes en el Internet.

- Refresco flexible del estado: por ejemplo en cambio de enrutamiento, fallas en el enlace, etc.

¿Cómo trabaja RSVP?

Hosts y enrutadores usan RSVP para entregar peticiones sobre QoS hacia los enrutadores a lo largo del camino, además para mantener el estado especialmente de ancho de banda y retardo. Un *host* usa RSVP para solicitar un servicio específico de QoS, en nombre del flujo de datos de la aplicación. El protocolo RSVP lleva la petición a través de la red, visitando cada nodo que usa la red, donde intenta hacer la reservación de recursos usando su propio módulo de admisión de control, el cual le indicará si hay en el nodo recursos suficientes para satisfacer las necesidades de la petición de QoS, si no hay recursos disponibles se retorna un error hacia la aplicación que solicitó ciertos parámetros de calidad.

❖ *Estilos de reservación*

RSVP soporta algunos estilos de reservación, los mismos que determinan la manera de fijar en los enrutadores los requerimientos de recursos solicitados, entre los más importantes se tiene:

- *Wildcard*: usa una especie de filtro que no identifica la fuente, en los enrutadores no se suma los valores de ancho de banda de todas las peticiones, sino toman el mayor valor de las peticiones generadas; esto permite, que una sola asignación de recursos sea hecha a través de las trayectorias. Este método es conveniente para sesiones *multicast*, aplicaciones como audio conferencia, donde en la mayoría de ocasiones, un pequeño número de fuentes está activo simultáneamente y puede compartir la asignación de recursos.

- *Fixed - filter*: el filtro aquí selecciona fuentes en particular, un receptor escoge, de qué fuentes recibir las peticiones de reservación. Para cambiar las especificaciones del filtro se tiene que re-invocar el control de admisión. Este mecanismo es conveniente para aplicaciones como video conferencia, donde una ventana es requerida por cada transmisor y todas estas ventanas necesitan ser actualizadas simultáneamente.

- *Dynamic – filter*: permite al receptor modificar las fuentes que escoge sin necesidad de re-invocar un control de admisión; sin embargo requiere que estén asignados recursos suficientes para manejar el peor de los casos, cuando todos los receptores tomen como entrada diferentes fuentes.

❖ *Mensajes RSVP* [14]

RSVP tiene dos mensajes principales; PATH y RESV.

- PATH: la fuente es la que transmite este mensaje, lleva la siguiente información:

  - Dirección origen, número de puerto, que permite identificar flujos del remitente de otros flujos RSVP.

  - Características de tráfico del flujo de datos, (TSpec).

  - Especificaciones del tipo de servicios que pueden ofrecer los equipos de la red, y la cantidad de recursos de QoS disponibles, (AdSpec).

- RESV: es generado por el receptor, contiene una petición de recursos a ser reservados. Son enviados en forma reversa por el camino que vino el mensaje PATH. La petición de reservación de recursos, es expresada por *filter specification* (define el paquete en el flujo que

recibirá una clase específica de servicio) y *flow specification* (es usada por *packet schedule*).

❖ *Problemas RSVP*

- Complejidad en los enrutadores, ya que necesitarán manejar clasificación de paquetes, *packet scheduling*, módulos de control de admisión, lo que disminuye la velocidad de procesamiento de los mismos.

- Si por el *backbone* cruzan una gran cantidad de flujos, ocasionará saturación en los enrutadores de *core*.
- Otro aspecto importante es el establecimiento de políticas de control, ya que no se conoce quién debe realizar la reservación, y por ende tener el control de los recursos, los ISPs podrían tener un remitente autorizado y un receptor haciendo las peticiones, de tal manera que se pueda cobrar por los recursos utilizados al usuario.

1.4.2.2 Servicios Diferenciados

Los servicios diferenciados proveen QoS, basados en las necesidades de un grupo de usuarios, en lugar de flujos de tráfico. El usuario marca los paquetes con un determinado nivel de prioridad; los enrutadores van agregando las demandas de los usuarios y propagándolas por el trayecto. Es un modelo multiservicio, que puede satisfacer diferentes requerimientos de QoS. La red trata de entregar un tipo particular de servicio; para esto hay especificaciones de QoS en cada paquete. La red usa las especificaciones de QoS para clasificar, marcar, modelar, y establecer políticas de tráfico, y después ejecutar el encolamiento.

El enrutador de ingreso es el que normalmente se encarga de clasificar el tráfico. Dependiendo del modelo particular de *DiffServ* los paquetes pueden ser rechazados o marcados con un nivel diferente de prioridad.

En *DiffServ* no hay reserva de recursos por flujo, no hay protocolo de señalización, no hay información de estado en los enrutadores. Las propiedades de escalabilidad se logran alcanzar mediante el marcado de la cabecera de cada paquete, con uno de los *code points* estandarizados.

1.4.2.2.1 Arquitectura

Se basa en un modelo, donde el tráfico entrante es clasificado y posiblemente condicionado en los límites de la red, y asignado a diferentes conjuntos de paquetes con la misma conducta, ésta será identificada por un *codepoint* DS. En los *enrutadores* internos, los paquetes serán tratados usando el comportamiento por salto (*Per-Hop-Behavior*) asociada al *codepoint* DS.

- *Dominio DiffServ*

Es un conjunto contiguo de nodos DS, siendo éstos de frontera o periféricos, e internos como se muestra en la figura 1-12.

Nodos Límite y Nodos Interiores: deben poder aplicar el PHB[1] apropiado a los paquetes basados en DS *codepoint*.

[1] Más adelante se definirá este término.

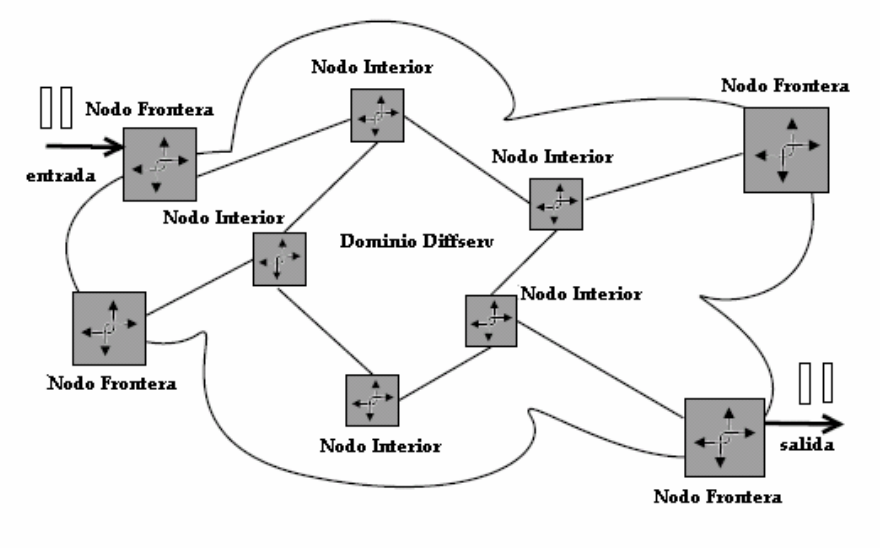


Figura 1- 12: Dominio *DiffServ* [6]

❖ *Región DiffServ*

Es un conjunto de uno o más dominios *DiffServ* contiguos. Son capaces de soportar servicios diferenciados a lo largo del camino.

❖ *Clasificación y acondicionamiento de tráfico*

La clasificación de tráfico identifica el subconjunto de tráfico que puede recibir servicio diferenciados por el condicionamiento del *codepoint* DS dentro del dominio DS.

El acondicionamiento de tráfico ejecuta mediciones, *shaping*, *policing* y re-marcado, para asegurar que el tráfico entrante al dominio DS está conforme a las reglas especificadas en el TCA (*Traffic Conditioning Agreement*).

- Clasificadores: seleccionan paquetes en un flujo de tráfico, basados en el contenido de una porción de la cabecera del paquete, se tienen dos tipos: clasificación *Behavior Aggregate*[1] y *Multi-Field*[1]

[1] Basado solo en el Codepoint DS.

- Acondicionadores de tráfico

  - Métricas (*Meters*)
  - Marcadores (*Markers*)
  - Modeladores (*Shapers*)
  - Descartador (*Dropper*)

- *Per-Hop-Behavior*: PHB es la medida con la cuál un nodo asigna recursos hacia un conjunto de paquetes. El modelo *DiffServ* define el comportamiento de los paquetes en cada salto, denominado PHB, el cual se combina con una gran cantidad de políticas en los enrutadores límite, para así proveer un rango de servicios.

  Por ejemplo PHB podría especificar que una clase de tráfico siempre reciba una prioridad estricta por encima de otras clases. *DiffServ* no estandariza ninguna disciplina de encolamiento, se puede usar por ejemplo encolamiento prioritario, WFQ, o cualquiera siempre que la conducta sea tal como lo especifica PHB.

- *Per - Domain Behavior*[2]: describe el comportamiento experimentado por los paquetes cuando pasan a través de un dominio *DiffServ*. Se usan métricas especificas para cuantificar el tratamiento que los paquetes con un DSCP particular esperan recibir, estas métricas resultarían convenientes si se habla de SLAs entre dominios.

- ToS (*Type of Service*) en IPv4 existe un campo de ToS, como se muestra en la figura 1-13, los 4 bits para ToS pueden ser interpretados de diferentes formas en los enrutadores, algunos enrutadores que no lo soportan, simplemente ignoran este campo.

---

[1] Se basan en un valor que se obtiene de la combinación de uno o más campos de la cabecera como dirección origen o destino al igual que el puerto.
[2] Este mecanismo se detalla en el *RFC* 3086

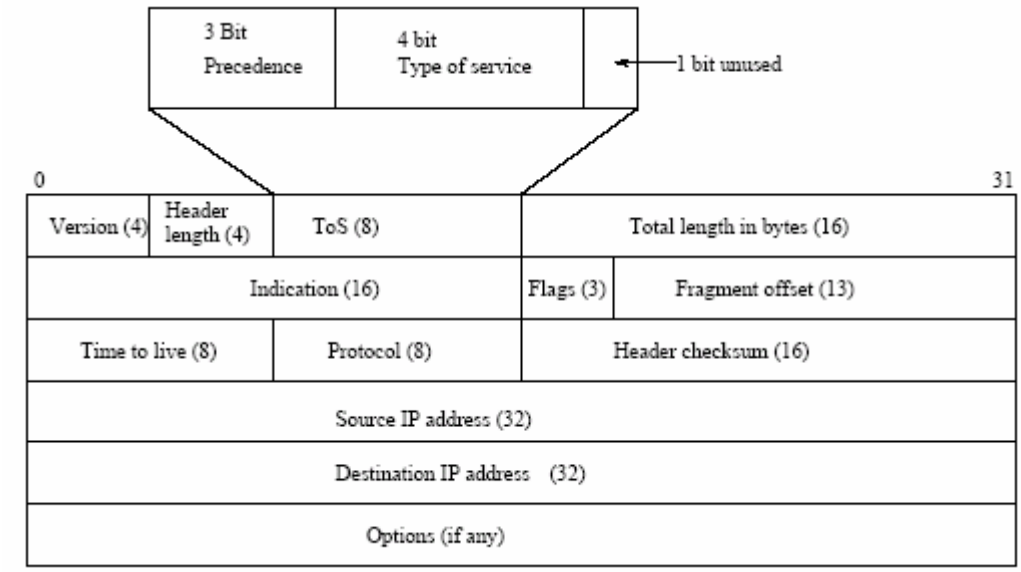


Figura 1- 13: Cabecera del paquete IPv4 [6]

- *DiffServ Codepoint*: *DiffServ* trata de facilitar el viaje de los paquetes a través de la red, en el caso de paquetes marcados con un DSCP (*Differentiated Services CodePoint*) específico, el comportamiento se reflejará en cada salto. El grupo de trabajo *DiffServ* ha estandarizado la definición y uso del campo ToS, ahora usa este campo con el *byte* DS para marcar paquetes con diferentes códigos, (ver figura 1-14).

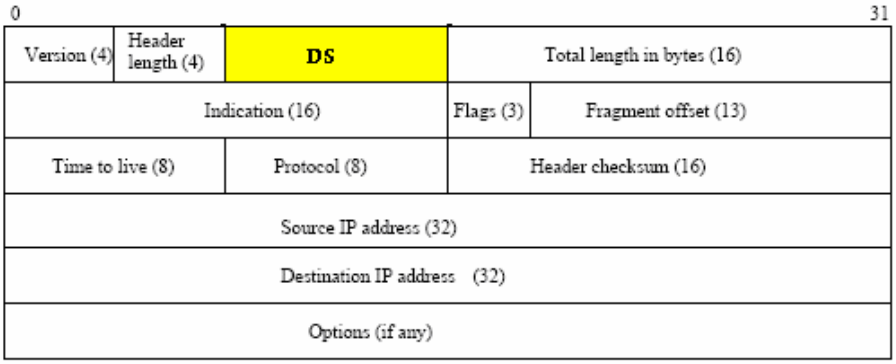


Figura 1- 14: Modificación de campo ToS por DS [6]

Codepoint Space	*Assignment*
xxxxx0	Standard action
xxxx11	Experimental/local action
xxxx01	Experimental/local action (subject to standardization)
000000	Best-effort forwarding
xxx000	For IP precedence compatibility

Figura 1- 15: *CodePoint Diffserv* [6]

El campo DS tiene los siguientes componentes:

- DSCP: *Differentiated Services CodePoint*. Se compone de seis *bits* que indican el tratamiento que debe recibir este paquete en los enrutadores.

- CU: *Currently Unused* (reservado). Este campo se utiliza actualmente para control de congestión.

Tipos de servicio en *DiffServ*:

- *Expedited Forwarding o Premium*[1]: es el que da más garantías, equivale a una línea dedicada, garantiza caudal, tasa de pérdidas, retardo y *jitter*, valor 101110 en DSCP.

- *Assured Forwarding*[2]: asegura un trato preferente, pero sin fijar garantías (no hay SLA), se definen cuatro clases y en cada una, tres niveles de descarte de paquetes.

- *Best Effort* con prioridad: sin garantías, pero obtendrá trato preferente frente a '*best effort*' sin prioridad.

- *Best Effort* sin prioridad: ninguna garantía.

[1] Mecanismo descrito en el *RFC* 2598
[2] Mecanismo descrito en el *RFC* 2597

1.4.2.2.2 Diffserv en enrutadores

En un enrutador que trabaja con el modelo *DiffServ* se tienen los siguientes pasos a seguir, como se muestra en la figura 1-16.

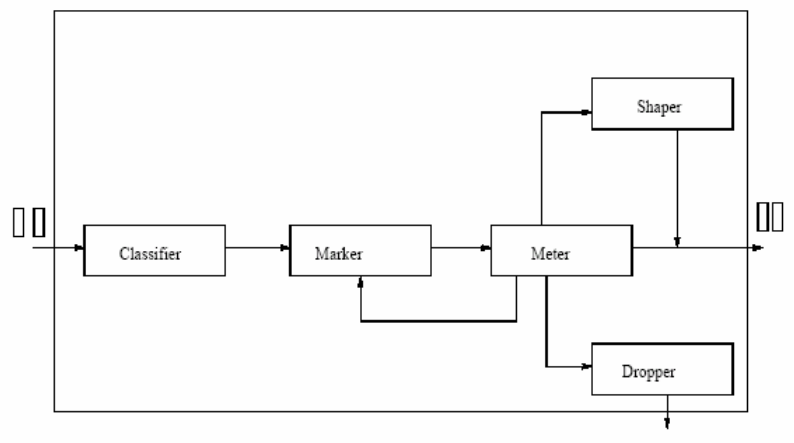


Figura 1- 16: Modelo de *DiffServ* en enrutadores [6]

Clasificador: el paquete recibido por un enrutador *DiffServ*, es clasificado en base a valores de uno o más campos de la cabecera del paquete.

Marcador: una vez hecha la clasificación se procede al marcado, el trabajo de éste es insertar el valor correcto de DSCP en el *byte* DS para que el paquete reciba un servicio correcto en los enrutadores posteriores. Una vez que el paquete ha sido marcado, los enrutadores de *core* o interiores ejecutan la clasificación BA (*Behavior Aggregate*).

Métrica: es usado para comparar el flujo entrante con el perfil de tráfico negociado, si hubiere paquetes que no cumplan con el perfil son enviados al modelador y al descartador o remarcar el paquete con un servicio menor.

- *Encolamiento en enrutadores*: se tiene los siguientes mecanismos:

  - Priority Queuing
  - Weighted Fair Queuing

- FWFQ

Modelador: este módulo introduce algo de retardo con el objeto de llevar el flujo conforme al perfil negociado. Usualmente tienen *buffers* limitados si llegara a haber paquetes que no encajan en los mismos, podrían ser descartados.

Descartador: Es el descarte de paquetes por no encontrarse en el perfil indicado.

La combinación de estos mecanismos es lo que hace la red *DiffServ* escalable; se tiene QoS garantizado, que se alcanza por el uso de DSCPs diferentes por flujos separados y el uso de mecanismos de *shaping* y *policing traffic*.

1.4.2.2.3 Problemas con DiffServ

- El servicio puede ser fácilmente robado en redes *DiffServ*, con simplemente marcar la cabecera paquete con un código DSCP apropiado.

- No hay control de admisión dinámico.

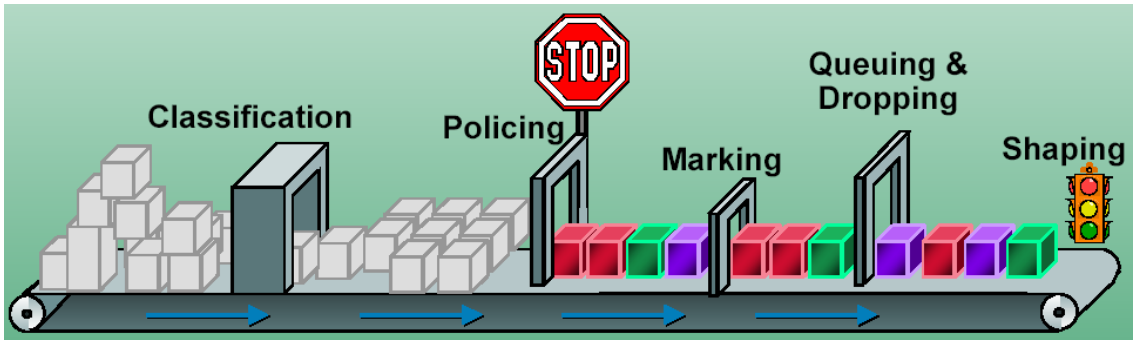


Figura 1- 17: Tratamiento de los paquetes en enrutadores con *DiffServ* [6]

1.4.3 OPTIMIZACIÓN DE DESEMPEÑO

Se refiere a como organizar los recursos en una red de la manera más eficiente para maximizar la probabilidad de entregar los compromisos acordados en cuanto

a recursos, y minimizar los costos de la entrega de los mismos. Para administrar el rendimiento en una red es necesario tener un control específico sobre el camino que atraviesa el flujo de tráfico para poder colocarlo de tal forma que la maximice. Tiene los siguientes mecanismos o procesos: MPLS (*Multiprotocol Label Switching*) y *Traffic Engineering*.

1.4.3.1 Conmutación de Etiquetas Multiprotocolo (MPLS)

Es una nueva tecnología que apunta a reducir los cuellos de botella que se forman en los enrutadores del *backbone*, las características más importantes son:

- Combina la conmutación de capa 2 y las funciones de ruteo de capa 3 con el fin de obtener mayor escalabilidad.

- La jerarquía de enrutamiento soportada por redes MPLS reduce el tamaño de la tabla de ruteo en enrutadores internos dentro de un dominio.

- MPLS utiliza algoritmos que permiten descubrimiento de vecinos y recuperación de rutas alternativas si se diera el caso que una ruta destino quedara deshabilitada o tuviera alguna falla.

La técnica que MPLS usa es conocida como *label switching*, en la cabecera del paquete se codifica una etiqueta, luego estos paquetes son transmitidos por redes basadas en celdas aumentando el *throughput*[1]. Está diseñada para trabajar con diferentes tecnologías por ejemplo, *frame relay*, PPP, *Sonet*/SDH y *Ethernet.*

1.4.3.2 Ingeniería de tráfico

La ingeniería de tráfico consiste en trasladar flujos determinados, que están por ir sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta, es decir con menos saltos, (ver figura 1-18).

[1] Esto es básicamente por que analiza únicamente una etiqueta y no toda la cabecera IP.

El objetivo aquí es enrutar los datos a través de la red, pero asegurando la disponibilidad de recursos en el presente y a futuro. Con ayuda de monitoreo constante de recursos se recibe retroalimentación para así disponer de recursos.

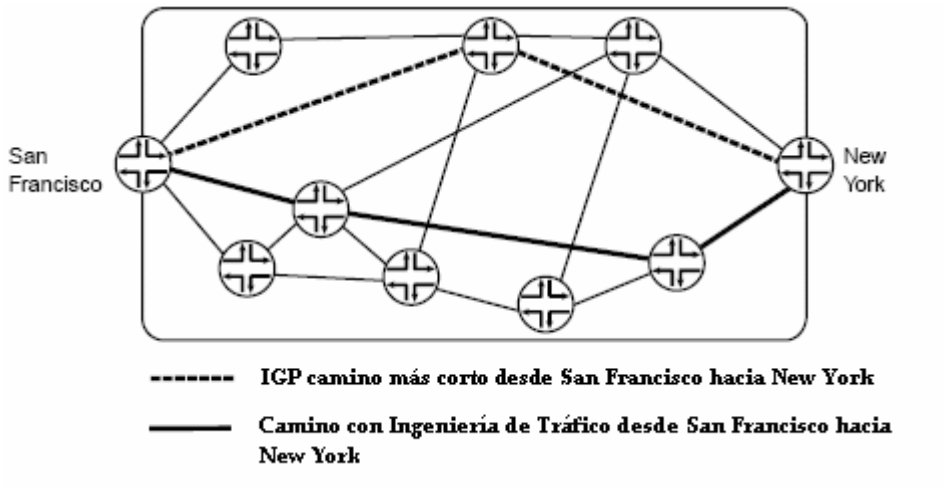


Figura 1- 18: *Traffic Engineering Path vs. IGP Shortest Path* [6]

Los protocolos para *gateway* Internet existentes, pueden contribuir al congestionamiento de la red, ya que no toman en cuenta la disponibilidad de ancho de banda y características de tráfico al construir las tablas de envío. Entre las principales aplicaciones de la ingeniería de tráfico están:

- Proveer un control preciso de sobre como el tráfico es reenrutado, cuando el camino principal se enfrenta con una o múltiples fallas.

- Mejorar características de la red, minimizando pérdida de paquetes, períodos prolongados de congestión, y maximizando el *throughput*.

- Proveer balanceo de carga, para evitar sobre utilización de recursos que vayan por un cierto conjunto de redes.

- Brindar más opciones, bajos costos y mejor servicio para los usuarios.

1.4.4 CALIDAD DE SERVICIO PERCIBIDA [18]

La calidad de servicio percibida se basa en como percibe el usuario el servicio prestado, entre los parámetros más importantes se tiene: éxito en la conexión, velocidad de transferencia de archivos, disponibilidad, fiabilidad del servicio.

Existen prestaciones no funcionales que reflejan el nivel de satisfacción que el cliente recibe en su relación con el proveedor del servicio, las más relevantes son: tiempo de demora en atención a quejas, precisión y corrección en facturación.

A nivel económico se han propuesto modelos para detectar el grado de satisfacción del cliente, se tiene el modelo objetivo, el modelo subjetivo y fisiológicos[1], para redes IP, se trata de conseguir métodos fiables para medir el grado de satisfacción del usuario, se han combinado tanto la parte objetiva como lo subjetiva, incluso se adaptan los diversos modelos subjetivos para una correcta evaluación lo que hace necesario conocer en primer lugar cuál es la interacción del usuario con el entorno de Internet, no es lo mismo un usuario particular que no requerirá el mismo nivel de conectividad que un usuario corporativo.

Se han realizado varios estudios sobre el tema la mayoría de ellos se basan el modelo SERVQUAL[2], la adaptabilidad de los modelos se ha hecho con el fin de adaptarlos a diferentes requerimientos de sistemas como: sistemas de información o ya más desmenuzado para un servicio como ejemplo navegación web.

La calidad de servicio que percibe el cliente es de vital importancia, dado que con esto se logrará mantener niveles competitivos, además para el cliente será transparente el cómo está diseñada la red, lo que verdaderamente le va a importar es obtener un servicio que se ajuste a sus expectativas.

---

[1] El modelo objetivo se basa en indicadores como el número de quejas, el modelo subjetivo usualmente va orientado a encuestas y el modelo fisiológico en reacciones involuntarias del cuerpo.

[2] Consiste en un conjunto de entrevistas y encuestas, se mencionan algunos desajustes por ejemplo las expectativas del cliente y la calidad que percibe, lo que el proveedor ofrece y lo que realmente entrega.

CAPÍTULO 2

ANÁLISIS DE LA SITUACIÓN ACTUAL DEL ISP "READYNET"

ReadyNet Cia. Ltda., es una empresa proveedora de servicios de Internet que funciona desde marzo de 1999, con permiso No.466-19-CONATEL-2000 del Consejo Nacional de Telecomunicaciones[1], permitiéndole durante el tiempo transcurrido comercializar servicios de Internet y sus aplicaciones, tanto a clientes *dial - up*, como corporativos (usualmente utilizan accesos banda ancha).

Se encuentra dentro de la clasificación de ISPs, como un ISP local [19], que sirve a una ciudad en especial (Quito), aunque con las facilidades de prestación de última milla, se brinda acceso a otras ciudades, pero sólo enlaces corporativos.

Los datos que se presentan en este proyecto, sobre infraestructura, tipos de usuarios, análisis de tráfico y sistema de seguridad presente en el ISP, son tomados hasta noviembre del 2005, para el posterior diseño del sistema de mejoramiento de seguridad y administración de tráfico, que se presentará en el capítulo 3.

2.1 INFRAESTRUCTURA

Está formada por enrutadores de acceso a la Internet, enrutadores de acceso para clientes hacia la red del ISP, plataformas de servicio (servidores), servidor de acceso remoto, *módems*, y *switchs*. En este ítem se presenta un breve análisis de las funciones que desempeñan los enrutadores y *módems* de acceso, además se especifica el tipo de enlace que ofrecen los proveedores de última milla (Andinadatos, Suratel, Stheal Telecom) a los clientes del ISP[2]. La figura 2-1, muestra el esquema de la red, con sus diferentes componentes.

[1] ANEXO A.1 (Permiso de explotación de servicio)
[2] Los enlaces que ofrecen son: enlaces xDSL, Frame Relay, IP CONNECT, enlaces Spread Spectrum..

INFRAESTRUCTURA DEL NODO PRINCIPAL

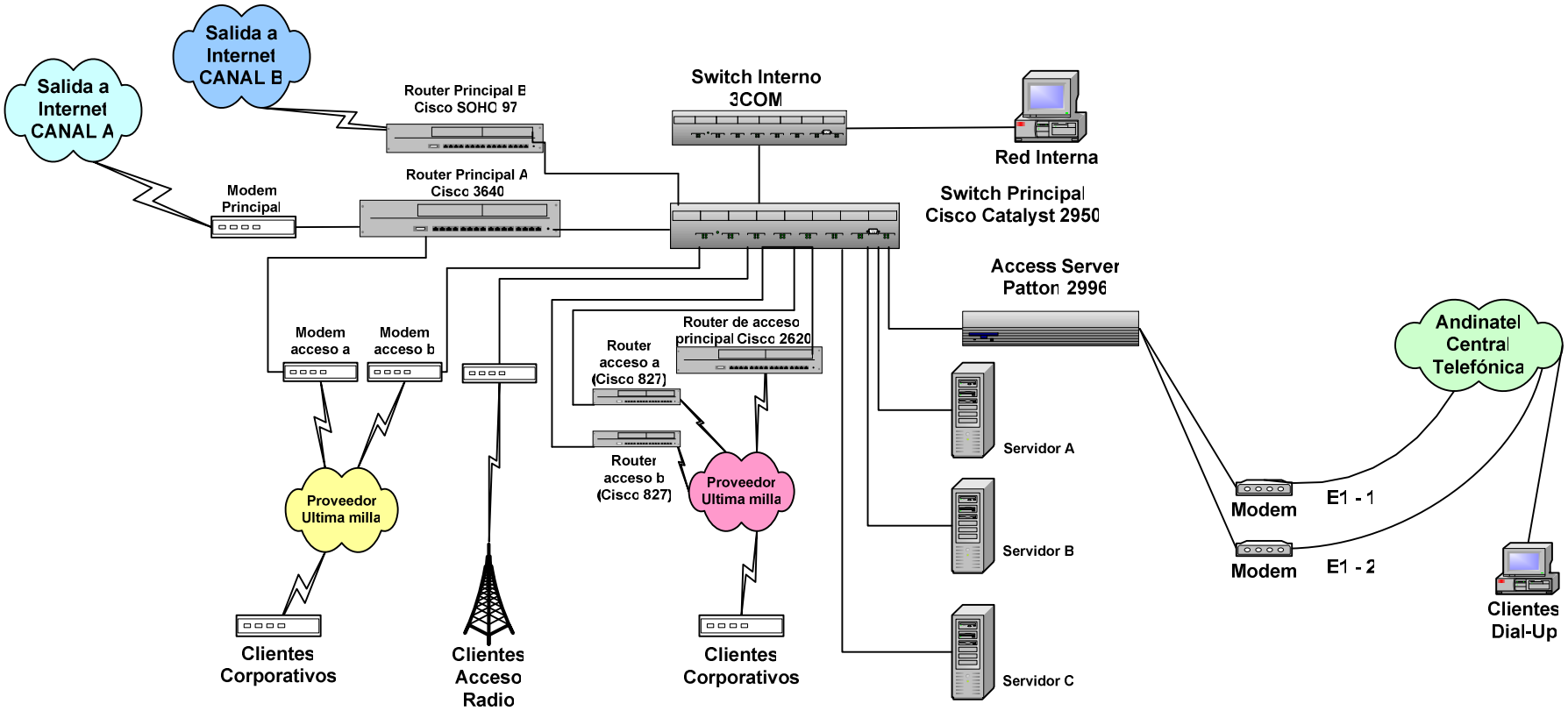


Figura 2- 1: Nodo Principal Quito

2.1.1 DESCRIPCIÓN DE LA INFRAESTRUCTURA DE ACCESO A INTERNET[1]

2.1.1.1 Enrutador principal A

Permite el acceso a Internet[2] (Proveedor de acceso IMPSAT), es una plataforma *Cisco* de la serie 3600 (modelo 3640, *software* (C3640-I-M), versión 12.0 (22), *release* (fc1)), se conecta al proveedor (Impsat) mediante un *módem* (DTU) de acceso, por una interfaz V.35, y a la red del ISP mediante una conexión *Ethernet* a 10 Mbps.

