



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.1221

(03/2002)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA
INFORMACIÓN Y ASPECTOS DEL PROTOCOLO
INTERNET

Aspectos del protocolo Internet – Arquitectura, acceso,
capacidades de red y gestión de recursos

**Control de tráfico y control de congestión en
las redes basadas en el protocolo Internet**

Recomendación UIT-T Y.1221

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN Y ASPECTOS DEL PROTOCOLO INTERNET

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestion de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T Y.1221

Control de tráfico y control de congestión en las redes basadas en el protocolo Internet

Resumen

En esta Recomendación se presenta una descripción general así como los objetivos y los procedimientos para el control del tráfico y de la congestión en las redes basadas en el protocolo IP. En particular, se describen los conceptos del contrato de tráfico entre un usuario y la red. Se especifican las capacidades de transferencia de IP (IPTC) incluyendo, para cada IPTC, el modelo de servicio, los diagramas de tráfico asociados y la definición de conformidad.

Orígenes

La Recomendación UIT-T Y.1221, preparada por la Comisión de Estudio 13 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 16 de marzo de 2002.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

© UIT 2002

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

Página

1	Alcance	1
2	Referencias	1
2.1	Referencias normativas	1
2.2	Referencias informativas	2
3	Abreviaturas y terminología	2
3.1	Abreviaturas	2
3.2	Terminología	3
4	Introducción.....	4
5	Parámetros y descriptores de tráfico.....	4
5.1	Definiciones.....	4
5.1.1	Clasificación de los paquetes IP	4
5.1.2	Flujo IP y subflujo IP	5
5.1.3	Parámetro de tráfico	5
5.1.4	Descriptor de tráfico	5
5.1.5	Contrato de tráfico	5
5.2	Requisitos de los parámetros de tráfico y los descriptores de tráfico.....	5
5.3	Especificaciones de los parámetros de tráfico	5
5.3.1	Configuración de referencia	5
5.3.2	Descripción de los parámetros de tráfico	5
6	Capacidades de transferencia IP	6
6.1	Capacidad de transferencia con anchura de banda dedicada (DBW).....	6
6.1.1	Descripción.....	6
6.1.2	Modelo de servicio	6
6.1.3	Descriptor de tráfico	7
6.1.4	Definición de conformidad.....	7
6.1.5	Compromisos de QoS.....	7
6.2	Capacidad de transferencia con anchura de banda estadística (SBW)	7
6.2.1	Descripción.....	7
6.2.2	Modelo de servicio	7
6.2.3	Descriptor de tráfico	8
6.2.4	Definición de conformidad.....	8
6.2.5	Compromisos de QoS.....	8
6.3	Capacidad de transferencia de tipo mejor esfuerzo (BE)	8
6.3.1	Descripción.....	8
6.3.2	Modelo de servicio	8
6.3.3	Descriptor de tráfico	8

	Página
6.3.4 Definición de conformidad.....	8
6.3.5 Compromisos de QoS.....	8
7 Funciones para el control de tráfico, control de congestión y tratamiento de la sobrecarga.....	9
7.1 Funciones de control de tráfico	9
7.1.1 Gestión de recursos de red.....	9
7.1.2 Control de admisión	9
7.1.3 Control de parámetros	9
7.1.4 Marcación de paquetes	9
7.1.5 Conformación de tráfico.....	10
7.1.6 Calendarización de paquetes	10
7.2 Funciones para el control de la congestión y el tratamiento de la sobrecarga.....	10
7.2.1 Control de descarte de paquetes	10
7.2.2 Notificación de congestión explícita	10
8 Métodos y herramientas para la ingeniería de tráfico IP	10
Anexo A – El colector de testigos y el algoritmo genérico de velocidad de octetos (GBRA)	10
A.1 El colector de testigos.....	11
A.2 El colector de testigos de estado continuo.....	11
A.3 El algoritmo genérico de velocidad de octetos.....	12
A.4 El algoritmo de velocidad de octetos por calendarización virtual.....	12
A.5 El algoritmo de velocidad de octetos por colector con fugas de estado continuo	12
Anexo B – Comportamiento de dos algoritmos de velocidad de octetos genéricos coordinados.....	13
Apéndice I – Ilustración del comportamiento del colector de testigos	14
I.1 Caracterización de un flujo con una sola velocidad y un solo tamaño colector de testigos	15
I.2 Caracterización de un flujo con dos velocidades y dos colectores de testigos ($B_p < B_s$).....	17
I.3 Caracterización de un flujo con dos velocidades y dos colectores de testigos ($B_p > B_s$).....	18
Apéndice II – Relación entre especificaciones de clase de QoS e IntServ/DiffServ de IETF.....	19
II.1 IPTC con anchura de banda dedicada asociada con una clase de QoS adecuada	20
II.2 IPTC con anchura de banda estadística asociada con una clase de QoS adecuada	20

Recomendación UIT-T Y.1221

Control de tráfico y control de congestión en las redes basadas en el protocolo Internet

1 Alcance

En esta Recomendación se describen los procedimientos de control del tráfico y de la congestión para las redes basadas en IP. Éstos son necesarios para el soporte de servicios con QoS, cuando la QoS se negocia entre un usuario y la red.

El control del tráfico se refiere a todas las acciones de la red orientadas a satisfacer los objetivos de calidad de funcionamiento negociados en una red basada en IP y para propiciar que se eviten condiciones de congestión.

El control de la congestión se refiere a todas las acciones de la red orientadas a minimizar la intensidad, dispersión y duración de la congestión.

En esta Recomendación se presenta una descripción general así como los objetivos y los procedimientos para el control del tráfico y de la congestión. En particular, se describen los conceptos del contrato de tráfico entre un usuario y la red. Se especifican las capacidades de transferencia de IP (IPTC) incluyendo, para cada IPTC, el modelo de servicio, los diagramas de tráfico asociados y la definición de conformidad.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones, por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

2.1 Referencias normativas

- Recomendación UIT-T I.371 (2000), *Control de tráfico y control de congestión en la RDSI-BA*.
- Recomendación UIT-T Y.1241 (2001), *Soporte de servicios basados en el protocolo Internet de transferencia de protocolo Internet que utilizan capacidades*.
Recomendación UIT-T Y.1540 (1999), *Servicio de comunicación de datos con protocolo Internet – Parámetros de calidad de funcionamiento relativos a la disponibilidad y la transferencia de paquetes de protocolo Internet*.
- Recomendación UIT-T Y.1541 (2002), *objetivos de calidad de funcionamiento de la red para servicios basados en protocolo Internet*.

2.2 Referencias informativas

- IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program – Protocol Specification*.
- IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: an Overview*.
- IETF RFC 2210 (1997), *The use of RSVP with IETF Integrated Services*.
- IETF RFC 2211(1997), *Specification of the Controlled-Load Network Element Service*.
- IETF RFC 2212 (1997), *Specification of Guaranteed Quality of Services*.
- IETF RFC 2698 (1999), *A Two Rate Three Color Marker*.
- IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.
- IETF RFC 2481 (1999), *A Proposal to Add Explicit Congestion Notification (ECN) to IP*.
- IETF RFC 2597 (1999), *Assured Forwarding PHB Group*.
- IETF RFC 2598 (1999), *An Expedited Forwarding PHB*.

