

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2772

(04/2016)

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

Redes de la próxima generación – Seguridad

Mecanismos para los elementos de red con apoyo de la inspección detallada de paquetes

Recomendación UIT-T Y.2772

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	
General	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

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

Recomendación UIT-T Y.2772

Mecanismos para los elementos de red con apoyo de la inspección detallada de paquetes

Resumen

En la Recomendación UIT-T Y.2772 se ofrecen mecanismos para los elementos de red con apoyo de la inspección detallada de paquetes (DPI). En otras palabras, en esta Recomendación se identifican los procedimientos y aspectos metodológicos de la inspección detallada de paquetes respecto de las redes basadas en paquetes. Sirve para ayudar a entender los métodos relacionados con la DPI, la interfaz, el protocolo, los aspectos de procedimiento y los aspectos de procesamiento de los productos relacionados con la DPI.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T Y.2772	2016-04-29	13	11.1002/1000/12709

* 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 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 en la dirección <http://www.itu.int/ITU-T/ipr/>.

© UIT 2017

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

ÍNDICE

	Página
1 Alcance	1
2 Referencias	1
3 Definiciones	2
3.1 Términos definidos en otros documentos	2
3.2 Términos definidos en la presente Recomendación	3
4 Siglas y acrónimos	3
5 Convenios	4
6 Definición del mecanismo DPI	4
7 Repaso de los mecanismos DPI en apoyo de la identificación de aplicaciones	4
7.1 Aspectos generales de los mecanismos DPI	4
7.2 Estructura básica de un nodo DPI	4
7.3 Red típica que soporta funciones DPI	4
7.4 Mecanismo DPI relacionado con el nodo DPI	5
7.5 Mecanismo de una red con nodos DPI	6
8 Representación de los métodos DPI – Regla política de DPI-PIB	6
8.1 Aspectos generales	6
8.2 Método de representación de datos y mascara para las condiciones de la regla política de DPI	6
8.3 Método de representación de expresión regular para las condiciones de la regla política de DPI	7
8.4 Método de representación híbrida para las condiciones de la regla política de DPI	7
9 Flujos de información, procedimientos de procesamiento y métodos para una entidad DPI	8
9.1 Aspectos generales	8
9.2 Creación de interfaces	8
9.3 Flujo de información	9
9.4 Procedimiento de procesamiento	12
9.5 Método de protección	13
9.6 Método de sincronización de datos	13
10 Especificación del mecanismo operativo	14
10.1 Aspectos generales	14
10.2 Objetivos del mecanismo operativo	15
10.3 Rendimiento o implantación de nodos DPI	15
10.4 Análisis de las redes actuales	15
10.5 Confirmación del requisito DPI de la red	15
10.6 Elección de las entidades o sistemas DPI adecuados	16

	Página
10.7	Reconstrucción de la red actual con DPI..... 16
10.8	Supervisión y gestión de la red con DPI 16
10.9	Reconstrucción de la red con DPI en función de la supervisión del rendimiento..... 16
11	Especificación del mecanismo de gestión 16
11.1	Aspectos generales de la gestión de una red DPI..... 16
11.2	Interfaz de gestión 18
11.3	Protocolo y funciones de gestión..... 19
12	Consideraciones relativas a la seguridad 19
	Bibliografía 20

Recomendación UIT-T Y.2772

Mecanismos para los elementos de red con apoyo de la inspección detallada de paquetes

1 Alcance

En esta Recomendación UIT-T se presentan los mecanismos de aplicación de la inspección detallada de paquetes (DPI) en las redes de paquetes. Su principal objetivo es describir los modelos de aplicación, los protocolos conexos, las interfaces y los métodos de procedimiento y procesamiento de la DPI que pueden utilizarse para identificar flujos de información entre las funciones DPI y otras funciones de red.

La presente Recomendación contiene:

- la definición del mecanismo DPI;
- un repaso de los mecanismos DPI en apoyo de la identificación de aplicaciones;
- los procedimientos y flujos de información desde el punto de vista operativo;
- los procedimientos y flujos de información desde el punto de vista de la gestión, como la gestión de política DPI;
- otros procedimientos y flujos de información para posibles interfaces de entidad funcional (FE) DPI.

Quedan fuera del alcance de la presente Recomendación:

- los aspectos operativos y de gestión no específicos de las entidades DPI;
- las funciones de gestión relacionadas con los elementos comunes de red, pues ya se especifican en las Series M y X de Recomendaciones UIT-T.

Los ingenieros y usuarios de las técnicas descritas deberán cumplir la legislación, los reglamentos y las políticas nacionales y regionales aplicables. El mecanismo descrito en la presente Recomendación quizá no sea aplicable a la correspondencia internacional si se desea garantizar el cumplimiento de los requisitos jurídicos nacionales en materia de confidencialidad y soberanía aplicables a las telecomunicaciones y la Constitución y el Convenio de la UIT.

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.

- [UIT-T Y.2111] Recomendación UIT-T Y.2111 (2011), *Funciones de control de recursos y admisión en las redes de próxima generación.*
- [UIT-T Y.2704] Recomendación UIT-T Y.2704 (2010), *Mecanismos y procedimientos de seguridad en las redes de próxima generación.*
- [UIT-T Y.2770] Recomendación UIT-T Y.2770 (2012), *Requisitos para la inspección detallada de paquetes en las redes de la próxima generación.*
- [UIT-T Y.2771] Recomendación UIT-T Y.2771 (2014), *Marco para la inspección detallada de paquetes.*

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 inspección detallada de paquetes (DPI) [UIT-T Y.2770]: análisis, con arreglo a la arquitectura de protocolo por capas OSI-BRM [b-ITU-T X.200], de

- las propiedades de la carga útil y/o los paquetes (véase la lista de posibles propiedades en la cláusula 3.2.11/[UIT-T Y.2770]) para información de encabezamiento más profunda que las capas de protocolo 2, 3 ó 4 (L2/L3/L4);
- otras propiedades de los paquetes,

con el fin de identificar inequívocamente la aplicación.

NOTA – El resultado de la función DPI, junto con otra información adicional como la relativa al flujo, se suele utilizar en funciones posteriores, tales como las de notificación o acciones sobre los paquetes.

3.1.2 analizador DPI [UIT-T Y.2771]: una entidad subsiguiente en el trayecto de procesamiento DPI (que pertenece a la función de aplicación de políticas DPI) especializada en funciones de comparación entre los encabezamientos de paquetes concretos y cargas útiles de los flujos de paquetes preseleccionados. El principal ámbito de aplicación del analizador DPI está relacionado con la evaluación de las *condiciones* de política DPI respecto de los paquetes entrantes *preseleccionados*.

NOTA – El analizador DPI puede estar situado después del escáner DPI (véase la cláusula 3.2.5 [UIT-T Y.2771]). Además, puede ejercer la función de analizador del sistema de detección de intrusión (SDI).

3.1.3 motor DPI [UIT-T Y.2770]: subcomponente y parte central de la entidad funcional DPI que realiza todas las funciones de procesamiento de paquetes (por ejemplo, identificación de paquetes y otras funciones de procesamiento de paquetes de la Figura 6-1/[UIT-T Y.2770]).

3.1.4 nodo DPI [UIT-T Y.2771]: elemento o dispositivo de red que realiza funciones relacionadas con la DPI. Se trata de un término genérico para designar la materialización de una entidad física DPI.

NOTA – Perspectiva funcional: la función nodo DPI (DPI-NF) consta de la función de aplicación de políticas DPI (DPI-PEF) y la función de decisión de política local (opcional) (L-PDF), por lo que la DPI-NF es funcionalmente equivalente a la entidad funcional DPI.

3.1.5 acción de política DPI (acción en forma abreviada) [UIT-T Y.2771]: Define cómo aplicar una regla política cuando se cumplen las condiciones de dicha regla. Las acciones de política pueden dar lugar a la ejecución de una o varias operaciones que afectan y/o configuran el tráfico y los recursos de red, véase también [b-IETF RFC 3198].

3.1.6 condición de política DPI (también denominada *signatura (DPI)*) [UIT-T Y.2770]: representación del estado y/o prerequisites necesarios que identifican una aplicación y definen si deben realizarse las acciones de una regla política. El conjunto de condiciones de política DPI relacionadas con una regla política específica cuándo ésta es aplicable (véase también [b-IETF RFC 3198]).

