CALIDAD DE SERVICIO EN REDES ATM Y FRAME RELAY Y ESTÁNDAR 802.1P

BELKY ROCÍO BOSSIO NIETO

CARLOS ALBERTO CUADRADO GONZÁLEZ

INSTITUCIÓN UNIVERSITARIA TECNOLÓGICA DE BOLIVAR

INGENIERÍA DE SISTEMAS

CARTAGENA

2003

CALIDAD DE SERVICIO EN REDES ATM Y FRAME RELAY Y ESTÁNDAR 802.1P

BELKY ROCÍO BOSSIO NIETO

CARLOS ALBERTO CUADRADO GONZÁLEZ

Monografía presentada para optar al

Título de Ingeniero de Sistemas

Director, Isaac Zúñiga Silgado

Ingeniero de Sistemas

INSTITUCIÓN UNIVERSITARIA TECNOLÓGICA DE BOLIVAR

INGENIERÍA DE SISTEMAS

CARTAGENA

2003

Nota de aceptación

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

ARTICULO 107

La institución reserva el derecho de propiedad intelectual de todos los trabajos de grupo aprobados, los cuales no pueden ser explotados comercialmente sin su autorización. Esta observación debe quedar impresa en parte visible del proyecto.

Cartagena, 26 de mayo de 2003

Señores

Comité de facultad de Ingeniería de Sistemas

Institución Universitaria Tecnológica de Bolívar

Ciudad

Apreciados Señores.

Cordialmente me permito informarles que he llevado a cabo la dirección del trabajo de grado de los estudiantes BELKY ROCIO BOSSIO NIETO y CARLOS ALBERTO CUADRADO GONZÁLEZ, titulado: "CALIDAD DE SERVICIO EN REDES ATM Y FRAME RELAY Y ESTÁNDAR 802.1P"

Cordialmente,

_____

ISAAC ZÚÑIGA SILGADO

Cartagena, 26 de mayo de 2003

Señores

Comité de facultad de Ingeniería de Sistemas

Institución Universitaria Tecnológica de Bolívar

Ciudad

De la manera más atenta nos permitimos presentar a su consideración y aprobación el trabajo de grado titulado "CALIDAD DE SERVICIO EN REDES ATM Y FRAME RELAY Y ESTÁNDAR 802.1P". Elaborado por BELKY ROCIO BOSSIO NIETO y CARLOS ALBERTO CUADRADO GONZÁLEZ.

Esperamos que el presente trabajo se ajuste a las expectativas y criterios de la universidad para los trabajos de grado.

Cordialmente,

_____ _____

BELKY ROCIO BOSSIO NIETO CARLOS A. CUADRADO GONZÁLEZ

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

La calidad de servicio es fundamental para afrontar y dar eficiencia a diferentes tipos de aplicaciones (voz, datos y vídeo), controlar redes complejas y brindar un servicio predecible de aplicaciones en red. Al garantizar los resultados deseados, las características de QoS hacen posible servicios eficientes y previsibles para su organización.

La calidad de servicio se puede clasificar de acuerdo al tráfico de la red, de acuerdo a quien requiera el nivel de Calidad de Servicio, según las garantías o según el lugar de aplicación. Además posee una variedad de parámetros que son de gran importancia para su correcta aplicación en las redes existentes, tales como, retardo, latencia, ancho de banda, tráfico de red, rendimiento, disponibilidad, entre otros. Todos estos parámetros se deben tener presente a la hora de aplicar la calidad de servicio.

La calidad de servicio brinda muchas ventajas a las redes donde se está aplicando, beneficios para la empresa dueña de la red, para sus aplicaciones, y también para los proveedores de servicios de red. Dichas ventajas le ofrecen a la red una mejor aplicabilidad.

Obtener QoS en las tecnologías más conocidas y utilizadas en la actualidad, ATM, Frame Relay y redes Locales IEEE 802, no es tarea fácil. Para esto se deben tener en cuenta muchos aspectos, los cuales son los que permitirán su correcta aplicación.

ATM es una tecnología que simultáneamente transmite tráfico de datos, voz y vídeo sobre circuitos de alto ancho de banda. Esta tecnología puede proveer a los usuarios con una Calidad de Servicio (QoS) garantizada, dando a conocer a sus usuarios la clase de tráfico esperada que será transmitido en la conexión y el tipo de calidad de servicio que la conexión requiere, para esto se utilizan descriptores del tráfico y categorías de servicio.

Frame Relay se define, oficialmente, como un servicio portador RDSI de banda estrecha en modo de paquetes. En la aplicabilidad de QoS en esta tecnología, al cliente se le garantiza los servicios que le brindará la red, siempre por contrato, de esta forma el cliente puede contratar un nivel de calidad de servicio diferente para cada conexión.

Cuando se busca obtener algún tipo de Calidad de Servicio en redes LAN incluyendo Ethernet es necesario acudir al estándar 802.1p.

INTRODUCCION

Anteriormente, debido a la baja capacidad de las redes, realizar estudios o trabajos relacionados con información multimedia como video-conferencia, audio-conferencia, vídeo bajo demanda (VoD) o sistemas cooperativos (pizarras compartidas, teletrabajo, telemedicina, etc.), así como aplicaciones tradicionales (transferencia de ficheros, base de datos, WWW, etc.) era casi imposible; situación que en la actualidad es totalmente lo contrario, hoy en día el avance en el área de tecnologías de redes, aumenta cada vez más; el mayor de los avances que tenemos hasta hoy ha sido el auge de Internet y la facilidad de poder conectarse desde cualquier lugar utilizando solamente un computador, un módem y una línea telefónica. Por otra parte cada día se emplean más las tecnologías de fibra óptica que brindan un mayor ancho de banda requerida por las aplicaciones mencionadas, el cual necesita una eficaz y eficiente gestión, es decir, necesita un adecuado uso, garantizando la calidad de éste; Esto es lo que se conoce como calidad de servicio (QoS).

A continuación presentamos una explicación completa, precisa y globalizada de la definición del término calidad de servicio y cómo algunas de las tecnologías de redes más conocidas actúan para alcanzarla. Para esto se hará un estudio de todas

las medidas y parámetros que se requieren para conseguir calidad de servicio en dichas tecnologías, de igual manera se describirán los métodos usados para poder conseguir la calidad de servicio en cualquier red, tales como mecanismos de vigilancia y prevención para su buen funcionamiento y de esta forma evitar la congestión en las redes.

Por último presentaremos una guía de laboratorio donde se especificarán los pasos necesarios para conseguir Calidad de Servicio en Ethernet con **switches** Cisco Catalyst 2950.

OBJETIVO

Realizar un estudio que describa completamente cómo las tecnologías de redes más comunes actúan para garantizar calidad de servicio (QoS) y de esta manera ayudar a los administradores de redes a tomar decisiones tendientes a optimizar el desempeño de sus redes.

1. CALIDAD DE SERVICIO (QoS)

1.1 HISTORIA

A continuación presentamos una reseña histórica de las redes de computadoras, es importante conocer este proceso ya que nos indica cómo con el transcurrir de los años van surgiendo aplicaciones que exigen además de redes más y más robustas técnicas que permitan a esas aplicaciones tener un funcionamiento aceptable, una de esas técnicas es la Calidad de Servicio.

La gran industria de las redes de computadoras se empezó a formar en los años 80, con el surgir de diversos inventos relacionados con esta área, como es el caso de Alto Alhoa Network de Bob Metcalfe y Boggs, luego convertida en Ethernet y aplicada por la empresa 3Com en la primera LAN (1983); otro punto importante que se dio en esta década fue que se establecieron las normas OSI (**Open Systems Interchange**) por la Organización Estándar Internacional (ISO), también en esta misma década surge el Token Ring, una red local de datos inventada por la IBM.

La IEEE (**Institute of Electrical and Electronic Engineers**) designa un comité encargado de establecer normas para la transmisión de datos (el comité 802).

La interconexión entre redes, y la dilución de límites en ambientes locales convertidos en globales se da hasta 1985 con el surgimiento de los **routers**, pero el fortalecimiento y formalización del mercadeo en el campo de las redes se presentó en 1988, con la aparición de OpenView, la plataforma de administración y gestión de redes de Hewlett-Packard; y del Lan Manager, el sistema operativo de red de Microsoft que sustituía al MS-Net.

En la década del 90 surge la conmutación rápida de paquetes, y se inventa una tecnología nueva, la "Frame Relay", además se inicia la utilización del correo electrónico con la tecnología Token Ring. El 92 se inició con la tecnología ATM en un **switch** para redes privadas desarrollado por Network Equipment y fue aquí donde el término Calidad de Servicio se definió por primera vez en los protocolos de comunicaciones de esta tecnología (ATM), un año después, National Semiconductor implanta la tecnología Isonet, la cual admite la transmisión totalizada de servicios multimedia y toleraba protocolos Ethernet y RDSI. Después de ésta tecnología surgió la Fast Ethernet, basada en la norma 100 Base T, la cual contribuía con beneficios parecidos a las de Any LAN**.** Pero es sólo hasta finales de

los 90 que se desata la utilización de las redes, lo que consolidó el término Calidad de Servicio, debido a la incorporación de funciones de voz en redes de datos.

En estos últimos años se ha intensificado el manejo de funciones de seguridad, como la encriptación, la autenticación de usuarios, el **firewalls**, entre otros.

Estos sucesos acontecidos hasta el día de hoy ratifican que dentro de algunos años la voz gastará sólo una mínima porción del ancho de banda, y cualquier dificultad para los responsables del área de sistemas estará en gestionar apropiadamente un flujo de datos cada vez más denso y relevante.

1.2 DEFINICIÓN DE CALIDAD DE SERVICIO (QoS)

Los estudios más recientes en el campo de las redes, como aplicaciones empresariales ERP (**Entreprise Resource Planning**), minería de datos, el comercio electrónico y la multimedia, requieren de tiempos de respuesta lo más pequeño posible y un ancho de banda manejado eficientemente. Las redes antiguas no podrían distinguir entre información básica y primordial debido a que no fueron creadas pensando en esa necesidad y el tráfico de datos que en ellas se manipulaba, utilizaba métodos antiguos (FIFO - **First in-First out** o FCFS – **First come First served**), los cuales impedirían reconocer datos prioritarios

procesados en la red. Para solucionar esta clase de inconvenientes no basta sólo con el aumento del ancho de banda en la red en que se esté trabajando, ya que con el paso del tiempo las aplicaciones que se implementen requerirán probablemente un ancho de banda mayor al que se implementaría en el momento, inconveniente que podría causar problemas en la red a tal punto que dejara de funcionar. Por lo tanto para poder obtener un completo y eficaz control de una red es necesario aplicarle calidad de Servicio, lo que permitiría priorizar el flujo de su tráfico, brindar seguridad a las aplicaciones que se manejen dentro de la red y a sus usuarios, sincronizar tanto los requerimientos que se tienen para implementar una red como la forma que ésta actúe y almacenar el ancho de banda de la red para sus aplicaciones y usuarios.

Como se puede ver, definir el término calidad de servicio (QoS) es muy extenso y de cierta forma complejo, pues son muchos los conceptos que abarca este tema, los cuales de cierta forma dificultan el poder lanzar una definición exacta de éste término. La percepción más clara y exacta con la que se puede definir este concepto es la siguiente:

Calidad de Servicio (QoS): Beneficios de los servicios, obtenidos por el usuario final.

En una red se debe garantizar un cierto nivel de calidad de servicio para un nivel de tráfico, el cual sigue un grupo detallado de reglas o parámetros, las cuales establecen un contrato de intercambio de información entre el usuario y la red.

También se puede definir dependiendo del contorno de la red en que se aplique la Calidad de Servicio. En el ámbito de las telecomunicaciones, este término se define como: "el efecto colectivo del rendimiento de un servicio que determina el grado de satisfacción del usuario de dicho servicio", esta definición está totalmente ligada con la apreciación del usuario al obtener este servicio, debido a que es quien establece unos requerimientos mínimos para cualificar. En el campo de la telemática, QoS se define como la capacidad que posee un componente de red (Aplicación, Servidor, Usuario, **switch**, etc.) para asegurar que el tráfico y requisitos establecidos utilizados en su red se manejan de la manera más óptima y por ende queden satisfechos; también es definida como el grupo de tecnologías que dejan que los administradores de la red decidan ante las consecuencias o resultados de la congestión del tráfico en la red (antes de ampliar consecutivamente capacidad en la red) utilizando las distintas técnicas que ésta posee.

Existen dos conceptos que son primordiales para comprender cuando se habla de calidad de servicio:

- La clase de servicio (CS), que define un conjunto preciso de parámetros cuando se ofrece un servicio.

- El nivel acordado de servicios (**Service Level Agreement**: SLA), que establece la calidad de servicio pactada mediante un contrato.

1.3 CLASIFICACIÓN DE QOS

La calidad de servicio está clasificada siguiendo algunos patrones, tales como, tipo de tráfico, campo de aplicación, reserva de recursos de la red y algunos otros parámetros.

1.3.1 De acuerdo con el tráfico en la Red.

- QoS demasiado sensible al retardo. Para este caso, el ejemplo más práctico que se puede mostrar es el tráfico de vídeo comprimido. Se debe garantizar que exista un gran ancho de banda disponible para este tráfico en la red y además un valor de retardo el cual permita la transmisión de dicho tráfico, por lo que se requerirá emplear métodos de prioridad y organizar los flujos de datos.

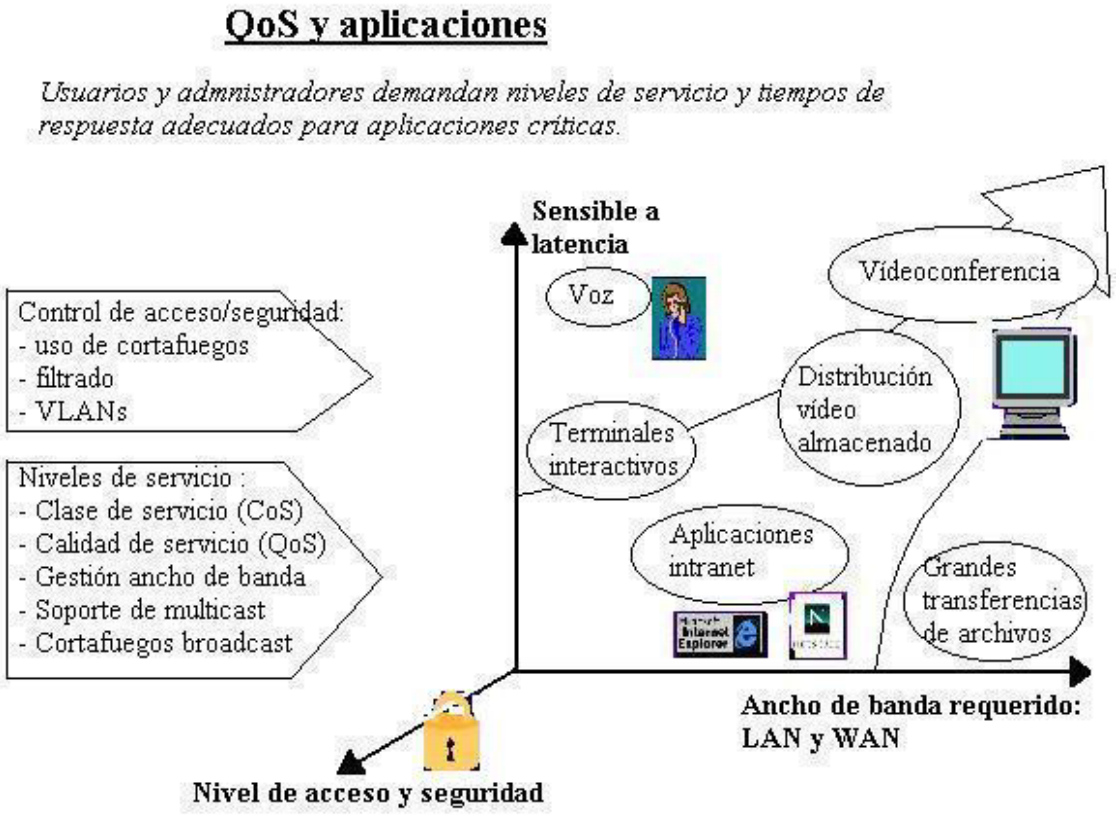
- QoS un poco sensible al retardo. Un caso práctico que ejemplifica esta clasificación de calidad de servicio es la aplicación de la emulación de circuito. También se debe garantizar que exista un ancho de banda disponible para el tráfico en la red aunque un poco menor que en el caso anterior, y también se requerirá establecer la priorización para el tráfico de información.

- QoS demasiado sensible a pérdidas. Este caso se puede reflejar en el tráfico de información en la red tradicional. En esta clasificación se puede deducir que si no se tienen pérdidas no se podrá descartar paquetes, ni se desbordarán los **buffers** de almacenamiento del flujo; esto proporcionará un mejor y mayor control en el tráfico de información.

- QoS insensible. En esta clase de Calidad de Servicio se utiliza la posibilidad de transmisión que exista y tomar la capacidad que poseen los **buffers** existentes como necesaria para el tráfico de información con la prioridad más baja. Un ejemplo de este tipo de QoS es el tráfico de servicios de noticias.

En la figura 1 es posible diferenciar de forma gráfica los tipos de tráfico y sus exigencias de ancho de banda y de sensibilidad a la latencia.

Figura 1. QoS y aplicaciones



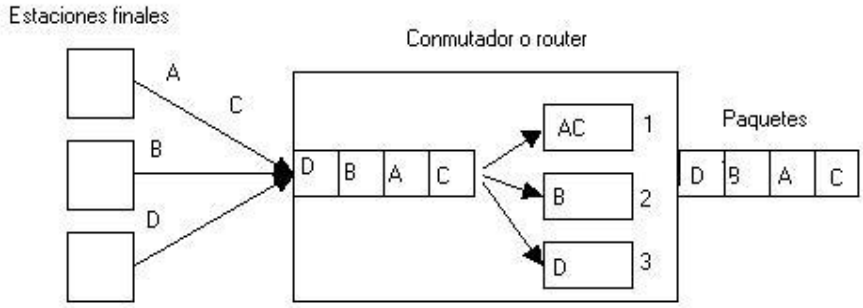
1.3.2 De acuerdo a quién requiera el nivel de calidad de servicio. En este caso la calidad de servicio puede ser necesitada y realizada por el usuario final o por los **routers** / **switches** de la red:

- QoS Implícita. El **router** / **switch** establece los niveles de calidad de servicio, siguiendo lo especificado o estipulado por el administrador (protocolos, dirección de origen). Esta clase de QoS la brindan todos los

routers y algunos **switches**, en el que las estaciones finales transmiten los paquetes, los cuales llegan al **switch** o **router**, en el que se analiza la información entrante y se prioriza, luego se reparte en distintas colas dependiendo de la prioridad de éstas; la información se vuelve a transmitir al próximo **switch** o **router**, en el cual se realiza el mismo proceso.

- QoS Explícita. En esta categoría los **routers** / **switches** reciben un servicio con un nivel escogido previamente por el usuario, en la cual las estaciones finales transfieren una petición RSVP, que si es aceptada, los paquetes son transmitidos; por lo tanto, la información que accede al **switch** o **router** es priorizada dependiendo de las instrucciones del nodo destino, y de esta forma llega al siguiente **switch** o **router**, en el que se repetirá el proceso.

Figura2. Ejemplo de visualización de QoS implícita y explícita



1.3.3 Según las garantías. Teniendo en cuenta la reserva de recursos del sistema para proporcionar los servicios, se tienen las siguientes clases de QoS:

- QoS Garantizada / **Hard QoS**. En este caso se genera una reserva absoluta de los recursos de la red para un tráfico estipulado, garantizando de esta forma niveles máximos para el tráfico de información en una red.

- QoS No Garantizada / **Lack of QoS.** Es el tipo de QoS correspondiente a los servicios **Best Effort** (Mejor Esfuerzo). En esta categoría no se tiene ninguna clase de garantía; el tráfico de información está dado por la red, el cual depende de los acontecimientos que en ella se den.

- QoS Servicios Diferenciados/ **Soft QoS**. Es el punto medio entre las dos categorías anteriores. En este caso se hace una diferenciación de tráfico, los cuales son analizados, solamente algunos de ellos, teniendo en cuenta la mejoría referenciada a sus características (expedición más rápida, más ancho de banda promedio, menos tasa de error promedio).

1.3.4 Según el lugar de aplicación.

- QoS Extremo a Extremo de la Red (**end-to-end**). En este caso la calidad de servicio se aplica de extremo a extremo de la red, se conoce también como calidad de Servicio Absoluta. Es factible aunque menos utilizada que la calidad de servicio entre dos bordes de la red. Por otro lado, con la aplicabilidad de este tipo de QoS se reducen los **switches** que se limitan a observar la marca de los paquetes (en el caso de 802.1p), sin calcular la clase de servicio de cada paquete reducido. Además las aplicaciones podrían escoger dinámicamente el nivel de QoS almacenando temporalmente en los directorios de red o en los **switches** una información estática de clases de servicio.

- QoS Borde a Borde (**edge-to-edge**). La calidad de servicio se aplica, en este caso, entre dos puntos cualesquiera de la red. Por otro lado, no necesita que los administradores de red toquen los extremos, esto es una ventaja para el caso de las empresas en las que la organización responsable de la infraestructura de red está separada del grupo de los servidores y del resto de los puestos de trabajo. Además son menos los dispositivos que tienen que ser manejados para la obtención de la QoS; y la accesibilidad por parte de un usuario cualquiera de la red o de un **hacker** para cambiar

las especificaciones de QoS es mucho menor. Por último al aplicar este tipo de calidad de servicio no es necesario conocer cómo poner en práctica las reglas de QoS de cada uno de los posibles sistemas operativos que podrían tener los servidores en el caso de aplicar QoS extremo-a-extremo.

1.4 PARÁMETROS DE QOS

Al aplicar la Calidad de Servicio en las redes se manejan diversos conceptos que son de gran importancia para su buen funcionamiento, algunos de éstos son:

- Tráfico de Red. Son los datos que se transportan dentro de la red, los cuales dependen de la forma de aplicación que transita en la red. Este se clasifica según su tipo de aplicación (tráfico habitual, multimedia, **multicast**, **broadcast**, tiempo real, etc.), y la sensibilidad al retardo (en este caso puede ser algo sensible, demasiado sensible al retardo, muy sensible a las pérdidas o nada sensible).

- Retardo. Indica la variación temporal y/o retraso en la llegada de los flujos de datos a su destino. Característica evidente en aplicaciones como video-conferencia. Teniendo en cuenta hacia qué tipo de aplicaciones se están

orientando las telecomunicaciones, es necesario que en las políticas de QoS definidas para nuestra red este parámetro sea reducido al mínimo.

- Latencia. Es el tiempo entre el envío de un mensaje por parte de un nodo y la recepción del mensaje por otro nodo. Abarca los retardos que suceden durante el envío de dicho mensaje, ya sea en el propio camino o en los dispositivos por los que pasa.

- **Jitter** (Inestabilidad o variabilidad en el retardo). Es lo que ocurre cuando los paquetes transmitidos en una red no llegan a su destino en debido orden o en el tiempo determinado, es decir, varían en latencia.

- Ancho de Banda. Medida de la capacidad de transmisión de datos, expresada generalmente en Kilobits por segundo (kbps) o en Megabits por segundo (Mbps) y últimamente en Gigabits por segundo (Gbps). Indica la capacidad máxima teórica de una conexión, la cual se ve disminuida por factores tales como el retardo de transmisión, que pueden causar un deterioro en la calidad. El aumento del ancho de banda significa poder transmitir más datos, pero también implica un incremento económico.

- Pérdida de Paquetes. Indica el número de paquetes perdidos durante la transmisión. Normalmente se mide en tanto por ciento.

- Disponibilidad. Indica la utilización de los diferentes recursos. Suele especificarse en tanto por ciento.

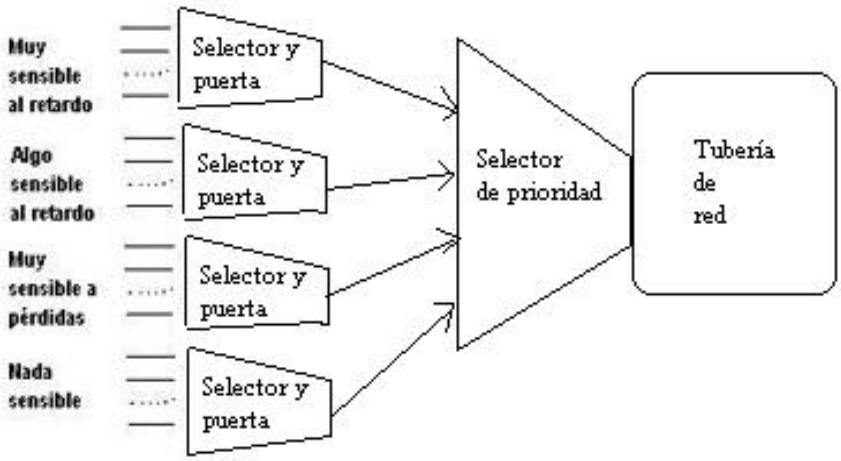
- Rendimiento. Mide el rendimiento de la red en relación a los servicios acordados (SLAs o acuerdos de nivel de servicio). El rendimiento es definido también por algunos profesionales como la velocidad teórica de transmisión de los paquetes por la red. Esta depende directamente del ancho de banda y su variación de las posibles situaciones de congestión de la red.

- Priorización. Consiste en la asignación de un determinado nivel de QoS al tráfico que circula por una red, asegurando así que las aplicaciones de mayor importancia sean atendidas con anterioridad a las de menor importancia. Es necesaria únicamente cuando la red no proporciona la suficiente capacidad para atender todo el tráfico presente en la misma.

- Encolado. Consiste en dividir y organizar el tráfico ante un determinado dispositivo de red para su posterior retransmisión por la misma según un determinado algoritmo que define la cola y que permite que determinados

paquetes sean reexpedidos antes que otros. Es una de las herramientas más utilizadas por la QoS. La idea es ofrecer un mejor servicio al tráfico de alta prioridad al mismo tiempo que se asegura, en diferentes grados, el servicio para los paquetes de menor prioridad. Pero no se asegura la llegada a tiempo de los paquetes.

Figura3. Encolado de servicio



- Planificación. Proceso de decidir qué paquetes enviar primero en un sistema de múltiples colas.

- Flujo. Conjunto de datos pertenecientes a una misma secuencia que, debido a su gran tamaño, han de ser enviados mediante distintos paquetes. Tienen la misma dirección IP fuente y destino, el mismo puerto de destino y el

mismo protocolo. En el caso de redes TCP / IP el flujo necesita llegar secuencialmente a su destino con una frecuencia constante.

- Acuerdos de Niveles de Servicio (SLA). Contrato de servicios entre un proveedor de servicios y su cliente, el cual define las responsabilidades del proveedor en términos del nivel de funcionamiento de la red (rendimiento, tasa de pérdidas, retrasos, variaciones) y la disponibilidad temporal, el método de medida, las consecuencias cuando los niveles de servicio no se consiguen o si los niveles de tráfico definidos son superados por el cliente, así como el precio de todos estos servicios.

1.5 VENTAJAS AL APLICAR QOS

Básicamente se enfatizará en el análisis de los beneficios o ventajas para las aplicaciones, para las empresas y para los proveedores de servicios.

1.5.1 Beneficios para las empresas. Actualmente, todas las empresas están considerando Internet como una nueva vía para incrementar su negocio y, por lo tanto, las expectativas que se tienen para garantizar una calidad son las mismas que si se tratase de una red privada o controlada. Internet está siendo utilizada para la formación y el crecimiento de **intranets** dentro de la empresa y

extranets que admiten el comercio electrónico con los socios del negocio. Es evidente, por tanto, que se está aumentando el acercamiento de los negocios hacia la **Web**, siendo cada vez más importante que los administradores de las redes aseguren que éstas entreguen unos niveles apropiados de calidad. Es aquí donde las tecnologías de QoS cobran especial importancia, proporcionando a los administradores las utilidades para la entrega de datos críticos del negocio en los periodos acordados y con unas garantías determinadas.

1.5.2 Ventajas para las aplicaciones. Las aplicaciones están consiguiendo ser cada vez más exigentes. Las denominadas críticas requieren cada vez más calidad, confiabilidad, y asegurar la puntualidad en la entrega. Un ejemplo claro son las aplicaciones de voz o vídeo, éstas deben ser manejadas cuidadosamente dentro de una red para preservar su integridad. Además es necesario tener en cuenta que el tráfico no es predecible, ni constante, si no que funciona a ráfagas, produciéndose en ocasiones picos máximos de tráfico que son los causantes, en parte, de la saturación de la red. Ejemplos clarificadores de este tipo de tráfico es el producido por el mundo **Web**, el correo electrónico y las transferencias de ficheros, que son virtualmente imposibles de predecir.

Las tecnologías de QoS permiten a los administradores de red manejar las aplicaciones sensibles al **jitter**, como las que manejan audio y vídeo, manejar el

tráfico sensible al retardo, como la voz en tiempo real y el control de pérdidas en los momentos en los que la congestión sea inevitable.

1.5.3. Beneficios para los proveedores de servicios. Claramente, las empresas y las corporaciones se están convirtiendo en negocios con requerimientos de misión-crítica sobre la red pública. Están delegando los servicios de sus redes a proveedores de servicios (**outsourcing**), lo que les permite centrarse más en el negocio interno y así reducir costosos capitales. Esto significa que los proveedores de servicio son quienes podrán ofrecer las garantías de calidad para el tráfico extremo-a-extremo (**end-to-end**) de la empresa. Las tecnologías de QoS permitirán a los proveedores de servicio ofrecer muchas más prestaciones, como el soporte del tráfico en tiempo real, o como la asignación específica de ancho de banda, que se suele especificar en los acuerdos de nivel de servicio (SLAs).

1.6 GESTIÓN DEL ANCHO DE BANDA VERSUS QOS

La capacidad de cualquier tipo de sistema siempre, o casi siempre, acaba por agotarse, así, los discos duros se llenan o las líneas telefónicas de una central se saturan. Pero donde este límite se suele alcanzar con particular rapidez es en la capacidad de la línea que conecta una organización con Internet (o en general

con una red IP) ante el imparable crecimiento de las aplicaciones sobre este medio.

Lo lógico es que, cuando las conexiones van lentas, se contrate más capacidad. Pero, aún así, las líneas vuelven a saturarse tras un breve período de tiempo y es una solución costosa, esta es la técnica conocida como sobreingeniería o método de la fuerza bruta. Es necesario preguntarse entonces si ésta es la solución correcta y al estudiar otras alternativas se ve que con éstas se pueden obtener mayores capacidades por menos costes mediante la optimización de la gestión del ancho de banda.

Por lo tanto, el ampliar el ancho de banda debe utilizarse como una solución puntual para resolver determinadas situaciones de congestión en determinados puntos de la red y para determinados tipos de redes. Esta alternativa es medianamente factible para redes LAN y prácticamente imposible para redes WAN, mientras los precios sigan siendo tan elevados. Es por tanto, una solución costosa, con durabilidad mínima debido al crecimiento del tráfico de la red y de las necesidades de ancho de banda de determinados tipos de tráfico.

La QoS sin embargo, conlleva, entre otras cosas, una correcta gestión del ancho de banda, presentándose como la forma más eficiente, hoy en día, para la mejora de la red.

2. CÓMO OBTENER CALIDAD DE SERVICIO

Exponemos a continuación las características más sobresalientes y el funcionamiento de las principales herramientas empleadas para conseguir Calidad de Servicios; estos mecanismos son los encargados de indicar cómo se obtiene QoS.

2.1 CONTROL DE CONGESTIÓN

Se entiende por congestión la circunstancia en la que el rendimiento de la red (o una parte de ella) se degrada debido a la presencia de demasiados paquetes / tramas.

Normalmente la congestión se produce porque se pretende pasar más tráfico por una línea de lo que ésta es capaz de absorber. Por ejemplo un **router** / **switch** recibe mucho tráfico de varias líneas de 2 Mb/s todo dirigido a una sola línea también de 2 Mb/s. Generalmente el cuello de botella es la línea de transmisión, pero en algunos casos la congestión puede ser causada por un **router** / **switch** sobrecargado o de poca capacidad para el tráfico que soporta.

Inicialmente los **buffers** intentan salvar la situación, pero si la situación dura bastante tiempo los **buffers** se llenan y los **routers** / **switches** empiezan a descartar paquetes.

Tanto en control de congestión como en control de flujo suelen utilizarse mecanismos de notificación al emisor para que baje el ritmo. La congestión es más compleja, ya que generalmente el emisor es un puro intermediario que se limita a reenviar hacia atrás al verdadero causante del problema el aviso recibido. En líneas de alta velocidad y elevado retardo (gran distancia) este problema se acentúa.

En muchos casos la solución a un problema de congestión se traduce en un control de flujo en el **host** que genera el tráfico.

2.1.1 Principios generales del control de congestión. Entre los parámetros que permiten detectar la presencia de congestión se encuentran por ejemplo:

- Porcentaje de paquetes / tramas descartados.

- Longitud media de las colas en las interfaces de los **routers** / **switches**.

- Número de paquetes / tramas que se retransmiten.

- Retardo medio por paquete / trama.

- Desviación media del retardo por paquete / trama.

Para resolver la congestión solo hay dos posibles medidas:

- Reducir el tráfico informando al emisor para que pare de enviar, o buscando rutas alternativas.

- Aumentar la capacidad.

2.1.2 Factores que pueden influir en la creación de situaciones de congestión. Entre los factores a nivel de enlace que pueden influir en el nivel de congestión se encuentran:

- El intervalo de **timeout**. Si es pequeño originará retransmisiones innecesarias.

- El tamaño de ventana. Si es grande es más fácil que se produzca congestión.

- El uso de retroceso o repetición selectiva. El retroceso genera más tráfico.

- El uso o no de ACK **piggybacked**. Si no se usa se genera más tráfico.

2.2 PERFILES DE TRÁFICO Y VIGILANCIA DEL TRÁFICO (TRAFFIC SHAPING Y TRAFFIC POLICING)

El tráfico a ráfagas es la principal causa de congestión. Si todos los ordenadores transmitieran siempre un flujo constante sería muy fácil evitar las congestiones.

Los perfiles de tráfico (**traffic shaping**) establecen unos márgenes máximos al tráfico a ráfagas. Suelen utilizarse para fijar una QoS entre el operador y el usuario, entre tanto el usuario respete lo establecido el operador se compromete a no descartar paquetes (actúa como una especie de contrato).

Se denomina vigilancia del tráfico (**traffic policing**) a la labor de monitorización o seguimiento del tráfico introducido por el usuario en la red para verificar que no excede el perfil pactado. En este proyecto se describirá el algoritmo del Pozal Agujereado (**Leaky Bucket**) el cual es uno de los sistemas más utilizados para establecer perfiles de tráfico.

2.3 ALGORITMO LEAKY BUCKET

Un **host** puede enviar ráfagas que son almacenadas en un **buffer** de la interfaz, la cual envía a la red un ancho de banda constante; si la ráfaga es de tal intensidad o duración que el **buffer** (pozal) se llena, los paquetes excedentes son descartados, o bien son enviados a la red con una marca especial que les identifica como de segunda clase; dichos paquetes de segunda serán los primeros candidatos a ser descartados en caso de apuro. Esta técnica se utiliza en ATM y en Frame Relay.

Para definir un pozal agujereado se utilizan dos parámetros, el ancho de banda *r* con que sale el flujo a la red, y la capacidad del **buffer** *C*.

Ejemplo: supongamos que con r =20 Mb/s y C = 10 Mbits un computador envía una ráfaga de 10 Mbits en 50 mseg (equivalente a 200 Mb/s), con lo cual llena el pozal, la ráfaga tardará en enviarse 500 mseg; si el computador envía otra ráfaga de 10 Mbits durante esos 500 mseg el **buffer** se llenará y se perderán datos (o se enviarán como de segunda clase).

El pozal agujereado suprime completamente las ráfagas en la red. A veces interesa algo más de flexibilidad, en esos casos se utiliza el algoritmo del pozal con créditos (**Token Bucket**). Se puede considerar como una versión mejorada del pozal

agujereado, que intenta compensar al usuario que alterna intervalos de tráfico con otros de inactividad, frente al que está siempre transmitiendo; cuando el **host** no envía datos a la interfaz ésta va sumando créditos (**tokens**) hasta un máximo igual a la capacidad del **buffer** (el pozal), los créditos acumulados pueden utilizarse después para enviar ráfagas con un ancho de banda *M* mayor de lo normal, cuando se agotan los créditos el ancho de banda vuelve a su valor normal *r* y funciona como un pozal agujereado. Se puede imaginar el pozal con crédito como dotado de dos agujeros, uno pequeño y uno grande, con un dispositivo mecánico que permite abrir uno u otro, pero no ambos a la vez, el agujero grande solo se puede abrir si el usuario tiene créditos, el usuario consigue créditos siempre que el pozal no está tirando líquido por el agujero pequeño, bien porque el pozal no tenga líquido que tirar o bien porque tenga abierto el agujero grande (y por tanto cerrado el pequeño). Los parámetros que definen un pozal con créditos son el caudal del agujero pequeño *r*, la capacidad del **buffer** *C* y el caudal del agujero grande *M* (normalmente igual a la velocidad de la interfaz física).

Ejemplo: Supongamos que r =20 Mb/s, C= 10 Mbits y M = 200 Mb/s. Suponemos que el **host** envía una ráfaga de 10 Mbits en 50 mseg; si el **buffer** está lleno de créditos cuando llega la ráfaga ésta será enviada a la red a 200 Mb/s, es decir a la misma velocidad que la envía el **host**. Si el **buffer** está solo medio lleno (5 Mbits de créditos) se producirá una ráfaga de 200 Mb/s durante 27,78 mseg y seguirá un

ancho de banda de 20 Mb/s durante 222,2 mseg (hay que tomar en cuenta que durante la ráfaga siguen llegando créditos pues está cerrado el agujero pequeño, pero no después ya que se van consumiendo a medida que llegan). Por último, si no hubiera créditos disponibles cuando llegara la ráfaga el comportamiento sería idéntico al del pozal agujereado.

Ahora averiguaremos de dónde proviene el valor 27,78 mseg mencionado en el ejemplo anterior para el caso del pozal medio lleno de créditos. Sabemos que mientras está abierto el agujero grande el pozal suma créditos a una velocidad de 20 Mb/s; por tanto el total de créditos obtenidos en un instante t será:

Créditos totales = créditos iniciales + créditos acumulados = 5000000 + 20000000 * t

Por otro lado, sabemos que mientras está abierto el agujero grande los créditos se consumen a razón de 200 Mb/s, o sea:

Créditos consumidos = 200000000 * t

Para calcular cuanto tiempo estará abierto el agujero grande igualamos las dos expresiones anteriores:

5000000 + 20000000 * t = 200000000 * t

De donde despejando se obtiene para t el valor 0,02778 seg.

En ocasiones se combina un pozal con créditos seguido de un pozal agujereado de *r* mayor, con lo que se permiten ráfagas pero de forma controlada.

2.4 ESPECIFICACIONES DE FLUJO

Se conocen con este nombre el conjunto de parámetros que especifican el ancho de banda y calidad de servicio esperados en una transferencia de datos entre dos entidades para poder realizar de forma eficiente el perfil de tráfico y la vigilancia de éste.

Estos parámetros fueron descritos en el capítulo 1 y aquí sólo se mencionarán algunos de ellos:

- Máximo tamaño de paquete (MTU, **Maximum Transfer Unit**).

- *r* y *C* si se utiliza pozal agujereado.

- *r*, *C* y *M* si se utiliza poza agujereado con créditos.

- Tasa de pérdidas.

- Cantidad máxima de paquetes consecutivos que pueden descartarse.

- Retardo máximo.

- Variación máxima en el retardo o **jitter.**

2.5 CONTROL DE ADMISIÓN (REDES DE CIRCUITOS VIRTUALES)

El control de admisión consiste en impedir el establecimiento de nuevos circuitos virtuales (para redes ATM y Frame Relay) que pasen por la zona congestionada. Si se conoce la capacidad que necesita cada circuito virtual es posible controlar el acceso de forma que nunca se produzca congestión. En general esta técnica no usa los recursos de manera eficiente, por lo que es normal prever un cierto grado de sobresuscripción, u **overbooking**.

2.6 PAQUETES DE ASFIXIA (CHOKE PACKETS)

Se puede aplicar tanto en redes de circuitos virtuales (ATM y Frame Relay) como de datagramas (Ethernet).

En esta técnica el **router** / **switch** sigue de cerca la situación de cada una de sus líneas, monitorizando por ejemplo el grado de utilización, la longitud de la cola o la ocupación del **buffer** correspondiente. Cuando el parámetro inspeccionado supera un determinado valor considerado umbral de peligro se envía un paquete de asfixia (**choke packet**) al **host** considerado culpable para que reduzca el ritmo.

La evaluación del parámetro a monitorizar se suele hacer con una fórmula del tipo:

$$U_n = au_{n-1} + (1-a)\, f$$

Donde *f* es el valor instantáneo medido del parámetro (utilización, tamaño de la cola u ocupación del **buffer**), u_n el valor medio en la n-ésima iteración, y *a* una constante que permite regular el peso que se le quiere dar a los valores anteriores, o dicho de otro modo con qué rapidez se quiere reaccionar a situaciones cambiantes.

Los paquetes de asfixia se envían al **host**, ya que es éste y no el **router** / **switch** el verdadero origen de la congestión. Los **hosts** cuando reciben estos paquetes suelen reducir a la mitad la velocidad con la que envían datos a la red. Esto lo pueden hacer reduciendo por ejemplo el tamaño de ventana (del protocolo a nivel de transporte) o cambiando los parámetros del pozal agujereado o pozal con créditos si utiliza alguno de estos algoritmos para controlar su flujo. En una situación de congestión normalmente serán muchos los **hosts** que recibirán este tipo de paquetes.

En ocasiones interesa que los paquetes de asfixia tengan un efecto inmediato en cada uno de los **routers** / **switches** que atraviesan en su camino hacia el **host** origen del tráfico; esto ocurre sobre todo cuando se trata de una conexión de alta velocidad y gran retardo. Se trata así de resolver la congestión de forma inmediata distribuyendo el tráfico en curso entre los **buffers** de los **routers** / **switches** que hay por el camino, entretanto el mensaje de alerta llega al verdadero causante de los problemas.

Por desgracia la obediencia a los paquetes de asfixia es completamente voluntaria, si un **host** decide hacer caso omiso de las advertencias no se le puede obligar. Si un **host** obedece las indicaciones y reduce su ritmo mientras otros no lo hacen el

primero saldrá perjudicado pues obtendrá una parte aún menor de la ya escasa capacidad disponible.

2.7 DERRAMAMIENTO DE LA CARGA

La solución extrema para resolver la congestión es descartar paquetes. En ocasiones los paquetes llevan alguna indicación de su grado de importancia, en cuyo caso los **routers** / **switches** intentan descartar los menos importantes primero. Por ejemplo, sería bastante grave si un **router** / **switch** para resolver una situación de congestión descartara paquetes de asfixia enviados por otro **router** / **switch**.

A veces el nivel de aplicación puede dar información sobre la prioridad de descarte de los paquetes. Por ejemplo en aplicaciones isócronas (audio y vídeo en tiempo real) suele ser preferible descartar el paquete viejo al nuevo ya que el viejo seguramente es inútil, mientras que en transferencia de ficheros es al contrario pues en muchos casos el receptor no aceptará el paquete nuevo mientras no reciba el viejo. En los ficheros MPEG (formato estándar de vídeo digital) algunos fotogramas son completos y otros son diferencias respecto a los fotogramas contiguos, descartar un paquete de un fotograma completo es más perjudicial. En ATM y Frame Relay existen situaciones en las que se le permite al usuario inyectar

en la red un ancho de banda superior al contratado, pero a condición de que dicho tráfico excedente sea susceptible de ser descartado en caso de congestión; para esto los **switches** ATM y Frame Relay marcan de cierta forma los paquetes que entran en la red con estas condiciones. En todos los casos es preciso que los paquetes poco importantes estén claramente identificados para que los **routers** / **switches** sepan descartarlos de manera selectiva en caso necesario.

2.8 CONTROL DEL JITTER (FLUCTUACIÓN)

En aplicaciones isócronas la fluctuación en el retardo o **jitter**, es tan importante o más que el retardo mismo.

Para intentar minimizar el **jitter** en la red es preciso que cada **router** / **switch** analice si el paquete va adelantado o atrasado respecto a su horario normal; si va adelantado lo pondrá al final de su cola, y si va atrasado lo pondrá al principio. De esta forma se reduce el **jitter** para todos los paquetes.

3. CALIDAD DE SERVICIO (QUALITY OF SERVICE, QOS) EN ATM

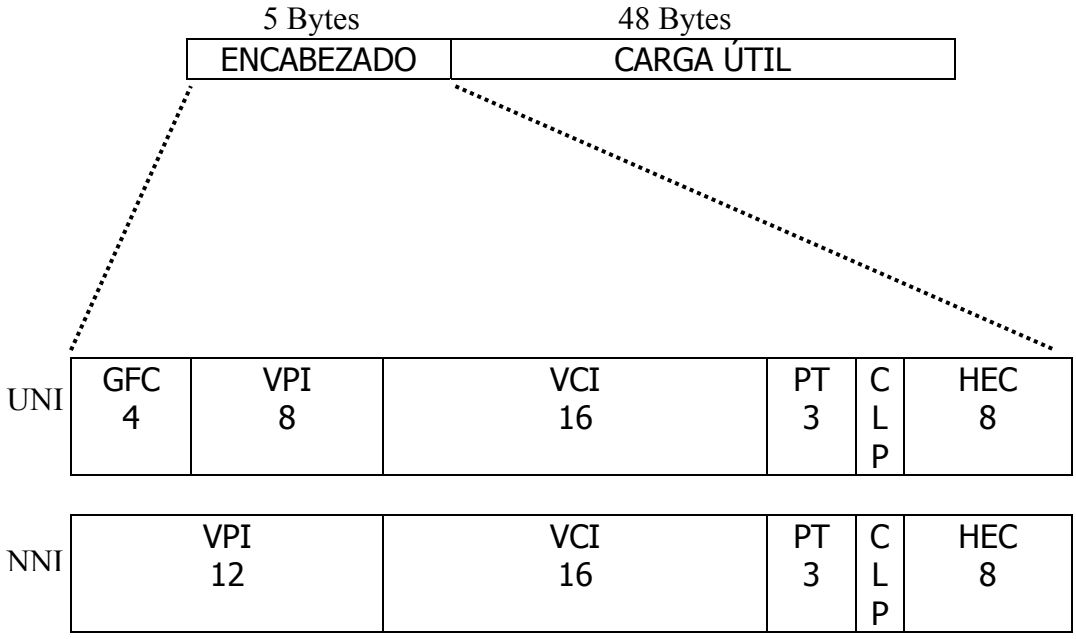
Las redes de modo de transferencia asíncrona (**Asynchronous Transfer Mode**, ATM), surgen como idea de un grupo de ingenieros de compañías telefónicas, como respuesta a una demanda de redes más rápidas y de mayor ancho de banda, para acomodarse a los crecimientos en los tamaños de ficheros y aplicaciones experimentados en el sector. Fundamentalmente ATM es una tecnología que simultáneamente trasmite tráfico de datos, voz y vídeo sobre circuitos de alto ancho de banda, generalmente cientos de mega bits por segundo (Mbps) en 1997 y Giga bits por segundo (Gbps) en la actualidad. La plataforma de **hardware** y **software** de ATM crea una arquitectura de comunicaciones basada en **switching** (conmutación) y transmisión de pequeñas unidades de información, llamadas celdas (**cells**), algunos también la llama células; estas celdas son de longitud fija, en concreto 53 bytes. Los bytes son enviados a la red uno a uno, en secuencia, y el propietario de la celda se determina por la información existente en la cabecera de la propia celda.

3.1 LA CELDA ATM

Como ya se ha mencionado ATM define una celda de tamaño fijo con una longitud de 53 bytes. Consta de dos partes: la carga útil o **payload** de 48 **bytes** que transporta la información generada por un emisor o transmisor, y el encabezamiento o **header** de 5 **bytes** que contiene la información necesaria para la transferencia de la celda. Las celdas son enviadas sobre una estructura de transmisión física, como por ejemplo el DS1, DS3 o SONET de Norte América; el E1, E3, E4 o STM de Europa.

Existen dos formatos de cabecera según se trate de la interfaz UNI (**Interface** usuario/red) o NNI (**Interface** nodo/red). La interfaz UNI conecta sistemas finales ATM (**hosts**, **routers**, etc.) a un **switch** ATM, mientras que la NNI puede ser definida como la interfaz que conecta a dos **switches** ATM.

Figura 4. Celda ATM



3.2 DESCRIPCIÓN DE LOS CAMPOS DE ENCABEZAMIENTO DE UNA CELDA ATM

- Control de Flujo Genérico (CFG, **Generic Flow Control**): Este campo consta de 4 bits que corresponden a los más significativos del primer byte. Este campo se puede utilizar desde la interfaz del usuario, para asegurar el acceso apropiado de varios terminales sobre un medio compartido (bus o anillo).

- Identificador de Camino Virtual (VPI, **Virtual Path Identifier**) y de Canal Virtual (VCI, **Virtual Circuit Identifier**): Representa una dirección lógica que identifica el circuito virtual al cual la celda esta conectada. Los campos de identificación VCI y VPI son esenciales para el enrutamiento y la multiplexación.

- Tipo de Carga Útil (PT, **Type Payload**): Este campo de información permite que el nodo ATM pueda distinguir en una conexión, si el contenido de las celdas corresponde a un usuario o es información de control y gestión de la red. El campo PT contiene 3 bits, en la tabla 1 se describen cada uno de los ocho valores posibles de este campo.

Tabla 1. Valores del Campo PT En La Celda ATM

VALOR PT	SIGNIFICADO
000	Celda de usuario tipo 0; no se detecta congestión
001	Celda de usuario tipo 1; no se detecta congestión
010	Celda de usuario tipo 0; se detecta congestión
011	Celda de usuario tipo 1; se detecta congestión
100	Información de mantenimiento entre conmutadores vecinos
101	Información de mantenimiento entre conmutadores de origen y destino
110	Celda de gestión de recursos (utilizada para control de congestión ABR)
111	Reservado

- Prioridad de Perdida de la Celda (CLP, **Cell Loss Priority**). Este campo se emplea para indicarle a la red cuáles celdas, dentro de una conexión determinada, son más sensibles a una pérdida que otra. Aquellas celdas que contienen el bit CLP en 1 tienen prioridad más baja y por tal motivo serán descartadas de la red en primera opción frente a una posible congestión de tráfico.

- Control de Errores de Encabezamiento (HEC, **Header Error Check**). Proporciona un CRC de los primeros 40 bits que detecta todos los errores simples y la mayoría de los errores múltiples. En el encabezamiento de las celdas, el transmisor calcula el valor HEC para la totalidad del encabezamiento de la celda, excluido el campo HEC.

3.3 FUNCIONAMIENTO DE ATM

Circuitos virtuales (VC, **virtual circuit**). ATM utiliza circuitos virtuales para crear enlaces (conexiones) individuales y transportar las celdas entre los nodos de la red. Las celdas de diferentes nodos pueden compartir un circuito virtual cuando viajan hacia un mismo destino. Estos circuitos virtuales llevan todas las

transmisiones de datos entre los nodos y mantienen la secuencia correcta de celdas y calidad de servicio a lo largo de toda la transmisión. Un circuito virtual puede atravesar más de un **switch** ATM. Los circuitos virtuales pueden ser permanentes o conmutados.

- Circuitos virtuales permanentes (PVC, **permanent virtual circuit**). Los Circuitos Virtuales Permanentes se configuran de manera estática en los **switches** y están presentes siempre que la red está operativa, estos circuitos son conexiones permanentes entre dos nodos de la red y operan como una línea física dedicada. En una implementación de PVC, la conectividad de red entre dos nodos es configurada estáticamente en los **switches**, y el identificador de Circuito Virtual (VCI **Virtual Circuit Identifier**) para cada nodo remoto es configurado en cada estación extremo.

- Circuitos virtuales conmutados (SVC, **switched virtual circuit**). Los circuitos virtuales conmutados, son creados dinámicamente para cada transmisión y son similares a la red telefónica de voz, en donde las conexiones entre dos puntos extremos de la red son creadas

dinámicamente para cada transmisión. Los SVC pretenden determinar la ruta disponible más corta desde la fuente hasta el destino.

Tanto para un PVC como para un SVC, antes de los que datos fluyan, los recursos requeridos tienen que ser asignados y luego que esto ocurra, permanecen asignados durante el circuito. Después de que el circuito ha sido establecido hay una política de seguimiento para que el tráfico cumpla con las condiciones acordadas. Cada **switch** a lo largo de la conexión valida que los recursos requeridos estén disponible.

El campo de información de las celdas ATM es llevado en forma transparente a través de la red. No se realiza ningún procesamiento, tal como control de errores, sobre este campo dentro de la red.

3.4 ATM Y LA CALIDAD DE SERVICIO

Después de conocer las características generales y el funcionamiento de ATM describiremos a continuación cómo la red de modo de transferencia asíncrona brinda calidad de servicio.

Debido a que ATM fue diseñada con el enfoque hacia la calidad de servicio, provee de alta velocidad, bajo retardo, bajo **jitter** (variación del retardo) y garantía de pérdida de celdas, características estas que definen la calidad de servicio para una conexión en particular, además de soportar prácticamente todos los tipos de tráfico.

Para conseguir las características mencionadas ATM realiza dos funciones muy importantes, primero que todo necesita hacer una diferenciación del tipo de tráfico soportado por esta red para lo cual define 4 clases de servicio donde agrupa el tráfico con exigencias de garantía similares; la segunda función es determinar unas políticas que permitan la mezcla de los distintos tipos de tráfico y que este fluya sin problemas.

3.4.1 Tipos de tráfico. Con el propósito de soportar varios tipos de tráfico se han definido las clases de servicios, cada una asociada a un grupo de parámetros de QOS.

Las clases o categorías de servicios con las que cuenta ATM se describen a continuación, éstas difieren en el nivel de garantía que dan al usuario respecto de la disponibilidad de los recursos de red solicitados.

3.4.2 Clases de servicios en ATM

- Servicio CBR **(Constant Bit Rate**, Tasa de Bits Constante). Garantiza una capacidad determinada y constante, independientemente de la utilización que haga de la red este u otros usuarios. Este servicio es el más sencillo de implementar y el más seguro de todos, ya que la red reserva la capacidad solicitada en todo el trayecto de forma estática. No se realiza ningún tipo de control de congestión, ya que se supone que ésta no puede ocurrir. Es equivalente a una línea dedicada punto a punto.

  La categoría de servicio CBR soporta aplicaciones en tiempo real, requiriendo una cantidad fija de ancho de banda. CBR soporta ajustadamente los parámetros MCTD (Máximo retardo de transferencia de una celda) y CDVT (Tolerancia en la variación en el retardo de una celda), los cuales se verán con más detalle a continuación. CBR es perfecto para aplicaciones que no puedan tolerar variaciones en la demora, como aquellas que manejan voz y vídeo en forma constante.

- Servicio VBR (**Variable Bit Rate**, Tasa de Bit Variable): Está pensado para cuando se prevé una elevada cantidad de tráfico de forma continuada. Tiene dos modalidades: RT-VBR (**Real Time** VBR), con requerimientos de

bajo retardo y **jitter** para cuando se trata de aplicaciones en tiempo real (videoconferencia, vídeo bajo demanda, etc.), y NRT-VBR (**Non Real Time** VBR) para cuando se trata de aplicaciones de tráfico elevado pero donde el retardo no es tan importante, por ejemplo correo multimedia o transmisión de ficheros MPEG por la red que son vistos luego por el usuario localmente de forma asíncrona en su computador. En VBR el usuario especifica un ancho de banda medio pero, en función de sus necesidades y del estado de la red, podrá en muchas ocasiones utilizar anchos de banda superiores, lo cual da mayor flexibilidad y permite al usuario ajustar más este recurso a sus necesidades medias reales. En algunos servicios VBR el tráfico excedente sale marcado con el bit CLP. Desde el punto de vista de la red VBR tiene una complejidad superior a CBR.

- Servicio ABR (**Available Bit Rate**, Tasa de Bit Disponible). ABR está pensado para tráfico a ráfagas, se supone que habrá instantes de gran demanda de capacidad seguidos de otros de total inactividad. La meta de este servicio es el de proveer dinámicamente el ancho de banda que actualmente no está en uso por otras categorías de servicios a usuarios que pueden ajustar sus transmisiones a esa tasa. ABR permite establecer un mínimo garantizado en el ancho de banda, y fijar un máximo orientativo. ABR es la única categoría de servicio ATM en la que se pronostica que la red

suministre control de flujo al emisor para que reduzca el ritmo en caso de congestión; esta circunstancia hace de ABR la categoría de servicio más apropiada para tráfico de datos, por ejemplo para enviar datagramas IP cuando no se utilicen aplicaciones isócronas, ABR también es recomendado en las interconexiones del tipo LAN, trasferencias de archivos de alta prestaciones, archivos de bases de datos y navegadores **web**. Sin embargo debido a su funcionalidad ABR es la categoría de servicio más compleja de implementar.

- Servicio UBR (**Unspecified Bit Rate**, Tasa de Bit No Especificada). Se puede considerar el de más baja calidad. No existe ningún tipo de garantías en cuanto al retardo o ancho de banda, y tampoco se informa al emisor en caso de congestión. UBR utiliza la capacidad sobrante en la red de las demás categorías de servicio. Puede utilizarse para emulación de LAN, IP sobre ATM y tráfico de misión no crítica.

La tabla 2 resume los distintos tipos de tráfico con sus exigencias para cada parámetro de calidad y la tabla 3 resume la aplicabilidad de cada uno de los servicios en las aplicaciones de mayor uso en ATM.

Tabla 2. Tipos de Tráfico Y Sus Exigencias de Calidad.

	RETARDO	VARIACIÓN DEL RETARDO	RELIABILITY
CORREO	BAJO	BAJO	ALTO
TRANSFERENCIA DE ARCHIVOS	BAJO	BAJO	ALTO
BASE DE DATOS	BAJO / MEDIO	BAJO	ALTO
VIDEOS (MPEG)	ALTO	MEDIO	BAJO
TELEFONÍA	ALTO	ALTO	BAJO
VIDEOCONFERENCIA	ALTO	ALTO	BAJO

Tabla 3. Resumen de Aplicación de Los Servicios de La Red ATM.

APLICACIÓN	CBR	RT - VBR	NRT - VBR	ABR	UBR
Datos Críticos	Bueno	Aceptable	Excelente	Aceptable	NO
Interconexión de LAN's	Aceptable	Aceptable	Bueno	Excelente	Bueno
Trasporte de WAN	Aceptable	Aceptable	Bueno	Excelente	Bueno
Emulación de Circuitos	Excelente	Bueno	NO	NO	NO
Telefonía y Videoconferencia	Excelente	Bueno	NO	NO	NO
Audio comprimido	Aceptable	Excelente	Bueno	Bueno	Aceptable
Distribución de video	Excelente	Bueno	Aceptable	NO	NO
Multimedia Interactivo	Excelente	Excelente	Bueno	Bueno	Aceptable

3.4.3 Parámetros de las clases de servicios. Como se mencionó anteriormente cada clase de servicio tiene asociada un grupo de parámetros que

definen los niveles mínimos de calidad que se debe ofrecer al usuario de la red para cada categoría de servicio. Estos parámetros podemos clasificarlos en dos grupos, los parámetros de tráfico y los parámetros de calidad de servicio.

3.4.3.1 Parámetros de tráfico.

- PCR (**Peak Cell rate**, Tasa De Celdas Máxima): Máxima velocidad con la que una conexión ATM puede enviar celdas sin que se produzcan pérdidas.

- SCR (**Sustained Cell Rate**, Tasa De Celdas Sostenida): Velocidad media con la que una conexión ATM puede enviar celdas.

- MCR (**Minimum Cell Rate**, Tasa De Celdas Mínima): Velocidad mínima que el usuario o la aplicación considera aceptable para efectuar la conexión.

- MBS (**Maximum Burst Size**, Tamaño Máximo De La Ráfaga): Máxima ráfaga que puede enviarse por una conexión sin que se produzcan pérdidas.

3.4.3.2 Parámetros de calidad de servicio para la Tecnología ATM.

- MCTD (**Maximum Cell Transfer Delay**, Máximo Retardo De Transferencia De Una Celda): Es el retardo o latencia máximo permitido, es decir, el tiempo máximo que puede tardar la red en transmitir una celda de un extremo a otro de la conexión.

- CDVT (**Cell Delay Variation Tolerance**, Tolerancia En La Variación En El Retardo De Una Celda): Es el **jitter** o máxima variación que se podrá producir en el retardo de las celdas.

- CLR (**Cell Loss Ratio**, Tasa De Pérdida De Celdas): Porcentaje máximo aceptable de celdas que la red puede descartar debido a congestión. Cuando una celda es entregada en el destino con un retardo superior a MCTD se considera perdida.

No todos estos parámetros tienen sentido en todas las clases de servicios, en la tabla 4 se muestran aquellos que normalmente son empleados por cada servicio.

Tabla 4. Resumen de Los Parámetros Empleados Por Cada Servicio ATM.

	CBR	VBR - RT	VBR -NRT	ABR	UBR	UBR +
PCR	SI	SI	SI	SI	NO	NO
SCR	NO	SI	SI	NO	NO	NO
MCR	NO	NO	NO	SI	NO	SI
MBS	NO	SI	SI	NO	NO	NO
MCTD	SI	SI	SI	SI	NO	NO
CDVT	SI	SI	NO	NO	NO	NO
CLR	SI	SI	SI	SI	NO	NO

3.4.4 Políticas de Tráfico. Los flujos en ATM se asocian a un circuito virtual (VC), los cuales pueden ser permanentes (PVC) o conmutados (SVC). Tanto para un PVC como para un SVC, antes de los que datos fluyan, los recursos requeridos tienen que ser asignados y permanecen asignados durante el circuito. Cada **switch** valida que los recursos requeridos estén disponibles. Después de que el circuito ha sido establecido hay una política de seguimiento para que el tráfico cumpla con las condiciones acordadas.

La designación de estas políticas es, precisamente, la segunda función realizada por ATM para garantizar la calidad de servicio, se determinan normas de tráfico para controlar que un usuario no exceda los límites de ancho de banda pactados en su contrato de servicio, esto se logra evaluando cada una de las celdas que entran en el **switch**.

La implementación de las políticas de tráfico se lleva a cabo a través del algoritmo **Leaky Bucket** descrito anteriormente.

3.4.5 Conformación y vigilancia del tráfico. Puesto que ATM está concebida para ofrecer calidad de servicio a sus usuarios es importante que dicho usuario no exceda los límites de ancho de banda pactados en su contrato de servicio. Las tareas dedicadas a este fin, que pueden ser desarrolladas tanto por el usuario o por la red, se denominan conformación de tráfico o **traffic shaping**. Además, la red ha de verificar que efectivamente el usuario no excede sus límites, y aplicar medidas correctoras en caso contrario; a esta labor de vigilancia se la denomina **traffic policing**, o vigilancia del tráfico, ambas tareas, conformación y vigilancia, están íntimamente relacionadas.

Los mecanismos de control de tráfico dependen mucho de la categoría de tráfico que se esté tratando. En el caso de tráfico CBR el usuario dispone de una capacidad asignada a él de forma absolutamente estática, por lo que la labor de conformación y vigilancia es muy simple.

Ejemplo: un usuario contrata un circuito CBR con un PCR de 10000 celdas/s (equivalente a 4,24 Mb/s), en este caso el usuario estará autorizado a introducir una celda en la red cada 100 ms, si su conexión física con la red ATM es un enlace

OC3 (155,52 Mb/s) el usuario tardará 2,7 ms en enviar una celda, por lo que después de cada envío deberá estar como mínimo 97,3 ms sin enviar otra, ya que de lo contrario excedería su PCR y el conmutador descartaría todas las celdas que llegaran antes del plazo previsto.

El otro extremo es el de tráfico UBR. Aquí el usuario no especifica ningún parámetro de calidad de servicio, por lo que recibe un servicio **best effort** (Mejor esfuerzo); normalmente esto se traduce en que los circuitos UBR utilizan la capacidad sobrante al resto de tráfico en la red, con lo que un usuario UBR puede llegar a emplear su enlace físico al máximo de su capacidad sin que se le apliquen medidas correctoras, pero este tráfico de mínima prioridad será desplazado en cuanto otros usuarios tengan alguna necesidad.

El tráfico ABR fija una capacidad mínima requerida (MCR) y una máxima prevista (PCR), en caso de ráfagas la red asegura la disponibilidad de MCR, pero no promete nada respecto a PCR, que estará sujeto a disponibilidad. Dado que el usuario recibe realimentación de la red en caso de congestión, se supone que si inyecta un tráfico superior a MCR y la red no puede soportarlo recibirá mensajes de congestión que le harán reducir el ancho de banda. No se establece la duración de las ráfagas (parámetro MBS) ya que éstas pueden tener una duración considerable en ratos de baja carga en la red.

El control de tráfico VBR es el más complejo. Los parámetros especificados, SCR, PCR y MBS permiten especificar un algoritmo **Leaky Bucket** (Pozal Agujereado). En el caso más sencillo se utilizaría SCR como ancho de banda *r*, MBS sería el tamaño del **buffer** *C*, y PCR el ancho de banda con que el **host** envía los datos al pozal (del algoritmo **Leaky Bucket**). Pero cabe aclarar que el ancho de banda medio de un tráfico VBR no debería nunca superar el SCR.

3.4.6 Control de congestión, control de admisión y reserva de recursos.

Como ATM ofrece un servicio orientado a conexión resulta relativamente sencillo comprobar en el momento de establecer la conexión si existen en la red recursos suficientes para ésta, y denegarla en caso contrario. En algunos servicios la solicitud de establecer el circuito virtual viene acompañada de unos requerimientos medios y máximos de ancho de banda, con los que es posible realizar una reserva de recursos en todas las líneas del camino.

4. CALIDAD DE SERVICIO (QUALITY OF SERVICE, QOS) EN FRAME RELAY

Frame Relay comenzó como un movimiento a partir del mismo grupo de normalización que dio lugar a X.25 y RDSI, El ITU (entonces CCITT). Sus especificaciones fueron definidas por ANSI, fundamentalmente como medida para superar la lentitud de X.25, eliminando la función de los **switches**, en cada salto de la red (control de errores y de flujo).

Frame Relay se define, oficialmente, como un servicio portador RDSI de banda estrecha en modo de paquetes. La información transmitida en una trama Frame Relay puede oscilar entre 1 y 8.000 bytes, aunque por defecto es de 1.600 bytes.

La técnica Frame Relay combina altas tasas de transferencia, bajos retardos, puertas compartidas y asignación dinámica de ancho de banda.

4.1 PRINCIPIOS BÁSICOS

El protocolo Frame Relay se basa en los tres principios siguientes:

- El medio de transmisión y las líneas de acceso están prácticamente libres de errores.

- La corrección de errores se proporciona por los niveles superiores de los protocolos de las aplicaciones de usuario.

- La red, en estado normal de operación, no está congestionada, y existen mecanismos estándares de prevención y tratamiento de la congestión.

4.2 LA TRAMA FRAME RELAY

Frame Relay es una red de conmutación de paquetes orientada a conexión, por Lo tanto para que la comunicación sea posible es necesario antes que se establezca un circuito virtual entre dos **hosts** de la red, igual que en ATM los circuitos virtuales pueden ser permanentes o conmutados, y se identifican mediante los DLCI (**Data Link Connection Identifier**). Estos DLCI tienen por defecto 10 bits de longitud, aunque se han definido extensiones que permiten utilizar DLCI's de 16, 17 o 23 bits.

Figura 5. Trama Frame Relay

1 Byte	2 Bytes	n Bytes	2 Bytes	1 Byte
SEÑALIZADOR	CABECERA	INFORMACIÓN (0 - 8188)	CFC	SEÑALIZADOR

Lo más importante de la trama Frame Relay se encuentra en el campo dirección, ya que es aquí donde se establecen las conexiones.

El campo dirección tiene la siguiente estructura:

Figura 6. Campo Dirección de La Trama Frame Relay

DLCI	CR	EA	DLCI	FECN	BECN	DE	EA

4.3 DESCRIPCIÓN DE LOS CAMPOS DE DIRECCIÓN DE UNA TRAMA FRAME RELAY

- DLCI (**Data Link Connection Identifier**). Este campo tiene una longitud total de 10 bits (aunque se encuentre dividido en dos partes). Especifica por cual circuito virtual debe circular la trama correspondiente.

- C/R (**Command/Response**). El significado de este bit es específico de la aplicación y no se utiliza en el protocolo Frame Relay estándar.

- FECN (**Forward Explicit Congestion Notification**). Como su nombre lo indica este campo de un bit se emplea en el control de congestión, detallado más adelante.

- BECN (**Backward Explicit Congestion Notification**). Este campo se explicará al referirnos al control de congestión en Frame Relay.

- DE (**Discard Elegibility**): Este bit sirve para marcar las tramas de segunda clase (de menor prioridad), que son aquellas que el usuario ha metido en la red superando el ancho de banda que tenía contratado.

4.4 FUNCIONAMIENTO DE FRAME RELAY

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay. También incorporan los nodos que conmutan las tramas Frame Relay en función del identificador de conexión, a través de la ruta establecida para la conexión en la red. Este equipo se denomina FRAD o

Ensamblador/Desensamblador Frame Relay (Frame Relay **Assembler Disassembler**) y el nodo de red se denomina FRND o Dispositivo de Red Frame Relay (Frame Relay **Network Device**).

Las tramas y cabeceras de Frame Relay pueden tener diferentes longitudes, ya que hay una gran variedad de opciones disponibles en la implementación.

4.5 FRAME RELAY Y LA CALIDAD DE SERVICIO

En Frame Relay cada conexión puede negociar varios parámetros, además esta red tiene sus mecanismos para el control de la congestión y el tráfico.

4.5.1 Control de tráfico en Frame Relay. El control de tráfico en Frame Relay se basa en la especificación de varios parámetros, sobre todo el denominado CIR (**Committed Information Rate**). El CIR se especifica en el momento de configurar los equipos en el caso de conexiones permanentes, o bien es solicitado por el usuario en el momento de efectuar una conexión temporal; en este último caso puede haber un proceso de negociación, es decir, la red puede no ser capaz de satisfacer la capacidad solicitada, en cuyo caso normalmente realiza una contraoferta, el usuario decide entonces si acepta dicha propuesta o si abandona para intentar en otro momento.

El control de tráfico en Frame Relay se realiza de la siguiente forma. El **switch** Frame Relay al que está conectado el equipo del usuario realiza una monitorización permanente del tráfico que el usuario inyecta en la red por cada conexión virtual que tiene establecida. Si el usuario no supera en ningún momento el CIR sus tramas viajarán todas con el bit DE a cero, sin embargo si el usuario excede dicha capacidad el **switch** Frame Relay pondrá a 1 el bit DE en aquellas tramas que hayan sido enviadas por encima de la capacidad especificada en el CIR. Un segundo parámetro, conocido como EIR (**Excess Information Rate**), especifica un ancho de banda que el usuario no deberá superar nunca, ya que las tramas recibidas por encima de este valor serán directamente descartadas por el **switch**.

La descripción realizada arriba utiliza en realidad otros dos parámetros:

- B_c Tamaño de ráfaga comprometida (**Committed burst size**). Indica la cantidad máxima de bits que la red se compromete a enviar en condiciones normales durante un intervalo de tiempo T. Estos datos pueden estar o no contiguos, es decir pueden formar parte de una o de varias tramas.

- B_e: Tamaño de ráfaga excedente (**Excess burst size**). Indica la máxima cantidad de bits que, además de B_c, , podrá el usuario intentar enviar por la

red, durante un intervalo de tiempo T. No hay compromiso en la transferencia de estos datos.

Entre los parámetros B_c y CIR se cumple la relación: $B_c = CIR * T$

Análogamente entre B_e y el EIR se cumple la relación: $B_e = EIR * T$

Ejemplo: supongamos que un usuario contrata con una empresa telefónica un acceso Frame Relay con una línea física E1, es decir con una capacidad máxima entre su computador y el **switch** Frame Relay de 2048 Kb/s. El usuario contrata además un PVC con un CIR de 1024 Kb/s; la empresa telefónica configura el enlace con un EIR de 384 Kb/s y establece el valor de T en 1 segundo (con lo que automáticamente han quedado fijados los valores de B_c y B_e en 1024000 y 384000 bits). Obsérvese que aunque se han definido varios parámetros el único especificado en el contrato del usuario con la empresa telefónica (y el único de cuyo valor el usuario tiene conocimiento oficial) es el CIR.

En esta situación el usuario desea enviar un flujo de vídeo en tiempo real a un destino remoto, sin ningún tipo de control de flujo por parte del receptor y sin atender a ninguna notificación de congestión que pueda venir de la red. Suponemos que el usuario dispone de un parámetro en su computador mediante

el cual puede fijar el ancho de banda de tráfico que inyecta en la red. Supongamos también que el envío se hace utilizando siempre tramas de 50000 bits (6250 bytes). Si el usuario fija el flujo de datos a transmitir en 2000 Kb/s estará inyectando en el **switch** Frame Relay 40 tramas por segundo; en estas condiciones las primeras veinte tramas serán aceptadas sin más, las ocho siguientes serán aceptadas pero se les pondrá a uno el bit DE ya que superan el valor de B_c, y las doce restantes serán simplemente descartadas puesto que superan el valor de B_e.

Si el usuario reduce ahora el ancho de banda a 1400 Kb/s enviará 28 tramas por segundo, 20 de las cuales tendrán el bit DE a cero y las ocho siguientes a uno, de esta forma el usuario está aprovechando casi al máximo la capacidad de la red, pero no tiene la seguridad de que todas las tramas lleguen a su destino.

Por último, si el usuario quiere tener máximas garantías de que todas las tramas llegarán a su destino deberá reducir el flujo a un valor no superior al CIR, por ejemplo a 1000 Kb/s, en cuyo caso emitirá 20 tramas por segundo y todas serán enviadas con el bit DE a cero.

El bit DE también puede ser puesto de forma voluntaria por el usuario. Esto serviría si el usuario (o la aplicación) puede identificar algunas tramas como más importantes que otras.

4.5.2 Control de congestión en Frame Relay. Cuando se produce congestión en una red Frame Relay se aplica la técnica de paquetes de asfixia que se describió en la sección 2 de esta monografía; de esta forma se advierte a los **hosts** emisores de la situación para que adopten medidas correctoras. En caso de que dichos avisos no sean atendidos, o no lleguen con la suficiente rapidez, la red empezará a descartar tramas, primero las que tengan a 1 el bit DE, y si esto no es suficiente también las demás.

Para detectar cuando hay peligro de congestión los **switches** Frame Relay monitorizan constantemente el tamaño de cada una de sus colas; cuando algún valor es superior a un límite considerado peligroso el **switch** correspondiente deberá identificar la conexión o conexiones causantes del problema, y advertir a los correspondientes **hosts**. Cualquier **switch** de la red puede tomar la iniciativa de enviar avisos de congestión a los **hosts** que considere responsables de la situación, o que sin ser responsables puedan poner remedio. El aviso de congestión normalmente viaja **piggybacked** en una trama de datos, en los bits

denominados FECN y BECN del campo dirección. El significado de los bits FECN y BECN es el siguiente:

- BECN (**Backward Explicit Congestion Notification**): se pone a uno para indicar a un **host** que existe congestión en la red, y que el problema se ve agravado por el tráfico que él está introduciendo precisamente por el DLCI por el que ha recibido el aviso, y que por tanto debe iniciar los procedimientos previstos para reducir el ancho de banda de tráfico que está inyectando en ese DLCI. La denominación **backward** indica que la congestión se está produciendo en sentido contrario al que viaja el aviso.

- FECN (**Forward Explicit Congestion Notification**): se pone a uno para indicar a un **host** que existe congestión en la red, y que el problema se ve agravado por el tráfico que él está recibiendo por el DLCI por el que ha recibido el aviso; por tanto el **host** deberá emplear los mecanismos a su alcance para conseguir que su interlocutor introduzca un ancho de banda de tráfico menor en ese DLCI. La denominación **forward** indica que la congestión en este caso se produce en el mismo sentido en que viaja el aviso.

Ejemplo: Supongamos que dos **hosts**, A y B, establecen un circuito a través de una red Frame Relay, y que se produce una situación de congestión en la red, de forma que afecta a la comunicación en el sentido A->B, pero no en el sentido contrario. En este caso las tramas que A recibirá de la red llevarán puesto a 1 el bit BECN, y las que reciba B llevarán a 1 el bit FECN.

En Frame Relay se prevé también la posibilidad de que un **switch** envíe una trama de control especial a un **host** en situaciones de congestión, cuando no haya tráfico de retorno en ese DLCI que permita enviar el aviso en el bit BECN.

En todos los casos Frame Relay no define las acciones a desarrollar en caso de congestión. Se supone que los protocolos de nivel superior adoptarán las medidas que consideren más oportunas.

5. ESTÁNDAR 802.1P

Como se estudió en los capítulos 3 y 4 la Calidad de Servicio es un tema relacionado directamente con las redes orientadas a conexión, como ATM y Frame Relay, por lo que no resulta tan sencillo poderlo implementar en redes no orientadas a conexión como la mayoría de las LAN's incluyendo Ethernet, sin embargo buscando obtener algún tipo de Calidad de Servicio en este tipo de redes se ideó el estándar 802.1p el cual estudiaremos en el presente capítulo.

5.1 NACIMIENTO DEL ESTANDAR 802.1P

El subcomité 802.1Q elaboró un estándar que permite etiquetar tramas en una LAN. Esto se utiliza normalmente con dos finalidades diferentes:

- Distinguir tramas pertenecientes a diferentes VLAN's (**Virtual LAN's**) cuando se mezclan en un enlace troncal. Para esto se utiliza un campo de 12 bits.

- Marcar un nivel de prioridad a cada trama. El funcionamiento de prioridades en la LAN lo especifica el estándar 802.1p, el que nos interesa en este proyecto. La norma 802.1p permite establecer calidad de servicio en una

LAN para satisfacer las exigencias de ciertas aplicaciones, como las de tiempo real.

Los desarrollos en 802.1p se centran en la definición de prioridades (clases de servicio) más que en calidad de servicio propiamente dicha.

5.2 CALIDAD DE SERVICIO CON 802.1P

A continuación veremos cómo es posible conseguir calidad de servicio en redes LAN's a través de este estándar, para tal motivo se explicarán los parámetros de QoS que estas redes están en capacidad de proporcionar y se mencionarán las distintas clases de servicios.

5.2.1 Parámetros de QoS. Las redes de área local no garantizan la mayoría de los parámetros, vistos en el capítulo 1, necesarios para la obtención de QoS, se muestran a continuación aquellos soportados:

- Disponibilidad. La disponibilidad del servicio se mide como esa fracción de un cierto tiempo total durante el cual se proporciona un servicio MAC. Las operaciones que realice el **switch** pueden aumentar o bajar la disponibilidad del servicio. Aumenta si evitan en el camino de datos aquellos

componentes de la red que estén fallando. Disminuye si falla el **switch**, si el puente deniega el servicio o debido al filtrado de tramas de los **switches**.

- Pérdida de tramas. MAC no garantiza la entrega de las tramas. Éstas pueden no alcanzar las estaciones finales como resultado de:

  Corrupción de la trama durante su transmisión/recepción a través de la capa física.

  Que la trama sea descartada por el **switch** debido a:

  1. No pueda transmitirla en el período máximo determinado, desechándola antes de que ésta supere su período de vida máximo.

  2. Los **buffers** donde se almacenan las mismas estén llenos sin darles tiempo a vaciarse.

  3. El tamaño de la unidad de datos de servicio sea mayor que el tamaño máximo soportado por el procedimiento MAC empleado en la LAN.

4. En ocasiones es necesario descartar tramas para mantener otras opciones de QoS.

- Reordenación de tramas. No se permite la reordenación de tramas según una prioridad de usuario para una determinada combinación dirección fuente – dirección destino.

- Duplicación de tramas. MAC no permite duplicar tramas. Los **switches** no introducen la duplicación de tramas de datos de usuario. Las posibilidades de duplicar se reducen al envío a través de distintos caminos entre fuente-destino.

- Retardo de tránsito. MAC introduce retardo dependiendo del tipo de medio utilizado. El valor de retardo se calcula sobre las unidades de datos transmitidas con éxito.

- También existe el retardo introducido por un determinado **switch**. Es el tiempo transcurrido entre la recepción de la trama más el tiempo en acceder al medio por el que va a ser transmitido.

- Tiempo de vida de la trama. Es un límite superior al retardo de tránsito. El máximo tiempo de vida de una trama es necesario para asegurar las operaciones correctas de los protocolos de capas superiores. Para asegurar este valor máximo los **switches** pueden optar por descartar tramas, asegurando así un retardo máximo en cada **switch**.

- Tasa de error de trama no detectada. MAC introduce un nivel muy bajo de tasa de error de trama no detectado en las tramas ya transmitidas. Para protegerse ante estos errores se utiliza un secuencia de chequeo de trama (FCS) dependiente del método MAC utilizado. El valor de FCS se recalcula cuando se está ante distintos métodos.

- Tamaño máximo de la unidad de datos de servicio. El tamaño máximo de esta unidad de datos varía con el método MAC utilizado. Hay que tener en cuenta que el valor máximo soportado por dos LAN's es el más pequeño del soportado independientemente por cada una de ellas.

- Prioridad. Un parámetro de QoS permitido e incluido por MAC es la prioridad de usuario. La subcapa MAC asocia las prioridades de usuario solicitadas sobre las prioridades de acceso soportadas por cada uno de los métodos individuales MAC utilizados.

- Rendimiento. Una red LAN construida con **switches** incrementa significativamente el rendimiento en comparación con cualquier simple red de área local, debido a las características de estos elementos, entre ellas porque los **switches** pueden localizar el tráfico dentro de las redes LAN's a través del filtrado de tramas.

5.3 PRIORIDADES DE USUARIO Y CLASES DE TRÁFICO

La norma 802.1p permite 8 tipos de clases de tráfico clasificados como prioridades de usuario (**user_priority**) por cada puerto del **switch**, siendo el rango de valores de prioridad de usuario del 0 al 7. Para conseguirlo se necesitan 3 bits.

La prioridad del tráfico en redes LAN va a depender también del número de colas existentes en cada puerto. El almacenamiento de las tramas en estas colas se realiza en base al campo **user_priority** y a la dirección origen y destino.

Una vez determinadas las clases de tráfico por **switch**, será necesario mapearlas (asociarlas) con el tipo de tráfico que circule por la red para asegurar que el tráfico en tiempo real, por ejemplo, sea atendido antes que el tráfico para el que un servicio de mejor esfuerzo basta.

El tráfico podría subdividirse en los siguientes grupos:

- Control de red (máxima importancia)
- Voz**:** retardo < 10 mseg.
- Vídeo: retardo < 100 mseg.
- Carga Controlada (algunas aplicaciones importantes).
- **Excellent Effort** (como mejor esfuerzo para usuarios importantes).
- Mejor esfuerzo (prioridad por defecto en la LAN).
- **Background** (juegos, etc.).

En la tabla 5 se muestra cómo se podría asociar el campo **user_priority** al tráfico:

Tabla 5 Campo User_Priority Y Tipos de Tráfico.

PRIORIDAD DE USUARIO	TIPO DE TRÁFICO
0	**Excellent Effort (or Business Critical)**
1	**Background**
2	**Spare**
3	**Best Effort**
4	Aplicaciones de carga controlada
5	Vídeo interactivo < 100 mseg latencia y **jitter**
6	Voz interactiva < 10 mseg latencia y jitter
7	Control de red

Teniendo en cuenta los distintos tipos de tráfico y el número de colas existentes, el tráfico se subdividirá en grupos, de forma que en el caso de que solo existieran dos colas por puerto se recomienda que a los tráficos de las clases 4 al 7 se les asigne la cola de alta prioridad y que a los tráficos de las clases 0 al 3 se les asigne la cola de baja prioridad, si existen 3 colas se hará una tercera subdivisión del tráfico y así consecutivamente.

5.4 FUNCIONAMIENTO DE LOS SWITCHES

Una vez establecidas todas estas asociaciones nos preguntamos cómo utiliza esta información el **switch**. El **switch**, para transmitir las tramas, mira por cada uno de los puertos la clase de tráfico que estos soportan, escogiendo de entre ese tipo de tráfico aquellas tramas que se encuentren en las colas de mayor prioridad (y si

hay colas de un nivel mayor deben estar vacías), habiéndose realizado previamente una asignación de colas según la tabla 5, enviando así el tráfico considerado más prioritario.

6. CONFIGURACIÓN DE QOS EN EL LABORATORIO DE REDES DE LA CUTB

En este capítulo se verá una guía genérica sobre cómo configurar QoS en **switches** Cisco Catalyst 2950, con los cuales se cuenta en el laboratorio de redes de la CUTB.

6.1 PRERREQUSITOS PARA CONFIGUAR QOS

Antes de configurar QoS, debes haber comprendido los siguientes ítems:

- Los tipos de aplicaciones usadas, el tráfico y el diseño en tu red.

- Las características y necesidades de tu red. ¿Está el tráfico en ráfagas? ¿Necesitas reservar ancho de banda para flujos de voz y vídeo ?.

- Requerimientos de ancho de banda y velocidad de la red.

- Localización de los puntos de congestión en la red.

6.2 CONFIGURACIÓN QOS POR DEFECTO DEL SWITCH CATALYST 2950

La tabla 6 muestra la configuración por defecto del **switch** Cisco Catalyst 2950.

Tabla 6. Configuración por defecto del switch Cisco Catalyst 2950.

El valor CoS por defecto del puerto es 0
El estado de obligación del puerto por defecto es sin obligación *
Las políticas de asociación no están configurados *
La Vigilancia no está configurada *
La asociación CoS – a – DSCP por defecto es mostrada en la tabla 12 *
La asociación DSCP – a – Cos por defecto es mostrada en la tabla 14 *

* Disponible solo en **switches** ejecutando el **software** mejorado.

6.3 GUÍA DE CONFIGURACIÓN

Antes de empezar con la configuración de QoS, debes tomar en cuenta la siguiente información:

- Si tienes puertos Ethernet configurados en tu **switch**, debes configurar clasificación QoS, vigilancia, asociación y encolado en cada puerto físico que contiene Ethernet.

- No es posible asociar fragmentos IP contra IP extendido configurado con ACL´s para forzar QoS. Los fragmentos IP son transmitidos como mejor

esfuerzo. Los fragmentos IP están denotados por campos en el encabezado IP.

- El control del tráfico recibido por el **switch** está sometido a todo el procesamiento QoS de entrada.

- Solo una ACL por clase asociada y solo un comando **match** por clase asociada están soportados. La ACL puede tener múltiples entradas de control de acceso, lo cual son comandos que asocian campos contra el contenido del paquete.

- Las políticas de asociación con clasificación ACL en la dirección de salida no están soportadas y no pueden ser adjuntadas a una interface usando el comando de configuración de interface **service-policy input policy-map-name.**

- En una asociación de política, la clase nombrada **class-default** no está soportada. El **switch** no filtra tráfico basado en la asociación de política definido por el comando de configuración de asociación de política **class-default.**

6.4 CONFIGURANDO CLASIFICACIÓN DE TRÁFICO USANDO EL ESTADO DE ACTIVACIÓN DE PUERTOS

En esta sección se describe cómo clasificar el tráfico entrante usando el estado de activación de puertos.

6.4.1 Configurando el estado de activación de puertos dentro de un dominio de QoS

Nota: esta característica está disponible solo si tu **switch** está ejecutando el **software** mejorado.

Los paquetes entrantes a un dominio QoS son clasificados en la frontera del dominio de QoS. Cuando los paquetes son clasificados en la frontera., el puerto del **switch** dentro del dominio de QoS puede ser configurado a uno de los estados de activación porque no hay necesidad de clasificar los paquetes en todo el **switch** dentro de dominio de QoS.

Se comienza en el modo EXEC privilegiado y se siguen los pasos indicados en la tabla 7 para configurar el puerto y obligar la clasificación del tráfico que recibe.

TABLA 7. Pasos para configurar puertos y obligar la clasificación del tráfico que recibe.

	Comando	Propósito
Paso 1	**Configure Terminal**	Entra al modo de configuración global
Paso 2	**Interface** Interface – id	Entra al modo de configuración de interface y especifica la interface a ser obligada.
Paso 3	**Mls qos trust** [**cos / dscp**]	Configura el estado de obligación del puerto. Por defecto el puerto no está obligado. Usa el parámetro **cos** si tu red está compuesta por LAN's Ethernet, **switches** Cisco Catalyst 2950 y no tienes más de dos tipos de tráfico. Use el parámetro **dscp** si tu red no está compuesta por solo LAN's Ethernet y estás familiarizado con sofisticadas características e implementaciones QoS. Entra el parámetro **cos** si quieres que los paquetes entrantes sean clasificados con los valores CoS del paquete. Para los paquetes IP etiquetados, el valor DSCP es modificado basado en la asociación CoS – a - DSCP la cola de salida asignada al paquete está basada en el valor CoS del paquete. Entra el parámetro **dscp** si quieres que los paquetes entrantes sean clasificados con sus valores DSCP.
Paso 4	**End**	Regresa al modo EXEC privilegiado.
Paso 5	**Show mls qos Inteffface** [interface – id] [**policers**]	Verifica las entradas.
Paso 6	**Copy running – config startup-config**	(Opcional) guarda las entradas en un archivo de configuración.

Para regresar un puerto a su estado de no activado, use el comando de configuración de interface **no mls qos trust.**

6.4.2 Configurando los valores de qos para una interface

Nota: ambos, el **software** mejorado y estándar soportan esta característica.

QoS asigna los valores de CoS especificados con el comando de configuración de interface **mls qos cos.**

Se comienza en el modo EXEC privilegiado y se siguen los pasos indicados en la tabla 8 para definir los valores CoS por defecto de un puerto o para asignar los valores CoS por defecto a todos los paquetes entrantes en el puerto.

Tabla 8. Pasos para definir los valores CoS por defecto de un puerto

	Comando	Propósito
Paso 1	**Configure Terminal**	Entra al modo de configuración global
Paso 2	**Interface** *Interface – id*	Entra al modo de configuración de interface y especifica la interface a ser obligada.
Paso 3	**Mls qos cos** { *default – cos* | **override** }	Configura los valores CoS por defecto para el puerto. Para *default – cos*, especificar un valor CoS por defecto para ser asignado a un puerto. Si el puerto está activado con Qos y los paquetes están sin etiquetar, los valores CoS por defecto se convierten en los valores CoS para el paquete. El rango de CoS

		es de 0 a 7. Usa el parámetro **override** para sustituir la configuración previa de estado de activación de la entrada de paquetes y aplicar los valores CoS por defecto del puerto a todos los paquetes entrantes. Por defecto Cos **Override** está deshabilitado. Use el parámetro **Override** cuando todos los paquetes entrantes en ciertos puertos merecen mayor prioridad que los paquetes entrantes de otros puertos. Incluso si un puerto tuvo una configuración previa de DSCP activado, este comando sustituye la configuración previa del estado de activación y todos los valores CoS de entrada son asignados al valor CoS por defecto configurado con este comando. Si un paquete entrante está etiquetado, el valor CoS del paquete es modificado con el CoS por defecto del puerto en el puerto de salida.
Paso 4	**End**	Regresa al modo EXEC privilegiado.
Paso 5	**Show mls qos Intefface**	Verifica las entradas.
Paso 6	**Copy running – config startup-config**	(Opcional) guarda las entradas en un archivo de configuración.

Para regresar a la configuración por defecto, use el comando de configuración de interface **no mls qos cos** { *default – cos* / **override** }

6.5 CONFIGURANDO POLÍTICAS DE QOS

Nota: esta característica está disponible solo si tu **switch** está ejecutando el **software** mejorado.

Configurar una política de QoS típicamente requiere la clasificación del tráfico en clases, configurar guardias o vigilantes (que controlen el tráfico) aplicados a estas clases de tráfico y añadir guardias a las interfaces.

6.5.1 Clasificando tráfico usando ACL's

Puedes clasificar tráfico IP usando ACL's IP estándar o IP extendido; puedes clasificar tráfico de capa 2 usando ACL's MAC de capa 2. En este proyecto solo veremos la clasificación de tráfico capa 2 que es el que nos interesa.

Se comienza en el modo EXEC privilegiado y se siguen los pasos indicados en la tabla 9 para crear una ACL MAC capa 2 para el tráfico de capa 2.

Tabla 9 Pasos para crear una ACL MAC capa 2 para el tráfico de capa 2.

	Comando	Propósito
Paso 1	**Configure Terminal**	Entra al modo de configuración global
Paso 2	**Mac access-list extended** *name*	Crea una ACL MAC capa 2 especificando el nombre de la lista. Después de entrar este comando, el modo cambia a la configuración de ACL MAC extendida.
Paso 3	{**deny | permit**} {**any | host** *source MAC address*} {**any | host** *destination MAC address*}	Entra **deny** o **permit** para especificar si niegas o permites el acceso si las condiciones son aprobadas. Para *MAC-addr,* entra la dirección MAC del **host** del cual el paquete será enviado. Especifica esto usando el formato hexadecimal. Para *dst-MAC-addr*, entra la dirección MAC del **host** del cual el paquete será enviado. Especifica esto usando el formato hexadecimal.
Paso 4	**End**	Regresa al modo EXEC privilegiado.
Paso 5	**Show access-list** [*number / name*]	Verifica las entradas.
Paso 6	**Copy running – config startup-config**	(Opcional) guarda las entradas en un archivo de configuración.

Para borrar una ACL, usa el comando de configuración global **no mac access-list extended** *access-list-name.*

6.5.2 Clasificando tráfico usando asociación de clases

Usa el comando de configuración global **class-map** para aislar un específico flujo de tráfico (o clase) de todo el otro tráfico y llamarlo. Las declaraciones de correspondencia pueden incluir criterios como una ACL, valores de prioridad IP o valores DSCP. El criterio de correspondencia es definido con una declaración de correspondencia entrada dentro del modo de configuración **class-map.**

Se comienza en el modo EXEC privilegiado y se siguen los pasos indicados en la tabla 10 para crear una asociación de clases y definir el criterio de correspondencia para clasificar el tráfico.

Tabla 10. Pasos para crear una asociación de clases y definir el criterio de correspondencia para clasificar el tráfico

	comando	Propósito
Paso 1	**configure terminal**	Entra al modo de configuración global.
Paso 2	**access-list** *access-list-number* {**deny** | **permit**} {*source source-wildcard* | **hos**t source | **any**} o **access-list** *access-list-number* {**deny** | **permit | remark**} *protocol* *{source source-wildcard* | **host**	Crea una ACL IP estándar o extendida para tráfico IP o una ACL MAC capa 2 para tráfico no IP, repitiendo el comando las veces que sea necesario. Nota: Las declaraciones de negación no están soportadas por las ACL´s de QoS.

	source | **any**} [*operator port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*] o **mac access-list extended** *name* {**deny** | **permit**} {**any** | **host** *source MAC address*} {**an**y | **host** *destination MAC address*}	
Paso 3	**Class-map** *class-map-name*	Crea una asociación de clase y entra al modo de configuración class- map Por defecto, las asociaciones de clases no están definidas. Para *class-map-name*, especificar el nombre de la asociación de clase.
Paso 4	**match** {**access-group** *acl-index* | **name** *acl-name*}	Define el criterio de correspondencia para clasificar el tráfico. Por defecto, el criterio de correspondencia no está configurado. Solo un criterio de correspondencia y una ACL por asociación de clase son soportados. Para **access-group** *acl-index* | *name acl-name*, especificar el número o nombre de la ACL creada en el paso 3.
Paso 5	**End**	Regresa al modo EXEC privilegiado.
Paso 6	**Show class-map** [*class-map-*	Verifica las entradas.

	name]	
Paso 7	**Copy running-config startup-config**	(Opcional) guarda las entradas en un archivo de configuración.

Para borrar una asociación de clase existente, usa el comando de configuración global **no class-map** *class-map-name*. Para remover un criterio de correspondencia usa el comando de configuración de asociación de clases **no match** {**acl-index** | **name** *acl-name*}.

6.5.3 Clasificando, vigilando y señalando el tráfico usando asociación de políticas. Una asociación de política especifica sobre cuál clase de tráfico actuar. Las acciones pueden incluir activar los valores Cos o DSCP en la clase de tráfico, ajustar un valor DSCP específico en la clase de tráfico, especificar las limitaciones de ancho de banda para cada clase de tráfico correspondido y las acciones a tomar cuando el tráfico esté fuera del perfil (señalización).

Una asociación de políticas también tiene estas características:

- Una asociación de políticas puede contener múltiples declaraciones de clases, cada una con diferente criterio de correspondencia y vigilancia.

- Puede existir una asociación de política separada por cada tipo de tráfico recibido a través de una interface.

Puedes adjuntar solo una clase de política por interface en la dirección de entrada.

Se comienza en el modo EXEC privilegiado y se siguen los pasos indicados en la tabla 11 para crear una asociación de política:

Tabla 11. Pasos para crear una asociación de política.

	Comando	Propósito
Paso 1	**configure terminal**	Entra al modo de configuración global.
Paso 2	**access-list** *access-list-number* {**deny | permit**} {*source source-wildcard* | **host** *source* | **any**} o **access-list** *access-list-number* {**deny** | **permit** | **remark**} *protocol* *{source source-wildcard* | **host** *source* | **any}*[**operator port**] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*] o **mac access-list extended**	Crea una ACL IP estándar o extendida para tráfico IP o una ACL MAC capa 2 para tráfico no IP, repitiendo el comando las veces que sea necesario. Nota: Las declaraciones de negación no están soportadas por las ACL´s de QoS

	name (**deny | permit**} {**any** | **host** *source MAC address*} {**an**y | **host** *destination MAC address*}	
Paso 3	**policy-map** *policy-map-name*	Crea una asociación de política entrando el nombre y al modo de configuración policy –map. Por defecto, las asociaciones de políticas no están definidas. El comportamiento por defecto de una asociación de política es ajustar el DSCP a 0 si el paquete es IP y ajustar el CoS a 0 si está etiquetado. La vigilancia no es llevada a cabo.
Paso 4	**class** *class-map-name* [**access-group** *acl-index-or-name*]	Define una clasificación de tráfico y entra al modo de configuración policy-map class. Por defecto las clases de asociación de políticas no están definidas. Si una clase de tráfico ha sido definida usando el comando de configuración global **class-map,** especifica su nombre por *class-map-name*. En **access-group** *acl-index-or-name*, especificar el número o nombre de la ACL creada en el paso 2. Nota: en una asociación de política, el nombre de la clase *class-default* no está soportada. El **switch** no filtra tráfico basado en la asociación de política definida por el comando de

		configuración **class class-default.**
Paso 5	**set** {**ip dscp** *new-dscp*}	Clasifica tráfico IP ajustando un Nuevo valor en el paquete. Por **ip dscp** *new-dscp*, entrar un Nuevo valor DSCP a ser asignado al tráfico clasificado. Los valores DSCP soportados son 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48 y 56.
Paso 6	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **dscp** *dscp-value*}]	Define un vigilante para el tráfico clasificado. Puedes configurar hasta 60 vigilantes en puertos GigabitEthernet y hasta 10 vigilantes en puertos 10/100 ethernet. En *rate-bps*, especificar la tasa promedio de tráfico en bits por segundo (bps). El rango es de 1 a 100 Mbps para puertos 10/100 Ethernet y de 8 a 1000 Mbps para los GigabitEthernet. En *burst-byte*, especificar en bytes el tamaño normal de ráfaga. Los valores soportados son 4096, 8192, 16384, 32768 y 65536 para puertos 10/100 y 4096, 8192, 16348, 32768, 65536, 131072, 262144 y524288 para los GigabitEthernet. (Opcional) especificar la acción a tomar cuando la tasa es excedida. Use el parámetro **exceed-action drop** para descartar el paquete. Use el parámetro **exceed-action dscp** *dscp-value* para señalar el valor DSCP y transmitir el paquete.

Paso 7	**exit**	Regresa al modo de configuración policy-map.
Paso 8	**exit**	Regresa al modo de configuración global.
Paso 9	i**nterface** *interface-id*	Entre al modo de configuración de interface y especifique la interface a adjuntar a la asociación de política.
Paso 10	**service-policy** {**input** policy-map-name}	Aplicar una asociación de política a la entrada de una interface en particular. Solo una asociación de política por interface es soportada. Use **input** *policy-map-name* para aplicar la asociación de política específica a la entrada de una interface.
Paso 11	**end**	Regresa al modo EXEC privilegiado.
Paso 12	**show policy-map** [*policy-map-name* **class** *class-name*]	Verifica las entradas.
Paso 13	**copy running-config startup-config**	(Opcional) guarda las entradas en un archivo de configuración.

Para borrar una asociación de política existente, se usa el comando de configuración global **no policy-*map*** policy-map-name. Para remover un valor DSCP asignado, use el comando de configuración de asociación de política **no** set {**ip dscp** *new-dscp*}, para remover un vigilante existente, use el comando de

configuración de asociación de política **no police** *rate-bps burst-byte* [**exceed-action** {**drop | dscp** *dscp-value*}]

6.6 CONFIGURANDO CORRESPONDENCIAS DE QOS

Nota: esta característica está disponible solo si tu **switch** está ejecutando el **software** mejorado.

6.6.1 Configurando la correspondencia de CoS a DSCP

Use la correspondencia CoS a DSCP para asociar los valores CoS en los paquetes entrantes a un valor DSCP que QoS usa internamente para representar la prioridad del tráfico.

La tabla 12 muestra la correspondencia CoS a DSCP por defecto.

Tabla 12. Correspondencia CoS – DSCP Por Defecto

Valor CoS	0	1	2	3	4	5	6	7
Valor DSCP	0	8	16	24	32	40	48	56

Si estos valores no son apropiados para tu red, necesitas modificarlos.

Se comienza en el modo EXEC privilegiado y se siguen los pasos indicados en la tabla 13 para modificar las correspondencias CoS a DSCP.

Tabla 13. Pasos para modificar las correspondencias CoS a DSCP.

	Comando	Propósito
Paso 1	**configure terminal**	Entra al modo de configuración global.
Paso 2	**mls qos map cos-dscp** dscp1...dscp8	Modifique las correspondencias CoS a DSCP. Para dscp1...dscp8, entre 8 valores DSCP que correspondan a valores CoS de 0 a 7. Separe cada valor DSCP con un espacio. Los valores DSCP soportados son 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48 y 56.
Paso 3	**end**	Regresa al modo EXEC privilegiado.
Paso 4	**show mls qos maps cos-dscp**	Verifica las entradas.
Paso 5	**copy running-config startup-config**	(Opcional) guarda las entradas en un archivo de configuración.

Para regresar a las correspondencias por defecto, use el comando de configuración global **no mls qos map cos-dscp**.

6.6.2 Configurando la correspondencia de DSCP a CoS

Use la correspondencia DSCP a CoS para asociar los valores DSCP en los paquetes entrantes a un valor CoS, el cual es usado para seleccionar una de las cuatro colas de salida.

El **switch** Cisco Catalyst 2950 soporta estos valores DSCP 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48 y 56.

La tabla 14 muestra la correspondencia DSCP a CoS por defecto.

Tabla 14. Correspondencia DSCP-CoS Por Defecto.

Valores DSCP	0	8, 10	16, 18	24, 26	32, 34	40, 46	48	56
Valores CoS	0	1	2	3	4	5	6	7

Si estos valores no son apropiados para tu red, necesitas modificarlos.

Se comienza en el modo EXEC privilegiado y se siguen los pasos indicados en la tabla 15 para modificar las correspondencias DSCP a CoS.

Tabla 15. Pasos para modificar las correspondencias DSCP a CoS.

	Comando	Propósito
Paso 1	**configure terminal**	Entra al modo de configuración global.
Paso 2	**mls qos map dscp-cos** *dscp-list* **to** *cos*	Modifique las correspondencias DSCP a CoS. En dscp-list, entrar hasta 13 valores DSCP separados por espacios. Entonces entra el parámetro **to**. En cos, entrar el valor CoS que corresponderá con el valor DSCP. Para dscp1...dscp8, entre 8 valores DSCP que correspondan a valores CoS de 0 a 7. Separe cada valor DSCP con un espacio. Los valores DSCP soportados son 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48 y 56. El rango CoS es de 0 a 7.
Paso 3	**end**	Regresa al modo EXEC privilegiado.
Paso 4	**show mls qos maps dscp-to-cos**	Verifica las entradas.
Paso 5	**copy running-config startup-config**	(Opcional) guarda las entradas en un archivo de configuración.

6.7 MOSTRANO INFORMACIÓN QOS

Para mostrar la actual información de QoS, use uno o más de los comandos mostrados en la tabla 16, en el modo EXEC privilegiado.

Tabla 16. Comandos Para Mostrar Información QoS.

Comando	Propósito
show class-map [*class-map-name*]	Muestra las asociaciones de clases QoS, las cuales definen el criterio de correspondencia para clasificar el tráfico.
show policy-map [*policy-map-name* [**class** *class-name*]]	Muestra las asociaciones de políticas de QoS, las cuales definen el criterio de clasificación para el tráfico entrante.
show mls qos maps [cos-dscp | dscp-cos]	Muestra información de asociación QoS. Las asociaciones son usadas para generar un valor DSCP interno, el cual representa la prioridad del tráfico.
show mls qos interface [*interface-id*] [**policers**]	Muestra información de QoS en el nivel de la interface, incluyendo la configuración de las colas de salida.
show mls masks [qos | security]	Muestra detalles referente a las máscaras usadas por QoS y las ACL's de seguridad.
show wrr-queue cos-map	Muestra la asociación de prioridad QoS con colas.

7. CONCLUSIONES

Al finalizar nuestra monografía pudimos darnos cuenta, que al realizar un análisis de un tema tan complejo y sobre todo tan actual como lo es la Calidad de Servicio se debe hacer una investigación exhaustiva sobre este tema, en la que se recopile toda la información necesaria para poder llevarla a cabo; pero a la vez siendo muy selecto a la hora de escoger dicha información, debido a que este tema, como ya se comentó al principio, engloba muchísima documentación.

Luego de seleccionar la información que se utilizó para la realización de nuestro proyecto, se hizo en primera instancia una breve historia, en la que se resaltan acontecimientos importantes que fueron la base para que se empezara a analizar la calidad de servicio en las redes existentes; seguidamente se da una definición del término QoS y se exponen todos aquellos parámetros que se relacionan con este término, sus ventajas y clasificación, lo que nos permitió entender su significado de una forma global. Entre las ventajas podemos mencionar, las utilidades que proporcionan QoS para la entrega de datos críticos de cualquier empresa en periodos establecidos y con unas garantías determinadas, los beneficios que le ofrecen a las empresas brindándoles un servicio de red con mayor calidad y confiabilidad, y asegurando la puntualidad en la entrega de la

información transitada en la red, y también le permitirán a los proveedores de servicio brindar mayores prestaciones, para un mejor manejo y gestión de la red.

Evidentemente, para determinadas aplicaciones de calidad de servicio en las redes, los bajos valores de retardo y de variabilidad en él mismo (**jitter**) asegurarán un tiempo adecuado de llegada de los paquetes al usuario final, buscando de esta forma el aumento de la productividad del negocio, pero en el caso de que estos valores sean muy altos será imposible obtener un correcto nivel de calidad para estas aplicaciones. También se debe tener presente que por la red van a transitar simultáneamente distintos tipos de tráfico, que deben llegar a su destino para su adecuada utilización; para ello se necesitarán todos los recursos que posee la red, esto hace que se le de un mayor uso de la capacidad de los sistemas que podría terminar agotándose. Toda esta clase de inconvenientes se pueden evitar; en algunos casos se amplía esta capacidad, aumentando el ancho de banda, lo cual podría ser sumamente costoso, en otros casos, la tecnología de red no lo permite; para este caso se utilizan herramientas y protocolos de calidad de servicio como la correcta gestión del ancho de banda y de los recursos de la red, dar prioridad a distintos tipos de tráfico, la señalización para la transmisión de información de clases de servicio, etc.; los cuales originarían algunas políticas que se deben seguir en la aplicación de QoS , ya sea QoS extremo a extremo, punto a punto o de arriba hacia abajo para nuestro sistema.

Estas políticas están basadas en el Acuerdo de Nivel de Servicio (SLA) contratado entre un proveedor de servicios y un cliente. En el mismo se van a definir los valores de rendimiento, tasa de pérdidas, retrasos y variaciones en el intercambio de datos, en consecuencia, qué nivel de calidad de servicio va a proporcionar el proveedor al cliente, así como las consecuencias cuando éste no se consigue y el precio de todos estos servicios.

ATM es una tecnología que soporta con altos niveles de garantía la tendencia actual de generación de tráfico multimedia, lo cual le brinda a esta tecnología una gran ventaja con respecto al resto de tecnologías.

ATM puede proveer a los usuarios con una Calidad de Servicio (QoS) garantizada, dando a conocer a sus usuarios de la clase de tráfico esperada que será transmitido en la conexión y del tipo de calidad de servicio que la conexión requiere, para esto se utilizan descriptores del tráfico y categorías de servicio. Además ATM proporciona mecanismos de control que permiten gestionar su funcionamiento para la obtención de calidad de servicio. Pero se debe tener presente que su principal desventaja es precisamente su elevado coste.

La tecnología Frame Relay no está diseñada especialmente para soportar tráfico multimedia, audio y video en tiempo real, no posee garantías sobre el retardo de

tránsito, pero las redes que aplican esta clase de tecnología suelen estar bien dimensionadas y presenta un mínimo retardo de tránsito que no varía notablemente. En la aplicabilidad de QoS en esta tecnología, al cliente se le garantiza los servicios que le brindará la red, siempre por contrato, de esta forma el cliente puede contratar un nivel de calidad de servicio diferente para cada conexión, esta característica la hace ser una posibilidad tan buena como la ATM y mucho más económica.

Mediante la asignación de valores para el ancho de banda medio garantizado, el intervalo de observación y el ancho de banda físico de la línea de acceso, será posible controlar que los usuarios solo transmitan el volumen de información comprometida y en exceso, esto no dejará perder datos que no superen el tráfico comprometido. Por otro lado se pueden marcar las tramas para así mostrar la importancia de unas respecto a otras, a través de la activación del bit existente en la trama Frame Relay.

Todas estas características, así como su elevado rendimiento y velocidad hacen que Frame Relay sea otra tecnología de red a implementar para poder obtener unos niveles apropiados de calidad de servicio.

El ESTANDAR 802.1P va a permitir diferenciar entre 8 tipos de clases de tráfico clasificados como prioridades de usuario (**user_priority**) por cada puerto del **switch**, siendo el rango de valores de prioridad de usuario del 0 al 7. Para conseguirlo se necesitan 3 bits, en los que será necesarios aumentar el formato básico de las tecnologías de 802, tal y como Ethernet. Una vez determinadas las clases de tráfico por **switch**, será necesario mapearlas (asociarlas) con el tipo de tráfico que circule por la red para asegurar que el tráfico en tiempo real sea atendido antes que otro tipo de tráfico considerado menos importante.

BIBLIOGRAFÍA

- http://www.windowstimag.com/atrasados/1999/28_feb99/articulos/qos.htm
- http://www.merca.net.co/s_07.html
- http://www.cisco.com/en/US/tech/tk543/tk766/tech_protocol_family_home.html
- http://www.cisco.com/en/US/tech/tk543/tk545/tech_protocol_family_home.html
- http://www.cisco.com/en/US/tech/tk543/tk762/tech_protocol_family_home.html
- http://atenea.udistrital.edu.co/estudiantes/lmartin/Doc/qos.htm
- http://www.aui.es/biblio/bolet/bole025/art_4.htm#Introduccion
- http://www.it.uc3m.es/~prometeo/rsc/apuntes/index.html
- http://www.angelfire.com/sc/itiuax/indice.html
- http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a008007e8de.html
- http://www.miguellencinas.com.ar/indexES.html
- http://www.unitec.edu.co/biblioteca/atm/1atm.html
- http://osmecon.net/cursos/redes4.html