国 际 电 信 联 盟

ITU-T

Y.2771

(07/2014)

国际电信联盟
电信标准化部门

Y系列：全球信息基础设施，
互联网的协议问题和下一代网络

下一代网络 – 安全

深度包检测框架

ITU-T Y.2771 建议书

ITU-T Y 系列建议书

全球信息基础设施、互联网的协议问题和下一代网络

全球信息基础设施	
概要	Y.100–Y.199
业务、应用和中间件	Y.200–Y.299
网络方面	Y.300–Y.399
接口和协议	Y.400–Y.499
编号、寻址和命名	Y.500–Y.599
运营、管理和维护	Y.600–Y.699
安全	Y.700–Y.799
性能	Y.800–Y.899
互联网的协议问题	
概要	Y.1000–Y.1099
业务和应用	Y.1100–Y.1199
体系、接入、网络能力和资源管理	Y.1200–Y.1299
传输	Y.1300–Y.1399
互通	Y.1400–Y.1499
服务质量和网络性能	Y.1500–Y.1599
信令	Y.1600–Y.1699
运营、管理和维护	Y.1700–Y.1799
计费	Y.1800–Y.1899
运行于NGN的IPTV	Y.1900–Y.1999
下一代网络	
框架和功能体系模型	Y.2000–Y.2099
服务质量和性能	Y.2100–Y.2199
业务方面：业务能力和业务体系	Y.2200–Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250–Y.2299
编号、命名和寻址	Y.2300–Y.2399
网络管理	Y.2400–Y.2499
网络控制体系和协议	Y.2500–Y.2599
智能泛在网络	Y.2600–Y.2699
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899
电信级开放环境	Y.2900–Y.2999
未来网络	Y.3000–Y.3499
云计算	Y.3500–Y.3999

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T Y.2771 建议书

深度包检测框架

摘要

建议书ITU-T Y.2771提供了一个有关深度包检测（DPI）的框架。该框架的主要目的在于一种用于描述设计、定义和实施DPI解决方案的结构化方法，以支持业务/应用感知，推动演变网络间的互操作性。它从主要的体系结构角度出发，用于确定和帮助理解网络问题。本建议书也从建模和性能角度出发，提供了有关DPI框架的观点。

特别是，此类框架的目的在于描述DPI功能与其它网络功能之间可能存在的关系，以帮助确定DPI功能的需求（对其它ITU-T建议书，如ITU-T Y.2770建议书，其本身是主观的），并为术语工作提供帮助（例如，当某个定义将与某个功能模型相关时）。

历史沿革

版本	建议书	批准日期	研究组	Unique ID*
1.0	ITU-T Y.2771	2014-07-18	13	11.1002/1000/12178

* 欲查阅建议书，请在您网络浏览器的地址字段内先输入URL http://handle.itu.int/，然后再输入该建议书独一无二的编号，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

© 国际电联 2015

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1 范围 1
2 参考文献 1
3 定义 2
3.1 他处定义的术语 2
3.2 本建议书定义的术语 3
4 缩写和首字母缩略语 4
4.1 通用缩写和首字母缩略语 4
4.2 数学符号 6
5 惯例 6
6 体系框架 7
6.1 网络体系框架 – 高层网络情形 7
6.2 协议体系框架–针对某些样例网络应用的包检测层 8
7 建模框架 16
7.1 功能模型 16
7.2 信息和数据模型 30
7.3 流量模型 31
7.4 可能之DPI-FE子部件的识别 37
7.5 容错模型 38
8 性能框架 43
8.1 目的和性能方面的考虑范围 43
8.2 性能测量 44
8.3 策略执行点的性能、定性性能行为的估计 52
9 DPI功能实体的分类 55
9.1 分类原则 55
9.2 依据条件处理的能力 55
9.3 依据行动处理的能力 55
9.4 DPI-FE类型 55
10 安全方面的考虑 56
附录I 基于Bloom过滤程序的、概率DPI的样例功能体系结构 57
I.1 概述 57
I.2 基于Bloom过滤程序的、概率DPI的功能模型 58
参考资料 59

ITU-T Y.2771 建议书

深度包检测框架

1 范围

本建议书提供了在基于包的网络中进行深度包检测（DPI）的框架。本建议书的主要目的是描述DPI的基本概念、功能部件和能力，DPI实体可用之来识别在基于包的网络中的信息流，以支持DPI要求规范，并引导构建基于包的网络的结构化解决方案（如NGN）。

本建议书提供了关于某些基本概念的高层系统信息，典型地，在实现DPI实体时，与之相关。不过，预期不会为DPI提供所有内含的详细规范。相反地，本建议书提供了一种高层的信息（即框架），旨在用作背景材料，供国际电联各研究组以及国际电联之外的其它专家组使用，例如作为其制定DPI功能详细标准的输入。

本建议书的范围包括：

a) 在各种各样的网络架构中结合DPI时，将会遇到的基本架构原则；

b) 从DPI角度来看的、协议体系结构方面的问题；

c) 样例功能模型及其在DPI用例情形中的应用；以及

d) 有助于开展DPI性能讨论的性能框架，如DPI相关之关键性能指标的识别。

本ITU-T建议书的实施者和用户应遵守所有适用的国家和地区法律、法规和政策。在本建议书中描述的机制可能并不适用于国际通信，以确保对电信运营商以及国际电联《组织法》和《公约》提出有关保密和国家主权的法律要求。

2 参考文献

下列ITU-T建议书和其它参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其它参考文献均面临修订，使用本建议书的各方应探讨使用下列建议书或其它参考文献最新版本的可能性。当前有效的ITUT-T建议书清单定期出版。

本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

[ITU-T E.800] Recommendation ITU-T E.800 (2008), *Definitions of terms related to quality of service*.

[ITU-T G.602] Recommendation ITU-T G.602 (1988), *Reliability and availability of analogue cable transmission systems and associated equipments*.

[ITU-T H.248.86] Recommendation ITU-T H.248.86 (2014), *Gateway control protocol: H.248 Support for deep packet inspection*.

