UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

GESTIÓN DEL TRÁFICO IP DE UNA EMPRESA MEDIANTE CALIDAD DE SERVICIO DIFERENCIADO

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

MIRTHA ELIDA MENDOZA SOVERO

PROMOCIÓN

2007 - I

LIMA – PERÚ
2012

GESTIÓN DEL TRÁFICO IP DE UNA EMPRESA MEDIANTE CALIDAD DE SERVICIO DIFERENCIADO

El presente trabajo está dedicado:

a mis padres Luisa y Hugo por su apoyo y compresión,

a mis hermanos por su apoyo.

SUMARIO

El presente trabajo contiene la descripción de los pasos y consideraciones a seguir para llegar a implementar herramientas de calidad de servicio sobre la arquitectura de servicios diferenciados (DiffServ), para permitir gestionar los parámetros de ancho de banda, pérdida de paquetes, jitter y delay del tráfico de las clases de servicio (CoS) en las cuales es clasificado el tráfico de una empresa que tiene contratado con un proveedor de servicios (ISP) el servicio RPVL (Red Privada Virtual Local) con calidad de servicio por clase de servicio. Al principio se da una introducción teórica sobre conceptos de características del tráfico, herramientas de calidad de servicio que pueden influenciar en las características del tráfico, se describe la arquitectura de servicios diferenciados (DiffServ) y Servicios Integrados (IntServ). También se describe las herramientas de calidad de servicio con la que dispone IOS (sistema operativo de equipos Cisco) de Cisco.

En la última parte se registran datos reales y los scripts de configuración de las herramientas de calidad de servicio implementadas en los routers CPE (equipo final del cliente), en el equipo de acceso de proveedor y en el equipo PE (equipo final del proveedor) del proveedor para dos sedes de la empresa. Finalmente se muestra los resultados del consumo de ancho de banda y la cantidad de paquetes descartados por clase de servicio de dos sedes de la empresa.

ÍNDICE

PROLOGO

Actualmente en nuestro país se viene dando un crecimiento económico que está permitiendo el crecimiento de las empresas, por lo que para algunas de ellas se hace necesario la apertura de nuevas sucursales que les permitirán seguir creciendo, ampliando su mercado y brindando un servicio que estará más cerca a sus usuarios. La apertura de una nueva sede involucra la implementación de los servicios de telecomunicaciones que le permitirá estar comunicado con las demás sedes y de esta forma desarrollar un trabajo sincronizado con las demás sedes en beneficio del crecimiento de la empresa.

Generalmente las sucursales de las empresas se ubican en distintos puntos geográficos por lo que para establecer la comunicación entre todas las sedes es necesario la contratación de un acceso WAN a un proveedor de servicio.

Dado que la contratación de un acceso WAN implica un costo monetario mensual, la empresa tiene que contratar un servicio de acceso WAN en la que se optimice el uso del ancho de banda contratado y se le brinde calidad de servicio al tráfico de las distintas aplicaciones que utiliza la empresa para la correcta operación de su negocio.

Las distintas aplicaciones tienen distintos requerimientos de ancho de banda, delay, jitter y pérdida de paquetes; se puede gestionar el ancho de banda, gestionar la pérdida de paquetes, influenciar en el delay y jitter mediante las herramientas de calidad de servicio, la gestión de estos parámetros permitirá que el tráfico de las distintas aplicaciones reciban un trato con calidad de servicio y como consecuencia se garantice la correcta operación de la aplicaciones de la empresa con un uso óptimo de los recursos de red.

En la actualidad se cuenta con dos arquitecturas que permiten la implementación de calidad de servicio. Una de las técnicas de QoS (Calidad de Servicio) es IntServ, el cual permite la reservación de recursos de red por medio de la señalización que se da antes del envió del flujo de tráfico de una aplicación, esto garantiza la calidad de servicio de extremo a extremo, como desventaja se tiene el consumo de recursos de red por la señalización continua para cada flujo activo. La otra técnica de QoS es Calidad de Servicio Diferenciado (DiffServ), la cual en cada salto por donde transita el tráfico se brinda un nivel de servicio a cada clase de tráfico en la cual se clasifica el tráfico de las distintas

aplicaciones, como ventaja de esta arquitectura se tiene su escalabilidad y uso óptimo de los recursos de red, como desventaja se tiene que no se garantiza la calidad de servicio de extremo a extremo.

En el presente trabajo se considera la arquitectura de servicios diferenciados para la gestión del ancho de banda, gestión de pérdida de paquetes y la influencia en el jitter y delay del tráfico WAN de una empresa que cuenta con una sede principal y 13 sedes remotas, la empresa en cada sede cuenta con una red convergente por lo que el tráfico que envía a nivel WAN está formado por tráfico de distintas aplicaciones con distintos requerimientos de ancho de banda, delay, jitter y pérdida de paquetes. El servicio WAN ofrecido por el proveedor de servicios es un servicio de red privada virtual con calidad de servicio que garantiza ancho de banda para cada clase de servicio. Se consideró DiffServ debido a su escalabilidad y a la habilidad de brindar un trato diferenciado por clase de servicio en la que se puede clasificar el tráfico de las aplicaciones de una empresa.

Como limitación del trabajo es que solo se considera la gestión de los parámetros de transmisión del tráfico mediante la implementación de herramientas de calidad de servicio, existen otras técnicas que permiten gestionar el ancho de banda que no se tocan en el presente informe debido a que no están basados en la implementación de herramientas de calidad de servicio.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

1.1. Descripción del Problema

El servicio de las telecomunicaciones es esencial para una empresa, la necesidad de estar comunicados es indispensable para el desarrollo y crecimiento de la empresa. Algunas empresas cuentan con más de una sede siendo necesario que todas las sedes de una empresa estén intercomunicadas para su adecuada operación. Generalmente las sucursales de una empresa se encuentran ubicadas en puntos geográficos distantes por lo que para lograr la comunicación entre todas las sedes es necesario contar con un acceso WAN (red de acceso de área amplia), la contratación de este acceso WAN implica un costo monetario por lo que su uso debe ser de forma óptimo y a la vez se debe garantizar que las aplicaciones que hacen uso de dicho recurso operen adecuadamente. En redes convergentes los recursos de red son compartidos, en el caso del recurso de ancho de banda de un acceso WAN también es un recurso compartido por las distintas aplicaciones, dado que se tiene que garantizar que las aplicaciones operen adecuadamente y debido a que las distintas aplicaciones tienen distintos requerimientos de ancho de banda, delay, jitter y pérdida de paquetes es necesario implementar herramientas de calidad de servicio que permitan gestionar el ancho de banda, gestionar la pérdida de paquetes, influenciar en el delay, influenciar en el jitter y de esta forma poder brindar un nivel de calidad de servicio al tráfico de las distintas aplicaciones lo cual permitirá la adecuada operación de la empresa con un uso óptimo de los recursos de red.

Para la implementación de QoS (calidad de servicio) existen dos arquitecturas, la arquitectura de Servicios Integrados (IntServ) y la arquitectura de Servicios Diferenciados (DiffServ). La arquitectura de servicios integrados reserva recursos en la red antes del envió del flujo de tráfico, de esta forma se garantiza la calidad servicio pero como desventaja se tiene el consumo de recursos por la señalización y la poca escalabilidad. La arquitectura de DiffServ en cada salto en la red camino al destino brinda un trato diferenciado a cada clase de servicio en la que se clasifica el tráfico, de esta forma hace

que sea un modelo escalable y como desventaja se tiene que no se garantiza la calidad de servicio de extremo a extremo.

Para la gestión de los cuatro parámetros del tráfico (ancho de banda, delay, jitter y pérdida de paquetes) de una empresa se eligió el modelo DiffServ debido a su escalabilidad y a su óptimo uso de los recursos de la red.

1.2. Objetivos del Trabajo

- Dar una alternativa para gestionar los parámetros de ancho de banda, delay, jitter y pérdida de paquetes del tráfico de una empresa que cuenta con varias sedes y utiliza aplicaciones con diferentes requerimientos de ancho de banda, delay, jitter y pérdida de paquetes, lo cual permitirá hacer uso óptimo de los recursos de red y a la vez garantizar la adecuada operación de las distintas aplicaciones.
- Hacer conocer la arquitectura de Servicios Diferenciados.
- Dar a conocer las diferentes herramientas de calidad de servicio con la que dispone el IOS de Cisco.
- Hacer conocer la forma de configuración de calidad de servicio en IOS Cisco.
- Dar a conocer las distintas herramientas de calidad de servicio que permiten gestionar la congestión y la pérdida de paquetes.
- Mostrar la implementación de calidad de servicio en la red de una empresa que cuenta con una sede principal y 13 sedes remotas.

1.3. Evaluación del Problema

Cuando se tiene un acceso WAN por la que se pasa el tráfico de distintas aplicaciones, es necesario que se garantice la correcta operación de las aplicaciones ya que estas influyen en la operación de la empresa, se puede optar por contratar un acceso WAN con un ancho de banda amplio lo cual implicaría un costo elevado para la empresa y a la vez no se contaría con la calidad de servicio que garantice que las aplicaciones operen correctamente y como consecuencia la operación de la empresa se vería afectada.

Ante esto se tiene la alternativa de contar con un acceso WAN con un ancho de banda garantizado por cada clase de servicio y a la vez cada clase de servicio puede contar con un nivel de servicio lo cual permitiría que las distintas aplicaciones operen adecuadamente.

Para garantizar un ancho de banda por clase de servicio se puede implementar herramientas de calidad de servicio que permiten gestionar el ancho de banda por clase de servicio, y mediante la implantación de otro tipo de herramientas de calidad de servicio se puede gestionar los parámetros de pérdida de paquetes, delay y jitter del tráfico de las

distintas aplicaciones lo cual permitirá que el tráfico de las aplicaciones operen adecuadamente y se utilicen de forma óptima los recursos de red.

1.4. Limitaciones del Trabajo

El presente trabajo en su solución, sólo considera algunos métodos que permiten gestionar los parámetros del tráfico (ancho de banda, delay, jitter y pérdida de paquetes).

Cabe señalar que en un acceso WAN se es dependiente del nivel de servicio (SLA) que el proveedor puede ofrecer, lo cual limita el número de clases de servicio en la que se pude clasificar el tráfico.

Los equipos CPE, y equipos del proveedor son de la marca Cisco, por lo que solo se muestra la forma de configuración de herramientas de calidad de servicio en equipos de la marca Cisco.

1.5. Síntesis del Informe

En el capítulo I se realiza el planteamiento de ingeniería del problema, se describe el problema y los objetivos del trabajo. A lo largo del capítulo II se expone el marco teórico, se expone conceptos de características del tráfico, herramientas de calidad de servicio que pueden influenciar las características del tráfico, se describe la arquitectura de Servicios Diferenciados (DiffServ), se describe brevemente la arquitectura de Servicios Integrados (IntServ), se describe las herramientas de calidad de servicio con la que dispone en IOS (sistema operativo de equipos Cisco) de Cisco, se brinda un explicación sobre la configuración de calidad de servicio en IOS de Cisco.

En el capítulo III se muestran los datos reales que se consideran en la implementación de calidad de servicio y gestión de la congestión del tráfico de una empresa que cuenta con una sede principal y 13 sedes remotas. Se muestran los scripts de configuración de las herramientas de calidad de servicio implementadas en los routers CPE, en el equipo de acceso de proveedor y en el equipo PE del proveedor (solo se consideró los scripts de la sede principal y una sede remota).

En la parte final del capítulo III, se muestra las capturas del consumo de ancho de banda en tiempo real por cada clase de servicio, se muestra la cantidad de paquetes que se descartan por clase de servicio.

CAPITULO II
MARCO TEÓRICO CONCEPTUAL

2.1. Definición de Calidad de servicio

En Networking, calidad de servicio (QoS) describe una gran variedad de conceptos y herramientas que pueden utilizar los paquetes para acceder a algún servicio.

Calidad de servicio se define como la habilidad de la red de proveer un mejor o especial servicio a un conjunto de usuarios o aplicaciones en detrimento de otros usuarios o aplicaciones.

En la actualidad se cuenta con dos arquitecturas para la implementación de calidad de servicio, se tiene la arquitectura de Servicios Diferenciados (DiffServ) y la Arquitectura de Servicios Integrados (IntServ), más adelante en el presente capitulo se describe las dos arquitecturas.

2.2. Características del tráfico y las herramientas de QoS que las pueden influenciar

Son cuatro las características del tráfico que las herramientas de QoS pueden influenciar: ancho de banda, delay, jitter y pérdida de paquetes.

Las herramientas de QoS pueden mejorar estas características para algún flujo de tráfico, las mismas herramientas pueden degradar el servicio para otro flujo por lo que se debe entender que es lo que necesita cada aplicación.

2.2.1. Ancho de banda

Cantidad de información que se transmite en un periodo de tiempo determinado desde un punto a otro, define la capacidad del medio de transmisión.

La falta de ancho de banda ocasiona que las aplicaciones se degraden debido al retraso y a la pérdida de paquetes.

Existen herramientas de QoS que pueden influenciar el ancho de banda.

La mejor herramienta de QoS para problemas de ancho de banda es más ancho de banda, sin embargo más ancho de banda no resuelve todos los problemas. En redes convergentes (redes con voz, video, y data), agregar más ancho de banda puede enmascarar problemas de delay que son resueltos a través de otras herramientas de QoS o a través de un mejor

diseño de QoS.

Algunas herramientas de QoS mejoran el ancho de banda reduciendo el número de bits requeridos para transmitir la data lo que se conoce como compresión.

La otra herramienta de QoS que directamente afecta el ancho de banda es Control de Admisión de Llamada (CAC). CAC decide si la red puede aceptar una nueva llamada de voz y video.

Las herramientas de encolamiento pueden afectar la cantidad de ancho de banda que cierto tipo de tráfico recibe. Las herramientas de encolamiento crean múltiples colas, y los paquetes son tomados de las colas basados en algún algoritmo de programación (scheduling). El algoritmo de programación puede incluir una característica que garantice una mínima cantidad de ancho de banda a una cola particular.

A continuación se describe cada una de las herramientas mencionadas anteriormente que influencian el ancho de banda:

a) Compresión

Reduce la cantidad de bits para transmitir los datos.

La compresión reduce la utilización del ancho de banda, haciendo paquetes más pequeños antes de la transmisión. Existen dos tipos de herramientas de compresión, las cuales son las de compresión de la carga y las de compresión de la cabecera. Las herramientas de compresión de carga comprimen el "paquete", la porción del frame de enlace de datos entre la cabecera frame y el tráiler. Las herramientas de compresión de la cabecera comprimen solo los encabezados.

Una vez realizada la compresión, no se puede obtener la señal original, aunque sí una aproximación a la señal original, dependerá del tipo de compresión.

A continuación en la tabla siguiente se muestra algunos codecs de compresión de voz y el respectivo ancho de banda que requiere por llamada telefónica.

Tabla 2.1 Codecs de compresión de voz

CODEC	Ethernet 14 Bytes of Header	PPP 6 Bytes of Header	ATM 53 Bytes Cells With a 48 Bytes Payload	Frame Relay 4 Bytes of Header
G.711 at 50 pps	85.6 kbps	82.4 kbps	106 kbps	81.6 kbps
G.711 at 33 pps	77.6 kbps	75.6 kbps	84 kbps	75 kbps
G.729A at 50 pps	29.6 kbps	26.4 kbps	42.4 kbps	25.6 kbps
G.729A at 33 pps	22.2 kbps	20 kbps	28 kbps	19.5 kbps

b) Control de Acceso de Llamadas (CAC):

Esta herramienta decide si la red puede aceptar una nueva llamada de voz y video. El permiso puede basarse en varios factores, varios de estos factores involucran una medida del ancho de banda.

c) Herramientas de gestión de colas:

Pueden afectar la cantidad de ancho de banda que ciertos tipos de tráfico reciben. Las herramientas de gestión de colas crean varias colas, y luego los paquetes se ponen sobre cada cola en base a un algoritmo de programación. El algoritmo de programación podría incluir una característica que garantice una cantidad mínima de ancho de banda para una determinada cola.

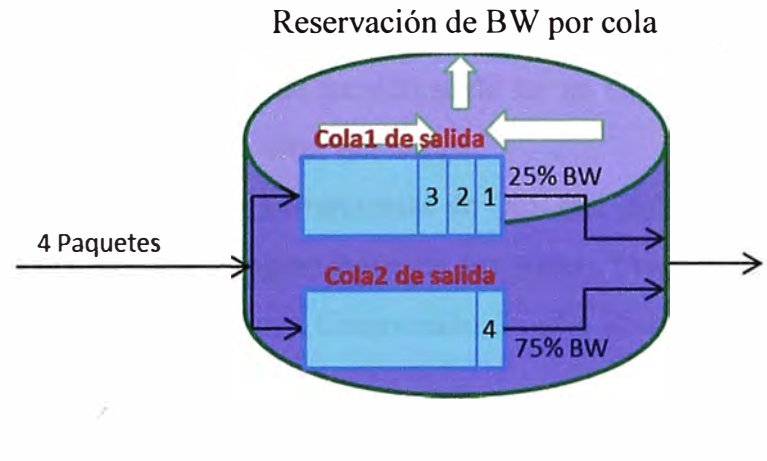

Figura 2.1 Reservación de BW usando herramientas de QoS de encolamiento

2.2.2. Delay

Todos los paquetes en una red experimentan algún delay entre cuando el paquete es enviado por primera vez y cuando este arriba a su destino.

El retardo de extremo a extremo que experimenta un paquete está constituido por los delays de: serialización, propagación, encolamiento, envió/procesamiento, Códec y compresión.

a) Delay de serialización

Es el tiempo que toma en poner los bits de un frame en el medio físico, se encuentra en función del tamaño del frame y de la velocidad del enlace.