3 Abreviaturas y terminología

3.1 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas:

<i>B</i>	Tamaño de colector de un colector de testigos (<i>bucket size of a token bucket</i>)
<i>BE</i>	Mejor esfuerzo (<i>best effort</i>)
<i>Bp</i>	Tamaño de colector de un colector de testigos de cresta (<i>bucket size of peak token bucket</i>)
<i>Bs</i>	Tamaño de colector de un colector de testigos sostenible (<i>bucket size of sustainable token bucket</i>)
<i>DBW</i>	Capacidad de transferencia de IP con anchura de banda dedicada (<i>dedicated bandwidth IP transfer capability</i>)
<i>DS</i>	Servicios diferenciados (campo encabezamiento IP) [<i>differentiated services (IP header field)</i>]
<i>GBRA</i>	Algoritmo genérico de velocidad de octetos (<i>generic byte rate algorithm</i>)
<i>GCRA</i>	Algoritmo genérico de velocidad de células (<i>generic cell rate algorithm</i>)
<i>IETF</i>	Grupo de tareas especiales de ingeniería en Internet (<i>Internet engineering task force</i>)
<i>IP</i>	Protocolo Internet (<i>Internet protocol</i>)
<i>IPDV</i>	Variación del retardo de IP (<i>IP delay variation</i>)
<i>IPLR</i>	Relación de pérdida de IP (<i>IP loss ratio</i>)
<i>IPTC</i>	Capacidad de transferencia de IP (<i>IP transfer capability</i>)
<i>IPTD</i>	Retardo de transferencia de IP (<i>IP transfer delay</i>)
<i>LR</i>	Velocidad de línea (<i>line rate</i>)
<i>M</i>	Tamaño máximo permitido del paquete (<i>maximum allowed packet size</i>)
<i>N</i>	Tamaño (en octetos) de un paquete IP [<i>size (in byte) of an IP packet</i>]
<i>PC</i>	Control de parámetros (<i>parameter control</i>)
<i>QoS</i>	Calidad de servicio (<i>quality of service</i>)
<i>R</i>	Velocidad de un colector de testigos (<i>rate of a token bucket</i>)

R_p	Velocidad de un colector de testigos cresta (<i>rate of peak token bucket</i>)
R_s	Velocidad de un colector de testigos sostenible (<i>rate of sustainable token bucket</i>)
SBW	Capacidad de transferencia de IP con anchura de banda estadística (<i>statistical bandwidth IP transfer capability</i>)
TB	Colector de testigos (<i>token bucket</i>)
TC	Capacidad de transferencia (<i>transfer capability</i>)
ToS	Tipo de servicio (campo encabezamiento IP, véase DS) (<i>type of service</i>)

3.2 Terminología

En esta Recomendación se definen los términos siguientes.

3.2.1 conformidad: La conformidad es la aplicación de uno o más criterios a un flujo, en una interfaz normalizada dada.

3.2.2 congestión: La congestión se define como un estado de los elementos de red (por ejemplo, encaminador, conmutadores) durante el cual la red no está apta para satisfacer los objetivos de calidad de funcionamiento de la red y los compromisos de la QoS negociadas para el flujo ya establecido.

3.2.3 flujo de protocolo Internet: Se define un flujo de IP en una interfaz dada como la incidencia en esa interfaz del conjunto de paquetes IP que corresponde a una clasificación dada (véase 5.1.2).

3.2.4 control de tráfico de protocolo Internet: Se refiere a las acciones de la red orientadas a satisfacer los objetivos de calidad de funcionamiento de la red y los compromisos de la QoS negociada.

3.2.5 control de congestión de protocolo Internet: Se refiere a todas las acciones de la red orientadas a minimizar la intensidad, dispersión y duración de la congestión.

3.2.6 capacidad de transferencia de protocolo Internet: La capacidad de transferencia de IP es un conjunto de capacidades de red proporcionado por la red basada en IP para transferir flujos de IP.

3.2.7 sobrecarga: Se define la sobrecarga como un estado de elemento de red en el cual el desbordamiento de la memoria intermedia tiene por consecuencia que se descarten paquetes en flujos en que no existen compromisos de QoS.

3.2.8 clasificación de paquetes: Se denomina clasificación de paquetes IP el proceso de distinguir entre paquetes IP con el fin de aplicar mecanismos apropiados de control de tráfico y congestión (véase 5.1.1).

3.2.9 contrato de tráfico: Para un flujo IP dado, la capacidad de transferencia de IP seleccionada (véase la cláusula 6), el descriptor de tráfico en una interfaz dada y la clase de QoS (véase la Rec. UIT-T Y.1541) definen el contrato de tráfico para esa interfaz. Véase 5.1.5.

3.2.10 descriptor de tráfico: Un descriptor de tráfico es el conjunto de parámetros de tráfico utilizados para captar las características de tráfico de un flujo IP en una determinada interfaz normalizada como parte del contrato de tráfico. Véase 5.1.4.

3.2.11 parámetro de tráfico: Un parámetro de tráfico describe un aspecto de un flujo. Véase 5.1.3.

4 Introducción

La función principal de los procedimientos de control de tráfico y de control de congestión es la protección de la red IP y del tráfico que accede a la red a fin de alcanzar los objetivos de calidad de funcionamiento de la red IP y cumplir los compromisos de QoS. El control de tráfico y de congestión facilita la optimización del uso de los recursos de la red IP.

En las redes basadas en IP, la congestión se define como un estado de los elementos de red (por ejemplo, encaminadores, conmutadores), durante el cual la red no está apta para satisfacer los objetivos de calidad de funcionamiento de la red y cumplir los compromisos de la QoS negociada para el flujo establecido. La congestión se debe distinguir del estado en el que el desbordamiento de la memoria intermedia provoca la pérdida de paquetes IP, aunque se satisface aun la calidad de servicio negociada. Para los servicios sin compromiso de QoS tales como los servicios de tipo "mejor esfuerzo", normalmente se utiliza el término sobrecarga en lugar de congestión.

En esta Recomendación se define un conjunto de capacidades de control de tráfico y de control de congestión. Puede resultar apropiado considerar conjuntos adicionales de tales capacidades, para los cuales se utilizarán mecanismos de control de tráfico adicionales para alcanzar una mayor eficiencia de la red.

Se debe observar que los procedimientos de control de tráfico se aplican a los flujos de paquetes IP. Para algunos flujos IP, la red se compromete a cumplir los objetivos de QoS, suponiendo que el flujo de paquetes IP generado por el usuario se ajusta al contrato de tráfico. Para los flujos IP sin un contrato de tráfico entre el usuario y la red, esta última puede proporcionar un servicio de tipo mejor esfuerzo.

5 Parámetros y descriptores de tráfico

5.1 Definiciones

5.1.1 Clasificación de los paquetes IP

Típicamente, los paquetes IP de muy diversas fuentes pueden cruzar una interfaz dada hacia muchos destinos diferentes. Para el propósito del control de tráfico y el control de congestión IP, es fundamental que no se traten todos los paquetes IP de la misma manera sino de manera diferente, según los objetivos y los compromisos establecidos. Por lo tanto, es útil distinguir los paquetes IP por categorías pertinentes. Se denomina clasificación de paquetes IP al proceso de distinguir entre los paquetes IP con el fin de aplicar mecanismos apropiados de control de tráfico y de congestión. La clasificación de los paquetes IP se basa en la información contenida en los siguientes campos de encabezamiento IP: dirección de origen, dirección de destino [RFC 791] y el campo ToS/DS [RFC 791/RFC 2474]. El nivel de detalle en la clasificación puede diferir, lo que dependerá de su utilización específica. Los siguientes ejemplos ilustran esta situación.

- Ejemplo 1 – A fin de reconocer los paquetes IP que fluyen de una dirección de origen dada a una dirección de destino dada, se utiliza en la clasificación la longitud completa de los campos dirección de origen y de destino.
- Ejemplo 2 – A fin de reconocer los paquetes IP que fluyen de una dirección de origen dada a una dirección de destino dada con un nivel de servicio dado, se utiliza en la clasificación la longitud completa de los campos de dirección de origen y de destino así como el campo DS.
- Ejemplo 3 – A fin de reconocer los paquetes IP que fluyen de un origen en una subred dada a un destino en otra subred dada, se aplican las respectivas plantillas de la subred a los campos de dirección de origen y de destino.

NOTA – En esta versión de la Recomendación solamente se hace referencia a la clasificación de paquetes para la versión 4 de IP. La clasificación para IPv6 y MPLS queda en estudio.

5.1.2 Flujo IP y subflujo IP

Se define un flujo IP en una interfaz dada como la ocurrencia en esa interfaz del conjunto de paquetes IP que corresponde a una determinada clasificación (véase 5.1.1). Un flujo IP puede consistir en paquetes de una sola sesión de aplicación, o puede ser una agrupación que comprenda el tráfico combinado de una cierta cantidad de sesiones de aplicación. Cuando una clasificación se puede subdividir en diferentes subclasificaciones (separadas o superpuestas) es posible reconocer diferentes subflujos IP en el flujo IP correspondiente.

