UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE PLATAFORMA DE CONTROL DE TRÁFICO IP

PARA UN ISP

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

HEBER HÉCTOR MILLA CABALLERO

PROMOCIÓN

1994 - II

LIMA - PERÚ

2006

DISENO DE PLATAFORMA DE CONTROL DE TRÁFICO IP PARA UN ISP

Dedico éste trabajo :

A mi hijita Fiorella, a mi hijito Héctor Eloy y a mi adorada esposa, por el amor, la paciencia y porque son la razón de mi vida.

A mi Madre y mis Hermanos, por haber nacido y crecido en un maravilloso hogar, que sembraron en mí la fortaleza, la perseverancia y la humildad; valores que permitieron y me permiten hasta hoy enfrentarme cualquier dificultad. En especial a mi hermano mayor Julio que siempre será un padre y un amigo, que con su ejemplo supo guiarnos hacia un camino difícil pero con destino claro.

A María, por su gran amor, su apoyo sincero e incondicional en los momentos más difíciles de mi etapa universitaria.

A mi cuñada Maritza, a mi tía Reyna y a todos los que me apoyaron para hacer de éste sueño una gran realidad.

SUMARIO

El intercambio de archivos, especialmente de música y vídeo, se realiza mediante redes ó protocolos P2P (peer-to-peer: entre iguales). Estas permiten distribuir el costo de la distribución entre los usuarios, de forma que cualquiera puede publicar contenidos a bajo costo, independientemente del número de destinatarios. Este tipo de consumo en Internet supone un notable aumento de costos para los ISP's (Internet Service Provider's: Proveedores de Acceso a Internet) debido al excesivo uso de ancho de banda que saturan su enlace (conexión) a Internet, demandando una mayor capacidad.

El propósito de éste trabajo es diseñar y proponer una alternativa de optimización de ancho de banda para un ISP a través de una plataforma de control de tráfico IP. Esta plataforma ofrece el monitoreo y control de tráfico por aplicaciones (ejm: P2P) de manera agregada ó por cada usuario.

El trabajo se presenta con una introducción teórica acerca de la Internet y los servicios principales que actualmente se ofrecen, en seguida se expone la problemática de ancho de banda con la que se enfrenta actualmente un ISP en el ámbito nacional e internacional, luego se presenta distintas formas ó tecnologías de control de tráfico, además se diseña y se propone, estableciendo un cronograma de implementación en el tiempo, la plataforma de control de tráfico IP de acuerdo a los requerimientos de un ISP típico. Para finalizar se analiza la viabilidad económica, comercial y legal de la propuesta.

ÍNDICE

PRÓLOGO

CAPÍTULO I

MARCO TEÓRICO

1.1. Internet 3

1.1.1.Evolución de la Internet 3

1.1.2.Proveedores de acceso a Internet (ISP's) 4

1.2. Servicios en Internet 6

1.2.1.Intercambio de archivos utilizando protocolos P2P 6

1.2.2.Voz sobre Internet 11

CAPITULO II

PROBLEMÁTICA DE ANCHO DE BANDA DE UN ISP

2.1. Comportamiento de tráfico Internet en el ámbito global 13

2.2. Comportamientode tráfico Internet en el Perú 13

2.2.1.Tráfico Internet total por aplicaciones 15

2.2.2.Tráfico Internet por tipo de usuarios 15

2.3. Causas del problema de ancho de banda de un ISP 17

CAPITULO III

FORMAS Ó TECNOLOGÍAS DE CONTROL DE TRÁFICO IP POR APLICACIONES

3.1. Control de tráfico IP en el Router de Interconexión 19

3.1.1.Acces List (ACL) ó Calidad de Servicios (QoS) por puertos TCP/UDP 20

3.1.2.Funcionalidades especiales (NBAR) 20

3.2. Control de tráfico IP con equipo especializado dedicado 21

3.2.1.Solución Cisco: Plataforma SCE (Service Control Engine: Motor de control de Servicio) 21

3.2.2.Solución Allot ("NetEnforcer") 30

3.3. Resumen del capítulo 32

CAPITULO IV

DIMENSIONAMIENTO Y PROPUESTA DE LA PLATAFORMA DE CONTROL DE TRÁFICO IP

4.1. Requerimientos de diseño 34

4.1.1.Demanda de acceso a Internet por Banda Ancha (ADSL) 34

4.1.2.Red de agregación y transporte IP del ISP para el 2007 36

4.1.3.Restricciones presupuestales del ISP 36

4.1.4.Especificaciones técnicas generales de los equipos 36

4.2. Propuesta de la plataforma de control de Tráfico IP 38

4.2.1.Selección de equipos 38

4.2.2.Propuesta de red con plataforma de control de tráfico IP para el ISP –2007 40

4.2.3.Inversión estimada 2007-2011 41

4.2.4.Cronograma de implementación de la plataforma de control de tráfico IP 43

CAPITULO V

VIABILIDAD DE LA PROPUESTA

5.1. Viabilidad económica 46

5.1.1.Ahorro de gastos 46

5.1.2.Flujo económico 48

5.2. Viabilidad comercial y legal 48

5.2.1.Viabilidad comercial 48

5.2.2.Viabilidad legal 49

CONCLUSIONES Y RECOMENDACIONES **51**

ANEXO A 53

ANEXO B 66

BIBLIOGRAFÍA **67**

ÍNDICE DE ILUSTRACIONES

Fig.1.1. Esquema de conectividad de acceso a Internet por Dial-Up 5
Fig. 1.2. Esquema de conectividad de acceso a Internet por ADSL 6
Fig. 1.3. Modelo de red Cliente-Servidor 7
Fig. 1.4. Modelo de red P2P 7
Fig. 1.5. Arquitectura de red del protocolo Blubster (Napster) 9
Fig. 1.6. Arquitectura de funcionamiento del protocolo Gnutella 10
Fig. 2.1. Análisis de Tráfico Global de Internet 14
Fig. 2.2. Análisis de Tráfico Internet por Aplicaciones 14
Fig. 2.3. Análisis de Tráfico de Internet en Perú 15
Fig. 2.4. Tráfico Internet en Perú por tipo de usuario 16
Fig. 2.5. Tráfico de las cabinas públicas Internet en el Perú 16
Fig. 2.6. Tráfico Internet de los Heavy User's en el Perú 17
Fig. 2.7. Tráfico Internet del osusuarios comunes 17
Fig. 3.1. Control de tráfico IP en el Router de Interconexión 19
Fig. 3.2. Control de tráfico IP con equipo especializado dedicado 22
Fig. 3.3. Ejemplo de control de tráfico IP por aplicaciones 22
Fig. 3.4. Arquitectura de la plataforma SCE de Cisco 24
Fig. 3.5. Proceso de clasificación en el SCE 25
Fig. 3.6. Proceso de Control en el SCE 27
Fig. 3.7. Intercambio de mensajes, de entrada-salida al sistema, entre el SM y el Radius 29
Fig. 3.8. Informes de volumen y ancho de banda -Plataforma SCE 30
Fig. 3.9. Informe de volumen de tráfico top por protocolos -Plataforma SCE 31
Fig. 3.10. Arquitectura de la plataforma Net Enforcer de Allot 32
Fig. 3.11. Arquitectura distribuida de control de tráfico IP 33
Fig. 4.1. Demanda de usuarios de Banda Ancha (ISP-X) 35
Fig. 4.2. Demanda de Ancho de Banda Total (ISP-X) 35
Fig. 4.3. Esquema de red del ISP para el 2007 37
Fig. 4.4. Nuevo esquema de red del ISP para el 2007 41

Fig. 4.5. Conectividad IP del Suscriber y Collection Manager con los equipos SCE-2000 42

Fig. 5.1. Evolución del ancho de banda con control de tráfico IP 47

Fig. 5.2. Evolución del flujo económico 48

Fig. 5.3. Cadena de valor de Internet 50

ÍNDICE DE TABLAS

Tabla 1.1.Cliente-Servidor vs. P2P 8
Tabla 4.1.Proyección de demanda de acceso a Internet por Banda Ancha (ISP-X) 34
Tabla 4.2.Resumen de evaluación del equipo de control SCE-2000 versus NetEnforcer AC-2500 39
Tabla 4.3.Inversión 2007, Plataforma de Control de Tráfico IP 42
Tabla 4.4.Inversión 2008-2011, Plataforma de Control de Tráfico IP 43
Tabla 4.5.Cronograma de implementación 2007 45
Tabla 5.1.Ahorro de Ancho de Banda (2007-2011) 47
Tabla 5.2.Ahorro de Gastos (2007-2011) 48
Tabla 5.3.Flujo Económico (2007-2011) 48

PROLOGO

La Internet ha hecho posible la expansión de las empresas de distribución de contenidos, sin embargo; en la actualidad los distribuidores están preocupados por la distribución paralela de sus contenidos en Internet. Millones de personas descargan vídeo y música, utilizando redes P2P, sin el permiso de los propietarios. Las medidas técnicas y legales no han producido efecto contra un comportamiento ya generalizado cuya tendencia es creciente.

El fenómeno de P2P, genera una situación complicada para el ISP, por una parte, la demanda de conexiones de banda ancha ha aumentado en gran medida, por otra, los usuarios generan un intenso tráfico que aumenta los costos de enlace a Internet.

Si la distribución de contenidos de alta definición da el salto definitivo a Internet, los ISP's no podrán hacer frente a la demanda. La única forma de combatir éste problema es racionalizando el uso de la conexión ó enlace a Internet del ISP.

Además, el consumo de ancho de banda del ISP por algunos usuarios, heavy user's (heavy user's: usuarios intensivos) genera actualmente insatisfacción de la gran mayoría de usuarios (usuarios comunes), por lo que se requiere compartir el ancho de banda en forma equitativa e incrementar la satisfacción de todos los clientes. Se trata, en resumen, de que el proveedor de acceso a Internet brinde buena calidad de servicio para todos sus clientes ó usuarios.

Ante la problemática descrita, el presente trabajo se plantea como objetivo general diseñar y proponer una plataforma de control de tráfico IP. Esta propuesta busca optimizar el ancho de banda del enlace a Internet de un proveedor de acceso a Internet (ISP) y aumentar el nivel de satisfacción de todos los usuarios.

Para alcanzar el objetivo general, se plantea los siguientes objetivos específicos:

- Estudiar los principales servicios que actualmente son bastante utilizados en Internet, tales como: P2P y VoIP (VoIP: Voz sobre IP)
- Sustentar las causas de la problemática de ancho de banda de un ISP.
- Estudiar y analizar las distintas formas y tecnologías que existen para controlar el tráfico IP de manera granular a nivel de usuario y de aplicaciones.

- Dimensionar y proponer la solución de plataforma de control de tráfico IP para un ISP típico.

- Evaluar la viabilidad económica, comercial y legal de la propuesta de plataforma de control de tráfico IP.

Sobre la base de los objetivos propuestos, el contenido del documento se desarrolla en cinco capítulos:

En el capítulo I, se desarrolla el marco teórico necesario de la red Internet, distintas modalidades de acceso a Internet que ofrecen los ISP's y los principales servicios de mayor consumo en Internet.

En el capítulo II, se analiza el tráfico Internet por aplicaciones ó servicios, tanto en el ámbito nacional como internacional, para sustentar la problemática actual con que se enfrenta el ISP (tráfico P2P)

En el capítulo III, se analizan las alternativas tecnológicas que existen para implementar una plataforma de control de tráfico IP. Se estudia la solución técnica de dos principales proveedores de tecnología de control de tráfico: Cisco y Allot.

En el capítulo IV, se dimensiona y se propone una plataforma de control de tráfico IP, sobre la base de los requermientos de un ISP típico.

En el capítulo V, se evalua la viabilidad económica, comercial y legal de la propuesta.

Se finaliza el documento realizando las conclusiones y recomendaciones obtenidas del presente trabajo, que serán útiles para futuras propuestas y/o implementaciones.

En general el presente trabajo puede ser usado, como metodología, para proponer una alternativa de solución para el control de tráfico IP de cualquier ISP.

CAPITULO I
MARCO TEÓRICO

1.1 Internet

Internet se conoce desde hace muchos años como la red de redes. Para José Daniel Sánchez Navarro (1996), en su libro el Camino fácil a Internet, define a la red como "Una gran comunidad de las que forman parte personas de todo el mundo, que usan sus computadoras para interactuar unas con otras, y con la posibilidad de obtener información" (p. 1) [8]

Una red de computadoras, según la Enciclopedia de Redes de Ton Sheldon (1996), es "Un sistema de comunicación de datos que enlaza dos o más computadoras y sus dispositivos en un conjunto de equipos de interconectados permanentemente de alguna manera, de forma que la capacidad operativa de la red es mayor que la suma de las capacidades de cada equipo" (p. 714) [8]

La necesidad de comunicación e información a través de la computadora hacen que Internet sea cada vez más utilizado. Para entender la importancia que Internet tiene en la sociedad actual se describe el proceso de evolución y los principales servicios que actualmente se ofrecen en ella.

1.1.1 Evolución de la Internet

- En 1969, Internet fue creada a partir de un proyecto del departamento de defensa de los Estados Unidos llamado DARPANET (Defense Advanced Research Project Network) y cuyo propósito principal era la investigación, desarrollo e implementación de protocolos de comunicación para redes de área amplia (WAN), para garantizar la comunicación entre lugares distantes en previsión de cualquier ataque nuclear, bajo responsabilidad de la ARPA[1]. Estas investigaciones arrojaron como resultado el protocolo de comunicaciones TCP/IP (Trasmission Con-

[1]En 1957, en plena Guerra Fría, la URSS lanzó el primer satélite artificial, el Sputnik, y como respuesta a este avance tecnológico el Departamento de Defensa de los Estados Unidos crea la Agencia de Proyectos de Investigación Avanzada (ARPA), con el fin de fomentar el desarrollo tecnológico aplicable a la defensa.

trol Protocol/Internet Protocol) un sistema de comunicaciones muy sólido y robusto en el cual se integran todas las redes que conforman actualmente la Internet.

- En 1970, las actividades militares se separaron y se interconectaron las principales universidades y centros de investigación científica de EE.UU.
- En 1982, el Reino Unido se conectó a Internet, sirviendo como puerta de acceso a los países europeos y marcando el comienzo de la globalización a la red.
- En 1986, Japón se conectó y la administración del segmento no militar de la red se transfirió a NSFnet (National Science Foundation Network: Red de la Fundación Nacional de Ciencias), quien mejoró la velocidad de las troncales o backbones de Internet. [8]
- Desde aquellos años 80, los usuarios descubrieron que la información que se encontraba en la red era muy útil y si cada institución que se conectaba aportaba algo crecería más el acervo de información existente.
- El Perú se conecta a la red de redes (Internet) en 1992, con la Red Científica Peruana cuyos objetivos fueron netamente académicos y sin fines de lucro, sin embargo; en 1996 con Telefónica del Perú se inicia el desarrollo de la Internet comercial en el país, con la implementación de los servicios InfoVía y UniRed. En la actualidad en el Perú, existe más de medio millón de usuarios de acceso a Internet por distintas modalidades de acceso, pero; principalmente por banda ancha (ADSL: Asimetric Digital Suscriber Line)

1.1.2 Proveedores de acceso a Internet (ISP's)

Las empresas proveedoras de servicios de acceso a Internet, denominadas comúnmente como ISPs (Internet Service Providers: Proveedores de acceso a Internet), ofrecen a los usuarios finales sus servicios de acceso a Internet. Para brindar sus servicios, los ISPs deben estar inscritos en el registro de empresas prestadoras de servicios de valor añadido del Ministerio de Transportes y Comunicaciones (MTC)

Los ISPs, para proveer sus servicios necesitan de dos conexiones: una conexión con la red internacional (backbone de Internet) y al NAP (Neuter Acces Point: punto de acceso neutro) local, y otra de acceso a los usuarios finales. La red de acceso al usuario final es proveída por las operadoras de telecomunicaciones que deben contar con la autorización del MTC a través de un contrato de concesión.

Existen distintas modalidades de acceso, tales como: la red telefónica fija conmutada (RTC), la red de televisión por cable, una línea dedicada alámbrica ó inalámbrica, la red de telefonía móvil, ADSL, WiFi, WiMAX, etc.

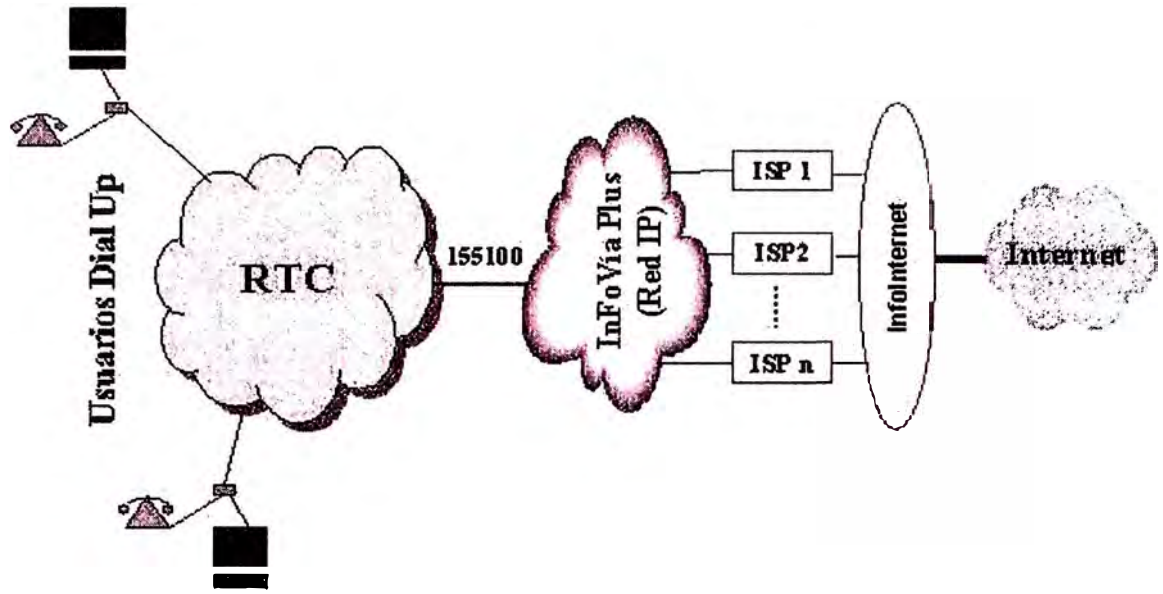


Figura 1.1: Esquema de conectividad de acceso a Internet por Dial-Up

El tipo de infraestructura de acceso al ISP, permite a algunas operadoras de telecomunicaciones integrarse verticalmente y ofrecer sus servicios en forma de paquete. Las principales modalidades de acceso, que ofrecen en la actualidad las grandes operadoras-ISP's (operadoras integrados verticalmente) son: la red telefónica conmutada (denominada también dial-up) y el ADSL, los cuales se describen en seguida.

a. ISP's con acceso dial-up.

En el caso del acceso a través de la red telefónica conmutada (RTC), dial-up, existe un menor grado de integración vertical; es decir, las empresas no brindan el servicio de Internet y de telefonía local como un paquete. Ello se debe a que el acceso a Internet se inicia a través de la RTC, y el mercado de servicios de acceso a Internet ha crecido como un mercado competitivo conformado por varios ISPs conectados a la RTC, los cuales son escogidos por los usuarios finales como sus proveedores de servicio de acceso a Internet. Ver figura 1.1.

b. ISP's con acceso de banda ancha (ADSL)

Con el desarrollo contínuo de nuevas tecnologías de acceso (XDSL, WiFi, WiMAX) y las nuevas condiciones de mercado con la liberalización del mercado de telecomunicaciones en el Perú desde 1998, las operadoras de telecomunicaciones se han enfrentado con nuevos retos y han tomado como estrategia la integración vertical, en consecuencia las grandes operadoras de telecomunicaciones se han convertido también en los principales proveedores de acceso a Internet (ISP's)

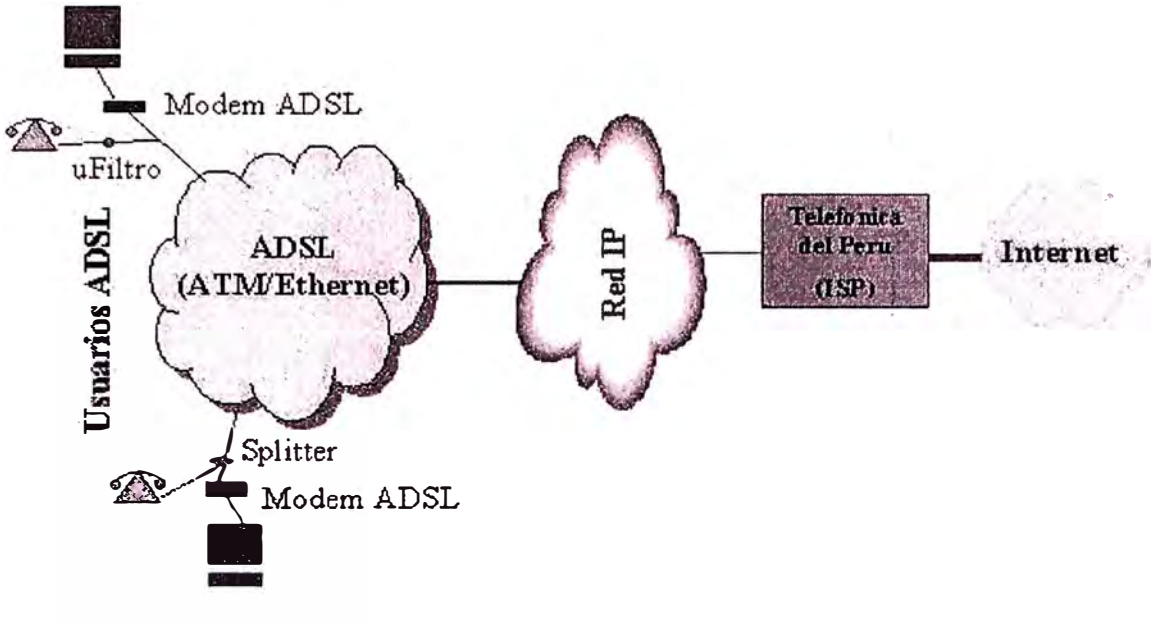


Figura 1.2: Esquema de conectividad de acceso a Internet por ADSL

La principal modalidad de acceso a Internet, hoy en día, es con tecnología ADSL, denominado acceso de banda ancha. El principal operador es Telefónica del Perú que ofrece el servicio Speedy. Ver figura 1.2.

1.2 Servicios en Internet

Internet es el nuevo medio de comunicación y de gestión de la información, que se realizan a través de los servicios disponibles, tales como:

- **Servicios de comunicación**: correo electrónico (E-Mail), foros de debate o grupos de noticias, conferencia electronicas (Chat), *Voz sobre Internet (VoIP)*
- **Servicios de Información**: sesiones remotas (telnet), transferencia de archivos (FTP), dirección de Información (Gopher), *intercambio de archivos utilizando protocolos P2P (Peer-to-Peer)*
- **El World Wide Web (WWW)**

De todos los servicios mencionados, los que se están usando con mayor intensidad y que están generando impacto a los proveedores de acceso a Internet en la actualidad son: el intercambio de archivos utilizando protocolos P2P y la voz sobre Internet.

1.2.1 Intercambio de archivos utilizando protocolos P2P

Los servicios basados en protocolos P2P permiten una computación cooperativa, social, mediante la comunicación directa entre dispositivos. Los protocolos P2P (peer-

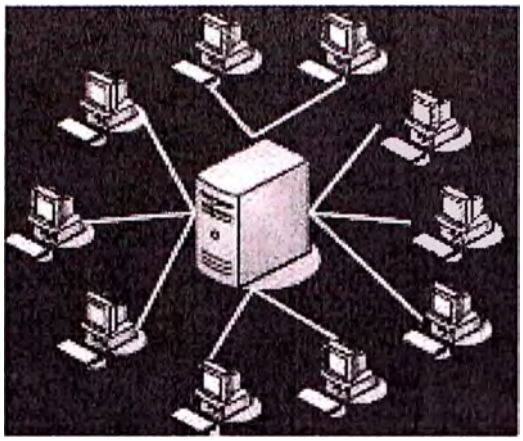


Figura 1.3: Modelo de red Cliente-Servidor

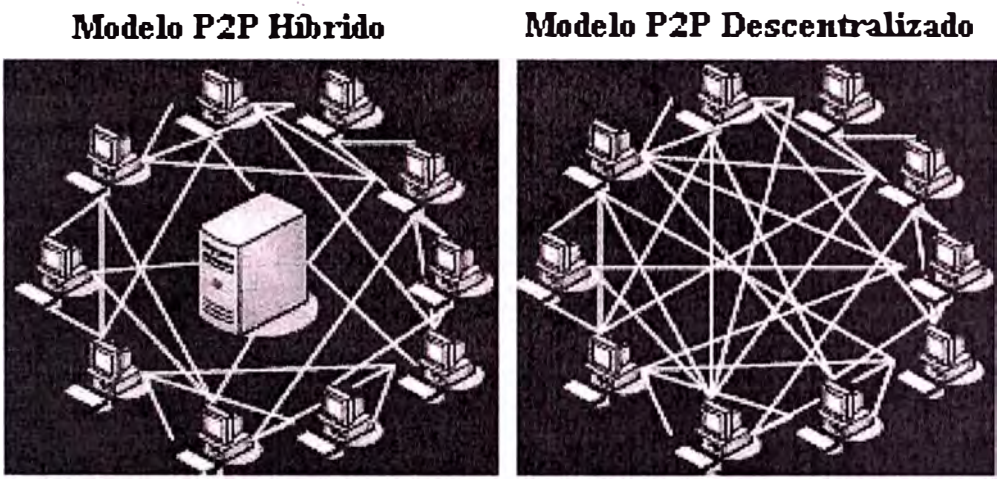


Figura 1.4: Modelo de red P2P

to-peer) definen un tipo de red en la que todos los participantes son servidores y clientes a la vez (estructura de red descentralizado), tiene una filosofía opuesta a la estructura de red típica en Internet, de cliente-servidor, donde existe un servidor y muchos clientes (estructura de red centralizada) tal como se muestra esquemáticamente en la figura 1.3. En la implementación, el protocolo P2P presenta dos modelos de red diferenciados: híbrido, que combina la arquitectura centralizado y descentralizado, y el modelo descentralizado propiamente dicho. Ver figura 1.4.

En el cuadro 1.1 se muestra de manera comparativa las diferencias principales de la arquitectura cliente-servidor y P2P, en donde se nota las grandes ventajas de la arquitectuta P2P frente a la arquitectura clásica cliente-servidor.

Existen muchas iniciativas y factores que impulsan el desarrollo de la tecnología P2P, éstos son:

- La creación de protocolos abiertos P2P de intercambios de ficheros, como, por

Tabla 1.1: Cliente-Servidor vs. P2P

Cliente-Servidor	**Peer-to-peer**
Gran ancho de banda requerido por el servidor	Menor ancho de banda requerido en el origen
No escalable	Escalable
Sensible a las caídas del servidor	Robusto frente a caídas

ejemplo, Gnutella.

- La creación de grupos de trabajo, en torno a las cuales se agrupan las empresas del sector con el fin de definir estándares P2P, como, por ejemplo, el Peer-to-Peer Working Group.
- La definición de plataformas P2P genéricas, como JXTA, promovida por Sun.
- La creación de plataformas de servicios distribuidos (sistemas con componentes web y componentes P2P), como Microsoft .NET.
- El desarrollo de sistemas comerciales P2P, como Groove.
- El desarrollo de aplicaciones P2P open source, como, por ejemplo, Opennap o Gnucleus.

El desarrollo de la tecnología P2P alcanza no solamente la descarga de archivos o la piratería sino que es posible ofrecer nuevos servicios, tales como:

- Procesos distribuidos.
- Telefonía Digital.
- Streaming de vídeo.

El presente trabajo está enfocado en el análisis y control de tráfico en Internet ocasionados principalmente por la descarga de archivos, por lo que se presta atención a los distintos protocolos P2P para descarga de archivos que se describen a continuación.

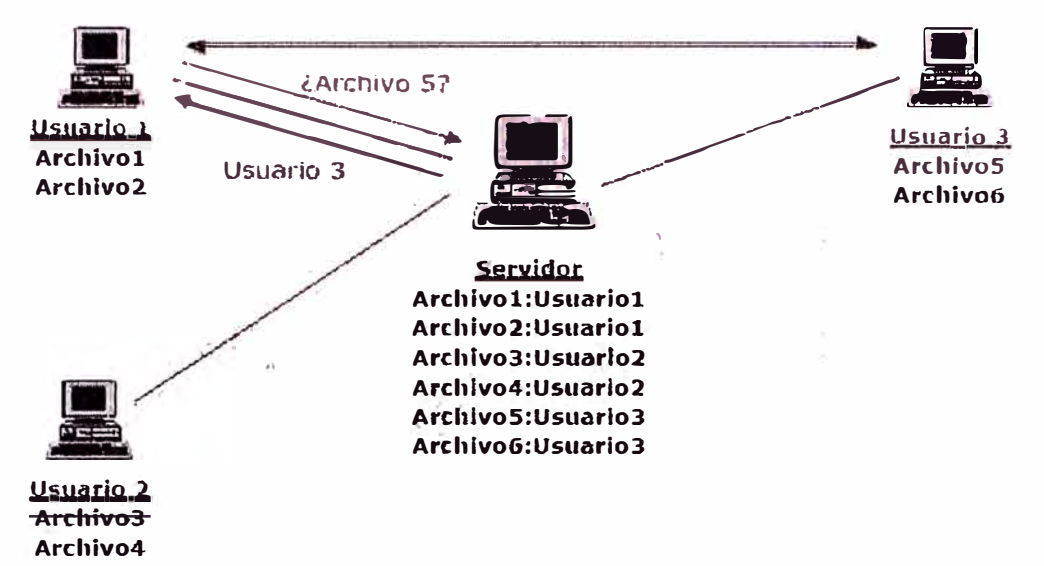


Figura 1.5: Arquitectura de red del protocolo Blubster (Napster)

a. Protocolo Blubster/Piolet.

Blubster es un programa para el intercambio de archivos (P2P) de audio con otros usuarios a través de Internet. El programa puede conectarse a las redes de intercambio más populares, tiene disponibilidad ilimitada de rangos de bits y realiza descargas desde múltiples fuentes.

Blubster usa el protocolo Multipunto P2P (MP2P) Inicialmente se realiza conexión con los servidores centrales de las redes para conocer la lista de los hosts P2P. Las conexiones P2P se realizan con el puerto 80 de TCP.

Blubster es similar al antigüo Napster, donde la lista de archivos locales compartidos se envia a un servidor central, si otro usuario requiere un archivo primero consulta al servidor la dirección IP del usuario que comparte el archivo y después se conecta directamente a la máquina de ese usuario, tal como se puede ver en la figura 1.5

En el 2001, una orden judicial provocó el cierre de Napster, desde entonces los desarrolladores crearon otros protocolos evitando un sólo servidor central, tales como: Fast Track, Gnutella, eDonkey.

b. Protocolo Fast Track.

Fast Track se basa en el concepto de "supernodo". Cuando un usuario lanza una búsqueda, el cliente acude a un supernodo central que a su vez envía la misma pregunta al resto de supernodos regados en Internet. Estos supernodos aparecen y desaparecen de acuerdo al ancho de banda disponibles por los clientes, de ésta manera un usuario, en cierto momento, puede comportarse como supernodo. Este protocolo usa cualquier

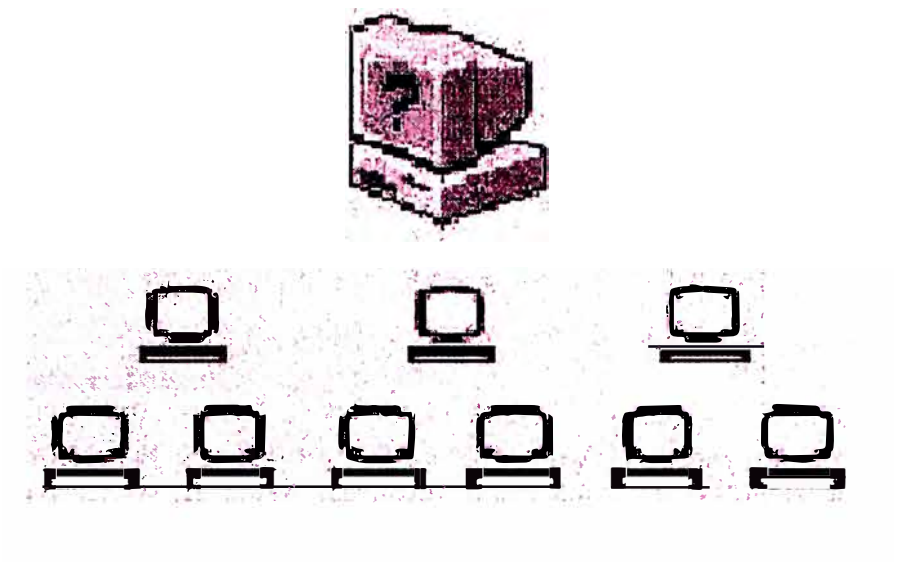


Figura 1.6: Arquitectura de funcionamiento del protocolo Gnutella

puerto abierto UDP/TCP.

Las aplicaciones más comunes con el protocolo Fast Track son KazaA, KazaALite, Grokster e iMesh. Morpheus debido a problemas con Fast Track, actualmente utiliza el protocolo Gnutella. El KazaA es la más utlizada, pero; el problema son los SpyWare´s, aunque el KazaALite es la versión mejorada que intenta superar dicha problemática.

c. Protocolo Gnutella.

Es un protocolo libre de patentes, se puede encontrar en la página web: `www.gnutella.com`, tiene más 50 aplicaciones y se puede usar con casi todos los sistemas operativos. El funcionamiento es el siguiente:

- Un usuario pregunta si existe un archivo.
- El resto de ordenadores contestan si lo tienen
- El usuario se conecta directamente con el ordenador (anfitrión) que alberga el archivo buscado. Ver figura 1.6

Este protocolo usa cualquier puerto abierto UDP/TCP para comunicarse con otro anfitrión P2P y desde allí se conecta a muchos anfitriones.

Las aplicaciones más comunes con el protocolo Gnutella son: BearShare, Limewire, Morpheus y ToadNode.

d. Protocolo eDonKey.

La estructura de red es muy similar a Napster, con la diferencia de que existen varios servidores que almacenan la información sobre la localización de los archivos.

eDonkey utiliza dos puertos, uno para las búsquedas de archivos y otro para las transferencias de archivos. Las búsquedas de archivos se realizan utilizando puertos UDP aleatorios tanto en el origen como en el destino. Las transferencias de archivos se realiza usando un puerto TCP/4662 de destino.

Una limitación de eDonKey es que solamente se puede intercambiar información entre usuarios conectados al mismo servidor.

1.2.2 Voz sobre Internet

Voz sobre Internet es una forma nueva de hacer y recibir llamadas telefónicas utilizando una conexión de Internet de banda ancha (broadband) en lugar de una línea telefónica corriente. VoIP (VoIP: Voz sobre IP) convierte la señal de voz de su teléfono en una señal digital que viaja a través de la Internet hasta llegar al teléfono de la persona que usted está llamando. Si usted llama a un número de teléfono fijo corriente, la señal se reconvierte al llegar al receptor de la llamada.

La telefonía sobre Internet abre un espacio muy importante dentro del universo de la Internet, es la posibilidad de estar comunicados a costos más bajos y es la puerta de entrada de nuevos servicios apenas imaginados.

El desarrollo de la voz sobre Internet se soporta en dos corrientes tecnológicas:

1. **Voz sobre IP tradicional.** Está basado en redes corporativas IP con un sistema central que soporta el servicio. Dentro de los protocolos disponibles en Voz IP tradicional, la combinación de SIP [2] y MGCP/MEGACO es la mejor posicionada, cuya ventaja fundamental respecto de H.323 es la simplicidad. Por otro lado, el alcance de éste protocolo se extiende a otros servicios complementarios como la mensajería instantánea. [4]

2. **Telefonía P2P.** Voz sobre IP a través de Internet mediante tecnología Peer To Peer (P2P) Skype es la aplicación más extendida en la actualidad y que ha sido fundada por los creadores de Kazaa. La gran ventaja de la telefonía P2P frente a la voz sobre IP tradicional es que el flujo de voz circula entre los extremos intervinientes en la comunicación como cualquier otro tráfico de datos,

[2] Según la IETF, SIP es un protocolo cliente-servidor que permite el intercambio de mensajes de texto entre usuarios y otras entidades, con el objetivo de establecer sesiones de audio, vídeo, chat, juegos interactivos y realidad virtual. La sesión se establece a través de un identificador, que, típicamente, será una dirección de correo electrónico, un número de teléfono o cualquier otra dirección asociada al nombre de una máquina de Internet. La trama de un mensaje SIP contiene parámetros que describen las características de las sesiones multimedia que se desean establecer. Se utiliza el protocolo de descripción de sesiones (SDP), que permite identificar el tipo de sesión (audio, vídeo o datos), el ancho de banda requerido, el tipo de codec (G.711, G.723.1, GSM-AMR, H.263, MPEG, etc.), la zona horaria, las claves de encriptación para protección de datos, etc. Aunque SIP no especifica el mecanismo de transporte para los datos multimedia, en la práctica se utiliza el protocolo RTP/RTCP

sin la mediación de ningún servidor que intervenga durante la comunicación, únicamente se emplea al servidor Skype durante el establecimiento de la llamada para conocer la dirección IP que en ese momento tiene el usuario al que queremos llamar. En el modelo P2P la red de la operadora se convierte únicamente en el transporte. [6]

CAPITULO II
PROBLEMÁTICA DE ANCHO DE BANDA DE UN ISP

Para descubrir la problemática existente de ancho de banda de un ISP, se analiza el comportamiento de tráfico Internet en el ámbito nacional (Perú) e Internacional (Global), finalmente se resumen las causas que originan el problema de ancho de banda que actualmente tienen los ISP's.

2.1 Comportamiento de tráfico Internet en el ámbito global

Del estudio de trafico global de Internet, realizado por Cache Logic Research - Junio 2004, mostrado en la figura 2.1, se nota claramente que en EE.UU. y Asia más del 60 % del tráfico a Internet corresponde al tráfico P2P y en Europa y Reino Unido más del 50 % es tráfico P2P.

En resumen el intercambio de archivos P2P supone más del 50 % [5] del volumen de tráfico de Internet, provocado por el gran tamaño de los archivos (música, películas, juegos) intercambiados entre los internautas.

En un segundo análisis de tráfico en Internet realizado por Cisco en el 2004, el que se muestra en la figura 2.2, [7] podemos notar que el tráfico P2P en el ámbito global representa el 70 % del tráfico total en Internet. Adicionalmente en el misma figura podemos apreciar que el eDonkey y el KazaA son los protocolos de intercambio de archivos P2P más utilizados. Del mismo modo utilizando equipos especializados, se determina que con KazaA los puertos TCP más utilizados son: 1214, 80, 2227, 3812 y 2287.

En resumen podemos ver que el tráfico P2P en Internet es el más representativo y por ende genera un impacto significativo en el ancho de banda de los proveedores de acceso a Internet.

2.2 Comportamiento de tráfico Internet en el Perú

El análisis de tráfico que se presenta se realiza sobre la base de un un estudio de tráfico Internet realizado por Telefónica del Perú en el 2006.

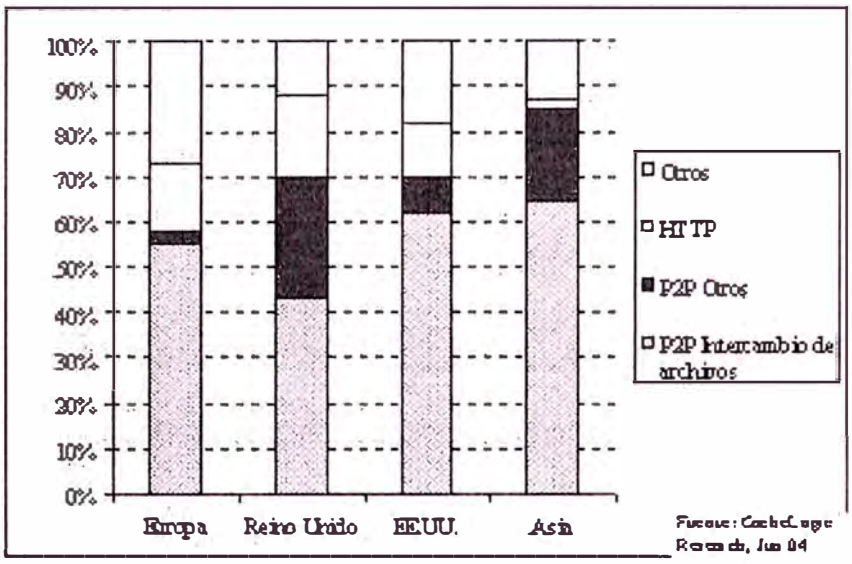


Figura 2.1: Análisis de Tráfico Global de Internet

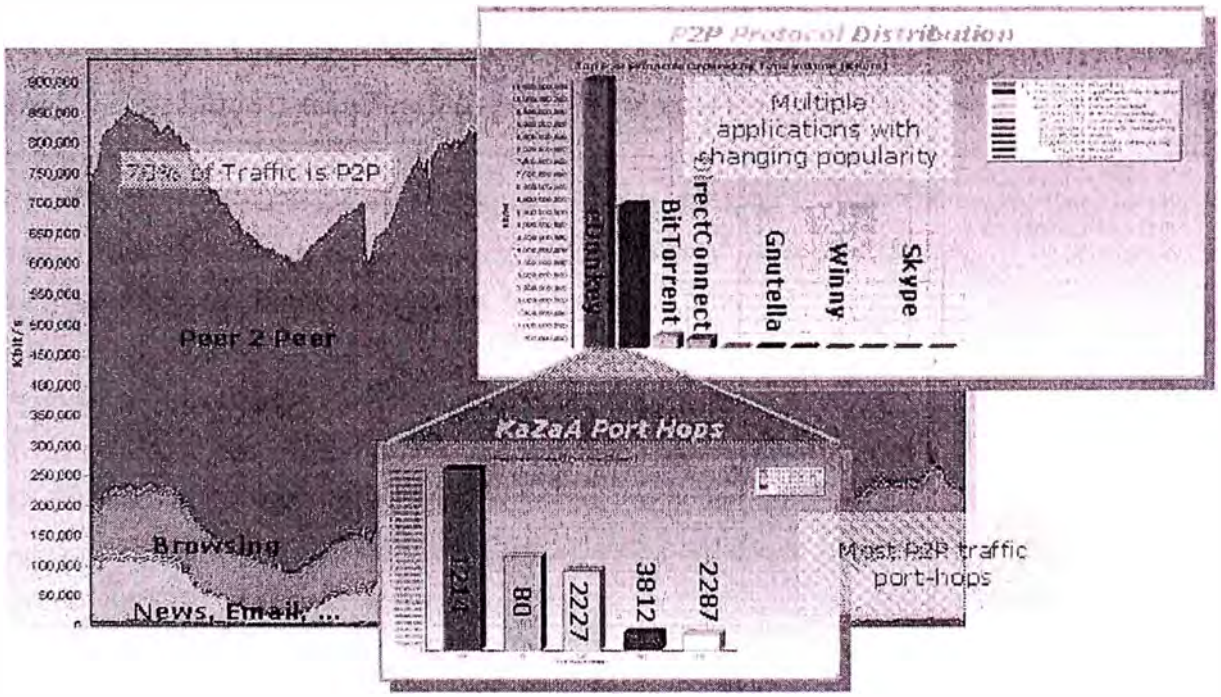


Figura 2.2: Análisis de Tráfico Internet por Aplicaciones

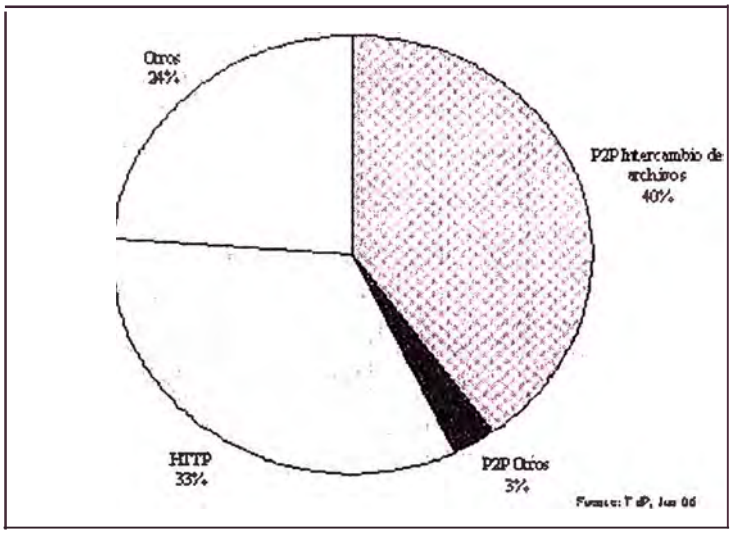


Figura 2.3: Análisis de Tráfico de Internet en Perú

Dado que en el mercado peruano existen tres tipos de usuarios diferenciados: cabinas, heavy user's y usuarios comunes, además del comportamiento de tráfico total por aplicaciones, se analiza el tráfico Internet por cada uno de los tres usuarios típicos identificados en el Perú.

2.2.1 Tráfico Internet total por aplicaciones

En la figura 2.3, se aprecia que el tráfico P2P representa el 40 % del tráfico total a Internet (Junio 2006), está seguido por el tráfico web (http) que representa el 33 % del tráfico total.

El 40 % de tráfico P2P es bastante representativa, si consideramos que el mercado peruano aún está en desarrollo, ésta cifra podría incrementarse con el tiempo hasta llegar a niveles similares al de Asia ó Europa.

El incremento del uso de los protocolos P2P para intercambio de archivos está generando la saturación del enlace a Internet de los Proveedores de acceso a Internet, como Telefónica del Perú (TdP) que brinda el servicio de acceso a Internet de banda ancha (Speedy) La necesidad de mantener satisfechos a todos los clientes obligan, al proveedor, incrementar el ancho de banda del enlace a Internet que impacta directamente en los costos del servicio.

2.2.2 Tráfico Internet por tipo de usuarios

De la figura 2.4 se concluye que entre las cabinas públicas de Internet y los heavy user's consumen el 51 % (cabinas: 23 %, heavy user's: 28 %) del ancho de banda total del acceso a Internet, sin embargo; sólo representan el 12 % (cabinas: 7 %, heavy user's:

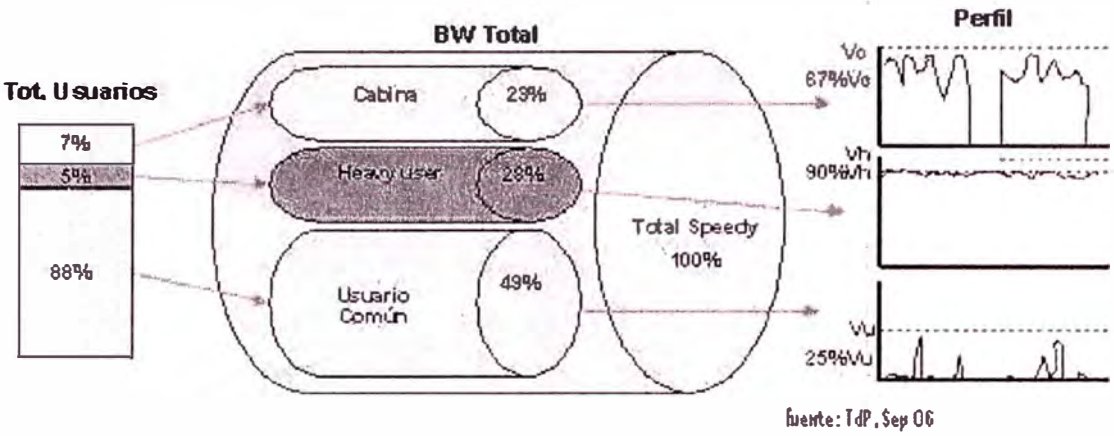


Figura 2.4: Tráfico Internet en Perú por tipo de usuario

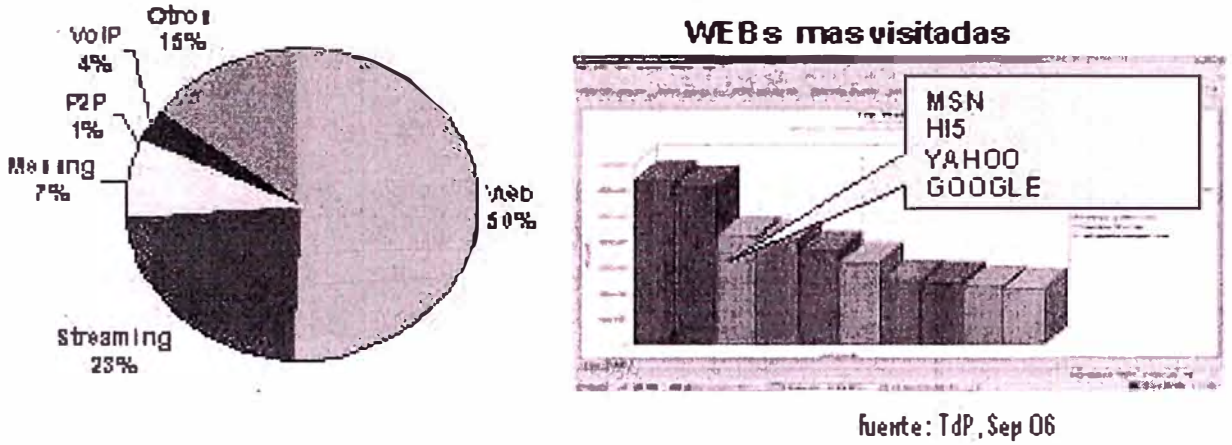


Figura 2.5: Tráfico de las cabinas públicas Internet en el Perú

5 %) de la planta total de usuarios de banda ancha. Los usuarios comunes representan el 88 % de los usuarios totales de banda ancha, pero consumen solamente el 49 % del ancho de banda total del ISP.

- **Cabinas públicas de Internet**. El perfil de tráfico de las cabinas se caracteriza por el alto consumo durante el día y parte de la noche. Las aplicaciones de mayor consumo son: Web (50 %), Streaming (23 %), Messenger (7 %) y VoIP (4 %) Ver figura 2.5.

- **Heavy user's (usuarios intensivos)**. El perfil de tráfico de los heavy user's es permanente durante las 24 horas del día, además es consumidor intensivo de aplicaciones P2P (77 %) y VoIP (3 %) Ver figura 2.6.

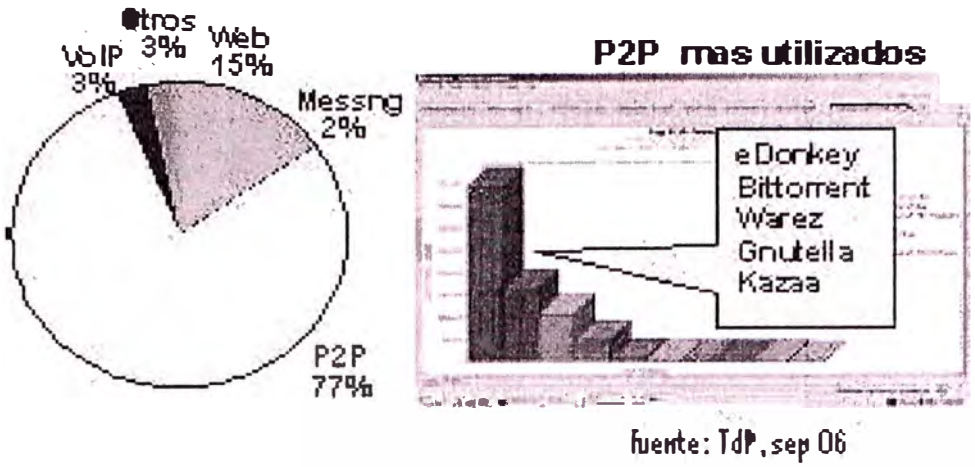


Figura 2.6: Tráfico Internet de los Heavy User's en el Perú

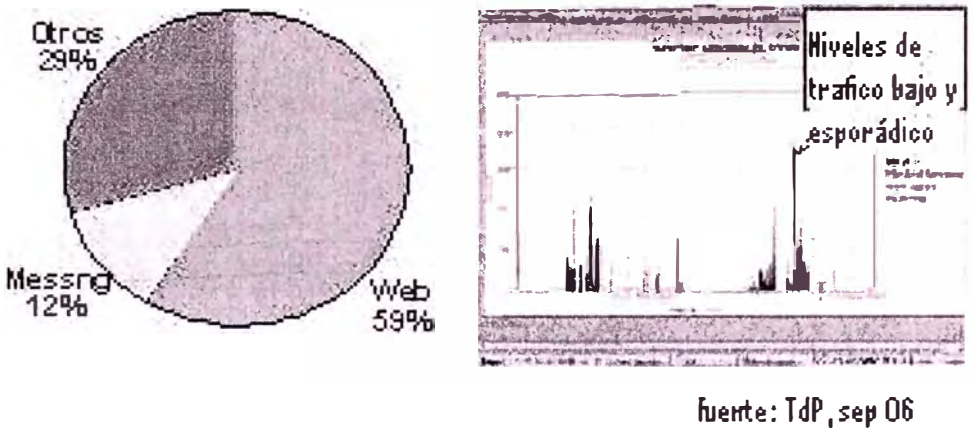


Figura 2.7: Tráfico Internet de los usuarios comunes

- **Ususarios comunes.** Los usuarios comunes se conectan solamente algunas horas del día y consumen principalmente aplicaciones web (59 %) y messenger (12 %). Es decir, un usuario común es un consumidor esporádico de aplicaciones Web. Ver figura 2.7.

En resumen, el 12 % de usuarios cabinas y heavy user's consumen el 51 % del ancho de banda del ISP. En consecuencia, dado que todos los usuarios cuentan con el mismo servicio, el costo del proveedor para brindar el servicio de banda ancha es mayor para los heavy user's y las cabinas públicas de Internet.

2.3 Causas del problema de ancho de banda de un ISP

A continuación se resumen las principales razones que originan el problema de ancho de banda que actualmente tiene un ISP:

- **Tráfico P2P**. Como debe haber concluido, el problema de ancho de banda de los ISP's se origina principalmente por el tráfico P2P. Está tan extendida las aplicaciones de intercambio de archivos con P2P que se puede considerar el *Killer aplication de Internet.* [5]. El P2P son utilizados principalmente para descargar archivos a su computadora y compartir archivos para otros usuarios que consumen tanto ancho de banda que sea posible. Normalmente intentan transferir varios archivos al mismo tiempo. Los IPS's necesitan satisfacer todo tipo de tráfico ó clases de servicios, tales como: Web, voz sobre IP, juegos y transferencias directas regulares que no son P2P. Si el P2P consume repentínamente mucho ancho de banda, la calidad de los otros servicios se perjudica, y los usuarios se quejan de la mala calidad del servicio.

- **Red de acceso asimétrico**. El tráfico P2P es simétrico, en consecuencia requiere de redes de acceso simétricas, sin embargo; las redes de acceso que actualmente utilizan las grandes operadoras son asimétricas, tales como el ADSL y la red cable.

- **Penetración de la red de banda ancha**. El atractivo de compartir archivos originales de manera gratuita en toda la red ha incrementado la penetración de la red de banda ancha.

Estos proveedores de acceso a Internet (ISP's) se encuentran dentro de un gran dilema respecto al fenómeno del intercambio de archivos P2P, por una parte; se ha incrementado en gran medida la demanda de conexiones de banda ancha, por otro lado los usuarios generan un intenso tráfico que aumenta los costos del enlace a Internet. La única forma de combatir ésta problemática, para el ISP, es racionalizando el uso de la conexión a Internet. [1]

CAPITULO III
FORMAS Ó TECNOLOGÍAS DE CONTROL DE TRÁFICO IP POR APLICACIONES

Para resolver la problemática de ancho de banda de un ISP, existen dos principales alternativas: implementación de cache's y el control de tráfico aplicando algunos criterios que el ISP puede implantar. El presente trabajo se enfoca principalmente al control de tráfico por aplicaciones ó por servicios en Internet (P2P, Voz sobre IP, Web, etc.) En el presente capítulo se describen las principales formas tecnológicas ó tecnologías que existen para realizar el control de tráfico Internet por aplicaciones.

3.1 Control de tráfico IP en el Router de Interconexión

Para brindar el servicio de acceso a Internet, los ISP's utilizan uno o más router's para conectarse a la red internacional de Internet (backbone Internet) Este elemento de red permite enrutar el tráfico IP de todos los usuarios a Internet, por lo que es posible controlar el tráfico en dicho router utilizando algunas funcionalidades que éstos equipos poseen (ver figura 3.1) A continuación se estudiará la forma y/o las funcionalidades existentes en los routers para controlar el tráfico IP.

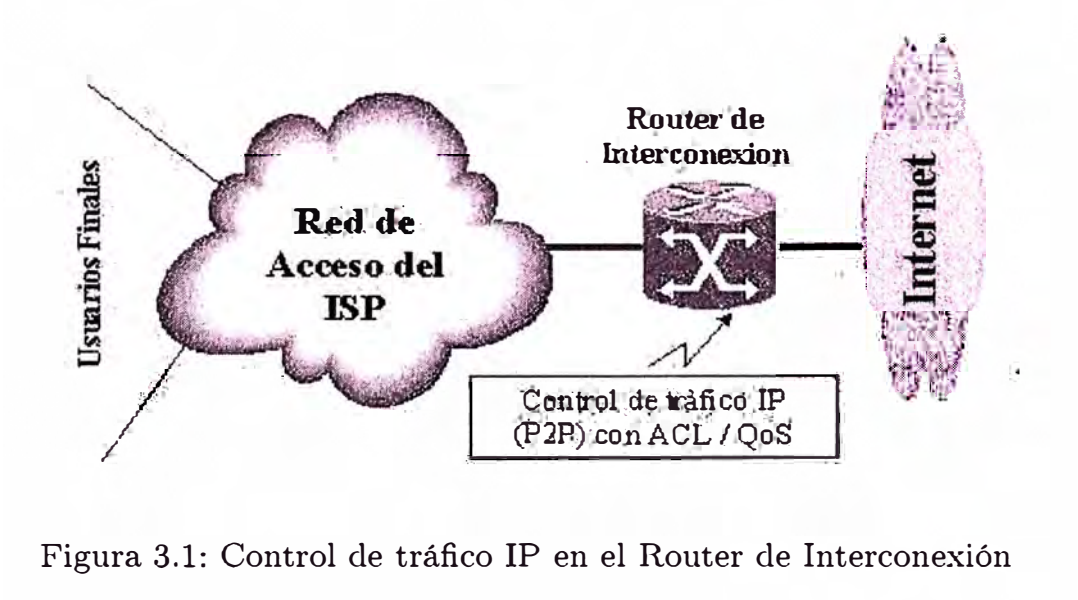


Figura 3.1: Control de tráfico IP en el Router de Interconexión

3.1.1 Acces List (ACL) ó Calidad de Servicios (QoS) por puertos TCP/UDP

Una de las funcionalidades de los router's es de filtrar el tráfico IP (funcionalidad denominada Acces List -ACL) ó aplicar políticas de calidad de servicio (QoS) por direcciones IP y puertos: TCP, UDP. Si tomamos en cuenta que algunos protocolos P2P estudiados utilizan ciertos puertos TCP o UDP definidos, entonces existe la posibilidad de realizar el control de tráfico aplicando ACL y/o QoS por puertos. A continuación se indica si existe la posibilidad de realizar algún control de tráfico IP por protocolos P2P para intercambio de archivos según los protocolos estudiados en el capítulo 2.

- **Control de tráfico Blubster.** Dado que para realizar la conexión P2P utiliza un servidor central conocido para publicar los hosts que poseen el archivo buscado, entonces si se bloquea dicho servidor utilizando acces acces list (ACL), no será posible descargar la lista de hosts disponibles y por lo tanto realizar el intercambio de archivos, ésto implica inhabilitar el programa P2P. No es posible aplicar QoS, dado que el puerto utilizado es el puerto 80, puerto que es utilizado por las aplicaciones Web.

- **Control de tráfico Fast Track**. Dado que utiliza puertos TCP/UDP aleatorios no es posible aplicar acces list (ACL) ni QoS por puerto.

- **Control de tráfico Gnutella**. En éste caso también se utiliza puertos TCP/UDP aleatorios, en consecuencia es imposible aplicar ACL ni QoS por puerto.

- **Control de tráfico eDonKey**. Dado que en éste protocolo se utiliza un puerto TCP definido (4662) para la descarga de archivos entonces es posible bloquear parcialmente utilizando ACL y aplicar políticas de QoS en dicho puerto. Se dice parcial, porque los usuarios utilizan otro puerto UDP aleatorio para la búsqueda de archivos en la red, por lo que es posible que visualicen los archivos compartidos pero no podrán descargar a menos que se cambie las opciones del programa para utilizar un puerto TCP distinto a 4662.

3.1.2 Funcionalidades especiales (NBAR)

NBAR (Network Based Application Recognition), es una funcionalidad existente únicamente en equipos de marca Cisco y series específicas (2600-XM, 3700, 7206, 7300 y 7500)

El NBAR posee dos funcionalidades:

1. **Identificación de aplicaciones y protocolos en capa cuatro (L4) y capa siete (L7)** Es decir descubre automáticamente el tipo de trafico que se cursa

por el router y puede clasificar aplicaciones que usan : TCP/UDP, no-UDP/no-TCP, puertos dinámicos TCP/UDP, sub-clasificación en HTTP (URL, mime o nombres), citrix, RTP, etc.

2. **Protocolo discovery** (Protocol Discovery), comúnmente es usado por NBAR para colectar estadísticas de las aplicaciones y protocolos (número de paquetes, número de bytes, etc.)

Con la funcionalidad NBAR, se puede reconocer una amplia variedad de aplicaciones, incluyendo las basadas en Web y Cliente/Servidor. Una vez que éstas aplicaciones son reconocidas, es posible invocarlas para una aplicación particular: control de tráfico, filtro de ICMP, reservar ancho de banda (BW), etc.

El NBAR es una aplicación basado en el sistema operativo del router (IOS), por lo que el uso impacta sustancialmente en el CPU, razón por la que los fabricantes, como Cisco, no ofrecen ésta funcionalidad para equipos de mayor capacidad, por el contrario recomiendan utilizar equipos dedicados para ésta función.

3.2 Control de tráfico IP con equipo especializado dedicado

Ante la problemática de ancho de banda, que los grandes proveedores de acceso a Internet se enfrentan en la actualidad, dado que sus niveles de tráfico Internet están por el orden de los 10Gbps, los fabricantes de equipos de telecomunicaciones ofrecen soluciones utilizando equipos especializados y dedicados para el control de tráfico IP, interconectados tal como se muestra en la figura 3.2. Estos equipos por lo general tienen como función monitorizar y controlar el tráfico Internet por aplicaciones, de manera agregada ó por cada uno de los usuarios que el ISP posee. Es decir, es posible definir políticas de control de ancho de banda a nivel de aplicaciones (P2P, VoIP, HTTP, e-mail, etc.) y por cada usuario, tal como se muestra a manera de ejemplo en la figura 3.3 [10].

De los distintos fabricantes que ofrecen soluciones con equipamiento de control de tráfico IP especializado, describimos la oferta de los dos más representativos: Cisco (SCE) y Allot (NetEnforcer)

3.2.1 Solución Cisco: Plataforma SCE (Service Control Engine: Motor de control de Servicio)

La plataforma SCE combina el procesamiento detallado y flexible por usuario del tráfico de la red, con un elemento de red dedicado, programable y de gran rendimiento.

El equipo SCE está estratégicamente ubicado en el borde de la red, que permite que se realice una inspección profunda de cada paquete IP que atravieza por el equipo. Sobre

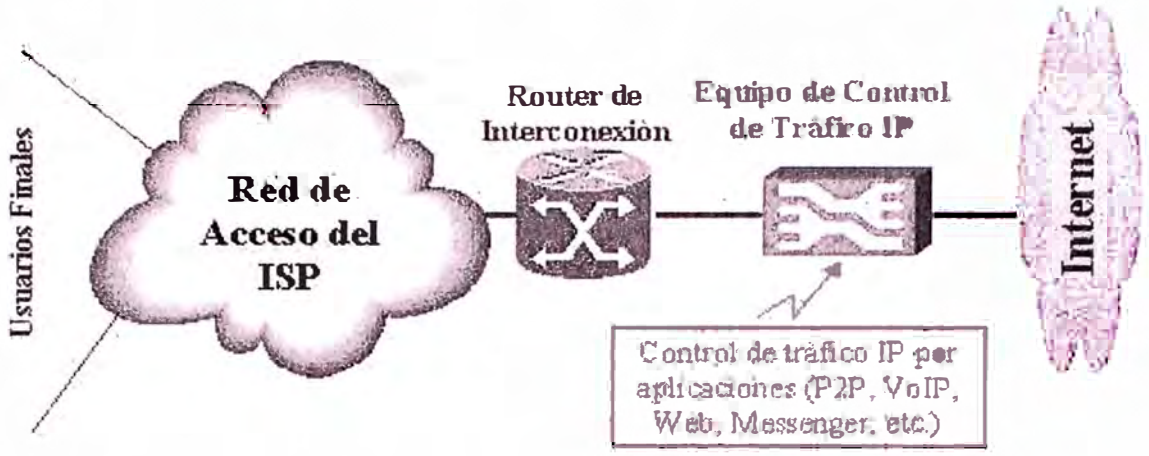


Figura 3.2: Control de tráfico IP con equipo especializado dedicado

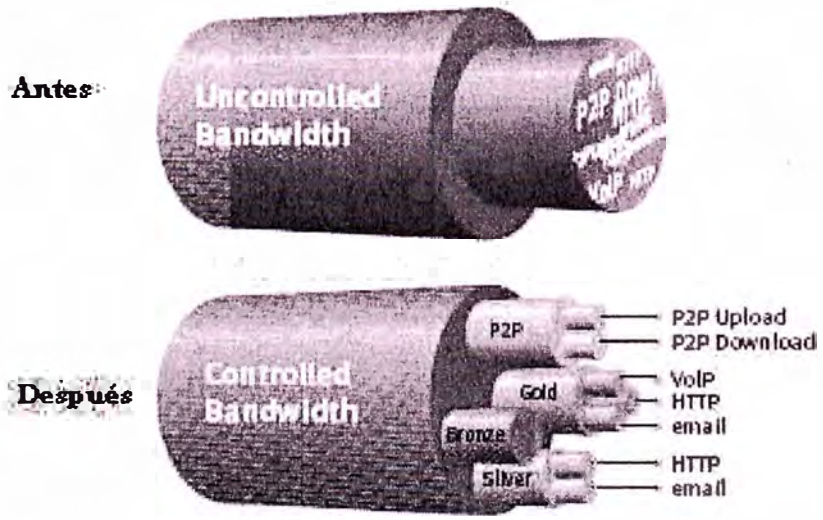


Figura 3.3: Ejemplo de control de tráfico IP por aplicaciones

la base de ésta inspección, la plataforma SCE puede llevar a cabo el reconeocimiento de las aplicaciones que se usan y es posible clasificarlo a nivel de sesiones y aplicaciones, del mismo modo; es posible monitorizar, aplicar una política de control y realizar la contabilidad por cada usuario.

La plataforma SCE cuenta con distintos módulos y componentes, tal como se puede apreciar en el diagrama de arquitectura mostrado en la figura 3.4, los cuales se describen a continuación:

a. El equipo de red SCE.

Es un equipo de red de gran rendimiento, es programable, ideal para balancear y flexibilizar la demanda de los ISP's que son intensivos en consumo de ancho de banda y cómputo de direcciones IP. Es el encargado de clasificar y realizar el control del tráfico definidas por la solución. Soporta diferentes modos de usuarios el cual te provee diferentes niveles de control con diferentes conceptos de integración, éste modo de operación permite controlar y medir el tráfico por grupo de usuarios. Existe dos modelos actualmente comercializados: SCE 1000 y SCE 2000[1] (mayor información de las especificaciones de éstos equipos ver el anexo A1) Algunos de los atributos importantes comunes a todos los equipos son:

- Máximo rendimiento y densidad de usuarios.
- Mecanismo de bypass integrado y automático: todos los dispositivos incluyen un mecanismo de bypass interno, ésto asegura la conectividad de la red cuando el equipo no esté operando adecuadamente por razones diversas e incluso de la pérdidad de energía.
- Un puerto para gestión fuera de banda. Posee una interfase 10/100 por lo que el equipo podrá ser monitorizado y gestionado, en forma independiente. Además cuenta con funcionalidades de filtro en el puerto de gestión para limitar el acceso de virus ó spyware's especiales y los puertos TCP/UDP.

Para una mayor comprensión del funcionamiento del equipo SCE se describe con más detalle el proceso de clasificación y control que el equipo realiza [9]:

1. **Proceso de clasificación.** El tráfico entrante es clasificado inicialmente a un protocolo y correlacionado a un usuario (éstos son procesos independientes) Sobre

[1]SCE 2000, provee cuatro interfases Gigabit Ethernet de fibra óptica (SX ó LX), puede procesar hasta 4Gbps de tráfico, capacidad máxima de 80,000 usuarios y se instala de manera redundante 1−1 con dos enlaces GE simultáneos.
SCE 1000, provee dos interfases Gigabit Ethernet de fibra óptica (SX ó LX), puede procesar hasta 2Gbps de tráfico y capacidad máxima de 40,000 usuarios.

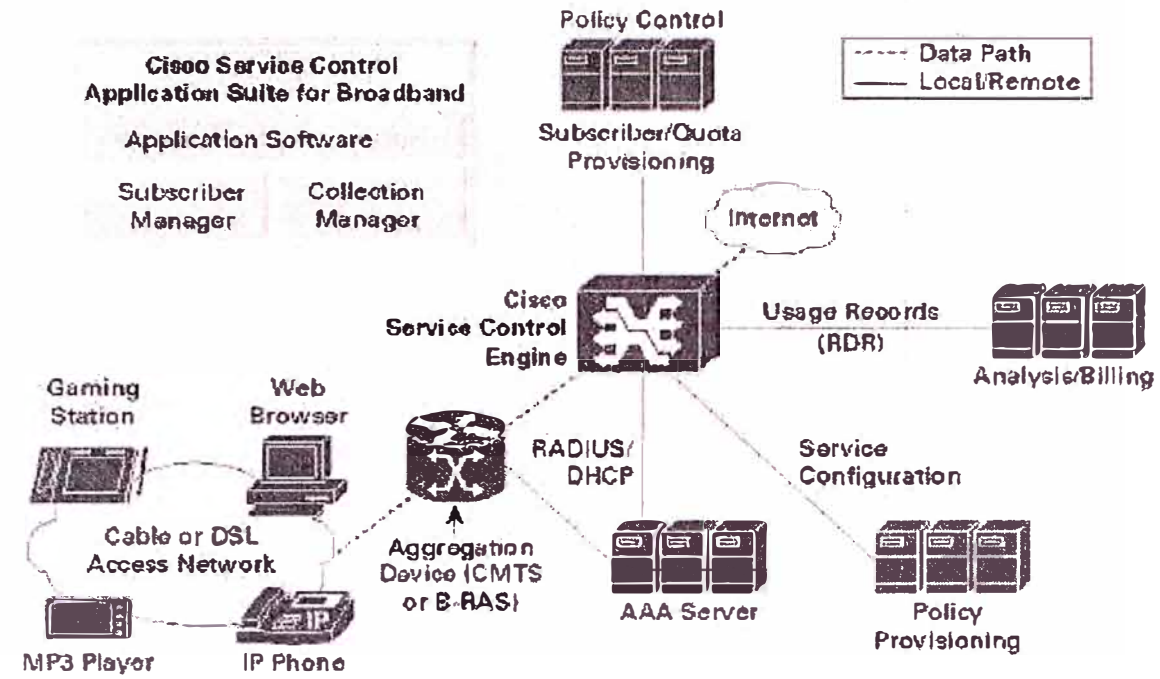


Figura 3.4: Arquitectura de la plataforma SCE de Cisco

la base de esta clasificación el tráfico es agrupado en grupos lógicos en término de servicios y grupo de usuarios, luego se selecciona las reglas ó políticas (parámetros) de control. Una vez seleccionado los parámetros de control se aplican sobre el tráfico cursado. Ver figura 3.5.

a) ***Clasificación de protocolos.*** Cuando se reciben los paquetes en el equipo SCE, se agrupan en flujos [2]. Cada flujo se clasifica por protocolo [3] que usa un puerto de destino ó una aplicación (firma) Sobre la base del intercambio de mensajes de los protocolos con la capa de aplicación (capa 7), los flujos adicionales pueden agruparse como flujo relevante. El operador puede manipular la lista de protocolos en el equipo con el puerto de gestión ó de consola (El SCE viene preconfigurado con aproximadamente 600 protocolos comunes) Es importante notar que existen aplicaciones que requieren mayor inspección cuyo proceso de clasificación se realizan con micro-flujos:

   1) Un ejemplo es RTSP (streaming) o SIP (voz) que usan flujos distintos

[2]Un flujo se define como la circulación de paquetes en ambas direcciones sobre una conexión simple en la capa de aplicación (ejm: conexión TCP ó UDP), el paquete se identifica por el siguiente tuple: <IP origen, IP destino, Puerto origen, Puerto destino, Protocolo IP>(note que para los flujos donde el puerto TCP ó UDP no es conocido se utiliza el número "0") El Tuple es un término de la teoría determinada que refiere a una colección de una o más cualidades.

[3]Un protocolo ó una firma, es un set de patrones y mensajes que identifican cierto protocolo de la capa de aplicación. Las firmas de protocolos pueden ser combinados con números de puertos específicos o no definidos (muchos de los protocolos de P2P, no usan un número de puerto específico)

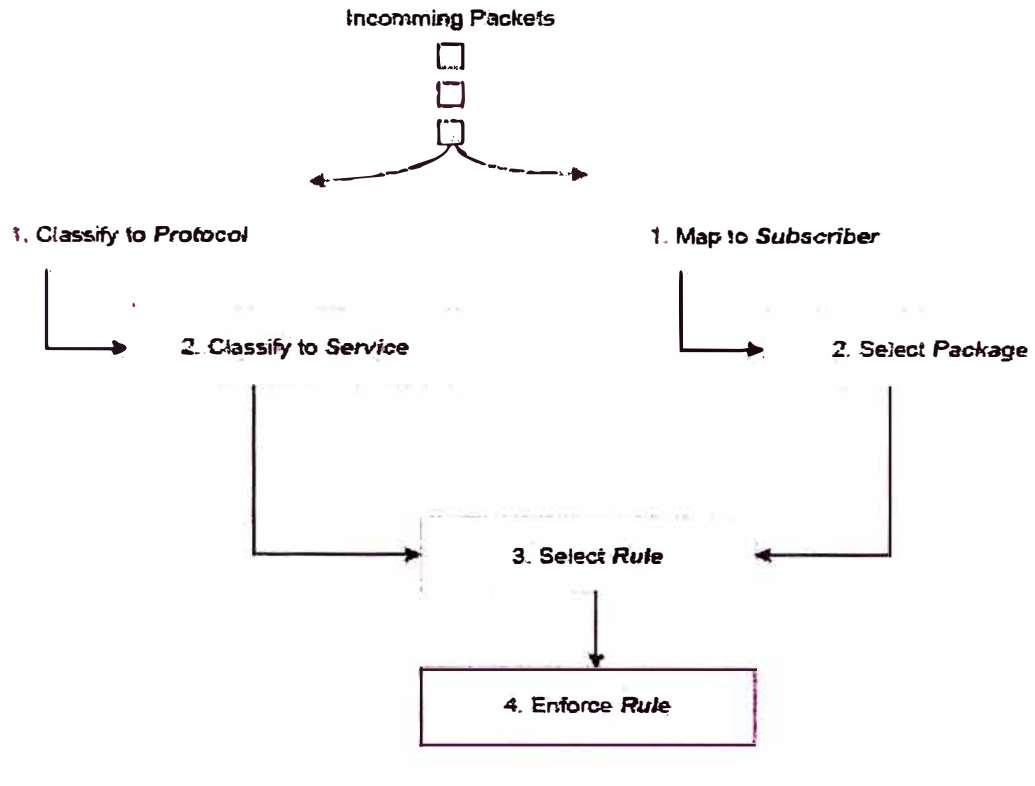


Figura 3.5: Proceso de clasificación en el SCE

para las transmisiones y señalizaciones. En éste caso, el proceso de clasificación detecta los números de puertos que negocian los micro-flujos y los agrupan en un solo paquete (flujo virtual)

2) Algunos protocolos no usan un número de puerto definido (principalmente P2P) y por lo tanto, además de interferencias por los números de puertos que pueden ser atribuidos a ellos, son buscados activamente como micro-flujos. Esto se lleva a cabo buscando una firma especial y comportamiento único de éstos protocolos en un micro-flujo (típicamente en el otro extremo de la comunicación existen varios paquetes que inician el flujo)

b) ***Clasificación de servicios.*** Cuando hay muchos protocolos, tienen que ser agrupados en entidades que pueden ser seguidas y controlados en forma paralela, éste grupo es un servicio. En cuanto se clasifica a un protocolo se define la lista de servicios para identificar el servicio al que pertenece. Algunos ejemplos de servicios son: todos los protocolos P2P (FastTrack_KazaA, Gnutella, WinMX, Winny, eDonkey, Hotline, Manolito, Dynamic-P2P), mail, noticias y protocolos de web (POP3, SMTP, HTTP Browsing, FTP, NNTP) Los parámetros de flujo que correlacionan el tipo de servicio son:

1) Protocolo (basado en la clasificación previa)
2) Iniciador (opcional): si el flujo fue iniciado por una entidad sobre el usuario ó es iniciado por el equipo SCE.
3) Lista (opcional): una lista del destino de la transacción. Este puede ser un único destino fijo (ejemplo: tráfico Web) o atravesar enlaces diferentes (ejemplo: tráfico P2P)

c) ***Mapeo del usuario.*** Es la habilidad de definir a "usuarios" múltiples y crear un motor de observación y ejecutor de tráfico virtual para cada uno de éstos abonados. Esto permite controlar recursos de la red por cada usuario, y monitorizar el uso de la red de manera individual por cada entidad definida. Un usuario se define con tres parámetros:<subscriber-ID, network-ID, policy-ID>

1) Suscriber-ID. Es una identificación lógica del usuario. Esta identificación se refiere al usuario como un objeto (en éste campo puede ir incluso el documento de identidad)
2) Network-ID. Es una lista de uno ó más direcciones IP que pertenecen al usuario que permiten correlacionar qué tráfico pertenecen a dicho usuario.
3) Policy-ID. Es una lista de parámetros que definen qué política aplicar sobre el tráfico del usuario.

d) ***Selección de reglas.*** Como se dijo anteriormente, para cada usuario se fija su policy-ID (lista de parámetros) como parte de su política. Esta identificación hace referencia a un paquete que contiene reglas (opcionalmente) para cada servicio. Cada regla contiene las acciones que se realizan por cada flujo clasificado en un servicio particular. Los parámetros de la regla, su semántica y el significado se describen en el Proceso de Control.

2. **Proceso de Control**. Se aplica una regla por un solo flujo y se divide en varios pasos, tal como se muestra en la figura 3.6.

a) ***Control de flujo, de usuario y ancho de banda global***. Una regla puede especificar para bloquear o desviar un flujo especial (puede servir para implementar un portal cautivo) [4], también para poner restricciones de ancho de banda de manera granular. Las reglas pueden afinarse con parámetros distintos para diferentes horas del día (ejemplo: reglas para la hora pico

[4]Permite intervenir en la aplicación http para desviar las solicitudes de aplicaciones web a un portal web específico designado por el ISP. Se utiliza cuando el ISP gusta de excibir una pantalla inicial denominado portal cautivo.

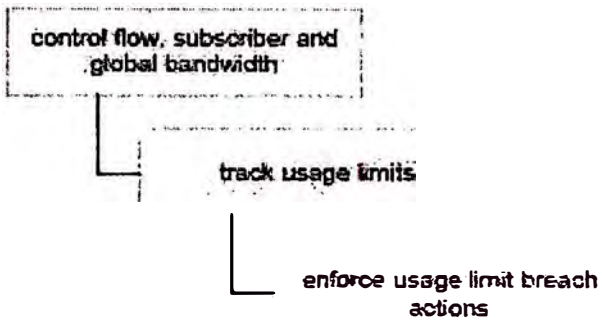


Figura 3.6: Proceso de Control en el SCE

versus las horas menos cargadas) Es posible realizar el control de ancho de banda jeráquico y multi-dimensional, es decir que es posible controlar el ancho de banda en varios niveles simultáneamente:

1) Por transacción (ejm: descarga de un archivo P2P)
2) Por usuario (ejm: tráfico total de upstream/downstream de un usuario particular)
3) Por usuario/servicio (ejm: tráfico total P2P de upstream/downstream de un usuario particular)
4) El tráfico de un servicio particular combinado de todos los usuarios (ejm: tráfico total P2P de upstream/downstream en el equipo SCE)

b) ***Límite de uso***. Cada regla puede definir un límite de uso para el consumo de un servicio y un usuario particular. Esto puede incluir los límites sobre el volumen y la cantidad de sesiones (en un flujo ó un paquete de flujos) en un cierto período de tiempo (ejemplo: un día)

c) ***Acciones para el incumplimiento del límite de uso***. Cuando se ha llegado al límite de uso, se define un juego diferente de acciones para el tráfico asociado al servicio y usuario particular.

Para mayor comprensión del proceso de control se presentan algunos ejemplos sencillos aplicados para el servicio P2P, aunque lo mismo es plicable para otros servicios.

- Limitar todo el tráfico P2P a 150Mbps (downstream) y 50Mbps (upstream), excepto los fines de semana.
- Limitar todo el tráfico P2P a 150Mbps (downstream) y 50Mbps (upstream), excepto los generados por usuarios de cierta sub-red.
- Limitar todo el tráfico P2P a 150Mbps (downstream) y 50Mbps (upstream) con un límite por usuario de 128Kbps/64Kbps para el tráfico de P2P.

- En congestión, priorizar usuarios con tráfico P2P respecto de otros.
- Tráfico ilimitado para los primeros 20Mbytes, luego reducir el tráfico P2P de cada usuario a 64Kbps/32Kbps.

b. Administrador de usuarios (SM: Subscriber Manager)

Es el módulo de software que opera cuando se trabaja en modo subscriber (usuario) En éste modo, el tráfico de cada usuario se controla individualmente de acuerdo a una política específica. Este módulo trabaja con la información que proveen otros servidores de servicio como el Radius ó DHCP, las principales informaciones que se éstos servidores proveen son:

- La dirección IP de los usuarios que son asignados dinámicamente en la mayoría de servicios de banda ancha.
- Las políticas aplicadas a cada usuario.

En los diagramas presentados en la figura 3.7, se muestran el intercambio de mensajes, entre un servidor Radius y el Suscriber Manager, durante el registro de entrada y salida del sistema de un usuario en una sesión.

El Subscriber Manager (SM) gestiona uno o más equipos SCE y provisiona éstos equipos con la información del usuario en tiempo real de acuerdo a la topología de red implementada:

- La conexión con los equipos SCE puede realizarse de manera local (Red Local: LAN) ó remota a través de redes IP.
- Envía la información de los usuarios que ingresan, salen ó cambian de política a todos los equipos SCE interconectados con el SM.
- Almacena la información de los usuarios y provee respuesta realizado por los usuarios a los equipos SCE.
- Almacena información del uso y las políticas por sesiones de cada usuario.
- Maneja la caída de servicio del equipo SCE y asegura las condiciones máximas de reinicio óptimo del mismo.

El Suscriber Manager provee una API a través del cual puede provisionarse la información del ususario en los equipos SCE y en tiempo real. Esta API soporta C/C+− y Java.

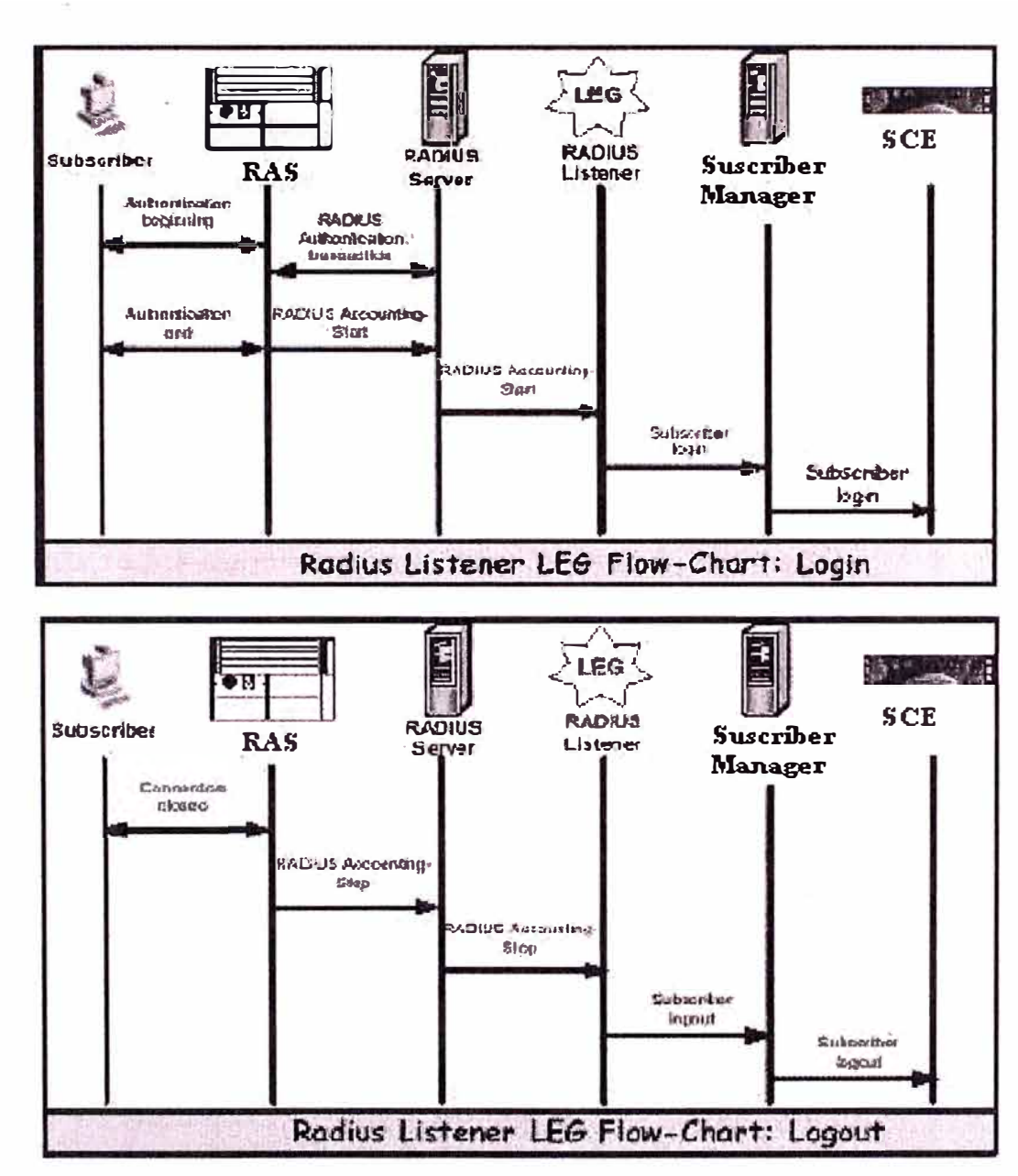


Figura 3.7: Intercambio de mensajes, de entrada-salida al sistema, entre el SM y el Radius

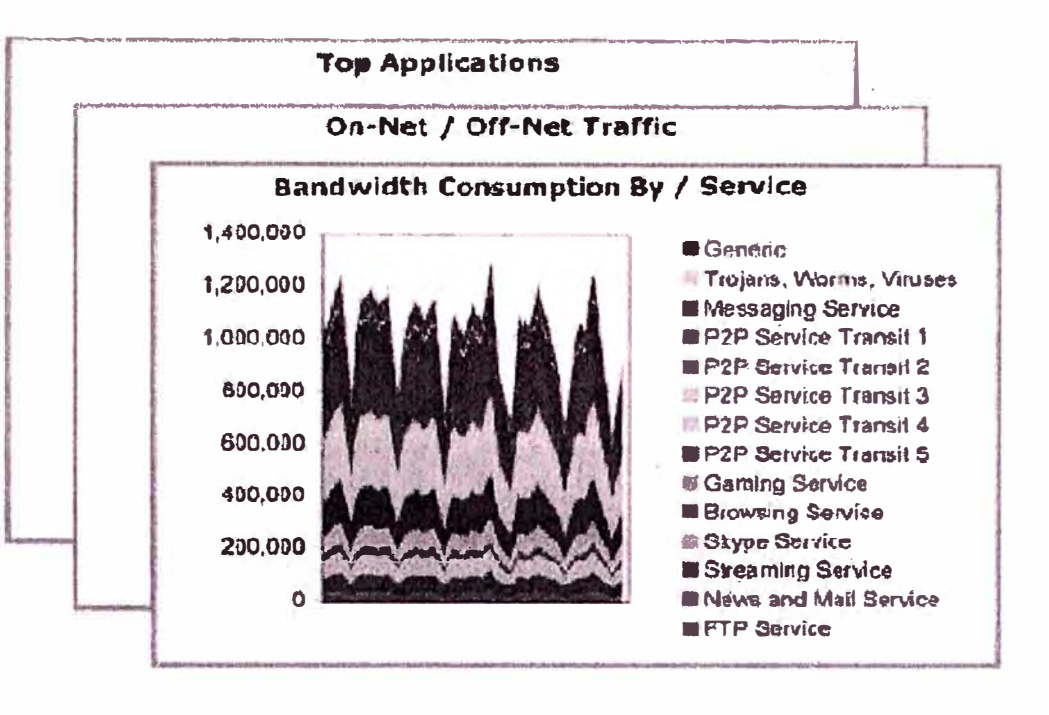


Figura 3.8: Informes de volumen y ancho de banda - Plataforma SCE

c. Administrador de colección (CM: Collection Manager)

El Collection Manager (CM), es un componente de software que colecciona estadísticas de la red e información de uso de los usuarios en uno ó más equipos SCE. Procesa éstos datos y los almacena en una base de datos local RDBMS (incluido en el software) ó como archivos simples CSV.

Los datos en la base de datos pueden ser consultados utilizando herramientas propios de la solución SCE, el cual produce varias clases de informes, tal como se puede apreciar en el informe de volumen y ancho de banda y protocolos top (denominado de monitoreo) que se presentan en la figuras 3.8 y 3.9 (más ejemplos de informes ver en el anexo A1.6) También puede accederse usando interfaz SQL ó programas propios desarrollados por el cliente.

Los archivos CSV proveen una interfaz simple para la tercera parte del sistema de Collection Manager, para obtener la información de uso se puede incluir en el sistema de gestión.

El Collection Manager es un sistema simple y de libre mantenimiento, que almacena estadísticas e información de uso. Provee una interfaz simple para reportes y también puede utilizarse para reportes con MRTG a través de interfaces usuales SNMP.

3.2.2 Solución Allot ("NetEnforcer")

De la misma manera que la solución de Cisco, se utiliza un equipo dedicado, denominado "NetEnforcer", que utiliza la tecnología de inspección profunda de paquetes

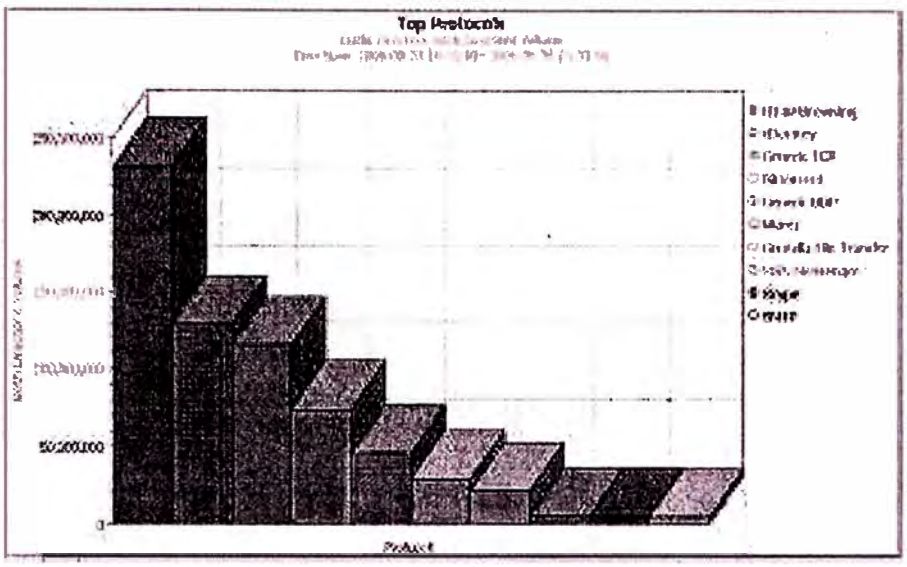


Figura 3.9: Informe de volumen de tráfico top por protocolos - Plataforma SCE

(deep packet inspection - DPI) con capacidad de aplicar QoS, monitorizar y controlar el comportamiento de tráfico del usuario en la red [10]. Los modelos más conocidos son: AC-2500 y AC-1000 (ver especificaciones técnicas de los equipos en el anexo A2) Las principales funcionalidades de éstos equipos son:

- Identificación de centenares de aplicaciones y protocolos, identificadas por firmas ó conductas de tráfico.
- Tecnologías de reconocimiento para control individual de diferentes aplicaciones en la Internet, como: P2P, VoIP, Streaming y Juegos.
- Soporta un sistema de gestión centralizado, para: reporte, análisis, seguridad y control global.
- Control por usuario y aplicación.
- Provisión dinámica por usuario y por servicio.
- Monitoreo contínuo (en línea) del tráfico.
- Detecta tráfico anómalo y mitiga cualquier amenaza de ataque a la red.
- Alta disponibilidad con equipos totalmente redundantes y utilizando equipos externos de bypass.

En la figura 3.10 se presenta la arquitectura de conectividad de la plataforma NetEnforcer, en donde podemos apreciar que los equipos pueden estar distribuidos en la red,

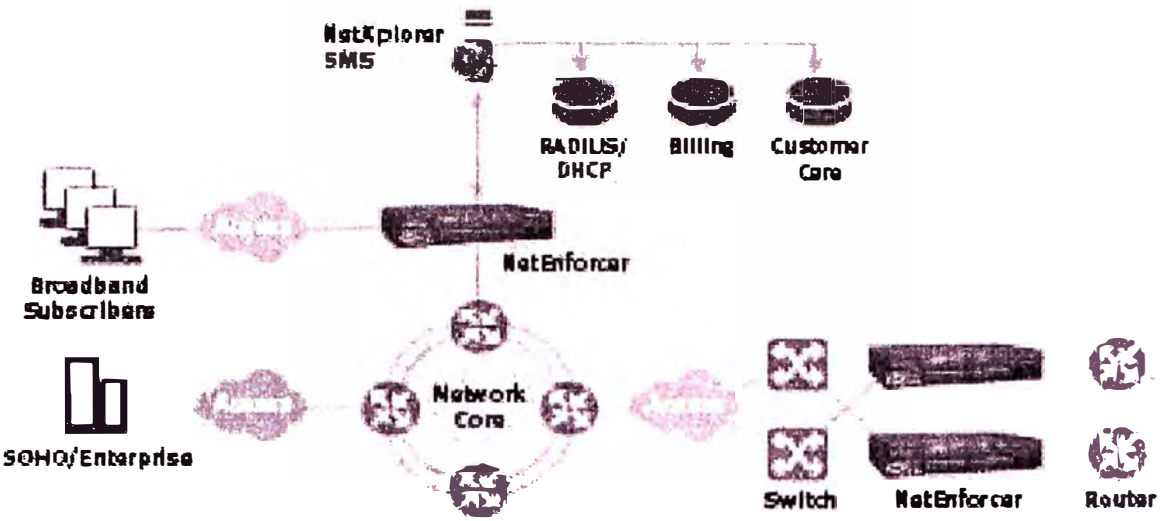


Figura 3.10: Arquitectura de la plataforma NetEnforcer de Allot

en el borde (especialmente para usuarios de banda ancha) ó en la salida Internet, pero; la gestión (Radius/DHCP, Billing, Customer Care [5]) puede estar centralizada.

3.3 Resumen del capítulo

De todas las soluciones tecnológicas estudiadas, se concluye que es posible, principalmente utilizando una plataforma con equipo especializado y dedicado para dicha función, realizar el control del ancho de banda de la conexión Internet de un ISP basado en aplicaciones (servicios) ó protocolos, especialmente el de P2P. No solamente se pueden controlar de manera total ó agregada sino a nivel de usuarios y servicios. Al mismo tiempo que se controla también es posible monitorizar y realizar informes detallados directamente con la plataforma ó realizar un desarrollo acorde a las necesidades del ISP.

Los equipos especializados para control de tráfico IP pueden ubicarse en los nodos de borde ó en la salida a Internet de la red del ISP, ésto dependerá del volumen de tráfico que se tiene. Para los ISP's que ofrecen acceso de banda ancha a Internet y que tienen un alto tráfico (por el orden de lo 10Gbps) se recomienda que los equipos de control de tráfico estén distribuidos en los nodos de borde (B-RAS)[6], tal como se muestra en la figura 3.11. Ésta arquitectura evita concentrar el riesgo, ante fallas, en un solo punto y además optimiza el consumo de ancho de banda de la red de transporte IP del ISP.

[5] Cuidado del cliente: administración/provisión de los usuarios, gestión de la información, etc.
[6] B-RAS: Servidor de acceso remoto de banda ancha

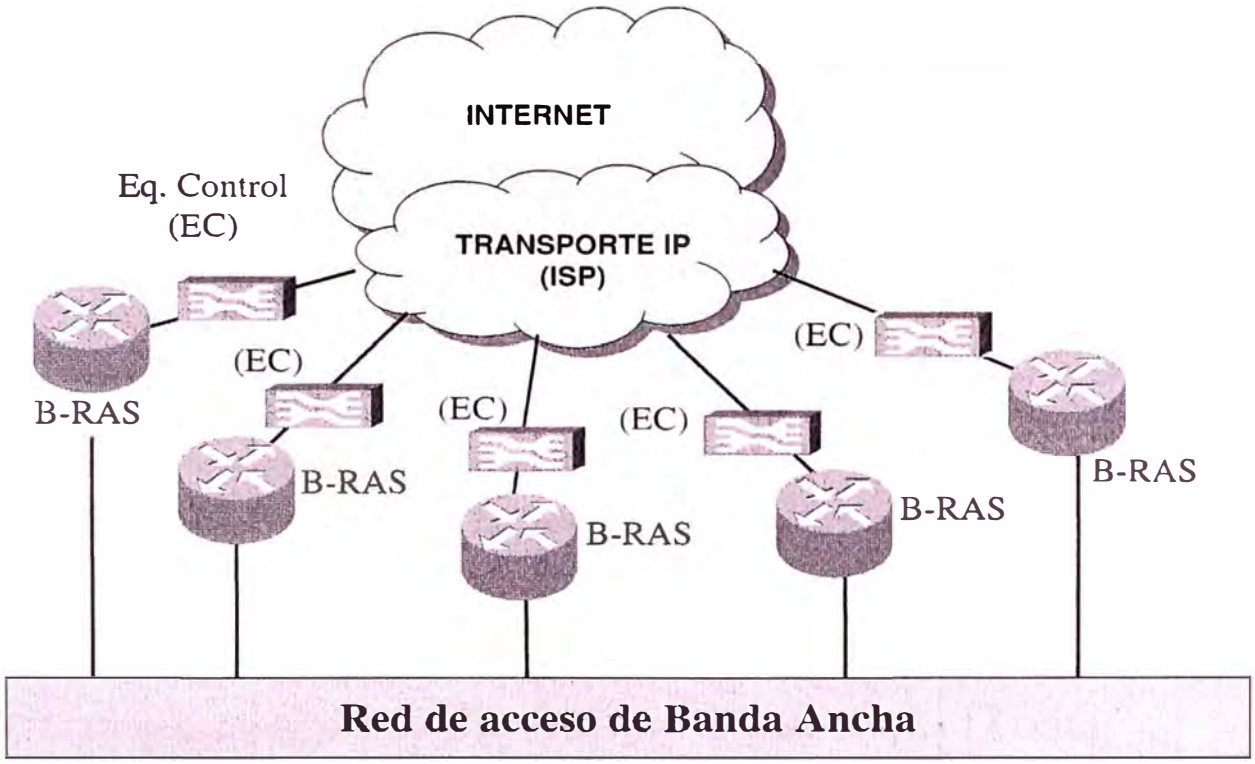


Figura 3.11: Arquitectura distribuida de control de tráfico IP

CAPITULO IV
DIMENSIONAMIENTO Y PROPUESTA DE LA PLATAFORMA DE CONTROL DE TRÁFICO IP

Está claro que es necesario de una plataforma de control de tráfico IP para resolver la problemática de ancho de banda de un ISP y que existe distintas formas ó tecnologías para controlar el tráfico, lo que queda ahora es dimensionar una plataforma de control de tráfico IP para un ISP típico. Éste ISP, que en adelante lo llamaremos ISP-X, se presenta sobre la base de la información disponible al momento de realizar el presente estudio, el cual corresponde a la operadora más representativa del Perú: Telefónica del Perú (TdP)

Se toma en cuenta la demanda de acceso a Internet por banda ancha, la arquitectura de red prevista para el 2007, la capacidad de los equipos y las resctricciones presupuestales del ISP-X para dimensionar y proponer la plataforma de control de tráfico IP. Finalmente se plantea un cronograma tentativo para su implementación.

4.1 Requerimientos de diseño

4.1.1 Demanda de acceso a Internet por Banda Ancha (ADSL)

La proyección de demanda para el 2007 es de medio millón de usuarios de banda ancha para el ISP-X, dado que se trata de un ISP bastante representativo podemos asumir que la demanda es de todo el país, tal como se muestra en la tabla 4.1 El ancho de banda total proyectado para el mismo año (2007) alcanza los 18Gbps.

Tabla 4.1: Proyección de demanda de acceso a Internet por Banda Ancha (ISP-X)

Descripción	2007	2008	2009	2010	2011
Usuarios (Miles)	500	560	610	660	710
BW medio (Kbps)	35	46	57	65	69
BW Total (Gbps)	18	26	35	43	49

Fuente: TdP, Dic-06

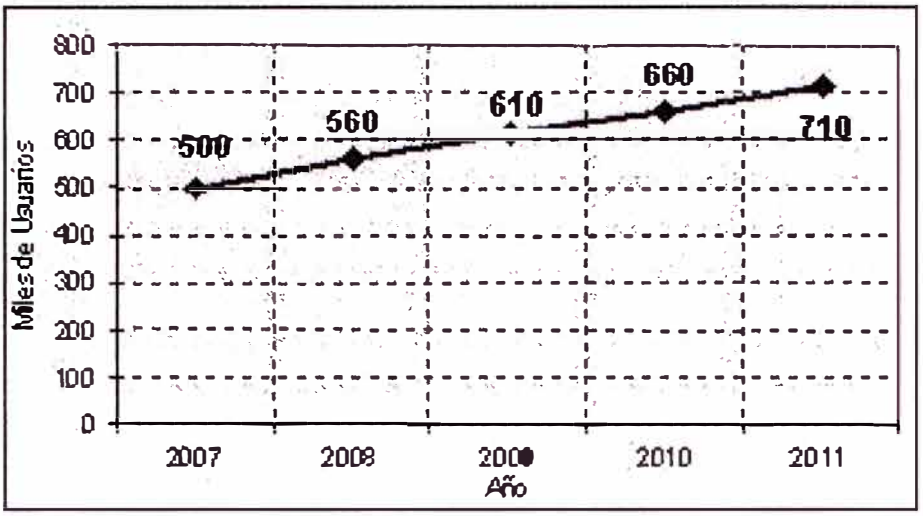


Figura 4.1: Demanda de usuarios de Banda Ancha (ISP-X)

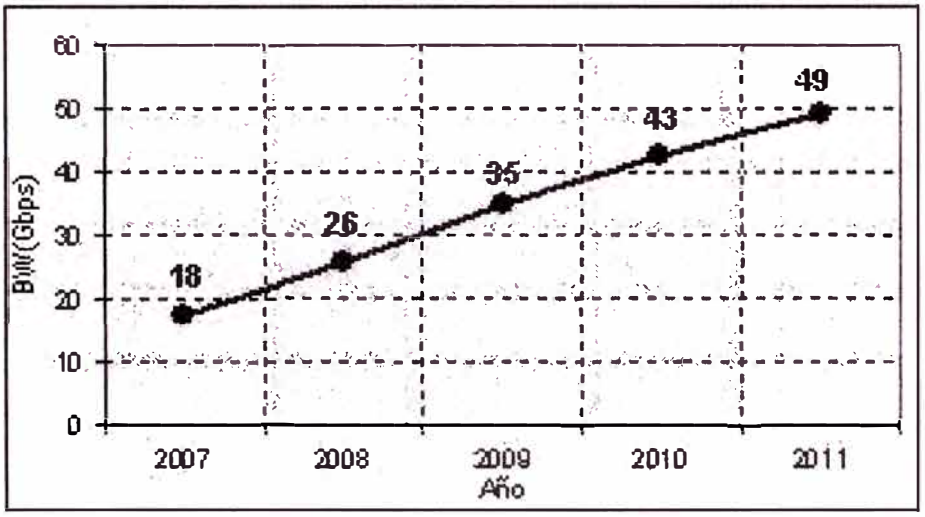


Figura 4.2: Demanda de Ancho de Banda Total (ISP-X)

Entre el 2007 y 20011, el crecimiento del ancho de banda promedio por usuario es creciente, desde 35Kbps hasta 69Kbps. Esto nos indica que crecerá la necesidad por mayor consumo de servicios o aplicaciones de los peruanos en la Internet. Del mismo modo existen más peruanos que contarán con el servicio de banda ancha que crece desde 500 mil usuarios hasta 710 mil usuarios entre el 2007 y 2011. Ver tabla 4.1 y figura 4.1.

El crecimiento de usuarios y el mayor consumo de servicios en Internet hacen que la demanda de ancho de banda también sea creciente, cuyas cifras pasan de 18Gbps hasta 49Gbps entre el 2007-2011. Ver figura 4.2.

El requerimiento del ISP-X es reducir el consumo de ancho de banda total de la conexión a Internet en por lo menos 4 %, controlando solamente de tráfico P2P (aprox.

15 %), es decir; para el año 2007 de 18Gbps debe reducirse a 16.8Gbps. Esta condición debe sostenerse durante los 5 años de operación del ISP (2007 - 2011)

4.1.2 Red de agregación y transporte IP del ISP para el 2007

Para satisfacer la demanda de usuarios y ancho de banda prevista para el 2007, el ISP-X tiene el esquema de red de agregación y transporte IP mostrado en la figura 4.3.

La red de agregación está compuesta por todos los B-RAS que sirven para agregar ó concentrar el tráfico de todos los usuarios de banda ancha y enrutarlos hacia la Internet a través de la red de transporte IP, para el 2007 se tiene 26 B-RAS distribuidos en distintos puntos de presencia en todo el territorio nacional, tales como: San Isidro (2), Washington (3) (Jr. Washington - Cercado), Monterrico (2), Miraflores (2), Higuereta (2), Los Olivos (2), San José (2), Magdalena (1), Trujillo (2), Arequipa (2), Piura (1), Chiclayo (1), Huancayo (1), La Oroya (1), Ica (1) y Tacna (1)

La red de transporte IP es el encargado de transportar el tráfico agregado hacia la Internet y está compuesto de conmutadores de concentración (switch de concentración), el núcleo IP (backbone IP) y los router's de interconexión (toll gates) Los conmutadores de concentración concentran el tráfico de acceso a través del anillo metro-ethernet y enrutan el tráfico agregado de los B-RAS hacia el núcleo IP, el núcleo IP enruta el tráfico hacia los router's de interconexión y finalmente éstos enrutan el tráfico hacia la Internet.

El requerimiento del ISP-X es que la plataforma de control de tráfico IP permita controlar el tráfico de todos los usuarios y del 100 % del tráfico agregado del acceso de banda ancha, es decir; controlar el tráfico que se cursa en todos los B-RAS existentes.

4.1.3 Restricciones presupuestales del ISP

Como en toda empresa, el ISP tiene limitaciones presupuestale y/o requiere tener márgenes aceptables para hacer de su negocio un negocio rentable. En tal sentido es que para el ISP-X se plantea la necesidad de ahorrar los gastos por la conexión a Internet en por lo menos 4 %, proporcional al ahorro de ancho de banda.

Adicionalmente a los gastos por la conexión a Internet, el negocio del ISP será rentable si las inversiones por la compra de equipos de comunicaciones para implementar la red y en particular la compra de la plataforma de control de tráfico IP sea lo mínimo posible, es decir; el ISP-X requiere que el monto de inversión para la compra de la plataforma sea igual ó menor al ahorro de gastos por la conexión a Internet.

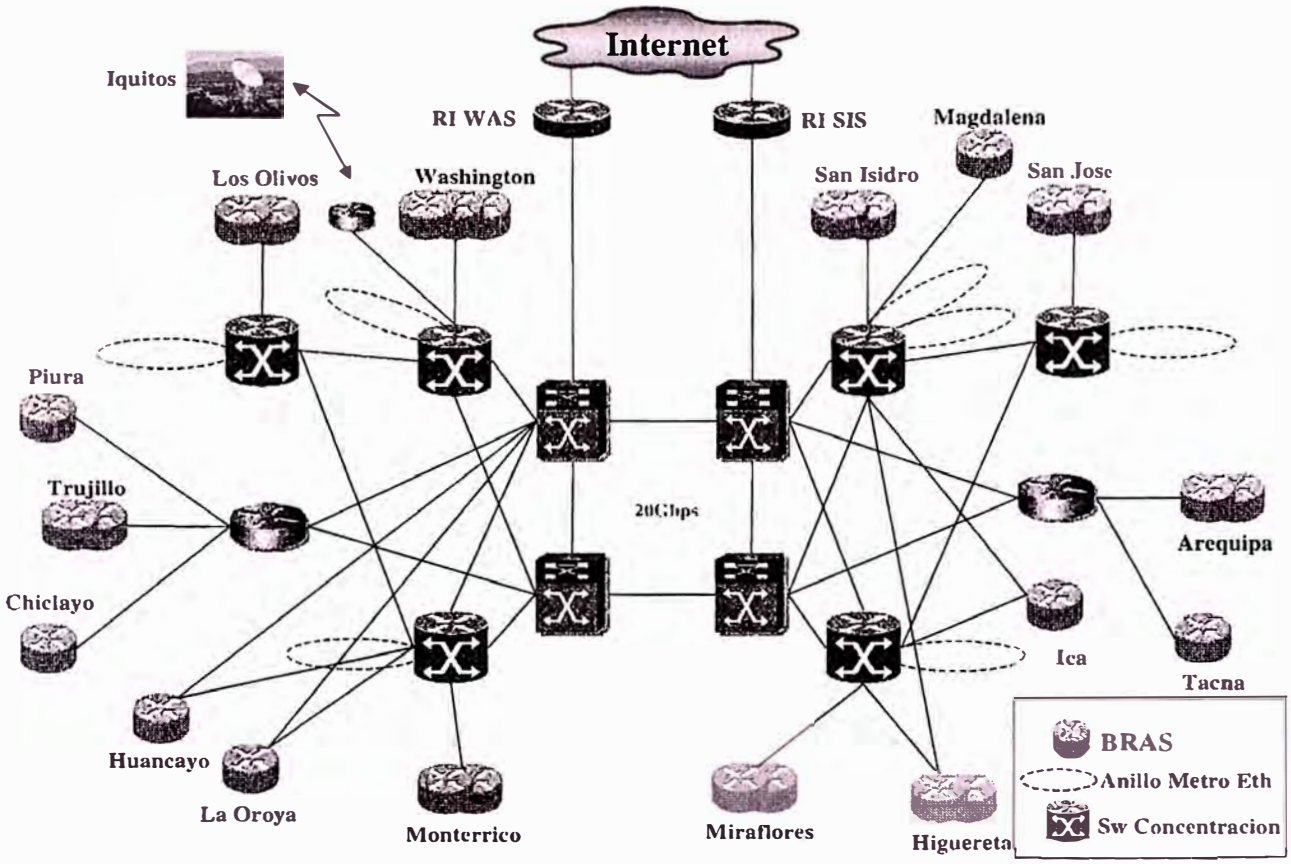


Figura 4.3: Esquema de red del ISP para el 2007

4.1.4 Especificaciones técnicas generales de los equipos

Para seleccionar un equipo se toma en cuenta principalmente las siguientes variables técnicas: cumplimiento de las funcionalidades requeridas, capacidad del equipo y alta disponibilidad. Tomando en cuenta éstas variables, los principales requisitos técnicos para el caso del ISP-X se resumen en lo siguiente:

1. **Requerimientos para el equipo de control de tráfico.**

   a) ***Principales funcionalides requeridas***. Monitoreo, control y reporte de tráfico IP por aplicaciones, a nivel agregado y por cada uno de los usuarios. A continuación se presenta un mayor detalle de éstos requerimientos:

      1) Monitoreo de tráfico IP: Comportamiento de tráfico por perfil de usuario, análisis de tráfico por tipo de aplicación (P2P, VoIP, HTTP, Streaming, etc)
      2) Control de tráfico IP: Control del tráfico por usuario para aplicaciones de capa 7 con ancho de banda determinado, control de tráfico por grupo de usuarios para aplicaciones de capa 7 (P2P, FTP, HTTP, etc) en número de flujos/conversaciones, control de tráfico global por uso de protocolos en capa 7 (P2P, FTP, HTTP, etc) en ancho de banda porcentual y establecemiento de políticas de calidad de servicio (QoS: Quality of Service) durante periodos de congestión.
      3) Reportes del tráfico IP: Reportes de volumen de tráfico P2P, reportes de tráfico por aplicaciones capa 7, por usuario y por grupo de usuarios.

   b) ***Capacidad***: Más de 40 mil usuarios, procesamiento de ancho de banda mínimo de 4Gbps, mayor ó igual a cuatro interfaces GE.

   c) ***Alta disponibilidad***: Procesador redundante y bypass interno.

2. **Requerimientos de hardware para los módulos de software**. Los módulos principales, tales como el Suscriber Manager y el Collection Manager, requieren de servidores, los cuales deben ser capaces de soportar los requerimientos de servicios en función a la demanda del ISP-X. Para 500 mil usuarios con las funcionalidades de control y reporte por cada usuario, se requiere:

   a) 2 Servidores para el Suscriber Manager, con las siguientes características mínimas: dos procesadores Ultra SPARC IIIi 1.6Ghz, memoria RAM de 4 GB y disco duro de 140 GB.

   b) 2 Servidores para Collecction Manager, con las siguientes características mínimas: procesador dual Ultra SPARC IV, memoria RAM de 8 GB, disco duro de 292 GB y capacidad de arreglo de discos externos con SCSI RAID.

Tabla 4.2: Resumen de evaluación del equipo de control SCE-2000 versus NetEnforcer AC-2500

Requerimientos Generales	**SCE-2000**	**Net Enforcer AC-2500**
Monitoreo de tráfico	OK	OK
Contról de tráfico	OK	OK
Reportes de tráfico	OK	OK
Capacidad	80mil/4Gbps	80mil/5Gbps
Alta disponibilidad	Bypass interno	Bypass externo
Costo estimado para: 18 equipos y 500 mil usuarios (Año 2007)	Lic: M$ 700 Eq: M$ 1,080 Total: **M$ 1,780**	Total Licencias y Equipos: **M$ 2,000**

Fuente: TdP, Dic-06

4.2 Propuesta de la plataforma de control de Tráfico IP

4.2.1 Selección de equipos

El proceso de selección de los equipos inicia por un concurso público en la que existen propuestas técnicas y económicas de distintos proveedores de tecnología. Recepcionado las propuestas técnicas y económicas, el proceso de selección continúa por un proceso de evaluación técnica y evaluación económica. Para el ISP-X la evaluación técnica y económica del equipo de control de tráfico IP se resume en la tabla 4.2.

De la tabla 4.2, se concluye que técnicamente los dos proveedores (Cisco y Allot) cumplen con las espectativas del ISP-X, según los requerimientos de diseño, sin embargo; existe una ligera ventaja del equipo SCE-2000 frente al NetEnforcer AC-2500 dado que el primero cuenta con bypass interno y el segundo necesita de uno externo.

Respecto a las propuestas económicas se observa claramente que el costo propuesto para soportar el tráfico de 500 mil usuarios con 18 equipos de control de tráfico, la solución con SCE-2000 es menor que con el equipo NetEnforcer AC-2500.

En resumen, por las ventajas técnicas y económicas, para el ISP-X, se selecciona el equipo SCE-2000 de Cisco. Para que ésta alternativa elegida cumpla con las espectativas económicas del ISP-X es necesario que se analice la viabilidad ecómica, específicamente comprobar que los montos de inversión compensen el ahorro de gastos por la conexión a Internet. Este análisis se realiza en el capítulo V del documento.

Respecto a los servidores se han seleccionado directamente a servidores SUN, dado que los dos proveedores, Cisco y Allot, recomiendan utilizar éstos equipos. Los servidores seleccionados son: Sun Fire 440 para el Suscriber Manager y Sun Fire 490 para Collection Manager. Para mayor información sobre las características técnicas de los servidores SUN dirigirse al Anexo A3.

4.2.2 Propuesta de red con plataforma de control de tráfico IP para el ISP - 2007

En la figura 4.4 se muestra el nuevo esquema de red propuesto para el ISP-X, que corresponde a la red de agregación y transporte IP, presentado en la figura 4.3, incluyendo la plataforma de control de tráfico IP.

La plataforma de control de tráfico IP está compuesto por:

- 18 equipos, SCE-2000, de control de tráfico IP distribuidos en todos los nodos de agregación (lugar donde existe por lo menos un equipo B-RAS)
- Los módulos de software de Suscriber Manager y Collection Manager centralizados en un solo lugar de la red (nodo de washington)

La conectividad de los equipos SCE-2000 se realiza con interfaces Giga Ethernet (GE) ópticos, dos ó cuatro por equipo (2GE de entrada y 2GE de salida), y se ubican en línea a los enlaces de conexión del B-RAS al backbone IP (conexión en línea) Esta conectividad permite que todo el tráfico agregado por el B-RAS atraviese el equipo de control de tráfico SCE-2000, de ésta forma se garantiza que el tráfico de todos los usuarios y de toda la red sean controlados por la plataforma de control de tráfico IP.

Para gestionar de manera centralizada el monitoreo y control de tráfico IP de toda la red del ISP, los servidores: Suscriber Manager y Collection Manager, alcanzan conectividad IP con todos los equipos SCE-2000 a través de la la propia red de agregación y transporte IP del ISP-X, tal como se muestra en la figura 4.5. Para dicha conectividad también es necesario de dos equipos de comunicaciones: un switch y un router, que

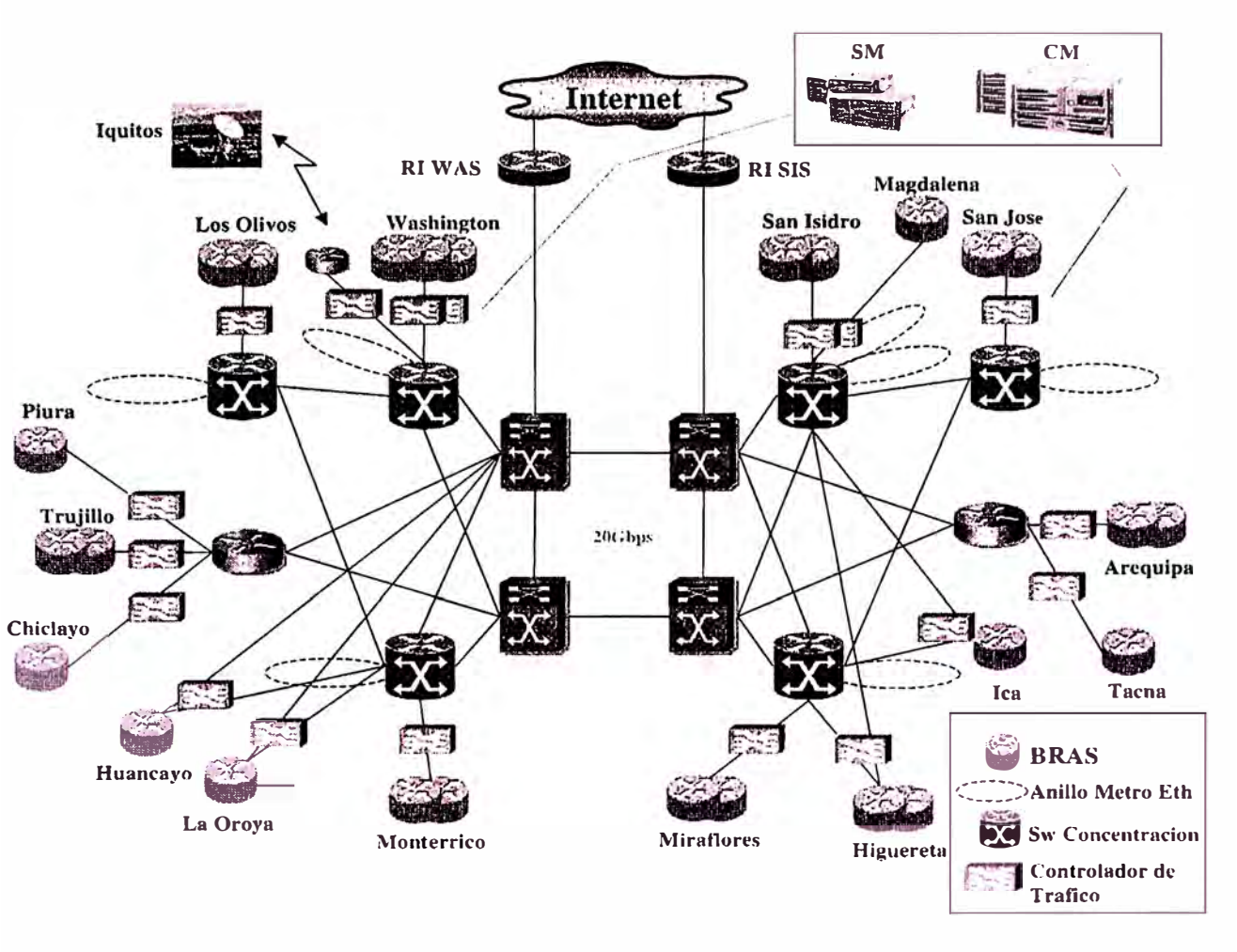


Figura 4.4: Nuevo esquema de red del ISP para el 2007

en éste caso se han elegido al switch cisco 3750 y el router cisco 7204VXR, como se muestra en la misma figura 4.5.

En resumen la propuesta de plataforma de control de tráfico IP, compuesta por equipos SCE-2000, servidores suscriber y collection manager, permiten controlar el tráfico de todos los usuarios del ISP-X distribuidos geográficamente en todo el territorio nacional.

4.2.3 Inversión estimada 2007 - 2011

Sobre la base de la propuesta de la plataforma de control de tráfico IP para el 2007, se estima la inversión necesaria para la adquisición e implementación de dicha plataforma. El detalle de ésta inversión se muestra en la tabla 4.3.

Dado que el ISP requiere sostener la misma política de control de tráfico IP durante 5 años, desde el 2007 hasta el 2011, es necesario incrementar la capacidad de la plataforma en los próximos años. El incremento de capacidad se estima en función al crecimiento de la demanda de usuarios y ancho de banda, tal como se muestra en la

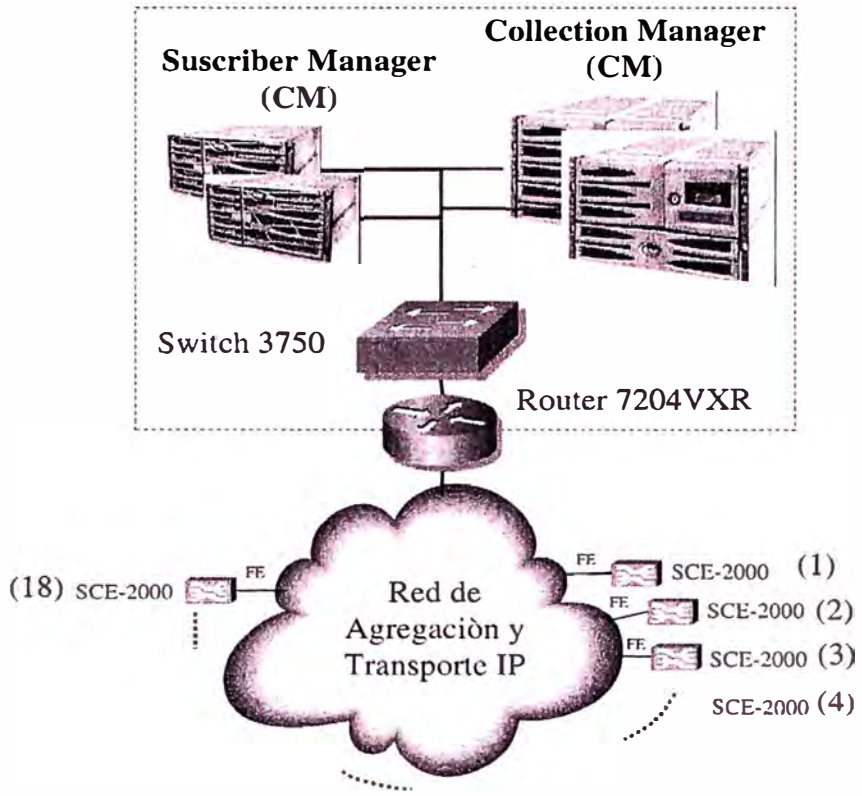


Figura 4.5: Conectividad IP del Suscriber y Collection Manager con los equipos SCE-2000

Tabla 4.3: Inversión 2007, Plataforma de Control de Tráfico IP

Descripción	Cantidad	Precio Unitario (US$)	Monto Total (US$)
Equipos SCE-2000	18	60,000	1'080,000
Licencias por usuarios	500,000	1.4	700,000
Servidores Sun Fire V440	2	30,000	60,000
Servidores Sun Fire V490	2	50,000	100,000
Switch 3750	1	10,000	10,000
Router 7204VXR	1	60,000	60,000
Servicios de Instalación			100,000
Soporte (1 año)			100,000
TOTAL			**2'210,000**

Tabla 4.4: Inversión 2008-2011, Plataforma de Control de Tráfico IP

Año	Usuarios (Miles)	Ancho de Banda Total (Gbps)	Incremento de Ancho de Banda (Gbps)	Incremento de Equipos SCE-2000	Monto de Inversión Incremental (US$)
2007	500	18	0	0	0
2008	560	26	8	4	324,000
2009	610	35	9	5	370,000
2010	660	43	8	4	310,000
2011	710	49	6	3	250,000

tabla 4.4.

Para el 2008, el incremento de usuarios, respecto al 2007, es de 60,000 y el incremento de ancho de banda es de 8Gbps. El incremento de usuarios requiere de 60,000 licencias adicionales de monitoreo y control de tráfico en la plataforma, y el incremento de ancho de banda hace necesario el incremento de 4 equipos SCE-2000 (considerando 2Gbps por equipo) Sobre la base del incremento de equipos y licencias, el monto de inversión resulta de 324,000 dólares. Respecto a los servidores, se estima que los cuatro servidores previstos para el 2007 se abastecen para la demanda adicional.

Para los años: 2009, 2010 y 2011; el criterio de la estimación de la inversión es la misma al utilizado para el año 2008, donde los montos de inversión resultan a: 370, 310 y 250 mil dólares americanos respectivamente.

4.2.4 Cronograma de implementación de la plataforma de control de tráfico IP

Asumiendo que el proyecto es viable, económica y legalmente, para el ISP-X; la implementación del proyecto en el 2007, incluyendo la actividad de gestión de compra, fabricación y transporte del equipamiento, tiene una duración total de cuatro meses (Enero - Mayo) Ver tabla 4.5.

Las actividades, de manera resumida por grupos de actividades, se describen a continuación:

- **Gestión de compra.** Son las primeras actividades del proyecto y que no tienen precedencia, cuya duración total se estima en 2 semanas.
- **Suministro.** Estas actividades tienen como precedente a las actividades de gestión de compra y se estima una duración total de 6 semanas.

- **Ingeniería de detalle**. Estas actividades no tienen ningún precedente y se pueden realizar en paralelo con la actividades de suministro. Se estima una duración total de 6 semanas.

- **Instalación y configuración de los equipos SCE-2000 en Lima**. Estas actividades requieren que las actividades de suministro e ingeniería de detalle estén culminados. Se estima una duración de 6 semanas.

- **Instalación y configuración de los equipos SCE-2000 en provincias**. Estas actividades, similar al anterior, requieren que las actividades de suministro e ingeniería de detalle estén culiminados, sin embargo; por limitaciones de recursos humanos se plantea realizar posterior a las actividades de instalación y configuración de los equipos SCE-2000 en Lima. Se estima también, una duración de 6 semanas.

- **Instalación y configuración de los servidores suscriber y collection manager**. Estas actividades se realizan en paralelo a las actividades de instalación y configuración de equipos SCE-2000, es decir; se inician desde cuando se realiza la primera instalación y configuración de equipo de control de tráfico SCE-2000 (nodo de Washington) y dado que existen actividades relacionadas de configuración y conectividad con todos los equipos SCE-2000 previstos para instalar, culminarán cuando se termine la instalación del último equipo de control de tráfico SCE-2000 (nodo de Tacna) En consecuencia, para éstas actividades se estima una duración total de 11 semanas.

- **Actividades complementarias**. Estas actividades corresponden a algunas actividades de capacitación y análisis relacionadas con la operación y/o explotación de la plataforma de control de tráfico. No tienen precedencia pero deben iniciarse antes de que culminen las instalaciones y configuraciones de los equipos de control de tráfico SCE-2000. Se estima una duración total de 4 semanas.

Tal como se ha descrito, existen algunas actividades en paralelo y otras que no teniendo precedencia se realizan en serie por limitaciones de recursos.

Finalmente para completar el planteamiento, la ampliación de equipos previstos para los próximos años: 2008, 2009, 2010 y 2011, se estima realizar en el primer trimestre (Enero-Marzo) de cada año respectivamente.

Tabla 4.5: Cronograma de implementación 2007

ACTIVIDADES	Ene				Feb				Mar				Abr				May			
	1s	2s	3s	4s	1s	2s	3s	4s	1s	2s	3s	4s	1s	2s	3s	4s	1s	2s	3s	4s
Gestión de Compra																				
Elaboración de pedidos																				
Emisión de Ordenes de Compra																				
Suministro																				
Fabricación																				
Transporte																				
Recepción de equipos																				
Ingeniería de Detalle																				
Estudio de campo para los equipos a instalar																				
Estudio de campo para los equipos a instalar																				
Implementación de Energía, Ambiente, etc.																				
Instalación y configuración de los equipos SCE - Lima																				
Nodo de washington																				
Nodo de San Isidro																				
Nodo de Monterico																				
Nodo de Miraflores																				
Nodo de Higuereta																				
Nodo de Los Olivos																				
Nodo de San José																				
Nodo de Magdalena																				
Instalación y configuración de los equipos SCE - Provincia																				
Nodo de Trujillo																				
Nodo de Chiclayo																				
Nodo de Piura																				
Nodo de Arequipa																				
Nodo de Ica																				
Nodo de Tacna																				
Instalación y configuración de servidores																				
Suscriber Manager y Collection Manager																				
Conectividad																				
Actividades complementarias																				
Estudios para manejar BBDD del Collection																				
Ingenieria para Etapas Posteriores																				

CAPITULO V
VIABILIDAD DE LA PROPUESTA

La propuesta de plataforma de control de tráfico IP para el ISP, estudiado en el capítulo anterior, permitirá monitorizar y controlar el total del tráfico generado en la red del ISP. Es decir, la solución técnica plateada satisface los requerimientos planteados por el ISP. Para completar el análisis de factibilidad ó viabilidad, se analiza el aspecto económico, comercial y legal de la propuesta.

5.1 Viabilidad económica

En ésta sección se busca averigüar si el ahorro de gastos por la conexión a Internet compensa las inversiones que se necesitan realizar, para lo cual se presenta un escenario de ahorro de gastos, de las inversiones y del flujo económico, ajustada a los requerimientos del ISP.

5.1.1 Ahorro de gastos

Tomando en cuenta los requerimientos del ISP, la plataforma de control de tráfico se configura para controlar el 15 % de tráfico P2P que en total representa un ahorro de 4 % del tráfico total. En la tabla 5.1, se muestra que el ahorro de ancho de banda se incrementa de 0.7Gbps en el año 2007 hasta 2Gbps en el año 2011. Este encremento de ahorro de ancho de banda durante los 5 años es proporcional al crecimiento de la demanda de ancho de banda, dado que la política de control se aplica porcentualmente (15 %) al ancho de banda del consumo de P2P y se asume que el consumo de P2P se mantiene constante durante éste período de tiempo (ver figura 5.1) Este supuesto es bastante conservador, dado que como se ha visto en el presente trabajo, el consumo de P2P tiende a crecer.

El gasto por la conexión a Internet para el 2007 debe ascender a 95.1 millones de soles, pero como existe un ahorro de 0.7Gbps resulta que el gasto se reduce a 91.4 millones de soles, lo que implica un ahorro de 3.7 millones debido a la aplicación de políticas de control de tráfico IP. El ahorro de gastos crece proporcional al ahorro de

Tabla 5.1: Ahorro de Ancho de Banda (2007-2011)

Descripción	2007	2008	2009	2010	2011
Total BW sin control de tráfico (Gbps)	18.0	26.0	35.0	43.0	49.0
Total BW con control de tráfico (Gbps)	17.3	25.0	33.6	41.3	47.0
Ahorro de BW (Gbps)	**0.7**	**1.0**	**1.4**	**1.7**	**2.0**

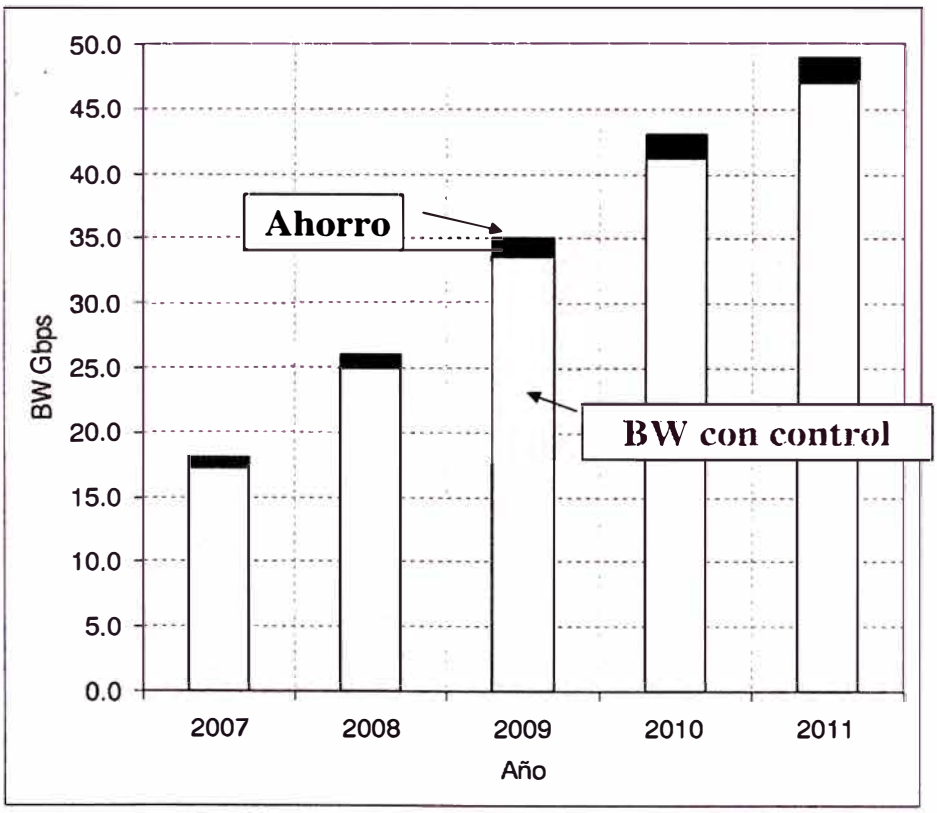


Figura 5.1: Evolución del ancho de banda con control de tráfico IP

Tabla 5.2: Ahorro de Gastos (2007-2011)

Descripción	2007	2008	2009	2010	2011
Gasto Total sin control de tráfico (MMS/.)	95.1	121.3	149.7	163.3	173.1
Gasto Total con control de tráfico (MMS/.)	91.4	116.6	143.7	156.8	166.0
Ahorro de Gastos (MMS/.)	**3.7**	**4.7**	**6.0**	**6.5**	**7.1**

Tabla 5.3: Flujo Económico (2007-2011)

Descripción	2007	2008	2009	2010	2011
Ahorro de Gastos (MMS/.)	3.7	4.7	6.0	6.5	7.1
Inversiones (MMS/.)	-2.21	-0.324	-0.370	-0.310	-0.250
Flujo Neto (MMS/.)	**1.49**	**4.34**	**5.62**	**6.15**	**6.82**

ancho de banda, pasando de 3.7 millones de soles en el 2007 hasta 7.1 millones de soles en el 2011. Mayor información ver en la tabla 5.2.

5.1.2 Flujo económico

En la tabla 5.3, se muestra el flujo económico en el período 2007 y 2011. En el cual se presenta el ahorro de gastos que se ha descrito anteriormente y el flujo de inversiones que también se ha determinado en el capítulo IV. Considerando que el ahorro de gastos es un flujo positivo y las inversiones un flujo negativo, se obtiene el flujo neto que es positivo en todos los años del período de evaluación (2007-2011)

El resultado del flujo neto genera un impácto económico positivo, por lo que se concluye que realizar las inversiones estimadas e implementar la plataforma de control de tráfico IP es rentable para el ISP. En la figura 5.2 se visualiza gráficamente éste resultado.

5.2 Viabilidad comercial y legal

5.2.1 Viabilidad comercial

El objetivo del ISP es satisfacer la necesidad de consumo de Internet de todos los usuarios, sin embargo; el abuso en el consumo de ancho de banda de algunos usuarios (heavy user's) perjudican la calidad de servicio de la gran mayoría de usuarios (usuarios comunes) Evitar éstos abusos, permite distribuir de manera más justa el consumo de ancho de banda del ISP y por lo tanto se consigue mayor porcentaje de satisfacción de clientes ó usuarios de banda ancha. Adicionalmente, la plataforma de control de tráfico

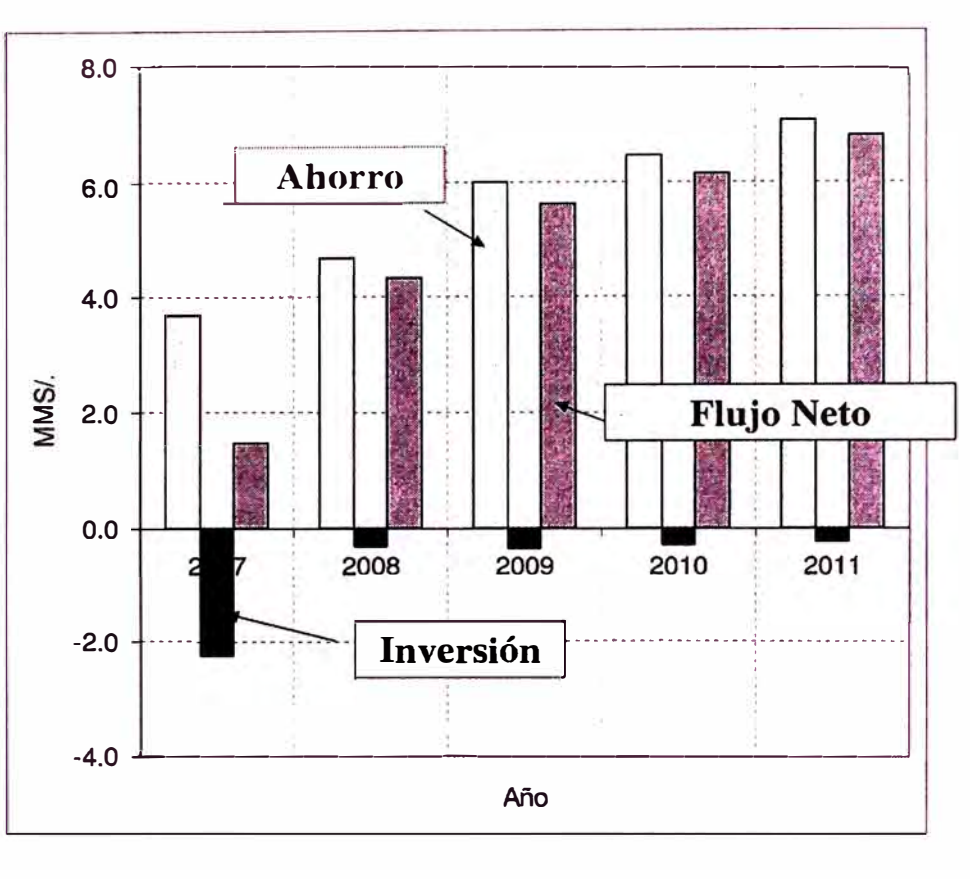


Figura 5.2: Evolución del flujo económico

IP:

- Se convierte en una herramienta de márketing potente para el negocio y abre mayores posibilidades para diseñar nuevos productos para grupos de clientes en función a su patrón de uso (por aplicaciones, por volumen, por tiempo, etc.)
- Por otro lado también se convierte en una heramienta de gestión importante para la operación de la red del ISP, puesto que permite monitorear continuamente la seguridad en la red y la protección contra tráficos anómalos y nuevas amenazas.

En resumen, la propuesta de implementar la plataforma de control de tráfico IP, genera mejoras en la calidad de servicio de la mayoría de usuarios y habre mayores posibilidades de negocio para el ISP.

5.2.2 Viabilidad legal

El servicio de acceso a Internet, está definido como servicio público de valor añadido, y está regido por las condiciones de uso según resolución del Consejo Directivo N° 015-2001-CD/OSIPTEL[1] de OSIPTEL publicado en el año 2001.

[1]Resolución N° 015-2001-CD/OSIPTEL fue publicada en El Peruano el: 30 de Abril de 2001 en la que se aprueban las Condiciones de Uso y Cláusulas Generales de Contratación de los Servicios

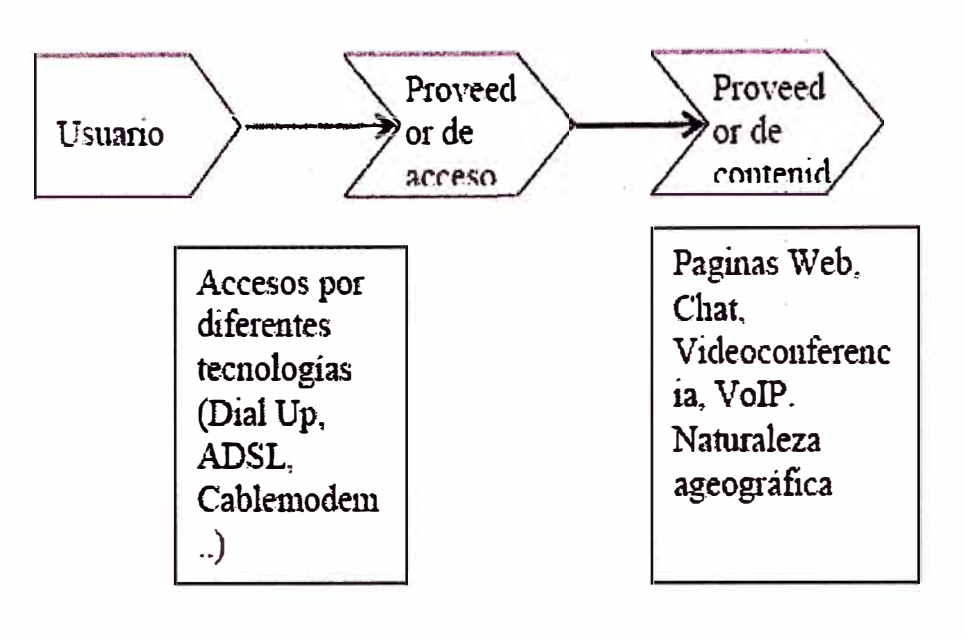


Figura 5.3: Cadena de valor de Internet

Dentro de las condiciones de uso, se establece que el proveedor de acceso a Internet debe garantizar que todas las aplicaciones utilizadas en Internet no estén restringidas para ningún usuario. Esto significa que el ISP no puede bloquear el tráfico P2P al 100 %, pero sí es posible regular el ancho de banda, dado que la velocidad no se garantiza en el servicio de acceso a Internet y debe estar claramente especificado como condición comercial dentro del contrato.

Respecto a la calidad de servicio se establece: que Internet, estructuralmente es una red conformada por redes de diferentes proveedores locales e internacionales, que intercambian tráfico mediante acuerdos privados, en la que se maneja el concepto de "MEJOR ESFUERZO", es decir que se hace todo lo posible para que el tráfico cursado llegue a su destino.

En la cadena de valor del Internet se puede observar que lo que el usuario valora en el Internet es el acceder a contenido (servicios como el correo electrónico, World Wide Web, el vídeo, el sonido, la telefonía IP), y naturalmente este contenido se encuentra disperso en cualquier parte del mundo. Ver figura 5.3.

En resumen, las normas legales en el Perú permiten que se pueda establecer algunas políticas de control de tráfico y el desarrollo de nuevos servicios con condiciones comerciales de control de tráfico establecidas claramente en el contrato del servicio. Es decir, la propuesta de la plataforma de control de tráfico IP es legalmente viable en el Perú.

Públicos de Difusión y de Servicios de Valor Añadido para Acceso a Internet

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

1. El uso de las redes o protocolos P2P está cada vez más extendida en la Internet. Como consecuencia de éste fenómeno los ISP's enfrentan un gran dilema: incremento de costos por el crecimiento de ancho de banda en el enlace a Internet e incremento de la demanda de usuarios de banda ancha.

2. La solución de control de tráfico IP, utilizando equipos dedicados para ésta función, permite evitar el abuso del consumo de ancho de banda por algunos usuarios intensivos (heavy user's), en consecuencia incrementan la satisfacción de los clientes del ISP.

3. La propuesta de plataforma de control de tráfico IP es económica, comercial y legalmente viable para el ISP. Es decir, las inversiones se rentabilizan con los ahorros de gastos del enlace a Internet, y se pueden desarrollar propuestas comerciales atractivas para el mercado peruano respetando las normas legales que regulan el servicio de acceso a Internet.

4. Existen otras alternativas de solución para resolver la problemática de ancho de banda del ISP, como la plataforma de caché's P2P, que en el presente trabajo no se han estudiado.

Recomendaciones:

1. Se recomienda utilizar la metodología utilizada en el presente trabajo para proponer soluciones de plataforma de control de tráfico IP para cualquier ISP.

2. Para no frenar el crecimiento del consumo de mayor ancho de banda en la Internet es necesario complementar la solución de control de tráfico con plataformas de caché's P2P.

3. Se recomienda a los grandes ISP's que la red de acceso asimétrico debe evolucionar a una red de acceso simétrico. Para lo cual deben iniciar con las investigaciones y planes de largo plazo correspondientes.

ANEXO A

HOJA DE DATOS DE LOS EQUIPOS

Se presentan a continuación las hojas técnicas de los equipos analizados y/o utilizados para el diseño y propuesta de la plataforma de control de tráfico IP. Estas hojas técnicas son proveídos por los fabricantes de los equipos.

A1. EQUIPO DE CONTROL DE TRAFICO IP DEL FABRICANTE CISCO - Service Control Engine (SCE 2000)

A1.1. CARACTERÍSTICAS DEL EQUIPO

Tabla A1.1 : Especificaciones de Hardware:

SCE 2000
System • Interfaces: 4xGBE 1000Base SX850nm, LX1310nm (SC) • Management: 10/100 Mbps Ethernet RJ-45 • Console: 2 x RS232 RJ-45
Regulatory • EMC: FCC part 15, FCC Class B, Full CE mark, EN500 82-1 • Safety: UL 60950, ULC 60950, IEC 60950 • Telecom: NEBS Level 3 design, ETS 300-019
Physical • Weight: 33.1lb (15Kg) • Dimensions: 3.54H x 17.3W x 18D (inches) • Mounting: Standard 19" Rack • Temperature: 23ºF to 131ºF (-5ºC to +55ºC) • Humidity: 5% to 95% (non-condensing) • Power: 100-120 or 200-240 VAC 47-63 Hz 200W -36 to -72 VDC 200W AC/DC dual PSU with dual line feeds • Cooling/Airflow: Redundant cooling fans
Additional • Management: CLI, SNMP (MIB-II & proprietary), GUI, Packet-Filter ACL on management port • Reliability: Hardware bypass (automatic and manual) to maintain link connectivity

Tabla A1.2 : Soporte y Protocolos de Clasificación:

Category	Protocols	Comments
General	• **Any protocol based on TCP port number** • **Any protocol based on UDP port number** • **Any protocol based on IP protocol number**	***Track traffic by TCP/UDP/IP connection*** ***Predefined list of 600+ protocols Including Instant-Messaging & Gaming protocols***
Browsing	• HTTP (Hyper Text Transfer Protocol)	*Identify application-layer messages exchange. Further classification using HTTP host-name & User-Agent* *Application-layer HTTP redirect*
FTP	• FTP (File Transfer Protocol)	*Identify application-layer message exchange* *Dynamic flow binding to classify downloads on random ports*
News & Mail	• NNTP (Network News Transfer Protocol) • SMTP (Simple Mail Transfer Protocol) • POP3 (Post-Office Protocol v3)	*Identify application-layer message exchange and extract semantic attributes*
Streaming	• HTTP Streaming • RTSP (Real Time Streaming Protocol) • MMS	*Dynamic flow binding to classify streaming media flows* *Identify application-layer message exchange and extract semantic attributes* *Application-layer HTTP/RTSP redirect*

Category	Protocols	Comments
P2P	• FastTrack/KaZaA (*KazaA, iMesh, Grokster*) • Gnutella (*LimeWire, BearShare, Morpheus*) • WinMX/OpenNAP/EzPeer • Winny • eDonkey (eMule) • DirectConnect • Manolito • Hotline • Bittorrent • Kuro *[DSS]* * Note: Many of the above protocols are supported by multiple client-applications. Names in parenthesis represents a sample list of such applications	*Identify P2P traffic on any port numbers using per-application signature* *Dynamic P2P support for additional signature based protocols*
Messaging	• SIP (Session Initiation Protocol) • Skype	*Dynamic flow binding to classify streaming media flows* *Identify Skype traffic on any port number using application signature*

[DSS] – signifies support is provided through the dynamic signature mechanism

Tabla A1.3 : Capacidad del modelo SCE2000 versus el SCE1000

	SCE2000	SCE1000
Max. Number of Subscriber Contexts	80,000	40,000
Max. Number of flows	o 2,000,000 (1,000,000 bi-directional) – global control o 1,400,000 (700,000 bi-directional) – subscriber-mode	o 900,000 (450,000 bi-directional) – global o 700,000 (350,000 bi-directional) – subscriber-mode

Tabla A1.4 : Límite de configuración de servicios y tamaño de estrutura de políticas, SCE 2000 versus SCE 1000

	SCE2000	SCE100
Max. Number of Services per Policy	31	31
Max. Number of Packages	64	64
Number of List Entries	10,000	10,000
Number of Subscriber BW Controllers	32	32
Number of Global Controllers	32 (16 per direction)	32 (16 per direction)

Tabla A1.5 : Rendimiento (performance), SCE 2000 versus SCE 1000

SCE 2000

Throughput & Delay	64Byte	512Byte	1518Byte
Line throughput (out of 4gbps)	69% (2.76GBPS)	93.5% (3.74GBPS)	93.5%(3.74GBPS)
Frame loss (percentage from 4gbps ingress)	29%	5%	5%
Delay	13.6 Micro	23.4 Micro	37.1 Micro
Connection Establish Rate	**ICMP**	**UDP**	**TCP**
Connection Established per second	43,478	45,704	35,411

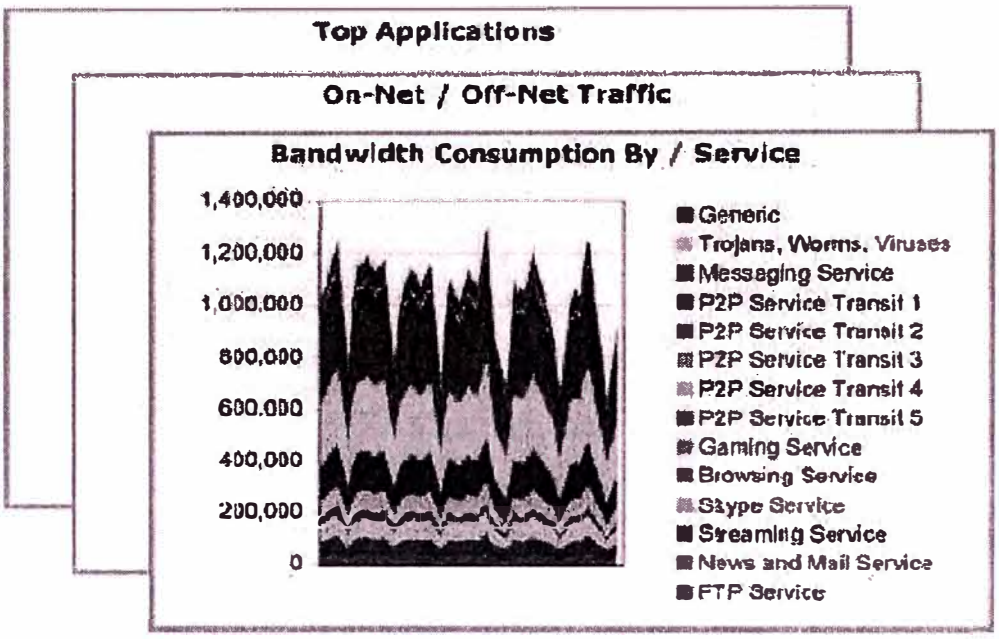
SCE 1000

	64Byte	512Byte	1518Byte
Line throughput (out of 2gbps)	91% (1.82GBPS)	100% (2GBPS)	100% (2GBPS)
Frame loss (percentage from 2gbps ingress)	18.3%	0%	0%
Delay	12.2 Micro	22.9 Micro	44.3 Micro

A1.2. EJEMPLOS TÍPICOS DE REPORTES

A1.2.1. Reportes de Monitoreo

Figura A1.1 : Informes de ancho de banda y de volumen



A1.2.2 Reportes para análisis (descubrimiento)

Figura A1.2 : Informe de datos demográficos de usuarios

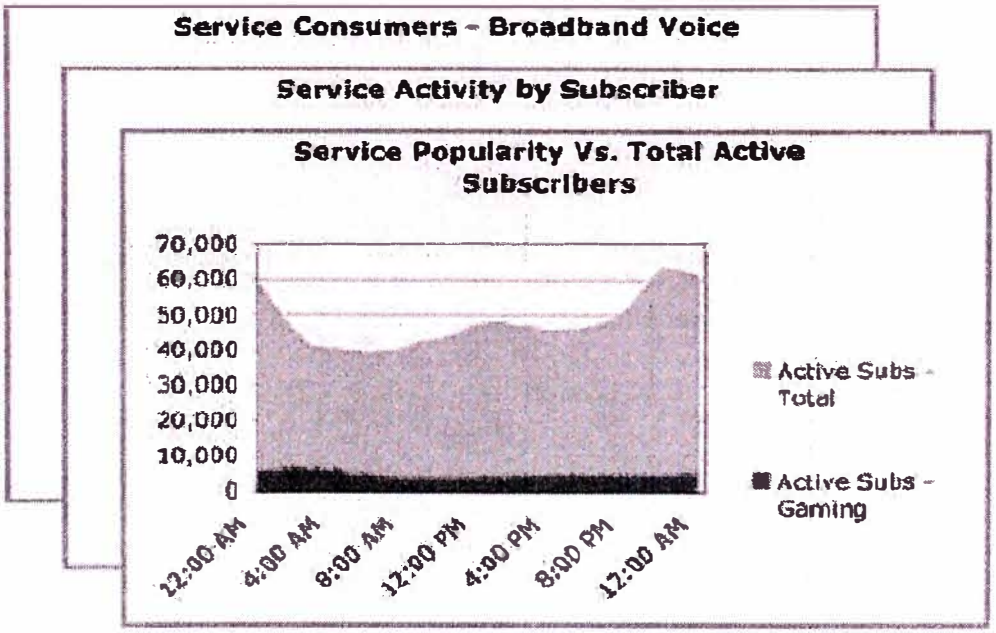


Figura A1.3 : Informe de tráfico P2P

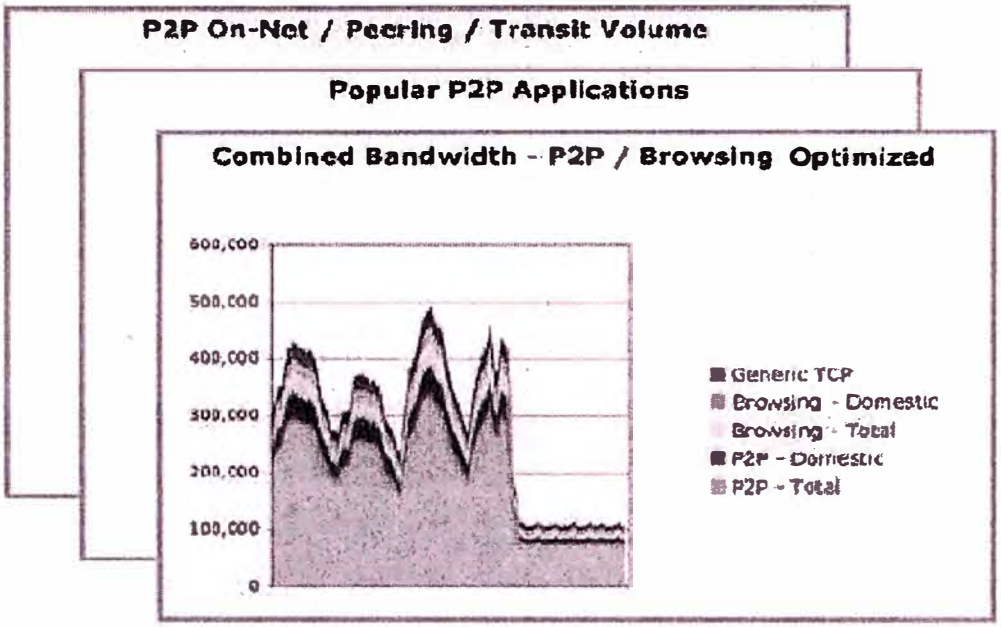


Figura A1.4 : Informe de tráfico malicioso

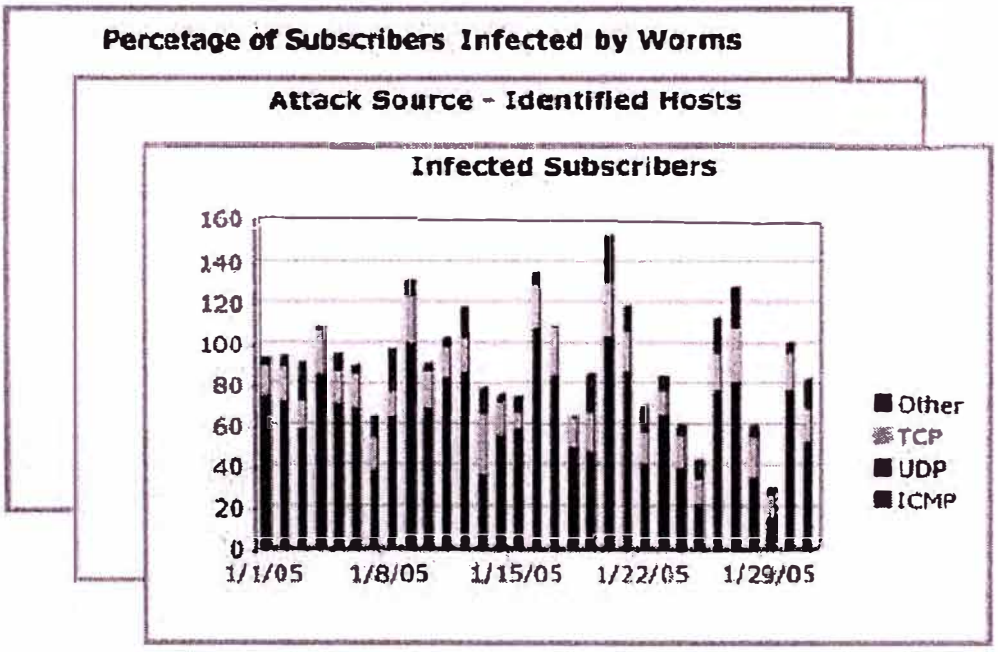
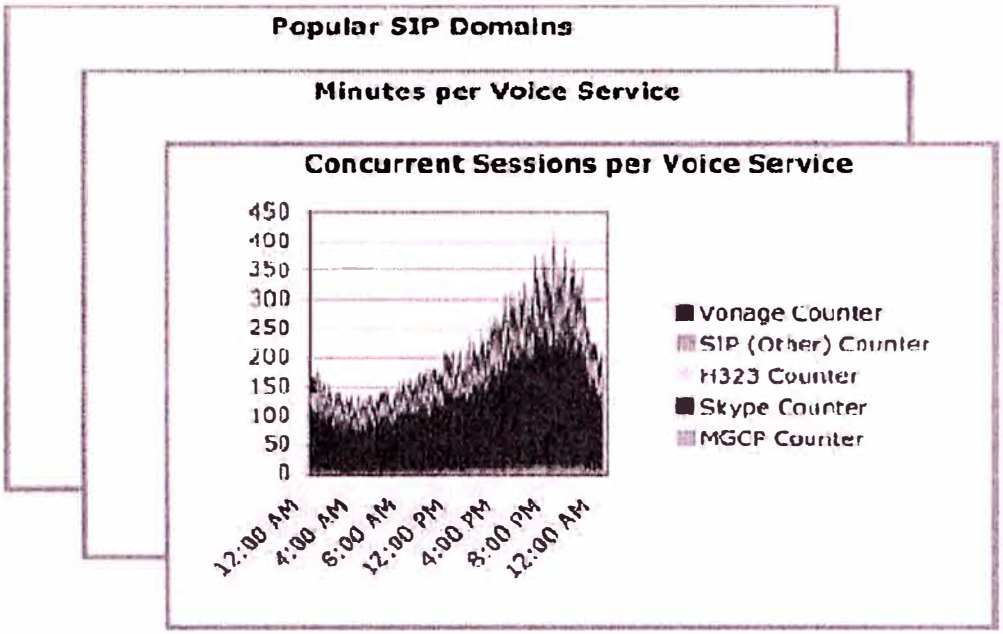


Figura A1.5 : Informe de tráfico VoIP



A2. EQUIPO DE CONTROL DE TRAFICO IP DEL FABRICANTE ALLOT-NetEnforcer (AC-2500/AC-1000)

A2.1. CARACTERÍSTICAS DEL EQUIPO

Tabla A2.1 : Especificaciones Técnicas de NetEnforcer AC-25000

	AC-2520	AC-2540
Capacity		
Number of Connections/Flows	2,000,000 / 4,000,000	
Throughput	5 Gbps (2.5 Gbps; Full Duplex)	
Pipes/Virtual Channels	40,000 / 80,000	40,000 / 80,000
No. of Subscribers	160,000	
Interfaces and Connections		
Management Interface	10/100 BaseT	
Network Interfaces (Internal / External)	4x1000 BaseT or 4x1 000BaseSX or 4x1000 BaseLX	8x1000 BaseT or 8x1000 BaseSX or 8x1000 BaseLX
Console Port	Serial, RJ-45 Connector	
Deep Packet Inspection (DPI) (Typical Examples)		
P2P Protocols	Including BitTorrent, eDonkey, Warez, WinMX, Kazaa	
VoIP Protocols	Including Skype, H.323, SIP, RTP, Net2Phone, Vonage	
Gaming Protocols	Including Doom, Diablo, MSN Game, SWAT, Ultima	
Web/Streaming Application Protocols	Including Abacast, iTunes, RTSP, Winamp MMS	
Traffic Encapsulation Protocols	Including L2TP, MPLS, PPPoE	
Traffic Shaping		
Monitoring	Yes	Yes
QoS Enforcement Levels	1 and 2 Gbps (Full Duplex)	310 Mbps and 1/2.5 Gbps (Full Duplex)
Policy Levels (Pipes/VCs)	4,000 / 8,000; 20,000 / 40,000; 40,000 / 80,000	
Redundancy	Serial, parallel and active (1:1, 1+1)	
Add-Ons: NetXplorer Enabler	Yes	Yes
NetXplorer Reporter	Yes	Yes
Physical		
Size (H x W x D)	Standard 2U by 19" rack mount	
Weight	9.1 kg (20 lb)	
Bypass Unit	External, 1U, 19" rack mount	
Power		
Input (AC/DC)	100 to 240 VAC, 80 W; -48 VDC, 80 W	
No. Power Supply Units	2 (Load Sharing)	
Redundancy for PSUs	1 + 1	
Safety and Certifications		
Safety	UL 60950-1/ CSA C22.2 60950 (ITE) EN 60950-1 ITE	
Emission	EN 55024:1998; A1:2001; A2:2003 Immunity for ITE EN 61000-3-2:2001 Harmonic Emissions EN 61000-3-3:1995; A1:2000 Voltage Fluctuations EN 55022:1998; A1:2000; A2:2003 Emissions for ITE VCCI FCC Part 15, Sub-Part B	

Tabla A2.2 : Especificaciones Técnicas de NetEnforcer AC-1000

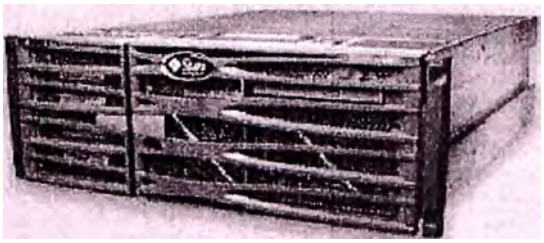
	AC-1010	AC-1020	AC-1040
Capacity			
Number of Connections/Flows	1,000,000 / 2,000,000		
Throughput	2 Gbps (1 Gbps, Full Duplex)		
Pipes/Virtual Channels	10,000 / 80,000	10,000 / 80,000	4,000 / 28,000
No. of Subscribers	100,000		
Physical and Connectivity			
Management Interface	10/100 BaseT		
Network Interfaces (Internal / External)	2x1000 BaseT or 2x1000 BaseSX or 2x1000 BaseLX	4x1000 BaseT or 4x1000 BaseSX or 4x1000 BaseLX	8x10/100 BaseT
Console Port	Serial, RJ-45 Connector		
Application Identification (DPI) Protocols (Security Incl.)			
P2P Protocols	Including BitTorrent, eDonkey, Warez, WinMX, Kazaa		
VoIP Protocols	Including Skype, H.323, SIP, RTP, Net2Phone		
Gaming Protocols	Including Doom, Diablo, MSN Game, SWAT, Ultima		
Web/Streaming Application Protocols	Including Abacast, iTunes, RTSP, Winamp MMS		
Traffic Encapsulation Protocols	Including L2TP, MPLS, PPPoE		
Control Options			
Monitoring Only	Yes	Yes	Yes
QoS Enforcement Levels	155, 310, 622 Mbps and 1 Gbps (Full Duplex)		400 Mbps (Full Duplex)
Policy Levels (Pipes/VCs)	2,000 / 8,000; 5,000 / 40,000; 10,000 / 80,000		4,000 / 28,000
Redundancy	Serial & parallel (1:1)	Serial, parallel & active (1:1, 1+1)	
Add-Ons: NetXplorer Enabler	Yes	Yes	Yes
NetXplorer Reporter	Yes	Yes	Yes
NetAccountant	Yes	Yes	Yes
NetRedirector	Yes	Yes	Yes
Dimensions			
Size (H x W x D)	Standard 2U by 19" rack mount		
Weight	8.3 kg (18.2 lb)		
By-pass Unit	External, 1U, 19" rack mount		
Power			
Input (AC/DC)	100 to 240 VAC, 80 W; -48 V DC, 80 W		
No. Power Supply Units	2 (Load Sharing)		
Redundancy for PSUs	1 + 1		
Safety & Emission Standards			
Safety	UL 60950-1/ CSA CS22.2 60950 (ITE) EN 60950-1 ITE		
Emission	EN 55024:1998; A1:2001; A2:2003 Immunity for ITE EN 61000-3-2:2001 Harmonic Emissions EN 61000-3-3:1995; A1:2000 Voltage Fluctuations EN 55022:1998; A1:2000; A2:2003 Emissions for ITE VCCI FCC Part 15, Sub-Part B		

A3. SERVIDORES SUN

Tabla A3.1 Características del equipo Sun Fire V440

Sun Fire™ V440 Server

A data center-class, rack-optimized server that sets the new standard for low-cost network computing



Key Feature Highlights

- Up to four 1.593-GHz UltraSPARC IIIi CPUs, each with 32 GB memory capacity
- Integrated dual-channel SCSI disk controller
- Two 10/100/1000 Mb/sec, Ethernet ports
- Solaris™ 8, Solaris 9, and Solaris 10 Operating System
- 1+1 hot-plug power supplies/hot-pluggable disks
- Six full-length, industry-standard PCI bus slots
- Rack-optimized, 4U enclosure
- Hardwar[illegible] disk mirroring
- Front [illegible] d fault LED indicators; rear power an[illegible]
- Expanded front-access capabilities: Up to four hot-plug disk drives, power switch, media bay, and power supplies
- Advanced Lights Out Manager
- System Configuration Card (SCC[illegible] allows system identity to be transferred to standby system[illegible]

Value, Availability, and Manageability

The Sun Fire V440 server is a data center-class, entry-lev el server that is powered by up to four 1.593-GHz UltraSPARC IIIi processors. Features such as six PCI slots, two 10/100/1000 Mb/s Ethernet ports, up to four disk drives, and 32 GB of memory prove the rack-optimized Sun Fire V440 server has the capacity to meet the needs of compute-intensive applications. The Sun Fire V440 server also contains high-availability and manageability features in a compact, 4U pack-age. Hot-plug, front-accessible disk drives; redundant hot-plug power supplies (with independent cords); and a System Configuration Card that permits easy and qu ick identity transfer enhance the Sun Fire V440 server's uptime. Easily visible system and component LEDs provide serviceability features that enable quick diagnosis and repairs, while the system's Advanced Lights Out Manager (ALOM) provides remote management and diagnostic capability.

Value

UltraSPARC IIIi delivers price/performance and rock-solid Solaris reliability in a rack-optimized enclosure on an entry-level server. Customers can run demanding, mission-critical applications in a low-cost, secure environment.

Low-Cost Network Computing UltraSPARC IIIi processors and support for the Solaris Operating System, Solaris Web[illegible] and Sun Cluster 3.0 make the Sun Fire™ V440 the ideal server for Web infrastructure computing, corporate compute farms, hosting, and custom-application deployment.

Reducing Complexity

Advanced Lights Out Manager (ALOM) provides remote management functionality, lowering the requirement for onsite staff. The System Configuration Card increases availability by allowing quick and easy system ID transfer. Support for the SunSM Install Check tool enables customers to confirm proper initial system configuration and installation.

Improve TCO

Low acquisition and support costs, low power and cooling requirements, and binary compatibility provide greater flexibility in high-density, horizontal-scaling environments.

Sun Fire V440 Server System Requirements

Architecture	
Processor	Two to four UltraSPARC IIIi 1.593 GHz
Architecture	64 bit, 4-way superscalar SPARC® V9
Cache	64 KB data, 32 KB instruction; and 1 MB integrated L2

Main Memory

4 DIMM slots per processor, registered DDR-1 SDRAM system configurations from 4 GB to 32 GB

Standard Integrated Interfaces

Network	Two 10/100/1000Base-T Ethernet
Network management	One 10Base-T Ethernet
Serial management	One TIA/EIA-232-F (RJ45) Port
Serial	One TIA/EIA-232-F asynchronous (DB9) Port
SCSI	One Ultra320 SCSI (LVD)
USB	Four OHCI 1.0 compliant interfaces, supporting dual speeds of 12 and 1.5 Mbits/sec. each
Expansion bus	Six internal PCI 2.2 compliant expansion slots: Three 64-bit 33/66 MHz 3.3V full-length Three 64-bit 33 MHz 5V full-length
System configuration card	Front-accessible for transfer of system configuration information, including host ID

Mass Storage and Media

Internal disk	Up to four hot-plug Ultra320 SCSI 73-GB disks
Internal DVD	One slimline ATAPI DVD-ROM
External disk	Sun StorEdge™ 3310 SCSI Sun StorEdge 3310 NAS Sun StorEdge 3510/3511 Sun StorEdge 3120 Sun StorEdge D240 Sun StorEdge S1 Sun StorEdge 6120/6320 Sun StorEdge 3900 Sun StorEdge 6900 Sun StorEdge 9900
External tape	Sun StorEdge DLT8000 Flexipack Sun StorEdge SDLT 220 Sun StorEdge SDLT 320 Sun StorEdge DAT 72 Sun StorEdge L702 Sun StorEdge L7 Sun StorEdge L8 Sun StorEdge L25 Sun StorEdge L100

Software

Operating	Solaris 8 (Hardware Release 07/03 or later), Solaris 9 12/03, and Solaris 10 (preinstalled)
Enterprise infrastructure software	Sun Java Enterprise System 2004Q2* available on select configurations only
Languages	C/C++, FORTRAN, Java™ programming language, all other standard Sun-supported languages
Networking	ONC™, NFS, TCP/IP, SunLink™, OSI, MHS, IPX™/SPX
Management	Sun™ Management Center, SunVTS™, SRS Ready, SRM, ALOM, Sun Install Check Tool

Power Supplies

One required, two for redundancy (hot plug) with separate power cords

Maximum AC Power	650 W
Typical AC Power	570 W

Environment

AC power	90 to 264 V AC (47 to 63 Hz)
Operating temperature	5° C to 40° C (41° F to 104°), 20% to 80% relative humidity, non condensing, 27° C max. wet bulb
Nonoperating temperature	-40° C to 60° C (-40° F to 140°), up to 93% relative humidity, noncondensing, 38° C max. wet bulb
Altitude (operating)	Up to 3000m
Altitude (non-operating)	Up to 12,000m
Acoustic noise	6.7 Bels operating and 6.7 Bels idle

Regulations (meets or exceeds the following)

Product safety	UL approval to UL 60950, EN60950, C22.2 No.60950, and CB Report for IEC 950; all including Amendments 1, 2, 3, 4 and 11 and full worldwide deviations. TUV approval to EN60950/IEC 950. GOST Certification for Eastern Block countries. Korean MIC Certification. China CCC mark using UL as agent. CE Declaration of Conformance (SDoC self-declaration) to The Electromagnetic Compatibility Directive and Low Voltage Directive with accompanying "Technical Data File." Approval to Argentinian standards using UL as agent.
EMI	47 CFR 15B (Code of Federal Regulations, Part 15, Subpart B) Class A; EN55022 Class A per EMC Directive 89/336/EEC (CE Mark); VCCI Class A; Industry Canada ICES-003; AS/NZ 3548 (Australia/New Zealand); CNS 13438 (Taiwan); KSC 5858 (MIC Mark/Korea)
RoHS	Restriction of Hazardous Substances — RoHS compliant configurations available

Get the details.
Find out more about the Sun Fire V440 server—an ideal solution for e-mail, hosting, e-commerce, OLTP, and online banking, supply chain, and database management, inventory management, CRM, ERP, EDA, MCAD, and simulations—by visiting: sun.com/v440.

Immunity Certifications

IEC 1000	EN55024 per EMC Directive 89/336/EEC, including IEC 61000-4-2 Electrostatic discharge immunity test IEC 61000-4-3 Radiated, radio-frequency, electromagnetic field immunity test
	IEC 61000-4-4 Electrical fast transient/burst immunity test IEC 61000-4-5 Surge immunity test IEC 61000-4-6 Immunity to conducted disturbances, induced by radio-frequency fields IEC 61000-4-8 Power frequency magnetic field immunity test
	IEC 61000-4-11 Voltage dips, short interruptions and voltage variations immunity tests
Line distortion	EN 61000-3-2 per EMC Directive 89/336/EEC
Voltage fluctuations and flicker	EN 61000-3-3 per EMC Directive 89/336/EEC

Dimensions and Weight

Height	174 mm (6.85 in.)
Width	440 mm (17.3 in.)
Depth (including bezel)	635 mm (25 in.)
Weight	37 kg (82 lb.) fully configured
Enclosure	Fits into a standard 19-inch wide rack-mount kit that complies with EIA-310-D1992 standard

Upgrades

Upgrades are available for SPARC server and Sun Enterprise™ systems. Contact your local Sun sales representative for details.

Warranty

Hardware support	3 years
Software install	90 days
Call response	8 hours
Delivery	Second business day, on-site

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com

Sun

Tabla A3.2 : Características del equipo Sun Fire V490

DATASHEET

Sun Fire™ V490 Server

Extreme optimization, utilization, reliability, and investment protection in the economies of a rack-optimized footprint.

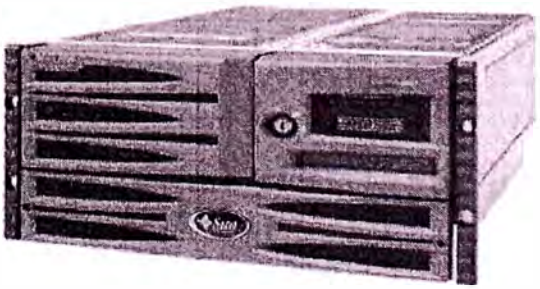
The Sun Fire™ V490 server, powered by the new UltraSPARC® IV+ processor and Solaris™ OS, offers faster performance in a low-cost, low-density footprint. This server delivers over 5 times the performance of UltraSPARC III servers, and over double the performance of UltraSPARC IV servers in the same footprint. As such, it provides greater value out of existing Sun Fire servers now, and assures long systems life by protecting IT investments over time. With up to four UltraSPARC IV+ Chip Multithreading (CMT) processors executing eight concurrent threads and up to 64 GB of memory in a dense, rack-optimized, 5-RU, 24-in.-deep enclosure, the Sun Fire V490 server delivers compute density with enterprise-class levels of throughput at a low-cost server price.

Because of Sun's industry-leading investment protection technologies, you can save costs over the life cycle of your hardware and applications. Sun's commitment to 100% application binary compatibility means that there is no disruption to your existing software infrastructure, as your Solaris applications just continue to run. Furthermore, for the first time in the industry, a 4-socket server supports mixed generations and speeds of UltraSPARC IV+ and UltraSPARC IV CPU/memory boards in the same system, allowing you to maintain existing investments while seamlessly upgrading your system with faster processors.

Leveraging advanced Solaris 10 OS capabilities such as Solaris Containers, the Sun Fire V490 server is an ideal platform to run multiple applications in an isolated and secure environment for projects such as enterprise messaging consolidation. The Sun Fire V490 server delivers significant productivity gains to address ever-demanding applications such as Application Serving, Business Processing, Database Services, IT Infrastructure, Application Development, Collaboration, and compute-intensive Scientific Engineering.

Key Feature Highlights

- Delivers over 5 times the performance of UltraSPARC III servers and over double the performance of UltraSPARC IV servers in the same footprint.
- Scales up to 4 processors with 8 threads and up to 64 GB memory in a 5U rack-optimized package.
- Unique Solaris OS application compatibility guarantee enables seamless migration to newer processor technologies.
- Mix and match UltraSPARC IV+ and IV processors in the same system for in-chassis upgrades to faster processors, preventing forced migrations.
- New RAS and security enhancements improve system uptime.
- Predictive Self-Healing for increased reliability and Sun Systems Controller for remote system administration.
- Dynamic Tracing (DTrace) allows further application performance optimization — up to 30x gains seen by customers.
- Ideal for consolidating applications using Solaris Containers technology.
- 6 PCI slots help ensure an expandable system.
- Three-year warranty with SunSpectrum™ Support upgrade options for integrated hardware and OS support.



Sun Fire V490 Server Specifications

Processor

Processor	Configure up to four UltraSPARC IVi and/or UltraSPARC IV processors
Architecture	Superscalar SPARC V9 RISC processor
Processor modules	One or two dual-processor/memory modules
Cache per UltraSPARC IV+ processor	Level 1: 64 KB data and 64 KB instruction per processor Level 2: 2 MB on chip Level 3: 32 MB external

Main Memory

Maximum memory 64 GB when configured with four processors

Standard Integrated Interfaces

Network	Two 10/100/1000 Mbps Ethernet
SCSI	Ultra 320 dual channel
Serial	RJ-45 serial port
Expansion capability	Six PCI slots compliant with PCI Hot-Plug Specification Revision 2.1 (3 @ 66 MHz, 64 bits wide, 3.3 volts; 3 @ 33 MHz, 64 bits wide, 3 volts)
USB	Two compliant with USB Revision 1.1

Mass Storage and Media

Internal slots	Two slots for hot-pluggable USB and dual DVD-ROM drives
Internal disk	Up to four 3.5" x 1.0" 15K RPM FC-AL disks (146 GB capacity), providing a maximum total capacity of 584 GB
External disk	Sun StorEdge T3 (T3B) Sun StorEdge 3510 FC Sun StorEdge 3120 Sun StorEdge 3511 SCSI RAID/JBOD Sun StorEdge 6120 Sun StorEdge 6130 FC RAID/JBOD Sun StorEdge 6320 Sun StorEdge 6140 Array Sun StorEdge 6920 Sun StorEdge 9910/9960/9970/9980
Tape media	Sun StorEdge DAT 72 desktop tape drive Sun StorEdge DLT VS1 desktop tape drive Sun StorEdge DLT VS160 desktop tape drive Sun StorEdge T3 desktop tape drive Sun StorEdge SDLT 320 desktop tape drive Sun StorEdge SDLT 600 desktop tape drive Sun StorEdge LTO Sun StorEdge AIT Sun StorEdge 9840 Sun StorEdge SL24 AIT Loader tape library Sun StorEdge SL500 tape library

Software

Operating system (minimum version)	The minimum OS version for UltraSPARC IV+ processors is Solaris 9 9/05, and Solaris 10 3/05 HW1 The minimum OS version for UltraSPARC IV processors is Solaris 9 9/05, Solaris 8 2/02, and Solaris 10 1/06
Enterprise administration software	Sun Java™ Enterprise System

Power Supplies

Input per power supply/system at nominal voltage, nameplate

Maximum AC input	1187 W per power supply
Maximum DC output	1440 W per power supply

Environmental

AC power	200–240 VAC, 47–63 Hz, 2000 VA
Operating	5°C to 35°C (41°F to 95°F), 20% to 80% relative humidity, noncondensing; 27°C max. wet bulb
Nonoperating	-40°C to 60°C (-40°F to 140°F), 93% relative humidity, noncondensing

Regulatory (product safety and electromagnetic compatibility requirements)

Product safety	UL/CSA 60950-1, EN/IEC 60950-1, IEC 60950-1 CB Scheme with all country deviations, SEMKO 1, 2, UL 1950 part 1/181, EN 61950
EMI/EMC	EN55022 Class A, 47 CFR 15B Class A, ICES Class A, VCCI Class A, AS/NZS 3548 Class A, CNS 13438 Class A, EN/IEC 61000 Class A, GB 9254 Class A, EN61000-3-2, GB 17625.1, EN61000-3-3
Immunity	EN55024/CISPR 24
Telecommunications	EN300 386
Regulatory markings	CE, IEC, ICES-003, GOST-R, VCCI, GOST-R, BSMI, MIC, UL/CUL, UL/S-mark
Other	Restriction of Hazardous Substances (RoHS) 6 substances/EU/EEC, labeled per Waste Electrical and Electronic Equipment (WEEE) Directive

Key RAS Features

- Hot-pluggable disk drives
- Redundant, hot-swappable power supplies
- Environmental monitoring and fault detection
- Automatic System Recovery (ASR) capabilities
- Remote Lights Out Management capability
- Dual-loop enabled FC-AL subsystem
- Support for disk and network multipathing with automatic failover capability
- Error correction and parity checking for improved data integrity

Sun Upgrade Advantage Program

The Sun Upgrade Advantage Program (UAP) offers upfront discounts for trade-in of qualified Sun and competitive servers to new state-of-the-art implementations of Sun Fire servers. Whether upgrading one system or consolidating many systems to one, Sun UAP offers the flexibility to trade in and receive credit to cover these new Sun system purchases. Upgrades are also available to Sun Fire server brands and I/O assemblies. For more information visit sun.com/trade/servers.

Dimensions and Weight

Height	22.2 cm (8.75 in.)
Width	44.6 cm (17.5 in.)
Depth	64.0 cm (25.2 in.)
Weight	36.8 kg (79 lb.) minimum; 44 kg (97 lb.) maximum

Warranty and Support Services

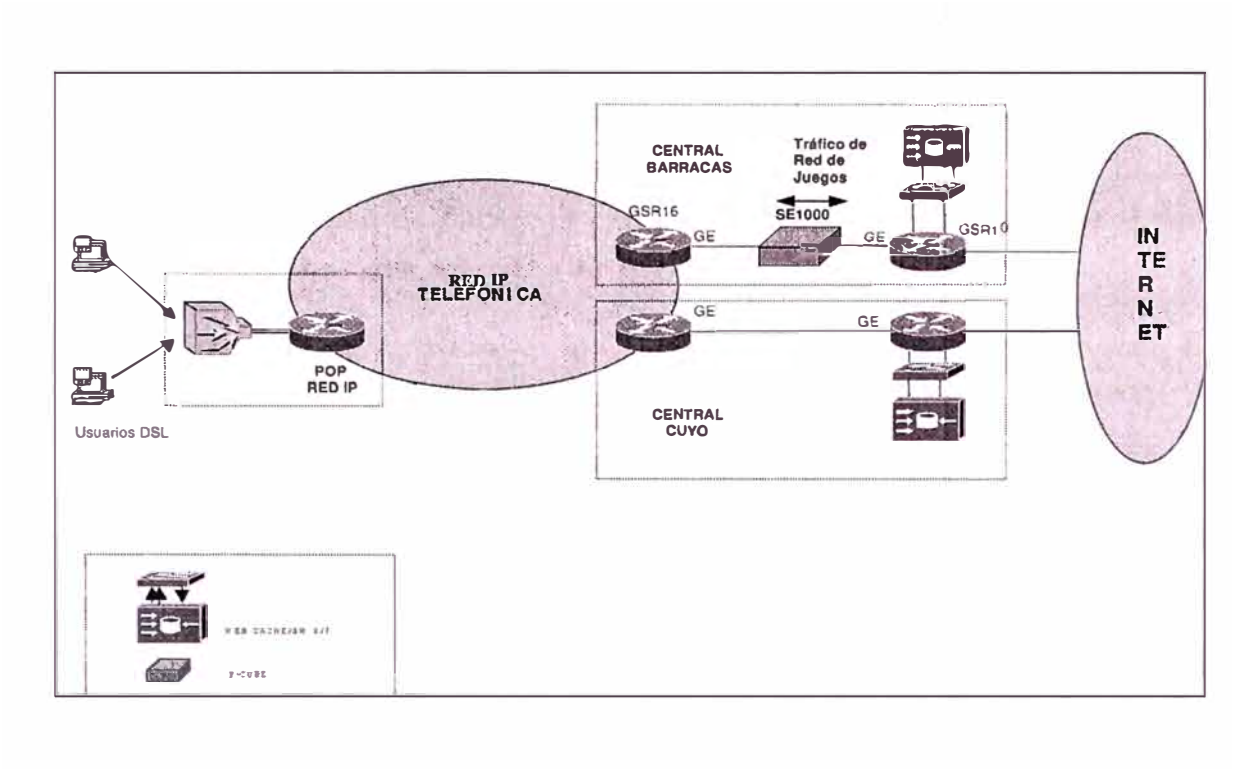
Hardware warranty	1 year, 8 AM business day, on site
Enhanced support	SunSpectrum Support Upgrades provide integrated hardware and OS coverage including Sun technical support, same-day hardware service and premium online resources. Choose from three options.
Implementation	System and software migration, installation and implementation services available.
Training	Available at sun.com/training

For More Information

Learn how the Sun Fire V490 server combines investment protection with extreme performance in a low-cost, compact footprint. Contact your Sun Representative at 1-800-555-9SUN, or visit sun.com/v490.

ANEXO B

Figura B1.1 Esquema de conectividad de Prueba piloto en Telefónica Argentina (TASA)



BIBLIOGRAFÍA

[1] Raul Jiménez Contreras , "Diseño de un protocolo de almacenamiento y distribución de ficheros orientado a la reducción de costes de proveedores de acceso a Internet", Universidad de Zaragoza - España, 2006. `jgawww.tslab.ssvl.kth.se/~raul/ant/doc/es/ant_es.pdf` (29 Diciembre 2006)

[2] Luis Enrique Torreyes Rico, " Voz sobre IP", Universidad Nacional Experimental Simón Rodríguez (U.N.E.S.R.) - Caracas-Venezuela, 1999. `http://www.monografias.com/trabajos3/voip/voip.shtml` (8 de Enero 2007)

[3] José Alfredo Picón Cabezud, "P2P: Nueva generación de productos y servicios", Telefónica I+D - Madrid, 2002.

[4] Antonio Javier Sánchez Esguevillas, Santiago Prieto Martín, David Artuñedo Guillé, "Servicios avanzados de voz sobre IP basados en SIP", Telefónica I+D - Madrid, 2002.

[5] Daniel Aubareda, "P2P, la gran descentralización de la Red", Centro de Predicción Económica de la UAM - Madrid-España, 2005.

[6] Luis Castejón, "Voz sobre IP: la revolución por llegar", IEEE-2005. Más información en: `www.cisco.com`.

[7] Presentation "Service Control", Cisco Systems - Perú, 2004.

[8] Franklin Sandoval, "Internet el Arte de Romper Paradigmas", Universidad Nacional Abierta Caracas Venezuela - Venezuela, 1998.

[9] "Product Overview Release 2.1 (Document revision-09)", Cisco (P-Cube Engage/Service Control Engine) - Luxemburgo, 2004. Más información en: `www.cisco.com`.

[10] P/N BR002E00, Rev. A, "Enabling Traffic and Subscriber Control in Broadband Networks / Traffic Management Solutions for Carriers and Service Provider", Allot Comunications, 2006. Más información en: `www.allot.com`