ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ESTUDIO DE UN ADMINISTRADOR DE ANCHO DE BANDA APLICADO A UN ISP"

TÓPICO DE GRADUACIÓN

Previa a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:

Roody Javier Cayambe Ortiz.
Holger Agustín Murillo Moreira.

GUAYAQUIL – ECUADOR
2006

A G R A D E C I M I E N T O

Gratitud infinita a DIOS y a nuestra Familia que en todo momento depositaron su confianza y apoyo al desarrollo de nuestras carreras.

Un agradecimiento para los Ingenieros Diego Solano y Jhonny García quienes nos brindaron su apoyo de forma desinteresada con sus conocimientos. Y en especial al Ingeniero José Escalante para incrementar con sus consejos la confianza y fe de persistir en el cumplimiento de nuestras metas.

DEDICATORIA

A mis padres por el
apoyo brindado, en
especial a mi madre
que siempre ha sido
mi fuerza moral.

Roody

DEDICATORIA

A Dios,

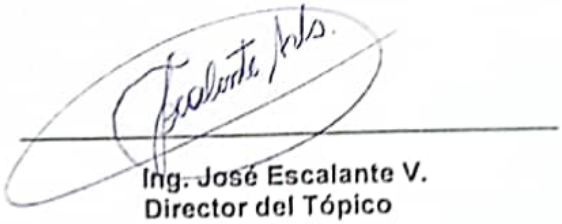
a mis padres por el

apoyo brindado.

Holger

TRIBUNAL DE GRADUACIÓN

Ing.Holger Cevallos
Subdecano de la FIEC



Ing. José Escalante V.
Director del Tópico

Ing. Gomer Rubio R.
Miembro del Tribunal

Ing. Sara Rios O.
Miembro del Tribunal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL."

Art. 12 del Reglamento de Graduación

Roody Javier Cayambe Ortiz

Holger Agustín Murillo Moreira

RESUMEN

Este estudio se basa en la necesidad de aprovechar al máximo el ancho de banda de los proveedores de Internet (ISP) controlando:

- El tráfico deseado y no deseado.
- Algunos programas que ocupan ancho de banda innecesariamente.
- Programas que son prioridad para la empresa dándole más ancho de banda
- La asignación de ancho de banda de forma dinámica.

En el primer capitulo se realiza un estudio de los conceptos fundamentales en que se basan los equipos para administrar el ancho de banda: capas del modelo OSI, Ancho de banda, Protocolo TCP/IP y TCP Rate Control.

El segundo capítulo presenta la justificación para el uso de un equipo para administrar el ancho de banda: Problemas que se presentan en los ISPs, debido a la naturaleza y características del Tráfico.

En el tercer capitulo estudiamos los diferentes equipos que administran las redes tales como: Bandwidth Manager, PacketShaper, QoSWorks, BWMeter, NetGrid y los costos de estos y sus características.

En el cuarto capitulo se hace un estudio del equipo administrador de ancho banda escogido, (PacketShaper) El funcionamiento, principales aplicaciones: la forma que hace la clasificación del tráfico, y las graficas de monitoreo de los clientes.

El quinto capítulo enfoca las aplicaciones específicas en un ISP que es nuestro tema de estudio y las principales ventajas que ofrece.

ÍNDICE GENERAL

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

4 ANÁLISIS Y ESTUDIO DE UN ADMINISTRADOR DE ANCHO DE BANDA (PACKETSHAPER) 94

CAPÍTULO V

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO DE TERMINOS.

ACK Notificación enviada por un dispositivo de la red a otro para comunicar que se produjo un evento determinado (por ejemplo, la recepción de un mensaje). A veces se abrevia ACK.

API El Programa Interfaces de Aplicación (Application Program Interface de Stradis) para windows simplifica la integración de los decodificadores Mpeg-2 de Stradis 4:2:2 en sus sistemas video - dando a su programa de uso control completo sobre todas las funciones del decodificador.

Apple Talk En informática, una red de área local de bajo precio desarrollada por Apple Computer que puede ser utilizada en ordenadores o computadoras Apple y de otras marcas para comunicaciones y para compartir recursos como impresoras y servidores de archivo.

Caching La más importante aproximación técnica para reducir el retardo y, como resultado, mejorar las prestaciones del sistema. Almacenar temporalmente los datos frecuentemente accedidos más cerca del solicitante de los mismos.

CLI	Comando de Interfaz de Línea. La forma de acceso a un terminal en un producto Packeteer, disponible vía remota o conexión directa de un terminal ASCII a un puerto consola. Los comandos son ingresados como texto en una sola línea.
DiffServ	Servicios diferenciados. El modelo de servicios diferenciados se basa en tráfico sin reservación. "Clasificación de los paquetes u Mecanismos de prioridad –DSCP –PHB "Su objetivo es asignar el ancho de banda a diferentes usuarios en una forma controlada.”
DNS	Sistema de denominación de dominio. Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.
FRC	Protocolo de transferencia de archivos. Protocolo de aplicación, parte de la pila de protocolo TCP/IP utilizado para la transferencia de archivos entre nodos de red. El FTP se define en RFC 959.

H.323	Es un Standard aprobado por la International Telecommunication Union (ITU) que define cómo se transmiten los datos en conferencias audiovisuales a lo largo de una red.
Host	Un computador que está conectado a la red TCP/IP.
IANA	Internet Assigned Numbers Authority. (Autoridad de Asignación de números de Internet)
IP	Protocolo de Internet. Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork no orientado a la conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad. Documentado en RFC 791.
OSI	interconexión de sistemas abiertos. Programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

PacketShaper	Un producto de Packeteer que es un sistema administrador de ancho de Banda y de tráfico basado en aplicaciones.
PacketWise	El software usado por PacketShaper de Packeteer.
RFC	Solicitud de comentarios. Documento oficial del Grupo de trabajo de ingeniería de Internet (IETF, Internet Engineering Task Force) donde se especifican los detalles de los protocolos incluidos en la familia TCP/IP.
RFC 1700	Asignación de números de puertos.
RFC 2474	Definición de los campos de servicios (DS Field) en las cabeceras Pv4 e IPV6.
RFC 3031	Define la arquitectura de MPLS (Multiprotocol Label Switching Architecture). Enero 2001.
SLA	Contrato de nivel de servicio. Números de puertos definidos por IANA

SMTP Protocolo de transferencia de correo simple. Protocolo Internet que suministra servicios de correo electrónico.

SNA Arquitectura de redes de sistema. Arquitectura de red grande, compleja, con gran cantidad de funciones, desarrollada en los 70 por IBM. Similar en algunos aspectos al modelo de referencia OSI, pero con varias diferencias. SNA está compuesto esencialmente por siete capas.

SNMP Protocolo de administración de red simple. Protocolo de administración de red que se utiliza casi exclusivamente en redes TCP/IP. SNMP suministra un medio para supervisar y controlar los dispositivos de red, y para administrar configuraciones, recoger estadísticas, el desempeño y la seguridad.

TCP Protocolo para el control de la transmisión. Protocolo de la capa de transporte orientado a conexión que proporciona una transmisión confiable de datos de full dúplex. TCP es parte de la pila de protocolo TCP/IP

TCP/IP	Protocolo de control de transporte/Protocolo Internet. Nombre común para el conjunto de protocolos desarrollados por el DoD de los EE.UU. en los años '70 para soportar el desarrollo de internetwork a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.
TCP Rate Control	La forma de control de tráfico, especificado en el protocolo TCP, y utilizado por PacketWise.
TELNET	Instrucción utilizada para verificar el software de capa de aplicación entre estaciones de origen y de destino. Este es el mecanismo de prueba más completo disponible.
TFTP	Protocolo de transferencia de archivos trivial. Versión simplificada de FTP que permite la transferencia de archivos de un computador a otro a través de una red.
TOS	Tipo de servicio. Es una porción de tres bits de la cabecera IP en un paquete TCP/IP reservado para controlar la calidad de servicio, QoS.

URL	Localizador universal de recursos. Esquema de direccionamiento estandarizado para acceder a documentos de hipertexto y otros servicios mediante un navegador de Web.

INTRODUCCIÓN.

El ancho de banda es un tema crítico, especialmente a la hora de seleccionar un buen proveedor de acceso a Internet. Mientras más se dispone, se obtiene más rapidez de acceso, pero eso no se da realmente. El ancho de banda se suele asimilar al diámetro de una tubería que sirve para canalizar el flujo de datos. Pero esa simplificación es excesiva. De entrada el ancho de banda es la capacidad de una línea para transmitir información.

Pero hay que tener en cuenta que la línea está compartida frecuentemente por muchos usuarios. Por tanto nos sirve de muy poco saber el ancho de banda que tiene un proveedor, si no sabemos cuantos usuarios comparten esa línea en un momento determinado. Hay pequeños proveedores con pocos clientes que utilizan una línea "estrecha"; sin embargo pueden ofrecer mejores tiempos de acceso que otros proveedores con canales más potentes, porque éstos tienen demasiados usuarios compartiendo la línea. La proporción es lo que cuenta, no el ancho en sí mismo.

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS.

1.1. Ancho de banda.

Las redes LAN y WAN siempre han tenido algo en común: el uso del término ancho de banda para describir sus capacidades. Este término es esencial para comprender las redes, y es el tema central de estudio.

1.1.1. Definición de ancho de banda.

Existen dos usos comunes del término ancho de banda: uno se refiere a las señales analógicas y el otro, a las señales digitales.

El ancho de banda analógico de una señal de información es la diferencia entre las frecuencias máxima y mínima contenidas en la información, y para un canal de comunicaciones es la diferencia entre las frecuencias máxima y mínima que pueden pasar, es decir su banda de paso. El ancho de banda de un canal de comunicaciones debe ser lo suficientemente grande para pasar todas las frecuencias importantes de información.

El ancho de banda digital es la medición de la cantidad de información que puede fluir desde un lugar hacia otro en un período de tiempo determinado. Bits por segundo es una unidad de medición. En la actualidad es posible comunicarse de modo más veloz. El gráfico proporciona un resumen de las diversas unidades.

Unidad de ancho de banda	Abrev.	Equivalencia
Bits por segundo	bps	1 bps = unidad fundamental de ancho de banda
Kilobits por segundo	kbps	1 kbps = 1.000 bps = 10^3 bps
Megabits por segundo	Mbps	1 Mbps = 1.000.000 bps = 10^6 bps
Gigabits por segundo	Gbps	1 Gbps = 1.000.000.000 bps = 10^9 bps

Fig. 1.1 Unidades de ancho de banda.

1.1.2. Importancia del ancho de banda.

En primer lugar, el ancho de banda es finito. En cualquier medio está limitado por las leyes de la física. Las limitaciones debidas a las propiedades físicas de los cables telefónicos de par trenzado que se encuentran en muchas casas, son las que limitan el rendimiento de los módem convencionales a alrededor de 56 Kbps. El ancho de banda del espectro electromagnético es finito: existe una cantidad limitada de frecuencias en el espectro de microondas, de ondas de radio e infrarrojo. Es por ello que la FCC (Comisión federal para las

comunicaciones) posee una división completa para el control del ancho de banda y de las personas que lo utilizan. La fibra óptica tiene un ancho de banda prácticamente ilimitado. Sin embargo, ahora se ha desarrollado e implementado la tecnología necesaria para crear redes que puedan usar plenamente el potencial de la fibra óptica.

Si se conoce de qué forma funciona, y si se tiene en cuenta que es finito, se puede ahorrar mucho dinero. Por ejemplo, el costo de las diversas opciones de conexión con los proveedores de servicios de Internet depende, en parte, del ancho de banda que se necesita durante el uso normal y en horas de uso máximo.

Existen dos conceptos principales que se deben entender con respecto a la "superautopista de la información". El primer concepto es que cualquier forma de información se puede almacenar como una larga cadena de bits. El segundo es que, aunque es útil guardar la información en forma de bits, esta no es una tecnología realmente revolucionaria. El hecho de que podamos compartir esos bits, billones de bits en 1 segundo, significa que la civilización moderna está llegando a un punto en que cualquier computador, desde cualquier lugar del mundo o del espacio exterior, se puede comunicar

con otro computador en cuestión de segundos o incluso en menos tiempo.

Es usual que una persona o una institución comienzan a utilizar una red, con el tiempo deseen tener un ancho de banda más grande, igual suceden con los programas de software multimedia. Los programadores creativos se están dedicando al diseño de nuevas aplicaciones capaces de llevar a cabo tareas de comunicación más complejas, que requieran por lo tanto canales de transmisión más grandes.

1.1.3. Variables importantes.

Latencia.

Medida de tiempo, específicamente el tiempo que le toma a un paquete viajar de un punto en la red a otro punto. Es un atributo de todo componente de red. Es el resultado de todos los procesos de comunicaciones (buffering, switching, retardo de propagación, etc.)

Se descompone en los tiempos de propagación, transmisión y colas, de la siguiente manera:

- Tiempo de Propagación: resulta de la razón entre la distancia a recorrer entre dos puntos, y la velocidad de la luz en el medio de propagación (cable, fibra, aire, etc.)

- Tiempo de Transmisión: es el tiempo que toma transmitir una unidad de datos y es resulta de la razón entre el tamaño del paquete de datos a enviar y el ancho de banda disponible.

- Tiempo en Colas: corresponde a los atrasos ocasionados por colas en la Red, debido a que los switches necesitan almacenar los paquetes por algunos momentos antes de direccionarlos.

Jitter.

Es la variación del retardo en un periodo de tiempo, producto de los distintos caminos que puedan toman los distintos paquetes de un mismo archivo, y tiene impacto negativo sobretodo para aplicaciones que utilizan video y audio, o comunicaciones sobre Internet.

Pérdida de paquetes.

Es la probabilidad promedio que un paquete sea descartado en la red. La pérdida de paquetes no siempre es mala.

Throughput.

Capacidad de un sistema para transferir información. La forma más usada de esta métrica es como medida de la eficiencia de la velocidad de transmisión que incluye el funcionamiento de los sistemas de transmisión y del protocolo mismo.

1.2. Modelo de referencia OSI.

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos.

Permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, se puede utilizar para comprender cómo viaja la información a través de una red. Además, visualiza cómo la información o los paquetes de datos viajan desde los programas de aplicación (por Ej. , hojas de cálculo, documentos, etc.), a través de un medio de red (por Ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aún cuando el transmisor y el receptor tengan distintos tipos de medios de red.

1.2.1. Protocolos.

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red utilizan el mismo lenguaje o protocolo. Un protocolo es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente.

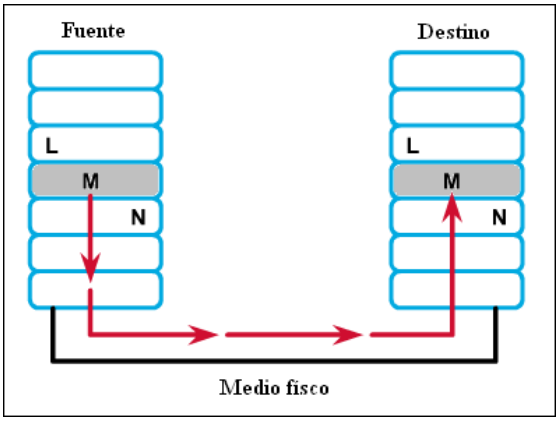


Fig. 1.2 Protocolo de comunicaciones.

Una definición técnica de un protocolo de comunicaciones de datos es: un conjunto de normas, o un acuerdo, que determina el formato y la transmisión de datos. La capa n de un computador se comunica con la capa n de otro computador. Las normas y convenciones que se utilizan en esta comunicación se denominan colectivamente protocolos de la capa n.

1.2.2. Las Capas del Modelo OSI.

Fig. 1.3 Las Capas del Modelo OSI.

La capa de aplicación.

Es la más cercana al usuario, suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias. La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

La capa de presentación.

Garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando uno común.

La capa de sesión.

Establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. Proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

La capa de transporte.

Segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la de sesión puede imaginarse como el límite entre los protocolos de aplicación y los de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están

relacionadas con asuntos de aplicaciones, las cuatro inferiores se encargan del transporte de datos.

La capa cuatro intenta suministrar un servicio de transporte de datos que aísla los niveles superiores de los detalles de implementación del transporte. Específicamente, la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.

La capa de red.

Es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

La capa de enlace de datos.

Proporciona tránsito de datos confiable a través de un enlace físico. Se ocupa del direccionamiento físico, la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

La capa física

Define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidos por las especificaciones de la capa física.

1.2.3. Ventajas del Modelo OSI.

Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.

- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.

- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.

- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.

- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

1.3. Protocolo TCP/IP.

Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el protocolo de control de transmisión / protocolo Internet (TCP/IP) El modelo de referencia TCP/IP y la pila de protocolo TCP/IP hacen que sea posible la comunicación entre dos computadores, desde cualquier parte del mundo, a casi la velocidad de la luz.

1.3.1. Las capas del modelo de referencia TCP/IP.

El modelo TCP/IP tiene cuatro capas: aplicación, transporte, Internet y acceso de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las del modelo OSI, pero realizan diferentes funciones en cada modelo.

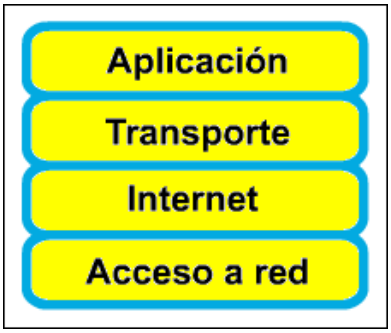


Fig. 1.4 Capas del Modelo TCP/IP.

1.3.1.1. Capa de aplicación

Soporta los protocolos de direccionamiento y la administración de red. Además tiene protocolos para transferencia de archivos, correo electrónico y conexión remota.

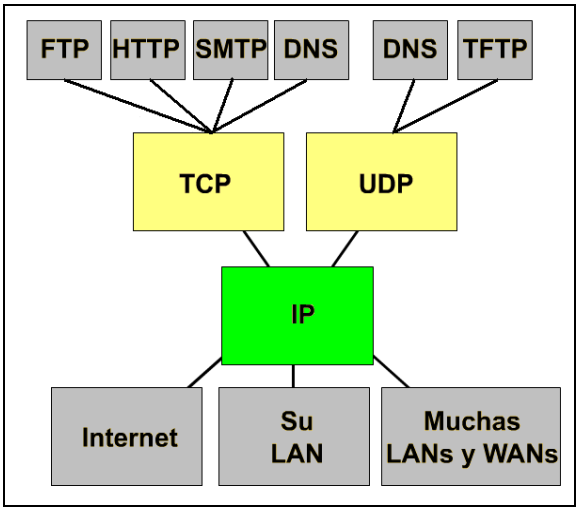


Fig. 1.5 Gráfico del protocolo TCP/IP.

SMTP (Protocolo simple de transferencia de correo) maneja la transmisión de correo electrónico a través de las redes informáticas. El único soporte para la transmisión de datos que suministra es texto simple.

SNMP (Protocolo simple de administración de red) es un protocolo que suministra un medio para monitorear y controlar dispositivos de red, y para administrar configuraciones, recolección de estadísticas, desempeño y seguridad.

FTP (Protocolo de transferencia de archivos) es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que soportan FTP. Soporta transferencias bidireccionales de archivos binarios y archivos ASCII.

TFTP (Protocolo trivial de transferencia de archivos) es un servicio no confiable no orientado a conexión que utiliza UDP para transferir archivos entre sistemas que soportan el protocolo TFTP. Es útil en algunas LAN porque opera más rápidamente que FTP en un entorno estable.

HTTP (Protocolo de transferencia de hipertexto) es el estándar Internet que soporta el intercambio de información en la World

Wide Web, así como también en redes internas. Soporta muchos tipos de archivos distintos, incluyendo texto, gráfico, sonido y vídeo. Define el proceso a través del cual los navegadores de la Web originan solicitudes de información para enviar a los servidores de Web. -

1.3.1.2. Capa de transporte

Permite que un dispositivo de usuario divida en segmentos varias aplicaciones de capas superiores para colocarlas en la misma corriente de datos del nivel cuatro, y permite que un dispositivo receptor pueda reensamblar los segmentos de las aplicaciones de los niveles superiores. La corriente de datos de capa cuatro es una conexión lógica entre los extremos de una red, y brinda servicios de transporte desde un host hasta un destino. Este servicio a veces se denomina servicio de extremo a extremo.

La capa de transporte también proporciona dos protocolos:

TCP: un protocolo confiable, orientado a conexión; suministra control de flujo a través de ventanas deslizantes, y confiabilidad a través de los números de secuencia y acuses de recibo. TCP vuelve a enviar cualquier mensaje que no se reciba y suministra

un circuito virtual entre las aplicaciones del usuario final. La ventaja de TCP es que proporciona una entrega garantizada de los segmentos.

UDP: protocolo no orientado a conexión y no confiable; aunque tiene la responsabilidad de transmitir mensajes, en esta capa no se suministra ninguna verificación de software para la entrega de segmentos. La ventaja de UDP es la velocidad. Como UDP no suministra acuses de recibo, se envía menos cantidad de tráfico a través de la red, lo que agilita la transferencia.

1.3.1.3. Capa de Internet.

Corresponde a la capa de red del modelo OSI. Tiene la responsabilidad de transportar paquetes a través de una red utilizando el direccionamiento por software.

Varios protocolos operan en la capa Internet de TCP/IP:

IP: suministra enrutamiento de datagramas no orientado a conexión, de máximo esfuerzo de entrega; no se ocupa del contenido de los datagramas; busca la forma de desplazar los datagramas al destino.

ICMP: aporta capacidad de control y mensajería.

ARP: determina direcciones a nivel de capa de enlace de datos para las direcciones IP conocidas.

RARP: determina las direcciones de red cuando se conocen las direcciones a nivel de la capa de enlace de datos.

1.3.1.4. Capa de acceso a red.

Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología LAN y WAN y todos los detalles de la capa física y de enlace de datos del modelo OSI.

1.3.2. Formato del protocolo TCP Y UDP.

El segmento TCP está formado por los siguientes campos:

- Puerto origen: número del puerto que realiza la llamada.
- Puerto destino: número del puerto que recibe la llamada.

- Número de secuencia: número que se utiliza para asegurar la secuencia correcta de los datos que se reciben.

Fig. 1.6 Formato del protocolo TCP.

- Número de acuse de recibo: siguiente octeto TCP esperado.

- HLEN: cantidad de palabras de 32 bits del encabezado.

- Reservado: se establece en 0.

- Bits de código: funciones de control, por Ej. , el establecimiento y terminación de una sesión.

- Ventana: cantidad de octetos que el emisor está dispuesto a aceptar.

- Suma de comprobación: suma de comprobación calculada de los campos de encabezado y datos.

- Señalador urgente: indica el final de los datos urgentes.

- Opción: la definida en la actualidad tamaño máximo del segmento TCP.
- Datos: Datos de protocolo de capa superior.

Los protocolos de la capa de aplicación deben brindar confiabilidad en caso de ser necesario. UDP no utiliza ventanas ni acuses de recibo. Está diseñado para aplicaciones que no necesitan ensamblar secuencias de segmentos. Como se puede observar en la figura, el encabezado UDP es relativamente pequeño.

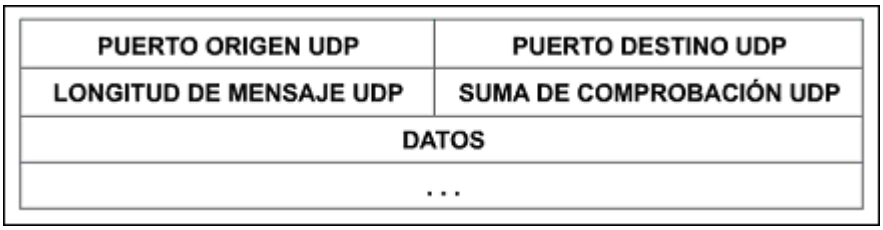


Fig. 1.7 Formato del protocolo UDP.

1.3.3. Números de Puerto TCP y UDP.

Son utilizados por los protocolos TCP como UDP para enviar información a las capas superiores y para mantener un registro de las distintas conversaciones que atraviesan la red al mismo tiempo.

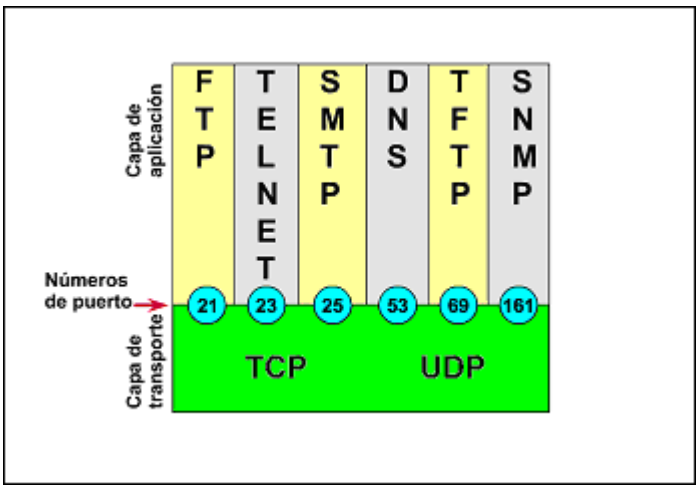


Fig. 1.8 Números de puerto.

Los creadores del software de aplicación han acordado utilizar los números de puerto conocidos que se definen en RFC 1700. Por ejemplo, cualquier conversación destinada a una aplicación FTP utiliza el número de puerto 21 como estándar.

A las conversaciones que no involucran ninguna aplicación que tenga un número de puerto conocido, se les asignan de forma aleatoria

dentro de un intervalo específico y sirven como direcciones origen y destino en el segmento TCP/UDP.

Algunos puertos son puertos reservados, tanto en TCP como en UDP, aunque es posible que algunas aplicaciones no estén hechas para soportarlos. Los números de puerto tienen los siguientes intervalos asignados:

- Los números inferiores a 255 corresponden a aplicaciones públicas.

- Los números entre 255-1023 se asignan a empresas para aplicaciones comercializables.

- Los números superiores a 1023 no están regulados.

- Los sistemas finales utilizan números de puerto para seleccionar la aplicación adecuada. El host origen asigna dinámicamente los números de puerto origen, por lo general un número mayor que 1023.

1.3.4. Saludo de tres vías (conexión abierta)

Los servicios orientados a conexión se dividen en tres fases:

- Fase de establecimiento de la conexión: se determina una ruta única entre el origen y el destino. Normalmente los recursos se reservan en este momento para garantizar un grado de servicio constante.

- Fase de transferencia de datos: los datos se transmiten secuencialmente siguiendo la ruta establecida, llegando a su destino en el orden en que se enviaron.

- La fase de terminación de la conexión: consiste en terminar la conexión entre el origen y el destino cuando no se necesita.

Los hosts TCP establecen una sesión orientada a conexión entre sí a través de un saludo de tres vías, que sincroniza una conexión en ambos extremos antes de transferir los datos. Este intercambio de números introductorios de secuencia, durante la secuencia de conexión es importante. Garantiza que, si se pierden datos debido a problemas de transmisión, se puedan recuperar.

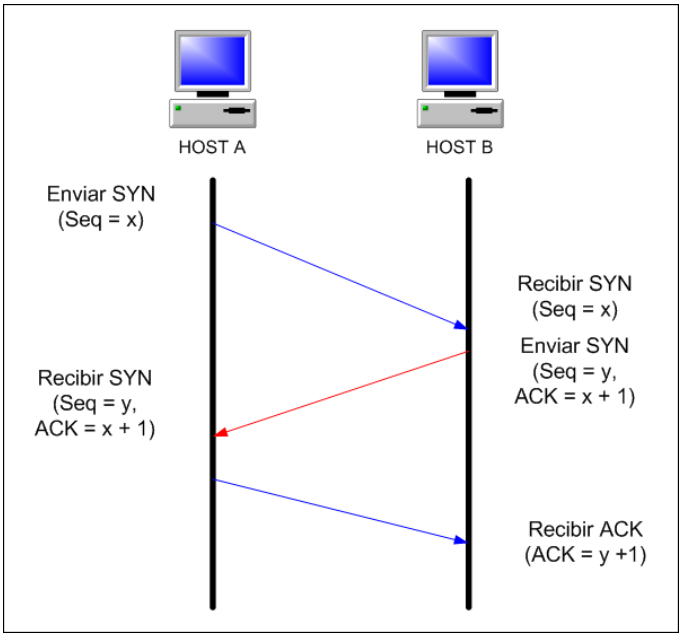


Fig. 1.9 Saludo de tres vías.

En primer lugar, un host inicia una conexión enviando un paquete que indica su número de secuencia inicial de x con cierto bit en el encabezado para indicar una petición de conexión. En segundo lugar, el otro host recibe el paquete, registra el número de secuencia x, responde con un acuse de recibo x + 1 e incluye su propio número de secuencia inicial y. El número de acuse de recibo x + 1 significa que el host ha recibido todos los octetos hasta e incluyendo x, y espera x + 1 a continuación.

El acuse de recibo y retransmisión positivos, o PAR, es una técnica común utilizada por muchos protocolos para proporcionar

confiabilidad. Con PAR, el origen envía un paquete, inicia un temporizador y espera un acuse de recibo antes de enviar el paquete siguiente. Si el temporizador expira antes de que el origen reciba un acuse de recibo, el origen retransmite el paquete y reinicia el temporizador.

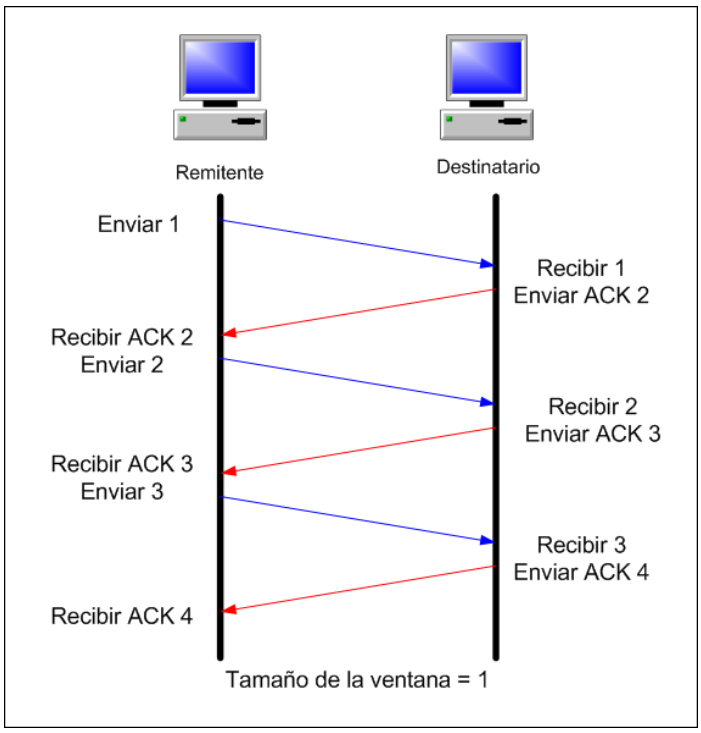


Fig. 1.10 Acuse de recibo simple.

El tamaño de ventana determina la cantidad de datos que se pueden transmitir en un determinado momento antes de recibir un acuse de recibo desde el destino. Cuanto mayor sea el número del tamaño de ventana, en bytes, mayor será la cantidad de datos que el host puede

transmitir. Después de que el host transmite la cantidad de bytes correspondiente al número de la ventana, el host debe recibir un acuse de recibo que indique que los datos han sido recibidos antes de poder enviar otros mensajes. Por ejemplo, con un tamaño de ventana de 1, se debe recibir un acuse de recibo para cada segmento individual antes de poder enviar el segmento siguiente.

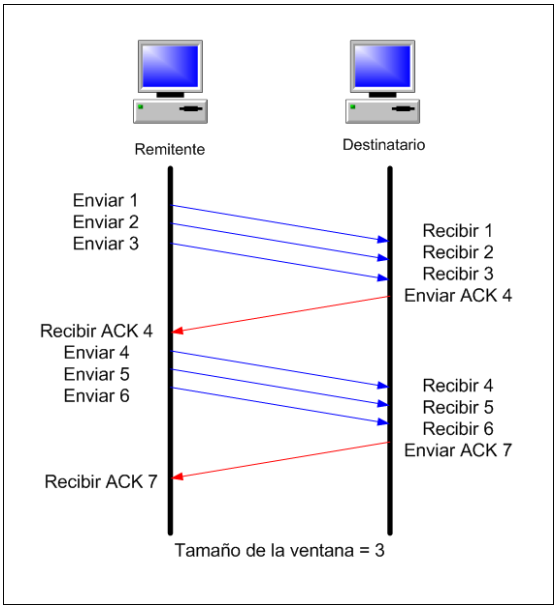


Fig. 1.11 Ventana deslizante.

TCP usa acuses de recibo de expectativa, lo que significa que el número del acuse de recibo se refiere al siguiente octeto esperado. Ventana deslizante, se refiere al hecho de que el tamaño de la ventana se negocia de forma dinámica durante la sesión TCP. Esto

da como resultado un uso poco eficiente del ancho de banda por parte de los hosts.

El uso de ventanas es un mecanismo de control de flujo que requiere que el dispositivo origen reciba un acuse de recibo desde el destino después de transmitir una cantidad determinada de datos. Por ejemplo, con un tamaño de ventana de tres, el dispositivo origen puede enviar tres octetos al destino. Entonces debe esperar un acuse de recibo. Si el destino recibe los tres octetos, envía un acuse de recibo al dispositivo origen, que ahora puede transmitir otros tres octetos. Si, por algún motivo, el destino no recibe los tres octetos, por ejemplo, debido a búferes cuya capacidad se ha excedido, no envía un acuse de recibo. Como el origen no recibe un acuse de recibo, sabe que los octetos se deben retransmitir y que la velocidad de transmisión debe reducirse.

TCP proporciona una secuencia de segmentos con un acuse de recibo de referencia de envío. Cada datagrama se numera antes de la transmisión. En la estación receptora, TCP reensambla los segmentos hasta formar un mensaje completo. Si falta algún número de secuencia en la serie, ese segmento se vuelve a transmitir. Si no

se recibe un acuse de recibo para un segmento dentro de un período de tiempo determinado, se produce la retransmisión.

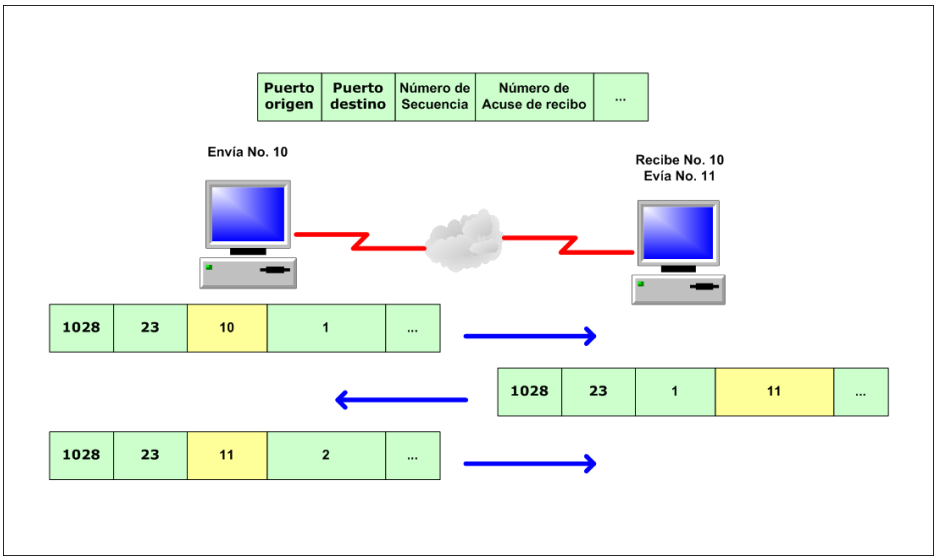
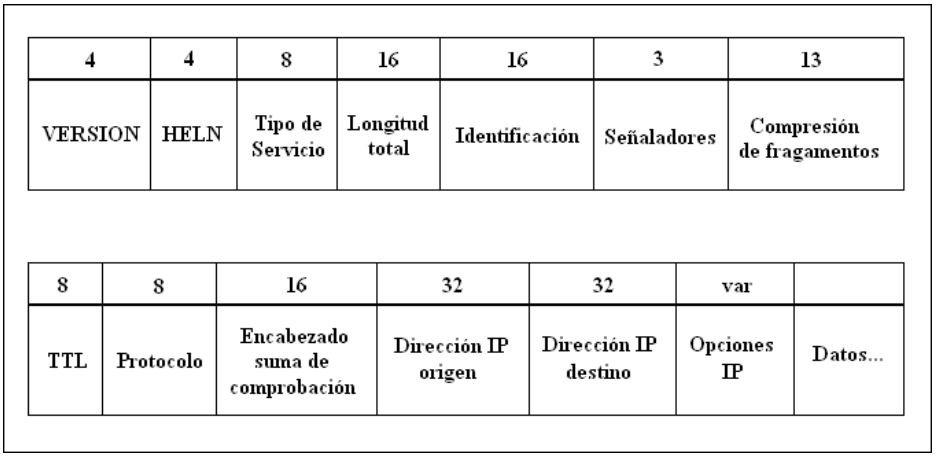


Fig. 1.12 Secuencia TCP y números de acuse de recibo.

1.3.5. Protocolos de Internet IP.

1.3.5.1. Datagrama del Protocolo IPV4.

Un datagrama IP contiene un encabezado IP y datos, y está rodeado por el encabezado de la capa de Control de Acceso al Medio (MAC) y la información final de la capa MAC. Un mensaje se puede transmitir como un conjunto de datagramas que se vuelven a ensamblar en el mensaje en la ubicación receptora. Los campos de este datagrama IPV4 son los siguientes:



4	4	8	16	16	3	13
VERSION	HELN	Tipo de Servicio	Longitud total	Identificación	Señaladores	Compresión de fragamentos

8	8	16	32	32	var	
TTL	Protocolo	Encabezado suma de comprobación	Dirección IP origen	Dirección IP destino	Opciones IP	Datos...

Fig. 1.13 Datagrama IPV4.

- *VERS:* número de versión.
- *HLEN:* longitud del encabezado, en palabras de 32 bits.
- *Tipo de servicio:* cómo se debe administrar el datagrama.
- *Longitud total:* longitud total (encabezado + datos)
- *Identificación, Señaladores, Compensación de fragmentos:* suministra fragmentación de datagramas para permitir distintas MTU en la internetwork.
- *TTL:* Tiempo de existencia.

- *Protocolo:* protocolo de capa superior (Capa 4) que envía el datagrama.

- *Checksum del encabezado:* verificación de integridad del encabezado.

