ESCUELA POLITECNICA DEL EJERCITO

FACULTAD DE INGNIERIA ELECTRONICA

PROYECTO DE GRADO PARA LA OBTENCION DEL TITULO EN INGENIERIA ELECTRONICA ESPECIALIDAD TELECOMUNICACIONES

"SISTEMAS ADMINISTRADORES DE ANCHO DE BANDA DE ENLACES WAN E INTERNET"

REALIZADO POR:

CHRISTIAN MARCELO LLERENA ANDRADE

SANGOLQUI – ECUADOR

2005

CERTIFICACION

Certificamos que el presente proyecto de grado titulado “Sistemas administradores de ancho de banda de enlaces WAN e Internet”, ha sido desarrollado en su totalidad por el señor Christian Marcelo Llerena Andrade, bajo nuestra dirección.

Ing. Fabián Sáenz	Ing. Carlos Romero
DIRECTOR	CODIRECTOR

AGRADECIMIENTO

Agradezco a Dios por ayudarme a culminar esta etapa de mi vida satisfactoriamente, a mis padres por su apoyo incondicional, por su paciencia y por los sabios consejos que día a día me imparten.

Agradezco a mis hermanos y a cada uno de mis amigos y compañeros que me ayudaron y colaboraron en los momentos en que necesité de su ayuda.

A mi tío Mario le doy mi más sincero agradecimiento por su ayuda y consejos durante el desarrollo de esta tesis.

CHRISTIAN LLERENA ANDRADE

DEDICATORIA

Dedico este proyecto de grado principalmente a mis padres Gustavo Llerena y Gloria Andrade, también lo dedico a mis hermanos Gustavo, Andrés y a mi sobrino Ismael, quienes son las personas más quiero y que me han apoyado en la culminación del proyecto.

CHRISTIAN MARCELO LLERENA ANDRADE

PROLOGO

El desarrollo constante de la humanidad y por tanto de la tecnología informática ha ocasionado que se incremente cada vez más, el número de aplicaciones y programas creados para trabajar sobre Internet y sobre enlaces de red entre oficinas.

Hoy en día cada empresa posee un enlace de Internet y/o un enlace de red entre oficinas, las aplicaciones y programas que atraviesan estos enlaces son generalmente basados en el protocolo más utilizado en la actualidad, este es el protocolo TCP/IP.

El protocolo TCP/IP trabaja bien sobre enlaces de Internet y enlaces entre oficinas, pero generalmente estos enlaces poseen un capacidad baja, por lo que el incremento de usuarios y aplicaciones puede afectar al rendimiento de estos enlaces, por esto ha sido necesario implementar criterios de calidad de servicio aplicados a aplicaciones y flujos importantes de tráfico. Esto se logra utilizando elementos de red como ruteadores o sistemas dedicados a implementar calidad de servicio.

El presente proyecto titulado “Sistemas administradores de ancho de banda de enlaces WAN e Internet” tiene por objetivo implementar una guía para la de solución de calidad de servicio de enlaces de Red de Area Amplia (WAN) e Internet, utilizando sistemas administradores de ancho de banda dedicados.

INDICE

CAPITULO I

MARCO TEORICO REFERENCIAL

CAPITULO II

SISTEMAS ADMINISTRADORES DE ANCHO DE BANDA

CAPITULO III

ESTUDIO DEL SISTEMA PACKETSHAPER

CAPITULO IV

PRUEBAS DEL SISTEMA PACKETSHAPER

CAPITULO V

ESTABLECIMIENTO DE POLITICAS

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

INDICE DE ANEXOS

CAPITULO I

MARCO TEORICO REFERENCIAL

1.1 INTRODUCCION

El protocolo de red más utilizado en la actualidad es la combinación del Protocolo de Control de Transmisión con el Protocolo de Internet (TCP/IP). El protocolo TCP/IP junto a su jerarquía de protocolos relacionados ofrecen muchas ventajas y fortalezas, pero la administración e implementación de Calidad de Servicio (QoS) no están entre ellas.

El Protocolo de Control de Transmisión (TCP) es considerado un mecanismo de transporte confiable, gracias a dos mecanismos: el primero es un mecanismo que intercambia información de control como números de secuencia y reconocimientos, y el segundo es un mecanismo de control de flujo de ventana deslizante manejado por el receptor. El segundo mecanismo controla el rendimiento de la red, así, el receptor reconoce la recepción inicial de datos, entonces anuncia cuantos datos puede manejar (ventana deslizante), finalmente el emisor puede transmitir datos hasta el tamaño de la ventana anunciado por el receptor. En realidad, el control de flujo del protocolo de control de transmisión es manejado por el mecanismo de ventana deslizante, pero existe un algoritmo llamado “slow start”, el cual altera el control de flujo del protocolo de transmisión. El algoritmo “slow start” intenta tomar ventaja total de la capacidad de la red con un incremento exponencial de la tasa de transmisión, este algoritmo usa una ventana de congestión como un mecanismo de control de flujo manejado por el emisor. Como resultado, el modo de operación del protocolo de control de transmisión para cada conexión individual en una red, es usar todo el ancho de banda disponible, mientras al mismo tiempo reaccionar y deducir problemas, para entonces tratar de aliviar la congestión, este modo de operación puede resultar problemático.

La congestión afecta a muchas redes de organizaciones con un ancho de banda limitado, por lo que a menudo, cuando existe congestión, los enlaces de Red de Área Amplia (WAN) no pueden manejar adecuadamente incrementos en el tráfico y las aplicaciones sensibles. Además, la congestión aumenta debido a mayores demandas de tráfico, usuarios de alta velocidad, tráfico web interactivo, aplicaciones basadas en web, arquitecturas par a par, aplicaciones basadas en servidor, entre otras, dando como resultado una baja en el rendimiento de la organización.

Ante el problema de congestión se propone dos soluciones: la primera solución es aumentar el ancho de banda del enlace red de área amplia, lo cual en la mayoría de los casos resulta demasiado costoso y con el paso del tiempo no solucionará definitivamente el problema; la segunda solución es implementar calidad de servicio al enlace red de área amplia y al protocolo TCP/IP, esta solución optimiza los recursos de red como ancho de banda, retardos y pérdidas de paquetes. La deficiencia de calidad de servicio del protocolo TCP/IP se intenta aliviar utilizando sistemas o elementos de red como ruteadores switches y **sistemas administradores de ancho de banda dedicados**, los cuales implementan estándares y procedimientos como: reservación de ancho de banda, clasificación por etiquetas, combinaciones de bits dentro de paquetes, prioridad, encolamiento de paquetes, mecanismos de control de protocolos, planeamiento y mecanismos de anulación de congestión.

Los sistemas administradores de ancho de banda son elementos ó cajas dedicadas, los cuales se colocan generalmente entre el ruteador del enlace de Red de Area Amplia (WAN) y el switch - hub de la Red de Area Local (LAN). Para implementar servicio diferenciado - calidad de servicio, los sistemas administradores de ancho de banda utilizan criterios técnicos como: monitoreo, clasificación, control y reportes; del tráfico generado por aplicaciones y protocolos dentro del enlace de red de área amplia.

El objetivo del proyecto es implementar una guía teórica-práctica para la solución de calidad de servicio de enlaces de Red de Area Amplia (WAN), utilizando **sistemas administradores de ancho de banda dedicados,** con este estudio se logrará conocer el tipo de calidad de servicio que implementan, los procedimientos que utilizan para ello, su

configuración; con el fin de realizar una prueba real del comportamiento del sistema administrador de ancho de banda aplicado sobre un enlace de red de área amplia e Internet.

La importancia del proyecto consiste en analizar: la teoría del protocolo más utilizado en la actualidad (TCP/IP), calidad de servicio para este protocolo, estudiar y comparar soluciones con las que se puede implementar calidad de servicio, y un estudio teórico-práctico de una solución mediante sistemas administradores de ancho de banda. Este estudio guiará al lector a la hora de adquirir un sistema administrador de ancho de banda para implementar calidad servicio, debido a que podrá tener una visión general de los sistemas administradores de ancho de banda.

La primera parte del proyecto describe un estudio preliminar del protocolo de control de transmisión, calidad de servicio, los términos utilizados en calidad de servicio y tipos de calidad de servicio.

La segunda parte del proyecto describe elementos de red existentes, específicamente se hará referencia a la marca Cisco, por ser una marca que ha sido líder en la implementación de los procedimientos que se utilizan para calidad de servicio; posteriormente se estudiará algunos sistemas administradores de ancho de banda, específicamente los preferidos a nivel mundial y en nuestro medio, ellos son NetEnforcer de Allot y PacketShaper de Packeteer, también se mencionará un tercer administrador de ancho de banda que es Accelerator de Expand; finalmente se realizará una comparación de procedimientos entre todos los sistemas.

La tercera parte del proyecto describe la configuración de un sistema administrador de ancho de banda, la configuración incluye: configuración inicial, monitoreo, análisis, clasificación y control. También se menciona una descripción de los protocolos y aplicaciones que un administrador de ancho de banda descubre automáticamente.

La cuarta parte del proyecto describe una prueba real del sistema administrador descrito en la tercera parte, la tercera y cuarta parte del proyecto se harán utilizando específicamente el sistema administrador de ancho de banda PacketShaper, debido al

liderazgo de PacketShaper entre los sistemas administradores y a la disponibilidad física del mismo.

La parte final del proyecto es desarrollar un esquema de políticas o reglas que puedan aplicarse a los flujos de tráfico que atraviesen un enlace de red de área amplia, este enlace se administrará utilizando un sistema administrador de ancho de banda, el desarrollo del esquema de políticas estará basado en las pruebas realizadas en la cuarta parte del proyecto.

1.2 MODELO DE REFERENCIA ISO/OSI

Debido al ambiente de red propietaria que existió a mediados de los años 1970, en 1978 la Organización Internacional de Estándares (ISO) comenzó el desarrollo de un modelo para protocolos de comunicación de computadores, el cual permitiría a las redes interoperar entre ellas. Como resultado en 1984 se publicó el modelo de Interconexión de Sistemas Abiertos (ISO/OSI) que permitió la interconexión de multivendedores y fue ampliamente aceptado, el modelo consta de siete capas. Es importante mencionar las capas de este modelo de referencia para entender el funcionamiento del Protocolo de Control de Transmisión - Protocolo de Internet (TCP/IP) y de los sistemas administradores de ancho de banda que se basan en las capas de este modelo.

1.2.1 Capa física.

La capa física describe las especificaciones físicas, eléctricas y de procedimientos requeridos para transmitir datos a través del medio físico o cables. También define conectores, la descripción de pines y niveles de corriente y voltaje. La capa física distribuye en unidades de bits.

1.2.2 Capa de enlace de datos.

La capa de enlace de datos mantiene una conexión fiable entre nodos adyacentes, particularmente para un canal físico propenso a error o ruido. Debe empaquetar los bits en bloques de datos, provee un mecanismo para direccionar nodos múltiples o estaciones de trabajo, y provee conexiones nodo a nodo, libres de error. La capa de enlace de datos distribuye en unidades de bloques.

1.2.3 Capa de red.

La capa de red es responsable del encaminamiento, conmutación y controla el flujo de información entre computadores. Existe una pequeña responsabilidad de la capa de red para Redes de Área Local (LAN) si hay solamente un camino de transmisión o una sola ruta. La capa de red es bastante importante para redes de área amplia o redes interconectadas. Las capas 1 hasta la 3, tomándolas colectivamente, constituyen las subredes de comunicaciones, una colección de nodos de conmutación que proveen un camino para los paquetes de datos. La capa de red distribuye en unidades de paquetes.

1.2.4 Capa de transporte.

La capa de transporte garantiza una conexión computador a computador libre de error, es decir asegura fiabilidad fuente a destino ó extremo a extremo. En muchos casos la red de comunicaciones requiere unidades de datos más pequeñas que la longitud del mensaje de la capa de transporte, por esto otras tareas de la capa de transporte son: separar el mensaje de longitud arbitraria en unidades más pequeñas, manejar sus transmisiones a través de la subred de comunicaciones y asegurar su correcto reensamblamiento en el extremo distante. La capa de transporte y las capas superiores distribuyen en unidades de mensajes.

1.2.5 Capa de sesión.

La capa de sesión establece y termina las sesiones de comunicación entre procesos de computadores. También maneja la sesión, desarrollando sincronización y traducción entre las bases de datos de nombre y dirección.

1.2.6 Capa de presentación.

La capa de presentación traduce el formato de datos del emisor al formato de datos del receptor. La capa de presentación provee servicios de usuarios, tales como conversión de código, compresión de datos o encriptación de archivos.

1.2.7 Capa de aplicación.

La capa de aplicación provee protocolos para aplicaciones o funciones comunes de usuario final, tales como transferencia de archivos, e-mail, manejo de red, o acceso remoto a bases de datos.

1.2.8 Modelo de interconexión de sistemas abiertos en redes de área amplia.

Cuando una red de área amplia conecta dos computadores, el modelo de interconexión de sistemas abiertos debe incluir componentes de red de área amplia, en la Figura 1.1. se observa que los nodos solo comprenden las capas de la uno a la tres, mientras que los computadores todas las siete capas. La capa de transporte es la primera capa extremo a extremo, asegurando entrega fiable de mensajes entre computadores.

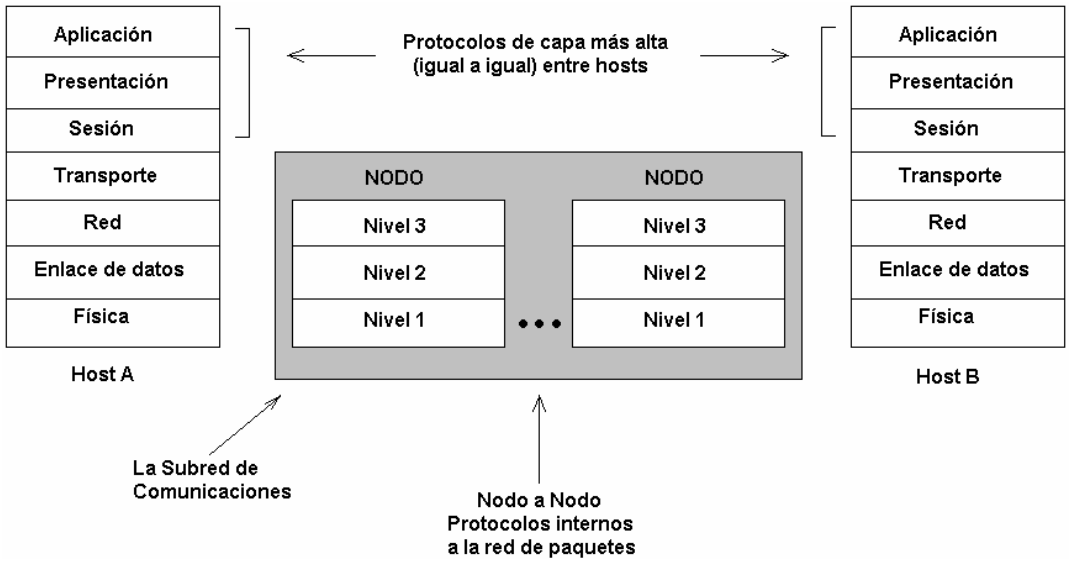


Figura. 1.1. Modelo de interconexión de sistemas abiertos en redes de área amplia.

1.2.9 Aplicando el modelo OSI a redes de área local.

En la Figura 1.2. se observa que la capa física es solo hardware, es decir cables, conectores, etc. Por otra parte las capas de usuario final, es decir desde la cuatro a la siete son solo software. La capa de enlace de datos puede ser una combinación de hardware y firmware, tales como manejadores de protocolo y circuitos integrados de memoria, que implementan funciones de software o alguna combinación de hardware - software. En la Figura 1.2. también se observa el modelo de interconexión de sistemas abiertos explicando las funciones y componentes de la red de área local para cada capa.

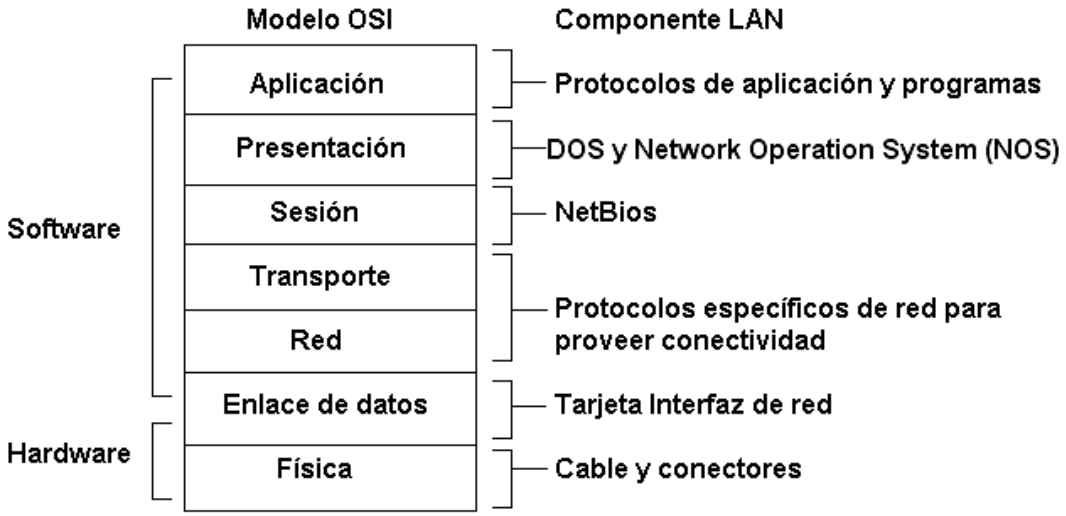


Figura. 1.2. Modelo de interconexión de sistemas abiertos en redes de área local.

1.3 PROTOCOLO TCP/IP

El protocolo TCP/IP no inició como un protocolo de red de área local, su inicio fue dado por la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) y esto dio como resultado la creación de la Red Avanzada de Agencias para Proyectos de Investigación (ARPANET), de la cual se desprendería el Departamento de Defensa de Estados Unidos (MILNET). ARPANET haría su evolución en lo que ahora es el Internet, que es la red con millones de usuarios conectados a ella.

TCP/IP está compuesto realmente de dos protocolos, el primero es Protocolo de Internet (IP) que se encarga del ruteo en capa 3, y el segundo es el Protocolo de control de Transmisión (TCP) que se encarga del transporte de datos extremo a extremo en capa 4. En la Figura 1.3. se observa una comparación entre el modelo de interconexión de sistemas abiertos y el modelo del protocolo TCP/IP.

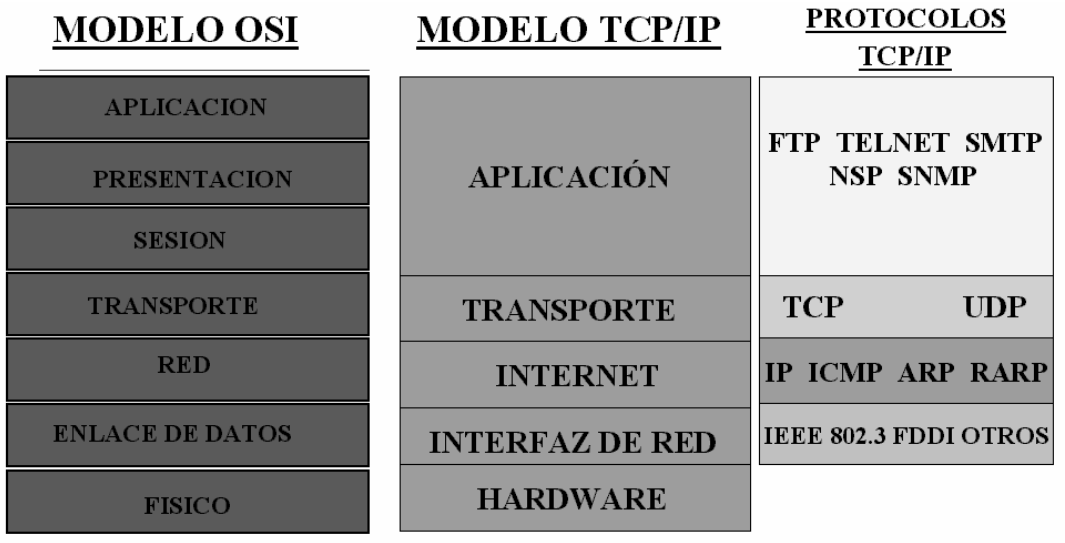


Figura. 1.3. Comparación entre el modelo OSI y el modelo del protocolo TCP/IP

1.3.1 Protocolo de Internet (IP).

El protocolo de Internet define: la unidad básica para la transferencia de datos, selección de rutas, conjunto de reglas para la entrega no confiable de paquetes, y además toma los datos del nivel superior (transporte) para insertarlos en la Internet como unidades de mensaje IP (datagramas). El protocolo de Internet utiliza el Protocolo de Mensajes de Control de Internet (ICMP) para reportar errores, se basa en servicio no orientado a la conexión, no es confiable, y no garantiza que el datagrama llegue a su destino. El protocolo de Internet es un servicio de entrega con el mejor esfuerzo (best effort). Los datagramas son independientes, es decir no hay relación entre ellos, los datagramas viajan por distintas redes como Ethernet, FDDI, Frame Relay, X.25, Token Ring, etc., para esto el protocolo de Internet puede tratar la fragmentación y el reensamblado de sus datagramas. Cada fragmento de los datagramas tiene una cabecera, la cual es copiada básicamente del datagrama original y de los datos que lo siguen. Los fragmentos se tratan como datagramas normales mientras son transportados a su destino, sin embargo si uno de los fragmentos se pierde, todo el datagrama se considerará perdido. En la Figura 1.4. se observa un esquema más detallado de la jerarquía de protocolos TCP/IP según sus capas.

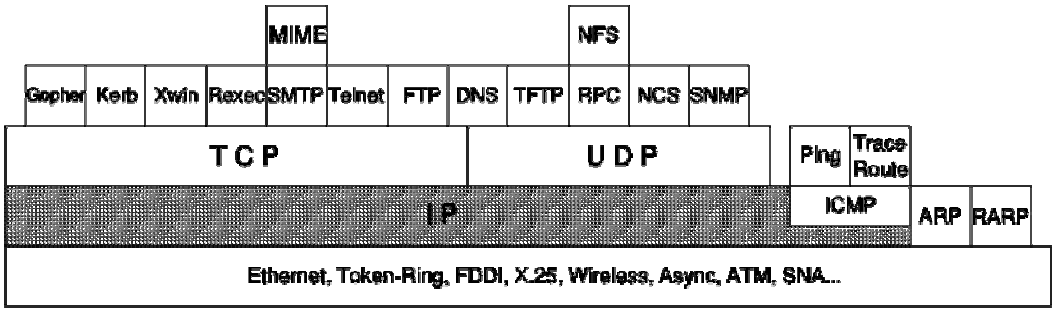


Figura. 1.4. Esquema de la jerarquía de protocolos de TCP/IP.

1.3.2 Formato del datagrama IP.

La cabecera del datagrama IP es de un mínimo de 20 bytes de longitud, en la Figura 1.5. se observa el formato del datagrama IP.

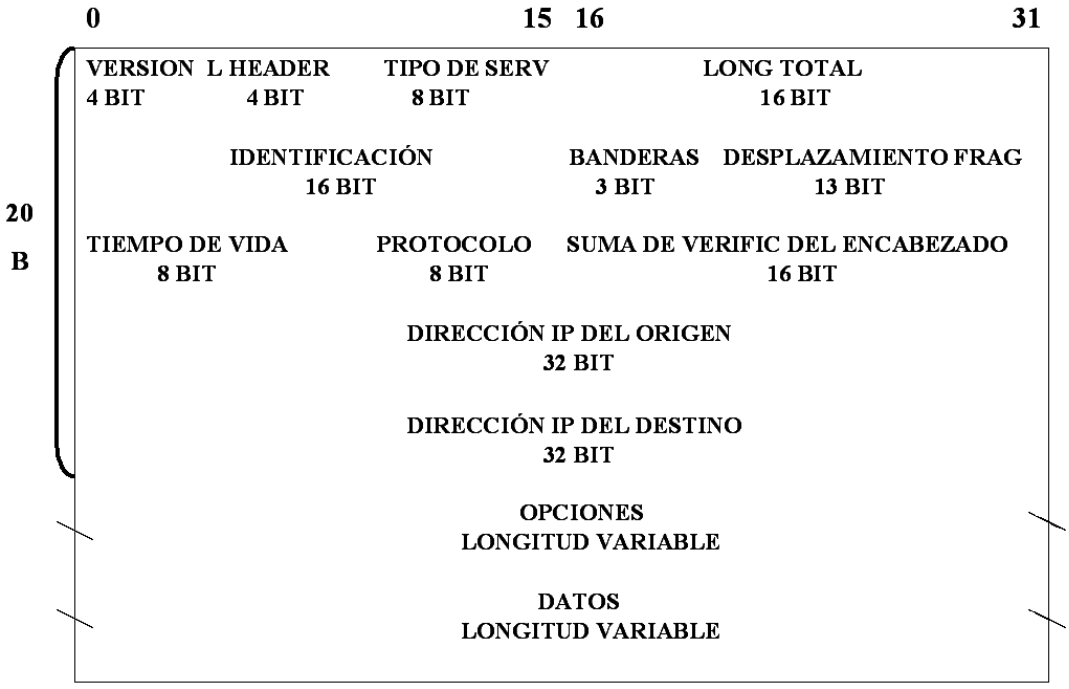


Figura. 1.5. Formato del datagrama IP.

Donde:

- *Versión.*- La versión del protocolo IP.

- *L. Header.*- La longitud de la cabecera IP contada en cantidades de 32 bits. Esto no incluye el campo de datos.

- *Tipo de Servicio.*- El tipo de servicio es una indicación del tipo y prioridad del servicio solicitado para este datagrama IP, en la Figura 1.6. se observa el formato de los bits del tipo de servicio.

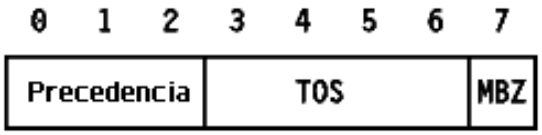


Figura. 1.6. Bits de tipo de servicio.

Donde:

- *Precedencia.*- Es una medida de la naturaleza y prioridad de este datagrama, en la Tabla 1.1. se observa la combinación de los tres bits y como definen la prioridad.

Combinación	Prioridad
000	Rutina
001	Prioridad
010	Inmediato
011	Relámpago
100	Sobre relámpago
101	Crítico
110	Control de interconexión de redes
111	Control de red

Tabla. 1.1. Combinación de bits que definen prioridad de datagrama.

- *TOS.*- En la Tabla 1.2. se observa la combinación de los cuatro bits y como definen el tipo de servicio.

Combinación	Tipo de Servicio
1000	Minimizar retardo
0100	Maximizar la densidad de flujo
0010	Maximizar la fiabilidad
0001	Minimizar el costo monetario
0000	Servicio normal

Tabla. 1.2. Combinación de bits que definen tipo de datagrama.

- *MBZ.*- Reservado para uso futuro debe ser cero, a menos que participe en un experimento con IP que haga uso de este bit.

- *Longitud total.*- La longitud total del datagrama, cabecera y datos, especificada en bytes.

- *Identificación.*- Un número único que asigna el emisor para ayudar a reensamblar un datagrama fragmentado. Los fragmentos de un datagrama tendrán el mismo número de identificación.

- *Banderas.*- Usadas para llevar información de control sobre la fragmentación del datagrama.

- *Desplazamiento fragmento.*- Usado con datagramas fragmentados, para ayudar al reensamblado de todo el datagrama.

- *Tiempo de vida.*- Especifica el tiempo en segundos que se le permite viajar a este datagrama. Cada ruteador por el que pase este datagrama ha de sustraer de este campo el tiempo tardado en procesarlo. En la realidad un ruteador es capaz de procesar un datagrama en menos de 1 segundo; por ello restará uno de este campo y el tiempo de vida se convierte más en una cuenta de saltos que en una métrica del

tiempo. Cuando el valor alcanza cero, se asume que este datagrama ha estado viajando en un bucle y se desecha. El valor inicial lo debería fijar el protocolo de alto nivel que crea el datagrama.

- *Protocolo.*- Indica el número de protocolo de alto nivel al que IP debería entregar los datos del datagrama.

- *Suma de verificación.*- Suma binaria en complemento a uno de cabeceras para detección de errores en el datagrama.

- *Dirección IP del origen.*- La dirección IP de 32 bits del elemento emisor.

- *Dirección IP del destino.*- La dirección IP de 32 bits del elemento receptor.

- *Opciones:* No requiere que toda implementación de IP sea capaz de generar opciones en los datagramas que crea, pero sí que sea capaz de procesar datagramas que contengan opciones. Puede haber cero o más opciones. Hay dos formatos para estas. Es usado para pruebas de red, depuración u opciones de encaminamiento.

- *Datos:* Los datos contenidos en el datagrama se pasan a un protocolo de nivel superior, como se especifica en el campo protocolo.

1.3.3 Puertos y zócalos.

Un puerto es un número de 16 bits empleado por un protocolo computador a computador para identificar a que protocolo del nivel superior o programa de aplicación se deben entregar los mensajes recibidos. Estos puertos son controlados y asignados por la Autoridad de Números Asignados a Internet (IANA) y en la mayoría de los sistemas sólo los puede utilizar los procesos del sistema o los programas que ejecutan usuarios privilegiados. Ocupan número de puerto comprendidos en el rango de 0 a 1023. Los

puertos con números en el rango de 1024 a 65535 no los controla IANA y en la mayor parte de los sistemas los pueden usar los programas de usuario.

Los principales protocolos de transporte están basados en el principio de uso de los puertos y se usan los mismos números en la medida de lo posible. Un zócalo es un tipo especial de descriptor de archivo que un proceso usa para solicitar servicios de red al sistema operativo, también es un punto terminal para la comunicación que puede ser nombrado y direccionado en una red, es básicamente la combinación de una dirección IP y un número de puerto.

1.3.4 Protocolo de Datagrama de Usuario (UDP).

El protocolo de datagrama de usuario es un protocolo de transporte que complementa a IP, no añade fiabilidad, control de flujo o recuperación de errores. Simplemente sirve como multiplexor/demultiplexor para enviar y recibir datagramas, usando los puertos de origen y destino para dirigir los datagramas, el control de flujo y recuperación de errores deben ser realizados por el programa de aplicación que use el protocolo de datagrama de usuario para el transporte.

Los datos de las aplicaciones se encapsulan en datagramas del protocolo de datagrama de usuario independientes de otras capas, cada datagrama del protocolo de datagrama de usuario se envía en un sólo datagrama de IP. Aunque el datagrama IP se fragmente durante la transmisión, la implementación de IP que lo reciba lo reensamblará antes de pasárselo a la capa de protocolo de datagrama de usuario. En la Tabla 1.3. se observa algunas asignaciones de puertos del protocolo de datagrama de usuario.

Número de puerto	Descripción
11	Usuarios activos
19	Generador de caracteres
37	Tiempo
53	Servidor de nombres de dominio
69	Descarga de archivos trivial
161	Monitor de red del protocolo de administración de red simple
162	Mensajes del protocolo de administración de red simple
514	Registro de sistema

Tabla. 1.3. Algunas asignaciones de puertos del protocolo de datagrama de usuario.

1.3.5 Protocolo de Control de Transmisión (TCP).

El protocolo de control de transmisión al igual que el protocolo de datagrama de usuario es un protocolo de la capa de transporte, pero es diferente al protocolo de datagrama de usuario en que permite intercambiar datos confiablemente entre estaciones de la red, también provee multiplexación/demultiplexación de puertos para identificar una aplicación en el computador.

Este protocolo de control usa números de secuencia y reconocimientos para conversar con otra estación en la red, los números de secuencia básicamente permiten el ordenamiento de los datos en los paquetes debido a que en una red los paquetes podrían no llegar en el mismo orden en el que fueron enviados, además permiten buscar paquetes perdidos. Los reconocimientos son usados para que el elemento que emite los paquetes tenga conocimiento de la llegada de los paquetes al elemento receptor.

Es un protocolo de secuenciamiento orientado al byte porque asigna un número de secuencia a cada byte dentro de los paquetes, lo cual suena un poco repetitivo pero originalmente fue diseñado para líneas seriales que introducían demasiado ruido y no redes de alta velocidad.

Con este protocolo una aplicación transmite datos haciendo una llamada al software del protocolo de control de transmisión y entonces pasa datos a este, el protocolo de control de

transmisión encapsula estos datos en segmentos y a su vez hace una llamada al software IP para que este transmita los datos al destino. El software del protocolo de control de transmisión del elemento receptor desencapsula los datos desde los paquetes y notifica el proceso correcto, es decir que estos datos han llegado.

1.3.5.1 Encabezado TCP.

En la Figura 1.7. se observa el encabezado usado por el protocolo TCP para el transporte y como este encaja en el formato de paquetes ethernet.

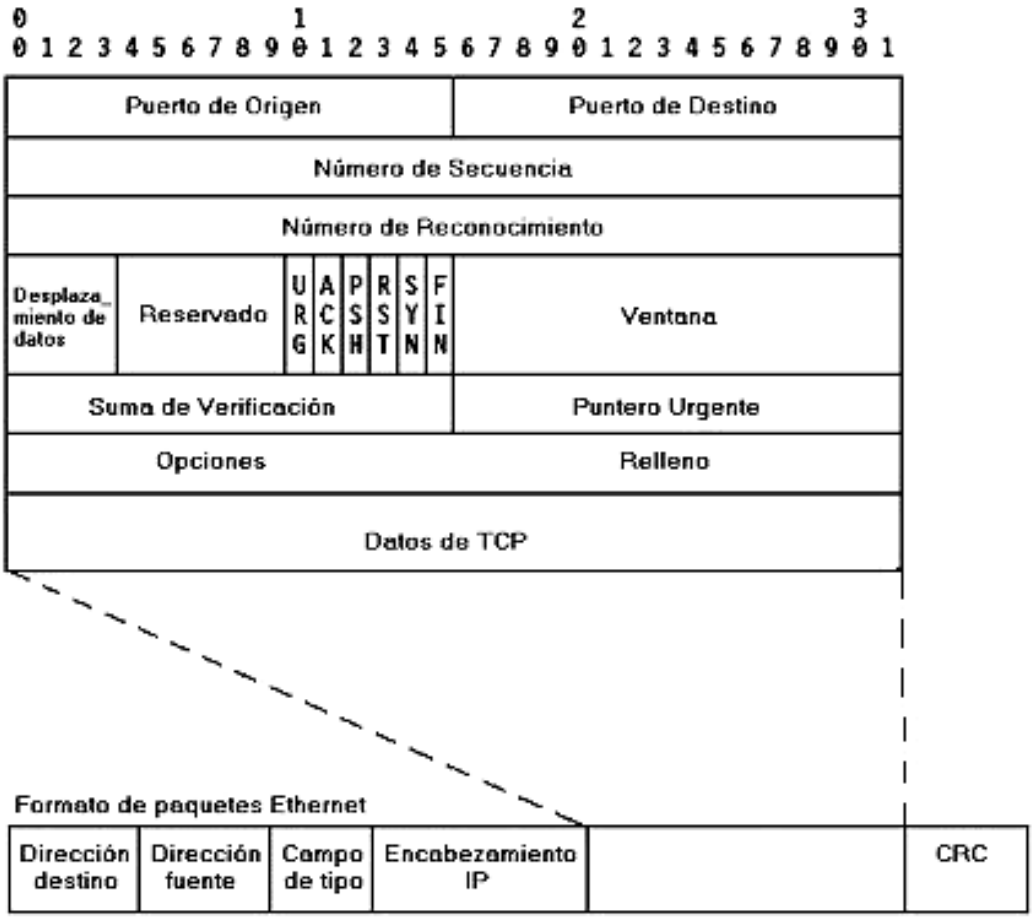


Figura. 1.7. Formato del encabezado TCP.

Donde:

- *Puerto de origen.*- El número de puerto de 16 bits del emisor, que el receptor usa para responder.

- *Puerto de destino.*- El número de puerto de 16 bits del receptor.

- *Número de secuencia.*- Asignado a paquetes TCP para indicar el número de byte inicial de un paquete de datos (varios bytes) a menos que el bit SYN sea 1, si este es el caso, el número de secuencia es el Número Inicial de Secuencia (ISN) aleatorio con un rango de 0 a 2,147,483,647 usado para establecer una conexión, luego el primer byte de datos es ISN+1.
- *Número de reconocimiento.*- Enviado por la estación de destino hacia la estación fuente, indicando un reconocimiento de un paquete o paquetes recibidos previamente. Si el bit de control ACK está a 1, este número indica el próximo número de secuencia que la estación de destino espera recibir. Una vez que la conexión es establecida, este campo está siempre fijo a 1.

- *Desplazamiento de datos.*- El número de palabras de 32 bits en el encabezado TCP, indica cuan largo es el encabezado TCP, es decir indica donde empiezan los datos y donde el encabezado TCP se suspende.

- *Reservado.*- Seis bits reservados para su uso futuro, deben ser cero.

- *Bits de control.*- Existen seis bits de control como se observa en la Tabla 1.4.

Bit de control	Función
ACK	Si es uno, este paquete contiene un reconocimiento.
PSH	Función push ó apuro.
RST	Reinicia la conexión. Una función para este es no aceptar una demanda de conexión.
SYN	Usado para establecer número de secuencia inicial.
FIN	No más datos vienen desde el emisor de la conexión.
URG	Puntero urgente.

Tabla. 1.4. Bits de control del encabezado TCP.

- *Ventana.*- Usado en segmentos de reconocimiento, especifica el número de bytes de datos que el receptor esta dispuesto a aceptar para cada paquete de datos que envíe el emisor.

- *Suma de verificación.*- Un número de detección de errores.

- *Puntero urgente.*- El puntero urgente apunta al número de secuencia del byte que sigue a los datos urgentes o importantes. Este campo es interpretado solamente en segmentos con el bit URG a 1.

- *Opciones.*- Es de longitud fija o variable, sólo para el caso de opciones de datagramas IP, las opciones pueden ser fin de la lista de opciones, no operación, tamaño máximo del segmento.

1.3.5.2 Establecimiento de la conexión de TCP.

A diferencia del Protocolo de Datagrama de Usuario (UDP), una conexión TCP entre dos estaciones debe ser establecida antes de que algún dato pueda pasar entre los dos. Las aplicaciones usan TCP a través de una serie de llamadas, estas incluyen abrir y cerrar una conexión, enviar y recibir a esa conexión, así como recibir estatus para una conexión.

Antes de que se pueda transferir cualquier dato, se ha de establecer una conexión entre los dos procesos. Normalmente el servidor lanza una llamada abrir pasiva, el otro elemento lanza una llamada abrir activa indicando el puerto de la aplicación que recibirá los datos, la estación que hace la llamada activa asigna aleatoriamente su propio puerto y cada conexión de cada estación con un servidor a la misma aplicación se diferencia por zócalos (IP y puerto). El abrir pasivo permanece dormido esperando hasta que otro proceso intente comunicarse con él a través de un abrir activo, TCP notará la aplicación a través del asignamiento de puertos.

Para el establecimiento de la conexión se intercambian tres segmentos TCP, este proceso completo se conoce como acuerdo en tres fases (handshake), los segmentos TCP intercambiados incluyen los números de secuencia iniciales de ambas partes, para ser usados en posteriores transferencias, en la Figura 1.8. se observa un diagrama del intercambio.

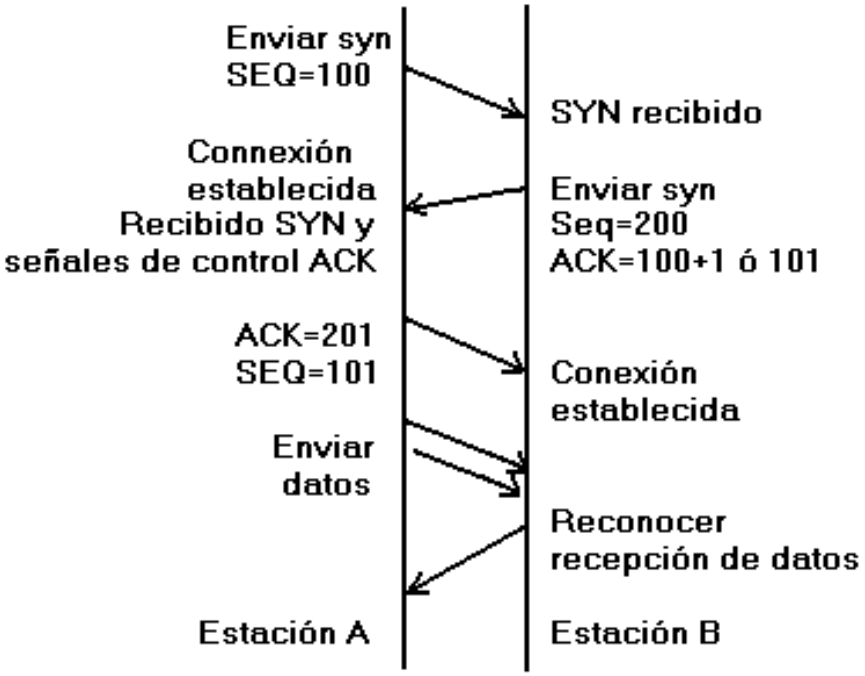


Figura. 1.8. Intercambio de segmentos de control de TCP.

En este proceso la estación A pone una llamada abrir activa a TCP para pedir conexión a una aplicación de estación remota de la red. La estación A construirá un encabezado

TCP con el bit SYN a 1 y entonces asigna un número inicial de secuencia (100) y lo pone en el campo de número de secuencia. Otros campos también son fijados en el encabezado TCP y el paquete será dado al protocolo IP para la transmisión a la estación B.

Luego la estación B recibirá este paquete y se da cuenta de un intento de conexión, si la estación B puede aceptar una conexión nueva reconocerá a la estación A construyendo un paquete nuevo. La estación B pondrá los bits SYN y ACK a 1 en el encabezado TCP, poniendo su propio número inicial de secuencia (200) y el campo de reconocimiento se fijará a 101 que es el número de secuencia de la estación A mas uno y a la vez es el número de secuencia que espera recibir posteriormente por parte de la estación A.

Seguidamente la estación A recibirá este paquete de respuesta y se da cuenta que es un reconocimiento para la conexión pedida. La estación A construirá un nuevo paquete, pone el bit ACK a 1, llena en el número de secuencia con 101, llena el número de reconocimiento con 200+1, y envía el paquete a la estación B. Una vez que se ha establecido la conexión, los datos y comandos de la aplicación pueden pasar sobre la conexión y cada lado de la misma mantendrá su propia tabla de números de secuencia.

1.3.5.3 Números de secuencia y reconocimientos durante el flujo de datos de TCP.

TCP calcula un número de secuencia para cada byte de datos en el segmento tomándolo como una suma. Para cada byte de datos a ser transmitido, el número de secuencia se incrementa en uno. En la Figura 1.9. se observa una conexión entre dos estaciones, la estación A envía un paquete de 4 bytes a la estación B con un número de secuencia 40 (primer byte del paquete de 4 bytes), el reconocimiento desde la estación B contiene el numero de reconocimiento 44 (número de secuencia que espera recibir), la estación A transmitirá el segundo paquete de 7 bytes con número de secuencia 44 a la estación B, el reconocimiento desde la estación B contiene el numero de reconocimiento 51.

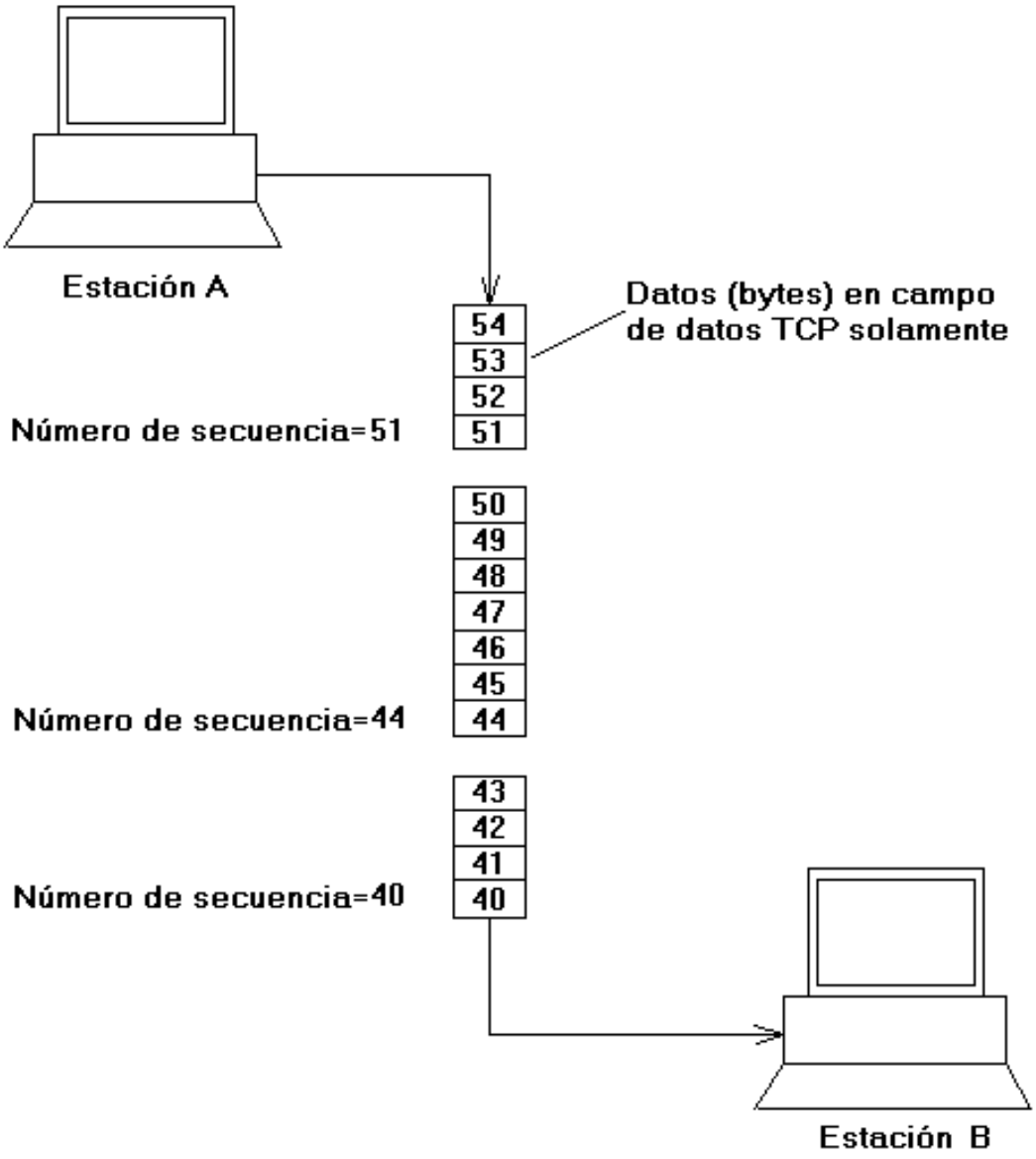


Figura. 1.9. Secuenciamiento de bytes en TCP.

Cada paquete contendrá tantos bytes como la ventana de transmisión lo permita, TCP logra comunicación bidireccional a través de la misma conexión. Cada paquete tendrá el bit ACK a 1, el número de reconocimiento es rellenado dentro de los paquetes de datos para hacer a TCP más eficiente y su cálculo se observa en la Ecuación 1.1.

Número de reconocimiento = Número de secuencia (primer byte) + bytes recibidos exitosamente (subsiguientes) + 1

Ecuación. 1.1. Cálculo del número de reconocimiento.

Este es un método rápido y eficiente para determinar que bytes fueron recibidos exitosamente y cuales no, el emisor debe guardar una copia del paquete enviado mientras no reciba el reconocimiento del receptor. Si el emisor no recibe el reconocimiento en un tiempo especificado, retransmitirá los datos empezando desde el primer byte no reconocido, después de un número de retransmisiones no exitosas TCP dará tiempos sin respuesta para la conexión.

1.3.5.4 Mecanismo de ventana deslizante en forma general.

Con este mecanismo el receptor de una conexión al enviar un reconocimiento al emisor indica también el número de bytes que puede recibir sin que se produzca sobrecarga y desbordamiento de su memoria intermedia interna (buffers). El receptor envía este valor para recibir sin problemas en el reconocimiento que para el emisor es el número de secuencia (datos) más elevado que puede alcanzar o enviar, este se conoce como mecanismo de ventanas. El mecanismo de ventana deslizante se observa en la Figura 1.10. este mecanismo en forma general utiliza las siguientes reglas:

- El emisor puede enviar todos los paquetes dentro de la ventana sin recibir un reconocimiento, pero debe disparar un cronómetro para el tiempo de cada uno de ellos.

- El receptor debe reconocer cada paquete recibido indicando el número de secuencia del último paquete bien recibido.

- El emisor desliza la ventana para cada reconocimiento recibido.

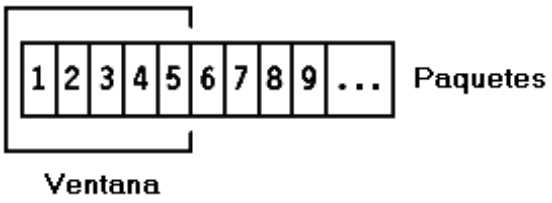


Figura. 1.10. Método de ventana deslizante.

En la Figura 1.11. se observa al emisor transmitiendo paquetes con número de secuencia del 1 al 5 sin esperar respuesta.

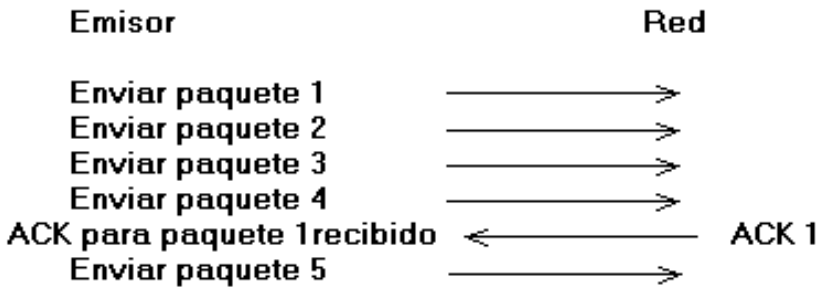


Figura. 1.11. Transmisión de 5 paquetes y recepción de reconocimiento 1.

En el momento en que el emisor recibe el reconocimiento 1, puede deslizar su ventana para excluir el paquete 1, como se observa en la Figura 1.12.

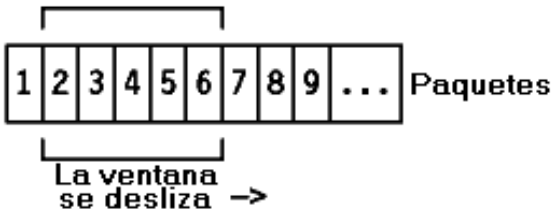


Figura. 1.12. Deslizamiento de la ventana.

En este punto, el emisor puede transmitir el paquete 6, también se puede imaginar algunos casos especiales:

- El paquete 2 se pierde, el emisor no recibirá el reconocimiento 2, luego reconocerá los paquetes 3, 4 y 5 con un reconocimiento 1, que fueron los últimos paquetes recibidos en secuencia por lo que su ventana permanecerá en posición 2 como se observa en la Figura 1.12. El emisor después de un tiempo indica la retransmisión del paquete 2. La recepción del paquete 2 en el receptor generará un reconocimiento 5, ya que se habrán recibido con éxito los paquetes del 1 al 5, y la ventana del emisor se deslizará cuatro posiciones al recibir el reconocimiento 5.

- El paquete 2 llegó, pero el emisor no recibe el reconocimiento 2 porque se perdió, pero recibe el reconocimiento 3. El reconocimiento 3 es un reconocimiento de todos los paquetes hasta el 3 incluyendo el 2 y el emisor ya puede deslizar su ventana hasta el paquete 4.

1.3.5.5 Mecanismo de ventana deslizante aplicado en TCP.

El mecanismo de ventana deslizante se utiliza en TCP, pero con unas cuantas diferencias:

- Como TCP proporciona una conexión con un flujo de bytes, los números de secuencia se asignan a cada byte del canal. TCP divide el flujo de bytes en segmentos. El principio de la ventana se aplica a nivel de bytes, es decir los segmentos enviados y los reconocimientos recibidos llevarán números de secuencia de forma que el tamaño de la ventana se exprese con un número de bytes en vez de número de paquetes.

- El tamaño de la ventana lo determina el receptor cuando se establece la conexión y puede variar durante la transmisión de datos. Cada reconocimiento incluirá el tamaño de la ventana que acepta el receptor en ese momento en el campo de ventana del encabezado TCP.

Con el mecanismo de ventana deslizante TCP consigue, transmisión fiable y control de flujo, el receptor conociendo la memoria libre de la que dispone asigna el tamaño de ventana que incluso podría ser cero si el receptor no puede aceptar datos, excepto si el bit URG está a 1, lo que significa que esos datos deben ser recibidos inmediatamente.

1.3.5.6 Finalización de una conexión TCP.

La finalización de una conexión se logra mediante el bit FIN del encabezado TCP, como la conexión TCP es bidireccional (full-duplex), cada lado de la conexión debe cerrar la misma, debido a que segmento FIN sólo cierra la conexión en un sentido del canal.

1.3.5.7 Tiempos sin respuesta de conexión TCP.

Si el emisor no recibe el reconocimiento de bytes de paquetes en un tiempo especificado, retransmitirá los datos empezando desde el primer byte no reconocido, después de un número de retransmisiones no exitosas TCP dará tiempos sin respuesta para la conexión o tiempo fuera (time out).

TCP registra el momento de envío de un segmento y registra también el tiempo de recepción del reconocimiento. Se promedia un valor para varios de estos viajes que se empleará como valor de tiempo sin respuesta de conexión para el siguiente segmento a enviar.

El tiempo fuera es una característica importante debido a que los retardos pueden ser variables en la red dependiendo de múltiples factores tales como la carga de las redes de área amplia o la saturación de ruteadores.

1.3.5.8 Algoritmos complementarios implementados en TCP.

Las implementaciones actuales del Protocolo de Control de Transmisión (TCP) contienen algoritmos entrelazados los cuales son parte de las publicaciones de las

Peticiones Para Comentar (RFC), entre los algoritmos principales están “slow start” y “congestion avoidance” que constan en los RFC 2001 y RFC 1122, estos algoritmos intentan mejorar el desempeño del protocolo TCP/IP.

1.3.5.8.1 “Slow Start”.

El protocolo TCP antiguo empieza una conexión con el emisor inyectando múltiples segmentos dentro de la red, hasta el tamaño de la ventana anunciada por el receptor, esto funciona bien para dos elementos en una misma red de área local, pero si hay ruteadores y enlaces lentos entre el emisor y el receptor los problemas aparecen. Los ruteadores deben encolar los paquetes y es posible que los ruteadores sufran de falta de espacio.

El algoritmo que intenta eliminar dichos problemas es “slow start”, el cual dice que la tasa en la que los paquetes deben ser inyectados dentro de la red por el emisor es la tasa en la que los reconocimientos son retornados desde el otro extremo, para esto se añade otra ventana al emisor llamada ventana de congestión (cwnd).

Con “slow start” cuando una conexión nueva es establecida con un elemento en otra red, la ventana de congestión es inicializada a un segmento que puede ser por ejemplo el tamaño de segmento anunciado por el receptor o por defecto 536 ó 512. Cada vez que un reconocimiento es recibido, la ventana de congestión es incrementada en un segmento, el emisor puede transmitir hasta el tamaño de su ventana de congestión y de la ventana deslizante del receptor. La ventana de congestión es un control de flujo impuesta por el emisor, mientras la ventana deslizante es un control de flujo impuesta por el receptor.

Así, el emisor empieza transmitiendo un segmento y esperando por su reconocimiento, cuando este es recibido la ventana de congestión es incrementada desde uno a dos, y dos segmentos pueden ser enviados, cuando cada segmento es reconocido, la ventana de congestión es incrementada a cuatro, esto prevé un crecimiento exponencial, aunque no es exactamente exponencial por que el receptor podría retardar los reconocimientos, típicamente enviando un reconocimiento por cada dos segmentos que este recibe. Así mismo la capacidad de la red puede rechazar el tráfico y un ruteador intermedio empezará

a descartar paquetes, esto le dice al emisor que la ventana de congestión es demasiado grande.

1.3.5.8.2 “Congestion Avoidance”.

La congestión puede ocurrir cuando los datos llegan desde una red de área local hacia una red de área amplia, es decir puede ocurrir cuando múltiples flujos llegan a un ruteador y su capacidad de salida es menor que la suma de sus entradas

Este algoritmo de anulación de congestión intenta aliviar la pérdida de paquetes, el algoritmo dice que la pérdida de paquetes causada por daños en la red es mucho menos que 1%, de ahí que la pérdida de paquetes que derivan en tiempos fuera y reconocimientos duplicados son señales de congestión entre la fuente y el destino.

En la práctica se implementan los algoritmos “slow start” y “congestion avoidance” juntos, “slow start” para aumentar la tasa de envío de paquetes y “congestion avoidance” para bajar la tasa de envío de paquetes cuando ocurre congestión, se requiere de dos variables para su funcionamiento la ventana de congestión y un umbral de comienzo (ssthres), los dos algoritmos operan de la siguiente forma:

- La inicialización para una conexión se da con una ventana de congestión de un segmento y un umbral de comienzo de 65535 bytes.

- La rutina de salida de TCP nunca envía más que el mínimo de la ventana de congestión y la ventana de advertencia del receptor.

- Cuando ocurre congestión, la mitad del tamaño mínimo de la ventana actual (el mínimo de la ventana congestión y la ventana de advertencia del receptor, pero al menos dos segmentos) es guardado en el umbral de comienzo. Adicionalmente si la congestión es indicada por tiempos sin respuesta de conexión, la ventana de congestión es puesta a un segmento (slow start).

- Cuando un dato nuevo es reconocido por el receptor, se incrementa la ventana de congestión, pero la forma en que se incrementa depende si TCP esta ejecutando “slow start” ó “congestion avoidance”. Si la ventana de congestión es menor o igual al umbral de comienzo TCP esta en “slow start”, caso contrario está ejecutando “congestion avoidance”. “Slow start” se ejecuta en TCP hasta que se presenten señales de congestión, entonces se guarda la mitad del tamaño de la ventana de congestión en el umbral de comienzo y se ejecuta “congestion avoidance”. “Congestion avoidance” dice que la ventana de congestión debe ser incrementada cada que un reconocimiento es recibido y calculado como segsize*segsize/cwnd (en bytes) donde segsize es el tamaño del segmento, dicho cálculo permite un crecimiento lineal y no exponencial (slow start) de la ventana de congestión, luego cuando se detecte señales de congestión se repite el proceso. Cada paquete lleva en su encabezado un sello de tiempo (timestamp), el receptor envía el sello de tiempo del último paquete recibido al emisor, este mide el tiempo cuando recibe este reporte y calcula el Tiempo de Viaje Redondo (RTT) como la diferencia entre el tiempo actual y el sello de tiempo del receptor. El aumento en la ventana de congestión debe ser al menos un segmento cada tiempo de viaje redondo.

1.4 CALIDAD DE SERVICIO (QOS)

Generalmente se piensa que se logrará mejorar una red incrementando el ancho de banda, pero como ya se ha explicado surge otro problema, la naturaleza del protocolo de control de transmisión el cual incrementa el ancho de banda de sus conexiones, consumiendo el ancho de banda y no necesariamente por el tráfico mas prioritario, y a la vez detectar congestión para reducir el ancho de banda de las conexiones teniendo enlaces más caros y que no tienen el rendimiento deseado, por lo que se ha definido la calidad de servicio en redes.

En el ámbito de las telecomunicaciones, según la publicación de 1984 del documento E-800 de la Unión Internacional de Telecomunicaciones (ITU), calidad de servicio es el efecto colectivo del rendimiento de un servicio que determina el grado de satisfacción del usuario de dicho servicio. En el ámbito de redes, calidad de servicio es la capacidad de un

elemento de red de asegurar que su tráfico y los requisitos del servicio previamente establecidos puedan ser satisfechos, estos son asegurar una tasa de datos o ancho de banda en la red, un retardo y una variación de retardo.

La calidad de servicio también suele ser definida como un conjunto de tecnologías como herramientas, protocolos, señalización y sistemas, que ayudan a la gestión de una red, tratan de evitar la congestión y proveer mejor servicio a ciertos flujos de datos, en lugar de ir aumentando continuamente capacidad, es necesario decir que la calidad de servicio no crea ancho de banda.

En este trabajo se estudiará específicamente el tipo de calidad de servicio que trata de usar eficientemente los enlaces de área amplia mediante sistemas administradores de ancho de banda dedicados, tratando de priorizar las aplicaciones más importantes para una organización, como bases de datos, aplicaciones de voz, aplicaciones en tiempo real y a la vez tratando de controlar los recursos, por ejemplo limitar al ancho de banda consumido por transferencias de archivos o aplicaciones para compartir de archivos.

La palabra servicio se asocia a flujos que sufren un tratamiento particular dentro del enlace, este tratamiento puede ser diferente al de todos los otros flujos. Un servicio puede ser tipo cualitativo o cuantitativo. Particularmente en un tipo de servicio cualitativo se usan varios parámetros que ayudan al estudio y comprensión de la calidad de servicio.

1.4.1 Definición de parámetros.

Son varios los parámetros manejados en el estudio de calidad de servicio, en este apartado se explicarán aquellos considerados importantes para el completo entendimiento de este trabajo.

1.4.1.1 Tráfico de red.

De forma simple se puede decir que tráfico de una red son los datos que la atraviesan, es dependiente del tipo de aplicación que por ella circulan, de esta manera se tiene una diferenciación del tráfico. Para utilizar sistemas administradores de ancho de banda se clasifica al tráfico (flujos) según el tipo de aplicación ó importancia para una organización, según la sensibilidad al retardo o latencia y según la sensibilidad a la inestabilidad (jitter); con esta clasificación se puede controlar eficientemente al tráfico de una red, principalmente minimizando el retardo y jitter de aplicaciones y protocolos críticos para una organización.

1.4.1.2 Retardo.

El retardo indica la variación temporal o retraso en la llegada de los flujos de datos a su destino, es una característica que se hace muy evidente en aplicaciones como la voz sobre protocolo IP, donde se experimenta cortes en la comunicación cuando el retardo de los paquetes es demasiado grande.

1.4.1.3 Latencia.

La latencia es el tiempo entre el envío de un mensaje por parte de un nodo y la recepción del mensaje por otro nodo. Abarca los retardos sufridos durante el propio camino o en los dispositivos por los que pasa. En un elemento de red como un ruteador, la latencia es la cantidad de tiempo existente entre la recepción de un paquete y su retransmisión, lo que también se conoce como retardo de propagación.

1.4.1.4 Jitter.

El jitter es la inestabilidad o variabilidad en el retardo, que ocurre cuando los paquetes transmitidos en una red no llegan a su destino en debido orden o en la base de tiempo

determinada., esta inestabilidad es particularmente perjudicial para el tráfico en tiempo real.

1.4.1.5 Ancho de banda.

El ancho de banda es una medida de la capacidad de transmisión de datos de un canal de comunicaciones, la transmisión digital pura se mide en bits o bytes por segundo, sin embargo la transmisión es expresada generalmente en Kilobits por segundo (Kbps) o en Megabits por segundo (Mbps), cabe mencionar que 1 Mbps es equivalente a 1024 Kbps. Indica la capacidad máxima teórica de una conexión, pero esta capacidad teórica se ve disminuida por factores negativos tales como el retardo de transmisión, que pueden causar un deterioro en la calidad.

Por ejemplo se tiene un ancho de banda de 1xE1 (estándar europeo) que es equivalente a 2 Mbps (2048 Kbps), cuando se habla del ancho de banda total de un enlace, es importante dejar un margen de guarda del enlace cuando se habla de porcentajes, debido a que el 100% del tamaño del enlace generalmente es menor a lo especificado aproximadamente en un 10% debido a información de encabezado necesaria para el enrutamiento, establecimiento y verificación de errores de un enlace. Así en un enlace de 1xE1, restándole una ranura (slot) de 64 Kbps utilizada por la información de señalización y una ranura de 64 Kbps utilizada por la Verificación Cíclica de la Redundancia (CRC4) tendría una capacidad neta de 1.875 Mbps equivalente al 93.75%.

Los sistemas administradores de ancho de banda poseen la capacidad de controlar el ancho de banda del enlace de Red de Area Amplia (WAN), puede asignar un porcentaje del ancho de banda total a aplicaciones y protocolos que atraviesen el enlace, el porcentaje que asigne el administrador de ancho de banda depende de la importancia de la aplicación o protocolo para la organización.

1.4.1.6 Pérdida de paquetes.

La pérdida de paquetes indica el número de paquetes perdidos durante la transmisión, normalmente se mide en tanto por ciento. Se toma en cuenta la cantidad de paquetes que llegan al receptor y la cantidad de paquetes transmitidos por el emisor, un ejemplo sería un enlace de área amplia que experimente 1% de pérdida de paquetes mensualmente.

1.4.1.7 Caudal de procesamiento (Throughput).

El caudal de procesamiento se calcula como rendimiento/velocidad de transmisión, mide el rendimiento de la red de área amplia en relación a los servicios acordados. El rendimiento es definido como la velocidad teórica de transmisión de los paquetes por la red.

1.4.1.8 Priorización.

La priorización consiste en la asignación de un determinado nivel de prioridad al tráfico que circula por una red, asegurando así que las aplicaciones de mayor importancia sean atendidas con anterioridad a las de menor importancia, estando o no ante una situación de congestión. Es necesaria únicamente cuando la red no proporciona la suficiente capacidad para atender todo el tráfico presente en la misma, en calidad de servicio para redes IP (sistemas administradores de ancho de banda) generalmente se tiene ocho prioridades, siendo la prioridad 0 la más baja y 7 la más alta, como se muestra en la Tabla 1.1.

1.4.1.9 Encolamiento (Queuing).

El encolamiento consiste en dividir y organizar el tráfico en un determinado elemento de red para su posterior retransmisión según un determinado algoritmo que define a la cola y que permite que determinados paquetes sean expedidos antes que otros por el elemento de red. Es una de las herramientas más utilizadas para implementar calidad de servicio, la

idea es ofrecer un mejor servicio al tráfico de alta prioridad al mismo tiempo que se asegura en diferentes grados el servicio para los paquetes de menor prioridad.

El encolamiento no garantiza que los datos importantes lleguen a su destino a tiempo (retardo) cuando se producen congestiones, lo único que aseguran es que los paquetes de alta prioridad llegarán antes que los de baja prioridad, existen varios tipos de encolamiento.

El encolamiento se suele situar en los ruteadores siendo áreas de memoria dentro del mismo, puede ser una solución costosa y complicada de gestionar, el encolamiento también es utilizado por la mayoría de los sistemas administradores de ancho de banda dedicados.

1.4.1.10 Planificación.

La planificación es un algoritmo de decisión implementado en diferentes métodos y sistemas, por ejemplo en encolamiento es el proceso de decidir que paquetes enviar primero en un sistema de múltiples colas. En sistemas administradores de ancho de banda la planificación es el algoritmo que especifica un límite estricto en la variación del retardo de paquetes en el, es decir cuanto tiempo puede sostener los paquetes desde que ingresan hasta que salen.

1.4.1.11 Flujo.

Un flujo es comparado con una vía, es el conjunto de datos pertenecientes a una misma secuencia, que han de ser enviados mediante distintos paquetes, es una combinación de direcciones IP origen/destino, puertos de origen/destino e identificador de sesión.

Recientemente aplicaciones más avanzadas han permitido una definición más avanzada de flujo, por instancia, por Localizador de Recurso Uniforme (URL), Extensiones de Correo de Internet Multipropósito (MIME) dentro de un paquete de Protocolo de Transferencia de HiperTexto (HTTP).

1.4.1.12 Clasificador.

Un clasificador es un elemento que selecciona paquetes y lo clasifica, en su forma más simple lo hace mediante el contenido de los encabezados de los paquetes, de acuerdo a reglas definidas.

Los sistemas administradores de ancho de banda pueden clasificar y controlar flujos de tráfico de aplicaciones y protocolos que atraviesen el enlace de Red de Area Amplia (WAN), pueden clasificar estos flujos a nivel de capa 4 (Transporte) y capa 7 (Aplicación) del modelo de Interconexión de Sistemas Abiertos (ISO/OSI) mencionado en el apartado 1.2., pueden clasificar por subredes, Conmutación de Etiquetas MultiProtocolo (MPLS), computadores, redes virtuales y encabezado de paquetes, la definición de encabezado de paquetes se menciona en la Tabla 1.1 y en los apartados 1.4.3. (CoS), 1.4.4 (ToS).

1.4.1.13 Marcador.

Un marcador es un elemento que realiza marcado del encabezado de paquetes, de acuerdo a reglas definidas.

Los sistemas administradores de ancho de banda pueden marcar los paquetes para Conmutación de Etiquetas MultiProtocolo (MPLS) y para las definiciones de encabezado de paquetes se menciona en la Tabla 1.1 y en los apartados 1.4.3. (CoS), 1.4.4 (ToS).

1.4.1.14 Medidor.

Realiza el proceso de medir las propiedades temporales como por ejemplo la tasa de bits de un flujo seleccionado por un clasificador. El proceso instantáneo de este proceso podría ser usado para afectar la operación de un marcador, modelador o descartador y/o podría ser usado para propósitos de cálculos o mediciones.

Los sistemas administradores de ancho de banda actúan como medidores del uso del ancho de banda del enlace de Red de Area Amplia (WAN) y de otros parámetros como por ejemplo retardos, estas mediciones se las puede observar gráficamente y estadísticamente.

1.4.1.15 Descartador.

Realiza el proceso de descarte, basado en reglas específicas o políticas. El proceso de descarte de paquetes se observa principalmente en elementos de red como ruteadores.

1.4.1.16 Política.

Es el proceso de descartar paquetes dentro de un flujo de acuerdo con el estado de un medidor correspondiente el cual refuerza un perfil de tráfico. Es decir se trata de mantener una tasa de datos configurada.

Para un administrador de ancho de banda son normas que se aplican a flujos, establecen un tipo de control de calidad de servicio, tasas garantizadas, tasas límite, control de admisión, prioridades, según el tipo de flujo y su importancia.

1.4.1.17 Modelador (Shaper).

Realiza el proceso de modelamiento de tráfico, usado para limitar el potencial del ancho de banda total de uno flujo o de varios flujos. Es usado para prevenir desbordamientos, manteniendo una tasa de transmisión configurada, el tráfico que sobrepasa la tasa configurada es guardada para su posterior transmisión. Retarda paquetes dentro de un flujo de acuerdo a algún perfil de tráfico definido.

Modeladores más avanzados como los sistemas administradores de ancho de banda permiten modelar a los flujos de tráfico valiéndose de tipo de control de calidad de servicio, tasas garantizadas, tasas límite, control de admisión y prioridades.

1.4.1.18 Acondicionamiento.

El acondicionamiento es el conjunto de funciones que son aplicadas a flujos de tráfico dependiendo del sistema, estas funciones son la clasificación, medición, políticas, priorización, descarte, modelamiento, planificación, encolamiento y marcado.

1.4.2 Requerimientos de calidad de servicio de las aplicaciones.

El incremento de la popularidad de IP ha hecho que se tenga un a gran cantidad de aplicaciones sobre IP, tales como video, voz sobre IP (VoIP), comercio en Internet, etc, muchas de las cuales necesitan variación de sus parámetros de calidad de servicio, es decir retardo, jitter, ancho de banda y pérdida de paquetes. En la Tabla 1.5. se observa los requerimientos de calidad de servicio de las diferentes aplicaciones.

Aplicación	Fiabilidad	Retardo	Jitter	Ancho de Banda
Correo electrónico	Alta	Alto	Alto	Bajo
Transferencia de ficheros	Alta	Alto	Alto	Medio
Acceso Web	Alta	Medio	Alto	Medio
Autenticación remota	Alta	Medio	Medio	Bajo
Multimedia	Media	Bajo	Bajo	Medio
Telefonía	Media	Bajo	Bajo	Medio
Videoconferencia	Media	Bajo	Bajo	Alto

Tabla. 1.5. Requerimientos de calidad de servicio de las aplicaciones.

Por ejemplo voz sobre IP requiere un jitter muy bajo, un retardo menor a 100 ms y un ancho de banda garantizado de 8 a 64 Kbps por canal de voz dependiendo del codificador utilizado.

1.4.3 Clase de Servicio (CoS).

La clase de servicio se define mediante la norma de prioridad IEEE 802.1p que forma parte de la norma IEEE 802.1q VLANs dictada por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), se logra mediante 3 bits que se ingresan en un campo adicional

denominada etiqueta (Tag) de 4 bytes del encabezado de capa 2 del modelo de Interconexión de Sistemas Abiertos (ISO/OSI). Una etiqueta es definida por la norma IEEE 802.1q para definir Redes de Área Local Virtual (VLAN) dentro de una Red de Área Local (LAN) extensa, específicamente en cada puerto de un switch o ruteador que cumpla con la norma, así se logra crear varios dominios de broadcast que pueden atravesar varios switches, incluso ruteadores ó enlaces de Red de Área Amplia (WAN), ver Anexo 1. Los 3 bits dentro de las etiquetas de VLANs permiten definir prioridades desde una mínima que es 0 hasta una máxima que es 7, para ajustar un umbral en el buffer de entrada y salida de un elemento de red para la descarga de paquetes.

Implica dos procedimientos, en primer lugar la priorización de los distintos tipos de tráfico claramente definidos a través de la red y en segundo lugar la definición de clases de servicio como se observa en la Tabla 1.6.

Combinación	**Clase de Servicio**	**Prioridad**
111	Red crítica	7
110	Voz Interactiva	6
101	Multimedia Interactiva	5
100	Flujo Multimedia (streaming media)	4
011	Negocios Críticos	3
010	Estándar	2
001	Segundo Plano	1
000	Mejor Esfuerzo	0

Tabla. 1.6. Clase de Servicio.

La priorización es importante en las puntos de congestión de la red donde las decisiones de priorización pueden ser realizadas por elementos de red como switches, sin embargo switches antiguos pueden no entender el estándar debido al cambio de la trama ethernet, la solución es reemplazar estos switches lo que puede resultar costoso. La clase de servicio en el encabezado de capa 2 puede ser leído directamente a nivel de switches que cumplan con la norma, en cambio, los ruteadores en donde se produce la conexión de Red de Área Local (LAN) con la Red de Área Amplia (WAN) no pueden manejar directamente esta priorización IEEE 802.1p, por esto la priorización en etiquetas es mapeada a un esquema de priorización en capa 3, conocido como Tipo de Servicio (ToS), mencionado en el punto 1.4.4 Tipo de Servicio (ToS).

No se debe confundir Clase de Servicio (CoS) con Calidad de Servicio (QoS) ya que a diferencia de calidad de servicio, clase de servicio no garantiza ancho de banda o latencia, independientemente de la diferenciación, tanto clase de servicio como calidad de servicio categorizan el tráfico para asegurar que el tráfico considerado crítico siempre fluya por la red, a pesar del ancho de banda demandado o de las aplicaciones de menor importancia.

Los sistemas administradores de ancho de banda se pueden trabajar en un ambiente de priorización IEEE 802.1p, identificando sus encabezados y marcándolos con una diferente prioridad si fuera necesario.

1.4.4 Tipo de Servicio (ToS).

Tipo de servicio es sinónimo de clase de servicio (capa 2) en capa 3, se especifica en el RFC 791, los diferentes tipos de servicio se definen como se observa en la Tabla 1.1. Sobre el protocolo IP se define el tipo de servicio con 3 bits del segundo byte del encabezado IP para asignar prioridades, se denomina señal de precedencia y se dice que es un tipo de señalización en banda.

1.4.5 Clasificación de la calidad de servicio.

La Fuerza de Tareas de Ingeniería de Internet (IETF) ha definido los siguientes modelos.

1.4.5.1 Mejor esfuerzo (Best effort)

Mejor esfuerzo es un servicio por defecto del protocolo IP que no tiene en cuenta las modificaciones de calidad de servicio, en este servicio una aplicación envía información cuando ella lo desea, en cualquier cantidad, sin ningún permiso requerido, sin informar previamente a la red y sin asegurar retardo, throughput o fiabilidad alguna. Se trata de una memoria interna del tipo Entra Primero – Sale Primero (FIFO).

1.4.5.2 Servicio Garantizado (Intserv).

El servicio garantizado es un modelo de calidad de servicio señalado, donde el elemento final señala su necesidad de calidad de servicio a la red. Aplica un concepto de reservación de recursos, es decir reservación de tasa de bit mediante el Protocolo de Reservación de Recursos (RSVP), al usuario se le reserva un ancho de banda dentro de la red para su uso exclusivo incluso en momentos de congestión.

Además la red debe mantener información del estado de sí misma por flujos, mirando la clasificación, normas, algoritmos de control y prevención de congestión, el problema principal del servicio garantizado es la escalabilidad debido a la necesidad de mantener información de estado en cada elemento de red y de cada flujo, esto hace inviable usar el protocolo de reservación de recursos en grandes redes, por ejemplo en la red de Internet.

1.4.5.3 Servicio Diferenciado (Diffserv).

El servicio diferenciado fue estudiado completamente en 1998 por la Fuerza de Tareas de Ingeniería de Internet (IETF) y define métodos simples para proveer calidad de servicio para tráfico de Internet y para soportar varios tipos de aplicaciones y requerimientos específicos de negocios.

1.4.5.3.1 Servicio diferenciado mediante elementos de red.

En este modelo los elementos de la red como ruteadores y switches capa 3 que implementen servicios diferenciados son configurados para servir a múltiples clases de tráfico con los requerimientos de calidad de servicio. Los elementos de red utilizan la capacidad de marcar el tráfico en la red con múltiples prioridades de tipo de servicio especificadas en cada paquete, se dispone de 7 bits en el encabezado del protocolo IP para diferenciar las aplicaciones sensibles a la congestión como se observa en la Figura 1.6. Al campo de precedencia de tres bits y al campo tipo de servicio excepto el cuarto bit juntos se los conoce como campo Servicio Diferenciado (DS) ó Punto de Código de Servicios

Diferenciados (DSCP) que es un campo de 6 bits según la RFC 2474 como se observa en la Figura 1.13.

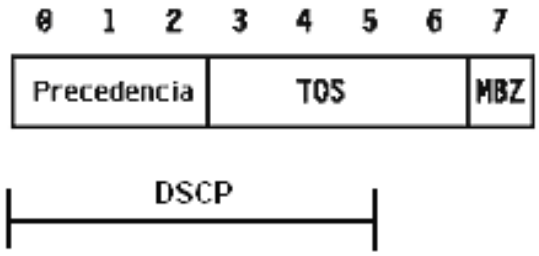


Figura. 1.13. Servicio diferenciado según la RFC 2474.

La RFC 2475 especifica la arquitectura de servicios diferenciados y define dos componentes mayores, el marcado de paquetes a través del campo de servicio diferenciado y el Comportamiento Por Salto (PHB). Los paquetes pueden ser marcados para lograr 64 clases de servicio, sin embargo la forma más usual de realizar la clasificación es desde valores como xxx000 donde x puede ser 0 ó 1, estos puntos de código son llamados puntos de código selectores de clase. Los puntos de código selectores de clase se reducen a los ocho clases de servicio definidas por el campo de precedencia IP como se observa en la Tabla 1.1.

Como en el servicio garantizado existe el protocolo de reservación, en el servicio diferenciado existe el Despachamiento hacia Adelante (EF), que es un tipo de comportamiento por salto que esencialmente se usa para aplicaciones como voz sobre IP que requiere pérdida baja de paquetes, ancho de banda garantizado, baja latencia, bajo retardo y bajo jitter, el valor del punto de código de servicios diferenciados recomendado para el despachamiento hacia adelante es 101110.

Después que los paquetes son marcados, se definen los comportamientos por salto que se refiere al planeamiento, encolamiento, políticas o modelamiento de un nodo en un paquete perteneciendo a un Agregado de Comportamiento (BA). El agregado de comportamiento se define como una colección de paquetes que atraviesan en una dirección

particular con un mismo punto de código de servicios diferenciados, cabe mencionar que el comportamiento por salto por defecto es el modelo mejor esfuerzo de IP.

Como se observa en la Figura 1.14. se define la región de servicios diferenciados que es compuesta por varios dominios de servicios diferenciados, cada dominio de servicios diferenciados está preparado para usar el punto de código de servicios diferenciados y los diferentes comportamientos por salto con un Acuerdo de Nivel de Servicio (SLA) ó política de usuario.

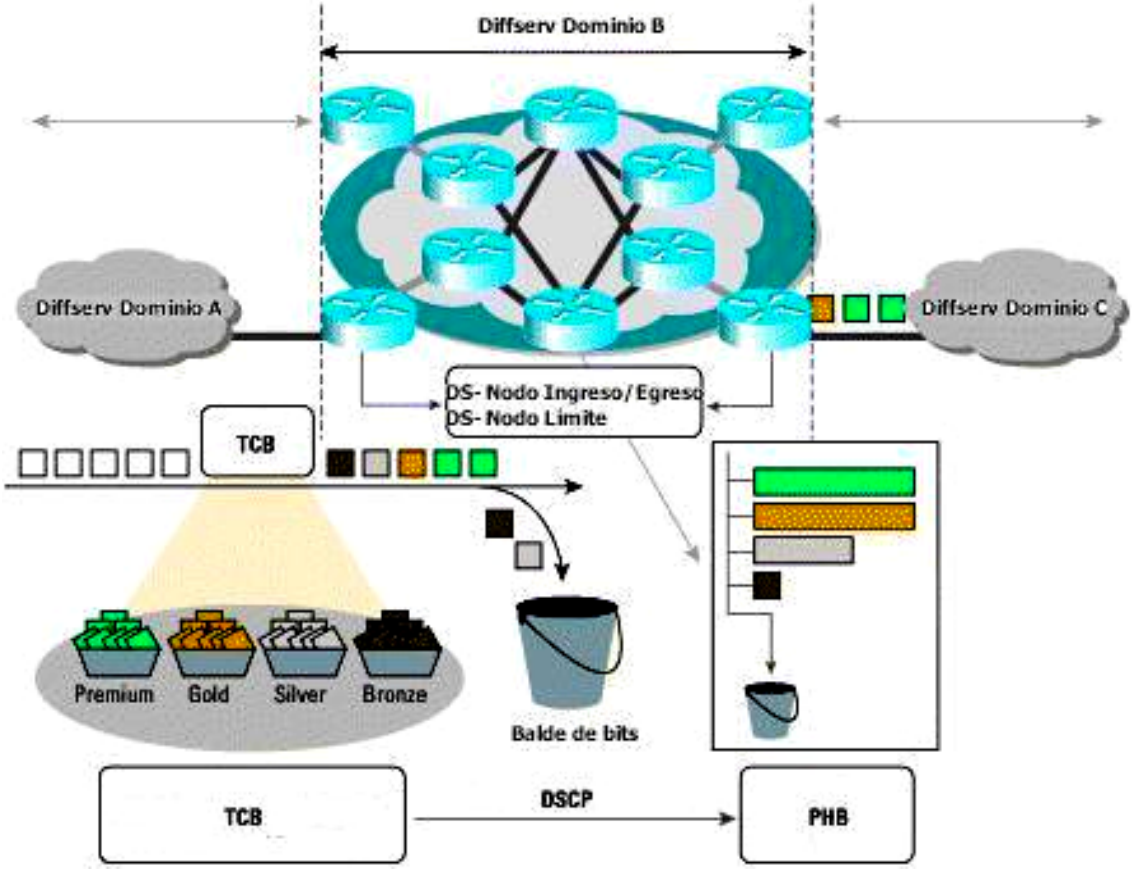


Figura. 1.14. Arquitectura de servicios diferenciados mediante elementos de red

Un dominio de servicios diferenciados posee nodos de ingreso, interiores y de egreso. Los nodos de ingreso y egreso se conocen también como nodos límite y ellos actúan generalmente como punto de demarcación del dominio de servicios diferenciados y la red de área local. Típicamente los nodos límite del dominio mediante ruteadores desarrollan

acondicionamiento de tráfico, es decir clasificación, medición, marcado/remarcado, y modelamiento. Un nodo de egreso tiene la obligación de quitar la información de servicios diferenciados de los paquetes si es que el dominio al que va a ir la información no es un dominio de servicios diferenciados.

Mediante switches capa 3 que implementen servicios diferenciados, un nodo interno del dominio refuerza los comportamientos por salto apropiados empleando técnicas de modelamiento o políticas de descarte, algunas veces remarcado de paquetes dependiendo del nivel de servicio.

Todos los elementos de red del dominio de servicios diferenciados pueden realizar las tareas de acondicionamiento, pero para proteger una capacidad escalable, la regla dice que los ruteadores más externos, es decir cerca o en el límite del dominio hagan el acondicionamiento, mientras que los switches internos refuercen los comportamientos por salto.

Como se observa en la Figura 1.15. el acondicionamiento de tráfico lo realiza el Bloque Condicionador de Tráfico (TCB), clasificando, midiendo, marcando, y modelando, para asegurar que el tráfico entrando en el dominio de servicios diferenciados está conforme a los niveles de servicio.

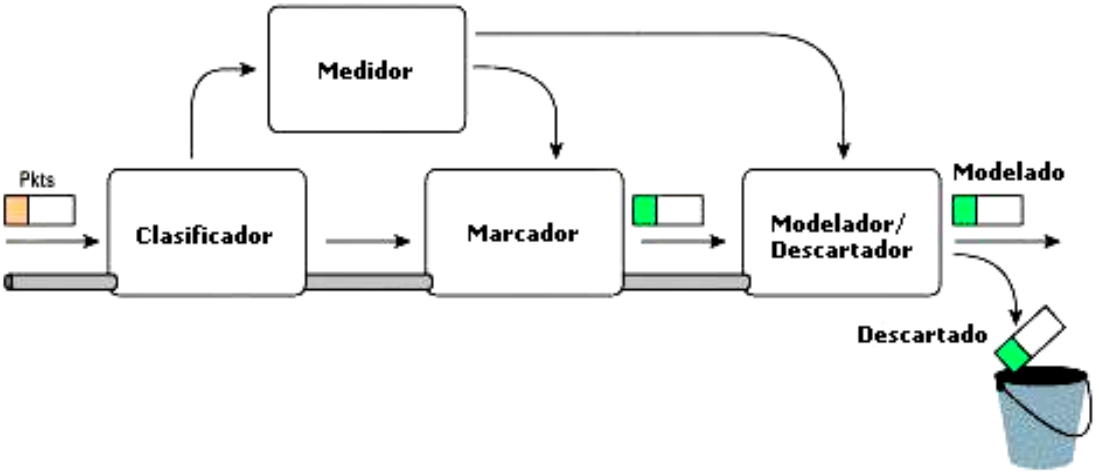


Figura. 1.15. Bloque Condicionador de Tráfico.

Este modelo ofrece soluciones empresariales completas extremo a extremo cuando se tiene varios dominios creando una región servicios diferenciados, ofrece soluciones para Proveedores de Servicio de Internet (ISP) que podrían transferir voz, datos, video y otras aplicaciones sensibles a retardos ofreciendo servicios diferenciados a sus consumidores, ofrece soluciones a organizaciones con negocios de tamaño medio y pequeño administrando su enlace red de área amplia en la mejor forma para sus aplicaciones de negocios, controlando el ancho de banda de las aplicaciones y priorizando aplicaciones.

Muchas veces resulta costosa la implementación debido a que los elementos existentes en una red no soportan servicios diferenciados ya sea por limitaciones de hardware o software, por lo que se hace necesario reemplazar dichos elementos de red. Los ruteadores podrían presentar problemas cuando el volumen de tráfico sea grande ya que su capacidad de procesamiento es principalmente utilizada para el ruteo del tráfico.

El estudio de los elementos de red que implementan este tipo de calidad de servicio se realizará haciendo referencia a la marca Cisco, que ha sido líder en el desarrollo de esta tecnología. Este estudio de Cisco permitirá al lector tener un conocimiento previo de algunos métodos que utilizan los administradores de ancho de banda de enlaces de Red de Area Amplia (WAN), así como una comparación para determinar la utilidad de los sistemas administradores respecto a los elementos de red.

1.4.5.3.2 Servicio diferenciado mediante sistemas administradores.

Los sistemas administradores de ancho de banda son elementos ó cajas dedicadas que se colocan generalmente entre el ruteador de la red de área amplia y el switch ó hub de la red de área local como se observa en la Figura 1.16., pueden implementar servicios diferenciados reforzando políticas de calidad de servicio, priorizan tráfico, pueden implementar servicio garantizado como por ejemplo ancho de banda mínimo a flujos, computadores o subredes. Brindan una gran alternativa costo-beneficio para una organización en lugar de aumentar el ancho de banda, cambiar o actualizar la mayoría de sus elementos de red.

Figura. 1.16. Servicios diferenciados y servicio garantizado mediante sistemas administradores

Los sistemas administradores de ancho de banda se instalan en la red para limitar el ancho de banda de aplicaciones no deseadas, garantiza mínimo throughput para usuario, grupos o protocolos y utiliza mejor los enlaces de área amplia ó Internet disminuyendo los incrementos explosivos de velocidad (bursty) de tráfico, por ejemplo se puede tener una plenitud de ancho de banda para tráfico tal como voz sobre IP, el cual es extremadamente sensitivo a la latencia y reducir el ancho de banda para tráfico menos sensitivo como descargas de archivos o respaldos remotos.

Existen varios fabricantes de estos sistemas administradores conocidos en el mercado como “traffic shapers”, se puede obtener múltiples modelos de un producto, los cuales usan el mismo mecanismo e interfaz pero difieren en las capacidades que pueden manejar, por ejemplo se puede adquirir un sistema que administre un enlace de 128 Kbps o un sistema más costoso que administre un enlace de 200 Mbps.

El servicio diferenciado mediante sistemas administradores de ancho de banda es recomendado en organizaciones que necesitan controlar los flujos de tráfico basados en consumidores que usan aplicaciones web, usuarios internos u oficinas remotas las cuales centralizan sus servicios en una oficina. Administran y refuerzan los niveles de servicio, proveen servicios diferenciados y otros servicios como ancho de banda particionado con acceso justo y equitativo, contención de ataques de Rechazo de Servicio (DoS) y soporte de web hosting a los consumidores. En redes educacionales pueden ser usados para bajar la prioridad de tráfico de aplicaciones que comparten archivos y música, pueden limitar el acceso a sitios particulares y aplicaciones durante horas importantes. También permiten

priorizar aplicaciones tales como voz y video sobre IP o reservar ancho de banda garantizado para este tipo de aplicaciones, en redes satelitales reducen las retransmisiones y retardos de datos gracias a una mejor distribución del tráfico del enlace satelital.

Para los sistemas administradores es indispensable identificar el tráfico que está ocasionando problemas al tráfico que es más sensitivo o más necesario, es así que se pueden ver los protocolos, servidores y clientes más activos, esto es importante ya que se tiene granularidad y se puede realizar un modelamiento de tráfico efectivo al identificar la fuente de los problemas. Por otro lado la identificación de tráfico solamente por puertos y protocolos no es muy precisa ya que hoy en día existe tráfico que utiliza el mismo puerto 80 de navegación web para otras aplicaciones, podría suceder que este tráfico atraviese un elemento de seguridad (firewall), un típico caso es el software KaZaA para compartir archivos conocidos como aplicaciones par a par (P2P) que conectan a varios usuarios en pares para compartir archivos, este software genera una gran cantidad de tráfico. Los enlaces de área amplia son generalmente saturados por este tipo de tráfico par a par, si el cliente se conecta por defecto con el puerto 80 y se hace una identificación en capa 4, es decir por puertos, se tiene un gran problema, ya que el tráfico par a par tendrá la misma política que el tráfico de navegación web. Es por esto que una gran ventaja de estos sistemas es su capacidad de realizar identificación de tráfico en capa 4 y capa 7 que es la capa de aplicación, lo que le permite identificar aplicaciones par a par y otras.

Los sistemas administradores utilizan varios métodos para implementar calidad de servicio, hay varios métodos para controlar el ancho de banda, sin embargo estos sistemas utilizan básicamente los métodos de priorización, encolamiento por flujo, reserva de ancho de banda y TCP rate control. Tienen un alto límite de políticas que permiten dar una mayor prioridad ó acceso al ancho de banda a cierto tipo de tráfico que es más necesario que otro, las políticas permiten también garantizar una cantidad específica de ancho de banda a cierto tráfico, usuario o grupos de usuarios; consecuentemente al crear políticas que prioricen el tráfico, garanticen el ancho de banda y controlen a las aplicaciones menos importantes, el rendimiento de la red se incrementará.

Los sistemas administradores son una solución de calidad de servicio integrada esto quiere decir que usa una sola interfaz de administración, además de que poseen

capacidades de reporte de actividades de control de ancho de banda y manejo de la interfaz, los cuales pueden ser gráficos o datos estadísticos, también reportes vía e-mail a alguna persona que puede ser el administrador de la red.

El objetivo de estos sistemas es eliminar la necesidad de realizar calidad de servicio en el ruteador, es decir encolar los paquetes y reducir la congestión en el ruteador. El estudio de estos sistemas se centrará en los dos más conocidos y que se encuentran disponibles en nuestro mercado, estos son PacketShaper de Packeteer y NetEnforcer de Allot, también se mencionará brevemente un tercer administrador de ancho de banda que es Accelerator de Expand.

CAPITULO II

SISTEMAS ADMINISTRADORES DE ANCHO DE BANDA

2.1 GENERALIDADES

En el capítulo anterior se estudió los tipos de calidad de servicio (QoS) en redes, no se puede estudiar las características de los sistemas administradores de ancho de banda dedicados sin antes conocer los tipos de tecnología y sistemas más utilizados para calidad de servicio.

En este capítulo se estudia tecnologías que implementan calidad de servicio para redes, entre las principales se encuentran los ruteadores, switches y los sistemas administradores de ancho de banda.

Es importante un estudio previo de ruteadores y switches por dos motivos: los sistemas administradores de ancho de banda pueden instalarse en redes que contengan este tipo de elementos que puedan implementar calidad de servicio o implementen otros tipos de protocolos en la red, y los sistemas administradores de ancho de banda en determinado momento pueden utilizar algún procedimiento, técnica o mecanismo de otra tecnología que implemente calidad de servicio.

Al final de este capítulo se compara todas las tecnologías, con el fin de mostrar las fortalezas y debilidades de los sistemas administradores de ancho de banda dedicados, el objetivo principal de este capítulo es mostrar la capacidad del administrador de ancho de banda, el cual se dispone físicamente para probarlo posteriormente.

2.2 ELEMENTOS DE RED

Existen distintas clases y marcas tanto de ruteadores como de switches, entre las principales marcas y fabricantes se puede mencionar a Cisco, MRV, 3Com, D-Link, Linksys, NetGear, Trendnet, Avaya, todos ellos implementan en sus elementos de red, principalmente la norma de Clase de Servicio (CoS) que se define mediante la norma IEEE 802.1p que se menciona en el apartado 1.4.3. y el Encolamiento de Prioridad (PQ) mencionado en el apartado 2.2.2.2.

MRV posee switches que se colocan en la Red de Area Local (LAN) y poseen características de calidad de servicio como clasificación de tráfico por: puerto/dirección de Control de Acceso al Medio (MAC), Red de Area Local Virtual (VLAN), protocolo, fuente o destino de IP, puerto del protocolo de Control de Transmisión (TCP) o del Protocolo de Datagrama de Usuario (UDP). Maneja: Encolamiento de Prioridad (PQ) con 4 colas de prioridad por puerto, maneja prioridad a través de la norma IEEE 802.1p, RFC 791 Tipo de Servicio (ToS). Permite Comportamientos por Salto (PHB) basado en el Punto de Código de Servicios Diferenciados (DSCP), acepta tráfico, redirecciona tráfico, deniega tráfico, implementa además limitación de tasa de bits.

Además MRV posee switches con capacidad de ruteo a los que se les puede colocar módulos de fibra óptica para Fast y Gigabit Ethernet, poseen características de calidad de servicio como clasificación de tráfico por: puerto/dirección de Control de Acceso al Medio (MAC), Red de Area Local Virtual (VLAN), protocolo, fuente o destino de IP, puerto del protocolo de Control de Transmisión (TCP) o del Protocolo de Datagrama de Usuario (UDP) y tráfico de Conmutación de Etiquetas MultiProtocolo (MPLS). Maneja Encolamiento de Prioridad (PQ) con 4 colas de prioridad por puerto, maneja prioridad a través de la norma IEEE 802.1p, RFC 791 Tipo de Servicio (ToS), listas de control de acceso (ACL). Permite Comportamientos por Salto (PHB) basado en el Punto de Código de Servicios Diferenciados (DSCP), acepta tráfico, redirecciona tráfico, deniega tráfico, implementa además limitación de tasa de bits, además permite realizar Detección Temprana Aleatoria (RED) nombrada en el punto 2.2.3.1.

3Com posee ruteadores que implementan: limitación de tasa de bits, encolamiento de prioridad, Tasa de Acceso Comprometida (CAR), Encolamiento Justo Pesado (WFQ), Entra Primero – Sale Primero (FIFO), Detección Temprana Aleatoria Pesada (WRED).

D-Link posee switches con capacidad de ruteo y que implementan: clasificación y priorización basado en Clase de Servicio (CoS), Tipo de Servicio (ToS) y números de puertos y zócalos TCP/UDP, limitación de tasa por puerto.

Avaya posee switches con capacidad de ruteo que implementan: clasificación y marcado basado en Clase de Servicio (CoS), Tipo de Servicio (ToS), Punto de Código de Servicios Diferenciados (DSCP), además implementa políticas basado en la clasificación anteriormente mencionada.

El estudio previo de los procedimientos de calidad de servicio se hará en base a la marca Cisco, debido a que esta marca ha investigado e implementado en sus elementos de red varios procedimientos, estos procedimientos han sido adoptados por los fabricantes más reconocidos en el medio, incluyendo a los mencionados anteriormente. Los elementos Cisco son los más reconocidos - utilizados en el mercado mundial y de nuestro país, estos elementos de red utilizan un software guardado en sus memorias llamado Cisco IOS que provee de inteligencia artificial a los elementos de red, una parte de este software llamada Cisco IOS QoS trata de predecir - controlar los tipos de tráfico y aplicaciones sobre un red, con el fin de mejorar la eficiencia de la misma.

Los elementos Cisco utilizan el esquema de servicios diferenciados para calidad de servicio, el software IOS QoS Servicios diferenciados provee al ruteador: métodos de identificación y marcado, manejo de congestión, encolamiento, es decir provee mecanismos para servicio diferenciado, el software IOS QoS Servicios Integrados provee servicio garantizado mediante protocolos de reservación.

Los modelos de ruteadores que soportan el software IOS QoS son Cisco 8xx, 16xx, 17xx, 25xx, 36xx, 4xxx, 72xx, 75xx, 85xx, 12xxx y switches que soportan el software IOS QoS son Catalyst 4xxx, 5xxx, 6xxx

La configuración de la calidad de servicio en los elementos de red Cisco es en base a comandos de línea, esto hace que el procedimiento de calidad de servicio se vuelva complicado y sea hecho por personas con un amplio conocimiento en configuración de estos elementos de red.

La última innovación del software Cisco IOS es Cisco AutoQoS que simplifica los trabajos de administración de la red, reduciendo la complejidad de la configuración de calidad de servicio para ruteadores y switches individualmente, Cisco AutoQoS se basa en cinco aspectos: clasificación de la aplicación, generación de la política, configuración o reforzamiento de calidad de servicio, monitoreo y reporte.

Otra innovación es el Administrador de Políticas de Calidad de Servicio (Cisco QPM) que complementa a Cisco AutoQoS brindando diseño de calidad de servicio, administración y monitoreo de tráfico a redes de gran escala vía Protocolo de Administración de Red Simple (SNMP). Los usuarios pueden medir caudal de procesamiento para las aplicaciones y pueden medir clases de servicio, así pueden localizar problemas en tiempo real e histórico. Las estadísticas de tráfico y calidad de servicio pueden ser vistas como gráficos de línea y barras en bits, paquetes por segundo, interfaz o política. También permite ver estadísticas de filtros específicos, incluyendo el filtro de Reconocimiento de Aplicación Basado en la Red (NBAR), tasa de tráfico antes de la calidad de servicio, tráfico transmitido después de la calidad de servicio y tráfico descartado, también las estadísticas de acción de calidad de servicio.

Otra innovación es el Administrador de Dispositivos de Calidad de Servicio (Cisco QDM) que provee una aplicación fácil de usar para configurar y monitorear calidad de servicio basada en IP en elementos de red Cisco. La aplicación es guardada en la memoria borrable (flash) del elemento de red y se ejecuta desde una estación de red que cumpla con los requerimientos mínimos como un navegador web, una vez que la aplicación se ha cargado en la memoria del elemento de red, en la estación de red se hace una conexión a la dirección IP del ruteador ó switch y se cargará la aplicación Cisco QDM, como se observa en la Figura 2.1.

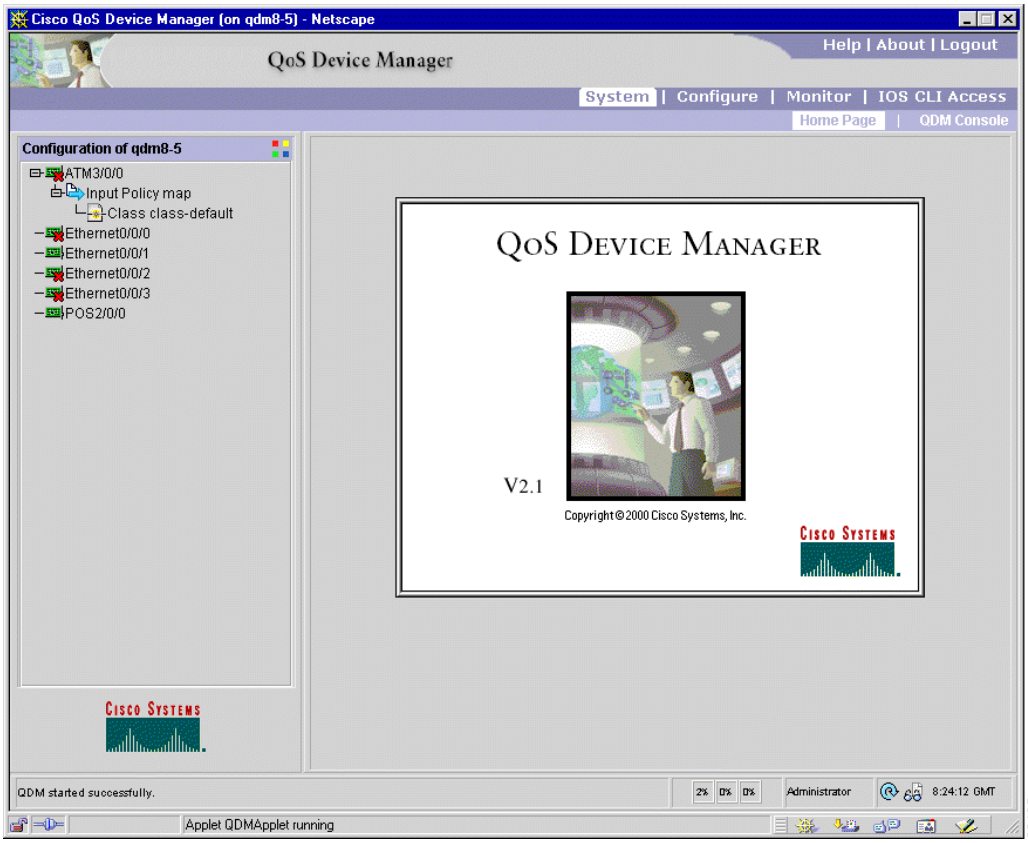


Figura. 2.1. Cisco Administrador de Dispositivos de Calidad de Servicio.

Es necesario desglosar los aspectos que toma en cuenta Cisco AutoQoS, mediante los cuales los elementos de red Cisco realizan calidad de servicio, especialmente el monitoreo a través de reconocimiento de aplicación basado en la red; la configuración que tiene que ver con mecanismos que refuerzan la calidad de servicio, entre los cuales se encuentran mecanismos de control y prevención de congestión de tráfico para realizar servicio diferenciado. Para servicio garantizado son necesarios mecanismos de reservación y señalización.

2.2.1 Técnicas de clasificación de tráfico.

Los paquetes primero deben ser identificados y luego marcados, estas dos tareas se denominan clasificación, se puede realizar por Lista de Control de Acceso (ACL) y luego

utilizar herramientas de manejo de congestión como mecanismos de encolamiento, pero esta técnica es para un solo ruteador, lo que contrasta con los bits de precedencia de IP.

Existen otros métodos, los cuales pueden asignar la precedencia (como se observa en la Tabla 1.1.) de los paquetes basándose en clasificación de listas de acceso extendidas, permitiendo una flexibilidad considerable, ya que incluye el asignamiento por aplicación o usuario, por destino o subred y otras más. Típicamente esta funcionalidad es desplegada tan cerca como sea posible del extremo de la red, tal que cada elemento de red subsiguiente puede proveer servicio basado en determinada política.

2.2.1.1 Ruteo basado en políticas.

Clasifica el tráfico basado en criterios de listas de acceso extendidas, asigna los bits de precedencia IP e incluso rutea a tráfico específico que requiera cierto tipo de calidad de servicio en la red. Asignando niveles de precedencia al tráfico entrante y usándolo en combinación con herramientas de encolamiento se puede crear un servicio diferenciado, estas herramientas permiten implementar políticas de calidad de servicio en la red.

2.2.1.2 Tasa de Acceso Comprometida (CAR).

Permite clasificar el tráfico en una interfaz entrante, también permite especificación de políticas para manejar tráfico que excede una cierta asignación de ancho de banda, trabaja con el método de Flujo Balde-Ficha (TBF) que trata de controlar la máxima tasa de paquetes desde una cola, entonces se puede crear una memoria intermedia conocida como balde (bucket) el cual es llenado constantemente por algunas piezas virtuales de información llamadas fichas (tokens), a una tasa específica administrativa (token bucket), por ejemplo se quiere tener una tasa máxima de 500 kbps, esto significa transmitir 62.5 Kbytes/seg, entonces se llenará un balde a una tasa de 64000 fichas por segundo.

El método CAR se estudia en tres escenarios, el primero es que los datos lleguen a una tasa igual que la tasa de fichas en este caso a cada paquete entrante le corresponde una ficha y pasa sin ningún problema, el segundo es que los datos lleguen a una tasa menor que la tasa de fichas en este caso las fichas sobrantes pueden ser utilizadas para enviar datos a

una velocidad mayor que la tasa administrativa y el tercer caso cuando los paquetes llegan a una tasa mayor que la tasa de fichas en este caso se produce una situación de desborde y los paquetes entrantes serán descartados lo cual permite modelar la tasa administrativa. El control lo hace marcando el campo de precedencia de IP (como se observa en la Tabla 1.1.) y la identificación de paquetes lo hace basado en puerto físico, dirección fuente o destino, dirección de Control de Acceso el Medio (MAC), tipo de protocolo.

2.2.1.3 Reconocimiento de Aplicación Basado en al Red (NBAR).

Es otra herramienta de clasificación, realiza clasificación a otro nivel, puede hacerlo mirando profundamente dentro de los paquetes, así esta herramienta puede identificar paquetes que utilizan el Protocolo de Transferencia de HiperTexto (HTTP) por Localizador de Recurso Uniforme (URL), computador ó tipo de Extensiones de Correo de Internet Multipropósito (MIME), además puede identificar varias aplicaciones que usan puertos que cambian constantemente; esto lo hace mirando los paquetes de control para determinar en que puertos la aplicación pasa los datos. Clasifica también otros tipos de tráfico como aplicaciones de bases de datos y protocolos utilizados en voz sobre IP. NBAR introduce otras características de clasificación nuevas que identifican los protocolos desde la capa 4 a capa 7 del modelo de Interconexión de Sistemas Abiertos (OSI), estas características son: números de puerto TCP y UDP asignados estáticamente, protocolos no TCP/IP y no UDP, números de puerto TCP y UDP asignados dinámicamente.

NBAR posee una lista de protocolos que puede identificar y provee estadísticas de cada uno de ellos. Existe la opción de cargar al ruteador, Módulos de Lenguaje de Descripción de Paquetes (PDLM) a su memoria borrable, esto permite añadir protocolos o clasificaciones personalizadas a la lista de NBAR.

NBAR puede clasificar tráfico de aplicaciones par a par (P2P), para esto se basa en protocolos para compartir archivos como Gnutella y FastTrack. El protocolo Gnutella es usado por aplicaciones como Gnutella, Morpheus, Mutella entre los más importantes. El protocolo FastTrack es usado por aplicaciones como KaZaA y Grokster.

NBAR no soporta más de 24: localizadores de recurso uniforme concurrentes, computadores o tipo de extensiones de correo de Internet multipropósito, además no soporta tráfico multicast, paquetes fragmentados, peticiones constantes que utilicen el protocolo de transferencia de hipertexto, paquetes originados o con destino final al ruteador ejecutando este reconocimiento, además no soporta interfaces con túneles virtuales y el uso de encriptación e interfaces telefónicas. Para tratar de evitar los problemas de túneles o encriptación, se debe utilizar NBAR en la interfaz del enlace de Red de Area Local (LAN) del ruteador antes de que el tráfico pase al enlace de Red de Area Amplia (WAN).

En la Figura 2.2. se observa un ejemplo de utilización del reconocimiento de aplicación basado en la red, se observa una red compuesta por dos oficinas que se conectan por un enlace de área amplia en donde, este reconocimiento se aplica en los puntos A y D, mientras que en los puntos B y C se aplican mecanismos que refuerzan la calidad de servicio donde se combinan el tráfico con incrementos explosivos de velocidad y enlaces de capacidad reducida (cuellos de botella).

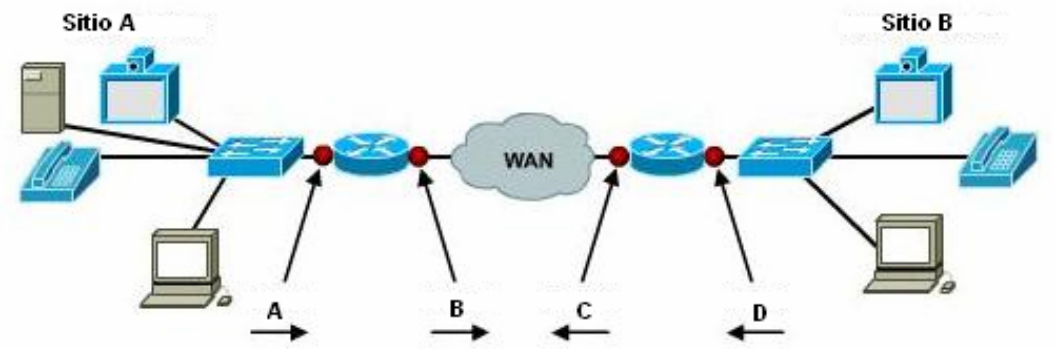


Figura. 2.2. Ejemplo del reconocimiento de aplicación basado en al red.

Los mecanismos aplicados en los puntos B y C son esencialmente 2.2.2.5 Encolamiento Justo Pesado Basado en Clases (CBWFQ) y modelamiento de tráfico, el cual es usado para limitar el potencial del ancho de banda total de uno flujo o de varios flujos.

2.2.2 Técnicas de control de congestión tráfico.

Una vez que el tráfico ha sido clasificado, el ruteador aplicará el control de congestión, usando mecanismos de encolamiento de paquetes, los cuales almacenan los paquetes en una memoria intermedia y le dan una prioridad especial dependiendo del tipo de mecanismo, cabe señalar que pueden ser los causantes de la pérdida de paquetes, latencia y jitter que experimenta el tráfico de una red.

El proceso general que siguen los mecanismos de encolamiento en un ruteador, son clasificar los paquetes que entran por la interfaz, dependiendo del mecanismo de encolamiento se tiene un número de colas en donde se van colocando los paquetes según una prioridad que le da el clasificador y finalmente se asigna un proporción del ancho de banda a las colas, la proporción y prioridad asignada varía según el mecanismo o algoritmo.

2.2.2.1 Entra Primero – Sale Primero (FIFO).

Este mecanismo de encolamiento se encarga de almacenar paquetes cuando hay congestión en la red y enviarlos cuando tiene la posibilidad, manteniendo el orden de llegada, es decir no ofrece ninguna prioridad de unos paquetes sobre otros, utiliza todo el ancho de banda disponible, generando de esta forma tiempos de respuesta pobres a ciertas aplicaciones cuando hay congestión. Este es el mecanismo que suele utilizar por defecto el Protocolo de Internet (IP), este mecanismo es utilizado por el tipo de clase de servicio de mejor esfuerzo. Al igual que ocurre con el resto de mecanismos de encolamiento, este mecanismo tiene como limitación la capacidad de su memoria intermedia en momentos de congestión.

2.2.2.2 Encolamiento de Prioridad (PQ).

Este mecanismo de encolamiento asegura que el tráfico importante (misión crítica) reciba un servicio rápido en cada punto de la Red de Area Amplia (WAN) donde este mecanismo esté presente, cada uno de los paquetes debe de ser colocado en una de las

cuatro posibles colas alta, media, normal y baja prioridad. Este mecanismo crea una lista de prioridad de los paquetes, esta lista indica al elemento de red como distribuir los paquetes a las colas, así los paquetes son clasificados por: protocolo o sub-protocolo de red, interfaz del ruteador por la que llegue el paquete, tamaño del paquete, Listas de Control de Acceso (ACL) y dirección de origen o destino, además los paquetes que no se puedan clasificar serán asignados a la cola de prioridad normal.

Los inconvenientes de este método son: es estático, no se adapta a los requerimientos de la red, y puede dejar fuera de servicio a tráfico menos prioritario, debido a que la cola con mas alta prioridad es atendida primero hasta que esté vacía, en la Figura 2.3. se observa el funcionamiento de este mecanismo.

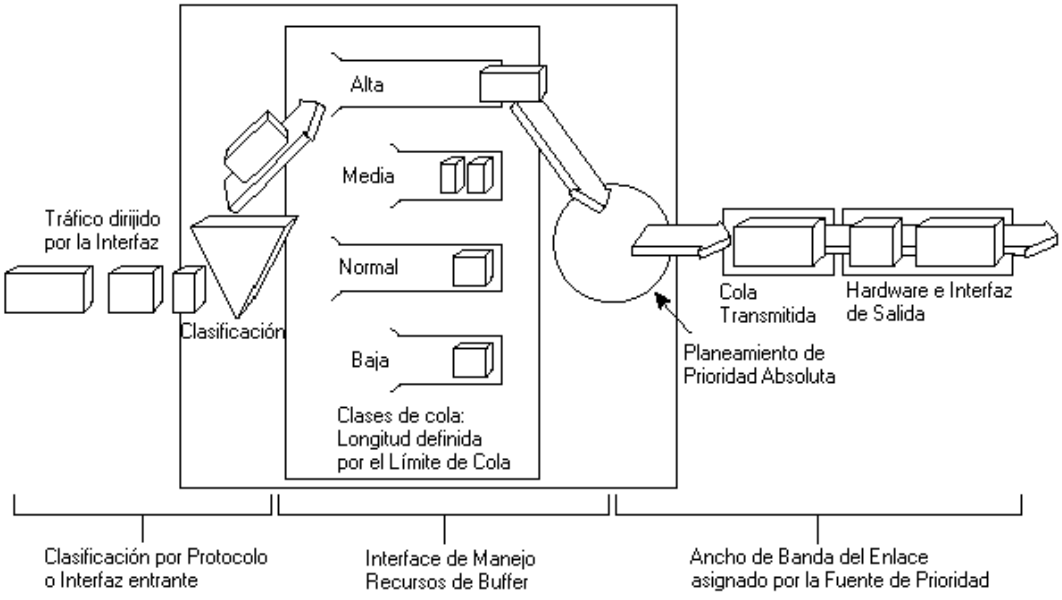


Figura. 2.3. Encolamiento de prioridad.

2.2.2.3 Encolamiento Personalizado (CQ).

Este mecanismo fue diseñado para permitir que cada una de varias aplicaciones compartieran la red con un ancho de banda mínimo garantizado y garantías aceptables en cuanto a los retardos, en este método el ancho de banda debe de ser compartido proporcionalmente entre las aplicaciones o usuarios en unidades de tiempo, sin dejar

tráfico fuera de servicio, además permite que el administrador especifique un porcentaje de ancho de banda para un protocolo determinado.

Este mecanismo permite configurar 16 colas de salida y una especial para mensajes del sistema para cada interfaz, esta es la cola con número 0 y es utilizada para paquetes de alta prioridad como paquetes de señalización. Cada cola es atendida secuencialmente de forma cíclica, transmitiendo un porcentaje de tráfico antes de pasar a la siguiente, requiere mucha más administración pero da una mayor flexibilidad, en la Figura 2.4. se observa el funcionamiento de este mecanismo.

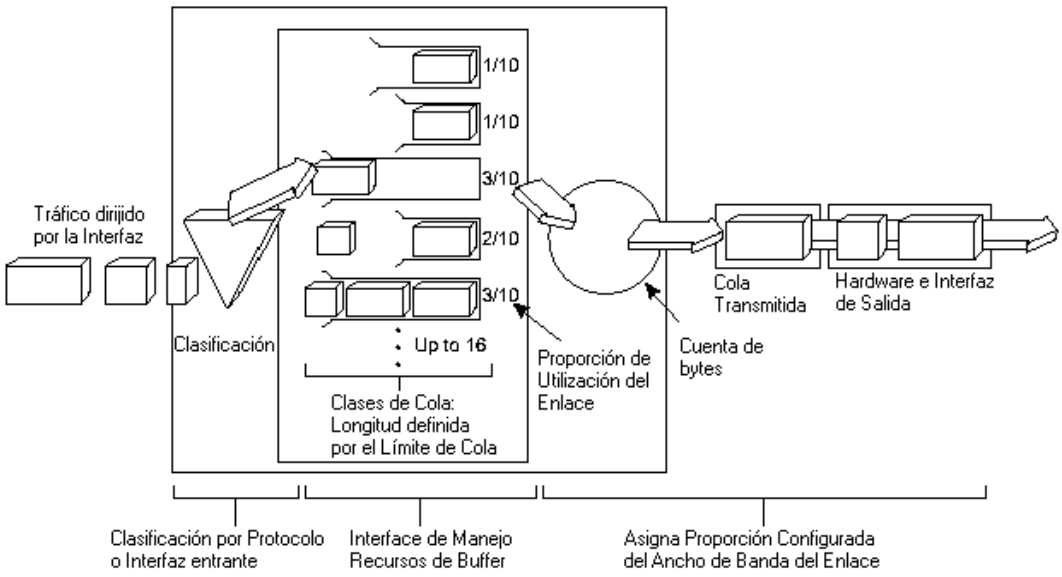


Figura. 2.4. Encolamiento personalizado.

2.2.2.4 Encolamiento Justo Pesado (WFQ).

Los mecanismos vistos anteriormente son estáticos, y por lo tanto no se adaptan a los cambios producidos en la red, por ello se creo un mecanismo como el encolamiento justo pesado, que es adaptativo y no requiere de Listas de Control de Acceso (ACL) para determinar el tráfico preferido en una interfaz serial. Es un método de planeamiento dinámico de pesos o prioridades que se aplica al tráfico, el cual es clasificado en dos clases de flujos: flujos de ancho de banda alto y flujos de ancho de banda bajo. Este método es un

algoritmo que simultáneamente distribuye interactivamente el tráfico a el frente de una cola para reducir los tiempos de respuesta y con justeza compartir la cantidad de ancho de banda sobrante a los flujos de ancho de banda alto.

Este método es adecuado para situaciones donde se necesite un buen tiempo de respuesta, tanto para usuarios que hagan tanto un uso elevado de la red como por ejemplo transferencia de archivos, como para los que hagan un uso más leve como por ejemplo una sesión de Protocolo de Emulación de Terminal (TELNET); sin añadir ancho de banda adicional.

Este mecanismo asegura que las diferentes colas no se queden privadas de un mínimo de ancho de banda, de modo que el servicio proporcionado al tráfico es más predecible, el ruteador clasifica el tráfico en diferentes flujos a partir de las siguientes características direcciones IP, direcciones de Control de Acceso el Medio (MAC), puertos, protocolo TCP, UDP, calidad de servicio ó tipo de servicio.

Este mecanismo detecta la precedencia del datagrama IP (como se observa en la Tabla 1.1.) y los distribuye a diferentes colas, además el Protocolo de Reservación de Recursos (RSVP) utiliza este método de encolamiento para obtener asignación de espacio de memoria intermedia, planeamiento de paquetes y así garantizar ancho de banda para los flujos reservados. Opera de forma similar a la Multiplexación por División de Tiempo (TDM), en donde cada cola tiene una porción de tiempo para enviar datos, pero si una cola esta vacía asigna su porción de tiempo a las otras, en la Figura 2.5. se observa el funcionamiento de este mecanismo.

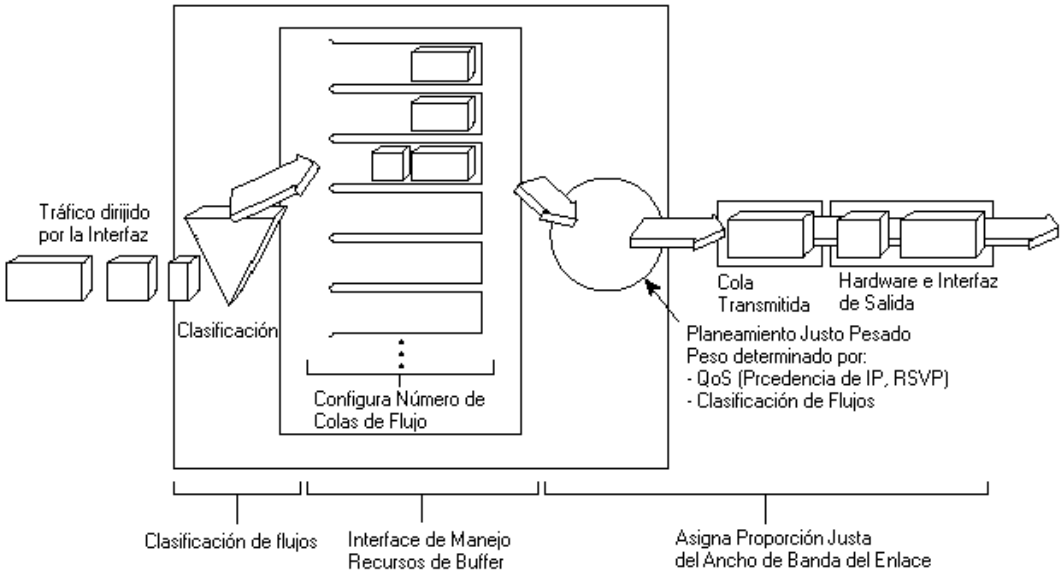


Figura. 2.5. Encolamiento justo pesado.

Generalmente este método no requiere configuración, es usado por defecto en interfaces seriales de velocidades E1 (2.048Mbps) o inferiores, el número de colas es configurable aunque por defecto usa 256 colas, no puede ser utilizado en conjunto con túneles virtuales o encriptación debido a que los encabezados de los paquetes son modificados. Esté método es adaptativo sin embargo no ofrece un control preciso sobre la asignación de ancho de banda tal como el Encolamiento Personalizado (CQ) o el encolamiento que se menciona continuación Encolamiento Justo Pesado Basado en Clases (CBWFQ).

2.2.2.5 Encolamiento Justo Pesado Basado en Clases (CBWFQ).

Este método extiende la funcionalidad del encolamiento justo pesado, proveyendo soporte para clases de tráfico definidas por el usuario. El usuario define las clases de tráfico basándose en criterios de clasificación mencionados en el encolamiento justo pesado e incluso basándose en Listas de Control de Acceso (ACL) e interfaces de entrada.

En este mecanismo una cola Entra Primero – Sale Primero (FIFO) es asignada a cada una de las 64 clases posibles, los paquetes que cumplen con los requisitos de clasificación de una clase son dirigidos a la cola asignada a esa clase. Una vez que se ha definido los criterios de clasificación para una clase, se puede asignarle características, como

asignación de ancho de banda, peso y límite máximo de paquetes. El ancho de banda asignado a una clase es el ancho de banda garantizado a una clase cuando hay congestión. Los paquetes llegando a una cola que excedan los límites configurados en esa cola, son descartados de la cola, la forma de descarte depende de la configuración de cada cola. Puede usarse el descarte de paquetes o Detección Temprana Aleatoria Pesada (WRED) el cual se menciona en 2.2.3.1 Detección Temprana Aleatoria (RED).

En este mecanismo la suma de toda la asignación de ancho de banda en una interfaz no puede exceder el 75% del ancho de banda total disponible de la interfaz, debido a que el 25% sobrante es utilizado por el encabezamiento de paquetes.

2.2.3 Mecanismos de prevención de congestión.

Los mecanismos de encolamiento distribuyen los paquetes en una interfaz en varias colas dependiendo del mecanismo, tratando de esta manera de liberar el tráfico de la mejor manera posible, sin embargo cuando existe congestión los paquetes llegando en exceso a las colas no pueden seguir siendo retenidos por el elemento de red, por esto es necesario la administración de los paquetes en exceso mediante la implementación de mecanismos de prevención de congestión.

2.2.3.1 Detección Temprana Aleatoria (RED).

Una posible solución al problema de congestión es descartar paquetes sólo de una conexión, la cual viole los caudales preestablecidos y dejar intacta las demás. Existen mecanismos como la Detección Temprana Aleatoria (RED) y su variación Detección Temprana Aleatoria Pesada (WRED) que son beneficiosos, evitan la congestión de la red y la probabilidad de pérdida de paquetes.

En caso de producirse una fuerte congestión estos mecanismos pueden ser capaces de realizar descartes de paquetes oportunos ó inteligentes, es decir no realizando un descarte de paquetes al azar, lo cual podría producir por ejemplo, la eliminación de un paquete clave que produjera la reacción negativa de alguna aplicación TCP.

La Detección Temprana Aleatoria (RED) provee a los operadores de la red, la posibilidad de aplicar normas para el manejo del tráfico y maximizar el caudal de procesamiento bajo condiciones de congestión. Trabaja junto al Protocolo de Control de Transmisión (TCP) debido a la posibilidad de retransmisión, evita la congestión aplicando una serie de tareas:

- Distingue entre ráfagas de tráfico temporal que pueden ser absorbidas por la red y cargas excesivas de tráfico que pueden saturar la red.

- Trabaja en cooperación con el extremo generador de tráfico, para evitar la oscilación producida por el protocolo TCP que puede causar ondas de congestión en la red.

- Trabaja con TCP para anticiparse y manejar la congestión en momentos de tráfico excesivo, para maximizar el caudal de procesamiento mediante el descarte de paquetes.

La Detección Temprana Aleatoria Pesada (WRED) combina las capacidades de la detección temprana aleatoria y del campo de precedencia del datagrama IP para proveer diferentes clases de servicio en función de las características de la información. También proporciona manejadores para tráfico prioritario en momentos de congestión, también puede colaborar con Protocolo de Reservación de Recursos (RSVP) proporcionando un controlador de carga o indicando si es factible una reserva de espacio en alguna cola, es un mecanismo utilizado para calidad de servicio, no es muy aconsejable usarlo para voz sobre IP, en la Figura 2.6. se observa el funcionamiento de este mecanismo.

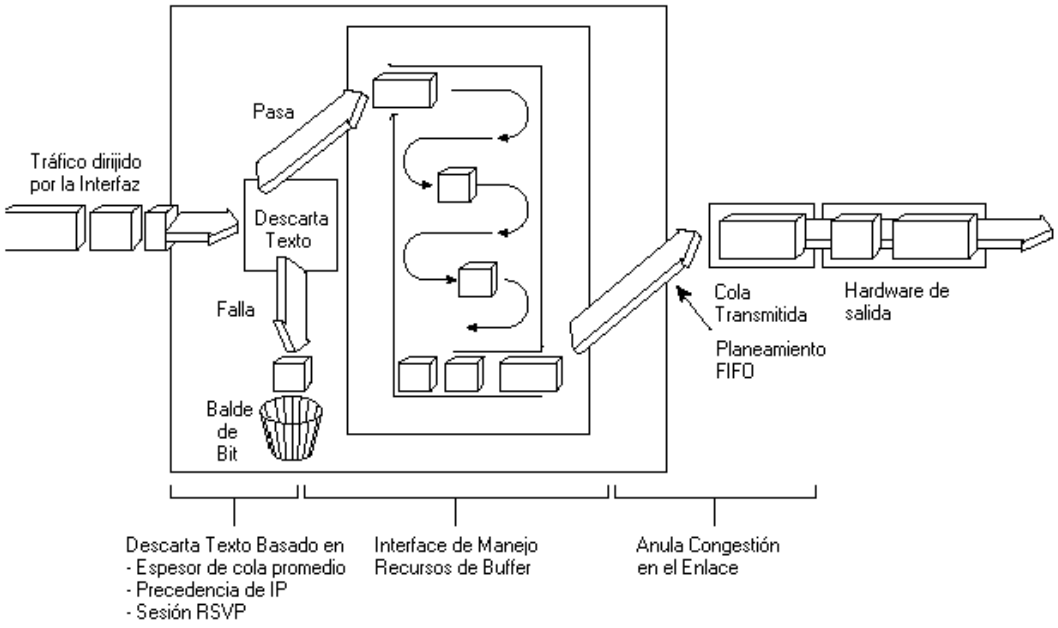


Figura. 2.6. Detección Temprana Aleatoria Pesada.

2.2.3.2 Notificación de Congestión Explícita (ECN).

Este esquema de control propone notificación de congestión marcando los paquetes en lugar de descartarlos como lo hace la detección temprana aleatoria, requiere un campo de notificación de congestión explícita en el encabezado IP, este campo es de dos bits, el primer bit Apto para Transporte de Notificación de Congestión Explícita (ECT) que debe ser ajustado por el emisor para indicar que los puntos extremos del transporte son capaces de hacer notificación de congestión explícita, el segundo bit Experimentó Congestión (CE) que debe ser ajustado por el ruteador para indicar congestión en los nodos extremos, sin embargo los ruteadores que tienen paquetes llegando a una cola llena deberían descartar el paquete.

Son designados como el campo notificación de congestión explícita, los bits 6 y 7 del byte de tipo de servicio del datagrama IP como se observa en la Figura 1.6., donde el bit 6 es el bit apto para transporte y el bit 7 es el bit experimentó congestión.

2.2.4 Mecanismos de reservación y señalización.

2.2.4.1 Protocolo de Reservación de Recursos (RSVP).

Es un protocolo utilizado para brindar un servicio garantizado, así como el Tipo de Servicio (ToS) se dice que realiza una señalización en banda, el protocolo de reservación de recursos se dice que realiza una señalización fuera de banda, este protocolo permite que un computador o elemento de red asegure la reservación de ancho de banda y por ende brinde calidad de servicio a lo largo de la red IP, es decir en todos los nodos intermedios del trayecto, este protocolo es orientado al receptor, es decir el receptor solicita la reservación y la interrumpe.

Existen dos formas de reservación del ancho de banda estas son estática y dinámica. La reservación estática permite asignar un porcentaje fijo del canal de comunicación a cada tipo de protocolo. El protocolo de reservación de recursos permite reservar el ancho de banda en forma dinámica para asegurar calidad de servicio en las redes IP. No es un protocolo de ruteo y solo se lo utiliza para reservar ancho de banda y memoria intermedia.

2.2.4.2 Protocolos de Transporte y Control en Tiempo Real (RTP y RTCP).

El protocolo de reservación de recursos es usado frecuentemente para trabajar en conjunto con el Protocolo de Transporte en Tiempo Real (RTP) y con el Protocolo de Control de Tiempo Real (RTCP), el protocolo de transporte en tiempo real es de capa 4 y trabaja sobre el Protocolo de Datagrama de Usuario (UDP), el protocolo de control en tiempo real permite completa al protocolo de transporte facilitando la comunicación entre extremos para intercambiar datos y monitorear de esta forma la calidad de servicio y obtener información acerca de los participantes en la sesión, para servicios de voz y vídeo en tiempo real.

Los clientes que utilizan voz sobre IP (VoIP) usan flujos UDP, el estándar de esta industria es H.323 empieza la conversación en un puerto (H.323), luego salta a otro puerto

(Q.931) y eventualmente se dividen un flujo de datos (RTP) y en un flujo de control (RTCP).

2.3 SISTEMAS ADMINISTRADORES DE ANCHO DE BANDA DEDICADOS

Los sistemas administradores de ancho de banda son elementos o cajas dedicadas que implementan calidad de servicio sobre los enlaces de área amplia e Internet, estos sistemas específicamente implementan servicio diferenciado y servicio garantizado.

Para un mejor estudio de sistemas administradores de ancho de banda se tomó como referencia un estudio comercial sobre administración y optimización WAN realizado por IDC, esta empresa es la primera inteligencia del mercado global, además es una firma de asesoría en tecnología de información e industrias de telecomunicaciones, ver Anexo 2.

IDC organiza a las industrias dedicadas a la administración y optimización WAN por las ventas realizadas en el año 2003 en el orden que se observa en la Tabla 2.1.

Descripción	Porción (%)
Packeteer	37
Allot Communications	10.2
Cisco	7.6
Expand	7.2
Peribit Networks	6.6
Nortel	6.6
Otros	24.8
Total	100

Tabla. 2.1. Administración y optimización WAN según IDC por ventas en el año 2003.

Como se observa en la Tabla 2.1. el grupo descrito como otros, incluye a: Compuware, NetQoS , Network Physics, RouteScience, Adlex, Ipsum Networks, Packet Design, Proficient Networks, Rocksteady , Riverbed, Bluewave, Alcatel, Juniper, Corvil, ITWorx, Sitara Networks, Niksun y ActivNetworks. El estudio comercial realizado por IDC indica que los sistemas administradores de ancho de banda preferidos son fabricados por Packeteer, Allot Communications, Expand, seguidos por Peribit Networks y Nortel. Los

sistemas administradores trabajan con filosofías similares de implementación de calidad de servicio con pequeñas diferencias especialmente en el control del tráfico. A continuación se realizará un estudio de los tres sistemas administradores de ancho de banda, con mayor porción según la clasificación de IDC, ampliando dicho estudio para PacketShaper de Packeteer y NetEnforcer de Allot por: ser los preferidos en el mercado mundial y en nuestro mercado, y por la disponibilidad física de PacketShaper para una prueba real.

2.3.1 PacketShaper.

PacketShaper es fabricado por Packeteer, posee varios modelos de sistemas, la elección del modelo tiene ver con la capacidad del enlace de Red Área Amplia (WAN). Su ubicación básica en la red es entre el ruteador de la red de área amplia y el switch ó hub de la Red de Área Local (LAN). Los modelos 1500 y 2500 que administran hasta 10 Mbps son utilizados a nivel de una organización, los modelos 4500, 6500, 8500, 9500 y 10000 que administran hasta 1 Gbps son utilizados a nivel de Proveedores de Servicio de Internet (ISP), los modelos se describen en la Tabla 2.2.

Componente	**Modelo 1500**	**Modelo 2500**	**Modelo 4500**	**Modelo 6500**	**Modelo 8500**	**Modelo 9500**	**Modelo 10000**
Max # de clases	256	512	512	1024	2048	2048	2048
Max # de particiones estáticas	128	256	256	512	1024	1024	1024
Max # de particiones dinámicas	*	512	512	5000	20000	20000	20000
Max # de políticas	256	512	512	1024	2048	2048	2048
Max # de reglas para aplicar	640	1280	1280	2500	5000	5000	5000
Max # de reglas para aplicar por clase	40	40	1000	1000	1000	1000	1000
Max # de flujos concurrentes (TCP/ otros IP) **	4500 /2250	18000 /9000	100000 /50000	100000 /50000	200000/ 100000	400000/ 200000	400000/ 200000
Max # de computadores IP a la vez **	5000	10000	25000	100000	100000	200000	200000
Max # de clases con clientes/servidores en mal estado habilitado	8	16	16	16	16	16	16
Max # de clases con habladores/escu_ chadores cumbre habilitado	12 en total habla_ dores + escu_ chado_ res	12 en total habla_ dores + escu_ chado_ res	12 en total habla_ dores + escu_ chado_ res	12 en total habla_ dores + escu_ chado_ res	12 en total habla_ dores + escu_ chado_ res	12 en total habla_ dores + escu_ chado_ res	12 en total habla_ dores + escu_ chado_ res
Tasa de enlace WAN soportada	2 Mbps	10 Mbps	45 Mbps	100 Mbps	200 Mbps	200 Mbps	1 Gbps
Velocidades de la interfaz de conexión	10 ó 100 Mbps full duplex auto detec_ ción	10 ó 100 Mbps full duplex auto detec_ ción	10 ó 100 Mbps full duplex auto detec_ ción	10 ó 100 Mbps full duplex auto detec_ ción	10 ó 100 Mbps ó 1 Gbps (Fibra) full duplex auto detec_ ción.	10 ó 100 Mbps ó 1 Gbps (Fibra) full duplex auto detec_ ción.	10 ó 100 Mbps ó 1 Gbps (Fibra) full duplex auto detec_ ción.

* Este modelo puede tener un máximo de 128 particiones, las cuales son una combinación de particiones estáticas y dinámicas.		** PacketShaper puede soportar más computadores y flujos, sin embargo esos valores representan los ideales para obtener resultados óptimos.

Tabla. 2.2. Modelos y características de PacketShaper.

Se puede obtener modelos de PacketShaper llamados ISP a partir del modelo 4500 (por ejemplo se tiene el modelo 4500/ISP) los cuales incrementan su capacidad de reglas, particiones, flujos, clases, computadores y mantienen su capacidad de ancho de banda.

PacketShaper es montable en un rack de 19 pulgadas, posee un puerto ethernet del enlace entrante (Inbound) y un puerto ethernet del enlace saliente (Outbound), en algunos modelos se puede instalar módulos de expansión de puertos que permiten al PacketShaper adaptarse a topologías que incorporan múltiples redes de área local, posee un puerto serial para configuración por consola, en la Figura 2.7. se observa la caja del PacketShaper.

Figura. 2.7. Caja del PacketShaper.

Packeteer divide al sistema PacketShaper en algunas partes, PacketSeeker que es la herramienta que se encarga de monitorear e identificar el tráfico de la red, mediciones y tareas analíticas; PacketShaper incorpora el monitoreo de PacketSeeker más características de control para corregir y prevenir problemas sin cambios en configuración de ruteador, topologías, servidores o estaciones, protege aplicaciones críticas, contiene el impacto de tráfico recreacional e indeseable, pasa aplicaciones de negocios que necesitan gran ancho

de banda y aprovisiona ancho de banda por aplicación, por usuario o por sesión para maximizar el throughput y el desempeño del control de aplicación, provee calidad de servicio gracias a mecanismos como priorización de tráfico, control de tasa de TCP y algoritmos de planeamiento, además puede marcar paquetes para su tratamiento uniforme a través de redes heterogéneas; PacketWise es el software que permite la configuración del PacketShaper ya sea vía línea de comandos o vía navegador web que es la mejor, está hecha con el Lenguaje de Marcado de Hipertexto (HTML) estándar de páginas web de Internet; PacketCapture le permite aprovecharse de la distribución de PacketSeeker en diversas localizaciones con el fin de capturar flujos de paquetes para su posterior análisis en analizadores de protocolo.

Packeteer ofrece una característica de hardware adicional para PacketShaper, esto es los Módulos de Expansión LAN (LEM) desde el modelo 2500 en adelante, que beneficia a las organizaciones con múltiples LANs sin la necesidad extra de switches o equipos para agregar tráfico. Esta característica de hardware de soporte de módulos de expansión y Pantalla de Cristal Líquido (LCD) de los modelos de PacketShaper son descritas en la Tabla 2.3

Modelo	**LCD**	**Ranuras de expansión de puertos LEM**
1500	No	Ninguna
2500	Si	2
4500	Si	2
6500	Si	2
8500	Si	2
9500	Si	2
10000	Si	2

Tabla. 2.3. Características adicionales de hardware.

PacketShaper posee una tecnología de derivación (bypass) que consiste en que el equipo se comporta como un elemento pasivo que pasa el tráfico a través de sus interfaces, cuando se producen fallas o cuando el equipo está apagado. Antes de conectarlo a la red se debe hacer una configuración inicial mediante cable de consola y aplicaciones de emulación de terminal como Hyperterminal de Windows, para fijar parámetros tales como claves de acceso, dirección IP, máscara de red, nombre de dominio, puerta de enlace por defecto,

Servidores de Nombres de Dominio (DNS) primario y secundario. También se configura sus interfaces, las interfaces ethernet en donde se señala parámetros como velocidad 10 ó 100 Mbps, tipo de comunicación bidireccional half ó full duplex, a la interfaz que maneja el acceso de red de área amplia se le debe indicar el ancho de banda, por ejemplo 2.048 Mbps (E1). Si es un enlace full duplex se debe indicar separadamente los anchos de banda de los enlaces entrante (Inbound) y saliente (Outbound), una vez conectado a la red el PacketShaper es configurable vía navegador web mediante su dirección IP. Sin embargo configuraciones avanzadas pueden requerir el uso de línea de comandos mediante el Protocolo de Emulación de Terminal (TELNET) ó Hyperterminal.

2.3.1.1 Topologías de red.

El sistema PacketShaper generalmente se ubica detrás de los ruteadores del enlace de Red de Área Amplia (WAN) y/o del enlace de Internet en los sitios principales y/o sitios remotos. La unidad debe ser posicionada tal que observe todo el tráfico que se quiere monitorear o administrar.

2.3.1.1.1 Administrando el sitio principal.

Para monitorear el o los enlaces de red de área amplia del sitio principal, se debe colocar a PacketShaper como se observa en la Figura 2.8.

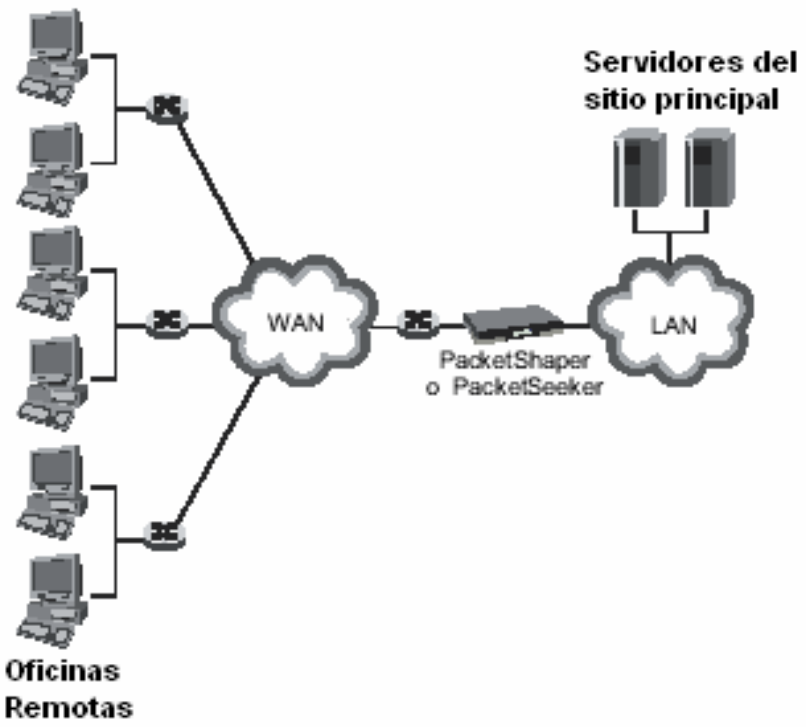


Figura. 2.8. PacketShaper administrando el sitio principal.

Para monitorear y controlar el desempeño de cada oficina remota efectivamente desde una localización centralizada, el Enlace de Red de Area Amplia (WAN) debe operar como un hub, es decir el tráfico de las oficinas remotas deben ir a través del PacketShaper en el sitio principal y no debe existir tráfico directo entre oficinas remotas. En esta ubicación PacketShaper observa todo el tráfico, incluso el acceso a Internet de las oficinas remotas, se basa en servidores colocados en el sitio principal, cabe señalar que PacketShaper no administra el tráfico entre oficinas remotas.

La operación como hub del enlace WAN no es necesaria solamente cuando se necesite administrar el enlace WAN del sitio principal y no se necesite administrar las conexiones WAN de cada oficina. En esta topología PacketShaper no puede ofrecer su capacidad adicional de compresión de datos sobre el enlace WAN. En esta topología de red, la suma de la velocidad de los enlaces de red de área amplia no debe sobrepasar la capacidad del sistema PacketShaper.

Esta topología es útil para aplicaciones o servidores colocados en el sitio principal, cada oficina debe acceder al Internet a través del sitio principal o a través de una conexión a Internet que no use la misma conexión de última milla del enlace WAN. El valor típico de oficinas que se puede monitorear y controlar varía desde 3 a 100 oficinas remotas.

Colocando PacketShaper en una red que se ajuste a esta topología se puede, ganar visibilidad de la red y del comportamiento de aplicaciones antes de realizar algún cambio, probar la tecnología haciendo una extensa investigación, aplicar políticas de calidad de servicio de acuerdo a lo experimentado y opcionalmente determinar la necesidad de sistemas PacketShaper en ciertas oficinas remotas (para controlar de manera óptima tráfico como VoIP o UDP). El algoritmo implementado por PacketShaper, control de tasa de TCP ayuda a controlar el tráfico TCP en ambas direcciones, lo que ayuda a minimizar la necesidad de otros sistemas en los sitios remotos, esto es una ventaja de esta topología debido a que el costo se reduce.

2.3.1.1.2 Administrando el enlace de Internet del sitio principal.

PacketShaper también puede monitorear el tráfico del enlace de Internet del sitio principal en el caso de que exista oficinas conectadas mediante Redes Privadas Virtuales (VPN), usuarios VPN con acceso telefónico, extranets de importancia o simplemente la Web. No se necesita ningún requerimiento especial para este tipo de topología, por ejemplo se puede controlar aplicaciones que permanecen en servidores del sitio principal y a las cuales se accede a través de la VPN desde las oficinas remotas.

Una VPN es una red de datos privada que usa la infraestructura de telecomunicaciones pública para extender un enlace de Red de Area Amplia (WAN) desde un sitio principal a oficinas remotas o usuarios con acceso telefónico. Los procedimientos de encriptación y seguridad mantienen una transferencia de datos privados, una compañía habilita una VPN para distribuir datos y aplicaciones sin la necesidad de líneas dedicadas, Frame Relay o líneas privadas. Puede resultar una alternativa WAN económica, sin embargo el desempeño de aplicaciones críticas a través de la VPN puede no ser el deseado, ver Anexo 3.

PacketShaper en este tipo de topología es muy útil cuando por el enlace de Internet de un sitio principal cursan aplicaciones críticas y tráfico casual, o cuando se necesita encontrar que tráfico está utilizando el enlace de Internet y como se comporta. En esta topología PacketShaper puede proteger tráfico VPN, usuarios con acceso telefónico, opcionalmente contener tráfico web indeseable tales como descargas de música y paso de multimedia para un desempeño óptimo, descubrir los 10 destinos webs más solicitados, entre otras funciones. Las características de clasificación Web de PacketShaper son muy útiles para este tipo de topología de administración del enlace de Internet, debido a que el tráfico Web puede variar en urgencia, sensibilidad a la latencia y requerimientos de desempeño específicos. PacketShaper permite una clasificación basada en dirección de destino, localización del servidor, tipo de Extensiones de Correo de Internet Multipropósito (MIME) como por ejemplo extensiones XML, MPEG, etc.; Localizador de Recurso Uniforme (URL), y otros criterios que ayudan a distinguir entre navegación casual, aplicaciones de negocios, actividades en línea de consumidores entre otras aplicaciones.

Con este tipo de topología PacketShaper ofrece todas sus características de control, además puede monitorear que cantidad de tráfico va hacia las VPNs de las oficinas y que cantidad de tráfico va para la navegación casual, por ejemplo permite asignar una tercera parte de enlace de Internet al tráfico VPN o a una extranet de importancia, o dar a cada usuario de la VPN un mínimo y máximo apropiados, asignar una tasa de datos apropiada para flujos multimedia, bloquear tráfico indeseable como acceso a sitios Web de contenido cuestionable.

Una limitación de esta topología es que no se puede controlar el desempeño del propio enlace de Internet de cada oficina remota, es decir PacketShaper no ayuda a un mejor desempeño del tráfico WAN de cada oficina remota las cuales usan una diferente red y un diferente enlace de Internet. Para escoger un modelo de PacketShaper adecuado para esta topología se debe tomar en cuenta la capacidad del enlace de Internet, se debe anticipar el número de flujos concurrentes posibles y se debe anticipar el número de usuarios.

Para el caso de una VPN, PacketShaper puede ser ubicado en cualquier extremo del gateway VPN, la posición con respecto al gateway VPN dicta si PacketShaper clasificará aplicaciones antes o después de la encriptación y si podrá soportar la opción adicional de

compresión de PacketShaper conocida como PacketShaper Xpress y que se menciona en el siguiente apartado 2.3.1.1.3.

En la Figura 2.9. se observa a PacketShaper entre el ruteador y el gateway VPN, en esta topología no se puede utilizar la función de compresión de PacketShaper Xpress, pero es una forma fácil y rápida de descubrir todo el tráfico VPN encriptado con el fin de protegerlo. PacketShaper en esta posición puede observar tanto el tráfico VPN encriptado como el tráfico web normal u otras aplicaciones, clasifica al tráfico VPN de acuerdo al protocolo de encriptación y no observa que aplicaciones son encriptadas. Diferencia automáticamente muchos tipos de tráfico seguro como Encapsulación de Seguridad IP-Encabezamiento de Autenticación (IPSec-AH), Encapsulación de Seguridad IP-Payload de Seguridad Encapsulado (IPSec-ESP), Protocolo para formar Túneles Punto a Punto (PPTP), Protocolo para formar Túneles Capa 2 (L2TP), DLS que es el protocolo de la Arquitectura de Red de Sistemas IBM (SNA) sobre TCP, protocolo de Capa de Zócalos Segura (SSL) para tráfico web seguro, protocolo de autenticación remoto Protección Segura (SSH), Servicio de Autenticación Remota de Llamada de Usuario (RADIUS), Encapsulación de Enrutamiento General (GRE), Intercambio de Clave en Internet (IKE).

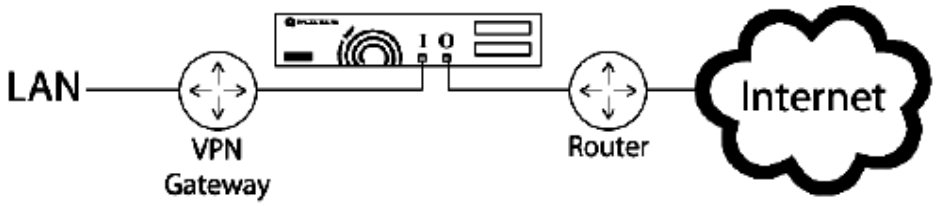


Figura. 2.9. PacketShaper entre el VPN gateway y el ruteador.

En la Figura 2.10. se observa a PacketShaper entre la LAN y el VPN gateway, esta topología permite utilizar la función de compresión PacketShaper Xpress siempre que la VPN permita tráfico de el Protocolo de Reservación de Recursos (RSVP), el Protocolo de Compresión del Payload IP (IPCOMP) usado para reducir el tamaño de los paquetes IP y la VPN no use Traducción de Dirección de Red (NAT). Adicionalmente esta topología permite diferenciar entre múltiples aplicaciones encriptadas.

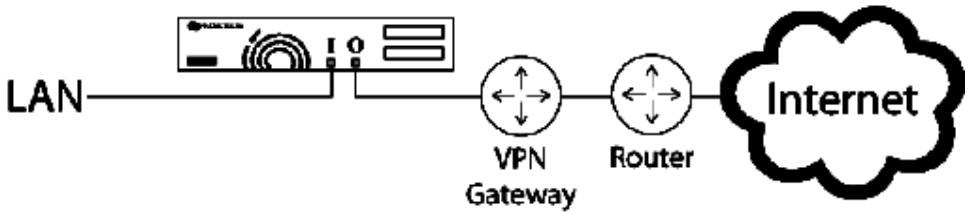


Figura. 2.10. PacketShaper entre la LAN y el VPN gateway.

La Traducción de Dirección de Red (NAT) permite a varios computadores de una Red de Area Local (LAN) utilizar una sola dirección IP para el enlace de área amplia, especialmente para acceso al Internet.

2.3.1.1.3 Administrando el sitio principal y los sitios remotos.

Una administración completa de la red incluye sistemas PacketShaper en el sitio principal y en cada oficina remota, como se observa en la Figura 2.11. Esta topología monitorea y/o controla el desempeño de todas las aplicaciones en todas las oficinas indiferentemente del tamaño de la red. Esta topología permite obtener una vista más granular del uso del ancho de banda y desempeño en redes tipo hub y tipo malla, esta topología no está diseñada para redes tipo token ring.

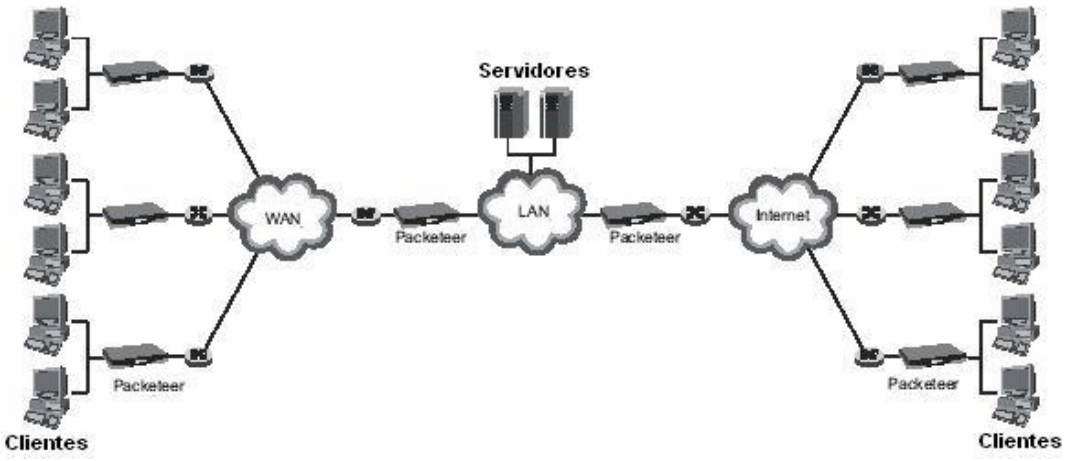


Figura. 2.11. PacketShaper administrando todos los sitios.

En este tipo de topología las aplicaciones a ser monitoreadas y/o controladas pueden encontrarse en servidores en el sitio principal o en las oficinas, no existe un límite específico del número de oficinas que se puede tener en esta topología, típicamente va desde 10 a varias centenas de oficinas

Esta topología es la más poderosa y flexible, es escalable, permite la administración de cada oficina, permite la administración de redes en malla para tráfico que no atraviese el sitio principal (como sucede en tipo hub), permite controlar tráfico desde oficina a oficina como voz sobre IP (VoIP), compartición de carpetas, herramientas comunes; permite la administración de los enlaces de Internet de cada oficina, permite ubicar los servidores de aplicaciones se pueden en el sitio principal o en las oficinas, permite a oficinas pequeñas acceder a aplicaciones centralizadas a través de enlaces WAN pequeños, este tipo de topología controla eficientemente aplicaciones no basadas en TCP, como en Protocolo de Datagrama de Usuario (UDP), también se recomienda para redes punto a punto que usan tecnología Frame Relay en su red de área amplia.

Esta topología es más adaptable a redes grandes y crecientes, cada oficina necesita un sistema PacketShaper que se ajuste a la capacidad del enlace WAN. Esta topología es más completa que las anteriores pero puede resultar más costosa debido a que la cantidad de sistemas se incrementa.

Además esta topología permite el uso de una nueva característica de PacketShaper que es PacketShaper Xpress, que es una herramienta de compresión en la red, crea túneles de compresión entre los sistemas PacketShaper cuando el tráfico es transmitido, sin embargo no se estudiará detalladamente esta característica del sistema puesto que no es el objetivo principal de este trabajo.

En la Figura 2.12. se observa como se ha creado un túnel A para el tráfico entre los clientes en la oficina A y los servidores del sitio principal. De igual forma crea un túnel B para el tráfico entre los clientes de la oficina B y los servidores del sitio principal. El túnel C es creado para el tráfico entre los clientes de la oficina A y los clientes de la oficina B.

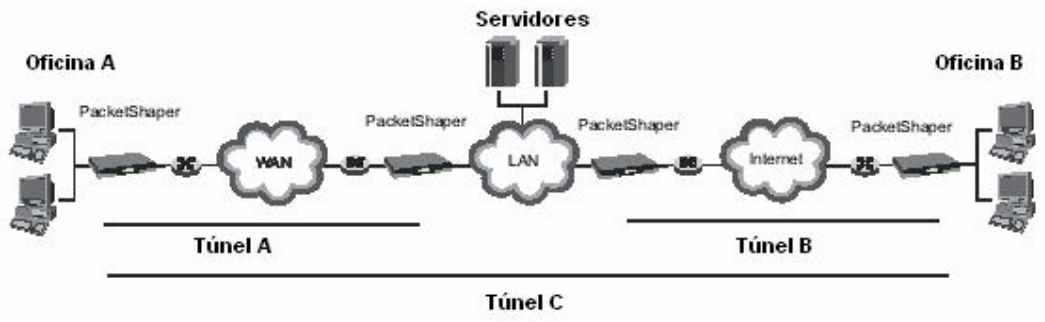


Figura. 2.12. PacketShaper Xpress.

2.3.1.1.4 Topología con múltiples redes de área local.

Se puede tener un ambiente con múltiples Redes de Area Local (LANs) conectadas a uno o más ruteadores vinculados al Enlace de Red de Area Amplia (WAN) o enlaces de Internet. Hasta tres LANs y tres ruteadores pueden ser conectados directamente a un sistema PacketShaper por medio de la característica de hardware adicional de PacketShaper los Módulos de Expansión LAN (LEM), que puede beneficiar a las organizaciones con múltiples LANs sin la necesidad extra de switches o equipos para agregar tráfico..

Esta topología sirve para a todo el tráfico usando cualquier porción del ancho de banda del enlace de acceso manejarlo junto con una estrategia cohesiva. No es efectivo reforzar una asignación de ancho de banda basado en política en una porción del tráfico de un ruteador, si existe tráfico sin controlar desde una LAN adicional que puede adjudicarse la capacidad del ruteador y disminuir cualquier ganancia potencial de desempeño.

Packeteer ofrece tres modelos de LEM diferentes dependiendo del tipo de enlace, 100 Megabit LEMs para enlaces 10/100BaseT, Gigabit LEMs para enlaces 10/100/1000BaseT, Gigabit LEMs de Fibra óptica para enlaces 1000Base-SX o 1000Base-LX. El modelo de PacketShaper que debe escogerse en base a la capacidad del enlace WAN y no en base a una LAN en particular.

En esta topología PacketShaper ofrece completo monitoreo, análisis y control para todo el tráfico en todos los puertos LEM. En la Figura 2.13. se observa un ejemplo de esta topología donde tres LANs son vinculadas a un simple switch, el cual es conectado al puerto del enlace de entrada (Inbound) de los puertos principal, superior e inferior en el PacketShaper, todos los puertos del enlace de salida (Outbound) son conectados a un simple ruteador. En este ejemplo se puede separar estrategias de estadísticas y control para cada LAN definiendo clases de tráfico basadas en direcciones o subredes IP para las LANs y posteriormente configurar una partición estática de ancho de banda para cada clase.

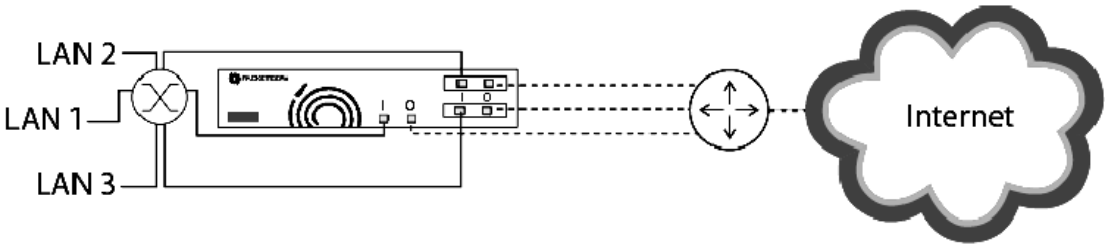


Figura. 2.13. PacketShaper y múltiples redes de área local conectadas a un switch.

En la Figura 2.14 se muestra un segundo ejemplo de esta topología donde se observa que los tres switches de las LANs son conectadas a los puertos de enlace de entrada (Inbound) principal, superior e inferior en el PacketShaper, todos los puertos del enlace de salida (Outbound) son conectados a la correspondiente WAN en el ruteador. En este ejemplo se puede clasificar el tráfico por Módulos de Expansión LAN (LEM) principal, superior e inferior para segregar el tráfico LAN en el árbol de clases.

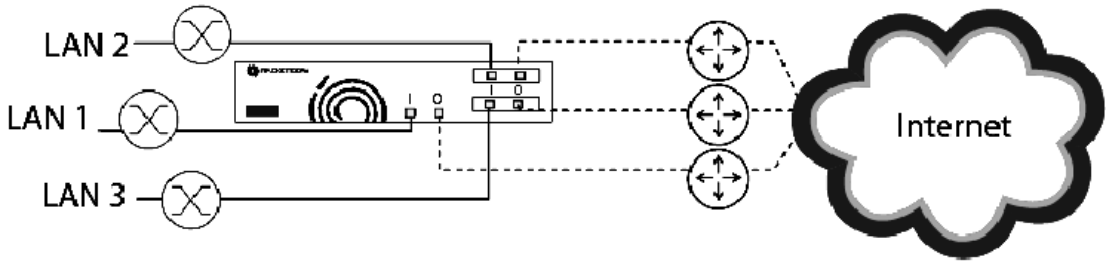


Figura. 2.14. PacketShaper y múltiples redes de área local conectadas a tres switches.

En el caso de que se tenga más de tres LANs compartiendo un simple enlace WAN o conexión de Internet, se de be considerar utilizar la topología que se observa en la Figura 2.13. es decir todas las LANs conectadas a un switch y todos los puertos del enlace de entrada de PacketShaper al mismo switch.

Otra topología con múltiples LANs incluye una red donde PacketShaper interactúa con un elemento de seguridad (firewall), aquí se requiere la consideración de la Traducción de Dirección de Red (NAT) y/o una Zona Desmilitarizada (DMZ). Un elemento de seguridad (firewall) crea dos Redes de Área Local (LAN), una red privada y una Zona Desmilitarizada (DMZ), se puede incorporar un módulo de expansión al PacketShaper para proveer puertos ethernet adicionales, así la red privada se conecta a los puertos que trae el sistema y la zona desmilitarizada se conectada a los puertos del módulo de expansión como se observa en la Figura 2.15.

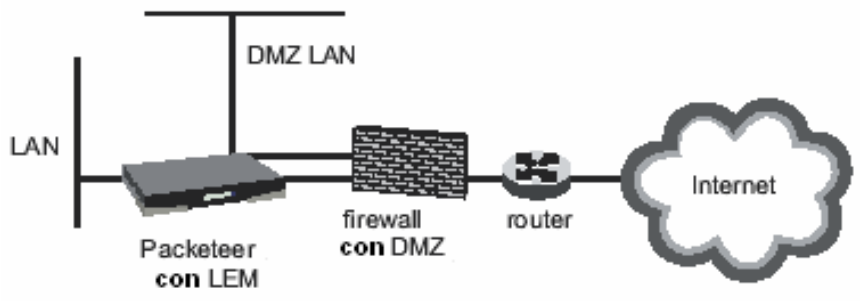


Figura. 2.15. Topologías con múltiples redes de área local.

PacketShaper maneja el tráfico de la LAN protegida de la manera común, es decir como si no se tuviera la DMZ. Si se tiene NAT, PacketShaper trata solamente con direcciones IP internas. Si el elemento de seguridad (firewall) es un punto de terminación de túneles VPN, entonces PacketShaper descubrirá solamente el tráfico no encriptado. PacketShaper posee características de clasificación inteligente de aplicaciones y la habilidad de control individual entre el elemento de seguridad y la LAN sin protección (DMZ), controla varios tipos de tráfico en vez de una masa grande de tráfico de seguridad como IPSec, por ejemplo asignar una tercera parte del enlace WAN a la DMZ y si la DMZ no está en uso distribuir su ancho de banda. Si se usa la función de descubrir las diez direcciones IP

internas que más interactúan con cualquier tipo de tráfico, las direcciones que descubra PacketShaper serán las direcciones IP reales de la LAN.

Es posible colocar a PacketShaper entre el ruteador y el elemento de seguridad, pero esta topología no es recomendada debido a que PacketShaper solamente descubrirá las direcciones NAT configuradas, si se utiliza la función de descubrir las diez direcciones IP internas que más interactúan con cualquier tipo de tráfico aparecerán como una dirección IP, la clasificación y control de tráfico VPN podría ser muy ordinario.

La elección de un sistema PacketShaper difiere de la presencia o no presencia de un elemento de seguridad (firewall) en la red, el sistema PacketShaper debe ser escogido en base a la capacidad del enlace de Red de Area Amplia (WAN) y a otros parámetros como número de clases y flujos de tráfico.

2.3.1.1.5 Topología con servidores

En la red puede existir algunos servidores entre los que se encuentra el servidor proxy que realiza la Traducción de Dirección de Red (NAT), esto debe ser considerado a la hora de ubicar el PacketShaper. Para que PacketShaper sea efectivo debe ser colocado entre el ruteador y el servidor proxy como se observa en la Figura 2.16. debido a que este servidor es el que empieza y termina las conexiones del Protocolo de Control de Transmisión (TCP).

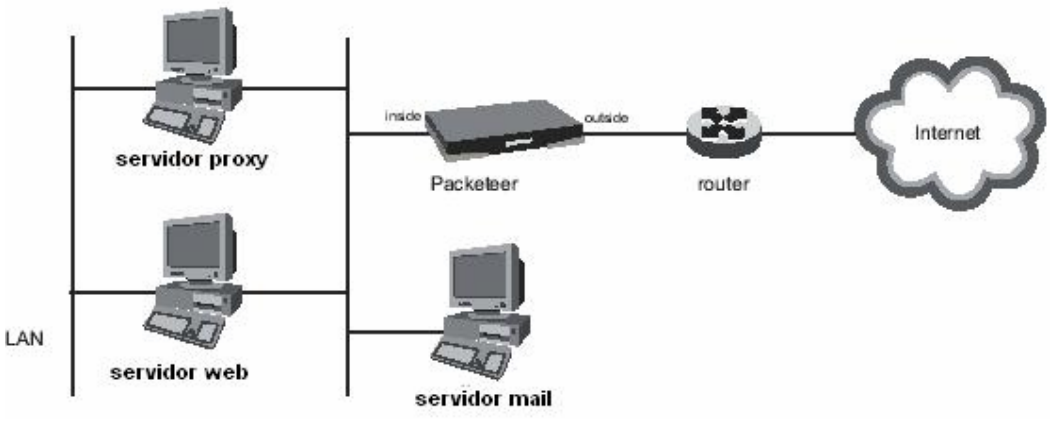


Figura. 2.16. Topología con servidor proxy.

2.3.1.1.6 Topologías con configuraciones redundantes.

PacketShaper ofrece dos modos para proveer redundancia, el primero es Estado de Espera Caliente (Hot Standby) que permite a unidades PacketShaper actuar como un par redundante conectado al mismo ruteador y la segunda es Estado de Espera Directo (Direct Standby) que permite a unidades PacketShaper trabajar en una topología de red redundante, en la cual cada unidad es conectada a un ruteador diferente.

Se puede colocar dos equipos de iguales características en una configuración redundante (Hot Standby) como se observa en la Figura 2.17., debido a que PacketShaper une dos elementos de red (bridge) utiliza el protocolo conocido como Arbol de Extensión (Spanning Tree), donde el tráfico pasa a través del PacketShaper primario y el PacketShaper secundario o de respaldo permanece inactivo solamente enviando información de estatus al primario, cuando el PacketShaper primario falla el PacketShaper secundario entra a funcionar tomando todas las responsabilidades del PacketShaper primario. Para implementar esta configuración es necesario deshabilitar la tecnología de derivación (bypass) de los PacketShapers, para evitar que ambas unidades envíen tráfico duplicado.

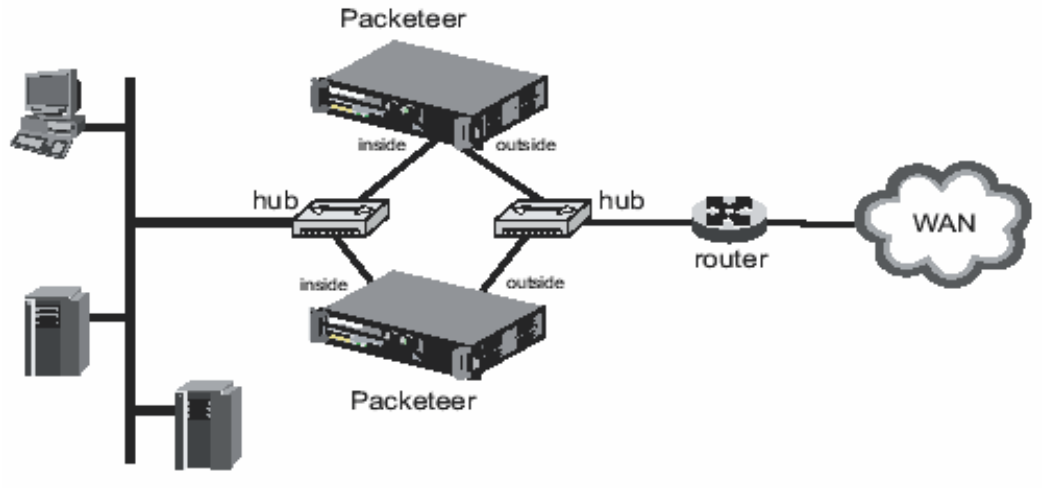


Figura. 2.17 Configuración "Hot Standby" de PacketShaper.

En sentido general, disponibilidad alta es una característica de topología de red, esta asegura que aplicaciones críticas estén disponibles el 100% del tiempo. Esta meta típicamente se cumple teniendo múltiples ruteadores de acceso con múltiples interfaces de Red de Area Amplia (WAN).

Las unidades PacketShaper pueden adaptarse en dichas topologías redundantes y cumplir las responsabilidades de administración sin interrumpir la configuración de alta disponibilidad existente. La configuración llamada Estado de Espera Directo (Direct Standby) como se observa en la Figura 2.18, permite a dos PacketShapers trabajar en una topología de red redundante, esto es con ruteadores redundantes, switches redundantes, dos caminos de datos, dos Redes de Area Local (LANs) y/o elementos de seguridad (firewalls) redundantes. Para implementar las configuraciones redundantes de estado de espera directo es necesario colocar Módulos de Expansión LAN (LEM), según la topología que se necesite administrar, los dos PacketShapers son conectados directamente uno con otro a través del puerto del enlace de salida (Outbound) del módulo LEM. Además es necesario que ambos PacketShapers tengan los mismos límites de configuración y memoria instalada, no se debería mezclar PacketShapers con diferentes capacidades porque las dos unidades observan el mismo tráfico y requiere configuraciones idénticas. La conexión directa entre las dos unidades debe ser igual o mayor en velocidad que cada uno de los enlaces WAN, este requerimiento asegura que cada unidad recibe la copia de tráfico desde

la otra unidad lo suficientemente rápido para prevenir paquetes fuera de orden. Para implementar esta configuración es necesario deshabilitar la tecnología de derivación (bypass) de los PacketShapers, para evitar que ambas unidades envíen tráfico duplicado. Debido a que la tecnología de derivación debe ser deshabilitada, los PacketShapers no deben ser apagados cuando ellos estén conectados en una topología de estado de espera directo, apagarlos puede causar pérdida de conectividad en el enlace y todo el tráfico sea enrutado al otro camino.

Por ejemplo en una topología básica de dos PacketShapers cada uno conectado a un ruteador diferente como se observa en la Figura 2.16, ambos PacketShapers son considerados activos y cada uno puede recibir y enviar tráfico. Para asegurar que ambas unidades obtengan el mismo árbol de clasificación tráfico y medición de datos, cada PacketShaper procesa los paquetes recibidos desde el otro. Cuando un PacketShaper recibe tráfico directamente, este copia el tráfico y lo transmite a la otra unidad. La otra unidad clasifica el tráfico de la misma forma que el que lo ha recibido directamente, pero no envía el tráfico hacia la LAN.

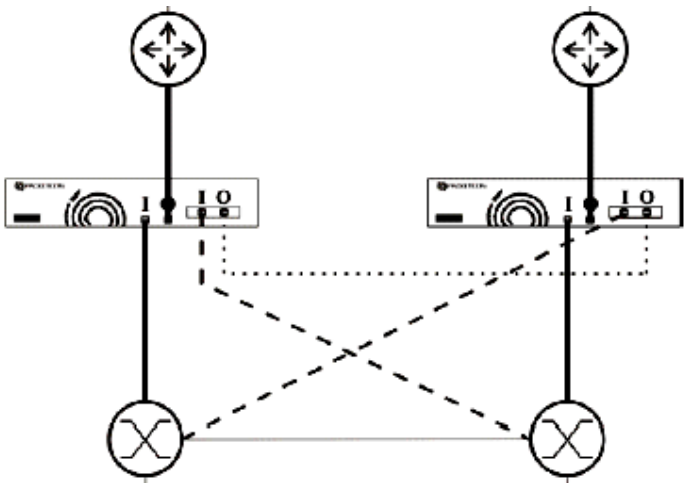


Figura. 2.18. Configuración "Direct Standby" de PacketShaper con ruteadores redundantes.

PacketShaper colocado en una topología de estado de espera directo ofrece todas sus características de monitoreo y análisis. Ofrece la mayoría de sus características de control incluyendo protección, contención, paso de tráfico, provisión de ancho de banda, el algoritmo de control de tasa de TCP, marcado de paquetes, supresión de ataques, además

se puede su función opcional de compresión. Limitaciones conocidas de PacketShaper colocado en esta topología son enlaces WAN que trabajen con tecnología Frame Relay y Modo de Transferencia Asincrónica (ATM).

En esta topología ambos PacketShapers deben ser idénticos, asumiendo que ambos enlaces están activos, cada PacketShaper necesita ser un modelo que pueda procesar la cantidad de throughput en ambos ruteadores, por ejemplo si se tiene dos enlaces de 45 Mbps y los dos están activos, cada PacketShaper necesita soportar 90 Mbps.

2.3.1.1.7 Topologías no en línea o modo observador.

La topología modo observador es usada para monitorear tráfico no en línea, donde PacketShaper nos es cableado en el camino de datos principal. Este tipo de topología se ajusta a empresas que tienen procedimientos de control de cambios estrictos o restricciones de seguridad de la introducción de elementos en línea dentro de la red.

PacketShaper configurado en modo observador monitorea pasivamente el tráfico en la red y desarrolla tareas de clasificación y reporte de todo el tráfico como si se encontrara en línea, brindando visión de las aplicaciones que están atravesando la red y descubriendo problemas de desempeño. PacketShaper no puede realizar modelamiento de tráfico en esta topología, es por esto que se puede tener la opción de tener solo la opción de monitoreo llamada PacketSeeker.

PacketShaper configurado en modo puede ayudar a realizar una auditoría de red o una valoración de las aplicaciones atravesando la red ofreciendo a la vez flexibilidad de topologías en ambientes de centros de datos complejos o restringidos, PacketShaper puede trabajar de forma similar a un probador de red pero sus capacidades de monitoreo extendidas pueden clasificar y grabar medición de datos por aplicaciones (capa 7), antes que una clasificación por puertos TCP. Esta topología también permite hacer un estimativo de la función de compresión de PacketShaper.

En la Figura 2.19. se observa un ejemplo de PackeShaper colocado en una topología en modo observador, PacketShaper monitorea el tráfico desde tres diferentes segmentos de Red de Area Local (LAN), esto se logra instalando dos Módulos de Expansión LAN (LEM). El puerto del enlace de salida (Outbound) se conecta a un switch o hub de la LAN1 y los otros dos puertos del enlace de salida se conectan a un puerto SPAN del switch de la LAN2 y LAN3 respectivamente. Se conecta los puertos del enlace de salida a los puertos SPAN de cada switch para que PacketShaper pueda tener acceso a todo el tráfico WAN, para esto se debe tener una copia del tráfico bidireccional del puerto del ruteador en el puerto SPAN del switch para que PacketShaper lo reciba y lo pueda monitorear. Se puede acceder y administrar a PacketShaper desde la LAN1 o se puede administrar a través de cualquiera de los tres puertos del enlace de entrada (Inside). En este ejemplo la mejor opción es realizar una clasificación de tráfico en direcciones IP para cada LAN.

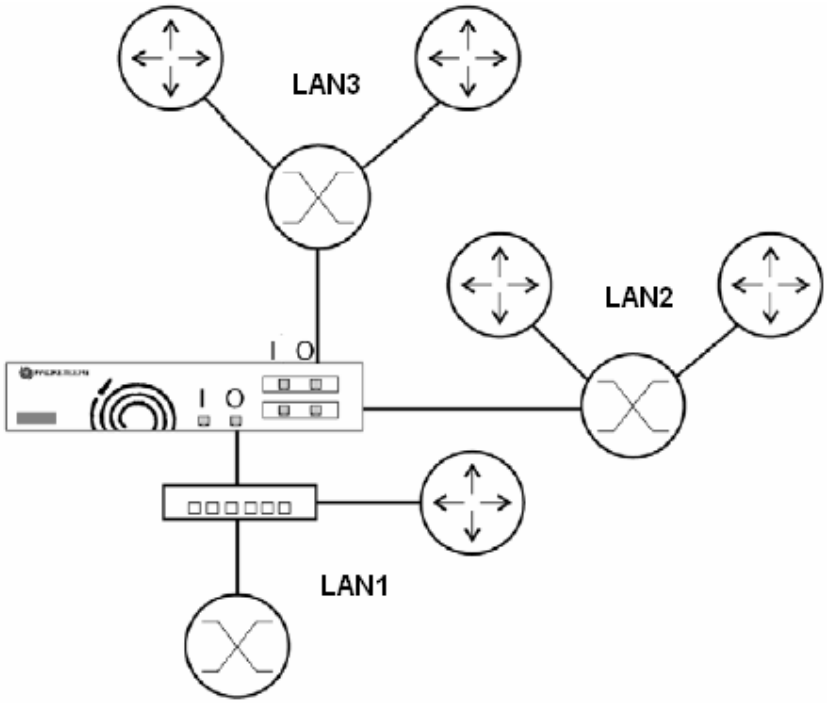


Figura. 2.19. PacketShaper colocado en una topología en modo observador.

Para escoger un modelo de PacketShaper adecuado para esta topología se debe tomar en cuenta la capacidad del enlace de Internet, se debe anticipar el número de flujos concurrentes posibles y se debe anticipar el número de usuarios. Si se monitorea el tráfico de varias LANs, se debe escoger un modelo basado en la capacidad total del enlace WAN

o la suma de los enlaces WAN y no se necesita tomar en cuenta la necesidad de una LAN en particular.

Todos los modelos pueden tener la opción de fuente de alimentación redundante dentro de un mismo equipo.

PacketShaper se basa en cuatro puntos básicos que son clasificación, análisis, control del tráfico y reporte.

2.3.1.2 Monitoreo y Clasificación.

El monitoreo y clasificación son hechas por PacketSeeker, tiene la habilidad para diferenciar cientos de tipos diferentes de tráfico, PacketShaper puede diferenciar tráfico basado básicamente en:

- Aplicación ó en capa 7, aplicaciones par a par (P2P) como KaZaA.
- Protocolo, número de puerto.
- Localizador de Recurso Uniforme (URL).
- Nombre de computador, lista de computadores.
- Servicios diferenciados, Tipo de servicio (ToS), Clase de Servicio (CoS).
- Conmutación de Etiquetas MultiProtocolo (MPLS)
- Tipo de servicio (ToS), Clase de Servicio (CoS).Dirección de Control de Acceso al Medio (MAC).

- Dirección IP fuente/destino, subred.

- Rango de velocidad de computador.

- Tipo de Extensiones de Correo de Internet Multipropósito (MIME).

- Bases de datos.

- Redes de Área Local Virtuales (VLAN) basadas en el estándar 802.1q y otras.

PacketSeeker aparece dentro de paquetes y encabezados observando marcas características o aplicaciones específicas, puede distinguir aplicaciones múltiples usando el mismo puerto TCP, descubre tráfico para bases de datos específicos y reconoce otro tráfico que se muestra ilusorio para ruteadores y soluciones similares, cada categoría de tráfico es llamada una clase de tráfico.

El tráfico que es monitoreado y clasificado se puede analizar mediante estadísticas proporcionadas en gráficos de PacketSeeker similar a un analizador de protocolos, si se necesita un tipo de información específica y PacketSeeker no lo proporciona, se puede configurar remotamente los parámetros mediante PacketCapture para capturar muestras de tráfico y descargarlos para su posterior análisis.

Los protocolos son designados como clases y se muestran en una lista del enlace de entrada (Inbound) para flujos entrantes y en una lista del enlace de salida (Outbound) para flujos salientes como se observa en la Figura 2.20. Las clases de tráfico que consumen mayor ancho de banda son mostrados en la parte superior de estas listas y los que no pueden ser clasificados se envían a una clase por defecto (Default).

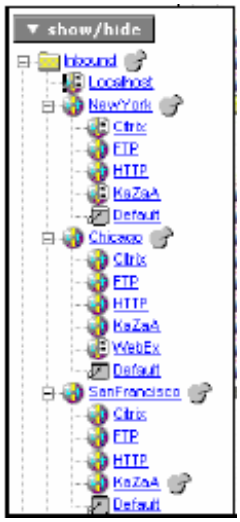


Figura. 2.20. Clases creadas por PacketSeeker.

Se pueden crear subclases personalizadas para clasificar tráfico basado en el nombre de computador, dirección, subred o puertos; por ejemplo la clase de tráfico del Protocolo de Transferencia de HiperTexto (HTTP) podría ser divida en subclases con dichos parámetros.

2.3.1.3 Análisis y reporte.

La gestión de tiempos de respuesta de PacketSeeker, basado en Medidas de Tiempo de Respuesta (RTM), permite analizar medidas de retardos y Tiempos de Viaje Redondo (RTT), proporciona reportes para análisis de transacciones, conexiones, estado de las sesiones TCP, eficiencia de la red, tiempos de intercambio de paquetes, tiempos de vida de ida y vuelta, además informes de utilización de enlaces con máximos, utilización de la clase con máximos, “top ten” de las aplicaciones que más consumen el ancho de banda, quién genera más un tipo de tráfico (top talkers), quién recibe más un tipo de tráfico (top listeners), retransmisiones de conexiones, distribución de tamaño de paquetes, octetos transmitidos, cumplimiento del nivel de servicio por enlace, tiempos de respuesta en milisegundos, flujos activos e historial de tráfico. Los reportes gráficos son de tipo pastel, línea o área, por ejemplo en la Figura 2.21. se observa un reporte gráfico tipo línea y se refiere a la utilización de un enlace.

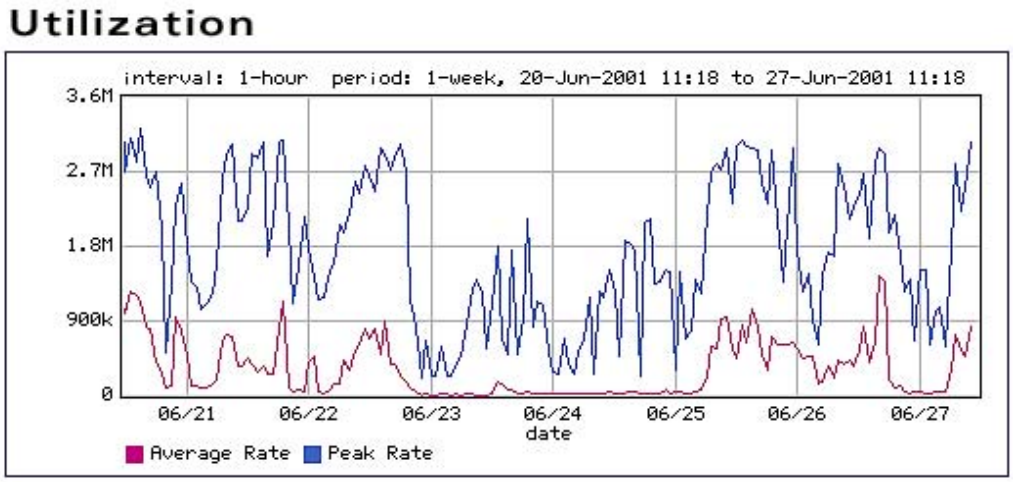


Figura. 2.21. Gráfico de utilización de PacketSeeker.

Otras medidas que se pueden obtener son caudal de procesamiento (throughput) para alguna clase; dirección IP, lista de computadores, subred, paquetes, transacciones ó conexiones; conteo y porcentaje de conexiones TCP que fueron negadas por una política o por falta de recursos, conexiones TCP ignoradas, abortadas ó rechazadas por servidores; conteo y porcentaje de paquetes TCP descartados, recibidos ó retransmitidos; número de mensajes de respuesta del Protocolo de Transferencia de HiperTexto (HTTP) con códigos de error; el número más grande de conexiones TCP simultáneas, conteo de flujos de tráfico que fueron bloqueados después de exceder un Rechazo de Servicio (DoS).

PacketShaper descubre rápidamente el tráfico en una red, sin embargo necesita tres días para obtener suficientes datos para aplicar eficientemente el control, PacketShaper guarda datos desde un día con intervalos de muestras de un minuto y guarda datos de hasta un mes con intervalos de muestras de una hora permitiendo realizar un análisis más amplio del comportamiento del tráfico en una red.

Permite enviar alarmas empleando e-mails, mensajes (traps) del Protocolo de Administración de Red Simple (SNMP), mensajes a un servidor Syslog, de esta forma el operador de red no requiere estar conectado constantemente al PacketShaper

2.3.1.4 Control.

Packetshaper realiza el control de tráfico mediante algunos mecanismos como priorización de tráfico, planeamiento de límite de retardo y control de tasa de TCP.

2.3.1.4.1 Control de tasa de TCP.

El control de tasa de TCP suaviza los flujos de tráfico detectando una velocidad de acceso del usuario remoto, factorizándolo con la latencia de la red y correlacionando este dato con otra información de flujo de tráfico, en lugar de hacer encolamiento de datos. Control de tasa de TCP es patentado por Packeteer y determina la tasa de TCP en base a tres variables, la tasa de reconocimientos, el número de reconocimiento y el tamaño de ventana máximo del receptor.

Específicamente dado un tamaño de ventana deslizante de TCP constante, la tasa de TCP es igual a la tasa de flujo de reconocimientos, el control de la tasa de reconocimientos permite ralentizar el incremento acelerado del tráfico debido al algoritmo “slow start”. PacketShaper puede retener y negociar reconocimientos, formando colas de reconocimientos, observa que paquetes guardados en las colas pueden ser considerados para el mantenimiento de estado por flujo activo. Basado en esta definición, PacketShaper reduce la cantidad de estado por flujo agregado, es decir paquetes más reconocimientos, esto incurre en menos retardos de transmisión y la negociación de reconocimientos resulta en la reducción en retardos producidos por encolamiento experimentados por la conexión en cuellos de botella o en los ruteadores.

Lo anterior asume una ventana deslizante de TCP constante, pero esta no lo es debido a que el lado derecho de la ventana es controlado por la ventana del receptor en los reconocimientos de TCP y el algoritmo “slow start” mediante la ventana de congestión (cwnd), mientras que el lado izquierdo de la ventana es controlado (deslizado) por el campo de número de reconocimiento en los reconocimientos de TCP. El control de tasa de TCP es predictivo, cambia las semánticas de TCP extremo a extremo desde su posición en el medio de la conexión, observa el control del tamaño de la ventana, calcula el Tiempo de

Viaje Redondo (RTT) y entonces negocia (sostiene) los reconocimientos lo que le permite controlar retardos producidos por encolamiento sin producir tiempos sin respuesta de conexiones (time outs), incrementar el caudal de procesamiento (throughput) individual de cada conexión TCP y con una granularidad fina.

2.3.1.4.2 Planeamiento de límite de retardo.

PacketShaper utiliza un planeamiento de límite de retardo (delay bound scheduling) para controlar tráfico del Protocolo de Datagrama de Usuario (UDP) que no puede ser controlado por el control de tasa de TCP, originalmente el planeamiento de límite de retardo es utilizado por ruteadores en servicios diferenciados, sin embargo Packeteer lo ha implementado en su sistema.

Para un flujo de tráfico que no exceda una tasa de datos configurada, la meta del planeamiento de límite de retardo es especificar un límite estricto en la variación del retardo de paquetes en un punto, por ejemplo el tráfico llega a una interfaz y es destinada por otra interfaz, lo esencial de la definición del planeamiento de límite de retardo es que la diferencia de tiempo cuando un paquete se podría haber liberado y cuando este es liberado nunca exceda un límite específico.

Dada un flujo de paquetes llegando a una interfaz sin exceder una tasa límite R, hay una secuencia de tiempo E(i) cuando estos paquetes con índice i se entregarían a la interfaz de salida en ausencia de tráfico simultáneo compitiendo, es decir E(i) son los tiempos más bajos en que los paquetes podrían ser liberados por el sistema, en presencia de tráfico simultáneo compitiendo, los paquetes serán retardados algún tiempo D(i), entonces el planeamiento de límite de retardo es definido como el comportamiento el cual asegura que para todos los paquetes con índices i, como se observa en la Ecuación 2.1.

$$D(i) - E(i) \leq S \bullet \left(\frac{MTU}{R} \right)$$

Ecuación. 2.1. Cálculo de planeamiento de límite de retardo.

Se calcula mediante la Unidad de Transmisión Máxima (MTU) o tamaño de paquete en la salida, R que es la tasa a la que llegan los paquetes y S que es un puntaje que indica una característica del equipo para encontrar el límite definido, S es una constante pequeña preferiblemente aunque depende del mecanismo de planeamiento y configuración del equipo.

PacketShaper calcula el planeamiento de límite de retardo más óptimo para tráfico UDP, sin embargo se puede variar este límite.

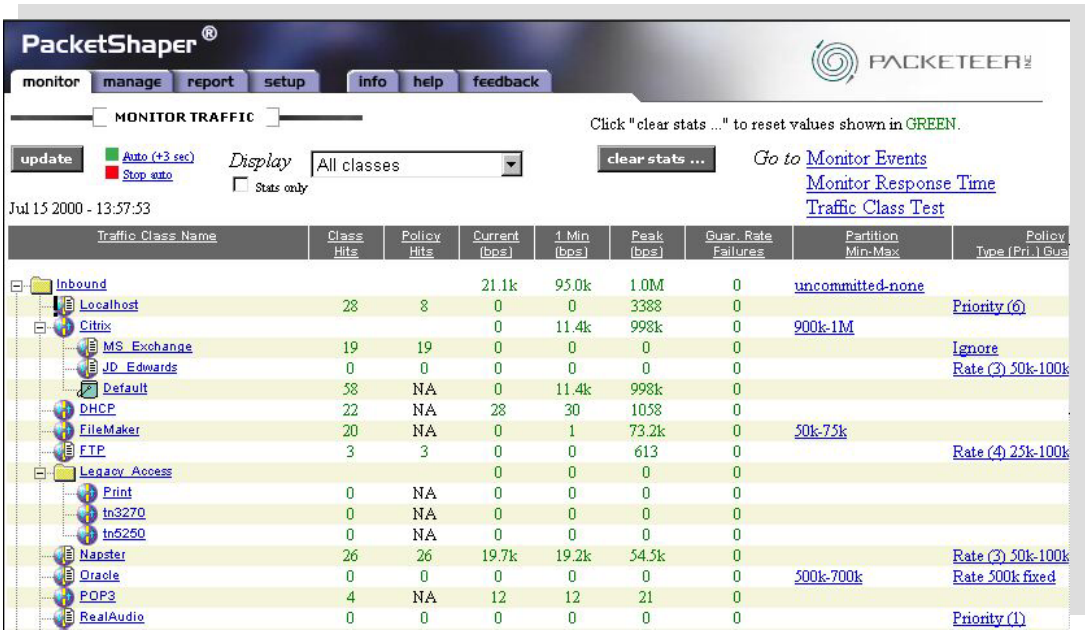
2.3.1.4.3 Otras tecnologías.

La tecnología auto tasa para TCP de Packeteer permite al PacketShaper detectar automáticamente la velocidad de conexión de un cliente o servidor en el otro lado de una conexión remota o en algún lugar del Internet, este mecanismo de detección de velocidad monitorea la velocidad del cliente mediante el acuerdo en tres fases de TCP y puede ajustar el manejo de ancho de banda según la velocidad de conexión la cual puede variar.

PacketShaper ofrece varias formas para resolver los problemas de desempeño de la red e implementar calidad de servicio; por medio de políticas que determinan como los flujos individuales de una clase son tratados; por medio de particiones en donde los flujos para una clase son tratados todos de la misma manera, se puede crear particiones dinámicas que permiten garantizar a cada usuario un mínimo y un máximo ancho de banda; por medio de políticas de prioridad puede asignar ancho de banda basado en una prioridad de 0 a 7 y además a cada prioridad asignar incremento explosivo de velocidad (bursty), así el tráfico con una mayor prioridad obtiene mayor ancho de banda, muy usado para aplicaciones que utilizan protocolo UDP; por medio de políticas de descarte que intencionalmente bloquean el tráfico y no informan de esto al usuario; por medio de políticas de nunca admitir que intencionalmente bloquean el tráfico pero informan de esto al usuario.

PacketShaper puede asignar a una clase una porción del ancho de banda y puede fijar tasas mínimas y máximas garantizando ancho de banda por conexión, en la Figura 2.22. se

observa los parámetros configurados en PacketShaper para algunas de las clases del enlace de entrada, implementando de esta manera calidad de servicio.



Traffic Class Name	Class Hits	Policy Hits	Current (bps)	1 Min (bps)	Peak (bps)	Guar. Rate Failures	Partition Min-Max	Policy Type (Pri.) Gua
Inbound			21.1k	95.0k	1.0M	0	uncommitted-none	
Localhost	28	8	0	0	3388	0		Priority (6)
Citrix			0	11.4k	998k	0	900k-1M	
MS_Exchange	19	19	0	0	0	0		Ignore
JD_Edwards	0	0	0	0	0	0		Rate (3) 50k-100k
Default	58	NA	0	11.4k	998k	0		
DHCP	22	NA	28	30	1058	0		
FileMaker	20	NA	0	1	73.2k	0	50k-75k	
FTP	3	3	0	0	613	0		Rate (4) 25k-100k
Legacy_Access			0	0	0	0		
Print	0	NA	0	0	0	0		
tn3270	0	NA	0	0	0	0		
tn5250	0	NA	0	0	0	0		
Napster	26	26	19.7k	19.2k	54.5k	0		Rate (3) 50k-100k
Oracle	0	0	0	0	0	0	500k-700k	Rate 500k fixed
POP3	4	NA	12	12	21	0		
RealAudio	0	0	0	0	0	0		Priority (1)

Figura. 2.22. Calidad de servicio mediante PacketShaper.

PacketShaper tal como un ruteador puede clasificar, marcar y remarcar tráfico basado en ambientes de Servicios Diferenciados (Diffserv), Clase de Servicio (CoS), Tipo de Servicio (ToS) y Conmutación por Etiquetas MultiProtocolo (MPLS), manipulando la información de encabezados de paquetes.

La Conmutación por Etiquetas MultiProtocolo (MPLS) es una alternativa para implementar redes que provean a portadores (carriers) de Redes Privadas Virtuales (VPN), calidad de servicio y permita implementar ingeniería de tráfico. Un dominio de conmutación por etiquetas multiprotocolo se crea mediante ruteadores extremos y switches internos, de manera similar a un dominio de servicios diferenciados, cuando los paquetes IP ingresan al dominio son convertidos a paquetes con etiquetas multiprotocolo por ruteadores extremos, estos paquetes son transportados por switches internos dentro del dominio basándose en técnicas de ruteo y conmutación mediante los paquetes con etiquetas multiprotocolo, trabaja a nivel de capa de enlace lo que lo hace más eficiente, ya que no

tiene problemas de direccionamiento. Cuando los paquetes multiprotocolo salen del dominio, son convertidos a paquetes IP por los ruteadores extremos, ver Anexo 4.

Dichas funciones de PacketShaper permiten al tráfico tener un tratamiento uniforme extremo a extremo en caso de tener otros elementos de red que puedan realizar otras funciones en la red.

PacketShaper no es un elemento de seguridad (firewall) pero ayuda a la detección de virus, gusanos y ataques mediante Rechazo de Servicio (DoS) en la red, emplea una variedad de métodos, puede limitar el número de conexiones desde algún computador, puede limitar la cantidad de tráfico del Protocolo de Mensajes de Control (ICMP), puede limitar el número de flujos de una aplicación o clase de tráfico y puede bloquear tráfico de fuentes no confiables.

PacketShaper permite autenticación en servidor de Servicio de Autenticación Remota de Llamada de Usuario (RADIUS) actuando como cliente de este servidor. Puede realizar un control de admisión que decide como manejar sesiones adicionales cuando ocurre una falta de recursos de ancho de banda, el control de admisión lo hace negando acceso, ajustando a otro usuario o redireccionando peticiones a páginas web. Es administrable vía plataformas que utilizan el Protocolo de Administración de Red Simple (SNMP) mediante archivos de Base de Información de Manejo (MIB).

2.3.2 NetEnforcer.

NetEnforcer es fabricado por Allot, posee varios modelos de sistemas, la elección del modelo tiene que ver con la capacidad del enlace de Red Área Amplia (WAN), su ubicación básica en la red es entre el ruteador de la red de área amplia y el switch ó hub de la Red de Área Local (LAN). Los modelos estándares que administran hasta 10 Mbps son utilizados a nivel de una organización, los modelos avanzados que administran desde 45 Mbps hasta 100 Mbps y los siguientes modelos de alta disponibilidad que administran desde 155 Mbps hasta 1 Gbps son utilizados a nivel de Proveedores de Servicio de Internet (ISP), los modelos se describen en la en la Tabla 2.4.

Modelo	Ancho de Banda	Tubos	Canales virtuales (VCs)	Conexiones	Interfaz de conexiòn
AC-101/128	128 Kbps	64	1024	1000	10 ó 100 Mbps full duplex auto detección.
AC-101/512	512 Kbps	128	1024	1000	10 ó 100 Mbps full duplex auto detección.
AC-201/2M	2 Mbps	256	2048	12000	10 ó 100 Mbps full duplex auto detección.
AC-201/10M	10 Mbps	256	2048	12000	10 ó 100 Mbps full duplex auto detección.
AC-302	45 Mbps	1024	4096	64000	10 ó 100 Mbps full duplex auto detección.
AC-601/SP	100 Mbps	4096	28000	256000	10 ó 100 Mbps full duplex auto detección.
AC-701/SP-F	155 Mbps	4096	28000	256000	1 Gbps (Fibra) full duplex.
AC-802/SP	310 Mbps	4096	28000	256000	10 ó 100 Mbps ó 1 Gbps (Fibra) full duplex auto detección.
AC-1010/SP-622M-PS-I-IT	622 Mbps	10000	80000	500000	10 ó 100 Mbps ó 1 Gbps (Fibra) full duplex auto detección.
AC-1010/SP-1G-PS-I-IT	1 Gbps	10000	80000	500000	10 ó 100 Mbps ó 1 Gbps (Fibra) full duplex auto detección.

Tabla. 2.4. Modelos de NetEnforcer.

Todos los modelos de NetEnforcer son montables en un rack de 19 pulgadas, poseen un puerto ethernet del enlace entrante (Inbound), un puerto ethernet del enlace saliente (Outbound), un puerto serial para configuración por consola. Además los modelos avanzados y de alta disponibilidad poseen un puerto ethernet para administración fuera de banda, los modelos de alta disponibilidad incluyen un módulo llamado Derivación de Fibra ó Cobre para interconectar dos NetEnforcer y obtener una plataforma de alta disponibilidad, en la Figura 2.23. se observa la caja del NetEnforcer.

Figura. 2.23. Caja del NetEnforcer.

Allot mejora al sistema NetEnforcer con módulos de software, el módulo NetBalancer que mejora a NetEnforcer dándole características tales como balanceo de carga de servidor, traducción de direcciones de red IP, traducción de puertos TCP y capacidades de respaldo de servidor; el módulo NetAccountant permite generar reportes basados en plantillas, además le da herramientas de reporte; el módulo CacheEnforcer mejora al sistema NetEnforcer ya que permite definir políticas de caché (mecanismo para incrementar velocidad), reforzadas y optimizadas de acuerdo a una información de tráfico específico tales como direcciones de red, protocolos, servicios, aplicaciones y hora del día; el módulo CacheEnforcer trabaja en conjunto con un sistema adicional llamado NetPure que posee características de filtraje de Internet.

Posee una tecnología de derivación (bypass) que consiste en que el equipo se comporta como un elemento pasivo que pasa el tráfico a través de sus interfaces, cuando se producen fallas o cuando el equipo está apagado.

Antes de conectarlo a la red se debe hacer una configuración inicial mediante cable de consola y aplicaciones de emulación de terminal como Hyperterminal de Windows, para fijar parámetros tales como claves de acceso, dirección IP, máscara de red, nombre de dominio, puerta de enlace por defecto, Servidores de Nombres de Dominio (DNS) primario y secundario. También se configura las interfaces, las ethernet en donde se señala parámetros como velocidad 10 ó 100 Mbps, tipo de comunicación bidireccional half ó full duplex, a la interfaz que maneja el acceso de red de área amplia se le debe indicar el ancho de banda, por ejemplo 2.048 Mbps (E1). Si es un enlace full duplex se debe indicar separadamente los anchos de banda de los enlaces entrante (Inbound) y saliente (Outbound), una vez conectado a la red NetEnforcer es configurable vía navegador web mediante su dirección IP. Sin embargo configuraciones avanzadas pueden requerir el uso

de línea de comandos mediante el Protocolo de Emulación de Terminal (TELNET) ó Hyperterminal.

2.3.2.1 Topologías de red.

Con NetEnforcer se puede implementar topologías básicas para implementar calidad de servicio, debido a que no se puede instalar módulos de expansión adicionales en el sistema NetEnforcer, funcionalidad que si posee PacketShaper, las topologías básicas que se puede realizar son similares a las mencionadas con PacketShaper, 2.3.1.1 Topologías de red.

2.3.2.1.1 Administrando el sitio principal.

En la topología que se observa en la Figura 2.24. NetEnforcer mediante su característica de tubo de tráfico, habilita administración de la red para manejar el tráfico de tres enlaces de Red de Área Amplia (WAN) diferentes y crear tres tubos de tráfico para cada uno de ellos.

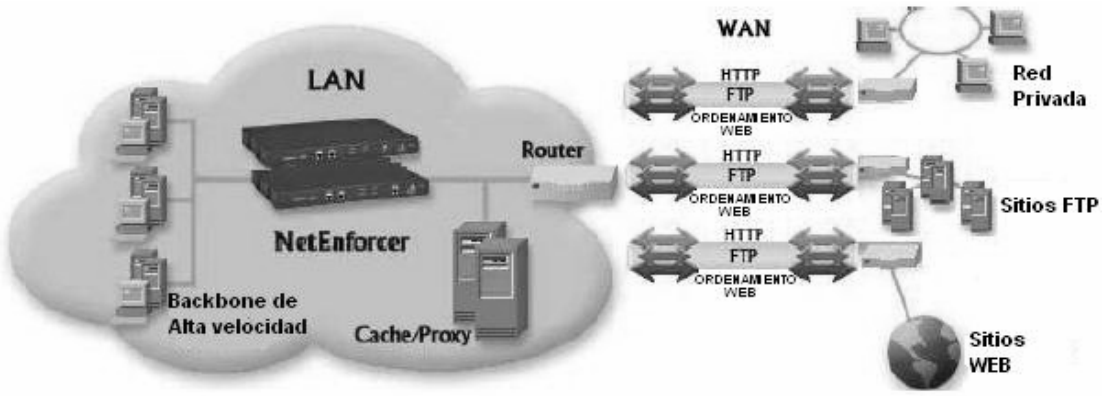


Figura. 2.24. NetEnforcer administrando el sitio principal.

Por ejemplo mediante administración de la red se podría crear un tubo para el enlace WAN 1 limitado a 2 Mbps con aplicaciones de negocios y tráfico multimedia clasificado mediante los bits de Tipo de Servicio (ToS). Además se podría limitar los dos enlaces

WAN restantes 2 y 3 a 2 Mbps cada uno, todo el tráfico a los enlaces es clasificado por la dirección IP de destino.

2.3.2.1.2 Administrando el enlace de Internet del sitio principal.

La topología de red más común donde NetEnforcer administra un enlace de Internet se observa en la Figura 2.25., en esta topología las direcciones IP de los usuarios de la Red de Área Local (LAN) son asignadas dinámicamente por un servidor de Protocolo de Configuración de Máquina Dinámico (DHCP), tiene un servidor Proxy para la salida de los usuarios a Internet, este servidor proxy traduce cada dirección IP de cada usuario de la LAN a una sola dirección IP la que servirá como entrada al Internet y NetEnforcer implementa calidad de servicio para el enlace de Internet y opcionalmente puede implementar filtrado de Internet por usuarios, los nombres de los usuarios son asignados por un Servidor de Nombre de Dominio (DNS) en la LAN.

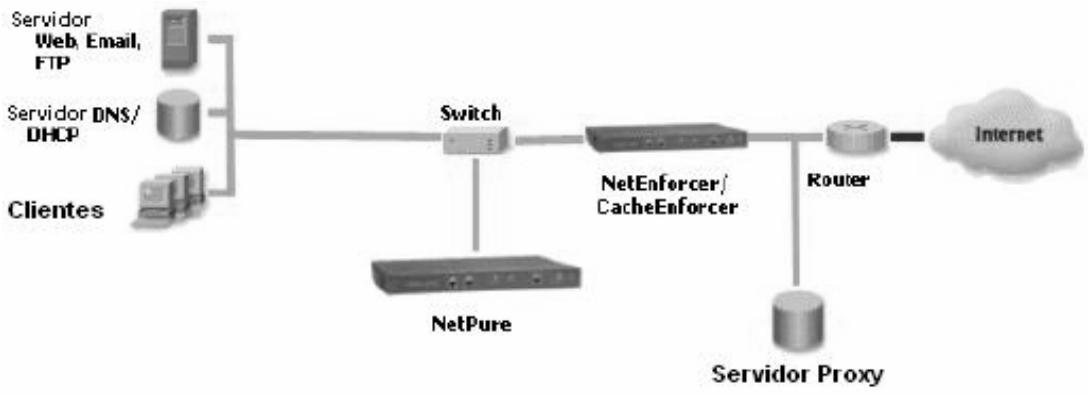


Figura. 2.25. NetEnforcer administrando un enlace de Internet.

NetEnforcer en conjunto con el módulo de software CacheEnforcer (redirección de caché) y en conjunto con el sistema NetPure (filtro de Internet) son colocados en la mismo segmento de la LAN, frente al ruteador conectado al Internet. En esta posición puede redireccionar todo el tráfico del Protocolo de Transferencia de Hipertexto (HTTP) usado para la navegación en Internet que va al servidor Proxy hacia NetPure que filtra el contenido de Internet.

NetEnforcer se encarga de implementar calidad de servicio incluyendo políticas de administración de ancho de banda, tales como tráfico de correo electrónico y navegación en Internet basándose en los clientes (usuarios) del Servidor de Nombre de Dominio.

2.3.2.1.3 Administrando el sitio principal y los sitios remotos.

Este tipo de topología se observa en la Figura 2.26., se utiliza para implementar calidad de servicio en redes corporativas propias las cuales transportan información de negocios entre los empleados de la empresa. Tiempos de respuesta pobres de la red son causadas por la mezcla de todo tipo de tráfico dentro del enlace de Red de Área Amplia (WAN) se traducen rápidamente en un decremento de la producción, pérdida de la ganancia e incremento de costos. El tráfico que se mezcla sobre la red son del tipo críticos como aplicaciones de negocios basadas en la red, e-mail, Internet, conferencia de video sensitivo al tiempo, voz sobre IP (VoIP), etc., todas estas aplicaciones mezcladas sobre el enlace WAN disminuyen el desempeño de la red e incrementa las demandas de tráfico que cursan la red.

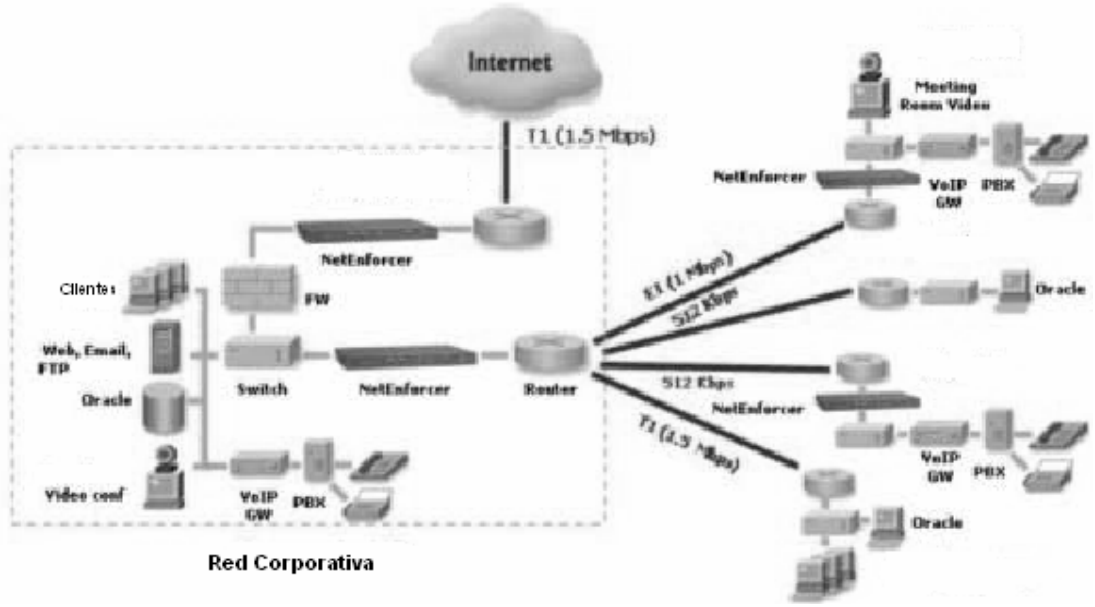


Figura. 2.26. NetEnforcer administrando el sitio principal y los sitios remotos.

NetEnforcer en esta topología puede asegurar un buen tiempo de respuesta para las aplicaciones críticas o de negocios, priorizando su tráfico y garantizando al mismo una porción del ancho de banda del enlace WAN, al mismo tiempo el tráfico menos crítico y menos sensitivo al tiempo de respuesta del enlace WAN pueden recibir un ancho de banda bajo limitado o una prioridad baja, NetEnforcer garantiza el desempeño de las aplicaciones críticas agrupándolas y definiendo políticas para cada grupo.

NetEnforcer en esta topología controla los recursos de la red importantes tales como ancho de banda del enlace WAN, servidores, aplicaciones y usuarios, también monitorea y registra información del uso de tráfico basado en clientes, servidores, aplicaciones, tiempo y bits de tipo de servicio.

2.3.2.1.4 Topologías con configuraciones redundantes.

La falla de un equipo administrador de ancho de banda dentro de la red puede ser catastrófico, causando que la red esté sin funcionamiento por largo tiempo lo que a la final se traduce en pérdidas de datos y pérdidas económicas para una organización, es por esto que NetEnforcer puede operar en paralelo o en configuración redundante.

La configuración redundante de los modelos para una organización y avanzados de NetEnforcer se la puede implementar con un cable de redundancia que conecta a dos sistemas mediante su puerto de respaldo (Backup), en este caso cada extremo del cable define la función de cada NetEnforcer, así uno de los NetEnforcer será el primario y el otro será el secundario como se observa en la Figura 2.27.

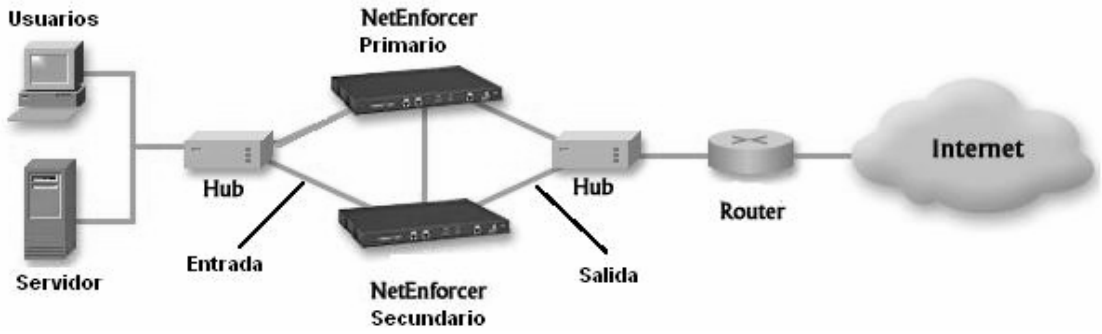


Figura. 2.27. NetEnforcer para organización y avanzado colocado en configuración redundante.

Solamente a los modelos NetEnforcer de alta disponibilidad es necesario adicionar un módulo de hardware adicional de derivación (bypass) que interconecta de forma segura a los NetEnforcer y garantiza una configuración redundante (Hot Standby) eficiente, este módulo conectado a un NetEnforcer e indicando sus otras conexiones se observa en la Figura 2.28., posee cuatro puertos ethernet, uno de enlace de entrada hacia un switch, otro de enlace de salida hacia un ruteador y dos de enlace de entrada y de salida que se conectan al NetEnforcer primario, además posee dos puertos de backup, uno primario y otro secundario que cada uno se conecta a un NetEnforcer primario y secundario respectivamente. Este módulo de derivación puede tener también la opción para conexión a fibra óptica.

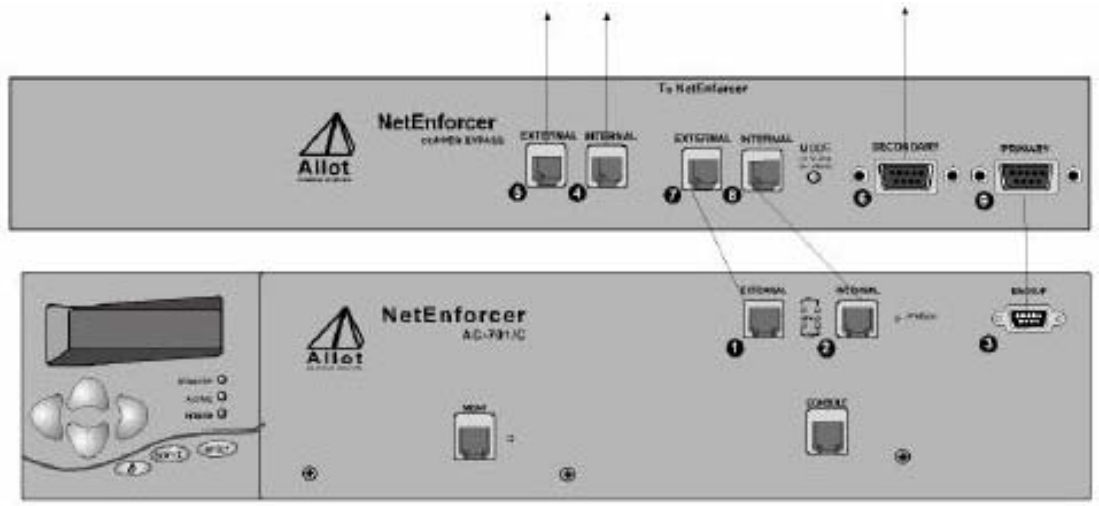


Figura. 2.28. NetEnforcer de alta disponibilidad colocado en configuración redundante.

El tráfico pasa a través del módulo de derivación hacia el NetEnforcer primario el cual se encuentra activo y el NetEnforcer secundario o de respaldo permanece inactivo solamente enviando información de estatus hacia el módulo de derivación. Cuando el NetEnforcer primario falla el NetEnforcer secundario entra a funcionar tomando todas las responsabilidades del NetEnforcer primario.

Como NetEnforcer es un elemento para unir redes (bridge), permite implementar una topología redundante adicional como se observa en la Figura 2.29., trabaja con el protocolo conocido como Arbol de Extensión (Spanning Tree) donde el NetEnforcer primario se encuentra activo y el NetEnforcer secundario o de respaldo permanece inactivo solamente enviando información de estatus hacia el NetEnforcer primario. Cuando el NetEnforcer primario falla el NetEnforcer secundario entra a funcionar tomando todas las responsabilidades del NetEnforcer.

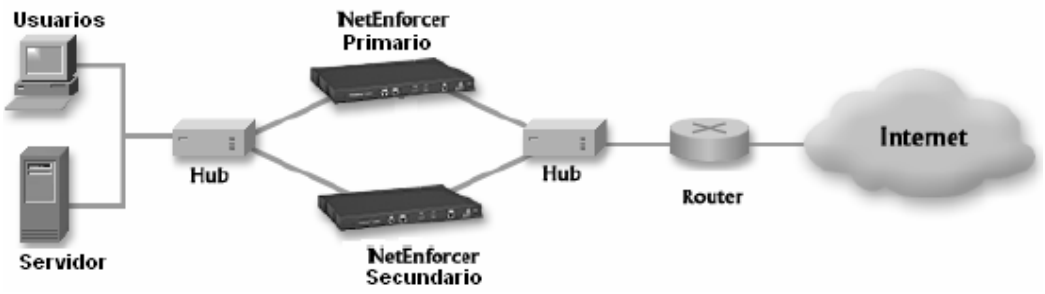


Figura 2.29. Configuración Hot Standby adicional de NetEnforcer.

Solo los modelos de alta disponibilidad tienen la opción de fuente de alimentación dentro de un mismo equipo.

NetEnforcer se basa en cuatro puntos básicos que son monitoreo, clasificación, reforzamiento y reporte.

2.3.2.2 Monitoreo y reporte.

El software NetWizard descubre y monitorea los protocolos y tráfico de capa 7 ó aplicaciones, así como el ancho de banda que usan en tiempo real, descubre software par a par (P2P) como KaZaA y otros, los cuales impactan negativamente en el rendimiento de la red, además soporta más de 200 protocolos diferentes, el usuario también puede definir sus propios protocolos, entre los tipos más importantes de tráfico que descubre se encuentran:

- América On Line (AOL), Apple, Citrix, bases de datos Oracle.
- Mensajería instantánea y chat.
- Protocolo de Transferencia de archivos (FTP).
- Protocolo de Transferencia de HiperTexto (HTTP).
- Correo.
- Pila de protocolos TCP/IP.
- Multimedia.
- Voz sobre IP

NetEnforcer identifica patrones de tráfico en la red durante horas pico, una vez que ha clasificado el tráfico, se puede asignar calidad de servicio a cada clasificación, esto se hace por políticas que son construidas y definidas sobre el tiempo y pueden adaptarse continuamente para encontrar los requerimientos de la red.

El procedimiento que utiliza el software NetWizard es preguntar un intervalo tiempo de monitoreo del tráfico, tiempo en el que recolecta información que le ayudan a diagnosticar que tipo de tráfico existe, lo hace de un tubo (pipe) cuyo tráfico se va a monitorear, en un inicio se selecciona un tubo por defecto (fallback) ya que no se tiene creado ninguno.

Una vez que se tiene un tubo para monitorear, se obtiene gráficos como se observa en la Figura 2.30., en las barras azules se observa el tiempo de monitoreo recorrido y el tiempo para recibir una nueva muestra de tráfico, la barra roja indica el porcentaje de la capacidad total del ancho de banda usada por el tráfico entrante (Inbound) acumulativo.

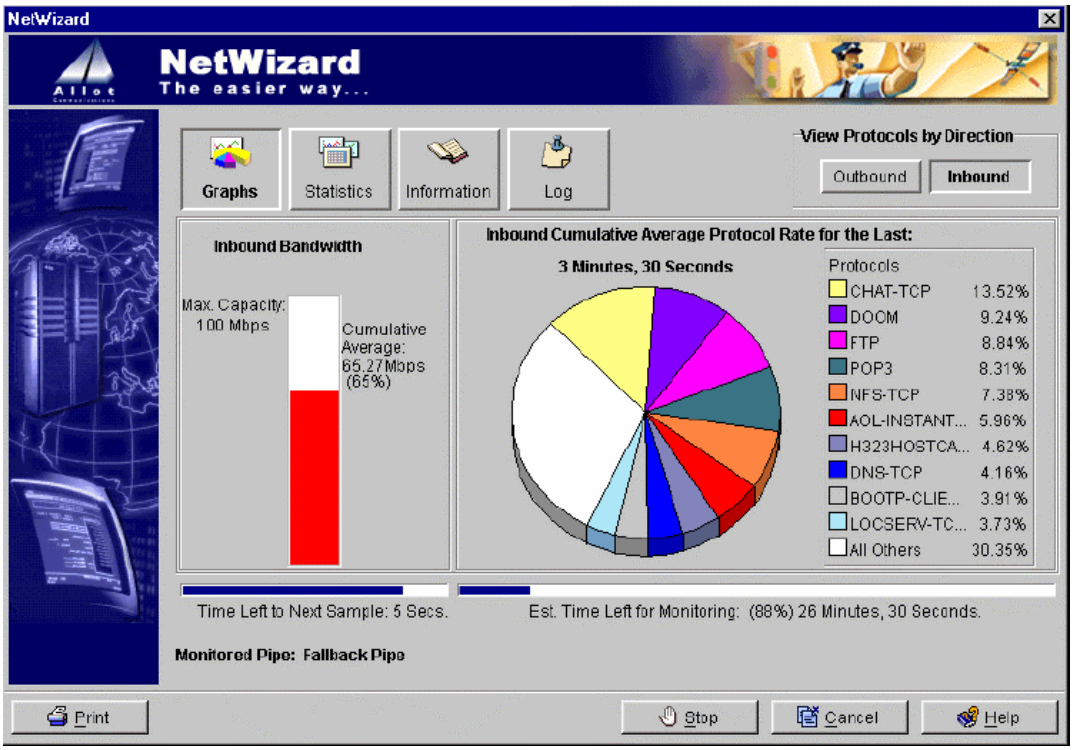


Figura. 2.30. Gráficos de monitoreo de NetEnforcer.

La siguiente ficha “Statics” que se observa en la Figura 2.30., muestra las estadísticas de uso de los protocolos monitoreados como se muestra en la Figura 2.31., estas estadísticas son nombre de protocolo, porcentaje relativo de uso, tasa, porcentaje del ancho de banda total disponible para el tubo usado por el protocolo, la máxima cantidad de ancho de banda usado durante esta sesión, el promedio de ancho de banda usado durante la sesión de

monitoreo para todos los protocolos, la máxima cantidad de ancho de banda disponible, los protocolos más activos se ordenan desde la parte superior.

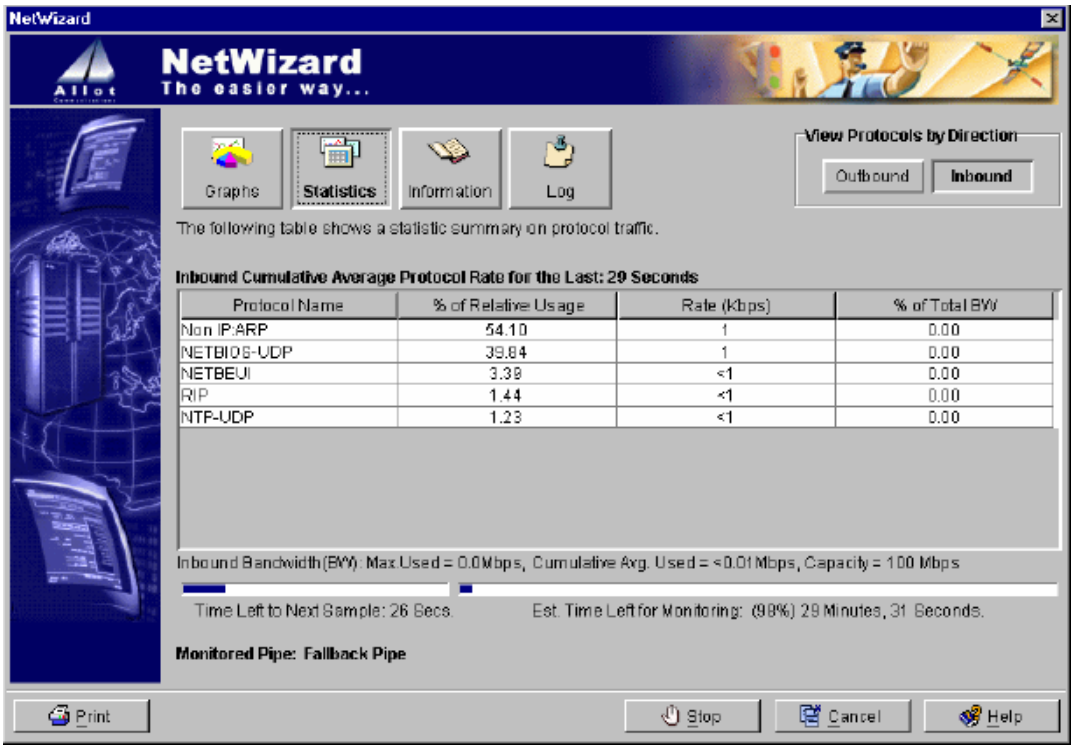


Figura. 2.31. Estadísticas de monitoreo de Allot.

En la ficha “Information” que se observa en la Figura. 2.30., se obtiene datos sobre la sesión de monitoreo como tiempos de inicio y fin, intervalos de muestreo del tráfico, muestras recogidas durante una sesión, tiempo transcurrido y restante.

En la ficha “Log” que se observa en la Figura. 2.30., se obtiene registro de información de eventos durante la sesión de monitoreo que pueden ser usados para corregir problemas en el sistema.

El software Netwizard puede obtener reportes gráficos por períodos de muestreo promedio o por rangos de tiempo definidos por el usuario, tiene diferentes tipos de gráficos como barras, pastel, área y línea. Los reportes gráficos incluyen ancho de banda del enlace de entrada y/o salida, ancho de banda promedio consumido, distribución de tubos,

distribución de canales virtuales, tubos más activos, canales virtuales más activos, clientes más activos, servidores más activos, distribución de protocolos, utilización del enlace, paquetes descartados, conexiones, en la Figura 2.32 se observa los paquetes descartados en un rango de tiempo del día.

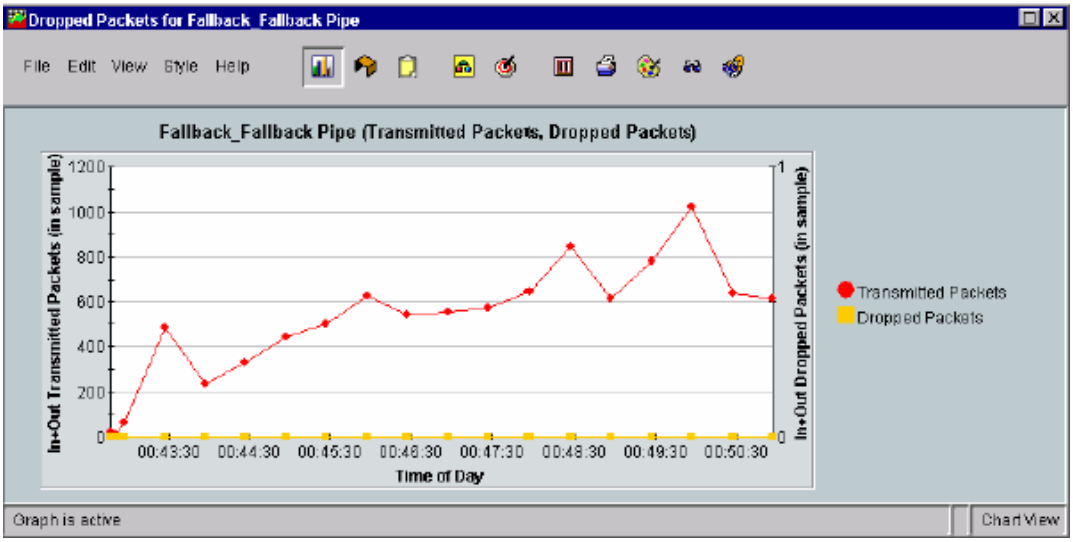


Figura. 2.32. Reporte gráfico de paquetes descartados en un rango de tiempo.

Adicionalmente la herramienta de monitoreo de NetEnforcer llamada NetHistory provee datos de hasta 24 horas previas con muestras desde uno a diez minutos, siendo útil para monitorear la red sobre un período más largo de tiempo.

NetEnforcer además posee otras características especiales como administración mediante el Protocolo de Administración de Red Simple (SNMP), que permite desde cualquier lugar de la red descubrir al sistema, monitorearlo, observar eventos generados y enviar mensajes (traps) o información a cierto lugar de la red como por ejemplo al administrador.

2.3.2.3 Clasificación.

La clasificación se logra con el uso de tubos y canales virtuales, un tubo y un canal virtual son definidos por una o más reglas y un conjunto de acciones. Un tubo incluye uno

o más canales virtuales y permiten manejar el ancho de banda total de forma que cada tubo se trate como un enlace independiente. Existen tubos y canales virtuales por defecto (fallback) cuyas reglas no pueden ser eliminadas o modificadas, en un inicio como no se crean tubos y canales el tráfico entra dentro de este tubo. Una conexión entrante corresponde a un tubo, según como las características de la conexión correspondan a las reglas del tubo, luego la conexión corresponde a las reglas de un canal virtual dentro del tubo.

Las acciones definidas para un tubo afectan a todos los canales virtuales dentro del tubo, así las acciones definidas para un canal virtual son reforzadas junto con las acciones del tubo. Una regla es un conjunto de seis condiciones y se definen a nivel de tubo o canal virtual y son:

- *Fuente de conexión.*- Define la fuente del tráfico. Por ejemplo, una dirección de Control de Acceso al Medio (MAC) ó IP específica, un rango de direcciones IP, direcciones de una subred IP, o nombres de computadores. El valor por defecto es para cubrir el tráfico desde cualquier fuente.

- *Destino de la conexión.*- Define el destino del tráfico. Por ejemplo, una dirección Control de Acceso al Medio (MAC) ó IP específica, un rango de direcciones IP, direcciones de una subred IP, o nombres de computadores. El valor por defecto es para cubrir el tráfico a cualquier destino.

- *Servicio.*- Define los protocolos relevantes a una conexión. Los protocolos pueden ser TCP/IP, UDP los cuales se pueden definir por puertos, además los protocolos no TCP, UDP ó IP. El Protocolo de Transferencia de HiperTexto (HTTP) puede definirse por directorios web, páginas ó Localizador de Recurso Uniforme (URL) específico. El valor por defecto es para cubrir todos lo protocolos.

- *Tipo de Servicio (ToS).*- Define los bits de precedencia contenidos en el encabezado IP del tráfico. El valor por defecto es para cubrir cualquier valor de tipo de servicio.

- *Red de Área Local Virtual (VLAN).*- Define los bits de red de área local virtual contenido en el encabezado IP del tráfico. El valor por defecto es el que cubre cualquier valor de red de área local virtual.

- *Tiempo.*- Define el período de tiempo durante el cual el tráfico se recibe. Por ejemplo diariamente entre 8 AM y 6 PM. El valor por defecto es para cubrir el tráfico todo el tiempo.

Cuando se crea un tubo ó canal virtual nuevo, posee las reglas por defecto y se modifican de acuerdo a los requerimientos del usuario.

2.3.2.4 Reforzamiento.

2.3.2.4.1 Encolamiento Por Flujo (PFQ).

NetEnforcer utiliza una aproximación del encolamiento por flujo que es un algoritmo para suministrar calidad de servicio tras la priorización de datos en el enlace de salida, así cada flujo de conexión nuevo obtiene su propia cola, esta nueva cola puede ser tratada de la misma forma que otras que tengan su misma política de prioridad. De esta forma se obtiene varias colas las cuales se clasifican en grupos de colas, cada grupo con una diferente prioridad.

2.3.2.4.2 Control de flujo de las colas.

NetEnforcer para realizar el control de flujo de las colas (creadas por el encolamiento por flujo), desarrolla una combinación de Encolamiento Justo Pesado (WFQ) y Encolamiento Justo Pesado Basado en Clases (CBWFQ), esta combinación de encolamientos se basa en las políticas de definidas por el usuario para enviar el tráfico. El encolamiento basado en clases le permite a NetEnforcer usar una aproximación jerárquica, donde subclases de tráfico pueden ser priorizadas independientemente dentro de una clase, mientras las diferentes clases de tráfico mantienen prioridades entre ellas.

2.3.2.4.3 Asignación de ancho de banda y retardo.

NetEnforcer realiza la asignación de ancho de banda de los flujos, mediante el algoritmo Flujo Balde-Ficha (TBF) mencionado en el apartado 2.2.1.2., realiza la asignación de retardos mediante un planeamiento de límite de retardo similar al de PacketShaper mencionado en el apartado 2.3.1.4.2.

2.3.2.4.4 Otras tecnologías.

NetEnforcer define la calidad de servicio como una acción aplicada a una conexión cuando cumple las reglas de un tubo ó canal virtual, la calidad de servicio aplicada incluye los siguientes métodos:

- *Ancho de banda priorizado.*- Libera niveles de servicio basado en el nivel de importancia y demanda de tráfico de una conexión con respecto a otras conexiones. Durante períodos de tráfico pico, NetEnforcer bajará la tasa de las aplicaciones de prioridad baja, dando como resultado el incremento de ancho de banda para aplicaciones con una prioridad más alta.

- *Ancho de banda garantizado.*- Habilita la asignación de cantidades de ancho de banda mínimo y máximo para tubos específicos, canales virtuales y conexiones. Cuando existe ancho de banda disponible las conexiones se apropian de este exceso, permitiendo el incremento explosivo de la velocidad (bursty) de las conexiones hasta el ancho de banda máximo. Las tasas garantizadas también permiten asegurar una predecible calidad de servicio para aplicaciones sensitivas a retardos, durante períodos de tráfico pico y no pico.

- *Ancho de banda reservado en demanda.*- Habilita la reservación de ancho de banda mínimo en el primer byte de una conexión hasta que la conexión es concluida, esto es muy útil cuando existe un cuello de botella en un enlace y este no es gobernado por NetEnforcer, limitando otras conexiones no garantizadas, NetEnforcer reserva suficiente ancho de banda requerido por el tubo o canal virtual.

- *Marcado de Tipo de Servicio (ToS).*- Habilita el marcado de conexiones admitidas independientemente de la regla del canal virtual. El perfil de tráfico de salida puede ser marcado con un valor diferente que el perfil de entrada para cada conexión.

- *Control de acceso.*- Determina si una conexión es aceptada, descartada o rechazada. Por ejemplo se puede especificar un tubo que acepte 100 conexiones del Protocolo de Mensajes de Control (ICMP) a un servidor y el resto las descarte. Se puede instruir a NetEnforcer para que acepte conexiones nuevas con una prioridad baja.

- *Control de admisión.*- Determina el ancho de banda asignado a un flujo basado en la demanda y el estado del sistema dependiendo del ancho de banda disponible, por ejemplo asigna un mínimo de 10 Kbps a un flujo.

NetEnforcer usa el software NetWizard para definir las políticas de calidad de servicio como se observa en la Figura 2.33., en base al monitoreo de un tubo, aquí se puede ver tasa y porcentaje de utilización de cada protocolo y se puede especificar a cada protocolo, un ancho de banda mínimo y/o máximo, así como especificar una prioridad alta, media o baja, se selecciona la casilla de la izquierda para habilitar las políticas de calidad de servicio que se haya creado y se guarda los cambios.

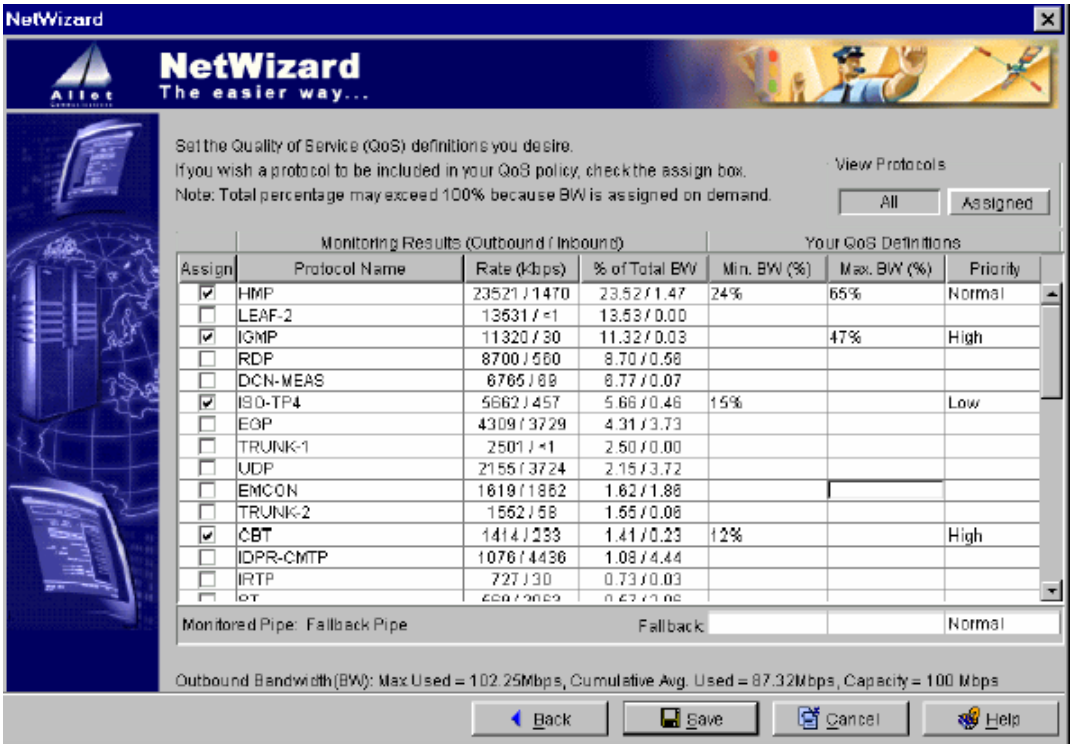


Figura. 2.33. Definiendo políticas de calidad de servicio en NetEnforcer.

NetEnforcer permite autenticación en servidor de Servicio de Autenticación Remota de Llamada de Usuario (RADIUS) actuando como cliente de este servidor. Soporta Redes de Área Local Virtuales (VLAN) que se habilita cuando se determina que NetEnforcer es manejado a través de tráfico etiquetado como una red virtual específica. Permite guardar su configuración en servidores de la red para en caso de falla restaurar su configuración desde estos servidores.

Existen otros sistemas administradores de ancho de banda que son similares a los sistemas más importantes y conocidos, estudiados en los puntos 2.3.1 PacketShaper. y 2.3.2 NetEnforcer. Se mencionará brevemente el tercer sistema administrador de ancho de banda según la clasificación de IDC mencionada en el punto 2.3 SISTEMAS ADMINISTRADORES DE ANCHO DE BANDA DEDICADOS, este es Accelerator fabricado por Expand Networks.

2.3.3 Accelerator.

Se divide en tres modelos y son Accelerator 1800/2800/4800. El modelo 1800 soporta un enlace de Red de Area Amplia (WAN) de hasta 256 Kbps y 20 conexiones a otro Accelerator, el modelo 2800 soporta hasta 512 Mbps y 50 conexiones a otro Accelerator, el modelo 4800 soporta hasta 6 Mbps y 50 conexiones a otro Accelerator, el modelo 6800 soporta hasta 45 Mbps (cobre o fibra) y 350 conexiones a otro Accelerator.

Accelerator es montable en un rack de 19 pulgadas, posee dos puertos ethernet 10/100 Mbps para conexión a la red, un puerto ethernet 10/100 Mbps para gestión fuera de banda, un puerto para configuración por consola, un puerto auxiliar para conexión a un módem externo, una memoria borrable y un interruptor para habilitar/deshabilitar la tecnología de derivación (bypass) desde línea de comandos (consola), esta tecnología de derivación permite a Accelerator en caso de fallas actuar como un elemento pasivo pasando el tráfico, en la Figura 2.34. se observa la caja de Accelerator.

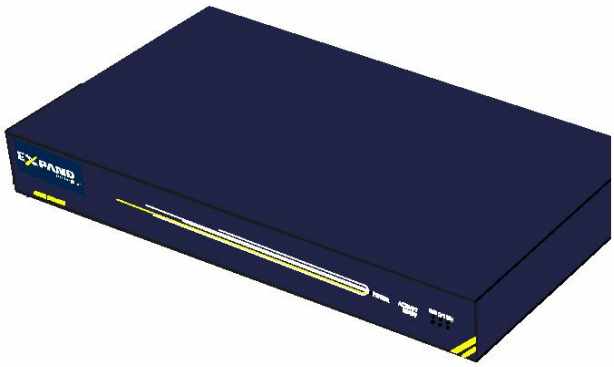


Figura. 2.34. Caja del Accelerator.

De forma similar a los dos administradores de ancho de banda estudiados anteriormente, Accelerator requiere una configuración inicial básica, luego de la cual, se puede acceder a Accelerator vía interfaz Web, una sesión de Protocolo de Emulación de Terminal (TELNET) o por Protocolo de Administración de Red Simple (SNMP)

La filosofía principal de este administrador de ancho de banda es acelerar (comprimir) el enlace WAN, por lo que la principal topología en la que debe ser colocado es administrando cada enlace WAN, conectado al switch de la Red de Area Local (LAN) y el ruteador de la WAN, como se observa en la Figura 2.35., en esta topología Accelerator incorpora la tecnología de derivación (bypass), adicionalmente le permite aplicar la optimización y calidad de servicio al tráfico antes de que el mismo alcance el ruteador.

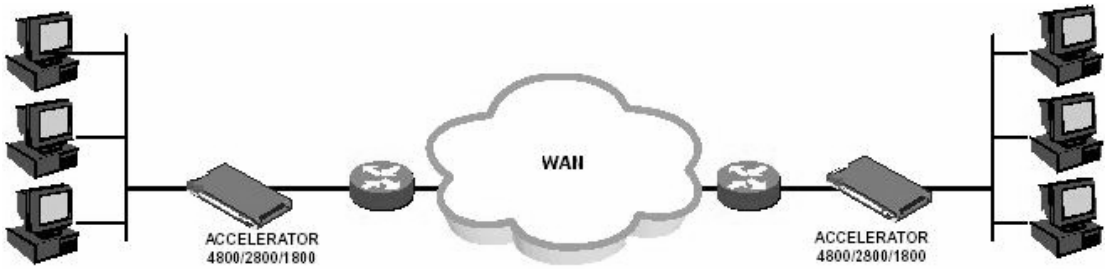


Figura. 2.35. Accelerator conectado al ruteador del enlace WAN.

Accelerator puede ser colocado directamente en la conexión LAN de la misma forma que un computador como se observa en la Figura. 2.36., en esta topología actúa como el siguiente salto para todo el tráfico que sale desde la LAN aplicando la optimización y calidad de servicio al tráfico, posteriormente los datos acelerados son direccionados hacia el Accelerator remoto (colocado en la LAN o colocado junto al ruteador), el cual reconstruye los datos y envía el tráfico hacia su destino final. Cuando Accelerator es colocado en la LAN puede trabajar con el Protocolo de Protección de Enrutamiento (HSRP) o el Protocolo de Redundancia de Ruteador Virtual (VRRP) que permite a Accelerator tener un respaldo de un ruteador, switch capa 3 u otro Accelerator colocado en la LAN, en caso de que falle su funcionamiento.

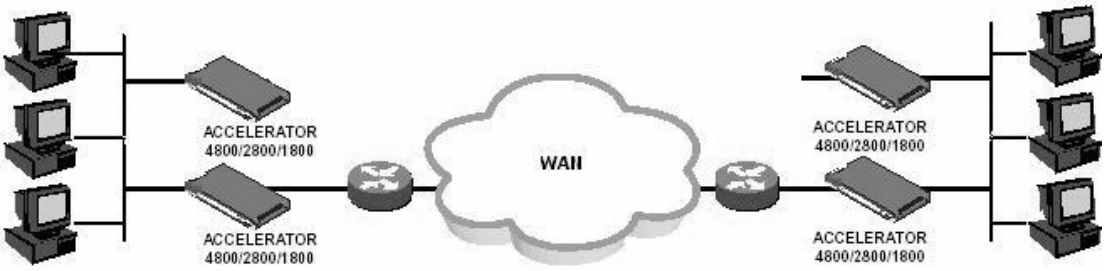


Figura. 2.36. Accelerator conectado dentro la LAN.

Según el modelo, cada Accelerator acepta hasta un número determinado de conexiones hacia otros Accelerators en una topología de estrella, ya sea total o parcial. Cabe mencionar que un Accelerator podría monitorear y controlar su enlace WAN sin la presencia de un Accelerator remoto, esto implica la implementación solamente de calidad de servicio y no de aceleración.

Accelerator puede ser colocado también en una topología de red de enlace privado, esta topología no es muy utilizada, se observa en la Figura 2.37., en esta topología Accelerator se conecta a través de interfaces seriales a elementos de la red externa como módems (línea dedicada) y ruteadores, los datos son pasados desde el ruteador hacia Accelerator, que usa una tecnología de caché para acelerar los datos hacia el otro Accelerator, el cual pasa los datos hacia el ruteador que finalmente se encarga de enviar los datos a su destino final.

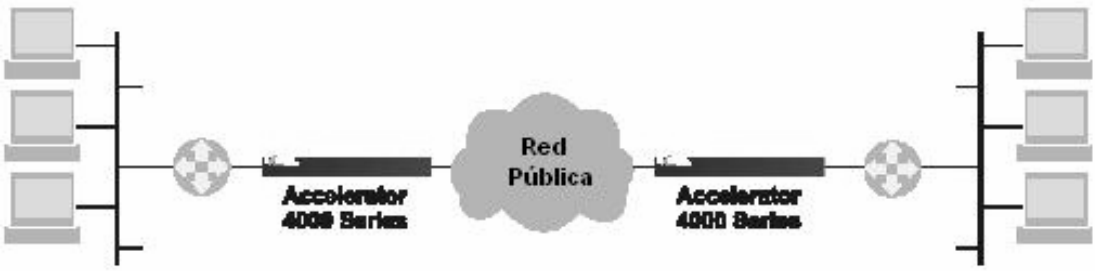


Figura. 2.37. Accelerator conectado a la red externa.

En la topología con un Accelerator en cada extremo de la red, la interfaz Web de Accelerator permite monitorear el tráfico, pudiendo definirse filtros como tráfico descubierto por defecto, aplicaciones definidas o todas. Existe una lista clasificada por las

aplicaciones reconocidas y una lista clasificada por el número de puerto del Protocolo de Control de Transmisión (TCP) de las aplicaciones no conocidas. Se presenta los detalles del tráfico de salida (Outbound), como nombre de la aplicación, uso de ancho de banda, prioridad, aceleración.

Se puede agregar nuevas aplicaciones, especificando un criterio de clasificación y/o política de calidad de servicio, como puerto TCP, puerto del Protocolo de Datagrama de Usuario (UDP), preserva o cambio de bits de Tipo de Servicio (ToS), su prioridad, ancho de banda mínimo y máximo.

De forma similar a los dos administradores de ancho de banda estudiados anteriormente, cuando se coloca, solo a un Accelerator administrando un enlace WAN, se debe definir el ancho de banda del enlace, se tiene listas de clasificación de aplicaciones según el tráfico entrante (Inbound) y saliente (Outbound), se puede definir filtros de clasificación de aplicaciones, se puede aplicar prioridades a aplicaciones, asignación de ancho de banda a aplicaciones, preserva o marcado de bits de Clase de Servicio (CoS) y Tipo de Servicio (ToS), clasificación de aplicaciones par a par (P2P) en capa 7.

Accelerator utiliza caché para acelerar aplicaciones comunes como Java, páginas web, imágenes, Citrix. También analizarlos encabezados de los paquetes dinámicamente y reduce el encabezado de los paquetes a través de la WAN, los paquetes son recuperados por un Accelerator remoto. Adicionalmente controla la tasa de transmisión de los paquetes hacia la WAN y recupera paquetes que se puedan perder por medio del Accelerator local y remoto, lo que permite la disminución de las retransmisiones.

Accelerator posee la característica de reporte de todo el tráfico que controla, analiza el tráfico y usa una interfaz Web para mostrar las estadísticas. De manera similar a los administradores de ancho de banda estudiados anteriormente, genera una variedad de gráficos estándar con medidas de utilización y aceleración del enlace, throughput, distribución de ancho de banda, entre otros. Un ejemplo de reporte de Expand se observa en la Figura 2.38.

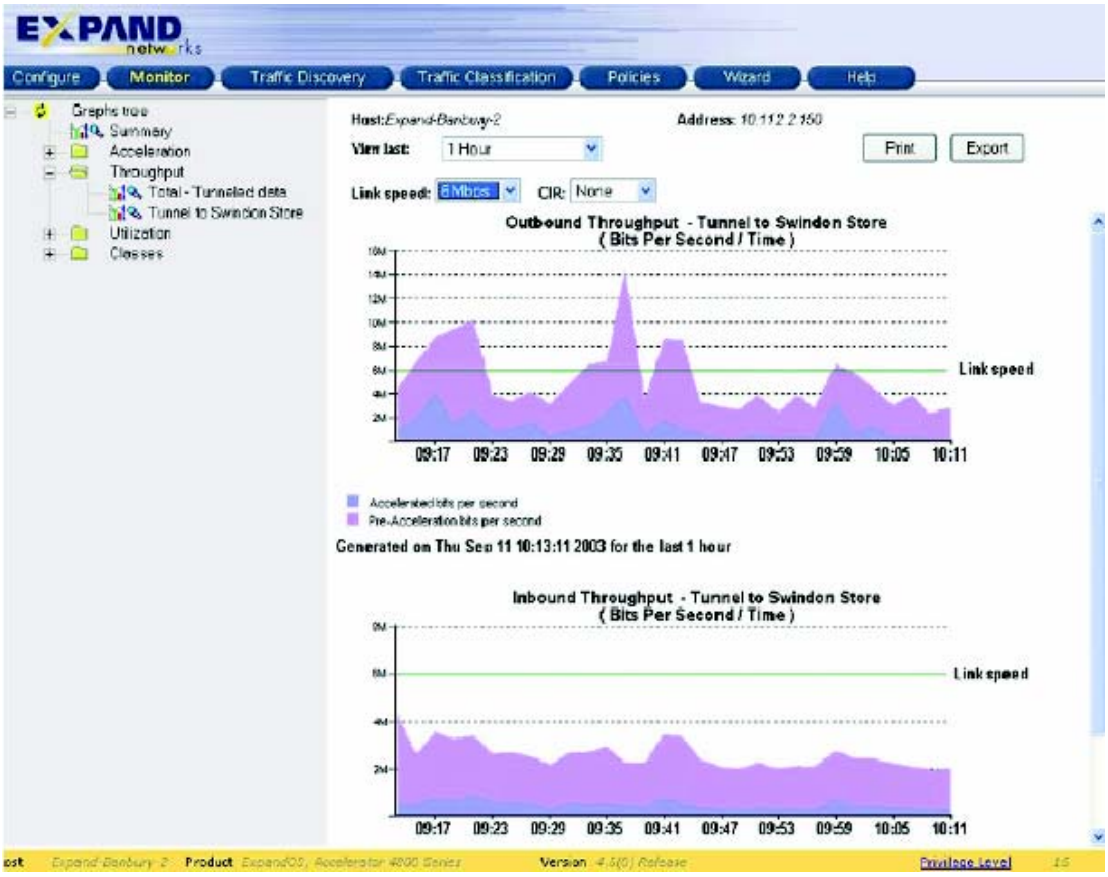


Figura. 2.38. Reporte de Accelerator con relación al caudal de procesamiento.

Los métodos que Accelerator usa para el control de tráfico e implementación de calidad de servicio son mecanismos de encolamiento. Utiliza los mecanismos mencionados en los puntos 2.2.2.1 Entra Primero – Sale Primero (FIFO), 2.2.2.2 Encolamiento de Prioridad (PQ), 2.2.2.3 Encolamiento Personalizado (CQ), 2.2.2.4 Encolamiento Justo Pesado (WFQ) y 2.2.2.5 Encolamiento Justo Pesado Basado en Clases (CBWFQ).

Accelerator se basa en cuatro puntos básicos que son monitoreo, clasificación, reforzamiento y reporte, los cuales son similares a los puntos básicos de los dos administradores de ancho de banda estudiados anteriormente.

2.4 COMPARACION DE TECNOLOGIAS PARA CALIDAD DE SERVICIO

El objetivo principal es comparar tecnologías de sistemas administradores de ancho de banda dedicados, sin embargo es indispensable hacer una comparación entre todas las tecnologías existentes para calidad de servicio, para de esta forma mostrar las fortalezas y debilidades de los sistemas administradores de ancho de banda. Adicionalmente con esta comparación el lector puede tener un mejor criterio para elegir una tecnología que brinde los mayores beneficios a la hora de adquirirla e implementarla.

La comparación se realizará en base a características básicas tales como monitoreo, reporte, clasificación, control y en base a características secundarias como servicios adicionales, flexibilidad y capacidad.

2.4.1 Monitoreo.

Una tecnología que implemente calidad de servicio es indispensable que realice monitoreo, debido a que se puede conocer que tipo de tráfico esta cursando la red, esto permite una mayor facilidad de administración de la red, además es más fácil emitir políticas de calidad de servicio cuando se conoce que tipo de tráfico se debe controlar.

Los elementos de red Cisco hacen un monitoreo mediante herramientas como NBAR, que le permiten descubrir aplicaciones que están cambiando de puertos constantemente, tráfico basado en Localizadores de Recurso Uniforme (URL) ó Extensiones de Correo de Internet Multipropósito (MIME) de un paquete que use el Protocolo de Transferencia de HiperTexto (HTTP), además puede identificar protocolos en capa 4 y en capa 7, aplicaciones para compartir archivos o par a par (P2P) que utilicen específicamente dos protocolos. Descubre puertos del Protocolo de Control de Transferencia (TCP), del Protocolo de Datagrama de Usuario (UDP), no TCP, no UDP y se puede agregar identificación de protocolos a una lista que se encuentra en una memoria borrable. Poseen algunas limitaciones sobre todo con tráfico que use el Protocolo de Transferencia de HiperTexto (HTTP) que es bastante usual en la red.

Los sistemas administradores de ancho de banda dedicado son los que mejor han desarrollado esta característica incluso realizan monitoreo a nivel de capa de aplicación (capa 7 del modelo OSI), el monitoreo es realizado mediante software especializado y descubre una gran cantidad de protocolos existentes hoy en día, incluyendo los de la pila de protocolos TCP/IP, varios protocolos de aplicaciones par a par (P2P) y protocolos de voz y video sobre IP.

Los administradores mencionados en este trabajo necesitan una configuración inicial básica, que consiste en brindarles un lugar en la red, luego de esto pueden descubrir automáticamente el tráfico cursando por la red, específicamente por el Enlace de Red Área Amplia (WAN) ó de Internet, se puede decir que los administradores descubren la misma cantidad de clases de tráfico. Dividen al tráfico en dos enlaces, entrante (Inbound) y saliente (Outbound).

PacketShaper crea los dos enlaces, entrante y saliente, cada uno contiene un árbol de clases, estas clases contienen los distintos tipos de tráfico descubiertos, las clases también se pueden crear según las necesidades de monitoreo y clasificación del usuario. Para cada clase se puede observar la tasa y la cantidad de ancho de banda que consume su tráfico. Accelerator trabaja de forma similar a PacketShaper.

NetEnforcer descubre el tráfico en el tubo por defecto en un inicio y muestra todo los tipos de tráfico descubiertos y los ordena en orden descendente, mostrando de igual forma la tasa y ancho de banda de banda consumido por cada tipo de tráfico.

En conclusión, los sistemas administradores de ancho de banda poseen una mejor tecnología para monitoreo que los elementos de red Cisco debido a algunas limitaciones que presentan en monitoreo de tráfico, además de la facilidad que presentan los administradores de ancho de banda para el monitoreo. Comparando los administradores de ancho de banda, estos poseen similares características de monitoreo.

2.4.2 Reporte.

Una vez monitoreado el tráfico es importante el reporte que pueda generar una tecnología, esto permite analizar el comportamiento del tráfico y de la red de una manera eficiente.

Los elementos de red Cisco poseen reportes gráficos gracias a innovaciones recientes como el Administrador de Políticas de Calidad de Servicio (Cisco QPM, tipo SNMP) y el Administrador de Dispositivos de Calidad de Servicio (Cisco QDM, por navegador web), generan reportes gráficos tipo línea y barras en tiempo real, gráficos históricos de parámetros como estadísticas de tráfico, paquetes por segundo, interfaz, política, además permite ver estadísticas de caudal de procesamiento (throughput). Posee filtros específicos, incluyendo el filtro de Reconocimiento de Aplicación Basado en la Red (NBAR), tasa de tráfico antes de la calidad de servicio, tráfico transmitido después de la calidad de servicio y tráfico descartado, también las estadísticas de reforzamiento de calidad de servicio

Los sistemas administradores de ancho de banda, poseen la capacidad de generar reportes del tráfico que han monitoreado y generalmente son reportes gráficos. NetEnforcer genera reportes gráficos tipo pastel, barras, línea continua y áreas basados en rango de tiempo o de muestras y de algunos parámetros como ancho de banda del enlace entrante y/o saliente, ancho de banda promedio consumido, distribución de tubos, distribución de canales virtuales, tubos más activos, canales virtuales más activos, clientes más activos, servidores más activos, distribución de protocolos, utilización del enlace, paquetes descartados y conexiones.

PacketShaper genera toda clase de reportes gráficos de tipo pastel, línea continua, áreas, históricos basados en un rango de tiempo y basados en varios parámetros como utilización del enlace, eficiencia de la red, conexiones, particiones, actividad de clase, las diez clases más activas, los servidores o clientes más activos que utilizan una clase ó tipo de tráfico. Además genera estadísticas de una gran cantidad de variables como tiempos, retardos, retransmisiones entre otras. Accelerator posee reportes similares a PacketShaper pero en menor cantidad.

Los sistemas son administrables vía plataformas que utilicen el Protocolo de Administración de Red (SNMP) y pueden enviar mensajes (traps) a cualquier lugar de la red.

En conclusión, los reportes básicos de los elementos de red de Cisco son comparables a los de los sistemas administradores de ancho de banda dedicados. Comparando los dos sistemas administradores se observa que brindan reportes similares en lo que se refieren al ancho de banda y su consumo, canales ó clases, utilización del enlace, conexiones, protocolos, canales ó clases más activas, sin embargo PacketShaper ofrece una mayor variedad de reportes que superan a NetEnforcer, Accelerator y Cisco. PacketShaper incluye reportes adicionales de tiempos, retardos, retransmisiones, entre otras que si bien no son esenciales pero al momento de realizar un análisis de la red pueden ser importantes.

2.4.3 Clasificación.

Una vez que se ha monitoreado el tráfico de una red, se generan reportes que generalmente son gráficos y son los más útiles, en ese momento las tecnologías implementando calidad de servicio, tienen mejores argumentos para realizar una clasificación. Además las personas que están supervisando la implementación de calidad de servicio en la red pueden agregar funciones de clasificación adicionales en los elementos de red para obtener un mayor beneficio a la hora de aplicar políticas que refuercen la calidad de servicio, concretamente en un enlace de red área amplia (WAN) o en un Dominio de Servicios Diferenciados (Diffserv).

Para los elementos de red de Cisco clasificación básicamente significa identificar el tráfico (monitoreo) y aplicar mecanismos de encolamiento que refuerzan calidad de servicio en la red y le pueden dar a cierto tráfico mayor prioridad y cierto ancho de banda que a otro tráfico. Así después de que actúa el filtro de Reconocimiento de Aplicación Basado en la Red (NBAR) se aplica 2.2.2.5 Encolamiento Justo Pesado Basado en Clases (CBWFQ) y modelamiento de tráfico. Si no se utiliza NBAR cada mecanismo de encolamiento puede clasificar el tráfico generalmente basándose en protocolo o sub-protocolo de red, interfaz del ruteador por la que llegue el paquete, tamaño del paquete,

Listas de Control de Acceso (ACL), dirección de origen o destino IP, direcciones de control de acceso el medio (MAC), puertos, protocolo TCP, UDP, calidad de servicio ó tipo de servicio.

Adicionalmente a la clasificación que ya se tiene por defecto debido al monitoreo, los sistemas administradores de ancho de banda dedicados pueden crear clasificación personalizada (minuciosa), esto es por protocolos, fuente de conexión, destino de la conexión, servicio, Tipo de Servicio (ToS), Redes de Área Local Virtuales (VLAN). Adicionalmente PacketShaper puede hacerlo por Clase de Servicio (CoS), Punto de Código de Servicios Diferenciados (DSCP) y Conmutación de Etiquetas MultiProtocolo (MPLS). Adicionalmente NetEnforcer puede hacerlo por horas del día.

En conclusión, los sistemas administradores de ancho de banda dedicados son superiores a los elementos de red de Cisco en clasificación, debido a que tienen una clasificación de tráfico por defecto entregada por el monitoreo y además pueden realizar una clasificación minuciosa basada en direcciones, bits, puertos y etiquetas. Comparando los sistemas dedicados PacketShaper supera a los otros administradores de ancho de banda debido a que brinda clasificación basada en los encabezados de los paquetes y conmutación de etiquetas.

2.4.4 Control.

Una vez que se ha monitoreado el tráfico, clasificado el tráfico y se ha analizado reportes sobre el comportamiento de una red, se tiene los argumentos necesarios para aplicar políticas que refuercen la calidad de servicio. En cada tecnología estas políticas se aplican a través del control y dependen de los criterios que se han obtenido de los procesos de análisis, las políticas refuerzan calidad de servicio a cierto tráfico de una red en base a su importancia, concretamente en un enlace de Red Area Amplia (WAN) o en un Dominio de Servicios Diferenciados (Diffserv).

Los elementos de red de Cisco básicamente identifican el tráfico, luego realizan el control mediante mecanismos de encolamiento, descarte y congestión que refuerzan calidad de servicio en la red y le darán a cierto tráfico mayor prioridad y ancho de banda.

Los administradores de ancho de banda una vez que han monitoreado y clasificado el tráfico, aplican el control basado en políticas que refuerzan calidad de servicio. Pueden aplicar políticas de prioridad dependiendo de la importancia del tráfico, pueden aplicar políticas de ancho de banda garantizado y reservación de ancho de banda. Adicionalmente PacketShaper posee su protocolo patentado control de tasa de TCP para administrar tráfico TCP y utiliza planeamiento de límite de retardo para tráfico no TCP. Adicionalmente NetEnforcer y Accelerator utilizan los mecanismos de encolamiento que utilizan los elementos de red Cisco para realizar el control.

En conclusión, los administradores de ancho de banda pueden realizar un mejor control que los elementos de red Cisco, debido a que el monitoreo y clasificación de tráfico es superior, además de la facilidad con que se realiza estos procedimientos comparados con los de los elementos de red Cisco que pueden resultar complicados. Todas las tecnologías pueden realizar control dando prioridades al tráfico, adicionalmente los administradores de ancho de banda garantizan y reservan ancho de banda para todo tipo de tráfico que descubran. Los elementos de red Cisco reservan ancho de banda esencialmente para tráfico en tiempo real como voz sobre IP. PacketShaper posee otras alternativas de control propias como control de tasa de TCP en lugar de usar encolamiento como los otros sistemas administradores de ancho de banda.

2.4.5 Elección del mejor sistema.

En la Tabla 2.5., se ha realizado un resumen sobre los criterios de calidad de servicio para cada uno de los sistemas estudiados.

Sistema / Criterio	Cisco	PacketShaper	NetEnforcer	Accelerator
Monitoreo	Mediante NBAR, capa 4 y capa 7 (solo dos protocolos), algunas limitaciones para HTTP, protocolos TCP/IP, UDP, no TCP/IP no UDP, VoIP.	Mediante PacketSeeker, capa 4 y capa 7 (incluso aplicaciones P2P), MPLS, CoS, ToS, DSCP, pila de protocolos TCP/IP, UDP, no TCP/IP no UDP, VoIP, direcciones.	Mediante NetWizard, capa 4 y capa 7 (incluso aplicaciones P2P), ToS, pila de protocolos TCP/IP, UDP, no TCP/IP no UDP, VoIP, direcciones.	Mediante software web, capa 4 y capa 7 (incluso aplicaciones P2P), CoS, ToS, pila de protocolos TCP/IP, UDP, no TCP/IP no UDP, VoIP, direcciones.
Reporte	Bueno, gráficos y estadísticas.	Muy bueno, gráficos y estadísticas.	Bueno, gráficos y estadísticas.	Bueno, gráficos y estadísticas.
Clasificación	Identificación por monitoreo y aplicación de mecanismos de calidad de servicio los cuales pueden también clasificar el tráfico basándose en listas, direcciones, protocolos y bits.	Por protocolos, fuente de conexión, destino de la conexión, servicio, ToS, VLANs, CoS, DSCP, MPLS, VoIP, aplicaciones específicas y de usuario.	Por protocolos, fuente de conexión, destino de la conexión, servicio, ToS, VLANs, MPLS, VoIP, aplicaciones específicas y de usuario, horas del día.	Por protocolos, fuente de conexión, destino de la conexión, servicio, ToS, VLANs, CoS, MPLS, VoIP, aplicaciones específicas y de usuario.
Control	Mecanismos de encolamiento, descarte y congestión.	Control de Tasa de TCP, mecanismos de prioridad, planeamiento de retardo, asignación de ancho de banda.	Mecanismo de encolamiento, mecanismos de prioridad, planeamiento de retardo, asignación de ancho de banda.	Mecanismo de encolamiento, mecanismos de prioridad, asignación de ancho de banda.
Facilidad de configuración	Complicada	Moderada	Moderada	Ligeramente complicada
Flexibilidad	Moderada	Muy flexible	Flexible	Flexible
Modo de falla	Redundancia	Derivación (Bypass)	Derivación (Bypass)	Derivación (Bypass)
Opción de aceleración de tráfico WAN	No	Si	No	Si

Administrables vía navegador de Internet	Si	Si	Si	Si
Administrables vía plataforma SNMP	Si	Si	Si	Si
Ayuda en seguridad, virus y ataques	Limitada	Buena	Moderada	Moderada

Tabla. 2.5. Resumen sobre criterios de calidad de servicio de los sistemas.

Los elementos de red Cisco y en general cualquier elemento de red como es conocido su principal función es la de ruteo y conmutación de tráfico, aunque también implementen calidad de servicio, sin embargo se necesita un elemento de red en cada nodo del dominio de servicios diferenciados o un ruteador que tenga capacidad de hacer calidad de servicios diferenciados en cada nodo del enlace de Red de Area Amplia (WAN). Son configurados y administrados esencialmente mediante línea de comandos, lo cual es complicado y generalmente es realizado por personal calificado para ese trabajo, sin embargo Cisco ha tratado de aliviar esta dificultad creando software que ayude al usuario a configurar más fácilmente la calidad de servicio, también ha creado software gráfico para configurar los elementos de red. Un elemento de red de cualquier fabricante realiza bien la tarea de calidad de servicio pero en situaciones de baja carga, cuando el tráfico se incrementa estos elementos podrían no funcionar correctamente. Por otra parte se necesita elementos de red que puedan manejar calidad de servicio, esto quiere decir que posean el software y hardware adecuado lo que podría resultar en un cambio mayoritario de los elementos en una red.

Los sistemas administradores de ancho de banda pueden realizar control extremo a extremo estando en un solo extremo de la red, es decir pueden controlar el enlace de Red de Area Amplia (WAN) sin estar en los dos extremos simultáneamente como requiere Cisco, permitiéndole de esa forma administrar también un enlace de Internet. Los sistemas administradores de ancho de banda implementan calidad de servicio para el enlace de red de área amplia, la ventaja de tener un elemento dedicado a implementar calidad de servicio es que se libera capacidad de procesamiento a los ruteadores que estén realizando calidad

de servicio, ese procesamiento liberado el ruteador lo puede emplear para realizar la función básica para la que se los crearon, ruteo.

Los sistemas administradores de ancho de banda además de implementar calidad de servicio, poseen funciones adicionales como aceleración de tráfico, control de admisión de las conexiones, brindan ayuda para control de ataques como virus, ataques (hackers), autenticación en servidores, son administrables mediante navegadores de Internet y plataformas de administración estándares, se los puede conectar en configuraciones redundantes, pueden marcar bits para servicios diferenciados, guardan información del tráfico por algún tiempo con lo que crean gráficos y estadísticas, su configuración y administración es gráfica y no es demasiado complicada salvo que se requiera hacer algo más específico que monitorear, clasificar, analizar y controlar, para lo cual se requiere utilizar línea de comandos.

Analizando los criterios de calidad de servicio que se observan en la Tabla 2.5. y esencialmente los cuatro puntos de comparación más importantes monitoreo, reporte, clasificación y control se observa cualidades superiores para brindar calidad de servicio en los sistemas administradores de ancho de banda dedicados con respecto a los elementos de red Cisco tomados como referencia en este trabajo.

Los administradores de ancho de banda ofrecen más tipos de servicios además de la implementación de calidad de servicio que los elementos de red Cisco. Por otra parte, entre los administradores de ancho de banda dedicados se observa características superiores al administrador de ancho de banda PacketShaper de Packeteer, este sistema administrador será mencionado en los siguientes capítulos, para lo cual se realizará un estudio teórico-práctico.

CAPITULO III

ESTUDIO DEL SISTEMA PACKETSHAPER

3.1 GENERALIDADES

PacketShaper es un sistema de administración de ancho de banda y flujos de tráfico basados en aplicaciones y protocolos. PacketShaper genera un desempeño predecible y eficiente para aplicaciones atravesando enlaces de Red de Area Amplia (WAN) e Internet. Asegura que las aplicaciones críticas (mission critical) obtengan el desempeño requerido, las aplicaciones no críticas no impidan el desempeño de las aplicaciones críticas y a la vez se desarrollen de forma eficiente.

PacketShaper se basa en cuatro pasos para reforzar Calidad de Servicio (QoS) en la red, descubrir y clasificar aplicaciones, obtener reportes y analizar el desempeño de las aplicaciones, reforzar la calidad de servicio basado en políticas y generar reportes de los resultados.

En este capítulo estudia el sistema PacketShaper modelo 1500 el cual es orientado a una organización, el estudio se basa en los aspectos más relevantes del equipo como son su conexión física a la red, configuración de calidad de servicio mediante el software PacketWise, PacketSeeker, PacketShaper. El capítulo finaliza con una descripción de aplicaciones y protocolos que son clasificados por este sistema administrador de ancho de banda.

3.2 INSTALACION DEL SISTEMA ADMINISTRADOR

Es necesario conocer como conectar al sistema a la red antes de configurarlo, PacketShaper es montable en rack de 19 pulgadas y se conecta a la red básicamente mediante dos cables, uno al ruteador y uno al switch o hub.

La primera parte de la instalación es observar que los elementos de red negocien correctamente las opciones ethernet como velocidad y tipo de comunicación half ó full duplex con los puertos del PacketShaper, cuando está encendido. Cuando está apagado funciona la tecnología de derivación (bypass) y se debe verificar que los elementos de red negocien entre ellos las opciones ethernet para evitar que la red deje de operar.

3.2.1 Panel Frontal.

El panel frontal del PacketShaper tiene dos puertos ethernet dentro (inside) y fuera (outside), además tiene un puerto serial DB-9 (9 pines) para conectarse a una PC para una configuración local por consola.

En la Figura 3.1. se observa el panel frontal de un PacketShaper, sin embargo este puede variar de un modelo a otro, en el caso del PacketShaper que se estudiará en este trabajo, no posee ranuras (slots) de expansión de puertos y no posee Pantalla de Cristal Líquido (LCD) para indicar las acciones del PacketShaper.

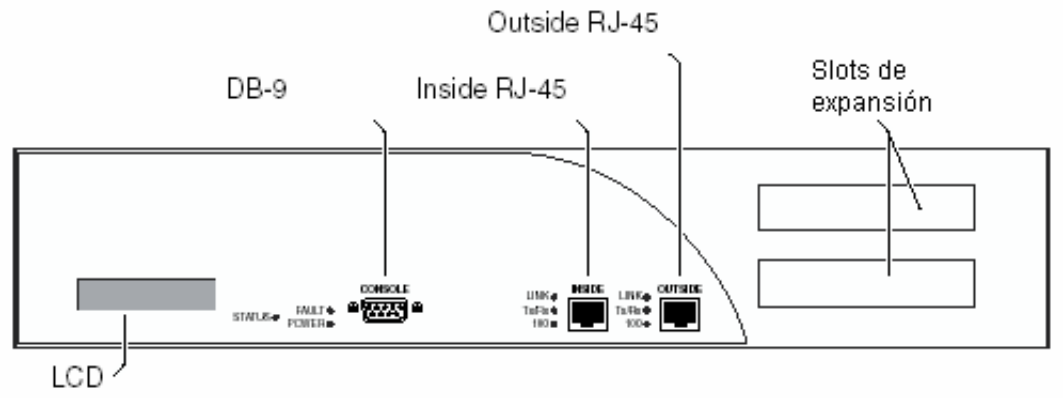


Figura. 3.1. Panel frontal del PacketShaper.

El panel frontal consta de indicadores (leds) que muestran el estatus del PacketShaper, "power" iluminado indica que está conectado y encendido, "fault" iluminado indica que la unidad opera en modo seguro ó corrupto, "link" iluminado indica enlace ethernet, "Tx/Rx" parpadea cuando transmite y recibe datos y "100" iluminado indica 100 Mbps y apagado 10 Mbps.

La forma de conectar un PacketShaper a la red es mediante cables ethernet directo y cruzado, el cable que se debe usar depende a que unidad se le va a conectar directamente, como se observa en la Tabla 3.1.

Conexión directa	**Cable ethernet**
Ruteador	Cruzado
Firewall	Cruzado
Servidor	Cruzado
Hub	Directo
Switch	Directo

Tabla. 3.1 Cables para conectar al PacketShaper a la red.

Por ejemplo para conectar un PacketShaper a una red común con ruteador y switch, se desconecta el cable directo entre el switch y el ruteador, luego se conecta un cable cruzado entre el puerto fuera (outside) del PacketShaper y por último se conecta un cable directo entre el puerto dentro (inside) del PacketShaper y el switch.

3.3 CONFIGURACION DEL SISTEMA ADMINISTRADOR

Después de que se ha instalado PacketShaper en la red, se necesita configurar el software PacketWise. El software PacketWise es configurable vía navegador web, consola y emulación de terminal, todos proveen una guía de configuración que sugiere los parámetros requeridos y provee ayuda para ayudar al usuario a tomar las decisiones de configuración.

3.3.1 Configuración vía navegador de Internet.

Se debe disponer de un navegador de Internet tal como Nestcape 4.7 ó superior e Internet Explorer 5 ó superior, además el navegador debe estar configurado para aceptar cookies, el lenguaje para páginas web JavaScript habilitado y el caché configurado a todas las visitas a la página. Para un obtener un rendimiento gráfico óptimo la pantalla gráfica debería configurarse a 1024x768 pixels.

El procedimiento de configuración es iniciar el navegador web, luego en la ventana de direcciones ingresar la dirección por defecto del equipo 207.78.98.254 o el nombre de Servidor de Nombres de Dominio (DNS) “unconfigured.PacketShaper.com” solo si se dispone de un servidor de nombres en la red. En este momento aparecerá la guía de configuración que ayudará a configurar el software PacketWise.

3.3.2 Configuración remota con autenticación.

Se puede escoger la utilidad remota con autenticación que se prefiera, por ejemplo el Protocolo de Emulación de Terminal (TELNET) para Windows. El procedimiento es realizar una conexión a la dirección por defecto 207.78.98.254 o el nombre de Servidor de Nombres de Dominio (DNS) “unconfigured.PacketShaper.com” solo si se dispone de un servidor de nombres en la red, un ejemplo sería telnet 207.78.98.254. En este momento aparecerá la dirección IP y una referencia de clave de acceso (password), aquí se presiona la tecla “Enter” para pasar a la guía de configuración. La clave y la dirección IP nuevas se configurarán posteriormente.

3.3.3 Configuración mediante cable de consola.

En caso de que las configuraciones vía navegador de Internet o conexión remota no tengan éxito, la configuración más segura es acceder directamente con un cable de módem nulo, este cable provee conectores DB-9 (9 pines) y DB-25 (25 pines) en cada extremo.

El procedimiento es conectar el cable a un puerto serial del computador, conectar el otro extremo al puerto "console" del PacketShaper, abrir un programa de emulación de terminal como Hyperterminal de Windows, configurar los parámetros de comunicación del puerto serial del computador a 9600 bps, 8 bits de datos, 1 bit de parada, sin paridad y control de flujo por hardware.

En este momento se enciende el PacketShaper aparecen los mensajes "booting" y "loading", luego se presiona varias veces la tecla "Enter" hasta que aparezca el mensaje "PackeShaper (console)" y "password". Se presiona la tecla "Enter" para ingresar a la guía de configuración, la clave de acceso y la dirección IP nuevos se configurarán posteriormente.

3.3.4 Configuración inicial.

Se ha llegado a la guía de configuración que configurará los parámetros del software PacketWise, a continuación se describirán los parámetros que se debe configurar.

- El sistema pregunta si se desea iniciar la guía de configuración, se responde "yes". En este momento el sistema despliega una lista de los elementos que van a configurar, con una pequeña descripción de cada uno de ellos.

- Se selecciona modo local o compartido. El modo local se selecciona cuando se tiene un PacketShaper en la red o cuando se tiene varios pero realizan una función única. El modo compartido se selecciona cuando se tiene varios PacketShaper y se los manejará mediante un producto separado de Packeteer llamado PolicyCenter,

que se coloca en un servidor y permite configurar los sistemas desde un sistema de administración central.

- Se ingresa una dirección IP correspondiente a la red, por ejemplo 192.168.2.50

- Se ingresa una máscara de subred, por ejemplo 255.255.255.0

- Se ingresa los parámetros velocidad y tipo de comunicación de los puertos ethernet "inside" y "outside" del PacketShaper, para la velocidad de los puertos se ingresa "10bt", "100bt" o "auto" (negociación), para el tipo de comunicación se ingresa "half", "full" o "auto" (negociación).

- Se ingresa la dirección IP del ruteador de la red del que se quiere administrar el ancho de banda, por ejemplo 192.168.2.1 o "none" para ninguna dirección del ruteador.

- Se ingresa una dirección IP de puerta de enlace, para que PacketShaper pueda realizar operaciones que no correspondan a la red local, por lo general esta dirección es la misma que la del ruteador del sitio, por ejemplo 192.168.2.1 ó 0.0.0.0 para ninguna puerta de enlace.

- Opcionalmente se puede ingresar las direcciones de Servidores de Nombres de Dominio (DNS), para que después de que se complete la guía de configuración, se pueda especificar nombres de dominio en lugar de direcciones IP, se puede ingresar una o varias direcciones IP separadas por espacios, por ejemplo 192.168.2.10 ó "none" para ningún servidor.

- El sistema pregunta si se desea programar las claves de acceso, se responde "yes", se ingresa la contraseña antigua de acceso total que permite monitoreo y configuración del sistema, luego se ingresa la nueva contraseña. De igual forma se programa el "password look" que permite solo monitoreo del sistema.

- Se ingresa la tasa de datos de los enlaces de entrada (Inbound) que es la tasa de datos llegando al sitio a través de la Red de Área Amplia (WAN) y del enlace de salida (Outbound) que es la tasa de datos saliendo del sitio a través de la red de área amplia, generalmente son iguales, se ingresa como un valor de bits entero de bits por segundo, seguido por "k" o "M" para miles o millones de bits por segundo respectivamente, o se especifica simbólicamente como "T1", "E1", "T3", "10BT", "100BT", "Ethernet".

- El sistema pregunta si se desea activar "shaping on" que es el modelamiento del tráfico, si se activa "on" las políticas de tráfico configuradas son reforzadas. Cuando no se activa "off" el tráfico atraviesa el PacketShaper transparentemente.

- El sistema pregunta si se desea activar "discovery on", si se activa "on" PacketShaper analiza el tráfico de los enlaces entrada y salida, además genera automáticamente un árbol de tráfico con clases basadas en los tipos de aplicaciones que puede descubrir. Cuando no se activa "off" el sistema no descubre el tráfico.

- El sistema para mantener el tiempo local y ajustar el reloj requiere que se ingrese una zona de tiempo, por ejemplo Los Angeles o ? para mostrar una lista con todas las opciones disponibles.

- Se ingresa los datos de tiempo en el siguiente formato año-mes-día-hora-minutos, por ejemplo 200011101605.

- Finalmente pregunta si se desea guardar los cambios, se responde "yes". Otro tipo de configuraciones se podrán hacer posteriormente.

3.3.5 Configuración avanzada.

Para la configuración se ingresa el "password touch", una vez autenticado aparecerá el software PacketWise el cual ayudará al usuario a configurar características especiales del sistema, específicamente de PackeetSeeker y PacketShaper.

El software tiene nueve fichas, cinco de ellas son para configuración del sistema y cuatro de ellas son para obtener información del sistema. Al ingresar al software PacketWise selecciona por defecto la ficha "Info", aquí se muestra información del modelo, dirección IP, número de serie, versión del software, entre otra información que tiene que ver con la configuración del sistema. Luego de que se ha efectuado cualquier configuración en el sistema es necesario aplicar los cambios.

Posteriormente se mencionará ciertas configuraciones que se consideran importantes para implementar calidad de servicio mediante este sistema.

3.3.5.1 Soporte del Protocolo de Administración de Red Simple (SNMP).

Este protocolo es ampliamente usado para monitorear redes de computadores, se configura PacketWise para enviar mensajes (traps), como notificaciones de eventos o advertencias de condiciones de alarma hacia una plataforma que utilice el protocolo de administración. PacketWise puede ser configurado para trabajar con plataformas estándares como HP OpenView o propietarias como ReportCenter de Packeteer, para configurar el soporte del protocolo de administración se sigue el siguiente procedimiento:

- En la ficha "setup" se selecciona "SNMP" como se observa en la Figura 3.2.

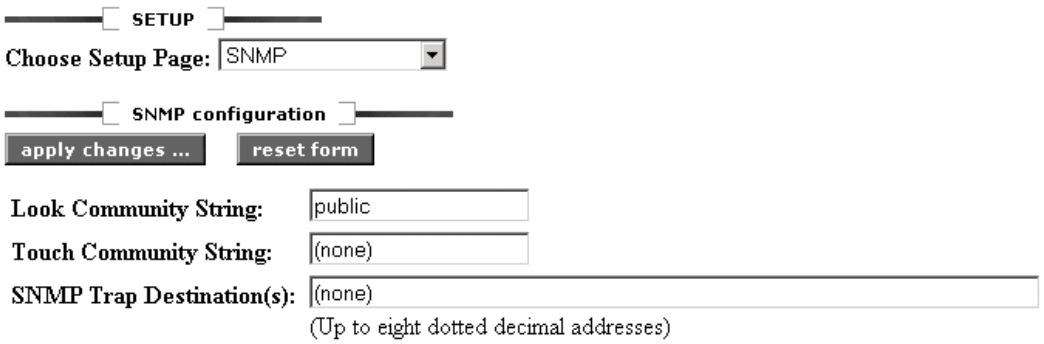


Figura. 3.2. Soporte del Protocolo de Administración de Red Simple (SNMP).

- Se debe ingresar "Look Community String", que es la clave de acceso para que la plataforma se autentique para monitoreo, por defecto es "public".

- Se debe ingresar "Touch Community String", que es la clave de acceso para que la plataforma se autentique para monitoreo y configuración, por defecto es "none".

Otro tipo de monitoreo es la notificación vía e-mail, para hacerlo PacketWise usa el Protocolo de Transferencia de Mail Simple (SMTP), por lo tanto necesita la localización de un servidor de correo que use el protocolo de transferencia de mail y necesita conocer la dirección e-mail a la que se enviará la notificación.

3.3.5.2 Configuración sobre falla.

Si el ruteador falla en su enlace de red de área amplia principal y tiene un enlace de respaldo, se puede configurar una configuración sobre falla para que PacketShaper se adapte al nuevo enlace. PacketWise toma datos cada dos segundos vía el Protocolo de Administración de Red Simple (SNMP) desde el ruteador para determinar el estado de los enlaces, para la configuración sobre falla en PacketShaper se sigue el siguiente procedimiento:

- En la ficha "setup" se selecciona "basic" para confirmar que se ha configurado la dirección IP del ruteador, se observa el parámetro "site router" que es un requisito para la configuración sobre falla.

- En la ficha "setup" se selecciona "failover" como se observa en la Figura 3.3.

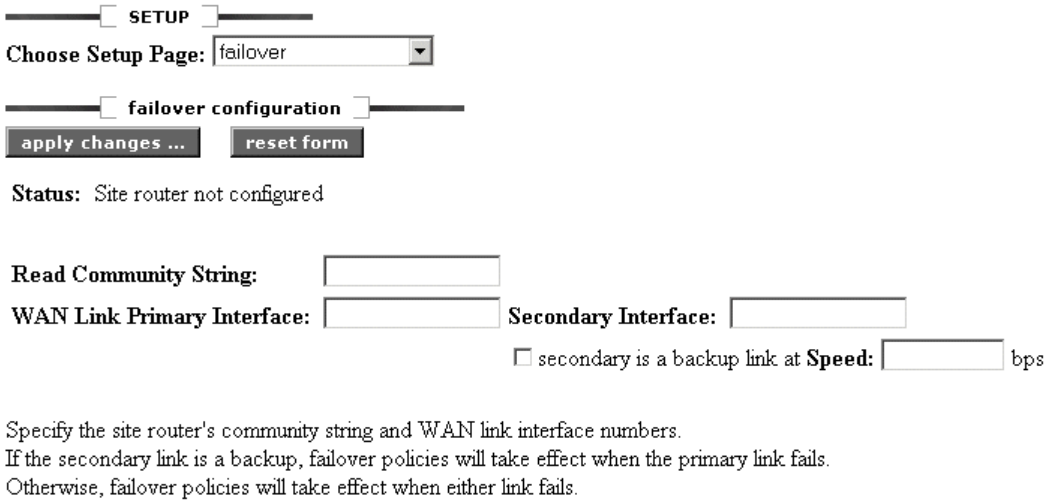


Figura. 3.3. Configuración sobre falla.

- Se debe ingresar "Read Community String", que es la clave de acceso del protocolo de administración para acceso al ruteador, si no se indica ninguna PacketWise usará por defecto "public".

- En "WAN Link Primary/Secondary Interface", se ingresan dos valores que son los índices del protocolo de administración que ha asignado el ruteador a los enlaces principal y de respaldo.

3.3.5.3 Reiniciar parámetros y el sistema.

Se puede reiniciar el árbol de tráfico a la configuración de clases de fábrica, lo que incluye las clases del enlace de entrada y salida, se puede reiniciar "Easy Configure" que

es una forma sencilla de configurar calidad de servicio en PacketShaper, se puede reiniciar los datos de medición, reiniciar toda la configuración de PacketWise a la configuración de fábrica y reiniciar el sistema en caso de actualizaciones de software, el procedimiento es el siguiente:

- En la ficha setup se selecciona "unit resets" como se observa en la Figura 3.4.

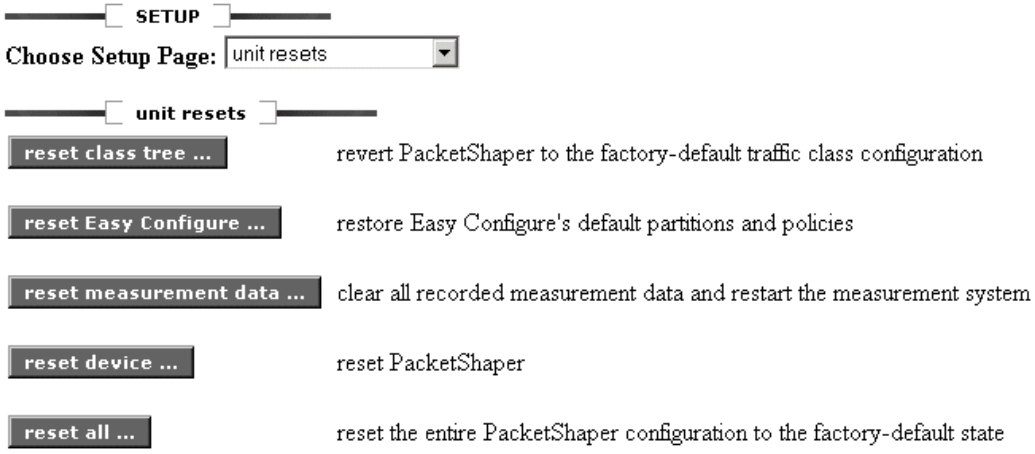


Figura. 3.4 Reinicio de parámetros y sistema.

3.3.6 Configuración de calidad de servicio.

En este tema se menciona los parámetros de configuración de monitoreo, análisis, clasificación y control necesarios para implementar calidad de servicio mediante este administrador de ancho de banda.

3.3.6.1 Utilización de "Easy Configure".

Es una opción de PacketWise que cuando está habilitada, ayuda al usuario a configurar sencillamente la calidad de servicio en PacketShaper, asigna aplicaciones y servicios a categorías, por ejemplo aplicaciones críticas o prohibidas y automáticamente crea políticas

y particiones adecuadas. Antes de mencionar “Easy Configure”, se emitirá tres conceptos que son fundamentales en la configuración de PacketShaper y son:

Clase: Es un grupo lógico de flujos de tráfico que comparten las mismas características, por ejemplo protocolo, dirección, aplicación específica, subred. Aparecen categorizadas por el sistema, sin embargo el usuario puede cambiar la categoría de las clases según su necesidad, hay dos clases que no se pueden categorizar y crea por defecto el sistema, “default” donde se encuentran flujos de tráfico que no pudieron ser clasificados y “localhost” que sirve para administración del sistema y tiene por defecto una prioridad 6, muy útil en caso de congestión.

Partición: Un tubo de ancho de banda asignado a una clase de tráfico dada, con el fin de proteger o restringir todos los flujos que forman parte de la clase, ver el punto 3.3.6.5 Particiones.

Política: Una regla asignada a una clase, dicha regla define como un flujo simple será manejado durante la asignación de ancho de banda, ver el punto 3.3.6.6 Políticas.

El procedimiento para utilizar “Easy Configure” es el siguiente:

- Para habilitarlo, en la ficha “setup” como se observa en la Figura 3.4. se activa “Easy Configure”.

- Se selecciona “top ten – average rate” en la casilla “view” de la ficha “top ten”, como se observa en la Figura 3.5.

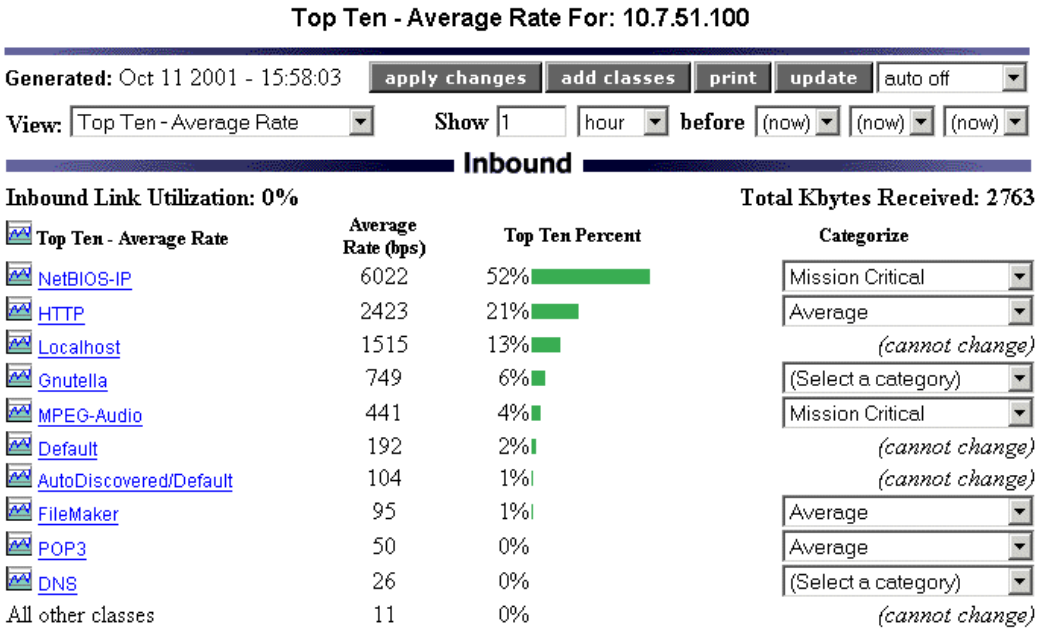


Figura. 3.5. Ficha "top ten" del PacketShaper.

- Aquí se muestra los diez servicios que más consumen el ancho de banda designados como clases tanto del enlace de entrada como el de salida, debe estar habilitado "traffic discovery".

  Las categorías disponibles para las clases son:

  - *Mission Critical.*- Tiene una alta prioridad, por ejemplo si son aplicaciones importantes para una empresa o tráfico de tiempo real.

  - *Average.*- Para aplicaciones que son importantes pero no necesitan una respuesta inmediata como misión critical.

  - *Low Prioriy.*- Para aplicaciones con baja prioridad, se pueden utilizar pero sin interrumpir las otras dos categorías de tráfico más importantes.

  - *Prohibited.*- Para servicios o aplicaciones que son prohibidas en la red.

Se puede también configurar clases fuera de “top ten” seleccionando “all classes” en la casilla “view” en la ventana “top ten”.

Asignar categorías a las clases implica crear tasas apropiadas o políticas de prioridad, “Easy Configure” asigna políticas de tasa a tráfico basado en TCP y políticas de prioridad a tráfico basado en UDP. Finalmente se crea un árbol inbound y otro outbound cada uno con particiones “mission critical”, “average”, “low priority” y “prohibited”. Cada partición contiene las clases según como se las haya categorizado.

Mediante “Easy Configure” se aplica calidad de servicio casi automáticamente, ahora se va configurar el sistema de una manera más avanzada. Para esto se necesita configurar manualmente algunos parámetros que se estudiarán a continuación.

3.3.6.2 Monitoreo y Clasificación.

Antes de poder implementar calidad de servicio, se debe determinar que aplicaciones se están ejecutando en la red. La característica para descubrir tráfico de PacketWise puede descubrir el tráfico automáticamente y crear una lista llamada árbol de tráfico que contiene todas las aplicaciones en la red. PacketWise diferencia una aplicación de otra evaluando características de los flujos y agrupándolos dentro de clases, cada clase de tráfico contiene al menos una regla (matching rule), estas reglas son un conjunto de características que identifican un tipo de tráfico específico como localización del servidor, computador/subred, criterio específico de aplicación, servicios diferenciados, conmutación por etiquetas, redes virtuales. La activación de “traffic discovery” se la realiza en el casillero “Choose Setup Page” en la ficha “setup” como se observa en la Figura 3.4.

3.3.6.2.1 Descubriendo el tráfico de clases individualmente.

Ciertas clases de tráfico, como por ejemplo redes virtuales, Citrix, subredes, pueden ser clasificadas más específicamente, para esto se sigue el siguiente procedimiento:

- Se elige la ficha “manage” del navegador web, aparece la ventana “Traffic Class” como se observa en la Figura 3.6., se selecciona la clase que se desea descubrir individualmente y se selecciona “Traffic Discovery within Class” si está disponible.

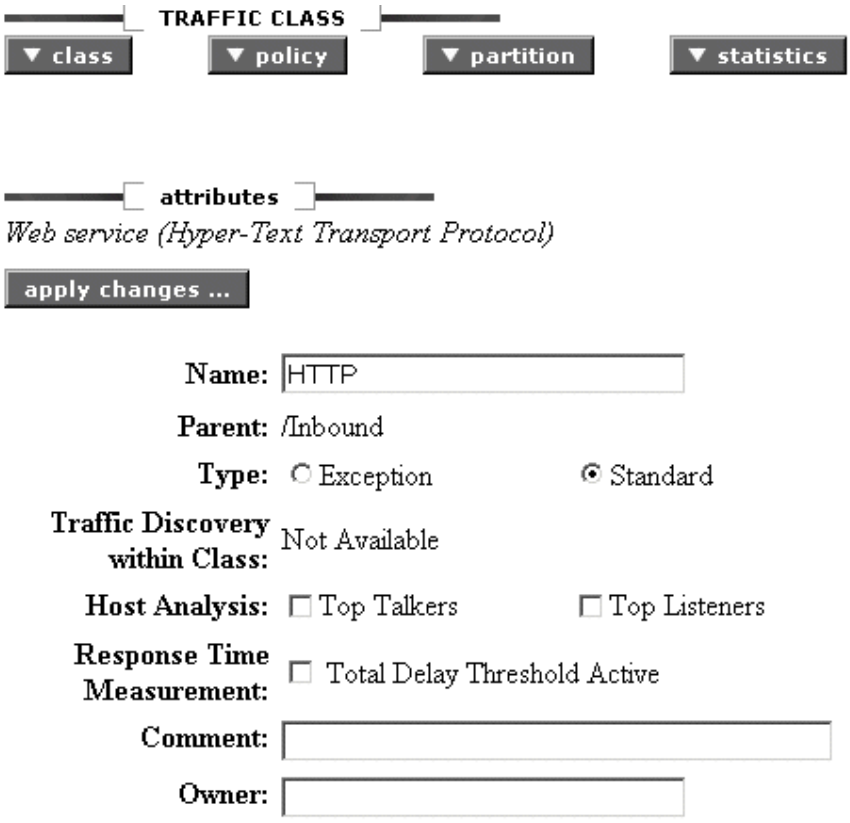


Figura. 3.6. Descubrir el tráfico de clases indivualmente.

3.3.6.2.2 Creando clases y aplicando “matching rules”.

La opción “traffic discovery” crea clases automáticamente, sin embargo se puede crear clases con reglas de clasificación “matching rules” específicas, esto es útil para manejar un tipo de tráfico más específico, por ejemplo para una oficina remota, el procedimiento para crear una clase con “matching rules” es el siguiente:

- Se elige la ficha “manage” del navegador web, aparece la ventana “Traffic Class” en donde se muestra las clases, se selecciona la clase donde se desea crear (clase padre), pueden ser también las clases “outbound” ó “inbound”.

- Se elige “class” y luego “add”, aparece la ventana de configuración de la nueva clase, como se observa en la Figura 3.7.

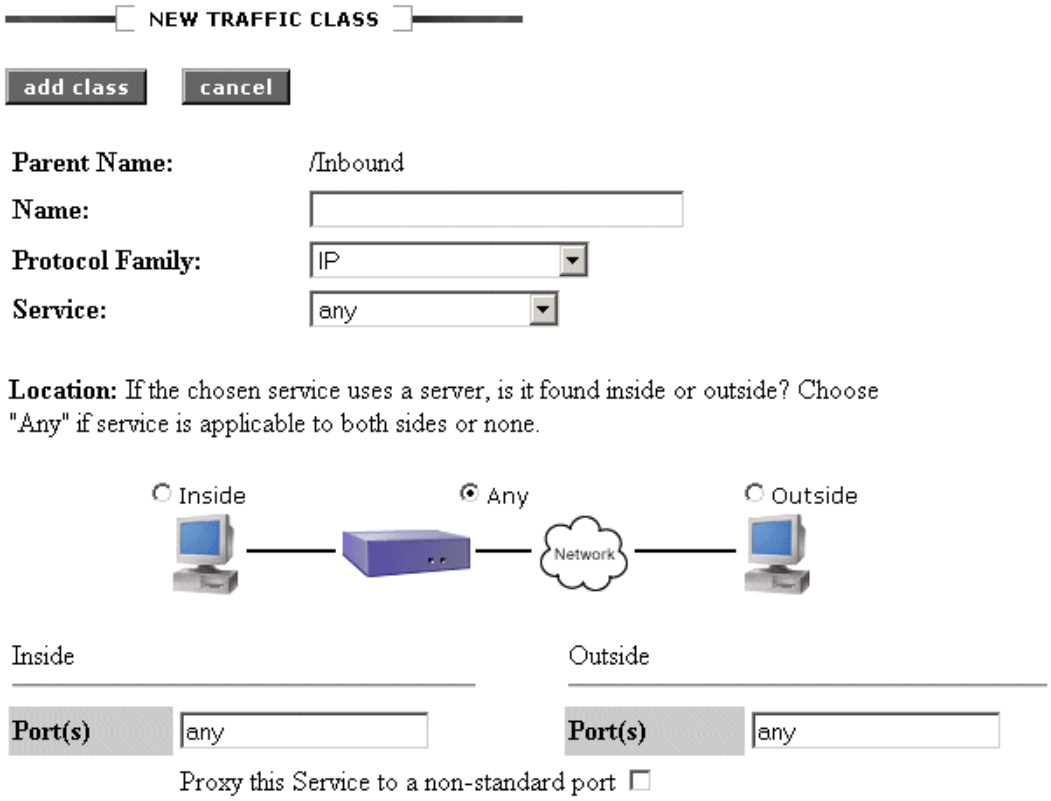


Figura. 3.7. Ventana de configuración para crear una clase.

- Se ingresa un nombre para la clase para luego aplicar las “matching rules”. Cuando se crea una clase (hija) dentro de otra clase (padre), en la clase hija debe ingresarse la misma “matching rule” de la clase padre, caso contrario ocurrirá un error de incompatibilidad, sin embargo se puede agregar “matching rules” adicionales a las clases hijas, una clase creada ó hija no hereda las “matching rules” de la clase que la contiene.

- En la casilla “Protocol Family”, se puede elegir entre familias de protocolos “IP”, “IPX”, “SNA”, “ApleTalk”, “NetBEUI”, “DECnet”, “FNA” (protocolos no IP), “others” (protocolos no IP no bien identificados) y “any” (todo el tráfico). Por ejemplo IP encierra la capa de red IP, la capa de transporte TCP/UDP y varios servicios de la pila de protocolos TCP/IP (FTP, HTTP, Web, Telnet, etc). Para una breve desecripción de aplicaciones y protocolos observar el punto 3.4 APLICACIONES Y PROTOCOLOS CLASIFICADOS POR PACKETSHAPER.

- En la casilla “Service”, se puede elegir una aplicación o servicio del protocolo especificado, por ejemplo para “IP”, se puede elegir “TCP”, “UDP”, “any” (todos), entre otros.

- Para servicios “IP” se selecciona la localización del servidor que provee los servicios escogidos como se observa en la Figura 3.8., se puede elegir “Inside” (red de área local), “Outside” (red de área amplia) ó “Any” (ambas redes). Para los protocolos no IP se selecciona “any” ya que estos protocolos no manejan referencias “Inside”, “Outside”.

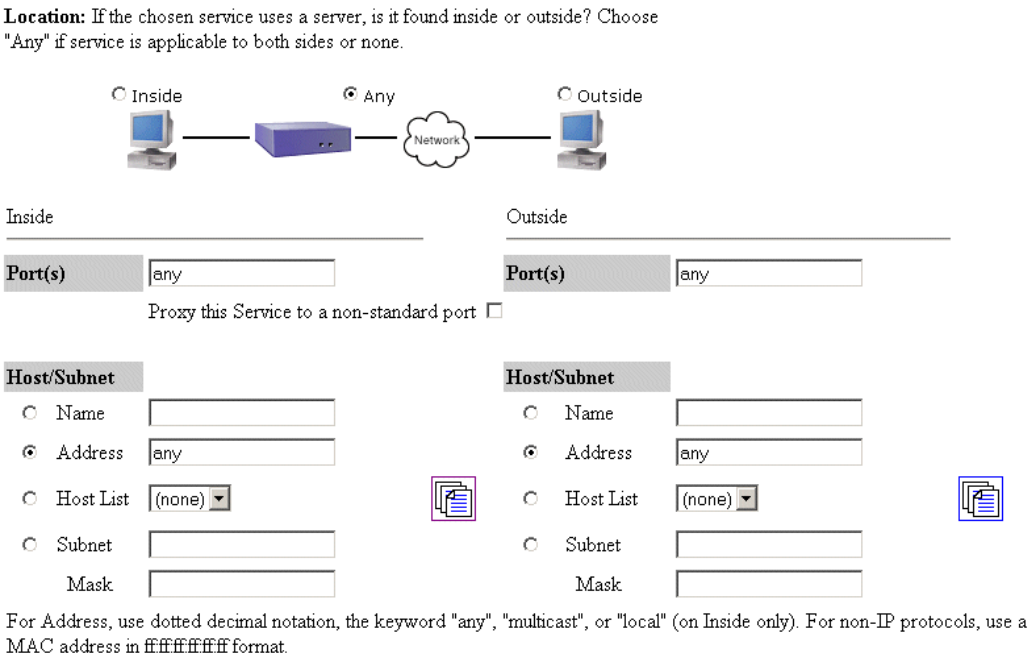


Figura. 3.8. "Matching rules".

- Se ingresa el o los puertos que utiliza el servidor para estos servicios, por ejemplo un rango 5001-5005, si no se conoce se ingresa "Any".

- Se puede seleccionar la opción "Proxy this Service to a Non-Standard Port", permite identificar aplicaciones ejecutándose en puertos que no cumplen con los estándares definidos por la Autoridad de Números Asignados a Internet (IANA).

- El campo "Host/Subnet" se usa para aislar un simple computador o un rango de computadores, se puede ingresar las siguientes opciones:

  - *Nombre.*- Si se tiene un servidor de nombres, se puede ingresar un nombre de dominio.

  - *Dirección.*- Se puede ingresar una dirección IP o un rango de direcciones IP, por ejemplo 10.10.10.10-10.10.10.20. Se puede ingresar "multicast" para especificar direcciones Clase D (224.0.0.0 a 239.255.255.255), se

puede ingresar una dirección de Control de Acceso al Medio (MAC) para clasificación de un computador que utilice protocolos no IP, por ejemplo 08:12:34:56:A1:5C, también se puede ingresar "any" para todas las direcciones.

- *Subred y máscara.*- Se ingresa una máscara de red y por ende se selecciona un subgrupo de computadores.

- *Lista de Hosts.*- Una lista de computadores que contiene un conjunto de direcciones y/o nombres asignados por un Servidor de Nombres de Dominio (DNS), aquí se puede crear, modificar o borrar listas de computadores.

- Para los servicios como el Protocolo de Transferencia de HiperTexto (HTTP), Arquitectura de Computador Independiente Citrix (Citrix-ICA), Protocolo de Mensajes de Control de Internet (ICMP), Oracle-NetV2 (bases de datos) y el Protocolo de Transporte en Tiempo Real (RTP-I), está disponible el campo "Criterion" para especificar criterios de aplicación, como se observa en la Figura 3.9.

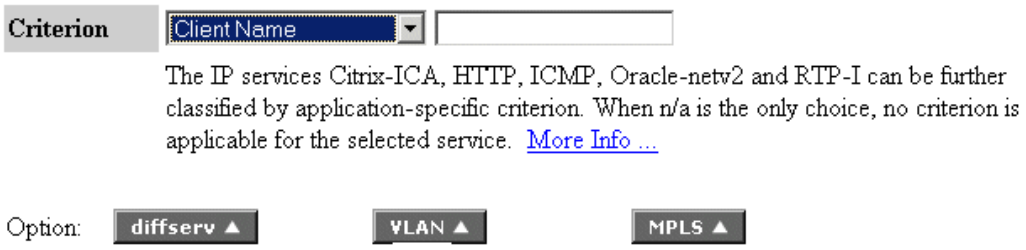


Figura. 3.9. Clasificación por criterios específicos de aplicación.

Los criterios de especificación se describen a continuación:

- *Citrix-ICA.*- Puede ser clasificado por aplicación publicada ingresando el nombre, por ejemplo PeopleSoft, por nombre de cliente ingresando el

nombre y por prioridad que asigna Citrix-ICA a los canales virtuales junto a un flujo ICA simple, se ingresa un valor de prioridad entre 0 (más alta) y 3.

- *HTTP*.- Puede ser clasificado ingresando el nombre asignado por el Servidor de Nombres de Dominio (DNS) ó dirección IP de un sitio web, ingresando un solo Localizador de Recurso Uniforme (URL), se puede ingresar opciones de clasificación de transferencia de archivos por ejemplo archivos de Grupo Fotográfico Junto (JPG), *.jpg. Hay dos opciones que necesitan la línea de comandos para ser utilizados son "Content Type" y "Web Browser o User Agent", la primera permite descubrir que tipo de archivos esta transportando HTTP por ejemplo archivos con Lenguaje de Marcado de Hipertexto (HTML), texto, gráficos, Grupo de Imágenes en Movimiento (MPG) y la segunda permite descubrir que tipo de software web cliente se está usando, por ejemplo Real Player, el comando que se utiliza es "class criteria track". Una vez que se ha descubierto se generan listas como la siguientes:

  Traffic Class: /Inbound/HTTP
  Application: Web
  Attribute: content-type (Content type)
  Recent Attribute Values (most recent first)
  ---
  1. text/html
  2. image/gif
  3. text/plain
  4. image/jpeg

  Traffic Class: /Inbound/HTTP
  Application: Web
  Attribute: user-agent (Web browser or user agent)

  Recent Attribute Values (most recent first)
  ---
  1. RealPlayer G2
  2. RMA/1.0 (compatible; RealMedia)
  3. QTS (qtver=4.1.1;os=Windows 95 B)

4. Mozilla/4.0 (compatible; MSIE 4.01; Windows 95)
5. Mozilla/4.06 [en] (Win95; U

Estas listas se deben ingresar en el campo "Criterion", con la opción que se seleccione.

- *ICMP Criteria.*- Puede ser clasificado ingresando tipos de paquetes generados como paquetes "echo" generado por el comando ping, destino no alcanzable (dest_unreachable), extinguir (quench), redireccionar (redirect), tiempo excedido (time_exceded), parámetro probable (param_prob), sello de tiempo (timestamp), información (info), máscara de dirección (address_mask).

- *Oracle Criteria.*- El tráfico Oracle-netv2 puede clasificarse ingresando el nombre de la base de datos.

- *RTP-I Criteria.*- Puede ser clasificado ingresando criterios estándares como nombre de codificación "Encoding Name" (GSM, JPEG); tipo de flujo "Media Type" ("a" para audio, "v" para video); tasa de reloj "Clock Rate" (8000, 16000, 44100, 90000).

- Se puede clasificar por otros servicios observando los encabezados de paquetes, eligiendo "diffserv" como se observa en la Figura 3.9, se puede seleccionar entre las siguientes opciones:

  - *Code Point.*- Se ingresa el Punto de Código de Servicios Diferenciados (DSCP) como un número de 0 a 63 que es el equivalente decimal del número binario.

  - *COS/TOS.*- Para clase de servicio (COS) se ingresa la prioridad de 0 a 7 (más alta) y para tipo de servicio (TOS) se ingresa los valores de nivel de

servicio 0, 1, 2, 4, 8. Estos valores son los equivalentes decimales de los números binarios.

- Se puede clasificar conmutación por etiquetas multiprotocolo, eligiendo "MPLS" como se observa en la Figura 3.9., se puede clasificar por una simple etiqueta ingresando un número entre 0 y 1048575, por un rango de etiquetas por ejemplo 250-350 y para cualquier flujo de tráfico que tenga etiquetas ingresando "any".

- Se puede clasificar por tráfico de redes virtuales, eligiendo "VLAN" como se observa en la Figura 3.9., se puede clasificar por una simple identificación de red virtual ingresando un número entre 0 y 4095, por un rango de identificaciones de redes virtuales por ejemplo 100-200 y para cualquier flujo de tráfico que tiene identificación de red virtual ingresando "any".

En la ficha "manage" se tiene otras características como "Exception Class" que se selecciona para una clase para hacerla clase excepción, PacketWise coloca los tipos de tráfico buscando en el árbol de tráfico desde arriba y coloca al tráfico en una clase cuando encuentra una que cumple con las características del tráfico y no busca más clases. La clase excepción se coloca en la parte superior del árbol para asegurar que un tipo de tráfico se colocará en esa clase.

Se tiene otra opción que es "Inheritable Class", sirve para que una clase (hija) creada dentro de otra clase (padre), herede las políticas de calidad de servicio de la clase padre. Las clases creadas por defecto "Default" son heredables y no se pueden cambiar.

Se tiene otra opción "traffic class test" que sirve para observar como PacketWise ha colocado un flujo de tráfico desde una dirección en una clase, en esta clase de prueba se puede definir las "matching rules" que se define cuando se crea una clase.

Se tiene otra opción "Top Talkers" y "Top Listeners", permite clasificar a los computadores que más transmiten (más habladores) y que más reciben (más escuchadores) dentro de esa clase. Se puede realizar otras opciones como copiar, mover y borrar clases,

también crear otros fólderes aparte de “inbound” y “outbound”, además la forma de mostrar el árbol de clases de tráfico.

3.3.6.3 Mediciones y reportes gráficos.

El software PacketWise brinda una capacidad de reporte extensa para PacketShaper, se puede ver gráficos de enlaces, uso y desempeño de aplicaciones, PacketWise recolecta datos sobre bastantes variables de medición, estos datos pueden ser mostrados como estadísticas o gráficos de varios tipos.

3.3.6.3.1 Estadísticas de variables de medición.

Para observar las estadísticas de variables de medición se elige la ficha “manage”, se elige “statistics” y se escoge “data” y aparece una ventana como se observa en la Figura 3.10.

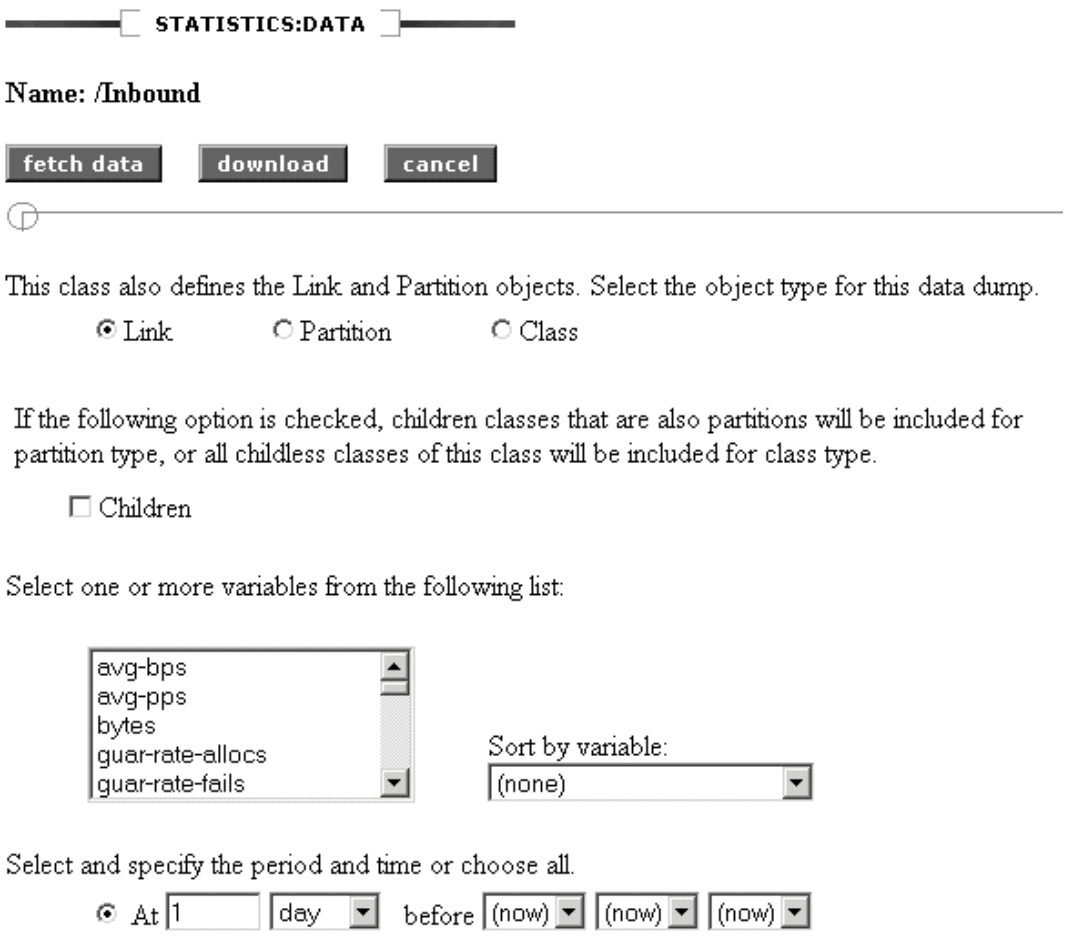


Figura. 3.10. Estadísticas de variables de medición.

Se escoge el objeto que puede ser enlace “link”, partición “partition”, clase “class”, si se quiere selecciona “Children” para obtener estadísticas de clases que estén dentro de otras, luego se selecciona las variables que se desea observar las estadísticas. Los tipos de variables de medición varían dependiendo del objeto, sin embargo las variables comunes están disponibles para cualquier tipo de objeto, la definición de partición se estudiará posteriormente en este capítulo. En la Tabla 3.2. se observa los tipos de variables de medición según el objeto.

Variables comunes	
Variable	**Descripción**
avg-bps	Uso, promediado sobre un intervalo, en bits por segundo
avg-pps	Tasa promedio de paquetes por segundo, pkts / sample-interval-secs
Bytes	Número de bytes que han pasado en un intervalo
Guar-rate-allocs	Conteo de asignaciones que fueron permitidas para garantizar tasa en un intervalo
Guar-rate-fails	Conteo de bloqueos de control de admisión cuando no hubo suficiente ancho de banda para garantizar tasa
Kbytes	Número de bytes que han pasado en un intervalo, dividido para 1000 y redondeado al más cercano Kbyte
peak-bps	Tasa pico asignada promediada sobre el intervalo
peak-guar-rate-flows	Conteo de picos de flujo de tasa garantizada
peak-tcp-conns	El número más alto de conexiones TCP simultáneas en un intervalo
Pkts	Número de paquetes que han pasado a través del sistema en un intervalo
sample-interval-msecs	Tiempo entre las muestras de medición en milisegundos
sample-interval-overruns	El número de veces que el sistema de medición estuvo demasiado ocupado como para escribir datos en el disco
sample-interval-secs	Tiempo entre las muestras de medición en segundos
Tcp-conn-aborts	Número de conexiones abortadas, por ejemplo un clic en “stop” en el navegador de Internet.
Tcp-conn-aborts%	Porcentaje de conexiones TCP abortadas, tcp-conn-aborts / tcp-conn-exits
Tcp-conn-exits	Número de conexiones TCP finalizadas
Tcp-conn-inits	Número de conexiones TCP iniciadas
Tcp-conn-self-denies	Número de conexiones TCP denegadas por políticas de descarte ó control de admisión
Tcp-conn-self-denies%	Porcentaje de conexiones TCP denegadas, tcp-conn-self-denies / tcp-conn-exits
tcp-conn-server-ignores	Número de conexiones TCP ignoradas por un servidor, este conteo se incrementa cuando PacketShaper implementa Rechazo de Servicio (DoS).
tcp-conn-server-ignores%	Porcentaje de conexiones TCP ignoradas, tcp-conn-server-ignores / tcp-conn-exits
Tcp-conn-server-refuses	Número de conexiones TCP rechazadas por un servidor
tcp-conn-server-refuses%	Porcentaje de conexiones TCP rechazadas, tcp-conn-server-refuses / tcp-conn-exits
Tcp-data-pkts	Conteo de paquetes de datos TCP, incluyendo retransmisiones
Tcp-early-retx-toss-pkts	Conteo de retransmisiones TCP desechadas, esto lo controla PacketShaper
tcp-early-retx-toss-pkts%	Tasa de retransmisiones TCP desechadas, tcp-early-retx-toss-pkts / tcp-early-retx-toss-pkts + tcp-retx-pkts
Tcp-efficience%	Porcentaje de bytes de datos TCP buenos, no retransmitidos
Tcp-retx-bytes	Conteo de bytes TCP retransmitidos
tcp-retx-pkts	Conteo de paquetes TCP retransmitidos, excluyendo los

	desechados
Tcp-retx-pkts%	Tasa de retransmisión TCP, tcp-retx-pkts / tcp-data-pkts
Variables de Enlace "link"	
hostdb-alloc-fails	Conteo de fallas de asignación de computador
ipdg-alloc-fails	Conteo de fallas de asignación UDP
link-size-bps	Tamaño del enlace configurado
Pkt-size-histogram	Histograma de número de paquetes recibidos en baldes (buckets) de tamaños diferentes. Los baldes de tamaños de paquete en bytes incluye: [0-63], [64-127], [128-255], [256-511], [512-1023], [1024-1517], [>=1518]
rx-errors	Conteo de paquetes recibidos que fueron desechados debido a errores de hardware
rx-no-buffers	Conteo de paquetes que fueron desechados debido a memoria intermedias (buffers) no disponibles
rx-pkts-dropped	Conteo total de paquetes recibidos que fueron desechados
Tcp-alloc-fails	Conteo de fallas de asignación TCP
total-rx-pkts	Número total de paquetes recibidos, no incluye paquetes desechados
total-tx-pkts	Número total de paquetes transmitidos, no incluye paquetes desechados
tx-errors	Conteo de paquetes transmitidos que fueron desechados debido a errores de hardware
tx-pkts-dropped	Conteo total de paquetes transmitidos que fueron desechados
unsolicited-icmp	Rechazo de Servicio (DoS), detecta una respuesta ICMP cuando no hubo una petición
Variables de Partición "partition"	
dynamic-cap-count	Número de flujos que se les dio control de admisión por parte de la partición dinámica porque ya tenía el número máximo de usuarios
dynamic-live-user	Número pico de usuarios activos en una partición dinámica durante el intervalo de medición
dynamic-no-partition-count	Número de flujos que fueron denegados porque PacketShaper ha llegado al número máximo de particiones y no puede crear más
lowest-fully-satisfied-priority	Nivel de tráfico de prioridad más baja que podría obtener exceso de ancho de banda
partition-burst-limit-bps	Límite de incremento explosivo de velocidad (burst) configurado para la partición, es el mismo que la partición si no se ha seleccionado "burst"
partition-over-limit-msecs	Tiempo acumulativo en el que el ancho de banda asignado excedió el tamaño mínimo de la partición, en milisegundos
partition-over-limit-secs	Tiempo acumulativo en el que el ancho de banda asignado excedió el tamaño mínimo de la partición, en segundos
partition-over-limit-time%	Porcentaje de tiempo que el ancho de banda asignado excedió el tamaño mínimo de la partición, partition-over-limit-msecs / sample-interval-msecs
partition-size-bps	Tamaño mínimo configurado de la partición
pvc-avg-bps	Tasa en bps basado en pvc-bytes sobre el intervalo
pvc-bytes	Número de bytes enviados o recibidos en el Circuito Virtual

	Permanente (PVC)
pvc-avg-fps	Tasa de grupos de bits (frames) por segundo
pvc-ecn-frames	Número de grupos de bits que tienen Notificación de Congestión hacia Adelante/Atrás (FECN/BECN)
pvc-ecn-frames%	Porcentaje de grupos de bits con notificación de congestión hacia adelante/atrás
pvc-frames	Número de grupos de bits en el intervalo
pvc-target-bps	Tasa objetivo promedio para el circuito virtual permanente
Variables de Clase "class"	
avg-round-trip-time	Número promedio de milisegundos que un paquetes toma para ir desde un cliente a un servidor y regresar nuevamente
class-hits	Conteo de "hits" de una clase
client-flood-block	Número de flujos que fueron bloqueados debido a que un cliente (inicia el flujo) excedió la tasa límite de flujo límite especificada para Rechazo de Servicio (DoS)
conn-speed-hist	Histograma de velocidad sobre velocidades bien conocidas. Este histograma provee un perfil de uso, por ejemplo, para módems telefónicos versus módems de alta velocidad. Estos datos son grabados sólo para conexiones de Protocolo de Transferencia de Archivos (FTP) e HiperTexto (HTTP).
license-overflows	Conteo de número de flujos que habrían excedido las licencias que son un número máximo de sesiones en una clase y se configura mediante línea de comandos
licenses-peak	El valor más grande de licencias en uso durante el intervalo
licenses-total	El valor límite de licencias en el final del intervalo
network-delay-avg	Número promedio de milisegundos que los paquetes de transacción de la clase consumieron en tránsito (retardo).
network-delay-histogram	Histograma del número de milisegundos que los paquetes de transacción de la clase consumieron en tránsito. Cada histograma contiene una tabla de datos donde el índice representa el límite más bajo de una rango de tiempo en milisegundos: [25000], [10000], [5000], [2500], [1000], [750], [500], [250], [100], [75], [50], [25], [10], [0]. Las celdas de la tabla contienen el número de transacciones cuyo tiempo de retardo baja junto con el rango representado por el índice
network-delay-median	Número medio de milisegundos que los paquetes de transacción de la clase consumieron en tránsito
network-delay-msec	La suma de los retardos de red en milisegundos de todas las transacciones en el intervalo especificado.
peak-ipdg-conns	Número pico de flujos UDP concurrentes
policy-hits	Conteo de "hits" de política
round-trip-time-msecs	La suma de Tiempos de Viaje Redondo (RTT) de todas las transacciones en el intervalo especificado, medido en milisegundos. Esta medida es tomada una por transacción y no una por paquete
server-delay-avg	Número promedio de milisegundos requerido por los servidores para procesar las peticiones de transacción de la clase. El tiempo empieza cuando el servidor ha recibido todos los paquetes de petición requeridos y finaliza cuando el

	servidor emite el primer paquete de respuesta
server-delay-histogram	Histograma del número de milisegundos requerido por los servidores para procesar las peticiones de transacción de la clase.
server-delay-median	Número medio de milisegundos requerido por los servidores para procesar las peticiones de transacción de la clase
server-delay-msec	La suma de los retardos del servidor de todas las transacciones en el intervalo específico
server-flood-block	Número de flujos que fueron bloqueados debido a que un servidor (destino del flujo) excedió la tasa límite de flujo límite especificada para rechazo de servicio (DoS)
service-level%	Porcentaje de transacciones que satisficieron sus requerimiento de desempeño, es decir transacciones suficientemente rápidas
service-level-errors	Número de intervalos de un minuto que no tienen el porcentaje requerido de transacciones rápidas
service-level-threshold%	Máximo porcentaje de transacciones lentas que cada intervalo de un minuto puede tener y todavía ser considerado intervalo aceptable
slow-transactions	Número de transacciones lentas
total-delay-avg	Número promedio de milisegundos para completar las transacciones de la clase, incluye retardos de servidor y red (retardo total)
total-delay-histogram	Histograma del número de milisegundos requeridos para completar las transacciones de la clase
total-delay-median	Número medio de milisegundos requeridos para completar las transacciones de la clase
total-delay-msec	La suma de los retardos de todas las transacciones en el intervalo específico, medido en milisegundos
total-delay-threshold	Número de milisegundos que se dice es “demasiado lento” para un retardo total (umbral)
total-trans	Número de transacciones, pares de petición y respuesta
trans-bytes	Tamaño de la transacción para aplicaciones basadas en TCP
Trans-bytes-avg	Número promedio de bytes por transacción, trans-bytes / total-trans
web-response-2XX	Número de mensajes de respuesta del Protocolo de Transferencia de HiperTexto (HTTP) con códigos de suceso 2XX, por ejemplo 200 “OK” y 201 “Created”
web-response-3XX	Número de mensajes de respuesta HTTP con códigos de suceso 3XX, por ejemplo 301 “Moved” y 302 “Found”
web-response-4XX	Número de mensajes de respuesta HTTP con códigos de suceso 4XX, por ejemplo 400 “Bad Request” y 404 “Not Found”
web-response-5XX	Número de mensajes de respuesta HTTP con códigos de suceso 5XX, por ejemplo 501 “Not Implemented” y 502 “Timed out”

Tabla. 3.2. Variables de medición.

Se selecciona en que orden se presentarán las estadísticas, luego se selecciona el intervalo de tiempo del que se desea obtener las estadísticas. Los modelos PacketShaper 1500 guardan datos de un día con intervalos de muestras de un minuto y guarda datos de aproximadamente 8 días con intervalos de muestras de una hora.

El paso final para obtener los datos es elegir “fetch data”, se muestra los valores separados por comas en el navegador, como se observa en la Figura 3.11. También se puede elegir “download” para guardar en un archivo con extensión “csv” en la ruta que se ingrese.

```
"link:/Inbound"
"time","avg-bps","bytes"
"03-Oct-2001 13:12:00",66704,500282
"03-Oct-2001 13:11:00",27607,207050
"03-Oct-2001 13:10:00",41959,314696
"03-Oct-2001 13:09:00",2323,17426
"03-Oct-2001 13:08:00",98,735
"03-Oct-2001 13:07:00",381,2859
"03-Oct-2001 13:06:00",85,641
"03-Oct-2001 13:05:00",123,924
"03-Oct-2001 13:04:00",261,1960
"03-Oct-2001 13:03:00",98,735
"03-Oct-2001 13:02:00",104,782
"03-Oct-2001 13:01:00",216,1617
"03-Oct-2001 13:00:00",98,735
"03-Oct-2001 12:59:00",104,782
"03-Oct-2001 12:58:00",241,1805
"03-Oct-2001 12:57:00",85,641
"03-Oct-2001 12:56:00",85,641
"03-Oct-2001 12:55:00",275,2063
"03-Oct-2001 12:54:00",112,843
"03-Oct-2001 12:53:00",148,1112
"03-Oct-2001 12:52:00",381,2859
"03-Oct-2001 12:51:00",92,688
"03-Oct-2001 12:50:00",85,641
"03-Oct-2001 12:49:00",334,2503
"03-Oct-2001 12:48:00",104,782
"03-Oct-2001 12:47:00",1032,7743
"03-Oct-2001 12:46:00",172,1288
"03-Oct-2001 12:45:00",3169,23764
"03-Oct-2001 12:44:00",862,6466
"03-Oct-2001 12:43:00",894,6707
"03-Oct-2001 12:42:00",3689,27667
```

Figura. 3.11. Presentación de estadísticas.

3.3.6.3.2 Reportes gráficos.

Para observar los reportes gráficos se elige la ficha "manage", se elige "statistics" y se escoge "graph", aparece una ventana como se observa en la Figura 3.12.

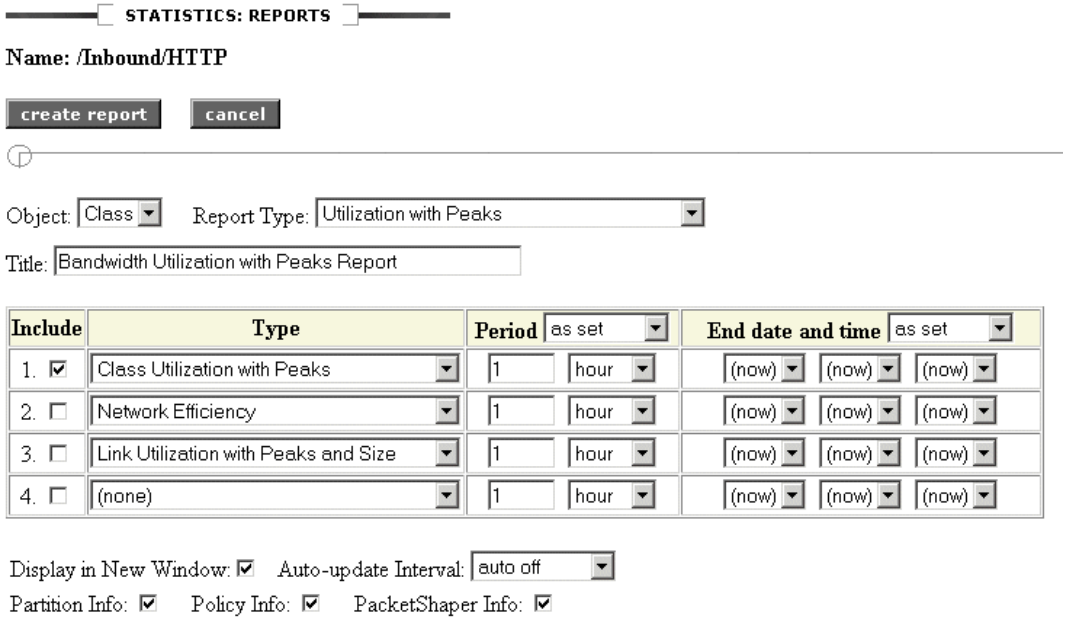


Figura. 3.12. Creando reportes gráficos.

Se elige el objeto, se selecciona el tipo de reporte gráfico en "Report Type", se puede graficar además la estadísticas de las variables de medición en los cuatro campos siguientes seleccionando el tipo de gráfico y el intervalo del que se obtendrán los datos. Se puede seleccionar opciones de información de políticas y particiones aplicadas al objeto. Los diferentes tipos de reportes gráficos que se obtienen con PacketShaper se detallan a continuación:

- *Average Transaction Size Graph.-* Es un gráfico que muestra el tamaño de transacción promedio de una aplicación basada en TCP. Este gráfico está disponible solamente si las Medidas de Tiempo de Respuesta (RTM) está disponible para el objeto seleccionado y se observa en la Figura 3.13.

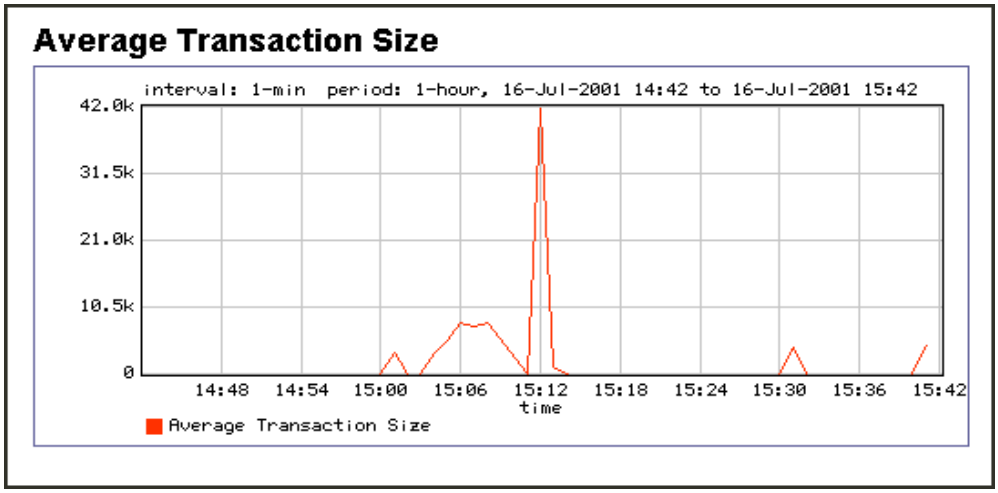


Figura. 3.13. Gráfico del tamaño de transacción promedio.

- *Bytes Transmitted Graph.-* Es un gráfico que compara el número de bytes retransmitidos para el objeto seleccionado y se observa en la Figura 3.14.

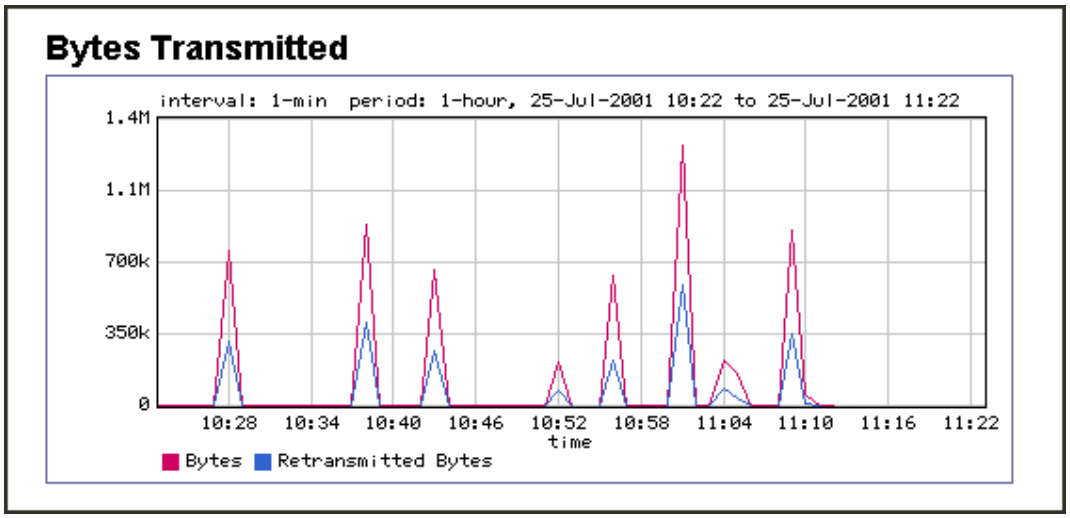


Figura. 3.14. Gráfico del número de bytes transmitidos.

- *Class utilization with Peaks Graph.-* Es un gráfico que muestra el consumo de ancho de banda pico y promedio de una clase de tráfico sobre el tiempo, se lo obtiene desde la ficha “top ten” y se observa en la Figura 3.15.

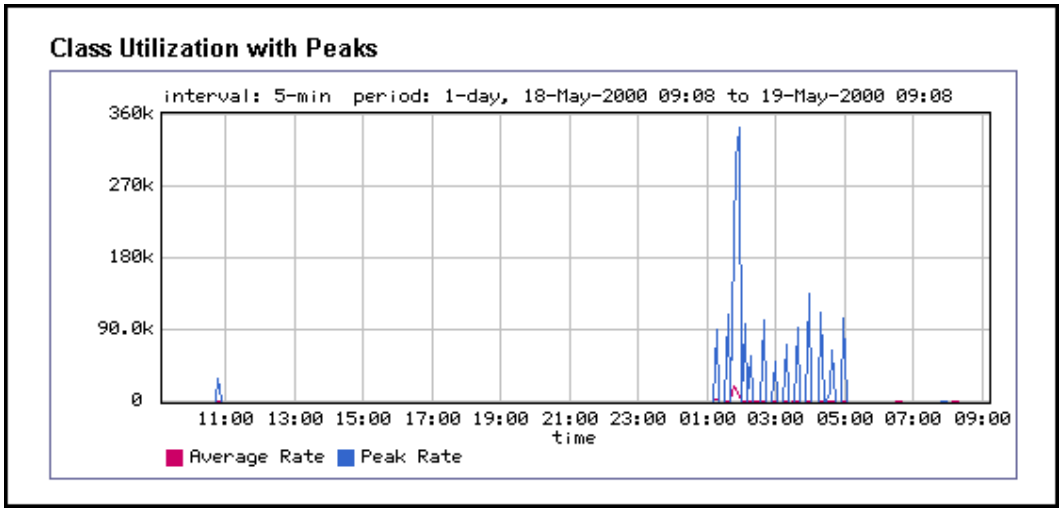


Figura. 3.15. Gráfico de la utilización de una clase con picos.

- *Class Utilization Graph.*- Es un gráfico que muestra una historia del consumo del ancho de banda promedio de una clase, es un gráfico similar al de la Figura 3.15.

- *Connection Retransmissions Graph.*- Es un gráfico que muestra la tasa de retransmisión de TCP con la tasa de desecho de TCP de un objeto y se observa en la Figura 3.16.

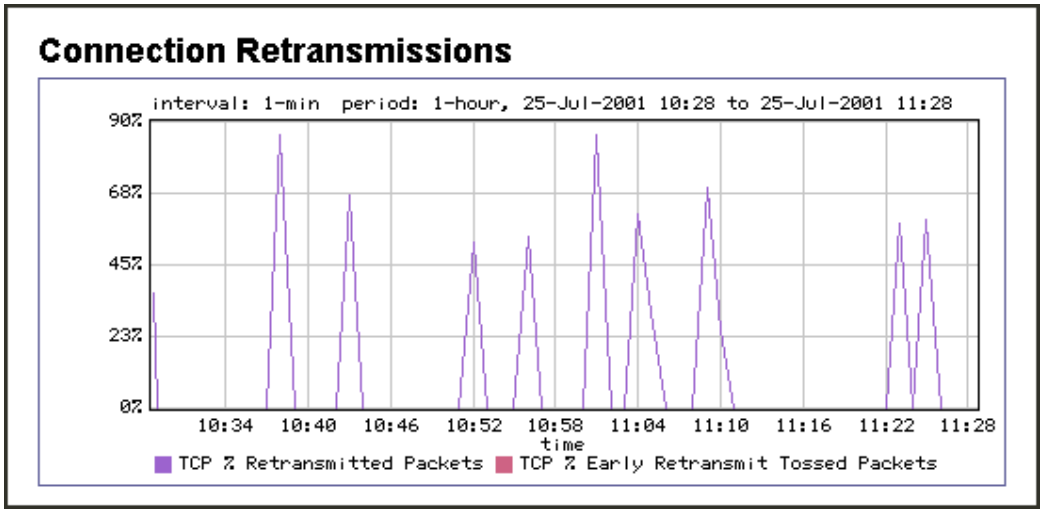


Figura. 3.16. Gráfico del tamaño de la tasa de retransmisión de TCP.

- *Dynamic Partition Usage.-* Es un gráfico que muestra estadísticas de uso perteneciente a una partición dinámica y se observa en la Figura 3.17.

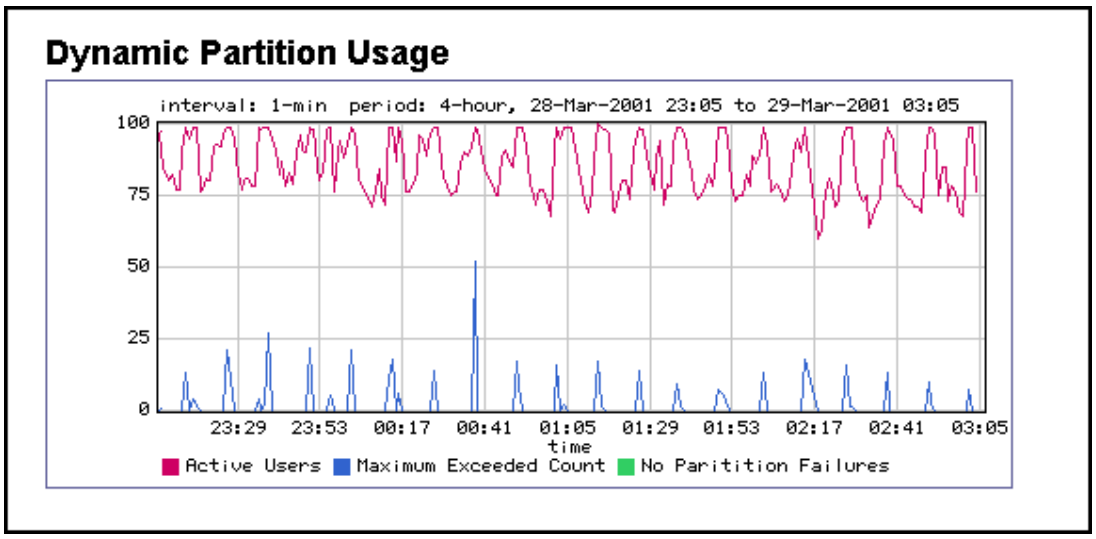


Figura. 3.17. Gráfico del uso de una partición dinámica.

- *Guaranteed Rate Failures Graph.-* Es un gráfico que muestra una historia del número de veces que PacketShaper no pudo proveer el ancho de banda garantizado en una política de clase y se observa en la Figura 3.18.

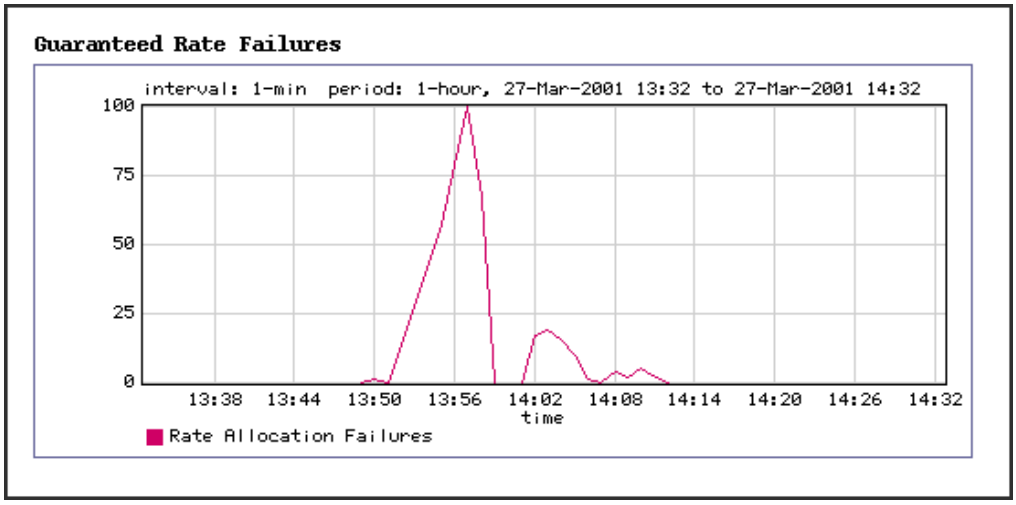


Figura. 3.18. Gráfico del número de veces que no se pudo garantizar tasa.

- *Link Utilization with Peaks and Size Graph.*- Es un gráfico que muestra el uso del ancho de banda pico y promedio de un enlace, muestra también la capacidad del enlace y se observa en la Figura 3.19.

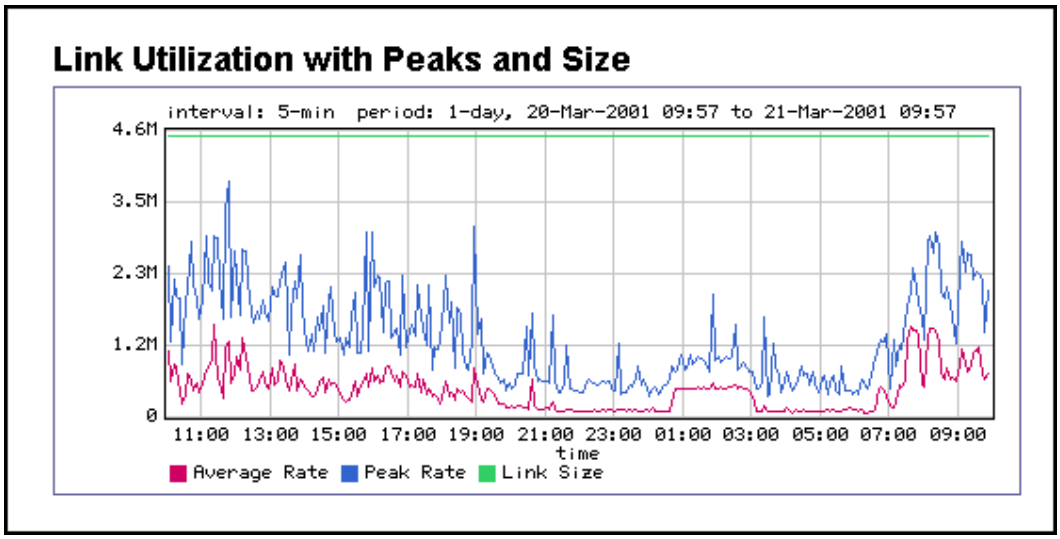


Figura. 3.19. Gráfico del uso del ancho de banda pico y promedio de un enlace.

- *Link Utilization with Peaks Graph.*- Es un gráfico similar al de la Figura 3.19., muestra el uso del ancho de banda pico y promedio de un enlace en bits por segundo, no muestra la capacidad del enlace.

- *Link Utilization and Size Graph.*- Es un gráfico similar al de la Figura 3.19., muestra el uso de ancho de banda promedio de un enlace en bits por segundo, muestra también el tamaño del enlace.

- *Network Delay Graph.*- Es un gráfico que muestra los tiempos de respuesta promedio en milisegundos de una clase de tráfico sobre el tiempo. Este gráfico muestra solamente la porción de tiempo de transacción correspondiente a la red, permitiendo analizar el retardo de la red. Este gráfico está disponible solamente si las Medidas de Tiempo de Respuesta (RTM) está disponible para el objeto seleccionado y se observa en la Figura 3.20.

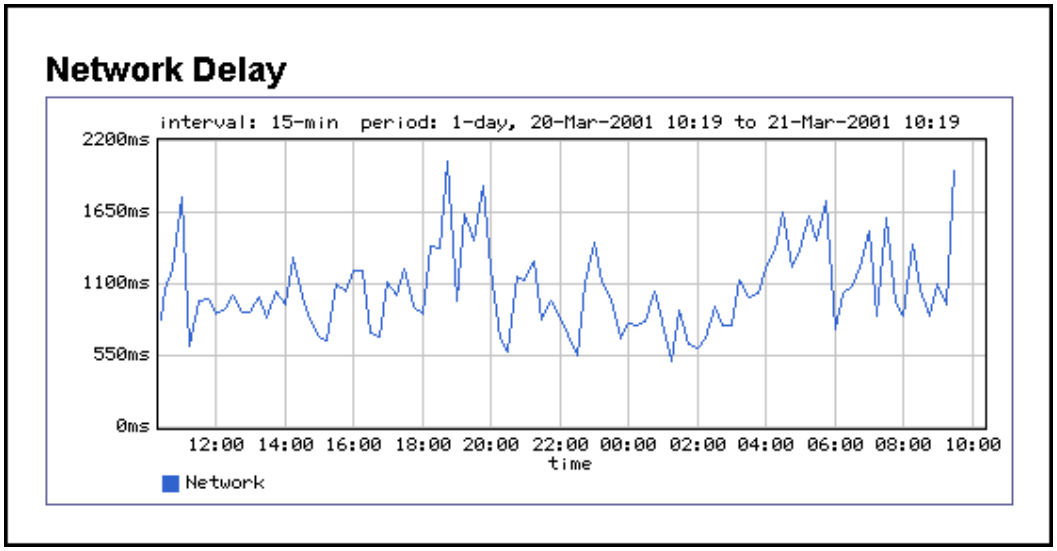


Figura. 3.20. Gráfico del retardo de red.

- *Network Delay Distribution.*- Es un gráfico que muestra un histograma del número de transacciones cuyo retardo de red cae dentro de los 14 baldes (buckets) de tiempo de transacción del eje horizontal del gráfico. Además el retardo medio es mostrado en la parte inferior del gráfico, este gráfico está disponible solamente si las Medidas de Tiempo de Respuesta (RTM) está disponible para el objeto seleccionado y se observa en la Figura 3.21.

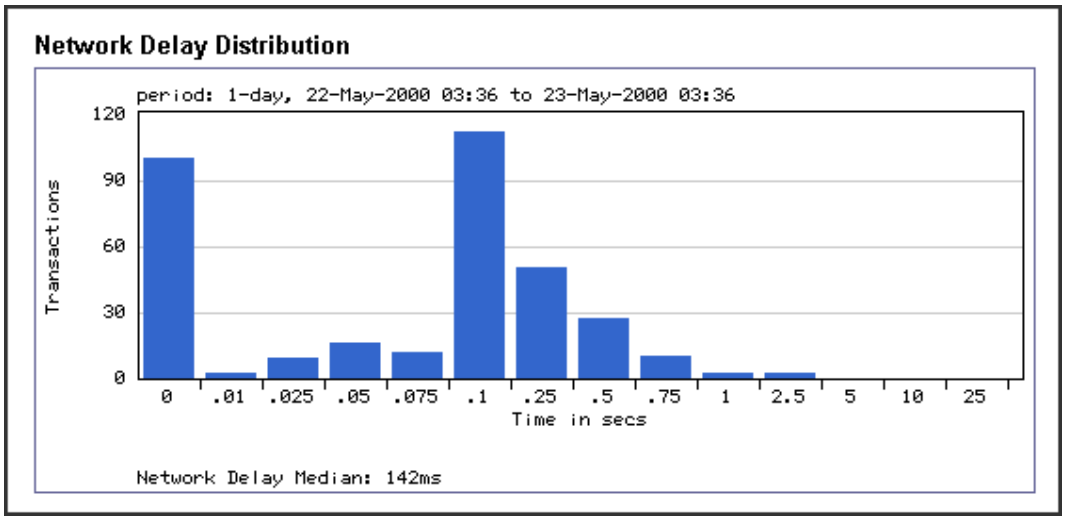


Figura. 3.21. Gráfico de la distribución del retardo de red.

- *Network Efficiency Graph.*- Es un gráfico que muestra la cantidad de tráfico TCP desperdiciado, mostrando el porcentaje de bytes que son transmitidos, además muestra la variable tcp-data-bytes como porcentaje y se calcula como [bytes - tcp-retx-bytes] / bytes y se observa en la Figura 3.22.

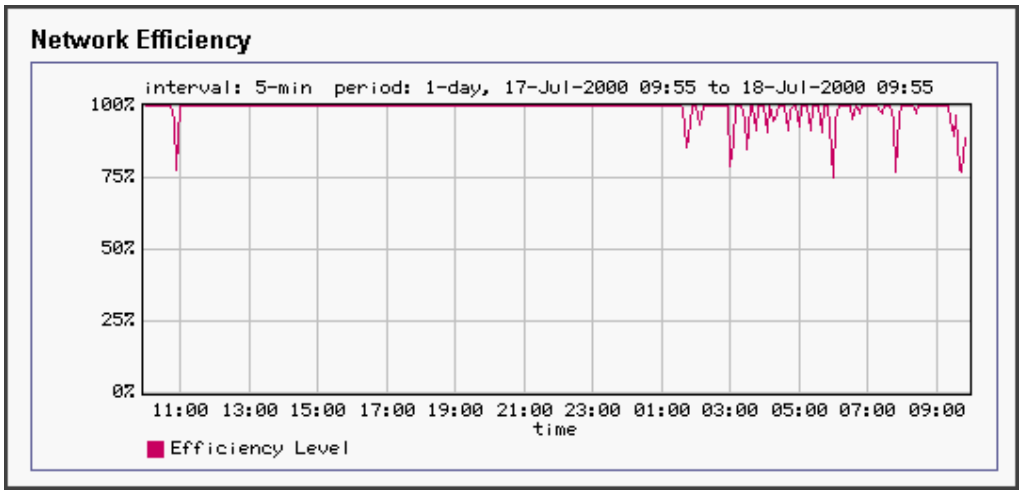


Figura. 3.22. Gráfico de eficiencia de la red.

- *Packet Round-Trip Time Graph.*- Es un gráfico que muestra el Tiempo de Viaje Redondo (RTT) de una transacción, es el número promedio de milisegundos gastados en el intercambio del bit SYN y su correspondiente reconocimiento (ACK) que realiza el protocolo TCP entre un cliente y el servidor, se calcula para un solo paquete de una transacción y se observa en la Figura 3.23.

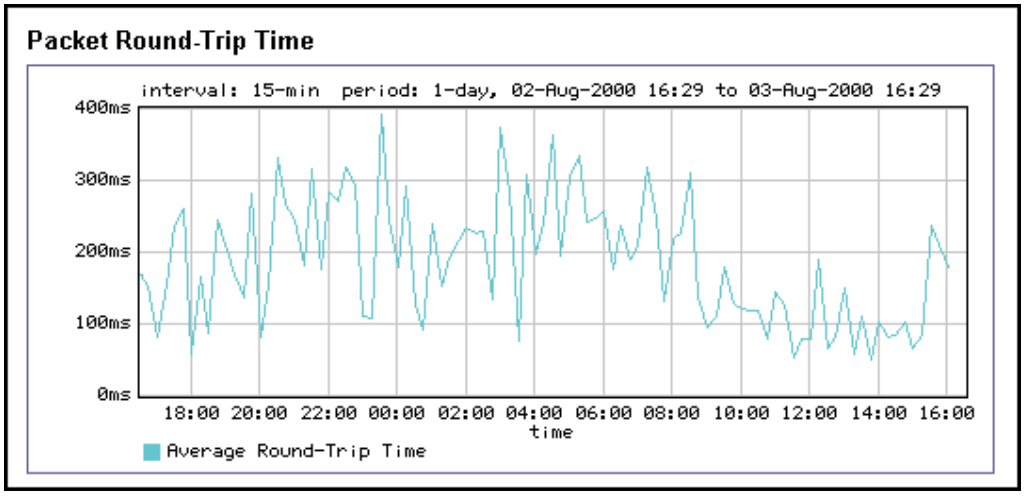


Figura. 3.23. Gráfico de Tiempo de Viaje Redondo (RTT).

- *Packet Size Distribution Graph.*- Es un gráfico que muestra un histograma de paquetes recibidos en el enlace "inbound" u "outbound", basado en tamaños de baldes (buckets) de la variable de medición pkt-size-histogram, es un gráfico similar al de la Figura 3.21.

- *Packets Transmitted Graph.*- Es un gráfico que muestra una comparación entre el número de paquetes transmitidos y retransmitidos para el objeto seleccionado, excluye paquetes desechados, se observa en la Figura 3.24.

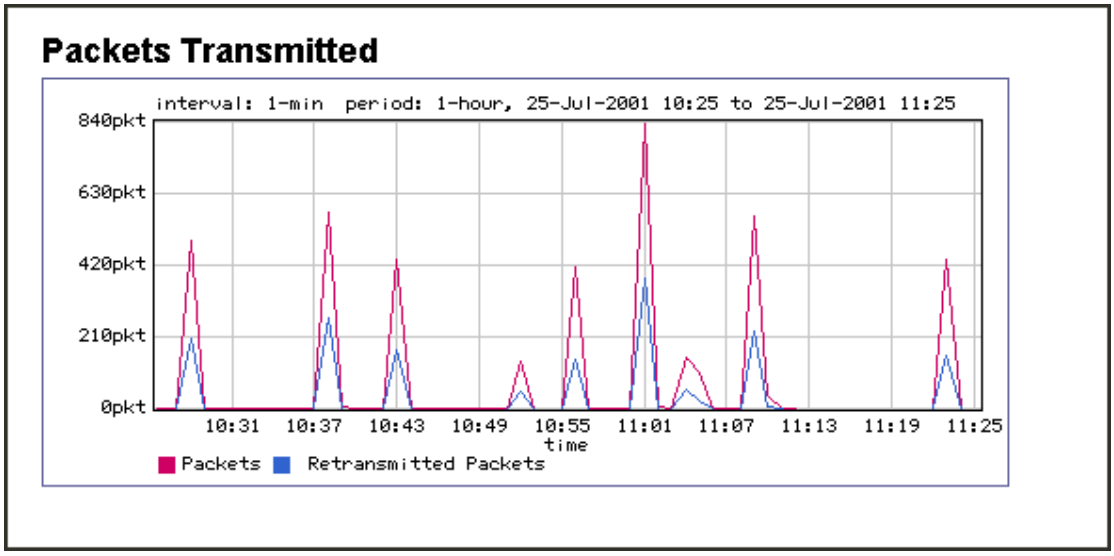


Figura. 3.24. Gráfico de paquetes transmitidos y retransmitidos.

- *Partition Utilization and Size Graph.-* Es un gráfico que muestra el uso del ancho de banda pico y promedio de una partición en bits por segundo, muestra el tamaño de la partición y su límite de incremento explosivo de velocidad (burst), se observa en la Figura 3.25.

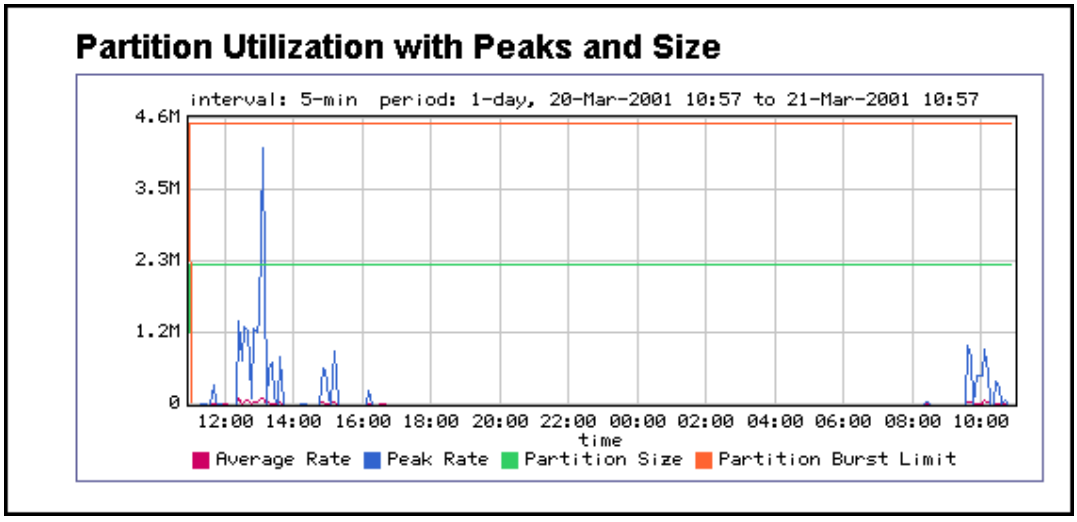


Figura. 3.25. Gráfico de tamaño y utilización de una partición.

- *Partition Utilization with Peaks Graph.*- Es un gráfico similar a la Figura 3.25., muestra el uso del ancho de banda pico y promedio de una partición en bits por segundo, no muestra el tamaño de la partición ni su límite de incremento explosivo de velocidad.

- *Partition Utilization and Size Graph.*- Es un gráfico similar a la Figura 3.25., muestra el uso del ancho de banda promedio de una partición en bits por segundo, muestra el tamaño de la partición y su límite de incremento explosivo de velocidad.

- *Server Delay Graph.*- Es un gráfico que muestra los tiempos de respuesta promedio en milisegundos de una clase de tráfico sobre el tiempo. Este gráfico muestra solamente la porción de tiempo de transacción correspondiente al servidor, permitiendo analizar el retardo del servidor. Este gráfico está disponible solamente si las Medidas de Tiempo de Respuesta (RTM) está disponible para el objeto seleccionado, es un gráfico similar al de la Figura 3.20.

- *Server Delay Distribution Graph.*- Es un gráfico que muestra el número de transacciones cuyo retardo de servidor cae dentro de los 14 baldes de tiempo de transacción del eje horizontal del gráfico. Además el retardo medio es mostrado en la parte inferior del gráfico, este gráfico está disponible solamente si las medidas de tiempo de respuesta está disponible para el objeto seleccionado, es un gráfico similar al de la Figura 3.21.

- *Service Level Compliance.*- Es un gráfico que muestra el umbral (threshold) fijado en las Medidas de Tiempo de Respuesta (RTM) como transacciones buenas, muestra mediciones de tiempos de respuesta para clases de tráfico, es decir el porcentaje actual de transacciones buenas. Este gráfico está disponible solamente si las medidas de tiempo de respuesta está disponible para el objeto seleccionado y se observa en la Figura 3.26.

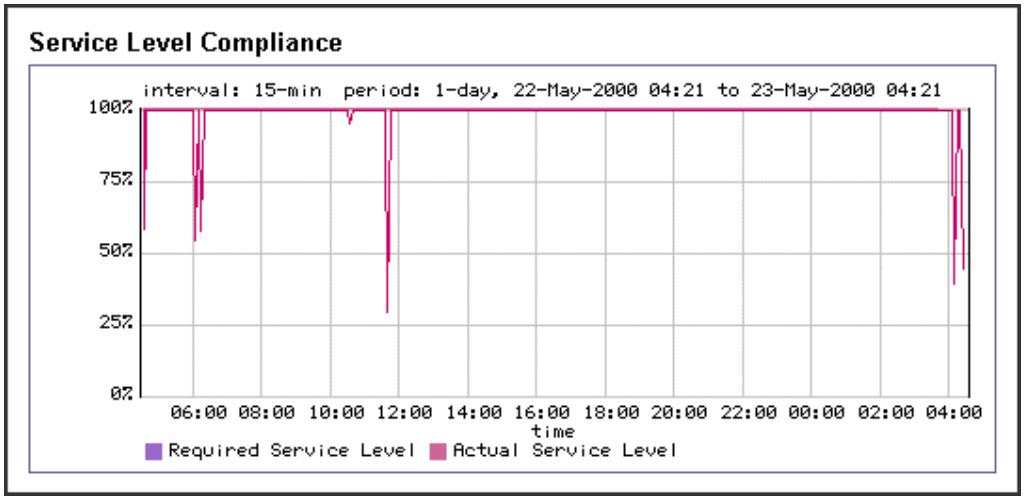


Figura. 3.26. Gráfico de cumplimiento de nivel de servicio.

- *TCP Connections Initiated Graph.*- Es un gráfico que muestra el número de conexiones TCP iniciadas en un período de tiempo específico y se observa en la Figura 3.27.

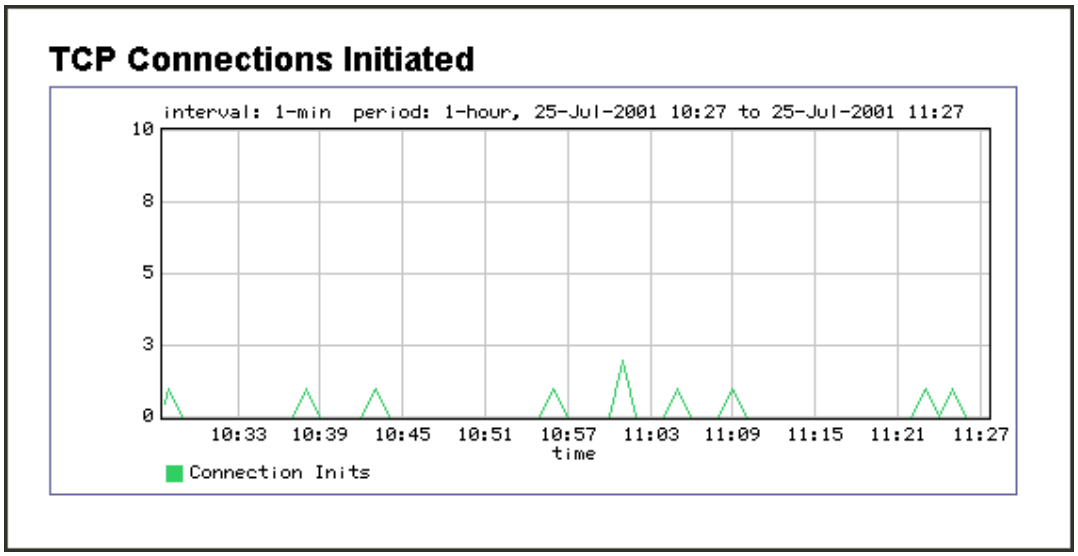


Figura. 3.27. Gráfico de conexiones TCP iniciadas.

- *TCP Health Graph.*- Es un gráfico que muestra el estado de las conexiones TCP para un objeto. Compara el número de conexiones TCP que fueron iniciadas,

abortadas, ignoradas o rechazadas por un servidor durante un período de tiempo específico, como se observa en la Figura 3.28.

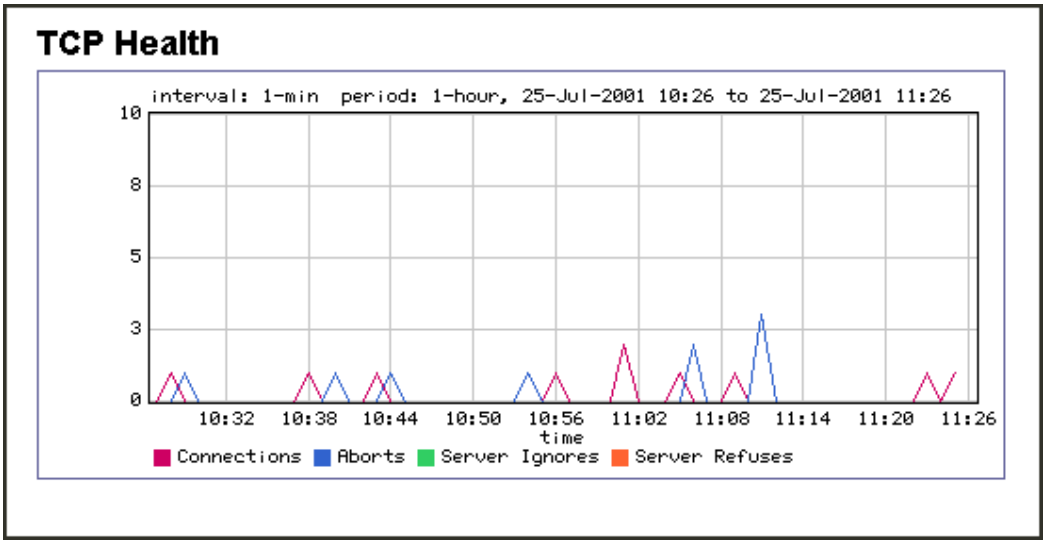


Figura. 3.28. Gráfico del estado de las conexiones TCP.

- *Top 10 Classes Graph.*- Es un gráfico tipo pastel que muestra las porciones relativas de ancho de banda asignado a las diez clases más activas, como se observa en la Figura 3.29.

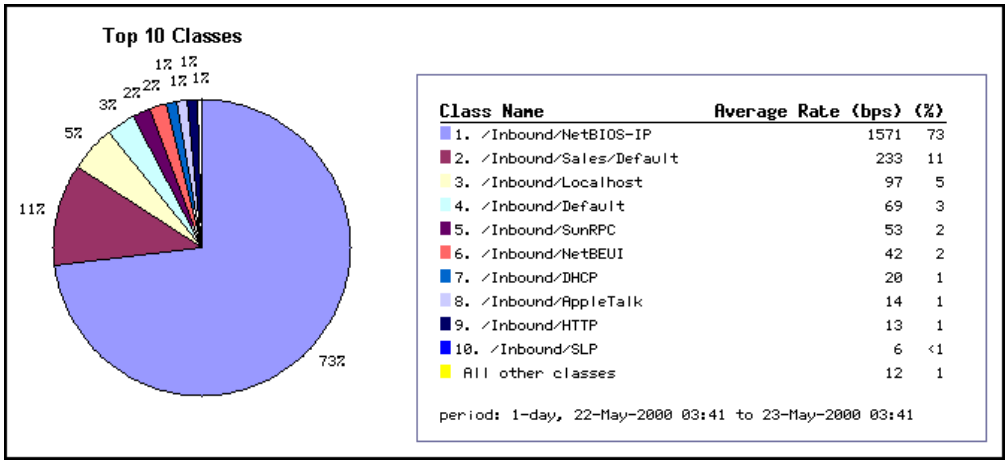


Figura. 3.29. Gráfico tipo pastel de las 10 clases más activas.

- *Top 10 Partitions Graph.*- Es un gráfico tipo pastel similar a la Figura 3.29., que muestra las porciones relativas de ancho de banda asignado a las diez particiones más activas.

- *Transaction Delay Graph.*- Es un gráfico que muestra los tiempos de respuesta promedio en milisegundos de una clase de tráfico sobre el tiempo. Este gráfico muestra las porciones de tiempos de transacción correspondientes a la red y servidor, además muestra el umbral de retardo total, este gráfico está disponible solamente si las Medidas de Tiempo de Respuesta (RTM) está disponible para el objeto seleccionado y se observa en la Figura 3.30.

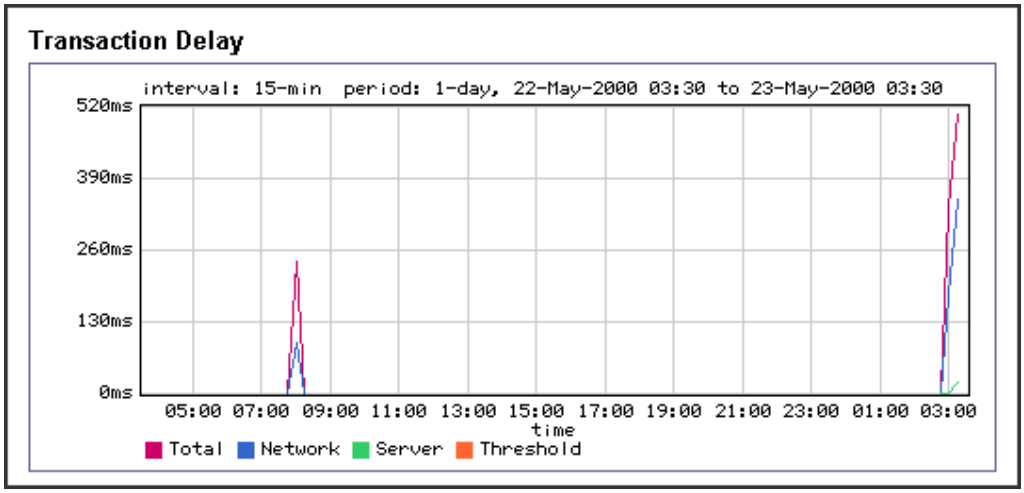


Figura. 3.30. Gráfico de retardo de transacción.

- *Transaction Delay Distribution Graph.*- Es un gráfico que muestra un histograma de retardos de red, servidor y total que caen dentro de los 14 baldes (buckets) de tiempo de transacción del eje horizontal del gráfico. Además el retardo medio total es mostrado en la parte inferior del gráfico, este gráfico está disponible solamente si las medidas de tiempo de respuesta está disponible para el objeto seleccionado, es un gráfico similar al de la Figura 3.21.

Algunos de los gráficos anteriores se obtienen automáticamente al elegir la ficha "report" en el navegador web. Además se puede también realizar reportes gráficos de tasa

y/o tiempos de respuesta pero de múltiples clases, para esto se elige la ficha “reports”, se elige “create report” y aparece una ventana como se observa en la Figura 3.31.

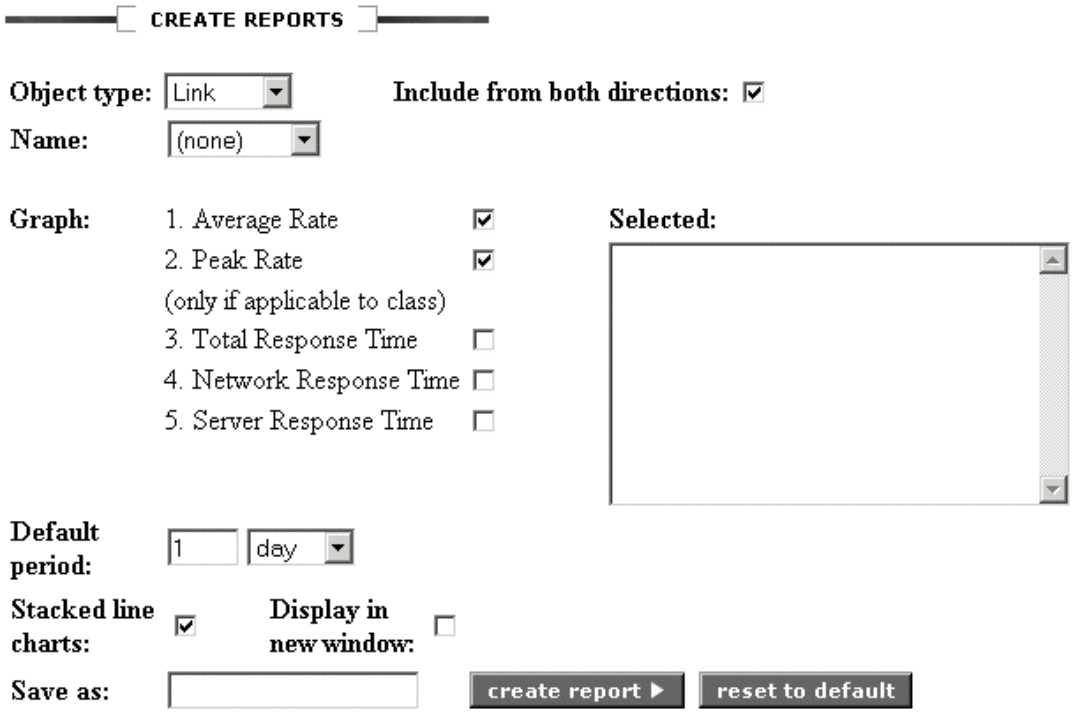
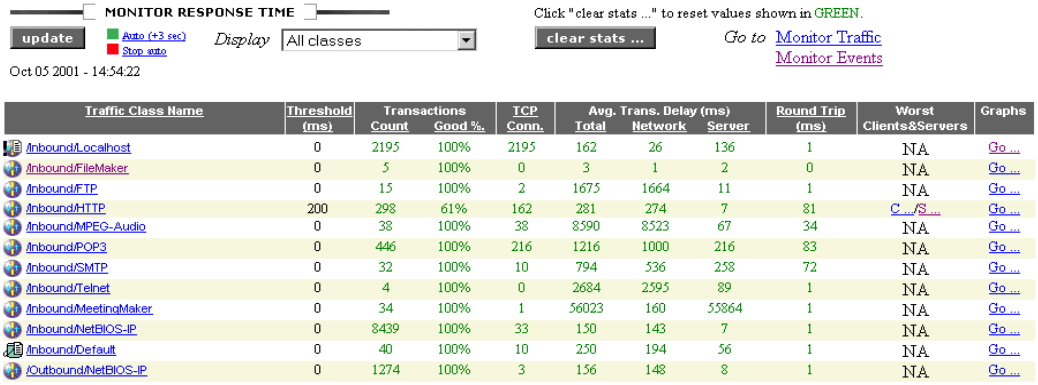


Figura. 3.31. Creando otros reportes gráficos.

Se selecciona el objeto en “Object type”, si se desea se selecciona “Include from both direction” para crear gráficos de “inbound” y “outbound”, se selecciona los tipos de gráficos que se desea crear, se elige un período de tiempo y se escoge otras opciones como graficar en una nueva ventana separados los gráficos por líneas y guardarlos.

3.3.6.3.3 Medidas de Tiempo de Respuesta (RTM).

Permite medir la calidad que experimentan los usuarios de la red, provee estadísticas de desempeño, umbrales de monitoreo, indicadores de problemas de alto nivel y gráficos de desempeño. Para monitorear las medidas de tiempo de respuesta se elige la ficha “monitor”, se elige “Monitor Response Time” y aparece una ventana como se observa en la Figura 3.32.



Traffic Class Name	Threshold (ms)	Transactions Count	Transactions Good %.	TCP Conn.	Avg. Trans. Delay (ms) Total	Avg. Trans. Delay (ms) Network	Avg. Trans. Delay (ms) Server	Round Trip (ms)	Worst Clients&Servers	Graphs
/Inbound/Localhost	0	2195	100%	2195	162	26	136	1	NA	Go ...
/Inbound/FileMaker	0	5	100%	0	3	1	2	0	NA	Go ...
/Inbound/FTP	0	15	100%	2	1675	1664	11	1	NA	Go ...
/Inbound/HTTP	200	298	61%	162	281	274	7	81	C .../S ...	Go ...
/Inbound/MPEG-Audio	0	38	100%	38	8590	8523	67	34	NA	Go ...
/Inbound/POP3	0	446	100%	216	1216	1000	216	83	NA	Go ...
/Inbound/SMTP	0	32	100%	10	794	536	258	72	NA	Go ...
/Inbound/Telnet	0	4	100%	0	2684	2595	89	1	NA	Go ...
/Inbound/MeetingMaker	0	34	100%	1	56023	160	55864	1	NA	Go ...
/Inbound/NetBIOS-IP	0	8439	100%	33	150	143	7	1	NA	Go ...
/Inbound/Default	0	40	100%	10	250	194	56	1	NA	Go ...
/Outbound/NetBIOS-IP	0	1274	100%	3	156	148	8	1	NA	Go ...

Figura. 3.32. Ventana de Medidas de Tiempo de Respuesta (RTM).

Se muestra una lista de las clases con las diferentes mediciones, algunas de las cuales se resumen también en la Tabla 3.2., las medidas de tiempo de respuesta son “Traffic Class Name”, “Threshold (ms)” que es un umbral aceptable de retardo y se puede configurar, “Transactions count”, “Transactions Good%”, “TCP Conn”, “Avg. Trans. Delay (ms)” que es el retardo total, “Round Trip (ms)” que es el tiempo de viaje redondo, “Worst Clients & Servers” que son enlaces a una lista con los clientes y servidores que presentan problemas respecto a umbrales, “Graphs” que es un enlace a tipos de gráficos de tiempos de respuesta descritos anteriormente.

Se puede analizar los tiempos de respuesta, es decir los retardos y configurar los umbrales máximos eligiendo la ficha “manage”, se elige “statics” y se escoge “response time”, aparece una ventana como se observa en la Figura 3.33.

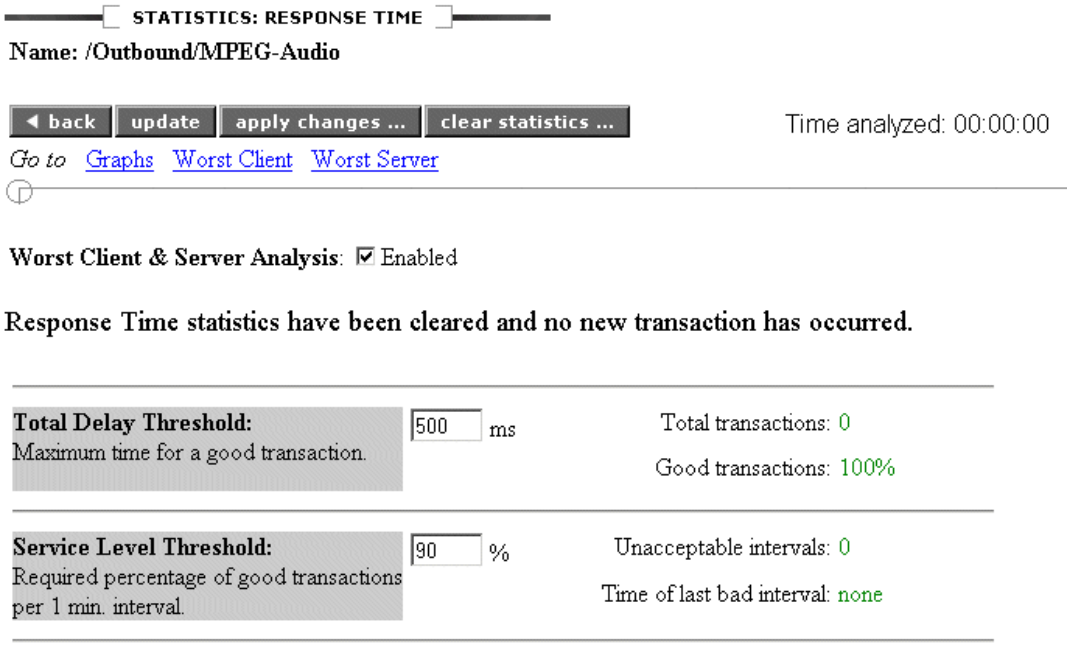
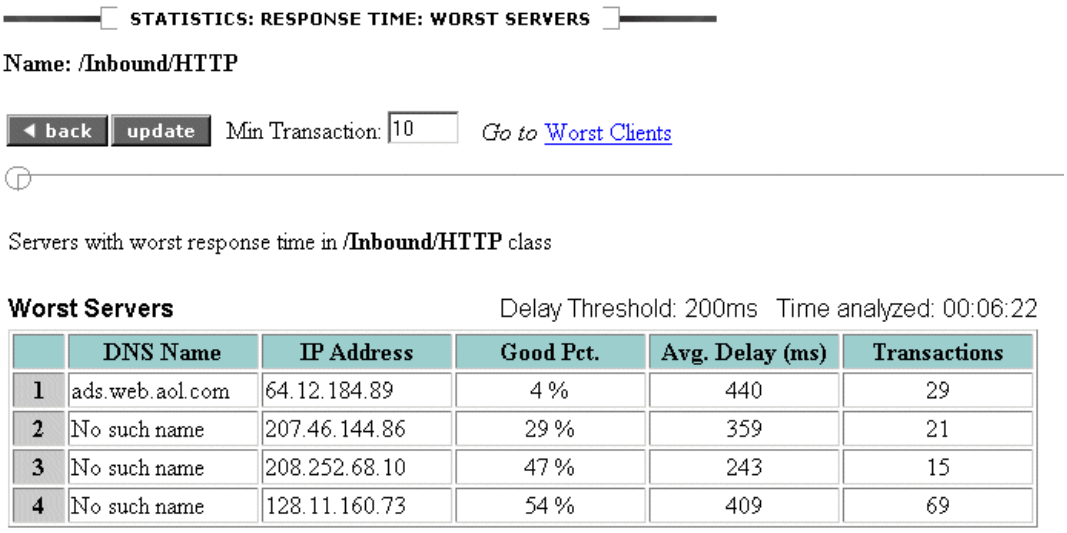


Figura. 3.33. Configurando umbrales para las medidas de tiempo de respuesta.

En esta ventana se observa los retardos total, de red y servidor, además se fija los umbrales (thresholds) permitidos, se ingresa "Total Delay Threshold" para indicar cual es el tiempo máximo para considerar a una transacción buena y se ingresa "Service Level Threshold" para indicar el porcentaje requerido de transacciones buenas en un minuto para cumplir un nivel de servicio.

Además se puede seleccionar la casilla "Worst Client & Server Analysis" y se activarán dos enlaces en la parte superior "Worst Client" y "Worst Server", ingresando a estos enlaces se obtiene una ventana que muestra lista de computadores que presentan problemas con respecto al umbral ingresado anteriormente, además en esta ventana se puede ingresar "Min Transaction" que es un número mínimo de transacciones malas para que un computador sea considerado malo, como se observa en la Figura 3.34.



STATISTICS: RESPONSE TIME: WORST SERVERS

Name: /Inbound/HTTP

◄ back | update | Min Transaction: 10 | *Go to* Worst Clients

Servers with worst response time in **/Inbound/HTTP** class

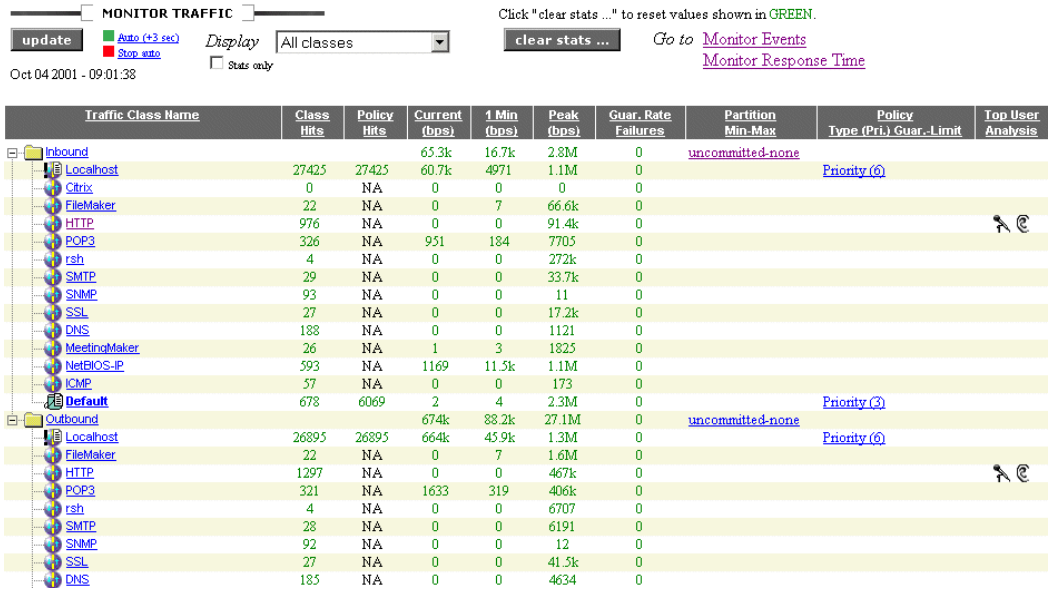
Worst Servers Delay Threshold: 200ms Time analyzed: 00:06:22

	DNS Name	IP Address	Good Pct.	Avg. Delay (ms)	Transactions
1	ads.web.aol.com	64.12.184.89	4 %	440	29
2	No such name	207.46.144.86	29 %	359	21
3	No such name	208.252.68.10	47 %	243	15
4	No such name	128.11.160.73	54 %	409	69

Figura. 3.34. Los servidores que presentan problemas.

3.3.6.4 Análisis.

Una vez que PacketSeeker ha descubierto y clasificado el tráfico de la red mediante PacketWise, se puede monitorear y analizar el tráfico para determinar cuanto ancho de banda se está utilizando, se puede observar que aplicaciones están consumiendo la mayoría del ancho de banda y que porcentaje del enlace utilizan, se elige la ficha “monitor” desde el navegador de Internet, como se observa en la Figura 3.35.


MONITOR TRAFFIC

update | Auto (+3 sec) | Stop auto | Display: All classes | Stats only

Oct 04 2001 - 09:01:38

Click "clear stats ..." to reset values shown in GREEN.

clear stats ... | Go to Monitor Events | Monitor Response Time

Traffic Class Name	Class Hits	Policy Hits	Current (bps)	1 Min (bps)	Peak (bps)	Guar. Rate Failures	Partition Min-Max	Policy Type (Pri.) Guar.-Limit	Top User Analysis
Inbound			65.3k	16.7k	2.8M	0	uncommitted-none		
Localhost	27425	27425	60.7k	4971	1.1M	0		Priority (6)	
Citrix	0	NA	0	0	0	0			
FileMaker	22	NA	0	7	66.6k	0			
HTTP	976	NA	0	0	91.4k	0			
POP3	326	NA	951	184	7705	0			
rsh	4	NA	0	0	272k	0			
SMTP	29	NA	0	0	33.7k	0			
SNMP	93	NA	0	0	11	0			
SSL	27	NA	0	0	17.2k	0			
DNS	188	NA	0	0	1121	0			
MeetingMaker	26	NA	1	3	1825	0			
NetBIOS-IP	593	NA	1169	11.5k	1.1M	0			
ICMP	57	NA	0	0	173	0			
Default	678	6069	2	4	2.3M	0		Priority (3)	
Outbound			674k	88.2k	27.1M	0	uncommitted-none		
Localhost	26895	26895	664k	45.9k	1.3M	0		Priority (6)	
FileMaker	22	NA	0	7	1.6M	0			
HTTP	1297	NA	0	0	467k	0			
POP3	321	NA	1633	319	406k	0			
rsh	4	NA	0	0	6707	0			
SMTP	28	NA	0	0	6191	0			
SNMP	92	NA	0	0	12	0			
SSL	27	NA	0	0	41.5k	0			
DNS	185	NA	0	0	4634	0			

Figura. 3.35. Análisis del tráfico.

Se tiene una columna con el nombre de la clase y las siguientes columnas de información:

- *Class Hits*.- Es el número de veces que un flujo de tráfico es clasificado en alguna clase, este conteo se realiza solo cuando un flujo empieza.

- *Policy Hits*.- Es el número de veces que una política de calidad de servicio ha sido reforzada.

- *Current (bps)*.- Es la tasa en ese instante en bits por segundo.

- *1 Min (bps)*.- Es la tasa promedio en el último minuto.

- *Peak (bps)*.- Son los valores pico en ese instante con una tolerancia de 6%, es decir es posible que este pico exceda el pico del enlace de entrada (inbound) global.

- *Guar.Rate Failures.*- Es el número de veces que la tasa garantizada falla, en un inicio este parámetro es cero.

- *Partition Min-Max.*- Muestra la cantidad máxima y mínima de ancho de banda asignada a una clase, si es que se ha asignado. “Uncommited” y una flecha hacia abajo significa particiones asignadas dinámicamente, “none” indica que la partición es “burstable” es decir no tiene límite para su incremento explosivo de velocidad.

- *Policy Type (Pri.) Guar-Limit.*- Muestra la política aplicada a una clase, si es que se ha asignado.

- *Top User Analisis.*- Muestra iconos de un micrófono y una oreja, se ha activado la opción “Top Talkers” y “Top Listeners”, se puede elegir estos iconos para observar las estadísticas.

Además en la casilla “Display” se puede cambiar opciones de monitoreo, se puede seleccionar “All classes”, “Active classes” que muestra las clases activas en ese instante, “Classes with partitions” y “Classes with policies”. También se puede borrar las estadísticas y cambiar la actualización de estadísticas a automática cada 3 segundos.

3.3.6.5 Particiones.

Una forma de aplicar calidad de servicio y resolver los problemas de la red es crear particiones en el PacketShaper, una partición administra el ancho de banda de una clase, tal que todos los flujos dentro de la clase son controlados como si fueran uno solo. Las particiones permiten garantizar que una clase obtenga una cantidad de ancho de banda, es decir reservar ancho de banda, también se pueden usar para limitar agresivamente la cantidad de ancho de banda de una clase.

Se pueden crear particiones para clases padres e hijas, pero se debe tomar en cuenta que la cantidad de ancho de banda asignada a un clase hija no puede ser igual ni sobrepasar la

cantidad de ancho de banda asignada a una clase padre. Para crear una partición, se elige la ficha "manage", se selecciona la clase en la cual se desea crear, se elige "partition" y se elige "add", aparece la ventana para configurar los parámetros de la partición como se observa en la Figura 3.36.

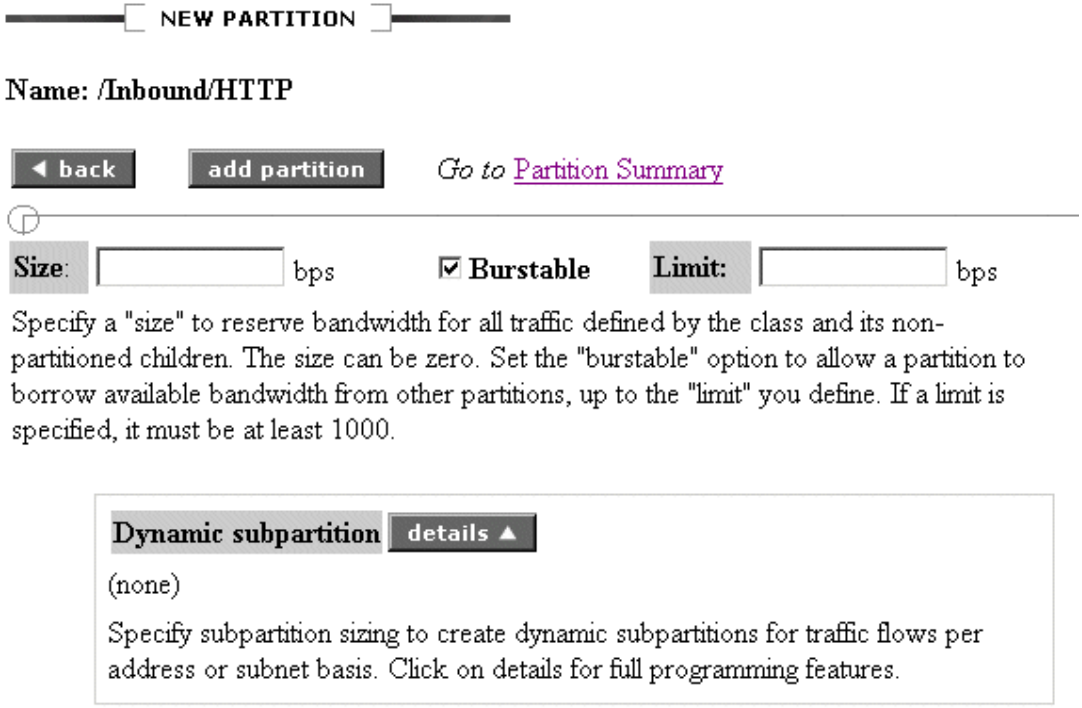


Figura. 3.36. Ventana de configuración de una partición.

Se define la partición en base a los siguientes parámetros:

- *Size.-* Se ingresa el tamaño de la partición en bits por segundo.

- *Burstable.-* Cuando se selecciona, permite a la partición usar el ancho de banda disponible en exceso. Cuando no se selecciona la partición tiene un tamaño fijo y el exceso de ancho de banda puede ser utilizado por otro tipo de tráfico.

- *Limit.-* Se ingresa la máxima cantidad de ancho de banda cuando se ha seleccionado "burstable". Este límite de ser mayor que la mínima cantidad de

ancho de banda asignada a la partición, se elige “add partition” para crear la partición.

Otra opción es crear una partición dinámica, aquí las subparticiones son creadas en base a los usuarios activos en una clase, las subparticiones dinámicas permiten justeza a la hora de distribuir la cantidad de ancho de banda a cada usuario, aún cuando el ancho de banda aumente debido a ancho de banda disponible en exceso, para crear una partición dinámica se sigue el siguiente procedimiento:

- Se debe tener creada una partición estática o crear una nueva, se elige “details” y aparece la ventana para configurar los parámetros de la subpartición, como se observa en la Figura 3.37.

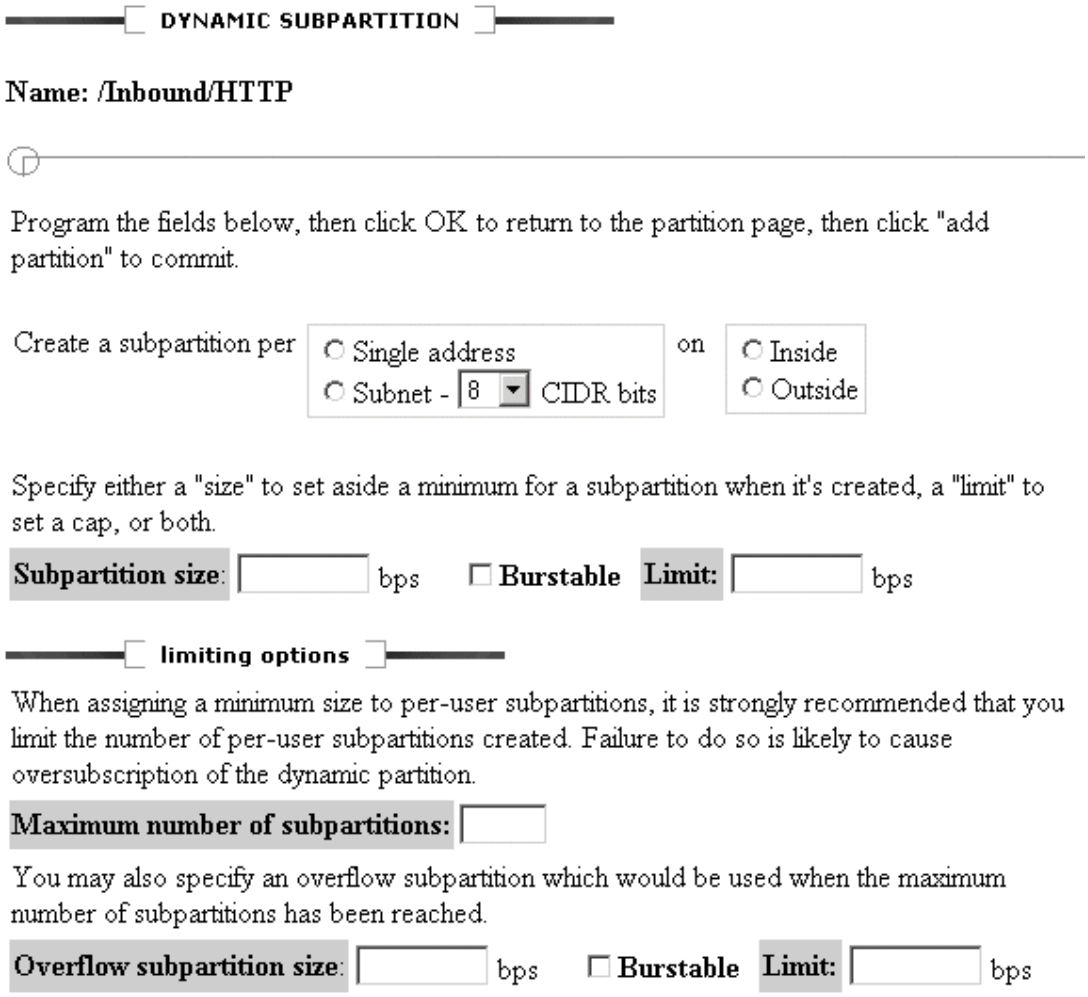


Figura. 3.37. Creando una subpartición dinámica.

- Seleccionar el usuario como “single IP” o como “subnet”, si se selecciona “subnet” se debe seleccionar el valor “CIDR” que representa el número de bits constantes en el rango de direcciones IP.

- Seleccionar el extremo “Inside” o “Outside”, en el cual se buscarán las direcciones IP diferentes o subredes que generarán las subparticiones dinámicas. Por ejemplo si el PacketShaper está situado entre una Red de Área Local (LAN) y el Internet, se selecciona “Inside” para crear una subpartición dinámica para cada cliente de la red de área local que se conecte a algún computador en el Internet.

- Se define la subpartición en base a los siguientes parámetros:

  - *Subpartition size.-* Se ingresa la cantidad mínima de ancho de banda a ser asignada a cada usuario en bits por segundo. Este campo configurado a cero asigna el ancho de banda equitativamente a cada subpartición, dividiendo el ancho de banda de la partición estática para el número de subparticiones.

  - *Burstable.-* Este campo se selecciona cuando se ha ingresado cero en "Subpartition size", a cada subpartición se asignará la misma cantidad de exceso de ancho de banda. Si se ha ingresado un valor explícito en "Subpartition size" no se selecciona "burstable" y las subparticiones tienen un tamaño fijo.

  - *Limit.-* Se ingresa la máxima cantidad de ancho de banda a ser asignado a cada subpartición, es útil cuando se desea sobrepasar límites de capacidad cuando existe acuerdos de servicio con cada usuario ó subred.

- Opcionalmente se puede ingresar "maximum number of subpartitions" que es una capacidad de número de usuarios activos en la partición dinámica, es necesario especificar este parámetro cuando se tiene particiones fijas que no son "burstables" para evitar problemas de sobre subscripciones.

- Opcionalmente se puede crear "Overflow subpartition size" para asignar ancho de banda a nuevos usuarios si la capacidad es excedida. Es necesario especificar este parámetro cuando se tiene particiones fijas que no son "burstables" para evitar problemas de sobre subscripciones. Si no se crea esta subpartición los flujos serán rechazados cuando se sobrepase la capacidad o cuando el limite de la partición es excedido. Se fijan los siguientes parámetros:

  - *Overflow Subpartition size.-* Se ingresa la cantidad mínima de ancho de banda a ser asignada a la subpartición.

- *Burstable.-* Cuando se selecciona la subpartición usará el ancho de banda disponible en exceso, caso contrario el ancho de banda disponible en exceso puede ser usado por otro tipo de tráfico.

- *Limit.-* Se ingresa la máxima cantidad de ancho de banda a ser asignado a la subpartición, debe ser mayor que "Overflow Subpartition size".

Una partición puede ser modificada ó borrada en la ficha "manage", "partition" y "delete partition".

3.3.6.6 Políticas.

Otra forma que PacketShaper utiliza para implementar calidad de servicio en la red es creando políticas, una política determina como los flujos individuales de las aplicaciones son tratados, es decir permite manejar el ancho de banda flujo a flujo. Mediante políticas se puede dar a cada flujo de tráfico el ancho de banda que necesite para un desempeño óptimo por ejemplo tráfico sensible ó importante, adicionalmente se puede limitar el crecimiento de tráfico menos urgente ó importante y así consuman un apropiado ancho de banda.

3.3.6.6.1 Usando políticas sugeridas.

El software PacketWise incluye un conjunto de políticas sugeridas para muchos protocolos y servicios, dichas políticas fueron desarrolladas tomando como referencia a varias empresas y podrían ajustarse o no a la necesidad del usuario. Se puede aplicar una política sugerida a una clase de tráfico creada manualmente ó automáticamente, si la característica "Automatic Policy" está habilitada dentro de la ventana de configuración básica, las políticas sugeridas se aplicarán a cada clase de tráfico que es descubierta por PacketShaper.

Todas las políticas sugeridas fijan la tasa garantizada a cero y se selecciona la opción "burstable", es decir pueden incrementar su tasa de tráfico si existe ancho de banda

disponible en exceso, para crear políticas usando las políticas sugeridas se sigue el siguiente procedimiento:

- Se elige la ficha "manage", se elige la clase a la que va aplicar la política.

- Se elige "policy" y se elige "add", aparecerá una ventana como se observa en la Figura 3.38.

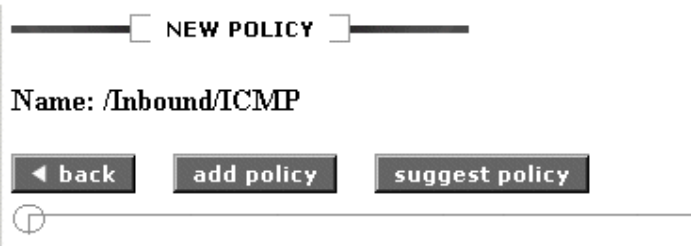


Figura. 3.38. Añadiendo una política sugerida por PacketShaper.

- Se elige "suggest policy", una pantalla de advertencia indicará que se va aplicar una política sugerida, finalmente se elige "add" para añadir la política sugerida a la clase, si esta política no se ajusta a la necesidad del usuario se puede cambiar los parámetros.

El procedimiento anterior también se utiliza para crear una política que no sea sugerida, omitiendo la elección de "suggest", cuando se va a crear una política se debe elegir el tipo de política, existen varios tipos que se mencionarán a continuación.

3.3.6.6.2 Política de tasa.

Una política de tasa permite establecer una tasa mínima para cada flujo de una aplicación, permite acceso priorizado al exceso de ancho de banda que pueda existir, fija un límite de ancho de banda que el flujo puede consumir, una política de tasa es recomendada para tipos de tráfico que tienden a crecer rápidamente.

Una tasa de tráfico permite un manejo preciso de tráfico TCP mediante el control de tasa de TCP y UDP mediante el planeamiento de límite de retardo, las políticas de tasa generalmente no son recomendadas para tráfico no IP, para crear una política de tasa se escoge el botón "rate", como se observa en la Figura 3.39.

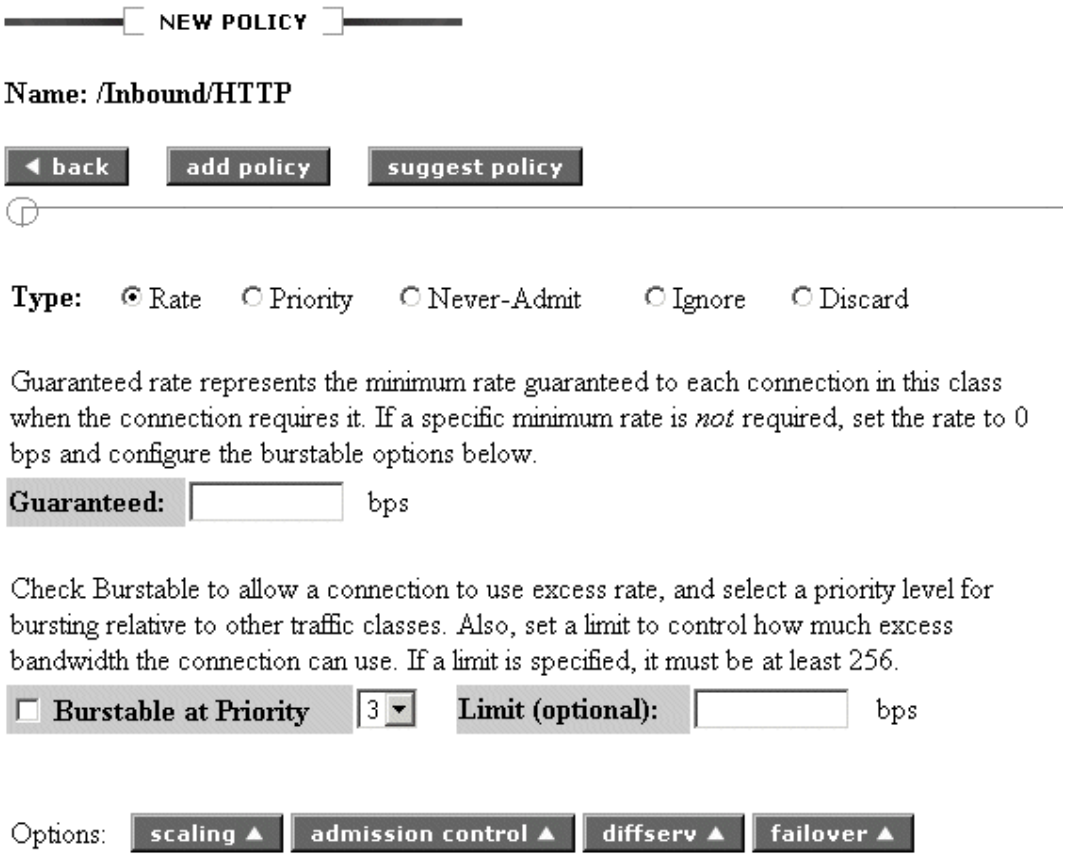


Figura. 3.39. Política de tasa.

Aquí se debe configurar algunos parámetros como:

- *Guaranteed.*- Es la tasa mínima garantizada, cuando no requiera una tasa mínima este parámetro debe ser cero y se configura la opción "burstable". Además si la clase tiene una partición, la tasa garantizada no debería sobrepasar el tamaño de la partición, si es así los flujos serán fijados a menos de 1 Kbps tomando en cuenta el control de admisión que se mencionará posteriormente.

- *Burstable at priority.*- Cuando se selecciona esta opción el ancho de banda disponible en exceso es usado según la prioridad especificada de 0 a 7 (la más alta).

- *Limit.*- Opcionalmente se puede ingresar un límite al que puede llegar el exceso de tasa, debe ser mínimo 256 y debe sobrepasar la tasa garantizada en la partición.

Además ciertos tipos de tráfico ofrecen opciones especializadas de políticas de tasa como son:

- *Scaling.*- Una política de tasa se puede configurar para discriminar clientes con conexiones de baja y alta velocidad, por ejemplo un cliente con una conexión vía módem y un cliente con una conexión de alta velocidad. La tasa dada al cliente es basada en una escala variable, dependiendo de la velocidad del cliente, PackeWise monitorea la velocidad del cliente mediante el acuerdo de conexión (handshake) de TCP y ajusta la asignación de ancho de banda del cliente. Para crear esto se elige "scaling" y aparece una ventana en donde se escoge "explicit", luego se ingresa las tasas mínimas y los límites tanto para las conexiones de velocidad baja como para las conexiones de velocidad alta.

- *Admission Control.*- Este mecanismo determina que pasa cuando no hay suficiente ancho de banda para satisfacer la tasa de ancho de banda requerida, permite configurar un nivel de servicio mínimo e incluso rechazar conexiones cuando ocurre congestión. Para crear esto se elige "admission control" y aparece una ventana como se observa en la Figura 3.40.

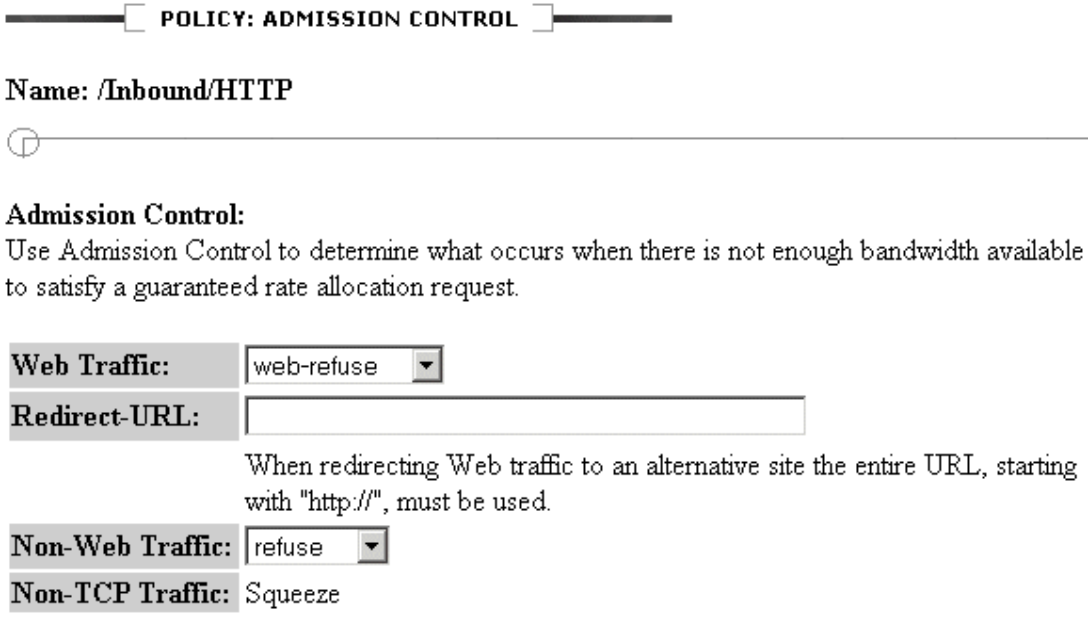


Figura. 3.40. Control de admisión.

En la ventana anterior se selecciona el tipo de control de admisión apropiado para la clase de tráfico como sigue:

- *TCP Non-Web.-* Se puede seleccionar entre "refuse" para rechazar una conexión sin notificación al usuario y "squeeze" para dar a las nuevas conexiones una tasa mínima que es menos de 1Kbps.

- *TCP Web.-* Se puede seleccionar entre "web-refuse" para rechazar una conexión con notificación al usuario, "web-squeeze" para dar a las nuevas conexiones una tasa mínima que es menos de 1Kbps y "web-redirect" que redirecciona el tráfico del Protocolo de Transferencia de HiperTexto (HTTP) a una dirección de Localizador de Recurso Uniforme (URL) específica que se debe ingresar cuando se selecciona esta opción, por ejemplo si no se permite el acceso a un servidor web se redirecciona a http://www.elcomercio.com.

- *Non-TCP.-* Se puede seleccionar "squeeze" para dar a las nuevas conexiones una tasa mínima que es menos de 1Kbps.

- *Delay Bound.-* Se puede usar esta opción para aplicaciones UDP y algunos tipos de tráfico no IP como IPX y AppleTalk para proveer control de flujo. Se recomienda no cambiar este parámetro que es predeterminado para un buen funcionamiento en la mayoría de ambientes de red, sin embargo pueden existir requerimientos de memoria intermedia (buffer) en donde es necesario cambiar este valor, se elige "delay bound" y se ingresa la máxima longitud de tiempo que el PacketShaper retendrá los paquetes.

- *Diffserv.-* Se puede crear políticas para realizar marcado de paquetes, se puede cambiar la precedencia o el nivel de servicio de una aplicación creando políticas para cambiar el Punto de Código de Servicios Diferenciados (DSCP) o substituir diferentes valores de Clase de Servicio (COS), Tipo de Servicio (TOS). Para hacer esto se elige "diffserv" en la ventana de política, se selecciona el botón "Code Point" o "COS/TOS", si se elige "Code Point" se ingresa un valor entre 0 y 63, si se elige "COS/TOS" para "COS" se selecciona un valor entre 0 – 7 y para "TOS" se ingresa un valor entre 0, 1, 2, 4, 8.

- *Failover.-* Para crear una política sobre falla se debe primero habilitar el modo "failover" del PacketShaper, luego en la ventana de política se elige "failover", en el campo "Failover Guaranteed" se ingresa la tasa garantizada que la política debería usar cuando el sistema está en modo sobre falla.

3.3.6.6.3 Política de prioridad.

Una política de prioridad establece una prioridad para el tráfico sin especificar una tasa particular, se recomienda usar política de prioridad para flujos de tráfico no continuos, cortos ó tráfico que no tiende a un incremento explosivo de su velocidad (burst). La prioridad determina la importancia de la clase de tráfico, se especifica un valor de prioridad de 0 a 7 (la más alta), las clases "Default" creadas por defecto tanto en "inbound"

como “outbound” tienen prioridad 3, para crear una política de prioridad se escoge el botón “priority”, como se observa en la Figura 3.41., aquí se debe elegir una prioridad para la clase de tráfico en entre 0 y 7 (la más alta).

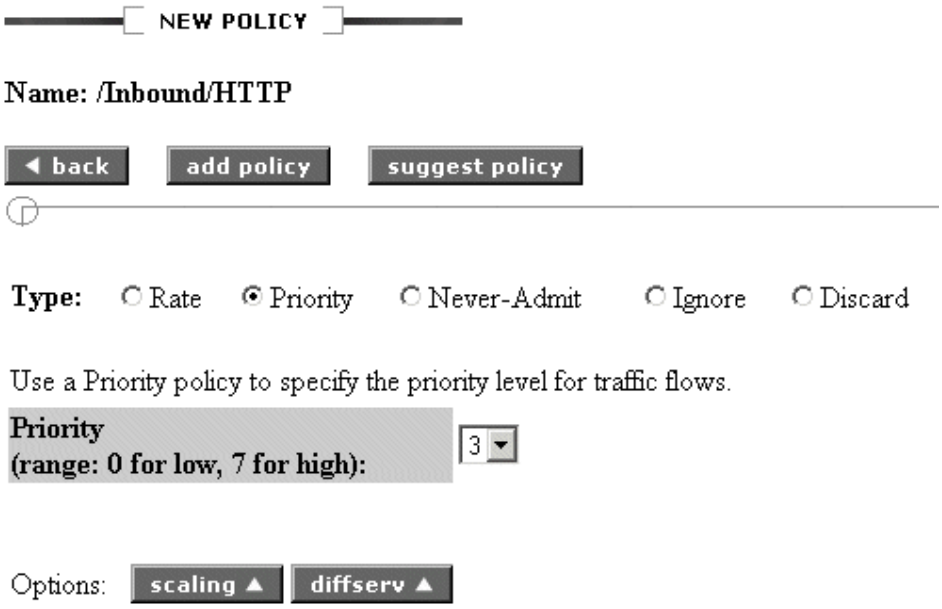


Figura. 3.41. Política de prioridad.

3.3.6.6.4 Política de nunca admitir.

Una política de nunca admitir permite a PacketShaper reforzar un control de admisión en el comienzo de un flujo, similar al que se estudió en una política de tasa. Es recomendado para clases de tráfico web TCP para notificar a usuarios que el sitio web no está disponible o redireccionarlos a un segundo sitio web, para clases no web TCP simplemente rechazar una conexión. No es recomendado y no se puede usar para tráfico UDP ó tráfico no IP, por ejemplo AppleTalk, para crear una política de nunca admitir se escoge el botón “Never-Admit”, como se observa en la Figura 3.42.

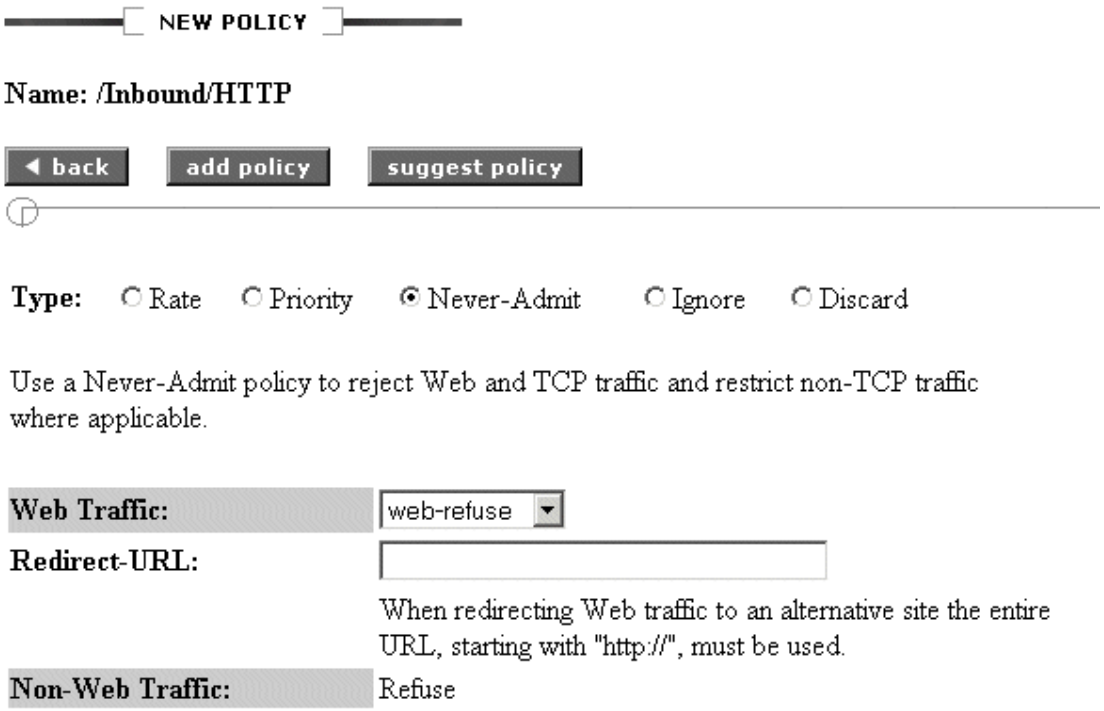


Figura. 3.42. Política de nunca admitir.

En "Web traffic" se puede seleccionar entre "web-refuse" para rechazar una conexión con notificación al usuario y "web-redirect" que redirecciona el tráfico del Protocolo de Transferencia de HiperTexto (HTTP) a una dirección de Localizador de Recurso Uniforme (URL) específica que se debe ingresar cuando se selecciona esta opción, por ejemplo si no se permite el acceso a un servidor web se redirecciona a http://www.elcomercio.com.

3.3.6.6.5 Política de Ignorar.

Una política de ignorar se usa para tipos de tráfico que pasan a través del sistema y no deben ser tomados en cuenta como parte del enlace de Red de Área Amplia (WAN) bajo administración, es decir tráfico que no sale a través del ruteador que está administrando PacketShaper, por ejemplo tráfico entre clientes y un servidor de una Red de Área Local (LAN), para crear una política de ignorar se escoge el botón "ignore".

3.3.6.6.6 Política de descarte.

Una política de descarte desecha todos los paquetes para una clase de tráfico, las razones para bloquear un servicio podrían ser demasiado consumo del ancho de banda, que no sea considerado esencial para un negocio o que sea simplemente prohibido en la red, una política de descarte es recomendada para bloquear clases de tráfico UDP y no IP. No es recomendado para tráfico como TCP ya que los paquetes desechados causarán tiempos sin respuesta para una conexión (time out) y un usuario esperará largos tiempos en obtener una respuesta, en algunos casos podría ser aplicado a propósito con el fin de provocar tiempos fuera (time out) y evitar ataques que intenten por ejemplo quebrar (crackear) un servidor. Para crear una política de descarte se escoge el botón “discard”, se debe tener cuidado al aplicar políticas de descarte, por ejemplo si se configura una política de descarte a “/Inbound/Default” se desechará los paquetes en el árbol “Inbound” de todas las clases que no tenga su propia política.

Todas las políticas creadas pueden ser modificadas o borradas posteriormente eligiendo la ficha “manage”, escogiendo la clase, eligiendo “policy” y seleccionando “open” para modificar y “delete” para borrar, para que las políticas aplicadas a las clases tengan efecto la opción “Shaping” de la ficha “setup” debe estar habilitada.

3.4 APLICACIONES Y PROTOCOLOS CLASIFICADOS POR PACKETSHAPER

En la Tabla 3.3. se observa el nombre y una breve descripción de los protocolos y aplicaciones que clasifica PacketShaper una vez que es conectado y configurado siguiendo los procedimientos descritos al inicio de este capítulo. La versión del software PacketWise es la 7.0

Nombre	Descripción
Cliente/Servidor	
CVSpserver	Sistema de Versiones Concurrentes, pserver
FIX	Intercambio de Información Financiera
FoldingAtHome	Protector de Pantalla de Computación Distribuido
INFOC-RTMS	Sistema Monitor de Tiempo de Respuesta INFOConnect
INT-1	Unisys Interactivo 1
MATIP	Grupo de Servicios de Mapeo de Tráfico de Aerolínea sobre IP (RFC 2351)
MeetingMaker	Fabricante de reuniones
NetIQ	Administrador de Aplicación NetIQ
OpenConnect-JCP	Clientes JCP OpenConnect
PEPGate	Puerta de enlace PEP (Unisys 2200)
Unisys-TCPA	Unisys-TCPA
Deliberación de contenido	
Apple-iTunes	Apple-iTunes, descarga de música
Ariel-419	Sistema de liberación de documentos Infotrieve, puerto 419
Ariel-422	Sistema de liberación de documentos Infotrieve, puerto 422
BackWeb	Tecnología liberadora
Chaincast	Sistema de liberación de contenido flexible Chaincast
EntryPoint	Tráfico liberador EntryPoint (formalmente PointCast)
Kontiki	Red de Distribución de Contenido
Marimba	Tráfico liberador Marimba Castanet
Napster2	Napster, pago por uso de música
NewsStand	Servicio de suscripción de publicación
PointCast	Ver EntryPoint
Webshots	Aplicación de fondos de pantalla con fotos
Bases de datos y software de Planeamiento de Fuente de Empresa (ERP)	
BAAN	Sistema de administración empresarial
FileMaker	Grupo de servicios de bases de datos
JDENet	Protocolo J. D. Edwards OneWorld
MSSQL	Grupo de servicios de Lenguaje de Preguntas Estructuradas de Microsoft
Oracle	Grupo de servicios de aplicación de bases de datos
PostgreSQL	Bases de datos SQL sin costo
Progress	Tráfico de bases de datos Progress
SAP	Servicios, aplicaciones y productos en procesamiento de datos
SAP.MCAST.NET	Protocolo de Anuncio de Servicio Multicast
Servicios de directorio	
CRS	Servicio de Replicación de Contenido de Microsoft
DHCP	Grupo de servicios del protocolo de Configuración de Computadores Dinámica, asigna direcciones IP a computadores de forma dinámica
DNS	Servidor de Nombres de Dominio, asigna nombres comunes a direcciones IP
Finger	Protocolo de información de usuario Finger
Ident	Protocolo de identificación
Kerberos	Servicio de autenticación de red
LDAP	Protocolo de Acceso de Directorio Peso liviano

mDNS	DNS Multicast (Apple)
RADIUS	Servicio de Autenticación Remota de Llamada de Usuario
RRP	Protocolo de Registro NSI
rwho	Comando remoto who de UNIX
SSDP	Protocolo de Descubrimiento de Servicio Simple
TACACS	Protocolo de computador de ingreso
WHOIS	Aplicación que identifica al propietario de un nombre de dominio
WINS	Servicio de Nombre de Internet de Windows
E-mail y colaboración	
Biff	Notificación de mail nuevo en UNIX
ccMail	Aplicación de e-mail de Lotus
DCOM	Modelo de Objeto de Componente Distribuido de Microsoft
Groupwise	Grupos de servicios de sistema de mensajería GroupWise de Novell
IMAP	Grupo de servicios del Protocolo de Acceso de Mail Interactivo
LotusNotes	Comunicación colaborativa para Groupware
MSSQ	Grupo de servicios de Mensajes en cola de Microsoft
OSI	Interconexión de Sistema Abierto sobre TCP (RFC 2126)
POP3	Protocolo de Oficina Postal, grupo de servicios de recepción de mail
SMTP	Protocolo de Transporte de Mail Simple, grupo de servicios de transmisión de mail
Servidor de archivos	
AFS	Grupo de servicios de Sistema de Archivo Andrew
CIFS-TCP	Servidor de Archivo de Internet Común sobre TCP
CU-Dev	Control de equipo Fujitsu en TCP/IP
Microsoft-ds	Sistema de Archivo de Internet Común de Microsoft
NetBIOS-IP	Grupo de servicios del protocolo de transporte NetBIOS sobre IP, generalmente dentro de una Red de Área Local (LAN) permite comunicarse a aplicaciones entre diferentes computadores
NFS	Sistema de Archivo de Red de UNIX; TCP y UDP
NW5-CMD	Netware 5, grupo de servicios de controladores de modo de compatibilidad
rsync	Protocolo de sincronización de archivo remoto de UNIX
SunND	Protocolo de disco de inicio de Sun Network
Juegos	
AsheronsCal	Juego de red de Microsoft
Battle.net	Juego de red
Doom	Juego de red
Half-Life	Juego de red
Kali	Protocolo de juego
LucasArts	Juego de red
MSN-Zone	Zona de juego en Red de Microsoft
Mythic	Juego de red
Quake	Juego de red
SonyOnline	Zona de juego de Sony

Tribes	Juego de red
Unreal	Juego de red
YahooGames	Zona de juego de Yahoo
Cuidado de bienestar	
DICOM	Comunicaciones e imágenes digitales en medicina
HL7	Séptimo Nivel de Salud
Acceso a computador	
ATSTCP	Tráfico de impresión y Terminal Galileo 2915
Attachmate-GW	Puerta de enlace INFOConnect-e-Vantage
Persona	Grupo de servicios Persona Persoft
SHARESUDP	ALC sobre UDP
SMTBF	Puerta de enlace Lantern
tn3270	Telnet para terminales IBM 3270
tn5250	Telnet para terminales IBM 5250
Protocolos de Internet	
ActiveX	Herramientas y tecnologías de programas orientados a objetos de Microsoft
BITS	Servicio de Transferencia Inteligente de Fondo de Microsoft
FTP	Grupo de servicios, comandos y datos del Protocolo de Transferencia de Archivos
Gopher	Aplicación de búsqueda
HTTP	Protocolo de Transferencia de Hipertexto, tráfico web
HTTP-Tunnel	Tráfico que es enviado a través de un túnel HTTP vía un servidor Proxy en el Internet
IP	Protocolo de Internet
IPIP	Protocolo de Encapsulación IP dentro de IP
IPv6	Protocolo de Internet versión 6
NNTP	Protocolo de Transferencia NetNews Usenet
SOAP-HTTP	Protocolo de Acceso de Objeto Simple sobre HTTP
TCP	Protocolo de Control de Transmisión
TFTP	Protocolo de Transferencia de Archivo Trivial
UDP	Protocolo de Datagrama de Usuario
UUCP	Protocolo de Copia Unix a Unix
Legado LAN o no IP	
AFP	Protocolo de Relleno de AppleTalk
AppleTalk	Protocolo de red de Apple
DECnet	Protocolo de red de la Corporación de Equipamiento Digital
FNA	Arquitectura de Red Fujitsu
IPX	Protocolo de networking de Novell
LAT	Soporte de Impresión de DEC
MOP	Protocolo de Operaciones de Mantenimiento
NetBEUI	Protocolo de red para PCs
PPPoE	Protocolo punto a punto sobre ethernet
SLP	Protocolo de Localización de Servicio
SNA	Protocolo de Arquitectura de Red de Sistemas IBM
Mensajería	
AOL	Grupo de servicios de mensajería de America On Line
IRC	Grupo de servicios de Conversación Transmitida en Internet

Lotus-IM	Mensajería instantánea de Lotus IBM
MSN-Messenger	Servicio de mensajería de MSN
Windows-POPUP	Aplicación que clasifica las ventanas de aviso que genera la aplicación de mensajería Windows Messenger
YahooMsg	Mensajería instantánea Yahoo
Software Intermedio	
CORBA	Protocolo Inter-ORB de Internet CORBA
JavaRMI	Grupo de servicios de Invocación de Método Remoto de Java 1.1.4 TCP
SmartSockets	Tráfico de Tibco SmartSockets v6.0.2 y anteriores, es un programa que permite distribución e intercambio de información en tiempo real
SunRPC	Grupo de servicios de Llamadas de Procedimiento Remoto de Sun
Multimedia (tráfico "streaming media")	
Abacast	Tecnología streaming distribuida Abacast
Motion	Video que usa DIGStream
MPEG	Grupo de Expertos de Imágenes en Movimiento, audio y video
QuickTime	Quicktime sobre HTTP
RadioNetscape	Aplicación de streaming musical
Real	Grupo de servicios para streaming de audio/video de Real Networks
RTP-B	Protocolo de Tiempo Real (Broadcast)
RTP-I	Protocolo de Tiempo Real (Interactivo)
RTSP	Protocolo de Streaming de Tiempo Real
Shoutcast	Streaming de audio de Shoutcast
ST2	Protocolo de Stream de Internet
StreamWorks	StreamWorks audio y video
VideoFrame	Grupo de servicios de pantalla de video de Citrix
WebEx	Plataforma de comunicaciones en tiempo real WebEx
WinampStream	Tráfico streaming de Winamp
WinMedia	Grupo de servicios de Microsoft Windows Media
Administración de Red	
CiscoDiscovery	Protocolo de descubrimiento de ruteador Cisco
Day-Time	Tiempo del día
Echo	Protocolo Eco
FlowRecords	Grabaciones de Detalle de Flujo Propietario de Packeteer
ICMP	Protocolo de Mensaje de Control de Internet
IPComp	Protocolo de Compresión de Payload de IP
NetFlowV5	NetFlow V5
NTP	Grupo de servicio de Protocolo de Tiempo de Red
RSVP	Protocolo de Reservación de Recursos
SMS	Microsoft SMS 2.0
SNMP	Grupo de servicios del Protocolo de Administración de Red Simple
Syslog	Ingreso al sistema UNIX
TimeServer	Servidor de Tiempo
Aplicaciones Par a Par	
Aimster	Grupo de servicios de aplicación para compartir archivos

Audiogalaxy	Comunidad para compartir archivos
BitTorrent	Sistema para compartir archivos
Blubster	Aplicación para compartir archivos
DirectConnect	Comunidad para compartir archivos
EarthStationV	Aplicación par a par
eDonkey	Grupo de servicios de aplicación para compartir archivos
FileRogue	Aplicación para compartir archivos
Filetopia	Aplicación par a par
Furthurnet	Aplicación par a par
Gnutella	Grupo de servicios de red de distribución y compartición de archivos
Groove	Aplicación par a par
Hotline	Grupo de servicios de aplicación para compartir archivos
iMesh	Intercambio de archivos multimedia usuario a usuario
KaZaA	Grupo de servicios de aplicación para compartir archivos
Napster	Grupo de servicios de comunidad de música
PeerEnabler	Altnet sobre KaZaA
ScourExchange	Comunidad para compartir archivos
Tripnosis	Aplicación para compartir archivos
Tráfico de Impresión	
IPP	Protocolo de Impresión de Internet
Printer	Impresor e línea de UNIX
tn3287	Tráfico de impresión 3270 deIBM
tn5250p	Tráfico de impresión 5250 deIBM
Protocolos de ruteo	
AURP	Protocolo de Ruteo basado en Actualización de AppleTalk
BGP	Protocolo de Puerta de Enlace de Borde
CBT	Árboles Basados en el Centro
DRP	Protocolo de Ruteo de DECnet
EGP	Protocolo de Puerta de Enlace Exterior
EIGRP	Protocolo de Ruteo de Puerta de Enlace Interior Avanzado
IGMP	Protocolo de Administración de Grupo de Internet
IGP	Protocolo de Puerta de Enlace Interior
OSPF	Primera Ruta más Corta Abierta
PIM	Protocolo de ruteo multicast independiente del protocolo
RARP	Protocolo de Resolución de Direcciones en Reversa
RIP	Protocolo de Información de Ruteo
SpanningTree	Árbol de Espaciamiento de Puente, IEEE802.1
Protocolos de seguridad	
DLS	Grupo de servicios de clasificación de tráfico de Switch de Enlace de Datos
DPA	Autenticación de Password Distribuida de Microsoft
GRE	Encapsulación de Ruteo General
IPMobility	Encapsulación mínima para IP
IPSec	Grupo de servicios de Encapsulación de seguridad de IP
ISAKMP	Intercambio de clave ISAKMP/IKE
L2TP	Protocolo basado en Túneles Capa 2 para conexiones VPN
PPTP	Protocolo basado en Túneles Punto a Punto

RC5DES	Estándar de Encriptación de Datos
SOCKS	Protocolo Proxy v.4 y v.5
SSH	Protocolo de ingreso remoto Escudo de Seguridad
SSL	Protocolo de Capa de Sockets Segura
SWIPE	Protocolo IP Encriptado Encapsulado de Capa de Red
Sesión	
GoToMyPC	Tráfico HTTP
pcAnywhere	Grupo de servicios para administración remota
radmin	Grupo de servicios para administración remota
Rexec	Protocolo de ejecución remota de UNIX
rlogin	Ingreso remoto
rsh	Comando de escudo remoto deUNIX
Telnet	Grupo de servicios de Terminal
Timbuktu	Grupo de servicios para control remoto
VNC	Grupo de servicios para administración remota
XWindows	Agente de ventanas X11 (UDP)
Cliente ligero o basado en servidor	
Citrix	Grupo de servicios de aplicación de conectividad de Citrix. Habilita a algún tipo de cliente acceder a aplicaciones a través de una conexión de red
CitrixIMA	Grupo de servicios de Arquitectura de Administración Integrada de Citrix
RDP	Protocolo de Escritorio Remoto
Voz sobre IP	
CiscoCTI	Interfaz de Telefonía de Computador de Cisco
Clarent-CC	Voz clara sobre Centro de Comando IP
CUSeeMe	Grupo de servicios de aplicación de servicios de video de conversación
Dialpad	Grupo de servicios de Telefonía de Internet
H.323	Grupo de servicios Estándar de Telefonía de Internet
I-Phone	Servicio de telefonía de Internet de Vocaltec
MCK	MCK, voz y señalización
Megaco	Control de Puerta de Enlace Multimedia
MGCP	Protocolo de Control de Puerta de Enlace Multimedia
Micom-VIP	Voz sobre IPde Micom
Net2Phone	Centro de comunicaciones
RTCP	Protocolo de Controlen tiempo real, broadcast e interactivo
SIP	Protocolo de Iniciación de Sesión
Skinny	Protocolo de Control de Cliente de Skinny de Cisco
Skype	Aplicación de telefonía par a par
T.120	Aplicación de colaboración
VDOPhone	Grupo de servicios para telefonía de Internet

Tabla. 3.3. Aplicaciones y protocolos clasificados por PacketShaper.

CAPITULO IV

PRUEBAS DEL SISTEMA PACKETSHAPER

4.1 GENERALIDADES

El objetivo de este capítulo es probar el acondicionamiento de tráfico utilizando el sistema administrador de ancho de banda PacketShaper, mostrar las ventajas y facilidades de monitoreo, reporte, análisis y control, que PacketShaper muestra con respecto a los otros sistemas similares administradores de ancho de banda y a los elementos de red.

Para esto se instalará a PacketShaper como elemento de una red para controlar su enlace de Internet, es decir monitorear y clasificar su tráfico en primera instancia, luego obtener reportes, para finalmente analizar y controlar los flujos de tráfico existentes en dicho enlace de Internet.

4.2 ENLACE DE INTERNET DE ALEGRO PCS

La prueba de acondicionamiento de tráfico se realizó con un sistema PacketShaper 1500, el cual es un administrador de ancho de banda de enlace de Red de Area Amplia (WAN) ó Internet cuya capacidad es hasta 2 Mbps, sus características se mencionan en el capítulo anterior. Se colocó al PacketShaper en el enlace de Internet, un canal limpio (clear channel) de 1 Mbps de entrada y de 1 Mbps de salida, fue instalado en serie entre el ruteador con dirección IP 200.41.114.129 y un switch. En esta posición PacketShaper permite monitorear, clasificar, obtener reportes, analizar y controlar el tráfico desde y hacia Internet, como se observa en la Figura 4.1.

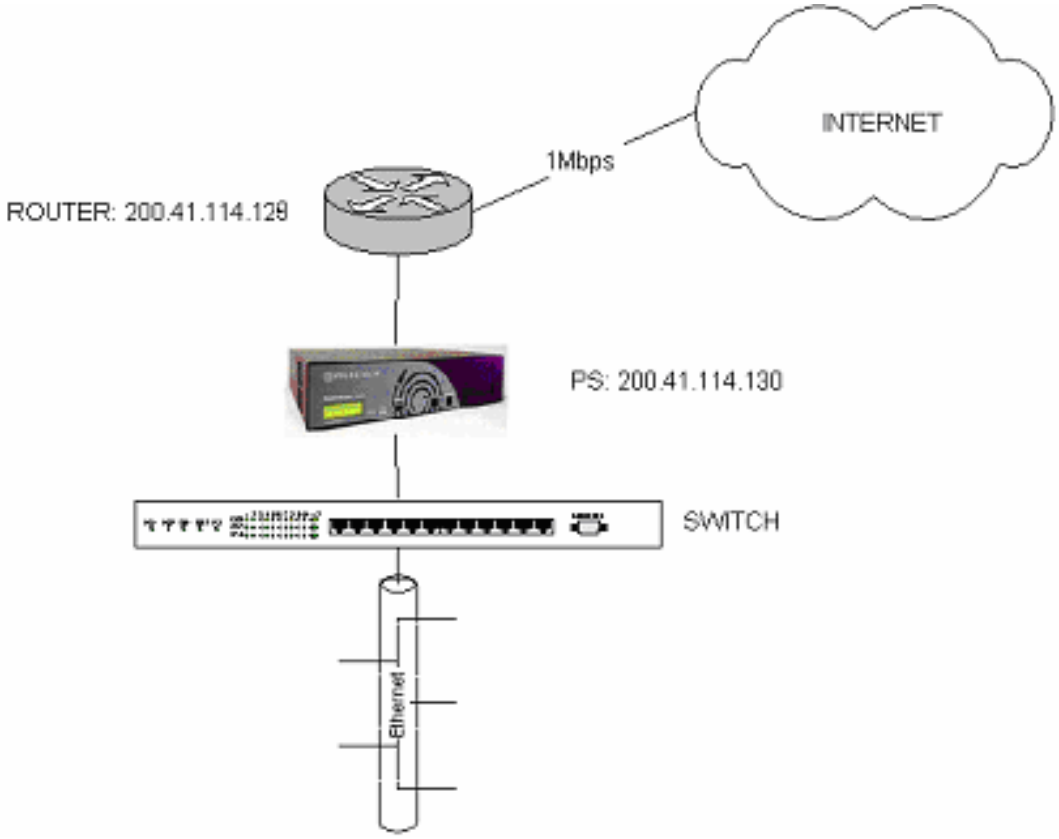


Figura. 4.1. PacketShaper administrando el enlace de Internet de Alegro PCs.

Al sistema PacketShaper se le configuró la dirección IP 200.41.114.130, un enlace de entrada (Inbound) de 1 Mbps y un enlace de salida (Outbound) de 1 Mbps. El período de pruebas de acondicionamiento se describen a continuación, el PacketShaper fue colocado el día martes 4 de mayo de 2004 y fue retirado el día miércoles 12 de mayo de 2004, primero se realizó el monitoreo, clasificación se obtuvo reportes y se realizó análisis. Para comprobar la funcionalidad de control se aplicó políticas de calidad de servicio desde el día viernes 7 de Mayo de 2004, lo que a su vez permitió tener una visión práctica del tráfico existente en un enlace de Red de Area Amplia (WAN) y cuales son las políticas que deben aplicarse a cada tipo de tráfico y que se mencionan en el capítulo posterior.

4.2.1 Monitoreo y clasificación.

El monitoreo y clasificación de tráfico se hizo por defecto y por un período de tres días, es decir no se añadió “matching rules” para la clasificación de flujos y se dejó a

PacketShaper descubrir los flujos de tráfico tanto para el enlace de entrada, como para el enlace de salida, PacketShaper autodescubrió el tipo y cantidad de flujos de tráfico que cada aplicación genera los clasificó en clases y guardó las estadísticas de uso. Para realizar el análisis del tráfico descubierto se utilizó una alternativa al método del navegador de Internet, se utilizó el comando "traffic tree" a través de una sesión al sistema mediante el Protocolo de Emulación de Terminal (TELNET), se hizo de esta forma para facilitar el trabajo de guardar el reporte debido a la gran cantidad de flujos de tráfico monitoreados y clasificados, en la Tabla 4.1. se observa el árbol de clases obtenido.

"PacketShaper# traffic tree"

Class name	Type	Class hits	Policy hits	Cur rate	1 Min avg	Peak rate
/Inbound	+		n/a	445k	394k	1.2M
Localhost	PE	4244	4244	0	0	0
eDonkey		33169	n/a	1981	1776	338k
FTP		1197	n/a	9	12	761k
Groupwise		185	n/a	0	0	47k
HTTP		442569	n/a	183k	139k	1.0M
IRC		5	n/a	0	0	11k
KaZaA		12947	n/a	127k	110k	1.0M
MPEG-Audio		111	n/a	0	0	400k
MPEG-Video		85	n/a	0	0	669k
MSN-Messenger		15344	n/a	3949	4853	526k
Napster		10	n/a	0	0	3529
Net2Phone		2	n/a	0	0	0
NTP		1869	n/a	0	6	313
POP3		2784	n/a	0	115	650k
QuickTime		8	n/a	0	0	1.0M
RDP		26	n/a	0	0	176k
Real		696	n/a	48k	44k	928k
RTCP-I		8	n/a	0	0	275
RTP-I		18	n/a	0	0	22k
SmartSockets		380	n/a	0	0	1157
SMTP		29098	n/a	874	9140	991k
SNMP		22324	n/a	0	25	144k
SSL		17239	n/a	10k	7396	782k
Telnet		39	n/a	0	3	19k
WebEx		12	n/a	0	0	283k
WinampStream		231	n/a	0	0	572k
Windows-POPUP		18	n/a	0	0	1
WinMedia		4789	n/a	66k	62k	952k
YahooGames		15	n/a	0	0	57k
YahooMsg		706	n/a	5	34	6080
AOL-AIM-ICQ		491	n/a	15	41	92k
DCOM		1165	n/a	0	2	20k
DNS		178962	n/a	1851	1296	49k
Gnutella		206	n/a	0	0	1667
H.323		24	n/a	0	0	508
ISAKMP		209	n/a	0	70	4511

PeerEnabler	3612	n/a	47	41	534k
RTSP	435	n/a	0	15	42k
TimeServer	9	n/a	0	0	995
ICMP	66851	n/a	503	97	6644
IPSec	1864	n/a	17k	7718	450k
DiscoveredPorts		n/a	1525	1073	103k
TCP_Port_16898	11	n/a	0	0	0
TCP_Port_1998	200	n/a	0	0	20k
TCP_Port_25	259	n/a	5	9	5356
TCP_Port_40001	37	n/a	0	0	2303
TCP_Port_62195	44	n/a	0	0	1888
TCP_Port_80	92	n/a	0	5	102k
TCP_Port_9000	35	n/a	0	0	68k
TCP_Port_9001	1453	n/a	286	78	1780
TCP_Port_9004	88278	n/a	1269	757	3482
TCP_Port_9008	2000	n/a	0	11	1732
UDP_Port_11764	12	n/a	0	0	0
UDP_Port_1387	2	n/a	0	0	0
UDP_Port_14856	264	n/a	0	0	8
UDP_Port_1493	0	n/a	0	0	0
UDP_Port_14968	11	n/a	0	0	0
UDP_Port_1560	14	n/a	0	0	0
UDP_Port_1781	11	n/a	0	0	0
UDP_Port_1897	25	n/a	0	0	0
UDP_Port_1919	0	n/a	0	0	0
UDP_Port_21721	0	n/a	0	0	0
UDP_Port_21884	32	n/a	0	0	164
UDP_Port_22482	12	n/a	0	0	0
UDP_Port_2297	15	n/a	0	0	0
UDP_Port_2327	24	n/a	0	0	167
UDP_Port_2463	0	n/a	0	0	0
UDP_Port_25742	47	n/a	0	0	13
UDP_Port_2618	1	n/a	0	0	0
UDP_Port_28825	16	n/a	0	0	0
UDP_Port_30260	66	n/a	0	0	122
UDP_Port_3208	0	n/a	0	0	0
UDP_Port_3372	12	n/a	0	0	0
UDP_Port_3591	15	n/a	0	0	0
UDP_Port_3620	19	n/a	0	0	0
UDP_Port_38929	25	n/a	0	0	1
UDP_Port_3916	59	n/a	0	0	0
UDP_Port_39557	0	n/a	0	0	0
UDP_Port_3973	17	n/a	0	0	0
UDP_Port_41474	41	n/a	0	0	0
UDP_Port_41812	0	n/a	0	0	0
UDP_Port_4246	215	n/a	0	0	2908
UDP_Port_43557	11	n/a	0	0	0
UDP_Port_43604	11	n/a	0	0	0
UDP_Port_4650	70	n/a	0	0	12
UDP_Port_46647	0	n/a	0	0	0
UDP_Port_48825	44	n/a	0	0	44
UDP_Port_49158	28	n/a	0	0	10
UDP_Port_49761	0	n/a	0	0	0
UDP_Port_51811	68	n/a	0	0	41
UDP_Port_57431	20	n/a	0	0	5
UDP_Port_57547	24	n/a	0	0	0
UDP_Port_57777	29	n/a	0	0	1231
UDP_Port_59304	13	n/a	0	0	917
UDP_Port_61755	38	n/a	0	0	10
UDP_Port_62336	60	n/a	0	0	406
UDP_Port_64281	19	n/a	0	0	7

UDP_Port_7001		507	n/a	0	0	365
UDP_Port_7275		2	n/a	0	0	30
UDP_Port_8683		0	n/a	0	0	0
Default	P I	40834	974261	272	367	616k
/Outbound	+		n/a	205k	183k	1.2M
Localhost	PE	33395	33395	0	0	0
DHCP		60	n/a	0	0	1265
eDonkey		37681	n/a	51k	50k	221k
FTP		1194	n/a	9	10	468k
Groupwise		185	n/a	0	0	51k
HTTP		383955	n/a	38k	26k	695k
IRC		5	n/a	0	0	1243
KaZaA		13409	n/a	4489	4299	917k
MPEG-Audio		111	n/a	0	0	9495
MPEG-Video		84	n/a	0	0	11k
MSN-Messenger		15414	n/a	1831	5645	256k
Napster		10	n/a	0	0	2016
Net2Phone		2	n/a	0	0	0
NTP		1936	n/a	0	6	155
POP3		2784	n/a	0	86	16k
QuickTime		8	n/a	0	0	18k
RDP		26	n/a	0	0	65k
Real		673	n/a	2205	1705	30k
RTCP-I		8	n/a	0	0	371
RTP-I		24	n/a	0	0	18k
SmartSockets		351	n/a	0	0	1159
SMTP		29076	n/a	22k	31k	1.1M
SNMP		23325	n/a	0	24	20k
SSL		17249	n/a	1410	1889	341k
Syslog		848	n/a	0	0	34
Telnet		39	n/a	0	0	36k
WebEx		19	n/a	0	0	6731
WinampStream		232	n/a	0	0	17k
WinMedia		4792	n/a	3017	2376	38k
YahooGames		15	n/a	0	0	3157
YahooMsg		705	n/a	10	30	3914
AOL-AIM-ICQ		494	n/a	4	13	8225
DCOM		1163	n/a	0	2	21k
DNS		166729	n/a	2619	1069	20k
Gnutella		201	n/a	0	0	6270
H.323		23	n/a	0	0	1708
ISAKMP		243	n/a	0	67	4508
Kontiki		1	n/a	0	0	0
NetBIOS-IP		744	n/a	0	0	4678
PeerEnabler		2717	n/a	44	40	34k
RTSP		540	n/a	0	3	18k
ICMP		222226	n/a	978	531	42k
IPSec		1425	n/a	16k	6832	521k
DiscoveredPorts			n/a	36k	41k	107k
TCP_Port_1998		196	n/a	0	0	6604
TCP_Port_21884		22	n/a	0	0	844
TCP_Port_25		296	n/a	10	18	1941
TCP_Port_55996		25	n/a	0	0	226
TCP_Port_9000		36	n/a	0	0	3413
TCP_Port_9004		88304	n/a	747	742	2604
UDP_Port_10410		11	n/a	0	0	0
UDP_Port_1138		16	n/a	0	0	42k
UDP_Port_1328		11	n/a	0	0	0
UDP_Port_1340		12	n/a	0	0	0

UDP_Port_1366	12	n/a	0	0	0
UDP_Port_1387	3	n/a	0	0	0
UDP_Port_14856	307	n/a	0	0	399
UDP_Port_1493	0	n/a	0	0	0
UDP_Port_17262	8	n/a	50k	39k	76k
UDP_Port_1731	23	n/a	0	0	0
UDP_Port_1852	1	n/a	0	0	4
UDP_Port_1897	27	n/a	0	0	0
UDP_Port_19017	15	n/a	0	0	0
UDP_Port_1907	13	n/a	0	0	0
UDP_Port_1950	25	n/a	0	0	435
UDP_Port_21721	0	n/a	0	0	0
UDP_Port_21884	34	n/a	0	0	43
UDP_Port_2239	13	n/a	0	0	0
UDP_Port_22482	26	n/a	0	0	216
UDP_Port_2327	16	n/a	0	0	288
UDP_Port_23698	58	n/a	0	0	0
UDP_Port_2463	0	n/a	0	0	0
UDP_Port_2570	0	n/a	0	0	0
UDP_Port_2587	26	n/a	0	0	0
UDP_Port_2647	12	n/a	0	0	0
UDP_Port_2731	31	n/a	0	0	3
UDP_Port_2744	12	n/a	0	0	0
UDP_Port_2774	15	n/a	0	0	43
UDP_Port_2873	1	n/a	0	0	0
UDP_Port_2912	14	n/a	0	0	0
UDP_Port_3016	19	n/a	0	0	95
UDP_Port_30245	14	n/a	0	0	0
UDP_Port_30260	66	n/a	0	0	1006
UDP_Port_3310	334	n/a	0	0	184
UDP_Port_33250	13	n/a	0	0	0
UDP_Port_34548	11	n/a	0	0	0
UDP_Port_3479	12	n/a	0	0	0
UDP_Port_3481	63	n/a	0	0	0
UDP_Port_35756	12	n/a	0	0	173
UDP_Port_3591	17	n/a	0	0	0
UDP_Port_3620	19	n/a	0	0	0
UDP_Port_3644	12	n/a	0	0	0
UDP_Port_3716	1	n/a	0	0	0
UDP_Port_3743	0	n/a	0	0	0
UDP_Port_3774	0	n/a	0	0	0
UDP_Port_38154	0	n/a	0	0	0
UDP_Port_3846	12	n/a	0	0	0
UDP_Port_3930	0	n/a	0	0	0
UDP_Port_39557	0	n/a	0	0	0
UDP_Port_3987	11	n/a	0	0	0
UDP_Port_41812	97	n/a	0	0	546
UDP_Port_4228	81	n/a	0	0	7
UDP_Port_4246	635	n/a	0	0	399
UDP_Port_43557	12	n/a	0	0	0
UDP_Port_44701	11	n/a	0	0	0
UDP_Port_4559	9	n/a	0	0	3
UDP_Port_45767	0	n/a	0	0	0
UDP_Port_4650	87	n/a	0	0	26
UDP_Port_46647	0	n/a	0	0	0
UDP_Port_46655	24	n/a	0	0	1
UDP_Port_48825	46	n/a	0	0	5
UDP_Port_49158	28	n/a	0	0	5
UDP_Port_49761	0	n/a	0	0	0
UDP_Port_51933	23	n/a	0	0	4
UDP_Port_5559	97	n/a	0	0	2

UDP_Port_57431		20	n/a	0	0	1
UDP_Port_57547		26	n/a	0	0	0
UDP_Port_58409		0	n/a	0	0	0
UDP_Port_60200		20	n/a	0	0	4
UDP_Port_62336		63	n/a	0	0	805
UDP_Port_63539		13	n/a	0	0	0
UDP_Port_64281		20	n/a	0	0	1
UDP_Port_7001		998	n/a	0	10	1131
UDP_Port_7275		2	n/a	0	0	25
UDP_Port_8190		22	n/a	0	0	0
UDP_Port_8665		43	n/a	0	0	0
UDP_Port_9		492	n/a	0	9	875
Default	P I	50782	1073769	767	473	286k

Tabla. 4.1. Árbol de clases del enlace de entrada y salida.

Este árbol muestra el monitoreo y la clasificación de flujos realizada por PacketShaper, en donde se observa que las clases de flujos que llaman la atención son eDonKey, KaZaA, HTTP, WinMedia, MPEG, MSN-Messenger, debido a que son las que más consumen el ancho de banda tanto en el enlace de entrada como en el de salida, lo anterior se deduce observando los parámetros mencionados en el capítulo anterior como son “peak rate” y “class hits”.

A continuación se presenta reportes y análisis detallados del tráfico que atraviesa el enlace de Internet, mediante las opciones que brinda el sistema administrador tales como los gráficos de “Top Ten”, utilización, eficiencia, bytes y otros análisis de las clases descubiertas.

4.2.2 Reportes y análisis antes de aplicar políticas.

4.2.2.1 Reporte general del tráfico del enlace de entrada.

En la Figura 4.2. se observa la utilización del enlace, tanto el tráfico pico (azul) como el tráfico promedio (rojo), se puede ver que en un lapso de tres días el enlace de entrada desde Internet hacia la red de Alegro, se satura gran parte del tiempo, por ejemplo desde el 04-05-2004 desde las 10:30 hasta la 22:00 el tráfico pico alcanza a la capacidad del enlace, en cuanto al tráfico promedio solamente en ocasiones llega a la totalidad del enlace, por ejemplo el 05-05-2004 a las 16:00.

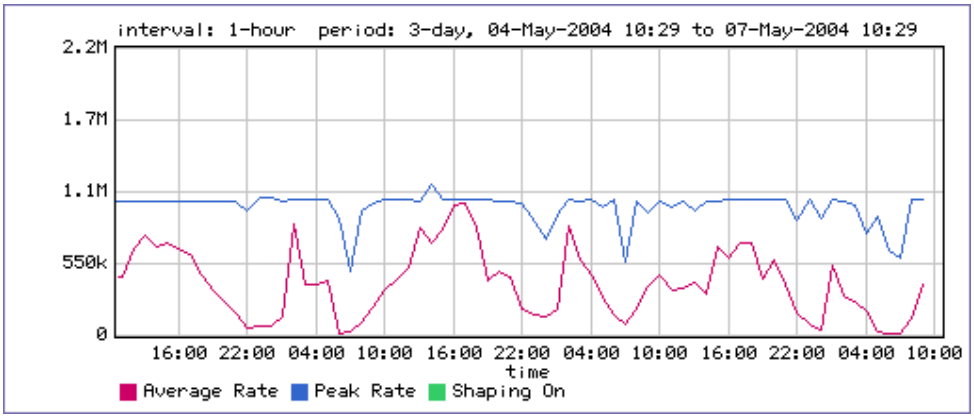


Figura. 4.2. Utilización del enlace de entrada.

En la Figura 4.3. se observa la eficiencia de la red en términos de retransmisiones y pérdidas de paquetes, en este gráfico se ve que existen momentos en que la eficiencia de red se degrada hasta un 80% aproximadamente.

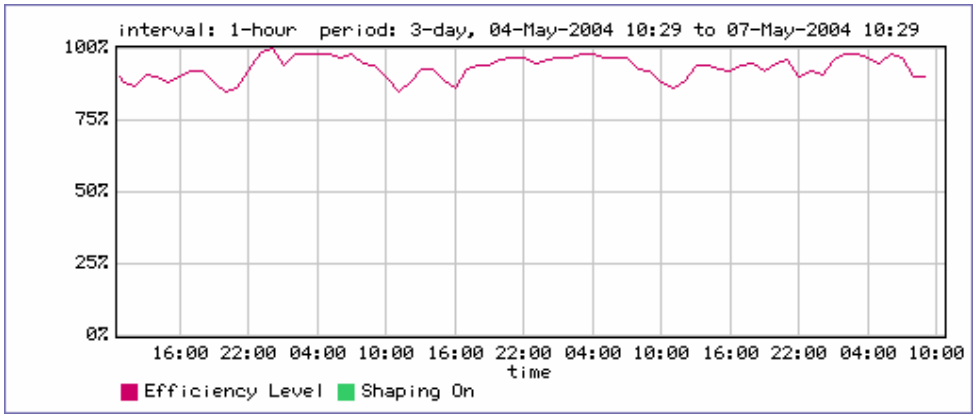


Figura. 4.3. Eficiencia de red del enlace de entrada.

Una vez que se ha analizado la utilización del canal y su eficiencia ahora se va a observar cuales son las aplicaciones que más consumen ancho de banda, en la Figura 4.4. se observa las 10 aplicaciones que más consumen ancho de banda promedio del enlace de entrada en un período de 3 días, se observa que existe un alto porcentaje de uso promedio del enlace de entrada de Internet por tráfico que no es importante para el desarrollo de la empresa.

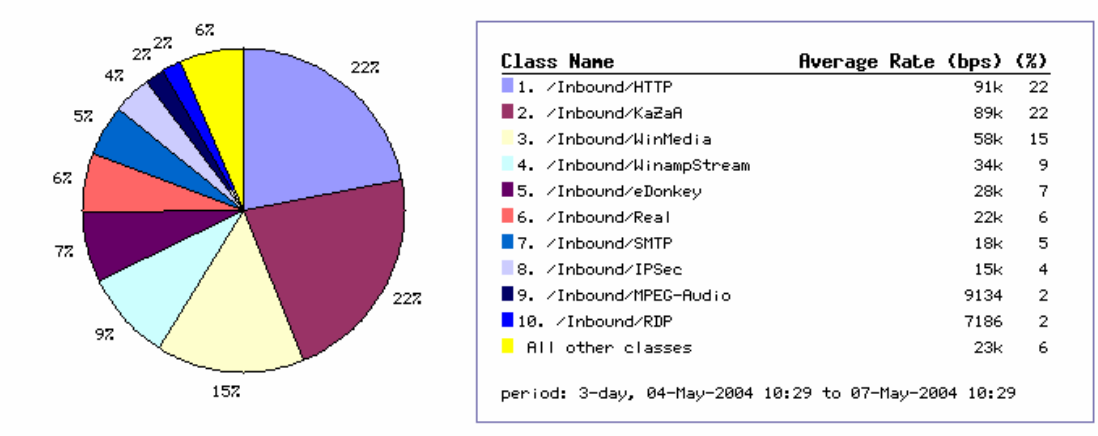


Figura. 4.4. "Top Ten" del enlace de entrada.

Todas las clases consumen un promedio de 394.32 Kbps del enlace de entrada, sumados los porcentajes de consumo de ancho de banda de los seis primeros tipos de tráfico el resultado da un aproximado de 81% equivalente a 322 Kbps promedio de consumo de los 394.32 Kbps, 59% equivalente a 231 Kbps de los 394.32 Kbps es de consumo de ancho de banda por tráfico no importante para la empresa (KaZaA, WinMedia, WinampStream, eDonkey, Real). En este período se comprueba la mala utilización del enlace de Internet, causando pérdidas económicas a la empresa, con los consumos anteriores por ejemplo si el costo mensual de un canal de Internet de 1 Mbps fuera de 4000 USD aproximadamente, por este tráfico de Internet se invierte 902 USD (231/1024*4000) mensuales, además de que sus empleados tal vez no brindan adecuadamente su tiempo para la empresa.

4.2.2.2 Reportes del tráfico "Top Ten" del enlace de entrada.

Se hizo un análisis más detallado de las aplicaciones que más consumen el ancho de banda de entrada ya que son aplicaciones que en su mayoría no son importantes para la empresa, causan pérdidas económicas y podrían causar problemas al enlace de Internet o a la Red de Area Local (LAN) en el futuro.

4.2.2.2.1 Protocolo de Transferencia de HiperTexto (HTTP).

En la Figura 4.5. se observa el uso del canal del enlace de entrada por tráfico del protocolo de transferencia, en el que se puede ver que el tráfico alcanza picos de hasta 1 Mbps y en promedio no supera los 500 Kbps.

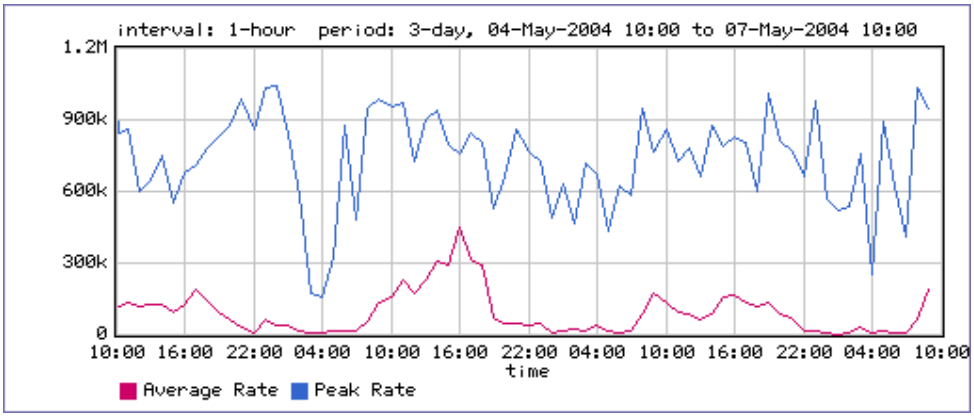


Figura. 4.5. Utilización del enlace de entrada por HTTP.

En la Figura 4.6. se observa el efecto que el protocolo de transferencia de hipertexto tiene sobre la eficiencia de la red.

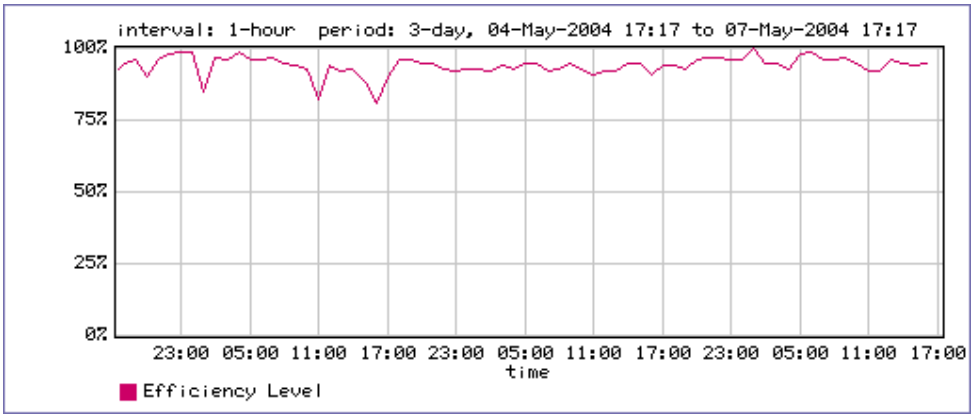


Figura. 4.6. Efecto de HTTP sobre la eficiencia de red del enlace de entrada.

4.2.2.2.2 KaZaA.

En la Figura 4.7. se observa el uso del canal del enlace de entrada por tráfico de la aplicación KaZaA, en el que se puede ver que alcanza picos de hasta 1 Mbps y el tráfico promedio también es alto con valores de hasta 800 Kbps.

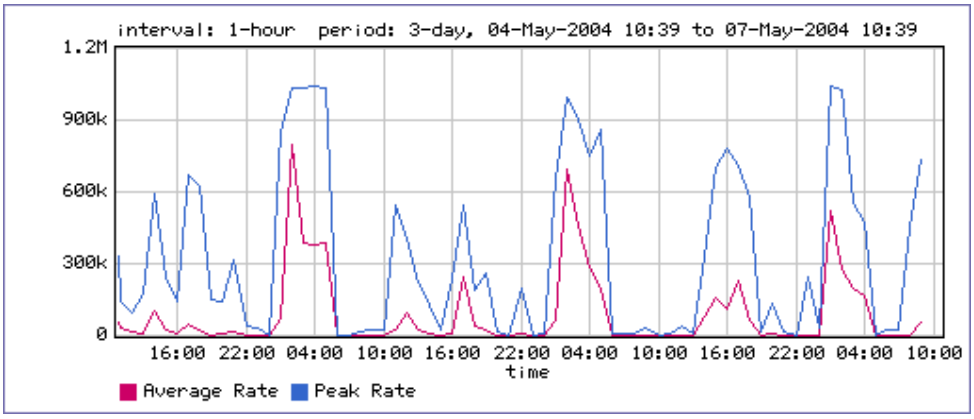


Figura. 4.7. Utilización del enlace de entrada por KaZaA.

En la Figura 4.8. se observa el efecto que la aplicación KaZaA tiene sobre la eficiencia de la red.

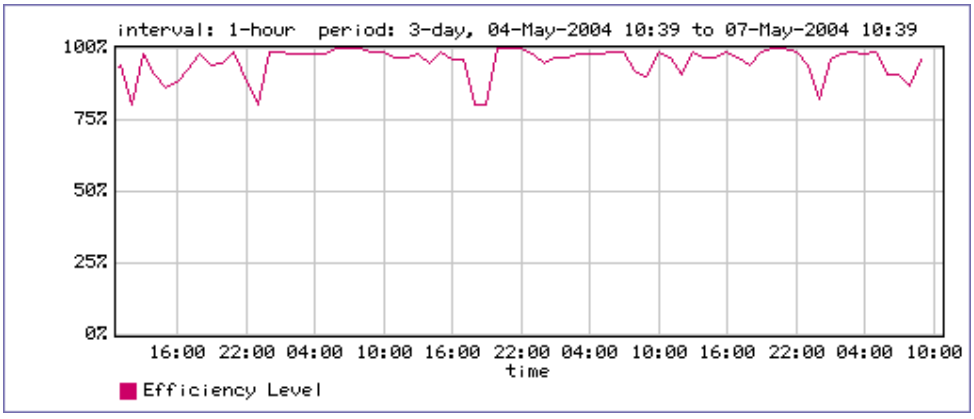


Figura. 4.8. Efecto de KaZaA sobre la eficiencia de red del enlace de entrada.

4.2.2.2.3 WinMedia.

En la Figura 4.9. se observa el uso del canal del enlace de entrada por tráfico de la aplicación WinMedia, en el que se puede ver que alcanza picos de hasta 1 Mbps y el tráfico promedio también es alto con valores de hasta 800 Kbps.

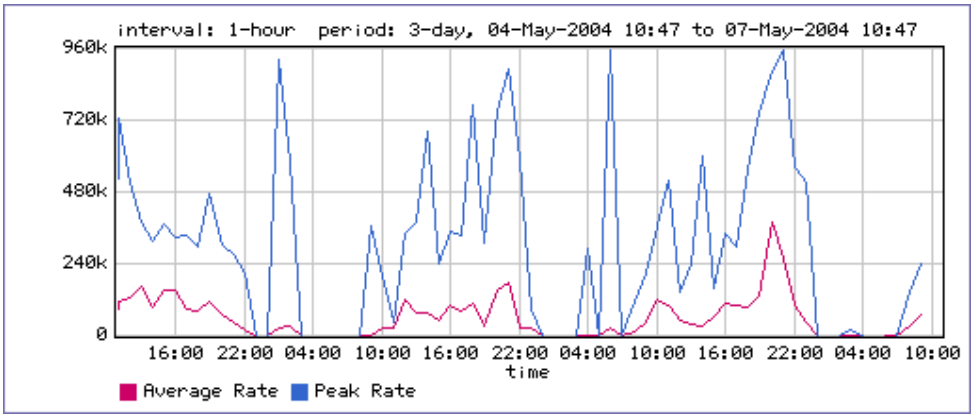


Figura. 4.9. Utilización del enlace de entrada por WinMedia.

En la Figura 4.10. se observa el efecto que la aplicación WinMedia tiene sobre la eficiencia de la red, en la que se puede apreciar que este tipo de tráfico afecta más a la eficiencia de la red comparando con las aplicaciones analizadas anteriormente.

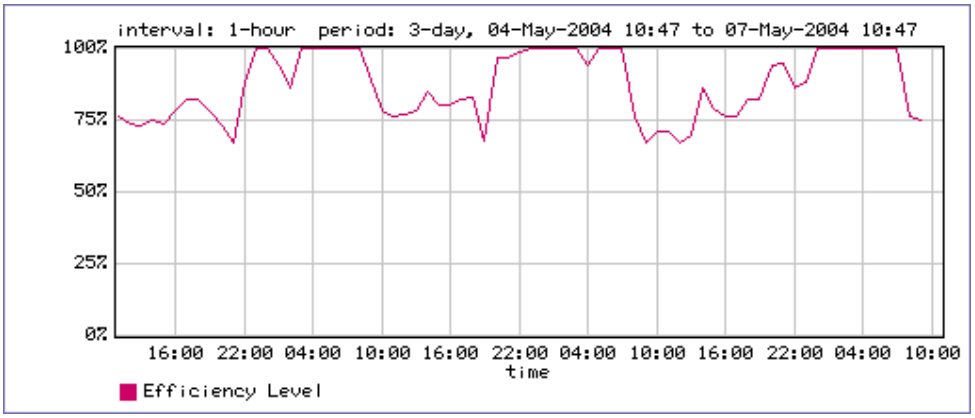


Figura. 4.10. Efecto de WinMedia sobre la eficiencia de red del enlace de entrada.

4.2.2.2.4 WinampStream.

En la Figura 4.11. se observa el uso del canal del enlace de entrada por tráfico de la aplicación WinampStream, en el que se puede ver que alcanza picos de hasta 580 Kbps y en promedio no sobrepasa los 280 Kbps.

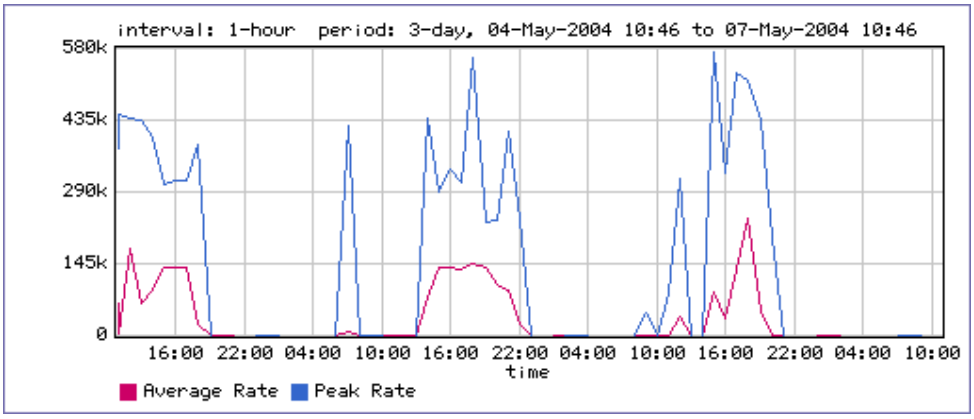


Figura. 4.11. Utilización del enlace de entrada por WinampStream.

En la Figura 4.12. se observa el efecto que la aplicación WinampStream tiene sobre la eficiencia de la red.

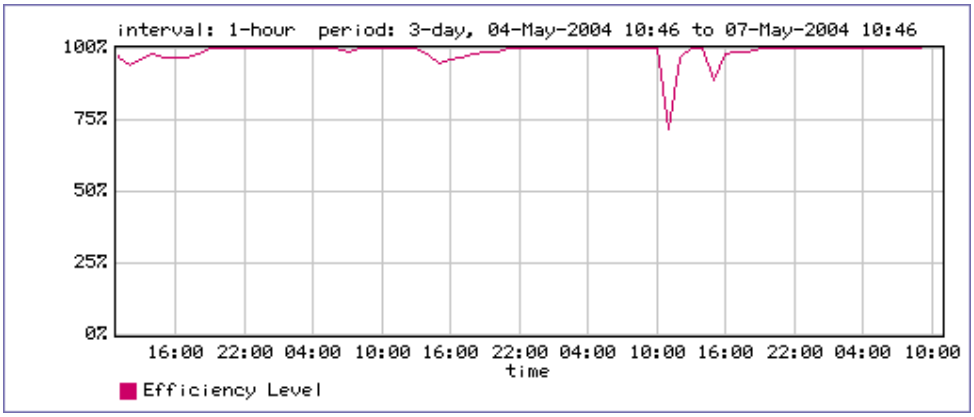


Figura. 4.12. Efecto de WinampStream sobre la eficiencia de red del enlace de entrada.

4.2.2.2.5 eDonkey.

En la Figura 4.13. se observa el uso del canal del enlace de entrada por tráfico de la aplicación eDonkey, en el que se puede ver que alcanza picos de hasta 340 Kbps y en promedio llega a valores de no mas de 100 Kbps.

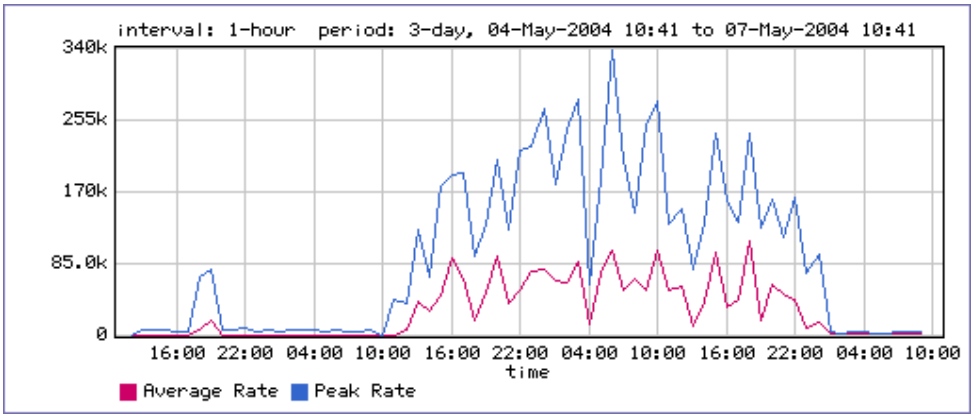


Figura. 4.13. Utilización del enlace de entrada por eDonkey.

En la Figura 4.14. se observa el efecto que la aplicación eDonkey tiene sobre la eficiencia de la red, en la que se puede apreciar que este tipo de tráfico la afectó en forma drástica bajando la eficiencia hasta cerca del 10% en un período cerca de las 10:00 del día 05-05-2004.

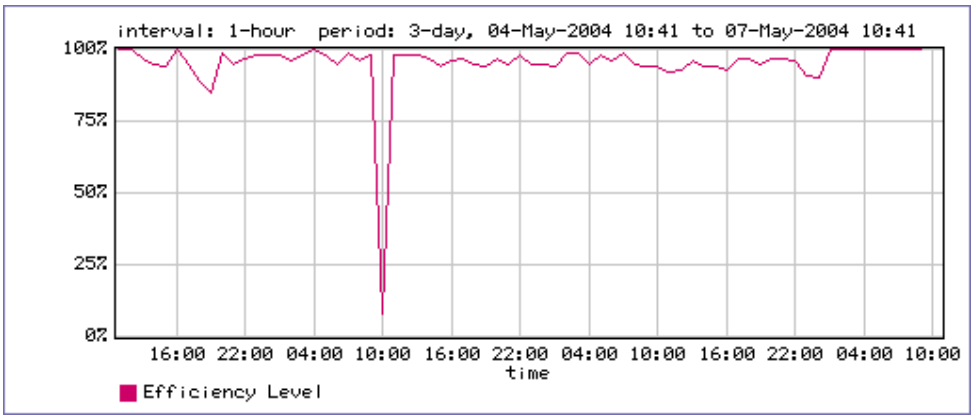


Figura. 4.14. Efecto de eDonkey sobre la eficiencia de red del enlace de entrada.

4.2.2.3 Reporte general del tráfico del enlace de salida.

En la Figura 4.15. se observa tanto el tráfico pico (azul), como el tráfico promedio (rojo), se observa que la utilización promedio del enlace de salida de la empresa hacia el Internet es baja en el lapso de tres días, con valores promedio de 350 Kbps como máximo, en tanto que el tráfico pico en algunos períodos satura el enlace de salida de Internet.

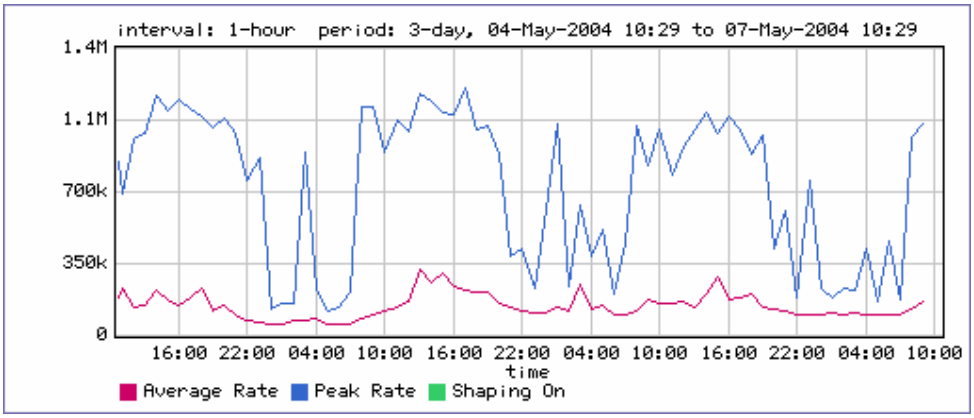


Figura. 4.15. Utilización del enlace de salida.

En la Figura 4.16. se observa la eficiencia de la red en términos de retransmisiones y pérdidas de paquetes, el gráfico muestra que la eficiencia de red para el enlace de salida no presenta problemas.

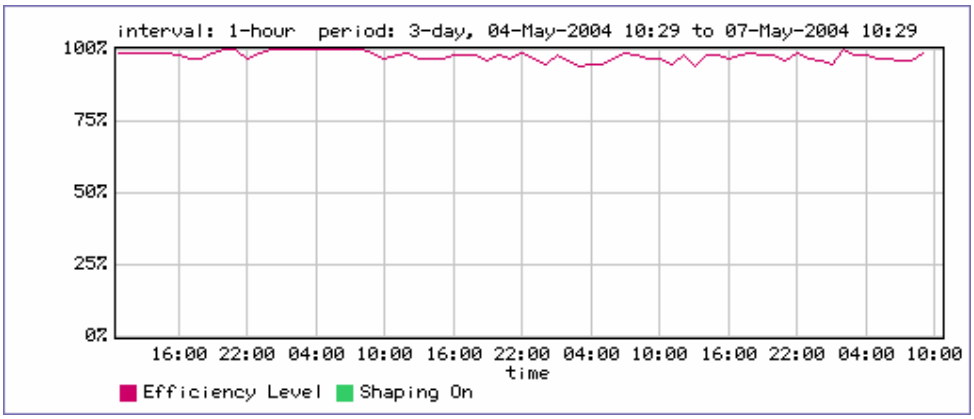


Figura. 4.16. Eficiencia de red del enlace de salida.

Una vez que se ha analizado la utilización del canal y su eficiencia ahora se va a observar cuales son las aplicaciones que más consumen ancho de banda, en la Figura 4.17. se observa las 10 aplicaciones que más consumen ancho de banda del enlace de salida en un período de 3 días, se observa que existe un considerable porcentaje de uso promedio del enlace de salida de Internet por tráfico que no es importante para el desarrollo de la empresa y un tipo de tráfico desconocido que utiliza protocolo UDP con puerto 17262, sin embargo este porcentaje de uso es menor comparado con el porcentaje del enlace de entrada.

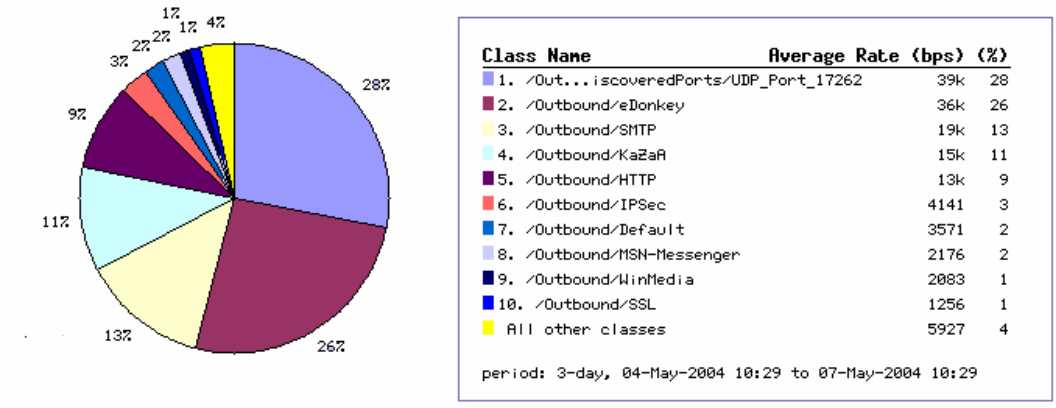


Figura. 4.17. "TopTen" del enlace de salida.

Todas las clases consumen un promedio de 141.154 Kbps del enlace de salida, sumados los porcentajes de consumo de ancho de banda de los seis primeros tipos de tráfico el resultado da un aproximado de 90% equivalente a 127.038 Kbps promedio de consumo de los 141.154 Kbps, 65% equivalente a 90 Kbps de los 141.154 Kbps de este consumo de ancho de banda es por tráfico no importante para la empresa y desconocido (Puerto UDP 17262, eDonkey, KaZaA). El consumo del enlace de salida es bajo en general y no presenta problemas, sin embargo este tráfico podría incrementarse debido al comportamiento de ciertas aplicaciones como KaZaA donde usuarios externos a la red de la empresa pueden conectarse simultáneamente incrementando el uso del enlace.

4.2.2.4 Reporte del tráfico "Top Ten" del enlace de salida.

Se hizo un análisis más detallado de las aplicaciones que más consumen el ancho de banda de salida ya que son aplicaciones que en su mayoría no son importantes para la empresa, podrían causar pérdidas económicas y problemas al enlace de Internet en el futuro.

4.2.2.4.1 KaZaA.

En la Figura 4.18. se observa el uso del canal del enlace de salida por tráfico de la aplicación KaZaA, en el que se puede ver que el tráfico pico alcanza valores de hasta 920 Kbps en tanto que el tráfico promedio no supera los 150 Kbps.

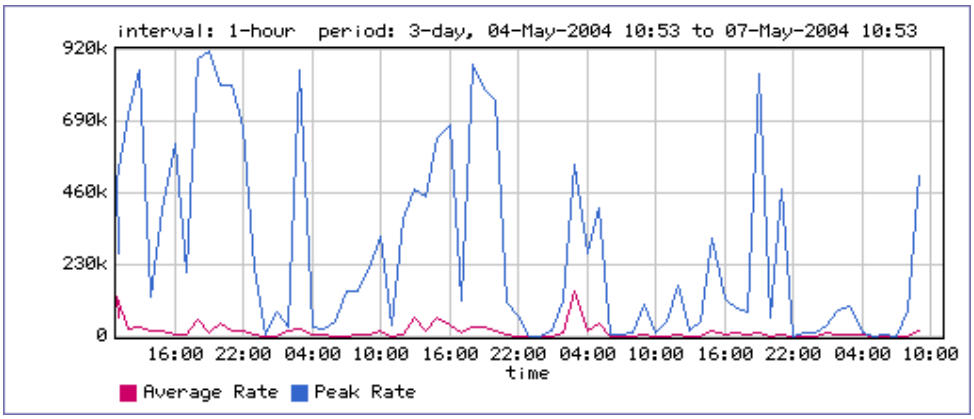


Figura. 4.18. Utilización del enlace de salida por KaZaA.

En la Figura 4.19. se observa el efecto que la aplicación KaZaA tiene sobre la eficiencia de la red.

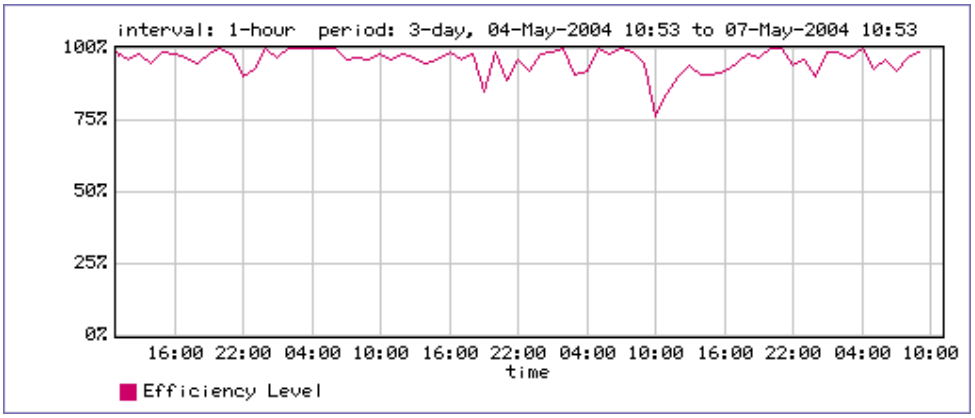


Figura. 4.19. Efecto de KaZaA sobre la eficiencia de red del enlace de salida.

4.2.2.4.2 eDonkey.

En la Figura 4.20. se observa el uso del canal del enlace de salida por tráfico de la aplicación eDonkey, en el que se puede ver que alcanza picos de hasta 240 Kbps y en promedio llega a valores de 60 Kbps.

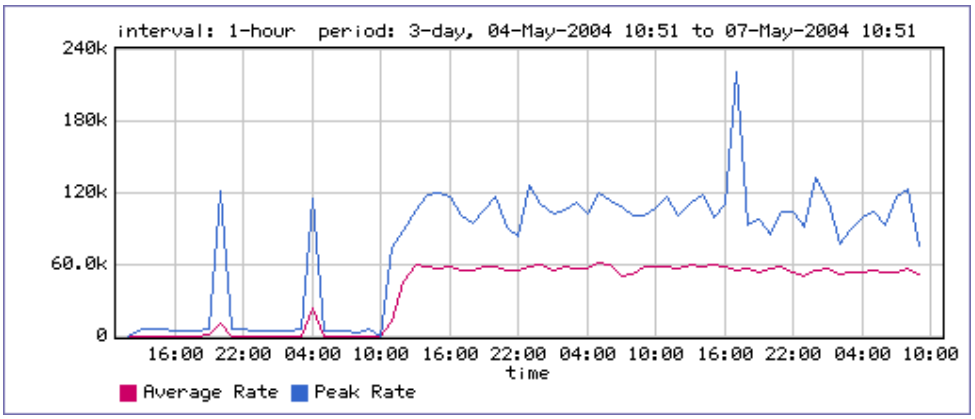


Figura. 4.20. Utilización del enlace de salida por eDonkey.

En la Figura 4.21. se observa el efecto que la aplicación eDonkey tiene sobre la eficiencia de la red, se observa que este tipo de tráfico no afecta mayormente a la red.

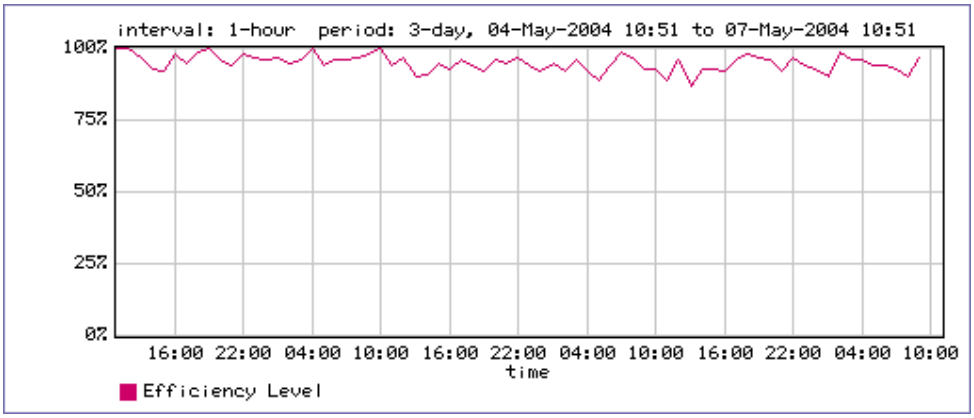


Figura. 4.21. Efecto de eDonkey sobre la eficiencia de red del enlace de salida.

4.2.2.4.3 Puerto UDP 17262.

En la Figura 4.22. se observa el uso del canal del enlace de salida para tráfico del puerto UDP 17262, en el que se puede ver que tanto el tráfico pico y promedio consumen 39 Kbps de manera continua y solamente en un período cerca de las 23:00 del 06-05-2004 el tráfico pico alcanzó un valor de 78 Kbps.

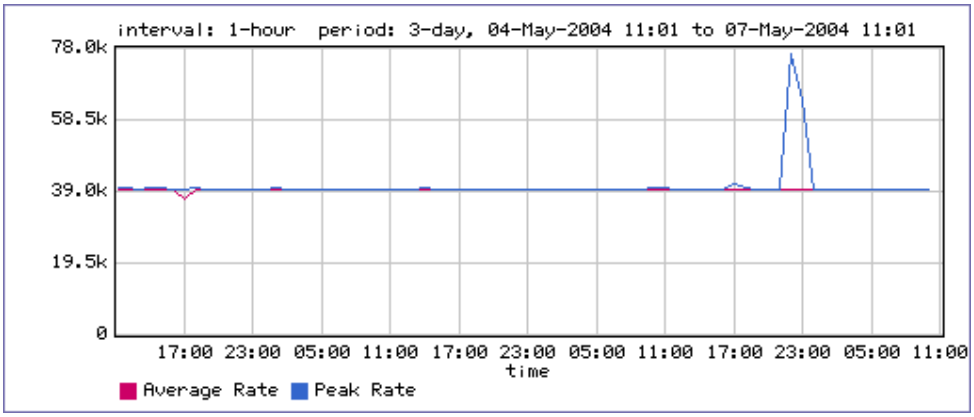


Figura. 4.22. Utilización del enlace de salida por UDP 17262.

En la Figura 4.23. se observa el efecto que el tráfico del puerto tiene sobre la eficiencia de la red, se observa que este tipo de tráfico no afecta a la red.

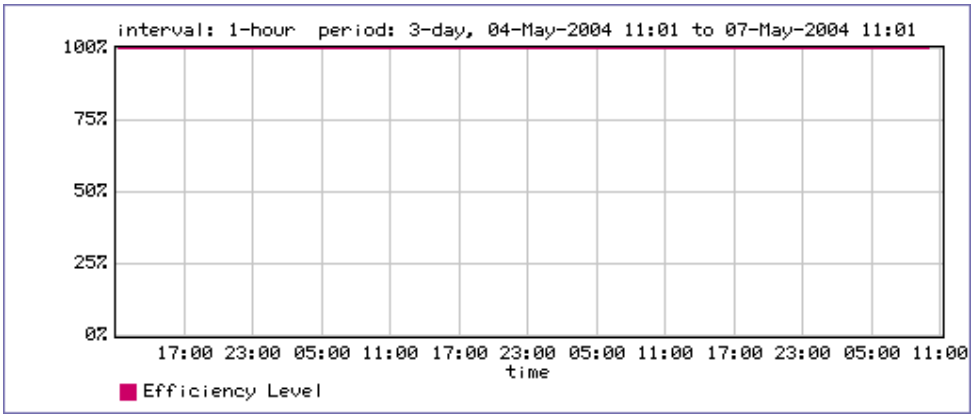


Figura. 4.23. Efecto de UDP 17262 sobre la eficiencia de red del enlace de salida.

Este tipo de tráfico no consume ancho de banda excesivamente y no afecta a la eficiencia de la red, pero se decidió investigarlo más detalladamente debido al consumo de ancho de banda extraño que presentaba, en la Figura 4.24. se observa la cantidad de bytes transmitidos, la cual alcanza 10 Mbps.

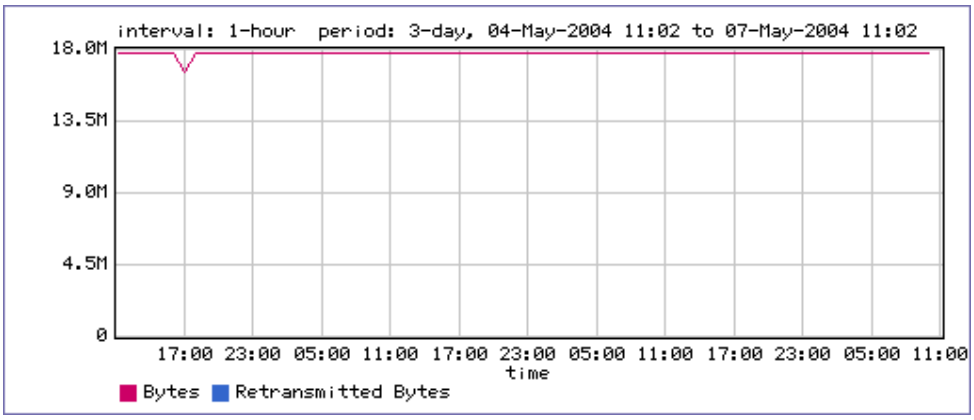


Figura. 4.24. Bytes transmitidos por UDP 17262 en el enlace de salida

En un análisis más amplio del tráfico de este puerto se obtuvo los computadores que generan y reciben este tráfico, para esto se utilizo el siguiente comando:

"PacketShaper# traffic flow /Outbound/DiscoveredPorts/UDP_Port_17262"

-----(/Outbound/DiscoveredPorts/UDP_Port_17262)-----

04-May-2004 17:13:18 UDP
200.41.114.253 35171
172.19.1.2 17262
04-May-2004 17:13:18 UDP
200.41.114.253 35171
172.19.1.1 17262
04-May-2004 17:13:18 UDP
200.41.114.253 35171
172.18.1.2 17262
04-May-2004 17:13:18 UDP
200.41.114.253 35171
172.18.1.1 17262

Este análisis indica que existe transmisión de información desde el servidor proxy con dirección IP 200.41.14.253 hacia las direcciones IP 172.19.1.2; 172.19.1.1; 172.18.1.2 y 172.18.1.1 en el Internet.

4.2.3 Políticas de control.

Del análisis anterior y pensando en cubrir las necesidades de control de Internet de la empresa, se decidió aplicar políticas como se observa en la Tabla 4.2.

Enlace	Tipo de tráfico	Política
Inbound	KaZaA	Nunca admitir
	eDonkey	Nunca admitir
	MPEG-Audio, WinampStream, WinMedia	Partición de 100 Kbps
Outbound	KaZaA	Nunca admitir
	eDonkey	Nunca admitir
	UDP_Port_17262	Partición de 20 Kbps

Tabla. 4.2. Políticas aplicadas al enlace de Internet.

Con estas políticas se trató de bloquear y controlar las principales aplicaciones descubiertas y clasificadas por PacketShaper en el enlace de Internet y que no son

productivas para la empresa, estas son KaZaA, eDonkey, Grupo de Expertos en Imágenes en Movimiento (MPEG) - Audio, WinampStream, WinMedia y tratar de limitar el ancho de banda a la aplicación desconocida que utiliza el puerto UDP 17262 con el fin de tratar de averiguar de que aplicación se trata.

No se aplicó políticas a las demás clases o aplicaciones debido a que su consumo de ancho de banda es bajo y no representan un problema para la red de la empresa.

En el enlace de entrada se creo dos carpetas, la primera llamada “controlado” a la que se le asignó la política de partición de 100 Kbps y contiene las clases MPEG-Audio, WinampStream, WinMedia como se observa en la Figura 4.25.

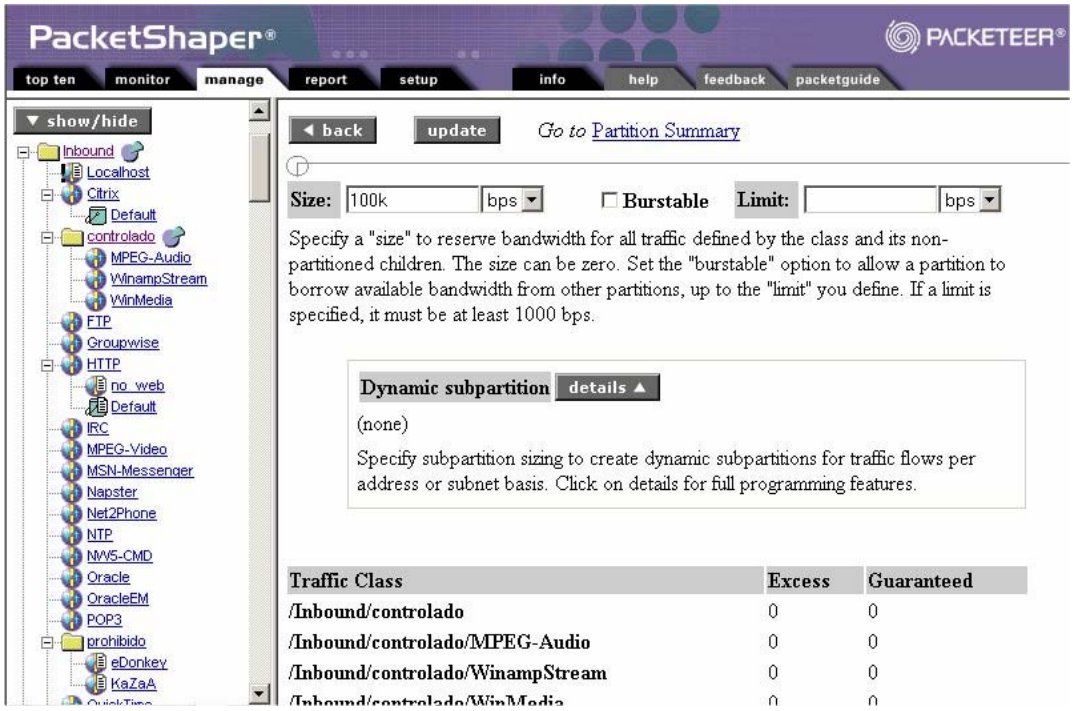


Figura. 4.25. Carpeta “controlado” con partición de 100 Kbps.

La segunda carpeta creada se la llamó “prohibido” a la que se le asignó la política de nunca admitir y contiene las clases de KaZaA y eDonkey como se observa en la Figura 4.26.

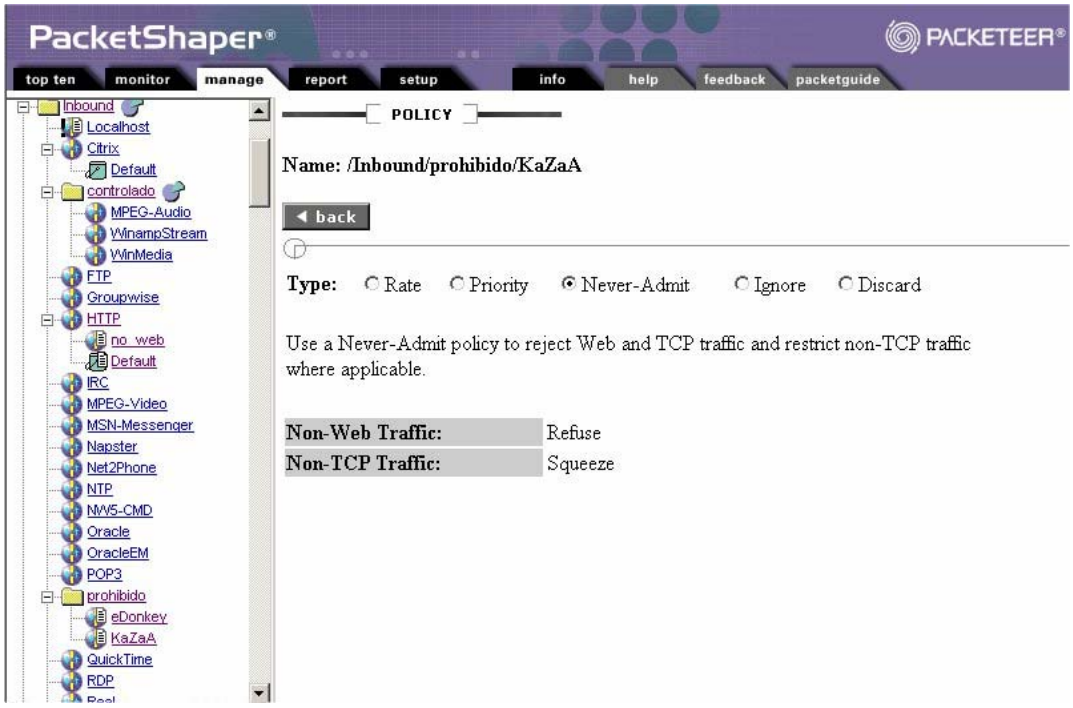


Figura. 4.26. Carpeta "prohibido" con política de nunca admitir.

En el enlace de salida se creo una carpeta "prohibido" a la que se le asigno la política nunca admitir y contiene las clases de KaZaA y eDonkey, además se aplicó directamente la política de partición de 20 Kbps a la clase UDP 17262, como se observa en la Figura 4.27.

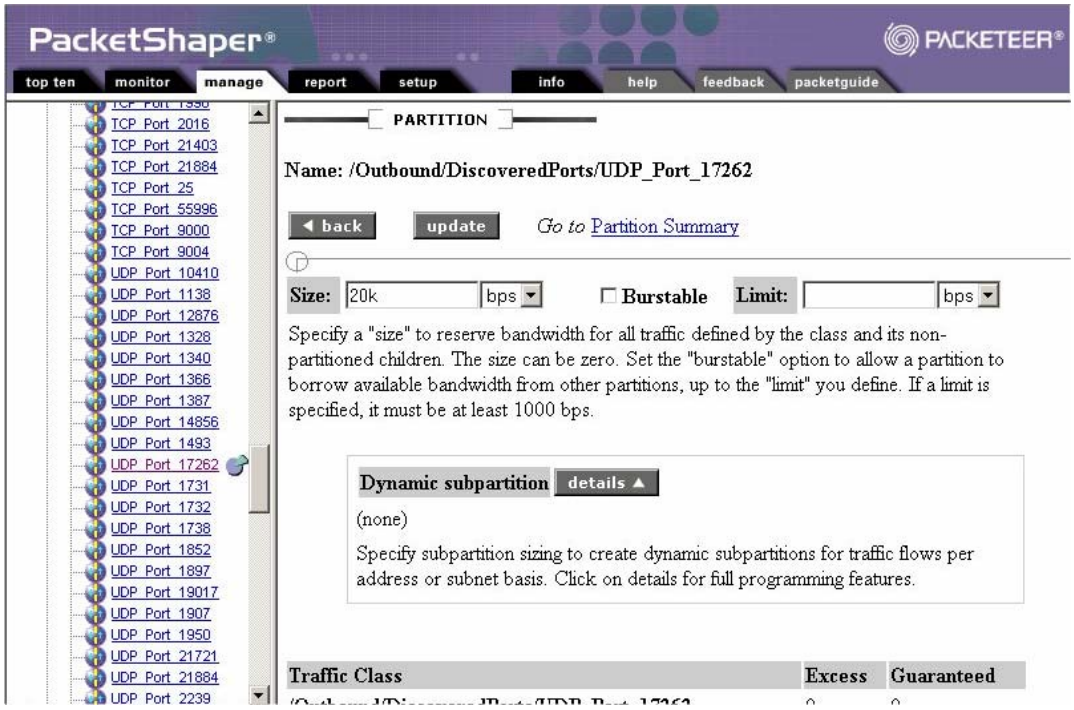


Figura. 4.27. Política de partición de 20 Kbps para UDP 17262.

4.2.4 Reportes y análisis después de aplicar políticas de control.

4.2.4.1 Reporte general del tráfico del enlace de entrada.

Se obtuvieron reportes de un período de un día para observar el comportamiento del enlace de Internet una vez aplicadas las políticas de control.

En la Figura 4.28. se observa el tráfico pico (azul), el tráfico promedio (rojo) y una línea que muestra que las políticas de control han sido aplicadas (verde), se observa que la utilización promedio del enlace de entrada desde Internet hacia Alegro es baja en el lapso de un día, con valores promedio de 300 Kbps como máximo, en tanto que el tráfico pico en algunos períodos cortos satura el enlace de entrada de Internet. La utilización promedio ha bajado después de aplicar políticas de control comparando con la utilización del enlace de entrada como se observa en la Figura 4.2 que es aproximadamente 390 Kbps, además el enlace de entrada se satura menos con tráfico pico después de haber aplicado las políticas de control.

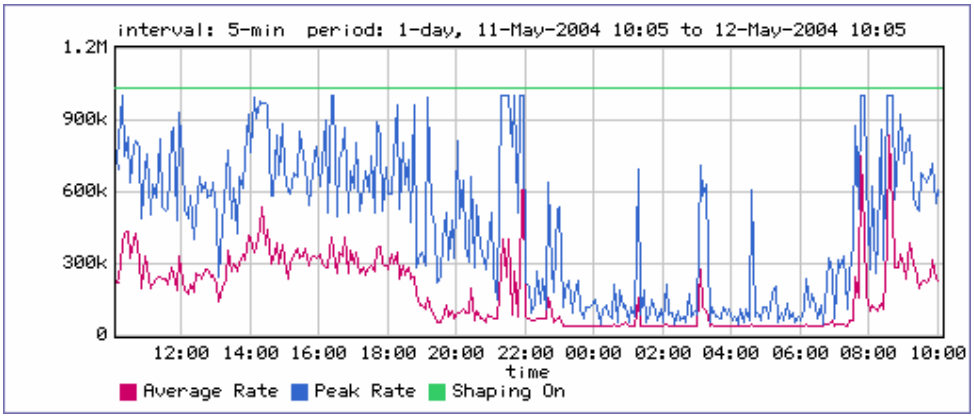


Figura. 4.28. Utilización del enlace de entrada con políticas.

En la Figura 4.29. se observa la eficiencia de la red en términos de retransmisiones y pérdidas de paquetes, el gráfico muestra que la eficiencia de red para el enlace de entrada sobrepasa la mayoría del tiempo el 87% mostrando una mejoría respecto a la eficiencia antes de aplicar políticas como se observa en la Figura 4.3.

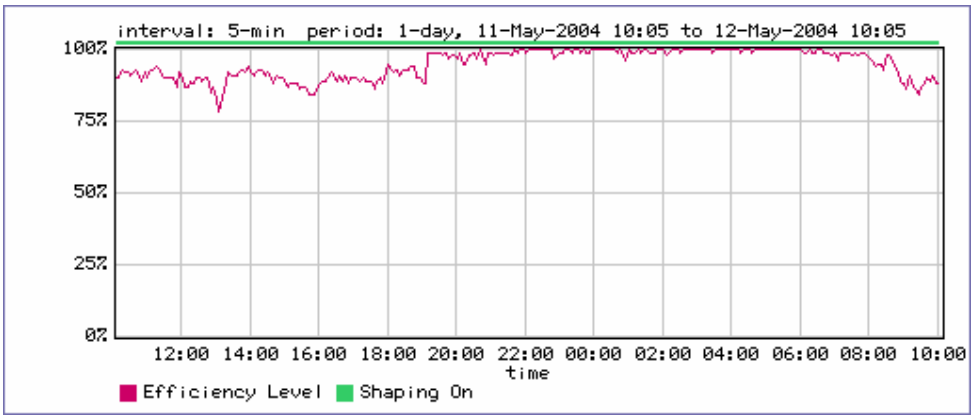


Figura. 4.29. Eficiencia de red del enlace de entrada con políticas.

Una vez que se ha analizado la utilización del canal y su eficiencia ahora se va a observar cuales son las aplicaciones que más consumen ancho de banda una vez aplicadas las políticas, en la Figura 4.30. se observa las 10 aplicaciones que más consumen el ancho de banda del enlace de salida.

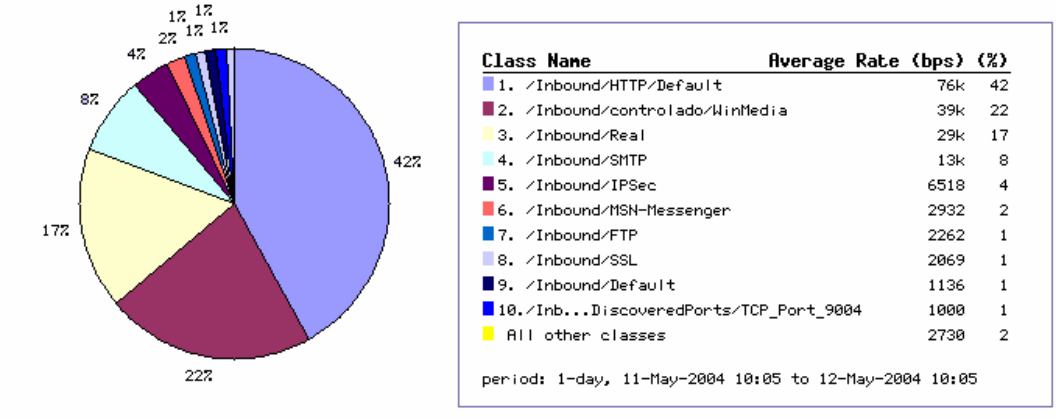


Figura. 4.30. "TopTen" del enlace de entrada con políticas.

Se observa que las aplicaciones prohibidas ya no aparecen en el "Top Ten" y de las aplicaciones controladas aparece solamente la aplicación WinMedia pero con un promedio bajo de 39 Kbps. El consumo total promedio de ancho de banda es 175.64 Kbps que es menor a los 394.32 Kbps antes de aplicar las políticas de control, este ahorro de ancho de banda logrado bloqueando y controlando aplicaciones no importantes puede ser utilizado por otras aplicaciones ó protocolos que necesiten más ancho de banda, como por ejemplo el Protocolo de Transferencia de HiperTexto (HTTP).

4.2.4.2 Reporte de tráfico "Top Ten" del enlace de entrada.

Se hizo un análisis más detallado de las mismas aplicaciones que se hizo antes de aplicar políticas de control.

4.2.4.2.1 KaZaA.

En la Figura 4.31. se observa que el tráfico de la aplicación KaZaA fue bloqueado a partir del 07-05-2004, es decir desde el instante en el que se le aplicó la política nunca admitir.

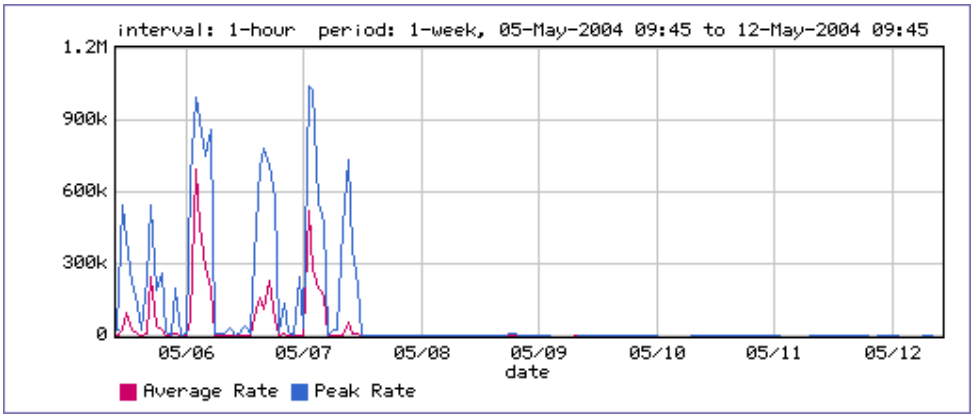


Figura. 4.31. Utilización del enlace de entrada por KaZaA con políticas.

En la Figura 4.32. se observa que a partir del momento en que se aplicó la política de control la eficiencia de red mejoró hasta el 100% respecto al tráfico de la aplicación KazaA mostrando que esta aplicación fue bloqueada completamente.

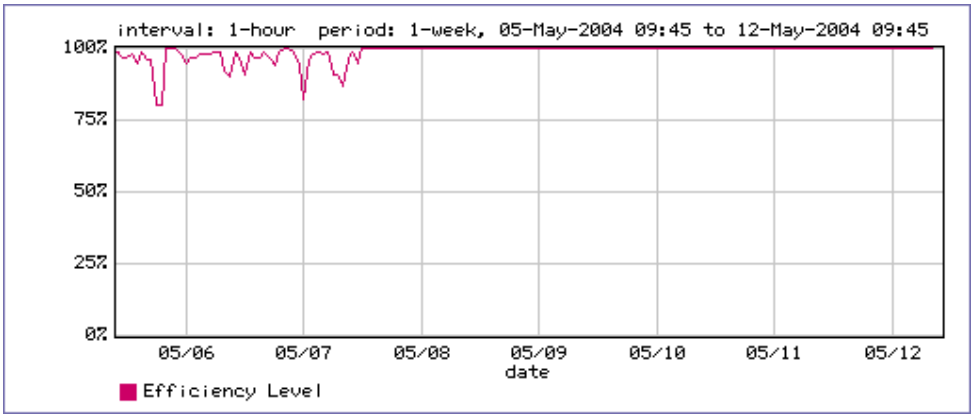


Figura. 4.32. Efecto de KaZaA sobre la eficiencia de red de "Inbound" con políticas.

4.2.4.2.2 eDonkey.

En la Figura 4.33. se observa que el tráfico de la aplicación eDonkey fue bloqueado a partir del 07-05-2004, es decir desde el instante en el que se le aplicó la política nunca admitir.

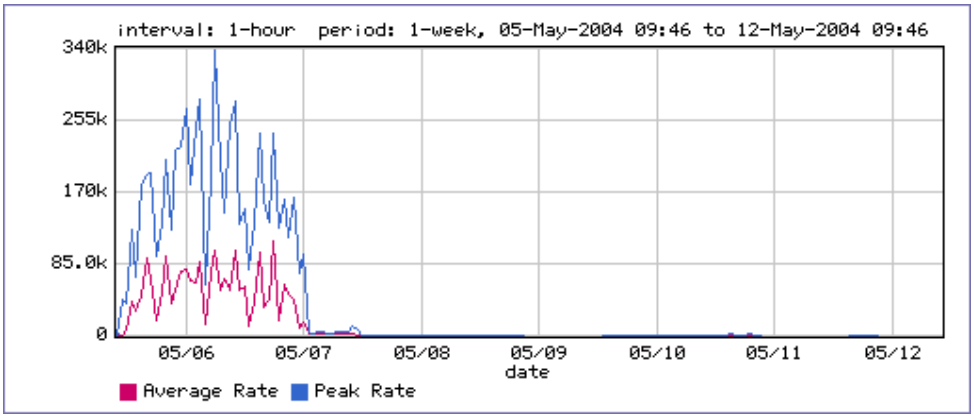


Figura. 4.33. Utilización del enlace de entrada por eDonkey con políticas.

En la Figura 4.34. se observa que a partir del momento en que se aplicó la política de control la eficiencia de red mejoró hasta el 100% respecto al tráfico de la aplicación eDonkey mostrando que esta aplicación fue bloqueada completamente.

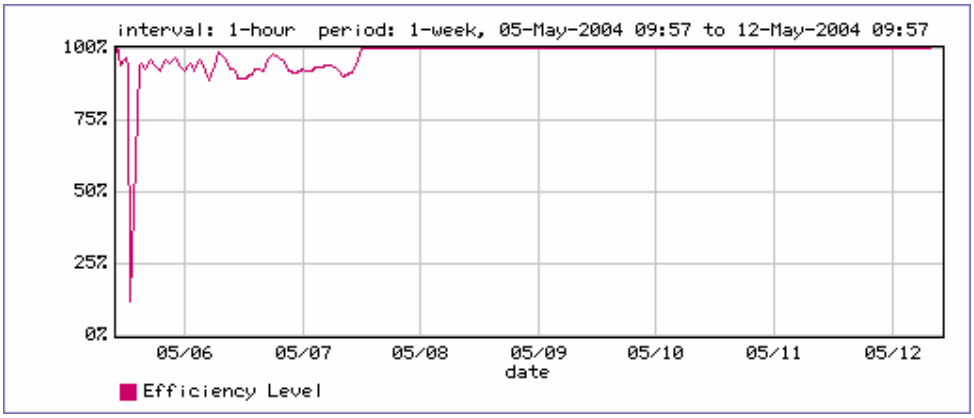


Figura. 4.34. Efecto de eDonkey sobre la eficiencia de red de "Inbound" con políticas.

4.2.4.2.3 Grupo de Expertos en Imágenes en Movimiento (MPEG) - Audio.

En la Figura 4.35. se observa que el tráfico de la aplicación MPEG-Audio fue controlado a partir del 07-05-2004, es decir desde el instante en el que se le aplicó la política no sobrepaso los 100 Kbps.

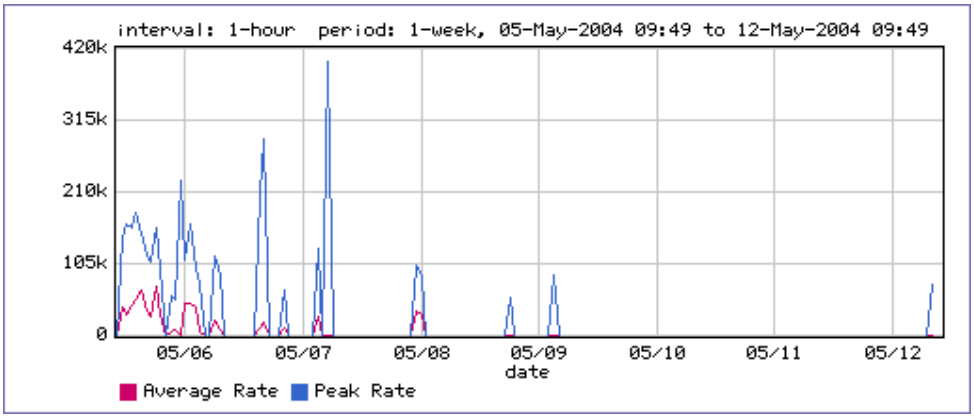


Figura. 4.35. Utilización del enlace de entrada por MPEG-Audio con políticas.

En la Figura 4.36 se observa que a partir del momento en que se aplicó la política de control la eficiencia de red mejoró hasta un 100% la mayoría del tiempo, decayendo en cinco períodos de aproximadamente 1 y 2 horas y máximo hasta un 90% respecto al tráfico de la aplicación MPEG-Audio mostrando que esta aplicación fue controlada.

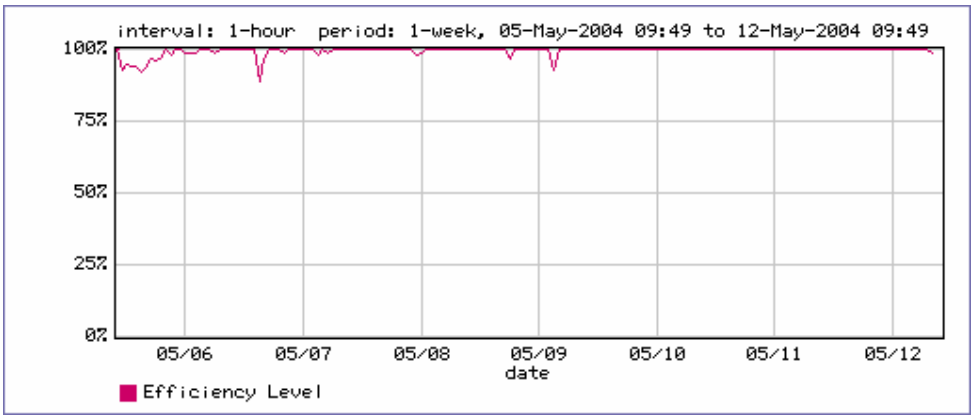


Figura. 4.36. Efecto de MPEG-Audio sobre la eficiencia de red de "Inbound" con políticas.

4.2.4.2.4 WinampStream.

En la Figura 4.37 se observa que el tráfico de la aplicación WinampStream fue controlado a partir del 07-05-2004, es decir desde el instante en el que se le aplicó la política no sobrepaso los 100 Kbps.

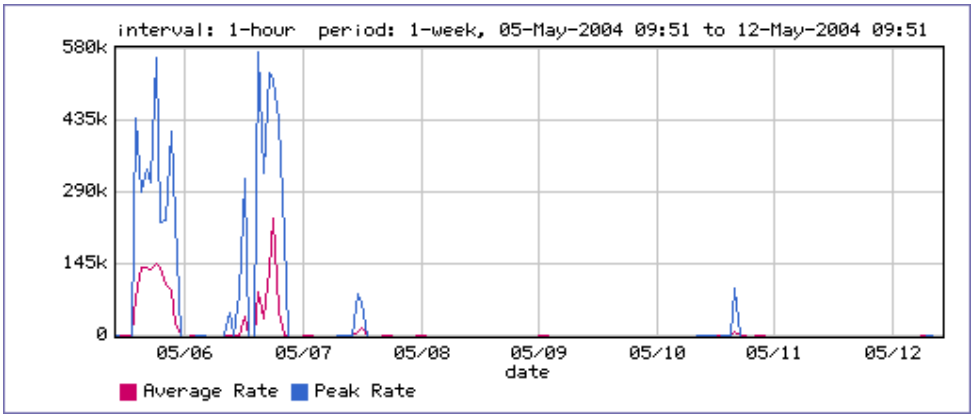


Figura. 4.37. Utilización del enlace de entrada por WinampStream con políticas.

En la Figura 4.38. se observa que a partir del momento en que se aplicó la política de control la eficiencia de red mejoró hasta un 100% la mayoría del tiempo, decayendo en dos períodos de aproximadamente 2 horas y máximo hasta un 90% respecto al tráfico de la aplicación MPEG-Audio mostrando que esta aplicación fue controlada.

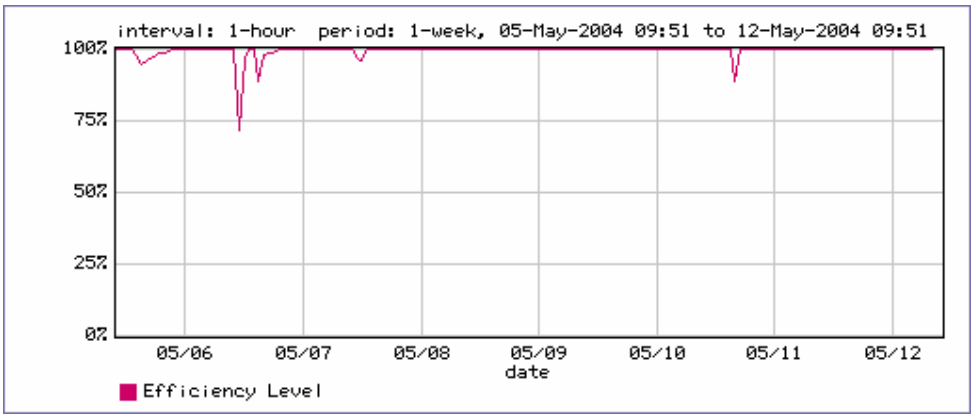


Figura. 4.38. Efecto de WinampStream sobre la eficiencia de red de "Inbound" con políticas.

4.2.4.2.5 WinMedia.

En la Figura 4.39 se observa que el tráfico de la aplicación WinMedia fue controlado a partir del 07-05-2004, es decir desde el instante en el que se le aplicó la política no sobrepaso los 100 Kbps.

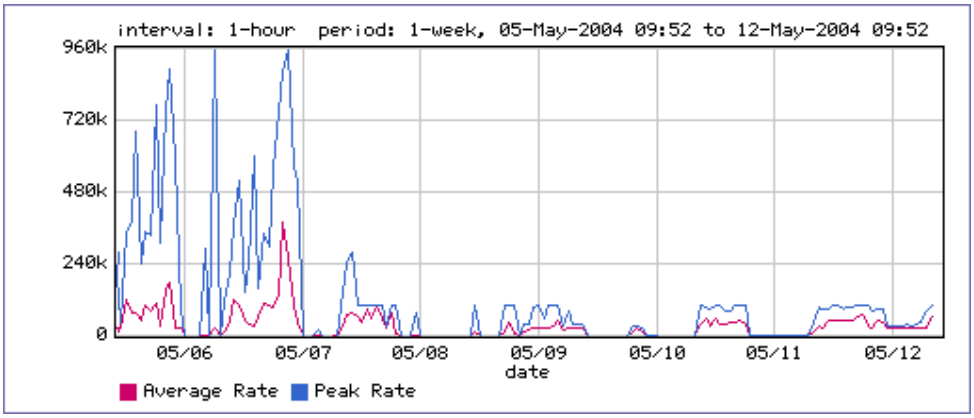


Figura. 4.39. Utilización del enlace de entrada por WinMedia con políticas.

En la Figura 4.40. se observa que a partir del momento en que se aplicó la política de control la eficiencia de red experimenta una mejoría con respecto a esta aplicación, sin embargo no es mucha la mejoría, la explicación es que antes de aplicar la política de 100 Kbps el tráfico promedio se mantenía cerca de 100 Kbps por lo que con esta política de 100 Kbps no se redujo su consumo de ancho de banda dando como resultado una eficiencia de red con políticas similar a la que se obtuvo antes de aplicar políticas. Para mejorar se debería aplicar una política de partición para esta aplicación con una tasa de datos menor que los 100 Kbps que se aplicó.

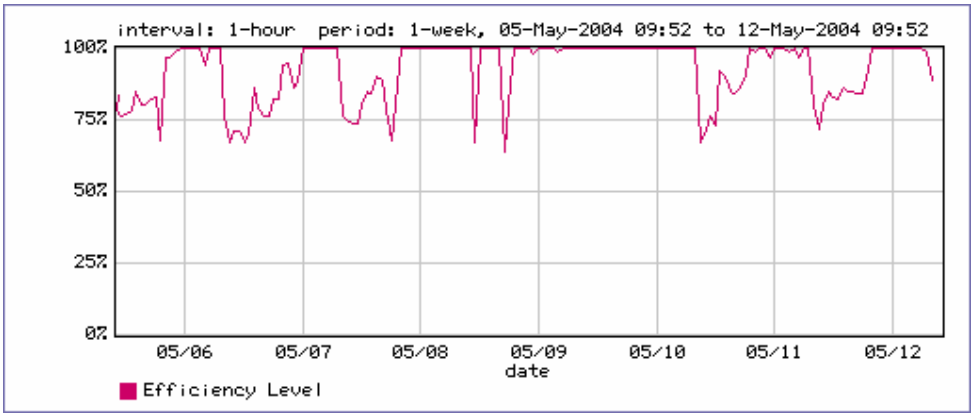


Figura. 4.40. Efecto de WinMedia sobre la eficiencia de red de "Inbound" con políticas.

4.2.4.3 Reporte general del tráfico de salida.

Se obtuvieron reportes de un período de un día para observar el comportamiento del enlace de Internet una vez aplicadas las políticas de control.

En la Figura 4.41. se observa el tráfico pico (azul), el tráfico promedio (rojo) y una línea que muestra que las políticas de control han sido aplicadas (verde), se observa que la utilización promedio del enlace de salida desde Alegro hacia el Internet es baja en el lapso de un día, con valores promedio aproximadamente de 80 Kbps como máximo, en tanto que el tráfico pico en algunos períodos cortos satura el enlace de salida de Internet. La utilización promedio ha bajado después de aplicar políticas de control comparando con la utilización del enlace de entrada como se observa en la Figura 4.15. que es aproximadamente 150 Kbps, además el enlace de salida se satura menos con tráfico pico después de haber aplicado las políticas de control.

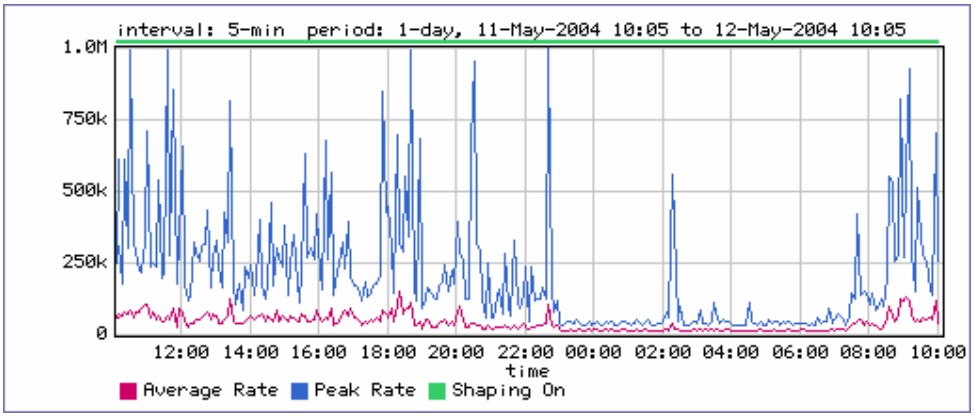


Figura. 4.41. Utilización del enlace de salida con políticas.

En la Figura 4.42. se observa la eficiencia de la red en términos de retransmisiones y pérdidas de paquetes, el gráfico muestra que la eficiencia de red para el enlace de salida sobrepasa la mayoría del tiempo el 87%, comparando esta eficiencia con la eficiencia antes de aplicar políticas como se observa en la Figura 4.16. no se encuentra mayor diferencia, esto se debe a que las aplicaciones prohibidas y controladas en el enlace de salida no presentaban un consumo importante del ancho de banda.

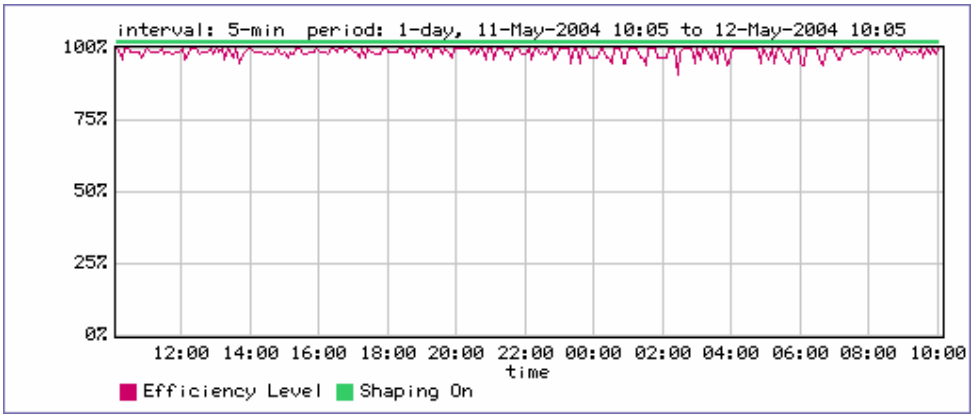


Figura. 4.42. Eficiencia de red del enlace de salida con políticas.

Una vez que se ha analizado la utilización del canal y su eficiencia ahora se va a observar cuales son las aplicaciones que más consumen ancho de banda una vez aplicadas las políticas, en la Figura 4.43. se observa las 10 aplicaciones que más consumen el ancho de banda del enlace de salida.

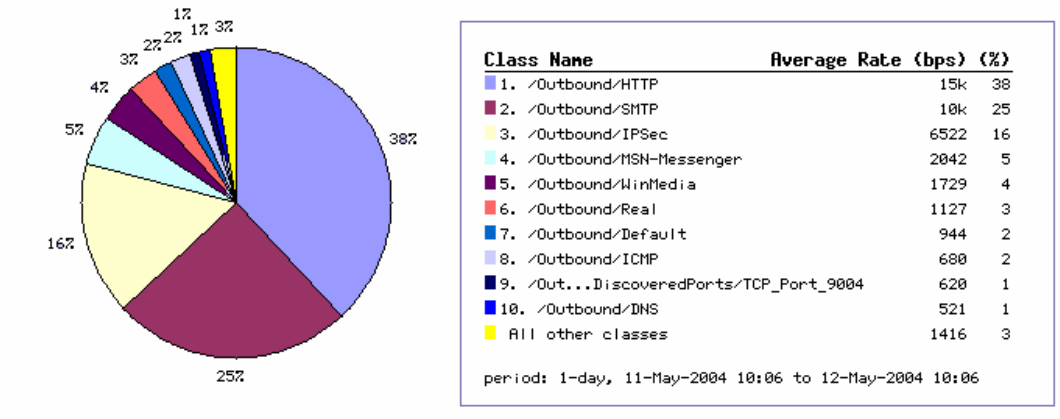


Figura. 4.43. "Top Ten" del enlace de salida con políticas.

Se observa que las aplicaciones prohibidas ya no aparecen en el "Top Ten" y de las aplicaciones controladas aparece solamente la aplicación WinMedia pero con un promedio bajo de 1.729 Kbps. El consumo total promedio de ancho de banda es 40.5 Kbps que es menor a los 141.154 Kbps antes de aplicar las políticas de control, este ahorro de ancho de banda logrado bloqueando y controlando aplicaciones no importantes puede ser utilizado

por otras aplicaciones o protocolos que necesiten más ancho de banda, como por ejemplo el Protocolo de Transferencia de HiperTexto (HTTP) y/o el Protocolo de Transferencia de Mail Simple (SMTP).

4.2.4.4 Reportes de tráfico "Top Ten" del enlace de salida.

Se hizo un análisis más detallado de las mismas aplicaciones que se hizo antes de aplicar políticas de control.

4.2.4.4.1 KaZaA.

En la Figura 4.44. se observa que el tráfico de la aplicación KaZaA fue controlado a partir del 07-05-2004, es decir desde el instante en el que se le aplicó la política nunca admitir.

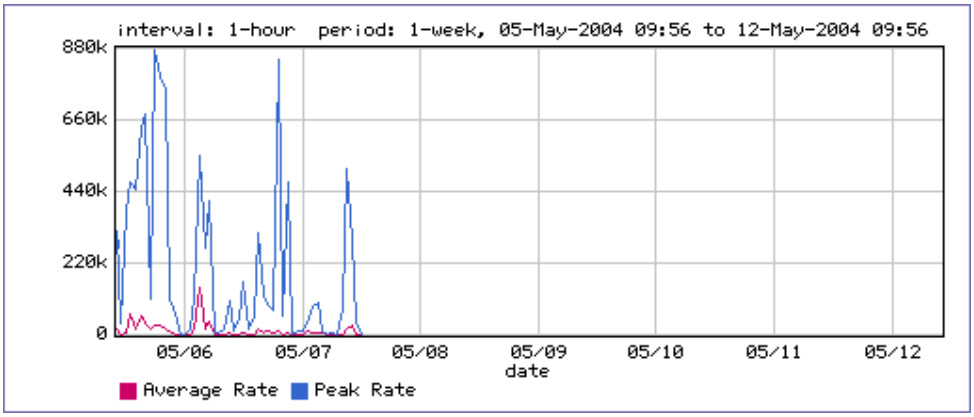


Figura. 4.44. Utilización del enlace de salida por KaZaA con políticas.

En la Figura 4.45. se observa que a partir del momento en que se aplicó la política de control la eficiencia de red mejoró hasta el 100% respecto al tráfico de la aplicación KazaA mostrando que esta aplicación fue bloqueada completamente.

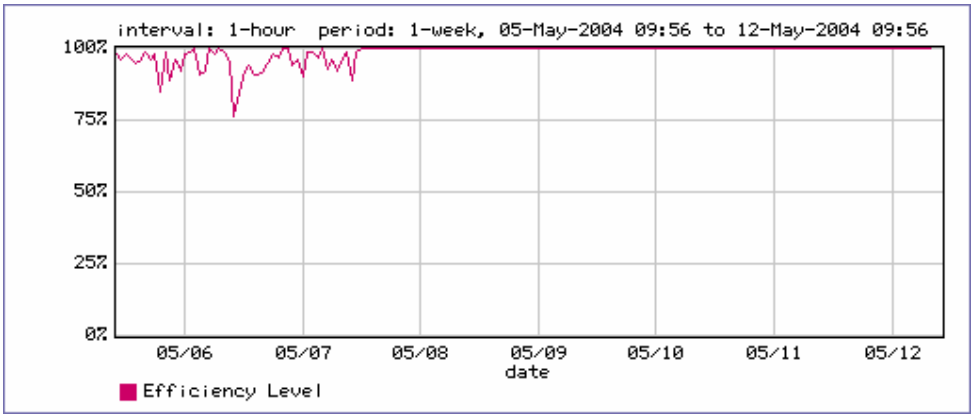


Figura. 4.45. Efecto de KaZaA sobre la eficiencia de red de "Outbound" con políticas.

4.2.4.4.2 eDonkey.

En la Figura 4.46. se observa que el tráfico de la aplicación eDonkey fue controlado a partir del 07-05-2004, es decir desde el instante en el que se le aplicó la política nunca admitir.

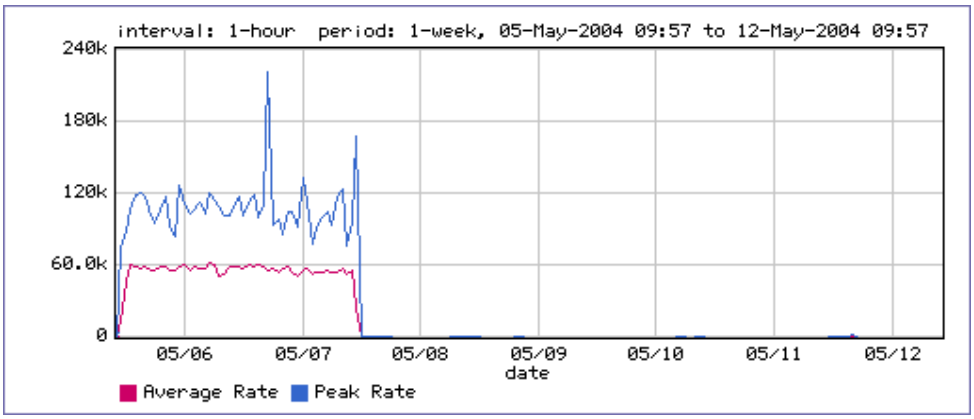


Figura. 4.46. Utilización del enlace de salida por eDonkey con políticas.

En la Figura 4.47. se observa que a partir del momento en que se aplicó la política de control la eficiencia de red mejoró hasta el 100% respecto al tráfico de la aplicación eDonkey mostrando que esta aplicación fue bloqueada completamente.

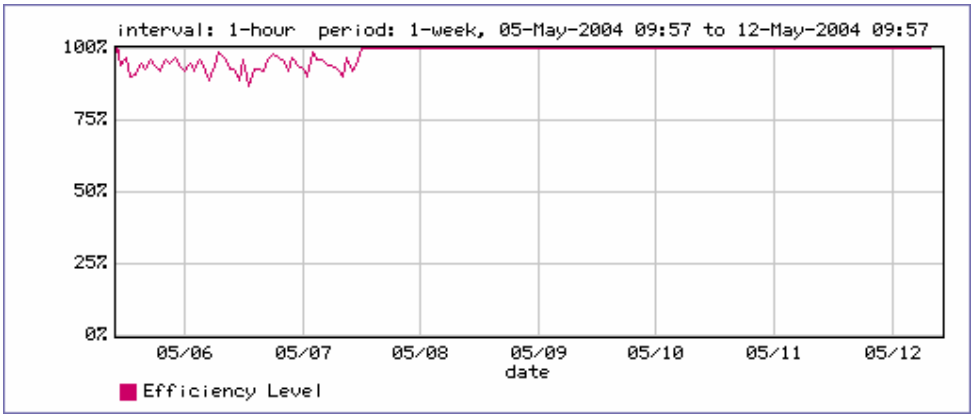


Figura. 4.47. Efecto de eDonkey sobre la eficiencia de red de "Outbound" con políticas.

4.2.4.4.3 Puerto UDP 17262.

En la Figura 4.48. se observa que el tráfico de UDP 17262 fue controlado a partir del 07-05-2004, es decir desde el instante en el que se le aplicó la política no sobrepaso los 20 Kbps hasta el 10-05-2004 en donde se cambió la política a 1 Kbps.

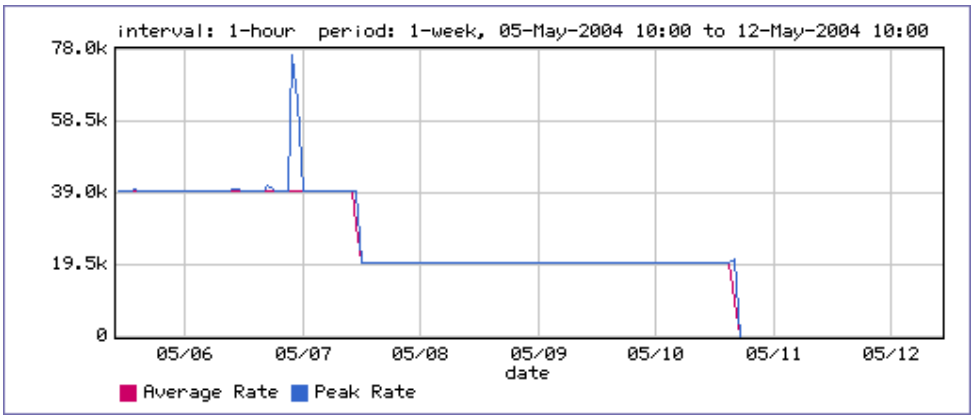


Figura. 4.48. Utilización del enlace de salida por UDP 17262 con políticas.

En la Figura 4.49. se observa que la eficiencia de la red no varía y se mantiene en 100% con respecto al flujo de este puerto UDP debido a que su consumo de ancho de banda es bajo.

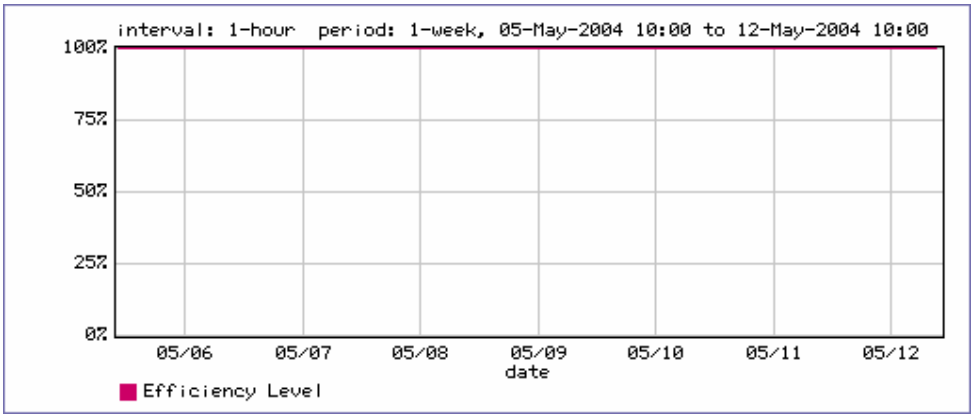


Figura. 4.49. Efecto de UDP 17262 sobre la eficiencia de red de "Outbound" con políticas.

En la Figura 4.50. se observa los bytes transmitidos por este flujo UDP, cuando se bajó la política de partición a 1 Kbps este flujo prácticamente dejó de transmitir datos.

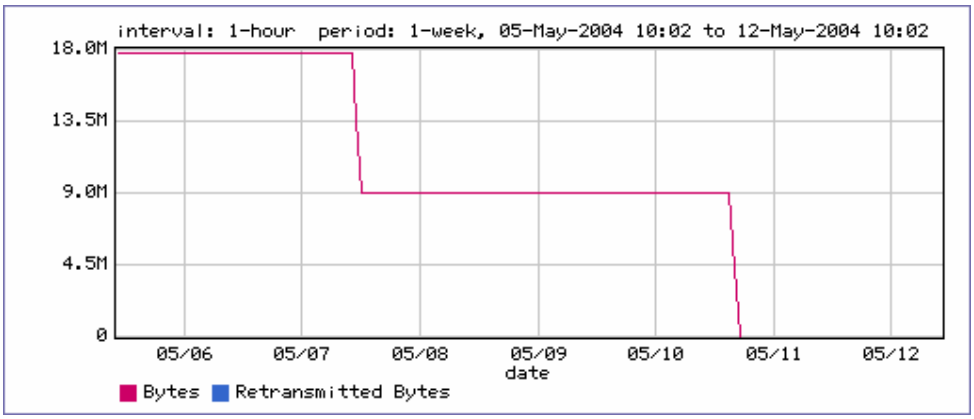


Figura. 4.50. Bytes transmitidos por UDP 17262 en el enlace de salida con políticas

Para este tráfico primero se creó una partición de 20 Kbps con el fin de limitar la transmisión de bytes y averiguar si esto afectaba al desempeño de alguna aplicación, dado que no se presentó ninguna anomalía, nuevamente se le restringió a esta aplicación pero ahora a solo 1 Kbps, ningún usuario mostró signos de molestias en su trabajo y ninguna aplicación resultó afectada al aplicar esta política de partición de 1 Kbps, debido a su comportamiento extraño y solo en el enlace de salida de la empresa se puede pensar que se trate de un ataque a la red ó un virus.

Con estas pruebas se ha probado las funciones del sistema administrador de ancho de banda PacketShaper para lograr acondicionamiento de tráfico e implementar calidad de servicio en un enlace de red de área amplia para Internet (WAN). Con esta visión práctica del sistema administrador y basado en comportamientos de protocolos y aplicaciones en el siguiente capítulo se nombrará los tipos de políticas que deberían aplicarse para cada clase o flujo monitoreado y clasificado por PacketShaper, con el fin de lograr implementar una apropiada calidad de servicio para un enlace red de área amplia y obtener su mejor rendimiento.

CAPITULO V

ESTABLECIMIENTO DE POLITICAS

5.1 GENERALIDADES

El objetivo de este capítulo es desarrollar un esquema de políticas de Calidad de Servicio (QoS) que PacketShaper puede implementar en un enlace de Red de Area Amplia (WAN) ó Internet y como utilizarlas, para esto se tomará como guía un análisis del comportamiento de protocolos y aplicaciones que PacketShaper monitoreo, clasificó y controló en las pruebas de acondicionamiento de tráfico del capítulo anterior.

5.2 ANALISIS DE LAS PRUEBAS DE PACKETSHAPER

5.2.1 Análisis del enlace de entrada (Inbound).

Del "Top Ten" que se observa en la Figura 4.4. y del árbol de clases que se observa en la Tabla 4.1. se deduce que las aplicaciones que más consumen el ancho de banda del enlace Inbound son HTTP, KaZaA, WinMedia, WinampStream, eDonkey, Real.

Como se explicó existía un consumo de 59% de ancho de banda del enlace de entrada por aplicaciones no importantes para la empresa por lo que se realizó un estudio más detallado de cómo estas aplicaciones influyen sobre el enlace de entrada, estas aplicaciones son a las que principalmente se debería aplicar las políticas.

Comparando los gráficos de utilización de estas clases que se observan en las Figuras 4.5., 4.7., 4.9., 4.11., 4.13 con el gráfico de utilización del enlace de entrada que se observa en la Figura 4.2. se deduce que el consumo del ancho de banda es tomado en su mayoría por estas aplicaciones. Comparando los gráficos de eficiencia de red de estas clases que se

observan en las Figuras 4.6., 4.8., 4.10., 4.12., 4.14. con el gráfico de eficiencia de red del enlace de entrada que se observa en la Figura 4.3. se deduce que la eficiencia de red del enlace de entrada se ve afectada en su mayoría por estas aplicaciones.

En la Figura 5.1. se observa un reporte de las clases que más consumen en promedio el ancho de banda, nombradas anteriormente.

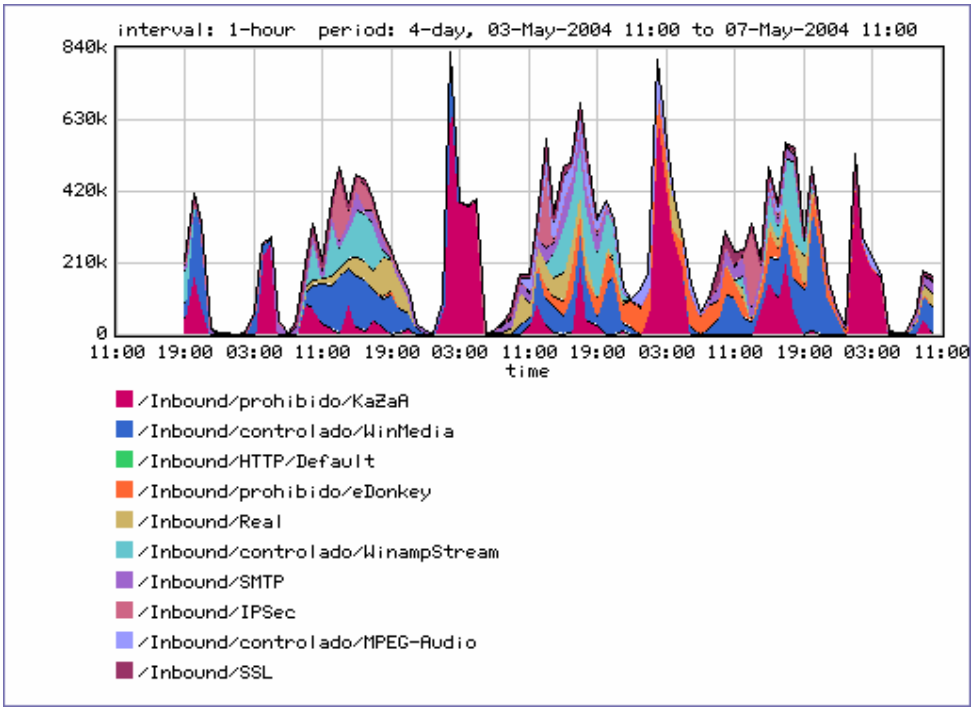


Figura. 5.1. Reporte de clases que más consumen el ancho de banda "Inbound".

El resto de aplicaciones y protocolos afectan al enlace pero no en la magnitud en la que lo hacen los que fueron nombrados anteriormente, en la Figura 5.2 se observa el consumo de otras aplicaciones descubiertas por PacketShaper en el enlace de entrada.

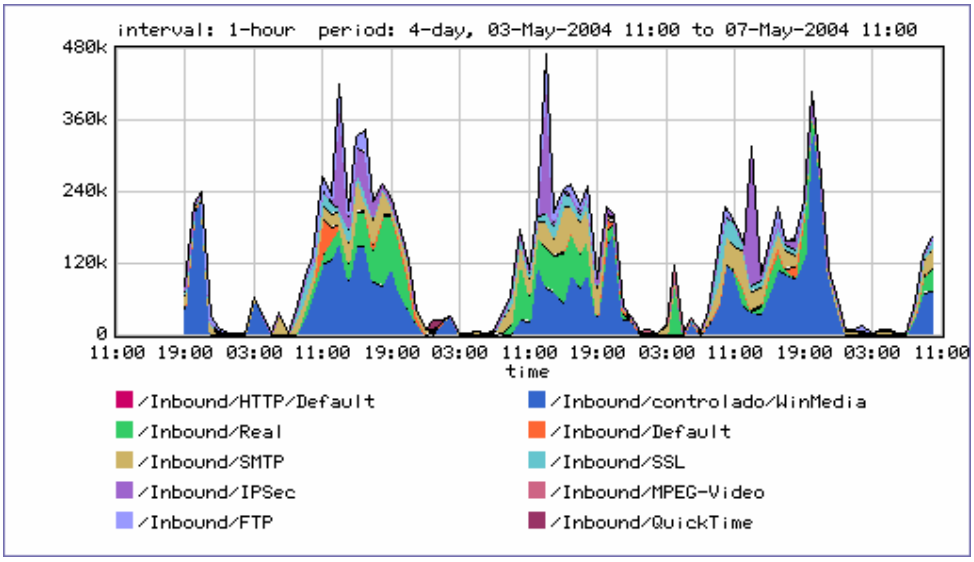


Figura. 5.2. Reporte de consumo promedio de otras clases del enlace de entrada.

5.2.2 Análisis del enlace de salida (Outbound).

Del Top Ten que se observa en la Figura 119. y del árbol de clases que se observa en la Tabla 11. se deduce que las aplicaciones que más consumen el ancho de banda del enlace de salida son UDP Port 17262, eDonkey, SMTP, KaZaA HTTP, IPSec, cabe mencionar que el consumo de ancho de banda promedio del enlace de salida es menor que el consumo de ancho de banda del enlace de entrada.

Como se explicó existía un consumo de 65% de ancho de banda del enlace de salida por aplicaciones no importantes para la empresa y una aplicación desconocida, por lo que se realizó un estudio más detallado de cómo estas aplicaciones influyen sobre el enlace de salida, estas aplicaciones son a las que principalmente se debería aplicar las políticas.

Comparando los gráficos de utilización de estas clases que se observan en las Figuras 4.18., 4.20., 4.22., con el gráfico de utilización del enlace de salida que se observa en la Figura 4.15., se deduce que el consumo del ancho de banda es tomado en su mayoría por estas aplicaciones. Tanto la eficiencia de red de estas clases que se observan en las Figuras 4.19., 4.21., 4.22., como la eficiencia de red del enlace de salida que se observa en la Figura 4.16. no presentan problemas.

En la Figura 5.3. se observa un reporte de las clases que más consumen en promedio el ancho de banda, nombradas anteriormente.

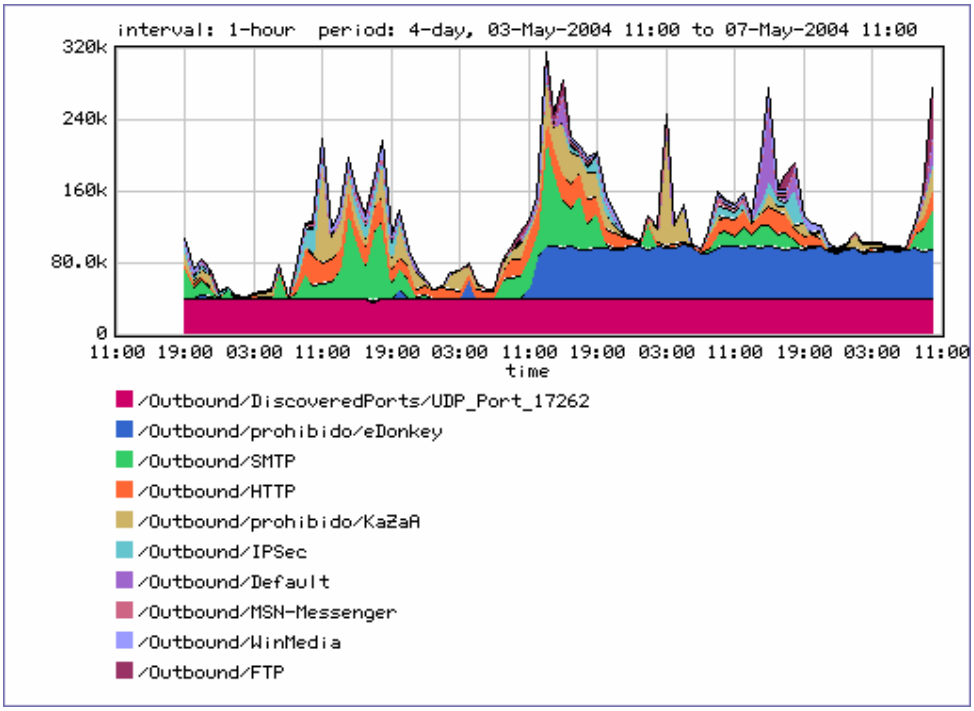


Figura. 5.3. Reporte de clases que más consumen el ancho de banda "Outbound".

En la Figura 5.4. se observa el consumo de otras aplicaciones descubiertas por PacketShaper en el enlace de salida.

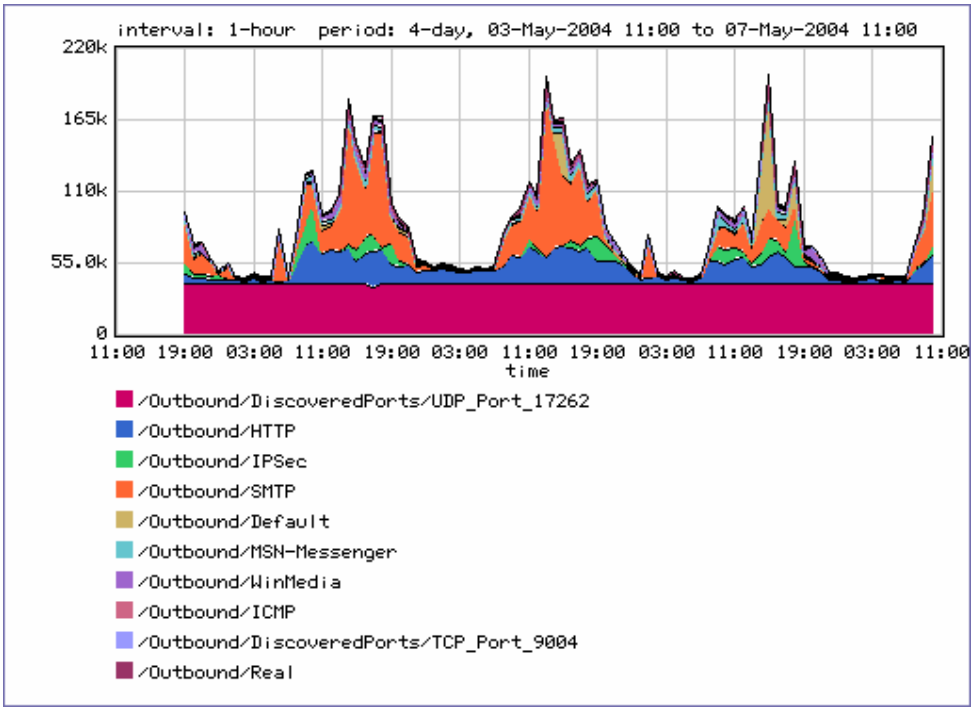


Figura. 5.4. Reporte de consumo promedio de otras clases del enlace de salida.

5.2.3 Análisis de comportamiento de los flujos de tráfico.

A continuación se realizará un análisis del comportamiento de los flujos de tráfico que más consumen el ancho de banda y afectan a la red tanto en el enlace de entrada como en el enlace de salida.

5.2.3.1 Análisis del Protocolo de Transferencia de HiperTexto (HTTP).

Este protocolo es utilizado para tráfico de páginas web e implementado principalmente en navegadores de Internet, es muy útil para los usuarios de la red, el tráfico de entrada es generalmente desde servidores web externos y el tráfico de salida es desde servidores en la red local, es un tipo de tráfico que crece incrementa rápidamente su velocidad (bursty) debido a que transfiere gran cantidad de información especialmente gráficos. En las pruebas realizadas con PacketShaper este protocolo mantiene un consumo promedio mediano, sin embargo el tráfico pico satura al enlace como se ve en la Figura 4.5., generalmente es algo sensible a retardos y pérdidas de paquetes.

5.2.3.2 Análisis de la aplicación KaZaA.

Es un programa muy popular par a par (P2P) usado para compartir archivos, genera un tipo de tráfico que incrementa rápidamente su velocidad (bursty) utilizando buena parte del ancho de banda especialmente del enlace de entrada como se observa en las Figuras 4.7. y 4.18 de las pruebas realizadas con PacketShaper. Esta aplicación no es importante para una organización e interfiere con aplicaciones de mayor importancia, no es sensible a retardos y pérdidas de paquetes, el programa Morpheus P2P puede ser clasificado como KaZaA debido a que sus funciones son las mismas.

5.2.3.3 Análisis de la aplicación eDonkey.

Grupo de servicios para compartir archivos, es un tipo de tráfico que incrementa rápidamente su velocidad (bursty) como se muestra en la Figura 4.7. de las pruebas realizadas con PacketShaper, el consumo es menor al de KaZaA en el enlace de entrada y mayor a KaZaA en el enlace de salida. Puede ser que este programa sea utilizado por una menor cantidad de usuarios. Esta aplicación no es importante para una organización e interfiere con aplicaciones de mayor importancia, no es sensible a retardos y pérdidas de paquetes.

5.2.3.4 Análisis de la aplicación WinMedia.

Grupo de servicios de Microsoft Windows Media usado para aplicaciones de audio y video del sistema operativo Windows mediante Internet, es un tipo de tráfico llamado “streaming media” cuyo contenido generalmente suele llegar al usuario de una manera lenta y con cortes, su consumo de ancho de banda es mediano como se observa en la Figura 4.9., es mayor el tráfico de entrada que el de salida. Para algunas organizaciones este tráfico puede ser importante por ser parte del sistema operativo Windows, es algo sensitivo a retardos y pérdidas de paquetes.

5.2.3.5 Análisis de la aplicación WinampStream.

Servicio que genera tráfico "streaming media" incluido con el popular programa de audio Winamp, su consumo de ancho de banda es promedio como se muestra en la Figura 4.11., es mayor el tráfico de entrada que el de salida. Generalmente este tráfico no es importante para una organización, es algo sensitivo a retardos y pérdidas de paquetes.

5.2.3.6 Análisis de Puerto UDP 17262.

Se sabe que esta aplicación usa como medio de transporte el protocolo UDP con puerto 17262, no existe asignación alguna de este puerto por la Autoridad de Números Asignados a Internet (IANA), este número de puerto es asignado por una aplicación de usuario. Por el análisis hecho con PacketShaper se sabe que existe comunicación entre el servidor proxy de la red y máquinas con varias direcciones IP que por estar en el Internet no se las puede identificar. En el Internet se encuentra pocas referencias a la asignación de este puerto, podría ser un flujo que intenta burlar la seguridad del enlace pero no se encontró una explicación precisa de su origen.

5.2.3.7 Otros protocolos descubiertos.

En la Tabla 5.1. se observa una explicación de los protocolos y aplicaciones que PacketShaper descubrió en las pruebas y que presentan un bajo consumo de ancho de banda, no representan un problema serio respecto a la eficiencia de la red por lo que no fue necesario aplicarles políticas de calidad de servicio.

Nombre	Descripción de la clasificación
File Transfer Protocol (FTP)	Grupo de servicios, comandos y datos del Protocolo de Transferencia de Archivos
Groupwise	Grupo de servicios Novell Groupwise, sistema de mensajes
Internet Relay Chat (IRC)	Grupo de servicios de Chat
Moving Pictures Experts Group (MPEG) Audio y Video	Flujos de audio y video del formato de codificación del Grupo de Expertos de Imágenes en Movimiento
MSN-Messenger	Mensajería instantánea de Hotmail
Napster	Aplicación par a par (P2P), comunidad de intercambio de música
Net2Phone	Aplicación para llamadas internacionales mediante Internet
Network Time Protocol (NTP)	Grupo de servicios del Protocolo del Tiempo de Red
POP3	Grupo de servicios de recepción de correo
QuickTime	Aplicación multimedia sobre el Protocolo de Transferencia de HiperTexto (HTTP), “streaming media”
Remote Desktop Protocol (RDP)	Protocolo de Escritorio Remoto, usado por la aplicación Microsoft Windows Terminal Server
Real	Grupo de servicios para aplicaciones de audio y video en tiempo real, “streaming media”
Real Time Control Protocol-Interactive (RTCP-I)	Protocolo de Control en Tiempo Real-Interactivo, usado para control de flujos de voz y video en tiempo real
Real-Time Transport Protocol-Interactive (RTP-I)	Protocolo de Transporte en Tiempo Real-Interactivo, usado para transporte de flujos de voz y video en tiempo real
SmartSockets	Tráfico de Tibco SmartSockets v6.0.2 y anteriores, es un programa que permite distribución e intercambio de información en tiempo real
Simple Mail Transport Protocol (SMTP)	Grupo de servicios del Protocolo de Transporte de Mail Simple, usado para el envío de correo
Simple Network Management Protocol (SNMP)	Grupo de servicios del Protocolo de Administración de Red Simple, usado por plataformas de administración
Secure Sockets Layer (SSL)	Protocolo que permite intercambio de flujos de tráfico web seguro
Telnet	Grupo de Servicios del Protocolo de Emulación de Terminal
WebEx	Plataforma de comunicación en tiempo real
Windows-POPUP	Aplicación que clasifica las ventanas de aviso que genera la aplicación de mensajería Windows Messenger
YahooGames	Juegos de Yahoo
YahooMsg	Mensajería instantánea Yahoo
AOL-AIM-ICQ	Mensajería instantanea de America On Line y programa de chat ICQ
Distributed	Modelo de Objeto de Componente Distribuido, aplicación de

Component Object Model (DCOM)	Microsoft
Domain Naming Server (DNS)	Servidor de Nombres de Dominio, asigna nombres comunes a direcciones IP
Gnutella	Grupo de servicios de red para compartir y distribuir archivos, aplicación par a par (P2P)
H.323	Grupo de servicios estándar de telefonía sobre IP
ISAKMP	Protocolos de intercambio de clave ISAKMP/IKE, funciona en conjunto con seguridad IP (IPSec)
PeerEnabler	Librerías par a par (P2P) v6.0.2 y anteriores de Altnet, trabaja con KaZaA v2.5
Real Time Streaming Protocol (RTSP)	Protocolo de Flujos en Tiempo Real
TimeServer	Servidor de tiempo, trabaja en el puerto 37
Internet Control Message Protocol (ICMP)	Protocolo de Mensajes de Control de Internet, usado por comandos de control de IP
IP Security (IPSec)	Grupo de servicios de seguridad IP
Dynamic Host Configuration Protocol (DHCP)	Grupo de servicios del protocolo de Configuración de Computadores Dinámica, asigna direcciones IP a computadores de forma dinámica
Syslog	Sistema de autenticación del sistema operativo multiusuario y multired creado por AT&T, UNIX
NetBIOS-IP	Grupo de servicios del protocolo de transporte NetBIOS sobre IP, generalmente dentro de una Red de Área Local (LAN) permite comunicarse a aplicaciones entre diferentes computadores

Tabla. 5.1. Aplicaciones y protocolos con bajo consumo del enlace.

5.2.4 Tipos de políticas de PacketShaper.

Se puede aplicar políticas y políticas de particiones, son similares con la diferencia que las políticas pueden aplicar control flujos individuales de protocolos ó aplicaciones y una política de partición se aplica a un conjunto de flujos tal que todos son controlados como uno solo.

5.2.4.1 Políticas de tasa.

Las políticas de tasa garantizan cantidades precisas de ancho de banda por flujo, utilizan el control de tasa de TCP para realizar la asignación de ancho de banda a tráfico TCP y planeamiento de límite de retardo para control de flujo de tráfico UDP y algunos no IP.

Asegura que cada sesión obtenga una porción justa del ancho de banda del enlace de Red de Área Amplia (WAN) ó Internet, previniendo de esta forma que los flujos crezcan hasta saturar el enlace, son buenas para contener a los flujos acaparadores de ancho de banda y proteger a las flujos críticos del enlace, son buenas para la mayoría de tipos de flujos TCP, son especialmente buenas para controlar aplicaciones que se caracterizan por flujos que incrementan rápidamente su velocidad (bursty), flujos continuos y grandes, son especialmente buenas para tráfico sensitivo al retardo el cual requiere un ancho de banda específico garantizado.

Recomendado principalmente para controlar el enlace de entrada, para aplicaciones y protocolos que requieren protección y/o contención de ancho de banda, por ejemplo con esta política de tasa se puede garantizar 10 Kbps para cada flujo de voz sobre IP.

5.2.4.2 Políticas de prioridad.

Las políticas de prioridad permiten priorizar aplicaciones específicas y tipos de tráfico dándoles un tratamiento con prioridad alta (preferencial) o de prioridad baja, el ancho de banda es asignado basado en prioridades de 0 a 7, siendo 7 la más alta prioridad.

Son buenas para tráfico que no incrementa rápidamente su velocidad (bursty), para tráfico que tiene flujos pequeños, para tráfico sensitivo al tiempo y para tráfico no IP, apropiadas cuando no es el objetivo principal asignar tasas por flujo, por ejemplo con esta políticas se puede asignar prioridad 7 para acceso a un computador.

5.2.4.3 Política de nunca admitir.

Una política de nunca admitir permite reforzar un control de admisión en el comienzo de un flujo, es recomendado para bloquear tráfico de páginas web TCP para notificar a usuarios que el sitio web no está disponible o redireccionarlos a un segundo sitio web, para tráfico TCP que no sea web simplemente bloquea una conexión, no es recomendado y no se puede usar para tráfico UDP ó tráfico no IP.

5.2.4.4 Política de Ignorar.

Una política de ignorar se usa para tipos de tráfico que pasan a través del sistema PacketShaper y no deben ser tomados en cuenta como parte del enlace de Red de Area Amplia (WAN) bajo administración, es decir tráfico que no sale a través del ruteador que está administrando PacketShaper, por ejemplo tráfico entre clientes y un servidor de una Red de Area Local (LAN).

5.2.4.5 Política de descarte.

Una política de descarte permite desechar todos los paquetes para una clase de tráfico, es recomendado para bloquear tráfico UDP y no IP, no es recomendado para tráfico TCP.

5.2.4.6 Políticas de particiones.

Las políticas de particiones son similares a las políticas de tasa excepto que se aplican a clases de tráfico enteras en vez de aplicar a cada flujo individualmente, en esencia reserva canales para llevar ciertos tipos de tráfico sin embargo pueden ser usadas por otras clases de tráfico si dichos canales están vacíos.

Se usa particiones cuando no se necesita administrar cada flujo individualmente pero se quiere asegurar que una clase de tráfico no interfiera a otro tráfico o no reciba interferencia de otro tráfico. Especialmente se usa para tipo de tráfico que crece rápidamente en el

enlace de entrada, por ejemplo con está política se puede reservar 20% del enlace para sesiones Telnet y protegerlo de otro tráfico más agresivo.

5.2.4.7 Políticas de particiones dinámicas.

Las políticas de particiones dinámicas permiten garantizar a cada usuario un mínimo y un máximo ancho de banda, son creadas en base a los usuarios activos en una clase, estas políticas permiten justeza a la hora de distribuir la cantidad de ancho de banda a cada usuario, aún cuando el ancho de banda aumente debido a ancho de banda disponible en exceso, por ejemplo se sabe que un 30% de estudiantes usan la red en un tiempo dado, la universidad configura particiones dinámicas que permitan asignar con justeza a cada estudiante un mínimo y un máximo de ancho de banda del enlace, eliminando la necesidad de que cada estudiante tenga una IP estática para controlarlo.

5.2.5 Análisis de aplicación de políticas.

Después que se obtuvo reportes de los enlaces de entrada, de salida y de las aplicaciones se hizo un análisis tomando en cuenta el análisis de tipo de tráfico, su importancia, su consumo de ancho de banda, como afecta a la eficiencia de la red y que políticas se debería aplicar.

5.2.5.1 Control del Protocolo de Transferencia de HiperTexto (HTTP).

Su consumo promedio es mediano tanto en el enlace de entrada como en el de salida, afecta medianamente a la eficiencia de la red, no se aplicó políticas de control principalmente por su importancia para la empresa y por que los usuarios no reportan problemas de congestión, por lo cual se decidió no interrumpir el desarrollo normal de esta aplicación.

5.2.5.2 Control de KaZaA y eDonkey.

Debido a su consumo de ancho de banda y como afectan a la eficiencia de la red durante el tiempo de análisis, se dedujo que el personal de la empresa utiliza regularmente estas aplicaciones, lo que en un futuro puede afectar al rendimiento de la red y del personal en su trabajo, se decidió bloquear estos tipos de tráfico tanto en el enlace de entrada como el de salida, para lo que se aplicó políticas de nunca admitir.

5.2.5.3 Control de MPEG-Audio, WinampStream y Winmedia.

Se agrupó los flujos "streaming media" que más consumen el ancho de banda y afectan a la red y se decidió aplicar una política de partición en el enlace de entrada limitando el consumo total de este tipo de tráfico creando una partición con un límite de ancho de banda de entrada de 100 Kbps, es decir aproximadamente el 10% del enlace.

5.2.6 Establecimiento de una estrategia para el acondicionamiento de tráfico.

- Obtener un reporte sobre el árbol de clases conteniendo los flujos de las aplicaciones y protocolos.

- Determinar que aplicaciones están interviniendo en el desarrollo de otras aplicaciones basándose básicamente en reportes como utilización promedio, la utilización pico del enlace y la eficiencia de la red. Con el reporte "Top Ten" se puede identificar que aplicaciones están consumiendo el mayor ancho de banda promedio. Generalmente las políticas se deberían aplicar a flujos que tengan el mayor consumo de ancho de banda promedio y que tengan un consumo pico mayor al 50% del enlace.

- Generar un listado clasificando el tráfico de las aplicaciones y protocolos según su importancia en la organización, tráfico interactivo sensible a retardos o que necesitan baja latencia, tráfico no sensible a latencia, tráfico que requiere de flujos

grandes que consuman en demasía el ancho de banda, tráfico que necesita ser uniforme o que es sensible a jitter, por ejemplo para la prueba de acondicionamiento de tráfico que se realizó el listado completo sería como se describe a continuación:

- *Trafico importante para la empresa.*- HTTP, NTP, POP3, RDP, RTCP-I, RTP-I, SmartSockets, SMTP, SNMP, SSL, Telnet, Webex, DNS, H.323, ISAKMP, TimeServer, ICMP, IPSec, DHCP, Syslog, NetBIOS-IP.

- *Tráfico medianamente importante para la empresa.*- Aplicaciones que generan tráfico "streaming media".

- *Tráfico no importante para la empresa.*- Especialmente aplicaciones par a par (P2P) y juegos en línea.

- *Tráfico interactivo sensible a retardos o que necesitan baja latencia.*- HTTP, NTP, RDP, SmartSockets, SNMP, SSL, Telnet, Webex, DNS, ISAKMP, TimeServer, ICMP, IPSec, DHCP, Syslog, NETBIOS-IP.

- *Tráfico que no es sensible a latencia.*- FTP, GroupWise, IRC, MSN-Messenger, SMTP, POP3, Windows-POPUP, YahooGames, YahooMsg, AOL-AIM-ICQ, DCOM, aplicaciones par a par.

- *Tráfico que requiere flujos grandes.*- Aplicaciones par a par, HTTP, FTP, POP3 y SMTP ó e-mails con grandes archivos adjuntos.

- *Tráfico que necesita bajo jitter.*- MPEG-Audio, MPEG-Video, Net2Phone, QuickTime, Real, RTCP-I, RTP-I, WinampStream, WinMedia, H.323, RTSP.

- Definir particiones y/o políticas para proteger y/o contener a los flujos de las aplicaciones y protocolos según la clasificación de tráfico, por ejemplo para la empresa se escogió las políticas como se observa en la Tabla 4.2.

  Las políticas deben aplicarse tomando en cuenta el listado de clasificación de los flujos de tráfico de la organización según los parámetros de calidad de servicio, sin embargo se va a establecer un esquema general que sirva como punto de partida al momento de aplicar políticas, como se observa en la Tabla 5.2.

Características de tráfico	Ejemplos de tráfico	Sugerencias de control
Tráfico no TCP	Protocolo de red Novell IPX, Protocolo de IBM SNA, Protocolo de Apple AppleTalk	Política de prioridad según su importancia
Flujos importantes, urgentes y pequeños	Telnet, DNS, SNMP	Política de prioridad alta
Flujos no urgentes, grandes, pero importantes	FTP, POP3, SMTP, HTTP	Política de tasa garantizando 0 Kbps, con incremento explosivo de velocidad (burstable) en prioridad media
Flujos grandes y no importantes	YahooGames, MSN-Zone	Partición que asigne a todos estos flujos menos del 5% del enlace ó Política de nunca admitir ó Política de tasa garantizando 0 Kbps, "burstable" con prioridad muy baja.
Flujos urgentes y grandes	Base de datos Oracle	Política de tasa garantizando 0 Kbps, "burstable" con alta prioridad.
Flujos "streaming media" en tiempo real	WindowsMedia, QuickTime, WinampStream	Partición que asigne a todos estos flujos un ancho de banda específico "burstable" con prioridad media-alta ó Política de tasa que garantice un ancho de banda específico por sesión "burstable" con prioridad media-alta, si son importantes estos flujos se debe garantizar un ancho de banda que garantice un buen desempeño de estos flujos.
Flujos no importantes, que no se desea prohibir pero si controlar adecuadamente	Descargas de música, URLs de contenido cuestionable	Política de tasa garantizando 0 Kbps "burstable" con prioridad 0 ó Partición que asigne a todos estos flujos un ancho de banda reducido.
Flujos no importantes, que se desea prohibir	Aplicaciones par a par, URLs prohibidas	Política de descarte para flujos UDP y no IP. Política de nunca admitir, con o sin redirección para tráfico web.

		Política de nunca admitir que bloquea tráfico TCP no web.
Aplicaciones en tiempo real que usan flujos grandes e importantes, como voz sobre IP que usa flujos UDP	Flujos pequeños H.323 y Q.931	Política de prioridad media-alta, por ejemplo 5
	Flujos RTCP, pequeños e intermitentes	
	Flujo RTP y otros protocolos de voz sobre IP, grandes y concurrentes	Política de tasa que garantice un ancho de banda "burstable" con prioridad 7, debe garantizarse suficiente ancho de banda para una comunicación sin cortes, los fabricantes indican una tasa aproximada de 21 Kbps por canal de voz dependiendo del codificador que utilice.
Impresión	NetBIOS-IP	Política de tasa garantizando 0 Kbps "burstable" con prioridad baja, por ejemplo 2.
Flujos no necesitan ser administrados por PacketShaper	Tráfico hacia y desde un servidor Intranet	Política de ignorar

Tabla. 5.2. Esquema general de políticas.

Las políticas no siempre se apegarán al esquema general, variarán dependiendo del criterio de una organización al momento de aplicar el control en su enlace de Red de Area Amplia (WAN) o Internet.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Calidad de servicio es la capacidad implementada en una red para asegurar un correcto flujo de su tráfico y para asegurar que los requisitos de todos sus usuarios puedan ser satisfechos.

- TCP/IP es un protocolo de red muy utilizado en la actualidad, sin embargo este protocolo por si solo no implementa el modelo de calidad de servicio conocido como servicios diferenciados.

- La meta de servicios diferenciados es proveer calidad de servicio a varios tipos de aplicaciones y requerimientos específicos de negocios en un dominio ó en un enlace de red de área amplia.

- Existen sistemas como ruteadores, switches y sistemas administradores de ancho de banda que implementan servicios diferenciados para el protocolo TCP/IP, UDP y protocolos no TCP/IP.

- El desarrollo de calidad de servicio se ha hecho en base a elementos de red como ruteadores y switches, que implementan técnicas ó algoritmos como técnicas de clasificación, control y prevención de congestión de tráfico.

- Los sistemas administradores de ancho de banda utilizan técnicas de los elementos de red, además de haber desarrollado nuevas técnicas para implementar servicios diferenciados.

- Los sistemas administradores de ancho de banda, son cajas dedicadas a calidad de servicio del enlace de red de área amplia, generalmente se colocan entre el ruteador y el switch ó hub de una red para implementar calidad de servicio en el enlace de red de área amplia.

- Se necesita un solo administrador de ancho de banda en un extremo del enlace de red de área amplia para administrarlo e implementar servicios diferenciados, aunque se puede tener uno por cada extremo del enlace de red de área amplia mejorando la granularidad en la clasificación, control del tráfico, mejor control de protocolos no TCP/IP y con algunos administradores de ancho de banda se puede implementar compresión de tráfico.

- Los sistemas administradores de ancho de banda se encuentran en varias marcas, las cuales presentan similares características para implementar servicios diferenciados, cada marca provee varios modelos de sistemas administradores dependiendo básicamente de la capacidad del enlace de red de área amplia que pueda administrar.

- Los aspectos en que se basan los sistemas administradores de ancho de banda para implementar calidad de servicio son monitoreo, clasificación, reporte y control del tráfico. Así los sistemas administradores de ancho de banda monitorean, clasifican, controlan y emiten reportes de una gran cantidad de flujos de tráfico de forma automática en capa 4 y capa 7 del modelo OSI, mejorando la calidad de servicio que implementan elementos de red.

- Los sistemas administradores de ancho de banda son flexibles permitiendo al usuario administrar flujos de tráfico basado en parámetros como direcciones, puertos, protocolos, subredes, ambientes de servicios diferenciados con ruteadores, ambientes de conmutación de etiquetas, redes virtuales.

- Los sistemas administradores de ancho de banda realizan el control de los flujos de tráfico TCP y no TCP mediante políticas las mismas que pueden garantizar ancho de banda, dar prioridad a flujos de tráfico y bloquear flujos de tráfico.

- Los sistemas administradores de ancho de banda poseen otras tecnologías, pueden formar topologías redundantes, permiten autenticación en servidores, poseen tecnologías de derivación que pasan el tráfico cuando están apagados ó fallan, pueden ser administrados por plataformas abiertas, aportan a la identificación de ataques y virus.

- Los sistemas administradores de ancho de banda son colocados en una red para implementar calidad de servicio, evitando delegar esta obligación a los ruteadores, de esta manera también se evita posibles actualizaciones de hardware y firmware de los ruteadores, así como su configuración de calidad de servicio la cual puede resultar complicada.

- PacketShaper posee la tecnología de control de tasa de TCP para realizar el control de los flujos de tráfico, en vez de utilizar mecanismos de encolamiento como el resto de sistemas.

- Las pruebas de monitoreo, clasificación, reporte y control realizadas con el sistema PacketShaper permitieron observar el proceso de administración de parámetros de calidad de servicio como utilización de ancho de banda, retardos y retransmisiones en términos de eficiencia de red de los flujos de tráfico.

- La configuración de calidad de servicio de PacketShaper es mediante interfaz gráfica, sin embargo algunas configuraciones especiales requieren del uso de línea de comandos mediante sesiones de emulación de terminal.

- Luego de la configuración de políticas se notó la mejoría de la eficiencia de la red, debido a que las políticas aplicadas controlaron el tráfico no importante para la

empresa, demostrando de esta forma la implementación de calidad de servicio en el enlace de red de área amplia de acuerdo a las necesidades de la empresa.

- Las pruebas realizadas con el sistema PacketShaper permitieron establecer una estrategia para implementar calidad de servicio y un esquema general de políticas de calidad de servicio basado en el comportamiento y requerimientos de las aplicaciones y protocolos.

- Las pruebas realizadas con el sistema PacketShaper mostraron que en la red existen buena cantidad de protocolos y aplicaciones en tiempo real.

- Las pruebas realizadas con el sistema PacketShaper mostraron una utilización alta del ancho de banda del enlace de red de área amplia por aplicaciones no importantes para la mayoría de organizaciones.

- Las pruebas realizadas con el sistema PacketShaper mostraron buena cantidad de protocolos y aplicaciones que no necesitaron ser controladas debido a que no interferían en el desarrollo normal del enlace de red de área amplia de la organización.

- La nueva versión del protocolo de Internet, llamada IPV6 además de permitir un direccionamiento utilizando 128 bits, implementa características de calidad de servicio, tal que los usuarios pueden pedir trato diferenciado y el equipamiento puede administrar diferentes tipos de tráfico. Actualmente aún no se implementa redes IPV6, se continúa trabajando con IPV4, por lo tanto es válida la utilización de los sistemas administradores de ancho de banda hasta que IPV6 sea adoptado de forma definitiva. Cabe mencionar que el firmware de un sistema administrador de ancho de banda puede ser actualizado y en el futuro lo más probable es que los sistemas administradores de ancho de banda soporten IPV6 e interactúen con el resto de equipamiento para implementar servicios diferenciados.

5.2 RECOMENDACIONES

- Al momento de adquirir un sistema administrador de ancho de banda se recomienda establecer la capacidad del enlace de red área amplia que va a controlar y el número de políticas de usuario adicionales que se tiene previsto implementar.

- Se recomienda hacer un análisis previo de la red donde se va a colocar el administrador de ancho de banda para un funcionamiento correcto del sistema y determinar posibles accesorios adicionales a instalarse en el sistema.

- Una vez colocado el sistema administrador de ancho de banda en la red, se recomienda conocer sus opciones de configuración con el fin de obtener el mayor beneficio de las características del sistema.

- Debido a que cada día aparecen nuevas aplicaciones y protocolos es recomendable pero no absolutamente necesario obtener mediante el proveedor las actualizaciones de firmware de los sistemas administradores de ancho de banda, de esta manera se posee las herramientas necesarias para controlar cualquier tipo de flujo de tráfico.

- Es recomendable colocar al sistema en la red y dejarlo que descubra las aplicaciones y protocolos de forma automática, posteriormente cuando el sistema haya creado la lista de protocolos y aplicaciones agregar la clasificación personalizada de usuario.

- Antes de aplicar políticas de calidad de servicio se recomienda analizar el comportamiento y requerimientos de las aplicaciones y protocolos existentes en la red, especialmente las que consumen un mayor ancho de banda.

- Para los protocolos y aplicaciones en tiempo real se recomienda una mayor prioridad al acceso del ancho de banda y un ancho de banda garantizado.

- Para aplicaciones no importantes se recomienda una baja prioridad al acceso del ancho de banda y no garantizar ancho de banda.

- Si se requiere un control muy preciso y compresión de datos, se recomienda utilizar un sistema administrador de ancho de banda en cada extremo del enlace de red de área amplia.

- En el sistema PacketShaper si se debe controlar gran cantidad de computadores se recomienda crear una política de partición dinámica con el fin de no asignar una política por cada computador y así no agotar el máximo de número de políticas que se puede configurar en el sistema.

BIBLIOGRAFIA

MILLER, Mark, **Lan Troubleshooting Handbook,** II, M&T Books, año 1993, Pags. 5-11.

NAUGLE, Matthew, **Network Protocol Handbook,** McGraw-Hill, año 1994, Pags. 6-8, 241-337.

FREEDMAN, Alan, **Diccionario de Computación**, V, McGraw-Hill, año 1993, Pags. 319, 334, 339, 380, 572-573, 717.

SIMONDS, Fred, **Lan Communications Handbook**, McGraw-Hill, año 1994, Pags. 253-258.

http://www.packeteer.com, Información de PacketShaper y calidad de servicio.

http://www.allot.com, Información de NetEnforcer y calidad de servicio.

http://www.expand.com, Información de Accelerator y calidad de servicio.

http://www.cisco.com, Información de Cisco y calidad de servicio.

http://www.mrv.com, Información de MRV y calidad de servicio.

http://www.autocont.cz, Información de 3COM.

http://www.dlink.com, Información de Dlink.

http://www.avaya.com, Información de Avaya y calidad de servicio.

http://www.idc.com, Clasificación de sistemas administradores.

http://www.faqs.org/rfcs, Especificaciones RFCs.

http://www.javvin.com, VLAN e IEEE802.1Q.

http://www.eveliux.com, Estándares de telecomunicaciones.

http://www.intel.com/network/connectivity/resources/doc_library/white_papers/solutions/diff_serv/diffserv.htm, Servicios Diferenciados.

http://www.telsyte.com.au/standardswatch/802.1p.htm, IEEE802.1Q.

http://www.cabledatacomnews.com/whitepapers/paper08.html, Calidad de servicio.

http://www.idg.es/comunicaciones, Encolamiento.

www.cs.unc.edu/~jasleen/papers, Encolamiento.

http://www.iis.ee.ic.ac.uk/~frank/surp00/article2/sl98, Calidad de servicio.

http://citeseer.ist.psu.edu, TCP/IP, calidad de servicio, encolamiento, control de tasa de TCP.

http://www.bmas.ja.net/papers/review/BMAS_Bandwidth_Management_Review.htm, Administración de ancho de banda.

http://msdn.microsoft.com/library/en-us/ias/ias/radius_authentication_and_accounting.asp?frame=true, RADIUS.

http://www.monografias.com/trabajos11/repri/repri.shtml, VPN.

http://www.uv.es/~montanan/redes/trabajos, MPLS.

http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2862374,00.html, IPV6.

ANEXO A

RED DE AREA LOCAL VIRTUAL E IEEE 802.1Q

LAN Virtual (VLAN) es un grupo de elementos en una o más LANs que son configurados tal que ellas pueden comunicarse tal como si estuvieran conectados al mismo cable, cuando en realidad están localizados en un número de segmentos de LAN diferentes. Debido a que las VLANs son basadas en conexiones lógicas y no físicas, es muy flexible para administración de usuarios, asignación de ancho de banda y optimización de recursos.

Existen los siguientes tipos de redes virtuales:

- VLAN basada en puerto, cada puerto físico del switch es configurado con una lista de acceso especificando el número de miembros en un conjunto de VLANs.

- VLAN basada en MAC, un switch es configurado con una lista de acceso mapeando direcciones MAC individuales al número de miembros de la VLAN.

- VLAN basada en protocolo, un switch es configurado con una lista de mapeo de tipos de protocolo capa 3 al número de miembros de la VLAN, por consiguiente filtrando tráfico IP desde estaciones finales usando un protocolo particular tal como IPX.

- VLAN ATM, usando el protocolo de Emulación de LAN (LANE) para mapear paquetes ethernet dentro de celdas ATM y enviarlas a su destino por la conversión de una dirección MAC en una dirección ATM.

La especificación IEEE 802.1Q establece un método estándar para etiquetar paquetes ethernet con información del número de miembros de la VLAN. El estándar IEEE 802.1Q define la operación de puentes (bridges) VLAN que permiten la definición, operación y

administración de topologías de LANs virtuales dentro de una infraestructura de LAN puenteada.

El estándar IEEE 802.1Q es proyectado para direccionar el problema de cómo seccionar redes grandes en redes más pequeñas tal que el tráfico broadcast y multicast no utilice más ancho de banda que el necesario. El estándar también ayuda a proveer un alto nivel de seguridad entre segmentos de redes internas.

ESTRUCTURA DE RED DE AREA LOCAL VIRTUAL E IEEE 802.1Q

La estructura de un paquete etiquetado para ethernet es el siguiente:

- Preámbulo (PRE): 7 bytes, es un patrón de unos y ceros que informan a las estaciones que reciben que un paquete esta llegando, provee un medio para sincronizar las porciones de recepción de paquetes de capas físicas con la muestra de bits entrante.

- Delimitador de Inicio de Paquete (SFD): 1 byte, es un patrón de unos y ceros , finaliza con dos unos consecutivos indicando que el siguiente bit es el más significativo en el byte más significativo de la dirección de destino.

- Dirección de Destino (DA): Identifica que estación debe recibir el paquete.

- TPID: Valor definido en 8100 hexadecimal, significa que es un paquete ethernet etiquetado.

- Información de Control de Etiqueta (TCI): 2 bytes, incluye información de prioridad, en su forma canónica indica el identificador de VLAN.

    - Prioridad de usuario: 3 bits, define 8 niveles de prioridad.

- Indicador de Forma Canónica: 1 bit, usado por razón de compatibilidad entre una red ethernet y una token ring.

- Identificador de VLAN (VID): 12 bits, es la identificación de la VLAN, es básicamente usado por el estándar 802.1Q. Permite la identificación de 4096 VLANs, VID = 0 es usado para identificar paquetes de prioridad y VID = 4095 es reservado, el máximo número de identificadores de VLANs configurables es 4094.

- Tipo/Longitud: 2 bytes, indica el número de bytes de datos de cliente MAC que están contenidos en el campo de datos del paquete o indica el identificador de tipo de paquete si el paquete fue ensamblado usando un formato opcional.

- Datos: Es una secuencia de n bytes ($42 \leq n \leq 1496$) de algún valor. El mínimo de un paquete total es 64 bytes.

- Secuencia de Chequeo de Paquete: Contiene un chequeo de redundancia cíclico para chequear paquetes incorrectos.

ANEXO B

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

EXCERPT

Packeteer the Clear Market Leader in WAN Optimization Management

Excerpted from: *Worldwide WAN Optimization Management 2004-2008 Forecast and Analysis* by Stephen Elliot, IDC #31237

IDC OPINION

The WAN optimization management market is a fast-moving market that is quickly gaining enterprise and service provider credibility throughout the world. Consisting primarily of hardware vendor solutions that use compression, quality-of-service (QoS) capabilities and, increasingly, monitoring, this market has a future that looks bright. The WAN optimization market will increase from $236 million in 2004 to $427 million in 2008 with a CAGR of 16.0%. IDC believes:

- WAN managers and IT architects are under pressure to cost-effectively manage bandwidth costs while improving application performance. Adding additional bandwidth to improve WAN application performance is the wrong approach as it does not provide cost efficiencies and utilization improvements.
- The WAN optimization market is evolving toward compression technology becoming a commodity feature play with low margins and heavy price competition. The market is maturing toward QoS capabilities, business policy integration, reduced TCP and application protocol chat, and application management.
- Packeteer has been and continues to be the major dominant vendor in this market. However, several emerging firms with innovative technologies are gaining traction. Hardware vendors, notably Cisco via its NetFlow-based application product, are an ever present threat to any vendor in this market.

Methodology

IDC defines the WAN optimization market as hardware or software products that compress data streams, monitor traffic flows, prioritize traffic via QoS policies, and/or manage applications from a protocol perspective. These tools analyze application traffic from an external WAN perspective that is generally delineated from the edge router out across the WAN to the user.

This study from which this excerpt was drawn forecasts and analyzes the WAN optimization management market for 2004–2008. The revenue in this forecast is derived from vendor software licenses, maintenance, and hardware. It does not include customization or integration services.

Filing Information: November 2004, IDC #, Volume: 1
Network and Service Management: Excerpt

SITUATION OVERVIEW

WAN optimization is seeing strong growth in the market from enterprise and service providers that are looking to reduce their bandwidth costs, improve quality of delivered services, and better manage remote offices. Vendors are seeing an uptake in products that help companies consolidate branch offices and improve the utilization of existing bandwidth pipes. Enterprise IT architectures are becoming more complex and often globally distributed, increasing the pain of WAN application performance degradation and business disruption. Some enterprises view bandwidth management as a logical solution to performance issues and fail to find that they are spending too much money on underutilized links. These IT organizations are looking more closely at WAN optimization vendors that provide sophisticated compression and traffic-shaping capabilities to improve utilization, reduce bandwidth costs, and increase application performance.

In a growing number of customers we have spoken with, IT organizations are using WAN optimization management tools to extend their security management to detect worms and DoS attacks based on irregular or suspicious traffic patterns. We recommend to some users that they implement certain WAN optimization technologies to address the growing issue of network integrity.

TABLE 1

Worldwide WAN Optimization Management Revenue by Vendor, 2003

	Revenue ($M)	Share (%)
Packeteer	72.7	37.0
Allot Communications	20.0	10.2
Cisco	15.0	7.6
Expand	14.1	7.2
Peribit Networks	13.0	6.6
Nortel	13.0	6.6
Other	48.9	24.8
Total	196.7	100.0

Note: "Other" includes Compuware, NetQoS , Network Physics, RouteScience, Adlex, Ipsum Networks, Packet Design, Proficient Networks, Rocksteady , Riverbed, Bluewave, Alcatel, Juniper, Corvil, ITWorx, Sitara Networks, Niksun, and ActivNetworks.

Source: IDC, 2004

FUTURE OUTLOOK

The WAN optimization market is moving toward a more mature, complete application management solution that includes compression, QoS, monitoring, and IT service management. Packeteer has set the standards in terms of install base and market penetration, but there remains a large opportunity of untapped enterprise branch offices that will require application management tools. Traditional user culture must change to stop adding bandwidth and start looking at more efficient ways to utilize existing bandwidth links. IDC believes the future of the WAN optimization market is strong and will evolve in a few key technical areas:

- Dynamic business policies that dictate quality of service per user group and applications that maximize dynamic visibility that improves bandwidth utilization and adjusts to changing business priorities
- The growing importance of "core correlation and pattern-matching technologies" that dictate the accuracy of data collection, analysis, and automated actions based on business policies (These include recognizing latency, throughput, jitter, BGP peering issues, UDP, TCP, and application protocols that use pattern recognition, fractal data models, SIGINT analysis, correlation engines, and predictive capabilities using Markov modeling, and deterministic algorithms.)
- Protocol analysis and collection with the ability to trigger automated action based on business policies and growing requirements to map specific application flows to user groups, business units, and packet layer with impact analysis
- Security reports and mechanisms that allow WAN and IT managers to better address security breaches and threats through flow pattern recognition and automated corrective actions to contain and minimize network exposure
- Scalability of models to adjust to the growing need to centralize management capabilities and increase potential data sharing models through XML , SDKs, and open APIs

TABLE 2

Worldwide WAN Optimization Management Revenue, 2003–2008

	2003	2004	2005	2006	2007	2008	2004–2008 CAGR (%)
Revenue ($M)	196.7	236.0	292.0	332.0	380.0	427.0	16.0
Growth (%)	NA	20.0	23.7	13.7	14.5	12.4	

Note: See Table 5 for key forecast assumptions.

Source: IDC, 2004

Copyright Notice

ANEXO C

RED PRIVADA VIRTUAL

1. INTRODUCCIÓN

Una RED se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones).

En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentas con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de los famosos firewalls y las VPN

2. OBJETIVO DE LA VPN

Cuando deseo enlazar mis oficinas centrales con alguna sucursal u oficina remota tengo tres opciones:

- Módem: Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia, a parte no contaría con la calidad y velocidad adecuadas.

- Línea Privada: Tendría que tender mi cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo necesito enlazar mi oficina central con una sucursal que se encuentra a 200 Kilómetros de distancia el costo sería por la renta mensual por Kilómetro. Sin importar el uso.

- VPN: Los costos son bajos porque solo realizo llamadas locales, además de tener la posibilidad de que mis datos viajen encriptados y seguros, con una buena calidad y velocidad.

3. DEFINICIÓN DE VPN

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública, observar Figura 1.

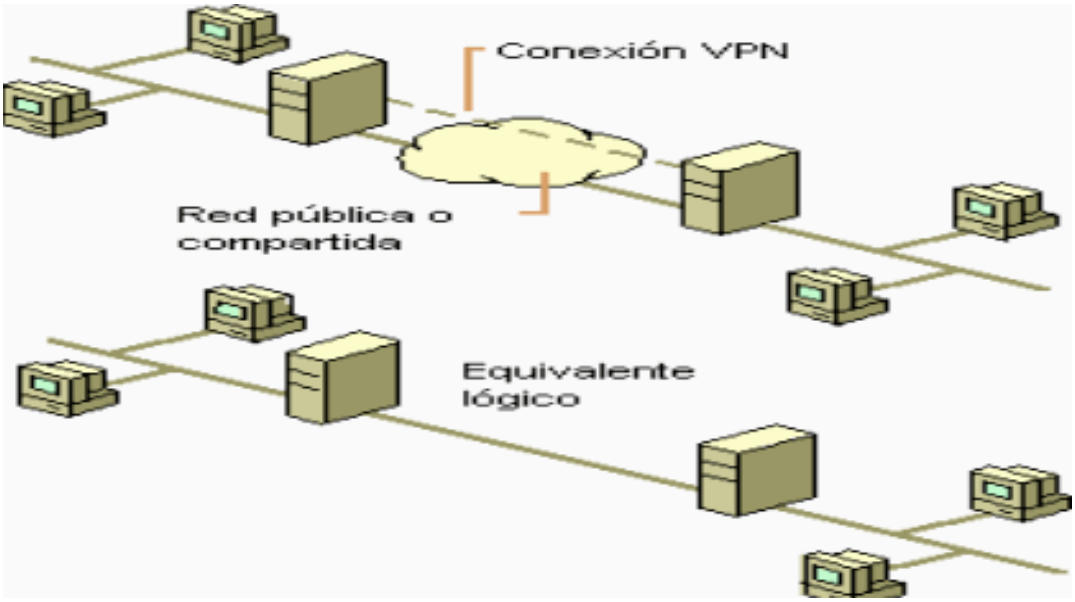


Figura 1.

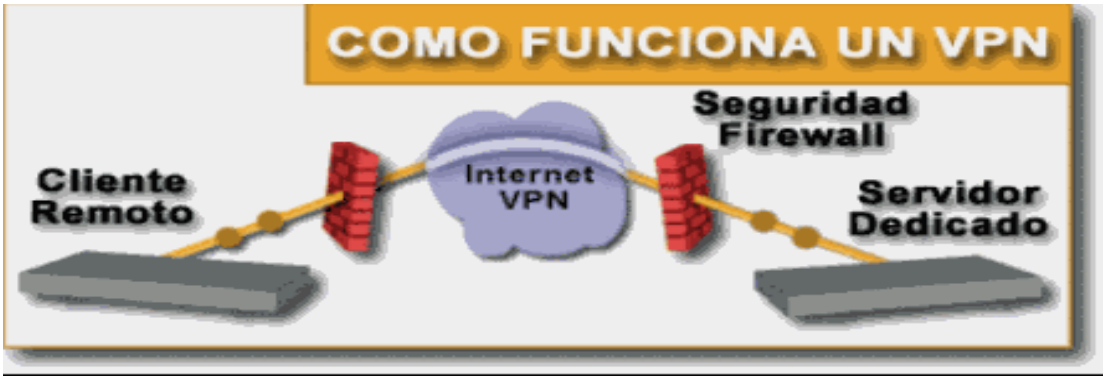


Figura 2.

En la Figura 2., se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a nube de Internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad garantizada, con un ancho de banda también garantizado y lleguen a su vez al firewall remoto y terminen en el servidor remoto.

Las VPN pueden enlazar mis oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como Internet, IP, Ipsec, Frame Relay, ATM como lo muestra la figura siguiente.

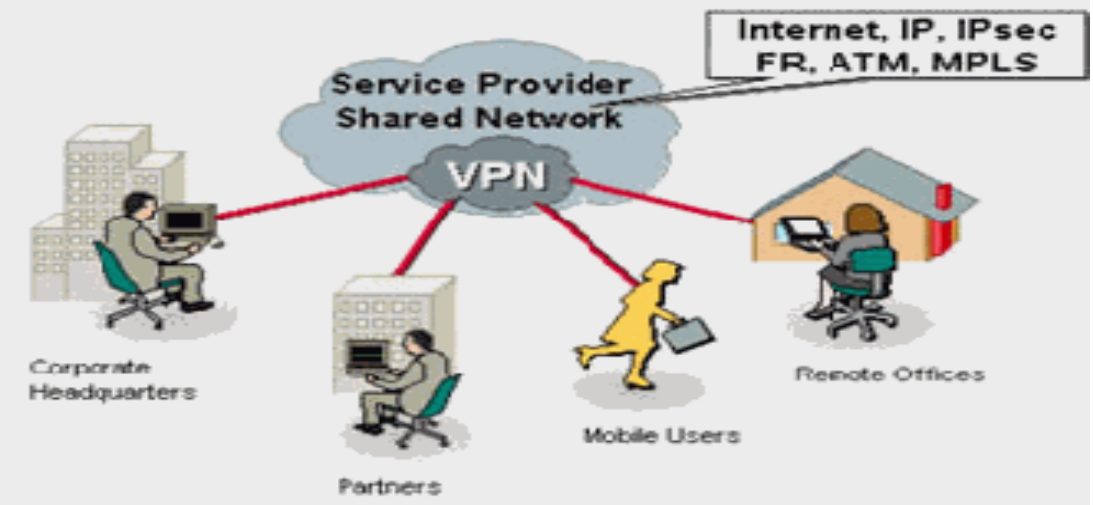


Figura 3.

4. TECNOLOGÍA DE TÚNEL

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

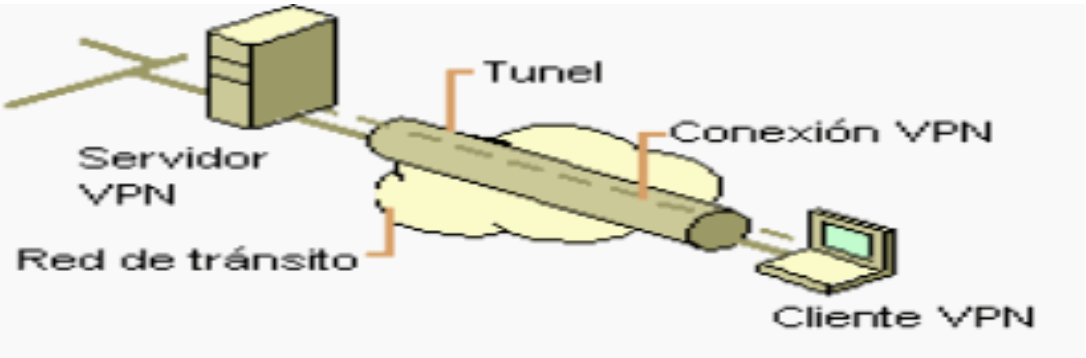


Figura 4.

El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de transito se envían los datos sin problemas.

5. REQUERIMIENTOS BÁSICOS DE UNA VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

- Identificación de usuario
- Administración de direcciones
- Codificación de datos
- Administración de claves
- Soporte a protocolos múltiples

5.1 Identificación de usuario.

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.

5.2 Administración de direcciones.

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

5.3 Codificación de datos.

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

5.4 Administración de claves.

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

Soporte a protocolos múltiples

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet (IPX) entre otros.

6. HERRAMIENTAS DE UNA VPN

- VPN Gateway
- Software
- Firewall
- Router

6.1 VPN Gateway.

Dispositivos con un software y hardware especial para proveer de capacidad a la VPN

6.2 Software.

Esta sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN.

7. VENTAJAS DE UNA VPN

Dentro de las ventajas más significativas podremos mencionar la integridad, confidencialidad y seguridad de los datos.

- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows.
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PCs remotas.

8. CONCLUSIÓN

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia

de datos de un lugar a otro, el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

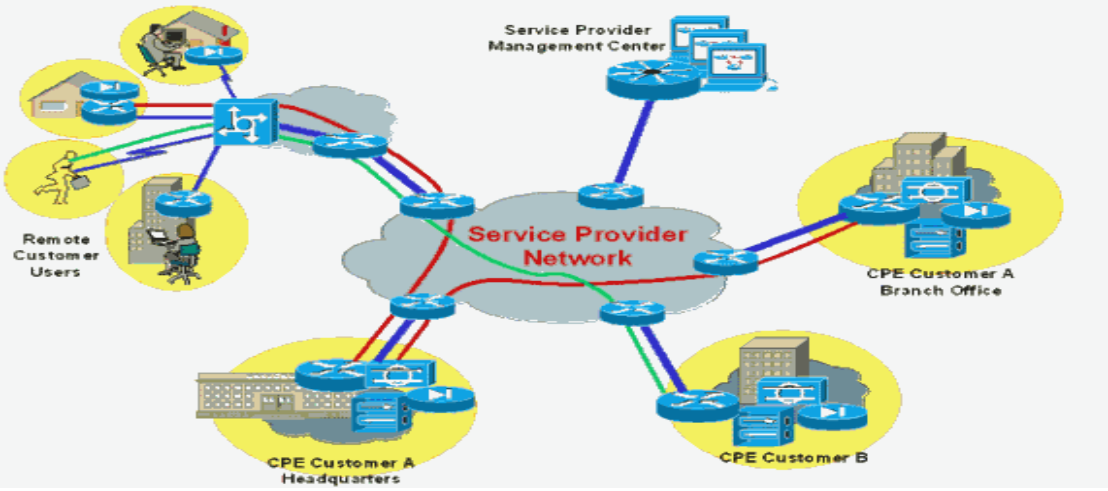


Figura 5.

ANEXO D

MULTIPROTOCOL LABEL SWITCHING

1. INTRODUCCIÓN

La red IP se ha convertido en una extensa red en la que las posibilidades de negocio y los mercados de consumo inducen al desarrollo de nuevas aplicaciones.

Son aplicaciones de voz y multimedia que requieren mayor ancho de banda y, que éste, esté garantizado durante todo el servicio. Estos requerimientos hacen que los recursos de la red estén sobre utilizados en términos de velocidad y ancho de banda. Además de estos requerimientos, se debe poder ofrecer clases diferenciadas de servicio a los distintos usuarios que utilizan la red.

Avanzamos hacia una convergencia entre voz y datos en la red IP y su infraestructura y protocolos han sido optimizados sólo para datos, así que IGPs (Interior Gateway Protocol) como RIP (Routing Information Protocol) y OSPF (Open Shortest Path First) y EGPs (Exterior Gateway Protocol) como BGP4 (Border Gateway Protocol v4), no son la solución óptima. Muchos de estos protocolos de *ruteo* están basados en algoritmos para obtener el camino más corto (como RIP y BGP4, basados en el vector distancia) sin tener en cuenta métricas adicionales como retardo, *jitter* y congestión del tráfico.

Todo esto se traduce en una sobrecarga en el *ruteador* IP, problemas de propagación de las rutas y la obligación de integrar redes IP con ATM.

MPLS ha sido desarrollado para eliminar varios de estos problemas. Tiene la capacidad de soportar cualquier tipo de tráfico en una red IP sin tener que supeditar el diseño de la red a las limitaciones de los diferentes protocolos de *ruteo*, capas de transporte y esquemas de direcciones.

2. QUÉ ES MPLS

MPLS (MultiProtocol Label Switching) es un grupo de trabajo específico del IETF (Internet Engineering Task Force) que trata sobre el encaminamiento, envío y conmutación de los flujos de tráfico a través de la red.

Las principales funciones de MPLS son:

Especificar mecanismos para gestionar flujos de tráfico de diferentes tipos (Ej.: flujos entre diferente *hardware*, diferentes máquinas,...).

- Quedar independiente de los protocolos de la capa de enlace y la capa de red.

- Disponer de medios para traducir las direcciones IP en etiquetas simples de longitud fija utilizadas en diferentes tecnologías de envío y conmutación de paquetes.

- Ofrecer interfaces para diferentes protocolos de *ruteo* y señalización.

- Soportar los protocolos de la capa de enlace de IP, ATM y Frame Relay.

En MPLS la transmisión ocurre en caminos de etiquetas conmutadas (LSP- Label Switched Path), que son secuencias de etiquetas en cada nodo del camino desde el emisor al receptor. Hay dos formas de requerir los LSPs:

- Antes de la transmisión de datos (control-driven).

- Una vez detectado un cierto flujo de datos (data-driven).

Las etiquetas se distribuyen utilizando un protocolo de señalización como LDP (Label Distribution Protocol) o RSVP (ReSource reserVation Protocol), o también, añadidas a protocolos de *ruteo* como BGP u OSPF.

Las etiquetas son insertadas al comienzo del paquete en la entrada de la red MPLS. En cada salto el paquete es encaminado según el valor de la etiqueta y sale por la interfaz correspondiente con otra etiqueta. Se obtiene una gran rapidez en la conmutación gracias a que las etiquetas son insertadas al principio del paquete y son de longitud fija, lo que hace que pueda hacerse una conmutación vía *hardware*.

3. DEFINICIONES

3.1 FEC (Forward Equivalence Class).

Conjunto de paquetes que comparten unas mismas características para su transporte, así todos recibirán el mismo tratamiento en su camino hacia el destino. La asignación de un paquete a un determinado FEC se produce una vez el paquete entra en la red. Cada FEC puede representar unos requerimientos de servicio para un conjunto de paquetes o para una dirección fija.

3.2 LSR (Label Switched Router).

Ruteador de gran velocidad en el núcleo de una red MPLS. Sus funciones son las siguientes:

- Participar en el establecimiento de los LSPs usando un protocolo de señalización apropiado.

- Conmutar rápidamente el tráfico de datos entre los caminos establecidos.

Para que los LSPs puedan usarse, las tablas de envío de cada LSR deben contener:

(interfaz de entrada, etiqueta asociada)→(interfaz de salida, etiqueta asociada')

A este proceso se le llama distribución de etiquetas. Como un LSP puede dar servicio a un *host* IP o a muchos, existe otra entrada en la tabla:

FEC→etiquetas asociadas

3.3 LER (Label Edge Router)

Ruteador en la frontera de la red al que se pueden conectar diversas redes (Frame Relay, ATM, Ethernet). Envía el tráfico entrante a la red MPLS utilizando un protocolo de señalización de etiquetas y distribuye el tráfico saliente entre las distintas redes.

Etiquetas.

Las etiquetas identifican el camino que un paquete puede atravesar. La etiqueta es encapsulada en la cabecera de la capa de enlace. Una vez el paquete ha sido etiquetado viajará a través del *backbone* mediante conmutación de etiquetas, es decir, cada *ruteador* examinará la etiqueta, consultará en sus tablas de envío para saber con qué etiqueta y por qué interfaz debe salir, intercambiará las etiquetas y lo enviará por el interfaz correspondiente.

Pasos para la asignación de etiquetas:

1. Cada paquete se clasifica como un nuevo FEC o se le asigna un FEC ya existente.

2. Se asigna una etiqueta a cada paquete. Éstas se derivan de la capa de enlace, es decir, para redes Frame Relay, ATM o redes ópticas, los identificadores de la capa 2 (DLCIs, VPIs/VCIs y longitud de onda DWDM, respectivamente) pueden servir como etiquetas. Para redes como Ethernet y PPP (Point to Point

Protocol), a la etiqueta se le añade una cabecera *shim* entre las cabeceras de la capa de enlace y la capa de red, que contendrá el campoTTL (Time To Live).

Las decisiones de asignación de etiquetas pueden estar basadas en criterios de envío como encaminamiento *unicast*, *multicast*, ingeniería de tráfico, VPN (Virtual Private Network) y QoS (Quality of Service).

Las etiquetas constan de 32 bits y tienen el siguiente formato:

Etiqueta (20 bits)	CoS (3 bits)	Pila (1 bit)	TTL (8 bits)

- Etiqueta (20 bits): contiene la etiqueta asignada.

- CoS (3 bits): indica la clase de servicio que requiere el paquete.

- Pila (1 bit): permite apilar etiquetas en un paquete para realizar un encaminamiento jerárquico.

- TTL (8 bits): tiene el mismo significado que en IP, se denomina cabecera *shim*.

Bucles:

El campo TTL indica el tiempo máximo de vida del paquete contado en saltos entre LSRs, este mecanismo permite mitigar los efectos de la creación de un bucle en la red haciendo desaparecer el paquete en el momento que supere este tiempo.

En ATM o Frame Relay donde no es posible utilizar TTL, los efectos de los bucles se minimizan mediante la limitación del espacio en *buffers* para un único VC (Virtual Channel).

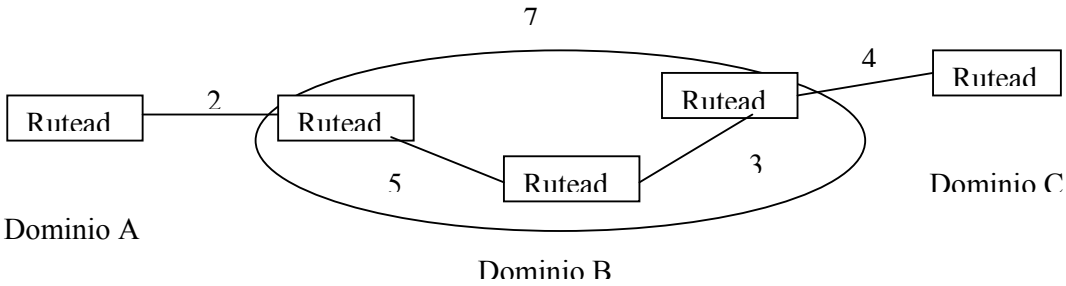
Otra alternativa para detectar bucles es mediante la técnica Vector de Rutas (Path Vector). Este vector contiene la lista de los LSRs que atraviesa el LSP, cuando un LSR propaga un mensaje de control del LDP (Label Distribution Protocol) añade su identificador al vector que irá en ese mensaje, por lo tanto, cuando un LSR reciba un mensaje en cuyo vector de caminos se encuentre su propio identificador se detectará el bucle.

Hay que hacer notar que los bucles sólo se producirán en el encaminamiento salto a salto y en el encaminamiento explícito tolerante que se verá más adelante.

Pila de etiquetas:

Permite operaciones jerárquicas en MPLS, cada nivel en la pila de etiquetas pertenece a un nivel jerárquico, esto facilita la creación de túneles en MPLS.

Para realizar el encaminamiento mediante túneles veamos un ejemplo:



Encaminamiento:

- La secuencia de etiquetas entre dominios es: 2-7-4

- La secuencia de etiquetas dentro del dominio B es: 5-3

Las operaciones que se realizarán son:

1. Del dominio A al B el paquete llevará la etiqueta 2.

2. En el *ruteador* de entrada al dominio B se intercambiará la etiqueta 2 por la 7, que identifica al nuevo dominio, y apila la etiqueta 5 que indica el siguiente salto en esa red.

3. En el siguiente *ruteador* se intercambiará la etiqueta 5 por la 3.

4. En el *ruteador* de salida se desapila 3 y ve que la etiqueta de entrada que tiene es 7, e intercambia ésta con 4 para llegar al siguiente dominio.

Distribución de etiquetas.

MPLS permite varios protocolos de señalización para la distribución de etiquetas entre LSRs, el uso de cada uno de ellos dependerá del *hardware* de la red MPLS y de las políticas de administración de ésta.

Protocolos de *ruteo* como BGP permiten llevar *piggybacked* información sobre las etiquetas entre los contenidos propios del protocolo, se utilizan para etiquetas externas en VPNs.

RSVP también ha sido extendido para soportar intercambio de etiquetas *piggybacked*.

Además, MPLS tiene su propio protocolo LDP para señalización y gestión del espacio de etiquetas, a éste se le han añadido extensiones para soportar, también, requerimientos de QoS y CoS (Class of Service), así tenemos CR-LDP (Constraint-based – LDP).

RSVP y CR-LDP se utilizan para la ingeniería de tráfico y reserva de recursos.
Para direcciones *multicast* tenemos PIM (Protocol-Independent Multicast).

LSP.

Cuando un paquete entra en la red MPLS se examina para determinar qué LSP debe asociársele y, a partir de aquí, qué etiqueta asignarle. Esta decisión se debe a factores como la dirección de destino, QoS y el actual estado de la red.

- Dominio MPLS: conjunto de dispositivos habilitados en MPLS.

Dentro de un dominio MPLS, un camino es establecido para que un paquete dado viaje con un determinado FEC. Existen dos mecanismos para establecer un LSP:

- Encaminamiento salto a salto: cada LSR selecciona independientemente el próximo salto para un FEC determinado (similar a la metodología utilizada en redes IP). El LSR utiliza cualquier protocolo de *ruteo* disponible como OSPF, ATM PNNI (ATM Private Network-Node Interface),etc.

- Encaminamiento explícito: El LER de entrada determina la secuencia de saltos explícita desde la entrada hasta la salida (ER-LSP, Explicit Routing LSP). Puede que la ruta no esté completamente especificada, es decir, puede haber un conjunto de nodos (Nodo Abstracto) que es representado como un único salto en la ruta. También puede contener un identificador de Sistema Autónomo que permite que el LSP sea encaminado a través de un área de la red que está fuera del control administrativo de quien inició el LSP. Dentro de estos dos casos se hará un encaminamiento salto a salto.

Puede clasificarse como **estricto** (*strict*), aquel camino que incluye todos los nodos, nodos abstractos y Sistemas Autónomos por los que pasa y el orden establecido; o como **tolerante** (*loose*), aquél que incluye todos los saltos y mantiene el orden, pero puede incluir saltos que sean necesarios para alcanzar algún salto específico.

El camino puede que no sea óptimo puesto que deben tenerse en cuenta los parámetros del servicio. Los recursos serán reservados a lo largo del camino para

asegurar QoS. Esto facilita la ingeniería de tráfico y el poder tener servicios diferenciados usando políticas de tráfico o métodos de gestión de red.

El establecimiento de un LSP para un FEC es unidireccional. El tráfico de vuelta debe tomar otro LSP.

Cuando se detecte un fallo en la red o la topología cambie se debe de proporcionar un nuevo LSP para re-encaminar el tráfico. En una ruta explícita estricta sólo se puede re-encaminar el tráfico en el LER de entrada que es quien decide la ruta, con lo que debe ser informado del error para proporcionar una ruta alternativa. En una ruta explícita tolerante cualquier LSP puede tomar un camino alternativo si es capaz de detectar el fallo del vecino, si la ruta ya está disponible o si un LSP de mayor prioridad requiere esos recursos reservados.

4. INGENIERÍA DE TRÁFICO

La ingeniería de tráfico es el proceso que mejora la utilización de la red mediante la distribución del tráfico en ella de acuerdo con la disponibilidad de los recursos, el tráfico actual y el esperado. CoS y QoS pueden ser factores a tener en cuenta en este proceso.

Como resultado, tenemos que se evita la congestión en cualquier camino. La mejora de la utilización de la red no implica necesariamente que se obtenga el mejor camino, pero sí el mejor camino para un determinado tipo de tráfico.

La ingeniería de tráfico permite al proveedor hacer un mejor uso de los recursos y permitir reservar enlaces para determinadas clases de servicio o clientes.

Aquí encontramos el caso de las **rutas forzadas**. La ruta que un LSP puede tomar puede forzarse para que cumpla unos requerimientos seleccionados en el LER de entrada (un caso particular de ellas son las rutas explícitas, donde el parámetro que fuerza este camino es el orden que debe seguir). Los parámetros que pueden ser utilizados para

describir esas rutas son el ancho de banda, el retardo, la prioridad, etc., que se desea para un flujo de tráfico.

Para calcular estas rutas existen dos métodos:

- calcular en el LER de entrada toda la ruta basándose en información sobre el estado de la red.

- calcular la ruta salto a salto con información local a cada LSR sobre la disponibilidad de los recursos.

Los dos métodos pueden combinarse si en alguna parte de la ruta la información no está disponible (p.ej. en un Sistema Autónomo).

Pero no basta sólo con obtener la ruta, es necesario reservar los recursos para poder satisfacer el servicio requerido.

Existen dos aproximaciones: TE-RSVP y CR-LDP, ambas utilizan el encaminamiento explícito para crear los LSPs e introducen una sobrecarga de información adicional al crear, mantener y destruir un LSP, pero ésta, es mínima comparada con la generada al procesar la cabecera IP.

4.1 TE-RSVP.

TE-RSVP (Trafic Engneering – RSVP) es una extensión del protocolo RSVP.

TE-RSVP es un protocolo de señalización *soft state* que utiliza UDP o datagramas IP para la comunicación entre compañeros LSR (LSR *peers*).

Creación de un ER-LSP:

1. El LER de entrada quiere establecer un nuevo LSP hacia el LER de salida. Los parámetros de tráfico determinan por dónde debe pasar la ruta, así que el LER de entrada envía un mensaje PATH con la ruta explícita hacia el LER de salida y con los parámetros de tráfico que requiere la sesión.

2. Cada nodo de la ruta que recibe el mensaje determina si es la salida para ese LSP, si no lo es, sigue enviando el mensaje PATH eliminándose de la ruta. En cualquier caso cada LSR creará una nueva sesión.

3. Una vez llega al LER de salida, éste determina qué recursos ha de reservar y devuelve un mensaje RESV que distribuirá la etiqueta que ha elegido para ese LSP y contendrá los detalles de la reserva.

4. Los LSRs intermedios emparejan los mensajes PATH y RESV que han recibido según el identificador de LSP, reservan los recursos que indica RESV, asignan una etiqueta para el LSP, rellenan la tabla de envío y envían la nueva etiqueta en otro mensaje RESV.

5. El LER de entrada, cuando lo recibe, enviará un mensaje de confirmación RESVConf para indicar que se ha establecido el LSP.

Después de haberse establecido el LSP se enviarán mensajes periódicos para mantener el camino y las reservas.

4.2 CR-LDP.

CR-LDP (Constraint-based LDP), a diferencia de TE-RSVP, no necesita de implementaciones adicionales ya que está basado en LDP y utiliza su misma estructura para los mensajes.

Es un protocolo *hard state* y utiliza sesiones TCP entre compañeros LSR.

Creación de un ER-LSP:

1. El LER de entrada quiere establecer un nuevo LSP hacia el LER de salida. Los parámetros de tráfico determinan por dónde debe pasar la ruta, así que el LER de entrada reserva los recursos que necesita y envía un mensaje LABEL_REQUEST con la ruta explícita hacia el LER de salida y con los parámetros de tráfico que requiere la sesión.

2. Cada nodo de la ruta que recibe el mensaje reserva los recursos y determina si es la salida para ese LSP, si no lo es, sigue enviando el mensaje LABEL_REQUEST eliminándose de la ruta. Puede reducir la reserva si los parámetros de tráfico están marcados como negociables.

3. Una vez llega al LER de salida, éste realiza cualquier negociación final sobre los recursos y hace la reserva. Asigna una nueva etiqueta al nuevo LSP y la distribuye en un mensaje LABEL_MAPPING que contiene los parámetros de tráfico finales reservados para el LSP.

4. Los LSRs intermedios emparejan los mensajes LABEL_REQUEST y LABEL_MAPPING que han recibido según el identificador de LSP, asignan una etiqueta para el LSP, rellenan la tabla de envío y envían la nueva etiqueta en otro mensaje LABEL_MAPPING.

5. En cuanto llegue al LER de entrada se habrá establecido el LSP.

4.3 Comparación de ambos métodos.

- TE-RSVP es *soft state,* lo cual significa que la información es intercambiada cuando se establece el LSP, pero se deben enviar mensajes periódicos para notificar que la conexión todavía se requiere. Por el contrario, CR-LDP es *hard state*, es decir, toda la información se intercambia al iniciar la conexión y no se produce más información adicional hasta que el LSP se elimine.

- El hecho que TE-RSVP sea *soft state* e introduzca una sobrecarga adicional hace que no sea escalable ya que esta sobrecarga crecerá proporcionalmente con el número de sesiones RSVP. Para evitar esto se intenta resumir la información y aprovechar un único mensaje para enviar varios mensajes de refresco.

- CR-LDP utiliza conexiones TCP lo que hace que éstas sean más fiables y seguras, mientras que TE-RSVP utiliza UDP o datagramas IP para establecer las comunicaciones, lo que supone mayor vulnerabilidad aunque puede utilizar IPSec o algún otro esquema de encriptación.

- Las conexiones TCP de CR-LDP permiten detectar un fallo mediante notificaciones propias de TCP. Esta notificación se procesa rápidamente así que las acciones oportunas sean iniciadas. Sin embargo, una conexión fallida en TE-RSVP será detectada cuando no se reciba un determinado mensaje de refresco y, dependiendo de cómo se haya configurado, detectar un fallo tardará segundos o minutos antes de que puedan iniciarse las acciones de recuperación.

- Ambos protocolos soportan re-encaminamiento (*re-ruteo*):

    - TE-RSVP puede crear una nueva ruta a partir de un salto diferente en un LSR, así, en el momento en que se detecte el fallo refrescará esta nueva ruta que pasará a ser operativa y, la antigua se eliminará cuando deje de recibir mensajes de refresco.

- Otra alternativa que soportan ambos protocolos es crear una ruta completa alternativa mientras se usa la antigua, en el momento que se produzca un fallo la nueva ruta será operativa y se eliminará la antigua.

– CR-LDP soporta que un LSP dé servicio a muchos *hosts* mediante la designación de FECs, mientras que RSVP sólo reserva ancho de banda a una única dirección IP.

La elección entre los diferentes protocolos se deberá a factores como la complejidad de la red, si las conexiones van a ser cortas o permanentes, qué grado de tolerancia a fallos se requiere, etc.

5. CONCLUSIÓN

MPLS hace posible conmutar el tráfico a través de *ruteadores* IP que siempre han tenido que procesar la cabecera IP para enviar los datos con la consiguiente sobrecarga en ellos. Esto se consigue a través de la etiqueta que se ha insertado que se corresponde con un camino establecido.

Este protocolo es simple, lo que facilita su implementación, además simplifica el envío de los paquetes utilizando conmutación mediante *hardware*. También ofrece QoS y CoS por lo que puede ofrecer garantías de servicio.

MPLS es capaz de integrar IP y ATM mediante la construcción de un puente entre las dos redes, también facilita la integración de IP sobre SONET en conmutación óptica.

La red MPLS es una red bastante segura ya que no se permite que los datos entren o salgan del LSP por lugares que no han sido establecidos por el administrador de la red, además, cuando los datos entran en el dispositivo para conmutarse no son vistos por capas superiores más que por el módulo de envío MPLS, que intercambiará la etiqueta conforme a la tabla de envío del LSR, lo que impide en gran medida que usuarios malintencionados “husmeen” la información.

Además, MPLS puede aplicarse a redes privadas virtuales (VPNs) mediante la construcción de túneles con etiquetas apiladas.

INDICE DE TABLAS

CAPITULO I

MARCO TEORICO REFERENCIAL

CAPITULO II

SISTEMAS ADMINISTRADORES DE ANCHO DE BANDA

CAPITULO III

ESTUDIO DEL SISTEMA PACKETSHAPER

CAPITULO IV

PRUEBAS DEL SISTEMA PACKETSHAPER

CAPITULO V

ESTABLECIMIENTO DE POLITICAS

INDICE DE FIGURAS

CAPITULO I

MARCO TEORICO REFERENCIAL

CAPITULO II

SISTEMAS ADMINISTRADORES DE ANCHO DE BANDA

CAPITULO III

ESTUDIO DEL SISTEMA PACKETSHAPER

CAPITULO IV

PRUEBAS DEL SISTEMA PACKETSHAPER

CAPITULO V

ESTABLECIMIENTO DE POLITICAS

GLOSARIO DE TERMINOS

A

- *ACK*.- Bit usado por TCP para indicar que el paquete recibido por el emisor es un reconocimiento por parte del receptor.

- *ACL (Access Control List)*.- Lista de control de acceso, usadas para clasificación en ruteadores.

- *Acondicionamiento*.- Conjunto de funciones que son aplicadas a flujos de tráfico dependiendo del sistema, estas funciones son la clasificación, medición, políticas, priorización, descarte, modelamiento, planificación, encolamiento y marcado.

- *Ancho de banda*.- Es una medida de la capacidad de transmisión de datos, expresada generalmente en Kilobits por segundo (kbps) o en Megabits por segundo (Mbps).

- *ARPANET (Advanced Research Projects Agency Network)*.- Red avanzada de agencias para proyectos de investigación, pionera en tecnología de conmutación de paquetes y fue la base de lo que ahora es el Internet.

- *ATM (Asynchronous Transfer Mode)*.- Modo de transferencia asincrónica, donde dos o más oficinas remotas son conectadas a una oficina principal por medio de circuitos virtuales (VCs). Todo el tráfico pasa a través de una nube WAN ATM y puede ser tuteado por un ruteador en la oficina principal. Para enviar tráfico entre oficinas algunos ruteadores pueden rutear tráfico entre VCs.

B

- *BA (Behavior Aggregate).*- Agregado de comportamiento, colección de paquetes que atraviesan en una dirección particular con un mismo servicio diferenciado.

- *Best effort.*- Mejor esfuerzo, implementado por defecto en el protocolo IP que transmite datos cuando lo desea, en cualquier cantidad y sin tomar en cuenta calidad de servicio.

- *Bit.*- Un dígito simple de un número binario que puede ser 1 ó 0.

- *Bridge.*- Componente de una red LAN que permite unir dos redes o segmentar una LAN demasiado grande.

- *Buffer.*- Memoria intermedia para almacenar información.

- *Bursty.*- Incrementos explosivos de velocidad, estos incrementos son generalmente de tráfico.

- *Bypass.*- Tecnología de derivación de un sistema administrador de ancho de banda para que se comporte como un elemento pasivo cuando falle o esté apagado.

- *Byte.*- Unidad común en comunicaciones compuesta por ocho bits.

C

- *Caché.*-Para Internet son datos que se guardan en un espacio de disco de cada máquina de usuario y permiten el acceso rápido a páginas ingresadas anteriormente.

- *CAR (Commited Access Rate).*- Tasa de acceso comprometida, en una interfaz trata de mantener constante una tasa de datos.

- *CBQ (Class Base Queuing).*- Encolamiento basado en clases, realiza encolamiento y ofrece la capacidad de regular el ancho de banda.

- *CBWFQ(Class Base Weighted Fair Queuing).*- Encolamiento justo pesado basado en clases es una variación del encolamiento justo pesado utilizado cuando se quiere garantizar ancho de banda a las aplicaciones de datos.

- *CE (Congestion Experienced).*- Experimentó congestión, utilizado en ECN, es un bit ajustado por un ruteador para indicar congestión en los nodos extremos.

- *Citrix-ICA (Independent Computer Architecture).*- Arquitectura de computador independiente Citrix.

- *Clase:* Para PacketShaper es un grupo lógico de flujos de tráfico que comparten las mismas características, por ejemplo protocolo, dirección, aplicación específica, subred.

- *Clasificador.*- Un elemento que selecciona paquetes y lo clasifica de acuerdo a reglas definidas.

- *Congestion Avoidance.*- Anulación de congestión, algoritmo implementado en TCP para disminuir la tasa de envío de paquetes del emisor en base a un umbral de comienzo o congestión.

- *Control de tasa de TCP.*- Algoritmo propietario de Packeteer, permite realizar un control de tasa de flujos de tráfico básicamente negociando reconocimientos de TCP.

- *CoS (Class of Service).*- Clase de servicio, priorización en capa 2 mediante tres de cuatro bits de una etiqueta (Tag) e implementado a nivel de switches.

- *CQ (Custom Queuing).*- Encolamiento personalizado, el ancho de banda debe de ser compartido proporcionalmente y se puede especificar ancho de banda personalizado.

D

- *DARPA (Defense Advanced Research Projects Agency).*- Agencia de proyectos de investigación avanzada de defensa.

- *Datagrama.*- Unidad de mensaje IP que contiene las direcciones origen y destino de la red y los datos.

- *Demultiplexor.*- Dispositivo que recupera varias transmisiones de una sola transmisión.

- *Descartador.*- Realiza el proceso de descarte, basado en reglas especificas o políticas.

- *DHCP (Dynamic Host Configuration Protocol).*- Protocolo de Configuración de Computadores Dinámica, asigna direcciones IP a computadores de forma dinámica

- *Dirección IP.*- La dirección IP de 32 bits de un elemento de red.

- *Dirección MAC (Médium Access Control).*- Dirección de control de acceso el medio, constituye la dirección física del equipo para identificarlo en una red.

- *Direct Standby*.- Configuración que permite a dos PacketShapers trabajar en una topología de red redundante junto con ruteadores, switches o firewalls redundantes.

- *DLS*.- Protocolo de la Arquitectura de Red de Sistemas IBM (SNA) sobre el protocolo de control de transmisión (TCP).

- *DMZ (Demilitarized Zone)*.- Zona desmilitarizada, red de área local no protegida y creada por un firewall.

- *DNS (Domain Name Server)*.- Una máquina dedicada a trasladar direcciones IP de usuario asignadas a nombres comunes o nombres de dominio de red.

- *DOS (Disk Operating System)*.- Sistema operativo de disco, utiliza línea de comando.

- *DoS (Denial of Service)*.- Rechazo de servicio, de flujos de tráfico anormales.

- *DSCP (Differentiated Services Codepoint)*.- Punto de código de servicios diferenciados, combinación de seis bits en el encabezado del protocolo IP para lograr hasta 64 servicios diferenciados.

E

- *E1*.- Medida de capacidad de un enlace equivalente a 2.048 Mbps.

- *ECN (Explicit Congestion Notification)*.- Notificación de congestión explícita, esquema de control que propone notificación de congestión marcando los paquetes.

- *ECT (Explicit Congestion Notification Capable Transport).*- Apto para transporte notificación de congestión explícita, bit ajustado por el emisor para indicar que los extremos son capaces de realizar ECN.

- *EF (Expedited Forwarding).*- Despachamiento hacia delante, reserva ancho de banda, asegura baja latencia, retardo, jitter y pérdida de paquetes en servicios diferenciados.

- *Encabezado.*- Códigos adicionales transmitidos con fines de control y verificación de errores.

- *Encolamiento (Queuing).*- Consiste en dividir y organizar el tráfico en un determinado elemento de red para su posterior retransmisión según un determinado algoritmo que define a la cola.

F

- *FIFO (First In- First Out).*- Entra primero – sale primero, utilizado por el servicio best effort e implementado por memoria intermedia o buffers.

- *FIN.*- Bit usado por TCP para indicar que el emisor no envía más datos, mediante este bit en cada lado un elemento de red cierra su canal de comunicación.

- *Firewall.*- Elemento brinda seguridad a una red, especialmente en el Internet.

- *Firmware.*- Una categoría de chips de memoria que mantienen su contenido sin energía eléctrica, incluye tecnologías ROM, PROM, EPROM, EEPROM.

- *Flujo*.- Es comparado con una vía, es el conjunto de datos pertenecientes a una misma secuencia generalmente es una combinación de direcciones, puertos e identificadores.

- *Frame Relay*.- Tecnología utilizada para enlaces de red de área amplia donde dos o más oficinas remotas son conectadas a una oficina principal por medio de circuitos virtuales permanentes (PVCs) y el tráfico pasa a través de un switch Frame Relay (nube WAN) y es ruteado por un Equipo de Acceso Frame Relay (FRAD).

- *Full duplex*.- Comunicación bidireccional simultánea a través de un canal.

G

- *GRE (General Routing Encapsulation)*.- Encapsulación de enrutamiento general, usado en redes virtuales privadas (VPN).

- *GUI (Graphical User Interface)*.- Interfaz de usuario gráfica.

H

- *H.323*.- Puerto usado por voz sobre IP.

- *Half duplex*.- Comunicación bidireccional pero transmite uno a la vez a través de un canal.

- *Handshake*.- Acuerdo en tres fases, intercambio de segmentos de control usado en TCP para establecer una conexión.

- *Hardware*.- Maquinaria y equipamiento que funciona en conjunto con el software.

- *Host*.- Computador.

- *Hot Standby*.- Configuración redundante o de protección, compuesta por dos administradores de ancho de banda, uno principal y otro de respaldo.

- *HSRP (Hot Standby Routing Protocol)*.- Protocolo de protección de enrutamiento usado por el administrador de ancho de banda Accelerator para implementar redundancia mediante un equipo similar o un ruteador dentro de una LAN.

- *HTML (Hypertext Markup Language)*.- Lenguaje de marcado de hipertexto, lenguaje estándar de páginas web de Internet.

- *HTTP (Hypertext Transfer Protocol)*.- Protocolo de transferencia de hipertexto, usado para transferencia de tráfico de navegación en Internet.

- *Hub*.- Repartidor, dispositivo que interconecta a grupos de usuarios, lo que emite uno le llega al resto, no es capaz de aislar el tráfico.

I

- *IANA (Internet Assigned Numbers Authority)*.- Autoridad de números asignados a internet, controla y asigna números de puertos a aplicaciones y protocolos.

- *ICMP (Internet Control Message Protocol)*.- Protocolo de mensajes de control de internet, usado por el protocolo IP para reportar errores en la conexión, en el sistema operativo DOS se utiliza el comando ping.

- *IEEE (Institute of Electrical and Electronics Engineers)*.- Instituto de ingenieros eléctricos y electrónicos, se encarga de normas y estándares de redes de área local y área amplia.

- *IETF (Internet Engineering Task Force)*.- Fuerza de tareas de ingeniería de Internet, define la clasificación de calidad de la calidad de servicio.

- *IKE (Internet Key Exchange)*.- Intercambio de clave en Internet.

- *Inbound*.- Denominado por PacketShaper al enlace de red de área amplia de entrada, por este enlace ingresa información a la red de área local desde otras redes externas.

- *Interfaz*.- Conexión e interacción entre hardware, software y usuario.

- *Internet Service Provider (ISP)*.- Proveedor de servicio de Internet.

- *IP (Internet Protocol)*.- Protocolo de Internet, define la unidad básica para la transferencia de datos, selección de rutas y conjunto de reglas para la entrega no confiable de paquetes a la capa de transporte.

- *IPSec-AH (IP Security Encapsulation-Authentication Header)*.- Encapsulación de Seguridad IP-Encabezamiento de Autenticación, usado en redes privadas virtuales (VPN).

- *IPSec-ESP (IP Security Encapsulation-Encapsulating Security Payload)*.- Encapsulación de Seguridad IP-Payload de Seguridad Encapsulado, usado en redes privadas virtuales (VPN).

- *ISN (Initial Sequence Number).*- Número inicial de secuencia aleatorio con un rango de 0 a 2,147,483,647 usado para establecer una conexión TCP.

- *ISO (International Standards Organization).*- Organización internacional de estándares, establece normas internacionales.

- *ITU (International Telecommunications Union).*- Unión Internacional de Telecomunicaciones, organismo que se encarga de normas y estándares de telecomunicaciones.

J

- *Jitter.*- Es la inestabilidad o variabilidad en el retardo.

K

- *Kernel.*- Núcleo o parte principal de algo, tal como un sistema operativo.

L

- *L2TP (Layer 2 Tunneling Protocol).*- Protocolo para formar Túneles Capa 2, usado en redes privadas virtuales (VPN).

- *LAN (Local Area Network).*- Red de área local, red de comunicaciones que sirve a usuarios dentro de un área geográficamente limitada.

- *Latencia.*- Es el tiempo entre el envío de un mensaje por parte de un nodo y la recepción del mensaje por otro nodo.

- *LEM (LAN Expansion Module).*- Módulo de expansión de LAN, usado por el administrador de ancho de banda PacketShaper, con el fin de ampliar su capacidad de hardware.

M

- *Manage Information Base (MIB).*- Base de información de manejo, bases de datos de un sistema utilizadas por plataformas de administración que usan SNMP.

- *Marcador.*- Un elemento que realiza marcado del encabezado de paquetes, de acuerdo a reglas definidas.

- *Maximum Transmission Unit (MTU).*- Unidad de transmisión máxima, es el tamaño máximo de un paquete, depende de la tecnología de red por la que se transmite.

- *Medidor.*- Realiza el proceso de medir las propiedades temporales como por ejemplo la tasa de bits de un flujo seleccionado por un clasificador.

- *MILNET.*- Departamento de defensa de estados unidos, posterior subdivisión militar de comunicaciones de ARPANET.

- *MIME (Multipurpose Internet Mail Extensions).*- Extensiones de correo de Internet multipropósito.

- *Modelador.*- Conocido como shaper, permiten modelar a los flujos de tráfico valiéndose de tipo de control de calidad de servicio.

- *MPLS (Multi Protocol Label Switching).*- Conmutación por etiquetas multiprotocolo, es un dominio de conmutación por etiquetas multiprotocolo a nivel de capa de enlace.

- *Multiplexor*.- Dispositivo que combina varias transmisiones en una sola transmisión.

N

- *NAT (Network Address Translation)*.- Traducción de dirección de red, permite a varios computadores de una red de área local utilizar una sola dirección IP para el enlace de área amplia, especialmente para acceso al Internet

- *Nodo*.- Punto de empalme o conexión en una red.

- *Número de reconocimiento*.- En TCP es el número enviado por el receptor hacia el emisor, indicando un reconocimiento de un paquete o número de secuencia que espera recibir.

- *Número de secuencia*.- Un número asignado a paquetes TCP para indicar el número de byte inicial de datos a menos que el bit SYN sea 1.

O

- *OSI (Open Standards Interconnection)*.- Interconexión de sistemas abiertos, modelo que fue definido por la ISO como norma de las comunicaciones mundiales.

- *Outbound*.- Denominado por PacketShaper al enlace de red de área amplia de salida, por este enlace sale información de la red de área local hacia otras redes externas.

P

- *PacketCapture.*- Herramienta de Packeteer que captura flujos de paquetes para su posterior análisis en analizadores de protocolos.

- *PacketSeeker.*- Herramienta de Packeteer que se encarga de monitorear e identificar el tráfico de una red.

- *PacketShaper.*- Herramienta de Packeteer que asigna el ancho de banda basado en las políticas y provee la calidad de servicio gracias a varios mecanismos.

- *PacketWise.*- Software de Packeteer que permite la configuración del PacketShaper ya sea vía línea de comandos o vía navegador web.

- *Partición.*- Para PacketShaper es un tubo de ancho de banda asignado a una clase de tráfico dada, con el fin de proteger o restringir todos los flujos que forman parte de la clase.

- *Peer to Peer (P2P).*- Par a par, metodología que utilizan aplicaciones para compartir archivos mediante el Internet.

- *PHB (Per Hop Behavior).*- Comportamiento por salto en servicios diferenciados.

- *Planeamiento de límite de retardo.*- Especifica un límite estricto en la variación del retardo de paquetes en un punto.

- *Planificación.*- Es un algoritmo de decisión implementado en diferentes métodos y sistemas.

- *Políticas*.- Normas que se aplican a flujos, establecen un tipo de control de calidad de servicio según el tipo de flujo y su importancia. Para PacketShaper es una regla asignada a una clase, dicha regla define como un flujo simple será manejado durante la asignación de ancho de banda.

- *PPTP (Point to Point Tunneling Protocol)*.- Protocolo para formar Túneles Punto a Punto, usado en redes privadas virtuales (VPN).

- *Precedencia*.- Es una medida de la naturaleza y prioridad de un datagrama IP.

- *Protocolo Punto a Punto (PPP)*.- Proporciona conexiones o transmisión ruteador a ruteador y computador a red.

- *PQ (Priority Queuing)*.- Encolamiento de prioridad, cada uno de los paquetes debe de ser colocado en una de las cuatro posibles colas alta, media, normal y baja prioridad.

- *Priorización*.- La priorización consiste en la asignación de un determinado nivel de prioridad al tráfico que circula por una red.

- *Protocolo*.- Normas y regulaciones que gobiernan las transmisión y recepción de datos.

- *Puerto*.- Un puerto es un número de 16 bits empleado por un protocolo computador a computador.

Q

- *QoS (Quality of Service)*.- Calidad de servicio, conjunto de tecnologías como herramientas, protocolos, señalización que ayudan a la gestión de una red,

asegurando que su tráfico y los requisitos del servicio previamente establecidos puedan ser satisfechos.

R

- *RADIUS (*Remote Authentication Dial-in User Service*).*- Servicio de Autenticación Remota de Llamada de Usuario.

- *Red.*- Canales de transmisión y el soporte de hardware y software.

- *RED (Random Early Detection).*- Detección temprana aleatoria, descarte inteligente de paquetes para evitar congestión y así el fenómeno oscilante producida en TCP.

- *Remote Autentication Dial In User Service (RADIUS).*- Servicio de autenticación remota de llamada de usuario, usado en servidores para obtener autenticación de usuarios que se conectan remotamente a una red.

- *Retardo.*- Indica la variación temporal o retraso en la llegada de los flujos de datos a su destino.

- *RFC (Request for comment).*- Petición para comentar, publicaciones de algoritmos por parte de investigadores hacia la comunidad de Internet.

- *Round Robin.*- Asignación cíclica ó acceso por turnos a algún recurso.

- *Router.*- Ruteador, dispositivo que selecciona un recorrido adecuado y encamina un mensaje de acuerdo a dicho recorrido a través de redes diferentes.

- *RSVP (Resource ReserVation Protocol).*- Protocolo de reservación de recursos, reserva ancho de banda dentro de la red aún en momentos de congestión.

- *RTCP (Real-time Control Protocol).*- Protocolo de control en tiempo real, lleva la información de control de los flujos de voz sobre IP, trabaja junto a RTP.

- *RTM (Response Time Metrics).*- Medidas de tiempo de respuesta implementado por PacketSeeker, permite analizar medidas de retardos y tiempos de viaje redondo.

- *RTP (Real-time Transport Protocol).*- Protocolo de transporte en tiempo real, lleva los flujos de datos de voz sobre IP, trabaja junto a RTCP.

- *RTT (Round Trip Time).*- Tiempo de viaje redondo, es la diferencia de tiempo entre un tiempo actual en que recibe un paquete el emisor y el tiempo en que el receptor envió dicho paquete al emisor.

S

- *Servicio Garantizado (Intserv).*- Tipo de calidad de servicio donde el elemento final señala su necesidad de calidad de servicio a la red, utiliza reservación de ancho de banda.

- *Servidor Proxy.*- Una máquina dedicada a traducir cada dirección IP de cada usuario de una LAN a una sola dirección IP la que servirá como entrada al Internet.

- *Servidor DHCP (Dinamic Host Configuration Protocol).*- Una máquina dedicada a asignar una dirección IP a cada usuario de una LAN.

- *SFQ (Stachastic Fair Queuing).*- Encolamiento justo estocástico, algoritmo el cual asigna estocásticamente los flujos a varias colas entra primero – sale primero.

- *SLA (Service Level Agreement).*- Acuerdo de nivel de servicio en servicios diferenciados.

- *Slow Start.*- Empieza lento, algoritmo implementado en TCP para determinar y aumentar la tasa de envío de paquetes del emisor en base a los reconocimientos del receptor.

- *SNA (System Network Architecture).*- Protocolo de la Arquitectura de Red de Sistemas IBM.

- *SNMP (Simple Network Management Protocol).*- Protocolo de administración de red simple, usado para administración de redes de gran escala.

- *Software.*- Una serie de instrucciones que realizan una tarea particular se lama programa ó programa de software.

- *SSL (Secure Sockets Layer).*- Protocolo de capa de zócalos segura, usada para tráfico web seguro.

- *SSH (Secure Shell).*- Protocolo de autenticación remoto protección segura.

- *Streaming media.*- Flujos de aplicaciones multimedia en tiempo real.

- *Switch.*- Conmutador, dispositivo que interconecta una fuente con varios destinos, interconecta subredes y aísla el tráfico de cada subred con respecto a las otras.

- *SYN.*- Bit usado por TCP para establecer como número de secuencia a ISN dentro de un paquete.

T

- *TCB (Traffic Conditioner Block).*- Bloque condicionador de tráfico, realiza funciones como clasificación, medición, marcado y modelado del tráfico en servicio diferenciados.

- *TCP (Transmission Control Protocol).*- Protocolo de control de transmisión, protocolo usado para transporte añade fiabilidad y control de flujo.

- *TCP/IP.*- Combinación de Protocolo de Control de Transmisión junto con el Protocolo de Internet para intercambio de información en una red.

- *TDM (Time Division Multiplexing).*- Multiplexación por división de tiempo, método de acceso en donde el tiempo se divide en porciones de tiempo al que tiene acceso un elemento.

- *TELNET.*- Protocolo de emulación de terminal, permite realizar sesiones de configuración de un sistema remotamente mediante una dirección IP.

- *Tiempo de vida.*- Especifica el tiempo en segundos que se le permite viajar a un datagrama.

- *Time out.*- Tiempo fuera o tiempo sin respuesta de conexión, se produce si TCP detecta que paquetes se han retrasado con respecto a una referencia de tiempo en una conexión o cuando el emisor retransmite varias veces paquetes y no obtiene reconocimientos.

- *Top Ten.*- Término utilizado por PacketShaper para señalar diez flujos de tráfico que sobresalen sobre los demás.

- *ToS (Type of Service).*- Tipo de servicio, priorización en capa 3 equivalente a CoS en capa 2 se logra mediante tres bits de precedencia del encabezado del protocolo IP e implementado a nivel de ruteadores.

- *Traffic Shapers.*- Sistemas administradores de ancho de banda dedicados, se colocan en una red para implementar servicios diferenciados.

- *Tráfico.*- Es los datos que atraviesan una red, es dependiente del tipo de aplicación que por ella circulan.

- *Traps.*- Mensajes que se observan en una plataforma de administración que utilice SNMP.

U

- *UDP (User Datagram Protocol).*- Protocolo de datagrama de usuario, protocolo usado para transporte de información no añade fiabilidad, ni control de flujo.

- *Umbral de comienzo.*- Abreviado como "ssthres", usado dentro del algoritmo congestion avoidance por el emisor para disminuir la tasa de envío de paquetes.

- *URL (Uniform Resource Locator).*- Localizador de recurso uniforme, nombre o dirección utilizada para la navegación en Internet.

V

- *Ventana.*- Usado en reconocimientos de TCP, especifica el número de bytes de datos que el receptor esta dispuesto a aceptar dependiendo de su memoria intermedia libre.

- *Ventana de congestión.*- Abreviada como “cwnd”, usada dentro del algoritmo slow start por el emisor para aumentar la tasa de envío de paquetes.

- *VLAN (Virtual Local Area Network).*- Red de área local virtual, creada por switches mediante etiquetas en los paquetes y se define en el estándar 802.1q.

- *VoIP.*- Voz transmitida sobre el protocolo IP.

- *VRRP (Virtual Router Redundancy Protocol).*- Protocolo de redundancia de ruteador virtual usado por el administrador de ancho de banda Accelerator para implementar redundancia mediante un equipo similar o un ruteador dentro de una LAN.

W

- *WAN (Wide Area Network).*- Red de área amplia, red de comunicaciones que sirve como enlace entre redes de área local.

- *WFQ (Weighted Fair Queuing).*- Encolamiento justo pesado, mecanismo adaptativo que transmite primero el tráfico de tiempo real y reparte equitativamente el ancho de banda.

- *WRED (Weighted Random Early Detection).*- Detección temprana aleatoria pesada, combina las capacidades de RED y del campo de precedencia del datagrama IP.

Z

- *Zócalo.*- Combinación de una dirección IP y un número de puerto.

ACTA DE ENTREGA

El proyecto de grado “Sistemas administradores de ancho de banda de enlaces WAN e Internet”, fue entregado a la Facultad de Ingeniería Electrónica y reposa en la Escuela Politécnica del Ejército desde:

Sangolquí,…….

Elaborado por:

_____
Christian Llerena Andrade

EL DECANO DE LA F.I.E.

_____
Ing. Xavier Martínez C.
TCRN. DE E.M.

EL SECRETARIO ACADEMICO

_____
Ab. Jorge Carvajal R.