Sistemas de Transporte de Datos

Ingeniería Informática (9186)

Manual de la Práctica 3:

Calidad de Servicio. Análisis de tráfico en redes IEEE 802.11

Francisco Andrés Candelas Herías

Santiago Puente Méndez

Grupo de **I**nnovación **E**ducativa en **A**utomática

Universitat d'Alacant
Universidad de Alicante

P3. Calidad de Servicio. Análisis de tráfico en redes IEEE 802.11

1. Objetivos

- Introducir los conceptos básicos sobre gestión de calidad de servicio (QoS).
- Conocer como un router puede clasificar el tráfico de una red, y como puede gestionar de forma diferente los distintos tipos de tráfico.
- Experimentar los efectos de una estrategia sencilla de gestión de calidad de servicio.
- Saber capturar, analizar e interpretar el tráfico en redes inalámbricas IEEE 802.11.

2. Conocimientos básicos

2.1. Calidad de servicio

El nivel de red de una arquitectura de red no solo debe realizar funciones de enrutamiento de paquetes, sino que también debe realizar otras tareas muy importantes, como son el control de congestión o la gestión de la calidad de servicio, dos aspectos que están muy relacionados. Los routers son los principales encargados de realizar esas tareas.

En primer lugar, se debe tratar de evitar que una red llegue a un estado de congestión, en donde los servicios que ofrece empiezan a degradarse rápidamente, como muestra la **Figura 1**, y, en caso de producirse esa congestión, detenerla cuanto antes. Esto se consigue mediante las técnicas de control de flujo de los protocolos y a una adecuada gestión de la calidad de servicio (o QoS: *Quality of Service*). Aunque la gestión de QoS no es necesaria cuando en una red no hay congestión, y se dispone de suficiente ancho de banda para el tráfico de datos soportado, es muy importante disponer de esa gestión cuando en la red empieza a producirse congestión, ya que si la gestión se aplica solo cuando la congestión es importante, resulta inútil.

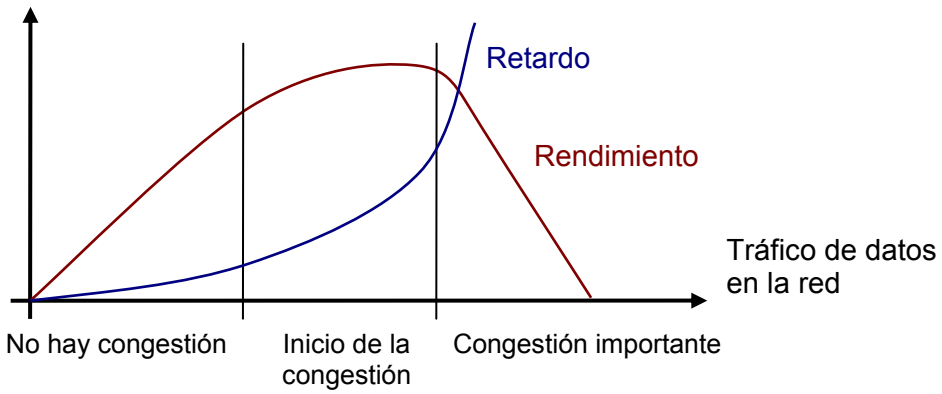

Figura 1. Rendimiento de una red frente al tráfico que soporta.

La gestión de QoS hace referencia a la capacidad que tiene una red para ofrecer un mejor servicio para determinado tipo de tráfico o usuarios sobre las diferentes tecnologías de transporte de datos en las que se apoya (TCP/IP; LAN Ethernet, ATM, SONET...). Hay que

tener en cuenta que aplicaciones diferentes demandan diferentes servicios, en relación a anchos de banda, retardos máximos, variación de los retardos (*jitter*) o fiabilidad ante errores y pérdidas de paquetes. Evidentemente no es igual el tráfico de datos generado por una aplicación multimedia que trasmite una señal de voz (como una basada en el estándar VoIP: *Voice Over IP*), que el tráfico generado al acceder a una pagina Web (protocolo HTTP), por poner un ejemplo, aunque los datos de ambas se transmitan sobre la misma red de datos. A pesar de las ventajas que proporciona la gestión de QoS, muchas veces no se aplica por desconocimiento, y se deja que la red simplemente proporcione el mejor servicio posible que ofrece su ancho de banda.

El objetivo general de la gestión de QoS es administrar los anchos de banda disponibles y los retardos de la red para asegurar los servicios demandados por las aplicaciones, y aumentar todo lo posible las prestaciones de la red. Esta gestión se puede llevar a cabo en distintas partes de la red. Primero, en los equipos de la red, especialmente en los de interconexión (routers), donde se aplican estrategias de colas, planificación y gestión y perfilado de tráfico. Segundo, en los protocolos de la red, que pueden incluir cierta información (llamada QoS *signaling*) para coordinar la gestión de calidad de servicio. Y, tercero, a nivel de administración, con políticas adecuadas de contabilidad y mantenimiento. Este bloque se centrará en las dos primeras posibilidades.

La gestión de QoS depende mucho de la necesidad de transportar distintos tipos de tráfico en redes multimedia, y los protocolos actuales proporcionan medidas e información para efectuar dicha gestión. En general, el QoS *signaling* es una forma de comunicación entre equipos para señalizar situaciones relativas a la gestión del QoS. Muchos protocolos (de nivel de enlace, de red o superiores) incluyen características que posibilitan esta comunicación, como por ejemplo, campos de control en el paquete o la trama del protocolo que sirven para especificar el tipo de paquete o la clase de tráfico que transporta.

Existen dos formas básicas de abordar la gestión de QoS: mediante reserva de recursos (también conocida como *Integrated Services*), o mediante gestión de prioridades o clasificaciones de diferentes tipos de tráfico de datos (también denominada *Differentiated Services*). Mientras que con la primera se reserva un ancho de banda exclusivo para un determinado tráfico crítico, la segunda no define reservas y simplemente define que un tipo de tráfico es más importante que otro. Aunque la gestión de prioridades requiere un marcado de los datos con las prioridades es bastante más sencilla de gestionar que la reserva, puesto que esta última requiere que los routers mantengan determinado estado de las conexiones y compartan información sobre ese estado con protocolos especiales. Además, la reserva es poco escalable, y llega a ser inviable en grandes redes troncales debido a la complejidad del estado que deben manejar los routers. Esta práctica se centra en la gestión de prioridades.

2.2. QoS signaling

2.2.1. QoS signaling con IP

Algunos protocolos antiguos ya incluían ciertos campos de control para efectuar una gestión sencilla. Es el caso del protocolo de red IP, para el que se definió originalmente un campo dentro de la cabecera de sus paquetes dedicado a diferenciar los distintos tipos de tráfico que pueden viajar en su campo de datos [1]. Este campo, de un byte de tamaño, se conoce como ToS (*Type of Service*), y ocupa el segundo byte de la cabecera de un paquetes (el primer byte de la cabecera incluye la versión de IP y el tamaño de la cabecera, y habitualmente tiene el valor 45h). El campo de ToS se desglosa a su vez en otros valores, como muestra la **Figura 2**.

Los tres bits de mayor peso del ToS representan un valor conocido como precedencia. Este valor permite clasificar el tráfico en ocho tipos diferentes. Realmente, de los ocho tipos se utilizan normalmente seis, ya que los valores 6 y 7 se reservan para uso interno de la red. El valor de precedencia 0 (*routine*) es el normal, con la prioridad más baja, y el que usa por defecto si no se indica otra cosa.

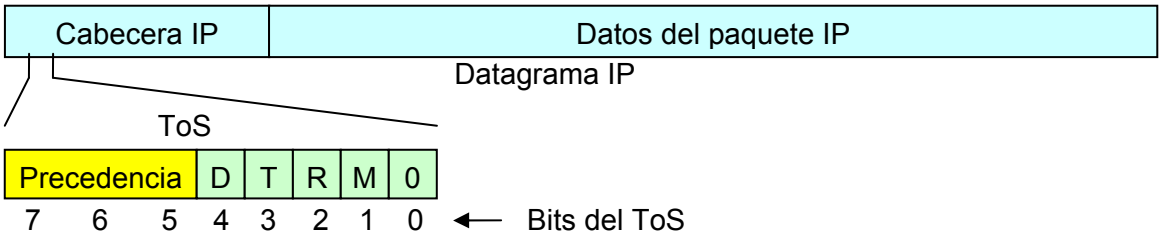

Figura 2. QoS Signaling en IPv4 según RFC 1349.

La siguiente tabla muestra cada valor de precedencia, con su nombre y el valor correspondiente para todo el campo de ToS, suponiendo que los bits D, T, R y M son cero.

Precendecia	ToS (Hex)	ToS (Dec)	Tipo de tráfico
0 – 000	00	0	Routine
1 – 001	20	32	Priority
2 – 010	40	64	Inmediate
3 – 011	60	96	Flash
4 – 100	80	128	Flash override
5 – 101	A0	160	Critic
6 – 110	C0	192	Internetwork control
7 – 111	E0	224	Network control

Mientras que para aplicaciones como el acceso a páginas Web con HTTP o el envío de correo electrónico con SMTP se puede mantener un valor de precedencia 0, para otras aplicaciones como VoIP (voz sobre IP), conviene escoger un valor de precedencia más alto.

En cuanto a los bits D, T, R y M, según la especificación sirven para indicar que interesa más para la transmisión del datagrama: minimizar el retardo (Delay), maximizar el rendimiento (Thoughput), maximizar la fiabilidad (Reliability) o minimizar el coste económico (Monetary cost) [1]. En la práctica, estos bits no se han llegado a utilizar de forma generalizada.

La definición de ToS no se ha extendido mucho, y los fabricantes no se han preocupado de garantizar una compatibilidad entre equipos de diferentes marcas. Sin embargo, es una forma sencilla de gestionar prioridades de datos en aplicaciones simples. Desde 1998 existe otra definición para el campo ToS, conocida como "*Differentiated Services Field*" o "DS Field" [2]. Esta nueva definición es compatible con la versión 6 de IP, descrita en el siguiente apartado.

2.2.2. QoS signaling con IPv6

La versión 6 del protocolo IP considera la capacidad de *QoS signaling* en los paquetes mediante el campo DS (*Differentiated Services*) [2], como muestra la **Figura 3**. Dentro del campo DS, los 6 bits DSCP (*Differentiated Services Code-Point*) indican que tratamiento que debe recibir este paquete en los routers. Los dos bits del campo ECN (*Explicit Congestion Notification*) se pueden utilizar para control de congestión [3].

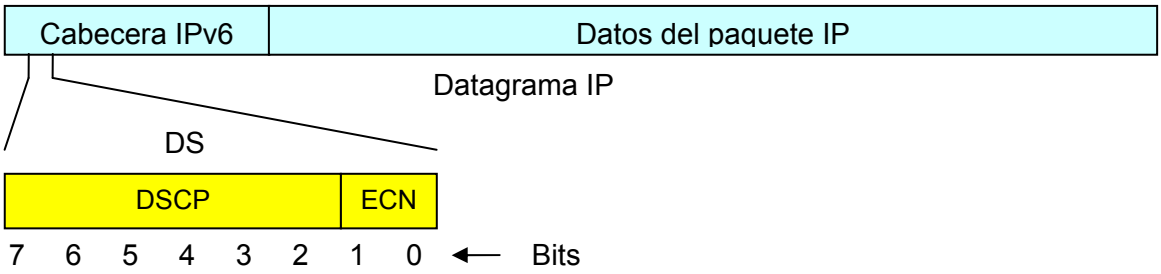

Figura 3. QoS Signaling en IPv6 según RFC 2474.

La siguiente tabla resume las diferentes categorías que permite el campo DSCP. Para mantener la compatibilidad, los tres bits de mayor peso del campo DSCP de IPv6, se pueden hacer corresponder con los tres bits de precedencia del campo TOS de IPv4.