- *Dirección IP origen y dirección IP destino:* direcciones IP de 32 bits.
- *Opciones IP:* verificación de la red, depuración, seguridad y otras opciones.

El campo de protocolo determina el protocolo de Capa 4 que se transporta dentro de un datagrama IP. Aunque la mayoría del tráfico IP utiliza TCP, otros protocolos también pueden utilizar IP.

Cada encabezado IP debe identificar el protocolo de Capa 4 destino para el datagrama. Los protocolos de la capa de transporte se numeran, de forma similar a los números de puerto.

1.3.5.2. Datagrama del Protocolo IPV6.

Una dirección IPV6 es de 128 bits de longitud y su representación es diferente, números hexadecimales separados por dos puntos,

el concepto de máscara es similar y se ha implementado una jerarquía mucho más rica para disminuir los problemas de enrutamiento y direccionamiento. Por ejemplo, una dirección IPV6 válida es 3ffe:8070:100f:1:a00:20ff:fec6:ba27/64 que indica la región geográfica, la institución, subred y computadora de forma única en la red mundial experimental de IPV6.

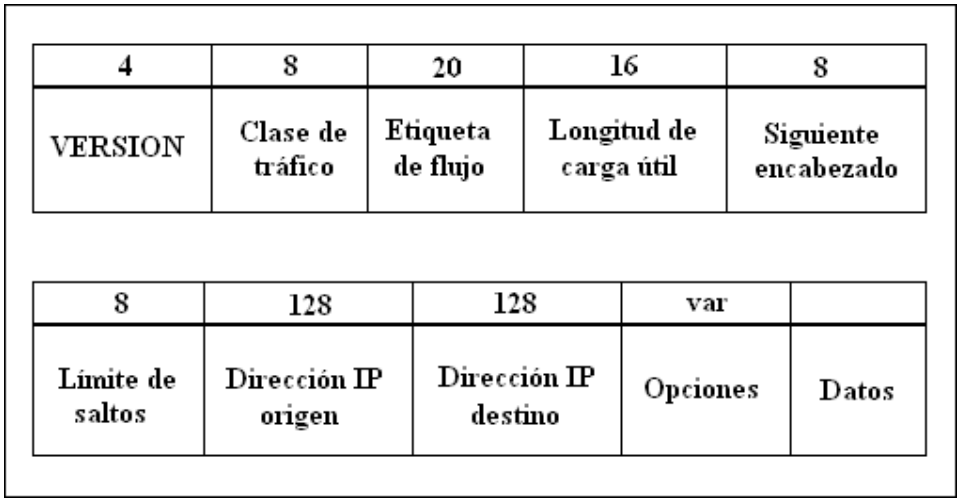


Fig. 1.14 Datagrama IPV6.

Existe un control universal por los organismos de Internet para la asignación de direcciones, de igual forma se está construyendo el direccionamiento para IPV6.

Los componentes del encabezado de IPV6 se muestran en la figura 1.14, la utilidad de los componentes se describe a continuación:

- Versión: Indica la versión, 6 para IPV6.

- Clase de tráfico: Campo de 8 bits para indicar los requerimientos de tráfico del paquete, similar a TOS de IPV4.

- Etiqueta de flujo: Campo de 20 bits, experimental.

- Longitud de carga útil: Campo de 16 bits que indica la longitud de la carga útil sin incluir el encabezado IPV6.

- Siguiente encabezado: Campo de 8 bits, para indicar el uso de cabeceras de extensión.

- Límite de saltos: Campo de 8 bits similares al TTL de IPV4.
- Dirección fuente y destino: Campos de 128 bits para las direcciones fuente y destino del paquete, respectivamente.

1.4. TCP Rate Control. (Control de Velocidad TCP)

1.4.1. Antecedentes.

El Protocolo de Transmisión de Control (TCP) proporciona servicios orientados a conexión para la capa de la aplicación de la serie protocolar, es decir, un cliente y un servidor deben establecer una conexión para intercambiar datos. TCP transmite datos en segmentos encapsulados en datagramas IP, junto con los checksums, usados para detectar datos corruptos, y números de secuencia para asegurar un flujo del byte ordenados. Se considera que TCP es un mecanismo de transporte fiable porque requiere a la computadora receptora para no sólo reconocer el recibo de datos sino también su integridad y sucesión. Si la computadora transmisora no recibe notificación de la computadora receptora dentro de un horario esperado, el remitente cronometra fuera y retransmite el segmento.

TCP usa un mecanismo de control de flujo de ventana deslizante para controlar el throughput de las redes de área ancha. Cuando el receptor reconoce el recibo inicial de datos, informa cuántos datos puede manejar, llamado tamaño de la ventana. El remitente puede transmitir paquetes múltiples, al tamaño de la ventana del destinatario, antes de que se detenga y espera por un

reconocimiento. El remitente llena el canal, espera por un reconocimiento, y llena el canal de nuevo.

Mientras el receptor típicamente maneja flujo de control TCP, el algoritmo del comienzo lento de TCP es un mecanismo de flujo de control manejado por el transmisor, diseñado para aprovecharse de capacidad de la red. Cuando una conexión se abre, sólo un paquete se envía hasta que un ACK se recibe. Para cada ACK recibido, el transmisor puede doblar el tamaño de la transmisión, dentro de los límites de la ventana del destinatario.

Los mecanismos que evitan la congestión de TCP intentan aliviar el problema de paquetes abundantes que llenan las colas de los routers. TCP incrementa la velocidad de la transmisión de una conexión usando el algoritmo del comienzo lento hasta que se da cuenta de un problema y entonces retrocede. Lo interpreta como paquetes perdidos y/o interrupciones como señales de congestión. La meta de TCP es para las conexiones individuales de expandirse demandando el uso de todo el ancho de banda disponible, mientras al mismo tiempo reacciona interviniendo en los problemas para aliviar la congestión.

1.4.2. TCP Rate Control.

El tráfico consiste en pedazos cortos y gruesos de datos que se acumulan en los enlaces de acceso donde la conversión de velocidad ocurre. Para eliminar los pedazos cortos y gruesos, TCP Rate Control controla el ritmo del flujo o lo allana descubriendo la velocidad de acceso de un usuario remoto, gestionando la latencia de la red, y correlacionando estos datos con otra información de flujo de tráfico.

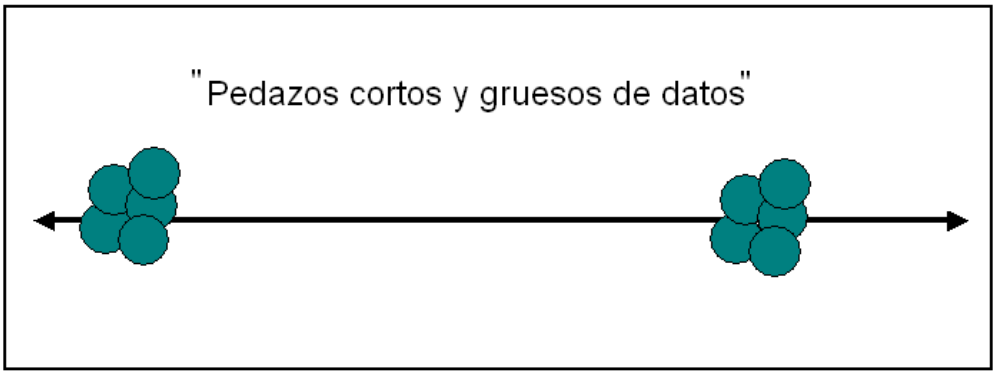


Fig.1.15 Tráfico sin Administrar

En lugar de colas de datos que pasan a través de la caja y midiendo la velocidad apropiada, Packeteer induce al remitente para enviar datos justo-a-tiempo. Cambiando los pedazos cortos y gruesos de tráfico, o extendidos, para óptimamente clasificarlos según tamaño y tiempo de los paquetes, Packeteer mejora eficacia de la red,

aumenta throughput, y entrega tiempos de respuesta más consistentes, predecibles, y puntuales.

TCP Rate Control utiliza tres métodos a controlar la velocidad de transmisiones:

- Detecta la velocidad del flujo en tiempo real.

- Mide los reconocimientos que regresan al transmisor.

- Modificas los tamaños de las ventanas de advertencia enviadas al transmisor.

Así como un router manipula la información de la cabecera de un paquete para influir en la dirección del paquete, Packeteer manipula la información de la cabecera de un paquete para influir en la velocidad del paquete.

TCP autobad es la tecnología de Packeteer, que permite descubrir la velocidad de conexión del cliente o servidor automáticamente al otro extremo de la conexión. Este mecanismo de descubrimiento de velocidad le permite a Packeteer adaptar estrategias de

administración de ancho de banda así como las condiciones variantes.

Packeteer incorpora un programa predictivo que anticipa el ancho de banda necesario y mide los ACKs y tamaño de la ventana de acordados. Usa autobaud, conociendo la conducta de TCP, y políticas de asignación de ancho de banda como criterio de predicción.

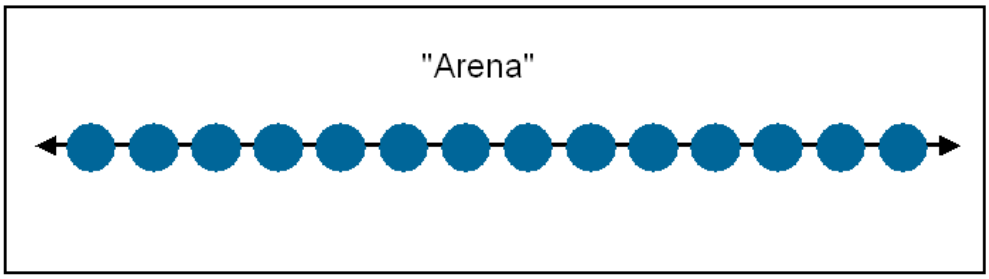


Fig. 1.16 Tráfico Administrado.

Packeteer cambia el significado end-to-end de TCP colocándose en la mitad de una conexión. Primero, usando autobaud, determina la velocidad de transferencia de una conexión para usar como una base para cronometrar transmisiones. Packeteer intercepta el reconocimiento de una transacción y la mantiene dentro él para la cantidad de tiempo que es requerida para aplanar el flujo de tráfico e incrementar el throughput sin incurrir en interrupciones de

retransición. También proporciona un tamaño de ventana que ayuda al transmisor a determinar cuándo enviar el próximo paquete y cuánto enviar para optimizar la velocidad de conexión en tiempo real.

Las transmisiones de paquetes uniformemente espaciados benefician significativamente el rendimiento de la red, evitando el prejuicio de la formación de colas de espera que obligan a los paquetes a acumularse y dando preferencia a los flujos de tráfico de bajo volumen. Como los paquetes acumulados son eliminados, la utilización de la red puede aumentar a 80 por ciento.

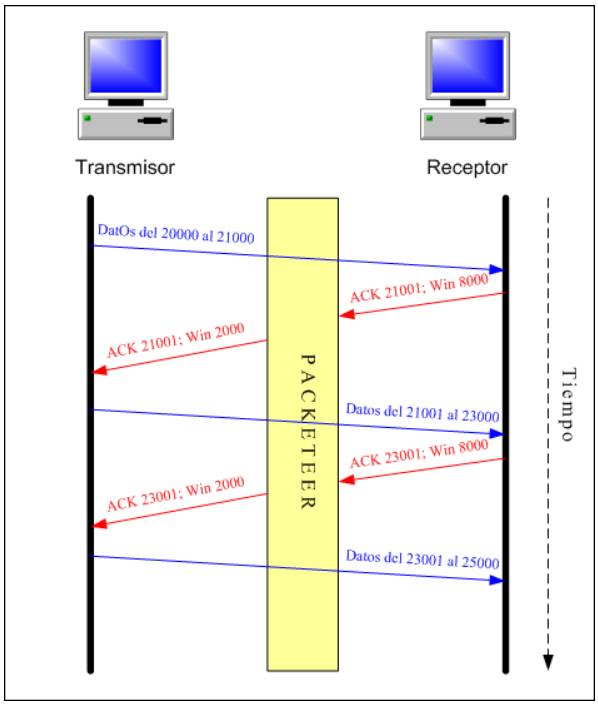


Fig. 1.17 Control de la conexión.

En este diagrama de paquetes, Packeteer interviene y controla la transmisión de los datos para entregar servicio predecible.

La secuencia descrita por el diagrama de paquetes incluye:

- Un segmento de datos es enviado al receptor.

- El receptor reconoce el dato y anuncia un tamaño de ventana de 8000 bytes.

- Packeteer intercepta el ACK y determina que el dato debe ser transmitido más lentamente. De otra forma, los segmentos de datos subsiguientes producirán colas de espera y los paquetes serán descartados por que el ancho de banda disponible es insuficiente. Además, los paquetes más pequeños y urgentes de las aplicaciones interactivas serían mantenidos detrás de estos datos más voluminosos.

- Packeteer revisa el ACK que va al transmisor, el cual inmediatamente emite los datos acordes al tamaño de la ventana acordado.

La figura 1.18 proporciona un ejemplo de los modelos de tráfico cuando se usan algoritmos de TCP naturales. Se puede ver que el segundo paquete debe transmitirse dos veces porque el transmisor no obtuvo respuesta en el tiempo que fue recibido, una pérdida innecesaria. Más abajo, se observa la expansión del paquete que ocurre. Esto es bastante típico del comienzo del crecimiento lento de TCP (pero grande después) y es lo que causa congestión y desbordamiento de buffer.

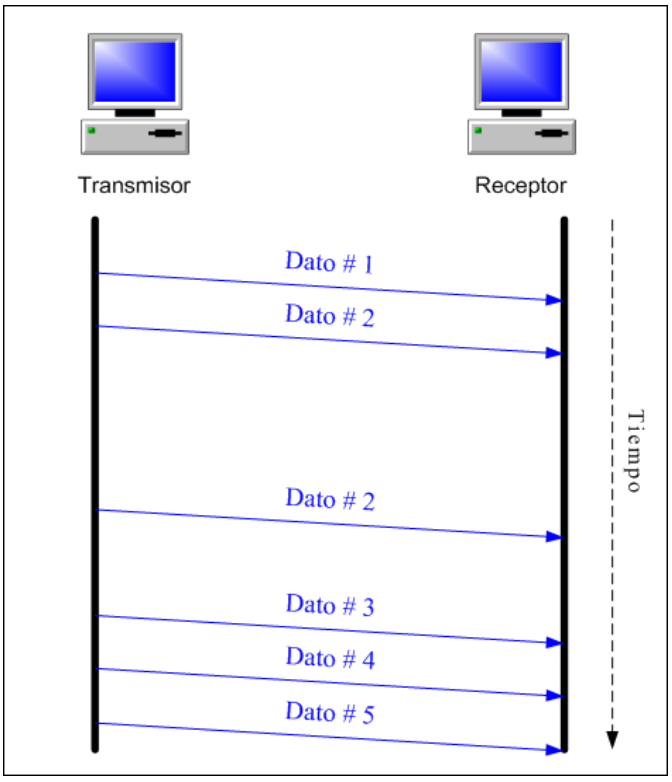


Fig. 1.18 Sin Packeteer.

La figura 1.19 proporciona un ejemplo de las transmisiones de los datos uniformemente espaciadas que ocurren cuando TCP Rate Control está activo. Este espacio nivelado no sólo reduce colas en los routers, también ayuda a incrementar el promedio de bits por segundo, y se aprovecha mejor el ancho de banda.

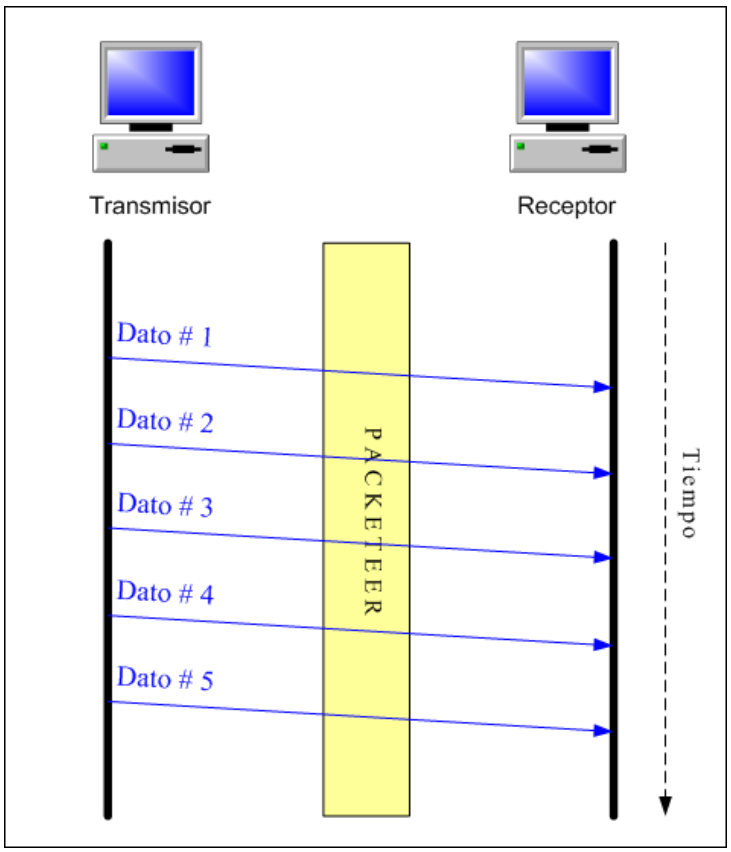


Fig. 1.19 Con Packeteer.

CAPÍTULO 2

ANTECEDENTES Y JUSTIFICACIÓN.

2.1 Ancho de banda en Internet.

El ancho de banda se asimila al diámetro de una tubería que sirve para canalizar el flujo de datos, es la capacidad de una línea para transmitir información. Pero hay que tener en cuenta que la línea está compartida frecuentemente por muchos usuarios. Por tanto nos sirve de muy poco saber el ancho de banda que tiene un proveedor, si no sabemos cuantos usuarios comparten esa línea en un momento determinado. Hay pequeños proveedores con pocos clientes que utilizan una línea "estrecha"; sin embargo pueden ofrecer mejores tiempos de acceso que otros proveedores con canales más potentes, porque éstos tienen demasiados usuarios compartiendo la línea. La proporción es lo que cuenta, no el tamaño en sí mismo.

2.1.1 Ancho de banda Teórico.

Es la velocidad de transmisión de datos, es decir, el flujo total de bits que puede enviar por segundo. En este valor se toma en cuenta toda la información que envía en cada sesión que realiza: bits de control, encabezados de transmisión y datos de usuario. Todos estos bits necesitan ser enviados en cada sesión para proveer la comunicación; los datos de usuario son una parte del flujo de datos.

2.1.2 Ancho de banda real o tasa efectiva.

Es la capacidad de transmisión de datos de usuario. Este valor muestra un valor aproximado del ancho de banda utilizado para transferir un archivo o datos entre un punto y otro y siempre es menor que el teórico.

WINDOWS presenta valores en Kbytes por segundo, así que si tiene una velocidad de 128Kbits por segundo probablemente observará valores menores o iguales a 16Kb/s en las pantallas que le muestra.

La siguiente relación es una muestra de un cálculo típico en una transferencia teórica.

Suponga que se va a transmitir un archivo de longitud 2,75Mbytes.

Implica entonces que tiene una longitud de:

2,75 Mbytes * 1024 Kbytes / 1 Mbyte * 1024 bytes / 1 Kbyte *
8 bits / byte * 1 Kbit / 1000 bits = 23068672 Kbits.

Conversión de Mega bytes a bits.

Esta es la cantidad total de datos de usuario a transferir. Ahora tenemos que considerar el Overhead que es la proporción de datos de control, encabezados, etc. que se adhieren a los datos de usuario. Su porcentaje depende del tamaño del archivo y conforme se aumenta el tamaño del archivo, el Overhead total tiende a ser constante. Si consideramos que para el ejemplo un 6%, implica que se transmiten 6% más de datos que los que se supone, por lo tanto el total de datos a transmitir será:

23068.672 Kbits * 1.06 = 24452.7923 Kbits

Cálculo considerando el Overhead.

Si se cuenta con un servicio de 128Kbps contratado, entonces el tiempo de transferencia será de aproximadamente:

24452.7923 Kbits / 128 Kbits por segundo = 191.0374 segundos = 3,1840 minutos.

Cálculo del tiempo de transferencia.

Este valor puede variar dependiendo de la ocupación de la red, pero usualmente debería estay muy próximo. Ahora si se tuviera un enlace de 256Kbps se tendría la mitad de este tiempo y así si se aumenta.

2.1.3 Velocidad de Transferencia óptima.

La velocidad de transferencia puede considerarse óptima cuando esta por encima del 75% de la velocidad máxima teórica, como se muestra en la tabla 2.1.

Ancho de banda teórico Kbits / seg.	Tasa de velocidad óptima Kbits / seg.	Tasa de velocidad óptima Kbytes / seg.
56	> 42	> 5,25
128	> 96	> 12
256	> 192	> 24
512	> 384	> 48
1.024	> 768	> 96
2.000	> 1.500	> 187,5

Tabla 2.1 Ancho de banda y tasa de velocidad.

2.1.4 La Suma del ancho de banda.

La suma del ancho de banda de todos los proveedores nacionales es mucho mayor que la capacidad de las líneas que conectan el país con el resto de Internet. Aunque el proveedor funcione correctamente y la velocidad del enlace no disminuya, no se puede contar con ello, porque el cuello de botella puede estar en otro sitio.

2.2 Problemas de los Proveedores de Servicios de Internet (ISPs)

2.2.1 Redes Frame Relay.

Las líneas utilizadas por los proveedores por lo general son del tipo Frame Relay. Esto significa que el ancho disponible no es siempre el mismo; de alguna manera la capacidad de la línea está compartida. El proveedor contrata un ancho máximo, por el que paga muy poco; también contrata un ancho o caudal mínimo garantizado conocido como CIR y por este concepto paga bastante más dinero. Estas líneas Frame Relay son gestionadas de la siguiente forma:

Cuando en todo el país hay pocos usuarios accediendo a Internet como por ejemplo a las cinco de la madrugada, cualquier proveedor podría utilizar todo el ancho máximo que tiene contratado, porque los otros proveedores no están utilizando masivamente el sistema; pero

precisamente por ser una hora inusual, ese proveedor también tendrá pocas necesidades, pocos clientes conectados.

Por el contrario, en las horas con más uso de Internet o horas pico todos los proveedores estarán reclamando el máximo de tráfico, por lo que la compañía canalizadora solo ofrecerá a cada proveedor su CIR o ancho mínimo garantizado. Así pues, resulta que este valor CIR es mucho más crucial que el ancho de banda máximo, que es el valor publicitado por el proveedor para aparentar más capacidad. Entonces, el factor crítico para elegir un proveedor es la relación entre el CIR y el número de conexiones simultáneas que tiene el proveedor en una hora pico.

La mayoría de los proveedores no informan a sus clientes los valores CIR contratados porque suelen avergonzarse de ellos; y no aumentan su CIR porque éste tiene un coste enorme. Tampoco informan el número de conexiones simultáneas disponibles o el número de internautas que tienen contratado el acceso.

2.2.2 Administración de Prioridades.

Ciertos servicios de uso regular, pero de menos prioridad o jerarquía, como correos con pesados anexos, largas colas de

impresión, tráfico para efectuar respaldos, transferencia de archivos de alta capacidad, Peer to Peer, sustraen el ancho de banda disponible y causan retraso y congestión en las redes provocando el colapso o inhabilitación de aplicaciones críticas, como Oracle, SAP, Citrix, VoIP, etc.

Usuarios efectuando compras o consultas en una organización deben recibir un tratamiento especial con una velocidad mayor y garantizada que el de otras personas que están tratando de bajar un demo o una canción, o simplemente navegando en sitios para adultos.

Las aplicaciones menos críticas o menos urgentes tienden a imponerse en la batalla por el canal de enlace o por los nodos congestionados de acceso WAN. A continuación se ilustra la competencia por el ancho de banda en la figura 2.1.

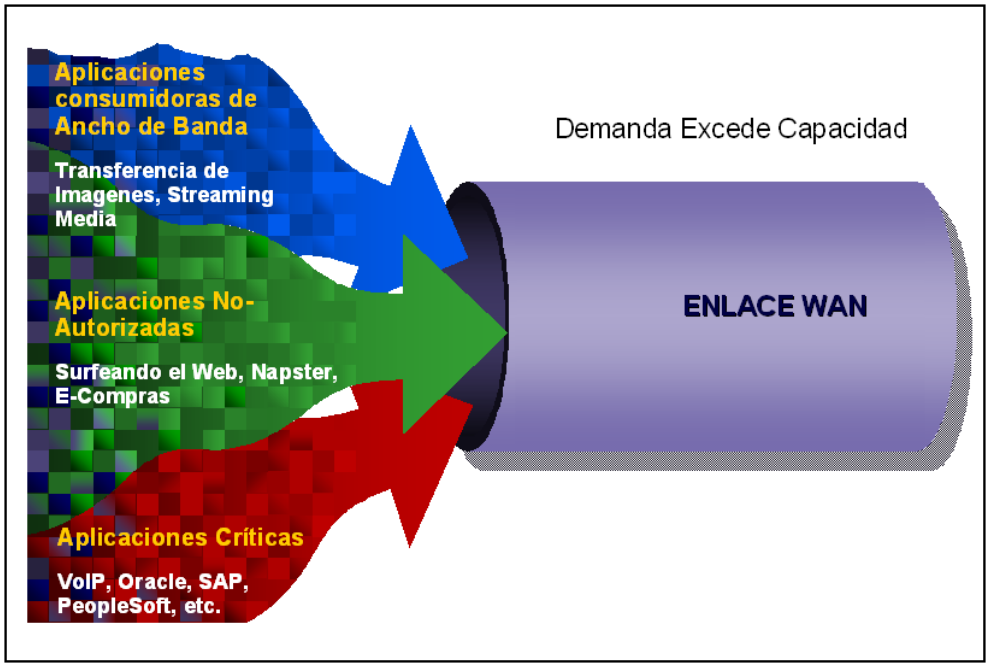


FIG. 2.1 Aplicaciones compiten por el ancho de banda.

2.2.3 Problema del Spam.

2.2.3.1 ¿En qué consiste el Problema del SPAM?

La mayor parte del spam que recibimos consiste en:

- Cadenas de mensajes.
- Esquemas piramidales, incluyendo las de marketing multinivel.
- Otros esquemas de "hágase rico fácilmente" o "gane plata rápidamente".

- Avisos de servicios y/o sitios pornográficos.

- Avisos de servicios de envío masivo de e-mails publicitarios

- Avisos de software y bases de datos para hacer spam.

- Ofertas de hosting, muchos de ellos toleran y/o hacen del spam su negocio.

- Avisos de acciones de empresas nuevas "que van a subir hasta el cielo".
- Productos milagrosos y remedios de muy dudoso efecto y origen.

- Software ilegal, películas y/o música pirateada.

2.2.3.2 Problemas que ocasiona el SPAM.

Enviar e-mails masivos es increíblemente barato. Con un modem de 28.000 bps y una conexión por teléfono un spammer puede enviar cientos de miles de mensajes por hora y mucho más con banda ancha. Sin embargo, cada persona que recibe su spam

debe pagar los costos relacionados, y los costos de los que recibe son mucho mayores de los que envía.

El problema es mucho mayor que el tiempo y esfuerzo de una persona borrando un par de e-mails. Hay muchos costos incurridos a lo largo del proceso de transmisión y entrega de cada e-mail.

Para un ISP o Proveedor de Servicios de Internet, su "tiempo" incluye la carga de procesador de sus servidores de e-mail, un recurso crítico para su operación. Cuando sus procesadores se ocupan de procesar spam, crean un atraso en el resto de los mensajes de la cola, sean éstos spam o no. También hay un problema con el filtrado de los mensajes: consume tremendas cantidades de tiempo de procesador y memoria y es la razón primaria por las cuales la mayoría de ISPs no pueden implementarlo como una estrategia para eliminar el spam.

El problema está ligado también al hecho de que muchos ISPs alquilan ancho de banda basándose en el uso proyectado por sus usuarios. Para muchos ISPs pequeños ó medianos, los costos del enlace están entre las porciones más grandes de su presupuesto. Sin el espacio que ocupa el correo basura, se podría dar mejor

servicio a más usuarios. Sin embargo, cuando un spammer comienza a consumirle canal, el ISP tiene pocas opciones:

- Dejar a sus Clientes con un servicio más lento.

- Hacerse cargo del costo extra de ancho de banda, que será igualmente consumido por más spam.

- Aumentar el costo que cobra por su servicio.

Con volúmenes como los que actualmente se manejan, es una terrible carga transferida a los ISPs guardar y procesar estas cantidades de información. Volúmenes que tiene que ver con los problemas de acceso, velocidad y confiabilidad que pueden darse hoy en muchos ISPs.

2.2.3.3 Problemas específicos que el SPAM produce en los ISP.

- Aumento del tráfico de correo y por ende mayor utilización de ancho de banda, lo cual afecta a los clientes por medio de un acceso más lento y obligaría al ISP a contratar más.

- Aumento de la utilización de recursos en plataforma de correos. Por ejemplo, del espacio en disco de los servidores de correo. Es un hecho el que las casillas de los clientes llegan a su cuota máxima, con material que en realidad no les interesa ni han solicitado, impidiendo que reciban más correos, que sí son de su interés.

- Aumento del encolamiento de correos, lo cual impacta en la capacidad de procesamiento, discos y memoria de servidores. En efecto, el congestionamiento en el envío y recepción de correo en servidores retrasa considerablemente el servicio para todos, lo que genera desconfianza respecto de la confiabilidad en el servicio.

- Aumento de conexiones concurrentes, lo cual impacta en la capacidad de procesamiento, memoria y ancho de banda.

- Bloqueo de direcciones IP por parte de organismos internacionales, tanto para los servicios del ISP como para los clientes, por medio de las llamadas "listas negras", lo que implica aumentar los esfuerzos de supervisión y operación. Por

ejemplo, los correos de clientes son bloqueados hacia otros sitios producto de las "listas negras".

- Aumento de los reclamos por Spam, lo cual impacta en el costo y operación del personal de Call Center, operaciones y/o soporte. Existe una suerte de desconfianza de los clientes respecto del mal uso de sus datos, piensan que el ISP distribuye/vende las bases de datos de usuarios, generando una mala imagen para el ISP.

- Obliga a pensar en invertir o implementar software de monitoreo y control de Spam.

- Impone la necesidad de hacer desarrollos adicionales para obtener información histórica del uso de servicios de correo, tratando de determinar fuentes de Spam frecuentes, comportamiento anómalo de usuarios, entre otros estudios.

2.3 Naturaleza del Tráfico de Red.

El estándar de red es el conjunto de protocolos TCP/IP, y arriba del 80% de tráfico TCP/IP es TCP. Aunque TCP ofrece muchas ventajas y fuerzas, la administración y la calidad de servicio no está en medio de

ellos. TCP tiene sus propios mecanismos de control que contribuyen a los siguientes problemas de funcionamiento:

- TCP retransmite cuando la nube de red deja caer los paquetes o tarda los reconocimientos. Cuando los paquetes se caen o se tardan los conocimientos debido a las condiciones de congestionamiento y sobreflujo en la cola del ruteador, las retransmisiones contribuyen más al tráfico y empeoran el problema original.

- TCP incrementa el ancho de banda exponencialmente. Con el algoritmo salida lento de TCP, los remitentes pueden iterativamente doblar el tamaño de la transmisión hasta que los paquetes se pierden y ocurren problemas. El algoritmo introduce una tasa de crecimiento exponencial y puede rápidamente dominar la capacidad. Sin considerar la urgencia del tráfico, los usuarios concurrentes o compitiendo por las aplicaciones, simplemente hacen a TCP extender el uso de cada flujo hasta que causa problemas. Esto convierte a cada flujo de tráfico regular en un consumidor hambriento de ancho de banda, potencialmente destructivo que podría recortar justas asignaciones o apropiarse de los recursos de la red.

- TCP impone sobrecarga en la red. Extiende las asignaciones hasta que se caen los paquetes o se tardan las contestaciones. Inunda los routers designados.

Grandes cantidades de datos se envían a los routers, más congestión se forma, la forma de las colas es más grande, más retraso se produce, más paquetes son descartados, más interrupciones ocurren, más retransmisiones se envían, más congestión se forma, y la espiral cíclica continúa.

Cuando se presentan los picos en la demanda y se pierden los paquetes, todo el tráfico experimenta los retrasos, sea grande o pequeño, interactivo o lote, urgente o secundario. Pero son las aplicaciones críticas o urgentes las más afectadas. Los usuarios se vuelven locos. La productividad se deteriora y se dan los declives comerciales.

2.4 Características del Tráfico.

La administración de la asignación del ancho de banda para la diversidad del tráfico actual es un desafío definido. El tráfico de red y las aplicaciones no comparten las mismas características o requisitos. No se tiene el mismo funcionamiento para los distintos tipos de tráfico. Por

consiguiente antes de elegir una estrategia de control, se debe caracterizar el tráfico.

Primero, se considera si la preocupación primaria es el funcionamiento de la aplicación o la carga de tráfico. Típicamente si nos preocupamos por los clientes o los empleados productivos, entonces nos preocupamos por el funcionamiento de la aplicación.

Pero si se proporciona el ancho de banda a usuarios u organizaciones y no se involucra las aplicaciones que corren, entonces nos preocupamos por la capacidad y volumen de tráfico. A continuación se presentan ejemplos en la tabla 2.2.

Ejemplos donde el funcionamiento es principal.	**Ejemplos donde la carga es principal.**
Una empresa que proporciona las aplicaciones para proveer al personal.	Un proveedor de servicios que ofrece cantidades acortadas de ancho de banda a negocios.
Un proveedor de servicio que ofrece administrar las aplicaciones a subscriptores.	Una universidad que provee a cada departamento de un justo ancho de banda.

Tabla 2.2 Características del tráfico.

Para cada tipo de tráfico que se desee manejar, considere el comportamiento de acuerdo a cuatro características: la importancia, la sensibilidad de tiempo, el tamaño y las fluctuaciones.

Importancia.

Algunas veces una misma aplicación es crucial para la función en una organización, e irritante en otra red.

En la tabla a continuación se citan ejemplos.

Importante	No Importante
SAP en un negocio industrial.	Juegos en un contexto de negocio.
PeopleSoft como soporte organizacional.	Real Audio en un negocio no-relacionado.
E_mail en los negocios.	Mensajería Instantánea en el aula.

Tabla 2.3 Clasificación por importancia

Sensibilidad al Tiempo.

Algunos tipos de tráfico, aunque son importantes, no son particularmente sensibles al tiempo. Por ejemplo, para la mayoría de las organizaciones, el tráfico de impresión es importante para los negocios.

Pero los empleados y la productividad probablemente no se impactarán sí un trabajo de impresión tarda unos pocos segundos. En contraste, cualquier aplicación crítica que parte de un usuario gerencial, de entrar en espera por una respuesta, es definitivamente tiempo sensible.

En la tabla a continuación se dan ejemplos de tráfico sensible y no sensible al tiempo.

Sensible al tiempo	No Sensible al Tiempo
Telnet.	Impresión.
Citrix.	Transferencia de archivos.
Oracle	Correo.

Tabla 2.4 Clasificación por sensibilidad.

Para el tráfico importante y sensible al tiempo se debe considerar una política de alta prioridad para flujos pequeños o en una política de velocidad para otros flujos. Se debe considerar una partición con un tamaño mínimo.

Tamaño.

Una sesión de tráfico que tiende a expandirse usando grandes cantidades de ancho de banda y producir grandes olas de paquetes, se denomina “bursty”. TCP por medio de su algoritmo lento – comienzo, crea tráfico bursty. Como TCP se esfuerza por dirigir la súbita demanda de una conexión expandible, entonces se presenta congestión y retransmisiones.

Las aplicaciones como FTP, componentes multimedia de tráfico HTTP, impresiones y descargas de música son consideradas como bursty, debido a que ellos generan grandes transmisiones de datos.

Las expectativas de los usuarios por este tráfico dependen del contexto. Por ejemplo, si un gran archivo multimedia está descargándose para usarse después, el usuario no requiere de una velocidad tan alta, como para sostener el progreso y tener la convicción que la descarga no tiene que ser reiniciada.

GRANDE Y BURSTY	PEQUEÑO Y BURSTY
Descargas de músicas.	Telnet.
Correo con archivos adjuntos.	ICMP.
Impresiones.	TN3270

Tabla 2.5 Clasificación por tamaño.

Para tráfico grande y expandible, considere una partición con un límite. Si el tráfico expandible es importante, considere una partición con un tamaño mínimo y con un tamaño máximo. Considere una política de proporción con un límite por sesión, si usted está involucrado con un usuario de alta capacidad, puede impactar a otros usando la misma aplicación. Considere una política de baja o mediana prioridad dependiendo de la importancia.

Para un flujo pequeño no expandible, considere una política de prioridad alta, si el flujo pequeño es importante.

JITTER.

Jitter o variación del retardo en un periodo de tiempo, tiene impacto negativo para aplicaciones de audio y video como VoIP, Windows Media o Real Audio.

JITTER	SIN JITTER
VoIP.	Core.
Windows Media.	Impresión.
Real Audio.	MS SQL.

Tabla 2.6 Clasificación según el jitter.

Para tráfico propenso a fluctuaciones, sobre todo si es importante, considere una política de proporción con una garantía por sesión. Si demasiados usuarios pudiesen inundar un servicio, use una partición con un límite y características de control de admisión.

2.5 Justificación del Proyecto.

Los proveedores de servicio de Internet y los proveedores de servicio de red, deben ser suficientemente ágiles para crear servicios innovadores, ofrecer distintos niveles de servicio, manejar los modelos de tráfico agresivos de hoy y la influencia de los usuarios, control de costos, e incremento de beneficios.

Los siguientes problemas son muy familiares:

- Algunos clientes exceden sus cantidades contratadas de ancho de banda, impactando de forma negativa a otros.

- Las intenciones de ofrecer un buen nivel de servicio no siempre se dan realmente.

- Los clientes que alquilan se quejan que no están obteniendo suficiente ancho de banda individual, aunque el total del cliente es correcto.

- Los clientes se quejan por la lentitud del funcionamiento multimedia de forma intermitente.

En el estudio que hemos realizado en ciertas empresas, se opta por agregar la cantidad contratada de ancho de banda, o realizan una inversión hacia las tecnologías de fibra óptica, aumentando la capacidad del flujo de tráfico. Pero el problema solo se soluciona en forma parcial, debido al desconocimiento del tráfico que circulando por sus enlaces de Internet. La mayor parte del tráfico es del tipo recreacional y no es controlable, es el responsable de los problemas de la congestión del enlace.

