Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2771

(07/2014)

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

Redes de la próxima generación – Seguridad

Marco para la inspección detallada de paquetes

Recomendación UIT-T Y.2771

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

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

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

Recomendación UIT-T Y.2771

Marco para la inspección detallada de paquetes

Resumen

En la Recomendación UIT-T Y.2771 se describe un marco para la inspección detallada de paquetes (IDP). El principal objetivo de este marco es describir una estructura para diseñar, definir y aplicar soluciones de IDP que admitan la detección de servicios/aplicaciones con el fin de facilitar la interoperatividad en las redes evolutivas. Este marco servirá para identificar y ayudar a comprender los problemas en la red, principalmente desde el punto de vista de la arquitectura. La presente Recomendación también describe los aspectos del marco IDP relativos a modelos y rendimiento.

El objetivo de estos marcos es sobre todo indicar las posibles relaciones entre la función IDP y otras funciones de red, con el fin de ayudar a definir los requisitos de las funciones IDP (que a su vez dependerá de otras Recomendaciones UIT-T como, por ejemplo Recomendación ITU-T Y.2770) y contribuir al trabajo de terminología (por ejemplo, cuando una definición guarde relación con un modelo funcional).

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T Y.2771	2014-07-18	13	11.1002/1000/12178

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

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de 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/.

ÍNDICE

Recomendación UIT-T Y.2771

Marco para la inspección detallada de paquetes

1 Alcance

La presente Recomendación describe un marco para la inspección detallada de paquetes (IDP) en las redes basadas en paquetes. El principal objetivo de esta Recomendación es describir los conceptos fundamentales, los componentes funcionales y las capacidades de IDP que pueden utilizar las entidades IDP para identificar flujos de información en redes de paquetes, contribuir a la especificación de los requisitos de IDP y dar pautas acerca de soluciones estructuradas para las redes de paquetes (tales como las NGN).

En la presente Recomendación se da información de sistema de alto nivel sobre algunos conceptos fundamentales que suelen ser importantes a la hora de crear entidades IDP. Ahora bien, la finalidad de esta Recomendación no es especificar con todo detalle la IDP, sino aportar información de alto nivel (es decir, un marco) y servir de material de referencia para las Comisiones de Estudio de la UIT y otros grupos de expertos ajenos a la UIT, por ejemplo, a fin de que la tengan en cuenta al elaborar sus normas detalladas sobre funcionalidades IDP.

En la presente Recomendación se describe:

a) los principios arquitectónicos básicos que surgirán al combinar IDP en diversas arquitecturas de red;

b) aspectos relativos a la arquitectura del protocolo desde la perspectiva de la IDP;

c) modelos funcionales de ejemplo y su aplicación a casos de utilización concretos de IDP; y

d) marcos de rendimiento que resulten útiles al examinar el rendimiento de la IDP, tales como la determinación de indicadores fundamentales de rendimiento relativos a la IDP;

Los ingenieros y usuarios de la presente Recomendación UIT-T 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 los operadores de 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.

[ITU-T E.800] Recomendación UIT-T E.800 (2008), *Definiciones de términos relativos a la calidad de servicio*.

[ITU-T G.602] Recomendación UIT-T G.602 (1988), *Fiabilidad y disponibilidad de los sistemas de transmisión analógica por cable y de los equipos conexos*.

[ITU-T H.248.86] Recomendación UIT-T H.248.86 (2014), *Protocolo de control de pasarelas: soporte H.248 para la inspección detallada de paquetes*.

[ITU-T X.200] Recomendación UIT-T X.200 (1994), *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico*.

[ITU-T X.731] Recomendación UIT-T X.731 (1992), *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de estados*.

[ITU-T Y.2704] Recomendación UIT-T Y.2704 (2010), *Mecanismos y procedimientos de seguridad en las redes de próxima generación*.

[ITU-T Y.2770] Recomendación UIT-T Y.2770 (2012), *Requisitos para la inspección detallada de paquetes en las redes de la próxima generación*.

[ETSI TS 132.410] ETSI TS 132 410 (2012), *Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);LTE; Telecommunication management; Key Performance Indicators (KPI) for UMTS and GSM (3GPP TS 32.410 version 11.0.0 Release 11*.

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program Protocol Specification*.

[IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

[IETF RFC 5101] IETF RFC 5101 (2008), *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*.

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 aplicación [ITU-T Y.2770]: puede referirse a lo siguiente:

- un *tipo de protocolo de aplicación* (por ejemplo, los protocolos de aplicación IP de vídeo UIT-T H.264 o el protocolo de inicio de sesión (SIP));
- un tipo de *aplicación del usuario del servicio* (por ejemplo, VoIP, VoLTE, VoIMS, VoNGN, y VoP2P), por ejemplo, "aplicación de voz por paquetes";
- una "aplicación específica del proveedor" de voz por paquetes, (por ejemplo, VoIP de proveedor 3GPP, VoIP de Skype); y
- una aplicación integrada en otra aplicación (por ejemplo, el contenido de aplicación en un elemento de SIP o un mensaje HTTP).

Cada aplicación se identifica mediante un identificador concreto (por ejemplo, un campo de bits, un patrón, una signatura o una expresión ordinaria como "condiciones a nivel de aplicación", véase también la cláusula 3.2.2 de [ITU-T Y.2770]), que es una característica común a todos los niveles de aplicaciones antes enumerados.

3.1.2 disponibilidad [ITU-T E.800]: Disponibilidad de un elemento para hallarse en estado de realizar una función requerida en un instante determinado o en cualquier instante de un intervalo de tiempo dado, suponiendo que se facilitan, si procede, los recursos externos necesarios.

3.1.3 descriptor de la aplicación (también denominado condiciones a nivel de aplicación) [ITU-T Y.2770]: Conjunto de condiciones normativas que identifican la aplicación (conforme a la cláusula 3.2.1 de [ITU-T Y.2770]).

En esta Recomendación se considera el descriptor de aplicaciones como un objeto en general, que es sinónimo de condiciones a nivel de aplicación. No se tiene en cuenta su estructura detallada, por ejemplo la sintaxis, la codificación y el tipo de datos.

3.1.4 inspección detallada de paquetes (IDP) [ITU-T Y.2770]: Análisis, con arreglo a la arquitectura de protocolo por capas OSI-BRM [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 de [ITU-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 IDP, junto con otra información adicional como la relativa al flujo, se suele utilizar en funciones ulteriores, tales como las de notificación o acciones sobre los paquetes.

3.1.5 motor IDP [ITU-T Y.2770]: subcomponente y parte central de la entidad funcional IDP 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 de [ITU-T Y.2770]).

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

Las condiciones de política IDP 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 IDP-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 IDP-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 entidad funcional de decisión política IDP (IDP-PDFE): La función remota respecto de la IDP-FE que decide las reglas basadas en la firma que se aplicarán en la IDP-FE. Algunas funciones de control y/o gestión no tienen por qué ser remota respecto de la IDP-FE.

3.1.8 descriptor del flujo (también denominado condiciones a nivel de flujo) [ITU-T Y.2770]: Conjunto de condiciones de reglas que se utiliza para identificar un determinado tipo de flujo (con arreglo a la cláusula 3.1.3 de [ITU-T Y.2770]) en el tráfico inspeccionado.

NOTA 1 – Esta definición de descriptor del flujo amplía la definición que figura en [b-ITU-T Y.2121] con elementos adicionales, como se describe en la cláusula 3.

NOTA 2 – En el Anexo A de [ITU-T Y.2770] se realiza un escáner normativo del descriptor del flujo con mayor detalle tal como se utiliza en [ITU-T Y.2770].

3.1.9 fiabilidad [ITU-T E.800]: Probabilidad de que una entidad realice la función requerida en unas determinadas condiciones dentro de un intervalo de tiempo dado.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 analizador IDP: Una entidad subsiguiente en el trayecto de procesamiento IDP (que pertenece a la función de aplicación de políticas IDP) 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 IDP está relacionado con la evaluación de las *condiciones* de política IDP respecto de los paquetes entrantes *preseleccionados*.

NOTA – El analizador IDP puede estar situado después del escáner IDP (véase la cláusula 3.2.5). Además, puede ejercer la función de analizador del sistema de detección de intrusión (SDI).

3.2.2 nodo IDP: Elemento o dispositivo de red que realiza funciones relacionadas con la IDP. Se trata de un término genérico para designar la materialización de una entidad física IDP.

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

3.2.3 acción de política IDP (acción en forma abreviada): 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].

3.2.4 función de aplicación de política IDP (IDP-PEF): entidad lógica que aplica decisiones de política, para unas reglas de política IDP dadas.

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

3.2.6 grupo de redundancia IDP "1+N": Grupo de componentes funcionales IDP (por ejemplo, nodo IDP, IDP-PIB, motor IDP, etc.) con una arquitectura de redundancia "1+N" (siendo $N \geq 1$), que consiste en un solo componente nominal y N componentes de protección.

NOTA – El grupo anterior se utiliza para ofrecer mayor fiabilidad y disponibilidad para un nodo IDP o una red que dispone de uno.

4 Siglas y acrónimos

4.1 Siglas y acrónimos generales

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

A_{IDP} Acción de política IDP

BRM Modelo de referencia básico

CAM Memoria de contenido direccionable

C_{IDP} Condición de política IDP

DiffServ Servicio diferencial

DNNF Función de determinación del nodo siguiente

FIB Base de datos de reenvío

FTP Protocolo de transferencia de ficheros

HTTP	Protocolo de transferencia de hipertexto
HW	Hardware
IDA	Identificación detallada de aplicaciones
IDH	Inspección detallada de encabezamientos
IDP	Inspección detallada de paquetes
IDP-AcEF	Función de ejecución de acciones IDP
IDP-AnF	Función de analizador IDP
IDP-FE	Entidad funcional IDP
IDP_{InP}	IDP en el trayecto
IDP-NF	Función nodo IDP
IDP_{OoP}	IDP fuera del trayecto
IDP-PDFE	Entidad funcional de decisión de política IDP
IDP-PE	Entidad física IDP
IDP-PEF	Función de aplicación de políticas IDP
IDP-PIB	Base de datos de políticas IDP
IDP-PIF	Función de identificación de paquetes IDP
IDP-ScF	Función de escáner IDP
IDS	Sistema de detección de intrusiones
IFR	Indicador fundamental de rendimiento
$IFRI_{IDP}$	Indicadores fundamentales de rendimiento para entidades IDP
IP	Protocolo Internet
IPFIX	Exportación de información sobre el flujo IP
L2VPN	Red privada virtual de capa 2
L-PDF	PDF local
LX	Capa X (del protocolo)
LX+	Capa superior a la LX (del protocolo)
L_XHI	Inspección de encabezamientos de la capa X del protocolo
L_XPI	Inspección de carga útil de la capa X del protocolo
MIB	Base de datos de gestión
MPI	Inspección moderada de paquetes
MPLS	Conmutación por etiquetas multiprotocolo
MTBF	Tiempo medio entre fallos
MTTR	Tiempo medio para la reparación
NA(P)T	Traducción de direcciones (y puertos) de red
NGN	Red de la próxima generación
OSI-BRM	Interconexión de sistemas abiertos – Modelo de referencia básico
PDF	Función de decisión política

PEP Punto de aplicación de política

PFF Función de reenvío de paquetes

PIB Base de datos de políticas

QoS Calidad del servicio

RACF Funciones de control de admisión y recursos

R_{IDP} Regla de política IDP

R-PDF PDF remota (es decir, PDF situada a distancia desde la perspectiva del nodo IDP)

RTSP Protocolo de secuenciación en tiempo real

S_D-PDF PDF dependiente de la sesión

SDU Unidad de datos de servicio

SIP Protocolo de inicio de sesión

S_I-PDF PDF independiente de la sesión

SPI Inspección superficial de paquetes

SW Software

TCAM Memoria ternaria de contenido direccionable

TCP Protocolo de control de transmisión

TOS Tipo de servicio

VoIMS Voz por el sistema de medios integrado

VoIP Voz por IP

VoLTE Voz por evolución a largo plazo (*long term evolution*)

VoNGN Voz por red de la próxima generación

VoP2P Voz por transmisión punto a punto

4.2 Símbolos matemáticos

En la presente Recomendación se utilizan los siguientes símbolos (nombre, unidad y breve descripción):

ε_{IDP}	(IDP) tasa de errores	–
$\varepsilon_{f\text{-}n}$	(IDP) tasa de errores de falsos negativos	–
$\varepsilon_{f\text{-}p}$	(IDP) tasa de errores de falsos positivos	–
$\phi_{P,In}$	(IDP) velocidad de procesamiento de paquetes entrantes	[s^{-1}]
$\phi_{P,Out}$	(IDP) velocidad de salida de paquetes	[s^{-1}]
$\phi_{P,Node,Out}$	Caudal de paquetes del nodo	–
$\phi_{P,Identified}$	Velocidad de paquetes identificados correctamente	–
$P_{Hit,BloomFilter}$	Grado de certidumbre de la información de probabilidad	–
Ndb	Número de reglas de política de IDP	–
Sp	Tamaño del paquete	–

N_{IDPeng}	Número de motores IDP	–
τ_{TD}	Retraso de transferencia interna al nodo (del nodo IDP)	[ns]
$\underline{\underline{A}}$	Conjunto de acciones de regla (política IDP)	–
$\underline{\underline{C}}$	Conjunto de condiciones de la regla (política IDP)	–
$\underline{\underline{R}}$	Conjunto de reglas (política IDP)	–

5 Convenios

Ninguno.

6 Marco arquitectónico

6.1 Marco arquitectónico de la red – Casos de red de alto nivel

Este marco describe las principales condiciones de contorno de un despliegue de la IDP en la infraestructura de red. Algunos de los principales casos del marco IDP pueden identificarse considerando criterios tales como:

- **Nivel de ubicación en la red** (es decir, la ubicación de la entidad IDP en un dominio de red por paquetes)
  - en el límite ("**IDP en la frontera**"), o
  - en la red ("**IDP en el núcleo**");
  - entre redes homólogas ("**IDP entre homólogos**").
- **Tipos de paquetes de red (trayecto)** (es decir, el tipo de paquetes que se inspeccionan)[1]
  - plano de usuario (estrato de transporte; por ejemplo, trayecto de datos IP, trayecto de medios IP, trayecto de portadora IP, túnel, MPLS LSR, pseudoalámbrico, etc.), o
  - plano de control (o estrato de servicio; por ejemplo, trayecto de señalización IP), o
  - plano de gestión, o
  - combinaciones.
- **Nivel de armonización con otras arquitecturas de red** (es decir, cómo se acopla la entidad IDP con la arquitectura de red de paquetes subyacente)
  - entidad **IDP aislada** (es decir, la entidad IDP es opaca para la red de paquetes),

    Ejemplos:
    - poquísimas entidades IDP situadas en puntos seleccionados en la red (sin el objetivo de "plena cobertura"; similar a una IDP en el trayecto de tipo sondeo);
    - entidades IDP fuera del trayecto;
  - *red* **IDP solapada** (es decir, existe una infraestructura de red IDP autónoma, superpuesta a la red de paquetes subyacente; las dos infraestructuras de red están separadas desde la perspectiva operativa),

    Ejemplos:
    - ejemplo genérico: una red de entidad IDP en el trayecto que comparten, por ejemplo, los trayectos del plano de usuario, pero emplean interfaces de control y/o gestión separadas;
    - ejemplo específico: por ejemplo, una función IDP para la detección de intrusión;

[1] El concepto de "tipo de paquetes" puede concretizarse al referirse a un "protocolo" o "pila de protocolo" específica. Sin embargo, tal grado de detalle no es necesario en este documento.

– entidad **IDP integrada** (es decir, la entidad funcional IDP está integrada en un elemento de red físico junto con otras entidades funcionales en lo que respecta al procesamiento de paquetes ajeno al IDP; esta entidad física debe contar con, por ejemplo, una sola interfaz OAM desde la perspectiva operativa costoeficiente, lo que implica un modelo de gestión armonizado entre todas las entidades funcionales),

  Ejemplos:

  • ejemplo genérico: una entidad IDP con una base de datos de gestión armonizada con la base de datos de gestión de otras entidades funcionales distintas a la IDP del mismo elemento de red físico;

  • ejemplo concreto: una entidad funcional IDP dentro de una RACF y con capacidad de gestión común, pero que no comparte ninguna interfaz de control RACF;

– **IDP** sistémica (es decir, una entidad IDP "totalmente integrada" en "la red de paquetes"),

  Ejemplos:

  • ejemplo genérico: modelo de referencia de red definido por organizaciones de normalización (arquitectura) teniendo en cuenta las entidades IDP;

  • ejemplo concreto: funciones RACF del UIT-T ampliadas mediante entidades IDP (que pueden utilizar los puntos de referencia existentes (por ejemplo "IDP controlada por *Rw*" o una interfaz *Rw* basada en H.248 ampliada por la [ITU-T H.248.86]) o mediante nuevos puntos de referencia).

Por consiguiente, existen numerosos casos de usuario desde la perspectiva de la integración en la red de una entidad IDP.

6.2 Marco arquitectónico del protocolo – Nivel de inspección de paquetes para algunas aplicaciones de red de ejemplo

6.2.1 Principio

Existen diversos niveles de inspección de paquetes. En el Cuadro 6-1 se muestra una descripción general de las aplicaciones de red típicas en lo que respecta a los "niveles de inspección de paquetes" exigidos. El nivel de inspección de paquetes puede especificarse

1) con arreglo al modelo de referencia básico (MRB) de las arquitecturas de protocolo estratificadas, en este caso columnas L_xHI y L_yPI); o

2) utilizando términos coloquialmente "antiguos" (que se describen en la cláusula 8.1 en [b-ITU-T Y-Sup.23]), en este caso las columnas de inspección superficial de paquetes (SPI), inspección moderada de paquetes (MPI), inspección detallada de encabezamientos (DHI) e inspección detallada de aplicaciones (DAI).

Véase además la cláusula 8 de [b-ITU-T Y-Sup.23] relativa a la IDP en arquitecturas de protocolo estratificadas.

6.2.2 Diferencia entre los casos de IDP y no IDP

Desde la perspectiva de las arquitecturas de protocolo estratificadas, el concepto de IDP es bastante general y comprende todas las capas de protocolo por encima de la capa 1 (véase la cláusula 3.2.5 de [ITU-T Y.2770]). Ahora bien, el ámbito de aplicación de la inspección de paquetes puede limitarse fundamentalmente al caso de aplicaciones de red específicas, principalmente las relacionadas con las capas de enlace, de red y/o de transporte exclusivamente.

Esta limitación está o estaba motivada normalmente por los aspectos históricos, relativos al servicio, y/o relativos a la implementación. Por ejemplo, las decisiones de carácter económico respecto al servicio IDP que puede lograrse con las últimas técnicas. Este tipo de inspección limitada de paquetes es o era conocido como *inspección superficial y moderada de paquetes* (SPI, MPI; véase asimismo la cláusula 8.1 de [b-ITU-T Y-Sup.23]).

Según [ITU-T Y.2770] la distinción de granularidad gruesas entre IDP y no IDP es suficiente, motivo por el cual se utiliza en la presente Recomendación. En este contexto, el concepto de 'IDP' significa reglas de inspecciones de política de poco rigor como las definidas en la presente Recomendación, mientras que 'no IDP' tiene más que ver con la inspección de paquetes tradicional en las capas de protocolo 2, 3 y/o 4 (es decir, SPI, MPI).

6.2.3 Ejemplos

En el Cuadro 6-1 figura una lista de ejemplos de aplicaciones de red con respecto a los niveles de inspección de paquetes, que suelen formar parte de dichas aplicaciones de red. Cabe destacar que las indicaciones que figuran en el Cuadro 6-1 son título de ejemplo y no es necesariamente exhaustivo.

Cuadro 6-1 – Nivel de inspección de paquetes para algunas aplicaciones de red de ejemplo

Aplicación de red (ejemplo)		Nivel de inspección de paquetes				Observaciones
		"Inspección detallada de paquetes" (IDP)				
		(Nota)	"Inspección detallada de encabezamientos" (IDE)		"Identificación detallada de aplicaciones" (DAI)	
			"Inspección moderada de paquetes" (IMP)			
			"Inspección superficial de paquetes" (SPI)			
		Inspección encabez. L2 (L2HI)	Inspección de encabez. L3,4 (L3,4HI)	Inspección de encabez. L4+ (L4+HI)	Inspección de carga útil L7 (L7PI)	
Security:						
1.1	Detección de intrusión en la red	–	**X**	**X**	**X**	Existen varios métodos de ID: a) detección de anomalías b) detección de utilización indebida (aquí)
1.2	Seguridad/Protección de los recursos de red (prevención de intrusión en la red, prevención de ataques de seguridad)	–	**X**	**X**	**X**	
1.3	Otras funciones relacionadas con la seguridad					

Cuadro 6-1 – Nivel de inspección de paquetes para algunas aplicaciones de red de ejemplo

Aplicación de red (ejemplo)		Nivel de inspección de paquetes				Observaciones
		"Inspección detallada de paquetes" (IDP)				
		(Nota)	"Inspección detallada de encabezamientos" (IDE)		"Identificación detallada de aplicaciones" (DAI)	
			"Inspección moderada de paquetes" (IMP)			
			"Inspección superficial de paquetes" (SPI)			
		Inspección encabez. L2 (L2HI)	Inspección de encabez. L3,4 (L3,4HI)	Inspección de encabez. L4+ (L4+HI)	Inspección de carga útil L7 (L7PI)	
Identificación:						
2.1	Abonado, usuario	–	**X**	–	–	Identificado mediante …? (por ejemplo, dirección de red)
2.2	Tipo de aplicación	–	–	**X**	**X**	Identificado mediante …? (por ejemplo, tipo de protocolo de la capa de aplicación)
2.3	Sesión	–	**X**	–	–	Identificado mediante …? (por ejemplo, conexión IP, conexión de transporte IP). Véase también la cláusula 7 en [ITU-T Y-Sup.23]
2.4	Protocolo de control de aplicaciones (por ejemplo, SIP, RTSP, HTTP, FTP, …)	–	**X** [depende del puerto conocido]	**X**	**X**	

Cuadro 6-1 – Nivel de inspección de paquetes para algunas aplicaciones de red de ejemplo

Aplicación de red (ejemplo)		Nivel de inspección de paquetes				Observaciones
		"Inspección detallada de paquetes" (IDP)				
		(Nota)	"Inspección detallada de encabezamientos" (IDE)		"Identificación detallada de aplicaciones" (DAI)	
			"Inspección moderada de paquetes" (IMP)			
			"Inspección superficial de paquetes" (SPI)			
		Inspección encabez. L2 (L2HI)	Inspección de encabez. L3,4 (L3,4HI)	Inspección de encabez. L4+ (L4+HI)	Inspección de carga útil L7 (L7PI)	
Características de los datos de aplicación:						
2.5	Contenido	–	–	X	X	por ejemplo, contenido ilícito
2.6	Tipo de medios (tipo de datos de aplicación)	–	–	X	X	
2.7	Formato de medios	–	–	X	X	
Modificación (de unidades de datos de protocolo):						
3.1	Modificación de 'contenido': Eliminación de virus	–	–	–	X	
3.2	Modificación de 'encabezamiento': marcaje de QoS	–	X	X	–	
3.3	Modificación de encabezamiento y 'contenido': "función ALG"	–	X	X	–	Función NA(P)T local en L3 (y L4) y en la capa de aplicación

Cuadro 6-1 – Nivel de inspección de paquetes para algunas aplicaciones de red de ejemplo

		Nivel de inspección de paquetes				Observaciones
		"Inspección detallada de paquetes" (IDP)				
		(Nota)	"Inspección detallada de encabezamientos" (IDE)		"Identificación detallada de aplicaciones" (DAI)	
			"Inspección moderada de paquetes" (IMP)			
Aplicación de red (ejemplo)			"Inspección superficial de paquetes" (SPI)			
		Inspección encabez. L2 (L2HI)	Inspección de encabez. L3,4 (L3,4HI)	Inspección de encabez. L4+ (L4+HI)	Inspección de carga útil L7 (L7PI)	
Supervisión de parámetros de utilización:						
4.1	Acuerdos sobre el nivel de servicio	–	**X**	**X**	**X**	
4.2	Control de parámetros de tráfico Ejemplos:	–	**X**	**X**	**X**	Dependiente del tipo de parámetros de tráfico
	Política de tasa de bytes L3 (velocidad pico, velocidad sostenida)	–	**X**	–	–	
	Política de tamaño PDU en L3 (mín, máx)	–	**X**	–	–	
	Política de tamaño de ráfaga en L3	–	**X**	–	–	
	Política de tamaño SDU de L7 ("carga útil de aplicación")	–	**X**	**X**	–	
	Política de velocidad de bytes en L7 ("volumen de aplicación")		**X**	**X**	–	

Cuadro 6-1 – Nivel de inspección de paquetes para algunas aplicaciones de red de ejemplo