[ITU-T X.200] Recommendation ITU-T X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[ITU-T X.731] Recommendation ITU-T X.731 (1992), *Information technology – Open Systems Interconnection – Systems management: State management function*.

[ITU-T Y.2704] Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN*.

[ITU-T Y.2770] Recommendation ITU-T Y.2770 (2012), *Requirements for deep packet inspection in next generation networks*.

[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 定义

3.1 他处定义的术语

本建议书使用了以下他处定义的术语：

3.1.1 应用（application）[ITU-T Y.2770]：以下情形之一的名称：

- 应用协议类型（如IP应用协议ITU-T H.264视频或会话启动协议（SIP））；
- 应用的业务用户实例（如VoIP、VoLTE、VoIMS、VoNGN和VoP2P），如“包语音应用”；
- 包语音的“提供商特定的应用”（如3GPP提供商VoIP、Skype VoIP）；以及
- 嵌入另一个应用的应用（如SIP或HTTP消息主体元素中的应用内容）。

一个应用可通过某个特定的标识符（如通过位字段、样式、签名或“应用等级条件”等常规表达式，也可参见[ITU-T Y.2770] 第3.2.2节）来识别，作为上面所列之所有应用等级的公共特性。

3.1.2 可用性（availability）[ITU-T E.800]：一个项目在给定时刻或给定间隔内的任何时刻，处于可行使要求功能之状态的可用性，假定必要时，需要提供外部资源）。

3.1.3 应用描述符（也称为应用级条件）（application descriptor (also known as application-level conditions)）[ITU-T Y.2770]：用于识别应用的一系列规则条件（根据 [ITU-T Y.2770]第3.2.1节）。

本建议书涉及作为一般意义上对象的应用描述符，它是应用级条件的同义词。它并不涉及句法、编码和数据类型等具体结构。

3.1.4 深度包检测（deep packet inspection (DPI)） [ITU-T Y.2770]：根据分层协议体系结构OSI-BRM [ITU-T X.200]分析：

- 负载与/或包属性（参见第3.2.11节/[ITU-T Y.2770]中的潜在属性清单）深于协议层2、3、4（L2/L3/L4）包头信息；以及
- 其它包属性

以便明确地识别应用。

注 – DPI功能的输出以及流信息等一些额外的信息，通常用于报告或对包采取行动等后续的功能中。

3.1.5 DPI引擎（DPI engine）[ITU-T Y.2770]：DPI功能实体的一个子部件和中心部分，它执行所有的包路径处理功能（例如，包识别功能以及[ITU-T Y.2770] 图6-1中所示的其它包处理功能）。

3.1.6 DPI策略条件（也称为DPI签名）（DPI policy condition (also known as DPI signature)）[ITU-T Y.2770]：识别应用并定义策略规则的行动是否应执行的必要状态与/或前提条件的表示。与策略规则有关的一系列DPI策略条件规定了何时策略规则是适用的（亦参见[b-IETF RFC 3198]）。

DPI策略条件必须包含应用级条件，并可包含其它选项，如状态条件与/或流级条件等：

1) 状态条件（可选）：
   a) 网络业务等级条件（如包路径中遇到的拥塞）；或者
   b) 网络元素状态（如DPI-FE局部过载条件）。
2) 流描述符/流级条件（可选）：
   a) 包内容（包头字段）；
   b) 包特性（如MPLS标签的号码）；
   c) 包处理（如DPI-FE的输出接口）。
3) 应用描述符/应用级条件：
   a) 包内容（应用包头字段和应用负载）。

注 – 条件涉及流级条件和应用级条件之正式描述中的“简单条件”。

3.1.7 DPI策略决定功能实体（DPI policy decision functional entity (DPI-PDFE)[ITU-T 2770]）：远离DPI-FE、决定 DPI-FE 中应执行之签名规则的功能。一些控制与/或管理功能不一定远离DPI-FE。

3.1.8 流描述符（也称为流级条件）（flow descriptor (also known as flow level conditions)）[ITU-T Y.2770]：用于在所检测流量中识别特定类型流（根据[ITU-T Y.2770] 第3.1.3节）的一系列规则条件。

注1 – 流描述符的该定义比[b-ITU-T Y.2121]中的定义增加了[ITU-T Y.2770]第3节中所述的要素。

注2 – 有关[ITU-T Y.2770]中所用之流描述符的进一步规范讨论，参见[ITU-T Y.2770]附件A。

3.1.9 可靠性（reliability）[ITU-T E.800]：在所述条件下，一个项目在给定时间间隔内可行使要求功能的概率。

3.2 本建议书定义的术语

本建议书定义了以下术语：

3.2.1 DPI分析程序（DPI analyzer）：DPI处理路径（在DPI策略执行功能内）中的一个后续实体，关注于特定包头与预选包流负载之间的比较功能。DPI分析程序的主要范围关系到依据预选输入包对DPI策略条件进行的评估。

注 – DPI分析程序可位于某个DPI扫描程序后（参见第3.2.6节）。DPI分析程序可以提供入侵检测系统（IDS）分析程序的功能。

3.2.2 DPI节点（DPI node）：用于实现DPI相关功能的一个网络元素或设备。因此，这是用于指定实现DPI物理实体的一个通用术语。

注 – 功能视角：DPI节点功能（DPI-NF），包括DPI策略执行功能（DPI-PEF）以及（可选的）本地策略决定功能（L-PDF格式），因此，DPI-NF在功能上等于DPI功能实体。

3.2.3 DPI策略行动（简称行动）（DPI policy action (action in short)）：在满足规则条件时，定义什么是必须要做的，以便执行策略规则。策略行动可能会导致一个或多个操作的执行，以影响与/或配置网络流量和网络资源，亦可参见[b-IETF RFC3198]。

3.2.4 DPI策略执行功能（DPI-PEF）（DPI policy enforcement function (DPI-PEF)）：执行策略决定的逻辑实体，假定通过DPI策略规则实现。

3.2.5 DPI扫描程序（也被用作“DPI扫描功能”）（DPI scanner (also used as “DPI scan function”)）：在DPI处理路径中的第一个实体（在DPI策略执行功能内），并通过依据所有的DPI输入包检查所有的DPI策略条件，来提供一个预选（关系到后续的DPI分析程序，参见第3.2.8节）。

3.2.6 DPI“1+N”冗余组（DPI "1+N" redundancy group）：“1+N”冗余体系结构（和N≥1）之后的DPI功能组件（例如，DPI节点、DPI-PIB、DPI引擎等），假定通过一个单个工作部件和N个保护部件实现。

注 – 上面的集合用于提供额外的可靠性，以及提高DPI节点或者以DPI节点部署的网络的可用性。

4 缩写和首字母缩略语

4.1 通用缩写和首字母缩略语

本建议书采用了以下缩写和首字母缩略语：

A_{DPI}	DPI策略行动
BRM	基本参考模型
CAM	内容可寻址存储器
C_{DPI}	DPI策略条件
DAI	深度应用识别
DHI	深度包头检测
DiffServ	差别服务
DPI	深度包检测
DPI-AcEF	DPI行动执行功能
DPI-AnF	DPI分析程序功能
DPI-FE	DPI功能实体
DPI_{InP}	路径内DPI
DPI-NF	DPI节点功能
DPI_{OoP}	路径外DPI
DPI-PDFE	DPI策略决定功能实体
DPI-PE	DPI物理实体
DPI-PEF	DPI策略执行功能
DPI-PIB	DPI策略信息库
DPI-PIF	DPI包识别功能

DPI-ScF DPI扫描功能
DNNF 确定下一个节点的功能
FIB 转发信息库
FTP 文件传输协议
HTTP 超文本传输协议
HW 硬件
IDS 入侵检测系统
IP 网际协议
IPFIX IP流信息出口
KPI 关键性能指标
KPI_{DPI} DPI实体的关键性能指标
L-PDF 本地PDF
L2VPN 第2层虚拟专用网络
L_XHI 协议第X层的包头检测
L_XPI 协议第X层的负载检测
LX （协议）第X层
LX+ 比LX更高的（协议）层
MIB 管理信息库
MPI 媒介深度包检测
MPLS 多协议标签交换
MTBF 故障间平均时间
MTTR 平均维修时间
NA(P)T 网络地址（和端口）转换
NGN 下一代网络
OSI-BRM 开放系统互连－基本参考模型
PDF 策略决定功能
PEP 策略执行点
PFF 包转发功能
PIB 策略信息库
QoS 服务质量
RACF 资源和接纳控制功能
R_{DPI} DPI策略规则
R-PDF 远程PDF（即从DPI节点来看，PDF距离较远）
RTSP 实时流协议
SDU 业务数据单元

SIP 会话启动协议
SPI 浅包检测
S_D-PDF 依赖于会话的PDF
S_I-PDF 独立于会话的PDF
SW 软件
TCAM 三元内容可寻址存储器
TCP 传输控制协议
TOS 业务类型
VoIP 经由IP的语音（IP语音）
VoLTE 经由LTE（长期演变）的语音
VoIMS 经由集成媒体系统的语音
VoNGN 经由下一代网络的语音
VoP2P 经由P2P（对等网络）的语音

4.2 数学符号

本建议书使用了以下符号（名称、单位和简述）：

ε_{DPI}	（DPI）错误率	–
$\varepsilon_{f\text{-}n}$	（DPI）错误地判为错的错误率	–
$\varepsilon_{f\text{-}p}$	（DPI）错误地判为对的错误率	–
$\phi_{P,\ In}$	（DPI）输入包的处理速率	$[s^{-1}]$
$\phi_{P,\ Out}$	（DPI）输出方向的包速率	$[s^{-1}]$
$\phi_{P,\ Node,\ Out\cdot}$	包节点吞吐量	–
$\phi_{P,\ Identified}$	包成功识别率	–
$P_{Hit,BloomFilter}$	估计的概率信息确定性	–
Ndb	DPI策略规则数量	–
Sp	包大小	–
N_{DPIeng}	DPI引擎数量	–
τ_{TD}	（DPI节点的）节点内部转发延迟	[ns]
A	（DPI策略）规则行动集	–
C	（DPI策略）规则条件集	–
R	（DPI策略）规则集	–

5 惯例

无。

6 体系框架

6.1 网络体系框架 – 高层网络情形

本框架描述了在网络基础设施中部署DPI的主要边界条件。有些原则性的DPI框架方案可以通过对类似准则的分析来确定。

- **网络位置层面**（即DPI实体在一个包网络域中的位置）
  - 在边缘（“边界DPI”）；或者
  - 在网络内（“核心DPI”）；
  - 在对等网络之间（“对等DPI”）；
- **网络数据包（路径）类型**（即检测数据包的类型）[1]
  - 用户平面（或传输层，如***IP***数据路径、***IP***媒体路径、***IP***承载者路径、隧道、***MPLS LSR***、伪线等）；或者
  - 控制平面（或业务层；如IP信令路径）；或者
  - 管理平面；或者
  - 组合。
- **与其它网络体系结构对齐的层面**（即一个DPI实体如何与基本的包网络体系结构耦合的层面）
  - **孤立DPI**实体（即DPI实体隐藏在包网络之外），示例：
    - 位于网络中选定点上的极少数DPI实体（无“全覆盖”目标；就像一个探针式的路径内DPI），
    - 路径外DPI实体；
  - **覆盖DPI**网络（即有一个专门的DPI网络基础设施，叠加到基本的包网络中；从操作角度来看，两个网络基础架构是分隔开的），

    示例：
    - 通用的例子：路径内DPI实体的网络共享如用户平面路径等，但使用独立的控制与/或管理接口；
    - 具体的例子：例如，带有入侵检测目的的一个DPI功能；
  - **嵌入式DPI**实体（即DPI功能实体与有关非DPI包处理的其它功能实体一起被嵌入在一个物理网络元素中；从成本效益运营角度来看，这样的一个物理实体应提供诸如一个单个的OAM接口，因此，这就意味着一个跨所有功能实体的、统一的管理模式）