Las condiciones de política DPI deben contener condiciones a nivel de aplicación y quizá otras opciones tales como condiciones de estado y/o condiciones a nivel de flujo:

- 1) Condición de estado (facultativo):
 - a) grado de condiciones de servicio en la red (por ejemplo, congestión experimentada en trayectos de paquetes); o
 - b) situación del elemento de red (por ejemplo, condición de sobrecarga local de DPI-FE).

- 2) Descriptor del flujo/condiciones a nivel de flujo (facultativo):
 - a) contenido del paquete (campos de encabezamiento);
 - b) características del paquete (por ejemplo, número de etiquetas MPLS);
 - c) tratamiento del paquete (por ejemplo, interfaz de salida del DPI-FE).
- 3) Descriptor de la aplicación/condiciones a nivel de aplicación:
 - a) contenido del paquete (campos del encabezamiento de la aplicación y carga útil de la aplicación).

NOTA – La condición está relacionada con la "condición simple" en las descripciones formales de las condiciones a nivel de flujo y a nivel de aplicación.

3.1.7 escáner DPI (también denominada "función de escáner DPI") [UIT-T Y.2771]: la primer entidad en el trayecto de procesamiento DPI (dentro de una función de aplicación de políticas DPI) que realiza una preselección (relacionada con el analizador DPI ulterior, véase la cláusula 3.2.8) tras verificar *todas* las *condiciones* de política DPI para *todos* los paquetes entrantes.

3.2 Términos definidos en la presente Recomendación

Ninguno.

4 Siglas y acrónimos

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

BRAS	Servidor de acceso a banda ancha a distancia (<i>broadband remote access server</i>)
CLI	Interfaz de línea de comando (<i>command line interface</i>)
CMIP	Protocolo común de información de gestión (<i>common management information protocol</i>)
DPI	Inspección detallada de paquetes (<i>deep packet inspection</i>)
DPI-PDFE	Entidad funcional de decisión política DPI (<i>DPI policy decision functional entity</i>)
DPI-PIB	Base de información de política DPI (<i>DPI policy information base</i>)
EMS	Sistema de gestión de elementos (<i>element management system</i>)
GUI	Interfaz gráfica de usuario (<i>graphical user interface</i>)
IP	Protocolo Internet (<i>Internet protocol</i>)
IPFIX	Exportación de información sobre el flujo IP (<i>IP flow information export</i>)
LAN	Red de área local (<i>local area network</i>)
L-PDF	PDF local (<i>local PDF</i>)
NMS	Sistema de gestión de red (<i>network management system</i>)
OAM	Operación, administración y gestión (<i>operation, administration and management</i>)
PDF	Función de decisión de política (<i>policy decision function</i>)
PIB	Base de información de política (<i>policy information base</i>)
SNMP	Protocolo simple de gestión de red (<i>simple network management protocol</i>)
SR	Encaminador de servicio (<i>service router</i>)
TCAM	Memoria ternaria de contenido direccionable (<i>ternary content-addressable memory</i>)

TCP	Protocolo de control de transmisión (<i>transmission control protocol</i>)
UDP	Protocolo de datagrama de usuario (<i>user datagram protocol</i>)
VLAN	Red de área local virtual (<i>virtual local area network</i>)

5 Convenios

Ninguno.

6 Definición del mecanismo DPI

En esta Recomendación se considera que el término "mecanismo" comprende los medios, métodos, procesos y procedimientos necesarios para realizar una función y cumplir un requisito. Habida cuenta de esa premisa, un mecanismo DPI puede describirse de la siguiente manera:

- Proceso concreto que puede utilizarse para realizar las funciones y capacidades definidas en [UIT-T Y.2771] y cumplir los requisitos definidos en [UIT-T Y.2770].
- Procedimiento detallado que puede adoptarse para realizar las funciones y capacidades definidas en [UIT-T Y.2771] y cumplir los requisitos definidos en [UIT-T Y.2770].
- Métodos adecuados que pueden emplearse para efectuar las funciones y capacidades definidas en [UIT-T Y.2771] y cumplir los requisitos definidos en [UIT-T Y.2770].
- Herramientas o medios especializados que pueden ayudar en la ejecución de las funciones y capacidades definidas en [UIT-T Y.2771] y el cumplimiento de los requisitos definidos en [UIT-T Y.2770].

7 Repaso de los mecanismos DPI en apoyo de la identificación de aplicaciones

7.1 Aspectos generales de los mecanismos DPI

Los mecanismos DPI tienen dos aspectos principales:

- mecanismos DPI en relación con el nodo DPI;
- mecanismos DPI correspondientes a la red que soporta las funciones DPI.

Antes de especificar esos dos aspectos, es necesario presentar la estructura básica del nodo DPI y la red típica que soporta las funciones DPI.

7.2 Estructura básica de un nodo DPI

En la Figura 6-1 de [UIT-T Y.2770] y la Figura 7-2 de [UIT-T Y.2771] se describe la estructura básica de un nodo DPI. Un nodo DPI real puede basarse en esta estructura.

7.3 Red típica que soporta funciones DPI

En la Figura 7-1 se describe una red típica con nodos DPI, donde, de arriba a abajo, las cinco capas lógicas son: nube, capa núcleo, capa combinada, capa de acceso y capa terminal. Cabe señalar que existe un enlace lógico entre cada nodo DPI y el sistema de gestión de elementos (EMS) o el sistema de gestión de red (NMS), aunque en la Figura 7-1 no se muestran todos los enlaces lógicos. Todos los nodos DPI puede cooperar con las entidades de red (como el encaminador, el conmutador y el servidor de acceso a banda ancha a distancia (BRAS), etc.) y los nodos DPI de la Figura 7-1 son independientes de esas entidades de red.

7.5 Mecanismo de una red con nodos DPI

El mecanismo correspondiente a las redes que soportan funciones DPI consiste básicamente en lo siguiente:

- aspectos operativos;
- aspectos de gestión.

8 Representación de los métodos DPI – Regla política de DPI-PIB

8.1 Aspectos generales

La regla política de DPI de la base de información política de DPI (DPI-PIB) es una de las partes fundamentales de un nodo DPI y casi todas las acciones del nodo DPI se basan en las condiciones fijadas por la regla política de DPI. Por consiguiente, es muy importante que la regla política de DPI se represente efectivamente y sea fácil de procesar. Se describen tres métodos de representación de las condiciones de la regla política de DPI: método de representación de datos y máscara, método de representación de expresión regular y método de representación híbrida.

8.2 Método de representación de datos y máscara para las condiciones de la regla política de DPI

El método de representación de la dirección IP y la máscara suele utilizarse en la pila de protocolo TCP/IP y los dispositivos de red conexos. El método de representación de datos y máscara es similar al método de representación de dirección IP y máscara. En el método de datos y máscara se utiliza una cadena de bytes (datos) para representar la palabra etiquetada que identifica un determinado flujo de datos, y se utiliza una cadena de bits (máscara) correspondiente a la cadena de bytes para decidir si un determinado bit de la cadena de bytes se ha de verificar o no. Normalmente, si un bit máscara es "1", el correspondiente bit de la cadena de bytes no se verifica. Por el contrario, si un bit máscara es "0", tendrá que verificarse el correspondiente bit de la cadena de bytes.

Para la DPI-PIB conviene utilizar el método de representación de datos y máscara, pues ofrece las siguientes ventajas:

- es sencillo y fácil de utilizar;
- es muy eficiente: muchos flujos de datos pueden compartir un único elemento;
- se ajusta bien a los dispositivos de uso común, como las memorias ternarias de contenido direccionable (TCAM).

Los dos ejemplos siguientes ilustran el método de representación de datos y máscara:

- 1) Ajuste a los flujos de datos cuyo puerto TCP de origen oscile entre 0x2100 y 0x21ff

En la DPI-PIB sólo se necesita un elemento para cumplir el requisito:

Elemento1: datos: 0x2100, máscara: 0x00ff

- 2) Ajuste a los flujos de datos cuya red de área local virtual (VLAN) esté en 16-63

En la DPI-PIB se necesitan dos elementos para cumplir el requisito:

Elemento1: datos: 0x0010, máscara: 0x000f

Elemento2: datos: 0x0020, máscara: 0x001f

8.3 Método de representación de expresión regular para las condiciones de la regla política de DPI

El método de representación de datos y máscara conviene a la representación de una palabra etiquetada con una posición fija y un valor determinado. Normalmente los encabezamientos de protocolo de la capa 2 a la capa 4 (L2-L4) se ajustan muy bien a este tipo de peticiones.

Sin embargo, las palabras etiquetadas de las aplicaciones de capa superior suelen ser inciertas y fáciles de cambiar. En ese caso, resulta difícil utilizar el método de representación de datos y máscara. Para esas aplicaciones resulta más conveniente utilizar para esos tipos de palabras etiquetadas el método de representación de expresión regular.

La expresión regular [b-UIT-T X.680] es un método de descripción muy conocido en informática. Queda fuera del alcance de esta Recomendación analizar y presentar detalladamente las expresiones regulares.

Los dos ejemplos siguientes ilustran el método de representación de expresión regular:

1) Ajuste al flujo de datos que incluya la palabra "Bittorrent" o "Bitcomment"

En la DPI-PIB sólo se necesita un elemento para cumplir el requisito:

Elemento 1: `"/Bit(torrent|comment)/"`

2) Ajuste al flujo de datos que incluya la palabra "Worm" cuando la palabra siguiente no sea "v1" o "v2"

En la DPI-PIB sólo se necesita un elemento para cumplir el requisito:

Elemento 1: `"Worm(?<!v1|v2)"`

8.4 Método de representación híbrida para las condiciones de la regla política de DPI

Las funciones DPI pueden ejecutarse de la capa 2 a la capa 7. Cuando se consideran las capas 2 a 4, la utilización del método de representación de datos y máscara es una buena opción para construir la DPI-PIB. Por otra parte, cuando se considera la utilización de palabras etiquetadas en la capa 7, es más conveniente para construir la DPI-PIB utilizar el método de representación de expresión regular.

Por consiguiente, en muchos entornos de aplicación resulta útil combinar los dos métodos de representación anteriores, obteniéndose lo que se denomina método de representación híbrida. En este método, algunas palabras etiquetadas se representan con el método de representación de datos y máscara, mientras que las otras palabras etiquetadas se representan con el método de representación de expresión regular.

El ejemplo siguiente ilustra el método de representación híbrida:

1) ajuste al flujo de datos que incluya la palabra "Bittorrent" o "Bitcomment" y cuando la VLAN del flujo de datos esté en 8-15

En la DPI-PIB sólo se necesita un elemento para cumplir el requisito:

Elemento1: Primera mitad: datos: 0x0008, máscara: 0x0007

Segunda mitad: `"/Bit(torrent|comment)/"`

Esas dos mitades pueden almacenarse en memorias distintas, pero están lógicamente conectadas la una a la otra.

9 Flujos de información, procedimientos de procesamiento y métodos para una entidad DPI

9.1 Aspectos generales

Una entidad DPI incluye muchas funciones necesarias y su ejecución depende de lo siguiente:

- realización de algunas interfaces necesarias (véase la cláusula 9.2);
- diseño de flujos de información entre componentes funcionales (véase la cláusula 9.3);

- procedimientos de procesamiento de los principales componentes funcionales (véase la cláusula 9.4);
- métodos para reforzar la fiabilidad (véase la cláusula 9.5);
- métodos para intercambiar la información y sincronizar los datos eficazmente (véase la cláusula 9.6);
- otros métodos beneficiosos para la realización de la entidad DPI.

9.2 Creación de interfaces

9.2.1 Aspectos generales de la interfaz

En [UIT-T Y.2770] se definen e ilustran diversas interfaces, incluidas las interfaces externas e1 y e2 y las interfaces internas i1, i2 e i3. Las interfaces externas e1 y e2 se muestran en la Figura 8-1 de [UIT-T Y.2770] y las interfaces internas i1, i2 e i3 se especifican en la Figura 8-2 de [UIT-T Y.2770]. Teóricamente, todas esas interfaces han de estar presentes en un nodo DPI.

Sin embargo, en función de los requisitos de aplicación, puede haber otras interfaces. Por ejemplo, en el contexto de la DPI bidireccional, se puede necesitar que el nodo DPI tenga la interfaz externa especial e3 (véase la Figura 11-4).

9.2.2 Interfaces internas

Las interfaces internas (véase la Figura 8-2 de [UIT-T Y.2770]) se utilizan para intercambiar información entre componentes funcionales internos del nodo DPI. Hay tres interfaces internas: i1, i2 e i3. En las siguientes cláusulas se especifican los detalles de estas interfaces internas.

9.2.2.1 Interfaz i1

La interfaz interna i1 es una interfaz entre la función de identificación de paquetes y otras funciones de procesamiento de paquetes de la DPI-FE. Por norma general, la interfaz i1 es una interfaz física materializada por el hardware a fin de garantizar la capacidad de tratamiento de un nodo DPI. La interfaz i1 puede conseguirse de diversas formas, como la memoria compartida, puertos de comunicación paralelos internos y puertos de comunicación en serie internos, etc.

9.2.2.2 Interfaz i2

La interfaz interna i2 es una interfaz entre la función de identificación de paquetes y la función de gestión local de la DPI-FE. La interfaz i2 es una interfaz lógica materializada por software, que puede diseñarse utilizando diversos métodos.

Si la misma CPU ejecuta, controla o gestiona la función de identificación de paquetes y la función de gestión local, la interfaz i1 puede conseguirse de diversas formas, como un grupo de funciones de interfaz de programación de aplicación (API), memoria compartida y comunicación entre procesos.

Si la función de identificación de paquetes y la función de gestión local están ejecutadas, controladas o gestionadas por distintas CPU, la interfaz i1 puede conseguirse con métodos de comunicación de datos. Por ejemplo, los dos componentes funcionales anteriores pueden intercambiar información a través del TCP o el UDP.

9.2.2.3 Interfaz i3

La interfaz interna i3 es una interfaz entre la biblioteca de firmas DPI y la función de gestión local en la DPI-FE. La interfaz i3 es una interfaz lógica materializada por software. Por norma general, la biblioteca de firmas DPI y la función de gestión local están diseñadas para que las controle una única CPU y la interfaz i3 puede conseguirse con un grupo de funciones API.

9.2.3 Interfaces externas

Las interfaces externas (véase la Figura 8-1 de [UIT-T Y.2770]) se utilizan para intercambiar información entre un nodo DPI y las demás entidades funcionales, como el NMS. También hay tres interfaces externas: e1, e2 y e3. Las interfaces externas e1 y e2 se muestran en la Figura 8-1 de [UIT-T Y.2770] y la interfaz externa e3 se ilustra en la Figura 11-4 de la presente Recomendación. En las cláusulas 9.2.3.1 a 9.2.3.3 se detallan estas interfaces externas.

9.2.3.1 Interfaz e1

La interfaz externa e1 es una interfaz entre una entidad funcional de decisión de política DPI (DPI-PDFE) y una entidad funcional DPI (DPI-FE). En [UIT-T Y.2770] se da una solución para lograr la interfaz: la interfaz e1 puede optativamente ser una interfaz de punto de referencia *Rw*, definida en [UIT-T Y.2111]. Aunque *Rw* es una solución viable, no es la única, ni es obligatoria.

Sea cual sea la solución por la que se opte para diseñar la interfaz e1, se ha de garantizar que los datos transportados por la interfaz son comprensibles tanto para la DPI-PDFE como para la DPI-FE, aun cuando la DPI-PDFE y la DPI-FE no estén diseñadas por el mismo fabricante.

9.2.3.2 Interfaz e2

La interfaz externa e2 es una interfaz entre una DPI-FE y una entidad de red distante distinta de la DPI-PDFE (por ejemplo, un NMS). En [UIT-T Y.2770] se da también una solución para diseñar la interfaz: se recomienda que la interfaz e2 utilice protocolos de exportación basados en la exportación de información de flujo IP (IPFIX, véase [b-IETF RFC 5101]). Aunque la interfaz e2 puede utilizar protocolos de exportación basados en IPFIX, también se puede intercambiar información entre una DPI-FE y entidades de red distantes distintas de la entidad funcional de decisión de política DPI (DPI-PDFE) con otros métodos.

Sea cual sea la solución por la que se opte para diseñar la interfaz e2, se ha de garantizar que la información transmitida por la interfaz es comprensible tanto para la entidad de red distante y la DPI-FE, pertenezcan o no la entidad de red distante y la DPI-FE al mismo fabricante.

9.2.3.3 Interfaz e3

La interfaz e3 es una interfaz entre dos DPI-FE independientes cuando se han de cumplir requisitos de aplicación de DPI bidireccional. En la cláusula 11 se especifica detalladamente esta interfaz.

9.3 Flujo de información

9.3.1 Flujo de información del motor DPI

En la Figura 9-1 se muestra el flujo de información originado desde el motor DPI. El intercambio de datos entre el motor DPI y la función de decisión de política local (L-PDF) se realiza dentro de la entidad DPI, mientras que el intercambio de datos entre la L-PDF y la PD-FE se realiza fuera de la entidad DPI.

El intercambio de datos relacionados con la DPI debe ser muy fiable. Por otra parte, la comunicación de datos dentro de la entidad DPI es más fiable que la comunicación de datos entre dos entidades independientes. Por consiguiente, es mejor utilizar un enfoque basado en la conexión para el intercambio de datos entre dos entidades independientes a fin de garantizar la fiabilidad de ese intercambio. El intercambio de datos dentro de una entidad DPI puede hacerse sin conexión a fin de reducir los recursos de sistema y aumentar la eficacia del intercambio.

Así, en la Figura 9-1, se recomienda diseñar el intercambio de datos entre el motor DPI y la L-PDF en modo sin conexión, porque el motor DPI y la L-PDF se encuentran en una sola entidad DPI. Sin embargo, se recomienda diseñar el intercambio de datos entre la L-PDF y la PD-EF en modo con conexión, porque la PD-FE no está en la misma entidad DPI.

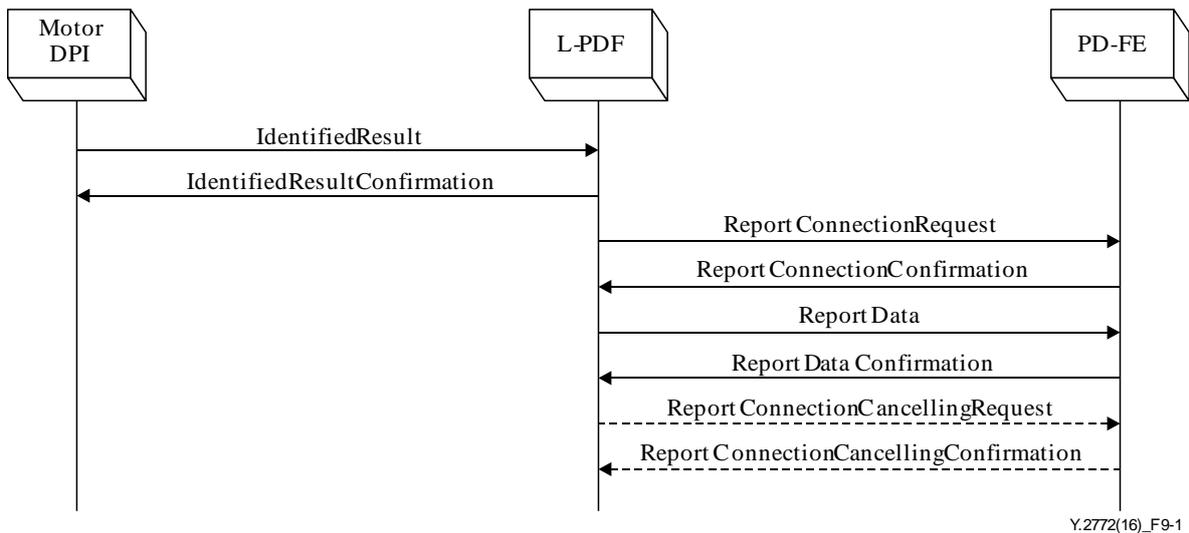


Figura 9-1 – Flujo de información del motor DPI

En la Figura 9-1, la primitiva "Identified Result" se utiliza para transportar datos generados por un motor DPI y la primitiva "Identified Result Confirmation" se utiliza para decir al motor DPI que se han recibido los datos anteriores. La pareja de primitivas "Report Connection Request" y "Report Connection Confirmation" se utiliza para establecer una conexión, y la pareja de primitivas "Report Data" y "Report Data Confirmation" se emplea para transportar los datos comunicados. Una vez finalizado el intercambio de todos los datos comunicados, la pareja de primitivas "Report Connection Cancelling Request" y "Report Connection Cancelling Confirmation" se puede utilizar para eliminar la conexión (representada por la línea discontinua en la Figura 9-1).

9.3.2 Flujo de información de la DPI-PIB

En la Figura 9-2 se muestra el flujo de información de la DPI-PIB. El intercambio de datos entre la DPI-PIB y la L-PDF se realiza dentro de la entidad DPI, y el intercambio de datos entre la L-PDF y la PD-FE se realiza fuera de la entidad DPI.

En la Figura 9-2, se recomienda diseñar el intercambio de datos entre la DPI-PIB y la L-PDF en modo sin conexión, y el intercambio de datos entre la L-PDF y la PD-EF en modo con conexión.

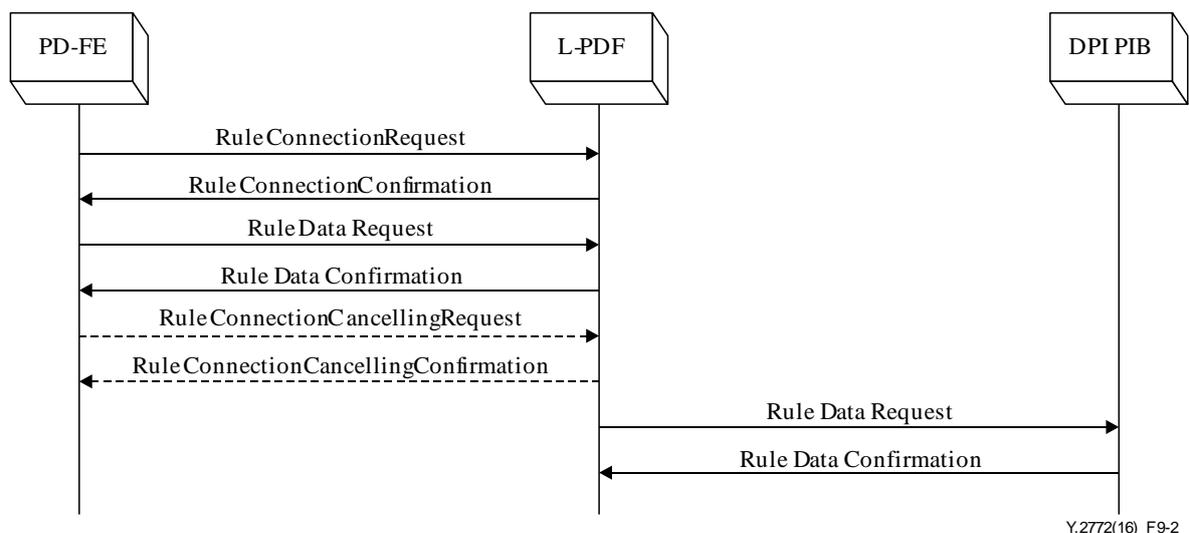


Figura 9-2 – Flujo de información de la DPI-PIB

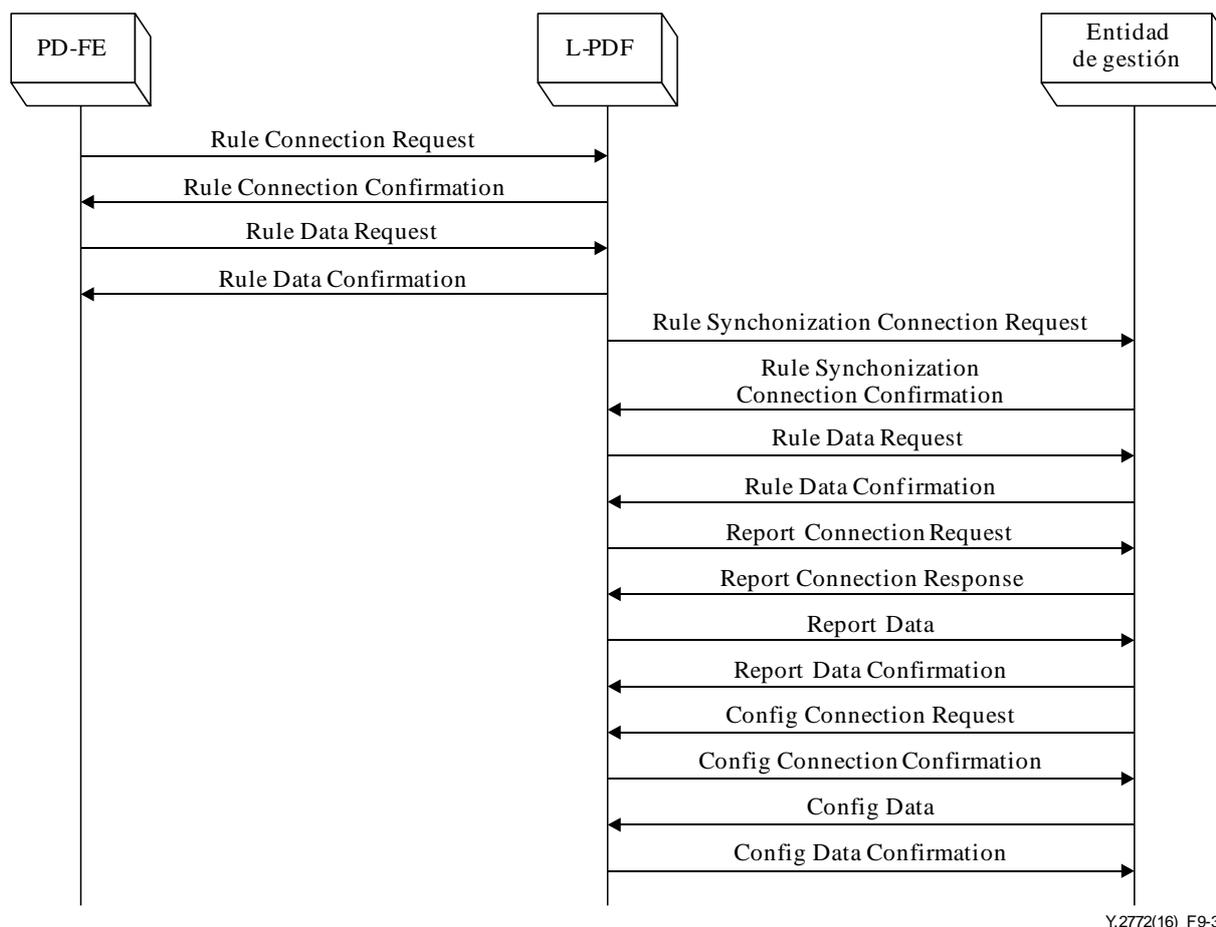
En la Figura 9-2, la pareja de primitivas "Rule Connection Request" y "Rule Connection Confirmation" se utiliza para establecer una conexión, y la pareja de primitivas "Rule Data Request" y "Rule Data Confirmation" para transportar los datos normativos. Una vez finalizado el intercambio de todos los datos normativos, se puede utilizar la pareja de primitivas "Rule Connection Cancelling Request" y "Rule Connection Cancelling Confirmation" para eliminar la conexión (representada por la línea discontinua en la Figura 9-2)

9.3.3 Flujo de información de la DPI L-PDF

En la Figura 9-3 se muestra el flujo de información de la DPI L-PDF. Tanto el intercambio de datos entre la L-PDF y la PD-FE como el intercambio de datos entre la L-PDF y la entidad de gestión se realizan fuera de la entidad DPI.

En la Figura 9-3, de entre los tres componentes funcionales, la PD-FE, la L-PDF y la entidad de gestión, no hay dos que pertenezcan a la misma entidad. Por consiguiente, se recomienda diseñar el intercambio de datos mutuo en modo con conexión.

En la Figura 9-3 se utilizan cuatro parejas de primitivas ("Rule Connection Request" y "Rule Connection Confirmation", "Rule Synchronization Connection Request" y "Rule synchronization Connection Confirmation", "Report Connection Request" y "Report Connection Confirmation", y "Config Connection Request" y "Config Connection Confirmation") para establecer la conexión correspondiente. Por otra parte, se utilizan otras cuatro parejas de primitivas ("Rule Data Request" y "Rule Data Confirmation", "Rule Data Request" y "Rule data Confirmation", "Report Data Request" y "Report Data Confirmation", y "Config Data Request" y "Config Data Confirmation") para transportar los datos correspondientes. Además, para cada tipo de conexión, una vez finalizado el intercambio de todos los datos correspondientes, puede utilizarse la pareja de primitivas "... Connection Cancelling Request" y "... Connection Cancelling Confirmation" para eliminar la conexión. Esta última pareja de primitivas no aparece en la Figura 9-3 para limitar su complejidad y evitar confusiones, aunque su función es similar a la de la pareja de primitivas "Rule Connection Cancelling Request" y "Rule Connection Cancelling Confirmation".



Y.2772(16)_F9-3

Figure 9-3 – Flujo de información de la L-PDF

9.4 Procedimiento de procesamiento

9.4.1 Procedimiento de procesamiento del motor DPI

Cuando un paquete entra en el motor DPI, éste lo escanea e identifica el paquete en función de la regla política definida en la DPI-PIB. A continuación, el analizador del motor DPI analiza el paquete identificado y registra el resultado del análisis. Posteriormente se ejecutará la acción política que corresponda a ese resultado.

Si no se identifica el paquete, se ejecutará la acción 'no identificado'. Si se identifica el paquete, el motor DPI ejecutará la acción que corresponda en función de la regla política definida en la DPI-PIB.

Por otra parte, el motor DPI registra el resultado obtenido para cada paquete y agrupa los resultados similares. Comunica los resultados a la entidad de gestión periódicamente. El periodo de informe depende de cada aplicación y queda fuera del alcance de esta Recomendación.

9.4.2 Procedimiento de procesamiento de la DPI-PIB

La DPI-PIB contiene una o varias reglas políticas de DPI. La DPI-PIB recibe los datos normativos de la L-PDF después de que la L-PDF los haya recibido de la PD-FE.

9.4.3 Procedimiento de procesamiento de la L-PDF

La L-PDF actualiza las entradas normativas para la DPI-PIB cuando recibe los datos normativos de las funciones de decisión política distantes (PDF). La L-PDF envía el resultado identificado a las PDF distantes cuando los recibe del motor DPI. La L-PDF puede también encargarse de resolver los problemas de interacción de reglas entre el conjunto de reglas de política DPI.

9.5 Método de protección

En [UIT-T Y.2771] se define el grupo de redundancia "1+N" para la tolerancia a fallos. Hay dos modelos de protección diferentes: el modelo "1+1" (N=1) y el modelo "1+N" (N>1). El modelo "1+1" se utiliza para un componente activo y un componente en reposo, mientras que el modelo "1+N" (N>1) se emplea para un componente activo y N componentes en reposo.

9.5.1 Modelo "1+1"

El modelo "1+1", también denominado modelo activo/en reposo, es un tipo de modelo de cambio en caso de fallo en el que, en caso de fallo, un componente en reposo libre asume el papel del componente en fallo. Según este modelo, el componente en reposo utiliza un detector de pulso para detectar el fallo del componente activo. El nivel de alta disponibilidad depende de la estrategia de replicación de componentes. Con el modelo activo/en reserva se recomienda utilizar una solución de reserva en caliente (utilización inmediata), que ofrece redundancia tanto de hardware como de software. Sin embargo, todos los cambios del estado del componente activo se replican en el componente en reserva, es decir, que el estado del componente activo siempre está actualizado. En caso de fallo del componente activo, el componente en reserva lo sustituye y sigue funcionando con el mismo estado.

El estado del componente se copia utilizando la replicación activa. Se utiliza un protocolo de compromiso para anunciar los cambios de estado al componente en reserva antes de que se ejecuten en el componente activo. Una vez ejecutados, el componente en reserva recibe un segundo mensaje para confirmar el cambio de estado. En caso de fallo, el componente en reserva ejecuta todos los cambios de estado no realizados. El protocolo de compromiso es propio de cada aplicación y queda fuera del alcance de esta Recomendación.

El modelo activo/en reserva en caliente ofrece una disponibilidad continua sin interrupción del servicio.

9.5.2 Modelo "1+N" (N>1)

El modelo "1+N" (N>1) se basa en múltiples componentes redundantes y más de dos componentes DPI (es decir, un grupo de redundancia "1+N" DPI cuyos componentes DPI son componentes funcionales), diseñados dentro de un nodo DPI, donde un componente DPI funciona como componente activo, mientras que los demás componentes DPI se mantienen en reserva.

Los procedimientos de procesamiento de este modo son semejantes a los del modelo "1+1". Los componentes en reserva utilizan mensajes de pulso para detectar el fallo del componente activo. Cuando el componente activo falla, uno de los componentes de reserva ocupa su lugar.

9.6 Método de sincronización de datos

Se ha de considerar la sincronización de datos en caso de conmutación de protección. Se recomienda que los componentes funcionales activos y los de reserva mantengan información completamente idéntica, como la base de datos (PIB), mediante el método de sincronización de datos.

9.6.1 Sincronización de datos en modo "1+1"

En caso de que el componente activo (incluidos el nodo DPI, el motor DPI y la DPI-FE) falle, el componente de reserva asume las funciones del componente activo. El componente de reserva debe enviar una '*Rule Synchronization Request*' a la entidad de gestión. La entidad de gestión enviará los datos normativos al componente de reserva.

9.6.2 Sincronización de datos en modo "1+N" (N>1) a nivel de componente

La sincronización de datos a nivel de componente en modo "1+N" es similar a la del modo "1+1". En caso de que el componente activo (incluidos el nodo DPI, el motor, DPI y la DPI-FE) falle, el

componente de reserva asume las funciones del componente activo. El componente de reserva debe enviar una *'Rule Synchronization Request'* a la entidad de gestión. La entidad de gestión enviará los datos normativos al componente de reserva.

9.6.3 sincronización de datos en modo "1+N" (N>1) a nivel de nodo

El modo "1+N" (N>1) a nivel de nodo se consigue en modo grupo, donde, si el nodo maestro falla, el nodo de reserva asume las funciones del nodo maestro. El nodo de reserva sincronizará los datos normativos de la entidad de gestión.

En caso de fallo del nodo subordinado, el tráfico pasado al nodo en fallo se redistribuirá a los demás nodos subordinados mediante encaminadores ascendentes gracias a un algoritmo de equilibrio de la carga. Estos nodos subordinados se activarán para sincronizar las nuevas reglas de la entidad de gestión.

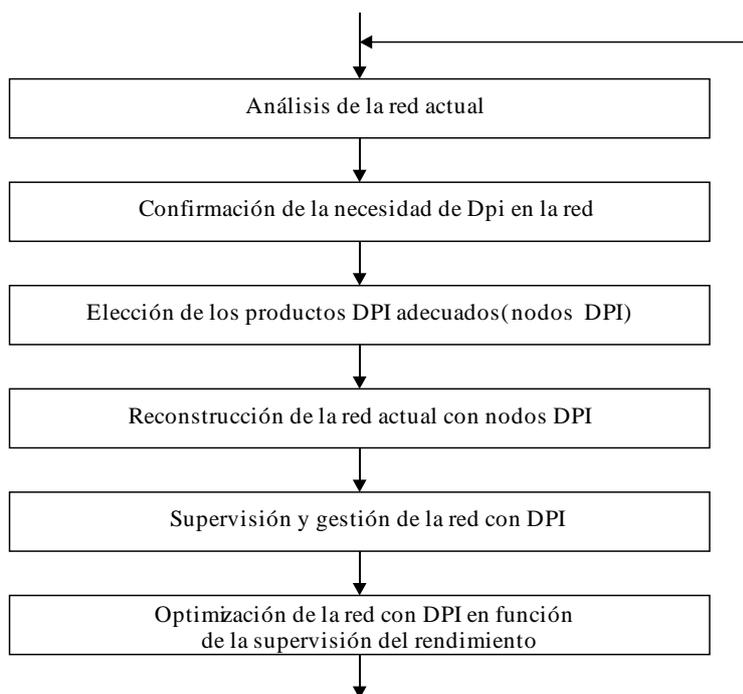
10 Especificación del mecanismo operativo

10.1 Aspectos generales

En esta cláusula se describen los aspectos operativos de las tecnologías DPI, incluidos los siguientes:

- metas de la tecnología DPI adoptada;
- aspectos de rendimiento del sistema DPI implantado;
- análisis de las redes actuales sin DPI;
- implantación de entidades físicas DPI y configuración de las redes conexas;
- funcionamiento, administración y mantenimiento de las redes DPI conexas;
- modificación y mejora de las redes actuales en función de la calidad de supervisión de las redes actuales.

En la Figura 10-1 se muestra el proceso general de construcción y explotación de una red con nodos DPI. Las funciones de las seis fases indicadas en la figura se describen en las cláusulas 10.3 a 10.8.



Y.2772(15)_F10-1

Figura 10-1 – Ilustración del proceso de construcción y explotación de una red con nodos DPI

10.2 Objetivos del mecanismo operativo

10.2.1 Objetivo general

Los objetivos generales para utilizar tecnologías DPI comprenden los tres siguientes:

- 1) supervisar del estado de la red actual;
- 2) encargar a los operadores la reconstrucción y optimización de la red;
- 3) mejorar el rendimiento de la red.

10.2.2 Objetivos específicos

Los objetivos específicos del mecanismo operativo son los siguientes:

- implantación de nodos DPI sin afectar al servicio en línea actual;
- supervisión de todos los tipos de tráfico de la red activa;
- identificación del tráfico inválido definido en las reglas políticas;
- análisis del estado de la red en función de una supervisión detallada del rendimiento de la red;
- reatribución de recursos de red en función del análisis del estado de la red;
- reconstrucción y mejora de la red en función de su estado;
- aumento de la satisfacción de los usuarios de la red.

10.3 Rendimiento o implantación de nodos DPI

En principio, la implantación de nodos DPI no debe interrumpir los servicios y aplicaciones de la red en curso. Sin embargo, en la práctica, durante la instalación de un nodo DPI en la red, los servicios y aplicaciones de la red pueden verse negativamente afectados. Una vez terminada la instalación, la influencia negativa de la implantación del nodo DPI se ajustará a requisitos especiales.

10.3.1 Especificación de la implantación de nodos DPI fuera del trayecto

Durante la inserción en la red de un nodo DPI fuera del trayecto, la interrupción de los servicios y aplicaciones en curso en la red será inferior a 50 milisegundos. En teoría, es posible implantar nodos DPI fuera del trayecto sin interrumpir los servicios y aplicaciones.

10.3.2 Especificación de la implantación de nodos DPI en el trayecto

Durante la inserción en la red de un nodo DPI en el trayecto, la interrupción de los servicios y aplicaciones en curso en la red será inferior a 50 milisegundos. Si se utilizan métodos o instrumentos auxiliares, es posible cumplir el objetivo de 50 milisegundos. Por ejemplo, se puede utilizar un enlace redundante antes de implantar el nodo DPI en el trayecto y suprimir dicho enlace cuando el nodo DPI en el trayecto pueda trabajar con normalidad.

10.4 Análisis de las redes actuales

Antes de implantar un nodo DPI se ha de tener cierta información sobre la red actual, como, por ejemplo, el ancho de banda máximo de todos los segmentos de la red, el tráfico medio activo de los segmentos de red, la distribución del tráfico de los segmentos de red en función de la fecha y la hora, y el grado de influencia durante la implantación del nodo DPI. Normalmente el NMS de la red puede obtener esta información.

Analizando esa información se puede diseñar el plan de construcción de una red con funciones DPI.

10.5 Confirmación del requisito DPI de la red

Se ha de conocer y confirmar la necesidad de un nodo DPI a partir del anterior análisis de la red.

10.6 Elección de las entidades o sistemas DPI adecuados

Las entidades DPI utilizadas para construir la red con funciones DPI debe ajustarse al requisito descrito en la cláusula 10.4.

10.7 Reconstrucción de la red actual con DPI

La implantación de dispositivos DPI no debe reducir el rendimiento de la red actual y, en particular, no se ha de ver afectado el servicio en línea. Resulta más fácil implantar las entidades físicas DPI fuera del trayecto que las entidades físicas DPI en el trayecto, aunque se pueden efectuar operaciones impropias para influir en el servicio. Por consiguiente, se han de seleccionar el tiempo y la ubicación adecuados a fin de minimizar esa influencia, y tal selección dependerá del tráfico en línea de la red.

Hay que subrayar que los nodos DPI deben soportar una función de evitación interna cuando se implantan en la red y que funciona como un nodo DPI en el trayecto. En la Figura 10-2 se muestra la función de evitación interna, representada por la línea discontinua. El paso de un flujo de paquetes por esa circunvalación equivale a que el nodo no esté en la red. Dicho de otro modo, desde el punto de vista del flujo de paquetes, el dispositivo de red anterior al nodo DPI se conecta directamente al dispositivo de red posterior al nodo DPI.

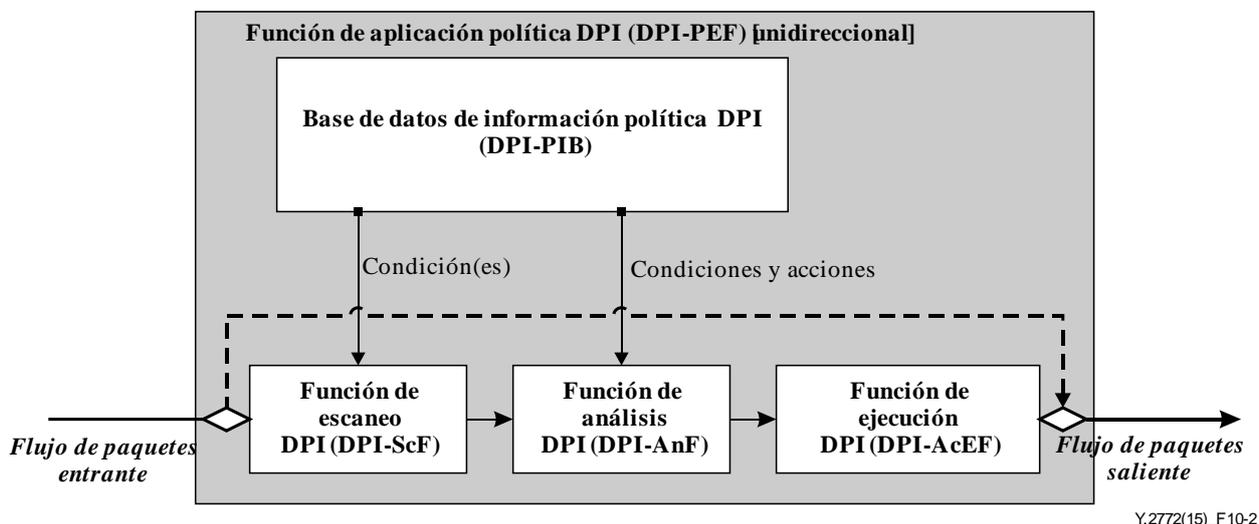


Figura 10-2 – Función de evitación interna de un nodo DPI

10.8 Supervisión y gestión de la red con DPI

En general, las redes con funciones DPI son más complejas que las redes sin funciones DPI. Por consiguiente, una red DPI siempre ha de utilizar la operación, administración y mantenimiento (OAM), es decir, que los nodos DPI y su PIB han de mantenerse y gestionarse.

10.9 Reconstrucción de la red con DPI en función de la supervisión del rendimiento

Por norma general, la construcción de una red con funciones DPI es un proceso adaptativo. La estructura de la red se ha de ir ajustando paulatinamente en función de los cambios en el rendimiento de la red. La supervisión del estado de la red depende de datos y análisis estadísticos adecuados.

11 Especificación del mecanismo de gestión

11.1 Aspectos generales de la gestión de una red DPI

Como cualquier elemento de red típico, un nodo DPI debe soportar las funciones de gestión de configuración, fallos, rendimiento y seguridad. Esas funciones de gestión están definidas en otras Recomendaciones y quedan fuera del alcance de la presente Recomendación. Sin embargo, se presentan aquí algunas consideraciones especiales que se han de tener en cuenta a la hora de gestionar las redes DPI.

En entornos de aplicación DPI bidireccional, las funciones DPI bidireccionales pueden realizarse con un único nodo DPI (modo nodo único, véase la Figura 11-1) o con un par de nodos DPI (modo nodo doble, véase la Figura 11-2). En muchos casos, el modo nodo doble es más ventajoso que el de nodo único. Por ejemplo, cuando se ha de bloquear tráfico especial, ese tráfico puede bloquearse más pronto si se utiliza el modo nodo doble.

Al ser imposible que dos nodos DPI relacionados sean físicamente independientes, y que la gestión de esos nodos DPI ha de estar unificada, la gestión será más compleja porque, en tales circunstancias, la gestión de red se ha de efectuar a nivel de subred y no a nivel de nodo.

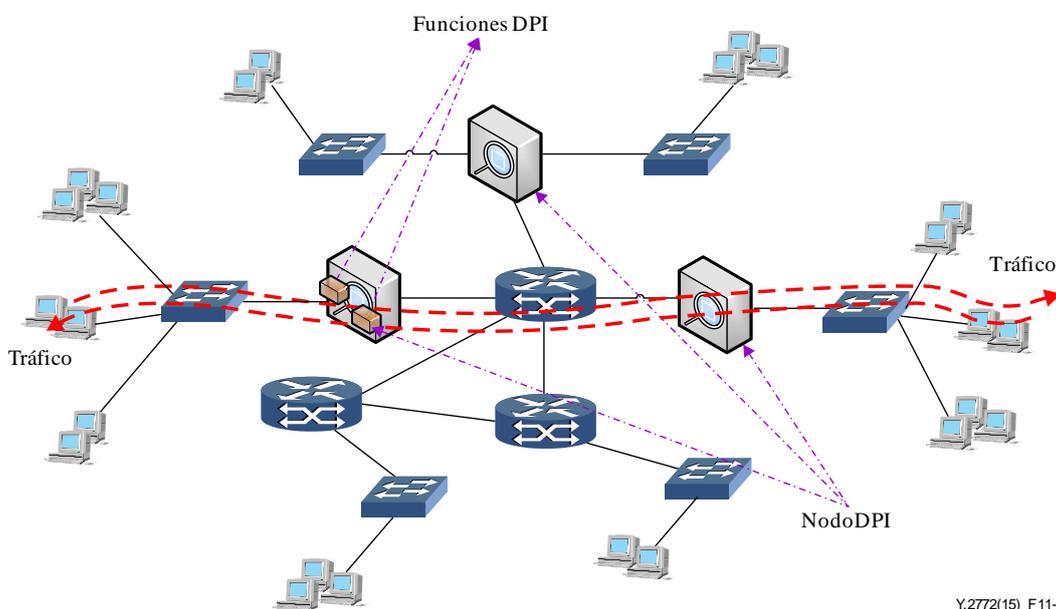


Figura 11-1 – Funciones DPI bidireccionales realizadas por un único nodo DPI (modo nodo único)

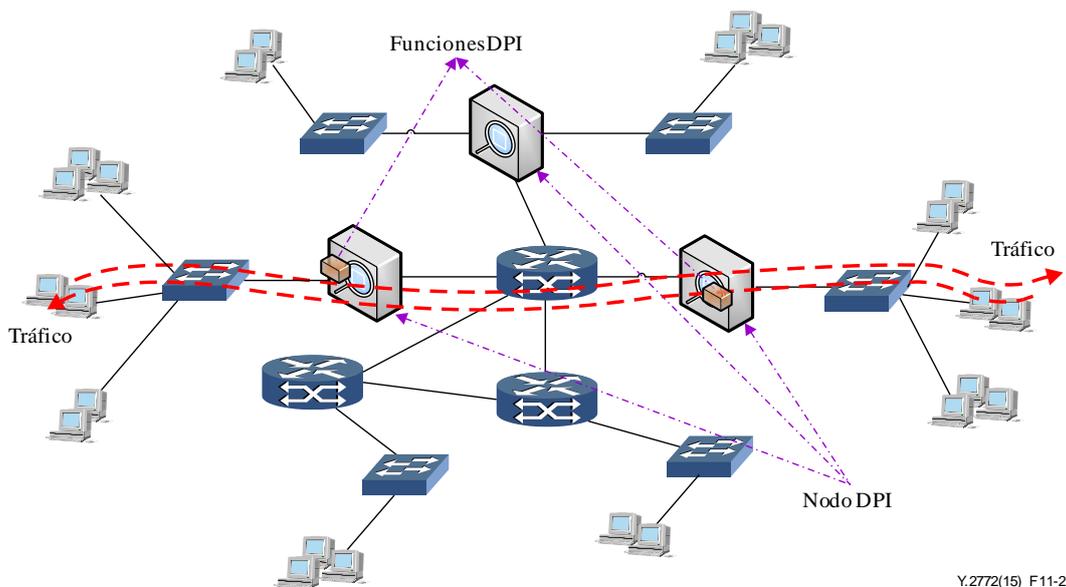


Figura 11-2 – Funciones DPI bidireccionales realizadas por un par de nodos DPI (modo nodo doble)

11.2 Interfaz de gestión

11.2.1 Interfaz de gestión DPI unidireccional

En la Figura 11-3 se muestra la gestión general de la DPI unidireccional, donde la conexión entre un nodo DPI y el sistema de gestión de red (NMS) no es una conexión física directa, sino una conexión lógica a través de una subred. Este enlace entre un nodo DPI y un NMS se representa en la Figura con una línea discontinua. Lógicamente, la interfaz de gestión entre el nodo DPI y el NMS puede describirse de la siguiente manera:

Interfaz de línea comando (CLI): el NMS gestiona y controla el nodo DPI a través de un puerto en serie y la acción de gestión se efectúa con una serie de comandos de una línea. El NMS puede gestionar sólo un nodo DPI en línea a la vez.

Interfaz gráfica de usuario (GUI): el NMS gestiona y controla el nodo DPI a través de un puerto Ethernet o de un puerto físico de otro tipo y la acción de gestión se efectúa mediante el intercambio de un grupo de paquetes de protocolo entre el nodo DPI y el NMS. El NMS puede gestionar uno o más nodos DPI en línea al mismo tiempo.

Interfaz Telnet: el NMS gestiona y controla el nodo DPI a través de un puerto Ethernet o de un puerto físico de otro tipo y la acción de gestión se efectúa con series de comandos de una línea. El NMS puede gestionar sólo un nodo DPI en línea a la vez.

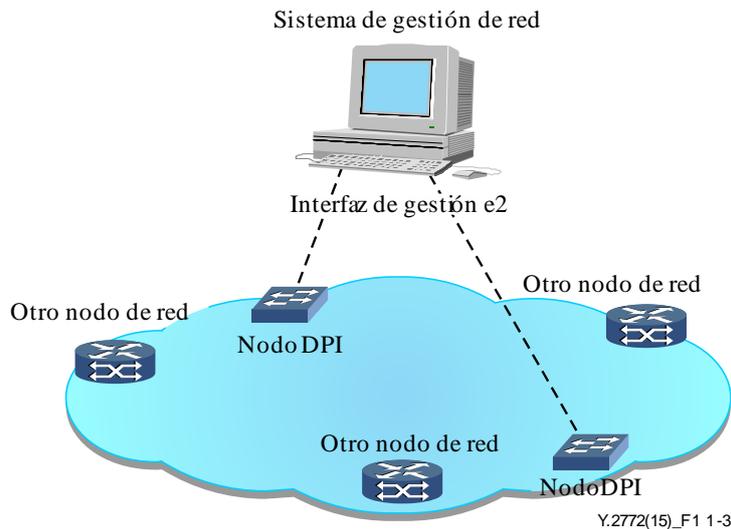


Figure 0-3 – Gestión de red de DPI unidireccional

11.2.2 Interfaz de gestión DPI bidireccional

En la Figura 11-4 se muestra la gestión de la DPI bidireccional. En comparación con la gestión de la DPI unidireccional, la DPI bidireccional (véanse las Figuras 11-1 y 11-2 anteriores) puede ser más compleja porque dos o más nodos DPI son interdependientes. Por tanto, es necesario establecer ciertas conexiones entre dos nodos DPI. Esas conexiones no son necesariamente físicas y directas, sino que pueden ser conexiones a través de una subred o un NMS. Esos enlaces se representan en la Figura 11-4 con una línea discontinua. Además de la interfaz de gestión DPI unidireccional, para la gestión de la DPI bidireccional se han de utilizar las siguientes interfaces de gestión:

Interfaz e3 (véase la Figura 11-2): interfaz entre dos nodos DPI relacionados que se utiliza para garantizar la unidad de la información de los dos nodos DPI y mantener la conexión lógica entre dos nodos DPI relacionados.

Cuando se utiliza la DPI bidireccional resulta más eficaz y económico realizar las funciones DPI bidireccionales mediante la cooperación entre un par de nodos DPI, siendo uno de ellos responsable de la función DPI en un sentido y el otro de la función DPI en el sentido contrario. Por consiguiente, las PIB de los dos nodos DPI han de estar correlacionadas, es decir, que los cambios de la PIB de un nodo deben causar la correspondiente modificación de la PIB del otro nodo DPI.

Por ejemplo, si se han de aplicar funciones DPI bidireccionales al tráfico entre los dispositivos de red A y B, se ha de configurar en un nodo DPI la regla de control política relativa al flujo de A a B y en el otro nodo DPI se ha de configurar la regla de control política relativa al flujo de datos de B a A. Téngase en cuenta que el sistema de gestión de red sólo necesita informar a los nodos DPI de que han de aplicar la función DPI bidireccional al tráfico entre A y B. Los nodos DPI completarán automáticamente la configuración de la PIB de los dos nodos DPI y, por tanto, esos nodos deben poder intercambiar información, lo que se hace a través de la interfaz e3.

Además, para intercambiar información entre los nodos DPI se ha de utilizar algún protocolo que conecte los nodos DPI y los paquetes de datos de protocolo también se comunican por la interfaz e3.

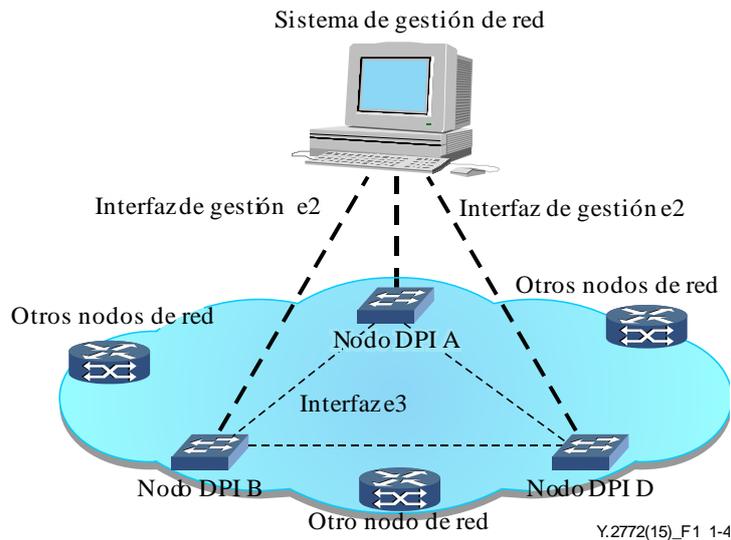


Figura 11-4 – Gestión de red DPI bidireccional

11.3 Protocolo y funciones de gestión

El protocolo de gestión entre el NMS y el nodo DPI o la subred DPI puede ser el protocolo simple de gestión de red (SNMP), el protocolo común de información de gestión (CMIP) o cualquier otro protocolo de gestión.

Las funciones de gestión comprenden la gestión de configuración tradicional, la gestión de alarmas y la gestión de rendimiento. Además, el NMS deberá ejercer la función de mantenimiento de la PIB de la subred DPI.

12 Consideraciones relativas a la seguridad

Los aspectos de la DIP relativos a la reglamentación, la privacidad y la seguridad quedan fuera del alcance de la presente Recomendación. Los fabricantes, operadores y proveedores de servicios tienen que tener en cuenta la reglamentación nacional y los requisitos de política al poner en práctica la presente Recomendación.

Según la ITU-Y.2770, la entidad DPI-FE y la información relativa a las operaciones DPI deben protegerse contra posibles amenazas. Los mecanismos especificados en [UIT-T Y.2704] abordan los requisitos de seguridad de [UIT-T Y.2770].

Bibliografía

- [b-UIT-T X.200] Recomendación UIT-T X.200 (1994), *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico.*
- [b-UIT-T X.680] Recomendación UIT-T X.680 (2015), *Tecnología de la información – Notación de sintaxis abstracta uno: especificación de la notación básica.*
- [b- ITU-T Y-Sup.25] ITU-T Y.2770-series Recommendations – Supplement 25 (2015), *Supplement on DPI use cases and application scenarios.*
- [b-IETF RFC 3198] IETF RFC 3198 (2001), *Terminology for Policy-Based Management.*
- [b-IETF RFC 5101] IETF RFC 5101 (2008), *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information.*

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