Categorías (Bin)	Categorías (Dec)	Precedencia equivalente	Significado
000 xxx	0 – 7	0	Best Effort (defecto = 000 000)
001 yy0	10 – 14	1	Assured Forwarding (AF) clase 1
010 yy0	18 – 22	2	Assured Forwarding (AF) clase 2
011 yy0	26 – 30	3	Assured Forwarding (AF) clase 3
100 yy0	34 – 38	4	Assured Forwarding (AF) clase 4
101 xxx	40 – 47	5	Expedited Forwarding (EF)
110 xxx	48 – 55	6	Control de la red
111 xxx	56 – 63	7	Control de la red

Los valores de DSCP que se aplican a datos de usuarios se dividen en tres grupos:

- Expedited Forwarding (EF) o Premium. Ofrece todas las garantías para la transmisión de datos, como si se dispusiera de una línea dedicada: caudal mínimo, retardo y variación de retardo acotados, y tasa de pérdidas máxima [3].
- Assured Forwarding (AF). Aunque ofrece un trato preferente en la transmisión de datos, no ofrece garantías [4]. Se definen cuatro clases, 1 a 4, siendo la clase 4 la de mayor prioridad. Además, para cada clase hay tres opciones de descarte: baja (yy=01), media (yy=10) y alta (yy=11). A mayor opción de descarte, menor prioridad.
- Best Effort. Simplemente se reenvían los paquetes, y la calidad está en función del estado de la red. Se dispone de 8 prioridades en función de los bits "*x*", donde el valor por defecto es 0.

Dentro de la categoría AF, se suelen nombrar las posibles opciones como "AFcd", siendo c la clase de 1 a 4, y d la opción de descarte de 1 a 3. Por ejemplo, el valor 22 de DSSP (en binario 010 110) corresponde con la categoría AF clase 2 (010) con opción de descarte 3 (11) o alta, lo que se referencia como AF23.

2.2.3. QoS signaling y los túneles

Uno de los inconvenientes que puede presentar la aplicación de un técnica de túnel es que el contenido del protocolo pasajero puede viajar a través de diferentes routers sin que se le apliquen las medidas establecidas de gestión de la calidad de servicio, puesto que el protocolo pasajero se transporta como datos, y las medidas de gestión se aplican al protocolo portador.

La forma habitual de evitar esto es copiar toda o parte de la información sobre QoS que tiene el protocolo pasajero al protocolo portador, cuando se realiza el proceso de encapsulación. Así, los routers de la red aplicarán las medidas de gestión de calidad de servicio al protocolo portador, con los mismos criterios que si se aplicasen al pasajero. Un ejemplo de esto es la posibilidad de configurar la "herencia" del campo de precedencia de un paquete IP pasajero en el paquete IP portador de un túnel de nivel 3, cuándo se realiza el proceso de encapsulación.

2.3. Gestión de la calidad de servicio en un router

2.3.1. Procesamiento del tráfico

Para gestionar el tráfico de una red y abordar el control de la congestión, los routers utilizan estrategias de clasificación de tráfico, asignación de diferentes prioridades a los paquetes y mecanismos de colas para almacenamiento temporal de los paquetes. La **Figura 4** esquematiza la gestión de tráfico que puede hacer un router.

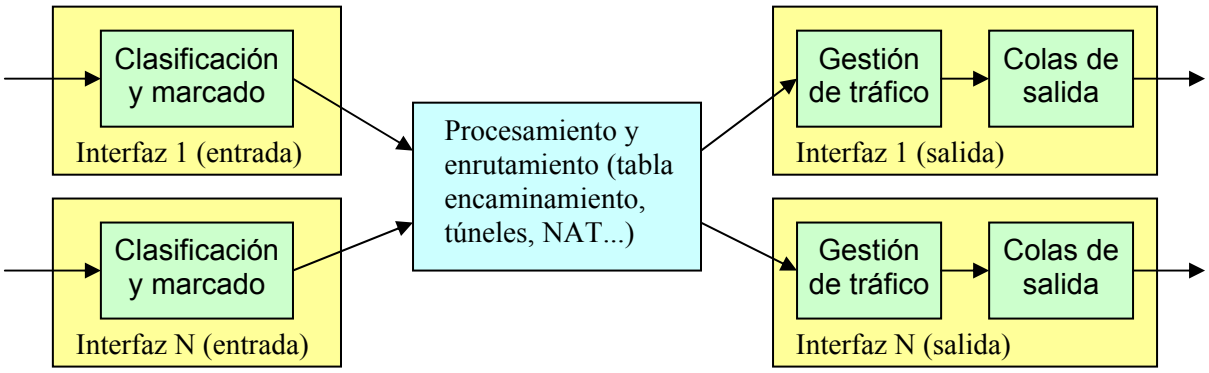

Figura 4. Etapas de proceso de paquetes en un router.

En primer lugar, los paquetes que llegan al equipo por los interfaces se pueden clasificar y marcar, asignando prioridades a distintos tipos de tráfico. Después los paquetes se encaminan, según las técnicas estudiadas en las dos prácticas anteriores. Y finalmente, antes de enviar los paquetes por la interfaz correspondiente, pueden ser procesados mediante esquemas de gestión de tráfico y almacenados temporalmente en las colas de salida. Estas dos últimas funciones se realizan en función de las clasificaciones previas de los paquetes y de los tipos de tráfico.

En la etapa de clasificación y marcado, el router explora los paquetes y los clasifica según algún criterio. La clasificación se puede hacer atendiendo a diferentes aspectos: protocolos (IP, IPX, AppleTalk...), servicios de aplicación (HTTP, FTP, mail...), tamaños de paquetes, interfaz de entrada, direcciones (de *host*, de red...), velocidades medias, valores de QoS *signaling* (como el ToS de IP), etc. Incluso, algunos routers, permiten que la clasificación se realice también en función de los usuarios que originan los paquetes, previa autentificación de los usuarios, a través de sistemas como RADIUS. Los paquetes clasificados pueden ser marcados estableciendo determinados valores para los campos de QoS *signaling* de los protocolos [3].

A la salida de una interfaz, la estrategia de colas de salida puede ser desde una simple cola FIFO (*First In*, *First Out*) hasta una con gestión de múltiples colas de prioridades diferentes. Dependiendo de reglas específicas, o mejor, de la clasificación asociada al tipo de tráfico al que pertenece un paquete (según QoS *signaling*), el paquete puede ser tratado de

diferente modo: se coloca en una cola específica, se elimina o se pasa a la cola de salida directamente. En los siguientes apartados se abordan con más detalle estas estrategias.

2.3.2. Colas de salida

La opción más sencilla, la **FIFO** (*First In First Out*) está basada en encolar los paquetes que llegan a una interfaz de salida cuando su red está congestionada manteniendo el orden de llegada de los paquetes, para enviarlos en ese mismo orden cuando la red esté disponible. Es la estrategia más simple y suele ser la estrategia configurada por defecto. Sin embargo tiene una desventaja importante: no tiene en cuenta la prioridad de los paquetes de datos, y todos los paquetes se tratan por igual. Pero las redes actuales demandan estrategias más "inteligentes".

Así, es mas común emplear estrategias de múltiples colas, como la esquematizada en la **Figura 5**, que encolan los paquetes en función de algún criterio de clasificación, o de un valor de QoS *signaling* establecido anteriormente en el mismo, como el mostrado en la siguiente figura. Luego, un planificador extrae los paquetes de las colas para enviarlos, atendiendo a las prioridades de las mismas, y tratando de asegurar un ancho de banda para cada tipo de tráfico. Es decir, se extrae más paquetes conforme la cola tiene más prioridad, pero sin dejar de atender las de prioridad inferior.

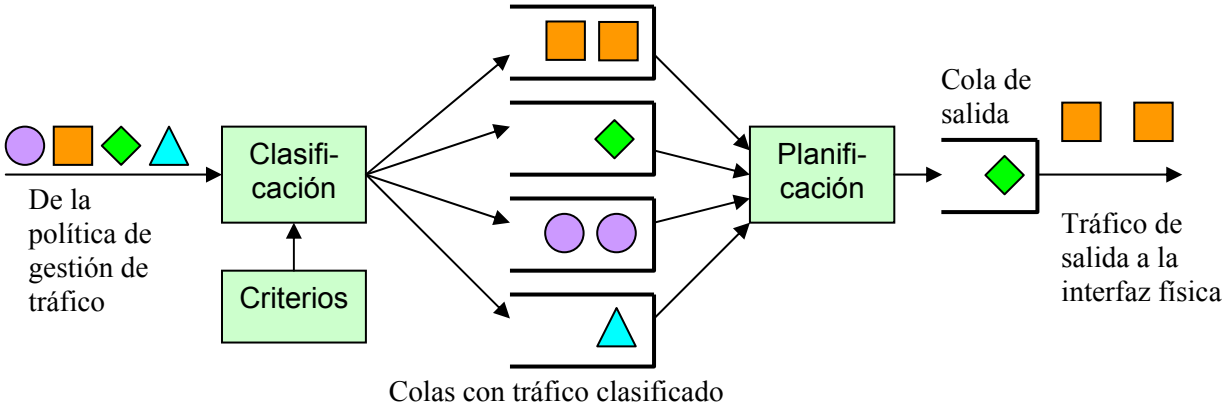

Figura 5. Planificador de paquetes en una interfaz de salida de un router.

Dependiendo del fabricante y del modelo de un router, este puede ofrecer distintas alternativas de técnicas de múltiples colas de salida. Una de las técnicas más importantes del IOS de Cisco Systems es **WFQ** (*Weighted Fair Queuing*: encolado equitativo ponderado) [6]. WFQ emplea un algoritmo de encolado que realiza dos tareas simultáneamente. Los paquetes del tráfico interactivo y que requiere poco ancho de banda (aplicaciones interactivas como Telnet o SSH, o basadas en transacciones como el acceso a bases de datos) reciben un trato preferencial y se colocan al principio de la cola para reducir los tiempos de respuesta. Mientras, el resto de ancho de banda se reparte entre los flujos no interactivos que requieren alto ancho de banda (como por ejemplo FTP), de forma proporcional a los pesos que se asignan a esos flujos. De esta forma se consigue que las largas cadenas de paquetes que puede producir un flujo tráfico constante no afecten a los paquetes esporádicos del tráfico interactivo.

Para determinar el tipo de tráfico, WFQ utiliza automáticamente valores como las direcciones de red (IP) o de enlace (MAC), protocolos, puertos, identificadores de circuito virtuales, y, por supuesto, valores de QoS Signaling como el campo ToS de IP. El funcionamientote WFQ es automático, y, básicamente, la única configuración que debe hacer el administrador es el número de colas utilizadas (por defecto 256 en IOS). Así, el principal

inconveniente de WFQ es que no permite un control preciso sobre el reparto de ancho de banda, en contraste con otras técnicas como es PQ (*Priority Queuing*) o CQ (*Custom Queueing* o encolado a medida).

Por ejemplo, PQ (Priority Queuing) es una alternativa sencilla que asegura que el tráfico importante se maneja más rápidamente que el resto de paquetes, conforme a una definición estricta de prioridades [6]. Como muestra la **Figura 6**, esta técnica utiliza cuatro colas para cuatro tipos de prioridad: alta, media, normal y baja. La cola de prioridad normal se usa para los paquetes no clasificados. Al planificador escogerá paquetes de la cola de prioridad más alta hasta que esta se vacía; entonces pasará a dar salida a los paquetes de la cola de prioridad media. Cuando se vacía la cola de prioridad media, se atienden los de la de prioridad normal, y finalmente los de baja prioridad. Esto es, hasta que una cola de más alta prioridad no se vacía, no se atienden las otras colas . La asociación de los paquetes a cada cola la puede hacer el administrador conforme al interfaz de entrada, al tamaño, o según una lista de acceso.

