INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS EN ELECTRONICA, COMPUTACION, INFORMACION Y COMUNICACIONES

CALIDAD DE SERVICIO (QOS) EN REDES DE TELECOMUNICACIONES

T E S I S

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADEMICO DE:
MAESTRO EN ADMINISTRACION DE LAS TELECOMUNICACIONES

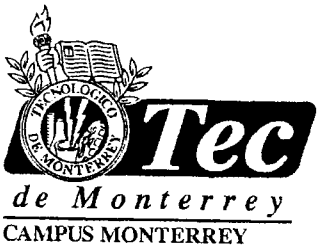
ARTURO LERMA LOPEZ

MONTERREY, N. L. DICIEMBRE DE 2002

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

PROGRAMA DE GRADUADOS EN ELECTRÓNICA, COMPUTACIÓN, INFORMACIÓN Y COMUNICACIONES.



CALIDAD DE SERVICIO (QOS) EN REDES DE TELECOMUNICACIONES

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA OBTENER EL GRADO ACADÉMICO DE:

MAESTRO EN ADMINISTRACIÓN DE TELECOMUNICACIONES

ARTURO LERMA LÓPEZ

MONTERREY, NL DICIEMBRE 2002

CALIDAD DE SERVICIO (QOS) EN REDES DE TELECOMUNICACIONES

POR:

ARTURO LERMA LÓPEZ

TESIS

Presentada al Programa de Graduados en Electrónica, Computación, Información y Comunicaciones.

Este trabajo es requisito parcial para obtener el grado de Maestro en Administración de Telecomunicaciones

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

DICIEMBRE 2002

DEDICATORIA

A mi esposa Edith por compartir mis sueños
para lograr el proyecto de vida que
tenemos juntos.

AGRADECIMIENTOS

A Dios, por permitirme estar junto a la gente que quiero.

A mi esposa, por impulsar todos los proyectos que hemos emprendido, por el esfuerzo y sacrificios hechos para realizar esta meta.

A mi hijo Antonio, por ceder parte de su tiempo tan importante.

A mis padres, por haberme dado la vida, por sus sacrificios para apoyarme a ser quien soy.

A mi hermana, por enseñarme a compartir y darme dos sobrinos preciosos.

A mis suegros, por apoyarnos cuando los hemos necesitado y a mis cuñados por su amistad.

Al Dr. Ramón M. Rodríguez Dagnino, por haber aceptado asesorarme para el desarrollo de ésta tesis, por sus valiosos comentarios y compartir su experiencia y conocimientos.

Al Dr. Ricardo Pineda Serna, por haber aceptado ser mi sinodal y compartir su experiencia en el mundo de las telecomunicaciones.

Al MC. Artemio Aguilar Coutiño, por haber aceptado ser mi sinodal, por compartir sus conocimientos en aquellas tareas de la clase de probabilidad y para ésta tesis. También por sus valiosos comentarios.

RESUMEN

La presente tesis inicia con un capítulo introductorio a las tecnologías de red donde es posible definir parámetros de Calidad de Servicio. Se describe la arquitectura de TCP/IP que es la base de Internet y como interactúa TCP o UDP con IP. En la especificación de IP se destinaron campos para establecer clases de servicio. Se explica la diferencia del protocolo actual de Internet IPv4 con IPv6 y también el concepto de ATM con sus atributos para transportar información con una clase de servicio diferenciada. MPLS por su parte puede ser implementado nativamente en equipos de conmutación ATM para rutear paquetes con calidad de servicio. Para terminar con éste primer capítulo, se define el protocolo de administración de redes SNMP el cual puede proveer información que sirva para administrar calidad de servicio en la red.

En el capítulo 3, se estudia el concepto de Calidad de Servicio de manera más profunda y se marca la diferencia entre Clases de Servicio y Calidad de Servicio. Se mencionan los tipos de servicio que puede tener una red, como el Servicio de Mejor Esfuerzo que es el que predomina actualmente en redes Ethernet y en Internet, donde se tratan todos los paquetes de información de igual manera, el Servicio Diferenciado en el que se ofrece prioridad a algún tipo de tráfico y el Servicio Garantizado donde se reserva un ancho de banda específico a una cierta aplicación. Se menciona como definir QoS basado en políticas de ruteo para crear servicios diferenciados. Se listan las diversas herramientas que se tienen para administrar o manejar el congestionamiento de tráfico y de esta manera clasificar el tráfico para darle prioridad en un enlace de salida y finalmente como monitorear los niveles de servicio que tiene una red, que deben ser previamente definidos en un acuerdo de nivel de servicio en el cual se especifica la disponibilidad, métricas, retardos, tasa de flujo de información, etc.

En los capítulos 4, 5 y 6 se muestran los parámetros de los distintos protocolos como IP, ATM y MPLS con respecto a QoS.

Hasta ahora se han manejado las tecnologías en forma aislada, por lo que es necesario estudiar los esquemas de interconexión entre ellas como se hace en el capítulo 7, todo esto bajo el concepto de calidad de servicio, para lo que se dividen en esquemas de asignación de recursos y optimización de rendimiento. En esta sección se incluye un nuevo concepto que se refiere al protocolo de reservación RSVP y como se utiliza con IP. Se incluyen los conceptos de Servicios Integrados y Diferenciados, se menciona como el concepto de servicios diferenciados surgió como alternativa para asignación de recursos ante las limitaciones de los servicios integrados. En lo que se refiere a optimización de rendimiento, es dirigido hacia enlaces de área amplia y sus beneficios al utilizar MPLS, IP sobre ATM e Ingeniería de tráfico en Internet como herramientas para implementar QoS.

El marco teórico termina con los capítulos anteriores, por lo que se destina el capítulo 8 como aportación a la presente tesis, haciendo una investigación de la manera en que se pueden implementar QoS en diferentes escenarios, una red local, una red metropolitana y una amplia, y los enlaces entre ellas para obtener QoS. Estos escenarios se consideran como los más comunes a los que se enfrentan los administradores de redes.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

1. INTRODUCCIÓN

Las innovaciones tecnológicas en software, protocolos y hardware han llevado a las redes de telecomunicaciones a nuevos niveles de rendimiento, mientras atacan costos agresivamente [Croll, 2000] Actualmente existen enlaces de telecomunicaciones más rápidos por solo una fracción de lo que, enlaces más lentos, costaban hace diez años. El ancho de banda es un recurso que debe ser medido como cualquier otro recurso para lograr su utilización óptima, porque tiene un costo y nunca será demasiado barato para desperdiciarlo.

Para poder lograr un uso eficiente del ancho de banda, es necesario implementar algún tipo de control para que las aplicaciones de los usuarios de una red no consuman demasiados recursos de la misma para fines que no son prioritarios o simplemente para dar prioridad a ciertos flujos de información que lo requieren como aplicaciones multimedia en tiempo real.

Calidad de servicio o QoS por sus siglas en inglés, puede ser implementada en diferentes maneras, una de ellas es sobre el protocolo de Internet IP, aunque es más comúnmente conocido como TCP/IP. También existe una especificación para implementar el concepto de calidad de servicio en un nivel más bajo de capa de red, en el nivel de enlace con la tecnología de ATM, del cual se deriva una variante que también es capaz de hacer diferenciación de flujos en MPLS. Se menciona también como el protocolo de administración de redes SNMP puede ser usado para proveer información para calidad de servicio.

La manera más simple de implementar una forma de calidad de servicio es diferenciando el tráfico en clases de servicio, definido solamente en el encabezado del paquete de información. Para implementar Calidad de Servicio de una manera más completa se requieren algunas modificaciones extras que pueden incluir el agregar hardware o software en los componentes de la red.

Podemos tener tres tipos de servicio en las redes de telecomunicaciones, el de mejor esfuerzo en el cual se tratan todos los paquetes de información de manera igual. El servicio diferenciado en el que se da prioridad a algún tipo de tráfico, pero todos se transportan con el mismo ancho de banda. Y el de servicio garantizado donde se reserva una cierta cantidad del ancho de banda total para un flujo específico prioritario.

El monitoreo de estos niveles de servicio es importante para verificar que la red se está comportando como se espera, hay diferentes tipos de monitoreo, desde las herramientas comunes de Internet hasta aplicaciones especializadas.

1.1 Justificación

Vivimos en una etapa de globalización económica, con la tendencia creciente del uso de redes de telecomunicaciones para comercio electrónico, tele conferencias, audio y video en tiempo real, telefonía, correo electrónico, datos entre los sistemas de procesamiento e Internet. Los cuales han convergido en redes digitales debido a las ventajas que brindan en rapidez de transferencia y confiabilidad. Estas redes de telecomunicaciones se han convertido en parte fundamental de nuestras vidas, ya sea directa o indirectamente, debido a que las compañías que nos proveen los productos o servicios que necesitamos no podrían trabajar de sin estos servicios. También existen diversas organizaciones como Gobiernos e Instituciones Educativas, entre otros, que hacen un uso extensivo de estas redes para sus actividades diarias.

Las redes IP han tomado ventaja sobre otras tecnologías de red, por lo que se han desarrollado especificaciones para implementar calidad de servicio en este tipo de redes.

La Calidad de Servicio o "QoS" por sus siglas en inglés, juega un rol muy importante, en especial para las aplicaciones críticas como voz y video en tiempo real, telefonía IP, videoconferencia, audio y video en demanda, ya que representan grandes ahorros al no tener que usar la red de telefonía pública para comunicarse o al evitar un viaje al hacer una junta por tele conferencia.

1.2 Objetivo

Proporcionar una guía a los administradores de redes de telecomunicaciones empresariales o universitarias, sobre los conceptos, las tecnologías que existen y las que están en desarrollo y los equipos para implementar Calidad de Servicio (QoS), para que de esta manera puedan determinar los requerimientos que deben cubrir en su red propietaria y las exigencias que se deben tener con los proveedores de telecomunicaciones y así asegurar la calidad de servicio que requieren las aplicaciones de los usuarios de su red.

1.3 Contribución

Al término de la presente tesis, se presentará un análisis de los diferentes escenarios donde intervienen las redes de telecomunicaciones y se puede implementar QoS, así como las tecnologías que son las más apropiadas y el costo de implementar dichas tecnologías. Puede ser posible que la mejor tecnología tenga un costo prohibitivo y dependiendo de las necesidades del administrador de redes se hará una recomendación de cuál es la más factible según sea el caso.

Con este análisis se pretende hacer también, una integración de información sobre los conceptos de QoS, las tecnologías que se usan y las que están en desarrollo, con el fin de ampliar el entendimiento del concepto desde un punto de vista neutral. Porque en el desarrollo de la tesis, encontré información en Internet, libros y revistas con tendencias hacia el tema del libro o de la revista y manejan su punto de vista como verdad absoluta, lo cual genera que la información existente esté muy dispersa y se obtenga una visión muy limitada.

Con esta integración de información, orientar a los administradores de redes de telecomunicaciones para que seleccionen la tecnología y pongan en operación la metodología más adecuada a sus necesidades y puedan tener las métricas necesarias para poder contratar y exigir una determinada calidad de servicio en la red de un proveedor de telecomunicaciones a través de un acuerdo de nivel de servicio.

También se pretende aclarar la responsabilidad que tiene tanto el administrador de la red como el proveedor de telecomunicaciones, ya que usualmente se culpa al proveedor cuando hay algún problema de calidad de servicio, siendo que también puede deberse a un problema en la red propietaria.

La Calidad de Servicio es un concepto que no siempre se considera al momento de planear y construir la infraestructura de una red nueva o al crecer una red existente.

1.4 Producto Final

El documento que se genere de esta tesis, se podrá usar como referencia para que los administradores de redes obtengan un panorama más amplio sobre Calidad de Servicio en redes de telecomunicaciones y puedan determinar los requerimientos para implementarla en su red. De esta manera, se defina la infraestructura necesaria para conformar una red que se comporte de acuerdo a las necesidades que tienen sus aplicaciones, sobre todo las críticas. Basándose en definición de políticas de tráfico, parámetros que se deben medir para configurar los enrutadores, conmutadores (switches) y administradores de ancho de banda. También deberá servir como guía para determinar los puntos que se deben tomar en cuenta al momento de diseñar una red local (LAN), una metropolitana (MAN) o de área amplia (WAN).

2. INTRODUCCIÓN A TCP/IP, ATM, MPLS Y SNMP

El objetivo de este capítulo, es ubicar al lector acerca de donde se encuentran o pueden aplicar los conceptos de Calidad de Servicio (QoS) dentro de las tecnologías de red que más se usan actualmente. Al tener una visión general de estos conceptos, será más fácil entender los nuevos conceptos que se incluyen en capítulos posteriores. La estructura de este capítulo se inicia con la descripción de la arquitectura TCP/IP debido a que es la base de Internet y sirve para entender como interactúan los diversos protocolos donde el principal es IP. La especificación de este protocolo contiene parámetros donde se puede especificar Calidad de Servicio. También es posible definir calidad de servicio con parámetros propios de la señalización de red como en el caso de ATM. Finalmente se menciona MPLS donde también se puede clasificar la información en clases para darle prioridad a alguna que sea de interés en redes WAN.

2.1 Arquitectura TCP/IP

El conjunto de protocolos TCP/IP se refiere a los dos protocolos conocidos como Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP), también intervienen otros, como el Protocolo de Datagramas de Usuario (UDP), el Protocolo de Control de Mensajes de Internet (ICMP) y las aplicaciones básicas como HTTP, TELNET y FTP. [León García, 2000]

La estructura básica de TCP/IP se muestra en la figura 2.1

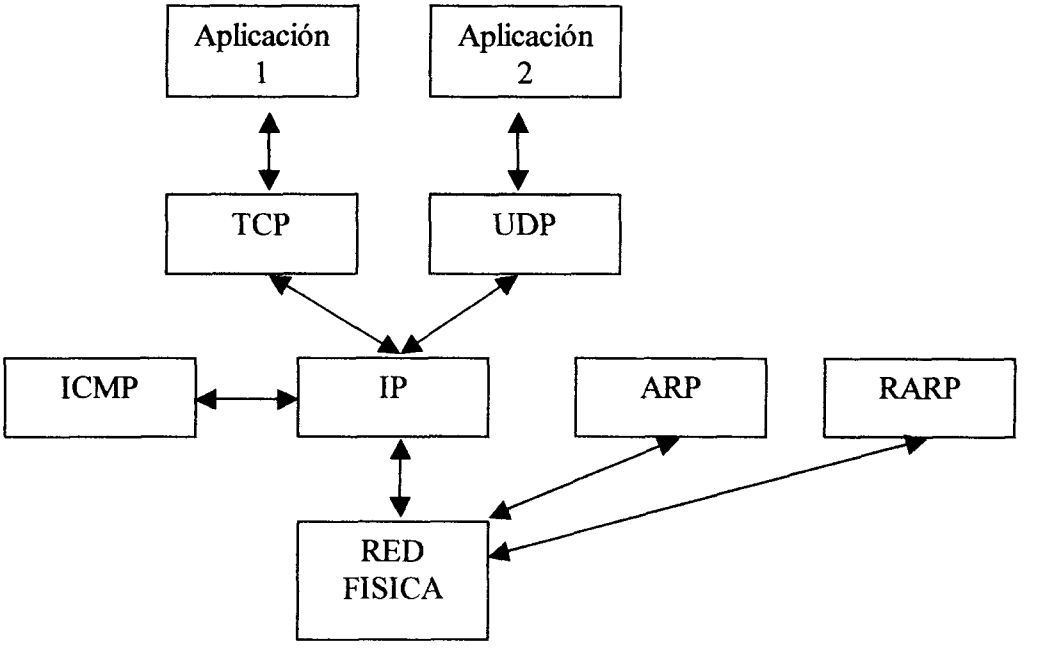


Figura 2.1 Conjunto de protocolos TCP/IP

Las aplicaciones son los programas que usamos que requieren servicios de la red Internet. Los protocolos de nivel de aplicación como HTTP y FTP envían mensajes usando TCP, mientras que SNMP y DNS envían sus mensajes usando UDP. [León García, 2000]

IP multiplexa segmentos de TCP y datagramas de UDP, realiza fragmentación de la información en caso de ser necesario. Las unidades de datos intercambiados por los protocolos IP se llaman paquetes IP o se conocen también como paquetes. Estos se transportan a la interfase de red para su envío a través de la red física.

En el lado del receptor, los paquetes entran por la interfase de red, y son demultiplexados al protocolo apropiado (IP, ARP o RARP) Entonces la entidad IP determina si un paquete debe ser enviado a TCP o UDP. Finalmente TCP o UDP envían cada segmento o datagrama a la aplicación apropiada basado en el número de puerto. [León García, 2000]

La red física puede ser implementada usando alguna de las tecnologías como Ethernet, Token Ring, ATM o PPP, sobre varios medios de transmisión como fibra óptica, cable o medios inalámbricos.

En esta arquitectura compuesta de varias capas, una capa le da servicio a la capa superior, siendo la aplicación que está corriendo en un sistema la última capa que se conoce como capa de aplicación.

Si una aplicación determinada necesita enviar un mensaje a otro equipo anfitrión (host), por ejemplo una petición para recibir una página WEB, se procede con el siguiente procedimiento: Para cuestiones prácticas vamos a definir el host que envía como host1, y el que recibe como host2.

- La aplicación en el host1 envía un mensaje a la capa que esta debajo de esta, la capa de transporte recibe el mensaje.
- En la capa de transporte, se agrega el encabezado de TCP, que se encarga de enviar el número de puerto que esta usando la aplicación, aparte de mandar retransmisiones de partes de la información en caso que un paquete haya sido descartado en el camino hacia host2 y hace la fragmentación de mensajes cuando transmite y el reensamble cuando recibe. La capa de Internet recibe el mensaje.
- En la capa de Internet, se tiene una dirección única para host1 y también para host2. Esta dirección es lógica, y se comentará a detalle más adelante. Esta dirección la usan los enrutadores para transferir información a través de múltiples redes.
- En la capa de Red o enlace físico se transmiten los bits, solo se tiene la dirección de las tarjetas de interfase de red (NIC) que mantienen la conexión física de la red. Esta información cambia cuando sale de un enrutador según se trate del puerto de salida en cuestión.

Las unidades de datos de programa o PDU de una capa se encapsula dentro del PDU de la capa que está debajo, como se muestra en la figura 2.2. [León García, 2000]

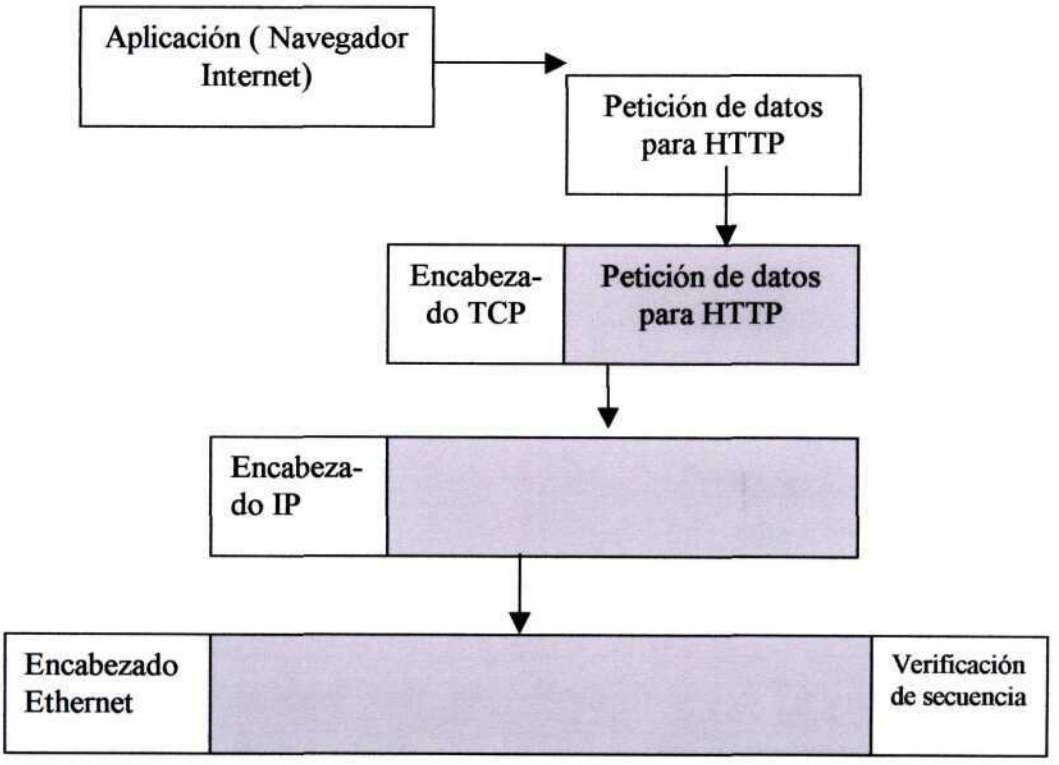


Figura 2.2 Encapsulamiento de PDU en TCP/IP

Encabezado TCP: Esta es la capa de **Transporte**, contiene los números de puerto fuente y destino.

Encabezado IP: Esta es la capa de **Internet**, contiene las direcciones IP fuente y destino, tipo de control de transporte.

Encabezado Ethernet: Esta es la capa de **Interfase de Red**, contiene dirección física de la fuente y destino, tipo de control de red.

Una vez que llega el mensaje, se repite el proceso inversamente en el lado del receptor, como se muestra en la figura 2.3

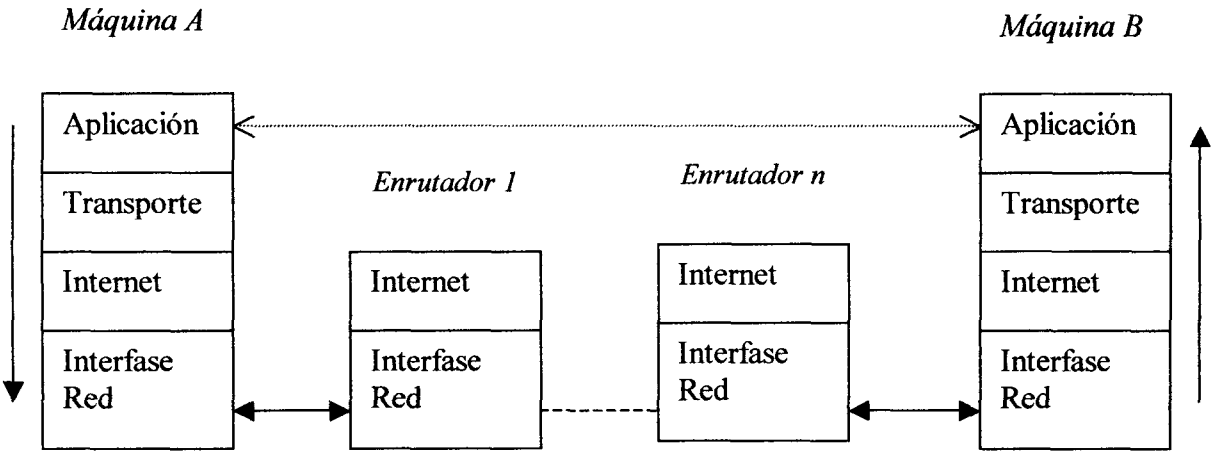


Figura 2.3 Capas de Internet e interfase de red

2.2 IP (Internet Protocol)

El Internet actual tiene sus orígenes en ARPANET, era una red de datos experimental fundada por la (U.S. Defense Advanced Research Projects Agency) o Agencia de Proyectos Avanzados de Investigación de Defensa (DARPA) de los Estados Unidos, en los años sesentas. Una meta importante era construir una red robusta que pudiera sobrevivir ataques militares como un bombardeo. Para lograr esto la ARPANET fue construida sobre el modelo de datagramas donde cada paquete se envía independientemente a su destino. [Wang, 2001]

Dentro de todo el sistema de la red, el protocolo IP es el que tiene el poder de definir que se de un trato diferente a un paquete. Se profundizará en este protocolo debido a que nos permitirá desarrollar el concepto de calidad de servicio (QoS)

El Protocolo de Internet (IP), habilita comunicaciones a través de una colección vasta y heterogénea de redes que están basadas en diferentes tecnologías. Cualquier computadora host que está conectada al Internet se puede comunicar con cualquier otra computadora host que también esté conectada al Internet. Por lo tanto el Internet ofrece conectividad ubicua y las economías de escala que resultan de implementaciones grandes. [León García, 2000]

El protocolo de Internet (IP) es el corazón del conjunto de protocolos TCP/IP. IP corresponde a la capa de red en el modelo OSI y provee transferencias de información no orientados a conexión. [León García, 2000] Una transferencia no orientada a conexión significa que no se tiene que establecer previamente un enlace de comunicación para poder transmitir la información, como en el caso de una llamada telefónica por ejemplo. Simplemente se transmite el paquete por el medio físico de red al que se está conectado y la información del destino al que llegará el paquete está contenida en el encabezado del mismo.

Este tipo de conexiones permite que llegue la información de un extremo al otro sin que estén conectados directamente.

Este tipo de redes se interconecta por medio de conmutadores (switches) de paquetes especiales llamados enrutadores. Al usar transferencias no orientadas a conexión, no es necesario que los enrutadores mantengan ninguna información en particular de un usuario en específico o de los flujos de paquetes, lo que permite que IP pueda operar en redes muy grandes. También se tiene la ventaja que se forma un sistema robusto, ya que se puede rutear el tráfico por una trayectoria diferente en caso de que falle algún elemento de la red.

Los enrutadores de IP se encargan de la transferencia de paquetes en una red IP. Una vez que se ha definido la dirección de ruteo, los paquetes se ponen en un búfer de espera para ser transmitidos hacia la próxima red, los paquetes de diferentes usuarios son multiplexados estadísticamente en estos búferes y la red siguiente es la responsable de retransmitir los paquetes hasta que lleguen a su destino.

El Internet ofrece dos servicios básicos de comunicación que operan sobre IP: El Protocolo de Control de Transmisión (TCP) y Protocolo de Datagramas de Usuario (UDP) Cualquier protocolo de aplicación que opera sobre TCP o UDP, opera automáticamente a través de la Internet. [León García, 2000]

IP hace su mejor esfuerzo para entregar los paquetes en su destino, pero no hace ninguna acción adicional cuando los paquetes se pierden o si llegan fuera de orden debido a que tomaron trayectorias diferentes, en este sentido el servicio provisto por IP no es confiable. El diseño de IP intenta mantener la operación de una Internet simple relegando funciones complejas a otros niveles de la red. Cuando se tiene congestión en la entrada de un enrutador, los paquetes se descartan, pero los mecanismos de punto a punto (TCP) de los extremos de la red permiten que se pida una retransmisión de lo que se perdió.

La transferencia de bloques individuales de información usando datagramas puede soportar muchas aplicaciones, pero requieren que se tenga una transferencia confiable de información con el arribo en secuencia correcta. El protocolo de control de transmisión (Transmission Control Protocol) TCP, provee una transferencia confiable sobre el protocolo no orientado a conexión IP. TCP provee control de flujo de punto a punto y resuelve los problemas que se pueden presentar por pérdida o retraso de paquetes. También incluye un mecanismo para reducir la tasa de transferencia cuando se detecta congestión en la red.

El IP que usamos actualmente en la Internet es el IPv4, aunque es un protocolo robusto, ha sido necesario hacer modificaciones a su definición, debido principalmente al espacio reducido de direcciones con el que fue concebido, esto se debe a que inicialmente IP era usado en principalmente en universidades, por lo que no se necesitaba un espacio de direcciones muy grandes ni aspectos de seguridad, tampoco se consideraron seriamente aspectos de Calidad de Servicio (QoS) Con el gran crecimiento de los servidores de Internet para fines comerciales y de usuarios donde cada uno necesita una dirección diferente, se desarrolló IPv6. Estas dos variantes se describen a detalle a continuación:

2.2.1 IPv4

IPv4 se conoce simplemente como IP, las direcciones IP consisten en cuatro bits expresados en notación decimal con puntos, por ejemplo 132.254.100.1. Tiene una longitud fija de 32 bits. La estructura fue definida originalmente para tener dos niveles de jerarquía, Identificador de red y de host. El Identificador de Red, es común para todos los host que estén conectados al mismo segmento de red. El Identificador de host identifica la conexión de red. [León García, 2000] Con este esquema, un enrutador puede enviar un paquete basado únicamente en el Identificador de red, lo que hace que se requiera menos procesamiento en el enrutador y por lo tanto se hace más rápido en envío.

Estas direcciones también pueden ser traducidas para que tengan un nombre, que se refiere al host en especifico que da un servicio en Internet, como www.mty.itesm.mx, la cual requiere de una traducción automática que es provista por un servidor de nombres de dominio (Domain Name Server DNS),

La estructura de direcciones IP está dividida en cinco clases: Clase A, Clase B, Clase C, Clase D, Clase E, identificados por los bits más significativos de la dirección. La clase A, tiene 7 bits para red y 24 bits para identificar el host, por lo que se pueden tener 126 redes y 16 millones de hosts por red. La clase B, tiene 14 bits para red y 16 bits para host, por lo que pueden tener hasta 16000 redes y 64000 hosts por red. La clase C, tiene 21 bits por red y 8 bits por host, por lo que puede tener 2 millones de redes y 254 hosts por red. Las direcciones de clase D, están reservadas para servicios de transmisión múltiple que permite enviar información a un grupo de hosts simultáneamente. Las de clase E, están reservadas para experimentos. El Identificador (ID) de red es asignada por la Internet Network Information Center (InterNIC) El Identificador del host es asignado por el administrador de la red del sitio local.

Debido a que la conmutación de paquetes no es orientada a conexión, se debe tener un encabezado de información para poder transferir el paquete a su destino. Como se muestra en la figura 2.4. El enrutador procesa cada paquete para decidir por cual puerto del mismo enrutador deberá salir el paquete. Este procesamiento induce retardos en la retransmisión de los paquetes de información, lo que representa el principal problema para que aplicaciones de tiempo real que requieren poco retraso sean implementadas sobre Internet.

Cuando un paquete IP entra a una interfase o puerto del enrutador, se hace el siguiente procesamiento:

1. Se verifica la suma de chequeo (checksum) del encabezado y se verifica que los datos del encabezado contengan valores válidos.
2. Los campos de IP se actualizan. Se cambia la suma de chequeo (checksum) del encabezado
3. Se identifica el camino o dirección de la próxima red por el que saldrá el paquete, para hacer esto consulta en sus tablas de ruteo.
4. Se reenvía el paquete a la próxima red.

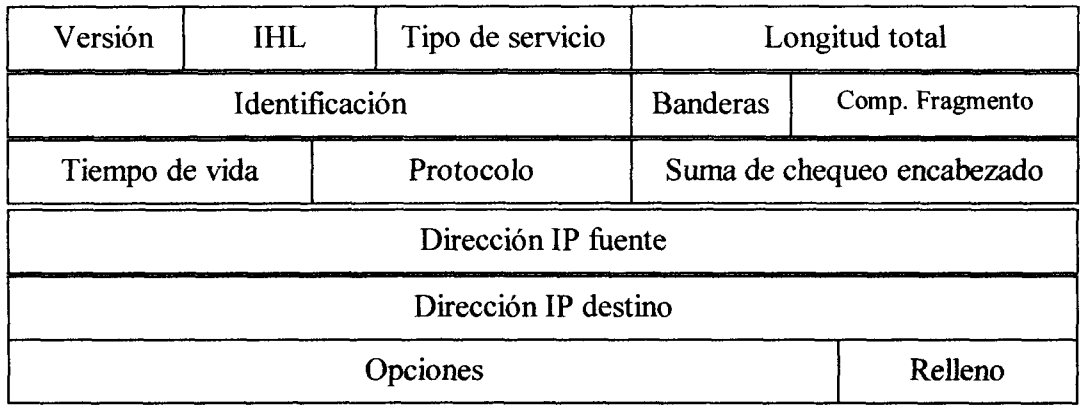


Figura 2.4 Encabezado de IP versión 4

Versión: este campo contiene la versión de IP que usa el paquete. La versión por defecto (default) es 4. La versión 5 se usa para el protocolo de tiempo real en flujo (stream) llamado ST2, la versión 6 se usa para la nueva generación de IP conocida como IPng o IPv6.

Longitud de encabezado IHL (Internet Header Length): especifica la longitud del encabezado en palabras de 32 bits, si no hay opciones presentes, se usa por defecto un valor de 5.

Tipo de servicio (Type of Service TOS): Este campo especifica la prioridad del paquete basado en requerimientos de retraso, velocidad de travesía (throughput), confiabilidad y costo. Se asignan 3 bits para niveles de prioridad también conocidos como precedencia y cuatro bits para el requerimiento específico. Trabajos recientes en el grupo de trabajo de servicio diferenciado de la IETF tratan de redefinir el campo TOS para dar soporte a otro tipo de servicios.

Longitud Total: Especifica el número de bytes del paquete IP, incluyendo el encabezado y los datos. Con 16 bits asignados a este campo, la longitud máxima del paquete es de 65535 bytes, pero en la práctica, la longitud máxima se usa en raras ocasiones, porque las redes físicas tienen su propia limitación de longitud, como Ethernet que limita la longitud a 1500 bytes.

Identificación, Banderas y Compensación (Offset) de fragmentación: Estos campos se usan para fragmentación y reensamble.

Tiempo de vida: Este campo es definido para indicar la cantidad de tiempo en segundos que se le permite al paquete permanecer en la red, algunos enrutadores interpretan este campo como el número de brincos (hops) que se le permite atravesar al paquete, originalmente el host fuente pone un valor en este campo, y cuando viaja el paquete a través de los enrutadores, estos disminuyen el valor de este campo en uno, si el campo tiene el valor de cero y no ha llegado a su destino, se descarta el paquete y se regresa un mensaje de error, esto evita que los paquetes anden vagando sin limite por Internet.

Protocolo: Este campo especifica el protocolo para los datos que recibirá el host destino, pueden ser TCP(6), UDP(17) e ICMP (1)

Suma de chequeo de encabezado: Este campo verifica la integridad del encabezado del paquete IP. Los datos no se verifican y de deja esta tarea para protocolos de capas superiores. Si falla la verificación, el paquete de descarta.

Dirección IP fuente y destino: Estos campos contienen la dirección de los host fuente y destino.

Opciones: El campo de opciones que es de longitud variable, le permite a un paquete pedir características especiales como nivel de seguridad, usar alguna ruta o trayectoria específica a seguir, o la marca de tiempo de cada enrutador por el que pasa. Esta opción es raramente usada, se usa por RSVP que se detalla posteriormente.

Relleno (Padding): Este campo se usa para hacer el encabezado un múltiplo de palabras de 32 bits.

2.2.2 IPv6

La IETF (Internet Engineering Task Force) empezó en la década de los 90's a desarrollar el sucesor del protocolo IPv4. El nuevo protocolo fue diseñado para ser capaz de operar con el anterior, porque pasarán muchos años antes que de deje de usar IPv4, algunos de los cambios que se tienen de IPv4 a IPv6 son las siguientes:

1. Campos de direcciones más grandes: La longitud de las direcciones se extiende de 32 bits a 128 bits, esta estructura provee más niveles de jerarquía, que en teoría puede dar soporte a 3.4×10^{38} hosts.
2. Formato de encabezado simplificado: Algunos campos de IPv4 como el de suma de verificación (checksum), IHL, banderas de identificación y compensación (offset) de fragmentación no aparecen en IPv6.
3. Soporte flexible para opciones: Las opciones en IPv6 aparecen en encabezados opcionales de extensión, que se codifican de una manera más eficiente.
4. Capacidad de etiquetas de flujo: IPv6 agrega etiquetas de flujo para identificar un cierto flujo de paquete que requiera Calidad de Servicio (QoS)
5. Seguridad: IPv6 tiene soporte para cargas (payloads) mayores de 64kbps, que se conocen como jumbo payloads.
6. Fragmentación sólo en la fuente: No se permite a los enrutadores fragmentar paquetes. Si un paquete necesita ser fragmentado, debe ser desde el host que lo transmite.
7. Campo de suma de chequeo (checksum): IPv6 no tiene campo de suma de chequeo, este puede ser removido para reducir el tiempo de procesamiento en un enrutador,

los paquetes que se transportan por una red física como Ethernet, Token Ring, X.25 o ATM ya tienen su propio checksum. Y en la capa superior, ya sea TCP o UDP tienen su propia verificación.

El formato del encabezado IPv6 se muestra en la figura 2.5

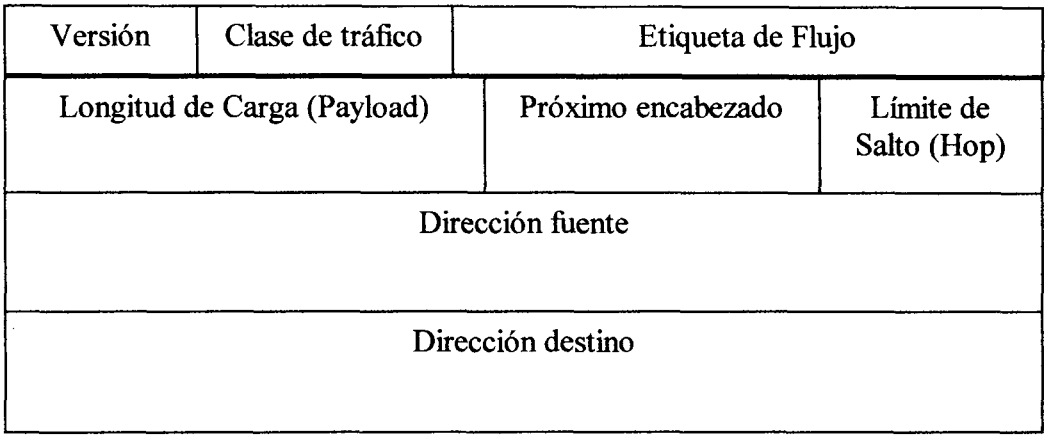


Figura 2.5 Encabezado básico IPv6

Versión: El campo de versión especifica el número de versión del protocolo, debe ser 6 para IPv6, el lugar y tamaño del campo no debe cambiar para que el software del protocolo lo reconozca rápidamente.

Clase de tráfico: Este campo especifica la clase de tráfico o prioridad del paquete, la intención de este es para dar soporte a tráfico diferenciado.

Etiqueta de Flujo: Este campo puede identificar la calidad de servicio requerida por el paquete, una aplicación que puede requerir esta etiqueta es un paquete de video que requiere que se entreguen los paquetes dentro de una restricción de tiempo.

Longitud de Carga (Payload): Este campo indica la longitud de datos sin incluir el encabezado. El campo es de 16 bits por lo que el payload esta limitado a 65535 bytes. Es posible mandar payloads mayores usando la opción en el encabezado de extensión.

Próximo encabezado: Este campo identifica el tipo de encabezado de extensión que sigue el encabezado básico, el encabezado de extensión es similar al campo de opciones en IPv4, pero es más flexible y eficiente.

Limite de salto (hop): este campo reemplaza el campo de tiempo de vida en IPv4, este valor especifica el número de saltos que tiene permitido viajar el paquete antes de ser descartado por un enrutador.

Dirección fuente y destino: estas direcciones identifican el host fuente de la información y el host destino a donde debe ser enviada. La dirección es de 128 bits, lo que incrementa de alguna manera el tráfico, pero con este espacio de direccionamiento, se tendrán direcciones suficientes por algunos años más.

Estas direcciones se dividen en 3 categorías:

1. "Unicast": direcciones que identifican una interfase de red sencilla
2. "Multicast": identifican un grupo de interfaces de red, típicamente en diferentes locaciones. Un paquete se envía a todas las interfaces de red del grupo.
3. "Anycast": estas direcciones también identifican un grupo de interfaces de red, pero solo se envía a una interfase en el grupo, usualmente a la más cercana.

Las direcciones IPv6 se expresan en notación hexadecimal para separar cada 16 bits con puntos dobles, por ejemplo 4BF5:AA12:0216:FEBC:BA5F:039B:BE9A:2176, pero pueden ser compactadas a una forma más corta.

El problema con IPv6 es que no es directamente compatible con IPv4, un nodo que solo maneja IPv4, no puede recibir un paquete nativo de IPv6, el cual requiere que el host que recibe el paquete tenga una actualización del software para manejar el nuevo protocolo.

Un error común es la creencia que no se podrán manejar paquetes IPv6 hasta que la infraestructura del trayecto de un paquete sea actualizada desde el origen hasta el destino, lo que incluye desde la intranet local, el Internet desde el proveedor local o ISP, la columna vertebral (backbone) de transmisión, el IP destino hasta la Intranet del destino. El diseño de IPv6 asegura que trabajará a pesar de que algún punto intermedio de transporte no soporte el reenvío de paquetes nativos IPv6. Como se mencionó anteriormente, no es directamente compatible, pero si se pueden transportar los paquetes encapsulado IPv6 en IPv4.

IPv6 trata a IPv4 como si fuera una capa de enlace, los paquetes IPv6 se encapsulan con un encabezado de IPv4 y se envían en el enlace que soporta IPv4. Hay varias tecnologías de transición para facilitar la comunicación de nodos IPv6/IPv4 en una infraestructura IPv4. Incluyendo 6 a 4 y el protocolo de direccionamiento túnel automático intra sitio. (ISATAP Intra Site Automatic Tunnel Addressing Protocol)

2.2.3 6to4

6to4 usa una dirección publica de IPv4 para crear el Identificador de sub-red de 64 bits, ISATAP usa una dirección IPv4 asignada localmente ya sea publica o privada para crear el Identificador de interfase de 64 bits. 6to4 es un encapsulamiento o técnica de direccionamiento que se describe en el RFC 3056, los host 6to4 no requieren ninguna configuración manual para crear direcciones 6to4, porque lo manejan los mecanismos de auto configuración estándar. Los enrutadores 6to4 requieren procesamiento adicional para encapsulamiento y decapsulamiento y dependiendo de la implementación, puede requerir configuración adicional.

2.3 ATM

ATM (Asynchronous Transfer Mode) es la única tecnología que permite el transporte de datos a 155Mbps, por esta razón, ha tenido éxito como pieza fundamental para formar la espina dorsal (backbone) de Internet. Aparte de tener una alta capacidad de transferencia de datos, también provee un complejo subconjunto de mecanismos de

administración de tráfico, controles para establecer circuitos virtuales (VC) y parámetros de calidad de servicio (QoS) Aunque algunas compañías sólo usan ATM como un mecanismo de transporte para Internet en redes de área amplia (WAN) sin aprovechar todos los atributos que ofrece la tecnología.

El origen de ATM proviene del concepto de multiplexar en tiempo diferentes tipos de datos, como textos y voz en una sola cadena de datos que viaja en un solo circuito físico y demultiplexar la cadena de datos en el extremo receptor, para volver a separar los datos como estaban originalmente. Este método sigue siendo económico y atractivo porque evita el tener que comprar circuitos individuales para cada aplicación. En el tiempo en el que se formuló ATM, el multiplexeo de paquetes era lento y requería procesamiento intensivo, de cualquier manera el desarrollo de técnicas de hardware han reducido los tiempos de procesamiento y han logrado que los paquetes de longitud variable sean viables.

El propósito de ATM es proveer un ambiente de multiplexeo y conmutación de alta velocidad, bajo retraso y baja diferencia de retrasos (jitter), que pueda dar soporte a cualquier tipo de tráfico como voz, datos o video.

ATM segmenta y multiplexea los datos del usuario en celdas de 53 bytes, cada una se identifica con identificadotes de VC y VP (VCI y VPI) las cuales indican como debe ser conmutada la celda desde el origen hasta el destino en la red ATM. Las celdas se reenvían por conmutadores ATM que tienen una tabla de búsqueda en el VCI para determinar el próximo puerto de salida y el VCI en el próximo enlace. Las redes ATM proveen transferencia de información orientada a conexión.

Debido a que se basa en paquetes de longitud fija, ATM puede manejar fácilmente servicios que generan información de manera de ráfaga o en tasas variables. El encabezado abreviado de ATM y la longitud fija de los paquetes, facilita la implementación en hardware que resulta en bajo retraso y altas velocidades.

ATM asume que hay una tasa de errores baja, por lo que el control de errores se hace en los extremos. La fase de configuración de conexión precede la transferencia de información, durante esta negociación se define el tipo de flujo que se va a ofrecer en la red, y la red se compromete a un cierto nivel de calidad d servicio que se proveerá al flujo de datos. También en esta fase, se define un camino a través de la red para reservar los recursos adecuados a lo largo del camino.

2.3.1 Conmutación (Switch) ATM

En la década de 1990, ATM fue una alternativa para el multiplexeo tradicional. En ATM se introduce el concepto de Circuitos Virtuales (VCs) y Trayectorias Virtuales (Virtual Paths) que se manejaban en Frame Relay, que ahora podían ser usados para múltiples fuentes de datos. Varios circuitos virtuales (VC) pueden ser transportados en una sola trayectoria virtual (VP) y varios VPs pueden ser transportados en un solo circuito físico. El tráfico es conmutado de punto a punto, desde el origen hasta el destino y cada VC o VP puede ser mapeado a una trayectoria específica a través de la red ya sea de manera estadística o dinámica con un protocolo de ruteo que sirve para determinar la mejor trayectoria desde un punto de la red ATM hasta el siguiente. ATM combina varias

características deseables de conmutación de paquetes y multiplexeo por división de tiempo (TDM), las cuales se dividen en cuatro criterios de comparación como lo podemos apreciar en la tabla 2.1

Criterio	TDM (Time división multiplexing) (Conmutación de circuitos)	Multiplexeo de Paquetes (Conmutación de paquetes)
1.Capacidad de apoyar servicios que generan información a una tasa variable.	Tienen dificultad para dar soporte a tasas de transferencias variable, porque estos sistemas transfieren información a una tasa constante, las tasas que puede dar soporte son múltiplas de alguna tasa básica como por ejemplo los 64kbps de las redes telefónicas	Fácilmente maneja tasas de transferencia variables, porque la información generada por el servicio es simplemente insertada en los paquetes, pueden ser acomodados fácilmente cuando los paquetes no generen datos a una tasa que exceda la velocidad de la línea de transmisión
2. Retraso que se requiere para atravesar la red	Una vez que se establece una conexión, los retrasos son pequeños y constantes.	Tiene retrasos de transferencia variables, porque requiere uso de filas de espera en los multiplexores, también tiene dificultad para proveer servicios particulares con poco retraso, por ejemplo cuando los paquetes tienen longitud variable, o cuando un paquete esta en transmisión, los demás paquetes, incluyendo a los urgentes deben esperar durante la duración de la transmisión.
3. Capacidad de soportar tráfico de ráfaga	Dedica recursos de transmisión que se conocen como ranuras a una conexión. Si ésta genera información en ráfaga, entonces muchos de las ranuras dedicadas se quedan sin uso, por lo que TDM no es eficiente para servicios que generan información en ráfagas.	Fue desarrollado para manejar tráfico de ráfaga de una manera eficiente.

4. Procesamiento	Maneja las ranuras de transferencia en hardware, por lo que el procesamiento es mínimo y puede ser hecho a alta velocidad	Tradicionalmente utiliza software para procesar la información de los encabezados de los paquetes

Tabla 2.1 Multiplexeo por división de tiempo (TDM) vs. Multiplexeo de paquetes

2.4 MPLS (Conmutación de Etiquetas con Múltiple Protocolo)

MPLS fue visto originalmente como una alternativa para dar soporte a IP sobre redes ATM. Algunas otras técnicas fueron estandarizadas, pero son complejas y tienen problemas de escalamiento. [Wang, 2001]

El documento de la IETF [Guerin, 1997] describe MPLS como una tecnología base de intercambio de etiquetas (label swapping) la cual se espera que mejore el precio y rendimiento de la capa de ruteo de red, mejore la escalabilidad de la capa de red y proporcione flexibilidad en el envío de nuevos servicios de ruteo al permitir que sean implementados sin un cambio en el paradigma de transporte (forwarding).

La necesidad de una integración IP / ATM llevó al desarrollo de MPLS en 1997. Esta integración permite que los protocolos de ruteo tomen control directo sobre los conmutadores ATM y por lo tanto el control de IP puede ser fuertemente estrechado con el resto de la red IP. [Wang, 2001]

MPLS usa conmutación de etiquetas para hacer circuitos virtuales en redes basadas en IP. Estos circuitos virtuales pueden seguir ruteo IP basado en destino, pero el mecanismo explícito en MPLS también se usa para especificar salto por salto la trayectoria entera de estos circuitos virtuales. El concepto de intercambio de etiquetas reemplaza la necesidad de hacer la correspondencia larga, por lo que se inserta una etiqueta de longitud fija entre el encabezado de la capa de red (Capa 3) y el encabezado de la capa de enlace (capa 2), como se muestra en la figura 6.1, la cual puede ser usada para hacer decisiones de ruteo que toman menos tiempo.

El término de conmutación de etiquetas (label switching) o intercambio de etiquetas (label swapping) se refiere a los mecanismos que se usan para el ruteo de paquetes en un enrutador. Actualmente se usa el método de correspondencia larga (longest match) cuando un enrutador hace referencia a una tabla de ruteo de longitud variable y guarda en la tabla el prefijo más largo o el más específico para subsecuentes transportes a la red que contiene esa dirección. Aunque parece que esto no tiene importancia, si tiene un alto costo en cuanto a procesamiento requerido que se traduce en tiempo y retraso para los paquetes a ser transportados.

Uno de los resultados esperados del intercambio de etiquetas es reducir el tiempo y recursos computacionales requeridos para hacer cálculos de las decisiones de ruteo, dado que el número de trayectorias siempre es menor que el número de prefijos de direcciones.

El intento es reducir las decisiones de conmutación en una configuración con "*n*" nodos a un cálculo de "*n*" veces el número de prefijos únicos, dentro de un espacio que puede llegar a *n!* sin las etiquetas.

A diferencia de una dirección IP que identifica un host específico o enrutador, una etiqueta identifica un circuito virtual entre dos enrutadores de conmutación de etiquetas (LSR Label switching routers) vecinos, y el significado de la etiqueta es significativo solo entre los dos vecinos. Una secuencia de LSR que seguirá un paquete se llama trayectoria conmutada de etiquetas (label switched path LSP), el cual es análogo a un canal virtual en ATM, con la diferencia que LSP es unidireccional. [León-García, 2000]

Aparte de integrar IP / ATM, MPLS puede ser usado para simplificar el envío de paquetes. La búsqueda de la etiqueta es mucho más fácil comparada con la búsqueda del prefijo en el reenvío de IP. Con MPLS el reenvío de paquetes puede hacerse independientemente de los protocolos de red.

Para sistemas cerrados, en el que el número de trayectorias de punto a punto es reducido, se tienen valores de "n" muy pequeños, esta técnica de etiquetado puede facilitar un proceso de transporte altamente eficiente dentro de un enrutador.

MPLS se conoce también como la capa de red 2.5, porque no reemplaza la capa 3, ni la capa 2, pero se inserta el algún punto entre las dos capas. La capa de red puede ser cualquiera de los protocolos que se usan actualmente, como IP, IPX, AppleTalk, etc. Por esta razón se conoce MPLS como de protocolos múltiples. MPLS puede ser implementado nativamente en el hardware de conmutación de ATM, donde las etiquetas son sustituidas y situadas en los identificadores de trayectorias virtuales (VP) o circuitos virtuales (VC).

Estas etiquetas son distribuidas por el protocolo de distribución dinámico y están delimitadas a un conjunto de prefijos. Un enrutador que tiene interfaces conectadas con otro que no maneja MPLS, el nodo que si tiene MPLS cambia la información de ruteo, la asocia localmente e inserta prefijos aprendidos vía capa 3.

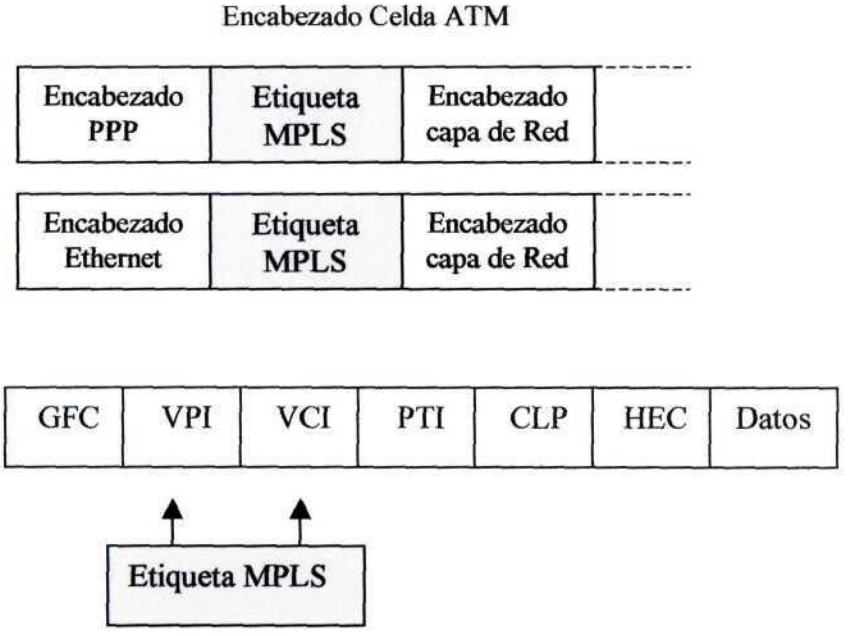


Figura 2.6 Insertando etiqueta MPLS

2.5 SNMP

Fue diseñado como una herramienta para poder medir y controlar el rendimiento de algunos dispositivos que conforman una red especifica. Sin embargo, esta herramienta no se le incorporo nativamente el concepto de calidad de servicio y recientemente se están desarrollando modificaciones o parches para poder utilizar este protocolo para ese objetivo.

Los principales detractores del uso de SNMP para mediciones de calidad en el servicio mencionan que SNMP no provee suficiente información en la base de datos administrativa (MIB) que originalmente se utiliza con dicho protocolo.

Empezaremos definiendo en que consiste el protocolo de administración de redes para comprender como funciona y posteriormente incorporar los conceptos calidad de servicio y demostrar la utilidad de SNMP para este fin.

2.5.1 Administración de Redes

[Black, 1992] define el término administración de redes tomando prestada la definición de administración de negocios, ya que involucra la planeación, organización, monitoreo y control de actividades y recursos.

[Stallings, 1998] dice que la idea básica de un sistema de administración de red es que haya dos tipos de sistemas en cualquier configuración en red:

1. Agentes: Cualquier nodo en la red que tiene que ser administrado incluye un módulo con un agente, como PC's, estaciones de trabajo, servidores, enrutadores, etc.
    a. El agente es responsable de:
        i. Recolectar y mantener información acerca de su medio ambiente local.
        ii. Proveer la información a un administrador, ya sea en respuesta a una petición de información o a una que no ha sido solicitada cuando algo sobresaliente pasa, como una alarma.
        iii. Responder a los comandos del administrador de alterar la configuración local o los parámetros de operación.
2. Administradores: Este es un programa que interactúa con los agentes, el cual tiene la capacidad de recibir información de los agentes, por lo general solo se tiene un administrador por varios agentes en una red específica a ser vigilada.

Es importante tener un estándar para el uso de alarmas, indicadores de eficiencia, estadísticas de tráfico, registros, estadísticas contables y otros elementos vitales de la red, ya que de esta manera todos los fabricantes de equipo implantarán el código de un agente compatible.

2.5.1.1 Protocolos de Administración de Redes

[Black, 1992], nos da una idea acerca de lo que existe en estándares para administración de redes:

1) Los modelos de protocolo del Open Systems Interconnection (OSI)
    a. Common Management Information Protocol (CMIP)
    b. Common Management Information Service Element (CMISE)

    Estos estándares proveen cinco áreas funcionales para la administración de redes como es: alarmas, eficiencia, configuración, contabilidad y seguridad.
2) Los protocolos de Internet
    a. Simple Network Management Protocol (SNMP)
    b. CMIP sobre TCP (CMOT)
3) Los protocolos propuestos por la IEEE
    a. CMIP sobre LLC (CMOL)
    b. Una aproximación de IEEE sin CMIP.

2.5.2 Definición SNMP

[Hein, 1995] define SNMP como un mecanismo de transporte de información entre componentes de la red que permite la administración mediante la supervisión y verificación de ciertas condiciones de la red.

[Stallings, 1998] define la función de este protocolo como el intercambio de información entre los agentes y el sistema de administración. Y comenta que SNMP es un protocolo de administración de redes que fue diseñado para ser fácil de implementar y consumir recursos mínimos de procesador y de red, pero [Hein, 1995] dice que "el término "Simple" es fuente de malos entendidos. SNMP no es simple en su especificación ni en su implementación real. No fue diseñado para ser "simple". Pero los conceptos integrados en el protocolo SNMP son de una simplicidad que varia desde bella hasta trivial. Esto hizo SNMP versión 1 decepcionantemente fácil de implementar. Muchos fabricantes de productos de comunicaciones desarrollaron su propia versión 1 de SNMP pero desestimaron el trabajo requerido para hacer de una especificación simple un producto vendible, lo que fue un error muy caro. La versión 2 de SNMP es por mucho más compleja que la versión 1."

También dentro de este protocolo, se usan bases de datos llamadas bases de administración de información (management information bases MIB)

En esencia el protocolo provee cuatro funciones:

a) Get: Usado por el administrador para recoger información del agente

b) Set: Usado por el administrador para definir un valor en el agente

c) Trap: Usado por el agente para mandar una alerta al administrador

d) Inform: Usado por el administrador para mandar una alerta a otro administrador.

2.5.2.1 Evolución de SNMP

[Stallings, 1998] comenta que SNMP tuvo su primera publicación en 1988 y ha llegado a ser la herramienta de administración de redes más comúnmente usada para TCP/IP.

El crecimiento que tuvo desde finales de los años ochenta no ha sido lo suficientemente rápido y lo ha llevado a tener algunas deficiencias principalmente de seguridad.

Algunas de estas deficiencias se trataron de resolver con una nueva versión del protocolo llamado SNMPv2, que fue publicado como un conjunto de "RFC" (Request for comments) en los cuales se definen los cambios propuestos e interviene gente de diferentes compañías para lograr un consenso.

[Stallings, 1998] describe como en 1993, la edición de SNMPv2 incluía una facilidad para seguridad, pero no se llegó a un consenso y más tarde una edición revisada de SNMPv2 fue hecha en 1996 y se llamó SNMPv2c.

Siguieron los trabajos y se creó SNMPv2u y SNMPv2*, estas aproximaciones fueron la base para crear el SNMPv3.

SNMPv3 no es un reemplazo para SNMPv1 o SNMPv2, define una estándar de seguridad para ser usado preferentemente con SNMPv2, pero también puede ser usado con SNMPv1.

Según el RFC 2570 (1999), La tercera versión del estándar de SNMP se deriva y construye del estándar original SNMPv1 y SNMPv2.

Todas las versiones (SNMPv1, SNMPv2, SNMPv3) comparten la misma estructura básica y de sus componentes y en adelante, todas las versiones de especificación deberán tener la misma arquitectura.

En Febrero del 2002, se difundió una noticia sobre las fallas de seguridad que tiene SNMP, ya que para esta fecha, muchos productos seguían usando la primera versión del protocolo, lo que nos muestra que no está siendo ampliamente usado, porque si así fuera, ya se hubieran actualizado a las versiones más recientes de dicho protocolo. Después de esta advertencia, los diversos fabricantes implantarán parches al código de los agentes para actualizarlo. También se emitieron una serie de recomendaciones sobre seguridad que no están directamente relacionadas con la programación del protocolo, sino que se refieren a cambiar los parámetros que vienen por defecto y son causa de intrusiones en la red.

2.5.3 SNMP para QoS

Se pueden usar los agentes RMON y RMON2 para obtener información de la red y de esta manera tener una idea del tráfico que en ella se transporta, para que, posteriormente, se puedan definir políticas de tráfico para QoS. El problema es que si se usan intensivamente, generan tráfico adicional a la red y si tenemos una red muy congestionada, el uso de estos agentes puede no ser recomendable, sin embargo se menciona esta posibilidad porque es una manera de implementar un esquema de calidad de servicio QoS. En los capítulos posteriores se menciona la manera de utilizar SNMP para este fin.

3. CALIDAD DE SERVICIO (QOS)

La filosofía fundamental de calidad de servicio se deriva de la terminología de administración de ancho de banda. "Había inicialmente dos campos grandes para administración de ancho de banda: clase de servicio (COS) y calidad de servicio (QoS)" [Croll, 2000] Donde COS dividía el tráfico en unas cuantas categorías de servicio y QoS permitía la negociación de servicios de red dinámicamente a través de reservación de ancho de banda.

Mientras se dependa de redes con entrega de paquetes bajo el modelo de mejor esfuerzo y se transporten de manera concurrente voz, video, datos y aplicaciones interactivas a través de una infraestructura común, se deben ofrecer a cada uno de estos tipos de tráfico las características de manejo que requieren. [Croll, 2000]

Una red con ancho de banda administrado, es capaz de ofrecer características de tráfico basado en el tipo de tráfico que maneja. El tráfico puede ser clasificado por aplicación, usuario o factores externos como el usuario y congestión de la red. [Croll, 2000]

Un aspecto importante de QoS es que las características de la red permanezcan predecibles, sin importar el mecanismo usado para dar preferencia a un tráfico sobre otros tipos de tráfico, estas características de comportamiento radican en: respuesta de punto a punto también conocida como RTT (round trip time), latencia, retraso de filas de espera, ancho de banda disponible, entre otros. Algunas de estas características son más predecibles que otras dependiendo del tipo de tráfico, características de asignación en filas de espera de los dispositivos de la red y la arquitectura de la red.

En términos de latencia, existe la real y la inducida. La real se refiere al retraso físico de la transmisión por el medio, que depende de las características del mismo medio de transporte, mientras que la inducida es el retraso inducido a la red por el retraso de las filas de espera en los dispositivos de la red, el retraso inherente al procesamiento en los dispositivos y la congestión presente en los puntos intermedios de las trayectorias de los datos. Existe un tercer tipo de latencia, que se llama latencia recordada, la cual se refiere a la relación de latencia en las redes y la percepción humana, en la que los usuarios tienden a recordar con más facilidad cuando la red tiene errores que el éxito en el envío de información, esta impresión deja al usuario con la idea que la calidad del servicio es pobre, aun cuando la calidad del servicio sea buena.

Los mecanismos de QoS tienen más demanda en los ambientes empresariales, académicos y otras intranets privadas que en el Internet Global y los proveedores de Internet (ISP), porque cada uno tiene diferentes requerimientos, aún entre corporaciones existen diferentes requerimientos.

Las tecnologías de QoS se pueden ver como los bloques fundamentales de construcción de la red que serán usados para aplicaciones futuras de negocios en las redes de: Un Campus, redes de área amplia (WAN) o proveedores de servicios.

QoS debe tener la habilidad de definir los parámetros para configurar una red para transportar un paquete entre dos nodos considerando rendimiento, disponibilidad y retardos óptimos.

Estos parámetros no son fijos y pueden variar dependiendo de la aplicación que este utilizando los servicios de la red. Por ejemplo, el retraso máximo esperado para una comunicación con voz con telefonía IP, es de 300ms punto a punto, si se tienen siete enrutadores con retraso promedio de 50ms cada uno, no se logrará una comunicación eficiente no importando que se tenga un buen ancho de banda disponible.

Calidad de servicio se refiere a la capacidad de una red para proveer un mejor servicio a tráfico de red seleccionado sobre varias tecnologías, incluyendo Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet y redes inalámbricas IEEE 802.11, SONET y redes IP que pueden usar cualquiera de estas tecnologías mencionadas.

La meta principal de QoS es proveer prioridad, incluyendo ancho de banda dedicado, jitter y latencia controladas, estos dos últimos parámetros son requeridos para tráfico en tiempo real o interactivo, es importante asegurarse que al proveer prioridad para uno o más tipos de flujos, no hacer que los otros tipo de flujo fallen.

QoS permite proveer mejor servicio a ciertos flujos de paquetes definidos, esto se hace incrementando la prioridad de un flujo o limitando la prioridad de otro flujo. Cuando se usan las herramientas de administración de congestionamiento, se trata de incrementar la prioridad poniendo en fila de espera a todos los paquetes y asignando servicio en diferentes maneras. Esta herramienta de administración de filas de espera se usa para evitar congestión e incrementar la prioridad descartando los flujos de baja prioridad antes que los de alta prioridad. Las prioridades se definen por políticas. Hay otras herramientas para eficiencia del enlace que limitan flujos grandes para dar una preferencia para flujos pequeños.

3.1 Calidad de Servicio vs. Clase de Servicio

Calidad de Servicio se refiere a la capacidad de diferenciar entre tráfico y tipos de servicio para que los usuarios puedan tratar una o más clases de tráfico diferente a las otras.

Clase de servicio implica que los servicios pueden ser clasificados en categorías de clases separadas, para lo que pueden ser tratados individualmente. La diferenciación es el concepto central de CoS.

3.1.1 Clases de Servicio (CoS)

Una red basada en COS es por mucho más simple que un sistema completo de QoS, un número pequeño y razonable de clases puede que no sea suficiente para muchas aplicaciones diferentes que lleguen en los próximos años, cada una de las cuales tendrán necesidades diferentes. Por otro lado, incrementar el número de clases deteriora la simplicidad de un modelo COS. [Croll, 2000]

La señalización de COS reside en el encabezado de cada paquete de datos. Esto le dice a los dispositivos la clase a la cual pertenece dicho paquete. [Croll, 2000]

COS es una manera de decidir como actuar cuando dos paquetes llegan de diferentes fuentes en diferentes puertos y deben ser enviados al mismo puerto destino o cuando la capacidad de ingreso excede la capacidad de egreso. CoS le dice al dispositivo a cual clase se debe favorecer bajo tal condición de congestión [Croll, 2000]

3.1.2 Calidad de Servicio (QoS)

La señalización de QoS ocurre mediante el Protocolo de Reservación de paquetes y la negociación de contratos de servicio ATM. Cada uno de estos intenta obtener una garantía del comportamiento de la red negociando características para el circuito o el flujo explícitamente. [Croll, 2000]

Son tres las piezas fundamentales para la implementación de QoS.

1. Identificación de QoS y técnicas de marcado para coordinar QoS de punto a punto entre los elementos de la red.
    a. **Clasificación**: Para proveer servicio preferencial a un tipo de tráfico, primero debe ser identificado, después el paquete puede o no ser marcado. Estas dos tareas hacen posible la clasificación. Cuando un paquete es identificado, pero no marcado, la clasificación es basada en un salto (hop), es decir, cuando la clasificación pertenece solo al dispositivo donde esta el paquete y no se pasa al siguiente enrutador. Esto es posible con el uso de filas de espera con prioridad y filas de espera configuradas previamente. Cuando los paquetes son marcados para su uso en toda la red, los bits de precedencia de IP pueden ser configurados como se explica más adelante en precedencia de IP y señalización para QoS diferenciado. Los métodos comunes de identificar flujos incluyen listas de control de acceso (ACL), ruteo basado en políticas, tasa de acceso predefinida (CAR) y por reconocimiento de aplicaciones basadas en red.
2. QoS dentro de un componente simple de la red.
    a. **Administración de congestión**: Debido a la naturaleza de ráfaga del tráfico de voz, video y datos, algunas veces la cantidad de tráfico excede el límite de velocidad de transferencia de un enlace. En este punto, el enrutador no puede guardar en un búfer todo el tráfico que no puede salir, por lo que se usan herramientas para evitar la congestión en la red, las cuales incluyen poner en fila de espera los paquetes según su prioridad, prioridad configurada previamente, fila de espera basada en peso y en clase.
    b. **Administración de filas de espera**: Debido a que las filas de espera no se pueden guardar en búferes de tamaño infinito, se pueden llenar y desbordarse, cuando se llena y no se puede guardar un dato más, el último paquete se descarta, aunque sea de alta prioridad por lo que necesitamos un mecanismo para dos cosas:

i. Tratar de asegurarse que la fila de espera no se llene, para que haya lugar para paquetes de alta prioridad.

ii. Permitir que se descarten paquetes de baja prioridad antes de que se llene el búfer, para que si llega uno de alta prioridad pueda tener cabida.

c. **Eficiencia del enlace**: Muchas veces la velocidad del enlace presenta un problema para paquetes pequeños, por ejemplo, la conversión a forma serial de un paquete de 1500 bytes en un enlace de 56kbps es de 214 milisegundos. Si un paquete de voz viene detrás de este gran paquete, el retraso para voz excedería el tiempo límite aun antes de salir del enrutador, la fragmentación del enlace permite que este paquete se segmente en paquetes pequeños, dando paso más rápido a otros paquetes pequeños.

i. Para hacer el cálculo de retraso:

1. Tamaño de paquete: (1500 bytes / paquete) * (8 bits / byte) = 12000 bits
2. Velocidad de la línea: 56,000 bits por segundo
3. 12,000 bits / 56,000 bits = .214 segundos o 214 milisegundos.

d. **Políticas de tráfico y conformación (shaping) de tráfico**: La conformación de tráfico limita el potencial del ancho de banda del flujo. Muchas redes usan Frame Relay en un diseño de concentrador (hub), en este caso el sitio central tiene un enlace de mayor velocidad mientras los sitios remotos tienen enlaces de menor velocidad, por ejemplo, el sitio central tiene un enlace de alta velocidad como un T1, mientras que los remotos pueden tener enlaces de 384 Kilo bits por segundo (Kbps), en este caso es posible que el tráfico del sitio central sobrepase el enlace de ancho de banda bajo, entonces la conformación es perfecta para regular el tráfico cerca de los 384 Kbps para evitar el sobre flujo del enlace remoto. El tráfico que esta cercano a la tasa de transferencia configurada se almacena en búfer para ser transmitida más tarde para mantener la tasa configurada. La regulación por políticas es similar a la conformación de tráfico, pero la diferencia es importante, si el tráfico rebasa la tasa configurada, los datos no se almacenan, solo se descartan.

3. Políticas de QoS, administración y funciones contables para controlar el tráfico punto a punto a través de una red.

a. **Administración de QoS**: ayuda a evaluar las políticas y metas de QoS, una metodología común promueve los siguientes pasos.

i. Hacer una referencia de la red usando pruebas de RMON de SNMP. Esto ayuda a determinar las características de tráfico de la red, también las aplicaciones que requieren QoS deben ser referenciadas, usualmente en términos de tiempo de respuesta.

ii. Desarrollar las técnicas de QoS cuando las características se han obtenido y también con las aplicaciones de que requieren QoS.

iii. Evaluar los resultados probando la respuesta de las aplicaciones seleccionadas para ver si las metas de QoS han sido satisfechas.

b. En los enrutadores de Cisco, hay una herramienta de administración de calidad de servicio (QPM) y de administración de calidad de dispositivos (QDM) Para verificación de niveles de servicio se puede usar el monitor de rendimiento de la red (IPM)

3.2 Niveles de QoS punto a punto

Los niveles de servicio se refieren a la capacidad actual de QoS de punto a punto o la capacidad de una red para llevar el servicio necesitado por un tráfico de red específico de punto a punto. Los servicios tienen diferencias en que tan estrictos son con el QoS. Lo que describe que tan cerca se puede medir el servicio en ancho de banda, retrasos (jitter) y características de pérdidas. Hay tres niveles básicos de QoS de punto a punto que pueden ser provistos a través de una red heterogénea como se muestra en la figura 3.1

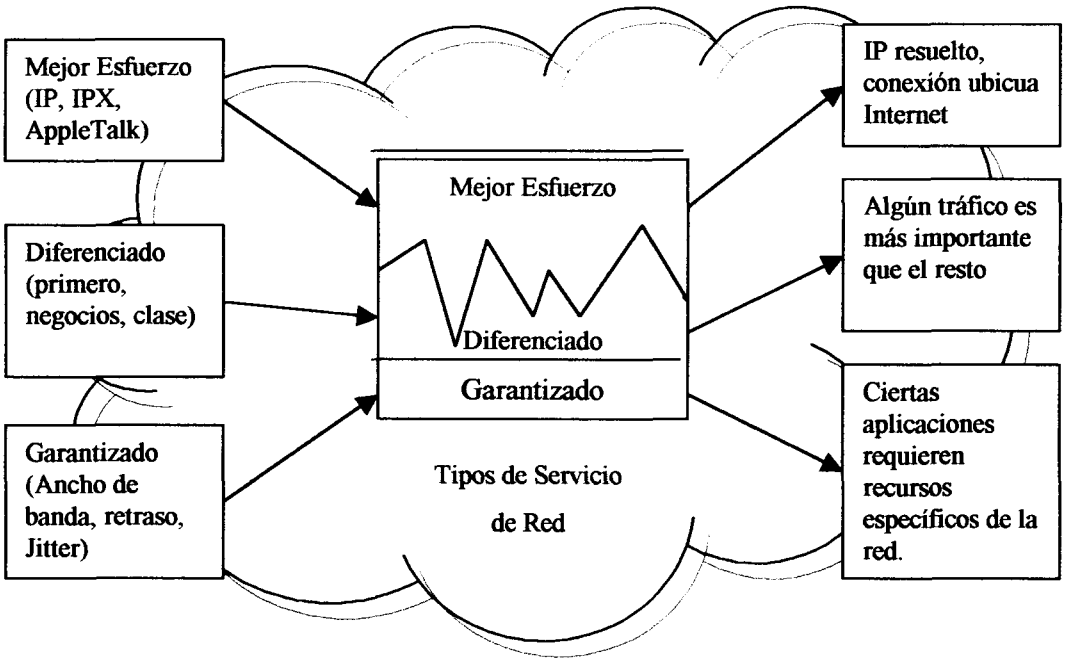


Figura 3.1 Niveles de QoS

3.2.1 Servicio de Mejor Esfuerzo, Diferenciado y Garantizado

Servicio de Mejor Esfuerzo: También se conoce como falta de QoS, este servicio se refiere a conectividad básica sin ninguna garantía. Esta se caracteriza por filas de espera tipo FIFO (primero que entra, primero que sale) que no tienen diferenciación entre flujos.

Servicios Diferenciados: También se conoce como QoS suave, donde algún tráfico se trata de mejor manera que el resto, que incluye manejo más rápido, más disponibilidad promedio de ancho de banda, y menores pérdidas. Esta es una preferencia estadística y no tiene garantía de rapidez. Se provee mediante la clasificación de tráfico y el uso de herramientas de QoS como PQ, CQ, WFQ y WRED que se describirán más adelante.

Servicio Garantizado: Este se refiere a una absoluta reservación de la red para un tráfico en específico. Se provee a través de herramientas de QoS como RSVP y CBWFQ que se describirán más adelante.

3.3 Clasificación e identificación de flujos

Para proveer prioridad a ciertos flujos, éste debe primero ser identificado y si se desea también marcarlo. Estas dos tareas se conocen también como clasificación.

La identificación de flujos era hecha usando listas de control de acceso (ACLs) Un ACL identifica el tráfico con herramientas de PQ y CQ, las cuales reemplazan los paquetes en los enrutadores cada vez que llegan a un enrutador, en otras palabras, las configuraciones de QoS pertenecen sólo a ese enrutador y no lo pasa al siguiente enrutador, la identificación del paquete se usa solamente cuando tenemos un solo enrutador. En Algunas circunstancias la clasificación CBWFQ es solo para un enrutador.

El ruteo basado en políticas y en tasa de transferencia comprometida (CAR) pueden ser usados para fijar la precedencia basada en clasificaciones de listas de acceso. Esto permite una flexibilidad considerable para asignación de precedencia, incluyendo asignación por aplicación o usuario, por destino y subred. Típicamente, esta funcionalidad es desarrollada en el extremo de la red (o dominio administrativo), lo más cerca posible de cada red interconectada.

El reconocimiento de aplicaciones basadas en red (NBAR) se usa para identificar el tráfico más a detalle, por ejemplo, URL´s en un paquete http puede ser identificado.

3.3.1 QoS con ruteo basado en políticas.

Este tipo de ruteo, nos permite clasificar el tráfico basado en listas extendidas de acceso, para definir los bits de precedencia en el encabezado de IP, y se necesita la ruta del paquete para permitir QoS específico a través de la red.

Usando los niveles de precedencia en el tráfico que se recibe y usándolos en combinación con las herramientas para hacer filas de espera, se puede crear servicio diferenciado. Estas herramientas nos dan opciones poderosas, simples y flexibles para implementar políticas de QoS en la red.

Al usar el ruteo basado en políticas, los mapas de ruteo se hacen para que coincidan con ciertos criterios de flujo y entonces se definen bits de precedencia cuando coinciden con las listas de acceso.

La capacidad de definir precedencia en los bits de IP no deben confundirse con la capacidad de (PBR) o ruteo basado en políticas configuradas. Algunas aplicaciones o tráfico se pueden beneficiar de los registros de transferencia de ruteo a una oficina corporativa, por ejemplo, en una conexión de mayor ancho de banda que tiene un costo mayor, por un periodo corto de tiempo, mientras que la aplicación de la rutina de transmisión como e-mail se puede hacer en una conexión de ancho de banda reducido con un costo menor. Los PBR pueden ser usados para dirigir paquetes para que tomen trayectorias diferentes que el que se tiene de los protocolos de ruteo.

También se pueden usar los mapas de ruteo como la capacidad de identificar los paquetes basados en el protocolo de frontera (Border Gateway Protocol) Esto se conoce como política de propagación vía BGP.

3.3.1.1 CAR: Políticas de precedencia IP

Es similar de alguna manera con el PBR, pero CAR nos permite clasificar el tráfico de una interfase de entrada de un enrutador. También permite especificar políticas para manejar el tráfico que excede las limitantes del ancho de banda. CAR busca en el tráfico que se recibe por una interfase o en un subconjunto de tráfico seleccionado por el criterio de las listas de acceso. Se compara la tasa con aquella configurada previamente y decide si lo descarta o rescribe la precedencia IP.

Hay alguna confusión al usar CAR con los bits de precedencia de IP. CAR se usa para describir el tráfico con una tasa de transferencia dedicada. Lo hace con un "token bucket", es un cubo o "vasija" con tokens en el que representan bytes (1 token = 1 byte) El cubo se llena con tokens a una tasa configurada por el usuario. Conforme llegan los paquetes, el sistema analiza los tokens, si hay suficientes tokens en el cubo que coinciden con el tamaño del paquete, esos tokens se remueven y el paquete se pasa al siguiente enrutador. Si no hay suficientes tokens, el paquete se descarta.

Cuando se usa la implementación de Cisco para CAR, se tienen más opciones que sólo pasar o descartar, cuando se definen los cubos para descartar y pasar con el mismo número, entonces ya no es una política, pero si un método para definir los bits de precedencia de IP.

3.3.1.2 NBAR: Identificación dinámica de flujos

Este es un método relativamente nuevo de reconocimiento de aplicaciones basadas en red. NBAR es solo una herramienta de identificación, pero se le considera también como una herramienta de clasificación. La parte más difícil es identificar el tráfico, marcando el paquete después de su arribo, lo hace tomando la porción de identificación a otro nivel buscando profundamente en el paquete, por ejemplo URL's de un paquete http. Esto es esencial conforme más aplicaciones son basadas en WEB, pero se necesita diferenciar entre el orden para ser puestos comparándolos con la navegación casual en navegadores WEB. NBAR decide buscando los paquetes de control para determinar que puertos se usaran para pasar la aplicación.

NBAR agrega algunas características que lo hacen valioso, la primera es la capacidad de descubrimiento del protocolo, que permite a NBAR definir una referencia para pasar los protocolos en una interfase determinada. Lista los protocolos que puede identificar y provee estadísticas de cada uno. Otra característica es el módulo de descripción de lenguaje (PDLM) que permite que protocolos adicionales puedan ser agregados fácilmente a la lista de protocolos identificables, estos módulos se cargan en la memoria no volátil del enrutador que cuando se reinicia no se pierden esos datos. Usando PDLM, se pueden agregar protocolos adicionales a la lista sin reiniciar el enrutador.

3.3.1.3 Precedencia IP: QoS Diferenciado.

Para definir la precedencia de IP, se usan los 3 bits de precedencia del encabezado del protocolo IPv4, para especificar la clase de servicio para cada paquete como se muestra en

la figura 3.2. Se puede dividir el tráfico hasta en seis clases de servicio usando la precedencia de IPv4, quedan otras dos clases que se reservan para uso interno de la red.

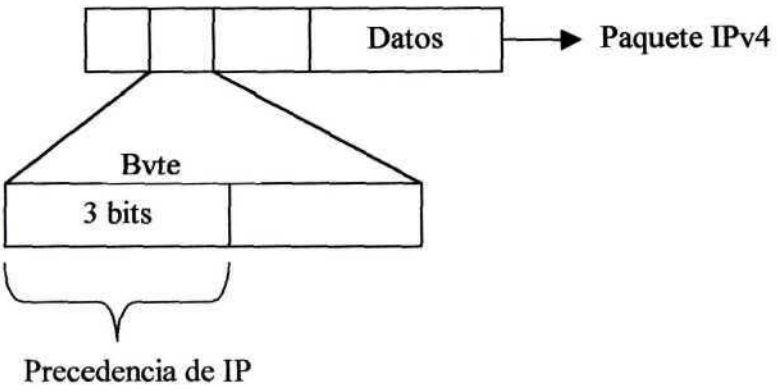


Figura 3.2 Byte de tipo de servicio en el protocolo IPv4

Los 3 bits más significantes (que corresponden a los valores 32, 64 y 128) son los que constituyen el campo de tipo de servicio (ToS), estos bits se usan para proveer prioridad de 0 a 7 (los valores 6 y 7 se reservan y no los debe fijar el administrador de la red)

Debido a que solo se pueden usar 3 bits del byte de ToS para precedencia IP, se necesitan diferenciar estos bits del resto del byte ToS, se toman del primero al tercer posiciones de bit viéndolos de izquierda a derecha, si los dos bits están en 1, se tiene un valor de 5, como se muestra en la figura 3.3

X	X	X						Bits Usados
128	64	32	16	8	4	2	1	Valor de los bits
1		1						Bits de precedencia IP
4	2	1	= 5					Valor del campo de precedencia

Figura 3.3 Byte de tipo de servicio

En el RFC2475, se extiende el número de bits usado en el byte TOS es de 3 a 6, que se usarán para definir precedencia (conocido como puntos de código DS), con los 2 bits más significativos. Esta especificación se conoce como Servicios Diferenciados (DiffServ) que se explica posteriormente.

3.4 Herramientas de Administración de Congestionamiento.

Existen varios métodos para manejar el sobre flujo del tráfico que llega a un enrutador, de alguna manera se tiene que clasificar el tráfico, y determinar algún método para darle prioridad por un enlace de salida.

Existen los siguientes métodos:

- Primero en entrar, primero en salir (FIFO)
- Filas de espera con prioridad (PQ Priority Queuing)
- Filas de espera configuradas (CQ Custom Queuing)
- Filas de espera basadas en peso justo (WFQ Weighted Fair Queuing)
- Filas de espera basadas por clase y peso (CBWFQ Class Based Weighted Fair Queuing)

Cada método de puesta en fila de espera fue diseñado para resolver un tipo específico de problema de red con un efecto particular en el desempeño de la red como se describe en la siguiente sección

3.4.1 FIFO: Capacidad básica de Guarda y Envía

En su forma más simple, el hacer una fila de espera involucra guardar los paquetes cuando la red se congestiona y se envían a la salida en el mismo orden en el que llegaron cuando la red ya no esta congestionada. FIFO es el algoritmo por defecto (default) en muchos lugares, por que no necesita configurarse y no hace ninguna decisión sobre la prioridad de los paquetes, el orden de la llegada determina el ancho de banda, pero no provee protección contra aplicaciones que no se comporten bien como fuentes de datos en ráfaga que pueden causar grandes retrasos en el envío de paquetes que son sensibles al tiempo. FIFO fue el primer paso para controlar el tráfico de red, pero las redes inteligentes actuales necesitan algoritmos más sofisticados, aparte que FIFO, cuando llena la fila de espera, causa que se descarten paquetes que llegan, aunque sean de alta prioridad. Por lo que el enrutador no puede prevenir que este paquete se descarte porque no había espacio en la fila de espera para guardarlo.

3.4.2 PQ: Tráfico con Prioridad

PQ asegura que el tráfico importante tiene un manejo rápido en cada punto donde pasa. Fue diseñado para dar prioridad estricta al tráfico importante. Este tipo de puesta en fila de espera con prioridad, puede ser flexible para mantener la prioridad de acuerdo al protocolo que se quiera como IP, IPX o AppleTalk, las interfaces de entrada, tamaño del paquete, dirección de fuente o destino. Cada paquete se pone en una de cuatro diferentes filas de espera, alta, media, normal y baja, según se le asigne la prioridad. Aquellos paquetes que no se puedan clasificar bajo este mecanismo, se consideran como tráfico normal. Durante la transmisión, el algoritmo asigna los paquetes de alta prioridad que se guardan en

la fila de espera de alta prioridad un tratamiento preferencial absoluto sobre las de baja prioridad.

3.4.3 CQ (Custom Queue): Ancho de banda Garantizado

CQ fue diseñado para permitir que varias aplicaciones u organizaciones compartan una red con un mínimo de ancho de banda y retardo (latency) garantizados. En estos ambientes, el ancho de banda debe ser compartido proporcionalmente entre aplicaciones y usuarios. Se puede definir este tráfico de ancho de banda garantizado para evitar algún cuello de botella y dejar el ancho de banda sobrante para el tráfico que no sea garantizado.

El CQ maneja el tráfico asignando una cantidad específica de espacio de la fila de espera a cada clase de paquete y asigna servicio en forma de "round robin". Por ejemplo, el SNA (Systems Network Architecture) requiere un ancho de banda o nivel de servicio mínimo garantizado, se puede reservar la mitad del ancho de banda para los datos de SNA y permitir la otra mitad para ser usada por otros protocolos como IP o IPX.

El algoritmo pone los mensajes en una de las 17 filas de espera, la fila de espera 0 mantiene los mensajes del sistema como señalización, y se vacía con la prioridad o peso que se le dio a cada una. El enrutador le da servicio del 1 al 16 en orden "round robin", esta característica asegura que ninguna aplicación tomara más de la proporción predeterminada de toda la capacidad cuando esta bajo estrés la conexión. Se configura estadísticamente y no se adapta a las condiciones de la red.

3.4.3.1 WFQ basado en flujo: Creando equidad entre flujos

Para situaciones en la cual es deseable proveer respuesta consistente para usuarios con tráfico pesado o ligeros, sin necesidad de agregar ancho de banda extra, la solución es WFQ el cual es un algoritmo que crea igualdad al permitir que cada fila de espera sea servida con de la misma manera. Por ejemplo, si una fila de espera tiene un paquete de 100 bytes y la fila de espera 2 tiene 2 paquetes de 50 bytes, el algoritmo tomará los 2 paquetes de la fila de espera 2, esto hace el servicio sea justo para cada fila de espera. 100 bytes cada vez que cada fila de espera tenga salida al enlace.

WFQ asegura que las filas de espera no se queden con necesidad de más ancho de banda y el tráfico se hace predecible. Los volúmenes bajos de tráfico son la mayoría del tráfico existente y reciben un servicio mejorado, al transmitir el mismo número de bytes por fila de espera como si fueran cadenas de bits de alto volumen.

Este comportamiento resulta en lo que aparenta un servicio preferente para tráfico de bajo volumen, cuando en realidad los distribuye igualmente. WFQ esta diseñado para minimizar la configuración y adaptarse automáticamente a las condiciones de tráfico de la red, de hecho hace un buen trabajo para la mayoría de las aplicaciones y se ha convertido en el estándar para las interfases seriales WAN que corren con líneas cuya velocidad es menor a una E1 (2048Mbps)

El WFQ basado en flujo, crea flujos basados en un número de características en un paquete, cada flujo se puede ver como una conversación que es dada con su propia fila de espera si se encuentra congestión en la red. Las características que definen el flujo incluyen

la dirección fuente y destino, número de enchufes (sockets) e identificadores de sesión. Para cada protocolo se usa un criterio diferente. La porción de WFQ que es balanceada, viene de los bits de IP de precedencia, y proveen buen servicio para ciertos tipos de filas de espera. Usando precedencia del 0 al 5 (6 y 7 son reservados)

WFQ es eficiente porque usa el ancho de banda que este disponible para enviar en tráfico de baja prioridad si no hay tráfico de alta prioridad presente. Esto es diferente de multiplexeo estricto por tiempo (TDM) que simplemente usa en ancho de banda definido y no usa el resto del ancho d banda si no hay tráfico de alta prioridad presente. WFQ puede trabajar con RSVP (Resource Reservation Protocol) y con la precedencia IP que ayudan a proveer QoS diferenciado y servicios garantizados. WFQ también ayuda a resolver el problema de la variación en el retraso de viaje redondo. Si hay múltiples conversaciones de alta prioridad y volumen de transferencia alto, sus tasas de transferencia son muy predecibles, por lo que si el servicio se comporta de una manera estable, ayuda a algoritmos como SNA, Control lógico de enlace (Logical Link Control) y TCP (Transmisión Control Protocol) El resultado es más predecible y el tiempo de respuesta también mejora para cada flujo activo.

3.4.3.2 Cooperación entre WFQ y Tecnologías de Señalización para QoS

Anteriormente se menciono que WFQ puede hacer uso de la precedencia IP, o sea, es capaz de detectar paquetes de alta prioridad marcados con precedencia y el distribuidor de IP puede programarlos más rápido, lo que provee una respuesta superior para este tipo de tráfico. Conforme aumenta el valor de precedencia, el algoritmo le reserva más ancho de banda a ese flujo de paquetes para asegurarse que se procese más rápido cuando ocurra una congestión. WFQ asigna un peso a cada flujo el cual determina el orden de transmisión para paquetes en espera, en este esquema los paquetes que tienen menos peso se transmiten con menos prioridad.

El peso es un número calculado del valor de precedencia IP para un paquete en movimiento. Este peso se usa en el algoritmo de WFQ para determinar cuando a un paquete se le asignará servicio.

$$\text{Peso} = (4096 / \text{Precedencia IP} + 1)$$

$$\text{Peso} = (32384 / \text{Precedencia IP} + 1)$$

Estos valores se pueden ver usando el comando "*show queue <interface>*" en un enrutador Cisco con software versión 12.

WFQ también toma en cuenta RSVP, el cual usa para distribuir el búfer y programar paquetes, lo que garantiza el ancho de banda para flujos reservados. Adicionalmente en una red Frame Relay, la presencia de congestión se pone en una bandera para explícitamente notificar la congestión (FECN) Los pesos de WFQ son afectados por la elegibilidad de descarte de paquetes de Frame Relay. Cuando se encuentra una bandera de congestión, los pesos usaos por el algoritmo para que se transmita en condición de congestión menos frecuentemente.

3.4.3.3 WFQ Basado en Clase: Asegurando el ancho de banda de la red.

WFQ basado en clase es una herramienta de administración de congestión de Cisco, que tiene gran flexibilidad. Cuando se quiere proveer un mínimo de ancho de banda garantizado se usa CBWFQ. Cuando se quiere usar un máximo de ancho de banda se utiliza CAR.

CBWFQ puede ser usado para prevenir que flujos múltiples de baja prioridad salgan antes que un flujo de alta prioridad. Por ejemplo, un flujo de video necesita la mitad del ancho de banda de un enlace T1, si hay dos o más flujos aparte del de video, WFQ le deja menos ancho de banda al de video porque WFQ crea tráfico balanceado, si hay 10 flujos, el video solo tendrá disponible 1/10 del ancho de banda total, lo que no es suficiente. Aún configurando el bit de precedencia en 5, no resuelve este problema.

Si el video toma 6/15 del ancho de banda, que es menos de lo que se necesita, un mecanismo se debe implementar para proveer la mitad del ancho de banda que necesita el video. CBWFQ soluciona este problema. El administrador de la red define una clase, pone el flujo de video en esa clase y le dice al enrutador que suministre 768 Kbps que es la mitad de un T1, y otra clase por omisión (default) se usa para el resto de los flujos. Ahora el video tiene el ancho de banda que necesita. Esto no quiere decir que WFQ no sirve, de hecho de acuerdo a las necesidades de cada aplicación en la red se debe implementar la herramienta de administración de red que se requiera. Si se quiere un flujo que tenga baja latencia, se puede usar una fila de espera LLQ, que es en esencia una fila de espera con prioridad, esta característica se puede ver como una fila de espera basada en prioridad balanceada que se conoce como PQCBWFQ (Class balanced weighted fair queuing)

3.4.4 Administración de filas de espera

El evitar la congestión en una red es una forma de administración de filas de espera, las técnicas que vigilan el tráfico de la red hace un esfuerzo para evitar la congestión en cuellos de botella comunes en la red, aunque se piensa que las herramientas de administración de la red sirven para controlar la cogestión en la red una vez que ha sucedido.

3.4.4.1 WRED: Evitando la congestión.

Los algoritmos RED (Random Early Detection) vigilan el tráfico de la red antes de que llegue a ser un problema. RED trabaja vigilando la carga de tráfico en puntos en la red y descarta los paquetes estocásticamente si la congestión empieza a aumentar. RED esta diseñado para trabajar principalmente con TCP/IP.

3.4.4.2 WRED: Cooperación con la tecnología de señalización de QoS.

WRED combina las capacidades del algoritmo RED con la posibilidad de usar precedencia IP. Esta combinación provee manejo preferencial del tráfico para paquetes de alta prioridad. Puede descartar selectivamente tráfico de baja prioridad cuando la interfase empieza a congestionarse y provee características de rendimiento diferenciado para diferentes clases de servicio. WRED también se puede usar con RSVP y provee servicios integrados de QoS con carga controlada.

Dentro de una fila de espera, solo un número finito de paquetes puede ser guardado, una fila de espera llena causa que el último se descarte. Este comportamiento no se desea porque puede ser un paquete de alta prioridad y el enrutador no tiene oportunidad de guardarlo en otra parte. Si la fila de espera no se ha llenado, el enrutador puede buscar la prioridad de todos los paquetes que llegan y tirar los de baja prioridad. Permitiendo los de alta prioridad guardarse en la fila de espera. La manera de administrar la cantidad de paquetes que se pueden guardar en una fila de espera, se hace tirando varios paquetes, el enrutador puede hacer tener mejor rendimiento asegurándose que la fila de espera no se llene y no se descartan los paquetes a causa de que la fila de espera este llena y no quepa ninguno más. Esto permite al enrutador seleccionar cuales son los que se pueden descartar.

3.4.4.3 RED para flujos que no son TCP.

Hay flujos que no son compatibles con TCP, para los que se usa "Flow RED", este incrementa la probabilidad de descartar un paquete se excede el umbral (threshold)

WRED basado en flujo hace dos aproximaciones para resolver el problema de descartar paquetes linealmente:

- Clasifica el tráfico entrante en flujos basados en parámetros como la dirección de entrada y de salida y los puertos que usa.
- Mantiene el estado de los flujos activos, los cuales tienen paquetes en las filas de espera de salida.

WRED basado en flujo usa esta clasificación para asegurar que cada flujo no consume más de lo que tiene permitido en los búfer de salida, por lo que determina que flujo está monopolizando recursos y penaliza estos flujos. Así es como WRED basado en flujo asegura la igualdad entre flujos y mantiene una cuenta del número de flujos activos que están en una interfase de salida. Dado este número se determina el número de búferes disponibles por flujo.

Para permitir algunos flujos en ráfaga, se escala el número de búferes disponibles por flujo por un factor configurado y permite a cada flujo activo tener un cierto número de paquetes en la fila de espera de salida. Este factor de escalamiento es común en todos los flujos. El Resultado de escalar el número de búferes se convierte en el limite por flujo. Cuando un flujo excede el limite por flujo, la probabilidad de que un paquete del flujo sea descartado se incrementa.

3.4.5 Herramientas para definir políticas y conformación (shaping) de tráfico.

Existen varias herramientas como la conformación de tráfico genérico (Generic Traffic Shaping) y conformación de tráfico Frame Relay (FRTS), para manejar el tráfico y la congestión.

3.4.5.1 CAR: Administrando políticas de Ancho de banda

Como se describió anteriormente, QoS provee prioridad ya sea aumentando la prioridad de un flujo o limitando la prioridad de otro, CAR se usa para limitar el ancho de banda de un flujo en orden a favor de otro flujo.

En la clasificación, que se menciono anteriormente, se describe un "token bucket", en esa clasificación los paquetes que cumplen con en criterio pasan y los que no se descartan.

Se pueden configurar ciertas acciones como transmitir o descartar los bits de precedencia y continuarlos, esta flexibilidad permite actuar de varias maneras en el tráfico como los ejemplos que se presentan.

- El tráfico de alta prioridad puede ser clasificado con una precedencia de 5 y el tráfico excedente puede ser descartado.
- El tráfico de alta prioridad puede ser transmitido con una precedencia IP de 5, mientras que el tráfico excedente puede ser transmitido con una precedencia IP de 1.
- El tráfico de alta prioridad puede ser transmitido, y el tráfico excedente se reclasifica a una precedencia IP más baja y mandarlos al próximo CAR para condiciones adicionales.

3.4.5.2 GTS: Controlando el tráfico de salida

GTS provee un mecanismo para controlar el tráfico en una interfase en particular, reduce el tráfico de salida para evitar congestión restringiendo tráfico específico a una tasa de transferencia fija. Mientras que pone el tráfico de ráfaga en la salida.

Esto difiere de CAR en que los paquetes no se ponen en fila de espera, solo que el tráfico que se apega a una descripción en especial se baja de ancho de banda, eliminando cuellos de botella en topologías donde la tasa de transferencia no es la misma.

GTS se aplica en cada interfase, puede usar listas de acceso para seleccionar el tráfico para afinar, trabaja con una variedad de tecnologías de capa 2 incluyendo Frame Relay, ATM y Ethernet. En una interfase Frame Relay, GTS puede adaptarse dinámicamente al ancho de banda disponible al integrar señales BECN, o puede ajustarse a una tasa predeterminada. GTS puede ser configurado en un procesador de interfase ATM/IP para responder a RSVP señalizado sobre circuitos permanentes ATM que son configurados estadísticamente.

3.4.5.3 FRTS: Administrando tráfico Frame Relay

FRTS provee parámetros que son útiles para administrar la congestión de tráfico, estos incluyen la tasa de información comprometida (committed information rate CIR), FECN y BECN y el bit DE. La característica FRTS para el soporte de Frame Relay, mejora la escalabilidad y rendimiento en una red Frame Relay, mejorando la densidad de circuitos virtuales y mejorando en tiempo de respuesta. Por ejemplo, se puede configurar un refuerzo en la tasa de transferencia. Una tasa pico configurada para limitar el tráfico de salida como la tasa de información en exceso (CIR Excess information rate) en un circuito virtual. También se puede definir la prioridad y puesta en fila de espera en el circuito virtual o en el nivel de sub-interfase. Esto permite definir prioridad y filas de espera para el tráfico, provee más control sobre el flujo de tráfico en un circuito virtual individual. Si se combina CQ con las filas de espera para circuitos virtuales, se habilita a los circuitos virtuales de Frame Relay a transportar múltiples tipos de tráfico como IP, SNA, IPX con un ancho de banda garantizado para cada tipo de tráfico.

FRTS puede eliminar cuellos de botella en redes Frame Relay con conexiones de alta velocidad en el sitio central y conexiones de baja velocidad en los sitios en las ramas. Se puede configurar refuerzo de tasa para limitar la tasa en la que se envían los datos en el circuito virtual del sitio central. También se puede usar con el Identificador de la característica para definir prioridad de la capa de datos (DLCI Data Link connection identifier) para mejorar el rendimiento en esta situación. FRTS se puede aplicar solo en Frame Relay y circuitos virtuales. Usando la información contenida en los paquetes recibidos de la red marcados con BECN, FRTS puede mantener los paquetes en el búfer del enrutador para reducir el flujo del enrutador en la red Frame Relay.

FRTS también provee un mecanismo para compartir información por múltiples circuitos virtuales. El refuerzo de tasa permite que la velocidad de transmisión usada por un enrutador sea controlada por otros criterios aparte de la velocidad, como el CIR o el EIR. Esta característica también puede ser usada para definir el ancho de banda de cada circuito, creando una red virtual DTM.

3.4.6 Mecanismos para eficientizar enlaces

Hay dos mecanismos para eficientizar enlaces, entrelazado de fragmentación de enlaces (LFI Link fragmentation interleaving) y el protocolo de compresión de encabezados en tiempo real (RTP-HC Real-time protocol header compression), el cual trabaja al poner en fila de espera y refinar el tráfico al mejorar la eficiencia y prediciendo los niveles de servicio de la aplicación.

3.4.6.1 LFI: Fragmentando y entrelazando tráfico IP

El tráfico interactivo (Telnet, Voz sobre IP) es susceptible a latencia y retraso no uniforme (jitter) cuando se procesan paquetes grandes en la red como sesiones de FTP que van por un enlace WAN, especialmente si van sobre enlaces de baja velocidad. LFI reduce el retraso en enlaces de baja velocidad separando los paquetes grandes en unos más pequeños que tienen menos retraso.

LFI fue diseñado para enlaces de baja velocidad en los cuales el retraso de la conversión a serial es significante. LFI requiere que el protocolo punto a punto (PPP) sea configurado en la interfase con el entrelazado encendido. Para implementar fragmentación sobre Frame Relay, se debe usar la característica FRF.12

3.4.6.2 Compresión de encabezados RTP

Incrementando la eficiencia de tráfico de tiempo real. El protocolo de tiempo real es un protocolo de host a host que se usa para llevar tráfico de multimedia, incluyendo audio y video en forma de paquetes sobre una red IP. Este protocolo de transporte en tiempo real provee funciones de transporte cuya intención es para ser usado en aplicaciones que transmiten en tiempo real como audio o video o datos de simulación sobre redes de múltiple transmisión (multicast) El encabezado de este protocolo incrementa la eficiencia en las aplicaciones sobre IP, especialmente en enlaces de baja velocidad. En la figura 3.4 se muestra el encabezado del protocolo de tiempo real.

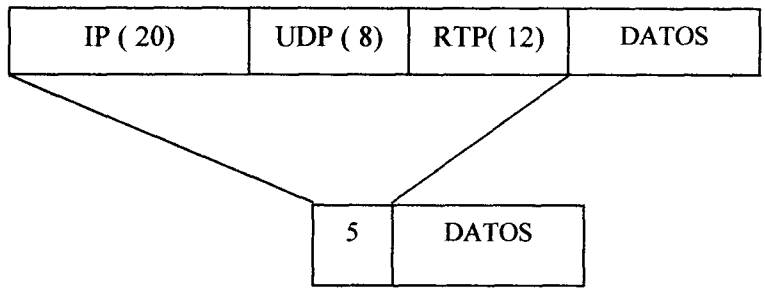


Figura 3.4 Encabezado RTP

Eficiencia Obtenida	Carga	Reducción del tamaño del paquete
VoIP	20 bytes	-240%
SOL	256 bytes	-13%
FTP	1500 bytes	-2.3%

Figura 3.5 Eficiencia Obtenida

También se obtiene una reducción de 5 milisegundos en retraso de conversión a serial de 64kbps.

3.4.6.3 RSVP: QoS Garantizando.

RSVP es un protocolo estándar de Internet (RFC2205) para permitir que una aplicación reserve ancho de banda dinámicamente. RSVP habilita aplicaciones para que pidan un QoS específico de un flujo de datos.

Los hosts y enrutadores usan RSVP para llevar QoS a los enrutadores en todo el camino del paquete de datos y mantener el estado del enrutador y del host para proveer el servicio requerido, frecuentemente lo que se busca es ancho de banda y retraso controlado. RSVP usa una media estadística, la cantidad más grande de datos que el enrutador mantendrá en fila de espera y el QoS mínimo para determinar el ancho de banda que se reservara. WFQ y WRED son la base para RSVP, definiendo la clasificación del paquete y programándolo para los flujos reservados. Usando WFQ, RSVP puede entregar servicios garantizados. Usando WRED puede entregar un servicio de carga controlada. WFQ provee ventajas al manejar el tráfico no reservado usando en ancho de banda remanente y balanceando el tráfico entre las conexiones de ancho de banda alto.

3.5 Administración de QoS

Se pueden hacer pruebas con RMON de SNMP y una aplicación como "Traffic Director" para desarrollar un buen modelo de las características del tráfico. Anteriormente, habíamos visto que con NBAR se puede tener una idea básica de la utilización de una interfase, pero con RMON, se puede obtener información más completa. También se puede tener una referencia del tiempo de respuesta de la línea para las aplicaciones. Esta información ayuda a validar la implementación de QoS. De estos datos se define e implementa la política de QoS.

Una vez que se ha desarrollado la validación, es importante evaluar las políticas de QoS para ver si se requerirán servicios adicionales. El monitor de rendimiento de Internet IPM (Internet performance monitor) puede ayudar en determinar si las políticas de QoS todavía son efectivas al medir los tiempos de respuesta de la red. Comparando estos datos con los obtenidos en las mediciones anteriores. Las pruebas de RMON deben monitorear continuamente la red porque las características de tráfico pueden cambiar. El tener una medición constante del tráfico de la red ayudara a visualizar tendencias y le permite al administrador prevenir problemas.

El administrador de políticas QPM (QoS Policy Manager) de los enrutadores Cisco, tiene una interfase grafica para administrar QoS en la red. En el RFC 2748, se propone un modelo cliente-servidor en el que se definen las políticas de control sobre los protocolos de señalización de QoS.

3.5.1 QoS en Ethernet.

El primer intento para tratar QoS en LAN aparece con la especificación 802.1D, que define la arquitectura del protocolo para conmutadores de capa 2 que operan al nivel de Media Access Control (MAC) 802.1D usa dos parámetros, *user priority* y *access priority*. En el caso de Ethernet (802.3) y LAN inalámbrica (802.11), no tienen soporte para prioridad, por lo que se tiene que hacer un mapeo de estos parámetros de prioridades a clases de tráfico usando IEEE 802.1Q.

Algunos conmutadores tienen la capacidad de proveer QoS en la capa 2, en esta capa el Frame usa la clase de servicio (CoS Class of service) de 802.1 que es el estándar de Ethernet. CoS usa 3 bits como en el encabezado de IP, y lo mapea de la capa 2 a la capa 3 y viceversa.

Los conmutadores tienen la capacidad de diferenciar estructuras (frames) basadas en CoS. Si múltiples filas de espera están presentes, las estructuras pueden ser puestas en diferentes filas de espera y ser despachadas con preferencia. Esto permite tener diferentes niveles de servicio para cada fila de espera. WRED usa estos valores como el punto de partida cuando un paquete será descartado en la capa 3.

Algunas implementaciones proveen mapeo de ToS (o precedencia de IP) a CoS, en el que la estructura de Ethernet puede ser mapeado al bit de precedencia de IP, esto provee prioridad de flujo de punto a punto.

3.5.1.1 SNA ToS

SNA ToS en conjunto con la conmutación en la capa de datos, permiten el mapeo de la clase de servicio de SNA en servicio diferenciado IP. DLSW abre cuatro sesiones y se mapea cada tráfico de SNA en cada una.

3.5.2 QoS para voz en paquetes.

Una de los usos más promisorios para redes IP es el permitir el tráfico de voz, esto puede ayudar a reducir el costo de las comunicaciones al compartir la infraestructura de datos actual.

Existen diversas soluciones de productos y tecnologías, incluyendo VoIP (Voice over IP), para proveer la calidad de voz requerida, se debe agregar la capacidad de QoS.

Las empresas pueden reducir sus costos en comunicación de voz combinando el tráfico de voz en su red existente de IP. El tráfico de voz se digitaliza en módulos de voz en procesadores 3600 de Cisco, Este tráfico puede ser enrutado vía el protocolo H.323 el cual requiere un QoS específico. En este caso la precedencia IP se define como alta para tráfico de voz. WFQ se habilita en todas las interfases de los enrutadores de esta red. WFQ automáticamente hace el cambio a alta precedencia reduciendo el retraso para este tráfico. En tráfico lento menor a una línea T1/E1, los paquetes de voz pueden ser forzados a esperar por los paquetes más grandes, lo que agrega decenas o cientos de milisegundos al retraso. Se puede usar LFI en conjunto con WFQ para romper estos datagramas grandes e intercalar el tráfico de voz para reducir este retraso.

3.5.3 QoS para video

Uno de los retos más grandes para las redes basadas en IP es el video dividido en paquetes, el cual ha sido provisto sólo en servicio del mejor esfuerzo, el cual provee algún tipo de garantía para diferentes tipos de tráfico. Esto ha sido un reto para aplicaciones de video el cual requiere una cantidad de ancho de banda reservado.

Se puede usar RSVP en conjunto con circuito virtual privado ATM para proveer ancho de banda garantizado en algunos lugares. RSVP se configura en el software del enrutador para proveer diferentes vías desde las redes de un enrutador, en los extremos y a través del núcleo de ATM.

La simulación de tráfico usa estas vías para satisfacer estas restricciones de simulación en tiempo real. Estas máquinas habilitadas para video también usan estas redes

para hacer videoconferencias en vivo. En estos casos los enlaces ópticos ATM OC-3 que son configurados con múltiples circuitos virtuales de 3Mbps conectados a varios sitios. RSVP asegura que el QoS para este circuito virtual es apropiado.

3.6 Monitoreo de niveles de servicio en una red

Una vez que está habilitado QoS en una red, necesitamos entender como se está comportando. Múltiples clases de tráfico hacen esto un reto. El saber la capacidad de un enlace alguna vez fue suficiente, pero ahora necesitamos considerar el enlace en términos de filas de espera, prioridades y reservaciones. Herramientas confiables como "traceroute" y "ping" pueden ser usadas en nuevas maneras para entender la salud de la red. [Croll, 2000]

3.6.1 Acuerdos de nivel de servicio

Un acuerdo de nivel de servicio era históricamente una medida de disponibilidad de red para describir la relación entre un cliente y un proveedor de servicio a Internet (ISP) Cuando los enlaces WAN eran circuitos, el retraso y el flujo estaban dados, y solo se tenía que cuidar la disponibilidad. Mientras la mayoría de los acuerdos de servicio de ahora tienen que ver con disponibilidad y métricas de tiempo para reparación, y están siendo extendidas para incluir latencia, velocidad de travesía (throughput), CIR (Committed Information Rate), niveles pico, promedio sostenido de tráfico sostenido y retaso (jitter) [Croll, 2000]

La mayoría de los sistemas de acuerdo de servicio, dependen de múltiples "ping". Estos deben ser monitoreados sobre un periodo razonable de varias semanas. Este monitoreo también ayuda a visualizar tendencias cíclicas y la disponibilidad con frecuencia diaria o semanal.

3.6.2 Monitoreo de aplicaciones (Sniffer)

Los sistemas de monitoreo modernos (sniffers) pueden buscar tráfico en un segmento de red y analizar el tiempo de respuesta tomando en consideración las necesidades de la aplicación. El beneficio de estos dispositivos es que no son intrusivos, porque no tienen acceso a información que el cliente y el servidor tienen. Una vez que los sniffers están integrados con los sistemas de directorio, pueden traducir los bits que ven en usuarios y grupos, y son por lo tanto más fáciles de entender. [Croll, 2000]

En redes conmutadas, los sniffers pueden ser puestos cerca del cliente o del servidor para generar información más útil, pero puede ser costoso poblar la red con estos sistemas, con el uso de información de RMON2 en los dispositivos de red, los sistemas de administración serán capaces de generar grandes cantidades de información sin hardware adicional. Puede ser difícil justificar instrumentación independiente en una red cuando las capacidades ya están puestas en los dispositivos como enrutadores. El problema con RMON y RMON2 es que generan tráfico sobre la red, lo que los hace poco apropiados para redes altamente congestionadas [Croll, 2000]

3.6.3 Agentes cliente

Los agentes de software prueban la pila del cliente para generar información valiosa, estos agentes buscan más a profundidad en las necesidades de la aplicación y el ambiente del cliente, como en el caso de aplicaciones que corren concurrentemente. A diferencia de un Sniffer que puede ver nada más que tráfico lento en un segmento, un cliente puede ver tráfico que va a otros lugares en la red. Estos clientes son muy útiles en el ambiente de computadoras de escritorio porque reportan el nombre del usuario en lugar de solo la dirección IP, porque se instalan en el nodo final y pueden ser activados remotamente por un operador para funciones simples de monitoreo y diagnóstico desde el comando ping y traceroute.

Las desventajas de los agentes cliente es que se tiene que instalar software en la computadora de escritorio, y puede introducir inestabilidad o hacer más lento el procesamiento o inducir retrasos. Y solo revela información de la máquina donde está instalada, por lo que es más difícil obtener una visión general de la red. [Croll, 2000]

3.6.3.1 Simulación de cliente

Los simuladores de cliente consultan aplicaciones en intervalos regulares y son capaces de medir la respuesta del servidor y características de red. La desventaja es que la simulación no puede medir el uso actual, por ejemplo en el caso de páginas html creadas dinámicamente, el simulador cree que es una página estática. Estos simuladores inducen retrasos por que crean más tráfico, por lo que los administradores deben balancear cuidadosamente la necesidad de profundidad de información que es requerida. [Croll, 2000]

Algunas organizaciones independientes ofrecen servicios de reportes que pueden calificar el desempeño de aplicaciones críticas como sitios Web, pidiendo la página en intervalos regulares, se obtiene un promedio del tiempo de respuesta y lo reporta a los administradores del sitio. [Croll, 2000]

3.6.4 Monitoreo activo y agentes de servidor

Un dispositivo de red o un posicionador de recursos virtuales, como un balanceador de carga, tiene acceso a todas las características de tráfico para un determinado servicio virtual. Un balanceador de carga conoce exactamente cuánto retraso se tiene desde el servidor y cuánto es inducido por la red. Para algunos enrutadores es necesario entrar en modo de depuración (debug) para poder monitorear, lo que introduce sobrecarga al procesador.

Los monitores activos pueden ser parte de aplicaciones de servidor, también pueden funcionar como agentes que residen en el servidor y vigilar servicios específicos, verifican la carga y métricas de salud y mantienen contadores y promedios para las aplicaciones. [Croll, 2000]

3.6.5 Métricas

Existen ciertos parámetros que se pueden usar para caracterizar la salud de un servicio. La clasificación del tráfico para manejo de filas de espera, profundidad de la fila de espera y seleccionador de rechazos pueden ser hechos de acuerdo a un número de métricas de tráfico. Una de las métricas más útiles es tomada del mundo ATM. [Croll, 2000]

Las características fundamentales de un servicio son latencia, jitter, confiabilidad, capacidad de manejar ráfagas y volumen de tráfico, si se conocen estos parámetros para un servicio, se tendrá un buen entendimiento de la salud de una red. [Croll, 2000]

Latencia: Se puede probar la respuesta de una red de tres maneras. Un simple "ping" es una medida de la latencia. Una prueba TCP (que involucra el abrir una sesión TCP y medir el tiempo de respuesta) mide un proceso específico del servidor. Finalmente una prueba de aplicación (que involucra una interacción completa de una aplicación como el pedir una página WEB) muestra el comportamiento real del servicio. [Croll, 2000]

Es importante el hacer las diferentes pruebas, por ejemplo, un servidor WEB cargado casi a su totalidad, es posible que responda al comando ping con relativa rapidez, pero al pedir una página WEB, es posible que tarde más.

Jitter: Es el reflejo de la inconsistencia del retraso. Altos niveles de jitter indican profundidad variable en filas de espera, que es un síntoma de congestión de tráfico en algunos cuellos de botella. Por otro lado, un nivel muy bajo de jitter para una clase de servicio en particular significa que esta clase tiene ventaja desproporcionada contra otras clases, lo que significa que se deben ajustar los pesos de cada clase. [Croll, 2000]

3.6.6 Monitoreo de condición de red con herramientas tradicionales

La manera tradicional de monitorear una red es midiendo la utilización. Hay varios problemas con esta aproximación, porque no brinda información que tenga gran utilidad en una red con clases de servicio, y no hace énfasis en el tiempo de viaje redondo ni del desempeño y no trabaja al nivel de aplicación. Existen varias maneras de solucionar estos problemas. Las redes de próxima generación están basadas en acuerdos de nivel de servicio que resultan del ping, traceroute, pruebas de TCP y aplicaciones, pruebas de reservación.

Utilización: Esta herramienta es común para planeación de capacidad y medición de salud de la red. La utilización varía según el tipo de enlace. Los sistemas basados en colisiones como Ethernet requieren un nivel de congestión sostenido que es mucho menor que el en teoría debe tener. [Croll, 2000]

Ping y QoS: El RFC 1700 indica que la petición de mensajes de eco que puede ser especificada con cualquier configuración de IPTOS (Byte de tipo de servicio en el encabezado de IP, dentro de este byte se destinan 4 bits para el manejo de tipo de servicio), aunque no cubre la precedencia. Un ping puede ser usado para caracterizar un tipo de servicio en una red porque la función que asigna políticas, no sobrescribe ni ignora los valores TOS. Por ejemplo, si un enrutador es configurado para tratar ping como un mensaje

de control de la red y altere la configuración TOS, entonces un ping puede obtener un excelente tiempo de respuesta, cuando de hecho la clase de tráfico en cuestión está experimentando congestión. [Croll, 2000]

Hay algunos moderadores de tráfico "firewalls" que rechazan las peticiones de ping o traceroute.

Traceroute y QoS: Un método para manejo preferencial puede ser el rutear diferentes clases de tráfico sobre diferentes trayectorias de red. La selección de la ruta se puede hacer basado en los estados dinámicos del enlace como rendimiento o carga, las trayectorias a través de la red pueden cambiar [Croll, 2000]

El problema es la señalización de la red, para que un paquete de traceroute pueda ser tratado como una aplicación con cierta clase.

3.6.7 Indicadores de rendimiento clave para redes con políticas

Algunas métricas críticas no son muy útiles. Las métricas de nivel de red permiten definir limites en sistemas de red administrados que pueden monitorear información de RMON, RMON2 o SNMP.

3.7 De quién es la responsabilidad

El precio del ancho de banda ha estado disminuyendo, se puede tener la tentación de simplemente agregar una conexión con más ancho de banda para mejorar el tiempo de respuesta de las aplicaciones en la red, bajo estas circunstancias todas las aplicaciones tendrían más ancho de banda utilizable, dejando las aplicaciones criticas y de tiempo real compitiendo con las otras. Sin un cuidado en la administración del ancho de banda, el tráfico de HTTP puede hacer imposible la implementación de voz sobre IP en la misma red.

Con el uso de herramientas de administración de ancho de banda, se puede habilitar la red para soportar más usuarios y aplicaciones porque se le dan un ancho de banda de acuerdo a su prioridad, la cual es determinada por los requerimientos de cada aplicación.

Este método ahorra en el costo del ancho de banda, elimina la necesidad de comprar más equipo, administrar otros equipos, invertir en más herramientas de diagnostico y tener personal más entrenado. Las compañías grandes prefieren tomar la responsabilidad de la función de calidad de servicio y requieren solo conectividad básica del proveedor de servicio, el problema es que los administradores pueden fácilmente tener problemas al hacer configuraciones manuales de calidad de servicio. El uso de administración de ancho de banda hace esta tarea tediosa y se pueden cometer errores.

Algunas soluciones están disponibles como software que se instala en los enrutadores en los extremos de la red, otros se implementan en hardware que requieren la compra de servicios dedicados que también se colocan en los extremos de la red. En cualquiera de los dos casos, estas interfaces permiten a los administradores definir distintas

clases de servicio para las diferentes aplicaciones y los dispositivos en los extremos saben como manejar los distintos tipos de tráfico.

Algunas compañías pequeñas que tienen recursos restringidos, pueden suscribir servicios administrados de un proveedor de comunicaciones integrales (PSI) que se manejan a través de IP, ATM y Frame Relay y de esta manera manejan las diversas aplicaciones de negocio que pueden estar en diferentes lugares. El PSI configura, instala y administra el equipo de acceso del cliente así como los enlaces, asegurando el funcionamiento óptimo de todas las aplicaciones. El desempeño debe ser respaldado con un contrato de nivel de servicio, reportes administrativos y servicios de mantenimiento.

Las compañías pequeñas y medianas pueden ser administradas con un PSI, con la ventaja que el PSI puede usar una red diferente como IP, ATM o Frame Relay para cada tipo de servicio, aun para llamadas de voz.

La consolidación de múltiple tipos de tráfico y la asignación de calidad de servicio para cada aplicación resulta en el uso de ancho de banda eficiente, tiempo de respuesta adecuado y ahorros de costos por no tener infraestructura y servicios desperdiciados, aparte de que se tiene la ventaja que es un solo proveedor, un solo contacto y un solo recibo mensual.

El PSI puede dividir el tráfico diferenciado por el protocolo a través de redes separadas, esto puede ser una ventaja cuando una compañía quiere conectividad a 10Mbps a Internet, en este caso, el PSI puede tomar el tráfico de IP de la compañía y pasarlo a través de redes multiservicio como un circuito virtual permanente de ATM configurado para un tráfico con tasa de transferencia constante, lo que asegura un flujo de tráfico suave hasta el próximo punto de acceso en la espina dorsal (backbone) de Internet.

Otra ventaja es que las compañías pequeñas, toman ventaja que usan la tecnología más apropiada y pueden migrar fácilmente como sus necesidades lo requieran, sin tener que negociar con múltiples proveedores de servicio, equipo e integradores de servicios de telecomunicaciones.

4. QoS EN IP (INTERNET PROTOCOL)

4.1 QoS en IPv4

En IPv4 se usa el bit de precedencia en el IP TOS del encabezado del protocolo, como un método para marcar los paquetes y distinguirlos. Como se menciona en el capítulo 2, el campo de TOS es parte de la especificación de IP desde el principio de desarrollo del protocolo pero se ha usado poco en el pasado. La semántica de este campo esta documentada en el RFC1349 del IETF "Tipo de servicio en el Internet Protocol Suite" el cual sugiere que los valores especificados en este campo sean usados para determinar la manera en como se tratan los paquetes con consideraciones monetarias. Por lo menos dos protocolos de ruteo, incluyendo OSPF (Open Shortest Path First) [RFC 1583] e IS-IS [RFC 1157] pueden ser configurados para calcular trayectorias por separado para cada valor especificado de TOS.

El campo de 4 bits de TOS se describen en el RFC791 original donde cada bit tiene su propio significado. El RFC 1349 intenta redefinir este campo como un conjunto de bits que se describen como sigue:

- 1000 Minimizar retraso
- 0100 Maximizar "throughput"
- 0010 Maximizar confiabilidad
- 0001 Minimizar costo monetario
- 0000 Servicio normal.

El problema con el campo de precedencia de IPv4, surge al suministrar el paquete al enrutador, donde hay la posibilidad que miles de flujos activos sean procesados antes que entre el que tiene prioridad y hasta entonces aplicar la regla que diferencia ese tipo de flujo.

La manera como se acomoda el campo TOS dentro del encabezado de IPv4 se muestra en la figura 4.1

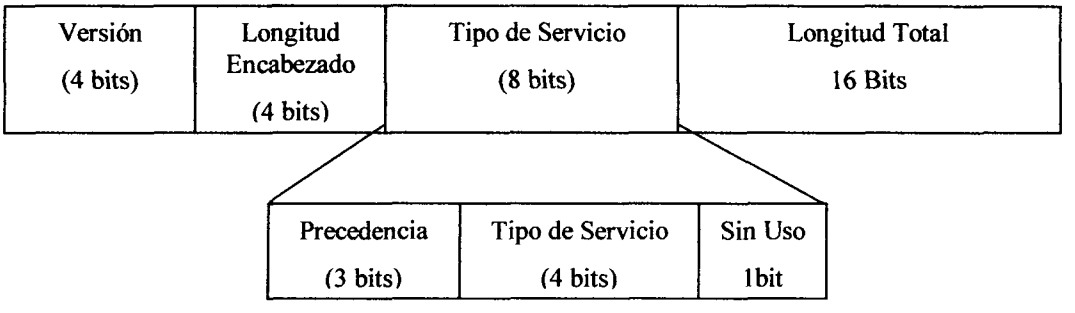


Figura 4.1 Campo TOS de IPv4

4.2 QoS en IPv6

IPv6 tiene mejoras a la especificación de IPv4, aunque IPv6 tiene integrados conceptos de QoS, no es una de las grandes mejoras que hay entre los dos protocolos.

Existen dos componentes del protocolo IPv6 que pueden proveer un método para diferenciar clases de servicio CoS. El primero es un campo de prioridad de 4 bits en el encabezado de IPv6, que es funcionalmente equivalente a los bits de precedencia de IPv4, el cual puede ser usado para discriminar tipos de tráfico basado en el contenido de su campo. El segundo componente es una etiqueta de flujo, la cual fue agregada para habilitar el etiquetado de los paquetes que pertenecen a flujos de tráfico particulares, en los que, el que envía debe pedir un manejo especial como el flujo para tráfico en tiempo real. En la figura 4.2 se muestran las etiquetas del encabezado. [León-García, 2000]

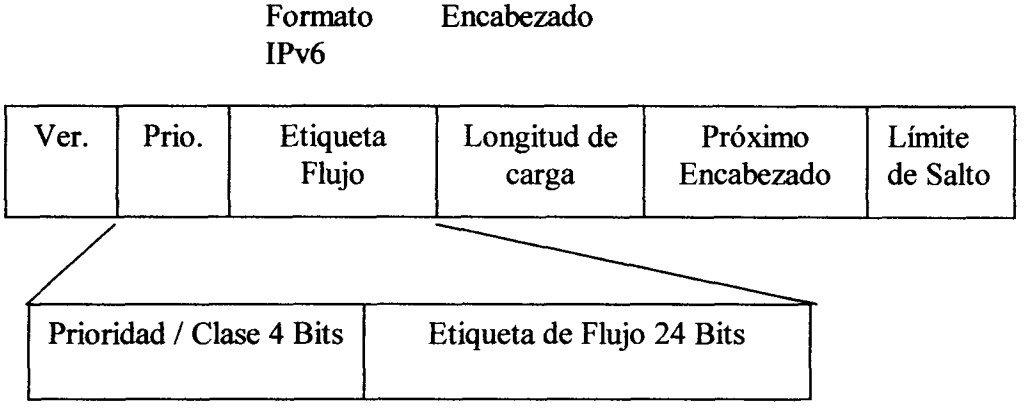


Figura 4.2 Etiqueta de prioridad y flujo en el encabezado IPv6

El campo de prioridad de 4 bits en el encabezado IPv6, fue diseñado para permitir que el tráfico de la fuente identifique la prioridad de envío de sus paquetes, como se compara con otros paquetes de la misma fuente de tráfico. Con los 4 bits obtenemos un rango de 0 a 16, del 0 al 7 especifica la prioridad del tráfico, valores de 8 a 15 especifica que en tráfico no responda a situaciones de tráfico como las de tráfico de tiempo real mandados a una tasa constante. Para tráfico controlado contra congestión [RFC1883], la IETF recomienda usar los valores de prioridad listados en la tabla 5.2.

Valor	Categoría
0	Tráfico sin categoría
1	Tráfico de relleno (NNTP)
2	Transferencias sin atención (SMTP)
3	Reservado
4	Transferencias en masa atendidas (FTP, NFS)
5	Reservado
6	Tráfico Interactivo
7	Tráfico de control de Internet (SNMP)

Tabla 4.1 Valores de prioridad para categorías de aplicaciones

4.2.1.1 Audio en tiempo real basado en QoS.

El audio en tiempo real es un componente importante en multimedia de Internet, sin embargo el Internet actual basado en IPv4 tiene poca eficiencia para transmitir este tipo de contenido debido a la falta de capacidad de manejar conceptos de calidad de servicio. IPv6, como he mencionado anteriormente, es el nuevo protocolo para Internet e incorpora el manejo de calidad de servicio. El encabezado de IPv6 tiene una etiqueta de flujo que permite la clasificación de los paquetes de acuerdo con su destino y servicio. Los protocolos de reservación RSVP (Resource Reservation Protocol) pueden hacer uso de este Identificador para reservar recursos para flujos en particular en los enrutadores que se encuentren en la trayectoria del paquete.

5. QoS EN ATM

5.1 QoS en ATM

ATM puede proveer QoS a diferentes conexiones, esto requiere que un contrato de servicio sea negociado entre el usuario y la red cuando se establece la conexión. Se requiere que el usuario describa el tráfico que utilizara y el QoS requerido cuando pide una conexión. Si la red acepta la petición, un contrato es establecido que garantiza el QoS si el usuario cumple con su descripción de tráfico. Los mecanismos de filas de espera con prioridad y organización implementados en los conmutadores ATM, proveen la capacidad de entregar QoS.

Para cumplir con los compromisos de QoS, la red ATM usa mecanismos de monitoreo para que se cumplan con las políticas del contrato de la conexión y puede descartar paquetes que no cumplan con el acuerdo.

Se pueden tener dos tipos de conexiones, punto a punto y punto a multipunto. Las conexiones punto a punto pueden ser unidireccionales o bi-direccionales. En el caso de los bi-direccionales, se pueden tener diferentes requerimientos de QoS para cada dirección. Las conexiones punto a multipunto siempre son unidireccionales.

5.1.1 Administración de tráfico y QoS

La administración de tráfico esta involucrada con la entrega de QoS para flujos de paquetes específicos. Vincula mecanismos para administrar los flujos de una red para controlar la carga que se aplica a varios enlaces y conmutadores, también involucra la definición de prioridad y organización en conmutadores, enrutadores y multiplexores para proveer trato diferenciado para paquetes y celdas pertenecientes a diferentes clases, flujos o conexiones. También se pueden involucrar las políticas de flujo de tráfico en cuanto entren paquetes en la red.

Para cumplir con los requerimientos de QoS, un conmutador multiplexor o ATM debe implementar estrategias para administrar como las celdas o paquetes son puestos en filas de espera, así como controlar las tasas de transmisión que son provistas a los diferentes flujos de información.

Dentro de estas estrategias tenemos:

- **FIFO y filas de espera con prioridad**
- **Filas de espera equitativas**
- **Filas de Espera equitativa con pesos**
- **QoS y conmutación en ATM**

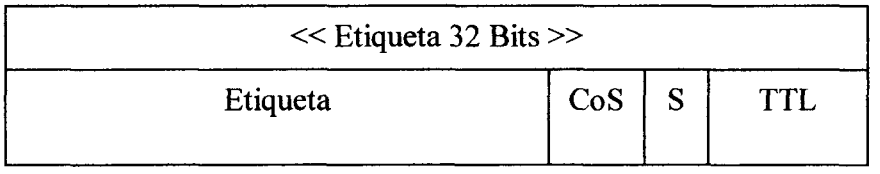
Una aspecto que se debe considerar es la integración de la capa 2 de conmutación en nuevas etapas de la topología de la red. Con la introducción de ATM y Frame Relay en las redes WAN, ha sido más difícil aislar las fallas de red y proveer administración de red.

ATM y Frame Relay tienen la flexibilidad de proveer circuitos virtuales entre dos puntos cualquiera de una red conmutada, sin importar el número de conmutadores de capa 2 en el camino entre los dos puntos. Aunque esto tiene mucha flexibilidad, tiene la desventaja que se pueden crear muchas redes de manera inadecuada o con descuidos. En redes más grandes, no se debe intentar usar dispositivos de capa 3 o enrutadores aunque solo estén a un salto (hop) uno del otro, porque dependiendo de protocolo de ruteo usado, puede introducir inestabilidad en el sistema de ruteo y si la red sigue creciendo, se requieren excesivos cálculos para mantener la tabla de ruteo de nodos adyacentes. Todos estos aspectos tienen gran importancia en la implementación de QoS en una red.

6. QoS EN MPLS

QoS tiene muchas posibilidades con MPLS, una de las más directas es la posibilidad de mapear los 3 bits de precedencia de IP que vienen en el encabezado del paquete IP entrante, al campo de CoS, como lo propone Cisco en su contribución a la estandarización de MPLS.

En cuanto los paquetes IP entran en el ambiente MPLS, el enrutador MPLS es responsable de mapear los bits de IP que se refieren a CoS dentro del encabezado de MPLS. Como se muestra en la figura 6.1



Etiqueta 20 bits

Clase de Servicio (CoS) 3 bits

Fondo de la pila (S) 1 bit

Tiempo para vivir 8 bits

Figura 6.1 Bits de clase de servicio en la etiqueta MPLS

Otro de los usos de MPLS es la capacidad de construir trayectorias explicitas "label switched", la cual da a los administradores la capacidad de definir trayectorias explicitas en una nube MPLS. Funciones como esta pueden definir una ingeniería de tráfico que contribuye a mejorar la calidad del servicio. Como resultado un método para ofrecer servicios diferenciados puede ser posible.

Pueden existir varias trayectorias paralelas de un extremo de la red MPLS a otro, las cuales pueden ser diferentes en ancho de banda y utilización, para lo cual es posible definir trayectorias que puedan ser escogidas para un CoS específico. Cada trayectoria ofrece una característica diferenciada. El tráfico etiquetado con CoS más alto puede ser entregado en otra línea de alta velocidad, con menos retrasos y el tráfico con CoS bajo puede ser servido en otra línea de menor velocidad. En este ejemplo se muestra como se da servicio diferenciado con MPLS. Existen diversas aproximaciones porque la especificación MPLS de la IETF sugiere que cualquier implementación que cumple con MPLS debe ser ínter operable con RSVP. Aunque este mandato no significa explícitamente que MPLS debe proveer entrega explicita del camino a través de una red en respuesta de los mensajes RSVP, el cual podría ser material para otro estudio.

7. ESQUEMAS DE INTERCONEXIÓN

El Internet corre más rápido y se incrementa de tamaño, pero su arquitectura básica permanece sin cambio desde sus inicios. Todavía opera como una red de datagramas donde cada paquete se entrega independientemente a través de la red. El tiempo de entrega de los paquetes no está garantizado y hasta pueden ser perdidos debido a la congestión dentro de la red. Esta falta de predicción no combina bien con nuevas aplicaciones como telefonía por Internet o conferencias por video digital, los cuales no pueden tolerar retrasos, jitter o pérdida de datos en la transmisión.[Wang, 2001]

Para solucionar estos problemas, la Internet Engineering Task Force ha desarrollado nuevas tecnologías y estándares para proveer recursos y diferenciar servicios en el Internet, bajo el concepto de Calidad de Servicio (QoS) Estas tecnologías las podemos dividir en dos esquemas. La primera es para asignación de recursos y la segunda es para optimización de rendimiento.

Asignación de Recursos: Esta se refiere a la asignación de recursos bajo el esquema de Servicios Integrados o Servicios Diferenciados.

Optimización de Rendimiento: Son herramientas de administración a proveedores de servicio, para ancho de banda y optimización de rendimiento. Usan el esquema de MPLS e Ingeniería de tráfico.

Con estas tecnologías podemos generar arquitecturas de red más avanzadas, y se usan también tecnologías que se han discutido previamente: IP y ATM. "IP fue diseñado para proveer funciones de interconexión de red capaz de correr sobre tecnologías de red variadas. ATM fue diseñado para proveer calidad de servicio (QoS) punto a punto." [León-García, 2000]

7.1 Asignación de Recursos

7.1.1 Servicios Integrados

El modelo de servicios integrados fue el primer intento para ofrecer QoS en Internet. Debido a que se tienen problemas con el modelo de entrega de paquetes en el esquema de mejor esfuerzo, el empuje real para arquitecturas de servicio mejorada empezó a principios de los años noventa, después de experimentos con video conferencia en Internet. Las aplicaciones en tiempo real son sensibles a retrasos de datos y no trabajan bien en Internet donde la latencia es típicamente impredecible. Por lo que los requerimientos de estas aplicaciones requieren un nuevo tipo de servicio que provea un nivel de aseguramiento de recursos a las aplicaciones[Wang, 2001]

El esquema de Servicios Integrados está basado en reservación de recursos por flujo, es decir, una aplicación debe hacer reservación antes de transmitir en la red.

En el proceso, la aplicación debe especificar sus requerimientos de recursos, posteriormente la red usa un protocolo de ruteo para encontrar un camino basado en los

recursos solicitados. Se usa un protocolo de reservación para instalar la reservación en todo el camino. En cada salto, el control de admisión verifica si hay suficientes recursos disponibles. Una vez que se establece la reservación, la aplicación puede empezar a enviar tráfico sobre el camino que tiene uso exclusivo de los recursos.

Los Servicios Integrados son enfocados para aplicaciones de larga duración y sensitivas al retraso. El uso del WEB domina el Internet y su tráfico es de transacciones de corta duración, por lo que no se recomienda usar estos servicios para WEB. Aparte que cada reservación requiere contabilizarse entre diferentes proveedores de servicio y por lo tanto aquellos que hacen una reservación tienen que pagar. [Wang, 2001]

El modelo de servicios integrados requiere un enrutador para mantener un estado de flujo específico para cada flujo que mantiene el enrutador, este requerimiento trae algunos problemas, como el que la cantidad de información almacenada se incrementa proporcionalmente con el número de flujos, por lo que los enrutadores necesitan espacios de almacenamiento grandes y gran poder de procesamiento, después nos encontramos con el problema que el modelo de servicios integrados puede hacer que los enrutadores se conviertan en algo muy complejo porque necesitan implementar el protocolo RSVP, control de admisión, clasificador de paquetes, aparte de algoritmos sofisticados para el organizador de paquetes. Debido a la escalabilidad y complejidad asociadas con el modelo de servicios integrados, la IETF introdujo otro modelo de servicio llamado modelo de servicios diferenciados (DS), el cual debe ser más simple y más escalable.

Para proveer diferentes grados de QoS, la IETF desarrollo el modelo de servicios integrados, que requiere recursos como ancho de banda y búferes reservados explícitamente para un flujo de datos dado, para asegurar que la aplicación recibe el QoS requerido. El modelo requiere el uso de clasificadores de paquetes para identificar flujos que se reciben con un cierto nivel de servicio, también requiere el uso de organizadores de paquetes para manejar los envíos de diferente manera que asegure que se cumplen los requerimientos de QoS. Un control de admisión se requiere para determinar si un enrutador tiene los recursos necesarios para aceptar un nuevo flujo, por lo que el modelo de servicios integrados es análogo al modelo ATM donde el control de admisión se acopla con políticas que proveen QoS a aplicaciones individuales.

El protocolo de reservación (RSVP) se usa en los servicios integrados para proveer los mensajes de reservación requeridos para ajustar un flujo con el QoS requerido en la red. RSVP es usado para informar a cada enrutador de la petición de QoS y si el flujo se encuentra admisible, cada enrutador ajusta su clasificador de paquetes para manejar dicho flujo de paquetes.

Un descriptor de flujo se usa para describir el tráfico y los requerimientos de QoS de un flujo, este descriptor de flujo consiste en dos partes: Una especificación de filtro (filterspec) y una especificación de flujo (flowspec), el primero provee la información requerida por el clasificador de paquetes para identificar los paquetes que pertenecen al flujo. El segundo consiste en una especificación de tráfico (Tspec) y una especificación de petición de servicio (Rspec) El Tspec especifica el comportamiento del tráfico de un flujo en términos de cubo

de tokens (token bucket) El Rspec especifica el QoS requerido en términos de ancho de banda, retraso de paquetes o pérdida de paquetes.

7.1.1.1 Servicio Garantizado

Provee retraso determinístico en el peor caso a través de control de admisión estricto y programación de paquetes en filas de espera con peso balanceado. Es diseñado para aplicaciones que requieren garantía absoluta de retraso [Wang, 2001]

El servicio garantizado puede ser usado para aplicaciones que requieren servicio de entrega en tiempo real, para lograr esto, cada enrutador debe conocer las características del flujo y usa control de admisión para determinar si un nuevo flujo puede ser aceptado. Una vez que el flujo es aceptado, el enrutador debe aplicar una política de flujo para asegurar que se cumplan las características prometidas de tráfico.

7.1.1.2 Servicio de carga controlada

Provee una garantía menos firme, más cercana a una red de mejor esfuerzo. RSVP es estandarizado para señalizar requerimientos de aplicación y reservar recursos en el camino. [Wang, 2001]

El servicio de carga controlada, fue diseñado para proveer aproximadamente el mismo servicio que el "servicio de mejor esfuerzo" en condiciones de carga de red ligeras, pero este opera en condiciones de red más severas, aunque no se especifican valores de retraso predeterminados o pérdidas.

Este servicio esta diseñado para aplicaciones adaptivas que pueden tolerar algún retraso, pero son sensitivas a condiciones de sobrecarga en la red. Estas aplicaciones se comportan satisfactoriamente en condiciones de carga ligera en la red, pero se degradan significativamente cuando la red esta muy cargada.

La implementación de este servicio tiene menos complejidad que el servicio garantizado, porque carece de especificaciones de retraso y pérdida.

Una aplicación que solicita el servicio de carga controlada, tiene que proveer a la red con la especificación del cubo de tokens (token bucket) de su flujo. La red usa políticas de control de admisión para asegurar que hay suficientes recursos disponibles para el flujo, de esta manera, los flujos que cumplen con la especificación del token bucket deben ser servidos con bajo retraso y poca pérdida, mientras que los que no cumplen con él, se tratan con el servicio de mejor esfuerzo.

7.1.1.3 RSVP

RSVP es el acrónimo de **ReSerVation Protocol**, fue diseñado como un protocolo de señalización IP para el modelo de servicios integrados. RSVP puede ser usado como un host para pedir un cierto recurso con QoS para un flujo en particular y para solicitar al enrutador en turno el QoS en todo el camino.

IP no tiene ningún protocolo de señalización, por lo que RSVP fue diseñado con libertad desde su inicio.

Tiene las siguientes características:

- Hace reservación de recursos para aplicaciones unicast y multicast (multipunto a multipunto), adaptándose dinámicamente a cambios en rutas.
- Solicita recursos en una dirección desde el que envía al que recibe y también hay reservación de recursos bidireccional que requiere que ambos sistemas inicien reservaciones separadas.
- Requiere que el receptor inicie y mantenga la reservación de recursos.
- Mantiene el mismo estado en cada enrutador intermedio, porque la reservación de recursos se mantiene en un enrutador por un tiempo limitado, así que el que envía, debe pedir la reservación frecuentemente.
- No se requiere que cada enrutador tenga implementado RSVP, pero estos enrutadores usan la técnica de entrega con mejor esfuerzo.
- Provee diferentes estilos de reservación, así que las peticiones pueden ser enviadas de varias maneras de acuerdo a las aplicaciones.
- Funciona con IPv4 e IPv6.

Para habilitar la reservación de recursos como un proceso RSVP, cada nodo tiene que interactuar con otros módulos.

7.1.1.4 Reservación iniciada por el receptor

RSVP adopta el principio de reservación iniciada por el receptor, debido a que el receptor inicia la reservación de recursos. Fue diseñado para dar soporte a conferencias múltiples con receptores heterogéneos, cada receptor sabe cuánto ancho de banda necesita. Supongamos que fuera al revés el proceso, que el remitente solicitara la reservación, sería necesario obtener el requerimiento de ancho de banda de cada receptor, lo que podría causar congestión de información para grupos grandes de receptores.

Un problema que se genera con este tipo de reservación es que el receptor no conoce directamente el camino tomado por los paquetes para llegar al remitente, para solucionar este problema RSVP manda mensajes que contienen el camino hasta el receptor. Una vez que ha llegado el mensaje con la información del camino, el receptor envía un mensaje al remitente usando el camino que se recibió y contiene pedimentos de reservación para los enrutadores por los que pasa hasta llegar al remitente.

7.1.1.5 Compartición de Reservaciones

Cuando hay múltiples receptores que pueden compartir una porción determinada del camino, no se reservan recursos para cada receptor, se comparten hasta el punto en que el camino de los receptores diverge. Cuando una petición de reservación se propaga hacia el remitente, esta se detiene en el punto en el que hay una reservación existente que sea igual o

mayor, por lo que la nueva reservación ya no se propaga más. Esto es útil por que se disminuye el tráfico de reservaciones.

7.1.1.6 Estilos de reservación

Existen tres estilos de reservación definidos en RSVP: filtro comodín, filtro fijo y explicito compartido.

El filtro comodín crea una reservación sencilla compartida por todos los remitentes, este estilo se puede comparar con una tubería compartida cuyo recurso es el mayor de las peticiones de todos los receptores. Este método es apropiado para aplicaciones que transmiten simultáneamente como audio conferencia.

El filtro fijo crea una reservación distinta para cada remitente, la reservación total es la suma de cada una de las reservaciones.

El estilo explicito compartido crea una reservación sencilla compartida por un conjunto de remitentes explícitos. Cuando las peticiones de reservación son juntadas, se selecciona la mayor y se hace esa petición.

7.1.1.7 Estado por temporizador (soft state)

Los estados de reservación son mantenidos por RSVP, cada nodo se refresca periódicamente usando mensajes Path y Resv, cuando un estado no es refrescado dentro de un tiempo definido, el estado se borra. El estado que es mantenido por un temporizador se llama "soft state" en contraste con el "hard state" donde el establecimiento y borrado son explícitamente controlados por mensajes de señalización.

Debido a que los mensajes RSVP son enviados como datagramas IP sin requerimientos de confiabilidad, se pueden tolerar pérdidas ocasionales si por lo menos uno de cada tres mensajes llega correctamente. Para evitar la sincronización periódica de los mensajes, el tiempo de refresco es variable usando una distribución uniforme en el rango de [0.5t,1.5t] y cada mensaje de reservación contiene el valor del tiempo correspondiente al tiempo de refresco.

7.1.1.8 Formato de mensaje RSVP

Cada mensaje de RSVP contiene un encabezado común y el cuerpo contiene un número variable de objetos que dependen del tipo del mensaje, los cuales proporcionan la información necesaria para hacer la reservación de recursos. El formato del encabezado común es como se muestra en la figura 7.1

Versión	Banderas	Tipo de Mensaje	Checksum RSVP
Tiempo de Vida		Reservado	Longitud RSVP

Figura 7.1 Encabezado común RSVP

Longitud	Clase de objeto	Subclase de objeto
Contenido del Objeto		

Figura 7.2 Formato de cada objeto RSVP

7.1.2 Servicios Diferenciados

Este esquema es desarrollado como alternativa al esquema de asignación de recursos, para redes de proveedores de servicios. A mediados de 1997, los proveedores de servicios sintieron que los servicios integrados no estaban listos para su implementación a gran escala.

A diferencia del modelo de servicios integrados que requiere que cada aplicación haga una reservación de recursos, el modelo de servicio diferenciado agrega los requerimientos completos de calidad de servicio del cliente, por lo que este debe tener un acuerdo de nivel de servicio (SLA) con el proveedor. El acuerdo de nivel de servicio es un contrato entre el cliente y el proveedor de servicio que especifica el servicio de envío que recibirá el cliente. Este acuerdo incluye un acuerdo de condicionamiento de tráfico que define servicio [León-García, 2000] PCC

[Wang, 2001] por su parte menciona que el esquema de Servicios Diferenciados, en lugar de hacer reservaciones por flujo, hace una combinación de políticas en los enrutadores del extremo de la red, aprovisionamiento y asignación de prioridad de tráfico para lograr diferenciación de tráfico. El tráfico del usuario es dividido en clases de reenvío. Para cada clase, la cantidad de tráfico que puede ser inyectado a la red es limitado en el borde o frontera de la red. Los proveedores de servicio pueden ajustar el nivel de servicio aprovisionando y controlando el grado de aseguramiento de recursos del usuario.

El enrutador de frontera o borde de la red se refiere al que interconecta la red propia del usuario con la red del proveedor de servicios, este enrutador es el responsable de mapear los paquetes a su clase apropiada de reenvío. Esta clasificación de paquetes se hace con el acuerdo de nivel de servicio entre el usuario y el proveedor. Estos nodos frontera también usan políticas para proteger la red de mal comportamiento y el tráfico que no cumpla con las políticas es descartado, retrasado o marcado con una clase diferente. Esta clase de reenvío es directamente marcada en el encabezado del paquete y cuando la red tiene congestión, primero descartará paquetes con la prioridad de descarte más alta.

Bajo el modelo de Servicios Diferenciados no se requiere reservación de recursos, por lo que no se tienen problemas de escalabilidad. Pero se tiene la desventaja que es más difícil y más caro proveer garantías determinísticas a través de aprovisionamiento que por reservación [Wang, 2001]

7.2 Optimización de Rendimiento

La Optimización del rendimiento de una red, se refiere a como organizar los recursos en una red de la manera más eficiente para maximizar la probabilidad de entrega.

La conexión entre la optimización del rendimiento y QoS puede verse menos directa comparada con la asignación de recursos, sin embargo, es un bloque fundamental para el desarrollo de QoS. Implementar QoS va más allá de solo agregar mecanismos como políticas de tráfico, clasificación y programación. Fundamentalmente se trata de desarrollar nuevos servicios en el Internet. Los proveedores de servicio deben hacer un buen caso de negocio para que los clientes estén dispuestos a pagar por los nuevos servicios y estos incrementen el retorno de su inversión en las redes. La efectividad de costo de estos nuevos servicios hace posible que las capacidades de QoS sean un factor mayor en el desarrollo de estos servicios. [Wang, 2001]

El datagrama de Internet no fue diseñado para optimizar el rendimiento de la red. Los principales objetivos de diseño fueron la escalabilidad y mantener conectividad en el caso de fallas. Los protocolos de ruteo típicamente seleccionan el camino más corto basado en algunas métricas simples como conteo de saltos o retraso. Estas aproximaciones simples no son suficientes para los fines que buscamos. El ruteo por el camino más corto no siempre usa la diversidad de conexiones disponibles en la red, de hecho el tráfico puede estar tan mal distribuido que puede generar congestión en algunos puntos de la red mientras otras partes de la red pueden estar con una carga muy ligera. La optimización del rendimiento requiere capacidades adicionales en el ruteo IP. Para administrar el rendimiento de una red es necesario tener control explícito sobre los flujos de tráfico que atraviesan la red para que puedan ser arreglados a maximizar las restricciones de recursos y utilización. MPLS tiene un mecanismo llamado ruteo explícito (explicit routing) que es ideal para este propósito. [Wang, 2001]

El proceso de optimizar el rendimiento a través de mejor control de flujos en la red y mejor aprovisionamiento se refiere a Ingeniería de tráfico, la cual usa algoritmos avanzados de selección de ruteo para formar troncales de tráfico dentro de los "backbones".

7.2.1 MPLS

7.2.1.1 Integración IP sobre ATM

Como se ha mencionado anteriormente, IP es la tecnología dominante para redes interconectadas, por lo que ATM se utiliza como una solución económica para obtener un enlace de alta velocidad, por esta razón existe mucho interés en montar IP sobre ATM. [León García, 2000]

Para mostrar como la conmutación de etiquetas puede simplificar la integración IP / ATM, se muestran las otras aproximaciones para correr IP sobre ATM y los problemas con estas aproximaciones.

7.2.1.2 IP sobre ATM (CLIP Classical IP over ATM)

En este modelo IP trata a ATM como otra subred, los conmutadores ATM no intervienen en las direcciones IP ni en los protocolos de ruteo de IP. El hacerlo de esta manera tiene la ventaja que la infraestructura de ATM e IP se pueden desarrollar independientemente. CLIP se describe en el RFC 2255 de la IETF, donde IP trata a ATM como otra subred donde están conectados hosts y enrutadores con direcciones IP, en este modelo, las subredes IP son puestas encima de la red ATM, la parte de ATM que corresponde a la misma subred de IP se conoce como "logical IP sub network" (LIS)

Todos los integrantes que se encuentran en el mismo LIS, deben usar el mismo prefijo de la dirección IP, donde se especifica el mismo número de red y número de subred. Dos integrantes que se encuentren dentro del mismo LIS se comunican directamente con un circuito virtual ATM. Cada LIS se comunica independiente de otro LIS en la misma red ATM. Para comunicarse fuera de la red LIS, se necesita un enrutador que este conectado a la misma red, por lo que miembros que pertenecen a diferentes LIS se tienen que comunicar por medio de enrutadores.

Se debe implementar un protocolo de resolución de direcciones ATM (ATM ARP) para que se pueda comunicar un nodo "A" a un nodo "B" en otra red, porque el nodo "A" no conoce la dirección ATM del nodo "B". La dirección ATM de cada host se registra en el servidor ATM ARP del mismo LIS. Cuando un host quiere tener la dirección ATM de otro host desde su dirección IP, pregunta al servidor ATM ARP por la dirección ATM, una vez que recibe dicha dirección, el host puede establecer un circuito virtual hacia el host destino y mandar paquetes sobre el circuito virtual.

Cuando el host destino pertenece a otro LIS el host establece un circuito virtual al enrutador conectado en la misma LIS, el enrutador examina la dirección IP y determina la dirección del próximo enrutador al que será transmitido el paquete, establece un circuito virtual hacia ese enrutador y así se repite el proceso hasta que el paquete llega hasta la red destino, y esa red entrega el paquete en el host que esta dentro de esa red.

7.2.1.3 Protocolo de Resolución de Próximo Salto (NHRP)

Next Hop Resolution Protocol (NHRP) habilita a una estación conectada a una red ATM para que resuelva la dirección ATM a partir de la dirección IP, permite a un host que determine la dirección ATM de otro host o enrutador desde la red ATM. El objetivo principal es encontrar el atajo más eficiente a través de la red ATM para evitar enrutadores intermediarios. Lo que la hace más eficiente para redes grandes. Esta basada en arquitectura cliente-servidor, una nube NHRP contiene entidades llamadas next-hop clients (NHC) los cuales son responsables de iniciar la resolución de los paquetes de petición.

7.2.1.4 Emulación de Red de Área Local (LANE)

LAN emulation (LANE) es una especificación del foro ATM, cuya intención es acelerar el desarrollo de ATM en las empresas. Un host usa una capa de red de protocolo

como IP sobre una LAN como Ethernet o Token Ring. LANE habilita cualquier software que corre sobre una LAN tradicional para que funcione con una red ATM sin ninguna modificación. LANE trabaja representando la capa de red con una interfase que es idéntica a la de la red tradicional, mantiene la misma interfase entre la capa de red y la capa de datos, por lo que ATM se puede hacer parecer a Ethernet o Token Ring y le da los mismos servicios a las capas superiores de red. Este comportamiento habilita a LANE para dar soporte a otros protocolos de red como IPX y AppleTalk.

Una red emulada tiene los siguientes componentes:

Conjunto de clientes de emulación (LEC), el cual reside en los sistemas terminales y tiene funciones de reenvío de datos, resolución de direcciones y funciones de control. Cada LEC es identificado por una dirección ATM única.

Servidor de emulación LAN (LES), el cual responde a las peticiones de resolución de direcciones, resolviendo las direcciones propias de la tarjeta de red (MAC) a una dirección ATM.

Servidor de transmisión y servidor desconocido(BUS): el cual maneja transmisiones (Broadcast), multicast y tráfico inicial, (antes que se establece un circuito virtual)

Servidor de configuración de emulación LAN (LECS): asigna LECS al correspondiente LES.

Las desventajas de LANE son que opera al nivel de red, por lo que es susceptible a transmisiones donde se dirigen a todos los nodos conocida como dirección broadcast. El hecho de que LANE hace que ATM esconda los detalles para la capa de red provoca que los atributos de QoS no puedan ser aplicados.

7.2.1.5 Protocolos Múltiples sobre ATM (MPOA)

Multi protocol over ATM (MPOA) fue diseñado por el foro ATM para proveer interconexión entre IP, IPX y AppleTalk sobre una red ATM.

Básicamente integra LANE y NHRP. Se usa LANE para establecer conexiones de capa 2 con el mismo LIS, y NHRP para establecer conexiones de capa 3, por lo que se habilita conexiones directas de ATM entre dispositivos MPOA, lo que hace posible usar las características de QoS de ATM.

Los dispositivos terminales (edge devices ED) reenvían paquetes entre otras redes y la red ATM, el ED contiene un cliente MPOA (MPC) que se usa principalmente para hacer circuitos virtuales. Una red MPOA puede contener dispositivos capaces de MPOA que se conectan directamente en la red ATM que incluye un MPC.

Cada enrutador contiene un servidor MPOA que usa un servidor NHRP para resolver las direcciones entre IP y ATM. Los MPC y MPS se comunican vía una red local emulada.

7.2.2 Ingeniería de Tráfico en Internet

El problema básico en ingeniería de tráfico es distribuir equitativamente el tráfico a través de la red con balanceo de tráfico y las tasas de retraso y pérdidas estén en sus puntos más bajos.

Obviamente estos objetivos no pueden ser logrados a través de ruteo IP basado en destinos porque no hay suficiente información disponible. En la ingeniería de tráfico, las técnicas avanzadas de selección de ruta comúnmente se refieren como "ruteo basado en restricciones" para poder diferenciarlas del ruteo por destino, y se usan para calcular los tráficos basados en objetivos de optimización. Un sistema de este tipo usualmente necesita información de la red completa, de su topología y de sus demandas de tráfico, por lo que la ingeniería de tráfico se confina a un dominio administrativo de red. [Wang, 2001]

Las rutas producidas por ruteo basado en restricciones son diferentes de aquellas en ruteo IP basado en destino. Por esta razón las rutas basadas en restricciones no pueden ser implementadas por reenvío basado en destino. En el pasado, algunos proveedores de servicio usaban ATM en los backbones para dar soporte a ruteo basado en restricciones. Los circuitos virtuales ATM pueden ser configurados para adecuarse a los patrones de tráfico, la red basada en IP es sobrepuesta encima de estos circuitos virtuales. MPLS ofrece una mejor alternativa porque ofrece funciones similares y puede ser integrada estrechamente con redes basadas en IP.

Los backbones de internet existentes han usado el overlay model, donde los proveedores de servicio construyen redes virtuales que comprenden una red de conexiones lógicas entre todos los nodos frontera. Usando las demandas de tráfico entre los nodos frontera como demanda, el ruteo basado en restricción selecciona las rutas de las conexiones lógicas para maximizar la utilización de la red. Una vez que son calculadas las rutas, MPLS puede ser usado para hacer conexiones lógicas con LSP's exactamente como se calcularon con el ruteo basado en restricción.

La parte negativa del modelo overlay es que no es capaz de escalarse a redes más grandes. Para configurar una red lógica con N nodos, cada nodo frontera se tiene que conectar con los otros (N-1) nodos. Esto puede agregar sobrecarga de mensajes en una red grande. Otro problema es que una topología de red completa aumenta el número de enrutadores que se comunican, por lo que un protocolo de ruteo tiene que manejarlo, la mayoría de las implementaciones actuales de protocolos de ruteo no pueden soportar un gran número de puntos (peers)

La ingeniería de tráfico sin estos problemas es todavía un reto. Una aproximación heurística que han usado algunos proveedores de servicio es ajustar la distribución de tráfico al cambiar los pesos de los enlaces en protocolos de ruteo IP. Por ejemplo, cuando un enlace está congestionado, el peso del enlace puede ser incrementado para mover el tráfico fuera de ese enlace. En teoría se puede lograr la misma distribución de tráfico que en el modelo overlay solo con manipular los pesos de los enlaces en el protocolo de ruteo de OSFP "Open Shortest Path First". Esta aproximación tiene la ventaja que puede ser fácilmente implementada en redes existentes sin cambios mayores a la arquitectura de red.

7.2.2.1 Arquitecturas de reenvío IP (IP forwarding architectures)

El crecimiento de la demanda de tráfico debido al crecimiento exponencial que ha tenido el Internet, ha saturado la infraestructura actual, lo que hace necesario tomar acciones para evitar congestión, algunos han actualizado sus backbones para enlaces con tecnología ATM, siendo necesario también actualizar los enrutadores y conmutadores para poder manejar las nuevas velocidades de los enlaces. Estos hechos han llevado a cambiar la arquitectura de los enrutadores para extender el alcance del rendimiento.

Para estas nuevas arquitecturas, [León García, 2000] las subdivide en dos categorías:

Categoría 1: mantiene el mismo tipo de enrutadores convencionales, reduciendo la congestión por cuello de botella en las interfaces de los enrutadores haciendo algunos cambios internos como el cambio a back planes más rápidos para proveer envío simultáneo de paquetes o empleando una maquina de búsqueda de IP en cada interfase. Estos cambios se usan en el diseño de los enrutadores gigabit.

Categoría 2: simplifica el proceso de búsqueda usando etiquetas cortas de longitud fija para los prefijos de IP. Con el uso de estas etiquetas usa un índice directo y puede ser procesado en hardware, lo que lo hace mucho más rápido. Este es el caso de IP sobre ATM. Esta categoría también la incluye en el "overlay model" y en el "peer model".

En el overlay model los conmutadores ATM no usan las direcciones IP y los protocolos de ruteo de IP. Este modelo sobrepone una red IP sobre una red ATM, creando dos infraestructuras de red con dos esquemas de direccionamiento y dos protocolos de ruteo. Cada host usa ambas direcciones ATM e IP que están desacopladas, por lo que se requiere un protocolo de resolución de direcciones para mapear una dirección en la otra, con la ventaja que la infraestructura ATM puede ser desarrollada independientemente de la infraestructura de IP. Ejemplos de este modelo es IP sobre ATM y protocolo múltiple sobre ATM.

En el peer model se usan las direcciones IP existentes para identificar los host destino y usa los protocolos de ruteo IP para hacer conexiones ATM. Tiene la ventaja que no requiere una resolución de direcciones para conectarse hacia espacios de direcciones enrutables y simplifica la administración de direcciones. Un nodo tiene integrado la conmutación ATM y la función de ruteo en IP, por lo que el nodo puede ser visto como un punto (peer) para otros enrutadores. Este modelo mantiene una infraestructura de red, un ejemplo de esto es MPLS.

8. IMPLEMENTACIÓN DE QoS EN DIFERENTES ESCENARIOS

Las tecnologías de Calidad de Servicio (QoS) tienen poco tiempo que fueron puestas a disposición como estándar, algunas de ellas son de 1999, por lo que la mayoría de los dispositivos de red de las compañías como conmutadores (switches) y enrutadores (routers) no tienen incorporados estas funciones. Ante las nuevas necesidades que se tienen, debido principalmente a aplicaciones como telefonía IP, videoconferencia y control de tráfico, es necesario implementar Calidad de Servicio en la red de telecomunicaciones y de esta manera evitar aumentar el ancho de banda actual.

En este apartado se hace un análisis para implementar QoS en diferentes escenarios, tomando como base la tecnología más adecuada para la aplicación y después se considera su costo. Se tratarán de cubrir los tres escenarios principales que se tienen como administrador de redes con el fin de sugerir, basado en costos y necesidades, la tecnología que más se adecua a la situación.

- El primer escenario es cuando se cuenta con una red de área local (LAN) y se necesita implementar QoS en ella debido a que se tienen aplicaciones sensibles al retraso de paquetes como telefonía sobre IP o SAP.
- El segundo escenario es considerando la interconexión de la red LAN con una de área amplia (WAN) Este es el caso más común de acceso a Internet desde compañías pequeñas hasta grandes corporativos y de interconexiones entre redes privadas en diferentes lugares.
- El tercer escenario es para proveedores de servicio, los cuales tienen los dos escenarios anteriores, más un tercero que se refiere a interconexiones en redes WAN, debido a que tienen requerimientos diferentes para implementación de QoS como reportes y facturación. En este caso se considera la red desde el punto de vista backbone.

8.1 QoS en Red de Área Local

Aunque las redes locales tienen la característica de contar con un ancho de banda grande, tienen la desventaja de trabajar con el esquema de servicio de mejor esfuerzo, donde se da el mismo trato a todo tipo de tráfico y se corre el riesgo de que una computadora personal conectada en la red, transfiera por ejemplo, un archivo de 100Mbytes y sature la red momentáneamente. Si en ese momento estamos usando una aplicación sensible a retrasos, no funcionaría bien.

Algunas publicaciones de redes como Network World [Greene, 2002] mencionan que las únicas empresas que están implementando QoS en LAN son aquellas que están usando telefonía sobre IP, aunque por otro lado se menciona que el costo por puerto de Gigabit Ethernet se está reduciendo y es más fácil aumentar ancho de banda que implementar Calidad de Servicio. Actualmente, el precio promedio de un puerto Gigabit Ethernet es de $531USD y se proyecta que el costo disminuya a menos de $200USD para el 2006. Estos precios pueden significar que las compañías prefieran actualizar su infraestructura para tener

más ancho de banda y no tener que aprender los detalles de 802.1P y 802.1Q. Estos factores hacen atractivo evitar implementar QoS en la red LAN.

Es cierto que se pueden usar aplicaciones como telefonía IP sin implementar Calidad de Servicio, pero no se tiene la certeza que funcione correctamente cuando la red se encuentre más congestionada por lo que se recomienda la implementación de QoS en LAN. De esta manera se garantiza el ancho de banda para aplicaciones clave, se puede evitar la necesidad de infraestructura más rápida y puede ayudar a planeación de la red porque se mide y administra el tráfico de la red.

Las tecnologías de red local predominantes en la actualidad son Ethernet (IEEE 802.3) y Acceso Inalámbrico (IEEE 802.11), aunque todavía existen otros tipos de tecnologías trabajando, como Token Ring (IEEE 802.5) En los capítulos anteriores se menciona que no se puede tener QoS directamente en el encabezado de la estructura (frame) de Ethernet o de LAN inalámbrico, pero se puede hacer un mapeo usando IEEE 802.1Q para mapear prioridades en clases de servicio. Se tienen 7 clases de servicio, por lo que se recomienda que se divida el tráfico como se menciona en la tabla 8.1

Clase de Servicio	Uso	Descripción
7	Control de Red	Crítica: tráfico de control de infraestructura.
6	Voz	Crítico en tiempo, retraso de menos de 10 milisegundos.
5	Video	Crítico en tiempo, retraso de menos de 100 milisegundos.
4	Carga Controlada	No crítico en tiempo, pero sensible a pérdidas como multimedia en modo de flujo (stream)
3	Esfuerzo Excelente	No crítico en tiempo, pero sensible a pérdidas, menos prioridad que carga controlada.
2	Mejor Esfuerzo	No crítico en tiempo y no sensible a pérdidas, modo tradicional.
1	Menos que Mejor esfuerzo	No crítico en tiempo y no sensible a pérdidas, modo tradicional para tráfico de segundo plano menos importante.
0	Background	No critico en tiempo y no sensible a pérdida, para que este tráfico no impacte el uso de la red.

Tabla 8.1 Clases de servicio para tráfico de LAN

La manera como se configura esto es usando 8 filas de espera en el conmutador (switch), donde cada una transportará un tipo de tráfico diferente y se procederá a transmitir

primero la prioridad más alta, hasta que se vacíe esa fila de espera, en seguida, se transmitirá la prioridad que sigue en turno, así hasta que se llegue a la más baja.

Compañías como 3Com, Cisco y Alcatel incluyen tecnología QoS en sus conmutadores LAN sin costo extra. También están desarrollando software con costo extra, que permite configurar QoS en el conmutador con una interfase gráfica. Alcatel tiene una plataforma de software que se llama "Policy View" que simplifica la configuración de QoS de aplicaciones comunes, por ejemplo, si se desea configurar un servicio con calidad de voz, solo hay que definir la sub-red que se usará para voz y el software selecciona el método más simple para configurar la mejor calidad de servicio disponible según el modelo de conmutador. Los usuarios no tienen que preocuparse por la tecnología que se está usando. En la tabla 8.2 se muestran las compañías que ofrecen QoS y los nombres de sus productos.

Compañía	Producto	Característica
Alcatel	Policy View	One Touch para tráfico de voz
Cisco	Cluster Management	Simplifica configuración de QoS
Enterasys	Net Sight Policy Manager	Simplifica configuración de QoS
Nortel	Optivity Policy Server	Asistentes de configuración

Tabla 8.2 Productos comerciales para configurar QoS en LAN

Con estos productos, se pueden configurar los parámetros de QoS para actuar basado en la dirección fuente-destino, protocolo, número de puerto UDP o TCP, Identificación de Virtual LAN, valores de tipo Ethernet y limitación de flujo.

8.1.1 QoS en IP sobre Ethernet.

Si tenemos aplicaciones que usan IP en redes LAN, la implementación de QoS se usa para aplicaciones que tienen sesiones de larga duración y que son sensibles a retrasos, por ejemplo telefonía IP, para lo cual se puede seleccionar la tecnología de reservación de recursos con el protocolo RSVP.

Una sesión de larga duración se denomina así cuando el protocolo de transporte TCP o UDP abren una sesión para comunicación y no la cierran hasta que la aplicación haya terminado de enviar datos. En el caso de un servidor WEB en la Intranet, no se necesita QoS por reservación de recursos debido a que durante el uso de la aplicación, se abren varias sesiones de corta duración de TCP y se generaría sobrecarga de tráfico en la red por el proceso de reservación.

Cabe mencionar que esta implementación sólo se puede hacer cuando se tiene una red local administrada por un enrutador o conmutador, con varias subredes y para comunicar una con otra el tráfico pasa a través del enrutador. Se necesita un dispositivo inteligente en la red en la cual se puedan implementar los requerimientos para QoS. No se toma en cuenta en este momento la conexión del enrutador con un puerto WAN que se detallará posteriormente.

8.2 QoS entre LAN y WAN

En esta sección se analizan las tecnologías descritas en los capítulos anteriores con el fin de cubrir los escenarios más comunes donde se hacen interconexiones de una red local con una red metropolitana o una amplia y se pueda aplicar Calidad de Servicio (QoS) Todo esto con el fin de recomendar el uso de la tecnología más apropiada para cada caso.

El acceso de red local (LAN) y de área amplia (WAN) han sido el punto clave en el diseño de redes porque se tienen dos ambientes diferentes. En el ambiente LAN se tiene alta velocidad y un principio de transmisión donde varios receptores toman información si les corresponde a ellos, si no, se ignora. Por otro lado, en el ambiente WAN se usan velocidades más bajas debido al costo de los enlaces y la señalización, dependiendo de la tecnología utilizada, también es diferente.

No solo difieren los mecanismos y protocolos sino también los tamaños de los paquetes y velocidades de transporte. Este es el punto donde se unen dominios seguros (LAN) con inseguros (WAN) para lo que se han implementado arquitecturas de seguridad.

Con una perspectiva más amplia de este escenario, se describirá la importancia de garantizar niveles de servicio en esta frontera ya que los paquetes marcados inicialmente en la frontera LAN / WAN pueden ser remarcados por otro mecanismo de transporte más adelante. Las tecnologías predominantes WAN son Frame Relay y ATM, donde cada una tiene sus propios mecanismos para implementar garantías de servicio.

8.2.1 Conexión Punto a Punto.

El caso más simple de este escenario es cuando se quieren unir dos redes locales que se encuentran en una misma ciudad. Para este objetivo se recomienda usar enlaces privados que ofrecen seguridad de la información. En este caso basta con contratar un enlace dedicado punto a punto ofrecido por compañías de acceso local y no se requieren los servicios de transporte en ATM o Frame Relay de una compañía de telecomunicaciones. El costo del enlace es proporcional a la distancia y a la velocidad contratada.

En la tabla 8.3 se muestran los costos en pesos mexicanos de diferentes compañías que ofrecen este servicio, estos precios fueron obtenidos de la Comisión Federal de Telecomunicaciones en Noviembre del 2002. Cabe mencionar que los enlaces se pueden hacer por cable, microondas o por fibra óptica dependiendo de la velocidad que ofrece la compañía. También existe la posibilidad de que los enlaces pasen por la compañía misma o sean directos.

Proveedor / Velocidad	Cargo por Instalación	Renta Mensual
Metro LAN Link	Enlace por fibra óptica	
10Mbps - Ethernet	$212,000	$19,400
100Mbps – Fast Ethernet	$329,000	$50,960
Maxcom		
64Kbps	$12,260	$860
128Kbps	$18,390	$1,630
256Kbps	$30,650	$2,450
512Kbps	$42,910	$3,160
1024Kbps	$55,180	$4,180
2048Kbps	$86,420	$5,050
RSL COM		
E1 (2.048 Mbps)	$10,000	Depende de la cuidad, desde $45253 hasta $75,693
ATSI Comunicaciones		
E1 (2.048Mbps)	$10,000	0-80Km $8000 82-160Km $16,000 162-805Km $30,000 806Km o más $40,000
E-3 (34Mbps)	$15,000	0-80km $50,000 82-161km $100,000 162-805 Km $250,000 806Km o más $300,000
DS-3 (44.7Mbps)	$15,000	0-80 Km $60,000 82-160 Km $120,000 162-805Km $300,000 806 o más $350,000
STM-1 (155.5 Mbps)	$50,000	0-81 Km $150,000 82-161Km $300,000 162-805 Km $740,000 806Km o más $865,000

Axtel		
64Kbps	$2,950	0-80 Km $451.80
128Kbps	$3438.40	0-80 Km $859.5
192/256 Kbps	$4298.40	0-80Km $1946.70
E1 2048Kbps	$9834.40	0-80Km $8,924.40
E3	$18000	0-80Km $68,420
Global Crossing		
E1	$10,000	Desde $39,942 hasta $91,684 dependiendo de la ciudad.
T3 / DS3	$150,000	$299,564 - $745,990
STM-1	$250,000	$827,665 - $1,657,757
STM-4	$350,000	$2,396,515 - $5,967,924

Tabla 8.3 Tabla de precios de Enlaces Dedicados.

Para poder comunicar el enlace con la red local se necesita un enrutador con una interfase para el tipo de enlace que se requiera. Algunas compañías incluyen el equipo dentro de sus coberturas de renta, para lo que se recomienda contactar con el representante de ventas de cada una cuando se decida elegir esta opción.

Una vez que se tiene el enlace funcionando, se deben tomar las consideraciones mencionadas en los capítulos anteriores para implementar calidad de servicio. Este tipo de enlaces privados tienen la característica de tener baja latencia y dependiendo de la velocidad contratada son ideales para comunicación con telefonía IP. Se recomienda configurar QoS basado en IP en el enrutador, así como considerar el hecho que, si la otra red se encuentra en la misma ciudad, no se logran ahorros significativos al utilizar VoIP porque las llamadas a través de la red convencional de telefonía no generan cargos de larga distancia. Pero si se puede controlar la utilización del ancho de banda para datos y no requerir utilizar un ancho de banda adicional que puede repercutir en costos de renta mensual más altos.

8.2.2 Enlace LAN- LAN en otra Ciudad.

Cuando se quieren unir dos redes locales que se encuentran en diferentes ciudades, es necesario tener un enlace dedicado hacia la compañía de telecomunicaciones que proveen los enlaces WAN, usando los servicios de ATM o Frame Relay se pueda llegar hasta otra ciudad y de ahí hacer otra conexión de ultima milla hacia el destino que son las instalaciones donde se encuentra la otra red. Por lo general las compañías que brindan el servicio de Frame Relay o ATM pueden requerir que el acceso del enlace dedicado sea con la misma compañía si se tiene disponible este servicio. Cabe mencionar que si no se quiere acceder a estos servicios públicos, se puede usar un enlace dedicado entre las dos ciudades como en el punto anterior, pero es mucho más costoso.

En la tabla 8.4 se muestran los costos de los enlaces Frame Relay y en la 8.5 los de ATM, estas tarifas de servicios son ofrecidos en México en Noviembre del 2002. Para efectos descriptivos solo consideramos tarifas para servicios en el territorio nacional, porque también se pueden contratar estos enlaces para cualquier parte del mundo. Estos costos se pueden consultar actualizados en la página de Internet de la Comisión Federal de Telecomunicaciones en la dirección http: //www.cft.gob.mx/html/4_tar/index.html

Compañía	Instalación por puerto	Renta mensual
Uninet (Telmex) Frame Relay Dedicado Renta mensual depende de la ciudad origen y destino.		10Kbps, de $44 a $1323 64Kbps, de $100 a $3000 128Kbps, de $200 a 6000 2048Kbps, de 2500 a 60,000
MidiTel Renta no depende de distancia.	64Kbps $2900 128Kbps $4320 2048Kbps $9700	64Kbps $2864 128Kbps $5442 2048Kbps $55188
Global Crossing Renta no depende de distancia.	$2375	64K $3534 128K $5990 2048K $28272
Avantel Renta mensual depende de la ciudad origen y destino.	$1650	64K, de $95 a $2850 128K, de $190 a $5820 2048K, de $2375 a $59400
AT&T (Alestra) Renta no depende de distancia.	64K a192K $1700 256K a 320 $2500 384K o más $4000	64K $1000 128K $1800 1984K $11750
RSL COM	Igual que AT&T	Igual que AT&T
Telefónica DATA Renta no depende de distancia en territorio nacional.	$1950	64K $750 128K $2418 1984K $18070

Tabla 8.4 Tarifas de Servicio Frame Relay

En el caso de que se quiera usar una conexión con ATM se tienen menos compañías disponibles que ofrezcan el servicio, debido principalmente a que no se ha desarrollado

suficientemente el mercado mexicano para utilizar estos enlaces y el retorno de inversión de las compañías puede ser más tardado.

En la tabla se muestran los precios disponibles del servicio ATM.

Compañía	Cargo por contratación	Velocidad / Renta Mensual
Telefónica DATA	$37300	E1 $71,000 E3 $350,000 STM1 $500,000
Global Crossing	$6,650 por puerto $950 por PVC	E1 $21,375 E3 $78,375 STM-1 (OC-3) $142,500
MetroRed	10Mbps –ATM $212,000 100Mbps –$329,000 155Mbps -$350,000	10Mbps $14,000 100Mbps $36,691 155Mbps $70,000

Tabla 8.5 Tarifas Servicio ATM

Para implementar Calidad de Servicio en este escenario, se debe marcar la prioridad del tráfico en el enrutador de salida hacia el puerto WAN y asegurarse que en el camino del paquete a través de las instalaciones del proveedor no se le cambien los atributos a la información. En la red WAN, el proveedor de servicio es el que configura la Calidad de Servicio de la conexión mediante acuerdos de nivel de servicio, que como se menciona en los capítulos anteriores, no se limita solo al ancho de banda contratado sino que también se deben considerar aspectos como retardos y la consistencia de los retardos (Jitter)

8.2.3 Enlace LAN-WAN

El caso que sigue en complejidad es cuando se quiere unir la red local a una WAN. Este es el caso clásico de acceso a Internet para toda la red local. Aquí se pueden usar distintas técnicas, desde un módem telefónico como medio de acceso a Internet, el uso de ISDN, xDSL, Frame Relay hasta ATM.

Si se trata de una oficina pequeña con un máximo de 10 empleados, con necesidades de acceso a Internet solo para correo electrónico y navegación por la WEB, se puede usar Windows® 2000 en una computadora configurando el acceso telefónico a redes en modo de compartir la conexión. Y conseguir una cuenta con un proveedor de servicio de Internet que ofrezca una conexión permanente para el tiempo que los empleados se encuentran en la oficina. La computadora que está compartiendo el módem tendrá una dirección IP fija de 192.168.0.1 para la red local, que se asigna automáticamente cuando se activa la compartición de la conexión telefónica y las demás computadoras en la red deberán ser configuradas para obtener la dirección IP automáticamente. De esta manera la computadora que comparte la conexión se convierte en un enrutador-gateway y asigna direcciones de red a través de un servidor DHCP. De esta manera todas las computadoras tienen acceso a Internet con una sola línea telefónica. No hay manera de asignar prioridades a usuarios y todos tienen el mismo nivel de servicio. Esta es la solución más económica para este fin. En teoría se pueden tener hasta 250 usuarios en esta modalidad, pero considerando que solo se tiene una conexión de salida de 56Kbps, no es buena opción tener más de 10 usuarios.

En la misma oficina pequeña, si se tienen más empleados, se puede tener una conexión más rápida a Internet a través de un módem ADSL que es la versión de DSL que se ofrece en México. El único proveedor de esta tecnología en México es Telmex. En la tabla 8.6 se muestran las características de este servicio.

Velocidad de Conexión	Número máximo de usuarios	Precio de contratación	Renta mensual
256Kbps	16	$2999	$499
512 Kbps	32	$2999	$899
2048 Kbps	64	$2999	$4499

Tabla 8.6 Especificaciones conexión ADSL

El módem tiene una conexión a la línea telefónica y tiene un puerto de Ethernet por el otro lado. Este puerto se puede conectar por medio de un cable de Ethernet en la modalidad de Cross-Over directamente al puerto Ethernet de una computadora. Si se desea compartir esta conexión a toda la red se puede conectar a un HUB o conmutador Ethernet para que las demás computadoras tengan acceso a Internet. En esta modalidad cada computadora debe tener instalado el protocolo PPPoE (Point to point protocol over Ethernet) para poder acceder a Internet.

Diagrama Esquemático de Conexión por Hardware con Módem ADSL Bridge + Ruteador

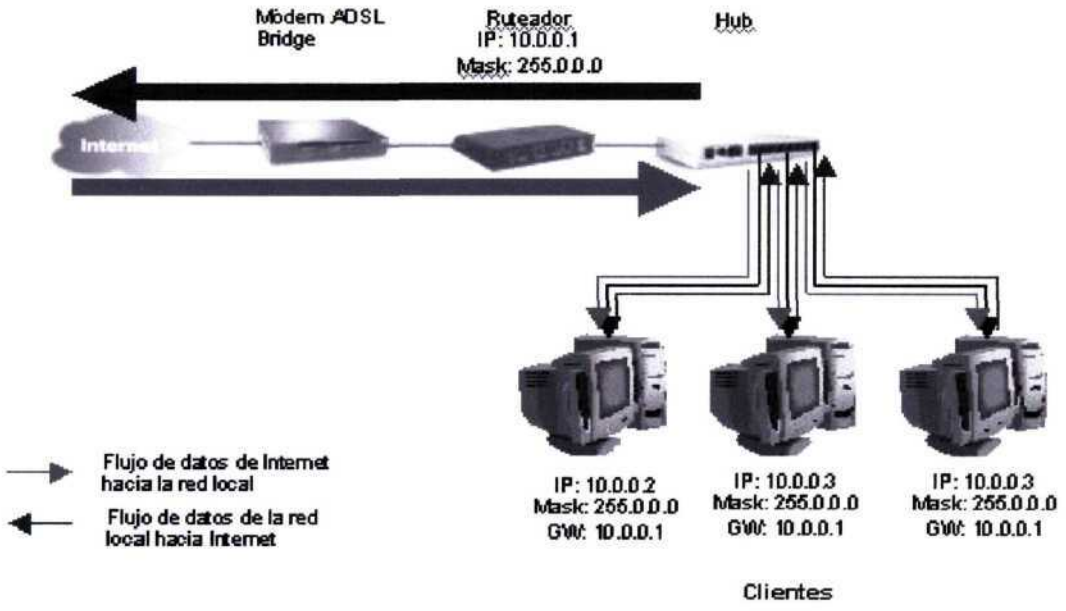


Figura 8.1 Arquitectura recomendada para ADSL (Fuente Telmex)

Lo que se recomienda hacer para poder tener QoS en una conexión DSL es usar un enrutador para DSL como se muestra en la figura 8.1. De esta manera cada computadora ve una conexión directa a Internet y no necesita tener instalado el protocolo PPPoE. El Enrutador con funciones de QoS funciona como filtro para el tráfico y detiene en filas de espera al tráfico que no tiene prioridad. En la figura 8.2 se muestra la pantalla de configuración de QoS de un enrutador para DSL marca LinkSYS en el cual se puede dar prioridad al tráfico por tipo de puerto específico que usan las aplicaciones como FTP, http, Telnet, SMTP para correo electrónico y POP3 también para correo electrónico. También se puede dar prioridad por el puerto LAN específico para dar prioridad a los usuarios según la conexión de red que tengan asignada.

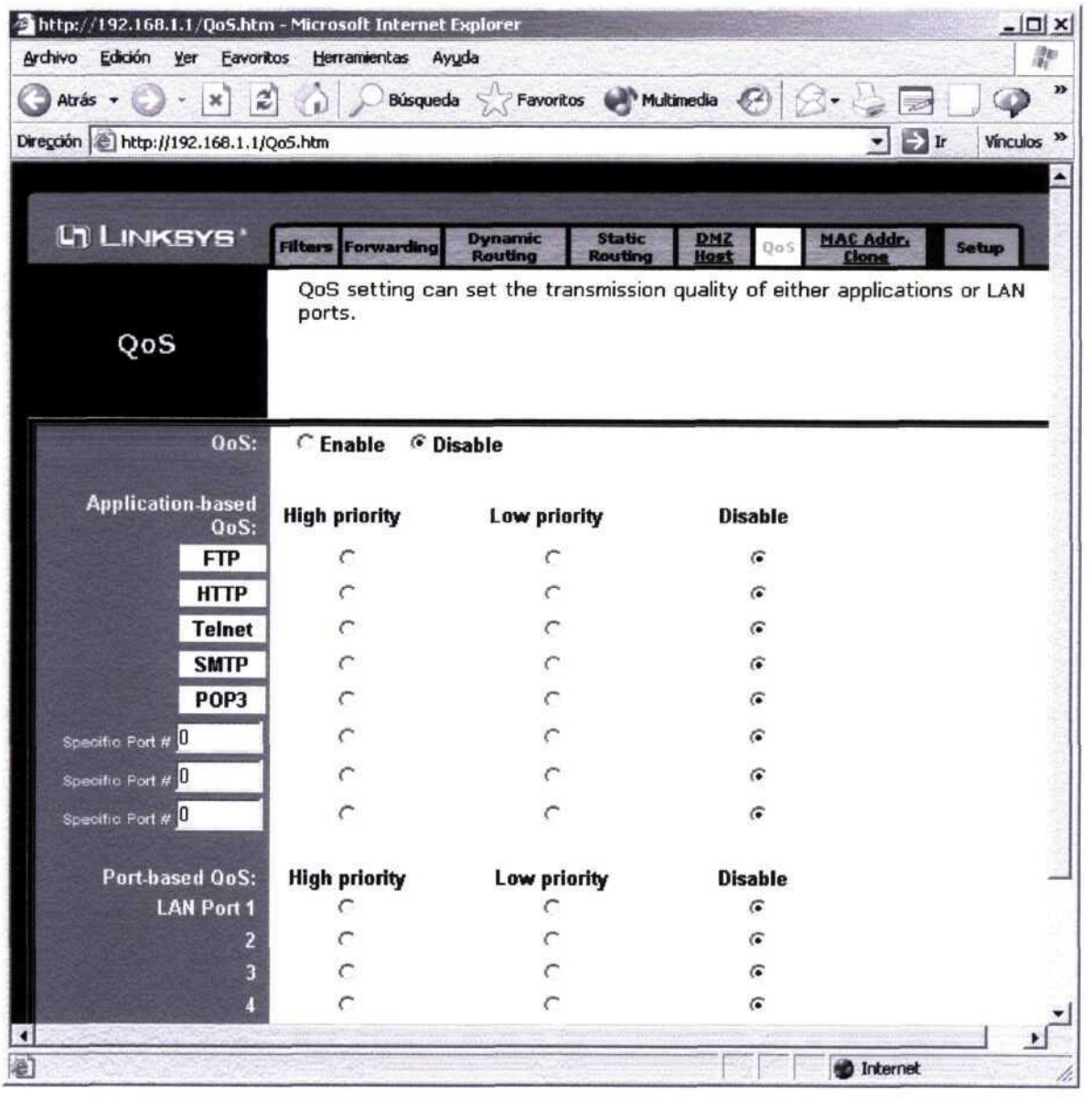


Figura 8.2 QoS en Enrutador DSL para Ethernet

8.2.4 Administradores de ancho de banda

Si la velocidad de los esquemas anteriores no es suficiente, se pueden obtener enlaces de mayor capacidad que tienen un costo más alto. Debido a que el costo de los enlaces WAN es demasiado alto, se tiene que cuidar el tráfico que pasa por la red y darle prioridad al tráfico crítico o sensible al tiempo usando las nuevas tecnologías de QoS.

Como se mencionó anteriormente, primero se debe hacer un análisis de las necesidades de tráfico que se tienen en la empresa. Dependiendo de esto se debe contratar un enlace local para acceder los servicios Frame Relay o ATM del proveedor de telecomunicaciones.

Con el objetivo de diferenciar el tráfico e implementar QoS en la frontera LAN-WAN, se pueden usar el enrutador de la frontera LAN-WAN, pero se pueden saturar por el procesamiento requerido, por lo que se recomienda usar un administrador de ancho de banda.

En la figura 8.3 se muestra una arquitectura LAN-WAN con administración de ancho de banda que se implementa en dispositivos entre el conmutador de la red local y el enrutador.

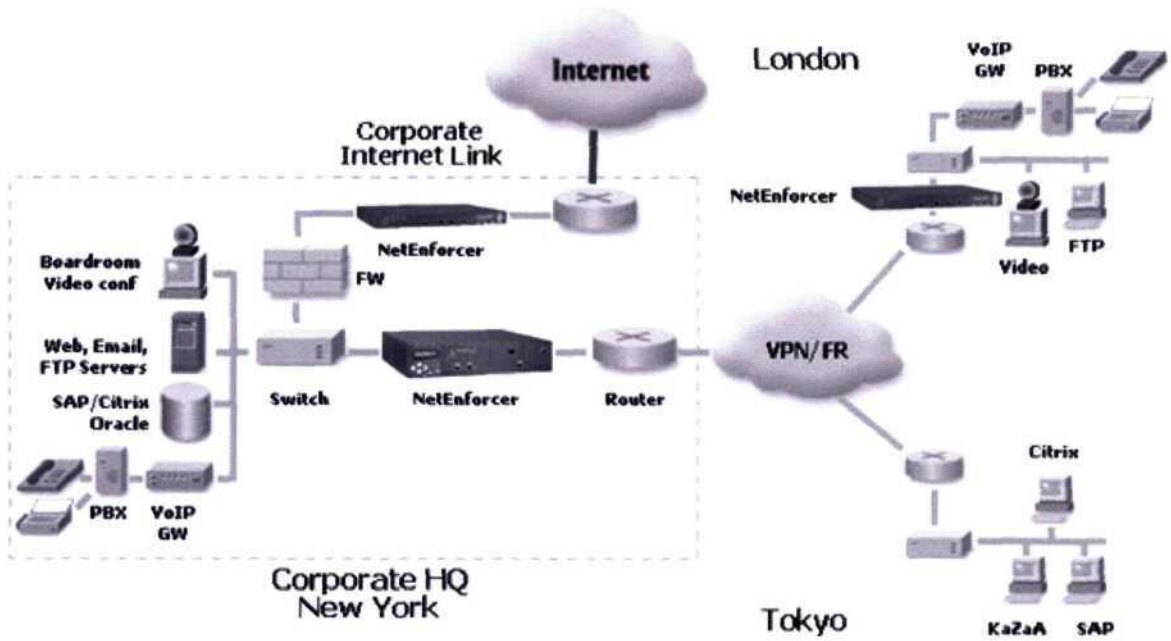


Figura 8.3 Arq. LAN-WAN con Administrador de Ancho de Banda

(Fuente: Allot Communications)

Existen varias compañías que ofrecen estas soluciones como Packeteer, Allot, IP Highway, Elron Software, Nreality. Los dos más comunes y completos son PacketShaper y NetEnforcer.

PacketShaper: Es un producto popular en Universidades, incluyendo instituciones como Stanford. Este producto ostenta 9 patentes y 29 pendientes en la tecnología de marcado de paquetes. El rango de estos productos es de 2Mbps hasta 200Mbps en modo full-dúplex. Tiene productos relacionados que agregan funcionalidades como Policy Center, un servidor central de administración de políticas y Report Center que es un servidor para grabar datos monitoreados. La tecnología Packet wise utiliza filas de espera con prioridad absoluta, control de tasa de transferencia para TCP y particiones de ancho de banda. El control de tasa de TCP utiliza el mecanismo de ventana de TCP para controlar la transmisión.

NetEnforcer: Este producto utiliza recomendaciones de Merit Networks, pero es relativamente desconocido. El rango de utilización es desde 128K hasta 155Mbps en modo

full-dúplex. Tiene como productos adicionales NetPolicy, NetAccountant, NetBalancer y CacheEnforcer. El mecanismo clave es la clasificación por filas de espera. En la tabla 8.7 se muestran los precios y algunas características de PacketShaper y NetEnforcer.

	PacketShaper		**NetEnforcer**		
	6500	8500	601C	701C	701F
Tasa de clasificación	200M	400M	200M	310M	310M
Precio de lista en USD.	$24,000	$32,000	$32,000	$38,000	$38,000
Particiones máximas	512	512	4,000	4,000	4,000
Clases Máximas	1,024	2,048	28,000	28,000	28,000
Particiones dinámicas máximo	5,000	20,000	28,000	28,000	28,000
Hosts IP máximo	25,000	100,000	N / D	N / D	N / D
Flujos máximos	150,000	300,000	256,000	256,000	256,000

Tabla 8.7 Precios y características de Administradores de ancho de banda y QoS

Estos productos se basan en definición de políticas, que permiten administrar el tráfico que atraviesa la frontera LAN / WAN eficientemente. NetEnforcer hace un análisis al nivel de capa 7 de aplicación, para pode definir la calidad de servicio requerida en el puerto WAN. La forma en que lo definen es usando MPLS, Servicios Diferenciados, etc.

Tienen las características que se mencionan a continuación:

1. Monitoreo de uso de ancho de banda y tráfico de red: Con esta característica se pueden autodescubrir aplicaciones nuevas en la red, se genera un reporte del uso de tráfico y con esta información se definen políticas de uso de acceso a la red de aplicaciones. Las actividades de tráfico se presentan en un monitor en tiempo real desde una ventana gráfica. Se puede descubrir quienes usan más tráfico y bloquear la presencia de ataques a los servidores WEB que originarían congestión.
2. Define políticas que enlazan prioridades del negocio: Mediante una interfase se puede definir la política de QoS, asignando porcentajes de ancho de banda y con capacidad de 10 prioridades de tráfico. Se pueden definir estas políticas basado en

direcciones, protocolos, marcas de VLAN, tipo de servicio y hasta la hora del día. Con esta función se puede limitar o bloquear aplicaciones punto a punto (peer to peer) o bajar música de la red.

3. Aseguran Retorno de inversión: porque detienen tráfico que no es para fines del negocio, en algunas redes se usa el 80% de los recursos de la red para usos como KaZaA y otras aplicaciones punto a punto.
4. Maximizan rendimiento: Se puede diferenciar el rendimiento de aplicaciones críticas usando canales virtuales o tuberías. Después de clasificar el tráfico en categorías, se mantiene el mismo nivel de servicio cuando hay congestionamiento en horas pico.
5. Reportes Contables: Se recolecta información del tráfico basado en dirección destino y fuente, tipo de aplicación y política. Con estos datos se facilita la planeación.
6. Permite QoS punto a punto: Se usan los protocolos estándar, Servicios Diferenciados (DiffServ) y tipo de servicio (ToS) Basado en los resultados de la clasificación, el equipo marca los paquetes con valores de DiffServ como "Asegurado" o "Mejor esfuerzo" para señalizar todo el camino de la red. También se puede usar MPLS para clasificar el tráfico.

Características Técnicas.

Clasificación de tráfico

- Direcciones IP / MAC con rango IP, opción de subred o nombre de host. Se puede obtener mediante directorios LDAP
- Protocolos de Red, IP y aplicaciones
- Aplicaciones con puertos dinámicos, H.323, FTP, Oracle, RSTP, etc.
- Retención tráfico para http, por tipo de contenido, método, host, nombre de usuario
- Autenticación de protocolo para http

QoS

- Jerarquía de políticas con administración de entrada / salida
- Ancho de banda máximo / mínimo por flujo o circuito virtual
- 10 niveles de prioridad
- Ancho de banda garantizado por flujo
- Equidad entre dos flujos de la misma prioridad
- Control de admisión
- Remarcación de byte ToS y Reservación bajo demanda para tráfico de alta prioridad.

Configuración

PacketShaper: Puede recibir instrucciones a través de una línea de comandos, usa una interfase propietaria de Cisco. También tiene la interfase HTML y JavaScript. Varios usuarios administrativos con privilegios pueden trabajar concurrentemente. Los cambios en la configuración son inmediatos. La pantalla se muestra en la figura 8.4

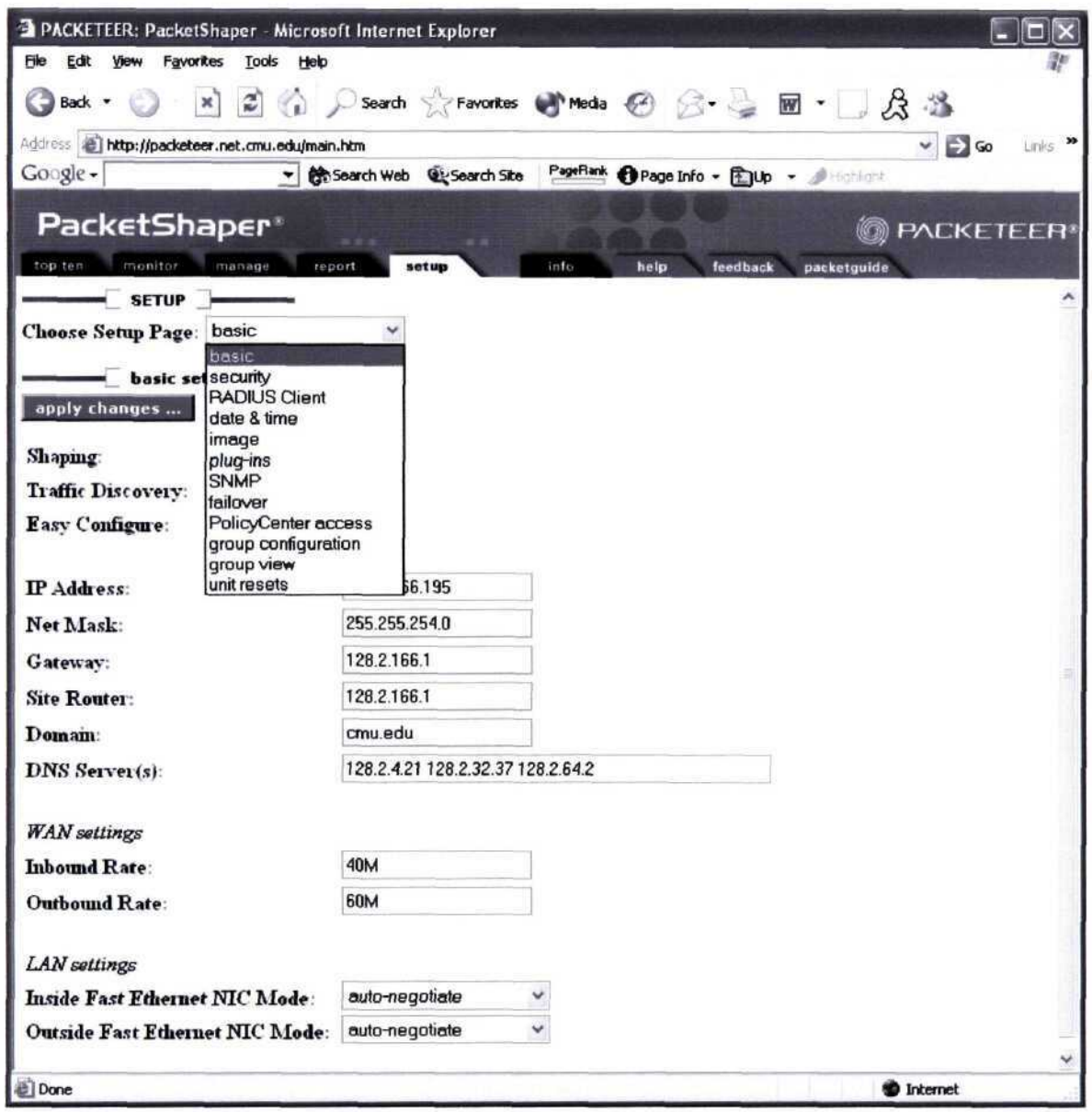


Figura 8.4 Configuración PacketShaper

NetEnforcer: Corre bajo Linux, por lo que tiene los comandos tradicionales. La configuración de parámetros específicos se puede hacer desde la línea de comandos. La interfase WAN es una consola basada en Java. Solo un usuario administrativo con privilegios puede acceder a la vez. La pantalla de configuración se muestra en la figura 8.5

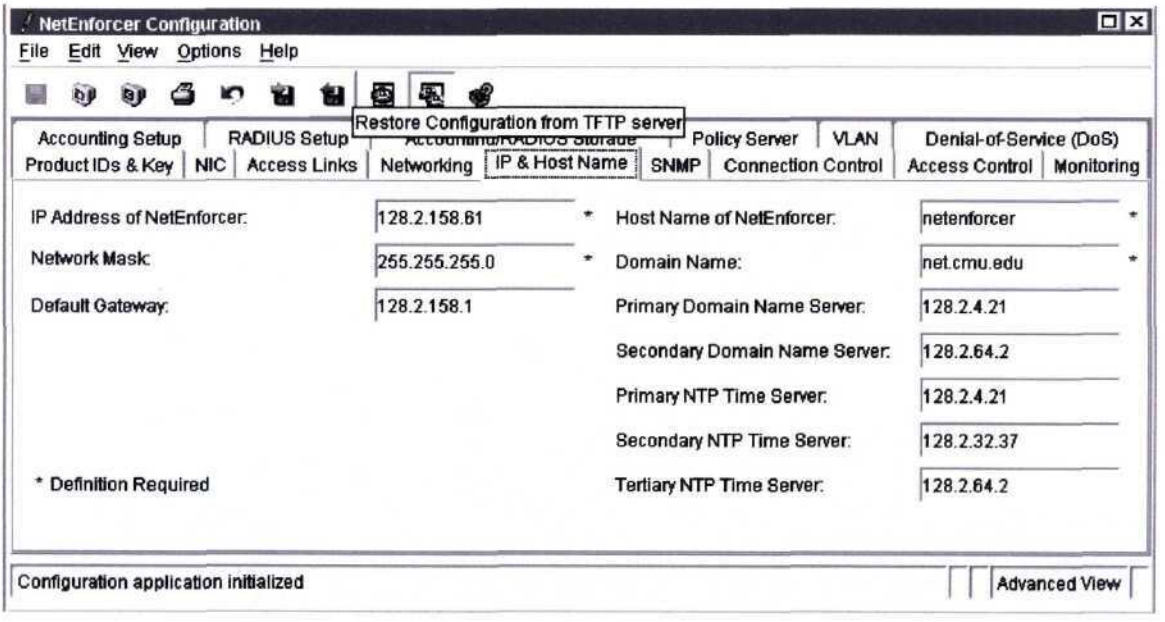


Figura 8.5 Configuración NetEnforcer

Entre estos dos productos, se puede recomendar NetEnforcer porque brinda soporte para división equitativa de ancho de banda (WFQ) entre las conexiones cuando se tienen varias conexiones WAN. En el PacketShaper, se obtiene un sesgo a llenar primero un enlace y después usar el otro.

8.3 QoS en una Red WAN

Esta sección se enfocará en las redes WAN de los proveedores de servicio. Los cuales tienen una base de suscriptores variada, desde hogares y pequeñas oficinas hasta grandes empresas. Cada grupo de suscriptores tiene necesidades diferentes por lo que se permite sobre-suscripción, ya que no todos accedan a los recursos al mismo tiempo. De esa manera se trata de maximizar el retorno de inversión. Esta situación causa que se tengan comportamientos de red impredecibles por lo que muchos usuarios estarían dispuestos a pagar por servicios "premium" que brinden otra clase de servicio mejor, con calidad de conexión para que puedan usar aplicaciones como VoIP o SAP.

Los mecanismos de QoS para redes WAN incluyen servicios diferenciados (DiffServ) y MPLS. Estos servicios pueden ser administrados por un enrutador, pero en el caso de redes grandes de proveedores de servicio, la capacidad de procesamiento del enrutador puede verse gravemente afectada.

8.3.1 QoS con enrutador

En este ambiente de proveedor de servicio se pueden recibir paquetes marcados con prioridad para ser transportados hacia el destino. Todos los enrutadores que intervienen en el camino deben ser capaces de interpretar estas características de tráfico para reservar el ancho de banda que requiere el cliente. Se requiere colectar información del tráfico que está enviando el cliente.

Se pueden marcar los paquetes de entrada en el enrutador para que se le asigne al cliente la calidad de servicio que tiene contratada mediante un acuerdo de nivel de servicio. Se usan principalmente las tecnologías vistas en los capítulos anteriores como MPLS o Diffserv. Se corre el riesgo que si el cliente tiene un enlace de última milla con mayor capacidad de lo que tiene contratado, se pueda usar más ancho de banda y esto afecta adversamente al cálculo de capacidades del proveedor de servicio.

Para saber que es lo que estamos recibiendo del cliente y así monitorear que el tráfico que se está recibiendo corresponda al del nivel de servicio, se necesita un analizador de paquetes el cual se puede bajar de Internet como el PacketStorm.

http://packetstorm.decepticons.org/defense.html

En la figura 8.6 se muestra una imagen de un analizador de paquetes bajado packetstorm.

Es importante mencionar que la aplicación de políticas de QoS no crea ancho de banda adicional, pero ayuda a dar prioridad a tráfico de alta importancia, dando un segundo plano a aplicaciones que no son criticas. Los resultados de estas mejoras son apreciadas por los usuarios de la red y la mayoría de los enrutadores nuevos o con actualizaciones de software recientes, ya tienen incorporado los conceptos de QoS. Solo es cuestión de saber que se necesita para poder configurar correctamente el conmutador o enrutador. Puede verse reflejado en disminución de costos al no tener que aumentar el ancho de banda en un futuro cercano o disminuir el ancho de banda que se tiene actualmente porque no es aprovechado como mínimo al 80% que es el límite teórico para el diseño de redes.

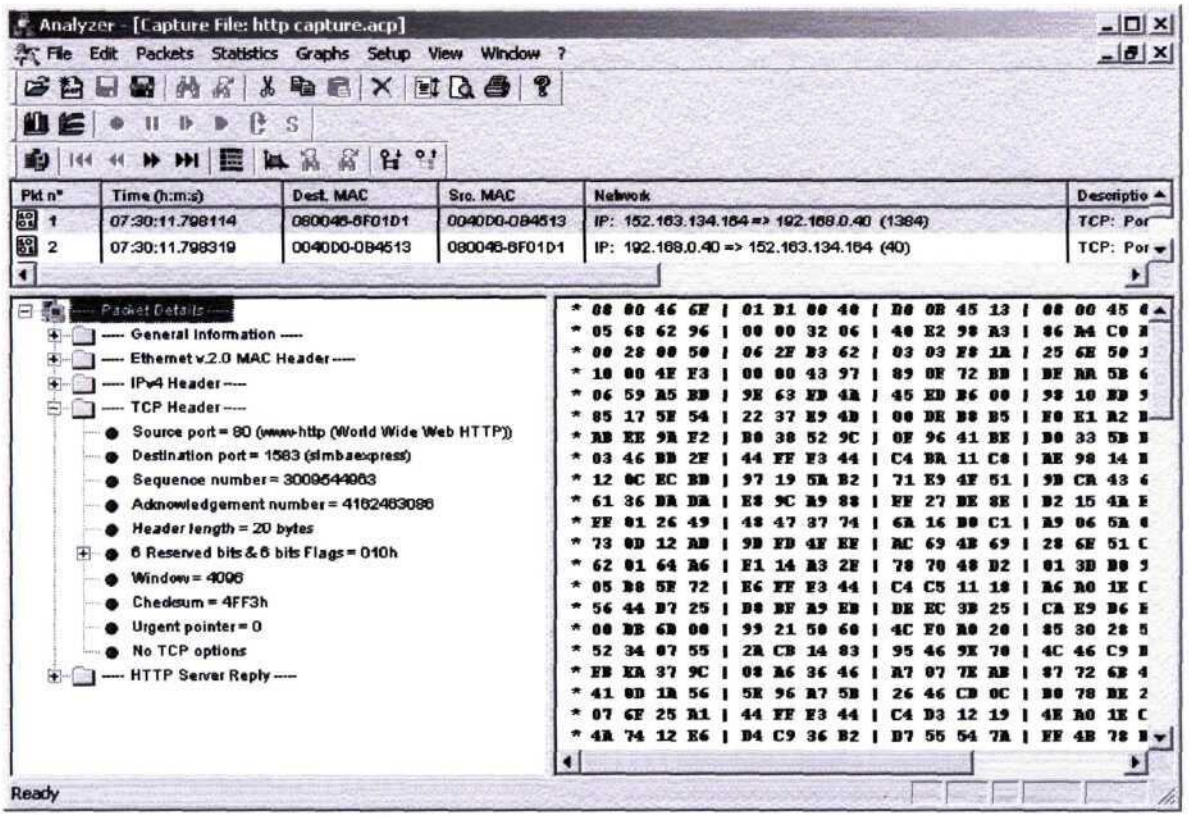


Figura 8.6 Sniffer o Analizador de paquetes

8.3.2 QoS con Administrador de Ancho de Banda

Se recomienda usar Administradores de ancho de banda (AAB) para poder liberar al enrutador del procesamiento para reconocer QoS y dejarlo en manos del administrador de ancho de banda que proporciona los servicios de QoS. Este administrador proveerá las funciones de QoS que permiten administrar la sobre-suscripción que tienen los proveedores de servicio, al tener acuerdos de nivel de servicio (SLA) Este dispositivo puede identificar y limitar a los clientes que consumen más ancho de banda del que tienen contratado y así reciben exactamente lo que contratan.

Se usa un archivo de configuración que contiene la información de los clientes en una lista en formato texto. Cuando se hace un cambio a este archivo, el AAB automáticamente aplica los cambios y modifica el acuerdo de nivel de servicio para definir el ancho de banda mínimo y máximo, así como los requerimientos de QoS.

Se pueden crear esquemas de facturación avanzados donde se tiene información detallada sobre direcciones, aplicaciones usadas, servicio aplicado y tráfico enviado. Estos reportes se pueden tener en una pantalla gráfica en ambiente WEB que se puede hacer disponible a los clientes de que se trate. En la figura 8.7 se muestra una pantalla con la información gráfica de las características de tráfico de una demostración.

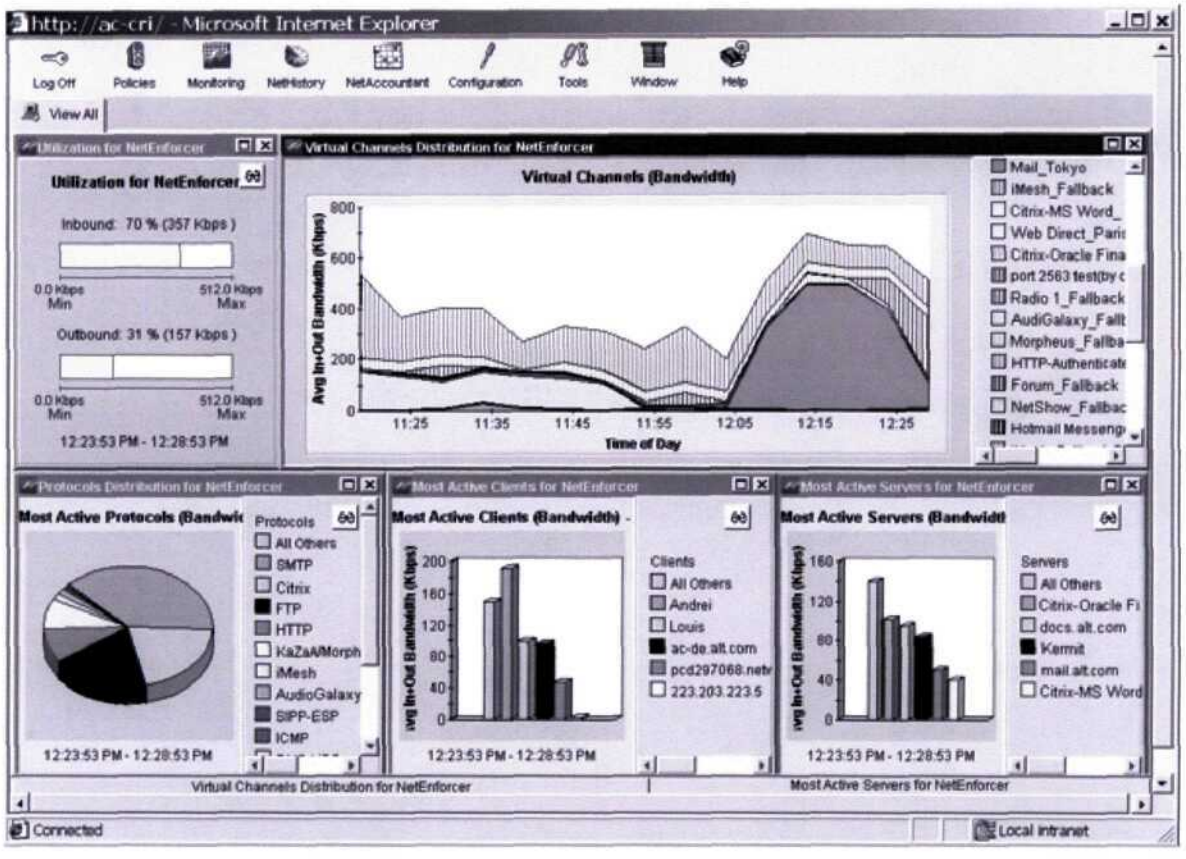


Figura 8.7 Gráfica de Información de características de tráfico

8.4 QoS punto a punto

Como punto final de todos los esquemas anteriores se busca tener Calidad de Servicio desde el origen hasta el destino. Este sería el estado ideal de la red pública de Internet, pero todavía está muy lejos de lograrlo. Se espera que cuando tenga mayor uso del protocolo IPv6 se pueda alcanzar este objetivo debido a las características de QoS que tiene incorporado. Para esto, los enrutadores que sean para IPv6, deberán considerar estas características. Esto es independiente de los protocolos para transporte de QoS en la red WAN que seguirán siendo MPLS o DiffServ.

Por ahora, seguimos utilizando IPv4, que aunque tiene características para marcar el tráfico con prioridad, parece que una opción mejor es usar un administrador de tráfico en el enrutador de la frontera LAN-WAN y utilizar Frame Relay o ATM que tienen mecanismos para transportar QoS y tener otro administrador de tráfico en la frontera del destino, esta arquitectura recomendada se muestra en la figura 8.3

9. CONCLUSIONES

En este apartado se presenta a manera de conclusión, una serie de recomendaciones para los administradores de redes sobre los distintos escenarios que se consideraron en este trabajo y de esta manera complementar su visión sobre el concepto de Calidad de Servicio.

El desarrollo de la sección de investigación de la tesis se realizó con un enfoque a "conexiones entre redes", porque se consideró que era un buen método didáctico y de esta manera se podía analizar y mostrar claramente la manera de implementar Calidad de Servicio. Otro motivo para hacerlo de esta manera, se debe al hecho que se facilita el discernimiento de los conceptos y tecnologías para ser aplicados en el ambiente o escenario correcto.

Quisiera mencionar que Calidad de Servicio no es únicamente ancho de banda, con esto me refiero a que el hecho de administrar el ancho de banda de una red no cubre el concepto de Calidad de Servicio en su totalidad, ya que existen otros puntos que se deben considerar como el rendimiento, disponibilidad y retardos. Para el rendimiento es importante el monitoreo de tráfico y aplicaciones para obtener información de las condiciones que se tienen en el momento para poder configurar los dispositivos. Para la disponibilidad y retardos es muy importante el diseño de la red, ya que no basta con clasificar el tráfico para proporcionarle una preferencia si no es capaz de llegar a tiempo a su destino aunque tenga un ancho de banda correcto. Otro aspecto importante es la capacidad de procesamiento de los sistemas terminales o host, ya que, si son muy lentos, los retrasos en el envío o recibo de información se pueden deber a esta causa. También existe la posibilidad que la red esté trabajando correctamente, pero existe un factor psicológico que puede dar la apariencia a los usuarios que la red no tiene el rendimiento esperado.

En el caso de las redes de área local se recomienda considerar la red en forma global, es decir, se debe tomar en cuenta el número total de usuarios que se tienen, ya que pueden existir redes locales muy grandes como las corporativas o en un Campus universitario, donde la cantidad de tráfico es importante. Esto se menciona porque existen algunos detractores para implementar QoS en redes locales, como en el artículo de la revista Network Wolrd Fusion [Greene, 2002] donde dice que aplicaciones como telefonía IP (VoIP) pueden trabajar en una red local sin necesidad de QoS. Esto puede ser cierto si se tiene una red sobredimensionada con pocos usuarios, pero seguramente tendrá problemas en una red más grande.

En las redes de área local grandes, se puede tener un ancho de banda alto ya que no se tiene que pagar renta por la comunicación entre sub-redes, que se hace con uno o varios ruteadores. Éste tipo de redes también se conoce como Intranet si se cuenta con servidores de Internet o de correo locales.

En el caso de la interconexión entre redes locales es importante resaltar que si se encuentran en la misma ciudad, no es necesario hacer uso de los servicios de compañías de enlaces WAN, porque estos están diseñados para efectuar enlaces entre sitios distantes. El uso de un enlace dedicado es suficiente, los costos de éstos enlaces se mencionan en el capítulo 8. La renta mensual depende de la velocidad del enlace y puede variar desde 800

pesos hasta 800,000. Hay clientes que contratan estos servicios desde pequeñas oficinas hasta bancos y grandes corporativos. Para implementar calidad de servicio entre estas dos redes es posible tomar las consideraciones de implementación de QoS en redes locales y configurar los ruteadores de estos enlaces para transportar los atributos de tráfico diferenciado entre ellas.

En el caso de la interconexión de redes locales con amplias, se recomienda hacer un estudio profundo del número de usuarios que hacen o harán uso de los servicios de la red, así como los requerimientos de ancho de banda necesario, retrasos y rendimiento que se espera de las aplicaciones y de se deben hacer las mismas consideraciones que en el caso pasado. Esto es muy importante para poder dimensionar correctamente los enlaces que se utilizarán para comunicar la red con el mundo exterior.

En el caso de las redes de área amplia.

Los problemas que enfrentan las redes LAN y WAN son diferentes, porque éstas últimas están diseñadas para dar acceso a múltiples redes y su backbone está basado en enrutadores GSR (Gigabit Switch Routers) en los cuales no se implementa QoS para evitar procesamiento innecesario que pueda afectar el rendimiento. Los esquemas de calidad de servicio se pueden implementar en los enrutadores frontera.

Otro enfoque sobre calidad de servicio en las redes WAN de los proveedores de servicio se refiere a la arquitectura de su red, porque la basan en capas de distribución con balanceadores de carga. En las capas de distribución, se tienen ruteadores con puertos para servicios como Frame Relay, VPN e Internet.

El usar administradores de ancho de banda en el corazón (core) de la red generaría un cuello de botella, ya que la capacidad máxima de éstos es de 155Mbps, siendo que para el backbone se utilizan enrutadores GSR con capacidades de entrada en el rango de 20 a 80Gbps.

Con esta aclaración se pretende proporcionar un panorama mayor sobre los distintos enfoques que se le puede dar a la calidad de servicio en redes WAN.

Ahora se considerará el escenario de los ruteadores frontera. Se recomienda recapacitar sobre la latencia de éstas redes, porque se puede tener la creencia de que este tipo de conexiones al estar conformados en su mayoría por fibras ópticas, tienen bajos retrasos. Por ser principalmente de circuitos virtuales, cada flujo tiene que ser procesado, lo cual induce retrasos que no siempre son consistentes.

Dependiendo tipo de red con el que se cuenta, se recomienda hacer un monitoreo de tráfico y aplicaciones a través de un administrador de ancho de banda para que se pueda tener una idea real sobre las condiciones de la red y se puedan definir las políticas correctas para tomar las decisiones guiadas por los intereses del negocio.

En este escenario, creo que el factor más importante para hacer un balance de costo-rendimiento son los precios de los enlaces WAN, ya que ser pueden ser altos y se debe escoger el que más se adecue a las necesidades de tráfico en primer lugar, pero también considerando la capacidad financiera de la empresa.

Porque como se comentaba en la introducción, tal vez la mejor tecnología pueda estar a un precio inaccesible, entonces, con la ayuda de Calidad de Servicio se puede lograr la utilización máxima del enlace.

El problema con los administradores de ancho de banda radica en que el proceso de implementación de Calidad de Servicio se tiene que hacer en dos partes.

1. **Proceso de recolección de datos:** ya sea mediante el monitoreo de aplicaciones, tráfico o tendencias de usuarios.
2. **Proceso de configuración de dispositivos de red:** para lograr el comportamiento deseado.

Algunos fabricantes de equipo como Cisco, están muy enfocados a redes corporativas, por lo que los proveedores de servicio, en especial los de redes WAN, tienen que encontrar soluciones propias para algunos de los problemas que representa el tener y administrar redes de este tamaño. Creo que Cisco debería ampliar su visión de negocio.

Cisco tiene la mala costumbre, a mi parecer, de implementar en sus equipos tecnologías para proveer Calidad de Servicio (entre otras), que no han sido estandarizadas previamente. Ésta compañía menciona que dichas tecnologías son una propuesta para proveer una solución a un problema en específico, pero no consideran que los clientes pueden tener en sus redes equipos de otras marcas que no tienen integrada esta solución propietaria y traer el problema que no pueda ser implementada. No por esto quiero decir que los productos de esta compañía son malos, únicamente se recomienda analizar que las tecnologías incluidas en los equipos para proveer calidad de servicios, hayan sido estandarizadas previamente.

Al comprar equipos para una red, se debe investigar profundamente sobre la tecnología que se usa para proveer Calidad de Servicio y verificar, basado en referencias actualizadas como libros, artículos en Internet o revistas, que la solución no sea propietaria.

Actualmente, parece haber una falta de interés por implementar Calidad de Servicio en las redes de telecomunicaciones, creo que esto se debe principalmente al desconocimiento de que esta tecnología está disponible, ya que es reciente y se encuentra integrada en equipos relativamente nuevos. Aunque en algunos casos, con una actualización de software en el enrutador se pueden incluir estos servicios.

Otro aspecto puede ser que, aunque se conozca la tecnología, en muchos de los casos para implementarla se tienen que cambiar los dispositivos de red con los que se cuenta actualmente y las compañías prefieren esperar a que la tecnología esté un poco más madura para invertir en otros equipos o simplemente esperar a que se termine el tiempo de vida contable, para que una vez depreciados, puedan hacer el cambio a nuevas tecnologías.

Creo que el problema principal se debe al dilema del área de sistemas, que para poder comprobar el beneficio de retorno de inversión de equipos nuevos, se deben tener resultados sólidos y el implementar calidad de servicio puede parecer algo no prioritario para la gente que toma decisiones financieras, si no conoce de los beneficios reales al poder ahorrar en otros gastos como el evitar un aumento de ancho de banda.

Se tienen esperanzas que con el uso del nuevo protocolo de Internet, IPv6, se pueda dar un empuje más sólido a implementar QoS, pero se estima que pasarán 10 años más antes que podamos ver resultados concretos en esta área.

10. TRABAJOS FUTUROS

Como se mencionó en el capítulo anterior, el hecho de administrar el ancho de banda de una red es sólo una parte del concepto global de Calidad de Servicio, por lo que se considera que para trabajos futuros, se puede hacer una investigación sobre los siguientes puntos. El orden de las ideas no implica la importancia de ellas.

1. **Monitoreo de aplicaciones y tráfico**: Las técnicas de monitoreo de aplicaciones pueden ser un punto medular para obtener información real de las condiciones de la red, porque los monitores actuales tienen problemas para ver el tráfico de servidores WEB con páginas dinámicas por ejemplo.
2. **Implementación automática de políticas**: Como se describe en la tesis, el proceso de implementación de políticas se tiene que hacer en dos pasos, el primero es obteniendo información del tráfico de la red y posteriormente el administrador de redes tiene que analizar cuál es el comportamiento que desea que tenga el mismo y proceder a configurar el dispositivo que se esté utilizando para proveer Calidad de Servicio ya sea que se trate de un ruteador o un administrador de ancho de banda. El ideal sería que el mismo dispositivo pudiera hacer el análisis automático o en tiempo real del tráfico y con base en esto, cambiar las políticas que está usando.
3. **Diseño de redes para proporcionar QoS**: Como se menciona en el capítulo anterior, no es suficiente con diferenciar el tráfico para darle prioridad, si no es capaz de llegar a su destino a tiempo, este problema se tiene cuando un paquete tiene que pasar por muchos ruteadores y cada uno agrega un tiempo de retraso.
4. **Perspectivas de negocio con QoS para Internet**: Las nuevas tendencias del mercado se dirigen hacia video en demanda. Se menciona que en algunos años ya no será necesario ir a rentar películas a un video-club, sino que podremos rentar la película en línea en cualquier momento que se desee, hacer pausa y luego continuarla. Se tienen más clientes potenciales con cada día que pasa debido al incremento de las facilidades para el acceso a Internet potenciado por nuevas tecnologías como DSL, CATV y tecnologías inalámbricas. Para lo que se debe estudiar el impacto de proveer Calidad de Servicio en redes como facilitador de nuevos negocios y comercio electrónico en general.
5. **QoS con Tipos de ruteo:** Se puede hacer una investigación sobre tendencias de implementación de QoS basado en tipos de ruteo. También se pueden incluir tecnologías como los "Gibabit Switch Routers".
6. **QoS para acceso a Internet:** Los proveedores de servicio a Internet, pueden ofrecer nuevos esquemas de conexión donde no solo se considere la velocidad del enlace, sino también la calidad del mismo y el retraso de su tráfico. De esta manera ofrecer servicios "premium" que podrían ser comprados por usuarios que tienen requerimientos de audio o video, pero no necesitan las prestaciones de un enlace dedicado.

11. BIBLIOGRAFÍA Y REFERENCIAS

[Black, 1992] Black Uyless, "*Network Management Standards, the OSI, SNMP and CMOL Protocols*", McGraw-Hill, 1992. ISBN 0-07-005554-8

[Croll, 2000] Croll Alistair, Packman Eric, "*Managing Bandwidth: Deploying QoS in enterprise networks*", Prentice Hall, 2000, ISBN 0-13-011391-3

[Ferguson, 1998] Ferguson Paul and Huston Geoff, "*Quality of Service: delivering QoS on the Internet and in corporate networks*", Wiley, 1998. ISBN 0-471-24358-2

[Greene, 2002] Greene Tim, "*Bandwidth: Quality over quantity?*" Network World Fusion http://www.nwfusion.com/news/2002/0408specialfocus.html

[Hein, 1995] Hein Mathias, Griffith David, "*SNMP Versions 1 & 2 Simple Network Management Protocol, Theory and practice*", International Thomson Computer Press, UK, 1995. ISBN 1-850-32139-6

[Stallings, 1998] IEEE Communications Surveys 1998 http://www.comsoc.org/pubs/surveys/4q98issue/stallings.html, Junio 2000

[Guerin, 1997] IETF Internet Draft, "A Framework for Multiprotocol Label Switching", draft-guerin-qos-routing-ospf-01.txt R. Guerin, S. Kamat, A. Orda T. Przygienda, D. Williams, March 1997.

[Leon Garcia, 2000] Leon Garcia Alberto, Widjaja Indra, *"Communications Networks, Fundamental Concepts and Key Architectures"*, McGraw Hill

[Muller, 2002] Muller Nathan, "*Quality of service Whose responsibility is it anyway?*", Communications News, Enero 2002, http://www.comnews.com

[Wang, 2001] Wang, Zheng "Internet QoS, architectures and mechanisms for Quality of Service", Academic Press, 2001.

[Zeichick, 1998] Zeichick Alan, "What is QoS Anyway?", Smart partner, October 30 1998, http://techupdate.zdnet.com/techupdate/stories/main/0,14179,364383,00.htm