ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

CONTROL DE TRÁFICO EN REDES TCP/IP FUNDAMENTADO EN PROCEDIMIENTOS Y TÉCNICAS DE CALIDAD DE SERVICIO A LO LARGO DE UNA INFRAESTRUCTURA DE TELECOMUNICACIONES

CARLOS ALBERTO CADENA SILVA

SANGOLQUÍ – ECUADOR

2010

CERTIFICACIÓN

Ing. Darwin Aguilar e Ing. Carlos Romero

CERTIFICAN

Que el trabajo titulado CONTROL DE TRÁFICO EN REDES TCP/IP FUNDAMENTADO EN PROCEDIMIENTOS Y TÉCNICAS DE CALIDAD DE SERVICIO A LO LARGO DE UNA INFRAESTRUCTURA DE TELECOMUNICACIONES, realizado por Carlos Alberto Cadena Silva, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

Debido a que cumple con normas establecidas y que su contenido permitirá una información importante, SÍ se recomienda su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato digital. Autorizan a Carlos Alberto Cadena Silva que lo entregue al Doctor Gonzalo Olmedo, en su calidad de Director de la Carrera.

Sangolquí, 28 de septiembre de 2010

Ing. Darwin Aguilar	Ing. Carlos Romero
DIRECTOR	**CODIRECTOR**

RESUMEN

La calidad de servicio se ha convertido en un factor muy importante dentro de los servicios convergentes actuales. Esta permite dar un funcionamiento adecuado a estos servicios, como voz, video o datos, de acuerdo al manejo de los parámetros críticos que causan problemas de rendimiento en ellos, como ancho de banda, pérdida de paquetes, *delay* y *jitter*. Dentro de este trabajo se presentan cada uno de los puntos a considerar de estos en relación a cada uno de los tipos de tráfico dentro de la red y sus respectivos modelos de servicio.

Para la aplicación de QoS se recomienda dentro de este trabajo seguir con el proceso que consiste en la marcación y clasificación de paquetes, basándose en el campo ToS de la cabecera IP; administrar la congestión, aplicando técnicas de encolamiento; y, prevención de congestión. En este estudio se muestra que antes de aplicar este procedimiento es necesario verificar las características de cada una de las aplicaciones, realizar una auditoría de tráfico, auditoría de negocio y determinar los niveles de servicio requeridos.

Finalmente se da a conocer cada uno de los métodos de QoS que se pueden aplicar sobre los diferentes tipos de tráfico en cada uno de los puntos de la infraestructura de telecomunicaciones, es decir en la red de *backbone*, la red de acceso y equipos terminales en el cliente.

DEDICATORIA

Este trabajo lo dedico a mis padres, que con su esfuerzo han logrado dar ejemplo de lucha y responsabilidad para alcanzar todas mis metas propuestas.

Carlos Alberto Cadena Silva

AGRADECIMIENTO

Agradezco totalmente a Dios por haberme dado la vida y la oportunidad de formación profesional en una prestigiosa institución, a mis padres y a mi hermana por el apoyo incondicional para alcanzar un logro más en mi vida. Finalmente a mis amigos por la confianza y los sabios consejos que en su momento supieron brindarme.

Carlos Alberto Cadena Silva

PRÓLOGO

Una implementación adecuada de mecanismos o procedimientos de gestión de tráfico y calidad de servicio, en la actualidad constituye un factor preponderante dentro de las redes de comunicación.

Inicialmente se puede señalar que el volumen de tráfico es siempre creciente en las redes de conexión empresarial principalmente, por lo que se constituye muy difícil solventar la congestión con solo incrementar el ancho de banda del enlace; esto porque en la actualidad cada servicio sobre la plataforma IP crece aceleradamente y para ello se necesita la identificación de cada tráfico que cruza por la red, ya que la percepción de calidad para un usuario final se refleja en la forma en cómo llega la información de cada uno de las aplicaciones establecidas en su red.

La inclusión de nuevas aplicaciones sensibles al retardo generan cambios en la distribución de tráfico, así como la ocurrencia de fallas en nodos o enlaces que puede resultar en patrones de congestión impredecibles, como los conocidos cuellos de botella, para esto es necesario políticas y procesos para una clasificación adecuada de la información lo cual es conseguido con la calidad del servicio dentro de un enlace de comunicación.

Por otra parte, se presenta el fenómeno de la convergencia de las redes de comunicación, esto es proveer de servicios de voz, vídeo, datos y multimedia sobre una misma plataforma, en este caso para la IP, lo cual ha generado un cambio en el modelo de trabajo para ofrecer además de transporte o simplemente salida al Internet, servicios de valor agregado sobre la red. Es decir, para un manejo adecuado de los servicios en redes convergentes, es necesario un procedimiento estricto de QoS, con ello brindar un rendimiento óptimo de los servicios involucrados y poder sortear cada uno de los problemas a presentarse por características innatas de los mismos, como por ejemplo uno de los más sensibles a lo antes mencionado, la voz sobre la plataforma IP.

Las empresas proveedoras de servicios, con la aparición de estos nuevos conceptos han visto la necesidad de introducir al mercado el tema de soluciones integrales sobre una red, esto abarca convergencia de servicios, calidad de servicio, soporte y mantenimiento de

cada red negociada, entre varias cosas, con ello la obligación del cumplimiento de niveles de servicio dentro de sus contratos hacia clientes finales; es por ello imprescindible el conocimiento de procedimientos y técnicas de QoS sobre redes con la plataforma IP.

Hablar de calidad de servicio sobre redes de empresas grandes representa un incremento en la productividad de la misma, ya que información como voz, vídeo y datos, viajará de una manera eficiente y eficaz sobre la red, con esto la comunicación entre cada uno de los puntos a nivel nacional y mundial será oportuna y sin ningún contratiempo; además, con la implementación de estas técnicas sobre la red se puede considerar una importante disminución de gastos para la empresa, ya que se introduce el concepto de convergencia de servicios con ayuda de la plataforma IP, para lo cual es necesario simplemente la negociación de tecnología de acceso, equipamiento y capacidad de la red a ser implementada.

Para esto dentro del estudio, se establece un procedimiento con el cual se puede implementar calidad de servicio sobre cualquier red de datos, este es, identificar cada tipo de tráfico y su comportamiento dentro de la red por medio de una auditoría de red, determinar la importancia de cada tipo de tráfico para el negocio de la compañía u organización por medio de una auditoría de negocio, determinar los niveles de servicios requeridos, marcar y clasificar los diferentes tipos de tráfico de la red, administrar y prevenir la congestión de la red.

Esto se logra a la par con la identificación de las características de las aplicaciones que cruzan por la red y de esta manera, tomar los métodos y técnicas de calidad de servicio correspondientes para un adecuado rendimiento de cada una de las aplicaciones en situaciones extremas dentro de la red de datos; finalmente poder establecer el equipamiento y la estructura dentro de la red de telecomunicaciones.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

802.1p. Estándar IEEE que proporciona priorización de tráfico y filtrado *multicast* dinámico. Proporciona un mecanismo para implementar QoS a nivel de MAC

ACLs. Son herramientas utilizadas para el filtrado de paquetes en función de ciertos parámetros como direcciones IP de origen y destino, puertos de origen y destino, tipo de protocolo, entre otros

AF. Es usado para proveer servicios asegurados al cliente, de modo que el cliente recibirá servicios fiables incluso en tiempos de congestión de red

Ancho de banda. Se refiere a la capacidad del canal usada o disponible

ATM. El modo de transferencia asíncrona

Bc. Tasa de ráfaga comprometida

Be. Tasa de ráfaga en exceso

Buffer. Registro de almacenamiento

CAR. Característica de QoS en los enrutadores que limitan la entrada o la salida de la tasa de transmisión en una interfaz basada en criterios de clasificación de paquetes

CBR. Tipo de *bit rate* en el que la velocidad de *bits* no varía

CBWFQ. Extiende la funcionalidad estándar de WFQ para proporcionar apoyo para las clases de tráfico definidas por usuarios

CE. Es el dispositivo de borde del consumidor

CIR. Es la tasa que se compromete el proveedor en entregar al cliente

Congestión. Se refiere a la ocupación de todo el ancho de banda del canal disponible

Conmutadores. Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 del modelo OSI

CoS. Es una técnica o método usado para entregar QoS dentro de una red

CQ. Tipo de encolamiento personalizado

CRC. Es un mecanismo de detección de errores en sistemas digitales

DCBWFQ. Extiende la funcionalidad estándar para proporcionar apoyo para clases de tráfico definidas por usuario en el procesador de interface versátil

Delay. Retardo de paquete

DiffServ. Servicio Diferenciado

DS3. Circuito digital con características de operación estandarizada y capacidad de transmisión igual a 28 DS1o 45.304 Mbps

DSCP. Hace referencia al segundo byte en la cabecera de los paquetes IP que se utiliza para diferenciar la calidad en la comunicación que quieren los datos que se transportan

DTE. Equipo terminal de datos, es el equipo donde los datos tienen origen y destino

DTS. Modelación de tráfico distribuido

DWFQ. Es una versión especial de alta velocidad de WFQ que corre sobre tarjetas VIP

Eco ICMP. Es un mensaje generado como contestación a un mensaje *Echo Request* (petición de Eco)

EF. Es usado para proveer servicios *premium* a los clientes

Enrutador. Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres del modelo OSI

Enrutadores de edge. Son enrutadores en la frontera de la red de backbone y la red de acceso

ETSI. Estandarización de la industria de las telecomunicaciones de Europa

FBWFQ. Se refiere a un método de identificación de cadenas de comunicación

FBWRED. WRED basado en flujo

FIFOQ. Tipo de encolamiento donde la información que ingresa primero sale primero, encolamiento básico

Flujo. Movimiento de tráfico en una dirección

FTP. Es un protocolo estándar utilizado para la transferencia de archivos de un ordenador a otro

GTS. Modelación de tráfico genérico

Hardware. Es la parte física de los dispositivos computacionales

Hosts. Son equipos conectados a la red, que proveen o utilizan servicios a/de ella

IETF. Comunidad de profesionales de muy diversos ámbitos, encargados de coordinar el uso y funcionamiento del Internet

IntServ. Servicio Integrado

IP RTP. Proporcionan un esquema de encolamiento de prioridad estricto para datos sensibles al retardo como los de voz

IPv4. Protocolo de Internet versión 4

IPv6. Protocolo de Internet versión 6

ITU-T. Organismo internacional para la estandarización y normalización en telecomunicaciones, antes denominado CCITT

Jitter. Variación del retardo

Leaky bucket. Algoritmo utilizado para controlar la tasa en la cual los datos son inyectados dentro de una red. Utiliza las siguientes especificaciones: considerar una cubeta con un hueco en el fondo; si los paquetes arriban son ubicados dentro de la cubeta, si la cubeta está llena estos son descartados; los paquetes en la cubeta son enviados con una tasa constante, equivalente al tamaño del hueco en esta

LLQ. Encolamiento de baja latencia

MAC. Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una Ethernet de red

MPLS. Es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes

MTU. Es la máxima unidad de transmisión

P. Término que define a los enrutadores dentro de la red del proveedor de servicios

PE. Es el dispositivo de borde del proveedor

PHB. Es una descripción observada externamente del comportamiento de envío de un nodo DS aplicada a un *behavior agregate* DS en particular

PIR. Es la tasa pico a la que puede llegar el tráfico del cliente

PQ. Clase de encolamiento de prioridad

PSTN. Red telefónica tradicional

QoS. Se refiere al desempeño del sistema de transmisión

RED. Es un algoritmo de gestión de cola activo

Red de backbone. Conjunto de equipos interconectados que transportan los datos

RER. Tasa de error residual

RSVP. Protocolo de señalización de la capa de transporte diseñado para reservar recursos de una red bajo la arquitectura de servicios integrados

SDH. La jerarquía digital síncrona

Sincronización global. Puede pasar a TCP / IP flujos durante períodos de congestión, ya que cada emisor reducirá su velocidad de transmisión en el momento mismo cuando se produce la pérdida de paquetes

SLA. Es un acuerdo de niveles de servicio que se firma entre el proveedor y el cliente

SNA. Conjunto de protocolos de comunicaciones para manejo de redes

Software. Es la parte lógica de los dispositivos computacionales

TCA. Es un acuerdo que especifica las reglas de clasificación y cualquier correspondiente perfil de tráfico a ser aplicados sobre los flujos de información

TCP/IP. Protocolo estándar para la transmisión de datos por Internet. Proporciona comunicación entre redes interconectadas formadas por equipos con distintas arquitecturas de hardware y distintos sistemas operativos

Throughput. Cantidad de datos movidos satisfactoriamente desde un punto hacia otro en un tiempo de periodo dado dentro de una comunicación

Token bucket. Es una definición formal para tasa de transferencia

Token Ring. Arquitectura de red desarrollada con topología lógica en anillo y técnica de acceso de paso de testigo

ToS. Tipo de servicio, campo dentro de la cabecera IP

Tráfico. Es el flujo de información por la red

VAD. Es una detección de actividad de voz

VoIP. Es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP

WFQ. Técnica de encolamiento que proporciona QoS en redes convergentes y trata de evitar la congestión controlando directamente las colas de los nodos mediante un tratamiento diferencial del tráfico proporcionado por una determinada disciplina de servicio

WRED. RED ponderado

CAPÍTULO 1

QUÉ ES LA CALIDAD DE SERVICIO

1.1. CONCEPTOS DE CALIDAD DE SERVICIO

Tomando como referencia estándares internacionales acerca del término calidad, se lo puede definir como un conjunto de características cualitativas y cuantitativas de una entidad que tiene que ver con la habilidad para satisfacer necesidades indicadas e implícitas.

De acuerdo a ITU-T (*International Telecommunication Union – Telecommunication Standardization Sector*) y a ETSI (*European Telecommunications Standards Institute*), la calidad de servicio QoS (*Quality of Service*) se interpreta como el efecto colectivo de funcionamiento del servicio el cual determina el grado de satisfacción de un usuario del servicio especificado.

En cambio la IETF (*Internet Engineering Task Force*) considera que la calidad de servicio QoS es la habilidad de segmentar tráfico o diferenciar entre los distintos tipos de tráfico que cruzan la red de datos para que cada flujo sea tratado distintamente.

Desde el punto de vista de la red de comunicación, la calidad de servicio QoS permite una administración y control de características de algunos tipos de tráfico, tal es el caso de audio, video, reproducción de imagen fija y datos digitales, dentro de los que se incluye aplicaciones de software, documentos, base de datos y archivos.

En definitiva, la calidad de servicio QoS permite una gestión de los flujos de tráfico ocasionados por los diferentes tipos de servicio que cruzan por la red de comunicación y con ello realizar una entrega de información con ciertas características que satisfagan la percepción del usuario final sobre las aplicaciones reproducidas.

1.2. PARÁMETROS DE CALIDAD DE SERVICIO

Los parámetros de QoS representan para el usuario final en sí la calidad de su servicio, ya que con el control de estos se puede tener un grado de aseguramiento de los servicios sobre la red de comunicación. Estos parámetros pueden cambiar de acuerdo al tipo de servicio, pero se enunciará a continuación los parámetros genéricos requeridos sobre una red de servicios convergentes.

1.2.1. Throughput

El *throughput* es un parámetro de modo de conexión que tiene una significación desde el inicio hasta el final de la entrega de información y se define como el número total de bits transferidos satisfactoriamente por una secuencia primitiva, dividido para el tiempo de entrada/salida en segundos de esta secuencia.

La transferencia satisfactoria de un paquete es definida como la entrega de información al destinatario adecuado sin errores, en la misma secuencia y antes de que el receptor termine la conexión en curso.

1.2.2. Retardo de paquete

El retardo o *delay* de paquete es el tiempo tomado por un paquete en viajar desde un punto de acceso de servicio hacia un destino determinado. Generalmente este parámetro incluye el tiempo de transporte en la red y el retardo de encolamiento del mismo.

1.2.3. Ancho de banda

El ancho de banda se refiere a la capacidad del canal usada o disponible. Los proveedores de servicio generalmente aseguran el máximo ancho de banda al cliente y esto debe estar claramente especificado dentro del acuerdo de nivel de servicio SLA (*Service Level Agreement*).

1.2.4. Tasa de error residual

La tasa de error residual RER (*Residual Error Rate*) es la porción total de paquetes erróneos, perdidos y duplicados en una transferencia de información entre usuarios durante un período de tiempo.

1.2.5. Variación del retardo

La variación del retardo puede causar el incremento de temporizadores de retransmisión ***TCP***[1] (*Transmission Control Protocol*) y una innecesaria pérdida de paquetes; por lo tanto, la variación del retardo en un parámetro muy importante dentro de la calidad de servicio, el mismo que puede ser medido por la dispersión del máximo retardo y el mínimo retardo durante un corto intervalo. Este parámetro es conocido como *jitter*.

1.2.6. Tasa de pérdida

La tasa de pérdida es la porción de paquetes perdidos del total de paquetes en tránsito entre un origen y un destino durante un intervalo de tiempo específico, el mismo que se encuentra expresado en porcentajes.

1.2.7. Disponibilidad

La disponibilidad es el porcentaje de la viabilidad del servicio en cada requerimiento de servicio particular, es decir, conectividad y funcionalidad en la capa de administración de la red. Conectividad se refiere a la conectividad física de los elementos de red y funcionalidad significa si los dispositivos de red asociados trabajan bien o no.

1.3. PARÁMETROS DE TRÁFICO

A continuación se presenta una referencia de parámetros de tráfico que son usados comúnmente para categorizar el flujo de información.

1.3.1. Tasa pico

La tasa pico es la tasa más alta en la cual una fuente de información puede generar tráfico. Está limitada por la tasa de enlace de transmisión y puede ser calculada del tamaño del paquete y el espacio entre paquetes consecutivos.

1.3.2. Tasa promedio

La tasa promedio es una tasa promediada sobre un determinado intervalo de tiempo y puede ser calculada de varias formas, y sus resultados pueden ser bastante diferentes. Es

[1] ***TCP***. Protocolo que proporciona un servicio de comunicación que forma un circuito, es decir el flujo de datos entre el origen y destino parece que sea continuo. Es orientado a la conexión, tiene chequeo de errores, control de flujo y capacidad de interrupción

importante conocer el método exacto y el intervalo de tiempo usado en el cálculo de la tasa promedio.

1.3.3. Tasa excedida

La tasa excedida está definida como la máxima cantidad de datos que pueden ser inyectados dentro de la red en la tasa pico. El tamaño de exceso refleja las ráfagas de tráfico enviadas desde una fuente de información.

1.4. ARQUITECTURA BÁSICA DE CALIDAD DE SERVICIO

Se configura características de calidad de servicio a través de la red con el objetivo de una entrega de calidad de servicio punto a punto. Los siguientes tres componentes son necesarios para una entrega de calidad de servicio a lo largo de toda la red:

- Calidad de servicio dentro de un elemento de red solo, esto incluye encolamiento, planificación y características de modelación de tráfico

- Técnicas de señalización de calidad de servicio para la coordinación de la entrega de información punto a punto entre los elementos de la red

- Políticas de calidad de servicio y funciones de administración para controlar y manejar el tráfico punto a punto a través de la red

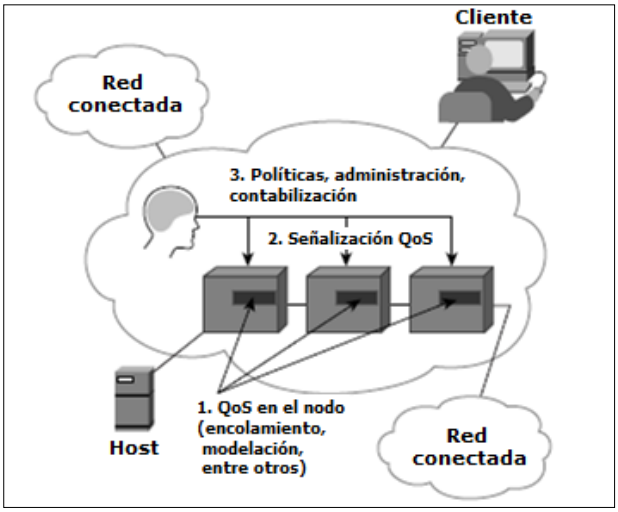


Figura. 1.1. Implementación básica de calidad de servicio[2]

[2] Internetworking Technology Handbook - Quality of Service (QoS) - Cisco Systems, http://www.cisco.com/en/US/docs/internetworking/technology/handbook/QoS.html#wp1020570, Publicación 2007, Consultado en Agosto 2009

Es importante tomar en cuenta que no todas las técnicas de calidad de servicio son apropiadas para todos los enrutadores de red, esto porque los enrutadores, tanto de borde o *edge* como de *backbone* en una red, no realizan necesariamente las mismas operaciones y por ende las tareas de calidad de servicio funcionan diferentemente.

Por ejemplo, para configurar una red IP con aplicaciones en tiempo real como el tráfico de voz, se necesita considerar las funciones de estas dos clases de enrutadores (*edge* y *backbone*) en la red, con el fin de seleccionar las características adecuadas de calidad de servicio.

Generalmente los enrutadores de *edge* cumplen con las siguientes funciones de calidad de servicio:

- Clasificación de paquetes
- Control de admisión
- Administración de configuración

En cambio, los enrutadores de *backbone*, presentan las siguientes funciones de calidad de servicio:

- Administrar la congestión de tráfico
- Evitar o prevenir la congestión de tráfico

1.5. BENEFICIOS DE LA IMPLEMENTACIÓN DE CALIDAD DE SERVICIO

Todas las redes pueden tomar ventaja de los aspectos de calidad de servicio para tornarse óptimas y eficientes. Diferentes categorías de usuarios de red poseen sus propios requerimientos de calidad de servicio en muchas áreas.

Redes empresariales, por ejemplo, deben poseer soluciones de calidad de servicio punto a punto a través de varias plataformas que comprende la red; proveer soluciones para plataformas heterogéneas requiere que se tome un enfoque diferente para la configuración de QoS en cada tecnología. Como las redes empresariales llevan aplicaciones complejas y

tráfico incrementado de aplicaciones Web multimedia, QoS sirve para priorizar este tráfico asegurando que cada aplicación alcance su fin requerido.

Los proveedores de servicios requieren escalabilidad y rendimiento asegurados. Por ejemplo, los ISPs siempre han ofrecido conectividad IP de mejor esfuerzo, ahora también transfieren datos de voz, video y otras aplicaciones en tiempo real. Las respuestas de calidad de servicio en cuanto a escalabilidad y rendimiento se necesita en este punto para poder distinguir diferentes tipos de tráfico.

En los segmentos de negocios de tamaño pequeño y mediano, los administradores están experimentando de primera mano el crecimiento de los negocios sobre la plataforma ***TCP/IP***[3]. Estos negocios sobre la red deben ser también implementados sobre aplicaciones complejas. La calidad de servicio deja que la red maneje la vía más eficiente en la conexión para dichas aplicaciones de negocios.

1.6. DESPLIEGUE DE CALIDAD DE SERVICIO DENTRO DE UNA RED

Las diferentes tareas de calidad de servicio que se pueden implementar en los dispositivos de red permiten a redes complejas controlar y servir fiablemente una gran variedad de aplicaciones de red y tipos de tráfico.

Cualquier red puede tomar las ventajas de calidad de servicio para una eficiencia óptima, si esta es una red corporativa pequeña, un proveedor de servicios o una red empresarial.

Aplicar técnicas de calidad de servicio promueve las siguientes características:

- Control sobre los recursos. Se tiene control sobre los diferentes recursos de la red, esto es ancho de banda, equipamiento, facilidades de área amplia, etc., que están siendo usados. Por ejemplo, se puede limitar el ancho de banda consumido sobre un enlace de backbone por transferencias ***FTP***[4] (*File Transfer Protocol*) o dando prioridad para el acceso a una importante base de datos

- Uso más eficiente de los recursos de red. Se conocerá que la red está siendo usada y que está corriendo diferentes servicios para el tráfico más importante del negocio

[3] ***TCP/IP***. Protocolo estándar para la transmisión de datos por Internet. Proporciona comunicación entre redes interconectadas formadas por equipos con distintas arquitecturas de hardware y distintos sistemas operativos
[4] ***FTP***. Es un protocolo estándar utilizado para la transferencia de archivos de un ordenador a otro

- Servicios adaptados. El control y la visibilidad entregada por la calidad de servicio, permite a los proveedores de servicios ofrecer un grado adaptado de servicios diferenciando a cada cliente

- Coexistencia de aplicaciones críticas. Las tecnologías de calidad de servicio permiten que la parte WAN de los enlaces sea usada eficientemente para aplicaciones críticas que son muy importantes para un determinado negocio, que el ancho de banda y los mínimos retardos requeridos para aplicaciones en tiempo real estén disponibles, y que otras aplicaciones usadas en el enlace alcancen su objetivo sin interferir con el tráfico de las aplicaciones críticas

1.7. CALIDAD DE SERVICIO EN IPv4 E IPv6

El protocolo de Internet IP (*Internet Protocol*) original es no orientado a la conexión y ofrece servicios del mejor esfuerzo, es decir sin ninguna identificación de calidad de servicio. El servicio recibido por un usuario final depende de la carga de la red de comunicación. La administración de colas dentro de los enrutadores es esencialmente a través de FIFO (*First In First Out*). En relación a las herramientas para identificar el flujo de tráfico, IP necesita ser diferenciado entre las versiones 4 y 6.

IPv4 ofrece dos maneras para marcar el tráfico:

1. Un vector compuesto por los siguientes campos: dirección IP origen, dirección IP destino, protocolo (los que se ubican en la cabecera IPv4), puerto TCP/UDP origen y puerto TCP/UDP destino, que se encuentran en la cabecera TCP/UDP. Esta opción está representada en la figura. 1.2., la misma que muestra la cabecera IPv4.

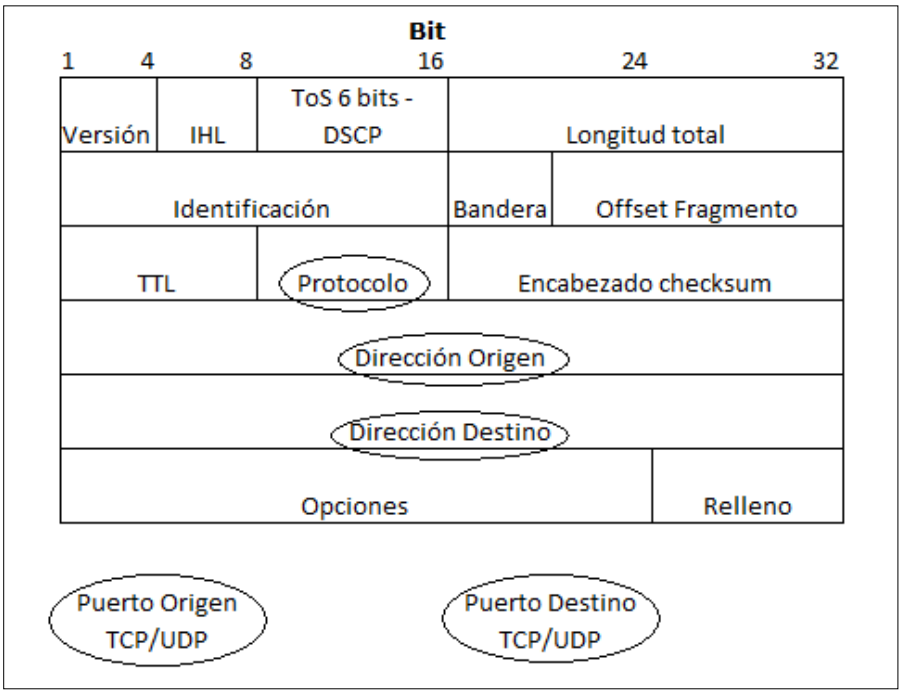


Figura. 1.2. Cabecera de paquete IPv4 e identificadores de flujo simple[5]

2. El campo ToS (*Type of Service*), el mismo que consta de 8 bits en la cabecera IPv4, de los cuales los 6 primeros bits definen campo DSCP (*Differentiated Services CodePoint*). Los paquetes que se envían a través de la red con el mismo identificador DSCP necesitan ser tratados coherentemente por cada enrutador que conforman la red. Esta opción se visualiza en la figura. 1.3.

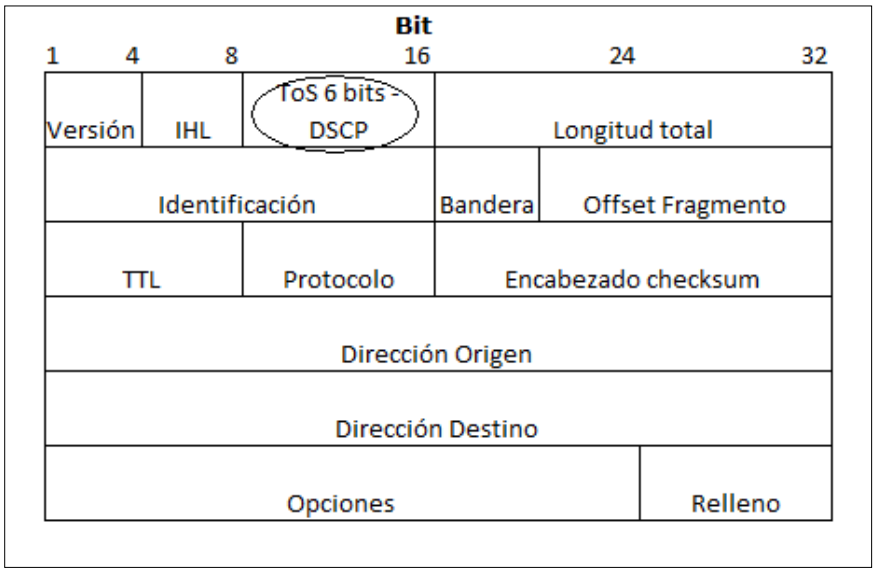


Figura. 1.3. Cabecera de paquete IPv4 e identificador de grupo de flujos[6]

[5] Marchese, Mario, *QoS over Heterogeneous Networks*, Editorial John Wiley&Sons LTD, England 2007, página 30
[6] Marchese, Mario, *QoS over Heterogeneous Networks*, Editorial John Wiley&Sons LTD, England 2007, página 30

La identificación del tráfico solamente es el inicio para garantizar la calidad de servicio dentro de una red de comunicación. Dos paradigmas han sido propuestos para juntar los requerimientos del mercado de QoS en redes IP: Servicios Integrados y Servicios Diferenciados, que se los tratará más adelante dentro de este trabajo.

En cambio, en IPv6 y para tener un conocimiento oportuno porque el trabajo se enfoca a IPv4, se usan dos campos directamente en la cabecera IP para la marcación del tráfico, como se muestra en la figura. 1.4.:

1. Campo Etiqueta de Flujo, que consta de 20 bits, y,

2. Campo Clase de Tráfico, formado por 8 bits, funcionalmente equivalente al campo ToS dentro de IPv4 y conteniendo el campo DSCP en los primeros 6 bits.

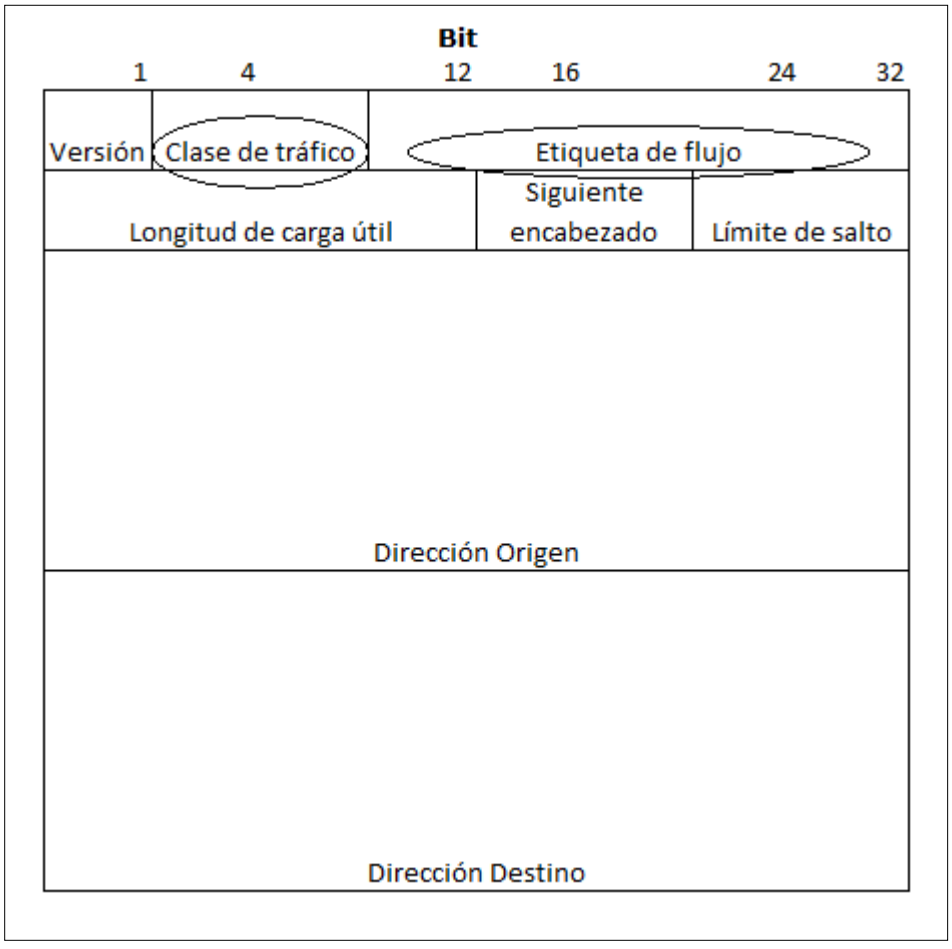


Figura. 1.4. Cabecera de paquete IPv6 e identificadores de flujo[7]

[7] Marchese, Mario, *QoS over Heterogeneous Networks*, Editorial John Wiley&Sons LTD, England 2007, página 39

La diferencia entre IPv4 e IPv6 es que IPv6 puede realizar marcación de tráfico a través de la etiqueta de flujo, así como un conjunto de flujos, a fin de mantener total escalabilidad juntos con el poder teórico para identificar un cliente simple, mientras que IPv4 puede identificar cualquier número limitado de flujos a través del campo DSCP o un flujo específico a través del vector dirección IP origen, dirección IP destino, protocolo, puerto TCP/UDP origen, puerto TCP/UDP destino. Por lo tanto, IPv6 desde el punto de vista de identificación de flujo, es una herramienta poderosa, si es usado con todas sus características.

1.8. MODELOS DE SERVICIO

La calidad de servicio dentro de una red de comunicación puede ser separada en tres niveles diferentes, también conocidos como modelos de servicio. Estos modelos de servicio describen un conjunto de capacidades de calidad de servicio punto – punto. La calidad de servicio punto – punto es la habilidad de una determinada red de proveer un específico nivel de servicio al tráfico desde un extremo de la red hacia el otro.

Los servicios difieren en su respectivo nivel de rigor de QoS, los mismos que describen cómo el servicio puede ser atado fuertemente por características de un específico ancho de banda, retardo, *jitter* y pérdidas.

1.8.1. Servicio del mejor esfuerzo

El servicio del mejor esfuerzo, también conocido como carencia de QoS, se presenta cuando la red trata de hacer un posible intento de entregar un determinado paquete a su destino, es decir, con este servicio no se garantiza que el paquete alcance su destino predeterminado.

Una aplicación puede enviar datos en cualquier cantidad, cuando lo necesite, sin solicitud de permisos o notificaciones de la red de comunicación. Algunas aplicaciones pueden trabajar bajo este modelo, como por ejemplo FTP, que puede soportar este servicio sin mucha dificultad.

Sin embargo, este servicio no es óptimo para aplicaciones que son sensibles a los retardos de la red, a las fluctuaciones de ancho de banda, y otras condiciones de cambio de la red. Por ejemplo, se tiene a la telefonía sobre la red de comunicación que requiere una mayor cantidad de consistencia en ancho de banda para funcionar correctamente. El

resultado del servicio del mejor esfuerzo sobre estas aplicaciones podría provocar fallo en las llamadas o interrupciones en el diálogo durante las mismas.

1.8.2. Servicio integrado

El servicio integrado es un mecanismo punto – punto basado en el flujo de tráfico para proveer calidad de servicio en la red. Los enrutadores deben mantener la pista sobre cada uno de estos flujos. Este modelo reserva los recursos a lo largo del trayecto de transmisión de la información vía RSVP (se tratará posteriormente a detalle), es decir, establece un circuito virtual.

Durante el proceso de reservación, un requerimiento se dirige a través del control de admisión, el mismo que concederá o denegará el requerimiento. Esto es realizado basándose en los recursos disponibles en cada enrutador, y es necesario preservar los requerimientos de QoS para otros flujos de tráfico activos en ese momento en el enrutador.

Se tiene dos clases de servicio dentro de este modelo: el servicio garantizado y el servicio de carga controlada.

Servicio garantizado.

Esta clase de servicio es usada para aplicaciones intolerables a la reproducción sin distorsión como la videoconferencia, por ejemplo. Esta clase ofrece perfecta confiabilidad sobre el límite superior de retraso.

Servicio de carga controlada.

También conocido como servicio predictivo, esta clase de servicio es más relajada sobre el límite de retraso. Es bastante confiable, pero no perfectamente confiable en proveer el límite de retraso.

