Unión Internacional de Telecomunicaciones

# UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

# O.211

(01/2006)

SERIE O: ESPECIFICACIONES DE LOS APARATOS DE MEDIDA

Aparatos de medida para redes de protocolo Internet

## Equipo de prueba y medición para realizar pruebas en la capa IP

Recomendación UIT-T O.211

UIT-T

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE O

**ESPECIFICACIONES DE LOS APARATOS DE MEDIDA**

| | |
|---|---|
| Generalidades | O.1–O.9 |
| Acceso para el mantenimiento | O.10–O.19 |
| Sistemas de medida automáticos y semiautomáticos | O.20–O.39 |
| Aparatos de medida para parámetros analógicos | O.40–O.129 |
| Aparatos de medida para parámetros digitales y analógicos/digitales | O.130–O.199 |
| Aparatos de medida para parámetros de canales ópticos | O.200–O.209 |
| **Aparatos de medida para redes de protocolo Internet** | **O.210–O.219** |

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

# Recomendación UIT-T O.211

## Equipo de prueba y medición para realizar pruebas en la capa IP

**Resumen**

En esta Recomendación se especifican una firma de medición de la calidad de funcionamiento de IP (IPPMS) y paquetes de prueba para medir la calidad de funcionamiento y la disponibilidad de los servicios de la red IP a través de zonas administrativas, redes compuestas y entre dispositivos heterogéneos. La IPPMS puede utilizarse para soportar la puesta en funcionamiento y el mantenimiento de redes basadas en IPv4 e IPv6.

**Orígenes**

La Recomendación UIT-T O.211 fue aprobada el 13 de enero de 2006 por la Comisión de Estudio 4 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

**Palabras clave**

Calidad de funcionamiento de red, medición activa.

## PREFACIO

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

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

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

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

## NOTA

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

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

# ÍNDICE

# Recomendación UIT-T O.211

## Equipo de prueba y medición para realizar pruebas en la capa IP

### 1 Alcance

Para poder soportar la puesta en servicio y el mantenimiento de redes basadas en el protocolo IP, conviene disponer de un formato de paquete de prueba IP normalizado común de modo que pueda lograrse el *interfuncionamiento* entre los equipos de prueba y la comparación de los resultados de las mediciones. Para la medición de la calidad de funcionamiento de las redes y servicios basados en IPv4 e IPv6 con diferentes Tipos-P (Type-P), resulta necesario el interfuncionamiento entre equipos de fabricantes heterogéneos a fin de poder realizar mediciones de los parámetros (IPER, IPLR, IPTD, IPDV, IPSLB, IPRR) conformes a las Recs. UIT-T Y.1540 [4] y M.2301 [1] a través de dominios administrativos o de redes compuestas. El formato del paquete debería facilitar no solamente la realización de las mediciones entre los dominios de los operadores, sino también la identificación del responsable de la prueba a cargo de la medición.

Esto es análogo a requisitos anteriores en las capas de red PDH/SDH (capa 1) y ATM (capa 2) especificados en las Recs. UIT-T O.181 [2] y O.191 [3]. El paquete de prueba debe contener la información adecuada necesaria para medir los parámetros de calidad de funcionamiento de la red principales que se especifican en las Recs. UIT-T Y.1540 [4] y M.2301 [1].

Esta Recomendación trata de la medición de la calidad de funcionamiento de los servicios de red IP.

Asimismo, las técnicas de medición deberán soportar los criterios de medición especificados por las Comisiones de Estudio 2, 4, 9, 12, 13, 15 y 16 del UIT-T, ATIS T1A1, ETSI TIPHON, EURESCOM, 3GPP y el IETF.

El objetivo de esta Recomendación es normalizar una firma de medición de la calidad de funcionamiento de IP común denominada IPPMS y paquetes de prueba a fin de poder medir la calidad de funcionamiento y la disponibilidad de los servicios de red IP a través de zonas administrativas, redes compuestas y entre dispositivos heterogéneos. La capa IP soporta muchos y diferentes servicios basados en IP que pueden tener distintos requisitos de calidad de funcionamiento, y por consiguiente los paquetes de prueba deben ser, en la medida posible, *representativos de los servicios* transportados por la capa IPv4 y/o IPv6 para las pruebas de establecimiento de servicio y la supervisión del mantenimiento, localización y la reparación de averías y los acuerdos de niveles servicios (SLA, *service level agreement*).

No es el objetivo de esta Recomendación especificar la forma en la que se activan o desactivan las mediciones, ni definir la gestión de los resultados de las mediciones. Sin embargo, la firma de la medición propiciará la identificación de una medida y su iniciador.

### 2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[1] Recomendación UIT-T M.2301 (2002), *Objetivos de rendimiento y procedimientos para establecer y mantener redes basadas en el protocolo Internet*.

[2] Recomendación UIT-T O.181 (2002), *Equipo de medición para determinar la característica de error en las interfaces de módulo de transporte síncrono de nivel N*.

[3] Recomendación UIT-T O.191 (2000), *Equipo para medir la calidad de transferencia de células de conexiones en modo de transferencia asíncrono*.

[4] Recomendación UIT-T Y.1540 (2002), *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*.

[5] Recomendación UIT-T Y.1541 (2006), *Objetivos de calidad de funcionamiento de red para servicios basados en el protocolo Internet*.

[6] Recomendación UIT-T Y.1241 (2001), *Soporte de servicios basados en el protocolo Internet que utilizan capacidades de transferencia de protocolo Internet*.

[7] 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)*.

[8] Recomendación UIT-T G.7041/Y.1303 (2005), *Procedimiento de entramado genérico*.

[9] Recomendación UIT-T M.1400 (2004), *Designaciones para la interconexión entre operadores de red*.

[10] IETF RFC 4148 (2005), *IP Performance Metrics (IPPM) Metrics Registry*.

[11] ISO 3166-1:1997, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*.

## 3 Definiciones

Las definiciones a continuación fueron extraídas de la Rec. UIT-T Y.1241 [6].

**3.1 servicio basado en el protocolo Internet**: Un servicio basado en el IP se define como un servicio proporcionado por el plano de servicio al usuario (por ejemplo, un anfitrión (sistema de extremo) o un elemento de red) y que utiliza las capacidades de transferencia IP y las funciones de gestión y control asociadas para entregar la información de usuario especificada por los acuerdos de nivel de servicio.

**3.2 servicio de red de protocolo Internet**: Un servicio de red IP se define como un servicio de transmisión de datos en el cual los datos que pasan a través de la interfaz entre el usuario y el proveedor son transferidos en forma de paquetes IP (a veces denominados datagramas). El servicio de red IP incluye el servicio proporcionado al utilizar las capacidades de transferencia IP.

**3.3 capacidad de transferencia de protocolo Internet**: La capacidad de transferencia IP se define como el conjunto de capacidades de red suministradas por la capa IP. Puede ser caracterizada por el contrato de tráfico así como por los atributos de calidad de funcionamiento soportados por funciones de control y de gestión de las capas de protocolo subyacentes.

En la Rec. UIT-T Y.1540 se definen el servicio IP de extremo a extremo y el punto de medición (MP, *measurement point*) de la siguiente manera:

**3.4 servicio basado en el protocolo Internet de extremo a extremo**: En esta Recomendación, el servicio IP de extremo a extremo se refiere a la transferencia de datagramas IP generados por el usuario (referidos como paquetes IP en esa Recomendación) entre dos anfitriones de extremo especificados por sus direcciones IP completas.

**3.5 punto de medición (MP, *measurement point*)**: Límite entre un anfitrión y un enlace adyacente en el cual pueden observarse y medirse eventos de referencia de calidad de funcionamiento. De acuerdo con la Rec. UIT-T I.353 [7], los protocolos Internet normalizados

pueden ser observados en los puntos de medición IP. La Rec. UIT-T I.353 ofrece más información acerca de los MP relativos a los servicios digitales.

**3.6 tipo-P**: En la norma RFC 2330 se define un marco de mediciones de calidad de funcionamiento. En esta norma se introduce la noción de tipo de paquete, el Type-P. Este corresponde a la pila de protocolos presente en el IP y a los encabezamientos SUB-IP del paquete. Un Type-P se representa como una lista de nombres de identificadores de protocolos. Los nombres correspondientes para IP se definen en la norma RFC 2896 del IETF. Los nombres de identificadores de protocolos específicos para IPv6 se definen en la norma RFC 3919 del IETF. Como un ejemplo, el Type-P ip.udp.snmp difiere del Type-P ip.ip6.udp.snmp porque el segundo tipo no es solamente un paquete SNMP por IPv6 sino que también es un paquete IPv6 encapsulado en IP. Esta definición se emplea en esta Recomendación únicamente para ofrecer ejemplos de encapsulación claros.

**3.7 definición de la firma de medición del protocolo Internet (IPPMS, *IP performance measurement signature*)**: Un paquete de prueba de IP es un paquete IP regular que contiene un bloque de campos normalizado necesario para realizar la medición. Este bloque se denomina firma de medición de la calidad de funcionamiento IP (IPPMS).

## 4 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

| | |
|---|---|
| 3GPP | Proyecto asociado de tercera generación (*third generation partnership project*) |
| ATIS | Alliance for Telecommunications Industry Solutions |
| ATM | Modo de transferencia asíncrono (*asynchronous transfer mode*) |
| BGP | Protocolo de pasarela de frontera (*border gateway protocol*) |
| CAC | Control de admisión de conexión (*connection admission control*) |
| CIF | Formato de identificador de controlador (*controller identifier format*) |
| CRC | Verificación por redundancia cíclica (*cyclic redundancy check*) |
| CRC32 | Verificación por redundancia cíclica de 32 bits (*32-bit cyclic redundancy check*) |
| DiffServ | Servicios diferenciados (*differentiated service*) |
| DoS | Denegación de servicio (*denial of servi*ce) |
| DSCP | Punto de código de servicio diferenciado (*differentiated service code point*) |
| DST | Destino (*destination*) |
| ETSI | Instituto Europeo de Normas de Telecomunicación (*European Telecommunications Standards Institute*) |
| EURESCOM | European Institute for Research and Strategic Studies in Telecommunications |
| FR | Retransmisión de trama (*frame relay*) |
| FTP | Protocolo de transferencia de ficheros (*file transfer protocol*) |
| HTTP | Protocolo de transferencia de hipertexto (*hyper text transfer protocol*) |
| ICMP | Protocolo de mensaje de control Internet (*Internet control message protocol*) |
| ID | Identificador (*identifier*) |
| IETF | Grupo de tareas especiales de ingeniería en Internet (*Internet engineering task force*) |
| IntServ | Servicio integrado (*integrated service*) |

| | |
|---|---|
| IP | Protocolo Internet (*Internet protocol*) |
| IPDR | Tasa de descarte de paquetes IP (*IP packet discard rate*) |
| IPDV | Variación de retardo del paquete IP (*IP packet delay variation*) |
| IPER | Tasa de errores en los paquetes IP (*IP packet error ratio*) |
| IPLR | Tasa de pérdida de paquetes IP (*IP packet loss ratio*) |
| IPOD | Dominio de operador IP (*IP operator domain*) |
| IPPM | Métricas de la calidad de funcionamiento IP (*IP performance metrics*) |
| IPPMS | Firma de medición de la calidad de funcionamiento del protocolo Internet (*IP performance measurement signature*) |
| IPRR | Tasa de reordenamiento de paquetes IP (*IP packet reordering ratio*) |
| IPRTD | Retardo de ida y vuelta del paquete IP (*IP packet round trip delay*) |
| IPSLBR | Tasa de bloques de paquetes IP con muchas pérdidas (*IP severely loss block ratio*) |
| IPTD | Retardo de transferencia de paquetes IP (*IP packet transfer delay*) |
| IPv4 | Protocolo internet versión 4 (*IP version 4*) |
| IPv6 | Protocolo internet versión 6 (*IP version 6*) |
| LL | Capas inferiores (*lower layers*) |
| MIB | Base de información de gestión (*management information base*) |
| MP | Punto de medición (*measurement point*) |
| MPEG | Grupo de expertos en imágenes en movimiento (*moving picture experts group*) |
| MTTR | Tiempo medio de restablecimiento (*mean time to restore*) |
| NAT | Traducción de dirección de red (*network address translation*) |
| NTP | Punto de terminación de red (*network termination point*) |
| OBGR | Encaminador de pasarela externa de operador (*operator border gateway router*) |
| PAM | Medición pasiva y activa (*passive and active measurement*) |
| PAT | Traducción de dirección de protocolo (*protocol address translation*) |
| PDH | Jerarquía digital plesiócrona (*plesiochronous digital hierarchy*) |
| PDU | Unidad de datos de protocolo (*protocol data unit*) |
| PING | Grupo de paquetes entre redes (Internet) (*packet inter-network* (*Internet*) *grouper*) |
| PPP | Protocolo punto a punto (*point-to-point protocol*) |
| QoS | Calidad de servicio (*quality of service*) |
| RMON | Supervisión de red a distancia (*remote network monitoring*) |
| RTP | Protocolo de transporte en tiempo real (*real time transport protocol*) |
| SDH | Jerarquía digital síncrona (*synchronous digital hierarchy*) |
| SDU | Unidad de datos de servicio (*service data unit*) |
| SLA | Acuerdo de nivel de servicio (*service level agreement*) |
| SN | Número de secuencia (*sequence number*) |
| SRC | Fuente (*source*) |

| | |
|---|---|
| STM-N | Modulo de transporte síncrono, nivel N (*synchronous transport module, level n*) |
| SUB-IP | Capa sub IP (*sub IP layer*) |
| TCP | Protocolo de control de transmisión (*transmission control protocol*) |
| TIPHON | Armonización de telecomunicaciones y protocolo Internet por las redes (*telecommunications and Internet protocol harmonization over networks*) |
| TSC | Control de indicación de tiempo (*timestamp control*) |
| TSF | Formato de indicación de tiempo (*timestamp format*) |
| Tx | Transmisor (*transmitter*) |
| UDP | Protocolo de datagrama de usuario (*user datagram protocol*) |
| VoIP | Voz sobre el protocolo Internet (*voice over IP*) |

## 5 Consideraciones relativas a lo más novedoso

### 5.1 PING de ICMP y Traceroute (trazo de trayecto)

Con la utilización de métodos simples como "PING" de ICMP o Traceroute se puede medir únicamente el retardo de ida y vuelta del paquete IP (IPRTD) y el retardo unidireccional no es, por supuesto, exactamente igual a la mitad del IPRTD en una red de paquetes. Cuando se utiliza PING hay otros dos problemas: la función de respuesta PING se ha venido desactivando cada vez con mayor frecuencia en los encaminadores a fin de reducir los ataques por piratería informática y denegación de servicio y, aun en el caso de que esté activada, PING tiene la prioridad más baja en el tratamiento de los paquetes en el encaminador. Por consiguiente, el retardo medido mediante PING no aporta una medición real del retardo experimentado por el tráfico de los clientes. De hecho, PING representa en realidad sólo una verificación de conectividad básica, aunque útil.

### 5.2 Soluciones de medición activa existentes

Los sistemas existentes de medición de la calidad de funcionamiento de las redes y servicios IP no interfuncionan entre fabricantes heterogéneos, aunque comparten la misma semántica y los mismos métodos. El paquete de prueba se crea por encima de un paquete IP normal. La serie de protocolos presente en el encabezamiento de IP permite describir el Type-P del paquete. Las piezas de información dedicadas a la medición se insertan en el paquete.

Los paquetes de medición difieren por el significado, el orden, el nombre, la unidad, el tamaño y por la ubicación de la información de prueba en los datos del paquete. Los campos comunes son:

– el dispositivo que ha enviado el paquete;
– la interfaz que ha enviado el paquete;
– el identificador del tren al que pertenece el paquete;
– la indicación de tiempo absoluta que corresponde al momento en que se envía el paquete;
– el número de secuencia del paquete;
– una suma de control o una CRC calculada en los campos anteriores o en todo el paquete IP.

En las implementaciones existentes se inserta la información de prueba al principio o al final de la SDU del paquete de prueba IP.

La Recomendación debe abarcar los dos diseños.

## 6 Requisitos y beneficios de un paquete de prueba IP

En la presente Recomendación se especifica un formato de paquete de prueba IP que se podrá utilizar cuando se lleve a cabo la puesta en servicio de la red y las pruebas de mantenimiento a fin de verificar los requisitos de la calidad de funcionamiento de la transferencia IP de los servicios basados en IP mediante la medición de las métricas de IP que se definen en las Recs. UIT-T Y.1540 [4] y M.2301 [1].

En esta cláusula se examinan los requisitos y los beneficios generales de un paquete de prueba normalizado.

### 6.1 Requisitos generales

En la Rec. UIT-T M.2301 [1] se presentan dos métodos de medición básicos.

Para las mediciones intrusivas se utilizan trenes de paquetes de prueba IP para crear flujos IP en el trayecto que será sometido a prueba. Estos paquetes de prueba se entrelazan con los flujos de tráfico normal entre dos puntos de medición (MP, *measurement point*), o se transmiten como un tren continuo de tráfico de seudoclientes.

Para las mediciones no intrusivas se utiliza uno de dos métodos:

– supervisión y recopilación de datos MIB de los elementos de la red tal como los encaminadores para la evaluación de la calidad de funcionamiento y el mantenimiento;

– medición de la calidad de funcionamiento de los paquetes IP de los clientes.

Las mediciones no intrusivas permiten supervisar no solamente los paquetes IP de los clientes, sino también los paquetes de prueba IP como tráfico IP regular. Existe un método de medición pasivo y activo que se denomina PAM, que podría considerarse como un "modo mixto" en el cual los paquetes de prueba se insertan de manera intrusiva, aunque se supervisan de manera no intrusiva. Como un ejemplo, los dispositivos de sondeo no intrusiva que se agregan en MP esenciales en la red tales como los encaminadores de pasarela pueden permitir la supervisión de los paquetes de prueba a fin de medir la calidad de funcionamiento entre los dominios.

Para medir la calidad de servicio, es importante disponer de un interfuncionamiento operacional entre los instrumentos de fabricantes heterogéneos y poder realizar la medición del retardo unidireccional y de la pérdida de paquetes unidireccional a través de zonas administrativas o de redes compuestas con paquetes Type-P diferentes.

Por consecuencia, en la Recomendación se deben considerar dos puntos principales:

– Cuando se llevan a cabo pruebas de puesta en funcionamiento de la red y de establecimiento de servicios, es crucial utilizar un tren de paquetes de prueba IP que simule las clases de servicios de aplicación que habrán de soportarse.

– Los datos IP no se transportan nunca directamente sobre IP. El tráfico de usuario se transporta principalmente por encima de UDP o TCP, pero no solo.

### 6.2 Beneficios de la normalización de un paquete de prueba IP

La normalización de un paquete de prueba IP tiene muchas ventajas:

– Los servicios basados en IP pueden ponerse en funcionamiento y establecerse consistentemente y la QoS puede establecerse de acuerdo con los SLA negociados.

– La calidad de servicio de la red y la QoS pueden supervisarse consistentemente y los resultados de las mediciones pueden compararse con referencia a los SLA y correlacionarse entre diferentes MP e instrumentos.

– Puede asegurarse el interfuncionamiento entre los instrumentos de diferentes fabricantes.

– Puede garantizarse el interfucionamiento de las mediciones entre dominios administrativos y redes compuestas.

## 6.3 Interfuncionamiento

La definición del paquete de prueba IP debe ofrecer el interfuncionamiento entre los instrumentos de fabricantes heterogéneos a fin de poder realizar mediciones de métricas a través de zonas administrativas y entre redes compuestas.

Actualmente, durante una prueba en la que participan equipos heterogéneos y/o zonas administrativas, el identificador de la medición (básicamente la identificación de la fuente) establecido por la fuente no tiene ningún significado para el destinatario.

Para mejorar el interfuncionamiento, el paquete de prueba IP debe transportar información que permita identificar de manera inequívoca el controlador de la medición.

## 6.4 Multidifusión IP y movilidad

La definición debe tener en cuenta la medición de la calidad de funcionamiento de los servicios multidifusión y de los servicios IP móviles.

## 6.5 Coexistencia de IPv4 e IPv6

Para posibilitar la medición de extremo a extremo, el paquete de prueba no debe depender de IPv4 o de IPv6.

Los mecanismos de traducción de protocolo entre IPv4 e IPv6 y la coexistencia de ellos representan fuentes que pueden impedir el interfuncionamiento de las mediciones.

El paquete de prueba no debe ser rechazado, siempre que sea posible, por la traducción entre IPv6/IPv4 o los mecanismos de transición.

## 6.6 Protocolo de transporte

En la figura 1 se muestra un modelo de capas de la calidad de funcionamiento del servicio IP que incluye UDP y TCP y que se describe inicialmente en la Rec. UIT-T Y.1540 [4].

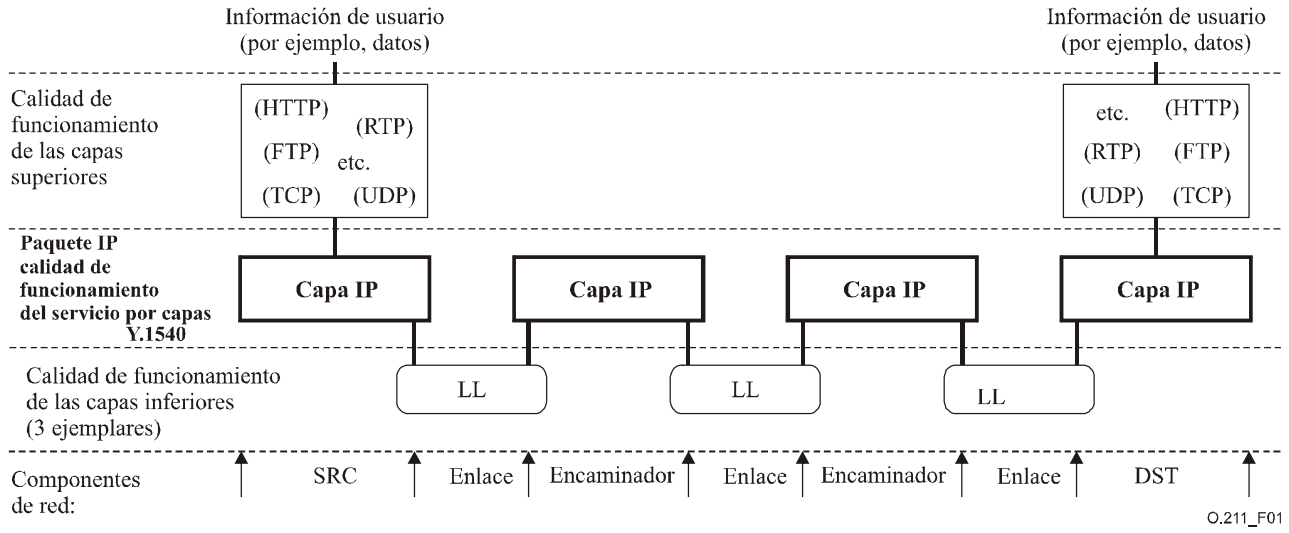


**Figura 1/O.211 – Ejemplo de un modelo de capas Y.1540 de la calidad de funcionamiento del servicio IP**

En muy raras ocasiones los datos IP se transportan directamente por encima de IP. En la actualidad, la información de los usuarios se transporta principalmente por encima de UDP o TCP. Por consecuencia, el paquete de prueba debe permitir la medición de la calidad de funcionamiento de los trenes UDP y TCP.

No obstante, la información de los usuarios no se transporta únicamente sobre UDP o TCP. En realidad, existen 46 protocolos definidos que pueden ser encapsulados directamente por IP. Idealmente, la definición del paquete de prueba debe permitir la medición de la calidad de funcionamiento de las redes y los servicios basados en IP que se apoyan en estos protocolos.

No se encuentra dentro del alcance de esta Recomendación identificar a cuáles de estos protocolos se les debe medir la calidad de funcionamiento. Además, esta Recomendación debe tener en cuenta el hecho de que a corto plazo se definirán nuevos protocolos.

Por consiguiente, esta Recomendación debe proporcionar al menos un paquete de prueba flexible para medir la calidad de funcionamiento de cualquier protocolo encapsulado directamente por encima de IPv4 o IPv6.

### 6.7 Paquete de prueba representantivo

Para que un tren de paquetes de prueba IP sea representativo de un servicio IP debe respetar, a menudo, la encapsulación de ese servicio.

La mayoría de las aplicaciones profesionales, a las que se tiene acceso desde la oficina, están disponibles a través de un NAT/PAT o un cortafuegos. La mayoría de ellas funcionan por encima de TCP, aunque no exclusivamente:

– Los paquetes de prueba deben pasar a través del NAT/PAT y del cortafuegos de la misma manera que los paquetes de los servicios IP.

La QoS se implementa, en la mayoría de los casos utilizando mecanismos CAC que establecen el punto de código DiffServ en el encabezamiento de cada paquete IP. Los encaminadores asignan prioridades a los paquetes con arreglo a sus valores de punto de código:

– El CAC debería clasificar el paquete de prueba con el mismo punto de código del servicio del que se pretende medir la calidad de funcionamiento con el paquete de prueba.

Como los servicios basados en IP no se encapsulan directamente en IP, no tiene sentido definir un paquete de prueba IP en el nivel IP bruto.

### 6.8 Relación con otras organizaciones o foros

El objetivo es aumentar el interfuncionamiento operacional. Básicamente, esto consiste en fomentar la necesidad de compartir los mismos paquetes de medición entre diversas organizaciones y foros, y en la reutilización de las normas que ya se han definido.

### 6.9 Criterios de medición y parámetros

En las Recs. UIT-T Y.1540 [4] y M.2301 [1] se definen criterios de medición y objetivos de calidad de funcionamiento para las redes basadas en IP.

En la cláusula 6/M.2301 [1] se presentan los métodos de medición y se identifican las métricas que pueden determinarse utilizando los paquetes de prueba. En el cuadro 1 se actualiza dicha correspondencia:

**Cuadro 1/O.211 – Medición intrusiva y no intrusiva de los parámetros de calidad de funcionamiento**

| Parámetro | Medición intrusiva | Medición no intrusiva |
|---|---|---|
| IPTD | √ | (Nota) |
| IPDV | √ | (Nota) |
| IPER | √ | √ |
| IPLR | √ | √ |
| IPDR | | √ |
| NOTA – IPTD e IPDV pueden calcularse a través de medición no intrusiva. Como un ejemplo, el mismo paquete se detecta y se le agrega una indicación de tiempo en dos lugares, y a continuación esta información se recopila a fin de calcular la diferencia de tiempo. En los documentos del Grupo de Trabajo relativo al muestreo de paquetes del IETF se describen dichas técnicas. | | |

### 6.9.1 Retardo de transferencia de paquetes IP (IPTD)

El IPTD es una métrica primaria que se define en 6.2/Y.1540 [4].

Las mediciones de la característica del retardo se realizan entre los MP. La prueba consiste en el envío de un tren de paquetes con indicaciones de tiempo, que se distribuye en el tráfico entre un extremo y el otro. Se registra la hora en la que se recibe cada paquete.

La hora en la que cada paquete fue transmitido se resta de la hora en la que fue recibido a fin de producir el resultado de IPTD unidireccional de ese paquete.

Por consecuencia, el parámetro IPPMS debe tener un campo de indicación de tiempo absoluto.

### 6.9.2 Variación de retardo del paquete IP (IPDV)

En la Rec. UIT-T Y.1540 [4] se presentan varias definiciones de la variación de retardo del paquete IP. En el apéndice II/Y.1541 [5] se define con claridad el parámetro IPDV como la variación de retardo entre paquetes. Se utiliza la misma definición de la norma RFC 3393.

En el caso del parámetro IPDV, durante el intervalo de medición el valor de IPTD más bajo se resta del más alto a fin de producir la variación de retardo.

Con el objeto de calcular los límites de error de la medición de IPDV el emisor del parámetro IPPMS debe disponer de un campo para transportar la precisión del reloj del emisor.

### 6.9.3 Tasa de errores en los paquetes IP (IPER)

IPER constituye una métrica secundaria que se define en 6.3/Y.1540 [4].

Las mediciones de la característica de error se transportan entre los MP. La prueba consiste en el envío de un tren de paquetes numerados, distribuidos en el tráfico de un extremo al otro. Cada paquete de prueba contiene bits de verificación de errores. En el extremo receptor se verifican los paquetes con error y se comprueba si falta alguno.

En el caso del parámetro IPER, se registra el número total de paquetes con error, así como el número total de paquetes recibidos. La relación entre los dos valores constituye la IPER.

El paquete de prueba debe transportar información para detectar los bits erróneos en el paquete cuando se realiza la medición en el nivel IP o en el nivel SUB IP.

### 6.9.4 Tasa de pérdida de paquetes IP (IPLR)

El parámetro IPLR es una métrica secundaria que se define en 6.4/Y.1540 [4].

En el caso de IPLR, se registran los paquetes faltantes, así como el número total de paquetes enviados. La relación entre los dos valores representa la IPLR.

Por consecuencia, el parámetro IPPMS debe disponer de un campo para numerar los paquetes en el tren de paquetes de prueba.

### 6.9.5 Tasa de bloques de paquetes IP con muchas pérdidas (IPSLBR)

El parámetro IPSLBR es una métrica secundaria que se define en 6.6/Y.1540 [4].

Este parámetro exige periodos de observación prolongados. Como los periodos de observación pueden realizarse en enlaces de alta velocidad necesitan un número de secuencia grande para identificar las secuencias de los paquetes de prueba. Por consiguiente, el número de secuencia del parámetro IPPMS debe tener una longitud de 32 ó 64 bits.

### 6.9.6 Tasa de reordenamiento de paquetes IP (IPRR)

El parámetro IPRR se define en el apéndice VII/Y.1540 [4].

Se produce un paquete fuera de orden o reordenado cuando el paquete tiene un número de secuencia más bajo que el valor del paquete esperado y por lo tanto el paquete está reordenado.

Por consiguiente, el número de secuencias del paquete de la definición debe ser suficientemente largo para contar una secuencia larga de paquetes de prueba. Una longitud de 32 ó 64 bits es apropiada.

### 6.9.7 No disponibilidad

En la Rec. UIT-T Y.1540 se definen los criterios que permiten declarar periodos de no disponibilidad. El servicio IP no está disponible en una base extremo a extremo si la IPLR es mayor o igual a 75% durante un intervalo de evaluación de 5 minutos. Esos valores deberían considerarse provisionales.

La indicación de tiempo debe ser lo suficientemente larga para almacenar 5 minutos de tiempo.

### 6.9.8 Consideraciones sobre el encaminamiento de paquetes IP

En el apéndice I/Y.1540 se introduce la necesidad de medir la influencia del encaminamiento IP en la calidad de funcionamiento IP.

Como la duración de la convergencia de BGP es cercana a 30 segundos, un campo con una longitud de 64 indicaciones de tiempo resulta apropiado.

### 6.9.9 Detección del paquete

La firma IPPMS debe proporcionar un modo que facilite la detección de los paquetes de prueba en los nodos intermedios por los que pasa el tren de los paquetes de prueba.

## 7 Marco de los paquetes de medición de la calidad de funcionamiento IP

El objetivo es normalizar una firma de paquete que permita medir la calidad de funcionamiento y la disponibilidad de las redes y los servicios basados en IPv4 e IPv6 a través de zonas administrativas, redes compuestas y entre dispositivos heterogéneos.

El primer paso consiste en la definición de un bloque de información común, es decir, la IPPMS.

El segundo paso consiste en la especificación de paquetes de prueba con arreglo a los requisitos y a las limitaciones. La primera limitación es tener en cuenta la ubicación de la IPPMS en el paquete de prueba.

El marco se define de la siguiente manera:

– tener en cuenta lo más novedoso en materia de medición;

– especificar un formato que posibilite el interfuncionamiento entre el plano de medición de sistemas de medición de distintos fabricantes;

– especificar un formato que permita identificar el controlador de la medición a fin de facilitar el diálogo entre los sistemas de medición y la gestión de la medición en el futuro;

– especificar un formato que permita la medición de los parámetros de calidad de funcionamiento de la UIT basado en la definición de las métricas de calidad de funcionamiento IP conformes a la norma RFC 4148 [10];

– especificar un formato que permita la medición de la calidad de funcionamiento de los protocolos IP que se definan en el futuro;

– especificar un paquete de prueba compatible con IPv4, IPv6 y con la coexistencia de IPv4 e IPv6;

– especificar un formato de paquete de prueba similar a los paquetes enviados por las aplicaciones IP reales;

– especificar un formato de paquete de prueba que pueda ser reconocido y tratado a alta velocidad;

– especificar un paquete de prueba que permita que los fabricantes incluyan información específica pero que preserve el interfuncionamiento.

## 7.1 Análisis de la ubicación de la IPPMS en el paquete de prueba

La firma IPPMS se concibió de manera que pueda insertarse al principio o al final del paquete tal y como se ilustra en la figura 2.

| IP | Encapsulamiento 1 | Encapsulamiento2… | Datos | Extensiones de la IPPMS | IPPMS |
|---|---|---|---|---|---|
| Conjunto de encabezamiento: longitud variable | | | Longitud variable | Longitud variable | Longitud fija |

**a) IPPMS al final de la SDU de IP**

| IP | Encapsulamiento 1 | Encapsulamiento2… | IPPMS | Extensiones de la IPPMS | Datos | Cola (si la hubiere) |
|---|---|---|---|---|---|---|
| Conjunto de encabezamiento: longitud variable | | | Longitud fija | Longitud variable | Longitud variable | Longitud variable |

**b) IPPMS al principio de la SDDU de la aplicación**

**Figura 2/O.211 – Opciones del formato del paquete de prueba IP**

Cuando la información de prueba se inserta al principio de la unidad de datos Type-P, los emisores y los receptores deben ponerse de acuerdo acerca del Type-P antes de la medición.

Cuando la información de prueba se inserta al final del paquete IP, su ubicación no depende del Type-P, siempre que esta PDU de Type-P no tenga ninguna cola. Por consiguiente, los emisores, los nodos intermedios y los receptores no tienen necesidad de ponerse de acuerdo con respecto al Type-P antes de la medición.

*Ejemplo:*

En el siguiente ejemplo se considera un paquete de prueba RTP. Su Type-P es IP.UDP.RTP.

**IPPMS al principio de la SDU de Type-P**

El emisor envía el siguiente paquete de prueba IP.UDP.RTP.IPPMS.data. Considérese que el receptor tiene capacidad para analizar sólo el nivel UDP, por lo cual, el receptor buscará la IPPMS al principio de la SDU de UDP y no de la SDU de RTP y por consecuencia, no decodificará el paquete como un paquete de prueba válido.

**IPPMS al final del paquete IP**

El emisor envía el siguiente paquete de prueba IP.UDP.RTP.data.IPPMS. Como el receptor buscará la IPPMS al final de la SDU de IP efectivamente podrá reconocerla.

### 7.1.1 IPPMS al final de la SDU de IP

Cuando se inserta la IPPMS al final del paquete IP se obtienen muchas ventajas.

La ventaja es que la especificación del paquete de prueba no depende de ningún protocolo por encima de IP. Por consiguiente, potencialmente es representativo de cualquier paquete de aplicación.

El paquete de prueba IP propuesto que se presenta en la figura 3 consiste en:

– conjunto de encabezamientos de protocolos IP (por ejemplo, ip.udp.snmp, ip6.tcp.http, etc.);
– un bloque de datos;
– una firma IPPMS.

### 7.1.2 IPPMS al principio de la SDU de la aplicación

El nivel de aplicación determina la encapsulación de IP y por consecuencia la ubicación de la IPPMS en el paquete. Cuando la IPPMS se inserta al principio de la SDU de la aplicación del paquete se requiere fijar la encapsulación necesaria o analizar sintácticamente cada uno de los encabezamientos del paquete.

La mayoría de los datos del usuario se transportan por encima de UDP o TCP.

#### 7.1.2.1 Posición del campo IPPMS

El campo IPPMS se ubica directamente después del encabezamiento de la aplicación en el paquete de prueba IP. Ya que la longitud del encabezamiento se conoce para un tipo específico de punto de medición, es muy fácil encontrar el inicio de campo IPPMS.

Otras ventajas de ubicar la IPPMS directamente después del encabezamiento son:

– la alineación automática de 32 bits simplifica el tratamiento en paralelo;
– extensión simple del campo IPPMS normalizado mediante la agregación de elementos de información patentados.

#### 7.1.2.2 Relación entre los mecanismos de Type-P y de QoS en la capa IP

Los requisitos específicos de servicio (por ejemplo, prioridades, retardo máximo, etc.) son tratados mediante la correspondencia de aplicaciones de extremo a extremo específicas con las diferentes clases de QoS o mediante reservación de recursos de red exclusivamente para esas aplicaciones.

Los encaminadores IP pueden implementar diferentes mecanismos de QoS tales como IntServ o DiffServ con los cuales se aplican diferentes reglas de retransmisión a los flujos individuales (IntServ) o a los paquetes asignados a determinadas clases de QoS (DiffServ).

Las decisiones de retransmisión de IntServ se basan en la dirección IP y el número de puerto de destino.

La decisión de retransmisión de Diffserv se basa en el valor del campo DSCP en el encabezamiento IP. El valor de este campo se fija mediante el CAC de un encaminador de entrada del trayecto. Este valor se obtiene analizando el encabezamiento del paquete.

#### 7.1.2.3 Representación de servicios de capa superior en la capa IP

Los únicos parámetros específicos de la aplicación además de la dirección, el número de protocolo, el número de puerto y el DSCP que están visibles en la capa IP son la longitud del paquete y el patrón de tráfico.

Por lo tanto, el paquete de prueba IP debe tener un campo de datos de longitud variable a continuación de la IPPMS.

#### 7.1.2.4 Estructura de encabezamiento fijo

El paquete de prueba más simple que contiene toda la información antes enumerada, tiene un formato de encabezamiento fijo que consta de un encabezamiento IP normalizado seguido de un encabezamiento UDP.

Esto está en armonía con otras actividades que tratan de las mediciones activas en las redes basadas en tramas (véanse las Recs. UIT-T M.2301 [1], O.181 [2] y O.191 [3].)

### 7.1.3 Paquete bruto de IP

El IETF no recomienda el envío de paquetes IP brutos, por consecuencia, en esta Recomendación se propone la utilización de UDP como el Type-P por defecto del paquete de prueba.

### 7.1.4 Paquete de prueba UDP

Las aplicaciones que envían datagramas a un anfitrión deben identificar un objetivo que sea más específico que la dirección IP, ya que por lo general, los datagramas se dirigen a determinados procesos y no al sistema en su totalidad.

El protocolo UDP sirve simplemente como un multiplexor/demultiplexor para el envío y la recepción de datagramas, utilizando puertos para dirigir los datagramas.

El paquete de prueba IP/UDP tiene un formato único caracterizado por:

– una estructura de encabezamiento fijo para el paquete de prueba IP;

– una posición fija de la firma de medición IP (IPPMS) inmediatamente después del encabezamiento UDP.

Este formato de paquete facilita la medición de la calidad de funcionamiento del servicio IP de extremo a extremo conforme a la Rec. UIT-T Y.1540 [4].

### 7.1.5 Protocolo TCP

Las pruebas de calidad de funcionamiento por encima de la capa IP, tales como la calidad de funcionamiento de la conexión TCP (véase la Rec. UIT-T Y.1540 [4] pueden exigir más elementos de información en la trama de prueba.

Esta cláusula será definida en el futuro.

### 7.1.6 Paquete de prueba con la firma IPPMS únicamente en la cabida útil Type-P

Cuando se inserta un bloque de medición ya sea al principio o al final de la SDU de Type-P éste difiere únicamente por la ubicación del IPPMS en el paquete.

Cuando no hay datos en la SDU, la IPPMS se ubica tanto al principio como al final del paquete de prueba. Esto se ilustra en la figura 3.

Este caso permite el interfuncionamiento entre los dos modos de encapsulación.

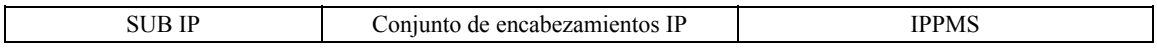


**Figura 3/O.211 – Formato de paquete de prueba común**

### 7.1.7 Resumen de modos de utilización

En el cuadro 2 se muestran las diversas posibilidades de ubicación de la firma IPPMS en el paquete de prueba y su influencia en el interfuncionamiento y el tamaño del paquete.

**Cuadro 2/O.211 – Ubicación de la firma IPPMS**

| Ubicación de la firma IPPMS | Interfuncionamiento | Tamaño del paquete |
|---|---|---|
| 1) Al final de la cabida útil | No es necesario analizar todo el conjunto de encabezamientos. | Cualquiera |
| 2) Al principio de la cabida útil | Requiere el análisis sintáctico del conjunto de encabezamientos.<br>Puede necesitar el conocimiento de la estructura del encabezamiento. | Cualquiera |
| 3) IPPMS = Cabida útil | Con 1 y 2 | Tamaño del paquete diferente del tamaño del paquete de la aplicación.<br>Tamaño de paquete pequeño únicamente. |

### 7.1.8 Generalización a la medición de la calidad de funcionamiento de la clase de servicio

La medición de la calidad de funcionamiento de IP puede necesitar la presencia de encapsulación de transporte o de aplicación para obligar que los paquetes de prueba se traten de la misma manera que los paquetes de aplicación normales.

Para medir la calidad de funcionamiento de una aplicación que se apoya en un protocolo específico se recomienda utilizar el formato que se define en 7.1.6.

Como ejemplo, en la figura 4 se presenta un paquete de prueba RTP.


**Figura 4/O.211 – Ejemplo de paquete de prueba RTP**

Las Recomendaciones en las que se necesita definir paquetes de prueba para medir la calidad de funcionamiento de una aplicación de red pueden utilizar este marco.

NOTA – Las encapsulaciones de algunos protocolos requieren una cola. En este caso, puede resultar necesario analizar la cola y el encabezamiento para localizar la firma IPPMS.

### 7.1.9 Otras posibles utilizaciones

La firma IPPMS especifica un bloque de información útil para medir la calidad de funcionamiento y la disponibilidad de la red. Por consecuencia, puede utilizarse para medir la calidad de funcionamiento de las redes basadas en tramas. En este caso, la firma IPPMS puede insertarse directamente en una trama bruta sin ningún encabezamiento IP.

## 8 Especificación de la firma de medición de la calidad de funcionamiento de IP (IPPMS)

En las siguientes cláusulas se define un formato de paquete de prueba IP que incluye las consideraciones de formato de trama y de cabida útil. Este formato puede utilizarse para mediciones intrusivas de la calidad de funcionamiento de la red IP a fin de soportar el nivel de servicio de QoS y como un estímulo para la supervisión de la calidad de funcionamiento IP no intrusiva en puntos clave de la red. Asimismo, puede emplearse para verificar el caudal si las características programables se fijan a la capacidad de transferencia IP seleccionada (contrato de tráfico) de un servicio de aplicación determinado. El instrumento de prueba necesita la conectividad SUB IP para poder enviar o recibir tráfico de prueba IP a fin de medir la calidad de funcionamiento y la QoS de la red IP. Esto podría incluir una diversidad de formatos de capa de enlace entre los que se encuentran PPP, FR, ATM, Ethernet, etc. Además, el instrumento de prueba tiene que habilitar cada servicio IP ante de medir su calidad de funcionamiento.

El Type-P de un paquete de prueba se define mediante la encapsulación SUB IP y el conjunto de cabeceras IP del paquete.

### 8.1 Tamaño del paquete de prueba IP

El tamaño máximo de un paquete IP es de 65535 bytes, con un tamaño por defecto común de 570 bytes. Cada paquete consiste en un conjunto de encabezamientos y una información de cabida útil. El tamaño del conjunto de encabezamientos IP depende de la versión de IP y de la aplicación encapsulada. El retardo de la paquetización y del tratamiento aumenta con el tamaño del paquete, que es uno de los factores que afectan a las aplicaciones de QoS.

El tamaño del paquete puede tener influencia en los resultados de la mayoría de los parámetros de calidad de funcionamiento de IP. Puede ser conveniente una gama de tamaños de paquetes ya que el tamaño de muchos de los flujos varía considerablemente. Por ejemplo, la aplicación VoIP utiliza paquetes cortos y el vídeo por IP emplea paquetes mucho más grandes. Sin embargo, la evaluación se simplifica con un tamaño de paquete único cuando se trata de evaluar la IPDV, o cuando la evaluación se concentra en los flujos que soportan fuentes de velocidad binaria constante, y por lo tanto, se recomienda un tamaño de campo de información fijo. De conformidad con la definición de IPTD en la Rec. UIT-T Y.1540 [4], la hora de inserción del paquete se incluye en los objetivos de calidad de funcionamiento de IPTD. En la Rec. UIT-T Y.1541 [5] se sugieren campos de información de 160 ó 1500 octetos, pero debe comunicarse cualesquiera que sea el tamaño del campo que se emplee. Además, se recomienda un campo de información de 1500 octetos para estimar los parámetros de calidad de funcionamiento de IP cuando se aplican pruebas de la capa inferior, tales como las mediciones de bits erróneos. Se sugiere que se disponga de paquetes de prueba IP de longitudes fijas de 80, 160, 200, 600 y 1500 bytes como una capacidad mínima a fin de simular tráfico de VoIP, de vídeo y de vídeo MPEG.

Para poder satisfacer las diferentes necesidades, el paquete de prueba incluye una zona de datos que por lo general se rellena según la longitud exigida por la medición.

### 8.2 Intervalo de medición

En las Recs. UIT-T Y.1541 [5] y M.2301 [1] se especifica la calidad de funcionamiento de IP en función del límite superior de cada parámetro. En la Rec. UIT-T Y.1541 [5] se sugiere un intervalo de evaluación de un minuto para IPTD, IPDV, IPER e IPLR. En la Rec. UIT-T Y.1540 [4] se recomienda un periodo de medición de 5 minutos para las mediciones de las métricas de disponibilidad. En las Recomendaciones del UIT-T y en los procedimientos de las operaciones actuales se sugiere medir la calidad de funcionamiento aplicando periodos de 15 minutos, 24 horas, 7 días o 1 mes.

Para tener en cuenta las limitaciones de medición de las métricas la indicación de tiempo de IPPMS se ajusta a dos tipos de utilización diferentes:

– el primero permite una indicación de tiempo absoluta para la medición de la calidad de funcionamiento de la red y los servicios de extremo a extremo a través de diferentes clases de equipos;
– el segundo permite una indicación de tiempo relativa para la medición de la calidad de funcionamiento del enlace.

### 8.3 Firma de medición de la calidad de funcionamiento de IP (IPPMS)

La firma IPPMS tiene una longitud de 32 bytes.

Se trata de la combinación de los siguientes elementos de información:

– un control de firma de medición de la calidad de funcionamiento de IP (control de IPPMS);
– un campo para identificar las métricas que habrán de medirse (Metric_ID);
– un campo reservado para utilización futura (reservado);
– un número de secuencia (Seq_Number);
– un elemento de información de indicación de tiempo de transmisión (Tx_Timestamp);
– un identificador de controlador (Controller_ID);
– un identificador de un flujo de paquetes de prueba (Flow_ID);
– un campo de protección de la firma IPPMS (CRC32).

Para garantizar el interfuncionamiento máximo, es obligatorio disponer únicamente de un formato de la firma del paquete de prueba y un número mínimo de opciones.

A continuación se presenta una propuesta de una firma de paquete de prueba. Ésta, integra todos los requisitos y tiene un tamaño constante de 32 bytes. En el cuadro 3 se enumeran los campos de la IPPMS.

**Cuadro 3/O.211 – Elementos de información de la firma IPPMS**

| Elementos de información | Tamaño (bytes) |
|---|---|
| Control | 2 |
| Metric_ID | 1 |
| Reservados | 1 |
| Seq_Number | 4 |
| Tx_Timestamp | 8 |
| Controller_ID | 10 |
| Flow_ID | 2 |
| CRC32 | 4 |

Esto da por resultado un formato IPPMS común, como se ilustra en la figura 5.

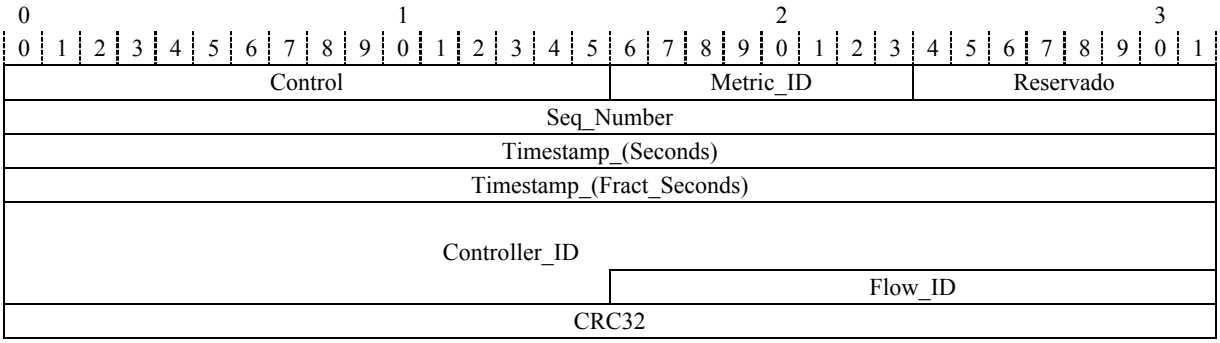


**Figura 5/O.211 – Formato de la firma IPPMS**

## 8.4 Formato detallado de la firma IPPMS

### 8.4.1 Campo de control de IPPMS (Control)

El campo de control de IPPMS tiene una longitud de 2 bytes y está constituido por 6 campos:

– el formato de indicación de tiempo (TSF);
– el control de indicación de tiempo del reloj que envió el paquete (TSC);
– la presencia de extensión (Ext);
– la versión de IPPMS (Ver);
– el formato del identificador del controlador (CIF);
– un campo reservado.

En el cuadro 4 se presentan los tamaños de cada campo.

**Cuadro 4/O.211 – Formato de encabezamiento**

| Campos | Tamaño (bits) |
|---|---|
| Formato de indicación de tiempo (TSF) | 1 |
| Control de indicación de tiempo (TSC) | 3 |
| Presencia de extensión (Ext) | 1 |
| Versión (Ver) | 2 |
| Formato del identificador del controlador (CIF) | 3 |
| Reservado | 6 |

#### 8.4.1.1 Formato de indicación de tiempo (TSF)

Este campo indica si la referencia de tiempo de la indicación de tiempo es absoluta o no.

"0" significa que no se emplea indicación de tiempo absoluta.

"1" significa que se emplea una indicación de tiempo absoluta.

#### 8.4.1.2 Control de indicación de tiempo (TSC)

Este campo transporta la precisión del reloj del emisor. En el cuadro 5 se enumeran los diferentes valores.

**Cuadro 5/O.211 – Control de indicación de tiempo**

| TSC | Valor | Significado: La precisión del reloj es mejor que: |
|---|---|---|
| 000 | 0 | El valor 0 significa que en el momento de envío del paquete, la fuente no estaba sincronizada con una referencia de tiempo absoluta |
| 001 | 1 | 10 ns |
| 010 | 2 | 50 ns |
| 011 | 3 | 500 ns |
| 100 | 4 | 10 µs |
| 101 | 5 | 50 µs |
| 110 | 6 | 500 µs |
| 111 | 7 | ≤10 ms |

#### 8.4.1.3 Presencia de extensión (Ext)

Este campo tiene una longitud de 1 bit.

Los puntos de medición pueden insertar datos patentados en el paquete de prueba preservando el interfuncionamiento de la medición. El campo 'Ext' indica la presencia de ese tipo de información.

Un valor 0 significa que no hay extensión (valor por defecto).

Un valor 1 significa que hay una extensión.

Para llevar a cabo la medición de IPER la extensión debería protegerse mediante una CRC32.

#### 8.4.1.4 Versión de la firma IPPMS (Ver)

Este campo tiene una longitud de 2 bits.

El campo versión, denominado 'Ver', ofrece la capacidad para definir hasta cuatro versiones de IPPMS.

Actualmente, 'Ver' tiene el valor 0.

#### 8.4.1.5 Formato del identificador del controlador (CIF)

Este campo tiene una longitud de 3 bits.

Este campo permite identificar el tipo actual del identificador del controlador. En el cuadro 6 se enumeran los distintos valores.

**Cuadro 6/O.211 – El formato del identificador de la medición**

| CIF | Valor | Significado: El valor del controlador actual transporta: |
|---|---|---|
| 000 | 0 | Reservado |
| 001 | 1 | Un código de operador |
| 010 | 2 | Un número de empresa |
| 011 | 3 | La dirección IPv4, el tipo de protocolo y el puerto del controlador |
| 100 | 4 | Los primeros 10 bytes de una dirección IPv6 del controlador |
| 101 | 5 | Los últimos 6 bytes de una dirección IPv6, el tipo de protocolo y el puerto del controlador |
| 110 | 6 | Patentado |
| 111 | 7 | Reservado |

### 8.4.2 Identificador de la métrica (Metric_ID)

En la norma RFC 4148 [10] se define un registro inicial del "Registro de las métricas de calidad de funcionamiento de IP (IPPM)". Se trata de un registro extensible mantenido por la autoridad de número asignado por Internet (IANA, *Internet assigned number authority*) que se encarga de asignar cada una de las métricas definidas por el Grupo de Trabajo IPPM del IETF con un número de identificación.

Metric_ID tiene una longitud de un byte. Éste, transporta el identificador de la métrica IPPM correspondiente al parámetro de calidad de funcionamiento que habrá de medirse.

Un valor 0 significa que el campo no se utiliza (valor por defecto).

Los paquetes de prueba subsiguientes pueden transportar la lista de métricas (parámetros primarios y secundarios) que habrán de llevarse a cabo. Esto ayuda al receptor a limitar el consumo de recursos.

### 8.4.3 Reservado

Este campo tiene una longitud de un byte.

Este campo no se utiliza en la versión 0 de IPPMS. El receptor no debe de tener en cuenta su valor.

### 8.4.4 Número de secuencia (Seq_Number)

La medición de la pérdida de paquetes exige un número de secuencia para poder identificar los huecos en la secuencia de los paquetes recibidos.

Cada vez hay más servicios IP que atraviesan pasarelas. Éstas pueden modificar el número de secuencia de los paquetes en el encabezamiento IP (por ejemplo, el valor inicial). Muchos cálculos de métricas se apoyan en el análisis del orden de los paquetes. Para proporcionar una secuencia de resultados fiable, es necesario que el número de secuencia se integre en la firma IPPMS. El punto de medición necesita disponer de la capacidad para rellenar y leer el número de secuencia. El número de secuencia de IPPMS (Seq_Number) aumenta con cada trama de prueba en una medición.

Este campo tiene una longitud de 32 bits y es obligatorio.

### 8.4.5 Indicación de tiempo de transmisión (Tx_Timestamp)

Este campo tiene una longitud de 64 bits.

Este campo se utiliza como un contador de 64 bits con retorno a 0 cuando la bandera TSF del elemento de información de control se fija a 0, o se emplea como una indicación de tiempo NTP cuando la bandera TSF se fija a 1.

#### 8.4.5.1 'Segundos' de NTP

Se trata de un campo con una longitud de 32 bits que representa los segundos de la indicación de tiempo NTP.

#### 8.4.5.2 'Fract_Seconds' de NTP

Se trata de un campo con una longitud de 32 bits que representa la parte fraccional de la indicación de tiempo NTP.

### 8.4.6 Identificador del controlador (Controller_ID)

Los instrumentos de medición actuales interfuncionan únicamente cuando pertenecen al mismo fabricante. Para gestionar la medición, los instrumentos de medición insertan 3 campos:

– el dispositivo que envió el paquete;

– la interfaz que envió el paquete;

– el identificador del tren al que pertenece el paquete.

Este tipo de marco no es adecuado para el interfuncionamiento de los instrumentos de prueba ni para el interfuncionamiento entre dominios debido principalmente a que los significados de 'dispositivo', 'interfaz' y 'tren' no son compartidos por el emisor y el receptor. Por consecuencia, en el contexto de una prueba entre dos instrumentos de prueba de diferentes fabricantes, cada instrumento utilizará sus propias reglas de numeración para identificar la prueba. Esto hace que el interfuncionamiento sea imposible ya que el controlador de la medición no proporciona un identificador único de la prueba.

Para posibilitar el interfuncionamiento, se necesita que el controlador de la prueba escoja el identificador de la misma. Como un instrumento de prueba puede ser utilizado simultáneamente por varios controladores, la firma IPPMS debe transportar la identificación del controlador.

Este identificador proporciona al transmisor y al receptor de la medición un identificador inequívoco del controlador de la medición que funciona a través de distintos dominios administrativos.

Su tipo depende del valor del campo CIF del campo de control IPPMS (véase el cuadro 6).

Su valor y tipo pueden cambiar a partir de los paquetes de pruebas subsiguientes. Esto permite transmitir la identificación completa del controlador y por consiguiente, la identificación del flujo.

Se han definido varios tipos para completar la identificación del controlador de la medición.

#### 8.4.6.1 Código del operador

El código del operador tiene una longitud de 10 bytes y su formato es el siguiente:

– 6 bytes para el ID de operador que se define en la Rec. UIT-T M.1400 [9];

– 1 byte para el carácter "/";

– 3 bytes para el indicativo de país que se define en ISO 3166-1 [11].

#### 8.4.6.2 Número de empresa

Identifica el fabricante del punto de medición que envía los paquetes. Esta información aumenta el interfuncionamiento operacional entre los dispositivos de distintos fabricantes.

Si no se utiliza el campo el número de empresa debe fijarse a 0.

#### 8.4.6.3 Dirección IPv4

El valor transporta la dirección, el tipo de protocolo y el puerto del controlador.

#### 8.4.6.4 Dirección IPv6

El valor transporta la dirección IPv6, el tipo de protocolo y el puerto del controlador. Esto se lleva a cabo en 2 pasos que se describen en la definición del campo CIF (cuadro 6).

#### 8.4.6.5 Patentado

Este valor transporta información patentada.

#### 8.4.6.6 Utilización entre dominios e interfuncionamiento

La dirección IP del controlador y el ID del flujo proporcionan un identificador absoluto de la medición.

El código de operador, el número de empresa y la dirección IP del controlador son obligatorios cuando se lleva a cabo una medición entre dos dominios administrativos o dos dispositivos de fabricantes diferentes.

### 8.4.7 Flow_ID (Identificador de flujo)

La firma IPPMS debe incluir un identificador del flujo de los paquetes de prueba correspondiente a la medición.

El flow_Id permite identificar los paquetes de prueba asociados con una medición.

Su longitud es de 2 bytes.

El originador de la medición asigna el ID de flujo.

### 8.4.8 Protección de la firma IPPMS (CRC32)

Este campo tiene una longitud de 32 bits y su presencia es obligatoria.

Este campo se utiliza para proteger la firma IPPMS.

El emisor calcula una CRC32 sobre la firma IPPMS e inserta el resultado en los últimos 4 bytes de la 'CRC32'.

Para verificar la integridad de la firma IPPMS, el receptor calcula una CRC32 y compara el resultado con el valor del campo 'CRC32'. Si los valores son idénticos, en ese caso la IPPMS no contiene ningún bit erróneo y el paquete recibido se clasifica como un paquete de prueba.

Los nodos intermedios pueden utilizar este campo para detectar la presencia de una IPPMS en un paquete.

Se utilizará la siguiente definición del polinomio generador para el cálculo de la CRC-32:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

El cálculo de la CRC debe seguir el procedimiento que se describe, por ejemplo, en la Rec. UIT-T G.7041/Y.1303 [8].

## 9 Paquetes de medición IP para los niveles IPv4 e IPv6

En esta cláusula se definen 6 paquetes de prueba de conformidad con el requisito de medición de la calidad de funcionamiento de la capa IP entre puntos de medición IP.

Una cabida útil no puede encapsularse directamente en la capa IP. Por lo tanto, los paquetes de prueba propuestos son en realidad paquetes UDP como se ilustra en la figura 6.


**Figura 6/O.211 – Formato del paquete de prueba UDP**

El tamaño de los paquetes de longitud fija facilita la detección y la extracción de la firma IPPMS en los nodos intermedios.

El conjunto mínimo de los tamaños del paquete de prueba IPv4 es 80, 160, 200, 600 y 1500. Con 20 bytes reservados para el encabezamiento IPv4, 8 bytes para el encabezamiento UDP y 32 bytes para la firma IPPMS, los números de los bytes de relleno correspondientes son 20, 100, 130, 530 y 1430. Para mejorar el tratamiento en alta velocidad se decidió alinear el relleno en fronteras de 32 bits. Por consiguiente, los tamaños de cabida útil que se utilizan son 52, 132, 164, 564 y 1464.

Además, se propone un paquete de prueba UDP que transporta únicamente los 32 bytes de la firma IPPMS.

## 9.1 Opciones de la firma IPPMS

El formato de IPPMS que se define en 8.3 ofrece mucha flexibilidad. Para aumentar al máximo el interfuncionamiento, se deben aplicar las siguientes configuraciones por defecto:

– no hay extensión;

– el campo CIF puede transportar sólo un código de operador (por ejemplo, entre dominios) y/o la dirección IPv4, el tipo de protocolo y el puerto del controlador (por ejemplo, distribuido) y/o información patentada (por ejemplo, utilización local);

– el valor del campo Metric_ID es 0. El receptor no debe tener en cuenta otros valores;

– patrón de relleno:

  • cualquier patrón de bits puede utilizarse como un patrón de relleno;

  • para las mediciones de IPER, el patrón de relleno debe protegerse utilizando la CRC-32 como se define en 8.4.8, a fin de facilitar la detección de errores. La CRC-32 debe calcularse sobre los primeros N-4 bytes del patrón de relleno, donde N representa la longitud del campo de relleno. Los últimos 4 bytes del campo de relleno representan la CRC-32;

  • el receptor no debe tener en cuenta el campo de relleno para las demás mediciones.

El cambio de estas configuraciones por defecto es responsabilidad del gestor de la prueba y queda fuera del alcance de esta Recomendación.

## 9.2 Tamaño de cabida útil de 32 bytes (con IPPMS únicamente)

Este paquete de prueba se describe en la figura 7.


**Figura 7/O.211 – Tamaño de cabida útil de 32 bytes**

## 9.3 Tamaño de cabida útil de 52 bytes

Este paquete de prueba se describe en la figura 8.

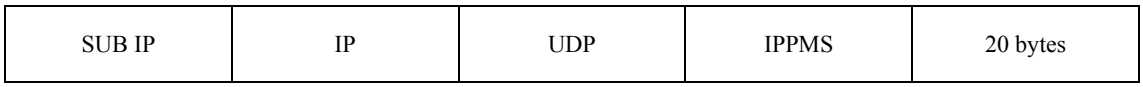


**Figura 8/O.211 – Tamaño de cabida útil de 52 bytes**

## 9.4 Tamaño de cabida útil de 132 bytes

Este paquete de prueba se describe en la figura 9.

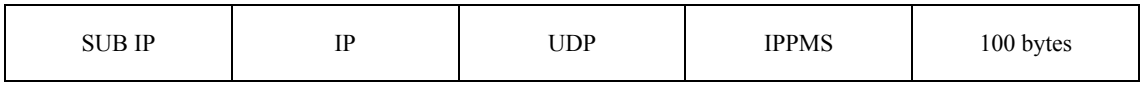


**Figura 9/O.211 – Tamaño de cabida útil de 132 bytes**

### 9.5 Tamaño de cabida útil de 164 bytes

Este paquete de prueba se describe en la figura 10.

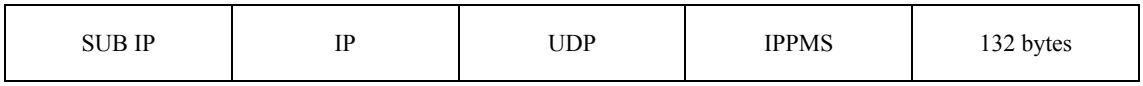


**Figura 10/O.211 – Tamaño de cabida útil de 164 bytes**

### 9.6 Tamaño de cabida útil de 564 bytes

Este paquete de prueba se describe en la figura 11.

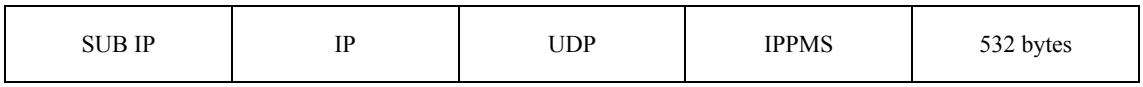


**Figura 11/O.211 – Tamaño de cabida útil de 564 bytes**

### 9.7 Tamaño de cabida útil de 1464 bytes

Este paquete de prueba se describe en la figura 12.

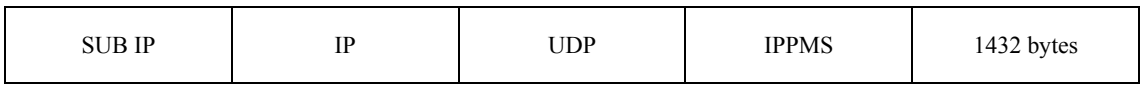


**Figura 12/O.211 – Tamaño de cabida útil de 1464 bytes**

## 10 Seguridad

En la Rec. UIT-T M.2301 [1] se recomienda observar que la medición de la calidad de funcionamiento intrusiva provoca un tráfico adicional a través de la red de manera que debe tenerse precaución de garantizar que la aplicación de esta prueba no genere congestión y la pérdida subsiguiente de paquetes de los clientes.

Para impedir que los sistemas de medición que se utilicen produzcan ataques, existe una estricta exigencia para proponer un mecanismo de seguridad que permita controlar el acceso a la configuración de las mediciones de la red.

Desde la perspectiva de la seguridad de la red, la principal debilidad de la seguridad en una medición de red es el paquete de prueba de control. La normalización de una firma de paquete no facilita el control de un dispositivo de sondeo para que no pueda llevar a cabo un ataque de tipo DoS.

# BIBLIOGRAFÍA


– IETF RFC 1305 (1992), *Network time protocol (Version 3) specification, implementation and analysis*.

– IETF RFC 2330 (1998), *Framework for IP performance metrics*.

– IETF RFC 2679 (1999), *A one-way delay metric for IPPM*.

– IETF RFC 2680 (1999), *A one-way packet loss metric for IPPM*.

– IETF RFC 2896 (2000), *Remote network monitoring MIB protocol identifier macros*.

– IETF RFC 3919 (2004), *Remote network monitoring (RMON) protocol identifiers for IPv6 and multi protocol label switching (MPLS)*.

– IETF RFC 3393 (2002), *IP packet delay variation metric for IP performance metrics (IPPM)*.

## SERIES DE RECOMENDACIONES DEL UIT-T

| | |
|---|---|
| Serie A | Organización del trabajo del UIT-T |
| Serie D | Principios generales de tarificación |
| Serie E | Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos |
| Serie F | Servicios de telecomunicación no telefónicos |
| Serie G | Sistemas y medios de transmisión, sistemas y redes digitales |
| Serie H | Sistemas audiovisuales y multimedios |
| Serie I | Red digital de servicios integrados |
| Serie J | Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios |
| Serie K | Protección contra las interferencias |
| Serie L | Construcción, instalación y protección de los cables y otros elementos de planta exterior |
| Serie M | 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 transmisión telefónica, instalaciones telefónicas y redes locales |
| Serie Q | Conmutación y señalización |
| Serie R | Transmisión telegráfica |
| Serie S | Equipos terminales para servicios de telegrafía |
| Serie T | Terminales para servicios de telemática |
| Serie U | Conmutación telegráfica |
| Serie V | Comunicación de datos por la red telefónica |
| Serie X | Redes de datos, comunicaciones de sistemas abiertos y seguridad |
| Serie Y | Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación |
| Serie Z | Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación |

Impreso en Suiza
Ginebra, 2006