<table>
<tr><td colspan="2" rowspan="5">Aplicación de red (ejemplo)</td><td colspan="4">Nivel de inspección de paquetes</td><td rowspan="5">Observaciones</td></tr>
<tr><td colspan="4">"Inspección detallada de paquetes" (IDP)</td></tr>
<tr><td>(Nota)</td><td colspan="2">"Inspección detallada de encabezamientos" (IDE)</td><td>"Identificación detallada de aplicaciones" (DAI)</td></tr>
<tr><td></td><td colspan="2">"Inspección moderada de paquetes" (IMP)</td><td></td></tr>
<tr><td></td><td>"Inspección superficial de paquetes" (SPI)</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>Inspección encabez. L2 (L2HI)</td><td>Inspección de encabez. L3,4 (L3,4HI)</td><td>Inspección de encabez. L4+ (L4+HI)</td><td>Inspección de carga útil L7 (L7PI)</td><td></td></tr>
<tr><td colspan="7">Calidad de servicio soportada:</td></tr>
<tr><td>5.1</td><td>Conformación del tráfico</td><td>-</td><td>X</td><td>–</td><td>–</td><td></td></tr>
<tr><td></td><td>Conformación de velocidad de bytes en L3</td><td>–</td><td>X</td><td>–</td><td>–</td><td>Véase por ejemplo [b-ITU-T Y.1221] o [b-ITU-T H.248.53]</td></tr>
<tr><td colspan="7">Análisis de la red:</td></tr>
<tr><td>6.1</td><td>Comportamiento usuario</td><td>–</td><td>X</td><td>X</td><td>X</td><td></td></tr>
<tr><td>6.2</td><td>Patrones de utilización</td><td>–</td><td>X</td><td>X</td><td>X</td><td></td></tr>
<tr><td colspan="7">Medición del rendimiento ("Indicadores fundamentales de rendimiento" (IFR)):</td></tr>
<tr><td>7.1</td><td>Recopilación de mediciones a distancia</td><td>–</td><td>X</td><td>X</td><td>X</td><td></td></tr>
<tr><td>7.2</td><td>Generación de mediciones locales</td><td>–</td><td>X</td><td>X</td><td>X</td><td></td></tr>
</table>

Cuadro 6-1 – Nivel de inspección de paquetes para algunas aplicaciones de red de ejemplo

<table>
<tr><td colspan="2" rowspan="5">Aplicación de red (ejemplo)</td><td colspan="4">Nivel de inspección de paquetes</td><td rowspan="5">Observaciones</td></tr>
<tr><td colspan="4">"Inspección detallada de paquetes" (IDP)</td></tr>
<tr><td>(Nota)</td><td colspan="2" rowspan="2">"Inspección detallada de encabezamientos" (IDE)</td><td rowspan="2">"Identificación detallada de aplicaciones" (DAI)</td></tr>
<tr><td rowspan="2">"Inspección moderada de paquetes" (IMP)</td></tr>
<tr><td>"Inspección superficial de paquetes" (SPI)</td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>Inspección encabez. L2 (L2HI)</td><td>Inspección de encabez. L3,4 (L3,4HI)</td><td>Inspección de encabez. L4+ (L4+HI)</td><td>Inspección de carga útil L7 (L7PI)</td><td></td></tr>
<tr><td colspan="7">Soporte de tasación/facturación:</td></tr>
<tr><td>8.1</td><td>Información basada en el tiempo</td><td>–</td><td>X</td><td>–</td><td>–</td><td></td></tr>
<tr><td>8.2</td><td>Información basada en el volumen de tráfico</td><td>–</td><td>X</td><td>–</td><td>X</td><td>Volumen de tráfico relacionado con la velocidad de bytes IP (L3) y/o datos de la aplicación</td></tr>
<tr><td>8.3</td><td>Información basada en eventos</td><td>–</td><td>X</td><td>X</td><td>X</td><td>Dependiente del tipo de evento (por ejemplo, el evento puede estar relacionado con el contenido)</td></tr>
<tr><td colspan="7">IDP orientada al enlace:</td></tr>
<tr><td>9.1</td><td>Aplicaciones IDP con posibles condiciones de política en la capa 2</td><td>X</td><td>X</td><td>X</td><td>X</td><td>Véase la Nota</td></tr>
<tr><td colspan="7">NOTA – Existe una diferencia fundamental entre la IDP basada en el enlace y la IDP basada en la red. La IDP orientada al enlace se limita al dominio de redes L2 y la IDP orientada a la red guarda relación con las firmas IDP que abarcan la información de protocolo en la capa de red (L3) y capas superiores.</td></tr>
</table>

7 Marco de modelización

7.1 Modelos funcionales

A continuación se presentan varios modelos funcionales que ilustran la gama de trayectos de reenvío de paquetes sin IDP (cláusula 7.1.2), IDP unidireccional (cláusula 7.1.3) hasta el modelo IDP bidireccional (cláusula 7.1.4).

Todos los modelos funcionales en esta cláusula son modelos funcionales de ejemplo.

7.1.1 IDP en el trayecto respecto de IDP fuera del trayecto

Existen dos principales posibilidad de desplegar la *función de nodo IDP* (IDP-NF) desde la perspectiva del trayecto de extremo a extremo:

- *IDP en el trayecto* (IDP_{InP}): la IDP-NF está situada en el trayecto de paquetes de extremo a extremo, la función de aplicación de política IDP (IDP-PEF) aplica las reglas de política IDP directamente al tráfico de paquetes (también denominado *IDP en línea*); o
- *IDP fuera del trayecto* (IDP_{OoP}): la IDP-NF *no* está situada en el trayecto de paquetes de extremo a extremo, sino que está centralizada en una red de paquetes, por lo que la IDP-PEF aplica las reglas de política IDP indirectamente, por ejemplo en un tráfico de paquetes muestreado (también denominado *IDP de derivación* o IDP *fuera de línea*).

Los dos modos IDP son diferentes desde la perspectiva del nodo físico que alberga la IDP-NF: la IDP_{InP} podría estar situada en un nodo de paquetes, y la IDP_{OoP} estaría en un nodo *sin* ninguna *función de reenvío de paquetes* (PFF, véase la cláusula siguiente).

7.1.2 Reenvió de paquetes genérico

El nodo de paquetes en una red de paquetes puede representarse de manera abstracta (a grandes rasgos) mediante una *función de reenvío de paquetes* (PFF) con arreglo a la Figura 7-1. La PFF puede ser, por ejemplo, una función de conmutación en el caso de encaminadores de conmutación por etiquetas MPLS (LSR) o conmutadores o puentes[2] Ethernet, o bien una función de reenvío/encaminamiento en el caso de IPv4 [IETF RFC 791] y encaminadores IPv6 [IETF RFC 2460]. La PFF debe determinar el siguiente nodo (por ejemplo, el tramo siguiente en redes IP) para cada paquete de entrada en la dirección de salida de las comunicaciones unidifusión.

NOTA 1 – En el caso de multidifusión se determinarían los diversos nodos siguientes.

La información utilizada por la función de determinación del nodo siguiente (DNNF) para esa función se almacena en una base de datos coubicada denominada *base de datos de reenvío* (FIB). Por ejemplo, la *MIB de la tabla de reenvío IP* según [b-IETF RFC 4292] en el caso de encaminadores IPv4, como se define en [b-IETF RFC 1812].

[2] NOTA – El término "paquete" sería en tal caso sinónimo de "trama" (L2).

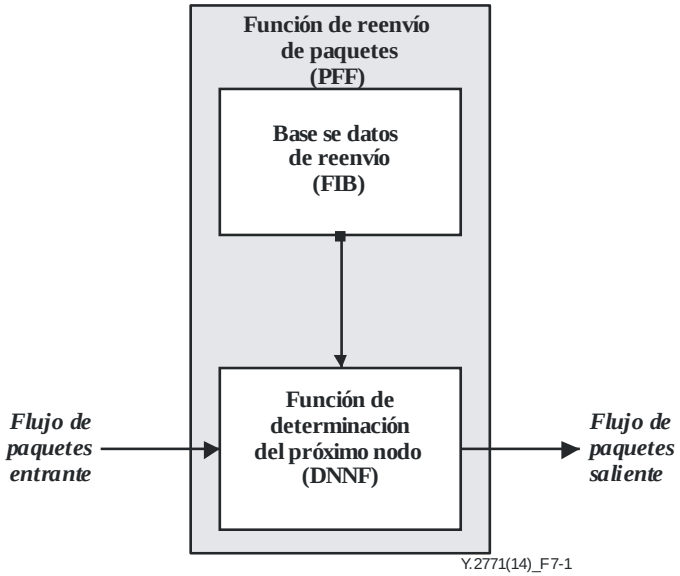


Figura 7-1 – Modelos funcionales de "reenvío genérico de paquetes"

Cabe observar que la PFF es un modelo unidireccional. La función IDP está ubicada (en su caso) en el trayecto de paquetes (es decir, el modo *IDP en el trayecto* (IDP_{InP})), normalmente antes de la PFF, véase la cláusula 7.13.

Toda información y requisitos de la PFF quedan fuera del alcance de la presente Recomendación, aunque la PFF se indica en algunos modelos funcionales a los efectos de:

- designar un posible comportamiento del nodo IDP sin aplicar ninguna regla de política IDP (por ejemplo, una condición temporal de la base de datos de política IDP vacía (IDP-PIB);
- mostrar que determinadas acciones políticas, como 'reenviar paquete', seguirían requiriendo la participación de la PFF; y
- especificar sin ambages los fundamentes para algunas métricas de rendimiento relacionadas con la IDP (véase la cláusula 8).

Cabe observar que la PFF podría estar vacía si hubiera un solo trayecto de paquetes (salida) (Nota 2).

NOTA 2 – Ejemplo: un nodo IDP en el trayecto situado entre los nodos de paquetes de L2 o L3, o un nodo IDP en el trayecto situado frente al equipo de usuario.

7.1.3 IDP unidireccional

7.1.3.1 Componentes de la función de aplicación de políticas IDP unidireccional

7.1.3.1.1 Modelo funcional general de alto nivel

En la Figura 7-2 se ilustra el modelo funcional de alto nivel, basado en la arquitectura de ejemplo de la entidad funcional IDP (IDP-FE) con arreglo a la cláusula 6.2 de [ITU-T Y.2770].

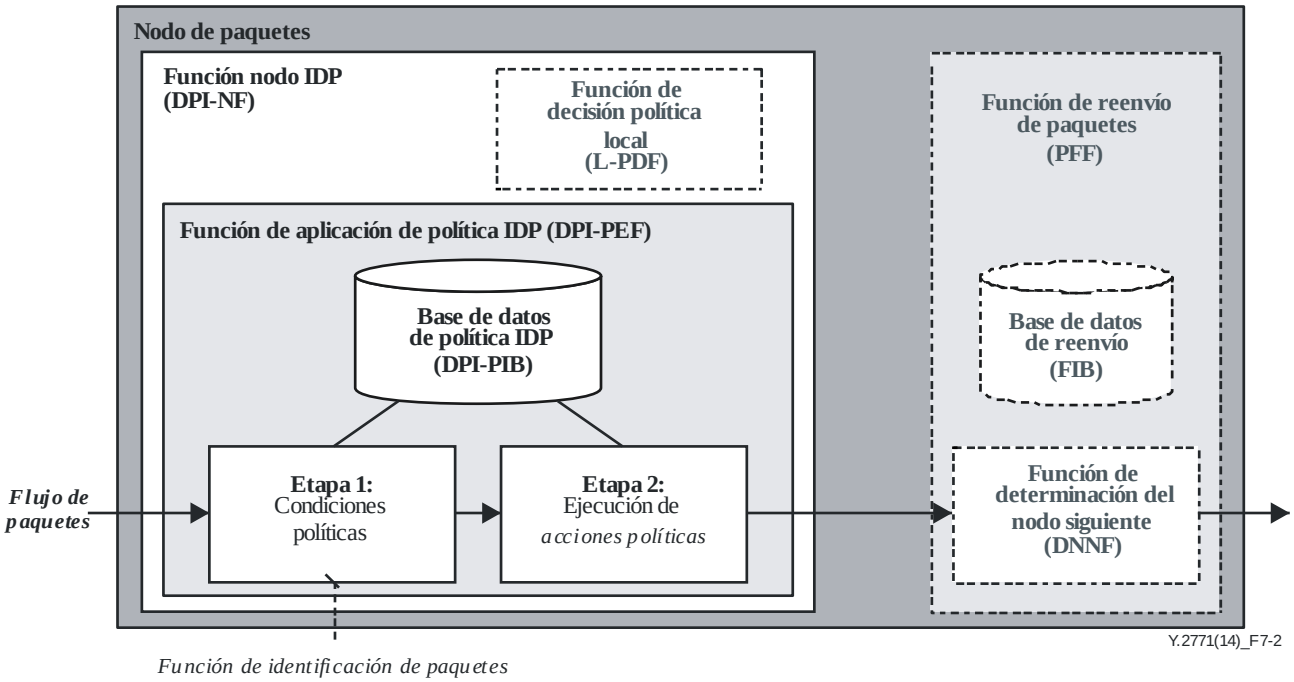


Figura 7-2 – Modelo funcional general de alto nivel

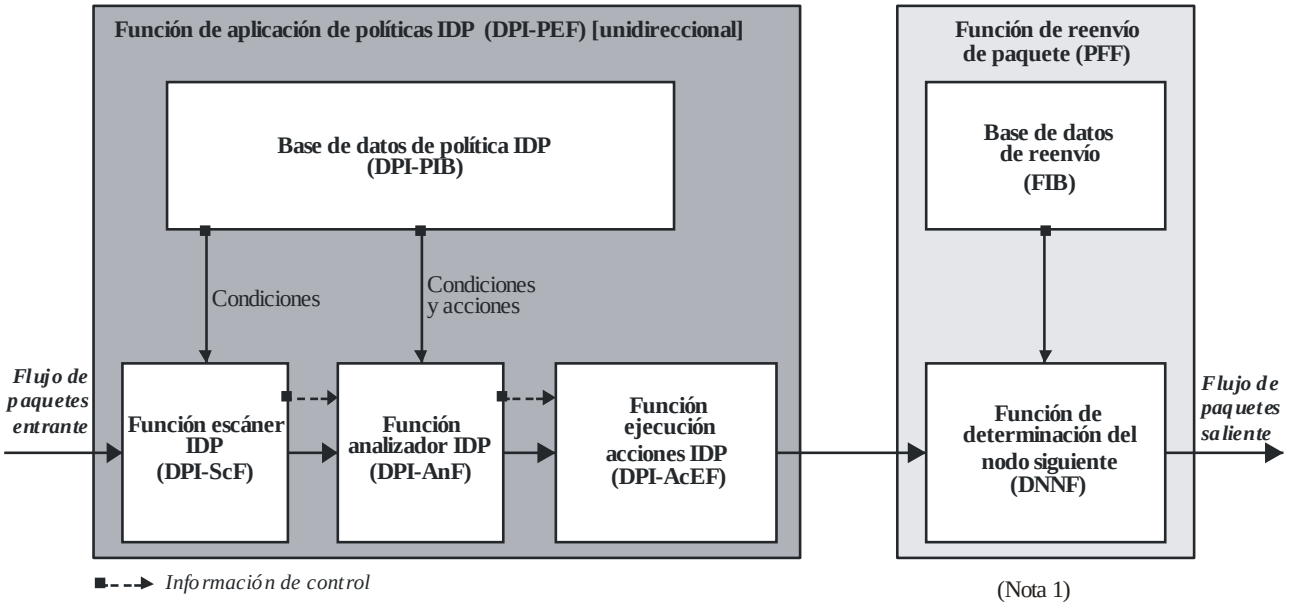
El trayecto de paquetes unidireccional se representa mediante un modelo de proceso por etapas. La etapa 1 representa la función de identificación de paquetes (véase asimismo la cláusula 7.3.2.1). Esta capacidad es esencial en el contexto de la IDP, por lo que en las cláusulas siguientes se describe en detalle (mediante ejemplos de modelos de descomposición funcional).

7.1.3.1.2 Componentes básicos en la topología de procesamiento en serie

La Figura 7-3 ilustra un ejemplo de modelo unidireccional (basado en el modelo de alto nivel de la Figura 7-2). La función de aplicación de política IDP (IDP-PEF) está situada antes de la PFF: todo paquete entrante se tramita primeramente en la IDP-PEF y luego se pasa a la PFF. La IDP-PEF puede también estructurarse en funciones de trayecto de paquetes más la tabla correspondiente para almacenar las reglas de política aplicadas, denominada base de datos de política de IDP (IDP-PIB) o *Biblioteca de signaturas IDP*. En este ejemplo, la aplicación de reglas específicas IDP está sujeta a:

- la función de escáner IDP (IDP-ScF);
- la función de analizador de IDP (IDP-AnF); y
- la función de ejecución de acciones IDP (IDP-AcEF).

Estos componentes funcionales se describen y explican en la siguiente cláusula.



NOTA 1 – LA PFF queda fuera del alcance de la presente Recomendación.
NOTA 2 – La PFF solamente figura en el modo IDP en el trayecto.

Y.2771(14)_F7-3

Figura 7-3 – Modelos IDP "Componentes de la función de políticas IDP unidireccionales"

7.1.3.1.3 Componentes adicionales

7.1.3.1.3.1 Dentro de la IDP-PEF

Los componentes adicionales dentro de la IDP-PEF todavía no se han descrito y serán objeto de un estudio ulterior.

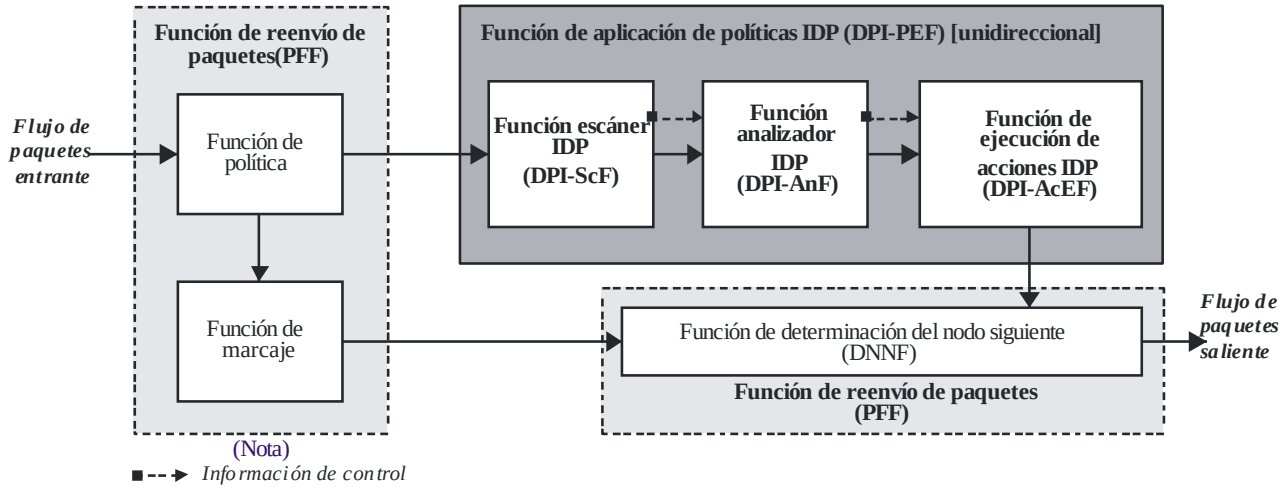
7.1.3.1.3.2 Dentro del PFF

La función de reenvío de paquetes puede incluir subelementos funcionales como de puesta en cola, encapsulado, conformación, políticas, marcaje, conmutación y DNNF. Estos elementos quedan fuera del alcance de la presente Recomendación.

7.1.3.1.4 Aspectos estructurales del trayecto de procesamiento de paquetes

En lugar de la ejecución en serie de funciones de procesamiento de paquetes (como se ilustra en la Figura 7-3) puede existir también arquitecturas de nodo IDP con paralelismos. Por ejemplo, la PFF también podría procesarse en paralelo a la IDP-PEF.

En la Figura 7-4 se muestra un modelo de trayecto de procesamiento de paquetes con procesamiento de paquetes en paralelo. En esta figura, la función de políticas supervisa los paquetes que llegan por cierto puerto de entrada, o los que cumplen criterios predefinidos (es decir, una condición de regla de política especial), por ejemplo un campo IPv4 TOS marcado con alta prioridad (o sea, reglas de política SPI). Si los paquetes o flujos entrantes infringen el acuerdo de ancho de banda, todos o algunos de los paquetes se marcan en consecuencia y se envían directamente a la DNNF.



NOTA – LA PFF queda fuera del alcance de la presente Recomendación.

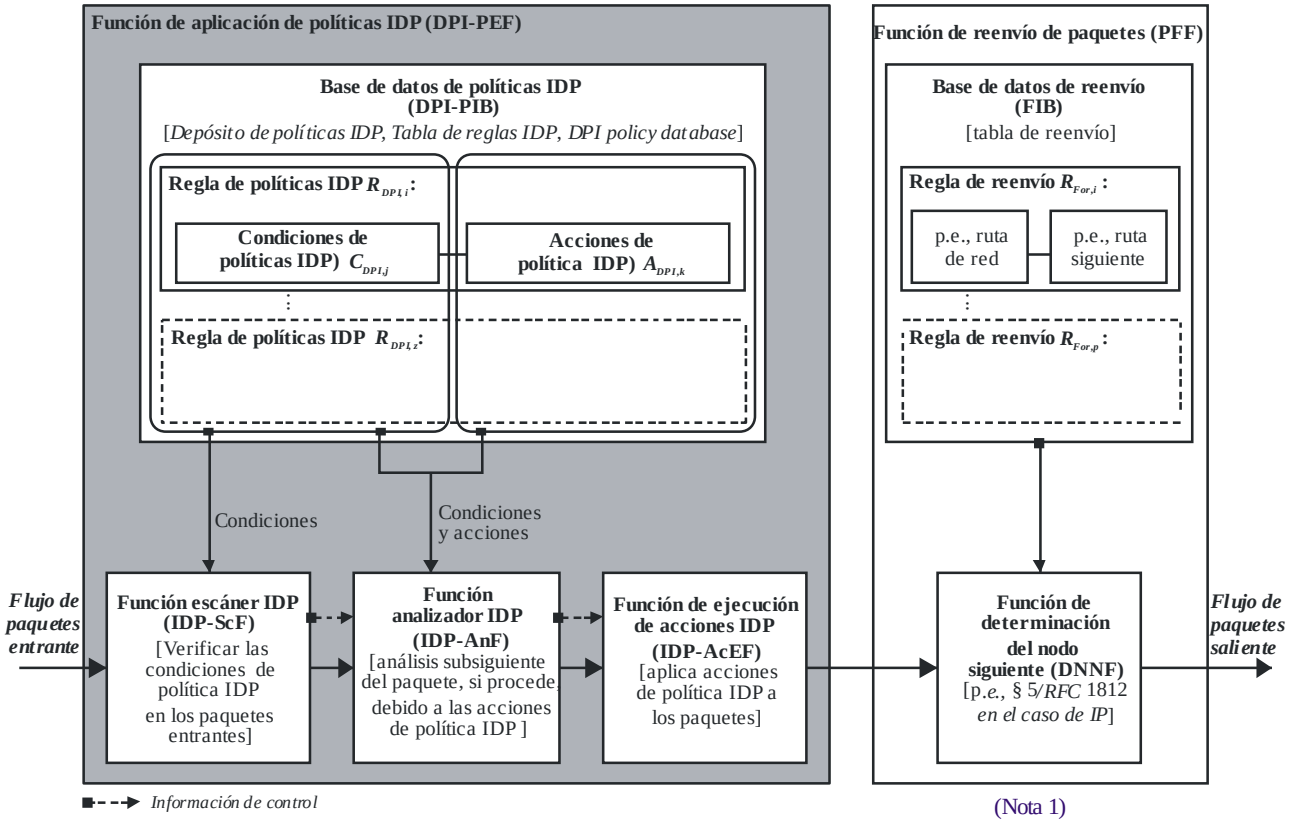
Y.2771(14)_F7-4

Figura 7-4 – Modelo IDP para la función de aplicación de política IDP con procesamiento de paquetes en paralelo

Cabe observar que los ejemplos de las Figuras 7-3 y 7-4 representan topologías lógicas, no físicas. No obstante, la materialización real debería responder al hecho de que el trayecto de procesamiento de toma un paquete o flujo puede ser diferente incluso en una misma instancia IDP.

7.1.3.2 Estructura de la base de datos de política IDP (Biblioteca de signaturas IDP)

En la Figura 7-5 se ilustra con mayor grado de detalle la estructura de la base de datos de políticas IDP, que están en consonancia funcional con la Figura 7-3. La regla de política (R) es una relación de correspondencia de un conjunto de acciones (A) con un conjunto de condiciones (C). Se evalúan las condiciones para determinar qué acciones se han de realizar. En el caso de las acciones relacionadas con el filtrado de paquetes la regla de política genérica también se conoce con el nombre de regla de filtro (específica) (véase además las cláusulas 7.3 y 7.6 en [b-ITU-T Y-Sup.23]).



NOTA 1 – LA PFF queda fuera del alcance de la presente Recomendación.
NOTA 2 – La PFF solamente figura en el modo IDP en el trayecto.

Y.2771(14)_F7-5

Figura 7-5 – Modelos IDP "estructura de la base de datos de política IDP"

Modelo de procesamiento para las *reglas de política IDP* R_{IDP}:

1) La función de escáner IDP (IDP-ScF) verifica todas (Nota 1) las condiciones de política IDP C_{IDP} del paquete entrante.

   NOTA 1 – La regla de política IDP puede abarcar todo el tráfico de paquetes reenviado por el nodo o limitarse a un determinado flujo (véase [ITU-T Y.2770]), determinado por un descriptor del flujo (véase [ITU-T Y.2770]). El flujo de paquetes podría, por ejemplo, estar sujeto a una sesión de extremo a extremo (véase la cláusula 6.7 de [ITU-T Y.2770]) entre instancias de aplicación (por ejemplo, en el caso de aplicaciones IP podrían tratarse de sesiones identificadas HTTP, RTSP, SIP, FTP, etc.). La aplicación de las reglas de política específicas de la sesión se suele llamar políticas dependientes de la sesión, a diferencia de las políticas independientes de la sesión (relacionadas con las reglas de política aplicables a todo el tráfico combinado de un nodo de aplicación de políticas). El concepto de flujo y sesión no se explican más detalladamente en esta cláusula, dado que no es indispensable para describir los modelos funcionales (de alto nivel).

2) La función de análisis IDP (IDP-AnF) sirve para verificar aún más las condiciones de política. La IDP-AnF se ejecuta secuencialmente después de la IDP-ScF, un vez que ésta ha analizado cada paquete (Nota 2). La IDP-AnF tiene por objeto mejorar el rendimiento.

   NOTA 2 – Por ejemplo, la función de escáner puede establecer una correlación entre un paquete entrante y una aplicación específica (por ejemplo, IP) y la función de análisis realiza luego una evaluación del paquete específica de la aplicación. El principio general por el que se divide en procesamiento en IDP-ScF e IDP-AnF tiene que ver con el concepto de aplicación en serie y/o jerárquica de políticas (por ejemplo, para satisfacer mejor los objetivos de rendimiento). La IDP-AnF se estudiará más detalladamente en un futuro.

3) La función de ejecución de acciones IDP (IDP-AcEF) aplica acciones de política IDP A_{IDP} en función del paquete escaneado y analizado.

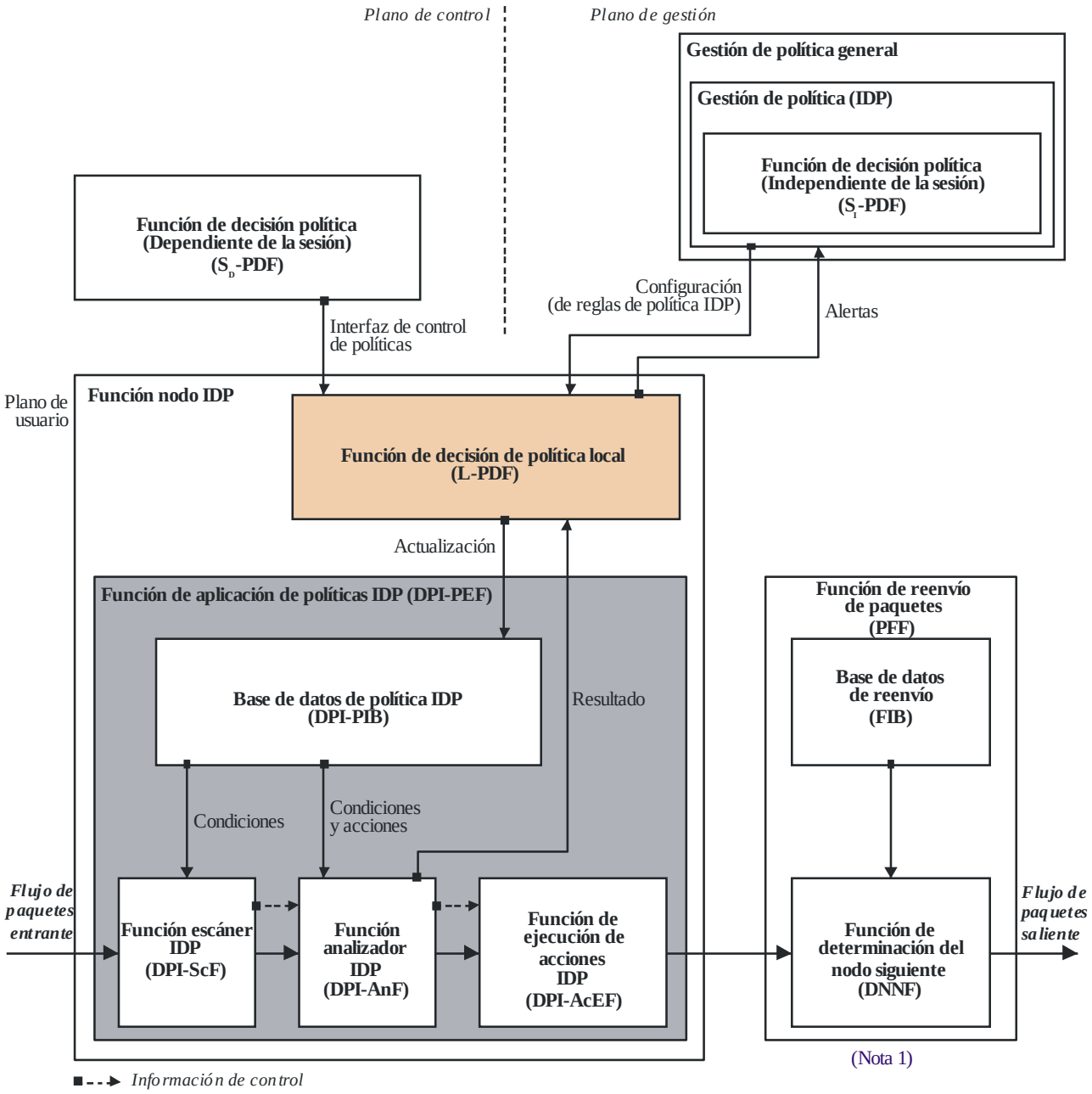
Después de haber pasado satisfactoriamente por la función IDP-PEF, cada paquete lo gestiona la PFF ordinaria (véase también la cláusula 7.1.2) en el caso del modo IDP en el trayecto.

7.1.3.3 Decisión política: modificación de la base de datos de políticas IDP

La IDP-PIB ofrece un conjunto de reglas de política IDP $R_{IDP,i}$, que determinan el comportamiento real de la función IDP-PEF. La entidad funcional de decisiones (IDP-PDFE) establece las reglas de política. En la Figura 7-6 se ilustra el ejemplo de PDF remotas, situadas en el plano de control y el plano de gestión (la Figura 7-7 muestra otro ejemplo, sin acceso (directo) alguno desde el plano de control). La PDF del plano de control puede encargarse de la decisión política IDP dependiente de la sesión (S_D-PDF). En la Nota 1 de la cláusula 7.1.3.2 se menciona un posible concepto de sesión. En [ITU-T H.248.86] se define este tipo de interfaz de control de política. La PDF del plano de gestión puede encargarse de la decisión de política IDP independiente de la sesión (S_I-PDF) en la Figura 7-6. La gestión de política puede definir principalmente reglas de política dependientes e independientes de la sesión (como en el ejemplo de la Figura 7-7).

NOTA 1 – La política dependiente de la sesión puede ser, por ejemplo, específica de una determinada aplicación, usuario, tipo de medios, etc. y la política independiente de la sesión puede comprender reglas de seguridad generales, por ejemplo, que se actualiza diariamente. Las reglas de política (IDP) de la S_D-PDF y la S_I-PDF con complementarias. La Figura 7-4 es sólo un ejemplo de configuración de red.

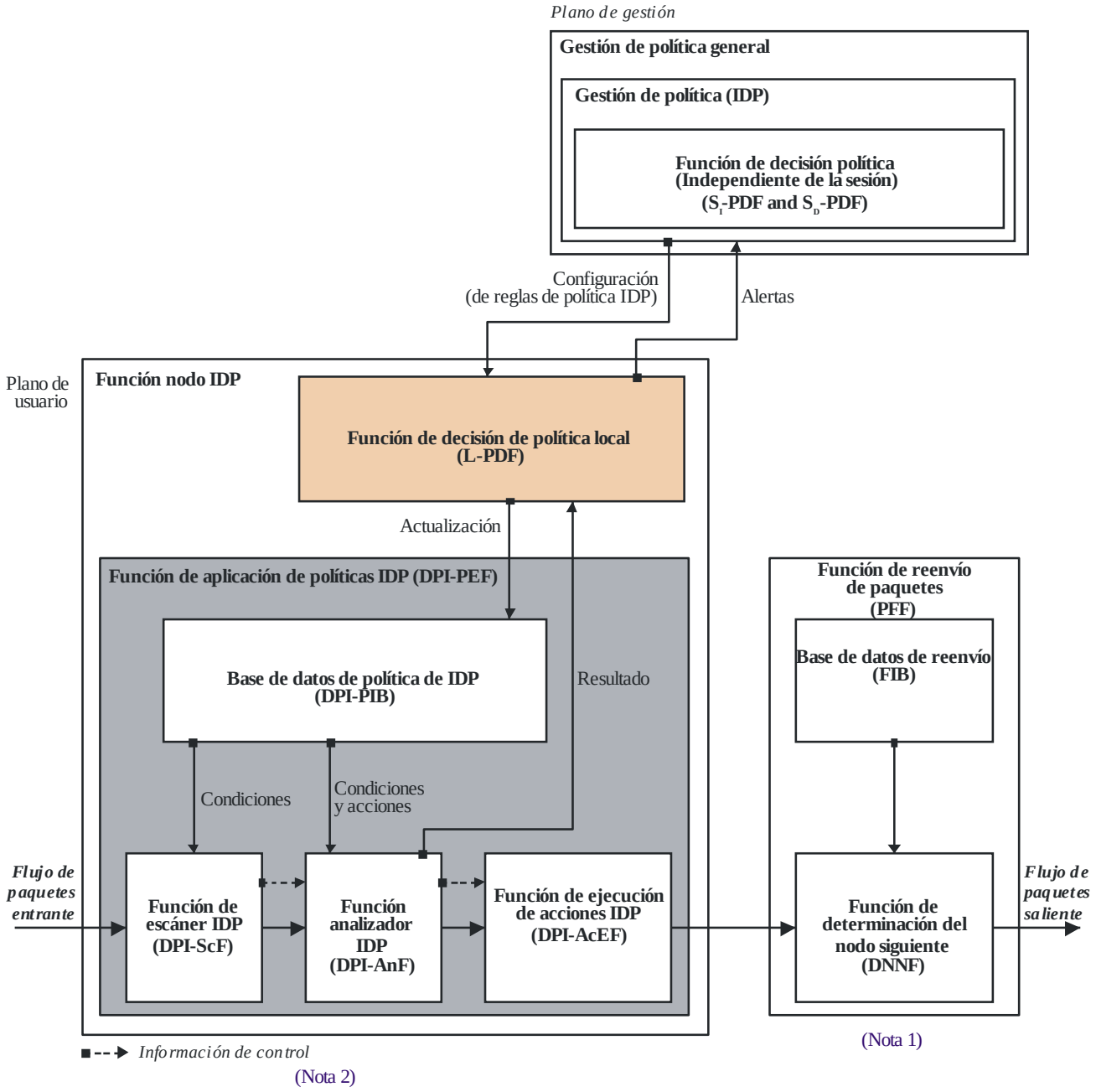
Por lo general, la gestión de política IDP forma parte de la entidad de gestión de política general, responsable también de las reglas de política ajenas a la IDP como la Inspección superficial de paquetes "tradicional" (SPI) o la inspección moderada de paquetes (MPI).



NOTA 1 – LA PFF queda fuera del alcance de la presente Recomendación.
NOTA 2 – La PFF solamente figura en el modo IDP en el trayecto.

Y.2771(14)_F7-6

Figura 7-6 – Modelos IDP "Modificación de la base de datos de política IDP a través del plano de control y gestión"



NOTA 1 – LA PFF queda fuera del alcance de la presente Recomendación.
NOTA 2 – El nodo IDP puede no estar conectado a cualquier otro elemento de red del plano de control .
NOTA 3 – La PFF solamente figura en el modo IDP en el trayecto.

Y.2771(14)_F7-7

Figura 7-7 – Modelos IDP "Modificación de la base de datos de política IDP a través del plano de gestión únicamente"

Las PDF suelen estar ubicadas en elementos de red geográficamente distantes, como se indica en la Figura 7-6 (y en la Figura 7-7) mediante la interfaz de control de políticas para la S_D-PDF y la interfaz de gestión de políticas para la S_I-PDF. Toda PDF puede estar temporalmente fuera de servicio, lo que estimula a que haya otra PDF local opcional PDF (L-PDF) para optimizar la disponibilidad del servicio IDP en la red.

La L-PDF junto con la IDP-PEF representa la función nodo IDP.

NOTA 2 – Está relacionada con el trayecto de decisión de política local en la Figura 7-1 de la cláusula 7.2.1 [ITU-T Y.2770].

La L-PDF proporciona (en su caso) comunicación externa con las PDF distantes y la interfaz interna con la IDP-PEF para actualizar la base de datos IDP-PIB y procesar los posibles resultados de la función de analizador IDP (IDP-AnF). La L-PDF puede también encargarse de resolver los problemas de interacción de reglas entre el conjunto de reglas de política IDP.

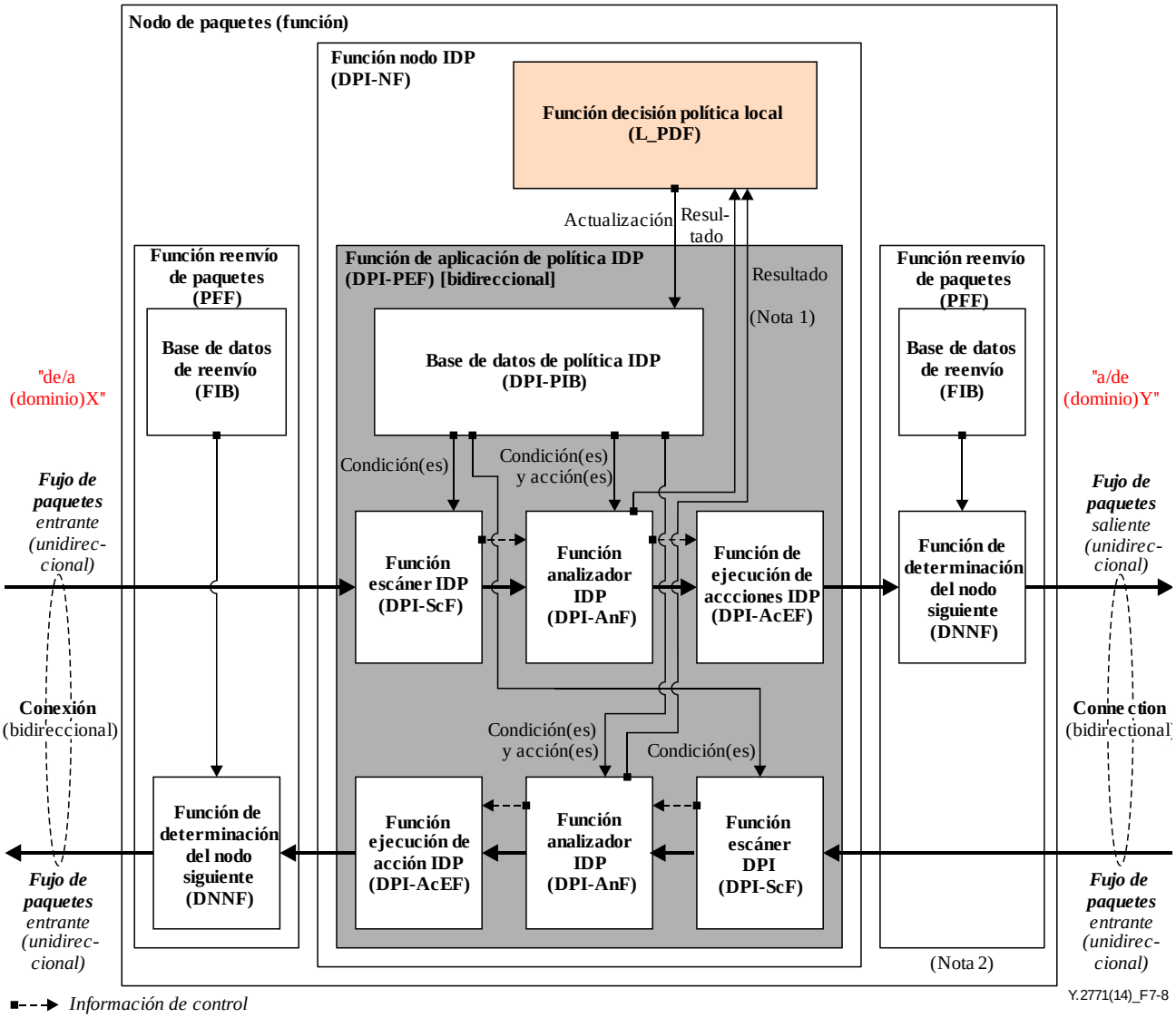
NOTA 3 – La detección y resolución de interacciones de reglas es una función fundamental para las PDF.

El resultado de la función de analizador IDP (IDP-AnF) puede generar alertas hacia la gestión de política (por ejemplo, la notificación de una nueva amenaza de seguridad).

El modelo fundamental de aplicación de políticas es unidireccional, pero puede ampliarse para trayectos de comunicación bidireccionales (véase la siguiente cláusula).

7.1.4 IDP bidireccional

La Figura 7-8 ilustra un ejemplo de modelo IDP bidireccional (véase la definición en la cláusula 3.2.4 de [ITU-T Y.2770]). La conexión de paquetes bidireccional consiste en dos flujos de paquetes unidireccionales. La base de datos IDP-PIB es el elemento que vincula los dos sentidos del tráfico desde la perspectiva de aplicación de políticas IDP. La regla de política IDP "bidireccional" proporcionará las condiciones de política IDP y/o las acciones pertinentes para los dos sentidos del tráfico.



NOTA 1 – La DPI-PIB puede organizarse internamente de manera dependiente de la dirección DPI-PIBs.e., DPIx ® y-PIB y DPIy ®
NOTA 2 – La PFF queda fuera del alcance de la presente Recomendación.
NOTA 3 – La PFF solamente figura en el modo IDP en el trayecto.

Figura 7-8 – Modelos IDP "IDP bidireccional"

La L-PDF es responsable de la IDP-PEF bidireccional y sirve de "función de mediación" al efectuar un postprocesamiento de los psibles resultados de las funciones de analizador unidireccional (IDP-AnF), que podría determinar la actualización de las reglas de política (local) y/o la notificación de las PDF distantes.

7.1.5 IDP con y sin estados

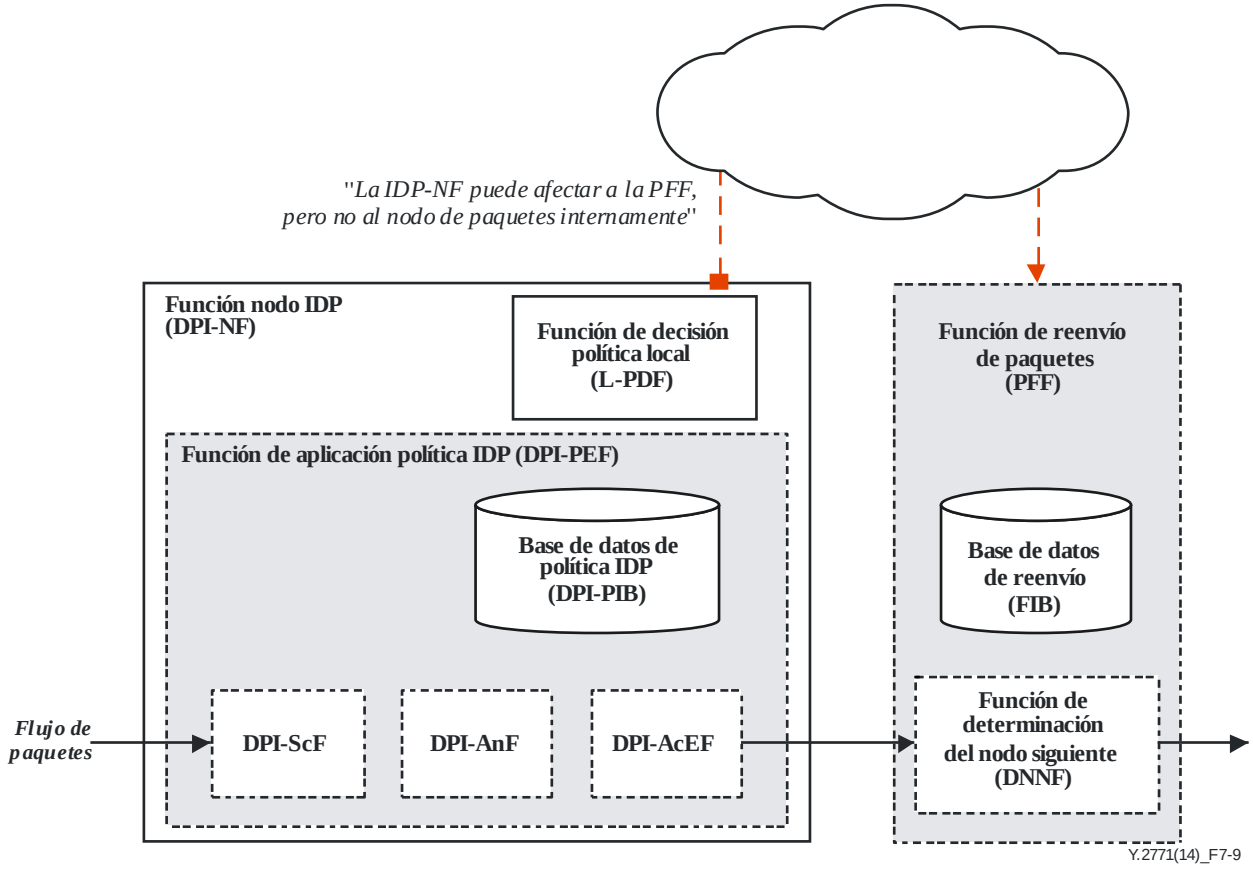
La IDP sin estados se refiere a reglas de política IDP que se aplican a todos y cada uno de los paquetes, sin que exista correlación alguna con otros paquetes de un flujo de paquetes unidireccional o la conexión de paquetes bidireccional (véase "condición de estado" en la cláusula 3.2.11 de [ITU-T Y.2770]).

La IDP con estados implica que existe una correlación (Nota), que se puede modelar mediante una máquina de estados (finitos). Este modelo funcional será específico de las reglas de política IDP y, por consiguiente, queda fuera del alcance de la presente Recomendación.

NOTA – Por ejemplo, una aplicación IP con transporte TCP de datos de aplicación. Puede haber condiciones de política especiales para la fase de establecimiento de la conexión TCP y otras condiciones de política para la siguiente fase de comunicación activa.

7.1.6 Incidencia de la IDP en la retransmisión de paquetes

La función nodo IDP puede afectar a la siguiente función de reenvío de paquetes (PFF), a condición de que la PFF esté disponible o "no vacía" (véase la cláusula 7.1.2). Ahora bien, la IDP-NF no estará autorizada para modificar la PFF local del nodo de paquetes. Esto es más bien una opción, generada por los elementos de red distantes, externos al nodo de paquetes (véase la Figura 7-9). La incidencia específica dependerá de las decisiones políticas y/o las reglas de política IDP especiales, por lo que queda fuera del alcance de la presente Recomendación.



NOTA 1 – La PFF queda fuera del alcance de la presente Recomendación.
NOTA 2 – La PFF solamente figura en el modo IDP en el trayecto.

Figura 7-9 – Posible incidencia de la IDP en el reenvío de paquetes a través de la entidad de red distante

Ejemplos:

- Actualización de la base de datos FIB (información de ruta de la red, véase también la Figura 7-5) debido al rendimiento de la red observada en relación con la topología de red.
- Actualización de la FIB mediante el bloqueo de ciertas rutas de red (por ejemplo, en el sentido inverso en el caso de la IDP bidireccional).

Cabe observar que cualquier modificación local de la PFF, generada por la IDP-NF y de acuerdo con las instrucciones de los elementos de red externos debe estar en consonancia con el marco global de la red subyacente en lo que respecta a los conceptos de reenvío de paquetes, conmutación y/o encaminamiento (por ejemplo, dado un dominio IPv6 DiffServ, un dominio MPLS, una topología L2VPN, etc.).

7.1.7 IDP en el contexto de redes de paquetes y de las NGN

La función de nodo IDP está integrada en el nodo de paquetes funcional, ya sea físico o virtual, que puede interactuar con otras funciones de la red de paquetes. La Figura 7-10 ilustra un ejemplo de contexto. En [ITU-T H.248.86] se define la tecnología de control IDP cuando las entidades IDP-PDFE y IDP-FE se hacen corresponder con un modelo de pasarela descompuesta.

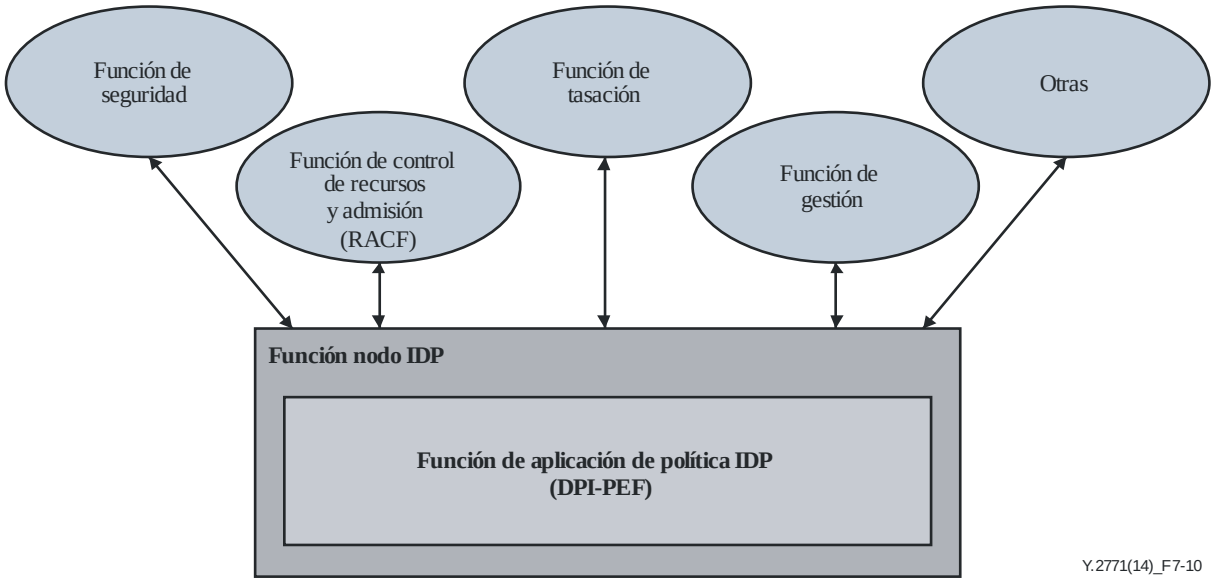


Figura 7-10 – IDP en el contexto de redes de paquetes y de las NGN

7.1.8 Modelos funcionales para la medición de flujos IETF

7.1.8.1 Características de la función de medición de flujos IETF IPFIX

La función de medición de flujos IETF IPFIX se define en [IETF RFC 5101] (véase también la cláusula 6.3.3.2 en [ITU-T Y.2770]). La noción de "flujo" se refiere a un flujo de paquetes con arreglo a la cláusula 3.1.3 de [ITU-T Y.2770] y la de "medición" a la medición de la métrica de rendimiento. La función de medición de flujos IPFIX incorpora, por lo tanto, parte de las condiciones de reglas para la identificación de flujos de paquetes (basadas en el identificador de flujos IPFIX (véase la cláusula 3.2.17 en [ITU-T Y.2770]) y una parte relacionada con las acciones de reglas de política para acciones de medición y notificación.

7.1.8.2 Función integrada de medición de flujos

El proceso de flujos IETF IPFIX se pueden obtener y describir mediante una regla de política IDP, y, por ende, hacerse corresponder directamente con una entidad IDP-FE. En la Figura 7-11 se ilustra este tipo de función integrada de medición de flujo. Los resultados de la medición se pueden comunicar a través de las interfaces externas e2 o e1.

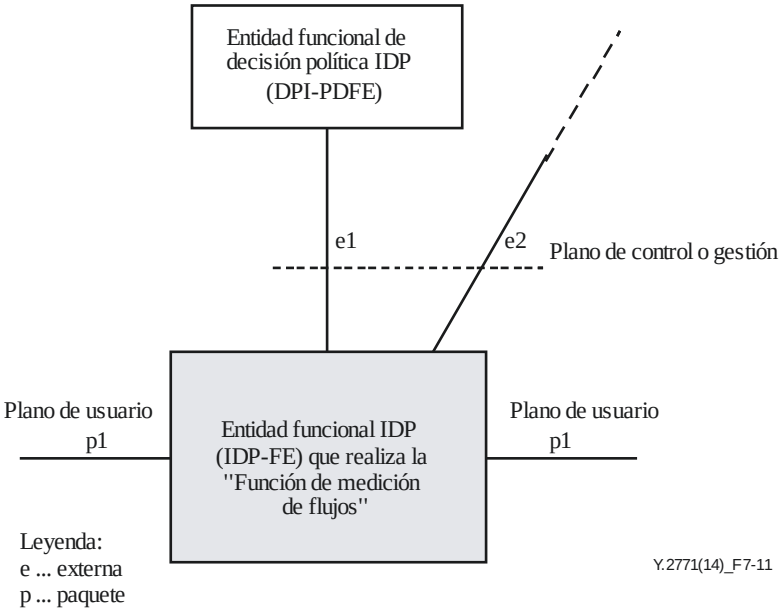


Figura 7-11 – Función integrada de medición de flujos

7.1.8.3 Función remota de medición de flujos

La función de medición de flujos también puede estar situada a distancia en el trayecto de paquetes p1, antes (Figura 7-12) o después de la entidad IDP-FE. La configuración de red con una función remota de medición de flujos se utiliza en casos tales como cuando la red existente dispone de una entidad física con medición de flujos y la entidad IDP-PE se instala adicionalmente después.

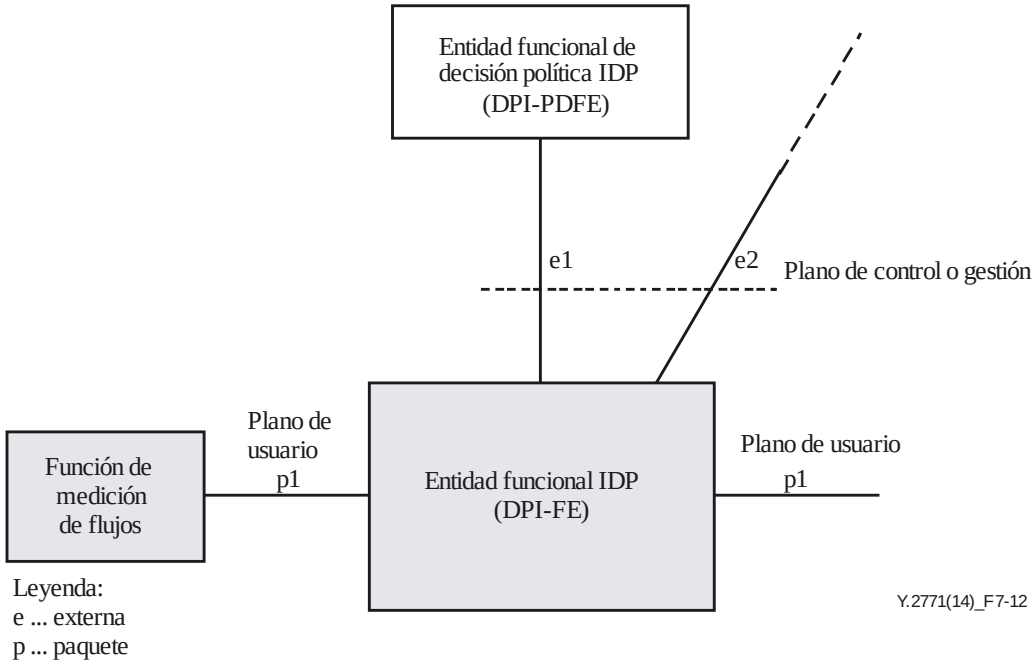


Figura 7-12 – Función remota de medición de flujos

La entidad IDP-FE y la función remota de medición de flujos pueden considerarse como una arquitectura distribuida con dos variantes:

1) Arquitectura desacoplada: las dos entidades funcionales sólo están conectadas a través de p1, por lo que están totalmente disociadas en el plano de control y gestión.

2) Arquitectura acoplada: por ejemplo, los resultados de la función de medición de flujos podrían comunicarse también a través del e2 de una entidad IDP-FE. Este tipo de modelo funcional de compartición requeriría sencillamente una nueva interfaz adicional (aparte de p1) entre las dos entidades funcionales.

Los casos de utilización para estas dos variantes quedan pendientes de estudio.

7.1.9 IDP probabilística

7.1.9.1 IDP probabilística en general

El proceso de identificación de paquetes puede ser inherentemente estadístico (a diferencia de la identificación de paquetes determinística), es decir, el resultado de la identificación (como los criterios de concordancia) se obtiene por probabilidad. Este tipo de inspección de paquetes se denomina IDP probabilística, también conocida como IDP indeterminada.

La IDP probabilística está relacionada con las reglas de política IDP cuyas condiciones son, por ejemplo:

– El conjunto de signaturas 'S' contiene las signaturas 'S_1', 'S_2', …, 'S_N'. El conjunto 'S' representa una combinación de condiciones políticas con arreglo a una forma normal disyuntiva booleana (DNF), es decir, las signaturas 'S_i' (i = 1, 2 ... N) se combinan en una lista basada en el operador OR. Las dos etapas de IDP tienen las siguientes características:

  etapa 1: generación de condiciones políticas basadas en procesos probabilísticos; y

  etapa 2: ejecución de las condiciones de política que culmina en resultados de concordancia determinística, lo que da lugar así una IDP probabilística.

El principal objetivo de la IDP probabilística es obtener rápida y eficientemente información acerca de si el paquete se corresponde con el conjunto de signaturas 'S'. La información de concordancia concreta – es decir, qué signatura 'S_i' específica se ha identificado – es secundaria. El conjunto de signaturas 'S' representa en general una opción de identificación para una aplicación particular. La correspondiente etiqueta de aplicación, por ejemplo 'paquete con firma en el conjunto S', pudiera ser objeto de notificación.

7.1.9.2 Filtro bloom basado en IDP probabilística

El filtro bloom basado en IDP es un ejemplo muy conocido y representativo de la IDP probabilística, debido a la tasa de errores inherentes ε_{IDP}, en lo que respecta a falsos positivos $\varepsilon_{f\text{-}p}$ (véase la cláusula 8.2.3.3.1), del método de inspección de paquetes subyacente.

Considérese el ejemplo específico de la aplicación realizado como filtro bloom:

– La aplicación IDP consiste en la detección del "tráfico de la aplicación x". El tráfico de la aplicación x se caracteriza por un conjunto de signaturas S = {'aplicación x v1', 'aplicación x v2', …, 'aplicación x vk'}, es decir, signaturas individuales relativas a las características específicas de la aplicación. Podría haber una regla de política IDP de ejemplo para detectar si el paquete contiene la "aplicación x", utilizando el conjunto de signaturas como condición de regla de política IDP, y descartar sencillamente el paquete cuando haya una concordancia, sin tener que saber de qué versión exacta de la aplicación x se trata.

  El principal motivo del filtro bloom basado en la IDP probabilística es llegar a un equilibrio entre la exactitud de la identificación y el consumo de recursos (por ejemplo, en cuanto a tiempo de CPU y/o memoria). Este método permite simplificar considerablemente el procesamiento IDP.

A continuación se describen las características probabilísticas de la IDP basada en el filtro bloom:

– Todo paquete entrante 'P' se compara con el filtro bloom que representa el conjunto completo de signaturas 'S' en paralelo; si un paquete 'P' se corresponde con una o varias signaturas del conjunto 'S', el resultado será una concordancia con un certidumbre de probabilidad de información estimada $P_{Hit,BloomFilter,'S'}$, que obedece a la siguiente ecuación:

$$P_{Hit,BloomFilter,'S'} = 1 - \varepsilon_{f-p} = 1 - \left(1 - e^{-kN/m}\right)^k \quad (7\text{-}1)$$

siendo:

m = tamaño del filtro bloom en bits

N = número de signaturas en el conjunto S

k = número de función de aleatorización utilizada para crear el filtro bloom.

La noción de "probabilística" está relacionada con la "exactitud de identificación " de una entidad IDP-FE que interviene en la identificación de un paquete, flujo, aplicación, etc., y estrechamente vinculada con la métrica del rendimiento en el ámbito de tasa de errores (véase la cláusula 8.2). Para más información sobre la IDP probabilística realizada mediante filtros bloom, véase el Apéndice I, indicador de rendimiento "tasa de errores de falsos positivos (IDP)" $\varepsilon_{f\text{-}p}$ y el indicador de rendimiento "tasa de errores de falsos negativos (IDP)" $\varepsilon_{f\text{-}n}$ es igual a cero.

7.2 Información y modelos de datos

El proceso de desarrollo por etapas de los servicios de comunicación [b-ITU-T I.130] distingue entre los niveles de abstracción de "información" y "datos" (tales como unidades de datos de protocolo). Los modelos de información se utilizan a muy alto nivel para describir la instancia del flujo de información entre entidades de red (véase por ejemplo [b-ITU-T I.130], [b-ITU-T X.1036]). El modelo de datos se utilizan a un nivel inferior para describir, por ejemplo, un elemento de información desde el punto de vista sintáctico (véase, por ejemplo, [b-ITU-T J.380.1]).

7.2.1 Modelo de información (marco de ejemplo)

Todo tipo de especificación detallada para crear modelos de reglas de política IDP relativas a información y flujos de información quedan fuera del alcance de una Recomendación de tipo "marco". Ahora bien, la creación de modelo de información de reglas de política IDP de [b–IETF RFC 3060] puede considerarse como ejemplo de referencia. En el Cuadro 7-1 se indican algunos ejemplos de elementos de información a título orientativo (sobre cómo crear un modelo concreto):

Cuadro 7-1 – Modelo de información de ejemplo, basado en [b-IETF RFC 3060]

Elemento de información (esta Recomendación y [ITU-T Y.2770]):	Modelo básico de información de política genérica según la [b-IETF RFC 3060]:
Regla de política IDP	Podría basarse en la clase "PolicyRule"
Condición (compuesta) de regla de política IDP	Podría basarse en la clase abstracta "PolicyCondition"
Condición (sencilla) de regla de política IDP	Podría basarse en la clase abstracta "PolicyCondition"
Acción de regla de política IDP	Podría basarse en la clase abstracta "PolicyAction"
Y así sucesivamente, como reglas de política IDP de agrupación y establecimiento de prioridades, y características tales como periodo de validez de las reglas, etc.	…

7.2.2 Modelo de datos (marco de ejemplo)

Todo tipo de especificación detallada para crear modelos de reglas de política IDP relativas a objetos de datos queda fuera del alcance de una Recomendación de tipo "marco" (porque en tal caso quedaría abierto el ámbito de desarrollo de sintaxis del protocolo).

Sin embargo, la modelización de datos de reglas de política IDP [b-IETF RFC 4011] podría servir de ejemplo de referencia. En el Cuadro 7-2 se indican algunos ejemplos de objetos de datos a título orientativo (sobre cómo crear un modelo en concreto):

Cuadro 7-2 – Ejemplo de modelo de datos, basado en [b-IETF RFC 4011]

Elemento de información la presente Recomendación y [ITU-T Y.2770]):	**Objeto de datos genérico, utilizando como ejemplo la MIB de gestión basada en políticas según [b-IETF RFC 4011]:**
IDP-PIB	Podría basarse en el objeto "pmPolicyTable", que a su vez está vinculado con el objeto "pmPolicyCodeTable" (Nota 1)
Regla de política IDP, es decir, elemento de la IDP-PIB	Podría basarse en el objeto "pmPolicyEntry"
Condición de regla de política IDP	Podría basarse en el objeto " pmPolicyCodeEntry" (Nota 2)
Acción de regla de política IDP	Podría basarse en el objeto " pmPolicyCodeEntry" (Nota 2)
Etc.	Etc.
NOTA 1 – La abstracción y separación entre la "descripción de la regla" y el "código de la regla" en dos tablas relacionadas permite definir de manera eficiente la "IDP-PIB". NOTA 2 – Es decir, la condición de la regla y la acción de la regla podría utilizar finalmente el mismo modelo de objeto de datos (en este ejemplo).	

Perspectiva del plano de red: cabe observar que el objeto de datos genérico podría verse como

- un objeto gestionado desde la perspectiva del plano de gestión IDP (véase la interfaz e2 de la cláusula 8 de [ITU-T Y.2770]), y/o
- un objeto controlado desde la perspectiva del plano de control IDP (véase la interfaz e1 de la cláusula 8 de [ITU-T Y.2770]).

Por ejemplo, podría indicarse una determinada regla de política IDP (a través del e1) mediante la entidad IDP PD-FE, o configurarse (a través del e2) mediante el sistema de gestión IDP, pero resultar el mismo elemento objeto de datos de la "regla de política IDP" en la IDP-PIB.

7.3 Modelos de tráfico

7.3.1 Introducción

Esta cláusula tiene por objeto describir algunas características interesantes de las entidades IDP (véase la definición en la cláusula 3.2.7 de [ITU-T Y.2770]) desde la perspectiva de la teoría del tráfico. Los aspectos derivados podrían ayudar en la ulterior definición de, por ejemplo, requisitos funcionales, de rendimiento o de disponibilidad, la indicación de aspectos arquitectónicos o la evaluación del rendimiento.

Los modelos de tráfico descritos son sólo ejemplos y no son necesariamente representativos de un determinado componente de IDP (tales como IDP-PE, IDP-FE, motor IDP, biblioteca de firmas IDP, etc.).

7.3.2 Modelos básicos de tráfico para el procesamiento en el trayecto de paquetes

La gestión de tráfico se efectúa al nivel de granularidad de paquetes, las funciones principales de una entidad IDP-FE, y se materializa en el motor IDP integrado (véase la definición en la cláusula 3.2.6 de [ITU-T Y.2770]).

El motor IDP es el principal componente de la entidad IDP-FE y desempeña una importante función en la IDP-FE. El tráfico IDP se procesa en el motor IDP. Cuando este motor se materializa en un componente físico, el procesamiento en paralelo puede ayudar a mejorar su rendimiento. En tal caso, habrá varias unidades de procesamiento dentro del componente físico que corresponda al motor IDP.

7.3.2.1 Modelo básico de tráfico de una entidad IDP-FE centrado en el motor IDP

La Figura 7-13 utiliza el modelo funcional IDP-FE de ejemplo con arreglo a la Figura 6-1 de [ITU-T Y.2770] con el fin de obtener un modelo de tráfico característico. El modelo de tráfico se basa exclusivamente en el trayecto de paquetes, por lo que sirve de modelo para un motor IDP.

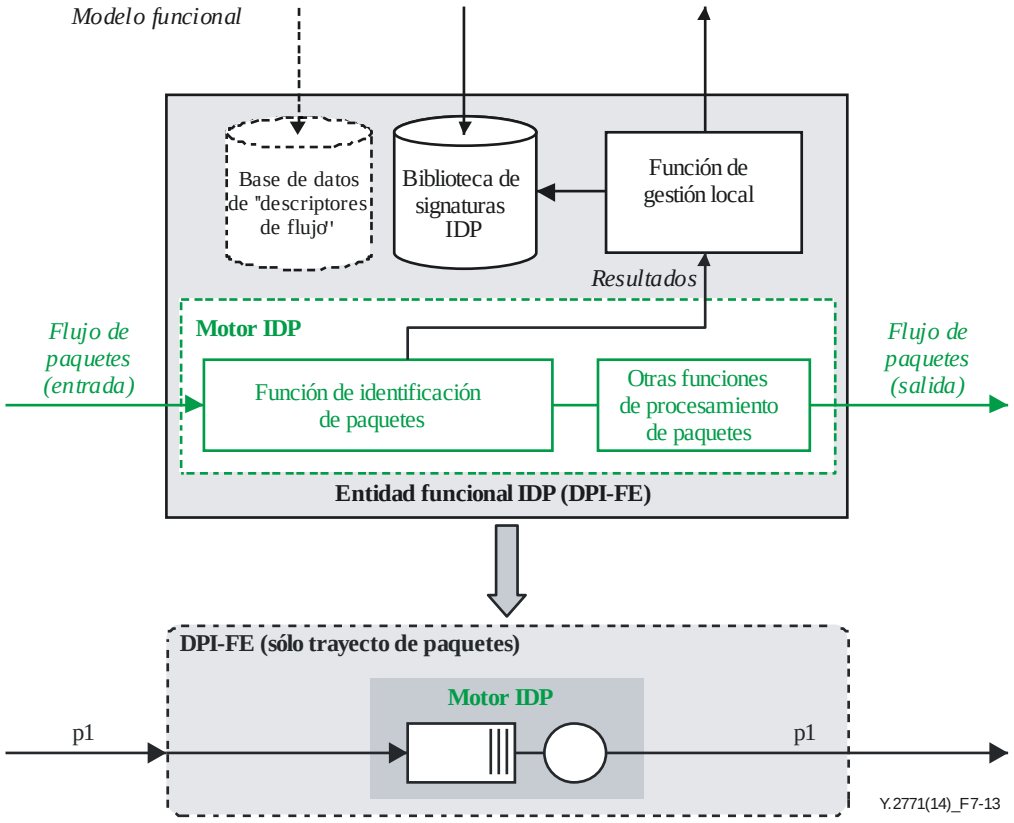


Figura 7-13 – Modelo básico de tráfico de una IDP-FE centrado en el motor IDP

El modelo se caracteriza por un solo servidor y una cola de espera finita. El servidor procesa todas las funciones del trayecto de paquetes. La etapa 1 del modelo de servidor representa el modelo de tráfico para un flujo de paquetes unidireccional.

7.3.2.2 Motor IDP: extensión a procesamiento multietapa en el trayecto de paquetes

7.3.2.2.1 Motor IDP basado en un servidor de dos etapas

En la Figura 7-14 se muestra un ejemplo de modelo de tráfico de un motor IDP de dos etapas.

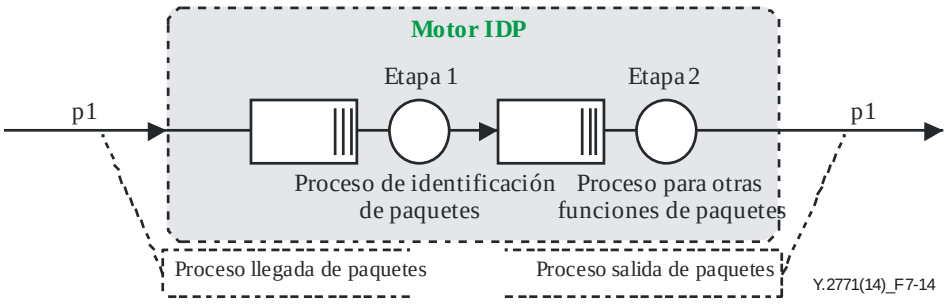


Figura 7-14 – Modelo de tráfico de un motor IDP: extensión al procesamiento en 2 etapas en el trayecto de paquetes

En este ejemplo, el primer servidor se encarga de procesar las condiciones de reglas IDP.

7.3.2.2.2 Motor IDP basado en un servidor de 3 etapas

El motor IDP podría realizarse internamente en la forma de un sistema distribuido, como una serie de elementos de procesamiento concatenados. En el ejemplo de modelo funcional basado en la Figura 7-3 se representan tres etapas de procesamiento, denominadas "escáner IDP, análisis IDP y ejecución de acciones IDP", con las siglas IDP-ScF, IDP-AnF e IDP-AcEF, respectivamente.

En la Figura 7-15 se muestra un ejemplo del correspondiente modelo de tráfico.

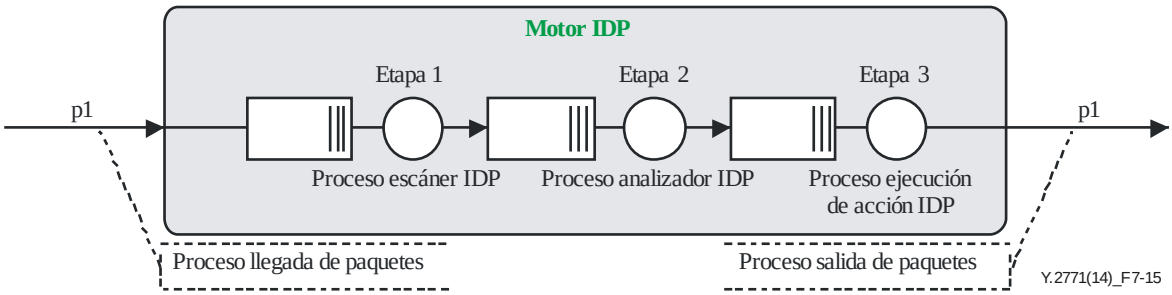


Figura 7-15 – Modelo de tráfico con motor IDP: extensión al procesamiento en 3 etapas en el trayecto de paquetes

7.3.3 Modelos de tráfico ampliados para motores IDP

7.3.3.1 Interfaz externa sencilla y paralelismo interno

Ejemplo: pudiera existir una entidad IDP fuera del trayecto (véase la cláusula 6.1), conectada por una sola ruta de red a la red de paquetes. Este tipo de entidad IDP podría servir para el procesamiento fuera de línea de numerosos flujos de paquetes, es decir, cuando se requiera una elevada capacidad de procesamiento. Una posible opción para lograr una alta capacidad es el procesamiento en paralelo. La Figura 7-16 ilustra un ejemplo de modelo de tráfico, con varios motores IDP en paralelo.