5.1.3 Parámetro de tráfico

Un parámetro de tráfico describe un aspecto de un flujo. Puede ser cualitativo o cuantitativo. Por ejemplo, un parámetro de tráfico puede describir la velocidad binaria de cresta, la velocidad de paquetes de cresta, la velocidad binaria promedio, el tamaño promedio o máximo del paquete, la longitud de ráfaga (promedio o máxima) de un flujo, etc.

5.1.4 Descriptor de tráfico

Un descriptor de tráfico es el conjunto de parámetros de tráfico que se utiliza para captar las características de tráfico de un flujo IP en una interfaz normalizada dada como parte del contrato de tráfico (véase 5.1.5).

5.1.5 Contrato de tráfico

Para un flujo IP dado, la capacidad de transferencia IP seleccionada (véase la cláusula 6), el descriptor de tráfico en una interfaz dada (véase 5.1.4) y la clase de QoS (véase la Rec. UIT-T Y.1541) definen el contrato de tráfico para esa interfaz.

5.2 Requisitos de los parámetros de tráfico y los descriptores de tráfico

Cualquier parámetro de tráfico que pueda estar relacionado con un descriptor de tráfico debe:

- tener la misma interpretación en ambos lados de una interfaz,
- tener sentido en los diagramas de atribución de recursos para cumplir con los requisitos de calidad de funcionamiento de la red,
- ser exigible a través del control de parámetros (PC, *parameter control*), véase 7.1.3.

5.3 Especificaciones de los parámetros de tráfico

5.3.1 Configuración de referencia

Queda en estudio.

5.3.2 Descripción de los parámetros de tráfico

Se definen los siguientes parámetros de tráfico que se pueden utilizar en el descriptor de tráfico.

5.3.2.1 Tamaño máximo permitido del paquete

El tamaño máximo permitido del paquete M se expresa en octetos. Es un parámetro de tráfico obligatorio para cada IPTC.

5.3.2.2 GBRA o colector de testigos

El algoritmo genérico de velocidad de octetos (GBRA, *generic byte rate algorithm*) o colector de testigos (TB, *token bucket*), descrito en el anexo A, se utiliza para caracterizar una velocidad y su correspondiente tendencia a presentarse en ráfagas. Ambos conceptos son equivalentes y utilizan el siguiente conjunto de dos parámetros:

- la velocidad R expresada en octeto/s;
- el tamaño del colector B expresado en octetos.

El descriptor de tráfico puede contener cero o más colectores de testigos (con los respectivos valores de R y B).

El conjunto actual de capacidades de transferencia IP (véase la cláusula 6) reconoce un TB de cresta (con parámetros velocidad de cresta R_p y tamaño de colector de cresta B_p) y un TB sostenible (con parámetros velocidad sostenible R_s y tamaño de colector sostenible B_s).

6 Capacidades de transferencia IP

Una capacidad de transferencia IP es un conjunto de capacidades de red proporcionado por las redes basadas en IP para transferir paquetes IP. Para cada capacidad de transferencia IP se define el modelo de servicio, el descriptor de tráfico, la definición de conformidad y cualquier compromiso de QoS. Una capacidad de transferencia IP es soportada por un conjunto de funciones de control de tráfico y de control de congestión.

A fin de ofrecer múltiples clases de QoS para múltiples aplicaciones y con objeto de optimizar la utilización de los recursos de red, las redes basadas en IP deben poder ofrecer múltiples capacidades de transferencia.

Se definen tres capacidades de transferencia IP:

- Capacidad de transferencia IP con anchura de banda dedicada (DBW, *dedicated bandwidth*);
- Capacidad de transferencia IP con anchura de banda estadística (SBW, *statistical bandwidth*);
- Capacidad de transferencia IP de tipo mejor esfuerzo (BE, *best-effort*).

El conjunto de capacidades de transferencia IP se basa en los modelos de servicio IP actuales y se podrá ampliar en el futuro.

6.1 Capacidad de transferencia con anchura de banda dedicada (DBW)

6.1.1 Descripción

La capacidad de transferencia con anchura de banda dedicada (DBW) está destinada a soportar aplicaciones con requisitos rigurosos de retardo. Tiene como objetivo soportar la entrega garantizada y oportuna de paquetes IP a lo largo del trayecto extremo a extremo de la red.

La capacidad de transferencia DBW se esfuerza por alcanzar la compatibilidad con el servicio garantizado [RFC 2212] y los servicios extremo a extremo basados en el comportamiento por salto reenvío expeditado [RFC 2598].

6.1.2 Modelo de servicio

La IPTC DBW puede ser utilizada por las aplicaciones que caracterizan el tráfico con un solo colector de testigo.

El compromiso establecido por la red es que la QoS de IP negociada esté asegurada para todos los paquetes cuando éstos se ajustan a las pruebas de conformidad. El usuario DBW debe esperar que los paquetes que no pasan las pruebas de conformidad (posiblemente todos) serán descartados por la red.

La capacidad DBW puede asociarse con compromisos de pérdida (relación de pérdida IP, IPLR) especificados y compromisos de retardo (retardo de transferencia IP, IPTD y variación de retardo IP, IPDV) especificado (véase la Rec. UIT-T Y.1541).

La red no fragmenta los paquetes. Además, la red se compromete a intentar, en la medida posible (por ejemplo hasta que se presente la necesidad de reencaminar el flujo) mantener la integridad de la secuencia de los paquetes.

6.1.3 Descriptor de tráfico

El descriptor de tráfico consta de los siguientes parámetros:

- la velocidad de cresta R_p y el tamaño de colector de cresta B_p especificado en 5.3.2.2;
- el tamaño máximo permitido de paquete M como se ha especificado en 5.3.2.2.

6.1.4 Definición de conformidad

Un paquete IP es conforme si la llegada se ajusta a las siguientes dos partes:

- la llegada es conforme al GBRA(R_p, B_p);
- la longitud real del paquete no excede el tamaño máximo permitido de paquete M .

El GBRA se actualiza solamente en el caso de paquetes conformes.

6.1.5 Compromisos de QoS

La capacidad DBW puede asociarse con los compromisos de pérdida especificados y los compromisos de retardo especificados.

Si todos los paquetes son conformes, los compromisos de QoS se aplican a todos los paquetes IP. El usuario DBW debe esperar que los paquetes no conformes (posiblemente todos) serán descartados por la red. Si no todos los paquetes son conformes, la red puede optar por un compromiso de QoS para algunos de los paquetes, por ejemplo para un volumen de paquetes que sean conformes.

6.2 Capacidad de transferencia con anchura de banda estadística (SBW)

6.2.1 Descripción

La capacidad de transferencia con anchura de banda estadística (SBW) tiene por objeto soportar aplicaciones que no tengan requisitos de retardo rigurosos. Está destinada al soporte de entrega garantizada de paquetes IP a lo largo del trayecto extremo a extremo de la red.

La capacidad de transferencia SBW se esfuerza para alcanzar la compatibilidad con el servicio de elemento de red de carga controlada [RFC 2211] y los servicios extremo a extremo basados en el comportamiento por salto reenvío asegurado [RFC 2597].

6.2.2 Modelo de servicio

La capacidad de transferencia SBW proporciona una velocidad sostenible (R_s) especificada para aplicaciones en tiempo no real con duración de ráfaga limitada y la expectativa de que el tráfico en exceso de GBRA(R_s, B_s) será entregado dentro de los límites de los recursos disponibles.

Los dos ejemplos siguientes describen el compromiso que se ofrecerá al usuario SBW:

- Si el usuario envía paquetes conformes a una velocidad constante menor que o igual que R_s , el compromiso es que todos estos paquetes se entregan a través de la red, en correspondencia con la clase de QoS asociada.
- Si el usuario no ha enviado paquetes por un tiempo prolongado y envía paquetes conformes en una ráfaga con una duración que no excede el límite establecido por GBRA(R_s, B_s), el compromiso es que todos estos paquetes se entregan a través de la red, en correspondencia con la clase de QoS asociada.

La capacidad SBW permite además que el usuario envíe paquetes conformes en exceso del GBRA(R_s, B_s), aunque el tráfico que excede este límite sólo será entregado dentro de los límites de los recursos disponibles.

La capacidad SBW puede estar asociada con un compromiso especificado relativo a la pérdida de paquetes.

La red no fragmenta los paquetes. Además, la red se compromete a intentar, en la medida posible (por ejemplo hasta que se presenta la necesidad de reencaminar el flujo), a mantener la integridad de la secuencia de los paquetes.

6.2.3 Descriptor de tráfico

El descriptor de tráfico consiste en:

- la velocidad de cresta R_p y el tamaño de colector de cresta B_p especificado en 5.3.2.2;
- la velocidad sostenible R_s y el tamaño de colector de testigos sostenible B_s especificado en 5.3.2.2;
- el tamaño máximo permitido del paquete M especificado en 5.3.2.1.

6.2.4 Definición de conformidad

Un paquete IP es conforme si la llegada se ajusta a las siguientes tres partes:

- la llegada es conforme con el GBRA de cresta (R_p, B_p);
- la llegada es conforme con el GBRA sostenible (R_s, B_s);
- la longitud real del paquete no excede el tamaño máximo del paquete M .

Los GBRA se actualizan en modo coordinado (véase el anexo B) sólo para los paquetes conformes.

6.2.5 Compromisos de QoS

La capacidad SBW puede estar asociada con compromisos de pérdida especificados.

Si todos los paquetes son conformes, los compromisos de QoS se aplican a todos los paquetes. De lo contrario, los compromisos de QoS se aplican a un cierto número de octetos en paquetes conformes. El tráfico no conforme será entregado dentro de los límites de los recursos disponibles.

6.3 Capacidad de transferencia de tipo mejor esfuerzo (BE)

6.3.1 Descripción

La capacidad de transferencia IP de tipo mejor esfuerzo es útil para soportar aplicaciones que no tienen requisitos de pérdida o retardo rigurosos.

6.3.2 Modelo de servicio

El modelo de servicio para el IPTC de tipo mejor esfuerzo (BE) requiere que se utilicen los recursos disponibles para el reenvío de los paquetes de los flujos de tipo mejor esfuerzo. Aun cuando no hay compromisos de QoS especificados, la expectativa es que se entregarán los paquetes siempre que estén disponibles suficientes recursos.

6.3.3 Descriptor de tráfico

- El tamaño máximo permitido de paquete M .

6.3.4 Definición de conformidad

Se requiere conformidad con el tamaño máximo de paquete M .

6.3.5 Compromisos de QoS

No existe ningún requisito de QoS en absoluto para esta capacidad de transferencia.

7 Funciones para el control de tráfico, control de congestión y tratamiento de la sobrecarga

El control de tráfico se refiere a un conjunto de funciones que controlan el flujo de los paquetes a través de una serie de funciones tales como el control de admisión, la gestión de recursos de red, y el control de parámetros de tráfico. El objetivo principal del control de tráfico es satisfacer requisitos del usuario tales como la calidad de servicio, al mismo que se asegura la utilización eficiente de la red.

A diferencia de la ingeniería de tráfico, el control de tráfico se lleva a cabo en una escala de tiempo corta. Por lo tanto, se dispone de un mecanismo bien establecido y automatizado para controlar el flujo de tráfico hacia el interior y hacia el exterior de la red.

En condiciones normales de funcionamiento, es decir cuando no se presentan fallos en la red, las funciones a que se hace referencia como de control de tráfico en esta Recomendación tienen por objeto evitar la congestión de la red.

No obstante, puede ocurrir congestión, por ejemplo debido a un mal funcionamiento de las funciones de control de tráfico provocado por fluctuaciones estadísticas impredecibles de los flujos de tráfico o de los fallos en la red. Por lo tanto, además de eso, las funciones a que se hace referencia como de control de congestión en esta Recomendación están destinadas a reaccionar a la congestión de red a fin de minimizar su intensidad, dispersión y duración.

El tratamiento de la sobrecarga se aplica sólo a los flujos de tráfico sin compromisos de QoS. Se refiere a un conjunto de funciones de la red que puede detectar y reducir la cantidad de sobrecarga.

7.1 Funciones de control de tráfico

Se identifican las siguientes funciones de control de tráfico:

- i) Gestión de recursos de red.
- ii) Control de admisión.
- iii) Control de parámetros.
- iv) Marcación de paquetes.
- v) Conformación de tráfico.
- vi) Calendarización de paquetes.

7.1.1 Gestión de recursos de red

La gestión de recursos de red se refiere a un conjunto de políticas y reglas para atribuir recursos de red tales como la anchura de banda y espacios de memoria intermedia en un conmutador o encaminador.

7.1.2 Control de admisión

El control de admisión se refiere a las políticas de la red para admitir compromisos de un nuevo flujo IP o para rechazar los compromisos cuando la demanda de recursos de red tales como la anchura de banda y espacios de memoria intermedia exceden la capacidad disponible en la red.

7.1.3 Control de parámetros

El control de parámetros es un conjunto de políticas que supervisa y controla que no se infrinja, por exceso, el contrato de tráfico.

7.1.4 Marcación de paquetes

Cuando se observa que un flujo IP no es conforme con uno o más aspectos del contrato de tráfico, los paquetes no conformes se pueden marcar modificando los bits pertinentes en el campo ToS/DS del encabezamiento IP.

7.1.5 Conformación de tráfico

La conformación de tráfico es una acción de la red para modificar las características de tráfico del flujo de manera que el flujo sea más adecuado para la red. Un ejemplo es la conformación de la velocidad de cresta de un flujo.

7.1.6 Calendarización de paquetes

La calendarización de paquetes es una función de la red con dos objetivos diferentes. Uno es vincular el retardo de cola para un flujo, el cual tiene requisitos de retardo rigurosos. El otro objetivo es dividir un recurso disponible (por ejemplo la anchura de banda) entre diferentes flujos de una manera específica para la red.

7.2 Funciones para el control de la congestión y el tratamiento de la sobrecarga

Se han identificado las siguientes funciones para el control de la congestión y el tratamiento de la sobrecarga.

- i) Control de descarte de paquetes.
- ii) Notificación de congestión explícita.

7.2.1 Control de descarte de paquetes

Se utiliza el control de descarte de paquetes para descartar el tráfico marcado en una situación de congestión. Otra aplicación del control de descarte de paquetes es, en una situación de congestión, descartar paquetes para los cuales no se aplican compromisos de QoS rigurosos.

7.2.2 Notificación de congestión explícita

La notificación de congestión explícita es un método facultativo con el cual la red puede informar al receptor acerca de la congestión existente en la red. El receptor puede utilizar esta información para ejecutar acciones apropiadas, por ejemplo informar al emisor a fin de que reduzca su velocidad de transmisión.

8 Métodos y herramientas para la ingeniería de tráfico IP

Queda en estudio.

Anexo A

El colector de testigos y el algoritmo genérico de velocidad de octetos (GBRA)

En este anexo se presentan varios algoritmos, los cuales se utilizan para definir la conformidad de los paquetes de un flujo IP con respecto a una velocidad R (en octetos por segundo) suponiendo un tamaño de colector B . Los algoritmos se consideran equivalentes en el sentido de que determinan que los mismos paquetes son conformes.

La medición del tráfico es un componente básico de las redes de paquetes que proporciona diversos niveles de calidad de servicio, tales como garantías de caudal y límites superiores de retardo y de pérdida. Un tren de paquetes IP tiene que ser conforme con un perfil de tráfico predefinido a fin de asegurar que los recursos de red atribuidos a ese tren puedan proporcionar el nivel de servicio esperado, y asegurar que el tren no provoca que otro tráfico de la red encuentre un nivel de servicio inaceptable.

El punto de inicio es el colector de testigos. Este algoritmo se considera equivalente al colector de testigos de estado continuo. A su vez se demuestra que este algoritmo es equivalente al algoritmo genérico de velocidad de octetos (GBRA, *generic byte rate algorithm*). El GBRA define las características que relacionan un parámetro de velocidad de información a un parámetro de tolerancia de ráfaga. Juntos, estos dos parámetros de tráfico y su interrelación forman la base para una prueba de conformidad de perfil de tráfico generalizada. Un objetivo secundario del GBRA es evitar la referencia a una o más opciones de implementación sobre la base de que no es central con respecto al concepto de conformidad y que es una fuente de propensión innecesaria. El GBRA especifica los aspectos fundamentales de una prueba de conformidad con un perfil único, y como tal no incluye otras funciones conexas de aplicación de políticas tales como las de medición multietapa, asignación de colores a los paquetes, marcación de paquetes, y descarte de paquetes.

A.1 El colector de testigos

Este algoritmo se describe como sigue (véase también por ejemplo RFC 2698):

El colector de testigos tiene dos parámetros fijos:

- La velocidad de colector de testigos R (en octetos por segundo).
- El tamaño de colector de testigos B (en octetos).

El colector de testigos utiliza la variable:

- La cuenta de testigos T_c (en octetos) la cual está completa inicialmente (a la llegada en el instante t_a del primer paquete del flujo), es decir, la cuenta de testigos $T_c(t_a) = B$.

De ahí en adelante, la cuenta de testigos T_c se aumenta en una unidad cada $1/R$ segundos hasta B .

Cuando llega un paquete de tamaño N octetos en el instante t_a , sucede lo siguiente:

- Si $T_c(t_a) - N < 0$, el paquete no es conforme, de lo contrario
- el paquete es conforme y T_c disminuye en N unidades.

NOTA – El tiempo o instante de llegada se considera aquel en que llega el último bit del paquete.

A.2 El colector de testigos de estado continuo

Para una mayor precisión y con el fin de evitar toda ambigüedad, se propone un colector de testigos de estado continuo que se considera equivalente al colector de testigos. El colector de testigos de estado continuo tiene la ventaja de ser fácilmente implementable.

El colector de testigos de estado continuo tiene dos parámetros fijos por cada flujo IP:

- La velocidad de colector de testigos R (en octetos por segundo) para el flujo.
- El tamaño de colector de testigos B (en octetos) para el flujo.

El colector de testigos de estado continuo utiliza las siguientes variables:

- La cuenta de testigos T_c (en octetos) del flujo.
- LCT es el último tiempo de conformidad del flujo (en segundos).

Inicialmente (en el instante t_a de la llegada del primer paquete del flujo):

- $T_c = B$
- $LCT = t_a$

A la llegada de un paquete con tamaño N (octetos) en el instante t_a :

$$Tc' = Tc + R \cdot (t_a - LCT)$$

Si $Tc' < N$

Entonces el paquete no es conforme

De lo contrario el paquete es conforme

$$Tc = \min(Tc', B) - N$$

Para el colector de testigos de estado continuo, las variables Tc y LCT sólo se modifican a la llegada del paquete.

NOTA – Un paquete nunca puede ser conforme si $N > B$.

A.3 El algoritmo genérico de velocidad de octetos

Existen dos variantes del algoritmo genérico de velocidad de octetos: una es el algoritmo de velocidad de octetos por calendarización virtual y la otra es el algoritmo de velocidad de octetos por colector con fugas de estado continuo.

Para ambos algoritmos, los parámetros fijos por cada flujo IP son:

- El incremento I en unidades de segundos por octeto. I está relacionado con R por $I = 1/R$
- El límite L en segundos. L está relacionado con R y B por $L = B/R$.

A.4 El algoritmo de velocidad de octetos por calendarización virtual

El algoritmo de velocidad de octetos por calendarización virtual utiliza la siguiente variable:

- TAT en unidades de segundos es el tiempo o instante de llegada teórico del paquete siguiente.

Inicialmente (en el instante t_a de la llegada del primer paquete del flujo):

- $TAT = t_a$

El tiempo de llegada teórico (TAT , *theoretical arrival time*) se actualiza solamente después de que el algoritmo determina que un paquete es conforme.

A la llegada de un paquete con tamaño N (octetos) en el instante t_a :

$$\text{Si } t_a < TAT + N \cdot I - L$$

Entonces el paquete no es conforme

De lo contrario el paquete es conforme

$$TAT = \max(t_a, TAT) + N \cdot I$$

A.5 El algoritmo de velocidad de octetos por colector con fugas de estado continuo

El algoritmo de velocidad de octetos por colector con fugas de estado continuo utiliza las siguientes variables:

- LCT es el último tiempo o instante de conformidad del flujo (en segundos).
- X es el contador de colector con fugas (en segundos).

Inicialmente (en el instante t_a de la llegada del primer paquete del flujo):

- $LCT = t_a$
- $X = 0$

A la llegada de un paquete con tamaño N (octetos) en el instante t_a :

$$X' = X - (t_a - LCT)$$

$$\text{Si } X' + N \cdot I > L$$

Entonces el paquete no es conforme

De lo contrario el paquete es conforme

$$X = \max(0, X') + N \cdot I$$

NOTA 1 – Equivalencia de los algoritmos:

- El algoritmo de velocidad de octetos por colector con fugas de estado continuo es equivalente al colector de testigos de estado continuo: simplemente se establece $T_c = (L - X) \cdot R$, $T_c' = (L - X') \cdot R$ y se utiliza $B = L \cdot R$.
- El algoritmo de velocidad de octetos por calendarización virtual es equivalente al algoritmo de velocidad de octetos por colector con fugas de estado continuo: simplemente se debe observar que después de que se han ejecutado los dos algoritmos, uno tiene $TAT = X + LCT$.

NOTA 2 – Relación entre el GBRA y el GCRA en la Rec. UIT-T I.371:

En el caso de ATM, el tamaño de célula es $N = 53$ octetos y $N \cdot I$ es igual a T que es el inverso de la velocidad de células. Si se establece $L = T + \tau$ donde τ es la tolerancia del GCRA, se observa que el GCRA es un caso especial del GBRA (véase el anexo A/I.371).

Anexo B

Comportamiento de dos algoritmos de velocidad de octetos genéricos coordinados

La definición de conformidad de la capacidad de transferencia anchura de banda estadística (SBW) se basa, además de en la prueba del tamaño máximo permitido de paquete, en dos ejemplares del algoritmo genérico de velocidad de octetos (GBRA) (véase el anexo A) donde los dos ejemplares funcionan en un modo coordinado. Modo coordinado significa que los estados del GBRA se actualizan si y solamente si una célula que llega es conforme con todos los ejemplares pertinentes del GBRA. Un paquete IP que pasa esta prueba es conforme cuando si al menos es conforme con el GBRA de cresta (R_p, B_p) y el GBRA sostenible (R_s, B_s).

En la figura B.1 se ilustra el comportamiento que resulta cuando dos ejemplares del GBRA funcionan en un modo coordinado.

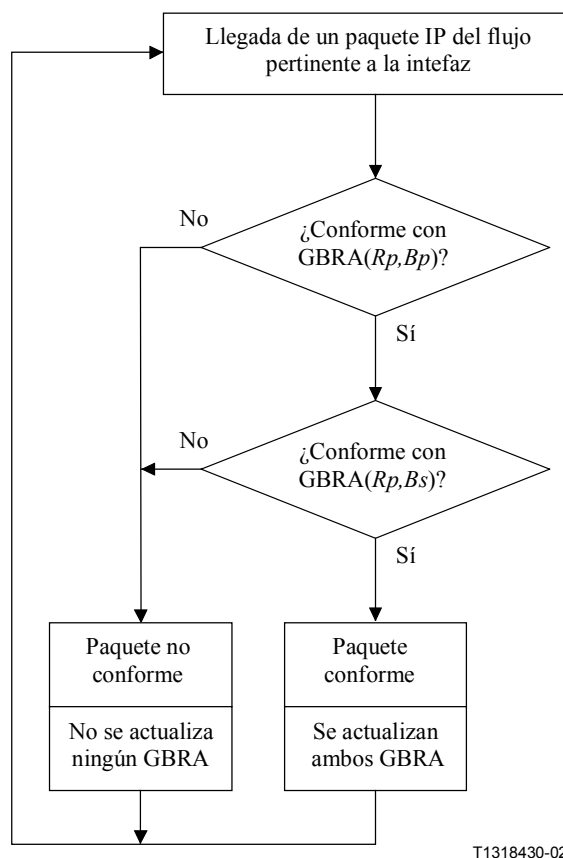


Figura B.1/Y.1221 – Comportamiento de dos algoritmos de velocidad de octetos genéricos coordinados

Apéndice I

Ilustración del comportamiento del colector de testigos

Introducción: Comportamiento del colector de testigos

Se puede utilizar una velocidad, expresada en octetos/s, para caracterizar parcialmente un flujo. El valor de la velocidad puede depender del periodo a lo largo del cual se efectúa la medición. Por ejemplo, una fuente que envía 50 octetos cada 1 ms es diferente de una fuente que envía 500 octetos cada 10 ms, aunque sus velocidades promedio a largo plazo son las mismas. Para permitir que se refleje esta diferencia se utiliza un colector de testigos (véase el anexo A) con una velocidad de colector R y un tamaño de colector B para caracterizar el flujo. En la práctica puede suceder que los flujos reales no muestren el mismo patrón recurrente como en los ejemplos anteriores. No obstante, el colector de testigos se puede utilizar para caracterizar el comportamiento de "caso más desfavorable" de todos los flujos posibles en los que todos los paquetes son conformes con un colector de testigos con determinados parámetros (R,B). Esto se describe e ilustra a continuación con mayor detalle.