    示例：
    - 通用的例子：一个带管理信息库的DPI实体，其管理信息库与相同物理网络要素之非DPI功能实体的管理信息库一致；
    - 具体的例子：在RACF内的一个带通用管理能力的DPI功能实体，但不共享任何RACF控制接口；
  - **集成的DPI**（即一个“完全集成”于“包网络”中的DPI实体）

---

[1] 可参照某个专门的“协议”或“协议栈”来确定“包类型”的概念。不过，在此对其详细程度没有要求。

示例：

- 通用的例子：考虑到DPI实体的一个SDO定义的网络参考模型（体系结构）；
- 具体的例子：例如，通过DPI实体扩展的ITU-T RACF（可以使用现有的参照点（如“RW控制的DPI”）（如一个基于H.248的RW，通过支持[ITU-T H.248.86]来扩展），或者可以引入新的参考点）；

因此，从某个DPI实体的网络集成情形角度来看，存在众多用例。

6.2 协议体系框架–针对某些样例网络应用的包检测层

6.2.1 原则

存在各种不同的包检测层。表6-1概述了关于“包检测层”要求涉及的、典型的网络应用。包检测层可表示为：

1) 根据分层协议体系结构的基本参考模型（BRM），此处为LxHI和LyPI列）；或者
2) 使用“旧的”、通俗的术语（在[b-ITU-T Y.Sup.23]的第8.1条中予以描述），此处列出了浅包检测（SPI）、中包检测（MPI）、深度包头检验（DHI）和深度应用检测（DAI）；

关于分层协议体系结构中的DPI问题，也可参见[b-ITU-T Y.Sup.23]中的第8节。

6.2.2 DPI和非DPI情况的差别

从分层协议体系结构的角度来看，DPI的概念相当宽泛，甚至包括第1层之上的所有协议层（参见[ITU-T Y.2770] 第3.2.5节）。不过，在特定的网络应用情况下，包检测的范围基本上是有限的，如主要只与链路、网络与/或传输层有关。

此类限制通常源自服务、历史或/与实施有关的问题。例如，就可实现的DPI业务与最先进的技术之间，在经济上所做的权衡决策。此类有限的包检测/也被称为浅包检测和中度包检测（SPI、MPI；也可参见第8.1节[b-ITU-T Y.Sup.23]）。

根据[ITU-T Y.2770]，DPI与非DPI之间的粗粒度差别是很大的，本建议书也这么认为。“DPI”的概念在此处指的是本建议书支持的、松散的策略检测规则，而“非DPI”更多地涉及协议第2、3与/或4层上的、传统的包检测（即SPI、MPI）。

6.2.3 样例

表6-1提供了一个有关示例网络应用与包检测层的列表，是此类网络应用的典型组成部分。应当指出的是，表6-1所列只是示例性的，不一定是详尽的。

表6-1 – 针对某些样例网络应用的包检测层

网络应用（示例）		包检测层				评注
		“深度包检测”（DPI）				
		(注)	“深度包头检测”（DHI)		“深度应用识别”（DAI)	
			“中深度包”			
			“浅包检测”（SPI)	“检测”（MPI)		
		L2 包头检测（L2HI）	L3, 4 包头检测（L3,4HI）	L4+包头检测（L4+HI）	L7 负载检测（L7PI）	
安全性：						
1.1	网络入侵探测	–	X	X	X	有不同的入侵探测方法： a) 异常探测 b) 滥用探测（此处）
1.2	网络资源的安全保护（网络入侵防御、安全攻击防御）	–	X	X	X	
1.3	其它安全相关的功能					

表6-1 – 针对某些样例网络应用的包检测层

网络应用（示例）		包检测层				评注
		“深度包检测”（DPI）				
		(注)	“深度包头检测”（DHI）		“深度应用识别”（DAI）	
			“中深度包”			
			“浅包检测”（SPI）	“检测”（MPI）		
		L2 包头检测（L2HI）	L3, 4 包头检测（L3,4HI）	L4+包头检测（L4+HI）	L7 负载检测（L7PI）	
识别：						
2.1	订户、用户	–	**X**	–	–	通过…来识别？（如网络地址）
2.2	应用类型	–	–	**X**	**X**	通过…来识别？（如应用层协议类型）
2.3	会话	–	**X**	–	–	通过…来识别？（如IP连接、IP传输连接）。也可参见[b-ITU-T Y.Sup.23]中的第7节。
2.4	应用控制协议（如SIP、RTSP、HTTP、FTP，...）	–	**X** (依赖于众所周知的端口)	**X**	**X**	
应用数据特性：						
2.5	内容	–	–	**X**	**X**	如非法的内容

表6-1 – 针对某些样例网络应用的包检测层

网络应用（示例）		包检测层				评注
		“深度包检测”（DPI）				
		(注)	“深度包头检测”（DHI）		“深度应用识别”（DAI）	
			“中深度包”			
			“浅包检测”（SPI）	“检测”（MPI）		
		L2 包头检测（L2HI）	L3, 4 包头检测（L3,4HI）	L4+包头检测（L4+HI）	L7 负载检测（L7PI）	
2.6	媒介类型（应用数据类型）	–	–	X	X	
2.7	媒介格式	–	–	X	X	
修改（协议数据单元）：						
3.1	修改“内容”：去除病毒	–	–	–	X	
3.2	修改“包头”：服务质量标记	–	X	X	–	
3.3	修改“包头与内容”：“ALG功能”	–	X	X	–	L3（和L4）和应用层上的本地NA(P)T功能