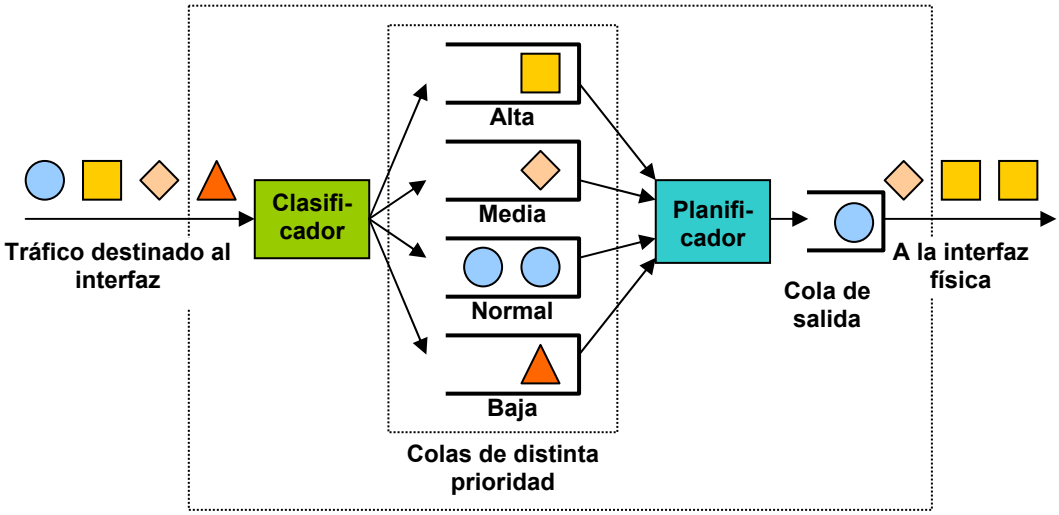

Figura 6. Planificador PQ.

La principal aportación de **CQ** en que permite al administrador especificar el número de bytes que se deben enviar de cada cola en cada servicio del planificador, asi como el número máximo de bytes que caben en cada cola, con lo que se puede distribuir con detalle el ancho de banda de un interfaz entre los tráficos de distintas aplicaciones [6]. Los problemas principales de las técnicas PQ y CQ son que se configuran estáticamente y no se adaptan a cambios en la red, y que consumen más tiempo de proceso que estrategias FIFO. Por ello no son muy adecuadas para interfaces LAN rápidos, y funcionan mejor en interfaces serie o WAN con un ancho de banda moderado.

Existen otras alternativas más sofisticadas que combinan características de las anteriores. Por ejemplo CBWFQ (*Class-Based Weighted Fair Queueing*: WFQ basada en clases) es una extensión más flexible de WFQ, que proporciona soporte para clases de tráfico definidas por el usuario conforme a protocolos, listas de acceso, o interfaces de entrada. Otra opción es LLQ (*Low Latency Queuing*: encolado de baja latencia), que aplica el concepto de prioridades estrictas a CBWFQ para lograr un procesamiento más rápido.

Finalmente, cabe tener en cuenta estos otros aspectos: sólo se puede especificar una estrategia de colas por *interface*, y en interfaces especiales (como túneles) no se pueden aplicar técnicas avanzadas como WFQ. También existen alternativas de configuración especiales para interfaces Frame Relay o protocolos como RTP.

2.3.3. Gestión de tráfico

Con las estrategias de colas de salida se pretende abordar el problema de la congestión en la redes de salida cuando ya existe. Pero, además, se requieren técnicas para evitar la congestión, esto es, técnicas que monitorizan el tráfico de la red para anticiparse a la congestión y evitarla. Y, habitualmente, la congestión se evita eliminando paquetes. La técnica más sencilla en este caso es la eliminación de paquetes de forma aleatoria a partir del momento en que se detecte que el tráfico aumenta por encima de una cota preestablecida, pero tiene el inconveniente de que no distingue diferentes tipos de tráfico. Se emplea más otras técnicas más sofisticadas como las de tipo RED (*Random Early Detection*: detección temprana aleatoria) o WRED (*Weighted* RED), capaces de actuar según la prioridad de los paquetes (precedencia de los paquetes IP), o incluso diferenciar entre los paquetes de distintas conexiones de TCP [7].

Otra técnica sencilla pero eficaz es la conocida como "*shaping*" o perfilado de tráfico, representada en la **Figura 7**. Esta se basa en clasificar primero los paquetes atendiendo a un criterio de los mencionados anteriormente, y después encolar los paquetes de cada tipo de tráfico clasificado en las colas, conocidas en este caso como "*leaky buckets*" (literalmente, "cubos que hacen agua") [6]. De esas colas se van extrayendo paquetes, normalmente a una tasa de bits inferior a la que puede ofrecer el ancho de banda del interfaz. El tráfico que no cumple con los criterios no se somete a ese proceso de clasificación y se envía directamente a la última cola de salida de la interfaz.

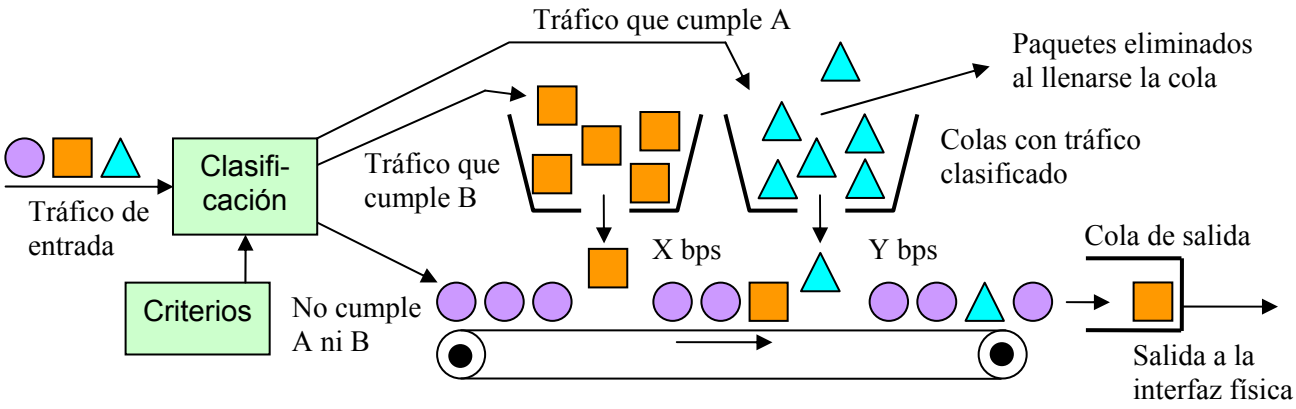

Figura 7. Esquema de perfilado de tráfico o "traffic shaping".

Dado el funcionamiento de "*shaping*", cuyo efecto está reflejado en la **Figura 8**a, esta técnica permite además limitar los anchos de banda disponibles a diferentes tipos de tráfico sobre un mismo interfaz. De este modo, se puede, por ejemplo, limitar el ancho de banda del tráfico de acceso a páginas Web con HTTP a un porcentaje del ancho de banda de una red.

En comparación con "*shaping*", otra estrategia conocida como "*policing*", no usa "cubos" o colas clasificadas para almacenar paquetes, y la limitación de ancho de banda se logra eliminando paquetes directamente. En este caso no se necesitan colas (o "cubos") adicionales, y el efecto provocado a un flujo de paquetes es similar las mostrado en la **Figura 8**b. En la **Figura 8** se puede observar cómo mientras que "*shaping*" suaviza la curva de tráfico para mantener la tasa de bits por debajo de los umbrales establecidos, "*policing*" recorta directamente los picos de tráfico superiores a los umbrales establecidos.

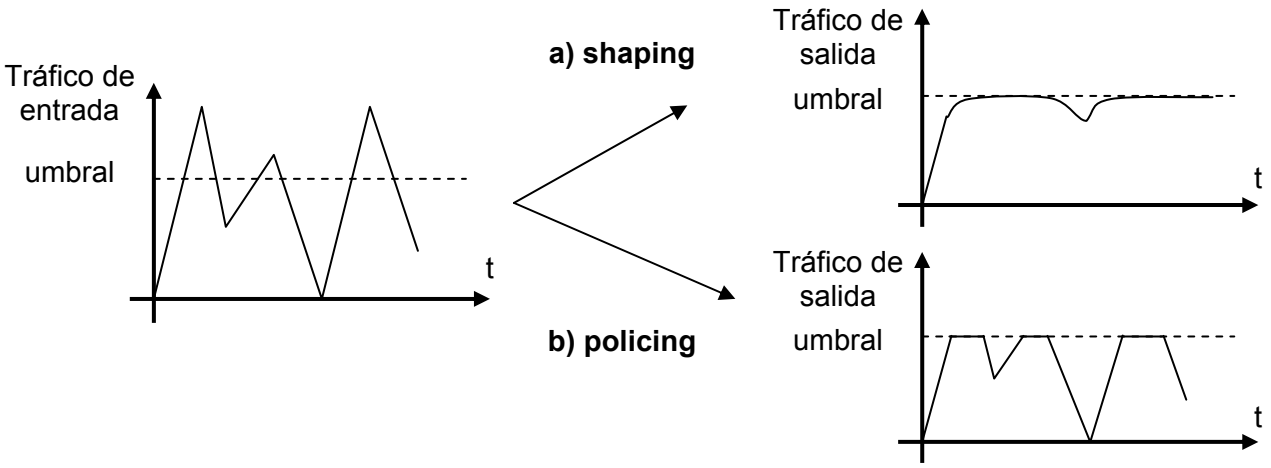

Figura 8. Comparación del efecto de las estrategias *shaping* y *policing*.

La siguiente tabla muestra las principales diferencias entre las dos alternativas, lo que pude ayudar a elegir la más adecuada para cada aplicación:

Criterio	Shaping	Policing
Objetivo	Almacenar temporalmente los paquetes que superan las velocidades establecidas.	Eliminar los paquetes que superan las velocidades establecidas.
Refresco	Las tasas de velocidad de los paquetes se evalúan en intervalos. Se configura en bits por segundo.	Funcionamiento continúo. Se configura en bytes.
Colas soportadas	CQ, PQ, FCFS, WFQ.	No se usan.
Efecto sobre las ráfagas	Suaviza los cambios de tráfico tras varios intervalos.	No se alteran las ráfagas de tráfico.
Ventajas	Si no hay exceso de tráfico, no elimina paquetes, y no se requiere retransmitir.	Evita los retardos de los paquetes en las colas.
Desventajas	Puede introducir retardos en los paquetes, sobre todo con colas grandes.	Al eliminar muchos paquetes, TCP ajusta su ventana a valores más pequeños, y esto disminuye el rendimiento.

Es importante tener en cuenta que el efecto de la eliminación de paquetes no es controlado por protocolos como IP-UDP, que no disponen de control de flujo, y no son capaces de reenviar los paquetes descartados. Así, en caso de una aplicación use estos protocolos y los routers decidan eliminar su tráfico, serán los protocolos de la misma aplicación los responsables de recuperar los datos perdidos. Pero con un protocolo como IP-TCP el efecto es muy diferente. TCP tiene un control de flujo avanzado de ventana deslizante con reenvío de los paquetes perdidos, y en el caso de que se descarten paquetes de una conexión suya, TCP los reenviará. Además TCP emplea algoritmos como el de Naggle, que le permiten adaptar sus conexiones al ancho de banda disponible, ajustando el tamaño de sus paquetes (MSS), o la cantidad de datos que se pueden enviar hasta recibir una confirmación (ventana). Así, las aplicaciones que usan TCP, no perciben pérdida de datos, y sólo perciben que el acceso a la red se realiza con mayor o menor velocidad.

Por ejemplo, el protocolo de aplicación FTP (*File Transfer Protocol*) trabaja sobre TCP, por lo que si se aplica la técnica de "*shaping*" que elimina o retrasa paquetes en la vuelta, TCP los recupera, y adapta el número de confirmaciones a la velocidad. Así, una aplicación de FTP no nota pérdida de paquetes, pero si el retardo que introduce el "*shaping*". Por este motivo, FTP es una buena aplicación para evaluar el efecto de "*shaping*".

2.3.4. CIR

El control de la calidad de servicio está muy relacionado con el uso de redes que trabajan con anchos de banda garantizados, como es el caso de enlaces Frame Relay. En casos como este, se define la una tasa de transferencia comprometida o garantizada denominada CIR (*Commited Information Rate*), que representa un velocidad de transmisión media (bps). El *CIR* se calcula como la relación entre la cantidad de información (bits) garantizada por la red para un flujo de datos, llamada *Bc* (*Committed Burst*), y el intervalo de tiempo de evaluación (segundos) utilizado en las medidas, denominado *Tc* (*Commited Time*):

$$CIR = \frac{Bc}{Tc}$$

Además se puede considerar otro parámetro adicional: el tamaño de ráfaga de exceso o *Be* (Excess Burst size) en que puede sobrepasarse *Bc*. En contraste con *Bc*, que es una cantidad de bits que la red garantiza llevar al destino, *Be* representa una cantidad de bits no garantizada, que solo será transmitida por la red sí esta no está congestionada. Así se dispone de un ancho de banda garantizado, dado por el CIR, y de un ancho de banda máximo, dado por *(Bc + Be) / Tc*. Los bloques de datos que contienen bits por encima de *Bc* serán marcados como posibles para ser eliminados si la red empieza sufrir congestión. Así, por ejemplo, en Frame Relay, se pondría a 1 el bit DE de las tramas. Si en un interfaz de red se configura *Be*=0, ese interfaz no enviará más bits de los garantizados, y tasa media de envío se mantendrá igual o menor al *CIR*.

Las estrategias de gestión de tráfico de "*shaping*" y "*policing*" aplican el concepto de *CIR* para evaluar la cantidad de tráfico de paquetes asociada a un flujo de datos y decidir si hay que retrasar (en el caso de "*shaping*"), o descartar (en el caso de "*policing*") paquetes.

2.4. Gestión de la calidad de servicio en los routers Cisco del laboratorio

Cada casa comercial de equipos de interconexión de redes, entre los que están los routers, utiliza en sus equipos diferentes sistemas operativos propietarios, con muchas particularidades de configuración y funcionamiento. Estos sistemas operativos ofrecen habitualmente una interfaz de líneas de comandos de texto, a la que se puede acceder a través de servicios TCP/IP estándar como Telnet o RSH, o a través de un interfaz serie tipo RS-232 o interfaz "de consola". Los equipos más recientes permiten configurara además los parámetros más sencillo a través de interfaces gráficas o Web, si bien para configuraciones más avanzadas sigue siendo necesario acceder al sistema mediante la interfaz de línea de comandos.

Como es sabido, en la red del laboratorio utilizada para las prácticas se dispone de tres routers de la marca Cisco Systems, modelos 2513, 1601 y 1720, con los cuales se va ha realizar una gestión básica de calidad de servicio.

La marca Cisco Systems utiliza su propio sistema operativo, el Cisco IOS [6]. Así, para experimentar con la gestión de calidad de servicio en el laboratorio es conveniente tener unas nociones muy básicas sobre la configuración de un router Cisco. Cabe destacar que IOS ofrece un mundo de posibilidades de configuración de las técnicas QoS, incluyendo "*shaping*" y "*policing*" [6]. Existen opciones específicas para una determina técnica, como es el caso de los conjuntos de comandos GTS (*Generic Traffic Shaping*) y FRTS (*Frame Relay Traffic Shaping*) para "*shaping*", y CAR (*Commited Access Rate*) para "*policing*". Además hay un conjunto de comandos genérico conocido como MQC (*Modular QoS command-line*). En esta práctica se analizarán configuraciones básicas de GTS y CAR. En los siguientes puntos se

muestran algunos comandos de configuración, a la vez que se explica cómo se realiza una sencilla gestión de calidad de servicio en un router de esa marca.

2.4.1. Gestión del CIR

Para implementar prácticamente un control de *CIR* en los routers, Cisco define el concepto de "*token bucket*" (cubo de testigo), según el cual un router no opera directamente con bits de datos, sino con unos testigos asociados a los flujos de datos [6]. De esta forma, el mecanismo de gestión de tráfico, que implementa una estrategia de "*shaping*" o "*policing*", no prioriza o descarta paquetes de datos sino que simplemente descarta testigos, lo cual resulta más eficiente.

Los testigos son generados y añadidos en el cubo cada cierto intervalo de tiempo. El cubo tiene además un tamaño máximo, y si éste se llena, los nuevos testigos que se generan son descartados. Cada testigo representa un permiso para que un origen pueda enviar un cierto número de bits. Cuando la gestión de tráfico decide transmitir un paquete de datos, debe eliminar del cubo un número de testigos acorde al tamaño del paquete. Si no quedan más testigos en el cubo, el paquete debe esperar en una cola de paquetes hasta que se generen más testigos (*shaping*) o debe ser descartado (*policing*).

El intervalo de tiempo en que se genera cada testigo depende de si la gestión de tráfico es de tipo "*shaping*" o "*policing*". En el caso de "*shaping*", se toma como duración del intervalo el valor *Tc=Bc/CIR*, y cada intervalo se añade un número de testigos equivalente a *Bc*. Como interesa que *Tc* no sea demasiado grande, un router limita el cálculo a un resultado máximo. Si el valor calculado para *Tc* supera ese límite, se escoge un valor predefinido más pequeño. En el cubo cabrán testigos para *Bc+Be* bits (*Be* puede ser 0), y el resto de testigos generados se descartan.

En contraste, cuando la gestión de tráfico usa "*policing*", no se establece un intervalo fijo de tiempo para generar testigos, y lo que se hace es añadir testigos al cubo en función del *CIR* y del tiempo entre paquetes de datos del mismo flujo según esta fórmula:

$$N = [(T2-T1) \cdot CIR] / 8$$

Así, cuando se procesa un nuevo paquete en el instante *T2*, se calcula la diferencia de tiempo con el instante *T1* de anterior paquete, que al multiplicarla por el *CIR* da un número de bytes *N* correspondiente a *Bc*. Así, se generan los testigos equivalentes a *N*. De este modo, los comandos de "*policing*" trabajan con ráfagas de bytes en vez de bits.

2.4.2. Listas de acceso

Una lista de acceso (o **ACL**: *Access List*) es una forma de definir criterios genéricos, que se pueden aplicar a multitud de comandos del router, como los de gestión de QoS, enrutamiento de nivel de red, NAT, conmutación de nivel de enlace, gestión de usuarios... Las ACLs son actualmente la piedra angular de muchos sistemas operativos de red, tales como el IOS de Cisco. Las ACLs pueden ser estáticas o dinámicas, para definir criterios que siempre permanecen igual, o que pueden modificarse con el tiempo.

Una ACL es una colección secuencial de condiciones "permite" (*permit*) y "deniega" (*deny*) que se aplican a paquetes de datos para decidir si deben ser procesados o bloqueados. Los paquetes sobre los que trabaja una ACL dependen del comando de IOS donde se utiliza la ACL. Por ejemplo, si la ACL se utiliza en la definición de características de la entrada de una interfaz de red, entonces se permite o se bloquean los paquetes que entran por esa interfaz, pero si la ACL se utiliza en la definición de una política QoS (*Quality of Service*),

entonces la ACL especifica a que paquetes se debe aplicar una restricción de velocidad y a cuáles no.

Cada ACL se identifica con un número, y las distintas condiciones de la ACL se definen como diferentes líneas en las que se indica ese número tras el comando "acess-list". Cuando una ACL debe evaluar un paquete de datos, se compara los campos existentes en dicho paquete con los atributos definidos en cada condición de la ACL, de forma secuencial. Si una condición se define con la sentencia "*permit*", y los campos del paquete de datos cumplen la condición, la ACL acabará y devolverá un valor "verdadero" al comando que la llamó. Sin embargo, si una condición se define con la sentencia "*deny*", y los campos del paquete de datos cumplen la condición, la ACL acabará y devolverá un valor "falso" al comando que la llamó. Además, siempre existe una condición "*deny any any"* implícito al final de cualquier ACL, de modo que los paquetes de datos que no cumplan ninguna de las condiciones de la ACL se descartan automáticamente. Es por tanto crítico el orden en que se aplican las líneas de la ACL, y merece especial atención en su diseño.

Por ejemplo, la ACL estática número 101 se podría definir con estos comandos:

```
Router(config)# access-list 101 remark Criterios para marcar precedencia 1
Router(config)# access-list 101 permit ip host 193.145.232.131 host 10.1.3.3
Router(config)# access-list 101 deny udp any 10.1.0.0 0.0.255.255 eq 80
Router(config)# access-list 101 permit ip host 193.145.232.132 host 10.1.2.2
```

La primera línea (*remark*) establece una descripción para la lista. La segunda línea define la primera condición; se devuelve "verdadero" para los paquetes IP que vienen desde el *host* 193.145.232.131 y van al 10.1.3.3. La tercera línea define una segunda condición: la lista devuelve "falso" para los paquetes UDP que vienen desde cualquier equipo (*any*) y van dirigidos a una dirección que empieza por "10.1." y al puerto 80. Con el lenguaje de IOS, en las listas de acceso no se especifican máscaras de red, como sería 255.255.0.0, sino un patrón como 0.0.255.255 que corresponde a la máscara de red invertida. La cuarta línea define otra condición más: devolver "verdadero" para los paquetes IP que van desde el *host* 193.145.232.132 al 10.1.2.2. Si no se cumple alguna de las tres condiciones, la lista devolverá "falso".

En general, las listas de acceso permiten establecer las condiciones no sólo por direcciones IP, sino también por puertos, protocolos, determinados bits de las cabeceras, tamaño de paquetes, valores de valores de QoS…, incluyendo también campos de otros protocolos diferentes al nivel de red.

Hay que considerar que los números utilizados para identificar las ACLs definen su ámbito de actuación. Las listas más utilizadas son las de tipo "IP estándar" (rangos 1-99 y 1300-1999) e "IP extendida" (rangos 100-199 y 2000-2699).

En un router con IOS, se puede comprobar la configuración de ACLs ejecutando el comando "*show access-lists*", que devolverá un resultado como el siguiente, donde el valor "*matches*" indica el número de paquetes que han cumplido alguna condición de la lista:

```
Router# show access-lists
Extended IP access list 101 (201 matches)
   remark Lista con criterios para marcar con precedencia 1
   permit ip host 193.145.232.131 host 10.1.3.3
   permit ip host 193.145.232.131 host 10.1.3.3
   deny udp any 10.1.0.0 0.0.255.255 eq 80
   permit ip host 193.145.232.132 host 10.1.2.2
```

2.4.3. Listas de acceso dinámicas

En contraste con las ACL estáticas, en una ACL dinámica se pueden agregar o quitar condiciones durante el funcionamiento normal del router. Esto se pude hacer incluso de forma automática desde otros equipos mediante acceso remoto al router, por ejemplo con la aplicación "*nc*" (netcat) para sistemas Linux/Unix, o el comando "*stdprac*" usado en las prácticas de STD.

Como ejemplo de aplicación puede considerarse el caso de que la dirección IP destino a la que se aplican las condiciones no fuera siempre la misma. Para ello habría que definir primero un patrón de lista de acceso dinámica. Con el siguiente comando se crea un patrón de ACL dinámica denominado "pre1", que en principio es valido para paquetes IP con cualquier par de direcciones:

```
Router(config)# access-list 102 dynamic pre1 permit ip any any
```

Después se puede incluir una condición dinámicamente en la lista con un comando como el siguiente, que en este caso permite los paquetes que van desde cualquier equipo ("*any*") hacia el *host* 10.1.3.3.

```
Router# access-template 102 pre1 permit ip any host 10.1.3.3 timeout 10
```

Además, se especifica que dicha condición deja de ser valida si no se usa durante 10 minutos seguidos. Para ello el router inicia un contador de tiempo a 10 minutos que va decreciendo mientras no se procesen paquetes que encajen en la condición. Si el router procesa un paquete que encaje en la condición, entonces se vuelve a iniciar la cuenta del temporizador.

La configuración de una ACL dinámica aparece de este modo al ejecutar el comando "*show access-lists*":

```
Router# show access-lists
Extended IP access list 102
    Dynamic pre1 permit ip any any
       permit ip any host 10.1.3.3 (73 matches) (time left 56)
```

El "*time left*" indica los segundos que le quedan de vida a la entrada dinámica, a no ser que se procese un paquete que encaje en ese criterio en ese tiempo, caso en el que se inicia de nuevo la cuenta de segundos al valor de "*timeout*" especificado al crear el criterio.

Se puede eliminar una condición de una lista dinámica usando el comando "*clear access-template*". Sin embargo en algunas versiones de IOS esto puede causar que el router se bloquee si se elimina la condición mientras el router está procesando tráfico. Entonces es mejor esperar a que la condición se borre sola al acabar su *timeout*.

```
Router# clear access-template 102 pre1 permit ip any host 10.1.3.3
```

2.4.4. Clasificación de tráfico y marcado de paquetes

Se puede definir de forma sencilla una clasificación del tráfico mediante el comando "*route-map*". De forma general, este comando permite especificar acciones a realizar con los paquetes que deben ser reenviados por el router, previamente a su encaminamiento. El siguiente ejemplo define un marcado de los paquetes IP mediante el establecimiento del valor de precedencia de los mismos a "*priority*" (valor 1), si los paquetes cumplen con el criterio definido en la lista de acceso 101. Esta lista podría ser la definida en el apartado anterior.

```
Router(config)# route-map CLASIF1 permit 10
Router(config-route-map)# match ip address 101
Router(config-route-map)# set ip precedence priority
```

A la clasificación se la denomina con el nombre "CLASIF1". El valor 10 tras la palabra clave "*permit*" indica el orden esta condición con respecto a otras condiciones definidas con "*route-map*" para el mismo nombre. Dentro de la configuración de un interfaz, se puede aplicar la clasificación "CLASF1" al tráfico de entrada de este modo:

```
Router(config)# interface fastethernet 0
Router(config-if)# ip policy route-map CLASIF1
```

También se puede comprobar la política "*route map*" establecida antes, así como los paquetes y bytes procesados según las listas de acceso indicadas, usando el comando "*show route-map*" de IOS, que devuelve lo siguiente:

```
Router# show route-map
route-map CLASIF1, permit, sequence 10
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    ip precedence priority
  Policy routing matches: 4 packets, 230 bytes
```

2.4.5. Gestión de tráfico con GTS (Generic Traffic Shaping)

Para aplicar GTS se utiliza el comando "*traffic-shaping*" directamente dentro de la configuración de un interfaz. Con este comando se logra que los paquetes deseados se reenvíen a una tasa de bits limitada. Esta limitación puede implicar que se eliminen paquetes si se llena el "cubo" de "*traffic-shaping*".

Por ejemplo, para establecer una tasa de velocidad media (CIR) de 50Kbps para todos los paquetes que salen por una interfaz, se debe usar este comando dentro de la interfaz:

```
Router(config)# interface fastethernet0
Router(config-if)# traffic-shape 50000 8000 8000
```

Los dos valores 8000 del comando definen los tamaños de ráfaga media (Bc) y máxima (Bc) de bits (en este caso la misma cantidad) que el tipo de tráfico de la lista 103 puede enviar en un intervalo de tiempo. El router evaluará en cada intervalo (Tc) el tráfico enviado por la interfaz, para comprobar si se transmite a un CIR de 50.000bps. En este caso, el router determinará el valor Tc es 160ms (8.000bits/160ms=50Kbps). Realmente sólo es imprescindible especificar la velocidad media deseada, y se puede dejar al sistema que calcule los valores de tamaño de ráfagas.

Si la misma política se quiere aplicar solo para los paquetes que cumplen las condiciones de la lista de acceso 103, el comando sería el siguiente:

```
Router(config)# access-list 103 permit tcp host 172.25.1.132 eq 80 any
Router(config)# interface fastethernet0
Router(config-if)# traffic-shape group 103 50000 8000 8000
```

La condición de la lista se verifica para los paquetes del protocolo TCP que proceden desde el equipo con dirección 172.25.1.132 con puerto origen igual (*eq*) a 80, y van dirigidos a cualquier equipo (*any*). El origen 172.25.1.132:80 puede ser un servidor Web, con lo que se estará limitando el tráfico de descarga de ese servidor.

Además, en la condición de la lista de acceso para el perfilado de tráfico de salida también se puede tener en cuenta la precedencia del paquete IP, si antes se había aplicado una clasificación de tráfico. Por ejemplo con esta lista:

```
Router(config)# access-list 103 permit ip host 172.25.1.132
                    any precedence routine
```

La lista se valida para el tráfico IP que va desde la dirección 172.25.1.132 a cualquier otra (*any*), y que está marcado con precedencia *routine* (0). Este valor puede ser el que ya tenía el paquete al llegar el router, o se puede haber establecido en un interfaz de entrada, conforme a lo explicado en el apartado anterior. En el ejemplo, los paquetes IP con una precedencia mayor a 0 no cumplirán el criterio de la lista de acceso 103, auque procedan de la dirección 172.25.1.132, y por ese motivo no se aplicará la restricción de 50.000bps a los mismos.

La configuración del perfilado de tráfico se puede comprobar con el comando "*show traffic-shape*", que para el ejemplo anterior devolverá algo así:

```
Router# show traffic-shape
       Access Target    Byte   Sustain   Excess    Interval  Increment Adapt
VC     List   Rate      Limit  bits/int  bits/int  (ms)      (bytes)   Active
-      103    50000     2000   8000      8000      160       1000       -
```

En la tabla, "*Target Rate*" es el CIR, "*Byte Limit*" es Bc+Be expresado en bytes, "*Sustain bits/int*" es Bc, "*Excess bits/int*" es Be, "*Interval (ms)*" es Tc, e "*Increment (bytes)*" representa los testigos aun disponibles en el "cubo" (ver 2.4.1).

Se puede obtener más información sobre el estado de las colas de "*shaping*" con el comando "*show traffic statistics*".

En routers con enlaces serie se puede disponer además de FRTS (*Frame Relay Traffic Shaping*), que es similar a GTS, pero además permite especificar condiciones en función de los bits DE, FECN y BECN de las tramas Frame Relay.

2.4.6. Gestión de tráfico con CAR (Commited Access Rate)

CAR permite especificar una estrategia "*policing*" para tráfico IP directamente sobre un interfaz mediante el comando "*rate-limit*". Por ejemplo, para fijar el CIR de salida del interface Serial0 a 512Kbps, con un tamaño de ráfaga media (Bc) de 56.000 bytes y de ráfaga máxima (Bc+Be) de 64.000 bytes se pueden usar estos comandos:

```
Router(config)# interface serial0
Router(config-if)# rate-limit output 512000 56000 64000
 conform-action transmit exceed-action drop
```

Las clausulas "*conform-action*" y "*exceed-action*" definen que debe hacerse con los paquetes que obedecen el CIR y los que lo exceden. Algunas acciones posibles son:

- *drop*. Se eliminan los paquetes.
- *set-prec-transmit* <*n*>. Cambia la precedencia IP del paquete a n y lo reenvía.
- *transmit*. Se reenvía el paquete.

También es posible definir múltiples "rate-limit" que deben ser aplicados a paquetes clasificados en determinadas clases, lo cual se hace con listas de acceso, como por ejemplo:

```
Router(config)# access-list 102 permit tcp any any eq www
Router(config)# access-list 103 permit tcp any any eq ftp
Router(config)# interface hssi0
Router(config-if)# rate-limit input access-group 102 20000000 24000 32000
 conform-action set-prec-transmit 2 exceed-action drop
Router(config-if)# rate-limit input access-group 103 10000000 24000 32000
 conform-action set-prec-transmit 5 exceed-action drop
```

Finalmente, es posible verificar el estado y las estadísticas de CAR con el comando "*show interfaces rate-limit*":

```
Router# show interfaces rate-limit
  Hssi0 45Mbps to R2
    Output
      matches: access-group 102
        params: 20000000 bps, 24000 limit, 32000 extended limit
        conformed 3 packets, 189 bytes; action: set-prec-transmit 5
        exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
        last packet: 309100ms ago, current burst: 0 bytes
        last cleared 00:08:00 ago, conformed 0 bps, exceeded 0 bps
      matches: access-group 103
        params: 10000000 bps, 24000 limit, 32000 extended limit
        conformed 0 packets, 0 bytes; action: set-prec-transmit 5
        exceeded 0 packets, 0 bytes; action: drop
        last packet: 19522612ms ago, current burst: 0 bytes
        last cleared 00:07:18 ago, conformed 0 bps, exceeded 0 bps
```

2.5. Introducción al análisis de tráfico en redes IEEE 802.11

Las serie de normativas 802.11 del IEEE regula el funcionamiento de equipos y protocolos para LANs inalámbricas. A su vez, Wi-Fi (*Wireless Fidelity*) es una marca de la Wi-Fi Alliance, una organización sin ánimo de lucro creada en 1999 y formada por multitud de fabricantes y otras compañías del sector de las telecomunicaciones, que adopta, prueba y certifica que los equipos cumplen los estándares IEEE 802.11.

Para experimentar con una red IEEE 802.11, en el laboratorio se ha configurado una red inalámbrica abierta, a la se podrán conectar los PC del laboratorio. En esta sección se describen los aspectos básicos a considerar cuando se analizan este tipo de redes.

2.5.1. Estructura de una red inalámbrica

La estructura de una LAN inalámbrica contemplada en norma IEEE 802.11 abarca desde una sencilla red temporal formada por pocos equipos con interfaces inalámbricos estándar (red ad-doc), hasta una red de infraestructura estable que consta de varias celdas de cobertura denominadas BSS (*Basic Service Set*). En la parte izquierda de la **Figura 9** se muestra un ejemplo de red de infraestructura con dos BSS [8].

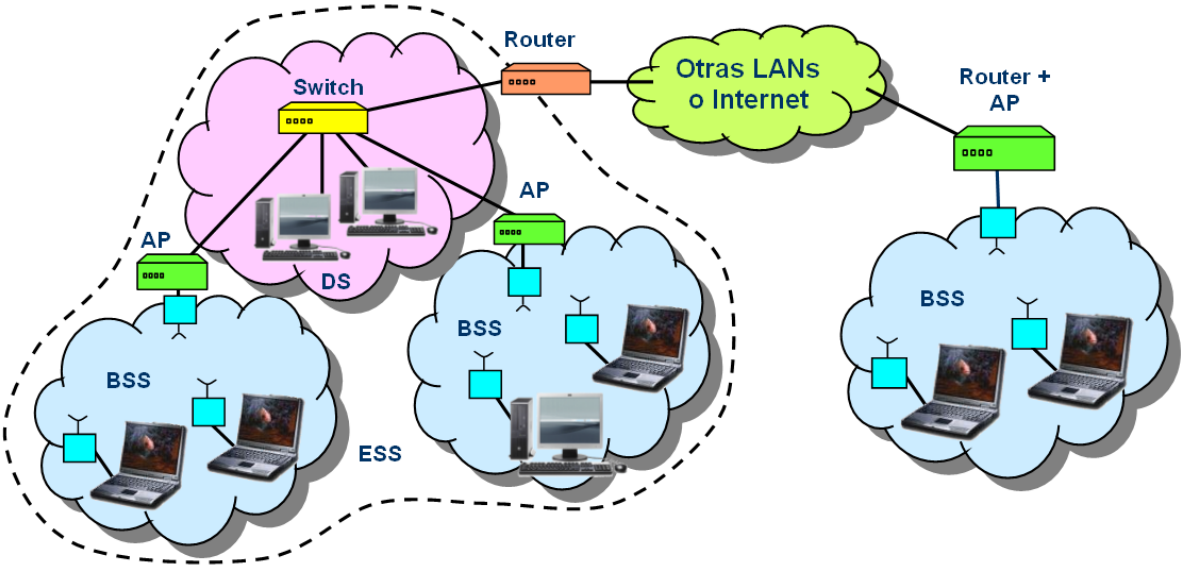

Figura 9. Topología simplificada de una red IEEE 802.11.

La diferencia principal de una red de infraestructura frente a una red ad-doc es que, con la primera, cada BSS dispone de un equipo llamado AP (*Access Point*: punto de acceso) que coordina las transmisiones entre los equipos de ese grupo, y hace de puente entre el BSS y las redes externas. Cuando se dispone de una LAN inalámbrica formada por varios BSS, se necesita una red principal para interconectar los BSS a través de los AP, la cual denomina DS (*Distribution System*). El conjunto recibe el nombre ESS (*Extended Service Set*: conjunto de servicios extendidos).

En esta práctica se trabajará con una red de infraestructura simplificada, que consta de un solo BSS, como el ejemplo mostrado en la parte derecha de la **Figura 9**, siendo esta la implementación habitual para uso doméstico y pequeños entornos de oficinas o laboratorios. En este caso, es común usar un equipo que incorpora las funciones de router además de AP.

Para que los posibles usuarios puedan reconocer una red inalámbrica y diferenciarla de otras, se puede asignar un nombre a cada BSS, o el mismo nombre a todos los BSS de un mismo ESS. Ese nombre es una cadena de hasta 32 caracteres que se denomina SSID (*Service Set Identifier*). Además, cada BSS tiene un identificador numérico único (BSSID), que se corresponde con la dirección MAC del AP del BSS.

2.5.2. TCP/IP sobre redes IEEE 802.11

Hay que tener en cuenta que IP se diseñó para funcionar sobre un enlace punto a punto con el protocolo PPP, o sobre LANs de difusión tipo CSMA/CD como Ethernet con la ayuda de ARP. Pero cuando hay que usar IP sobre otras tecnologías, como pueden ser una LAN IEEE 802.5 (Token Ring) o una LAN inalámbrica IEEE 802.11, se requiere cierta adaptación para enviar los protocolos IP y ARP sobre ellas [8]. IP y ARP necesitan que el nivel de enlace se comporte como Ethernet y aporte, además de las direcciones de enlace origen y destino (direcciones MAC), un campo de tipo que diferencie el protocolo usado (valores hexadecimales 0x806 para ARP y 0x800 para IP).

La solución pasa por encapsular los campos de la trama Ethernet que necesitan IP y ARP dentro de las cabeceras MAC y LLC de otras tecnologías LAN como IEEE 802.5 y 802.11, según muestra la **Figura 10** [9]. Dado que estas LAN emplean LLC (IEEE 802.2), se aprovecha la cabecera de este protocolo para incorporar la información de tipo, mientras que las direcciones MAC origen y destino se copian directamente en los campos correspondientes de la cabecera MAC. Este proceso, conocido como "encapsulación Ethernet", puede ser visto también como un túnel en el que se envía una trama de nivel de enlace Ethernet sobre tramas de nivel de enlace de redes IEEE 802.5 y 802.11.

La encapsulación Ethernet se puede realizar con dos métodos: la vieja norma de Internet RFC 1042 [8] y el estándar moderno IEEE 802.1H [10]. El primer método es específico para IP, y suele ser el empleado por los sistemas Linux. El segundo fue originalmente promovido por Microsoft, y es el que habitualmente usan los equipos con MS. Windows y MacOS, así como muchos puntos de acceso, ya que también puede ser aplicado a los protocolos de red IPX (OSI) y AppleTalk (Apple). En cualquier caso, en una red IEEE 802.11, el método lo fija el AP.

En la práctica, los dos métodos son prácticamente iguales, y básicamente consisten en especificar un código concreto en el campo de "código de organización" del mensaje LLC (valor hexadecimal 0x000000 o 0x0000F8) que avisa sobre la presencia del campo de "tipo Ethernet" al final de la cabecera LLC, antes de los datos del nivel superior, como muestra la **Figura 10**. Además, en los campos de SAP (*Service Point Access*) origen y destino se usa valor 0xAA, y los mensajes LLC son de tipo UI (*Unumbered Information*; código 0x03).

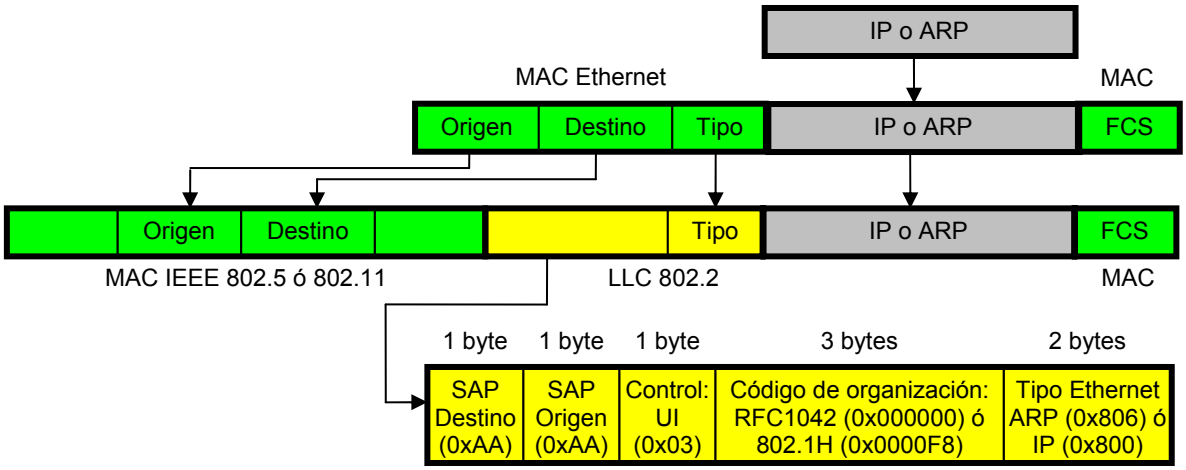

Figura 10. Encapsulación Ethernet: paquetes IP o ARP sobre otras LAN.

La encapsulación Ethernet afecta a aplicaciones que trabajan con protocolos de bajo nivel, como son los monitores de tráfico (por ejemplo tcpdump y Wireshark). Así, es habitual que, cuando se captura de un interfaz inalámbrico IEEE 802.11 en MS. Windows, se vean solamente tramas Ethernet y no toda la información de los protocolos de enlace. Esto es debido a que el controlador de la tarjeta de red que incorpora el S.O. (lo que se conoce como NDIS: *Network Driver Interface Specification*) no da acceso a la cabeceras MAC y LLC reales, sino a la Ethernet que pueden ver los protocolos de nivel de red. Para poder analizar con detalle el tráfico de una red IEEE 802.11 se requiere un hardware y un controlador que permitan acceso a ese tráfico. En el caso de Linux, es más fácil de encontrar controladores que permitan analizar el tráfico real.

2.5.3. Tramas IEEE 802.11

La **Figura 11** muestra el empaquetado completo que se aplica a un datagrama IP o de un mensaje de ARP cuando estos se envían por una red IEEE 802.11 con encapsulación Ethernet.

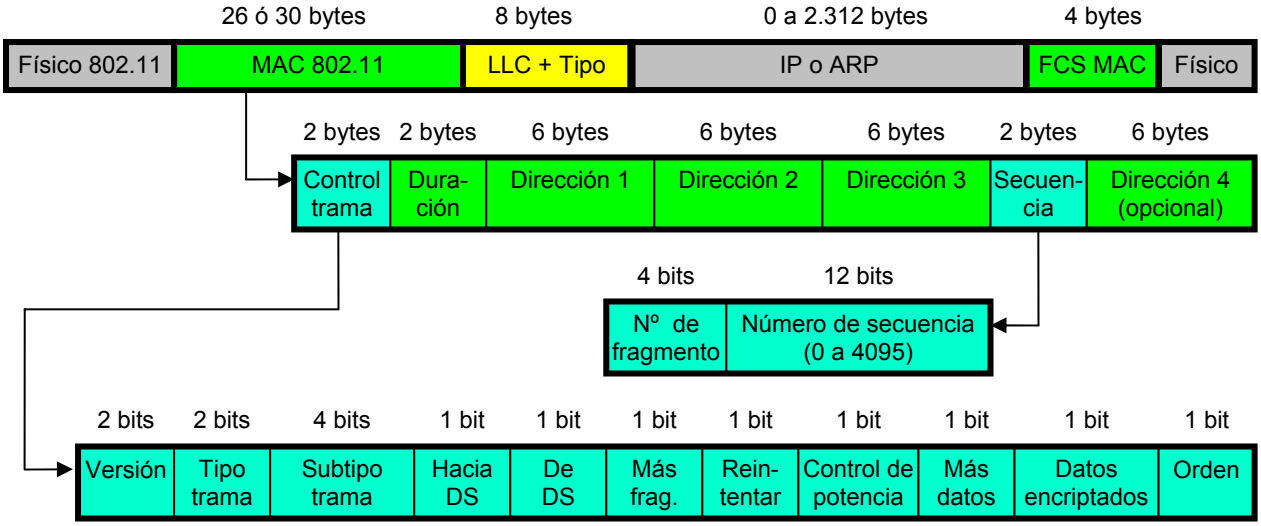

Figura 11. Formato de una trama IEEE 802.11 con un paquete IP o ARP.

Sobre el nivel físico, que depende de la norma específica utilizada (802.11*a*, *b*, *g*, *n*...), se envía una trama de subnivel MAC 802.11, que tiene el mismo formato independientemente de la alternativa de nivel físico utilizada [10]. La trama MAC transporta a su vez el mensaje

del subnivel LLC (ver **Figura 11**), lo cual es necesario siempre en una red 802.11, aunque por encima se estén utilizando protocolos TCP/IP y no protocolos OSI.

Dentro de la cabecera MAC, destaca la presencia de hasta cuatro direcciones. Normalmente las tramas de datos 802.11 emplean sólo tres direcciones, que son las necesarias para transmitir una trama entre estaciones de un mismo BSS, desde una estación al AP, o desde el AP a una estación. El uso de la cuarta dirección es solo necesario en redes 802.11 que se usan como DS inalámbricos (WDS) para otras redes 802.11 finales. Además, hay muchas de control de MAC que emplean sólo las dos primeras direcciones (origen y destino en el BSS), y tampoco incluyen el mensaje LLC. La siguiente tabla refleja el uso de los campos de dirección en las tramas de datos:

Hacia DS	De DS	Dirección 1	Dirección 2	Dirección 3	Dirección 4	Significado
0	0	Destino	Origen	BSSID	*No hay*	Trama entre estaciones de un mismo BSS
0	1	Destino	BSSID (AP origen)	Origen	*No hay*	Trama que va del AP hacia un equipo de un BSS
1	0	BSSID (AP destino)	Origen	Destino	*No hay*	Trama que va desde un equipo de un BSS al AP
1	1	AP destino	AP Origen	Destino	Origen	Trama de un equipo de un BSS a otro equipo de otro BSS pasando por una 802.11 intermedia (WDS)

En la tabla anterior se observa como, además de las direcciones de las estaciones origen y destino, en los tres primeros casos se indica también el BSSID. En redes de infraestructura con AP, el BSSID es la dirección MAC de la interfaz inalámbrica del AP.

El campo de "control de trama" incluye diferentes bits o *flags* que informan de muchos aspectos. Los campos "Tipo de trama" y "subtipo de trama" definen de si trama contiene datos de nivel superior, o es una trama de control MAC. Entre los otros campos, destacan los bits "hacia DS" y "de DS" que ayudan a interpretar el significado de los campos de dirección, el bit "mas fragmentos" que se utiliza de forma similar al bit MF de IP, y el bit "datos encriptados" que informa sobre el uso de un algoritmo de encriptación del contenido de la trama mediante WEP, TKIP u otra técnica.

El campo "duración" de la trama MAC es empleado por el algoritmo de control de acceso al medio CSMA/CA para estimar el tiempo que hay que esperar antes de hacer un nuevo intento de acceso al medio. El campo "número de secuencia" se usa para numerar las tramas de datos, con lo que un receptor puede descartar tramas duplicadas, o solicitar el reenvío de determinadas tramas perdidas.

2.5.4. Asociación a un AP.

Para averiguar los AP disponibles y sus características de conexión, las estaciones emiten una trama "*Probe Request*" y esperan una trama "*Probe Response*" de cada AP:

Tipo	Origen	Destino	Descripción
Probe Request	estación	Broadcast	Envía información sobre velocidades soportadas, pide información sobre los AP disponibles.
Probe Response	AP	estación	Envía información de conexión del AP, la estación recibe una trama por cada AP disponible.

Para que una estación pueda enviar tramas por una red inalámbrica primero debe autentificarse y asociarse a un punto de acceso para poder utilizarlo como enlace con la red de infraestructura. Para ello se definen las siguientes tramas:

Tipo	Origen	Destino	Descripción
Authentication	estación	AP	Datos de autentificación según el sistema que soporte el AP
Authentication	AP	estación	Acepta la autentificación de la estación.
Association Request	estación	AP	Envía solicitud de conexión al AP.
Association Response	AP	estación	Respuesta a la petición de asociación de la estación con el AP. Envía identificador de la asociación.

En el caso de la red de prácticas, al tratarse de una red abierta, la información de autentificación que se envía sólo incluye el tipo de autentificación: abierta.

Una vez establecida la asociación con el AP, hay que definir los parámetros de la comunicación a nivel de red. Para ello se suele utilizar el protocolo DHCP (*Dynamic Host Configuration Protocol*), que emplea las siguientes tramas:

Tipo	Origen	Destino	Descripción
DHCP Request	estación	Broadcast	Pide datos de conexión, puede incluir datos de conexión previas para que el servidor los confirme.
DHCP ACK	AP	Broadcast	Envía información de configuración de la estación.
Gratuitous ARP	estación	Broadcast	Informar a la red inalámbrica de la IP asignada.

Finalmente, cuando una estación decide desaociarse del AP envía una trama para informar al respecto:

Tipo	Origen	Destino	Descripción
Disassociate	estación	AP	Informa al AP que la estación se desasocia de él.

2.6. Bibliografía complementaria

[1] RFC 1349: Type of service in the Internet Protocol, 1992. Definición original de la función del campo ToS de la cabecera de IPv4. Ha sido sustituida por la RFC2474.

[2] RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, 1998. Nueva definición para el campo de la cabecera IP originalmente denominado ToS.

[3] RFC3168: The Addition of Explicit Congestion Notification (ECN), 2001.

[4] RFC 2598: An Expedited Forwarding PHB (Per-Hop forwarding Behaviors), 1999.

[5] RFC 2597: Assured Forwarding PHB (Per-Hop forwarding Behaviors) Group, 1999.

[6] Información y manuales en las páginas Web de Cisco Systems: http://www.cisco.com/. Algunos documentos están disponibles en el Campus Virtual.

[7] "Redes e Internet de alta velocidad: rendimiento y calidad de servicio", 2ª edición, William Stallings. Pearson - Prentice Hall, 2004.

[8] RFC 1042: A Standard for the Transmission of IP Datagrams over IEEE 802 Networks, 1988.

[9] "Redes Wireless 802.11". Matthew S. Gast. O'Reilly - Anaya Multimedia. 2006.

[10] IEEE 802.1H: Media Access Control (MAC) Bridging of Ethernet V2.0 in Local Area Networks, 1997.

3. Herramientas

En esta práctica se pueden utilizar las distintas herramientas y los monitores de red descritos y empleados en prácticas anteriores, tanto en el equipo del alumno como en los equipos Linux1, Linux2 y Linux3. A estos se equipos se puede acceder desde los PCs del laboratorio mediante un cliente Telnet o Putty, mediante el usuario "**alumnos**" y la contraseña indicada por el profesor de prácticas. Además, se emplearan nuevas opciones de los comandos "**stdprac**" y "**ping**", las cuales se describen a continuación.

3.1. Comando "stdprac"

Como en las prácticas anteriores, este comando del **Linux2** permite acceder a la configuración de los routers del laboratorio. Para esta práctica se utilizarán nuevas opciones relativas a gestión del QoS en el laboratorio. La sintaxis completa del comando es la siguiente:

```
stdprac <2513|1720|1601> <CMD1> [texto]
stdprac <1720> <CMD2> <IP> <PREC>
```

Comandos para la sintaxis tipo CMD1:

rutas	Muestra la tabla de encaminamiento. Ejecuta el comando "*show ip route*" en el router.
nat	Muestra la tabla NAT. Ejecuta el comando "show ip nat translations" en el router.
intf	Muestra información sobre los interfaces. Ejecuta el comando "*show ineterfaces*" en el router.
lst	Muestra configuración de las listas de acceso. Ejecuta el comando "*show access-list*" en el router.
rmap	Muestra configuración de la clasificación de tráfico. Ejecuta el comando "*show route-map*" en el router.
traf	Muestra la configuración de "*Traffic shaping*" con GTS. Ejecuta el comando "*show traffic*" en el router.
traf2	Muestra el estado de procesamiento del "Traffic Shaping" (paquetes procesados, tamaño de colas…). Ejecuta el comando "*show traffic statistics*" en el router.
rate	Muestra la configuración de "*Traffic policing*" con CAR. Ejecuta el comando "*show interfaces rate-limit*" en el router.
acc	Muestra cuenta de bytes y paquetes procesados. Ejecuta el comando "*show ip accounting*" en el router.
conf	Muestra configuración completa del router. Ejecuta el comando "*show conf*" en el router.
[texto]	Cadena opcional que se utiliza para filtrar el resultado. Por ejemplo, se puede especificar una dirección IP, el nombre de un interfaz, el número de una lista de acceso, etc. para obtener sólo la información buscada.

Comandos para la sintaxis tipo CMD2 (solo aplicable al router Cisco 1720):

qos Activa el control de calidad de servicio para los paquetes dirigidos a la dirección IP dada en <IP> (dirección del equipo del alumno), de forma que se marcan esos paquetes IP con la precedencia indicada en <PREC>, que debe ser 0, 1 o 2. Para ello, se añade una nueva condición de clasificación que incluye la dirección IP indicada en la lista de acceso dinámica correspondiente, ejecutando el comando "access-t 11<PREC> pre<PREC> any host <IP> timeout 1" en el router. El criterio de clasificación se desactiva automáticamente si transcurre 1 minuto sin que circulen paquetes que lo cumplan por el router.

Hay que tener en cuenta que, si se mete otro criterio existiendo uno ya activo, el router utilizará solo el que aparece primero en las lista de acceso, que será el de la lista de menor índice.

Por motivos de seguridad, los alumnos no pueden acceder directamente a la configuración de los routers del laboratorio. Pero ejecutar el comando "stdprac" en el Linux2 equivale a ejecutar los comandos descritos arriba en el router correspondiente.

3.2. Comando "ping" en Linux

Además de las opciones utilizadas en prácticas anteriores, "ping" incluye una opción relativa a la gestión de calidad de servicio, si bien esta opción no funciona bien en los equipos con Windows XP. En cambio, en un sistema Linux sí que se puede usar esa opción para generar paquetes IP-ICMP con un determinado valor del campo ToS/DS de la cabecera IP. En Linux, la sintaxis típica del comando y los parámetros más comunes son estos:

```
ping [-c <valor>][-s <valor>][-t <valor>][-T <valor>] <dirección IP>
```

-**c** cuenta Cantidad de solicitudes de eco a enviar.
-**s** tamaño Tamaño del bloque de datos del mensaje ICMP.
-**t** TTL Valor de tiempo de vida inicial.
-**T** ToS Valor del campo ToS/DS de la cabecera IP. En algunos equipos Linux esta opción se indica como "-**Q** ToS", como es el caso del Linux3.

Hay que considerar el valor indicado con la opción "–T" (o "–Q") es para todo el campo ToS (DS) del paquete IP, no solo para la precedencia (o DSCP). Así por ejemplo, la opción "-T 160" genera paquetes IP con precedencia 5 (ver apartados 2.2.1 y 2.2.2).

Si no se especifica la opción "-c", se enviarán solicitudes de eco hasta que se pulse "Control-C". Se puede obtener una descripción completa de las opciones del comando en un sistema Linux ejecutando "man ping".

3.3. Captura del tráfico IEEE 802.11 en la red del laboratorio

Debido a la encapsulación Ethernet (ver apartado 2.5.2), es muy posible que, al realizar una captura de tráfico en un interfaz inalámbrico IEEE 802.11, se obtengan solamente las tramas Ethernet en vez de las tramas MAC 802.11. Esto dependerá del sistema operativo, del adaptador de red, del controlador del adaptador de red y de la aplicación utilizada.

Para poder estudiar el tráfico de datos IEEE 802.11 en el laboratorio se usará el Linux3, con S.O. Linux Suse, una tarjeta 802.11b/g basada en el chipset Athereos, y el software Madwifi (http://madwifi-project.org), un controlador avanzado y estable para usar las tarjetas basadas en Athereos en sistemas Linux. Este equipo actúa a la vez como AP de un

BSS, y como monitor de tráfico 802.11, además de router IP. De esta forma, aunque el Linux 3 dispone de un único adaptador de red 802.11, en su configuración hay dos interfaces inalámbricos:

- **atho.** Este interfaz corresponde al AP del BSS con SSID "PracRedes", configurado en el canal 11, y tiene asignada la dirección IP 10.10.10.1. Permite capturar el tráfico de este BSS como las tramas Ethernet que utiliza IP.
- **ath1**. Interfaz en modo "monitor de red inalámbrica", que permite capturar el tráfico real 802.11 en el canal 11 para la zona laboratorio.

Se puede usar el programa "tcpdump" en Linux 3 para capturar tráfico sobre cualquiera de los dos interfaces anteriores. Conviene utilizar la opción "**–s**" del programa, para especificar un tamaño máximo para las tramas capturadas mayor al valor por defecto de 68 bytes. Por ejemplo, para capturar todo el tráfico 802.11 se puede usar:

```
sudo /usr/sbin/tcpdump –i ath1 –s 2000 –w miarchivo.cap
```

4. Experimentos a realizar

Antes de experimentar las cuestiones que se plantean a continuación, hay que ejecutar el *script* "C:\pracredes.bat" que hay en el PC.

4.1. El campo de precedencia de IP

1. Accede al Linux2 o al Linux3 para ejecutar comandos "ping" (ver 3.2). ¿Qué valor tienes que poner tras la opción "–T" (o **"–Q**" en Linux3) del comando "ping –c 5 –T <VALOR> <IP de tu equipo>" para generar paquetes IP con un valor de precedencia "Flash"? Verifica la respuesta utilizando el monitor de red Wireshark en tu equipo, o el "tcpdump" en otra consola Telnet o Putty en el Linux 2 o 3.
2. Envía paquetes por el túnel de nivel 3 (IP sobre IP) visto en la práctica 2 ejecutando el comando "ping -T 128 –c 5 10.5.2.2" en el Linux 2 o "ping -Q 128 –c 5 10.5.2.2" en el Linux 3. Con el monitor de red "tcpdump" en otra consola Telnet o Putty captura los paquetes ICMP en el túnel.
   a. ¿Qué precedencia lleva la cabecera IP del protocolo pasajero? ¿Qué precedencia lleva la cabecera IP del protocolo portador?
   b. ¿Son iguales los valores de precedencia para el protocolo IP portador y el IP pasajero? ¿Por qué se pone ese valor de precedencia en el protocolo portador?

4.2. Gestión de QoS en el laboratorio con GTS

3. Determina el camino que siguen los paquetes que tu equipo envía a una dirección IP de Internet, y el camino que, en general, siguen los paquetes de respuesta. ¿Por qué routers de laboratorio pasan?
4. Analiza la configuración del router Cisco 1720 (con el comando "stdprac" y sus opciones, según el apartado 3.1) y determina…
   a. ¿A qué interfaz se aplica una clasificación y marcado del tráfico de entrada? ¿Qué comandos definen la clasificación en ese interfaz? ¿Cómo se denomina la clasificación?

b. ¿En cuántos tipos se clasifican los paquetes marcados? ¿Qué listas de acceso definen los criterios de clasificación para el marcado de paquetes? ¿Son estáticas o dinámicas?

c. ¿A que interfaz se aplica una política de gestión de tráfico "Traffic Shaping"? ¿Qué comandos se utilizan? ¿Cuántos tipos de "Traffic Shaping" se definen y que valores de CIR definen?

d. ¿Qué listas de acceso definen los criterios para la política "Traffic Shaping"? ¿Son estáticas o dinámicas? ¿Qué criterios definen esas listas?

e. Usa el comando "stdprac 1720 intf" para averiguar qué estrategia de colas de salida (FIFO, WFQ, PQ…) tiene configurado cada interfaz del router 1720. Puedes analizar también los otros routers.

5. Accede al servidor FTP de la Universidad de Alicante con un navegador web (ftp://ftp.ua.es ó ftp://172.25.1.132). Accede a la carpeta "/ua/antivirus".

a. Activa la captura del monitor de red Wireshark en tu equipo para capturar los paquetes TCP que intercambia tu equipo con el servidor "ftp.ua.es", y después intenta descargar el archivo "spybotsd152.exe".

b. ¿Qué velocidad de descarga aproximada te marca el gestor de descargas del navegador? ¿Se descarga rápido o lentamente?

c. Accede a otro servicios y servidores (por ejemplo, el servicio Web de la Universidad de Alicante en "http://www.ua.es" o al Web de la EPS en "http://www.eps.ua.es/" para descargar algún documento o archivo, y evalúa la velocidad de acceso que se percibe. ¿Es mejor o peor que la de "ftp.ua.es"?

d. Ejecuta en el Linux2 "stdprac" para ver el estado de la gestión de control de QoS del Cisco 1720. ¿Procesa paquetes esa gestión?

e. Para la captura, y localiza en algún paquete IP el campo de ToS y el valor de precedencia. ¿Cómo denomina el monitor Ethereal al campo de ToS? ¿Qué valor de precedencia del ToS tienen los paquetes IP que envía tu equipo al servidor "ftp.ua.es"? ¿Y los que recibe de ese servidor?

f. En la captura localiza los paquetes recibidos del servidor "ftp.ua.es" en la conexión TCP de la descarga del archivo. ¿Qué tiempo aproximado hay entre cada dos paquete TCP de descarga? ¿Se pueden ver retrasmisiones de paquetes TCP?

g. ¿Qué estrategia de control de QoS se está aplicando a los paquetes correspondientes a la descarga del archivo?

6. Corta la descarga anterior del archivo "spybotsd152.exe" si no ha acabado, espera unos 2 minutos. Accede al Linux 2, y ejecuta "stdprac 1720 qos <IP DE TU PC> **2**" para añadir un criterio de clasificación para los paquetes que recibe tu equipo (ver 3.1).

a. Examina las listas de acceso en el router 1720 con "stdprac" y comprueba que aparece tu dirección IP en una lista con precedencia 2. ¿En qué lista aparece ahora? Si tu dirección aparece en más de una lista, espera un poco sin intercambiar datos con el servidor "ftp.ua.es" hasta que se desactive automáticamente una de ellas.

b. Repite los pasos de la cuestión 3 de este apartado.

4.3. Gestión de QoS en el laboratorio con CAR

7. Examina la configuración del router Cisco 1601 ejecutando "stdprac 1601 conf" en el Linux 2, y busca la configuración de control de QoS.
   c. ¿Qué comando de QoS se aplica? ¿De qué tipo de estrategia se trata, "*shaping*" o "*policing*"? ¿En qué interface se aplica? ¿Qué CIR se define?
   d. ¿Qué lista de acceso define los paquetes a los que se aplica la configuración de QoS? ¿Qué condiciones define esa lista de acceso?
8. Examina la configuración del router Cisco 2513 ejecutando "stdprac 2513 conf" en el Linux 2, y busca la estrategia de clasificación y marcado de paquetes IP que aplica.
   a. ¿Qué comando de clasificación y marcado se aplica? ¿Cuántas clases de tráfico se clasifican? ¿Cómo se marcan los paquetes IP que cumplen las condiciones de las clases de tráfico?
   b. ¿Qué listas de acceso definen las clases de tráfico para el comando de clasificación y marcado? ¿Qué condiciones define esas listas de acceso?
   c. Además del marcado de los paquetes, ¿Qué otra cosa establece el comando de clasificación y marcado?
   d. ¿En qué interfaz se aplica la clasificación?
9. En base a las dos cuestiones anteriores, determina el camino que siguen los paquetes que proceden del servidor 172.25.32.162 y llegan desde Internet hasta tu PC pasando por los routers del laboratorio.
10. Inicia una captura del monitor de red Wireshark en tu PC, y después accede a la página web "http://172.25.32.162/std" o "http://www.aurova2.ua.es/std" con un navegador Web, y descarga el archivo "spybotsd152.exe" de este servidor.
    a. ¿Qué velocidad de transmisión indica el gestor de descargas del navegador? ¿la descarga es rápida o lenta? Compara la velocidad con la de otros servidores Web.
    b. Ejecuta en el Linux2 "stdprac" varas veces, durante la descarga del archivo, para ver el estado de la gestión de control de QoS del Cisco 1601. Hay que usar la opción adecuada de "stdprac" para ver la configuración e CAR. ¿Procesa paquetes esa gestión? ¿Se descartan paquetes?
    c. Para la captura del monitor de red, y localiza los paquetes recibidos del servidor 172.25.32.162" en la conexión TCP de la descarga del archivo. ¿Qué tiempo aproximado hay entre cada dos paquete TCP de descarga? ¿Se pueden ver retrasmisiones de paquetes TCP?
    d. ¿Qué estrategia de control de QoS se está aplicando a los paquetes correspondientes a la descarga del archivo?

4.4. Análisis del tráfico en una red IEEE 802.11

Para resolver estas cuestiones se necesita el adaptador inalámbrico USB que debe repartir el profesor de prácticas. Tras conectar esté adaptador a tu PC, aparecerá el icono de las "conexiones de red inalámbricas" en la bandeja de MS. Windows XP. Pulsando en ese icono, se pude conectar a la red con SSID "PracRedes", o desconectarte de ella. Antes de desenchufar el adaptador USB, hay que extraer el dispositivo "D-Link AirPlus" pulsando en el icono "Extracción segura" de la bandeja. No olvides **devolver** el adaptador al profesor.

11. Antes de conectarte a una red inalámbrica, accede al Linux 3 para iniciar una captura por el interfaz "**ath1**" (ver apartado 3.3). Después accede al administrador de redes inalámbricas y conecta con la red "PracRedes". Ejecuta los comandos "ping 10.10.10.2" y "ping 10.10.10.1" en tu PC del laboratorio. Desconecta de la red inalámbrica y después para la captura. Analiza la captura en tu equipo para responder estas cuestiones.
    e. Localiza alguna trama "Probe Request" de las que envía tu equipo (comprueba que tu dirección MAC está en la dirección origen), y averigua las velocidades que soporta el adaptador inalámbrico de tu equipo.
    f. Localiza varias tramas "Probe Response" a lo largo de la captura y examina la información de gestión 802.11 que contienen. ¿A que redes (SSID) corresponden las tramas? Determina, para las diferentes redes que aparecen, las velocidades soportadas por los puntos de acceso, el canal de radio en que trabajan, y si se usan protocolos de seguridad (WEP, WPA,…).
    g. Averigua la dirección MAC del AP de la red "eduroam".
    h. Localiza y analiza el contenido de las tramas del proceso de autentificación y asociación de tu equipo al AP de "PracRedes". ¿Se emplea algún tipo de algoritmo de autentificación, o es abierta?
    i. Busca las tramas DHCP de la conexión de tu equipo, y analiza la respuesta "DHCP Ack" del AP-Router. ¿Qué dirección IP se asigna a tu equipo? ¿A qué subred pertenece? ¿Para cuánto tiempo sirve esa dirección IP? ¿Se asigna algún otro parámetro de configuración IP a tu equipo?
    j. Busca las tramas que contienen los paquetes IP-ICMP del ping al destino 10.10.10.2 que has ejecutado en tu equipo. ¿Cuántas direcciones MAC tienen esas tramas? ¿A que equipos pertenecen esas direcciones MAC?
    k. Busca las tramas con los paquetes IP-ICMP del ping al destino 10.10.10.1. ¿A que equipos pertenecen las direcciones MAC de estas tramas?
    l. Analiza unas de las tramas que contienen paquetes IP-ICMP y determina el tipo de de encasulapción Ethernet utilizada en la red "PracRedes" ¿Por qué se usa ese tipo de encapsulación? ¿En qué protocolo de la trama aparece el campo "tipo Ethernet" con el valor 800Hex? ¿Qué significa ese valor?
12. Accede al Linux 3 para iniciar una captura por el interfaz "**atho**" (ver apartado 3.3) y después conecta con la red "PracRedes". Ejecuta el comando "ping 10.10.10.2" en tu PC del laboratorio y después para la captura. Analiza la captura en tu equipo.
    m. ¿Qué tipo de nivel de enlace aparece? ¿Se puede ver información relativa a la red inalámbrica?
13. Inicia una captura en tu equipo a través del interfaz de la red inalámbrica usando Wiresharlk. y después conecta con la red "PracRedes". Analiza la captura en tu equipo.
    n. ¿Qué tipo de nivel de enlace aparece? ¿Se puede ver información relativa a la red inalámbrica?
14. Mientras tu equipo está conectado a la red inalámbrica "RedesPrac", inicia una captura de las tramas 802.11 desde el interfaz "**ath1**" del Linux 3, y usa el comando "ping -l 3000 -n 2 10.10.10.2"en tu PC del laboratorio para enviar paquetes IP de gran tamaño.
    o. ¿De qué tamaño máximo son los fragmentos de IP? ¿Qué MTU está utilizando IP para fragmentar?

p. ¿Fragmenta el MAC 802.11? ¿Qué tamaño de datos tienen las tramas MAC 802.11 que transportan los fragmentos IP más grandes? ¿Cuántos bytes añaden las cabeceras LLC y MAC al datagrama IP?