I.1 Caracterización de un flujo con una sola velocidad y un solo tamaño colector de testigos

Se dice que un flujo está confinado o limitado por encima por un colector de testigos con velocidad R y un tamaño de colector de testigos B si todos los paquetes del flujo son conformes con el algoritmo de colector de testigos con velocidad de colector R y tamaño de colector B (véase el anexo A).

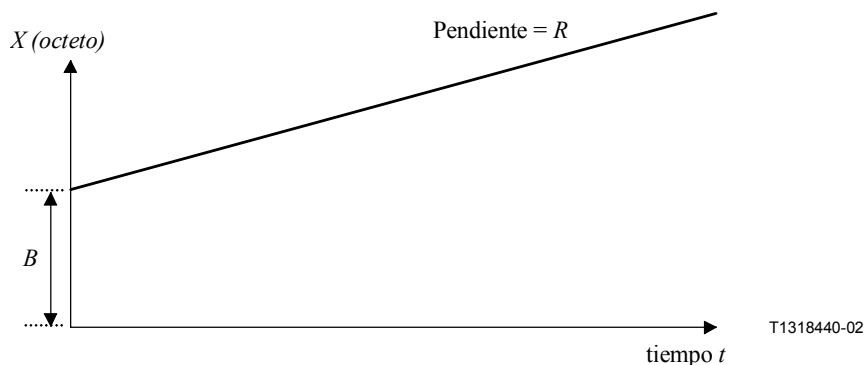


Figura I.1a/Y.1221 – Colector de testigos con una sola velocidad y un solo tamaño de colector – Flujo de "caso más desfavorable"

En la figura I.1a se muestra el comportamiento de un flujo para el caso teórico más desfavorable que es conforme con el algoritmo de colector de testigos con tamaño de colector de testigos B y velocidad R y donde la velocidad de línea se supone infinita. El eje horizontal representa el tiempo desde el primer paquete en ese flujo, y el eje vertical representa el número de octetos X que se podrían haber enviado como máximo en el flujo y que aún pueden pasar el colector de testigos hasta un instante t . Este flujo teórico de caso más desfavorable ha envidado una ráfaga de B octetos (a velocidad infinita) seguida por un flujo constante de paquetes de 1 octeto cada $1/R$ segundos. Obsérvese que en una red IP existente en la práctica, con un tamaño mínimo de paquete de más de 1 octeto, un flujo real no puede tener tal velocidad de paquetes. Se verifica fácilmente que éste es el comportamiento máximo permitido por el colector de testigos y, que se indica por la línea superior con pendiente igual a la velocidad de colector de testigos R (es decir, $X \leq B + t \times R$).

Otro flujo para el caso más desfavorable puede mostrar un patrón recurrente de B octetos (a velocidad infinita) a intervalos regulares de manera que la velocidad promedio a largo plazo sea igual a la velocidad de colector R . En la figura I.1b se indica la trayectoria de este flujo como una línea discontinua. En una red IP existente en la práctica, un flujo real puede realizar o aproximarse a ese comportamiento. Se puede verificar fácilmente que, para enviar la segunda ráfaga de B octetos, el flujo debe mostrar una actividad reducida (por ejemplo, estar en silencio) a fin de que se reabastezca una cantidad suficiente de testigos.

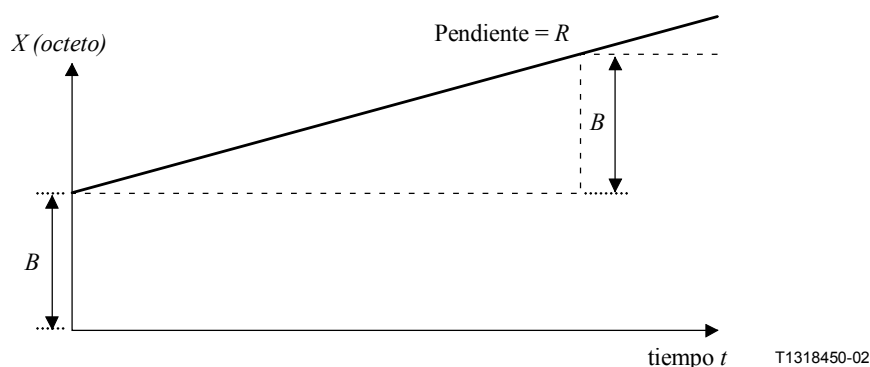


Figura I.1b/Y.1221 – Colector de testigos con una sola velocidad y un solo tamaño de colector – Flujo de "caso más desfavorable" en condiciones de ráfaga

En la figura I.1b se muestra además que la expresión $X \leq B + t \times R$ sigue siendo válida aunque no es en todo momento una representación exacta de la cantidad real de octetos enviados en este flujo.

En un tercer ejemplo se muestra un flujo que es menos activo durante algún tiempo y después adopta un comportamiento de "caso más desfavorable" similar al de los primeros dos ejemplos. Eso se ilustra en la figura I.1c.

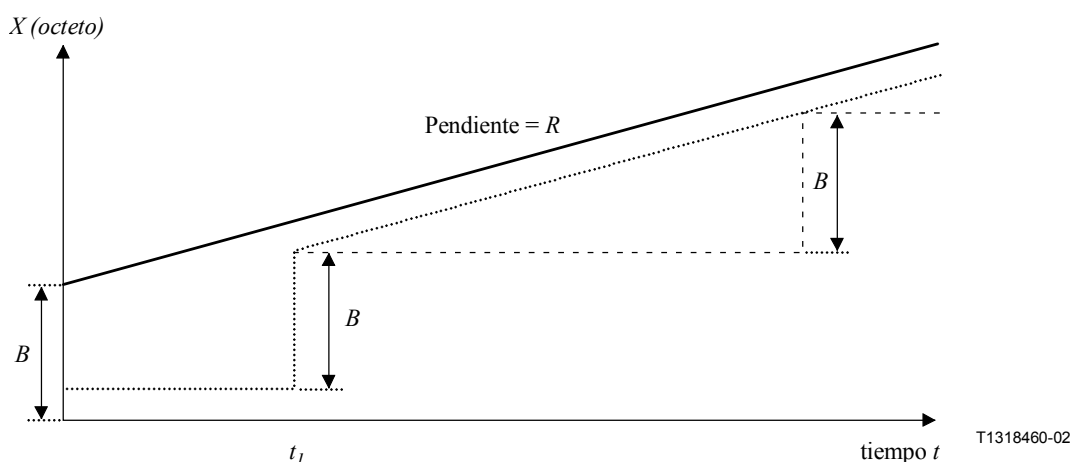


Figura I.1c/Y.1221 – Colector de testigos con una sola velocidad y un solo tamaño de colector – Flujos de "caso más desfavorable" después de un periodo de inactividad

El primer flujo para el caso teórico más desfavorable reanuda su máxima actividad en el instante t_1 . Debido a la modesta actividad en la etapa pre- t_1 , el colector de testigos se ha reabastecido totalmente a B octetos. Eso significa que, en el instante t_1 , el flujo está limitado a enviar una ráfaga de no más de B octetos (a velocidad infinita) y puede mostrar posteriormente el comportamiento de caso más desfavorable (sólo teóricamente posible) enviando paquetes de 1 octeto cada $1/R$ segundos. En la figura I.1c se ilustra la trayectoria de este flujo como una línea de puntos.

Un segundo flujo del caso más desfavorable, el cual reanuda su máxima actividad en el instante t_1 , muestra un patrón recurrente de B octetos (a velocidad infinita). Este flujo se encuentra también limitado por un tamaño de colector de testigos B y, cuando se han consumido todos los testigos, necesita esperar al menos B/R segundos antes de enviar los siguientes paquetes de tamaño B. La figura I.1c ilustra la trayectoria de este flujo como una línea discontinua.

Los flujos reales pueden mostrar muchas características diferentes, por ejemplo enviado paquetes de tamaños diferentes y transmitiendo a velocidades diferentes durante el tiempo de vida del flujo.

Es el algoritmo del colector de testigos quien, en cualquier momento, confina el flujo de dos maneras:

- confina el flujo a un tamaño de ráfaga (sin exceder B octetos), y
- confina el flujo a una velocidad (R octeto/s) medida durante un periodo suficientemente largo (sin exceder B/R s) e ignorando el tamaño de ráfaga permitido.

Dado un conjunto apropiado de parámetros de colector de testigos, la red puede basarse en estas características de flujo simplificadas para su atribución de recursos, en lugar de requerir que el originador del flujo especifique su flujo real (posiblemente muy complicado, y muy diverso) o las características fuente y tomarlas en cuenta. Para un flujo dado puede haber más de un conjunto de conjuntos de parámetros de colector de testigos (R, B) para caracterizar el flujo. Es responsabilidad de los usuarios seleccionar un conjunto de parámetros adecuado para su flujo.

NOTA – Se debe observar que, después de un periodo suficientemente largo de actividad reducida, la expresión $X \leq B + t \times R$ sigue siendo válida, aunque ya no es una representación exacta de la cantidad máxima de octetos que se puede enviar en el flujo.

I.2 Caracterización de un flujo con dos velocidades y dos colectores de testigos ($B_p < B_s$)

Cuando se definen dos velocidades para un flujo, se utilizan dos colectores de testigos. La mayor de las dos velocidades se designa como la velocidad de cresta (R_p), y la velocidad menor es la velocidad sostenible (R_s). Cuando el tamaño de colector de testigos para la velocidad de cresta es menor que el tamaño de colector de testigos para la velocidad sostenible (como es el caso para GS y CLS de IETF), la velocidad de cresta representa el caudal a corto plazo. La velocidad sostenible (R_s) representa el caudal a largo plazo.

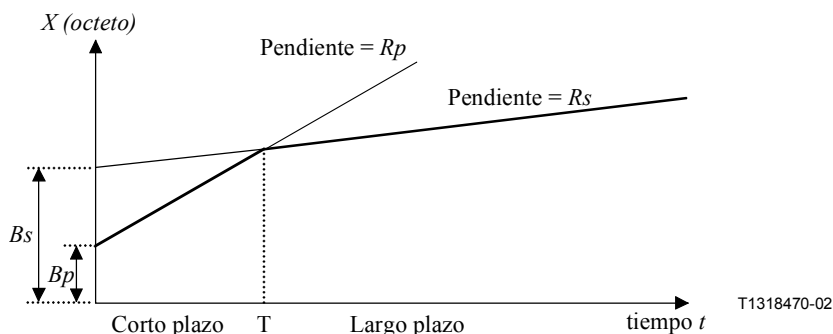


Figura I.2/Y.1221 – Dos colectores de testigos con dos velocidades ($B_p < B_s$) – Flujo de "caso más desfavorable"

En la figura I.2 se ilustra el comportamiento de un flujo de caso teórico más desfavorable que es conforme con dos colectores de testigos de los cuales uno tiene velocidad R_p con un tamaño de colector de testigos B_p y el otro tiene una velocidad R_s con un tamaño de colector de testigos B_s , y $B_p < B_s$. Se supone que la velocidad de la línea es infinita. El número X de octetos es la cantidad máxima de octetos que se podrían haber enviado en el flujo como una función del tiempo t desde la llegada del primer paquete y aún pasar ambos colectores de testigos. El número X se determina por las líneas cuyas pendientes son iguales a las velocidades del colector de testigos R_p y R_s . En los tiempos anteriores a T el colector de testigos con la velocidad más alta (es decir, R_p) rige el comportamiento del flujo de caso más desfavorable, mientras que en los tiempos posteriores a T el colector de testigos con la velocidad más baja (es decir, R_s) rige el comportamiento del flujo de caso más desfavorable. Estas regiones se indican como corto plazo y largo plazo en la figura I.2.

Las siguientes relaciones definen el valor máximo del número X en función del tiempo t y se indican con líneas gruesas en la figura I.2.

$$X \leq B_p + R_p \times t \quad (0 \leq t \leq T)$$

$$X < B_s + R_s \times t \quad (t \geq T)$$

En forma similar al caso descrito en I.1, se puede utilizar un conjunto apropiado de parámetros de colector de testigos para caracterizar mejor algunos flujos que los que serían posibles con un colector de testigos de una sola velocidad y la red puede basarse en estas características del flujo para la atribución de recursos.

NOTA – Al igual que en el caso descrito en I.1, se debe notar que, después de un periodo suficientemente largo de actividad reducida, las expresiones anteriores seguirán siendo válidas aunque ya no son una representación exacta de la cantidad máxima de octetos que se puede enviar en el flujo.

I.3 Caracterización de un flujo con dos velocidades y dos colectores de testigos ($B_p > B_s$)

Cuando se utilizan dos velocidades y el tamaño del colector de testigos para la velocidad de cresta es mayor que el tamaño del colector de testigos para la velocidad inferior (como sucede en Diffserv de IETF), las dos líneas de perfil que se muestran en la figura I.2 ya no se cruzan. El descriptor de tráfico incluye (R_p, B_p) y (R_s, B_s) y define un colector de testigos de velocidad comprometida $TB(R_s, B_s)$, en el cual R_s es la velocidad inferior, que representa el perfil de tráfico bajo el que la red garantiza la entrega de los paquetes. Los paquetes que son conformes con este TB son paquetes conformes. Esto es muy similar al caso de los paquetes conformes para la caracterización con una sola velocidad en I.1. Para facilitar el examen de este tema, estos paquetes conformes también se indican como paquetes "verdes".

El descriptor de tráfico también define un colector de testigos de cresta $TB(R_p, B_p)$, en el cual R_p es la velocidad superior que representa el perfil de tráfico por encima del cual la red no ofrece ninguna garantía de entrega. Esto permite distinguir asimismo entre paquetes que no son conformes con el TB sostenible.

Un paquete que no es conforme con el TB de velocidad de cresta se conoce por un paquete "rojo". Esto es muy similar al caso de un paquete no conforme en la caracterización con una sola velocidad en I.1, con un conjunto diferente de parámetros de colector de testigos.

Un paquete que no es conforme con el colector de velocidad inferior pero sí con el colector de velocidad de cresta se conoce por un paquete "amarillo". La red puede ofrecer diferentes "compromisos" a estos paquetes no conformes (es decir, a los paquetes amarillos y rojos). Por ejemplo, a los paquetes amarillos se les puede aplicar un compromiso menor que a los paquetes conformes (verdes) y un compromiso mejor que el que se aplica a los paquetes rojos. En la figura I.3 se ilustran las líneas con pendientes R_s y R_p , las cuales dividen el espacio en tres regiones, a saber:

$$X \leq B_s + R_s \times t \quad \rightarrow \text{región conforme (verde)}$$

$$X > B_p + R_p \times t \quad \rightarrow \text{región no conforme (rojo)}$$

$$B_s + R_s \times t < X \leq B_p + R_p \times t \quad \rightarrow \text{región no conforme (amarilla)}$$

NOTA – Se ha solicitado que se aclaren las razones para distinguir entre las dos regiones no conformes (amarilla y roja).

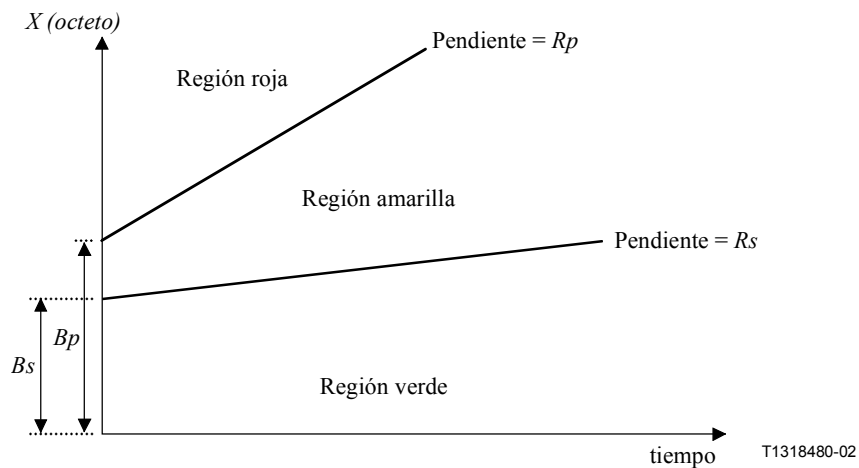


Figura I.3/Y.1221 – Dos velocidades, dos colectores de testigos ($B_p > B_s$) – flujo de "caso más desfavorable"

La descripción de las posibles características de un flujo de "caso más desfavorable" en esta configuración resulta más confusa.

Al igual que para los flujos de caso más desfavorable descritos en I.1, se puede describir también un flujo "verde de caso más desfavorable" en el cual todos los paquetes son conformes con $TB(R_s, B_s)$.

También se puede describir un flujo "amarillo de caso más desfavorable" en el cual todos los paquetes son conformes con el $TB(R_p, B_p)$. Obsérvese que un flujo "amarillo de caso más desfavorable" consiste no solamente en paquetes amarillos sino de una combinación de paquetes verdes y amarillos.

Finalmente, un flujo que no es conforme con $TB(R_p, B_p)$ consistirá en una combinación de paquetes rojos, amarillos y verdes, que dependerá de la severidad con la que se exceden los respectivos colectores de testigos.

Apéndice II

Relación entre especificaciones de clase de QoS e IntServ/DiffServ de IETF

En el cuerpo principal de esta Recomendación se describen dos capacidades de transferencia IP (véanse 6.1, 6.2) con las cuales se trata de alcanzar la compatibilidad con las descripciones y especificaciones de servicio generadas por los grupos IntServ y DiffServ de IETF. Se pretende que los elementos de red y las redes conformes con estas especificaciones sean probablemente aptos o adaptables para el soporte de las capacidades de transferencia IP especificadas en esta Recomendación.

En este apéndice informativo se indican las diferencias más importantes entre las capacidades de transferencia IP y sus homólogos en IETF, y se explican las razones por las que existen tales diferencias.

II.1 IPTC con anchura de banda dedicada asociada con una clase de QoS adecuada

La descripción de la capacidad de transferencia IP DBW (véase 6.1.1) incluye que la capacidad DBW intenta alcanzar la compatibilidad con el servicio garantizado (GS, *guaranteed service*) [RFC 2212] y los servicios extremo a extremo basados en el comportamiento por salto reenvío acelerado (EF-PHB, *expedited forwarding per-hop behavior*) [RFC 2598].

Dado que el UIT-T utiliza una combinación de una IPTC y una clase de QoS, en el texto a continuación se supone que se selecciona una clase de QoS con compromisos de pérdida especificados y compromisos de retardo (variación del retardo) especificados para un flujo dado. Un flujo caracterizado por la capacidad DBW en combinación con tal clase de QoS se designa en lo sucesivo por "DBW". De manera similar, a un flujo que utiliza el GS o un flujo que emplea EF-PHB se designan por "GS" y "EF" respectivamente.

La propiedad común entre DBW, GS y EF es que la red se compromete a transportar paquetes IP con una capacidad especificada [octetos/s] con poco retardo y con poca variación del retardo.

Se observan las siguientes diferencias:

- La capacidad DBW permite al proveedor de red descartar (posiblemente todos) los paquetes no conformes, en tanto que en GS y EF se espera que los paquetes no conformes se transporten sobre una base de mejor esfuerzo. Se espera que la aptitud para restringir el flujo entrante de paquetes DBW a la velocidad convenida y caracterizada por GBRA(R_p, B_p) simplifique considerablemente el control de tráfico en la red (por ejemplo prioridad de colas) y minimice los retardos en las colas para todo el tráfico conforme. Se espera además que la mayoría de las aplicaciones que utilicen DBW (por ejemplo los medios en flujo continuo) sean capaces de especificar parámetros adecuados y generar tráfico dentro de estos límites (paquetes conformes).
- La asociación con una clase de QoS permite que se den a conocer al usuario a priori (antes de acordar un contrato de tráfico) los compromisos extremo a extremo. El GS permite (por ejemplo mediante el protocolo RSVP) informar al usuario respecto al retardo máximo en cola que se espera encontrar en un determinado trayecto del flujo. Esta información se proporciona a posteriori (después de efectuada la reservación). Además, se ha demostrado que en un trayecto con muchos saltos la acumulación de valores de retardo máximo en cola por salto conduce a valores mucho mayores que el "retardo máximo" (o a un cuantil acumulado del mismo) encontrado en ese trayecto. En consecuencia, la información acumulada es de poco o ningún valor práctico para el usuario. EF no especifica un límite superior para el retardo (variación del retardo).
- La capacidad DBW aplica (además del tamaño máximo de paquete) la caracterización del tráfico mínimo con un conjunto único de parámetros de colector de testigos (R_p, B_p). GS requiere la especificación de un parámetro de velocidad de cresta adicional, pero sin la posibilidad de especificar una tolerancia a la variación del retardo de paquete de 1 punto relacionada con esa velocidad. Por otra parte, GS se invoca utilizando dos conjuntos de parámetros de tráfico (Tspec y Rspec, que pueden tener valores diferentes) más el denominado "término de relajación".

II.2 IPTC con anchura de banda estadística asociada con una clase de QoS adecuada

La descripción de la capacidad de transferencia IP SBW (véase 6.2.1) incluye que la capacidad SBW se esfuerza por alcanzar la compatibilidad con el servicio de elemento de red carga controlada (CL, *controlled-load network element service*) [RFC 2211] y los servicios extremo a extremo basados en el comportamiento por salto reenvío asegurado (AF-PHB, *assured forwarding per-hop behavior*) [RFC 2597].

Puesto que el UIT-T utiliza una combinación de una IPTC y una clase de QoS, en el texto siguiente se supone que una clase de QoS con compromisos de pérdida especificados y posiblemente compromisos de retardo (variación del retardo) no especificados se selecciona para un flujo dado. Un flujo caracterizado por la capacidad SBW en combinación con tal clase de QoS se designa en lo sucesivo por el "SBW". En forma similar, un flujo que utiliza la CL o un flujo que emplea el PHB/PSC de AF se designan por "CL" y "AF" respectivamente.

La propiedad común entre SBW, CL y AF es que la red se compromete a transportar los paquetes IP cuando menos con una capacidad especificada [octetos/s] y permite que se transporte tráfico adicional (en exceso) dentro de los límites de los recursos de red disponibles.

Se observan las siguientes diferencias:

- La capacidad SBW y el comportamiento AF están destinados a soportar aplicaciones que no tengan requisitos de retardo rigurosos. CL no se compromete a ofrecer propiedades de retardo cuantificadas sino que tiene como objetivo propiedades "en condiciones de ausencia de carga", es decir una variación de retardo que es pequeña en comparación con el retardo mínimo (por ejemplo retardo de propagación). Se prevé que esta propiedad será difícil de realizar en combinación con la aptitud para soportar eficientemente tráfico en exceso más allá y además de la velocidad garantizada.
- La capacidad SBW aplica (además del tamaño máximo de paquete) un doble conjunto de parámetros de colector de testigos (R_p, B_p) y (R_s, B_s). CL también requiere la especificación del parámetro velocidad de cresta, pero sin la posibilidad de especificar una tolerancia a la variación del retardo de paquete de 1 punto relacionada con esa velocidad. Además, CL se invoca utilizando dos conjuntos de parámetros de tráfico: Tspec y Rspec, los cuales pueden tener valores diferentes.
- Actualmente, la capacidad SBW distingue entre paquetes conformes y no conformes. AF distingue entre tres denominadas "precedencia de separación, pero debe soportar como mínimo dos probabilidades de separación diferentes.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación