

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.1540

(12/2019)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA
INFORMACIÓN, ASPECTOS DEL PROTOCOLO
INTERNET, REDES DE PRÓXIMA GENERACIÓN,
INTERNET DE LAS COSAS Y CIUDADES
INTELIGENTES

Aspectos del protocolo Internet – Calidad de servicio y
características de red

**Servicio de comunicación de datos con
protocolo Internet – Parámetros de calidad de
funcionamiento relativos a la disponibilidad y la
transferencia de paquetes del protocolo Internet**

Recomendación UIT-T Y.1540

RECOMENDACIONES UIT-T DE LA SERIE Y

**INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET,
REDES DE PRÓXIMA GENERACIÓN, INTERNET DE LAS COSAS Y CIUDADES INTELIGENTES**

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 gestión 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
Televisión IP sobre redes de próxima generación	Y.1900–Y.1999
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
Mejoras de las NGN	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Redes basadas en paquetes	Y.2600–Y.2699
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899
Entorno abierto con calidad de operador	Y.2900–Y.2999
REDES FUTURAS	Y.3000–Y.3499
COMPUTACIÓN EN LA NUBE	Y.3500–Y.3999
INTERNET DE LAS COSAS Y CIUDADES Y COMUNIDADES INTELIGENTES	
Generalidades	Y.4000–Y.4049
Definiciones y terminologías	Y.4050–Y.4099
Requisitos y casos de utilización	Y.4100–Y.4249
Infraestructura, conectividad y redes	Y.4250–Y.4399
Marcos, arquitecturas y protocolos	Y.4400–Y.4549
Servicios, aplicaciones, computación y proceso de datos	Y.4550–Y.4699
Gestión, control y calidad de funcionamiento	Y.4700–Y.4799
Identificación y seguridad	Y.4800–Y.4899
Evaluación y valoración	Y.4900–Y.4999

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

Recomendación UIT-T Y.1540

Servicio de comunicación de datos con protocolo Internet – Parámetros de calidad de funcionamiento relativos a la disponibilidad y la transferencia de paquetes del protocolo Internet

Resumen

La Recomendación UIT-T Y.1540 define los parámetros que se pueden utilizar para especificar y evaluar la calidad de funcionamiento en cuanto a velocidad, exactitud, seguridad de funcionamiento y disponibilidad de la transferencia de paquetes IP de los servicios de comunicación de datos regionales e internacionales con protocolo Internet (IP). Los parámetros definidos se aplican a un servicio IP de extremo a extremo, punto a punto, y a tramos de la red que proporcionan, o contribuyen, a la prestación de ese servicio de conformidad con las referencias normativas especificadas en la cláusula 2. El transporte sin conexión es un aspecto diferenciador del servicio IP que se considera en la presente Recomendación.

Tras más de 20 años de recorrido como Recomendación en vigor, la edición de 2019 recoge numerosos cambios en el diseño de los servicios IP y en los protocolos empleados por los usuarios finales. Esta edición incluye un nuevo Anexo A, en el que se definen los parámetros de capacidad de la capa IP de una forma propicia a su evaluación, y se detallan los requisitos aplicables a los métodos de medición de la capacidad de la capa IP. Este nuevo anexo es fruto de años de estudio y de la aplicación de los principios adoptados por la Comisión de Estudio 12 del UIT-T para evaluar con precisión los parámetros de calidad de funcionamiento y los métodos de medición con respecto a una referencia "real" en las mediciones de laboratorio y sobre el terreno. Los parámetros de caudal relacionados con el flujo y los métodos de medición conexos (transporte de entrega fiable) siguen siendo objeto de estudio y, en el texto, se hace una clara distinción entre los parámetros de capacidad de esta capa IP. Los parámetros que describen la calidad de funcionamiento de un protocolo específico de la capa de transporte fiable (TCP) también se hallan en fase de estudio y se reconoce que los protocolos de transporte fiable para Internet cambian constantemente y están siempre en el punto de mira de la investigación.

En el Anexo B se presenta un segundo algoritmo de búsqueda más capaz para el método de medición de la capacidad de la capa IP definido en el Anexo A.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T I.380	26-02-1999	13	11.1002/1000/4573
1.0	UIT-T Y.1540	26-02-1999	13	11.1002/1000/5302
2.0	UIT-T Y.1540	14-12-2002	13	11.1002/1000/6189
2.1	UIT-T Y.1540 (2002) Enm. 1	01-08-2003	13	11.1002/1000/6975
3.0	UIT-T Y.1540	13-11-2007	12	11.1002/1000/9270
3.1	UIT-T Y.1540 (2007) Enm.1	19-03-2009	12	11.1002/1000/9727
4.0	UIT-T Y.1540	01-03-2011	12	11.1002/1000/11079
4.1	UIT-T Y.1540 (2011) Enm.1	21-01-2016	12	11.1002/1000/12761
5.0	UIT-T Y.1540	29-07-2016	12	11.1002/1000/12975
6.0	UIT-T Y.1540	05-12-2019	12	11.1002/1000/13933
6.1	UIT-T Y.1540 (2019) Enm. 1	06-02-2020	12	11.1002/1000/14161

* Para acceder a la Recomendación, sírvase digitar el URL <http://handle.itu.int/> en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, <http://handle.itu.int/11.1002/1000/11830-en>.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) 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.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

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 la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en <http://www.itu.int/ITU-T/ipr/>.

© UIT 2022

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	4
3 Abreviaturas y acrónimos	4
4 Modelo estratificado por capas de calidad de funcionamiento de servicio IP.....	6
5 Modelo de calidad de funcionamiento de servicio IP genérico.....	7
5.1 Componentes de red	8
5.2 Enlaces de central y secciones de red.....	9
5.3 Puntos de medición y secciones medibles.....	10
5.4 Eventos de referencia de transferencia de paquetes IP (IPRE)	11
5.5 Resultados de la transferencia de paquetes IP.....	12
6 Parámetros de calidad de funcionamiento de la transferencia de paquetes IP	18
6.1 Calificaciones de los paquetes.....	19
6.2 Retardo de transferencia de paquetes IP.....	19
6.3 Tasa de errores en los paquetes IP (IPER)	22
6.4 Tasa de pérdida de paquetes IP (IPLR)	22
6.5 Tasa de paquetes IP espurios	23
6.6 Tasa de reordenación de paquetes IP (IPRR)	23
6.7 Tasa de bloques con pérdidas severas de paquetes IP (IPSLBR).....	24
6.8 Tasa de duplicación de paquetes IP (IPDR)	24
6.9 Tasa de paquetes IP replicados (RIPR)	24
6.10 Parámetros de reparación de trenes	24
6.11 Parámetros de capacidad	24
6.12 Parámetros relacionados con el flujo.....	27
7 Disponibilidad de servicio IP.....	28
7.1 Función de disponibilidad de servicio IP	28
7.2 Parámetros de disponibilidad de servicio IP	30
Anexo A – Parámetros de capacidad y relacionados con el flujo basados en IP y métodos de medición.....	31
A.1 Antecedentes.....	31
A.2 Parámetros de capacidad de acceso de la capa IP y métodos de medición (acceso de los consumidores a Internet).....	32
A.3 Parámetros de caudal relacionados con el flujo y los métodos de medición conexos (transporte de entrega fiable).....	36
A.4 Plan para calificar y comparar los métodos de medición del acceso	36
Anexo B – Algoritmo adicional de búsqueda de parámetros de capacidad basados en IP y métodos de medición	41
B.1 Algoritmo de búsqueda.....	41
Apéndice I – Consideraciones relativas al encaminamiento de paquetes IP	46

	Página
Apéndice II – Terminología secundaria aplicable a la variación del retardo de paquetes IP ..	47
II.1 Introducción.....	47
II.2 Definición de variación del retardo entre paquetes	47
II.3 Definición de la variación del retardo de paquetes de 1 punto.....	48
II.4 Directrices para la aplicación de los diferentes parámetros	48
Apéndice III – Parámetros relacionados con la velocidad y la capacidad de caudal.....	50
Apéndice IV – Pruebas del estado de disponibilidad del servicio IP y estimación por muestreo de los parámetros de disponibilidad del servicio IP.....	51
IV.1 Prueba mínima del estado de disponibilidad del servicio IP (para metodologías de prueba y aparatos de prueba).....	51
IV.2 Prueba del estado de disponibilidad del servicio IP (mediante la prueba de relación de probabilidad secuencial)	51
IV.3 Prueba alternativa de significación estadística para determinar la disponibilidad del servicio IP	53
IV.4 Estimación por muestreo de la disponibilidad del servicio IP	54
Apéndice V – Material pertinente para los métodos de medición de la calidad de funcionamiento IP.....	55
Apéndice VI – Fundamentos de la disponibilidad de servicio IP.....	56
VI.1 Introducción.....	56
VI.2 Antecedentes.....	56
VI.3 Definiciones de las regiones de la Figura VI.1.....	56
VI.4 Resumen	57
Apéndice VII – Parámetros de calidad de funcionamiento de los paquetes a efectos de la optimización de las técnicas para la reparación de trenes	58
VII.1 Introducción.....	58
VII.2 Breve descripción de las técnicas de reparación de trenes en la capa de aplicaciones	59
VII.3 Modelo simple de técnicas de reparación de trenes en la capa de aplicaciones	60
VII.4 Ejemplo de parámetros de calidad de funcionamiento para caracterizar las variables de reparación de trenes.....	60
VII.5 Análisis de la medición y el uso de los parámetros.....	60
VII.6 Consideraciones adicionales.....	61
Apéndice VIII – Marco de capacidad de la capa IP.....	63
VIII.1 Introducción.....	63
VIII.2 Terminología y relación con IETF RFC 5136.....	63
VIII.3 Asuntos que quedan en estudio	64
Apéndice IX – Explicación de la inadecuación de la medición basada en TCP para cumplir los requisitos normativos.....	65
IX.1 Introducción.....	65
IX.2 Comparación con los requisitos normativos.....	65

Apéndice X – Resumen de los resultados de laboratorio (fase 1) y de campo (fase 2):	
plan de evaluación del Anexo A.....	67
X.1 Introducción.....	67
X.2 Configuración de las pruebas de laboratorio de la fase 1	67
X.3 Configuración detallada de las pruebas	68
X.4 Herramientas de pruebas	69
X.5 Calibración de los resultados comunicados con iPerf 2	70
X.6 Resumen del enfoque y los resultados de las pruebas.....	70
X.7 Resumen de las pruebas en que se compara la capacidad medida con las velocidades PHY calibradas	71
X.8 Resumen de las pruebas que comparan la capacidad medida con el retardo de ida y vuelta	71
X.9 Resumen de las pruebas con tráfico en competencia	72
X.10 Pruebas con la implantación temprana de una nueva herramienta de pruebas UDP.....	75
X.11 Pruebas de los efectos de la pérdida de paquetes de bajo nivel.....	75
X.12 Examen de las limitaciones máximas de transmisión de las herramientas de pruebas y de la plataforma.....	76
X.13 Examen de las pruebas con degradaciones tempranas en los trenes UDP	77
X.14 Examen de los parámetros del conformador TBF utilizados en las pruebas y comparación con el filtro regulador	77
X.15 Resumen de las pruebas de laboratorio de la fase 1	77
X.16 Especificaciones de la plataforma	78
X.17 Resumen de los resultados de las pruebas de campo de la fase 2	78
Apéndice XI – Breve estudio sobre la investigación de la QoS y la QoE relacionadas con el acceso a Internet.....	79
XI.1 Introducción.....	79
XI.2 Principales conclusiones.....	79
XI.3 Análisis de las publicaciones científicas relacionadas con las mediciones de la QoS y la QoE	81
XI.4 Tendencias generales relacionadas con la calidad de funcionamiento del acceso a Internet	85
Apéndice XII – Mediciones exactas de la velocidad binaria	87
XII.1 Introducción.....	87
XII.2 Principales conclusiones.....	87
XII.3 Estimación del error de medición del ancho de banda provocado por la longitud del encabezamiento	88
XII.4 Ejemplo de cálculo de tara para una interfaz Ethernet IEEE 802.3 alámbrica	90
XII.5 Descripción de la funcionalidad del filtro del colector de testigos.....	91
Apéndice XIII – Parámetros relacionados con el flujo basados en IP y métodos de medición	92

	Página
XIII.1 Antecedentes.....	92
XIII.2 Por qué la MBM cumple los requisitos de esta Recomendación	92
XIII.3 Función y situación del método de medición MBM	93
XIII.4 Selección del tren de pruebas	93
XIII.5 Puntos de medición.....	94
XIII.6 Especificación de los parámetros del modelo objetivo	95
XIII.7 Establecimiento de criterios de aceptación e interpretación de los resultados.....	95
XIII.8 Métodos de prueba	95
XIII.9 Ejemplo(s)	95
Bibliografía	96

Recomendación UIT-T Y.1540

Servicio de comunicación de datos con protocolo Internet – Parámetros de calidad de funcionamiento relativos a la disponibilidad y la transferencia de paquetes del protocolo Internet

1 Alcance

La presente Recomendación define los parámetros que se pueden utilizar para especificar y evaluar la calidad de funcionamiento en cuanto a velocidad, exactitud, seguridad de funcionamiento y disponibilidad de la transferencia de paquetes IP de los servicios de comunicación de datos regionales e internacionales con protocolo Internet (IP). Los parámetros definidos se aplican al servicio IP de extremo a extremo, punto a punto, y a tramos de la red que proporcionan, o contribuyen, a la prestación de ese servicio de conformidad con las referencias normativas especificadas en la cláusula 2. El transporte sin conexión es un aspecto diferenciador del servicio IP que se considera en la presente Recomendación.

En esta Recomendación, el servicio IP de extremo a extremo se refiere a la transferencia de datagramas IP generados por el usuario (designados como paquetes IP en esta Recomendación) entre dos computadores principales de extremo especificados por sus direcciones IP completas. Esto difiere de los límites implícitos en la expresión "de extremo a extremo" en otras Recomendaciones. Por ejemplo, en [UIT-T P.10] se define la calidad de extremo a extremo como aquella relacionada con las características de un sistema de comunicación, incluidos todos los equipos terminales. Para servicios vocales la calidad de extremo a extremo es equivalente a la calidad boca-oído.

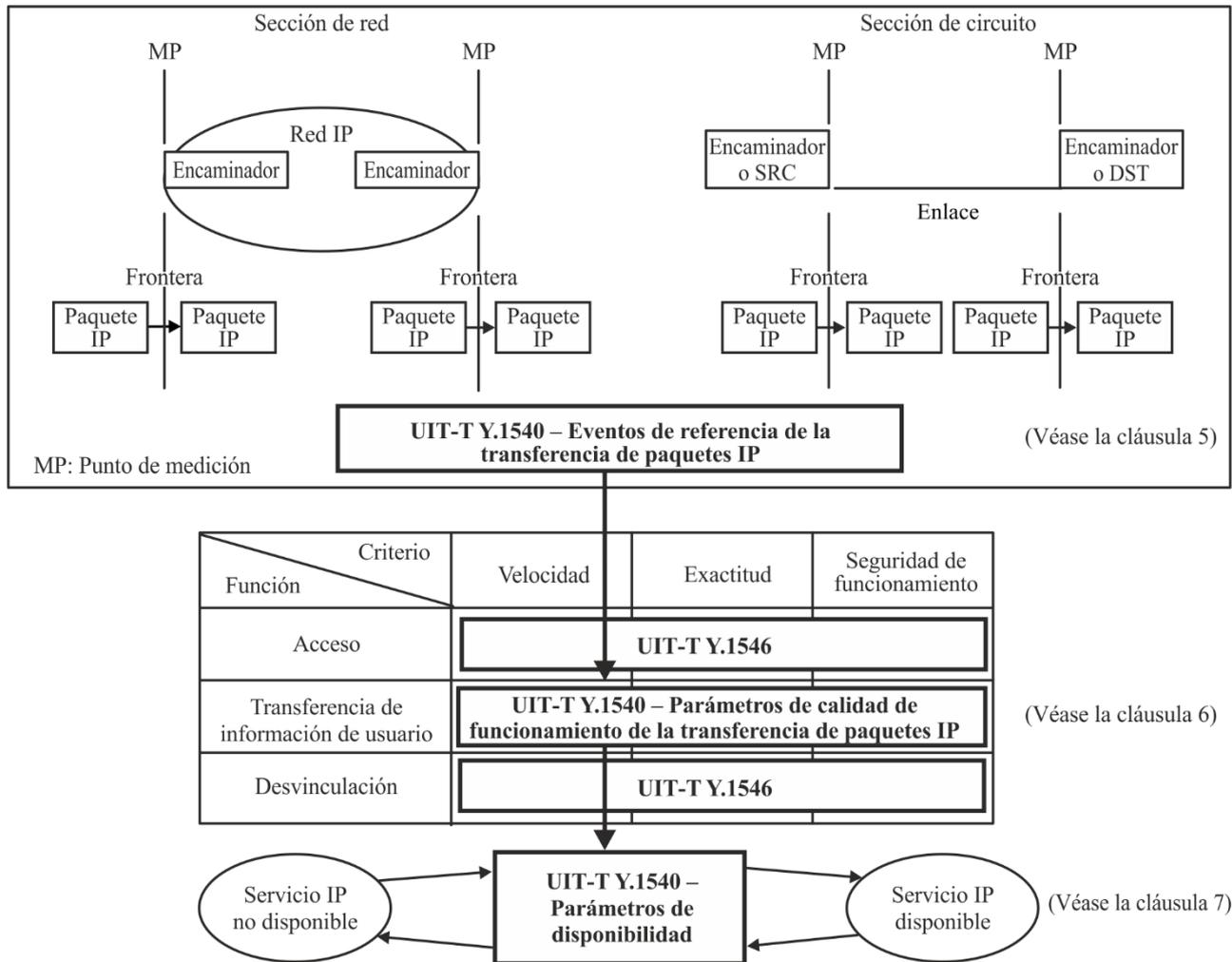
NOTA 1 – La presente Recomendación define los parámetros que se pueden utilizar para caracterizar el IP proporcionado utilizando la versión 4 del protocolo Internet (Ipv4) y la versión 6 del protocolo Internet (Ipv6); la aplicabilidad o la ampliación de esta Recomendación a otros protocolos (por ejemplo, el protocolo de reserva de recursos) queda en estudio.

NOTA 2 – Las Recomendaciones relativas a la calidad de funcionamiento del servicio IP punto a multipunto están actualmente en elaboración.

La utilización prevista de los parámetros de calidad de funcionamiento y los métodos de medición [UIT-T Y.1540] (cuando se especifican) es la planificación y la oferta de servicios IP regionales e internacionales. Entre los usuarios a los que va dirigida la presente Recomendación figuran los proveedores de servicios IP, los fabricantes de equipos, los usuarios finales (abonados a los servicios de PI) y otras partes interesadas en realizar evaluaciones y/o supervisar los servicios de PI. Esta Recomendación puede ser utilizada por los proveedores de servicios para planificar, desarrollar y estimar servicios IP que satisfagan las necesidades de los usuarios en materia de calidad de funcionamiento; por los fabricantes de equipos como fuente de información sobre esa calidad de funcionamiento que influirá en el diseño de los equipos; y por los usuarios finales para evaluar la calidad del servicio IP.

En la Figura 1 se muestra de manera resumida el alcance de esta Recomendación. Los parámetros de calidad de funcionamiento del servicio IP se definen sobre la base de eventos de referencia de transferencia de paquetes IP (IPRE, *IP packet transfer reference events*) que se pueden observar en puntos de medición (MP, *measurement points*) asociados con fronteras funcionales y jurisdiccionales. A efectos de comparabilidad y exhaustividad, la calidad del servicio IP se considera en el contexto de la matriz de calidad de funcionamiento de 3×3 definida en [UIT-T I.350]. En dicha matriz se identifican tres funciones de comunicación independientes del protocolo: acceso, transferencia de información de usuario y desvinculación. Cada función se considera con respecto a tres aspectos del funcionamiento en general (o "criterios de calidad de funcionamiento"): velocidad, exactitud y seguridad de funcionamiento. Un modelo de dos etapas asociado proporciona la base para la descripción de la disponibilidad del servicio IP.

NOTA 3 – En esta Recomendación, la función de transferencia de información de usuario ilustrada en la Figura 1 se refiere al intento de transferir cualquier paquete IP, con independencia de su tipo o contenido.



Y.1540(11)_F01

Figura 1 – Alcance de esta Recomendación

Los parámetros de calidad de funcionamiento definidos en esta Recomendación describen la velocidad, exactitud, seguridad de funcionamiento y disponibilidad de la transferencia de paquetes IP que proporciona el servicio de comunicación de datos IP. La calidad de funcionamiento de extremo a extremo de los servicios IP regionales e internacionales que proporcionan las funciones de acceso y desvinculación (por ejemplo, el servicio de nombre de dominio) y las capacidades de transporte de capas superiores (por ejemplo, el protocolo de control de la transmisión) se han tratado en Recomendaciones aparte, como el Anexo C de [UIT-T Y.1546] para la disponibilidad de servicios basados en IP.

Esta Recomendación está estructurada como sigue: la cláusula 1 especifica su alcance; la cláusula 2 especifica sus referencias normativas; la cláusula 3 contiene una lista de abreviaturas; la cláusula 4 ilustra el modelo estratificado por capas que crea el contexto para la especificación de la calidad de funcionamiento IP; la cláusula 5 define el modelo utilizado de calidad de funcionamiento IP, incluyendo secciones de red y puntos de medición, eventos de referencia y resultados; la cláusula 6 utiliza este modelo para definir los parámetros de calidad de funcionamiento de la transferencia de paquetes IP; y la cláusula 7 define a continuación los parámetros de disponibilidad del servicio IP.

En el Anexo A se definen los parámetros de capacidad de la capa PI de una forma propicia a su evaluación y se describen los requisitos para los métodos de medición, junto con un plan para evaluar los posibles métodos de medición en el laboratorio y en las redes de producción (de campo) (nuevo en la versión de 2019). En el Apéndice I se hacen algunas consideraciones relativas al encaminamiento de paquetes IP y sus efectos en la calidad de funcionamiento. El Apéndice II contiene una serie de terminología secundaria aplicable a la variación del retardo de los paquetes IP. El Apéndice III (parámetros relacionados con la velocidad y la capacidad de caudal) queda obsoleto en la edición de 2019. El Apéndice IV describe la estimación de la disponibilidad del servicio IP. En el Apéndice V se hacen algunas consideraciones respecto de la medición de los parámetros [UIT-T Y.1540]. El Apéndice VI aporta cierta información sobre los fundamentos de la disponibilidad del servicio IP. El Apéndice VII ofrece información general sobre los parámetros de reparación de trenes, y el Apéndice VIII añade información sobre los parámetros de capacidad (en particular, una correspondencia con métricas anteriores del IETF y elementos para un estudio posterior). En el Apéndice IX se explica por qué las mediciones basadas en TCP no cumplen los requisitos normativos de la cláusula 6.12.

En la versión de 2019 se añaden muchos apéndices nuevos. Uno de ellos, el Apéndice X, proporciona material básico sustancial en el que se sustentan los parámetros de capacidad IP y los métodos de medición, incluido un resumen de los resultados de las pruebas de laboratorio y de campo que comparan diferentes métodos de medición. El Apéndice XI contiene un estudio de documentos académicos que describen campañas de medición en las que se realizan comparaciones similares. En el Apéndice XII se detallan los cálculos necesarios para realizar mediciones y comparaciones exactas de la velocidad binaria en las diferentes capas de la pila del protocolo. En el Apéndice XIII se aporta información sobre los parámetros y métodos de medición relacionados con el flujo IP, que queda en estudio, y se indica la función complementaria con respecto a las métricas de capacidad IP y los métodos de medición.

NOTA 4 – Los parámetros UIT-T Y.1540 se podrán aumentar o modificar en función de ulteriores estudios de los requisitos de las aplicaciones IP (por ejemplo, interactivas, de bloques, de trenes) que se han de soportar.

NOTA 5 – Los parámetros UIT-T Y.1540 de velocidad, exactitud y seguridad de funcionamiento tienen por objeto caracterizar el servicio IP en el estado de disponibilidad.

NOTA 6 – Los parámetros definidos en esta Recomendación se pueden aplicar a un único servicio IP de extremo a extremo entre dos computadores principales de extremo identificados por sus direcciones IP. Los parámetros se pueden aplicar también a los paquetes IP de un determinado servicio IP de extremo a extremo ofrecidos a una determinada sección de red o enlace de central (EL).

NOTA 7 – Los parámetros UIT-T Y.1540 se han concebido para caracterizar la calidad de servicio proporcionada por elementos de red entre fronteras de secciones especificadas. Sin embargo, los usuarios de esta Recomendación deberán ser conscientes de que los elementos de red situados fuera de las fronteras especificadas pueden influir a veces en la calidad de funcionamiento medida de los elementos que se hallan entre esas fronteras. En el Apéndice V se describen ejemplos al respecto.

NOTA 8 – Los parámetros definidos en esta Recomendación se pueden aplicar también a cualquier subconjunto de los paquetes IP ofrecidos a un determinado conjunto de equipos de red. Los métodos de cómputo de la calidad de funcionamiento en un conjunto de equipos de red o en una red completa quedan fuera del alcance de esta Recomendación.

NOTA 9 – Esta Recomendación no proporciona las herramientas para caracterizar de manera explícita la estabilidad del encaminamiento. Sin embargo, los efectos de la inestabilidad de la ruta se pueden cuantificar utilizando los parámetros de pérdida, retardo y pérdida severa definidos en esta Recomendación.

NOTA 10 – La especificación de objetivos numéricos de calidad de funcionamiento para algunos o la totalidad de los parámetros de calidad de funcionamiento UIT-T Y.1540 se puede consultar en [UIT-T Y.1541].

NOTA 11 – En esta Recomendación, la palabra "provisional" se utiliza en el sentido de que hay un acuerdo sobre la estabilidad del valor al que se hace referencia, pero que dicho valor puede modificarse a raíz de un nuevo estudio o según la experiencia de funcionamiento que se obtenga de las redes reales.

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. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

- [UIT-T I.350] Recomendación UIT-T I.350 (1993), *Aspectos generales de calidad de servicio y de calidad de funcionamiento en las redes digitales incluidas las redes digitales de servicios integrados*.
- [UIT-T P.10] Recomendación UIT-T P.10/G.100 (2017), *Vocabulario sobre calidad de funcionamiento, calidad de servicio y calidad de la experiencia*.
- [UIT-T Y.1541] Recomendación UIT-T Y.1541 (2011), *Objetivos de calidad de funcionamiento de red para servicios basados en el protocolo Internet*.
- [UIT-T Y.1546] Recomendación UIT-T Y.1546 (2014), *Rendimiento de traspaso entre redes de acceso múltiple*.
- [UIT-T Y.1565] Recomendación UIT-T Y.1565 (2011), *Parámetros de calidad de funcionamiento de las redes domésticas*.
- [IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.
<<http://www.ietf.org/rfc/rfc791.txt>>
- [IETF RFC 4737] IETF RFC 4737 (2006), *Packet Reordering Metrics*.
<<http://www.ietf.org/rfc/rfc4737.txt>>
- [IETF RFC 5136] IETF RFC 5136 (2008), *Defining Network Capacity*.
<<http://www.ietf.org/rfc/rfc5136.txt>>
- [IETF RFC 5481] IETF RFC 5481 (2009), *Packet Delay Variation Applicability Statement*.
<<http://www.ietf.org/rfc/rfc5481.txt>>
- [IETF RFC 8200] IETF RFC 8200 (2017), *Internet Protocol, Version 6 (IPv6) Specification*.
<<http://www.ietf.org/rfc/rfc8200.txt>>
- [IETF RFC 8337] IETF RFC 8337 (2018), *Model-Based Metrics for Bulk Transport Capacity*.
<<http://www.ietf.org/rfc/rfc8337.txt>>

3 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

ARQ	Petición automática de repetición (<i>automatic repeat-request</i>)
ATM	Modo de transferencia asíncrono (<i>asynchronous transfer mode</i>)
BTC	Capacidad de transferencia en bloque (<i>bulk transfer capacity</i>)
DSCP	Punto de código de servicio diferenciado (<i>differentiated services code-point</i>)
DST	Computador principal de destino (<i>destination host</i>)
EL	Enlace de central (<i>exchange link</i>)
ER	Encaminador de borde (<i>edge router</i>)
FEC	Corrección de errores en recepción (<i>forward error correction</i>)
FTP	Protocolo de transferencia de ficheros (<i>file transfer protocol</i>)

HTTP	Protocolo de transferencia de hipertexto (<i>hypertext transfer protocol</i>)
IP	Protocolo de Internet (<i>Internet protocol</i>)
IPDR	Tasa de duplicación de paquetes del protocolo Internet (<i>Internet protocol packet duplicate ratio</i>)
IPDV	Variación del retardo de los paquetes del protocolo Internet (<i>Internet protocol packet delay variation</i>)
IPER	Tasa de errores en los paquetes del protocolo Internet (<i>Internet protocol packet error ratio</i>)
IPIBR	Tasa de bloques degradados en los paquetes del protocolo Internet (<i>Internet protocol packet impaired block ratio</i>)
IPIIR	Tasa de intervalos con errores en los paquetes del protocolo Internet (<i>Internet protocol packet impaired block ratio</i>)
IPLR	Tasa de pérdida de paquetes del protocolo Internet (<i>Internet protocol packet loss ratio</i>)
IPOR	Tasa de paquetes IP basada en octetos
IPPM	Métricas de la calidad de funcionamiento IP (<i>IP performance metrics</i>)
IPPR	Tasa de paquetes del protocolo Internet (<i>Internet protocol packet rate</i>)
IPRE	Evento de referencia de transferencia de paquetes del protocolo Internet (<i>Internet protocol packet transfer reference event</i>)
IPRR	Tasa de reordenación de paquetes del Protocolo Internet (<i>Internet protocol packet reordered ratio</i>)
IPSLB	Resultado de bloques con pérdidas severas de paquetes del protocolo Internet (<i>Internet protocol packet severe loss block outcome</i>)
IPSLBR	Tasa de bloques con pérdidas severas de paquetes del protocolo Internet (<i>Internet protocol packet severe loss block ratio</i>)
IPTD	Retardo de transferencia de paquetes del protocolo Internet (<i>Internet protocol packet transfer delay</i>)
IPv4	Versión 4 del protocolo Internet
IPv6	Versión 6 del protocolo Internet
ISP	Proveedor de servicios de Internet (<i>Internet service provider</i>)
LL	Capas inferiores, protocolos y tecnología que soportan la capa del protocolo Internet (<i>lower layers</i>)
M _{av}	Número mínimo de paquetes recomendado para evaluar el estado de disponibilidad (<i>the minimum number of packets recommended for assessing the availability state</i>)
MBM	Métricas basadas en modelos (<i>model-based metrics</i>)
MP	Punto de medición (<i>measurement point</i>)
MTBISO	Tiempo medio entre interrupciones del servicio IP (<i>mean time between IP service outages</i>)
MTTISR	Tiempo medio de restablecimiento del servicio del protocolo Internet (<i>mean time to Internet protocol service restoral</i>)
N	Número de paquetes en una sonda de caudal de tamaño N
NS	Sección de red (<i>network section</i>)

NSE	Conjunto de secciones de red (<i>network section ensemble</i>)
NSP	Proveedor de servicio de red (<i>network service provider</i>)
PDH	Jerarquía digital plesiócrona (<i>plesiochronous digital hierarchy</i>)
PDV	Variación del retardo de paquetes (<i>packet delay variation</i>)
PIA	Porcentaje de disponibilidad de servicio del protocolo Internet (<i>percent Internet protocol service availability</i>)
PIU	Porcentaje de indisponibilidad de servicio del protocolo Internet (<i>percent Internet protocol service unavailability</i>)
QoS	Calidad de servicio (<i>quality of service</i>)
R	Encaminador (<i>router</i>)
RIPR	Tasa de paquetes del protocolo Internet replicados (<i>replicated Internet Protocol packet ratio</i>)
RSVP	Protocolo de reserva de recursos (<i>resource reservation protocol</i>)
RTCP	Protocolo de control en tiempo real (<i>real-time control protocol</i>)
RTO	Temporización de retransmisión (<i>retransmission time-out</i>)
RTP	Protocolo de transporte en tiempo real (<i>real-time transport protocol</i>)
RTT	Tiempo de ida y vuelta (<i>round-trip time</i>)
SDH	Jerarquía digital síncrona (<i>synchronous digital hierarchy</i>)
SPRT	Prueba de relación de probabilidad secuencial (<i>sequential probability ratio test</i>)
SRC	Computador principal de origen (<i>source host</i>)
STD	Norma (<i>standard</i>)
T _{av}	Duración mínima del tiempo de disponibilidad del protocolo Internet; duración mínima del tiempo de indisponibilidad del protocolo Internet (<i>minimum length of time of Internet protocol availability; minimum length of time of Internet protocol unavailability</i>)
TBF	Filtro del colector de testigos
TCP	Protocolo de control de transmisión
T _{max}	Retardo máximo de paquete del protocolo Internet a partir del cual se considera que el paquete se ha perdido (<i>maximum Internet protocol packet delay beyond which the packet is declared to be lost</i>)
ToS	Tipo de servicio (<i>type of service</i>)
T _s	Duración que define el bloque en el resultado de bloques con pérdidas severas (<i>length of time defining the block in the severe loss block outcome</i>)
TTL	Tiempo de vida (<i>time to live</i>)
UDP	Protocolo de datagrama de usuario (<i>user datagram protocol</i>)

4 Modelo estratificado por capas de calidad de funcionamiento de servicio IP

La Figura 2 ilustra la naturaleza estratificada por capas de la calidad de funcionamiento de un servicio IP. La calidad de funcionamiento proporcionada a los usuarios del servicio IP depende de la calidad de funcionamiento de otras capas:

- capas inferiores (LL) que proporcionan (vía "enlaces") transporte con conexión o sin conexión que soporta la capa IP. Los enlaces se terminan en puntos en los que los paquetes IP son reenviados (es decir, en "encaminadores", "SRC" y "DST") y por ello no tienen significado de extremo a extremo. En los enlaces pueden intervenir diferentes tipos de tecnología, por ejemplo, modo de transferencia asíncrono (ATM), retransmisión de tramas, jerarquía digital síncrona (SDH), jerarquía digital plesiócrona (PDH), RDSI y líneas arrendadas. Puede haber varias capas de protocolos y servicios por debajo de la capa IP, y éstos, en último extremo, utilizan diversos tipos de medios físicos;
- la capa IP que proporciona transporte sin conexión de datagramas IP (es decir, paquetes IP). La capa IP tiene significado de extremo a extremo para un determinado par de direcciones IP de origen y destino. Ciertos elementos de los encabezamientos de los paquetes IP pueden ser modificados por las redes, pero los datos de usuario IP no pueden ser modificados en la capa IP ni por debajo de ella;
- capas superiores, soportadas por el IP, que posibilitan más aún las comunicaciones de extremo a extremo. Las capas superiores pueden incluir, por ejemplo, el protocolo de control de la transmisión (TCP), el protocolo de datagrama de usuario (UDP), el protocolo de transferencia de ficheros (FTP), el protocolo de transporte en tiempo real (RTP) y el protocolo de transferencia de hipertexto (HTTP). Las capas superiores podrán modificar y mejorar la calidad de funcionamiento de extremo a extremo proporcionada en la capa IP.

NOTA 1 – La cláusula 5 define un modelo de calidad de funcionamiento de servicio IP y define de manera más precisa los términos clave utilizados en este modelo estratificado por capas.

NOTA 2 – Las interacciones de calidad de funcionamiento entre estas capas quedan en estudio.

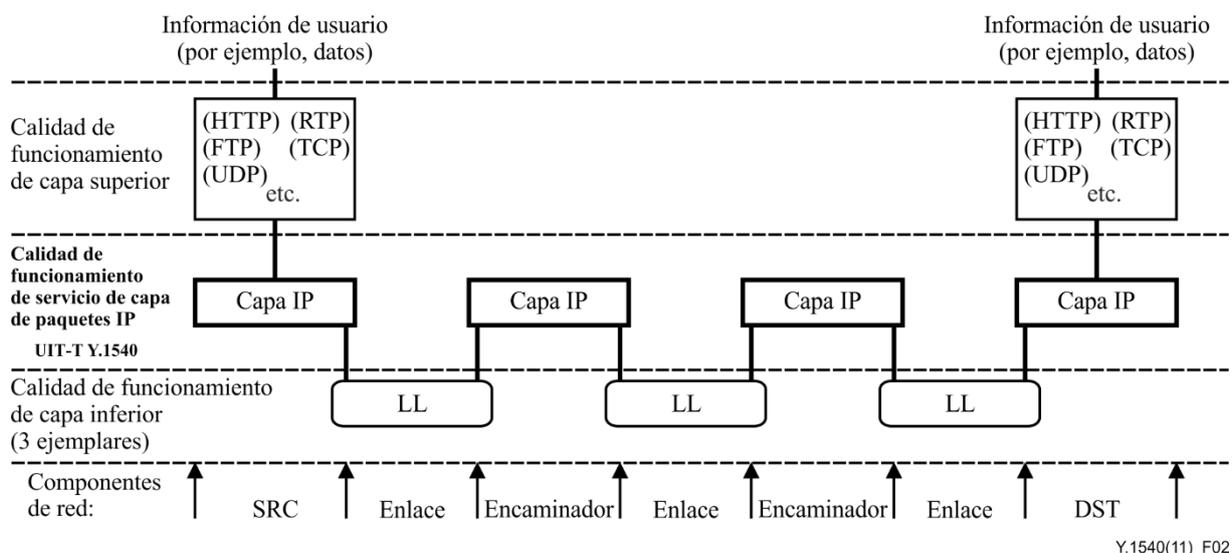


Figura 2 – Modelo estratificado por capas de calidad de funcionamiento de servicio IP – Ejemplo

5 Modelo de calidad de funcionamiento de servicio IP genérico

En esta cláusula se define un modelo de calidad de funcionamiento de servicio IP genérico. El modelo se compone sobre todo de dos tipos de secciones: enlaces de central y secciones de red (NS). Dichas secciones, que se definen en la cláusula 5.2, proporcionan los bloques de construcción con los que se puede representar cualquier servicio IP de extremo a extremo. Todos los parámetros de calidad de funcionamiento definidos en esta Recomendación se pueden aplicar a la transferencia unidireccional de paquetes IP por una sección o un conjunto concatenado de secciones.

La cláusula 5.4 especifica el conjunto de eventos de referencia de transferencia de paquetes IP en el que se basa la definición de los parámetros de calidad de funcionamiento. Los eventos de referencia

se derivan de las definiciones pertinentes de servicios IP y protocolos, y son coherentes con ellas. En la cláusula 5.5 se utilizan esos eventos de referencia para enumerar los resultados posibles cuando se entrega un paquete en una sección.

NOTA – La incorporación de la totalidad o parte del modelo de calidad de funcionamiento UIT-T Y.1540 y de los eventos de referencia en [b-UIT-T I.353] queda en estudio.

5.1 Componentes de red

5.1.1 Computador principal

Un computador principal es un computador que se comunica utilizando los protocolos Internet. Aplica funciones de encaminamiento (es decir, funciona en la capa IP) y puede implementar funciones adicionales que incluyan protocolos de capa superior (por ejemplo, el TCP en un computador principal de origen o destino (DST)) y protocolos de capa inferior (por ejemplo, ATM).

5.1.2 Encaminador

Un encaminador es un computador principal que permite la comunicación entre otros computadores principales reenviando los paquetes IP en función del contenido de su campo de dirección de destino IP.

5.1.3 Computador principal de origen (SRC)

Un computador principal de origen es un computador principal y una dirección IP completa en donde se originan los paquetes IP de extremo a extremo. Por lo general, un computador principal puede tener más de una dirección IP; sin embargo, un computador principal de origen (SRC) constituye una única asociación con una sola dirección IP. Los computadores principales de origen originan también protocolos de capa superior (por ejemplo, TCP) cuando se implementan tales protocolos.

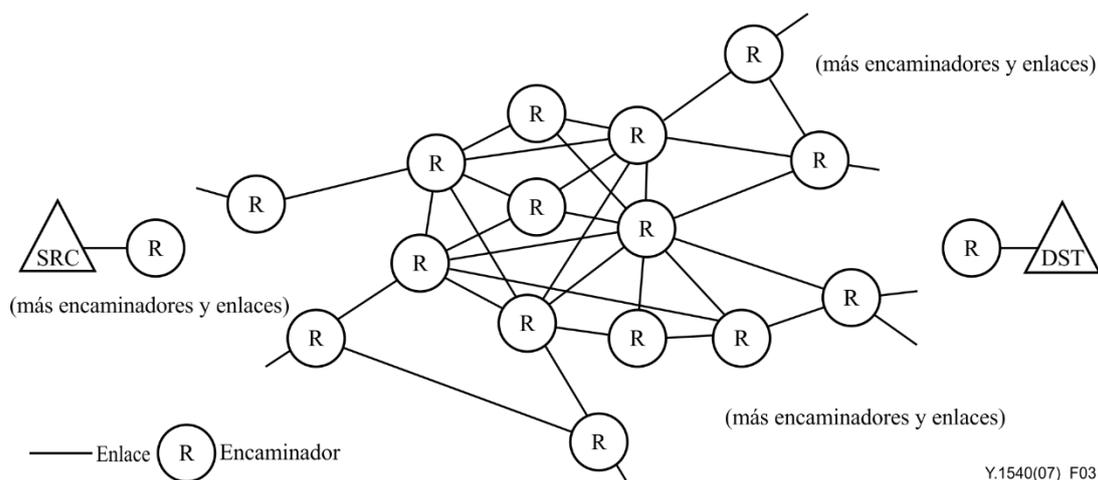
5.1.4 Computador principal de destino (DST)

Un computador principal de destino es un computador principal y una dirección IP completa en donde se terminan los paquetes IP de extremo a extremo. Por lo general, un computador principal puede tener más de una dirección IP; sin embargo, un computador principal de destino constituye una única asociación con una sola dirección IP. Los computadores principales de destino terminan también protocolos de capa superior (por ejemplo, TCP) cuando se implementan tales protocolos.

5.1.5 Enlace

Un enlace es una conexión punto a punto (física o virtual) utilizada para transportar paquetes IP entre un par de computadores principales. No incluye parte alguna de los computadores principales ni ningún otro computador principal; funciona por debajo de la capa IP. Un enlace podría ser, por ejemplo, una línea arrendada, o podría implementarse a modo de conexión lógica por una red Ethernet, una red de retransmisión de tramas, una red ATM o utilizando cualquier otra tecnología de red que funcione por debajo de la capa IP.

La Figura 3 muestra los componentes de red que interesan en un servicio IP entre un SRC y un DST. Los enlaces, que podrían ser conexiones de marcación, líneas arrendadas, anillos o redes, se indican mediante líneas entre computadores principales. Los encaminadores se muestran en forma de círculos y tanto el SRC como el DST se representan en forma de triángulos.



Y.1540(07)_F03

Figura 3 – Componentes de red IP

5.2 Enlaces de central y secciones de red

5.2.1 Enlace de central (EL)

Este es el enlace que conecta:

- 1) un computador principal de origen o destino a su computador principal adyacente (por ejemplo, un encaminador) posiblemente en otra jurisdicción a veces denominada enlace de acceso, enlace de ingreso o enlace de egreso; o
- 2) un encaminador de una sección de red con un encaminador de otra sección de red.

Se señala que la responsabilidad respecto a un enlace de central, su capacidad y su calidad de funcionamiento son compartidas normalmente por las partes conectadas.

NOTA – "Enlace de central" es aproximadamente equivalente al término "central" definido en [b-IETF RFC 2330].

5.2.2 Sección de red (NS)

Una sección de red es un conjunto de computadores principales unidos por todos sus enlaces de interconexión que juntos proporcionan una parte del servicio IP entre un SRC y un DST, y están bajo una única responsabilidad jurisdiccional (o colaborativa). Algunas secciones de red constan de un solo computador principal sin enlaces de interconexión. Las NS de origen y las NS de destino son casos particulares de secciones de red. Los pares de secciones de red están conectados por enlaces de central.

NOTA – "Sección de red" es aproximadamente equivalente al término "nube" definido en [b-IETF RFC 2330].

Cualquier conjunto de computadores principales interconectados por enlaces podría considerarse como una sección de red. Sin embargo, a los efectos (futuros) de atribución de la calidad de funcionamiento IP, será importante centrarse en el conjunto de computadores principales y enlaces que están bajo una única responsabilidad jurisdiccional (o colaborativas) (por ejemplo, un proveedor de servicios de Internet (ISP) o un proveedor de servicio de red (NSP)). Dichos computadores tienen normalmente el mismo identificador de red en sus direcciones IP. Por lo general, tienen sus propias reglas de encaminamiento interno. Los procesos globales y las políticas locales dictan las opciones de encaminamiento a destinos fuera de esta sección de red (a otra NS vía enlaces de central). Las fronteras de estas secciones de red son normalmente encaminadores que aplican los protocolos de pasarela exterior IP.

5.2.3 Sección de red de origen (NS de origen)

La sección de red de origen es una NS que incluye el SRC dentro de su responsabilidad jurisdiccional. En algunos casos, el SRC es el único computador principal dentro de la NS de origen.

5.2.4 Sección de red de destino (NS de destino)

La sección de red de destino es una NS que incluye el DST dentro de su responsabilidad jurisdiccional. En algunos casos, el DST es el único computador principal dentro de la NS de destino.

La Figura 4 ilustra la conectividad de red que interesa en el servicio IP entre un SRC y un DST. En los bordes de cada NS, encaminadores pasarela reciben y envían paquetes a través de enlaces de central.

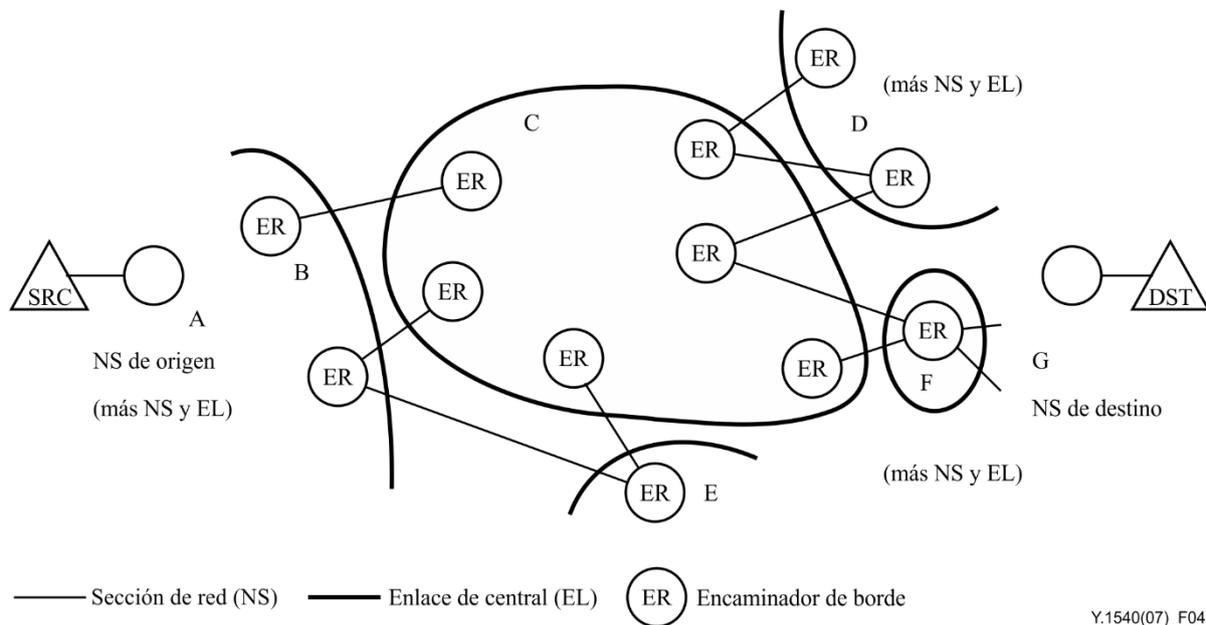


Figura 4 – Conectividad de red IP

5.3 Puntos de medición y secciones medibles

5.3.1 Punto de medición (MP)

El punto de medición es la frontera entre un computador principal y un enlace adyacente en donde pueden observarse y medirse eventos de referencia de calidad de funcionamiento. De conformidad con [b-UIT-T I.353], los protocolos Internet normalizados se pueden observar en puntos de medición (MP) IP. En [b-UIT-T I.353] se aporta más información sobre los MP para servicios digitales.

NOTA – La ubicación exacta del MP del servicio IP dentro de la pila de protocolos IP queda en estudio.

Una sección o una combinación de secciones es medible si está limitada por un conjunto de puntos de medición (MP). En esta Recomendación son medibles las siguientes secciones.

5.3.2 Sección básica

Las secciones básicas pueden ser un EL, una NS, un SRC o un DST. Las secciones básicas están delimitadas por MP.

La calidad de funcionamiento de cualquier EL o NS se puede medir en relación con cualquier servicio IP de extremo a extremo unidireccional dado. Los *MP de ingreso* son el conjunto de MP cruzados por paquetes de ese servicio cuando entran en la sección básica. Los *MP de egreso* son el conjunto de MP cruzados por paquetes de ese servicio cuando salen de la sección básica.

5.3.3 Red con protocolo Internet de extremo a extremo

Conjunto de EL y NS que proporcionan el transporte de paquetes IP transmitidos de un SRC a un DST. Los MP que limitan la red IP de extremo a extremo son los MP del SRC y el DST.

La calidad de funcionamiento de una red IP de extremo a extremo se puede medir en relación con cualquier servicio IP de extremo a extremo unidireccional dado. El *MP de ingreso* es el MP cruzado por paquetes de ese servicio cuando entran en la red de extremo a extremo en el SRC. El *MP de egreso* es el MP cruzado por paquetes de ese servicio cuando salen de la red de extremo a extremo en el DST.

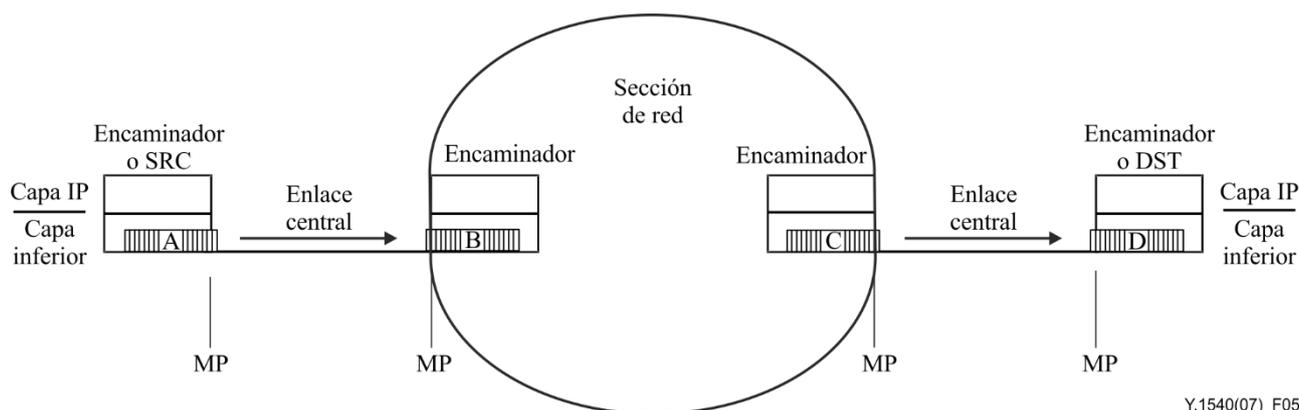
5.3.4 Conjunto de secciones de red (NSE)

Un conjunto de secciones de red (NSE) es cualquier subconjunto conectado de NS junto con todos los EL que las interconectan. El término "NSE" se puede utilizar para referirse a una sola NS, dos NS o cualquier número de NS y el EL que las conecta. Los pares de NSE distintos están conectados por enlaces de central. El término "NSE" se puede utilizar también para representar toda la red IP de extremo a extremo. Los NSE están delimitados por puntos de medición (MP).

La calidad de funcionamiento de cualquier NSE dado se puede medir en relación con cualquier servicio IP de extremo a extremo unidireccional. Los *MP de ingreso* son el conjunto de MP cruzados por paquetes de ese servicio cuando entran en ese NSE. Los *MP de egreso* son el conjunto de MP cruzados por paquetes de ese servicio cuando salen de ese NSE.

5.4 Eventos de referencia de transferencia de paquetes IP (IPRE)

En el contexto de esta Recomendación, las definiciones que siguen se aplican en un servicio IP de extremo a extremo especificado. Los términos definidos se ilustran en la Figura 5.



Y.1540(07)_F05

NOTA 1 – Eventos de salida IP para paquetes A y C.
NOTA 2 – Eventos de entrada IP para paquetes B y D.

Figura 5 – Ejemplo de eventos de referencia de transferencia de paquetes IP

Un evento de transferencia de paquetes IP ocurre cuando:

- un paquete IP cruza un MP; y
- se aplican procedimientos IP normalizados al paquete para verificar la validez de la suma de control del encabezamiento; y
- los campos de dirección de origen y destino del encabezamiento del paquete IP representan las direcciones IP del SRC y el DST previstos.

NOTA – El encabezamiento de un paquete IP contiene información como por ejemplo el tipo de servicio (ToS) o el punto de código de los servicios diferenciados (DSCP). Queda en estudio establecer en qué medida esa información puede afectar a la calidad de funcionamiento de la transferencia de paquetes.

Los eventos de referencia de transferencia de paquetes IP se definen sin tener en cuenta la fragmentación de los paquetes. Dichos eventos ocurren cada vez que un paquete IP cruza cualquier MP con independencia del valor contenido en la "bandera de más fragmentos".

Se definen cuatro tipos de evento de transferencia de paquetes IP:

5.4.1 Evento de entrada de paquetes IP en un computador principal

Un evento de entrada de transferencia de paquetes del protocolo Internet en un computador principal ocurre cuando un paquete IP cruza un MP entrando en un computador principal (encaminador de NS o DST) desde el EL conectado.

5.4.2 Evento de salida de paquetes IP de un computador principal

Un evento de salida de transferencia de paquetes del protocolo Internet de un computador principal ocurre cuando un paquete IP cruza un MP saliendo de un computador principal (encaminador de NS o SRC) hacia el EL conectado.

5.4.3 Evento de ingreso de paquetes IP en una sección básica o NSE

Un evento de ingreso de transferencia de paquetes IP en una sección básica o NSE ocurre cuando un paquete IP cruza un MP de ingreso entrando en una sección básica o un NSE.

5.4.4 Evento de egreso de paquetes del protocolo Internet de una sección básica o NSE

Un evento de egreso de transferencia de paquetes IP de una sección básica o NSE ocurre cuando un paquete IP cruza un MP de egreso saliendo de una sección básica o un NSE.

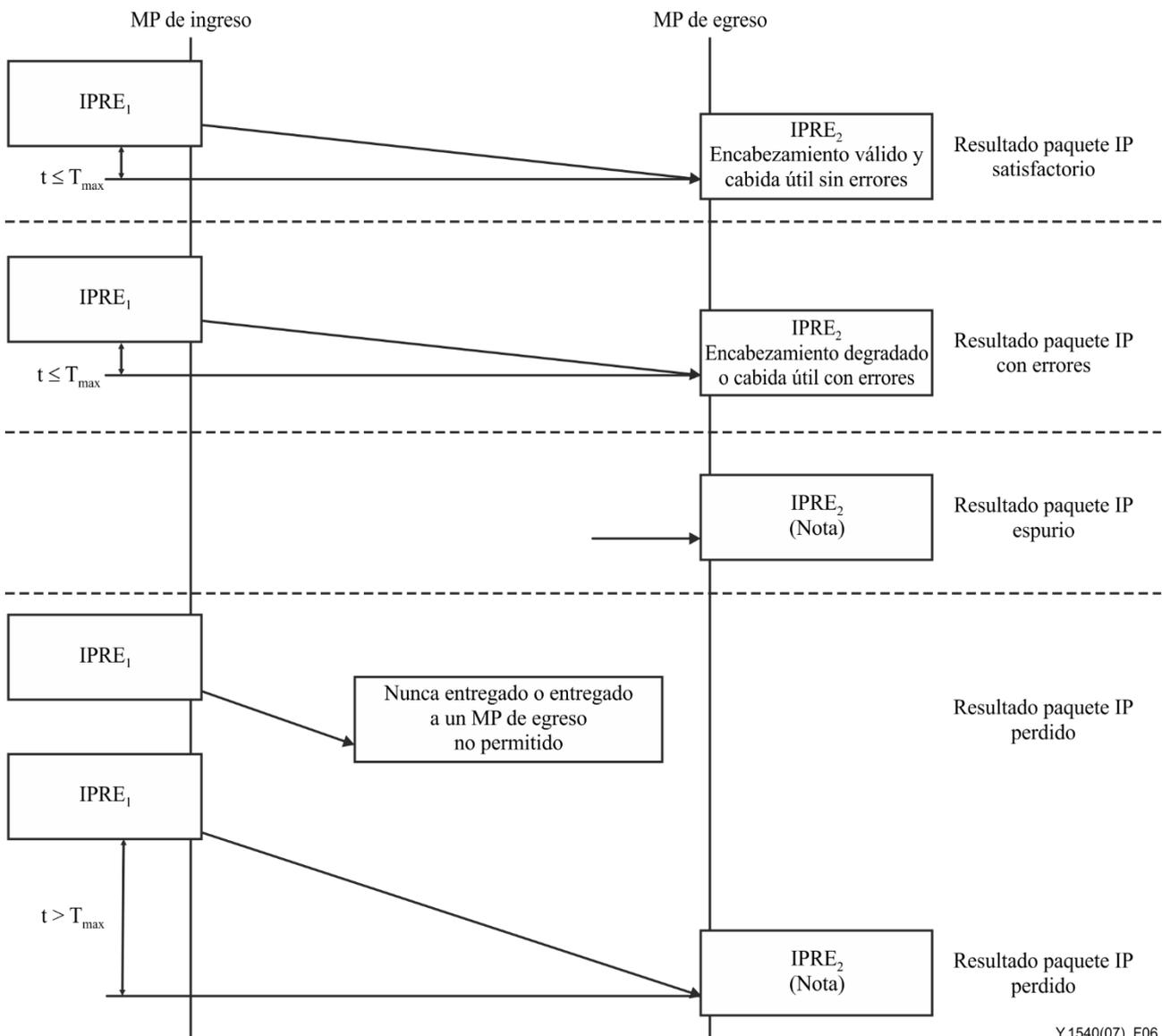
NOTA 1 – Los eventos de entrada y salida de paquetes IP representan siempre, respectivamente, entrada en y salida de un computador principal. Los eventos de ingreso y egreso de paquetes IP representan ingreso en y egreso de una sección o un NSE. Para ilustrar este punto, se señala que un ingreso en un EL crea un evento de salida del computador principal precedente, mientras que un ingreso en una NS es un evento de entrada porque, por definición, una NS tiene siempre computadores principales en sus extremos.

NOTA 2 – Para efectuar mediciones en la práctica, no es preciso observar los eventos de referencia de transferencia de paquetes IP en la pila de protocolos IP del computador principal. El momento en que ocurren esos eventos de referencias se puede aproximar, en cambio, observando los paquetes que cruzan una interfaz física asociada. La interfaz física deberá estar, no obstante, tan cerca como sea posible del MP deseado. Cuando los eventos de referencia se supervisan en una interfaz física, el momento en que ocurre un evento de salida de un computador principal se aproxima por la observación del primer bit del paquete IP que sale del computador principal o del equipo de prueba. El momento en que ocurre un evento de entrada en un computador principal se aproxima por la observación del último bit del paquete IP que entra en el computador principal o en el equipo de prueba.

5.5 Resultados de la transferencia de paquetes IP

Al considerar los eventos de referencia de transferencia de paquetes IP, se pueden definir varios resultados posibles de la transferencia IP para cualquier paquete que intente cruzar una sección básica o un NSE. Al efectuar la transmisión de un paquete IP, es posible que *se transfiera de manera satisfactoria, se le introduzcan errores o se pierda*. Un paquete IP entregado para el que no se haya ofrecido un paquete IP correspondiente se dice que es *espurio*. La Figura 6 ilustra los resultados de la transferencia de paquetes IP.

Las definiciones de los resultados de la transferencia de paquetes IP se basan en los conceptos de *MP de ingreso permisible, MP de egreso permisible y paquetes correspondientes*.



Y.1540(07)_F06

NOTA – El resultado se produce con independencia del contenido del paquete IP.

Figura 6 – Resultados de la transferencia de paquetes IP

5.5.1 Información de encaminamiento global y enlaces de salida permisibles

En teoría, en una red IP conectada, se puede entregar un paquete a cualquier encaminador, NS o NSE, porque de todos modos llega a su destino. Sin embargo, la información de encaminamiento global define un conjunto restringido de direcciones de destino a las que cada red (sistema autónomo) está dispuesta a dar servicio, y puede dar servicio, en nombre de cada una de sus NS contiguas. Es razonable suponer que (en el peor de los casos) una NS desechará por completo cualesquiera paquetes con direcciones de destino respecto a las cuales esa NS haya anunciado que es incapaz (o no desea) darles servicio. Por consiguiente, los paquetes (y fragmentos de paquetes) IP que salgan de una sección básica deberán ser reenviados solamente a otras secciones básicas *permitidas* por la información de encaminamiento global disponible.

A efectos de calidad de funcionamiento, el transporte de un paquete IP por un NSE se considerará satisfactorio solamente cuando ese NSE reenvíe el contenido completo del paquete a otras secciones básicas permitidas por la información de encaminamiento global disponible actualmente. Si la dirección de destino corresponde a un computador principal conectado directamente a este NSE, el único resultado permitido y el único transporte de IP satisfactorio consiste en el reenvío al computador principal de destino.

NOTA 1 – Los procedimientos IP incluyen la actualización de la información de encaminamiento global. Una NS que fuera permisible puede no serlo ya tras una actualización de la información de encaminamiento compartida por secciones de red (NS). De manera alternativa, una NS que no fuera permisible anteriormente, puede serlo ya tras una actualización de la información de encaminamiento global.

NOTA 2 – La información de encaminamiento se puede complementar con información sobre la idoneidad relativa de cada uno de los enlaces de salida permitidos. Las implicaciones en cuanto a calidad de funcionamiento de esa información adicional quedan en estudio.

En un momento determinado, y en relación con un servicio IP de extremo a extremo dado y una sección básica o un NSE:

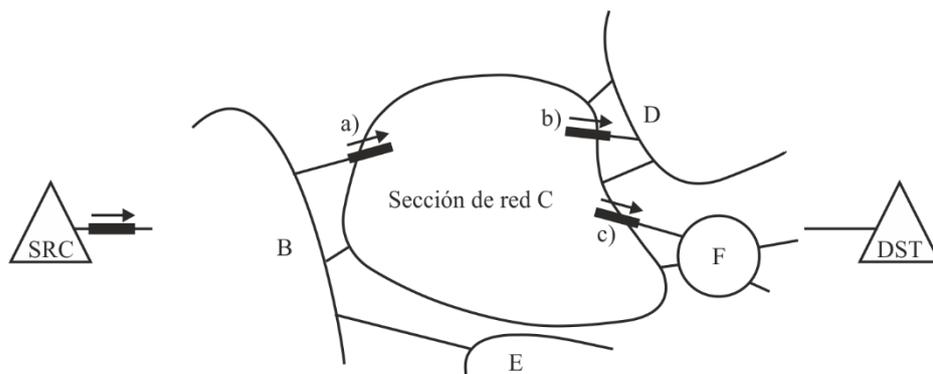
- un MP de ingreso es un *MP de ingreso permisible* si el cruce de este MP hacia esa sección básica o ese NSE está permitido por la información de encaminamiento global;
- un MP de egreso es un *MP de egreso permisible* si el cruce de este MP lleva hacia otra sección básica que está permitida por la información de encaminamiento global.

5.5.2 Eventos correspondientes

El análisis de la calidad de funcionamiento hace necesario asociar los paquetes que cruzan un MP con los paquetes que han cruzado un MP diferente. Encaminamiento sin conexión significa que un paquete puede salir de una sección básica por uno de los (posiblemente) varios MP de egreso permisibles. Fragmentación de un paquete significa que un paquete que está entrando en una sección básica puede salir de la misma en fragmentos, que posiblemente entren en otras varias secciones básicas diferentes. Por último, el encaminamiento IP sin conexión puede incluso devolver un paquete o fragmento de paquete a una sección básica que ya ha atravesado (debido quizás a la actualización de los cuadros de encaminamiento).

Se dice que un evento de egreso IP *corresponde* a un evento de ingreso anterior si fueron creados por el "mismo" paquete IP. Este concepto se aplica tanto si el paquete en el MP de egreso es el paquete en su totalidad o sólo un fragmento del original. La Figura 7 ilustra un caso en el que un paquete entra en la NS C procedente de la NS B y es fragmentado en dos partes en la NS C. Uno de los fragmentos se envía a la NS D y el otro a la NS F. Estos dos eventos de egreso *corresponden* al único evento de ingreso. Para evitar la confusión resultante de la reentrada de paquetes en el NSE, este concepto de *correspondencia* exige además que ésta sea la primera vez (desde su ingreso) que el contenido de que se trate salga del NSE.

La determinación práctica de si los eventos de referencia IP son eventos correspondientes se hace normalmente caso por caso y a menudo se basará en el análisis de las direcciones IP, la información de encaminamiento global, el campo de identificación del paquete IP, otra información de encabezamiento y el contenido del paquete IP.



Un paquete IP de SRC a DST entra en la NS C, crea un evento de ingreso, es fragmentado, y crea dos eventos de egreso correspondientes, b) y c).

Y.1540(07)_F07

Figura 7 – Eventos correspondientes cuando se produce fragmentación

5.5.3 Notas sobre las definiciones de resultados de paquetes satisfactorios, con errores, perdidos y espurios

Las definiciones de resultados de paquetes que siguen se basan en la observación de eventos de referencia IP en los puntos de medición IP. Seleccionando los puntos de medición IP apropiados, cada definición se puede utilizar para evaluar la calidad de funcionamiento de un EL particular, una NS particular y un NSE particular, y se pueden aplicar a la calidad de funcionamiento de los servicios de extremo a extremo.

Los resultados se definen sin limitarse a un determinado tipo de paquetes (ToS, DSCP, protocolo, etc.). La calidad de funcionamiento IP será diferente según el tipo de paquete.

En cada definición se tiene en cuenta la posibilidad de fragmentación del paquete incluyendo la posibilidad de que un único evento de referencia IP dé lugar a varios eventos subsiguientes. Se señala que si se pierde cualquier fragmento, se considera perdido todo el paquete original. Si no se pierde ningún fragmento, pero algunos de ellos quedan con errores, se considera erróneo todo el paquete original. Para que la entrega del paquete original se considere satisfactoria, debe entregarse satisfactoriamente cada uno de los fragmentos a uno de los EL de salida permisibles.

5.5.4 Resultado satisfactorio de transferencia de paquetes IP

Se produce un resultado satisfactorio de transferencia de paquete cuando un solo evento de referencia de paquetes IP en un MP_0 de ingreso permisible da lugar a uno (o más) evento(s) de referencia correspondientes en uno (o más) MP_i de egreso, todos ellos dentro de un plazo de tiempo $T_{m\acute{a}x}$ especificado a partir del evento de ingreso original y:

- 1) todos los MP_i de egreso en donde ocurren los eventos de referencia correspondientes son permisibles; y
- 2) el contenido completo del paquete original observado en MP_0 está incluido en el (los) paquete(s) entregado(s);
- 3) o bien el contenido binario del (de los) campo(s) de información del (de los) paquete(s) IP entregado(s) no es conforme exactamente al del paquete original;
- 4) o bien el (los) campo(s) de encabezamiento del (los) paquete(s) entregado(s) es (son) válido(s).

NOTA – Se recomienda establecer el valor de $T_{m\acute{a}x}$ en 3 segundos para uso general. Algunos trayectos globales de extremo a extremo quizá requieran un valor de $T_{m\acute{a}x}$ más grande para asegurar que los paquetes con tiempos de transferencia largos tengan la oportunidad adecuada de llegar. El valor de 3 segundos es el que se ha utilizado en la práctica.

5.5.5 Resultado de paquete IP con errores

Se produce un resultado de paquetes con errores cuando un solo evento de referencia de paquetes IP en un MP_0 de ingreso permisible da lugar a uno (o más) evento(s) de referencia correspondiente(s) en uno (o más) MP_i de egreso, todos ellos dentro de un plazo de tiempo $T_{m\acute{a}x}$ a partir del evento de referencia original y:

- 1) todos los MP_i de egreso en donde ocurren los eventos de referencia correspondientes son permisibles; y
- 2) el contenido completo del paquete original observado en MP_0 está incluido en el (los) paquete(s) entregado(s);
- 3) o bien:
 - el contenido binario del (de los) campo(s) de información del (de los) paquete(s) IP entregado(s) no es conforme exactamente con el del paquete original; o
 - uno o más de los campo(s) de encabezamiento del (de los) paquete(s) entregado(s) está(n) corrompido(s).

NOTA – La mayoría de los paquetes con encabezamiento con errores no detectados por la suma de control del encabezamiento en la capa IP serán descartados o redireccionados por otros procedimientos de capa IP (por ejemplo, en función de la corrupción de los campos de dirección o ToS/DSCP). El resultado es que no se crea ningún evento de referencia para los protocolos de capa superior que esperan recibir este paquete. Puesto que no hay ningún evento de referencia IP, estos intentos de transferencia de paquetes se clasificarán como de resultado de paquete perdido. Los encabezamientos con errores que no den lugar a un descarte o direccionamiento erróneo se clasificarán como de resultado de paquete con errores.

5.5.6 Resultado de paquetes IP perdido

Se produce un resultado de paquete perdido cuando hay un único evento de referencia de paquete IP en un MP_1 de ingreso permisible, y cuando parte o todo el contenido correspondiente a ese paquete de ingreso no da lugar a un evento de referencia de paquete IP en un MP_n de egreso permisible dentro de un plazo de tiempo $T_{m\acute{a}x}$.

Un resultado de paquete perdido puede ser, de hecho, uno o más resultados de paquetes mal direccionados (que no fueron observados), como se define a continuación.

Aparece un paquete mal direccionado cuando un solo evento de referencia de paquetes IP en un MP_0 de ingreso permisible da lugar a uno (o más) evento(s) de referencia correspondiente(s) en uno (o más) MP_i de egreso, todos ellos dentro de un plazo de tiempo $T_{m\acute{a}x}$ especificado a partir del evento de referencia original y:

- 1) el contenido completo del paquete original observado en MP_0 está incluido en el (los) paquete(s) entregado(s); pero
- 2) uno o más de los MP_i de egreso donde ocurren los eventos de referencia correspondientes no son MP de egreso permisibles.

5.5.7 Resultado de paquete IP espurio

Se produce un resultado de paquete IP espurio en una sección básica o un NSE de extremo a extremo cuando un paquete IP único crea un evento de egreso para el que no hay un evento de ingreso correspondiente.

5.5.8 Resultados de paquetes IP secundarios

Los siguientes resultados se basan en los resultados fundamentales descritos anteriormente.

5.5.8.1 Resultados de paquetes IP ordenados y reordenados

La definición de los resultados de estos paquetes IP requiere un examen preliminar.

La entrega de paquetes en orden es una propiedad de las transferencias satisfactorias de paquetes, de modo que los paquetes se reciben en el computador principal de destino (o punto de medición) en el mismo orden en que fueron enviados. El orden de llegada se determina por la posición relativa a otros paquetes de interés, aunque la medida en la cual se ha reordenado un determinado paquete se puede cuantificar en unidades de posición, tiempo y distancias de bytes de cabida útil. El parámetro de calidad de funcionamiento de paquetes reordenados es importante para la mayoría de las aplicaciones, especialmente cuando se evalúa la aptitud de la red para trenes de medios en tiempo real, debido a su capacidad limitada de restablecer el orden, o cuando la calidad de funcionamiento conlleva una falta de esa capacidad. Normalmente los paquetes contienen algún tipo de identificador único aplicado en el SRC, que a veces se supone que es un número de secuencia, por lo que este número u otra información (como las marcas de tiempo que se introducen en el MP_0) es la referencia del orden inicial en la fuente. La evaluación del orden de llegada requiere también la capacidad de determinar qué paquete específico es el "siguiente esperado", y esto se simplifica enormemente cuando los números de secuencia son enteros consecutivos crecientes.

El resultado de paquetes ordenados se produce cuando un solo evento de referencia de paquete IP en un punto de medición de egreso permisible da lugar a lo siguiente:

- El paquete tiene un número de secuencia mayor o igual al siguiente valor esperado del paquete. El siguiente valor esperado aumenta para reflejar la llegada de este paquete, estableciendo un nuevo valor de expectativa.

El resultado de paquetes reordenados o desordenados se produce cuando un solo evento de referencia de paquetes IP en un punto de medición de egreso permisible da lugar a lo siguiente:

- El paquete tiene un número de secuencia inferior al siguiente valor esperado del paquete y, por lo tanto, el paquete se reordena. El siguiente valor esperado no cambia como consecuencia de la llegada de este paquete.

5.5.8.2 Resultado de bloques con pérdidas severas de paquetes IP

Se produce un resultado de bloques con pérdidas severas de paquetes IP (IPSLB) para un bloque de paquetes observado durante el intervalo de tiempo T_s en el MP_0 de ingreso cuando la proporción de paquetes perdidos en el MP_i de egreso con respecto al total de paquetes del bloque es superior a s_1 .

El valor del intervalo de tiempo T_s se establece provisionalmente en 10 segundos. El valor del umbral s_1 se fija provisionalmente en 0,2. La evaluación de los bloques (intervalos de tiempo) sucesivos no debería solaparse.

NOTA – Estos valores están concebidos para identificar los cambios de ruta IP debidos a las actualizaciones de encaminamiento, que causan una degradación significativa en la mayoría de las aplicaciones de usuario. Estos valores pueden cambiar tras realizar nuevos estudios y obtener experiencia. Si se utilizaran valores inferiores de s_1 , se capturarían otros eventos de red que podrían afectar al funcionamiento de las aplicaciones sensibles a la conectividad. Además, la degradación importante en aplicaciones vídeo y audio se puede correlacionar fácilmente con el resultado IPSLB cuando se utilizan longitudes de bloque T_s de aproximadamente 1 segundo, y la utilización de este valor puede resultar importante en el futuro.

El mínimo número de paquetes que deberían utilizarse para evaluar el resultado bloque con muchas pérdidas es M_{lb} y esos paquetes no deberían extenderse más allá del intervalo T_s . El valor de M_{lb} será objeto de un nuevo estudio.

5.5.8.3 Resultado de paquetes IP duplicados

Un resultado de transferencia de paquetes duplicados, que es un subconjunto de resultados satisfactorios de transferencia de paquetes, ocurre cuando un solo evento de referencia de paquetes IP en un MP_0 de ingreso permisible da lugar a dos o más eventos de referencia correspondientes en al menos un MP_i de egreso permisible, y los campos de información binaria de todos los paquetes de salida son idénticos a los del paquete original. El evento de referencia de egreso en MP_i para un paquete duplicado ocurre después de que se haya producido al menos otro evento de referencia de egreso correspondiente para el paquete original (normalmente también en MP_i).

Obsérvese que en la comunicación punto a punto solo hay un MP_i de egreso permisible cuando el computador principal de destino está conectado directamente al NSE. En la comunicación punto a multipunto puede haber muchos MP_i de egreso permisibles para los distintos destinos.

5.5.8.4 Resultado de paquetes IP replicados

Se produce un resultado de transferencia de paquetes replicados cuando un solo evento de referencia de paquetes IP en un MP_0 de ingreso permisible da lugar a dos o más eventos de referencia correspondientes en al menos un MP_i de egreso permisible, y los campos de información binaria de todos los paquetes de salida son idénticos a los del paquete original. El evento de referencia de egreso en MP_i para un paquete replicado es el primero para el paquete original y ocurre antes de que se haya producido al menos otro evento de referencia de egreso para el paquete duplicado (normalmente también en MP_i).

5.5.9 Resultados de paquetes IP de reparación de trenes

Los siguientes resultados se basan en los resultados fundamentales, con un análisis adicional basado en un modelo de sistemas de reparación de trenes. En el apéndice VII se proporcionan más antecedentes sobre este tema y sobre las técnicas de mitigación del deterioro (por encima de la capa IP) que se abordan.

5.5.9.1 Modelo simple de técnicas de reparación de trenes en la capa de aplicaciones

En el Apéndice VII se define también un modelo sencillo, que se describe a continuación. Cada tren de paquetes de la capa de aplicaciones se modela como si contuviera dos categorías de paquetes:

- intervalos o bloques de paquetes de información;
- el número máximo de paquetes reparables asociados al bloque de información.

El reto para el diseñador de la técnica de reparación es elegir el tamaño del bloque de información en combinación con la capacidad (máxima) de reparación que sea suficiente para compensar un alto porcentaje de degradaciones de las redes de paquetes (pérdida, retardo excesivo y corrupción), al tiempo que se trabaja dentro de los límites de la capacidad global de transferencia de paquetes del sistema y se ofrece una calidad suficiente en el tren de aplicaciones.

Los nuevos parámetros de calidad de funcionamiento deberían ayudar a tomar estas decisiones.

5.5.9.2 Resultado de paquetes degradados y resultado de intervalos con errores en los paquetes IP

Se produce un *resultado de intervalos con errores en los paquetes IP* para un conjunto de paquetes observado durante el intervalo de tiempo T_I en el MP_0 de ingreso cuando el número de resultados de paquetes degradados en el MP_i de egreso es superior a x . Obsérvese que el intervalo de tiempo T_I incluye la información y la tara de los paquetes de reparación (si están incluidos en el tren de ingreso).

Los *resultados de paquetes degradados* son la suma de los siguientes resultados:

- resultados de paquetes perdidos, utilizando un $T_{m\acute{a}x}$ asociado a T_I y al tiempo de transferencia nominal, y posiblemente igual al retardo mínimo de transferencia de paquetes para la población de interés más (un múltiplo de) T_I . Esto incluiría los paquetes que están sujetos a un encolamiento excesivo y los que nunca llegan;
- resultados de paquetes con errores.

Obsérvese que un factor distintivo entre este resultado y otras métricas de pérdida/bloqueo de paquetes es la combinación de paquetes con retardos excepcionales (más allá de un umbral de variación de retardo) con paquetes que nunca llegan (y que se pierden realmente durante la transferencia) en una única categoría: paquetes degradados.

No se establecen valores provisionales para el intervalo de tiempo T_I y el umbral x . En su lugar, el análisis puede abarcar una gama de valores para el intervalo T_I y el umbral x . También se debería especificar la longitud de la cabida útil de paquetes IP, ya que influye en el tiempo de serialización y, por lo tanto, en el intervalo de tiempo ocupado por un bloque de paquetes.

5.5.9.3 Resultado de bloques degradados de paquetes IP

Se produce un *resultado de bloques degradados de paquetes IP* para un conjunto de paquetes de tamaño de bloque b , observado en el MP_0 de ingreso cuando el número de resultados de paquetes degradados en el MP_i de egreso en el bloque es superior a x . No se establecen valores provisionales para el tamaño de bloque b y el umbral de reparación x .

6 Parámetros de calidad de funcionamiento de la transferencia de paquetes IP

Esta cláusula define un conjunto de parámetros de calidad de funcionamiento de la transferencia de información de paquetes IP utilizando los resultados de la transferencia de paquetes IP definidos en

la cláusula 5.5. Los parámetros se pueden estimar sobre la base de las observaciones efectuadas en los MP que limitan la sección básica o el NSE sometido a prueba.

NOTA – Las definiciones de parámetros de calidad de funcionamiento de transferencia de paquetes IP adicionales (por ejemplo, tasa de bloques de paquetes IP con muchos errores) quedan en estudio.

6.1 Calificaciones de los paquetes

Esta cláusula define la terminología clave para calificar la aplicabilidad de los parámetros de calidad de funcionamiento a los conjuntos de paquetes.

6.1.1 Poblaciones de interés

La mayoría de los parámetros de calidad de funcionamiento se definen en conjuntos de paquetes llamados *poblaciones de interés*. Para el *caso extremo a extremo*, la población de interés es normalmente el conjunto total de paquetes que se envía de un SRC a un DST. Los puntos de medición en el caso extremo a extremo son el MP del SRC y el DST.

Para una sección básica o un NSE en relación con un par SRC y DST determinado, la población de interés en un MP de ingreso permisible particular es el conjunto de paquetes enviados del SRC al DST que se encaminan entrando en la sección básica o el NSE a través de ese MP específico. Esto es lo que se llama el *caso de ingreso específico*.

La población de interés total para una sección básica o un NSE en relación con un par SRC y DST determinado es el conjunto total de paquetes del SRC al DST que se entregan entrando en la sección o el NSE a través de cualquiera de sus MP de ingreso permisibles. Esto es lo que se llama el *caso independiente del ingreso*.

Cada uno de estos parámetros de calidad de funcionamiento IP se define sin hacer referencia a un determinado tipo de paquetes (ToS, DSCP, protocolo, etc.). La calidad de funcionamiento diferirá según el tipo de paquetes y cualquier declaración a propósito de la calidad de funcionamiento medida deberá contener información sobre qué tipo o tipos de paquetes se incluyeron en la población.

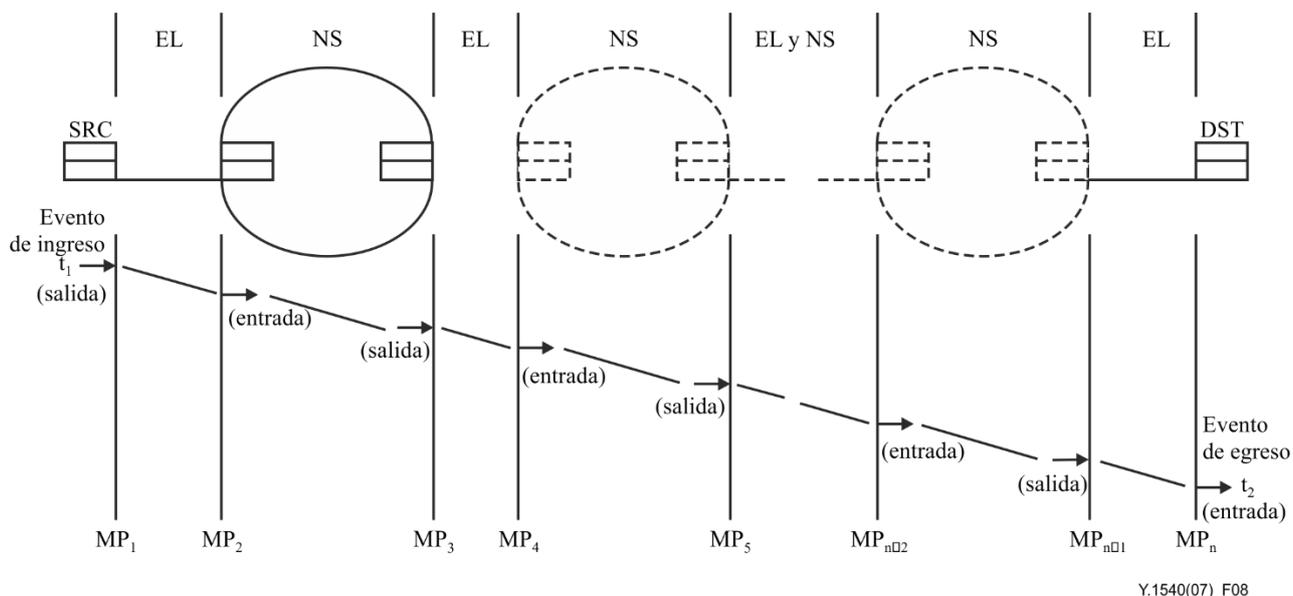
6.1.2 Flujo de paquetes

Un flujo de paquetes es el tráfico asociado con un tren de bits con conexión o sin conexión determinado, que tiene el mismo computador principal de origen (SRC), computador principal de destino (DST), clase de servicio e identificación de sesión (por ejemplo, números de puerto de un protocolo de capa superior). En otros documentos se pueden utilizar los términos microflujo o subflujo para referirse a trenes de tráfico con este grado de clasificación. Un flujo de paquetes es el ejemplo más común de una población de interés.