Calculo del delay de serialización:

$$Tamaño\ del\ paquete\ (byte) \times 8 / Velocidad\ del\ enlace\ (bps) \qquad (2.1)$$

b) Delay de propagación

Define el tiempo que tarda en llegar un único bit de un extremo del enlace hasta otro. El delay de propagación ocurre cuando un bit atraviesa el enlace físico.

La única variable que afecta el delay de propagación es la longitud del enlace.
Forma para calcular el delay de propagación:

$$Longitud\ del\ enlace\ (metros)/(\ 2.1 \times \frac{10^8 metros}{segundo}) \qquad (2.2)$$

c) Delay de encolamiento

Consiste en el tiempo en las colas que un paquete tiene que esperar en el interior de un dispositivo, generalmente solo en las colas de salida del router ya que la cola de entrada suele ser insignificante en la entrada de un router. El delay de encolamiento puede ser grande, puede estar alrededor de cientos de milisegundos o mucho más.

d) Delay de reenvío

Es el tiempo de procesamiento entre cuando el frame es totalmente recibido y es puesto en la cola de salida. El delay de reenvió suele ser un componente pequeño como para no ser considerado en el cálculo total del retraso.

Se cuenta con las siguientes herramientas de QoS que influencian en el delay de reenvió: Encolamiento (lógica de programación de las colas), Fragmentación e intercalado (Link Fragmentation and Interleaving), Compresión, Traffic Shaping.

- **Encolamiento:**

Consiste en crear varias colas en la cuales se colocan los paquetes y luego se eligen los paquetes en las diferentes colas, algunos paquetes dejaran el router antes que otros por lo que algunos paquetes tendrán que esperar más tiempo. Se puede disminuir el retraso de los paquetes sensibles al retardo y aumentar el retraso a los paquetes poco sensibles al retardo.

- **Fragmentación e intercalado:**

El tiempo requerido para serializar un paquete está en función de la velocidad del enlace, y el tamaño del paquete. LFI (Link Fragmentation and Interleaving) fragmenta paquetes grandes en más pequeños antes de ser enviados, esto permite que pequeños paquetes sensibles al retardo sean enviados luego del envió de un pequeño fragmento sin tener que esperar que todo un paquete grande sea enviado.

- **Compresión**

La compresión toma un paquete, o cabecera de un paquete, y comprime los datos para que utilice menos bits.

La compresión reduce el delay de serialización, por que el número de bits usados para enviar un paquete decrece. Sin embargo, el delay puede también incrementarse por el tiempo de procesamiento que toma la compresión y descompresión del paquete.

- **Traffic Shaping**

Traffic Shaping actualmente incrementa el delay, en un esfuerzo por reducir la pérdida de paquetes.

2.2.3. Jitter

Paquetes consecutivos que experimentan diferentes tiempos de retraso se dice que experimentan jitter.

En una red de paquetes, con componentes de delay variables, el jitter siempre ocurre. Típicamente, las aplicaciones de datos experimentan algún jitter, y este no causa degradación. Algunos tráficos como voz digitalizada, requiere que los paquetes sean transmitidos de manera coherente y uniforme (por ejemplo cada 20 ms). Los paquetes deben de llegar a su destino con el mismo espacio entre ellos. (Este tipo de tráfico es llamado tráfico asíncrono).

La voz y el video se degradan rápidamente cuando ocurre el jitter. Las aplicaciones de Datos suelen ser más tolerantes al jitter, aunque largas variaciones de jitter afectan a aplicaciones interactivas.

Agregar más ancho de banda ayuda a reducir el jitter, esto debido a que ayuda a reducir el delay, entonces el jitter también será menor. Más ancho de banda decrece el delay de serialización, por lo que decrecerá el jitter. No todos los problemas de jitter se resuelven aumentando el ancho de banda.

Varias herramientas de QoS mejoran el jitter, pueden decrecer el jitter para un conjunto de paquetes o pueden incrementar el jitter para otros.

Herramientas de QoS que influencian el jitter: Encolamiento, Fragmentación e intercalado (Link Fragmentation and Interleaving), Compresión, Traffic Shaping.

a) Encolamiento

Permite ordenar los paquetes para que los paquetes con mayor sensibilidad al delay salgan primero que los paquetes con menor sensibilidad al delay.

b) Fragmentación e intercalado

LFI fragmenta paquetes grandes en pequeños paquetes antes de enviarlos. Paquetes pequeños sensitivos al delay pueden ser enviados después de un pequeño fragmento, en lugar de tener que esperar a que un paquete de mayor tamaño original sea serializado.

c) Compresión

Reduce el número de bit requeridos para transmitir la data. Requiriendo menos ancho de banda, las colas se reducen, lo cual reduce el delay. También el delay de serializacion se

reduce, porque se requiere menos bits. La compresión también agrega algún delay de procesamiento.

d) Trafic shaping

Artificialmente incrementa delay para reducir el descarte de paquetes.

2.2.4. Pérdida de paquetes

La pérdida de paquetes por errores de bits es pequeña, típicamente una tasa de BER es menor a 10^-9, la perdida de paquetes más grande se puede dar en la pérdida de un buffer o de una cola completa.

El término "tail-drop" se refiere cuando un router descarta un paquete debido a que la cola se encuentra llena.

Son pocas las herramientas de QoS que pueden ayudar con problemas de perdida de paquetes. Mayor ancho de banda ayuda pero no resuelve todos los problemas, más ancho de banda permite que los paquetes sean transmitidos con más rapidez, reduciéndose la longitud de las colas.

A continuación se describe dos herramientas que ayudan a evitar la pérdida de paquetes.

a) Encolamiento

Implementando colas más largas se aumenta el retraso pero se reduce la pérdida de paquetes.

b) Randon Early Detection (RED)

Implementando RED los paquetes son descartados aleatoriamente antes de que la cola se llene. Esto reduce la congestión de las colas, mientras que afecta solo a algunos usuarios

2.3. Características del tráfico de voz, video y datos

Las aplicaciones tienen distintos requerimientos de ancho de banda, delay, jitter y pérdida de paquetes. Con QoS una red pude proveer mejor los recursos de QoS para cada aplicación.

2.3.1. Características del tráfico de video

Se requiere que el tráfico de video sea transmitido en un sentido con un delay no mayor a 150 ms, el jitter debe ser menor a 30 ms y como máximo se puede tener una pérdida de paquetes menor al 1%. Se debe de contar con un ancho de banda garantizado por llamada de video-stream más 10-20% Kbps. El Control de Acceso de llamadas debe estar habilitado.

2.3.2. Características del tráfico de voz

El tráfico de voz debe de tener un delay de extremo a extremo menor a 150ms, el jitter

debe ser menor a 30ms y la pérdida de paquetes debe ser menor al 1%. El Control de Acceso de llamadas debe estar habilitado.

2.3.3. Características de tráfico de Datos

Diferentes aplicaciones tienen diferentes características de tráfico, diferentes versiones de una misma aplicación pueden tener diferentes características de tráfico.

Los Datos se pueden clasificar en cinco modelos de clases:

- Misión-critica apps: se encuentra el tráfico crítico del negocio de la empresa (aplicaciones cliente servidor).
- Transaccional/interactiva apps: se encuentra el tráfico de aplicaciones interactivas
- Bulk data apps: se encuentra el tráfico FTP, e-amil, backups, contenido de distribución.
- Best effort apps: Tráfico class default
- Opcional Scavenger apps: Tráfico peer-to-peer apps, tráfico de juegos.

2.4. Requerimiento de Calidad de Servicio de las aplicaciones

A continuación se muestra los requerimientos en cuanto a calidad de servicio de distintas aplicaciones.

Tabla N° 2.2 Requerimiento de QoS de algunas aplicaciones

Aplicación	Fiabilidad	Retardo	Jitter	Ancho de Banda
Correo electrónico	Alta (*)	Alto	Alto	Bajo
Transferencia de ficheros	Alta (*)	Alto	Alto	Medio
Acceso Web	Alta (*)	Medio	Alto	Medio
Login remoto	Alta (*)	Medio	Medio	Bajo
Audio bajo demanda	Media	Alto	Medio	Medio
Video bajo demanda	Media	Alto	Medio	Alto
Telefonía	Media	Bajo	Bajo	Bajo
Videoconferencia	Media	Bajo	Bajo	Alto

2.5. Arquitectura de Servicios Diferenciados (DiffServ)

La arquitectura de servicios diferenciados se basa en un modelo simple donde el tráfico que ingresa a la red es clasificado y posiblemente acondicionado en la frontera de la red, y asignado a diferentes BA ("*behavior aggregates*"). Cada *behavior aggregate* es identificado por un simple DS codepoint (*DiffServ Codepoint* " DSCP"). Dentro del core de la red los paquetes son enviados de acuerdo al PHB (comportamiento por salto " *per-hob-behavior*") asociado con el DS codepoint. El PHB es el comportamiento de reenvió de un paquete externamente observable en un nodo que aplica DiffServ.

En la Arquitectura DiffServ los paquetes de datos se colocan en un número limitado de

clases de tráfico, cada router en la red está configurado para diferenciar el tráfico en función de su clase. Cada clase de tráfico se puede manejar de diferente manera, se garantiza un trato preferencial para el tráfico de mayor prioridad en la red.

Los router en un dominio diffserv ponen en práctica el comportamiento por salto, que define las propiedades de envió de los paquetes asociados con una clase de tráfico.

Diferentes PHBs se pueden definir para ofrecer, por ejemplo, baja pérdida, baja latencia de envió o envió con el mejor esfuerzo.

Todo el tráfico que fluye a través de un router que pertenece a la misma clase se conoce como un agregado comportamiento (BA).

Los valores DSCP marcan los paquetes para seleccionar un PHB. Dentro del núcleo de la red, los paquetes se transmiten de acuerdo con el PHB que está asociado con el DSCP.

Los servicios diferenciados se definen según la IETF en las RFCs que se listan a continuación:

- RFC 2474 "Definition of the Differentiated Services Fiel (DS Field) in the IPv4 and IPv6 Headers".

Contiene los detalles del campo de 6-bits DSCP en la cabecera IP.

- RFC 2475 "An Architecture for Differentiated Service".

Este es el documento de conceptos básicos de DiffServ.

- RFC 2597 "Assured Forwarding PHB Group"

Define un juego de 12 DSCP valores y una convención para su uso.

- RFC 2598 "An Expedited Forwarding PHB"

Define un solo valor DSCP como una convención para usar como una clase de baja latencia.

- RFC 3260 "New Terminology and Clarifications for DiffServ"

Aclaran pero no sustituyen las RFCs DiffServ existentes.

2.5.1. Dominio de servicios diferenciados (DS dominio)

Un dominio de servicios diferenciados es un conjunto de nodos DS (nodo que soporta servicio diferenciado) que operan con una política de aprovisionamiento de servicios común y un conjunto de grupos PHB (per-hop behavior) implementados en cada nodo. Un dominio DS tiene un límite bien definido que consiste en nodos DS frontera que clasifican y posiblemente acondicionan el tráfico que ingresa para garantizar que los paquetes que transitan en el dominio sean apropiadamente marcados para seleccionar un PHB de uno de los grupos PHB soportados en el dominio. Los nodos en el dominio DS seleccionan el

comportamiento de envió de los paquetes en función de su DS codepoint, y lo hacen mapeando el valor de cada uno de los soportados PHBs con los correspondientes valores del DSCP.

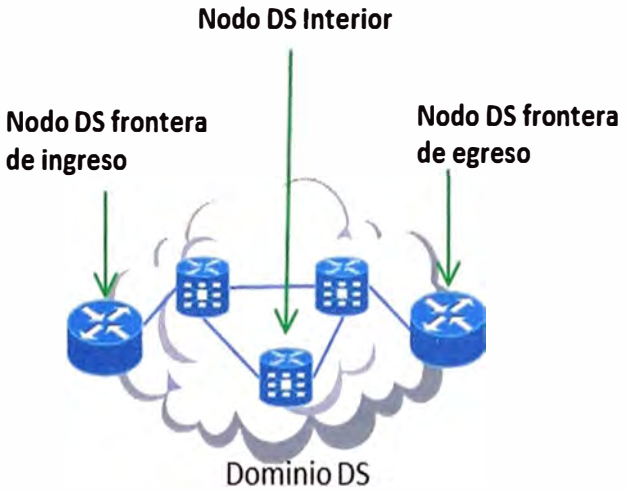

Fig.2.2 Dominio DS

a) Nodos DS frontera y nodos DS interiores

Un dominio DS consiste de nodos DS frontera y nodos DS interiores. Los nodos DS frontera interconectan los dominios DS con otros dominios DS o también pueden conectarse con otros dominios que no soportan servicios diferenciados. Los nodos DS interiores solo se conectan a otros nodos DS interiores o frontera dentro del mismo dominio DS.

Ambos nodos DS frontera e interiores deben ser capaces de aplicar el apropiado PHB a los paquetes basados en el DS codepoint, además los nodos frontera pueda ser que requieran ejecutar condicionamiento del tráfico.

Los nodos interiores pueden ser capaces de realizar funciones limitadas de acondicionamiento de tráfico como remarcado de DS codepoint. Los nodos interiores que implementan funciones más complejas de clasificación y condicionamiento de tráfico son análogos a nodos DS frontera.

b) Nodo DS de ingreso y egreso

Los nodos DS frontera actúan como un nodo DS de ingreso y egreso para tráfico en diferentes direcciones. El tráfico ingresa a un dominio DS en el nodo DS de ingreso y deja el dominio DS en el nodo DS de egreso. Un nodo DS de ingreso es responsable de asegurar que el tráfico que entra en el dominio DS se ajuste a cualquier Acuerdo de Acondicionamiento de Tráfico (TCA) entre él y el otro dominio al que está conectado el nodo de ingreso. Un nodo DS de egreso puede realizar funciones de acondicionamiento de

tráfico que se envía a un dominio conectado directamente, dependiendo de los detalles del TCA entre los dos dominios. Hay que notar que un nodo frontera puede actuar como un nodo interior para un conjunto de interfaces.

c) Región de servicios diferenciados

Una región de servicios diferenciados (DS región) es un conjunto de uno o más dominios DS contiguos. DS regiones son capaces de soportar servicios diferenciados a lo largo de las rutas que abarcan los dominios de la región.

El dominio DS en una región DS puede soportar diferentes grupos PHB internamente y diferentes codepoint asociados a PHBs. Sin embargo, para permitir servicios que se extienden a través de los dominios, los dominios de interconexión deben establecer un Acuerdo de Nivel de Servicio (SLA) que defina un TCA (acondicionamiento de tráfico acordado) que especifique como es acondicionado el tráfico que transita de un dominio DS en la frontera entre los dos dominios.

Es posible que varios dominios DS dentro de una región DS puedan adoptar una común política de aprovisionamiento de servicio y poder soportar un conjunto de grupos PHB mapeados a codepoint, eliminando la necesidad de acondicionamiento de tráfico entre esos dominios.

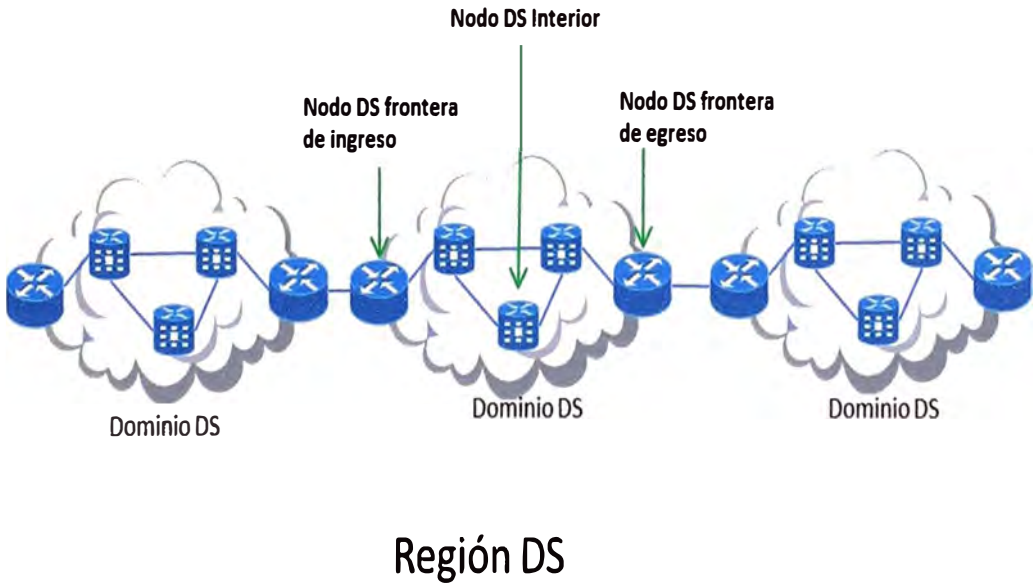

Fig.2.3 Región DS

2.5.2. Clasificación y acondicionamiento de tráfico

El SLA puede especificar las reglas de clasificación y re-marcado de paquetes y también puede especificar los perfiles de tráfico y las acciones a flujos de tráfico que están en o fuera del perfil. El TCA entre los dominios es derivado de estos SLA.

Las políticas de clasificación de paquetes identifican el subconjunto de tráfico que puede recibir un servicio diferenciado por la que están acondicionados y/o asignados a uno o más comportamientos agregados (por remarcado DS codepoint) dentro del dominio DS.

El acondicionamiento de tráfico realiza medición, shaping, policing y/o re-marcado para asegurar que el tráfico que ingresa al dominio DS cumple con las normas especificadas en el TCA, de acuerdo con la política de aprovisionamiento de servicios del dominio. Las extensiones de acondicionamiento de tráfico requeridas dependen de los detalles de la oferta de servicios, y puede variar desde un simple remarcado de codepoint a complejas operaciones de policing y shaping.

a) Clasificadores

Los clasificadores de tráfico seleccionan paquetes en un flujo de tráfico basados en el contenido de alguna porción de la cabecera del paquete. Se define dos tipos de clasificadores. El BA (Behavior Aggregate) clasificador clasifica paquetes basado solo en el DS codepoint. El MF (Multi-campo) clasificador selecciona paquetes basados en la combinación de valores de uno o más campos de la cabecera, como son dirección de origen, dirección destino, campo DS, ID del protocolo, número de puerto origen y destino, y otra información como interface de entrada.

b) Perfil de tráfico

Un perfil de tráfico especifica las propiedades temporales de un flujo de tráfico seleccionado por un clasificador. Provee reglas para determinar si un paquete particular está dentro o fuera de un perfil.

El perfil de tráfico es un componente opcional de un TCA y su uso depende de las especificaciones del servicio ofrecido y las políticas de aprovisionamiento del servicio en el dominio.

c) Acondicionadores de tráfico

Un acondicionador de tráfico puede contener los siguientes elementos: medidores, marcadores, shaper, y dropper. Un flujo de tráfico es seleccionado por un clasificador, que conduce los paquetes a una instancia lógica de un acondicionador de tráfico. Un medidor es usado (si procede) para medir el flujo de tráfico contra un perfil de tráfico. El estado de un medidor con respecto a un particular paquetes puede ser usado para afectar una acción de marcado, dropping, o shaping.

Cuando un paquete sale del acondicionador de tráfico de un nodo DS frontera el DS codepoint de cada paquete se debe establecer a un valor apropiado.

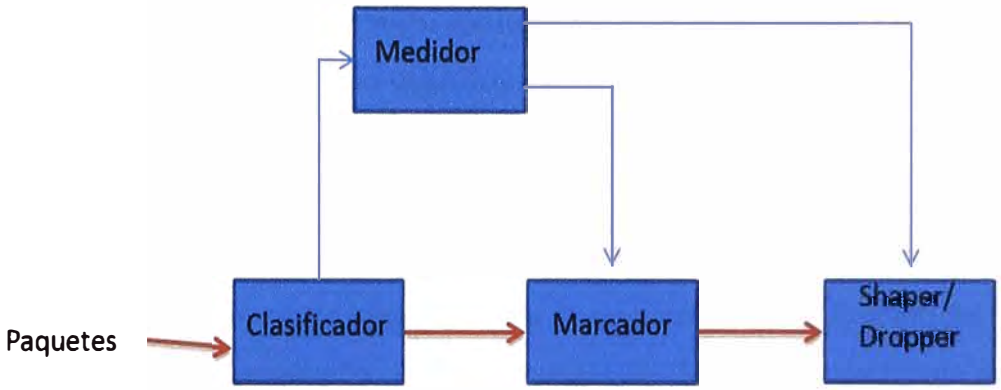

Fig.2.4 Muestra la lógica de clasificación y acondicionado de tráfico

- **Medidores**

Los medidores de tráfico miden las propiedades temporales del flujo de paquetes seleccionados por un clasificador contra un perfil de tráfico especificado en un TCA. Un medidor pasa la información de estado a las funciones de acondicionamiento para desencadenar una particular acción para cada paquete dentro o fuera del perfil.

- **Marcadores**

Los marcadores de paquetes establecen el campo DS de un paquete a un particular codepoint, agregando el paquete marcado a un particular DS Comportamiento Agregado (BA). El marcador puede ser configurado para marcar todos los paquetes con un único codepoint particular, o puede ser configurado para marcar un paquete a una de un conjunto de codepoint usados para seleccionar un PHB en un grupo de PHB, acorde con el estado de un medidor. Cuando un marcado cambia el codepoint en un paquete se dice que se a re-marcado el paquete.

- **Moldeador (Shapers)**

El modelador retrasa alguno o todo los paquetes de un flujo de tráfico para cumplir con el perfil de tráfico. Un modelador usualmente tiene un buffer de tamaño finito, y los paquetes pueden ser descartados si es que no hay suficiente espacio en el buffer para almacenar los paquetes retrasados.

- **Descartadores (droppers)**

Los droppers descartan alguno o todos los paquetes de un flujo de tráfico con el fin de que el flujo cumpla con el perfil de tráfico. Este proceso es conocido como "policing (control)" del flujo. Notar que un dropper puede ser implementado como caso especial de un shaper configurando el tamaño del buffer del shaper a cero paquetes.

2.5.3. Localización de Acondicionadores de tráfico y Multi-clasificadores

Los acondicionadores de tráfico son usualmente localizados en los nodos DS frontera

de ingreso y egreso, pero puede también ser localizado en nodos dentro del interior de un dominio DS, o en un dominio que no tiene capacidades de servicio diferenciado.

a) Dentro del dominio origen

Se define el dominio de origen, como el dominio que contiene el nodo o los nodos que originan el tráfico recibiendo un particular servicio. Las fuentes de tráfico y los nodos intermedios dentro de un dominio origen pueden llevar a cabo la clasificación del tráfico y las funciones de acondicionamiento. El tráfico originado de un dominio fuente puede ser marcado directamente por la fuente de tráfico o por nodos intermedios antes de dejar el dominio fuente. Esto es referido como un inicial marcado o pre-marcado.

Hay algunas ventajas de marcar los paquetes cerca de la fuente de tráfico. Primero, una fuente de tráfico puede tomar en cuenta más fácilmente las preferencias de las aplicaciones cuando decide que paquetes deben recibir un mejor trato de envío. También la clasificación de paquetes es mucho más simple antes de que el tráfico sea agregado con paquetes de otras fuentes, reduciéndose el número de reglas de clasificación que se necesitan aplicar dentro de un nodo.

Dado que el marcado de paquetes se puede distribuir en múltiples nodos, el dominio DS fuente es responsable de asegurar que el tráfico agregado hacia el dominio DS del proveedor conforme el apropiado TCA.

El nodo frontera del dominio fuente debe supervisar la conformidad del TCA, y de controlar, dar forma, o remarcar los paquetes según sea necesario.

b) En la frontera de un dominio DS

El flujo de tráfico debe ser clasificado, marcado, y acondicionado en cualquiera de las fronteras del enlace. El SLA entre los dominios debería especificar que dominio tiene la responsabilidad de mapear el flujo de tráfico en un DS Comportamiento Agregado (DS BA) y del acondicionamiento de esos agregados en conformidad con el apropiado TCA. Sin embargo, un nodo DS de ingreso debe poder asumir que el tráfico que ingresa puede no estar conforme con el TCA y debe estar preparado para hacer cumplir el TCA de acuerdo con la política local.

c) En dominios que no cuentan con capacidades de servicios diferenciados

Fuentes de tráfico o nodos intermedios en un dominio que no tiene capacidades de servicios diferenciados pueden emplear acondicionadores de tráfico para pre-marcar el tráfico antes de llegar al ingreso de un dominio DS. De este modo, las políticas locales para la clasificación y el marcado pueden ser ocultadas.

d) En nodos DS interiores

Aunque la arquitectura básica asume que la clasificación compleja y funciones de acondicionamiento son localizadas solo en los nodos de ingreso a la red y los nodos de frontera de egreso, la implementación de estas funciones en el interior de la red no es excluyente.

2.5.4. Comportamiento en cada salto (Per-Hop Behaviors)

Un per-hop behavior (PHB) es una descripción del externamente observable comportamiento de envío de un nodo DS aplicado a un particular DS behavior aggregate (BA). El PHB es el medio por el cual un nodo asigna recursos a los behavior aggregates, y es la parte superior de esta base "hop-by-hop" mecanismo de asignación de recursos útiles.

Dos de las RFCs DiffServ, 2597 y 2598, son dedicadas a describir un juego de valores DSCP, y algunas sugerencias PHBs que pueden ser asociados con cada valor DSCP.

IP define un byte tipo de servicio (ToS) en la RFC 791, que salió en setiembre de 1981. Los creadores del protocolo IP entendieron el byte ToS para ser usado como un campo a marcar en un paquete para el tratamiento con herramientas de QoS. Dentro del byte ToS, los 3 primeros bits fueron definidos como un campo llamada IP Precedence, que puede ser marcado para los propósitos de implementación de una particular clase de servicio. El valor del campo de precedencia implica que el valor mayor, el trafico más importante. Se dieron los siguientes nombres a cada valor de IP precedence: de rutina (precedencia 0), para critico (precedencia 5) y control de red (precedencia 7).

En adición a el campo precedencia, el byte ToS incluye otro campo flag que se activa o desactiva para implicar un particular QoS servicio – por ejemplo, bajo o elevado delay puede señalarse por un 1 ó 0 en el bit delay. Los bits de 3 a 5 (RFC 795) comprenden en campo ToS dentro del byte ToS, los flags para rendimiento, delay, y confiabilidad. RFC 1349 expande el campo ToS de 3 bits a 6 bits, adicionando el flag costo. Por ejemplo, los creadores del byte ToS original previeron la habilidad de seleccionar una ruta diferente, usando un enlace más confiable, para paquetes con el flag confiabilidad seteado.

El campo DS redefine el byte ToS en la cabecera IP. Si se remueve la definición de los 4 bits ToS (bits 3 a 6). DiffServ crea un reemplazo para el campo Precedencia con un nuevo campo de 6 bits llamado el campo "Differentiated Services (DS)". (Los 2 bits restantes son usados como bits de control de flujo con una característica de "Notificacion Explicita de la Congestión (ECN)", como se especifica en la RFC 3168.

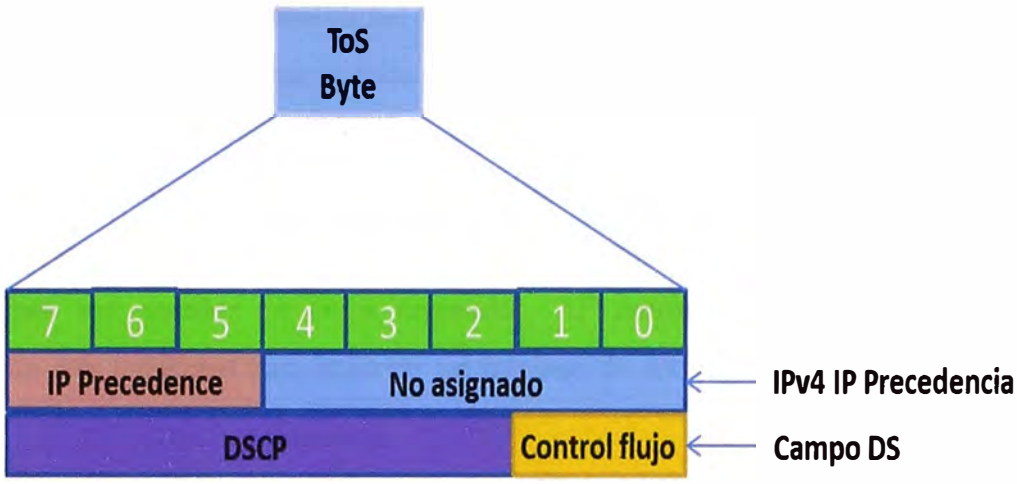

Fig.2.5 Campos dentro del byte ToS y el campo DS

Existen cuatro tipos de PHB con los valores DSCP:

a) Class Selector PHB y los valores DSCP

Usa 8 DSCP con valores de ceros en los tres últimos bits. Usado para la compatibilidad con IP precedence.

La lógica que utiliza es: el valor más alto de DSCP obtiene el mejor trato de QoS.

TABLA N° 2.3 Valores DSCP Class Selector

Nombre de DSCP Class Selector	Valor DSCP binario	Valor precedence equivalente
Default	000000	0
Class 1	001000	1
Class 2	010000	2
Class 3	011000	3
Class 4	100000	4
Class 5	101000	5
Class 6	110000	6
Class 7	111000	7

b) PHB por defecto

Con los 3 bits más significativos puestos en cero del IP precedence y DSCP se obtiene un resultado best-effort. Este PHB no brinda un tratamiento específico de calidad de servicio.

c) Assured Forwarding PHB y valores DSCP

La RFC 2597 define el "assured forwarding per-hop behavior". Esta RFC sugiere que un buen diseño DiffServ debe permitir cuatro diferentes clases de colas. Cada cola, debe implementar tres niveles de probabilidad de descarte.

Un individual PHB describe que sucede en un simple salto, típicamente un router. En el caso de AF (Assured Forwarding), cada PHB contiene dos QoS funciones separadas, típicamente realizadas por dos herramientas QoS diferentes. La primera función es encolamiento, cada router clasifica los paquetes en cuatro diferentes clases, y los paquetes de cada clase son puestos en colas separadas. AF también especifica el método de encolamiento con habilidad para reservar un mínimo de ancho de banda configurado por cada clase.

El AF PHB define "Congestion Avoidance (evitar la congestión)" como el segundo comportamiento que comprende el AF PHB. Los routers descartan paquetes cuando una cola está llena y el router necesita colocar paquetes en la cola; esta acción es llamada tail drop. Las herramientas para evitar la congestión descartan paquetes antes de que el tail drop sea requerido, con la esperanza de que menos paquetes sean descartados.

El AF PHB no define una garantía de que cada paquete será entregado, ni implica alguna forma de recuperación de errores.

Para marcar los paquetes, 12 valores DSCP son necesitados, el nombre de estos valores inician con AF (assured forwarding). AFxy son los nombre para los valores DSCP, donde el valor de "x" indica una de las cuatro clases (ninguna clase tiene ventaja sobre la otras, depende del modo de configuración) e "Y" indica la probabilidad de descarte del paquete, cuanto más bajo valor de "Y" se tiene menos probabilidad de descarte.

TABLA N°2.4 Lista los valores DSCP Assured Forwarding.

Clase	Probabilidad baja de descarte	Probabilidad media de descarte	Probabilidad alta de descarte
Class 1	AF11	AF12	AF13
Class 2	AF21	AF22	AF23
Class 3	AF31	AF32	AF33
class 4	AF41	AF42	AF43

Los valores binarios DSCP indican la clase de cola con los 3 primeros bits, y la preferencia de dropeo se indica con los dos bits siguientes.

Cada clase AFx es compatible con un valor IP precedence.

TABLA N° 2.5 Lista los valores decimal y binario de DSCP Assured Forwarding.

Clase	Probabilidad baja de descarte	Probabilidad media de descarte	Probabilidad alta de descarte
Class 1	AF1 1 DSCP 10 001010	AF12 DSCP 12 001100	AF13 DSCP 14 001110
Class 2	AF21 DSCP 18 010010	AF22 DSCP 20 010100	AF23 DSCP 22 010110
Class 3	AF31 DSCP 26 011010	AF32 DSCP 28 011100	AF33 DSCP 30 011110
class 4	AF41 DSCP 34 100010	AF42 DSCP 36 100100	AF43 DSCP 38 100110

d) Expedited Forwarding PHB y valores DSCP

La RFC 2598 define el comportamiento expedited forwarding per-hop. Esta RFC define un muy simple PHB (baja latencia, con un límite de ancho de banda), y usa un solo DSCP (EF) para representar esto, el nombre de este DSCP es EF cuyo valor binario es 101110 con un valor decimal de 46.

PHB EF tiene dos componentes: encolamiento que provee bajo delay, jitter, pérdida y además garantizar una cantidad de ancho de banda, y el otro componente son las políticas que permiten prevenir que otros tipos de tráfico ocupen el ancho de banda.

2.6. Servicios Integrados (IntServ)

IntServ define un proceso de señalización por cada flujo individual, puede requerir que la red reserve ancho de banda y delay necesarios para el flujo.

El proveedor garantiza por flujo, la IntServ RFC 1633 describe dos componentes: reservación de recursos y control de admisión. La reservación de recurso señala a los elementos de red sobre cuanto ancho de banda y delay necesita un particular flujo. Si la señalización se completa satisfactoriamente, los varios componentes de red tienen la necesidad de reservar ancho de banda. El conjunto de nodos IntServ reservan la cantidad apropiada de ancho de banda y delay en respuesta a los mensajes de señalización.

IntServ control de admisión decide cuando un requerimiento de reservación puede ser rechazado. Si todos los requerimientos son aceptados, eventualmente mucho tráfico puede ser introducido en la red, y ninguno de los flujos puede obtener el servicio requerido.

InteServ usa el protocolo Resource Reservation (RSVP) para la señalización de reservación del ancho de banda, la señalización se realiza al inicio del envío del flujo y

durante el envió para asegurarse que el flujo continúe recibiendo la necesaria cantidad de ancho de banda. La reservación de recursos se realiza salto por salto, sin un salto no tiene los recursos disponibles el flujo tendrá que esperar.

2.7. DiffServ en Cisco IOS

El modelo DiffServ solo define el uso de los DSCP y los cuatro PHBs. El PHBs describe el comportamiento de envió de un nodo DS. El modelo no especifica como los PHBs deben ser implementados. Una variedad de técnicas de encolamiento, policing, medición y shaping pueden ser usadas para efectos de habilitar el acondicionamiento de tráfico y PHBs.

2.7.1.Herramientas de QoS en IOS

a) Clasificación y marcado

Las herramientas de QoS clasificación categoriza paquetes examinando el contenido del frame, cell, y cabecera de los paquetes, mientras que la herramientas de marcación permite cambiar la cabecera del paquete para una fácil clasificación.

Clasificación involucra diferenciar un paquete de otro, típicamente examinando campos dentro de cabecera.

Después de la clasificación, una herramienta de QoS puede tratar a los paquetes en una clase diferente a los demás.

Por ejemplo para solo dar preferencia al tráfico de VoIP sobre otro tráfico, la herramienta de encolamiento necesita clasificar el tráfico en una de las dos categorías: VoIP o no-VoIP.

Debido a que la mayoría de herramientas de QoS necesitan diferenciar entre paquetes, la mayoría de herramientas de QoS tienen la característica de clasificación.

Algunas herramientas de QoS permiten que se puedan clasificar usando ACL.

La lógica general para la clasificación y marcado del tráfico entrante puede ser descrito como sigue:

- Para los paquetes que ingresan en una interfaz y cumplen con el criterio 1, entonces se marca un campo con un valor.

- Si el paquete no coincidió, entonces se pasa a comparar con el criterio 2, y luego se marca un campo potencialmente diferente con un potencialmente diferente valor.

- Sigue buscando hasta encontrar una coincidencia.

- Si el paquete no coincide, no hay acciones específicas que se toman con el paquete, el paquete es reenviado como si no se hubiera configurado calidad de servicio.

Marcar involucra setear algunos bits dentro de la cabecera del frame de enlace de la cabecera del paquete de la capa de red, con el objetivo de las herramientas de calidad de servicio de otros dispositivos clasifiquen en función del valor de la marca. Se puede marcar una variedad de campos, y cada uno tiene un propósito en particular. Algunos campos son más usados que otros.

Los dos campos de marcado más populares para calidad de servicio son IP Precedence e IP DSCP.

El campo IP Precedence se encuentra localizado en la cabecera IP, tiene una longitud de 3 bits, está contenido en los tres primeros bits del byte ToS.

El campo IP DSCP se encuentra localizado en la cabecera IP y tiene una longitud de 6 bits. Esta contenido dentro de los 6 primeros bits del campo DS, que reemplaza el byte ToS (Type of service).

b) Encolamiento

Provee la habilidad de reordenar los paquetes cuando la congestión ocurre. A veces el encolamiento ocurre en la interface de entrada, llamada " input queuing", la mayoría de métodos de encolamiento solo implementan encolamiento en la salida (output queuing).

Se debe buscar lo siguiente cuando se comparan las herramientas de puesta en cola:

- **Capacidad de clasificación:** particularmente los campos de la cabera de un paquete pueden compararse para clasificar un paquete en una cola particular. En algunos casos, las herramientas de encolamiento automáticamente clasifican el tráfico, mientras que otras herramientas requieren que se configure los valores a ser comparados en los paquetes explícitamente.
- **El máximo número de colas:** algunas veces llamados el máximo número de clases. Si se necesita distinguir entre “X” diferentes tipos de tráfico por encolamiento, se necesita “X” colas.
- **El algoritmo de programación:** para algunas herramientas de encolamiento, Cisco publica el algoritmo usado para decidir que paquete es tomado de que cola.

  Las herramientas de QoS encolamiento, provee una variedad de métodos de encolamiento, más adelante serán descritos con más detalle algunos métodos de encolamiento

En la siguiente tabla se muestra una comparación de los distintos métodos de encolamiento, se compara la cantidad de colas que puede soportar cada método, la capacidad de clasificación y el algoritmo de servicio de la cola.

TABLA N° 2.6 Comparación de métodos de encolamiento

Comparación de métodos de encolamiento			
Método de encolamiento	**máximo número de colas**	**Capacidad de clasificación**	**Algoritmo de servicio de cola/ resultado final del algoritmo**
Priority queuing (PQ)	4	IP ACL, interface de entrada, fragmentos	servicio estricto, siempre sirve a la cola de prioridad-elevada sobre baja cola
Custom queuing (CQ)	16	IP ACL, interface de entrada, fragmentos	sirve a un número configurado de bytes por la cola, por round-robin pasar a través de las colas
Weighted fair queuing (WFQ)	4096	Automático, basado en flujos. (flujos identificados por dirección y numero de puerto fuente/destino, además de tipo de protocolo).	Cada flujo usa una cola diferente. Colas con bajo volumen y mayor IP precedencia obtienen más servicio; volumen elevado, flujos de baja precedencia obtienen menos servicio.
Class-based weighted fair queuing (CBWFQ)	64	IP ACL, NBAR, mismo marcado como CB	No publicado; resultados en un porcentaje de ancho de banda establecido para cada cola con carga
Low latency queuing	N/A	Igual que CBWFQ	LLQ en una variante de CBWFQ, lo que hace es que algunas colas prioridad, siempre obtengan servicio si un paquete está esperando en esa cola.
Modified deficit Round-Robin (MDRR)	8	IP precedence	Similar a CQ, pero cada cola obtiene un porcentaje exacto de ancho de banda, también soporta mecanismos LLQ

c) Shaping y Policing

Shaping y policing proveen dos diferentes funciones, podrá preguntarse por qué shaping y policing están cubiertas aquí al mismo tiempo, las redes que usan policing típicamente necesitan shaping también. También ambos shaping y policing miden la tasa con la que el tráfico se envía y recibe en la red, algunos de las características son subyacentes. Ambos pueden ser descritos usando una metáfora similar a "token buckets". Finalmente, desde una perspectiva de negocios, shaping y policing son típicamente implementados en o cerca del borde entre una empresa y un proveedor de servicios.

Cuando se produce un desajuste de velocidad, el shaping puede ser capaz de reducir la posibilidad de que los paquetes se descarten

Algunas razones detrás de shaping y policing son las siguientes:

- Los paquetes pueden perderse en una WAN multiacceso debido a un desajuste en la tasa de velocidad.
- Traffic shaping pone en cola los paquetes cuando la configuración de la tasa de tráfico excede, demorando estos paquetes, para evitar que probablemente los paquetes se pierdan.
- Policing descarta los paquetes cuando la configuración de la tasa de tráfico es excedida, protegiendo otros flujos de ser invadido por un cliente particular.

Cisco IOS provee como de costumbre varias opciones, se puede considerar algunos factores cuando compares estas herramientas.

Primero no todas las herramientas de shaping y policing soportan protocolos de enlace de datos. Segundo, algunas pueden estar habilitadas en subinterfaces, pero no en un identificador de enlace de datos (DLCI); por lo tanto, en casos donde una red use subinterfaces multipunto, una herramienta puede dar más granularidad para shaping/policing.

d) Evitando la congestión

Cuando una red se congestiona, las colas de salida se empiezan a llenarse. Cuando un paquete nuevo está agregándose a la cola llena, el paquetes es descartado – en un proceso llamado "tail drop". Tail drop sucede en la mayoría de redes cada día, el efecto de la pérdida de paquetes degrada significativamente los flujos de voz y video; para los flujos de datos, la perdida de paquetes causa en la capas mayores la retransmisión para aplicaciones basadas en TCP, que probablemente se incrementa la congestión en la red.

Existen dos soluciones al problema de tail-drop. Una solución es alargar las colas, y por lo tanto disminuir la probabilidad de tail drop. Con largas colas, menos paquetes son descartados, pero el promedio de demora de encolamiento se incrementa. Otra solución requiere a la red para pedir a los dispositivos el retraso del envío de paquetes en la red antes de que las colas se llenen que es exactamente lo que hace la herramienta que evitan la congestión "Congestión Avoidance".

La herramienta de Congestión Avoidance opera bajo la asunción que el descarte de un segmento TCP, causa que el emisor del segmento TCP reduzca la ventana de congestión a un 50 por ciento de la ventana previa.

Si un router experimenta congestión, antes que las colas estén completamente llenas, este puede a propósito descartar varios segmentos TCP, haciendo que algunos emisores TCP reduzcan el tamaño de su ventana. Reduciendo esta ventana TCP, estos particulares emisores envían menos tráfico en la red, dando tiempo al router congestionado para que se recupere. Si las colas continúan creciendo, más segmentos TCP son descartados a propósito, para hacer más lentos a los emisores TCP.

Si las colas son menos congestionadas, el router puede detener el descarte de paquetes.

e) Eficiencia del enlace

La categoría de eficiencia del enlace abarca dos tópicos relacionados: compresión y fragmentación.

La compresión reduce la utilización del ancho de banda, haciendo paquetes más pequeños antes de la transmisión. Dos tipos generales de herramientas de compresión existen en IOS - compresión de la carga y compresión de la cabecera. La compresión de la carga comprime el "paquete "la porción del frame de enlace de datos entre la cabecera frame y tráiler. La compresión de la cabecera comprime solo los encabezados en particular.

Las herramientas de compresión difieren en la cantidad de carga que ellos crean en la CPU y que parte del frame ellos comprimen. Basados en la carga del CPU y que es comprimido, se puede tomar una buena decisión sobre cuando se usa cada herramienta.

La compresión de la carga puede ser aplicada a todos los paquetes, con algunos buenos resultados. Supongamos que el algoritmo de compresión consigue comprimir X bytes de carga útil en la mitad del tamaño – una razonable relación de compresión de 2:1. El router se ahorra mucho ancho de banda con la compresión de un paquete de 1500-bytes en un paquete de 750-bytes. Dada la variación y la naturaleza impredecible del contenido de los paquetes, relaciones de compresión de 2:1 y 4:1 son razonables con Compresión de Carga útil.

La compresión de la cabecera toma ventaja del hecho que las cabeceras que se comprimen son predecibles. Ahora, la compresión de la cabecera solo opera en cabeceras. Por ejemplo, compresión RTP comprime cabeceras IP/UDP/RTP entre 2 y 4 bytes. Para un mínimo tamaño de paquete de 60 bytes, típicamente de llamadas VoIP G. 729, cRTP reduce el paquete de 60 bytes a entre 22 a 24 bytes, una significativa mejora. Ahora la compresión

de la cabecera no provee muchos beneficios para paquetes largos, porque la cabecera forma un pequeño porcentaje del paquete.

La otra categoría mayor de la herramienta de link-efficiency es el "enlace de fragmentación e intercalado" (LFI), también solo llamado fragmentación. El concepto es simple: cuando un router inicia el envió de paquetes, este nunca deja de enviar el paquete para enviar un paquete de mayor prioridad – este finaliza el envió del primer paquete y luego envía el paquete con mayor prioridad. En un enlace lento, el tiempo que toma en serializar un paquete grande puede causar mucho retraso, particularmente para tráfico VoIP y video. Herramientas LFI fragmenta paquetes largos en paquetes pequeños, e intercalan paquetes de elevada prioridad entre los fragmentos. (Cisco recomienda usar LFI cuando la velocidad del enlace es 768 kbps o menos).

La mayoría de herramientas de link-efficiency tienen una específica aplicación que es evidente cuando se descubre que es lo puede o no puede hacer cada herramienta. No todas las herramientas de Compresión y LFI soportan cada tipo de enlace de datos. Ambas herramientas de compresión y LFI pueden operar en un subconjunto de paquetes que salen de una interface. Por ejemplo la compresión de la cabecera de TCP solo comprime paquetes IP que solo tienen cabeceras TCP. La fragmentación Frame Relay solo opera en un subconjunto de paquetes, basados en cuál de los dos estilos de fragmentación es configurado. Así que dependiendo de lo que usted quiere lograr con eficiencia del enlace, usted puede normalmente usar una sola herramienta.

f) Control de admisión de llamada

Call Admission Control (CAC) protege el ancho de banda de la red, previniendo más flujos concurrentes de voz y video que la red puede soportar. De esta manera, no solo protege tráfico de datos, sino que también protege la calidad de las llamadas de voz y video que ya están establecidas. Si un ingeniero de red diseña una red para soporta tres concurrentes llamadas G.729 , por ejemplo, que tiene alrededor de 85kbps, dependiendo del enlace de datos usado, si 10 concurrentes llamadas ocurren, tomando alrededor de 285 kbps, algo malo sucede. Las aplicaciones de datos no pueden tener suficiente ancho de banda. También todas las llamadas de voz se degradan – no solo las llamadas extras.

2.8. Gestión de colas y la congestión

El encolamiento tiene un impacto en todas las cuatro características de QoS (ancho de banda, delay, jitter, y pérdida de paquetes. El encolamiento es una de las más importantes herramientas de QoS.

2.8.1. Conceptos de encolamiento en routers Cisco

IOS almacena paquetes en memoria mientras procesa los paquetes. Cuando un router a completado todo el trabajo requerido excepto el envió del paquete, si la interface de salida está ocupada, el router solo mantiene el paquete en memoria a la espera de que la interface esté disponible. Para administrar el conjunto de paquetes que esperan en memoria para salir por la interface, IOS crea una cola. Una cola solo organizan los paquetes esperando salir por una interface, las colas no es más que un conjunto de punteros para los buffers de memoria que contiene a los paquetes que están esperando salir por la interface.

Cada interface tiene un sistema de cola de hardware y software, los paquetes primero se almacenan en la cola de hardware de la interface, si la cola de hardware está llena entonces los paquetes se almacenan en la cola software. El sistema de cola de hardware siempre utiliza la cola de tipo FIFO (cola en la que el primero que ingresa es el primero que sale), en el sistema de cola por software se puede seleccionar y configurar el tipo de cola a utilizar.

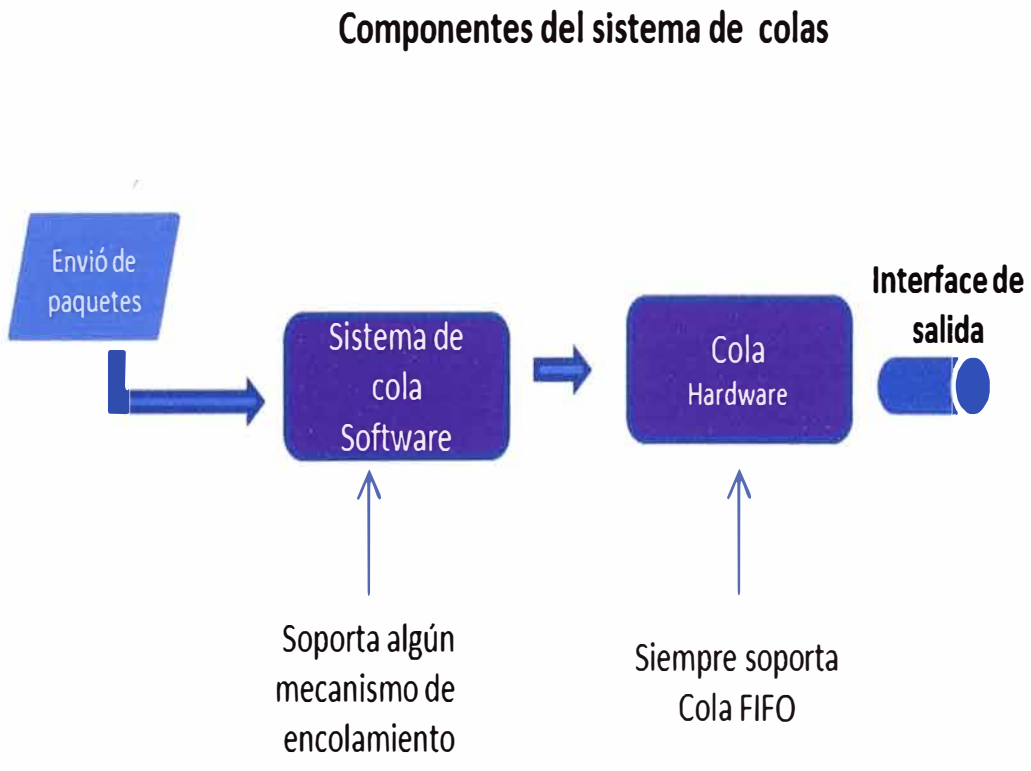

Fig.2.6 Componentes del sistema de colas

Cada mecanismo de encolamiento tiene tres componentes: Clasificación (clasifica los paquetes), inserción de políticas (determina que paquetes pueden ser encolados) y servicio de políticas (programación de la puesta de paquetes en la cola de hardware).

A continuación se muestra los tres componentes de un mecanismo de encolamiento.

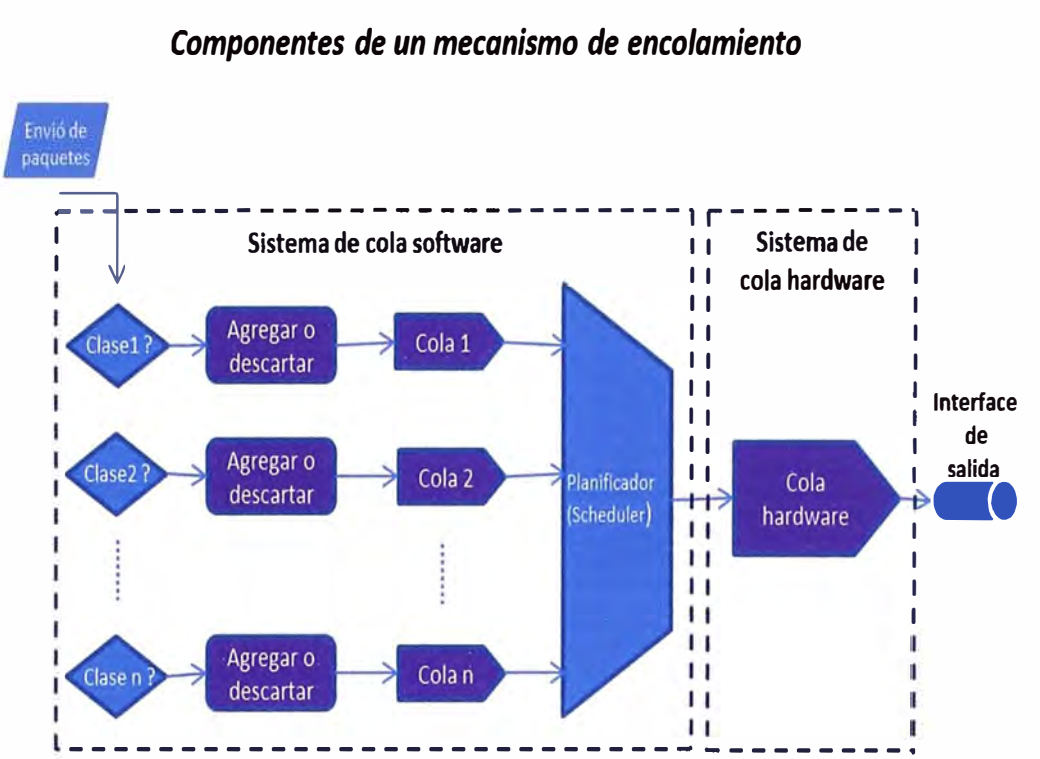

Fig. 2.7 Componentes de un mecanismo de encolamiento

A continuación de describe los tipos de colas.

a) Cola FIFO (Firts-in Firts-out)

Utiliza una sola cola, los paquetes se ponen en la cola esperando ser enviados, el primero que ingresa a la cola es el primero en salir (firts-in, first-out). No se tiene en cuenta la clase de paquete ni la prioridad, lo cual puede causar que algunas aplicaciones que requieren de un bajo delay presenten degradación.

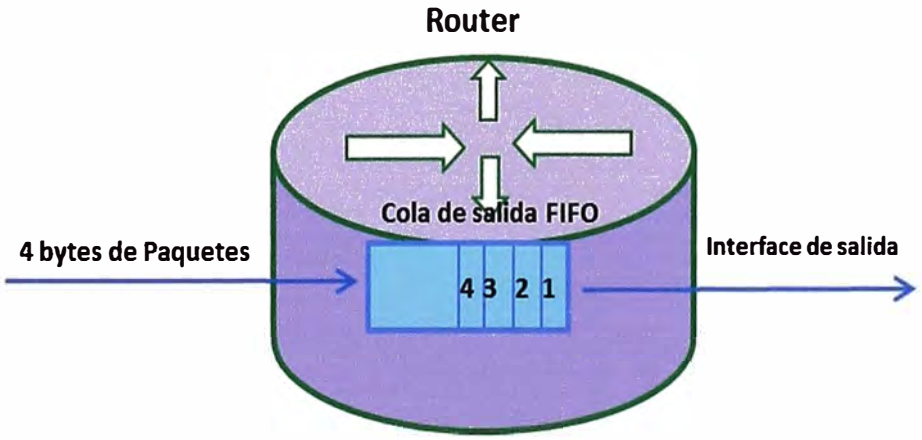

Fig.2.8 Cola FIFO

La cola FIFO está habilitada por defecto en todas las interfaces que tienen un ancho de banda de más de 2Mbps. Weighted fair queuing (WFQ) está habilitado por defecto si el ancho de banda es menor a 2Mbps, se tiene que deshabilitar el encolamiento WFQ para habilitar la cola FIFO en una interface con ancho de banda menor a 2 Mbps.

Encolamiento FIFO permite almacenar en la cola de salida un máximo de 40paquetes, es posible incrementar o disminuir el máximo número de paquetes.

b) Priority Queuing (PQ)

Priority Queuing, cuenta con cuatro colas de prioridad (alta, media, normal, y baja). Es necesario determinar que paquetes estarán en cada cola, de lo contrario los paquetes serán asignados a la cola con prioridad normal. PQ prioriza el tráfico que se encuentra en la cola de prioridad alta, siempre que se tenga paquetes en la cola de prioridad alta estos serán enviados hasta que la cola quede vacía, para luego enviar un solo paquete de la cola media y retornar a enviar los paquetes de la cola alta, en caso no se tenga paquetes en la cola de prioridad alta, se pasa a la cola de prioridad media, en caso ésta tampoco tenga paquetes se pasa a enviar un solo paquete de la cola de prioridad normal y luego retornar a la cola de prioridad alta, así sucesivamente se repite el algoritmo.

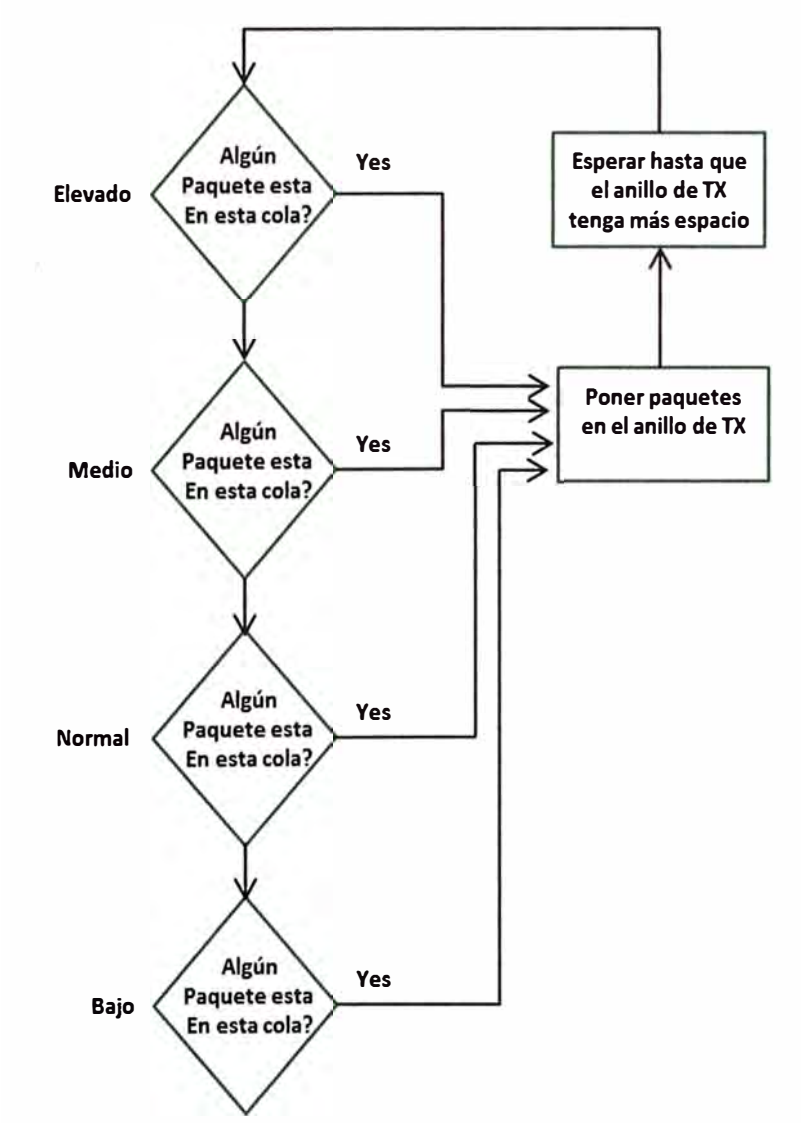

Fig.2.9 Lógica del algoritmo PQ (figura tomado de Cisco- IP Telephony Self Estudy)

c) Round Robin (RR)

En el método RR existen un conjunto de colas a las que se les asigna distintos tipos de tráfico, se envía un paquete de cada cola y se pasa a la siguiente, el algoritmo se repite así sucesivamente. No es posible priorizar tráfico debido a que las colas son tratadas igualmente.

d) Weighted Round Robin (WRR)

WRR es una versión modificada de RR en la que se pueden asignar pesos a las colas, haciendo que esos valores correspondan con el ancho de banda que tiene permitido utilizar, de esta manera se puede favorecer a determinadas colas para que puedan enviar más cantidad de datos que otras durante su turno.

e) Weighted Fair Queuing (WFQ)

WFQ es el método de encolamiento por defecto en los routers Cisco para interfaces seriales de 2,048 Mbps o inferiores y es utilizado por CBWFQ y LLQ.

WFQ clasifica paquetes basados en flujos. Un flujo consiste de todos los paquetes que tienen la misma dirección IP origen y destino, y los mismos números de puerto origen y destino. WFQ siempre favorece flujos de bajo volumen, flujos de elevada precedencia sobre flujos de gran volumen y de baja precedencia. Cada flujo utiliza una cola diferente, se pude tener una máximo de 4096 colas por interface.

A continuación se muestra los comandos de configuración de WFQ:

Router(config-if)# fair-*queue [cdt [dynamic-queues [reservable-queues]]]*

Habilita el encolamiento WFQ en la interfaz

Router(config-if)# hold-queue {max-limit} out

Configura el máximo número de paquetes que una interfaz puede almacenar en su cola software de salida.

f) Class Based Weighted Fair Queuing (CBWFQ)

CBWFQ permite la definición manual de clases, cada una de las cuales es asignada a su propia cola. Las clases se definen mediante class-map. Cada una de las colas tiene definido un mínimo ancho de banda que puede utilizar, en caso de haber más ancho de banda disponible podría emplearlo.

Si alguna cola no utiliza su ancho de banda por un corto periodo, el ancho de banda se reparte entre las otras clases. Cisco en realidad no ofrece más detalles sobre cómo funciona el programador lógico de CBWFQ.

CBWFQ soporta 64 colas, con una longitud máxima de la cola y por defecto varían

dependiendo del modelo de router y la cantidad de memoria instalada. Todas las 64 colas se pueden configurar, pero una clase de cola denominada clase por defecto se puede configurar automáticamente. Si la clasificación configurada explícitamente no coincide con un paquete, el IOS coloca el paquete en la clase por defecto. Es posible cambiar la configuración de la clase por defecto, pero esta clase siempre existe.

A continuación se muestran los comandos de configuración de CBWFQ:

*Router(*config-*pmap-c)#*

Bandwidth {bandwidth}

Queue-limit {queue-limit}

#Asigna una cantidad fija de ancho de banda a una clase

#Setea el máximo número de paquetes que esta cola puede mantener, el máximo número por defecto es 64.

Router(config-pmap-c)#

Bandwidth percent {percent}

#Asigna un porcentaje de ancho de banda a una clase

Router(config-pmap-c)#

Fair-queue [dynamic-queues]

La clase "Class-default" puede ser configurada para usar WFQ

g) Low Latency Queuing (LLQ)

Low Latency Queuing, es una herramienta de encolamiento que ofrece baja latencia para tráfico sensitivo al retardo, cuenta con una cola de prioridad estricta que es usada para aplicaciones en tiempo real que son sensitivas al retraso y al jitter. La cola LLQ de prioridad estricta está limitada, esto impide que se anule a las demás colas, asigna un ancho de banda a la cola, en caso haya congestión solo usará el ancho de banda que se le asigno.

LLQ se puede considerar como una opción de CBWFQ en la que se trata con estricta prioridad a una o más colas.

Al igual que en el encolamiento PQ la lógica del planificador de LLQ siempre comprueba la cola de baja latencia en primer lugar, y toma un paquete de la cola. Si no hay paquetes de la cola de baja latencia, la lógica del planificador se aplica a las otras colas, dándoles su ancho de banda garantizado.

LLQ ofrece garantías de ancho de banda para las colas que no son prioritarias aplicando políticas que permiten descartar paquetes cuando se supera el ancho de banda configurado para la cola de prioridad estricta.

- **Configuración de LLQ**

La configuración de LLQ requiere uno o más comandos adicionales a los usados para la configuración de CBWFQ.

En lugar de utilizar el comando ancho de banda en una clase, se utiliza el comando "priority" para la cola de prioridad estricta.

La sintaxis del comando en como sigue:

Priority { bandwidth – kpbs, porcentaje } [burts]

Este subcomando habilita LLQ en esta clase, reserva ancho de banda, y habilita la función policing. También se puede configurar el burts para el policer con este subcomando, el burts por defecto está configurado al 20% de la configuración de la tasa del policing.

2.8.2. Evitando la congestión

Existen mecanismos de QoS para evitar la congestión que permitirán en lo posible evitar que se produzca el descarte de paquetes cuando la cola está llena lo cual se conoce como el fenómeno de tail-drop.

El fenómeno tail-drop se produce cuando un paquete nuevo llega a una cola que está llena y este se descarta debido a que no hay lugar donde encolarse.

A continuación se describen algunos mecanismos que ayudan a evitar la congestión.

a) Random Early Detection (RED)

Es un mecanismo que previene el tail-drop, descarta paquetes aleatoriamente antes de que se produsca el tail-drop, la cantidad de paquetes que se descartan depende del tamaño de la cola de salida de la interfaz, si la cola crece se descartaran más paquetes. RED no diferencia los paquetes que se descartan, es decir no hace diferencia entre flujos.

El descarte de paquetes se realiza basado en dos parámetros de umbral mínimo y máximo. Si el tamaño de la cola es menor al umbral mínimo, no se descartan paquetes. Si el tamaño de la cola es mayor al umbral mínimo pero menor al umbral máximo, se descartaran algunos paquetes aleatoriamente. Si el tamaño de la cola es superior al tamaño máximo, se descartaran todos los paquetes. La cantidad de paquetes que se descartan aleatoriamente cuando el tamaño de la cola se encuentra entre el umbral mínimo y máximo depende de un valor llamada denominador de probabilidad de marca (MPD) y se descartaran 1 de cada cierta cantidad de MDP. Por ejemplo si el valor de MPD se establece en 10 y el tamaño de la cola tiene establecido un umbral mínimo y máximo, RED descartara 1 de cada 10 paquetes.

En la figura siguiente, se muestra un ejemplo de cómo actúa RED

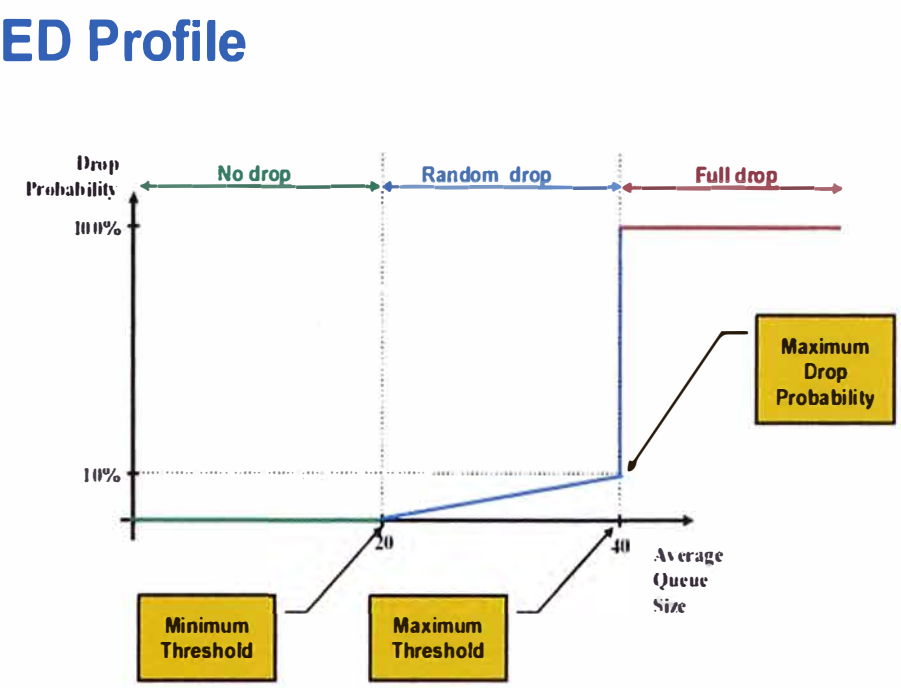

Fig.2.10 Perfil RED (figura tomado de CISCO Systems)

b) Weighted Random Early Detection (WRED)

Funciona de manera similar a RED pero con capacidad de poder decidir qué tipo de tráfico se descarta en caso sea necesario, es posible configurar diferentes perfiles de umbral mínimo, máximo y MPD (Denominador de Probabilidad de Marca) para dar más prioridad a unos flujos de tráfico que a otros. La prioridad se basa en los valores IP precedence o DSCP.

En la figura se muestra un ejemplo de cómo actúa WRED

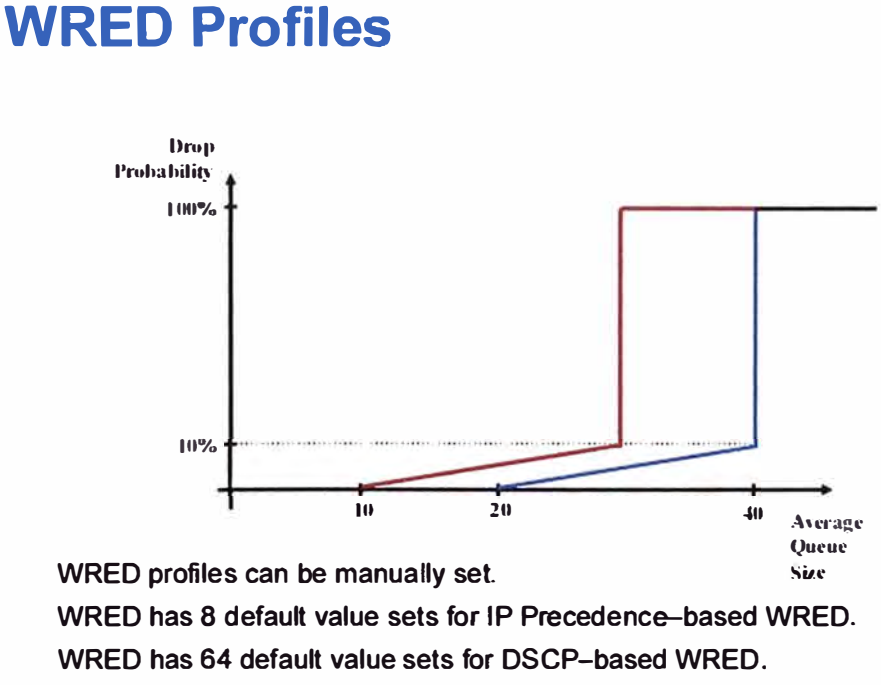

Fig.2.11 RED (figura tomado de CISCO Sytems)

c) Class Based Wighted Random Early Detection (CBWRED)

Es el resultado de aplicar WRED a CBWFQ. Dentro del sistema CBWFQ, WRED se utiliza para realizar el descarte por cada clase de cola. Por lo tanto cada clase de cola tiene su propio método WRED. Por tanto por cada cola se puede configurar una política de dropeo separada para implementar diferentes políticas de dropeo para todas las clases de tráfico.

- **A continuación se muestra los comando de configuración de CBWRED**

Se utiliza el comando *random-detect* para habilitar CBWRED en una interfaz. Con IP precedence existen 8 perfiles disponibles, mientras que con DSCP existen 64 perfiles. El tráfico que no es IP es categorizado con valor IP Precedence 0. CBWRED se configura a través del comando ramdom-detect en cada una de las clases del policy-map. Por cada valor de IP Precedence o DSCP es posible configurar un perfil con umbral mínino, máximo y un MPD.

Comandos para la configuración de WRED basado en DSCP.

*Router(router-*policy-*c)# random-detect dscp-based*

Router(router-policy-c)# random-detect {dscp dscp-value min-threshold max-threshold mark-prob-denominator}

Comandos para la configuración de WRED basado en IP Precedence

Router(router-policy-c)# random-detect precedence-based

Router(router-policy-c)# random-detect precedence {precedence-value min-threshold max-threshold mark-prob-denominator}

2.9. Traffic Shaping y Traffic Policing.

Ambos miden la tasa a la que la data es enviada o recibida. Policing descarta lo paquetes en exceso, de modo que la tasa total vigilada no es excedida. Shaping pone en cola los paquetes en exceso. En otros casos, ambos policing y shaping previenen el tráfico en exceso de la tasa definida por el policer o shaper.

La mayoría de las implementaciones de shaping y policing ocurre en los puntos finales de dos redes diferentes.

2.9.1. Token bucket

Un token bucket es una definición formal de una tasa de transferencia. Tiene tres componentes: un tamaño de ráfaga (Bc), una tasa media (CIR), y un intervalo de tiempo (TC). Aunque la tasa media se representa generalmente como bits por segundo, cualquiera de los dos valores se pueden derivar de la tercera por la relación que muestra como sigue:

$$Tasa\ media = \frac{Tamaño\ de\ ráfaga}{Intervalo\ de\ tiempo} \quad \text{.....(2.3)}$$

Estas son algunas de las definiciones de estos términos:

- **La tasa media (CIR):** Denominada también la tasa de información comprometida (CIR), que especifica la cantidad de datos que puede ser enviado o transmitido por unidad de tiempo promedio.
- **Tamaño de ráfaga (Bc):** También llamado tamaño de burts comprometido (Bc), especifica en bits (o bytes) por ráfaga la cantidad de tráfico que pueden ser enviados dentro de una unidad de tiempo determinado para no crear problemas de shaping . Para un shaper, como GTS, especifica los bits por ráfaga, para un policer, tal como CAR, especifica bytes por ráfaga.
- **El tiempo de intervalo (TC):** también llamado el intervalo de medición, especifica la cuantía de tiempo en segundos por ráfaga.

Un token bucket se utiliza para administrar un dispositivo que regula los datos de un flujo, por ejemplo, el regulador podría ser un traffic policing, tales como CAR (Committed access rate), o un conformador de tráfico, tales como FRTS (Frame relay traffic shaping) o GTS (Generic traffic shaping). Un token bucket en sí no descarta o prioriza paquetes, se podría explicar el funcionamiento de token bucket con la metáfora de la cubeta con fichas, las fichas se colocan en el recipiente a una cierta velocidad. El propio cubo tiene una determinada capacidad, si la capacidad del cubo se llena, las fichas recién llegadas se descartan. Cada ficha tiene el permiso de la fuente para enviar un cierto número de bits en la red. Para enviar un paquete, el regulador debe quitar de la cubeta un número de fichas iguales en representación del tamaño del paquete. Si no hay suficientes fichas en la cubeta para enviar un paquete, el paquete o bien espera hasta que el cubo tenga suficientes fichas (en el caso de GTS) o se descarta o es remarcado con una prioridad menor (en el caso de CAR).

2.9.2. Traffic Policing

Traffic Policing permite controlar la velocidad máxima de la tasa de transferencia del tráfico que se envía o recibe en una interface, y permite la partición de una red en múltiples niveles de prioridad o clases de servicio.

La función del traffic policing de controlar la máxima tasa de transferencia de tráfico, se lleva a cabo a través de un algoritmo de "token bucket ". El algoritmo de token bucket puede usar los valores configurados por el usuario para determinar la máxima tasa de transferencia de tráfico que se permitirá en una interface en un momento de tiempo dado.

El algoritmo de token bucket se ve afectado por todo el tráfico de entrada o salida (dependiendo de dónde se configura la política de tráfico con el traffic policing) y es útil en la gestión de ancho de banda de red en los casos en que varios paquetes grandes se envían en el mismo flujo de tráfico.

El algoritmo de token bucket proporciona a los usuarios tres acciones para cada paquete: una acción de conformidad, una acción en caso de exceso, y una acción opcional en caso de transgresión.

El traffic policing a menudo se configura en las interfaces en el borde de una red para limitar la velocidad del tráfico que entra o sale de la red. En las configuraciones más comunes de traffic policing, el tráfico que es conforme se transmite, el tráfico en exceso se envía con una prioridad menor o se descarta. El tráfico que ingresa a una interface con traffic policing configurado es puesto en una de estas tres categorías. Dentro de estas tres categorías los usuarios pueden decidir el tipo de tratamiento que se puede dar a un paquete.

Traffic policing a menudo es configurado en una interface en el extremo de una red para limitar la tasa de transferencia del tráfico entrante o saliente de la red. En las más comunes configuraciones de traffic policing, el tráfico que es conforme es transmitido y el tráfico que excede se envía con una prioridad menor o es descartado. Los usuarios pueden cambiar estas opciones de configuración para adaptarse a sus necesidades de red.

a) Beneficios de traffic Policing

- Gestión del Ancho de banda a través de limitación de velocidad: Traffic policing permite controlar la velocidad máxima del tráfico enviado o recibido en una interfaz. Traffic policing a menudo se configura en las interfaces en el borde de una red para limitar el tráfico dentro o fuera de la red. El tráfico que entra dentro de los parámetros de velocidad se envía, mientras que el tráfico que sale de los parámetros se descarta o se envía con una prioridad distinta.
- Marcado de paquetes a través de precedencia IP, Grupo de QoS, y configuración del valor de DSCP:

Marcado de paquetes que permite crear en la red varios niveles de prioridad o clases de servicio (CoS), de la siguiente manera.

- Utilice el traffic policing para establecer los valores de precedencia IP o el punto de código de servicios diferenciados (DSCP) de los paquetes que entran en la red. Los dispositivos dentro de su red, podrán utilizar los valores ajustados de precedencia IP para determinar cómo el tráfico debe ser tratado. Por ejemplo, la función de DWRED

utiliza los valores de precedencia IP para determinar la probabilidad de que un paquete se descartará.

- Utilice traffic policing para asignar paquetes a un grupo de calidad de servicio. El router utiliza el grupo de calidad de servicio para determinar cómo dar prioridad a los paquetes

b) Mecanismos de Policing:

- **Class-based Policing**

Es usado para limitar una clase de tráfico a una tasa de bit configurado. Class-based policing puede descartar o remarcar y transmitir exceso de tráfico, pude ser implementado usando un simple o doble token bucket que determinan si un paquete es conforme con la tasa de transferencia promedio, excede la tasa de transferencia promedio pero este está dentro de exceso de burts permitido, excede ambos la tasa promedio de transferencia de bit y el exceso de burts permitido.

Class-based policing es configrado usando el Modular Línea de comandos de CISCO (MQC).

A continuación de muestra los comando de configuración de Class-Based Policing.

*Router(config-*pmap-*c)#*

Police avg-rate [Bc [Be]] [conform-action] [action] [exceed-action [action] [violate-action [action]]]]

2.9.3. Traffic shaping

Traffic Shaping permite controlar el tráfico que va hacia fuera de una interfaz con el fin de igualar su flujo a la velocidad de la interfaz de destino remoto y para asegurar que el tráfico se ajuste a las políticas contraídas por ella.

Las razones principales por la que se utiliza traffic shaping son: para controlar el acceso al ancho de banda disponible, para garantizar que el tráfico se ajuste a las políticas establecidas, y para regular el flujo de tráfico con el fin de evitar la congestión que puede ocurrir cuando el tráfico enviado excede la velocidad de la interfaz remota de destino.

a) Traffic Shaping y la Tasa de Transferencia

Traffic shaping limita la velocidad de transmisión de datos. Puede limitar la transferencia de datos a una de las siguientes tasas:

Una tasa específica configurada.

Una tasa derivada basada en el nivel de congestión.

La tasa de transferencia depende de estos tres componentes que constituyen el token bucket: tamaño de ráfaga, la tasa media, la medición del intervalo (tiempo)

La tasa media es igual al tamaño de la ráfaga dividida por el intervalo de tiempo.

Cuando está habilitado traffic shaping, la velocidad de bits de la interfaz no deberá exceder la tasa media por encima de cualquier múltiplo entero del intervalo. En otras palabras, durante cada intervalo, un máximo de tamaño de ráfaga puede ser enviado. Dentro del intervalo, sin embargo, la tasa de bits puede ser más rápida que la velocidad media en cualquier momento dado.

Una variable adicional se aplica en el traffic shaping: el tamaño de burts en exceso (Be), el tamaño de exceso de Burst (Be) se corresponde con el número de bits no comprometidos que están fuera del CIR, que todavía son aceptados por el switch Frame Relay, pero marcados como elegible de descarte (DE).

En otras palabras, el tamaño del Be permite más que el tamaño del burts (Bc) para ser enviado durante un intervalo de tiempo en ciertas situaciones. El conmutador permitirá el envió de los paquetes que pertenecen a la ráfaga de exceso de burts, pero se marca en ellos el bit DE. Si se envían los paquetes depende de cómo esté configurado el conmutador.

Cuando el tamaño del Be es igual a 0, la interfaz no envía más que el tamaño del burts en cada intervalo. Sin embargo, cuando el tamaño del Be es mayor que 0, la interfaz puede enviar tantas como Bc + Be bits en una ráfaga, si en un período de tiempo anterior, la cantidad máximo no se envió.

b) Mecanismos de shaping:

- **Class-based shaping**

Es usado para limitar paquetes, tiene dos métodos de shaping:

Tasa promedio: envía paquetes en la tasa de transferencia promedio configurado que permite una ráfaga por encima del Be cuando hay extra tokens disponibles, este es método más común.

Tasa pico: envía paquetes en la tasa pico de Bc +Be cada Tc, se calcula mediante la formula

$$Tasa\ pico = Tasa\ promedio \times (1 + Be/Bc) \qquad (2.4)$$

El tráfico que se envía sobre el CIR puede ser dropeado durante la congestión.

Class-based shaping usa un simple token bucket con un maximo tamaño de token bucket de Be+Bc.

Configuracion de class-based shaping

*Router(*config-*pmap-c)#*

Shape { average *, peak} bit-rate [Bc [be]]*

Bc y Be pueden ser omitidos para dejar que el router seleccione el valor óptimo, que es lo lo recomendado.

2.10. El modular QoS CLI (MQC)

El modular QoS CLI (MQC) es un mecanismo de aprovisionamiento en IOS Cisco, que permite clasificar los paquetes, aplicar políticas a las clases definidas y aplicar las políticas a una interface o subinterface. El MQC forma la base para la provisión de DiffServ, y todos los mecanismos de QoS son parte de los class-maps (clasificación), o policy-map (policing, shaping, encolamiento, evitar la congestión, marcado de paquetes, etc).

Los paquetes que entran en un dominio DiffServ (DS-dominio) pueden ser medidos, marcados, formados, controlados para implementar políticas de tráfico. En Cisco IOS, la clasificación y marcado es hecho usando el MQC's class-maps. La medición es hecha usando algoritmo token bucket, shaping es hecho usando Class-based Traffic Shaping (CBTS), o Class-based Frame Relay Traffic Shaping (CB-FRTS), y el control es hecho usando class-based policing.

2.10.1.Comandos principales de MQC

- El Class-map comando define los parámetros de matching para clasificar paquetes en clases de servicio.
- Porque diferentes herramientas crean diferentes PHBs, las acciones PHB (marcación, encolamiento) son configurados bajo herramientas policy-map.
- Porque MQC opera en paquetes que estos ingresan o salen en una interface, los policy map necesita ser habilitados en una interface usando un comando service-policy.

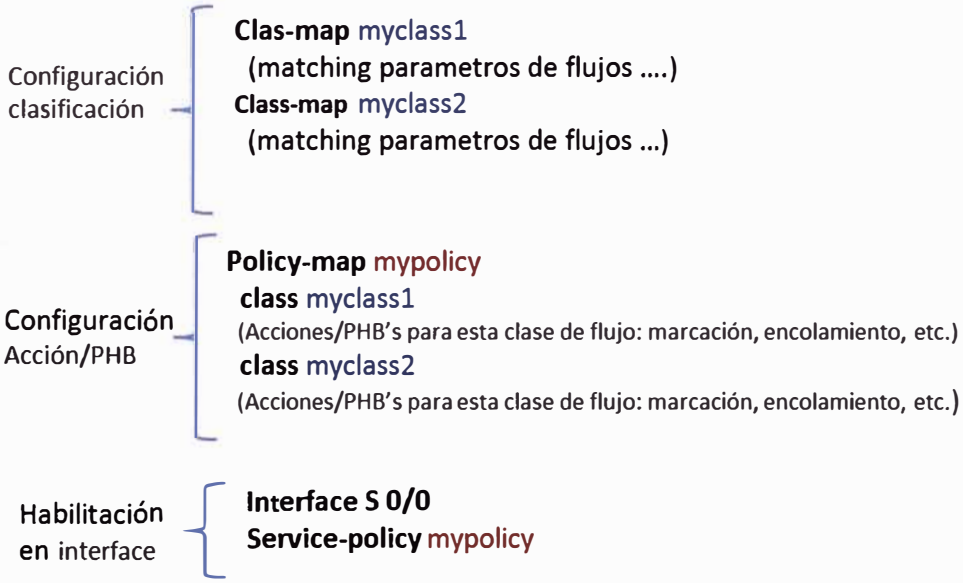

Fig.2.12 Muestra el flujo general de los comandos

Cada comando **class-map** deber ser seguido por un subcomando **match**, que define los parámetros actuales que son comparados con el contenido de la cabecera de un paquete para su clasificación.

Para cada clase, alguna acción QoS (PHB) necesita ser aplicado, la configuración para estas acciones es hecha bajo el comando **policy-map**. Bajo un simple policy map, múltiples clases son referidas. Dentro de un solo policy map se puede configurar para cada clase separadas acciones QoS, por ejemplo se puede aplicar diferente marcado de paquetes para cada clase. Cuando un comando **service-policy** es aplicado a una interface, la característica QoS es habilitada.

CAPÍTULO III
PLANTEAMIENTO DE SOLUCIÓN DE LA IMPLEMETACION DE QoS EN LA RED DE UNA EMPRESA CON 13 SEDES REMOTAS Y 1 SEDE PRINCIPAL

3.1. Arquitectura de red

A continuación se muestra la implementación de Calidad de Servicio en la red de una empresa que cuenta con una sede principal y 13 sedes remotas, las sedes remotas se encuentran ubicadas en distintos puntos de la ciudad de Lima y la sede principal se encuentra ubicada en el distrito de Pueblo Libre, cada una de las sedes cuenta con un acceso WAN el cual es contratado a un proveedor de servicios que ofrece servicios de red privada virtual con QoS para asegurar el ancho de banda por clase de servicio.

En la solución que se implementa para gestionar el ancho de banda, la pérdida de paquetes, delay y jitter mediante Calidad de servicio, se consideró contratar al proveedor WAN tres clases de servicios con QoS para permitir enviar el tráfico que se genera en la red LAN del cliente con un trato diferenciado por cada clase de servicio en la que se clasifica el tráfico de la empresa.

A nivel LAN cada una de las sedes de la empresa cuenta con una central telefónica IP Avaya y un router Cisco-871 que se conecta a la red del proveedor, la sede principal cuenta con 8 servidores de aplicaciones del negocio de la empresa, una central telefónica IP Avaya y un router Cisco 2821. El cliente utiliza el códec G729.a para la compresión de su tráfico de voz.

Todas las sedes remotas acceden a Internet a través de la sede principal, la sede principal tiene contratado al proveedor un acceso a Internet de 10Mbps y que es garantizado al 100% tanto para el tráfico de subida como de bajada.

El tráfico de cada una de las sedes de la empresa es clasificado en tres clases de servicio que son clase de servicio 3 (CoS3), clase de servicio 2 (CoS2) y clase de servicio 1 (CoS1). Para la clasificación del tráfico, el cliente brindo los datos del requerimiento en cuanto a ancho de banda de sus aplicativos, la sensibilidad al retardo y pérdida de paquetes de sus aplicativos.

Dentro de la clase de servicio CoS3 se clasificó al tráfico de voz de la empresa, esto debido a que esta clase se encuentra configurado con el nivel de prioridad más elevado dentro de las tres clases de servicio que brinda el proveedor de servicios.

Dentro de la clase de servicio CoS2 se clasificó al tráfico de los aplicativos del negocio de la empresa, esto debido a que esta clase se encuentra configurado con el segundo nivel de prioridad dentro de las 3 clases de servicio que brinda el proveedor de servicios.

Dentro de la clase de servicio CoS1 se encuentra el tráfico restante, es decir el tráfico que no pertenece a la clase de servicio CoS3 y CoS2.

La cantidad de ancho de banda para CoS3 se consideró teniendo en cuenta la cantidad de teléfonos IP que el cliente cuenta en cada sede.

La cantidad de ancho de banda en CoS2 se dimensiono con los datos brindados por el cliente en cuanto requerimiento de ancho de banda de los aplicativos de su negocio.

El ancho de banda que se consideró para CoS1 fue decidido por el cliente según sus requerimientos de conectividad hacia Internet y la conectividad hacia su servidor mail.

Para la gestión del ancho de banda se utiliza la herramienta de policing-traffic CB-policing traffic.

Para la gestión de congestión se emplea las herramientas de encolamiento LLQ, CBWFQ y CBWRED

3.2. Topología de la empresa

A continuación se muestra la topología de la red privada virtual de la empresa.

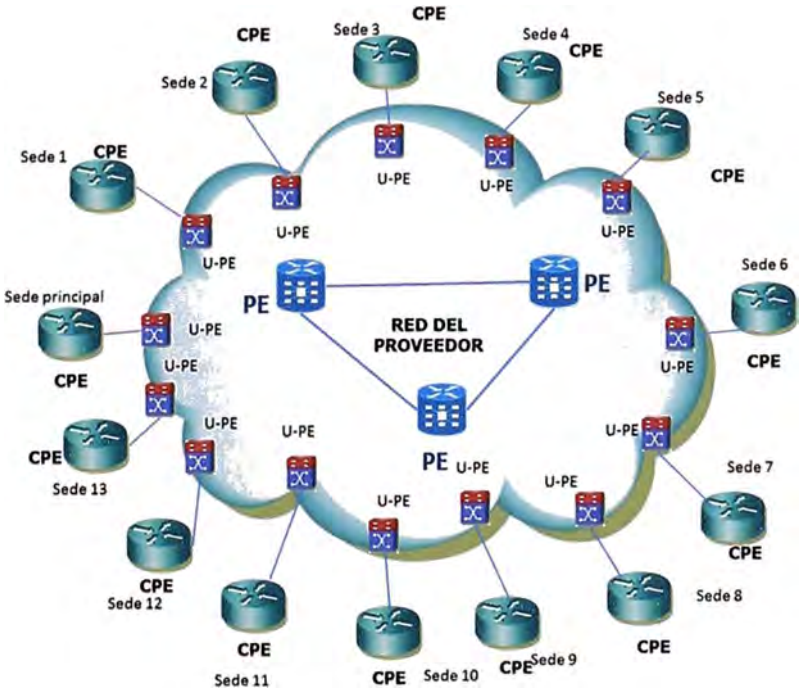

Fig.3.1 Topología de la Red Privada Virtual de la empresa

3.3. Asignación de direcciones IPs LAN y WAN para cada sede.

A continuación se detalla las direcciones IPs LAN Y WAN que se asignaron a cada sede de la empresa.

TABLA N° 3.1 Dirección IP LAN y WAN

Sede	IP/Máscara LAN	IP/Máscara WAN
Principal	192.168.0.0/24	10.17.72.94/30
Sucursal 1	192.168.19.0/24	10.10.46.54/30
Sucursal 2	192.168.17.0/24	10.10.39.6/30
Sucursal 3	192.168.12.0/24	10.10.46.102/30
Sucursal 4	192.168.16.0/24	10.17.8.222/30
Sucursal 5	192.168.15.0/24	10.17.0.206/30
Sucursal 6	192.168.14.0/24	10.17.72.98/30
Sucursal 7	192.168.13.0/24	10.17.0.210/30
Sucursal 8	192.168.11.0/24	10.14.0.10/30
Sucursal 9	192.168.21.0/24	10.17.0.202/30
Sucursal 10	192.168.20.0/24	10.10.46.14/30
Sucursal 11	192.168.23.0/24	10.15.16.110/30
Sucursal 12	192.168.22.0/24	10.17.0.214/30
Sucursal 13	192.168.13.0/24	10.234.157.24/30

3.4. Nivel de servicio acordado con el proveedor (SLA)

Según el SLA que se tiene contratado, el proveedor ofrece conectividad de extremo a extremo full-mesh entre todas las sedes y ofrece tres clases de servicio (CoS) aplicando políticas de calidad de servicio al ancho de banda contratado.

Niveles de clases de servicios ofrecidos por el proveedor:

- CoS-3: para voz o video, aplicaciones multimedia y video conferencia
- CoS-2: para aplicaciones de datos críticos
- CoS-1: para aplicaciones de datos normales

En ausencia de tráfico asociado al CoS2 y CoS3, el tráfico de CoS1 puede utilizar el total del ancho de banda del acceso (100%). En caso del tráfico asociado al CoS2, ante un excedente de tráfico, este desborda al ancho de banda disponible en CoS1. En el caso del CoS3, el tráfico excedente no podrá utilizar el ancho de banda de las otras clases, se limita al ancho de banda contratado.

3.5. Ancho de banda contratado al proveedor por clase de servicio

El ancho de banda que se contrató al proveedor por clase de servicio se encuentra en función de la cantidad de usuarios por sede y el requerimiento en cuanto a ancho de banda de cada aplicativo para su correcta operación, el aplicativo SAP (Servicios Aplicaciones, Operación) que la empresa utiliza consume un ancho de banda de 20kbps por conexión. Para el tráfico de voz se considera que las centrales IP que se tiene instalada en cada sede de la empresa tienen configurado el códec de compresión de voz G.729A el cual comprime la voz, haciendo que cada llamada ocupe un ancho de banda de 29kbps.

A continuación la tabla muestra el ancho de banda de acceso y el ancho de banda por CoS ofrecido por el proveedor.

TABLA N° 3.2 Ancho de banda de acceso y CoS ofrecido por el proveedor

	Anchos de Banda
Ancho de banda de acceso local (BWT)	64K, 96K, 128K, 192K, 256K, 384K, 512K, 768K, 1024K, 1536K, 2M, 3M, 4M, 5M, 6M, 7M, 8M, 10M, 15M, 20M, 30M, 40M, 50M, 60M, 70M, 80M, 100M, 155M, 200M.
Ancho de banda por clase de servicio (CoS)	32K, 64K, 96K, 128K, 192K, 256K, 384K, 512K, 768K, 1024K, 1536K, 2M, 4M, 5M, 6M, 7M, 8M, 10M, 15M, 20M, 30M, 40M, 50M, 60M, 70M, 80M, 100M, 155M.

3.6.Clasificación del tráfico en tres clases de servicio

Se clasifica el tráfico en cada una de la sedes en tres clases de servicio según el SLA contratado con el proveedor.

Para cada una de las sedes se considera en la clase de servicio 3 (CoS3) al tráfico de voz debido a la máxima prioridad de calidad de servicio que ofrece el proveedor para este CoS. Se considera en la clase de servicio 2 (CoS2) al tráfico dirigido a los servidores de base de datos, esto debido a que para la operación de la empresa es de suma importancia la conexión a estos servidores. En la clase de servicio 1 (CoS1) se encuentra el tráfico que no pertenece a tráfico de voz ni al tráfico de las conexiones que se establecen con los servidores de base de datos, dentro de esta clase se encuentra el tráfico dirigido hacia Internet, tráfico entre PCs que se encuentran en distintas sedes y tráfico mail.

A continúan se detalla el tipo de tráfico que forma cada una de las tres clases de servicio (CoS) de cada una de las sedes de la empresa.

TABLA N° 3.3 Tipo de Tráfico

	Tipo de tráfico que forma cada clase de servicio		
Sede	CoS3	CoS2	CoS1
Principal	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 1	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 2	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 3	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 4	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 5	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 6	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 7	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 8	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 9	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 10	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 11	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 12	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)
Sucursal 13	Voz	Datos dirigidos a servidores de base de datos	Tráfico que no es voz ni de conexiones a base de datos (Tráfico Internet, mail)

La tabla muestra el tipo de tráfico de las 13 sedes de la empresa.

A continuación se detalla la cantidad de usurarios por sede.

TABLA N° 3.4 Tabla de cantidad de usuarios

Sede	Cantidad de usuarios
Principal	70
Sucursal 1	26
Sucursal 2	27
Sucursal 3	50
Sucursal 4	51
Sucursal 5	55
Sucursal 6	52
Sucursal 7	53
Sucursal 8	26
Sucursal 9	53
Sucursal 10	27
Sucursal 11	52
Sucursal 12	54
Sucursal 13	25

A continuación se describen los anchos de banda contratados al proveedor por clase de servicio para cada sede.

TABLA N° 3.5 Tabla de cantidad de ancho de banda contratado por sede

Sede	BW COS3	BW COS2	BW COS1
Principal	2 Mbps	10 Mbps	4 Mbps
Sucursal 1	256Kbps	512Kbps	256Kbps
Sucursal 2	256Kbps	512Kbps	256Kbps
Sucursal 3	256Kbps	1024Kbps	256Kbps
Sucursal 4	256Kbps	1024Kbps	256Kbps
Sucursal 5	256Kbps	1024Kbps	512Kbps
Sucursal 6	256Kbps	1024Kbps	512Kbps
Sucursal 7	256Kbps	1024Kbps	256Kbps
Sucursal 8	256Kbps	256Kbps	256Kbps
Sucursal 9	256Kbps	1024Kbps	256Kbps
Sucursal 10	256Kbps	256Kbps	256Kbps
Sucursal 11	256Kbps	1024Kbps	256Kbps
Sucursal 12	256Kbps	1024Kbps	512Kbps
Sucursal 13	256Kbps	512Kbps	256Kbps

Numero de Pcs, teléfonos IPs, central telefónica, servidor de base datos, servidor web y servidor mail por sede.

TABLA N° 3.6 Tabla de cantidad de equipos por sede.

Sede	PCs	Teléfonos IP	Central telefónica	Servidor Base Datos	Servidor Web	Servidor Mail
Principal	70	70	1	8	1	1
Sucursal 1	26	26	1	0	0	0
Sucursal 2	27	27	1	0	0	0
Sucursal 3	50	50	1	0	0	0
Sucursal 4	51	51	1	0	0	0
Sucursal 5	55	55	1	0	0	0
Sucursal 6	52	52	1	0	0	0
Sucursal 7	53	53	1	0	0	0
Sucursal 8	26	26	1	0	0	0
Sucursal 9	53	53	1	0	0	0
Sucursal 10	27	27	1	0	0	0
Sucursal 11	52	52	1	0	0	0
Sucursal 12	54	54	1	0	0	0
Sucursal 13	25	25	1	0	0	0

3.7.Configuración en el router CPE para la clasificación del tráfico y aplicación de políticas de QoS para asegurar el BW por clase de servicio.

Se clasifica el tráfico de cada sede mediante listas de acceso extendidas que definen la dirección IP origen y destino del tráfico. Cada sede tiene configurado dos listas de acceso extendida, una que clasifica en tráfico en CoS3 y otra que clásica el tráfico en CoS2. Para la clasificación en CoS1 no se define ninguna lista de acceso ya que dentro de esta clase se encontrara el tráfico restante, es decir que no pertenece a CoS3 ni a CoS2.

Una vez clasificado el tráfico se marcan los paquetes y se aplica las políticas de calidad de servicio de aseguramiento de ancho de banda por clase.

Todo el tráfico que pertenece al CoS3 se marca con el DSCP CS5 (esto debido a que la red del proveedor le brinda un trato de máxima calidad de servicio), el tráfico con CoS2 se marca con el DSCP CS2 y el tráfico perteneciente al CoS1 se marca con el DSCP CS1.

3.7.1. Script de configuración del router CPE de la sede principal

#Clasificación de tráfico

```
ip access-list extended qos2
permit ip host 192.168.0.3 any
permit ip host 192.168.0.5 any
permit ip host 192.168.0.6 any
permit ip host 192.168.0.7 any
```

permit ip host 192.168.0.9 any

permit ip host 192.168.0.11 any

permit ip host 192.168.0.18 any

permit ip host 192.168.0.20 any

permit ip 192.168.0.0 0.0.0.255 host 192.168.21.14

permit ip 192.168.0.0 0.0.0.255 host 192.168.21.96

ip access-list extended qos5

permit ip host 192.168.0.250 192.168.0.250 0.0.255.0

class-map match-any P2

match ip dscp cs2

match access-group name qos2

class-map match-any P5

match ip dscp cs5

match access-group name qos5

class-map match-any qos5

match ip dscp cs5

class-map match-any qos1

match ip dscp cs1

class-map match-any qos2

match ip dscp cs2

#Marcado de paquetes

policy-map SetDscpLan

class P5

set ip dscp cs5

class P2

set ip dscp cs2

class class-default

set ip dscp cs1

#Creación de políticas y colas para el tráfico

policy-map wan

class qos5

priority 2048

police 2048000 384000 768000 conform-action transmit exceed-action drop

class qos2

bandwidth 10240

police 10240000 1920000 3840000 conform-action transmit exceed-action set-dscp transmit cs1

class qos1

bandwidth 4096

class class-default

fair-queue

policy-map Shape16384

class class-default

shape average 16384000

service-policy wan

#Aplicación de políticas a la interface LAN para el marcado de paquetes

interface GigabitEthernet0/1

ip address 192.168.0.2 255.255.255.0

no ip redirects

no ıp proxy-arp

load-interval 30

duplex auto

speed auto

service-policy input SetDscpLan

#Aplicación del policy-map al tráfico de salida

interface GigabitEthernet0/0

description Enlace WAN RPVL CID-568627

ip address 10.17.72.94 255.255.255.252

no ip redirects

no ıp proxy-arp

load-interval 30

duplex full

speed 100

service-policy output Shape16384

3.7.2. Script de configuración del router CPE de las sedes remota1

#Clasificación de tráfico

ip access-list extended qos2

permit ip 192.168.19.0 0.0.0.255 host 192.168.0.3

permit ip 192.168.19.0 0.0.0.255 host 192.168.0.5

permit ip 192.168.19.0 0.0.0.255 host 192.168.0.6

permit ip 192.168.19.0 0.0.0.255 host 192.168.0.7

permit ip 192.168.19.0 0.0.0.255 host 192.168.0.9

permit ip 192.168.19.0 0.0.0.255 host 192.168.0.11

permit ip 192.168.19.0 0.0.0.255 host 192.168.0.18

permit ip 192.168.19.0 0.0.0.255 host 192.168.0.20

permit ip 192.168.19.0 0.0.0.255 host 192.168.21.14

permit ip 192.168.19.0 0.0.0.255 host 192.168.21.96

ip access-list extended qos5

permit ip host 192.168.19.250 192.168.0.250 0.0.255.0

class-map match-any qos5

match ip dscp cs5

class-map match-any qos1

match ip dscp cs1

class-map match-any qos2

match ip dscp cs2

class-map match-any P2

match ip dscp cs2

match access-group name qos2

class-map match-any P5

match ip dscp cs5

match access-group name qos5

#Marcado de paquetes

policy-map SetDscpLan

class P5

set ip dscp cs5

class P2

set ip dscp cs2

class class-default

set ip dscp cs1

#Creación de políticas y colas para el tráfico

policy-map wan

class qos5

priority 256

police 256000 48000 96000 conform-action transmit exceed-action drop

class qos2

bandwidth 512

police 512000 96000 192000 conform-action transmit exceed-action set-dscp-transmit cs1

class qos1

bandwidth 256

class class-default

fair-queue

policy-map Shape1024

class class-default

shape average 1024000

service-policy wan

#Aplicación de políticas a la interface LAN para el marcado de paquetes

interface Vlan1

description ENLACE LAN

ip address 192.168.19.1 255.255.255.0

no ip redirects

no ıp proxy-arp

load-interval 30

service-policy input SetDscpLan

#Aplicación del policy-map al tráfico de salida

interface FastEthernet4

description Enlace WAN CID568623

ip address 10.10.46.54 255.255.255.252

no ip redirects

no ıp proxy-arp

load-interval 30

speed 10

full-duplex

service-policy output Shape1024

3.8. Configuración de políticas de QoS en los equipos del proveedor.

Se muestra la configuración asociado al servicio de la sede principal y una de las sedes remotas.

En la red de proveedor se aplican políticas de QoS de traffic-policer, traffic-shaping y la herramienta para CBWRED que evita el descarte de paquetes cuando las colas están llenas.

3.8.1. Script de configuración en el router U-PE de acceso del proveedor

a) Script de configuración en el router U-PE para el servicio de la sede principal

Se configura traffic-policer que se encargan de limitar el ancho de banda por clase de servicio según lo contrado al proveedor, el traffic-policer se configura tanto para el tráfico entrante como para el tráfico saliente.

#Política para el tráfico de entrada

Policy Map Policer_IN_16384_2048_10240_4096

Class qos5

police 2048000 bps 384000 byte conform-action transmit exceed-action drop

Class qos2

police 10240000 bps 1920000 byte conform-action transmit exceed-action drop

Class qos1

police 16384000 bps 3072000 byte conform-action transmit exceed-action drop

Class class-default

set dscp cs1

police 128000 bps 24000 byte conform-action transmit exceed-action drop

#Política para el tráfico de salida

Policy Map Policer_OUT_16384_2048_10240_4096

Class qos5

police 2048000 bps 384000 byte conform-action transmit exceed-action drop

Class qos2

police 10240000 bps 1920000 byte conform-action transmit exceed-action

policed-dscp-transmit

Class qos1

police 16384000 bps 3072000 byte conform-action transmit exceed-action drop

Class class-default

police 128000 bps 24000 byte conform-action transmit exceed-action drop

#Aplicación del policy-map al tráfico de entrada y salida en la interface de acceso del servicio.

interface GigabitEthernet1/42

description IDE 568034 RPVL UIGV sede principal

switchport access vlan 1480

switchport mode access

switchport port-security

switchport port-security maximum 10

switchport port-security violation restrict

service-policy input Policer_IN_16384_2048_10240_4096

service-policy output Policer_OUT_16384_2048_10240_4096

b) Script de configuración del router U-PE de acceso del proveedor para el servicio contratado para la sede remota 1.

Se configura policer-traffic que se encargan de limitar el ancho de banda por clase de servicio, se configura tanto para el tráfico entrante como para el tráfico saliente, el policer-traffic se aplicara en la interface del router U-PE de acceso que se conecta al router CPE (equipo que se instala en la sede del cliente).

#Política para el tráfico de entrada

Policy Map Policer_IN_1024_256_512_256

Class qos5

police 256000 bps 48000 byte conform-action transmit exceed-action drop

Class qos2

police 512000 bps 96000 byte conform-action transmit exceed-action drop

Class qos1

police 1024000 bps 192000 byte conform-action transmit exceed-action drop

Class class-default

set dscp cs1

police 128000 bps 24000 byte conform-action transmit exceed-act

#Política para el tráfico de salida

Policy Map Policer_OUT_1024_256_512_256

Class qos5

police 256000 bps 48000 byte conform-action transmit exceed-action drop

Class qos2

police 512000 bps 96000 byte conform-action transmit exceed-action policed-dscp-transmit

Class qos1

police 1024000 bps 192000 byte conform-action transmit exceed-action drop

Class class-default

police 128000 bps 24000 byte conform-action transmit exceed-action drop

#Aplicación del policy-map al tráfico de entrada y salida en la interface de acceso del servicio, la interface GigabitEthernet 4/13 corresponde a la interface del equipo U-PE que se conecta al router CPE.

interface GigabitEthernet4/13

description IDE 568108 RPVL UIGV Sede 1

switchport access vlan 2850

switchport mode access

switchport port-security

switchport port-security maximum 10

switchport port-security violation restrict

service-policy input Policer_IN_1024_256_512_256

service-policy output Policer_OUT_1024_256_512_256

logging event link-status

load-interval 30

speed 10

duplex full

qos trust dscp

tx-queue 3

priority high

spanning-tree portfast

spanning-tree bpduguard enable

spanning-tree guard root

end

3.8.2. Script de configuración del router PE del proveedor para el servicio contratado en la sede principal y la sede remota 1.

En la configuración para la clase con elevada prioridad se configura el tipo de encolamiento LLQ, en la clase con elevada prioridad no se configura herramientas que

evitan el descarte de paquetes por tail-drop, esto debido a que las aplicaciones de voz son sensibles al descarte de paquetes, para las clases de servicio CoS2 y CoS1 se configura la herramienta de encolamiento CBWFQ y la herramienta para evitar la congestión de CBWRED.

a) A continuación se muestra el script de configuración en equipo PE del proveedor para la sede principal

Policy Map WAN_16384_2048_10240_4096
Class qos5
priority

police cir 2048000 bc 384000 be 768000
conform-action transmit
exceed-action drop
Class qos2bandwidth 10240
random-detect precedence-based
random-detect precedence 2 2000 packets 8000 packets 1
Class qos1
bandwidth 4096
random-detect precedence-based
random-detect precedence 1 2000 packets 8000 packets 1
Class class-default
random-detect precedence-based
Policy Map Shape16384
Class class-default
shape average 16384000

#Aplicación de traffic-shaping en la subinterface del equipo PE

interface GigabitEthernet2/1/7.101480
description CID 568627 RPVL UIGV Sede Principal
encapsulation dot1Q 1480
ip vrf forwarding 01378
ip address 10.17.72.93 255.255.255.252
no ip directed-broadcast
no cdp enable
service-policy input Shape16384

service-policy output Shape16384_2048_10240_4096

b) A continuación se muestra el script de configuración en equipo PE del proveedor para la sede remota 1

Policy Map WAN_1024_256_512_256

Class qos5

priority

police cir 256000 bc 48000 be 96000

conform-action transmit

exceed-action drop

Class qos2

bandwidth 512

random-detect precedence-based

random-detect precedence 2 2000 packets 8000 packets 1

Class qos1

bandwidth 256

random-detect precedence-based

random-detect precedence 1 2000 packets 8000 packets 1

Class class-default

random-detect precedence-based

#Configuración del Policy Map Shape

Policy Map Shape1024_256_512_256

Class class-default

shape average 1024000

service-policy WAN_1024_256_512_256

3.9. Resultados

A continuación se muestra el resultado de aplicar las herramientas de encolamiento LLQ, CBWFQ, traffic-policing , traffic-shaping, y la herramienta para evitar el tail-drop CBWRED al tráfico que se genera en la red LAN de la empresa y es transmitida por la red WAN del proveedor y de esta forma se logra la comunicación adecuada entre sedes que se ubican en puntos geográficos distantes, en los resultados solo se muestra la captura del tráfico que cursa la sede principal y la sede remota 1 ya que lo que se busca es mostrar como influencian las herramientas de calidad de servicio en la utilización del ancho de banda por clase de servicio, la cantidad de paquetes que se descartan por clase de

servicio y la prioridad en el envió del tráfico de las aplicaciones sensibles al delay y jitter. A continuación se observa el tráfico que se cursa por clase de servicio en una muestra en tiempo real.

rUIGV Sede1# sh policy-map int fastEthernet 4

FastEthernet4

Service-policy output: Shape1024

Class-map: class-default (match-any)

52455507 packets, 5732119994 bytes

30 second offered rate 41000 bps, drop rate 0 bps

Match: any

Traffic Shaping

Target/Average Byte Sustain Excess Interval Increment

Rate Limit bits/int bits/int (ms) (bytes)

1024000/1024000 6400 25600 25600 25 3200

Adapt Queue Packets Bytes Packets Bytes Shaping

Active Depth Delayed Delayed Active

0 52455499 1437145583 449949 386887885 no

Service-policy : wan

Class-map: qos5 (match-any)

39769575 packets, 3545993442 bytes

30 second offered rate 5000 bps, drop rate 0 bps

Match: ip dscp cs5 (40)

39769575 packets, 3545993368 bytes

30 second rate 5000 bps

Queueing

Strict Priority

Output Queue: Conversation 72

Bandwidth 256 (kbps) Burst 6400 (Bytes)

(pkts matched/bytes matched) 90077/8674340

(total drops/bytes drops) 7/7061

police:

cir 256000 bps, bc 48000 bytes

conformed 39769575 packets, 3545993442 bytes; actions:

transmit

exceeded 0 packets, 0 bytes; actions:

drop conformed 5000 bps, exceed 0 bps

Class-map: qos2 (match-any)

128172 packets, 26438544 bytes

30 second offered rate 0 bps, drop rate 0 bps

Match: ip dscp cs2 (16)

128172 packets, 26438544 bytes

30 second rate 0 bps

Queueing

Output Queue: Conversation 73

Bandwidth 512 (kbps)Max Threshold 64 (packets)

(pkts matched/bytes matched) 582/207710

(depth/total drops/no-buffer drops) 0/0/0

police:

cir 512000 bps, bc 96000 bytes

conformed 128172 packets, 26438544 bytes; actions:

transmit

exceeded 0 packets, 0 bytes; actions:

set-dscp-transmit cs1

conformed 0 bps, exceed 0 bps

Class-map: qos1 (match-any)

12469702 packets, 2137670619 bytes

30 second offered rate 32000 bps, drop rate 0 bps

Match: ip dscp cs1 (8)

12469702 packets, 2137670673 bytes

30 second rate 32000 bps

Queueing

Output Queue: Conversation 74

Bandwidth 256 (kbps)Max Threshold 64 (packets)

(pkts matched/bytes matched) 359195/377989440

(depth/total drops/no-buffer drops) 0/1/0

Class-map: class-default (match-any)

88057 packets, 22017335 bytes

30 second offered rate 0 bps, drop rate 0 bps

Match: any

Queueing

Flow Based Fair Queueing

Maximum Number of Hashed Queues 64

(total queued/total drops/no-buffer drops) 0/0/0

 # EN PE DEL PROVEEDOR

rMPLSChinchon#sh policy-map interface GigabitEthernet3/1/6.102850

GigabitEthernet3/1/6.102850

Service-policy input: Shape1024 (6880)

Class-map: class-default (match-any) (12772721/0)

148032818 packets, 19094537242 bytes

30 second offered rate 50000 bps, drop rate 0 bps

Match: any (7838994)

Shape Queue: 354

Shape:

cir 1024 kbps, Be 204800 bits

Queue-limit: 256 packets (default) Threshold drop 0 pkts, 0 bytes

Current queue-depth: 0 packets, Maximum queue-depth: 82 packets

Average queue-depth: 0.000 packets

Service-policy output: Shape1024_256_512_256 (6882)

Class-map: class-default (match-any) (12797297/0)

170598392 packets, 88288735873 bytes

30 second offered rate 60000 bps, drop rate 0 bps

Match: any (14258178)

Shape:

cir 1024 kbps, Be 204800 bits

Service-policy : WAN_1024_256_512_256 (2495936)

Class-map: qos5 (match-any) (9132161/12)

104991559 packets, 10210984319 bytes

30 second offered rate 48000 bps, drop rate 0 bps

Match: ip dscp 40 (15244114)

Match: ip dscp 48 (15242066)

Match: ip dscp 46 (15242578)

Match: ip precedence 5 (2843810)

Class of service queue: 1256

Queue-limit: 256 packets (default) Threshold drop 0 pkts, 0 bytes

Current queue-depth: 0 packets, Maximum queue-depth: 14 packets Average queue-depth: 0.000 packets

Priority

police:

256000 bps, 48000 limit, 96000 extended limit

conformed 104991549 packets, 10210980594 bytes; actions:

transmit

exceeded 10 packets, 3725 bytes; actions:

drop

conformed 48000 bps, exceed 0 bps

Class-map: qos2 (match-any) (9132113/18)

543661 packets, 299302514 bytes

30 second offered rate 0 bps, drop rate 0 bps

Match: ip dscp 16 (6499234)

Match: ip dscp 26 (6495138)

Match: ip dscp 28 (6494626)

Match: ip dscp 30 (6492578)

Match: ip precedence 2 (4632210)

Class of service queue: 1254

Queue-limit: 16384 packets (default) Threshold drop 0 pkts, 0 bytes

Current queue-depth: 0 packets, Maximum queue-depth: 50 packets

Average queue-depth: 0.000 packets

Bandwidth: 512 kbps

Random-detect: precedence-based

Precedence	RED Label	Minimum threshold	Maximum threshold	Mark probability
0	0	262143	262143	1
1	0	262143	262143	1

2 1 3904 8000 1

3 0 262143 262143 1

4 0 262143 262143 1

5 0 262143 262143 1

6 0 262143 262143 1

7 0 262143 262143 1

Random-detect statistics

Minimum Maximum Random Threshold

Threshold Threshold Drops Drops

3904 8000 0 pkts 0 pkts

0 bytes 0 bytes

Class-map: qos1 (match-any) (9132097/15)

64957187 packets, 77768338727 bytes

30 second offered rate 11000 bps, drop rate 0 bps

Match: ip dscp 8 (8261490)

Match: ip dscp 18 (12335042)

Match: ip dscp 20 (12332994)

Match: ip dscp 22 (12333506)

Match: ip precedence 1 (10292882)

Class of service queue: 1255

Queue-limit: 16384 packets (default) Threshold drop 0 pkts, 0 bytes

Current queue-depth: 0 packets, Maximum queue-depth: 706 packets

Average queue-depth: 0.000 packets

Bandwidth: 256 kbps

Random-detect: precedence-based

Precedence RED Label Minimum Maximum Mark

threshold threshold probability

0 0 262143 262143 1

1 1 3904 8000 1

2 0 262143 262143 1

3 0 262143 262143 1

4 0 262143 262143 1

5 0 262143 262143 1

6 0 262143 262143 1

7 0 262143 262143 1

Random-detect statistics

Minimum Maximum Random Threshold

Threshold Threshold Drops Drops

3904 8000 0 pkts 0 pkts

0 bytes 0 bytes

Class-map: class-default (match-any) (14872353/0)

105985 packets, 10110313 bytes

30 second offered rate 0 bps, drop rate 0 bps

Match: any (10515090)

Class of service queue: 1253

Queue-limit: 128 packets (default) Threshold drop 0 pkts, 0 bytes

Current queue-depth: 0 packets, Maximum queue-depth: 1 packets

Average queue-depth: 0.000 packets

Random-detect: precedence-based

Precedence RED Label Minimum Maximum Mark

threshold threshold probability

0 0 262143 262143 1

1 0 262143 262143 1

2 0 262143 262143 1

3 0 262143 262143 1

4 0 262143 262143 1

5 0 262143 262143 1

6 0 262143 262143 1

7 0 262143 262143 1

Random-detect statistics

Minimum Maximum Random Threshold

Threshold Threshold Drops Drops

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Es posible gestionar el ancho de banda y la pérdida de paquetes, influenciar en el delay y jitter mediante herramientas de calidad de servicio que operan bajo la arquitectura de servicios diferenciados.
2. La arquitectura de calidad de servicio diferenciado (DiffServ), es una arquitectura que tiene como ventaja su escalabilidad y la habilidad de soportar diferentes niveles de servicio, tiene como desventaja la complejidad de su implementación y no se garantiza absolutamente la calidad de servicio.
3. La arquitectura de servicios diferenciados permite definir niveles de servicio y clases de tráfico, cada clase de tráfico recibirá un nivel de servicio.
4. Las distintas aplicaciones tienen distintos requerimientos de ancho de banda, pérdida de paquetes, delay y jitter, por lo que es necesario tener en cuenta estos parámetros al momento de realizar su clasificación en las clases de servicio.
5. Cuando la congestión se produce de forma temporal los dispositivos almacenan los paquetes en colas. Existen distintas herramientas de calidad de servicio que permiten administrar las colas de software, las colas de software cuentan con un algoritmo de programación que define el orden y la cantidad en el cual se pasan los paquetes de las colas de software a la cola de hardware, la cola de hardware es única y es la cola de salida de la interfaz. Según el mecanismo de encolamiento que se aplique, algunas clases de tráfico podrían recibir un trato prioritario lo cual es conveniente para el tráfico de voz y tráfico de video.
6. Cuando las colas de software de un dispositivo están llenas se produce el descarte de los paquetes nuevos que llegan a la cola, existen herramientas de calidad de servicio que permiten prevenir el descarte de paquetes debido a la falta de espacio para almacenar un nuevo paquete, antes de que se produzca este fenómeno se pueden implementar herramientas que permiten descartar los paquetes de una cola antes de que esta se llene. Se debe de tener cuidado al implementar las herramientas de descarte de paquetes para el

tráfico de voz, ya que el tráfico de voz es sensible al descarte de paquetes, de producirse el descarte de paquetes del tráfico de voz se tendría una conversación entrecortada.

7. Mediante herramientas de calidad de servicio de "Policing-Traffic" se puede administrar el ancho de banda de las clases de servicio.

8. Las herramientas de calidad de servicio sobre una arquitectura de servicios diferenciados permiten que un uso más óptimo de los recursos de red.

Recomendaciones

1. Se recomienda realizar el estudio de la configuración de calidad de servicio en equipos de otros fabricantes aparte de CISCO ya que en una empresa se puede contar con equipos de distintos fabricantes.

ANEXO A
GLOSARIO DE TÉRMINOS

AF PHB:	Assured Forwarding Per-hop Behavior
BW:	Ancho de banda
Bc:	Burst Committed
BA:	Behavior aggregates
CPE:	Router final del cliente
CAC:	Control de Admisión de Llamada
cRTP:	Compressed Real-Time Protocol
CBWRED:	Class Based Wighted Random Early Detection
CBWFQ:	Class Based Weighted Fair Queuing
CIR:	Committed information rate
CAR:	Committed access rate
DiffServ:	Servicios Diferenciados
DS Region:	Región de servicio diferenciado
DS Domain:	Dominio de Servicios Diferenciados
DSCP:	DiffServ Code Point
EF PHB:	Expedited Forwarding
FIFO:	Cola Firts-in Firts-out
FRTS:	Frame relay traffic shaping
G.729A:	Codec de compresión de voz
GTS:	Generic traffic shaping
IntServ:	Servicios Integrados
ISP:	Internet service provider
LAN:	Red de Area Local
LLQ:	Low Latency Queuing
MPLS:	Multiprotocol Label Switching
MPD:	Denominador de probalidad de marca
PE:	Equipo terminal del proveedor
PQ:	Prority Queuing
PHB:	Per-hop Behavior
QoS:	Calidad de servicio (Quality of Service)
RPVL:	Red Privada Virtual Local
RTP:	Real-time Transport Protocolo
RR:	Round Robin

RED:	Random Early Detection
SLA:	Service Level Agreement (nivel de servicio acordado).
Scheduling:	Programación
TCP:	Transmission Control Protocol
TCA:	Traffic Conditioning Agreement (Acondicionamiento de trafico acordado).
UDP:	User Datagram Protocol (UDP)
VoIP:	Voz sobre el protocolo IP
WAN:	Red de area amplia
WRR:	Weighted Round Robin
WRED:	Weigthed Random Early Detection
WFQ:	Weighted Fair Queuing

BIBLIOGRAFÍA

[1] Wendell Odom, Michael J. Cavanaugh "IP Telephony Self-Study Cisco QOS Exam Certification Guide", Cisco Press – USA, Segunda Edición, 2005

[2] Ernesto Ariganello, Enrique Barrientos Sevilla"Redes Cisco CCNP a Fondo Guia de estudio para profesionales", Alfaomega – México, Primera Edición, 2010.

[3] Cisco Systems, "DiffServ-the scalable end-to-end quality of service model", Cisco – EEUU, 1992- 2006

[4] Tim Szigeti, Christina Hattingh, "End-to-End QoS Network Design", Cisco Press – USA, Primera edición, 2005.

[5] RFC 2475-Internet Engineering Task Force, "An Architecture for Differentiate services", WWW.ietf.org/rfc/rfc2475.txt

[6] RFC 2474-Internet Engineering Task Force, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers" www.ietf.org/rfc/rfc2474.txt

[7] Cisco Systems, "Cisco IOS Quality of Service Solutions Configuration Guide,Realease 12.2" http://www.cisco.com

[8] Andrew S. Tanenbaum, "Redes de Computadoras", Pearson Educación – México, Cuarta Edición, 1999.

[9] http://www.cisco.com

[10] http://www.avaya.com