1210

CALIDAD DE SERVICIO EN REDES IP

Sobre los problemas de calidad de servicio en la redes IP; los umbrales de QoS definidos, las herramientas disponibles para hacerlo posible y protocolos necesarios para servicios de tiempo-real.

1- CALIDAD DE SERVICIO QoS (Quality of Service)

1.1- LOS PROBLEMAS

Se entiende por calidad de servicio la posibilidad de asegurar una tasa de datos en la red (ancho de banda), un retardo y una variación de retardo (jitter) acotados a valores contratados con el cliente. En las redes Frame Relay o ATM la calidad de servicio se garantiza mediante un contrato de **CIR** (*Commitated Information Rate*) con el usuario. Para disponer de una calidad de servicio aceptable en redes soportadas en protocolo IP se han diseñado herramientas a medida como ser los protocolos de tiempo-real RTP y de reservación RSVP. Por otro lado, un problema evidente es que cuando se soporta un servicio de voz sobre IP (VoIP) por ejemplo, los paquetes son cortos y el encabezado es largo comparativamente. En este caso se requiere un encabezado reducido y un proceso de fragmentación e intercalado **LFI**. Mediante **QoS** (*Quality os Service*) se tiende a preservar los datos con estas características.

Los servicios tradicionales de la red Internet (SMTP o FTP) disponen de una calidad denominada "*best effort*"; es decir que la red ofrece el mejor esfuerzo posible para satisfacer los retardos mínimos; lo cual no es mucho pero es suficiente para servicios que no requieren tiempo-real como el web. Para servicios del tipo "*real-time*" (voz y vídeo) se requiere una latencia mínima.

LATENCIA-JITTER. Se denomina **latencia** a la suma de los retardos en la red. Los retardos están constituidos por el retardo de propagación y el de transmisión (dependiente del tamaño del paquete), el retardo por el procesamiento "*store-and-forward*" (debido a que los switch o router emiten el paquete luego de haber sido recibido completamente en una memoria buffer) y el retardo de procesamiento (necesario para reconocimiento de encabezado, errores, direcciones, etc). Un tiempo de latencia variable se define como **jitter** (fluctuación de retardo) sobre los datos de recepción.

La solución al jitter es guardar los datos en memorias buffer, lo cual introduce un retardo aun mayor. Se han implementado diversas formas de buffer garantizados mediante software:
-Cola prioritaria: donde el administrador de la red define varios niveles (hasta 4) de prioridad de tráfico.
-Cola definida: donde el administrador reserva un ancho de banda para cada tipo de protocolo específico.
-Cola ponderada: mediante un algoritmo se identifica cada tipo de tráfico priorizando el de bajo ancho de banda. Esto permite estabilizar la red en los momentos de congestión.

1.2- VARIANTES DE SERVICIOS.

Los servicios de datos y multimediales tienen distintos requerimientos de calidad referido a latencia y jitter. Para satisfacer los requerimientos de calidad se acude al manejo de las colas de paquetes, la reservación de ancho de banda y la gestión del tráfico. Para obtener estos objetivos en diversos ámbitos se han definido variantes de servicios.

En La **Tabla 01** se encuentran las siguientes variantes de servicios: clase de servicio en redes LAN, tipo de servicio sobre protocolo IP y calidad de servicio sobre redes IP. Por otro lado se han definido las características de la calidad de servicio que se entregan en la misma Tabla: servicio garantizado (mediante reservación de nacho de banda), diferenciado (mediante prioridad de tráfico) y el "mejor esfuerzo".

Tabla 01. Calidad de servicio: variantes y clasificación.

	VARIANTES EN CAPA 2, 3 y 4
-CoS	-(*Class of Service*). CoS se logra mediante 3 bits que se ingresan en un campo adicional de 4 Bytes (etiqueta denominada *Tag* o *Label*) dentro del protocolo MAC. Estos 3 bits permiten definir prioridades desde 0 (máxima) a 7 (mínima) y ajustar un umbral en el buffer de entrada y salida del switch LAN para la descarga de paquetes. Para más detalles ver el servicio VLAN que es soportado por esta versión de funcionamiento para servicios de capa 2. Se ocupa la IEEE 802.x en los siguientes standard.
.IEEE 802.1p	-Determina el uso de un Tag en el encabezado de MAC con 3 bits de precedencia. Se define el protocolo para registración de CoS **GARP** (*Generic Attribute Registration Protocol*). Las aplicaciones específicas del GARP son la registración de direcciones multicast **GMRP** (*Multicast GARP*) y de usuarios VLAN con protocolo **GVRP** (*LAN GARP*).
.IEEE 802.1Q	-Servicio VLAN para realizar enlaces troncales punto-a-punto en una red de switch.
.IEEE 802.3x	-Este standard examina el control de flujo en enlaces Ethernet del tipo full-dúplex. Se aplica en enlaces punto-a-punto (Fast y Gigabit Ethernet). Si existe congestión se emite hacia atrás un paquete llamado "*pause frame*" que detiene la emisión por un período de tiempo determinado. Una trama denominada "*time-to-wait zero*" permite reiniciar la emisión de paquetes.
.IEEE 802.1D	-Define el protocolo **STP** (*Spanning-Tree Protocol*). Se diseñó para permitir que en una red de bridge y switch de muchos componentes se formen enlaces cerrados para protección de caminos. Se intercambia información de la topología de la red que permiten construir el árbol. De esta forma se crean puertas redundantes en el cableado, el protocolo STP deshabilita automáticamente una de ellas y la habilita en caso de falla de la otra. Cada puerto tiene una ponderación en costo (el administrador de la red puede modificar el costo para dar preferencia a cierta puerta).
-ToS	-(*Type of Service*). Es sinónimo de CoS en la capa 3. Sobre el protocolo IP se define el ToS con 3 bits (del segundo byte del encabezado IP) para asignar prioridades. Se denomina señal de precedencia.
-QoS	-(*Quality of Service*). En redes IP se define la tasa de acceso contratada **CAR** (*Committed Access Rate*) en forma similar al CIR de Frame Relay y ATM. La calidad QoS se ve garantizada mediante protocolos de reservación **RSVP** y de tiempo real **RTP** que se describen en este mismo capítulo.
	CLASIFICACION DE LA QoS
Guaranteed	-El servicio garantizado es utilizado para requerir un retardo máximo extremo-a-extremo. Se trata de un servicio análogo al CBR (*Constant Bit Rate*) en ATM. Se puede aplicar un concepto de reservación de tasa de bit (utiliza RSVP) o el método *Leaky-bucket*. Al usuario se le reserva un ancho de banda dentro de la red para su uso exclusivo aún en momentos de congestión. Se lo conoce como *Hard QoS*.
Differentiared	-El servicio diferenciado utiliza la capacidad de particionar el tráfico en la red con múltiples prioridades o **ToS** (*Type of Service*). Se dispone de 3 bits de precedencia para diferenciar las aplicaciones sensibles a la congestión (se brindan mediante el encabezado del protocolo IPv4). Es por lo tanto un *Soft QoS*. El control de aplicación es del tipo *leaky-bucket*. Se puede soportar la función **CAR** permite un management del ancho de banda (política de tráfico). La primer línea de defensa frente a la congestión es el uso de buffer de datos; lo cual implica el armado de una cola de espera y el retardo correspondiente dependiendo de la prioridad asignada en dicha cola.
Best-effort.	-Este es un servicio por *default* que no tiene en cuenta las modificaciones por la QoS. Se trata de una memoria buffer del tipo FIFO. Por ejemplo, el software Microsoft NetMeeting para aplicaciones multimediales utiliza la norma H.323 (E.164); trabaja sobre redes LAN y redes corporativas. Esta norma no tiene previsto garantizar la calidad de servicio QoS.

1.3- CACHING.

Existen 3 armas que utiliza el router para mejorar la eficiencia de la red reduciendo el tráfico que circula por la misma:
-el manejo de nombres y direcciones mediante **DNS**,
-los servicios *proxis* (se entiende por *proxi* a un elemento de la red que actúa en representación de otro) y
-el *cache* local.

Un servidor proxy es confundido con un servidor cache; sin embargo hay diferencias. Un proxy es un intermediario entre el usuario (localizado detrás del firewall) y la Internet. El proxy no necesariamente incluye una memoria cache. El Cache está localizado junto al router y se lo utiliza para reducir la carga de tráfico hacia la Internet.

Un *Cache* es un block de memoria para mantener a mano los datos requeridos frecuentemente por varios procesos. Cuando un proceso requiere información primero consulta el cache, si la información se encuentra allí se produce una mejora de la performance de funcionamiento reduciendo el retardo de procesamiento. Si no se la encuentra en el cache se buscará en otras alternativas de memoria y luego se lo encontrará disponible en el cache para una próxima oportunidad.

Una ventaja adicional de ciertos cache es la posibilidad de reducir el dialogo para transferencia de información. Por ejemplo una consulta web lleva una sesión de innumerable cantidad de objetos que son transferidos mediante un HTTP *Get-Request*. Puede reducirse la cantidad de paquetes transferidos mediante una sesión en paralelo de objetos.

Algunos tipos de memoria cache son:
-Cache del procesador: es parte del procesador y es de más fácil acceso que la memoria RAM y a una velocidad mayor.
-Disco cache: pertenece a la memoria RAM y contiene información del disco. En algunos casos se mueve en forma anticipada la información desde el disco al cache en la RAM.
-Cache cliente-servidor: se trata de un banco de memoria ubicado en el cliente para agilizar el movimiento de datos.
-Cache remoto: permite reducir los retardos cuando se accede a información de un sistema remoto en una WAN. Se resuelve mediante un *caching* de información del terminal remoto ubicado en el sistema local.
-Cache de servidor intermedio: entrega información a un grupo de clientes (*Local Workgroup*) en un sistema cliente-servidor.

WEB-CACHING. Para un ISP el uso de cache en el punto de presencia POP puede reducir el tráfico en su red (aumentando la velocidad de respuesta al usuario y el costo de la conexión WAN). Un tráfico muy común y apropiado para el cache es el Web. El cache se conecta directamente al router, el cual deriva todos los paquetes de requerimiento al cache (por ejemplo los paquetes con port-TCP de destino 80 -indica el protocolo http-), de esta forma puede verificar si la información está disponible. Su ventaja se incrementa en la medida que el número de usuarios es mayor.

Los componentes de este complejo son los siguientes:
-La memoria cache que se denominan *Cache Engine*. El cache posee suficiente memoria (ejemplo, 24 Gbytes) y capacidad de transacciones (algunos miles de sesiones TCP simultáneas).
-El router conocido como *Home Router*. El cache se conecta directamente al router de borde de la red (en la conexión hacia la Internet).
-Un router puede poseer varios cache que se denominan *cache farm*. En este caso se forma una jerarquía entre cache para sucesivas investigaciones sobre el requerimiento del usuario.
-Un router que administra el cache dialoga con la memoria mediante un protocolo **WCCP** *(Web Cache Control Protocol)*. El cache puede trabajar también en modo *Proxy* sin el protocolo WCCP y dialogando con un *Browser* configurado en forma manual.

NOTAS.
1- La desventaja del Web-Caching es que pueden aparecer diferentes versiones de un documento en la web. La duración de un documento en el cache debe ser limitada en el tiempo para reducir este efecto. La duración normalmente está especificada por el generador de la página web.

2- La introducción de firewall para seguridad de acceso a los web ha generado la idea del *Caching-Proxy*. En este contexto el proxy es un programa que interactúa entre el cliente y los servers; se trata de **URL** (*Uniform Resource Locator*). Esta posición es ideal para general el cache del web; el primer software disponible para esta función fue el servidor de web del CERN en el año 1993.

3- Existen 3 formas para medir la performance del Caching: la tasa de hit, la tasa de Byte y el tiempo de respuesta promedio. En los dos primeros casos se compara la cantidad de hits y Bytes aportados por el cache y por la Internet. El tiempo de respuesta compara el promedio del retardo de la información aportada por el cache y la Internet.

4- Existen dos protocolos para el manejo de cache en paralelo (escalabilidad del sistema): el **ICP** (*Internet Caching Protocol*) y el **CARP** (*Cache Array Routing Protocol*).

2- HERRAMIENTAS PARA QoS.

2.1- MANEJO DE CONGESTION Y TRAFICO

En la **Tabla 02** se relacionan los distintos tipos de herramientas que se disponen para asegurar una QoS dentro de una red IP. Se trata de mecanismos que previenen o manejan una congestión, distribuyen el tráfico o incrementan la eficiencia de la red. Los protocolos involucrados en asegurar la calidad de servicio son los indicados en la misma Tabla; a los mismos se refiere como mecanismos de señalización. En el ítem siguiente se analizan con detalle a los mismos.

Tabla 02. Herramientas disponibles para asegurar la QoS.

	CONTROL DE CONGESTION EN EL BUFFER DE DATOS.
-FIFO	-(*First In, First Out*). El primer mensaje en entrar es el primero en salir. Este es el mecanismo de QoS por *Default* en las redes IP. Es válido solo en redes con mínima congestión. No provee protección, no analiza el ancho de banda ni la posición en la cola de espera.
-PQ	-(*Priority Queuing*). Este mecanismo de control de congestión se basa en la prioridad de tráfico de varios niveles que puede aportar el encabezado del datagrama IP (**ToS** *Type of Service*). Se trata de 3 bits disponibles en el Byte 2 del encabezado de IPv4 (bits de precedencia).
-CQ	-(*Custom Queuing*). Este mecanismo se basa en garantizar el ancho de banda mediante una cola de espera programada. El operador reserva un espacio de buffer y una asignación temporal a cada tipo de servicio. Es una reservación estática.
-WFQ	-(*Weighted Fair Queuing*). Este mecanismo asigna una ponderación a cada flujo de forma que determina el orden de tránsito en la cola de paquetes. La ponderación se realiza mediante discriminadores disponibles en TCP/IP (dirección de origen y destino y tipo de protocolo en IP, número de *Socket* -port de TCP/UDP-) y por el ToS en el protocolo IP. En este esquema la menor ponderación es servida primero. Con igual ponderación es transferido con prioridad el servicio de menor ancho de banda. El protocolo de reservación RSVP utiliza a WFQ para localizar espacios de buffer y garantizar el ancho de banda.
	CONTROL DE TRAFICO
-WRED	-(*Weighted Random Early Detection*). Trabaja monitoreando la carga de tráfico en algunas partes de las redes y descarta paquetes en forma random si la congestión aumenta. Está diseñada para aplicaciones TCP debido a la posibilidad de retransmisión. Esta pérdida en la red obliga a TCP a un control de flujo reduciendo la ventana e incrementándola luego en forma paulatina. Un proceso de descarte generalizado, en cambio, produce la retransmisión en "olas" y reduce la eficiencia de la red. La versión ponderada WRED realiza el drop de paquetes de forma que no afecta al tráfico de tipo RSVP. Una versión superior debería considerar el tráfico de aplicación.
-GTS	-(*Generic Traffic Shaping*). Provee un mecanismo para el control del flujo de tráfico en una interfaz en particular. Trabaja reduciendo el tráfico saliente limitando el ancho de banda de cada tráfico específico y enviándolo a una cola de espera. De esta forma permite una mejor performance en topologías con tasa de bit diferentes. Este control de tráfico se relacióna con **CAR**.
	INCREMENTO DE LA EFICIENCIA. SEÑALIZACIÓN.
-LFI	-(*Link Fragmentation and Interleaving*). El tráfico interactivo como Telnet y VoIP es susceptible de sufrir latencia y jitter con grandes paquetes en la red o largas colas en enlaces de baja velocidad. Se basa en la fragmentación de datagramas y el intercalado de los paquetes de tráfico.
-RSVP	-(*Resource Reservation Protocol*). Se trata de implementar el concepto de Señalización. Se dispone de dos tipos de señalización: en-banda (por ejemplo los bits de precedencia para ToS) y fuera-de-banda (mediante un protocolo de comunicación como el RSVP). Este protocolo permite que un host o un router asegure la reservación de ancho de banda a lo largo de la red IP.
-RTP-HC	-(*Real-Time Protocol-Header Compression*). El protocolo de tiempo real RTP es estudiado por separado más adelante. La compresión del encabezado permite mejorar la eficiencia del enlace en paquetes de corta carga útil. Se trata de reducir los 40 bytes de RTP/UDP/IP a una fracción de 2 a 5 bytes, eliminando aquellos que se repiten en todos los datagramas.

No todas las herramientas disponibles son usadas en los mismos routers. Por ejemplo, la clasificación de paquetes, el control de admisión y el manejo de la configuración se usan en los router de borde (*eage*), en tanto que en los centrales (*backbone*) se gestiona la congestión. El tratamiento de la congestión se fundamenta en el manejo de las colas en buffer mediante diferentes técnicas. El buffer es la primer línea de defensa frente a la congestión. El manejo correcto (mediante **políticas de calidad** de servicio) del mismo permite determinar el servicio de calidad diferenciada. Una segunda defensa es el control de flujo. El problema del control de flujo en TCP es que se ha planea de extremo-a-extremo y no considera pasos intermedios. En TCP cada paquete de reconocimiento (*Acknowledgment*) lleva una crédito (*Window*) con el tamaño del buffer disponible por el receptor. Un sobreflujo de datos en los routers de la red se reporta mediante el mensaje *Source Quench* en el protocolo ICMP. Estos mecanismos son ineficientes y causan severos retardos en la conexión.

2.2 PRIORIZACION DE TRAFICO

ToS/IEEE 802.1Q. Los standard IEEE 802.10 y 802.1Q fueron propuestos para el manejo de las redes VLAN; este último es el utilizado con regularidad. En el standard 802.1Q se define el VLAN *Tagging Switch* que permite una identificación de la VLAN y la posibilidad de priorización del servicio. La trama del paquete en capa MAC incluye 4 Bytes adicionales al IEEE 802.3 que se colocan luego de las direcciones MAC y antes del *Type/Length*. Los 4 Bytes son indicados a continuación. Obsérvese la presencia de 3 bits para prioridad de tráfico y 12 bits para identificación de VLAN.

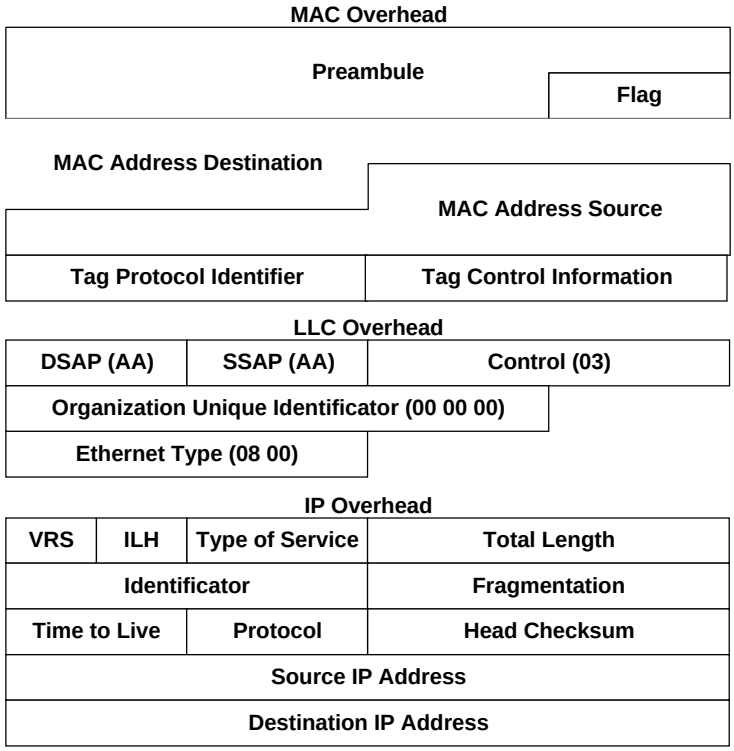
Tabla 03. Campos para manejo de Tipo de Servicio en IEEE 802.3

-TPID	(*Tag Protocol Identifier*). 2 Bytes. Usados para identificación del protocolo. En Ethernet es hexa=8100.
-TCI	(*Tag Control Information*). 2 Bytes usados para las siguientes funciones:
.UP	3 bits para prioridad del usuario (*User Priority*). Se trata de CoS desde 0 a 7. Esta información permite poner en práctica la CoS definida en IEEE 802.1p.
.CFI	(*Canonical Format Indicator*). 1 bit para ser usado por Token Ring.
.VLANI	(*VLAN Identifier*). Este campo de 12 bits permite identificar la VLAN (válido desde 1 a 1005). Permite la interoperación entre diferentes productores.

El mecanismo que se define para la CoS (clase 0 a 7 desde alta a baja prioridad) se compone de las colas de recepción y transmisión. El umbral para extraer los paquetes de la cola de recepción son:
-Clase de servicio CoS 0/1: umbral del 50% (máxima prioridad).
-CoS 2/3: umbral al 60%.
-CoS 4/5: umbral al 80%.
-CoS 6/7: umbral al 100% (mínima prioridad).

En transmisión existen dos colas la de alta y baja prioridad. Su relación con la CoS es la siguiente:
-Cola de baja prioridad (corresponde al umbral del 80%) y CoS 0/1: umbral al 40%; con CoS 2/3: umbral al 100%.
-Cola de alta prioridad (corresponde al umbral del 20%) y CoS 4/5: umbral al 40%; con CoS 6/7: umbral al 100%.

Por ejemplo, una puerta del switch que no fue configurada para CoS tiene un valor por default de umbral del 100%. Un servicio clase CoS=2/3 en el buffer de recepción (entrada al switch) tiene un umbral al 60% para la extracción de paquetes, mientras que en el de transmisión se coloca en alta prioridad (umbral al 20%) y con CoS=2/3 tiene una prioridad adicional del 80%.



QoS/RFC. El campo de precedencia en el encabezado de IPv4 permite definir varios tipos de servicio ToS. Se trata de 3 bits que por razones históricas tienen diferentes nombres (routing, priority, etc) y que pueden ser usados para signar prioridad. Se

aplica un control de acceso extendido EACL para definir la política de la red en términos de congestión. En redes heterogeneas se debe mapear este tipo de servicio en equivalentes (tag switch, Frame Relay y ATM).

Con Los bits de precedencia se pueden realizar 3 tipos de acciones: routing basado en políticas **PBR** (*Policy-Based Routing*) (por ejemplo direcciones IP, port de TCP, protocolo, tamaño de paquetes, etc); propagar la política de QoS mediante el protocolo de routing BGP-4 y desarrollar una política de tasa de acceso contratada CAR. La **CAR** (*Committed Access Rate*) se ofrece especificando políticas de tráfico y ancho de banda. El umbral de CAR se aplica a la puerta de acceso para cada puerta IP o por flujo de aplicación individual. Una técnica disponible para manejar el CAR es el *netflow switch* que se comenta más adelante.

Algunas opciones de política de CAR son:
-Política de prioridad:
  CAR máximo (el exceso de ancho de banda es descartado);
  CAR premium (el exceso es señalado con un nivel de preferencia más bajo);
  CAR best effort (por encima de un umbral se cambia la preferencia y sobre otro los paquetes son eliminados);
-Política de asignación:
  CAR por aplicación (diferentes políticas son usadas en distintas aplicaciones; por ejemplo bajo nivel para HTTP).
  CAR por puerta (los paquetes que ingresan por un port son clasificados con alto nivel de prioridad).
  CAR por dirección (puede diferenciarse entre la dirección IP de origen y destino y asignar la prioridad en cada caso).

2.3- FORMACIÓN DE ANILLOS

El protocolo **STP** (*Spanning-Tree Protocol*) es desarrollado originalmente en Digital DEC y luego fue incorporado a **IEEE 802.1d**. En las redes construidas mediante Switch-Ethernet se debe cuidar que no ocurran loop debido a que los caminos duplicados pueden generar paquetes duplicados. El uso de STA permite eliminar el problema de los loops y mantener las ventajas derivadas de la redundancia de enlaces (este párrafo puede leerse asi: “como generar pequeños anillos que permitan una reconfiguración en caso de corte de un enlace principal”).

Se trata de configurar la red de switch con enlaces en loop para incrementar la redundancia. Los loops están prohibidos en Ethernet pero mediante el protocolo STP se puede configurar la red en forma automática para detectar los loops e interrumpirlos hasta que una falla los habilite como necesarios. Las posibles configuraciones son:
-El STP se puede habilitar para cada VLAN en particular.
-A los port se les asigna una prioridad y un costo para que STP determine el mejor camino.
-Se puede determinar el estado de la port (bloqueado, deshabilitado, forwarding, etc). Desde bloqueo a forward se pasa por listening y learning.
-*PortFast* es una función que habilita a pasar desde el bloqueo a forward sin pasar por los estados intermedios.
-*UplinkFast* permite una rápida convergencia para cambios con enlaces redundantes. Otra variante es *BackboneFast*.

La port que utiliza la función STP se encuentra en algunos de los siguientes estados: bloqueado (no participa de la transmisión), listening (es un estado transitorio luego del bloqueo y hacia el forwarding), learning (es otro estado transitorio antes de pasar al forwarding), forwarding (transmite las tramas en forma efectiva) y dehabilitado (se trata del estado no-operacional). Si todas las port tienen la misma prioridad el forward lo realiza la port de menor número.

Este protocolo permite identificar los loop y mantener activa solo una puerta del switch. Por otro lado, utiliza un algoritmo que permite identificar el mejor camino libre-de-loops en la red de switch. Para lograr este objetivo, se asigna a cada puerta un identificador consistente en la dirección MAC y una prioridad. La selección de la puerta se puede asignar en términos de prioridad (valor entre 0 y 63; por default es 32) y costo (0 a 65535).

El STP consiste en un intercambio de mensajes de configuración en forma periódica (entre 1 y 4 seg). Cuando se detecta un cambio en la configuración de la red (por falla o cambio de costo de la port) se recalcula la distancia (sumatoria de costos) para asignar una nueva puerta. Las decisiones se toman en el propio switch. En condiciones normales se selecciona un switch para que trabaje como *Root Switch* para determinar un topología de red estable (es el centro lógico de la topología en *Tree*). Por *default* el switch que posee la dirección MAC más baja es el seleccionado como root.

Los mensajes disponibles se denominan *Bridge-PDU* y son de dos tipos: *Configuration* y *Topology-change*. Los campos del mensaje de configuración incluyen 35 Bytes y el de cambio de topología solo los 4 Bytes iniciales. Por ejemplo, el mensaje de configuración contiene los siguientes campos de información.

Tabla 04. Campos para el protocolo STP.

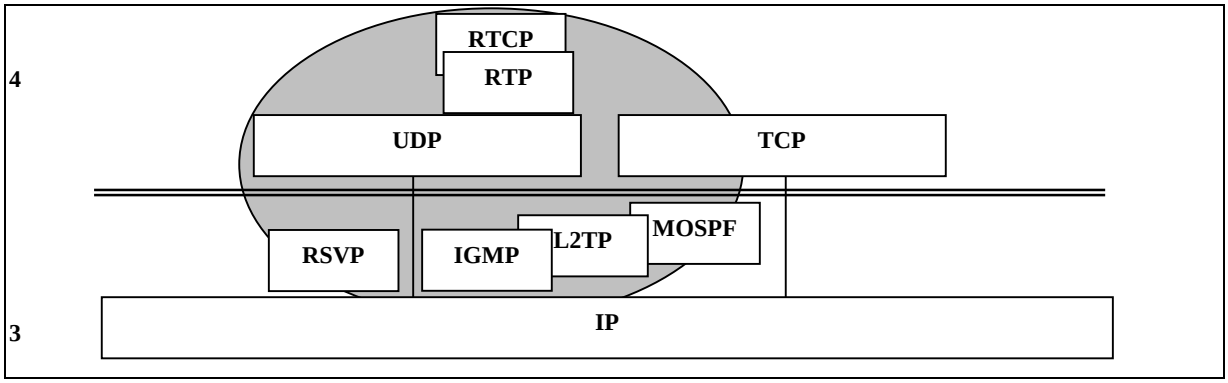
3 Bytes	Indica el Identificador de Protocolo (2) y la Versión (1).
1 Byte	Identifica el Tipo de Mensaje (0 para configuración y 128 para cambio de topología).
1 Byte	Flag para indicar el cambio de configuración de la red.
12 Bytes	Se identifica la raíz (*Root*) mediante 8 Bytes y con 4 Bytes se identifica el costo de la ruta.
10 Bytes	Se identifica el switch mediante 8 Bytes y con 2 Byte se identifica la puerta del mismo.
4 Bytes	2 Bytes para identificar el tiempo de emisión del mensaje (*Age*) y 2 Byte para el tiempo máximo de vida.
2 Bytes	Indica el período de intercambio de mensajes de configuración *Hello*.
2 Bytes	Indica el tiempo de espera para emitir un mensaje en caso de detectar un cambio de configuración.

3- PROTOCOLOS RSVP/RTP

En la **Tabla 05** se enumeran los protocolos que se estudian a continuación para asegurar la calidad de servicio en aplicaciones de tiempo-real.

Tabla 05. Protocolos para asegurar la calidad de servicio QoS.

RSVP	-(*Resource Reservation Protocol*). Este protocolo permite que un host o un router asegure la reservación de ancho de banda a lo largo de la red IP. Es del tipo orientado al receptor (el receptor solicita la reservación) y es útil para aplicaciones de tipo símplex (unidireccional). Puede funcionar como unicast o multicast.
RTP	-(*Real-time Transport Protocol*). Se utiliza sobre el protocolo UDP para aplicaciones como H.323 o VoIP.
RTCP	-(*Real-Time Transport Control Protocol*). Este protocolo se utiliza para control de calidad de servicio sobre aplicaciones que trabajan sobre RTP.
IGMP	-(*Internet Group Management Protocol*). Este protocolo se utiliza para aplicaciones del tipo multicast cuando se requiere distribuir la misma información sobre un grupo (multicast) de usuarios y reduciendo el ancho de banda ocupado. Se emite un mismo paquete con dirección multicast en lugar de uno para cada dirección unicast. Es estudiado en otro trabajo.



3.1- RESERVACION DE ANCHO DE BANDA (RSVP)

Los servicios del tipo SMTP o FTP en Internet son con calidad "best effort"; es decir, no prevén una calidad de servicio. Esto tiene como consecuencia una latencia variable y jitter sobre la información del tipo tiempo-real (audio o vídeo). RSVP permite la reservación de ancho de banda para asegurar una QoS. El protocolo RSVP trabaja en conjunto con el protocolo de transporte **RTP** para servicios de voz y vídeo en tiempo-real. El RSVP está disponible en RFC-2205.

Existen dos formas de reservación del ancho de banda: estática y dinámica. La reservación estática permite asignar un porcentaje fijo del canal de comunicación a cada tipo de protocolo (por ejemplo, 10% a HTTP, 15% a FTP, 3% a Telnet, etc). El protocolo RSVP permite reservar el ancho de banda en forma dinámica para asegurar una calidad de servicio **QoS** en las redes IP. La QoS permite garantizar el servicio en forma CAR similar al CIR de Frame Relay.

El protocolo RSVP se define para los servicios integrados en Internet. Es utilizado por el host para solicitar una QoS al router para una aplicación particular y es usado por el router para establecer un ancho de banda con todos los nodos intermedios del trayecto.

Opera tanto sobre IPv4 como sobre IPv6; no es un protocolo de routing y solo se lo utiliza para reservar ancho de banda y buffer. En el modelo de capas el protocolo RSVP ocupa la función de la capa 3 sobre IP, en la misma forma que los protocolos de routing (OSPF y BGP), de multicast (IGMP), de gestión (ICMP) y de transporte (TCP y UDP). Una sesión manejada por del protocolo RSVP está definida mediante 3 direcciones: la dirección IP de destino (receptor), el identificador de protocolo y la port de UDP.

Está definido para operar en forma de unicast o multicast. En el caso de operar con protocolo multicast primero se establece el enlace mediante IGMP (para establecer el grupo) y luego mediante RSVP (para establecer la reservación). Por otro lado el RSVP es un protocolo de carácter símplex, es decir unidireccional. Está orientado-al-receptor; en el sentido que es el receptor el que solicita la reservación y la interrumpe.

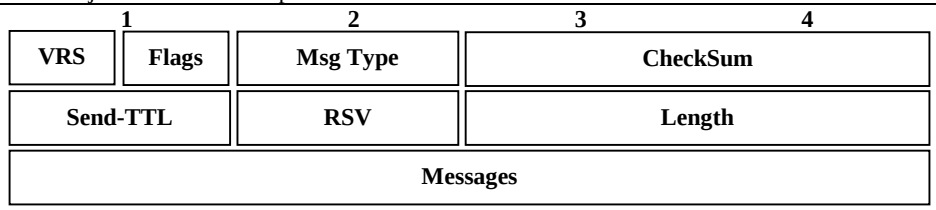
CONTROL DE TRAFICO. La QoS es implementada por un mecanismo de flujo de datos denominado "control de tráfico". Este mecanismo incluye 3 etapas:

-la clasificación del paquete para determinar la QoS y la ruta de cada paquete;
-el control de admisión para asegura la disponibilidad de la reservación y
-el proceso de determinación temporal de emisión (*Packet Scheduler*).
El requerimiento de reservación es iniciado por host receptor y pasa por los distintos router de la red. Si algún mecanismo intermedio falla se genera un reporte de error. Se dispone de dos mensajes de error: *ResvErr* y *PathErr*.

Este protocolo mantiene en forma "soft" el estado de los routers y host, entregando un soporte dinámico para cambios de miembros y adaptación automática de cambios de routing. No es un protocolo de routing pero depende de los mismos. Los mensajes de *Path* y *Reservation* se utilizan a estos propósitos. Una lista más completa de los tipos de mensajes (denominado *State Block*) del protocolo RSVP se encuentran en la **Tabla 06**.

Tabla 06. Campos que componen el paquete de RSVP (*Reservation Protocol*).

-VRS	4 bits. Versión del protocolo (actualmente la versión 1).
-Flags	4 bits. No se han definido bits de flag hasta el momento.
-Msg Type	1 Byte. Identifica el tipo de mensaje que ocupa el campo de longitud variable al final del paquete. Se dispone de los siguientes casos: Path, Reser, PathErr, ResvErr, PathTear, ResvTear, ResvConf.
-Checksum	2 Bytes. Chequeo de paridad del protocolo RSVP.
-Send-TTL	1 Byte. Se trata del tiempo de vida de IP con que se emite el paquete de RSVP.
-RSV	1 Byte. No usado.
-Lenght	2 Bytes. Longitud total del mensaje en bytes incluyendo la longitud variable.
-Messages	Nx4 Bytes. Mensaje de longitud variable en palabras de 32 bits.
.Resv	-Mensaje emitido paso-a-paso desde el receptor al emisor para reservación de ancho de banda.
.Path	-Mensaje emitido en forma regular para cada flujo de datos del emisor al receptor. No se enruta mediante RSVP para asegurar la llegada al receptor mediante las direcciones IP.
-Teardown	-Mensajes (*Path and Reservation*) usados para desarmar el camino y la reservación efectuada.
-Error	-Reporta errores en el procesamiento del mensaje *Path* o *Resv*.
-Resv Conf	-Mensaje emitido como respuesta al *Resv*.



3.2- PROTOCOLO DE TIEMPO-REAL (RTP) (*Real-Time Transport Protocol*).

Tanto el protocolo de transporte en tiempo-real RTP como el protocolo de control RTCP se encuentran disponibles en RFC-1889 del año 1996. El protocolo RTP tiene como objetivo asegurar una QoS para servicios del tipo tiempo-real. Incluye la identificación del payload, la numeración secuencial, la medición de tiempo y el reporte de la calidad (protocolo RTCP). Entre sus funciones se encuentran la memorización de datos, la simulación de distribución interactiva, el control y mediciones de aplicaciones.

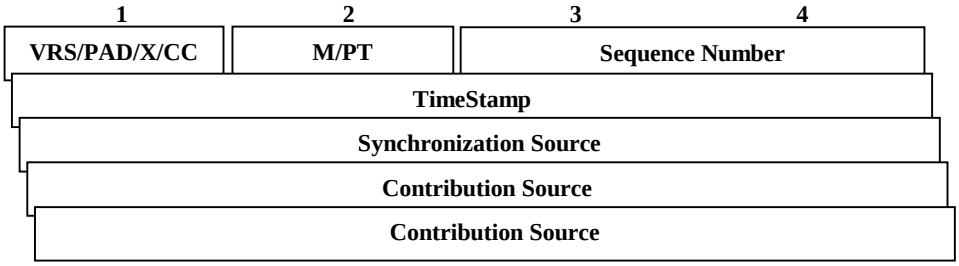
Este protocolo **RTP** es de transporte (capa 4) y trabaja sobre **UDP** de forma que posee un checksum para detección de error y la posibilidad de multiplexación de puertas (port UDP). Las sesiones de protocolo RTP pueden ser multiplexadas. Para ello se recurre a un doble direccionamiento mediante las direcciones IP y el número de port en UDP. Sobre RTP se disponen de protocolos de aplicación del tipo H.320/323 para vídeo y voz (H.32x forma una familia del ITU-T de normas para videoconferencia). El protocolo de H.323 se detalla entre los servicios de las redes IP. Junto a RTP se dispone del protocolo de control **RTCP**.

El RTP funciona en conjunto con **RSVP** (capa 3) para la reservación de ancho de banda y asegurar de esta forma la calidad del servicio QoS del tipo Garantizada. La QoS del tipo Diferenciada se logra mediante la priorización de tráfico que puede adoptar dos alternativas. En IP se pueden asignar diversos alternativas de prioridad para formar una cola de espera en routers. Un algoritmo particular de gestión de prioridad de tráfico es el **WFQ** (*Weighted Fair Queuing*) que utiliza un modelo de multiplexación TDM para distribuir el ancho de banda entre clientes. Cada cliente ocupa un intervalo de tiempo en un *Round-Robin*. El **ToS** (*Type of Service*) en IP puede determinar un ancho de banda específico para el cliente. Un servicio sensible al retardo requiere un ancho de banda superior. En IP además del ToS se puede utilizar la dirección de origen y destino IP, tipo de protocolo y número de *socket* para asignar una ponderación.

RTP además provee transporte para direcciones unicast y multicast. Por esta razón, también se encuentra involucrado el protocolo **IGMP** para administrar el servicio multicast. El paquete de RTP incluyen un encabezado fijo y el payload de datos; RTCP utiliza el encabeza del RTP y ocupa el campo de carga útil. Los campos del encabezado fijo del protocolo RTP se muestran en la **Tabla 07**.

Tabla 07. Protocolos para Tiempo-Real RTP (*Real-Time Protocol*).

-OH	2 Bytes de encabezado fijo para aplicaciones de identificación.
.VRS	2 bits. Es la versión del protocolo. Actualmente se utiliza la versión 2 (RFC-1889).
.PAD	1 bit. El bit de padding activo informa que luego del encabezado existen bytes adicionales (por ejemplo para algoritmos de criptografía).
.X	1 bit. Con el bit de extensión activado existe solo una extensión del encabezado.
.CC	4 bits. (*CSRC Count*). Identifica el número de identificadores CSRC al final del encabezado fijo.
.M	1 bit de *Marker*. La interpretación está definida por el perfil.
.PT	7 bits. (*Payload Type*). Identifica el formato de payload y determina la interpretación de la aplicación.
-SN	2 Bytes. (*Sequence Number*). Numera en forma secuencial los paquetes de RTP y permite la identificación de paquetes perdidos.
-TS	4 Bytes. (*TimeStamp*). Refleja el instante de muestreo del primer Byte en el paquete RTP. Permite el cálculo del tiempo y jitter en la red. Por ejemplo, en una aplicación de audio que comprime cada 160 muestras, el reloj se incrementa en 160 en cada bloque.
-SSRC	4 Bytes. (*Synchronization Source*). Identifica la fuente de sincronismo de forma que dos sesiones del mismo RTP tengan distinta SSRC.
-CSRC	Nx4 Bytes. (*Contribution Source*). Identifica la fuente que contribuye al payload contenido en el paquete. El valor de N lo da el campo CC.



RTP-HC (*Real-Time Protocol-Header Compression*). La compresión del encabezado permite mejorar la eficiencia del enlace en paquetes de corta carga útil. Se trata de reducir los 40 bytes de RTP/UDP/IP a una fracción de 2 a 5 bytes, eliminando aquellos que se repiten en todos los datagramas. (*RTP*). Como los servicios de tiempo-real generalmente trabajan con paquetes pequeños y generados en forma periódica se procede a formar un encabezado de longitud reducida que mejore la eficiencia de la red.

3.3- PROTOCOLO DE CONTROL RTCP (*Real-Time Control Protocol*).

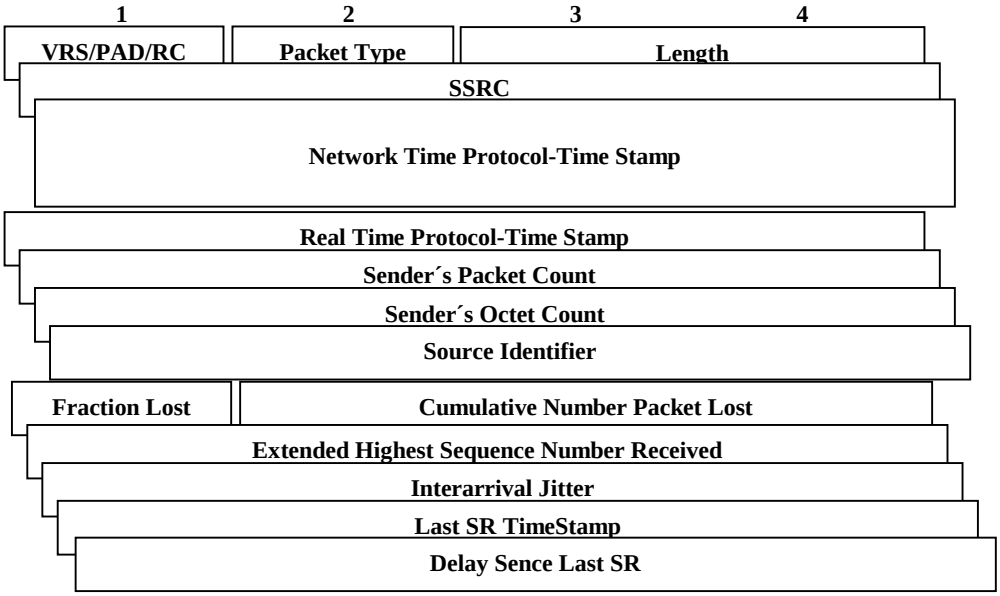
Este protocolo permite completar a RTP facilitando la comunicación entre extremos para intercambiar datos y monitorear de esta forma la calidad de servicio y obtener información acerca de los participantes en la sesión. RTCP se fundamenta en la transmisión periódica de paquetes de control a todos los participante en la sesión usando el mismo mecanismo RTP de distribución de paquetes de datos. El protocolo UDP dispone de distintas puertas (*UDP Port*) como mecanismo de identificación de protocolos. La función primordial de RTCP es la de proveer una realimentación de la calidad de servicio; se relaciona con el control de congestión y flujo de datos.

RTCP involucra varios tipos de mensajes (uno de los más interesantes el *send report* se informa en la **Tabla 08**):

-Send report	para emisión y recepción estadísticas (en tiempo random) desde emisores activos.
-Receiver Report	para recepción estadísticas desde emisores no activos.
-Source Description	para un identificador de nivel de transporte denominado CNAME (*Canonical Name*).
-Bye	para indicar el final de la participación.
-Application	para aplicaciones específicas.

Tabla 08. Protocolo de control RTCP (*Real-Time Control Protocol*). Mensaje *Sender Report.*

	ENCABEZADO COMUN
-OH	1 Byte de encabezado con las siguientes funciones:
.VRS	2 bits. Identifica la actual versión (2) del protocolo.
.PAD	1 bit. Indica si luego de este paquete existe un padding adicional (por ejemplo, para completar el número de Bytes para criptografía en múltiplo de 8).
.RC	5 bits. (*Reception Report Count*). Contiene el número de bloques de reportes (unidades de 6x4 Bytes) que contiene el paquete. Un paquete puede contener más de un reporte de retorno.
-PT	1 Byte. (*Packet Type*). Identifica el tipo de paquete (decimal=200 para el paquete *Sender Report* que se enumera en este ejemplo).
-Length	2 Bytes. Indica la longitud del paquete en unidades de 4 Bytes.
-SSRC	4 Bytes. Identifica la fuente de temporización para el generador del reporte.
	INFORMACION PARA EVALUACION DE PARAMETROS
-NTP-TS	8 Bytes. (*Network Time Protocol-TimeStamp*). Es el tiempo relativo al UTC 00:00:00 horas del día 01-01-1900. Este campo de 8 Byte y es el *TimeStamp* completo. Para otras aplicaciones se utiliza una versión reducida de 4 Bytes con la información de tiempo más significativa.
-RTP-TS	4 Bytes. Se refiere al *TimeStamp* que es emitido en el RTP.
-SPC	4 Bytes. (*Sender´s Packet Count*). Es el total de paquetes emitidos por el transmisor desde el inicio de la sesión.
-SOC	4 Bytes. (*Sender´s Octet Count*). Es el total de Bytes transmitidos desde el inicio de la sesión como carga útil. Es usado para estimar la tasa de datos promedio de payload en conjunto con SPC.
	REPORTES DE PARAMETROS EVALUADOS
-SSRC-n	4 Bytes. (*Source Identifier*). Identifica la fuente SSRC de información en el reporte de recepción.
-FL	1 Byte. (*Fraction Lost*). Indica la relación fraccional (paquete perdido/total de paquetes) de paquetes perdidos desde el último reporte.
-CNPL	3 Bytes. (*Cumulative Number Packet Lost*). Indica el total de paquetes perdidos desde el inicio de la recepción.
-EHSNR	4 Bytes. (*Extended Highest Sequence Number Received*). Indica la numeración secuencial de recepción. Si el inicio de la recepción es distinto implica que los distintos posibles receptores (multicast) tienen un campo EHSNR diverso.
-IJ	4 Bytes. (*Interarrival Jitter*). El jitter se mide como la desviación de recepción respecto de la transmisión (en unidades de timestamp). Equivale a la diferencia de tiempo de tránsito relativo.
-LSR-TS	4 Bytes. (*Last SR TimeStamp*). Es el último *timestamp* (información más significativa) de los paquetes recibidos.
-DLSR	4 Bytes. (*Delay Since Last SR*). Es el retardo (entre la emisión y recepción) en unidades de 1/65536 seg del último paquete recibido.



El mensaje *Send Report* disponen de 3 secciones bien diferenciadas:
-Los primeros 8 Bytes (desde la versión hasta el identificador de la fuente de temporización SSRC) se refieren a un encabezado común.
-La segunda parte de 20 Bytes (desde el tiempo universal de emisión NTP-TS hasta el conteo de octetos emitidos SOC) permite la evaluación de diferentes parámetros (retardo, jitter, eficiencia de datos, etc).

-La tercera parte de 24 Bytes lleva reportes que han sido obtenidos desde el último reporte informado. Obsérvese la presencia de reporte referido a la cantidad total de paquetes RTP perdidos y a la proporción de los mismos; la cantidad de paquetes recibidos y el jitter entre paquetes; el horario del último paquete recibido y el retardo de transmisión del mismo.

La medición de tiempo se realiza mediante la emisión del **NTP-TS** (*Network Time Protocol-TimeStamp*) de 8 Bytes de longitud. Es el tiempo relativo al UTC 00:00:00 horas del día 01-01-1900. La precisión es de 32 bits a cada lado de la coma para el segundo. Como esto puede ser innecesario en diversas aplicaciones se utilizan variantes reducidas de Byte. Por ejemplo para la medición de jitter se utiliza unidades de 1/65536 seg (2^{16}).

El lector informado sobre redes ATM puede comparar este formato de RTCP con el utilizado en AAL5/ATM para reportes y mediciones de calidad de servicio (tasa de error, tasa de celdas perdidas, etc). La riqueza de lo proyectado en RTCP es sustancialmente superior.