Los paquetes IPv6 tienen un campo adicional para que el computador principal de origen etiquete secuencias de paquetes que deberían recibir algún tratamiento especial en los encaminadores IPv6. Este campo se denomina etiqueta de flujo y, en combinación con la dirección de origen, define de forma única un flujo de paquetes.

6.2 Retardo de transferencia de paquetes IP

El retardo de la transferencia de paquetes IP se define para todos los resultados de paquetes satisfactorios y con errores a través de una sección básica o un NSE. El IPTD es el tiempo ($t_2 - t_1$) que transcurre entre la ocurrencia de dos eventos de referencia de paquetes IP correspondientes, evento de ingreso $IPRE_1$ en el momento t_1 y evento de egreso $IPRE_2$ en el momento t_2 , siendo ($t_2 > t_1$) y ($t_2 - t_1$) $\leq T_{m\acute{a}x}$. Si el paquete se fragmenta dentro del NSE, t_2 es el momento en que se produce el evento de egreso correspondiente final. El retardo de la transferencia de paquetes IP de extremo a extremo es un retardo unidireccional entre el MP del SRC y el DST, como se ilustra en la Figura 8.



**Figura 8 – Eventos de retardo de transferencia de paquetes IP
(ilustración de la transferencia de extremo a extremo de un solo paquete IP)**

6.2.1 Retardo medio de transferencia de paquetes IP

El retardo medio de la transferencia de paquetes IP es la media aritmética de los retardos de la transferencia de paquetes IP de una población de interés.

6.2.2 Retardo mínimo de transferencia de paquetes IP

El retardo mínimo de la transferencia de paquetes IP es el valor más pequeño del retardo de transferencia de paquetes IP entre todos los retardos de transferencia de paquetes IP de una población de interés. Esto incluye el retardo de propagación y los retardos de encolamiento comunes a todos los paquetes. Por lo tanto, este parámetro puede no representar el retardo mínimo teórico del trayecto entre los MP.

6.2.3 Retardo mediano de transferencia de paquetes IP

El retardo mediano de la transferencia de paquetes IP es el percentil 50 de la distribución de frecuencia de los retardos de la transferencia de paquetes IP de una población de interés. La mediana es el valor medio una vez que los retardos de transferencia han sido ordenados. Para obtener este valor medio cuando la población contiene un número par de valores, se utiliza la media de los dos valores centrales.

6.2.4 Variación del retardo de paquetes IP entre 2 puntos de extremo a extremo

También es importante la variación del retardo de la transferencia de paquetes IP. Las aplicaciones en modo serie podrían utilizar información sobre la gama total de variación del retardo IP para evitar la infrautilización o el desbordamiento de la memoria tampón. Las variaciones extremas del retardo IP provocarán el aumento de los umbrales del temporizador de retransmisión TCP y quizás den lugar también a que se retarden las retransmisiones de paquetes o se retransmitan paquetes innecesariamente.

La variación del retardo de paquetes (PDV) IP entre dos puntos de extremo a extremo se define en función de las observaciones de llegadas de paquetes IP correspondientes en los MP de ingreso y egreso (por ejemplo, MP_{DST} , MP_{SRC}). Dichas observaciones caracterizan la variabilidad del esquema de eventos de llegada de paquetes IP en el MP de egreso y el esquema de eventos correspondientes en el MP de ingreso con respecto a un retardo de referencia.

La PDV entre dos puntos (v_k) para un paquete IP k entre el SRC y el DST es la diferencia entre el retardo de transferencia de paquetes IP absoluto (x_k) del paquete y un retardo de transferencia de paquetes IP de referencia definido, $d_{1,2}$, entre esos mismos MP (véase la Figura 9): $v_k = x_k - d_{1,2}$.

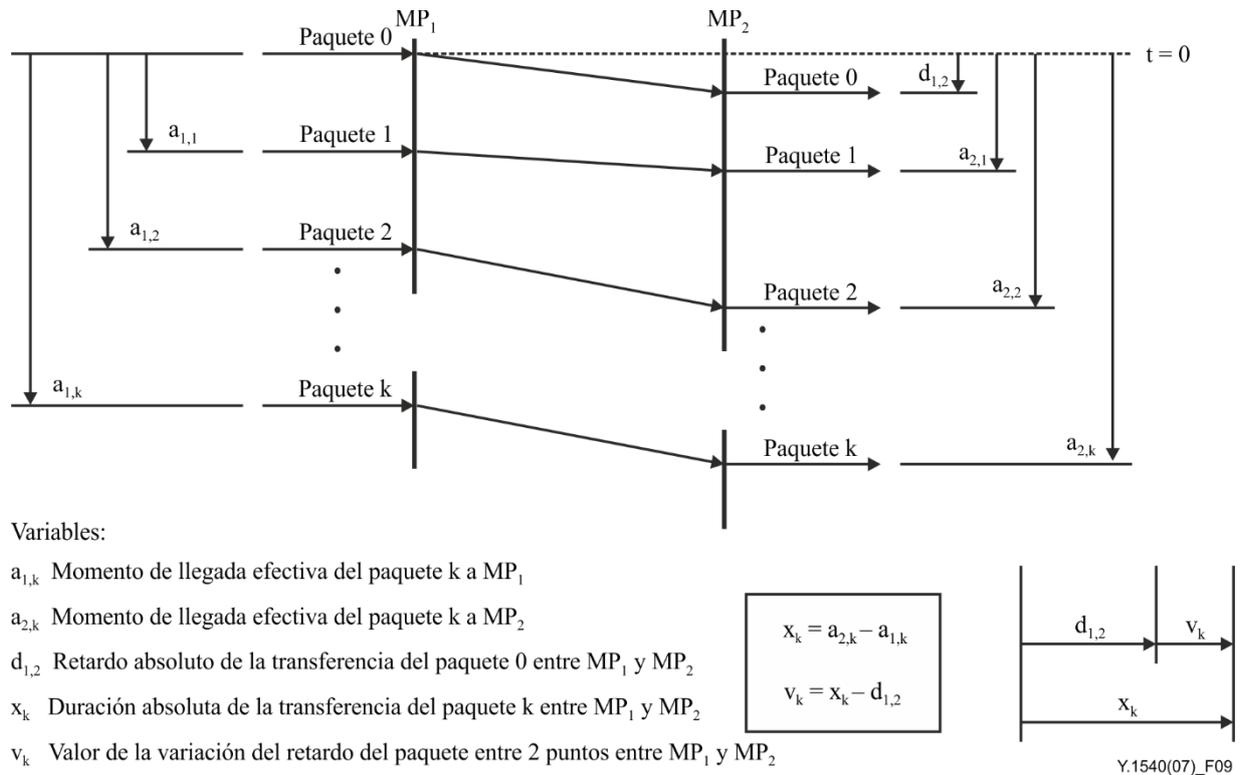


Figura 9 – Variación del retardo de paquetes IP entre dos puntos

El retardo de transferencia de paquetes IP de referencia, $d_{1,2}$, entre el SRC y el DST es el retardo de transferencia de paquetes IP absoluto que tiene un paquete IP seleccionado entre esos dos MP.

Los valores positivos de la variación de retardo de paquetes IP entre dos puntos (IPDV) corresponden a retardos de transferencia de paquetes IP superiores a los que tiene el paquete IP de referencia; los valores negativos de PDV entre dos puntos corresponden a retardos de transferencia de paquetes IP inferiores a los que tiene el paquete IP de referencia. La distribución de PDV entre dos puntos es idéntica a la distribución de los retardos de transferencia de paquetes IP absolutos desplazados en un valor constante igual a $d_{1,2}$.

6.2.4.1 Utilización del retardo mínimo como base de la variación del retardo

Como se ilustra en la Figura 9, la variación del retardo de un paquete individual se define naturalmente como la diferencia entre el retardo efectivo experimentado por ese paquete y un retardo nominal o retardo de referencia. La referencia preferida (utilizada en los objetivos de UIT-T Y.1541 IPDV) es el retardo mínimo de la población de interés. Esto garantiza que todas las variaciones se notificarán como valores positivos, y simplifica la notificación de la gama de variación (el valor máximo de la variación es igual a la gama). Las distribuciones de la variación del retardo en las redes IP suelen mostrar un sesgo hacia el mínimo (por ejemplo, el mínimo y el modo son iguales). En [IETF RFC 5481] se detallan muchas más capacidades útiles de esta forma de variación del retardo – PDV, utilizando el retardo mínimo como referencia.

El uso del retardo medio como referencia de la variación del retardo se descarta en esta versión de la presente Recomendación.

En versiones anteriores de esta Recomendación, existía una alternativa a la utilización del retardo del primer paquete mínimo como retardo nominal, a saber: la utilización del retardo medio de la

población de paquetes de interés como retardo nominal o de referencia. Esto tiene el efecto de centrar en cero la distribución de los valores de variación del retardo (cuando la distribución es simétrica), y produce variaciones tanto positivas como negativas. Sin embargo, el retardo medio de la población puede ser claramente diferente del retardo de cualquier paquete individual, creando una referencia artificial para la variación (por ejemplo, cuando hay una distribución bimodal).

6.2.4.2 Límites basados en cuantiles para la variación del retardo de paquetes IP

El método preferido (utilizado en los objetivos de UIT-T Y.154) para resumir la variación del retardo de una población de interés consiste en seleccionar los cuantiles superior e inferior de la distribución de la variación del retardo y, a continuación, medir la distancia entre esos cuantiles. Por ejemplo, se selecciona el cuantil $1 - 10^{-3}$ y el cuantil 0 (o mínimo), se realizan mediciones y se observa la diferencia entre los valores de la variación del retardo en estos dos cuantiles. Este ejemplo ayudaría a los diseñadores de aplicaciones a determinar el tamaño de la memoria intermedia de deflucción para que no haya más de un 0,1% de desbordamiento total de la memoria.

Se podría establecer un objetivo para la variación del retardo de los paquetes IP eligiendo un límite superior para la diferencia entre cuantiles preestablecidos de la distribución de la variación del retardo. Por ejemplo, "La diferencia entre el cuantil 99,9 y el mínimo de la variación del retardo de los paquetes no debe ser superior a 50 ms".

6.2.4.3 Límites basados en intervalos para la variación del retardo de paquetes IP

Un método alternativo para resumir la variación del retardo de paquetes IP experimentada por una población de interés es especificar previamente un intervalo de variación del retardo, por ejemplo 50 ms, y observar a continuación los porcentajes de variaciones de retardo de célula individuales que caen fuera y dentro de ese intervalo. Si se utiliza el intervalo de 50 ms, las aplicaciones con tamaños de memoria intermedia fijos de 50 ms o próximos a ese valor sabrían entonces aproximadamente cuántos paquetes causarían desbordamiento o infrautilización de la memoria intermedia.

NOTA – Si se utiliza este método para resumir la variación del retardo de paquetes IP, la variación del retardo de los paquetes individuales debería calcularse utilizando el retardo mínimo como nominal en la cláusula 6.2.4.1, en lugar de la definición de la cláusula 6.2.4, que utiliza el primer paquete. Utilizando la definición de la cláusula 6.2.4, el intervalo preseleccionado (por ejemplo, el de 50 ms podría anclarse ocasionalmente en un valor inusualmente grande o inusualmente pequeño.

Podría establecerse un objetivo de variación del retardo de paquetes IP eligiendo un límite inferior para el porcentaje de variaciones de retardo de paquetes individuales que estén comprendidos en un intervalo previamente especificado. Por ejemplo, "≥99% de las variaciones del retardo de paquetes deberían estar comprendidas dentro del intervalo [0 ms, 50 ms]".

6.2.4.4 Parámetros secundarios para la variación del retardo de paquetes IP

Puede ser de utilidad disponer de uno o más parámetros que capten el efecto de las variaciones del retardo de paquetes IP en diferentes aplicaciones. Conviene diferenciar las variaciones del retardo paquete a paquete (normalmente pequeñas) de las discontinuidades potencialmente mayores del retardo que pueden derivarse de un cambio en el encaminamiento IP. El Apéndice II contiene varias definiciones secundarias de la variación de retardo y directrices para su utilización.

6.3 Tasa de errores en los paquetes IP (IPER)

La tasa de errores en los paquetes IP (IPER) es la relación entre el total de resultados de paquetes IP con errores y el total de resultados de transferencia satisfactoria de paquetes IP más los resultados de paquetes IP con errores en una población de interés.

6.4 Tasa de pérdida de paquetes IP (IPLR)

La tasa de pérdida de paquetes IP (IPLR) es la relación entre el total de resultados de paquetes IP perdidos y el total de paquetes IP transmitidos en una población de interés.

NOTA – En [b-IETF RFC 3357] figuran las métricas para describir patrones de pérdidas en un solo sentido. La pérdida consecutiva de paquetes tiene un interés especial en ciertas aplicaciones de tiempo real inelásticas, como por ejemplo, voz y vídeo.

6.5 Tasa de paquetes IP espurios

La tasa de paquetes IP espurios en un MP de egreso es el número total de paquetes IP espurios observados en ese MP de egreso durante un intervalo de tiempo especificado dividido por la duración del intervalo de tiempo (equivalente al número de paquetes IP espurios por segundo de servicio)¹.

6.6 Tasa de reordenación de paquetes IP (IPRR)

La tasa de reordenación de paquetes IP (IPRR) es la relación entre el total de resultados de paquetes reordenados y el total de resultados de transferencia satisfactoria de paquetes IP en una población de interés.

La Figura 10 ilustra un resultado de paquete desordenado para el paquete 2, y una tolerancia hipotética en el tiempo de llegada con una memoria intermedia de reproducción que puede restaurar el orden.

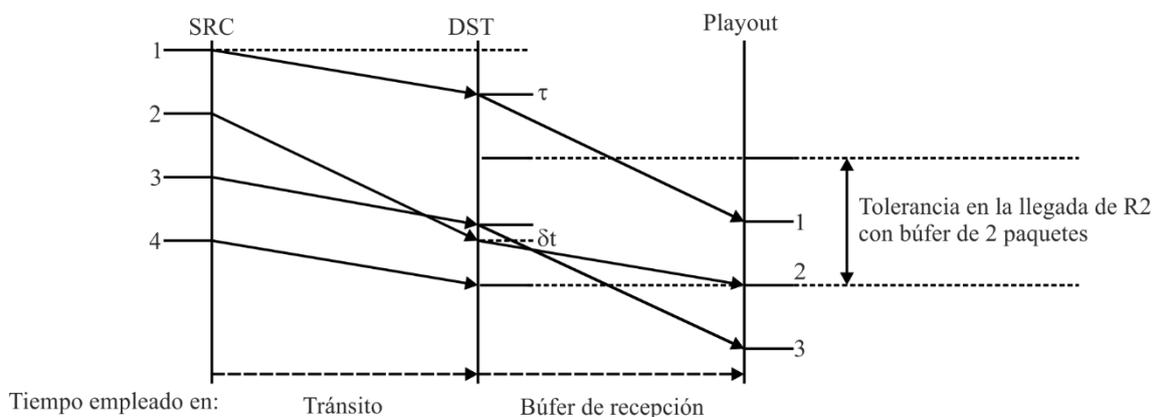


Figura 10 – Ilustración de recepción reordenada

Si es posible distinguir cada uno de los eventos de reordenación, también se podrá informar de un cómputo de eventos (junto con los criterios de eventos).

También es posible determinar el grado de reordenación de un paquete. Todo paquete cuyo número de secuencia haga que el siguiente valor esperado se incremente en más del incremento normal indicará una discontinuidad en el orden de recepción. A partir de este momento, todo paquete (reordenado) con un número de secuencia inferior al siguiente valor esperado puede cuantificarse con una distancia respecto de la discontinuidad. La distancia puede expresarse en unidades de posición, tiempo o la suma de cabidas útiles en bytes de los paquetes que intervienen. En referencia a la Figura 10, por ejemplo, cabe afirmar que el paquete 2 se recibe "tarde" por δt segundos, o 1 paquete en términos de la posición.

Consúltese [IETF RFC 4737] para conocer otros parámetros de reordenación.

¹ Puesto que previsiblemente los mecanismos que generan paquetes IP espurios tienen poco que ver con el número de paquetes IP transmitidos a través de las secciones sometidas a prueba, este parámetro de calidad de funcionamiento no se expresa como una relación, sólo como una tasa.

6.7 Tasa de bloques con pérdidas severas de paquetes IP (IPSLBR)

La tasa de bloques con pérdidas severas de paquetes IP (IPSLBR) es la relación entre los resultados de bloques con pérdidas severas de paquetes IP y el número total de bloques en una población de interés.

NOTA – Mediante este parámetro se pueden determinar múltiples cambios de trayectos IP debidos a actualizaciones de encaminamiento, también conocidas como variación de ruta, que causa una degradación importante en la mayoría de las aplicaciones de usuario.

6.8 Tasa de duplicación de paquetes IP (IPDR)

La tasa de duplicación de paquetes IP (IPDR) es la relación entre el total de resultados de paquetes IP duplicados y el total de resultados de transferencia satisfactoria de paquetes IP menos los resultados de paquetes IP duplicados en una población de interés.

6.9 Tasa de paquetes IP replicados (RIPR)

La tasa de paquetes IP replicados (RIPR) es la relación entre el total de resultados de paquetes IP replicados y el total de resultados de transferencia satisfactoria de paquetes IP menos los resultados de paquetes IP duplicados en una población de interés.

6.10 Parámetros de reparación de trenes

Lo ideal sería conocer la probabilidad de que un determinado intervalo de paquetes (o bloque de información, b) contenga más de x paquetes degradados.

$$P(b, x) = p, \text{ o bien } P(T_I, x) = p$$

La medición de los resultados de paquetes degradados que ocurren en una *población de interés* debería proporcionar una evaluación empírica de la probabilidad durante el tiempo de disponibilidad.

6.10.1 Tasa de intervalo de paquetes IP degradados (IPIIR)

La tasa de intervalo de paquetes IP degradados es la relación entre los resultados de intervalos de paquetes IP degradados y el total de intervalos no solapados en una población de interés.

6.10.2 Tasa de bloques degradados en los paquetes IP (IPIBR)

La tasa de bloques degradados en los paquetes IP (IPIBR) es la relación entre los resultados de bloques degradados de paquetes IP y el número total de bloques no solapados en una población de interés.

6.11 Parámetros de capacidad

Un servicio de transferencia de paquetes IP de extremo a extremo atraviesa una secuencia ordenada de secciones básicas desde un computador principal de origen hasta un computador principal de destino. Los parámetros de capacidad que se describen a continuación definen las propiedades de las secciones básicas en cuanto a su capacidad para transportar tráfico IP, y las propiedades correspondientes para los NSE, también denominados "trayectos". Es importante señalar que una sección básica, al igual que una secuencia de secciones básicas, está asociada a una dirección. La dirección es significativa, ya que las propiedades de una secuencia de secciones en el sentido directo no tienen por qué ser las mismas que en el sentido inverso.

Obsérvese que, a diferencia de los parámetros relacionados con el flujo definidos en la cláusula 6.12, los parámetros relacionados con la capacidad no dependen de protocolos de capa superior además de IP (por ejemplo, TCP). Asimismo, téngase en cuenta que los parámetros de capacidad utilizada, utilización y capacidad disponible no son mensurables externamente y requieren el apoyo de sistemas de comprobación técnica con acceso a las mediciones de utilización de los enlaces, etc.

6.11.1 Métrica de secciones

6.11.1.1 Bits de la capa IP transferidos

Para una determinada población de interés, los bits de capa IP transferidos se definen como ocho (8) veces el número de octetos en todos los paquetes IP que generan resultados satisfactorios de transferencia de paquetes IP en un punto de medición de egreso, desde el primer octeto del encabezamiento IP hasta el último octeto de la cabida útil de paquetes IP, ambos incluidos.

Obsérvese que esta definición es idéntica a la definición de bits de la capa IP en [IETF RFC 5136]. Además, la definición de bits de la capa IP es independiente de la versión de IP.

6.11.1.2 Capacidad de la sección de la capa IP

Para una determinada población de interés, la capacidad de la sección de la capa IP es:

$$C(t, \Delta t) = \frac{n_0(t, \Delta t)}{\Delta t}$$

siendo n_0 el mayor número (total) de bits de la capa IP que pueden transferirse por una sección básica generando resultados de transferencia satisfactoria de paquetes IP en el punto de medición de egreso durante un intervalo de tiempo especificado $[t, t + \Delta t]$.

Téngase en cuenta que se trata de una definición conceptual, antes que de una métrica que pueda medirse repetidamente. La expresión "el mayor número" de bits es algo confusa, excepto en el caso de las evaluaciones repetidas. Lo más probable es que se refiera al total de bits en los resultados de transferencia satisfactoria durante $[t, t + \Delta t]$. Véase en el anexo A una definición normativa de la capacidad de sección de la capa IP mensurable.

6.11.1.3 Capacidad de la sección utilizada de la capa IP

Para una determinada población de interés, la capacidad de la sección utilizada de la capa IP es:

$$U(t, \Delta t) = \frac{n(t, \Delta t)}{\Delta t}$$

siendo n el número real de bits de la capa IP transferidos por una sección básica generando resultados de transferencia satisfactoria de paquetes IP en el punto de medición de egreso durante un intervalo de tiempo especificado $[t, t + \Delta t]$.

6.11.1.4 Utilización de la sección de la capa IP

Para una determinada población de interés, la utilización de la sección de la capa IP $V(t, \Delta t)$ se define como la relación entre la capacidad de la sección utilizada de la capa IP $U(t, \Delta t)$ y la capacidad de la sección de la capa IP $C(t, \Delta t)$. Es decir:

$$V(t, \Delta t) = U(t, \Delta t) / C(t, \Delta t)$$

6.11.1.5 Capacidad de la sección disponible de la capa IP

Para una determinada población de interés, la capacidad de sección disponible de la capa IP, $A(t, \Delta t)$, es la parte no utilizada de la capacidad de sección de la capa IP durante un intervalo de tiempo $[t, t + \Delta t]$. Se puede calcular como la diferencia entre la capacidad de sección de la capa IP y la capacidad de sección utilizada de la capa IP. Es decir,

$$A(t, \Delta t) = C(t, \Delta t) - U(t, \Delta t)$$

o, lo que es lo mismo:

$$A(t, \Delta t) = C(t, \Delta t)(1 - V(t, \Delta t))$$

6.11.2 Métrica de NSE

6.11.2.1 Capacidad del NSE de la capa IP

La definición de la capacidad de sección de la capa IP puede hacerse extensiva a un NSE, también denominado "trayecto". Para una determinada población de interés, la capacidad del NSE de la capa IP $C_{NSE}(t, \Delta t)$ durante un intervalo de tiempo especificado $[t, t + \Delta t]$ se define como la menor capacidad de sección de la capa IP a lo largo de ese NSE. Es decir, la capacidad del NSE de la capa IP es:

$$C_{NSE}(t, \Delta t) = \min_{i=1..n} C_i(t, \Delta t)$$

siendo C_i la capacidad de la sección de la capa IP del número de sección i ($i=1..n$) en el NSE.

6.11.2.2 Capacidad del NSE disponible de la capa IP

La definición de la capacidad de sección disponible de la capa IP puede hacerse extensiva a un NSE, también denominado "trayecto". Para una determinada población de interés, la capacidad del NSE disponible de la capa IP $A_{NSE}(t, \Delta t)$ durante un intervalo de tiempo especificado $[t, t + \Delta t]$ se define como la menor capacidad de sección disponible de la capa IP a lo largo de ese NSE. Es decir,

$$A_{NSE}(t, \Delta t) = \min_{i=1..n} A_i(t, \Delta t)$$

siendo A_i la capacidad de la sección disponible de la capa IP del número de sección i ($i=1..n$) en el NSE. Téngase en cuenta que el número de sección que determina la capacidad del NSE disponible de la capa IP puede diferir del número de sección que determina la capacidad del NSE de la capa IP.

6.11.2.3 Capacidad de la sección ajustada de la capa IP

Para una determinada población de interés, la sección ajustada de la capa IP se define como la sección de un NSE con la menor capacidad de sección disponible de la capa IP. Téngase en cuenta que, si hay varias secciones que cumplen esta condición, la sección ajustada de la capa IP no está definida unívocamente.

Para una determinada población de interés, la capacidad de la sección ajustada de la capa IP de un NSE es la capacidad de la sección ajustada de la capa IP.

Obsérvese que la capacidad de sección disponible de la capa IP de la sección ajustada de la capa IP es igual a la capacidad disponible de NSE de la capa IP. Es decir, la capacidad de la sección ajustada de la capa IP es:

$$C_{TL}(t, \Delta t) = C_i(t, \Delta t) \text{ por lo que } A_i(t, \Delta t) = A_{NSE}(t, \Delta t)$$

Téngase en cuenta que la sección ajustada de la capa IP no ha de ser necesariamente la misma que la que determina la capacidad del NSE de la capa IP.

6.11.3 Variabilidad

Cada métrica de capacidad P representa un valor medio en un intervalo de tiempo $[t, t + \Delta t]$. Para un conjunto de observaciones consecutivas $P_1..P_N$ respecto de un determinado parámetro P a lo largo de un intervalo $[T, T + \Delta T]$, siendo $T > t$, cabe utilizar el promedio, la desviación típica y los cuantiles para describir la variabilidad.

6.11.3.1 Promedio

El promedio se calcula como:

$$a_p(T, \Delta T) = \frac{1}{n} \sum_{i=1..n} P_i(t, \Delta t)$$

6.11.3.2 Desviación típica

La desviación típica se calcula como:

$$s_p(T, \Delta T) = \sqrt{\sum_{i=1..n} (P_i(t, \Delta t) - a_p(T, \Delta T))^2}$$

6.11.3.3 Cuantiles

Para una lista ordenada de N valores $P_1..P_n$, el k ésimo cuantil 100 (es decir, el k ésimo percentil) se define como:

$$P_I : I = \left\lceil N \frac{k}{100} \right\rceil$$

siendo P_I el valor de los datos correspondiente al k ésimo cuantil 100. (El símbolo $\lceil \rceil$ significa que, si $N \frac{k}{100}$ no es un número entero, debería redondearse al siguiente número entero superior para obtener el índice de lista I .)

Los cuantiles para el valor mínimo ($k = 0$), mediano ($k = 50$) y máximo ($k = 100$) son de especial interés y deberían comunicarse. También pueden utilizarse otros cuantiles, como $k = 95$ o $k = 99$.

6.12 Parámetros relacionados con el flujo

Conviene caracterizar la calidad de funcionamiento en términos de parámetros relacionados con el flujo o el caudal que evalúan la capacidad de las redes o secciones IP de transportar cantidades de paquetes IP. Hay que tener en cuenta que un parámetro destinado a caracterizar el caudal de una aplicación IP no sería igual a la cantidad de recursos (capacidad) disponibles para esa aplicación (cuantificada en la cláusula 6.11 y medida con los métodos del Anexo A). Esto es así porque los protocolos de capa superior que emplean el control de flujo de bucle cerrado sobre IP (por ejemplo, el control de flujo TCP) también influyen en el caudal de la capa IP.

En la presente versión de esta Recomendación, se recomienda que los parámetros relacionados con el flujo o el caudal cumplan los siguientes requisitos:

- 1) Un parámetro que caracterice el caudal ofrecido a un servicio IP deberá poner en relación la cantidad de paquetes IP transportados de manera satisfactoria por una red o sección IP con la cantidad de parámetros IP que fueron entregados en esa red o sección.
- 2) Los parámetros relacionados con el caudal deberán aplicarse a una red IP de extremo a extremo y al transporte IP a través de un EL, una NS o un NSE.

Algunos parámetros relacionados con el flujo o el caudal tratan de caracterizar la capacidad de caudal de una red IP, es decir, las posibilidades que tiene la red de mantener una determinada tasa de transferencia de paquetes IP. Se recomienda que cualesquiera de esos parámetros y métodos de medición cumplan los siguientes requisitos adicionales:

- 1) Deberá describir el esquema del tráfico ofrecido a la red o sección IP, ya que la capacidad de la red o sección IP de entregar de manera satisfactoria esos paquetes depende de dicho esquema de tráfico.
- 2) La tasa a la que se ofrece el tráfico no deberá ser superior a la capacidad (en bits por segundo) del enlace que conecta las secciones sometidas a prueba con las secciones de destino no sometidas a prueba.

- 3) En cualquier declaración individual sobre la calidad de funcionamiento del caudal deberá indicarse el tipo de paquetes IP de que se trata (donde el tipo incluye la versión IP, la presencia de encabezamientos de extensión, el protocolo de la capa de transporte, los demás encabezamientos de protocolo y cualquier otra información pertinente, como la longitud de los paquetes utilizados).
- 4) Algunas formas de control de flujo aplicadas en la capa IP o superior pueden dar lugar a errores de medición. Por ejemplo, una medición de caudal de la capa IP que está sujeta a un seguimiento de acuse de recibo de capa superior, a limitaciones de tamaño de ventana y/o a un control de flujo para mitigar la congestión (por ejemplo, TCP) requiere la evaluación y el informe del error de medición asociado. El error de medición indica la posible capacidad no utilizada de la capa IP cuando se comparan las especificaciones del servicio de Internet y los resultados de los métodos que utilizan el control de flujo.

También se recomienda seguir las directrices para los parámetros relacionados con el caudal y su medición, que se encuentran en el marco IETF RFC 3148 para las métricas de capacidad de transferencia en bloque (BTC).

Los parámetros relacionados con el flujo y el caudal se especifican en el Anexo A. En el Apéndice IX se describe cómo las mediciones que utilizan TCP no cumplen los requisitos de esta cláusula.

NOTA – El Apéndice III (parámetros relacionados con la velocidad y la capacidad de caudal) queda obsoleto en la edición de 2019.

7 Disponibilidad de servicio IP

La disponibilidad de servicio IP es aplicable a los servicios IP de extremo a extremo, a secciones básicas y a un NSE.

Una función de disponibilidad (definida en la cláusula 7.1) sirve para dividir el tiempo de servicio programado total de un servicio IP en periodos disponibles e indisponibles. Sobre la base de esta clasificación se definen en la cláusula 7.2 los porcentajes de disponibilidad y de indisponibilidad del servicio IP. Por último, un modelo de dos etapas de disponibilidad de servicio IP sirve para definir en la cláusula 7.2 los parámetros de disponibilidad conexos.

NOTA – A menos que un proveedor del servicio IP indique otra cosa, se supone que el tiempo de servicio programado para un servicio IP es de 24 horas al día, siete días a la semana.

7.1 Función de disponibilidad de servicio IP

La función de disponibilidad de un servicio IP se basa en un umbral de la característica IPLR.

El servicio IP está disponible de extremo a extremo si la IPLR de ese caso de extremo a extremo es inferior al umbral c_1 definido en el Cuadro 1.

Cuadro 1 – Función de disponibilidad de servicio IP

Criterio de interrupción	Umbral
IPLR > c_1	$c_1 = 0,20$
<p>NOTA – El valor de 0,20 de c_1 se considera provisional y queda en estudio. El valor provisional anterior de c_1 era de 0,75. También se han propuesto los valores de 0,9 y 0,99 para c_1. Ahora bien, en el momento de la aprobación de esta Recomendación, la mayoría de las causas de indisponibilidad parecen provenir de fallos en los que la tasa de pérdidas es fundamentalmente del 100%, y muchas aplicaciones de redes IP dejan de funcionar cuando la tasa de pérdidas es >0,20. Cuando las redes IP soportan múltiples calidades de servicio, quizá convenga considerar valores diferentes de c_1 para los diferentes servicios. En ese caso, se han sugerido valores de c_1 entre 0,03 y 0,2 (obtenidos a partir de la resiliencia de los codificadores vocales diferentes) para los servicios que ofrecen clase 0 o clase 1 UIT-T Y.1541 y un c_1 de 0,75 para la clase 5 UIT-T Y.1541.</p> <p>El umbral c_1 solo se ha de utilizar para determinar cuando los recursos de la red IP son (temporalmente) incapaces de soportar un servicio útil de transferencia de paquetes IP. El valor de c_1 no deberá considerarse como una indicación de la característica IPLR ni como un objetivo adecuado de IPLR para cualquier aplicación IP. Los objetivos de calidad de funcionamiento establecidos a propósito de la IPLR deberán excluir todos los periodos de indisponibilidad del servicio, es decir, todos los intervalos de tiempo en los que la $IPLR > c_1$.</p>	

Respecto a un par de SRC y DST determinado, *una sección básica o un NSE están disponibles para el caso independiente del ingreso*, si la IPLR de ese par es inferior al umbral c_1 , medido en todos los MP de ingreso permisibles.

Respecto a un par de SRC y DST determinado, *una sección básica o un NSE están disponibles para el caso de ingreso específico*, si la IPLR de ese par es inferior al umbral c_1 , medido a partir de un MP de ingreso permisible.

NOTA 1 – Desde la perspectiva de las operaciones, será posible medir y/o supervisar la disponibilidad a partir de un MP de ingreso específico y utilizar a continuación esa información para establecer deducciones sobre la disponibilidad con independencia del ingreso.

NOTA 2 – La relación cuantitativa entre la disponibilidad de un servicio IP de extremo a extremo y la disponibilidad del servicio IP de la sección básica o el NSE sigue siendo objeto de estudio.

Si el criterio de interrupción indicado en el Cuadro 1 se cumple (es decir, la IPLR supera su umbral), el servicio IP está en el estado de indisponibilidad (sufrir una interrupción). El servicio IP está en el estado de disponibilidad (ausencia de interrupción) si no se cumple el criterio de interrupción. El número mínimo de paquetes que se deberán utilizar para evaluar la función de disponibilidad del servicio IP es M_{av} (el valor de M_{av} queda en estudio. Cuando en las pruebas de disponibilidad se utiliza tráfico generado por el usuario extremo, se ha sugerido un valor de M_{av} igual a 60 paquetes, distribuidos dentro de T_{av} a un paquete por segundo). La duración mínima del intervalo de tiempo durante el cual se ha de evaluar la función de disponibilidad del servicio IP es T_{av} . T_{av} se ha fijado provisionalmente en un minuto. El estudio ha demostrado que este valor es coherente con los límites prácticos impuestos al funcionamiento de la capa IP. La supervisión de la calidad de funcionamiento de capas inferiores y de los fallos en los elementos de red puede permitir determinar indisponibilidades inminentes en un menor plazo y aplicar las medidas correctivas). En el Apéndice VI se explica la definición actual de la función de disponibilidad del servicio IP y los valores de T_{av} y c_1 .

NOTA 3 – Se prevé que el criterio de interrupción basado en la IPLR caracterice de manera satisfactoria la disponibilidad del servicio IP. Sin embargo, la disponibilidad del servicio IP también podría tener en cuenta una calidad de funcionamiento severamente degradada por lo que se refiere a la IPER y/o la tasa de paquetes IP espurios. La inclusión de parámetros de decisión de disponibilidad adicionales y sus correspondientes umbrales queda en estudio.

NOTA 4 – Esta definición unidireccional de disponibilidad viene motivada por el hecho de que los paquetes IP atraviesan a menudo del SRC al DST rutas muy diferentes de las que atraviesan del DST al SRC. Si, desde la perspectiva de un usuario de la red IP, se necesita una definición de disponibilidad bidireccional, dicha definición se puede derivar fácilmente a partir de la presente definición unidireccional, sumando el tiempo no disponible no solapado del trayecto inverso.

Se pretende que esta definición de disponibilidad de servicio IP sea aplicable tanto al tráfico IP generado por el usuario de extremo (es decir, el flujo normal de paquetes IP entre el SRC y el DST) como al tráfico generado por aparatos y sistemas de prueba. En cualquier caso, el origen del tráfico IP deberá estar documentado cuando se notifiquen los resultados relativos a la disponibilidad. Dicha documentación deberá incluir los tipos específicos de paquetes utilizados en cada sentido del flujo.

El tráfico generado de manera específica para probar el estado de disponibilidad deberá limitarse de tal modo que no provoque una congestión. La congestión podría afectar a otro tráfico y/o podría aumentar de manera significativa la probabilidad de que se superara el criterio de interrupción.

En el Apéndice IV figura más información sobre la determinación del estado de disponibilidad.

7.2 Parámetros de disponibilidad de servicio IP

7.2.1 Porcentaje de indisponibilidad del servicio IP (PIU)

El porcentaje de indisponibilidad del servicio IP (PIU) es el porcentaje del tiempo de servicio IP programado total (porcentaje de intervalos $_{av}$) que se clasifica como periodo indisponible utilizando la función de disponibilidad de servicio IP.

7.2.2 Porcentaje de disponibilidad del servicio IP (PIA)

El porcentaje de disponibilidad del servicio IP (PIA) es el porcentaje del tiempo de servicio IP programado total (porcentaje de intervalos $_{av}$) que se clasifica como periodo disponible utilizando la función de disponibilidad de servicio IP; el PIU y el PIA se relacionan del siguiente modo:

$$PIU = 100 - PIA$$

NOTA – Puesto que la IPLR aumenta normalmente al aumentar la carga ofrecida del SRC al DST, la probabilidad de que se rebase el umbral c_1 aumenta al aumentar la carga ofrecida. Por consiguiente, los valores del PIA probablemente sean menores cuando la demanda de capacidad entre el SRC y el DST sea mayor.

El Apéndice IV contiene información sobre muestreo para determinar el PIA y el PIU.

Anexo A

Parámetros de capacidad y relacionados con el flujo basados en IP y métodos de medición

(El presente anexo forma parte integrante de esta Recomendación.)

A.1 Antecedentes

La normalización de las arquitecturas de medición que caracterizan "el servicio de Internet" comenzó en 2013. Un producto de acceso a la red destinado a los consumidores que soporta el protocolo Internet es una forma común de conectarse a Internet. Tradicionalmente, la mayoría de las aplicaciones de consumo se comunican utilizando el transporte TCP, que proporciona una transmisión fiable de datagramas. Al tratar de caracterizar un servicio de Internet mediante mediciones normalizadas, se han utilizado métodos de caracterización de las propiedades de la capa de transporte TCP para evaluar las propiedades de Internet o de la capa de enlace, como el ancho de banda de acceso. Se ha planteado la preocupación de que este enfoque no funcione correctamente y se han propuesto métodos alternativos para caracterizar los servicios de acceso a Internet de los consumidores sobre la base de las mediciones.

Al mismo tiempo, existe una fuerte tendencia a sustituir el transporte TCP por el transporte UDP, las cabidas útiles por segmentos abiertos y encriptados, y la retransmisión y el control de la congestión de la capa de aplicaciones. El uso del protocolo QUIC de Google y la inminente aprobación del protocolo QUIC del IETF [b-QUIC] conllevarán una rápida modificación del panorama del transporte en Internet, y los consumidores que utilizan los navegadores más populares son/serán algunos de los primeros usuarios en adoptarlos.

En el presente anexo se especifican los parámetros y métodos para la medición del ancho de banda de acceso de la capacidad máxima de la capa IP. En el futuro, los parámetros y el método de medición relacionados con el flujo (rendimiento de transporte) podrán especificarse aquí tras un estudio más profundo. Estos parámetros y métodos de medición son plenamente aplicables tanto a los abonados a los servicios de Internet (usuarios finales) como a los proveedores de servicios de Internet, con la advertencia de que los puntos de medición de ingreso y egreso seleccionados determinan plenamente la aplicabilidad al comparar las mediciones con las especificaciones de servicio de la capa IP.

La Comisión de Estudio 12 (CE 12) del UIT-T tiene experiencia en la elaboración de normas de medición y modelización para las telecomunicaciones. Además, dispone de conocimientos sobre metodología estadística y conjuntos de herramientas que permiten una comparación objetiva entre las mediciones y los métodos de modelización propuestos. La utilización de los conocimientos y métodos de la CE 12 para decidir sobre la aplicabilidad de las propuestas competidoras relacionadas con la caracterización del "servicio de Internet para consumidores" se considera una buena manera de pasar de un intercambio de opiniones a una prueba y comparación de conceptos en condiciones de ensayo reproducibles. En [b-UIT-T P.800] se establecen los siguientes requisitos:

Es importante especificar y establecer correctamente las condiciones simuladas en la prueba, realizar mediciones precisas antes y después de cada experimento, ... y llevar registros fieles de los resultados de cada prueba.

El IETF aprobó y publicó el documento RFC 8337, "Model-Based Metrics for Bulk Transport Capacity", en marzo de 2018 [IETF RFC 8337]. El trabajo de métricas basadas en modelos (MBM) fue el resultado de muchos años de análisis del problema de la medición de la capacidad de transporte, principalmente en el Grupo de Trabajo sobre Métrica de la calidad de funcionamiento IP (IP Performance Metrics, IPPM) del IETF. En la especificación se describen minuciosamente los numerosos problemas y dificultades de repetibilidad cuando se realizan pruebas con TCP conforme a la norma (sección 4), y se resuelven estos problemas principalmente mediante el diseño de un método y un conjunto de pruebas de diagnóstico en las que se desactiva el control de flujo de TCP.

El método conlleva la evaluación de la calidad de funcionamiento de un transporte objetivo en términos de velocidad de transmisión y tiempo de ida y vuelta (RTT).

Hasta esta Recomendación, se disponía de herramientas (por ejemplo, iPerf) y de algunas referencias a las mediciones de capacidad IP basadas en UDP en normas e informes publicados. En la actualidad, el sector considera que la entrega de una norma de medición y una herramienta conforme es la forma ideal de presentar nuevas métricas y métodos. Este anexo proporciona una especificación suficientemente detallada para que se obtengan resultados estadísticamente equivalentes en la implementación (como se describe en [b-IETF RFC 6576] a partir de la labor del IPPM). Se proporcionará por separado una herramienta de medición que sea conforme con este anexo.

En este anexo se incluye el plan de pruebas para evaluar los métodos de medición pertinentes. El plan de pruebas utiliza los principios de la CE 12 de [b-UIT-T P.800] para establecer una "referencia real" que permita comparar los métodos de medición propuestos. Las pruebas se dividieron en fases: Las pruebas de laboratorio se llevaron a cabo de acuerdo con el plan de la fase 1, en la que se pudieron examinar en condiciones controladas la aplicación de la "referencia real", los límites de la plataforma de pruebas y los métodos de medición propuestos. Las pruebas de la fase 2 se realizaron sobre el terreno, según el plan de pruebas.

Los resultados resumidos de la evaluación (basados en el plan de pruebas) se proporcionan en el Apéndice X (informativo), tanto para las pruebas de laboratorio de la fase 1 como para las de la fase 2 realizadas sobre el terreno. Otros apéndices proporcionan información recopilada para apoyar el consenso desarrollado aquí, y detalles adicionales sobre los cálculos y los factores de conversión entre las mediciones en diferentes capas.

A.2 Parámetros de capacidad de acceso de la capa IP y métodos de medición (acceso de los consumidores a Internet)

A.2.1 Definición de la métrica de capacidad IP medible

En la cláusula 6.11.1.2 se define un parámetro idealizado para la capacidad de sección de la capa IP, que evalúa el "mayor número (total) de bits de la capa IP que pueden transferirse ... durante un intervalo de tiempo especificado $[t, t + \Delta t]$ ". En la presente cláusula se define una versión medible (más práctica) de la definición idealizada.

Para una población de interés dada, la capacidad máxima de sección de la capa IP durante el intervalo de tiempo $[t, t + \Delta t]$ es:

$$\text{máxima } C_{-}(t, \Delta t) = \frac{\text{máx}_{[t, \Delta t]}(n_0(dt_n, dt_{n+1}))}{dt}$$

donde:

el intervalo de tiempo $[t, t + \Delta t]$ se compone de x subintervalos iguales de duración dt ;

n_0 es el número total de bits de encabezamiento y de cabida útil de la capa IP que pueden transferirse por una sección básica generando resultados de transferencia satisfactoria de paquetes IP en el punto de medición de egreso durante un intervalo de tiempo especificado, desde $[dt_1, dt_2]$ u otros intervalos de duración dt , y

la máxima $C(t, \Delta t)$ corresponde al valor máximo de n_0 medido en cualquier subintervalo $[dt_n, dt_{n+1}]$ dentro del intervalo de tiempo $[t, t + \Delta t]$, dividido por la duración del subintervalo.

Obsérvese que se utilizará el transporte UDP cuando se evalúe la métrica de capacidad IP medible.

El método de medición necesita también una definición para su tasa de envío, según se indica a continuación.

A.2.1.1 Velocidad binaria de envío de paquetes IP (IPSBR)

Para una determinada población de interés, la velocidad binaria de envío de paquetes IP (IPSBR) generada por un emisor en un MP de ingreso es 8 veces el número total de octetos transmitidos en los encabezamientos y cabidas útiles de paquetes IP que dan lugar a un evento de referencia de transferencia de paquetes IP en ese MP de ingreso durante un intervalo de tiempo especificado, dividido por la duración del intervalo de tiempo. De manera equivalente, el número de bits en los encabezamientos y cabidas útiles de paquetes IP que dan lugar a eventos de referencia de paquetes IP por servicio-segundo.

A.2.2 Método de medición

Los pasos generales del método (procedimiento) son los siguientes:

- El emisor se encargará de enviar y recibir el tren de paquetes IP utilizando la capa de transporte UDP con los parámetros clave definidos, a saber:
 - τ el tipo de paquete, incluyendo las longitudes del encabezamiento y de la cabida útil, los encabezamientos y las opciones presentes y cualquier marca para un tratamiento especial en la red;
 - τ la tasa inicial/variable de envío de paquetes durante un intervalo de tiempo especificado (por ejemplo, el intervalo compatible con el parámetro HZ, muy inferior a dt , que es el subintervalo a efectos de informes durante las pruebas);
 - τ la longitud, duración y características de un preámbulo de prueba o fase de iniciación (esencial para ciertos tipos de redes, como las redes móviles);
 - τ la disciplina de envío específica, que incluye las ráfagas permitidas o previstas (envíos consecutivos).
- Durante una prueba, la tasa de envío deberá variar de acuerdo con un algoritmo de búsqueda especificado, con:
 - un objetivo de búsqueda especificado, que incluye uno o más parámetros medidos y sus correspondientes umbrales operativos, así como la tolerancia por encima y por debajo de dichos umbrales;
 - σ la duración especificada de los ensayos, que se componen de los pasos individuales de un algoritmo de búsqueda;
 - τ el conjunto de mediciones en subintervalos, dt , que sustentan el resumen de las mediciones realizado al final de cada ensayo;
 - τ la duración máxima del proceso de búsqueda (límite de tiempo).

Habrà un algoritmo de búsqueda obligatorio especificado en este anexo; los demás algoritmos son de aplicación obligatoria u opcional (como se especifica en la cláusula o el anexo que contiene el algoritmo). El uso de un algoritmo de búsqueda obligatorio u opcional se comunicará al usuario junto con los resultados.
- Todas las mediciones (resultados de los ensayos) recogidas durante la búsqueda se almacenarán como series temporales para permitir el análisis del proceso de búsqueda.
- Deberà haber un procesamiento posterior definido de todas las mediciones (resultados de los ensayos) recogidas a lo largo de la búsqueda, para determinar el valor o valores resumidos finales de un proceso de búsqueda particular. Entre otros ejemplos (para la tasa de recepción, o aquí, la capacidad medida, otros parámetros son la latencia, la pérdida y la reordenación) cabe citar los siguientes:
 - calcular un promedio de todos los valores medidos de la tasa de recepción para todos los ensayos;

calcular un promedio de todos los valores medidos de la tasa de recepción en los que se ha cumplido el objetivo de búsqueda;

calcular un máximo de todos los valores medidos de la tasa de recepción en los que se ha cumplido el objetivo de búsqueda;

calcular un promedio de todos los valores medidos de la tasa recibida para todos los ensayos en los que se ha cumplido un criterio de exclusión de resultados especificado (por ejemplo, la eliminación de valores atípicos, según los criterios especificados);

resumen de los parámetros relacionados (véase la cláusula A.2.3).

- Habrá criterios definidos para invalidar los resultados de un determinado proceso de búsqueda, como la detección de que no se ha alcanzado la velocidad de envío requerida, o la detección de tráfico competidor (pero este tráfico no puede detectarse exhaustivamente en todas las circunstancias).
- Cuando se repitan las pruebas para examinar la coherencia de los resultados o por otros motivos, el proceso de resumen de los resultados debería incluir el correspondiente análisis posterior a la prueba para garantizar la calidad de los datos y detectar y excluir datos parásitos (cuando sea posible). Los métodos de análisis posteriores a las pruebas, en su caso, se publicarán con los resultados.
- Seguridad: El receptor de la prueba (o el servidor) procederá a aceptar las solicitudes de prueba solo de la población de usuarios autorizados, y rechazará las demás.
- Capacidad: El receptor de las pruebas (o servidor) procederá a aceptar las solicitudes de prueba solo cuando se disponga de suficientes recursos de computador principal e interfaz, y rechazará las solicitudes cuando no se cumpla esta condición.
- Comunicación de resultados: El sistema de medición informará de la capacidad máxima de IP, el índice de pérdida de paquetes IP de prueba y demás métricas cuando estén disponibles (véase la cláusula A.2.4). El sistema de medición también podrá informar de la capacidad UDP en términos de bits de cabida útil UDP entregados, ya que se trata de la capacidad disponible para las aplicaciones de usuario una vez eliminados los encabezamientos IP y UDP.

A.2.2.1 Algoritmo de búsqueda obligatorio

El sistema de medición cumple los requisitos de la cláusula A.2.2, y añade las siguientes capacidades para apoyar el algoritmo de búsqueda:

- 1) El probador debería formular una recomendación sobre el tamaño máximo de los paquetes de prueba, y permitir cierta tara inesperada para evitar la fragmentación.
- 2) Hay un cuadro que contiene las tasas de transmisión (IPSBR), el número de paquetes enviados durante cada intervalo y los tamaños de los paquetes. El cuadro muestra valores ascendentes para las tasas de carga ofrecidas, entre las tasas de carga mínima y máxima soportadas, ambas incluidas.
- 3) El receptor de la carga ofrecida medirá los siguientes parámetros: tasa recibida, pérdida, reordenamiento, variación de retardo (según esta Recomendación) y retardo de ida y vuelta [Y.1565].
- 4) El receptor de la carga ofrecida enviará periódicamente al emisor un mensaje de retorno con información de estado en el que se incluirán los resultados de las métricas realizadas.
- 5) Basándose en los resultados que figuren en el mensaje de retorno con información de estado, el emisor ajustará su carga ofrecida de acuerdo con el diagrama de flujo de la Figura A.1. En el diagrama de flujo, "un paso" es un cambio en la velocidad que se logra utilizando un nuevo valor (en la fila superior o inferior a la fila actual del envío) en el cuadro de velocidades de carga ofrecidas.

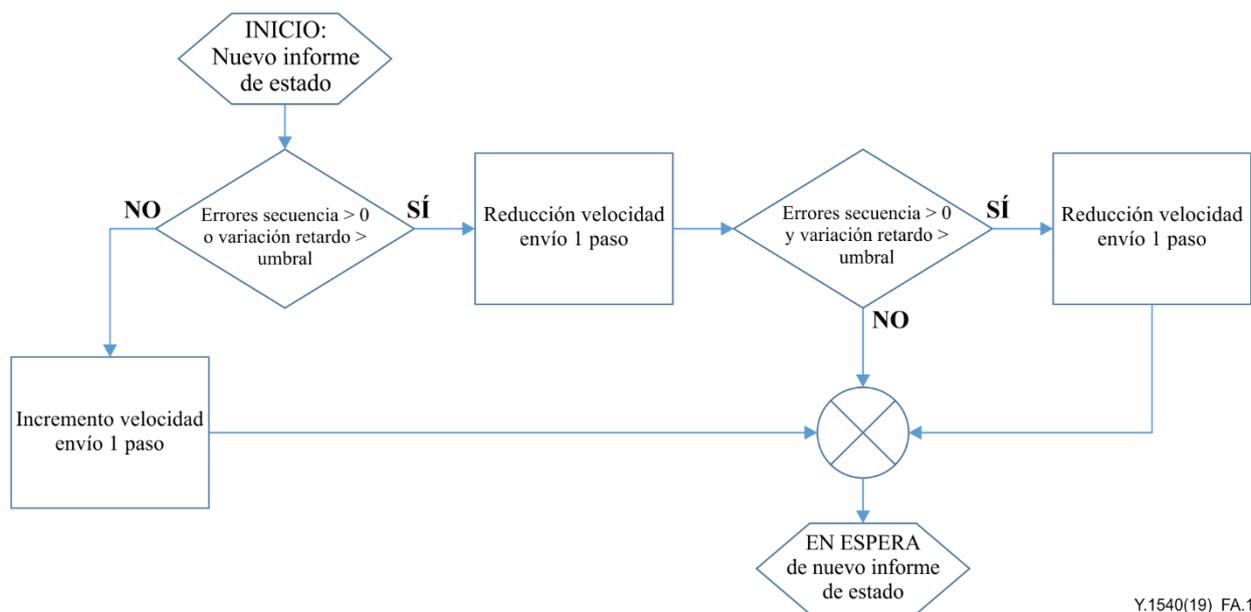


Figura A.1 – Diagrama de flujo para el ajuste de la carga ofrecida como parte de un algoritmo de búsqueda

NOTA – Las decisiones algorítmicas podrían ser ejecutadas por uno de los dos computadores principales participantes en el sistema de medición, lo que permitiría que la implementación en el otro computador principal fuera mucho menos compleja e independiente de la versión del algoritmo. Esto también permite actualizar el algoritmo en un computador principal más accesible.

En el futuro, los algoritmos de búsqueda alternativos, obligatorios u opcionales se especificarán en anexos separados.

A.2.3 Medición de la tasa de pérdida de paquetes IP (IPLR) de prueba

Para una determinada población de interés, la tasa de pérdida de paquetes IP (IPLR) de prueba es la relación entre el total de resultados de paquetes IP perdidos y el total de resultados de paquetes IP perdidos más satisfactorios durante cada prueba (o subintervalo, dt).

Téngase en cuenta que la IPLR de prueba varía ligeramente de la definición de IPLR en el cuerpo del texto, porque no es posible usar un tiempo de espera largo (T_{max}) para distinguir los resultados de paquetes satisfactorios de los resultados de paquetes perdidos cuando se evalúan los resultados de cada prueba (o subintervalo, dt) y se transfieren inmediatamente los resultados al algoritmo de búsqueda. Los paquetes inusualmente retardados o reordenados se contabilizarían en las mediciones de los ensayos posteriores, en todos los parámetros, incluida la IPDV.

A.2.4 Parámetros y métodos conexos

Claramente, la IPLR de prueba, el IPTD (evaluado como tiempo de transferencia de ida y vuelta, o latencia RT, de acuerdo con el parámetro en [Y.1565]) y la IPDV son de interés y se informará al respecto junto con el resumen final de la tasa recibida (capacidad medida).

Se podrán medir también otros parámetros:

- la duración real del proceso de búsqueda (se pretende que sea Δt);
- el número total de paquetes perdidos observados durante el proceso de búsqueda;
- la gama y la variación de los resultados a lo largo de procesos de búsqueda repetidos.

A.3 Parámetros de caudal relacionados con el flujo y los métodos de medición conexos (transporte de entrega fiable)

Esta cláusula, que queda en estudio, especificará las métricas y los métodos de medición para el caudal relacionado con el flujo, de conformidad con la cláusula 6.12 de la presente Recomendación. Obsérvese que en el Apéndice X de esta Recomendación se explica por qué el TCP normal con control de flujo de bucle cerrado no cumple estos requisitos. En el Apéndice XIII de esta Recomendación se describe una propuesta de métrica y método que cumple los requisitos de la cláusula 6.12.

A.3.1 Definición de los parámetros

Queda en estudio; véase el Apéndice XIII.

A.3.2 Método de medición

Queda en estudio.

A.3.3 Parámetros y métodos conexos

Queda en estudio.

A.4 Plan para calificar y comparar los métodos de medición del acceso

La Recomendación UIT-T P.800 y otras Recomendaciones de esa serie, aunque se centran principalmente en la voz, proporcionan una orientación general sobre cómo establecer, realizar y evaluar campañas de medición con el objetivo de comparar los modelos basados en datos de medición con condiciones reales. Para comprender las capacidades y los límites de las pruebas, las herramientas y los resultados diseñados para caracterizar los tipos de acceso a Internet, es útil seguir un proceso similar, según se describe a continuación.

Se debería organizar un conjunto de diversas condiciones de transmisión para las pruebas de laboratorio. En primer lugar, deberían definirse las condiciones de transmisión que se aproximan a las condiciones operacionales reales. Las condiciones deberían ser estables y verificables durante las pruebas, utilizando equipos de medición de laboratorio. A continuación, cada método diseñado para caracterizar los distintos tipos de acceso a Internet puede probarse con un conjunto de condiciones diversas. Se pueden caracterizar los errores de medición. A partir de los resultados obtenidos con cada parámetro y método, cabe identificar los ámbitos operacionales (condiciones) en que un método de medición es ventajoso y aquellos en que es menos fiable (y se pueden cuantificar las fuentes de error de medición).

A continuación se enumeran las condiciones de ensayo.

A.4.1 Puntos de medición

En [b-IETF RFC 7398] se define una ruta de referencia y puntos de medición para las métricas de calidad de funcionamiento más utilizadas. Otros proyectos de medición similares también pueden utilizar las extensiones aquí descritas para la localización de puntos de medición. La finalidad de [b-IETF RFC 7398] es crear una forma eficiente de describir la ubicación del punto o puntos de medición utilizados para realizar una determinada medición, especialmente señalando en qué momento una medición incluye subtrayectos gestionados y no gestionados (red privada).

Obsérvese que la ruta de medición, delimitada por los puntos de medición [b-IETF RFC 7398], determina la aplicabilidad de los parámetros de suscripción, como las tasas de datos típicas ofrecidas, y la cuestión de si los parámetros de suscripción informan la selección de parámetros como `target_data_rate` (velocidad de datos objetivo) de la MBM [IETF RFC 8337]. Lo mismo cabe decir de parámetros como el tamaño de trama utilizado en las pruebas UDP, al tener en cuenta la capa en la que se inserta el tráfico de prueba, para evitar la fragmentación.

A.4.2 Condiciones de prueba

Todas las configuraciones y el comportamiento del tráfico de fondo deberían ser lo más parecidos posible a las condiciones operacionales de la red. Se propone definir una prueba de referencia y luego variar los parámetros de prueba. Esta es la fase 1 de las pruebas.

A.4.2.1 Condiciones de las pruebas de laboratorio de la fase 1

De conformidad con los requisitos del ORECE [b-ORECE], la primera fase de pruebas se hará con conformadores de tráfico (y con reguladores de tráfico de hasta 10 Mbps, [b-Google-Police]), y el probador debe conocer la capa donde los conformadores, reguladores, observadores pasivos, remitentes, receptores y resultados de la prueba miden los paquetes. Además, se implementarán y probarán las degradaciones de la red, como el retardo.

La figura siguiente ilustra dos utilidades diferentes que proporcionan un control flexible del tráfico/velocidad en una plataforma informática genérica. Las diferentes utilidades de control de tráfico pueden aplicarse de tres maneras.

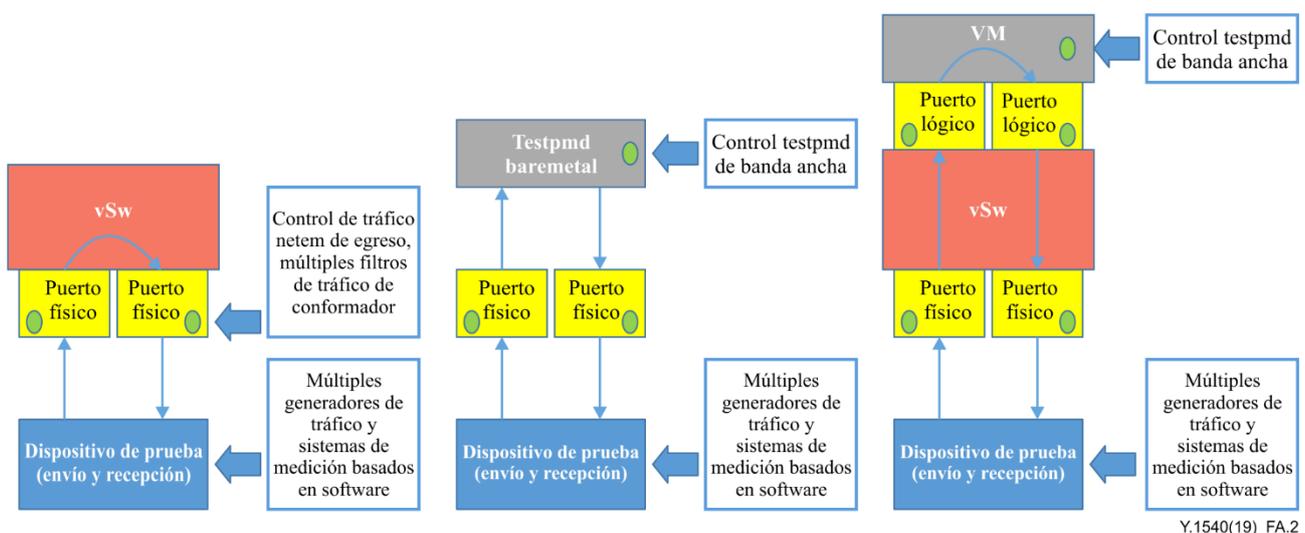


Figura A.2 – Tres trayectos de prueba alternativos en una plataforma informática genérica

En la Figura A.2, el dispositivo de prueba está conectado a un computador principal genérico general mediante enlaces físicos a 10 Gbps. El dispositivo de prueba también es un computador principal genérico, pero está completamente aislado del computador principal que realiza el control del tráfico, lo que permite que cada nodo dedique recursos a sus funciones únicas en el entorno de prueba. A través del nodo de control de tráfico se pueden instalar y probar diferentes implementaciones de métodos de medición.

Hay tres formas de implementar la función de conformación del tráfico. La primera, que se muestra a la izquierda, emplea el emulador equipado con el kernel de Linux, netem, que puede emular el retardo y ayudar al control del tráfico, una vez configuradas la tarjeta de interfaz de red (NIC) y las interfaces físicas correctas. El vSwitch simplemente conmuta las tramas entre sus dos puertos. Esta configuración se denomina comúnmente "phy2phy".

La segunda forma (centro de la figura) presupone la instalación y configuración de la utilidad testpmd de Intel DPDK, a fin de realizar el reenvío de tramas entre las interfaces físicas correctas, junto con el control del ancho de banda que pasa por el trayecto de reenvío.

En la última forma (parte derecha de la figura) se utiliza testpmd instalada en una máquina virtual, o VM, y se emplea un vSwitch con configuración para conectar las interfaces físicas a los puertos correctos en la VM. De nuevo, testpmd (u otra utilidad que se ejecute en la VM) controla el ancho de banda del trayecto entre los puertos lógicos.

Estas tres configuraciones son posibles en el POD del proyecto OPNFV VSPERF, asignado para las pruebas, el desarrollo y las evaluaciones mediante la herramienta VSPERF [b-Pod12].

Por lo tanto, se pueden aplicar diferentes condiciones para las pruebas individuales. En cada prueba, solo se cambia una propiedad con respecto a la prueba de referencia, mientras que todas las demás propiedades de la configuración permanecen inalteradas.

- El ancho de banda del conformador/regulador se ajusta a las velocidades sugeridas por el ORECE, hasta la gama de Gbps, y deberá someterse a pruebas.
- Los RTT se ajustan a los siguientes valores: 5, 10, 20, 40 ms.
- La tasa de pérdida de paquetes aleatoria se ajusta a los siguientes valores: 0, 10^{-4} , 10^{-5} .
- La tolerancia a las ráfagas del conformador puede establecerse en 0 o hasta el máximo que permita el conformador (5kbit).
- Los métodos de limitación de velocidad son conformación y regulación (pero no ambos al mismo tiempo).
- La estrategia de desbordamiento de cola es supresión en un extremo (*tail drop*).
- Las pruebas se ejecutarán sin tráfico de fondo. Se puede realizar una prueba adicional con tráfico de fondo (en competencia). Los resultados y la carga media de fondo se publicarán con los resultados.
- Todas las pruebas y el tráfico de fondo se harán con el mayor esfuerzo posible.
- El intervalo máximo de medición para una medición individual es de 30 segundos.
- En cada medición individual, la tolerancia del ancho de banda configurado en comparación con un ancho de banda medido durante una prueba debe estar dentro del 5% para aceptar un ancho de banda correctamente medido por el sistema de medición candidato.
- El software de medición utilizado para la prueba debe estar disponible bajo una licencia de código abierto. Los productos comerciales pueden aplazar este requisito hasta que comience la normalización de un método. Los sistemas de prueba deben estar calibrados, y Q17 debe conocer los límites de cualquier sistema sometido a su evaluación. Asimismo, deben facilitarse los detalles del entorno de desarrollo y del sistema operativo requerido.
- Los resultados se publicarán como apéndice de la presente Recomendación.
- Los tamaños de las tramas ETH corresponden a un tamaño de trama de capa 2 de 64 bytes y, además, a un tamaño máximo de MTU ETH de 1512 (y 1516 incluyendo el CRC ETH) bytes.
- Es conveniente realizar las pruebas utilizando la familia de direcciones IPv6, además de IPv4.

Los equipos de prueba normalizados de laboratorio pueden servir para calibrar las propiedades de la red [b-TST 009], como el ancho de banda máximo de la capa IP, el tiempo mínimo y máximo de ida y vuelta, la profundidad del búfer, etc., antes de cada herramienta de medición por condición de prueba de la red. De este modo, es posible obtener información de referencia sobre la calidad de funcionamiento de la red, a fin de comparar con ella los resultados de las herramientas de medición y las evaluaciones conexas.

El punto de referencia para el correcto funcionamiento del conformador según la configuración y, en última instancia, para la correcta evaluación de las condiciones del canal (de conformidad con [b-PAM-12]) es la transmisión UDP CBR. Si la capacidad UDP y la configuración del conformador difieren, un tercer árbitro de la corrección es la captura de paquetes del tren UDP. La identificación y el examen de los errores observados es esencial en la evaluación comparativa.

Se han completado las pruebas preliminares de laboratorio para la calibración y la evaluación del método de medición. Tomando como guía el texto existente del Anexo A de esta Recomendación y los requisitos del ORECE para la verificación de las herramientas de medición, AT&T probó una de las tres configuraciones alternativas utilizando una plataforma informática genérica que cumple los requisitos (phy2phy).

Los puntos clave que cabe extraer de estas pruebas son los siguientes:

- El caudal bidireccional fue de 213,85 Mbps, bastante cercano al valor configurado de 100 Mbps x2. El exceso puede ser un artefacto del tamaño de ráfaga permitido.
- La búsqueda binaria con verificación de pérdidas se configuró de manera que permitiera una tolerancia bastante grande en Mbps para aceptar el resultado. Esta tolerancia debería reconsiderarse cuando se prueben velocidades inferiores a un Gbps.

A.4.2.2 Condiciones de las pruebas de la fase 2

A fin de avanzar en el programa de pruebas, este plan empleará la referencia UDP en redes en servicio (con especificaciones de parámetros de servicio validadas) para realizar más comparaciones de especificaciones y métodos de servicio, como los métodos TCP de iPerf 2 y los métodos basados en UDP. Esto es similar a [b-PAM-12], y demás referencias, según se describe a continuación.

La prueba de las configuraciones de los equipos de red en servicio de producción también PUEDE realizarse en el entorno del laboratorio, siempre que sea posible y de forma voluntaria.

Las pruebas de la fase 2 se llevarán a cabo de forma similar al trabajo de 2012 de Goga y Teixeira [b-PAM-12]. A tenor de los conocimientos de que se dispone sobre los sistemas de medición utilizados de forma generalizada en la actualidad, ninguno utiliza el método que se ha demostrado en el pasado que produce la estimación más precisa de la capacidad IP: las mediciones basadas en UDP [b-PAM-12]. Lamentablemente, [b-PAM-12] se realizó cuando las capacidades de acceso típicas eran <50 Mbps, y ahora (más de 5 años después), esta gama de capacidad se ha superado incluso en el acceso a Internet móvil. Los puntos clave que hay que extraer de [b-PAM-12] son:

- Se utilizó iperf para emular las herramientas basadas en un algoritmo de inundación, ya que nos permite establecer el número de conexiones paralelas, la duración o el tamaño de la transferencia, entre otros parámetros.
- "Punto de referencia. La primera línea del Cuadro 1 muestra la capacidad UDP obtenida al inundar el enlace con iperf en UDP..... La capacidad UDP representa la tasa IP máxima alcanzable para cada línea".
- Spruce, *pathload* con grandes sondas y TCP paralelo son las herramientas más precisas para estimar el ancho de banda disponible (también conocido como capacidad residual), pero hay regiones en las que las pruebas de TCP paralelo no arrojan resultados útiles, sobre todo si hay tráfico paralelo no identificado.

Los inconvenientes generales de los sistemas de medición existentes en uso durante el periodo de 2012 se analizan en [MortonPQS].

Las pruebas de la fase 2 deberían realizarse para cada tipo de acceso básico.

Tipos de acceso básicos:

Alámbrico: Acceso al consumidor por DSL, acceso por cable de banda ancha, acceso por fibra, otros.

Inalámbrico: Zona de acceso (*hot spot*) WiFi, UMTS, acceso inalámbrico LTE, otros.

Los resultados y trayectos de prueba utilizados en la fase 1 se definen como base para la fase 2. La fase 2 abarcará varios tipos de acceso a Internet, por ejemplo, un acceso con propiedades típicas de un mercado nacional de telecomunicaciones. Lo mismo ocurre con todos los demás parámetros, por ejemplo, debería darse por supuesto un RTT típico para contenidos populares, el tráfico de fondo debería ser típico, etc. Por lo tanto, las condiciones de la red deberían asemejarse a las del entorno de un abonado real.

Por lo tanto, se pueden aplicar diferentes condiciones para las pruebas individuales. En cada prueba, solo se cambia una propiedad con respecto a la prueba de referencia, mientras que todas las demás propiedades de la configuración permanecen inalteradas.

- El tráfico de fondo puede añadirse en el acceso (con o sin características Diffserv, como cabría esperar en un mercado concreto).

Además, se pueden utilizar equipos de prueba de laboratorio normalizados para investigar las propiedades de la red medida.

Debería especificarse el tamaño de los paquetes cuando se conoce, pero existe una variabilidad potencial de tamaño y esta variación puede ser resultado de las condiciones de red que requieren retransmisión (principalmente para TCP, otras herramientas pueden utilizar tamaños fijos o variables).

Anexo B

Algoritmo adicional de búsqueda de parámetros de capacidad basados en IP y métodos de medición

(El presente anexo forma parte integrante de esta Recomendación.)

B.1 Algoritmo de búsqueda

Este sistema de medición cumple los requisitos de la cláusula A.2.2, y añade las siguientes capacidades para soportar un algoritmo de búsqueda alternativo y de implementación obligatoria, denominado Algoritmo de Búsqueda del Anexo B (que es independiente del protocolo de prueba):

- 1) El probador debería formular una recomendación sobre el tamaño máximo de los paquetes de prueba, y permitir cierta tara inesperada para evitar la fragmentación.
- 2) Un cuadro de velocidades de transmisión, que son el número de paquetes enviados durante cada intervalo de tiempo (correspondiente a bits por segundo y a una capa de protocolo especificada) y los tamaños de los paquetes. El cuadro muestra valores ascendentes para las tasas de carga ofrecidas, entre las tasas de carga mínima y máxima soportadas, ambas incluidas.
- 3) El receptor de la carga ofrecida medirá los siguientes parámetros: tasa recibida, pérdida, reordenamiento, variación de retardo (según esta Recomendación) y retardo de ida y vuelta [UIT-T Y.1565].
- 4) El receptor de la carga ofrecida enviará periódicamente al emisor un mensaje de retorno con información de estado en el que se incluirán los resultados de las métricas realizadas.
- 5) Basándose en los resultados que figuren en el mensaje de retorno con información de estado, el emisor ajustará su carga ofrecida de acuerdo con el diagrama de flujo de la Figura B.1. En el diagrama de flujo, "un paso" es un cambio en la tasa que se logra utilizando un nuevo valor (de la fila superior o inferior a la fila actual para la velocidad de envío y los tamaños de los paquetes) en el cuadro de velocidades de carga ofrecidas.

En el diagrama de flujo de la Figura B.1 se utilizan muchos nombres de variables y, en algunos casos, umbrales configurables que determinan las decisiones del diagrama de flujo. El diagrama de flujo describe tres trayectos principales: cuando la realimentación indica que no hay degradaciones medidas, o cuando las degradaciones se miden por primera vez y puede haber cierta congestión pero se aplaza el cambio de velocidad de envío, o cuando las degradaciones medidas se confirman mediante la realimentación de las mediciones repetidas.

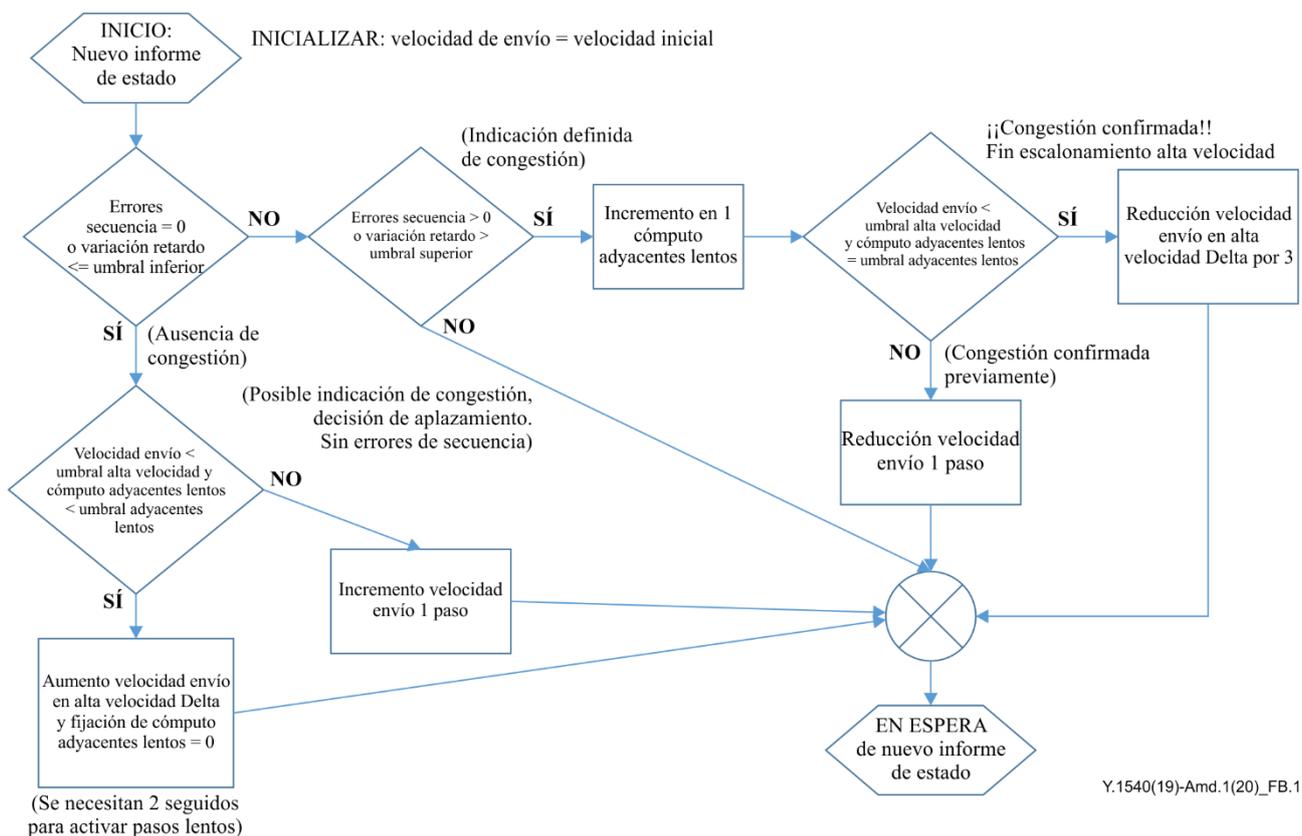


Figura B.1 – Diagrama de flujo para el ajuste de la carga ofrecida, Algoritmo de Búsqueda de Tipo B

NOTA – Las decisiones algorítmicas podrían ser ejecutadas por un extremo de los computadores principales participantes en el sistema de medición, lo que permitiría que la implementación en el otro computador principal fuera mucho menos compleja e independiente de la versión del algoritmo.

Las variables y los umbrales utilizados en la Figura B.1 se explican en el Cuadro B.1.

Cuadro B.1 – Variables del organigrama, descripciones, gamas y valores por defecto

Categoría/ Nombre de variable	Descripción	Unidad	Gama	Valor por defecto
Velocidad de envío	La velocidad de envío actual (equivalente a una fila del cuadro), inicializada en la velocidad mínima de envío del cuadro de velocidades de envío	Kbps	$500 \leq \# \leq 10\,000\,000$ (10 Gbps)	Véase la velocidad inicial
Velocidad de envío inicial	Valor inicial de la velocidad de envío	Kbps	NA	500 Kbps
Seq Errors	Cómputo de cualquiera de las degradaciones de pérdida o reordenación medidas (eventos en los que el número de secuencia del paquete recibido no aumentó en una unidad)	número	NA	0 (sin errores de secuencia)

Cuadro B.1 – Variables del organigrama, descripciones, gamas y valores por defecto

Categoría/ Nombre de variable	Descripción	Unidad	Gama	Valor por defecto
DelayVar	Gama de tiempo de ida y vuelta, RTT (o variación del retardo de un paquete de un solo sentido, por encima del retardo mínimo cuando las mediciones de DelayVar unidireccional son fiables)	ms	NA	NA
LowThresh	Umbral bajo en la gama de variación del tiempo de ida y vuelta, RTT (la gama comprende los valores por encima del RTT mínimo)	ms	$5 \leq ms \leq 250$	30 ms por defecto
UpperThresh	Umbral alto en la gama de variación del tiempo de ida y vuelta, RTT (la gama comprende los valores por encima del RTT mínimo)	ms	$5 \leq ms \leq 250$	90 ms por defecto
HighSpeedDelta	El número de filas que hay que mover en un solo ajuste cuando se aumenta inicialmente la carga ofrecida (para acelerar rápidamente)	Número de filas	≥ 2	10 filas de cuadro (10 Mbps actualmente)
SlowAdjCount	Número de informes de estado consecutivos que indican pérdida y/o variación de retardo por encima de UpperThreshold	Cómputo de ocurrencias	NA	Véase SlowAdjThresh
SlowAdjThresh	Umbral en SlowAdjCount utilizado para inferir la congestión. Utilícense valores > 1 para evitar interpretaciones erróneas de las pérdidas transitorias	Cómputo de ocurrencias	> 1	2
HSpeedThresh	Umbral para la transición entre tamaños de pasos de velocidad de envío baja y alta (como 1 Mbps y 100 Mbps). Puede dar lugar al uso de tramas jumbo si está permitido.	Gbit/s		1 Gbit/s

En el Cuadro B.2 se indican los factores de entrada por defecto para el método del Anexo A, para su uso con el Anexo B.

Cuadro B.2 - Variables de medición, gamas y valores por defecto

Categoría/ Nombre de la variable	Parámetro	Unidad	Gama	Valor por defecto
Capacidad máxima de la capa IP				
	Número de conexiones paralelas	#	$1 \leq \# \leq 10$	1 conexión
	Duración del preámbulo de la prueba	s	$0 \leq s \leq 5$	~2 s
Δt	Duración de la prueba (ya sea de enlace descendente o ascendente) con el algoritmo de búsqueda utilizado, que sirve como duración máxima del proceso de búsqueda.	s	$5 \leq s \leq 60$	10 s
Δt	Duración de la prueba de velocidad fija (enlace descendente o ascendente)	s	$5 \leq s \leq 60$	10 s
dt	Duración de los intervalos intermedios de información	s	$0,1 \leq s \leq 10$	1 s
	Valor de temporización	s	$5 \leq s \leq 30$	5 s
	Tipo de paquete de prueba incluyendo las longitudes del encabezamiento y de la cabida útil, los encabezamientos y las opciones presentes y cualquier marca para un tratamiento especial en la red	NA	IPv4 o IPv6 UDP DSCP	No hay valor por defecto UDP 00 = el mayor esfuerzo
	Tamaño de referencia de la cabida útil UDP	KB	Mínimo 1 Kbyte, máximo a 1 472 bytes (máximo 9 000 con Jumbo Frames)	No hay valor por defecto, se recomienda el mayor valor que evite la fragmentación.
	Periodo de mensajes de retorno con información de estado (el receptor de la carga ofrecida devuelve mensajes al emisor con los resultados de las métricas realizadas)	s	$0,005 \leq s \leq 0,250$	0,050 s
Métricas de apoyo	Son métricas que se realizan en el mismo tren que la capacidad IP			
IPLR	Y.1540, RFC 7680			
Tmax	Tiempo máximo de espera para la llegada de paquetes	s	$0,05 \leq s \leq 3$	1 s
RTT de muestreo	Y.1545, RFC 2681: El RTT utiliza mensajes de retorno del receptor con información de estado.			

Cuadro B.2 - Variables de medición, gamas y valores por defecto

Categoría/ Nombre de la variable	Parámetro	Unidad	Gama	Valor por defecto
Tmax	Tiempo máximo de espera para la llegada de paquetes	s	$0,05 \leq s \leq 3$	3 s
	Resolución de las indicaciones de tiempo	ms	$0,001 \leq ms \leq 1$	Propuesta para el acceso fijo: 0,001 (según la aplicación actual)
Métrica de apoyo: IPDV	Y.1540, RFC 3393, RFC 5481(PDV)			
Tmax	Tiempo máximo de espera para la llegada de paquetes	s	$0,05 \leq s \leq 3$	1 s
	Resolución de las indicaciones de tiempo	ms	$0,001 \leq ms \leq 1$	Propuesta para el acceso fijo: ,001 (según la aplicación actual)

Las conexiones paralelas introducen complejidad y la ventaja de alcanzar velocidades más altas.

Entre los posibles beneficios destacan los siguientes:

- Se pueden utilizar sistemas paralelos para producir la velocidad agregada necesaria con conexiones paralelas.
- Las conexiones paralelas pueden utilizarse como una forma de saturar el trayecto sometido a prueba con un solo par de computadores principales de prueba.
- Se puede obtener información adicional con fines de diagnóstico o para validar el proceso de prueba. Por ejemplo, la comparación de las velocidades de datos en cada conexión podría ser informativa, ya que la presencia de velocidades de datos muy divergentes podría ser indicativa de un funcionamiento anormal.

La visión actual es que cada conexión tendría su propio canal de realimentación, cálculo de medidas y diagrama de flujo, y un informe de los resultados agregados sobre todas las conexiones.

Apéndice I

Consideraciones relativas al encaminamiento de paquetes IP

(Este apéndice no forma parte integrante de la presente Recomendación.)

En este apéndice se exponen consideraciones relativas al encaminamiento de paquetes IP de interés para la caracterización de la calidad de funcionamiento del servicio IP.

El encaminamiento de paquetes IP viene determinado por las políticas y configuraciones de los protocolos de encaminamiento de cada operador de red, así como por las elecciones de los propios protocolos. Por ejemplo, los operadores configuran un parámetro para el "costo" de atravesar cada enlace en su red, y el algoritmo de encaminamiento calcula la ruta de menor costo hasta el punto de destino basándose en su conocimiento del estado actual de la topología de la red. Evidentemente, el trayecto que sigue un paquete desde el origen hasta el destino influye en gran medida en el retardo de transferencia que experimentará (tanto por el transporte como por el encolamiento), así como en la exposición a otras degradaciones como pérdidas, errores, duplicación y reordenación.

Otra forma en que los protocolos de encaminamiento influyen en la calidad de funcionamiento de la transferencia de paquetes es su respuesta automatizada a las alteraciones de la topología de la red, como los fallos de los enlaces o de los encaminadores, o las acciones de mantenimiento para dejar fuera de servicio un elemento de la red. Cuando la topología de la red cambia debido a un fallo, un proceso de recuperación restablece la conectividad afectada sobre la topología de red restante, si es posible. Este proceso se denomina "reencaminamiento" o "reconvergencia", y suele contener los siguientes pasos (cada uno de los cuales requiere tiempo de ejecución):

- 1) detección de fallos/eventos;
- 2) cálculo de la trayectoria;
- 3) advertencia;
- 4) actualización de la tabla de reenvío.

De nuevo, las opciones de los temporizadores configurados por el operador determinan en gran medida la duración del proceso de reencaminamiento. Los operadores también tienen la opción de establecer tiempos de espera entre las ejecuciones del algoritmo de encaminamiento, lo que conserva los recursos de procesamiento pero puede alargar la respuesta a un fallo en algunos casos.

Las tecnologías de redes sub-IP, como los anillos SONET y el reencaminamiento rápido MPLS-TE, permiten la restauración en subsegundos de los fallos de los enlaces o de los encaminadores.

Apéndice II

Terminología secundaria aplicable a la variación del retardo de paquetes IP

(Este apéndice no forma parte integrante de la presente Recomendación.)

II.1 Introducción

En esta Recomendación se especifica una sola definición primaria/normativa para calcular la variación en un conjunto de retardos con respecto a un retardo de referencia. En las siguientes cláusulas de este apéndice se dan dos definiciones informativas/secundarias (que se basan en la variación del retardo entre paquetes definida por el IETF, y una modificación de la variación del retardo de célula de un punto). En este apéndice también se indica qué parámetro es el más adecuado en cada caso y relaciona los resultados de las observaciones con los diferentes parámetros. En [IETF RFC 5481] se detallan comparaciones adicionales entre diferentes formas de variación de retardo.

Hay otros dos métodos para cuantificar la variación de retardo.

- 1) un parámetro basado en [b-IETF RFC 3393] que determina la variación del retardo entre paquetes;
- 2) un parámetro similar a la variación de retardo de células de 1 punto, que se describe en [b-UIT-T I.356], y que sirve para calcular la diferencia en el tiempo de llegada de paquetes en una misma interfaz con respecto a un intervalo de recepción idóneo.

Obsérvese que [b-UIT-T I.356] incluye dos definiciones de variación diferentes: 2 puntos y 1 punto.

Los objetivos de calidad de funcionamiento en [UIT-T Y.1541] para PDV se describen en cuanto al parámetro normativo de variación de retardo de paquete de 2 puntos en esta Recomendación.

II.2 Definición de variación del retardo entre paquetes

En [b-IETF RFC 3393] se define la variación del retardo del modo siguiente:

- Se puede definir la IPDV para paquetes que forman parte de un mismo tren de paquetes.
- La IPDV de un par de paquetes en un tren de paquetes se define para un determinado par de paquetes que van desde el punto de medición MP1 al punto de medición MP2.
- La IPDV es la diferencia entre el retardo en un solo sentido de esos determinados paquetes.

Mediante una función de selección se determina de manera inequívoca el par de paquetes que se utiliza en cada cálculo de la métrica de variación del retardo. En los cálculos de la IPDV solo se utilizan los paquetes que llegan satisfactoriamente.

La primera función de selección se ha definido para paquetes adyacentes en el tren. Para determinar la IPDV del paquete actual se ha de restar al retardo en un solo sentido de este paquete el retardo en un solo sentido del paquete anterior. Si uno de los paquetes (o los dos) se pierde, entonces la IPDV queda indeterminada.

Otro ejemplo importante es la función selección que produce un resultado de la variación del retardo equivalente al parámetro PDV de 2 puntos definido en la cláusula 6.2.4. El par de paquetes siempre incluye el paquete actual y el paquete con el mínimo retardo en un solo sentido en el tren. La PDV de 2 puntos para todos los paquetes que llegan se calcula restando a sus valores de retardo en un solo sentido el retardo mínimo (el retardo de referencia es el retardo mínimo).

II.3 Definición de la variación del retardo de paquetes de 1 punto

La idea fundamental del parámetro de variación del retardo de 1 punto es la comparación entre el patrón de recepción real y el previsto (que normalmente es periódico). Algunas variantes de esta definición incluyen un ajuste de "salto de reloj" (cuando las celdas o paquetes llegan tarde/con retraso respecto de su hora de llegada idónea), como en [b-UIT-T I.356]. La definición que se presenta a continuación no implementa la característica de "salto de reloj", ya que no hay un sesgo claro si el patrón de referencia se establece de forma arbitraria.

La PDV de 1 punto (y_k) para el paquete k en un MP es la diferencia entre el tiempo de llegada de referencia del paquete (c_k) y el tiempo de llegada real (a_k) en el MP: $y_k = c_k - a_k$. El patrón de tiempo de llegada de referencia (c_k) se define del siguiente modo:

$$c_0 = a_0 = 0,$$

$$c_{k+1} = c_k + T$$

donde T es el espaciamiento idóneo entre paquetes.

Los valores positivos de PDV de 1 punto (llegadas "tempranas" de paquetes) corresponden a la aglomeración de paquetes; los valores negativos de PDV de 1 punto (llegadas de paquetes "tardías") corresponden a los espaciamientos en el tren de paquetes.

II.4 Directrices para la aplicación de los diferentes parámetros

Las directrices prácticas para la medición son las siguientes:

- Cuando no sea posible sincronizar los relojes (o no se puedan utilizar temporalmente) en los dispositivos de medición:
 - 1) un posible sustituto de la gama/histograma de retardos de un solo sentido es la variación del retardo de paquetes de un punto (PDV de un punto), aplicable a las mediciones que se realizan en trenes de paquetes con tiempos de envío periódicos (una vez que se ha fijado adecuadamente el tiempo de llegada de referencia);
 - 2) la variación del retardo entre paquetes de la métricas de calidad de funcionamiento IP (IPPM) es aplicable a todos los tipos de flujo de tráfico;
 - 3) cuando el error de reloj es estable, se puede calcular y utilizar el PDV de 2 puntos de UIT-T Y.1540.
- Cuando se pueden sincronizar los relojes en los dispositivos de medición:
 - 1) el cálculo de la gama o el histograma de retardo de un solo sentido PDV de UIT-T Y.1540 es útil para una serie de tareas de evaluación, incluida la evaluación del tamaño de la memoria intermedia;
 - 2) la variación del retardo entre paquetes IPPM añade un parámetro sensible a la variación secuencial/de corta duración y cierta inmunidad frente a cambios de ruta.

La métrica entre paquetes, IPDV, definida por el grupo de trabajo del IETF IPPM, es similar al cálculo de la medición de la fluctuación de fase entre recepciones en los informes del protocolo de control en tiempo real (RTCP). El cálculo de la fluctuación entre recepciones se describe en la cláusula 6.4 de [b-IETF RFC 3550] del RTP y en un apéndice se incluye un ejemplo de implementación. Aunque los métodos tienen algunas diferencias (la fluctuación entre recepciones RTCP utiliza el orden de llegada, en lugar de la secuencia de envío con IPDV) debería haber una comparación favorable entre una "fluctuación suave" calculada utilizando semifallos IPDV y los informes RTCP de la fluctuación en muchas circunstancias (si se reordenan muchos paquetes, los resultados no serán probablemente acordes). Sería valioso disponer de un parámetro que se pueda relacionar con las mediciones realizadas en los puntos extremos de los usuarios. La métrica IPDV con pares de paquetes adyacentes

también es menos susceptible a los cambios de ruta durante un intervalo de medición, en la que el efecto sólo se observaría en pares de mediciones que abarquen el cambio de ruta.

Un atributo positivo de la PDV de 1 punto es su simplicidad. La capacidad de evaluar trenes periódicamente en un mismo elemento de red es muy ventajoso.

Un aspecto que debe estar claro en todas las especificaciones de parámetros de variación es el efecto de la longitud del paquete. Como el tiempo de inserción está incluido en el retardo de transferencia (del primer bit al último) los paquetes de distinto tamaño tendrán una variación del retardo inherente. En las especificaciones y las pruebas de las redes se deberían utilizar paquetes de un mismo tamaño para simplificar la interpretación de los resultados (y se debería registrar el tamaño utilizado).

Apéndice III

Parámetros relacionados con la velocidad y la capacidad de caudal

(Este apéndice no forma parte integrante de la presente Recomendación.)

Este apéndice queda obsoleto en la edición de 2019.

Apéndice IV

Pruebas del estado de disponibilidad del servicio IP y estimación por muestreo de los parámetros de disponibilidad del servicio IP

(Este apéndice no forma parte integrante de la presente Recomendación.)

Este apéndice, que queda en estudio, describe las pruebas para determinar si un servicio IP, una sección básica o un NSE está en estado de disponibilidad o de indisponibilidad. En una versión futura, el presente apéndice contendrá métodos de estimación por muestreo de los parámetros de disponibilidad del servicio IP.

IV.1 Prueba mínima del estado de disponibilidad del servicio IP (para metodologías de prueba y aparatos de prueba)

En la cláusula 7.1 se exige que se utilicen al menos M_{av} paquetes para evaluar el estado de disponibilidad. Las metodologías de prueba y los aparatos de prueba deberán intentar la evaluación con al menos M_{av} paquetes dispersos a lo largo de un intervalo de tiempo T_{av} . Para el tráfico generado por el usuario de extremo, se podrían concatenar T_{av} intervalos de tiempo sucesivos hasta que se cumpla el requisito de al menos M_{av} eventos de ingreso. Estos aspectos quedan en estudio.

A continuación se describe la tarea mínima que es preciso realizar para decidir respecto al estado de disponibilidad durante un solo intervalo de tiempo T_{av} . Se necesita aplicar varias veces esta prueba para determinar el PIA y el PIU. La prueba mínima de disponibilidad del servicio IP se puede efectuar para probar metodologías y aparatos de prueba; en la cláusula 7.1 se presentan algunos de los requisitos con respecto al tráfico generado por el usuario de extremo. Cualquier otra prueba de disponibilidad del servicio IP que (estadísticamente) tenga unos resultados de calidad equivalente a los de esta prueba es una prueba aceptable. La presente prueba de disponibilidad IP se aplica de extremo a extremo o, en el caso de ingreso específico, a una sección básica o un NSE.

- Paso 1: Determinar el SRC y el DST.
- Paso 2: Posicionar los aparatos de prueba o activar los guiones de prueba en los puntos de medición apropiados.
- Paso 3: En un momento determinado previamente, iniciar el envío de M_{av} paquetes IP distribuidos durante el periodo de tiempo T_{av} .
- Paso 4: Si el número de resultados paquete perdido es superior a $c_1 \times M_{av}$, el servicio IP está indisponible durante el intervalo de tiempo T_{av} .
- Paso 5: Si, de acuerdo con los resultados del paso 4, el servicio IP (sección básica o NSE) no se declara indisponible, ello quiere decir que está disponible durante este intervalo de tiempo T_{av} .

La prueba mínima proporciona un nivel de confianza desconocido en función del tamaño de la muestra, M_{av} , por lo que se prefiere la siguiente prueba.

IV.2 Prueba del estado de disponibilidad del servicio IP (mediante la prueba de relación de probabilidad secuencial)

Esta cláusula describe una prueba no paramétrica, que no presupone la distribución subyacente sobre las pérdidas, y que se basa en la prueba de relación de probabilidad secuencial (SPRT) para determinar si se ha superado el umbral de pérdida c_1 con un nivel de error predeterminado. La SPRT también permite al probador detener la prueba cuando se ha observado una tasa de pérdidas mucho menor en un número de paquetes y un periodo de tiempo determinados. El resultado también puede ser indeterminado, en cuyo caso se justifica la realización de nuevas pruebas. La SPRT se aplicó por

primera vez en [b-Morton] para evaluar las tasas de pérdidas de paquetes en relación con las tasas objetivo en las pruebas de Internet.

Para la hipótesis nula, H0, fijamos la probabilidad de pérdida (o de defectos) igual a $c_1 = p_0 = 0,20$. También fijamos la probabilidad de pérdidas para la hipótesis alternativa, H1, en $p_1 = 0,05$. Por último, los errores de tipo I y II son $\alpha = \beta = 0,001$.

A continuación se muestran las ecuaciones de SPRT [b-Montgomery], [b-Wald]:

$$X_A = -h_1 + sn \text{ (línea de aceptación)} \quad (1)$$

$$X_R = h_2 + sn \text{ (línea de rechazo)} \quad (2)$$

donde n aumenta linealmente en todos los paquetes enviados, y

$$h_1 = \left(\log \frac{1-\alpha}{\beta} \right) k^{-1} \quad (3)$$

$$h_2 = \left(\log \frac{1-\beta}{\alpha} \right) k^{-1} \quad (4)$$

$$k = \log \frac{p_1(1-p_0)}{p_0(1-p_1)} \quad (5)$$

$$s = \left(\log \frac{(1-p_0)}{(1-p_1)} \right) k^{-1} \quad (6)$$

para p_0 y p_1 como se define anteriormente en las hipótesis nula y alternativa.

Utilizando las ecuaciones anteriores, se calcula el número mínimo de paquetes necesarios para aceptar H0 cuando se observan x defectos, por ejemplo $x=0$ (sin pérdidas).

$$X_A = 0 = -h_1 + sn \quad (7)$$

$$n = \frac{h_1}{s} \quad (8)$$

Al establecer $c_1 = p_0 = 0,20$ como nivel H0, $p_0 = 0,05$ para la alternativa H1 y errores a 0,001, se constata que se necesitan al menos 41 paquetes para preferir H1 (con cero pérdidas) y que la observación de 9 pérdidas en esos 41 paquetes daría lugar a una preferencia por H0.

En la Figura IV.1 se muestran los resultados de la herramienta R [b-Rdev] que funciona con el paquete [b-CVST] instalado utilizando los valores anteriores.

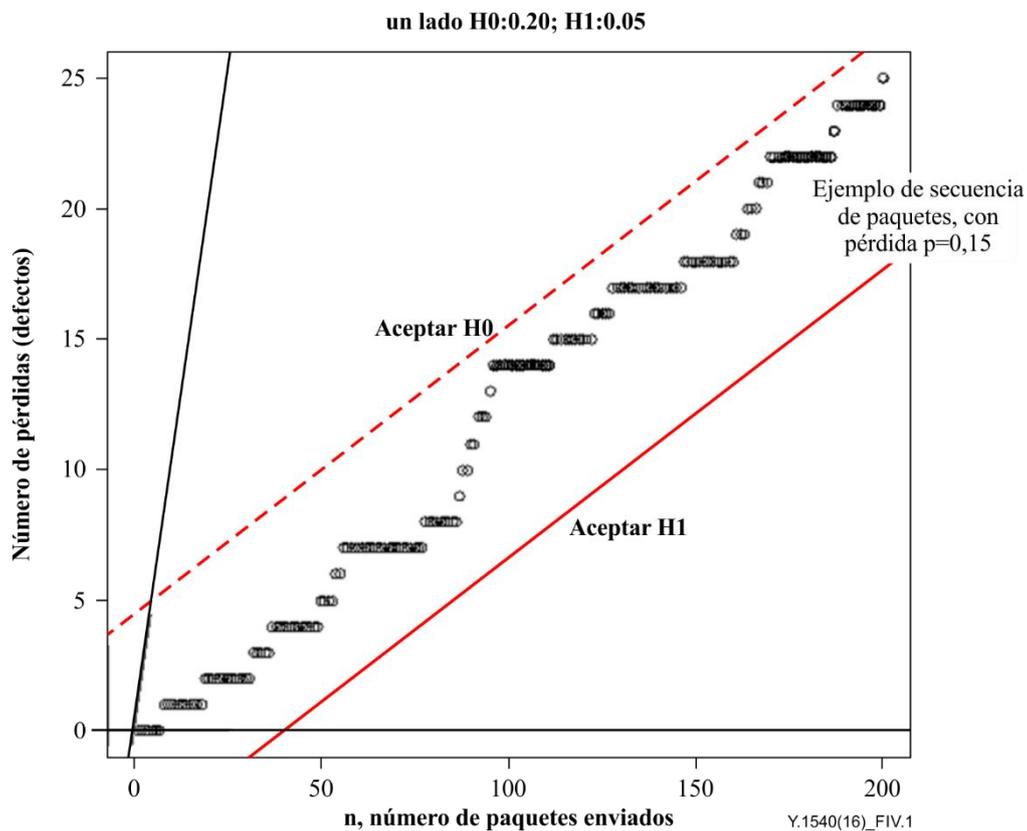


Figura IV.1 – Ejemplo de prueba de relación de probabilidad secuencial

La Figura IV.1 ilustra que se necesitan al menos 41 paquetes para preferir H_1 (con cero pérdidas), y la observación de 9 pérdidas en estos 41 paquetes daría lugar a una preferencia por H_0 .

IV.3 Prueba alternativa de significación estadística para determinar la disponibilidad del servicio IP

[UIT-T Y.1540] determina que el servicio IP está disponible durante un intervalo de medición si la IPLR para ese intervalo es menor que el umbral c_1 . Dado que un paquete se transmite satisfactoriamente o se pierde, la pérdida de paquetes puede modelarse mediante una distribución binomial.

La hipótesis nula H_0 es que el servicio IP está disponible durante el intervalo de medición. Se supone que H_0 es verdadera si la pérdida media de paquetes durante el intervalo de medición es inferior o igual a c_1 (en la prueba z se considera que el servicio IP está disponible si la tasa de pérdida de paquetes es igual a c_1). La hipótesis H_1 es que el servicio IP no está disponible durante el intervalo de medición (pérdida de paquetes $> c_1$ durante el intervalo de medición). Se propone una prueba z para decidir si mediante la medición se corrobora la hipótesis H_0 o la H_1 . Siguiendo la propuesta de [b-C-298] se toma como nivel de confianza el 95% (lo que significa que el nivel de significación es $\alpha=0,05$).

La prueba consiste en comparar una muestra con un umbral, c_1 . La media del umbral $\mu_0 = c_1$ y su varianza aplicable a la prueba es $\sigma = c_1 * (1 - c_1)$.

El número de paquetes $n = \text{paquetes}_{\text{transmitidos}} + \text{paquetes}_{\text{perdidos}}$. Por lo tanto, la tasa media de pérdida de paquetes es $x_{\text{media}} = \text{paquetes}_{\text{perdidos}} / n$.

El estadístico de prueba para un texto umbral $z_{\text{disponible}} = \text{sqrt}(n) * (x_{\text{media}} - \mu_0) / \sigma$.

Con el valor z para un nivel de confianza del 95% y $\alpha = 0,05$ para una prueba unilateral, se acepta H_1 (el servicio IP no está disponible durante las mediciones) si $z_{\text{disponible}} > 1,645$.

Con el valor z para un nivel de confianza del 99,9% y $\alpha = 0,001$ para una prueba unilateral, se acepta H_1 (el servicio IP no está disponible durante las mediciones) si $Z_{\text{disponible}} > 3,09$.

IV.4 Estimación por muestreo de la disponibilidad del servicio IP

Muestras aleatorias del estado de disponibilidad utilizando la prueba mínima arriba indicada pueden ser suficientes para estimar el PIA y el PIU. Para estimar la duración de los periodos de tiempo contiguos en estado de disponibilidad o en estado de indisponibilidad, el muestreo debe ser mucho más frecuente. [b-UIT-T X.137] contiene procedimientos para redes UIT-T X.25/UIT-T X.75 que podrían servir también para el servicio IP.

Apéndice V

Material pertinente para los métodos de medición de la calidad de funcionamiento IP

(Este apéndice no forma parte integrante de la presente Recomendación.)

En este apéndice, que queda en estudio, se describirán asuntos importantes a considerar a medida que se desarrollen métodos de medición de la calidad de funcionamiento IP. Se presentarán en él los efectos de las condiciones externas a las secciones sometidas a prueba, incluidas consideraciones relativas al tráfico, sobre la calidad de funcionamiento medida.

Deberán especificarse las siguientes condiciones, que habrán de ser controladas durante las mediciones de calidad de funcionamiento IP:

- 1) Cuáles son exactamente las secciones que se miden:
 - los SRC y los DST de las mediciones de extremo a extremo;
 - los MP que limitan el NSE que se mide.

NOTA – No es necesario medir entre todos los pares de MP o todos los pares de SRC y DST para caracterizar la calidad de funcionamiento.

- 2) Tiempo de medición:
 - durante cuánto tiempo se recogieron muestras;
 - cuándo tuvo lugar la medición.
- 3) Características exactas del tráfico:
 - tasa a la que el SRC ofrece tráfico;
 - esquema de tráfico del SRC;
 - tráfico competidor en el SRC y el DST;
 - tamaño de los paquetes IP.
- 4) Tipo de medición:
 - en servicio o fuera de servicio;
 - activa o pasiva.
- 5) Resúmenes de los datos medidos:
 - valores medios, valores del caso más desfavorable y cuantiles empíricos;
 - periodo que se resume:
 - periodo corto (por ejemplo, una hora);
 - periodo largo (por ejemplo, un día, una semana, un mes).

Apéndice VI

Fundamentos de la disponibilidad de servicio IP

(Este apéndice no forma parte integrante de la presente Recomendación.)

VI.1 Introducción

En este apéndice se establecen los fundamentos de la definición de la función de disponibilidad de servicio IP actual dada en la cláusula 7, a fin de aportar más información general y contribuir a la valorización de este tema que es complejo e importante.

VI.2 Antecedentes

La disponibilidad puede describirse de diversas maneras y los puntos de vista permiten evaluarla a través de varias sensibilidades y escalas tiempo. En esta Recomendación se utiliza una definición simple y apropiada (desde el punto de vista del operador de red) que especifica las condiciones mínimas de evaluación necesarias. Para entender si la función de disponibilidad de servicio IP es satisfactoria, es necesario conocer las causas de la indisponibilidad.

En la Figura VI.1 se muestra un diagrama de Venn en el que el universo es todo el tiempo de servicio. En el texto de esta Recomendación se observa que los proveedores de servicio IP pueden identificar intervalos de mantenimiento en los que no se garantiza la disponibilidad de servicio. Por tanto, el universo de tiempo de servicio suele diferir del universo de *todo* el tiempo.

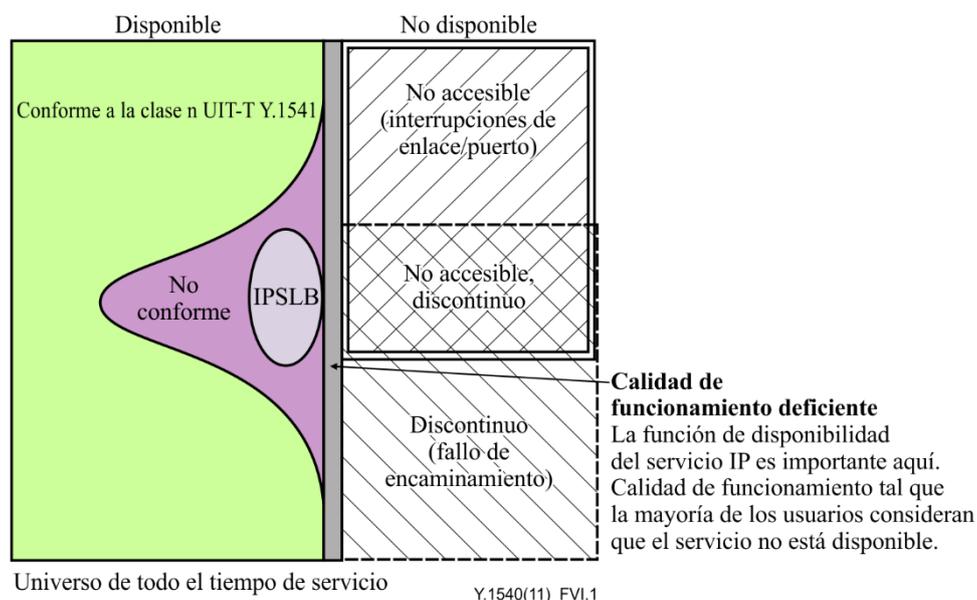


Figura VI.1 – Diagrama de Venn del tiempo de servicio

Se indica que el tiempo de servicio se divide en dos categorías principales: tiempo disponible (a la izquierda) y tiempo indisponible (a la derecha). Obsérvese que los tamaños relativos no son a escala, ya que el tiempo disponible suele ser mucho mayor que el no disponible.

VI.3 Definiciones de las regiones de la Figura VI.1

El tiempo **indisponible** se compone de las siguientes zonas:

- **No accesible:** Un fallo en elementos de transporte de la red de acceso o de la red provoca que el usuario del servicio no pueda comunicarse con la red IP. Esto se debe, con frecuencia, a fallos en el enlace o en la interfaz de encaminamiento. La tasa de pérdida de paquetes suele

ser 100% y a menudo son necesarios más de 1 minuto para corregir el fallo. Convendrá que los sistemas de gestión de fallos avisen inmediatamente a los encargados del mantenimiento.

- **Discontinuo:** Un fallo en la información de encaminamiento global de red IP provoca que el usuario del servicio no pueda comunicarse en el destino deseado. Si bien es posible comunicarse con algunos destinos, no lo es con el deseado. La tasa de pérdida de paquetes suele ser 100% y, a menudo, son necesarios más de 1 minuto para corregir el fallo.
- **No accesible, discontinuo:** El usuario del servicio no puede comunicarse mientras coexistan las dos condiciones anteriores.
- **Calidad de funcionamiento deficiente:** El usuario del servicio no puede obtener una comunicación fiable con el destino deseado. La tasa de pérdida de paquetes es mayor o igual a 20%, y el usuario califica el servicio como indisponible para comunicarse con casi cualquier tipo de aplicación de red IP. Si este nivel de pérdida de paquete se debe principalmente a la congestión, convendrá activar el control de flujo extremo a extremo [suministrado en el protocolo de control de transmisión (TCP)] para disminuirla.

El tiempo **disponible** se compone de las siguientes regiones:

- **Conforme a la clase n [UIT-T Y.1541]:** El usuario del servicio puede comunicarse con el destino deseado y la calidad de funcionamiento de la transferencia de paquetes es conforme a los objetivos de la clase acordada. La evaluación de este estado suele efectuarse en intervalos de 1 minuto. Obsérvese que cualquier aplicación de usuario tiene necesidades específicas de capacidad; también se ha de considerar la capacidad de soportar un contrato de tráfico (definido en [b-UIT-T Y.1221]).
- **No conforme:** Aunque el usuario de servicio puede comunicarse con el destino deseado, la calidad de funcionamiento de transferencia de paquetes no cumple uno o varios de los objetivos de la clase acordada. La evaluación de este estado suele efectuarse en intervalos de 1 minuto.
- **Bloques de paquetes IP con muchas pérdidas (IPSLB):** Aunque el usuario de servicio puede comunicarse con el destino deseado, la calidad de funcionamiento de transferencia de paquetes no cumple uno o varios de los objetivos de la clase acordada. En particular la tasa de pérdida es suficiente para determinar que ha ocurrido un IPSLB (que se define, provisionalmente, como una pérdida mayor de 20% en un intervalo de 10 segundos).

VI.4 Resumen

Se observa que los criterios de la función de disponibilidad de servicio IP sólo son importantes en la región de calidad de funcionamiento deficiente, y que la contribución de esta región al tiempo indisponible es pequeña comparada con las otras causas de indisponibilidad. Por lo tanto, se considera suficiente la evaluación del estado sobre la base únicamente de la pérdida, y basta con los criterios acordados provisionalmente para dicha evaluación (1 minuto, 20% de pérdida).

Apéndice VII

Parámetros de calidad de funcionamiento de los paquetes a efectos de la optimización de las técnicas para la reparación de trenes

(Este apéndice no forma parte integrante de la presente Recomendación.)

VII.1 Introducción

Los parámetros de rendimiento de la capa IP tienen diversos usos, siendo uno de ellos la supervisión de la red y la identificación de problemas. Los parámetros también se utilizan como base de los acuerdos de nivel de servicio (SLA). Ambos usos mencionados describen la transferencia de paquetes como una caracterización de la red que proporcionó el transporte UNI-UNI.

Hay una segunda perspectiva: Los parámetros de calidad de funcionamiento de la capa IP también caracterizan las redes en términos que pueden ser de interés para el diseñador de aplicaciones. Aunque muchos de los parámetros utilizados en la supervisión de la red son útiles para los diseñadores de aplicaciones, es probable que haya parámetros únicos para cada caso de utilización. La Figura VII.1 ilustra las dos perspectivas diferentes, o los casos de utilización de los parámetros de calidad de funcionamiento IP.

La Recomendación UIT-T Y.1540 define los parámetros de rendimiento y disponibilidad para las redes basadas en IP. Define los resultados primarios y secundarios de la transferencia de paquetes y una serie de parámetros de calidad de funcionamiento de paquetes basados en estos resultados, incluida la función de disponibilidad del servicio IP.

Esta versión de la Recomendación UIT-T Y.1540 se basa en las definiciones y conceptos fundamentales para normalizar un nuevo conjunto de parámetros normativos de calidad de funcionamiento a efectos de la reparación de trenes. El objetivo de los nuevos parámetros es proporcionar información pertinente para el diseño y la configuración de técnicas de capa superior (capa de aplicaciones) para compensar la pérdida de paquetes debida a diversas causas (incluidos los errores y la variación del retardo). Así pues, el diseño y/o la optimización y la estimación de la calidad de funcionamiento de las técnicas de reparación de trenes de aplicaciones deberían simplificarse si estas nuevas métricas para la evaluación de la calidad de funcionamiento de los paquetes cumplen su objetivo.

Este apéndice comienza con una breve descripción de las técnicas de reparación de trenes en la capa de aplicaciones. Seguidamente, se ofrece un modelo muy sencillo que está concebido para aplicarse a numerosas técnicas de reparación.

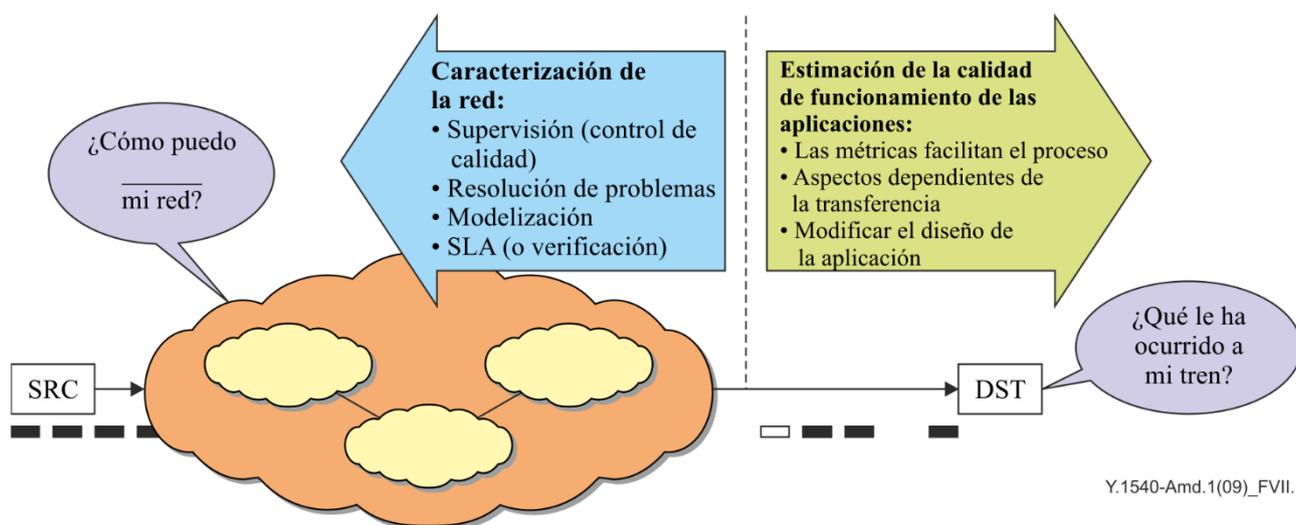


Figura VII.1 – Dos casos diferentes de utilización de los parámetros de calidad de funcionamiento IP

El procedimiento habitual consiste en introducir nuevas métricas como apéndices informativos, de modo que los usuarios potenciales tengan la oportunidad de evaluarlas antes de su incorporación como parámetros normativos en el texto de la Recomendación. Estas nuevas métricas han seguido el primer trayecto informativo hasta su incorporación a la Recomendación UIT-T Y.1540. En sus estudios, el UIT-T ha tenido en cuenta muchas contribuciones que detallan la experiencia con parámetros de calidad de funcionamiento de reparación de trenes que sirve de base para su promoción al rango normativo.

VII.2 Breve descripción de las técnicas de reparación de trenes en la capa de aplicaciones

Existen tres tipos principales de técnicas de la capa de aplicaciones para compensar las degradaciones del transporte de paquetes. Nos centramos en las aplicaciones en tiempo real basadas en flujo continuo (audio, vídeo) que no son elásticas, donde la entrega de información debe producirse con arreglo a un calendario predeterminado, y no en la clase de aplicaciones elásticas de transferencia de datos que suelen basarse en TCP y en sus servicios de transferencia de trenes de octetos fiables.

Corrección de errores en recepción (FEC, *forward error correction*): Se trata de una técnica en la que los trenes de paquetes se organizan en bloques antes de la transferencia. Se realizan cálculos en cada bloque y se añaden paquetes de tara al tren que el receptor puede utilizar para reproducir alguna fracción de los paquetes del bloque si se pierden, o si llegan satisfactoriamente pero se retrasan, o se corrompen en el transporte. La sobrecarga típica representa entre el 5% y el 20% del bloque de información. En un esquema FEC *idóneo*, el número de paquetes perdidos que pueden corregirse es *igual* al número de paquetes de tara. Los aspectos clave de este esquema son los siguientes:

- el tamaño del bloque de información, en paquetes y tiempo;
- la cantidad de paquetes de tara en relación con el bloque de información, que representa aproximadamente la capacidad correctiva del esquema.

Petición automática de repetición (ARQ): En esta técnica se dispone de un canal de comunicación inverso en el que el receptor, tras detectar que determinados paquetes individuales se han perdido, se han retrasado o se han corrompido, puede solicitar la retransmisión (lo que se denomina una ARQ selectiva). Los paquetes perdidos se reenvían a tiempo para que ocupen su lugar mientras la información se transfiere a capas superiores para su decodificación y reproducción. En ocasiones, se ha modificado el TCP para prestar servicio a trenes no elásticos en la función de ARQ. Hay un tiempo de espera para determinar si los paquetes simplemente se retrasan o se pierden, y esto es similar al bloque de información utilizado en los esquemas FEC. También puede haber un límite de paquetes

retransmitidos que pueden acompañar al tren primario en cualquier intervalo de tiempo, y esto es paralelo a la tara de los esquemas FEC. El número de paquetes perdidos que la técnica ARQ puede retransmitir en un bloque es igual a su límite de tara de retransmisión. Téngase en cuenta que los paquetes retransmitidos representarán una tara en un bloque posterior de paquetes de información, pero el concepto sigue siendo válido.

Por lo tanto, las técnicas ARQ y FEC pueden describirse con las mismas variables básicas de tamaño de bloque de información y tamaño máximo reparable.

Ocultación de errores en la capa de aplicaciones: Se trata de una técnica en la que los decodificadores tratan de compensar la información perdida o corrompida, por medio de diversas técnicas específicas de la aplicación, algunas de las cuales se han normalizado. La aplicabilidad del modelo simple (descrito a continuación) a esta clase de técnicas queda en estudio.

VII.3 Modelo simple de técnicas de reparación de trenes en la capa de aplicaciones

Cada tren de paquetes de la capa de aplicaciones se modela como si contuviera dos categorías de paquetes:

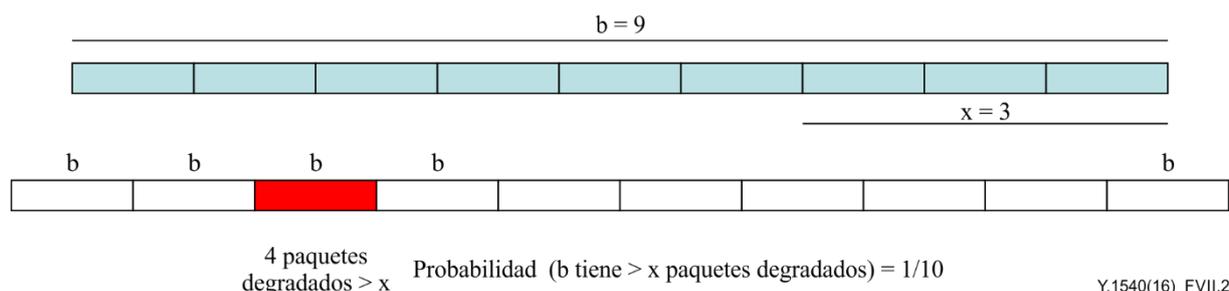
- 1) intervalos de tiempo, T_I , o bloques, b , de paquetes de información;
- 2) paquetes de tara, o el máximo de paquetes reparables, x , asociados al bloque de información.

La principal dificultad para el diseñador de la técnica de reparación es elegir el tamaño del bloque de información en combinación con la cantidad (máxima) de paquetes de tara que será suficiente para compensar un alto porcentaje de degradaciones de la red de paquetes (pérdida, retardo excesivo y corrupción), al tiempo que se trabaja dentro de los límites de la capacidad global de transferencia de paquetes del sistema y se ofrece una calidad suficiente en el tren de aplicaciones.

Los nuevos parámetros de calidad de funcionamiento (que se describen en la cláusula 6.10) deberían ayudar a tomar estas decisiones.

VII.4 Ejemplo de parámetros de calidad de funcionamiento para caracterizar las variables de reparación de trenes

En la Figura VII.2 se muestra un ejemplo de los cálculos de los parámetros de reparación de trenes, donde $b = 9$ paquetes y $x = 3$ paquetes.



Y.1540(16)_FVII.2

Figura VII.2 – Ilustración del parámetro de calidad de funcionamiento de la reparación de trenes

VII.5 Análisis de la medición y el uso de los parámetros

Cuando se intenta estimar la calidad de funcionamiento de un sistema de reparación con una alineación de bloques desconocida, los intervalos de tiempo, T_I , o los bloques, b , pueden solaparse para permitir la evaluación de diferentes alineaciones de intervalos y degradaciones (análisis de intervalo deslizante). El uso de un único intervalo fijo no solapado para la estimación y el análisis de la calidad de funcionamiento plantea el problema de que el bloque de información real más la tara puede perder calidad de funcionamiento debido a la diferencia de alineación.

Cabe adoptar dos posibles enfoques al caracterizar los trenes de paquetes para determinar la combinación óptima de las variables de reparación de trenes:

- 1) utilizar (múltiples) intervalos de paquetes establecidos arbitrariamente (según criterios de tiempo o número de paquetes), como se ha hecho anteriormente;
- 2) computar los intervalos de paquetes consecutivos degradados y los intervalos de transferencias de paquetes no degradados.

El enfoque que consiste en computar intervalos consecutivos parece tener una flexibilidad que no está presente en la evaluación basada en intervalos fijos; puede determinar el tamaño real de los intervalos degradados/no degradados en un tren y elude el problema de la alineación de los intervalos. Sin embargo, los parámetros resumidos que describen las longitudes de los intervalos degradados/no degradados son independientes de la secuencia real en la que se produjeron. Esta secuencia de cambios entre los intervalos degradados y los intervalos no degradados puede ser importante. Además, el cálculo de intervalos consecutivos requiere evaluar de alguna forma si se ha superado el umbral x , ya que esto es esencial para la definición de un resultado degradado. Si hay que evaluar más de un valor de x , pueden ser necesario pasar varias veces por los datos almacenados.

En cualquier caso, los resultados pueden expresarse como distribuciones de probabilidad o acumulativas sobre las variables dependientes e independientes, como muestra el ejemplo siguiente (Figura VII.3).

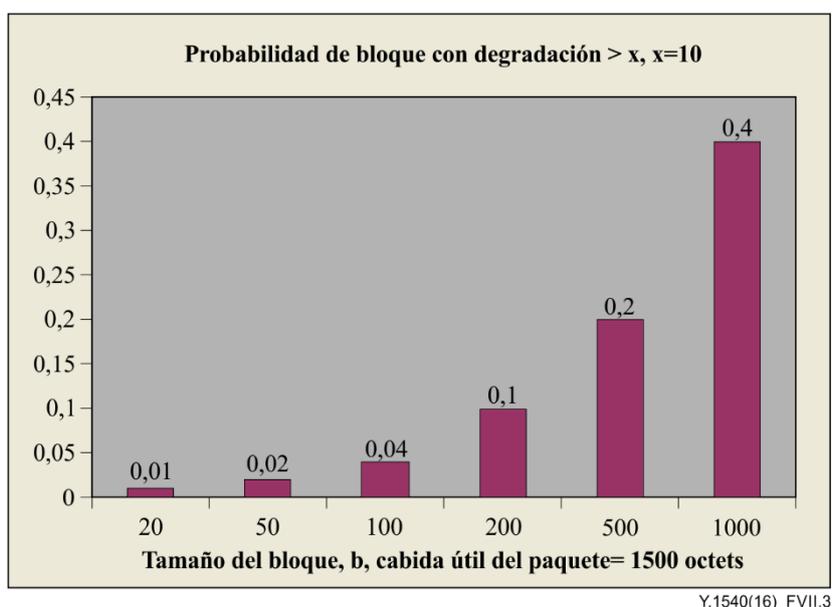


Figura VII.3 – Ejemplo de gráfico de los resultados de los parámetros de reparación de trenes para una gama de tamaños de bloque, donde x es un valor fijo y el tamaño del paquete es fijo

VII.6 Consideraciones adicionales

Aunque la caracterización de la red mediante los parámetros definidos anteriormente puede ser útil, deberían conocerse los detalles del sistema de reparación de aplicaciones para empezar a predecir la calidad entregada a los usuarios. Las técnicas FEC y ARQ producen diferentes patrones de pérdida de paquetes cuando operan más allá de su capacidad para realizar una corrección completa de las pérdidas. Los tamaños de bloque típicos asociados a cada técnica son diferentes y suelen ser mayores en el caso de ARQ.

Los esquemas FEC organizan el bloque de información y los paquetes de tara de diferentes maneras (a veces denominadas formas unidimensionales o bidimensionales) con esquemas menos sofisticados que tienen mayor sensibilidad entre el patrón exacto de pérdidas y su capacidad para corregirlas. El

diseñador debería conocer y tener en cuenta el margen de calidad de funcionamiento entre los esquemas FEC simples y el esquema de calidad de funcionamiento idóneo previsto por los parámetros anteriores.

Algunas aplicaciones pueden utilizar cadenas de las diversas técnicas descritas anteriormente. Por ejemplo, un sistema puede utilizar FEC o ARQ en combinación con la ocultación de errores en la capa de aplicaciones. En otro ejemplo, podría utilizarse FEC en una parte del trayecto, reservando ARQ o una FEC diferente para otra parte del trayecto, y finalmente emplear la ocultación de errores de la capa de aplicaciones.

Por último, los parámetros de calidad de funcionamiento a corto plazo definidos anteriormente pueden ser útiles para la resolución de problemas, ya que ayudan a identificar las firmas de los problemas de red, pero estos aspectos quedan en estudio.

Apéndice VIII

Marco de capacidad de la capa IP

(Este apéndice no forma parte integrante de la presente Recomendación.)

VIII.1 Introducción

Este apéndice proporciona información complementaria relacionada con las métricas de capacidad definidas en la cláusula 6.11.

Saber cuánta capacidad de la capa IP está disponible en tiempo real en una red IP (congestionada o no) es una información valiosa para los operadores de red y para los usuarios de las aplicaciones. Este parámetro puede utilizarse con fines de optimización de redes, supervisión de redes, resolución de problemas, selección de servidores o pasarelas, equilibrio de cargas, control de admisión, control de congestión, o para verificar el acuerdo de nivel de servicio (SLA) de una oferta de servicio garantizado o de categoría empresarial a través de un proveedor de red.

Los parámetros y métodos de medición definidos en el anexo normativo A sustituyen a la lista de proyectos académicos y ejemplos de herramientas que figuraban anteriormente en este apéndice, y abordan varios puntos que se enumeran a continuación con miras a su estudio ulterior.

VIII.2 Terminología y relación con IETF RFC 5136

En la bibliografía se utilizan indistintamente los términos "capacidad disponible" y "ancho de banda disponible". En [IETF RFC 5136] se examina la terminología, en particular la cuestión de si se debe utilizar la palabra *capacidad* o la expresión *ancho de banda* para describir las características IP. En [IETF RFC 5136] se propone utilizar el término *capacidad*, y a fin de armonizar criterios con el IETF, ese mismo término se utiliza también en la Recomendación UIT-T Y.1540.

En [IETF RFC 5136] se definen los parámetros relacionados con la capacidad de manera similar a como se definen en la cláusula 6.11. Sin embargo, una diferencia importante entre las definiciones del UIT-T y del IETF es que la Recomendación UIT-T Y.1540 tiene en cuenta que los anfitriones de red pueden afectar a los valores de los parámetros de capacidad de la capa IP. Esta cuestión no se aborda en [IETF RFC 5136], pero ha sido objeto de debate en el IETF. Los parámetros de UIT-T Y.1540 se definen sobre secciones básicas que tienen en cuenta de forma inherente la capacidad tanto de los enlaces como de los anfitriones de esa sección.

En el Cuadro VIII.1 se muestra una correspondencia entre los parámetros que constituyen las definiciones de la cláusula 6.11 y las definiciones de [IETF RFC 5136].

Cuadro VIII.1 – Asignación de parámetros entre UIT-T Y.1540 e IETF RFC 5136

Cláusula 6.11 de UIT-T Y.1540	IETF RFC 5136
Bits de la capa IP transferidos	Bits de la capa IP
Capacidad de la sección de la capa IP	Capacidad de enlace IP tipo P
Capacidad de la sección utilizada de la capa IP	Uso de enlaces IP tipo P
Utilización de la sección de la capa IP	Utilización de enlaces IP tipo P
Capacidad de la sección disponible de la capa IP	Capacidad de enlace IP tipo P disponible
Capacidad de NSE de la capa IP	Capacidad de trayecto IP tipo P
Capacidad de NSE disponible de la capa IP	Capacidad de trayecto IP tipo P disponible
Capacidad de la sección ajustada de la capa IP	No definido

VIII.3 Asuntos que quedan en estudio

En las definiciones de los parámetros de capacidad expuestas en esta Recomendación no se abordan expresamente los trayectos multipunto; sin embargo, se señala que este es un tema que queda en estudio.

Examinar e identificar los métodos de medición conformes con los requisitos de los operadores en lo que se refiere a la precisión de la medición, la velocidad y la tara.

¿Existe alguna forma de introducir un sistema de identificación del enlace estrecho de la capa IP?

Con miras a los futuros métodos de medición, las funciones de regulación causan la pérdida de paquetes, y esta forma de limitación puede requerir un método de evaluación diferente de aquellos que se basan en la dispersión de paquetes.

Apéndice IX

Explicación de la inadecuación de la medición basada en TCP para cumplir los requisitos normativos

(Este apéndice no forma parte integrante de la presente Recomendación.)

IX.1 Introducción

A los lectores de la presente Recomendación les puede resultar útil comprender las implicaciones de los requisitos normativos de la cláusula 6.12 al examinar las metodologías de medición, especialmente las basadas en las implementaciones disponibles del protocolo TCP. Si bien las mediciones basadas en el protocolo TCP se consideran útiles para realizar estudios informativos sobre la experiencia de los usuarios, no constituyen la base de métricas, métodos de medición u objetivos numéricos normalizados. La comparación del protocolo TCP con los requisitos de la cláusula 6.12 de este apéndice aclara su condición de método de medición.

IX.2 Comparación con los requisitos normativos

Los requisitos de la cláusula 6.12 se organizan en dos listas numeradas. La primera lista de requisitos se aplica a todos los parámetros, mientras que la segunda se refiere a los parámetros que evalúan la capacidad de mantener una determinada velocidad de transferencia de paquetes IP.

Respecto de la primera lista de requisitos (todos los parámetros):

- 1) Por lo que se refiere al requisito de computar la entrega de paquetes en la red y la transferencia satisfactoria: Algunas versiones de TCP pueden ofrecer el recuento de segmentos retransmitidos durante una conexión (a través de una interfaz de gestión), pero las retransmisiones se basan en la temporización de retransmisión (RTO) adaptable, no en la cuestión de si los paquetes realmente se perdieron o si se reconocen una vez transcurrida la temporización, o de si se perdió un ACK después de la entrega satisfactoria. Los receptores TCP no distinguen si los paquetes originales o retransmitidos (o ambos) llegan de forma satisfactoria. Además, los diferentes algoritmos de control de la congestión TCP varían en sus métodos para lograr la equidad con respecto a otros flujos y caudales, lo que incrementa el número de paquetes perdidos cuando se utilizan algoritmos agresivos, o reduce innecesariamente las velocidades de envío cuando las pérdidas de paquetes se interpretan de forma incorrecta como una señal de congestión (obsérvese la correspondencia fija de la pérdida de paquetes interpretada como congestión en el control de flujo TCP).
- 2) Por lo que se refiere a la capacidad necesaria para medir los trayectos parciales: El control de la congestión de TCP es muy sensible al tiempo de ida y vuelta (RTT) de forma no lineal y a veces inesperada. Por lo tanto, la medición basada en TCP en un trayecto parcial (EL o NS) no suele predecir la calidad de funcionamiento de un trayecto completo, y la dependencia del RTT en el TCP es una razón clave.

Respecto de la lista de requisitos para la evaluación de la velocidad de paquetes sostenida:

- 1) Por lo que se refiere a la descripción necesaria del patrón de tráfico ofrecido a la red: Las fases de inicio lento y de evitación de la congestión en TCP determinan el patrón de envío, y estos patrones varían notablemente según las condiciones del trayecto, especialmente la presencia de tráfico cruzado y las características de los atascos observados. Por lo tanto, el patrón es difícil o imposible de restringir o predecir con el funcionamiento del control de flujo de TCP.

- 2) Por lo que se refiere al requisito de limitar la velocidad de tráfico a un nivel inferior a la capacidad de los enlaces de conexión: El control de flujo de TCP sigue siendo útil para probar la capacidad disponible, en el supuesto de que las condiciones puedan cambiar. No es práctico limitar un emisor TCP a una capacidad exacta utilizando los parámetros disponibles, en parte debido a la variación del RTT durante la vida de una conexión TCP. Dicho de otro modo, un TCP siempre puede enviar tráfico a una velocidad que supere los enlaces de conexión.

Todas las dificultades causadas por el control de flujo TCP se agravan aún más al operar múltiples conexiones TCP simultáneas, cada una de las cuales evalúa independientemente su conexión en el mismo trayecto.

En conclusión, el protocolo de transporte se determina e implementa en los anfitriones de los usuarios, y queda fuera del ámbito de los proveedores de servicios de transferencia de paquetes basados en IP. Las evaluaciones normalizadas de la calidad de funcionamiento del proveedor de servicios deberían evitar la contribución de las capas elegidas por otros y deberían cumplir los requisitos normativos de la cláusula 6.12.

Apéndice X

Resumen de los resultados de laboratorio (fase 1) y de campo (fase 2): plan de evaluación del Anexo A

(Este apéndice no forma parte integrante de la presente Recomendación.)

X.1 Introducción

En su reunión intermedia de abril de 2018, y en las reuniones ad hoc durante la siguiente Plenaria de la CE 12 celebrada en mayo de 2018, respecto de la Cuestión 17/12 se acordó un plan para desarrollar métricas (también conocidas como parámetros) y métodos de medición para la evaluación de la capacidad IP (junto con la latencia y la pérdida de paquetes, otras métricas clave de la calidad de funcionamiento). Los trabajos comenzaron con la elaboración de un plan para la evaluación en laboratorio de algunas métricas y métodos existentes. En un nuevo Anexo A se documenta el plan para calificar y comparar las métricas, métodos, modelos y herramientas de medición del acceso en un entorno de laboratorio estable y repetible. Los trabajos se basan en los parámetros actuales de la cláusula 6.11 y en los requisitos de la cláusula 6.12.

Con el avance los trabajos, quedó claro que se requeriría un esfuerzo paralelo para armonizar la calidad de funcionamiento IP normalizada entre las diversas organizaciones de normalización para lograr una adopción amplia y rápida por parte de la industria. Entre esos esfuerzos cabe destacar la propuesta de un nuevo trabajo en TC ETSI STQ, y un llamamiento a la colaboración en el grupo de trabajo del IETF sobre mediciones de calidad de funcionamiento IP (con 2 voluntarios). Otras organizaciones de normalización (la CE 11 del UIT-T, ETSI TC INT y BBF) han recibido múltiples declaraciones de coordinación que describen los progresos actuales.

En las reuniones del otoño de 2018 se adoptó la decisión de dividir el plan de evaluación en dos fases, y se recogieron los primeros resultados de las pruebas de la fase 1. El plan de pruebas de la fase 1 se basó en la evaluación del ORECE de los sistemas de medición del acceso a Internet, que puede consultarse en [b-ORECE], donde el requisito 127 describía la prueba obligatoria de la precisión de la velocidad utilizando "software o hardware de conformación del tráfico" a múltiples velocidades de hasta 500 Mbps. No se aportaba información más detallada y se omitía el factor crítico de la latencia. En el nuevo anexo A se abordan estas y otras omisiones del plan del ORECE. En la evaluación de la fase 2 se investigarán las conclusiones de la fase 1 sobre las redes de acceso.

Las contribuciones a la C17/12 también se incluyeron dos encuestas de investigación académica sobre la medición de la calidad de funcionamiento del acceso a Internet. Al final de esta contribución se recoge la encuesta más reciente, junto con los puntos del taller de la CE 12 de noviembre de 2018, y se resumen varios puntos clave, siendo el más relevante que las pruebas basadas en UDP se consideran el punto de referencia para la capacidad.

En esta contribución se resumen las pruebas y los resultados de CE 12-C275, TD 627 y TD 701-R2, hasta enero de 2019. Una contribución complementaria da seguimiento a los debates y preguntas en la reunión intermedia de la C17 (virtual, enero de 2019), y proporciona nuevos resultados de laboratorio para múltiples métricas, herramientas y métodos de medición.

X.2 Configuración de las pruebas de laboratorio de la fase 1

En esta cláusula se describen dos alternativas principales para crear un entorno de prueba controlado y aislado como base para las comparaciones repetibles entre los métodos de prueba.

La figura siguiente ilustra dos utilidades diferentes que proporcionan un control flexible del tráfico/velocidad en una plataforma informática genérica. Las diferentes utilidades de control de tráfico pueden aplicarse de tres maneras.

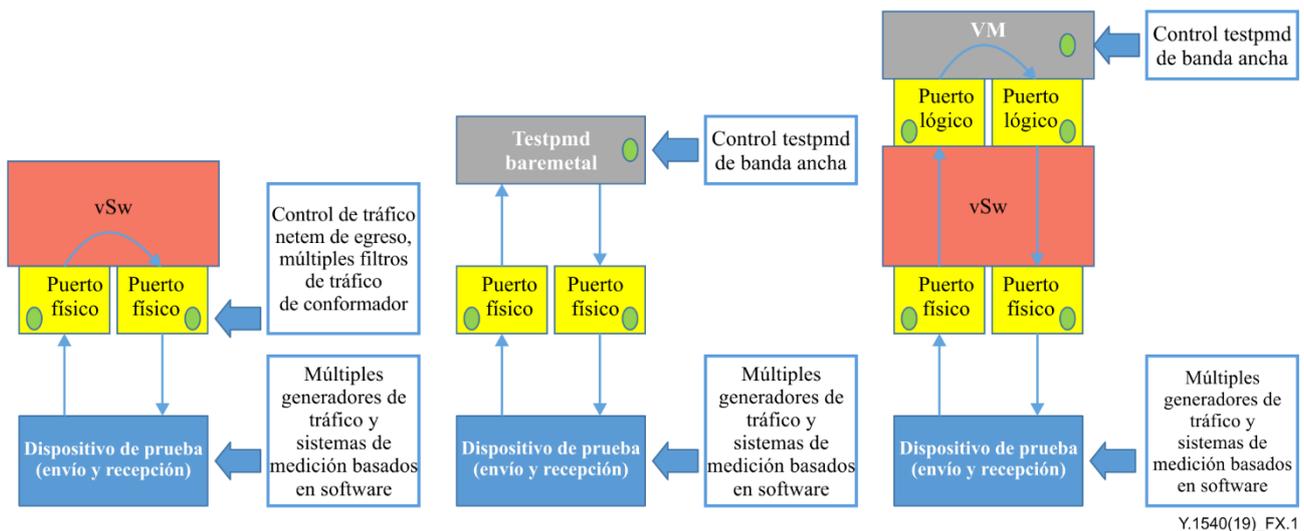


Figura X.1 – Tres posibles trayectos de ensayo en una plataforma informática genérica

En la Figura X.1, el dispositivo de prueba está conectado a un computador principal genérico general mediante enlaces físicos a 10 Gbps. El dispositivo de prueba también es un computador principal genérico, pero está completamente aislado del computador principal que realiza el control del tráfico, lo que permite que cada nodo dedique recursos a sus funciones únicas en el entorno de prueba. A través del nodo de control de tráfico se pueden instalar y probar diferentes implementaciones de métodos de medición.

Hay tres formas de implementar la función de conformación del tráfico. La primera, que se muestra a la izquierda, emplea el emulador equipado con el kernel de Linux, netem, que puede emular el retardo y ayudar al control del tráfico, una vez configuradas la tarjeta de interfaz de red (NIC) y las interfaces físicas correctas. El vSwitch simplemente conmuta las tramas entre sus dos puertos. Esta configuración se denomina comúnmente "phy2phy".

La configuración phy2phy se utilizó para las pruebas y los resultados que se describen a continuación. Véase una descripción de las configuraciones restantes (utilizando el testpmd de Intel DPDK) en el Anexo A.

X.3 Configuración detallada de las pruebas

La figura siguiente ilustra los detalles de la configuración de la prueba "phy2phy" con dos nodos anfitriones, sistemas de medición, interfaces de red con enlaces de 10 Gbps y configuraciones que incluyen un espacio de nombres de red y un conmutador virtual abierto (OVS). Los anfitriones se encuentran en un laboratorio OPNFV gestionado por Intel [b-Pod12].

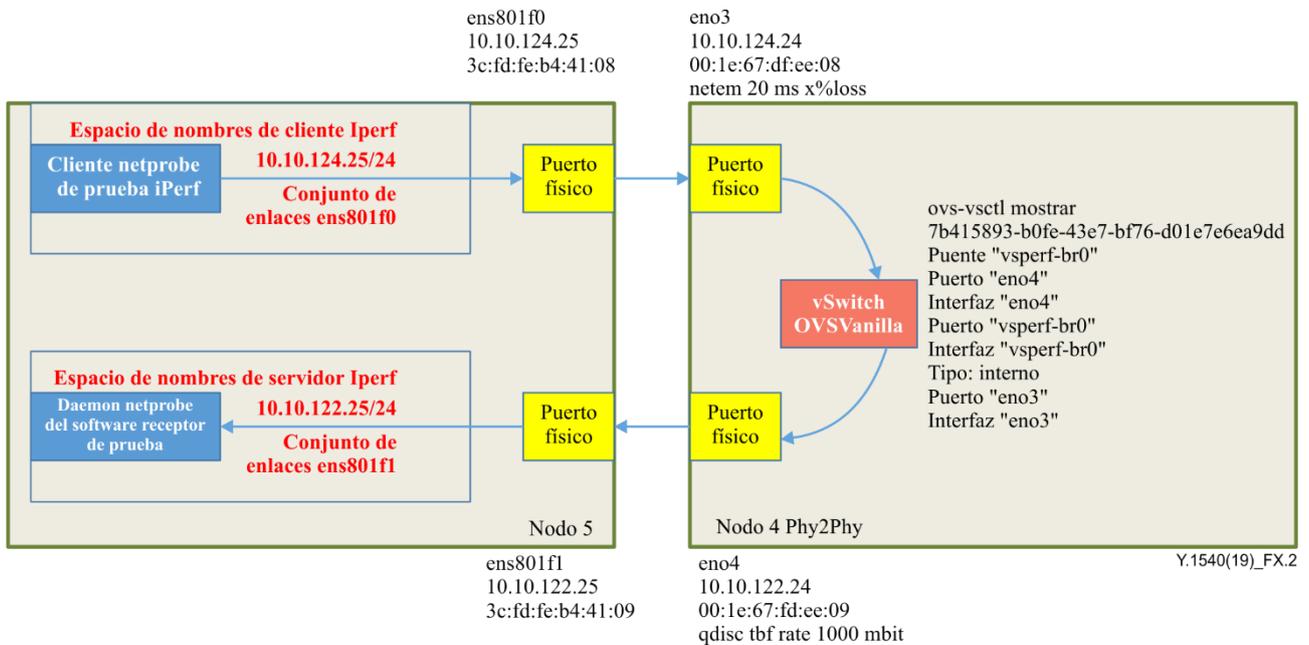


Figura X.2 – Configuración de la prueba con iPerf, red calibrada (DUT) y tráfico en competencia (mediciones)

El espacio de nombres de la red es esencial para obligar al tráfico a salir por las interfaces de red asociadas y evitar el encaminamiento interno a través del núcleo. La herramienta Netprobe puede proporcionar tanto el tráfico UDP en competencia como un subtren del tráfico global con mediciones de pérdida y latencia por paquete (de un solo sentido y de ida y vuelta en resolución de milisegundos).

X.4 Herramientas de pruebas

En las evaluaciones se han utilizado diversas herramientas de medición de código abierto que han dado lugar al presente resumen y a las decisiones tomadas durante el proceso. Se trata de Ciscos' T-rex, iPerf 2, iPerf 3, NetProbe y una nueva herramienta que todavía carece de nombre. Las funciones de conformación y de regulación de tráfico forman parte de la distribución típica de Linux, al igual que el emulador de degradación de la red netem.

Las primeras pruebas UDP con T-rex apoyaron la evaluación de la fase 1, y desplegaron el algoritmo de búsqueda avanzada binaria con verificación de pérdidas (BSwLV) especificado en [b-TST 009]. Sin embargo, las opciones metodológicas (determinación de la pérdida mediante contadores Tx y Rx no sincronizados) y la difícil activación de las pruebas TCP alentaron la investigación de otras herramientas.

Aunque iPerf 2 ha sido superada por el desarrollo de iPerf 3, las pruebas actuales han determinado que la configuración de iPerf 2 es más predecible, una vez que se dominan algunos detalles de su funcionamiento. En todo este resumen se utiliza iPerf 2 (salvo si se indica otra cosa). Se utilizan paquetes de tamaño MTU en todo momento. iPerf 3 en Linux presenta algunas "características" que no parecen resueltas (algunas configuraciones encuentran límites de velocidad de envío). Actualmente coexisten diversos desarrollos paralelos de iPerf3, y es necesario especificar el número de subversión para distinguir las diferentes fuentes.

NetProbe se ha utilizado exclusivamente como sistema de medición complementario (pues proporciona mediciones de latencia que iPerf 2/3 no ofrece), y como generador de tráfico en competencia (con capacidad de medición).

X.5 Calibración de los resultados comunicados con iPerf 2

La herramienta iPerf 2 informa de las mediciones de velocidad basadas en los bytes de cabida útil de transporte entregados (por encima de la capa UDP o TCP). La velocidad del filtro de colector de testigos (TBF) se especifica en "bits en tramas de capa 2 sin CRC ETH", de manera que los encabezamientos añadidos a las cabidas útiles de transporte se incluyen en los cálculos del TBF (la velocidad incluye ETH, IP y bits de encabezamiento de transporte).

Los cálculos de la velocidad de recepción "con OH" incluyen la tara por paquete de octetos en los siguientes encabezamientos: ETH (14), IP(20) y UDP(8) o TCP(20). Una velocidad de cabida útil UDP típica de 972 Mbps corregida por la tara (1,0286) es de 999,799 Mbps.

El tamaño de una trama TCP es variable, ya que iPerf 2 envía un bloque de 8kB al remitente, lo que da como resultado cinco tramas con tamaño MTU y 892 bytes restantes para completar el bloque. Sin embargo, el tamaño de los paquetes varía con respecto a este modelo cuando se observa en una traza de paquetes. El factor de corrección más sencillo para la tara (OH) en los trenes TCP utiliza solo el tamaño de segmento máximo (MSS) en el cálculo:

$54+1446 = 1500$; $1500/1446 = 1,0373$ * la velocidad de cabida útil TCP medida.

Una velocidad de cabida útil TCP del extremo superior con 3 conexiones (y sin factores de complicación como el retardo) de 956 Mbps es de 991 Mbps cuando se corrige la tara. La mayoría de las velocidades de cabida útil TCP medidas con una velocidad de conformación calibrada de 1 Gbps son sensiblemente inferiores a 956 Mbps (véanse las figuras X.4 y X.5).

También hay cierta incoherencia entre el tamaño máximo de la ventana de recepción TCP (RWIN) calculado por iPerf 2 y el valor medido con 20 ms de RTT. Una prueba con 3 conexiones TCP dio como resultado:

$956 \text{ Mbps} / 3 \text{ conexiones} = 318\ 666\ 666 \text{ bps}$ por conexión;

$318\ 666\ 666 / 50 \text{ ventanas por segundo} = 6\ 373\ 333,32 \text{ bits en RWIN}$

o $796\ 666 \text{ bytes} \sim 0,8 \text{ MBytes}$ (no $0,08 \text{ MBytes}$ como informó iPerf 2).

X.6 Resumen del enfoque y los resultados de las pruebas

En la siguiente figura se resume parte de las pruebas iniciales (hasta noviembre de 2018).

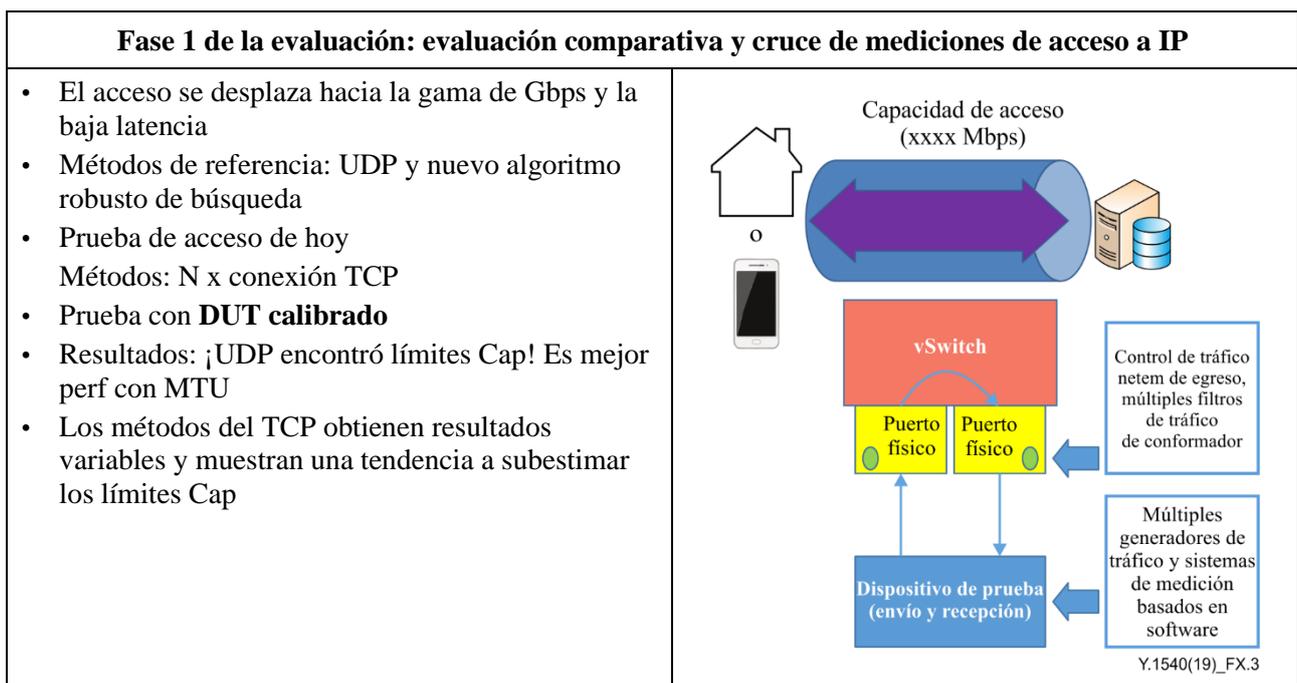
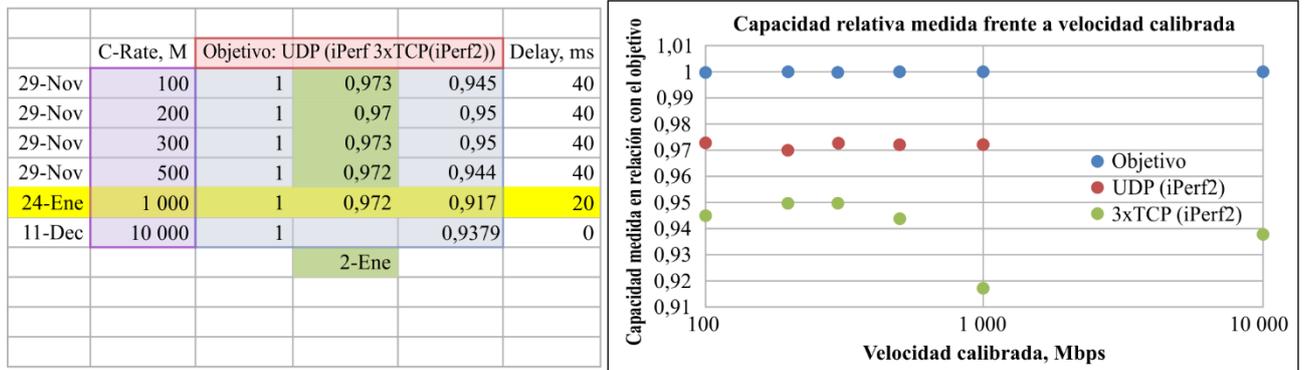


Figura X.3 – Resumen de las pruebas iniciales

X.7 Resumen de las pruebas en que se compara la capacidad medida con las velocidades PHY calibradas

La configuración de la prueba (descrita en la Figura X.2) consiste en un filtro del colector de testigos (TBF, *token bucket filter*) en el Nodo 4 eno4 con una velocidad objetivo configurable y permite definir la frecuencia de ráfagas, pero también establece el tiempo máximo que cualquier paquete puede permanecer en el procesamiento (normalmente 4 ms). 100 Mbps es una de las velocidades más altas que se pretendía utilizar en [b-ORECE] para las verificaciones en Req-127. La mayoría de los resultados de esta sección están influidos por el retardo simulado (en netem).



Y.1540(19)_FX.4

Figura X.4 – Resumen de la capacidad medida frente a las velocidades calibradas

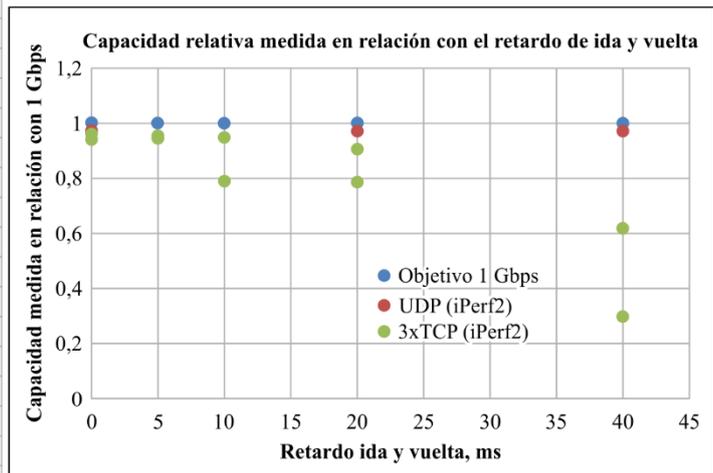
Como muestra la Figura X.4, los métodos basados en UDP de iPerf 2 funcionan aproximadamente sin pérdidas a la velocidad configurada en el TBF, por ejemplo, 972 Mbps en cargas útiles UDP (que se corrige a 1 001 Mbps teniendo en cuenta los encabezamientos). Las mediciones con 3 conexiones TCP son sensibles al retardo de ida y vuelta, sobre todo cuando la velocidad del TBF aumenta a 1 000 Mbps (y la corrección de los encabezamientos no es suficiente para compensar (aunque el momento de inicio del TCP es un factor, se alcanzan 956 Mbps después de 2 segundos).

Las mediciones de enlaces de 10 000 Mbps (10 Gbps) por sí solas (sin TBF ni netem) representan una fuente muy práctica de limitación de la velocidad. Las pruebas con 3 conexiones TCP y 5 conexiones TCP en estas condiciones realistas siguieron subestimando la velocidad PHY después de aplicar los factores de corrección de encabezamiento. iPerf 2 y T-rex no pudieron generar un solo tren UDP por encima de ~5 Gbps en esta configuración de prueba (este resultado se investigó más a fondo: dos clientes de iPerf 2 generaron simultáneamente 3,94 + 4,18 = 8,12 Gbps, y parece que se necesita un tercer tren).

X.8 Resumen de las pruebas que comparan la capacidad medida con el retardo de ida y vuelta

Utilizando una única velocidad TBF objetivo de 1 Gbps, se emuló un retardo constante en el trayecto de ida y vuelta (en el nodo 4 eno3) mediante netem.

	Retardo, ms	Objetivo: 1G UDP (iPerf 3xTCP(iPerf2))		
27-Ene	40	1	0,972	0,62
27-Ene	40	1	0,972	0,312
27-Ene	40	1	0,972	0,313
27-Ene	40	1	0,972	
27-Jan	20	1	0,972	0,786
27-Feb	20	1		0,906
27-Feb	10	1		0,952
27-Feb	10	1		0,792
27-Feb	5	1		0,953
27-Feb	5	1		0,948
11-Dec	0	1	0,972	0,9379
27-Feb	0	1		0,956



Y.1540(19)_FX.5

Figura X.5 – Resumen de la capacidad medida frente al retardo de ida y vuelta a 1 Gbps

Las mediciones de latencia de Netprobe (véase la siguiente sección) confirman que, cuando el TBF limita la velocidad (y algunos paquetes se descartan), la latencia configurada del TBF añade hasta 4 ms a la latencia de netem (20 o 40 ms más) en el caso de algunos paquetes. Los resultados de las pruebas de capacidad UDP son inmunes a la latencia, pero permiten añadir las mediciones de latencia UDP de manera sencilla. Sin embargo, el bucle de control de flujo TCP es sensible a la latencia (en concreto, al tiempo de ida y vuelta), y sus mediciones de capacidad sufren el aumento del retardo (especialmente cuando el ancho de banda multiplicado por el retardo del producto supera la configuración del tamaño de la ventana de recepción máxima; véanse las mediciones a 40 ms en la Figura X.5).

A petición de los miembros de ETSI STQ, se realizaron pruebas de TCP a 5 ms y 10 ms, y se repitieron todas las pruebas de 0 ms a 20 ms. Los resultados muestran que la medición basada en TCP tiene resultados variables, y el retardo tiende a aumentar la variabilidad potencial. En [IETF RFC 8337] se señala este problema para las mediciones con control de flujo TCP, en la sección 4.

X.9 Resumen de las pruebas con tráfico en competencia

En esta cláusula se resumen tres pruebas en las que los trenes UDP y TCP intentan realizar mediciones de capacidad IP en presencia de un tren de tráfico en competencia (un tren a velocidad binaria constante de NetProbe, lo que permite medir el retardo de los paquetes y la variación del retardo de los paquetes, o PDV).

Cuadro X.1 – Tráfico a 1 Mbps en competencia con filtro del colector de testigos a 1 000 Mbps + Retardo "phy2phy"

Notas	Velocidad TBF	Ráfaga TBF, latencia	Latencia RT de netem	Herramienta	Tamaño trama, bytes	Velocidad Rx, Mbps	Med. lat.	Cómputo pérdidas	Precisión de la velocidad
27 de enero con netprobe enviando 1 156 800 bps	1 000 Mbps	5 kb 4,0 ms	40 ms (eno3)	iPerf2; UDP unidir - b 972000000	1 470 datos	971 Mbps	Fig X.6	798 en la mayoría de las pruebas	0,971
27 de enero con netprobe enviando 1 156 800 bps			40 ms (eno3)	iPerf2; UDP unidir - b 971000000	1 470 datos	971 Mbps	Fig X.7	245 (solo en el 1 ^{er} segundo)	0,971
27 de enero con netprobe enviando 1 156 800 bps			20 ms (eno3)	iPerf2; conexión TCP 3 unidir 12 seg.	5 MTU + resto 892	786 Mbps promedio Se alcanzan 955 M después de 10 segundos	Fig X.8	X	0,786 promedio 0,955 pico

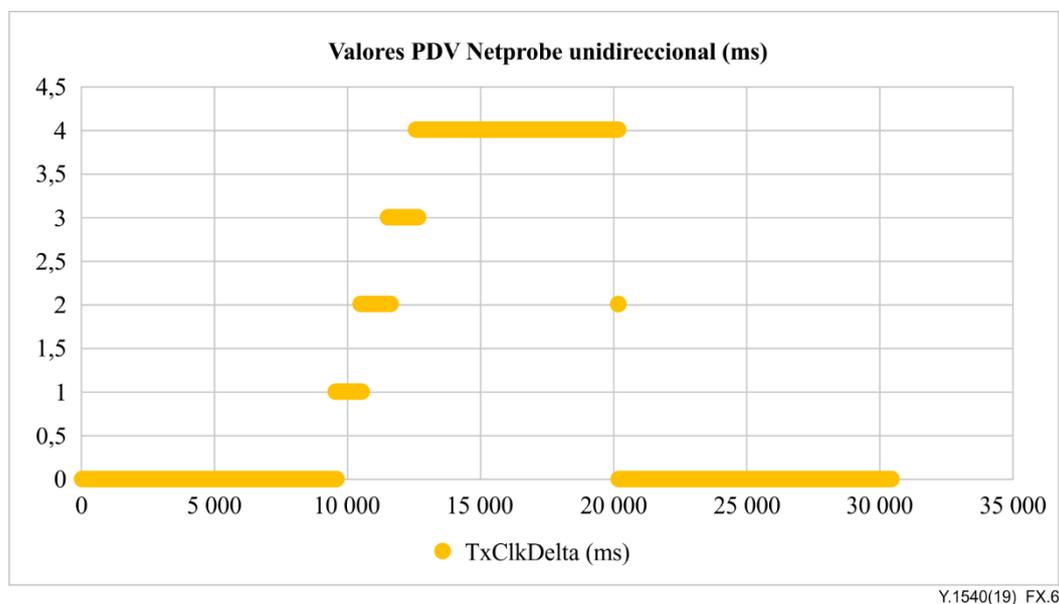


Figura X.6 – Medición con NetProbe de la variación del retardo de los paquetes durante 11 segundos UDP a 972 Mbps

Las mediciones con NetProbe ilustran el retardo observado cuando se excede la velocidad del filtro del colector de testigos (en aproximadamente 1 Mbps) durante el transcurso de la prueba iPerf UDP de 11 segundos (durante la prueba con NetProbe de 30 segundos). Hubo 3 pérdidas de paquetes en el tren de NetProbe, enviando 1 156 800 bps. La evaluación de la velocidad UDP se reduce por la cantidad de tráfico en competencia en esta prueba. Las mediciones de latencia de la Figura X.6 (PDV unidireccional) indican que la latencia máxima de TBF se alcanzó unos segundos después de que comenzara el tren iPerf 2.