2.1.1.2 Enrutador principal B

De forma similar al *router* principal A, permite acceso a la Internet (Proveedor de acceso Andinadatos), es una plataforma *Cisco* SOHO97 (*software* (SOHO97-K9OY1-M), versión 12.2 (8) YN, *release* (fc1)), enlazada al proveedor de última milla por una interfaz ADSL. En la red del ISP el acceso es mediante una conexión *Ethernet* a 10 Mbps.

Como se observa en la figura 2-1, los enrutadores principales están enlazados con diferentes proveedores, la configuración esta implementada de tal manera que permitan acceso a clientes predeterminados para cada enlace, de ninguna manera el uno es respaldo del otro.

2.1.2 DESCRIPCIÓN DE LA RED DE ACCESO DE CLIENTES

Para el acceso de clientes hacia la red del ISP, éstos usarán los servicios de última milla que ofrecen diferentes proveedores de la zona, por ende es necesario tener la infraestructura para enlazar la red de acceso hacia la red del ISP; en algunos casos el proveedor de última milla es el que provee el equipo terminal en el lado del ISP.

---

[1] En el ANEXO A.2, se incluye los *datasheets*, de las plataformas Cisco 3640, Cisco Catalyst 2950, y del Cisco 2620, que son de propiedad del ISP, el resto de equipamiento es de los proveedores.
[2] En el ítem 2.4 se expone detalles sobre el acceso al *backbone* principal de Internet.

2.1.2.1 Enrutador de acceso principal

Este equipo brinda acceso a clientes que se enlazan al ISP bajo la infraestructura de Andinadatos, con accesos xDSL, y en capa 2 Frame Relay. Es una plataforma *Cisco* de la serie 2600 (*Router Cisco* 2620 *software* (C2600-I-M), versión 12.0 (5) T1, *release* (fc1)), enlazada mediante un *módem* de acceso con un canal E1 a la red de Andinadatos, ver figura 2-2, este enrutador es el encargado de discriminar el tráfico de clientes para que accedan a la Internet, ya sea por la salida A o B.

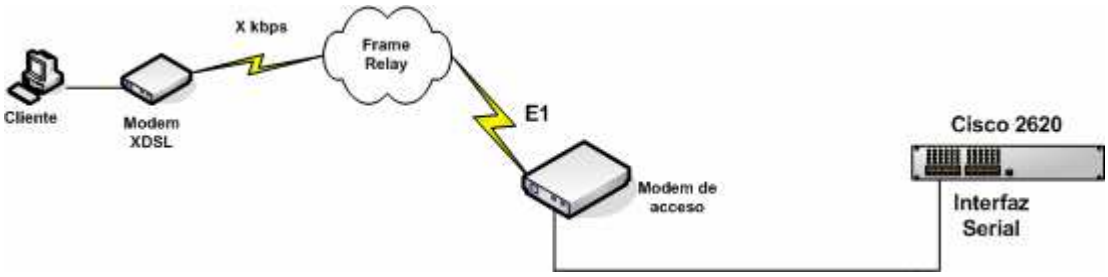


Figura 2- 2: Red de acceso de clientes xDSL

2.1.2.2 Enrutadores de acceso a y b

Son enrutadores de acceso xDSL y manejan a nivel de capa 2, ATM mediante el proveedor de última milla Andinadatos, bajo la plataforma *Cisco* de la serie 800 (específicamente enrutadores cisco 827), estos se enlazan a Andinadatos mediante una interfaz ADSL, y en la red del ISP se enlazan con una conexión *Ethernet* a 10 Mbps, brindan acceso a la Internet únicamente mediante el canal A. (ver figura 2-1).

2.1.2.3 Modem de acceso a

Este equipo es proporcionado por el proveedor de última milla (Suratel), por ende la administración y configuración del mismo está bajo su dominio. El servicio prestado a clientes que acceden mediante esta infraestructura, es a nivel de capa 2, *Frame Relay*. El *módem* (Tellabs 8110 CTE-S) en el lado del ISP requiere un

enrutador para operar, de forma similar al sitio del cliente, como se muestra en la figura 2-3.

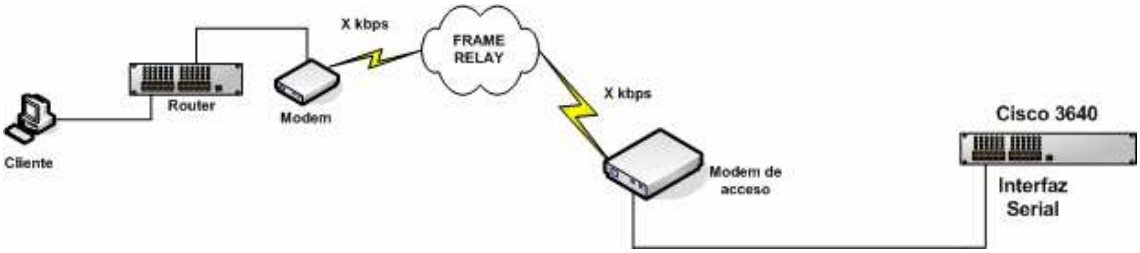


Figura 2- 3: Red de acceso clientes *Frame Relay*

2.1.2.4 Modem de acceso b

Es proporcionado y administrado por el proveedor de última milla (Suratel), provee acceso a clientes hacia la infraestructura del ISP, mediante la tecnología IP CONNECT, que simplemente es una extensión de la red LAN del ISP, y se enlazan mediante una conexión *Ethernet* a la red del ISP.

2.1.2.5 Acceso vía radio

La infraestructura es proporcionada por un proveedor de última milla inalámbrica, bajo el estándar 802.11 (a,b), usan como tecnología *Spread Spectrum*, en este caso el proveedor de última milla maneja toda la infraestructura. En el lado del ISP y del cliente la configuración es la siguiente (ver figura 2-4).

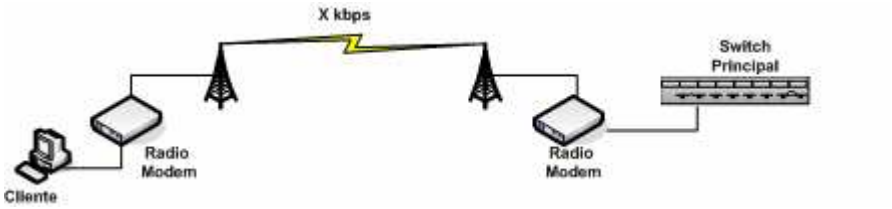


Figura 2- 4: Acceso vía radio

2.1.2.6 Acceso *dial – up*

Este tipo de acceso se lo hace mediante un *Access Server Patton* modelo 2996 que permite conexiones con tecnología V.34, V.90 y V.92. Se conectan dos E1s, que darán acceso a clientes a través de la PSTN (*Public Switched Telephone Network*).

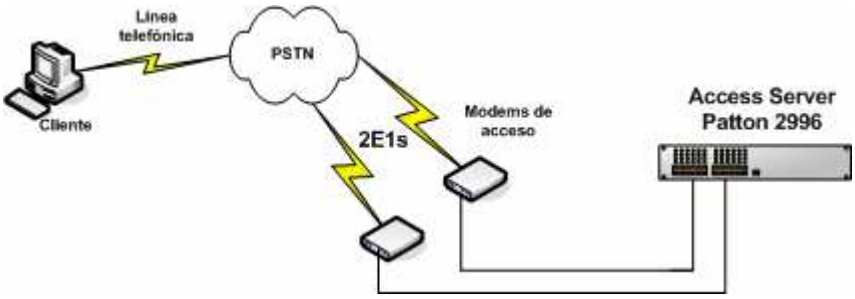


Figura 2- 5: Acceso dial-up

Todas estas plataformas excepto el *modem* de acceso a[1], se enlazan a la red del ISP con una conexión *Ethernet* a un *switch Cisco Catalyst* 2950.

2.1.3 DESCRIPCIÓN DE LAS PLATAFORMAS DE SERVICIO

2.1.3.1 Servidor A

Es una plataforma de arquitectura abierta, con procesador *Intel Pentium* III-1000 Mhz, con sistema operativo *Linux Red Hat* 8.0, presta los siguientes servicios:

- Servidor DNS principal
- Servidor de correo, soportando los protocolos SMTP y POP3
- Servidor de Autenticación y contabilización de tiempo de conexión de usuarios con sistema RADIUS
- Servidor de páginas Web

[1] Este *módem* se enlaza a una interfaz serial del enrutador principal A.

2.1.3.2 Servidor B

De forma similar al servidor A, es una plataforma de arquitectura abierta, *Intel Xeon* SE7500 SCSI *Server*, con 2 procesadores *Intel Xeon* de 2.4 GHz, con sistema operativo *Linux Red Hat Enterprise* 3.0, presta los siguientes servicios:

- Servidor DNS secundario
- Servidor de correo alterno para clientes corporativos, soportando los protocolos SMTP y POP3.
- Servidor principal de páginas Web
- Servidor principal de transferencia de archivos (FTP)
- Servidor *proxy* para clientes
- *Webmail*, para acceso *web* a correo de clientes

2.1.3.3 Servidor C

Servidor *Web*, bajo la plataforma *Windows* 2003 *Server*, tiene arquitectura abierta con procesador *Intel* PIV, de 1.8 GHz. Actualmente sirve páginas que se encuentran diseñadas para trabajar bajo plataforma *Microsoft*.

2.2 TIPOS DE USUARIOS

La clasificación de usuarios en el ISP, está hecha de acuerdo a las necesidades del cliente (aplicaciones que ejecutará), ya que de acuerdo a estos parámetros se establecerán los costos y garantías del servicio.

Dependiendo del tipo de enlace, el usuario podrá conectarse con velocidades en Kbps de 64, 128, 256, etc, sean estas asimétricas o simétricas. Los proveedores que prestan servicios de última milla al ISP son Andinadatos (enlaces ADSL corporativos, SDSL, y ADSL Home), Suratel (enlaces Frame Relay e IPConnect) y Stealth Telecom (enlaces de radio).

2.2.1 USUARIOS CORPORATIVOS

Este tipo de usuarios tienen acceso a la red del ISP mediante el uso de la infraestructura del proveedor de última milla, podrán contratar velocidades desde 64 kbps, en adelante; dependiendo del tipo de enlace que contrate, la velocidad de acceso podrá ser simétrica o asimétrica. Estos clientes gozan de ciertas garantías o ventajas que ofrece el ISP como se mencionan a continuación:

- Servicio técnico personalizado
- Administración de dominio
- Cuentas de correo ilimitadas
- Monitoreo de enlace 24/7/365
- Configuración de servidor Linux si el cliente lo requiere sin costo adicional
- Soporte a red interna, entre otras

A nivel de última milla, este tipo de clientes son atendidos por fallas en la red del proveedor en un tiempo de dos horas máximo[1].

2.2.2 USUARIOS BÁSICOS

Tienen acceso a la red del ISP, mediante la infraestructura del proveedor de última milla (Andinadatos), el tipo de enlace que contratarán es un enlace ADSL h Home, con velocidades desde 128/64 kbps, con una tasa de compresión propia del proveedor de ultima milla de 1:8[2], a nivel del ISP comparten un canal de 640 kbps, entre varios usuarios sin restricción, los tiempos de respuesta ante fallas en la red del proveedor de ultima milla es de 48 horas, por parte del ISP gozan de las siguientes ventajas:

- Servicio técnico personalizado
- Administración de dominio

[1] Dato proporcionado por proveedor de última milla Andinadatos.
[2] Dato proporcionado por el proveedor Andinadatos

- Cuentas de correo limitadas dependiendo del número de equipos en la red que el cliente contrate
- Monitoreo del enlace 24/7/365

2.2.3 USUARIOS *DIAL – UP*

Estos usuarios usan la PSTN (*public switched telephone network*) para el acceso a la red del ISP y un *módem* de acceso telefónico, el ISP se encarga de otorgar nombre de usuario y contraseña para el acceso, el cliente tendrá que marcar al número de PBX que el ISP indique. Los tipos de planes de acceso son ilimitado, noches y fines de semana, y el servicio por horas de conexión. Entre los servicios adicionales que cuentan son:

- Una cuenta de correo bajo el dominio del ISP
- Soporte telefónico 7/24/365
- Soporte presencial sin costo adicional
- Entrenamiento de uso (navegación y correo)
- Reportes de conexión, acceso vía *Web*

2.3 ANÁLISIS Y ADMINISTRACIÓN DE TRÁFICO

Con el objetivo de presentar estadísticas del tráfico que cruza por la red del ISP, este proyecto se basa en las herramientas: MRTG (*Multi Router Traffic Grapher*) y *ManageEngine™ NetFlow Analyzer*[1] (demo).

2.3.1 ANÁLISIS DE TRÁFICO

El ISP tiene contratado con el proveedor A, un enlace de 1792 kbps simétrico y con el proveedor B un enlace de 640 kbps simétrico. A continuación se presentará un breve análisis del tráfico que cruza por la red del ISP, con destino hacia la Internet. Para esto ha sido necesario tomar muestras de tráfico, en un período

[1] Es una herramienta para monitorear el ancho de banda, y analizar el tráfico de una interfaz, presenta datos vía *Web* y usa *NetFlow* como mecanismo para exportar datos.

aproximado de un mes (Octubre 2005), además de datos recolectados de meses anteriores de tráfico entrante y saliente.

2.3.1.1 Acceso a Internet mediante el canal A

Sobre este canal cruza tráfico de clientes corporativos y básicos con diferentes velocidades de acceso, sumando en total 3744 kbps (*downlink*) contratado por los mismos, a esto se añade el tráfico generado por los usuarios *dial-up* con 25 usuarios pico conectados, tráfico de la red interna del ISP, y el tráfico que generan los tres servidores.

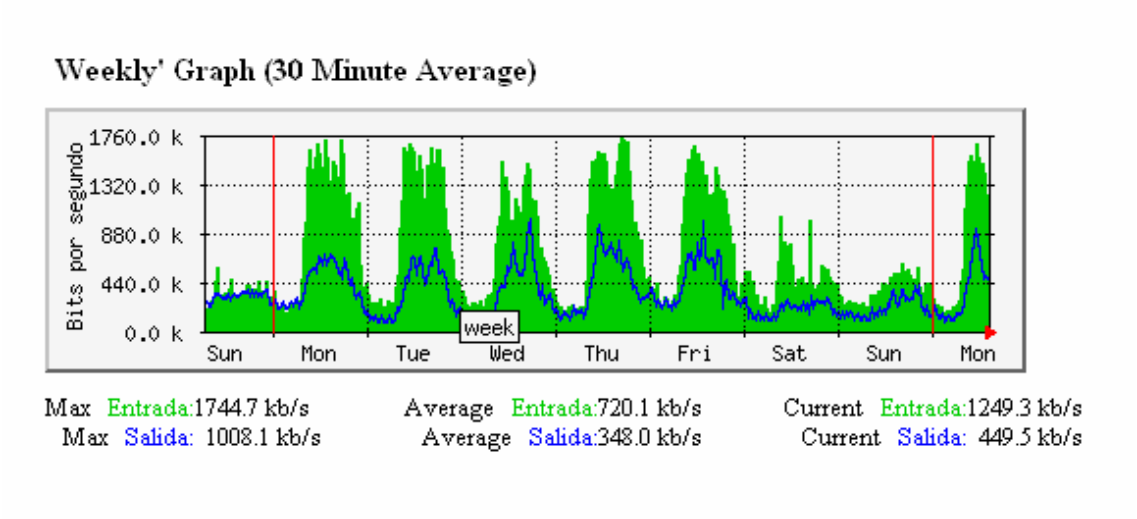


Figura 2- 6: Muestra de tráfico canal A

Como se observa en la figura 2-6 (muestra de tráfico semana 17-23 de octubre 2005), el enlace no permanece saturado todo el tiempo[1], pero sí tiene horas pico, siendo éstas principalmente en horas de la mañana (9h00 a 12h00) y en la tarde (15h00 a 18h00), cuando el enlace presenta saturación[2] es notorio por el aumento en tiempos de respuesta hacia un URL, en la figura 2-7, se presenta el resultado de ejecutar el comando ping hacia www.cisco.com, mostrando como promedio 582.260 ms, además de presentar pérdida de paquetes alrededor del 25%, siendo lo normal en períodos sin congestión tiempos de menos de 120 ms y 0% de paquetes perdidos.

[1] Uno de los problemas de este enlace son los accesos vía radio, los cuales llegan a saturar el canal.
[2] El enlace comienza a saturar al llegar más o menos a 1760 kbps, un 98.2%.

```
[root@uio root]# ping www.cisco.com
PING www.cisco.com (198.133.219.25) from 64.76.194.10 : 56(84) bytes of data.
64 bytes from www.cisco.com (198.133.219.25): icmp_seq=1 ttl=112 time=582 ms
64 bytes from www.cisco.com (198.133.219.25): icmp_seq=2 ttl=112 time=580 ms
64 bytes from www.cisco.com (198.133.219.25): icmp_seq=3 ttl=112 time=587 ms
64 bytes from www.cisco.com (198.133.219.25): icmp_seq=4 ttl=112 time=579 ms
64 bytes from www.cisco.com (198.133.219.25): icmp_seq=6 ttl=112 time=586 ms
64 bytes from www.cisco.com (198.133.219.25): icmp_seq=7 ttl=112 time=578 ms

--- www.cisco.com ping statistics ---
8 packets transmitted, 6 received, 25% loss, time 7011ms
rtt min/avg/max/mdev = 578.725/582.260/587.117/3.347 ms
```

Figura 2- 7: *Ping* a un URL(www.cisco.com)

Durante la misma semana el tráfico por aplicación es el siguiente:

2.3.1.1.1 Tráfico entrante

La figura 2-8, presenta en modo gráfico la utilización del enlace, mostrando el porcentaje de tráfico por aplicación en el período comprendido entre el 17 de octubre del 2006 y el 24 de octubre del mismo año. De un total de 56442.13 MB, el 61% es tráfico http, seguido por edonkey2000 14%, smtp 5%, https 1%, POP3 <1%, el porcentaje restante no se presenta ya que la herramienta distingue las aplicaciones más comerciales, cabe resaltar que la herramienta presenta porcentajes de utilización de aplicaciones que corren sobre TCP y UDP pero que no se las puede reconocer por su nombre comercial, entonces las junta en TCP_App o UDP_App. La forma de clasificar el tráfico por aplicación da una idea clara de la situación actual de ISP respecto al tráfico que cruza por la red.

La figura 2-8 que tiene la gráfica en forma de pastel presenta porcentajes respecto a los 56442,13 MB mencionados en el párrafo anterior, coincide con los datos que se presentan en forma horizontal, cabe recalcar que el 7% del tráfico total no es identificado por la herramienta la cual no reconoce en la totalidad todas las aplicaciones que cruzan por la red.

2.3.1.1.2 Tráfico saliente

En la figura 2-9 se detalla el tráfico que cruza por la red, incluso presenta las aplicaciones más relevantes (en el gráfico denominadas *Top Traffic*). Se envían aproximadamente 25894.36 MB, de los cuales el 25% es http, 21% smtp, 17% edonkey2000, 5% POP3.

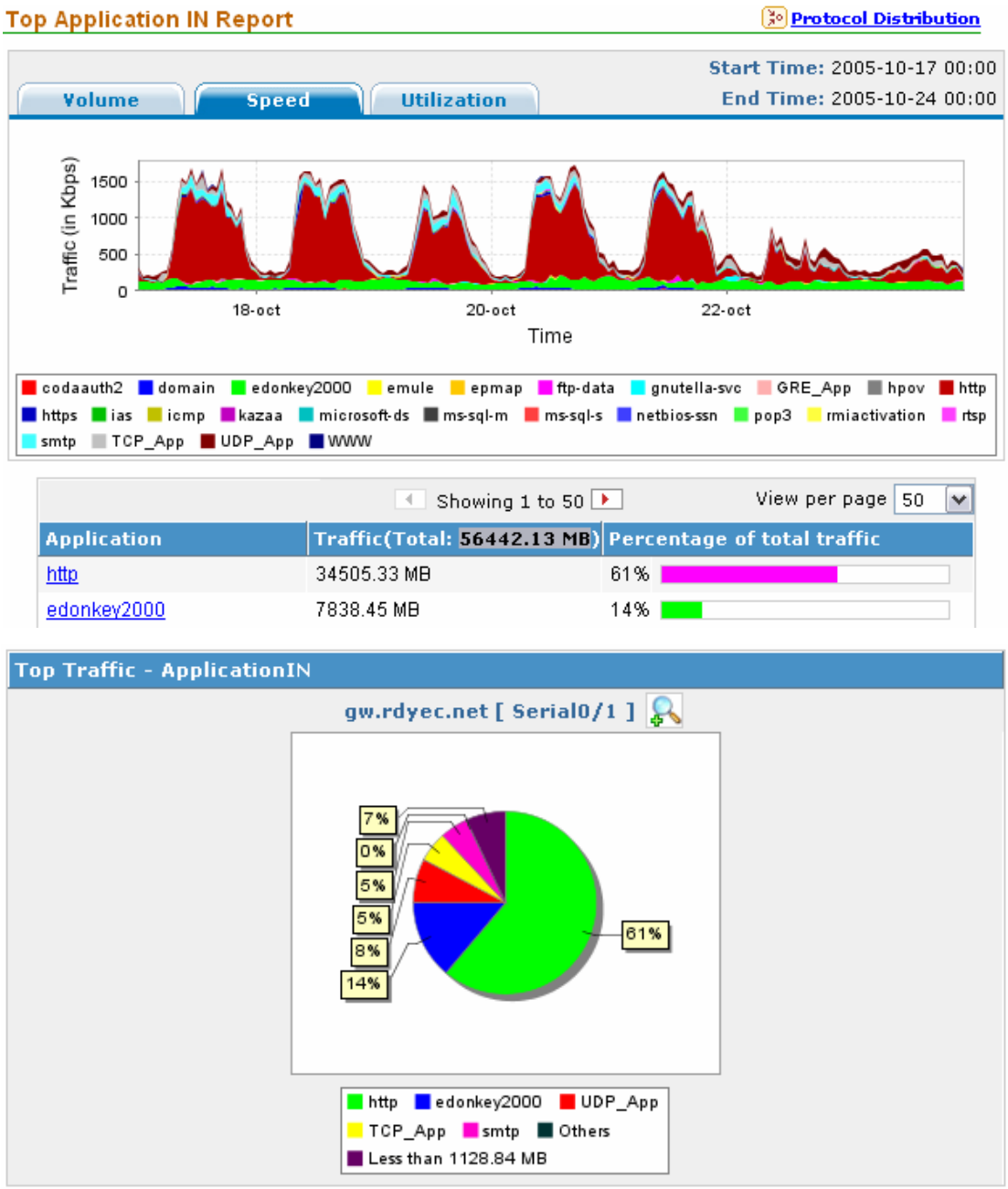


Figura 2- 8: Muestra de tráfico por aplicación

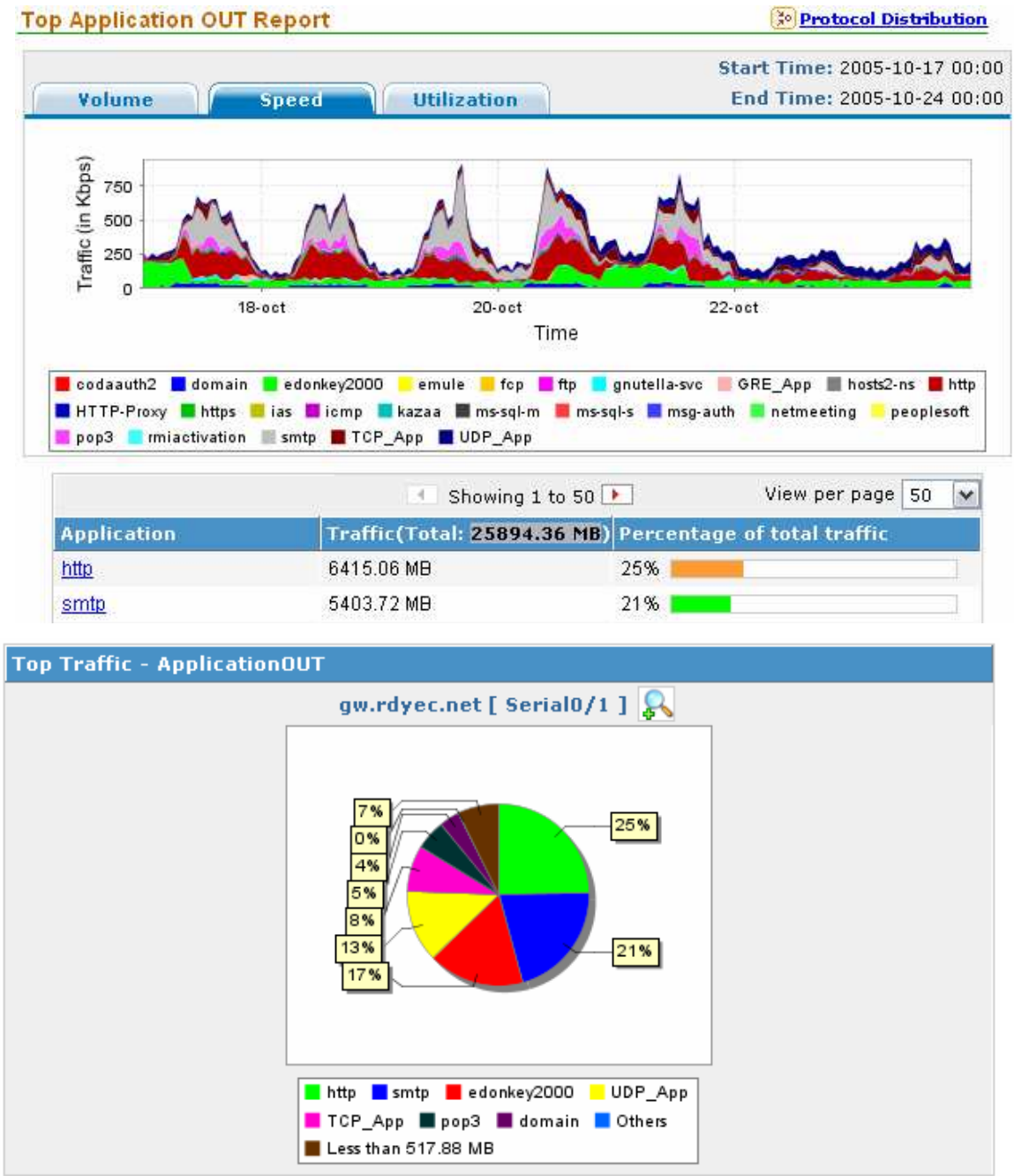


Figura 2- 9: Muestra de tráfico por aplicación

2.3.1.2 Acceso a Internet mediante el canal B

Éste canal está dedicado especialmente para clientes básicos, en total suman un ancho de banda contratado de 3328 kbps, pero el enlace tiene la capacidad de 640 kbps. El tráfico estadístico en una semana (15 al 23 de octubre de 2005) de este enlace es el siguiente, ver figura 2-10.

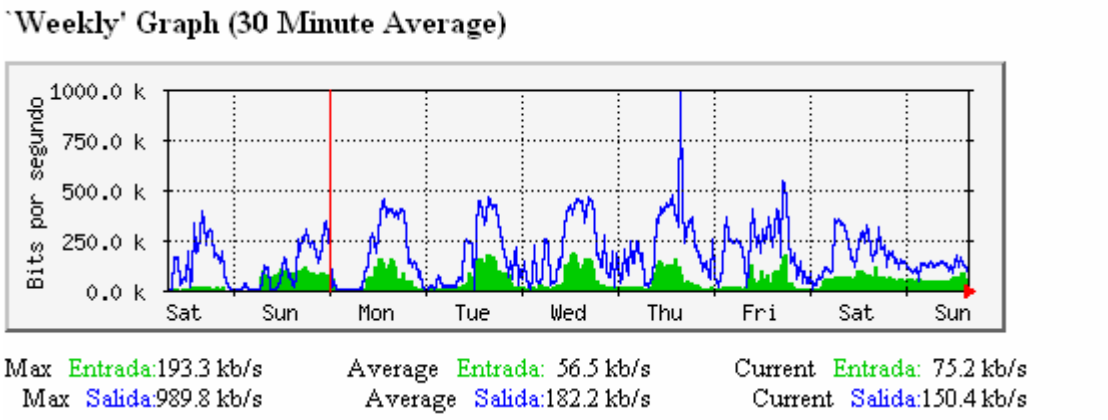


Figura 2- 10: Muestra de tráfico, canal B

2.3.1.2.1 Tráfico entrante

El tráfico por aplicación sobre este canal, que la herramienta *ManageEngine™ NetFlow Analyzer* entrega en la misma semana[1], está distribuido de la siguiente manera: de un total de 4683,11 MB trasmitidos el 28,52% es tráfico P2P (*Edonkey 2000, Gnutella, kazaa, etc*), 17,92% SMTP, 17,63% http, como se puede apreciar, la mayoría de tráfico es P2P, el motivo de éste cambio con respecto al canal anterior es que este canal es de uso exclusivo para clientes *home*, donde en la mayoría de los casos usan el enlace para descargas P2P, muy comunes en la actualidad. Estos datos se calcularon en base a los valores expuestos en la tabla 2-1, están en porcentaje mostrados gráficamente en la figura 2-11.

Tráfico Total (MB)	HTTP	HTTPS	TCP	UDP	P2P	POP3	DOMAIN	SMTP
4683,11	825,48	38,58	1230,62	264,36	1335,54	16,26	27,31	839,35

Tabla 2- 1: Tráfico por aplicación

[1] Dado que el enrutador principal B, no posee las facilidades para recolectar los datos mediante NetFlow, la herramienta genera un archivo en formato .xls (ANEXO A.3), donde sólo se muestran datos numéricos de la cantidad de paquetes que han cursado por la interfaz del enrutador sobre el cual es necesario obtener los datos del tráfico por aplicación. Para presentarlos gráficamente se utiliza las herramientas de Excel para graficar los resultados.

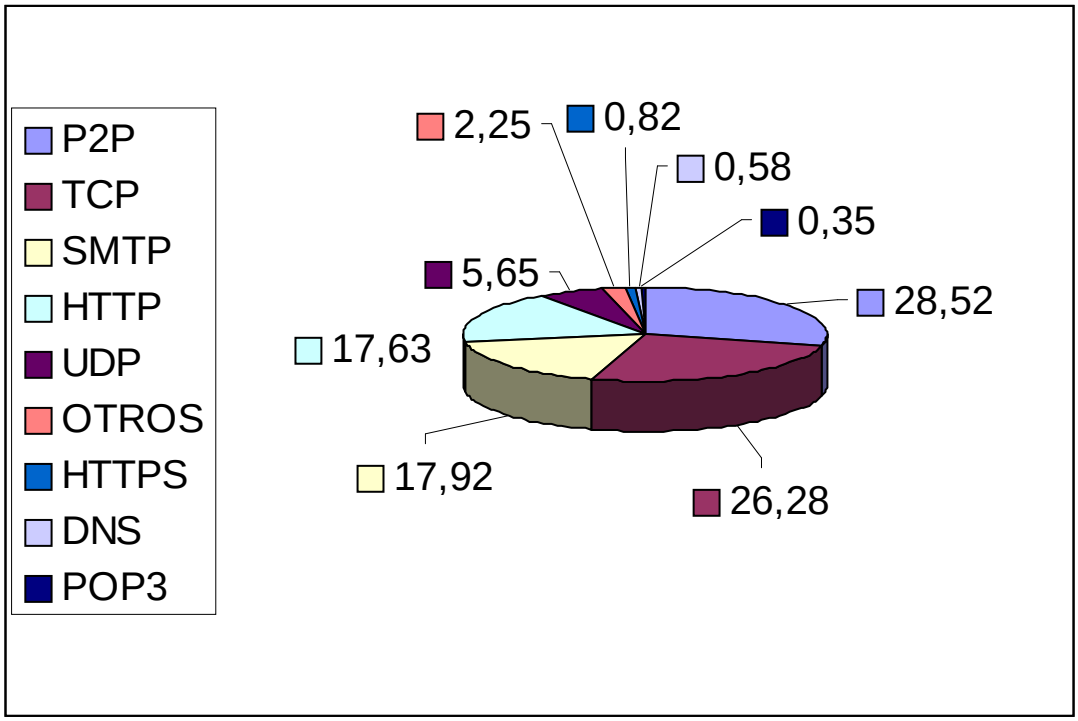


Figura 2- 11: Tráfico por aplicación

2.3.2 ADMINISTRACIÓN DE TRÁFICO

En éste ítem, se analiza brevemente la forma en que el ISP administra el tráfico que generan tanto clientes como servidores, hacia la Internet por los canales A y B.

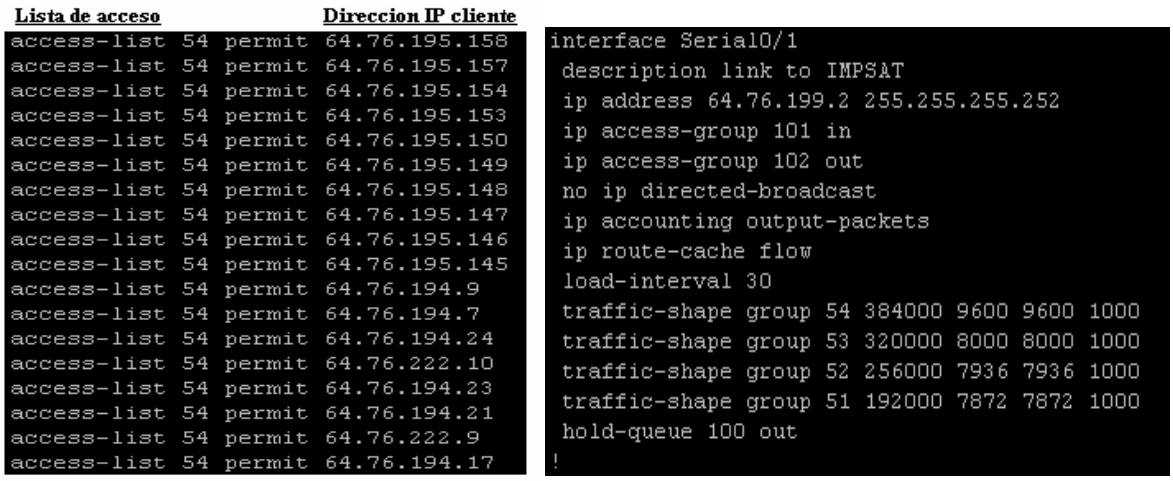
2.3.2.1 Canal A

La administración de tráfico[1] para este canal se la hace mediante las facilidades que presta la plataforma *Cisco* 3600 que se detalló en el análisis de las infraestructuras de red al inicio de este capítulo.

Se crean listas de acceso en el enrutador, a cada lista se le añaden las direcciones IP asignadas a clientes, y posterior a esto se asigna una determinada velocidad[2] mediante un mecanismo propio de la plataforma (***traffic-shape group*** *access-list-number bit-rate* [*burst-size* [*excess-burst-size*]]), y esto se aplica a la

[1] Tráfico de subida (*upload*).
[2] Se lo conoce como *bit – rate*, es una velocidad que se configura para determinada lista de acceso.

interfaz por la cual se tiene acceso a la Internet. La figura 2-12 muestra un ejemplo aplicado en el enrutador principal A del ISP.



Lista de acceso	Direccion IP cliente
access-list 54 permit	64.76.195.158
access-list 54 permit	64.76.195.157
access-list 54 permit	64.76.195.154
access-list 54 permit	64.76.195.153
access-list 54 permit	64.76.195.150
access-list 54 permit	64.76.195.149
access-list 54 permit	64.76.195.148
access-list 54 permit	64.76.195.147
access-list 54 permit	64.76.195.146
access-list 54 permit	64.76.195.145
access-list 54 permit	64.76.194.9
access-list 54 permit	64.76.194.7
access-list 54 permit	64.76.194.24
access-list 54 permit	64.76.222.10
access-list 54 permit	64.76.194.23
access-list 54 permit	64.76.194.21
access-list 54 permit	64.76.222.9
access-list 54 permit	64.76.194.17

```
interface Serial0/1
 description link to IMPSAT
 ip address 64.76.199.2 255.255.255.252
 ip access-group 101 in
 ip access-group 102 out
 no ip directed-broadcast
 ip accounting output-packets
 ip route-cache flow
 load-interval 30
 traffic-shape group 54 384000 9600 9600 1000
 traffic-shape group 53 320000 8000 8000 1000
 traffic-shape group 52 256000 7936 7936 1000
 traffic-shape group 51 192000 7872 7872 1000
 hold-queue 100 out
!
```

(a) (b)

Figura 2- 12: Administración de tráfico canal A

Como se muestra en la figura 2-12 (a), a una lista de acceso se le asignan diferentes direcciones IP, las cuales corresponden a IPs de clientes y de otros equipos en la red del ISP, para asignar un determinado ancho de banda a este conjunto de IPs, se usa el mecanismo de *Traffic Shaping*, como se muestra en la figura 2-12 (b), el mismo que es aplicado directamente a la interfaz que da acceso a la Internet.

Bajo este esquema se comparte el ancho de banda de subida contratado que tiene el ISP con el proveedor A, con todos los clientes que tienen acceso a la Internet por este canal. Los servidores del ISP no tienen un control del ancho de banda que usan, dado que no se aplica el mecanismo antes mencionado.
Una muestra tomada un fin de semana (ver, figura 2-13) permite notar que el *shaping* está activo solo para 2 listas de acceso, dado que las demás no generan tráfico que sobrepase lo asignado.

```
gw#show traffic-shape statistics
                Access  Queue     Packets   Bytes     Packets   Bytes     Shaping
I/F             List    Depth                         Delayed   Delayed   Active
Se0/0.1                 0         195680    35720546  16237     14186765  no
Se0/0.2                 0         7624      2159860   696       896710    no
Se0/0.3                 0         3636      957648    52        41070     no
Se0/0.4                 0         95822     37429372  22481     21655572  no
Se0/1           54      2         2237840   591351827 372464    140348939 yes
Se0/1           53      44        4689704   3183115619 4396474   2962863319 yes
Se0/1           52      0         1562293   424013923 54175     17156702  no
Se0/1           51      0         385867    50052183  5405      1408169   no
gw#
```

Figura 2- 13: Estadísticas de *Traffic Shaping*, aplicado en una interfaz

Este mecanismo no controla tráfico de bajada (*download*), y éste es el mayor tráfico en la red del ISP, incluso es el que satura en determinadas horas.

2.3.2.2 Canal B

Por éste canal por el momento no se aplica ninguna restricción del tráfico hacia la Internet, ya que la plataforma utilizada no presta las facilidades para hacer una distribución de tráfico como en el canal A.

Cabe mencionar que por el momento los clientes que acceden por este canal están limitados en velocidad, simplemente por lo que determina el proveedor de última milla. Pueden llegar a experimentar congestión cuando el canal en si esté congestionado.

2.4 ACCESO AL BACKBONE PRINCIPAL DE INTERNET

El ISP tiene acceso al *backbone* principal de Internet, mediante dos proveedores (Impsat y Andinadatos), las características se detallan a continuación.

2.4.1 CANAL A

Para el acceso mediante este canal a la Internet, se ha contratado un canal de 1792 kbps, a nivel de última milla se tiene un enlace de cobre, el cual físicamente

se conectara a un *módem* (*KeyMile - Music* 200), y éste a su vez al enrutador 3640, mediante una interfaz V.35, conector DB60. En capa 2 se comunica con el proveedor (Impsat) usando el protocolo HDLC (*High-level Data Link Control*), que a su vez accede al NAP de las Américas mediante Transnexa.

2.4.2 CANAL B

El proveedor para este enlace es Andinadatos, para enlazarse a la red del proveedor, se ha contratado un canal de 640 kbps, el ISP tiene a nivel de última milla un enlace de cobre que se conecta físicamente a un *Cisco* SOHO, mediante una conexión xDSL, y a nivel de capa 2 se tiene ATM, con encapsulación AAL5.

2.5 PARÁMETROS DE CALIDAD DE SERVICIO

Actualmente el ISP, no ofrece calidad de servicio a nivel de aspectos funcionales de la red, ya que no posee la infraestructura necesaria para priorizar ningún tipo de tráfico. El tráfico entrante a la red del ISP, y saliente del mismo, no tiene ningún tratamiento en especial en este aspecto. Si el canal de acceso a Internet se encuentra libre, obviamente no experimentarán retardo los paquetes de las diferentes aplicaciones, el problema surge cuando existe congestionamiento de la red, en este caso el conjunto de usuarios experimenta problemas en el acceso.

A nivel de calidad de servicio percibida por el usuario, no se ha hecho un estudio, sobre la satisfacción del servicio al que acceden, sin embargo el ISP, para alivianar problemas que puedan surgir a nivel de red del cliente, proporciona sin recargo soporte personalizado a red interna y asesoramiento en mantenimiento de la red del cliente, ayudando de esta manera a controlar tráfico indeseado desde la red del cliente hacia la Internet y viceversa, controlando en parte congestión a nivel del cliente.

2.6 SISTEMA DE SEGURIDAD

El sistema actual de seguridad tiene algunas falencias y se detallará en los siguientes ítems, las medidas que se han implementado para defender la red del ISP y los servicios que este ofrece.

2.6.1 SEGURIDAD FÍSICA

El ISP cuenta con los siguientes mecanismos para proteger la organización y los recursos que dispone.

- Guardias de seguridad para control de acceso a la organización
- Alarma y vigilancia las 24 horas del día
- Respaldo eléctrico de 6 horas (baterías y UPS)
- Protectores de línea para accesos xDSL, y accesos de otros proveedores con pares de cobre
- Alimentación eléctrica para los equipos, regulada
- Equipos asegurados contra robos y fallas

Entre los aspectos más destacados está el que no cuenta con una política y procedimientos de seguridad, el acceso al cuarto de equipos no tiene ningún control, no hay control de temperatura, control de incendios, etc.

2.6.2 RED DE ACCESO A INTERNET

Para limitar accesos no autorizados hacia la red del ISP desde la Internet o viceversa, se han aplicado restricciones mediante el uso de listas de acceso (ACLs), las principales son:

- Se usan listas de acceso extendidas, especialmente para bloquear o permitir protocolos de capa 4 o puertos destino de la misma.

- En el caso del ISP se han creado listas de acceso extendidas 101 y 102, las cuales son aplicadas a la interfaz que provee acceso hacia o desde la Internet, negando accesos como *Telnet* o SSH a equipos de la red del ISP.

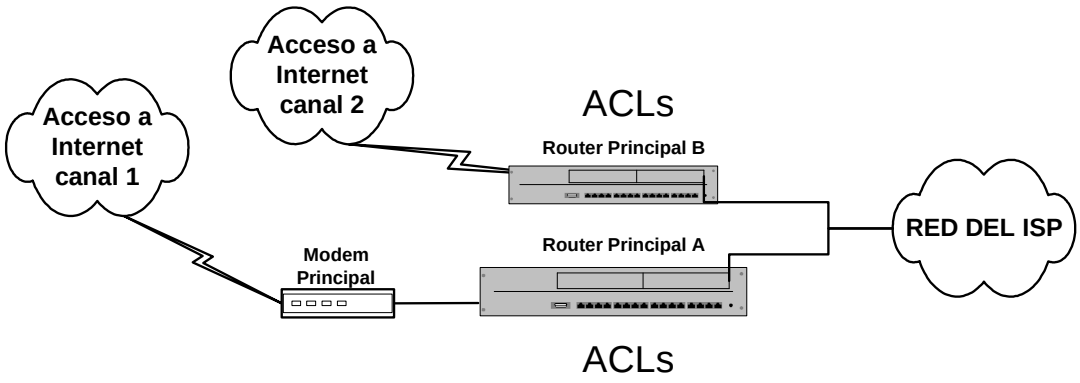


Figura 2- 14: Seguridad perimetral

Las medidas de seguridad aplicadas en este punto, proveerán en cierto grado, protección a los clientes de la organización y de alguna forma protegerá a la Internet de los clientes de la organización.

2.6.3 RED DE ACCESO CLIENTES

Considerando los diferentes tipos de usuarios que acceden, se analizará cada enrutador o mecanismo de acceso de los mismos.

En los enrutadores de acceso de usuarios que son: enrutador de acceso principal, enrutadores de acceso a y b, así como en los otros medios de acceso de clientes mediante proveedores de última milla, no existe un control de acceso mediante ACLs. Se considera que el acceso desde el exterior, a estos equipos está restringido en el enrutador principal (se usa aquí ACLs), aunque esto no garantiza accesos no autorizados que provengan del interior, en definitiva ataques internos.

Para usuarios *dial-up*, uno de los mecanismos de seguridad es mediante autenticación de usuarios usando usuario y contraseña, bajo el estándar RADIUS, usando protección de contraseñas mediante los protocolos PAP, CHAP.

2.6.4 PLATAFORMAS DE SERVICIO

Los mecanismos de seguridad implementados para asegurar los servidores de la organización son:

- Protección desde el exterior mediante control de acceso en el enrutador principal

- Control de acceso en los servidores en base a usuario, contraseña y dirección IP origen, se usa además permisos del sistema de archivos

- El acceso remoto a servidores es mediante SSH, al acceso mediante *Telnet* está bloqueado

- Respaldos diarios de la configuración e información

- Se han bajado servicios no necesarios en cada servidor, sin embargo se debería revisar ya que como se muestra en el ANEXO A.4 todavía existen falencias en este ámbito

2.6.5 SEGURIDAD EN SERVICIOS

Los mecanismos para asegurar los servicios que el ISP ofrece son:

- Actualización oportuna del software servidor de cada servicio ofrecido: *Apache*, *Sendmail*, BIND, etc, previniendo ataques a vulnerabilidades propias del software.

- Control de acceso a clientes que actualizan páginas *Web* publicadas por el ISP.

- Para el servicio de correo electrónico, se maneja control antivirus, y antispam, las herramientas usadas son: *MailScanner*, *Clam* antivirus.

- Para asegurar el acceso remoto a los equipos en el lado del cliente, se han creado restricciones.

2.6.6 ESCANEO DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

Las pruebas conocidas como *ethical hacking* son una de las partes fundamentales en el análisis de la seguridad en una organización, este ítem presentará algunas muestras tomadas respecto a las vulnerabilidades que presenta el ISP en las plataformas de servicio, en la protección que actualmente está brindando mediante la implementación de seguridad perimetral, y los resultados de implementar un filtro antispam en el servidor de correo.

En la figura 2-15, se muestra como mediante la utilización de un scanner[1] se obtiene información de las plataformas cisco que se encuentran en la red del ISP, se toma como ejemplo una de las subredes que maneja la organización, la herramienta entrega datos como el modelo de la plataforma, versión de IOS que se halla instalada, cabe recalcar que estos datos se los obtiene desde la parte externa del ISP, es decir a través de la Internet.

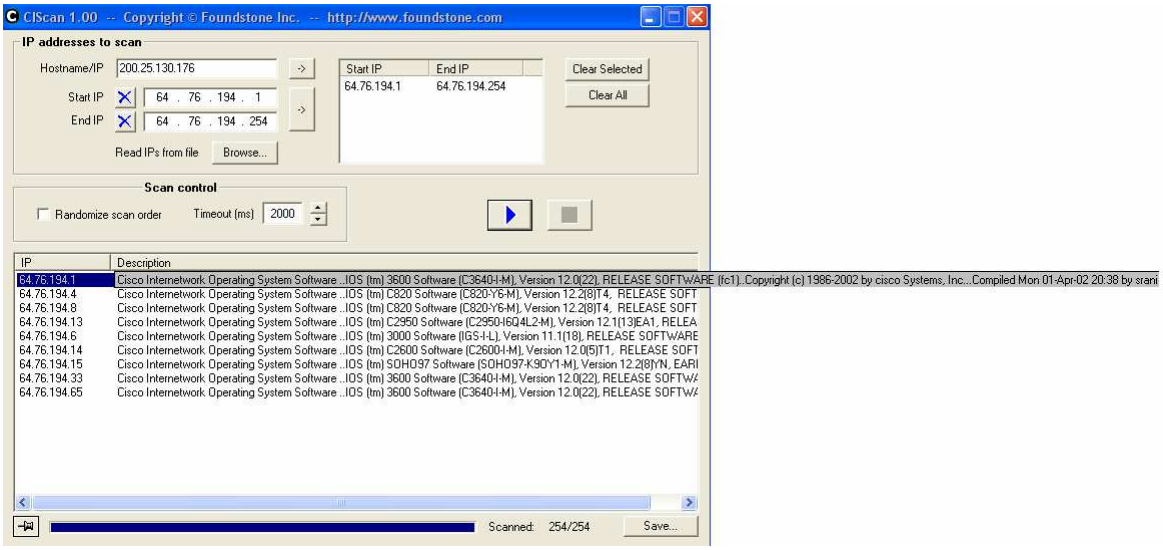
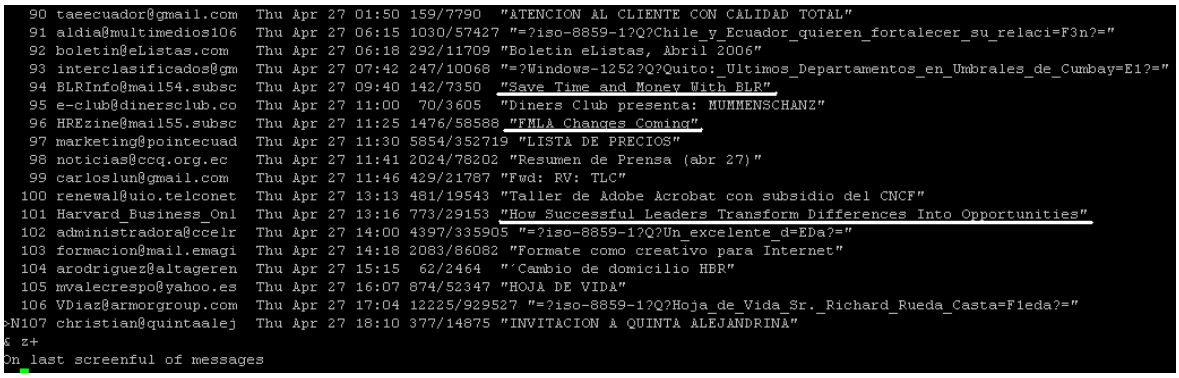


Figura 2- 15: Escaneo de datos referente a plataformas Cisco

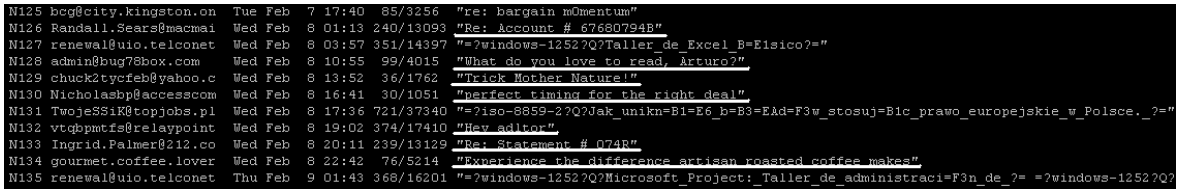
[1] CIScan, software que permite obtener información sobre las plataformas cisco que se encuentran en la red.

Mediante la herramienta *Retina – Network Security Scanner* (demo), se recolectan datos del estado de los servidores de la organización (servidor A y B) considerando vulnerabilidades que presenta los mismos. Además se escanea el enrutador principal A en busca del vulnerabilidades, los datos recogidos se encuentran en el ANEXO A.5.

De los datos detallados en el ANEXO A.5, se tiene que el servidor A presenta 45 vulnerabilidades de las cuales 17 son de alto riesgo[1], especialmente en la versión de los paquetes de software instalados en el mismo. En el servidor B, no se hallan vulnerabilidades con la herramienta que se usa para el escáner, sin embargo esto no es una garantía de que las mismas no existen dado que la herramienta usada es versión demo. Para el enrutador principal A, se tiene como resultado del escáner, 9 vulnerabilidades en total de las cuales 5 son de alto riesgo.

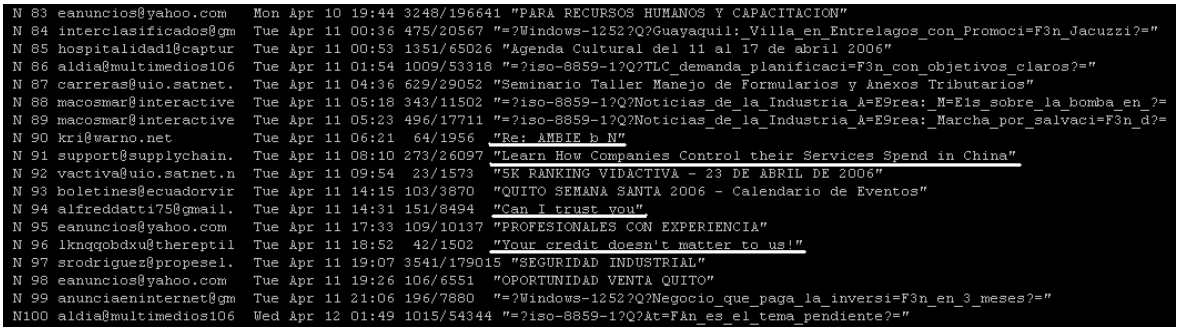


a)



b)

[1] La herramienta las denomina de alto riesgo.



c)

Figura 2- 16: Muestra de correos *spam*

En la figura 2-16, se ha tomado muestras del *spam* que puede ingresar a las cuentas de los usuarios a pesar de que existe un mecanismo que trata de controlar esto. Las gráficas muestran los correos recibidos en un día, en la gráfica a), de 18 correos recibidos se tiene 3 correos denominados *spam*, alrededor del 16.67% de correo basura. En la gráfica b) y c) alrededor del 77.78% y 25% respectivamente de correo basura. Es importante recalcar que aunque existe mecanismos de control para evitar que el correo basura o *spam* llegue al usuario existe un porcentaje todavía alto que ingresa, siendo de vital importancia una inmediato control del problema.

El control de antivirus como cualquier otro sistema de seguridad no es 100% efectivo, cabe mencionar que los usuarios se quejan sobre el ingreso de los mismos vía correo electrónico. Obviamente para contrarrestar el impacto el usuario final deberá instalar herramientas personales para que ayuden a la identificación de potenciales virus.

CAPÍTULO 3

DISEÑO DEL SISTEMA DE MEJORAMIENTO DE SEGURIDAD Y ADMINISTRACIÓN DE TRÁFICO PARA EL ISP “READYNET”

El presente diseño tiene como finalidad mejorar la seguridad del ISP, y ayudar en la administración del tráfico, tanto entrante como saliente hacia Internet. Con los datos obtenidos en el capítulo 2, se diagnosticará el estado de la red del ISP, en los ámbitos propuestos, para presentar una solución óptima.

Para comenzar el diseño del sistema de mejoramiento de seguridad en el ISP, se establecerán y definirán políticas de seguridad necesarias, que deberán seguirse para el correcto funcionamiento del sistema, considerando tres áreas principales: red de acceso desde Internet, red de acceso de los clientes y el segmento de red en el que se encuentran las plataformas de servicio.

Al hacer un estudio de nuevos requerimientos del ISP en los campos de seguridad y administración de tráfico, se mencionará como estos mecanismos, de ser implementados, mejorarán los parámetros de calidad de servicio, considerando medidas técnicas, y la percepción del usuario.

Se presentará el diseño en detalle, el cual en base a la problemática actual del ISP, propone algunas alternativas para mejorar el sistema, considerando especificaciones básicas de los equipos que se introducirán en la red del mismo, las ventajas, y posibles desventajas de la implementación de dichas alternativas.

Para finalizar, se mencionarán fundamentos sobre acuerdos de niveles de servicio, y como el ISP podrá considerarlos dentro del esquema actual que sostiene en este ámbito.

3.1 DIAGNÓSTICO Y ESTUDIO DE NUEVOS REQUERIMIENTOS

3.1.1 DIAGNÓSTICO DEL SISTEMA DE SEGURIDAD

En términos generales, el sistema de seguridad del ISP presenta algunas falencias, las principales se mencionarán a continuación:

- No existe política de seguridad formalizada, que defina lo que se quiere proteger y porque, aunque existen mecanismos de protección para las diferentes áreas del ISP, son sólo mecanismos básicos, por ejemplo el mayor mecanismo de seguridad con que se cuenta, es el acceso restringido a través del enrutador principal[1], no cuenta con mecanismos de seguridad profundos.

- Existe monitoreo, únicamente en forma manual, por ejemplo, para saber si algún cliente está generando demasiado tráfico, se deberá recurrir a analizar las estadísticas del flujo de tráfico en el enrutador. Si se quisiera automatizarlo, debería hacerse en base a herramientas que recojan datos del enrutador para una posterior interpretación.

- No existen registros de ejecución de pruebas de defensa contra intrusiones en el ISP, además a esto se suma la problemática de falta de políticas de personal, especialmente el que ha dejado de prestar servicios en la organización.

- No existe segmentación de la red, es decir ningún elemento encuentra separación efectiva, con la finalidad de proteger a cada sistema dependiendo de las necesidades de cada uno.

Entre los servicios a mencionar con inconvenientes están; el servicio de correo electrónico, que si bien cuenta con algunos mecanismos de control de virus y *spam*, se debería tratar de mejorarlos pues como se mencionó en el ítem 2.6.6,

[1] Bajo este esquema se asume que no habrán ataques internos.

ingresa todavía una gran cantidad de correo basura lo cual afecta notablemente al usuario final del servicio, dado que tiene que descargar una gran cantidad de correo basura para recibir unos cuantos correos válidos.

3.1.1.1 Nuevos requerimientos

Entre los requerimientos más importantes se tienen los siguientes:

- Establecer la política y procedimientos de seguridad, con esto se conocerá que es lo que se va a proteger, y los mecanismos que se ejecutarán para alcanzar un mayor grado de seguridad en el ISP.

- A nivel de la red del ISP, se deberá segmentarla para una correcta administración de los recursos, e implementar mecanismos de seguridad para cada área del mismo.

- Mejorar el nivel de protección de la red del ISP, mediante el uso de tecnologías apropiadas, de tal manera que se obtenga un sistema de seguridad en profundidad.

- Implementar un sistema de monitoreo más efectivo; en lo posible, que se entreguen datos en tiempo real, para mitigar lo más pronto posible problemas que surjan en la red del ISP, y realizar pruebas de penetración a la red, para posteriormente documentarlas.

3.1.2 DIAGNÓSTICO DEL SISTEMA DE ADMINISTRACIÓN DE TRÁFICO

En el ámbito de administración de tráfico en la red del ISP, como se mencionó en el capítulo 2, existen varios problemas que deben ser corregidos, con el objetivo primordial que tanto clientes, y proveedor aprovechen los recursos disponibles en el canal hacia Internet de la forma más óptima. Para obtener datos estadísticos del estado de la red fue indispensable monitorear el tipo de tráfico que cursa por la misma, especialmente obtener visibilidad del porcentaje de ocupación del canal

por aplicación (HTTP, SMTP, P2P, etc.); otro factor a ser considerado es la cantidad de tráfico que los clientes generan, enfocándose principalmente a si están sobrepasando lo contratado con el proveedor.

La problemática se resume en la falta de control de tráfico desde Internet hacia la red del ISP, ocasionando saturación del enlace, dado que el tráfico saliente es mínimo, y por ende no afecta el enlace. Los problemas de tráfico entrante se agravan cuando en determinados clientes, el proveedor de la última milla no limita el ancho de banda, y así, consumen más recursos de los contratados con el ISP[1].

Otro de los problemas es que si bien para solventar el congestionamiento de la red se contrata más ancho de banda, esto se agrava cuando el ISP intenta competir con otros proveedores que ofrecen mecanismos para priorizar cierto tipo de tráfico que el cliente cursa por la red, además ofrecen canales compartidos a costos inferiores.

Se verificó el tipo de aplicaciones que están dominando el ancho de banda, con los datos obtenidos se puede ver que el tráfico HTTP es el dominante en el canal A, P2P es el segundo en el canal A y el primero en el canal B, el cual quita recursos para otro tipo de aplicaciones más sensibles en la red.

Lo expuesto en los párrafos anteriores muestra que el enlace (canal A) se encuentra en el borde de la congestión la mayoría del tiempo[2], lo que genera lentitud en el acceso a los servicios. El canal B si bien por el momento no presenta congestionamiento, también tiene problemas en la distribución de recursos, el problema es que ciertos clientes que tienen contratados servicios a costos de canales compartidos en la mayoría del tiempo se llevan todo el canal sin permitir la reutilización del canal con otros clientes con el mismo nivel de compartición[3].

[1] ANEXO B.1
[2] ANEXO B.2
[3] ANEXO B.3

3.1.2.1 Requerimientos para administración de tráfico

Es indispensable una solución para administrar el tráfico que cursa por la red del ISP hacia Internet y viceversa, que cumpla con el objetivo de modelarlo, mejorar la calidad de servicio ofrecida al cliente, priorizar aplicaciones críticas, dado que nuevas aplicaciones están apareciendo todo el tiempo, y los usuarios desearán tomar ventaja de éstas; ofertar acceso a Internet con costos inferiores mediante la creación de planes compartidos y de esta manera ser más competitivos en el mercado.

Lo expuesto lleva a crear políticas de control de tráfico, con el fin de evitar extensos periodos de congestión en el enlace por la gran cantidad de tráfico que cruza por la red, sin dejar de prestar el servicio en condiciones aceptables para todos los usuarios.

Para la red del ISP de estudio necesariamente se deberá cumplir con los siguientes requerimientos:

- Segmentación del ancho de banda, mediante agrupar tipos de usuarios, por ejemplo corporativos, básicos o residenciales y dial – up.
- Políticas de administración de tráfico, como ejemplo la limitación de cierto tráfico dependiendo del tipo de usuario.
- Ofertar servicios con prioridades dependiendo del tipo de aplicación.

Actualmente hay soluciones para administración del ancho de banda, en base a clasificación de aplicaciones, tipos de clientes, además de proporcionar un análisis detallado sobre la utilización de la red, del rendimiento de aplicaciones y de la eficiencia de la red.

3.2 ESTABLECIMIENTO Y DEFINICIÓN DE POLÍTICAS DE SEGURIDAD [20]

3.2.1 INTRODUCCIÓN

Antes de comenzar a escribir las políticas de seguridad, que se aplicarán al ISP, se debe especificar cual es la meta de establecer y definir las políticas de seguridad.

El propósito de establecer las políticas de seguridad es: alcanzar niveles aceptables de seguridad en la organización, y de alguna manera, extender la misma seguridad a los clientes finales. Este proceso contemplará normar el acceso, garantizar la disponibilidad, y el correcto funcionamiento de los servicios que ofrece el ISP.

Las áreas del ISP donde se establecerán y definirán políticas de seguridad son: red de acceso a Internet, red de acceso de usuarios, segmento de red de plataformas de servicio y servicios que se ofrecen.
Entre los problemas y amenazas a proteger en términos generales se tienen: accesos no autorizados, ataques de negación de servicio, *spam*, virus, etc.

3.2.2 EXPOSICIÓN DE POLÍTICAS DE SEGURIDAD PARA EL ISP "READYNET"

Las políticas de seguridad se aplicarán a las siguientes áreas, (ver figura 3-1):

- Red de acceso a Internet,
- Red de acceso por usuarios,
- Plataformas de servicio y
- Políticas generales para los servicios que se brindan

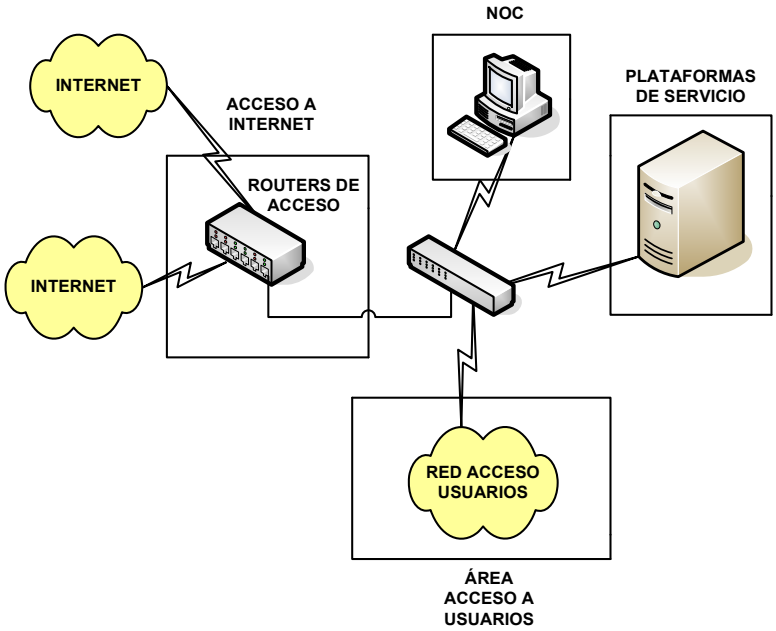


Figura 3- 1: Áreas donde se aplicarán las políticas de seguridad

3.2.2.1 Políticas para Seguridad Física del ISP

3.2.2.1.1 Propósito

Normar la localización, el acceso, y la recuperación ante desastres de la infraestructura física de la organización.

3.2.2.1.2 Alcance

Se aplicará a la infraestructura actual y nueva que llegue a formar parte de la organización, personal de la empresa, y personal externo que obligatoriamente llegare a necesitar acceso a las instalaciones.

3.2.2.1.3 Exposición de políticas

- Localización y medio ambiente

- La infraestructura de red[1] y servicios deberán ubicarse en el cuarto de equipos, los cuales contarán con facilidad de acceso para alimentación eléctrica regulada, y un correcto sistema de puesta a tierra.

- Las condiciones ambientales deberán cumplir estándares de control de temperatura, humedad, e incendios.

- Se debe identificar claramente la infraestructura de red y servicios, para llevar un correcto inventario de los recursos presentes en la organización.

❖ Acceso a instalaciones de la empresa

- El acceso a la empresa estará supervisado por guardias de seguridad, los cuales estarán en la obligación de restringir el paso a quien no se identifique y tenga la autorización respectiva para el ingreso.

- El acceso al cuarto de equipos de la organización será restringido, permitiéndose sólo el ingreso a personal autorizado.

❖ Recuperación ante desastres

- Antes de que ocurra un desastre o alguna situación que deje a la organización fuera de funcionamiento, se deberá contratar una empresa aseguradora que responda ante estos acontecimientos.

- Deberán existir los respectivos respaldos en caso de falla de energía eléctrica.

[1] Equipamiento de conectividad, plataformas de servicio, y servidores de bases de datos de la organización.

3.2.2.2 Políticas para red de acceso a Internet

3.2.2.2.1 Propósito

Normar el acceso a la información que contiene la infraestructura de red y garantizar la transmisión de datos generados por las redes que acceden a Internet mediante la misma, incluso cuando se presenten fallas, ataques, u otros contratiempos.

3.2.2.2.2 Alcance

Se aplicarán a la infraestructura de red de acceso (enrutadores de acceso a Internet), y al personal técnico autorizado para el acceso a dichas plataformas.

3.2.2.2.3 Exposición de políticas

- Las plataformas de acceso deberán cumplir con altas normas de seguridad con respecto a *software* del sistema operativo y configuración, entre las más importantes.

- Se aplicará control de tráfico hacia o desde las plataformas.

- Deberá existir control de acceso, ya sea local o remoto, exclusivo para personal técnico autorizado.

3.2.2.3 Políticas para red de acceso de usuarios

3.2.2.3.1 Propósito

Brindar seguridad perimetral considerando acceso a la red de usuarios, garantizar accesos no autorizados desde el exterior y extender la seguridad del ISP a los usuarios mediante segmentación de la red en el ámbito de seguridad.

3.2.2.3.2 Alcance

Se aplicará a la infraestructura de la red de acceso de usuarios.

3.2.2.3.3 Exposición de políticas

- Las plataformas de acceso deberán cumplir con altas normas de seguridad considerar como referencia el ítem *3.2.2.2.3*, el primer párrafo.

- Deberá existir control de tráfico entrante y saliente.

- Se deben mantener lineamientos de control de acceso a las plataformas de acceso a usuarios, que están físicamente en la red del ISP y por ende se extiende hacia la red del usuario.

- Los usuarios que acceden hacia la red del ISP, usando la PSTN para acceso *dial-up*, deberán hacerlo mediante usuario y contraseña proporcionada por el ISP, deberá existir un mecanismo de autenticación apropiada para los mismos.

3.2.2.4 Políticas para la red de plataformas de servicio

3.2.2.4.1 Propósito

Proporcionar un nivel de seguridad aceptable, en configuración, acceso, y administración de las plataformas de servicio del ISP.

3.2.2.4.2 Alcance

Se aplicarán a las plataformas de servicio presentes en el ISP, y al personal técnico autorizado, en la configuración y administración de las mismas.

3.2.2.4.3 Exposición de políticas

- Las plataformas de servicio deberán cumplir con altas normas de seguridad con respecto a la versión del software del sistema operativo, y la configuración del sistema.

- Los servidores deberán ser instalados y configurados sólo para proveer los servicios necesarios.

- Se controlará el acceso para configuración y administración, implicando accesos externos a las mencionadas plataformas.

- Las plataformas de servicio no deberán situarse en el mismo segmento de red que el resto de la infraestructura, se creará una zona desmilitarizada, con el objeto de proporcionar seguridad de la información que se encuentra en las plataformas de servicio, y fácil acceso a los mismos por parte de los usuarios.

- Debe existir monitoreo constante, para obtener información sobre posibles violaciones al sistema de seguridad aplicado a las plataformas de servicio.

- Se deberán obtener los respectivos respaldos del sistema, por lo menos una vez al día.

- Para la configuración y administración de plataformas de servicio, se deberá asignar personal técnico calificado.

3.2.2.5 Políticas para servicios ofrecidos por el ISP

3.2.2.5.1 Propósito

- Brindar seguridad contra ataques que puedan dejar fuera los servicios que se ofertan.

- Normar el uso del servicio de correo electrónico, garantizar disponibilidad, confidencialidad y protección contra ataques al servicio.

- Normar el acceso remoto a la infraestructura de red de la organización, y de cierta manera extender estas normas a la plataforma de usuarios, excepto casos especiales.

3.2.2.5.2 Alcance

- Garantizar la continuidad de los servicios incluso ante eventualidades que intentaren dejarlos sin funcionamiento.

- Las políticas para servicio *Web* se aplicarán a la infraestructura de red y administrador de la misma.

- En el servicio de correo electrónico serán aplicadas a los usuarios del servicio, y ciertas políticas se implementaran en la infraestructura de red correspondiente.

- Para acceso remoto se aplicarán a la infraestructura de red de la organización y al personal técnico autorizado.

3.2.2.5.3 Exposición de políticas

- Se deberá configurar y administrar correctamente todos los servicios proporcionados al usuario.

- Deberá existir infraestructura de seguridad que permita detectar amenazas y ataques de negación de servicio.

- Es indispensable un monitoreo constante sobre el correcto funcionamiento de todos los servicios que el ISP presta a los usuarios.

- Deberán existir mecanismos de seguridad para identificar contenido con código malicioso y bloquearlo.

- Los servidores *Web* deberán correr sólo programas y *scripts* confiables, que se ejecuten como parte del CGI con el servicio *Web*.

- La organización deberá revisar los mensajes de correo que pasen a través de sus servidores, verificando la existencia de virus, gusanos, u otro tipo de amenazas de seguridad para la red. Los correos infectados no deberán ser entregados al usuario.

- Se deberá limitar el tamaño de los casilleros de correo dependiendo del tipo de usuario.

- Se entregará usuario y contraseña, al usuario del servicio, garantizando la confidencialidad de estos datos.

- Se evitará el uso del servicio de correo electrónico para envío de correos que se consideren *spam*.

- Se deben usar protocolos y aplicaciones seguras para acceso remoto, negando el acceso mediante mecanismos inseguros, excepto casos especiales[1].

- Sólo personal técnico autorizado deberá manejar datos para el acceso, por ejemplo usuario y contraseña.

[1] Dependiendo de las plataformas y la versión de software si los mismos permiten o no accesos remotos con protocolos seguros.

3.2.2.6 Políticas internas del ISP

3.2.2.6.1 Propósito

Normar el acceso a los servicios, desde la red interna del ISP, y garantizar confidencialidad en la información que se maneje.

3.2.2.6.2 Alcance

Estas políticas se aplicaran al CAC (centro de atención al cliente), y a la red de acceso de área administrativa, se excluye la red de clientes.

3.2.2.6.3 Exposición de políticas

- Se restringirá acceso a sitios *Web* que el grupo de seguridad estime necesario, de acuerdo a las necesidades de negocio.

- Existirá monitoreo sobre sitios visitados por los empleados.

- Los usuarios no deberán transmitir ningún tipo de información que revele propiedad intelectual sobre la inteligencia de negocio de la organización.

- Se deberán cumplir las normas de correo electrónico que estipule el grupo de seguridad de la organización.

3.2.2.7 Penalidades

Se consideran política interna de READYNET CIA LTDA, razón por la cual quién llegare a incumplir estas normas, se sujetará a las sanciones estipuladas por el grupo de seguridad de la organización[1]. Como propuesta se exponen algunas de las penalidades que se asignarán a quien el alcance de las políticas cubra.

[1] Se deberá nombrar este grupo, para un correcto funcionamiento de las políticas de seguridad expuestas

3.2.2.7.1 Red de acceso a Internet, y red de acceso a usuarios

Mediante auditorias se verificará que el sistema cuente con los respectivos niveles de seguridad, si se llegare a incumplir con los requisitos estipulados en estas políticas, será amonestado verbalmente el administrador de la red encargado de mantener el sistema en las mejores condiciones.

3.2.2.7.2 Red de plataformas de servicio

El incumplimiento de dichas políticas generará llamadas de atención al personal técnico, encargado del área de seguridad de la organización.

3.2.2.7.3 Servicios del ISP

El grupo de seguridad de la organización fijará las sanciones para el personal encargado de mantener en correcto funcionamiento los sistemas.

3.2.3 PROCEDIMIENTOS

3.2.3.1 Seguridad Física

El grupo de seguridad de la organización, y el área financiera, contratará los servicios de una empresa que se encargue del aseguramiento físico, de forma especial en el sistema de control ambiental.

El departamento técnico será el encargado de controlar y asignar la ubicación de la infraestructura de red y servicios de la organización, manteniendo las respectivas normas de cableado estructurado.

Anualmente se hará el inventario de la infraestructura actual de la organización, con el fin de llevar un completo control de todos equipos pertenecientes a la misma.

3.2.3.1.1 Acceso a la organización

- Personal de la empresa

  - Se llevará un registro automatizado con el objetivo de controlar al personal entrante y saliente.

  - Sólo personal del área técnica autorizado podrá ingresar al cuarto de equipos, mediante acceso electrónico (tarjeta de identificación).

  - El acceso al cuarto de equipos de la organización estará bajo la responsabilidad del departamento técnico, además serán responsables de mantener esta área cerrada, restringiendo así el acceso por cualquier eventualidad, de personal no autorizado.

- Visitantes

  - Tendrán la obligación de identificarse y esperar autorización para el ingreso a cualquier área de la organización.

  - Sólo en casos especiales se autorizará el ingreso, a personal externo[1] al cuarto de equipos.

3.2.3.2 Red de acceso a Internet

El administrador de la red será el encargado de mantener los sistemas actualizados en las últimas versiones estables de los sistemas operativos de la infraestructura de red, hasta donde el *hardware* lo permita, posterior a esto se planeará escalamiento de *hardware*.

Deberá llevar un minucioso control sobre la configuración de los sistemas, vigilando que no existan cosas configuradas por defecto.

[1] Personal técnico autorizado perteneciente a proveedores de enlaces de última milla

El administrador de la red será el único responsable de otorgar permisos para accesos remotos por personal técnico capacitado, y el acceso será mediante mecanismos seguros.

En los enrutadores de acceso se configurarán ACLs de tal manera que se limite el tráfico entrante y saliente de la organización considerando la recomendación citada en el RFC 1918.

3.2.3.3 Red de acceso a la red de usuarios

Al igual que en el apartado 3.2.3.2, el administrador de la red será el encargado de mantener actualizados los sistemas a las versiones más estables.

Se segmentará la red, separando de esta manera las redes que operan en la red del ISP. Se aplicarán controles en los enrutadores de acceso mediante la creación de ACLs.

Para accesos *dial-up*, el mecanismo de autenticación será RADIUS, siguiendo con el esquema que actualmente sostiene el ISP.

3.2.3.4 Plataformas de servicios ofrecidos por el ISP

El administrador de la red será el encargado de mantener los sistemas instalados y configurados de la manera más óptima, evitando dejar configuraciones que vienen por defecto.

El mecanismo de seguridad aplicado a esta área será la creación de una DMZ (red desmilitarizada), mediante la instalación y configuración de un *firewall*, con el objetivo de separar esta área del resto de redes del ISP.

Para accesos locales y remotos a estas plataformas, serán autorizados por el administrador de la red. Los respaldos de cada plataforma de servicio serán diarios, y deberán ser almacenados en medios seguros, preferentemente en otro

disco que puede encontrarse en la misma plataforma, o en otra que se designe para estos fines.

Para mejorar la seguridad de servicios, se aplicarán mecanismos para analizar contenido, antivirus, *spam* y las respectivas auditorias de los sistemas para vigilar el correcto funcionamiento de los servicios ofrecidos por el ISP.

3.2.3.5 Red interna de la organización[1]

Todo acceso desde la red interna, será monitoreado. El mecanismo de control de acceso *Web* será regulado por un *proxy*, de tal manera que permita un monitoreo sobre sitios visitados por los usuarios, además de aplicar restricciones de navegación.

Los accesos a plataformas de servicio e infraestructura de red, serán mediante aplicaciones que permitan la administración usando protocolos seguros.

Se limitará algunos parámetros del servicio de correo electrónico, entre ellos el tamaño del casillero de correo, y el límite de envío de información por este medio. Como norma estrictamente necesaria, se eliminarán las cuentas de usuario del personal que deje de laborar en la empresa. Si fuera el caso de personal del departamento técnico que hubiere obtenido contraseñas de acceso a equipos de la organización, éstas deberán ser cambiadas por motivos de seguridad.

3.3 MEJORAMIENTO DE PARÁMETROS DE CALIDAD DE SERVICIO [21]

Allot Communications, fabricante de sistemas de administración de ancho de banda, define la calidad de servicio de la siguiente manera; “Calidad de servicio o administración de ancho de banda, es el término general dado a un amplio rango de tecnologías que permiten modelar el tráfico en una red.”

[1] CAC y área administrativa

Significa que una red que ofrece calidad de servicio, permite a las aplicaciones pedir y recibir un apropiado ancho de banda, controlar el *jitter* y el retardo. En base a calidad de servicio, se habla también de asignación de ancho de banda dependiendo de las prioridades de ciertas aplicaciones, pudiendo ser críticas como *Citrix*, ERP, además asegurar la entrega de aplicaciones sensibles al retardo como son VoIP, y video conferencia.

La calidad de servicio en ISPs es importante, porque los recursos de ancho de banda en estas organizaciones y en los enlaces que disponen, es un ancho de banda finito, pudiendo experimentar largos periodos de congestión; esto genera problemas en aplicaciones críticas, la mayoría de las veces sucede que aplicaciones hambrientas de ancho de banda consumen todos los recursos disponibles en la red.

Existen algunas estrategias que se deben considerar para entregar calidad de servicio en una red, y son las siguientes:

- Visibilidad y clasificación de tráfico
- Administración y control de tráfico
- Compresión

3.3.1 ESTRATEGIAS PARA ADMINISTRACIÓN DE ANCHO DE BANDA

La principal preocupación de varias organizaciones, entre ellas un ISP, es el desempeño de diversas aplicaciones que cursan la red, sobre todo, lo que se quiere evitar es que el canal hacia la Internet se congestione por aplicaciones que tienden a llevarse la mayoría de recursos de la red.

El crecimiento de aplicaciones que usan los recursos de la Internet ha sido a pasos agigantados, no es extraño encontrar redes con el comportamiento de la figura 3-2, donde la mayoría de tráfico que cursa por la red es recreacional, según expresa el gráfico el 53% del ancho de banda está siendo usado por aplicaciones recreacionales como son: *Real Audio*, *KaZaa*, *Internet Gaming*, *Web*

Browsing, por ende, para garantizar el correcto uso de recursos de una red, es necesario administrar el tráfico que cursa por la misma, siguiendo los siguientes lineamientos.

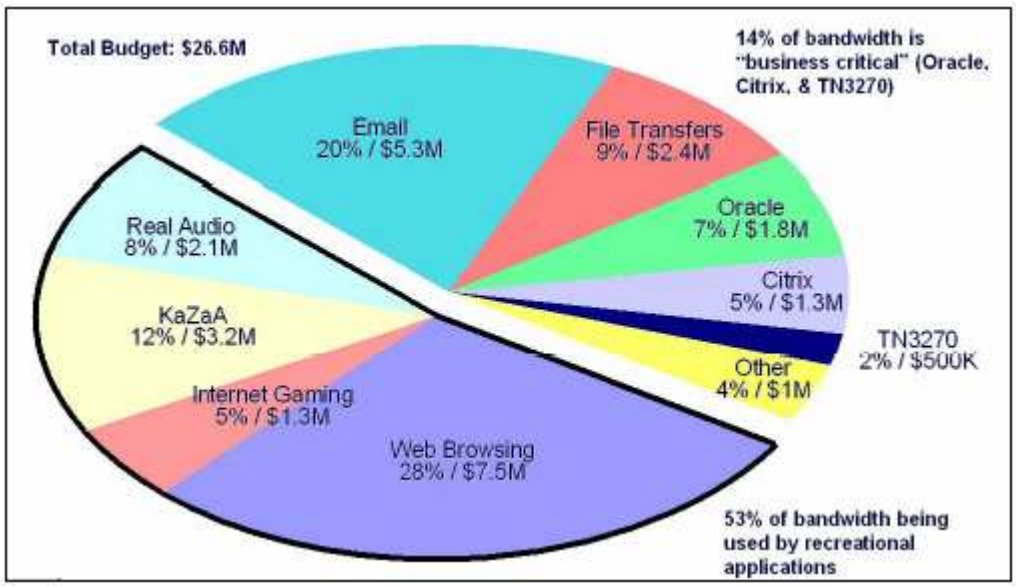


Figura 3- 2: Ejemplo de utilización del enlace por aplicación [7]

3.3.1.1 Visibilidad y clasificación de tráfico

Si el objetivo es administrar el tráfico que cursa por una red, es necesario identificar y categorizar qué tipo de tráfico está cursando, y más importante aun, la porción del ancho de banda que está siendo consumido por éste.

Existen varios mecanismos para identificar tráfico, por ejemplo, se tiene a nivel de capa 3 identificaciones por dirección IP, subredes, etc. A nivel de capa 4 se habla de identificación por puertos, rangos y listas de puertos, y existe identificación por firmas de aplicaciones, es decir a nivel de capa 7.

Si ya existe visibilidad de lo que cursa por la red, es necesario clasificar el tráfico, ya sea por aplicación, redes, subredes, tipos de usuarios, etc. Dado este precedente, se pueden garantizar diferentes tipos de servicio según sean las estrategias de negocio.

3.3.1.2 Administración y control de tráfico

Si se habla de administración y control de tráfico, se asocia normalmente con congestión de canales, motivo por el cual hay que emplear mecanismos para solventar este inconveniente; si bien se puede aplicar control sobre enlaces congestionados, es mejor evitar congestionamiento en el enlace.

En la mayoría de casos, el administrador de la red observará cómo aplicaciones P2P o adjuntos de gran tamaño en correo electrónico inundan el canal, dejando aplicaciones críticas con casi ningún recurso de la red. Para ayudar a controlar estos abusos, se han creado mecanismos de control, entre los más conocidos se tienen: aplicación de políticas de restricción para cierto tipo de tráfico (ej. recreacional, aplicaciones hambrientas de ancho de banda, etc.), marcado de paquetes con el fin de priorizarlos (en caso de aplicaciones críticas), encolamiento, rechazo de paquetes, compresión e incluso cuando el canal está congestionado, se recurre a lo más fácil, incremento del ancho de banda, obviamente cada uno de estos mecanismos tendrán ventajas y desventajas que deberán ser consideradas si se implementan.

3.3.1.3 Compresión

Este mecanismo permitirá obtener más con menos, es decir optimizar recursos de ancho de banda mediante comprimir la información pero de tal manera que no se vea afectada al momento de descomprimirla. Una de las plataformas que permiten obtener esta ventaja es *PacketShaper Xpress* de la marca *Packeteer*. El esquema funcional de esta plataforma se orienta a enlaces WAN, ya que el requerimiento es que exista una plataforma de estas en cada extremo, de tal manera que la una comprima el tráfico saliente y en el otro extremo el otro *appliance* descomprima el tráfico entrante.

3.3.2 PLATAFORMAS PARA ADMINISTRACIÓN DE ANCHO DE BANDA

3.3.2.1 Plataformas *CISCO* [22]

Cisco System, Inc. uno de los mayores productores de infraestructura para *networking*, ha creado un conjunto de herramientas para proporcionar QoS en diferentes tipos de redes, se resumirán algunos mecanismo en los siguientes ítems.

3.3.2.1.1 Visibilidad, clasificación y monitoreo

- *Visibilidad*: para entregar visibilidad sobre el tráfico que cursa por la red, se ha empleado el mecanismo denominado *Network-Based Application Recognition* (NBAR), que identifica una amplia variedad de aplicaciones, incluyendo las que están basadas en *Web*, y otros protocolos difíciles de identificar que usan puertos TCP/UDP dinámicos, identificación de tráfico HTTP por URL, *host* o por tipo de MIME, tráfico *Citrix Independent Computing Architecture* (ICA), entre los más importantes.

NBAR tiene una característica especial de descubrimiento de protocolos, que determina que protocolos de aplicación están atravesando por una interfaz[1] y en base a esto genera estadísticas asociadas con cada protocolo que posteriormente podrán ser utilizadas para definir clases de tráfico y aplicar políticas.

Existen las siguientes restricciones al uso de NBAR:

- No soporta más de 24 URLs, *hosts*, o MIME concurrentes
- Tráfico que no sea IP
- Paquetes fragmentados
- Peticiones HTTP que viajan a través de un túnel
- URL/*host*/MIME a través de HTTP seguro, etc.

[1] ANEXO B.4

No es configurable en las siguientes interfaces: *Fast EtherChannel*, interfaces donde se usen *tunneling* o encripción, VLANs, interfaces *dialer* y *Multilink* PPP.

- *Clasificación*: uno de los mecanismos más usados para clasificar tráfico es: *IP Precedence*, y en base a éste se pueden usar otros mecanismos como *Policy – Based Routing*, *BGP Policy Propagation*, *Committed Access Rate* (clasificación de paquetes), *Class – Based Packet Marking*, QoS para VPNs, y NBAR, para especificar y mejorar políticas sobre tratamiento de tráfico.

IP Precedence: permite especificar la clase de servicio para un paquete, usando los bits de precedencia del campo ToS de la cabecera del paquete IPv4, con esto es posible definir hasta seis clases de servicio, además ayuda a implementar otros mecanismos, por ejemplo en métodos de encolamiento (WFQ, WRED) se usan estos bits para priorizar tráfico.

Policy – Based Routing: permitirá clasificar tráfico basado en listas de acceso extendidas, mediante *IP Precedence* otorgará a la red la habilidad de diferenciar clases de servicio, y enrutar paquetes hacia caminos específicos. Las políticas se pueden basar en dirección IP, puertos, protocolos o tamaño del paquete. Los paquetes que transitan por una interfaz que tiene habilitado PBR pasan por filtros conocidos como *route maps*, entonces éstos serán los que dicten las políticas que seguirán los paquetes.

Committed Access Rate: esta opción que ofrece *Cisco*, no sólo permite clasificar tráfico, sino también aplicar políticas para limitar velocidad. CAR permite segmentar la red en múltiples niveles con distinta prioridad o clases de servicio, trabajando en conjunto con *IP Precedence*, y el tráfico clasificado mediante este mecanismo puede ser sujeto a una subclasificación de acuerdo a políticas que se implementen.

- Monitoreo: existen herramientas que permiten configurar y controlar la funcionalidad avanzada de calidad de servicio (QoS) basada en IP en los enrutadores *Cisco*, QDM (*QoS Device Manager*) es una aplicación de

administración de redes basada en *Web* que proporciona una interfaz fácil de utilizar; esta herramienta también provee mecanismos básicos de monitoreo, combinando las funcionalidades de NBAR. Otra herramienta es QPM (*QoS Policy Manager*), es parte del paquete *CiscoWorks*, permite al administrador definir políticas de QoS y distribuirlas a través de la red hacia todos los dispositivos que manejan QoS, posteriormente en base a NBAR MIB, se tiene acceso a información del protocolo NBAR entregando datos sobre el consumo de ancho de banda de los protocolos más usados.

3.3.2.1.2 Mecanismos de control

Cisco Systems, Inc, tiene mecanismos para evitar congestión en una red y para administrar la misma. Para evitar congestión se tiene WRED (*Weighted Random Early Detection*) y DWRED (*Distributed WRED*). En cambio, la administración de congestión exige la creación de colas; una vez clasificados los paquetes serán asignados a estas colas. Los mecanismos de encolamiento manejados por *Cisco* son: FIFO, WFQ (*Weighted Fair Queueing*), CQ (*Custom Queueing*), PQ (*Priority Queueing*), (ver tabla 3-1).

	Flow – Based WFQ	**CBWFQ/DCBWFQ**	**CQ**	**PQ**
Número de colas	Número de colas configurable, máximo 256	Una cola por clase, 64 clases	16 colas	4 colas
Tipo de servicio	Asegura equidad a todo el trafico existente	Provee garantías de ancho de banda para clases de tráfico	Servicio Round - Robin	Colas de alta prioridad son servidas

Tabla 3- 1: Comparación de mecanismos de encolamiento [23]

- *WRED (Weighted Random Early Detection)*: es la implementación de RED (*Random Early Detection*)[1] en las plataformas Cisco, este mecanismo permite evitar congestión en la red mediante descarte de paquetes, pero evitando sincronización global[2], toma ventaja del mecanismo de control de congestión TCP, a más de usar las características de *IP Precedence*, para manejar tráfico preferencial, es decir los paquetes que tengan alta prioridad podrían no ser descartados, generalmente WRED descarta paquetes basado en *IP Precedence*, los de menor valor serán descartados en su mayoría.

- *Shaping* y *Policing*: estas herramientas permiten detectar violaciones de tráfico, la diferencia es la forma en que responden a dicha violaciones. *Policing* típicamente descarta paquetes, en cambio *shaping*, retarda el exceso de tráfico usando *buffers* o mecanismos de encolamiento.

- *Traffic Policing*: permite controlar la tasa máxima de tráfico enviado y recibido en una interfaz mediante un algoritmo de *token bucket,* y particionar la red en múltiples clases de servicio. Usualmente este mecanismo se lo configura en interfaces de enrutadores de borde. Si se diera el caso de exceso de tráfico, lo que se hace es descartarlo o enviarlo con prioridad diferente.

- *Traffic Shaping*: permite controlar el tráfico saliente en una interfaz, este mecanismo intenta evitar pérdida de paquetes, usa mecanismos de encolamiento. Existen tres tipos de *traffic shaping*, GTS, *class – based* y FRTS, la diferencia entre estos son los mecanismos de encolamiento usados[3].

Estos mecanismos de visibilidad, clasificación, monitoreo y control se implementan en enrutadores de la serie 7500, y en algunos casos, en enrutadores 36xx, y 26xx.

[1] Controla el tamaño promedio de la cola, para indicar al *host* extremo que temporalmente debe bajar la transmisión de paquetes.
[2] Se manifiesta cuando múltiples *host* reducen sus tasas de transmisión en respuesta al descarte de paquetes.
[3] GTS y class – based usan WFQ, mientras que FRTS usa CQ o PQ.

3.3.2.2 *Allot Communications* [24]

Allot Communications ofrece soluciones para administración de ancho de banda que mejoran el rendimiento de la red, orientado para empresas y proveedores de servicios IP, Las soluciones que brinda son una combinación de hardware y software, la solución *NetEnforcer* es un *appliance* LAN que permite inspeccionar, monitorear y controlar tráfico por aplicación y por usuario. *NetEnforcer* identifica cientos de aplicaciones y protocolos, a más de perfiles de usuario para posteriormente aplicar políticas de tráfico.

3.3.2.2.1 Clasificación y visibilidad

Allot tiene desarrollados mecanismos para reconocimiento a nivel de aplicación de protocolos de red, mediante firmas de aplicaciones, usando identificación por puertos bien conocidos, además de inspección de contenido.

Clasificación de tráfico:

- Por dirección IP/MAC, se incluye rango de IPs, subredes, nombre de *host*.
- Protocolos de red, protocolos IP y aplicaciones.
- Clasificación a nivel de capa 7, para aplicaciones P2P (KaZaA, eDonkey, WinMX y más), aplicaciones de negocio (Citrix, Oracle), VoIP y streaming (H.323, MSPlayer), y protocolos de Internet (FTP, HTTP, Instant Messaging y más)
- Mediante contenido de la aplicación para HTTP (URL, tipo de contenido, *host*), para Oracle (base datos, nombre, nombre de usuario), y H.323 (audio/video, CODEC).
- VLAN ID (802.1Q), prioridad de la VLAN (802.1p).

- Byte ToS – DiffServ o bits de *IP Precedence*.

Métodos de clasificación de tráfico: *Allot* para clasificar tráfico usa *Pipes* (permite dividir el ancho de banda total y administrarlo como si fuera un enlace independiente, dentro de este pueden existir varios *virtual channels*), y *virtual channels*.

Monitoreo de actividad de la red: se tiene el mecanismo llamado *Java-based Traffic Monitor,* que presenta más de 100 vistas en tiempo real del tráfico y comportamiento del mismo, por ejemplo entrega gráficas de la utilización del ancho de banda de usuarios. A continuación se presentan las más importantes características de monitoreo, alertas y *accounting*.

Monitoreo en tiempo real de distribución de protocolos, clientes, servidores, VCs, y *pipes*, los más activos en la red (TOP, ver figura 3-3).

- Soporta recolección de estadísticas por VC y *pipe*, mediante SNMP.

- Alertas inteligentes, sobre eventos principales en la red para, tomar las medidas correctivas, *accounting* opcional mediante *NetAccountant*, siendo posible obtener datos de tráfico por sesión.

Protección DoS: detecta ataques conocidos de negación de servicio, y presenta una línea de defensa que mejora el rendimiento de *firewalls* y dispositivos de protección de red interna, mediante *NetEnforcer* se puede monitorear, registrar y bloquear flujos de tráfico malicioso, y alertar al usuario de ataques inminentes.

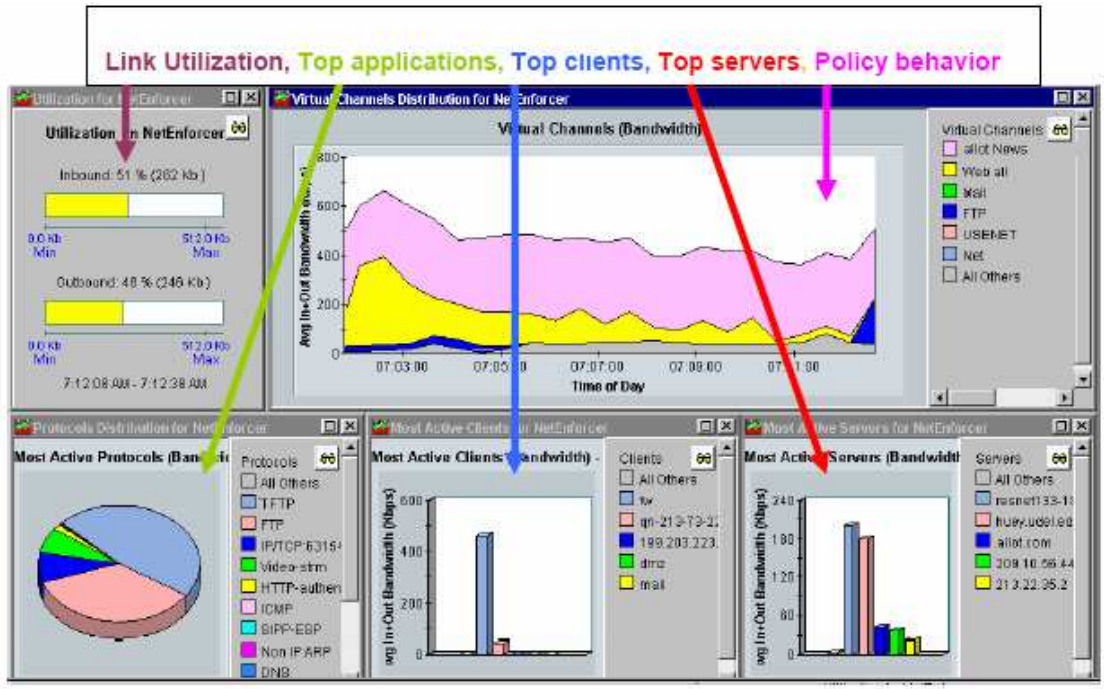


Figura 3- 3: *Java-based Traffic Monitor* [8]

3.3.2.2.2 Mecanismos de control

Las políticas de calidad de servicio consisten en un conjunto de reglas, y un conjunto de acciones aplicadas a *pipes* y canales virtuales.

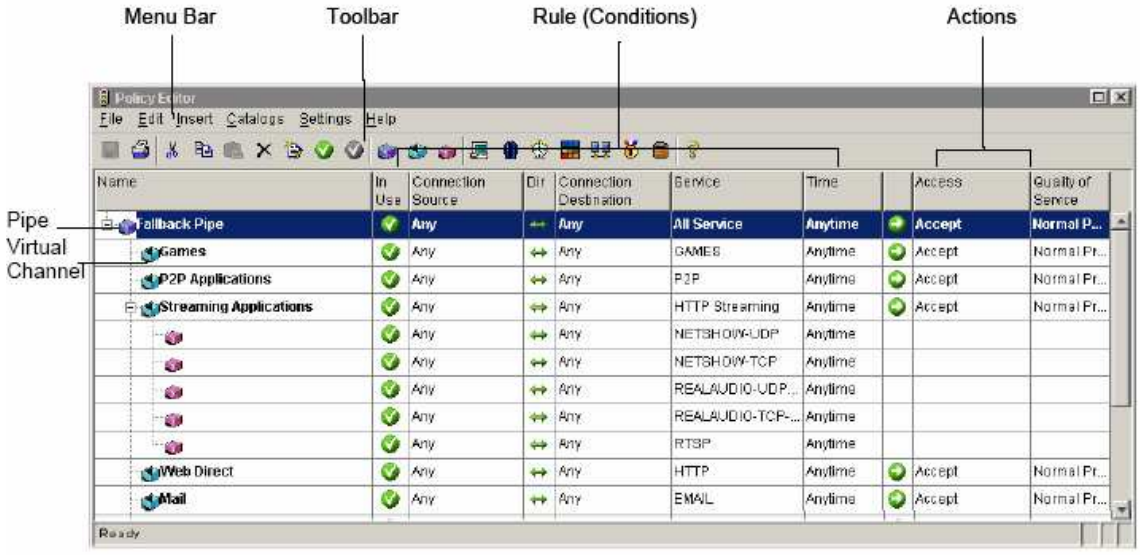


Figura 3- 4: Editor de políticas [8]

Reglas: una regla es un conjunto de seis condiciones, éstas pueden ser definidas a nivel de *pipe* o canal virtual, y son las siguientes:

- Fuente de conexión, como ejemplo IPs, rango de IPs, hosts, etc.
- Destino de la conexión, puede ser por IP, rango de IPs, subredes, etc.
- Por servicio, define los protocolos relevantes en una conexión, los de tipo IP, TCP, UDP, no TCP, no UDP, no IP.
- TOS, considera el byte TOS de la cabecera IP.
- VLAN
- *Time*, define el período del tiempo en el cual el tráfico es recibido.

Acciones: son asignadas al tráfico que se encuentra clasificado dentro de las reglas asignadas, ya sea a un *pipe* o canal virtual. Hay dos acciones que se pueden definir y son: control de acceso y calidad de servicio; solo si el control de acceso se pone ***Accept***, la calidad de servicio puede ser aplicada.

- Control de acceso: los mecanismos ejecutados son, *accept*, *drop* y *reject*.

- Calidad de servicio: se puede aplicar las siguientes acciones al tráfico:

    - Prioridad por *pipe* o canal virtual
    - Prioridad por conexión (sólo canal virtual)
    - Ancho de banda mínimo y máximo por *pipe* o canal virtual
    - Ancho de banda mínimo y máximo por conexión (sólo canal virtual)
    - Garantía de ancho de banda por conexión (sólo canal virtual)
    - *Traffic shaping* usando CBR o *burst level* (sólo canal virtual)
    - Marcas de TOS por canal
    - Control de admisión (número de conexiones)
    - Reserva bajo demanda (a nivel de *pipe*)
    - Admisión condicionada

Per Flow Queuing (PFQ): este algoritmo de calidad de servicio permite a cada flujo de una nueva conexión obtener su propia cola. Esta nueva cola va a ser tratada de forma similar a otros flujos que ya tienen políticas establecidas de prioridad, además define un proceso donde el *scheduler* vacía la cola de acuerdo a cada política de flujo. *Allot Communications* implementa también un algoritmo inteligente de procesamiento de la cola, con cronometrajes exactos de envío y recepción de paquetes.

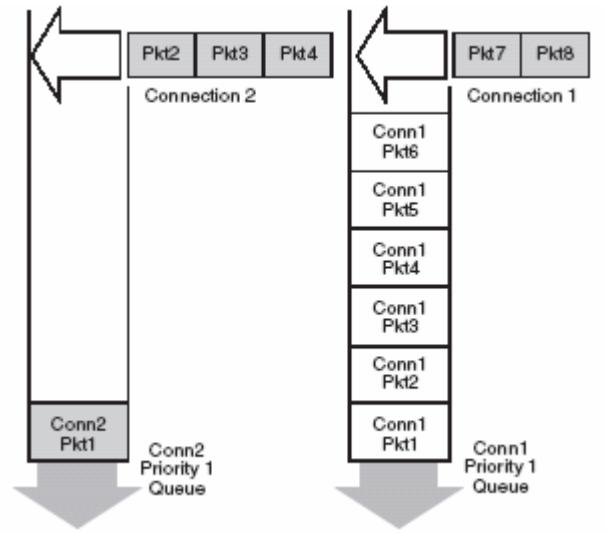


Figura 3- 5: *Per Flow Queuing* [9]

PFQ maximiza la utilización de enlaces WAN, y minimiza los desperdicios de ancho de banda, además se utilizan mecanismos estándar construidos en base a algoritmos de control de TCP. También se usa una única combinación de PFQ y *Smart Queue Scheduling*, para un control preciso de ancho de banda para tráfico entrante y saliente.

3.3.2.3 *Packeteer* [25]

Packeteer a través de sus *appliances* (*PacketShaper)* provee mecanismos para monitorear, modelar, controlar, comprimir, en sí administrar tráfico de diversas aplicaciones a través de enlaces WAN.

3.3.2.3.1 Clasificación y Visibilidad

Clasificación: Packeteer ofrece un amplio rango de mecanismos para clasificar tráfico entre los más importantes están:

- Reconocimiento avanzado de aplicaciones mediante firmas o indicadores de capa 7

- Subclasificación de aplicaciones como: *Oracle* y *PostgreSQL*, *Citrix*, FTP (por nombre de archivo o extensión), NNTP, VoIP (por protocolo o CODECs)

- Subclasificación HTTP por URL, tipo de contenido, tipo MIME, tipo de buscador y túnel http
- Subclasificación SSL

- A nivel de capa 4 por puertos UDP y TCP, rangos de puertos y listas de puertos

- En capa 3 por dirección IP, rango de direcciones, subredes, rangos de subredes, otras clasificaciones como direcciones MAC, listas de *hosts*, entre otras

- Por marcas de QoS, se incluye *DiffServ*, IP – ToS, IP – CoS (Clases de servicio), *IP Precedence*, etiqueta MPLS

- Por interfaz Frame Relay , PVC/DLCI, ATM PVC, interfaz ATM , ISL-VLAN, 802.1q-VLAN, 802.1p-LAN

La clasificación de *Packeteer* (*PacketSeeker*) es jerárquica, se va formando un árbol de clasificación de tráfico; cada categoría de tráfico se denomina clase de tráfico, (ver figura 3-6).

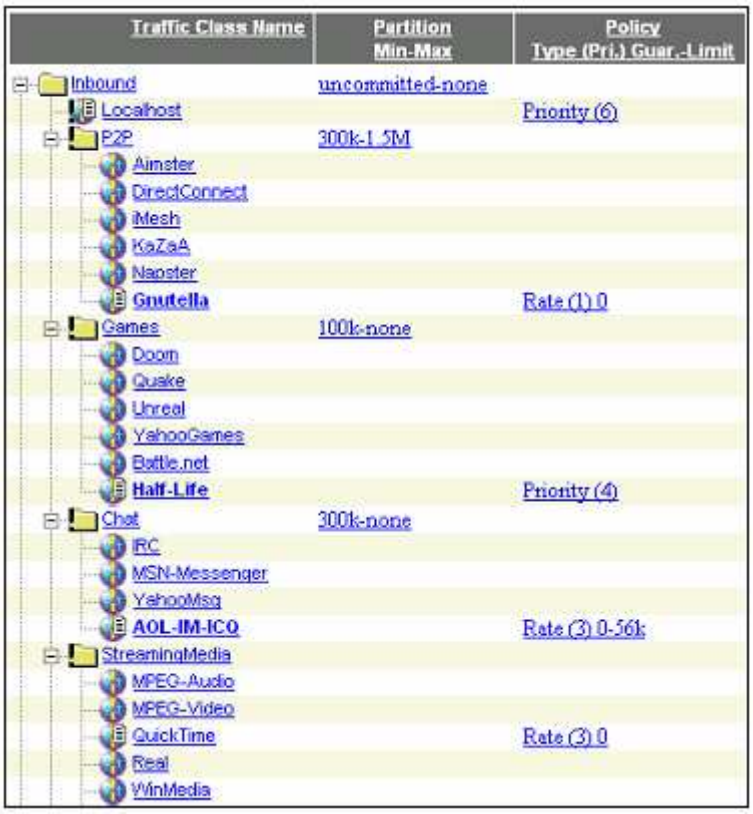


Figura 3- 6: Árbol de clasificación de tráfico [10]

Visibilidad: permitirá conocer cómo se está utilizando el ancho de banda, cuales aplicaciones están consumiendo demasiados recursos, y el efecto en otras aplicaciones, incluso si fuere necesario adquirir más ancho de banda.

- *Utilización de ancho de banda*: mediante mecanismos propios de la plataforma, hay la posibilidad de mostrar gráficamente las clases más usadas (*TOP 10* ver figura 3-7), incluso las clases hijas dentro de una clase, mediante la característica de *host accounting,* se podrán obtener datos estadísticos de utilización, ya sea por dirección IP, *host*, subred, permite desplegar gráficos estadísticos *de traffic rates*, *average rate*, *peak rate*, utilización, conexiones TCP, retransmisiones entre otras.

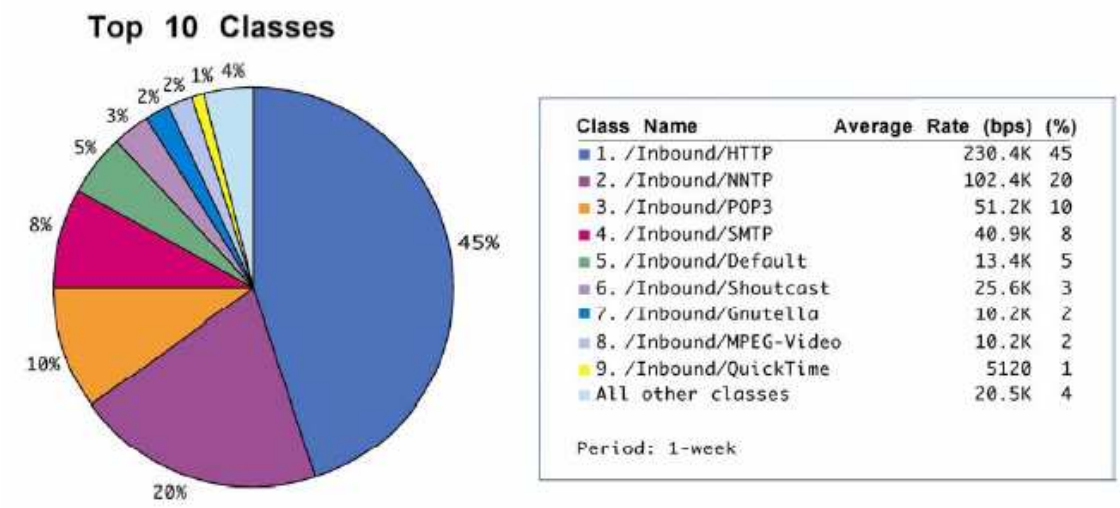


Figura 3- 7: *TOP clases* [7]

La figura 3-7, está demostrando que para el ejemplo se ha dividido en diferentes clases, cada clase contiene una aplicación, una vez que se ha tomado la muestra se obtiene que la aplicación HTTP en el tráfico entrante llega a consumir el 45% del total del tráfico que cruza por la red, de manera similar para POP3 que es el 10% del tráfico que ingresa a la red, con estos datos la herramienta genera una gráfica en forma de pastel el cual mostrará gráficamente la utilización en porcentaje de las 10 más importantes clases.

- *Rendimiento de la aplicación*: con la característica de RTM (*Response Time Management*), es posible ofrecer estadísticas de rendimiento, lo que permite al administrador de la red medir tiempos de repuesta por aplicación, *host*, subredes, y cualquier tráfico TCP. El conocimiento de estos datos es vital para evaluar niveles de servicio.

3.3.2.3.2 Mecanismos de control

Packeteer ofrece un amplio rango de herramientas y tecnologías para controlar tráfico, que permitirán asignación de ancho de banda máximo y mínimo[1], priorización, control sobre tráfico entrante y saliente, control sobre aplicaciones

[1] Esto lo hace por aplicación, sesión, usuario, localización, y cualquier subconjunto de tráfico.

que intentan monopolizar el canal. Una de las características importantes es la detección de virus, gusanos, ataques de negación de servicio, y limitar el impacto que estos pueden causar en la red.

- *Reservación o límite por clase*: se crea una partición[1] que permite manejar el tráfico por una especie de canal independiente, se puede configurar *burst* sobre el ancho de banda asignado, no desperdician el ancho de banda cuando no lo usan, lo comparten con otro tráfico.

- *Rate policies por sesión*: mediante éste mecanismo se puede entregar una velocidad mínima por cada sesión de una clase de tráfico, permitiendo limitar el ancho de banda que ésta pueda usar, o entregar garantías mínimas para que el servicio pueda ser usable.

- *Priority policies por sesión*: permite asignar ancho de banda de acuerdo a cierta prioridad asignada, los niveles de prioridad van de 0 a 7. Existen otras políticas como: *discard policies, never-admit policies, ignore policies*.

- *TCP Rate Control*: permite controlar tráfico de manera eficiente, mediante reportes a la estación al otro extremo, que hay congestión, y que tiene que disminuir la velocidad con la que envía los paquetes. La forma en que lo hace es la modificación del tamaño de la ventana TCP.

- *UDP Rate control y encolamiento*: controlar tráfico UDP es uno de los retos más grandes, sin embargo *Packetshaper*[2], controla tráfico de salida mediante disminución de la velocidad con la que salen los paquetes desde un destino hacia un canal congestionado. Sin embargo, en tráfico entrante no tiene control, pues antes de llegar a la plataforma de control ya ha cruzado por un enlace congestionado; lo que se usa son mecanismos de encolamiento, pero hacia el destinatario final. Los mecanismos más apropiados para manejar tráfico UDP son políticas de priorización, y *rate policies*, de tal manera que se

[1] Hay dos tipos de particiones jerárquicas y dinámicas.
[2] Producto diseñado por *Packeteer*, para controlar tráfico

le asigne solo un mínimo de ancho de banda para tráfico que tiende a monopolizar el canal.

3.4 DISEÑO EN DETALLE

En base a la problemática expuesta en el numeral 3.1 de este capítulo, se presentará una alternativa para proporcionar un sistema de administración del ancho de banda, que a más de garantizar una apropiada distribución de recursos a los usuarios, también permita al ISP competir en el mercado de nuevos servicios proporcionados por otros ISPs.

Para mejorar el sistema de seguridad actual, se propone un esquema que complemente los mecanismos de seguridad ya existentes en el ISP, enfocado a proteger especialmente al área de plataformas de servicio y la red administrativa del mismo.

3.4.1 ADMINISTRACIÓN DE TRÁFICO

La problemática del ISP, es la falta de administración de tráfico entrante y saliente, además de no poseer mecanismos para implementar nuevos servicios hacia clientes potenciales sin afectar el ancho de banda disponible, o a su vez ofrecer servicios que posteriormente se verán afectados con la presencia de enlaces saturados.

Para solventar los problemas expuestos, se escoge como mejor opción[1] introducir en la red, un sistema de administración de ancho de banda constituido por *hardware* y *software* (*PackeShaper*) que comúnmente se sitúan donde se requiere obtener visibilidad y control de tráfico, especialmente detrás de enrutadores de enlace WAN o enrutadores de enlace con Internet.

El sistema de administración de ancho de banda se integra transparentemente con la infraestructura existente de red, no impone cambios, ya sea en la

[1] Se detalla en el capítulo 4

configuración de enrutadores, topologías, servidores, o *hosts*. Es un complemento con otros *appliances* que se pueden encontrar en la red como son: balanceadores de carga, *firewalls*, entre otros.

3.4.1.1 Esquema propuesto

En la propuesta para administrar el ancho de banda en el ISP READYNET, no se cambiará la infraestructura ya instalada, sino más bien se añadirá a la red existente un sistema de administración de ancho de banda, que preste las facilidades y cubra la mayoría de los requerimientos que se encuentran en el ítem 3.1.2.1, como se muestra en la figura 3-8, el equipo administrador de ancho de banda va detrás de los enrutador de acceso a Internet, permitiendo cubrir los siguientes aspectos:

- Obtener visibilidad sobre el tráfico entrante y saliente de la red del ISP.
- Una vez establecidas las políticas de administración de tráfico, se permitirá controlar el uso del ancho de banda disponible.
- Y como complemento a la parte dos de este proyecto, servirá como una de las primeras líneas de defensa en el ámbito de seguridad del ISP.

3.4.1.1.1 Consideraciones del diseño técnico

Como factores a considerarse en el diseño se pueden anotar los siguientes:

- Planificación para segmentar ancho de banda en la red del ISP
- Establecimiento de políticas de administración de ancho de banda y tráfico de la red
- Especificaciones de la red

❖ *Planificación para segmentar ancho de banda en la red del ISP*

Se deben tomar en consideración las metas y servicios a cumplir, entre las más importantes se tienen las siguientes:

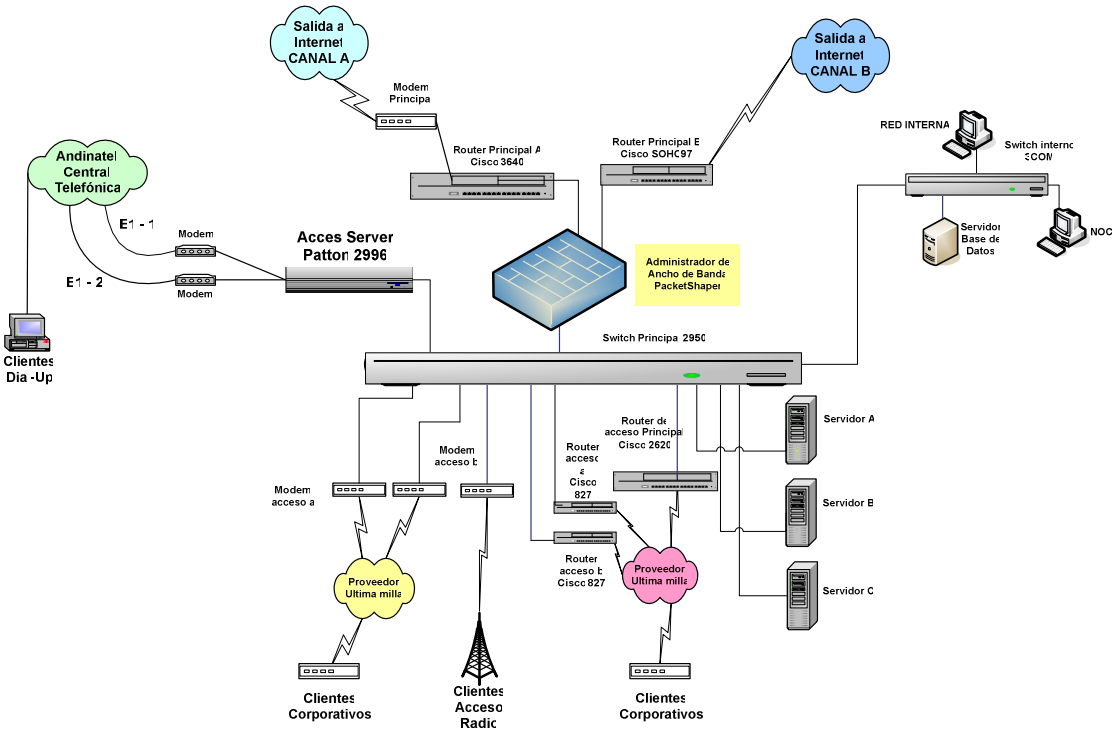


Figura 3- 8: Esquema de red propuesto

- Proveer niveles de servicios contratados
- Crear nuevos planes de acceso que disminuyan costos
- Ofertar servicios con prioridades

- En primera instancia se agruparán tipos de servicio por categorías, siendo las siguientes: Corporativo Premium, Corporativo Plus, Corporativo, básico o *home*, *dial – up*, posterior a esto se clasificará a los clientes en subredes, las cuales servirán como mecanismo de identificación del cliente dentro de una categoría.

  - Corporativo Premium: clientes enlazados al ISP vía radio, ya que el ancho de banda consumido por este tipo de clientes no es bien controlado a nivel del proveedor de última milla.

  - Corporativo Plus: clientes con canales simétricos, y con cero nivel de compartición en ancho de banda.

- Corporativo: clientes con canales asimétricos y niveles de compartición de hasta 2:1.

- Básico o *home*: clientes con niveles de compartición de 4:1 y 8:1, motivo por el cual, esta categoría se segmentará en dos subcategorías.

- *Dial –up*: clientes que accedan a la Internet mediante la PSTN.

- Red Interna (CAC y administración) del ISP

  - Dependiendo de la demanda se creará, una categoría de clientes especiales a los cuales se les ofertará servicios con prioridad de aplicaciones que estos necesitaren.

❖ *Establecimiento de políticas de administración de ancho de banda y tráfico de la red*

Al introducir la plataforma de administración de ancho de banda, primero se analizará cuál es el comportamiento de cada categoría sin establecer controles, para posteriormente implementar mecanismos de control, sin afectar los niveles de calidad de servicio, pero tampoco afectando el nivel de negocio del ISP.

En cada categoría se marcarán los niveles mínimos y máximos de ancho de banda que podrán consumir. Además se crearán políticas de control de tráfico P2P[1] entre los más importantes.

❖ *Especificaciones generales de la red*

Los datos más relevantes sobre la red son:

[1] Estas políticas podrán variar ya que el comportamiento de la red no es el mismo todo el tiempo, razón por el cual el monitoreo del funcionamiento del sistema es de vital importancia.

- Número de canales que serán administrados por la plataforma: 2 canales con proveedores distintos.

- Ancho de banda total manejado en la red del ISP, hacia la Internet: 2432 kbps, contratados con los dos proveedores de acceso.

- Conexiones simultáneas: en base a una muestra tomada como máximo 1700, como se puede observar en la figura 3-9 en la cual se presentan dos datos; las conexiones pico que han ocurrido en un determinado intervalo de tiempo que en este caso son las *Live Conns* y las nuevas conexiones que se generan por segundo que son *New Conns Per Sec*, las que se consideran para el diseño son las conexiones pico, sin embargo, esto puede aumentar, pero la capacidad de los equipos sería notablemente mayor como se verá posteriormente.

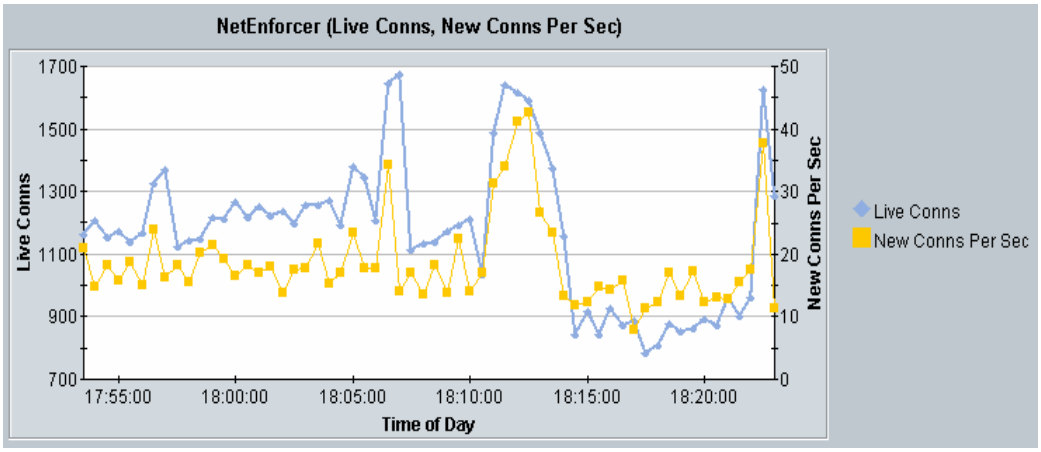


Figura 3- 9: Número de conexiones

3.4.1.1.2 Selección de la plataforma

La plataforma a ser seleccionada para formar parte de la infraestructura del ISP deberá cumplir los siguientes requerimientos:

- Manejar mínimo el ancho de banda actual más un porcentaje de crecimiento (20 % por año)[1], dimensionado para 5 años como mínimo.

$$\text{Total AB} = 2432 + 5 * 486.4 = 4864 \approx 5000 \text{ kbps}$$

  Este valor es aproximado, sin embargo estaría sobredimensionado ya que la estrategia será administrar de forma correcta el ancho de banda, de tal forma que la compra de ancho de banda sea por requerimiento, no por falta de administración del ancho de banda disponible.

- El número de conexiones es un dato importante, sin embargo las plataformas de administración de ancho de banda que pueden escoger como solución, manejan alrededor de 64000 conexiones simultáneas, que para la red del ISP de estudio está sobredimensionado.

- Número de interfaces, mínimo 2

Dado el esquema que requiere el ISP, el número de políticas o esquemas de segmentación no sobrepasarán lo ya establecido en algunas de las marcas de administradores de ancho de banda, que manejan capacidades desde 6 a 10 Mbps.

3.4.2 MEJORAS AL SISTEMA DE SEGURIDAD

Disponer de una estrategia de administración del riesgo que incluya una protección adecuada de los servicios que el ISP oferta, resulta esencial para el éxito de la organización. La clave para implementar mecanismos correctos de seguridad consiste en seguir una estrategia de defensa en profundidad, que defina múltiples niveles de seguridad, y que no dé por supuesto que cierta área por sí sola protege por completo la infraestructura.

[1] Dato obtenido en el último año de crecimiento, y considerando usuarios del tipo *home*.

Para implementar esta estrategia de defensa en profundidad, la arquitectura se debe dividir en redes físicas o segmentos de red independientes[1]. De este modo, se segmenta el sistema, y se consigue crear a nivel de islas el sistema de seguridad.

3.4.2.1 Esquema propuesto

Se prestará atención fundamental en dos áreas distintas, completamente definidas:

- Seguridad de la red
- Seguridad basada en *host* (relacionada con las plataformas de servicio)

Se debe recordar que el ISP, ya tiene implementados algunos mecanismos de seguridad en los dos ámbitos, por lo que el esquema propuesto tiene como finalidad mejorar el sistema actual.

3.4.2.1.1 Seguridad de la red

Para la seguridad de la red se basará en la división mediante segmentos, y la protección de cada uno de ellos frente a ataques mediante diversos dispositivos de red, como son enrutadores (con restricciones de redes, puertos, etc.), además se introducirá un sistema de *firewall* como si se tuviere un servidor de seguridad dedicado.

Un esquema completo podría incluir un filtro de contenido acompañado de un IPS, con la finalidad de prestar servicios de seguridad a potenciales usuarios, por ejemplo, filtrado *Web*. El IPS (*Intrusion protection system*), con el objeto de prevenir y detectar intrusos en la red del ISP, sin embargo aunque estos sistemas de seguridad resulten importantes en la red, los costos elevados de los mismos no son viables económicamente por el momento, razón por la cual se los deja para una futura implementación de estos sistemas, (ver figura 3-10).

[1] Pueden ser a nivel de VLANs, siempre y cuando los recursos del ISP lo permitan.

Como precedente se tiene que existen listas de acceso en el enrutador principal A; bajo los mismos criterios se deberán añadir listas de acceso en el enrutador principal B, principalmente considerando lo siguiente:

- Limitar acceso a la infraestructura de red desde redes externas por medio de *Telnet* o SSH.

- Limitar acceso por puertos mayores a 1023, a menos que se requiera que se abra alguno por necesidad.

- Extender la seguridad a las plataformas de clientes si se deseare.

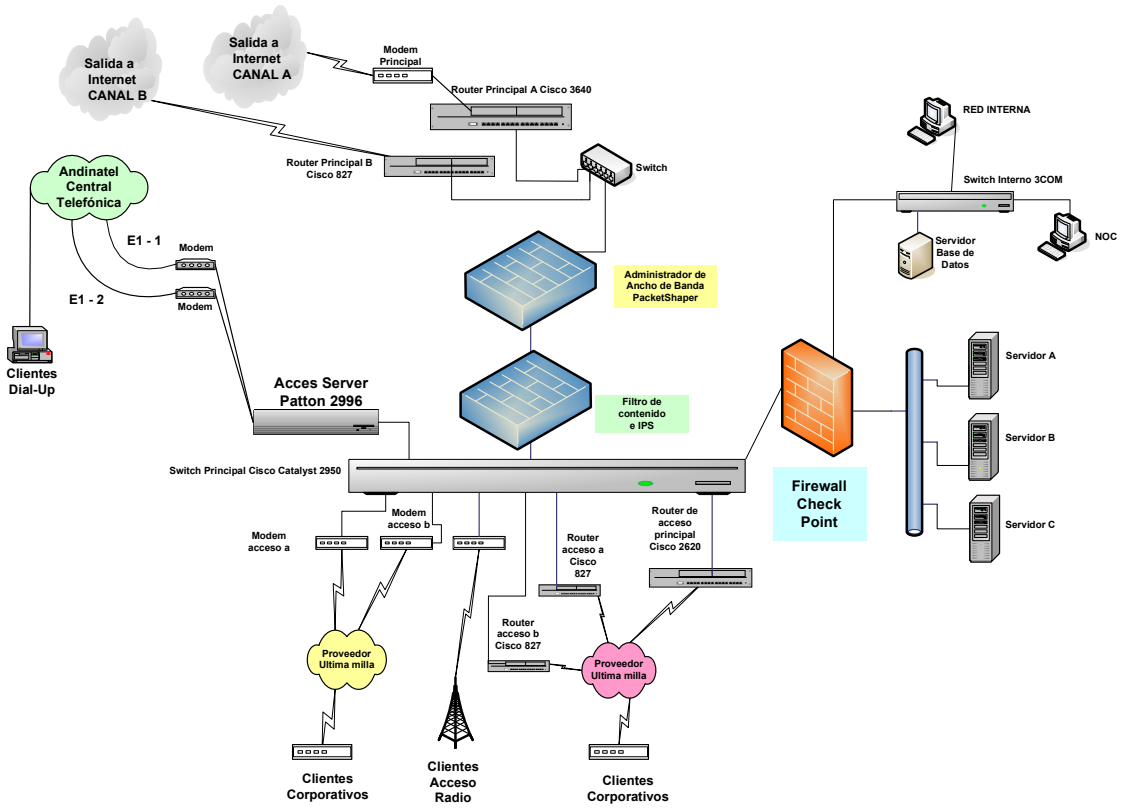


Figura 3- 10: Esquema propuesto

Como segunda fase, la segmentación física de los servidores, y la red interna de la organización de la red de acceso de clientes y del acceso directo a la salida principal de Internet.

❖ *Segmentación de la red de servidores*

Los servidores serán colocados en un *switch*, el cual estará conectado directamente a un sistema de *firewall* (configurada una DMZ), que tiene que cumplir con los siguientes requerimientos:

- *Filtrado de paquetes*: se bloquearán direcciones IP fuente o destino que no fueren autorizadas al acceso de las plataformas de servicio, se incluye números de puertos origen y destino, además de protocolos.

- *Stateful inspection*: permitiendo controlar el número de sesiones, especialmente las de origen extraño, además trabajar a nivel de capas superiores.

- Debe tener incorporado 3 puertos LAN 10/100 Mbps, el motivo es que se manejará tres segmentos de red, el primero es la red de servidores, segundo la red interna (área administrativa), y como último el tercer puerto para que se enlace con el *switch* principal *cisco catalyst* 2950.

❖ *Segmentación de la red interna*

Principalmente para entregar protección al servidor de facturación y contabilidad de la organización. Además de eso, proteger los equipos del CAC, ya que estos tendrán acceso a los servidores y equipos de red de la organización para la administración de los mismos.

Para el CAC y equipo del administrador de red permitir el uso de protocolos como SSH, *Telnet*, para administración de las plataformas de red, además acceso a los

servicios que presta el ISP, para motivos de monitoreo del correcto funcionamiento de la red.

3.4.2.1.2 Seguridad basada en host

La seguridad basada en *host*, tiene la finalidad de proporcionar a cada servidor de la arquitectura tanta seguridad inherente como sea posible, sin basar completamente su protección en la red.

A más de la seguridad ya provista por el enrutador con ACLs, la seguridad prestada por el *firewall*, las plataformas de servicio deberán estar configuradas de tal forma que solo los servicios prestados estén levantados.

Para los servidores de la organización, los servicios levantados en cada uno serán los siguientes:

Servidor A:

- Servicio DNS (puerto respectivo), dado que este servidor es el servidor de dominio primario.

- Servicio de correo (POP3, SMTP, IMAP), este servidor es el servidor de correo principal.

- Protocolo HTTP, puerto 80, este servidor maneja la autenticación de usuarios *dial – up*, y levanta la página *Web* que permite la creación de los diferentes tipos de usuarios.

Servidor B:

- Servicio DNS (puerto respectivo), servidor de dominio secundario.

- Servicio de correo (POP3, SMTP, IMAP), maneja el *webmail* de la organización.

- Protocolo HTPP, puerto 80, es el servidor de páginas *Web*.

- Protocolo FTP, presta el servicio FTP para actualización de páginas *Web* alojadas en el mismo.

- Puerto 3128 por utilización de Proxy que presta el ISP a sus usuarios.

Servidor C:

- Protocolo HTTP, puerto 80, levanta páginas *Web* bajo plataformas *Microsoft*.

- Protocolo FTP, dado que permite la actualización de páginas *Web* alojadas en el mismo de forma remota.

El resto de servicios deberán estar abajo, y el puerto correspondiente cerrado. El servidor de correo debe mantener actualizado el antivirus instalado, para el correcto funcionamiento del escáner de virus que lleguen, en correos destinados a clientes de la organización, o que salieren mediante el servidor de correo.

3.4.2.2 Dimensionamiento de la plataforma

Dados los dos segmentos de red a ser protegidos por la plataforma, se puede dimensionar de la siguiente manera:

- Segmento de red que contiene plataformas de servicio, con nivel de protección del 25%, este porcentaje se limita exclusivamente porque la protección será a nivel de acceso para administración de las mismas, y seguridad a nivel de ataques de negación de servicio, entonces el máximo *throughput* de datos es 50%, entonces aproximadamente 50 Mbps.

- Segmento de red designado para el CAC y red de administración, con nivel de protección del 75%, esto se debe a que se encuentra el servidor de base de datos de la empresa, pero por aspectos económicos, este mismo equipo hace las veces de *proxy* interno por el cual acceden al Internet los usuarios de la red interna. Se dimensiona con utilización del 50% hacia plataformas de servicio, entonces alrededor de 50 Mbps. De los datos expuestos se tiene que el máximo *throughput* de datos es 100 Mbps.

Las sesiones a manejar son:

- 20 usuarios de la red interna, si a cada usuario se le asigna como máximo 10 sesiones se tendrían un total de 200 sesiones.

- Las sesiones manejadas hacia las plataformas de servicio son internas y externas, las internas son mínimas por el número de usuarios, pero las externas se segmentan de la siguiente manera:

    - Clientes de la organización = 100 corporativos[1] * 30 clientes internos de los mismos = 3000, se tiene aproximadamente 300 cuentas *dial - up*[2], como total se tienen aproximadamente 3300 usuarios, si se le asigna un máximo de 10 sesiones a cada uno entonces se tienen 33000 sesiones, las sesiones manejadas desde la Internet a los servidores de la organización es mínima, ya que las aplicaciones que se alojan ahí no son de mayor interés, más que para los usuarios del ISP.

- Total de sesiones a manejar: 33200.

[1] Clientes corporativos que hasta Octubre del 2005 tiene el ISP, obviamente se considera un aproximado de usuarios de la red interna del cliente.
[2] Cuentas *dial – up,* que acceden a los servicios que ofrece el ISP.

3.4.2.3 Productos disponibles en el mercado

Los sistemas de *firewall*, disponibles en el mercado son:

3.4.2.3.1 Check point [26]

Sistema de protección basado en *software*, que puede ser instalado en algunas plataformas como Nokia, Sun, HP, Dell. Entre las características más importantes se tiene:

- Protección de ataques con inteligencia a nivel de aplicación
- Control de acceso basado en *stateful inspection*
- Administración inteligente
- Prevención de intrusos
- Calidad de servicio
- NAT (*Network Address Translation*)
- Inspecciona aplicaciones *Web*, mensajería instantánea, tráfico P2P
- *SmartDefense* bloquea automáticamente y registra en *logs*, ataques a nivel de red como son DoS, paquetes de gran tamaño, SYN floods, entre otros.
- Manejo de VPNs
- Información de ataques en tiempo real

3.4.2.3.2 CiscoPIX [27]

La serie *Cisco* PIX 515E *security appliance* brinda una gran gama de políticas robustas a nivel de aplicación, provee protección de ataques y conectividad segura a través de un amplio rango de servicios, entre los más importantes se tienen los siguientes:

- Servicios avanzados de *firewall* a nivel de aplicación
- Seguridad multimedia y VoIP
- Seguridad en acceso remoto mediante VPNs (IPSec)
- Soluciones de administración flexibles

- *Stateful Inspection*
- Protección de ataques multi-vector
- Administración basada en *Web*
- Soporta ACLs en la interfaz (*inbound* y *outbound*)

Figura 3- 11: Cisco PIX 515E Security Appliance [11]

3.4.2.3.3 Multi -tech systems [28]

Presenta como solución de *firewall* el siguiente sistema: *RouteFinder™ Internet security appliance* (ver figura 3-12), diseñado para maximizar la seguridad de la red sin comprometer el rendimiento de la misma. Entre las características más importantes se tienen:

- Soporta IPSec y PPTP VPN *tunneling*
- Utiliza encripción 3DES y AES
- Con tecnología *Stateful Packet Inspection* que incluye reglas de filtrado de paquetes, DNAT, SNAT e *IP MASQUERADE*
- Un año de suscripción como filtro de contenido
- Filtrado de *spam*
- Sistema automático de actualizaciones para proteger la red contra nuevas amenazas y DoS.
- Seguridad a nivel de capa aplicación (SMTP, HTTP, DNS, *proxies* SOCKS)
- 3 puertos *Ethernet* (LAN, WAN, DMZ)
- Reportes y monitoreo de tráfico
- 2 años de garantía

Figura 3- 12: RouteFinder™ Internet security appliance [12]

3.4.2.3.4 Fortinet [29]

Ofrece varias soluciones que pueden incorporase en una misma plataforma como son: *firewall*, antivirus, *antispam*, control de contenido e incluso un sistema de prevención de intrusos.

- *Sistema de control de contenido*: incluye control de acceso a sitios *Web* no apropiados que pueden poner en peligro la seguridad de la red, y consumir ancho de banda valioso de la organización.

- *Sistema de prevención de intrusos*: inspecciona paquetes entrantes y salientes que pudieren contener contenido malicioso o malintencionado, permite obtener datos reales mediante el monitoreo de tráfico que será recogido en *logs*.

El equipo escogido por las ventajas que presenta ante los otros como son: mayor visibilidad por la interfaz gráfica muy amigable, la escalabilidad que presenta ya que permite añadir más puertos LAN, si se llegare a un crecimiento que amerite la utilización del mismo, es la solución que presenta *Check Point* bajo la plataforma DELL[1].

[1] Se analizará con más detalle en el capítulo 4.

3.5 SLAS (SERVICE LEVEL AGREEMENTS) [30]

3.5.1 INTRODUCCIÓN

Un acuerdo de nivel de servicio es un contrato entre un proveedor de servicios y un cliente, que define los términos de responsabilidad del proveedor de servicios hacia el usuario, el tipo y alcance de la penalización, si estos no se llegaren a cumplir.

La percepción de los roles, varían en gran manera desde el punto de vista del proveedor de servicio y el usuario, por ende, es de vital importancia definir los roles a llevarse a cabo. En la mayoría de ocasiones el usuario olvida que para acceder a cierto servicio tendrá que hacer uso de múltiples proveedores, tecnologías, entre otras cosas, aunque esto aparentemente sea transparente para este; razón por la cual el proveedor de servicio deberá considerar lo siguiente al momento de establecer un SLA, alcance del SLA, disponibilidad, clases de servicio, atención y servicio al cliente, emisión de créditos, entre otras cosas.

3.5.1.1 Alcance del SLA

Se definirá hasta donde llega el acuerdo de nivel de servicio, el proveedor solo podrá garantizar lo que puede controlar, si llegare ofrecer más de eso, probablemente llegará a incumplir lo acordado. Sin embargo pueden existir extensiones de SLAs, es decir una cadena donde el proveedor se convierte en cliente de otro proveedor, y a su vez éste garantiza el correcto funcionamiento dentro del ámbito controlado por el mismo, ver figura 3-13.

3.5.1.2 Disponibilidad

Se presenta como un porcentaje en un acuerdo de nivel de servicio, está relacionado con el tiempo en el cual el servicio estará disponible, como base se tendrá un período de tiempo de medición, en la mayoría de los casos será

mensual[1], o anual. Dependiendo de la responsabilidad de la falla, el cliente puede acceder a una nota de crédito, es decir un descuento en la facturación.

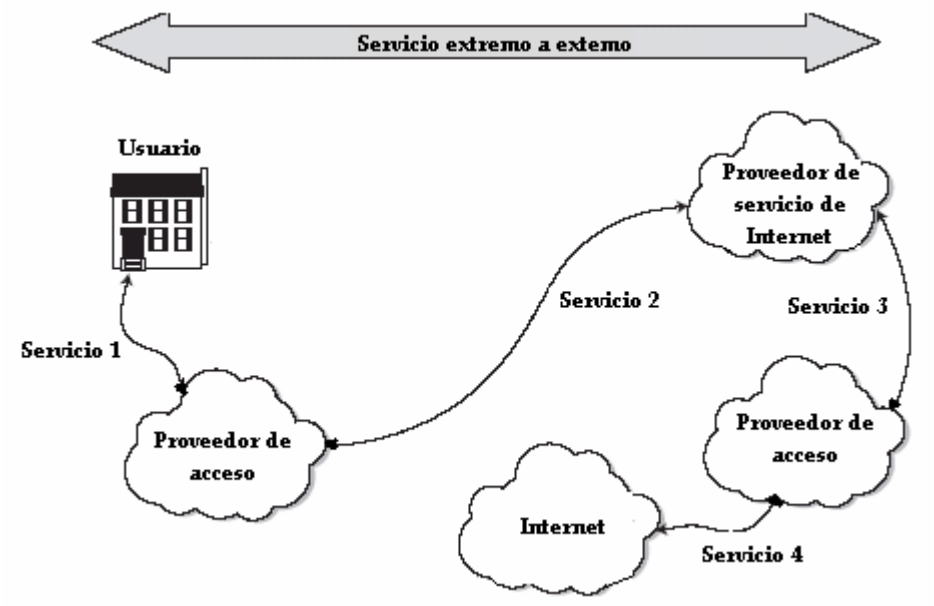


Figura 3- 13: Servicio extremo a extremo [13]

3.5.1.3 Clases de servicio

Las redes IP trabajan bajo el esquema *Best Effort*, sin embargo si el proveedor dentro de su red puede priorizar cierto tipo de tráfico, se clasificaría el servicio por la calidad que se entrega. Entre los parámetros más usados para medir las clases de servicio están: retardo, *jitter*, pérdida de paquetes, entre otras.

Retardo: se considera la cantidad de tiempo que demora un paquete en llegar al destino final (receptor) luego de haber sido despachado por el emisor. En el caso de acceso a Internet esto es casi impredecible ya que la Internet versión 4, no se la diseño con el objeto de satisfacer calidad de servicio, pues depende de varios puntos en el trayecto, inclusive si el servidor al que se hace la petición se halla ocupado, entonces la respuesta a dicha petición tardará más tiempo.

[1] Ya que la mayoría de servicios se facturan mensualmente, pudiendo variar.

Jitter: es la variación del retardo que existe entre el arribo de un paquete y el siguiente paquete que arriba al destino, por ejemplo si un paquete llega en 100ms y el siguiente en 125ms, la variación será de 25ms, en la red de acceso a Internet existen variaciones dependiendo de si el canal esta congestionado o no, de la capacidad de respuesta de los equipos servidores que atienden las peticiones hechas a las mismas entre otros factores.

Pérdida de paquetes: es una comparación entre el número de paquetes transmitidos y recibidos con éxito de la totalidad de paquetes enviados, usualmente se expresa el porcentaje de paquetes que fueron descartados, la pérdida de paquetes está típicamente en función de la disponibilidad, por ejemplo si una red es altamente disponible (normalmente en períodos de no congestión), entonces es posible que la pérdida de paquetes sea cero, pero si la red experimenta congestión posiblemente la pérdida de paquetes puede llegar a ser alta.

En el caso de un ISP los términos que se han definido aquí no se pueden garantizar, especialmente por que se trabaja paralelamente con varios proveedores, como se muestra en la figura 3-13, además, aquí en el Ecuador no existe una norma vigente que estipule los parámetros de calidad de servicio que se entregaran al usuario[1], y dado que los ISP no obtienen ninguna garantía a más de la disponibilidad del servicio, un ISP local no puede hacer una extensión de los mismos a los usuarios finales.

3.5.1.4 Atención y servicio al cliente

Este punto tiene algunos segmentos, en primera instancia se tiene un *call center* donde se recibirán las notificaciones de problemas en el servicio, a esto sigue soporte técnico en sitio o remoto, el tiempo de respuesta máximo es de vital importancia. El proveedor tiene la obligación de notificar fechas y horarios de mantenimiento, en horas de menos tráfico, para tener el menor impacto en el

[1] El CONATEL a Marzo del 2006, extiende una propuesta de regulación respecto a la calidad de servicio en Internet, ver ANEXO B.5.

usuario. Se deberá entregar reportes de disponibilidad con el fin de informar el motivo de averías en el sistema, y la duración de las mismas.

3.5.1.5 Emisión de créditos

Éstos son valores a descontarse en la facturación, debido al incumplimiento de algún parámetro que se encuentre en el SLA.

3.5.1.6 Obligaciones del Cliente

El cliente deberá informar sobre mantenimientos que se haga a la red o infraestructura del mismo, con el fin de registrar tiempos de indisponibilidad del servicio, pero provocados por el cliente. Debe garantizar que las instalaciones, alimentación eléctrica, etc, sean adecuadas para el correcto funcionamiento de la infraestructura que instala el proveedor.

3.5.2 ACUERDOS DE NIVELES DE SERVICIO PARA EL ISP “READYNET”

Hasta la fecha, el ISP no entrega formalmente un contrato que contemple cláusulas que envuelvan acuerdos de niveles de servicio, sin embargo en las ofertas de servicio entregadas al usuario, se contemplan parámetros como disponibilidad, y servicio al cliente.

Considerando que READYNET CIA. LTDA, es un ISP local y depende de otro ISP de mayor tamaño, debe extender hacia el cliente final los parámetros que el proveedor ofrece a la organización.
READYNET CIA. LTDA como proveedor de servicios de Internet, no está en la facultad de entregar acuerdos de niveles de servicio relacionados con el proveedor de la última milla, más bien debe cubrir solo el ámbito que el ISP abarca. Sin embargo, dado que para cierto servicio denominado ADSL Básico READYNET tiene la facultad de revender servicios, se deberían extender los parámetros que el proveedor entregue al ISP.

3.5.2.1 Cláusula propuesta

Es de vital importancia que el contrato que se lleva a cabo entre READYNET CIA. LTDA, y el usuario, contemple cláusulas que indiquen los parámetros a considerarse en el ámbito de calidad y clases de servicio.

Para la elaboración de la siguiente cláusula se hace una extensión de los acuerdos de niveles de servicio provistos por los proveedores de acceso a Internet. En la tabla 3.2, se detalla los acuerdos entregados por cada proveedor.

	PROVEEDORES DE ACCESO A INTERNET	
SLAs	**Impsat**	**Andinadatos**
Disponibilidad	99,6%	99,5%
Soporte Técnico	Horario hábil de trabajo: Lunes a Viernes de 8h00 a 19h00, excluyendo feriados. Horario extendido Lunes a Viernes de 19h01 a 7h59, las 24 horas fines de semana y feriados.	24 horas al día, 7 días de la semana (esquema 7x24x365). Supervisión y administración del enlace las 24 horas del día.

	PROVEEDORES DE ULTIMA MILLA		
SLAs	**Andinadatos**	**Suratel**	**Stheal Telecom**
Disponibilidad	99,6% servicio ADSL y SDSL PLUS 98,3 % servicio ADSL básico	99,6%, servicio Premium.	97%
Reacción frente a fallas	2 horas servicio plus. 4 horas servicio básico.	30 minutos valoración del problema.	No disponen de un reglamento vigente sobre el tema.
Tiempo máx. solución de problemas de	4 horas servicio plus. 6 horas servicio básico.	4 horas problemas tramo red urbana	No disponen de un reglamento vigente sobre el tema.

enlace			
Tiempo máx. solución problemas en el backbone	6 horas	6 horas	No disponen de un reglamento vigente sobre el tema.
Soporte Técnico	Para servicio Plus, 24 horas al día, 7 días de la semana (esquema 7x24x365). Supervisión y administración del enlace las 24 horas del día. En el caso de servicio básico en horario de 8h00 a 18h00.	Bajo el esquema 7x24x365, es decir los 7 días de la semana, 24 horas al día y los 365 días del año, el que le proporcionará los servicios de monitoreo y gestión de red.	24 horas y los 365 días del año, debiendo informar el cliente si por cualquier motivo el sistema dejara de operar a nuestros números de contacto para soporte técnico que son 2248583/233/887 y celular 098762555 que corresponde a nuestro Jefe Técnico, e-mail y soporte@stealthtelecom.net

Tabla 3- 2: SLAs de proveedores de acceso a Internet y última milla

CLÁUSULA DÉCIMA TERCERA: Calidad de servicio

LA EMPRESA pone a disposición las clases y calidad de servicio expuesto en la siguiente tabla, que EL CLIENTE puede hacer uso dependiendo del servicio contratado.

Clase de servicio	Disponibilidad *	Servicio y atención al Cliente
Corporativo Premium	99.5% anual	ANEXO 1
Corporativo Plus	99.5% anual	ANEXO 1
Corporativo	99.5% anual	ANEXO 1
Básico	98.3% mensual	ANEXO 1
Dial – up	99.5 % anual	ANEXO 1

* La disponibilidad se ofrece desde la red del ISP, no contempla disponibilidad provista por el proveedor de última milla, dado que EL CLIENTE es usuario final solo en última milla del proveedor (Suratel, Stheal Telecom, Andinadatos, etc).

ANEXO 1

LA EMPRESA fija los siguientes parámetros en servicio y atención al cliente:

1. **Atención al cliente**: EL CLIENTE podrá acceder a notificaciones, y reclamos en el área de facturación en el siguiente horario: lunes a Viernes de 9h00 a 13h00 y de 15h00 a 18h30.

2. **Soporte Técnico**: EL CLIENTE puede acceder a soporte telefónico y soporte presencial dependiendo del problema que se presentare.

    - Soporte Telefónico: Los 365 días del año, 24 horas (24*7*365), distribuidos de la siguiente manera:

        - PBX 2509810: Lunes a Viernes: 8h30 a 21h00 sin interrupción, Sábado, Domingo y feriados: 10h00 a 12h00 y de 15h00 a 17h00
        - Celular 097756229: los 365 días de al año, 24 horas (24*7*365)

    - Soporte Presencial: Lunes a Viernes de 9h00 a 17h00

En caso de presentarse problemas a nivel de última milla se tiene los siguientes parámetros a considerarse dependiendo del servicio contratado.

Servicio corporativo: esta sujeto dependiendo del proveedor de última milla, se anexa al contrato los datos del proveedor.

Servicio Básico: la última milla es provista por Andinadatos y se detalla a continuación.

- Reacción frente a fallas o peticiones de servicio: 4 horas laborables
- Tiempo máximo de solución de problemas de enlace: 6 horas laborables
- Tiempo máximo frente a fallas de red troncal o de *backbone*: 8 horas laborables
- Soporte técnico en horas laborables: 8h00 a 18h00

CAPÍTULO 4

ANÁLISIS TÉCNICO Y ECONÓMICO

4.1 VIABILIDAD TÉCNICA [31]

4.1.1 INTRODUCCIÓN

En varios proyectos la tendencia es aplicar los procedimientos y tecnologías más modernas, sin embargo este tipo de soluciones suelen ser óptimas técnicamente, pero no resultan económicamente viables. Motivo por el cual se analizará la solución expuesta en el capítulo 3, abarcando el área de administración de tráfico y seguridad en la red del ISP, y se presentará valores aproximados del costo de la implementación, para ser analizados posteriormente en el ítem 4.2.

El objetivo de este estudio es, definir si existen las condiciones mínimas necesarias para garantizar la viabilidad de la implementación, tanto en lo estructural como en lo funcional. Justificar técnicamente el impacto positivo de la implementación del proyecto en la red del ISP, y mostrar las ventajas hacia el usuario final.

Dado que pueden existir algunas alternativas a la ya expuesta en el capítulo 3, se presentarán las ventajas de la opción escogida, en comparación con una posible alternativa, que es el uso de plataformas CISCO configuradas de tal forma que intenten solventar el problema que existe en el ámbito de administración de tráfico en el ISP.

En la alternativa de seguridad se analizará cuál plataforma es conveniente introducir para mejorar el sistema de seguridad ya presente en la red del ISP, presentando las posibles ventajas sobre otras plataformas existentes en el mercado.

4.1.2 ANÁLISIS DE LA PROPUESTA

4.1.2.1 Administración de tráfico

En el capítulo anterior se presentó el diseño del sistema de administración de tráfico enfocado principalmente a un sistema de administración de ancho de banda con las respectivas políticas, sin embargo en este ítem, se presenta a breves rasgos una opción en base a enrutadores CISCO, con el fin de mostrar las ventajas del sistema de administración de ancho de banda *appliance*, sobre la mencionada solución en base a enrutadores.

4.1.2.1.1 Solución en base a enrutadores CISCO

El esquema que se puede ejecutar en la red del ISP es, segmentar la red, principalmente la red de clientes de la siguiente manera (ver figura 4-1), se propone los ruteadores 2500 y 3810, por disponibilidad de los mismos en la organización, y para los fines propuestos se los puede utilizar.

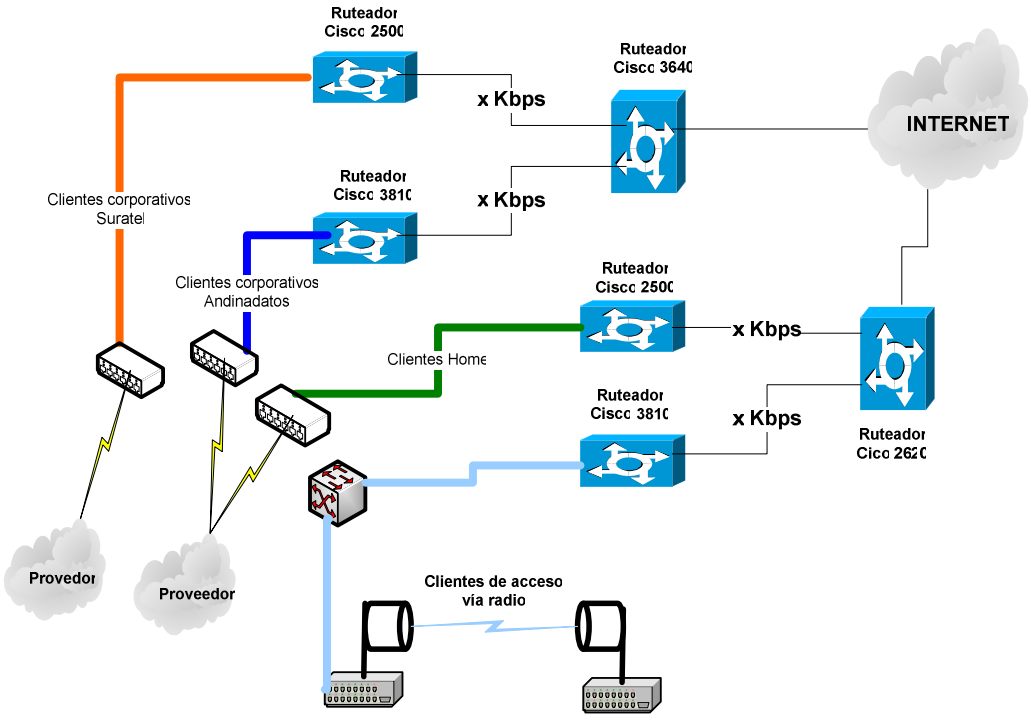


Figura 4- 1: Red de clientes segmentada con ruteadores

- *Red de clientes de acceso vía radio*: dado que el proveedor de última milla no restringe de forma exacta el ancho de banda contratado por estos usuarios, la opción seria que el enlace de estos llegue a un *switch*, y éste se conecte de forma directa a un enrutador y la salida se restrinja en base a la utilización de la interfaz serial del enrutador, y ésta interfaz conectarla a una de las interfaces seriales del enrutador principal, de tal forma que la conexión sea *back-to-back*.

- *Red de acceso clientes xDSL*: primero segmentar el acceso de tal forma que por un E1 ingresen sólo clientes denominados *home* o básicos y por otro E1 manejar los clientes corporativos, para posterior a esto, asignar el ancho de banda calculado, dependiendo del nivel de compartición. De forma similar a la anterior se segmentaría mediante enrutadores de acceso interconectando interfaces seriales.

A esta solución mostrada en la figura 4-1, se puede agregar, la actualización del IOS del enrutador principal para manejar calidad de servicio (aplicar *traffic shape*, por ejemplo), de esta manera brindar prioridades de tráfico para cierto tipo de aplicaciones. El inconveniente en esta solución es que no se puede controlar el tráfico *download*, que llega por el enlace WAN antes de ingresar a la red del ISP, por ende, la salida a Internet continuará saturada.

4.1.2.1.2 Comparación de alternativas

En la tabla 4-1, se mostrarán las características principales en cuanto a visibilidad, clasificación y control de tráfico de cada solución:

Las ventajas del sistema de administración de tráfico basado en introducir en la red, una plataforma de administración de ancho de banda, comparado con la solución de segmentación física de la red en base a enrutadores son:

- Fácil implementación, se adapta de forma transparente a la infraestructura de red. Con enrutadores se necesita dejar la red fuera algún tiempo, hasta probar como se adapta la reestructuración hecha a la red del ISP.

Solución	Visibilidad	Clasificación	Control
Enrutadores Cisco (Modelo 3640, 2620, 2500, 3810)	No en forma directa sino usando herramientas de visualización extras, como la que se usó en el capitulo 2.	Clasificación a nivel de capa 7, sólo mediante puertos ya conocidos, y esto se hace manualmente en base a configuración vía comandos. Se puede configurar NBAR	La mayoría de mecanismos de control es para tráfico de subida, no para tráfico *inbound*.
Administradores de Ancho de banda (*NetEnforcer* y *PacketShaper*)	Proveen mecanismos propios de la plataforma para mostrar de forma inteligente el tipo de tráfico que cruza por la red a ser analizada.	Los mecanismos de clasificación son a nivel de capa aplicación, mediante firmas, existen varios mecanismos de clasificación por puertos, dirección IP, etc.	Permite controlar tráfico *inbound* y *outbound*, mediante mecanismos de control como TCP *rate control* o PFQ (*Per Flow Queuing*), controla tráfico sin necesidad de bloquearlo completamente.

Tabla 4- 1: Comparación de soluciones para administración de tráfico

- En caso de falla, simplemente se aísla el equipo de la red, y el tráfico atraviesa por los enrutadores principales de forma normal. En el caso de algunos enrutadores en una red, implica más de un punto de falla.

- La falta de visibilidad de usuarios que acceden a la red, y como estos usan los recursos de la misma es una gran desventaja de la solución basada en segmentar la red con enrutadores.

- Los mecanismos de clasificación, como se mostró en la tabla 4-1, son mínimos en comparación con la solución de la plataforma de administración de ancho de banda.

- Si bien con la solución en base a enrutadores, se lograría controlar parte del ancho de banda, no se modelaría o administraría el tráfico en la red, por ejemplo, si bajo un canal se tiene una gran porción de clientes *home* y como es un hecho, la mayoría usa aplicaciones P2P por ejemplo, las cuales tienden a apoderarse de gran parte de los recursos del canal, entonces para el resto de clientes con otras aplicaciones el servicio se degradaría.

- El control de tráfico *outbound*, se puede controlar, sin embargo el tráfico *inbound* no es controlado con la solución basada en segmentar la red. La solución con la plataforma de administración de ancho de banda permite controlar el tráfico mediante comunicación con el punto extremo (TCP *rate control*), en el caso de tráfico TCP. Además existen otros mecanismos de control para otro tipo de tráfico.

4.1.2.1.3 Plataformas Seleccionadas para el ISP[1]

Las plataformas que cumplen los requerimientos del ISP, en el ámbito de visibilidad, clasificación y control de tráfico son: *NetEnforcer* (*Allot*) AC-202/10M y *PacketShaper* 2500 L006M, manejando 10 y 6 Mbps de enlace WAN respectivamente. A continuación se presentará las características generales de las dos plataformas (ver tabla 4-2).

Si bien existen ventajas y desventajas en cada plataforma, los requerimientos básicos que requiere el ISP se cumplen en las dos plataformas y con mayor peso la plataforma de *Packeteer* (comunicación con el *host* del extremo, usando TCP rate control), motivo por el cual para el ISP se presenta como mejor opción la

[1] En el ANEXO C.1, se encuentran las especificaciones técnicas de las plataformas de administración de ancho de banda (*NetEnforcer* y *PacketShaper*).

plataforma de administración de ancho de banda *PacketShaper 2500 6M*, dado que se quiere controlar los enlaces *WAN* (acceso a Internet por los CANALES A y B), los costos que involucra la adquisición de esta plataforma son analizados en el ítem 4.2.

El motivo por el que se da mayor peso al ámbito de control es porque es uno de los requerimientos más importantes del ISP, dado que existe mal uso de los recursos del ancho de banda actualmente. El hecho de que se haga un control con el punto extremo significa que si cierta clase está pidiendo más de lo que debería entonces en el extremo se disminuya la velocidad con la que los paquetes son despachados.

En el aspecto de clasificación ambas plataformas trabajan con esquemas similares, motivo por el cual no se halla ventaja o desventaja si se toma la una o la otra solución.

La visibilidad es importante y la interacción con el usuario, sin embargo aunque *Packeteer*, no es muy amigable genera la información necesaria en el caso específico del ISP de estudio. Hay que resaltar que la plataforma propuesta por *Allot*, ofrece una de las mayores ventajas en el ámbito de monitoreo, por la capacidad gráfica que presenta en los reportes en tiempo real.

	***PacketShaper* 2500 L006M**	***NetEnforcer AC-202/10M***
Visibilidad	La interfaz de usuario no es amigable sin embargo tiene las siguientes características: • Entrega reportes de utilización de Ancho de banda. • Gráficamente permite obtener las 10 clases con mayor porcentaje de utilización. • Ofrece estadísticas de rendimiento.	Ofrece una interfaz completamente amigable, donde muestra los siguientes datos: • Más de 100 vistas en tiempo real. • Entrega gráficos de la utilización de ancho de banda de usuarios. • Soporta colección de estadísticas mediante SNMP.

Clasificación	• Clasificación a nivel de capa 7. • Sub – clasificación de aplicaciones, distingue oracle, Citrix, VoIP. • Clasificación HTTP, por URL, MIME, etc. • Por dirección IP, MAC, subredes.	• Por dirección IP/MAC, se incluye rango de IPs, subredes, nombre de *host*. • Clasificación a nivel de capa 7, para aplicaciones P2P (KaZaA, eDonkey, WinMX y más), aplicaciones de negocio (Citrix, Oracle), VoIP y streaming (H.323, MSPlayer), y protocolos de Internet (FTP, HTTP, Instant Messaging y más) • Mediante contenido de la aplicación para HTTP (URL, tipo de contenido, *host*), para Oracle (base datos, nombre, nombre de usuario), y H.323 (audio/video, CODEC). Byte ToS – DiffServ o bits de *IP Precedence*.
Control	• Reservación o límite por clase. • *Rate policies* por sesión. • TCP *rate control*. • Encolamiento • Políticas de prioridad por sesión.	• Control de acceso. • Prioridad de aplicaciones. • Manejo de ancho de banda mínimo y máximo. • El mecanismo de control usado en encolamiento por flujo.
Características Generales	• 6 Mbps en AB de enlace WAN • Max 256 clases • 20000 flujos concurrentes • 640 matching rules	• 10 Mbps en AB de enlace WAN • 512 Pipes • 2048 políticas • 24000 conexiones simultáneas

Tabla 4- 2: Características de plataformas de administración de AB

4.1.2.2 Mejoras al sistema de seguridad

Con el objeto de mejorar el sistema de seguridad de la organización se propuso en el capítulo 3, el establecimiento y definición de la política de seguridad, la misma que marca los lineamientos a seguirse en las diferentes áreas del ISP, entre los requerimientos está la adquisición de una plataforma de seguridad (*firewall*) para separar la red de plataformas de servicio, y la red del área de administración y monitoreo. Entre las plataformas más comerciales se tienen Cisco con su *firewall* Cisco PIX 515E, y *Check Point Express*.

4.1.2.2.1 Comparación de alternativas

Las aparentes ventajas y desventajas que pueden tener cada una de las plataformas se orienta al manejo de las mismas, Cisco en la mayoría de los casos presenta una interfaz no muy amigable, la configuración se realiza en base a línea de comandos, en cambio *Check point*, presenta interfaz gráfica más amigable al usuario; como plataforma, el *firewall* de Cisco en un *appliance*, mientras *Check point*, es *software* que se puede instalar en diferentes plataformas, y sobre varios sistemas operativos, probablemente siendo una de las debilidades, porque en muchos de los casos el sistema operativo sobre el cual corre, puede en sí tener vulnerabilidades, llegando a ser este un punto de falla.

Los niveles de seguridad que ambas plataformas entregan a los segmentos de red a proteger en la organización, son aceptables como se muestran en los anexos adjuntos (ver ANEXO C.2). Para la red del ISP, es de vital importancia la visibilidad, por esto se escoge la solución que presenta *Check Point*, bajo la plataforma *Dell*.

Es de vital importancia introducir en la red mecanismos de control de contenido, con el objetivo de prestar servicios de seguridad, como filtrado *Web*, mecanismos más sofisticados y actualizados con mayores bases de datos, en el tema de *spam*, código malicioso, virus y gusanos. Se plantea la opción de una plataforma

de control de contenido a futuro, con el fin de crear como ventaja competitiva el nivel de seguridad que el ISP preste al usuario final.

4.2 VIABILIDAD ECONÓMICA [32]

4.2.1 INTRODUCCIÓN

El análisis completo de un proyecto conlleva algunas etapas como por ejemplo un estudio de mercado, evaluación técnica, evaluación financiera, esta última a más de generar información construye los flujos de caja y evalúa el proyecto. El impacto económico de un proyecto es de vital importancia para la organización, por ende es necesaria una correcta evaluación financiera, con el objeto de identificar desde el punto de vista del inversionista, los ingresos y egresos que va a generar el mismo, y lo más importante la rentabilidad que este ofrece.

En materia de evaluación financiera, se tiene que cumplir con lo siguiente: determinar hasta que punto los costos van a ser cubiertos y en que tiempo, de tal forma que se pueda diseñar un plan de financiamiento, otro de los aspectos es medir la rentabilidad de la inversión, y comparar con otras alternativas de inversión. Para medir la rentabilidad de un proyecto se tienen algunas alternativas y estas son: cálculo del valor presente neto (VPN), la tasa interna de retorno (TIR), relación costo beneficio, y periodo de recuperación del capital entre los más destacados.

En este proyecto se usará el método de evaluación del TIR, para lo cual es necesario obtener un flujo de fondo de donde se partirá para el cálculo de este indicador.

4.2.1.1 Definiciones

4.2.1.1.1 Tasa mínima aceptable de rendimiento (TMAR) [32]

La TMAR de un proyecto usualmente tiene referencia con la tasa máxima que ofrecen los bancos a una inversión a plazo fijo, dado que existe inflación, entonces se puede tomar como referencia el índice inflacionario, pero como el inversionista quiere que su dinero crezca mas allá del índice inflacionario, hay otro factor que influye en la TMAR; que es el premio al riesgo; para el caso de estudio es el porcentaje de riesgo país. La fórmula para el cálculo es la siguiente:

$$TMAR = i + f$$
$$i \approx \text{premio al riesgo}$$
$$f \approx \text{tasa de inflación}$$

4.2.1.1.2 Valor presente neto (VPN) [32]

El valor actual neto ó valor presente neto, es uno de los más usados en la evaluación de proyectos de inversión, consiste en determinar la equivalencia en el tiempo cero, de los flujos de efectivo futuros, que generará un proyecto comparándolo con el desembolso o la inversión inicial para el mismo, cuando dicha equivalencia es mayor que el desembolso o inversión inicial, entonces el proyecto es aceptable.

4.2.1.1.3 Tasa interna de retorno (TIR)

Evalúa el proyecto en base a una única tasa de rendimiento por período con la totalidad de los rendimientos actualizados. El TIR podría representar “la tasa de interés más alta que un inversionista podría pagar sin perder dinero, si todos los fondos para el financiamiento de la inversión se tomaran prestados y el préstamo se pagara con las entradas en efectivo de la inversión a medida que ésta fuera produciendo”[1].

[1] Bierman y Smidt, El presupuesto, página 39.

4.2.1.2 Planificación de la implementación del proyecto

Por la naturaleza del proyecto, éste se tiene que implementar en periodos diferentes, dado que la organización no dispone de recursos propios para implementar todas las etapas del proyecto al mismo tiempo. La planificación para el mismo se muestra en la figura 4-2.

De las dos áreas fundamentales a cubrir en este proyecto, en el primer año se adquiere la plataforma de administración de ancho de banda[1], por la necesidad que presenta en este aspecto la organización, no solo por factores de ahorro de recursos de ancho de banda, y proporcionar nuevos servicios a los usuarios, sino con el objetivo de competir en el mercado ecuatoriano con costos, pero sin degradar la calidad del servicio percibido por el usuario.

En el segundo año se proyecta la adquisición de la plataforma de seguridad (*firewall*), con el fin de asegurar las plataformas de servicio y crear un ambiente de confianza en la organización previniendo ataques de DoS y control de acceso no autorizado, entre los aspectos más importantes que se consideró en este proyecto. En el ANEXO C.4, se presentarán los costos que incurren la adquisición y puesta en marcha del sistema. Posterior a esto se debería planificar la implantación de la plataforma de filtrado de contenido que permita brindar servicios de seguridad a los clientes del ISP.

En la tabla 4-3, se especifica el costo total del proyecto, para el primer y segundo año, sin embargo como la implementación se realizará por etapas el cálculo del financiamiento se lo hará con miras a cumplir la implementación de la plataforma de administración de ancho de banda.

[1] ANEXO C.3, costos de plataformas de administración de ancho de banda.

Etapas	Descripción de la solución	Costo Unitario	Costo Total
1[era] etapa: Plataforma de administración de ancho de banda (*PacketShaper*)	*PacketShaper* modelo 2500, 6Mbps	$ 9246,00	$ 9246,00
2[da] etapa: *Firewall* (*Check Point* bajo plataforma *Dell*)		$ 10264,80	$ 10246,80
		TOTAL*	$ 19510,80

* Costo incluido impuestos

Tabla 4- 3: Costo total de implementación

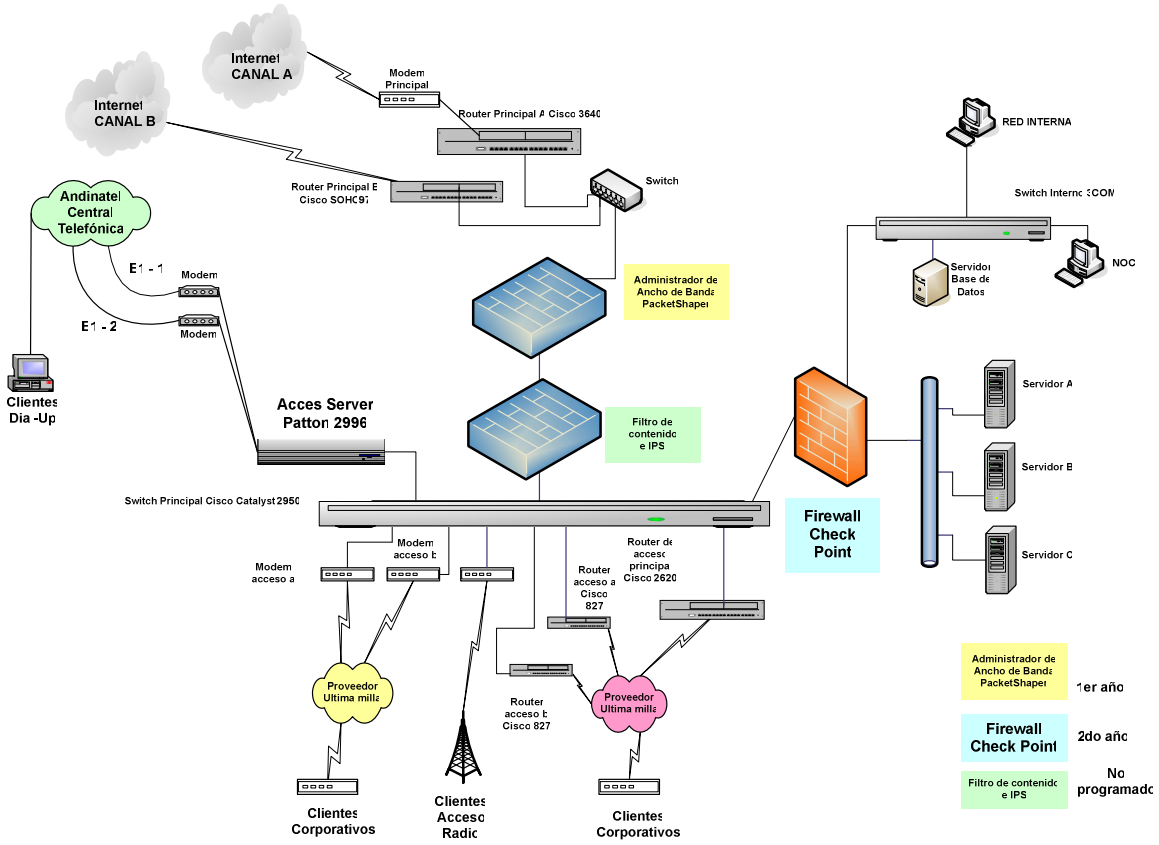


Figura 4- 2: Etapas de implementación del proyecto

4.2.1.3 Flujo de fondos con financiamiento

En base a proyección de ventas y con nuevos planes a ofrecerse se construye el flujo de fondos neto para el primer año[1], que contiene ingresos y costos (costos de inversión, costos de operación), depreciación y amortización. Para la adquisición de la plataforma, el mecanismo es mediante un préstamo a una entidad financiera. Para el caso del ISP de estudio el flujo de fondos en un año es el siguiente (ver tabla 4-4):

Mes	Flujo de fondos neto
marzo-06	-580,00
abril-06	-314,69
mayo-06	52,31
junio-06	86,62
julio-06	178,26
agosto-06	506,13
septiembre-06	737,78
octubre-06	1003,81
noviembre-06	1527,74
diciembre-06	959,35
enero-07	2515,02
febrero-07	2162,49

Tabla 4- 4: Flujo de fondos Neto

Todos los cálculos de proyección de ventas, ingresos, egresos y el flujo de fondo neto se encuentran en el ANEXO C.5, cabe acotar que el proyecto se evalúa usando el método del TIR, con el resultado siguiente:

Para el cálculo del TMAR, se considera el índice riesgo país que es 6.69%, y la tasa de inflación que es 4.76%[2].

TMAR = 6.69% + 4.76%

= 11.45%

[1] Para el segundo año los cálculos serán en base a datos actualizados tanto en inversión, costos e ingresos.
[2] http://www.cedatos.com.ec/contenido.asp?id=93

TIR = 34%

La Tasa Interna de Retorno es 34%, que es mayor al TMAR, por lo tanto el proyecto se considera viable.

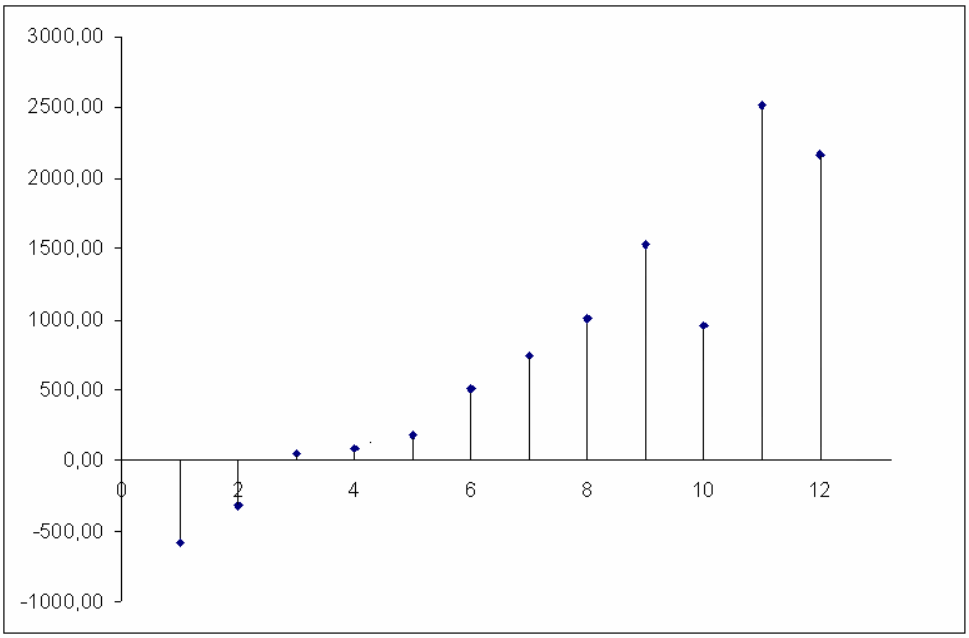


Figura 4- 3: Flujo de Fondos Neto

4.3 ESTUDIO DE TARIFAS

4.3.1 ANTECEDENTES

“Ecuador tiene el acceso a Internet más caro del mundo”. Así inició la charla entre cinco expertos en telecomunicaciones que hablaron del tema en la Facultad Latinoamericana de Ciencias Sociales (Flacso)[1], celebrada el 1 de Febrero del 2006.

La problemática surge por dos factores principales, la falta de penetración del mercado de Internet en el país (4% en el 2005), y porque el Ecuador siempre ha

[1] http://www.elcomercio.com/noticia.asp?id=24180&seccion=6

tenido que pagar un peaje alto por la conexión internacional al Internet, esto se da porque, si bien existe una salida al cable panamericano desde Punta Carnero, esta se encuentra saturada; para solventar este problema la mayoría de proveedores buscan una salida a cables submarinos internacionales de gran capacidad mediante territorio colombiano o peruano, lo que encarece los costos.
Se añade a lo expuesto, que el usuario final en el caso de un acceso *dial – up*, a más de pagar el costo de Internet al ISP, tiene que pagar el costo de la telefonía que también es alto. Lo mismo se puede expresar en accesos conocidos como banda ancha, si el ISP no es proveedor de última milla, ya que el cliente final tendrá que pagar un costo elevado de última milla a otro proveedor.

4.3.1.1 Composición del precio de acceso a Internet [33]

Los costos de acceso a Internet (orientado a acceso de banda ancha), se pueden segmentar en cuatro elementos, (ver figura 4-4), la tabla 4-4 muestra en porcentaje el costo de cada elemento, destacándose el costo de transporte internacional y acceso a Internet, y si a esto se añaden los costos referenciales que muestra la tabla 4-5 (costos de un STM-1), se nota la razón porque los costos en el Ecuador son muy altos referenciados a países como Chile y Brasil, entre otros.

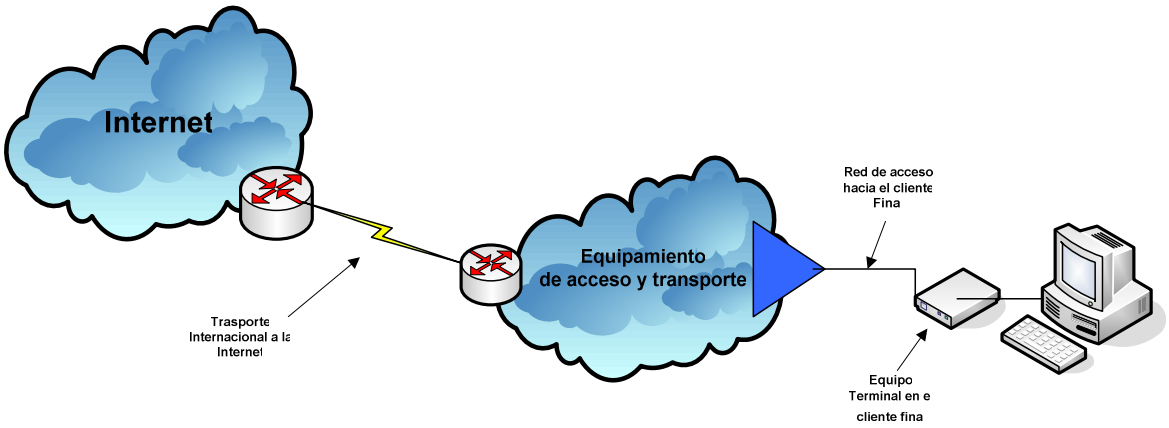


Figura 4- 4: Elementos para acceso a Internet

Elemento	Porcentaje en el costo	Comentario
Equipo terminal CPE	8.5%	Depende de la cantidad adquirida.
Red de acceso (medio físico)	10.2 %	Se puede llegar absorber como costo ya pagado en otros servicios (Andinatel).
Equipamiento de acceso, *ruteo* y trasporte	24.8 %	Depende de la capacidad instalada.
Transporte Internacional y acceso a la Internet	**56.5 %**	Costo muy elevado
TOTAL	100%	

Tabla 4- 5: Costo en porcentaje por elemento

Salida Actual	Costo
Quito – Pasto	$35.000,0
Pasto – Cartagena	$44.000,0
Cartagena – Miami (ARCOS)	$52.000,0
TOTAL	*$131.000,0*
(1 E1 tiene un costo de $1.730,89 aprox.)	

Tabla 4- 6: Costos referenciales de conexión internacional

4.3.2 TARIFAS DE ACCESO A INTERNET EN EL ECUADOR[1]

Las tarifas de acceso a Internet varían dependiendo la tecnología de acceso, y el nivel de compartición del canal que presente un acceso de banda ancha. Entre los principales planes se tiene: Internet ilimitado *dial – up*, limitado por horas *dial – up*, acceso banda ancha *home* o residencial, acceso corporativo o empresarial; estos términos dependerán del proveedor de servicios de Internet.

Entre las principales tecnologías de acceso de banda ancha que se ofrecen en el mercado ecuatoriano se tienen: acceso xDSL, cable módem, acceso vía radio, acceso satelital. Para acceso residencial, las tecnologías mas usadas son ADSL,

[1] ANEXO C.6, referencias en tarifas de diferentes proveedores.

y cable módem, aunque se despliegan con rapidez tecnologías de acceso inalámbrico.

La tabla 4-6, resume algunas tarifas que manejan diferentes ISPs, con ofertas de servicio residencial y corporativo, cada una de las cuales manejan diferentes valores agregados al servicio como tal[1].

Proveedor	Tipo de enlace	Velocidad Kbps	Compartición	Tarifa	Instalación	Servicio adicional
SATNET *	Home	200/200		49 + IVA	45 + IVA (50% por mes de enero)	2 ctas. De correo, servicio para 2 PCs
		400/400	8 a 1	75 + IVA	45 + IVA	3 ctas. De correo, servicio para 3 PCs
		800/800	8 a 1	125 + IVA	45 + IVA	5 ctas. De correo para 5 PCs
INTERACTIVE	Home	128/64	8 a 1	45 + IVA	50 + IVA	1 cta. De correo
	Corporativo	96/96		90 + IVA	180 + IVA	4 a 5 ctas. de correo
		192/192		149 + IVA	180 + IVA	
PUNTONET	Home	128/64	6 a 1	44.90 + IVA	100 + IVA	2 buzones de mail
		256/128	6 a 1	69.90 + IVA	100 + IVA	
	Corporativo	128/64	6 a 1	150 + IVA	100 + IVA	5 buzones de mail
		256/128	6 a 1	241 + IVA	100 + IVA	
QUICKNET	Home	128/64	8 a 1	67.20 + IVA	84 + IVA	1 cta. De correo
	Corporativo	128/64	8 a 1	90 + IVA	84 + IVA	4 ctas. De correo
TELCONET	Home			Los mismos precios de TRANSTELCO		
	Corporativo	64/64	4 a 1	55 + IVA	90 + IVA	
TRANSTELCO	Home	64/64	4 a 1	55 + IVA	90 + IVA	1 cta. De correo
	Corporativo	96/96	1 a 1	90 + IVA	180 + IVA	5 ctas. De correo
		192/192	1 a 1	149 + IVA	180 + IVA	

[1] Valores especialmente para la ciudad de Quito, a nivel de otras provincias los costos se elevan notablemente, dependiendo si hay cobertura con Andinadatos, o si el proveedor tiene infraestructura propia de última de milla.

ACCESS RAM	Home	No cuenta con servicio Home				
	Corporativo	256/256	1 a 1 pero comprimen el canal al 100, 75, 30 %	300 + IVA	Dependiendo de la distancia que este el cajetín	10 ctas. De correo
INTERTEL	Home	128/32	1 a 1	60 + IVA	130 + IVA	1 cta. De correo
ECUTEL	Home	128/64	15:1	69 + IVA	150 + IVA	2 PCs, 3 ctas. De correo
	Corporativo	128/64	1 a 1	610 + IVA	250 + IVA	20 PCs, 15 ctas. De correo
ANDINANET	Home	128/64	No se especifica	39,90 +IVA	50 + IVA 49,90 + IVA costo de modem usuario	No se especifica

* Servicio mediante cable MODEM

Tabla 4- 7: Tarifas de acceso banda ancha

El servicio de acceso *dial – up*, dependiendo del proveedor varía de 15 a 20 dólares mensuales, por una cuenta de acceso ilimitada, las cuenta de acceso por horas tienen tarifas referenciales, por ejemplo, se tiene 10 horas con tarifa de 9 a 10 dólares dependiendo del proveedor.

4.3.3 ANÁLISIS TARIFARIO PARA "READYNET"

Como se mencionó en el capítulo 2, READYNET, no es un portador, por ende, a más de manejar costos de acceso a Internet, propios del ISP, tiene que a estos sumarle el costo de última milla dependiendo del servicio contratado, lo que puede llegar a encarecer el acceso dependiendo del proveedor de última milla.

Los costos más elevados los maneja la empresa Suratel, seguidos por el proveedor de radio Stealth Telecom, y los costos más accesibles en el mercado son los provistos por Andinadatos, así que en la mayoría de los casos se usará la

infraestructura de Andinadatos para proveer acceso de última milla, a menos que no exista factibilidad en el sector[1].

El siguiente análisis de tarifas para acceso a Internet, se basa únicamente en costos netos de Internet, no se consideran últimas millas[2], y egresos operativos, administrativos de la empresa, con el objetivo de mostrar los niveles de compartición que se deberían manejar para que el servicio, a más de proveer acceso, pueda ofrecer calidad en el servicio, es decir no degradar el acceso a la Internet mediante niveles de compartición elevados.

No se considera en este análisis el porcentaje de reutilización del canal, que se presenta por el hecho de que no todos los usuarios acceden a la Internet de forma simultanea, ya que este ahorro de ancho de banda se consideraría como recursos a ser utilizados en gastos operativos y administrativos de la organización.

4.3.3.1 Costos aproximados de acceso a Internet

READYNET accede a la Internet mediante dos proveedores, los cuales manejan diferentes costos, para el presente análisis se ha hecho un promedio entre los dos proveedores y estos se reflejan en la tabla 4-7.

Para servicios *dial – up* y corporativos, el ISP maneja costos competitivos en el mercado, probablemente un 5 a 10% superior en algunos casos. La problemática se presenta para acceso *home* o residencial, razón por la cual es necesario considerar parámetros de compartición del canal e incluso negociar el costo que el proveedor entrega al ISP por acceso a Internet.

Si se consideran los datos expuestos en la tabla 4-6, se nota que existen tarifas referenciales que el proveedor de Internet propone para la reventa de Internet al ISP, pero se nota claramente pérdida si se llegare a considerar esas tarifas con niveles de compartición de 1:4 o 1:8, para niveles superiores de compartición

[1] Anexo C.7, costos referenciales de última milla.
[2] Se tomará como referencia costos de última milla con Andinadatos con el objetivo de hacer una comparación con costos que propone el mismo, para acceso a Internet incluida la última milla.

sería prestar mala calidad en el servicio, razón por la cual se propone costos más elevados, que por una parte ofrecen niveles aceptables de compartición y son negocio para el ISP.

Uno de los factores principales que podría volver competitivo al ISP, es la reducción sustancial del costo de acceso a Internet, tal y como se propone en el cuadro comparativo, ya que si llega a manejar un costo de USD 100,00 por cada 64 kbps, las tarifas pueden aproximarse a las propuestas por el proveedor y por ende llegar a ser competitivas en el mercado ecuatoriano.

Servicio Básico	Costo Ultima Milla*	Costo Propuesto **	Ingreso Internet x usuario	Costo ReadyNet	Ingreso Internet x usuario	Comp.	Ingreso Propuesto	Ingreso ReadyNet	Costo Internet	% Propuesto	% ReadyNet	Desviación costo Propuesto %	Desviación costo ReadyNet %
128/64	20	44,9	24,9	79	59	4	99,6	236	**262**	38,02	90,08	-61,98	-9,92
256/128	25	69,9	44,9	200	175	4	179,6	700	**524**	34,27	133,59	-65,73	33,59
512/128	28	84,9	56,9	350	322	4	227,6	1288	**1048**	21,72	122,90	-78,28	22,90
Nivel de compartición de 1:8													
128/64	20	44,9	24,9	59	39	**8**	199,2	312	262	76,03	119,08	-23,97	19,08
256/128	25	69,9	44,9	150	125	**8**	359,2	1000	524	68,55	190,84	-31,45	90,84
512/128	28	84,9	56,9	200	172	**8**	455,2	1376	1048	43,44	131,30	-56,56	31,30
Reducción de costos en Internet * **													
128/64	20	44,9	24,9	79	59	4	99,6	236	**200**	49,80	118,00	-50,20	18,00
256/128	25	69,9	44,9	200	175	4	179,6	700	**400**	44,90	175,00	-55,10	75,00
512/128	28	84,9	56,9	350	322	4	227,6	1288	**600**	37,93	214,67	-62,07	114,67
Nivel de compartición de 1:8													
128/64	20	44,9	24,9	49	29	**8**	199,2	232	200	99,60	116,00	-0,40	16,00
256/128	25	69,9	44,9	125	100	**8**	359,2	800	400	89,80	200,00	-10,20	100,00
512/128	28	84,9	56,9	200	172	**8**	455,2	1376	600	75,87	229,33	-24,13	129,33

* Costos referenciales al 15 de Febrero del 2006

** Costos propuestos por el proveedor Andinadatos para ISPs

*** Costo que el ISP propone al proveedor de Internet

Tabla 4- 8: Tarifas de acceso a Internet en base a compartición del canal y costo de Internet

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- En el ISP READYNET los mecanismos de seguridad y administración de tráfico son ineficientes, basándose en el estudio de la situación actual del mismo, dando como resultado limitaciones para implementar nuevos servicios que el usuario requiere, y por ende la lucha por convertirse en una empresa competitiva en el mercado de Internet se ha visto limitada.

- Con el diseño de un nuevo esquema en el ámbito de seguridad que mejore el sistema actual, el ISP no sólo protegerá los recursos de la organización, sino generará mayor confianza en el usuario, que si bien para éste es transparente el uso de nuevas tecnologías que permitan mejorar los servicios, el impacto está directamente enfocado a satisfacer los requerimientos del mismo.

- La propuesta de la política y procedimientos de seguridad permitirán marcar los lineamientos principales en asegurar la red del ISP, no solo de ataques externos sino de los más comunes que son los de carácter interno.

- El esquema de seguridad en profundidad, con las ventajas que presenta brindar protección a cada sistema como si fuera una isla con su propia seguridad, permiten asegurar a la red del ISP en sus diferentes áreas, empezando en el perímetro de la red y posterior a éste, un sistema de *firewall* a nivel de aplicación.

- La introducción de tecnologías, como un *firewall stateful inspection* con el objetivo de asegurar en primera instancia las plataformas de servicio, permitirán prevenir ataques como *Denial of Service* que puedan dejar fuera los

servicios principales que ofrece el ISP (DNS, correo electrónico, alojamiento *Web*, etc.)

- Aunque se proyecta a futuro la implementación de mecanismos que permitan filtrar contenido, es un esquema que permitirá al ISP, crear nuevos servicios, en este caso serían servicios de seguridad, como es el caso de filtrado de páginas con contenido malicioso o restricción de acceso a ciertas URLs que el usuario las cataloga como perniciosas.

- En el ámbito de administración de tráfico, la problemática del ISP es mayor, ya que el canal con la salida a Internet se encuentra en el borde de la saturación, por lo que es indispensable proponer un sistema que permita optimizar los recursos de ancho de banda disponible, sin dejar a un lado la calidad de servicio ofertada al cliente.

- Los sistemas de administración de tráfico se basan especialmente en el control de aplicaciones hambrientas de ancho de banda, que en un determinado instante resultan improductivas a las organizaciones, si bien en un ISP las aplicaciones no pueden ser restringidas, se intenta asignar recursos dando prioridad a aplicaciones más sensibles.

- La introducción del sistema de administración de ancho de banda permitirá al ISP, brindar nuevos esquemas de servicio, que hoy en día hacen que los costos de acceso a Internet sean más asequibles en el mercado, sin afectar a los clientes que prefieren calidad de servicio aunque los costos sean superiores.

- Como complemento a la creación de nuevos productos en base a niveles de compartición del canal de acceso a Internet, la introducción de un sistema que controle tráfico, permitirá asignar el ancho de banda contratado a los usuarios en base a políticas de control sin que estos lo sobrepasen, que en el caso del ISP de estudio es uno de los problemas existentes.

- En el capítulo 4 de este proyecto se presenta un esquema que permite manejar canales compartidos en base a enrutadores, sin embargo este esquema no es una solución para el ISP, porque si bien el usuario no podrá acceder a más recursos de ancho de banda cuando su enlace segmentado se sature, la problemática continúa para la red de acceso principal que permitirá el tráfico de bajada según la capacidad del canal contratado con el proveedor de acceso internacional.

- La solución propuesta en base a la plataforma de administración de ancho de banda de *Packeteer*, es más robusta por la forma de controlar el tráfico especialmente el de bajada o *download*, usando *TCP rate control*, permitiendo de esta manera comunicación con el punto extremo, para que los datos sean despachados a menor velocidad mediante la disminución de la ventana TCP.

- El contemplar en el contrato como una cláusula del mismo, acuerdos de niveles de servicio, permite al cliente diferenciar al proveedor de servicios, y al ISP le brinda un compromiso de seriedad con el cliente, por ende si los SLAs son mejores que el de otro proveedor, READYNET podrá tomar ventaja en el mercado convirtiéndose en una empresa más competitiva.

- El análisis financiero es un complemento al diseño propuesto que permite mediante una proyección de ventas recuperar la inversión en un año de la primera etapa del proyecto, y además ofrece rentabilidad a la empresa.

- Para llegar a ser más competitivos en el mercado, como se expone en el estudio de tarifas realizado, los costos de acceso internacional deben ser más asequibles, de esta forma no solo las empresas que han formado un monopolio podrán ofertar servicios a menor costo.

- La seguridad en redes en el mundo convergente que predomina ahora no es opcional para las empresas, cualquiera que fuere su ámbito de acción, ya que los ataques a organizaciones cada día son mayores, dejando pérdidas sustanciales de los recursos de las mismas.

- El proceso de aseguramiento continuo de una organización, ayuda día a día a mejorar la seguridad que ésta necesite, razón por la cual es necesario que exista un grupo de seguridad que sea el encargado de marcar los lineamientos a seguirse en este campo.

- La tendencia ahora es realizar una gran cantidad de transacciones mediante una de las mayores redes públicas que es la Internet, por lo que ha sido necesario interconectar redes privadas a la misma que si bien el acceso es fácil, los mecanismos de seguridad son mínimos, lo que ha motivado a la mayoría de organizaciones a implementar mecanismos de seguridad como *firewalls*, sistemas de detección de intrusos, por mencionar los principales, con el objetivo de evitar que la red interna sufra ataques del exterior, además, se considera la creación de políticas y procedimientos de seguridad como uno de los pilares más fuertes en un esquema de seguridad que brinde protección de ataques internos y externos que pueda sufrir.

- Para un proveedor de servicios de Internet es de vital importancia establecer mecanismos de seguridad que permitan, no solo protegerse así mismos, sino extender esta seguridad a los usuarios y además a la Internet.

- El establecimiento, definición y ejecución de políticas y procedimientos de seguridad a seguirse en el ámbito de un ISP, no sólo van a garantizar obtener niveles aceptables de seguridad en la organización, sino que creará confianza en el usuario que es una de las metas a conseguir en una empresa que presta servicios de acceso a Internet.

- La calidad de servicio en Internet tiene que ser medida considerando dos aspectos fundamentales que son la calidad de servicio funcional que presta la red y la calidad de servicio que percibe el usuario.

- La Internet no fue desarrollada para garantizar calidad de servicio, sin embargo la tendencia actual a cruzar diferentes tipos de aplicaciones con diferentes requerimientos sobre una red orientada a la transmisión de paquetes usando el

mecanismo del mejor esfuerzo, ha generado que grupos de investigación propongan soluciones como reservar recursos del ancho de banda o priorizar cierto tipo de aplicaciones sin afectar a las demás.

RECOMENDACIONES

- La implementación del proyecto deberá ser por etapas, en vista de que los costos de los equipos son rubros altos que el ISP, como empresa no puede manejarlos.

- Para mejorar el sistema de seguridad será necesario que a futuro se implemente una solución para filtrar contenido, y un sistema de protección contra intrusos, evaluando los beneficios y costos de los mismos, considerando la seguridad desde el punto de vista de negocio, más no como un gasto que no produce ventajas económicas a la empresa.

- Es necesario en la red del ISP implementar un proceso de escalamiento de *hardware* y *software*, que permitirá actualizar los sistemas e introducir nuevas tecnologías que permitan segmentar la red de tal forma que se pueda brindar mayor seguridad a la misma.

- Se recomienda brindar charlas sobre seguridad interna, pues es uno de los problemas que la mayoría de empresas hoy en día tienen como enfoque principal para la protección de recursos de la organización.

- La creación de políticas de administración y control de tráfico más detalladas para un correcto uso del sistema de administración de ancho de banda que será implantado en la red del ISP.

- La inclusión de acuerdos de niveles de servicio en el contrato, para que el usuario y el proveedor tengan un compromiso serio en el cual basarse. Como

READYNET depende de terceros en ofertar el servicio de acceso a Internet, deberá exigir acuerdos de niveles de servicio con los proveedores, de tal manera que pueda extender estos acuerdos al cliente.

- Aunque la tendencia es bajar costos para el usuario final, se debe considerar que la calidad de servicio es muy importante, motivo por el cual se deben manejar con mesura los niveles de compartición del canal.

REFERENCIAS BIBLIOGRÁFICAS

[1].- "*Network Security Bible*", Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, Wiley Publishing, Inc., 2005, capítulo 8, 9, 10.

[2].- "*Implementing Secure Intranets and Extranets",* Kaustubh M. Phaltankar, Artech House, 2000, capítulo 5.

[3].- "*Fundamentals of Network Security*", John E. Canavan, Artech House, 2001, capítulo 1, páginas 9, 16 – 19, capítulo 6.

[4].- "*The Technical Side of Being an Internet Service Provider*", *International Technical Support Organization,* octubre de 1997.

[5].- "*Building Internet Firewalls*", Elizabeth D. Zwicky, Simon Cooper D. Brend Chapman, O'Reilly, June 2000, 2nd Edition capítulo 2, página 36, capítulo 16,

[6].- "*ISP Security Essentials — Best Practice Cisco IOS® and Other Techniques to Help an ISP Survive in Today's Internet*", version 1.5., 2001.

[7].- "Arbor & Cisco: Realizing Infrastructure Security" Danny McPherson, http://arbornetworks.com.

[8].- "ftp://ftp-eng.cisco.com/ftp/cons/isp/security/", D-Preparation-OPSEC-Team-v3-0.pdf.

[9].- "ftp://ftp-eng.cisco.com/ftp/cons/isp/security/", I-Identification-v3-0.pdf.

[10].- "ftp://ftp-eng.cisco.com/ftp/cons/isp/security/", M-Postmortem-v3-0.pdf.

[11].- *"Router Security Configuration Guide",* version 1.1, septiembre 27, 2002 capítulo 3.

[12].- "*Security Fundamentals for E-Commerce*", Vesna Hassler, Artech House, 2001, parte 4. y *"Building Internet Firewalls"*, Elizabeth D. Zwicky, Simon Cooper D. Brend Chapman, O'Reilly, June 2000, 2nd Edition, parte III.

[13].- "*Network Security Assessment*", Chris McNab, O'Reilly, March 2004, capítulo 7, tabla 7-6.

[14].- "*Ingineering Internet QoS* ", Sanjay Jha, Artech House, 2002, capítulo 5 y RFC 1633, capítulo 6.

[15].- "TCP/IP Tutorial and Technical Overview", Adolfo Rodriguez, John Gatrell, John Karas, Roland Peschke

[16].- "*Internet QoS Architectures and Mechanisms for Quality of Service*" ZHENG WANG, Marzo 2001, capítulo 1.

[17].- "*An Admission Control Algorithm for Predictive Real-Time Service*", Jamin, S., Shenker, S., Zhang, L., and D. Clark,Extended abstract, in Proc. Third International Workshop on Network and Operating System Support for Digital Audio and Video, San Diego, CA, Nov. 1992, pp. 73-91.

[18].- "Contribución a las metodologías para la evaluación de calidad de servicio en redes heterogéneas", Luis Bellido Triana, 2004.

[19].- "Planificación de un proveedor de servicios de Internet y diseño de su sistema de seguridad", Febrero 2002, Caicedo Jaramillo, María Soledad; Yánez Andagana, Fernando Isaías, Director: Ing. Pablo Hidalgo.

[20].- "*Writing Information Security Policies*", Scott Barman.

[21].- "*Strategies for Managing Application Traffic*", Packeteer.

[22].- "*Cisco IOS Quality of Service Solutions Configuration Guide***",** Release 12.2, QoS_Cookbook

[23].- "*Cisco IOS Quality of Service Solutions Configuration Guide Release 12.2*", página QC-79

[24].- *"NetEnforcer® Enterprise WAN Traffic Management", Allot.*

[25].- "*PACKETEER TECHNICAL PRODUCT OVERVIEW, Strategies for Managing Application Traffic Using Visibility, Control, and Compression to Deliver Performance"*

[26].- *"FireWall-1,The industry's most proven perimeter security", Check Point.*

[27].- "*CISCO PIX 515E SECURITY APPLIANCE*", Data Sheet

[28].- http://www.multitech.com/PRODUCTS/Families/RouteFinder/

[29].- http://www.fortinet.com/solutions/ips.html

[30].- "*Integrating Service Level Agreements Optimizing Your OSS for SLA Delivery*", John J. Lee, Ron Ben-Natan, Wiley Publishing, Inc.,2002.

[31].- "Preparación y evaluación de proyectos", Nassir Sapag Chain, 3era edición, 1998.

[32].- "Preparación y evaluación de proyectos", Nassir Sapag Chain, 3era edición, 1998.

"Formulación, evaluación y gestión de proyectos", Ing. Tarquino Sánchez, Abril 2004.

"Estudio y Diseño de una red basada en tecnología MPLS para un *carrier* de datos",

Ing. Jorge Baez, Ing. Cesar Cevallos, Noviembre 2002.

Datos proporcionados por el departamento comercial de “READYNET”

[33].- Presentación Ing. Diego Salazar, foro, El Ecuador tiene el acceso a Internet más caro del mundo, FLACSO, 01/02/2006.

Otras:

- http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/es/security-guide/ch-sgs-ov.html
- “*Cisco IOS Quality of Service Solutions Configuration Guide”,* Release 12.2
- "*An Admission Control Algorithm for Predictive Real-Time Service*", Jamin, S., Shenker, S., Zhang, L., and D. Clark,Extended abstract, in Proc. Third International Workshop on Network and Operating System Support for Digital Audio and Video, San Diego, CA, Nov. 1992, pp. 73-91.
- “Internetworking technologies handbook ”, capítulo 49
- “*Internet QoS: Architectures and Mechanisms for Quality of Service”,* Zheng Wang, Morgan Kaufmann, March 15, 2001, 1st edition.
- www.juniper.net/solutions/ literature/white_papers/200004.pdf.
- “Tratamiento borroso del intangible en la valoración de empresas de Internet”, Mª Carmen Lozano Gutiérrez, Federico Fuentes Martín. http://www.eumed.net/cursecon/libreria/index.htm
- RFC 3013 - Recommended Internet Service Provider Security Services and Procedures
- Datos proporcionados por el departamento técnico y comercial de READYNET CIA. LTDA
- http://www.ewh.ieee.org/sb/argentina/unsj/Aimp/Inflacion.pdf
- http://www.economia.unam.mx/secss/docs/tesisfe/MartinezSCM/cap4.pdf
- http://www.cedatos.com.ec/contenido.asp?id=93
- www.satnet.net

REFERENCIAS BIBLIOGRÁFICAS DE FIGURAS

[1] "*Implementing Secure Intranets and Extranets",* Kaustubh M. Phaltankar, Artech House, 2000, capítulo 5, página 129.

[2] "*Security Fundamentals for E-Commerce*", Vesna Hassler, Artech House, 2001, parte 3, página 170.

[3] "Network Security Bible", Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, Wiley Publishing, Inc., 2005, capítulo 9, páginas 315,330 y .

[4] "*ISP Security Essentials — Best Practice Cisco IOS® and Other Techniques to Help an ISP Survive in Today's Internet*", version 1.5., 2001, páginas 8,10,75 y 111.

[5] "*Network Security Assessment*", Chris McNab, O'Reilly, March 2004, capítulo 8.

[6] "*Ingineering Internet QoS* ", Sanjay Jha, Artech House, 2002, capítulo 5 y RFC 1633, capítulo 6.

[7] "*PACKETEER TECHNICAL PRODUCT OVERVIEW, Strategies for Managing Application Traffic Using Visibility, Control, and Compression to Deliver Performance", página 4.*

[8] *"NetEnforcer® AC-1000 Series Carrier-Grade Service Control and QoS/SLA Enforcement Operation Guide Version 6.1.1(Doc. No. D354002)",capítulo 4.*

[9] *"Multi-Level Traffic Management" página 1.*

[10] *"Gaining Visibility into Application and Network Behavior", PACKETEER TECHNICAL PAPER, página 5.*

[11] "*CISCO PIX 515E SECURITY APPLIANCE*", Data Sheet

[12] http://www.multitech.com/PRODUCTS/Families/RouteFinder/

[13] "*Integrating Service Level Agreements Optimizing Your OSS for SLA Delivery*", John J. Lee, Ron Ben-Natan, Wiley Publishing, Inc.,2002.

GLOSARIO

- Amenaza: es un evento o actividad que tiene el potencial de causar daño a la red, ya sea interrumpiendo la operación, funcionamiento, integridad o disponibilidad de la red o del sistema.

- Autorización: son los privilegios que tiene un individuo o entidad para acceder a los recursos del sistema o la red. Existirán niveles de acceso los cuales van a determinar a cuanta información se accederá y a que recursos.

- Bombas lógicas.- es código malicioso que se activa cuando ocurre algo específico, se alcanza una condición lógica, o se cumple una fecha o tiempo determinado.

- Código malicioso.- tiene la intención de causar daño, romper, o engañar las funciones de un computador o una red. Este código puede ser móvil como *Applets* de *Java* o código en ambientes *Active X*.

- *Droppers*.- es un programa usado para instalar virus en computadores, no está infectado con código malicioso de manera que evade software destinado a encontrar virus en el sistema. Incluso puede llegar a descargar actualizaciones de virus que residen en el sistema.

- Encripción: es un método para transformar datos legibles en un formato no legible, los cuales luego de ser transmitidos podrán se recuperados usando una llave especial.

- Gusanos.- se reproducen y propagan por si mismos, no usan archivos *host* como los virus. Usualmente suelen atacar por medio de adjuntos que viene en correo electrónico, empezando a enviarse a todas las cuentas de la libreta de direcciones y sobrecargando servidores de correo.

- Identificación: es el proceso de declarar la identidad de un usuario dentro del sistema, saber con quien se está comunicando.

- Incidente: es el acto de violar una política de seguridad implícita o explícitamente[1].

- Responsabilidad: determina las acciones y conducta de un individuo dentro de un sistema. Además se refiere a la habilidad de rastrear o auditar lo que esta haciendo un individuo o entidad dentro del sistema o la red. Se considera por ejemplo: archivos a los cuales se ingreso, e información alterada.

- Troyanos.- es un programa que dentro de sí esconde otro programa con funciones maliciosas como la de crear una puerta de ingreso para atacantes, por ejemplo abriendo puertos.

- Virus.- es un programa que no funciona de forma independiente, sino usa un programa *host* al cual se vincula. Cuando el programa infectado se ejecuta, el virus se propaga. Se transmite por diferentes formas como son: archivos descargados de Internet o adjuntos en correo electrónico.

- Vulnerabilidad: es una debilidad que puede ser explotada por una amenaza y causar daño a la red o sistema.

[1] Definición dada por **CERT/CC.**