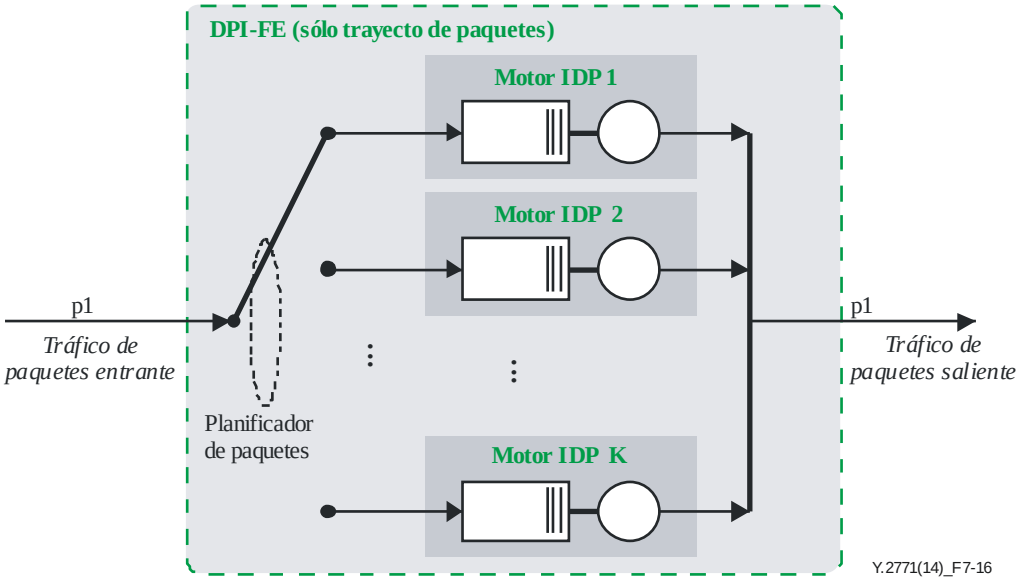


Figura 7-16 – Motores IDP – Interfaz externa sencilla y paralelismo interno

En este modelo de tráfico se ha de disponer de una función de planificador de paquetes para asignar cada paquete entrante a un motor IDP (servidor). Esta función queda fuera del alcance de la presente Recomendación.

NOTA – Por ejemplo, el planificador de paquetes podría ser:

a) un simple algoritmo equilibrado de carga (es decir, planificación basada exclusivamente en el estado de carga estimado de los servidores de motores IDP), que sólo tiene realmente sentido para la IDP sin estados;

b) basarse en la información del descriptor de flujo (para resolver la IDP con estados), pero en este caso habrá al menos un modelo de servidor de 2 etapas desde el punto de vista de la modelización de tráfico; o

c) cualquier otro tipo de métodos de planificación.

7.3.3.2 Múltiples interfaces externas y paralelismo interno

La entidad IDP en el trayecto situada en el núcleo de red (véase la cláusula 6.1) suele proporcionar varias interfaces físicas p1. Los diversos motores IDP puede actuar en paralelo sobre todos los flujos de paquetes entrantes (véase la Figura 7-17). Se suele exigir que todos los motores IDP (por ejemplo, *K*) estén conectados a todas las interfaces p1 de paquetes entrantes (por ejemplo, *N*). A tal efecto, se necesita una función de entretejido de conmutación de paquetes *N-a-K*. Dicha función queda fuera del alcance de la presente Recomendación.

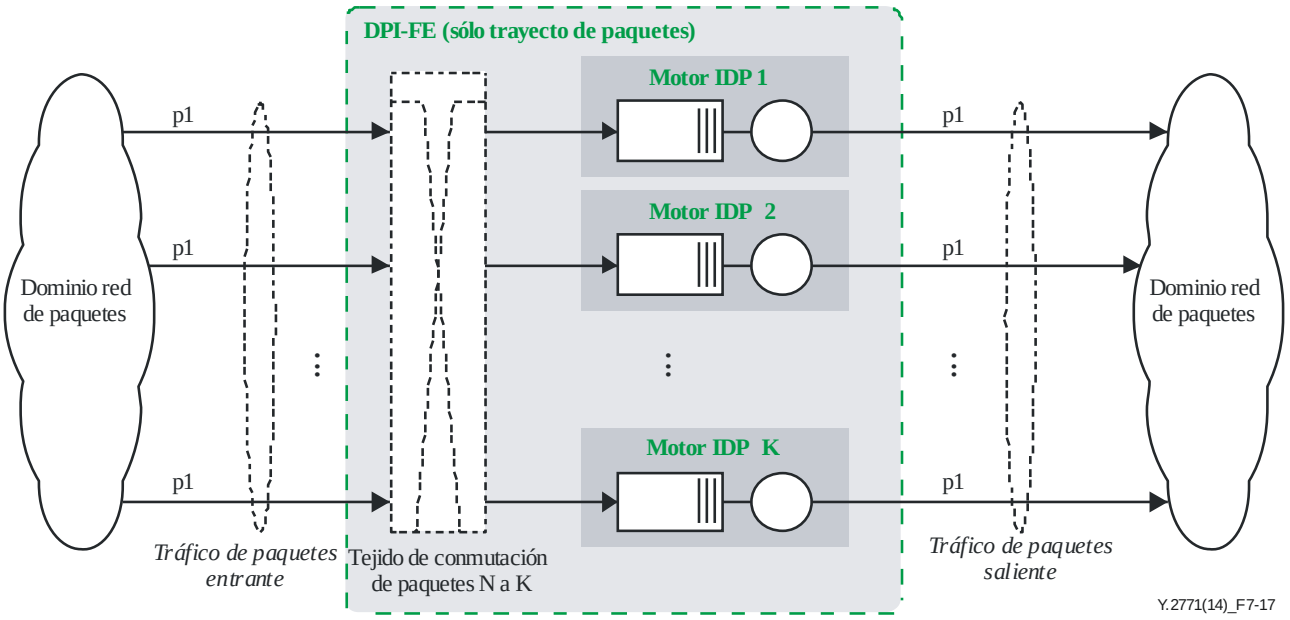


Figura 7-17 – Múltiples interfaces externas y paralelismo interno

7.3.3.3 Motores IDP en paralelo basados en modelos de servidor de 3 etapas

Las Figuras 7-18 y 7-19 ilustran un modelo ampliado, basado en la combinación de modelos de motor IDP de 3 etapas (cláusula 7.3.2.2.2) y paralelismo a nivel de motores IDP (cláusula 7.3.3.1).

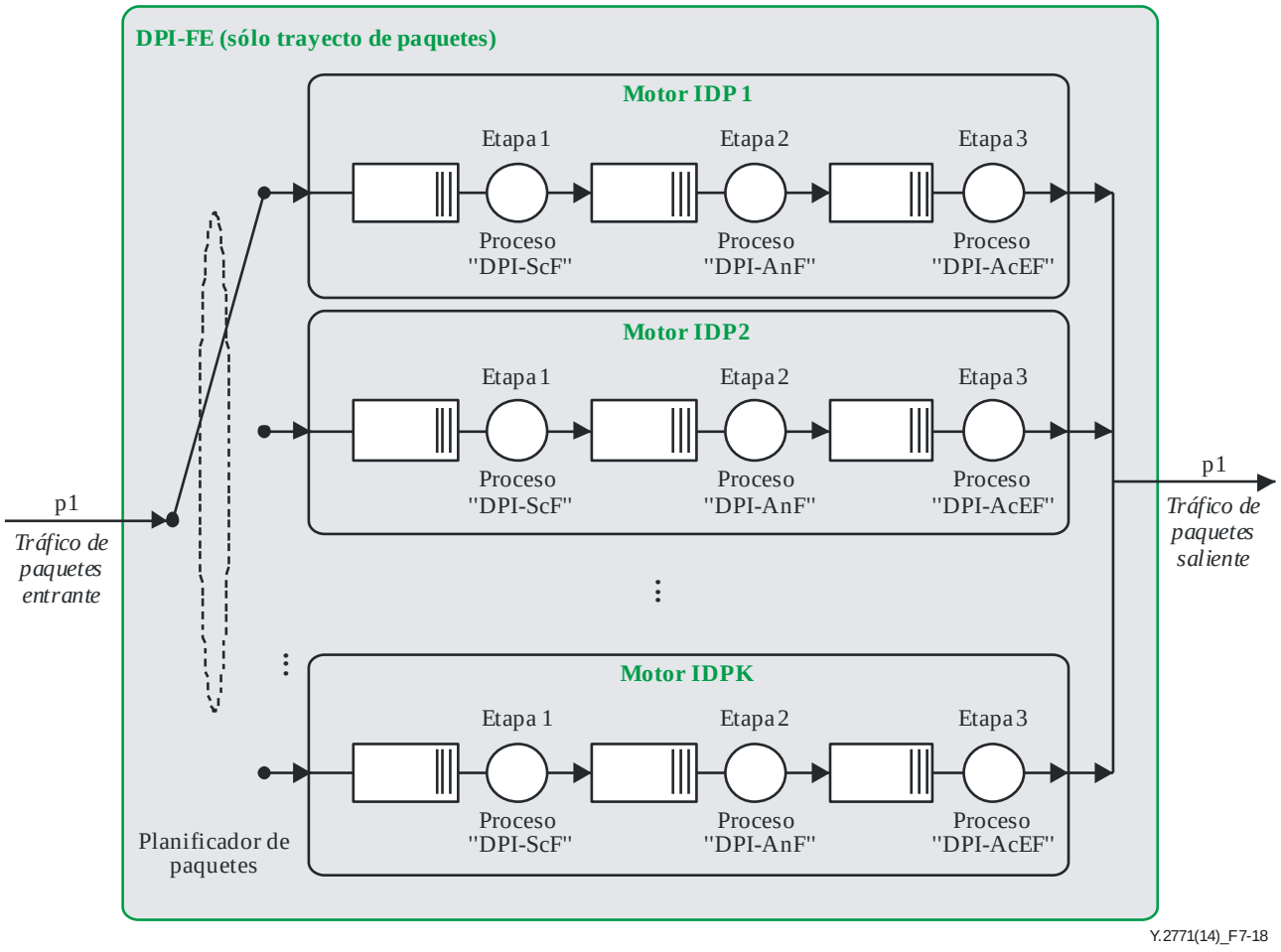


Figura 7-18 – Motores IDP en paralelo basados en modelos de servidor de 3 etapas (interfaz externa sencilla)

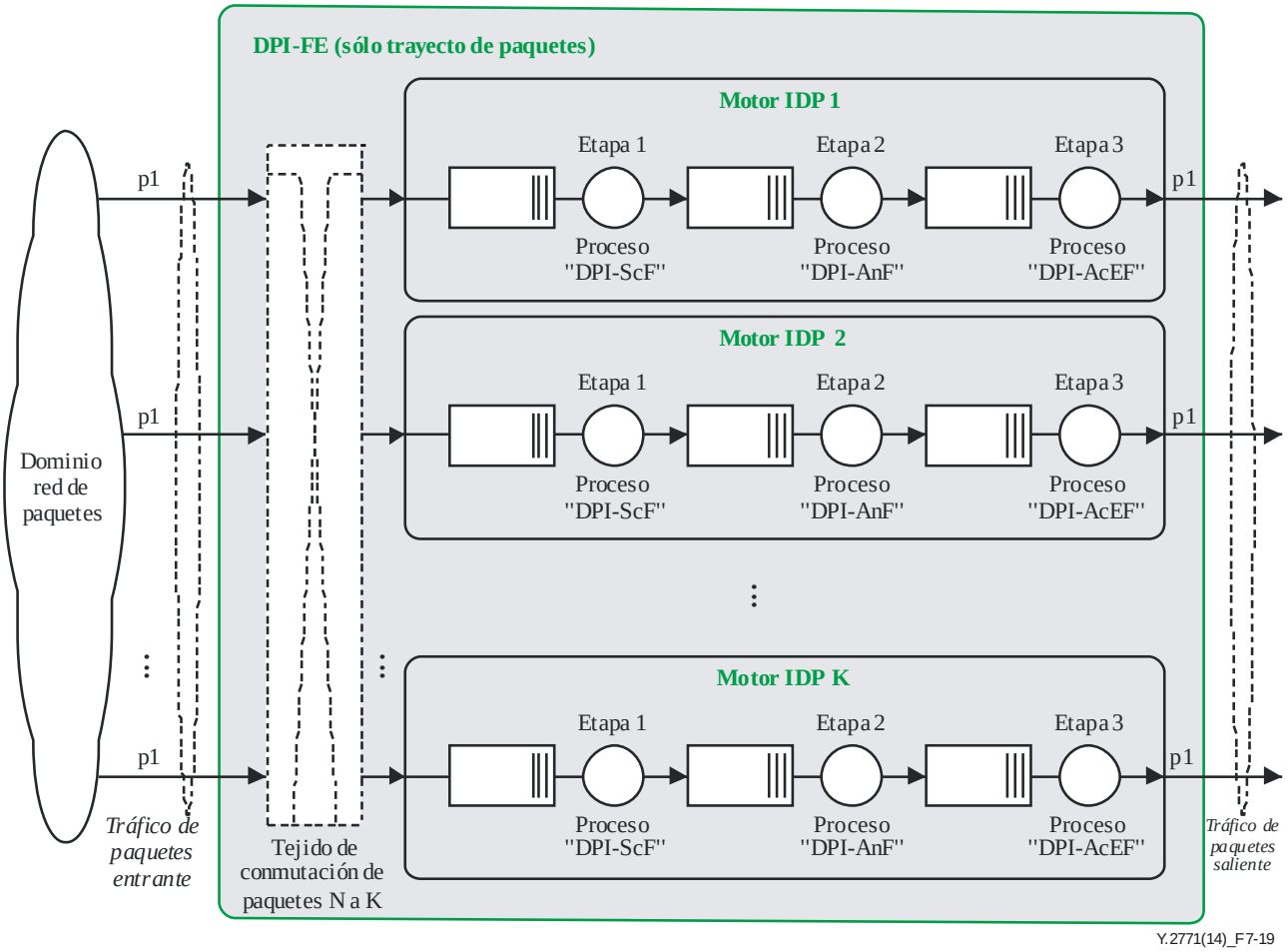


Figura 7-19 – Motores IDP en paralelo basados en modelos de servidor de 3 etapas (múltiples interfaces externas)

Los modelos de tráfico se caracterizan por motores IDP que funcionan de manera totalmente simultánea, es decir, sin interdependencias. El máximo rendimiento de esta arquitectura IDP-PE se lograría cuando la carga de todos los servidores sea "óptima" (es decir, ningún servidor está sobrecargado o infrautilizado), lo que significa una distribución homogénea de la carga en las dos dimensiones del modelo de tráfico. El diseño de esta arquitectura es bastante complejo, y quizá sólo sea posible para algunos tipos de distribuciones de tráfico en lo que respecta a la carga de paquetes ofrecida.

Partiendo de esta base se pueden crear arquitecturas diferentes, como por ejemplo la que se expone en la cláusula siguiente.

7.3.3.4 Motor IDP sencillo basado en tres etapas y paralelismo interno

Las Figuras 7-20 y 7-21 ilustran un ejemplo de este tipo de motor IDP sencillo, basado en las tres etapas de procesamiento y paralelismo por etapas. El paralelismo puede efectuarse a nivel de etapa, es decir, habrá diferentes servidores por etapa (esto es, valores diferentes de K1, K2 y K3).

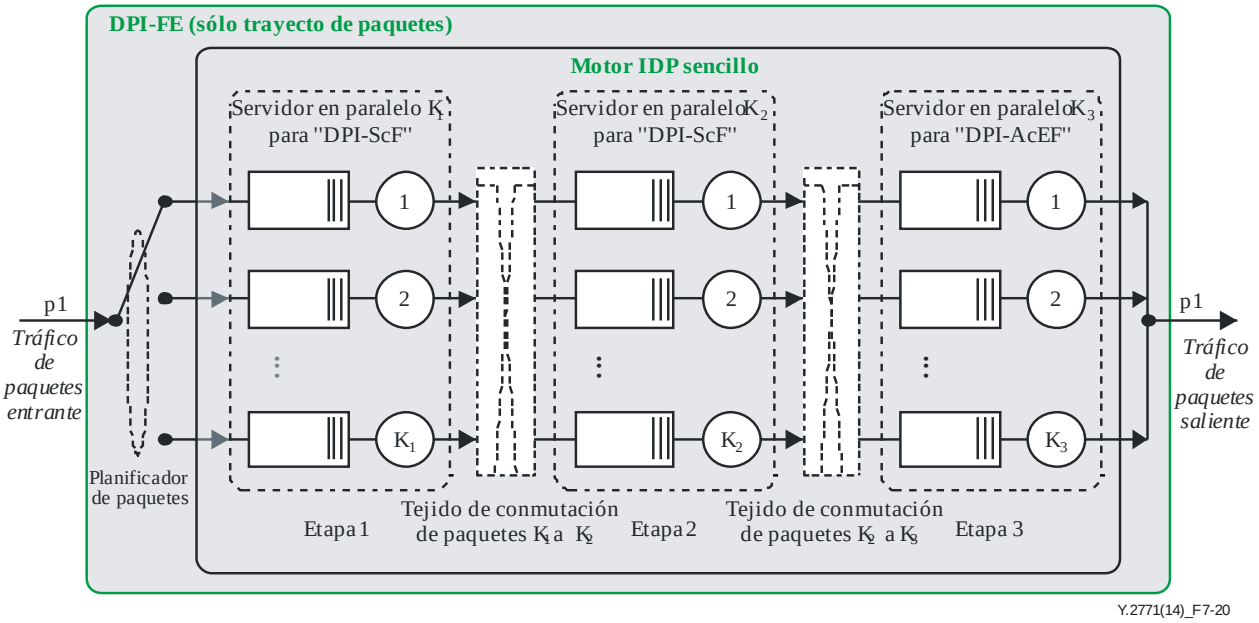


Figura 7-20 – Motor IDP sencillo basado en tres etapas y paralelismo interno (interfaz externa sencilla)

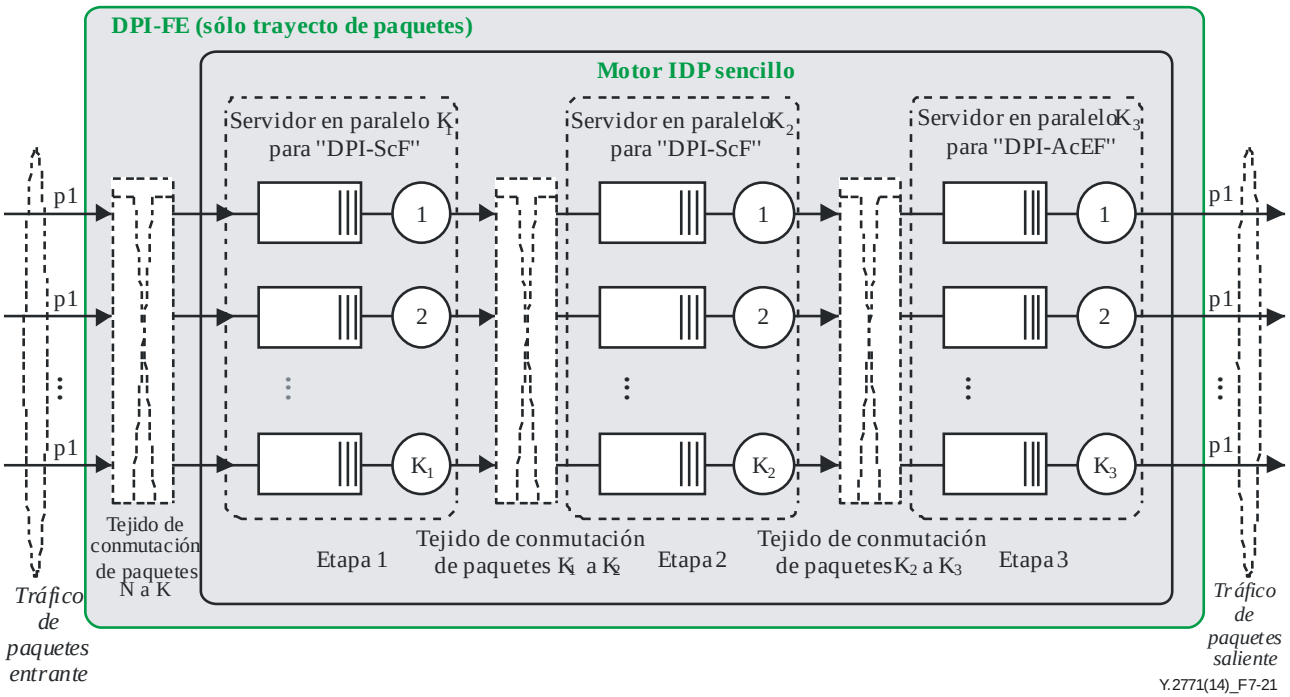


Figura 7-21 – Motor IDP basado en tres etapas y paralelismo interno (múltiples interfaces externas)

Cuando el motor IDP tiene que admitir el modo IDP con estados, es posible que se hayan de encaminar todos los paquetes del mismo flujo por el mismo trayecto de servidores, debido a la "información de estado" local. Este aspecto queda fuera del alcance del modelo de tráfico anterior.

7.4 Identificación de posibles subcomponentes de la entidad IDP-FE

Una entidad IDP-FE puede estar dividida en subcomponentes funcionales, como se ilustra por ejemplo en los modelos funcionales de las cláusulas anteriores. En el Cuadro 7-3 se resumen los subcomponentes funcionales más característicos de la entidad. La lista de componentes no es

exhaustiva, y en las cláusulas siguientes se hace referencia a los mismos (por ejemplo, cuando se examinan aspectos relativos al rendimiento, posibles requisitos funcionales u operacionales, etc.).

Cuadro 7-3 – Subcomponentes típicos de la entidad IDP-FE

Componente	Descripción
Función de aplicación de políticas IDP (IDP-PEF):	Elemento funcional que aplica reglas de política IDP y que consta al menos de una base de datos de política IDP, una función de identificación de paquetes IDP y una función de ejecución de acciones IDP
Descripción detallada de la entidad IDP-PEF: 1) Trayecto de procesamiento de paquetes	
1.1) Función de identificación de paquetes IDP (IDP-PIF) Ejemplo de descomposición funcional:	Elemento funcional responsable del procesamiento de condiciones de política IDP respecto del tráfico de paquetes entrante
1.1.1) Función de escáner IDP (IDP-ScF):	Elemento funcional (que forma parte de IDP-PIF) que realiza funciones de comparación inicial, determinadas por las condiciones de regla de política IDP
1.1.2) Función de analizador IDP (IDP-AnF):	Elemento funcional (que forma parte de IDP-PIF) que realiza las siguientes funciones de comparación, determinadas también por las condiciones de reglas de política IDP (por ejemplo, relativas a los parámetros del encabezamiento o al contenido (en las cargas útiles de paquetes))
1.2) Función de ejecución de acciones IDP (IDP-AcEF):	Elemento funcional que efectúa operaciones en los paquetes considerados, con arreglo a las acciones de reglas de política IDP identificadas
2) Función de base de datos de política IDP (IDP-PIB; Nota 1):	Elemento funcional que representa una base de datos que contiene uno o varios conjuntos de elementos de reglas de política (véase *infra*)
a) Elemento de regla de política IDP:	Elemento del cuadro que contiene una regla de política IDP (Nota 2)
i) Condición de regla de política IDP (abreviada como "condición de regla"):	Expresión (por lo general de tipo booleano). También denominada criterio de concordancia (debido, por ejemplo, a los tipos de condición que representan una concordancia parcial, completa, de prefijo, de prefijo largo, etc.)
ii) Acción de regla de política IDP (abreviada 'acción de regla'):	Acción que se ejecuta después de haber evaluado todas las condiciones de política específicas de la regla y la conclusión de dicha acción
NOTA 1 – También denominado tabla de reglas, biblioteca de signaturas de política o simplemente biblioteca de signaturas. NOTA 2 – Se pueden aplicar una o varias reglas de política. Éstas pueden estar estadísticamente predefinidas (mediante la gestión de la configuración del nodo de paquetes, denominada gestión de políticas IDP), o indicadas por señalización (a través de la interfaz de control de políticas) o generadas local y dinámicamente (por una PDF local). Las reglas de política IDP se utilizan para comparar información de control de protocolo (PCI, es decir, elementos de encabezamiento de paquetes) o cabida útil/contenido de los flujos de paquetes para una serie de condiciones a fin de determinar si hay o no concordancias.	

7.5 Modelos de tolerancia a fallos

La fiabilidad y disponibilidad de un nodo de red (por ejemplo, nodo IDP) son muy importantes para la red en la que éste se implanta. Cuando un nodo de red queda fuera de servicio (véase, por ejemplo, el modelo de estado operativo [ITU-T X.731]) las consecuencias pueden ser catastróficas para la red y puede suceder que todos los usuarios de la misma queden fuera de línea. Esta situación produciría la pérdida masiva de información valiosa. Por ese motivo, es esencial que los nodos de red tengan una alta fiabilidad y disponibilidad. En cuanto nodo de red,el nodo IDP también debe tener alta fiabilidad y disponibilidad.

Basado en el método de tolerancia a fallos, el grupo de redundancia "1+N" de IDP tiene por objeto mejorar la fiabilidad y disponibilidad de la red creada con nodos IDP.

La fiabilidad del grupo de redundancia "1+N" IDP puede calcularse mediante los siguientes parámetros:

1) MTBF: Tiempo medio entre fallos, es el tiempo medio entre dos fallos del grupo de redundancia "1+N" IDP.

2) MTTR: Tiempo medio para reparación, es el tiempo que tarda el grupo de redundancia "1+N" IDP en volver a la normalidad después de producirse un fallo.

La disponibilidad del grupo de redundancia "1+N" IDP puede calcularse mediante las siguientes fórmulas (véase [ITU-T G.602]):

3) Disponibilidad = Tiempo activo/(tiempo inactivo + tiempo activo) o

4) Disponibilidad = MTBF/(MTBF + MTTR)

5) Dentro del grupo de redundancia "1+N" IDP, el número de componentes funcionales de redundancia dependen de la realización concreta y queda fuera del alcance de la presente Recomendación. Los componentes funcionales dentro de un grupo de redundancia trabajan en modo activo/auxiliar: sólo uno de los componentes funcionales está activo, mientras que los demás componentes funcionales son auxiliares. Cuando los componentes activos quedan fuera de servicio, sólo uno de los auxiliares pasa a ser el nuevo componente funcional activo y el anterior se convierte en uno auxiliar.

6) La interfaz entre el componente funcional activo y el auxiliar, que se utiliza en la conmutación entre componentes funcionales activos y auxiliares, es independiente de la IDP y específica de la realización en concreto, por lo que queda fuera del alcance de la presente Recomendación.

7) Se presentan varios modelos de tolerancia a fallos, a saber el modelo de tolerancia a fallos a nivel de nodo IDP (cláusula 7.5.1), el modelo de tolerancia a fallos a nivel de la función IDP-PEF (cláusula 7.5.2) , el modelo de fiabilidad a nivel de la IDP-PIB (cláusula 7.5.3) y el modelo de tolerancia a fallos a nivel del motor IDP (cláusula 7.5.4).

8) Todos los modelos de tolerancia a fallos se basan en el grupo de redundancia "1+N" IDP (es decir, en la redundancia de los componentes funcionales, por ejemplo, los nodos IDP de la Figura 7-22).

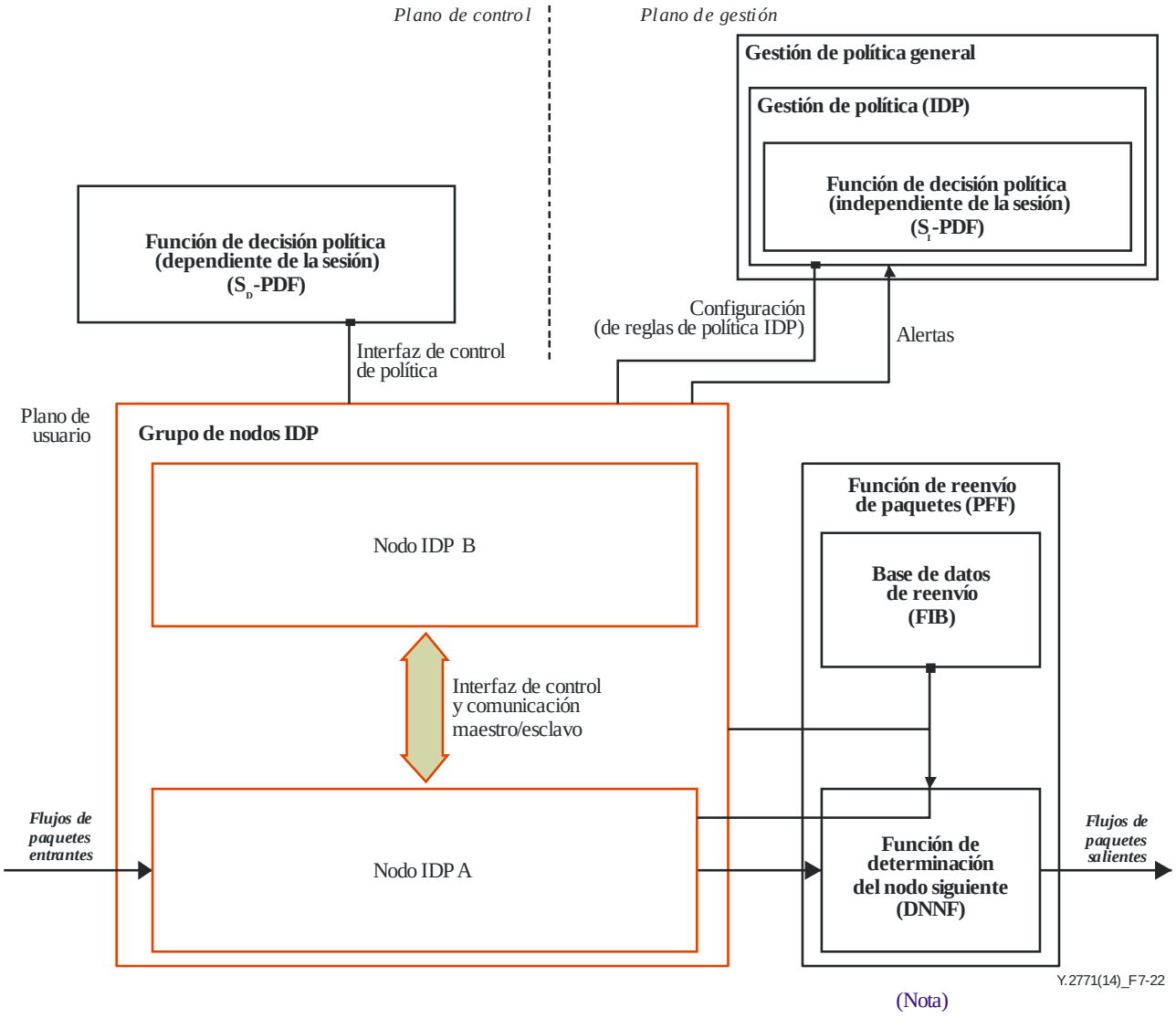
9) Los componentes funcionales activos y los auxiliares deben mantener información completamente idéntica, como la base de datos PIB, mediante el método de sincronización de datos. Este método depende de la realización en concreto y queda fuera del alcance de la presente Recomendación.

7.5.1 Modelo de tolerancia a fallos a nivel de nodo IDP

En la Figura 7-22 se ilustra un modelo IDP con fiabilidad garantizada a nivel del nodo IDP, en el que se despliegan juntos dos o más nodos IDP para crear un grupo de nodos IDP (un grupo de redundancia "1+N" IDP cuyos componentes funcionales son nodos IDP), donde un nodo IDP funciona como nodo IDP activo, mientras que los otros son nodos IDP auxiliares. Además, los

nodos IDP activos y auxiliares tienen que duplicar la información interna, como se exige para el modo de funcionamiento normal. Cuando el nodo IDP activo queda fuera de servicio, uno de los nodos IDP auxiliares se convierte automáticamente en el nodo IDP activo.

Aunque en la Figura 7-22 sólo se ilustran dos nodos IDP, el modelo de tolerancia a fallos es similar cuando hay más de dos nodos IDP (debido al concepto de redundancia "1+N").



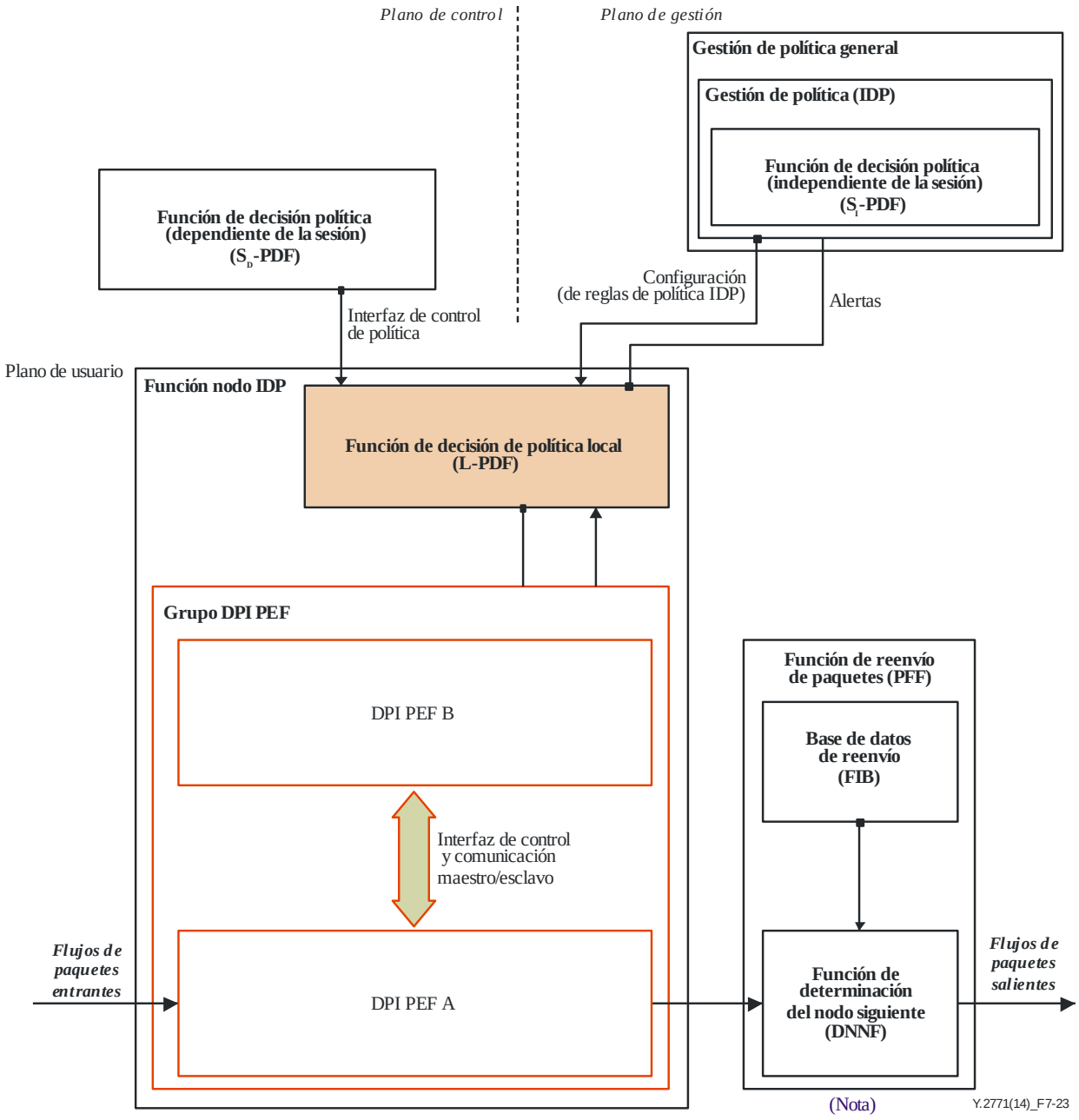
NOTA – La PFF queda fuera del alcance de la presente Recomendación.

Figura 7-22 – Modelo IDP con fiabilidad garantizada a nivel de nodo IDP

7.5.2 Modelo de tolerancia a fallos a nivel de la función IDP PEF

En la Figura 7-23 se ilustra un modelo IDP con fiabilidad a nivel de la función IDP PEF, en el que el nodo IDP consta de dos o más componentes IDP PEF (es decir, un grupo de redundancia "1+N" IDP cuyos componentes IDP PEF son componentes funcionales), un componente IDP PEF está activo mientras que los otros componentes IDP PEF son auxiliares. Los procedimientos de conmutación en caso de fallo son similares a los del nivel de fiabilidad del nodo (véase la cláusula 7.5.1).

Aunque en la Figura 7-23 sólo se ilustran dos componentes PEF, el modelo de tolerancia a fallos cuando haya más de dos componentes PEF es similar.



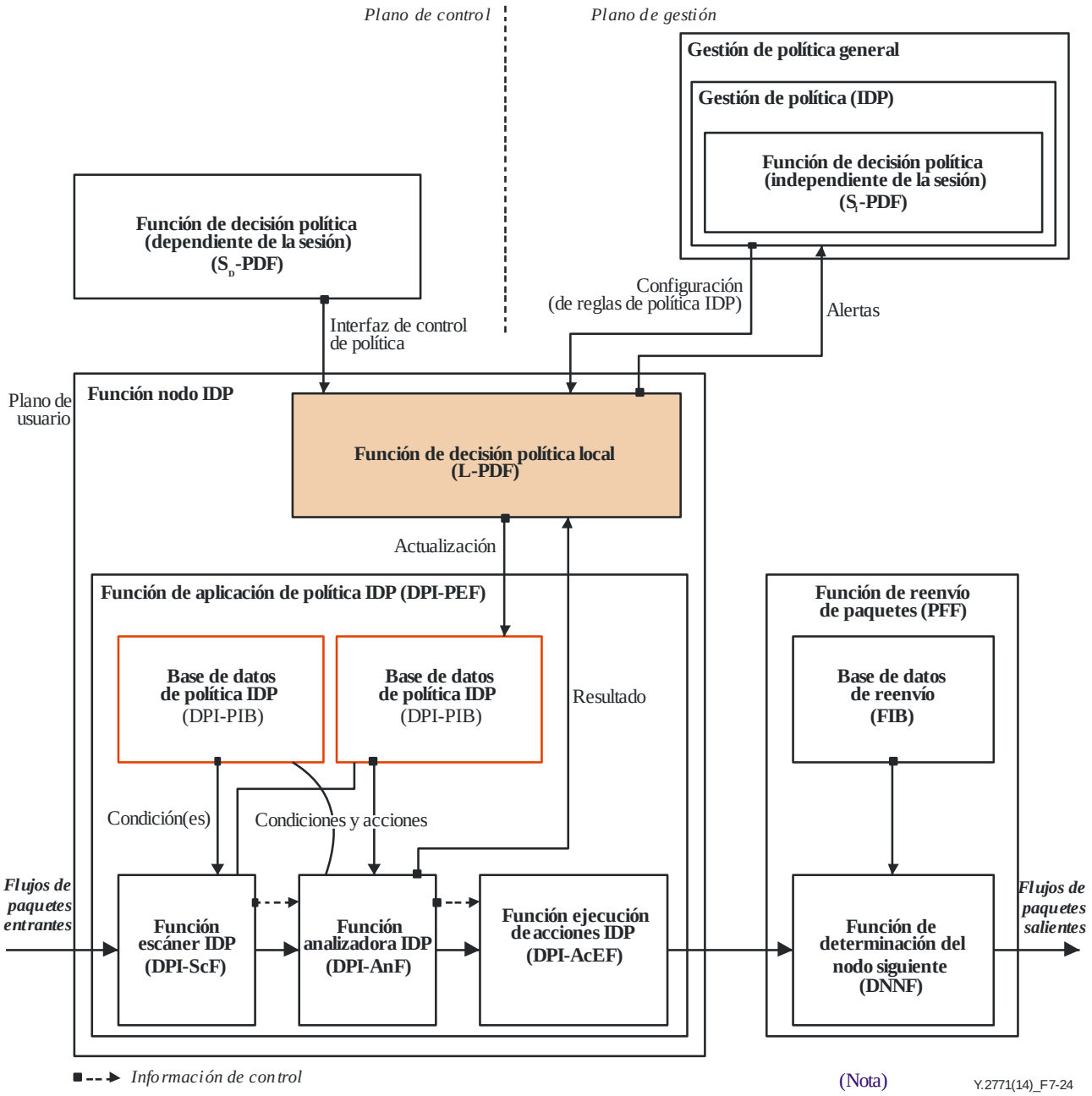
NOTA – La PFF queda fuera del alcance de la presente Recomendación.

Figura 7-23 – Modelo IDP con fiabilidad a nivel de IDP PEF

7.5.3 Modelo de tolerancia a fallos a nivel de IDP-PIB

En la Figura 7-24 se ilustra un modelo IDP con fiabilidad a nivel de IDP PIB, en el que el nodo IDP contiene dos o más copias de la base de datos IDP PIB (es decir, el grupo de redundancia "1+N" IDP está compuesto por dos o más copias de la IDP PIB), y todas las bases de datos IDP PIB están sincronizadas, por lo que contienen información idéntica. Una IDP-PIB está activa, y las demás son auxiliares. Cuando la PIB activa queda fuera de servicio, una de las PIB auxiliares pasa al modo activo.

Aunque en la Figura 7-24 sólo se ilustran dos IDP PIB, el modelo de tolerancia a fallos cuando haya más de dos IDP PIB es similar.



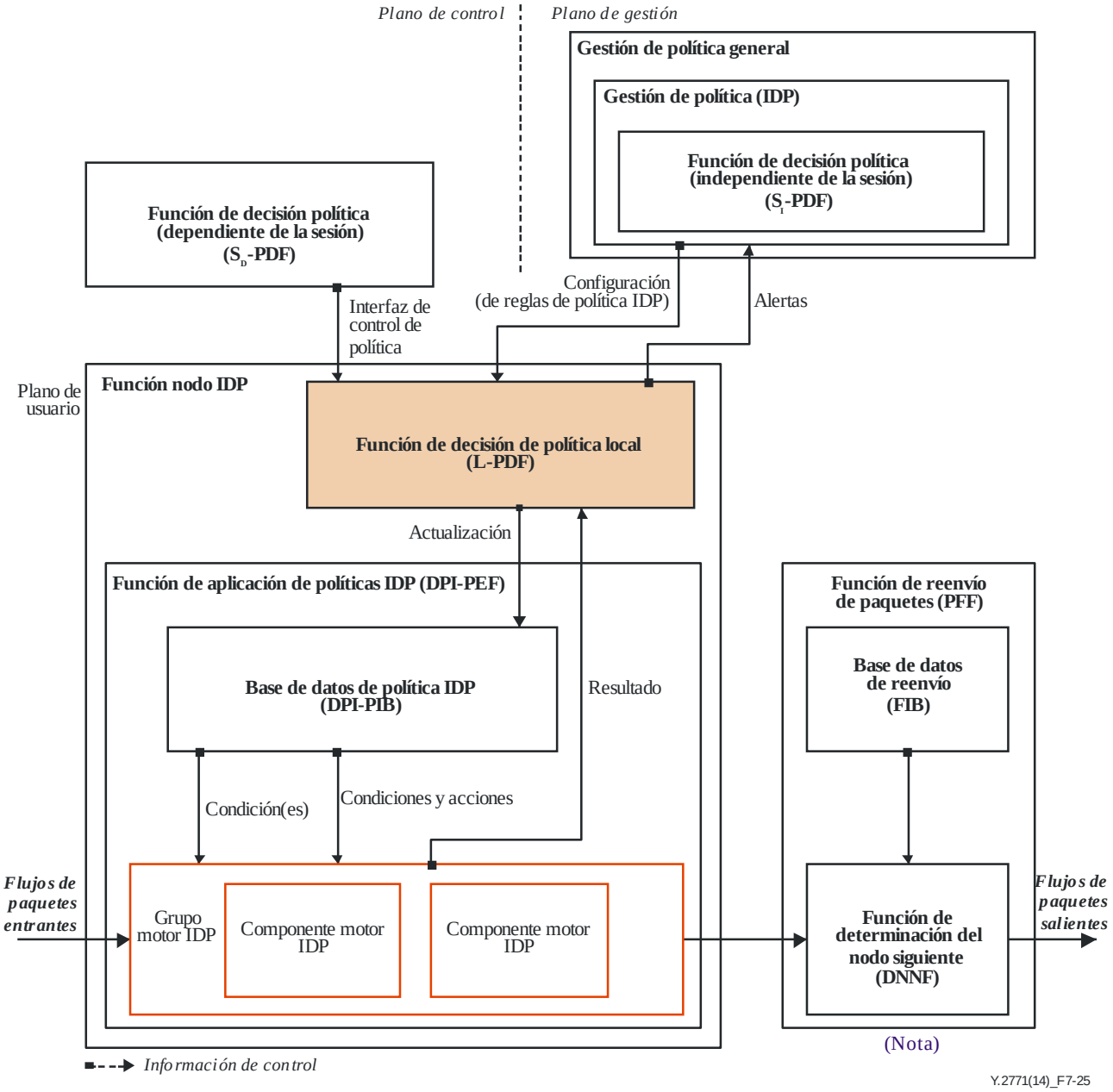
NOTA – La PFF queda fuera del alcance de la presente Recomendación.

Figura 7-24 – Modelo IDP con fiabilidad garantizada a nivel de IDP PIB

7.5.4 Modelo de tolerancia a fallos a nivel de motor IDP

La Figura 7-25 muestra un modelo IDP con fiabilidad a nivel de motor IDP. Los principios de tolerancia a fallos son idénticos a los de los modelos anteriores de niveles más altos.

Aunque en la Figura 7-25 sólo se ilustran dos componentes de motor IDP, el modelo de tolerancia a fallos cuando haya más de dos componentes de motor IDP es similar.



NOTA – La PFF queda fuera del alcance de la presente Recomendación.

Figura 7-25 – Modelo IDP con fiabilidad garantizada a nivel de motor IDP

8 Marco de rendimiento

8.1 Objetivo y alcance de las consideraciones relativas al rendimiento

En esta cláusula se describe el marco y el procedimiento para identificar y desarrollar métricas de rendimiento relativas a la IDP, que pueden utilizarse para caracterizar el comportamiento de entidades IDP.

El marco de rendimiento abarca básicamente los siguientes ámbitos:

1) Métrica de rendimiento:

   Permite caracterizar la capacidad, disponibilidad y rendimiento de una entidad IDP. El principal objetivo es:

   a) aclarar si puede reutilizarse la métrica existente de rendimiento ajena a la IDP;

b) reconocer las métricas de rendimiento específicas de la IDP, que ya han adoptado otras organizaciones que estudian la IDP;

c) identificar nuevas métricas de rendimiento específicas de la IDP, lo que implica definir tal métrica; y

d) clasificar el conjunto de métricas en indicadores fundamentales de rendimiento (IFR) y otros indicadores.

2) Requisitos de rendimiento:

Este tipo de requisitos IDP están relacionados con una determinada métrica del rendimiento. Los requisitos de calidad que dependen de la realización concreta quedan fuera del alcance de la presente Recomendación. Así, resulta posible obtener requisitos cualitativos o relativos de la calidad de funcionamiento. La especificación de requisitos cuantitativos o absolutos adicionales del rendimiento sólo es posible en determinados ámbitos (por ejemplo, si el balance del retardo máximo de transferencia en el nodo estuviese sujeto a consideraciones de red generales de extremo a extremo…).

3) Valores comparativos del rendimiento:

La determinación de valores comparativos es un campo bastante difícil en lo que respecta a la identificación y especificación de casos comparativos significativos y ampliamente reconocidos. La definición de valores comparativos del rendimiento IDP queda fuera del alcance de la presente Recomendación, aunque ésta facilita información y orientaciones sobre aspectos que se han de tener en cuenta al tratar de especificar valores comparativos del rendimiento para entidades IDP.

La definición de nuevos tipos de métrica del rendimiento (también denominados indicadores de rendimiento) debería basarse en las directrices de [b-IETF RFC 6390] y, por ende, incorporar como mínimo:

- nombre y descripción de la métrica;
- método de medición o de cálculo;
- unidad de medida; y
- una definición de la métrica de rendimiento que no esté ligada a un parámetro estadístico como el mínimo, el máximo, la media, la PDF, la varianza, etc. Estos aspectos están bastante sujetos a la especificación de requisitos.

8.2 Métrica del rendimiento

8.2.1 Descripción – Indicadores de rendimiento para los nodos IDP

Los requisitos de rendimiento están relacionados con la métrica de rendimiento. Los tipos de métrica esencial se denominan indicadores (IFR), que representan un subconjunto del conjunto global de métricas.

8.2.1.1 Directrices para clasificar como IFR la métrica del rendimiento relacionada con la IDP IFR

En la presente Recomendación se utiliza la siguiente definición de IFR (NOTA 1 – Procedente de [ETSI TS 132.410]):

- **Indicadores fundamentales de rendimiento (IFR) en general**:

  Son las métricas primarias para evaluar el rendimiento de procesos, en cuanto indicadores de la función principal del elemento de red.

- **Indicadores fundamentales de rendimiento para entidades IDP** (IFR_{IDP}):

  Un IFR_{IDP}, –en el contexto de la presente Recomendación– caracteriza, por tanto, el rendimiento del motor IDP (véase la cláusula 3.2.6 de [ITU-T Y.2770]; también conocido como trayecto de procesamiento de paquetes IDP).

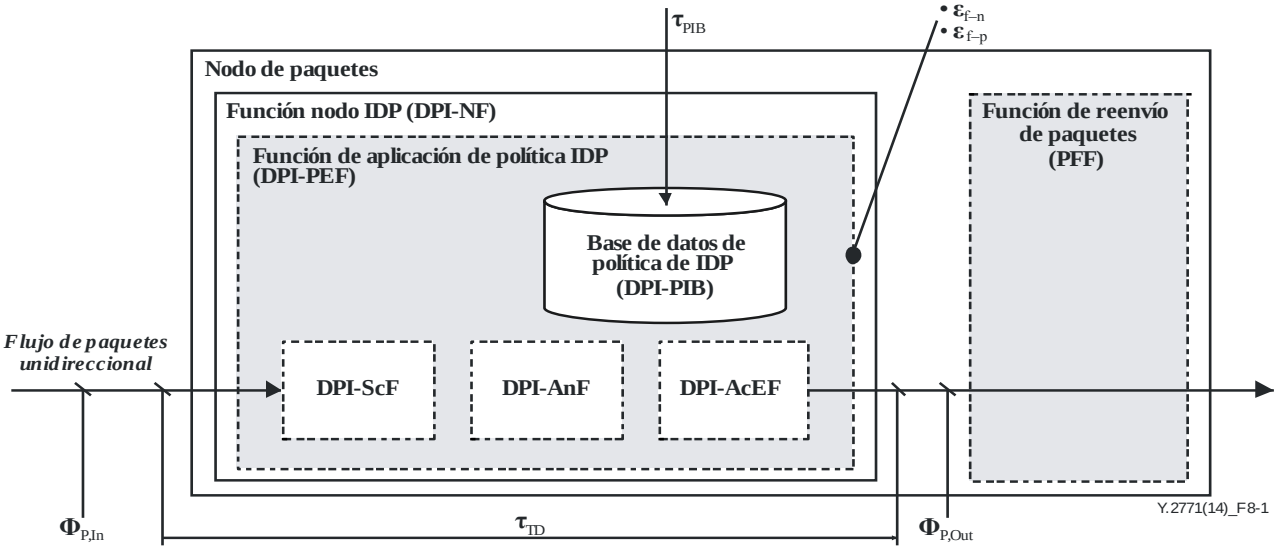
NOTA 2 – En la presente Recomendación el concepto de indicador de rendimiento (IR) es sinónimo de métrica de rendimiento.

A los efectos de clasificar la métrica del rendimiento IDP en IFR y no IFR, deberían tomarse en consideración los siguientes criterios. El IFR para entidades IDP debería cumplir las siguientes condiciones:

1) la métrica del rendimiento debe estar vinculada con el propio trayecto de procesamiento de paquetes, donde se aplican las reglas de política IDP a objetos de paquete (por tanto, no se requiere ninguna otra función IDP fuera del trayecto de paquetes IDP); y
2) la métrica del rendimiento debe ser independiente del caso de utilización de la IDP (es decir, que no dependa de la aplicación específica de servicios IDP en particular); y
3) la métrica del rendimiento debe ser independiente de protocolos específicos inferiores y superiores a la capa IP (por tanto, no es específica de un determinado protocolo de transporte IP (como el TCP), el protocolo de aplicación IP, etc.); y
4) la métrica de rendimiento debe ser independiente de la realización física de las entidades (por consiguiente, no debe guardar relación con aspectos específicos de la implementación, tales como el consumo de energía, la disipación de potencia, los componentes de procesamiento modernos, etc.).

8.2.1.2 Indicadores fundamentales de rendimiento más comunes para los nodos IDP

En la Figura 8-1 se ilustran varios IFR bien conocidos para nodos IDP (la lista de IFR_{IDP} no es exhaustiva). Los tipos de IFR_{IDP} se enumeran en el siguiente diagrama. Los correspondientes requisitos de rendimiento (en su caso) se describen en cláusulas separadas.



NOTA 1 – El nodo de paquetes y la función PFF se muestran para un especificación inequívoca de la métrica de rendimiento, pero ambas entidades quedan fuera del alcance de la presente Recomendación.
NOTA 2 – la PFF solamente figura en el modo IDP en el trayecto.

Figura 8-1 – Descripción general – Indicadores fundamentales de rendimiento para nodos IDP

Las principales métricas del rendimiento suelen ser las siguientes:

- IFR "(IDP) **retardo de transferencia interno del nodo**" τ_{TD} [µs]: véase la cláusula 8.2.3.1.
- IFR "(IDP) **velocidad de procesamiento de paquetes**" $\phi_{P,In}[s^{-1}]$: véase la cláusula 8.2.3.2.
- IFR "(IDP) **tasa de errores**" ε_{IDP}: véase la cláusula 8.2.3.3.
  - IFR "(IDP) **tasa de errores de falsos positivos**" $\varepsilon_{f\text{-}p}$.
  - IFR "(IDP) **tasa de errores de falsos negativos**" $\varepsilon_{f\text{-}n}$.
- IFR "(IDP) **velocidad de paquetes identificados satisfactoriamente**" $\phi_{P,Identified}[s^{-1}]$: véase la cláusula 8.2.3.4.

8.2.2 Plantilla oficial para la definición de métricas del rendimiento

Las definiciones de métrica de rendimiento en la presente Recomendación se utilizan en la plantilla del Cuadro 8-1, que a su vez procede de la plantilla del IETF, con arreglo a la cláusula 5.4.4 de [b-IETF RFC 6390] "Plantilla para la definición de métricas del rendimiento".

Cuadro 8-1 – Plantilla oficial para la definición de métricas del rendimiento

Nombre de la métrica:	N	
Símbolo:	I	
Descripción de la métrica:	N	
Método de medición o cálculo:	N	
Unidades de medida:	N	
Puntos de medición en el posible dominio de medición:	N	
Tiempo de medición:	N	
Realización:	I	
Verificación:	I	
Usos y aplicaciones:	I	Por ejemplo, "IDP en tiempo real", "IDP en tiempo no real"
Modelo de notificación:	I	
De tipo "IFR": ¿sí/no?	I	Es decir, "IFR", "no IFR" o "sin clasificar"
NOTA – N: elemento de descripción normativa; I: elemento de descripción informativa.		

La plantilla se utiliza para garantizar una mínima calidad de especificación en las métricas descritas en la presente Recomendación. Ahora bien, en primer lugar se presentan los elementos cuya descripción es *normativa* debido al "tipo de marco" de esta Recomendación. Los elementos cuya descripción está vacía (*informativa*) indican que la utilización de esta métrica en un especificación real del rendimiento requeriría una labor de especificación previa para obtener una métrica aplicable y completa. Por ejemplo, la descripción de la "realización" queda fuera del alcance de la Recomendación "marco", o una definición de métrica sin la información de "verificación" resulta inútil (porque se requiere, por ejemplo, para calibrar la función de medición).

8.2.3 Definiciones generales de la métrica de rendimiento para entidades IDP

8.2.3.1 Métrica IDP "retardo de transferencia interna del modo"

Las reglas de política relativa a la IDP se aplican por separado a cada paquete de un flujo de paquetes. Este tipo de aplicación de política introduce un tiempo de espera y de servicio adicional en el trayecto de reenvío de un nodo de paquetes (por ejemplo, un tramo IP) con soporte de "motor IDP" (es decir, un punto de aplicación de políticas (PEP) que ofrece IDP). El retardo de transferencia interna del nodo de la métrica del rendimiento representa el retardo de trasferencia de paquetes que introduce el propio elemento de red.

En el Cuadro 8-2 figura la definición de la métrica.

Cuadro 8-2 – "Retardo de transferencia interno del nodo" de la métrica IDP

Nombre de la métrica:	N	retardo de transferencia interno del nodo
Símbolo:	I	τ_{TD}
Descripción de la métrica:	N	La suma de los tiempos de espera y de servicio de un paquete a través del nodo IDP
Método de medición o cálculo:	N	Este valor se calcula midiendo los tiempos de entrada y salida ($T_{in,i}$ y $T_{out,i}$) de cada paquete en cada una de las interfaces de una representación física o lógica de una función de nodo IDP. Condición: la entidad de medición debe ser capaz de identificar paquetes individuales. Atención: esta métrica suele depender de la carga, dado que el *retardo de transferencia* interno del nodo está compuesto por los *tiempo de servicio* y *de espera*. La carga, o más precisamente la carga IDP $A_{IDP\text{-}NF}$, viene dada por la velocidad de llegada de paquetes $\phi_{P,In}$ y el tiempo medio de servicio por paquete $T_{H,Packet}$ según la expresión: $$A_{DPI-NF} = \phi_{P,In} \cdot T_{H,Packet}$$ Dependencia principal de la carga (véase también la cláusula 8.3): $$\tau_{TD} = f(A_{DPI-NF})$$
Unidades de medida:	N	ns
Puntos de medición en el posible dominio de medición:	N	Véase la Figura 8-1 (modelo de tráfico)
Tiempo de medición:	N	Esta métrica puede utilizarse en una gran variedad de intervalos de tiempo
Realización:	I	–
Verificación:	I	–
Usos y aplicaciones:	I	"IDP en tiempo real"
Modelo de notificación:	I	Normalmente forma parte de la gestión del rendimiento
De tipo "IFR": ¿sí/no?	I	"IFR"
NOTA – N: elemento de descripción normativa; I: elemento de descripción informativa.		

8.2.3.1.1 Análisis en profundidad

a) Nodos IDP respecto a nodos no IDP:

Ejemplo de nodo IP: el retardo de transferencia de un nodo IDP puede ser fundamentalmente mayor que el retardo de transferencia de un nodo IP tradicional (es decir, un tramo IP o un encaminador según [b–IETF RFC 1812]) debido a la función de servicio adicional por encima de la funcionalidad de reenvío IP nativa.

b) Relaciones características:

El retardo de transferencia interno del nodo τ_{TD} puede depender (en función de la realización concreta) de los siguientes parámetros:

– número de reglas de política IDP N_{db} (por ejemplo, mayor tiempo de servicio cuando varias reglas de política IDP se aplican en serie);

– el tamaño del paquete *Sp*[bit] (por ejemplo, mayor tiempo de búsqueda o comparación al verificar las condiciones de política IDP), que puede estar relacionado con el valor del tamaño de trama L2 que figura en [b-IETF RFC2544]; y

– el número de motores IDP N_{IDPeng} (por ejemplo, la consideración de paralelismos internos, véase la cláusula 7.3.3).

Así, en este ejemplo, τ_{TD} será una función de los parámetros *Ndb, Sp* y N_{IDPeng}, es decir:

$$\tau_{TD} = f(N_{db}, S_P, N_{DPleng})$$

Por consiguiente, los tres parámetros influyen en el tiempo medio de servicio por paquete $T_{H,Packet}$ (como se indica en el Cuadro 8-3): los dos primeros parámetros son factores que lo aumentan, mientras que el tercero reduce el tiempo medio de servicio.

c) Requisitos de rendimiento cualitativo:

El retardo de transferencia (inclusive el tiempo de servicio adicional debido al procesamiento IDP) no deberá rebasar los requisitos de tiempo real de extremo a extremo relativos al servicio de comunicación general.

NOTA 1 – Esta capacidad de reenvío de paquetes también se conoce coloquialmente con el nombre de "procesamiento de velocidad alámbrica".

NOTA 2 – Este objetivo de rendimiento puede limitar el número de reglas de política aplicadas por paquete (debido precisamente al limitado balance de tiempo de servicio).

8.2.3.2 Métrica IDP "velocidad de procesamiento de paquetes"

En el Cuadro 8-3 se indica la definición de la métrica.

Cuadro 8-3 – Métrica IDP "velocidad de procesamiento de paquetes"

Nombre de la métrica:	N	Velocidad de procesamiento de paquetes
Símbolo:	I	$\phi_{P,In}$
Descripción de la métrica:	N	Velocidad de paquetes, procesados por la función IDP-PEF. Se trata de la velocidad de entrada de paquetes, dado que las reglas de política IDP se aplican a cada paquete entrante. La velocidad de salida es igual o inferior a la velocidad de entrada (debido al posible descarte de paquetes), $\phi_{P,In} \leq \phi_{P,Out}$
Método de medición o cálculo:	N	Número de paquetes que entran por la interfaz *p1* durante un periodo de tiempo. El valor se calcula dividiendo el número por el intervalo de tiempo
Unidades de medida:	N	s^{-1}
Puntos de medición en el posible dominio de medición:	N	Véase la Figura 8-1 (modelo de tráfico)
Tiempo de medición:	N	Esta métrica se utiliza principalmente en una amplia gama de intervalos de tiempo. El intervalo de tiempo suele ser del orden de unos segundos
Realización:	I	–
Verificación:	I	–
Usos y aplicaciones:	I	"IDP en tiempo real"
Modelo de notificación:	I	Por lo general forma parte de la gestión del rendimiento
De tipo "IFR": ¿sí/no?	I	"IFR"
NOTA – N: elemento de descripción normativa; I: elemento de descripción informativa.		

La velocidad de procesamiento de paquetes IDP ϕ_P, depende de muchos parámetros, por ejemplo la combinación de:

– el número de reglas de política IDP, o el tamaño de la base de datos IDP PIB, *Ndb*,

– el tamaño del paquete, *Sp*, que puede estar relacionado con los valores del tamaño de trama L2 estipulados en [b-IETF RFC2544], y

– otros posibles parámetros.

Ejemplo: Cuando $(\phi_P, N_{db}, Sp) = (200, 1000, 64)$, la velocidad de procesamiento es como mínimo de 200 paquetes/segundo, para un número de reglas de política inferior a 1000 y un tamaño de paquete de 64.

El comportamiento cualitativo se describe en la cláusula 8.3. La actualización de la base de datos IDP-PIB ya sea la adición, supresión o modificación de reglas de política IDP, no afecta a la *velocidad de procesamientos* nominal de paquetes IDP ϕ_P (siendo ϕ_P igual a $\phi_{P,In}$).

8.2.3.3 Métrica IDP "tasa de errores"

La suma de los *falsos negativos* y los *falsos positivos* está relacionada con la tasa de errores de un nodo IDP. Estas métricas de rendimiento sólo guardan relación con decisiones *estadísticas* (en su caso) de un nodo IDP. La función IDP-PEF proporciona el comportamiento determinístico para la gran mayoría de reglas de política IDP, aunque algunas reglas de política IDP con condiciones de política estadísticas o flujos de paquetes con información estadística del tráfico pudieran dar lugar a decisiones incorrectas de la IDP-PEF.

En el Cuadro 8-4 se indica la definición de la métrica.

Cuadro 8-4 – Métrica IDP "tasa de errores"

Nombre de la métrica:	N	Tasa de errores
Símbolo:	I	ε_{IDP}
Descripción de la métrica:	N	Suma de *falsos negativos* (véase la cláusula 8.2.3.3.1) y *falsos positivos* (véase la cláusula 8.2.3.3.2) del nodo IDP
Método de medición o cálculo:	N	Medición directa: imposible (Nota 2) Medición indirecta (cálculo): $\varepsilon_{DPI} = \varepsilon_{f-n} + \varepsilon_{f-p}$
Unidades de medida:	N	–
Puntos de medición en el posible dominio de medición:	N	Véase la Figura 8-1 (modelo de tráfico)
Tiempo de medición:	N	El intervalo de medición depende de la escala de tiempo desde la perspectiva del usuario del servicio (Nota 3)
Realización:	I	–
Verificación:	I	–
Usos y aplicaciones:	I	"IDP en tiempo real"
Modelo de notificación:	I	Suele formar parte de la gestión del rendimiento
De tipo "IFR": sí/no?	I	"IFR"
NOTA 1 – N: elemento de descripción normativa; I: elemento de descripción informativa. NOTA 2 – Esta métrica de rendimiento se denomina también métrica *compuesta*, es decir, no puede medirse directamente, pero puede obtenerse a partir de métricas *de base* medidas previamente (véase la cláusula 5.3.1 de [b-IETF RFC 6390]). NOTA 3 – El usuario del servicio en general representa una entidad remota ("el usuario"), interesado en las mediciones. Ejemplos: sistema de gestión del rendimiento, entidad IDP PD-FE.		

8.2.3.3.1 Métrica IDP "tasa de errores de falso positivo"

En el Cuadro 8-5 se describe la definición de la métrica.

Cuadro 8-5 – Métrica IDP "tasa de errores de falsos positivos"

Nombre de la métrica:	N	Tasa de errores de falsos positivos
Símbolo:	I	$\varepsilon_{f\text{-}p}$
Descripción de la métrica:	N	Proporción de resultados negativos notificados por error como positivos
Método de medición o cálculo:	N	Las mediciones de esta métrica son inherentemente difíciles, por lo que en la presente Recomendación sólo se dan algunas indicaciones: Normalmente, un patrón conocido de una serie suficientemente larga de paquetes se envía a la entidad IDP. El resultado *esperado* (de aplicar las reglas de política IDP) se compara con los resultados *medidos* en el proceso IDP. La medición puede ser intrusiva o no
Unidades de medida:	N	–
Puntos de medición en el posible dominio de medición:	N	Véase la Figura 8-1 (modelo de tráfico)
Tiempo de medición:	N	El intervalo de medición depende de la escala de tiempo desde la perspectiva del usuario del servicio
Realización:	I	–
Verificación:	I	–
Usos y aplicaciones:	I	"IDP en tiempo real"
Modelo de notificación:	I	Suele formar parte de la gestión del rendimiento
De tipo "IFR": ¿sí/no?	I	Sí
NOTA – N: elemento de descripción normativa; I: elemento de descripción informativa.		

Ejemplo 1:

Una condición de política IDP C_i implica la identificación de una "aplicación de tipo *X*" y la función de identificación de paquetes (IDP-PIF) identifica a un determinado paquete de la "aplicación de tipo Y" como perteneciente a la "aplicación de tipo *X*", lo que constituye un falso positivo.

Ejemplo 2:

El cálculo de esta métrica es posible para la IDP probabilística basada en el filtro bloom (véase el Apéndice I). Dado un filtro bloom con los siguientes valores de los parámetros:

- m = tamaño del filtro bloom en bits
- n = número de signaturas en el conjunto S
- k = número de funciones de aleatorización utilizadas para generar el filtro bloom.

La tasa de falsos positivos, $\varepsilon_{f\text{-}p}$, viene dada por la ecuación:

$$\varepsilon_{f-p} = \left(1 - e^{-kn/m}\right)^k$$

Así, el resultado calculado y el previsto se pueden verificar midiendo.

8.2.3.3.2 Métrica IDP "tasa de errores de falsos negativos"

En el Cuadro 8-6 se indica la definición de la métrica.

Cuadro 8-6 – Métrica IDP "tasa de errores de falsos negativos"

Nombre de la métrica:	N	Tasa de errores de falsos negativos
Símbolo:	I	$\varepsilon_{f\text{-}n}$
Descripción de la métrica:	N	Proporción de resultados positivos notificados por error como negativos
Método de medición o cálculo:	N	Véase el elemento correspondiente en el Cuadro 8-5
Unidades de medida:	N	–
Puntos de medición en el posible dominio de medición:	N	Véase la Figura 8-1 (modelo de tráfico)
Tiempo de medición:	N	El intervalo de medición depende de la escala de tiempo desde la perspectiva del usuario del servicio
Realización:	I	–
Verificación:	I	–
Usos y aplicaciones:	I	"IDP en tiempo real"
Modelo de notificación:	I	Suele formar parte de la gestión del rendimiento
De tipo "IFR": sí/no?	I	Sí
NOTA – N: elemento de descripción normativa; I: elemento de descripción informativa.		

Ejemplo:

> La condición de política IDP C_i implica la identificación de "aplicación de tipo *X*" y la función de identificación de paquetes IDP (IDP-PIF) no identifica un paquete de la "aplicación de tipo *X*" como perteneciente a la "aplicación de tipo *X*", lo que constituye un falso negativo.

8.2.3.3.3 Relación con los errores en tiempo de ejecución

El motor IDP, en cuanto entorno de ejecución de reglas de política IDP, no está inherentemente libre de errores. Ahora bien, la tasa de errores en tiempo de ejecución y la métrica IDP "tasa de errores" constituyen dos indicadores diferentes del rendimiento.

Introducción:

Por ejemplo, el evento de excepción en tiempo de ejecución según la cláusula 4.1 de [b-IETF RFC 4011] ofrece información acerca del concepto de errores en tiempo de ejecución:

> […] Excepción en tiempo de ejecución (RTE) – **Error** fatal que se produce en el procesamiento del lenguaje o la función. Si al llamar un programa (script), se produce una excepción en tiempo de ejecución, la ejecución de tal programa termina de inmediato. Si una condición de política experimenta una excepción en tiempo de ejecución durante el procesamiento de un elemento, éste no cumplirá dicha condición y no se ejecutará la acción correspondiente sobre dicho elemento. […]

8.2.3.4 Métrica IDP "tasa de paquetes identificados satisfactoriamente"

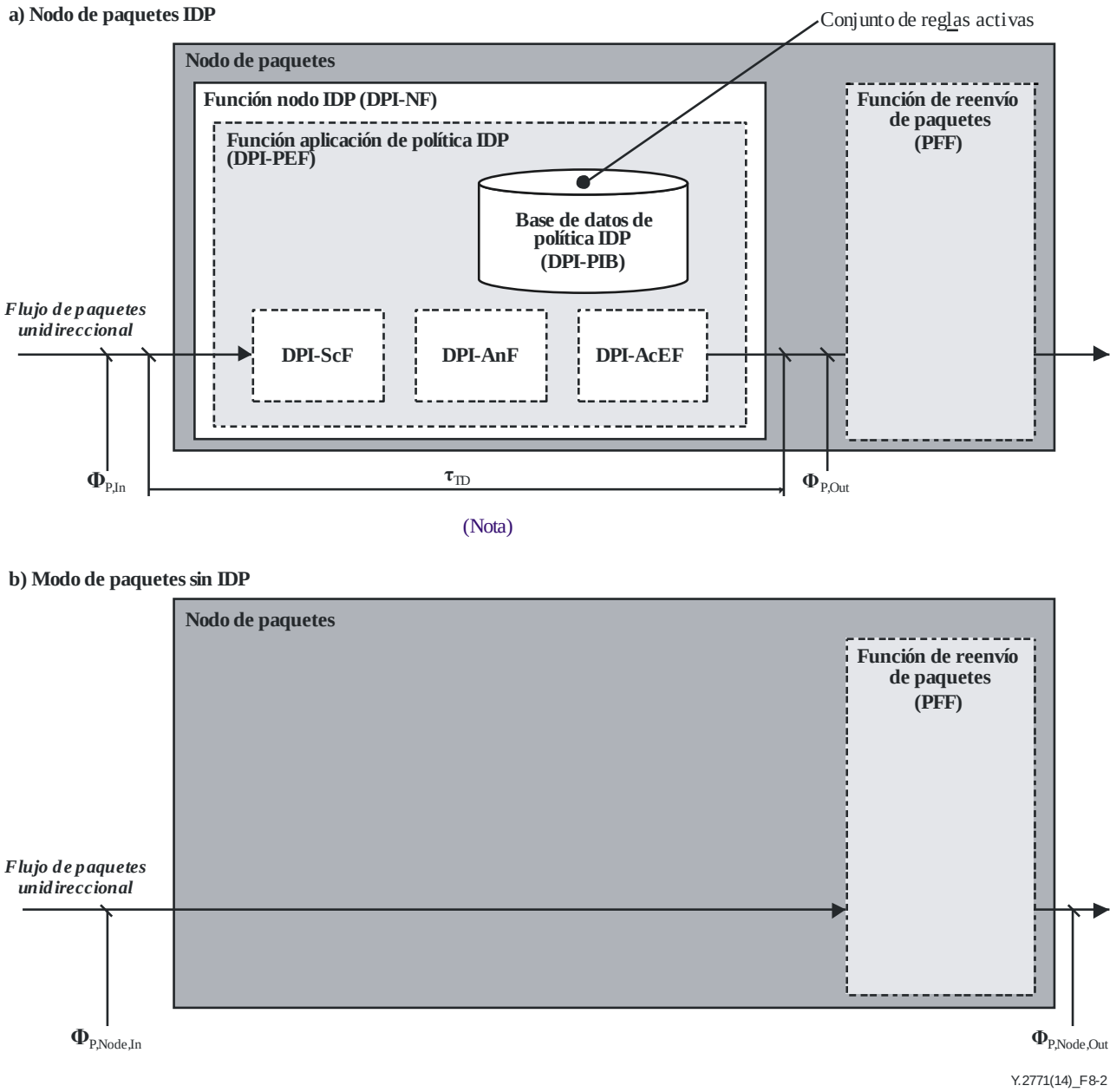
En el Cuadro 8-7 se indica la definición de la métrica.

Cuadro 8-7– Métrica IDP "tasa de paquetes identificados satisfactoriamente"

Nombre de la métrica:	N	Tasa de paquetes identificados satisfactoriamente
Símbolo:	I	$\phi_{P,\text{Identified}}$
Descripción de la métrica:	N	Un paquete entrante se ha "identificado satisfactoriamente" (por la función de identificación de paquetes) cuando las condiciones de la regla de política IDP (para al menos una regla de política IDP) "concuerdan" para el paquete inspeccionado. El tipo de "concordancia" (total, parcial, determinística, con probabilidad, etc.) no se especifica. La "tasa" se refiere al número de paquetes identificados satisfactoriamente por unidad de tiempo
Método de medición o cálculo:	N	1. Medición directa: Por ejemplo: aplicación de una conocida regla de política IDP y generación de un flujo de paquetes de características conocidas (es decir, cuya relación de tráfico que debe concordar (o no) se conoce de antemano). El valor medido se compara luego con el valor nominal. 2. Medición indirecta (cálculo): $\phi_{P,Identified} = \phi_{P,In} \cdot (1 - \varepsilon_{DPI})$
Unidades de medida:	N	s^{-1}
Puntos de medición en el posible dominio de medición:	N	Véase la Figura 8-1 (modelo de tráfico)
Tiempo de medición:	N	El intervalo de medición depende de la escala de tiempo desde la perspectiva del usuario del servicio
Realización:	I	–
Verificación:	I	Véase el método anterior de "medición directa"
Usos y aplicaciones:	I	"IDP en tiempo real"
Modelo de notificación:	I	Suele formar parte de la gestión del rendimiento
De tipo "IFR": ¿sí/no?	I	"IFR"
NOTA – N: elemento de descripción normativa; I: elemento de descripción informativa.		

8.3 Rendimiento de los puntos de aplicación de política, estimación del comportamiento del rendimiento cualitativo

La finalidad de esta cláusula es ofrecer información complementaria sobre las estimaciones de rendimiento cualitativo para la aplicación de políticas dependientes de la capa del protocolo. La Figura 8-2 muestra un nodo de paquetes (a) con una función de nodo IDP y (b) sin aplicación de IDP. El indicador fundamental de rendimiento considerado en este caso es el caudal del nodo de paquetes $\phi_{P,Node,Out}$.



NOTA – El nodo de paquetes y la función PFF se muestran para una especificación inequívoca de la mé trica de rendimiento, pero ambas entidades quedan fuera del alcance de la presente Recomendación.

Figura 8-2 – Rendimiento de aplicación de políticas – caudal del nodo de paquetes $\phi_{P,Node,Out}$ en función del conjunto de reglas de política aplicadas $\underline{\underline{R}}$ por paquetes

La Figura 8-3 ilustra algunas de las principales curvas del caudal. La función de aplicación de política específica (eje y) se caracteriza por el número de reglas de política $\underline{\underline{R}}$ por paquete y por los aspectos de interacción de reglas. La aplicación de una regla de política particular consume determinados recursos del trayecto de paquetes en cuanto a tiempo de procesamiento, memoria de paquetes, memoria TCAM/CAM, bases de datos de política, etc.

La norma simplificada es: "cuantas más reglas por paquete se hayan de aplicar, más recursos requerirá la aplicación de políticas".

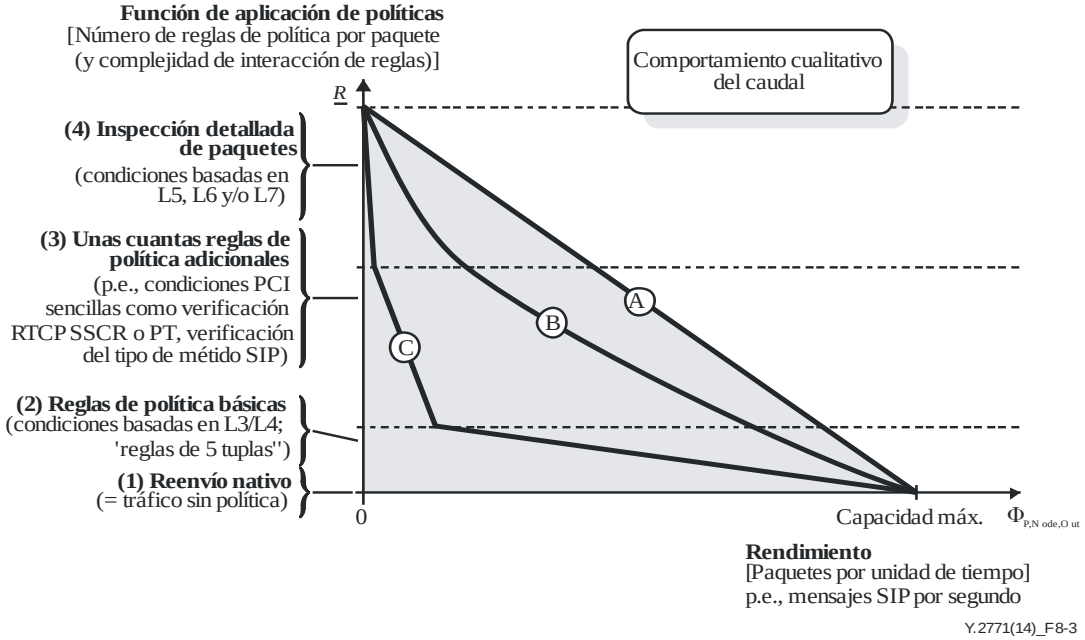


Figura 8-3 – Rendimiento de aplicación de políticas – Comportamiento cualitativo del caudal

Una realización ideal lograría un comportamiento "lineal" como la curva *A*. En cambio, un modelo más realista y costoeficiente seguiría la curva *C*.

La dificultad técnica (y comercial) de logar el comportamiento *C* es que la relación es *no lineal*, véase la Figura 8-4, y no es nada trivial diseñar un punto de carga nominal y/o lograr el equilibrio necesario para limitar las reglas de política aplicadas.

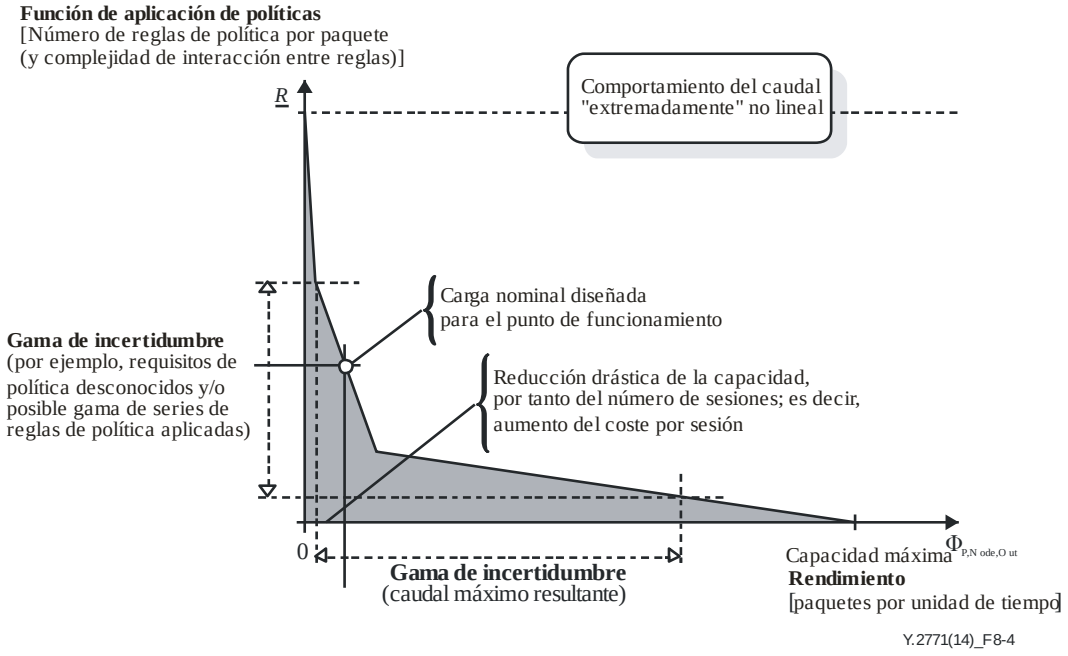


Figura 8-4 – Rendimiento de aplicación de políticas – Ejemplo de utilización de la curva *C* en el caso más desfavorable

9 Clasificación de entidades funcionales IDP

Las entidades IDP no suelen soportar todo el conjunto de requisitos IDP según [ITU-T Y.2770], sino solamente un subconjunto determinado por la utilización prevista. Por consiguiente, se puede distinguir entre diferentes tipos de entidades IDP-FE.

9.1 Principios de clasificación

Cada capacidad identificable de una entidad IDP podría vincularse con requisitos IDP, como se especifica en [ITU-T Y.2770]. A alto nivel existen:

- capacidades de procesamiento de condiciones;
- capacidades de procesamiento de acción; y
- otras posibles capacidades.

Los criterios típicos para la identificación de tipos particulares de entidades IDP-FE son casos de despliegue (casos de utilización de la IDP), la complejidad de la lógica de procesamiento, factores de costes, etc.

9.2 Capacidades de procesamiento de condiciones

Las capacidades de procesamiento de condiciones pueden dividirse en dos clases: L4 PI (inspección de carga útil L4 activada) y no L4 PI (inspección de carga útil desactivada).

9.3 Capacidades de procesamiento de acciones

Véase la cláusula 6.3.3.1 en [ITU-T Y.2770] en relación con los niveles jerárquicos de acciones y ejemplos.

9.4 Tipos de entidades IDP-FE

En el Cuadro 9-1 se describen los tres tipos correspondientes, utilizando para ello los principios de clasificación definidos en las cláusulas 9.2 y 9.3.

Cuadro 9-1 – Categoría de tipos de entidades IDP-FE

<table>
<tr><td colspan="3" rowspan="3">Tipo de IDP-FE</td><td colspan="2">Capacidades de procesamiento de acciones</td></tr>
<tr><td colspan="2">Soporte de IDP-AcEF</td></tr>
<tr><td>No</td><td>Sí</td></tr>
<tr><td rowspan="2">Capacidades de procesamiento de condiciones</td><td rowspan="2">Soporte de Inspección de carga útil L4</td><td>No</td><td colspan="2">Tipo 1</td></tr>
<tr><td>Sí</td><td>Tipo 2</td><td>Tipo 3</td></tr>
</table>

Según las capacidades funcionales IDP de la entidad IDP-FE, ésta se clasifica del modo siguiente (Cuadro 9-2):

Cuadro 9-2 – Descripción detallada de los tres tipos

Tipo	Procesamiento de reglas
1	Entidad funcional (FE) sin capacidad de inspección de carga útil L4 ($L_4PI = L_{4+}HI \cup L_7PI$), es decir, del tipo no IDP-FE (por ejemplo, una SPI-FE)
2	IDP-FE sin capacidad de ejecución de acciones (IDP-AcFE), pero con inspección de carga útil L4 ($L_4PI = L_{4+}HI \cup L_7PI$)
3	IDP-FE con capacidad de ejecución de acciones (IDP-AcFE) y de inspección de carga útil L4 ($L_4PI = L_{4+}HI \cup L_7PI$)

El tipo de IDP FE puede ser el resultado de factores tales como:

1) cantidad de recursos disponibles: capacidades de una entidad física IDP específica (IDP-PE) (como componentes hardware (HW) o software (SW)); o

2) cantidad de recursos atribuidos/activados para el procesamiento IDP: a través de la gestión de la configuración (por ejemplo, a través de entidades de gestión de política (véase la cláusula 7) mediante la configuración de un conjunto de capacidades especiales).

Obsérvese que la entidad de gestión de una determinada DIP FE tipo *n* puede configurarla como de tipo *m* (n > m) (dado que, por ejemplo, el "conjunto de capacidades IDP de tipo 3" es un superconjunto para los demás tipos).

La entidad IDP FE debería poder notificar su tipo a las entidades funcionales conexas (por ejemplo a las funciones RACF).

Dependiendo de las capacidades funcionales IDP de la entidad IDP-FE, la IDP-FE de tipo 3 puede subdividirse además del modo siguiente (Cuadro 9-3):

Cuadro 9-3 – Subvariantes del tipo 3

Tipo	Reglas de procesamiento
3.1	Entidad IDP-FE con capacidad de recopilación de información y notificación
3.2	Tipo 3.1 más la capacidad de control de tráfico, pero sin la capacidad de modificar el contenido de los paquetes
3.3	Tipo 3.2 más la capacidad de modificar el contenido de los paquetes

10 Consideraciones relativas a la seguridad

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

Apéndice I

Ejemplo de arquitectura funcional de IDP probabilística basada en el filtro bloom

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

I.1 Introducción

El filtro bloom se describe en [b-Bloomfilter]:

"Los filtros bloom recurren a una técnica de aleatorización para comprobar si un elemento es miembro de un conjunto de cadenas. Dada una cadena, el filtro bloom calcula *k* funciones hash y produce unos valores hash en la gama de 1 a *m* (véase la Figura I.1). Luego asigna el valor 1 a *k* bits en un vector de longitud a m bits en las direcciones correspondientes a los *k* valores hash, siendo *k* menor o igual que *m* (véase también la Ecuación 7-1). Este mismo procedimiento se repite para todos los miembros del conjunto, proceso denominado "programación" del filtro. El proceso de consulta es similar al de programación, y consiste en pasar por el filtro una cadena para verificar si forma parte del conjunto. El filtro bloom genera *k* valores hash utilizando las mismas funciones hash utilizadas al programar el filtro. Se buscan los bits en el vector de longitud m bits, en las posiciones correspondientes a los *k* valores hash. Si al menos uno de estos bits no tiene valor 1, se declara que la cadena no es miembro del conjunto. Si todos los bits están puestos a 1, se dice que la cadena pertenece al conjunto con cierta probabilidad. La incertidumbre se debe a que dichos *k* bits del vector de m bits puede haberlos puesto a 1 cualquier otro miembro. Es decir, que un bit esté puesto a 1 no implica necesariamente que lo haya puesto así la cadena particular cuya pertenencia al conjunto se está comprobando. Ahora bien, si uno de los bits está puesto a cero implica, sin lugar a dudas, que la cadena no pertenece al conjunto, puesto que si lo fuera todos y cada uno de los *k* bits estarían indudablemente puestos a 1, tras haber programado el filtro bloom con dicha cadena. Esto explica por qué en este método se pueden dar falsos positivos y no falsos negativos."

Por ejemplo, en la Figura I.1, se genera el filtro bloom BF (B[0..m-1]) mediante 3 funciones hash, h1, h2 y h3, en las cadenas x1 y x2, donde en la IDP basada en el filtro bloom, las cadenas IDP x1 y x2 son las signaturas IDP. Las cadenas y1 e y2 se verifican mediante 3 funciones hash h1, h2 y h3 sobre las cadenas y1 e y2 con el filtro bloom BF (que viene dado por el vector de bits B[0..m-1]), donde en la IDP basada en el filtro bloom, las cadenas y1 e y2 representan las estructuras de datos inspeccionadas y que vienen dadas, por ejemplo, por la carga útil de los paquetes entrantes.

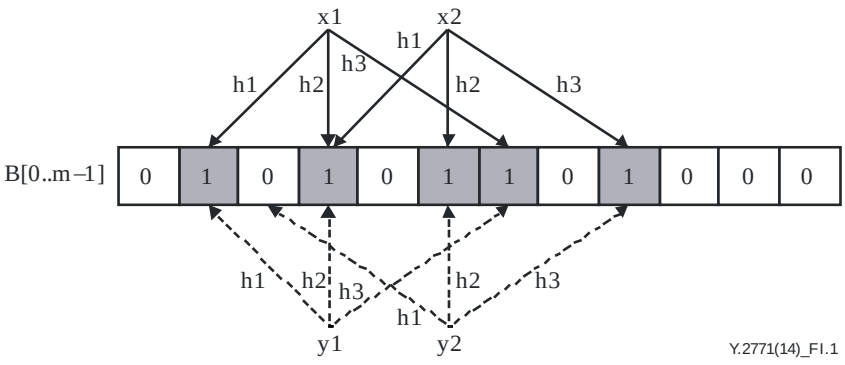


Figura I.1 – Programación y consulta del filtro bloom (BF igual al vector de bits B[0..m-1])

La tasa de falsos positivos, $\varepsilon_{f\text{-}p}$, se expresa mediante la Ecuación (I-1)

$$\varepsilon_{f-p} = \left(1 - e^{-kn/m}\right)^k \tag{I-1}$$

siendo, *n* el número de cadenas programas en el filtro bloom. El valor de $\varepsilon_{f\text{-}p}$ puede reducirse seleccionando los valores adecuados de *m* y *k* para un determinado tamaño del conjunto de miembros, *n*.

I.2 Modelo funcional del filtro bloom basado en IDP probabilística

En la Figura I.2 se muestra el modelo funcional del filtro bloom basado en IDP probabilística. La regla de política para la IDB probabilística podría ser:

Si el paquete 'P' contiene signaturas del conjunto *'S'* de signaturas IDP (en cuanto a condición política), siendo el conjunto de signaturas *'S'={'S1',' S2',..., 'Sm'}*, se descarta el paquete (en cuanto acción de política).

El filtro bloom BF_S para el conjunto de signaturas S se genera mediante el conjunto de funciones hash H_1, H_2, …, H_k . La regla de política adquiere la siguiente forma:

Si H_1('P'), H_2('P'),…, H_k('P') concuerda con BF_S, entonces se descarta.

Antes de que el analizador IDP compare el paquete entrante con respecto a esta condición de regla de política IDP, el escáner IDP necesita determinar el desplazamiento y longitud en el paquete de llegada que se utiliza para comparar respecto de las condiciones de reglas de política IDP.

Hay dos opciones principales:

1) Para condiciones de reglas IDP conscientes de la pila de protocolo, el desplazamiento y la longitud de la signatura en el conjunto 'S' se conocen, y el escáner comunica dicha información directamente al analizador IDP.

2) Para condiciones de reglas IDP sin conocimiento del protocolo, el escáner IDP examina y determina el desplazamiento y la longitud. El escáner IDP comunica dicha información al analizador IDP.

El analizador IDP genera el resultado hash del paquete P utilizando H_1, H_2, …, H_k, comprueba la concordancia de los resultados mediante el filtro BF, informa del resultado de dicha concordancia a la función de ejecución de acciones IDP. La función de ejecución de acciones IDP informa el resultado de la concordancia ("Verdadero" o "Falso") y descarta el paquete cuando el resultado se estima Verdadero; de lo contrario transmite el paquete a la función de reenvío de paquetes. Si el resultado de la concordancia generado no se corresponde con BF_s, el escáner IDP tiene que escanear desde el byte 'desplazamiento+1' (desplazamiento= desplazamiento+ 1), y así sucesivamente hasta el final del paquete.

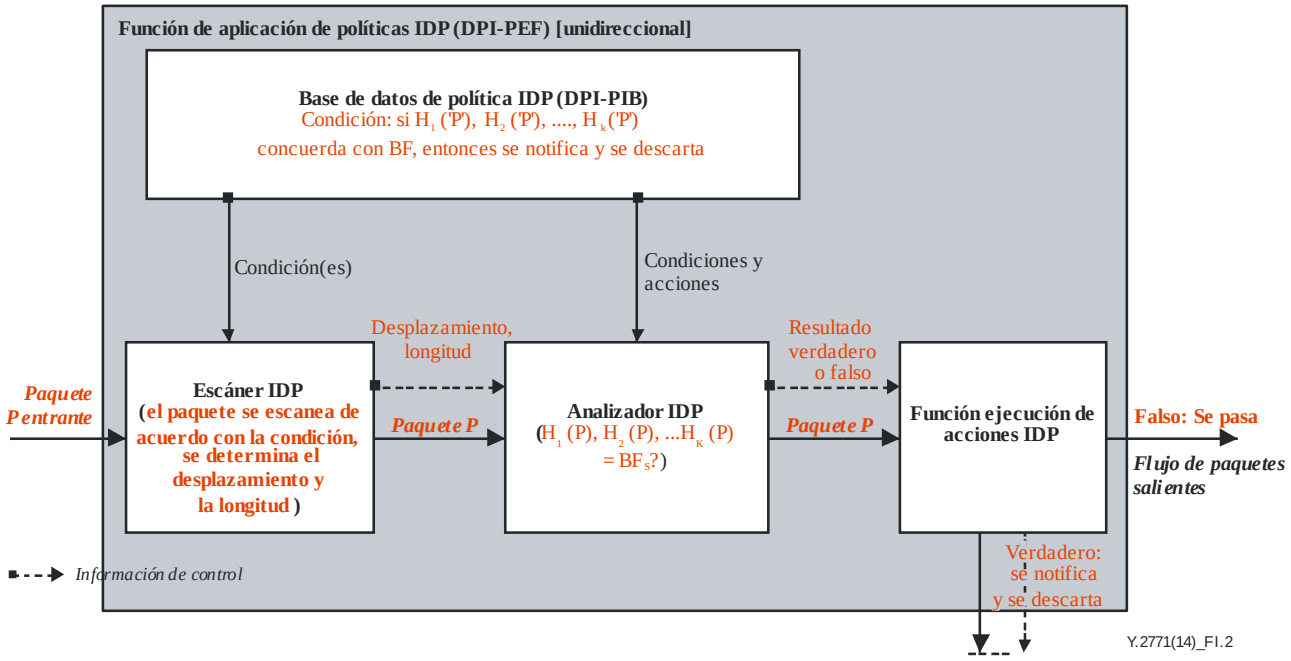


Figura I.2 – Modelo funcional del filtro bloom basado en IDP probabilística

Cabe observar que el resultado del analizador IDP es de tipo booleano, es decir, verdadero o falso, es decir, no se trata de una probabilidad del tipo "*concordancia positiva con una probabilidad* ***p*** (estando p entre 0% y 100%)". Ahora bien, todas las etapas del trayecto de procesamiento de paquetes IDP generan resultados de IDP probabilística, debido a la tasa de falsos positivos $\varepsilon_{f\text{-}p}$, que es inherente a la condición de política IDP.

Bibliografía

[b-ITU-T H.248.53] Recomendación UIT-T H.248.53 (2009), *Protocolo de control de pasarela: lotes para la gestión del tráfico*.

[b-ITU-T I.130] Recomendación UIT-T I.130 (1988), *Método de caracterización de los servicios de telecomunicación soportados por una RDSI y de los capacidades de red de una RDSI*.

[b-ITU-T J.380.1] Recommendation UIT-T J.380.1 (2011), *Digital program insertion – Advertising systems interfaces – Advertising systems overview*.

[b-ITU-T X.1036] Recomendación UIT-T X.1036 (2007), *Marco para la creación, almacenamiento, distribución y ejecución de políticas para la seguridad de las redes*.

[b-ITU-T Y.1221] Recomendación UIT-T Y.1221 (2010), *Control de tráfico y control de congestión en las redes basadas en el protocolo Internet*.

[b-ITU-T Y.2121] Recommendation ITU-T Y.2121 (2008), *Requirements for the support of flow-state-aware transport technology in NGN*.

[b-ITU-T Y-Sup.23] ITU-T Y-series Recommendations – Supplement 23 (2013), *ITU- Y.2770-series – Supplement on DPI terminology*.

[b-IETF RFC 1812] IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*.

[b-IETF RFC 2544] IETF RFC 2544 (1999), *Benchmarking Methodology for Network Interconnect Devices*.

[b-IETF RFC 3060] IETF RFC 3060 (2001), *Policy Core Information Model – Version 1 Specification*.

[b-IETF RFC 3198] IETF RFC 3198 (2001), *Terminology for Policy-Based Management*.

[b-IETF RFC 4011] IETF RFC 4011 (2005), *Policy Based Management MIB*.

[b-IETF RFC 4292] IETF RFC 4292 (2006), *IP Forwarding Table MIB*.

[b-IETF RFC 6390] IETF RFC 6390 (2011), *Guidelines for Considering New Performance Metric Development*.

[b-Bloomfilter] Dharmapurikar, S. et al., (2003), *Implementation of a Deep Packet Inspection Circuit using Parallel Bloom Filters in Reconfigurable Hardware. IEEE Proceedings of 11th Symposium on High Performance Interconnects. Stanford University, Wiley, John & Sons, Inc*.

[b-CRTC] Canadian Radio-Television and Telecommunications Commission (2009), *ISP Traffic Management Technologies: The State of the Art*.

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 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	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	Terminales y métodos de evaluación subjetivos y objetivos
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, 2015