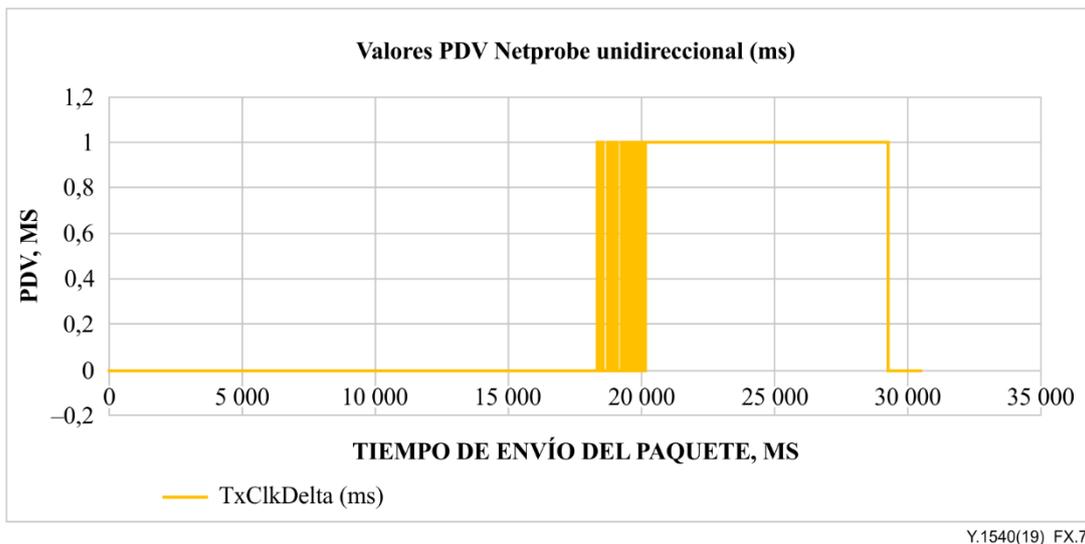


Figura X.7 – Medición con NetProbe de la variación del retardo de los paquetes durante 11 segundos UDP a @971 Mbps

Las mediciones con NetProbe ilustran el retardo observado cuando se alcanza la velocidad del filtro del colector de testigos (en aproximadamente 1 Mbps) durante el transcurso de la prueba iPerf UDP de 11 segundos (durante la prueba con NetProbe de 30 segundos). Hubo cero pérdidas de paquetes en el tren de NetProbe, enviando 1 156 800 bps.

La velocidad de envío UDP se redujo para adaptarla al tráfico en competencia, lo que indica que la prueba anterior (Figura X.6) evaluó correctamente la capacidad restante cuando había tráfico en competencia. Los trenes combinados se ajustan más a la velocidad de TBF. Las mediciones de latencia (PDV unidireccional) de la Figura X.7 indican que no se observó la latencia máxima del TBF (y que la latencia puede ser un dato de entrada útil para un algoritmo de búsqueda de velocidad [b-TST 009], además de la pérdida de paquetes).

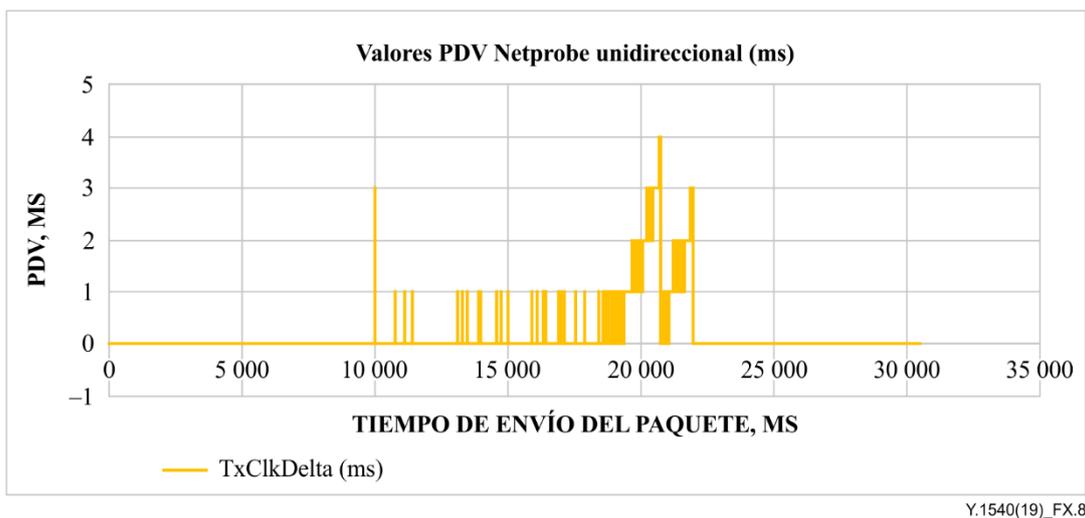


Figura X.8 – Medición con NetProbe de PDV durante 12 segundos de tres conexiones TCP

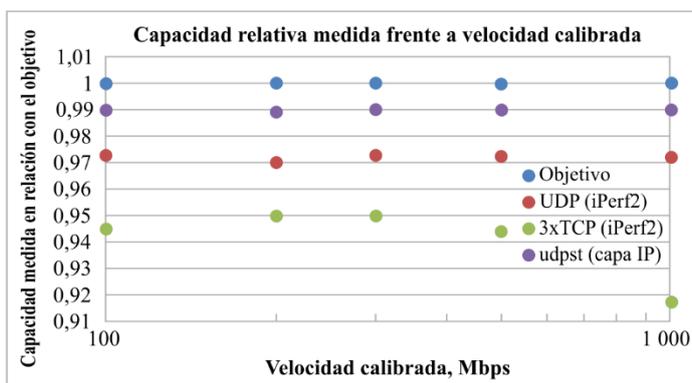
Las mediciones con NetProbe ilustran el retardo observado cuando se alcanza la velocidad del filtro del colector de testigos (en aproximadamente 1 Mbps) durante el transcurso de la prueba de conexión iPerf TCP 3 de 12 segundos (durante la prueba con NetProbe de 30 segundos). Hubo cero pérdidas de paquetes en el tren de NetProbe, enviando 1 156 800 bps. Cerca del final de la prueba TCP de 12 segundos, las 3 conexiones parecen haberse sincronizado y el PDV de NetProbe indica un retardo

en diente de sierra en el TBF (posiblemente siguiendo el patrón AIMD), hasta la latencia máxima del TBF de 4 ms.

X.10 Pruebas con la implantación temprana de una nueva herramienta de pruebas UDP

Una de las características de que carecen las pruebas UDP de iPerf 2 y 3 es un algoritmo de búsqueda que pueda determinar la capacidad IP de forma automatizada. En las pruebas anteriores, una prueba exploratoria de iPerf 2 determinaba la velocidad máxima de paquetes recibidos para el trayecto de prueba (normalmente mientras se perdía un volumen significativo de paquetes), y una segunda prueba a esa velocidad máxima de paquetes recibidos determinaba si era posible enviar a esa velocidad con cero pérdida de paquetes. La herramienta T-rex utilizó la búsqueda binaria [b-TST 009] con algoritmo de verificación de pérdida y logró detectar la velocidad de conformación real, pero requiere varias pruebas. Se observó que podría ser útil disponer de un algoritmo de búsqueda más rápido que tuviera en cuenta las pérdidas y otras degradaciones.

Velocidad C, M	Objetivo	UDP (iPerf 3xTCP(iPerf2))	udpst (IP-layer)	Hack-104
100	1	0,973	0,945	0,99
200	1	0,97	0,95	0,9892
300	1	0,973	0,95	0,9899
500	1	0,972	0,944	0,99
1 000	1	0,972	0,917	0,99
		2-Ene		



Y.1540(19)_FX.9

Figura X.9 – Comparación de la herramienta "udpst ver1.4" con la capacidad medida por iPerf frente a las velocidades calibradas

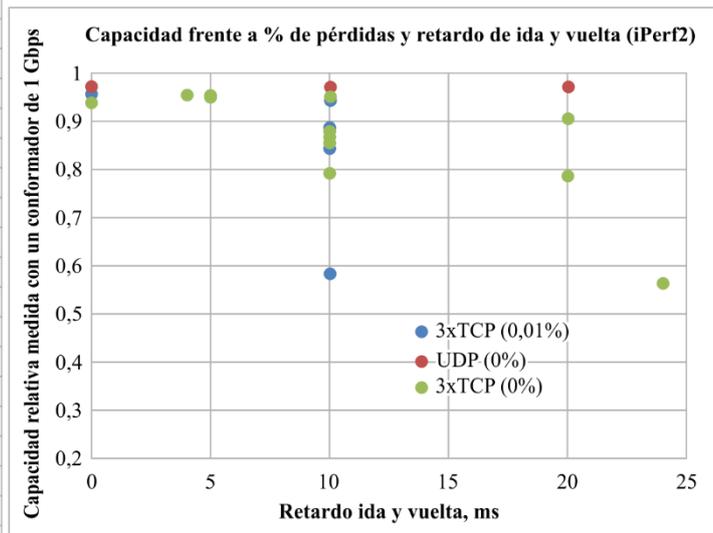
El udpst es un prototipo de herramienta de medición creado por Len Ciavattone. El algoritmo de búsqueda de udpst busca la máxima capacidad de IP ajustando su velocidad de envío según los mensajes de retorno que incluyen mediciones de pérdida y reordenación, junto a otra información sobre la variación del retardo. El receptor udpst envía mensajes de estado a intervalos regulares (por defecto 50 ms). La pérdida de paquetes, la reordenación o la variación excesiva del retardo provocarán reducciones de la velocidad de envío, hasta que las degradaciones dejen de estar presentes. Los resultados se notifican en la capa IP, incluyendo los bits del encabezamiento. Esto significa que el factor de corrección de una tara solo incluye el encabezamiento ETH (14 octetos). Un factor de corrección de la sobrecarga de 1,0112 (1264/1250) aplicado a la medición típica de 990 Mbps da como resultado 1,001 Gbps para la tasa de conformación calibrada de 1 Gbps.

X.11 Pruebas de los efectos de la pérdida de paquetes de bajo nivel

Una de las variables de evaluación de laboratorio de la fase 1 era la pérdida de paquetes. Las tasas de pérdidas iniciales seleccionadas fueron 10^{-4} y 10^{-5} , es decir, el 0,01% y el 0,001% del total de paquetes (como se especifica en **netem**). La distribución de pérdidas no estaba especificada, por lo que se eligió la aleatoria.

La Figura X.10 ilustra los resultados de la prueba, en la que se obtuvieron nuevos resultados con un 0,01% de pérdida o sin pérdida en varios retardos (el 22 de abril), y se representaron gráficamente junto con los resultados anteriores de condiciones sin pérdida.

	Retardo, ms	3xTCP (0.01% UDP (0%))	3xTCP (0%)
22-Abr	0	0,956	
22-Abr	0	0,957	
22-Abr	4		0,954
22-Abr	10	0,888	0,855
22-Abr	10	0,584	0,972 0,87
22-Abr	10	0,844	0,879
22-Abr	10	0,85	
22-Abr	10	0,942	
22-Abr	24		0,564
27-Ene	20		0,972 0,786
27-Feb	20		0,906
27-Feb	10		0,952
27-Feb	10		0,792
27-Feb	5		0,953
27-Feb	5		0,948
11-Dic	0		0,9379
27-Feb	0		0,956



Y.1540(19)_FX.10

Figura X.10 – Resumen de la capacidad medida frente a las pérdidas y el retardo de ida y vuelta a 1 Gbps

En primer lugar, hay que tener en cuenta que la pérdida del 0,01% por sí sola, sin retardo añadido, tuvo poco efecto en la capacidad medida con TCP en la capa de transporte. Por supuesto, una tasa de pérdida más alta (del 1%) causaría una reducción bastante significativa en la velocidad medida (aproximadamente un factor de 10 de reducción). Cuando se añade un retardo de ida y vuelta de 10 ms, la variación de las velocidades TCP es sustancial con o sin pérdidas. Una prueba con pérdidas y un retardo de 10 ms dio como resultado <600 Mbps, y este escaso rendimiento fue similar a una medición reciente de 24 ms de retardo (posiblemente con la presencia de una pequeña cantidad de pérdidas). En un caso con 10 ms de retardo, la inserción de la pérdida del 0,01% parecía aumentar la velocidad TCP, que es el tipo de calidad de funcionamiento no lineal descrita en la sección 4 de [IETF RFC 8337].

Al probar UDP con iPerf2, las tasas de pérdida emuladas se reflejan en los resultados (con la variabilidad esperada de 1 segundo entre los informes) y en la suma final.

La conclusión es que la variabilidad de las mediciones TCP está dominada principalmente por el retardo de ida y vuelta cuando la tasa de pérdidas es baja (del 0,01%).

X.12 Examen de las limitaciones máximas de transmisión de las herramientas de pruebas y de la plataforma

Aunque las velocidades calibradas/reales de hasta 1 Gbps eran el objetivo principal del plan de pruebas de laboratorio de la fase 1, también es útil conocer los límites superiores del software de las herramientas de prueba en combinación con el hardware que las alberga. Se realizaron pruebas para examinar esta limitación con iPerf2 para el transporte UDP y TCP en varias ocasiones. La configuración de la prueba es simplemente la ruta hacia el OVS vSwitch a través de enlaces de 10 Gbps sin conformador de tráfico TBF ni impedimentos netem.

Las pruebas más concluyentes de estos límites se realizaron durante el hackathon IETF-104. Dos pruebas con conexiones 3xTCP produjeron 9 385 Mbps y 9 380 Mbps, y esto se comparó favorablemente con pruebas que datan de 11 de diciembre de 2018. Las pruebas con trenes 3xUDP produjeron 9 308 Mbps, y hubo un 1,8% de pérdida y unos 1 500 paquetes reordenados en una prueba de 10 segundos (cada tren intentaba generar 3 330 Mbps, pero no alcanzó esta velocidad).

La conclusión fue que hay suficiente capacidad de generación y recepción de paquetes UDP y TCP para realizar pruebas a 1 Gbps, y probablemente a velocidades algo mayores teniendo en cuenta las mediciones de casi 10 Gbps anteriores.

X.13 Examen de las pruebas con degradaciones tempranas en los trenes UDP

En varias pruebas de UDP de iPerf 2, se informó de que el primer segundo del tren de paquetes daba lugar a una reordenación de paquetes (normalmente menos de 40 paquetes) y una pequeña cantidad de pérdida de paquetes, y estas observaciones se aplican a casos con un conformador TBF de 1 Gbps. Para investigar la causa de las primeras degradaciones, se analizó el tren UDP (utilizando tshark) en la interfaz eno4 (justo antes de la operación del conformador).

Los datos obtenidos de paquetes se examinaron más a fondo con la herramienta Wireshark, especialmente la sincronización de los primeros paquetes en el tren UDP. Se comprobó que los tiempos de llegada de los primeros paquetes eran irregulares hasta la entrada de 20 paquetes o más en el tren, donde finalmente se alcanzó el espaciado nominal de 12 microsegundos. No se indican los números de secuencia, por lo que el remitente de iPerf o el trayecto de prueba pueden haber causado cierto reordenamiento en la parte del tren con ráfagas, y el conformador puede haber descartado los paquetes que excedieran de sus especificaciones.

X.14 Examen de los parámetros del conformador TBF utilizados en las pruebas y comparación con el filtro regulador

Se realizó una serie de pruebas para determinar si los parámetros de conformación utilizados en la mayoría de las pruebas habían perjudicado de modo desigual a los trenes TCP. Las pruebas con velocidades de conformación de 1 Gbps concluyeron que cuando el parámetro TBF de latencia máxima se redujo de 4 ms a 0,1 ms, la capacidad medida de TCP disminuyó significativamente (las pruebas de TCP con 4 ms registraron un máximo de 956 bps, pero la calidad de funcionamiento con una latencia de 0,1 ms fue muy variable y se situó en la gama de 763 a 862 Mbps). Por otra parte, el aumento del parámetro TBF de latencia máxima de 4 ms a 20 ms no ofreció ningún beneficio para la capacidad medida de TCP. Las pruebas UDP de iPerf 2 fueron insensibles a estos cambios.

Cuando se implementó un filtro regulador en lugar del conformador, de nuevo la capacidad medida de TCP disminuyó significativamente, a pesar de los intentos de mejorar la calidad de funcionamiento con el ajuste de parámetros (las pruebas de TCP con conformador obtuvieron un máximo de 956 Mbps, mientras que la calidad de funcionamiento más alta con el regulador fue de 2,02 Mbps). Las pruebas UDP de iPerf 2 fueron insensibles al uso del filtro regulador, debido a su tren a velocidad binaria constante.

X.15 Resumen de las pruebas de laboratorio de la fase 1

Las evaluaciones basadas en TCP con iPerf 2 tienden a subestimar la capacidad calibrada, y las estimaciones son:

- menos precisas que las de UDP para velocidades elevadas, como 1 Gbps (el estado actual del servicio de acceso a Internet);
- más sensibles al retardo de ida y vuelta que las de UDP, especialmente en lo que respecta a la variabilidad de las mediciones TCP, debido al control de flujo de TCP;
- más sensibles al tráfico en competencia, lo que da lugar a una medición promedio baja debido al mayor tiempo necesario para alcanzar el equilibrio.

Las mediciones UDP con iPerf 2 confirman el estado de "punto de referencia" para la evaluación de la capacidad, en consonancia con las velocidades calibradas (los datos reales experimentales) y la investigación sustancial con tecnologías/velocidades de acceso de menor categoría.

La latencia puede ser una entrada útil para un algoritmo de búsqueda de velocidad basado en UDP, además de la pérdida de paquetes, como se especula en [b-TST 009]. Un prototipo de herramienta de prueba UDP (udpst ver1.4) aspira a satisfacer esta necesidad de buscar automáticamente una velocidad máxima con UDP.

X.16 Especificaciones de la plataforma

Véase: <https://wiki.opnfv.org/display/pharos/Intel+POD12>.

X.17 Resumen de los resultados de las pruebas de campo de la fase 2

Los resultados que se resumen a continuación (realizados en dos campañas de prueba) se obtuvieron con los siguientes tipos de acceso:

- 1) Fijo: Módem de cable DOCSIS 3.0 con capacidad de tría y WiFi integrado y conmutador GigE por cable.
- 2) Móvil: Teléfono móvil LTE con un módem Cat 12 (600 Mbps de enlace descendente, 50 Mbps de enlace ascendente).
- 3) Fijo: red óptica pasiva (PON) "F", servicio de 1 Gbps.
- 4) Fijo: Servicio PON "T", 1 000 Mbps.
- 5) Fijo: VDSL, servicio a varias velocidades <100 Mbps.
- 6) Fijo: ADSL, 1,5 Mbps.
- 7) Móvil: Encaminador habilitado para LTE con ETH LAN a anfitrión (estacionario).

El consenso sobre los resultados de las mediciones fue que UDP es el protocolo de transporte preferido para la evaluación de la capacidad:

- UDP indicó resultados más sistemáticos.
- Las herramientas UDP pudieron medir la pérdida, el retardo, la variación del retardo y el reordenamiento.
- TCP registró velocidades más bajas que las pruebas de UDP y una mayor variabilidad de la velocidad en diversas circunstancias.
- Las mediciones de TCP en la PON de 1 Gbps muestran una subestimación significativa de la capacidad.
- Las conclusiones de laboratorio sobre UDP como punto de referencia y TCP como subestimación de la capacidad se vieron respaldadas por las mediciones de campo.
- Las pruebas de acceso a LTE indicaron una variabilidad significativa, como es de esperar en cualquier red inalámbrica.

Apéndice XI

Breve estudio sobre la investigación de la QoS y la QoE relacionadas con el acceso a Internet

(Este apéndice no forma parte integrante de la presente Recomendación.)

XI.1 Introducción

Los proveedores de servicios, las autoridades reguladoras (y de protección del consumidor), así como los vendedores y operadores de sistemas de medición, tienen interés en las mediciones de la velocidad de acceso a Internet (IAS) por diversas razones. Las encuestas que caracterizan los productos de acceso a Internet de los proveedores de servicios están bien establecidas en muchos países. En este ámbito, la normalización puede consistir en el seguimiento de los despliegues existentes. Las encuestas que informan de las estimaciones de la IAS no requieren una gran precisión y suelen ser aceptadas por los proveedores de servicios que compiten entre sí, si la parte que realiza la encuesta proporciona de forma transparente un conjunto equilibrado de parámetros relacionados con la campaña de medición a los proveedores de servicios que serán objeto de la encuesta.

También revisten interés las mediciones exactas normalizadas de la IAS. Al igual que ocurre con otras mediciones exactas de velocidad o volumen en las que se basan las obligaciones o sanciones en los mercados comerciales, las mediciones exactas normalizadas de la IAS requieren una precisión definida. La determinación de una precisión de medición requiere la determinación de un punto de referencia de medición.

Se espera que las publicaciones científicas permitan a otros investigadores reproducir los resultados publicados. Esta contribución examinó un conjunto de publicaciones científicas, buscando resultados pertinentes para los parámetros de calidad del servicio relacionados con el acceso a Internet, las mediciones y la evaluación. El enfoque incluye las mediciones de la IAS, pero no se limita a este factor. La comunidad investigadora está interesada principalmente en la medición de la calidad de experiencia (QoE) y en los parámetros de calidad de servicio (QoS) relacionados con el acceso a Internet. Algunos de los enfoques adoptados por la investigación relacionada con la QoE parecen indicar parámetros de QoS que caracterizan el acceso a Internet y los componentes que intervienen en una comunicación de extremo a extremo de forma más exhaustiva que la estimación de la velocidad de acceso. También se investiga este último conjunto de parámetros de QoS. Los extractos de texto y las referencias proporcionadas por esta contribución ayudan a basar el debate sobre la evolución de las normas en argumentos y no en opiniones.

Obsérvese que, siempre que ha sido posible, se han elegido estudios basados en enfoques validados por mediciones más o menos a gran escala utilizando accesos comerciales. Las referencias [2], [4], [6], [7], [8] y [10] cumplen este criterio.

XI.2 Principales conclusiones

En esta cláusula se resume la calidad del servicio (QoS) relacionada con el acceso a Internet y el uso del acceso, los indicadores fundamentales de rendimiento (IFR) y los métodos de medición recogidos en publicaciones científicas.

Una medida de referencia de la velocidad de acceso máxima alcanzable se obtiene inundando el enlace de acceso con tráfico UDP [1]. Además, en un estudio científico a gran escala se utiliza UDP para medir con precisión la velocidad de acceso [2]. Un importante proveedor de OTT incluye funciones de medición UDP en una herramienta interna de medición de velocidad [3].

Una conclusión relacionada con las mediciones basadas en TCP paralelo es que pueden utilizarse para estimar el ancho de banda de acceso a Internet [1]. En algunas publicaciones se discuten factores específicos que afectan a la precisión de las mediciones basadas en TCP paralelo y se examinan con mayor detalle algunas de estas degradaciones [1], [2], [4]. Las mediciones basadas en TCP paralelo capturan el ancho de banda efectivo disponible en presencia de tráfico de fondo [1]. Obsérvese que el ancho de banda disponible es idéntico a la velocidad de acceso a Internet solo en ausencia de tráfico de fondo. Las mediciones basadas en TCP paralelo no detectan la presencia de tráfico de fondo. Existen herramientas y métodos para diagnosticar la presencia de tráfico de fondo [1], [2].

En [14] se constató que UDP es un protocolo de transporte común viable. Esta afirmación se basa en pruebas realizadas en América del Norte y del Sur, Europa, Asia y Oceanía (sobre todo en África). Los autores observaron que el tráfico UDP se bloquea en algunos puertos o de forma total en casos raros. Se ha comprobado que la degradación de UDP se produce en las redes empresariales y en las "redes de regiones geográficas con una conectividad de otro tipo". En los casos en que falla el transporte UDP, se recomienda un repliegue al transporte TCP. El impacto de la Wi-Fi en la QoE de las aplicaciones puede caracterizarse mediante la recogida pasiva de estadísticas de puntos de acceso básicos, como propone [10]. Los autores documentan una reducción general de la QoE para la media de TxPhy por Wi-Fi inferior a 15 Mbit/s.

Muchas aplicaciones aplican el transporte cifrado. En esos casos, la información de los paquetes y del flujo IP se analiza en la evaluación de la QoE basada en la red. [11], [12] y [13] sugieren parámetros de QoS de red que se correlacionan con la QoE de los flujos continuos. Los parámetros propuestos en esas referencias pueden ser útiles para comparar y caracterizar también el acceso IP.

La difusión de los teléfonos inteligentes acrecienta el interés de los OTT, los proveedores de servicios y la investigación en la QoE resultante de la QoS de la red móvil. Las publicaciones científicas analizadas indican o declaran explícitamente que las mediciones paralelas basadas en TCP no proporcionan información útil para este fin.

La fluctuación del ancho de banda de la red móvil se correlaciona con la QoE del abonado en las condiciones habituales de la red inalámbrica (como, por ejemplo, la movilidad del abonado). Los flujos continuos de vídeo populares adaptan la calidad de vídeo para hacer frente a esas condiciones. En un entorno con fluctuaciones de ancho de banda, la correlación de la QoE del abonado con los IFR de la QoS requiere tener en cuenta otro parámetro aparte del ancho de banda medio disponible, como el máximo caudal medio; véase [6], [7], [8]. En general, las mediciones de la latencia de las aplicaciones del usuario o del RTT se mencionan como IFR obligatorios. Las publicaciones indican que, a fin de deducir la satisfacción del abonado con el acceso a Internet LTE a partir de las mediciones de la QoS, es necesario obtener IFR relacionados con el producto-anchura de banda-retardo (o bits en vuelo) o la fluctuación del ancho de banda, respectivamente [6], [7], [8].

El ancho de banda sigue siendo barato en los mercados pertinentes de un importante proveedor de OTT. La calidad de funcionamiento de la web percibida por el usuario es la principal métrica de los servicios de red modernos para este OTT. La latencia de la web es el principal impedimento para mejorar la QoE del usuario en los mercados pertinentes del OTT [5]. El diseño del TCP limita las mejoras desde la perspectiva de los OTT. Cierta tiempo después de la publicación de [5], el IETF comenzó a trabajar en QUIC, un nuevo protocolo de transporte basado en UDP.

En una publicación se concluye que, en los entornos LTE móviles de muchos mercados principales de OTT, las implicaciones de su investigación para el usuario final parecen claras: los abonados no necesitan un contrato de telefonía móvil de superalta velocidad, si su uso principal del acceso móvil es el flujo continuo de vídeo o la navegación por la web ([7], obsérvese que esta afirmación solo es válida de forma fiable para la ubicación y el momento de la evaluación). Se hicieron afirmaciones similares para el acceso fijo a Internet [5], y [9] también parece indicar lo mismo. Estas evaluaciones no son válidas a nivel mundial. Las conclusiones indican que la satisfacción del abonado con el acceso a Internet puede dejar de estar relacionada con la velocidad de acceso a Internet, si ésta proporciona un rendimiento medio estable muy superior al necesario para producir una alta QoE del abonado.

XI.3 Análisis de las publicaciones científicas relacionadas con las mediciones de la QoS y la QoE

En los años 2010 a 2012, las mediciones de la velocidad de acceso a Internet fueron objeto de algunas publicaciones científicas. Posteriormente, el interés de la comunidad investigadora se desplazó hacia la calidad de la experiencia del consumidor de Internet. Esto no significa que el ancho de banda de acceso a Internet, sus propiedades y las mediciones de la calidad del servicio hayan quedado fuera del alcance de los investigadores en los últimos años. Los parámetros de QoS del acceso a Internet y su medición se siguen investigando, si su medición se correlaciona con la QoE del consumidor.

XI.3.1 Medición de la velocidad de acceso a Internet fija

Goga y Texeira [1] investigaron herramientas que sirven para estimar la velocidad de acceso a Internet. A fin de eliminar las interferencias no deseadas, las mediciones se realizaron en horas no pico y con una red fija. El objetivo del trabajo era comparar las herramientas de medición de ancho de banda disponibles. A tal efecto, se determinó la precisión y la carga de medición de estas herramientas midiendo el acceso a Internet de proveedores comerciales de ADSL y cable con tráfico cruzado controlado.

Los autores evaluaron la IAS midiendo la capacidad de acceso UDP obtenida al inundar el enlace con tráfico UDP. Después estimaron la IAS mediante herramientas basadas en TCP.

En ausencia de tráfico cruzado, pueden calcularse los siguientes errores relativos de estimación frente a la referencia a partir de sus resultados obtenidos en mediciones fuera de las horas punta o sin tráfico cruzado:

Inundación basada en TCP ("Speedtest"): 4,06% en el mejor de los casos, 5,28% de error medio, 6,8 % en el peor de los casos

Por término medio, se subestima el ancho de banda de acceso.

La inundación basada en TCP no detecta el tráfico cruzado. Esto se demuestra con una prueba en la que un único flujo TCP está activo mientras se realiza una prueba de velocidad basada en TCP. Esta última estima su ancho de banda disponible, pero no la IAS. Existen herramientas para detectar la presencia de tráfico de fondo.

Los autores detectan que las tasas de procesamiento de paquetes de las pasarelas domésticas son limitadas, si estas actúan como traductores de direcciones de red. De ahí que la selección del tamaño de los paquetes de medición afecte a la precisión de la medición de la IAS.

Por último, los autores informan sobre la carga necesaria para estimar la IAS. Las pruebas de velocidad basadas en TCP son las que crean la mayor carga, mientras que otras herramientas estiman la IAS en menos del 10% de la carga creada por las pruebas de velocidad basadas en TCP.

Asimismo, Kanuparth [2] utiliza mediciones basadas en UDP para medir la IAS. Observa que la presencia de conformadores en el enlace del estrechamiento disminuye la precisión de las estimaciones de IAS basadas en pruebas de velocidad TCP. En el mejor de los casos, dicha prueba informa de una velocidad entre la velocidad del enlace y la velocidad de conformación.

Flach et al. [4] proporcionan un algoritmo que determina la velocidad (y otras propiedades) de los reguladores utilizados para limitar el ancho de banda de acceso a Internet. La estimación de la IAS no se discute directamente. En promedio, los flujos TCP regulados experimentan una pérdida de paquetes seis veces mayor que los que no están regulados. Las estimaciones de la IAS obtenidas mediante las pruebas de velocidad basadas en TCP sin el algoritmo sugerido serán probablemente de escasa precisión.

Los autores añaden que, en el momento de la publicación, la regulación seguía desplegándose en cierta medida para los productos comerciales de acceso a Internet en Asia y África.

Una prueba basada en herramientas y mediciones para investigar si el UDP es una base viable como protocolo general de transporte de Internet muestra que, efectivamente, el UDP es un protocolo de transporte común viable [14]. Esta afirmación se basa en pruebas realizadas en América del Norte y del Sur, Europa, Asia y Oceanía (sobre todo en África). Los autores observaron que el tráfico UDP se bloquea en algunos puertos o de forma total en casos raros. En los casos en que falla el transporte UDP, se recomienda un repliegue al transporte TCP.

El bloqueo de UDP se produjo en entre el 2% y el 4% de las redes de acceso terrenal. El bloqueo de UDP estaba vinculado principalmente a una red de acceso. Los autores de [14] observaron que la degradación de UDP se concentra especialmente en las redes empresariales y en las redes situadas en regiones geográficas con una conectividad de otro tipo. En los casos en que UDP funcionaba en estas redes de acceso terrenal, no se encontraron pruebas de una degradación sistemática del tráfico con encabezamientos UDP.

Para que se produzca un repliegue a TCP, el nodo no necesita medir o recordar nada sobre sus pares, sino solo sobre su conectividad a Internet (esta recomendación dada por los autores de [14] indica también que las degradaciones de UDP se basan en enlaces de acceso específicos y no en redes).

XI.3.2 Medición de la velocidad de acceso a la LAN inalámbrica

Kanuparth [2] investigó anteriormente la calidad de funcionamiento del acceso WLAN IEEE 802.11. Da Hora, Van Doorselaer, Van Oost y Teixeira publicaron un modelo para estimar el impacto de una red Wi-Fi en la QoE del consumidor [10]. Los autores de este último modelo se basan en parámetros recogidos pasivamente de puntos de acceso Wi-Fi básicos. Una campaña de medición en redes de proveedores permite concluir que la mayoría de las redes Wi-Fi tienen una buena calidad de funcionamiento. Aún así, más del 10% de los puntos de acceso mostraron una MOS estimada < 3 durante al menos el 5% de todas las muestras recogidas (o más).

Se recogieron los siguientes parámetros Wi-Fi ([10], Cuadro II):

Cuadro X1.3.2-1 – Métricas Wi-Fi medidas en el punto de acceso (cuadro II de [10])

Métrica	Descripción	Periodo
BUSY	% de tiempo que el medio está ocupado	2s
WiFi	% de tiempo ocupado debido al tráfico Wi-Fi	2s
nonWiFi	% de tiempo ocupado debido al tráfico no Wi-Fi	2s
TxPhy	Velocidad PHY de la última trama enviada	1s
FDR	Tramas enviadas / retransmitidas a la estación	1s
RSSI	Indicador de intensidad de la señal recibida	1s

Las muestras tomadas por los autores contienen el promedio, la desviación típica, el mínimo, el máximo, el percentil 25 y el percentil 75 para cada métrica del Cuadro X1.3.2-1.

Las estadísticas de la muestra se evalúan durante un periodo T que depende de la aplicación:

- T = 10s para los experimentos de audio y vídeo.
- T = 10s para la navegación web.
- T = 120s para el flujo continuo de YouTube (cada vídeo se reprodujo durante dos minutos durante la prueba).

Los investigadores observaron que los siguientes subconjuntos de vectores de características de aplicaciones son los que mejor correlacionan la QoE de las aplicaciones de los consumidores con el subconjunto de características Wi-Fi ([10], Cuadro III):

- Vídeo: percentil 25 de TxPhy, percentil 25 de BUSY, valor máximo de BUSY, valor medio de RSSI, percentil 75 de RSSI, percentil 25 de WiFi.

- Audio: valor mínimo de TxPhy, desviación típica de RSSI, percentil 25 de WiFi, valor máximo de WiFi, valor máximo de nonWiFi, valor medio de FDR.
- YouTube: mediana de TxPhy, percentil 75 de BUSY, valor medio de RSSI, percentil 25 de RSSI, percentil 25 de WiFi, valor mínimo de nonWiFi.
- Web: valor máximo de TxPhy, desviación típica de BUSY, valor mínimo de RSSI, valor máximo de WiFi, valor máximo de nonWiFi, valor medio de FDR.

El enfoque adoptado en [10] se basa en el aprendizaje automático. Esta contribución no discute si los resultados de [10] son aplicables en general. Se da por supuesto que los parámetros de QoS mencionados están correlacionados con la QoS de la aplicación. El modelo completo y el enfoque de ajuste de parámetros por aplicación pueden encontrarse en el documento referenciado. Como nota final y norma general aquí citada, los autores de [10] esperan una QoE reducida cuando el valor medio de TxPhy es inferior a 15 Mbit/s.

XI.3.3 Medición de la QoE y la velocidad de acceso a la red móvil

Las publicaciones de Dimopoulos et al. [6] y Casas et al. ([7] y [8]) tratan sobre la medición de la QoE del flujo continuo de vídeo para terminales móviles, mientras que [7] investiga otras aplicaciones. En [7] se concluye que la QoE del abonado "para determinadas aplicaciones es muy sensible a las fluctuaciones del ancho de banda. Las fluctuaciones de la calidad de funcionamiento debidas a la variación del ancho de banda son muy comunes en las redes celulares, pero, lamentablemente, su efecto en la QoE no se refleja en las mediciones de red actuales, ya que normalmente solo se tienen en cuenta los valores de caudal promedio". Obsérvese que "las mediciones de red actuales" se refieren a las mediciones basadas en la inundación TCP.

Además, [6] muestra que la calidad de funcionamiento promedio de TCP no se correlaciona bien con la QoE del abonado, si hay variabilidad en el caudal.

Las publicaciones correlacionan la QoE del abonado con las mediciones de QoS de la red según los siguientes parámetros:

- [6] concluye que conviene utilizar el valor medio del producto-anchura de banda-retardo, las retransmisiones máximas de paquetes, el promedio de bits máximos en vuelo y la suma acumulativa del caudal mínimo.
- [6] propone además "reducir el ruido introducido por la fase de arranque en la detección de las variaciones de resolución" "eliminando los primeros 10 segundos de todas las sesiones de vídeo de su conjunto de datos". El caudal en esta fase de arranque parece desviarse del caudal y de sus fluctuaciones durante el resto del tiempo de la transmisión de vídeo (la duración media de la sesión fue de 180 segundos).
- [7] proporciona resultados de mediciones de laboratorio con fluctuaciones de caudal y [8] introduce dos métricas de QoS para reflejar esos parámetros: caudal de flujo de enlace descendente de sesión máxima y caudal de flujo de enlace descendente de sesión media. Estos se clasifican como los "parámetros más pertinentes".
- [8] evaluaron más indicadores fundamentales de rendimiento y su correlación con la predicción de MOS y su precisión. Además del caudal medio y máximo, se observó que los siguientes IFR afectan a la precisión de la predicción de la MOS: la intensidad media de la señal, el volumen y la duración de la sesión.
- Los IFR estudiados en [8] se basan en mediciones realizadas en una zona que ofrece un acceso óptimo a la red móvil. En [7] se muestran resultados de laboratorio, que indican que otros IFR como el RTT y las interrupciones de ancho de banda de corta duración (causadas por trasposos) pueden tener un efecto más o menos significativo en la QoE.
- [7] menciona además la neutralidad de la red como un tema pertinente. Una de las aplicaciones estudiadas tenía un ancho de banda limitado por uno de los proveedores de servicios de Internet participantes.

XI.3.4 Medición de la QoE de las aplicaciones cifradas

La evaluación de la QoE de las aplicaciones cifradas basadas en la red requiere una investigación más exhaustiva de los parámetros de QoS pertinentes en comparación con el uso compartido de la QoE de las aplicaciones no cifradas. Los parámetros propuestos también caracterizan las propiedades de acceso. [11], [12] y [13] sugieren parámetros para este fin. Su objetivo común es reconocer u optimizar los siguientes parámetros de QoE del flujo continuo de vídeo mediante la observación de los parámetros de QoS de la red:

- retardo en el arranque inicial (tiempo de arranque);
- velocidad binaria media de varios tramos (segmentos);
- cambios en la velocidad binaria media del tren (causados por la variación de los niveles de calidad de vídeo);
- tasa de realmacenamiento temporal.

El enfoque habitual consiste en medir el caudal de un tren de vídeo (y audio [12]). La duración recomendada de una muestra es la duración típica de un tramo o segmento del tren de vídeo (o audio, respectivamente). Esta se sitúa entre 2 y 15 segundos, con un valor de 4 segundos registrado para los trenes de vídeo de YouTube [13].

Se recomienda capturar en Mbit/s la velocidad del tren de datos de vídeo dirigido al terminal de reproducción mediante muestras de 1 segundo, que luego se evalúan mediante estadísticas relacionadas con la duración del tramo [11], [13]. La velocidad binaria media se calcula mediante muestras de media móvil simple de 5 segundos según [11]. [13] amplía esta idea para capturar datos de "lapsos" de 10 segundos consecutivos (lo que da lugar a 5 valores medios de por cada lapso, cada uno calculado a partir de cinco muestras de 1 segundo).

[13] propone los siguientes parámetros y estadísticas de QoS para correlacionar las propiedades de la capa de transporte (que pueden no ser detectables por la red) con los parámetros de la capa de red durante una fase de aprendizaje:

Cuadro XI.3.4-1 – Lista de características generales examinadas a partir de [13], Cuadro I

	Capa de red	Capa de transporte
Lapso de evaluación de 10 s	Cómputo de bytes Cómputo de paquetes Caudal Tiempo de inactividad	Cómputo de banderas TCP (SYN, ACK, FIN, URG, PSH y RST) Bytes/paquetes en orden incorrecto Caudal eficaz TCP ‡Tasa de retransmisión (tasa de 0, 1, 2 y >2) En el caso de la evaluación de la QoE en tiempo real: Bytes en vuelo iniciales Bytes en vuelo finales
Paquete Estadísticas: valor medio, valor mínimo, valor máximo, mediana, desviación típica, asimetría, curtosis.	Intervalos de tiempo entre llegadas de paquetes Bytes por paquete	Retransmisiones por paquete Lapso de recepción de transporte RTT (solo para el tráfico ascendente) Bytes en vuelo

Se pueden encontrar definiciones e instrucciones de medición más detalladas en [13].

Para correlacionar las mediciones de red y de transporte, se propone un aprendizaje en laboratorio en condiciones de red controladas.

[13] caracteriza la fase de arranque solo por las estadísticas recopiladas durante la primer lapso de evaluación de 10 segundos.

Para caracterizar los eventos de retransmisión y realmacenamiento temporal, [13] evalúa y compara las propiedades de los primeros cinco segundos de cada lapso con las propiedades de los segundos cinco segundos de cada lapso de evaluación.

[13] observa que los siguientes parámetros de red se correlacionan con la QoE de YouTube:

- retardo inicial del arranque (mediana de los bytes descargados, intervalos medios de tiempo entre de llegadas de paquetes, mediana del caudal descendente – estadísticas de los paquetes comparadas después de 3,3, 6,6 y 10 segundos);
- eventos de realmacenamiento temporal (bytes mínimos descargados en la primera mitad del lapso de evaluación, caudal descendente en la primera mitad del lapso de evaluación);
- calidad de vídeo (caudal descendente, caudal ascendente).

[13] añade un enfoque de aprendizaje automático para desarrollar y parametrizar un modelo de QoE. Esta contribución solo extrae las medidas de QoS que se correlacionan con la QoE de la aplicación. Los lectores interesados pueden encontrar el modelo completo en [13].

XI.4 Tendencias generales relacionadas con la calidad de funcionamiento del acceso a Internet

Dos informes proporcionan también declaraciones generales respecto de las necesidades del mercado.

Flach et al. [5] afirman que, en un entorno en el que "el ancho de banda sigue siendo relativamente barato, la latencia de la web es ahora el principal impedimento para mejorar la calidad de funcionamiento percibida por el usuario". Esta afirmación se refiere al acceso a la red fija, pero se indica que una de las razones de esta tendencia es la comodidad de los teléfonos inteligentes como dispositivos finales. Hay que tener en cuenta que algunos de los autores trabajan con un importante OTT.

Los autores de [9] midieron la QoE según la Recomendación UIT-T P.1203 con una pantalla de 1920×1080 píxeles utilizando el contenido recibido de un importante OTT a través de un acceso DSL de red fija comercial. Se insertó un conformador entre el dispositivo de medición y el encaminador DSL y se alteró el ancho de banda descendente en 11 pasos entre 0,256 y 37,5 Mbit/s. Se obtuvieron valores MOS de 4 y superiores para anchos de banda descendentes de 3,073 Mbit/s.

Los autores de [7], un documento relacionado con las redes móviles, concluyen "que un ancho de banda de enlace descendente de 4 Mbps es lo suficientemente alto como para alcanzar resultados casi óptimos en términos de calidad general y aceptabilidad para [el flujo continuo de vídeo] cuando se accede a ella mediante teléfonos inteligentes. Las implicaciones para el usuario final son evidentes: ...En la actualidad no se necesita un costoso contrato LTE para conseguir una experiencia casi óptima". Obsérvese que el documento se publicó en 2016 y que los autores utilizaron vídeos HD720p para obtener sus resultados.

Las tres afirmaciones indican que, si el ancho de banda de acceso a Internet es suficientemente alto, la satisfacción de los abonados y los proveedores de contenidos con la calidad de funcionamiento de un acceso a Internet puede ser independiente de la velocidad máxima de acceso a Internet.

Referencias para el Apéndice XI

- [1] "Speed Measurements of Residential Internet Access", Oana Goga y Renata Teixeira, PAM 2012, 2012.
- [2] "End-to-end Inference of Internet Performance Problems", Partha Kanuparth, tesis doctoral, Georgia Institute of Technology, 2012.

- [3] "Diagnosing Path Inflation of Mobile Client Traffic", Kyriakos Zarifis, Tobias Flach, Srikanth Nori, David Choffnes, Ramesh Govindan, Ethan Katz-Bassett, Z. Morley Mao, y Matt Welsh, 2014.
- [4] "An Internet-Wide Analysis of Traffic Policing", Tobias Flach, Pavlos Papageorgey, Andreas Terzis, Luis D. Pedrosa, Yuchung Chengy, Tayeb Karimy, Ethan Katz-Bassett, y Ramesh Govindan, IEEE SIGCOMM, 2016.
- [5] "Reducing Web Latency: the Virtue of Gentle Aggression" Tobias Flach, Nandita Dukkupati, Andreas Terzis, Barath Raghavan, Neal Cardwell, Yuchung Cheng, Ankur Jain, Shuai Hao, Ethan Katz-Bassett, y Ramesh Govindan, IEEE SIGCOMM 2013.
- [6] "Measuring Video QoE from Encrypted Traffic", Giorgos Dimopoulos, Ilias Leontiadis, Pere Barlet-Ros, y Konstantina Papagiannaki, IMC '16, 2016.
- [7] "Next to You: Monitoring Quality of Experience in Cellular Networks from the End-devices", Pedro Casas, Michael Seufert, Florian Wamser, Bruno Gardlo, Andreas Sackl, y Raimund Schatz, IEEE Transactions on Network and Service Management, Vol 13, número 2, 2016.
- [8] "Predicting QoE in Cellular Networks using Machine Learning and in-Smartphone Measurements", Pedro Casas, Alessandro D'Alconzo, Florian Wamser, Michael Seufert, Bruno Gardlo, Anika Schwind, Phuoc Tran-Gia, Raimund Schatz, QoMEX 2017.
- [9] "Measuring YouTube QoE with ITU-T P.1203 under Constrained Bandwidth Conditions", Werner Robitza, Dhananjaya G. Kittur, Alexander M. Dethof, Steve Göring, Bernhard Feiten, Alexander Raake, QoMEX 2018.
- [10] "Predicting the effect of home Wi-Fi quality on QoE: Extended Technical Report." Diego Da Hora, Karel Van Doorselaer, Koen Van Oost, Renata Teixeira. [Research Report] INRIA; Technicolor; TelecomParisTech. 2018. <hal-01676921>
- [11] "QoE-based low-delay live streaming using throughput predictions." Konstantin Miller, Abdel-Karim Al-Tamimi, y Adam Wolisz. 2016. ACM Trans. Multimedia Comput. Commun. Appl. 13, 1, artículo 4 (octubre de 2016), 24 páginas. DOI: <http://dx.doi.org/10.1145/2990505>.
- [12] "eMIMIC: Estimating HTTP-based Video QoE Metrics from Encrypted Network Traffic", Tarun Mangla, Emir Halepovicy, Mostafa Ammar, Ellen Zegura. Georgia Institute of Technology yAT&T Labs – Research.
- [13] "Real-time Video Quality of Experience Monitoring for HTTPS and QUIC", M. Hammad Mazhar, Zubair Shafiq, The University of Iowa.
- [14] "copycat: Testing Differential Treatment of New Transport Protocols in the Wild", Korian Edeline, Mirja Kühlewind, Brian Trammell, Benoit Donnet, ANRW '17, Praga.

Apéndice XII

Mediciones exactas de la velocidad binaria

(Este apéndice no forma parte integrante de la presente Recomendación.)

XII.1 Introducción

Cada medidor de tráfico a lo largo de un trayecto de comunicación está configurado para obtener o imponer una velocidad binaria en una sola capa de comunicación (o lo hace por defecto). El conocimiento de la capa de comunicación a la que se impone una velocidad binaria de estrechamiento reduce el error de medición.

Los dispositivos intermedios a lo largo de un trayecto de medición de laboratorio o de red pueden estar configurados para condicionar el tráfico, y a falta de ellos una interfaz física puede imponer una velocidad binaria. Un sistema de medición de la velocidad binaria podría indicar una velocidad superior o inferior a la velocidad binaria que impone el estrechamiento, si ambos no miden la velocidad binaria en la misma capa de comunicación.

Las pruebas de referencia y la calibración requieren especialmente un conocimiento preciso de las capas en las que se mide el tráfico mediante estos acondicionadores de tráfico o interfaces físicas. La transferencia de los resultados de las mediciones de ancho de banda de una capa a otra requiere conocer los tamaños de los encabezamientos de los paquetes de medición en las diferentes capas. La presentación precisa y comprensible de los resultados de las mediciones requiere indicar la capa en la que se aplica una velocidad binaria y la información que la acompaña, como el tamaño de PDU del paquete en esa capa.

Conviene tener en cuenta que los errores causados por no conocer los encabezamientos de los paquetes y la capa en la que se aplica la velocidad binaria son una fuente de error en la medición de la velocidad binaria, pero no la única. Las mediciones que utilizan la realimentación de la congestión de bucle cerrado basada en el descarte de paquetes, como TCP o QUIC, introducen fuentes adicionales de error, que dependen del retardo de ida y vuelta y de la pérdida de paquetes.

En este apéndice también se incluye información sobre los filtros de colectores de testigos, que son un componente clave de los conformadores y reguladores de tráfico.

XII.2 Principales conclusiones

La calidad de funcionamiento de las interfaces y los protocolos se presenta de forma comprensible mediante una velocidad o un ancho de banda en Mbit/s. Con fines generales, como las encuestas, el conocimiento aproximado de un ancho de banda caracteriza suficientemente el resultado de una medición. Esto cambia si las mediciones de ancho de banda tienen como objetivo calibrar o comparar la calidad de funcionamiento de un dispositivo o de un trayecto de comunicación sometido a prueba. Para poder comparar los resultados de las mediciones de ancho de banda recogidos por diferentes métodos o recogidos a lo largo de trayectos de medición con múltiples puntos de condicionamiento del tráfico, los resultados solo serán precisos si se basan en información adicional. El error introducido por un sistema de medición y una aplicación de la velocidad binaria en diferentes capas es parte de esa información adicional (pero no necesariamente la única).

Considérese una configuración simple de medición de ancho de banda como la que se muestra en la Figura XII.2-1.

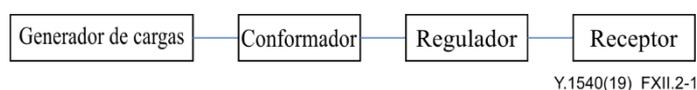


Figura XII.2-1 – Una configuración sencilla de la medición del ancho de banda

Téngase en cuenta que no se afirma que la configuración mostrada sea típica. Algunas partes de ella pueden estar presentes en muchas redes.

El objetivo de la prueba puede ser determinar el máximo ancho de banda de la configuración de prueba sin pérdidas. El umbral con el que se comparan los resultados de las mediciones es el ancho de banda con el que están configuradas las velocidades del conformador y del regulador (supongamos que ambos están configurados a la misma velocidad C_{Acceso}).

Una medición puede revelar un ancho de banda sin pérdidas máximo de $0,95 * C_{\text{Acceso}}$. Sin embargo, si el objetivo de la prueba es calibrar o evaluar la calidad de funcionamiento del conformador y del regulador, este resultado por sí solo no será significativo (ni siquiera si se recoge en un laboratorio en condiciones controladas).

Supongamos que el generador de carga y el receptor son el mismo dispositivo. Por defecto, este dispositivo genera y cuantifica los tamaños de los paquetes y las velocidades binarias resultantes como C_{Acceso} en la capa 2. Si el conformador y el regulador están configurados para cuantificar y programar o restringir el ancho de banda en la capa 1, pueden reenviar con precisión el tráfico con el ancho de banda C_{Acceso} , si C_{Acceso} se mide en la capa 1. Todos los dispositivos funcionan correctamente según su diseño y configuración. La aparente inexactitud del 5% de desviación del resultado esperado se debe a la capa en la que los dispositivos utilizados en la configuración de la prueba miden el tráfico.

Ahora considérese que las personas encargadas de la prueba introducen un pequeño cambio, como la disminución del tamaño de los paquetes de medición en un 50%. La medición del ancho de banda resultante puede ser ahora de $0,93 * C_{\text{Acceso}}$. Supongamos que el estrechamiento no está causado por la calidad de funcionamiento limitada (en paquetes por segundo) de ningún procesador a lo largo de la configuración de la prueba. Entonces este resultado indicará una incompatibilidad de capa o de medición, respectivamente, a lo largo del trayecto probado. Los paquetes más pequeños darán lugar a una menor velocidad binaria en la capa 2, mientras que la velocidad binarias de la capa 1 permanecerá constante. La cadena de producción funciona correctamente tal y como está configurada.

Si se desconoce el ancho de banda del flujo de prueba en el dispositivo de acondicionamiento o no se puede controlar configurando el emisor, o si se desconoce la capa en la que el dispositivo de acondicionamiento limita el tráfico, la calibración o evaluación comparativa de dicho dispositivo solo es posible con una precisión limitada.

XII.3 Estimación del error de medición del ancho de banda provocado por la longitud del encabezamiento

El tráfico se limita a una velocidad binaria constante solo en la capa de comunicación en la que funciona el conformador acondicionador. El regulador o la interfaz física funciona. No se debería esperar que los conformadores y reguladores funcionen en una capa concreta y bien especificada. En algunos casos, los dispositivos de los proveedores de red permiten configurar la capa en la que funcionan los medidores de velocidad de los conformadores y reguladores.

Para comparar con precisión las mediciones de ancho de banda con fines de calibración y evaluación comparativa, se requiere la siguiente información:

- la capa de comunicación y el tamaño de PDU del emisor y el receptor;
- todos los tamaños de encabezamientos añadidos o eliminados, si el emisor y el receptor no miden el tráfico en la misma capa;
- la capa de los parámetros de configuración de los dispositivos de acondicionamiento del tráfico que se van a calibrar o comparar. Si el estrechamiento es una interfaz física, generalmente se conocerá el ancho de banda de la interfaz de la capa 1;
- los tamaños exactos de los encabezamientos insertados o eliminados, si el emisor, el receptor y los dispositivos de acondicionamiento del tráfico no miden el ancho de banda exactamente en la misma capa con tamaños de PDU idénticos;

- la capa de un umbral con la que se compara un resultado de medición y todos los tamaños de encabezamiento que se añaden o eliminan, si la capa del umbral no es idéntica a las capas del emisor o del receptor.

Se producen deficiencias en las mediciones si la velocidad binaria del umbral con que se comparan los resultados de las mediciones de ancho de banda de un emisor y un receptor no se encuentran en la misma capa de comunicación. Además, cuanto mayor sea el número de nodos activos, la regulación y los puntos de interfuncionamiento a lo largo de un trayecto de producción, más probable será la presencia de encabezamientos adicionales que pueden estar ausentes en el dispositivo emisor y receptor, por ejemplo, encabezamientos de túnel entre la capa 2 y la capa 3 o entre la capa 3 y la capa 4.

Si se van a utilizar encabezamientos Ethernet en los cálculos, se debería conocer la presencia y el número de etiquetas VLAN.

En algunos casos, la capa 1 requiere secuencias de escape para una trama correcta. La presencia de una secuencia de código de escape puede depender de los patrones de bits de cabida útil. En ese caso, la precisión de la medición es limitada.

En general, una velocidad binaria C_x está limitada a un ancho de banda (físico o) configurado en una capa x . En esta capa x , y solo en esta capa x , se cumple la siguiente ecuación para la velocidad binaria C_x que debe medirse en la capa x (generalizada a partir de UIT-T Y.1540):

$$C_x(t, \Delta t) = N_x(t + \Delta t) / \Delta t \quad (1)$$

siendo N_x el número total de bits de la capa x que pueden transferirse a través de una sección básica generando un resultado de transferencia satisfactoria de paquetes de la capa x en el punto de medición de egreso durante un intervalo de tiempo especificado $[t, t + \Delta t]$. En una capa de comunicación y que transporta paquetes de la capa x , es necesario añadir un encabezamiento de paquete de longitud constante h_y bits por cada paquete de la capa x . Si el único ancho de banda conocido o medido es el de la capa x , solo puede determinarse el ancho de banda de la capa y consumido por el tren de paquetes medido si se conoce el número de paquetes p_x de la capa x y el tamaño del encabezamiento h de la capa y :

$$C_y(t, \Delta t) = [N_x(t + \Delta t) + p_x * h_y] / \Delta t = C_x(t, \Delta t) + p_x * h_y / \Delta t \quad (2)$$

Hay dos cambios que influyen de forma evidente en el error de medición:

- Como era de esperar, el ancho de banda C_y de la capa y es mayor que el ancho de banda C_x de la capa x .
- C_y depende del número de paquetes p_x de la capa x , mientras que C_x es independiente del número de paquetes p_x de la capa x .

El número de paquetes p_x y el tamaño medio de los paquetes s_x están relacionados por la ecuación (3):

$$s_x = C_x(t, \Delta t) / p_x \quad (3)$$

El tamaño de paquete s_x de la capa x influye en la velocidad binaria resultante C_y medida en la capa y .

Las normas, las especificaciones públicas y la información sobre los productos pueden permitir determinar los tamaños de encabezamiento y de paquetes máximos en las diferentes capas de comunicación para algunos mercados. La capa en la que un dispositivo de red o proveedor de servicios aplica una velocidad configurada debe considerarse desconocida.

La mayor mejora de la exactitud de una medición del ancho de banda se consigue si se tiene en cuenta la información detallada sobre el tamaño de los paquetes de medición y la información del formato de encabezamiento del estrechamiento especificado en el mayor número posible de capas diferentes.

A falta de información detallada, una suposición conservadora es el tamaño mínimo de tara compatible con la configuración de medición utilizada o con la información general sobre un acceso,

si no se dispone de una especificación de formato de encabezamiento de capa respecto dicho acceso. Esto todavía permite reducir el error de medición resultante.

Los tamaños medios de los paquetes de medición recibidos o el número de paquetes de medición recibidos deben conocerse para reducir el error de medición.

Si no se conocen con exactitud los encabezamientos de capa y el tamaño o número medio de paquetes de medición recibidos, pero se pueden determinar los valores máximos y mínimos, cabe determinar un corredor de resultados de medición corregido.

Las fórmulas (1), (2) y (3) permiten calcular los anchos de banda en las diferentes capas de comunicación, si se conocen los encabezamientos de la capa de comunicación y el tamaño o el número medio de paquetes de medición recibidos o los valores máximos y mínimos de estos últimos (además del resultado de la medición del ancho de banda).

XII.4 Ejemplo de cálculo de tara para una interfaz Ethernet IEEE 802.3 alámbrica

Téngase en cuenta que todos los cálculos que se muestran a continuación solo son válidos para un estrechamiento que transmita paquetes a través de un enlace físico conforme a Ethernet según las especificaciones de la serie de normas IEEE 802.3.

En este proyecto de la CE 12 se realizaron pruebas de medición de ancho de banda de acceso en laboratorio (véase el Apéndice X). La herramienta de medición "iPerf 2" informa de las mediciones de velocidad basadas en los bytes de cabida útil de transporte entregados (por encima de la capa UDP o TCP). La tasa del filtro del colector de testigos [de un conformador configurado para actuar como estrechamiento] se especifica en "bits en el cable", por lo que los encabezamientos añadidos a las cabidas útiles de transporte se incluyen en los cálculos del filtro del colector de testigos (la velocidad incluye bits de ETH, IP y encabezamiento de transporte).

Es sabido que la cabida útil UDP de una primera medición es de 1 470 bytes. La conexión Ethernet es nativa (sin encabezamientos VLAN).

Cálculos de encabezamiento de la capa inferior:

- Encabezamiento UDP: 8 bytes;
- Encabezamiento IPv4: 20 bytes;
- Ethernet.

Encabezamiento

14 bytes (capa 2 sin comprobación de redundancia cíclica, CRC);
18 bytes (capa 2 con comprobación de redundancia cíclica, CRC);
26 bytes (capa 1).

El 97,2% de la velocidad configurada se recibió sin pérdida de paquetes en varias velocidades de estrechamiento configuradas. Al principio se dio por supuesto que el tamaño de la trama de la capa 2 de Ethernet incluía los bytes CRC. Con un encabezamiento de 46 bytes por paquete, se obtuvo un factor de corrección de 1,0313. Se calculó que el ancho de banda del conformador "bits en el cable" era 1,00242 veces la velocidad configurada. El error es del 0,24%, lo que representa un valor bajo.

Una investigación más detallada revela que la tasa de conformación excluye los bytes CRC. La corrección de encabezamiento basada en un tamaño de encabezamiento de 42 bytes es entonces de 1,0286. Se calculó que el ancho de banda del conformador "bits en el cable" era 0,999799 veces la velocidad configurada. El error es del -0,02%, que es otro orden inferior. Un error de medición de 2 ppm indica que la configuración del conformador de laboratorio funcionó con bastante exactitud en la capa 2 de Ethernet (sin bytes CRC).

Obsérvese que también el equipo del proveedor de red puede medir el tráfico Ethernet en la capa 2 sin CRC. Como todavía no hay una capa de medición de la velocidad binaria de Ethernet por defecto,

el hardware del proveedor de red puede medir Ethernet en la capa 1 o en la capa 2 incluyendo también los bytes CRC.

XII.5 Descripción de la funcionalidad del filtro del colector de testigos

Los conformadores y los reguladores limitan las velocidades de tráfico. El control de velocidad subyacente suele basarse en un filtro del colector de testigos. Un filtro del colector de testigos funciona genéricamente del siguiente modo:

- Se configura una *Rate* (velocidad) en [bits/s].
- Se configura una *Burst-Tolerance_Byte* (tolerancia a las ráfagas) en [bytes].

Opcionalmente, los sistemas suelen ofrecer la configuración de *Burst-Tolerance_ms* en [ms]. Se espera que el sistema asigne internamente la siguiente memoria intermedia:

$$Burst-Tolerance_Byte [byte] = Rate / 8 / Burst-Tolerance_ms * 1000 \quad (4)$$

Un regulador de colector de testigos añadirá un testigo de un bit al colector cada $1/Rate$ segundos. Si el colector se llena con testigos de *Burst-Tolerance_Byte*, se descartan los colectores adicionales.

Cuando llega un paquete de bytes de *Packet-Length* (longitud de paquete), el filtro comprueba si los testigos correspondientes a la *Packet-Length* están presentes en el colector.

- En caso afirmativo, el paquete se reenvía y los bytes *Packet-Length* se eliminan del colector.
- En caso negativo, el paquete se descarta y el colector permanece sin cambios (a menos que haya una memoria intermedia adicional del conformador; véase la nota más abajo).

Un conformador del colector de testigos funciona como un regulador, pero maneja una memoria intermedia adicional de *Buffer_bytes*. Si el regulador descarta el paquete, este se almacena en la memoria intermedia, siempre que esta no se desborde. Una vez que un número suficiente de testigos está presente en el filtro del colector de testigos, se reenvía el primer paquete almacenado en la memoria intermedia (dado que se aplica la programación de primero en entrar, primero en salir (*first-in-first-out*)).

Si la memoria intermedia del conformador se agota por los paquetes que llegan, se descarta cualquier paquete adicional.

Obsérvese que los conformadores tienen una memoria intermedia adicional que puede ser configurable en *Buffer_ms* [ms] o en un número de *Packets*, y normalmente se da por supuesto un tamaño medio de paquete cuando el sistema asigna bytes a la memoria intermedia de paquetes. De nuevo, la *Rate* configurada se utiliza para calcular la profundidad de la memoria intermedia interna del sistema (*Buffer_bytes*) como se muestra en (1).

Apéndice XIII

Parámetros relacionados con el flujo basados en IP y métodos de medición

(Este apéndice no forma parte integrante de la presente Recomendación.)

XIII.1 Antecedentes

El IETF aprobó y publicó el documento RFC 8337, "Model-Based Metrics for Bulk Transport Capacity", en marzo de 2018 [IETF RFC 8337]. El trabajo de métricas basadas en modelos (MBM) fue el resultado de muchos años de análisis del problema de la medición de la capacidad de transporte, principalmente en el Grupo de Trabajo sobre Métrica de la calidad de funcionamiento IP (IP Performance Metrics, IPPM) del IETF. En la especificación se describen minuciosamente los numerosos problemas y dificultades de repetibilidad cuando se realizan pruebas con TCP conforme a la norma (sección 4), y se resuelven estos problemas principalmente mediante el diseño de un método y un conjunto de pruebas de diagnóstico en las que se desactiva un control de flujo de TCP. El método conlleva la evaluación de la calidad de funcionamiento de un transporte objetivo en términos de velocidad de transmisión y tiempo de ida y vuelta (RTT).

La evaluación de MBM comenzó antes de que se publicara la RFC. En el artículo "Improved Internet speed tests can enhance QoS and QoE", Morton examinó diversos métodos de medición para evaluar el marco del modelo MBM en el contexto de la identificación de los numerosos problemas de precisión de las técnicas de medición de Internet existentes y el inicio de los trabajos para resolverlos [MortonPQS].

XIII.2 Por qué la MBM cumple los requisitos de esta Recomendación

En la cláusula 6.12 se establece un conjunto de requisitos que debe cumplir cualquier método de medición relacionado con el flujo, como participante razonable en el contexto de los recursos compartidos de Internet. La MBM cumple estos requisitos, como se describe a continuación (véanse los términos y definiciones en la sección 3 [IETF RFC 8337]).

Todos los parámetros relacionados con el flujo o el caudal deberían cumplir los siguientes requisitos numerados:

- 1) Un parámetro que caracterice el caudal ofrecido a un servicio IP deberá poner en relación la cantidad de paquetes IP transportados de manera satisfactoria por una red o sección IP con la cantidad de parámetros IP que fueron entregados en esa red o sección.

El número de paquetes enviados ("entregados en esta red o sección") está completamente controlado por la selección del flujo de prueba. Además, el "transporte satisfactorio" de paquetes IP se mide directamente en el método MBM (para obtener la tasa de pérdidas y medir la longitud de gama de repeticiones).

- 2) Los parámetros relacionados con el caudal deberán aplicarse a una red IP de extremo a extremo y al transporte IP a través de un EL, una NS o un NSE.

Las métricas y mediciones MBM están diseñadas para ser independientes del punto de ventaja y, por lo tanto, aplicables a los trayectos de prueba EL, NS o NSE (al igual que el cumplimiento de otros requisitos clave, véase la sección 4.3 de [IETF RFC 8337]).

A continuación se enumeran otros requisitos de esta Recomendación, con un análisis del cumplimiento de la MBM:

Algunos parámetros relacionados con el flujo o el caudal tratan de caracterizar la capacidad de caudal de una red IP, es decir, las posibilidades que tiene la red de mantener una determinada tasa de transferencia de paquetes IP. Se recomienda que cualesquiera de esos parámetros cumplan los siguientes requisitos adicionales:

- 1) Deberá describir el esquema del tráfico ofrecido a la red o sección IP, ya que la capacidad de la red o sección IP de entregar de manera satisfactoria esos paquetes depende de dicho esquema de tráfico.

El patrón de tráfico ("ofrecido a la red IP o sección") se controla constantemente mediante la selección del tren de prueba (conforme a los parámetros de prueba especificados).

- 2) La tasa a la que se ofrece el tráfico no deberá ser superior a la capacidad (en bits por segundo) del enlace que conecta las secciones sometidas a prueba con las secciones de destino no sometidas a prueba.

El patrón de tráfico ofrecido se selecciona y controla bajo las restricciones del tren de prueba y el parámetro del modelo MBM (*target_rate*).

- 3) En cualquier afirmación individual sobre la calidad de funcionamiento del caudal debería declararse el tipo de paquete IP examinado.

El marco de la calidad de funcionamiento IP del IETF (IPPM) [b-IETF RFC 2330] (que orienta todo el desarrollo de métricas y las mediciones realizadas según sus especificaciones) establece requisitos claros para especificar los detalles de los paquetes; véase la sección 13, Paquetes de tipo P. Téngase en cuenta que esta sección se está actualizando para incluir los requisitos de IPv6 y otros desarrollos recientes.

Obsérvese que en el Apéndice IX se explica por qué las mediciones que utilizan TCP conforme a la norma no cumplen los requisitos de la cláusula 6.12.

XIII.3 Función y situación del método de medición MBM

La función del método MBM es determinar si un trayecto o subtrayecto tiene suficiente calidad de funcionamiento para soportar una velocidad objetivo de transferencia de flujo de bytes fiable de una conexión de capa de transporte simple. Este método resulta útil cuando se evalúa si un trayecto o subtrayecto presenta la velocidad de transporte requerida por una determinada aplicación, como por ejemplo el subtrayecto entre un servidor de entrega de contenidos y el encabezamiento de un enlace de acceso. Por otro lado, la evaluación de la capacidad IP a velocidades Gigabit no es la función de los métodos MBM.

En las restantes secciones de este apéndice se describen los temas que quedan en estudio en este momento. Es necesario realizar más evaluaciones de laboratorio y de campo.

XIII.4 Selección del tren de pruebas

En la sección 6 de [IETF RFC 8337] se sugieren diferentes diseños de trenes de prueba que pueden seleccionarse como parte de una serie de diagnóstico IP dirigido (TIDS, *targeted IP diagnostic suite*).

En la sección 6.1 se describe el diseño del tren para **imitar el arranque lento de TCP** (que se produce al principio de cada conexión TCP). Los parámetros clave del tren son (téngase en cuenta que los valores objetivo vienen determinados por el abono al servicio y el trayecto objeto de la prueba):

- tamaño de la ráfaga en paquetes (4, pero también se pueden utilizar tamaños menores);
- *target_window_size* (tamaño del lapso objetivo);
- *target_RTT* (RTT objetivo);
- *target_data_rate* (velocidad de datos objetivo).

En [IETF RFC 8337] se afirma lo siguiente: "...en plazos más largos que el *target_RTT* y cuando el tamaño de la ráfaga es igual al *target_window_size*, la velocidad media es igual a la *target_data_rate*".

En la sección 6.2 se describe el diseño del **tren de velocidad binaria pseudoconstante (CBR) de lapso constante**, junto con el problema de que un lapso de tamaños de paquetes enteros combinada con un RTT fijo puede hacer que la velocidad de datos entregada represente exactamente la

target_data_rate (operando ligeramente por encima o por debajo de la *target_data_rate*), por ejemplo, cuando el RTT o la *target_data_rate* son pequeños.

Una vez más, los cuatro parámetros clave del tren son los que se enumeran para que el tren imite el arranque lento de TCP.

La variación de la *target_data_rate* también puede producirse cuando varía el RTT, debido al uso de la autotemporización en este tren (las llegadas de TCP ACK determinan la velocidad de envío, y dependen del RTT). El tráfico inesperado en competencia puede causar la variación del RTT (aumento y disminución).

Como se sugiere en [IETF RFC 8337], "el tráfico de medición de ritmo convencional puede ser más apropiado para estos entornos" en los que la *target_data_rate* no se puede igualar o el RTT/autotemporización presenta problemas. El **tráfico pseudo-CBR** puede seguir conteniendo ráfagas, pero se envía a la *target_data_rate* durante toda la prueba.

Los trenes de tráfico pseudo-CBR indicados anteriormente se utilizan en evaluaciones básicas de la velocidad de los datos, sustentando la prueba de la sección 8.1.2 de [IETF RFC 8337], por ejemplo.

Obsérvese que la sección 6.3, en la que se describe la generación de flujos pseudo-CBR con exploración de lapsos, acrecienta la complejidad para lograr un mayor realismo en la respuesta a las condiciones de la red, y queda en estudio en este momento.

XIII.5 Puntos de medición

En [b-IETF RFC 7398] se define una ruta de referencia y puntos de medición para las métricas de calidad de funcionamiento más utilizadas. Otros proyectos de medición similares también pueden utilizar las extensiones aquí descritas para la localización de puntos de medición. La finalidad de [b-IETF RFC 7398] es crear una forma eficiente de describir la ubicación del punto o puntos de medición utilizados para realizar una determinada medición, especialmente señalando en qué momento una medición incluye subtrayectos gestionados y no gestionados (red privada).

Téngase en cuenta que el trayecto de medición, delimitado por los puntos de medición [b-IETF RFC 7398], determina la aplicabilidad de los parámetros del abono, como las velocidades de datos típicas ofrecidas y si los parámetros de abono informan de la selección de los parámetros MBM, como la *target_data_rate*.

En la figura siguiente se indican dos ámbitos de medición no superpuestos: el ámbito de acceso y el ámbito de distribución.

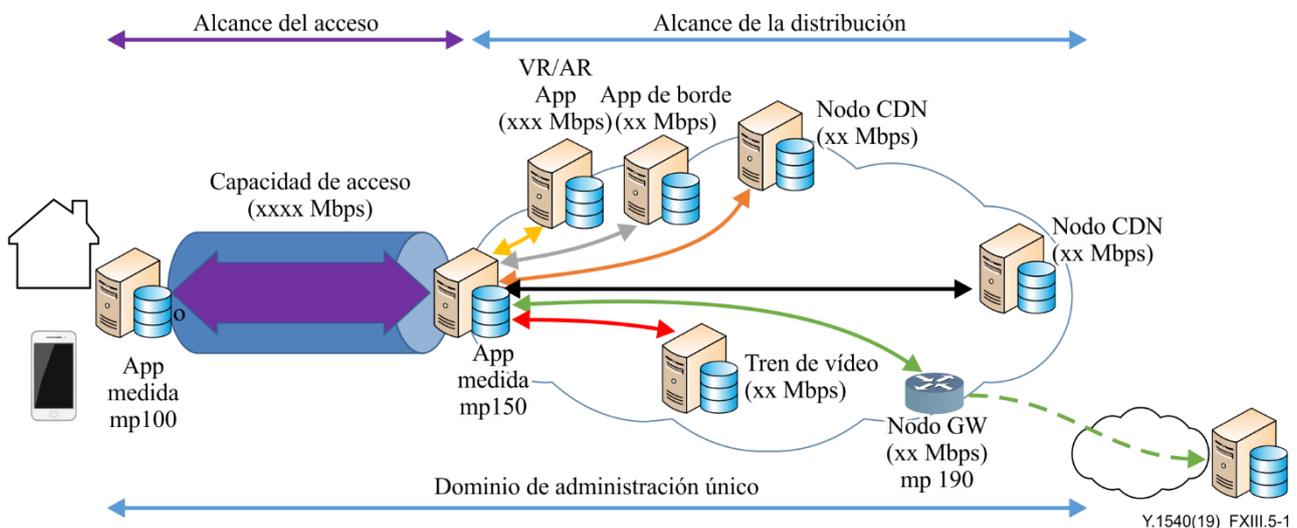


Figura XIII.5-1 – Mediciones separadas de acceso y distribución

En [b-IETF RFC 7398], el ámbito de acceso existe entre mp100 y mp150, y este es el ámbito previsto para la métrica de capacidad IP basada en UDP y los métodos del Anexo A.

Por otro lado, el ámbito de distribución está comprendido entre [b-IETF RFC 7398] mp150 y mp190, y esta es la aplicación prevista de los métodos de evaluación de *target_data_rate* basados en MBM (entre anfitriones en los extremos o dentro del ámbito de distribución) cuando se perfeccionen más.

XIII.6 Especificación de los parámetros del modelo objetivo

Véanse las secciones 5.1 y 5.2 de [IETF RFC 8337].

XIII.7 Establecimiento de criterios de aceptación e interpretación de los resultados

Véanse las secciones 7.1 y 7.2 de [IETF RFC 8337].

XIII.8 Métodos de prueba

[b-IETF RFC 6673] y [MortonPQS] señalan el uso de muchas pruebas repetidas. Una sola prueba no constituye una evaluación precisa de ningún servicio de abono que ha de estar disponible bajo demanda, pero puede ser suficiente con fines de verificación simple cuando los resultados confirman las expectativas.

XIII.9 Ejemplo(s)

Véase la sección 9 de [IETF RFC 8337].

Bibliografía

- [b-UIT-T I.353] Recomendación UIT-T I.353 (1996), *Eventos de referencia para definir los parámetros de calidad de funcionamiento de la red digital de servicios integrados (RDSI) y de la red digital de servicios integrados de banda ancha (RDSI-BA)*.
- [b-UIT-T I.356] Recomendación UIT-T I.356 (2000), *Calidad de funcionamiento en la transferencia de células en la capa de modo de transferencia asíncrono de la RDSI-BA*.
- [UIT-T P.800] Recomendación UIT-T P.800 (1996), *Métodos de determinación subjetiva de la calidad de transmisión.*
- [b-UIT-T X.25] Recomendación UIT-T X.25 (1996), *Interfaz entre el equipo terminal de datos y el equipo de terminación del circuito de datos para equipos terminales que funcionan en el modo paquete y están conectados a redes públicas de datos por circuitos especializados*.
- [b-UIT-T X.75] Recomendación UIT-T X.75 (1996), *Sistema de señalización con conmutación de paquetes entre redes públicas que proporcionan servicios de transmisión de datos*.
- [b-UIT-T X.137] Recomendación UIT-T X.137 (1997), *Valores de disponibilidad para redes públicas de datos que prestan servicios internacionales de conmutación de paquetes*.
- [b-UIT-T Y.1221] Recomendación UIT-T Y.1221 (2002), *Control de tráfico y control de congestión en las redes basadas en el protocolo Internet*.
- [b-IETF RFC 768] IETF RFC 768 (1980), *User Datagram Protocol*.
<<http://www.ietf.org/rfc/rfc768.txt>>
- [b-IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.
<<http://www.ietf.org/rfc/rfc792.txt>>
- [b-IETF RFC 793] IETF RFC 793 (1981), *Transmission Control Protocol*.
<<http://www.ietf.org/rfc/rfc793.txt>>
- [b-IETF RFC 919] IETF RFC 919 (1984), *Broadcasting Internet Datagrams*.
<<http://www.ietf.org/rfc/rfc919.txt>>
- [b-IETF RFC 922] IETF RFC 922 (1984), *Broadcasting Internet datagrams in the presence of subnets*.
<<http://www.ietf.org/rfc/rfc922.txt>>
- [b-IETF RFC 950] IETF RFC 950 (1985), *Internet Standard Subnetting Procedure*.
<<http://www.ietf.org/rfc/rfc950.txt>>
- [b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol*.
<<http://www.ietf.org/rfc/rfc959.txt>>
- [b-IETF RFC 1305] IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.
<<http://www.ietf.org/rfc/rfc1305.txt>>
- [b-IETF RFC 1786] IETF RFC 1786 (1995), *Representation of IP Routing Policies in a Routing Registry (ripe-81++)*.
<<http://www.ietf.org/rfc/rfc1786.txt>>
- [b-IETF RFC 1812] IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*.
<<http://www.ietf.org/rfc/rfc1812.txt>>

- [b-IETF RFC 2018] IETF RFC 2018 (1996), *TCP Selective Acknowledgment Options*.
<<http://www.ietf.org/rfc/rfc2018.txt>>
- [b-IETF RFC 2330] IETF RFC 2330 (1998), *Framework for IP Performance Metrics*.
<<http://www.ietf.org/rfc/rfc2330.txt>>
- [b-IETF RFC 3148] IETF RFC 3148 (2001), *A Framework for Defining Empirical Bulk Transfer Capacity Metrics*.
<<http://www.ietf.org/rfc/rfc3148.txt>>
- [b-IETF RFC 3357] IETF RFC 3357 (2002), *One-way Loss Pattern Sample Metrics*.
<<http://www.ietf.org/rfc/rfc3357.txt>>
- [b-IETF RFC 3393] IETF RFC 3393 (2002), *IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)*.
<<http://www.ietf.org/rfc/rfc3393.txt>>
- [b-IETF RFC 3432] IETF RFC 3432 (2002), *Network performance measurement with periodic streams*.
<<http://www.ietf.org/rfc/rfc3432.txt>>
- [b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.
<<http://www.ietf.org/rfc/rfc3550.txt>>
- [b-IETF RFC 6576] IETF RFC 6576 (2012), *IP Performance Metrics (IPPM) Standard Advancement Testing*.
<<https://www.rfc-editor.org/rfc/rfc6576.txt>>
- [b-IETF RFC 6673] IETF RFC 6673 (2012), *Round-Trip Packet Loss Metrics*.
<<https://www.rfc-editor.org/info/rfc6673>>
- [b-IETF RFC 7398] IETF RFC 7398 (2015), *A Reference Path and Measurement Points for Large-Scale Measurement of Broadband Performance*.
<<https://www.rfc-editor.org/info/rfc7398>>
- [b-BEREC] BoR (18) 32: TENDER SPECIFICATIONS, No BEREC/2018/01/OT Net Neutrality Measurement Tool, marzo de 2018.
- [b-C-298] Kotanis, Irina (2015), *Proposals for E.802 Annex: minimum required of samples, statistical significance for benchmarking and quality trends evaluations and minimum required number of mobile agents, (with revisions)*, ASCOM, Suiza.
- [b-CVST] Krueger, T. y M. Braun (2012), *R package: Fast Cross – Validation via Sequential Testing, version 0.1*.
- [b-Damjanovic] Damjanovic, Welzl et al. (2008), *Extending the TCP Steady-State Throughput Equation for Parallel TCP Flows*, University of Innsbruck, Budapest University of Technology.
<<http://heim.ifi.uio.no/~michawe/research/publications/mulPadhye-TechnicalReport.pdf>>
- [b-Ekelin] Ekelin, S., Nilsson, M., Hartikainen, E., Johnsson, A., Mångs, J., Melander, B., Björkman, M. (2006), *Real-time measurement of end-to-end available bandwidth using kalman filtering*, IEEE/IFIP Network Operations and Management Symposium, Vancouver, Canadá.
- [b-Google-Police] "An Internet-Wide Analysis of Traffic Policing", Flach, Papageorge et al., University of Southern California y Google, 2016.
- [b-Lautenschlaeger] Lautenschlaeger, W. (2014), *A Deterministic TCP Bandwidth Sharing Model*, Bell-Labs Alacatel-Lucent
<<https://arxiv.org/abs/1404.4173>>

- [b-Montgomery] Montgomery, D. (1990), *Introduction to Statistical Quality Control – 2nd edition*, ISBN 0-471-51988-X.
- [b-Morton] Morton, Al (2013), *Improved Internet speed tests can enhance QoS and QoE*, Proceedings of the 4th International Workshop on Perceptual Quality of Systems (PQS 2013), Viena, Austria.
- [b-Mou] Mou, M. (2017), *Evaluating a TCP Model-Based Network Performance Measurement Method*, tesis de máster en el MIT, junio de 2017.
<<https://dspace.mit.edu/handle/1721.1/113177>>.
- [b-PAM-12] Oana Goga & Renata Teixeira (2012), *Speed Measurements of Residential Internet Access*, Passive and Active Measurements Conference, PAM-12.
<<https://people.mpi-sws.org/~ogoga/papers/PAM12-speed.pdf>>
- [b-Pod12] OPNFV Project, Intel POD12.
<<https://wiki.opnfv.org/display/pharos/Intel+POD12>>
- [b-Prasad] Prasad, R.S., Murray, M., Dovrolis, C., Claffy, K.C. (2003), *Bandwidth Estimation: Metrics, Measurement Techniques, and Tools*, IEEE Network.
- [b-QUIC] "draft-ietf-quic-recovery-11", Iyengar y Swett. Trabajo en curso, IETF 2018.
<<https://datatracker.ietf.org/doc/draft-ietf-quic-recovery/>>
- [b-Rdev] R Development Core Team (2016), *R: A language and environment for statistical computing*, R Foundation for Statistical Computing, Viena, Austria. ISBN 3-900051-07-0.
<<http://www.r-project.org/>>
- [b-TST 009] ETSI GS NFV-TST 009 V3.1.1, (2018), *Network Functions Virtualisation (NFV) Release 3; Testing; Specification of Networking Benchmarks and Measurement Methods for NFVI*.
<https://www.etsi.org/deliver/etsi_gs/NFV-TST/001_099/009/03.01.01_60/gs_NFV-TST009v030101p.pdf>
<https://docbox.etsi.org/ISG/NFV/Open/Drafts/TST009_NFVI_Benchmarks>
- [b-Wald] Wald, A. (1947), *Sequential Analysis*, Wiley.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
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 multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
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, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación