UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

CALIDAD DE SERVICIO EN REDES MULTISERVICIOS

T E S I S

PARA OBTENER EL TÍTULO DE :

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A N :
JUAN ANTONIO CRUZ LÓPEZ
CÉSAR RAFAEL HERNÁNDEZ RAMÍREZ
D I R E C T O R D E T E S I S
ING. ADALBERTO GARCÍA ESPINOSA
CIUDAD UNIVERSITARIA MAYO 2005

Agradecimientos

A mis padres por la educación que me brindaron, por sus consejos, por su apoyo incondicional y por mostrarme el buen camino con su ejemplo. A mis hermanos por crecer junto conmigo y ayudarme en todo momento.
A la UNAM y a la Facultad de Ingeniería por darnos la oportunidad de estudiar en tan prestigiosa institución. A los profesores de la Facultad de Ingeniería por sus clases de excelente calidad, las cuales me dieron grandes lecciones no solo de ingeniería sino también de vida.
A la RCDT, por facilitarnos el uso de sus laboratorios de pruebas, sin el cual no hubiera sido posible la realización de ésta tesis.
Al Ingeniero Adalberto García Espinosa, por haber dirigido esta tesis, y al Ingeniero Rodolfo Arias Villavicencio por su ayuda durante el desarrollo del mismo.
A César Hernández Ramírez, por su gran amistad. Por todo su apoyo durante estos años en la Facultad, y durante el desarrollo de nuestra tesis. A mis amigos de la FI, por esos ratos de esparcimiento.
Juan Antonio Cruz López
A Dios y a la Virgen de Santa Lucia, por brindarme fortaleza y por iluminarme en los momentos de oscuridad.
A mis padres por ese apoyo tan grande que he recibido durante todo este tiempo, por enseñarme a no descuidar nunca mis obligaciones. A mis hermanos por apoyarme cuando más los he necesitado.
A la Facultad de Ingeniería, a la UNAM y a sus profesores, por brindarme esta oportunidad única de hacer mis estudios en esta gran Institución. Me han dado grandes satisfacciones como también grandes lecciones que nunca olvidaré.
A la RCDT, al Ingeniero Adalberto García Espinosa, por haber dirigido este trabajo y al Ingeniero Rodolfo Arias Villavicencio por su gran ayuda.
A Juan Antonio Cruz López, fue para mi una gran experiencia el que hayamos podido realizar este trabajo, así como lo hemos hecho durante todas las asignaturas que hemos compartido, aprendimos a trabajar en equipo alo largo de estos años. A mis compañeros que me han dejado gratos recuerdos que nunca olvidaré.
Gracias a todos.
César Rafael Hernández Ramírez

Índice

1 Introducción

La actual demanda de aplicaciones relacionadas con información multimedia, como son la video-conferencia, audio-conferencia, video bajo demanda (VoD), voz sobre IP (VoIP) o sistemas cooperativos (pizarras compartidas, teletrabajo, telemedicina, etc.) y su coexistencia con aplicaciones más clásicas (bases de datos, transferencias de ficheros, WWW, etc.), requieren tecnologías de comunicaciones capaces de ofrecer elevadas prestaciones.

En la actualidad se están implantando nuevas tecnologías de fibra óptica que proporcionan el gran ancho de banda requerido por las aplicaciones anteriores, pero no basta solo con el aumento del mismo, es necesario gestionarlo de manera eficiente: utilizarlo en un porcentaje elevado asegurando una calidad determinada. Esto es lo que se conoce como calidad de servicio (QoS).

La calidad de servicio (QoS) puede definirse como el rendimiento de los servicios observados por el usuario final. Una red debe garantizar que puede ofrecer un cierto nivel de calidad de servicio para un nivel de tráfico que sigue un conjunto especificado de parámetros.

El objetivo de esta tesis es describir la necesidad por Calidad de Servicio (QoS) en redes multiservicios (voz, datos y vídeo) analizando y comparando los diferentes mecanismos para otorgarla; proporcionar lineamientos de diseño y aplicarlos a una red verdadera en producción que opera bajo los protocolos básicos.

Definición del problema

En la actualidad la mayoría de las empresas mantienen infraestructuras separadas para sus servicios de voz, datos y vídeo, lo que resulta en incrementos en sus costos de operación que repercuten directamente en la productividad y competitividad de las mismas. En el mundo existe una tendencia por unificar estos servicios dentro de una red multiservicios, que sea capaz de soportar tráfico de voz, datos y vídeo. La naturaleza diferente de cada tipo de tráfico hace que los requerimientos de red de cada uno de ellos sean diferentes, siendo un reto para los diseñadores y administradores de red el satisfacer los requerimientos, y el hacer un uso de eficiente de los recursos limitados.

Esta tesis pretende lograr través de la comparación y el análisis de los mecanismos y tecnologías existentes para otorgar QoS en redes multiservicios, una propuesta de diseño e implementación para una red en producción basándose en los requerimientos y servicios de la misma; permitiendo a esta red la integración de aplicaciones de datos tradicionales y aplicaciones multimedia que no sólo le ayuden a un incremento en productividad y competitividad, sino además un incremento en los servicios que brinda y en su confiabilidad.

Esta tesis esta basada en una red en producción, pero por motivos de privacidad, no se puede mencionar el nombre ni la compañía a la cual pertenece. Aquí se menciona como RC-JC.

Cabe mencionar que nuestro desarrollo sólo se hace para la parte WAN de la red y no se toca en ningún momento la parte LAN.

Método

El método principal para el desarrollo de la tesis se basa principalmente en la investigación de las tecnologías y mecanismos disponibles, para después analizarlos, compararlos y escoger los que mejor resuelvan la problemática de la red en cuestión. Para después aplicarlos en dicha red.

Este análisis se concentrará en los mecanismos y tecnologías en las capas 2 y 3 del modelo de referencia OSI (capas de enlace de datos y de red), haciendo énfasis en aquellos que involucren el protocolo IP.

Resultados Esperados

Al finalizar la implementación de la propuesta la red analizada deberá de soportar tráfico de voz, datos y vídeo garantizando el nivel de servicio otorgado a cada uno de ellos.

La composición del trabajo está dividido en 8 capítulos.

En el capítulo 2 se da una descripción de algunas tecnologías referentes a las capas 2 y 3 del modelo de referencia OSI. Se da una visión general de las Redes de Datos Tradicionales y Redes Multiservicios, así como las problemáticas que enfrenta cada una. Además se define el concepto de Calidad de Servicio (QoS).

En el capítulo 3 se describe la Calidad de Servicio en Redes LAN, WAN y redes IP, se muestra una descripción de algunos parámetros importantes en estas tecnologías para poder brindar QoS.

En el capítulo 4 se describen los mecanismos que se necesitan para poder brindar Calidad de Servicio (QoS) en una red.

En el capítulo 5 se describen los requerimientos y las características que tiene la red ala cual se le van a aplicar los mecanismos de Calidad de Servicio (QoS).

En el capítulo 6 se describe la propuesta que se va a utilizar, cuales mecanismos se van a utilizar de acuerdo a las especificaciones que debe de cumplir la red.

En el capítulo 7 se describen las pruebas que se hicieron en base a la propuesta de diseño, implementando una maqueta que cumple con el modelo jerárquico de la red estudiada, así como la configuración de cada uno de los routers que se hizo en la fase de implementación.

En el capítulo 8 y 9 se describen los resultados obtenidos durante la implementación y finalmente las conclusiones de este trabajo.

2 Marco Teórico

2.1 Redes de Datos Tradicionales

2.1.1 Redes LAN Ethernet

Ethernet es la tecnología de red LAN más usada, resultando idóneas para aquellos casos en los que se necesita una red local que deba transportar tráfico esporádico y ocasionalmente pesado a velocidades muy elevadas. Las redes Ethernet se implementan con una topología física de estrella y lógica de bus, y se caracterizan por su alto rendimiento a velocidades de 10-100 Mbps.

El origen de las redes Ethernet hay que buscarlo en la Universidad de Hawai, donde se desarrollo, en los años setenta, el Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones, CSMA/CD (Carrier Sense and Multiple Access with Collition Detection), utilizado actualmente por Ethernet. Este método surgió ante la necesidad de implementar en las islas Hawai un sistema de comunicaciones basado en la transmisión de datos por radio, que se llamó Aloha, y permite que todos los dispositivos puedan acceder al mismo medio, aunque sólo puede existir un único emisor en cada instante. Con ello todos los sistemas pueden actuar como receptores de forma simultánea, pero la información debe ser transmitida por turnos.

Las redes Ethernet son de carácter no determinista, en la que los hosts pueden transmitir datos en cualquier momento. Cuando un dispositivo tiene información que transmitir:

1. Verifica que el medio de transmisión esté libre. En este momento no existe señal alguna sobre el medio de transmisión.
2. Transmite su información.
3. Si el medio está ocupado, espera hasta que este esté libre.
4. Si ocurre que dos dispositivos comienzan a transmitir al mismo tiempo, se produce una colisión, la cual es detectada por los dispositivos como una variación inusual de voltaje. Detectada la colisión, se interrumpe inmediatamente la transmisión de la trama, y se transmite una señal de “jam” (32 bits, comúnmente sólo unos) y se espera un tiempo aleatorio para volver a intentar acceder al medio.

Una colisión se produce pues cuando dos máquinas escuchan para saber si hay tráfico de red, no lo detectan y, acto seguido transmiten de forma simultánea. En este caso, ambas transmisiones se dañan y las estaciones deben volver a transmitir más tarde. Existen dos tipos de colisiones:

- La colisión *temprana* es la que ocurre normalmente en una red ethernet bien dimensionada y consiste en cualquier colisión que ocurre antes de haber transmitido 512 bits en el medio, lo cual permite que los dispositivos involucrados en la colisión detecten la misma y puedan retransmitir la información en proceso de transmisión.

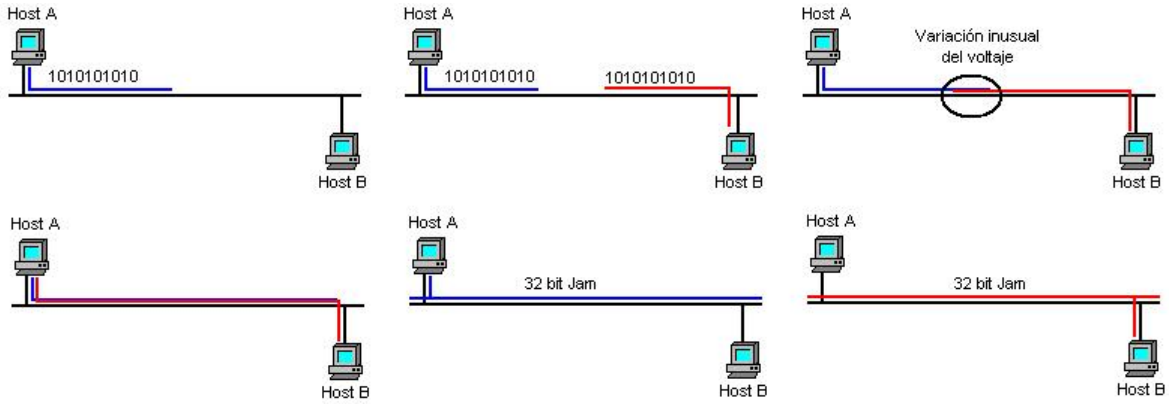

Fig. 2.1. Secuencia de una colisión temprana.

- La colisión *tardía* consiste en cualquier colisión que ocurre después de haberse transmitido 512 bits en el medio, lo cual no permite que todos los dispositivos involucrados en una colisión se enteren que su información recién transmitida fue dañada y por lo tanto se requiere su retransmisión.

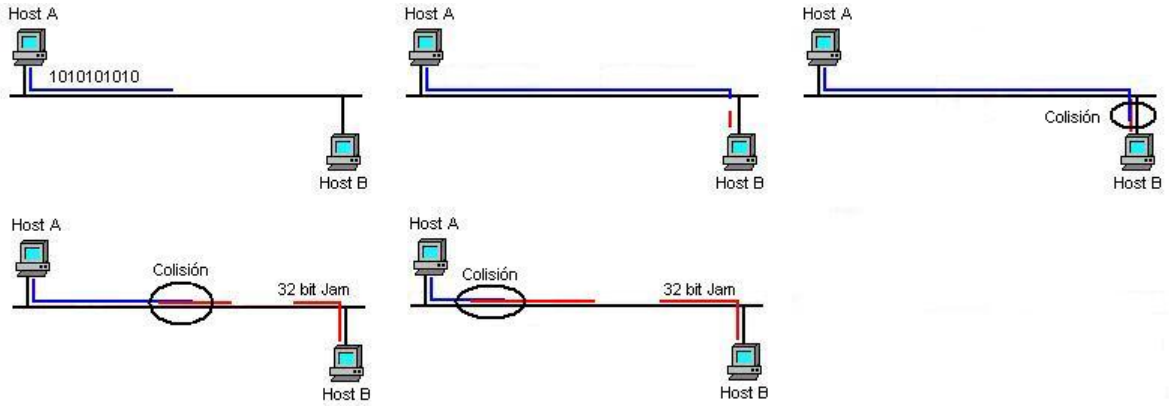

Fig. 2.2. Secuencia de una colisión tardía.

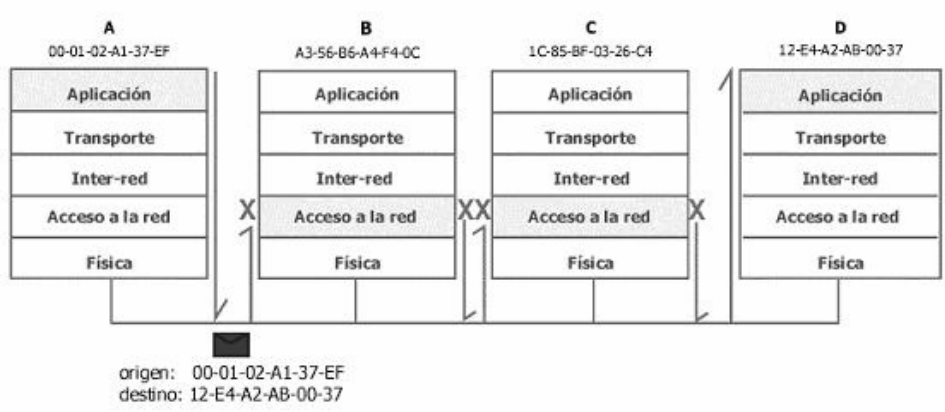

Fig. 2.3. Transmisión broadcast en redes Ethernet.

Existen dos especificaciones diferentes para un mismo tipo de red, Ethernet e IEEE 802.3. Ambas son redes de broadcast, lo que significa que cada máquina puede ver todas las tramas, aunque no sea el destino final de las mismas. Cada máquina examina cada trama que circula por la red para determinar si está destinada a ella. De ser así, la trama pasa a las capas superiores para su adecuado procesamiento. En caso contrario, la trama es ignorada.

Ethernet proporciona servicios correspondientes a las capas físicas y de enlace de datos del modelo de referencia OSI, mientras que IEEE 802.3 especifica la capa física y la porción de acceso al canal de la capa de enlace de datos, pero no define ningún protocolo de Control de Enlace Lógico.

Ethernet es una tecnología de broadcast de medios compartidos. El método de acceso CSMA/CD que se usa en Ethernet ejecuta tres funciones:

1. Transmitir y recibir paquetes de datos.
2. Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI.
3. Detectar errores dentro de los paquetes de datos o en la red.

Tanto Ethernet como IEEE 802.3 se implementan a través de la tarjeta de red o por medio de circuitos en una placa dentro del host.

Formato de trama Ethernet

Existen 4 tipos de trama para Ethernet, siendo estos Ethernet versión 2, 802.3, Novell y SNAP. Todos ellos tienen una longitud mínima de 64 bytes y una máxima de 1518 bytes (sin contar el campo preámbulo).

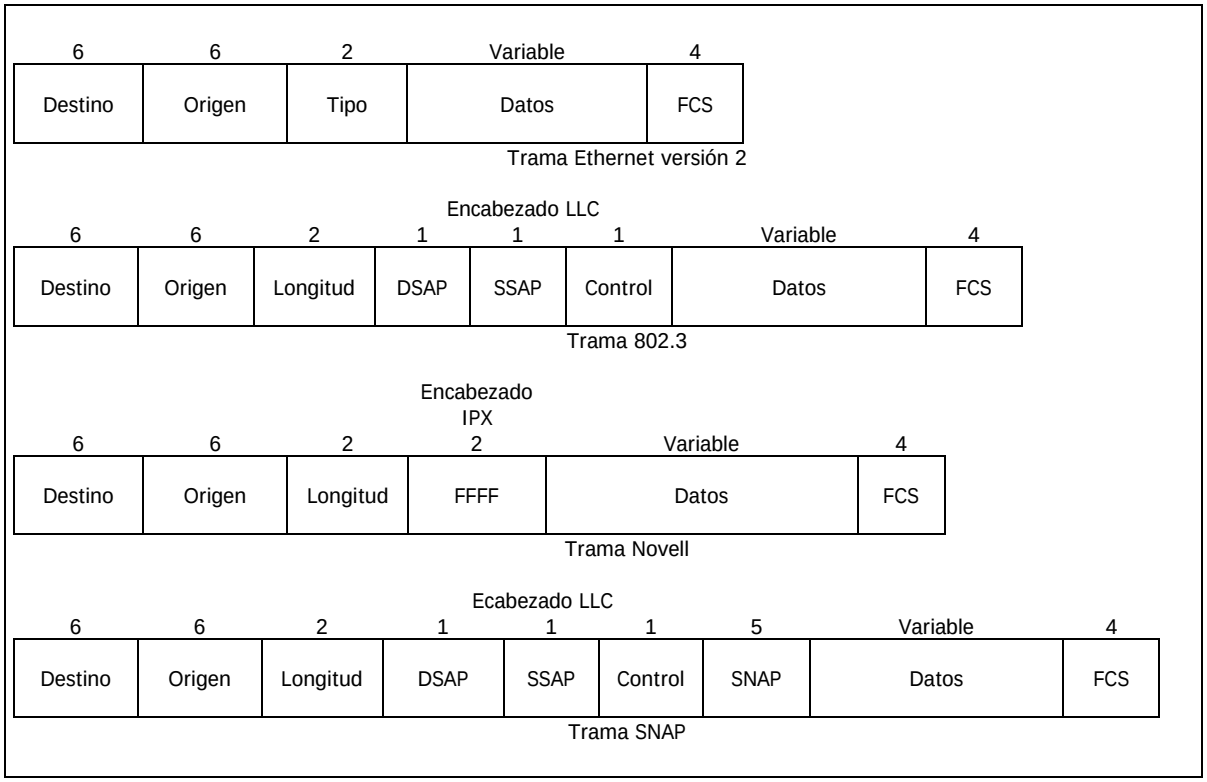

Fig. 2.4. Tipos de trama para Ethernet.

El contenido de los campos es el siguiente:

- *Preámbulo.* Secuencia de 64 bits consistentes en unos y ceros alternados con terminación en "11". La sincronía y el inicio del campo de dirección destino (MAC) se logran con este campo.
- *Origen y Destino.* Consisten en 6 bytes cada uno que contienen la dirección MAC origen y destino.
- *Tipo.* 2 bytes que identifican a qué protocolo de la capa superior va dirigida la información.
- *Longitud.* 2 bytes que proporcionan la longitud del campo Datos.
- *Encabezado LCC.* 3 bytes de Encabezado LCC o 802.2. DSAP y SSAP están puestos cada uno en AA hexadecimal, el byte de Control identifica el tipo de trama LCC y usualmente tiene el valor de 05 hexadecimal.
- *Encabezado IPX.* 2 bytes nunca usados y puestos en FFFF.
- *Datos.* De 44 a 1498 bytes. Contiene la información destinada a capas superiores.
- *FCS.* 4 bytes que contienen el código generado por un proceso polinomial sobre los campos Destino, Origen, Tipo y Datos. La máquina receptora genera este código cuando recibe la trama la compara con la recibida en él mismo. Si son iguales la información está correcta, si están diferentes, la información tiene errores y la trama es descartada.

Tipos de redes Ethernet

Existen por lo menos 18 variedades de Ethernet, relacionadas con el tipo de cableado empleado y con la velocidad de transmisión.

Tipo	Medio	Ancho de banda máximo	Longitud máxima de segmento	Topología Física	Topología Lógica
10Base5	Coaxial grueso	10 Mbps	500 m	Bus	Bus
10Base-T	UTP cat. 5	10 Mbps	100 m	Estrella; Estrella Extendida	Bus
10Base-FL	Fibra óptica multimodo	10 Mbps	2000 m	Estrella	Bus
100Base-TX	UTP cat. 5	100 Mbps	100 m	Estrella	Bus
100Base-FX	Fibra óptica multimodo	100 Mbps	2000 m	Estrella	Bus
1000Base-T	UTP cat. 5	1000 Mbps	100 m	Estrella	Bus

Tabla 2.1. Variedades de red Ethernet

Las tecnologías Ethernet más comunes y más importantes las son:

Ethernet 10Base2. Usa un cable coaxial delgado, por lo que se puede doblar más fácilmente, y además es más barato y fácil de instalar, aunque los segmentos de cable no pueden exceder de 200 metros y 30 nodos. Las conexiones se hacen mediante conectores en T, más fáciles de instalar y más seguros.

Ethernet 10Base5. También llamada Ethernet gruesa, usa un cable coaxial grueso, consiguiendo una velocidad de 10 Mbps. Puede tener hasta 100 nodos conectados, con una longitud de cable de hasta 500 metros. Las conexiones se hacen mediante la técnica denominada

derivaciones de vampiro, en las cuales se inserta un polo hasta la mitad del cable, realizándose la derivación en el interior de un transceiver, que contiene los elementos necesarios para la detección de portadores y choques. El transceiver se une al computador mediante un cable de hasta 50 metros.

Ethernet 10Base-T. Cada estación tiene una conexión con un hub central, y los cables usados son normalmente de par trenzado. Son las LAN más comunes hoy en día. Mediante este sistema se palian los conocidos defectos de las redes 10BAse2 y 10Base5, a saber, la mala detección de derivaciones no deseadas, de rupturas y de conectores flojos. Como desventaja, los cables tienen un límite de sólo 100 metros, y los hubs pueden resultar caros.

Ethernet 10Base-FX. Basada en el uso de fibra óptica para conectar las máquinas, lo que la hace cara para un planteamiento general de toda la red, pero idónea para la conexión entre edificios, ya que los segmentos pueden tener una longitud de hasta 2000 metros, al ser la fibra óptica insensible a los ruidos e interferencias típicos de los cables de cobre. Además, su velocidad de transmisión es mucho mayor.

Fast Ethernet. Las redes 100BaseFx (IEEE 802.3u) se crearon con la idea de paliar algunos de los fallos contemplados en las redes Ethernet 10Base-T y buscar una alternativa a las redes FDDI Son también conocidas como redes Fast Ethernet, y están basadas en una topología en estrella para fibra óptica. Con objeto de hacerla compatible con Ethernet 10Base-T, la tecnología Fast Ethernet preserva los formatos de los paquetes y las interfaces, pero aumenta la rapidez de transmisión hasta los 100 Mbps. En la redes Fast Ethernet se usan cables de cuatro pares trenzados de la clase 3, uno de los cuales va siempre al hub central, otro viene siempre desde el hub, mientras que los otros dos pares son conmutables. En cuanto a la codificación de las señales, se sustituye la codificación Manchester por señalización ternaria, mediante la cual se pueden transmitir 4 bits a la vez. También se puede implementar Fast Ethernet con cableado de la clase 5 en topología de estrella (100BaseTX), pudiendo entonces soportar hasta 100 Mbps con transmisión full dúplex.

2.1.2 Protocolo IP

Internet es un conjunto de redes diferentes que comparten una pila de protocolos comunes. Cada una de estas redes es administrada por una entidad diferente: universidades, redes académicas nacionales, ISPs (Internet Service Providers), operadores, empresas multinacionales, etc. Como consecuencia, de esto las políticas de uso son muy variadas.

Técnicamente a nivel de red Internet puede definirse como un conjunto de redes o sistemas autónomos conectados entre sí que utilizan el protocolo de red IP. IP es una red de datagramas, no orientada a conexión, con servicio “best effort”, es decir, no ofrece QoS. La entrega de los paquetes no está garantizada ya que en momentos de congestión éstos pueden ser descartados sin previo aviso por los enrutadores que se encuentren en el trayecto.

En una red IP toda la información viaja en unidades de información denominadas paquetes IP. Es decir, tanto la información de control que tenga que intercambiarse (enrutamiento dinámico, mensajes de error, etc.) como los datos de nivel superior, viajan de la misma forma, usando un servicio no orientado a la conexión.

Encabezado IP

El paquete IP tiene dos partes: encabezado y datos del nivel superior. El encabezado tiene una parte fija de 20 bytes y una opcional que va entre 0 y 40 bytes, pero siempre es un múltiplo de 4. Los campos son los siguientes:

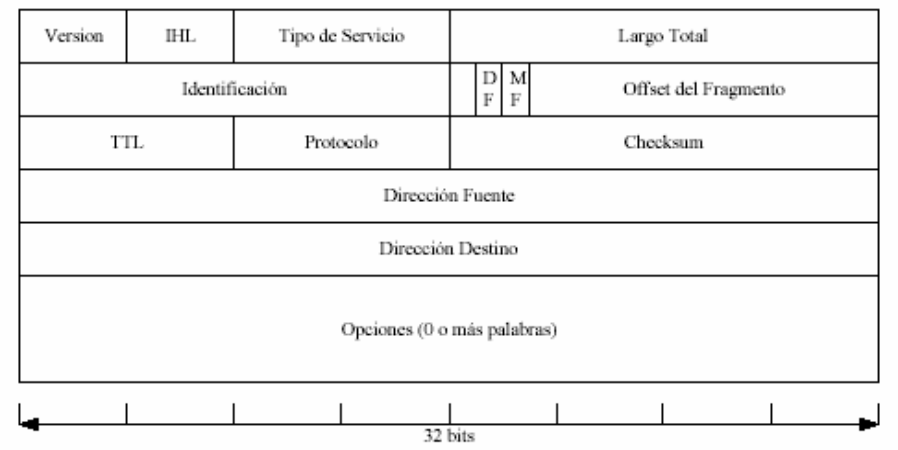

Fig. 2.5. Encabezado del Paquete IP.

- *Versión.* (4 bits) Indica la versión usada de IP. La versión actual es la 4, pero desde hace algún tiempo se empezó ya a extender el uso de la versión 6 con una estructura de paquete diferente al de la 4.
- *IHL.* (4 bits) Especifica la longitud del encabezado, ya que este puede variar por la presencia de campos opcionales. Se codifica en palabras de 32 bits (4 Bytes), donde la longitud mínima es 5 y la máxima 15.
- *Tipo de Servicio.* (1 Byte) Permite establecer que calidad de servicio requiere el paquete. Se pueden establecer varios tipos de confiabilidad y velocidad (por ejemplo, rapidez en vez de confiabilidad para aplicaciones como audio o video, confiabilidad para transferencia de archivos, etc.). Este campo tiene subcampos de importancia: *P* (precedencia) son 3 bits de prioridad, un Flag tres bits D, T y R que permite especificar que importa mas Retardo, Throughput o Confiabilidad. Recientemente, el campo Differentiated Services ha sustituido a este campo. Su finalidad es implementar QoS en redes IP mediante la arquitectura denominada Servicios Diferenciados o Diffserv.
- *Largo Total.* (2 Bytes) Especifican la longitud del paquete completo, encabezado incluido, en bytes.
- *Identificación.* (2 Bytes) Este campo permite al destino determinar a que paquete pertenece el fragmento que ha llegado a él. Está relacionado con la fragmentación de paquetes.
- *DF.* (1 bit) Indica no fragmentar el paquete.
- *MF.* (1 bit) indica que vienen más fragmentos. Todos los fragmentos que pertenecen a un mismo paquete, salvo el último, tienen este bit en 1.
- *Offset del Fragmento.* (13 bits) Indica a que parte, del paquete total, pertenece el fragmento que se está recibiendo.
- *TTL.* (1 Byte) Permite descartar un paquete una vez que ha dado un número excesivo de saltos o ha pasado un tiempo excesivo viajando por la red. Es un contador regresivo que indica el tiempo de vida restante del paquete, y su valor está medido en segundos, de forma al llegar a cero el paquete debe ser descartado. Esto permite evitar que se produzcan loops y un paquete pueda permanecer “flotando” indefinidamente en la red. Como no resulta simple calcular con precisión el tiempo que un paquete emplea en el tránsito entre dos enrutadores, en la práctica lo que se hace es restar el TTL en uno por cada salto, y en caso de que el paquete se encuentre durante más de un segundo esperando en un enrutador, se resta uno por cada

segundo de espera. Como los paquetes casi nunca están más de un segundo en un enrutador, en realidad, este parámetro funciona como un contador de saltos. En el caso de producirse fragmentación, el host receptor puede retener paquetes durante varios segundos, mientras espera a recibir todos los fragmentos. En este caso, el host restará uno del TTL por cada segundo de espera, pudiendo llegar a descartar paquetes por este motivo. Los valores de TTL típicos están entre 64 y 128.

- *Protocolo.* (1 Byte) Especifica a que protocolo de nivel de transporte corresponde el paquete. La tabla de protocolos válidos y sus correspondientes números son controlados por el IANA (Internet Assigned Number Authority), en la siguiente tabla se muestran algunos de los posibles valores de este campo. Llama la atención el valor 4 de la tabla que está reservado para el uso de IP para transportar IP, es decir, el hacer un túnel de un paquete IP dentro de otro. Esta técnica permite realizar ruteo desde el origen de los paquetes encapsulando el paquete en otro dirigido al nodo intermedio por el que se quiere pasar. Una técnica similar se sigue para hacer un tunneling de IP versión 6 en IP versión 4.

Valor	Protocolo	Descripción
0	Reservado	
1	ICMP	Internet Control Message Protocol
2	IGMP	Internet Group Management Protocol
3	GGP	Gateway-to-Gateway Protocol
4	IP	IP en IP (encapsulado)
5	ST	Stream
6	TCP	Transmission Control Protocol
8	EGP	Exterior Gateway Protocol
17	UDP	User Datagram Protocol
29	ISO-TP4	ISO Transport Protocol Clase 4
38	IDRP-CMTP	IDRP Control Message Transport Protocol
80	ISO-IP	ISO Internet Protocol (CLNP)
88	IGRP	Internet Gateway Routing Protocol (Cisco)
89	OSPF	Open Shortest Path First
255	Reservado	

Tabla 2.2. Algunos valores del campo Protocolo.

- *Checksum.* (2 Bytes) Sirve para detectar errores en el encabezado del paquete. El checksum permite evitar al paquete de una alteración en alguno de los campos del encabezado que pudiera producirse, por ejemplo, por un problema de hardware en un enrutador. El checksum sólo cubre el encabezado del paquete, no los datos. El campo checksum se ha de recalcular en cada salto, ya que al menos el TTL cambia. Notar que en enrutadores con alto tráfico, el volver a calcular del checksum supone un inconveniente desde el punto de vista de rendimiento.
- *Dirección Fuente.* (4 Bytes) Corresponden a la dirección IP origen.
- *Dirección Destino.* (4 Bytes) Corresponden a la dirección IP destino.
- *Opciones.* Campo de longitud variable que no siempre está soportado en los enrutadores y se utiliza muy raramente. Fue diseñado para permitir expansiones al protocolo, experimentos, etc. Las opciones son de tamaño variable, comenzando siempre por un byte de codificación, y siempre son rellenadas a múltiplos de 4 bytes. Entre las opciones se encuentran: *Record Route* que pide a cada enrutador por el que pasa el paquete que anote en el encabezado su dirección, obteniéndose un trazado de la ruta seguida (debido a la limitación a un máximo de 40 bytes en la parte opcional del encabezado, como máximo pueden registrarse 9 direcciones). *Timestamp* actúa de manera similar a record router, pero además de anotar la dirección IP de cada enrutador atravesado se anota en otro campo de 32 bits el instante en que el paquete pasa por dicho enrutador. El uso de dos campos de 32 bits aumenta el problema antes mencionado, del poco espacio disponible para grabar esta información. *Source Enrutamiento* permite al emisor especificar la ruta que debe seguir el paquete hasta llegar a su destino. Existen dos variantes:

strict source enrutamiento que especifica la ruta exacta salto a salto, de modo que si en algún caso la ruta marcada no es factible por algún motivo, se producirá un error. La segunda es loose source enrutamiento donde se establece claramente los enrutadores por los que debe pasar el paquete, pero se da libertad a la red para que use otros enrutadores cuando lo considere conveniente. La limitación en la longitud de las opciones impone un límite máximo en el número de saltos que pueden especificarse. El uso de los campos opcionales del encabezado IP tiene generalmente problemas de rendimiento, ya que las implementaciones de los enrutadores optimizan el código para las situaciones normales, es decir, para paquetes sin campos opcionales. Las opciones están implementadas y funcionan, pero lo hacen generalmente de forma poco eficiente ya que en el diseño del software no se ha hecho énfasis en su optimización.

Fragmentación

El tamaño de un paquete IP se especifica en un campo de dos bytes, por lo que su valor máximo es de 65535 bytes. Sin embargo, muy pocos protocolos o tecnologías a nivel de enlace admiten enviar frames de semejante tamaño. Normalmente, el nivel de enlace no fragmenta, por lo que tendrá que ser IP el que adapte el tamaño de los paquetes para que quepan en los frames del nivel de enlace. Por lo tanto, en la práctica el tamaño máximo del paquete viene determinado por el tamaño máximo del frame característico de la red utilizada. Este tamaño máximo de paquete se conoce como MTU o Maximum Transfer Unit. La siguiente tabla muestra algunos valores característicos de MTU de las tecnologías de redes más usadas.

Protocolo a nivel de enlace	MTU (Bytes)
PPP (valor por defecto)	1500
PPP (bajo retardo)	296
SLIP	1006 (límite original)
X.25	1600 (RFC 1356)
Frame Relay	1600 (depende de la red)
SMDS	9235
Ethernet DIX	1500
Ethernet LLC-SNAP	1492
IEEE 802.4/802.2	8166
Token Ring 16Mbps	17940 (token holding time 8 ms)
Token Ring 4Mbps	4440 (token holding time 8 ms)
FDDI	4352
Hyperchannel	65535
IP clásico sobre ATM	9180

Tabla 2.3. Valor de MTU para protocolos comunes de nivel de Enlace.

Existen dos situaciones en que se produce fragmentación. La primera, denominada *fragmentación en ruta*, se produce cuando un paquete es creado por un host en una red con un valor determinado de MTU y en su camino hacia el host de destino ha de pasar por otra red con una MTU menor. En estos casos, el enrutador que hace la transición a la red de MTU menor ha de fragmentar los paquetes para que no excedan el tamaño de la nueva red. La segunda, llamada *fragmentación en origen*, se produce como consecuencia del diseño de la aplicación. Por ejemplo, muchas implementaciones del sistema de archivos de red NFS, que es bastante usado en máquinas Unix, generan paquetes de 8 KBytes de datos (8212 bytes con el encabezado IP). Un host en una red Ethernet que utilice NFS tendrá que fragmentar cada paquete en seis fragmentos antes de enviarlo, aún cuando el host de origen y destino se encuentren ambos en el mismo segmento Ethernet, debido al tamaño máximo que puede tener un frame Ethernet o IEEE 802.3.

La fragmentación se realiza cortando la parte de datos del paquete en trozos del tamaño máximo permitido por la nueva red. Todos los campos del encabezado del paquete original se repiten en los fragmentos, excepto aquellos que se emplean para distinguirlos entre sí. Una vez fragmentado, un paquete no se reensambla hasta que llegue al host de destino, aún cuando en el trayecto pase a través de redes que admitan una MTU mayor. Los estándares Internet recomiendan que todas las redes que soporten TCP/IP tengan una MTU de al menos 576 bytes, condición que cumplen la mayoría de las redes. La MTU mínima imprescindible para funcionar en TCP/IP es de 68 bytes, valor que corresponde a 60 bytes de encabezado (el máximo con todos los campos opcionales) y 8 bytes de datos, que es el fragmento mínimo de datos que puede hacerse.

El campo identificación del encabezado IP es usado por el emisor para marcar cada paquete emitido. De esta forma, en caso de que se produzca fragmentación, el receptor podrá reconocer las partes que corresponden al mismo paquete, ya que todas irán acompañadas de la misma identificación.

El bit DF cuando está en 1 indica a los enrutadores que este paquete no debe fragmentarse, situación que normalmente se hace por uno de los dos motivos siguientes:

1. El receptor no está capacitado para reensamblar los fragmentos.
2. Cuando se aplica la técnica de descubrimiento de MTU del trayecto o “path MTU discovery” que permite averiguar el MTU de una ruta. Esta técnica consiste en que el host de origen envía un paquete del tamaño máximo al host de destino con el bit DF en 1. Si el paquete no puede pasar en algún punto del trayecto el enrutador correspondiente genera un mensaje de error que es devuelto al host emisor. Entonces, este envía otro paquete más pequeño, también con el bit DF en 1. Así, usando prueba y error, se consigue que algún paquete pase sin fragmentar al host destino. Para acelerar el proceso, algunos enrutadores incorporan en los mensajes de error información sobre la MTU máximo que puede admitir la red que ha provocado el rechazo.

El campo Offset del Fragmento del paquete IP sirve para indicar, en el caso de que el paquete sea un fragmento, en que posición del original se sitúan los datos que contiene el fragmento actual. Las divisiones de un paquete siempre se realizan en múltiplo de 8 bytes, que es la unidad elemental de fragmentación, por lo que este campo cuenta los bytes en grupos de 8.

Como los fragmentos de un paquete pueden llegar desordenados a su destino, el receptor podrá identificarlos gracias al campo Identificación. La longitud total del paquete puede calcularla cuando recibe el último fragmento, que está identificado por el bit MF en 0. A partir de los campos Longitud y Offset del Fragmento la longitud será: *Fragment Offset* * 8+*Longitud*.

Cuando se fragmenta un paquete, el host receptor retiene en su buffer los fragmentos y los reensambla cuando los ha recibido todos. Mientras mantiene retenido un fragmento, el host va restando cada segundo una unidad al campo TTL. Cuando el valor de TTL es igual a cero, descarta el fragmento. Si alguno de los fragmentos de un paquete se pierde, el resto terminarán desapareciendo a medida que agoten su TTL.

En IP, no existe ningún mecanismo que contemple el reenvío de paquetes o de fragmentos. Si el protocolo utilizado a nivel superior maneja reenvío de datos perdidos, como es el caso de TCP a nivel de transporte, se provocará el reenvío del paquete correspondiente. Normalmente, el segundo envío se verá sometido a la misma fragmentación que el primero, pero el segundo no podrá en ningún caso aprovechar fragmentos residuales que pudiera haber en el host receptor correspondientes al primer envío, ya que desde el punto de vista del nivel IP se trata de dos paquetes distintos e independientes que reciben identificaciones diferentes.

2.1.2.1 Protocolo TCP

TCP (Transmission Control Protocol) es el protocolo de transporte confiable utilizado en Internet en el nivel de transporte. Este protocolo ha adquirido su popularidad gracias a las características que presenta:

Protocolo Orientado a Conexión. Las aplicaciones solicitan la conexión al destino y luego usan esta conexión para entregar y transferir los datos, garantizando que estos serán entregados sin problema.

Punto a Punto. Una conexión TCP tiene dos extremos, que son los entes que participan en la comunicación, es decir, emisor y receptor.

Confiabilidad. TCP garantiza que los datos transferidos serán entregados sin ninguna pérdida, duplicación o errores de transmisión.

Full Duplex. Los extremos que participan en una conexión TCP pueden intercambiar datos en ambas direcciones simultáneamente.

Conexión de Inicio Confiable. El uso del three-way handshake garantiza una condición de inicio confiable y sincronizada entre los extremos de la conexión.

Término de Conexión Aceptable. TCP garantiza la entrega de todos los datos antes de la finalización de la conexión.

Debido a que TCP, al igual que UDP, está en la capa de transporte, necesita valerse de IP para el envío de sus segmentos o mensajes. De esta manera, IP trata al mensaje TCP como la información que debe entregar y en ningún momento intenta interpretar su contenido, como generalmente se hace al pasar un mensaje de una capa a otra inferior. Los extremos de la conexión son identificados por puertos, lo garantiza que se puedan establecer múltiples conexiones en cada host y que los puertos puedan estar asociados con una aplicación o un puerto directamente. De lo anterior se desprende que los routers o cualquier dispositivo de nivel tres sólo puede observar los encabezados IP (nivel de red) para el reenvío de los datagramas, y nunca interpretarán los datos de un nivel superior, pues esto supone violar el modelo de capas. Por lo tanto, TCP en la máquina destino, es el encargado de interpretar los mensajes TCP, después de recibirlos de la capa de red, quien previamente le ha quitado el encabezado IP.

TCP usa diversas técnicas para proveer la entrega confiable de datos. Estas técnicas permiten a TCP recobrarse de errores como paquetes perdidos, duplicados, retardo, diferentes velocidades de transmisión entre nodos y congestión.

Paquetes perdidos

TCP usa confirmación positiva con retrasmisión para lograr la entrega de datos confiable. De este modo, el receptor envía mensajes de control de confirmación (ACK) al emisor para verificar la recepción exitosa de la información. A su vez, el emisor inicializa un timer al transmitir la información. Si el timer expira antes que la confirmación llegue, el emisor debe retransmitir la información inicializando un nuevo timer.

Paquetes duplicados

Si el receptor recibe un paquete duplicado no lo toma en cuenta y procede a su descarte, ya que este habrá sido tomado y marcado como recibido.

Retardo de paquetes

Si un paquete no es recibido y el siguiente si, el receptor no mueve la ventana deslizante hasta que el segmento faltante sea recibido. De esta manera el receptor al no recibir el ACK correspondiente al paquete retrasado lo reenvía.

Diferentes velocidades de transmisión

Al establecer la conexión TCP, tanto el emisor como el receptor indican cual es su capacidad de almacenamiento intermedio (buffers) para acordar cual será la velocidad a la cual la transmisión se llevará a cabo.

Ventana Deslizante (Sliding Window)

TCP implementa una política en la cual mantiene una ventana para medir la congestión, cada vez que un temporizador expira, esta ventana es reducida. Para la decisión de envío de datos, el emisor toma en cuenta el tamaño de esta ventana para crear el tamaño de la ventana deslizante de datos.

Para proveer transparencia, cada aplicación entrega arbitrariamente toda la información como un flujo de datos, luego TCP se encarga de separar esta información en segmentos, cada uno de los cuales tiene a lo más el tamaño de un paquete IP. El flujo dado por la aplicación es numerado por la cantidad de bytes transferidos, y cada uno de estos segmentos contiene un número de secuencia de los bytes de información. Así, el receptor envía un segmento con el número de secuencia de la información confirmada, no de los segmentos. Los ACKs son acumulativos, de esta manera un ACK puede ser la confirmación de varios segmentos. Para poder sintonizar el timeout de TCP, este debe estar basado en el round trip time (RTT) que tenga un paquete de red, ya que si es menor que este se creará un tráfico innecesario y no habrá comunicación entre los extremos de la conexión. Sin embargo, existe un problema: el emisor no puede saber de antemano en RTT de ningún paquete antes de la transmisión. Debido a esto, el emisor usa un timeout de retransmisión (RTO) obtenido de RTTs previos.

Debido a que el tráfico excesivo que pueda presentar una red es una de las causas de la pérdida de paquetes, algunos protocolos como TCP, proveen la retransmisión como mecanismo para garantizar la llegada de los mensajes. Esta solución más que una buena solución es un arma de doble filo, ya que la retransmisión excesiva puede contribuir a la congestión.

La pérdida de paquetes es interpretada por TCP como un indicador de congestión. El mecanismo de control de TCP es usado por el nodo emisor para detectar el nivel de congestión y si este está sobre un cierto nivel umbral considerado el máximo aceptable, la retransmisión de paquetes es reducida. El mecanismo utilizado consiste en que un host envía un paquete, y si una confirmación llega sin perdida, el emisor envía dos paquetes y comienza a aumentar la ventana en potencias de dos. Cuando TCP envía un número de paquetes igual a la mitad del tamaño de una ventana, la tasa de incremento disminuye hasta recibir las confirmaciones de los paquetes enviados.

Puertos TCP

Un puerto es un número entero entre 0 y 65535 (lo que corresponde a un número entero positivo de 16 bits) que especifica la dirección TSAP a la cual se dirige una conexión TCP o UDP. En

un mismo host, un número de puerto puede ser utilizado simultáneamente por una aplicación para UDP y por otra para TCP, lo que no plantea ningún conflicto, ya que son TSAPs diferentes.

Puerto	Aplicación	Descripción
9	Discard	Descarta todos los datos recibidos (para pruebas)
19	Chargen	Intercambio de strings (para pruebas)
20	FTP-Data	Transferencia de datos en FTP
21	FTP	Intercambio de información de control en FTP
22	SSH	Sesión remota segura en una máquina
23	Telnet	Sesión remota en una máquina
25	SMTP	Envío de mails a través de servidor de correos
53	DNS	Consulta y transferencia de datos de servicio de nombres
80	HTTP	Protocolo http para intercambio de páginas web
110	POP3	Lectura de correo electrónico
139	NetBIOS	Intercambio de datos usando NetBIOS en redes locales con Windows
143	IMAP	Lectura de correo electrónico
179	BGP	Sesión de intercambio de información del protocolo BGP
443	HTTPS	Protocolo HTTP para intercambio de páginas web seguras

Tabla 2.5. Puertos TCP mas usados.

Por convenio los números 0 a 1023 están reservados para el uso de servicios estándar, por lo que se les denomina puertos bien conocidos (well-known ports). Cualquier número por encima de 1023 está disponible para ser utilizado libremente por los usuarios. En la tabla 2.5 se presentan algunos de los puertos más utilizados.

Encabezado TCP

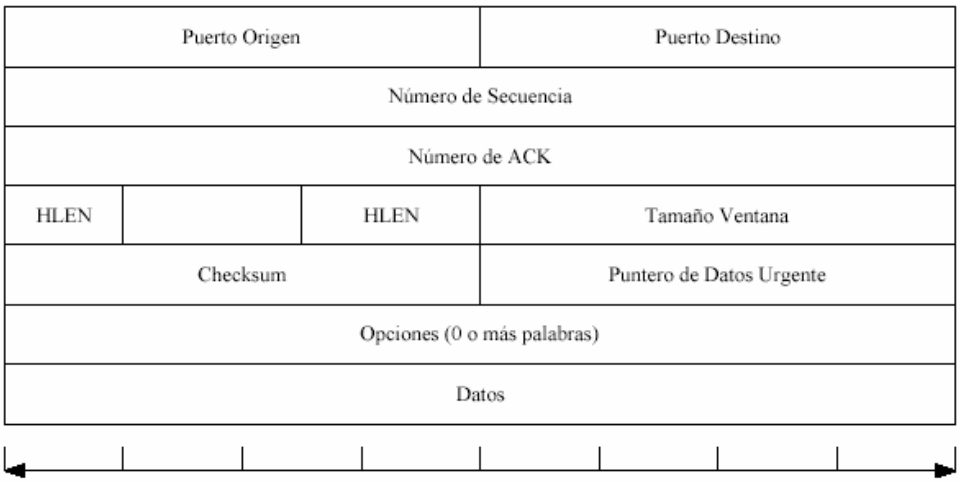

Fig. 2.6. Encabezado TCP.

Puerto Origen y Destino. 2 Bytes cada uno que identifican los puertos que se van a utilizar en cada host para comunicar con las aplicaciones que intercambian datos.

Número de Secuencia. 4 Bytes, indican el número de secuencia que corresponde, en la conexión, al primer byte que se envía en el campo datos de ese segmento.

Número de ACK. 4 Bytes que apuntan al número de secuencia del primer byte del próximo segmento que se espera recibir del otro lado.

Longitud de Encabezado TCP. 4 bits que especifican el largo del encabezado, en palabras de 32 bits. Este valor no incluye el campo datos, y el campo opciones hace que esta longitud pueda variar.

Bits de Codificación. 6 bits que se presentan a continuación de 6 bits no utilizados. Corresponden a bits flag, cuyo nombre y significado es el siguiente: URG (urgent, sirve para indicar que el segmento contiene datos urgentes, y el campo puntero de datos urgentes contiene la dirección donde terminan estos), ACK (acknowledgement, indica que en este segmento el campo Número de ACK tiene el significado habitual , de lo contrario carece de significado; en la práctica, el bit ACK esta a 1 siempre, excepto en el primer segmento enviado por el host que inicia la conexión), PSH (push, indica que el segmento contiene datos PUSHED, es decir, que deben ser enviados rápidamente a la aplicación correspondiente sin esperar a acumular varios segmentos), RST (reset, usado para indicar que se debe abortar una conexión porque se ha detectado un error de cualquier tipo), SYN (synchronize, este bit indica que se está estableciendo la conexión y está puesto en 1 s´olo en el primer mensaje enviado por cada uno de los dos hosts en el inicio de la conexión) y FIN (finish, indica que no se tienen más datos que enviar y que se quiere cerrar la conexión; se usa ya que para que una conexión se cierre de manera normal cada host ha de enviar un segmento con el bit FIN puesto en 1).

Tamaño de Ventana. 2 Bytes que indican la cantidad de bytes que se está dispuesto a aceptar del otro lado en cada momento. Mediante este parámetro el receptor establece un control de flujo sobre el flujo de datos que puede enviar el emisor.

Checksum. 2 Bytes y sirve para detectar errores en el segmento recibido. Estos podrían ser debidos a errores de transmisión no detectados, a fallos en los equipos o a problemas en el software.

Puntero de Datos Urgentes. 2 Bytes, indican el final de un flujo de datos de tipo urgente, ya que el segmento podría contener datos no urgentes. TCP no marca el principio de los datos urgentes, es responsabilidad de la aplicación averiguarlo.

Opciones. Cero o más Bytes que habilitan un mecanismo por el cual es posible incluir extensiones al protocolo. Entre las más interesantes se encuentran las siguientes: tamaño máximo de segmento, uso de repetición selectiva (en vez de retroceso n), uso de NAK (acuse de recibo negativo en caso de no recepción de un segmento), uso de ventana mayor de 64 KBytes mediante el empleo de un factor de escala.

2.1.2.2 Protocolo UDP

TCP tiene la robustez y funcionalidades propias de un protocolo de transporte orientado a conexión; sin embargo esa robustez y funcionalidad tienen aparejadas una cierta complejidad. Por ejemplo, cualquier transmisión de información TCP requiere como mínimo el intercambio de seis mensajes para establecer la comunicación y terminarla. Además, mientras una conexión existe ocupa una serie de recursos en el host que está llevándola a cabo.

En determinadas oportunidades no se requiere toda la funcionalidad que TCP provee en las conexiones, más aún, cualquier transmisión de información TCP presenta el retardo ya comentado de seis mensajes como mínimo, lo que puede llegar a ser significativo para alguna aplicación determinada. Por esto, en algunos casos se prefiere que el nivel de transporte preste un servicio más sencillo, no orientado a conexión y no confiable.

Algunos ejemplos de situaciones en las que es más conveniente un servicio no orientado a conexión son: aplicaciones tiempo real como audio o video, donde no se puede tolerar el retardo producido por los ACK, consultas a servidores en que se requiere el envío de uno o dos mensajes únicamente como es el caso del DNS, etc.

UDP (User Datagrama Protocol) es el protocolo no orientado a conexión de Internet y entre las aplicaciones que utilizan UDP se encuentran TFTP (Trivial File Transfer Protocol), DNS (Domain Name Server), SNMP (Simple Network Management Protocol), NTP (Network Time Protocol), NFS (Network File System) , etc.

Los TPDUs intercambiados por UDP se denominan mensajes o datagramas UDP. Una de las características más interesantes de UDP es que puede ser utilizado por aplicaciones que necesitan soporte de tráfico multicast o broadcast. Con TCP esto no es posible debido a la naturaleza punto a punto, orientada a conexión del protocolo.

UDP no suministra ningún mecanismo de control de flujo o control de congestión. Cuando lo que se envía es únicamente un mensaje esto es innecesario, ya que presumiblemente un mensaje aislado no creará problemas de congestión y será siempre aceptado en destino. Si se desea enviar un flujo de mensajes, por ejemplo video o audio en tiempo real, se deberán tomar las medidas adecuadas para asegurar la capacidad suficiente en la red y evitar la congestión no excediendo lo solicitado en el momento de hacer la reserva.

En caso de congestión en la red parte de los datagramas serán descartados por la red sin informar por ningún mecanismo al emisor, ni al receptor. En caso de saturación del receptor, este sencillamente ignorará los datagramas que no pueda aceptar. En algunos casos, se contemplan a nivel de aplicación mecanismos de control que permiten al receptor detectar si se producen pérdidas (por ejemplo, numerando los datagramas) informando al emisor para que baje el ritmo de emisión si se supera un umbral determinado.

Puertos y Encabezado UDP

De forma similar a los segmentos TCP, los datagramas UDP se dirigen a la aplicación adecuada mediante el puerto de destino, especificado en el encabezado. Análogamente a TCP los puertos UDP se identifican mediante un campo de 16 bits (números entre 0 y 65535). A un en el caso de coincidir en número con un puerto TCP son TSAPs diferentes. Al igual que en TCP los valores por debajo de 1024 están reservados para los puertos bien conocidos, aunque su significado es diferente en la mayoría de los casos.

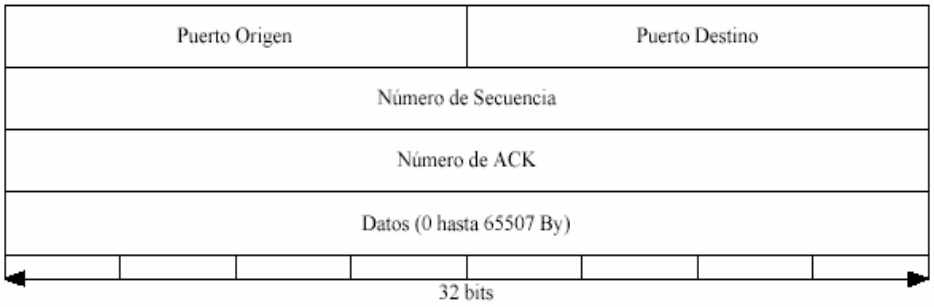

Fig. 2.7. Encabezado de un Datagrama UDP.

Puerto Origen y Destino. 2 Bytes cada uno, que especifican el puerto de la aplicación que genera y recibe el mensaje. A diferencia de TCP, el campo origen valdrá normalmente cero, salvo que la aplicación solicite una respuesta.

Longitud. 2 Bytes que indican la longitud del mensaje, incluyendo los campos de encabezado.

Checksum. 2 Bytes. Su uso es opcional en IPv4 y obligatorio en IPv6, ya que en ese caso se ha suprimido el checksum a nivel de red. Cuando se envía información en tiempo real su uso puede omitirse. Si la verificación del checksum en el receptor arroja un error, el mensaje es descartado sin notificarlo al nivel de aplicación ni al emisor.

Datos. contiene los datos a transmitir.

De la misma forma que un host o un router pueden tener que fragmentar un datagrama que contenga un segmento TCP, es posible que el host emisor o algún router intermedio tengan que fragmentar un mensaje UDP porque sea mayor que la MTU permitida en la red por la que ha de enviarse. Análogamente a los segmentos TCP la fragmentación ocurre de forma transparente a UDP y el encabezado del mensaje sólo aparecerá en el primer fragmento. En cambio, cada fragmento deberá incluir un nuevo encabezado IP.

2.1.3 ATM

ATM (Asynchronous Transfer Mode) es un estándar de la ITU-T para la transmisión de celdas con información de múltiples servicios tales como voz, video y datos. ATM tuvo sus orígenes en 1988 cuando la ITU-T seleccionó ATM como la base para desarrollar el estándar B-ISDN (Broadband Integrated Services Digital Network), y fue concebido originalmente como una tecnología de alta velocidad para voz, video y datos sobre redes públicas. El foro de ATM extendió la visión de la ITU-T al permitir el uso de ATM en redes públicas y privadas. Algunas de las especificaciones del foro son:

- User-to-Network Interface (UNI) 2.0
- UNI 3.0
- UNI 3.1
- Public-Network Node Interface (P-NNI)
- LAN Emulation

ATM es una tecnología de conmutación y multiplexación de celdas que combina los beneficios de la conmutación de circuitos (capacidad garantizada, y un retardo de transmisión constante) con los de la conmutación de paquetes (flexibilidad y eficiencia para tráfico intermitente). Además provee escalabilidad en el ancho de banda de algunos megabits por segundo a muchos gigabits por segundo.

ATM posee la habilidad de multiplexar diversos tipos de servicios (voz, video, datos, etc.) en una única red física no canalizada (unchannelized). Este método de multiplexaje de las celdas ATM define el concepto de modo de transferencia asíncrono, en donde el término asíncrono se refiere a la capacidad de la red ATM de enviar datos asociados a una conexión sólo cuando realmente hay datos que transmitir. En contraste con las redes canalizadas (channelized), en donde aún cuando el canal está libre, es necesario enviar un patrón especial en cada ranura de tiempo (time slot) que representa a un canal libre. De lo contrario, el receptor no sería capaz de recuperar la información presente en el resto de los time slots. Esta es la esencia de las redes que emplean modos de transferencia síncronos, en donde, a cada fuente se le asigna un ancho de banda fijo basada en una posición, por ejemplo, una banda de frecuencia en FDM o un time slot en TDM. El tráfico en ATM, por el contrario:

- No está basado en una posición fija en el flujo de datos, ya que un encabezamiento en la información ATM identifica hacia donde debe ser dirigido el tráfico.
- Es bajo demanda, en otras palabras, si no hay tráfico no se emplea ancho de banda, por lo cual el ancho de banda disponible puede ser empleado para otras conexiones. Esto, evidentemente, supone una gran ventaja frente a otros sistemas.

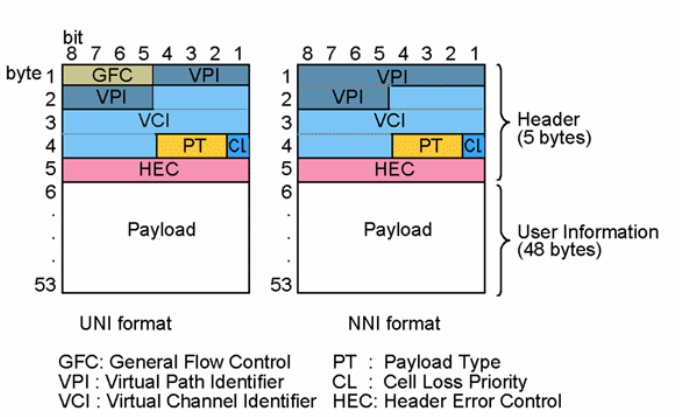

Fig. 2.8. El formato de las celdas tal y como ha sido definido por el forum ATM.

Dos de los conceptos más significativos del ATM, Canales Virtuales y Rutas Virtuales, están materializados en dos identificadores en el encabezado (header) de cada célula (VCI y VPI) ambos determinan el enrutamiento entre nodos. Existen dos formatos de células: la UNI (User Network Interface) utilizado en el interfaz red/usuario y la NNI Network Interface) cuando circulan por la red.

Modelo de Referencia ATM/B-ISDN

El modelo ATM está compuesto por tres planos que abarcan todas las capas:

- *Control.* Este plano es responsable de administrar la transferencia de información.
- *Administración.* Este plano ha sido subdividido en dos planos más:
  - *Administración de capas.* Administra funciones específicas de cada capa como la detección de fallas y problemas con los protocolos.
  - *Administración de planos.* Administra y coordina funciones relativas a el sistema completo. Actualmente es un concepto abstracto con poca estandarización. Puede ser visto como una bolsa para las cosas que no se adaptan en otras porciones del modelo y cumple un papel de administrador global del sistema.

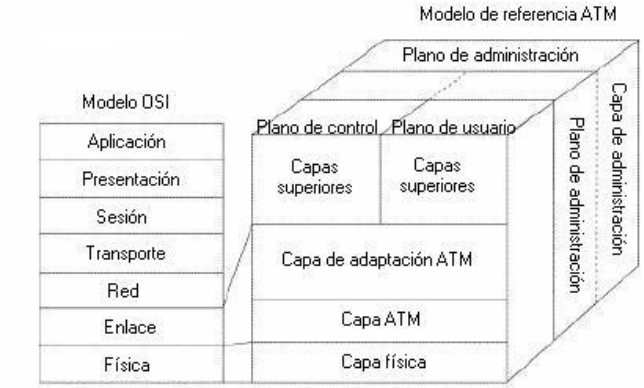

Fig. 2.9. Las funcionalidades de ATM abarcan la capa física y parte de la capa de enlace del Modelo OSI.

Capa Física (Physical Layer)

La capa física provee transmisión de celdas ATM sobre un medio físico que conecta dispositivos ATM. Esta capa tiene cuatro funciones:

- Convertir bits a celdas.
- Controlar la transmisión y recepción de bits sobre el medio físico.
- Rastrear los límites de las celdas ATM.
- Empaquetar las celdas en el tipo apropiado de frame de acuerdo al medio físico.

ATM es independiente del transporte físico. Las celdas ATM pueden ser transportadas en redes SONET (Synchronous Optical Network), SDH (Synchronous Digital Hierarchy), T3/E3, TI/EI, par trenzado o aún en módems de 9600 bps.

El Nivel Físico debe adaptar la secuencia de celdas a la estructura y a la velocidad del canal de transmisión utilizado.

Capa ATM

La capa ATM (ATM Layer) combinada con la capa de Adaptación ATM (AAL), es análoga a la capa de enlace del modelo de referencia OSI. La capa ATM es responsable de establecer conexiones y pasar las celdas por la red ATM. Todo esto lo hace con la información del encabezado de cada celda ATM. Esta capa es independiente del servicio.

El formato de una celda ATM consiste de 5 bytes de cabecera y 48 bytes para información. Las celdas son transmitidas serialmente y se propagan en estricta secuencia numérica a través de la red. El tamaño de la celda ha sido escogido como un compromiso entre una larga celda, que es muy eficiente para transmitir largas tramas de datos y longitudes de celdas cortas que minimizan el retardo de procesamiento de extremo a extremo, que son buenas para voz, vídeo y protocolos sensibles al retardo. A pesar de que no se diseñó específicamente para eso, la longitud de la celda ATM acomoda convenientemente dos Fast Packets IPX de 24 bytes cada uno.

Los comités de estándares han definido dos tipos de cabeceras ATM: los User-to-Network Interface (UNI) y la Network to Node Interface (NNI).

La UNI es un modo nativo de interfaz ATM que define la interfaz entre el equipo del cliente (Customer Premises Equipment), tal como hubs o ruteadores ATM y la red de área ancha ATM (ATM WAN).

La NNI define la interfase entre los nodos de la redes (los switches o conmutadores) o entre redes. La NNI puede usarse como una interfase entre una red ATM de un usuario privado y la red ATM de un proveedor público (carrier). Específicamente, la función principal de ambos tipos de cabeceras de UNI y la NNI, es identificar las "Virtual paths identifiers" (VPIS) y los "virtual circuits" o virtual channels"(VCIS) como identificadores para el ruteo y la conmutación de las celdas ATM.

Capa de Adaptación ATM (AAL)

La tercera capa es la ATM Adaptation Layer (AAL). La AAL juega un papel clave en el manejo de múltiples tipos de tráfico para usar la red ATM, y es dependiente del servicio. La función principal es convertir flujos de celdas en formatos que pueden ser usados por un amplio rango de

aplicaciones. Adapta los servicios dados por la capa ATM a aquellos servicios que son requeridos por las capas más altas, tales como vídeo, audio, frame relay, etc. La AAL recibe los datos de varias fuentes o aplicaciones y las convierte en los segmentos de 48 bytes. Cinco tipos de servico AAL están definidos actualmente.

Tipos de Servicio ATM

- *CBR (Constant Bit Rate).* Soporta aplicaciones en tiempo real que requieren una cantidad fija de ancho de banda. Algunos ejemplos de las aplicaciones que soporta son aplicaciones de voz, video con una tasa constante de transmisión.
- *rt-VBR (Real time Variable Bit Rate).* Soporta aplicaciones sensibles al tiempo que necesitan inhibición del retraso y requerimientos en la variación del retardo, pero que se transmiten a una tasa variable. Las aplicaciones de voz y video sin una tasa de transmisión constante utilizan esta clase de servicio.
- *nr-VBR (Non-real-time Variable Bit Rate).* Soporta aplicaciones que no son sensibles al retardo o variaciones en el retardo, pero que tienen características de transmisión variable, y ráfagas de tráfico. Entre las aplicaciones se tienen las sesiones de terminal y las transferencias de archivos.
- *ABR (Available Bit Rate).* Trabaja en cooperación con recursos que pueden cambiar su tasa de transmisión en respuesta a las condiciones de la red. ABR provee de acceso dinámico a ancho de banda que no se encuentra utilizado en el momento. Las interconexiones LAN, las transferencias de archivos de alto desempeño, y el almacenamiento de bases de datos, WEB son aplicaciones que utilizan esta clase de servicio.
- *UBR (Unspecified Bit Rate).* Este servicio es llamado de "mejor esfuerzo", es utilizado por tráfico que soporta variación en el retraso o jitter, y no garantiza calidad de servicio específica. Este tipo de tráfico se encuentra en riesgo ya que no hay ninguna garantía en el desempeño. La mayoría de las implementaciones de LAN e IP utilizan el servicio de mejor esfuerzo, por lo que las aplicaciones que utilizan esta clase de servicio son IP sobre ATM y tráfico no crítico.

Capa de adaptación ATM (AAL)

La función principal de la capa de Adaptación ATM (AAL) es convertir flujos de celdas en formatos que pueden ser usados por un amplio rango de aplicaciones. Esta capa del modelo de referencia ATM/B-ISDN se encuentra definida en las recomendaciones de la ITU-T I.362 y I.363.

- *AAL1.* Ofrece servicios orientados a conexión para manejar aplicaciones de voz y video conferencia. AAL1 Requiere de sincronización entre origen y destino, por lo que es dependiente del medio.
- *AAL3/4.* Soporta servicios orientados a conexión y servicios no orientados a conexión. Fue diseñado para proveedores de servicio de red y para transmitir paquetes SMDS sobre una red ATM.
- *AAL5.* Soporta servicios orientados y no orientado a conexión. Soporta clásico IP sobre ATM y LANE

El Nivel de Adaptación ATM adapta cada tráfico a su velocidad inicial, segmenta/reensambla la información en trozos de 48 bits, detecta celdas erróneas o perdidas, y mantiene el sincronismo entre los usuarios conectados.

Formato de la celda de ATM

Los estándares de ATM definen una célula con un tamaño fijo de 53 octetos (o bytes), que consisten en un Header (H) de 5 octetos y una carga útil (P) de 48 octetos.

Campos del encabezado de la celda de ATM

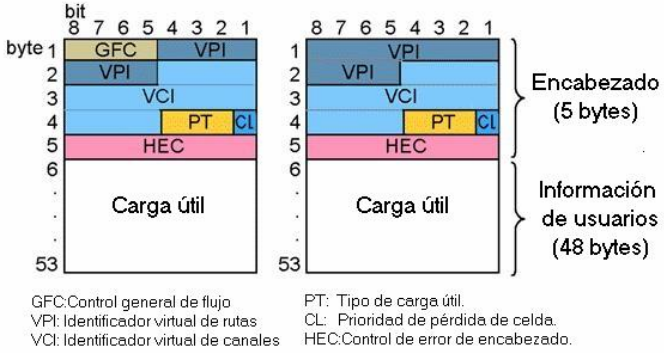

Fig. 2.10. Formato de las celdas ATM.

- *Generic Flow Control (GFC).* Provee funciones locales, tal como la identificación de múltiples estaciones que comparten una misma interfase ATM, y permite a un multiplexor controlar la tasa de transmisión de una terminal. Este campo generalmente no se utiliza en los estándares del foro ATM.
- *Virtual Path Identifie (VPI)*. En conjunto con el VCI, identifica el siguiente destino de una celda mientras atraviesa una serie de switches ATM hacia su destino.
- *Virtual Channel Identifier (VCI).* En conjunto con el VCI, identifica el siguiente destino de una celda mientras atraviesa una serie de switches ATM hacia su destino.
- *Payload Type (PT).* Indica en el primer bit si la celda contiene información de usuario o de control. Si la celda contiene información de usuario, el segundo bit indica congestión, y el tercer bit indica si la celda es la última de una serie de celdas que representa una trama sencilla AAL5.
- *Congestion Lost Priority (CLP).* Indica si la celda debe ser descartada si encuentra congestión extrema en la red. Si el CLP es igual 1 indica que la celda debe ser descartada en preferencia a celdas con CLP igual a 0.
- *Header Error Control (HEC).* Calcula un checksum del encabezado exclusivamente.

Direccionamiento ATM

El direccionamiento ATM esta basado en las direcciones ITU-T definidas en el estándar E.164, que es muy similar a los números telefónicos. El foro de ATM extendió éste direccionamiento para incluir redes privadas, para esto se optó por un modelo de subred o de revestimiento, en el que la capa de ATM es responsable para mapear las direcciones de la capa de red con direcciones ATM.

Conexiones y Enrutamiento

Los conmutadores de VP modifican los identificadores VPI para redirigir las rutas de entrada hacia una salida específica. Un conmutador de VP no analiza ni modifica el campo VCI, ya que al operar en un nivel inferior conmuta todos los Canales asociados a dicha Ruta. Los conmutadores de

VC aplican un mayor nivel de complejidad ya que manejan atributos como nivel de errores, calidad servicio, ancho de banda o servicios relacionados con la tarificación. Las tablas de enrutamiento de cada nodo pueden estar ya predefinidas, o bien deben construirse dinámicamente en el tiempo del establecimiento de las conexiones realizadas mediante el protocolo Q.2931 similar al Q.931 utilizado en el ISDN para banda estrecha.

Una Ruta Virtual puede ser Permanente (PVP) o Conmutada (SVP). Si es conmutada, es decir si se ha establecido explícitamente para una comunicación, todos sus Canales Virtuales (VC) asociados son dirigidos a través de ese camino y no será necesario conmutarlos. Si el VP es permanente es probable que sólo conecte troncales de la red por lo que los VC deberán ser conmutadas en algún nodo de la red. El enrutamiento de Canales y Rutas Virtuales es realizado mediante etiquetas, nunca con direcciones explícitas. Por ejemplo un nodo de conmutación debe leer el identificador VCI = i de cada célula que entra por el puerto K y de acuerdo con su tabla de enrutamiento, la envía por el puerto Q modificando el header al escribir VCI = j.

La capa ATM es el núcleo real de la tecnología. Se ocupa de añadir y extraer las cabeceras, mantener los identificadores de conexión para realizar el encaminamiento entre nodos, y de multiplexar y demultiplexar las celdas a través del medio físico, manteniendo un secuenciamiento correcto de las celdas.

Ventajas de ATM

En comparación con un red IP tradicional, la velocidad de transito de los dos se ve incrementada.

Además de que hay mayor seguridad en el establecimiento de circuitos y transmisión de datos a través de ellos por su carácter orientado a conexión.

Desventajas de ATM

- Tiene un mayor costo que una red IP tradicional.
- Se necesitan dispositivos específicos para esta tecnología.
- Flexibilidad reducida a l ser una tecnología orientada a conexion.
- No existen mecanismo de corrección de errores en esta tecnología, lo cual hace necesario un medio altamente confiable, que resulta muy caro.

2.1.4 Frame Relay

Frame Relay es un protocolo WAN que opera en las capas 1 y 2 del modelo de referencia OSI. Es una tecnología de conmutación de paquetes que permite a estaciones compartir dinámicamente el acceso a la red y el ancho de banda disponible. Tramas de longitud variable son usadas para una transmisión flexible y transparente, las cuales son conmutadas a través de varios segmentos de red hasta alcanzar su destino final.

Técnicas de multiplexado estadístico controlan el acceso al medio, dando mayor flexibilidad y eficiencia al uso del ancho de banda disponible en la red.

Frame Relay es descrita como la versión estilizada de X.25, ya que aprovechando la confiabilidad de los medios de transmisión digitales, algoritmos robustos para la detección y corrección de errores ya no son implementados, haciendo su operación más rápida y eficiente.

Propuestas iniciales para la estandarización fueron presentadas a la CCITT en 1984, aunque no hubo un gran avance entre la interoperativilidad de equipos hasta 1990 cuando Cisco, Digital Equipment, Northern Telecom. y StrataCom formarón un consorcio enfocado al desarrollo de la tecnología Frame Relay. Este consorcio desarrollo una especificación que era conformada por las especificaciones básicas del protocolo y extensiones que proveían mejoras y aplicaciones más complejos. Estas extensiones son conocidas colectivamente como Local Management Interface (LMI).

La ANSI y la CCITT estandarizaron después sus propias variaciones de la especificación original LMI.

Dispositivos

Los dispositivos conectados en una red Frame Relay caen en dos categorías: DTE (Data Terminal Equipment) y DCE (Data Circuit-terminating Equipment).

Generalmente los DTE´s son equipos terminales y están administrados por los usuarios de la red, tales como terminales, computadoras personales, enrutadores y puentes. Los equipos DCE´s están a cargo del administrador de la red y tienen como función proveer servicios de conmutación y el relog a los dispositivos DTE´s. En la mayoría de los casos se trata de conmutadores de paquetes.

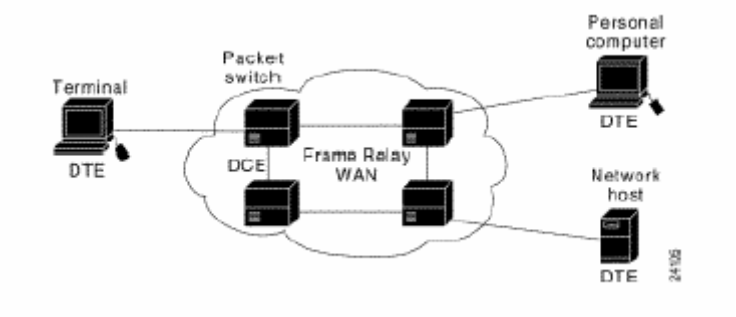

Fig. 2. 11. Circuitos Virtuales.

Tecnología

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, conocidos como anexos a las definiciones del estándar básico. 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 red Frame Relay obtiene datos de los usuarios en las tramas recibidas, comprueba que sean válidas, y las enruta hacia el destino, indicado en el DLCI del campo "dirección". Si la red detecta errores en las tramas entrantes, o si el DLCI no es válido, la trama se descarta.

Trama Frame Relay

Bandera 8 Bits	DLCI 6 Bits	C/R 1 Bit	EA 1 Bit	DLCI 4 Bits	FECN 1 Bit	BECN 1 Bit	DE 1 Bit	EA 1 Bit	Datos 8 A 65512 Bits	FCS 16 Bits	Bandera 8 Bits

Fig. 2.12. Trama Frame Relay.

El significado de los diversos campos es el siguiente:

- *DLCI (Data Link Connection Identifier):* este campo tiene una longitud total de 10 bits (aunque se encuentre dividido en dos partes). Especifica por que 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 indica este campo de un bit se emplea en el control de congestión del que hablaremos más tarde.
- *BECN (Backward Explicit Congestion Notification):* lo veremos en el control de congestión.
- *DE (Discard Elegibility):* este bit tiene una finalidad similar al CLP (Cell Loss Priority) de ATM, es decir, sirve para marcar las tramas de 'segunda clase', que son aquellas que el usuario ha metido en la red superando el caudal que tenía contratado
- *Flag (bandera)*: es la secuencia de comienzo y fin de trama.

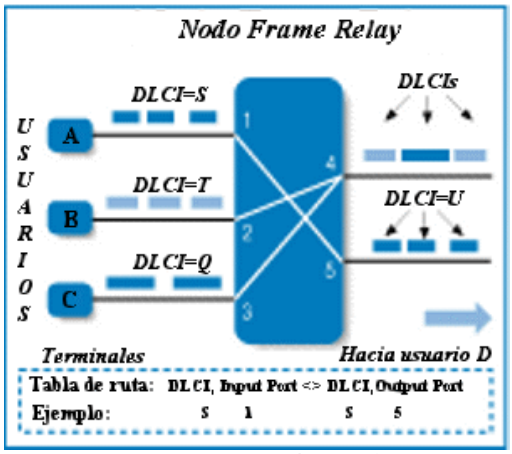

Fig. 2.13. Multiplexación estadística.

El campo de "dirección" contiene el DLCI y otros bits de congestión. Los datos de los usuarios se meten en el campo "Información", de longitud variable que permite transmitir un paquete entero de protocolos LAN.

La figura 2.13 representa cómo se transmite la información de dos usuarios. Lo primero es conectar a los usuarios mediante un acceso Frame Relay (puerto en el nodo de la red más línea de acceso). Después hay que definir en la red un CVP entre los accesos, que es el camino lógico para la transmisión de información. Un usuario puede definir más de un CVP hasta distintos destinos a través de un único acceso Frame Relay. Este concepto se llama multiplexación estadística.

Parámetros de dimensionamiento de CVP (CIR, Bc, Be):

- *CIR:* (Committed Information Rate, o tasa de información comprometida). Tasa a la cual la red se compromete, en condiciones normales de operación, a aceptar datos desde el usuario y transmitirlos hasta el destino. Puede ser distinto en cad a sentido. Son las tramas 1 y 2 del ejemplo.
- *Bc:* (Committed Burst Size o ráfaga comprometida). Es la cantidad de bits transmitidos en el periodo T a la tasa CIR (CIR=Bc/T). En las redes Frame Relay se permite al usuario enviar picos de tráfico a la red por encima de CIR, durante int ervalos de tiempo muy pequeños, incluidos en el periodo T.
- *Be:* (Excess Burst Size, o ráfaga en exceso): es la cantidad de bits transmitidos en el periodo T por encima de la tasa CIR. Si la red tiene capacidad libre suficiente admitirá la entrada de este tipo de tráfico en exceso (trama 3 del ejem plo), marcándolo con DE activo.

El tráfico entrante en la red, por encima de Bc + Be, es el descartado directamente en el nodo de entrada, (trama 4 del ejemplo).

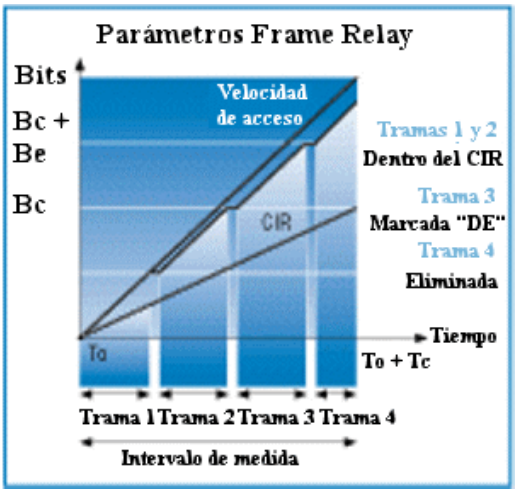

Fig. 2.14. Parámetros Frame Relay.

Frame Relay es el protocolo idóneo para el transporte consolidado de diferentes protocolos de datos, como los del entorno LAN (TCP/IP, IPX, DECNet, etc), los tradicionales (X.25, SDLC, asíncrono, etc.), y las conexiones de Hosts que requieran una interface multiplexada económica, como los FEP IBM 3745.

2.2 Problemática en Redes de Datos

En la actualidad, el tráfico de red es muy diverso, cada tipo de tráfico tiene requerimientos específicos en términos de ancho de banda, retraso, latencia y disponibilidad.

Con el explosivo crecimiento de Internet, la mayor parte del tráfico de red está basado en el protocolo IP. Contar con un único protocolo de transporte de punta a punta es beneficioso, ya que el equipo de redes se simplifica en términos de mantenimiento, con la consecuente disminución de costos operativos. Ese beneficio, sin embargo, se enfrenta al hecho de que el protocolo IP es un protocolo sin conexión, es decir que los paquetes IP no toman un camino específico al atravesar la red.

El protocolo IP fue desarrollado originalmente para asegurar que un paquete llegue a su destino sin prestar demasiada atención al tiempo que necesitaba para llegar hasta allí. Pero ahora, las redes IP deben transportar diferentes tipos de aplicaciones, muchas de las cuales requieren baja latencia. Si esto no se cumple, la calidad que reciba el usuario final puede verse afectada considerablemente, e incluso, en algunos casos, es posible que la aplicación no funcione.

Por ejemplo, las aplicaciones de voz tuvieron su origen en las redes de teléfonos públicos que usaban la tecnología TDM (por sus siglas en inglés, Time Division Multiplexing), la cual tiene una conducta muy determinista. En las redes TDM, el tráfico de voz sufría un retraso bajo ya determinado, pero sin pérdidas. Si tomamos esa aplicación de "voz TDM" y la transportamos sobre una red IP de máxima calidad, la red presentará un retraso impredecible y variable en los paquetes de voz. Por eso, las aplicaciones de voz necesitan el mismo nivel de calidad de "voz TDM" para satisfacer las expectativas de los usuarios. Para ello, las técnicas de QoS pueden ser aplicadas a este tipo de redes para que puedan soportar VoIP con una calidad de voz predecible, consistente y aceptable.

Desde comienzos de los 90 existe una tendencia a transportar todos los servicios sobre la misma infraestructura de red. Tradicionalmente existían redes dedicadas, separadas para los distintos tipos de aplicaciones, pero el uso de muchas de estas redes se está consolidando, con el objetivo de reducir costos operativos o para mejorar los márgenes de ganancia.

Hasta hace poco, una empresa podía contar con una red de voz privada basada en TDM, una red IP para Internet, una red ISDN para videoconferencias, una red SNA y una LAN multiprotocolo (IPX, Apple Talk, etc.). Del mismo modo, un proveedor de servicios podía tener una red de voz basada en TDM, una red ATM o SONET para el backbone y una red de acceso ISDN o Frame Relay.

Actualmente, en cambio, todas las redes de datos convergen en el transporte IP ya que, cada vez con más frecuencia, las aplicaciones tienden a estar basadas en este protocolo. Cuando las diversas aplicaciones contaban con redes dedicadas, las tecnologías de QoS tenían un papel menor, ya que el tráfico era similar en términos de conducta y las redes dedicadas estaban preparadas para satisfacer los requerimientos de conducta de cada aplicación en particular. Pero las redes de convergencia mezclan distintos tipos de tráfico, cada uno de ellos con requerimientos muy diversos. Estos distintos tipos de tráfico pueden llegar a reaccionar de manera desfavorable al funcionar juntos.

2.3 Redes Multiservicios

A continuación se listan las principales redes multiservicios que operan actualmente en México así como sus principales características.

Multiservicios IP de Avantel

Multiservicios IP Avantel es una red de nueva generación con tecnología de punta compuesta de soluciones a la medida de su empresa que le ayudan a mejorar la productividad y obtener grandes ahorros.

Son redes privadas virtuales (VPN) que integran voz, datos, video e Internet en una sola conexión basada en el protocolo IP, que le permite una comunicación entre sus oficinas (Intranets) y con sus socios o clientes (extranets) de manera eficiente y con calidad al tiempo que reduce sus gastos en telecomunicaciones.

Multiservicios IP cuenta con las siguientes modalidades de servicio:

- *VPN Multimedia*. Red Privada Virtual basada en protocolo IP, con calidad en el servicio dando prioridad al tráfico que permite la transmisión de voz, datos, video y telefonía por el mismo enlace con uso dinámico del ancho de banda.
- *VPN Integral*. Red Privada Virtual basada en protocolo IP, con calidad en el servicio dando prioridad al tráfico que permite la transmisión de voz, datos, video, telefonía y acceso a la red mundial de Internet por el mismo enlace con uso dinámico del ancho de banda.

UNINET RPV multiservicios

Servicio que permite implementar Redes Privadas Virtuales (RPV) utilizando el protocolo de transporte IP. Se ofrece en tres diferentes "Clases de Servicio" con el fin de otorgar al cliente diferentes prioridades en la transmisión de su información a través de la red, las cuales se identifican como:

- *Datos*. Clase de Servicio básica de transporte en la que el Cliente puede transmitir archivos de su operación diaria, sin ninguna prioridad.
- *Datos Críticos*. Clase de Servicio que permite al Cliente asignar una mayor prioridad de transporte a su información.
- *Voz/Vídeo*. Clase de Servicio diseñada para transmitir aplicaciones muy sensibles al retraso como son Voz y Vídeo.

Los parámetros de Calidadpara el Serviciode RPV Multiservicios están en función de la jerarquía que tiene el POP (Punto de Presencia) de UNINET que recibe el Acceso Local del Cliente, de acuerdo a las siguientes latencias:

- 100 ms para Sitios Remotos localizados en ciudades de Backbone.
- 150 ms para Sitios Remotos localizados en ciudades de concentración Regional.
- 200 ms para Sitios Remotos localizados en ciudades Sectoriales.

Se entenderá por:

- *Latencia:* tiempo en que tarda un paquete en recorrer la distancia round trip (ida y vuelta) entre dos puntos de referencia, esta medida se expresa en milisegundos, la latencia es independiente de la Clase de Servicio contratada y aplica para medición de extremo a extremo de la red del Cliente (end to end).
- *Pérdida de Paquetes:* es la cantidad (porcentaje) de paquetes que se pierden en la transmisión de los mismos, desde el enrutador origen hasta el enrutador destino, aplica exclusivamente a la red de transporte, es decir, aplica exclusivamente sobre la red de UNINET (nodos Sectoriales, Regionales y Backbone).

Prioridad del Tráfico	Calidad	% de Pérdida de Paquetes	Paquetes Perdidos
3	Voz/Video	<0.01%	1/10,000
2	Datos Críticos (SNA)	<0.05%	1/2,000
1	Datos	<0.5%	1/200

Tabla 2.5. Pérdida de paquetes para cada Clase de Servicio.

La tabla anterior describe la Pérdida de Paquetes para cada una de las Clases de Servicio (Datos, Datos Críticos y Voz/Video).

Estos parámetros son considerando que el tamaño del paquete es de 100 bytes y que el porcentaje de ocupación en los Accesos Locales WAN sea del 75%.

2.4 Problemática en Redes Multiservicios

Existe una cantidad de parámetros de QoS que se pueden medir y controlar para determinar si el servicio que se brinda o que se recibe es el deseado, éstos son:

- Disponibilidad de la red
- Ancho de banda
- Delay
- Jitter
- Pérdida

También existen parámetros que afectan el rendimiento de la Calidad de Servicio que no se pueden medir pero que brindan mecanismos de administración de tráfico para ruteos de red y switches. Se trata de:

- Prioridad de emisión
- Prioridad de descarte

Cada uno de estos parámetros afecta las aplicaciones y la experiencia del usuario final.

Disponibilidad de la red

La disponibilidad de la red puede afectar considerablemente la Calidad de Servicio. Si la red no está disponible (aún por períodos cortos de tiempo), el usuario o la aplicación pueden experimentar un rendimiento no deseado e impredecible.

La disponibilidad de la red es la suma de la disponibilidad de muchos elementos que se usan al generar una red, como la redundancia de aparatos de la red, es decir, interfaces redundantes, tarjetas de procesador o fuentes de energía en routers y switches, protocolos de red de rápida recuperación, conectores físicos múltiples (como fuentes de energía de backup, de fibra o cobre), entre otros.

Los operadores de redes pueden aumentar la disponibilidad de la red implementando grados variables de cada uno de estos elementos. Actualmente, el desafío más grande para los operadores es brindar redes IP que puedan tener cada vez mayor disponibilidad.

Ancho de banda

El ancho de banda es uno de los parámetros más importantes en cuanto a la injerencia que puede tener en la Calidad de Servicio. La asignación del ancho de banda se puede subdividir en dos tipos: ancho de banda disponible y ancho de banda garantizado.

Ancho de banda disponible

Muchos operadores de red venden suscripciones en exceso para maximizar el retorno de la inversión en la infraestructura o en el alquiler del ancho de banda. Vender suscripciones en exceso significa que el ancho de banda al cual se suscribió un usuario puede no estar siempre disponible y obtener menor o mayor ancho de banda dependiendo de la cantidad de tráfico que generen otros usuarios en la red en un momento determinado.

Ancho de banda garantizado

Los operadores de red ofrecen un servicio que brinda un mínimo de ancho de banda garantizado y un mayor ancho de banda en la SLA. Como el ancho de banda está garantizado, el servicio es más costoso que el de ancho de banda disponible. El operador debe garantizar que aquellos que se suscriben al ancho de banda garantizado reciban un tratamiento preferencial con respecto a quienes están suscriptos al ancho de banda disponible. En algunos casos, el operador separa a los suscriptores en distintas redes físicas o lógicas, como VLANs, circuitos virtuales, etc. En otros casos, el servicio de ancho de banda garantizado comparte la misma infraestructura de red que el servicio de ancho de banda disponible; esto es lo que generalmente sucede cuando las conexiones de redes son costosas o el ancho de banda es contratado a través de otro proveedor de servicios. En este último caso, el operador debe priorizar el tráfico de los suscriptores de ancho de banda garantizado, de manera que en los momentos en que ocurren congestiones en la red se cumplan los SLA por sobre el mínimo garantizado. Se pueden activar ciertos mecanismos de QoS para descartar el tráfico que se encuentre por encima del ancho de banda mínimo garantizado al cual el suscriptor adhirió en la SLA.

Delay

El delay de la red se define como el tiempo de tránsito que experimenta una aplicación desde el punto de ingreso al punto de egreso en una red. Este puede causar problemas en la Calidad de Servicio en aplicaciones tales como SNA y transmisiones de fax que simplemente se retrasan y sufren condiciones de delay excesivas. Algunas aplicaciones pueden compensar ciertas cantidades de delay finitos, pero una vez que se excede cierta cantidad, la Calidad de Servicio se ve comprometida.

Por ejemplo, algunos equipos de redes pueden "imitar" una sesión SNA al brindar reconocimientos locales cuando el delay de red podría causar la suspensión de la sesión SNA. Del mismo modo, los portales VoIP y los teléfonos brindan cierta amortiguación local para compensar los retrasos en la red.

Finalmente, el delay puede ser fijo o variable.

Algunos ejemplos de delay fijo son:

- Delay en las aplicaciones, por ejemplo, el tiempo del procesamiento de codificación-decodificación de voz y el tiempo de creación de paquetes IP con el "stack" de software TCP/IP.
- Transmisión de datos (queuing delay) sobre medios de red físicos en cada salto de la red.
- Propagación del delay a lo largo de la red debido a la distancia de transmisión.

Con respecto al delay variable, algunos ejemplos son:

- Delay de ingreso para el tráfico que entra en un nodo de la red.

- Competencia con otro tráfico en cada nodo de la red.
- Delay de egreso para el tráfico que sale a través de un nodo de la red.

Algunas aplicaciones pueden compensar ciertas cantidades de delay finitos, pero una vez que se excede cierta cantidad, la Calidad de Servicio se ve comprometida.

Jitter

El jitter es la medida de variación de delay entre paquetes consecutivos en un determinado flujo de tráfico. Genera un efecto importante sobre las aplicaciones sensibles al delay en tiempo real, como voz y video, que deben recibir paquetes en una tasa relativamente constante, con un delay fijo entre los paquetes consecutivos. A medida que varía la tasa de delay, el jitter impacta sobre el rendimiento de la aplicación. Una cantidad mínima de jitter puede ser aceptable, pero a medida que éste se incrementa, esa aplicación puede terminar siendo inútil.

Algunas aplicaciones, como portales de voz y teléfonos IP, pueden compensar una cantidad finita de jitter; pero como las aplicaciones de voz necesitan que el audio trabaje a una tasa constante, si el próximo paquete no llega dentro del tiempo de playback, la aplicación volverá a reproducir el paquete de voz anterior hasta que llegue el próximo paquete de voz. Sin embargo, si el paquete siguiente se retrasa demasiado, simplemente se descarta al llegar, lo cual implica una menor cantidad de audio distorsionado.

Todas las redes presentan cierta cantidad de jitter debido a la variabilidad de delay que presenta cada nodo de la red mientras llegan los paquetes. De todos modos, siempre que el jitter esté controlado, se puede mantener la Calidad de Servicio.

Pérdida

La pérdida puede ocurrir debido a errores provenientes del medio de transmisión físico. Por ejemplo, la mayoría de las conexiones inalámbricas tiene muy baja pérdida al ser medida con la Tasa de Error de Bits (BER, Bit Error Rate). Sin embargo, otras conexiones inalámbricas, como satélites y redes inalámbricas fijas o móviles, tienen una tasa de error que varía de acuerdo a las condiciones ambientales o geográficas (neblina, lluvia, interferencias RF, etc.) y los obstáculos físicos (árboles, edificios, montañas, etc.). Las tecnologías inalámbricas con frecuencia transmiten información redundante, ya que los paquetes terminarán cayéndose en algún momento debido a la naturaleza del medio de transmisión.

La pérdida también puede producirse cuando los nódulos congestionados de la red dejan caer los paquetes. Algunos protocolos de redes, como TCP, brindan protección de caída de paquetes al retransmitir los paquetes que pueden haber caído o que pueden haber sido corrompidos por la red. A medida que la red se congestiona más, caen más paquetes y hay más retransmisiones de tipo TCP. Si la congestión continúa, el rendimiento de red disminuirá considerablemente, ya que se utilizará gran parte del ancho de banda para la retransmisión de paquetes caídos. Finalmente, el TCP reducirá el tamaño de la ventana de transmisión para que se transmitan paquetes cada vez más pequeños, la congestión disminuirá y habrá menor cantidad de paquetes caídos.

Debido a que la congestión tiene un impacto directo sobre la pérdida de paquetes, se suelen desplegar mecanismos de evasión de congestión. Uno de ellos es RED (Random Early Discard), cuyos algoritmos dejan caer paquetes al azar pero intencionalmente una vez que el tráfico traspasa uno o más de los límites de congestión configurados. RED aprovecha el mecanismo de obturación del tamaño de la ventana del protocolo TCP y brinda una administración de la congestión más

eficiente para los flujos basados en TCP (el control de congestión que ofrece este mecanismo sólo es eficiente para aplicaciones o protocolos con mecanismos de obturación tipo TCP).

Prioridades de emisión

Las prioridades de emisión determinan el orden en que el tráfico es enviado a medida que sale de un nodo de la red y la cantidad de latencia que el mecanismo de espera de los nodos de red inserta en el tráfico.

Por ejemplo, las aplicaciones que toleran delay, como el correo electrónico, están configuradas para tener una emisión de prioridad más baja que las aplicaciones en tiempo real sensibles al delay, como las de voz o video. Estas aplicaciones que toleran el delay pueden ser amortiguadas mientras se transmiten aplicaciones sensibles al delay.

En su forma más simple, las emisiones de prioridad usan un esquema de transmisión de prioridades. El inconveniente de esto es que los datos con baja prioridad de transmisión tal vez nunca obtengan servicio si siempre hay tráfico con alta prioridad de emisión, pero sin límite de tasa de ancho de banda.

Un esquema más complejo brinda un programa balanceado para la transmisión de tráfico que mejora la imparcialidad. Es decir, el tráfico de baja prioridad de emisión no debe esperar hasta que se transmita el tráfico con mayor prioridad de transmisión. Finalmente, algunos esquemas de prioridad de transmisión brindan una mezcla de programas de prioridad y balanceo.

Prioridades de descarte

Las prioridades de descarte se utilizan para determinar el orden en que se descarta el tráfico, que puede caer debido a la congestión en los nodos de la red o por encontrarse fuera de perfil (es decir, el tráfico excede la cantidad preestablecida de ancho de banda para determinado período de tiempo).

Cuando hay congestión, el tráfico con mayor prioridad de descarte cae antes que el tráfico con menor prioridad de descarte. Esto permite que el tráfico tenga el mismo rendimiento cuando los nodos de la red no están congestionados. Sin embargo, cuando los nodos se encuentran congestionados, la prioridad de descarte se usa para descartar el tráfico preferencial primero.

La prioridad de descarte también permite que los distintos tráficos de la misma prioridad de emisión sean descartados cuando el tráfico se encuentre fuera de perfil. Sin estas prioridades de descarte, el tráfico necesitaría ser separado en distintas hileras en el nodo de red para brindar diferenciación de servicio.

2.5 Necesidad por Calidad de Servicio (QoS)

La actual demanda de aplicaciones relacionadas con información multimedia, como son la video-conferencia, audio-conferencia, video bajo demanda (VoD) o sistemas cooperativos (pizarras compartidas, tele trabajo, telemedicina, etc.) y su coexistencia con aplicaciones más clásicas (bases de datos, transferencias de ficheros, WWW, etc.), requieren tecnologías de comunicaciones capaces de ofrecer elevadas prestaciones.

Hace pocos años, debido básicamente a la baja capacidad de las redes, la posibilidad de llevar a cabo cualquiera de las aplicaciones referenciadas anteriormente era prácticamente impensable, pero en estos momentos es una realidad. Se ha avanzado mucho en compresión de audio y vídeo, y en tecnologías de redes. Aún así, quizás el mayor avance haya sido el auge de Internet y la capacidad de conectarse desde casa utilizando únicamente un ordenador personal y un módem.

Afortunadamente, en la actualidad se están implantando nuevas tecnologías de fibra óptica que proporcionan el gran ancho de banda requerido por las aplicaciones anteriores, pero no basta solo con el aumento del mismo, es necesario gestionarlo de manera eficiente: utilizarlo en un porcentaje elevado asegurando una calidad determinada. Esto es lo que se conoce como calidad de servicio (QoS).

Hasta hace poco este término no era importante en la mayoría de los sistemas. Para comprobarlo tan solo tenemos que pensar en los algoritmos que se usan actualmente en la transmisión de paquetes por la red (pensar en el sistema Best Effort utilizado en Internet), estos algoritmos suelen garantizar la llegada de todos los paquetes, pero no dan ninguna cota respecto al límite de su llegada a destino. Esta forma de transmisión es buena para muchas aplicaciones, como por ejemplo la transmisión de ficheros (FTP), la navegación por el Web, el correo electrónico, donde lo importante es que los datos lleguen correctamente. Para el tráfico en tiempo real, en cambio, los datos necesitan llegar a su destino en un tiempo determinado, ya que tardar un poco más implica que la aplicación se detendría por falta de datos, lo cual sería inadmisible.

La mayoría de las redes de ordenadores, a excepción de ATM, no han sido diseñadas para proporcionar implícitamente unos niveles de calidad de servicio necesarios para la transmisión del tráfico multimedia, IP y Ethernet ofrecen un servicio Best Effort (mejor esfuerzo) inadecuado para la excesiva carga de las aplicaciones actuales, por lo tanto para poder soportar este tipo de tráfico es necesario crear diferentes protocolos, así como una serie de políticas para la gestión de los diferentes recursos de la red, intentando obtener una calidad de servicio extremo a extremo y garantizando la compatibilidad de las distintas técnicas a causa de la heterogeneidad de las redes.

Beneficios al aplicar QoS

Ventajas para las aplicaciones

Hoy en día, todas las empresas están considerando Internet como una nueva vía para incrementar su negocio y, en consecuencia, 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 permiten el comercio electrónico con los socios del negocio. Es evidente, por tanto, que se está incrementando 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 y con unas garantías determinadas.

Beneficios para las empresas

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 del IP 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.
- El control de pérdidas en los momentos en los que la congestión sea inevitable.

Beneficios para los proveedores de servicio

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 servicio (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).

2.6 Definición de Calidad de Servicio (QoS)

La calidad de servicio (QoS) es el rendimiento de extremo a extremo de los servicios electrónicos tal y como se observan por un usuario final. Los parámetros QoS son: el retardo, la variación del retardo y la pérdida.

La calidad de servicio (QoS) puede definirse como el rendimiento de los servicios observados por el usuario final. Una red debe garantizar que puede ofrecer un cierto nivel de calidad de servicio para un nivel de tráfico que sigue un conjunto especificado de parámetros. En su conjunto, esas condiciones forman un contrato de tráfico entre el usuario y la red.

Las siguientes definiciones son importantes para comprender cuando se habla de calidad de servicio:

- La clase de servicio (CS) define un conjunto preciso de parámetros cuando se ofrece un servicio.
- El nivel acordado de servicios (*Service Level Agreement*: SLA) establece la calidad de servicio pactada mediante un contrato.

El concepto de calidad de servicio se originó en las técnicas y estándares de redes, pero también puede extenderse al Web, las aplicaciones y los servidores de contenido para administrar las clases de servicio a lo largo de todos los recursos de transmisión y procesamiento que forman la infraestructura de Internet. Las computadoras locales y remotas también pueden administrarse con calidad de servicio para optimizar las tareas de procesamiento de aplicaciones en Internet (siguiendo el nivel acordado de servicios bajo una verdadera arquitectura distribuida). Deben establecerse protocolos qos eficientes entre las redes y los servidores para administrar la red y las computadoras, según lo establece el nivel acordado de servicios, adaptándose a las condiciones reales de la red y los servidores, que cambian a cada momento.

Las redes pueden introducir retardos, pérdida de paquetes o errores debido a problemas de multiplexaje, conmutación o transmisión en nodos congestionados, impactando entonces la calidad

del servicio. Cuando se maneja asignación de recursos de voz, datos y video, las condiciones de la red se tensan al máximo para poder garantizar el desempeño de los servicios múltiples. La calidad de servicio se definió inicialmente en los protocolos de comunicaciones ATM y luego evolucionó al protocolo IP para disponer de las herramientas para manejar la infraestructura de las redes de nueva generación (NGN).

Las computadoras existentes en Internet pueden presentar problemas de sobrecarga en el procesador, la memoria y los dispositivos de E/S, lo cual disminuye la calidad de servicio. Las aplicaciones deben considerar redundancia, balanceo de cargas y prioridades de asignación de recursos a lo largo de todos los elementos de cómputo disponibles. Las tecnologías qos son bastante nuevas en la industria de las computadoras, especialmente cuando se establecen protocolos entre redes y procesadores distribuidos.

El acceso y la seguridad son dos componentes centrales de las tecnologías aplicadas a los servicios corporativos distribuidos mediante Internet, así como dos tecnologías paralelas incluidas en una solución QoS. De hecho, el acceso, la seguridad y los protocolos QoS deben interoperar en forma natural con los entornos privados virtuales (VPE) para conformar aplicaciones tipo QoS a lo largo de la red y los servidores. Los recursos de las computadoras y la red pueden programarse para diferenciar los servicios por usuario y por aplicación. Se pueden definir clases de servicio para cada usuario y aplicación que se ejecute en Internet (hasta llegar al nivel de las funciones específicas o los componentes de cada aplicación). Promediando los parámetros de la clase de servicio empleados por los usuarios y sus aplicaciones, cada paquete IP puede ser procesado en forma diferente, de modo tal que se puede disponer de los recursos de la infraestructura de acuerdo con el nivel de servicios pactado.

Aun cuando los costos del ancho de banda se reducen en algunos países, las aplicaciones de nueva generación (NGA) requieren cada vez más recursos de Internet. A medida que la infraestructura cambia con rapidez en todo el mundo, las empresas requieren la calidad de servicio no sólo para garantizar la entrega eficiente y económica de las aplicaciones en Internet, sino también para programar la asignación de los recursos de cómputo y red y aplicar las políticas corporativas. Cuando los recursos de Internet se administran mediante la calidad de servicio, la frase "la computadora es la red" se vuelve real. Internet se ha hecho tan grande que requiere de mejores herramientas para administrarla.

Las tecnologías QoS permiten recuperar el mismo control que existía en los entornos centrados en las aplicaciones, como en los mainframes (como si todo se estuviera procesando en una sola computadora).

3 Calidad de Servicio en redes multiservicios

3.1 Calidad de Servicio en redes LAN

3.1.1 802.1p

Mediante la norma 802.1p es posible conseguir calidad de servicio en redes 802. A continuación revisaremos los parámetros de QoS que proporcionan estas redes y la división en varias clases de servicio y su asociación a los distintos tipos de tráfico para asegurar niveles de prioridad.

Parámetros de QoS

Las redes de área local no garantizan la mayoría de los parámetros necesarios para la obtención de QoS, tal y como se definen a continuación:

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 puente puede aumentar o bajar la disponibilidad del servicio. Aumenta evitando en el camino de datos aquellos componentes de la red que estén fallando. Disminuye si falla el puente, si el puente deniega el servicio o debido al filtrado de tramas de los puentes.

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 puente 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. Las primitivas MA_UNITDATA.indication que se corresponde a MA_UNITDATA.request, con la misma prioridad y para la misma combinación dirección fuente y destino, son recibidas en el mismo orden que las .request.

Duplicación de trama

MAC no permite duplicar tramas. Los puentes 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 retardo de tránsito de trama es el tiempo transcurrido entre una primitiva MA_UNITDATA.request y la correspondiente MA_UNITDATA.indication. Su valor se calcula sobre las unidades de datos transmitidas con éxito.

También existe el retardo introducido por un determinado puente: 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 puentes pueden optar por descartar tramas, asegurando así un retardo máximo en cada puente.

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 estamos ante distintos métodos.

Tamaño máximo de la unidad de datos de servicio

El tamaño máximo de esta unidad de datos varia con el método MAC utilizado. Hay que tener en cuenta que el valor máximo soportado por dos LANs 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. Una primitiva de request con mayor prioridad tendrá preferencia sobre otra realizada desde la misma estación o desde cualquier otra estación de la misma LAN.

La subcapa MAC mapea las prioridades de usuario solicitadas sobre las prioridades de acceso soportadas por cada una de las métodos individuales MAC utilizados.

Una utilidad es la posibilidad de gestionar el retardo de transmisión de una trama en un puente, asociándole una *user_priority* (prioridad de usuario) a la misma. Este tipo de retardo comprende:

- Retardo en la cola de almacenamiento hasta que la trama logra situarse en primera línea de transmisión sobre el puerto. Este tipo de retardos se gestionan utilizando user_priority.
- Retardo de acceso, para la transmisión de la trama. Se usará *user_priority* en aquellas tecnologías que soporten más de una prioridad de acceso.

La prioridad va a poder ser asignada por el usuario en base a la dirección destino, el puerto de entrada, el puerto de salida, la prioridad de acceso o por VLAN.

Rendimiento

Una red LAN construida con puentes incrementa significativamente el rendimiento en comparación con cualquier simple red de área local, debido a las características de estos elementos anteriormente citadas, entre ellas porque los puentes pueden localizar el tráfico dentro de las redes LANs a través del filtrado de tramas.

Primitivas de Servicio

Hemos hablado anteriormente de varios campos necesarios para asociar prioridades, veamos pues su significado y ubicación.

1) Primitiva **M_UNITDATA.indication** {
frame_type,
mac_action,
destination_address,
source_address,
mac_service_data_unit,
user_priority,
frame_check_sequence
}

El significado de los campos es:

- *Frame_type*: tipo de trama (de usuario, mac o reservada)
- *Mac_action*: la acción a ejecutar tras el tipo de trama. Ej. si el tipo de trama es de datos de usuario, las acciones que se podrían realizar son petición de respuesta o sin respuesta.
- *Destination_address*: dirección destino individual o de grupo.
- *Source_address:* dirección MAC origen.
- *Mac_service_data_unit*: datos de usuario.
- *User_priority*: prioridad solicitada por el usuario de servicio. Su valor está en el rango de 0 a 7, siendo el 7 el valor máximo. Los puentes tienen la capacidad de cambiar su valor, almacenado en una tabla de prioridades por cada uno de los puertos. Posteriormente

veremos las clases de servicio existentes y cómo asociarlas según el tipo de tráfico que circula por la red.

- *Frame_check_sequence (FCS):* para controlar la emisión de parejas de primitivas .indication - .request., protegiéndose así de posibles errores no detectados para tramas que ya han sido transmitidas.

2) Primitiva **M_UNITDATA.request** {
frame_type,
mac_action,
destination_address,
source_address,
mac_service_data_unit,
user_priority,
access_priority,
frame_check_sequence
}

Esta primitiva introduce , respecto a la anterior, el campo *access_priority* para indicar la prioridad de salida de la trama. Depende del tipo de método MAC utilizado y su valor debe estar basado en el valor user_priority.

La siguiente tabla muestra las relaciones para algunas redes LAN :

User_priority	Prioridad de acceso de salida según método MAC utilizado				
	802.3 (Ethernet)	8802-4 (Token b.)	8802-5 (Token R.)	8802-6 (DQBD)	FDI
0	0	0	0	0	0
1	0	1	1	1	1
2	0	2	2	2	2
3	0	3	3	3	3
4	0	4	4	4	4
5	0	5	5	5	5
6	0	6	6	6	6
7	0	7	6	7	6

Tabla 3.1. Valor de User_priority según método MAC utilizado.

Como vemos, para el caso de una Ethernet la prioridad de salida de la trama basada en el campo access_priority va a ser siempre la mínima (0), independientemente de que la prioridad de usuario sea mayor.

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 puente, 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 Ethernet. En la siguiente tabla se pueden observar las prioridades:

Prioridad de usuario	Prioridad de usuario por defecto	Rango
0	0	0-7
1	1	0-7
2	2	0-7
3	3	0-7
4	4	0-7
5	5	0-7
6	6	0-7
7	7	0-7

Tabla 3.2. Prioridades de Usuario.

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 para el tráfico unicast y en base al campo user_priority y la dirección destino para tramas multicast.

Una vez determinadas las clases de tráfico por puente, 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 best effort es más que suficiente.

El tráfico podría subdividirse en los siguientes grupos:

- Control de red (máxima importancia)
- Voice : retardo < 10 msg
- Vídeo : retardo < 100 msg
- Carga Controlada (algunas aplicaciones importantes)
- Excellent Effort (como best effort para usuarios importantes)
- Best Effort (prioridad por defecto en la LAN)
- Background (juegos, etc.)

La siguiente tabla muestra cómo se podría asociar el campo user_priority al 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 ms latencia y jitter
6	Voz interactiva < 10 ms latencia y jitter
7	Control de red

Tabla 3.3. Asociación de Prioridad de usuario y Tráfico.

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, tal y como muestra la tabla 3.4.

Una vez establecidas todas estas asociaciones nos preguntamos cómo utiliza esta información del puente. El puente, 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 antes descrita, enviando así el tráfico considerado más prioritario.

Número de colas	Tipos de tráfico
1	{a, b, c, d, e, f ,g}
2	{a, b, c, d } {e, f , g}
3	{a, b} {c , d } {e, f , g}
4	{a , b} {c, d } {e , f } {g}
5	{a , b} {c} {d } {e, f} {g}
6	{a ,b} {c} {d} {e} {f } {g}
7	a b c d e f g

Tabla 3.4. Mapeado tipo de tráfico a Clase de tráfico.

3.1.2 802.1Q

Un método más práctico para asignar la prioridad a los paquetes es por un sistema final que asigna la prioridad dependiendo de la información del usuario o de la aplicación. El estándar definido por la IEEE para el manejo de redes virtuales (VLANs) 802.1Q extiende la capacidad del manejo de las prioridades en los puentes (nivel 2), utilizando para ello un campo de prioridad dentro del encabezamiento del VLAN tag, es decir, añade algunos bits dentro de cada paquete que identifican la VLAN a la que pertenece el paquete y la prioridad del mismo. Este tag (marca o etiqueta) es mostrado en la siguiente figura:

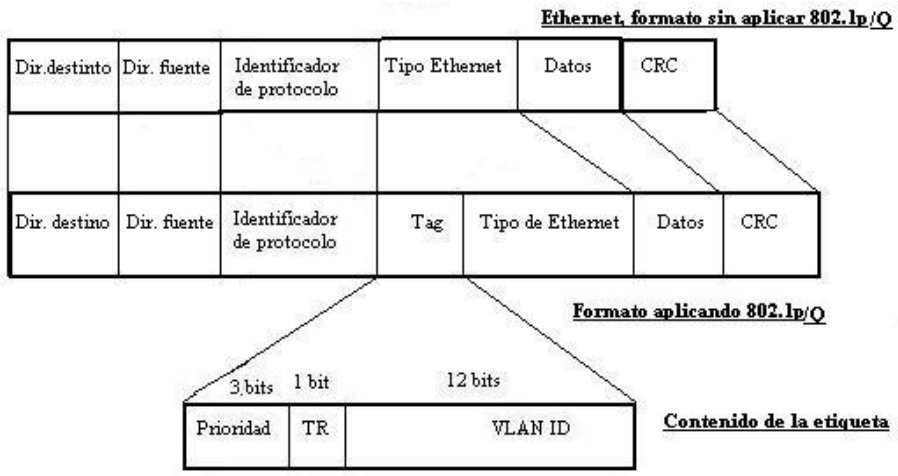

Fig. 3.1. Marca en el paquete según 802.1Q.

Como se observa en la figura, se han añadido cuatro octetos a la trama Ethernet aumentando la longitud máxima de la misma de 1518 a 1522 octetos. En estos 4 octetos, 3 dígitos binarios van a permitir asignar hasta ocho niveles de la prioridad (similares a *IP Precedence*) basándose en 802.1P y otros 12 dígitos binarios van a permitir identificar la VLAN de las 4094 posibles (802.1Q).

Además de en el nivel 2, los encaminadores y los conmutadores de nivel 3 también pueden definir el campo de protocolo de las tramas 802.1Q basados en la información de nivel 3, como la dirección IP destino, tipo de tráfico (unicast, multicast, broadcast), o dependiendo de las capacidades del conmutador de nivel 3, basados en la información de nivel 4, como el número del puerto o socket de TCP, lo que va a permitir obtener un mayor rendimiento.

Tipos de VLAN

Los miembros de una VLAN pueden clasificarse por puerto, dirección MAC y tipo de protocolo.

VLAN capa 1 : Miembros por puerto

Los miembros pueden ser definidos basándose en los puertos que pertenecen a la VLAN. La siguiente tabla muestra un ejemplo, en el que los puertos 1,2 y 4 pertenecen a una VLAN 1 y el 3 a una VLAN 2.

Puerto	VLAN
1	1
2	1
3	2
4	1

Tabla 3.5. Ejemplo VLAN por puerto.

La principal desventaja de este método es que no permite la movilidad de usuario. Si un usuario se mueve a una nueva localización lejos del puente asignado el administrador de la red tendrá que reconfigurar la VLAN.

VLAN capa 2 : Miembros por dirección MAC

Para configurar la VLAN se basa en la dirección MAC de las estaciones de trabajo. El conmutador anota las direcciones MAC pertenecientes a cada VLAN, tal y como muestra la siguiente tabla. Como la dirección MAC es proporcionada por la tarjeta de red, si un puesto es movido, no es necesaria la reconfiguración si este puesto se vuelve unir a la misma VLAN.

Dirección MAC	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1

Tabla 3.6. Ejemplo VLAN por dirección MAC

El principal problema de este método es que los miembros deben asignarse inicialmente. En redes formadas por miles de usuarios esta no es una tarea fácil. Además en entornos donde se utilizan portátiles la dirección se asocia a la estación donde éste se conecta. De esta forma, cuando un portátil se conecta desde otro lugar la VLAN debe reconfigurarse.

VLAN capa 2 : Miembros por tipo de protocolo

Para la capa 2 la VLAN también se puede basar en el campo tipo de protocolo de la cabecera, por ejemplo para IP una VLAN distinta que para IPX.

VLAN capa 3 : Miembros por dirección IP

Se basa en la cabecera de capa 3, utilizando la dirección de subred IP para clasificar a los posibles miembros de la VLAN. La siguiente tabla muestra un ejemplo de formación:

IP Subred	VLAN
172.10.10.0	1
172.10.11.0	2

Tabla 3.7. Ejemplo VLAN por Subred.

En este caso los usuarios pueden mover sus estaciones de trabajo sin tener que reconfigurar su dirección de red. El único problema es que generalmente se tarda más en enviar paquetes basándose en la información de la capa 3 que usando direcciones MAC.

VLAN's de capas superiores

Es posible definir también miembros de VLAN basándonos en aplicaciones. Por ejemplo, podría aplicarse FTP en una red VLAN y TELNET en otra.

Hay que tener en cuenta que el estándar 802.1Q define tan solo redes privadas virtuales de capas 1 y 2. No contempla las basadas en el tipo de protocolo y en capas superiores.

Tipos de conexiones

Los dispositivos de una VLAN pueden conectarse de tres maneras, teniendo en cuenta que existen dispositivos que habilitan VLAN (que son conscientes de esta) y otros que no la reconocen.

Conexión troncal

Todos los dispositivos conectados al tronco, incluidas las estaciones de trabajo, deben ser VLAN-conscientes. En este caso, las tramas incluyen en su cabecera una etiqueta que permite referenciar la VLAN.

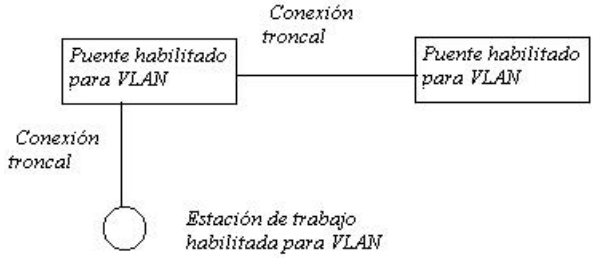

Fig. 3.2. Conexión troncal entre dos puentes VLAN-conscientes.

Enlace de acceso

Este tipo conecta dispositivos que no habilitados para VLAN con el puerto de un puente que sí la permite. Todas las tramas no están etiquetadas implícitamente. Un ejemplo de dispositivo no habilitado para VLAN puede ser un segmento LAN con estaciones de trabajo o dispositivos que no están habilitados para redes virtuales. LA siguiente figura muestra este caso:

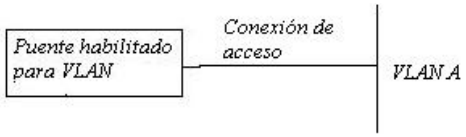

Fig. 3.3. Conexión de acceso entre un puente que permite VLAN y un dispositivo que no la permite.

Conexión híbrida

Es una combinación entre las dos anteriores. En este caso las tramas podrán estar etiquetadas o no.

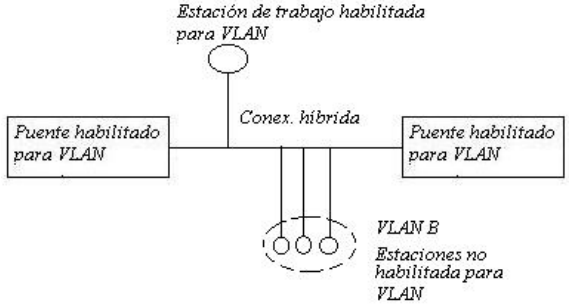

Fig. 3.4. Conexión híbrida.

Procesado de tramas

Un puente recibiendo datos determina a qué VLAN pertenece los datos estén las tramas etiquetadas de forma implícita o explícita. En la explícita se añade una cabecera de etiqueta a los datos. El puente además mantiene la información de los miembros de la VLAN a través de una base de datos de filtrado, necesaria para determinar dónde se van a enviar los datos.

A continuación se explica el contenido de la base de datos de filtrado y el formato de la etiqueta en la cabecera.

Base de datos de filtrado

Al igual que pasaba en 802.1p, en VLAN se utiliza una base de datos para almacenar información de los miembros de la VLAN. De la misma manera, esta base está formada por varias entradas:

- *Entradas estáticas.* Su información no se cambia de manera automática. Existen dos tipos: entradas de filtrado estáticas y entradas de registro estáticas. Las primeras especifican para cada puerto que tramas son enviadas a una dirección MAC o VLAN específica y cuales deben ser descartadas. El segundo tipo indica que tramas deben etiquetarse o no y que puertos pertenecen a qué VLANs.

- *Entradas dinámicas.* Se crean gracias al proceso de aprendizaje del puente, éste observa el puerto desde el que se recibe una trama con una determinada dirección fuente y un identificador VLAN (VID) y actualiza su valor en la base de datos. Existen tres tipos de entradas dinámicas: las entradas de filtrado dinámicas, las entradas de registro de grupos y las entradas de registro dinámicas. Para añadir y/o borrar entradas en el segundo grupo se utiliza el protocolo GRMP, permitiendo que el tráfico multicast sea enviado tan solo a una VLAN particular. Para el tercer grupo se utiliza el protocolo GARP VLAN (GVRP), anteriormente mencionado.

El protocolo GVRP no se utiliza únicamente para las entradas de registro dinámicas, también se utiliza para intercambiar información entre puentes que permiten VLAN.

Para enviar información al destino correcto todos los puentes deberían contener la misma información en sus respectivas bases de datos de filtrado. GVRP va a ser el protocolo que lo permita. Los puentes habilitados para VLAN registrarán y propagarán los miembros hacia todos los puertos que sean parte de la topología activa de la VLAN. Esta topología se determina en el momento en que los puentes se conectan o cuando se percibe un cambio en el estado de la topología actual. Para especificarla se utiliza el algoritmo del árbol en expansión que evita la formación de lazos en la red al desactivar puertos. Una vez que se tiene la topología de la red los puentes lo que harán será determinar una topología activa para cada VLAN, de esta manera se obtendrá una topología distinta para cada una de ellas o una común para todas. En cualquier caso, la topología VLAN será un subconjunto de la topología activa de la red. Para comprender mejor este funcionamiento ver la figura siguiente.

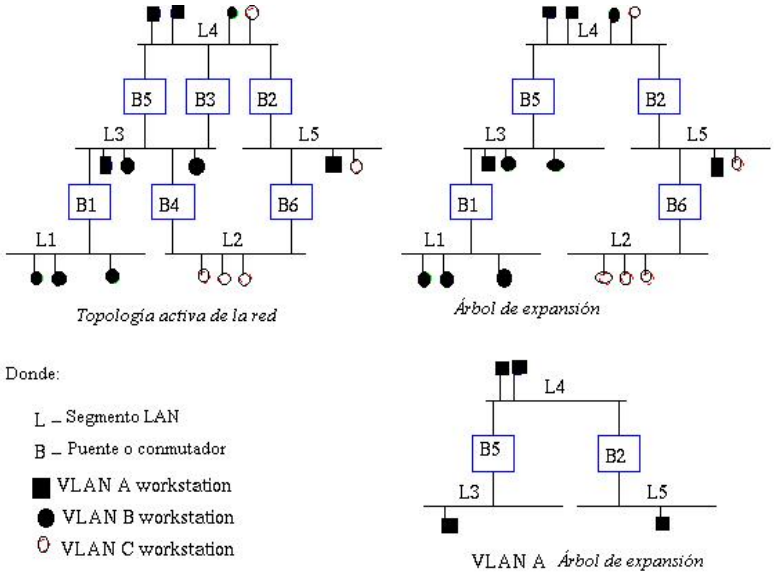

Fig. 3.5. Topología activa de toda la red y de la VLAN A utilizando "árbol de expansión".

Etiquetado

Cuando se envían las tramas a lo largo de la red es necesario indicar a que VLAN pertenece la trama para que el puente envíe las tramas únicamente a aquellos puertos que pertenezcan a la citada VLAN, en lugar de enviarla a todos los puertos (inundación). Para conseguirlo se añade una etiqueta en la cabecera, que permite especificar información de la prioridad de usuario e indicar el formato de las direcciones MAC. Aquellas tramas donde es añadida esta etiqueta se las conoce como "etiquetadas" y se envían a través de conexiones troncales e híbridas.

En el etiquetado es necesario tener en cuenta el formato de las tramas. Para el caso de 802.1Q sobre Ethernet, tal y como se indico al principio de esta cláusula, nos encontramos con los siguientes campos:

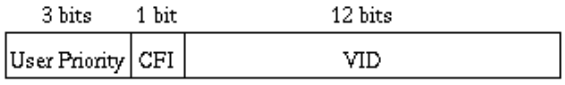

Fig. 3.6. Formato etiquetado.

Para identificar la VLAN a la que pertenece la trama existe el campo VID, existiendo como máximo (2^{12} - 1) posibles VLAN's .

Todas estas características mencionadas de forma genérica han de ser tenidas en cuenta si queremos aplicar el estándar 802.1Q en nuestra red. Para obtener una mayor información es necesario acudir a su borrador original proporcionado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).

3.2 Calidad de Servicio en redes WAN

3.2.1 ATM

Veamos como proporciona calidad de servicio el modo de transferencia asíncrono.

Control del retardo

El retardo en una red ATM es determinado por diferentes partes en la red, las cuales individualmente contribuyen al retardo total.

La información es ensamblada en celdas en el equipo terminal emisor y es desensamblada en el equipo terminal receptor. Internamente en la red, sólo existen celdas. De aquí, los parámetros que contribuyen al retardo total en la red son:

- *Retardo de transmisión (TD)*, denominado comúnmente retardo de propagación. Este retardo depende de la distancia entre los dos puntos y de la velocidad de propagación. Dependiendo del medio de transmisión empleado, el TD varía típicamente entre 4 y 5 ms por km. Este retardo es independiente del tipo de tecnología o modo de transferencia empleado.
- *Retardo de paquetización (PD)*. Este retardo es introducido cada vez que un servicio en tiempo real (tal como voz y video) es convertido en celdas y depende de la longitud del paquete y de la velocidad a la cual la fuente genera los bits.
- *Retardo de conmutación*. En un switch ATM, el retardo de conmutación está compuesto de dos partes:
  - *Retardo de conmutación fijo (FD, Fixed Switching Delay)*, que como su nombre lo indica, es un retardo fijo. Este retardo es dependiente de la implementación, y es determinado por la transferencia interna de la celda a través del hardware del switch. Este retardo es el encontrado cuando el switch se encuentra con cero carga.
  - *Retardo de la cola (QD, Queuing Delay)*, el cual es una parte variable determinada por las colas en el switch.

Parámetros del tráfico

Los parámetros del tráfico, que permiten describir las características del tráfico de una fuente, de los que proporcionaremos posteriormente una descripción más detallada. Así tenemos:

- Velocidad pico o de cresta (peak cell rate, PCR)
- Velocidad media o sostenida (sustainable cell rate, SCR)
- Longitud máxima de la ráfaga (maximum burst size, MBS)
- Velocidad mínima (minimum cell rate, MCR)

Calidad de servicio o descriptores de tráfico

Uno de los principales beneficios de las redes ATM es que pueden proveer a los usuarios con una Calidad de Servicio (QoS) garantizada. Para poder realizar esto, el usuario debe informar a la red, durante el establecimiento de la conexión, de la clase de tráfico esperada que será transmitido en la conexión y del tipo de calidad de servicio que la conexión requiere. La clase esperada de tráfico es descrita por medio de una serie de parámetros de tráfico, mientras que la calidad de servicio de la conexión es especificada por una serie de parámetros QoS. El nodo origen debe

informar a la red, durante el establecimiento de la conexión, de los parámetros de tráfico y de la deseada QoS para cada dirección de la conexión solicitada, ya que los mismos pueden ser diferentes en cada dirección de la conexión.

Para una conexión dada, los parámetros de tráfico de una fuente son agrupados en lo que se denomina descriptor del tráfico de la fuente, el cual a su vez es un componente del descriptor de tráfico de una conexión. Las redes ATM, por otro lado, también ofrecen un serie específica de categorías de servicio. El usuario debe solicitar a la red, durante el establecimiento de la conexión, una clase de servicio para esta conexión. Las categorías de servicio son empleadas para diferenciar entre diferentes tipos específicos de conexiones, en donde cada una de las mismas posee unas características de tráfico y de parámetros QoS particulares. Como resultado, se obtienen las características negociadas de una conexión, la cual constituye el contrato de tráfico.

Un descriptor del tráfico de una fuente es una agrupación de parámetros de tráfico para una conexión dada pertenecientes a una fuente ATM. Este descriptor es empleado durante el establecimiento de una conexión para capturar las características de tráfico intrínsecas de la conexión solicitada por la fuente particular.

El descriptor de tráfico de una conexión especifica las características de tráfico de una conexión. Este descriptor incluye el descriptor del tráfico de una fuente, la tolerancia a la variación de retardo de celdas (CDVT, cell delay variation tolerance) y la definición de conformidad, la cual es empleada para especificar las celdas conformes de una conexión. El descriptor del tráfico de la conexión contiene la información necesaria requerida para las pruebas de conformidad de las celdas de la conexión en la UNI.

Durante el establecimiento de la conexión, el nodo solicitante informa a la red del tipo de servicio requerido, de los parámetros de tráfico del flujo de datos en cada dirección, la CDVT (cell delay variation tolerance) y de la QoS solicitados para cada dirección. En resumen, los descriptores del tráfico de una conexión según el ATM Forum son:

- Descriptor del tráfico de la fuente
- Velocidad pico o de cresta (peak cell rate, PCR)
- Velocidad media o sostenida (sustainable cell rate, SCR)
- Longitud máxima de la ráfaga (maximum burst size, MBS)
- Velocidad mínima (minimum cell rate, MCR)
- La CDVT (cell delay variation tolerance) o tolerancia de variación del retardo de células
- Definición de conformidad, basada en una o más aplicaciones del algoritmo de tasa de células genéricas o GCRA (generic cell rate algorithm)

CDVT es un parámetro de la función de vigilancia (UPC) e indica cómo de tolerante puede ser la función de vigilancia al fenómeno de cell clumping. Es utilizado en conjunto con el monitoreo de la PCR y de la SCR para asegurar que las celdas que fueron generadas en el intervalo apropiado, pero que han sufrido de una CDV positiva, también sean vistas como conformes a los descriptores de tráfico.

Categorías de Servicio

ATM ha sido concebido como una tecnología multiservicio. Debido a la presencia de una variedad de tipos de tráfico y a la necesidad de asignar adecuadamente los recursos de la red para cada componente de tráfico, es que han sido definidas las categorías de servicio dentro de la capa ATM.

Las Categorías de Servicio permiten al usuario el seleccionar combinaciones específicas de parámetros de tráfico y de desempeño.

Funciones tales como CAC, UPC, Controles de Feedback, Asignación de Recursos, etc., disponibles dentro de los equipos ATM, son generalmente estructurados de forma diferente de acuerdo con cada Categoría de Servicio.

Las categorías de servicio ATM han sido definidas por las organizaciones de estandarización ITU-T y por el ATM Forum. La arquitectura de servicios provista en la capa ATM consiste de seis categorías de servicios, en donde cada categoría de servicio está designada para un grupo particular de aplicaciones:

- Constant Bit Rate (CBR)
- Variable Bit Rate (VBR)
- Variable Bit Rate-Real Time (rt-VBR)
- Variable Bit Rate-Non Real Time (nrt-VBR) (rt-VBR y nrt-VBR son definidas en el ATM Forum Traffic Management Specification versión 4)
- Available Bit Rate (ABR)
- Unspecified Bit Rate (UBR)
- Guaranteed Frame Rate (GFR)

Estas categorías se empleadas para diferenciar entre diferentes tipos específicos de conexiones, en donde cada una de las mismas posee unas características de tráfico y de parámetros QoS particulares. En otras palabras, para conexiones CBR solo PCR y CDVT están definidos.

En la Tabla siguiente se muestra la relación entre las categorías de servicio, las clases QoS y las clases ITU-T.

Categorías de servicio	Clases QoS	Clases ITU-T	Aplicaciones Típicas
CBR	1	A	Emulación de circuito, video con velocidad constante, ejemplo: E1, T1
VBR (equivalente a rt-VBR)	2	B	Audio y video con compresión y velocidad variable, ejemplo: JPEG
VBR (equivalente a nrt-VBR)	3	C	Transferencia de datos orientado a conexión, ejemplo: Frame Relay
ABR	4	D	Tráfico LAN, IP y Emulacion LAN Transferencia de datos sin conexión, ejemplo: SMDS
UBR	0 Sin especificar	X	Transferencia no garantizada / con baja calidad
GFR	X	X	TCP/IP

Tabla 3.8. Relación entre categorías de servicio, clases QoS y clases ITU-T.

Servicio CBR

La categoría de servicio CBR es empleada por conexiones que requieren de una cantidad de ancho de banda constante (estática), la cual está continuamente disponible durante el tiempo de vida de la conexión. Esta cantidad de ancho de banda está caracterizada por el valor PCR. La red garantiza una velocidad de celda de cresta (PCR), la cual es la máxima velocidad de datos que la conexión ATM puede soportar sin riesgos de pérdida de celdas. La fuente puede emitir celdas a una PCR negociada, igual o menor que la misma, durante cualquier período de tiempo y duración, teniéndose el compromiso de la QoS.

Cuando una aplicación negocia la clase de servicio CBR, la misma solicita un límite en la tolerancia de la variación del retardo de la celda (CDV), la cual especifica el máximo jitter que la transmisión puede soportar y todavía mantener los datos intactos.

El servicio CBR soporta aplicaciones en tiempo real que requieren una determinada variación de retardo CTD y CDV (tales como, voz, video, emulación de circuitos), pero no necesariamente están restringidos a estas aplicaciones.

El principal compromiso que la red debe mantener es que una vez que la conexión ha sido establecida, la QoS negociada debe ser asegurada para todas las celdas conformes. Se asume que las celdas que son retardadas más allá del valor especificado por la CTD deben ser de valor muy poco significativo para la aplicación.

Servicio rt-VBR

Esta categoría de servicio soporta aplicaciones en tiempo real, que requieren un determinado retardo (CDT) y variación de retardo (CDV).

Las conexiones rt-VBR están caracterizadas en términos de una PCR, SCR y MBS. Se espera que las fuentes transmitan a una velocidad que puede variar con el tiempo. Asimismo, la fuente puede ser descrita como “bursty“.

Esta clase de servicio puede ser empleada en aplicaciones de compresión de video con velocidad variable.

Se asume que las celdas que son retardadas más allá del valor especificado por la CTD deben ser de valor muy poco significativo para la aplicación. El servicio VBR-rt puede soportar el multiplexaje estadístico de fuentes de tiempo real.

Servicio nrt-VBR

La categoría nrt-VBR soporta aplicaciones que no son en tiempo real y cuyas características de tráfico son en ráfagas. Es caracterizada por una PCR, SCR y MBS.

Para aquellas celdas que son transferidas de acuerdo al contrato de tráfico, se espera una pérdida de celdas (CLR) muy baja, pero no posee un límite de retardo asociado (CTD o CDV). El servicio VBR-nrt puede soportar el multiplexaje estadístico de conexiones.

Esta clase de servicio puede ser utilizada para el internetworking con Frame Relay, en donde la CIR (committed information rate) de las conexiones es mapeada dentro de un ancho de banda garantizado por la red ATM.

Servicio ABR

Está diseñada para soportar aplicaciones que no pueden caracterizar efectivamente su comportamiento de tráfico durante el establecimiento de la conexión, pero que pueden adaptar su tráfico, bien sea incrementando o reduciendo su velocidad de transmisión. Para esto ABR emplea un mecanismo de control de flujo el cual soporta diversos tipos de feedback para controlar la velocidad de la fuente en respuesta a cambios en las características de transferencia de la capa ATM. Este feedback es transmitido hacia la fuente a través de celdas de control específicas llamadas Resource Management Cells (RM-cells). Aunque ningún parámetro QoS especifico es negociado, se espera que los sistemas finales, los cuales adaptan su tráfico de acuerdo con el feedback, experimentarán una relación de pérdidas de celdas (CLR) baja y podrán compartir equitativamente el ancho de banda disponible de acuerdo con normas o criterios de asignación específicos de la red. La categoría de servicio ABR no está planificada para soportar aplicaciones en tiempo real, por lo tanto, no requieren un determinado retardo (CTD) o variación de retardo (CDV). A pesar de que Cell Delay Variation (CDV) no es controlado en este servicio, las celdas admitidas no son retardadas innecesariamente.

El sistema final, durante el establecimiento de la conexión ABR, debe especificar a la red dos valores:

- El máximo ancho de banda requerido, denominado PCR.
- El mínimo ancho de banda a utilizar, denominado MCR. MCR puede ser cero.

ABR esta diseñado para mapear los protocolos LAN existentes, los cuales emplean tanto ancho de banda como sea disponible desde la red, el cual puede ser retrocedido o almacenado en buffer en presencia de congestión. Debido a esto ABR es ideal para el tráfico LAN a través de redes ATM.

Servicio UBR

La categoría de servicio UBR soporta aplicaciones que no son críticas, que no son en tiempo real, y que por lo tanto, no requieren un determinado retardo o variación de retardo. Ejemplo de tales aplicaciones son aplicaciones tradicionales de comunicación entre computadores, tales como file transfer o e-mail. El servicio UBR soporta un alto grado de multiplexaje estadístico entre fuentes.

UBR no ofrece ningún servicio garantizado. No existe ningún compromiso numérico en cuanto a garantía en pérdida de celdas (CLR) o la existencia de un límite superior de retardo (CTD), por lo tanto, no requiere de ningún conocimiento previo sobre las características del tráfico. Una red puedo o no aplicar la PCR a las funciones CAC y UPC. En el caso en que la red no haga cumplir la PCR, el valor PCR es sólo para información. Cuando la PCR no se hace cumplir, es todavía de ayuda el negociar la PCR, ya que esto le permite a la fuente el descubrir la limitación de ancho de banda más pequeña en el camino de la conexión. El control de congestión en UBR puede ser realizado en capas superiores o empleando una base extremo a extremo.

El servicio UBR es indicado por el Indicador “Best Effort“ en el elemento de información “ATM user cell rate“.

El usuario tiene la libertad de enviar cualquier cantidad de datos hasta un cierto máximo especificado. La red, por el otro lado, no hace ninguna garantía en relación con la velocidad de pérdida de celdas, retardo y variación de retardo que los datos puedan experimentar.

UBR no dispone de ningún mecanismo de control de flujo para controlar o limitar la congestión y sólo está presente la notificación de congestión, la cual puede ser empleada por los sistemas finales para adaptarse al estado de congestión de la red. Es por esto que es conveniente que los

switches ATM soporten tamaños de buffers adecuados para minimizar la probabilidad de pérdida de celda cuando múltiples ráfagas prolongadas de datos son recibidas al mismo tiempo en el switch o implementen mecanismos de control, tales como el uso del EFCI bit (explicit forward congestion indication bit). Sin embargo, tal y como está especificado en el ATM Forum, el uso del bit EFCI es opcional para los sistemas finales, por lo tanto, la red no debe confiar en este mecanismo de control de congestión.

Servicio GFR

El servicio de Trama Garantizada (ATM Guaranteed Frame Rate (GFR)) ha sido creado para mejorar el tráfico best effort (mejor servicio) en un mínimo de garantías de rendimiento. Los dispositivos de los bordes de la red que conectan redes LANs con una red ATM pueden usar este servicio GFR para transportas múltiples conexiones TCP/IP sobre un simple circuito virtual GFR. Estos dispositivos multiplexarán normalmente los circuitos virtuales dentro de una sola cola FIFO. Se ha demostrado que este tipo de cola no es suficiente para proporcionar unas mínimas garantías, por lo que el encolado vía circuito virtual con GFR es necesario.

Este servicio ha sido propuesto recientemente por ATM para mejorar el servicio UBR GFR, tal y como se ha mencionado, proporciona un mínimo de tasa de garantías al circuito virtual a nivel de trama, permitiendo además el uso de ancho de banda extra de la red y es usado por aquellas aplicaciones que no pueden cumplir los requerimientos de VBR ni tienen la capacidad de ABR.

La Tabla siguiente provee una lista de los atributos ATM (parámetros de tráfico, parámetros QoS y características de feedback) para algunas de las categorías de servicio expuestas e indica si éstos son soportados o no para cada una de las categorías de servicio.

Atributo	Categorías de servicio de la capa ATM					Tipo de parámetro
	CBR	Rt-VBR	Nrt-VBR	ABR	UBR	
CLR	✔	✔	✔	n.e.	n.e.	QoS
MaxCTD	✔	✔	n.e.	n.e.	n.e.	QoS
Pico a pico CDV	✔	✔	n.e.	n.e.	n.e.	QoS
PCR y CDVT	✔	✔	✔			Tráfico
SCR,MBS,CDVT	n.a.	✔	✔	n.a.	n.a.	Tráfico
MCR + parámetros de comportamiento	n.a.	n.a.	n.a.	✔	n.a.	Tráfico
Control de congestión (feedback)	n.a.	n.a.	n.a.	✔	n.a.	
Garantía de BW	✔	✔	✔	✔	n.a.	

Tabla 3.9. Categorías de servicio y los parámetros aplicables. En donde: n.a.: no aplicable y n.e.: no especificado

Clase de servicio	Garantía de ancho de banda	Garantía de variación de retardo	Garantía de caudal de tráfico (throughput)
CBR	Si	Si	Si
VBR	Si	Si	Si
UBR	No	No	No
ABR	Si	No	Si

Tabla 3.10. Clases de Servicio ATM Forum.

Mecanismos de control

Para proporcionar un sistema de calidad es necesario utilizar una serie de mecanismos que permitan controlar la red. Dichos mecanismos que se aplican en ATM son:

Control de Admisión de Conexión (CAC)

El control de admisión de conexión o CAC representa una serie de acciones tomadas por la red durante la fase de establecimiento (call set-up) de un SVC, durante el establecimiento de un PVC o durante la fase de renegociación de alguno de éstos con la finalidad de:

- Aceptar o rechazar una nueva conexión VCC (PVC o SVC)
- Cambiar la categoría de servicio o descriptores de tráfico de un VCC existente.

La aceptación de la solicitud de una conexión para una nueva llamada se realiza sólo cuando están disponibles suficientes recursos para llevar esta conexión a través de toda la red con la calidad de servicio (QoS) solicitada por la misma y cuando al mismo tiempo es posible mantener las QoS de las conexiones ya existentes en la red (esto se aplica también durante la renegociación de los parámetros dentro de una llamada). Si no es posible que la conexión reciba estos recursos, la red ATM no aceptará dicha conexión. CAC debe tomar en cuenta cada recurso compartido de todos los componentes de la red, en donde un recurso compartido puede ser, por ejemplo, la cola de celdas (cell queue) y su enlace de transmisión correspondiente. En otras palabras, CAC al rechazar conexiones o cambios en configuraciones que pueden producir congestión, asegura que la garantía de la pérdida de celdas (CLR) y el retardo de celdas (CTD) fijados para una conexión sean cumplidos.

Durante el establecimiento de la llamada una serie de informaciones, establecidas en un contrato de tráfico, deben ser negociadas y acordadas entre el usuario y la red para permitir que el CAC tome las decisiones adecuadas en cuanto a la aceptación/rechazo de la conexión.

Para cada solicitud (request) de un VCC, CAC emplea la siguiente información para poder tomar la decisión de admisión/rechazo:

- La QoS solicitada.
- Los valores de los parámetros en el descriptor de tráfico del VCC.
- La definición de conformidad UPC solicitada.
- Las rutas.
- El factor de reservación (booking), de existir.

La función CAC es responsable de la asignación de recursos de red para una conexión dada. Según los estándares, estos esquemas son específicos del operador de la red.

La función CAC asigna una ancho de banda a cada conexión y limita la asignación del ancho de banda total a la capacidad de cada recurso (por ejemplo a la velocidad del enlace).

La cantidad de recursos de red que una conexión requiere puede ser representada en términos de un Ancho de Banda Virtual VBW (también denominado ancho de banda equivalente) mediante el empleo de los descriptores de tráfico específicos de específicos de la conexión. El ancho de banda virtual representa la cantidad de ancho de banda empleada por la conexión una vez incluido los requerimientos de la QoS (principalmente CLR) y el tamaño del buffer.

La función CAC más simple asigna un ancho de banda virtual equivalente a la PCR para cada conexión. En el caso VBR, puede existir una asignación estadística del ancho de banda en el caso en que el parámetro SCR sea tomado en consideración.

El cálculo del ancho de banda virtual es muy complejo y requiere de grandes suposiciones del comportamiento del tráfico. Continuas investigaciones son realizadas en este aspecto con la finalidad de encontrar el modelo con la mayor precisión que refleje los requerimientos de ancho de banda de cada tipo de comportamiento de tráfico. En la Tabla siguiente se muestra una estrategia comúnmente empleada para la asignación del ancho de banda para cada una de las categorías de servicio.

Categoría de Servicio	Ancho de Banda asignado
Constant Bit Rate (CBR)	$PCR \leq V_{BW} \leq$ Link Rate
Variable Bit Rate (VBR)	$SCR \leq V_{BW} \leq PCR$
Available Bit Rate (ABR)	$MCR \leq V_{BW} \leq PCR$
Unspecified Bit Rate (UBR)	No se le asigna V_{BW}

Tabla 3.11. Asignación del ancho de banda según la categoría de servicio.

Conformado del tráfico (Traffic Shaping)

Traffic shaping es un mecanismo que altera las características de tráfico del flujo de celdas de una conexión para alcanzar una mejor eficiencia en la red mientras se mantienen los objetivos QoS o con la finalidad de asegurar que el flujo de celdas sea conforme con los parámetros de tráfico de acuerdo con la configuración del algoritmo leaky bucket del contrato de tráfico. El traffic shaping puede ser empleado, por ejemplo, para reducir la velocidad pico, limitar la longitud de la ráfaga o reducir la CDV por medio del espaciamiento adecuado de las celdas en el tiempo. El uso y ubicación de esta función es específica de la red.

El contrato de tráfico entre el cliente y la red especifica las características negociadas de una conexión. Este contrato puede consistir de:

- El descriptor de tráfico de una conexión.
- Una serie de parámetros QoS para cada dirección de la conexión.
- La definición de cumplimiento de la conexión.

La definición exacta del cumplimiento no está definida en los estándares, es decir, es dependiente de la red. La red, basada en acciones de la función UPC, puede decidir si una conexión es conforme o no. En el caso de que la conexión es conforme, la red debe soportar la QoS para todas las conexiones conformes.

Control de prioridad de pérdida de celda

Cuando las celdas son conmutadas a través de una red ATM, se van formando colas como una consecuencia natural de los retardos de propagación (demasiadas celdas a ser transmitidas por un enlace de salida) y de los retardos de procesamiento en los nodos de la red. Las celdas en las colas deben ser colocadas en buffers hasta que puedan ser atendidas. Las redes ATM, bajo cualquier tipo de condición, deben poseer mecanismos adecuados para el servicio de los buffers en los nodos ATM. Bajo condiciones de congestión (es decir, demasiadas celdas en la red), debe existir un mecanismo de prioridad que permita remediar la situación de congestión, como por ejemplo el descarte de ciertas celdas, con la finalidad de poder servir al resto de las celdas con los adecuados parámetros QoS. Para esto se requiere de un método que permita a los nodos ATM identificar

rápidamente celdas que puedan ser descartadas de aquellas celdas que no pueden ser descartadas, a excepción de condiciones extremas de congestión. El control de prioridad es realizado a través de un bit localizado en el encabezamiento de la celda denominado bit de prioridad de la celda (CLP).

3.2.2 Frame Relay

Control de congestión

Una de las características de Frame Relay reside en su gran sensibilidad respecto a las situaciones de congestión. Frame Relay no posee mecanismos de control local del flujo. Cuando la congestión aumenta hasta alcanzar niveles considerables, el retraso de la red se incrementa en gran medida. Este inconveniente conlleva, sin embargo, una de las principales ventajas de esta tecnología, ya que agiliza y simplifica la transferencia de las tramas Frame Relay: las tramas desechables son descartadas y las válidas sólo son procesadas en orden a asegurar que el destino consiste en un identificador DLCI (Data Link Connection Identfier).

El control de congestión, por tanto, no es una función local, sino global (participan todos los sistemas).

Se puede distinguir entre:

- *Tráfico ofrecido*: Evidentemente su propio nombre indica la funcionalidad del mismo.
- *Tráfico cursado*: Si ahora nos fijamos en la gráfica siguiente, queda claro que el objetivo de la tecnología de redes será evitar entrar en la zona de congestión. Es evidente que una red congestionada es una red incapaz de proporcionar los servicios de una manera eficiente.

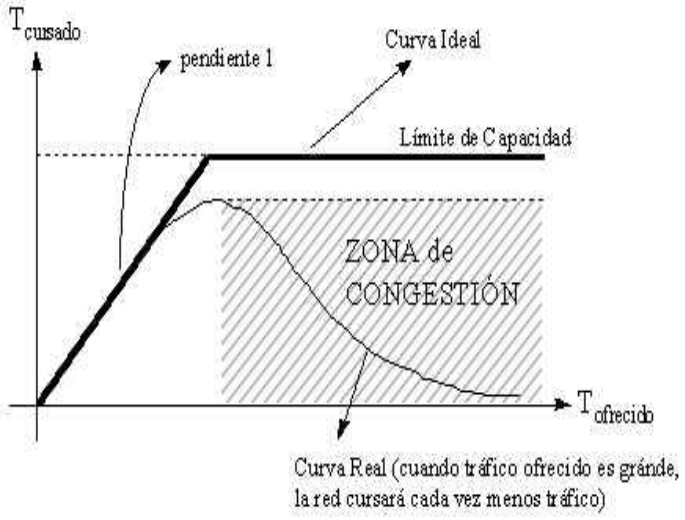

Fig. 3.7. Zona de congestión.

En redes de medio compartido, la red pierde tiempo en solucionar las colisiones.

En redes sin medio compartido, esta gráfica se debe a la limitación de la capacidad de conmutación de los nodos. Cuando a un nodo le llegan datos que no puede cursar, los descarta, quedándose sin llegar a su destino (la curva cae).

El intentar no llegar a esta Zona de Congestión, es decir, procurar que se curse la mayor cantidad de tráfico ofrecido, significa utilizar técnicas de control de congestión.

Los controles de congestión consisten en técnicas estadísticas, nunca deterministas. En Frame-Relay, esta función está implementada en parte en el Plano de Usuario.

En Frame-Relay se usa el mecanismo de *notificación y descarte*, cuyo comportamiento podría ser la siguiente:

"Cuando se detecta una zona congestionada, se notifica al usuario que envía los datos que pasan por esa parte de la red, el cual disminuye la tasa de tráfico inyectado. Si el usuario no lo hace, la red descartará los datos que considere oportuno (aceptable, ya que F-R es un servicio no fiable). Esta pérdida, si es de porcentaje elevado, provoca el cese del funcionamiento a las entidades de nivel superior, por lo que el usuario intentará evitar este tipo de situaciones".

Debemos recordar que en Frame-Relay, este descarte de tramas tiene lugar a Nivel 2.

La implementación de la técnica de *notificación y descarte* se realiza mediante los campos FECN, BECN y DE en el campo de control de la trama:

- *FECN (Forward Explicit Congestion Notification)*: Notificación de congestión en el sentido de la transmisión.
- *BECN (Backward Explicit Congestion Notification)*: Notificación de congestión en el sentido contrario a la transmisión.
- *DE (Discard Eligibility)*: Las tramas que tienen este bit a "1" son susceptibles de descarte en situaciones de congestión.

El bit BECN y el FECN se usan para avisar que hay congestión (la red los cambia de 0 a 1 y viceversa):

Hay que señalar que la congestión es unidireccional, pues puede haber caminos distintos para los dos sentidos de la transmisión y mientras uno puede estar sufriendo problemas de tráfico (congestión), el otro puede no tenerlos. Los bits FECN y BECN notifican congestión a los dos extremos de una conexión de la siguiente forma: a una trama que atraviesa una zona congestionada se le pone su bit FECN a '1'. La red identifica las tramas de esa conexión que circulan en sentido contrario y en ellas marca el bit BECN también a '1'. Es decir, la red F-R sólo notifica la congestión al origen y al destino, y del N. Superior dependerá seguir estas indicaciones (indicando al N. Superior del origen que reduzca la tasa, etc.) o no hacerlo, en cuyo caso, F-R procederá a descartar tramas.

QoS

En FR es posible contratar para cada conexión una calidad de servicio distinta. Dicha calidad está definida mediante ciertos parámetros:

CIR (Committed Information Rate) (bits/s): Es la tasa de información comprometida, es decir, el caudal medio garantizado que la red se compromete a dar en una conexión durante un intervalo de tiempo definido (Tc). Es un parámetro asociado a cada sentido de la transmisión de cada circuito virtual.

Por lo tanto se define una relación entre el tiempo real y el volumen de información transferida:

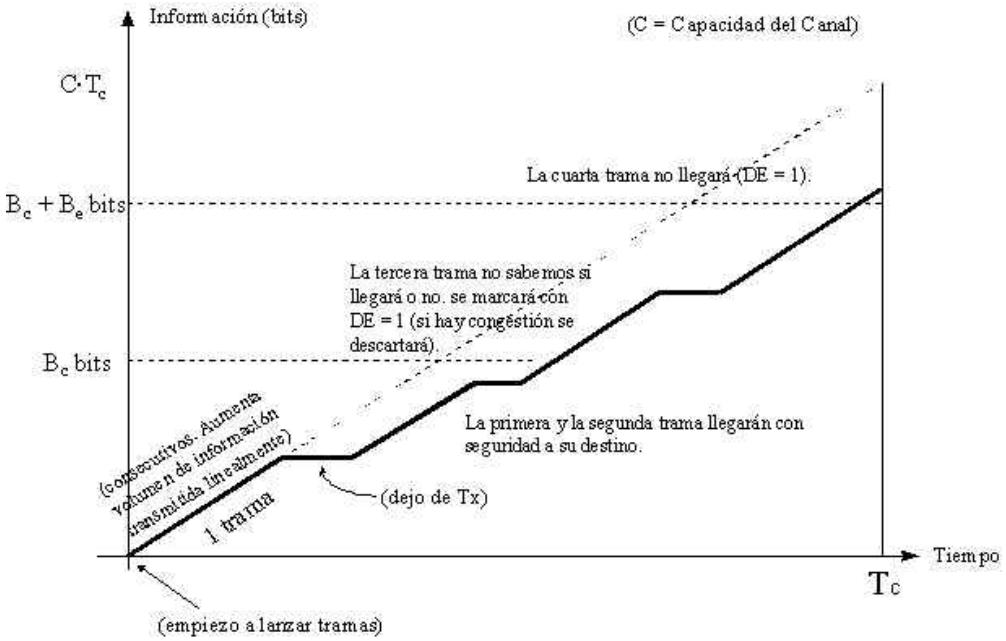

Fig. 3.8. Diagrama QoS en FR.

T_c (Commited rate measurement interval): Intervalo de observación (es el tiempo hasta el cual ha sido representado la gráfica anterior). Parámetro del algoritmo para calcular el CIR).

$C \cdot T_c$: Máximo volumen de información que se podría cursar en T_c (es lo que posibilita el canal).

El caudal físico (C) de la línea de acceso también se contrata. Así el operador dimensiona la red en función de los parámetros contratados por sus abonados.

En el interfaz usuario-red se controla, para cada circuito virtual, que los usuarios se ajusten a los parámetros Bc, y Be que han negociado. En consecuencia, si la red está bien diseñada no debe perder datos que no superen el tráfico comprometido.

Definimos dos zonas en el diagrama anterior:

B_c (Committed burst size): Es el volumen de información comprometida: durante el intervalo T_c la compañía se compromete a transmitir un volumen B_c.

B_e (Volumen de información en exceso): la información cursada durante el intervalo T_c que exceda de $B_c + B_e$ no se sabe si llegará o no a su destino (la compañía no lo garantiza). El volumen de información que exceda de $B_c + B_e$ seguro que no llegará.

Este método se aplicará para cada circuito virtual de ingreso a la red.

Existe un bit en la trama (bit DE) que es activado por la red en tramas que superen Bc (es decir aquellas que pertenezcan a Be) para indicar que esas tramas deberían ser descartadas en preferencia a otras, si es necesario. El servicio permite que el propio usuario también pueda marcar este bit para indicar la importancia relativa de una trama respecto a otras (en este caso, estas tramas no se contabilizan como pertenecientes a la zona bajo B_c, sino como perteneciente a la zona sobre B_c y bajo $B_c + B_e$, no contando para el CIR). (La mayoría de las compañías operadoras sólo definen el parámetro B_e).

El parámetro $C \cdot T_c$ está asociado a la capacidad física de las líneas, y es lo primero que contrata el abonado. Luego, sobre esa línea física, se definen mallas de circuitos virtuales, cada uno con su CIR asociado.

$$B_c = CIR \cdot T_c$$

El CIR no es la capacidad física a la que se transmite. Esa velocidad es la de la capacidad del canal. El CIR sólo es el caudal medio (estadístico).

Si el T_c se toma grande, existe la posibilidad de transmitir grandes picos de información en algunos momentos y nada de información en otros. Por tanto, un T_c pequeño nos garantiza el que la transmisión sea más homogénea (esto interesa a la empresa, ya que así se evita sobredimensionar las redes).

3.3 Calidad de Servicio en redes IP

3.3.1 Modelos de Calidad de Servicio

Las redes IP fueron diseñadas para el transporte óptimo del tráfico de datos, por lo que la Calidad de Servicio (QoS) requerida en las mismas se basó únicamente en la integridad de los datos, esto es, no pérdida de contenido y ni secuencia de los mismos. En este sentido IP fue concebido, es decir, para mover por la red, de forma óptima y segura, tráfico sin requerimientos de tiempo real. Para esto el servicio que brinda IPv4 es del tipo Best-Effort., es decir, el mejor esfuerzo.

Por otra parte, el tráfico de audio y vídeo no solo requiere ser transferido por las redes IP de forma íntegra, sino que además requiere ser transferido en el tiempo adecuado, al ritmo adecuado, en correspondencia con la cadencia que es generado. En consecuencia, la QoS en relación con el tráfico que tiene requerimientos de tiempo real necesita considerar otros parámetros de calidad, tales como la latencia (retardo y jitter) y el ancho de banda.

Dados estos requerimientos de QoS impuestos por el tráfico con características de tiempo real, como es audio y el vídeo, se necesitan mecanismos de señalización que propicien tener bajo control dichos parámetros de calidad, y dar garantía de QoS.

Un modelo de servicio, también es llamado un nivel de servicio, describe las capacidades de una QoS fija de extremo a extremo. La QoS extremo a extremo es la habilidad de la red de entregar el servicio requerido por el tráfico de la red específico de un extremo de la red a otro. El software de Cisco IOS soporta tres tipos de modelos de servicio:

1. El mejor esfuerzo (best effort)
2. Servicios integrados (Int-serv)
3. Servicios diferenciados (Diff-serv).

El mejor esfuerzo (Best Effort)

El mejor esfuerzo es un modelo de un solo servicio en que una aplicación envía los datos las veces que esta deba, en cualquier cantidad, y sin pedir el permiso o informar la red primero. Para el servicio del mejor esfuerzo, la red entrega los datos si puede, sin cualquier convicción de

fiabilidad, límites de retraso, o rendimiento. La QoS de Cisco IOS ofrecen implementar el servicio del mejor esfuerzo es el encolamiento de FIFO. El servicio del mejor esfuerzo es conveniente para una amplia variedad de aplicaciones como transferencia de archivos en general o correo electrónico (e-mail).

3.3.2 Servicios Integrados (Intserv)

Es un modelo multiservicio que puede acomodar múltiples requerimientos de QoS. Está basado en el protocolo RSVP (Resource ReSerVation Protocol, RFC 1633), implica una reserva de recursos en la red para cada flujo de información de usuario, así como el mantenimiento en la red (en los enrutadores) de un estado para cada flujo, esto es, mantenimiento de la reserva (tablas de estados de reserva). Esto conduce a un considerable tráfico de señalización y ocupación de recursos en cada enrutador para cada flujo, con la consiguiente complejidad en el hardware, al margen del aporte que esta señalización hace a la congestión de la red. No es una solución escalable, no es una solución adecuada para grandes entornos como Internet, aunque si lo es para entornos más limitados y también para redes de acceso al backbone.

RSVP es un protocolo señalización de QoS, y posibilita:

- Dar a las aplicaciones un modo uniforme para solicitar determinado nivel de QoS.
- Encontrar una forma de garantizar cierto nivel de QoS.
- Proveer autentificación.

RSVP es un protocolo que se desarrolla entre los usuarios y la red, y entre los diferentes nodos (enrutadores) de la red que soportan este protocolo. Consiste en hacer reservas de recursos en dichos nodos para cada flujo de información de usuario, con la consecuente ocupación de los mismos. Esto requiere, lógicamente, intercambio de mensajes RSVP entre dichos entes funcionales, así como mantener estados de reserva en cada nodo RSVP. De manera que tanto la solicitud de las reservas, como el mantenimiento de éstas durante la comunicación, y la posterior cancelación, implican el intercambio de mensajes de señalización, lo que representa un tráfico considerable cuando de entornos como Internet se trata.

RSVP ofrece dos tipos de servicios:

- *Servicio de carga controlada*: se entiende en general que la pérdida de paquetes debe ser muy baja o nula.
- *Servicio garantizado*: se basa en solicitar determinado ancho de banda y cierta demora de tránsito máxima.

De los dos tipos de servicios que RSVP soporta, el más adecuado para aplicaciones con requerimientos de tiempo real es el servicio garantizado, aunque es más complejo de implementar que el servicio de carga controlada.

El Protocolo RSVP define dos sentidos para la transferencia de sus mensajes de señalización, downstream y upstream. El flujo downstream se efectúa desde la fuente al receptor o receptores, y el flujo upstream en sentido contrario.

PATH y RESV son dos mensajes básicos del protocolo RSVP, y son en definitiva los mensajes a través de los cuales se lleva a cabo la reserva de recursos en la red previo a la comunicación. Los mensajes PAHT´s son generados por la fuente de mensajes de usuario necesitados de garantía de QoS, e indica las características de éstos en cuanto a recursos que necesita. La ruta que deben

seguir estos mensajes es la misma que siguen los datos de usuario, para lo cual se requiere previamente un diálogo entre el proceso RSVP y el proceso de enrutamiento, pues dicha ruta quien la determina es el protocolo de enrutamiento, de lo contrario para nada serviría RSVP.

En su paso por cada enrutador RSVP los mensajes PATH´s se actualizan y se retransmiten, consistente esto en poner la dirección IP del enrutador que lo actualiza y reenvía. Cada enrutador RSVP también almacena la dirección del enrutador anterior. Así, con los mensajes PATH´s se posibilita indicar al receptor, o receptores, no solo las características del tráfico de usuario, sino también la ruta por donde debe solicitar las correspondientes reservas de recursos. Los enrutadores que no soporten RSVP transfieren transparentemente los mensajes PATH´s.

Los mensajes RESV´s son producidos por el receptor (o receptores) de los flujos de información de usuario, como respuesta a los mensajes PATH´s, y solicitan a la red (a los enrutadores RSVP) las correspondientes reservas de recursos para soportar la comunicación con cierta QoS, fluyendo hasta la fuente del stream de datos de usuario, es decir, en sentido upstream. Con la información de ruta que suministran previamente los mensajes PATH´s, los mensajes RESV´s dirigen las solicitudes de reservas a los enrutadores RSVP apropiados, esto es, por donde fluirán los streams de datos.

Los mensajes RESV´s especifican el ancho de banda mínimo que se requiere para obtener determinada demora en un stream de datos específico. Vale decir además, que es posible efectuar reservas compartidas, esto es, una misma reserva aplicable a varios streams de datos de usuario.

Estas reservas de recursos en los enrutadores RSVP de la red se materializan mediante soft-states en dichos enrutadores, estados que requieren para mantenerse de refrescamientos periódicos, por lo que durante toda la comunicación se necesita señalizar para mantener las reservas previamente efectuadas. En consecuencia, esto conlleva a cierta señalización permanente durante la fase de transferencia de información de usuario, con la consiguiente carga de tráfico que implica.

La reserva de recursos extremo a extremo que posibilita RSVP será válida si, y solo si, la congestión y demora que introduzcan los enrutadores no RSVP no es significativa.

Otros mensajes del protocolo RSVP son:

- PATHTEAR: son mensajes generados por la fuente de datos de usuario para eliminar los estados path´s en todos los enrutadores RSVP. Siguen la misma ruta que los mensajes.
- PATH´s. También pueden ser originados por cualquier nodo cuando se agota el timeout del estado path.
- RESVTEAR: son generados por los receptores para borrar los estados de reserva en los enrutadores RSVP, por tanto viajan en el sentido upstream. Pueden ser también originados por nodos RSVP al agotarse el timeout del estado de reserva de los mismos.
- PATHERR: viajan en sentido upstream hacia el emisor siguiendo la misma ruta que los mensajes PATH´s, y notifican errores en el procesamiento de mensajes PATH´s, pero no modifican el estado del nodo por donde ellos pasan en su viaje hacia la aplicación emisora.
- RESVERR: notifican errores en el procesamiento de mensajes RESV, o notifican la interrupción de una reserva. Se transfieren en la dirección downstream hacia el receptor o receptores apropiados.

Protocolo básico

Las solicitudes de reserva conducen a que en cada enrutador RSVP se establezca un estado soft (Soft-State), es decir, una reserva en cada enrutador es un estado Soft con un determinado timeout, que debe ser refrescada periódicamente por los receptores, de lo contrario vence el

timeout y se deshace la correspondiente reserva, con la consecuente generación de un mensaje RESVTEAR.

La liberación de recursos reservados mediante RSVP se puede materializar de diferentes maneras, así la solicitud para dar baja a determinada reserva puede ser originada: por el emisor, por el receptor o por un nodo de la red.

Por parte del emisor o de un receptor acontece cuando así lo decide la aplicación correspondiente, en cuyo caso esto se produce mediante la generación de un mensaje PATHTEAR o un mensaje RESVTEAR, respectivamente.

Por parte de un nodo se lleva a cabo cuando vence el timeout correspondiente del estado path o del estado de reserva, lo que origina la emisión de un mensaje PATHTEAR o un mensaje RESVTEAR, respectivamente.

3.3.3 Servicios Diferenciados (Diffserv)

Se basa en marcar los paquetes IP, y la red (los enrutadores) los tratarán en base a esa marca, esto es, se desarrolla un tratamiento diferenciado de los paquetes IP en los enrutadores. Define y utiliza diferentes tipos de enrutadores. Esta diferenciación no es la misma en los diferentes nodos, sino depende de si se trata de un nodo interior o un nodo frontera. En consecuencia, y a diferencia de la solución Servicios Integrados (basada en RSVP), la red con nodos Diff-Serv no establece ni mantiene estados de las conexiones por flujos de paquetes. Es una solución escalable, más apropiada para grandes entornos como Internet. Puede ser fácilmente implementada en las redes IP existentes.

La versión 6 de IP contempla este marcado de paquetes, mediante el campo DS (Differentiated Service), byte DS de la cabecera IP. El byte de Clase se puede utilizar como byte de servicios diferenciados, teniendo el mismo significado que en IPv4.

También IPv4 permite dicho marcado de paquetes, a través del byte ToS (Type of Service), y en tal caso se utiliza éste como byte DS. IP Precedente son usados los primeros tres bits del campo TOS para dar 8 posibles valores de precedencia.

- 000 (0) - Routine.
- 001 (1) – Priority.
- 010 (2) – Immediate.
- 011 (3) – Flash.
- 100 (4) - Flash Override.
- 101 (5) – Critical.
- 110 (6) - Internetwork Control.
- 111 (7) – Network Control.

DiffServ introduce el concepto de DiffServ Code Point (DSCP), que usa los primeros 6 bits del campo TOS para dar 2^6=64 diferentes valores

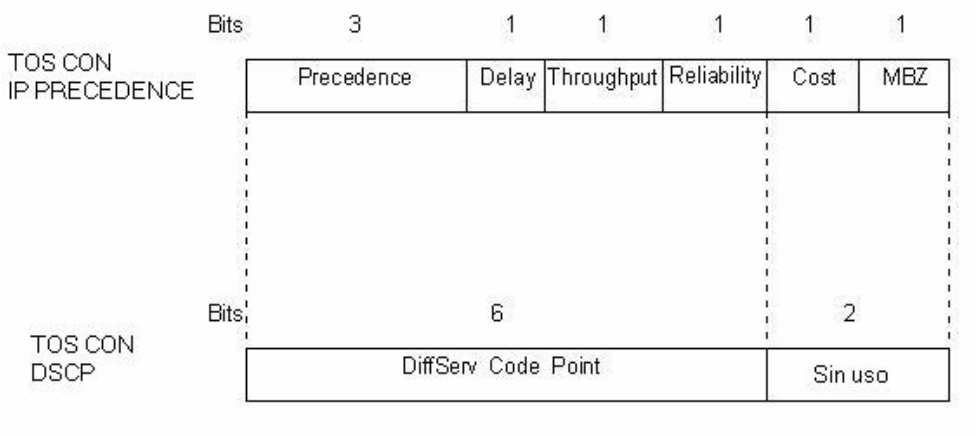

Fig. 3.9. El campo DSCP.

El sexto bit del campo DS es usado como DSCP (Diffserv Code Point) para seleccionar el PHB (Per Hop Behavior), es decir, con dicho código se selecciona clases de tráfico entre interfases. Un campo de dos bits (CU), actualmente sin uso, es reservado para la notificación de congestión explícita (ECN).

Un Per Hop Behavior es una forma efectiva de transporte de un flujo en particular o varios grupos de flujos de paquetes. La siguiente tabla muestra valores de DSCP:

PHB		DiffServ Code Point (DSCP)			IPPrecedence
Default					0
		000000			
Transporte seguro		Baja probabilidad de desecho	Probabilidad media de desecho	Alta probabilidad de desecho	
	Class 1	AF11	AF12	AF13	1
		001010	001100	001110	
	Class 2	AF21	AF22	AF23	2
		010010	010100	010110	
	Class 3	AF31	AF32	AF33	3
		011010	011100	011110	
	Class 4	AF41	AF42	AF43	4
		100010	100100	100110	
Transporte expedito		EF			5
		101110			

Tabla 3.12. Valores de DSCP.

Se han definido dos tipos de Diff-Serv con garantía de QoS: Assured Forwarding Service (AFS) y Expedited Forwarding Service (EFS).

- *EFS*: equivale a una línea arrendada virtual, por lo que se garantiza cierto ancho de banda y reducida demora de cola. Emula un circuito.
- *AFS*: los paquetes se etiquetan con alta prioridad, aunque no se garantiza un ancho de banda. Se posibilita una QoS superior al servicio tradicional best-effort de Internet. Brinda cuatro clases de servicios, cada una con tres niveles diferentes de dropping. Un nodo DS

es, en principio, una combinación de cinco módulos funcionales, aunque no todo enrutador DS tiene que contener la totalidad de éstos:

- *Clasificador de tráfico*: clasifica los paquetes en base a uno o varios campos de su cabecera.
- *Medidor de tráfico (Traffic Meter)*: mide las propiedades temporales de los paquetes.
- *Marcador de paquetes (Packet Markers)*: establece un codepoint en el campo DS del paquete.
- *Conformador (Shapers)*: establece cierta demora para uno o más paquetes de un stream.
- *Droppers*: descarta algunos o todos los paquetes de un stream de tráfico.

Los tipos de enrutadores en redes Diff-Serv se clasifican así:

- *First Hop Router*: es el enrutador más próximo al host emisor de paquetes. Los flujos de paquetes son clasificados y marcados acorde a la etiqueta SLA (Service Level Agreement). Es responsable de que el tráfico esté acorde con el ancho de banda del perfil.
- *Ingrees Router*: Se sitúan en los puntos de entrada al backbone Diff-Serv (dominio DS), efectuando la clasificación de los paquetes en base al campo DS o en base a múltiples campos de la cabecera de éstos.
- *Egress Router*: Se ubican en los puntos de salida de redes Diff-Serv (dominio DS), controlando el tráfico. Efectúan la clasificación de paquetes en base solo al campo DS de las cabeceras.
- *Interior Router*: Tienen la misión de sumar flujos, realizar la clasificación DS y reenvio de paquetes. Se sitúan dentro del backbone DS (dominio DS).

Componentes de Diffserv

Los siguientes componentes constituyen la solución de cisco:

1. Condicionadotes de tráfico usando TCA.
2. Clasificación y Marcado de paquetes usando DSCP.
3. Manejo de la congestión a través de CBWFQ.
4. Prevención de la congestión usando WRED.

Todos estos componentes se describen en el capítulo 4 de esta tesis.

El proceso de señalización en VoIP es muy diferente a las soluciones clásicas de las redes de Telecomunicación, por cuanto en éstas el problema de la QoS no es negociable, está implícito, por tanto no implica señalización para este fin. Con el advenimiento de las redes Frame-Relay y redes ATM esto ha sufrido cierta transformación en el sentido de que es posible mediante señalización negociar QoS.

En el caso de VoIP se han planteado otras soluciones, es el caso ahora de redes de datagramas, y no de circuitos físicos (redes modo circuitos) o circuitos virtuales (Frame-Relay y ATM). Así, la obtención de QoS en el caso de VoIP requiere una señalización de forma explícita, que en principio puede anteceder o suceder a la señalización en el sentido tradicional para establecer la conexión (conexión lógica en este caso).

4 Mecanismos para Calidad de Servicio

Los mecanismos existentes para poder brindar la QoS necesaria son:

1. Mecanismos de clasificación y marcado.
2. Mecanismos para evitar la congestión.
3. Mecanismos para la administración de congestión.
4. Mecanismos para eficientar el uso del Ancho de Banda (Bw).
5. Mecanismos condicionadores de tráfico.
6. Mecanismos de Control de Admisión de llamada.

A continuación de describe cada uno de ellos de acuerdo a las especificaciones de CISCO SYSTEMS.

4.1 Mecanismos de clasificación y marcado

Clasificación

La Clasificación implica usar un descriptor de tráfico para clasificar un paquete dentro de un grupo específico. Después de que el paquete ha sido clasificado, éste es accesible para el manejo de QoS en la red.

Usando clasificación de paquetes, se puede dividir el tráfico de la red en múltiples niveles de prioridad o clases de servicio. Cuando la fuente acepta adherirse a los términos de la red, los descriptores de tráfico son usados para clasificar el tráfico, y la red promete una calidad de servicio. Los Traffic policers, traffic shapers, y las técnicas de encolamiento usan el descriptor de tráfico del paquete (clasificación del paquete) para asegurar adherencia a ese agregado.

Marcado

El marcado de paquetes está relacionado con su clasificación. El marcado permite clasificar un paquete o trama basándose en un descriptor de tráfico específico. Marcar un paquete o trama con esta clasificación permite poner información en el encabezado de las capas 2, 3 o 4, e incluso poner información dentro de la carga útil del paquete, por eso el paquete o trama puede ser identificado y distinguido de otros paquetes o tramas.

Capa 2 Clase de Servicio (CoS)

El estándar 802.1p soporta ocho clases de servicios. El valor 0 de CoS representa un servicio rutinario (sin prioridad).

Una trama ethernet puede ser compatible con 802.1p/Q. Si lo es, entonces son insertados 4 bytes en el campo Etiqueta (Tag) de la trama Ethernet. Los primeros tres bits, conocidos como los bits de prioridad de usuario, son bits de 802.1p. El resto del campo está formado por el CFI (Identificador de Formato Canónico), y campos de identificación de VLAN (VLAN ID), que es campo de 802.1Q. El campo Tag a veces es llamado campo 802.1p/802.1Q.

Así que cuando la trama ethernet de capa 2 es marcada por prioridad, los tres bits de prioridad de usuario de 802.1p son puestos a un valor 0-7.

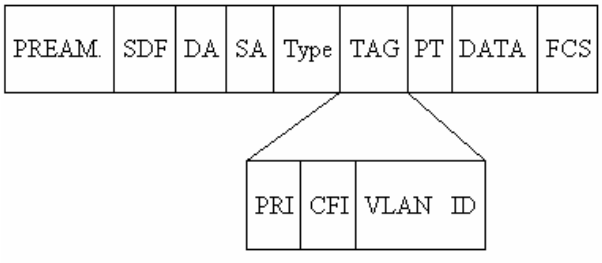

Fig. 4.1. Campo TAG.

Capa 2 – QoS

Los estándares ATM definen una muy rica infraestructura de QoS para soportar diferentes tipos de tráfico, muchos parámetros QoS ajustables (como tasa de celda máxima PCR, tasa de celda mínima MCR,etc.), señalización, y Control de Admisión de Conexión (CAC). Frame Relay, por otro lado proporciona un muy simple juego de mecanismos para proveer una Tasa de Información Prometida (CIR), notificación de congestión, y el recientemente introducido Frame Relay Fragmentation (FRF.12).

Sin embargo estos mecanismos de QoS existen en tecnologías de transporte de capa 2, un verdadero QoS de punta a punta no es alcanzable, a menos que una solución de capa 3 sea cubierta. Los proveedores de servicios ofrecen ambos servicios ATM/Frame Relay e IP buscando proveer una solución de QoS robusta a los clientes. El mapeo de capa 2 QoS hacia capa 3 QoS es el primer paso para lograr una completa solución, eso no depende de alguna tecnología de capa 2 específica. IntServ y DiffServ pueden ser implementados sobre transportes de QoS-aware como ATM y Frame Relay. Con DiffServ, los paquetes marcados con un valor difetente en el byte ToS pueden ser enviados sobre ATM PVCs o CVCs diferentes. De manera semejante, el tráfico en Frame Relay Traffic Shaping (FRTS) (disminuir la tasa de transmisión por el bufer, en respuesta a la notificación de congestión de los switches FR), FRF.12 (fragmentación de paquetes e intercalar en links FR de baja velocidad), y otros mecanismos pueden ser usados para complementar QoS en IP.

Por lo tanto, un verdadero QoS de punta a punta comprende QoS en capa 2 y capa 3, y es un medio independiente. La introducción de un enlace Gigabit Ethernet en algún lugar a lo largo de la ruta de los paquetes no plantea problema de entregar QoS, como el QoS de capa 3 aún se preserva e incluso puede ser mejorado mapeando el mecanismo de QoS en 802.1p (prioridad de usuario) sobre Ethernet.

Capa 3 Tipo de Servicio (ToS)

Prioridad IP usa los tres bits de prioridad en el campo ToS del encabezado de IPv4 para especificar la clase de servicio para cada paquete. Se puede dividir el tráfico hasta en seis clases de

servicio que usa Prioridad IP (las posiciones 6 y 7 están reservadas para uso de la red interna). Las tecnologías de encolamiento en toda la red pueden usar entonces esta señal para proveer un apropiado manejo de aceleración.

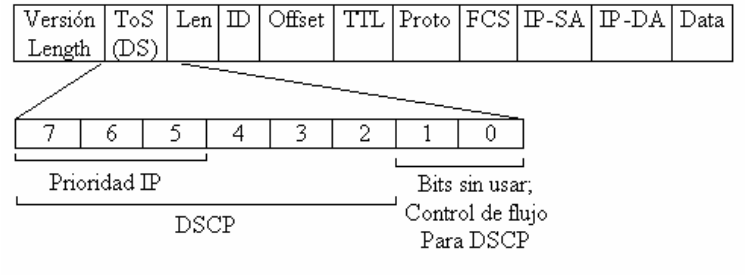

Fig. 4.2. Campo ToS.

Características como direccionamiento basado en políticas (policy-based routing), marcado basado en la clase (class-based marking) y tasa de acceso prometida (CAR) pueden ser usadas para fijar la prioridad sobre la base de la clasificación de la lista de acceso extendida. Esto permite una considerable flexibilidad para asignar la prioridad, incluyendo asignación por aplicación, usuario, destino, subred de origen, etc. Típicamente esta funcionalidad es desplegada tan cerca del borde de la red como es posible así cada elemento de la siguiente red puede proveer servicio basándose en la política resuelta.

Prioridad IP también puede ser puesto en el host o el cliente de la red, y esta señalización puede ser usada opcionalmente; sin embargo, esto puede ser invalidado por la política dentro de la red.

Prioridad IP permite clases de servicio para ser establecida usando una red existente con mecanismos de encolamiento (por ejemplo, WFQ o WRED) sin cambios para aplicaciones existentes o complicados requisitos de la red. Este mismo es fácilmente aplicado a IPv6 usando su campo Prioridad.

DiffServ es un nuevo modelo que reemplaza, y es compatible con Prioridad IP. DiffServ usa seis bits de prioridad, los cuales permiten clasificación de hasta 64 valores (0 - 63). El valor de DiffServ es llamado Punto Clave de Servicios Diferenciados (DSCP).

Con DiffServ, el campo DS reemplaza el octeto ToS de IPv4 y el octeto Clase de Trafico de IPv6. Seis bits del campo DS son usados como el DSCP para seleccionar el Comportamiento por Salto (PHB) en cada interfaz. Un campo de dos bits actualmente sin uso (CU) es reservado para notificacion de congestión explícita (ECN). El valor de los bits CU es ignorado por las interfaces compatibles con DS cuando determina el PHB a aplicar a un paquete recibido.

DiffServ Per Hop Behavior

Un Comportamiento por Salto (PHB) es el comportamiento de envío exteriormente observable aplicado en un nodo compatible con DiffServ a un agregado de comportamiento (BA) de DiffServ.

Con la habilidad del sistema de caracterizar paquetes de acuerdo con los parámetros DSCP, la colección de paquetes (cada uno con los mismos parámetros DSCP y enviados en una dirección particular) pueden ser agrupados dentro del BA. Paquetes de múltiples fuentes o aplicaciones pueden pertenecer al mismo BA.

Los cuatro estándares de PHB disponibles son:

- Default PHB (definido en RFC 2474)
- PHB de Envío Seguro (AFny) (definido en RFC 2597)
- PHB de Envío Acelerado (EF) (definido en RFC 2598)
- PHB Selector de Clase (definido en RFC 2474)

El PHB por defecto (Default PHB) especifica que un paquete marcado con un PHB de 000000 (recomendado) recibe un servicio de "best-effort" de un nodo DS compatible. Si un paquete llega a un nodo DS compatible y el valor de DSCP no es mapeado por algún otro PHB, el paquete es mapeado por el PHB por defecto.

El PHB de Envío Seguro define cuatro clases de AFny (n=1-4: AF1, AF2, AF3 y AF4). Cada clase es asignada a una cantidad específica de espacio en el buffer y un ancho de banda de interfaz, de acuerdo con el contrato de nivel de servicio (SLA) con el proveedor de servicio o el mapa de políticas. Dentro de cada clase de AF, se puede especificar tres valores de prioridad de drop (y=1-3). Los paquetes de la clase AF13 son soltados antes que los paquetes de la clase AF12, los cuales son soltados antes que los paquetes en la clase AF11.

El PHB de Envío Acelerado provee bajas pérdidas, baja latencia, bajo jitter y garantiza el servicio de ancho de banda. Esto es comparable con el Protocolo de Reservación de Recursos (RSVP) de IntServ, el cual provee un servicio de ancho de banda garantizado. EF PHB debe ser reservado para las aplicaciones mas críticas, en casos de congestión de tráfico, esto no es viable para tratar todo o mucho tráfico de alta prioridad. EF PHB es ideal para aplicaciones como VoIP que requieren bajo ancho de banda, ancho de banda garantizado, bajo delay, y bajo jitter. El valor recomendado de DSCP para EF PHB es 101110.

El PHB Selector de Clase es el PHB asociado con el class-selector code point. Los valores de DSCP llamados class-selector code point (con la forma xxx000, donde x puede ser 0 o 1) preserva compatibilidad con Prioridad IP. (El valor de DSCP para un paquete con 000000 de Default PHB también es llamado class-selector code point) Por ejemplo, paquetes con un valor de DSCP de 110000 tienen trato de envío preferencial, comparado con un paquete con valor de DSCP de 100000.

PHB				DSCP			Prioridad IP
Default (Best Effort)				000000			0
Envío Seguro	Pef. baja	Pref. media	Pref. alta				
Clase 1	AF11	AF12	AF13	001010	001100	001110	1
Clase 2	AF21	AF22	AF23	010010	010100	010110	2
Clase 3	AF31	AF32	AF33	011010	011100	011110	3
Clase 4	AF41	AF42	AF43	100010	100100	100110	4
Envío Acelerado	EF			101110			5

Tabla 4.1. Valores equivalentes entre PHB, DSCP y Prioridad IP.

4.2 Mecanismos para evitar la congestión

Las técnicas de prevención de congestión supervisan las cargas de tráfico de la red en un esfuerzo por anticiparse y evitar la congestión de los cuellos de botella de la red. Entre los mecanismos más comúnmente usados para la prevención de congestión están.

- RED (Random Early Detection). Detección aleatoria temprana.

- WRED (Weighted Random Early Detection). RED basada en el peso.

Cada uno de estas técnicas se describe a continuación con más detalle.

RED (Random Early Detection)

Los algoritmos de detección temprana al azar son diseñados para evitar la congestión entre redes antes de que esta se vuelva un problema. RED supervisa la carga de tráfico en diferentes puntos de la red y desecha paquetes de forma estocástica si aumenta el nivel de congestión. El resultado es que la fuente detecta esta situación, retardando su transmisión.

Antes de que se presente alta congestión, RED aleatoriamente desecha paquetes, por lo que las fuentes disminuyen su tasa de transmisión. Si dicha fuente está usando TCP, esta disminuye su tasa de transmisión hasta que todos los paquetes alcancen su destino, anunciando que la congestión ha sido eliminada. RED se ha diseñado para trabajar en entornos TCP e IP principalmente.

La probabilidad de que un paquete llegue a ser desechado está basada en tres parámetros configurables:

- *Umbral mínimo*. Cuando la profundidad promedio de un encolamiento esta por arriba del umbral mínimo, RED empieza a desechar paquetes. La tasa de paquetes desechados incrementa linealmente como el tamaño de la cola promedio incrementa, hasta que el tamaño de la cola promedio alcance el umbral máximo.
- *Umbral máximo*. Cuando el tamaño promedio del encolamiento esta por arriba del umbral máximo, todos los paquetes serán desechados. Si la diferencia entre el umbral máximo y mínimo es demasiado grande, un gran número de paquetes podrían ser desechados de inmediato, resultando una sincronización global.
- *Denominador de probabilidad de marca*. Esta es la fracción de paquetes desechados cuando la profundidad promedio de una cola está en el umbral máximo. Por ejemplo si el denominador es 512, 1 de 512 paquetes es desechado cuando la cola promedio está en el máximo.

La siguiente figura ilustras estos parámetros:

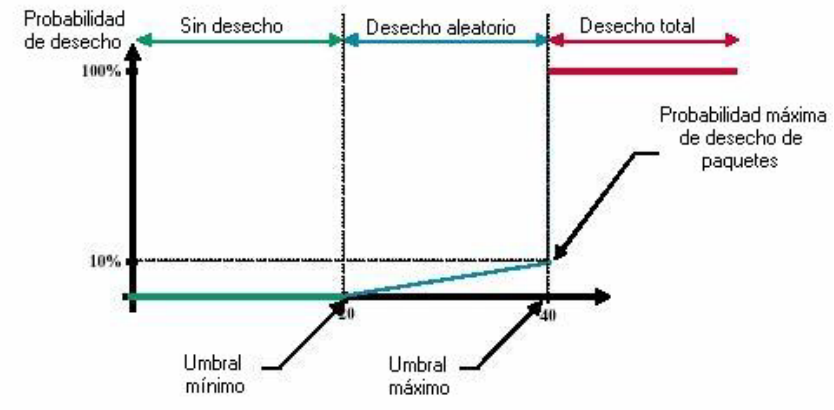

Fig. 4.3. Parámetros de RED

RED distribuye perdidas en tiempo y mantiene normalmente baja profundidad de encolamiento mientras son absorbidos los picos.

WRED (Weighted Random Early Detection)

WRED es una implementación de RED para plataformas del estándar CISCO IOS. Combina las capacidades de RED con precedencia IP o señalización DSCP.

Si este mecanismo no es configurado, los enrutadores usan un mecanismo para desechar paquetes por default llamado Tail Drop (desechar el último en llegar al encolamiento). Tail Drop: Trata todo el tráfico igualmente y no diferencia entre clases de servicio. Las colas se llenan durante los períodos de congestión. Cuando la cola de salida está llena, se desechan paquetes hasta que la congestión sea eliminada y la cola ya no este llena.

WRED monitorea la profundidad promedio de una cola en los enrutadores y determina cuando se va a empezar a desechar paquetes. Cuando la profundidad promedio de una cola atraviesa el umbral mínimo especificada por el usuario, WRED empieza a desechar paquetes (tanto en TCP como UDP) con cierta probabilidad. Si se atraviesa el umbral máximo entonces WRED deja de operar, entrando en operación Tail Drop. La idea detrás de usar WRED es para mantener la profundidad de la cola en un nivel en algún punto entre el umbral máximo y mínimo.

Este mecanismo puede selectivamente desechar tráfico de baja prioridad cuando la interfaz empieza a congestionarse y provee características de realización de discriminación para diferentes clases de servicio.

Para interfaces configuradas para usar RSVP, WRED elige paquetes de otros flujos para preferentemente desecharlos en lugar de los flujos de RSVP. Además, IP Precedence o DSCPs controla cuales paquetes serán desechados, el tráfico que es de baja prioridad, tiene una alta tasa de desecho.

Esta combinación mantiene tráfico preferencial que maneja como paquetes de prioridad más alta. Puede selectivamente desechar el tráfico de menor prioridad cuando el interfaz empieza a congestionarse y proporciona características de gestión distintas para las diferentes clases de servicio. Pero WRED también permite RSVP, ofreciendo servicios integrados de QoS de carga controlada.

Además, WRED desecha más paquetes de grandes usuarios que de pequeños. Por consiguiente, las fuentes que generen más tráfico son las más probables a ser retardadas que las fuentes que generen menor tráfico.

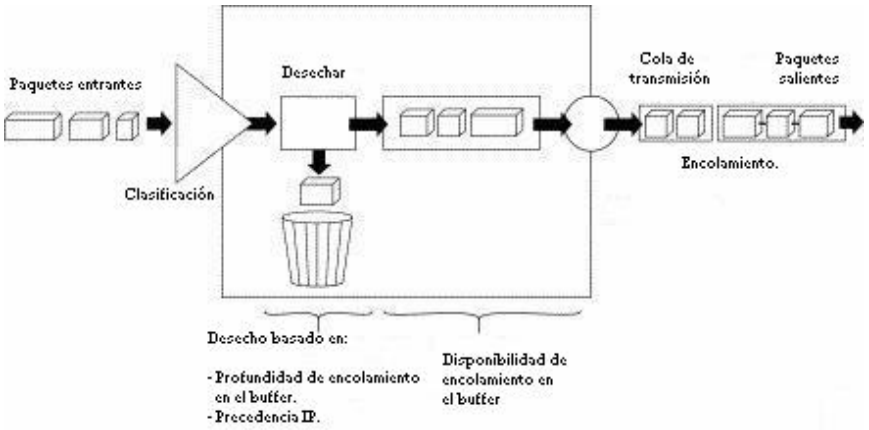

Fig. 4.4. Funcionamiento de WRED.

Impide los problemas de sincronización global que ocurren cuando Tail Drop es usado como mecanismo para evitar la congestión. La sincronización global se presenta cuando hosts TCP reducen imultáneamente su tasa de transmisión en respuesta a paquetes desechados, luego incrementan su tasa de transmisión una vez más en el momento en que la congestión es reducida.

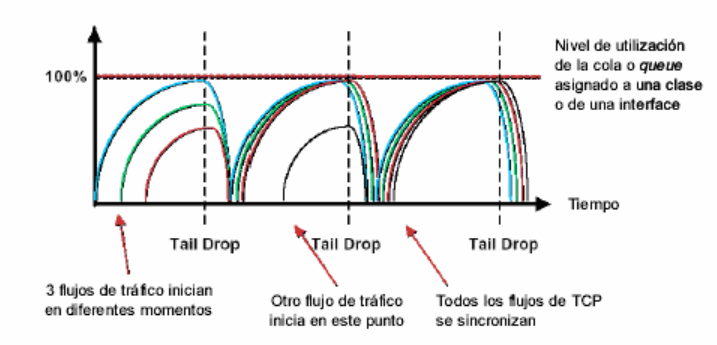

Fig. 4.5. Sincronización Global.

Sólo es útil cuando la gran mayoría del tráfico es TCP/IP. Con TCP, el desecho de paquetes indica congestión, así las fuentes reducen sus tasas de transmisión. Con otros protocolos, las fuentes no podrían responder o podrían reenviar paquetes que ya han sido desechados a la misma tasa, y por lo tanto no disminuiría la congestión. Además, WRED trabaja preferentemente con tráfico IP.

WRED trata a los tráficos que no son IP con precedencia 0, que es la más baja. Por consiguiente, en general son más probablemente desechados que el tráfico de IP.

Este mecanismo debe ser usado dondequiera que halla un cuello de botella potencial (link de congestión), el cual muy bien podría ser un link de borde de acceso. Sin embargo WRED es usado en los enrutadores centrales de una red, en vez de los de la orilla de la red. Los enrutadores de la orilla asignan Precedencia IP a los paquetes, cuando ellos entran en la red, dicha precedencia es usada para dar trato diferente a cada tipo tráfico.

Notamos que este mecanismo no es recomendado para encolamiento de voz. La red no debe ser diseñaba para perdida de paquetes de voz puesto que dicha perdida reduce la calidad de la voz. WRED controla la congestión impactando otro tráfico priorizado, ayudando a evitar la congestión para asegurar la calidad de la voz.

4.3 Mecanismos para la administración de congestión

Los elementos de red unidireccionales deben de poder manejar grandes tasas de tráfico de llegada, para ello usan algoritmos de encolamiento que clasifiquen el tráfico y aplicar después algún método de priorización para su expedición.

Algunos algoritmos de gestión de colas de espera son los siguientes:

1. FIFO (First-in, First-out): Primero en entrar, primero en salir de la cola.
2. PQ (Priority Queuing): Prioridad de encolamiento.
3. CQ (Custom Queuing): Encolamiento por costumbre.
4. WRR (Weighted Round Robin): Round Robin pesado.
5. WFQ (Weighted fair queuing): Encolamiento justo basado en el peso.

6. CBWFQ (Class Based WFQ): WFQ basado en clases.
7. IP RTP Priority (IP Real Time Protocol Priority): También conocido como PQ/WFQ.
8. Frame Relay IP RTP Priority.
9. LLQ (Low Latency Queuing): Encolamiento de baja latencia.

Cada algoritmo de encolamiento ha sido diseñado para resolver un problema específico de tráfico de la red, obteniendo así un determinado efecto en el funcionamiento de la red, tal y como se describe en cada uno de ellos.

La siguiente tabla muestra un resumen de algunas características clave de las técnicas de encolamiento.

	PQ	CQ	WRR	WFQ	CBWFQ	IP RTP PRIORITY	LLQ
Clasificación	Protocolo, interfaz	Protocolo, interfaz	CoS, ToS/DSCP	IP prec RSVP, protocolo puerto	Mod CLI	VoFR e IP RTP Priority	VoFR y Mod CLI
Número de colas	4	16	2 o 4	Por flujo	64 clases	1 PQ +WFQ	1 PQ + CBWFQ
Ordenamiento	Prioridad estricta	Round Robin	Round Robin	Equitativo: peso, tiempo de arribo	Equitativo: peso y BW	PQ: estricto WFQ:equitativo	Si
Retardo garantizado	Si	No	No	No	No	Si	Si
BW garantizado	No	Si	No	No	Si	PQ: Si WFQ: No	Si
Usado para voz	No	No	Si, dentro de un campus		No	Si	Si

Tabla 4.2. Algunas técnicas de encolamiento.

1. FIFO (First-in, First-out)

En su forma más simple, el algoritmo FIFO implica almacenar los paquetes cuando se congestiona la red y expedirlos, teniendo en cuenta el orden de llegada, cuando la red no está tan congestionada. FIFO es el algoritmo por defecto, por lo que no requiere ninguna configuración, sin embargo tiene varios defectos. El más importante es que no toma decisiones sobre la prioridad de los paquetes, es el orden de llegada el que determina el ancho de banda y el buffer a asignar. No proporciona protección contra aplicaciones (fuentes) corruptas. El tráfico a ráfagas puede causar grandes retardos en la entrega del tráfico basado en aplicaciones sensibles al tiempo, así como al control de la red y a los mensajes de señalización que circulan por la misma. FIFO fue, en definitiva, un primer paso necesario para el control del tráfico de a red, pero hoy en día las redes inteligentes necesitan algoritmos más sofisticados.

2. PQ (Priority Queuing)

PQ asegura que el tráfico importante sea administrado más rápidamente en cada punto donde se utilice. Fue diseñado para dar mayor prioridad al tráfico importante. Este algoritmo puede dar la prioridad de forma flexible según el protocolo de red utilizado (por ejemplo IP, IPX, o AppleTalk), la

interfaz entrante, el tamaño del paquete, la dirección fuente y/o destino, y mucho más. En PQ cada paquete es colocado en una de las cuatro colas de prioridad: alta, media, normal (default) y baja. Basándose en las especificaciones del usuario, asignándose prioridad normal para aquellos paquetes que no tengan ninguna prioridad asignada. Durante la transmisión el algoritmo concede un tratamiento preferencial a las colas de mayor prioridad sobre las de menor prioridad.

PQ se puede utilizar para cualquier interfaz. PQ introduce extra overhead que es aceptable para interfaces lentas, pero podría no ser aceptable para interfaces de alta velocidad tales como ethernet, ya que los paquetes son clasificados por el procesador del sistema.

Con este método se podría dar el caso de que el tráfico de baja prioridad nunca llegue a su destino por lo que se propone usar otros algoritmos, los cuales se mencionan a continuación.

PQ es útil para cerciorarse de que el tráfico que atraviesa varias conexiones WAN, sea considerado crítico y consiga un tratamiento prioritario. Este algoritmo usa una configuración estática, no adaptándose así automáticamente a los requisitos cambiantes de las redes.

3. CQ (Custom Queuing)

CQ fue diseñado para permitir que varias aplicaciones u organizaciones compartan la red, entre aquellas aplicaciones que necesiten anchos de bandas o requisitos de latencia mínimos. En estos entornos debe compartirse proporcionalmente el ancho de banda entre las aplicaciones y los usuarios. CQ puede utilizarse para proporcionar ancho de banda garantizado en aquellos puntos donde se produzca congestión, asegurando a un tráfico específico una porción fija de ancho de banda disponible y dejando el tráfico restante para cualquier otro tipo de tráfico. Las colas clientes manejan el tráfico asignando una cantidad específica del espacio de la cola a cada clase de paquete, aplicando posteriormente el sistema Round-Robin.

El algoritmo de encolamiento coloca los mensajes en una de las 17 colas (la cola 0 se utilizada para almacenar mensajes de sistema como mantenimiento, señalización, etc.) y se vacía con prioridad pesada. Los servicios de enrutamiento van desde la cola 1 a la 16 según el orden asignado por Round-Robin, desencolando un número específico de bytes de cada cola por cada ciclo antes de moverse a otra cola. Esto asegura que ninguna aplicación (o grupo de aplicaciones) logre una mayor proporción de capacidad global cuando la línea se encuentre bajo presión. El ancho de banda usado por una cola particular es especificado indirectamente en términos de un contador de bytes y la longitud de la cola.

Al igual que PQ, CQ se configura estáticamente y no se adapta automáticamente a las condiciones cambiantes de las redes.

4. WRR (Weighted Round Robin)

Es similar en operación a CQ, pero es ajustado para su operación en Switches de Capa 2 y 3. Hay generalmente de 2 a 4 colas, y su clasificación está basada en CoS o ToS/DSCP.

5. WFQ (Weighted fair queuing)

Para situaciones en las que es deseable proporcionar un tiempo de respuesta consistente a cualquier tipo de usuarios sin necesidad de aumentar el ancho de banda de forma excesiva, entonces la solución es WFQ. Es un algoritmo de encolamiento basado en el flujo que realiza dos

tareas simultáneamente: sitúa el tráfico interactivo a principio de la cola para reducir el tiempo de respuesta y permite así compartir el resto del ancho de banda entre flujos que requieren gran ancho de banda.

Se clasifica el tráfico en diferentes flujos, basados en la información del encabezado del paquete. Hay dos categorías de flujo: sesión de alto ancho de banda y sesión de bajo ancho de banda

Se asegura que las colas no se quedarán sin ancho de banda, proporcionando a ese tráfico un servicio predecible. Así mismo, las ráfagas de tráfico de bajo volumen (la mayoría del tráfico) reciben servicio preferencial, transmitiéndolas rápidamente. Las ráfagas de tráfico de gran volumen compartirán la capacidad restante de forma proporcional entre ellos.

Ha sido diseñado para minimizar en esfuerzos al configurar, adaptándose automáticamente a las condiciones cambiantes del tráfico de la red.

WFQ es eficaz pues permite que se pueda asignar cualquier cantidad de ancho de banda para flujos de tráfico de baja prioridad si no está presente ningún flujo de alta prioridad. Esto es diferente del multiplexado por división en el tiempo (TDM) que simplemente mide el ancho de banda y permite que este no se utilice si no está presente un determinado tipo de tráfico.

Además, trabaja con las técnicas IP Precedence y RSVP para proporcionar QoS diferenciada así como servicios garantizados.

Este algoritmo también trata el problema de la variabilidad del atraso durante la transmisión. Si hay múltiples conversaciones de alto volumen activas, sus tasas de transferencia, así como sus periodos de llegada se hacen más predecibles. WFQ refuerza algoritmos como el SNA Control de Enlace Lógico (LLC) y el control de congestión del Protocolo de Control de Transmisión (TCP), obteniendo como resultado una expedición y un tiempo de respuesta más predecible para cada uno de los flujos activos.

6. CBWFQ (Class Based WFQ)

Con WFQ, todos los flujos son servidos, bajo condiciones donde el número de colas llega a ser grande, incluso la alta prioridad de tráfico empieza a experimentar una latencia inaceptable. CBWFQ resuelve este problema fijando el ancho de banda para colas de voz y encolamientos exhaustivos.

Brinda soporte a las clases de tráfico definidas por el usuario. Se pueden definir las clases de tráfico basadas en el criterio de correspondencia o identidad, incluyendo los protocolos, listas de control de acceso (ACLs) e interfaces de entrada. Los paquetes que satisfacen el criterio de identidad, constituyen el tráfico para esa clase. Una cola es reservada para cada clase, y el tráfico que pertenece a una clase es dirigido hacia su cola correspondiente.

Una vez que se ha definido una clase según su criterio de correspondencia, se le puede asignar características. Para caracterizar una clase, se le asigna ancho de banda, peso y límite de paquetes máximos. El ancho de banda asignado a una clase es el ancho de banda garantizado entregado a la clase durante la congestión.

Para caracterizar una clase, se puede especificar también el límite de la cola para esa clase que es el número máximo de paquetes permitidos para ser acumulados en la cola para la clase. Los

paquetes que pertenecen a una clase están sujetos al ancho de banda y los límites de la cola que caracterizan la clase.

Después de que una cola ha cumplido con esta configuración del límite de encolamiento, el encolamiento de paquetes adicionales a la clase provoca tail drop o paquetes desechados, dependiendo de cómo la política de clases es configurada.

Tail Drop es usado por las clases de CBWFQ a menos que se configure el modo de operación para una clase para que use WRED como un medio de evitar la congestión. Si se usa WRED para desechar paquetes en vez de tail drop para una o más clases que comprenden un mapa de la política u operación, se debe asegurar que WRED no se configura para la interfaz hacia la cual se sujeta esa política de servicio.

Si una clase default es configurada con el comando de configuración *Bandwidth policy-map,* todo el tráfico que no esté clasificado se pone en una sola cola y se le da un trato según el ancho de banda configurado. Si una clase default es configurada con el comando *fair-queue* (cola equitativa), todo el tráfico que no este clasificado, entrará en esta clase y se le dará el trato del mejor esfuerzo. Si ninguna clase default se configura, entonces por defecto, el tráfico que no corresponda a ninguna de las clases configuradas es flujo clasificado y se le da el tratamiento del mejor esfuerzo. Una vez que un paquete es clasificado, todos los mecanismos normales o estándar que pueden usarse para diferenciar el servicio entre las clases se aplican.

Para CBWFQ, el peso especificado para la clase se vuelve el peso de cada paquete que encuentra el criterio de correspondencia de la clase.

Los paquetes que llegan a la interfaz de salida son clasificados según el filtro del criterio de correspondencia definido, entonces a cada uno se le es asignado un peso apropiado. El peso para un paquete que pertenece a una clase específica se deriva del ancho de banda que se asignó a la clase cuando se configuró; en este sentido el peso para una clase es configurable por el usuario.

Después de que el peso para un paquete es asignado, el paquete es encolado en la cola de la clase apropiada. CBWFQ usa los pesos asignados a los paquetes encolados para asegurar que la cola de la clase se le da justamente el servicio que requiere.

7. IP RTP Priority (PQ/WFQ)

Proporciona un estricto esquema de prioridad de encolamiento para datos sensibles al retraso, como la voz. El tráfico de voz puede ser identificado por los números del puerto del protocolo de Transporte en Tiempo Real (RTP) y clasificado en una cola de prioridad configurada por el comando ip_rtp_priority. El resultado es que la voz se presenta como prioridad estricta en la preferencia a otro tipo de tráfico.

Con el comando IP RTP Priority se permite especificar un rango de puertos (UDP)/RTP cuyo tráfico tendrá servicio garantizado de prioridad estricta por encima de otras colas o clases que usan la misma interfaz de salida. Los paquetes que existen en la cola de prioridad, son desencolados y enviados primero, antes de los paquetes de otras colas.

Esta característica puede usarse junto con WFQ o CBWFQ en la misma interfaz de salida. En cualquier caso, el tráfico perteneciente al rango de puertos especificados por la cola de prioridad es garantizado con estricta prioridad encima de otras clases CBWFQ o flujos de WFQ; siempre se le da servicio primero a paquetes en la cola de prioridad.

- Cuando es usado junto con WFQ, el comando ip_rtp_priority proporciona prioridad estricta para la voz, y el ordenamiento de WFQ es aplicado a las colas restantes.
- Cuando se usa junto con CBWFQ, el comando ip_rtp_priority proporciona prioridad estricta para la voz. CBWFQ puede usarse para formar clases de otros tipos de tráfico, estos necesitan dedicar ancho de banda y necesitan ser tratados al mejor esfuerzo y no como prioridad estricta; el tráfico que no es voz se le da servicio equitativamente basado en la asignación de pesos a los paquetes encolados.

Puesto que los paquetes de voz son pequeños en tamaño y la interfaz puede tener paquetes grandes que salen, también debe ser configurado Fragmentación del Link y Entrelazando (LFI), en interfaces de baja velocidad. Cuando se habilita LFI, los paquetes grandes son divididos para que los paquetes de la voz pequeños puedan entrelazarse entre los fragmentos de los datos que constituyen un paquete de datos grande. LFI impide que un paquete de voz necesite esperar hasta que un paquete grande sea enviado. En cambio, el paquete de la voz puede enviarse en una cantidad más corta de tiempo.

Puesto que el comando ip_rtp_priority da la prioridad absoluta encima de otro tráfico, debe usarse con cuidado. En caso de congestión, si el tráfico excede el ancho de banda configurado, entonces todo el tráfico en exceso será desechado. El comando ip_rtp_priority y el comando ip_rtp_reserve, no pueden ser configurados en la misma interfaz. Necesita un mecanismo de Control de Acceso de Llamada (CAC), para proteger a PQ de sobre suscripción.

8. Frame Relay IP RTP Priority

Proporciona un esquema de encolamiento de prioridad estricto en un circuito virtual permanente (PVC) de Frame Relay, para datos sensibles retraso como la voz.

El tráfico de voz puede ser identificado por los números del puerto del protocolo de Transporte en Tiempo Real (RTP) y clasificado en una cola de prioridad configurada por el comando frame_relay_ip_rtp_priority. El resultado es que presenta una prioridad estricta en preferencia a otro tráfico.

Permite especificar un rango de puertos UDP, cuyo tráfico de voz es un servicio garantizado de prioridad estricta, sobre cualquier otra cola o clases que usan la misma interfaz de salida. Los paquetes que pertenecen a la cola de prioridad, son desencolados y enviados primero, antes de los paquetes que están en otras colas.

Los datos sensibles a retrasos tienen un trato preferente encima de otro tipo de tráfico. Este proceso ha realizado en una base de per-PVC, en lugar del nivel del la interfaz.

Puesto que el comando frame_relay_ip_rtp_priority da prioridad absoluta encima de otro tráfico, debe usarse con cuidado. En caso de congestión, si el tráfico excede el ancho de banda configurado, entonces todo el tráfico de exceso será desechado. Por consiguiente, alguna forma del Control de Acceso de Llamada (CAC), puede ser usado para prevenir la sobre admisión del PQ.

9. Low Latency Queuing (LLQ) o (PQ-CBWFQ)

Provee encolamiento con prioridad para CBWFQ, reduciendo el jitter en conversaciones de voz. Configurado con el comando priority, LLQ habilita el uso de una sola pila con prioridad dentro de CBWFQ para el nivel de la clase.

Para encolar una clase de tráfico para la cola de prioridad, se configura el comando priority para la clase después se especifica el nombre de la clase dentro del mapa de monitoreo (policy map). Dentro del mapa de monitoreo se pueden dar una o más estados a las clases de prioridad, todo el tráfico de estas clases es encolado hacia la misma y única cola de prioridad.

Los beneficios que se obtiene son configuraciones coherentes y opera a través de todos los tipos de medios: Frame Relay, ATM, líneas arrendadas. Además el criterio de admisión para una clase puede ser definida por un ACL. No limitado por puertos UDP como IP RTP Priority. Garantiza límites confiables que están definidos para garantizar una simple clasificación y entrada a la cola.

4.4 Mecanismos para eficientar el uso del Ancho de Banda (Bw)

Antes de empezar a describir dichos mecanismos, debemos definir el retardo de serialización, que es simplemente el tiempo que toma en colocar bits sobre un circuito.

Existen algunos mecanismos que mediante el encolado y el conformado del tráfico proporcionan eficiencia y predicción, tales como:

1. LFI (Link Fragmentation and Interleaving): Fragmentación e intercalado de enlaces.
2. MPL Interleaving (LFI for Multilink PPP Media). LFI para medios PPP multienlace.
3. FRF. 12 (LFI for Frame Relay data PVCs). LFI para PVC de datos en Frame Relay.
4. FRF. 11 Annex C (LFI for Frame Relay VoFR PVCs).). LFI para PVC de VoFR en Frame Relay.
5. CRTP (Compression for Real Time Protocol): Compresión del encabezado para el Protocolo de tiempo real.

A continuación se describe más a profundidad cada uno de estos:

1. LFI (Fragmenting and Interleaving IP Traffic)

El tráfico interactivo, tal y como Telnet, voz sobre IP, es susceptible a aumentos de latencia y jitter cuando la red tiene que procesar paquetes grandes (por ejemplo un paquete de LAN a LAN vía FTP atravesando un enlace WAN), sobre todo si necesitan ser encolados en enlaces de red menores. LFI reduce el retardo y el jitter en los enlaces de menor velocidad rompiendo los paquetes grandes y entrelazando los paquetes de menor retardo obteniendo así paquetes más pequeños.

Esta herramienta fue diseñada especialmente para enlaces de poca velocidad en los que el retardo al serializar es significativo. LFI es equivalente al borrador del IETF denominado Multiclass Extensions to Multilink PPP (MCML).

2. MLP Interleaving

MLP proporciona un método de cortar y recombinar datagramas de secuencia a través de enlaces de datos lógicos múltiples.

El esquema de LFI es relativamente simple: Los datagramas grandes son encapsulados en multienlaces (multilink) y fragmentados en paquetes de un tamaño pequeño suficiente para

satisfacer los requisitos de retardo del tráfico sensible al retardo; los paquetes pequeños sensibles al retardo no son encapsulados en multilinks, pero son entrelazados entre los fragmentos de datagramas grandes.

MLP permite la fragmentación de paquetes para ser enviados al mismo tiempo sobre múltiples enlaces punto a punto a la misma dirección remota. Los múltiples links aparecen en respuesta a un umbral de carga de marcador que se define. La carga puede calcularse en el tráfico entrante, el tráfico que sale, o en cualquiera de los dos, casi tan necesitado para el tráfico entre los sitios específicos. MLP proporciona el ancho de banda en demanda y reduce la latencia de transmisión a través de los links WAN.

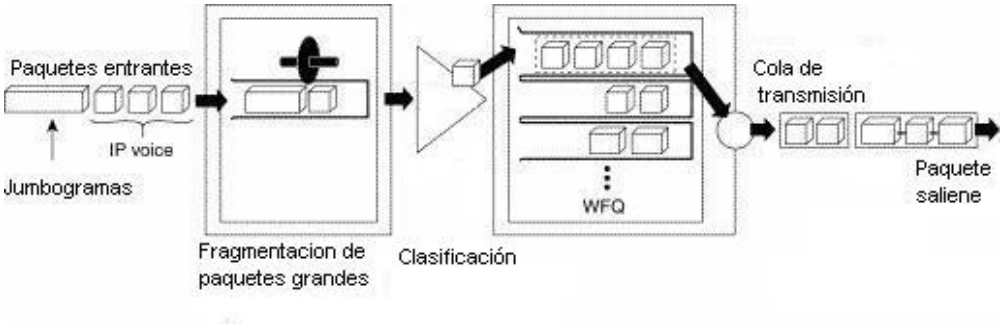

Fig. 4.6. Mezcla de tráfico.

La figura muestra la mezcla de tráfico destinada para una interfaz, los cuales incluyen tanto jumbogramas como pequeños datagramas, paquetes de voz IP sensibles al tiempo. Basado en sus clasificaciones, estos paquetes entrantes son clasificados dentro de las colas. Después de que los paquetes son encolados, los jumbogramas son fragmentados en paquetes más pequeños, como un paso antes para entrelazarlos con los paquetes de voz IP sensibles al tiempo. Puesto que WFQ se configura para la interfaz, los paquetes de cada cola son entrelazados y organizados (equitativamente y basado en su peso) para la transmisión en la salida de la cola de la interfaz.

Para asegurar el orden correcto de transmisión y reensamblaje, LFI agrega encabezados del multilink a los fragmentos del datagrama después de que los paquetes son los desencolados y listos para ser enviados.

3. Fragmentación Frame Relay FRF.12

FRF.12 es un acuerdo de implementación definida para soportar voz y otros datos en tiempo real sensibles a retardo en enlaces de baja velocidad. Acomoda las variaciones en los tamaños del frame en una manera que permite una mezcla de datos de tiempo real y datos que no requieren tiempo real.

FRF.12 estipula que cuando la fragmentación está activa para un identificador de conexión de link de datos (DLCI), sólo los datos del frame que exceden el tamaño de fragmentación especificado, serán fragmentados. Este arreglo permite que pequeños paquetes de voz sobre IP (VoIP), los cuales no son fragmentados debido a su tamaño, sean entrelazados con frames entre paquetes de datos grandes que se han sido fragmentados dentro de frames menores. Esto mejora el retardo de serialización para paquetes que dejan el enrutador y previene que los paquetes de voz esperen a que los paquetes grandes sean procesados.

En una implementación de VoIP, Frame Relay (protocolo de capa 2) no puede distinguir entre VoIP y frames de datos. FRF.12 fragmenta todos los paquetes grandes como el tamaño del fragmento puesto (setting).

4. Fragmentación Frame Relay FRF.11 Anexo-C

Una implementación Voz sobre Frame Relay (VoFR) usa el FRF.11 para definir cómo se encapsulan los datos y la voz en Frame Relay DLCI. De esa manera, datos, fax y voz usan la encapsulación de FRF.11 cuando se envían en un DLCI que lleva voz.

FRF.11 mezcla éstos tipos de tráfico en un DLCI definiendo los subcanales (identificado por las IDs de los canales) dentro del DLCI. Cada subcanal tiene un campo de encabezado que describe el tipo de frame de carga útil. Hasta 255 subcanales pueden ser especificados por un DLCI.

FRF.11 Anexo-C Fragmentación

FRF.11 Fragmentación describe la forma en que los datos se llevan en un FRF.11 DLCI (configurado para VoFR). El Anexo-C de FRF.11 incluye una especificación de fragmentación para los subcanales de datos.

Solo se fragmentan los frames con el tipo de carga útil de datos. Frame Relay distingue los frames de voz de los datos que no requieren tiempo real porque la carga útil de FRF.11 especifica el tipo de tráfico. Por consiguiente, sin tener en cuenta el tamaño de frame de voz, desvía el engine (parte que trata determinados datos) fragmentación.

Fragmentación FRF.12 contra FRF.11

Hay varias formas reconocidas de fragmentación FR.

- La fragmentación FRF.11 Anexo-C: Usado en DLCIs configurada para VoFR.
- La fragmentación de FRF.12: Usado en DLCIs que lleva lo tráfico de datos (FRF.3.1), incluso VoIP. Los paquetes de VoIP son considerados los datos por la capa 2 del protocolo de FR.

Hay un concepto de de equivocación común que la fragmentación de FRF.12 se usa para soportar VoFR, y un desconocimiento general que FRF.11 también especifica un esquema de fragmentación. Esta confusión resulta en malentendido sobre la fragmentación para VoFR y VoIP sobre FR. La siguiente lista pone en claro algunas diferencias cruciales:

- Un Frame Relay DLCI ejecuta cualquiera FRF.12 o FRF.11. Nunca ambos, ellos son mutuamente exclusivos.
- Si el DLCI se configura para VoFR, este usa FRF.11. Si la fragmentación está encendida para este DLCI, esta usa el Anexo-C de FRF.11 para los encabezados de fragmentación.
- Si el DLCI no se configura para VoFR, este usa la encapsulación de datos FRF.3.1. Si la fragmentación está activa para este DLCI, usa FRF.12 para los encabezados de fragmentación. DLCIs que llevan VoIP usan la fragmentación FRF.12 porque VoIP es una tecnología de capa 3 que es transparente a la capa 2 de FR.
- VoIP y VoFR pueden ser soportados en diferentes DLCIs en la misma interfaz, pero no en el mismo DLCI.
- FRF.12 fragmenta los paquetes de voz si el parámetro de tamaño de fragmentación se pone a un valor menor que el tamaño de paquete de voz. El Anexo-C de FRF.11 (VoFR) no fragmenta los paquetes de la voz a pesar qué el tamaño de fragmentación es configurado.
- El Anexo-C de FRF.11 sólo necesita ser soportado por plataformas que soportan VoFR. Porque FRF.12 se usa predominantemente para VoIP, es importante para soportar FRF.12

como una característica general en plataformas Cisco IOS que transportan VoIP sobre enlaces WAN de velocidad lenta (más lento que 1.5Mbps).

5. CRTP. Comprensión del encabezado del protocolo de transporte de tiempo real. Aumentando la eficiencia del tráfico en Tiempo Real.

El Protocolo de Transporte en Tiempo Real es un protocolo host-to-host usado para llevar las nuevas aplicaciones multimedia, incluyendo audio y vídeo, sobre redes IP. RTP proporciona funciones de transporte de red extremo a extremo para las aplicaciones citadas.

Esta compresión ayuda a RTP a ejecutarse más rápidamente, sobre todo en enlaces de menor velocidad, al comprimir la cabecera de RTP/IP/DP de 40 bytes al rango "de 2 a 5". Esto es muy beneficioso para los paquetes más pequeños (como el tráfico de voz sobre IP) en uniones lentas (385 Kbps y menores), donde la compresión puede reducir significativamente el retraso.

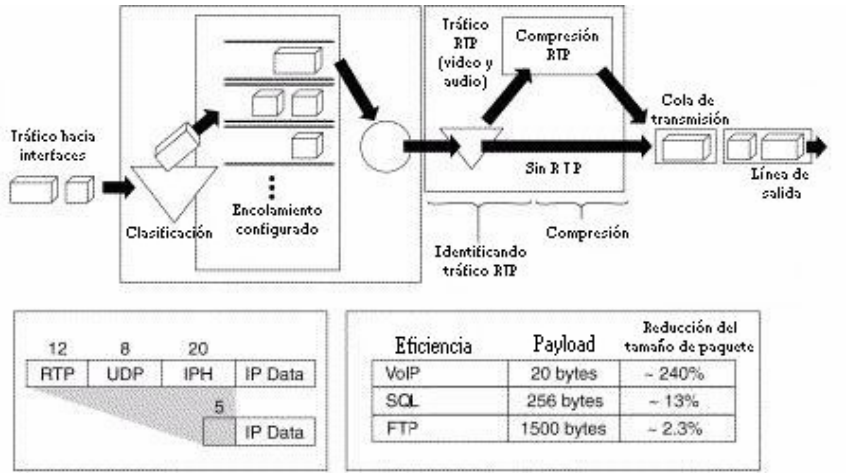

Fig.4.7. CRTP.

La parte del encabezado de RTP es considerablemente grande. Los 12 bytes mínimos del encabezado de RTP, combinada con 20 bytes de encabezado de IP (IPH) y 8 bytes de encabezado de UDP, crea un encabezado de 40-byte de IP/UDP/RTP. Para las aplicaciones audio de carga útil comprimida, el paquete RTP tiene típicamente de 20-byte a 160-byte de carga útil. Dado el tamaño del encabezado de la combinaciones IP/UDP/RTP, es ineficiente enviar el encabezado de IP/UDP/RTP sin comprimirlo.

Los descompresores pueden reconstruir el encabezado original sin alguna pérdida de información.

CRTP es un esquema de compresión de salto a salto similar a RFC 1144 para compresión de encabezado TCP.

4.5 Mecanismos condicionadores de tráfico

Los mecanismos Shaping y Policing son usados en la red para controlar la tasa de entrada a la red. Ambos mecanismos usan clasificación, así que pueden diferenciar el tráfico.

La diferencia entre Shaping y Policing puede ser descrita en términos de su implementación de rate-limiting:

- Shaping mide la tasa de tráfico y retrasa el tráfico excesivo con el propósito de mantenerla dentro de la tasa límite deseada. Con Shaping, los estallidos de tráfico son aislados causando un flujo de datos regular. Reducir los estallidos de tráfico ayuda a reducir la congestión en el núcleo de la red.
- Policing retira el tráfico excesivo por orden para controlar el flujo dentro de los límites especificados. Policing no introduce ningún retardo al tráfico que se ajusta a políticas de tráfico. Sin embargo, puede causar mas retransmisiones TCP porque el tráfico superior a los límites especificados es retirado.

Ventajas de Rate Limiting

Rate Limiting es usado para satisfacer uno de los siguientes requisitos:

- Prevención y manejo de congestión en redes ATM y Frame Relay, donde anchos de banda asimétricos son usados a lo largo de la ruta de tráfico. Esto impide a las redes de capa 2 retirar grandes cantidades de tráfico por retiros diferentes de tráfico excesivo al entrar en redes ATM o Frame Relay basadas en información de capa 3 (por ejemplo: Prioridad IP, DSCP, listas de acceso, tipo de protocolo, etc.).
- Limitar la tasa de acceso sobre una interfaz cuando una infraestructura física de alta velocidad es usada en el transporte, pero una sub-tasa de acceso es deseada.
- Ingeniería de ancho de banda con el propósito de que la tasa de tráfico para ciertas aplicaciones o clases de tráfico sigan una política de tasa de acceso específica.
- Implementar un sistema TDM virtual usando una red IP, pero teniendo las características de ancho de banda de un sistema TDM (ancho de banda disponible máximo fijo). Policing entrante y saliente puede ser usado, por ejemplo, en un router para compartir un solo enlace punto a punto en dos o mas enlaces punto a punto virtuales para asignar una parte del ancho de banda a cada clase, por lo tanto impedir la monopolización del enlace en cualquier dirección.

Aplicaciones de Rate Limiting

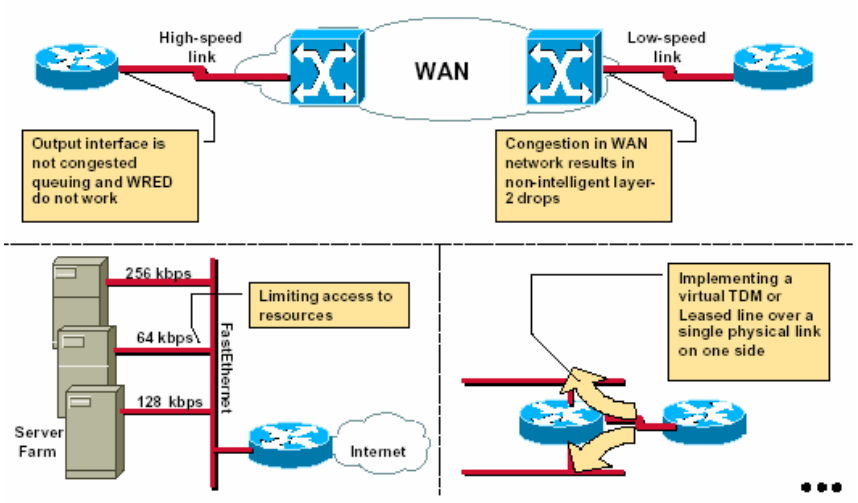

Fig. 4.8. Aplicaciones de Rate Limiting.

La figura 4.8 muestra tres posibles aplicaciones de mecanismos de Rate Limiting (Shaping o Policing). La primer figura muestra una WAN de capa 2 con anchos de banda de enlace diferentes a lo largo de una ruta de capa 3. La entrada a la red (izquierda) tiene un enlace de alta velocidad disponible en el backbone de capa 2, que le permite enviar tráfico a una tasa alta. En el equipo de salida, el tráfico enviado llega a un enlace de baja velocidad, y la red de capa 2 es forzada a retirar una grán cantidad de tráfico. Si el tráfico fuera Rate Limiting en la entrada, ocurre un flujo de tráfico óptimo, resultando en un retiro mínimo dropping en la red de capa 2.

La segunda figura muestra una granja de servidores, que es accesible desde internet por un enlace compartido. Dependiendo del contrato de servicio, el proveedor de hosting puede ofrecer diferentes anchos de banda garantizados a los clientes, y puede limitar los recursos que un servidor especial usa. Rate Limiting puede ser usado para dividir el recurso compartido (enlace de subida) entre muchos servidores.

La tercera figura muestra la opción de implementar líneas arrendadas virtuales sobre una infraestructura de capa 3, donde el ancho de banda reservado de tasa limitada está disponible sobre un enlace compartido.

Shaping vs. Policing

Shaping

Retrasa el tráfico excesivo usando un buffer, o mecanismo, para detener paquetes y dar forma al flujo cuando la tasa de datos del origen es mayor de la esperada. Incrementa la utilización del buffer en un router pero causa retraso no determinista de paquetes. También puede interactuar con una red Frame Relay, se adapta a las señales de congestión de capa 2 en la WAN.

Policing

- Retira el tráfico que no se ajusta a las reglas.
- Soporta marcación de tráfico.
- Es mas eficiente en términos de utilización de memoria (no necesita buffer adicional).
- No incrementa el uso del buffer.

Tanto Shaping como Policing aseguran que el tráfico no exceda un límite de ancho de banda, pero tienen impactos diferentes sobre el tráfico:

- Policing retira paquetes más a menudo, generalmente causando mas retransmisión de protocolos orientados a conexión.
- Shaping añade retardo variable al tráfico, causando posiblemente jitter.

Medición de la tasa de tráfico

Para llevar a cabo Rate Limiting, los routers deben medir tasas de tráfico a través de sus interfaces. Para imponer una tasa límite, el tráfico medido es marcado para:

- Ajustar a la tasa límite, si la tasa de tráfico es menor o igual a la tasa límite configurada.
- Exceder la tasa límite, si la tasa de tráfico está por encima de la tasa límite configurada.

La medición es llevado a cabo generalmente con un modelo abstracto llamado Token Bucket, que es usado cuando se procesa cada paquete. Token Bucket puede calcular si el paquete actual se ajusta o excede la tasa límite en una interfaz.

Token Bucket

Token Bucket (Balde de Fichas) es un modelo matemático usado en un dispositivo que regula el flujo de datos. El modo tiene dos componentes básicos:

- Tokens (fichas): donde cada ficha representa el permiso de enviar un número fijo de bits en la red.
- Bucket (balde): que tiene la capacidad de contener una cantidad específica de fichas.

Las fichas son puestas en el balde a una cierta tasa por el sistema operativo. Cada paquete, si se envía, toma fichas del balde, representando el tamaño del paquete.

Si el balde se llena por completo, las fichas recién llegados son descartados. Las fichas descartadas no estarán disponibles para los futuros paquetes.

Si no hay suficientes fichas en el balde para enviar el paquete, el regulador puede:

- Esperar que suficientes fichas se acumulen en el balde (Traffic Shaping).
- Descartar el paquete (Policing).

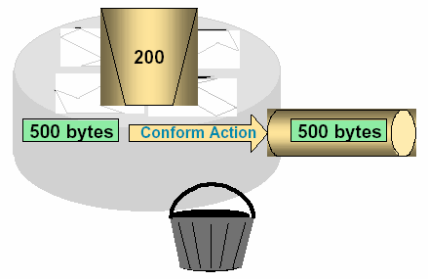

Fig. 4.9. Token Bucket.

La figura muestra un balde, con una capacidad actual de 700 bytes. Cuando un paquete de 500 bytes llega a la interfaz, éste tamaño es comparado con la capacidad del balde (en bytes). El paquete se ajusta a la tasa límite (500 bytes < 700 bytes), y el paquete es enviado. 500 fichas son sacadas del balde dejando 200 fichas para el siguiente paquete.

Cuando el siguiente paquete llega inmediatamente después del primer paquete, y ninguna nueva ficha ha sido añadida al balde (lo cual es hecho periódicamente), el paquete excede la tasa límite. El tamaño del paquete es mayor que la capacidad actual del balde, entonces se puede descartar el paquete (policing) o esperar a que suficientes fichas se acumulen en el balde (traffic shaping).

La implementación de Token Bucket generalmente depende de tres parámetros: CIR, Bc y Be.

CIR es la Tasa de Información Prometida (también llamada Tasa Prometida o shaped rate). Bc es conocido como capacidad de reviente (burst capacity). Be esconocido como capacidad de reviente excesiva (excess burst capacity). Tc es n intervalo constante que representa el tiempo. Un número Bc de fichas es enviado sin restricción en cada intervalo Tc.

En la metáfora del Token Bucket, las fichas son puestos en el balde a cierta tasa, esto es Bc fichas cada Tc segundos. El balde mismo tiene una capacidad específica. Si el balde se llena por completo (Bc + Be), este se inundará y por lo tanto las fichas recién llegadas son descartadas. Cada ficha concede el permiso a una fuente para enviar un cierto número de bits en la red.

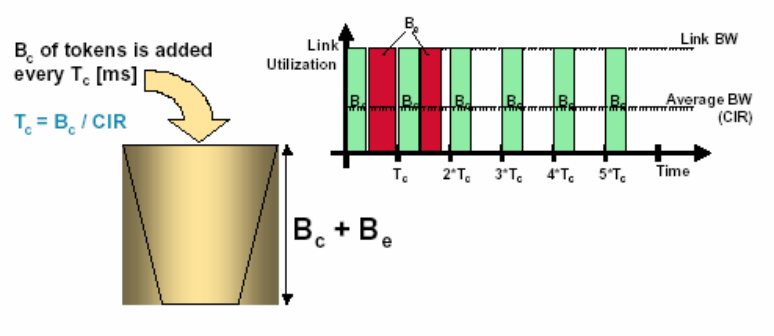

Fig. 4.10. Parámetros CIR, Bc y Be.

Por ejemplo, si el equivalente en fichas a 8000 bytes son puestos en el balde cada 125 milisegundos, el router puede transmitir regularmente 8000 bytes cada 125 milisegundos, si el tráfico llega al router constantemente.

Si no hay tráfico en absoluto, 8000 bytes por 125 milisegundos son acumulados en el balde, hasta el tamaño máximo (Bc + Be). La acumulación en un segundo, por lo tanto, reúne el equivalente en fichas a 64000 bytes, que pueden ser transmitidos inmediatamente en caso de reviente. El límite superior, Bc + Be, define la máxima cantidad de datos que pueden ser transmitidos en un solo reviente, en la tasa de línea.

El mecanismo Token Bucket usado para Traffic Shaping tiene tanto un balde como una "cola" usados para retardar paquetes. Si el Token Bucket no tuviera un buffer de datos, sería un mecanismo de policing. Para Traffic Shaping, paquetes que llegan y no pueden ser enviados inmediatamente (porque no hay fichas suficientes en el balde) están retrasados en el buffer.

Aunque Token Bucket permite desborde, los estallidos de tráfico están unidos. Esta garantía es hecha con el propósito de que el flujo de tráfico nunca transmitirá más rápido que la capacidad del Token Bucket. Esto significa que la tasa de transmisión no excederá la tasa establecida en que las fichas son puestas en el balde (la tasa prometida).

La siguiente tabla muestra los mecanismos Token Bucket basados en Rate Limiting disponibles en el IOS de Cisco.

Shaping	Policing
Generic Traffic Shaping	Committed Access Rate
Frame Relay Traffic Shaping	Class-based Policing
Class-based Shaping	

Tabla 4.3. Mecanismos Token Bucket basados en Rate Limiting.

Generic Traffic Shaping (GTS)

GTS da forma al tráfico reduciendo el flujo de tráfico de salida para evitar la congestión. Esto se logra restringiendo el tráfico a una tasa de bit particular usando el mecanismo Token Bucket. GTS es aplicado sobre la base de la interfaz y puede usar listas de acceso para seleccionar el tráfico que forme. Funciona en varias tecnologías de capa 2, incluyendo Frame Relay, ATM, SMDS (Switched Multi-megabit Data Service) y Ethernet.

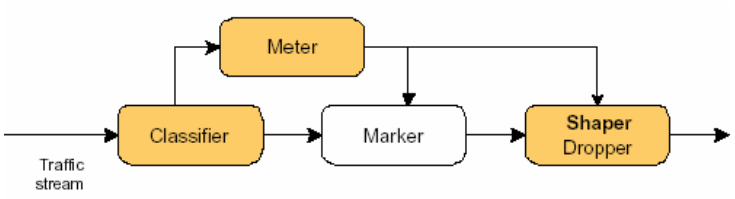

Fig. 4.11. Diagrama de bloques de GTS.

Como se muestra en el diagrama de bloques, GTS efectúa tres funciones básicas:

- Clasificación de tráfico, para que diferentes clases de tráfico puedan tener políticas diferentes aplicadas a ellos.
- Medición, usando un mecanismo Token Bucket, para distinguir cuando se ajusta y cuando se excede el tráfico.
- Shaping, usando buffer, para retardar el tráfico excedente y darle forma a la tasa límite configurada.

Componentes básicos de GTS

GTS es implementado como un mecanismo de encolamiento, donde hay colas de retardo de WFQ distintas para casa clase de tráfico. Cada cola WFQ retrasa paquetes hasta que se ajusten a la tasa límite, y también los programas de acuerdo con el algoritmo WFQ. El tráfico ajustado es enviado entonces por la interfaz física.

Los paquetes que llegan primero son clasificados en una de las shaping classes. El tráfico que no se clasifica en alguna clase no se le aplica el shaping. La clasificación puede ser implementada usando listas de acceso.

En cuanto un paquete es clasificado en una shaping class, su tamaño es comparado con la cantidad de fichas disponibles en el balde de esa clase. El paquete es enviado a la cola de la interfaz principal si hay suficientes fichas. Un número de fichas sacadas del balde es igual al tamaño del paquete (en bytes).

Si, por otro lado, no hay suficientes fichas para enviar el paquete, el paquete se guarda en el buffer del sistema WFQ asignado a esta shaping class. El router rellena periódicamente el balde y verifica si hay suficientes fichas para enviar uno o mas paquetes fuera de la shaping queue. Los paquetes son programados fuera de la shaping queue de acuerdo con el algoritmo de planificación de WFQ.

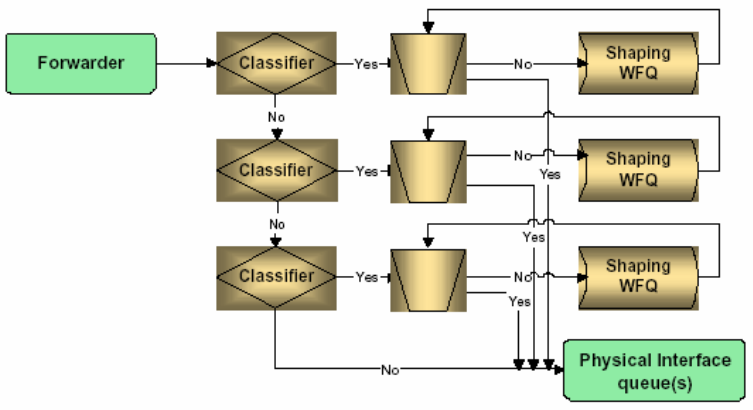

Fig. 4.12. Componentes básicos de GTS.

Frame Relay Traffic Shaping

FRTS puede eliminar los obstáculos en redes Frame Relay que tienen conexiones de alta velocidad en el sitio central y conexiones de baja velocidad en las ramificaciones. El forzamiento de tasa (rate enforcement) puede ser configurado para limitar la tasa a la que los datos son enviados sobre los VC (Circuitos Virtuales) en el sitio central.

Usando FRTS, rate enforcement puede ser configurado para el CIR o algún otro valor definido como la tasa de excesiva de información en la base del VC. La habilidad de permitir que la velocidad de transmisión utilizada por el router sea controlada por los criterios aparte de la velocidad de línea (es decir, por el CIR o por la tasa excesiva de información) proporciona un mecanismo para compartir medios por múltiples VCs. El ancho de banda puede ser asignado por el VC, creando una red virtual TDM (Multiplexación por División de Tiempo).

PQ(encolamientos preferenciales), CQ (encolamientos normales) y WFQ (encolamientos de pesado expuesto) también pueden ser definidas en el VC o nivel de subinterface. Usar estos métodos de encolamiento permite tener mas control sobre el flujo de tráfico en un VC individual. Si CQ es combinado con el encolamiento del VC y la capacidad de ejecución de la tasa, los VCs de Frame Relay están habilitados para llevar múltiples tipos de tráfico, como IP, SNA e IPX, con el ancho de banda garantizado para cada tipo de tráfico.

Usando información contenida en los paquetes recibidos de la red etiquetados por BECN, FRTS también puede estrangular el tráfico enérgicamente. Con el estrangulamiento basado en BECN, los paquetes son puestos en el buffer del router para reducir el flujo de datos al router en la red Frame Relay. El estrangulamiento está listo sobre la base del VC y la tasa de transmisión es ajustada basándose en el número de paquetes recibidos etiquetados por BECN.

Componentes básicos de FRTS

En el diagrama de bloques, se muestra la operación de FRTS sobre una interfaz física de Frame Relay. No hay pre-clasificación global del tráfico, pero los paquetes son enviados a su VC individual. Shaping es llevado a cabo sobre la base del VC, con un shaping Token Bucket / Cola separado para cada VC. Paquetes que salen de sus shapers de cada VC individuales son enviados a la interfaz física de cola (cola de Tx / anillo de Tx).

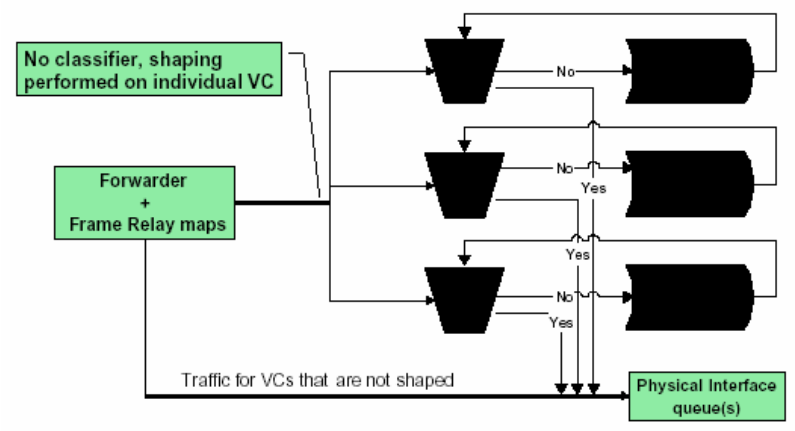

Fig. 4.13. Componentes básicos de FRTS.

FRTS es una implementación de shaping que soporta múltiples protocolos. A diferencia de GTS que efectúa una planificación basada en WFQ en la entrada del shaper con un mecanismo de planificación arbitrario sobre la interfaz física. FRTS lleva a cabo sus operaciones al contrario.

FRTS solo puede ser configurado sobre la salida de una interfaz.

La siguiente tabla muestra una comparación entre GTS y FRTS.

Generic Traffic Shaping (GTS)	Frame Relay Traffic Shaping (FRTS)
Trabaja en cualquier (sub)interfaz.	Trabaja solo sobre Frame Relay.
Forma el tráfico sobre la base de la (sub)interfaz.	Forma el tráfico de circuitos virtuales individuales.
Cualquier interfaz física de colas puede ser usada.	Sólo WFQ puede ser usado sobre una interfaz física.
Sólo WFQ puede ser usado para la formación de la cola.	CQ, PQ o WFQ pueden ser usados en la formación de la cola.

Tabla 4.4. Comparación entre GTS y FRTS.

Commited Access Rate (CAR)

CAR proporciona la capacidad de permitir que el proveedor de servicios limite la tasas de tráfico dentro y fuera de las interfaces del router, así, permite varias formas de limitar la tasa de entrada y salida en una red. CAR es un mecanismo de policing, no un mecanismo de colas. Por lo tanto, no retarda ni guarda paquetes en un buffer, lo cual puede o no ajustarse a las políticas, pero sólo limita la tasa de acuerdo con una política simple de “forward or drop”, de acuerdo con la configuración. CAR también usa un mecanismo de medición Token Bucket, similar a GTS, pero sin una cola de retardo.

La característica de CAR de limitar la tasa maneja la política de ancho de banda de acceso de una red asegurando que el tráfico enviado cae dentro de los parámetros de tasa especificados,. Mientras retira paquetes que exceden la cantidad aceptable de tráfico o enviándolos con una prioridad diferente. CAR a menudo es configurado sobre interfaces en el borde de una red para limitar el tráfico dentro o fuera de la red.

CAR puede ser usado para marcar paquetes. El operador puede determinar una política que determina qué paquetes deben ser asignados a qué clase de tráfico, y usar CAR para implementar el marcado. El encabezado de IP ya proporciona un mecanismo para hacer esto, son los tres bits de prioridad en el campo ToS del encabezado de IP. CAR permite la configuración de políticas, basándose en la información del encabezado de IP o TCP como dirección IP, puerto de aplicación, puerto físico o subinterfaz, protocolo IP, etc. para decidir como deben ser marcados o “coloreados” los bits de prioridad. Una vez marcados, un tratamiento apropiado puede ser dado en el backbone para asegurar que los paquetes premium reciben un servicio premium en términos de asignación de ancho de banda, control de retardo, etc.

CAR es implementado usando los siguientes mecanismos abstractos:

- El clasificador, que diferencia el tráfico en múltiples clases, que puede ser tratado de una manera discriminatoria.
- El medidor, que usa un esquema Token Bucket para medir la tasa de tráfico clasificado.
- El marcador, que puede ser usado para marcar o remarcar el tráfico clasificado (por ejemplo, que valores de prioridad o DSCP).

- El gotero, que puede dejar caer paquetes (en caso de tasa limitada) de acuerdo con la política configurada.

CAR puede ser configurado sobre las interfaces de entrada o salida de un router. Cuando se configura sobre el equipo de entrada, CAR es procesado usualmente al final de una serie de mecanismos de QoS. Por lo tanto limitar la tasa y el marcado ocurren justo antes de la decisión de envío.

En el equipo de salida, CAR es procesado justo después de la decisión de envío. Por lo tanto, todos los mecanismos QoS de salida (colas, WRED, etc.) son procesados generalmente después del CAR.

La función básica de CAR para limitar la tasa hace lo siguiente:

- Permite el control de la tasa máxima transmitida o recibida en una interfaz.
- Provee la habilidad de definir el agregado de capa 3 o los límites de tasa granulares y especificar políticas de manejo de tráfico tampoco se ajusta o excede los límites especificados de tasa.
- Usa límites de tasa en ancho de banda granulares que correspondan a un tipo de tráfico particular basándose en la prioridad, dirección MAC, o otros parámetros.

Cuando CAR está vigente, el tráfico es primero clasificado y luego pasa al procesamiento CAR. Entonces CAR mide el tráfico y basándose en los resultados de las mediciones, el tráfico se ajusta o supera las política configurada.

Hay tres acciones básicas posibles sobre cada paquete, dependiendo de si se ajusta o supera la política configurada:

- Transmisión: el paquete es enviado.
- Retirar: el paquete es descartado.
- Continuar: el paquete es evaluado usando la siguiente política de tasa en una cadena de límites de tasa. Si no hay otra política de tasa, el paquete es enviado.

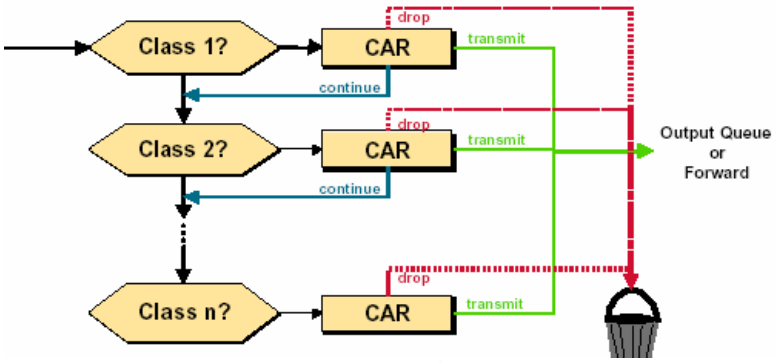

Fig. 4.14. Funcionamiento básico de CAR.

Como se dijo previamente, CAR puede ser usado para marcar o remarcar el tráfico además de efectuar limitaciones de tasa. Dependiendo de la conformidad del tráfico, la siguiente acción de marcar/remarcar se puede efectuar dentro del proceso CAR:

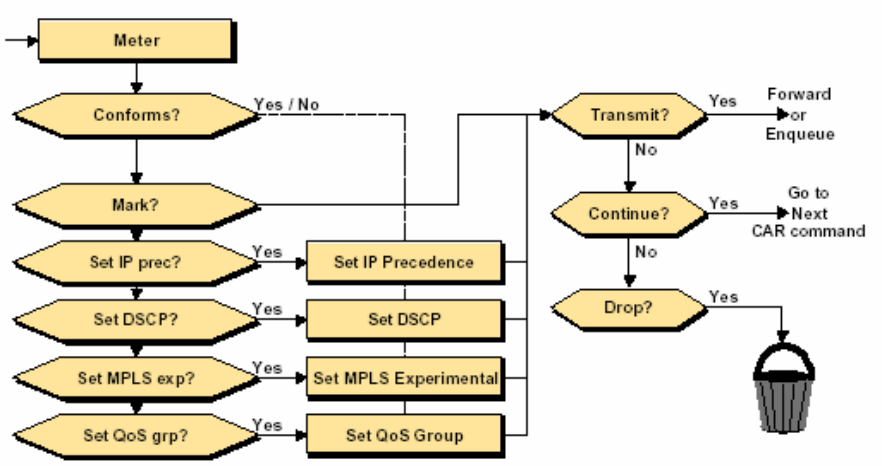

Fig. 4.15. Acción de marcar/remarcar dentro del proceso CAR.

- *Fijar la prioridad (o valor DSCP) y transmitir.* La Prioridad IP (ToS) o bits DSCP en el encabezado del paquete son reescritos. Entonces el paquete es enviado. Esta acción puede ser usada para marcar (fijar la prioridad) o remarcar (modificar la prioridad de paquete existente) el paquete.
- *Fijar los bts experimentales de MPLS y transmitir.* Los bits experimentales de MPLS pueden ser fijados. Éstos son usualmente usados para indicar parámetros de QoS en una nube MPLS.
- *Fijar el grupo de QoS y transmitir.* El grupo de QoS puede ser fijado. Esto es usado solamente a nivel local dentro del router. El grupo de QoS puede ser usado en mecanismos QoS posteriores y llevado a cabo en el mismo router, como CB-WFQ.

4.6 Mecanismos de Control de Admisión de llamada

El control de admisión determina si una petición de conexión puede ser llevada a cabo por la red. Los algoritmos determinan la apropiada asignación de recursos para un nuevo flujo (si este es admitido), tales como los servicios garantizados y la QoS requerida para que un nuevo flujo sea satisfecho.

Las principales consideraciones tras esta decisión son la carga del tráfico actual, la QoS que se puede lograr, el perfil de tráfico pedido, la QoS solicitada, el precio. Los servicios garantizados pueden ser cuantitativos (garantizar tasa o retardo definido) o cualitativos (retardo promedio bajo).

Esta herramienta es, por lo tanto, aplicación de una política de calidad de servicio definida en la empresa. Requiere, a su vez, una correcta monitorización del sistema que nos permita visualizar en cada momento el estado del mismo para poder aplicar esa política de admisión.

Hay tres estrategias básicas para el control de admisión de llamada:

1. CAC local.
2. Resource-Based Mechanisms
3. Measurement-Based Mechanisms

Los cuales se mencionan a continuación:

1. CAC Local

Los mecanismos Local CAC funcionan en la salida del gateway. La decisión de CAC está basada en la información nodal tal como el estado del link saliente LAN o WAN. Si el paquete de enlace de una red local (local packet net link) está roto, no hay ningún sitio ejecutando la decisión lógica compleja basada en el estado del resto de la red, porque esa red es inalcanzable. Los mecanismos locales incluyen los detalles de la configuración para imposibilitar más de un número fijo de llamadas.

2. Control de Admisión basado en recursos (resource-based mechanisms)

Hay dos tipos de mecanismos basados en recursos: aquéllos que calculan los recursos necesitados y/o disponibles, y aquellos que reservan recursos para la llamada. Los recursos de interés incluyen el ancho de banda del enlace (link), slots de tiempo DSPs y DS0 en los troncales de conexión TDM, poder del CPU y memoria. Algunos de estos recursos podrían ser obligados en absoluto a uno o más de los nodos de la llamada que atravesará su destino.

Cuando un flujo requiere servicio de tiempo real, este puede ser distinguido para que la red pueda tomar la decisión en el control de admisión.

3. Control de Admisión basado en monitoreo (measurement-based mechanisms)

Las técnicas basadas en la medición CAC miran hacia adelante en la red de paquetes para calibrar (o medir) el estado de la red con el propósito de determinar como permitir una nueva llamada. Evaluando el estado de la red sugiere enviar pruebas al destino con la dirección IP (normalmente el gateway terminando o terminando el gatekeeper) la que regresará al gateway saliente con alguna información (medida) sobre las condiciones de la prueba encontrada mientras atravesó la red hacia el destino. Típicamente, pérdidas y características de retardo son los elementos interesantes de información para voz.

5 Requerimientos y baseline de la red de datos a analizar

La topología de la red RC-JC* está basada en un modelo jerárquico de tres niveles: Dorsal, Distribución y Acceso. Compuesta en su totalidad por enrutadores Cisco.

1. *Nivel Dorsal.* Constituye la parte de la red que se encarga del transporte de datos a alta capacidad, dada su criticidad para la conectividad en la empresa, cuenta con componentes redundantes, es altamente confiable y es capaz de adaptarse a cambios rápidamente.

2. *Nivel de Distribución.* El nivel de distribución realiza funciones de transporte de tráfico, siendo su capacidad de ancho de banda mediana respecto al ancho de banda implementado en el nivel dorsal. Para mantener un alto nivel de desempeño en la dorsal, el nivel de distribución puede hacer redistribución de información de enrutamiento entre protocolos de enrutamiento altamente demandantes de recursos usados en el nivel de acceso en algún protocolo optimizado para el nivel dorsal. Por la criticidad que representa este nivel, los equipos a usarse deberán ser altamente confiables y robustos.

3. *Nivel de Acceso.* Concentra, distribuye y direcciona la información del usuario de la red, es propiamente el acceso del usuario a la red. Permite la aplicación de políticas de administración, cifrado, encapsulamiento y enrutamiento de tráfico sin comprometer el desempeño global de la red.

Ventajas del Modelo Jerárquico

Este modelo permite la asignación de funciones específicas para cada nivel, con lo cual se tienen las siguientes ventajas:

Administración:

- Facilidad de control de configuraciones en enrutadores al ser similares.
- Predicción del comportamiento de la red frente a cambios.
- La separación en redes divisionales permite la identificación y el control del tráfico de las aplicaciones actuales y/o nuevas.

* Por motivos de privacidad no se menciona el nombre de la red ni la compañía a la cual pertenece. Se usará el nombre RC-JC.

Seguridad:

- Control sobre los flujos de tráfico mediante listas de acceso.
- Implementación de filtros por direcciones y/o aplicaciones.
- Definición clara de puntos de interconexión con otras redes y al Internet.

Eficiencia:

- Mejor convergencia de la red.
- Facilita el establecimiento de conectividad entre redes.
- Mejora tiempos de respuesta.
- Facilita el diagnóstico de fallas.

La Red Dorsal

La red dorsal de la RCD (Red Corporativa de Datos) está diseñada para soportar grandes cantidades de tráfico y servicios. La topología en este nivel esta compuesta por dos enrutadores. La red dorsal cuenta con enrutadores de alto desempeño. Es una plataforma que soporta desde 155 Mbps (STM-1) hasta 2.5 Gbps (STM-16) por interfaz.

Red de Distribución

Los enrutadores del nivel distribución están conectados de forma redundante y simétrica a los dos enrutadores dorsales, concentrando ellos mismos una gran cantidad de nodos de acceso en una topología del tipo estrella.

Red de Acceso

Los enrutadores del nivel acceso están conectados a un único nodo distribuidor para su conexión a la WAN, en una topología del tipo estrella.

En la siguiente tabla se muestran los enlaces:

NODO DISTRIBUIDOR	ACCESO	VEL. ENLACE	PTO. DISTRIB.	RED	PTO. ACCESO	RED CLIENTE
DISTRIB_01	NEVADO	E1	.1	172.16.0.0/30	.2	172.16.4.0/24
	VALLE_CHALCO	256k	.5	172.16.0.4/30	.6	172.16.5.0/25
	AMECAMECA	E1	.9	172.16.0.8/30	.10	172.16.6.0/24
	LOS_REYES	E1	.13	172.16.0.12/30	.14	172.16.7.0/24
	NEXTENGO	E1	.17	172.16.0.16/30	.18	172.16.8.0/24
	VALLEJO	E1	.21	172.16.0.20/30	.22	172.16.9.0/24
	IXTAPALUCA	E1	.25	172.16.0.24/30	.26	172.16.10.0/24
Total: 7						
DISTRIB_02	PORTALES	128k	.1	172.17.0.0/30	.2	172.17.4.0/26
	LORETO	E1	.5	172.17.0.4/30	.6	172.17.5.0/24
	COAPA	E1	.9	172.17.0.8/30	.9	172.17.6.0/24
	SAN_JERÓNIMO	E1	.13	172.17.0.12/30	.14	172.17.7.0/24
	CARRASCO	E1	.17	172.17.0.16/30	.18	172.17.8.0/24
	CULHUACAN	E1	.21	172.17.0.20/30	.22	172.17.9.0/24
	MAGDALENA	E1	.25	172.17.0.24/30	.26	172.17.10.0/24
	IZTACCIHUATL	E1	.29	172.17.0.28/30	.30	172.17.11.0/24
	MIXCOAC	E1	.33	172.17.0.32/30	.34	172.17.12.0/24
	ORIENTE	E1	.37	172.17.0.36/30	.38	172.17.13.0/24

	SN_PEDRO_ATOCPAN	E1	.41	172.17.0.40/30	.42	172.17.14.0/24
	XOCHIMILCO	E1	.45	172.17.0.44/30	.46	172.17.15.0/24
Total: 12						
DISTRIB_03	MALINALCO	256k	.1	172.18.0.0/30	.2	172.18.4.0/25
	METEPEC	E1	.5	172.18.0.4/30	.6	172.18.5.0/24
	ALVARO_OBREGÓN	E1	.9	172.18.0.8/30	.9	172.18.6.0/24
	HUIXQUILUCAN	128k	.13	172.18.0.12/30	.14	172.18.4.128/26
	ATLACOMULCO	128k	.17	172.18.0.16/30	.18	172.18.4.192/26
	CONSTITUCIÓN	E1	.21	172.18.0.20/30	.22	172.18.7.0/24
	TIANGUISTENGO	E1	.25	172.18.0.24/30	.26	172.18.8.0/24
	LERMA	E1	.29	172.18.0.28/30	.30	172.18.9.0/24
	MILTEPEC	E1	.33	172.18.0.32/30	.34	172.18.10.0/24
	TOLUCA	E1	.37	172.18.0.36/30	.38	172.18.11.0/24
	TOLLOCAN	E1	.41	172.18.0.40/30	.42	172.18.12.0/24
	VALLE_DE_BRAVO	E1	.45	172.18.0.44/30	.46	172.18.13.0/24
	INDEPENDENCIA	E1	.49	172.18.0.48/30	.50	172.18.14.0/24
	TENANCINGO	E1	.53	172.18.0.52/30	.54	172.18.15.0/24
	ATLACOMILCO	E1	.57	172.18.0.56/30	.58	172.18.16.0/24
Total: 15						
DISTRIB_04	CHIMALHUACAN	E1	.1	172.19.0.0/30	.2	172.19.4.0/24
	STA_MARTHA	E1	.5	172.19.0.4/30	.6	172.19.5.0/24
	MOCTEZUMA	E1	.9	172.19.0.8/30	.9	172.19.6.0/24
	IZTACALCO	256k	.13	172.19.0.12/30	.14	172.19.7.0/25
	TLAHUAC	E1	.17	172.19.0.16/30	.18	172.19.8.0/24
	CUAJIMALPA	E1	.21	172.19.0.20/30	.22	172.19.9.0/24
	FRONTERA	E1	.25	172.19.0.24/30	.26	172.19.10.0/24
Total: 7						
DISTRIB_05	POPOTLA	E1	.1	172.20.0.0/30	.2	172.20.4.0/24
	TACUBA	E1	.5	172.20.0.4/30	.6	172.20.5.0/24
	LA_PERLA	192k	.9	172.20.0.8/30	.9	172.20.6.0/25
	CHAMPA	E1	.13	172.20.0.12/30	.14	172.20.7.0/24
	NAUCALPAN	E1	.17	172.20.0.16/30	.18	172.20.8.0/24
Total: 5						
DISTRIB_06	BALBUENA	E1	.1	172.21.0.0/30	.2	172.21.4.0/24
	CHAMIZAL	192k	.5	172.21.0.4/30	.6	172.21.5.0/25
	SAN_JUAN	E1	.9	172.21.0.8/30	.9	172.21.6.0/24
	AYOTLA	E1	.13	172.21.0.12/30	.14	172.21.7.0/24
	ZARAGOZA	E1	.17	172.21.0.16/30	.18	172.21.8.0/24
	VALLE_GOMEZ	E1	.21	172.21.0.20/30	.22	172.21.9.0/24
	LONDRES	E1	.25	172.21.0.24/30	.26	172.21.10.0/24
	NEZA	E1	.29	172.21.0.28/30	.30	172.21.11.0/24
	TORRES	E1	.33	172.21.0.32/30	.34	172.21.12.0/24
	TLATELOLCO	E1	.37	172.21.0.36/30	.38	172.21.13.0/24
	TLAHUAC	256k	.41	172.21.0.40/30	.42	172.21.5.128/25
	MEYEHUALCO	E1	.45	172.21.0.44/30	.46	172.21.14.0/24
	CUIHUACAN	E1	.49	172.21.0.48/30	.50	172.21.15.0/24
	VIADUCTO	192k	.53	172.21.0.52/30	.54	172.21.16.0/25
Total: 14						
DISTRIB_07	BOSQUES_DEL_LAGO	E1	.1	172.22.0.0/30	.2	172.22.4.0/24
	VILLA_DE_LAS_FLORES	E1	.5	172.22.0.4/30	.6	172.22.5.0/24
	MORELOS	E1	.9	172.22.0.8/30	.9	172.22.6.0/24
	VILLA_NICOLAS	E1	.13	172.22.0.12/30	.14	172.22.7.0/24
	TEOTIHUACAN	E1	.17	172.22.0.16/30	.18	172.22.8.0/24
	OJO_DE_AGUA	256k	.21	172.22.0.20/30	.22	172.22.9.0/25
	ZUMPANGO	E1	.25	172.22.0.24/30	.26	172.22.10.0/24
	IZCALLI	E1	.29	172.22.0.28/30	.30	172.22.11.0/24
	CIUDAD_LABOR	E1	.33	172.22.0.32/30	.34	172.22.12.0/24
	TEPOTZOTLAN	E1	.37	172.22.0.36/30	.38	172.22.13.0/24
Total: 10						
DISTRIB_08	PORTALES	E1	.1	172.23.0.0/30	.2	172.23.4.0/24
	MIXCOAC	128k	.5	172.23.0.4/30	.6	172.23.5.0/26

	PICACHO	E1	.9	172.23.0.8/30	.9	172.23.6.0/24
	SAN_ANGEL	E1	.13	172.23.0.12/30	.14	172.23.7.0/24
	URRAZA	E1	.17	172.23.0.16/30	.18	172.23.8.0/24
	SARO	E1	.21	172.23.0.20/30	.22	172.23.9.0/24
	CUAJIMALPA	E1	.25	172.23.0.24/30	.26	172.23.10.0/24
	NEXTENGO	E1	.29	172.23.0.28/30	.30	172.23.11.0/24
	SAN_JERÓNIMO	E1	.33	172.23.0.32/30	.34	172.23.12.0/24
	SANTA_LUCIA	E1	.37	172.23.0.36/30	.38	172.23.13.0/24
	VALLE	E1	.41	172.23.0.40/30	.42	172.23.14.0/24
	COAPA	E1	.45	172.23.0.44/30	.46	172.23.15.0/24
	CARRASCO	E1	.49	172.23.0.48/30	.50	172.23.16.0/24
	POPOCATEPETL	E1	.53	172.23.0.52/30	.54	172.23.17.0/24
	AGUILAS	E1	.57	172.23.0.56/30	.58	172.23.18.0/24
Total: 15						
DISTRIB_09	PALMAS	192k	.1	172.24.0.0/30	.2	172.24.4.0/25
	SN_ANDRES_TOTOLTEPEC	E1	.5	172.24.0.4/30	.6	172.24.5.0/24
	RIO_GRIJALVA	E1	.9	172.24.0.8/30	.9	172.24.6.0/24
	LAGO_ONEGA	E1	.13	172.24.0.12/30	.14	172.24.7.0/24
	CONDESA	E1	.17	172.24.0.16/30	.18	172.24.8.0/24
	CHIAPAS	E1	.21	172.24.0.20/30	.22	172.24.9.0/24
	MIXCOAC	E1	.25	172.24.0.24/30	.26	172.24.10.0/24
	TACUBAYA	E1	.29	172.24.0.28/30	.30	172.24.11.0/24
	SANTA_FE	256k	.33	172.24.0.32/30	.34	172.24.4.128/25
	CHAPULTEPEC	E1	.37	172.24.0.36/30	.38	172.24.12.0/24
	RIO_DANUBIO	E1	.41	172.24.0.40/30	.42	172.24.13.0/24
	ANTONIO_CASO	E1	.45	172.24.0.44/30	.46	172.24.14.0/24
	RIO_NAZAS	E1	.49	172.24.0.48/30	.50	172.24.15.0/24
Total: 13						
DISTRIB_10	TEXCOCO_1	E1	.1	172.25.0.0/30	.2	172.25.4.0/24
	TEXCOCO_2	E1	.5	172.25.0.4/30	.6	172.25.5.0/24
	NEXTENGO	E1	.9	172.25.0.8/30	.9	172.25.6.0/24
Total: 3						
DISTRIB_11	NEVADO	E1	.1	172.26.0.0/30	.2	172.26.4.0/24
	SAN_JUAN	E1	.5	172.26.0.4/30	.6	172.26.5.0/24
	CUAUTITLAN	128k	.9	172.26.0.8/30	.9	172.26.6.0/26
	ESTRELLA	E1	.13	172.26.0.12/30	.14	172.26.7.0/24
	NEXTENGO	E1	.17	172.26.0.16/30	.18	172.26.8.0/24
	ROMA	E1	.21	172.26.0.20/30	.22	172.26.9.0/24
	POPOCATEPETL	E1	.25	172.26.0.24/30	.26	172.26.10.0/24
	CULHUACAN	E1	.29	172.26.0.28/30	.30	172.26.11.0/24
Total: 8						
DISTRIB_12	BALBUENA	E1	.1	172.27.0.0/30	.2	172.27.4.0/24
	CHAMIZAL	E1	.5	172.27.0.4/30	.6	172.27.5.0/24
	CULHUACAN	E1	.9	172.27.0.8/30	.9	172.27.6.0/24
	MEYEHUALCO	256k	.13	172.27.0.12/30	.14	172.27.7.0/25
	ERMITA	E1	.17	172.27.0.16/30	.18	172.27.8.0/24
	SAN_LORENZO	E1	.21	172.27.0.20/30	.22	172.27.9.0/24
	TEXCOCO	E1	.25	172.27.0.24/30	.26	172.27.10.0/24
	RIO_RHIN	E1	.29	172.27.0.28/30	.30	172.27.11.0/24
	TLAHUAC	E1	.33	172.27.0.32/30	.34	172.27.12.0/24
Total: 9						
DISTRIB_13	PRADOS	256k	.1	172.28.0.0/30	.2	172.28.4.0/25
	VILLA_DE_LAS_FLORES	128k	.5	172.28.0.4/30	.6	172.28.4.128/26
Total: 2						
						Total accesos: 122

Tabla 5.1. Enlaces de la red RC-JC.

La siguiente figura ilustra el mapa WAN de la red:

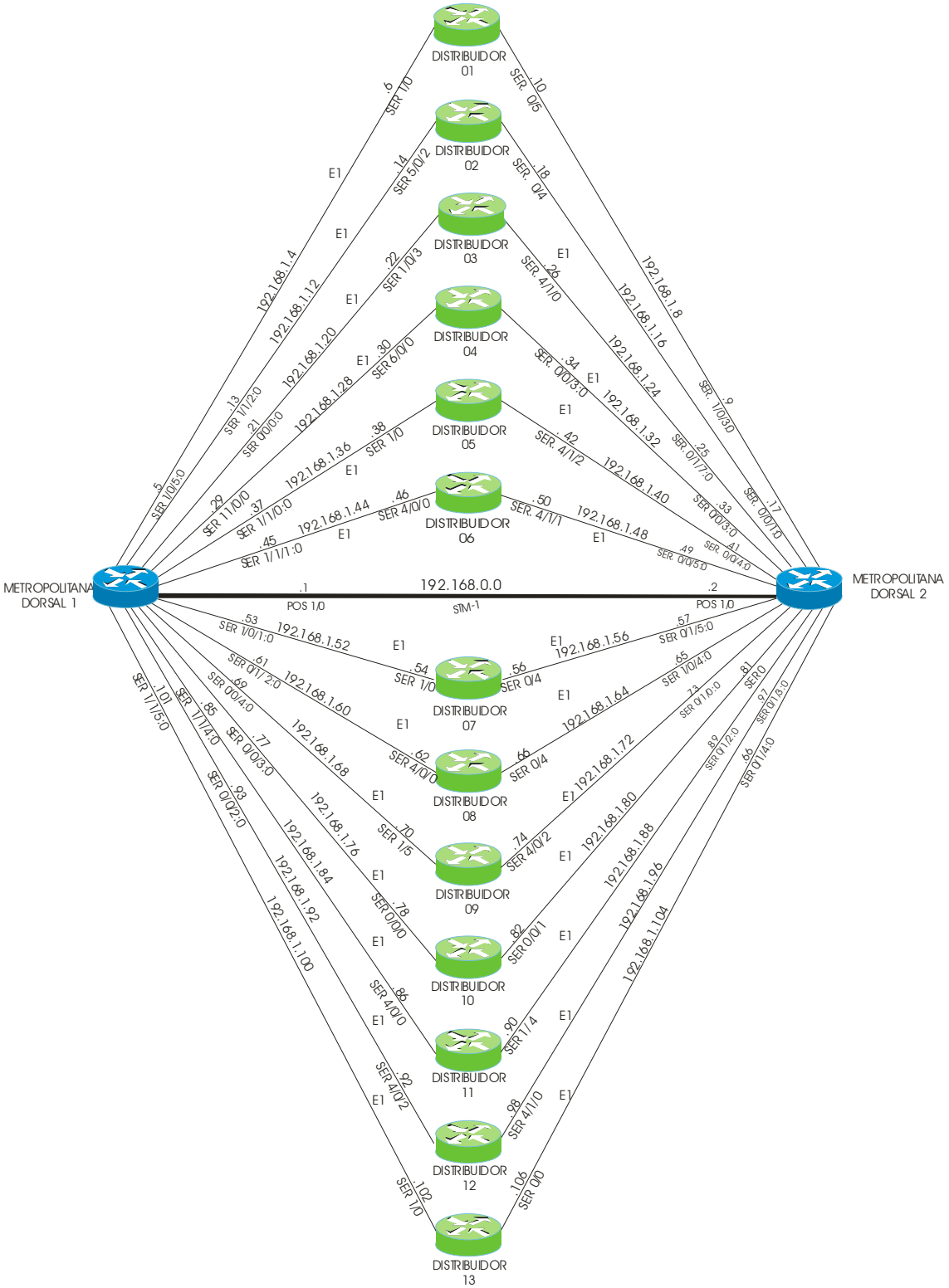

Fig. 5.1. Mapa WAN de la RC-JC.

Hardware

Dados los altos índices de confiabilidad y desempeño que los equipos dorsales deben mantener, se optó por usar las plataformas de enrutadores Cisco 7500.

Los requerimientos generales de los nodos de distribución son los mismos que los de nivel dorsal, por que se usan los mismos enrutadores. El nodo de acceso es un enrutador Cisco, y el modelo es 3600.

Cabe mencionar que estos enrutadores cuentan con tarjetas VIP, que tienen la ventaja de tener un procesamiento distribuido, es decir, que el procesador no tiene que hacer toda la labor sino que se ayuda de tarjetas procesadoras. Esto se refleja en la gran escalabilidad de los enrutadores.

Versiones de Software

La Versión de IOS debe ser superior o igual a la 12.0(22)

- Distribuidor y Dorsal serie 7500 versión IOS 12.0(23)S6 Service provider/Secured Shell 3DES. Que soporta EIGRP, Q oS Packet Marking, Low Latency Queue, Modular QoS CLI, CBWFQ/DCBWFQ, MPLS, TDP Y LDP, MPLS QoS Enhancements, HDLC. PPP, Multilink PPP, SNMP v2, Listas de acceso estándar y extendidas, entre otras.
- Acceso serie 3600 Versión de IOS 12.2(23a) TELCO. Que soporta EIGRP, HDLC, QoS, Class-Based Weigthed fair queueing (CBWFQ), Listas de acceso estándar y extendidas, entre otras.

Políticas de transporte

Para simplificar la administración de la RCHR, se ha determinado que todos los protocolos de usuario de capa 3 deberán ser encapsulados en IP en el Nivel de Acceso para su transporte a través de la red, claro exceptuando el caso en el que el protocolo nativo sea IP.

Protocolos de enrutamiento

Un punto crítico para la administración y análisis de la red, es el poder predecir el comportamiento de la misma durante su operación normal y en casos de contingencia. Este comportamiento se derivará en la mayoría de los casos del protocolo de enrutamiento implementado, por lo que su selección debe tomar al menos los siguientes criterios:

- Rápida convergencia.
- Uso de máscaras de longitud variable.
- Sumarización de rutas.
- Estabilidad y bajo consumo de CPU.

El protocolo IGP seleccionado fue EIGRP, el cual se encuentra operando en el nivel dorsal, distribución y nodos de acceso con el número de proceso 125.

Las características más importantes de EIGRP son las siguientes:

EIGRP es un Protocolo IGP clasificado como híbrido de los protocolos "link-state" y "vector distance". La ventaja de este protocolo sobre los demás es su capacidad de integrar tres protocolos a través de la WAN, reduciendo el tráfico originado por el manejo individual de ellos. Los protocolos integrados son IPX, IP y AppleTalk. EIGRP ofrece adicionalmente las siguientes ventajas:

- Actualizaciones incrementales
- Su velocidad de convergencia es igual o mejor que los protocolos con los cuales compite.
- Soporta VLSM y sumarización

Una desventaja de este protocolo es que es un protocolo propietario de Cisco Systems.

6 Propuesta de diseño

La implementación de QoS se hará solamente en la parte WAN de la red, es decir, en los niveles de acceso, distribución y dorsal.

En el nivel de acceso se aplicarán los siguientes mecanismos de QoS:

- Debido a que todo el tráfico es IP o está encapsulado en IP, se usará DiffServ para el marcado de paquetes. Esto se hace usando los tres bits de prioridad en el campo ToS del encabezado de IPv4 para especificar la clase de servicio para cada paquete. Se pueden definir hasta 8 clases, las cuales se pueden definir de acuerdo al tipo de aplicación o a la importancia de la información.
- Para definir las clases se tomaron listas de acceso que diferencian el tráfico. Se uso LLQ y CBWFQ, dando prioridad absoluta a una clase además de WFQ para prevenir congestión.
- En algunos casos, en el nivel de acceso se tiene un enlace menor a un E1. Aquí se recomienda usar una técnica para optimizar el ancho de banda, como LFI (Link Fragmentation and Interleaving).

Para el nivel de distribución aplicarán los siguientes mecanismos de QoS:

- Mecanismos para prevención y manejo de congestión, como WRED (Weight Random Early Detection), CBWFQ (Class Based Weighted fair queuing) y LLQ (Low Latency Queueing). Esto se hace para dar trato preferencial a aplicaciones sensibles al retardo en caso de congestión. Se recomienda el uso de CBWFQ ya que se pueden definir las clases de tráfico basadas en el criterio de correspondencia o identidad, incluyendo los protocolos, listas de control de acceso (ACLs) e interfaces de entrada.
- En este nivel es necesario fragmentar el enlace con LFI hacia el nivel de acceso para que exista coherencia en las tasas de transmisión. Pero hacia le nivel dorsal no es necesario debido a las altas tasas de transmisión que se manejan.

Debido a que los enlaces en el nivel dorsal son de capacidades altas, no es tan necesaria la implementación de algún mecanismo para asegurar QoS, aunque sería recomendable usar una técnica de encolamiento como CBWFQ.

La prioridad que se dará a cada clase de tráfico en la red se muestra en la siguiente tabla:

Prioridad	Clase
7	Reservado (manejada por el enrutador)
6	Protocolos de enrutamiento, señalización y operaciones propias de la red
5	Voz
4	Videoconferencia y aplicaciones sensibles al retardo o muy importantes para la empresa
3	Señalización
2	HTTP corporativo
1	Tráfico RCD no prioritario y/o de aplicaciones no sensibles al retardo
0	Tráfico hacia o desde Internet

Tabla 6.1. Prioridad para cada clase de tráfico.

7 Prueba piloto

En la fase de implementación se simuló la red haciendo una maqueta para simplificar las pruebas, se tomaron solo ocho enrutadores los cuales respetaban la topología del modelo jerárquico original.

- Dos enrutadores que hacían el trabajo del nivel dorsal.
- Dos enrutadores que hacían el trabajo del nivel de distribución.
- Cuatro enrutadores que hacían el trabajo del nivel de acceso.

Para hacer dicha maqueta se conectaron los enrutadores según se muestra la figura 7.1, utilizándose cables seriales tipo G.703 con conectores tipo DB9 tanto para los E1 como los enlaces de 128Kbps y 256 Kbps, además de un enlace óptico STM-1 para la conexión entre enrutadores dorsales.

Se le asignó una dirección IP a cada puerto físico según su posición, una vez que se levantaban los enlaces se procedió a establecer un protocolo de comunicación entre los enrutadores el cual les brindaba interconectividad entre todos los enrutadores de la red, se opto por EIGRP con número de proceso 100.

Los enrutadores utilizados fueron cisco series 7500 tanto para dorsal como para nivel de distribución y las series 3600 para nivel de acceso.

Se conectó un teléfono a cada enrutador de acceso, se generó tráfico de datos a través de una terminal que generaba un ping a cada uno de los enlaces dentro de la red WAN para que éste se saturara.

Como ya se mencionó en el capitulo anterior solo se aplicaron algunos mecanismos de QoS, dicha configuración se encuentra en las tablas al final de este capítulo. Donde se observa la programación de todos lo mecanismos para que funcione la red, además de los mecanismo QoS.

Para simular tráfico en la red, se conectó una Terminal a uno de los accesos desde la cual se enviaban pings con diferente tamaño de paquetes a cada uno de los enlaces de la red, con lo cual se simulo todo tipo de tráfico de datos. Estos pings se quedaban saltando dentro de cada enlace entre enrutadores, por lo que la red se saturaba. Esto se observa en la figura 7.1, donde las flechas rojas indican la dirección de los pings.

Por limitaciones técnicas, no se pudo probar video en tiempo real en nuestras pruebas, pero se simuló el tráfico con paquetes del mismo tamaño.

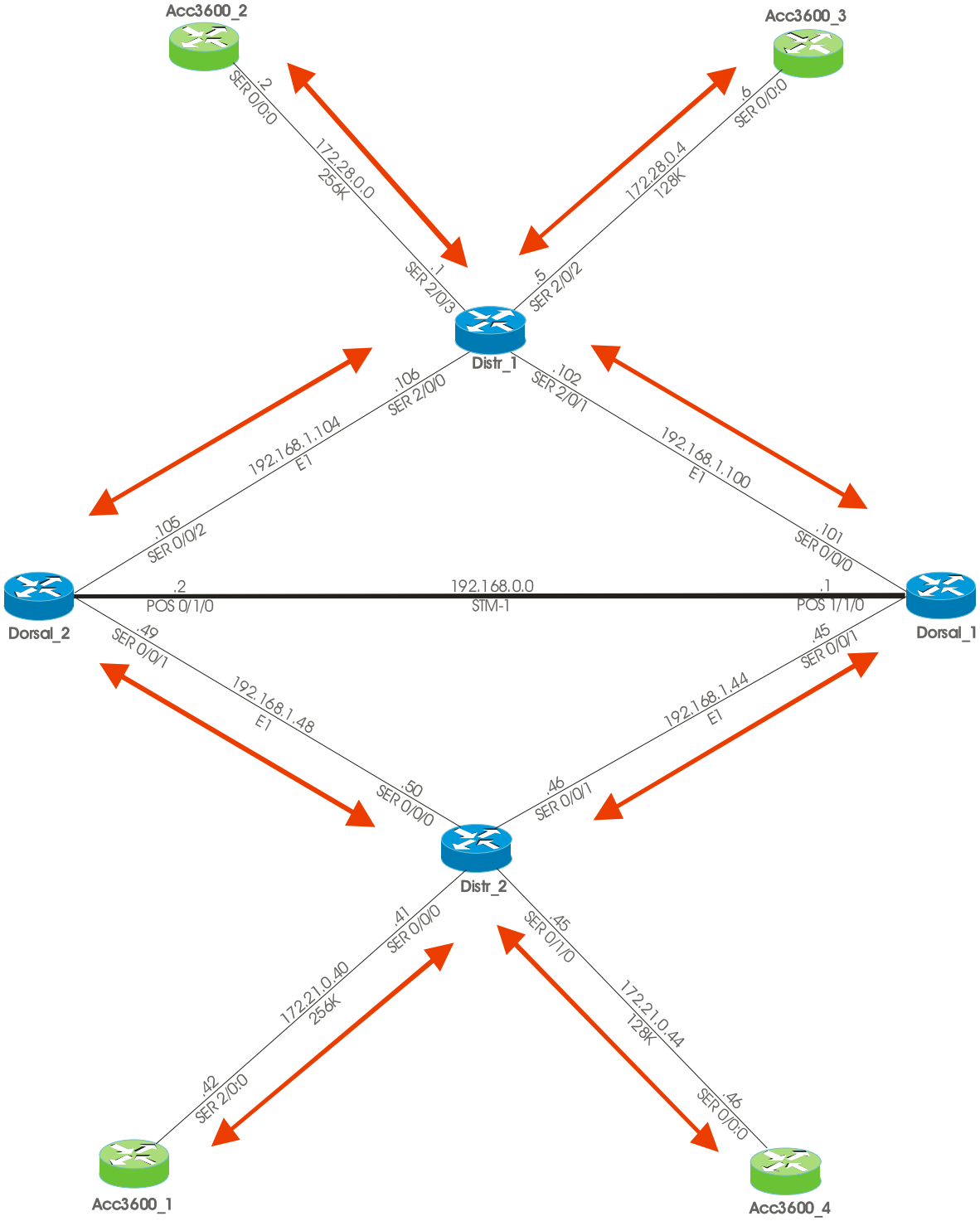

Figura 7.1. Maqueta.

Las siguientes tablas muestran la configuracion de cada router para la prueba:

Router dorsal 7500 Dorsal_1

```
Current configuration : 1985 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service single-slot-reload-enable
!
hostname Dorsal_1
!
redundancy
 no keepalive-enable
 mode hsa
enable password cesar
!
ip subnet-zero
ip cef distributed
!
class-map match-all internet
  match ip precedence 0
class-map match-all VoIP
  match ip precedence 5
class-map match-all traf_int
  match ip precedence 2
class-map match-all video
  match ip precedence 4
!
policy-map marcado
  class internet
    bandwidth percent 5
    random-detect
  class traf_int
    bandwidth percent 10
    random-detect
  class video
    bandwidth percent 35
    random-detect
  class VoIP
    priority percent 25
!
 interface Serial0/0/0
 ip address 192.168.1.101 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 no ip mroute-cache
 service-policy output marcado
!
interface Serial0/0/1
 ip address 192.168.1.45 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 service-policy output marcado
interface Serial0/0/2
no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0/0/3
 no ip address
 no ip directed-broadcast
 shutdown
!
 interface Serial0/1/0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0/1/1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0/1/2
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0/1/3
 no ip address
 no ip directed-broadcast
 shutdown
!
interface POS1/1/0
 ip address 192.168.0.1 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 delay 10
 service-policy output marcado
 clock source internal
 pos framing sdh
!
router eigrp 100
 redistribute static
 network 192.168.0.0
 network 192.168.1.0
!
ip classless
ip route 10.1.4.0 255.255.255.0 192.168.1.102
ip route 10.1.5.0 255.255.255.0 192.168.0.2
ip route 10.1.7.0 255.255.255.0 192.168.1.46
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password cesar
 login
!
 end
```

Router dorsal 7500 Dorsal_2

```
Current configuration : 1617 bytes
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service single-slot-reload-enable
!
hostname Dorsal_2
!
redundancy
 no keepalive-enable
 mode hsa
enable password cesar
!
ip subnet-zero
ip cef
!
class-map match-all internet
  match ip precedence 0
class-map match-all VoIP
  match ip precedence 5
class-map match-all traf_int
  match ip precedence 2
class-map match-all video
  match ip precedence 4
!
policy-map marcado
  class VoIP
    priority percent 25
  class video
    bandwidth percent 35
  class traf_int
    bandwidth percent 10
  class internet
    bandwidth percent 5
!
interface Serial0/0/0
 ip address 192.168.1.49 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
!
interface Serial0/0/1
 ip address 192.168.1.49 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
!
interface Serial0/0/2
 ip address 192.168.1.105 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
!
interface Serial0/0/3
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface POS0/1/0
 ip address 192.168.0.2 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 delay 10
 clock source internal
 pos framing sdh
!
router eigrp 100
 redistribute static
 network 192.168.0.0
 network 192.168.1.0
!
ip classless
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password cesar
 login
!
end
```

Router de distribución 7500 distr_1

```
Current configuration : 2099 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname distr_1
!
enable password cesar
!
ip subnet-zero
!
ip cef distributed
!
class-map match-all internet
  match ip precedence 0
class-map match-all VoIP
  match ip precedence 5
class-map match-all traf_int
  match ip precedence 2
class-map match-all video
  match ip precedence 4
!
policy-map marcado
  class video
    bandwidth percent 35
    random-detect
  class traf_int
    bandwidth percent 10
    random-detect
  class internet
    bandwidth percent 5
    random-detect
  class VoIP
    bandwidth percent 25
    random-detect
    shape average 64000 256 256
!
interface Multilink1
 ip address 172.28.0.5 255.255.255.252
 no ip route-cache cef
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 5
 ppp multilink interleave
 multilink-group 1
!
interface Multilink2
 ip address 172.28.0.1 255.255.255.252
 no ip route-cache cef
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 3
ppp multilink interleave
 multilink-group 2
!
interface Serial2/0/0
 ip address 192.168.1.106 255.255.255.252
 encapsulation ppp
 service-policy output marcado
 serial restart-delay 0
!
interface Serial2/0/1
 ip address 192.168.1.102 255.255.255.252
 encapsulation ppp
 service-policy output marcado
 serial restart-delay 0
!
interface Serial2/0/2
 no ip address
 encapsulation ppp
 timeslot 1-2
 ts16
 serial restart-delay 0
 ppp multilink
 multilink-group 1
!
interface Serial2/0/3
 no ip address
 encapsulation ppp
 timeslot 1-4
 ts16
serial restart-delay 0
 ppp multilink
 multilink-group 2
!
router eigrp 100
 redistribute static
 network 172.28.0.0
 network 192.168.1.0
 auto-summary
 no eigrp log-neighbor-changes
!
ip classless
ip route 10.1.1.0 255.255.255.0 172.28.0.2
ip route 10.1.2.0 255.255.255.0 172.28.0.6
ip route 10.1.3.0 255.255.255.0 192.168.1.105
ip route 10.1.4.0 255.255.255.0 192.168.1.101
no ip http server
!
line con 0
line aux 0
line vty 0 4
password cesar
 login
!
end
```

Router de distribución 7500 distr_2

```
Current configuration : 2050 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service single-slot-reload-enable
!
hostname distr_2
!
redundancy
 no keepalive-enable
 mode hsa
enable password cesar
!
ip subnet-zero
ip cef distributed
!
class-map match-all internet
  match ip precedence 0
class-map match-all VoIP
  match ip precedence 5
 class-map match-all traf_int
  match ip precedence 2
class-map match-all video
  match ip precedence 4
!
policy-map marcado
  class internet
    bandwidth percent 5
    random-detect
  class traf_int
    bandwidth percent 10
  class video
    bandwidth percent 35
    random-detect
  class VoIP
    priority percent 25
!
interface Multilink1
 ip address 172.21.0.41 255.255.255.252
 no ip directed-broadcast
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 5
 ppp multilink interleave
 multilink-group 1
!
interface Multilink1
 ip address 172.21.0.45 255.255.255.252
 no ip directed-broadcast
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 5
 ppp multilink interleave
 multilink-group 2
!
interface Serial0/0/0
 ip address 192.168.1.50 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
 no ip mroute-cache
!
interface Serial0/0/1
 ip address 192.168.1.46 255.255.255.252
 no ip directed-broadcast
 encapsulation ppp
!
interface Serial0/0/2
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 timeslot 1-4
 ts16
 ppp multilink
 multilink-group 1
!
interface Serial0/0/3
 ip address 172.21.0.17 255.255.255.252
 no ip directed-broadcast
 shutdown
!
interface Serial0/1/0
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 timeslot 1-2
 ts16
 ppp multilink
 multilink-group 2
!
interface Serial0/1/1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0/1/2
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0/1/3
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Virtual-Template3
 no ip address
 no ip directed-broadcast
!
router eigrp 100
 redistribute static
 network 172.21.0.0
 network 192.168.1.0
!
ip classless
ip route 10.1.6.0 255.255.255.0 192.168.1.49
ip route 10.1.7.0 255.255.255.0 192.168.1.45
ip route 10.1.8.0 255.255.255.0 172.21.0.42
ip route 10.1.9.0 255.255.255.0 172.21.0.46
!
line con 0
line aux 0
line vty 0 4
 password cesar
 login
!
end
```

Router de acceso 3600 acc3600_1

```
Current configuration : 2024 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname acc3600_1
!
enable password cesar
!
ip subnet-zero
!
multilink virtual-template 3
call rsvp-sync
!
controller E1 2/0
 framing NO-CRC4
 channel-group 0 timeslots 1-4
!
controller E1 2/1
 description line
!
class-map match-all internet
  match ip precedence 0
class-map match-all VoIP
  match ip precedence 5
class-map match-all traf_int
  match ip precedence 2
class-map match-all video
  match ip precedence 4
!
policy-map encolamiento
  class internet
   bandwidth percent 5
   random-detect
  class traf_int
   bandwidth percent 10
   random-detect
  class video
   bandwidth percent 35
   random-detect
  class VoIP
    priority 64
!
policy-map marcado
class internet
set ip precedence 0
class traf_int
set ip precedence 2
class video
set ip precedence 4
!
 interface Multilink1
  ip address 172.21.0.42 255.255.255.252
  service-policy output marcado
  ppp multilink
  ppp multilink fragment-delay 5
  ppp multilink interleave
  multilink-group 1
!
interface Serial2/0:0
 no ip address
encapsulation ppp
 ppp multilink
 multilink-group 1
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Virtual-Template3
 ip unnumbered Serial2/0:0
 ppp multilink
 ppp multilink fragment-delay 10
 ppp multilink interleave
!
interface Ethernet1/0
 ip address 172.28.3.1 255.255.255.0
service-policy input marcado
 half-duplex
!
router eigrp 100
 redistribute static
 network 172.21.0.0
 auto-summary
!
ip classless
ip route 10.1.8.0 255.255.255.0 172.21.0.41
ip http server
!
ip access-list extended internet
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 192.0.0.0 0.255.255.255
ip access-list extended traf_int
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq telnet
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
dial-peer cor custom
!
dial-peer voice 1 pots
 destination-pattern 3601
 port 1/1/0
!
dial-peer voice 2 voip
 destination-pattern 3602
 session target ipv4:172.28.0.2
 ip precedence 5

dial-peer voice 3 voip
 destination-pattern 3603
 session target ipv4:172.28.0.6
 ip precedence 5
!
dial-peer voice 4 voip
 destination-pattern 3604
 session target ipv4:172.21.0.46
 ip precedence 5
line con 0
line aux 0
line vty 0 4
 password cesar
 login
!
end
```

Router de acceso 3600 acc3600_2

```
Current configuration : 2074 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname acc3600_2
!
enable password cesar
!
ip subnet-zero
!
call rsvp-sync
!
!controller E1 0/0
 framing NO-CRC4
 channel-group 0 timeslots 1-4
!
controller E1 0/1
!
class-map match-all internet
  match ip precedence 0
class-map match-all VoIP
  match ip precedence 5
class-map match-all traf_int
  match ip precedence 2
class-map match-all video
  match ip precedence 4
!
policy-map encolamiento
  class VoIP
   bandwidth percent 25
   random-detect
  class video
   bandwidth percent 35
   random-detect
  class internet
   bandwidth percent 5
   random-detect
  class traf_int
   bandwidth percent 10
   random-detect
!
policy-map marcado
class internet
set ip precedence 0
class traf_int
set ip precedence 2
class video
set ip precedence 4
!
interface Multilink2
 ip address 172.28.0.2 255.255.255.252
 service-policy output encolamiento
 ppp multilink
 ppp multilink fragment-delay 3
 ppp multilink interleave
 multilink-group 2
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0:0
 no ip address
encapsulation ppp
 ppp multilink
 multilink-group 2
!
interface Ethernet1/0
 ip address 172.28.4.1 255.255.255.0
service-policy input marcado
 full-duplex
!
interface Ethernet1/1
 no ip address
 shutdown
 half-duplex
!
router eigrp 100
 redistribute static
 network 172.28.0.0
 auto-summary
!
ip classless
ip route 10.1.1.0 255.255.255.0 172.28.0.1
ip http server
!
ip access-list extended internet
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 172.0.0.0 0.255.255.255
 permit ip any any
ip access-list extended traf_int
 permit tcp any any eq ftp-data
 permit tcp any any eq ftp
 permit tcp any any eq telnet
!
voice-port 3/0/0
!
voice-port 3/0/1
!
dial-peer cor custom
!
dial-peer voice 5 pots
 destination-pattern 3602
port 3/0/0
!
dial-peer voice 6 voip
 destination-pattern 3601
 session target ipv4:172.21.0.42
 ip precedence 5
 no vad
!
dial-peer voice 7 voip
 destination-pattern 3603
 session target ipv4:172.28.0.6
 ip precedence 5
 no vad
!
dial-peer voice 8 voip
 destination-pattern 3604
 session target ipv4:172.21.0.46
 ip precedence 5
!
line con 0
line aux 0
line vty 0 4
 password cesar
 login
!
end
```

Router de acceso 3600 acc3600_3

```
Current configuration : 2104 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname acc3600_3
!
enable password cesar
!
memory-size iomem 10
ip subnet-zero
!
call rsvp-sync
!
controller E1 0/0
 framing NO-CRC4
 channel-group 0 timeslots 1-2
!
controller E1 0/1
!
class-map match-all internet
  match ip precedence 0
class-map match-all VoIP
  match ip precedence 5
class-map match-all traf_int
  match ip precedence 2
class-map match-all video
  match ip precedence 4
!
policy-map encolamiento
  class VoIP
   bandwidth percent 25
   random-detect
  class video
 bandwidth percent 35
   random-detect
  class internet
   bandwidth percent 5
   random-detect
  class traf_int
   bandwidth percent 10
   random-detect
!
policy-map marcado
class internet
set ip precedence 0
class traf_int
set ip precedence 2
class video
set ip precedence 4
!
interface Multilink1
 ip address 172.28.0.6 255.255.255.252
 service-policy output encolamiento
 ppp multilink
 ppp multilink fragment-delay 5
 ppp multilink interleave
 multilink-group 1
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0:0
 no ip address
 encapsulation ppp
 ppp multilink
 multilink-group 1
!
interface Ethernet1/0
 ip address 172.28.5.1 255.255.255.0
service-policy input marcado
 full-duplex
!
interface Ethernet1/1
 no ip address
 shutdown
 half-duplex
!
router eigrp 100
 redistribute static
 network 172.28.0.0
 auto-summary
!
ip classless
 ip route 10.1.2.0 255.255.255.0 172.28.0.5
ip http server
!
ip access-list extended internet
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 172.0.0.0 0.255.255.255
ip access-list extended traf_int
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq telnet
!
voice-port 3/0/0
!
voice-port 3/0/1
!
voice-port 3/1/0
!
voice-port 3/1/1
!
dial-peer cor custom
!
!
dial-peer voice 9 pots
 destination-pattern 3603
 port 3/1/0
!
dial-peer voice 10 voip
 destination-pattern 3601
 session target ipv4:172.21.0.42
 ip precedence 5
 no vad
!
dial-peer voice 11 voip
 destination-pattern 3602
 session target ipv4:172.28.0.2
 ip precedence 5
 no vad
!
dial-peer voice 12 voip
 destination-pattern 3604
 session target ipv4:172.21.0.46
 ip precedence 5
!
line con 0
line aux 0
line vty 0 4
password cesar
 login
!
end
```

Router de acceso 3600 acc3600_4

```
Current configuration : 2104 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname acc3600_4
!
enable password cesar
!
memory-size iomem 10
ip subnet-zero
!
call rsvp-sync
!
controller E1 0/0
 framing NO-CRC4
 channel-group 0 timeslots 1-2
!
controller E1 0/1
!
class-map match-all internet
  match ip precedence 0
class-map match-all VoIP
  match ip precedence 5
class-map match-all traf_int
  match ip precedence 2
class-map match-all video
  match ip precedence 4
!
policy-map encolamiento
  class VoIP
   bandwidth percent 25
   random-detect
  class video
 bandwidth percent 35
   random-detect
  class internet
   bandwidth percent 5
   random-detect
  class traf_int
   bandwidth percent 10
   random-detect
!
policy-map marcado
class internet
set ip precedence 0
class traf_int
set ip precedence 2
class video
set ip precedence 4
!
interface Multilink1
 ip address 172.21.0.46 255.255.255.252
 service-policy output encolamiento
 ppp multilink
 ppp multilink fragment-delay 5
 ppp multilink interleave
 multilink-group 1
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
speed auto
!
interface Serial0/0:0
 no ip address
 encapsulation ppp
 ppp multilink
 multilink-group 1
!
interface Ethernet1/0
 ip address 172.28.6.1 255.255.255.0
service-policy input marcado
 full-duplex
!
interface Ethernet1/1
 no ip address
 shutdown
 half-duplex
!
router eigrp 100
 redistribute static
 network 172.21.0.0
 auto-summary
!
ip classless
 ip route 10.1.9.0 255.255.255.0 172.21.0.45
ip http server
!
ip access-list extended internet
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 172.0.0.0 0.255.255.255
ip access-list extended traf_int
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq telnet
!
 voice-port 3/0/0
 !
 voice-port 3/0/1
 !
 voice-port 3/1/0
 !
 voice-port 3/1/1
 !
 dial-peer cor custom
 !
 !
 dial-peer voice 13 pots
  destination-pattern 3604
  port 3/1/0
 !
 dial-peer voice 14 voip
  destination-pattern 3601
  session target ipv4:172.21.0.42
  ip precedence 5
  no vad
 !
 dial-peer voice 15 voip
  destination-pattern 3602
  session target ipv4:172.28.0.2
  ip precedence 5
  no vad
 !
 dial-peer voice 16 voip
  destination-pattern 3604
  session target ipv4:172.21.0.46
  ip precedence 5
 !
 line con 0
 line aux 0
 line vty 0 4
  password cesar
  login
 !
 end
```

8 Resultados Obtenidos

Previo a la implementación de los mecanismos de QoS, se puso en operación la red como se hace de manera habitual (mejor esfuerzo), garantizando la conectividad entre cada enrutador mediante el protocolo de enrutamiento EIGRP, cumpliendo los requerimientos y necesidades de la red.

Una vez hecho esto, se procedió a saturar la red, se usó una Terminal desde la cual se enviaban pings con diferente tamaño de paquetes a cada uno de los enlaces de la red, con lo cual se simulo todo tipo de tráfico de datos.

Se hacía una llamada telefónica e inmediatamente después se saturaba la red con pings, con lo cual la voz sufría un retardo considerable. Después de un tiempo la llamada simplemente se perdía debido a que la red estaba demasiado saturada con los pings. Esta es la forma en que operan muchas redes, su principal prioridad es que exista conectividad, sin preocuparse por la forma en que fluye el tráfico.

Al implementar los mecanismos de QoS la red, se hicieron las mismas pruebas saturando la red con los mismos pings, con lo cual las llamadas telefónicas no sufrían algún retardo considerable, además de que no se perdían como en el caso de la red sin QoS.

Al monitorear los enlaces y analizar las clases de tráfico que diferenciamos en cada punto de la red se observaba como a la voz se le reservaba el ancho de banda que se le asignó, al igual que todas las demás clases, siendo el trafico más afectado el de datos e Internet, debido a la política establecida.

Al nosotros poder establecer políticas propias en la red, podemos manipular la manera en que es afectada cada aplicación en la red, en periodos de congestión, siendo mas eficiente el uso del ancho de banda para aplicaciones que se consideren de prioridad absoluta, como la voz; las demás aplicaciones que no son tan sensibles a retardos, esperaran su turno a pasar por la red, hasta que terminen los periodos de congestión.

Se pudo observar también que en los enlaces entre nodos distribuidores y accesos, a pesar de tener enlaces de menor capacidad, el tráfico no se veía afectado ya que en estos enlaces se implementó un mecanismo de fragmentación.

Implementación

Con base en los resultados obtenidos, se puede concluir que la implementación es factible en la red RC-JC. Como esta red se encuentra en producción, sólo se implementarían los mecanismos de QoS.

La implementación se hace comenzando en el nivel dorsal, luego en el nivel distribuidor y al final en el nivel de acceso. Se hace de esta manera para que cuando los accesos tengan los mecanismos de QoS configurados, el resto de la red ya se encuentre lista para dar Calidad de Servicio. Si se hiciera de manera contraria, comenzando por los accesos, no serviría de nada ya que sólo se estarían marcando los paquetes de diferentes tipos de tráfico pero la red no estaría lista para garantizar Calidad de Servicio a ningún tipo de tráfico.

9 Conclusiones

Con los resultados obtenidos en la implementación que realizamos sin Calidad de Servicio (QoS), demostramos la problemática de una red que no gestiona el ancho de banda con el que dispone de manera eficiente. Se trato de hacer que distintas aplicaciones compartieran el ancho de banda de la red, funcionó durante un pequeño periodo de tiempo, pero después se sobresaturo la red, impidiendo que algunas aplicaciones no se pudieran ejecutar correctamente, como la voz, ya que no pudo ser transmitida sobre la red saturada, ya que la misma no permitía que más tráfico circulará por ella.

Esto sucede hoy en día con muchas redes, que fueron diseñadas para darle un trato del "mejor esfuerzo" a todo aquel tráfico que transite por esta. Así que, por esta situación muchas empresas se ven en la necesidad de usar infraestructuras separadas, una para datos, una red conmutada para voz, y un enlace de alta capacidad para videoconferencia. Esto es un costo extra que deben de pagar para poder estar comunicados y operando en todo momento.

Propusimos una solución para esta necesidad de ahorrar costos de operación, una red capaz de soportar todo tipo de tráfico usando una sola infraestructura. Esto se demostró en la segunda etapa, donde se implemento un esquema de Calidad de Servicio (QoS) con políticas de servicio y mecanismos que garanticen la apropiada asignación de recursos de la red. Estas políticas de servicio deben de estar bien diseñadas, para que se puedan adaptar a los requerimientos y necesidades que se tengan, como fue el caso de este trabajo, donde antes de diseñar los mecanismos de Calidad de Servicio (QoS), se estudiaron los requerimientos de la red, logrando así adaptar cada mecanismo en cada nivel de la misma.

Se demostró que bajo un estricto control de recursos, se puede tener una misma infraestructura que pueda transportar datos, voz, y video sin ningún problema.

Para un proveedor de servicios, esto es un gran avance ya que puede ofrecer mas servicios sobre su misma infraestructura y sin afectar la calidad de cada uno de estos. Para los clientes, esto significa una gran reducción de costos, ya que no necesita contratar varios servicios por separado con diferentes proveedores.

Con este trabajo damos las herramientas generales de Calidad de Servicio (QoS). Cabe mencionar que este trabajo se enfoca en un problema particular, una red en operación, por lo cual no se hubo necesidad de implementar todos los mecanismos de QoS mencionados a lo largo de este trabajo. Si se desea aplicar a otro problema en particular, se debe hacer el análisis de requerimientos de la red y ver cuales mecanismos de QoS se adaptan a esta.

Bibliografía

Libros:

- Comer Douglas E., *Internetworking with TCP/IP*, 3ª Edición,Vol. 1, Prentice Hall, 1995.
- Graham Buck, *TCP/IP addressing*, 2ª Edición, Morgan Kaufmann, 1997.
- Held Gilbert, *Frame Relay Networking*, 1ª Edición, JOHN WILEY & SONS, LTD, 1999.
- Chao H. Jonathan, Guo Xiaolei, 1ª Edición, JOHN WILEY & SONS, LTD, 2002.
- McQuerry Steve, McGrew Kelly, Foy Stephen, *Cisco Voice over Frame Relay, ATM, and IP*, Cisco Systems, 2001, USA.
- McDysan David E., Spohn Darren L., *Hands-On ATM*, McGraw-Hill.
- Arias Villavicencio Rodolfo, *Redes de Teleinformática Apuntes de clase*, Semestre 2003-2
- García Espinoza Adalberto F., *RDSI Apuntes de clase*, Semestre 2004-1.
- *Deploying Cisco QoS for Enterprise Networks Students Guide*, Vol. 1, Cisco Systems, 2001.
- *Deploying Cisco QoS for Enterprise Networks Students Guide*, Vol. 2, Cisco Systems, 2001.

Páginas de Internet:

- www.cisco.com
- www.redes.upv.es
- www.redeya.com
- www.avantel.com.mx
- www.uninet.com.mx