Este servicio trabaja bien cuando la red está ligeramente cargado, sin embargo, si la red está saturada, se puede experimentar algunos paquetes perdidos o retardos. Este es el punto medio entre garantizado y mejor esfuerzo; pudiendo ser utilizado en aplicaciones tolerantes como video MPEG-2.

Esta clase de servicio es más eficiente en la utilización de los recursos porque permite otros flujos de tráfico para compartir sus recursos cuando no están en uso. Por

ejemplo, una aplicación puede necesitar 5 Mbps, pero la tasa de bit puede variar entre 2 y 5 Mbps; en lugar de perder los 3 Mbps extras, esta clase permite otro flujo de tráfico para usar los 3 Mbps extras.

Arquitectura de servicios integrados.

Un marco de referencia de aplicación ha sido especificado en ***RFC 1633***[8], para entender el modelo de servicios integrados en base a su arquitectura. La figura. 1.5., muestra los principales componentes en el modelo de referencia. El modelo puede ser dividido lógicamente en dos planos: el plano de control y el plano de datos.

La función del plano de control es la creación de la reservación de recursos; en cambio, el plano de datos tiene como fin el envío de paquetes de datos basados en el estado de reservación.

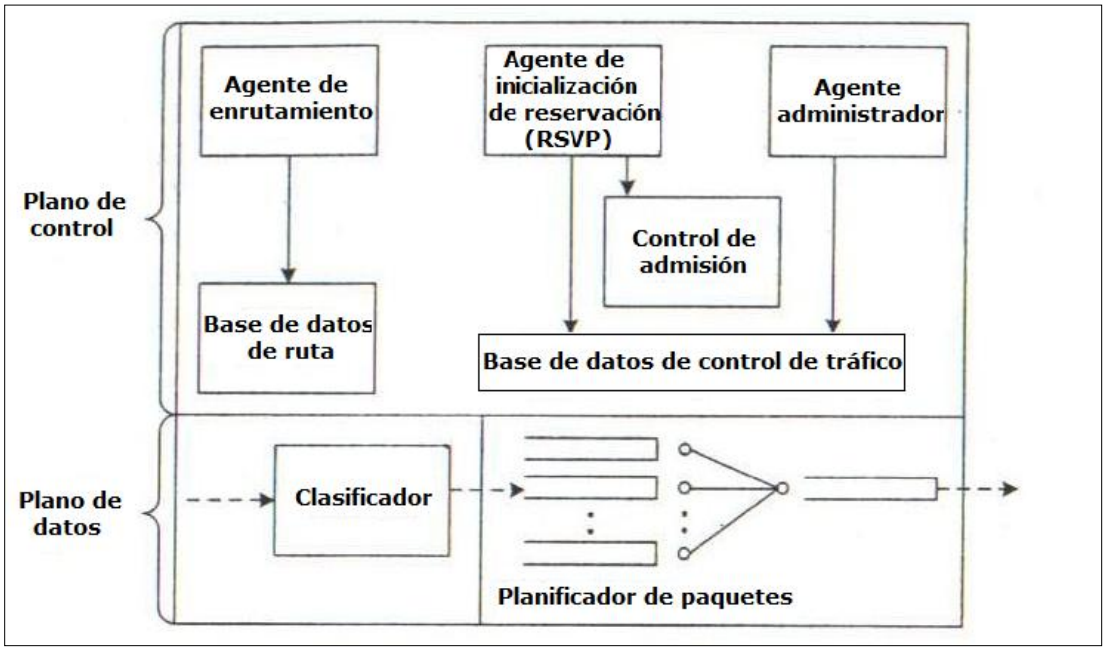


Figura. 1.5. Modelo de referencia *IntServ* para enrutadores[9]

Se detalla a continuación un resumen de los principales elementos en el modelo de referencia para los servicios integrados.

[8] ***RFC 1633***. Arquitectura de Servicios Integrados en el Internet
[9] Chao, Jonathan; Liu, Bin, *High Performance Switches and Routers*, Editorial Wiley-Interscience a John Wiley&Sons INC Publication, United States of America 2007, página 118

Protocolo de reserva de recursos.

Las conexiones son establecidas usando un agente de configuración de reservación conocido como protocolo de reserva de recursos RSVP (*Resource Reservation Protocol*), el mismo que realiza reservas punto – punto sobre una red no orientada a la conexión.

RSVP es responsable del cambio de la base de datos de control de tráfico (usado para almacenar, clasificar y planificar políticas) para acomodar los requerimientos de QoS. El agente de administración es usado para crear las políticas del clasificador y del planificador de paquetes.

Características del RSVP.

- Es un protocolo de señalización para establecer una ruta de QoS garantizado entre el origen y el destino de la información
- Establece reservas punto – punto sobre redes no orientadas a conexión
- Es robusto cuando los enlaces presentan fallas, el tráfico es reenrutado y una nueva reserva se establece
- Es simple (reserva el tráfico de datos unidireccional) y receptor orientado
- Opera en *estado suave*, responde a cambios en el enrutamiento
- Provee operación transparente a través de enrutadores que no soportan RSVP
- Es independiente de las versiones del protocolo IP, es decir, se aplica igualmente tanto para IPv4 como para IPv6

Operación del RSVP.

La figura. 1.6., muestra como RSVP establece las reservaciones de recursos entre orígenes y destinos.

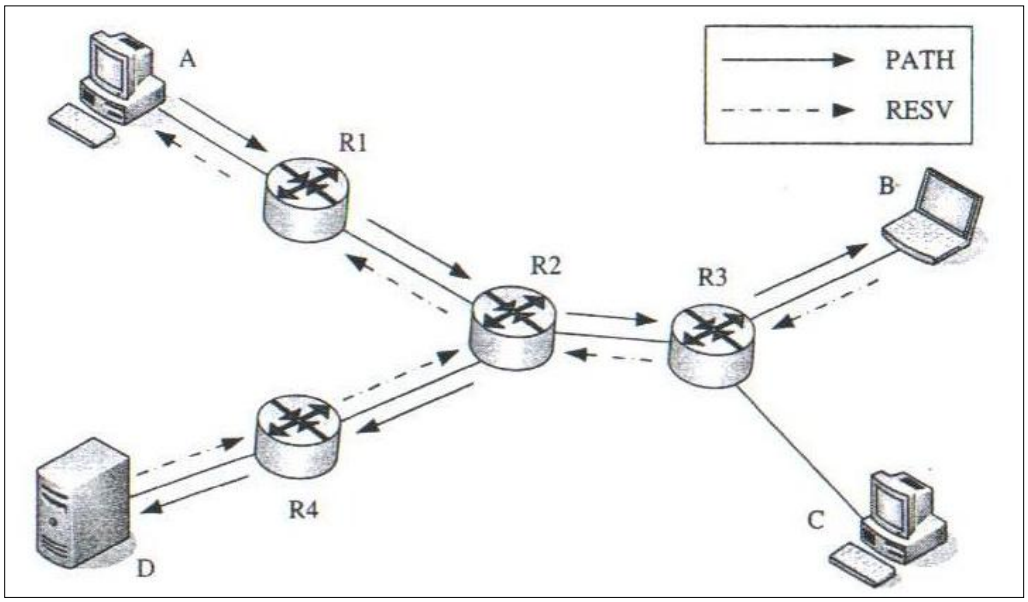


Figura. 1.6. Operaciones RSVP[10]

El requisito clave para recordar con RSVP es que el receptor es el nodo que solicita los recursos de QoS especificados, no el emisor.

El procedimiento de RSVP consiste en que el emisor envía un mensaje de ruta en bajada hacia el nodo receptor. Este mensaje de ruta recoge la información sobre los parámetros y capacidades de QoS de cada nodo en la ruta del tráfico. Cada nodo intermedio mantiene la caracterización de ruta para los transmisores de tráfico en los parámetros *Tspec* de envío.

Luego de ello, el receptor procesa los requerimientos en conjunto con las habilidades de QoS de los nodos intermedios y después envía una solicitud de reserva calculada *Resv* en subida hacia el transmisor a lo largo de la misma ruta de salto. Este mensaje de retorno especifica los parámetros de QoS deseados, los mismos que son asignados al tráfico de datos en cada nodo de la ruta. Solo después de que el transmisor recibe el mensaje *Resv* satisfactorio desde el receptor destinado comienza un flujo de datos. Esta operación del RSVP maneja algunos mensajes en la ruta del tráfico, los mismos que se detallan.

Mensajes de solicitud de reserva.

Estos mensajes son enviados por cada *host* receptor hacia el nodo de transmisión. Cada mensaje es responsable de la creación de parámetros de QoS adecuados a lo largo de

[10] Chao, Jonathan; Liu, Bin, *High Performance Switches and Routers*, Editorial Wiley-Interscience a John Wiley&Sons INC Publication, United States of America 2007, página 119

la ruta de salto reversa. Los mensajes *Resv* contienen información que definen el estilo de reserva, el filtro *spec* que identifica el transmisor y el objeto de flujo *spec*. El flujo *spec* es usado para crear un proceso clasificador de paquete de nodo y el filtro *spec* es utilizado para controlar el clasificador de paquete.

Los mensajes *Resv* son enviados periódicamente para mantener el estado de reserva a lo largo de la ruta del flujo de información; a diferencia de un circuito conmutado, el flujo de información es conocido como un circuito de *estado suave* y puede ser modificado durante el período de comunicación.

El parámetro de flujo *spec* difiere dependiendo del tipo de reserva que se solicita. Si solo un servicio de carga controlada está siendo requerido, el flujo *spec* solo contendrá un *Tspec* de receptor; sin embargo, si un servicio garantizado es requerido, el flujo *spec* contiene los elementos *Tspec* y *Rspec*.

Mensajes de ruta.

El mensaje de ruta contiene tres elementos informativos: la plantilla de emisor, el *Tspec* de emisor y el *Adspec*.

La plantilla de emisor contiene información que define el tipo de tráfico de datos que el emisor estará enviando. Esta plantilla está compuesta de una especificación de filtro que únicamente identifica el flujo de datos del emisor desde otros nodos. El *Tspec* de emisor define las propiedades del flujo de datos que el emisor espera generar. Ninguno de estos parámetros son modificados por nodos intermedios en el flujo de información, sino más bien sirven como únicos identificadores.

El *Adspec* contiene información única que se pasa a cada uno de los nodos de control de procesos. Cada nodo basa sus características de QoS y manipulación de paquetes en *Adspec* y actualiza este campo con información de control relevante que es pasada en la subida a los nodos cuando esta sea necesaria. El *Adspec* también transporta bits bandera que son usados para determinar si el nodo no-IntServ o no-RSVP está en la ruta de datos trazada. Si por ejemplo un bit es configurado, toda la información en el *Adspec* es considerada poco fiable y puede resultar una clase de entrega del mejor esfuerzo.

Mensajes de error y confirmación.

Existen tres tipos de mensaje de error y confirmación: mensajes de error de ruta (*Patherr*), mensajes de error de solicitud de reserva (*Resverr*) y mensajes de reconocimiento de solicitud de reserva (*Resvconf*).

Los mensajes *Patherr* y *Resverr* son simplemente enviados en la subida hacia el emisor que creó el error, pero no modifican el estado de ruta en cualquiera de los nodos por donde pasan. El mensaje *Patherr* indica un error en el proceso de la declaración de la ruta y es enviado al emisor de datos. El mensaje de *Resverr* indica un error en el proceso de mensajes de reserva y es enviado al receptor.

Los mensajes de error que pueden ser incluidos son:

- Falla de admisión
- Ruta ambigua
- Ancho de banda no disponible
- Especificación de flujo malo
- Servicio no soportado

Los mensajes de confirmación pueden ser enviados por cada nodo en una ruta de flujo de datos si una reserva RSVP desde el nodo receptor es recibida la cual contenga un objeto de confirmación de reserva opcional.

Mensajes de derribo.

Los mensajes de derribo son usados para remover el estado y la ruta de reserva desde todos los nodos habilitados con RSVP en una ruta de flujo de datos sin la espera de un corte de comunicación. El derribo puede ser iniciado por el nodo emisor o receptor, o por un nodo de tránsito intermedio si este ha alcanzado un estado de corte de comunicación.

Hay dos tipos de mensajes de derribo soportados por RSVP: derribo de ruta y derribo de solicitud de reserva. El derribo de ruta elimina el estado de ruta y todos los estados de reserva asociados en la ruta de flujo de datos, efectivamente, esto marca la terminación del

flujo de datos individual y libera los recursos de la red. El derribo de solicitud de reserva elimina el estado de reserva de QoS pero mantiene el flujo de ruta fijo. Estos mensajes son usados principalmente si el tipo de comunicación entre los puntos extremos cualitativamente cambia y requieren de diferentes parámetros de QoS.

Clasificador.

Los paquetes necesitan ser mapeados en alguna clase para el proceso de control de tráfico. Los paquetes de la misma clase tendrán el mismo trato del planificador de paquete. Una clase puede ser basada en cabeceras de red, cabeceras de transporte, cabecera de aplicación o cualquier combinación de estas. Por ejemplo, un flujo IP es normalmente identificado por la dirección IP de origen, la dirección IP destino, el ID de protocolo, el puerto origen y el puerto destino.

Control de admisión.

El control de admisión es responsable de permitir o denegar flujos en el enrutador. Es usado para decidir si un nuevo flujo puede ser concedido para el QoS solicitado sin realizar garantías. Si el enrutador decide que no tiene recursos solicitados para cumplir el QoS requerido, el flujo alcanza una admisión denegada.

El control de admisión posee dos funciones básicas. La primera es determinar si una nueva reserva puede ser creada en base a políticas de control de admisión. La segunda función es monitorear y medir los recursos permitidos.

Enfoque basado en los parámetros y enfoque basado en la medición son los dos métodos básicos del control de admisión. En el enfoque basado en parámetros, un grupo de parámetros se utiliza precisamente para caracterizar flujos de tráfico; luego, el agente de control de admisión calcula el recurso requerido basado en estos parámetros. En lugar de depender de una caracterización previa de tráfico, el enfoque basado en la medición mide la carga de tráfico actual y la usa para el control de admisión.

Planificador de paquetes.

El planificador de paquetes reordena la transmisión del paquete de modo que algunos flujos pueden ser colocados en base a sus niveles y clase de servicio. Por ejemplo, paquetes

que requieren servicio garantizado serían colocados antes de aquellos que requieren un servicio de carga controlado o un servicio de mejor esfuerzo.

El planificador de paquete es responsable de hacer cumplir la asignación de recursos, los cuales afectan directamente al retardo. La tarea principal de un planificador de paquete es seleccionar el paquete para transitar cuando el enlace saliente esté listo.

1.8.3. Servicio diferenciado

El servicio integrado y el RSVP proveen una estructura para un control muy detallado de QoS para tráfico individual que recorre una red IP de enrutadores. Lastimosamente, la escalabilidad de la solución de servicio integrado, el mismo que es principalmente causado por su compleja clasificación y planificación por flujo, aún continúa en duda. El servicio integrado requiere enrutadores para almacenar y procesar cada flujo individual que va atravesándolos, lo cual es abrumador en el Internet.

La arquitectura del servicio diferenciado DS (*Differentiated Services o DiffServ*) fue entonces desarrollada relativamente simple, en respuesta a la necesidad, creando métodos para proveer diferentes niveles de servicio para el tráfico de datos.

La ventaja del DS es que muchos flujos de tráfico pueden ser agregados en uno de un conjunto pequeño de agregados de comportamiento, usando el mismo comportamiento por salto PHB (*Per Hop Behavior*) transmitido en el enrutador, de esta manera simplificando el procesamiento y almacenamiento asociado.

El PHB es una descripción del comportamiento de transmisión observable externamente de un nodo DS aplicada a un particular comportamiento DS agregado. Además, no existe señalización, distinto de lo que se lleva a cabo en el punto de código DS DSCP (*DS Codepoint*) de cada paquete. Otro proceso relacionado no es requerido en el núcleo de la red DS, desde que la calidad de servicio es invocada en una base de paquete por paquete. Antes de mostrar los detalles, se presenta un breve resumen del *DiffServ*:

- Demandas de los clientes por una diferencia de servicio
- Surgimiento de nuevas aplicaciones multimedia para las cuales el servicio del mejor esfuerzo en la actualidad no pueden soportar

- Definición del significado del campo DS, esto es, el campo de tipo de servicio ToS en IPv4 o el campo clase de tráfico en IPv6, en la cabecera del paquete IP para cada clase de servicio

- Marcar el campo DS de los paquetes basados en sus clases de servicio y procesados diferentemente

- Forzando a la mayor cantidad de complejidad de los nodos internos de una red a nodos frontera, los cuales procesan volúmenes más bajos de tráfico y números más pequeños de flujo

- Descargando el procesamiento por flujo y la administración de estado al nodo frontera

El *DiffServ* es diferente al *IntServ* en muchos aspectos, cuya principal diferencia es que el *DiffServ* distingue un número pequeño de transmisión de las clases en lugar de flujos individuales. *IntServ* utiliza el protocolo de señalización RSVP para reservar los recursos para los flujos individuales, mientras que *DiffServ* asigna recursos en una base por clase la cual está basada en el octeto ToS en la cabecera IPv4 o en el octeto clase de tráfico en la cabecera IPv6.

Cada enrutador a lo largo del camino examina este octeto y fabrica una decisión de QoS basada en las políticas creadas en cada enrutador. Como resultado, toda la información que el enrutador necesita para manejar el paquete está contenida en la cabecera del paquete; entonces los enrutadores no necesitan aprender o almacenar información sobre flujos individuales. No hay necesidad de mensajes de refrescamiento de *estado suave*; no hay la preocupación de los paquetes que temporalmente no alcanzan su propio manejo de QoS después de que han sido reenrutados; no hay el problema de la escalabilidad asociada con la necesidad para el enrutador de manejar paquetes por flujo. Cada enrutador es independiente uno del otro, por lo tanto, para proveer consistencia en QoS, los enrutadores deberían ser configurados con políticas similares.

Acuerdo de nivel de servicio.

El acuerdo de nivel de servicio SLA (*Service Level Agreement*) es un contrato de servicio entre el cliente y un proveedor de servicios, que especifica el servicio de intercambio de información que el cliente debería recibir.

Un cliente puede ser una organización (dominio origen) u otro dominio DS (dominio subida). Donde un dominio DS es un grupo contiguo de nodos que operan con un grupo común de políticas de aprovisionamiento de servicio y definiciones PHB.

Un SLA puede ser dinámico o estático. Los SLAs estáticos son negociados en una base regular, por ejemplo, mensualmente o anualmente. Los SLAs dinámicos en cambio, usan un protocolo de señalización para negociar el servicio sobre demanda.

El SLA típicamente contiene:

- El tipo y naturaleza de servicio a ser proveído, el cual incluye la descripción del servicio a ser proveído, como el manejo de instalación, servicios de red y soporte técnico

- El nivel de desempeño esperado del servicio, el mismo que incluye dos aspectos importantes: fiabilidad y capacidad de respuesta. La fiabilidad incluye disponibilidad de requerimientos, cuando el servicio está disponible y cuáles son los límites sobre la interrupción del servicio que pueden ser esperados. En cambio, capacidad de respuesta incluye qué tan pronto el servicio se realiza en el curso normal de operación

- El proceso para reportar problemas con el servicio, el cual forma una gran parte de un típico SLA. Este incluye información acerca de la persona a ser contactada para la resolución de problemas, el formato en el que las quejas tienen que ser archivadas, los pasos a llevarse a cabo para resolver rápidamente el problema, y más

- El intervalo de tiempo de respuesta y solución del problema, el mismo especifica un tiempo límite en el cual alguien iniciaría la investigación de un problema que fue reportado, y más

- El proceso para el monitoreo y reporte del nivel de servicio, el cual esboza como los niveles de rendimiento son monitoreados y reportados, esto es, quién realizaría el monitoreo, qué tipos de estadísticas serían recolectadas, como serían recolectadas y como acceder a estadísticas pasadas o presentes

- Los créditos, cargas u otras consecuencias para el proveedor de servicios donde no llegue su obligación o responsabilidad

- Cláusulas y limitaciones, incluyendo las consecuencias si el cliente no cumple con su obligación, de calificar el acceso a los servicios. Cláusulas son condiciones bajo las cuales el nivel de servicio no es aplicado, o bajo las cuales esto es considerado no razonable cumplir con el requisito del SLA

Acuerdo de condicionamiento de tráfico.

Un SLA también define un acuerdo de condicionamiento de tráfico TCA (*Traffic Conditioning Agreement*) el cual establece las reglas usadas para realizar el servicio, lo que el cliente debe hacer para alcanzar el servicio deseado y lo que el proveedor de servicios haría para cumplir con los límites.

Un TCA es un acuerdo específico que clasifica las reglas y los correspondientes perfiles de tráfico, además de las reglas de medición, marcado, descartes y/o modelaciones que se aplican en los flujos de tráfico seleccionados por el clasificador.

Un TCA abarca todas las normas de condicionamiento de tráfico explícitamente especificadas dentro de una SLA junto con todas las reglas implícitas desde los requerimientos de servicio pertinentes y/o desde una política de provisión de servicio del dominio DS.

Un perfil de tráfico especifica las propiedades temporales de un flujo de tráfico seleccionado por un clasificador. Este provee normas para determinar si un paquete en particular está en el perfil o fuera del perfil. El concepto de fuera o dentro de perfil puede ser extendido en más de dos niveles, por ejemplo, niveles múltiples de conformidad con un perfil pueden ser definidos y ejecutados.

Como los paquetes dentro de un dominio, pueden ser clasificados dentro de un agregado de tráfico basado en el filtro especificado en la interfaz de entrada de dominio en el enrutador de borde. El filtro debe ser asociado con el perfil de tráfico que especifica la tasa de información comprometida CIR (*Commited Information Rate*) y una información de cómo esta puede ser medida.

El perfil de tráfico también puede incluir otros parámetros de tráfico. Estos parámetros pueden ubicar limitaciones adicionales en paquetes en los cuales la garantía se aplica, o pueden diferenciar más tráfico que excede el CIR. Dichos parámetros podrían

incluir: la tasa de información pico PIR (*Peak Information Rate*), el tamaño ráfaga pico PBS (*Peak Burst Size*), el tamaño ráfaga de exceso EBS (*Excess Burst Size*) o incluso un segundo intervalo de tiempo promedio T2.

Arquitectura de servicios diferenciados.

El DS divide una red en varios dominios como se puede apreciar en la figura. 1.7. La arquitectura de servicios diferenciados se encuentra publicada bajo la ***RFC 2475***[11].

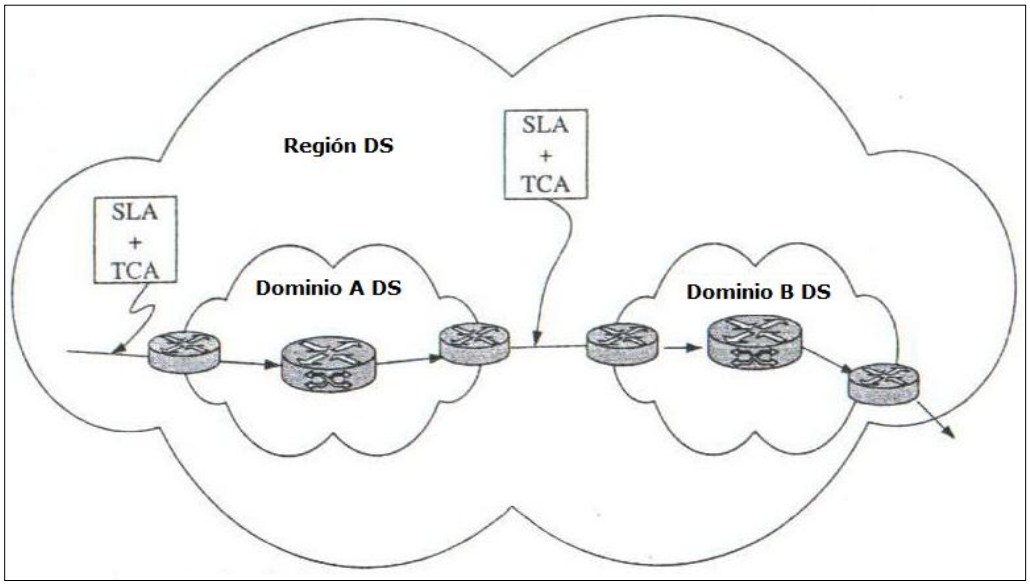


Figura. 1.7. Arquitectura de red de servicios diferenciados[12]

Un dominio DS es un conjunto de nodos que operan con un grupo común de políticas de dotación de recursos y definiciones PHB. Este tiene un límite bien definido y hay dos tipos de nodos asociados con un dominio DS: nodos de borde y nodos interiores. Los nodos de borde o exteriores conectan la nube DS a otros dominios; en cambio, los nodos interiores son conectados a otros nodos interiores o a nodos de borde, pero con el detalle que debe ser dentro del mismo dominio DS.

Los nodos de borde tienen la tarea de clasificar el ingreso de tráfico de manera que los paquetes son marcados apropiadamente para escoger uno de los grupos PHB soportados dentro del dominio. También hacen cumplir el TCA entre su propio dominio DS con el otro dominio al que se conecta. El TCA define las normas usadas para ejecutar el servicio, como lo es la medición, la marcación y el descarte.

[11] ***RFC 2475***. Arquitectura para Servicios Diferenciados
[12] Chao, Jonathan; Liu, Bin, *High Performance Switches and Routers*, Editorial Wiley-Interscience a John Wiley&Sons INC Publication, United States of America 2007, página 124

Los nodos interiores mapean los *codepoints* DS para cada paquete dentro del grupo de PHBs y ejecutan el comportamiento de transmisión apropiado. Cualquier nodo no compatible dentro de un dominio DS resulta en un rendimiento imprevisible y una pérdida de QoS extremo a extremo. Generalmente un dominio DS es formado por una organización Intranet o un proveedor de servicios, esto es, redes controladas por una sola entidad.

DiffServ es extendido a través de dominios por SLA entre ellos. Un SLA especifica normas como marcación de tráfico, acciones a ser tomadas para tráfico fuera de perfil, y otras más. Los TCAs entre dominios son decididos de este SLA.

Dependiendo de la dirección de flujo de tráfico, los nodos límite DS pueden ser nodos de entrada o salida. El tráfico ingresa a la nube DS a través de los nodos de entrada y abandona la nube por los nodos de salida. Un nodo de entrada es responsable del cumplimiento del TCA entre el dominio DS y el dominio del nodo emisor; en cambio, los nodos de salida forman el tráfico de salida para que sea compatible con el TCA entre su dominio y el dominio del nodo receptor.

Los flujos son clasificados por normas predeterminadas de modo que puedan encajar dentro de un grupo limitado de clases de flujo. Los enrutadores de borde usan el campo ToS de ocho bits de la cabecera del paquete, llamada campo DS, para marcar al paquete para un trato preferencial por los enrutadores interiores. Solo los enrutadores de borde necesitan mantener estados por flujo y ejecutar las políticas y formaciones. Esto es ventajoso ya que por lo general los enlaces entre el cliente y el proveedor de servicio son lentos, además el retardo computacional no constituye un gran problema para las interfaces del enrutador en estos enlaces. Por tanto, esto es asequible para realizar las estrategias de políticas y modelación de tráfico intensivo en los enrutadores de borde. Pero una vez dentro del núcleo de los proveedores de servicio, los paquetes necesitan ser enrutados o transmitidos rápidamente por lo que esto debe incurrir a un retardo computacional mínimo en cualquier enrutador o conmutador. Desde que el número de flujos en los enrutadores de borde es muy pequeño que en la red núcleo, esto también es una ventaja para hacer control de flujo en los enrutadores de borde.

Condicionamiento y clasificación de tráfico límite de red.

Los acondicionadores de tráfico realizan varias funciones de QoS y se encuentran ubicados en los bordes de red. Los enrutadores de borde clasifican o marcan el tráfico por la configuración del campo DSCP y monitorean le tráfico de entrada de la red por cumplimiento de perfil. El campo DSCP indica que tratamiento el paquete debería recibir en un dominio DS. Las funciones QoS pueden ser clasificación de paquetes, marcación DSCP o funciones de medición de tráfico. La figura. 1.8., muestra la estructura lógica de la clasificación de tráfico y las funciones de condicionamiento.

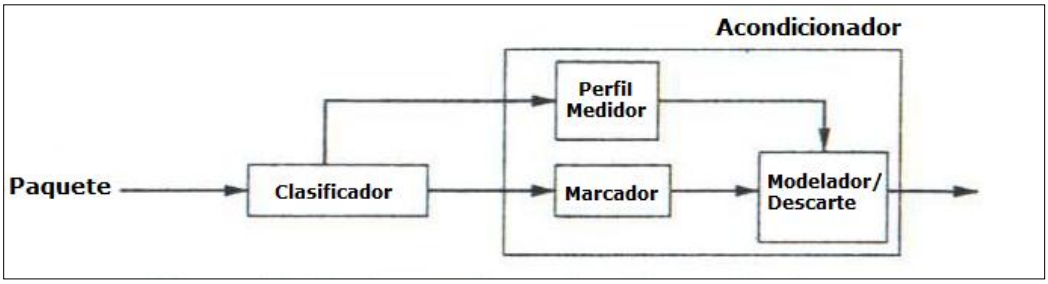


Figura. 1.8. Clasificador de paquete y acondicionador de tráfico[13]

La clasificación de paquetes puede ser hecha en una de las dos formas, dependiendo de la conectividad del enrutador de borde. Algunos enrutadores de borde son conectados a la red de clientes y otros son conectados a otros proveedores de servicios.

Un enrutador de borde que es conectado a una red de cliente usa seis campos en un paquete IP de entrada para determinar el PHB que el paquete debería recibir en la red núcleo. Estos seis campos son la dirección IP origen, la dirección IP destino, el protocolo ID, el campo en la cabecera del paquete de entrada, el puerto origen y el puerto destino en la cabecera de transporte respectivamente. Una norma que mapea un paquete a un PHB no necesita especificar los seis campos. Estas normas se refieren a las de clasificación. Cuando una norma de clasificación no especifica cualquier valor específico para un campo, este campo específico no es usado para el propósito de clasificación.

Los enrutadores de borde podrían usar solo un campo en el paquete IP de entrada para determinar el PHB para su red. Este campo podría ser el campo DS contenido en el paquete de entrada. Un enrutador de borde simplemente cambiaría el campo DS a cualquier otro valor correspondiente a un específico PHB en los enrutadores de núcleo.

[13] Chao, Jonathan; Liu, Bin, *High Performance Switches and Routers*, Editorial Wiley-Interscience a John Wiley&Sons INC Publication, United States of America 2007, página 125

Este tipo de clasificación sería esperada en los puntos de intercambio de otros proveedores de servicios. El dominio del proveedor de servicios vecino pudo haber estado usando un grupo diferente de PHBs o puede usar diferentes valores de campo DS para representar el mismo PHB. El enrutador de borde puede limitar el número total de paquetes que pueden ser enviados dentro de cada clase. Si se comprueba que un paquete no puede ser mapeado dentro de cualquier PHB porque un límite sería excedido, este puede ser mapeado dentro de un diferente PHB o puede ser descartado.

Los medidores verifican la conformidad de flujos de tráfico a ciertos parámetros y pasan los resultados al marcador y al modelador/descarte. Los medidores miden las propiedades temporales del flujo de paquetes seleccionado por un clasificador contra un perfil de tráfico especificado en un TCA. Un medidor pasa información de estado a otras funciones condicionales para activar una acción particular para cada paquete que sea dentro de perfil o fuera de perfil.

El marcador es responsable de la escritura y sobrescritura de los valores DSCP. Puede marcar paquetes basados en el clasificador de emparejamiento o basados en resultados de los medidores. Los medidores de paquetes establecen el campo DS de un paquete a un punto de código particular, agregando el paquete marcado a un conjunto particular de comportamiento DS. El marcador puede ser configurado para señalar todos los paquetes que se dirigen a él, a un punto de código simple, o puede ser configurado para señalar un paquete a uno de un grupo de puntos de código usados para seleccionar un PHB en un grupo de ellos, de acuerdo al estado de un medidor. Cuando el marcador cambia el punto de código en un paquete, se dice que el paquete fue remarcado.

El modelador/descartar es responsable de dar forma al tráfico para ser compatible con el perfil y también puede descartar paquetes cuando exista congestión. Los modeladores retardan algunos o todos los paquetes en un flujo de tráfico a fin de que el flujo cumpla con un perfil de tráfico. Un modelador usualmente tiene un ***buffer***[14] de tamaño finito, y los paquetes pueden ser descartados si no existe suficiente espacio en el *buffer* para mantener los paquetes retardados. En este módulo se descartan algunos o todos los paquetes en un flujo de tráfico a fin de que el flujo cumpla con un perfil de tráfico. Este proceso es conocido como políticas de flujo. Nótese que un descarte puede ser

[14] ***Buffer***. Dispositivo de memoria que se utiliza para almacenar temporalmente información o datos

implementado como un caso especial de un modelador mediante la configuración del tamaño de *buffer* del modelador a cero o a unos pocos paquetes.

Comportamiento por salto.

De acuerdo a la RFC 2475, el comportamiento por salto PHB es el medio por el cual un nodo localiza recursos a un conjunto de flujos. Un ejemplo es que un PHB define un porcentaje de la capacidad de un enlace. Los enrutadores interiores en el modelo DS solo necesitan enviar paquetes de acuerdo al PHB especificado. Si solo un comportamiento agregado ocupa el enlace, el comportamiento de envío observable generalmente solo dependerá de la congestión del enlace. Distintos patrones de comportamiento solo son observados cuando múltiples agregados de comportamiento compiten por el *buffer* o los recursos de ancho de banda en un nodo como muestra la figura. 1.9.

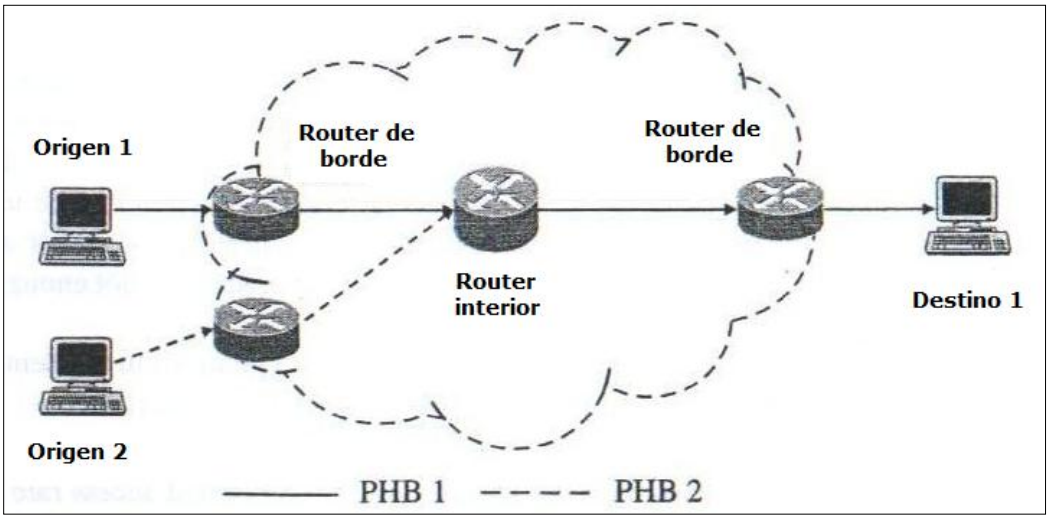


Figura. 1.9. Comportamiento por salto en DS[15]

Existen dos flujos: origen1 – destino1 y origen2 – destino1. Estos flujos tienen diferentes clasificaciones y serán tratados diferentemente por el enrutador interior, por ejemplo, usando diferente planificación y/o preferencia de descarte. Un nodo de red asigna recursos a los comportamientos agregados con la ayuda de los PHBs. Los PHBs pueden ser definidos en términos de sus recursos (*buffer* y ancho de banda), en términos de su relativa prioridad con otros PHBs o en términos de sus relativas propiedades de tráfico (retardo y pérdida). Múltiples PHBs se agrupan juntos para formar un grupo PHB para asegurar consistencia. PHBs son implementados en nodos a través de algunas gestiones de *buffer* o

[15] Chao, Jonathan; Liu, Bin, *High Performance Switches and Routers*, Editorial Wiley-Interscience a John Wiley&Sons INC Publication, United States of America 2007, página 126

mecanismos de planificación de paquete. Un grupo particular PHB puede ser implementado en una variedad de formas porque PHBs son definidos en términos de características de comportamiento y no son implementaciones dependientes.

El estándar para *DiffServ* describe PHBs como la construcción de bloques de servicio. El centro está sobre la aplicación de un SLA entre el usuario y el proveedor de servicios. Los clientes pueden marcar el octeto DS de sus paquetes para indicar el servicio deseado, o tenerlos marcados por el enrutador límite basado en clasificación multicampo, tal como dirección IP destino y origen, número de puertos de transporte, ID de protocolo, y otros. Dentro del núcleo, los paquetes son enviados de acuerdo a sus comportamientos agregados. Estas normas son derivadas del SLA. Cuando un paquete va de un dominio a otro, el octeto DS puede ser reescrito por los nuevos enrutadores de borde de red. Un PHB para un paquete es seleccionado en un nodo en base a su punto de código DS.

Los PHBs más usados son: comportamiento por defecto, selector de clase, transmisión segura AF y transmisión acelerada EF. El mapeo desde los puntos de código hacia el PHB puede ser 1 a 1 o N a 1. Todos los puntos de código deben tener algunos PHBs asociados con ellos. Por otra parte, los puntos de código son mapeados a un PHB por defecto.

Campos del servicio diferenciado.

Los valores DS son conocidos como punto de código de servicio diferenciado DSCP. La tabla. 1.1., muestra los formatos de octeto del ToS y DSCP.

Tabla. 1.1. Octeto ToS de IPv4 y octeto DS

<table>
<tr><td>OCTETO ToS</td><td>P2</td><td>P1</td><td>P0</td><td>T3</td><td>T2</td><td>T1</td><td>T0</td><td>Cero</td></tr>
<tr><td rowspan="2">OCTETO DS</td><td>DS5</td><td>DS4</td><td>DS3</td><td>DS2</td><td>DS1</td><td>DS0</td><td>ECN1</td><td>ECN0</td></tr>
<tr><td colspan="3">Selector de clase</td><td colspan="3">Precedencia de descarte</td><td></td><td></td></tr>
</table>

En IPv4, solo los tres primeros bits son usados para propósito de QoS. En *DiffServ*, seis bits son usados. El mismo octeto ahora es referido como el campo DS. El campo DS se divide en tres bits de selector de clase y tres bits de precedencia de dispersar. Un cuadro más completo entre el octeto ToS y el octeto DS es presentado en el Anexo A1.

Comportamiento por defecto.

El PHB por defecto o de mejor esfuerzo corresponde al paquete de mejor esfuerzo por defecto enviado en la red IP tradicional. Los paquetes pertenecientes a este PHB podrían ser transmitidos en cualquier manera sin ninguna restricción. El punto de código recomendado por la IETF para el PHB de mejor esfuerzo es 0x000000.

Selector de clase.

Los tres bits más a la izquierda del campo DS o del ToS IP definen ocho clases. Un paquete con un valor numérico más alto en el campo selector de clase es definido para tener una mejor o igual prioridad en la red para la transmisión que un paquete con un valor numérico más bajo. Un enrutador no necesita implementar ocho diferentes niveles de prioridad en la red para soportar el selector de clase PHBs. Puede reclamar el cumplimiento con los estándares mediante el apoyo de solo dos niveles de prioridad, con los ocho valores numéricos mapeados a una de las dos clases.

Transmisión asegurada.

El PHB transmisión asegurada AF (*Assured Forwarding*) es usado para proveer servicios asegurados al cliente, de modo que el cliente recibirá servicios fiables incluso en tiempos de congestión de red. Las clases 1 a 4 son conocidas como los niveles de servicio AF. Porque toman una decisión basada solo en el selector de clase que es muy tosca, el PHB AF fue creado para proveer más granularidades en la gestión del *buffer*. Esta clase hace uso de los bits de precedencia de descarte, DS2 a DS0 como se muestra en tabla. 1.1.

Cuando los paquetes atrasados de una clase AF transmitida excede un específico umbral, los paquetes con la prioridad más alta para descartar son descartados primero y luego los paquetes con la más baja prioridad para descartar. Las prioridades para descartar en AF son específicas para la clase de transmisión; comparando dos prioridades de descarte en dos diferentes clases AF no siempre pueden ser significativas. Por ejemplo, cuando un nodo DS empieza a descartar los paquetes con la más alta prioridad en una clase de transmisión, los paquetes en otras clases de transmisión no pueden experimentar ningún paquete descartado. Cada clase de transmisión tiene su ancho de banda asignado. Descartar paquetes solo toma lugar en la clase de transmisión en la cual el tráfico excede sus propios recursos.

En general, un nodo DS puede reordenar paquetes de diferentes clases AF pero no debería reordenar paquetes con diferentes prioridades de descarte en la misma clase. Los nodos de borde deberían evitar división de tráfico de la misma solicitud de flujo en diferentes clases ya que daría lugar a paquetes reordenados con un micro flujo en la red.

Transmisión acelerada.

La clase 5 es conocida como transmisión acelerada EF (*Expedited Forwarding*). El PHB EF es usado para proveer servicios *premium* a los clientes. Tiene un retardo bajo, bajo *jitter* en el servicio junto a una tasa de bit constante CBR (*Constant Bit Rate*) para el cliente. El SLA especifica la tasa de bit pico en la cual las aplicaciones de los clientes serán recibidas y el no exceder esta tasa es una responsabilidad del cliente.

El PHB EF es implementado en una variedad de formas. Por ejemplo, si una prioridad de encolamiento es usada, entonces debe haber un límite superior, configurada por el administrador de red, en la tasa de tráfico de EF que debería ser permitido. El tráfico de EF que excede el límite es descartado.

1.8.4. Servicio integrado y diferenciado en combinación

Una posible mejora de los proveedores de servicios por arquitecturas *DiffServ* es representada por una combinación de enfoque *IntServ/DiffServ*.

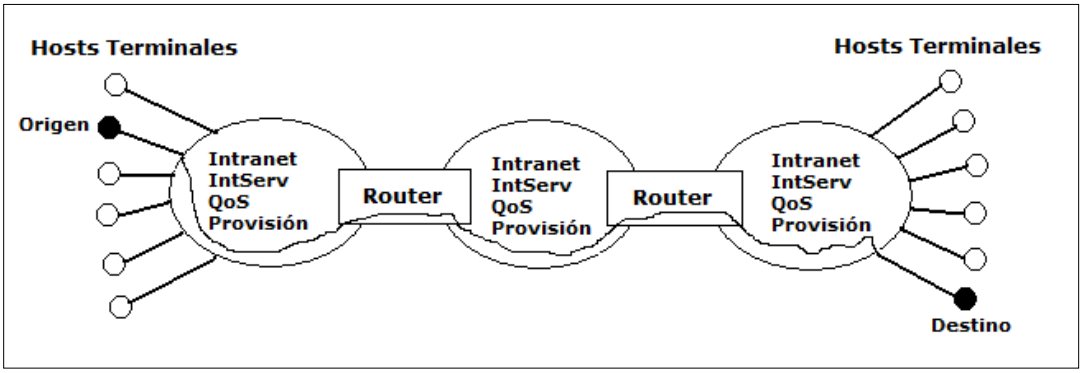


Figura. 1.10. Arquitectura *IntServ/DiffServ*[16]

La figura. 1.10., muestra un ejemplo de esto: se tiene un origen y un destino del servicio marcados en los círculos de los extremos; las líneas en negrilla junto con la línea trazada muestran el camino del flujo de datos a través de la red; dos enrutadores separan el

[16] Marchese, Mario, *QoS over Heterogeneous Networks*, Editorial John Wiley&Sons LTD, England 2007, página 34

dominio *DiffServ* del resto de la red. Dentro del dominio *DiffServ*, el tráfico es agregado en clases, mientras dentro del dominio *IntServ* cada cliente puede ser identificado y tratado separadamente.

La arquitectura mostrada en la figura. 1.10., pasa en la hipótesis de que dentro de las pequeñas redes privadas donde la disponibilidad del ancho de banda es reducida, cada cliente necesita ser identificado y merece un tratamiento especial, mientras que el *backbone* de una red tiene disponibilidad completa de ancho de banda y la diferenciación del tráfico a través de pocas clases de tráfico es suficiente para garantizar el SLA requerido.

Actualmente, el enfoque de *IntServ* puede ser reservado a pequeñas Intranets privadas donde no hay problemas de escalabilidad y el enfoque de *DiffServ* puede ser usado a la interconexión de *backbones*. La indicación percibida de conferencias y revistas internacionales es que la comunidad de Internet por si misma recomienda *IntServ* para pequeñas redes privadas y para el acceso de segmento. No obstante, esto significa que QoS no cuantitativo puede ser proveído sobre el *backbone* para cada cliente, también en caso de necesitarlo. Esto es aceptable teniendo el servicio de Internet de mejor esfuerzo en mente y la prestación de servicios cualitativos, pero esto puede ser difícilmente aplicado a redes de ofrecimiento cuantitativo basado en el SLA de servicios garantizados de QoS en ambientes peligrosos. Esto es verdad, en particular, si el ambiente de aplicación incluye enlaces de baja velocidad y no tiene gran disponibilidad de ancho de banda, como a menudo ocurren con muchas aplicaciones: redes satelitales o de radio, redes ad hoc y redes de sensores. Las redes mencionadas a menudo transportan servicios que requieren un muy estricto SLA: monitoreo del ambiente, aplicaciones militares y servicios de salud.

Una comparación entre *IntServ* y *DiffServ* es mostrada en la tabla. 1.2. Ventajas e inconvenientes de soluciones IP QoS son resumidas en la tabla. 1.3.

Tabla. 1.2. *IntServ* versus *DiffServ*

CARACTERÍSTICAS	*IntServ*	*DiffServ*
Garantía QoS	Por flujo	Por agregado
Rango de garantía QoS	Extremo a extremo (aplicación a aplicación)	Dominio *DiffServ* (borde a borde)
Reserva de recurso	Controlado por aplicación	Configurado en los nodos de borde basados en el SLA
Administración de recursos	Distribuido	Centralizado dentro del dominio *DiffServ*
Señalización	Protocolo dedicado RSVP	Basado en DSCP
Escalabilidad	Limitado por el número de flujos	Limitado por el número de clases
Servicios QoS	GS, CLS, mejor esfuerzo	EF, AF, mejor esfuerzo
Complejidad	Alta	Baja
Disponibilidad	Sí	Sí

Tabla. 1.3. Soluciones IP QoS, puntos de fuerza e inconvenientes

PUNTOS DE FUERZA	INCONVENIENTES
Difusión. IP es extensa: usuarios terminales, LANs, accesos de red, *backbones*, debido al desarrollo de Internet	**QoS.** *IntServ* (RSVP) y *DiffServ* pueden manejar QoS dentro del mundo IP pero cada uno tiene limitaciones referidas a los requerimientos de rendimiento de usuario
Integración simple WEB. Las interfaces WEB son muy usadas, sobre el Internet y sobre redes privadas	***IntServ*.** Es considerado también complejo y no escalable para ser usado dentro de backbones y redes multi usuarios. RSVP usa un mecanismo de refrescamiento que introduce ineficientes recursos de gestión
Compresión de cabecera. Esto es muy importante para reducir la transmisión superpuesta (en particular la pila RTP/UDP/IP para la voz)	***DiffServ*.** Es escalable pero difícilmente puede proporcionar soluciones extremo a extremo para ambientes de calidad alta esto a causa de limitado número de bits para identificar el flujo

1.9. CALIDAD DE SERVICIO Y FACTORES HUMANOS

Los factores humanos proporcionan el mejor sistema para obtener los objetivos de QoS describiendo los límites y coacciones del usuario final. Más factores humanos tales como los límites sensoriales o sistemas cognitivos son bien entendidos y son incambiables, a diferencia de la tecnología. Proporcionan un objetivo sólido contra el que un servicio puede ser determinado para satisfacer, decepcionar o superar las necesidades de los usuarios finales. Como estos límites aplican en todas las demografías de usuarios es bien entendido y su relativa invariancia hace ideal como un punto de partida. Proveen un escudo contra el argumento de que los objetivos de QoS siempre serán reforzados porque los usuarios siempre quieren lo mejor y más rápido. Por ejemplo, en la industria de la película el número de tramas por segundo (24 a 30) ha sido escogida para tener ventaja de parpadeo

de fusión. Una tasa de menos tramas por segundo impide a los usuarios la percepción de suave movimiento. Muchas más tramas por segundo son desperdiciadas porque la gente no puede percibir alguna diferencia. Este estándar ha sido ubicado durante casi un siglo, independientemente de las particularidades de la tecnología de película, porque es basado en los factores humanos fundamentales.

1.10. TIPOS DE SERVICIO COMO FUNCIÓN DE CALIDAD DE SERVICIO

Surgen cuatro categorías de servicio en términos de retardo, cuando se considera al QoS desde un punto de vista de factores humanos. Con el fin de no perder de vista que factores humanos corresponden a cada categoría, y por lo tanto su justificación, son nombrados usando términos que corresponden al sistema humano al cual se refieren:

- Perceptivo. Basado en los límites perceptivos de los sistemas sensoriales humanos, como auditivo o visual. Estos límites son los menores en términos de retardo, típicamente dentro de 200 milisegundos

- Cognitivo. Basado en límites como memoria a corto plazo y lapso de atención natural, el cual tiene un rango de 0.25 a 3 segundos

- Social. Basado en expectativas sociales del tiempo de respuesta razonable cuando una pregunta o solicitud es planteada. El entendimiento de usuario de cuan complicado fue la solicitud puede mitigar estos límites. Típicamente estos son retardos sobre los 10 segundos

- Postal. Basado en expectativas de entrega a otra persona de cosas como correo o fax. El rango esperado es de 10 segundos hasta algunos minutos y, en algunos casos, horas. Al contrario de la categoría social la respuesta por este tipo de servicio es generalmente percibido por una persona distinta del remitente, lo cual es una de las razones para las necesidades de ritmo relajado

En términos humanos, la reproducción del material origen debe ser también precisa o puede ser perdonado. Usualmente preciso corresponde al origen digital. Perdonado usualmente corresponde al origen análogo.

Las categorías perceptiva y cognitiva son basadas en la neurología y son por tanto validas en todas las demografías. Las categorías social y postal pueden ser sujetas a

variación cultural y experiencia relatada. Afortunadamente para los diseñadores de servicio y red, las categorías más estrictas son las más invariantes. Esto evita el problema de tener los objetivos más difíciles cambiando con el tiempo.

CAPÍTULO 2

MARCADO Y CLASIFICACIÓN DE PAQUETES

2.1. INTRODUCCIÓN

Para proporcionar prioridad a ciertos flujos, primeramente el flujo debe ser identificado y, si se desea, marcado. Simplemente estas dos tareas son referidas como clasificación. La clasificación implica el uso de descriptores de tráfico para categorizar un paquete dentro de un grupo específico con lo que se determina qué paquete y qué lo hace accesible a la manipulación de QoS en la red. Usando la clasificación de paquete, se puede dividir el tráfico de red en múltiples niveles de prioridad o clases de servicio. Cuando los descriptores de tráfico son usados para clasificar tráfico, el origen acuerda adherir a los términos contratados y la red promete calidad de servicios.

La clasificación de paquetes es fundamental para técnicas de política que seleccionan paquetes atravesando un elemento de red o una interfaz particular para diferentes tipos de QoS. Por ejemplo, se puede usar la clasificación para marcar ciertos paquetes por precedencia IP y se puede identificar otros como pertenecientes a flujos RSVP.

Los métodos de clasificación alguna vez estuvieron limitados para usar los contenidos de la cabecera del paquete. Los métodos actuales de marcación de paquete con su clasificación permiten colocar información en las cabeceras de capa 2, 3 o 4, o incluso el establecimiento de información dentro de la carga útil de un paquete.

A continuación se describen algunos métodos importantes para la marcación y la clasificación de paquetes dentro de la calidad de servicio.

2.2. PRECEDENCIA IP

La precedencia IP utiliza los tres bits precedentes en el campo ToS de la cabecera IPv4 para especificar la clase de servicio para cada paquete, como se muestra en la figura. 2.1.

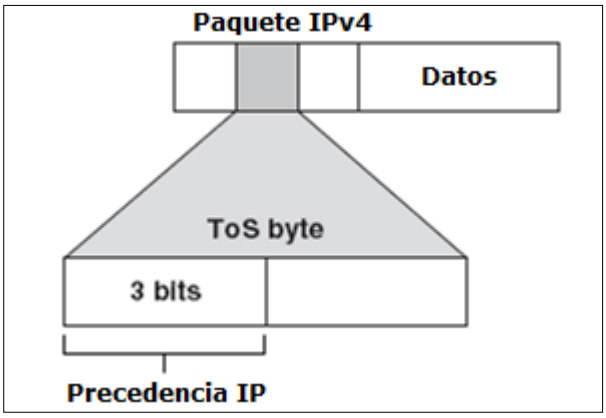


Figura. 2.1. Precedencia IP del campo ToS en la cabecera IPv4[17]

Se puede dividir tráfico en no más de seis clases de servicio usando la precedencia IP (los otros dos son reservados para uso interno de la red). Entonces, las tecnologías de encolamiento a lo largo de la red pueden usar esta señalización para proporcionar la apropiada manipulación acelerada.

Los tres bits más significativos del campo ToS en la cabecera IP constituyen los bits usados para la precedencia IP. Estos bits son usados para proporcionar una prioridad de 0 a 7 (los ajustes de 6 o 7 son reservados y no son configurados por un administrador de red) para el paquete IP.

Debido a q solo tres bits del byte ToS son usados para la precedencia IP, se necesita diferenciar estos bits del resto dentro del byte ToS. En la figura. 2.2., un 1 en la primera y tercera posición de bit, visto de izquierda a derecha, se correlaciona a una precedencia IP fijada de 5, pero cuando el byte ToS es visto por medio de una traza de ***sniffer***[18], se lo muestra como 160. Por lo tanto se necesita ser capaz de traducir este valor, y una pequeña explicación se muestra en la figura. 2.2.

[17] Internetworking Technology Handbook - Quality of Service (QoS) - Cisco Systems, http://www.cisco.com/en /US/docs/internetworking/technology/handbook/QoS.html #wp1020698, Publicación 2007, Consultado en Agosto 2009
[18] ***Sniffer***. Es un programa de captura de las tramas de red para diferentes análisis

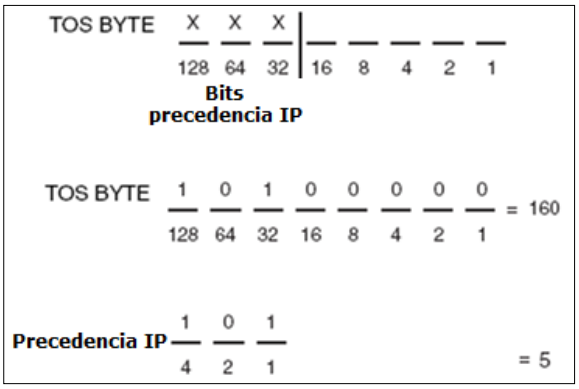


Figura. 2.2. Precedencia IP[19]

El tráfico que es identificado puede ser marcado por la colocación de los bits de precedencia IP. En consecuencia, el tráfico necesita ser clasificado solamente una vez. RFC 2475 extiende el número de bits usados en el byte ToS de 3 a 6. Los seis bits más significativos serán usados para la colocación de la precedencia (conocida como puntos de código DS), con los 2 bits menos significativos (los dos bits más a la derecha) reservados para un uso futuro. Esta especificación es comúnmente referida al *DiffServ*.

2.2.1. Clasificación de paquetes usando precedencia IP

Como se mencionó anteriormente, se usan tres bits de precedencia IP en el campo ToS de la cabecera IP para especificar la clase de servicio asignada para cada paquete, adicional a esto, se debe usar políticas de red con el objetivo de definir términos de manipulación de congestión y asignación de ancho de banda para cada clase.

Por razones históricas cada precedencia tiene un nombre. La tabla. 2.1., presenta los valores y sus correspondientes nombres, desde el menos al más importante.

Tabla. 2.1. Valores de precedencia IP

VALOR	NOMBRE
0	Rutina
1	Prioridad
2	Inmediato
3	Urgente
4	muy urgente
5	Crítico
6	Internet
7	Red

[19] Internetworking Technology Handbook - Quality of Service (QoS) - Cisco Systems, http://www.cisco.com/en/US/docs/internetworking/technology/handbook/QoS.html #wp1020698, Publicación 2007, Consultado en Agosto 2009

Sin embargo, la característica de la precedencia IP permite una considerable flexibilidad para la asignación de precedencias. Esto es, se puede definir un mecanismo propio de clasificación. Por ejemplo, se puede querer asignar precedencia basada en la aplicación o en el acceso de enrutador. La asignación del bit de precedencia IP 6 y 7 son reservados para el control de información de red tal como las actualizaciones de enrutamiento.

2.2.2. Valores de la precedencia IP

Por defecto, generalmente en los equipos usados para la gestión de QoS el valor de precedencia IP no se lo toca, es decir se preserva el valor de precedencia colocado en la cabecera, permitiendo de esta manera a todos los dispositivos internos de la red proporcionar servicios basados en la precedencia IP disponible. Esta política sigue la propuesta de estándar estipulada al tráfico de red que debería ser ordenada dentro de varios tipos de servicio en el perímetro básico de la red y que estos tipos de servicio deberían ser implementados en el núcleo de la red. Enrutadores en el núcleo de la red pueden entonces usar los bits de precedencia, por ejemplo, para determinar el orden de transmisión, la probabilidad de descartar el paquete y más.

Porque el tráfico entrante en la red puede tener precedencia establecida por dispositivos exteriores, se recomienda reajustar la precedencia para todo tráfico entrante de la red. Por control de la precedencia IP establecida, se prohíbe a usuarios que ya tienen configurada la precedencia IP desde un mejor servicio adquirido simplemente por su tráfico mediante el establecimiento de una alta prioridad para todos sus paquetes.

2.3. TASA DE ACCESO COMPROMETIDA

La tasa de acceso comprometida CAR (*Committed Access Rate*) es uno de los métodos usados ampliamente para el marcado de paquetes en la red de borde en los puntos de entrada y salida. CAR puede operar, en términos generales, en una de las dos funciones: limitación de tasa y clasificación de paquete a través de precedencia IP y configuración de grupo QoS.

Con el mecanismo de limitación de tasa de CAR, se puede controlar la tasa base del tráfico recibido o transmitido en una interface. Típicamente, la clasificación y el marcado

ocurren en la entrada, en cambio, la limitación de tasa ocurre en la salida. CAR define de tres formas al tráfico para la limitación de tasa: tasa promedio, ráfaga normal y tamaño de ráfaga excedida.

En lo concerniente a las ráfagas, es importante notar que CAR no modela ni arregla el tráfico. No tiene capacidades de *buffer* de ráfaga. Porque de esto, CAR añada retardo entre paquetes; sin embargo, esto también significa que los grandes beneficios de CAR ocurren en enlaces de alta velocidad, en velocidades ***DS3***[20] o mayores. Enlaces de baja velocidad que deben contar con una cantidad significante de *buffer* para negociar con tráfico de ráfaga no verían los beneficios de CAR como lo harían los enlaces de velocidades altas.

La característica de la limitación de tasa de CAR trabaja en el principio de un *token bucket*. El fondo del *bucket* es indicativo del tamaño de ráfaga que es configurado para el enlace. Las capacidades de la tasa de tráfico pueden ser configuradas en segmentos de 8k sobre la capacidad física del enlace. Si un paquete llega y existen suficientes *tokens* dentro del *bucket*, el paquete es autorizado para pasar. Sin embargo, si hay carencia de *tokens*, el paquete es permitido pedir prestado *tokens* sobre el tamaño de ráfaga excedido. Este fondo de exceso de paquete es un préstamo contra el tráfico futuro y debe ser reconstruido de los períodos de tráfico bajo. La idea es permitir para una reducción gradual en el tráfico de paquete utilizar un procedimiento adecuado en lugar de descartar los paquetes hacia la cola en el dispositivo de red. Si el tamaño acumulativo excede el límite de tamaño de ráfaga, los paquetes serán descartados. Cuando el tráfico ha sido clasificado como perteneciente a una tasa específica, una de varias acciones mostradas a continuación ocurrirá, dependiendo en como el administrador de red ha configurado la respuesta.

- Se transmite el paquete
- Se descarta el paquete
- Se coloca la precedencia y se transmite. El paquete puede tener una muy baja precedencia establecida y puede ser transmitido con un bajo QoS

[20] ***DS3***. Circuito digital con características de operación estandarizada y capacidad de transmisión igual a 28 DS1o 45.304 Mbps

- Si además existen declaraciones de CAR, el paquete continuará para ser procesado. En el fin de la cadena, el paquete será transmitido

Es importante notar que, para los procedimientos de limitación de tasa, solo los paquetes que están en el modo ráfaga son sometidos a cambios en la precedencia o QoS. Los paquetes que están dentro de la tasa promedio no son modificados y se transmiten como especifican sus parámetros de QoS.

En relación al QoS, las capacidades de marcación de CAR son de principal importancia. CAR tiene la habilidad de marcar paquetes mediante la configuración de los bits de precedencia IP. Mientras existen ocho diferentes posibles niveles de precedencia IP, es estrictamente recomendado que el administrador de red solo use los primeros seis niveles. Los dos niveles más altos son reservados para control de red crítico y protocolos de enrutamiento que deben pasar de dispositivo en dispositivo para asegurar la funcionalidad propia de la red.

CAR puede marcar tráfico basado en el puerto físico, dirección IP origen y destino, dirección MAC, tipo de protocolo IP o cualquier otra diferenciación que puede ser especificada por una lista. La clave es que CAR solo funcionará sobre tráfico IP. El tráfico que no es IP es conmutado normalmente y no es afectado por las características de limitación de tasa y marcado de CAR.

2.4. ENCAMINAMIENTO BASADO EN POLÍTICAS

El encaminamiento basado en políticas PBR (*Policy – Based Routing*) proporciona un medio flexible de enrutamiento de paquetes permitiendo configurar una política definida para flujos de tráfico, disminuyendo la dependencia en enrutadores derivados de protocolos de enrutamiento. Con este fin, PBR da más control sobre el encaminamiento mediante la ampliación y complementación de mecanismos existentes proporcionados por los protocolos de enrutamiento. PBR permite configurar la precedencia IP. También permite especificar un camino para cierto tráfico, tal como tráfico prioritario sobre un enlace de alto costo.

Se puede configurar PBR como una forma para enrutar paquetes basados en políticas configuradas. Por ejemplo, se implementa políticas de enrutamiento para permitir o

denegar caminos basados en la identidad de un sistema final en particular, un protocolo de aplicación o el tamaño de paquetes.

PBR permite realizar las siguientes tareas:

- Clasificar tráfico basado en el criterio de ***listas de acceso***[21]. Después ellas establecen el criterio de emparejamiento

- Configurar los bits de precedencia IP, proporcionando a la red la habilidad para habilitar clases de servicio diferenciado

- Enrutar paquetes a caminos específicos de tráfico diseñado; se podría necesitar enrutar los paquetes para permitir un específico QoS a través de la red

Las políticas pueden ser basadas en direcciones IP, número de puertos, protocolos o tamaño de paquetes. Para una política simple, se puede usar cualquiera de estos descriptores; para una política complicada, se pueden usar todos.

Por ejemplo, la clasificación de tráfico a través de PBR permite identificar tráfico para diferentes clases de servicio en el borde de la red y luego implementar QoS definido por cada clase de servicio en el núcleo de la red usando alguna técnica de encolamiento. Este proceso obvia la necesidad de clasificar tráfico explícitamente en cada interface WAN en la red núcleo de *backbone*.

En cuanto al funcionamiento de PBR, todos los paquetes recibidos en una interfaz con PBR habilitado son pasados a través de filtros de paquetes mejorados conocidos como mapas de rutas. Los mapas de rutas usados por PBR dictaminan la política, determinando a dónde los paquetes son transmitidos. Los mapas de ruta son compuestos de sentencias. Las sentencias del mapa de ruta pueden ser marcadas como permitidas o denegadas, y pueden ser interpretadas en las siguientes formas:

- Si los paquetes no coinciden con alguna sentencia del mapa de ruta, todas las cláusulas configuradas son aplicadas

[21] ***Listas de Acceso ACL***. Son herramientas utilizadas para el filtrado de paquetes en función de ciertos parámetros como direcciones IP de origen y destino, puertos de origen y destino, tipo de protocolo, entre otros

- Si una sentencia es marcada como denegada, los paquetes agrupados en el criterio de concordancia son enviados a través de los canales de transmisión normal y el enrutamiento basado en destino es ejecutado

- Si la sentencia es marcada como permitida y los paquetes no se agrupan en alguna sentencia del mapa de ruta, los paquetes son enviados a través de los canales de transmisión normal y el enrutamiento basado en destino es ejecutado

Es importante señalar que se especifica PBR en la interfaz que recibe el paquete, más no en la interfaz en la que el paquete es enviado. Se podría habilitar PBR si se desea a ciertos paquetes enrutados de alguna otra manera que el obvio camino más corto. Por ejemplo, PBR puede ser usado para proveer las siguientes funcionalidades:

- Acceso equitativo

- Enrutamiento de protocolo susceptible

- Enrutamiento de origen susceptible

- Enrutamiento basado en tráfico interactivo versus tráfico de grupo

- Enrutamiento basado en enlaces dedicados

Algunas aplicaciones o tráfico pueden beneficiarse del enrutamiento específico QoS; por ejemplo, se puede transferir los registros existentes a una oficina corporativa en un mayor ancho de banda, en un mayor costo de enlace por un corto tiempo mientras se envía la aplicación de datos rutinaria como el correo electrónico sobre un menor ancho de banda, un menor costo de enlace.

2.5. MARCACIÓN DE PAQUETES BASADO EN CLASES

La característica de la marcación de paquetes basado en clases provee medios para una eficiente marcación de paquetes mediante los cuales, los usuarios pueden diferenciar paquetes basados en las marcaciones designadas. Permite a los usuarios realizar las siguientes tareas:

- Marcar paquetes por configuración de los bits de la precedencia IP o DSCP en el byte IP ToS

- Marcar paquetes por configuración del valor clase de servicio CoS (*Class of Service*) de capa 2

- Asociar un valor de grupo QoS local con un paquete

2.5.1. Marcación de precedencia IP y DSCP IP

Asociar un paquete con una precedencia IP o con una marcación DSCP IP permite a los usuarios clasificar tráfico basado en estos valores, dependiendo de qué valor esté marcado. Estas marcaciones pueden ser utilizadas para identificar tráfico dentro de la red, y otras interfaces pueden emparejar tráfico basado en la precedencia IP o en las marcaciones DSCP.

La precedencia IP y las marcaciones DSCP son usadas para decidir como los paquetes deberían ser tratados en WRED (será tratado adelante). Haciendo referencia al WRED se dice que, la detección aleatoria temprana RED (analizada posteriormente) es un mecanismo para evitar la congestión del tráfico de red que aprovecha el mecanismo de control TCP. Al descartar los paquetes aleatoriamente durante los períodos de congestión alta, RED reconoce el paquete origen para disminuir su tasa de transmisión. Asumiendo que el paquete origen está usando TCP, este disminuirá su tasa de transmisión hasta que todos los paquetes alcancen su destino, indicando que la congestión es borrada. Ahora, generalmente RED ponderado (WRED) dispersa selectivamente paquetes basados en la precedencia IP o DSCP. Los paquetes con la más alta precedencia IP son menos probables que se descarten como los paquetes con la más baja precedencia. En consecuencia, la prioridad de tráfico más alta es entregada con una muy alta probabilidad que la prioridad de tráfico más baja. Sin embargo, también se puede configurar WRED para ignorar la precedencia IP cuando se ejecutan las decisiones de descarte de modo que el comportamiento no-ponderado RED es logrado. WRED es útil en cualquier interfaz de salida donde se espera tener congestión. Sin embargo, WRED es usualmente utilizado en los enrutadores de núcleo en una red, en lugar de los de borde. Los enrutadores de borde asignan precedencias IP a los paquetes de acuerdo a como entran a la red. WRED usa estas precedencias para determinar cómo tratar diferente tipo de tráfico.

El valor del DSCP IP está en los primeros 6 bits del byte ToS, mientras que el valor de la precedencia IP está en los primeros 3 bits. Actualmente, el valor de precedencia IP es parte del valor DSCP IP. Por lo tanto, ambos valores no pueden ser configurados simultáneamente. Si esto sucede, el paquete es marcado con el valor DSCP IP.

Si se necesita marcar paquetes en la red y todos los dispositivos soportan la marcación DSCP, es recomendable usarla para la marcación de paquetes, ya que esta característica proporciona más opciones de marcación. No obstante, si la marcación por DSCP IP no es deseable, o si no se tiene la seguridad de que todos los dispositivos en la red soporten estos valores de marcación, se debe usar la precedencia IP para la marcación de paquetes. Es probable que el valor de la precedencia IP sea soportado por todos los dispositivos en la red. Se puede tener 8 diferentes marcaciones de precedencia IP y 64 marcaciones de DSCP IP.

2.5.2. Marcación del valor clase de servicio CoS

Tratar a un paquete con un valor local de clase de servicio CoS permite a los usuarios asociar un valor de CoS de capa 2 con un paquete. Entonces el valor puede ser usado para clasificar paquetes basados en requerimientos definidos por los usuarios.

El mapeo de capa 2 a capa 3 también puede ser configurado para emparejar el valor de CoS, esto porque los conmutadores ya presentan esta capacidad. Si un paquete que necesita ser marcado para diferenciar servicios QoS definidos por usuarios está saliendo de un enrutador y entrando a un conmutador, el enrutador debería configurar el valor CoS del paquete, porque el conmutador puede procesar la marcación de cabecera CoS de capa 2. Un usuario puede asignar 8 diferentes marcaciones CoS.

2.5.3. Marcación de valor de grupo QoS

Agrupar un paquete con un grupo local de QoS permite al usuario asociar un grupo ID con un paquete. El grupo ID puede ser usado para clasificar paquetes dentro de los grupos QoS basado en prefijos, sistemas autónomos o cadenas de comunidades.

Esta marcación de grupo QoS solo puede ser usada para clasificar tráfico dentro de un enrutador y no puede ser usada para marcar paquetes salientes de enrutador. El usuario puede configurar 100 diferentes marcaciones de grupo QoS.

2.5.4. Beneficios

La marcación de paquetes permite particionar a la red en niveles múltiples de prioridad o clases de servicio, como las siguientes:

- Usar la marcación QoS de paquetes para configurar valores de precedencia IP o DSCP IP para paquetes entrantes de la red. Entonces los dispositivos dentro de la red pueden usar los valores recientemente marcados de precedencia IP para determinar como el tráfico debería ser tratado. Por ejemplo, WRED basado en clase usa los valores de precedencia IP para determinar la probabilidad en que el paquete sería descartado. Adicionalmente, los paquetes de voz pueden ser marcados con un color particular (precedencia / DSCP). Entonces el encolamiento de latencia baja LLQ (descrita más adelante) puede ser configurado para colocar todos los paquetes de esta marca dentro de la cola de prioridad

- Usar la marcación de paquetes para asignar paquetes a un grupo QoS. Los enrutadores usan el grupo QoS para determinar cómo priorizar paquetes para la transmisión

- Usar la marcación CoS de paquete para asignar paquetes a configurar el valor de prioridad de paquetes ***802.1p*** [22]. Los enrutadores usan el valor CoS para determinar cómo priorizar paquetes para la transmisión y pueden usar estas marcaciones para realizar el mapeo de capa 2 a capa 3

[22] ***802.1p***. Estándar IEEE que proporciona priorización de tráfico y filtrado multicast dinámico. Proporciona un mecanismo para implementar QoS a nivel de MAC

CAPÍTULO 3

ADMINISTRAR LA CONGESTIÓN DE TRÁFICO

3.1 CARACTERÍSTICAS

Los diferentes procedimientos a ser tratados permitirán un control en la congestión de red por medio de la determinación del orden en el cual el paquete es enviado por una interfaz basada en prioridades asignadas a cada uno de esos paquetes.

La administración de tráfico implica la creación de colas, asignación de paquetes a estas colas basados en la clasificación del paquete y la planificación de los paquetes en una cola para la transmisión.

En cuanto a QoS, la administración de paquetes brinda cuatro tipos principales de protocolos de encolamiento, cada uno de los cuales permite especificar la creación de un número diferente de colas, ofreciendo un mayor o menor grado de diferenciación de tráfico, y especificar el orden en el cual este tráfico es enviado.

Durante los períodos de tráfico ligero, esto es, cuando no existe congestión, los paquetes son enviados por cada interfaz tan pronto como arriban. Durante los períodos de transmisión de la congestión en las interfaces de salida, los paquetes llegan más rápido que la interfaz puede enviarlos. Si se usa la característica de la administración de tráfico, los paquetes acumulados en una interface son encolados hasta que la interfaz está libre para enviarlos; entonces estos son programados para la transmisión de acuerdo a la prioridad asignada y el mecanismo de encolamiento configurado para la interfaz. El enrutador determina el orden de transmisión del paquete mediante el control por el cual los paquetes son ubicados en cada cola y cómo son los servicios de cada cola con respecto a las otras.

3.2. IMPORTANCIA DE LA UTILIZACIÓN

Las redes de comunicación incluyen diferentes protocolos usados para las aplicaciones, dando lugar a la necesidad de priorizar tráfico para satisfacer aplicaciones de tiempo crítico mientras que todavía debe hacer frente a las necesidades de las aplicaciones de menos tiempo dependientes, como la transferencia de archivos. Diferentes tipos de

tráfico compartiendo un camino de datos a través de la red puede interactuar con otro en formas que afecten el rendimiento de la aplicación. Si la red es diseñada para soportar diferentes tipos de tráfico que comparte un camino simple de datos entre enrutadores, se debe considerar la utilización de técnicas de administración de congestión para asegurar equidad de tratamiento a través de varios tipos de tráfico.

A continuación se detallan algunos factores a considerar para determinar la configuración de mecanismos de administración de congestión en QoS:

- La priorización de tráfico es muy importante para la sensibilidad del retardo, por ejemplo aplicaciones basadas en la transacción interactiva o videoconferencia de escritorio que requiere una alta prioridad a comparación de la transferencia de archivos

- La priorización es más efectiva en enlaces WAN donde la combinación del tráfico de ráfagas y las tasas de datos relativamente bajas pueden causar congestión temporal

- Dependiendo del tamaño promedio de paquete, la priorización es más efectiva cuando es aplicada en enlaces con velocidades de ancho de banda de **T1**[23]/**E1**[24] o inferiores

- Si los usuarios de aplicaciones corriendo a través de la red perciben un tiempo de respuesta malo, se debe considerar usar los mecanismos de administración de congestión. Estos son dinámicos, adaptándose a las condiciones actuales de la red. Sin embargo, si se considera que un enlace WAN está constantemente congestionado, la priorización de tráfico no puede resolver el problema. La solución más apropiada es la adición de ancho de banda al enlace

- Si no existe congestión en el enlace WAN, no hay razón para implementar la priorización de tráfico

Los siguientes ítems muestran aspectos que se deben considerar para determinar si se debería establecer e implementar políticas de encolamiento para la red:

- Determinar si la WAN está congestionada, esto es, si los usuarios de ciertas aplicaciones perciben una degradación en el rendimiento de las mismas

[23] ***T1***. Estándar de entramado y señalización para transmisión digital de voz y datos basado en PCM, usado en Norteamérica, Corea del Sur y Japón. Proporciona una tasa de 1.544 Mbps
[24] ***E1***. Formato de transmisión digital que da una tasa de 2.048 Mbps. Estándar utilizado principalmente en Europa y Sudamérica

- Determinar los fines y objetivos en el tráfico mixto basados en las necesidades a manejar, la topología de red y el diseño. En la identificación de lo que se quiere conseguir, considerar si el objetivo está entre los siguientes puntos:

- Establecer una distribución equitativa de asignación de ancho de banda a través de todos los tipos de tráfico identificados

- Otorgar una priorización estricta al tráfico de clases especiales de aplicaciones de servicio, por ejemplo aplicaciones multimedia interactivas

- Personalizar la asignación de ancho de banda de modo que los recursos de red son compartidos entre todas las aplicaciones de servicio, cada uno teniendo requerimientos de ancho de banda específicos después de haberlos identificado

- Configurar efectivamente el encolamiento. Se debe analizar el tipo de tráfico usado en la interfaz y determinar cómo distinguirlo

3.3. POLÍTICAS DE ENCOLAMIENTO

3.3.1. Encolamiento primero entra / primero sale FIFOQ

Como el tráfico de red llega a un punto de entrada o salida, como a una interfaz de enrutador, debe ser capaz de procesar adecuadamente el tráfico como este está siendo recibido. El encolamiento primero entra / primero sale FIFOQ (*First In / First Out Queuing*) es el enfoque más básico para ordenar tráfico en una comunicación adecuada. Una cola FIFO ubica todos los paquetes en una línea simple como van ingresando a la interfaz.

Los paquetes son procesados por el enrutador en el mismo orden que ingresan a la interfaz. No se asigna una prioridad determina a los paquetes. La razón importante del uso del encolamiento FIFO es que durante el proceso de enrutamiento, cuando un paquete se dirige de una interfaz de enrutador a otra, este a menudo cambia el tipo de interfaz y la velocidad. Por ejemplo, se considera un flujo de comunicación simple yendo de una interfaz de 100BaseT FastEthernet hacia una conexión serial a 512 Kbps. La figura. 3.1., muestra el proceso de encolamiento FIFO para el flujo en mención. El flujo encuentra un desajuste de velocidad. El segmento FastEthernet alimenta al flujo del enrutador en

100 Mbps, mientras que la conexión serial de salida envía el flujo en 512 Kbps. La cola FIFO es usada para ordenar los paquetes y mantenerlos hasta que el enlace serial pueda procesarlos correctamente.

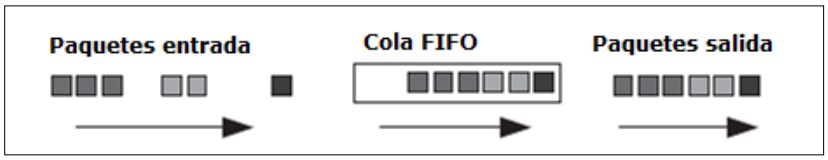


Figura. 3.1. Cola FIFO en operación[25]

La cola FIFO permite al enrutador procesar comunicaciones de muy alta velocidad de salida a través de una velocidad media más baja. En los casos donde la comunicación FastEthernet está compuesta de pequeñas ráfagas, la cola FIFO manipula todos los paquetes sin dificultad. Sin embargo, una mayor cantidad de tráfico de alta velocidad proveniente de la interfaz FastEthernet puede a menudo causar que la cola FIFO se desborde. Esta situación es conocida como *caída de la cola*, porque los paquetes son descartados desde la parte de atrás de la cola. La cola continuará con el descarte de paquetes en la parte de atrás hasta que procese los paquetes de adelante, liberando así el espacio dentro de la cola para acomodar los nuevos paquetes de entrada desde el fin de la parte de atrás. La figura. 3.2., muestra este procedimiento.

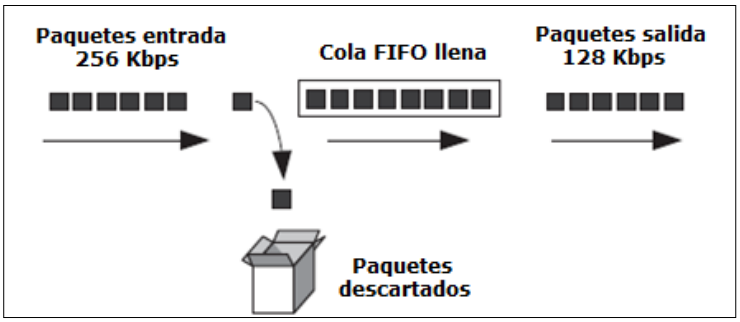


Figura. 3.2. Fin de la caída de cola FIFO[26]

La desventaja del encolamiento FIFO viene dado por la simplicidad. Puesto que no tiene un mecanismo para distinguir los paquetes que manipula, no tiene manera de asegurar que procese los paquetes justa y equitativamente. Este encolamiento simplemente procesa los paquetes en el mismo orden que ingresan a la cola. Esto significa que los protocolos de

[25] Durand, Benoit; Sommerville, Jerry; Buchmann, Mark; Fuller, Ron, *Administering CISCO QoS in IP Networks*, Syngress Media Inc, United States of America Marzo 2001, página 219
[26] Durand, Benoit; Sommerville, Jerry; Buchmann, Mark; Fuller, Ron, *Administering CISCO QoS in IP Networks*, Syngress Media Inc, United States of America Marzo 2001, página 219

tráfico alto, como el protocolo de transferencia de archivos FTP, pueden usar porciones significantes de la cola FIFO, dejando a los protocolos sensibles de tiempo, como Telnet, con un pequeño ancho de banda para operar. En tal caso, la sesión Telnet debería parecer interrumpida y sin respuesta, ya que la mayor parte de la cola es usada para transferir el FTP.

Es evidente que FIFO es un mecanismo de encolamiento muy básico que permite al enrutador ordenar y procesar paquetes de acuerdo a como concurren para salir de una interfaz. Los paquetes pueden venir de una o múltiples interfaces conectadas al enrutador. Es bueno señalar que este principio de cola simple es la base de los otros mecanismos de encolamiento, los cuales se construyen sobre este principio para ofrecer una mejor calidad de servicio dependiendo de los requerimientos de tráfico.

Se tiene claro que FIFO no parece ser un sofisticado o incluso deseable método de encolamiento, considerando las ricas características de otros mecanismos de encolamiento. Sin embargo, FIFO puede ser un método de encolamiento muy eficiente en ciertas circunstancias. Por ejemplo, un segmento Ethernet 10BaseT conectado a un enrutador que a su vez se conecta a una WAN a través de un segmento E1; en este caso, no existe opción que la comunicación de 10 Mbps de entrada pueda postrar al tubo de 2 Mbps de salida. El enrutador todavía requiere la cola FIFO para ordenar los paquetes en una línea simple con el fin de alimentarlos a la interfaz E1 para el procesamiento. El uso de un mecanismo simple de encolamiento reduce el retardo experimentado por los paquetes como el enrutador los procesa. En las aplicaciones sensibles al retardo, como voz o video, esto puede ser un factor inapropiado.

Una consecuencia negativa cuando los paquetes entran en el proceso de *caída de la cola* es que las retransmisiones son requeridas en capas superiores del modelo OSI.

3.3.2. Encolamiento de prioridad PQ

El encolamiento de prioridad PQ (*Priority Queuing*) permite a los administradores de red priorizar tráfico basado en criterios específicos. Estos criterios incluyen tipos de protocolo o subprotocolo, interfaces origen, tamaño de paquetes o cualquier parámetro identificado a través de una lista de acceso. PQ ofrece cuatro diferentes colas:

- Prioridad baja

- Prioridad normal
- Prioridad media
- Prioridad alta

A través de la configuración adecuada de PQ, cada paquete es asignado a una de estas colas. Si no es asignada una clasificación a un paquete, este es ubicado en la cola de prioridad normal. La prioridad de cada cola es absoluta. Cuando los paquetes son procesados, PQ examina el estado de cada cola, siempre sirviendo a las colas de más alta prioridad antes que las colas de prioridad más baja. Esto significa que mientras exista tráfico en la cola de prioridad más alta, las colas de prioridad más baja no serían procesadas. Por tanto, PQ no utiliza un reparto equitativo de recursos entre sus colas. Estrictamente PQ las atiende en base de las clasificaciones de prioridad configuradas por el administrador de red. La figura. 3.3., muestra el PQ en acción.

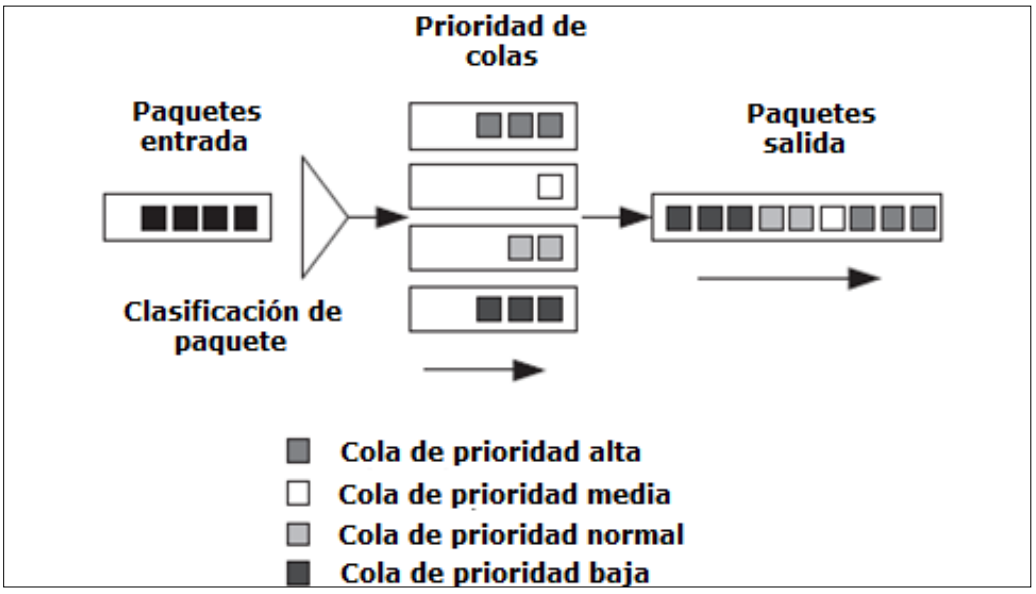


Figura. 3.3. Encolamiento de prioridad en operación[27]

Cada una de estas colas actúa como ***leaky bucket***[28] individual la cual es propensa al descarte de la cola. Los tamaños de cola por defecto se muestran en la tabla. 3.1. Estos tamaños de cola pueden ser ajustados manualmente de 0 a 32767 paquetes.

[27] Durand, Benoit; Sommerville, Jerry; Buchmann, Mark; Fuller, Ron, *Administering CISCO QoS in IP Networks*, Syngress Media Inc, United States of America Marzo 2001, página 222

Tabla. 3.1. Tamaños de cola por defecto de PQ

LÍMITE	TAMAÑO
Límite de cola de prioridad alta	20 paquetes
Límite de cola de prioridad media	40 paquetes
Límite de cola de prioridad normal	60 paquetes
Límite de cola de prioridad baja	80 paquetes

El encolamiento de prioridad puede parecer un enfoque tosco para la priorización de tráfico, pero permite dar a ciertas clases de tráfico prioridad sobre otras. Por ejemplo, muchos sistema heredados tal como *mainframes* usan arquitectura de red de sistemas SNA (*Systems Network Architecture*) como método de transporte. SNA es muy susceptible a los retardos por lo que sería un excelente candidato para una cola de prioridad alta. Si Telnet es el negocio central de una empresa, podría también ser colocado en la cola de alta prioridad sobre otros tipos de tráfico cualquiera. Esto asegura que los protocolos de volumen alto como FTP no impacten negativamente a las aplicaciones críticas del negocio.

Hay que recordar que la configuración de PQ dispone cómo el proceso de encolamiento operaría en ese enlace. Si nuevas aplicaciones usando protocolos nuevos son desplegadas dentro del ambiente de red, simplemente PQ ubicaría estos protocolos en la cola de prioridad normal. Por consiguiente, la configuración de PQ debería ser periódicamente revisada para asegurar la validez de la configuración de encolamiento.

Cuando se usa PQ, se debe dar una consideración seria a la priorización de tráfico. Si el tráfico asignado a la cola de alta prioridad es pesado, las colas de más baja prioridad nunca serían útiles. Esto conduce a que el tráfico en estas colas nunca está siendo transmitido y el tráfico adicional asignado a estas colas está siendo descartado de la cola. La figura. 3.4., representa esta situación.

[28] ***Leaky bucket***. Algoritmo utilizado para controlar la tasa en la cual los datos son inyectados dentro de una red. Utiliza las siguientes especificaciones: considerar una cubeta con un hueco en el fondo; si los paquetes arriban son ubicados dentro de la cubeta, si la cubeta está llena estos son descartados; los paquetes en la cubeta son enviados con una tasa constante, equivalente al tamaño del hueco en esta

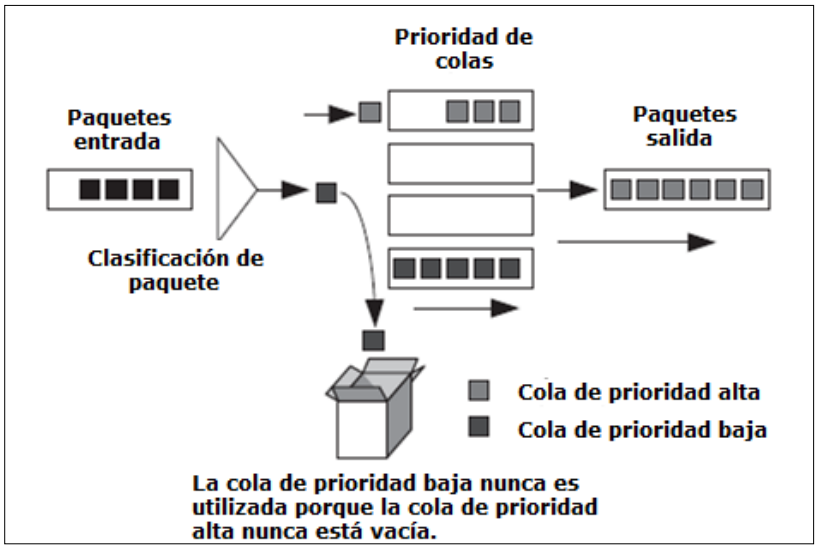


Figura. 3.4. Necesidad de cola en el encolamiento de prioridad[29]

3.3.3. Encolamiento personalizado CQ

Se ha visto como el encolamiento de prioridad permite asignar tráfico a diferentes colas, cada cola es tratada estrictamente dependiendo de su prioridad. El encolamiento personalizado CQ (*Custom Queuing*), desplaza el servicio de colas desde un mecanismo absoluto basado en la prioridad hacia un efecto ***round-robin***[30], atendiendo cada cola secuencialmente.

El encolamiento personalizado permite la creación de más de 16 colas de usuario, cada cola es atendida en secuencia por el proceso CQ. También existe una cola adicional, conocida como *cola* 0 (es una cola especial usada por el sistema para pasar paquetes de control de red, como por ejemplo paquetes de señalización, entre otros; tiene prioridad sobre todas las otras colas y así es vaciada antes de cualquier cola definida por el usuario), la misma que es creada automáticamente por el proceso de CQ. Esta cola es configurada por el usuario, pero esto no es recomendable. Cada una de las colas configurables por el usuario, e incluso la cola 0, representan un *leaky bucket* individual, el cual también es susceptible a los *descartes de la cola*.

El encolamiento personalizado asegura que cada cola sea atendida, evitando así la situación potencial en la cual cierta cola nunca sea procesada. Este encolamiento lleva su nombre del hecho que los administradores de red pueden controlar el número de colas en

[29] Durand, Benoit; Sommerville, Jerry; Buchmann, Mark; Fuller, Ron, *Administering CISCO QoS in IP Networks*, Syngress Media Inc, United States of America Marzo 2001, página 223
[30] ***Round – Robin***. Se refiere a un procedimiento por turnos o en cadena

los procesos de encolamiento. Adicionalmente, la cantidad de bytes o la cuenta de bytes para cada cola pueden ser ajustadas con el fin de gastar más tiempo en ciertas colas en los procesos de CQ. Por lo tanto, el encolamiento personalizado puede ofrecer un mecanismo de encolamiento más refinado, pero no puede asegurar prioridad absoluta como el encolamiento de prioridad.

El encolamiento personalizado opera mediante el servicio de colas configuradas por el usuario, individuales y secuenciales, para una cantidad específica de bytes. La cuenta de byte por defecto para cada cola es 1500 bytes, sin ninguna personalización, CQ debería procesar 1500 bytes de la cola 1, después 1500 bytes de la cola 2, luego 1500 bytes de la cola 3, y demás.

El tráfico puede ser clasificado y asignado a cualquier cola a través de los mismos métodos como en el encolamiento de prioridad, esto es, tipos de protocolo o subprotocolo, interfaces origen, tamaño de paquete o cualquier otro parámetro identificable a través de una lista de acceso. La figura. 3.5., muestra la operación del encolamiento personalizado.

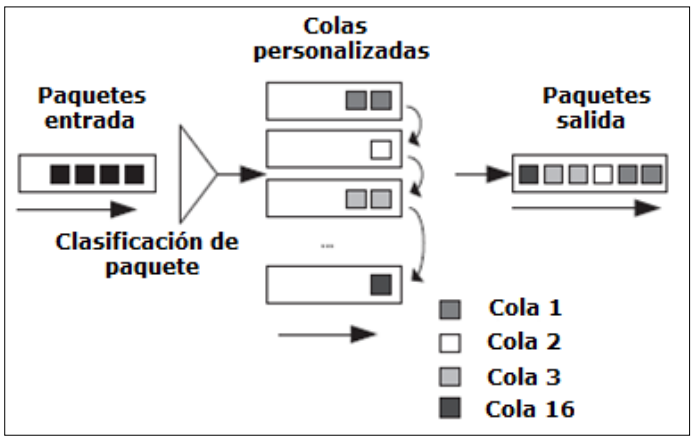


Figura. 3.5. Proceso del encolamiento personalizado[31]

A través de un prudente uso de la cuenta de byte de cada cola, es posible realizar asignaciones de ancho de banda usando encolamiento personalizado. Por ejemplo, en una comunicación de datos determinada, se quiere restringir el tráfico de navegación al 30% del total del ancho de banda, el tráfico de SSH a un 20% del total del ancho de banda y el 50% restante del ancho de banda para cualquier otro tráfico; para lo cual se podría configurar el encolamiento personalizado con tres colas, la cola 1 debería manipular todo

[31] Durand, Benoit; Sommerville, Jerry; Buchmann, Mark; Fuller, Ron, *Administering CISCO QoS in IP Networks*, Syngress Media Inc, United States of America Marzo 2001, página 225

el tráfico de navegación con una cuenta de byte por defecto de 1500 bytes, la cola 2 debería manipular todo el tráfico SSH también con una cuenta de byte por defecto de 1500 bytes, por último la cola 3 debería manipular todo el tráfico restante, pero sería manualmente asignada un valor de byte de 3000 bytes. La figura. 3.6., muestra esta configuración del encolamiento personalizado.

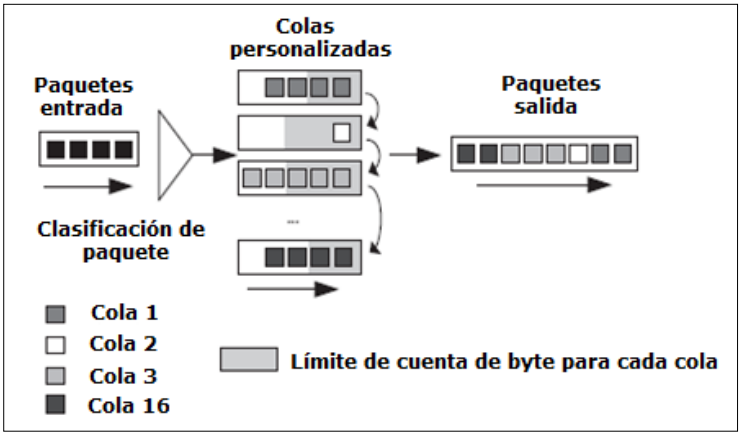


Figura. 3.6. Encolamiento personalizado con cuenta de byte[32]

En este caso, CQ procesaría 1500 bytes del tráfico de navegación, luego 1500 bytes del tráfico SSH y por último 3000 bytes del tráfico restante, dando el 30%, el 20% y el 50% de la asignación deseada. Si es disponible más ancho de banda llevando a una carga de tráfico de red ligera, CQ puede procesar más información desde cada cola. Haciendo referencia a la figura. 3.6., si solo las colas 1 y 2 tienen tráfico en ellas, serían cada una asignadas el 50% del total de ancho de banda. Los valores de cuenta de byte indican la asignación de ancho de banda en una situación congestionada.

El encolamiento personalizado no realiza fragmentación de paquete. Si un paquete es más grande que la asignación de cuenta de byte total de cada cola, CQ procesa de todas maneras el paquete entero. Esto significa que una cola de 1500 bytes atendería un paquete de 3000 bytes en su intervalo de 1500 bytes. En Ethernet o HDLC por ejemplo, donde la unidad de transmisión máxima MTU (*Maximum Transmission Unit*) tiene un tamaño de 1500 bytes, el valor de cuenta de byte por defecto de CQ es apropiado. En otros ambientes como *Token Ring* por ejemplo, donde el MTU puede crecer a 4098 bytes, el uso de colas de 1500 bytes para asignar ancho de banda puede conducir a una asignación de recurso incorrecta. Esta última observación es necesaria en una variedad de situaciones. Se ha visto

[32] Durand, Benoit; Sommerville, Jerry; Buchmann, Mark; Fuller, Ron, *Administering CISCO QoS in IP Networks*, Syngress Media Inc, United States of America Marzo 2001, página 225

que si una interfaz es permitida para enviar 1500 bytes y el primer paquete en la cola es de 1501 bytes o más, el paquete entero sería enviado. Sin embargo, también es cierto que si el primer paquete es de 1499 bytes y el segundo paquete es de 1500 bytes o más, el primer paquete entero sería enviado, y porque un byte adicional es permitido para ser transmitido, el segundo paquete entero también sería enviado.

La desventaja del encolamiento personalizado es que, como el encolamiento de prioridad, se debe crear sentencias de políticas en la interfaz para clasificar el tráfico a las colas. Si no se crean las políticas de encolamiento personalizado en la interfaz, todo el tráfico es ubicado en una cola simple (la cola por defecto) y es procesado en una base de encolamiento FIFO. El tamaño por defecto de cada cola CQ es 20 paquetes, al igual que el encolamiento de prioridad. Los tamaños de cola pueden ser ajustados manualmente de 0 a 32767 paquetes.

En cuanto a las interacciones de protocolos con el encolamiento personalizado es importante entender que este no proporciona garantías absolutas con respecto a la asignación de ancho de banda. El encolamiento personalizado soporta los protocolos de red, pero también este depende de las operaciones de estos protocolos. El encolamiento personalizado es un excelente mecanismo para realizar asignación de ancho de banda en enlaces de tráfico alto. Este permite a los administradores de red controlar el flujo de paquetes y proporcionar un *troughput* asegurado a servicios preferidos. Este mecanismo de encolamiento asegura que cada cola es atendida secuencialmente, no se adapta automáticamente a los cambios de ambiente de red. Todos los protocolos nuevos que no están definidos en la configuración CQ serían asignados a la cola por defecto para el procesamiento de la información.

3.3.4. Encolamiento equitativo ponderado WFQ

El encolamiento equitativo ponderado WFQ (*Weighted Fair Queuing*) clasifica dinámicamente el tráfico de red dentro de flujos individuales y asigna a cada flujo una participación equitativa del total de ancho de banda. Cada flujo es clasificado como un flujo de ancho de banda alto o un flujo de ancho de banda bajo. Los flujos de ancho de banda bajo como por ejemplo el Telnet, obtienen prioridad sobre los flujos de ancho de banda alto como el tráfico FTP.

Si múltiples flujos de ancho de banda alto ocurren simultáneamente, estos compartirán el ancho de banda restante uniformemente una vez que los flujos de ancho de banda bajo han sido atendidos. Cada uno de estos tráficos es ubicado dentro de una cola individual que sigue la analogía del *leaky bucket*. Si los paquetes de un flujo específico excedieron la capacidad de la cola a la cual es asignado, esta cola es sujeta al *descarte de la cola* como todas las otras colas.

Los enrutadores equipados con ***tarjetas de procesador de interface versátil VIP***[33] (*Versatile Interface Processor*) pueden descargar el proceso WFQ a estas tarjetas. En este caso, el proceso es referido como encolamiento equitativo ponderado distribuido DWFQ (definido posteriormente). Delegar el proceso WFQ a la tarjeta VIP crea memoria y ciclos de CPU adicionales desde el procesador principal disponible del enrutador. Esta arquitectura distribuida permite enrutadores de alta potencia para realizar un número largo de tareas concurrentes sin exceso en el procesador del enrutador.

En cuanto al funcionamiento, WFQ primero identifica cada flujo individual y lo clasifica como flujo de ancho de banda alto o bajo. Cada flujo es caracterizado usando la información del Anexo A2.

Una vez clasificados, los flujos son ubicados en una cola equitativa. El número por defecto de las colas dinámicas es 256. Cada cola es atendida en una manera *round-robin*, como en el encolamiento personalizado, dando prioridad a las colas de ancho de banda bajo. Cada cola es configurada con un umbral de descarte congestivo por defecto que limita el número de mensajes en cada cola, este valor por defecto para cada cola es de 64 paquetes.

Para flujos de ancho de banda alto, los mensajes que intentan entrar en la cola una vez alcanzado el umbral de descarte, son descartados. Sin embargo, los mensajes de ancho de banda bajo todavía pueden entrar a la cola aunque el umbral de descarte congestivo es excedido por esta cola. Los límites para las colas dinámicas y el umbral de descarte congestivo pueden ser ajustados sobre un valor de 4096 paquetes.

Hasta ahora el proceso descrito muestra un tratamiento igual de todas las conversaciones ocurridas en una interface de salida. Aparte de la diferenciación entre flujos

[33] ***Tarjeta VIP***: Es en esencia un enrutador dentro de un enrutador. Estas tarjetas tienen los cerebros y el poder computacional necesario para realizar ciertas funciones que normalmente serían enviadas al procesador principal

de velocidad alta y baja, estas conversaciones no tiene ninguna prioridad o peso la una sobre la otra. Por lo tanto, este proceso sería referido como encolamiento equitativo.

Ahora bien, el factor ponderado empieza a afectar el proceso de encolamiento cuando el campo ToS o el campo de precedencia IP son diferentes. WFQ toma en cuenta la precedencia IP y da tratamiento preferencial a los flujos de precedencia más alta ajustando sus pesos. Si todos los paquetes tienen el mismo valor de precedencia por defecto, entonces el factor ponderado no afecta el proceso WFQ.

El peso de los flujos, donde los valores presentes de ToS son diferentes, es calculado mediante la adición de 1 a la precedencia del paquete. El peso total de todos los flujos representa el ancho de banda total a ser dividido entre los flujos individuales. Por ejemplo, si tres flujos utilizan una precedencia IP por defecto de 0, cada flujo tiene un peso de 1 (0+1). El peso del ancho de banda total es 3 (1+1+1), y cada flujo representa un tercio del total del ancho de banda. En cambio, si dos flujos tiene una precedencia IP de 0, y un tercer flujo tiene una precedencia de 5, el peso total es 8 (1+1+6). Los primeros dos flujos representan cada uno un octavo del ancho de banda, mientras que el tercer flujo recibe seis octavos del ancho de banda.

Cabe indicar que cuando WFQ es configurado en un enlace, el protocolo de reservación de recurso RSVP hace uso de diferentes colas dentro del proceso de WFQ con el fin de asegura que los requerimientos de QoS de las conversaciones RSVP sean respetados. El número por defecto reservado de las colas RSVP es 0. Esto significa que con el fin de que WFQ soporte adecuadamente RSVP, este debe ser configurado manualmente a otro valor que el valor por defecto.

WFQ es simple de implementar, es un mecanismo de encolamiento dinámico el cual asegura que toda conversación en la red alcance una compartición equitativa del ancho de banda. A diferencia de PQ y CQ, los cuales necesitan ser configurados manualmente, WFQ se adapta dinámicamente a los cambios de la red, incluyendo nuevos protocolos y aplicaciones. Si no existe tráfico crítico que debe ser dado prioridad sobre otro tráfico, WFQ es un método fácil y eficiente para proporcionar el mejor nivel de servicio a todo usuario de red.

Encolamiento equitativo ponderado basado en flujo FBWFQ.

El término basado en flujo FB (*Flow-Based*) se refiere a un método de identificación de cadenas de comunicación. Esto es como WFQ asigna tráfico a diferentes colas. El encolamiento de prioridad y el encolamiento personalizado utilizan un método estático de clasificación de tráfico.

Los paquetes de entrada al proceso de encolamiento son clasificados por protocolo, puerto, dirección de red u otros factores determinados por el administrador de red. Por ejemplo, si el tráfico SSH es asignado a una cola de prioridad alta en PQ, todo el tráfico SSH, a pesar el origen o destino, sería asignado a la cola de prioridad alta. PQ trataría todo el tráfico SSH igual. Consecuentemente, si un *host* tiene más tráfico SSH que otro *host*, el encolamiento de prioridad no podría asegurar cualquier tipo de equidad dentro de esta cola de alta prioridad. En cambio, WFQ clasifica el tráfico usando una combinación de todos los parámetros encontrados en el Anexo A2. Esto significa que el tráfico SSH desde el *host* A hacia el *host* B sería considerado como un flujo, y el tráfico SSH desde el *host* A hacia el *host* C sería considerado como un flujo separado.

Encolamiento equitativo ponderado distribuido DWFQ.

El encolamiento equitativo ponderado distribuido DWFQ (*Distributed Weighted Fair Queuing*), como ya se lo mencionó, es una versión especial de alta velocidad de WFQ que corre sobre tarjetas VIP.

Existen dos formas del WFQ distribuido:

- Basado en flujo. En esta forma, los paquetes son clasificados por flujo. Los paquetes con la misma dirección IP de origen, dirección IP de destino, puerto origen TCP o UDP, puerto destino TCP o UDP, protocolo o campo ToS pertenecen al mismo flujo. Cada flujo corresponde a una cola de salida separada. Cuando un paquete es asignado a un flujo, este es ubicado en la cola para ese flujo. Durante periodos de congestión, DWFQ asigna una contribución igual del ancho de banda para cada cola activa. DWFQ basado en flujo es también llamado encolamiento equitativo porque todos los flujos son igualmente ponderados y asignados igual ancho de banda

- Basado en clase. En esta forma, los paquetes son asignados a diferentes colas basadas en el grupo de QoS o la precedencia IP en el campo ToS. Los grupos de QoS permiten personalizar las políticas QoS. Un grupo QoS es una clasificación interna de paquetes usada por el enrutador para determinar cómo los paquetes son tratados por ciertas características de QoS, como DWFQ y CAR. Si se quiere clasificar los paquetes basados solo en los dos bits de precedencia IP bajos, se usa DWFQ basado en ToS. Especifica un peso por cada clase. En los períodos de congestión, cada grupo es asignado un porcentaje de ancho de banda de salida igual al peso de la clase. Por ejemplo, si una clase es asignada un peso de 40, los paquetes de esta clase serían asignados por lo menos el 40% del ancho de banda de salida durante los períodos de congestión. Cuando la interfaz no está congestionada, las colas pueden usar cualquier ancho de banda disponible

DWFQ realiza un seguimiento del número de paquetes en cada cola y el número total de paquetes en todas las colas. Cuando el número total de paquetes está por debajo del límite agregado, las colas pueden almacenar más paquetes que el límite de cola individual. Cuando el número total de paquetes alcanza el límite agregado, la interfaz empieza a hacer cumplir los límites de cola individual. Cualquier paquete nuevo que arriba para una cola que tiene excedido su límite de cola individual, es descartado. Los paquetes que ya están en la cola no serían descartados, incluso si la cola está sobre el límite individual.

Encolamiento equitativo ponderado basado en clase CBWFQ.

El encolamiento equitativo ponderado basado en clase CBWFQ (*Class-Based Wighted Fair Queuing*) extiende la funcionalidad estándar de WFQ para proporcionar apoyo para las clases de tráfico definidas por usuarios. Para CBWFQ, se define clases de tráfico basadas en criterios de emparejamiento incluyendo protocolos, listas de control de acceso e interfaces de entrada. La satisfacción de los paquetes del criterio de emparejamiento para una clase constituye el tráfico para dicha clase. Una cola FIFO es reservada para cada clase, y el tráfico perteneciente a una clase es dirigido a la cola para dicha clase.

Una vez que una clase ha sido definida de acuerdo a su criterio de emparejamiento, se puede asignar sus características. Para caracterizar una clase, se asigna su ancho de

banda, ponderación y límite de paquetes máximo. El ancho de banda asignado a una clase es el ancho de banda entregado y garantizado a la clase durante la congestión.

Para caracterizar una clase, también se especifica el límite de cola para dicha clase, el cual es el número máximo de paquetes permitidos a acumular en la cola para la clase. Los paquetes pertenecientes a una clase son sujetos a los límites de ancho de banda y cola que caracterizan la clase.

Después que una cola ha alcanzado su límite de cola configurado, el encolamiento de paquetes adicionales a la clase causa descarte de la cola o de paquetes a tomar efecto, dependiendo en como la política de clase es configurada.

Se debe tomar algunos aspectos en cuenta dentro de esta técnica de encolamiento, como por ejemplo, si una clase por defecto es configurada basando su política de clase en el ancho de banda, todo el tráfico no clasificado es puesto dentro de una cola FIFO simple y dado el tratamiento acorde al ancho de banda configurado; en cambio, si una clase por defecto es configurada basada en la cola equitativa, todo el tráfico no clasificado es clasificado flujo y dado el tratamiento de mejor esfuerzo. Ahora bien, si la clase por defecto no es configurada, entonces por defecto el tráfico que no coincide con ninguna de las clases configuradas es clasificado flujo y dado el tratamiento de mejor esfuerzo. Una vez que un paquete es clasificado, todos los mecanismos estándares pueden ser utilizados para aplicar servicio diferenciado entre clases.

La clasificación de flujo es tratamiento estándar WFQ. Esto es, los paquetes con la misma dirección IP de origen, dirección IP de destino, puerto TCP o UDP origen son clasificados como pertenecientes al mismo flujo. WFQ asigna una parte igual de ancho de banda para cada flujo. Se debe recordar que WFQ basado en flujo es también llamado encolamiento equitativo porque todos los flujos son igualmente ponderados.

Para CBWFQ, la ponderación especificada para la clase se convierte en la ponderación de cada paquete que conoce el criterio de emparejamiento de la clase. Los paquetes que arriban en la interfaz de salida son clasificados de acuerdo a los filtros de criterio de emparejamiento que se definen, entonces cada uno es asignado la ponderación apropiada. La ponderación para un paquete perteneciente a una clase específica es derivada

del ancho de banda asignado a la clase donde se configura; en este sentido la ponderación para una clase es configurable por el usuario.

Después que la ponderación para un paquete es asignada, el paquete es encolado en la cola de clase apropiada. CBWFQ utiliza las ponderaciones asignadas a los paquetes encolados para asegurar que la cola de clase es atendida completamente.

Existen tres procesos a tomar en cuenta cuando se desea configurar CBWFQ, estos son:

- Definir las clases de tráfico para especificar la política de clasificación. Este proceso determina cuantos tipos de paquetes son diferenciados uno del otro

- Asociar las políticas con cada clase de tráfico, estas son las características de clase. Este proceso implica la configuración de políticas a ser aplicadas a los paquetes pertenecientes a una de las clases previamente definidas. Para este proceso, se configura la política que especifica a cada clase de tráfico

- Adjuntar las políticas a las interfaces. Este proceso requiere que se asocie una política existente con una interfaz para aplicar el conjunto de políticas a dicha interfaz

Existen algunos factores que se debería considerar para determinar si es necesario aplicar el procedimiento de CBWFQ en una aplicación, los mismos son:

- Asignación de ancho de banda. CBWFQ permite especificar la cantidad exacta de ancho de banda a ser asignada para una clase específica de tráfico. Teniendo en cuenta el ancho de banda disponible en la interfaz, se puede configurar un máximo de 64 clases y controlar la distribución entre ellas

- Más granularidad y escalabilidad. CBWFQ permite definir qué constituye una clase basándose en criterios que exceden los confines de flujo. CBWFQ permite usar listas de control de acceso y protocolos o nombres de interfaces de entrada para definir cómo el tráfico sería clasificado, de este modo proporcionar más granularidad. No es necesario mantener la clasificación de tráfico en un flujo base. Además se puede configurar un máximo de 64 clases discretas en una política de servicio

En cuanto a RSVP, puede ser usado en conjunto con CBWFQ. Cuando RSVP y CBWFQ son configurados para una interfaz, ambos actúan independientemente, exhibiendo el mismo comportamiento si fueran ejecutados solos. RSVP sigue trabajando como lo hace cuando CBWFQ no está presente, incluso en relación a la valoración de disponibilidad de ancho de banda y asignación.

Encolamiento equitativo ponderado basado en clase distribuido DCBWFQ.

Anteriormente se expuso que WFQ ofrece dinámica, encolamiento equitativo que divide el ancho de banda a través de las colas de tráfico basado en ponderaciones. WFQ asegura que todo el tráfico es tratado completamente, dándose ponderaciones.

El encolamiento equitativo ponderado basado en clase distribuido DCBWFQ (*Distributed Class – Based Weighted Fair Queueing*) extiende la funcionalidad estándar para proporcionar apoyo para clases de tráfico definidas por usuario en el procesador de interface versátil VIP.

El número máximo de paquetes permitidos para acumular en una cola de clase de tráfico es conocido como límite de cola. Los paquetes pertenecientes a una clase de tráfico están sujetos a la asignación de ancho de banda garantizado y los límites de cola que caracterizan la clase de tráfico. Después de que una cola ha alcanzo el límite de cola configurado, el encolamiento de paquetes adicionales a la clase de tráfico causa *descarte de la cola* u otro tipo de descarte, dependiendo de cómo la política de servicio es configurada. Hay que recordar que el *descarte de la cola* es un medio para evitar la congestión que trata a todo el tráfico igualmente y no diferencia entre clase de servicio. Las colas se llenan durante períodos de congestión. Cuando la cola de salida está llena y el *descarte de la cola* se efectúa, los paquetes son descartados hasta que la congestión es eliminada y la cola ya no está llena.

Se tiene que para la interacción entre DCBWFQ con RSVP, cuando se configuran ambos actúan independientemente uno del otro. RSVP y DCBWFQ asignan ancho de banda entre sus clases de tráfico y flujos de acuerdo a un ancho de banda no asignado disponible en el punto de congestión subyacente. Cuando un flujo RSVP es creado, el sistema de encolamiento de VIP reserva la unidad de asignación de ancho de banda en una

cola RSVP, de manera similar una cola de clase de tráfico es asignada a una clase de tráfico DCBWFQ. Las clases de tráfico DCBWFQ no son afectadas por los flujos RSVP.

3.3.5 Prioridad IP RTP

Las características de la prioridad IP del protocolo de transporte de tiempo real IP RTP (*IP Real - Time Transport Protocol*) proporcionan un esquema de encolamiento de prioridad estricto para datos sensibles al retardo como los de voz. El tráfico de voz puede ser identificado por sus números de puerto RTP y clasificado dentro de una cola de prioridad configurada con prioridad IP RTP.

IP RTP permite especificar un rango de puertos UDP/RTP cuyo tráfico está garantizado en el servicio de prioridad estricta sobre cualquier cola o clase usadas sobre la misma interfaz de salida. Prioridad estricta significa que si los paquetes existen en la cola de prioridad, estos son desencolados y después los paquetes en otras colas son desencolados.

IP RTP no requiere que se conozca el puerto de una llamada de voz. Más bien, la característica da la habilidad para identificar un rango de puertos cuyo tráfico es colocado dentro de la cola de prioridad. Por otra parte, se puede especificar todo el rango de puertos de voz (16384 - 32767) para asegurar que todo el tráfico de voz sea un servicio de prioridad estricta. La prioridad IP RTP es especialmente útil en enlaces cuya velocidad es inferior que 1.544 Mbps.

Esta característica puede ser usada en conjunto con WFQ o CBWFQ en la misma interfaz de salida. En cualquier caso, el tráfico empareja el rango de puertos especificado para la cola de prioridad que está garantizada para prioridad estricta sobre otras clases CBWFQ o flujos WFQ; los paquetes en la cola de prioridad siempre son atendidos primero. Notar las siguientes condiciones al utilizar la prioridad IP RTP:

- Cuando es usada en conjunción con WFQ, la prioridad IP RTP proporciona una prioridad estricta a la voz, y el procedimiento WFQ es aplicado a las restantes colas

- Cuando es usada en conjunción con CBWFQ, la prioridad IP RTP proporciona una prioridad estricta a la voz. CBWFQ puede ser usado para la creación de clases para otro tipo de tráfico que necesita ancho de banda dedicado y necesita ser tratado mejor que el

mejor esfuerzo y no como prioridad estricta; el tráfico que no es de voz es atendido completamente basado en las ponderaciones asignadas a los paquetes encolados

En cuanto a la asignación de ancho de banda, es importante considerar las características de control de admisión y políticas de la prioridad IP RTP. Cuando se usa la prioridad IP RTP para configurar la cola de prioridad para la voz, se especifica una limitación de ancho de banda estricta. Esta cantidad de ancho de banda es garantizada para el tráfico de voz encolado en la cola de prioridad.

Las políticas de la prioridad IP RTP utilizan estrechamente el ancho de banda para la cola de prioridad, asegurando que la cantidad asignada no esté excedida en el momento de congestión. Esta prioridad prohíbe la transmisión de paquetes adicionales una vez que el ancho de banda asignado esté consumido. Si se determina que la cantidad configurada de ancho de banda es excedida, la prioridad IP RTP descarta paquetes, un evento que es pocamente tolerado por el tráfico de voz. La política cerrada permite un justo tratamiento de otros paquetes de datos encolados en otras colas, CBWFQ o WFQ. Evitar el descarte de paquetes, es estar seguro de asignar a la cola de prioridad la cantidad más óptima de ancho de banda, considerando el tipo de códec usado y las características de la interfaz. La prioridad IP RTP no permitirá tráfico más allá de la cantidad asignada.

Es siempre seguro asignar a la cola de prioridad algo más de la conocida cantidad requerida de ancho de banda. ***Por ejemplo***[34], ‘’suponer que se asigna 24 Kbps de ancho de banda, la cantidad estándar requerida para la transmisión de voz, a la cola de prioridad. Esta asignación parece segura porque la transmisión de paquetes de voz sucede en una tasa de bit constante. Sin embargo, porque la red y el enrutador o conmutador pueden usar algo del ancho de banda e introducir *jitter* y retardo, la asignación de poco más de la cantidad requerida de ancho de banda, como 25 Kbps, asegura constancia y disponibilidad’’.

La política de control de admisión de la prioridad IP RTP toma en cuenta la compresión de la cabecera RTP. Por lo tanto, al configurar los parámetros de ancho de banda para la prioridad IP RTP solo se necesita configurar para el ancho de banda de la llamada comprimida. ***Por ejemplo***[35], ‘’si una llamada de voz con G.709 requiere 24 Kbps de ancho de banda no comprimida pero solo 12 Kbps de ancho de banda comprimido, se

[35] y [36] Ejemplos tomado de Internetworking Technology Handbook - Quality of Service (QoS) - Cisco Systems, http://www.cisco.com/en/US/docs/internetworking/technology/handbook/QoS.html, Publicación 2007, Consultado en Agosto 2009

necesita configurar un ancho de banda de 12 Kbps. Se necesita asignar suficiente ancho de banda para todas las llamadas si habría más de una llamada''.

La suma de toda la asignación de ancho de banda para la voz y flujos de datos en una interfaz no puede exceder el 75% del ancho de banda total disponible. La asignación de ancho de banda para los paquetes de voz toma en cuenta además la carga útil de las cabeceras IP, RTP y UDP, pero no la cabecera de capa 2. Permitir el 25% del ancho de banda para otra sobrecarga es conservativo y seguro.

Si se conoce cuanto ancho de banda es requerido para la sobrecarga adicional en un enlace, bajo circunstancias agresivas en las cuales se quiera dar tráfico de voz tanto como el ancho de banda sea posible se puede anular el 75% de asignación máxima para la suma de ancho de banda asignada a todas las clases o flujos usando la característica de ancho de banda máximo reservado.

Otra alternativa, si la importancia del tráfico de voz es más que los datos, se puede asignar más del 75% del ancho de banda usado para flujos y clases a la cola de prioridad de voz. El ancho de banda no usado en cualquier punto se pondrá a disposición para otros flujos o clases.

3.3.6. Encolamiento de baja latencia LLQ

El encolamiento de baja latencia LLQ (*Low Latency Queueing*) logra un estricto PQ a CBWFQ. PQ estricto permite a los datos sensibles al retardo como la voz ser desencolados y enviados antes que los paquetes en otras colas sean desencolados.

Sin LLQ, CBWFQ proporciona WFQ basado en clases definidas con cola de prioridad no estricta disponible para tráfico en tiempo real. CBWFQ permite definir las clases de tráfico y luego asignar características a esas clases.

Para CBWFQ, la ponderación para un paquete perteneciente a una clase específica es derivada del ancho de banda asignado a la clase cuando se configura. Por tanto, el ancho de banda asignado a los paquetes de una clase determina el orden en el cual los paquetes son enviados. Todos los paquetes son atendidos completamente sobre la ponderación; no se concede prioridad estricta a la clase de paquetes. Este esquema plantea problemas para el tráfico de voz que es sumamente intolerante al retardo, especialmente variaciones de

retardo. Para le tráfico de voz, las variaciones en retardo introducen irregularidades de transmisión manifestadas como *jitter* el momento de escuchar la conversación.

LLQ proporciona encolamiento de prioridad estricta para CBWFQ, reduciendo el *jitter* en las conversaciones de voz. LLQ permite el uso de una simple cola de prioridad estricta dentro de CBWFQ en el nivel de clase, permitiendo direccionar tráfico perteneciente a una clase a la cola de prioridad estricta CBWFQ. Para encolar tráfico de clase a una cola de prioridad estricta, se especifica la clase nombrada dentro de una política y luego se configura la prioridad para la clase. Dentro de la política, se puede dar una o más estados de prioridad de clase. Cuando múltiples clases dentro de una política simple son configuradas como clases de prioridad, todo el tráfico de estas clases es encolado a la misma cola de prioridad estricta.

Una de las maneras en la cual el PQ estricto usado dentro de CBWFQ difiere de su uso fuera de CBWFQ está en los parámetros que toma. Fuera de CBWFQ, se puede utilizar la prioridad IP RTP para especificar el rango de puertos UDP cuyos flujos de tráfico de voz son dados servicio de prioridad. Usar LLQ, no se limita a un número de puerto UDP para estipular prioridad de flujos porque se puede configurar el estado de prioridad para una clase dentro de CBWFQ. En lugar de que todo el criterio de emparejamiento valido usado para especificar tráfico para una clase, ahora aplica a la prioridad de tráfico. Estos métodos de especificación de tráfico para una clase incluyen emparejamiento en listas de acceso, protocolos e interfaces de entrada. Por otra parte, dentro de una lista de acceso se puede especificar que tráfico emparejado es permitido, basado en el valor DSCP que es colocado.

Aunque es posible encolar varios tipos de tráfico en tiempo real a la cola de prioridad estricta, se recomienda que se direccione solo el tráfico de voz a esta porque el tráfico de voz es bien comportado, mientras que otro tipo de tráfico en tiempo real no lo es. Además, el tráfico de voz requiere que el retardo no varíe con el fin de evitar el *jitter*. El tráfico en tiempo real como el video podría introducir variación en el retardo, frustrando con ello la estabilidad del retardo necesario para el éxito de la transmisión del tráfico de voz.

CAPÍTULO 4

PREVENCIÓN DE CONGESTIÓN DE TRÁFICO

4.1. VISIÓN

Las técnicas de prevención de congestión de tráfico controlan las cargas de tráfico de red en un esfuerzo por anticipar y evitar la congestión en un cuello de botella común dentro de una red de comunicación. La prevención de congestión es lograda a través del descarte de paquetes.

Uno de los mecanismos más usados para evitar la congestión de tráfico sobre la red es la detección aleatoria anticipada RED (tratada más adelante), la misma que es óptima para redes con una elevada velocidad de tránsito.

En la mayoría de equipos de implementación de QoS existe un mecanismo tosco de descarte de paquetes por defecto conocido como *descarte de la cola*, el mismo que realiza un tratamiento de tráfico equitativo y no hace diferenciación entre clases de servicio. Las colas se llenan durante los períodos de congestión. Cuando la salida de cola se encuentra llena y el *descarte de la cola* está en ejecución, los paquetes son descartados hasta que la congestión termine y la cola ya no se presente llena.

4.2. POLÍTICAS Y MODELACIÓN

Existen dos tipos de mecanismos de regulación de tráfico conocidos como políticas y modelación. Se puede implementar cada una de las características inmersas dentro de estos mecanismos a través de la red de comunicación, con el objetivo de asegurar que un paquete o que datos de origen se adhieran a un convenio estipulado y determinar la calidad de servicio a ser entregada al paquete. Los mecanismos de política y modelación usan el descriptor de tráfico para un paquete, indicado por el proceso de clasificación del paquete, para asegurar adherencia y servicio.

Generalmente estos mecanismos identifican las violaciones del descriptor de tráfico de la misma manera, sin embargo, difieren en la forma de responder a dichas violaciones, por ejemplo, una política típicamente descarta tráfico de paquetes; en cambio, una

modelación retarda el tráfico excedido usando un *buffer* o mecanismos de encolamiento para mantener los paquetes y la forma de flujo cuando la tasa de datos del origen es mucho más alta de lo esperado.

4.2.1. Token bucket

Un *token bucket* es una definición formal para tasa de transferencia y posee tres componentes principales: tamaño de ráfaga, tasa promedio e intervalo de tiempo (Tc).

Aunque generalmente la tasa promedio es representada como bits por segundo, cualquiera de los dos valores puede derivarse del tercero por la siguiente relación:

$$tasa\_promedio = tamaño\_ráfaga / Intervalo\_tiempo$$

Dentro de la que se debe entender las siguientes definiciones para los términos en mención:

- Tasa promedio. Conocida como CIR, especifica cuanta información puede ser enviada o transmitida por unidad de tiempo en promedio

- Tamaño de ráfaga. También llamada tasa de ráfaga comprometida Bc (*Burst commited*), indica en bits o bytes por ráfaga cuánto tráfico puede ser enviado dentro de una unidad de tiempo para no crear problemas en lo programado

- Intervalo de tiempo. Denominado medida de intervalo, representa la parte de tiempo en segundos por ráfaga

Por definición, sobre cualquier múltiplo entero del intervalo, la tasa de bit de la interfaz no excedería a la tasa promedio. Sin embargo, la tasa de bit puede ser arbitrariamente rápida dentro del intervalo.

Un *token bucket* es usado para manejar un dispositivo que regula los datos en un flujo. Un *token bucket* por sí solo no tiene políticas de descarte o prioridad, más bien, un *token bucket* descarta muestras y dirige al flujo el problema de manejar su cola de transmisión si el flujo sobrepasa el regulador.

Para entender la metáfora de *token bucket*, se puede decir que algunas fichas (*tokens*) son colocadas dentro de una cubeta (*bucket*) a una cierta tasa. La cubeta por si misma tiene

una capacidad especificada. Si la cubeta llena su capacidad, las fichas recién recibidas son descartadas. Cada ficha está permitida por el origen enviar un cierto número de bits dentro de la red. Al enviar un paquete, el regulador debe remover desde la cubeta un número de muestras equivalente en representación al tamaño de paquete.

Si no están suficientes fichas en la cubeta para enviar un paquete, el paquete espera hasta que la cubeta las tenga o el paquete es descartado, esto depende del mecanismo a ser usado. Si la cubeta ya está llena de fichas, las fichas entrantes se desbordan y no están disponibles para los futuros paquetes. En consecuencia, en cualquier tiempo, la ráfaga más grande que un origen puede enviar dentro de la red es aproximadamente proporcional al tamaño de la cubeta.

Se nota que el mecanismo de *token bucket* usado para la modelación de tráfico tiene un *token bucket* como tal y un *buffer* de datos (o encolamiento); si este no tiene un *buffer* de datos, sería una política de tráfico. Para la modelación de tráfico, los paquetes que arriban y no pueden ser enviados inmediatamente son retardados en el *buffer* de datos.

Para la modelación de tráfico, un *token bucket* permite ráfagas pero las limita. Este garantiza que las ráfagas de tráfico estén limitadas de modo que el flujo nunca se enviaría más rápido que la capacidad del *tocken bucket*, dividido por el intervalo de tiempo, más la tasa establecida en la que las fichas son colocadas en la cubeta. Esto se resume en la siguiente fórmula:

$$(capacidad\_token\_bucket\_en\_segundos / Intervalo\_tiempo\_en\_segundos) + tasa\_establecida\_en\_bps = velocidad\_flujo\_Maxima\_en\_bps$$

Este método de limitación de ráfaga también garantiza que la tasa de transmisión a largo plazo no exceda a la tasa establecida en la que las fichas con colocadas en la cubeta.

4.2.2. Políticas con CAR

La tasa de acceso comprometida CAR (*Commited Access Rate*) encarna una característica de limitación de tasa para las políticas de tráfico, las cuales manejan la política de acceso de ancho de banda para una red garantizando que el tráfico que se encuadra dentro de parámetros de tasa especificados sea enviado, mientras que descartan

paquetes que exceden la cantidad aceptable de tráfico o los envían con una prioridad diferente. La acción exceder para CAR es descartar o rebajar paquetes.

Las funciones de limitación de tasa realizan lo siguiente:

- Permite controlar la tasa máxima de tráfico enviada o recibida en una interfaz
- Proporciona la habilidad para definir capa 3 total o parcial en los límites de tasa de ancho de banda de entrada o salida, y, de especificar las políticas de manejo de tráfico cuando este sea conforme o superior a los límites de tasa especificada. Los límites de tasa de ancho de banda total ajustan todos los paquetes sobre las interfaces o subinterfaces. Los límites de tasa de ancho de banda parcial ajustan un tipo particular de tráfico basado en precedencia, direcciones MAC u otro parámetro.

CAR es configurado generalmente en interfaces de borde de una red para limitar el tráfico dentro o fuera de la misma.

Funcionamiento.

CAR examina el tráfico recibido sobre una interfaz o un subconjunto seleccionado de ese tráfico mediante el criterio de listas de acceso. A continuación se compara la tasa de tráfico a un *token bucket* configurado y toma una acción basada en el resultado. Por ejemplo, CAR descartaría el paquete o reescribiría la precedencia IP restableciendo los bits de tipo de servicio (ToS). Se puede configurar CAR para enviar, descartar o establecer una precedencia.

Algunos aspectos sobre la limitación de tasa con CAR son expuestos en las siguientes secciones y estos son:

- Criterios de correspondencia
- Límites de tasa
- Acciones ajustadas y excedidas
- Políticas de tasa múltiple

CAR utiliza una medida de *token bucket*. Las fichas son insertadas dentro de la cubeta en la tasa comprometida. La profundidad de la cubeta es el tamaño de ráfaga. El tráfico que llega a la cubeta cuando están disponibles suficientes fichas es llamado conforme y el número correspondiente de fichas son borradas de la cubeta. Si un número suficiente de fichas no está disponible, el tráfico es denominado excedido.

Criterios de correspondencia.

Correspondencia de tráfico implica identificación de tráfico de interés para la limitación de tasa, establecer precedencia o ambas. Las políticas de tasa pueden ser asociadas con una de las siguientes cualidades:

- Interfaces de entrada
- Todo tráfico IP
- Precedencia IP (definida por una lista de acceso de límite de tasa)
- Dirección MAC (definida por una lista de acceso de límite de tasa)
- Valor experimental de conmutación de etiquetas multiprotocolo ***MPLS***[36] (*Multiprotocol Label Switching*) (definido por una lista de acceso de límite de tasa)
- Lista de acceso IP (***estándar y extendida***)[37]

CAR proporciona acciones configurables como envío, descarte o establecimiento de precedencia cuando el tráfico cumple o excede el límite de tasa.

Límites de tasa.

CAR propaga ráfagas. Este no hace arreglo o modelación de tráfico, y por tanto no almacena y no añade retardo. CAR es muy optimizado para correr sobre interfaces de alta velocidad como DS3, por ejemplo.

Los límites de tasa definen qué paquetes conforman o exceden la tasa definida basándose en los siguientes parámetros:

[36] ***MPLS***. Mecanismo de transporte que opera entre la capa de enlace de datos y la capa de red del modelo OSI
[37] La lista de acceso estándar se utiliza para especificar solamente una dirección origen; en cambio, la lista de acceso extendida especifica direcciones origen, destino, puertos TCP/UDP, protocolos, entre los más importantes

- Tasa promedio. Esta determina la tasa de transmisión promedio a largo plazo. El tráfico que corresponde a este tipo de tasa siempre se ajusta

- Tamaño de ráfaga normal. Determina como las ráfagas de tráfico grandes pueden estar antes de que algún tipo de tráfico supere el límite de tasa

- Tamaño de ráfaga en exceso. El tamaño de ráfaga en exceso Be (*Excess burst*) determina como las ráfagas de tráfico grandes pueden estar antes de que todo tráfico supere el límite de tasa. El tráfico que cae entre el tamaño de ráfaga normal y el tamaño de ráfaga excedido supera el límite de tasa con una probabilidad que aumenta de acuerdo a como aumenta el tamaño de ráfaga

El número máximo de fichas que una cubeta puede contener es determinado por el tamaño de ráfaga normal configurado por el *token bucket*.

Cuando el límite de tasa CAR es aplicado a un paquete, CAR borra de la cubeta fichas que son equivalentes en número al tamaño de byte del paquete. Si un paquete llega y el tamaño de byte del paquete es mayor que el número de fichas disponibles en el *token bucket* estándar, la capacidad de ráfaga extendida está comprometida si esta es configurada.

La ráfaga extendida es configurada mediante el establecimiento del valor de ráfaga extendida mayor que el valor de ráfaga normal. Establecer el valor de ráfaga extendida igual al valor de ráfaga normal excluye la capacidad de ráfaga extendida. Si la ráfaga extendida no es configurada, dado el escenario de ejemplo, la acción excedida de CAR toma efecto porque un número suficiente de fichas no están disponibles.

Cuando la ráfaga extendida es configurada y este escenario ocurre, el flujo está autorizado en tomar prestado las fichas necesarias para permitir al paquete ser enviado. Esta capacidad existe a fin de evitar el comportamiento de *descarte de la cola*, y, en cambio, realizar el funcionamiento como el de la detección temprana aleatoria RED.

El trabajo de la capacidad de ráfaga extendida consiste en que si un paquete llega y necesita tomar prestado n número de fichas porque el *token bucket* contiene menos fichas que su tamaño de paquete requiere, entonces CAR compara los dos siguientes valores:

- El valor del parámetro de ráfaga extendida

- El resto compuesto, que es calculado como la suma sobre todas las *ai*:

- *a* indica el valor actual del resto del flujo después de que el paquete *i* es enviado. El resto actual es simplemente una cuenta de cuantas fichas el flujo actualmente ha tomado prestado

- *i* indica el i-ésimo paquete que intenta tomar prestado fichas desde la última vez que un paquete fue descartado

Si el resto compuesto es mayor que el valor de ráfaga extendida, la acción excedida de CAR toma efecto. Después que un paquete es descartado, el resto compuesto es efectivamente marcado a 0. CAR calculará un nuevo valor de resto compuesto igual al resto actual para el siguiente paquete que necesita tomar prestado fichas.

Si el resto actual es mayor que el límite extendido, todos los paquetes serán descartados hasta que el resto actual esté reducido mediante la acumulación de fichas en el *token bucket.*

La comprobación de tráfico TCP recomienda que el valor de ráfaga normal y extendido escogidos debería estar en el orden de varios segundos del valor del tráfico en la tasa promedio configurada, esto es, si la tasa promedio es 10 Mbps, entonces un tamaño de ráfaga normal de 10 a 20 Mbps y un tamaño de ráfaga en exceso de 20 a 40 Mbps serían apropiados.

Como recomendación para los valores de los parámetros de ráfaga normal y extendida, se toma lo siguiente:

$$ráfaga\_normal = tasa\_configurada * (1byte)/(8bits) * 1.5segundos$$

$$ráfaga\_extendida = 2 * ráfaga\_normal$$

A continuación se muestra un ejemplo del resto actual y compuesto[38]. ‘’Se asumen los siguientes parámetros para el ejemplo:

[38] Ejemplo tomado de Internetworking Technology Handbook - Quality of Service (QoS) - Cisco Systems, http://www.cisco.com/en/US/docs/internetworking/technology/handbook/QoS.html, Publicación 2007, Consultado en Agosto 2009

- Tasa de fichas es 1 unidad de datos por unidad de tiempo
- Tamaño de ráfaga normal es 2 unidades de datos
- Tamaño de ráfaga extendida es 4 unidades de datos
- 2 unidades de datos llegan por unidad de tiempo

Después de 2 unidades de tiempo, la cadena ha utilizado su ráfaga normal y debe comenzar a tomar prestado 1 unidad de datos por unidad de tiempo, la unidad de tiempo 3 comienza:

Tabla. 4.1. Ejemplo resto actual y compuesto, proceso 1

TIEMPO	UD LLEGADAS	RESTO ACTUAL	RESTO COMPUESTO
1	2	0	0
2	2	0	0
3	2	1	1
4	2	2	3
5	2	3 (temporal)	6 (temporal)

En este tiempo un paquete es descartado porque el nuevo resto compuesto (6) excedería al límite de ráfaga extendida (4). Cuando el paquete es descartado, el resto compuesto efectivamente se convierte a 0, y el resto actual está en 2. Los valores de 3 y 6 son temporales y no permanecen válidos en el caso donde un paquete es descartado. El valor final para la unidad de tiempo 5 sigue. La cadena comienza a tomar prestado otra vez en la unidad de tiempo 6.

Tabla. 4.2. Ejemplo resto actual y compuesto, proceso 2

TIEMPO	UD LLEGADAS	RESTO ACTUAL	RESTO COMPUESTO
5	2	2	0
6	2	3	3
7	2	4 (temporal)	7 (temporal)

En la unidad de tiempo 6, otro paquete es descartado y los valores de resto son ajustados correspondientemente’’.

Tabla. 4.3. Ejemplo resto actual y compuesto, proceso 3

TIEMPO	UD LLEGADAS	RESTO ACTUAL	RESTO COMPUESTO
7	2	3	0

Acciones ajustadas y excedidas.

CAR utiliza un *token bucket*, en consecuencia CAR puede pasar temporalmente ráfagas que excedan el límite de tasa siempre y cuando las fichas estén disponibles. Una vez que un paquete ha sido clasificado como conforme o superior a un límite de tasa particular, el enrutador realiza una de las siguientes acciones en el paquete:

- Transmitir. El paquete es enviado
- Descartar. El paquete es descartado
- Establecer precedencia y transmitir. Los bits de precedencia IP (ToS) en la cabecera del paquete son reescritos. Luego el paquete es enviado
- Continuar. El paquete es evaluado usando la siguiente política de tasa en una cadena de límites de tasa. Si no existe otra política de tasa, el paquete es enviado
- Establecer precedencia y continuar. Coloca los bits de precedencia IP a un valor específico y después evalúa la siguiente política de tasa en una cadena de límites de tasa

Políticas de tasa múltiple.

Una política de tasa CAR simple incluye información sobre el límite de tasa, acciones cumplidas y acciones excedidas. Cada interfaz puede tener múltiples políticas de tasa CAR correspondiendo a diferentes tipos de tráfico. Por ejemplo, la prioridad baja de tráfico puede ser limitada a una tasa más baja que la prioridad alta de tráfico. Cuando existen múltiples políticas de tasa, el enrutador examina cada política en el orden ingresado hasta que el paquete coincida. Si la correspondencia no es encontrada, la acción por defecto es enviar el paquete.

Las políticas de tasa pueden ser independientes: cada política de tasa negocia con un diferente tipo de tráfico. Alternativamente, las políticas de tasa pueden estar en cascada: un paquete puede ser comparado a múltiples políticas de tasa diferentes en sucesión.

La cascada de políticas de tasa permite una serie de límites de tasa a ser aplicados a los paquetes para especificar más políticas granulares o para emparejar los paquetes contra una secuencia ordenada de políticas hasta que un límite de tasa aplicable se encuentre.

4.2.3. Políticas de tráfico

Características.

Las políticas de tráfico permiten controlar la tasa máxima de tráfico enviada o recibida sobre una interfaz, y dividir una red de comunicación en múltiples niveles de prioridad o clases de servicio CoS.

La característica de la política de tráfico maneja la tasa máxima de tráfico a través del algoritmo *token bucket*. Este algoritmo puede usar los valores de usuarios configurados para determinar la tasa máxima de tráfico permitida sobre una interfaz en un momento dado en el tiempo. El algoritmo es influido por todo el tráfico entrante o saliente y es útil en administración de ancho de banda de la red en casos donde varios paquetes grandes son enviados en la misma cadena de tráfico.

El algoritmo *token bucket* proporciona usuarios con tres acciones para cada paquete: una acción conforme, una acción excedida y una acción violada opcional. El tráfico entrante de la interfaz con políticas de tráfico configuradas es ubicado en una de las tres categorías. Dentro de estas tres categorías, los usuarios pueden decidir el tratamiento del paquete. Por ejemplo, los paquetes conformes pueden ser configurados para ser transmitidos, los paquetes excedidos pueden ser configurados para ser enviados con una prioridad disminuida y los paquetes violados pueden ser configurados para ser descartados.

Con frecuencia la política de tráfico es configurada sobre interfaces en el borde de la red de comunicación para limitar la tasa de tráfico entrante o saliente de la red. En las configuraciones más comunes de la política de tráfico, el tráfico conforme es transmitido y el tráfico excedido es enviado con prioridad disminuida o es descartado. Cada usuario

puede cambiar estas opciones de configuración para adaptarse a las necesidades de cada red.

Beneficios.

- Administración del ancho de banda a través de la limitación de tasa. Como se mencionó anteriormente, las políticas de tráfico permiten controlar la tasa máxima de tráfico enviado y recibido sobre una interfaz, además de que a menudo son configuradas sobre interfaces en el borde de una red, con el fin de limitar el tráfico de entrada y salida de la red. El tráfico que cae dentro de los parámetros es enviado, mientras que el tráfico que excede los parámetros es descartado o enviado con prioridad disminuida

- Marcación de paquetes a través de precedencia IP, grupo QoS y estableciendo el valor DSCP. La marcación de paquetes permite dividir la red en múltiples niveles o clases de servicio CoS, como las siguientes:

- Se usa las políticas de tráfico para establecer la precedencia IP o los valores DSCP para paquetes entrantes de la red. Por tanto, los dispositivos de red pueden usar los valores ajustados de precedencia IP para determinar cómo el tráfico debería ser tratado

- Se utiliza las políticas de tráfico para asignar paquetes a un grupo QoS. El enrutador usa el grupo QoS para determinar cómo priorizar los paquetes

4.2.4. Modelación de tráfico

Definición.

La modelación de tráfico permite controlar el tráfico saliente de una interfaz con el fin de enlazar su tráfico a la velocidad de la interfaz remota de destino y asegurar que el tráfico sea conforme para políticas contratadas por este. En consecuencia, la adhesión de tráfico a un perfil particular puede ser modelado para cumplir requerimientos de bajada de información, de este modo eliminar cuellos de botella en topologías con desajustes de tasa de datos.

Las principales razones por la que se debería usar modelación de tráfico son para controlar el acceso al ancho de banda disponible, para asegurar que el tráfico sea conforme

a las políticas establecidas por este, y para regular el flujo de tráfico a fin de evitar congestión que puede ocurrir cuando el envío de tráfico excede la velocidad de acceso de su interfaz remota de destino.

A continuación algunos ejemplos en los que se debería usar modelación de tráfico:

- Controlar el acceso al ancho de banda cuando, por ejemplo, la política dicta que la tasa de una interfaz dada no debería exceder el promedio de cierta tasa aún cuando la tasa de entrada exceda la velocidad

- Configurar modelación de tráfico sobre una interfaz si se tiene una red con diferentes tasas de entrada, lo cual podría ocasionar fallas sobre la aplicación usada en el enlace. Un caso similar más complicado sería una red de capa de enlace, dando indicaciones de congestión, que tiene diferentes tasas de entrada en distintos ***DTEs***[39] adjuntos; la red puede ser capaz de entregar más velocidad de tránsito a un dispositivo DTE dado, al mismo tiempo que otro

- Si se ofrece un servicio de sub-tasa. En este caso, la modelación de tráfico permite usar el enrutador para dividir sus enlaces T1 o T3 en canales más pequeños

La modelación de tráfico previene la pérdida de paquetes, esto es muy importante ya que la pérdida de paquetes puede resultar en consecuencias perjudiciales para aplicaciones en tiempo real o aplicaciones interactivas.

La modelación de tráfico arregla tráfico por almacenamiento del mismo por encima de la tasa configurada en una cola. Cuando un paquete llega en la interfaz para la transmisión, la siguiente secuencia sucede:

1. Si la cola está vacía, el paquete arribado es procesado por el modelador de tráfico

- Si es posible, el modelador de tráfico envía el paquete

- Caso contrario, el paquete es ubicado en la cola

2. Si la cola no está vacía, el paquete es ubicado en la cola

[39] ***DTE***. Equipo terminal de datos, es el equipo donde los datos tienen origen y destino

Cuando los paquetes están en la cola, el modelador de tráfico borra el número de paquetes que puede enviar desde la cola en todo el intervalo de tiempo.

Modelación de tráfico genérico.

La modelación de tráfico genérico GTS (*Generic Traffic Shaping*) forma tráfico mediante la reducción del flujo de tráfico de salida para evitar congestión limitando tráfico a una tasa de bit particular usando el mecanismo de *token bucket*.

GTS se aplica en función de cada interfaz y puede usar listas de acceso para seleccionar el tráfico a modelar. Este procedimiento puede trabajar sobre una variedad de tecnologías de capa 2, según el modelo de referencia OSI.

GTS es compatible con la mayoría de los medios físicos de comunicación y los tipos de encapsulación en el enrutador. Adicional a esto, también puede ser aplicado a una lista de acceso específica en una interfaz.

A continuación se muestra la figura. 4.1., en la cual se puede observar el funcionamiento de este tipo de modelación de tráfico.

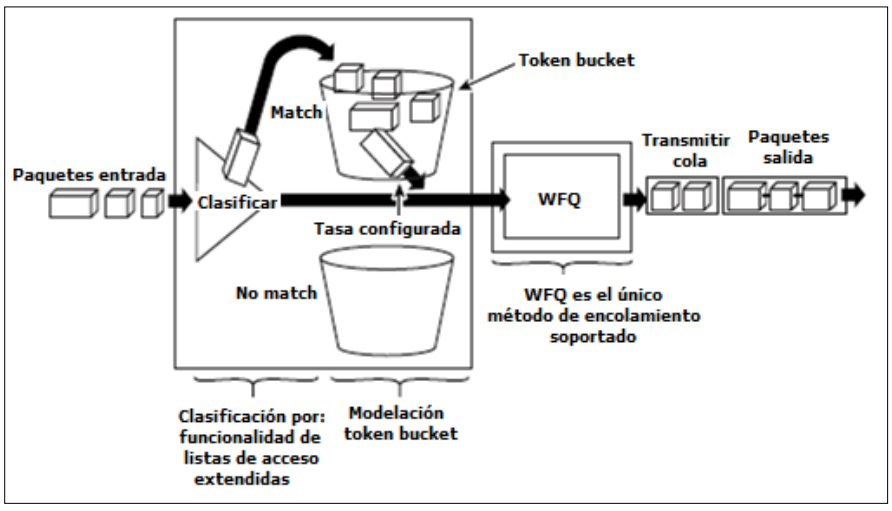


Figura. 4.1. Funcionamiento de la modelación de tráfico genérico[40]

Modelación basada en clase.

La modelación basada en clase puede ser habilitada en cualquier interfaz que soporte GTS. Utilizando estas características de modelación, se puede realizar lo siguiente:

[40] *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2, Cisco Systems Inc, United States of America 2006, Consultado en Septiembre 2009, página QC-219

- Configurar GTS en una clase de tráfico. GTS proporciona una mayor flexibilidad a las clases para la configuración de la modelación de tráfico. Previamente, esta habilidad fue limitada con el uso de ACLs

- Especificar la tasa promedio o tasa pico de la modelación de tráfico. La especificación de la tasa pico de modelación permite realizar un mejor uso del ancho de banda, autorizando más información que el CIR a ser enviado si el ancho de banda está disponible

- Configurar CBWFQ dentro de GTS. CBWFQ permite especificar la cantidad exacta de ancho de banda que se asigne para una clase específica de tráfico. Teniendo en cuenta el ancho de banda disponible en la interfaz, se puede configurar hasta 64 clases y controlar la distribución entre ellas, lo cual no es el caso con WFQ basado en flujo. WFQ basado en flujo aplica pesos al tráfico para clasificarlo dentro de conversaciones y determinar la cantidad de ancho de banda en cada conversación está permitido relativo a otras conversaciones. Estos pesos y la clasificación de tráfico, son dependientes y limitados a los siete niveles de precedencia IP. CBWFQ permite definir lo que constituye una clase basado en criterios que exceden a los límites del flujo. Esta técnica permite utilizar ACLs y protocolos o nombres de interfaces de entrada para definir como el tráfico debería ser clasificado, proporcionando de esta manera una gran granularidad. No se necesita mantener clasificación de tráfico en un flujo base; por otra parte, se puede configurar hasta 64 clases discretas en una política de servicio.

Modelación distribuida de tráfico.

La modelación distribuida de tráfico DTS (*Distributed Traffic Shaping*) provee un método de gestión del ancho de banda de una interfaz para evitar congestión, satisfacer necesidades del sitio remoto y ajustar a una tasa de servicio que es proporcionada en una interfaz.

DTS utiliza colas para almacenar aumentos repentinos de tráfico que pueden congestionar una red y enviar la información dentro de la red en una tasa regulada. Esto asegura que el tráfico se comportará en el descriptor de configuración, según la definición de CIR, Bc y Be. Con la tasa de bit promedio definida y el tamaño de ráfaga que es aceptable en la entidad formada, se puede obtener un valor de intervalo de tiempo.

4.3. DETECCIÓN TEMPRANA ALEATORIA

4.3.1. Definición

La detección temprana aleatoria RED (*Random Early Detection*) es un mecanismo propuesto por *Sally Floyd* y *Van Jacobson* a principios de los 90s para direccionar la congestión de red en una respuesta más bien de manera reactiva. Lo fundamental en este mecanismo es la premisa que la mayor parte de tráfico se ejecuta sobre las implementaciones de transporte de datos que son sensibles a la pérdida y temporalmente se retardaría cuando algo de su tráfico sea descartado. TCP, el cual responde apropiadamente, incluso con firmeza, al descarte de tráfico mediante el retardo de su transmisión de tráfico, efectivamente permite el comportamiento de descarte de tráfico de RED para trabajar como un mecanismo de señalización de prevención de congestión.

Al considerar la utilidad de RED cuando transportes robustos como TCP son generalizados, es importante considerar seriamente las implicaciones negativas de emplear RED cuando un porcentaje significante de tráfico no es robusto en respuesta a la pérdida de paquetes.

En definitiva, RED es un mecanismo que previene situaciones de congestión mediante el tratamiento de comunicaciones de red cuando el enlace comienza a presentar signos tempranos de saturación. En consecuencia, con RED habilitado, un enlace nunca debería alcanzar el punto de congestión porque este mecanismo limitará el flujo de paquetes antes que esto suceda. Esto también tiene como efecto la normalización del ancho de banda usado en un enlace y mantenerlo en la capacidad pico.

4.3.2. Funcionamiento

RED trabaja por descarte aleatorio de paquetes de diferentes conversaciones. Utiliza ventana deslizante de TCP/IP y mecanismos de recuperación rápida para forzar la comunicación a reducir la velocidad en la cual se están transmitiendo paquetes, en consecuencia reduce el uso de ancho de banda de esa conversación particular. Mediante la aplicación de este principio aleatorio a varias comunicaciones en marcha, RED puede retrasar las cosas ya que detecta que un enlace se aproxima a un estado de congestión. RED no es apropiado en situaciones donde el tráfico UDP es predominante, esto porque RED no tiene efectos apreciables sobre este.

Con el fin de comprender como opera RED, es importante entender el mecanismo fundamental que RED utiliza para reducir las comunicaciones. La figura. 4.2., muestra el mecanismo de ventana deslizante de TCP.

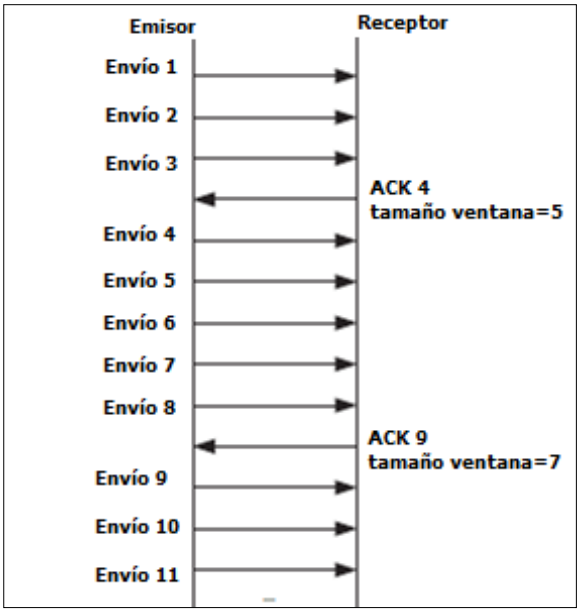


Figura. 4.2. Ventana deslizante de TCP[41]

A medida que el remitente envía trenes de paquetes, el receptor reconoce el último paquete del tren e informa que la transmisión fue satisfactoria. Además, instruye al remitente que puede aumentar el número de paquetes por tren o tamaño de ventana, en su siguiente transmisión. En la figura. 4.2., el tamaño de la ventana de la transmisión aumenta de 3 a 5 a 7 paquetes. Si no se controla, las sesiones TCP incrementarán su tamaño de ventana hasta que un paquete es descartado y un NAK es enviado por el receptor, o hasta que una salida de secuencia ACK es recibida por el remitente. En este punto, TCP recupera en la última secuencia ACK satisfactoria y reduce el tamaño de ventana en un intento de lograr una comunicación exitosa.

Cuando múltiples sesiones TCP operan sobre un enlace común, todas aumentarán el tamaño de sus ventanas deslizantes tanto como las ACKs satisfactorias son recibidas. Gradualmente esta progresión sincronizada consume el ancho de banda del enlace hasta que el enlace este congestionado. En este punto, todas las conversaciones TCP experimentan un error de transmisión, resultando un descarte considerable en el uso de

[41] Durand, Benoit; Sommerville, Jerry; Buchmann, Mark; Fuller, Ron, *Administering CISCO QoS in IP Networks*, Syngress Media Inc, United States of America Marzo 2001, página 233

ancho de banda tal como todas las conexiones TCP se mueven a tamaños de ventana deslizante más pequeños simultáneamente. Este proceso es llamado *sincronización global*, y crea problemas sobre el enlace debido al hecho que todas las corrientes de entonces comenzarán a retroceder simultáneamente, guiando a otra situación de congestión. Este ciclo continúa una y otra vez, creando picos y valles de utilización de ancho de banda en el enlace.

RED trata de prevenir esta fluctuación en ancho de banda mediante el descarte aleatorio de paquetes de varias conexiones mientras el enlace se aproxima a un estado de congestión. Por lo tanto, las ventanas de las conexiones TCP se reducen una por una tal como el algoritmo aleatorio de RED desecha paquetes desde sus conexiones. Esto resulta en una normalización de tráfico de red cerca al punto de congestión del enlace, en lugar de tener retornos masivos tal como todas las conexiones TCP descartan paquetes cuando alcanzan el punto de congestión de la conexión. La figura. 4.3., muestra el efecto de RED en un tamaño de ventana deslizante TCP cuando descarta un paquete al azar de esa conexión. En este ejemplo, cuando RED descarta el paquete 7, el siguiente paquete recibido por el receptor es el paquete 8, el mismo que está fuera de secuencia. El receptor envía de regreso un segundo ACK por el último tren paquete válido recibido y reduce el tamaño de la ventana deslizante a usar por el remitente.

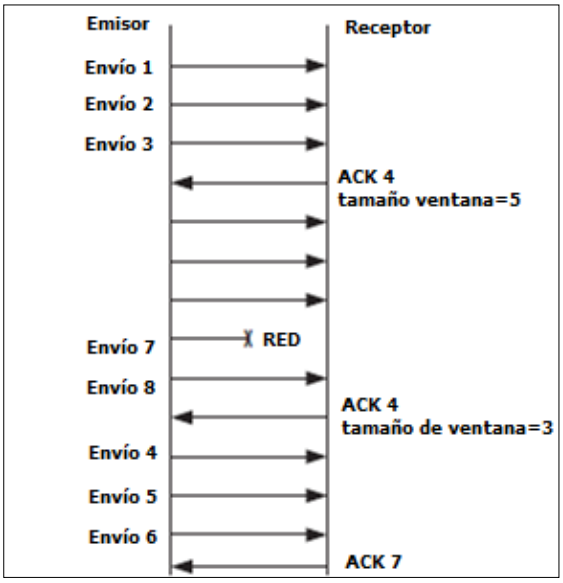


Figura. 4.3. El efecto de RED en un tamaño de ventana deslizante TCP[42]

[42] Durand, Benoit; Sommerville, Jerry; Buchmann, Mark; Fuller, Ron, *Administering CISCO QoS in IP Networks*, Syngress Media Inc, United States of America Marzo 2001, página 234

4.3.3. Probabilidad de descarte de paquete

La probabilidad de descarte de paquete está basada en el umbral mínimo, en el umbral máximo y en el denominador de probabilidad de marca.

Cuando la profundidad de cola promedio está por encima del mínimo umbral, RED comienza con el descarte de paquetes. La tasa de descarte de paquete aumenta linealmente de acuerdo a cómo el tamaño de cola promedio aumenta hasta que alcance el máximo umbral.

El denominador de probabilidad de marca es la fracción de paquetes descartados cuando la profundidad de cola promedio está en el máximo umbral. Por ejemplo, si el denominador es 256, uno de cada 256 paquetes es descartado cuando la cola promedio está en el máximo umbral.

Cuando el tamaño de cola promedio está por encima del máximo umbral, todos los paquetes son descartados. La figura. 4.4., resume la probabilidad de descarte de paquete.

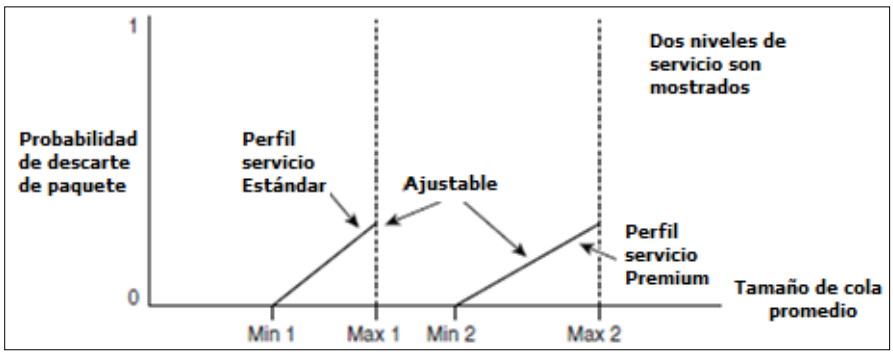


Figura. 4.4. Probabilidad de descarte de paquete RED[43]

El valor mínimo de umbral debería ser establecido lo suficientemente alto como para maximizar la utilización de la conexión. Si el mínimo umbral es demasiado bajo, los paquetes podrían ser descartados innecesariamente, y la conexión de transmisión no sería utilizada totalmente.

La diferencia entre el umbral máximo y el mínimo debería ser lo suficientemente grande como para evitar la *sincronización global* de los *hosts* TCP. Si la diferencia entre

[43] *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2, Cisco Systems Inc, United States of America 2006, Consultado en Septiembre 2009, página QC-177

ellos es demasiado pequeña, muchos paquetes serían descartados a la vez, dando lugar a la *sincronización global*.

4.3.4. Necesidad sobre una red de comunicación

RED es útil en conexiones donde la congestión de tráfico TCP/IP es esperada. No utiliza clasificación de tráfico o priorización en relación los descartes aleatorios, sino más bien indiscriminadamente descarta paquetes cuando detecta inminente congestión de la conexión. El beneficio de RED es que la utilización de la conexión se normalizará cerca de su capacidad máxima. Sin RED, la utilización promedio en realidad será menor, con el uso real fluctuante tal como las conexiones alcanzan el punto de congestión y luego todas las sesiones TCP retornan simultáneamente.

Esta distribución razonable de descartes no toma en cuenta otros factores como una precedencia IP de paquete. Como con la técnica de encolamiento equitativo, RED puede hacer uso de un mecanismo que toma en cuenta la precedencia IP de un paquete. Por lo tanto, fijaría descartes menos aleatorios proporcionando menos descartes para paquetes con precedencia alta. Este proceso es conocido como WRED el cual será analizado a continuación.

4.4. DETECCIÓN TEMPRANA ALEATORIA PONDERADA

4.4.1. Definición

La detección temprana aleatoria ponderada WRED (*Weighted Random Early Detection*) combina las capacidades del algoritmo RED con la característica de la precedencia IP de proporcionar un tratamiento preferencial para el tráfico que incluye paquetes de mayor prioridad. Selectivamente, WRED puede descartar tráfico de prioridad más baja cuando la interfaz comienza a estar congestionada y proveer características de funcionamiento diferenciado para diferentes clases de servicio.

Para interfaces configuradas para utilizar RSVP, WRED escoge paquetes de otros flujos para descartar en lugar de los flujos con RSVP. Además, la precedencia IP domina cuáles paquetes son descartados, el tráfico que está con una precedencia baja tiene una tasa de descarte mayor y por lo tanto es más probable que se reduzca.

WRED difiere de otras técnicas de prevención de congestión como las estrategias de encolamiento porque procura anticipar y evitar la congestión además de controlar la congestión una vez que esta se produzca.

4.4.2. Beneficios

WRED efectúa detección temprana de congestión y suministra para múltiples clases de tráfico. También protege contra la *sincronización global*. Por estas razones, WRED es útil en cualquier interfaz de salida donde se espera que ocurra saturación.

Sin embargo, por lo general WRED es utilizado en los enrutadores de núcleo de una red en lugar de los enrutadores de borde sobre esta. Los enrutadores de borde asignan precedencias IP a los paquetes mientras van ingresando a la red de comunicación. WRED utiliza estas precedencias para determinar los diferentes tipos de tráfico.

WRED establece los umbrales por separado y pondera las diferentes precedencias IP, permitiendo proporcionar diferentes calidades de servicio en lo que respecta al descarte de paquetes para diferentes tipos de tráfico. El tráfico estándar puede ser descartado más frecuentemente que otra clase de tráfico durante los períodos de congestión.

4.4.3. Funcionamiento

Al descartar paquetes aleatoriamente antes de los períodos de congestión, WRED anuncia al origen de paquetes para disminuir su velocidad de transmisión. Si el origen de paquete está utilizando TCP, disminuye su velocidad de transmisión hasta que todos los paquetes alcanzan su destino, lo cual indica que la congestión está clareada.

Generalmente WRED descarta paquetes basado en la precedencia IP. Los paquetes con una precedencia IP mayor son menos probables para ser descartados que los paquetes con una precedencia menor. En consecuencia, si mayor es la prioridad de un paquete, mayor es la probabilidad de que el paquete será entregado.

WRED reduce las posibilidades de descarte de cola de forma selectiva descartando paquetes cuando la interfaz de salida empieza a mostrar signos de congestión. Al descartar paquetes tempranamente en lugar de esperar hasta que la cola se llene, WRED permite descartar números largos de paquetes a la vez y minimizar las posibilidades de la

sincronización global. Por lo tanto, WRED permite a la línea de transmisión ser usada completamente en todo tiempo.

Adicionalmente, estadísticamente WRED descarta más paquetes de los grandes usuarios que de los pequeños. Por lo tanto, los orígenes de tráfico que generan el mayor tráfico son más probables a ser retardados que los orígenes de tráfico que generan tráfico pequeño.

WRED evita los problemas de globalización que ocurren cuando el *descarte de la cola* es utilizado como mecanismo de prevención de congestión. La *sincronización global* se manifiesta cuando múltiples hosts TCP reducen sus velocidades de transmisión en respuesta al descarte de paquetes, entonces aumenta sus velocidades de transmisión una vez más cuando la congestión es reducida.

WRED solo es útil cuando la mayoría de tráfico es tráfico TCP/IP. Con TCP, paquetes descartados indican congestión, por lo que el origen de paquete reducirá sus velocidades de transmisión. Con otros protocolos, los orígenes de paquete pueden no responder o pueden reenviar paquetes descartados en la misma tasa. En consecuencia, el descarte de paquetes no disminuye la congestión.

WRED trata al tráfico no IP como precedencia 0, la más baja precedencia. Por tanto, el tráfico no IP, en general, es más probable a ser descartado que el tráfico IP. La figura. 4.5., ilustra como WRED trabaja.

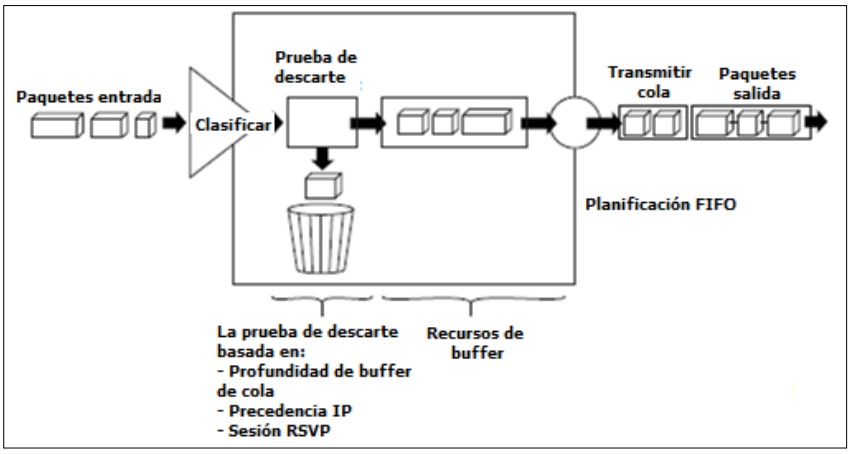


Figura. 4.5. Detección temprana aleatoria ponderada WRED[44]

[44] *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2, Cisco Systems Inc, United States of America 2006, Consultado en Septiembre 2009, página QC-180

4.4.4. Promedio de tamaño de cola

Automáticamente el enrutador determina los parámetros a utilizar en los cálculos de WRED. El tamaño de cola promedio está basado en el promedio anterior y en el tamaño actual de la cola. La fórmula es la siguiente:

$$promedio = \left(promedio\_anterior * \left(1 - 2^{-n}\right)\right) + \left(tamaño\_cola\_actual * 2^{-n}\right)$$

Donde *n* es el factor ponderado exponencial, un valor configurable por el usuario.

Para valores altos de *n*, el promedio anterior se hace más importante. Un factor grande suaviza los picos y baja en longitud la cola. El tamaño de cola promedio es improbable cambiar muy rápidamente, evitando cambios drásticos en el tamaño. El proceso WRED será lento al arrancar el descarte de paquetes, pero puede continuar descartando paquetes por un tiempo después de que el tamaño de cola actual haya caído por debajo del umbral.

Para valores bajos de *n*, el tamaño de cola promedio sigue de cerca al tamaño actual de cola. El promedio resultante puede fluctuar con cambios en los niveles de tráfico. En este caso, el proceso WRED responde rápidamente a colas largas. Una vez que la cola caiga por debajo del umbral mínimo, el proceso parará el descarte de paquetes. Si el valor de *n* es muy bajo, WRED reaccionará a ráfagas de tráfico temporal y descartará el tráfico innecesario.

4.5. DETECCIÓN TEMPRANA ALEATORIA PONDERADA DISTRIBUIDA

4.5.1. Definición

La detección temprana aleatoria ponderada distribuida DWRED (*Distributed Weighted Random Early Detection*) es una implementación de WRED para el procesador de interfaz versátil VIP. DWRED proporciona un grupo completo de funciones para el VIP.

Se puede configurar DWRED y DWFQ sobre la misma interfaz, pero no se puede configurar DWRED sobre una interfaz en la cual está configurado CQ basado en RSVP, PQ o WFQ.

4.5.2. Funcionamiento

Cuando el paquete arriba y está habilitado DWRED, los siguientes eventos ocurren:

- El tamaño de cola promedio es calculado
- Si el promedio es menos que el umbral de cola mínimo, los paquetes que llegaron son encolados
- Si el promedio está entre el umbral de cola mínimo y el umbral de cola máximo, el paquete es descartado o encolado, esto depende de la probabilidad de descarte de paquete
- Si el tamaño de cola promedio es más que el umbral de cola máximo, el paquete es automáticamente descartado

4.5.5. Beneficios

DWRED proporciona un rendimiento más rápido que WRED basado en RSVP. Se debería correr DWRED sobre VIP si se quiere alcanzar velocidades muy altas como la tasa de de 155 Mbps de OC-3, por ejemplo.

Cuando WRED o DWRED no están configurados, el descarte de cola es promulgado durante los períodos de congestión. Habilitando DWRED se evita los problemas de *sincronización global* que resultan cuando el *descarte de la cola* es utilizado para evitar la congestión.

Las características de DWRED proveen el beneficio de los flujos de tráfico consistentes. Cuando RED no está configurado, los *buffers* de salida se ocupan durante los períodos de congestión. Cuando estos están llenos, el *descarte de la cola* ocurre; todos los paquetes adicionales son descartados. Por el motivo de que los paquetes son descartados todos a la vez, la *sincronización global* de hosts TCP puede ocurrir como múltiples hosts TCP pueden reducir sus velocidades de transmisión. La congestión se elimina y los hosts TCP incrementan sus velocidades de transmisión, resultando en ondas de congestión seguidas por períodos cuando la conexión de transmisión no está completamente usada.

4.6. DETECCIÓN TEMPRANA ALEATORIA PONDERADA BASADA EN FLUJO

4.6.1. Definición

La detección temprana aleatoria ponderada basada en flujo FBWRED (*Flow – Based Weighted Random Early Detection*) es una característica que obliga a WRED permitir la mayor equidad a todos los flujos sobre una interfaz con respecto a cómo los paquetes son descartados.

4.6.2. Beneficios

Antes de considerar las ventajas que el uso de FBWRED ofrece, esto ayuda a pensar acerca de cómo WRED, sin FBWRED configurado, afecta diferentes tipos de flujos de paquetes. Incluso antes de que FBWRED clasifique flujos de paquetes, los flujos pueden ser considerados como pertenecientes a una de las siguientes categorías:

- Flujos no adaptativos, los cuales son flujos que no responden a la congestión
- Flujos robustos, los cuales en promedio tienen una tasa de datos uniforme y se retardan en respuesta a la congestión
- Flujos frágiles, los cuales, aunque conscientes de la congestión, tienen menos paquetes almacenados en una puerta de enlace que los flujos robustos

WRED tiende hacia el prejuicio en contra de los flujos frágiles porque todos los flujos, incluso aquellos con un número relativamente menor de paquetes en la cola de salida, son susceptibles al descarte de paquetes durante períodos de congestión. Aunque los flujos frágiles tienen menos paquetes almacenados, estos son descartados en la misma tasa como los paquetes de otros flujos.

Para proporcionar equidad a todos los flujos, FBWRED tiene las siguientes características:

- Asegura que los flujos que responden a los descartes de paquete WRED, son protegidos de los flujos que no responden a los descartes de paquete WRED
- Prohíbe un flujo simple de monopolización de recursos de almacenamiento en una interfaz

4.6.3. Funcionamiento

FBWRED depende de los siguientes dos enfoques principales para remediar el problema de descarte de paquete no permitido:

- Clasifica el tráfico de entrada dentro de flujos basado en parámetros como direcciones y puertos de origen y destino

- Mantiene el estado sobre los flujos activos, los cuales son flujos que tienen paquetes en las colas de salida

FBWRED utiliza esta clasificación e información de estado para asegurar que cada flujo no consuma más que su parte permitida de los recursos de almacenamiento de salida. FBWRED determina que flujos monopolizan recursos y penalizan en mayor medida estos flujos.

Para asegurar la equidad entre los flujos, FBWRED mantiene una cuenta del número de flujos activos que existen a través de una interfaz de salida. Dado el número de flujos activos y el tamaño de cola de salida, FBWRED determina el número de *buffers* disponibles por flujo.

Para que haya una cierta explosividad, FBWRED escala el número de *buffers* permitidos por flujo mediante un factor configurado y permite a cada flujo activo tener un cierto número de paquetes en la cola de salida. Este factor de escalamiento es común en todos los flujos. El resultado del número escalado de *buffers* se convierte en el límite por flujo. Cuando un flujo excede el límite por flujo, la probabilidad que un paquete de ese flujo será descartado, aumenta.

CAPÍTULO 5

CONSIDERACIONES DE DISEÑO PARA IMPLEMENTACIÓN DE CALIDAD DE SERVICIO

5.1. CARACTERÍSTICAS DE LOS SERVICIOS CONVERGENTES

A continuación se muestran algunas razones para implementar calidad de servicio sobre una topología de red de comunicación:

- Dar prioridad a ciertas aplicaciones de misión crítica dentro de la red
- Maximizar el uso de la inversión en infraestructura de la red actual
- Mejor rendimiento para aplicaciones sensibles al retardo como la voz y el video
- Responder a cambios en los flujos de tráfico en la red

El último enunciado puede parecer trivial. Nadie pudo haber previsto que la navegación Web despegaría como lo hizo, sin embargo, hoy, la mayoría del tráfico fluyendo a través del Internet portan el prefijo *'http'*. Con el fin de adaptar a estos cambios en los requerimientos de ancho de banda, QoS puede ser usado para asegurar que los usuarios escuchen cualquier tipo de tráfico sobre IP sin ahogar el tráfico de red vital para la compañía.

A menudo, en la práctica se determina que el método más simple para lograr un mejor desempeño en una red es lanzar más ancho de banda sobre el problema. En este tiempo de redes Gigabit Ethernet y ópticas, mayores capacidades están disponibles. De todos modos, más ancho de banda no siempre garantiza un cierto nivel de rendimiento. Es muy posible que muchos de los protocolos que producen la congestión en primer lugar, simplemente consuman el ancho de banda adicional; lo cual lleva a los mismos problemas de congestión experimentados antes de la actualización de ancho de banda. Un enfoque más prudente es analizar el tráfico que fluye por el cuello de botella, determinando de esta manera la importancia de cada protocolo y aplicación, y determinar una estrategia para priorizar el acceso al ancho de banda. QoS permite a los administradores de red tener el

control sobre el ancho de banda, la latencia y el *jitter*, y así, minimizar la pérdida de paquetes dentro de la red mediante la priorización de varios protocolos. El ancho de banda es la medida de la capacidad en una red o una conexión específica, la latencia es el retardo de un paquete viajando por la red y el *jitter* es el cambio de latencia sobre un período de tiempo determinado. Implementar ciertos procedimientos o técnicas de calidad de servicio puede controlar estos tres parámetros críticos dentro de las aplicaciones especiales.

Actualmente dentro de algunas redes corporativas, QoS no está ampliamente implementado. Pero con el fomento de aplicaciones como el *multicast*, multimedia *streaming* y voz sobre IP, la necesidad de ciertos niveles de calidad es mucho más inherente. Especialmente porque este tipo de aplicaciones son susceptibles al *jitter* y al retardo, y un rendimiento pobre es inmediatamente notificado por el usuario final.

Para esto se ha detallado a continuación una serie de características que deben ser tomadas en cuenta dentro del análisis y diseño de la implementación de mecanismos de calidad de servicio sobre la redes de comunicación por parte de los administradores de red.

Previamente a la aplicación de las características de cada servicio, de manera global se tiene que considerar aspectos muy importantes dentro de cada red de comunicación, siendo el comportamiento de esta muy diferente en el sentido de negocio de cada compañía, es por ello que se recomienda tomar los siguientes pasos al inicio de un diseño de calidad de servicio:

- Auditoría de red. Con el propósito de identificar cada tipo de tráfico sobre la red
- Auditoría del negocio. Dentro de la que se tiene que determinar cómo cada tipo de tráfico es importante para el negocio de la compañía
- Niveles de servicio requeridos. Para determinar el tiempo de respuesta requerido dentro de cada tipo de tráfico

5.1.1. Voz

Se entiende por voz sobre protocolo de Internet VoIP (*Voice over Internet Protocol*) la digitalización de la voz y su transmisión a través de la red siguiendo el protocolo de Internet, es decir, mediante la conmutación de paquetes en los que la información se transmite conmutada. La conmutación de paquetes se basa en que la información

transmitida, en este caso voz, se divide en paquetes y cada paquete se envía de forma independiente con la misma dirección de destino donde vuelve a reagruparse y, de esta forma, se recupera toda la información. Esto se diferencia notablemente de la telefonía tradicional o ***PSTN***[45] (*Public Switched Telephone Network*).

Cuando se va a utilizar VoIP hay que tener presente que los paquetes de datos de todas las aplicaciones van a compartir las mismas *'carreteras'* de datos. Por este motivo, se debe tener muy claro el ancho de banda necesario de cada aplicación y su respectiva prioridad, con el objetivo de que la red de comunicación cumpla con los requerimientos de cada tipo de aplicación, identificando el tráfico más crítico para el negocio de la organización para que la red pueda diferenciarlo y priorizarlo.

El tráfico de voz posee las siguientes características marcadas:

- Fluido y llano
- Benigno
- Sensible al descarte
- Sensible al retardo
- Prioridad UDP

Con respecto al ancho de banda dentro de esta aplicación, hay que tener presente el requerido en cada comunicación y el número de comunicaciones simultáneas necesitadas. ***Por citar un ejemplo***[46], ''en un entorno LAN, dentro del cual se utiliza tecnología *Switch* a 10 o 100 Mbps, se puede elegir una compresión G.711 con un ancho de banda de 87.2 Kbps ya que se obtiene mayor calidad y se dispone de suficiente ancho de banda; en cambio, en una ambiente WAN, donde el ancho de banda es escaso y costoso a la vez, se podría elegir la compresión G.723 con un ancho de banda de 21.9 Kbps''. En el Anexo A3 se encuentra detallada una tabla donde se pueden observar las diferentes características de los códec de voz a ser utilizados dentro de una implementación. El ancho de banda puede reducirse entre 30% y 40% cuando se utiliza la detección de silencios ***VAD***[47] (*Voice*

[45] ***PSTN***. Red de telefonía tradicional, la cual se diferencia de VoIP en que durante el tiempo que la comunicación está en ejecución, se produce una asignación permanente de circuitos que quedan exclusivamente dedicados para esta comunicación hasta que finaliza
[46] Ejemplo tomado de White Paper: QoS en Telefonía IP, NextiraOne, España
[47] ***VAD***. Es una técnica usada en el procesamiento del habla en la cual la presencia o ausencia del habla humano es detectado

Activity Detection). También en las líneas WAN, los enrutadores pueden utilizar la compresión de cabeceras IP cRTP para reducir las cabeceras de 40 a 24 bytes.

Para el caso de la pérdida de paquetes, los equipos de red como enrutadores o ***firewalls***[48], debido a la prioridad de flujo y a los picos de tráfico pueden perder paquetes de datos y producir retardos en la transmisión. Estos paquetes perdidos son retransmitidos y de este modo no se pierde información, no obstante mientras que en las aplicaciones de datos no suele tener impacto, si lo tiene en la VoIP. Por lo tanto, la pérdida de paquetes debe ser inferior o igual al 1%.

Para el retardo dentro de la VoIP, es decir, el tiempo de tránsito de los paquetes desde el origen al destino y vuelta, las personas son capaces de mantener una conversación cómodamente aunque existe cierto retardo, sin embargo llegado a un umbral puede empezar a ser incómodo para mantener una conversación, razón por la cual es recomendable tener un retardo menor o igual a 150 [ms].

Con referencia al *jitter*, no todos los paquetes sufren un retardo constante, este retardo variable o *jitter* disminuye la calidad de la voz al pasar de cierto umbral, para el caso de VoIP se necesita un *jitter* menor o igual a 30 [ms].

En definitiva, la figura. 5.1., muestra los niveles de calidad en los que se encuentran los parámetros críticos que afectan una determinada aplicación, en este caso la voz.

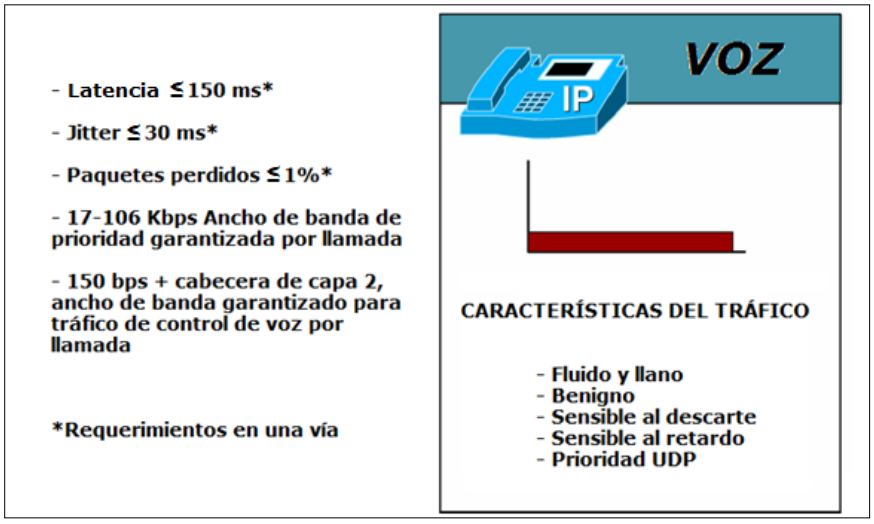


Figura. 5.1. Parámetros para la calidad de voz[49]

[48] ***Firewall***. Dispositivo de red de datos utilizado para brindar seguridad en la misma
[49] *Implementing Cisco Quality of Service,* Volumen 2, Version 2.2, Cisco Systems Inc, United States of America 2006, página 9-9

5.1.2. Video

La calidad de servicio de video sobre IP percibida por un usuario final es afectada principalmente por los parámetros de la red y por el tipo de codificación implementada. Resulta muy claro que el efecto de la pérdida de paquetes depende mucho del tipo de codificación usada; esto resulta crítico en aplicaciones de video de alta calidad en donde, con el objetivo de disminuir el ancho de banda consumido, se implementan codificaciones que hacen uso de cuadros predictivos (MPEG-1, MPEG-2, MPEG-4, obsérvese más información acerca de los códecs de video en el Anexo A4) cuya pérdida resulta en falta de información para decodificar los cuadros siguientes.

Otro de los factores que afectan la calidad percibida está directamente relacionado con la fuente de video, encontrando dentro de este conjunto la resolución del cuadro, la luminancia o niveles de gris, la profundidad del color o número de bits por pixel y la tasa de generación de cuadros. Cabe indicar que la sincronización entre el audio y el video también afecta sobre la percepción del usuario final en cuanto a calidad, y es un tema que hay que tomarlo en cuenta aunque técnicamente se conozca que no existe una relación directa entre ellos en lo que respecta al transporte, debido a que se transmiten por distintos canales y con distinta codificación.

La variación del retardo entre paquetes es otro factor que será expuesto más adelante que afecta a la calidad esperada.

Finalmente, un factor importante a considerar dentro de la calidad de servicio en el video es el aspecto temporal del video transmitido. Un video con poca variación espacial entre cuadros será más robusto frente a pérdidas y jitter en el sentido de que al usuario final le será más difícil notar la falta o retardo de la información.

Hay que tomar en cuenta las siguientes características influyentes sobre el tráfico de video en una red de comunicaciones:

- Tipo ráfaga
- Codicioso
- Sensible al descarte

- Sensible al retardo

- Prioridad UDP

En lo que corresponde a la pérdida de paquetes, se debe notar que es la principal causa de la degradación de la calidad. De acuerdo a la forma en que se codifica el video, la pérdida de un paquete en un cuadro puede afectar a los cuadros siguientes. Es importante acotar que no solo importa la media de paquetes perdidos, también importa la distribución de dichas pérdidas. ***Por ejemplo***[50] ‘’la distorsión total debido a dos pérdidas consecutivas es mayor que si las pérdidas fueran independientes’’.

También es determinante en la influencia de las pérdidas sobre la calidad de servicio el códec utilizado. En la figura. 5.2., se puede observar la diferencia entre la distorsión producida por la pérdida de paquetes para un mismo video, codificado en MPEG-1 y en MPEG-4. En ambos casos la pérdida de paquetes se traduce en una pérdida de macro bloques.

Se recomienda una pérdida de paquetes menor o igual al 1% para evitar estos problemas con la calidad del video.

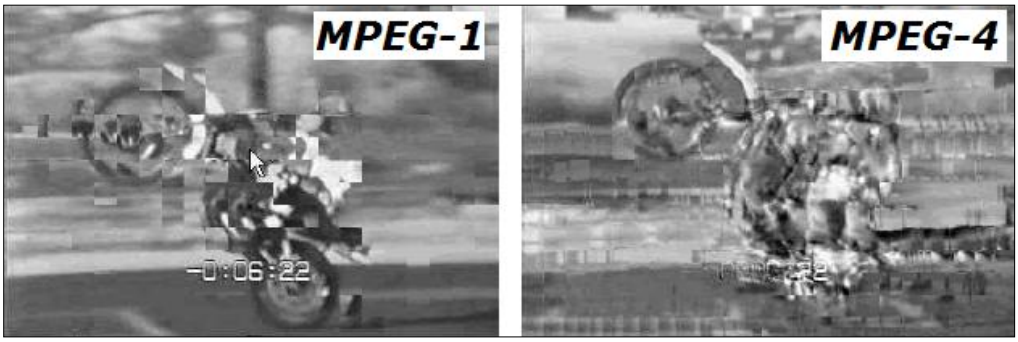


Figura. 5.2. Distorsión producida por pérdida de paquetes[51]

En lo que respecta al *jitter*, la variación del tiempo entre arribos hace que la decodificación no sea realizada en el momento correcto y, dependiendo de qué tan grande sea dicha variación, puede llegar a considerarse que el paquete se ha perdido. El usuario final observará la imagen del último cuadro decodificado congelada hasta la llegada del próximo cuadro. El cuadro retardado será reproducido en un tiempo menor al requerido,

[50] Ejemplo tomado de Casas, Pedro; Guerra, Diego; Irigaray, Ignacio, *Calidad de Servicio Percibida en Servicios de Voz y Video sobre IP*, Facultad de Ingeniería Universidad de la República, Uruguay Agosto 2005, página 24
[51] Casas, Pedro; Guerra, Diego; Irigaray, Ignacio, *Calidad de Servicio Percibida en Servicios de Voz y Video sobre IP*, Facultad de Ingeniería Universidad de la República, Uruguay Agosto 2005, página 25

con el fin de mantener el secuenciamiento temporal con el próximo cuadro. La figura. 5.3., muestra una gráfica de lo expuesto anteriormente con el efecto del jitter sobre el video.

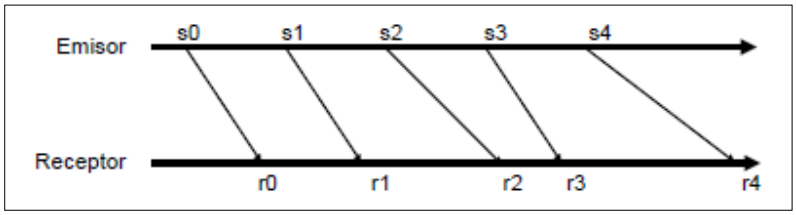


Figura. 5.3. Flujo con jitter[52]

Al convertirse en parámetros críticos sobre la aplicación de video, se recomiendo que el jitter se encuentre menor o igual a 30 [ms] y el que retardo sea menor o igual a 150 [ms].

La figura. 5.4., muestra un resumen de los puntos clave a considerar sobre las características de aplicaciones de video sobre una red de comunicación.

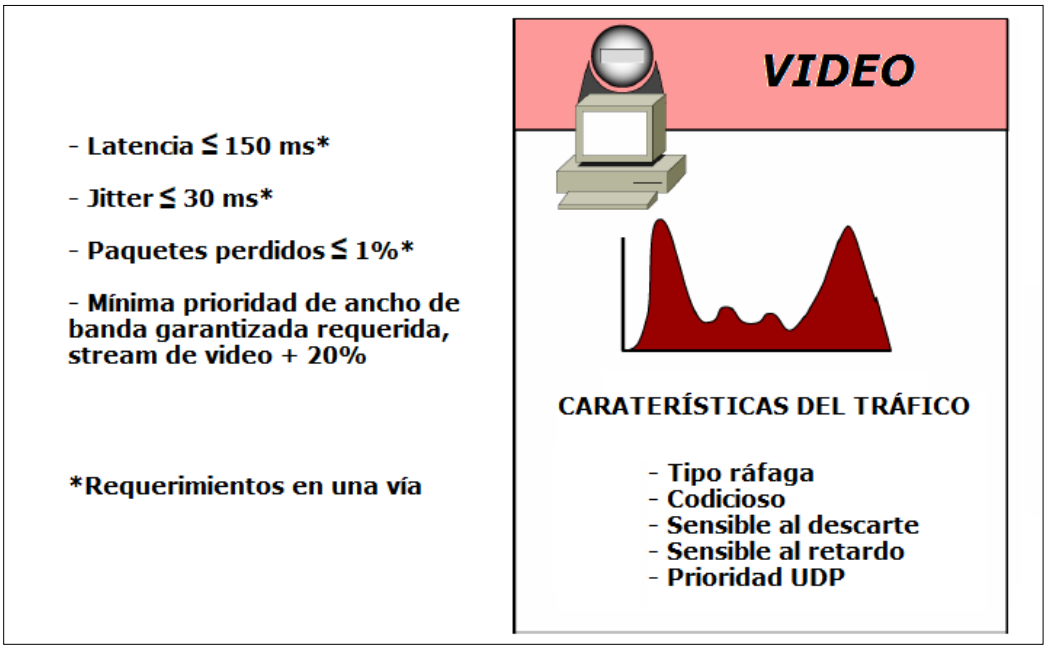


Figura. 5.4. Parámetros para la calidad de video[53]

5.1.3. Datos

La calidad de servicio sobre el tráfico de datos, obviamente exceptuando al de voz y video, depende de muchas de las aplicaciones pertenecientes a la organización y es por ello que su tratamiento debe ser clasificado en función de esto. Es decir, una empresa puede

[52] Casas, Pedro; Guerra, Diego; Irigaray, Ignacio, *Calidad de Servicio Percibida en Servicios de Voz y Video sobre IP*, Facultad de Ingeniería Universidad de la República, Uruguay Agosto 2005, página 26
[53] *Implementing Cisco Quality of Service,* Volumen 2, Version 2.2, Cisco Systems Inc, United States of America 2006, página 9-12

cursar tráfico sobre la red de comunicación como correo electrónico, FTP, HTTP, Telnet, aplicaciones de escritorio remoto, entre otras, dentro de las cuales se necesita establecer prioridades en cuanto al negocio que mueve la empresa.

Dentro de las características de este tráfico de datos se puede exponer las siguientes:

- Flujo constante o variable según el tipo de aplicación
- Benigno o codicioso, igualmente según la aplicación
- No es sensible al descarte
- No es sensible al retardo
- Posee retransmisiones TCP, generalmente

En cuanto a los parámetros críticos sobre la calidad de servicio del tráfico de datos, se puede citar que en cuanto a ancho de banda se lo puede dimensionar de acuerdo a la aplicación; este tráfico es sensible a la pérdida de paquetes lo cual podría ocasionar problemas en la ejecución de la aplicación; y finalmente se toma a este tráfico como insensible al retardo y *jitter*.

Es recomendable clasificar los datos dentro de modelos de prioridad relativa con no más de cuatro o cinco clases, como por ejemplo:

- Aplicaciones de misión crítica. Las mismas que son localmente definidas por el administrador de la red e indican que aplicación se la puede considerar como crítica
- Transaccional. Correspondiente al tráfico interactivo, es decir un servicio de datos preferido
- Mejor esfuerzo. Como por ejemplo el Internet, correo electrónico, tráfico no especificado
- Menos que mejor esfuerzo. Dentro de esta clase podrían considerarse aplicaciones punto a punto como *Kazaa* por ejemplo

En la figura. 5.5., se muestra un resumen de las características para una calidad de servicio aceptable dentro del tráfico de datos.

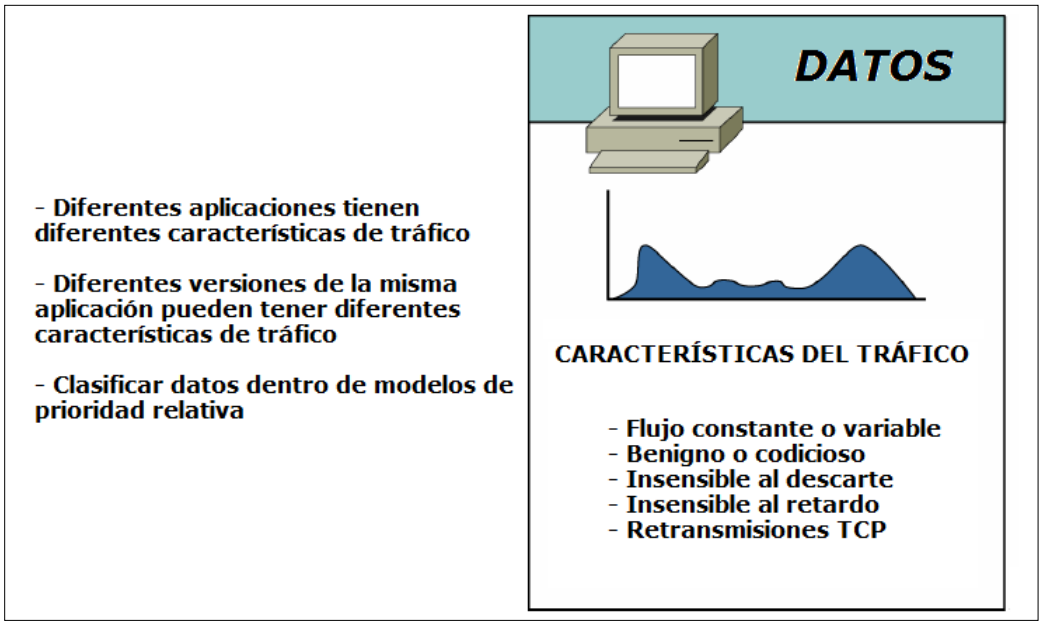


Figura. 5.5. Parámetros para la calidad de datos[54]

5.2. QoS ÚTIL PARA PROBLEMAS EN REDES CONVERGENTES

Esta sección describe los cuatro problemas claves de calidad sobre las redes convergentes: la falta de ancho de banda, el retardo extremo a extremo, la variación de retardo y la pérdida de paquetes.

Con una inadecuada preparación de la red, la transmisión de voz es entrecortada e ininteligible. Los desajustes en el habla son particularmente problemáticos cuando la comunicación es intercalada con silencios.

La interactividad de llamadas pobres en calidad, es resultado del retardo. Esta interactividad causa los siguientes problemas:

- Eco. Es causado por la señal que refleja la voz del hablante nuevamente desde el equipo telefónico remoto

[54] *Implementing Cisco Quality of Service,* Volumen 2, Version 2.2, Cisco Systems Inc, United States of America 2006, página 9-13

- Superposición del hablante. Es causado cuando el retardo en una vía llega a ser mayor que 250 [ms]. Cuando esto ocurre, la comunicación toma un comportamiento de *walkie talkie* o *push to talk*

Las llamadas desconectadas son el peor caso. Si existen grandes desfases en el habla, las partes se cuelgan. Si hay problemas en la señalización, las llamadas se desconectan. Estos eventos son completamente rechazados en las comunicaciones de voz, sin embargo son comunes sobre una red de datos inadecuadamente preparada que intenta transmitir voz.

Como se ha dicho, el tráfico multimedia, como el utilizado en telefonía IP o videoconferencia, puede ser extremadamente sensible a los retardos y puede crear demandas de QoS únicas sobre las redes que los transportan. Cuando los paquetes son entregados usando el modelo de mejor esfuerzo, estos no arriban en orden, en una manera oportuna o en ambas. El resultado son imágenes no claras, desiguales y movimientos lentos, y el sonido no se lo obtiene sincronizado con la imagen.

A continuación se presentan los aspectos críticos que causan la mayor parte de problemas en aplicaciones especiales y los procedimientos de calidad de servicio para combatirlos dentro de las redes convergentes.

5.2.1. Falta de ancho de banda

Este problema corresponde a que varios flujos entran en competencia por una cantidad limitada de ancho de banda. Archivos grandes de gráficos, usos multimedia e incremento del uso de voz y video causan problemas de capacidad de ancho de banda sobre las redes de datos.

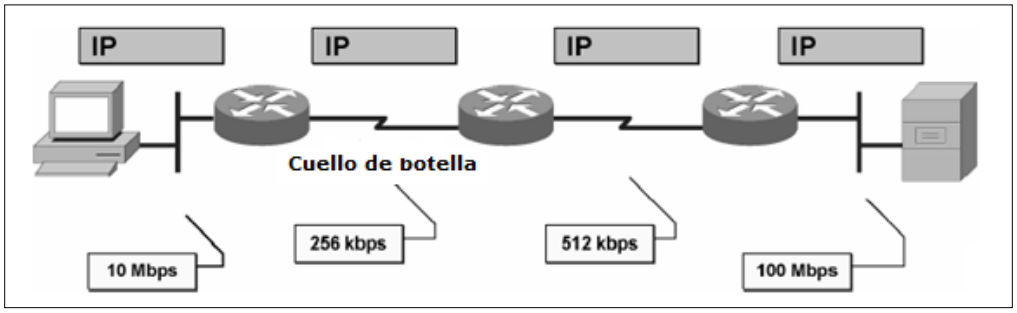


Figura. 5.6. Falta de ancho de banda dentro de una red de datos[55]

[55] *Implementing Cisco Quality of Service,* Volumen 1, Version 2.2, Cisco Systems Inc, United States of America 2006, página 1-8

La figura. 5.6., ilustra una red de datos sin carga con cuatro saltos entre un servidor y un cliente. Cada salto está utilizando diferentes medios de transmisión con un diferente ancho de banda cada uno. El ancho de banda máximo disponible es igual al ancho de banda de las conexiones de menor capacidad.

$$AB\max = \min(10Mbps, 256Kbps 512Kbps, 100Mbps) = 256Kbps$$

Donde *ABmax* es el ancho de banda máximo y *min* es el valor mínimo de ancho de banda entre las conexiones.

El cálculo del ancho de banda disponible, no obstante, es mucho más complejo en casos donde varios flujos atraviesan la red de datos. Se muestra una aproximación de este cálculo en la siguiente fórmula.

$$ABdisp = AB\max / \ flujos$$

Donde *ABdisp* es el ancho de banda disponible, *ABmax* es el ancho de banda máximo y *flujos* es el número de flujos que cruzan la red.

La mejor manera para aumentar el ancho de banda es incrementar la capacidad del enlace con el fin de adaptar todas las aplicaciones y usuarios, con algún ancho de banda extra libre. Aunque esta solución parece simple, incrementar el ancho de banda es costoso y toma tiempo su implementación. Por lo general, existen limitaciones tecnológicas en las actualizaciones de un muy alto ancho de banda, como por ejemplo la capacidad de los equipos terminales, las tecnologías de acceso, entre otros.

Otra opción para contrarrestar este problema es clasificar el tráfico dentro de clases de QoS y priorizar tráfico de acuerdo a la importancia del mismo. El tráfico de voz y el crítico para el negocio deberían tener suficiente ancho de banda para soportar sus requerimientos dentro de la aplicación, la voz debería tener priorizada su transmisión y el tráfico menos importante debería obtener cualquier cantidad de ancho de banda del sobrante. Existe una variedad de mecanismos expuestos anteriormente, con los cuales se puede presentar garantías en el ancho de banda como:

- Encolamiento de prioridad PQ o encolamiento personalizado CQ

- Tipo de servicio distribuido basado en el campo ToS y calidad de servicio basado en grupos de encolamiento equitativo ponderado WFQ

- Encolamiento equitativo ponderado basado en clase CBWFQ

- Encolamiento de baja latencia LLQ

Optimizando el uso de la conexión por compresión de la carga útil de las tramas, virtualmente, se incrementa el ancho de banda del enlace. Por otro lado, la compresión también incrementa el retardo por motivo de la complejidad de los algoritmos de compresión. Utilizando compresión de hardware se puede acelerar las compresiones de carga útil del paquete.

Otro de los mecanismos para proporcionar eficiencia al enlace es la compresión de cabecera. Este procedimiento es especialmente efectivo en redes en las cuales muchos paquetes transportan cantidades pequeñas de datos, es decir donde la carga útil es pequeña. Ejemplos de esta opción para evitar la falta de ancho de banda son la compresión de cabecera TCP y la compresión de cabecera RTP.

5.2.2. Retardo extremo a extremo

Los paquetes de datos tienen que atravesar algunos dispositivos de red y enlaces de diferentes características, entre su origen y destino, lo que provoca un incremento de la totalidad del retardo del paquete. El retardo es el tiempo tomado por un paquete en alcanzar el punto final de recepción después de ser transmitido desde un punto de envío. Este período de tiempo es conocido como retardo extremo a extremo y consta de dos componentes:

- Retardo de red fijo. Dos tipos de retardos fijos son la serialización y los retardos de propagación. La serialización es el proceso de colocar bits en el circuito, cuanto mayor sea la velocidad del circuito, menor será el tiempo de colocación de bits sobre el mismo. El retardo de propagación en cambio, es el tiempo que toma por tramas transmitir al medio físico; sin embargo, generalmente es ignorado pero puede llegar a

ser significante. El eco ***ICMP***[56] (*Internet Control Message Protocol*) es una manera de medir el tiempo de ida y vuelta de los paquetes IP dentro de una red

- Retardo de red variable. El retardo de procesamiento es un tipo de retardo variable, y es el tiempo requerido por un equipo de red en buscar la ruta, cambiar el encabezado y completar las otras tareas de conmutación. En algunos casos, el paquete es manipulado, como por ejemplo cuando el tipo de encapsulación o la cuenta de salto son cambiados. Cada uno de estos pasos contribuyen al retardo de procesamiento. Otro tipo de retardo variable es el retardo de encolamiento, que se lo puede definir como el tiempo que un paquete permanece en la cola de salida de un enrutador. Este retardo depende del número y tamaño de paquetes actuales en la cola, del ancho de banda de la interfaz y del mecanismo de encolamiento

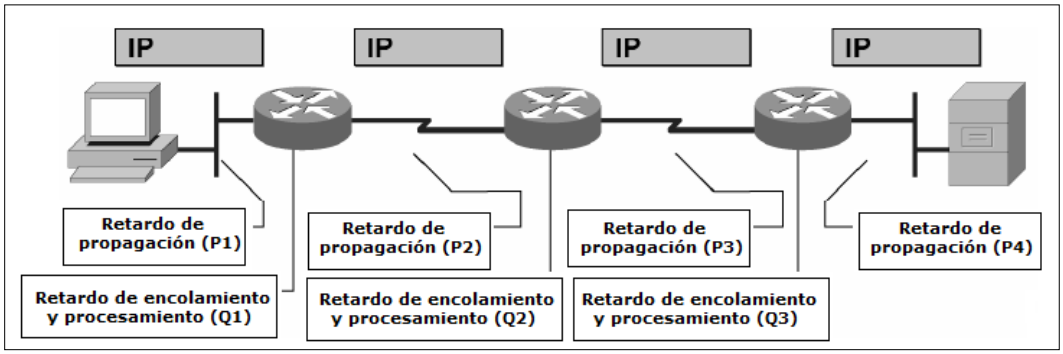


Figura. 5.7. Retardo extremo a extremo en una red de datos[57]

La figura. 5.7., muestra el impacto que una red tiene sobre el retardo extremo a extremo de paquetes a lo largo de toda la comunicación establecida. Cada salto añade una cantidad de retardo sobre el total por los tipos de retardos experimentados en el trayecto.

Asumiendo que un enrutador es lo suficientemente potente para realizar una decisión de transmisión rápidamente, la mayor parte de procesamiento, encolamiento y retardo de serialización es influenciada por los siguientes factores:

- Longitud promedio de la cola

- Longitud promedio de paquetes en la cola

[56] ***ICMP***. Protocolo de control y notificación de errores de IP. Dentro de este se tiene las herramientas *ping* y *traceroute* que envían mensajes de petición eco ICMP y recibe mensajes de respuesta eco, para determinar si un *host* está disponible o marcar los *hosts* por los que pasa

[57] *Implementing Cisco Quality of Service,* Volumen 1, Version 2.2, Cisco Systems Inc, United States of America 2006, página 1-10

- Ancho de banda del enlace

Los siguientes mecanismos permiten acelerar el despacho de paquetes de flujos sensibles al retardo:

Incrementar la capacidad el enlace.

Suficiente ancho de banda causa que las colas se contraigan de modo que los paquetes no esperen mucho tiempo antes de la transmisión. Más ancho de banda reduce el tiempo de serialización. Este puede ser un factor irreal por los costos asociados al incremento de ancho de banda.

Priorizar los paquetes sensibles al retardo.

Este es un factor más efectivo en cuanto a costo. PQ, CQ, prioridad estricta y LLQ tienen capacidades de encolamiento preventivas.

Comprimir la carga útil.

La compresión de la carga útil reduce el tamaño del paquete, de este modo virtualmente se incrementa en ancho de banda del enlace. Los paquetes comprimidos son más pequeños y toman menos tiempo para ser transmitidos.

Compresión de cabecera.

Esta compresión puede ser utilizada como otro mecanismo para reducir los retardos. Especialmente es usada sobre los paquetes de voz que poseen una mala carga útil en relación a la cabecera, la cual puede mejorar mediante la reducción de la cabecera del paquete (compresión de cabecera RTP). Minimizando el retardo, se puede también reducir el *jitter*, cabe indicar que el retardo es más predecible.

5.2.3. Pérdida de paquetes

Los paquetes pueden ser descartados cuando un enlace está congestionado. La pérdida de paquetes es generalmente ocasionada por la cogestión del tráfico sobre la WAN, resultando en conversaciones descartadas o un efecto entrecortado si el lado de emisión trata de acomodar mediante repetición los paquetes previos.

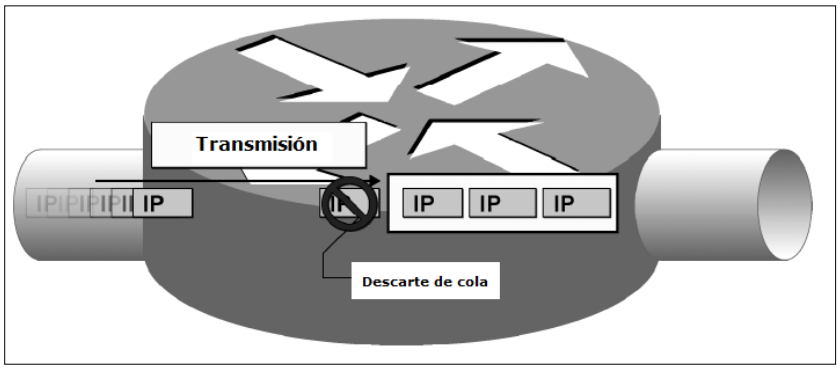


Figura. 5.8. Pérdida de paquetes en una red de datos[58]

La pérdida de paquetes usualmente ocurre cuando los enrutadores acaban su espacio de almacenamiento para una particular cola de interfaz de salida. La figura. 5.8., ilustra una cola llena en la interfaz de salida, lo que causa que un paquete nuevo sea descartado.

Los enrutadores pueden también descartar paquetes por las siguientes razones:

- Descarte de cola entrante. El CPU principal está saturado y no puede procesar paquetes, es decir la cola entrante se encuentra llena
- Ignorar. El enrutador se quedó sin espacio de almacenamiento
- Exceso. El CPU está congestionado y no puede asignar un *buffer* libre a un nuevo paquete
- Errores de trama. Existe un error detectado por *hardware* en una trama, como pueden ser los ***CRCs***[59] (*Cyclic Redundancy Checking*), entre otros

La pérdida de paquetes generalmente es el resultado de saturación sobre una interfaz. Muchas de las aplicaciones que usan TCP experimentan atraso porque TCP se ajusta a los recursos de red. Los segmentos TCP descartados causan que las sesiones TCP reduzcan sus tamaños de ventana. Existen otras aplicaciones que no utilizan TCP y no pueden manejar cortes.

Se puede seguir los siguientes enfoques para prevenir cortes en aplicaciones sensibles:

[58] *Implementing Cisco Quality of Service*, Volumen 1, Version 2.2, Cisco Systems Inc, United States of America 2006, página 1-8
[59] ***CRC***. Es un código de detección de error que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida

- Incrementar la capacidad del enlace a comodidad o prevenir la congestión

- Garantizar el suficiente ancho de banda o incrementar espacios de almacenamiento para acomodar ráfagas de aplicaciones frágiles. Existen algunos mecanismos que permiten garantizar el ancho de banda y proveen de una transmisión priorizada a aplicaciones sensibles de cortes, como los antes mencionados: PQ, CQ, priorización IP RTP, CBWFQ o LLQ

- Prevenir la congestión mediante el descarte de otros paquetes antes que la congestión ocurra. Para ello se puede utilizar la detección temprana aleatoria ponderada WRED para empezar a descartar otros paquetes antes que la congestión suceda

Existen otros mecanismos que ayudan a evitar la congestión sobre una red de datos, los mismos que ya fueron detallados en los capítulos anteriores:

- Modelación de tráfico. La cual retarda los paquetes en lugar de descartarlos tomando en cuenta procedimientos como la modelación de tráfico genérico GTS o la modelación basada en clase

- Políticas de tráfico. Pueden limitar la tasa de los paquetes menos importantes para proporcionar un mejor servicio a paquetes sensibles a los cortes, utilizando técnicas como la tasa de acceso comprometida CAR y políticas basadas en clase

5.3. QoS EN LA INFRAESTRUCTURA DE TELECOMUNICACIONES

5.3.1. Aspectos generales

Actualmente se ha visto que las redes de datos tienen una importante influencia sobre la vida diaria de las personas, ya que han llegado a permitir interactuar de una manera novedosa en las comunicaciones del entorno. Se utilizan estas redes de diferentes formas, entre ellas las aplicaciones Web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación, entre otros.

Para que tenga efecto esta interacción entre personas y la utilización de diferentes aplicaciones para su comunicación, la red de datos se encuentra dotada de toda una infraestructura de telecomunicaciones, y en función al modelo TCP/IP utiliza el equipamiento que permiten una adecuada transmisión de la información. Los principales

dispositivos a considerarse dentro de la red de datos son los enrutadores y los conmutadores.

Enrutadores.

Son dispositivos en los que se centraliza el paso de la información en la red, es decir, un enrutador conecta una red con otra. Por lo tanto, este equipo es responsable de la entrega de paquetes a través de diferentes redes, y es por ello que este equipo ingresa dentro de la capa de red del modelo OSI. Es responsabilidad de los enrutadores la entrega de paquetes a su debido tiempo, ya que la efectividad de las comunicaciones depende, en gran medida, de la capacidad de estos dispositivos de enviar paquetes de una manera muy eficiente.

Para garantizar niveles de servicio en cuanto a las demandas de las redes actuales, los enrutadores también pueden ser utilizados para las siguientes acciones:

- Aseguran una disponibilidad de ***24x7***[60]; y, con el fin de garantizar la posibilidad de conexión entre redes, se utiliza dentro de estos equipos rutas alternativas en caso de que la ruta principal falle

- Proveen servicios integrados de datos, video y voz en redes conectadas por diferentes medios físicos. Para garantizar estos servicios, los enrutadores proporcionan prioridad a los paquetes IP según el QoS de cada servicio, con el objetivo de que tráfico en tiempo real no se descarte ni tampoco retarde. Al soportar QoS, estos equipos ofrecen las siguientes funciones: *DiffServ* e *IntServ,* ancho de banda garantizado, aumenta el control de recursos de red, clasifica y prioriza el tráfico, y maneja la congestión de la red

- Los enrutadores que manejan QoS incluyen los siguientes componentes: marcador/clasificador, encolamiento, administración de *buffer,* y modelación

- Además, los enrutadores pueden dar un grado de seguridad a la red disminuyendo el impacto de gusanos, virus y otros ataques mediante el permiso o denegación del reenvío de paquetes

[60] ***La disponibilidad 24x7*** significa que la operación del servicio prestado estará las 24 horas del día y los 7 días de la semana

Conmutadores.

Los conmutadores son dispositivos de interconexión de redes de computadoras que operan en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas de la red.

Entre las principales funciones que ofrece para obtener una adecuada calidad en el paso de la información, los conmutadores poseen:

- Funcionamiento similar a un filtro en la red, lo que mejora el rendimiento y la seguridad, principalmente dentro de las LANs

- Configuración de calidad de servicio, en algunos casos, proporcionando las siguientes características: administración de tráfico basado en clases de flujo, clasificación, priorización y perfiles de ancho de banda

5.3.2. Calidad de servicio sobre una red de acceso

Una red de acceso es aquella parte de la red de datos global que se encarga de la conexión de los usuarios finales con la red de transporte de la información, la misma que puede ser propia o perteneciente a algún proveedor de servicios, y realiza una función complementaria con la red de backbone dentro de toda la infraestructura de telecomunicaciones.

Esta red de acceso puede también ser tratada como una red WAN constituida principalmente por dos elementos sobresalientes el borde del consumidor CE (*Customer Edge*) y el borde del proveedor PE (*Provider Edge*), tales elementos se pueden observar en la figura. 5.9.

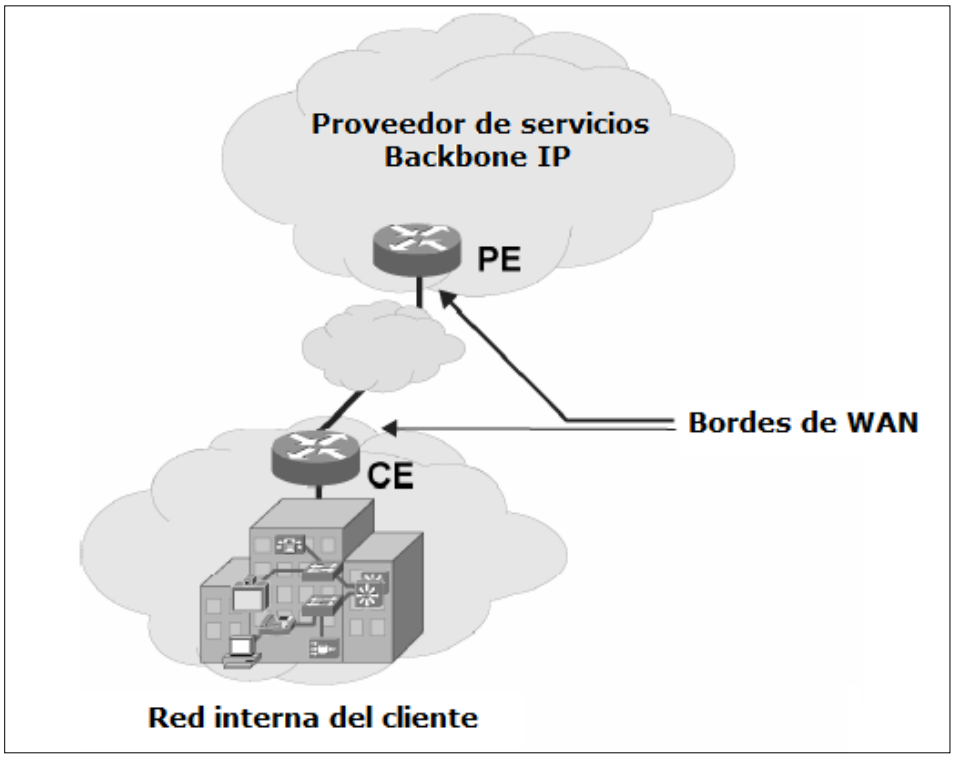


Figura. 5.9. Constitución de una red de acceso[61]

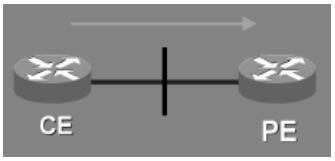
Con respecto a mecanismos de calidad de servicio, en el enlace WAN entre el CE y el PE generalmente son requeridos LLQ o CBWFQ, modelación de tráfico y cRTP.

Para un acertado análisis de los mecanismos a utilizar en esta parte de red de la red global de comunicación, es necesario identificar los tráficos de entrada y salida tomando un punto de referencia, en este caso se tomará la administración del tráfico desde el backbone o desde el proveedor de servicios para explicar los cuadros posteriores.

La tabla. 5.1., muestra una distribución del tráfico en cuanto a sus características y mecanismos de calidad de servicio que se recomienda aplicar sobre los bordes de WAN con respecto al tráfico de salida desde la red interna del consumidor, es decir el direccionamiento de tráfico será desde el CE hasta el PE, tomando en cuenta dos escenarios importantes para el control del tráfico, cuando el administrador de red maneja el CE y cuando no lo hace. Esto se justifica porque los requerimientos de calidad de servicio son diferentes en los dos escenarios.

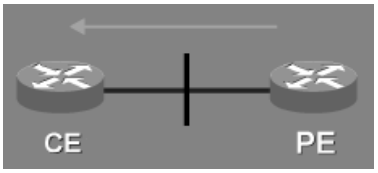
[61] *Implementing Cisco Quality of Service*, Volumen 2, Version 2.2, Cisco Systems Inc, United States of America 2006, página 9-43

Tabla. 5.1. Requerimientos y mecanismos de QoS para tráfico del CE al PE

	CE Manejado	CE no Manejado
DIRECCIÓN DEL TRÁFICO		
REQUERIMIENTOS DE QoS	- La política de QoS de salida en el CE debe ser manejada y configurada por la administración del *backbone* - La administración del *backbone* puede hacer cumplir el SLA para cada clase de tráfico usando las políticas de QoS de salida sobre el CE - Las políticas de salida utilizan encolamiento, descarte y modelación probablemente - Elaborar una clasificación de tráfico o búsqueda de marcaciones - Se podría necesitar cRTP	- La política de QoS de salida en el CE no debe ser manejada y tampoco configurada por la administración del *backbone* - La administración del *backbone* puede solo hacer cumplir el SLA para cada clase de tráfico en la entrada del PE - Las políticas de entrada utilizan el proceso de políticas en sí y la marcación de paquetes - Elaborar una clasificación de tráfico o búsqueda de marcaciones en el PE
MECANISMOS DE QoS	- Al manejar el CE, los mecanismos de QoS sobre el mismo son manejados por la administración del *backbone* - Se utilizan políticas de salida sobre el CE para clasificar y marcar el tráfico - LLQ y/o CBWFQ, y WRED, son utilizados para el manejo y prevención de la congestión -La modelación de tráfico es usada para compensar errores de la velocidad - Se puede implementar cRTP	- Al no manejar el CE, los mecanismos de QoS sobre el PE no son tomados en cuenta por la administración del *backbone* - En las interfaces de entrada del PE generalmente se utiliza políticas de tráfico para limitar la tasa del tráfico de entrada proveniente del CE - Con el control mediante políticas de tráfico se garantiza que no se exceda en la tasa contratada y especificada en el SLA

Ahora bien, se necesita aplicar procedimientos de QoS sobre el tráfico que ingresa al CE proveniente del PE; para esto, la tabla. 5.2., muestra los requerimientos y mecanismos de QoS utilizados sobre este caso del flujo del tráfico.

Tabla. 5.2. Requerimientos y mecanismos de QoS para tráfico del PE al CE

	CE Manejado	CE no Manejado
DIRECCIÓN DEL TRÁFICO		
REQUERIMIENTOS DE QoS	- La administración del *backbone* hace cumplir el SLA utilizando políticas de QoS de salida en el PE - Las políticas de salida utilizan encolamiento, descarte y modelación probablemente - Se podría necesitar Crtp - No se necesita políticas de QoS de entrada en el CE	- La administración del *backbone* hace cumplir el SLA utilizando políticas de QoS de salida en el PE - Las políticas de salida utilizan encolamiento, descarte y modelación probablemente - Se podría necesitar cRTP - Las políticas de QoS de entrada son irrelevantes en el CE
MECANISMOS DE QoS	- Se tienen políticas de salida de QoS en el PE como LLQ y/o CBWFQ, y WRED, que son utilizados para el manejo y prevención de la congestión - La modelación de tráfico es usada para compensar errores de la velocidad - Se puede implementar cRTP	- Se tienen políticas de salida de QoS en el PE como LLQ y/o CBWFQ, y WRED, que son utilizados para el manejo y prevención de la congestión - La modelación de tráfico es usada para compensar errores de la velocidad - Se puede implementar cRTP

5.3.3. Calidad de servicio sobre una red de *backbone*

La red de *backbone* puede definirse como la conexión principal entre los extremos de la red global de comunicación, es decir es una red de transporte de información dentro de la cual se permite la comunicación aplicando diferentes tecnologías de transmisión de datos, entre las que se puede citar como importantes:

El modo de transferencia asíncrona ATM (*Asynchronous Transfer Mode*).

Es una tecnología de telecomunicación orientada a conexiones de alta velocidad para el transporte de varios tipos de tráfico a través de una red. ATM empaqueta los datos en una celda de 53 bytes de longitud fija que se puede intercambiar rápidamente entre conexiones lógicas de una red.

La jerarquía digital síncrona SDH (*Synchronous Digital Hierarchy*).

Son redes que se fundamentan en este sistema de transmisión, como consecuencia de la utilización de fibra óptica como medio de transmisión, así también como la necesidad de encontrar sistemas más flexibles y que soporten anchos de banda mucho más grandes. Cada trama se encapsula en una estructura especial conocida como contenedor. Luego de ello se van añadiendo cabeceras de control que identifican el contenido de la estructura y el conjunto, después de un proceso de multiplexación, se integra dentro de la estructura STM-1, que se considera la trama básica de SDH.

La conmutación de etiquetas multiprotocolo MPLS (*Multiprotocol Label Switching*).

Es un procedimiento de transporte de datos creada para operar entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios. En este proceso se asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los enrutadores intermedios, ya que solo se mira la etiqueta y no la dirección de destino.

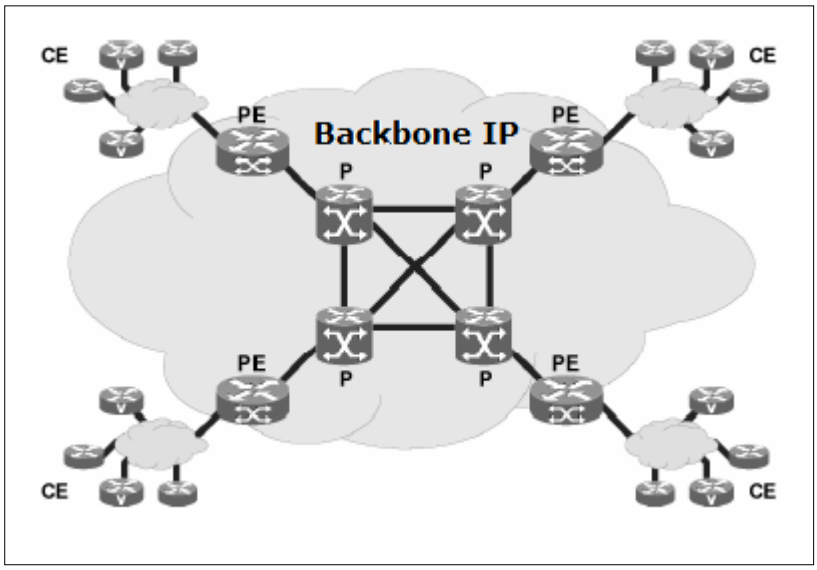


Figura. 5.10. Red de backbone e interconexión con la red de acceso[62]

La figura. 5.10., muestra una conexión típica en la red de backbone entre los enrutadores PE y los enrutadores P (*Provider*). Como se indicó anteriormente este tipo de red puede ser administrada directamente por una empresa de negocio o por un proveedor de servicios.

El núcleo del backbone IP es utilizado para proporcionar transporte de paquetes a altas velocidades. Por lo tanto, todas las marcaciones, políticas y modelaciones de tráfico deberían ser realizadas solo en el enrutador PE, esto es sobre el enlace PE a CE y no en el núcleo.

Utilizando el modelo *DiffServ*, solo el borde requiere una política de QoS compleja. En el núcleo, solo encolamiento y WRED son requeridos. La operación de encolamiento y WRED estará basada en las marcaciones hechas en el PE. Un mecanismo de encolamiento típicamente utilizado sobre el equipamiento de núcleo es LLQ.

Dos de los métodos de diseño de backbone IP incluyen un backbone de mejor esfuerzo con aprovisionamiento y un backbone *DiffServ*.

El enfoque más tradicional es usar un backbone de mejor esfuerzo con aprovisionamiento. Sin embargo, para satisfacer las necesidades de las aplicaciones

[62] *Implementing Cisco Quality of Service,* Volumen 2, Version 2.2, Cisco Systems Inc, United States of America 2006, página 9-54

actuales (VoIP, videoconferencia, ***e-learning***[63], entre otras), el despliegue de un backbone *DiffServ* y el ofrecimiento de SLAs para las diferentes clases de tráfico pueden reducir el costo y mejorar el retardo, el *jitter* y la pérdida de paquetes, y atender los requerimientos de QoS en la red de comunicación.

Con aprovisionamiento, generalmente los administradores de red de backbone utilizan un factor de 2, es decir, se aprovisiona a la máxima capacidad de la red con el doble de la carga de tráfico acumulado en la misma. Existen algunos problemas con este diseño de backbone:

- Si la capacidad planeada no es exacta y se produce una congestión en la red, porque los tipos de tráfico no están diferenciados, los paquetes de VoIP por ejemplo, no serían tratados con una prioridad más alta que otros paquetes de datos, resultando un tratamiento poco óptimo para los paquetes de voz

- El aprovisionamiento para cada tráfico es muy costoso de implementar

- Durante la planeación de la capacidad, todos los escenarios de falla deben ser analizados. Las fallas que no estuvieron planeadas pueden causar una congestión inesperada en la red

- La red puede experimentar demandas de tráfico inesperadas, con lo cual se puede congestionar la red de comunicación

- Denegar los ataques de un servicio podría afectar a los otros servicios

Utilizando *DiffServ* en la red de backbone, el tráfico es aislado dentro de diferentes clases, y cada clase de tráfico es aprovisionada con una diferente política de tráfico basada en los requerimientos de QoS. Por este motivo, se indicó que esta implementación reduce el costo y provee un mejor tratamiento para el retardo, el *jitter* y la latencia, factores críticos sobre las aplicaciones de la red.

Por lo tanto, los beneficios que se obtiene de la implementación de *DiffServ* sobre la red de backbone son:

[63] ***E-learning***. Sistema de educación electrónico en el que se utilizan las tecnologías de la información para la capacitación y formación de estudiantes en línea

- Permite el soporte de múltiples clases de tráfico con diferentes proporciones de aprovisionamientos por clase de servicio
- Un máximo potencial beneficio económico de *DiffServ* es cuando el tráfico requiere el más alto SLA

- Mediante el aislamiento de tráfico en diferentes clases de tráfico, luego el trato de las clases de tráfico con diferentes PHBs, *DiffServ* puede reducir el ancho de banda requerido en la red

Es muy importante recordar que en las conexiones de la red de backbone, es decir PE con P, viceversa y P con P, las políticas de tráfico denominadas políticas de salida son configuradas para proporcionar LLQ o CBWFQ, y WRED. Cada clase de tráfico que garantiza el ancho de banda es configurada utilizando un porcentaje en lugar de un ancho de banda fijo en Kbps.

5.3.4. Principales fabricantes de equipos para soluciones de redes convergentes

Cisco Systems, Inc.[64]

Información General.

Fundada en 1984, en Cisco los clientes son lo primero y una parte integral es la creación de asociaciones duraderas con el fin de trabajar con los clientes para identificar sus necesidades y ofrecer soluciones que garanticen su éxito. Desde sus inicios Cisco se ha visto obligado a abordar el concepto de soluciones con desafíos específicos de los clientes. *Len Bosack* y *Sandy Lerner*, que trabajaban para la Universidad de Stanford, quisieron enviarse entre ellos correos desde sus respectivas oficinas situadas en diferentes edificios, pero no pudieron debido a las deficiencias tecnológicas. Una tecnología tenía que ser inventada para hacer frente a diferentes protocolos de área local, y como resultado de la solución de su problema, el enrutador de múltiples protocolos nació. Desde entonces, Cisco ha dado forma al futuro del Internet, creando valor y oportunidades sin precedentes para clientes, empleados, inversores y socios del ecosistema, convirtiéndose de esta manera en el líder mundial en redes.

[64]Información tomada de la página Web principal de Cisco Systems, Inc. Disponible en http://newsroom.cisco.com/dlls/corpinfo/corporate_overview.html

Transiciones en el mercado.

Cisco tiene un historial probado de éxito en la captura de transiciones en el mercado. A partir de 1997 con la realidad que de la voz y el video sean uno, de pasar a la red de redes en el año 2000 y la red se convierta en plataforma para todas las tecnologías y el núcleo de las soluciones de los clientes; también, la transición de mercado más reciente de colaboración y tecnologías Web. Se ha convertido en guía para los clientes y siempre ha quedado por delante de los cambios del mercado de manera que ayudan a los clientes a evolucionar, ya que su industria y sus necesidades evolucionan.

Tecnología/Oferta de productos.

Las transiciones del mercado evolucionan y con ello Cisco hace la oferta de productos. Con el tiempo, Cisco ha evolucionado de la empresa y el servicio de proveedor de soluciones para hacer frente a las necesidades de los clientes en muchos otros segmentos como empresas pequeñas, de consumo y comerciales. Como resultado, Cisco está cambiando la forma de trabajar, vivir, jugar y aprender. Se esfuerzan por ser "mejor en el mundo" y "mejor para el mundo", ofreciendo soluciones que respondan a las necesidades del cliente, superando sus expectativas y contribuyendo al mundo de una manera positiva. Conexión y colaboración con otros es un elemento clave de la cultura de Cisco. Hacer del mundo un lugar más pequeño gracias a la tecnología y usarla para mejorar las experiencias de la vida. Esa es la "red humana", un lugar donde se conecta todo el mundo.

Academia de Red Cisco.

La Academia de Red Cisco es una iniciativa de educación global que ofrece tecnología de la información y habilidades de comunicación para ayudar a mejorar la carrera y las oportunidades educativas para las personas en comunidades de todo el mundo. En los últimos 12 años, la Academia de Red Cisco ha desarrollado un ecosistema de asociaciones público-privadas para extender los beneficios del programa a más de 750.000 estudiantes al año en más de 165 países.

Prácticas empresariales sostenibles.

Cisco está comprometido a operar de una manera ambientalmente responsable, la creación de productos eficientes en energía, proporcionando a los clientes soluciones que

les ayuden a cumplir sus objetivos ambientales, e inspirar a los empleados a involucrarse y tomar medidas. Cisco cree en la oportunidad para que la industria de las ***TIC***[65] reduzca las emisiones de manera desproporcionada, mientras se ayuda a otros a reducir las suyas.La visión es, "si se puede conectar a Internet, puede ser verde".

Soluciones convergentes[66].

En este mundo complejo de trabajo, la colaboración eficaz es fundamental. La mano de obra está geográficamente dispersa. Los viajes y los presupuestos se han reducido. La sobrecarga de información se considera normal. Las soluciones de colaboración de Cisco ayudan a construir los equipos más efectivos en los límites corporativos, para empresas, y entre continentes. Proporcionar a los clientes acceso inmediato a expertos de la compañía. Formar equipos rápidamente, compartir la información empresarial más relevante. Conocer a tres clientes en tres países en un día, como si todo el mundo está en la misma habitación. Se puede mejorar la interacción, fomentar la innovación y la creatividad, a tomar mejores decisiones más rápido y aumentar la capacidad de respuesta a los clientes y el mercado. La cartera de colaboración de Cisco, junto con los servicios de Cisco y sus socios, reúnen a:

- Conferencia
- Atención al Cliente
- *Software* de empresa social
- Comunicaciones IP
- Mensajería
- Aplicaciones móviles
- Telepresencia

[65] ***TIC***. Tecnologías de la información y la comunicación
[66] Información tomada de la página Web principal de Cisco System, Inc. Disponible en http://www.cisco.com/en/US/netsol/ns1007/index.html

Nortel Networks[67]

Información general.

Nortel ha dado forma a la evolución de las comunicaciones por más de un siglo. Con clientes en más de 150 países, las soluciones de Nortel potencian al top 25 de los proveedores de servicios de redes en el mundo, sirven como cimientos de centros económicos y financieros del mundo, y manejan las comunicaciones que enriquecen las regiones rurales y subdesarrolladas a través del globo. Desde el diseño, instalación y presentación de nuevas redes, hasta la actualización, soporte y manejo de los sistemas existentes, el portafolio de soluciones de Nortel es uno de los más comprensivos en la industria. Clientes alrededor del mundo confían sus comunicaciones a Nortel debido al equipo experimentado, a la visión en la fabricación de negocios simples y a la habilidad para reducir la complejidad de las comunicaciones para los clientes.

Misión.

El propósito de Nortel es claro, crear un alto rendimiento a las compañías del siglo 21 impulsado por el poder de empleados con una pasión para deleitar a los clientes y manejar los resultados de negocio. Implícito en esto se encuentra un compromiso inquebrantable para aprovechar la tecnología innovadora para solucionar problemas y crear oportunidades para los clientes. Esto es conocido como promesa de fabricación simple de negocio. Esta es la filosofía que se está convirtiendo rápidamente en el modo en que Nortel desarrolla y despliega productos y soluciones, sirviendo a los clientes y realizando negocios.

Productos y servicios.

Nortel entrega soluciones en hardware y software diseñadas para mejorar la manera de los clientes y la comunicación de las empresas, reduciendo la complejidad, incrementando la productividad y realizando comunicaciones más efectivas en costo. Nortel también ofrece servicios profesionales que las empresas y los proveedores de servicio necesitan para simplificar el diseño y la entrega de servicios de comunicación. Manejando la transformación de las redes actuales, Nortel está investigando en una variedad de tecnologías enfocadas en áreas de banda ancha inalámbrica 4G, transporte

[67]Información tomada de la página Web principal de Nortel Networks. Disponible en http://www.nortel.com/corporate/pressroom/collateral/corporate_backgrounder_oct2008.pdf

Ethernet, óptico, servicios y aplicaciones de siguiente generación, unificando las comunicaciones y asegurando las redes de datos.

Movilidad y convergencia.

Movilidad y convergencia es la visión de Nortel, permitiendo entregar a los clientes banda ancha inalámbrica en la actualidad. Esto permite a los clientes mover sus redes hacia el tipo de infraestructura basada en IP que los posibilitaría a beneficiarse de nuevos servicios y controlar costos de su infraestructura de red. Efectividad en costo, las redes de siguiente generación serían agnósticas en el acceso, su eficiencia no dependerá de que dispositivo se encuentre conectado a ellas. La siguiente generación de movilidad estaría manejada por 4G en el espacio de transporte. Redes con cable e inalámbricas convergerán alrededor de una plataforma IP.

Servicios y soluciones.

Servicios y soluciones son la esencia de la fabricación de negocios simples. La hiperconectividad pondrá una enorme presión en operadores y empresas para asegurar que sus redes estén desplegadas, manejadas y envueltas para soportar la capacidad incrementada y compleja. El equipo *Leveraging Nortel's Global Services* permite a los clientes concentrar en su núcleo de negocio y adquirir la experiencia de Nortel en planificación, construcción y operación de redes hiperconectadas.

3Com Corporation[68]

Información general.

3Com Corporation es una empresa proveedora de soluciones de redes empresariales que establece un nuevo estándar de precio/rendimiento para los clientes. 3Com cuenta con tres marcas globales H3C, 3Com y *TippingPoint*, que ofrecen la creación de redes de alto rendimiento y soluciones de seguridad para empresas grandes y pequeñas. El portafolio de redes empresariales de H3C, una marca líder en china, incluyen productos que abarcan desde el centro de datos hasta el borde de las redes, mientras *TippingPoint*, redes basadas en sistemas de prevención de intrusión y soluciones de control de acceso de redes, entregan a profundidad, soluciones sin compromiso, infraestructura y protección de rendimiento. En 3Com no se cree que las empresas deban comprometer el rendimiento y la funcionalidad

[68]Información tomada de la página Web principal de 3Com Corporation. Disponible en http://www.3com.com/corpinfo/en_US/index.html

de sus compras de TI en red, por las limitaciones presupuestarias. Se ofrece una amplia cartera de nuevos productos y soluciones que alteran el status quo de la industria, y entrega verdadera ‘’sin compromiso’’ de redes de datos. Las redes empresariales es el único negocio de 3Com. 3Com ha sido un contribuidor importante al desarrollo de redes empresariales desde la invención de Ethernet en la década de los 70s por el fundador de 3Com. Con sede en Massachusetts, USA, 3Com se enorgullece de su compromiso continuo con la innovación. La compañía aprovecha más de 2400 ingenieros de clase mundial para desarrollar la industria para redes y soluciones de seguridad. 3Com tiene más de 1400 patentes Estadounidenses y cerca de 180 patentes Chinas, más de 1050 aplicaciones pendientes Chinas, así como las aplicaciones pendientes de 35 invenciones separadas fuera de China que cubren una amplia gama de tecnologías.

Soluciones de 3Com para pequeñas y medianas empresas.

3Com ha servido durante mucho tiempo a las necesidades de red de pequeñas y medianas empresas con un completo portafolio de conmutadores, enrutadores, inalámbricos, seguridad, administración de red y productos de telefonía IP. Los productos 3Com ofrecen ventajas destacadas en precio/rendimiento. Si una organización tiene 5 o 500 personas, 3Com tiene los productos de red de datos y voz para entregar conectividad, confiabilidad y seguridad necesitada para alcanzar los objetivos del negocio. 3Com trabaja con socios del mejor canal de la industria para llevar los beneficios de su portafolio ***PYMES***[69] a organizaciones alrededor del mundo.

Aplicaciones convergentes.

Basándose en la historia de ser el primero en introducir al mercado extraordinariamente robusto, soluciones de red amigables al usuario, 3Com ofrece un nuevo enfoque de telefonía IP que permite rapidez, implementación efectiva en costos de aplicaciones y comunicaciones de empresas, asegura comunicaciones de supervivencia, incluso en el caso de interrupción de hardware y/o redes de área extensa WAN, y maneja capacidades de comunicación enriquecidas a lo largo de una organización con soluciones fáciles de desplegar, usar y mantener.

[69] ***PYMES***. Corresponde al acrónimo de pequeña y mediana empresa.

Huawei Technologies Co., Ltd.[70]

Información general.

Huawei es un proveedor líder de soluciones de telecomunicación global con grandes asociaciones con operadores alrededor del mundo. Con empleados apasionados y capacidades inigualables permite responder rápida y eficazmente a las necesidades de los clientes con un comprensivo y personalizado conjunto de soluciones extremo a extremo y productos. Trabajando en conjunto con clientes, se ha comprometido en enriquecer la vida de persona a través de las comunicaciones. Las soluciones y productos de Huawei abarcan productos inalámbricos, productos de núcleo de red, productos de red, aplicaciones y software, así como también equipos terminales. Los mejores productos son diseñados en base al chipset ASIC de Huawei y utiliza plataformas compartidas para proporcionar calidad y bajo costo en los productos.

Negocio de Huawei.

Huawei continuará invirtiendo y desempeñando un papel destacado en la prestación de estrategias convergentes IP para garantizar que los usuarios finales sean capaces de experimentar servicios de comunicación consistentes en cualquier momento y lugar. Huawei ha construido portafolios de productos que incluyen redes móviles, redes banda ancha, basadas en IP, redes ópticas, servicios de telecomunicaciones de valor agregado y terminales. Huawei tiene una ventaja en la transición hacia el desarrollo orientado al futuro y puede proporcionar soluciones de comunicación competitivas y servicios para todos los clientes.

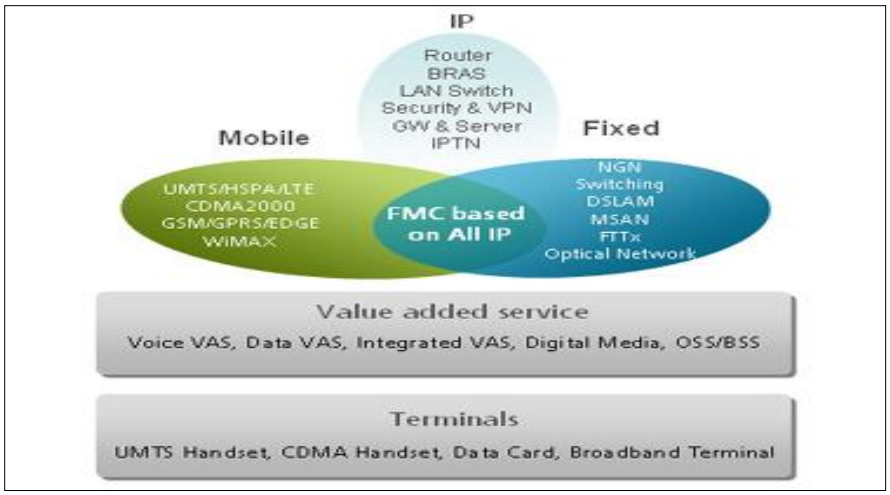


Figura. 5.11. Portafolio de productos de Huawei

[70]Información y figura 5.11., tomada de la página Web principal de Huawei Technologies Co., Ltd. Disponible en http://www.huawei.com/corporate_information.do

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Existen algunos procedimientos y técnicas utilizados para aplicar calidad de servicio en una red TCP/IP que pueden ser clasificados dentro de tres aspectos puntuales para aplicar QoS, como lo son: la marcación y clasificación de paquetes, definidos principalmente por la manipulación del campo ToS dentro de la cabecera IP, con ello se da prioridades en escala para la identificación de cada flujo de tráfico; la administración de la congestión, utilizando métodos de encolamiento y manejo de colas dentro de los equipos de comunicación, con el fin de dar un tratamiento adecuado a los diferentes tipos de tráfico; y, la prevención de la congestión, utilizando estrategias automáticas que monitorean el estado de la red para evitar que se sature de acuerdo al tráfico que cruza la red de datos. Estos aspectos deben ser aplicados a lo largo de la infraestructura de comunicaciones en base a modelos de servicio de cada ente administrador de la red en comunión con los acuerdos de servicios de los usuarios finales.

- Es necesario aplicar QoS a servicios convergentes dentro de una red TCP/IP ya que permite la identificación de diferentes tipos de tráfico que cruzan sobre un mismo medio físico de transmisión, al ser identificados se los puede dar un tratamiento de acuerdo a la importancia de la información que poseen, asignando prioridades y controlando que la congestión del enlace no afecte el paso de esta información, que puede llegar a ser crítica.

- Los factores humanos influyen notablemente en la decisión de QoS sobre el servicio adquirido al usuario final. Los límites sensoriales y sistemas cognitivos son bien entendidos y son incambiables a diferencia de la tecnología, proporciona un objetivo sólido contra la satisfacción, decepción o superación de las necesidades del usuario final. Los servicios que se deben tomar en cuenta dentro de este aspecto son: perceptivo, cognitivo, social y postal.

- Para considerar los procedimientos o técnicas de QoS a implementar se debe tomar en cuenta los parámetros críticos que afectan las aplicaciones que cruzan la red de servicios convergentes, esto es, para la falta de ancho de banda, se tiene que utilizar PQ o CQ como

técnicas de encolamiento, esto porque dentro de ellos se puede manejar prioridades, también se puede utilizar servicios distribuidos basados en el campo ToS, WFQ, CBWFQ y LLQ, con el fin de clasificar el tráfico en cuando a prioridad; para el retardo extremo a extremo, se puede incrementar el ancho de banda con el fin de que las colas se contraigan y reducir los tiempos de serialización (no es muy recomendable ya que incurre en costos), utilizar PQ, CQ o LLQ para priorización de paquetes sensibles al retardo, compresión de carga útil y cabecera también ayuda a controlar este parámetro; y , para la pérdida de paquetes, PQ, CQ o LLQ para garantizar el ancho de banda que es lo que ocasiona este parámetro cuando existe saturación, WRED para prevenir la congestión por descarte de paquetes, también modelación de tráfico para retardar los paquetes y políticas de tráfico para limitar la tasa de paquetes.

- Para el análisis punto-punto dentro de una infraestructura de telecomunicaciones, hay que tomar en cuenta que los equipos y las redes que intervienen es esta manejen adecuadamente la calidad de servicio, este es el caso de los enrutadores, que deben garantizar disponibilidad, proveen servicios integrados y manejan marcación, clasificación, colas y *buffers*, así como también seguridades; los conmutadores, los cuales deben soportar administración de tráfico, clasificación, priorización y perfiles de ancho de banda; la red de acceso para el enlace WAN entre CE-PE se utilizan LLQ, CBWFQ, modelación de tráfico y cRTP; y, para la red de backbone, es importante definir un modelo apropiado para evitar complejidad y permitir escalabilidad de la red.

RECOMENDACIONES

- Antes de aplicar los procedimientos y técnicas de la calidad de servicio, se deber realizar un análisis de la red actual o de la red a implementar, ya que se debe tener en cuenta aspectos como escalabilidad, comportamiento del equipamiento y de los medios físicos, y fundamentalmente realizar un análisis de las características de los tipos de tráfico a cruzar por la red de comunicación.

- Se tiene que cumplir con los siguientes pasos para tener una adecuada implementación y decisión sobre la calidad de servicio de la red: auditoría de tráfico, auditoría de negocio y establecimiento de niveles de servicio.

- Dentro de los parámetros críticos en cada una de las aplicaciones convergentes comunes se debe tener en cuenta lo siguiente para un adecuado funcionamiento de las

mismas: para la voz, latencia ≤150[ms], jitter ≤30[ms], paquetes perdidos ≤ 1%, de 17-106 [Kbps] de ancho de banda de prioridad garantizada por llamada; para el video, latencia ≤150[ms], jitter ≤30[ms], paquetes perdidos ≤ 1%, mínima prioridad de ancho de banda garantizada requerida, *stream* video +20%; y, para datos, depende de la aplicación a ser transmitida sobre la red.

- Para tener un control y un correcto manejo de QoS sobre la infraestructura de comunicaciones, se debe tener presente que en la red de acceso se utiliza clasificación de paquetes; en la WAN de borde admisión de control, prevención de congestión y administración de congestión; y, en la red de *backbone* QoS de núcleo, como prevención y administración de congestión.

ANEXOS

ANEXO A1

MAPEO DE ToS IPv4 A DSCP[71]

La siguiente tabla muestra un mapeo completo entre el octeto ToS y el octeto DS.

Precedencia IP (3 bits)			DSCP (6 bits)				
Nombre	**Valor**	**Bits**	**PHB**	**Selector de clase**	**Precedencia de descarte**	**Nombre de Codepoint**	**Bits DSCP (decimal)**
Rutinario	0	000	Por defecto			Por defecto	000 000(0)
Prioridad	1	001	AF	1	1: Baja	AF11	001 010(10)
					2: Media	AF12	001 100(12)
					3: Alta	AF13	001 110(14)
Inmediato	2	010	AF	2	1: Baja	AF21	010 010(18)
					2: Media	AF22	010 100(20)
					3: Alta	AF23	010 110(22)
Flash	3	011	AF	3	1: Baja	AF31	011 010(26)
					2: Media	AF32	011 100(28)
					3: Alta	AF33	011 110(30)
Invalidar flash	4	100	AF	4	1: Baja	AF41	100 010(34)
					2: Media	AF42	100 100(36)
					3: Alta	AF43	100 110(38)
Crítico	5	101	EF	5		EF	101110(46)
Control Internetwork	6	110					(48-55)
Control de red	7	111					(56-63)

[71] Chao, Jonathan; Liu, Bin, *High Performance Switches and Routers*, Editorial Wiley-Interscience a Wiley&Sons Publication, United States of America 2007, páginas 128

ANEXO A2

CAMPOS DE IDENTIFICACIÓN DE FLUJO PARA WFQ[72]

WFQ primero identifica cada flujo individual y lo clasifica como un flujo alto o bajo ancho de banda. Cada flujo es caracterizado utilizando la siguiente información.

PROTOCOLO	CAMPOS DE IDENTIFICACIÓN DE FLUJO WFQ
TCP/IP	Protocolo IP Dirección IP origen Dirección IP destino Puerto origen Perto destino Campo ToS
Appletalk	Red, nodo y socket origen Red, nodo y socket destino Tipo de protocolo
IPX	Red, nodo y socket origen Red, nodo y socket destino Tipo de protocolo nivel 2
DECnet	Dirección origen Dirección destino
Frame Relay	Valor DLCI
Puente transparente	Dirección MAC origen y destino
CLNS	NSAP origen NSAP destino
Banyan VINES	Red y host origen Red y host destino Tipo de protocolo nivel 2
Apollo	Red, host y socket origen Red, host y socket destino Tipo de protocolo nivel 2
Todos los otros	Protocolos de control (uno por cola)

[72] Durand, Benoit; Sommerville, Jerry; Buchmann, Mark; Fuller, Ron, *Administering CISCO QoS in IP Networks*, Syngress Media Inc, United States of America Marzo 2001, página 229

ANEXO A3

CÓDECS UTILIZADOS PARA EL TRÁFICO DE VOZ[73]

La siguiente tabla contiene cálculos para los tamaños de carga útil de voz por defecto bajo el protocolo H.323.

INFORMACIÓN DE CÓDEC				CÁLCULOS DE ANCHO DE BANDA			
CÓDEC&TASA DE BIT (kbps)	TAMAÑO DE MUESTRA DE CÓDEC (Bytes)	INTERVALO DE MUESTRA DE CÓDEC (ms)	MEAN OPTION SCORE (MOS)	TAMAÑO DE CARGA ÚTIL DE VOZ (Bytes)	TAMAÑO DE CARGA ÚTIL DE VOZ (ms)	PAQUETES POR SEGUNDO (PPS)	ANCHO DE BANDA ETHERNET (Kbps)
G.711 (64 Kbps)	80	10	4.1	160	20	50	87.2
G.729 (8Kbps)	10	10	3.92	20	20	50	31.2
G.723.1 (6.3 Kbps)	24	30	3.9	24	30	34	21.9
G.723.1 (5.3 Kbps)	20	30	3.8	20	20	34	20.8
G.726 (32 Kbps)	20	5	3.85	80	20	50	55.2
G.726 (24 Kbps)	15	5		60	20	50	47.2
G.728 (16 Kbps)	10	5	3.61	60	30	34	31.5

Explicación de los términos.

Tasa de bit del códec (Kbps). Basado en el códec, es el número de bits por segundo que necesitan ser transmitidos para entregar una llamada de voz.

$$tasa\_bit\_códec = tamaño\_muestra\_códec / \text{int}ervalo\_muestra\_códec$$

Tamaño de muestra de códec (Bytes). Basado en el códec, es el número de bytes capturados por el procesador de seña digital DSP (*Digital Signal Proccesor*) en cada intervalo de muestra de códec.

Intervalo de muestra de códec (ms). Es el intervalo de muestra en el cual el códec opera.

MOS. Es un sistema de clasificación de la calidad de voz de conexiones telefónicas. Con MOS, un amplio rango de oyentes juzga la calidad de la voz en una escala de 1 (malo) a 5 (excelente). Los resultados son promediados para proporcionar el MOS al códec.

[73] *Voice over IP – Per Call bandwidth Consumption*, Cisco Systems Inc. Mayo 2005, páginas 2 - 4

Tamaño de carga útil de voz (bytes). Representa el número de bytes o bits que son completados en un paquete. El tamaño de carga útil de voz debe ser un múltiplo del tamaño de muestra de códec.

Tamaño de carga útil de voz (ms). Puede también ser representado en términos de las muestras de códec.

Paquetes por segundo PPS. Representa el número de paquetes a ser transmitidos cada segundo a fin de entregar la tasa de bit del códec.

Fórmulas de cálculo de ancho de banda.

Los siguientes cálculos son usados:

$$tamaño\_paquete\_total = (cabecera\_capa2) + (cabeceraIP/UDP/RTP) + (tamaño\_carga\_útil\_voz)$$

$$PPS = (tasa\_bit\_códec)/(tamaño\_carga\_útil\_voz)$$

$$Ancho\_de\_banda = tamaño\_paquete\_total \times PPS$$

ANEXO A4

CÓDECS DE VIDEO[74]

A continuación se presentan los códecs más utilizados en video:

H.261 Es un códec pensado para utilizarse con teleconferencias sobre ISDN, por lo que su calidad no es lo más destacable. Consume un ancho de banda múltiplo de 64kbps (P*64 Kbps, con P natural), por lo que se lo conoce como P*64. Cuenta con un mecanismo para controlar la calidad en función del movimiento de la secuencia. Cuánto mayor el movimiento, menor la calidad de la imagen, de forma que la tasa sea constante.

H.263 Es una versión mejorada del H.261. Mejora la compensación de movimiento tiene una mayor configurabilidad (menor tasa de bits o mayor recuperación frente a errores). También agrega soporte para pictures del tipo P y B. Además, soporta una mayor variedad de resoluciones que su antecesor, por lo que su uso se extiende más allá de la videoconferencia.

MJPEG Aunque no es un CODEC de video propiamente dicho, se utiliza muy a menudo una sucesión de cuadros codificados con el formato JPEG. O sea, no se utiliza compresión temporal de ningún tipo.

MPEG-1 Genera datos a una tasa entre 1 y 1.5 Mbps. Tiene la calidad del VHS (352 X 288 y 30 fps). Está pensado para utilizarse en medios como el CD-i, por lo que utiliza ancho de banda sin mayor cuidado. Además, tiene una gran susceptibilidad a las pérdidas por su extenso uso de cuadros tipo P y B (el uso de éstas últimas hace que su utilización en aplicaciones con algún tipo de interactividad no sea lo más adecuado por la latencia extra). Por último, no implementa ningún tipo de escalabilidad (que sería explicado más adelante).

MPEG-2 Es la extensión de MPEG-1, pero soporta mayores resoluciones aún y mejores prestaciones en audio. Esto trae como contrapartida un mayor ancho de banda consumido (entre 4 y 15 Mbps). Implementa algunas escalabilidades. Esto es enviar una transmisión base con lo necesario para que la calidad sea aceptable, y además enviar otras transmisiones (capas superiores) con la información extra necesaria para que la calidad sea la requerida. Esto es útil cuando se necesitan descartar algunos paquetes, pues se puede

[74] Casas, Pedro; Guerra, Diego; Irigaray, Ignacio, *Calidad de Servicio Percibida en Servicios de Voz y Video sobre IP*, Facultad de Ingeniería Universidad de la República, Uruguay Agosto 2005

comenzar por los que pertenecen a las capas superiores. MPEG-2 implementa tres: escalabilidad SNR, espacial y temporal. La primera es cuantizar la base con menor cantidad niveles, y las capas superiores con mayor precisión. En la espacial se envía en la base la resolución mínima, y en las capas superiores se envía información para ir aumentando la resolución. Por último, la escalabilidad del tipo temporal es aquella donde se envía como base la cantidad mínima de cuadros por segundo, y se marcan como capas superiores los cuadros entre aquellos que forman la base. Nuevamente la idea para la que fue diseñado fue para la utilización en medios como el DVD o la transmisión satelital (donde se logra un mejor aprovechamiento del ancho de banda de los canales analógicos), y es por eso que no se usa casi en transmisiones por Internet.

MPEG-4. Este códec soporta tres rangos de generación de datos:

1. Menor a 64 Kbps

2. Entre 64 y 384 Kbps

3. Entre 384 y 4000 Kbps

Fue diseñado para utilizarse en Internet y para reproducir video de calidad variada. En el rango inferior, utiliza las mismas técnicas que MPEG tradicional (utilización de macro-bloques, bloques I, P y B, etc). En los rangos superiores utiliza un enfoque completamente distinto, pues separa la imagen en regiones (objetos). No se utilizan más los macro-bloques de tamaño fijo y se pasa a trabajar con macro-bloques de tamaño variable, donde cada macro-bloque puede llegar a representar un objeto (o partes del mismo) en la secuencia. Además se diseño mucho más tolerante a errores mediante el uso de marcadores de resincronización, cabeceras, etc. Sigue teniendo la escalabilidad de MPEG-2, pero ahora con los objetos. Por ejemplo, supongamos que tenemos una secuencia que consta de una persona hablando delante de un fondo relativamente estático. Se puede configurar que la resolución tanto temporal como espacial del objeto fondo sea la mínima, y darle gran calidad al objeto persona. Por último, tiene una estructura de capas:

- **VOP** Es la muestra temporal de un objeto

- **GOV** Un conjunto de VOP se puede agrupar en un GOV para facilitar la resincronización o el acceso aleatorio a la secuencia

- **VOL** Cada nivel o capa de la escalabilidad de cada objeto se encuentra en los VOL
- **VO** Es un objeto de la secuencia
- **VS** Es la secuencia completa

Sin embargo, el concepto de objeto no se utiliza en las implementaciones de este códec por cuestiones claras de eficiencia. Cualquier algoritmo de segmentación (necesario para identificar objetos dentro de una imagen) implica tiempos de cálculo y recursos importantes que inhabilitan su uso. Por lo tanto, los macro-bloques en MPEG-4 difícilmente representen objetos.

REFERENCIAS BIBLIOGRÁFICAS

Marchese, Mario, *QoS over Heterogeneous Networks*, Editorial John Wiley&Sons LTD, England 2007, páginas 1-8, 29-44

Turner, Kenneth; Magill, Evan; Marples, David, *Service Provision, Technologies for Next Generation Communications*, Editorial John Wiley&Sons LTD, England 2004, páginas 117-129

Muller, Nathan, *IP Convergence: The Next Revolution in Telecommunications*, Editorial Artech House, England 2000, páginas 1-47

Chao, Jonathan; Liu, Bin, *High Performance Switches and Routers*, Editorial Wiley-Interscience a Wiley&Sons Publication, United States of America 2007, páginas 114-175

Durand, Benoit; Sommerville, Jerry; Buchmann, Mark; Fuller, Ron, *Administering CISCO QoS in IP Networks*, Syngress Media Inc, United States of America Marzo 2001

Casas, Pedro; Guerra, Diego; Irigaray, Ignacio, *Calidad de Servicio Percibida en Servicios de Voz y Video sobre IP*, Facultad de Ingeniería Universidad de la República, Uruguay Agosto 2005

Implementing Cisco Quality of Service, Volumen 1 y 2, Version 2.2, Cisco Systems Inc, United States of America 2006

Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2, Cisco Systems Inc, United States of America 2006

Internetworking Technology Handbook - Quality of Service (QoS) - Cisco Systems, http://www.cisco.com/en/US/docs/internetworking/technology/handbook/QoS.html, Publicación 2007, Consultado en Agosto 2009

HOJA DE FIRMAS CON FECHA DE ENTREGA

ELABORADO POR

Carlos Alberto Cadena Silva

DIRECTOR DE CARRERA

Ing. Gonzalo Olmedo, Ph. D

Sangolquí, 28 de septiembre de 2010