Se ve la necesidad de realizar un estudio que ofrezca a los proveedores de Internet la habilidad para entregar alta calidad de servicio, solucionando problemas comunes de contrato de ancho de banda como

los mencionados arriba, y creando obligados servicios diferenciados. En el capitulo tres se realiza un estudio de los administradores de ancho de banda que se encuentran en el mercado, para seleccionar uno que ayude a dar un servicio dispuesto en niveles, asigne mínimos del ancho de banda y máximos en por cliente, por usuario, por aplicación, o otra base.

CAPÍTULO 3

SOFTWARE ADMINISTRADOR DE ANCHO DE BANDA DE LAS REDES.

Los Equipos que administran el ancho de banda son necesarios para tener una red mas descongestionada y aprovechando al máximo toda su infraestructura. La principal aplicación de alguno de ellos es controlar los enlaces innecesarios que ocupan mucha capacidad, a continuación hacemos un breve estudio y sus principales características.

3.1 Bandwidth Manager BM-2100 - 100Mbps.

Aplicaciones críticas de negocios tales como VoIP o procesos transaccionales necesitan un ancho de banda específico garantizado. El nuevo BM-2100 de 100Mbps de Planet ofrece a los administradores de red un medio fácil y poderoso de asignar los recursos de la red basados en las prioridades de la empresa, además de ordenar, analizar y

controlar el uso de ancho de banda. Los costosos recursos de la red WAN se utilizan con más eficacia, evitando la necesidad de mejoras costosas y sin dejar de satisfacer las prioridades de cada negocio. El BM-2100 de Planet es fácil de instalar, con dos puertos Ethernet de 10/100Mbps para conectar respectivamente a la red local y al router WAN. Un panel LCD de 16x2 caracteres hace fácil y más eficiente la instalación y el mantenimiento.

Fig. 3.1 Bandwidth Manager -2100 - 100Mbps.

Para la gerencia del ancho de banda, los paquetes se pueden clasificar basándose en Subnet de direcciones IP y el número de acceso de TCP/UDP. El dispositivo tiene más de 20 de los protocolos más comunes tales como H.323, ORACLE, HTTP, TFP, etc. Para la facilidad de la definición; el administrador puede entonces definir políticas para asegurar los niveles confiados y máximos del ancho de banda para el

tráfico de entrada / salida en cada clase. El administrador puede también definir tres niveles de prioridad para que cada política se asegure que los paquetes de la alta prioridad reciben el máximo ancho de banda disponible. Además, cada política puede tener un horario definido para cuando la política se activa o se hace inactivo.

El BM-2010 también permite a administradores medir con eficacia tráfico en la red y proporcionar informes gráficos comprensivos sobre cómo se está utilizando el ancho de banda. El administrador puede ver cada tráfico de entrada y de salida internamente del host o el tráfico de entrada y de salida de cada servicio de red. También proporciona un informe gráfico para los diez host internos superiores o los servicios que generan tráfico. Una utilidad libre, es el analizador del ancho de banda, también se proporciona para ayudar a hacer el análisis adicional del uso. Para el acceso interrumpido del Internet, el BM-2010 también proporciona una función para mantener el servicio del Internet disponible.

3.1.1 Funcionamiento del Bandwidth Manager BM-2100 100Mbps.

Una red de la compañía puede contener muchas clases de tráfico. Se puede bloquear tráfico menos urgente que consume el ancho de banda de la red WAN.

Sin embargo, los usos no críticos tales como Gnutella pueden colapsar los enlaces WAN limitados e interrumpir el tráfico de VoIP.

Desplegando un controlador de ancho de banda, el administrador de la red puede asignar el ancho de banda basado en las prioridades del negocio dando el ancho de banda garantizado para el tráfico de VoIP y para Oracle una prioridad más alta.

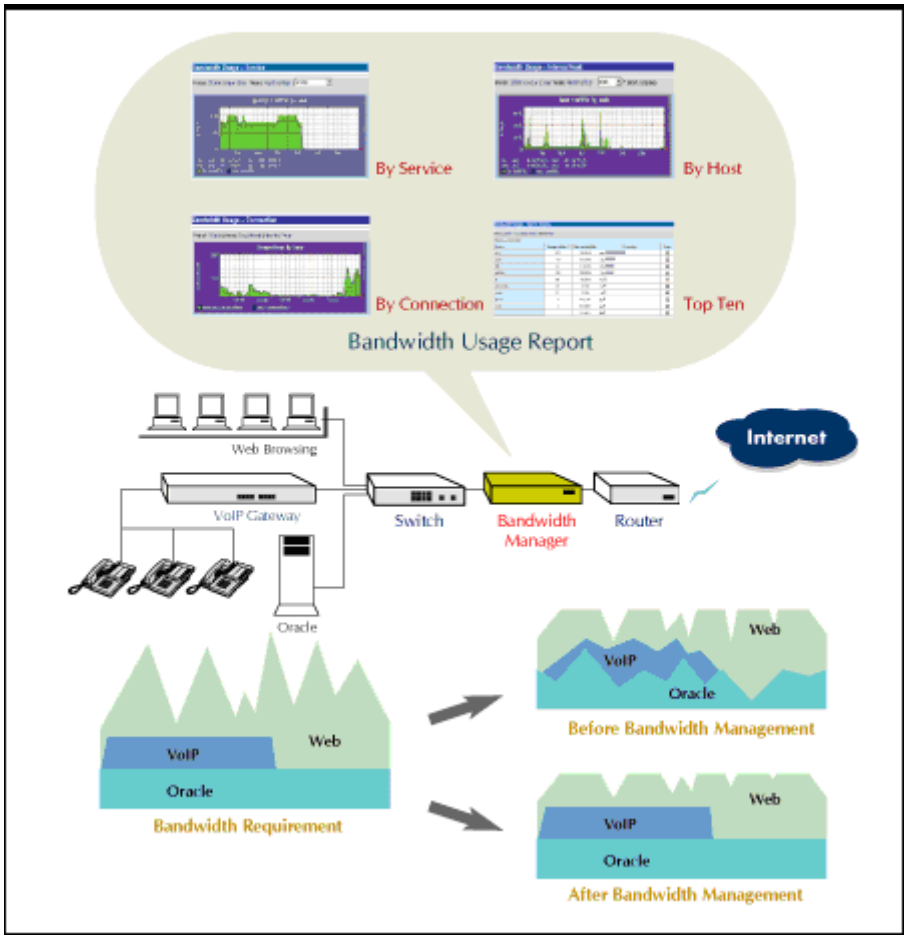


Fig. 3.2 Bandwidth Manager BM-2100 - 100Mbps

3.1.2 Beneficios del BM-2100-100Mbps Bandwidth Manager

Garantizar un ancho de banda para aplicaciones de negocios críticas y sensibles al tiempo como VoIP. Ofrecer a los administradores de red un medio fácil y poderoso para colocar los recursos de la red basados en prioridades de negocios además de, analizar y controlar el ancho de banda usado. Evitar la necesidad de costosas actualizaciones cuando todavía cumple con las prioridades de negocios.

3.2 PacketShaper.

PacketShaper es capaz de organizar el tráfico existente en nuestra red y dar un alto rendimiento a las aplicaciones que lo necesiten. Permite bloquear tráfico en la red para que aplicaciones de uso no comercial como Kazaa, Gnutella o mensajerías instantáneas no sean utilizadas y perjudiquen el ancho de banda de las aplicaciones de producción.

Los modelos 9500 y 10000 de PacketShaper® permiten incorporar el software PacketWise ISP de Packeteer para proporcionar a los proveedores de servicio soluciones vitales de suministro y gestión de ancho de banda IP. PacketShaper / ISP permite a los proveedores de servicio de Internet (ISPs) administrar el recurso más codiciado por sus suscriptores, el ancho de banda. Desde el acceso a Internet hasta las redes privadas virtuales (VPNs), desde el alojamiento de sitios Web

hasta los edificios inteligentes, PacketShaper y su software especial para ISPs proporcionan un rendimiento fiable y eficiente a lo largo de una amplia gama de servicios. Es la respuesta a las peticiones de proveedores de servicio de una solución de alta capacidad que dé servicios diferenciados, asegure un acceso justo y equitativo, haga respetar las políticas de usuario y mejore los márgenes derivados de diversos servicios de ubicación compartida.

3.2.1 Optimización del rendimiento de las aplicaciones con los objetivos de negocio.

El enfoque en cuatro pasos de PacketShaper para optimizar el rendimiento de las aplicaciones permite controlar los nodos congestionados de la red de área extendida (WAN) y de acceso a Internet.

Clasificación del tráfico.

PacketShaper clasifica automáticamente el tráfico de red en categorías, basándose en criterios de aplicación, protocolo, subred, URL y otro, lo que proporciona, en potencia, miles de categorías. PacketShaper va más allá de los esquemas estáticos de correspondencia de número de puerto y de dirección IP. Su clasificación en Nivel 7 identifica cientos de aplicaciones, desde Oracle y SAP hasta Gnutella y Kazaa.

Análisis del tráfico de la red.

PacketShaper recopila más de 60 métricas por cada tipo de tráfico, a fin de proporcionar un análisis detallado de la utilización de la red, del rendimiento de aplicaciones y de la eficiencia de la red. Un diagnóstico con detenimiento revela la fuente de problemas complejos de rendimiento.

Control del tráfico de la red.

PacketShaper protege y acelera las aplicaciones críticas gracias a la asignación del ancho de banda, el control del tráfico y la aceleración de éste mediante políticas predeterminadas. Así, pueden especificarse mínimos y máximos para proteger las aplicaciones críticas, prohibir el tráfico no autorizado y contener a aplicaciones que desbordan los recursos sin ser urgentes. Distribuye la capacidad dinámicamente por aplicación, usuario o cliente.

Informes del tráfico de red.

PacketShaper ofrece una gran variedad de información: gráficas y estadísticas vía protocolo simple de gestión de red (SNMP) y XML. Gracias a los compromisos sobre el nivel de servicio (SLAs), pueden definirse los estándares de rendimiento, comparar el rendimiento actual con los objetivos de nivel de servicio y generar informes sobre el cumplimiento de dichos objetivos.

3.2.2 Transmisión fiable de aplicaciones críticas a través de Internet y de la Red de Área Extendida (WAN)

PacketShaper es un sistema versátil de gestión del tráfico de aplicaciones. Puede ser adaptado para encajar en las necesidades específicas de una organización por medio de características de supervisión que identifican y analizan el rendimiento, la capacidad de conformación de tráfico para asignar los recursos una vez se ha llevado a cabo una valoración del comportamiento de la red, y de una función de aceleración que permite mejorar el rendimiento.

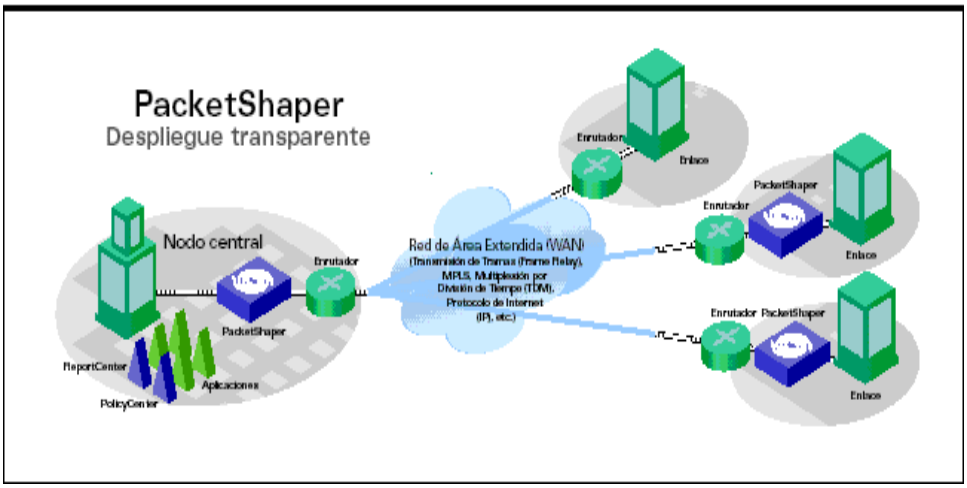


Fig.3.3. Despliegue transparente.

Por todas estas características PacketShaper es el equipo escogido y analizado en el siguiente capítulo.

3.3 QoSWorks.

QoSWorks de Sitara Networks es una herramienta para enfrentar problemas de congestionamiento en las redes. Es un equipo con un software, que puede administrar 45 Mbps de ancho de banda, es una solución de administración apropiada para corporativos.

3.3.1 Solución QoS completa y escalable

Permite a los administradores establecer políticas para priorizar cualquier tipo de tráfico, IP o no IP, en la red; además es escalable para soportar redes de hasta 100 Mbps.

3.3.2 Sistema de administración de políticas intuitivo y flexible.

Combina una variedad de herramientas sin precedentes con manejo de políticas basadas en grupos jerárquicos para administrar el tráfico desde niveles agregados hasta flujos individuales.

3.3.3 Facilidad de Manejo.

QoSWorks ofrece administración remota de dispositivos individuales utilizando interfaces estándar.

3.3.4 Refuerza políticas empresariales con una retroalimentación continua de información.

Proporciona clasificación wire-speed de todo el tráfico que recorre la WAN y políticas que controlan simultáneamente el ancho de banda para cada aplicación, usuario ó grupo. Reportes específicos proporcionan una vista instantánea sobre la eficacia de las políticas y automáticamente lanzan alarmas si estas son necesarias.

3.3.5 Instalación transparente

Diseñado para un alto grado de automatismo, sin intervención de operadores y a prueba de fallos en la red, QoSWorks elimina la necesidad de reconfigurar la infraestructura existente de equipos o la instalación y sincronización de dispositivos secundarios.

3.3.6 Características de QoSWorks.

QoSWorks es el primer dispositivo de red QoS altamente escalable que integra todos los mecanismos necesarios para manejar el amplio rango de tráfico con la mayor eficacia a cualquier velocidad, incluyendo:

- Administrador de Tráfico Sitara AccuRate que combina y coordina múltiples mecanismos de gestión de tráfico QoS.

- Política inteligente de Web caching.

- Clasificación wire speed.

- Aplicaciones QoS específicas.

- Administración intuitiva y flexible de políticas.

- Monitorización y obtención de informes en tiempo real.

3.3.6.1 Política inteligente de Web caching.

Además de integrar y coordinar múltiples mecanismos de administración de red con AccuRate, QoSWorks incorpora su propia caché, crítico para controlar y administrar tráfico HTTP Web que demandan gran ancho de banda que podrían comprometer aplicaciones críticas o sensibles a los tiempos de recuperación de datos.

La caché QoSWorks almacena las páginas Web que se acceden más frecuentemente en una caché local, evitando así el tener usuarios navegando por la WAN para obtener las mismas páginas una y otra vez. El uso no solo reduce el tráfico sobre la WAN, sino que también mejora los tiempos de respuesta para los usuarios finales.

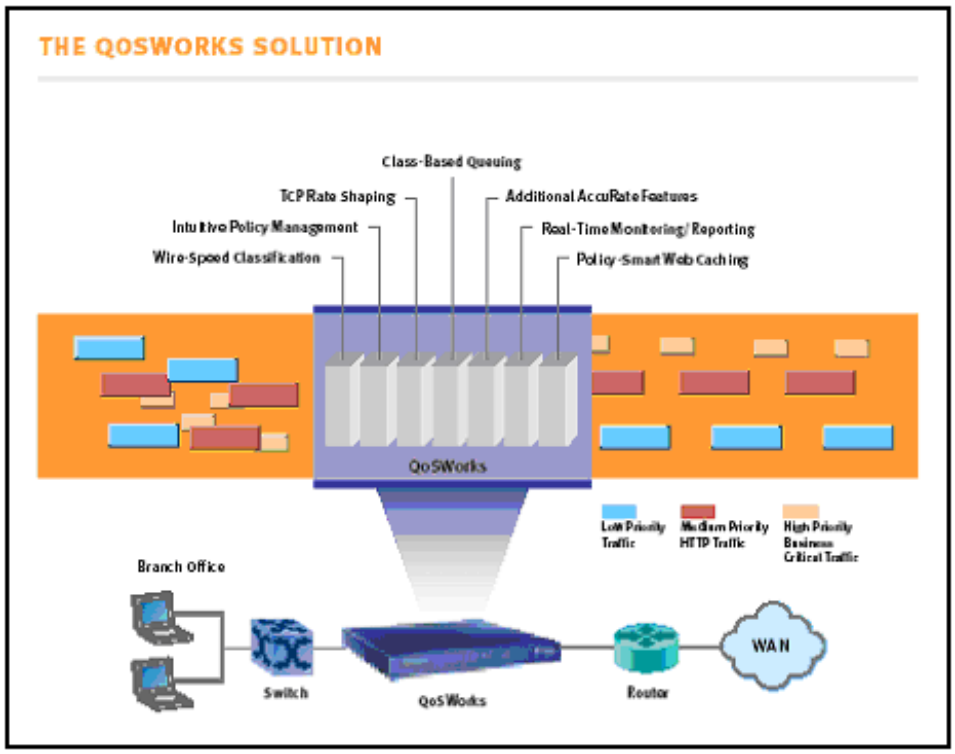


Fig.3.4 La solución QoSWorks.

A diferencia de una caché independiente y un administrador de tráfico, donde cada dispositivo tiene su propio clasificador y requiere que cada paquete sea procesado dos veces, la caché Web integrada de Sitara no requiere la reconfiguración de routers, navegadores o la instalación de un switch de 4 Capas para redirigir peticiones a la caché.

La caché integrada QoSWorks' utiliza "Política Inteligente". Esto permite al administrador:

- Habilitar o deshabilitar el uso de la caché sobre la base de una política determinada.

- Crear políticas que controlen la renovación de peticiones o prebúsquedas de tal modo que estas funciones no puedan poner en peligro el rendimiento de aplicaciones críticas.

3.3.6.2 Aplicación específica QoS.

La arquitectura QoSWorks proporciona genuina QoS específica a las aplicaciones superiores a una simple clasificación. Utilizando una técnica llamada Proxy transparente, el tráfico es identificado transparentemente, interceptado y redirigido a Proxies especializados. Por ejemplo, con caché HTTP, la conexión debe finalizarse, la petición HTTP debe procesarse para determinar si la información está disponible en la caché, y una nueva conexión establecerse cuando sea requerida hacia el servidor de origen.

QoSWorks es el primer dispositivo de red QoS altamente escalable que integra todos los mecanismos QoS necesarios para manejar el amplio rango de tráfico con la mayor eficiencia a cualquier velocidad. En el pasado, empresas que consideraban que una solución QoS tenía que instalar múltiples dispositivos de red en las oficinas satélites y en las sucursales. Debido al alto

costo asociado en la instalación de múltiples dispositivos a lo largo de múltiples ubicaciones, compañías y proveedores de servicios, encontraban difícil justificar un QoS. QoSWorks proporciona una solución de fácil administración que elimina la necesidad de tratar con múltiples políticas en múltiples dispositivos que serían necesarias en una política end-to-end.

3.3.6.3 Clasificación Wire-speed.

Cuando QoSWorks es instalado sobre la red, inmediatamente comienza a monitorizar los flujos de tráfico activo y desarrolla rápidamente una clasificación tanto de tráfico IP como no IP. Esto proceso de auto-descubrimiento funciona “escuchando” las conversaciones existentes como los flujos de tráfico sobre la red e identificando los diferentes tipos de tráfico, como el tráfico WEB (HTTP y FTP), e-mail y aplicaciones ERP. Las aplicaciones y usuarios están clasificados por varios parámetros, incluyendo:

- Direcciones IP fuente y de destino
- Protocolo de red
- Puerto de red
- Sub-Red

Para proporcionar una solución end-to-end, QoSWorks utiliza señalización de paquetes DiffServ a través de la configuración de bit TOS, Precedencia IP, para cada política. QoSWorks está también diseñado para proporcionar la clasificación de la capa 2 a la 7.

3.3.6.4 Política de administración flexible e intuitiva.

QoSWorks simplifica dramáticamente la configuración de políticas con su interfaz intuitiva y un conjunto de filtros predefinidos que permiten a los administradores de red establecer políticas sofisticadas, sin embargo efectivas en menos de 15 minutos. QoSWorks también proporciona una alta modularidad en la administración para políticas de afinamiento que se correspondan con las necesidades del negocio. QoSWorks utiliza un sistema jerárquico basado en grupos que permite a los administradores de red dividir un enlace físico en un número anidado de enlaces virtuales lógicos que acotan el diseño lógico de la red.

Para cada aplicación y/o usuario / grupo de usuarios los siguientes parámetros están especificados en el enlace virtual:

- Ancho de banda mínimo garantizado.

- Ancho de banda máximo para ráfagas.

- Configuración de 5 prioridades.

- Ancho de banda de la sesión, Kbps por flujo, utilizado para el control de admisión.

- Control de Admisión (disminución, caída, negación).

- Caché (habilitada / deshabilitada).

- Alarmas sobre umbrales de rendimiento (alto y bajo).

QoSWorks habilita simultáneamente el control de ancho de banda y prioridades para cada grupo aplicado a todos los tipos de tráfico incluyendo tráfico TCP/IP y UDP y tráfico no IP como IPX y AppleTalk. Cualquier ancho de banda asignado y no utilizado puede ser compartido dentro del grupo basándose en las prioridades. El programador integrado QoSWorks almacena múltiples políticas que pueden ser ejecutados automáticamente en varios momentos del día.

3.3.6.5 Configuración de política jerárquica.

El control modular y la flexibilidad están proporcionados por el conjunto de políticas de grupo jerárquicas, QoSWorks puede ser instalado en oficinas centrales, oficinas remotas o ambas. En este

ejemplo, en las oficinas centrales QoSWorks se utiliza para controlar enlaces individuales, mientras que en las oficinas remotas se utiliza para controlar usuarios y aplicaciones.

Plataforma estándar.

QoSWorks está basada en software y hardware estándar para la industria, facilitando de este modo el rápido desarrollo de nuevas y robustas características. La protección de la inversión está proporcionada a través de opciones instalables por el usuario y por actualizaciones para mejorar el rendimiento.

3.3.6.6 Beneficios del QoSWorks

Hay numerosas ventajas en un dispositivo con una solución QoS integrada, incluyendo:

Compacto

Un dispositivo pequeño es especialmente crítico en oficinas donde el espacio es siempre un premio.

Económico

Las soluciones de extremo pueden llegar a ser costosas porque siempre surgen nuevas conexiones remotas, es significativamente

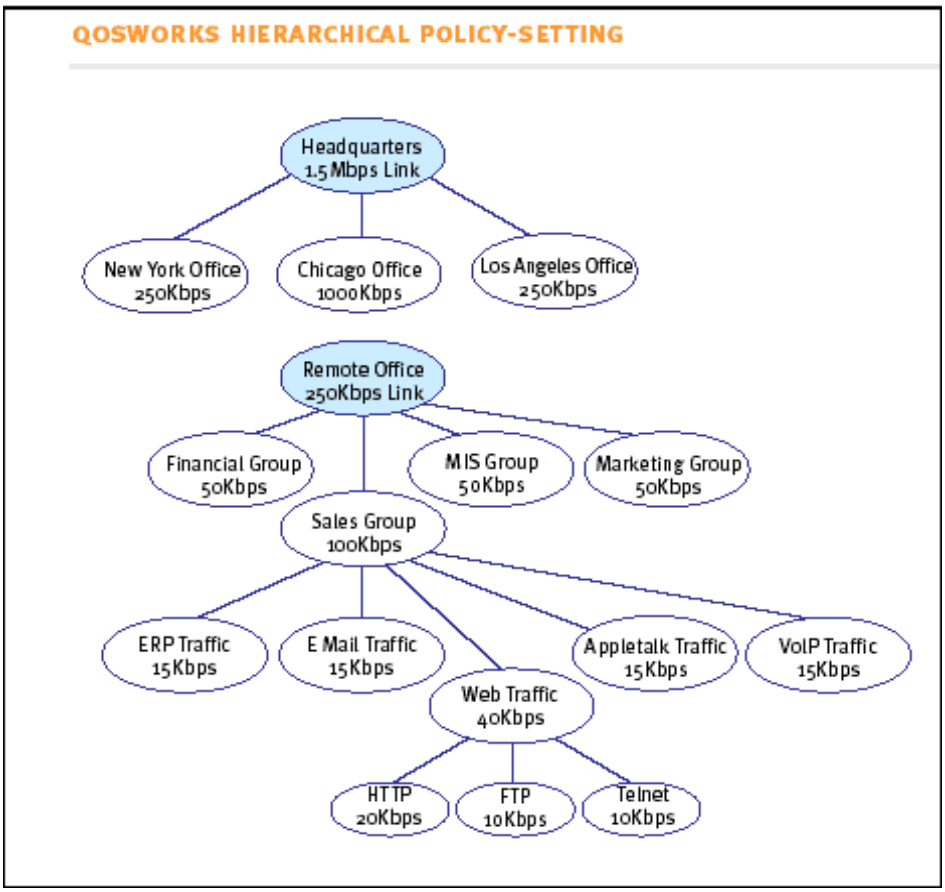


Fig.3.5. Ajuste jerárquico de las políticas

económico comprar un solo equipo para cada emplazamiento que comprar varios.

Mejor solución optimizada

El encadenamiento de múltiples dispositivos QoS de propósito específico provoca el incremento de latencia en la conexión al exigir a los paquetes atravesar la pila de protocolos al menos una vez en cada dispositivo. El rendimiento de la red será también

optimizado aplicando simplemente la tecnología adecuada a cada problema, por ejemplo, siendo capaz de modelar el tráfico que necesita cruzar la WAN y utilizando una caché para el tráfico que puede ser servido de modo local.

Proporciona garantías de rendimiento para el tráfico crítico

QosWorks permite a los administradores de red establecer razones de transferencia y tiempos de respuesta para aplicaciones críticas para el negocio. También permite a los administradores de red determinar el rendimiento de la portadora contra el Service Level Agreements (SLAs).

Requerimientos de integración única de QoS.

Normalmente, una solución integrada significa simplemente que el vendedor ha cogido varios dispositivos, los ha integrado en un único chip, tarjeta o software, y los ha instalado en una carcasa o chasis. Esto proporciona todos los beneficios añadidos de reducción de costos, simplicidad de manejo y mantenimiento, etc., como se describe más arriba. Pero en el caso de una integración QoS, no es simplemente la integración física de diferentes funciones en un único chasis (lo que es clave), sino también la coordinación lógica de las distintas funciones. Tomemos la relación entre la caché y la modelación de tráfico como ejemplo.

Con el uso de la caché eliminamos tráfico de la WAN y con la modelación de tráfico administramos mejor el tráfico que debe fluir sobre la WAN.

3.4. BWMETER 2.3.0

BWMeter se instala cómodamente en la bandeja de sistema del PC controlando todo el tráfico de entrada y salida de tu sistema, tanto en Internet como en red local (LAN), en caso de que se tenga.

Es capaz de analizar los paquetes de datos y determinar detalles como su procedencia, su destino o qué puerto y protocolo usan. También permite usar filtros para distinguir diversos tipos de tráfico lo que permite saber cuántos datos hay descargados de ciertas páginas o servidores.

El programa muestra el resultado de sus controles en forma numérica y gráfica, y puede también generar estadísticas diarias, semanales, mensuales y anuales. Es muy fácil de configurar y usar, y tiene muchas opciones de personalización.

3.5 NetGrid 4.1.5.0

Controla el tráfico, la velocidad de subida y bajada de tu conexión**.** Monitoriza el rendimiento, velocidad y tráfico de tu conexión a Internet,

recogiendo datos tanto de la transferencia de bajada como la de subida y creando con ellos detallados informes.

El programa coloca un icono en la bandeja de sistema desde donde puedes acceder a todas sus funciones, y te permite observar una gráfica generada en tiempo real con el tráfico de tu conexión.

Crea también informes sobre el tráfico producido cada día, semana, mes o año. Puedes configurarlo para que te avise en caso de que la conexión este por debajo de una determinada velocidad, e incluye además utilidades de calculadora y cronómetro. Cuenta con una elegante interfaz totalmente personalizable, y con opciones de transparencia para Windows 2000 y XP.

3.6 Soft Perfect Bandwidth Manager.

Administrador de equipos que controla el ancho de banda en un área local, este equipo es útil en redes pequeñas.

3.6.1 Controla la distribución de conexión en tu red local.

Esta herramienta permite tener un control total sobre el uso de la conexión a Internet, a fin de poder acabar con posibles “cuellos de botella” o poner un límite al uso inapropiado de los recursos en una empresa.

Con Soft Perfect Bandwidth Manager se crea una serie de reglas que controlan el ancho de banda asignado a cada usuario mediante dirección IP, el máximo tráfico de datos que puede usar cada uno, el uso de determinados protocolos o puertos de conexión asociados a ciertas aplicaciones.

No hay necesidad de modificar los parámetros de configuración de tu red local. De esta forma la conexión y el ancho de banda estarán perfectamente controlados y se distribuirán de la forma establecida.

3.7. Costos de los equipos administradores de ancho de banda.

Los costos de los administradores varían según su modelo y marcas a continuación presentamos las tablas de estos equipos.

Numero de parte	Descripción detallada del producto	Precio	Cantidad
MFG Part: BM-2100	Planet BM-2100 – 100 MBPS	$135,980.00	**1**

Tabla 3.1. -Precio del BM-2100 – 100 Mbps de Planet.

Numero de parte	Descripción detallada del producto	Precio	Cantidad
PS6500-l000M-2000	PacketShaper 6500/ISP, Solo Monitoreo, 2000 particiones (MSRP: $17,000.00)	$15,300.00	1
PS6500-L100M-2000	PacketShaper 6500/ISP, up to (sobre) 100 Mbps, formando 2000 particiones (MSRP: $34,000.00)	$30,600.00	**1**
PS9500-L000M-5000	PacketShaper 9500/ISP, Copper GigE, solo monitoreo, 5000 particiones (MSRP: $32,000.00)	$28,800.00	**1**
PS9500-L200M-5000	PacketShaper 9500/ISP, Copper GigE, up to 200 Mbps formando, 5000 particiones (MSRP: $51,000.00)	$45,900.00	**1**
PS9500-L000M-5000-SX	PacketShaper 9500/ISP, Fiber GigE, solo monitoreo, 5000 particiones (MSRP: $32,000.00)	$28,800.00	**1**
PS9500-L200M-5000-SX	PacketShaper 9500/ISP, Fiber GigE, up to 200 Mbps formando, 5000 particiones (MSRP: $51,000.00)	$45,900.00	**1**

Tabla 3.2. Precios de los productos PacketShaper ISP

Numero de parte	Descripción detallada del producto	Precio	Cantidad
PS6500U-L000M-100M-2000	PacketShaper 6500/ISP, solo monitoreo to 100M upgrade (MSRP: $17,000.00)	$15,300.00	**1**
PS9500U-L000M-200M-5000	PacketShaper 9500/ISP, solo monitoreo to 200M upgrade (MSRP: $19,000.00)	$17,100.00	**1**

Tabla 3.3. Actualizaciones de la serie PacketShaper ISP

Numero de parte	Descripción detallada del producto	Precio	Cantidad
PS6500-L000M-2000-CSP	PacketShaper 6500/ISP, solo monitoreo, 2000 particiones, Programa de soporte para un cliente. (MSRP: $2,890.00))	$2,745.50	**1**
PS6500-L100M-2000-CSP	PacketShaper 6500/ISP, up to 100 Mbps formando, 2000 particiones, Programa de apoya para un cliente. (MSRP: $5,780.00)	$5,491.00	**1**
PS9500-L000M-5000-CSP	PacketShaper 9500/ISP, Copper GigE, solo monitoreo, 5000 particiones, programa de apoya para un cliente. (MSRP: $5,440.00)	$5,168.00	**1**
PS9500-L200M-5000-CSP	PacketShaper 9500/ISP, Copper GigE, up to 200 Mbps formando, 5000 particiones, Programa de apoya para un cliente. (MSRP: $8,670.00)	$8,236.50	**1**
PS9500-L000M-5000-SX-CSP	PacketShaper 9500/ISP, Fiber GigE, solo monitoreo, 5000 particiones, Programa de apoya para un cliente. (MSRP: $5,440.00)	$5,168.00	**1**
PS9500-L200M-5000-SX-CSP	PacketShaper 9500/ISP, Fiber GigE, up to 200 Mbps formando, 5000 particiones, Programa de apoya para un cliente. (MSRP: $8,670.00)	$8,236.50	**1**

PS6500U-L000M-100M-2000-CSP	PacketShaper 6500/ISP, solo monitoreo to 100M upgrade, Programa de apoya para un cliente. (MSRP: $2,890.00)	$2,745.50	**1**
PS9500U-L000M-200M-5000-CSP	PacketShaper 9500/ISP, solo monitoreo to 200M upgrade, Programa de apoya para un cliente. (MSRP: $3,230.00)	$3,068.50	**1**
PS6500-L000M-2000-PSS	PacketShaper 6500/ISP, solo monitoreo, 2000 particiones, Packeteer Software suscrición para un cliente. (MSRP: $2,040.00)	$1,938.00	**1**
PS6500-L100M-2000-PSS	PacketShaper 6500/ISP, up to 100 Mbps formando, 2000 particiones, Packeteer Software suscripción para un cliente. (MSRP: $4,080.00)	$3,876.00	**1**
PS9500-L000M-5000-PSS	PacketShaper 9500/ISP, Copper GigE, solo monitoreo, 5000 particiones, Packeteer Software suscripción para un cliente. (MSRP: $3,840.00)	$3,648.00	**1**
PS9500-L200M-5000-PSS	PacketShaper 9500/ISP, Copper GigE, up to 200 Mbps formando, 5000 particiones, Packeteer Software suscripción para un yr. (MSRP: $6,120.00)	$5,814.00	**1**
PS9500-L000M-5000-SX-PSS	PacketShaper 9500/ISP, Fiber GigE, solo monitoreo, 5000 particiones, Packeteer Software suscripción para un cliente. (MSRP: $3,840.00)	$3,648.00	**1**

PS9500-L200M-5000-SX-PSS	PacketShaper 9500/ISP, Fiber GigE, up to 200 Mbps formando, 5000 particiones, Packeteer Software suscripción para un cliente. (MSRP: $6,120.00)	$5,814.00	**1**
PS6500U-L000M-100M-2000-PSS	PacketShaper 6500/ISP, solo monitoreo para 100M upgrade, Packeteer Software suscripción para un cliente. (MSRP: $2,040.00)	$1,938.00	**1**
PS9500U-L000M-200M-5000-PSS	PacketShaper 9500/ISP, solo monitoreo para 200M upgrade, Packeteer Software suscripción para un cliente. (MSRP: $2,280.00)	$2,166.00	**1**

Tabla 3.4. Lista de equipos de Packeteer PacketShaper

Numero de parte	Descripción detallada del producto	Precio	Cantidad
QW-6100	QoSWorks 5000 – Enlaces rápidos arriba de 3512Kbps	$4,000.00	**1**
QW-7110	QoSWorks 7110 – Enlaces rápidos arriba deT1/E1, Full Duplex	$8,000.00	**1**
QW-8110	QoSWorks 8110 – Enlaces rápidos arriba de10Mbps, Full Duplex	$10,000.00	**1**
QWX-9110	QoSWorks 9110 – Enlaces rápidos arriba deT3/E3, Full Duplex	$20,000.00	**1**
QWX-10110	QoSWorks 10011 -Enlaces rápidos arriba de100Mbps, Full Duplex	$25,000.00	**1**
QWX-11000	QoSWorks 11000 -Enlaces rápidos arriba de155Mbps, Full Duplex, Fiber GE interfaces	$32,000.00	**1**
AOS SWUPG	AOS Software Upgrade - Per QoSWorks Device	$1,500	**1**

Tabla 3.5. Lista de equipos de QoSWorks® Family.

3.8. Comparación de los equipos administradores de ancho de banda.

Se realiza la comparación de los equipos en base a sus caracteristicas mas relevantes.

Tabla 3.6 Comparación de las caracteriticas de los equipos administradores

Administrador de Ancho de Banda	Hardware	Software	Monitoreo	Protocolos y aplicaciones	Precio	Priorizar el trafico
Bandwidth Manager BM-2100-100Mbps	x	x	x	+20	135.980.00	3
Packet Shaper 9500/ISP	x	x	x	+100	28.800.00	7
QoSWorks QWX-11000	x	x	x	+40	32.000e00	5
BWMETER 2.3.0		x	x		libres	
NETCRID 4. 1 5.0		x	x		libres	
Soft Perfect Bandwidth Manager		x	x		libres	

CAPÍTULO 4.

ANÁLISIS Y ESTUDIO DE UN ADMINISTRADOR DE ANCHO DE BANDA (PACKETSHAPER).

PacketShaper ISP es un instrumento de provisión de ancho de banda que está situado entre una WAN y una LAN. Maneja todo el tráfico entrante, (Inbound) y que sale, (Outbound), categoriza y analiza los paquetes cuando ellos pasan, y asignando el ancho de banda apropiadamente con criterios basado en políticas. PacketShaper ISP proporciona beneficios a una variedad de ambientes: cable, inalámbrico fijo, satélite, un rango de tasa de velocidades WAN y LAN, y servidores. PacketShaper ISP igual se ajusta suavemente en redes del proveedor con VLANs múltiple, así como para separar el tráfico de cada cliente o el tráfico administrativo.

4.1 Instalación y configuración inicial.

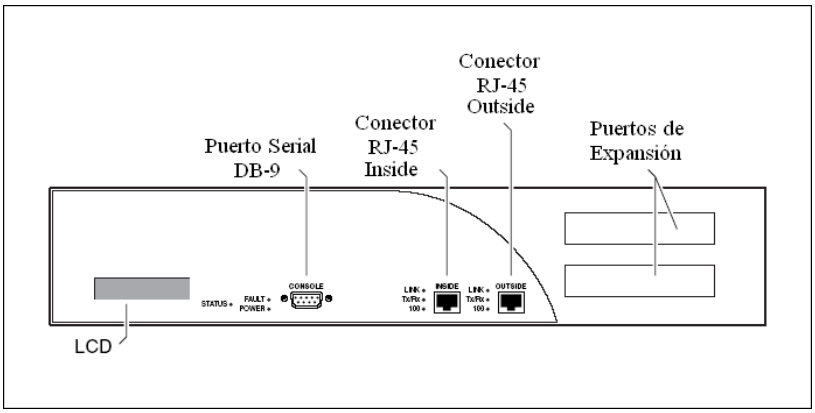


Fig. 4.1 Panel frontal.

El panel frontal de la unidad de PacketShaper, mostrado en figura 4.1, tiene dos puertos de la red, INSIDE y OUTSIDE. La unidad tiene un puerto serial Al DB-9 (CONSOLA) para conectar un terminal o PC a la unidad para la configuración local. Un cable de null-modem es provisto para este propósito. El panel LCD (display de cristal líquido) en el frente de algunos modelos de Packeteer indican el estado de operación de la unidad. El PacketShaper es considerado como un equipo activo. Usaremos pues el cable derecho para unirlo a un HUB o un switch, y un cable cruzado para la máquina o el router.

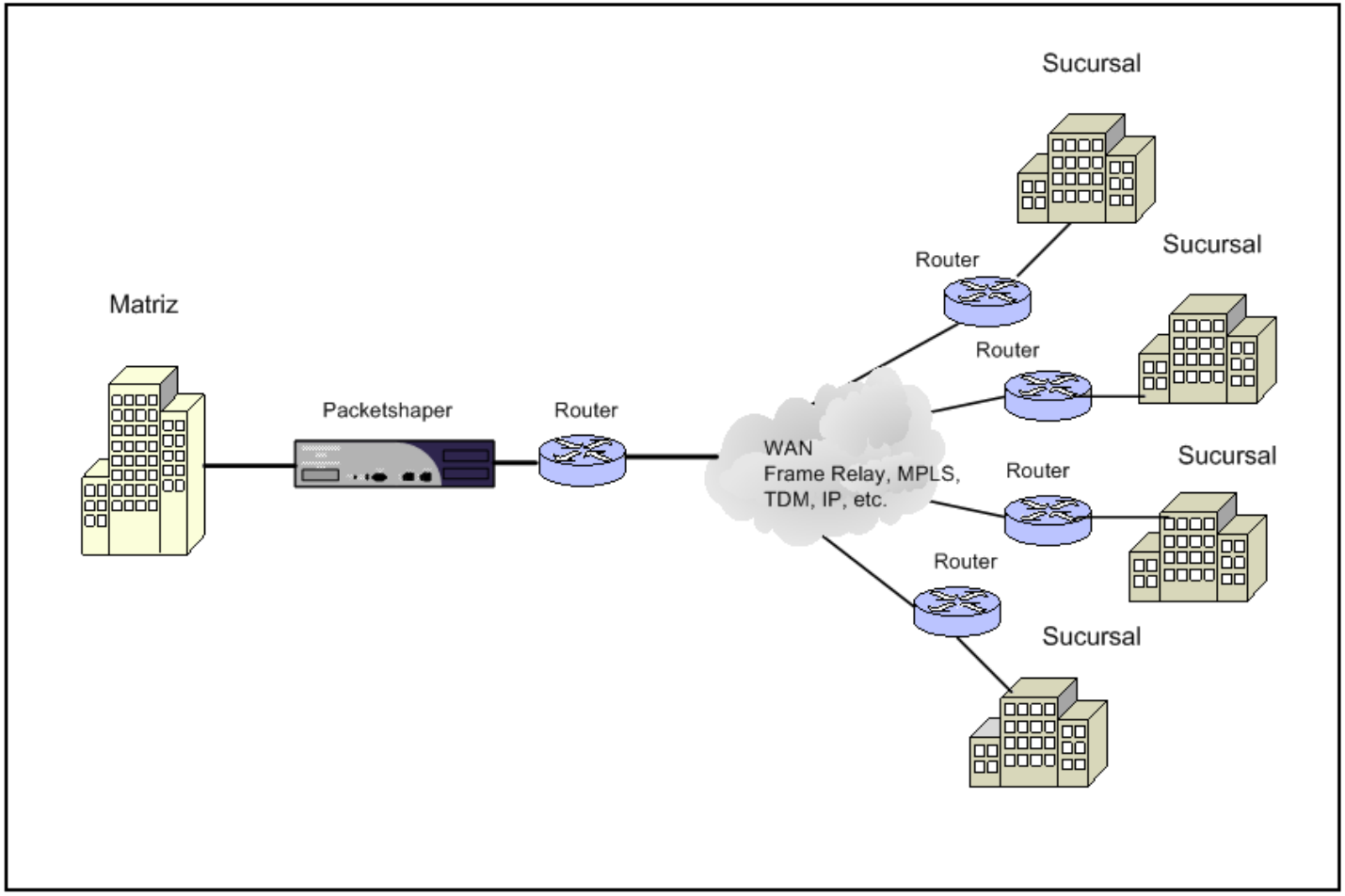


Fig. 4.2 Ubicación del PacketShaper

La instalación de PacketShaper ISP consiste en conectar dos cables y entrar la dirección IP y acceso de información de configuración basado en una página Web. Accedemos a la URL http://unconfigured.packetshaper.com y aparecerá una pantalla que le pedirá varios datos necesarios para entrar en la demostración del PacketShaper.

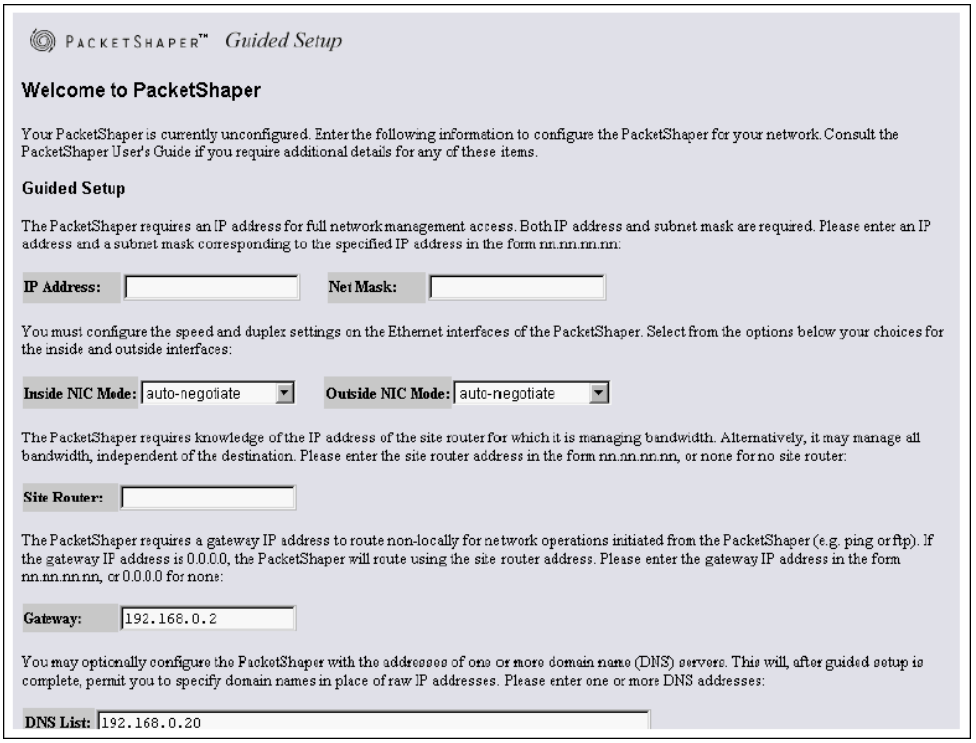


Fig. 4.3 Configuración inicial.

Estos son los diferentes campos que se deben rellenar:

- Dirección IP del PacketShaper.

- Net Mask: la máscara de red del PacketShaper.

- La velocidad de las tarjetas de red: autonegociación por defecto.

- Nodo router: si especifica una dirección, el PacketShaper organizará todos los flujos que vengan de o vayan a esta dirección. Si necesitara el valor « none»(no hay router), el PacketShaper organizaría los flujos que lo atraviesan.

- Inbound link: la velocidad de la línea de entrada (512k, 2M etc.…)

- Outbound link: la velocidad de salida (512k, 2M etc.…)

- Gateway: la dirección IP del gateway por defecto.

PacketShaper ISP se integra claramente con infraestructura de red existente, no impone ningún cambio en la configuración de los routers, topologías, desktops, o servidores. Además, airosamente complementa otras aplicaciones de red y topologías como Firewalls, cargas balanceadas, routers redundantes, y soluciones cache. Una interfase de usuario basado en Web ofrece acceso a PacketShaper ISP de cualquier desktop con un Web browser.

Un comando de interfaz de línea ofrece un rápido y detallado control de una sesión Telnet de manera segura. Uno elige que el nivel de seguridad requerido para examinar y alterar la configuración de PacketShaper ISP y la medida de los datos. Las contraseñas, listas de acceso, RADIUS, y las normas basadas en SSL son algunas de las opciones de seguridad.

4.2 Clasificación del tráfico.

Para entender la clasificación del tráfico es de utilidad entender los siguientes términos:

- Clases: Una agrupación lógica de flujos de tráfico que tienen las mismas características y son analizadas y controladas conjuntamente.

- Reglas de Juego: La porción de una clase definida que especifica el tráfico asociado con la clase, una aplicación especifica, protocolo, dirección o grupo de direcciones.

- Partición: Un tubo de ancho de banda asignado a una clase dada para proteger o restringir todo el flujo en esa clase.

- Políticas: Una regla asignada a una clase dada que define como un solo flujo será manipulado durante la administración del ancho de banda. Las políticas actúan en flujos de tráfico individuales, por ejemplo una conexión http a un servidor Web.

4.2.1 Árbol de tráfico.

PacketShaper utiliza una estructura de ramificación jerárquica para organizar y clasificar el tráfico que está pasando, formando un árbol de tráfico. El árbol ordena las clases de tráfico en clases padre, hijo, y relaciones de parentesco, similar a las carpetas y archivos en un sistema del archivo Standard. Una clase de tráfico identifica un tipo de tráfico que se desea manejar de manera conjunta, puede ser una aplicación, un protocolo, todo el tráfico a una situación, y muchas otras posibilidades. Una clase puede tener uno o más clases de hijos secundarios con características más específicas que su antecesor.

El siguiente fragmento de árbol indica que el tráfico es primeramente organizado por dirección de viaje, en este caso Inbound, después por aplicación (SAP, FTP, o Citrix), y después, algunas veces, de forma adicional, refinado por aplicación (PeopleSoft sobre Citrix, MS Word sobre Citrix). SAP, FTP, y Citrix son clases hermano y todos ellos comparten la misma clase padre Inbound. Cuando se hace referencia

a una clase, se usa un slash adelante entre cada nivel, por ejemplo, /Inbound/Citrix/MsWord. Se puede crear hasta 11 niveles en un árbol de tráfico.

Por ejemplo, la estructura de un fragmento del árbol de tráfico podría lucir así:

- - Inbound
    - + SAP
    - + FTP
    - - Citrix
        - + PeopleSoft
        - + MsWord
        - ...y así sucesivamente...

El árbol es automáticamente ordenado desde el más al menos específico; las clases con más criterio específico están en la cima del árbol. Por ejemplo, una clase Web para una URL específica vendría antes de la clase HTTP general. Las clases que tienen el mismo nivel relativo específico se ordenan alfabéticamente. PacketShaper automáticamente determina el orden de las clases en el árbol y la

única manera de cambiar el orden es creando una clase de excepción.

4.2.2 Iconos de las clases de tráfico.

Junto a cada nombre de la clase en el árbol de tráfico hay un icono, o una combinación de iconos. Los iconos representan las propiedades básicas de una clase de tráfico, indica si una política o la partición se han aplicado y, si la clase es Standard, de excepción, o clase Default. La tabla siguiente describe cada uno de los iconos de clase de tráfico.

Icono	Descripción
	Clase de tráfico standard. Una clase que tiene uno o más reglas de juego y no es una clase total de juego
!	Clase de tráfico de excepción. Una clase que se ha sido etiquetada para ordenar encima de la clase standard (sin excepción) en el árbol de tráfico. Las clases excepción le dan la habilidad de redefinir el orden de la búsqueda que usa PacketShaper para encontrar una pareja para un flujo de tráfico.
	Políticas. Una clase que tiene una política asociada con esta

	Partición. Una clase que tiene asociada una partición con esta
Icono	. Descripción
	Carpeta. Una clase sin reglas de juego. La carpeta se usa para organizar la estructura del árbol y sólo sirve como un contenedor. No asocia tráfico, y no puede tener una política aplicada a él.
	Todas las reglas de juego. (Default) Una clase que típicamente aparece al fondo de un subárbol. El balde retiene cualquier flujo de tráfico no compatible con sus clases hermanos en el subárbol. Una clase Default, es creada cuando el primer hijo se agrega a una clase de tráfico de padre.

Tabla 4.1 Iconos de las clases de tráfico

4.2.3 Combinación de iconos.

Los iconos de clase de tráfico pueden combinarse para designar una clase con características múltiples. La tabla siguiente proporciona los ejemplos de las combinaciones de iconos que se pueden ver en un árbol de tráfico.

Icono	Descripción
	Clase de tráfico Standard con una política. Una clase de tráfico Standard que tiene una política asignada para controlar la calidad de servicio para el tipo de tráfico.
	Clase de tráfico de Excepción con una política. Una clase de tráfico de excepción con una política asignada. Packetshaper automáticamente crea una clase de host local que es definida como una clase de excepción con una política de prioridad fijada a una prioridad 6. Esta clase especial permite a un administrador siempre poder acceder la unidad a pesar de congestión.
	Todas las clases de juego con una política. Una clase total de juego, con el nombre Default, aparece al fondo de los árboles /Inbound /Outbound. Estas clases Default tienen políticas heredables.

Tabla 4.2 Combinación de iconos.

4.3 Ideas para la formación de arboles de tráfico.

Se dan 4 ideas para la formación de un árbol de tráfico, se pueden crear muchas más, eso depende de las necesidades de la empresa y de la imaginación del administrador.

4.3.1 Creación de un árbol de tráfico basado en aplicaciones.

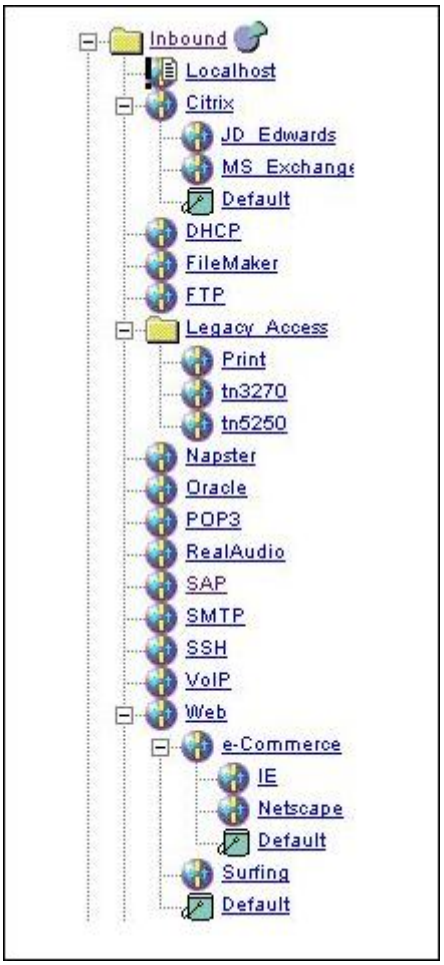


Fig. 4.4 Árbol basado en aplicaciones.

Ayuda a saber qué aplicaciones están corriendo en la red, entender su conducta, rastrear los tiempos de respuesta, o controlar su desempeño. Un árbol basado en aplicaciones es simple de crear y usar.

Un árbol basado en aplicaciones es apropiado para un WAN o enlace de Internet a cualquier matriz o sucursal donde se desea variar las estrategias de dirección de tráfico según su tipo, como una aplicación, en lugar de un destino o situación. Un árbol basado en aplicaciones es muy común en sucursales y los enlaces de Internet matrices.

4.3.2 Creación de un árbol de tráfico basado en localización simple.

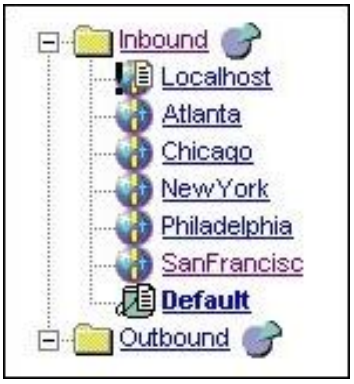


Fig. 4.5 Árbol basado en localización simple.

Un árbol basado en localización simple es para redes WAN o enlaces principales de Internet con tráfico que va a las sucursales múltiples o a los departamentos múltiples. Categoriza primero por dirección de viaje y después por situación.

Es apropiado para las ocasiones cuando el interés primario es aprovisionar ancho de banda, y no importa cómo se usa o cómo las aplicaciones funcionan. Adicionalmente, puede ser apropiado para una matriz en topologías donde otras unidades de PacketShaper manejan aplicaciones en cada situación, y el sitio matriz apenas maneja la cantidad de tráfico que sale a cada rama.

4.3.3 Creación de un árbol de tráfico basado en localización con aplicaciones.

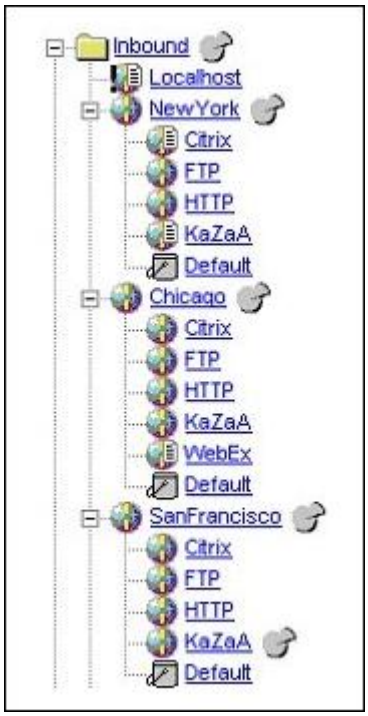


Fig. 4.6 Árbol basado en localización con aplicaciones.

Este árbol es apropiado para redes WAN o enlaces de Internet principales con tráfico que va a sucursales múltiples o departamentos. Este árbol ofrece mejor visión y más control de las aplicaciones. Pero impone consideraciones del escalamiento y tarda más tiempo para configurar. Categoriza primero por dirección de viaje, después por situación, y finalmente por aplicación.

Por ejemplo, si se desea saber cuánto tráfico de New York está circulando, y se desea saber cuánto tráfico de SAP está pasando, y cuánto se tiene en New York, entonces este árbol de tráfico es la mejor alternativa.

4.3.4 Creación de un árbol de tráfico global basado en localización y aplicaciones.

Un árbol de tráfico basado en localización y con aplicaciones globales es apropiado para redes WAN o enlaces de Internet principales con tráfico que va a sucursales múltiples. Categoriza el tráfico primero por dirección de viaje, después por situación. Después aplica políticas por aplicación al tráfico de cada localización, de las clases no heredables, listadas debajo de las clases de localización. Pero todo el tráfico de la aplicación se maneja con una estrategia, independiente de la sucursal.

Fig. 4.7 Árbol de tráfico Global basado en localización y aplicaciones.

4.4 Políticas.

Una política determina cómo los flujos individuales de una aplicación son tratados en el contexto de aplicaciones en competencia, y permite administrar el ancho de banda en una base de flujo por flujo. Con políticas, se puede dar el necesario para un funcionamiento óptimo a cada flujo de tráfico crítico, así como proteger del tráfico codicioso y menos importante. Además, las políticas pueden guardar flujos de tráfico no urgentes, como FTP, que consumen más de la porción apropiada de ancho de banda.

PacketShaper ofrece los siguientes tipos de políticas:

- Prioridad: Establece una prioridad por tráfico sin especificar una proporción particular. Se usa políticas de prioridad para tipos de tráfico no IP, o tráfico que no produce congestión, por ejemplo, Telnet.

- Rate: Suaviza tráfico expansivo, como HTTP, usando la tecnología TCP Rate Control de Packeteer, que es un mecanismo avanzado que evita la congestión cuya meta es prevenir el tráfico que es enviando a velocidades más altas que la conexión WAN y para eso reduce las colas en los buffers de los router y mejora la eficacia global.

- Descartar: Elimina todos los paquetes para una clase de tráfico y bloquea el servicio. Se usa este tipo de la política para una aplicación que es no esencial en el negocio y consume demasiado ancho de banda en la red.

- Ignorar: Exenta una clase de tráfico de asignación de ancho de banda y es tratado como tráfico de paso. Es decir, el tráfico no se contará como parte del tráfico del enlace bajo administración. Debe

tenerse cuidado al usar esta política. Si una política ignorada es puesta en una clase que es un el mayor consumidor del ancho de banda, otra asignación del ancho de banda podría ser impactada.

- No admitir: Restringe el tráfico no-TCP e inteligentemente rechaza tráfico Web y tráfico TCP. Esta política es usada para remitir a ciertos usuarios Web para alternar URLs.

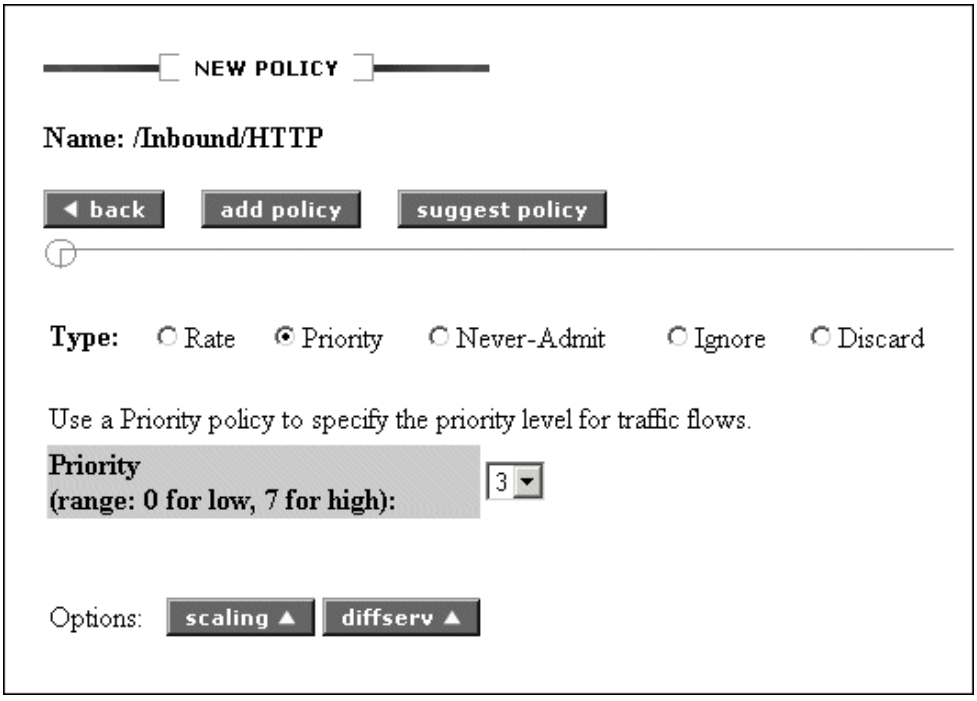


Fig. 4.8 Políticas.

Sólo pueden aplicarse políticas a las clases "hojas", es decir, que no tienen hijos. Por ejemplo, una clase padre, /Inbound/HTTP, puede tener

clases hijos para diferenciar un website de otro: /Inbound/HTTP/ESPN y /Inbound/HTTP/MyCompany. En este ejemplo, pueden ponerse políticas en las clases ESPN y MyCompany, solo si ellos no tienen hijos, pero no en la clase padre /Inbound/HTTP.

Si una clase tiene una política y después se crea una clase hijo, una clase Default se crea automáticamente en este subárbol y la política de clase padre se transfiere a esta clase. Si todas las clases hijo son anuladas después, la política se transfiere de nuevo a la clase padre.

4.5 Particiones.

Una partición administra ancho de banda para un flujo agregado de clases de tráfico, para que todos los flujos de la clase se controlen juntos como uno solo.

Las particiones se usan para:

- Proteger tráfico crítico, garantizando que una clase de tráfico siempre obtenga una cantidad definida de ancho de banda.

- Limitar el tráfico agresivo no crítico permitiendo que esa clase de tráfico consuma sólo una cantidad asignada de ancho de banda.

- Dividir la capacidad.

- Asignar ancho de banda dinámicamente a los usuarios.

4.5.1 Proteger el tráfico.

Las particiones protegen tráfico garantizando una cantidad definida de ancho de banda para las clases de tráfico críticas, por ejemplo, se puede fijar una partición de 128 Kbps para tráfico SNA. Esta partición asegura que SNA siempre tendrá por lo menos 128 Kbps de ancho de banda disponible. Las olas de tráfico imprevisibles no interferirán con tráfico SNA.

4.5.2 Limitar el tráfico.

Las particiones limitan tráfico menos importante poniendo un tope en la cantidad de ancho de banda una clase de tráfico puede usar, por ejemplo, se tiene un enlace de 128K. Se puede asignar una partición de 64 Kbps al tráfico de FTP. Esto impide al tráfico FTP consuma todo el enlace y bloquee el tráfico más importante (como Oracle o Citrix)

Otro ejemplo de limitar el tráfico, es restringiendo cuánto ancho de banda puede usar una subred clase C, sin tener en cuenta cuántas

sesiones estén activas. Se puede crear una partición 256 Kbps, ajustable a 512 Kbps. El tráfico del subnet siempre recibiría por lo menos 256 Kbps, y podría usar hasta 512 Kbps si ese ancho de banda está disponible.

4.5.3 Dividir la capacidad.

Algunos el tráfico, como Voz sobre IP (VoIP), requiere una cierta cantidad de ancho de banda para que la calidad de la transmisión sea aceptable, por ejemplo, se puede crear una clase VoIP.

Una partición para la clase de tráfico VoIP maneja el tráfico VoIP agregado y los flujos concurrentes para la clase. Se puede combinar la partición con una política Rate que define una proporción mínima para cada flujo.

En este ejemplo, combinando una política de velocidad con una partición, se asegura siempre que VoIP tiene suficiente ancho de banda para apoyar los flujos múltiples durante una sesión VoIP. Sin esa reservación de ancho de banda, la conversación online estaría congestionada e ininteligible, y la calidad de servicio sufriría.

Las particiones, como las clases de tráfico, son tan necesarias para crear una partición para cada dirección de un tipo de tráfico.

4.5.4 Asignar ancho de banda dinámicamente.

Con particiones dinámicas, las sub-particiones son creadas instantáneamente según se van creando los usuarios activos en una clase de tráfico. Esta capacidad permite a proveedores de servicio o a clientes de la empresa garantizarle una cantidad mínima de ancho de banda en todo momento a un usuario. Esta estrategia es útil cuando una porción pequeña de usuarios estará activa en cualquier periodo de tiempo dado.

Por ejemplo, un ISP podría tener 20,000 clientes, con 2,000 usuarios conectados en un momento dado. Con una partición dinámica establecida, se crean sub-particiones automáticamente para los usuarios cuando ellos conectan. La sub-partición dinámica asigna una mínima y máxima cantidad de ancho de banda a cada usuario. Para acomodar a los nuevos usuarios cuando el número del máximo de usuarios se alcanza, la sub-partición no activa más antigua se remueve para que pueda liberarse ancho de banda para los usuarios activos.

4.6 Particiones jerárquicas.

Todas las particiones son definidas como jerárquicas, es decir, las particiones pueden contener particiones. Por ejemplo, se podría definir una partición fija para FTP y después se podría crear particiones hijos expansibles para grupos de usuarios que usan esta aplicación.

Esta aproximación jerárquica habilita la administración de las aplicaciones para los grupos múltiples, mientras controla el grupo en conjunto. Por ejemplo, un ISP puede subdividir la partición de un subscriptor con particiones hijo para cada uno de las secciones del subscriptor. Igualmente, una empresa puede asignar cantidades diferentes de ancho de banda para una aplicación particular a los grupos diferentes de usuarios. Por ejemplo, una empresa podría tener una clase de PeopleSoft con una partición fija. Dentro de esta partición, los Recursos Humanos podrían tener una partición hijo extensible mayor y la Contabilidad podría tener una partición extensible más pequeña.

El concepto de la clave para las particiones jerárquicas es que esa mínima partición de hijos es limitada al mínimo de partición de padre. Cuando la suma del tamaño mínimo de las particiones de los hijos excede el tamaño mínimo de la partición del padre, el padre sobrescribe

el exceso y las particiones de los hijos se escalarán proporcionalmente. Vea los ejemplos siguientes.

4.6.1 Ejemplos de particiones jerárquicas.

Un ISP podría configurar una partición por cliente (por nombre del servidor o dirección IP) para asociar el Contrato de Nivel de Servicio del cliente (SLA) Las particiones le permiten al ISP reforzar los SLAs para clientes que desean expandirse más allá de sus límites. En el ejemplo siguiente, las clases FTP y HTTP (ambos 384 Kbps mínimo) se han sobrescrito en exceso a su partición padre (512 Kbps mínimo) por 256 Kbps. Cuando una partición sobrescribe el exceso para sus particiones hijo, todas las particiones en su subárbol son escaladas acordemente. En este ejemplo, se asignarán a ambas clases hijo 256 Kbps para que la suma no exceda el tamaño del mínimo del padre.

- Inbound
    - Customer1 (minimum partition size = 1 Mbps)
    - Customer2 (minimum partition size = 512 Kbps)
        - FTP (minimum partition size = 384 Kbps)
        - HTTP (minimum partition size = 384 Kbps)
- Default

En el próximo ejemplo, la suma del tamaño mínimo para las particiones FTP y HTTP son menores de su padre, Customer2. En este caso, ambas clases del niño obtendrán 256 Kbps por lo menos y pueden extenderse al tamaño de Customer2 (1024 Kbps) Si una partición es burstable y el ancho de banda está disponible, la partición puede acceder el ancho de banda disponible si la necesita.

- Inbound
    - Customer1 (minimum partition size = 512 Kbps)
    - Customer2 (minimum partition size = 1024 Kbps)
        - FTP (minimum partition size = 256 Kbps, burstable to 512 Kbps)
        - HTTP (minimum partition size = 256 Kbps, burstable to 512 Kbps)
- Default

4.6.2 Tipos de particiones.

Hay dos tipos de particiones que se pueden crear: estática o dinámico.

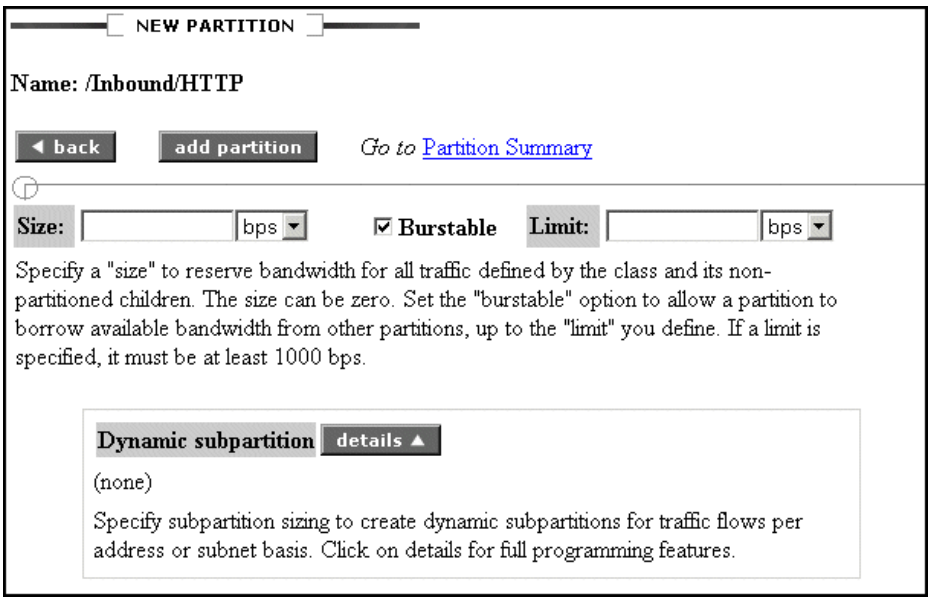


Fig. 4.9 Tipos de particiones.

Una partición estática maneja ancho de banda para todos los flujos dentro de una clase de tráfico particular. Las particiones estáticas pueden ser fijas ó extensibles. (Burstable)

Una partición fija permite que una clase de tráfico use una cantidad definida de ancho de banda, si la necesita. Una partición fija no sólo asegura que una cantidad específica estará disponible, sino también limitará el tráfico a ese mismo nivel.

Una partición burstable o extensible, permite que una clase de tráfico use una cantidad definida de ancho de banda, y acceder al que está sin uso, si lo necesita. Se puede poner un límite en una partición

burstable y puede permitir acceder a la cantidad máxima, o consumir todo el ancho de banda disponible.

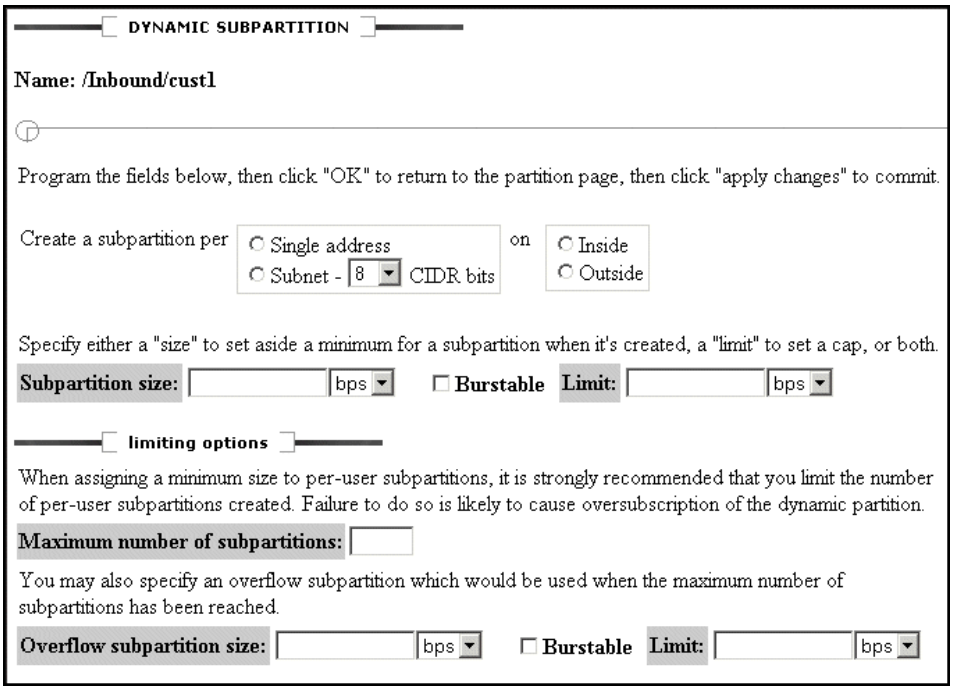


Fig. 4.10 Partición dinámica.

En situaciones donde se desea aplicar límites del ancho de banda a los usuarios individuales, se puede establecer sub-particiones dinámicas para las clases de tráfico. Una partición dinámica afina al ancho de banda de una partición estática y crea sub-particiones instantáneamente para los nuevos usuarios. Sub-particiones son los hijos de una partición estática.

4.7. Reglas de juego. (Matching Rules)

Las reglas de juego definen el criterio usado por PacketShaper para identificar tipos de tráfico. Cada clase de tráfico debe tener una regla de juego por lo menos. Cuando descubre tráfico, se crea una clase y una o más reglas de juego para caracterizarlo. En una forma similar, cuando se crea una clase manualmente, se debe especificar las reglas de juego que describan los flujos de la aplicación.

Una clase de tráfico puede tener reglas de juego múltiples, los cuales son tratados como especificaciones separadas y distintas. Cuando PacketShaper intenta trazar un flujo de tráfico a una clase, compara el flujo con el criterio en la primera regla de juego de clase. Si PacketShaper no encuentra una pareja, continúa a través de las reglas hasta que una pareja es encontrada o hasta que terminan las reglas de juego, en ese caso sigue a la siguiente clase en el árbol. Si una clase de tráfico específica no puede encontrarse para un flujo, el tráfico es clasificado en la clase de tráfico Default para el subárbol.

Los campos son encontrados en las ventanas New Traffic Class y New Matching Rule.

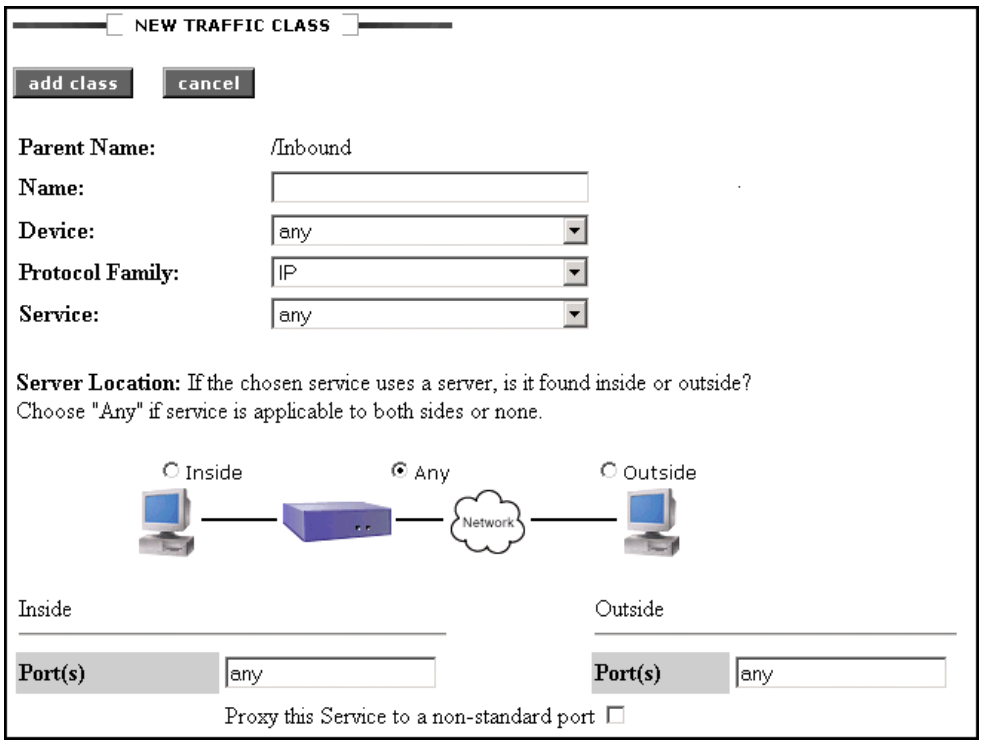


Fig. 4.11 Reglas de juego (1)

4.7.1 Dispositivo.

Para asociar el tráfico que está atravesando una interfase específica, se puede crear una clase que especifica un puerto físico en la unidad de Packeteer. Por ejemplo, se puede crear una clase que clasifica todo el tráfico que sale en el Módulo de Expansión LAN (LEM) superior. Se puede encender class discovery para la clase LEM y PacketShaper automáticamente descubrirá todas las aplicaciones, servicios, y protocolos en este LEM. El campo Device lista sólo las interfaces instaladas en su unidad. Los posibles valores son:

- any (no clasificará por dispositivo)
- main (en construcción)
- lower (bajo LEM)
- upper (alto LEM)

4.7.2 Localización del servidor.

Para las clases de trafico del protocolo IP, la sintaxis de la regla juego usa los términos inside y outside para referirse a la localización del servidor de aplicaciones, relativo a la unidad. Si el router local es el de acceso, los hosts internos forman la LAN y los de afuera forman la WAN o Internet.

Nota: Cuando se configura Inside u Outside, si el servicio elegido usa un servidor, se debe saber si el servidor está localizado fuera o dentro de la unidad.

Si se desea capturar tráfico en una clase dada sin tener en cuenta la situación del servidor, se selecciona “any”. Se desea hacer esto cuando crea una regla de juego por dirección IP del cliente o subnet. PacketShaper creará dos reglas juego, uno para dentro y otro para afuera. Además, PacketShaper no soporta el concepto de un servidor para protocolos sin IP, NetBEUI, IPX, AppleTalk, SNA, DECnet, y

FNA, así que estos protocolos no tienen una referencia de adentro o afuera. Para estos tipos del protocolo, seleccione any para el servidor local.

4.7.2.1 Clasificando por localización del servidor.

Si se desea administrar el tráfico con mas precisión, se crean clases separadamente para la localización del servidor afuera o adentro, es decir, /Inbound/HTTP/Inside, /Inbound/HTTP/Outside, /Outbound/HTTP/Inside, y /Outbound/HTTP/Outside. Por ejemplo si se desea crear esas clases separadamente para ser capaces de distinguir entre uploads y downloads.

4.7.2.2 Ejemplo de localización del servidor.

Se puede crear clases de tráfico manualmente para considerar para una localización del servidor de aplicaciones. Por ejemplo, MySportsCompany, Inc. (una compañía ficticia) instaló una unidad en su red. El diseñador de la Web MySportsCompany descarga imágenes del website de ESPN. La siguiente tabla describe la actividad del tráfico y las clases que asocian la actividad:

Acción y tráfico descubierto.	Regla de clase de tráfico.
1. Una unidad se despliega en la LAN MySportsCompany.	
2. MySportsCompany accede al website de ESPN, un HTTP es solicitado. El servidor Web de ESPN está fuera.	/Outbound/HTTP/Outside
3. Los gráficos Web de ESPN son enviados a MySportsCompany. El servidor Web ESPN está aun fuera de MySportsCompany.	/Inbound/HTTP/Outside
4. El personal de Marketing de ESPN desea ver el Website de MySportsCompany, un HTTP es solicitado. El servidor Web de MySportsCompany está dentro.	/Inbound/HTTP/Inside
5. La página Web MySportsCompany es transmitida a ESPN. El servidor de MySportsCompany está dentro.	/Outbound/HTTP/Inside

Tabla 4.3 Localización del servidor.

4.7.3 Puertos.

En el campo de los puertos interior y exterior, se puede listar el puerto o los puertos asociados con los servicios para esta clase. En general, sólo se debe especificar un número cuando se desea restringir clasificación a uno específico. Puesto que muchas aplicaciones ya no limitan transmisiones para el número puerto asignado, es mejor especificar un nombre de servicio.

Se puede definir un servicio en un puerto no Standard; sin embargo, el puerto debe ser un número que no ha sido asignado. Por ejemplo, en la regla de juego, se puede definir el servicio como HTTP y el puerto como 8088.

4.7.3.1 Rango de números de puertos.

Especificar un rango de números del puerto, por ejemplo, del 5001 al 5005, se debe usar un guión (-) para separar los valores bajos y altos del rango (5001-5005)

4.7.3.2 Números de puertos no continuos.

Especificar números del puerto no continuos, por ejemplo, sólo puertos 5001 y 5025, se definen reglas de juego separadas dentro de la misma clase.

4.7.3.3 Servicio Proxy a un puerto no estándar.

Un servicio Proxy permite identificar aplicaciones que corren en puertos que no obedecen los bien conocidos números del puerto definidas por IANA. Por ejemplo, para saber que cierto host (a menudo un servidor Proxy) está ejecutando un servicio particular en un puerto Standard no especifico. En la regla de juego, se especifica una combinación de atributos, como host y puerto, y entonces se usa el Proxy de este Servicio a la opción del puerto no Standard para asociar el tráfico con un servicio conocido.

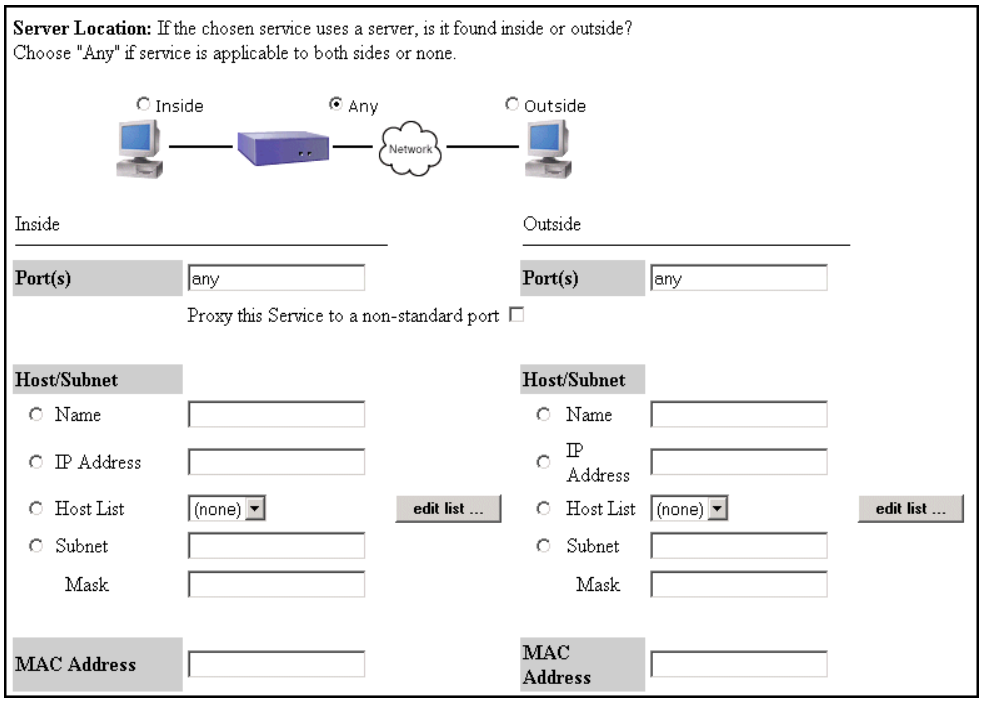


Fig. 4.12 Reglas de juego (2)

4.7.4 Host/Subnet.

Se usa el campo de las reglas de juego para aislar un solo host o un rango de hosts, quizás el PC del administrador de la red o un grupo de usuarios de prioridad alta.

Se puede especificar los host fuente y destino de varias maneras: por nombre, dirección de IP, un rango de direcciones de IP, una lista de nombres, o dirección del subnet y máscara.

4.7.4.1 Nombre.

Cuando se tiene configurado un servidor de DNS en PacketShaper, se puede especificar un nombre del dominio en una regla de juego. Si hay configurado un nombre del dominio predefinido, se puede usar nombres del dominio no calificados totalmente. Si el nombre no existe que cuando se crea la regla de juego, PacketShaper advierte sobre el nombre desconocido.

PacketShaper renueva los nombres DNS lookups en las reglas de juego siempre que ellos expiren, según la vida que es retornada en el lookup. Esto se configura separadamente en cada servidor de nombre. Esta conducta del cliente es compatible con DNS dinámico.

Dns lookup.- Lista la(s) dirección(es) asociadas con un nombre del dominio. PacketShaper mantiene los datos mapeados actualizados, así, cuando un sitio cambia una dirección IP, la regla de juego sepa sobre el cambio.

4.7.4.2 Dirección IP.

Se puede especificar una dirección IP usando una de las siguientes formas:

- Entre una sola dirección IP en anotación decimal separada por puntos, por ejemplo, 207.78.98.254.

- Especificar un rango de direcciones de IP por separado, la primera y última dirección con un guión, por ejemplo, 10.10.10.10-10.10.10.20.

Nota: Cuando una clase padre tiene un rango dirección IP Interior y su clase hijo tiene un rango de direcciones IP Outside, diferente del rango del padre, hay que especificar el rango de IPs padre Outside en las reglas de juego de la clase hijo. (El rango no se hereda.) Si hay descuido en el rango padre de entrada, un error de incompatibilidad en la regla de juego puede ocurrir.

Para los servicios multicast, entre el keyword multicast para especificar las direcciones IP Clase D (224.0.0.0 a través de 239.255.255.255) para el lado destino, eso es, inside de para la clases Inbound, outside paras las clase Outbound.

El proceso de clasificación puede manejar la transmisión y otro tráfico multicast si se especifica en la regla juego. En este caso, PacketShaper asume que, desde que está atravesando este tráfico a sitios remotos, necesita contar este tráfico.

Usar any para indicar cualquier host, es decir, sin una dirección en particular.

4.7.4.3 Lista de hosts.

Una lista de host contiene las direcciones IP, nombres de DNS, y/o subnets que las reglas de juego de las clases de tráfico pueden referenciar. Las listas de host permiten especificar muchos hosts en una sola regla de juego de clase de tráfico. Las direcciones en una lista de host no necesitan ser contiguas.

4.7.4.4 Subnet y máscaras.

Especificar una máscara de subnet para enmascarar los bits de dirección de red, de este modo, definir un subconjunto de hosts en una red, por ejemplo, 255.255.255.0

4.7.4.5 Direcciones MAC.

Se puede entrar una dirección de MAC en vez de una IP o protocolo no IP para habilitar la clasificación de tráfico hacia y desde un host conocido. En la dirección debe entrarse en formato de octeto de seis números, por ejemplo, 08:12:34:56:A1:5C. No se puede clasificar broadcasts Ethernet (FF:FF:FF:FF:FF:FF)

Cuando el host reside fuera de la unidad, hay que especificar la dirección MAC en la columna "Outside" . Si el host está delante, dentro de la unidad, se usa la columna "Inside". Para asociar todo el tráfico desde un host, sin tener en cuenta si está dentro o fuera de la unidad, se necesita crear dos reglas de juego separadas.

Esta funcionalidad permite crear clases para tráfico que pasa a través de un router específico y/o interfase del router. Por ejemplo, la unidad PacketShaper está conecta a dos routers WAN. Con esta característica, se puede crear una clase separada para cada

router especificando la dirección de MAC de la interfase del router en la regla de juego. Se puede entonces asignar una partición a cada clase para controlar uso del ancho de banda del enlace.

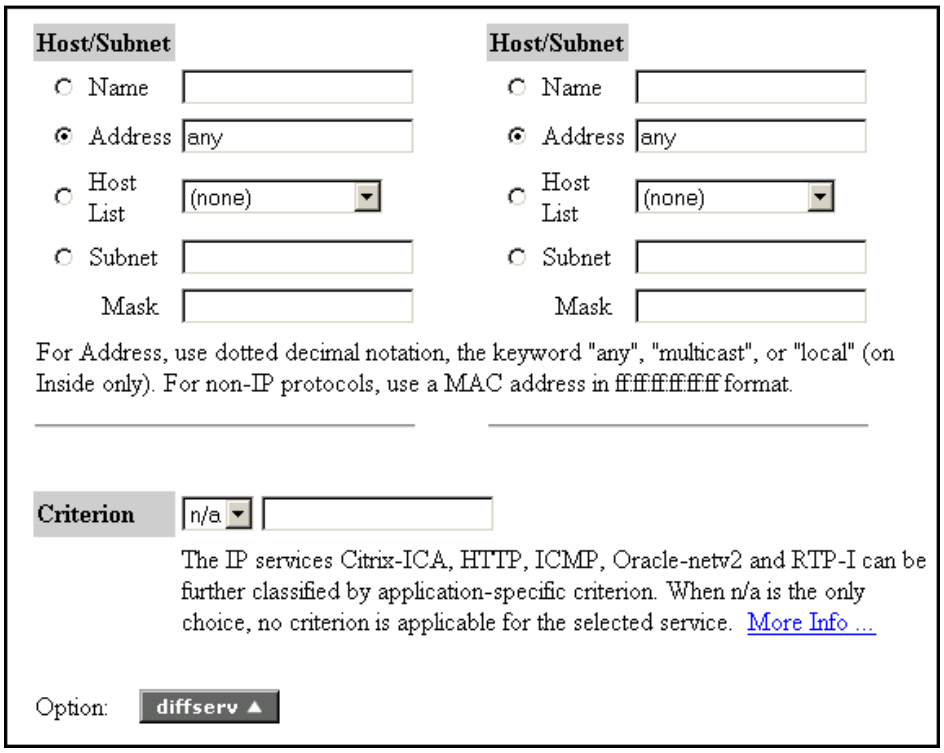


Fig. 4.13 Reglas de juego (3).

4.7.5 Criterio para aplicaciones especificas.

El campo Criterion está disponible para ciertos tipos de tráfico, específicamente Citrix-ICA, DICOM, FTP-Data-Clear, HTTP, HTTP-Tunnel, ICMP, NNTP-Clear, Oracle-netv2, PostgreSQL, RTCP-I, RTP-I, SMTP-Clear, SOAP-HTTP, y SSL. Este campo permite más que diferenciar estos tipos de tráfico. Por ejemplo, el tráfico Web

puede ser diferenciado por nombre de host DNS o dirección, URL, tipo de contenido, o Web browser(agente del usuario).

4.7.6 Diffserv.

Al escoger diffserv cuando se crea una clase o regla de juego, la ventana Diffserv aparece. En esta ventana, se puede seleccionar Code Point o COS/TOS.

4.7.6.1 Code Point.

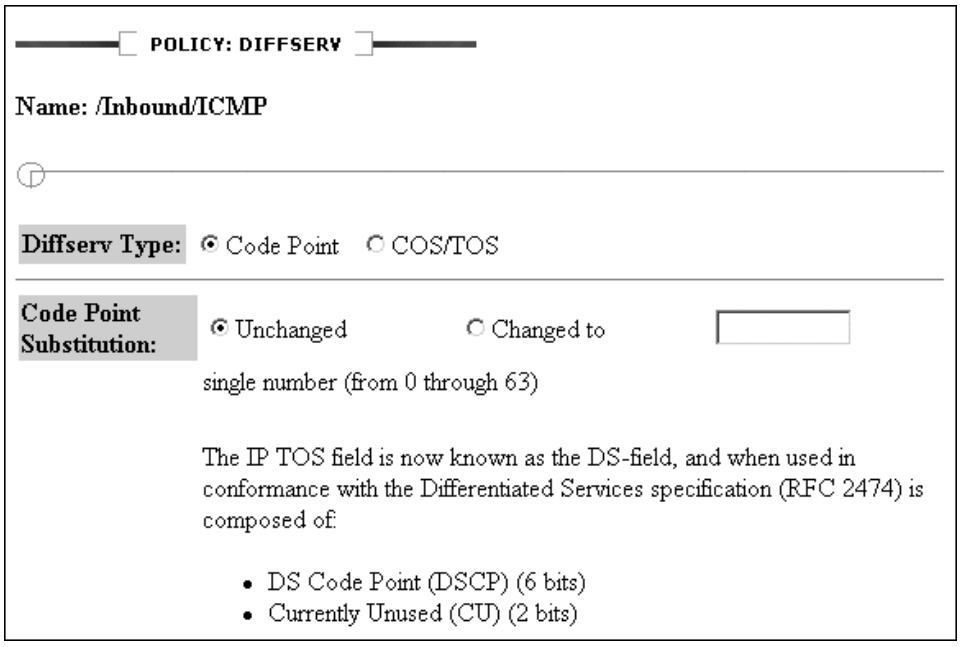


Fig. 4.14 Diffserv: Code point.

El campo Tipo de Servicio (TOS) en la cabecera IP es conocido como el campo de Servicios Diferenciados, así definió en la especificación de Servicios Diferenciados (RFC 2474). Este campo es dividido en los subcampos siguientes:

- Punto de Código de Servicios Diferenciados (DSCP) (6 bits). Entrar un valor desde 0 hasta 63.

- Actualmente sin uso. (CU) (2 bits)

4.7.6.2 COS / TOS.

Muchos protocolos hacen decisiones de la asignación de ruta basadas en el Tipo de Servicio (TOS) en el campo en la cabecera IP. Este campo es un indicador de la calidad de servicio que se espera.

El campo ToS contiene:

- El sub-campo precedente a IP, también conocido como el sub-campo Clase de Servicio (COS), el cual es un campo de 3 bits.

- El sub-campo Tipo de Servicio (TOS) que es campo de 4 bits.

- Bit sin uso que se configurar en cero.

Las aplicaciones configuran este campo, para decirle a los routers cómo priorizar los paquetes. Por ejemplo, la información de los algoritmos weighted fair queuing (WFQ)(WFQ) lo usan los routers.

Se puede decirle a PacketShaper que asocie estos bits precedentes de IP durante la clasificación de protocolos IP, después se aplican políticas específicas para manejar éstos tipos de tráfico. Por ejemplo, se puede aplicar una política que sustituye un valor de precedente diferente, así, se puede controlar la prioridad del paquete cuando alcanza al router.

En el campo precedente a IP (COS), se especifica el valor a asociar. Se introduce un valor de precedente de 0 a 7 (donde 7 son el precedente más alto), o un rango de valores.

PacketShaper puede verificar el campo Tipo de Servicio (TOS) en la cabecera IP para asociar en un nivel de servicio para una aplicación. Se debe seleccionar uno de los valores siguientes asociar:

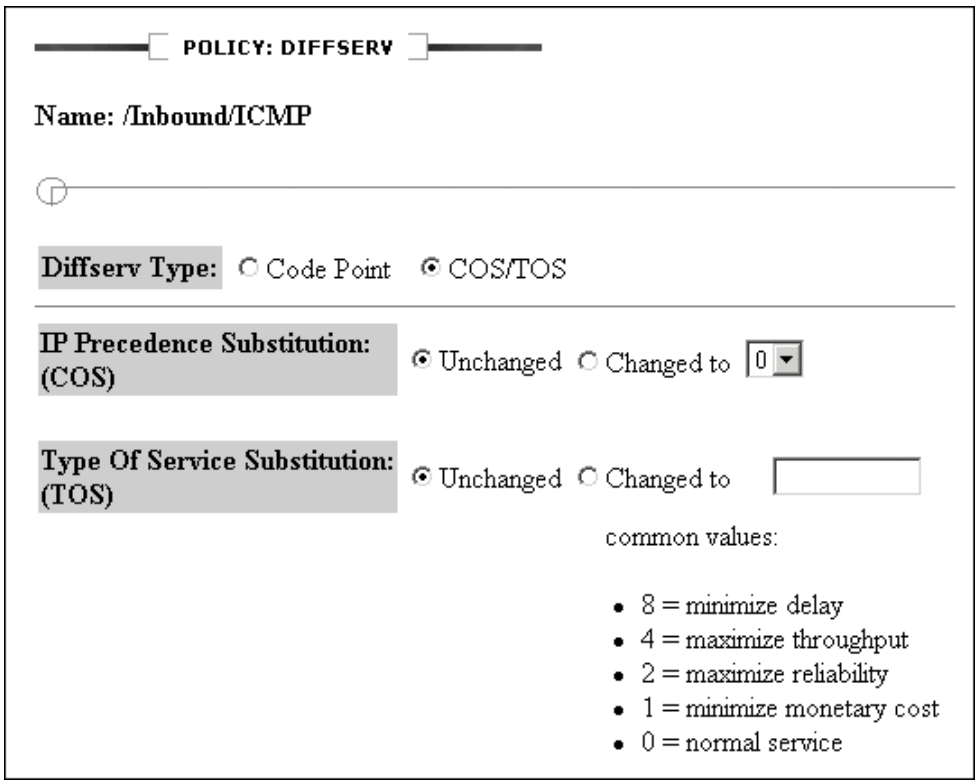


Fig. 4.15 Diffserv: COS / TOS.

- 8 = mínimo delay
- 4 = máximo throughput
- 2 = máximo reliability
- 1 = mínimo costo monetario
- 0 = normal service

Se podría asociar en el campo TOS, después, usar una política para cambiar el valor.

4.7.7 Clasificación MPLS.

Multiprotocol Label Switching (MPLS) es un método de enviar paquetes a una tasa alta de velocidad. Cuando los paquetes pasan por routers en el borde de la red, el router vincula una etiqueta que contiene información sobre el destino del paquete, ancho de banda, delay, la fuente de a dirección IP, número de socket de capa 4, y servicios diferenciados. PacketShaper puede clasificar tráfico basado en la etiqueta de MPLS. La implementación de MPLS de Packeteer está basada en RFC 3031 y 3032. Se puede crear una Regla de juego MPLS que está basado en:

- Una sola etiqueta MPLS (un numero entre 0 y 1048575)

- Un rango de etiquetas MPLS (por ejemplo, 250-350)

- Cualquier flujo de tráfico que tiene una etiqueta MPLS (especificar cualquiera en lugar de un número específico)

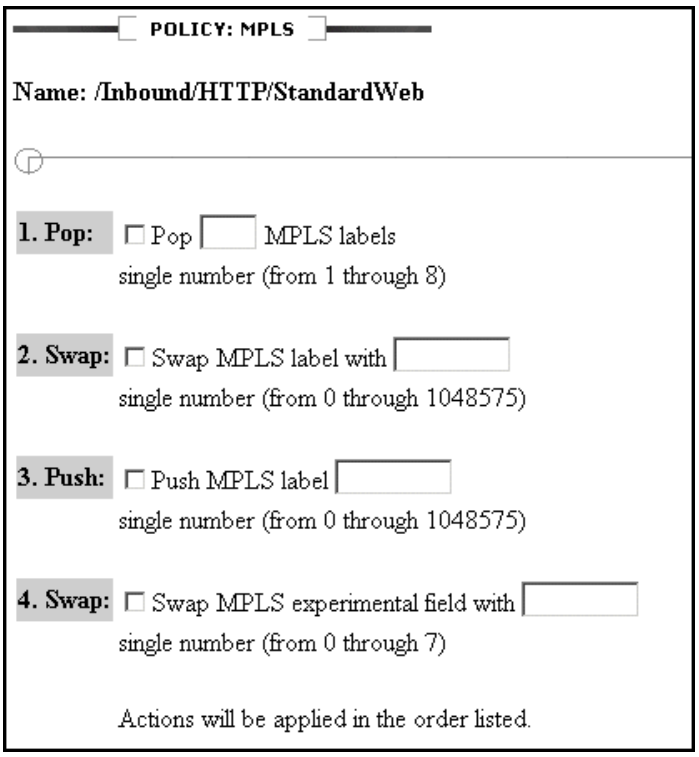


Fig. 4.16 Regla MPLS.

4.7.8 Identificación VLAN.

PacketShaper tiene la habilidad de clasificar tráfico de las aplicaciones dentro de LANs virtuales múltiples en un solo segmento de Ethernet (un conducto 802.1q) Para un ambiente de VLAN múltiple (donde paquetes que atraviesan la unidad tendrán más de una cabecera de VLAN), sólo la cabecera de VLAN extrema se usa para la clasificación. Las otras cabeceras se ignoran.

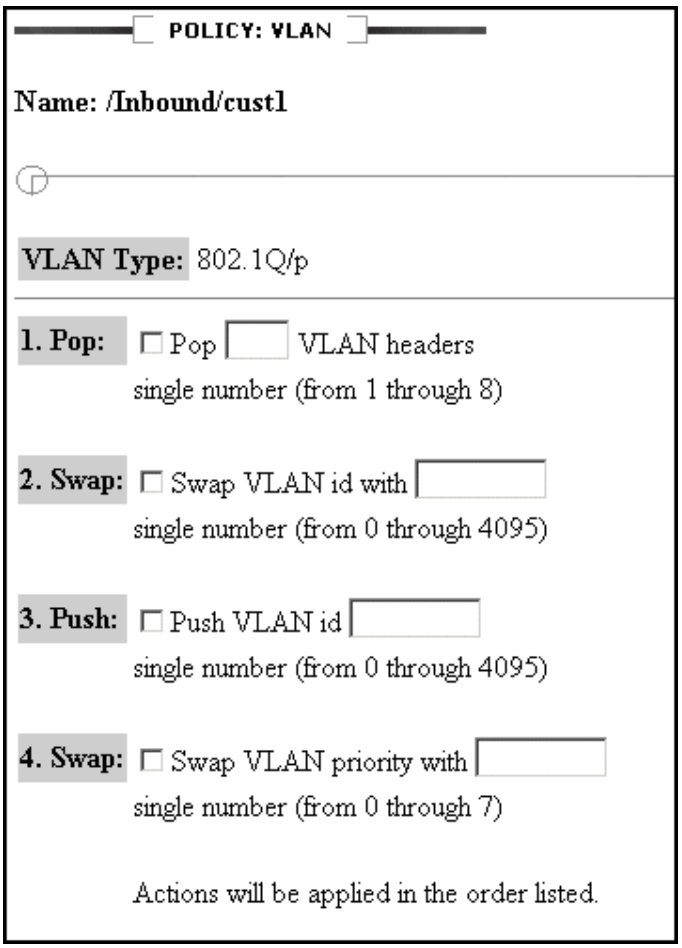


Fig. 4.17 Regla VLAN.

Se puede crear una regla de juego de identificación VLAN basada en:

- Una sola ID VLAN (un número entre 0 y 4095)

- Un rango de IDs VLAN (por ejemplo, 100-200)

- Cualquier flujo de tráfico que tiene una ID VLAN (especificar cualquiera en vez de un número especifico)

4.8 Gráficos de monitoreo.

En esta sección se describe todos los gráficos disponibles en la ventana de Statistics: Reports. (No disponible en el modelo 1200 de Packeteer.). Estos gráficos se agrupan en las categorías básicas siguientes:

- Ancho de banda en uso.

- Eficiencia.

- Top-10.

4.8.1 Ancho de banda en uso.

Existen seis tipos de gráficos: Utilización de clases, Partición dinámica, Enlace, Enlace con picos, Partición y Partición con picos.

4.8.1.1 Utilización de las clases.

El gráfico de utilización de clase muestra una historia del consumo promedio de ancho de banda de las clases en bits por segundo.

Este gráfico nos dice cuanto ancho de banda utiliza determinada clase, por ejemplo, la clase FTP.

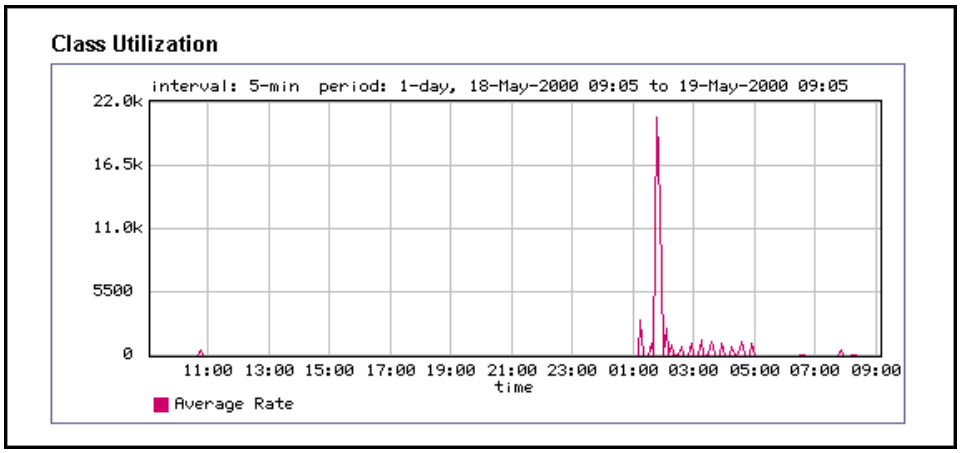


Fig. 4.18 Gráfico de utilización de clases.

Aunque la utilización del ancho de banda promedio sobre el tiempo también es desplegada en el gráfico de utilización de clase, las mismas figuras pueden parecer diferentes con el gráfico de Picos. Esto es porque la escala del gráfico cambia si hay una diferencia regular entre el promedio y figuras de los picos.

El ancho de banda promedio, sin picos, puede mostrar amplia capacidad, sobre todo cuando las unidades de tiempo más largas son moderadas. Verificando los picos, se puede ver si una clase de tráfico frecuentemente se está acercando al límite de capacidad.

4.8.1.2 Utilización de las clases con picos.

La utilización de la clase con gráfico de Picos despliega un promedio de clases de tráfico y consumo de ancho de banda pico, en bits por segundo, sobre el tiempo. PacketShaper determina la velocidad pico, mirando la velocidad por segundo registrada para el sub-intervalo más ocupado, es decir, el intervalo subalterno que tenía la velocidad más alta.

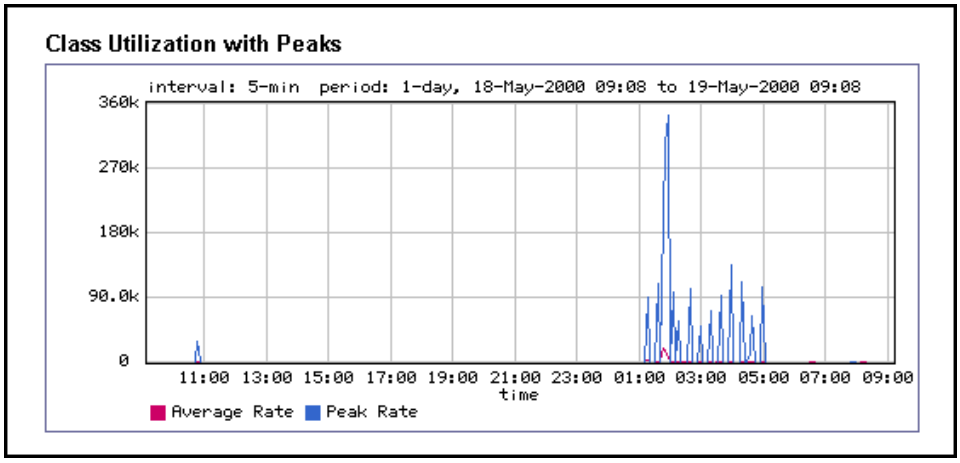


Fig. 4.19 Gráfico de utilización de clases con picos.

4.8.1.3 Partición dinámica.

El gráfico de uso de partición dinámico proporciona tres estadísticas que pertenecen a una partición dinámica particular:

- El número de usuarios activos, es decir, el número de sub-particiones activas.

- El número de sub-particiones que PacketShaper intentó crear después que el límite de la partición fue alcanzado.

- Número de sub-particiones dinámico que PacketShaper intentó crear pero no pudo porque el número de particiones en la unidad había alcanzado su límite. El número del máximo de particiones en una unidad depende del modelo. Por ejemplo, el Packeteer 4500 puede crear 256 particiones.

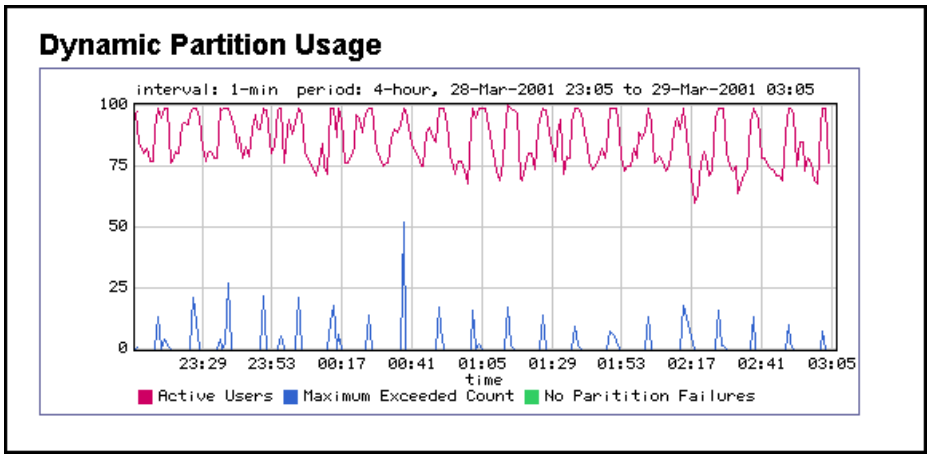


Fig. 4.20 Gráfico de utilización de las particiones dinámicas.

4.8.1.4 Enlace.

El gráfico de utilización del enlace muestra el uso de ancho de banda promedio del enlace en bits por segundo. Cuando se elige

desplegar el tamaño del enlace al crear el gráfico, una línea horizontal indica la capacidad del enlace.

Este gráfico dice si varía mucho el uso del enlace y cuales es la capacidad promedio que es necesario.

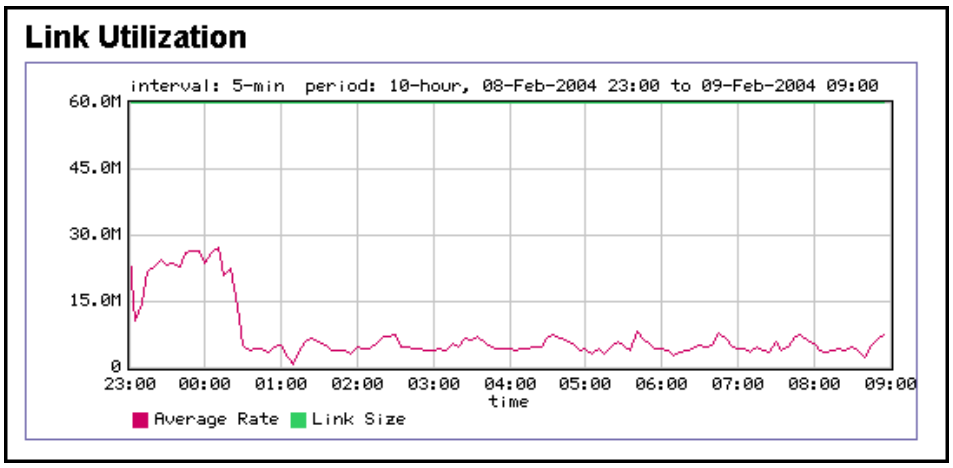


Fig. 4.21 Gráfico de utilización del enlace.

4.8.1.5 Enlace con picos.

El gráfico de utilización del enlace con picos muestra el ancho de banda usado promedio del enlace y uso pico en bits por segundo. PacketShaper determina la velocidad pico mirando la velocidad grabada para el sub-intervalo más ocupado, en segundos, es decir, el sub-intervalo que tenía la velocidad más alta.

Si se escoge desplegar el tamaño del enlace al crear el gráfico, una línea horizontal indica la capacidad del enlace. El gráfico puede determinar con que frecuencia el tamaño del enlace fue insuficiente y cuál es la capacidad promedio que es necesario.

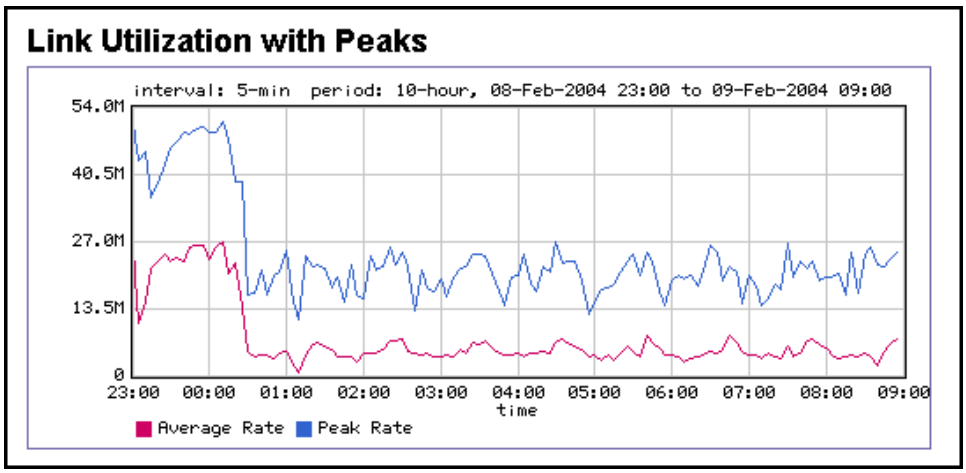


Fig. 4.22 Gráfico de utilización del enlace con picos.

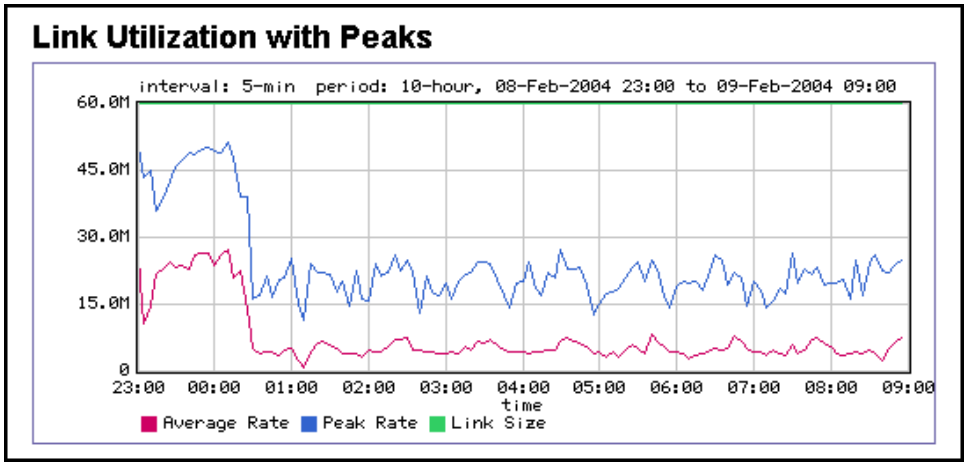


Fig. 4.23 Gráfico de utilización del enlace con picos burstable.

4.8.1.6 Partición.

El gráfico de utilización de partición muestra el uso del ancho de banda promedio de una partición en bits por segundo. Cuando se escoge desplegar el tamaño de la partición al crear el gráfico, las líneas horizontales indican el mínimo de la partición y límites de tamaño burstable. En el gráfico, la partición se cambió de no-burstable a burstable durante el periodo de tiempo que era graficado. Es fácil ver ese exceso de ancho de banda que se utilizó cuando la partición se hizo burstable.

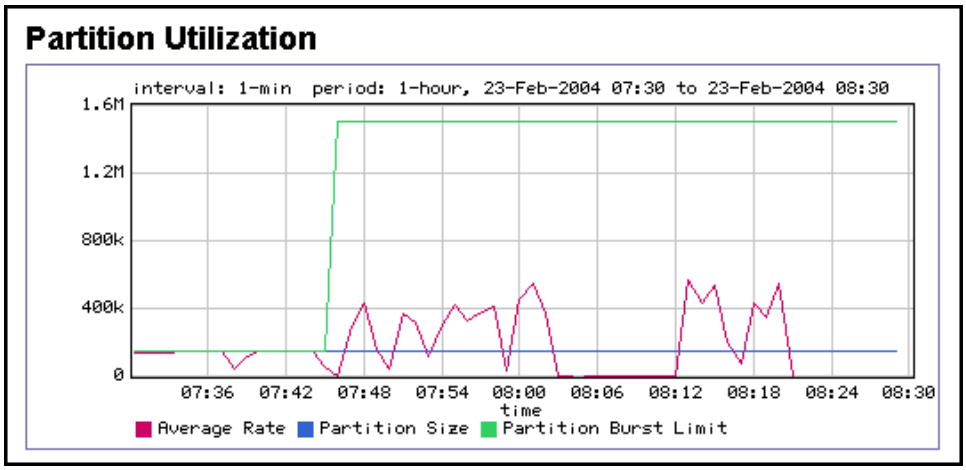


Fig. 4.24 Gráfico de utilización de una partición.

4.8.1.7 Partición con picos.

El gráfico de utilización de la partición con picos muestra el promedio de una partición y uso del ancho de banda pico en bits por segundo. PacketShaper determina la velocidad pico mirando

la velocidad grabada para sub-intervalo más ocupado, es decir, el sub-intervalo que tenía la velocidad más alta.

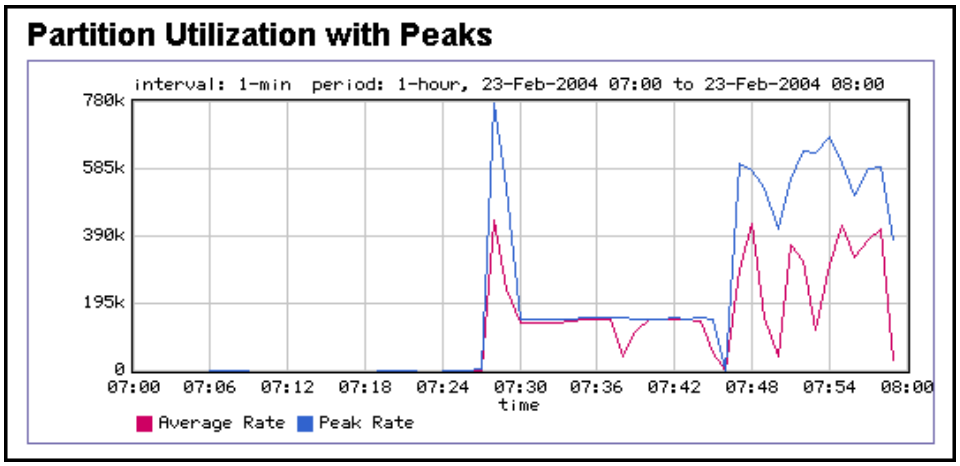


Fig. 4.25 Gráfico de utilización de una partición con picos.

Si se elige desplegar el tamaño de la partición que cuándo se crea el gráfico, las líneas horizontales indican el mínimo de la partición y límites de tamaño burstable (como mostrado debajo) Este gráfico puede indicar si la cantidad reservada es la partición que se necesita realmente. En la Fig. 4.25 se cambió de no-burstable a burstable durante el periodo de tiempo que era el graficado. Es fácil ver ese ancho de banda excedente se utilizó cuando la partición se hizo burstable.

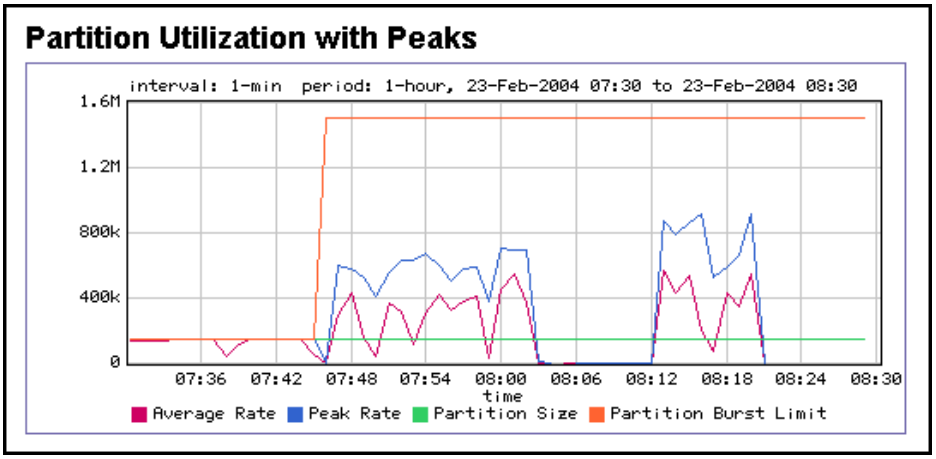


Fig. 4.26 Gráfico de utilización de una partición con picos burstable.

4.8.2 Análisis de eficiencia.

Existen cinco tipos de gráficos para medir la eficiencia: Bits transmitidos, Fallas de velocidad, Eficiencia de la red, Distribución del tamaño de los paquetes y Paquetes transmitidos.

4.8.2.1 Bits transmitidos.

Determina el volumen real, como número de gigabytes, que se transmiten en un periodo de tiempo para un enlace específico, partición, o clase. Además, compara el número de bytes transmitidos al número de bytes retransmitidos.

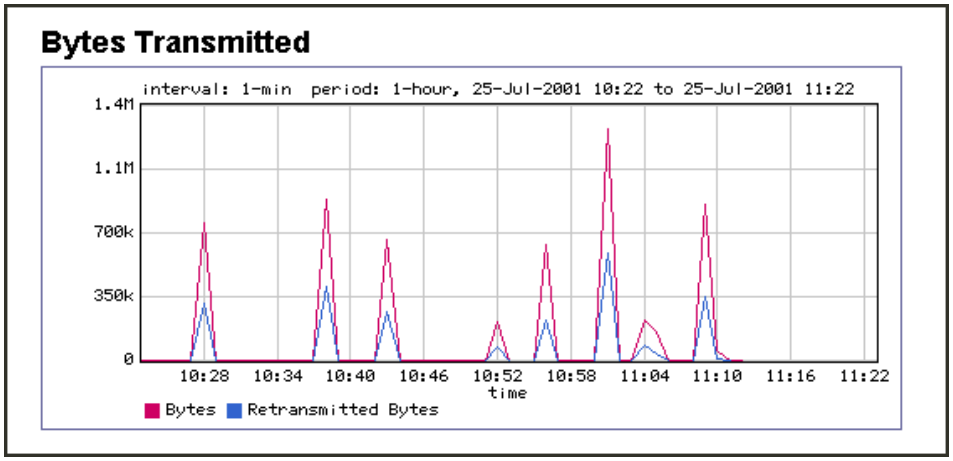


Fig. 4.27 Gráfico de bytes transmitidos.

4.8.2.2 Fallas de velocidad garantizada.

Ayuda a ver el número de tiempos que PacketShaper es incapaz de proporcionar el ancho de banda garantizado por la política de clase; permitiendo analizar la efectividad de una política. Si la clase seleccionada no tiene una velocidad garantizada asociada, el gráfico muestra ceros.

Si este gráfico muestra un aumento inaceptable en fallos de velocidad, puede ser por los motivos siguientes:

- Garantía de velocidad inapropiada.

- Tener un número imprevisto de flujos.

- La partición no ofrece una garantía para trabajar apropiadamente.

- La política de admisión de control no esta configurada adecuadamente.

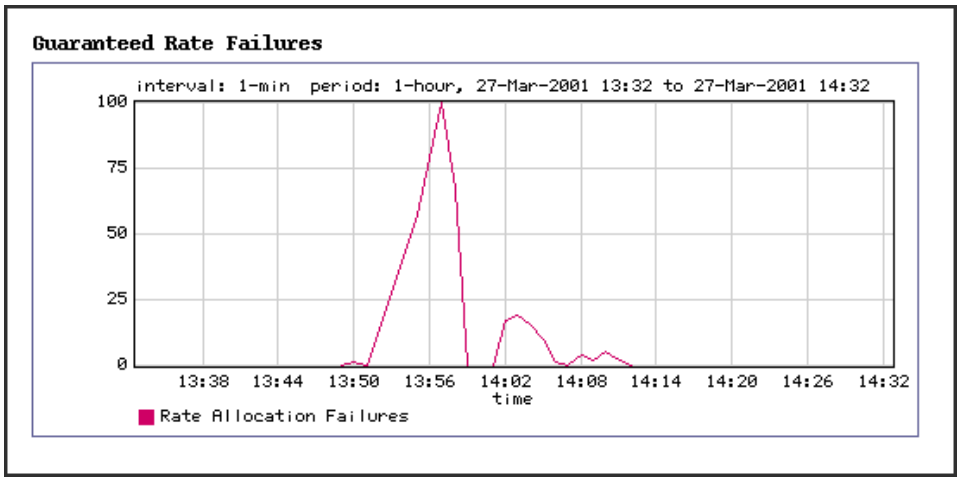


Fig. 4.28 Gráfico de fallas de velocidad garantizada

4.8.2.3 Eficiencia de la red.

Ayuda a ver qué porcentaje de tráfico TCP de la red se dedica a retransmisiones de paquetes. De hecho, este gráfico muestra el porcentaje de paquetes que no son retransmitidos. Por ejemplo, si la eficacia de la red es 90%, entonces 10% de los paquetes son retransmisiones.

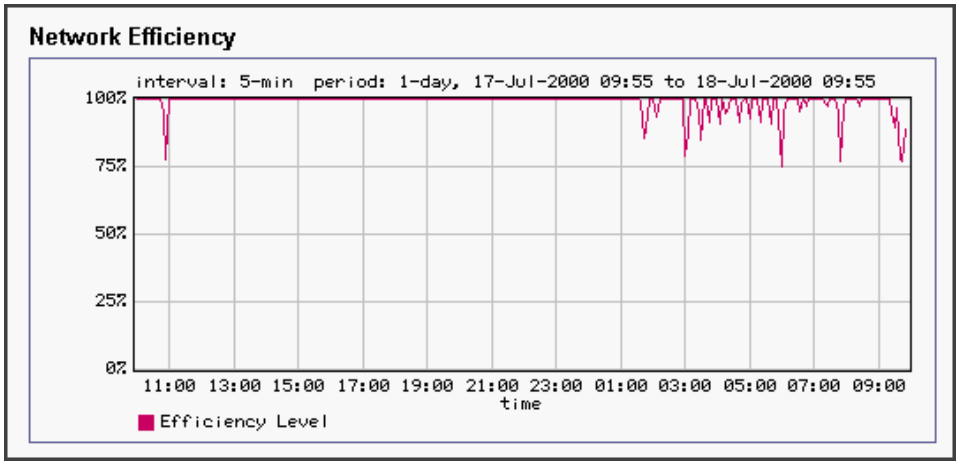


Fig. 4.29 Gráfico de eficiencia de red.

El gráfico de eficacia de red puede ayudarle a descubrir tendencia a errores. Los paquetes descartados y retransmitidos bajan el porcentaje de eficiencia. Una red eficiente, desplegada con fluctuaciones menores de 100%, necesita pocas intervenciones. Un porcentaje más bajo indica que un gran porcentaje de capacidad de la red es por retransmisiones. En este caso, se debe reevaluar las particiones y políticas actuales.

4.8.2.4 Distribución del tamaño de los paquetes.

El gráfico de distribución del tamaño de los paquetes es un histograma de paquetes recibidos en el enlace Inbound u Outbound, en siete bloques con rangos diferentes. Los rangos del tamaño de los paquetes, en bytes, incluyen: [0-63], [64-127], [128-255], [256-511], [512-1023], [1024-1517], [>=1518] En el ejemplo

de la Fig. 4.30, aproximadamente se recibieron 340,000 paquetes que estaban en el bloque "127", es decir, el rango del tamaño de 64-127 bytes.

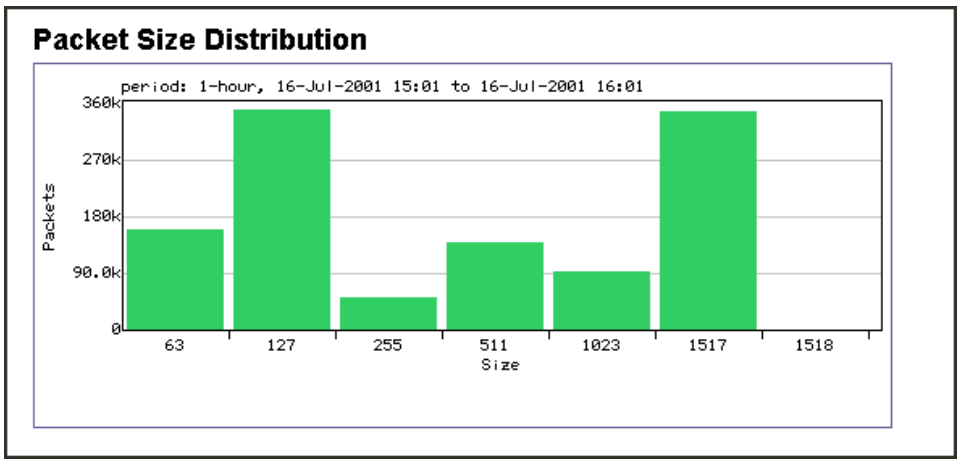


Fig. 4.30 Gráfico de distribución

4.8.2.5 Paquetes transmitidos.

Determina la causa de un retraso de la red. Compara el mapa de los paquetes transmitidos de la clase correspondiente o mapa de utilización del enlace para determinar si un enlace o clase está desbordándose por paquetes pequeños. El desbordamiento de paquetes pequeños reduce la velocidad a la que se transmiten paquetes de mayor tamaño, lo que podría reducir la velocidad la red.

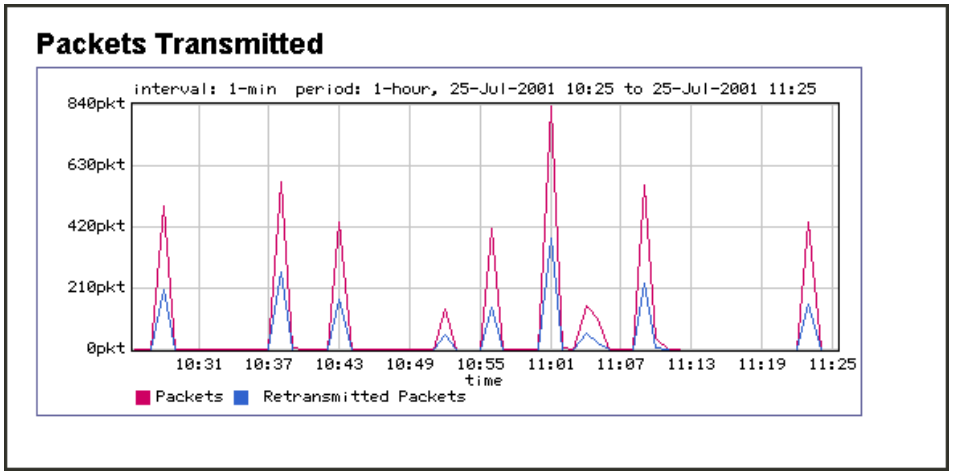


Fig. 4.31 Gráfico de paquetes transmitidos.

4.8.3 Gráficos para analizar el Top Ten.

Existen tres tipos de gráficas: Para Particiones, Clases y Clases hijos.

4.8.3.1 Las particiones Top 10.

El gráfico Top-10 de las particiones, es un plano del pastel que muestra las porciones relativas de ancho de banda asignado a las diez particiones más activas, asociadas con la clase seleccionada o sus descendientes. Este gráfico despliega el promedio de ancho de banda de cada partición usado, en bits por segundo, y el porcentaje de ancho de banda total usado por el grupo.

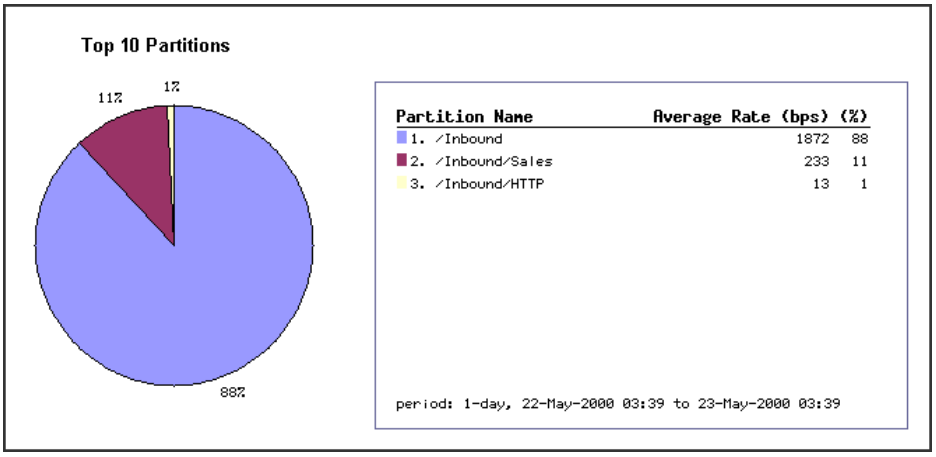


Fig. 4.32 Gráfico de las particiones Top-10

4.8.3.2 Las clases Top 10.

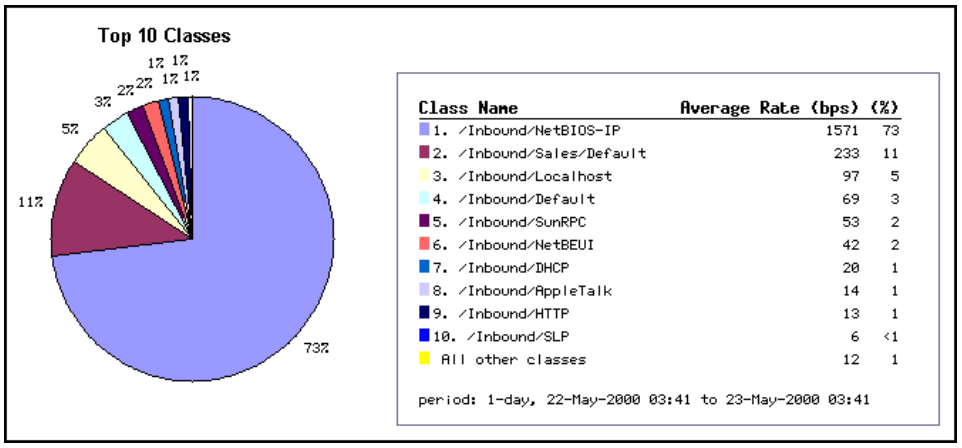


Fig. 4.33 Gráfico de las clases Top 10.

El gráfico Top 10 de las clases, es un mapa de pastel que muestra las porciones relativas de ancho de banda asignado a las diez clases más activas asociadas con la clase seleccionada y todos sus descendientes. Este gráfico despliega el ancho de

banda promedio de cada clase usado, en bits por segundo, y su porcentaje del ancho de banda total usados por el grupo.

4.8.3.3 Las clases hijos Top 10.

El gráfico Top 10 de las clases hijos, es un mapa del pastel que muestra las porciones relativas de ancho de banda asignado a las diez clases hijo más activo de la clase padre seleccionado. Este gráfico es similar al gráfico Top 10, excepto que este despliega los hijos directos solamente, mientras que el gráfico Top de las clases muestra las clases hojas, es decir, de las que no tienen ningún hijo propio. En otras palabras, el gráfico Top 10 de clases de los hijos le permite graficar un hijo, sin nietos.

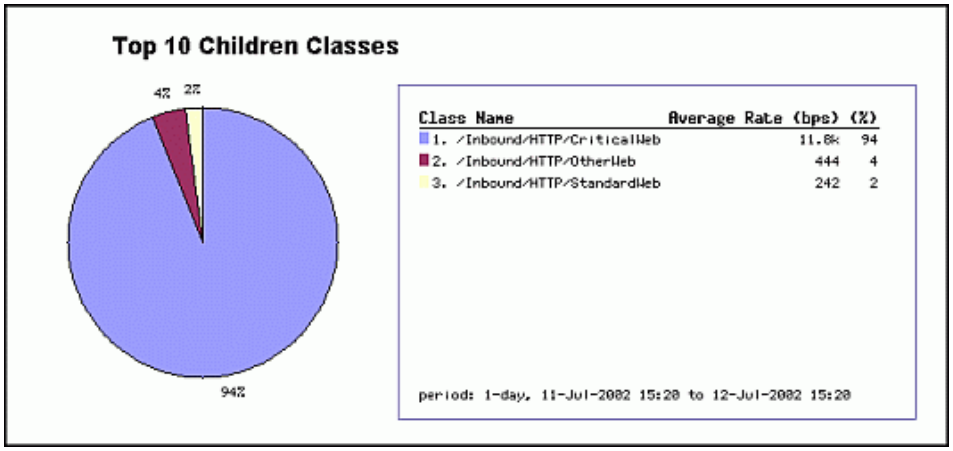


Fig. 4.34 Gráfico de las clases hijos Top 10.

CAPÍTULO 5.

APLICACIÓN DEL PACKETSHAPER EN UN ISP.

5.1 Ubicación del equipo.

En la figura 5.1 se muestra la infraestructura general de un ISP, y la ubicación del equipo, el PacketShaper.

La red de acceso hacia los clientes puede ser por líneas conmutadas o dial-up, líneas dedicadas y líneas ADSL.

La red de distribución está situada en el borde de la red de datos. Tiene como función concentrar las conexiones de los clientes, conmutados y dedicados, en los puntos de presencia del proveedor.

La red troncal o Core tiene las funciones de concentrar el tráfico procedente de las redes de acceso y distribución, e interconectar a otras redes y proveedores de tránsito.

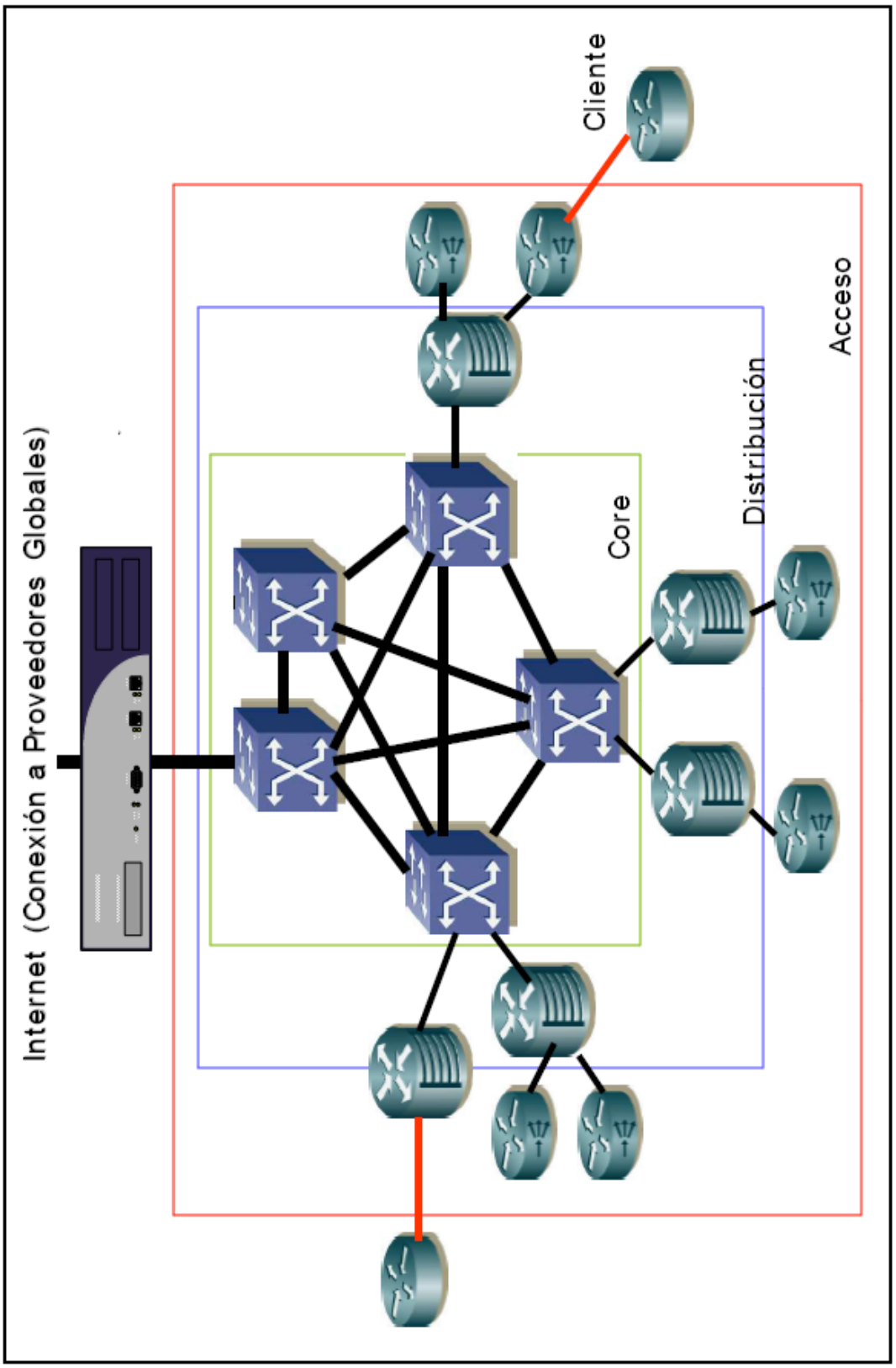


Fig. 5.1 Ubicación del PacketShaper en un ISP

5.2 Asignación de ancho de banda.

PacketShaper ISP controla asignación por cliente, por usuario, por grupos de usuarios, por-sesión, y/o por base de servicios. Este control se traduce en un servicio de administrador de ancho de banda obligado y fácil.

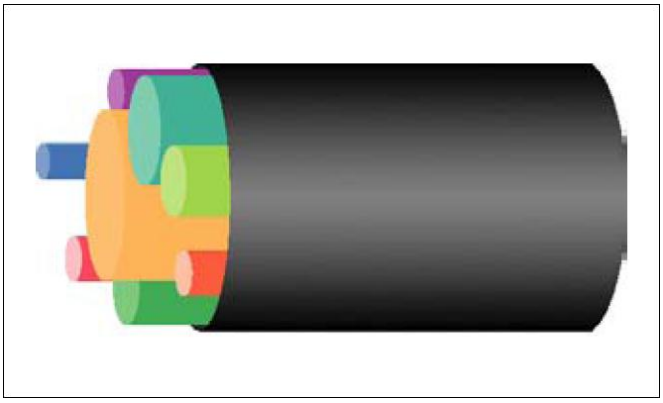


Fig. 5.2 Asignación virtual del ancho de banda.

5.2.1 Asignación por cliente.

Las particiones de PacketShaper ISP permiten crear un tubo separado virtual para cada cliente (u otros subconjuntos). Las particiones funcionan semejantemente a los PVCs de Frame Relay, pero con el importante beneficio agregado de compartir su ancho de banda excedido sin usar con otro tráfico. Uno especifica el tamaño del enlace reservado, decide si puede expandirse, llamado bursting, y opcionalmente el límite de su crecimiento. Además, se puede encajar

particiones con otros, llamadas particiones jerárquicas, para control más fino. Con una partición, un cliente tiene siempre acceso a su cantidad definida de ancho de banda, no importa que los otros clientes estén activos. Si hay exceso y está disponible, entonces el cliente puede tener más ancho de banda, arriba del límite de su partición. Una partición no protege a los usuarios individuales o sesiones unos de otros.

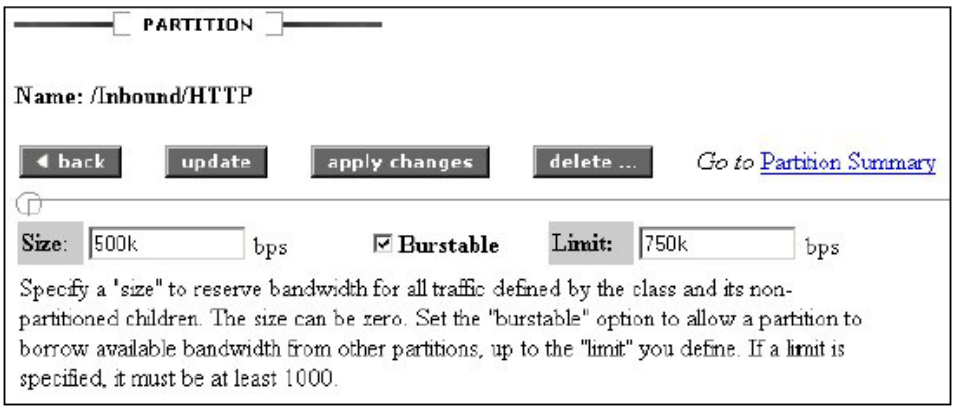


Fig. 5.3 Asignación por cliente

Ideas de servicio:

- Reservar la proporción contratada de 512 Kbps para un nuevo cliente sin preocuparse que otros lo usurparán, a menos que el nuevo cliente no está usándolo y está disponible.

- Para cuentas más pequeñas, no se le permite a un cliente consumir más de su cantidad base de 512 Kbps.

- Para una actualización de cuentas, se permite a un cliente expandirse más de su cantidad base cuando el ancho de banda está disponible de 512 Kbps a 1 Mbps, por ejemplo.

- Aumentar la cantidad base del cliente o limitarla para una cuenta actualizada adicional.

- Ofrecer un nivel de servicio escalonado a los clientes. Por ejemplo:

  Plan Bronze: Outbound fijado en 64 Kbps; Inbound fijado en 64 Kbps.

  Plan Silver: Outbound fijado en 128 Kbps; Inbound fijado en 256 Kbps.

  Plan Gold: Outbound fijado en 128 Kbps; Inbound fijado en 728 Kbps.

  Plan Gold Plus: Outbound mínimo de 384 Kbps con un máximo de 512 Kbps; Inbound mínimo de 1024 Kbps con un máximo de 1.5 Mbps.

- Limitar las obligaciones para los servicios promocionales.

- Dar libertad o reducir el precio de los servicios para clientes selectos, escuelas o las bibliotecas públicas por ejemplo. Aunque se desea continuar entregando estos servicios, no se desea que ellos impacten el ancho de banda con cuentas llenas de clientes. Priorizando acceso al ancho de banda disponible excedente, se puede dar una parte a una biblioteca pública pero controlando el acceso basado en la necesitad de otros en ese momento.

5.2.2 Asignación por grupos.

PacketShaper ISP permite controlar la asignación del ancho de banda para cada usuario o cada grupo de usuarios. Éstos características de control pueden usarse en adición a técnicas por cliente o de manera exclusiva.

Las sub-particiones dinámicas por usuario de PacketShaper ISP son una solución ideal para las situaciones donde un cliente se preocupa más de la asignación equitativa de ancho de banda que sobre cómo ponerla en uso. Las sub-particiones dinámicas se crean ligeramente como tráfico inicial de usuarios de una clase dada. Cuando el número

del máximo de sub-particiones se alcanza, un slot inactivo se suelta para cada nuevo usuario activo. De otra manera, se escoge si se rechazan a los rezagados o se los comprimen en un área del desbordamiento.

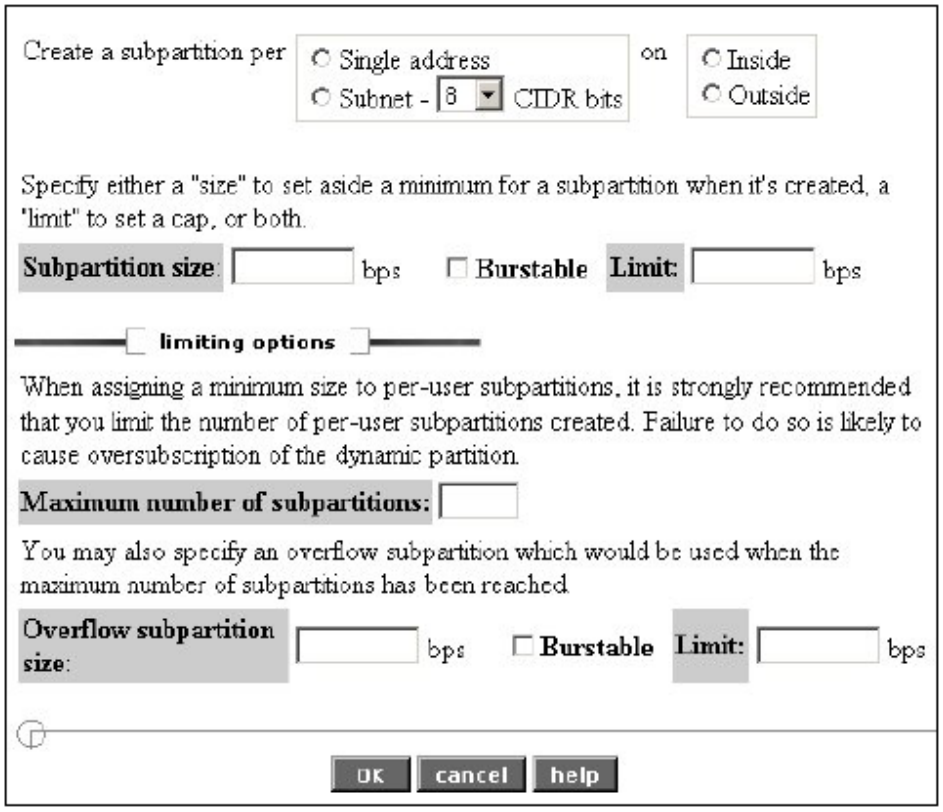


Fig. 5.4 Asignación por grupos.

Las sub-particiones dinámicas simplifican grandemente las cabeceras administrativas y permiten una sobre suscripción. Es tan fácil controlar a 5,000 usuarios si fueran solamente uno. Como siempre, PacketShaper ISP presta cualquier ancho de banda sin uso

a otros clientes que lo necesiten. Además, estos mismas sub-particiones pueden crearse para un grupo de usuarios dentro de un rango de direcciones IP.

Ideas de servicio.

- Ofrecer un servicio para las instituciones educativas donde cada estudiante del dormitorio recibe un mínimo de 20 Kbps y un máximo de 60 Kbps para usarlo en cualquier forma que é/ella lo desee.

- Asignar ancho de banda equitativamente a cada ocupante con facilidad de compartir. Si hay mucha actividad, ellos obtienen porciones iguales más pequeñas. Si hay menos actividad, ellos obtienen porciones iguales más grandes.

- Reforzar la tasa contratada por usuario, sea inalámbrica o cable. Limitar cada usuario Bronze en 100 Kbps, cada usuario Gold en 150 Kbps, y cada usuario Platinum en 200 Kbps. O implemente cualquier número de otros esquemas.

- Crear un servicio donde se protege y/o limita el Ancho de banda para los distintos departamentos dentro de una

compañía, por ejemplo contabilidad, recursos humanos, mercadeo, y así sucesivamente.

5.2.3 Asignación por servicio / sesión.

Para los proveedores de servicio de ancho de banda que han expandido sus servicios para incluir unos pocos servicios del ancho de banda enfocados por aplicación. Por ejemplo, proveer a un cliente corporativo que también hace uso de sesiones de WebEx (un facilitador de encuentros online), para los encuentros de campo distribuidas. Ofrecer un servicio que se adapte de las necesidades de ancho de banda del tráfico WebEx, usando PacketShaper ISP para reforzar las características apropiadas y asegurar el funcionamiento de WebEx.

5.2.3.1 Control por sesión.

Cuando se asigna ancho de banda modelado para un servicio específico basado en aplicaciones, las políticas de tasa de velocidad de PacketShaper ISP son muy útiles, especialmente cuando se combina con una partición. Una política de tasa de velocidad limita o garantiza ancho de banda a cada sesión individual de una clase de tráfico, manteniendo al tráfico ansioso en línea y protege aplicaciones sensibles a la latencia. Una política controla el tráfico para cada

sesión de cada aplicación separadamente, en vez de controlar todo el tráfico de todos los usuarios juntos. Se especifica un mínimo garantizado de tasa de velocidad y/o dar prioridad a las sesiones accediendo a más ancho de banda, si está disponible.

Ideas de servicio.

Las siguientes ideas de servicio combinan algunas características de distribución de ancho de banda:

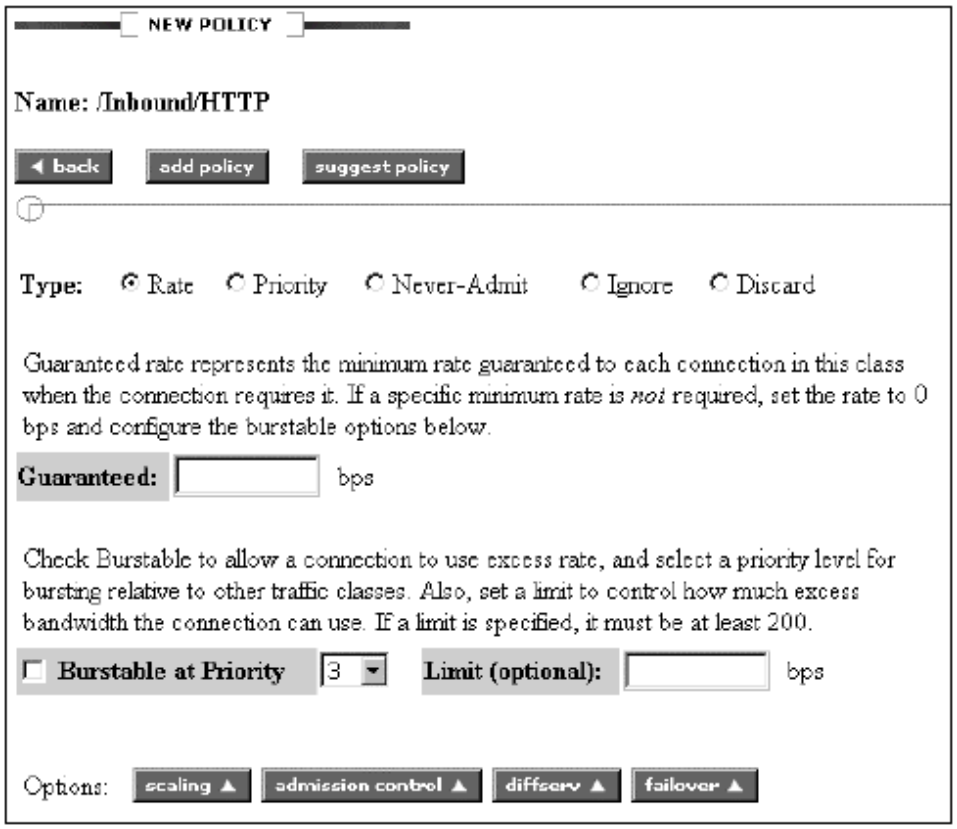


Fig. 5.5 Asignación por sesión.

- Descargas de música:

  Crear un servicio para descubrir descarga de música, limitándolos a un 10 por ciento de la capacidad de la red del cliente, e impídale a un amante de música de alta capacidad dominar todo. Dejar el restante 90 por ciento para todos los otros usos.

- Voz sobre IP.

  Ofrecer un paquete de VoIP que reserve el 20 por ciento de capacidad de la red para todo el tráfico de la voz, dar 24 Kbps a cada sesión de VoIP para evitar jitter y estática, y remitir a los rezagados a un mensaje cortés durante el periodo de la alta demanda.

- Canales multimedia.

  Crear un servicio para asegurar funcionamiento uniforme para canales multimedia, asignando precisamente la mínima tasa de velocidad bits por segundo requerida para una buena recepción.

- Juegos.

  Se da la opción al cliente de impedir juegos como Unreal Tournament, Quake, Doom, Mythic, y Diablo desde cualquier entrada del ancho de banda del cliente.

5.3 TCP Rate Control.

TCP Rate Control patentado de Packeteer es un mecanismo para evitar la congestión, para asegurar el funcionamiento a tiempo. Sobrepone las limitaciones de TCP, proactivamente previene la congestión del tráfico entrante y saliente. TCP Rate Control le dice a las estaciones finales reducir la tasa de velocidad, así que el envío de paquetes, a cualquier tasa de velocidad, será aceptado una vez que ellos lleguen. En lugar de desechar paquetes de una cola congestionada, TCP Rate Control marca el paso de los paquetes para prevenir congestión. Ejecuta una tasa uniforme de velocidad de flujo que maximiza el throughput. TCP Rate Control mide la latencia de la red, prevé tiempos de la llegada de paquetes, ajusta el tamaño ventana TCP clasificándolo acordemente, y reconoce los acuses de recibo para asegurar entrega a tiempo de las transmisiones.

Ideas de servicio.

Ofrecer los beneficios TCP Rate Control en su paquete de servicio standard como un diferenciador de la competencia ó para incluirlo como una mejora. El control de tasa de velocidad es un servicio agregado que mejora el throughput global y reduce retransmisiones.

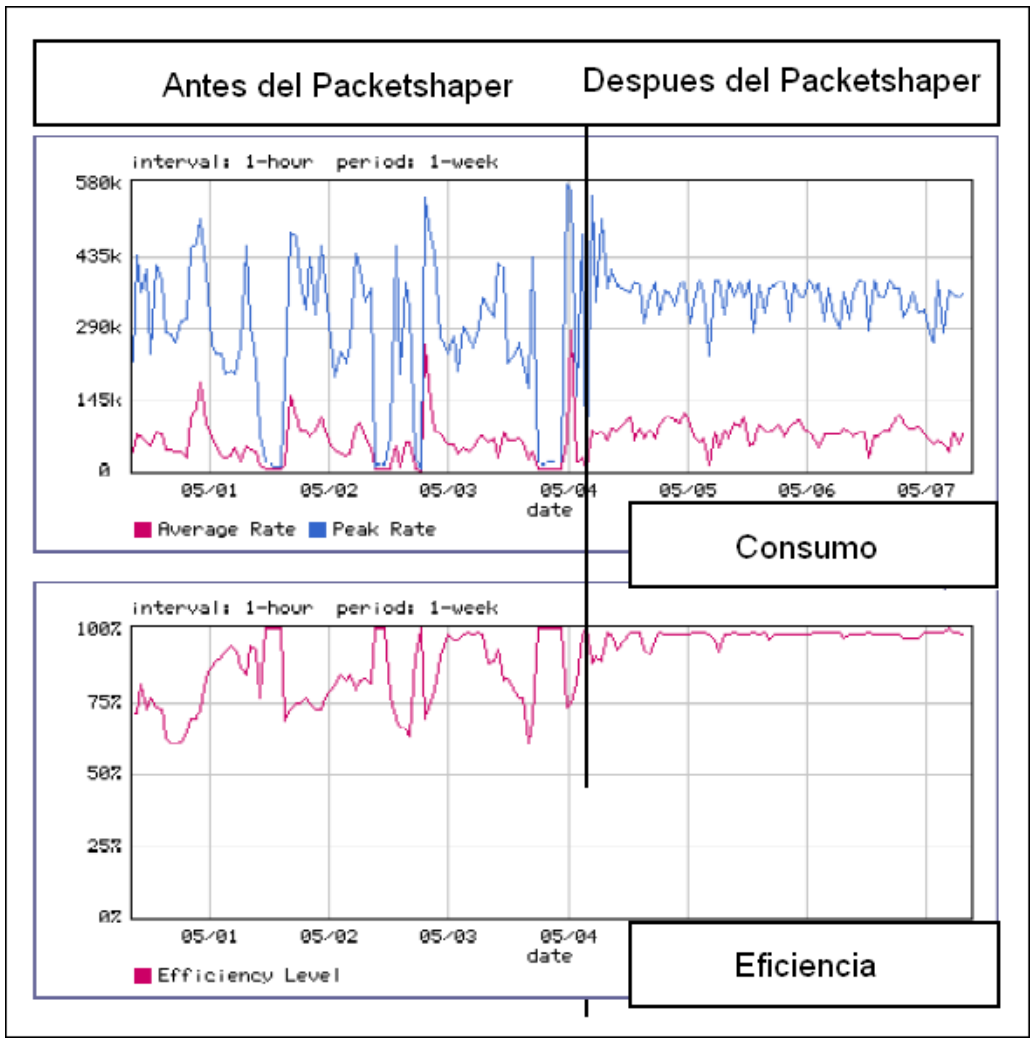


Fig. 5.6 TCP Control Rate.

5.4 Utilidad de los gráficos.

PacketShaper ISP analiza tráfico de la red cuando está pasando y acumula métricas relevantes para uso posterior. Se puede importar métricas dentro de reportes para terceros, facturar paquetes o verlos en un formato más intuitivo, en la colección de gráficos de PacketShaper ISP, tablas, e informes. Cuando se está integrando métricas de situaciones múltiples, Packeteer ReportCenter ofrece informes integrados.

El compromiso de un nivel de servicio, validado se convierte en parte del contrato. Prometer es fácil. Pero midiendo el servicio actual entregado es la única manera de comparar que lo prometido es realidad. La mediación proveedor-cliente, en gran parte, está basada en la habilidad de poder demostrarlo. PacketShaper ISP rastrea los promedios y el nivel de tráfico de pico, identifica usuarios que están conectados y las aplicaciones, además evalúa la eficacia de la red. Los gráficos y estadísticas pueden ayudar a reasegurar que clientes están obteniendo por lo que ellos pagan, ayudando a rastrear el progreso de los clientes y diagnostico de problemas.

5.4.1 Validación.

Un gráfico del promedio de tasa sobre el tiempo muestra a los clientes su imagen real del consumo. Si un cliente teme que no está obteniendo el ancho de banda que está pagando, se debe asegurar que ellos vean su uso pico, no sólo del promedio.

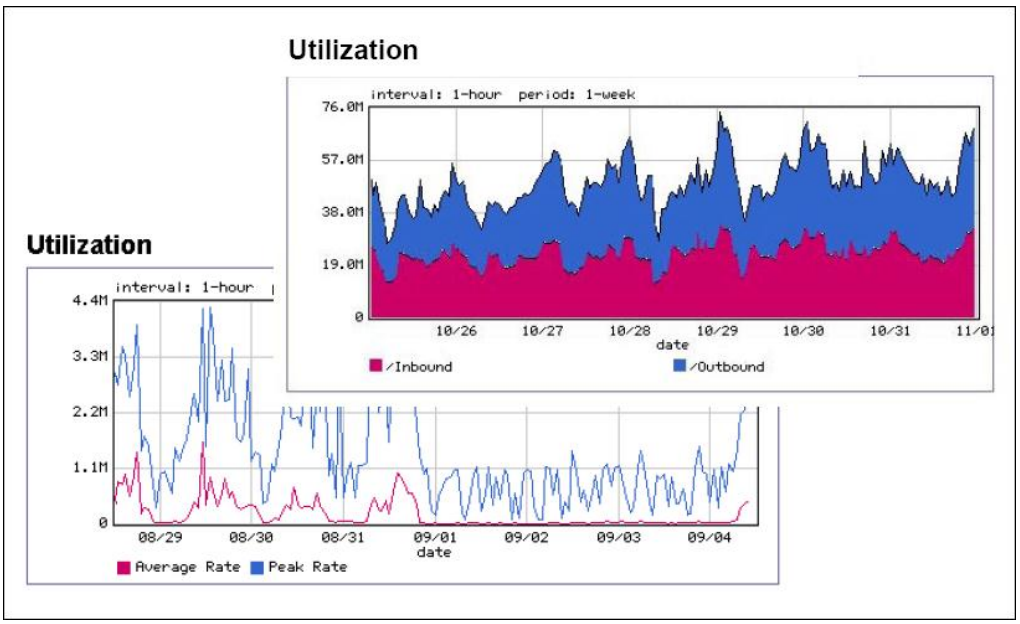


Fig. 5.7 Gráfico de consumo.

5.4.2 Asistente de ventas.

Si el gráfico de utilización de un cliente muestra que frecuentemente está usando todo su ancho de banda asignado, se requiere una actualización. Las gráficas de utilización de PacketShaper ISP traza la cantidad adquirida de ancho de banda del cliente con la cantidad

usada actualmente. Si el uso permanece cerca del límite comprado, es tiempo para vender una tasa más alta o más servicios.

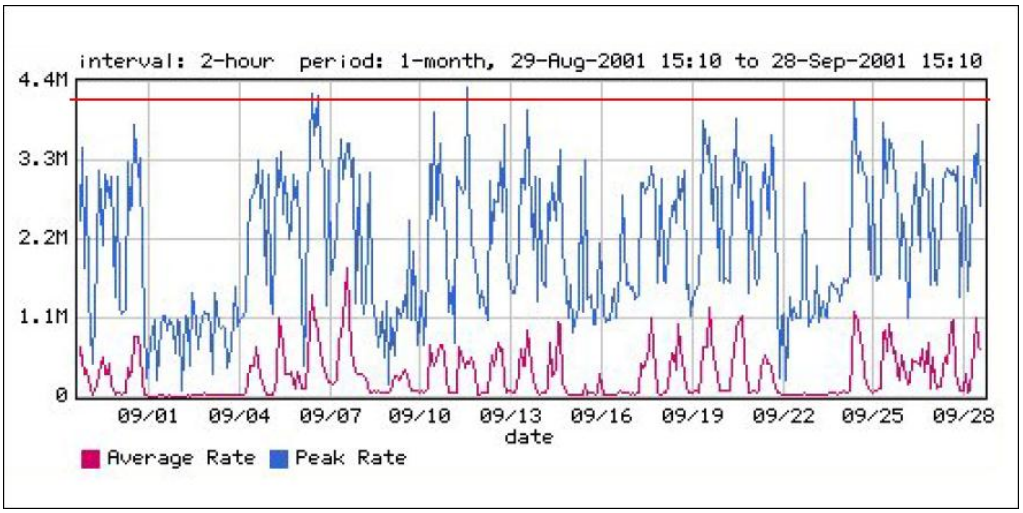


Fig. 5.8 Gráfico de máximo consumo.

5.4.3 Planificación de la capacidad.

Los gráficos de PacketShaper ISP pueden ayudar a descubrir la carga de la red y sus tendencias. Por ejemplo, un gerente del edificio desea dar una cantidad fija de ancho de banda a cada uno de sus 80 oficinas, por ejemplo 50 Kbps. En la planificación se debe considerar los siguientes aspectos:

- Número de oficinas/usuarios activos al mismo tiempo.

- Los tiempos pico.

- La cantidad que necesita comprar este gerente. ¿Debe ser (80 * 50 Kbps)? ¿La mitad cantidad suficiente? ¿Que decir sobre las dos terceras partes?

Un gráfico como el uso de particiones dinámicas de PacketShaper ISP podría contestar estas preguntas y podría mostrar el número de particiones en uso en cualquier momento dado.

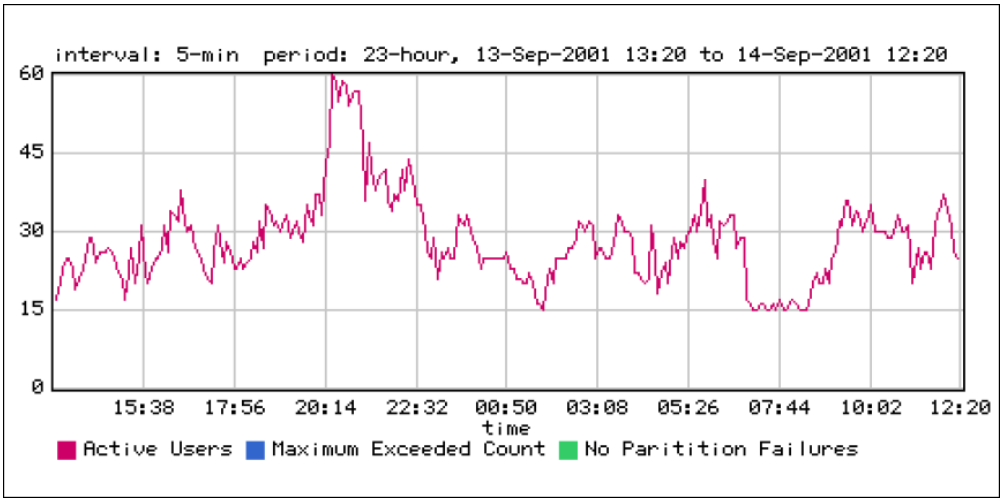


Fig. 5.9 Gráfico de particiones dinámicas.

5.4.4 Facturación.

Las métricas de PacketShaper ISP pueden ser usadas con una variedad de productos de facturación en el mercado. Se puede elegir una estructura de facturación de tarifa plana o variable, o estructura

de facturación basado en el consumo, PacketShaper ISP ayuda a asegurar que los cargos sean precisos.

5.4.4.1 Facturación de tarifa plana.

Muchos proveedores permanecen con una estructura de facturación de tarifa plana porque es más simple y fácil. Cuando se usa una estructura de tarifa plana, es común que algunos clientes usan mucho más ancho de banda de lo que ellos están pagando. Con asignación precisa, basado en las políticas de asignación de PacketShaper ISP, se da fuerza al uso al conformar los límites contratados.

5.4.4.2 Facturación basada en el SSO.

Los paquetes de facturación sólo son tan eficaces como los datos que usan. Por ejemplo, si se proporciona un software de facturación de las estadísticas, por sitio, mes, entonces esa es la magnitud de la flexibilidad de facturación. Con PacketShaper ISP, se puede proveer el uso y otras métricas basadas por cliente, usuario, servicio.

La característica de cálculo de host de PacketShaper ISP ofrece cálculo de bytes de throughput para cada dirección IP, grupo de usuarios en una lista de hosts, uno o más clases de tráfico, o subnet. Ésta es una característica importante, puesto que permite:

- Facturación departamental. Recursos humanos y marketing lo usan mucho.

- Facturación basada en cuotas. Un precio para un nivel de uso, un precio más alto para más consumo.

- Facturación basada en el nivel de servicio. El servicio Gold paga más que el servicio Silver por el mismo uso.

- Facturación flexible de grupos. (Agrupar individualmente usando figuras dentro de un grupo total)

- Cortar y sacarlos, (después que un usuario prescrito excede el ancho de banda, el accedente es bloqueado)

Las características de integración de PacketShaper ISP alimentan las métricas a los paquetes de facturación existentes. Una vez

que los ingresos del proveedor se unen a los resultados, la confianza del cliente se incrementa con el tiempo con retención del cliente. Los clientes sabrán que esos cargos son calculados en más que buenas intenciones.

5.5 Detección y protección de ataques.

Aunque PacketShaper ISP no es un firewall, ayuda a descubrir los ataques DOS (denegación de servicio) y reducir su impacto.

Estos ataques insidiosos emplean una variedad de mecanismos que producen estragos en una red. Por ejemplo, los ataques tipo desbordamiento inician un número grande de conexiones ilegítimas que consumen ancho de banda inundan los hosts receptores.

PacketShaper ISP emplea una variedad de métodos para ayudar a tratar con los ataques. Puede limitar el número de conexiones desde o a cualquier host. O limitar la cantidad de tráfico ICMP, un frecuente vehículo del ataque que normalmente contribuye con un porcentaje pequeño de tráfico, limita el número de flujos en una aplicación o clase de tráfico. Descubre y bloquea SQL Slammer, Blaster, y gusanos similares. O bloquea tráfico que está pretendiendo venir de una fuente confiada.

Algunas ideas para protección extra contra complicaciones de DOS incluyen:

- Limitar la tasa de nuevos flujos o de un único host.
- Poner un límite en el número de flujos concurrentes para una clase de tráfico.

- Limitar ICMP a un máximo de 5 por ciento del tamaño del enlace.

- Bloquear o limitar el tráfico en un puerto reservado para una blanco común del DOS. Por ejemplo, bloquear el puerto 1434 si usted no tiene servidores del SQL. De esta manera, se limita el flujo y la capacidad del ancho de banda para prevenir infecciones de los servidores que bloquean la red enteramente.

- Bloquear el tráfico que lleva las muestras indicadoras de gusanos actuales.

5.6 Optimizando el desempeño de MPLS.

MPLS (Multiprotocol Label Switching) es una tecnología basada en normas que puede mejorar el desempeño de la red y calidad de servicio (QoS) para el tráfico selecto. MPLS ofrece clases múltiples de servicio, cada uno asociado con diferentes tipos de tráfico. Por ejemplo, las aplicaciones críticas de una empresa, como Oracle, podría estar en una clase de servicio Gold, las aplicaciones menos importantes podrían estar en un servicio de Silver, las aplicaciones recreativas, como los juegos, mensajería instante, y P2P, podría estar en un servicio Best Effort, y el tráfico VoIP podría estar en su propia clase de servicio que reduciría el jitter.

Típicamente, MPLS opera en la red del carrier, requiriendo el router WAN en la parte del cliente (el router CPE) para diferenciar entre los diferentes tipos de tráfico. Basado en el tipo de aplicación y la clase de servicio a que se asigna, el router CPE aplica una etiqueta Diffserv o ToS a cada paquete, indicando la clase de servicio. Cuando el paquete llega al router de etiqueta del borde (LER) en la red del carrier, el LER puede mirar la etiqueta de Diffserv y puede traducir eso en la etiqueta de MPLS apropiada.

Las capacidades de clasificación de aplicaciones de los routers están limitadas, debido a que al router CPE le falta precisión y exactitud al etiquetar el tráfico con las etiquetas Diffserv. PacketShaper tiene habilidades de clasificación extensas. Puede descubrir, identificar, y clasificar las aplicaciones, y después asigna la etiqueta apropiada QoS, como las etiquetas de Diffserv, por ejemplo, puede identificar el tráfico Oracle y puede asignarle una etiqueta de DSCP, como 23. Cuando el paquete llega al LER en la red del carrier, el router mira la etiqueta de DSCP y le asigna la etiqueta MPLS correspondiente (por ejemplo 5, la etiqueta asoció con el servicio Gold). El LER después envía los paquetes en el camino de MPLS para el servicio Gold, asegurando que los requisitos de ancho de banda, jitter, y especificaciones de latencia son conocidos.

Las unidades de PacketShaper son ubicadas al borde de la red, como se muestra en la topología de la figura.

PacketShaper además de etiquetar el tráfico, usa políticas y particiones para aliviar los cuellos de botella que se forman en los puntos de la entrada a la red core MPLS. Entre el enlace local LAN y el enlace core MPLS, típicamente, es la porción más baja de capacidad de la red y puede producir congestión. Con PacketShaper, se protege el

desempeño de las aplicaciones, aprovisiona canales seguros para tráfico de voz y video para asegurar desempeño uniforme, y detiene las aplicaciones y usuarios que monopolizan el enlace.

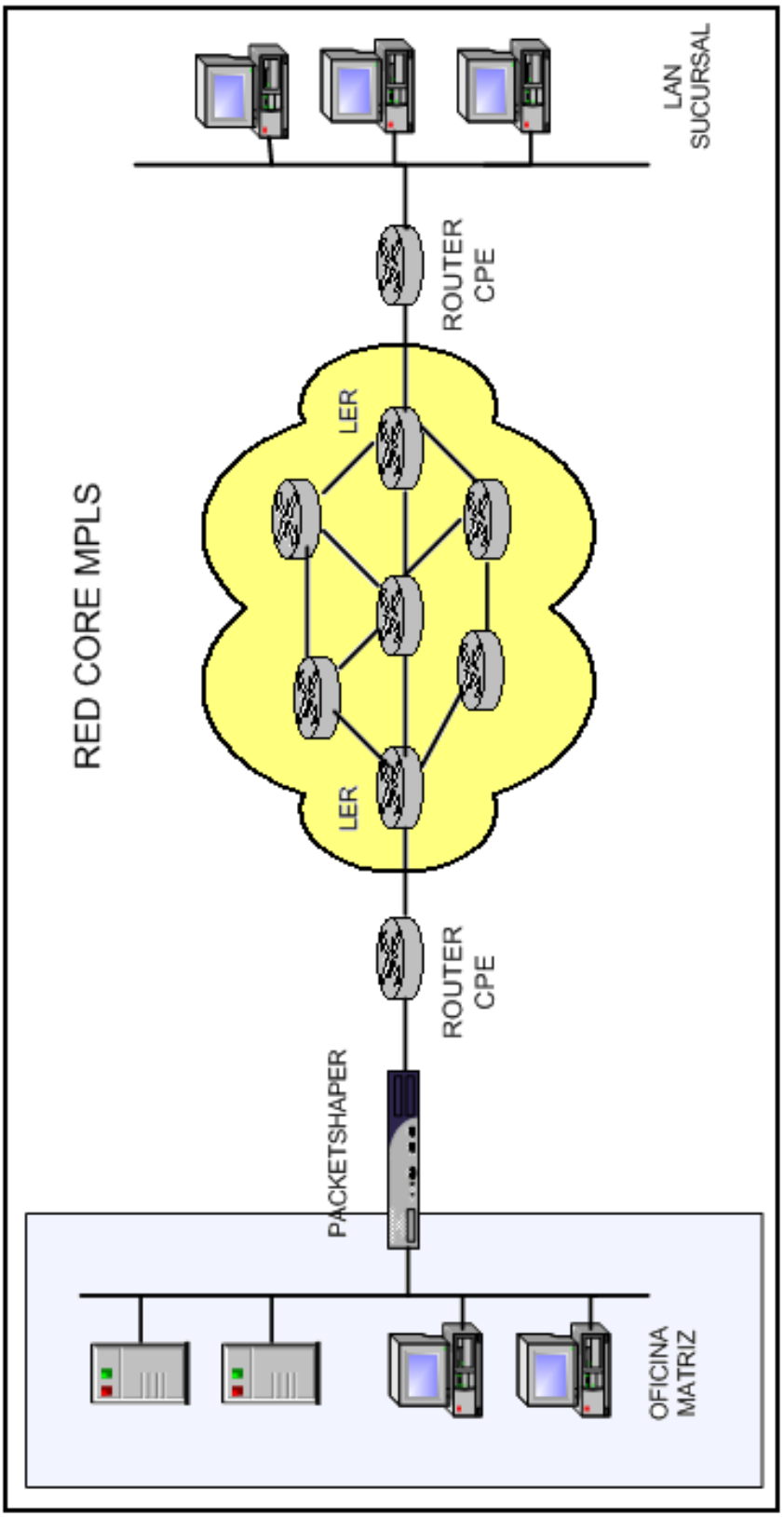


Fig. 5.10 Red MPLS

Las capacidades de análisis de PacketShaper permiten determinar los requisitos de ancho de banda de las aplicaciones de prioridad al desplegar MPLS. Por ejemplo, se desea saber cuánto ancho de banda se necesita para una aplicación. Usando las gráficas de monitoreo para ver el tráfico de esa clase, se calcula la cantidad de ancho de banda requerida para esa aplicación, multiplicando la proporción por el número de sesiones concurrentes que se desea mantener.

En resumen, la funcionalidad de PacketShaper complementa instalaciones de MPLS de las maneras siguientes:

- Descubre, identifica, y clasifica diversas aplicaciones y asigna etiquetas de QoS distintas, como las etiquetas Diffserv.

- Ayuda a determinar los requisitos de ancho de banda antes de un despliegue de MPLS.

- Descongestiona los cuellos de botella que se forman en los puntos de la entrada a la red core MPLS.

- Extiende los beneficios del funcionamiento de MPLS en el borde de la red y las premisas de los usuarios.

- Ayuda a las compañías a evaluar y administrar la transición a los servicios WAN basados en MPLS, permitiéndoles clasificar según tamaño, capacidad y desempeño con precisión para las diferentes clases de servicio.

- Mide y grafica el funcionamiento por aplicaciones y clases MPLS, permitiendo cumplir con el nivel de servicio acordado.

5.7 Optimizando el desempeño de Frame Relay.

En una topología Frame Relay se conectan dos o más oficinas sucursales a una oficina central por medio de circuitos virtuales permanentes (PVCs). Todo el tráfico atraviesa un switch Frame Relay (la nube WAN) y se rutea por un Dispositivo de Acceso Frame Relay (FRAD) en la oficina central. Para enviar el tráfico entre oficinas sucursales, los FRADs dirigen el tráfico de un PVC al otro. Cuando un PVC se congestiona, se envían los bits de notificación de congestión explícita forward/backward (FECN y BECN) a los FRADs de ambos extremos del PVC, en un esfuerzo por reducir la velocidad del tráfico. En congestión extrema, se dejan caer los paquetes y deben ser retransmitidos.

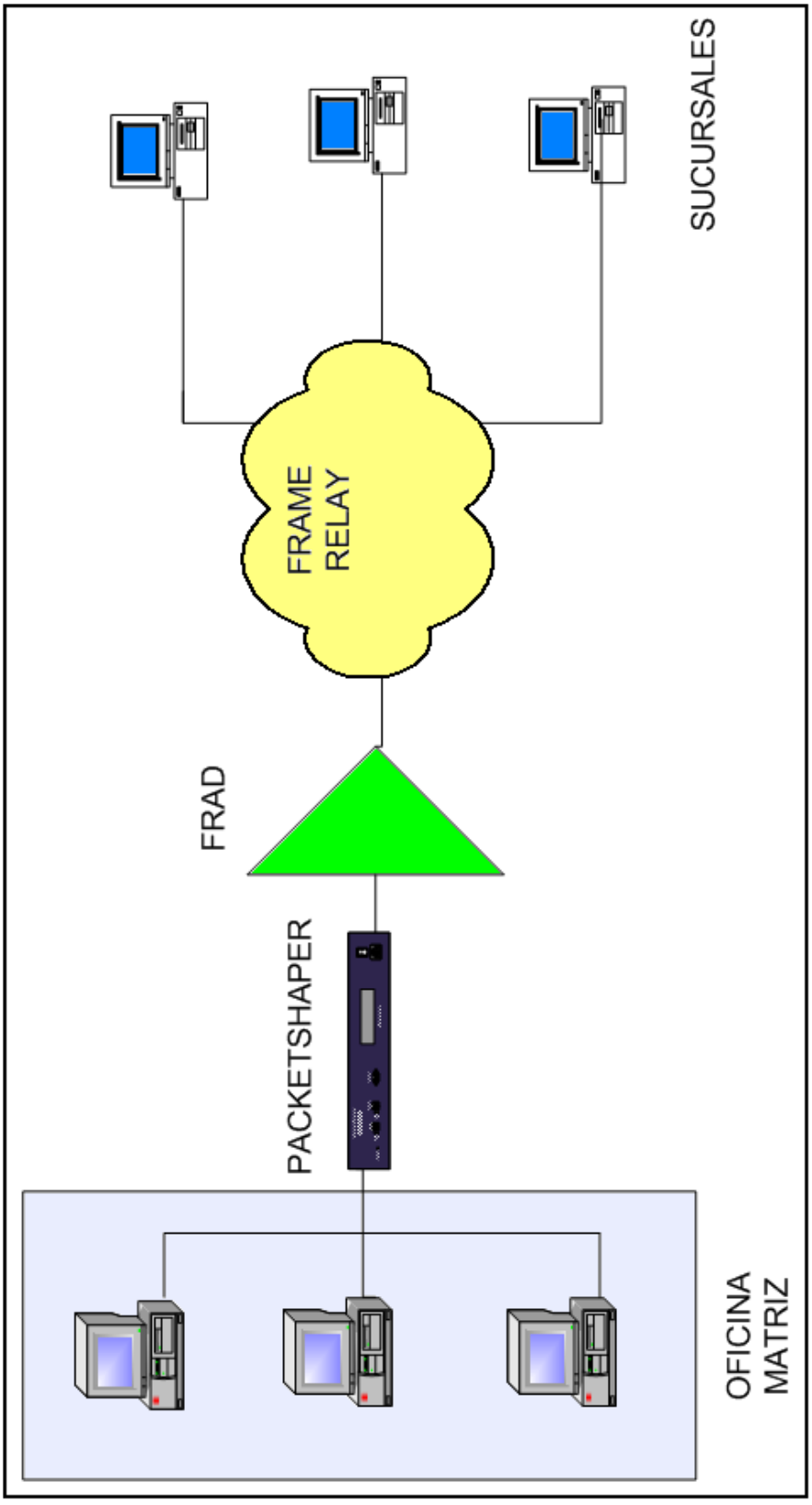


Fig. 5.11 Red Frame Relay

Las unidades de PacketShaper mejoran la red Frame Relay de varias maneras. Primero, las unidades aseguran que cada PVC obtiene la velocidad de información comprometida (CIR), encima de la velocidad de información de exceso (EIR). Esto se lleva a cabo con las características de partición de PacketShaper.

- El CIR traza el tamaño de la partición de PacketShaper y EIR traza la cantidad del exceso por que la partición puede extenderse.

- Segundo, TCP Rate Control ayuda a suavizar el flujo de tráfico TCP, reduciendo la probabilidad de paquetes caídos.

- Tercero, las políticas de PacketShaper permiten a los administradores de red controlar la velocidad, respuesta, y prioridad de aplicaciones individuales que corren por un enlace WAN o LAN.

- Cuarto, PacketWise crea una clase de tráfico automáticamente para cada PVC que usando la información de ruteo de la IP dinámica en el FRAD, ahorrando tiempo de tener que especificar

todas las direcciones de las subnets/IP manualmente para cada PVC.

- Finalmente, PacketWise acelera el tráfico de regreso en respuesta a la presencia de los bits FECN/BECN en el flujo para evitar una gran congestión de los PVCs.

Las unidades de PacketShaper se instalan detrás del FRAD en la oficina matriz y, opcionalmente, entre el FRAD y LAN en cada oficina de la sucursal. El software de PacketWise usa que SNMP para recoger los datos necesita del FRAD local. Basado en esta información, PacketWise puede determinar cuánto tráfico está pasando en el PVCs y puede descubrir cuántos bits FECN/BECN se han generado en el PVCs. Teniendo conocimiento de todo el tráfico que cruza el enlace de acceso, PacketWise puede administrar el ancho de banda del enlace eficazmente.

5.8 Limites de configuración.

La tabla siguiente menciona las capacidades de los equipos PacketShaper ISP con sus componentes de PacketWise 7.2.

Tabla 5.1 Límites de Configuración

Componente	Modelo 4500/ISP	Modelo 6500/ISP	Modelo 8500/ISP	Modelo 9500/ISP		Modelo 10000/ISP	
Máx. # de clases	1000*	2000	5000	2500	5000	2500	5000
Máx. # de particiones estáticas	1000	2000	5000	2500	5000	2500	5000
Máx. # de particiones dinámicas	2000	5000	20000	20000	20000	20000	20000
Máx. # de políticas	1000	2000	5000	2500	5000	2500	5000
Máx. # de matching rules	2500	5000	12500	6250	12500	6250	12500
Máx. # de matching rules por clase	1000	1000	1000	1000	1000	1000	1000
Máx. # de flujos concurrentes (TCP / IP otros)	150000/ 75000	200000/ 100000	500000/ 200000	1000000 / 400000	1000000 / 400000	1000000/ 400000	1000000/ 400000
Optimal max # of IP hosts at one time**	50000	75000	20000	400000	400000	400000	400000

Componente	Modelo 4500/ISP	Modelo 6500/ISP	Modelo 8500/ISP	Modelo 9500/ISP		Modelo 10000/ISP	
Max # of classes with Top Talkers/Listeners enabled	12 talkers + listeners en total	12 talkers + listeners en total	12 talkers + listeners en total	12 talkers + listeners en total	12 talkers + listeners en total	12 talkers + listeners en total	12 talkers + listeners en total
Supported WAN link rates (full duplex)	45 Mbps	100 Mbps	200 Mbps	45 Mbps 100 Mbps	200 Mbps	1 Gbps	200 Mbps 310 Mbps 620 Mbps
Network interface connection speeds	10 Mbps 100 Mbps auto-detect	10 Mbps 100 Mbps auto-detect	10 Mbps, 100 Mbps, or 1 Gbps auto-detect Fiber: 1 Gbps	10 Mbps, 100 Mbps, or 1 Gbps auto-detect Fiber: 1 Gbps	10 Mbps, 100 Mbps, or 1 Gbps auto-detect Fiber: 1 Gbps	10 Mbps, 100 Mbps, or 1 Gbps auto-detect Fiber: 1 Gbps	10 Mbps, 100 Mbps, or 1 Gbps auto-detect Fiber: 1 Gbps
LEM options***	10/100M	10/100M 10/100/1000 M 1000-SX 1000-LX	10/100M 10/100/1000 M 1000-SX 1000-LX	10/100/1000 M (Copper LEM2 or Fiber-Optic LEM w/ SFP ports	10/100/1000 M (Copper LEM2 or Fiber-Optic LEM w/ SFP ports	10/100/1000 M (Copper LEM2 or Fiber-Optic LEM w/ SFP ports	10/100/1000 M (Copper LEM2 or Fiber-Optic LEM w/ SFP ports

*PacketShaper 4500/ISP soporta hasta 1,000 direcciones IP basadas en subnet o basados en clases. Usando otros tipos de clases, PacketShaper 4500/ISP debe configurarse con 750 clases o menos

**Estos números han sido redondeados. PacketShaper puede soportar más hosts y flujos, sin embargo estas cifras representan el máximo ideal por producir resultados óptimos. Es normal ver el número de hosts concurrentes en su límite.

***1000-SX = 1000Base-SX w/LC o puertos SC (fibra óptica); 1000-LX = 1000Base-LX w / LC puertos (fibra óptica)

5.9 Aplicaciones, protocolos y servicios.

PacketWise soporta una variedad de aplicaciones, protocolos, y servicios para la clasificación del tráfico. El proceso de descubrimiento de tráfico detecta muchos de ellos, automáticamente crea clases de tráfico. También se las puede crear clases manualmente vía interfase browser o comandos de línea, y especifica los servicios y protocolos listados en las tablas que se encuentran en el anexo.

Se listan varios servicios como "grupos de servicio", también llamados servicios agregados. Un grupo de servicio abarca una combinación de servicios. Cuando se crea una clase de tráfico para un grupo de servicio, se crearán reglas de juego múltiples para manejar los tipos de tráfico representados por el grupo. Puesto que un grupo de servicio representa una combinación de reglas de juego, no se puede especificar números del puerto para los grupos de servicio.

CONCLUSIONES Y RECOMENDACIONES.

El ancho de banda es costoso y finito por lo tanto se lo debe administrar con eficiencia y seleccionar un proveedor que tenga un número de conexiones simultáneas en una adecuada proporción a su enlace y que ofrezca un CIR que no sea tan inferior al ancho de banda publicitado en el caso de las redes Frame Relay. El factor crítico para elegir un proveedor es la relación entre el CIR y el número de conexiones simultáneas que tiene el proveedor en una hora pico.

La aplicación de un sistema para la administración de tráfico y ancho de banda brinda un funcionamiento eficiente y predecible para aplicaciones que operan sobre redes WAN o Internet, lo que deriva en un mayor control sobre estas aplicaciones.

El tráfico que circula por una red no tiene el mismo comportamiento en una aplicación que en otra. Unas aplicaciones tienden a consumir más ancho de

banda que otras, y generalmente las primeras son las aplicaciones no críticas.

Para un ISP es muy importante poder ofrecer un buen servicio con diferentes niveles, de acuerdo a las necesidades de cada cliente. Con el equipo administrador PacketShaper se consigue este objetivo, y además según el cliente, se puede asignar un ancho de banda de manera que pueda expandirse más allá de sus límites, siempre y cuando halla disponibilidad.

Con la tecnología TCP Rate Control se previene que el tráfico sea enviado a velocidades más altas que la conexión WAN puede soportar y para eso reduce las colas en los buffers de los router y mejora la eficacia global, evitando de esta forma la congestión de la red.

Las gráficas de monitoreo de Packetshaper son una ayuda muy importante para un ISP, por lo que permiten mostrar a los clientes el consumo que han tenido durante un día, un mes, o cualquier intervalo de tiempo que se configure. De esta manera se puede aconsejar a algún cliente si necesita adquirir más o menos ancho de banda.

En la administración de ancho de banda las particiones juegan un papel muy importante, por lo que cumplen 4 funciones, proteger el tráfico, limitarlo, dividir la capacidad, y asignar de forma dinámica.

Las políticas son las herramientas que proporcionan la Administración de tráfico de un cliente si este así lo desea, se puede restringir, limitar o dar prioridad a las aplicaciones que atraviesan la red, optimizando el enlace.

Packetshaper consigue analizar el tráfico que atraviesa la red, según las reglas del juego que se hayan configurado en el equipo, asociándolo de acuerdo una clase, puerto, dirección IP, o protocolo.

Maneja todo el tráfico entrante (INBOUND), y que sale (OUTBOUND), categoriza y analiza los paquetes cuando ellos pasan.

Proporciona beneficios a una variedad de ambientes: cable, inalámbrico, fijo, satélite.

Integra claramente con infraestructura de red existente, no impone ningún cambio en la configuración de los routers, topologías, desktops o servidores.

Complementa otras aplicaciones de red y topologías como Firewalls, cargas balanceadas, routers redundantes y soluciones cache.

Tiene normas de seguridad, como contraseñas, listas de acceso y reglas SSL.

PacketShaper ayuda a evitar los ataques DOS, reduciendo el riesgo que pueden producir. Descubre y bloquea SQL Slammer, Blaster, y gusanos similares. Puede bloquear tráfico que está pretendiendo venir de una fuente confiada.

Comparando nuestro producto PacketShaper ISP con otros productos como el Bandwidth Manager BM-2100, QoSWorks, BWMeter 2.3.0, o el NETGRID 4.1.5.0; podemos concluir que es el que ofrece más funciones y alternativas de administración. Por lo tanto es el que se recomienda a los proveedores de servicios de Internet.

De acuerdo a la capacidad y a la proyección a futuro del ISP se debe escoger el modelo del equipo. Por el costo del equipo, es recomendable solo para empresas relativamente grandes, por las que atraviese grandes cantidades de tráfico.

También existen equipos administradores de ancho de banda para empresas pequeñas que son software y realizan monitoreos.

ANEXO

Tablas de servicios

Tabla 1. Cliente / Servidor

Nombre de la clase	Descripción	Versión de PackeShaper
CVSpserver	CVS (Concurrent Versions System) pserver	5.2.3
CVSup	CVS-Optimized Network File Distribution System	5.1
FIX	Financial Information eXchange	Pre-5.0.0
FoldingAtHome	Distributed Computation Screen Saver (foldingathome.stanford.edu)	5.0.2
INFOC-RTMS	Attachmate INFOConnect Response Time Monitor System	5.0.0
INT-1	Unisys Interactive 1 (2200, ClearPath IX)	5.0.0
MATIP	Mapping of Airline Traffic over IP (RFC 2351) service group	5.0.0
MATIP-A	MATIP Type A	5.0.0
MATIP-B	MATIP Type B	5.0.0
MeetingMaker	Meeting Maker	5.0.0

NetIQ	NetIQ AppManager	5.1
OpenConnect -JCP	OpenConnect JCP clients (browser-based access to host applications)	pre-5.0.0
PEPGate	Attachmate PEP Gateway (Unisys 2200)	5.0.0
Unisys-TCPA	Unisys TCPA (A Series, ClearPath LX, NX)	5.0.0

Tabla 2. Entrega de contenido

Nombre de la clase	Descripción	Versión de PackeShaper
Apple-iTunes	Apple iTunes - Music Downloads	6.0.2
Ariel-419	Infotrieve document delivery system (on port 419)	6.0.2
Ariel-422	Infotrieve document delivery system (on port 422)	6.0.2
BackWebe	Push technology. Polite BackWeb has an agent on the client to prevent BackWeb background traffic from interfering with other IP network applications.	pre-5.0.0
Chaincast	Chaincast Flexible Content Delivery System	5.2.3
EntryPoint	EntryPoint push traffic (formerly PointCast)	5.0.0
Kontiki	Kontiki - Content Distribution Network	5.2.2
Marimba	Marimba Castanet push traffic	pre-5.0.0
Napster2	Napster Pay-Per-Use Music Note: The original Napster and Napster P2P clients are classified in the Napster service.	6.2.0

Napster2-Data	Napster Music File Downloads	6.2.0
Napster2-Other	Other Napster Traffic	6.2.0
NewsStand	NewsStand-Reader - publication subscription service	pre-5.0.0
PointCast	See EntryPoint	pre-5.0.0
Webshots	Webshots Desktop (photo screensaver application)	pre-5.0.0

Tabla 3. Software de planeación de recursos empresariales y base de datos

Nombre de la clase	Descripción	Versión de PackeShaper
BAAN	Baan enterprise management system	Pre-5.0.0
FileMaker	FileMaker Pro database service group	Pre-5.0.0
FileMaker-DB	FileMaker database access	Pre-5.0.0
FileMaker-R	FileMaker network host response	Pre-5.0.0
JDENet	J. D. Edwards OneWorld JDENet protocol	5.0.0
MSSQL	Microsoft Structured Query Language service group	Pre-5.0.0
MSSQL-Mon	SQL monitoring traffic	Pre-5.0.0
MSSQL-Server	SQL server traffic	Pre-5.0.0
Oracle	Oracle database application service group	Pre-5.0.0
Oracle-netv1	Oracle SQL*Net v1-based traffic (v6, Oracle7) Note: Oracle-netv1 traffic is no longer autodiscovered by PacketWise; however, you can create this class manually.	5.0.0
Oracle-netv2	Oracle SQL*Net v2/Net8-based traffic (Oracle7, 8, 8i, 9i, 10g)	pre-5.0.0 5.2.1 (Oracle 9i)

Oracle-JVM-SSL	Oracle JVM (IIOP) traffic over SSL	pre-5.0.0
Oracle-SSL	Oracle database over SSL	pre-5.0.0
OracleClient	Oracle Java client (Webforms)	pre-5.0.0
OracleEM	Oracle Enterprise Manager	5.2.1
OracleEM1	Oracle Enterprise Manager-1	5.2.1
OracleEM2	Oracle Enterprise Manager-2	5.2.1
PostgreSQL	PostgreSQL freeware SQL database	6.0.2
Progress	Progress database traffic	5.0.0
SAP	SAP - Systemanalyse and Programmentwicklung (Services, Applications and Products in Data Processing)	5.0.0 7.0 (enhanced)
SAP.MCAST.NET	Multicast Service Announcement Protocol: 224.2.127.254	5.0.0

Tabla 4. Servicios de directorio

Nombre de la clase	Descripción	Versión de PackeShaper
CRS	Microsoft Content Replication Service	Pre-5.0.0
DHCP	Dynamic Host Configuration Protocol service group	Pre-5.0.0
DHCP-C	DHCP or BootP Client	Pre-5.0.0
DHCP-S	DHCP or BootP Server	Pre-5.0.0
DNS	Domain Name Service	pre-5.0.0 7.2.1 (enhanced)
Finger	Finger User Information Protocol	Pre-5.0.0
Ident	Identification Protocol	Pre-5.0.0
Kerberos	Network Authentication Service (ticket granting and checking)	Pre-5.0.0
LDAP	Lightweight Directory Access Protocol service group	Pre-5.0.0
LDAP-Clearr	LDAP	Pre-5.0.0
LDAP-Secure	Secure LDAP	Pre-5.0.0
mDNS	Multicast DNS (Apple Rendezvous)	7.0

RADIUS	Service group for Remote Authentication Dial-in User Service	Pre-5.0.0
RADIUS-Acct	RADIUS accounting service	Pre-5.0.0
RADIUS-Auth	RADIUS authentication service	Pre-5.0.0
RRP	NSI Registry Registrar Protocol	5.1
rwho	UNIX remote who (rwho) command; reports current users for all hosts on the local network	Pre-5.0.0
SSDP	Simple Service Discovery Protocol	5.3
TACACS	Login host protocol	pre-5.0.0
WHOIS	WHOIS service (application that identifies the owner of a domain name)	pre-5.0.0
WINS	Windows Internet Name Service	pre-5.0.0

Tabla 5. Emails y colaboraciones

Nombre de la clase	Descripción	Versión de PackeShaper
Biff	UNIX new mail notification	Pre-5.0.0
ccMail	Lotus cc:Mail email application	Pre-5.0.0
DCOM	Microsoft Distributed Component Object Model	Pre-5.0.0
Groupwise	Novell Groupwise messaging system service group	Pre-5.0.0
Groupwise-MTA	Novell Groupwise Message Transfer Agent	Pre-5.0.0
Groupwise-POA	Novell Groupwise Post Office Agent	Pre-5.0.0
IMAP	Interactive Mail Access Protocol service group	Pre-5.0.0
IMAP-Clear	Interactive Mail Access Protocol	Pre-5.0.0
IMAP-Secure	Secure Interactive Mail Access Protocol	Pre-5.0.0
LotusNotes	Groupware for collaborative communication	pre-5.0.0 7.2.1 (enhanced)
MSSQ	Microsoft Message Queue service group	Pre-5.0.0

MSSQ-CQ	MSSQ Client Queue	Pre-5.0.0
MSSQ-IS	MSSQ Information Store	Pre-5.0.0
MSSQ-Ping	MSSQ Ping Mechanism	Pre-5.0.0
MSSQ-QMT	MSSQ Queue Manager Traffic	Pre-5.0.0
MSSQ-SQ	MSSQ Server Queue	Pre-5.0.0
OSI	Open System Interconnection (OSI) over TCP (RFC2126), e.g., Microsoft Exchange X.400	Pre-5.0.0
POP3	Mail reception (Post Office Protocol) service group	Pre-5.0.0
POP3-Clear	Post Office Protocol for e-mail	Pre-5.0.0
POP3-Kerberos	Secure Mail Reception (Post Office Protocol with Kerberos)	5.0.2
POP3-Secure	Secure Post Office Protocol for e-mail	Pre-5.0.0
SMTP	Simple Mail Transport Protocol (mail transmission) service group	Pre-5.0.0
SMTP-Clear	Mail transmission	pre-5.0.0 7.1.0 (enhanced)
SMTP-Secure	Secure mail transmission with SSL	pre-5.0.0

Tabla 6. Servidor de archivos

Nombre de la clase	Descripción	Versión de PackeShaper
AFS	Andrew File System service group	5.0.2
AFS-FS	Andrew File System file server	5.0.2
AFS-VL	Andrew File System volume location database	5.0.2
CIFS-TCP	Common Internet File System (SMB) over TCP	5.0.0
CU-Dev	Fujitsu Device Control (CU-DEV on TCP/IP)	pre-5.0.0
lockd	NFS file lock daemon	pre-5.0.0
Microsoft-ds	Microsoft Common Internet File System / Server Message Block (SMB) protocol	5.0.0
NetBIOS-IP	NetBIOS over IP service group (NetBIOS is a program that allows applications on different computers to communicate within a LAN)	pre-5.0.0
NetBIOS-IP-DGM	NetBIOS Datagram Service	pre-5.0.0

NetBIOS-IP-NS	NetBIOS Name Service	pre-5.0.0
NetBIOS-IP-SSN	NetBIOS Session Service	pre-5.0.0
NFS	UNIX Network File System (both TCP and UDP)	pre-5.0.0
NW5-CMD	Netware 5 - Compatibility Mode Drivers service group	pre-5.0.0
NW5-CMD-TCP	Netware 5 - Compatibility Mode Drivers over TCP	pre-5.0.0
NW5-CMD-UDP	Netware 5 - Compatibility Mode Drivers over UDP	pre-5.0.0
NW5-NCP	Netware 5 Core Protocol	pre-5.0.0
rsync	UNIX remote file synchronization protocol	5.3
SunND	Sun Network Disk boot protocol	6.1.0

Tabla 7. Juegos

Nombre de la clase	Descripción	Versión de PackeShaper
AsheronsCall	Asheron's Call network game by Microsoft	5.0.2
Battle.net	Blizzard Entertainment online gaming services, including Diablo, Warcraft, and StarCraft	5.0.1, 5.2.3 (Warcraft III, Diablo II), 7.0.1 (enhanced)
Doom	Doom game	pre-5.0.0
Everquest	classified as SonyOnline	5.2.1
Half-Life	Service group for Half-Life network games by Valve and Sierra Studios (including Opposing Forces, CounterStrike, and Team Fortress)	5.0.2
Half-Life-TCP	Half-Life chat and server	5.0.2
Half-Life-UDP	Half-Life request and game play	5.0.2
Kali	Gaming protocol	pre-5.0.0
LucasArts	Jedi Knight II: Jedi Outcast	5.2.3
MSN-Zone	Microsoft Network Gaming Zone, including Age of Empires	5.0.2
MSN-Zone-	Microsoft Network Gaming Zone - TCP	5.0.2

TCP	traffic	
MSN-Zone-UDP	Microsoft Network Gaming Zone - UDPtraffic	5.0.2
Mythic	Mythic Entertainment games (Dark Age of Camelot)	pre-5.0.0
Quake	Quake game service group	pre-5.0.0
Quake-A	Quake (port 26000)	pre-5.0.0
Quake-B	Quake (port 27500)	pre-5.0.0
Quake-II-TCP	Quake II over TCP	pre-5.0.0
Quake-II-UDP	Quake II over UDP	pre-5.0.0
Quake-III	Quake III Arena	5.0.2
SonyOnline	Games by Sony Online Entertainment (e.g., EverQuest)	5.2.1
Tribes	Starsiege Tribes network game by Sierra Studios (includes Tribes 2)	5.0.2, 5.2.1 (Tribes 2)
Unreal	Unreal Tournament PC Game	5.0.2
Unreal-Browser	Unreal Tournament - Browser	5.0.2
Unreal-Ping	Unreal Tournament - Info Ping	5.0.2

Unreal-Play	Unreal Tournament - Game Play	5.0.2
Unreal-Status	Unreal Tournament - Status Request	5.0.2
YahooGames	Yahoo! Games	5.0.2

Tabla 8. Healthcare

Nombre de la clase	Descripción	Versión de PackeShaper
DICOM	Digital Imaging and Communications in Medicine	5.2.3
HL7	Health Level Seven	5.2.3

Tabla 9. Acceso a host

.

Nombre de la clase	Descripción	Versión de PackeShaper
ATSTCP	Galileo 2915 Terminal and Printer Traffic	5.0.0
Attachmate-GW	Attachmate INFOConnect-e-Vantage Gateway	5.0.0
Persona	Persoft Persona service group	5.0.0
Persona-Clear	Persoft Persona non-encrypted (port 1917)	5.0.0
Persona-Secure	Persoft Persona secure SSL	5.0.0
SHARESUDP	Unisys Interactive 1 (2200, ClearPath IX)	5.0.0
SMTBF	Attachmate Lantern Gateway	5.0.0
tn3270	Telnet for IBM 3270 terminals and 3270 emulation	pre-5.0.0
tn5250	IBM 5250 terminal traffic over Telnet	pre-5.0.0

Tabla 10. Protocolos de Internet

Nombre de la clase	Descripción	Versión de PackeShaper
ActiveX	Microsoft object-oriented program technologies and tools	pre-5.0.0
BITS	Microsoft Background Intelligent Transfer Service	6.2.0
FTP	File Transfer Protocol service group classification - both FTP commands and data	Pre-5.0.0
FTP-Cmd-Clear	File Transfer Protocol command channel	Pre-5.0.0
FTP-Cmd-Secure	Secure FTP command channel (SSL)	Pre-5.0.0
FTP-Data-Clear	FTP data transport channel	Pre-5.0.0
FTP-Data-Secure	Secure FTP data transfer channel (SSL)	Pre-5.0.0
Gopher	Search application	Pre-5.0.0
HTTP	Web traffic - Hypertext Transport Protocol	Pre-5.0.0

HTTP-Tunnel	HTTP Tunnel Traffic (traffic that is sent through an HTTP tunnel via an HTTP proxy server on the Internet - perhaps to bypass firewall rules) See the Tech Info Library for information about restricting traffic in an HTTP tunnel.	6.0 7.0 (enhanced)
IP	Internet Protocol (not autodiscovered)	Pre-5.0.0
IPIP	IP-within-IP Encapsulation Protocol	5.2.1
IPv6	Internet Protocol version 6 (IPng)	Pre-5.0.0
NNTP	Usenet NetNews Transfer Protocol	Pre-5.0.0
NNTP-Clear	Clear Text Usenet newsgroup transmission	Pre-5.0.0
NNTP-Secure	Secure Usenet newsgroup transmission	Pre-5.0.0
SOAP-HTTP	Simple Object Access Protocol over HTTP	7.0
TCP	Transmission Control Protocol - all Internet TCP traffic (not autodiscovered)	Pre-5.0.0
TFTP	User Datagram Protocol - all Internet UDP traffic (not autodiscovered)	Pre-5.0.0
UDP	User Datagram Protocol - all Internet UDP traffic (not autodiscovered)	Pre-5.0.0
UUCP	Unix-to-Unix Copy Protocol	Pre-5.0.0

Tabla 11. Legado LAN o sin IP

Nombre de la clase	Descripción	Versión de PackeShaper
AFP	AppleTalk Filing Protocol (AppleShare IP)	pre-5.0.0
AppleTalk	Apple network protocol	pre-5.0.0
DECnet	Digital Equipment Corporation network protocol	pre-5.0.0
FNA	Fujitsu Network Architecture (a variant of SNA)	pre-5.0.0
FNAonTCP	FNA on TCP service group	pre-5.0.0
FNAonTCP-1	Transport Independent Convergence (FNA on TCP port 492)	pre-5.0.0
FNAonTCP-2	Transport Independent Convergence (FNA on TCP port 493)	pre-5.0.0
IPX	Novell networking protocol	pre-5.0.0
LAT	DEC Printer Support (Local Area Transport)	pre-5.0.0
MOP-DL	Maintenance Operations Protocol Dump/Load	5.1
MOP-RC	Maintenance Operations Protocol Remote Console	5.1
NetBEUI	NetBEUI - Network protocol for PCs	pre-5.0.0

PPPoE	Point-to-Point Protocol over Ethernet	5.2.1
PPPoE-Control	Point-to-Point Protocol over Ethernet – Control	5.2
PPPoE-Data	Point-to-Point Protocol over Ethernet - Data	5.2
SLP	Service Location Protocol	pre-5.0.0
SNA	IBM Systems Network Architecture protocol	pre-5.0.0

Tabla 12. Mensajería

Nombre de la clase	Descripción	Versión de PackeShaper
AOL-AIM-ICQ	AOL 8.0 - AOL Instant Messenger & ICQ service group	5.0.1
AOL-IM	AOL - Instant Messenger & ICQ Client-Server	5.0.1
ICQ-2000	ICQ – ICQ2000 Client to Client Protocol	5.0.2
AOL-IM-Talk	AOL Instant Messaging Point-to-Point Talk	5.2.1
AOL-IM-IMAGE	AOL Instant Messaging Point-to-Point Chat	5.2.1
AOL-IM-File	AOL Instant Messaging Point-to-Point File Transfer	5.2.1
AOL-ISP	AOL 8.0 ISP client traffic	6.0
AOL-Default	Unknown AOL traffic	6.0
IRC	Internet Relay Chat service group	pre-5.0.0
IRC-Chat	Internet Relay Chat - General chat traffic	5.2.1
IRC-DCC	Internet Relay Chat - Direct Client-to-Client traffic	5.2.1
IRC-Secure	Secure Internet Relay Chat with SSL (port 994)	pre-5.0.0

IRC-Servers	Internet Relay Chat - Server-to-Server traffic	5.2.1
IRC-194	IRC on port 194	pre-5.0.0
IRC-6665	IRC on port 6665 (server to server)	pre-5.0.0
IRC-6667	IRC on port 6667 (client to server)	pre-5.0.0
Lotus-IM	IBM Lotus Instant Messaging Note: Some Instant Messenger traffic is classified into pre-existing services: Broadcast Service will classify into RTSP, Meeting Data into T.120, and Meeting Updates into LotusNotes. In order to track and manage Lotus messaging traffic most effectively, you may want to group Lotus-IM, RTSP, T.120, and LotusNotes into a single folder.	6.0.2
Lotus-IM-CommC	IBM Lotus Instant Messaging - Tunnelled Community Service	6.0.2
Lotus-IM-CommS	IBM Lotus Instant Messaging - Community Service	6.0.2
Lotus-IM-MtgS	IBM Lotus Instant Messaging - Meeting Service	6.0.2
Lotus-IM-SrvrEx	IBM Lotus Instant Messaging - Server Exchange	6.0.2
MSN-	MSN Messenger Chat Service	5.0.1

Messenger		
Windows-POPUP	Windows Messenger Delivery (RPC); classifies Windows Messenger spam pop-up windows that were sent out with applications such as DirectAdvertising	6.0.2
YahooMsg	Yahoo! Messenger	pre-5.0.0

Tabla 13. Middleware

Nombre de la clase	Descripción	Versión de PackeShaper
CORBA	CORBA Internet Inter-ORB Protocol (IIOP)	pre-5.0.0
JavaRMI	Java 1.1.4 TCP Remote Method Invocation service group	5.0.0
JavaRMI-Act	Java 1.1.4 TCP Remote Method Invocation - Activate	5.0.0
JavaRMI - Call	Java 1.1.4 TCP Remote Method Invocation - Call	5.0.0
JavaRMI-Reg	Java 1.1.4 TCP Remote Method Invocation - Registry	5.0.0
SmartSockets	Tibco SmartSockets traffic	6.0.2
SunRPC	Sun Remote Procedure Calls (UDP) service group	pre-5.0.0
SunRPC-Call	Sun Remote Procedure Calls	pre-5.0.0
SunRPC-PortMap	Sun Remote Procedure Calls Port Mapper	pre-5.0.0

Tabla 14. Multimedia

Nombre de la clase	Descripción	Versión de PackeShaper
Abacast	Abacast distributed streaming technology	7.0
Motion	Motion video (ESPN Motion, etc.) using DIGStream	7.0
MPEG-Audio	Moving Picture Experts Group - Audio Streams	pre-5.0.0
MPEG-Video	Moving Picture Experts Group - Video Streams	pre-5.0.0
Ogg	Ogg over HTTP	7.1.0
QuickTime	QuickTime over HTTP	5.0.0 7.0 (enhanced)
RadioNetscape	Radio@Nestcape streaming music application, powered by Spinner	6.2.0 7.0 (enhanced)
Real	Service group for Real Networks streaming audio/video application	pre-5.0.0
Real-BackChan	Real Networks multicast back-channel traffic	pre-5.0.0
Real-Encoder	Real Networks encoder traffic over HTTP or RTSP	pre-5.0.0

Real-Multicast	Real Networks real data transport UDP multicast traffic	pre-5.0.0
Real-Player	Real Networks Player traffic over HTTP or RTSP	pre-5.0.0
Real-RDT-TCP	Real Networks Real Data transport TCP traffic	pre-5.0.0
Real-RDT-UDP	Real Networks Real Data transport UDP traffic	pre-5.0.0
Real-RTP-TCP	Real Networks Real-time Transport Protocol TCP traffic	5.0.0
Real-RTP-UDP	Real Networks Real-time Transport Protocol UDP traffic	pre-5.0.0
Real-Web	Real Networks traffic over HTTP or RTSP	pre-5.0.0
RTP-B	Real-Time Protocol (Broadcast)	pre-5.0.0
RTP-I	Real-Time Protocol (Interactive)	pre-5.0.0 7.1.0 (enhanced)
RTSP	Real-Time Streaming Protocol	pre-5.0.0
Shoutcast	Shoutcast streaming audio	pre-5.0.0
ST2	Internet Stream protocol, version 2	pre-5.0.0
StreamWorks	StreamWorks Audio and Video	pre-5.0.0

VideoFrame	Citrix VideoFrame service group	pre-5.0.0
VideoFrame-TCP	Citrix VideoFrame control (TCP)	pre-5.0.0
VideoFrame-UDP	Citrix VideoFrame streaming data (UDP)	pre-5.0.0
WebEx	WebEx Real-Time Communications Platform	5.2.1 7.0 (enhanced)
WinampStream	Winamp streaming traffic	6.0.2
WinMedia	Microsoft Windows Media service group	pre-5.0.0
WinMedia-Mcast	Windows Media Streaming over UDP Multicast	5.0.0
WinMedia-MSBD	Windows Media Encoder	5.0.0
WinMedia-TCP	Microsoft Windows Media (NetShow) Streaming over TCP	pre-5.0.0
WinMedia-UDP	Windows Media Streaming over UDP Unicast	pre-5.0.0

Tabla 15. Administración de red

Nombre de la clase	Descripción	Versión de PackeShaper
CiscoDiscovery	Cisco Router Discovery Protocol	pre-5.0.0
Day-Time	Day-Time (port 13)	5.0.2
Echo	Echo Protocol	5.2.1
FlowRecords	Packeteer Proprietary Flow Detail Records	7.0
ICMP	Internet Control Message Protocol	pre-5.0.0
IPComp	IP Payload Compression Protocol (IPComp); a protocol to reduce the size of IP packets	6.0
NetFlowV5	NetFlow v5	7.0
NTP	Network Time Protocol service group	pre-5.0.0
RSVP	Resource Reservation Protocol	5.0.0
SMS	Microsoft SMS 2.0 - Service Pack 2 or later	5.2.1
SMS-Auth	SMS authentication	5.2
SMS-Chat	SMS remote chat	5.2
SMS-File	SMS file transfer	5.2
SMS-RC	SMS remote control	5.2

SNMP	Simple Network Management Protocol service group	pre-5.0.0
SNMP-Mon	SNMP monitoring traffic	pre-5.0.0
SNMP-Trap	SNMP event notification	pre-5.0.0
Syslog	UNIX system logging	pre-5.0.0
TimeServer	Time Server (port 37)	5.0.2

Tabla 16. Aplicaciones Peer-to-Peer (P2P)

Nombre de la clase	Descripción	Versión de PackeShaper
Aimster	Aimster file sharing application service group	5.1
Aimster-Cmd	Aimster command traffic	5.1
Aimster-Data	Aimster file transfer traffic (upload/download)	5.1
Aimster-Init	Aimster initial connection to redirector	5.1
Audiogalaxy	Audiogalaxy Satellite File Sharing Community (including Rhapsody)	5.0.2 5.3 (Rhapsody)
BitTorrent	Bit Torrent Distributed File Sharing System	6.0.1 7.2.1 (enhanced)
Blubster	Blubster File Sharing Application	5.0.0
DirectConnect	NeoModus Direct Connect File Sharing Community	5.1
EarthStationV	EarthStation V p2p	7.0
EarthV-Search	EarthStation V search traffic	7.0
EarthV-HTTP	EarthStation V over HTTP	7.0
EarthV-SSL	EarthStationV secure traffic	7.0

EarthV-PXP	EarthStation V pxp file transfers	7.0
eDonkey	eDonkey2000 File Sharing Application service group	5.2 6.0.1 (eMule, Overnet)
eDonkey-TCP	eDonkey2000 data traffic	5.2
eDonkey-Ping	eDonkey2000 host location ping requests	5.2
FileRogue	FileRogue File Sharing Application	5.2.3
Filetopia	Filetopia community traffic	6.0.2
Furthurnet	Furthur Network Peer to Peer File Sharing	5.3
Gnutella	File sharing and distribution network service group (a variety of look-alike clients get classified as Gnutella, for example Mutella, Shareaza, Xolox, Ares, Acquisition, Phex, Qtraxmax, and Morpheus).	5.0.0 7.1.0 (enhanced)
Gnutella-Cmd	Gnutella command and query traffic	5.0.0
Gnutella-Download	Gnutella file transfer from the outside to the inside	5.0.0
Gnutella-Init	Gnutella initial connection	5.0.0
Gnutella-Upload	Gnutella file transfer from the inside to the outside	5.0.0

Groove	Groove Peer-to-Peer Application	5.1
Hotline	Hotline File Sharing Community service group	5.1
Hotline-TCP	Hotline File Sharing Community - TCP	5.1
Hotline-UDP	Hotline File Sharing Community - UDP	5.1
iMesh	User-to-User Media Exchange.	5.0.0
KaZaA	KaZaA File Sharing Application service group Note: MusicCity Morpheus also classifies as KaZaA	5.1
KaZaA-Cmd	KaZaA command traffic	5.1
KaZaA-Download	KaZaA file transfer from the outside to the inside	5.1
KaZaA-Query	KaZaA peer server query	5.2.3
KaZaA-Upload	KaZaA file transfer from the inside to the outside	5.1
Napster	Napster Music Community service group Note: This is the orginal protocol that classifies Napster or Napster look-alike P2P clients. The pay-for-music Napster protocol is classified with Napster2.	5.0.0

Napster-Cmd	Napster command traffic	5.0.0
Napster-Data	Napster data traffic (upload/download)	5.0.0
Napster-Init	Napster initial connection to napster.com	5.0.0
Naptser-UDP	Napster UDP traffic (upload/download)	5.0.0
PeerEnabler	Altnet over KaZaA (v2.5) and PeerEnabler traffic	5.0.0
ScourExchange	ScourExchange File Sharing Community.	5.0.0
Scour-Web	Scour Exchange - web traffic	5.0.0
Scour-CSC	Scour Exchange - CSC protoco	5.0.0
Soulseek	Soulseek P2P Filesharing Application	7.1.0
Tripnosis	Tripnosis File Sharing Application	5.1

Tabla 17. Tráfico de impresión

Nombre de la clase	Descripción	Versión de PackeShaper
IPP	Internet Printing Protocol	5.0.0
Printer	UNIX line printer spooler (LPR)	pre-5.0.0
tn3287	IBM 3270 print traffic (TN 3287 extensions)	pre-5.0.0
tn5250p	IBM 5250 print traffic over Telnet	pre-5.0.0

Tabla 18. Protocolos de ruteo

Nombre de la clase	Descripción	Versión de PackeShaper
AURP	AppleTalk Update-based Routing Protocol	pre-5.0.0
BGP	Border Gateway Protocol	pre-5.0.0
CBT	Core-Based Trees (Multicast Routing Protocol)	pre-5.0.0
DRP	DECnet Routing Protocol	pre-5.0.0
DTP	Dynamic Trunking Protocol	7.2.1
EGP	Exterior Gateway Protocol (network routing information)	pre-5.0.0
EIGRP	Enhanced Interior Gateway Routing Protocol	pre-5.0.0
IGMP	Internet Group Management Protocol	pre-5.0.0
IGP	Interior Gateway Protocol	5.0.0
OSPF	Open Shortest-Path First network routing information	pre-5.0.0
PAgP	Port Aggregation Protocol	7.2.1
PIM	Protocol-Independent Multicast Routing Protocol	pre-5.0.0

PVSTP	Cisco Per-VLAN Spanning Tree Plus protocol (PVST+)	7.2.1
RARP	Reverse Address Resolution Protocol	pre-5.0.0
RIP	Routing Information Protocol (UDP)	pre-5.0.0
SpanningTree	IEEE802.1 Bridge Spanning Tree	pre-5.0.0
VLAN-Bridge	VLAN Bridge Protocol	7.2.1
VTP	VLAN Trunking Protocol	7.2.1

Tabla 19. Protocolos de seguridad

Nombre de la clase	Descripción	Versión de PackeShaper
DLS	SNA over TCP transport - Service group classification of Data Link Switch traffic, both read and write port numbers	pre-5.0.0
DLS-RPN	Data Link Switch Read Port Number	pre-5.0.0
DLS-WPN	Data Link Switch Write Port Number	pre-5.0.0
DPA	Microsoft Distributed Password Authentication	pre-5.0.0
GRE	General Routing Encapsulation	pre-5.0.0
IPMobility	Minimal encapsulation for IP [RFC 2004]	6.1.0
IPSec	IP Security Encapsulation service group	pre-5.0.0
IPSec-AH	IPSec Authentication Header	pre-5.0.0
IPSec-ESP	IPSec Encapsulating Security Payload	pre-5.0.0
ISAKMP	ISAKMP/IKE key exchange	pre-5.0.0
L2TP	Layer 2 Tunneling Protocol for VPN connections (UDP encapsulation)	pre-5.0.0
PPTP	Point-to-Point Tunneling Protocol	pre-5.0.0

RC5DES	DES (data encryption standard) encryption-cracking application	pre-5.0.0
SOCKS	SOCKSv4 and SOCKSv5 proxy protocol	pre-5.0.0
SoftEther	Japanese SSL VPN secure traffic	7.1.0
SSH	Secure Shell remote login protocol	pre-5.0.0
SSL	Secure Sockets Layer protocol (secure Web traffic)	pre-5.0.0
SSL-Shell	SSL Secure Shell remote login protocol	pre-5.0.0
SWIPE	swIPe: network layer encapsulated encrypted IP protocol	6.1.0

Tabla 20. Sesiones

Nombre de la clase	Descripción	Versión de PackeShaper
GoToMyPC	GoToMyPC HTTP traffic	6.0.2
pcAnywhere	Remote management collaboration tool service group	pre-5.0.0
pcAnywhere-D	pcAnywhere data	pre-5.0.0
pcAnywhere-OD	pcAnywhere data (old port)	pre-5.0.0
pcAnywhere-OS	pcAnywhere status (old port)	pre-5.0.0
pcAnywhere-S	pcAnywhere status	pre-5.0.0
radmin	Remote Administrator (remote control software)	6.2.0
RemotelyAnywhere	RemotelyAnywhere Remote Desktop Services	7.2.1
rexec	UNIX remote execution protocol	pre-5.0.0
rlogin	Remote login	pre-5.0.0
rsh	UNIX remote shell command	5.1
Telnet	Telnet terminal service group	pre-5.0.0

Telnet-Clear	Network terminal protocol	pre-5.0.0
Telnet-Secure	Secure Network terminal protocol	pre-5.0.0
Timbuktu	Timbuktu Pro service group (networked remote control)	pre-5.0.0
Timbuktu-Ctl	Timbuktu Control Channel	pre-5.0.0
Timbuktu-HS	Timbuktu Handshaking	pre-5.0.0
Timbuktu-Obs	Timbuktu Observe Channel	pre-5.0.0
Timbuktu-Snd	Timbuktu Send Channel	pre-5.0.0
Timbuktu-Xch	Timbuktu Exchange Channel	pre-5.0.0
VNC	Virtual Network Computing	5.0.0
XWindows	X11 Windowing agent (UDP)	pre-5.0.0
XWindows-DM	XWindows Display Manager (XDMCP)	pre-5.0.0
XWindows-S	XWindows Server	pre-5.0.0

Tabla 21. Basado en servidor o Thin Client

Nombre de la clase	Descripción	Versión de PackeShaper
Citrix	Citrix connectivity application service group. Enables any type of client to access applications across any type of network connection.	5.1
Citrix-ICA	Citrix Independent Computer Architecture (ICA)	5.1
Citrix-SB	Citrix Server Browsing (UDP)	pre-5.0.0
CitrixIMA	Citrix Integrated Management Architecture service group	5.0.1
CitrixIMA-CMC	Citrix IMA Management Console	5.0.1
CitrixIMA-Svr	Citrix IMA Server to Server	5.0.1
RDP	Remote Desktop Protocol - Microsoft Windows Terminal Server	pre-5.0.0

Tabla 22. Voz sobre IP (VoIP)

Nombre de la clase	Descripción	Versión de PackeShaper
CiscoCTI	Cisco Computer Telephony Interface	5.2.3
Clarent-CC	Clarent Voice over IP Command Center	pre-5.0.0
Clarent-Complex	Clarent complex traffic	pre-5.0.0
Clarent-Mgmt	Clarent complex traffic	pre-5.0.0
Clarent-Voice-S	Clarent voice traffic (simple)	pre-5.0.0
CUSeeMe	Video chat services application service group	pre-5.0.0
CUSeeMe-AV	Video chat services audio/video	pre-5.0.0
CUSeeMe-CC	Video chat services connection control	pre-5.0.0
CUSeeMe-CE	Video chat services connection establishment	pre-5.0.0
Dialpad	Dialpad Internet Telephone service group	5.2.1
Dialpad-Ctrl	Dialpad Internet Telephone - control traffic	5.2
Dialpad-Stream	Dialpad Internet Telephone - RTP stream	5.2

H.323	Internet telephony standard service group	pre-5.0.0
H.323-GKD	H.323 Gatekeeper Discovery	pre-5.0.0
H.323-H.245	H.323 call control	pre-5.0.0
H.323-Q.931	H.323 call setup	pre-5.0.0
H.323-RAS	H.323 Gatekeeper Control (Registration, Admission, and Status)	pre-5.0.0
I-Phone	Vocaltec Internet telephone service	pre-5.0.0
MCK-Signaling	MCK Signaling (not autodiscovered)	5.0.0
MCK-Voice	MCK Voice (not autodiscovered)	5.0.0
Megaco	Media Gateway Control (H.248)	6.0
Megaco-Text	Media Gateway Control (H.248) Text	6.0
Megaco-Bin	Media Gateway Control (H.248) Binary	6.0
MGCP	Media Gateway Control Protocol	6.0
MGCP-Gateway	Media Gateway Control Protocol Gateway	6.0
MGCP-CallAgent	Media Gateway Control Protocol CallAgent	6.0
MGCP-KpAlive	Media Gateway Control Protocol KeepAlive Connection	6.0

Micom-VIP	Micom Voice over IP (V/IP)	pre-5.0.0
Net2Phone	Net2Phone CommCenter	5.2.3
Net2Phone-TCP	Net2Phone Call Setup and Control	5.2.3
Net2Phone-UDP	Net2Phone Internet Phone Calls	5.2.3
RTCP-B	Real-Time Control Protocol (Broadcast)	pre-5.0.0
RTCP-I	Real-Time Control Protocol (Interactive)	pre-5.0.0
SIP	Session Initiation Protocol	6.0
SIP60	Session Initiation Protocol over port 5060	7.1.0
SIP61	Session Initiation Protocol over port 5061	7.1.0
Skinny	Cisco's Skinny Client Control Protocol (SCCP) Note: This service is not autodiscovered, but you can create a class manually for this service.	6.0
Skype	Skype P2P Telephony Application	7.0 7.1.0(enhanced) 7.2.1 (enhanced)
SkypeCommand	Skype Command	7.0

SkypeData	Skype Data	7.0
T.120	Collaboration application	pre-5.0.0
VDOPhone	Service group for Internet telephone service group (not autodiscovered)	pre-5.0.0
VDOPhone-a	Internet telephone application - TCP port 1 (not autodiscovered)	pre-5.0.0
VDOPhone-b	Internet telephone application - TCP port 2 (not autodiscovered)	pre-5.0.0
VDOPhone-UDP	VDOPhone real-time media (not autodiscovered)	pre-5.0.0
Vonage	Vonage VoIP	7.1.0
Vonage-SIP	Vonage Session Initiation Protocol	7.1.0
Vonage-RTP	Vonage Real-Time Control Protocol	7.1.0

BIBLIOGRAFÍA

- TOMASSI Wayne, Sistemas de Comunicaciones Electrónicas, Pearson Educación, 2003.
- Tutoriales de cisco

OTRAS REFERENCIAS

- Jorge R. Hernández, 18 de Noviembre del 2004, Modelo OSI y el protocolo de Internet (IP versión 6), http://www.monografias.com/trabajos29/modelo-osi/modelo-osi.shtml
- Packeteer, 2003-2006, Provisioning with Power for Providers of Managed Bandwidth Services. http://www.packeteer.com/resources/prod-sol/ControlDrillDown.pdf
- Packeteer, 2003-2006, Provisioning with Power for Providers of Managed Bandwidth Services

http://www.packeteer.com/resources/prod-sol/PSISPOverview.pdf

- SoftPerfect, 2000-2006, SoftPerfect Bandwidth Manager, http://www.softperfect.com/products/bandwidth/manual/welcome-intro.htm
- Softonic International, Septiembre 2005, http://www.softonic.com/ie/31021
- Softonic International, Septiembre 2005, netgrid.softonic.com/ie/38496
- Jalercom S.A. de C.V., Septiembre 2005, 10Mbps Bandwidth Manager http://www.jalercom.com/Brochures/planet-BM2010-esp.pdf
- Sitara Networks, Septiembre 2005, The First Integrated QoS Platform for Enabling e-Business Networks http://www.btwsa.com.ar/sitePDF/qoswdatasheet.pdf