表6-1 – 针对某些样例网络应用的包检测层

网络应用（示例）		包检测层				评注
		“深度包检测”（DPI）				
		(注)	“深度包头检测”（DHI）		“深度应用识别”（DAI）	
			“中深度包”			
			“浅包检测”（SPI）	“检测”（MPI）		
		L2 包头检测（L2HI）	L3, 4 包头检测（L3,4HI）	L4+包头检测（L4+HI）	L7 负载检测（L7PI）	
使用参数监控：						
4.1	服务层协议	–	X	X	X	
4.2	流量参数控制示例：	–	X	X	X	依赖于流量参数类型
	L3字节率控制（峰值速率、可持续的速率）	–	X	–	–	
	L3 PDU大小（最小，最大）监管	–	X	–	–	
	L3突发大小监管	–	X	–	–	
	L7 SDU大小监管（“应用负载”）	–	X	X	–	

表6-1 – 针对某些样例网络应用的包检测层

网络应用（示例）		包检测层				评注
		“深度包检测”（DPI）				
		(注)	“深度包头检测”（DHI）		“深度应用识别”（DAI）	
			“中深度包”			
			“浅包检测”（SPI）	“检测”（MPI）		
		L2 包头检测（L2HI）	L3, 4 包头检测（L3,4HI）	L4+包头检测（L4+HI）	L7 负载检测（L7PI）	
	L7 字节率监管（“应用容量”）	–	X	X	–	
服务质量支持：						
5.1	流量整形	–	X	–	–	
	L3字节率整形	–	X	–	–	参见如[b-ITU-T Y.1221]或[b-ITU-T H.248.53]
网络分析：						
6.1	用户行为	–	X	X	X	
6.2	使用样式	–	X	X	X	

表6-1 – 针对某些样例网络应用的包检测层

网络应用（示例）		包检测层				评注
		“深度包检测”（DPI）				
		(注)	“深度包头检测”（DHI）		“深度应用识别”（DAI）	
			“中深度包”			
			“浅包检测”（SPI）	“检测”（MPI）		
		L2 包头检测（L2HI）	L3, 4 包头检测（L3,4HI）	L4+包头检测（L4+HI）	L7 负载检测（L7PI）	
性能测量（“关键性能指标”（KPI））：						
7.1	远程测量结果收集	–	X	X	X	
7.2	本地测量结果产生	–	X	X	X	
收费/计账支持：						
8.1	基于时间的信息	–	X	–	–	
8.2	基于流量的信息	–	X	–	X	与IP字节率（L3）或/与应用数据相关的流量
8.3	基于事件的信息	–	X	X	X	依赖于事件类型（如事件可能与内容相关联）

表6-1 – 针对某些样例网络应用的包检测层

网络应用（示例）		包检测层				评注
		“深度包检测”（DPI）				
		(注)	“深度包头检测”（DHI）		“深度应用识别”（DAI）	
			“中深度包”			
			“浅包检测”（SPI）	“检测”（MPI）		
		L2 包头检测（L2HI）	L3, 4 包头检测（L3,4HI）	L4+包头检测（L4+HI）	L7 负载检测（L7PI）	
面向链路的DPI：						
9.1	带可能的第2层策略条件的DPI应用	**X**	**X**	**X**	**X**	参见“注”
注 – 面向链路的DPI与面向网络的DPI之间存在根本性区别。面向链路的DPI限于L2网络域，面向网络的DPI与包含网络层（L3）和更高层协议信息的DPI签名相关。						

7 建模框架

7.1 功能模型

陈述了多个功能模型，说明了包转发路径的谱系，从不带任何DPI模型（第7.1.2节）、单向DPI模型（第7.1.3节）到双向DPI模型（第7.1.4节）。

本节中的所有功能模型都是样例功能模型。

7.1.1 路径内DPI对路径外DPI

从端到端包路径的角度来看，一个*DPI节点功能*（DPI-NF）有两种基本的部署情形：

- 路径内DPI（DPIInP）：将DPI-NF置于端到端包路径中，DPI策略执行功能（DPI-PEF）直接对包流量执行DPI策略规则（也称为在线DPI）；或者
- 路径外DPI（DPIOoP）：不将DPI-NF置于端到端包路径中，而集中于一个包网络中，因此，例如，间接对所采样包流量执行DPI策略规则（也称为旁路DPI、离线DPI）。

从物理节点（DPI-NF封装）的角度来看，这两种DPI模式是不同的：DPI_{InP}可置于一个包节点中，而DPI_{OoP}将置于一个不带任何*包转发功能*的节点中（PFF，参见下一节）。

7.1.2 一般性包转发

在基于包的网络中的一个包节点，可根据图7-1，通过*包转发功能*（PFF）来抽象。例如，在MPLS标签交换路由器（LSR）或以太网交换机或网桥的情况下，PFF可以是一种转换功能[2]，或者在IPv4[IETF RFC791]和IPv6[IETF RFC 2460]路由器的情况下，可以是一种转发/路由功能。对为单播通信（注：多播将导致需要确定多个下一节点）而在输出方向发送的每一个输入包，PFF都必须确定下一个节点（如IP网络中的下一跳）。

注1 – 组播将导致多个下一个节点的确定。

为该功能而由确定下一节点功能（DNNF）所使用的信息，存储于称为*转发信息库*（FIB）的某个并列配置数据库中。例如，在由[b-IETF RFC1812]定义IPv4路由器的情况下，根据[b-IETF RFC4292]，为IP*转发表*MIB。

[2] 注 – 术语“包”而后将同义于（L2）“帧”。

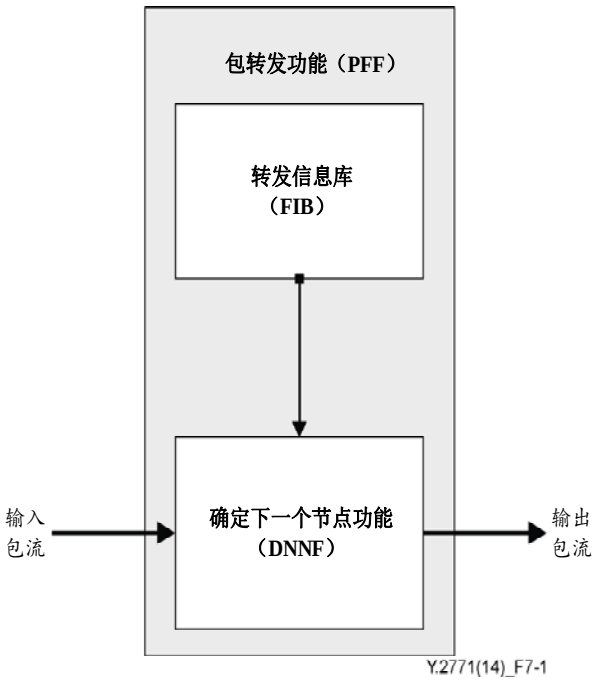


图7-1 – 功能模型“一般性包转发”

需要指出的是，该PFF是一种单向模型。DPI功能（如果存在的话）置于包路径中（即路径内*DPI*（DPI_{InP}）模式），通常是PFF之前，参见第7.1.3节。

PFF的任何细节和要求均超出了本建议书的讨论范围，不过，出于以下原因，在某些功能模型中指明了PFF：

- 未用任何强制执行的DPI策略规则制定一种可能的DPI节点行为（例如，一个空DPI策略信息库（DPI-PIB）的临时条件）；
- 表明特定的策略行动将依然包括PFF的参与，如“转发包”；以及
- 针对某些DPI节点相关性能指标的、一个明确的规范基线（参见第8节）。

应该指出的是，如果只是一个单一（输出）包路径（参见注2），那么PFF可能是无效的。

注2 – 样例情形：置于两个L2或L3包节点之间的一个路径内DPI节点，或者在用户设备前的路径内DPI节点。

7.1.3 单向DPI

7.1.3.1 单向DPI策略执行功能的部件

7.1.3.1.1 通用高层功能模型

根据[ITU-T Y.2770] 第6.2节，基于DPI功能实体（DPI-FE）的样例体系结构，图7-2提供了顶层功能模型。

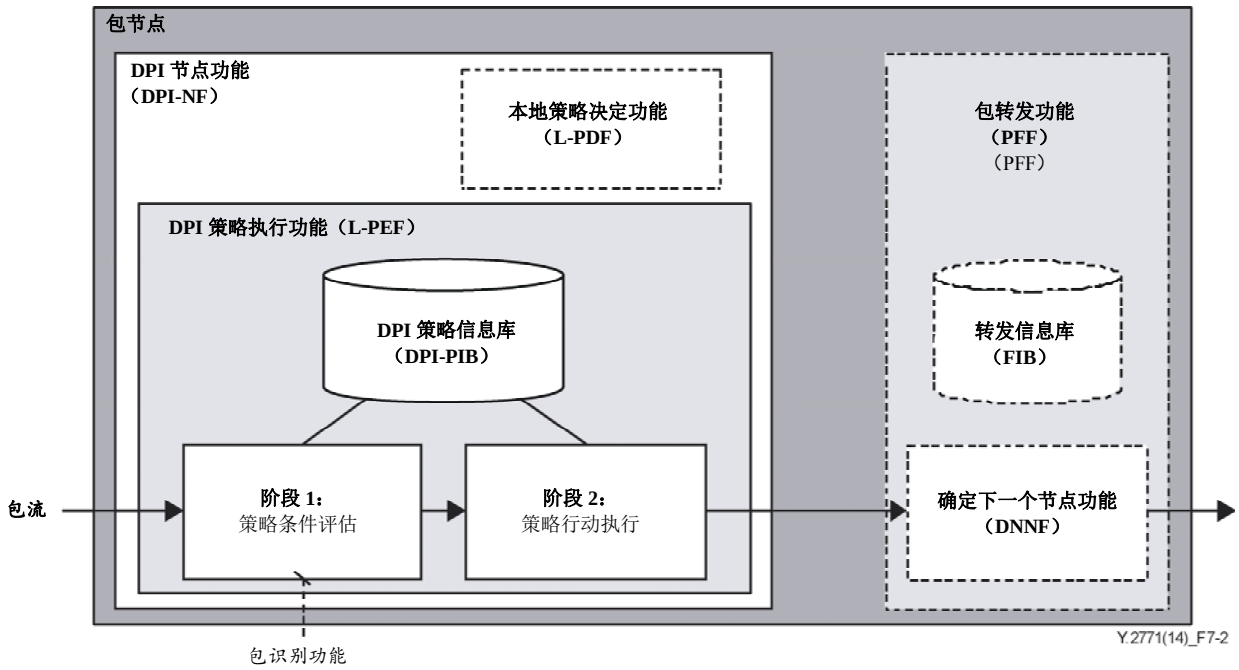


图7-2 – 通用高层功能模型

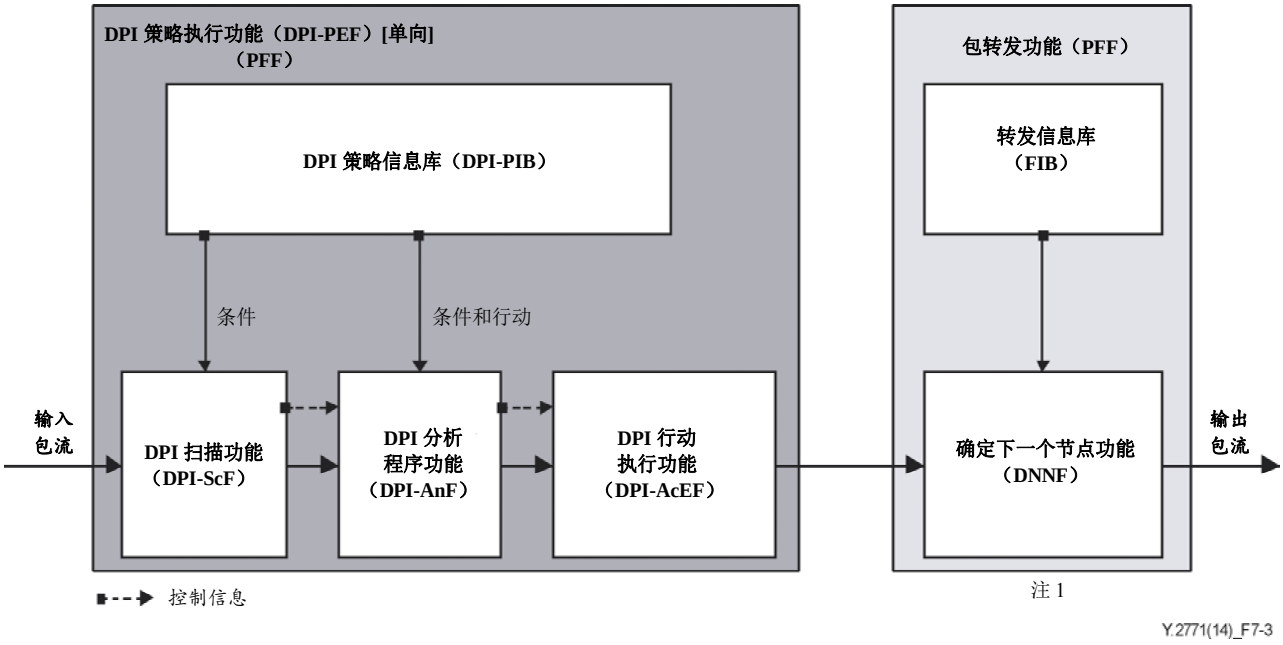
单向包路径建模为一个分阶段的过程。第1阶段表示包识别功能（也可参见第7.3.2.1节）。在DPI情形下，这种能力是一种至关重要的功能，因此，在后续各节中，会做更详细的说明（见功能分解模型示例）。

7.1.3.1.2 在串行处理拓扑结构中的基本部件

图7-3描绘了一个样例单向模型（有可能从图7-2的顶层模型中获得）。*DPI*策略执行功能（DPI-PEF）位于PFF之前：任何输入包都首先通过DPI-PEF处理和PFF处置。DPI-PEF也可在包路径功能以及一个关联表中进行结构化，作为所用策略规则的存储器，称为*DPI*策略信息库（DPI-PIB）或*DPI*签名库。在这个例子中，DPI特定策略规则的执行受制于：

- DPI扫描功能（DPI-ScF）；
- DPI分析程序功能（DPI-AnF）；以及
- DPI行动执行功能（DPI-AcEF）。

这些功能部件将在下一节中引入和激活。



注1 – PFF已超出本建议书的讨论范围。
注2 – PTF只出现在路径内DPI模式中。

图7-3 –DPI模式的“单向DPI策略执行功能部件”

7.1.3.1.3 额外的部件

7.1.3.1.3.1 在DPI-PEF内

对DPI-PEF内额外的部件尚未进行描述，有待进一步研究。

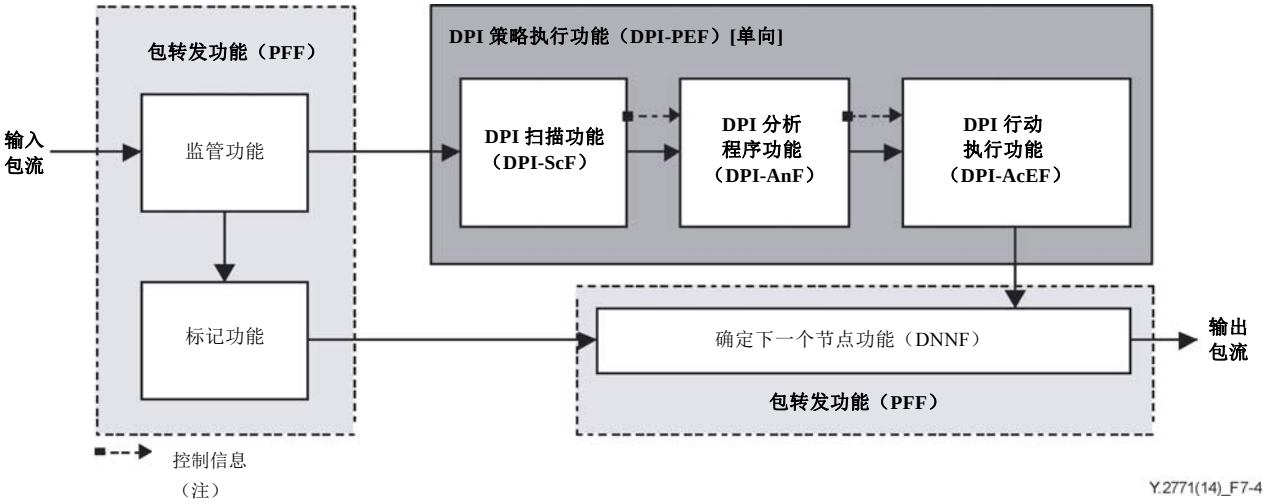
7.1.3.1.3.2 在PFF内

包转发功能可以包括子FE，如排队、封装、整形、监管、标记、交换和DNNF等。不过，这些都超出了本建议书的讨论范围。

7.1.3.1.4 包处理路径的结构方面问题

取代包处理功能的串行执行（如图7-3所示），也可能存在并行的DPI节点体系结构。例如，PFF也可并行处理DPI-PEF。

在图7-4中，显示了带平行包处理的包处理路径模型。在此，监管功能监控进入某个输入端口的包，或者带预定义准则的包（即一个专门的策略规则条件），如标有高优先级的IPv4 TOS字段（即基于SPI的策略规则）。如果这些输入包或流违反带宽协议，那么可相应地对所有的或部分的包进行标记，并直接发送给DNNF。



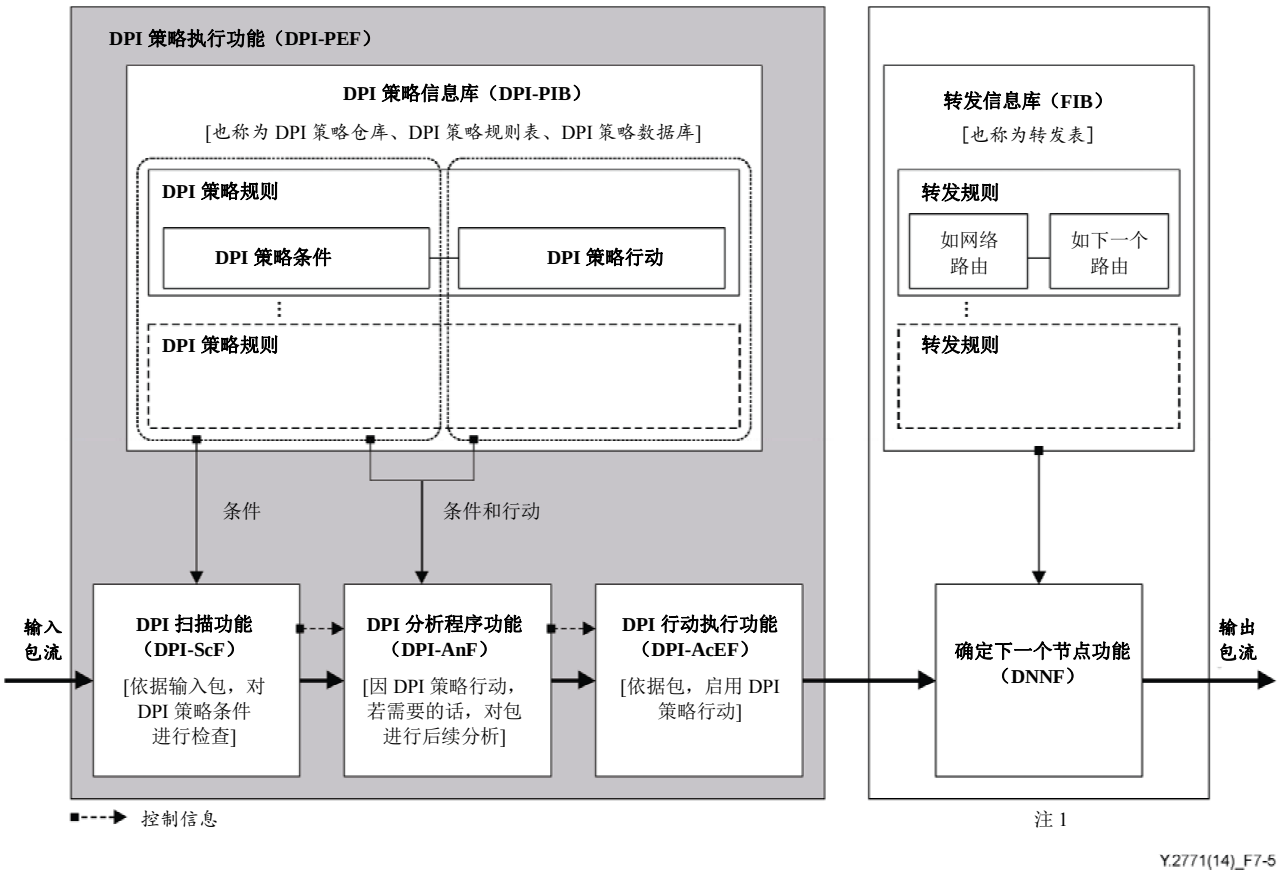
注1 – PFF已超出本建议书的讨论范围。

图7-4 – 针对带并行包处理的、单向DPI策略执行功能的DPI模型

应当指出的是，图7-3和图7-4中的样例表示的是逻辑拓扑，而非物理拓扑。不过，实际的实施方案应反映这样一个事实，即甚至在单个DPI样例中，包或流采用的包处理路径也可能会有所不同。

7.1.3.2 DPI策略信息库的结构（DPI签名库）

DPI策略信息库的更多细节和进一步结构由图7-5提供，功能上图7-3做了足够描述。策略规则（*R*）涉及一组动作（*A*）与一组条件（*C*）的绑定。对条件进行评估，以确定是否执行行动。在行动涉及包过滤行为的情况下，一般性术语策略规则也被称为（特定的）过滤程序规则（和可参见[b-ITU-T Y.Sup.23]中的第7.3节和第7.6节）。



注1 – PFF已超出本建议书的讨论范围。
注2 – PTF只出现在路径内DPI模式中。

图7-5 – DPI模型“DPI策略信息库结构”

DPI策略规则R_{DPI}的处理模型：

1) 依据一个输入包，DPI扫描功能（DPI-ScF）对所有的（注1）DPI策略条件CDPI进行检测；

注1 – 一个DPI策略规则的范围可覆盖通过节点转发的整个包流量，或限定于由流描述符（参见[ITU-T Y.2770]）给出的某个特定流（参见[ITU-T Y.2770]）。例如，包流可限定于应用实例之间的端到端会话（参见[ITU-T Y.2770]的第6.7节）（例如，在IP应用的情况下，端对端会话可以是在确定的HTTP、RTSP、SIP、FTP等上的会话）。执行会话特定的策略规则通常被称为会话相关的监管，而非会话无关的监管（相关于有关某个策略执行节点的整个流量集）。流和会话的概念在本节中不做进一步阐述，原因是，无关于显示的（高层）功能模型。

2) DPI分析功能（DPI-AnF）用于进一步验证策略条件。在DPI-ScF对每一个包做初步筛选后（注2），利用DPI-ScF，以流水线方式，对DPI-AnF进行操作。DPI-AnF旨在提升性能。

注2 – 例如，扫描功能可将输入包关联于某个特定的（如IP）应用，而后分析功能可对该包做应用特定的评估。DPI-ScF和DPI-AnF分隔背后的一般原则与串行与/或分层策略执行概念有关（例如，为了满足性能目标要求）。关于DPI-AnF的更详细信息有待进一步研究。

3) 依据所扫描和所分析的包，DPI行动执行功能（DPI-AcEF）运用DPI策略行动ADPI。

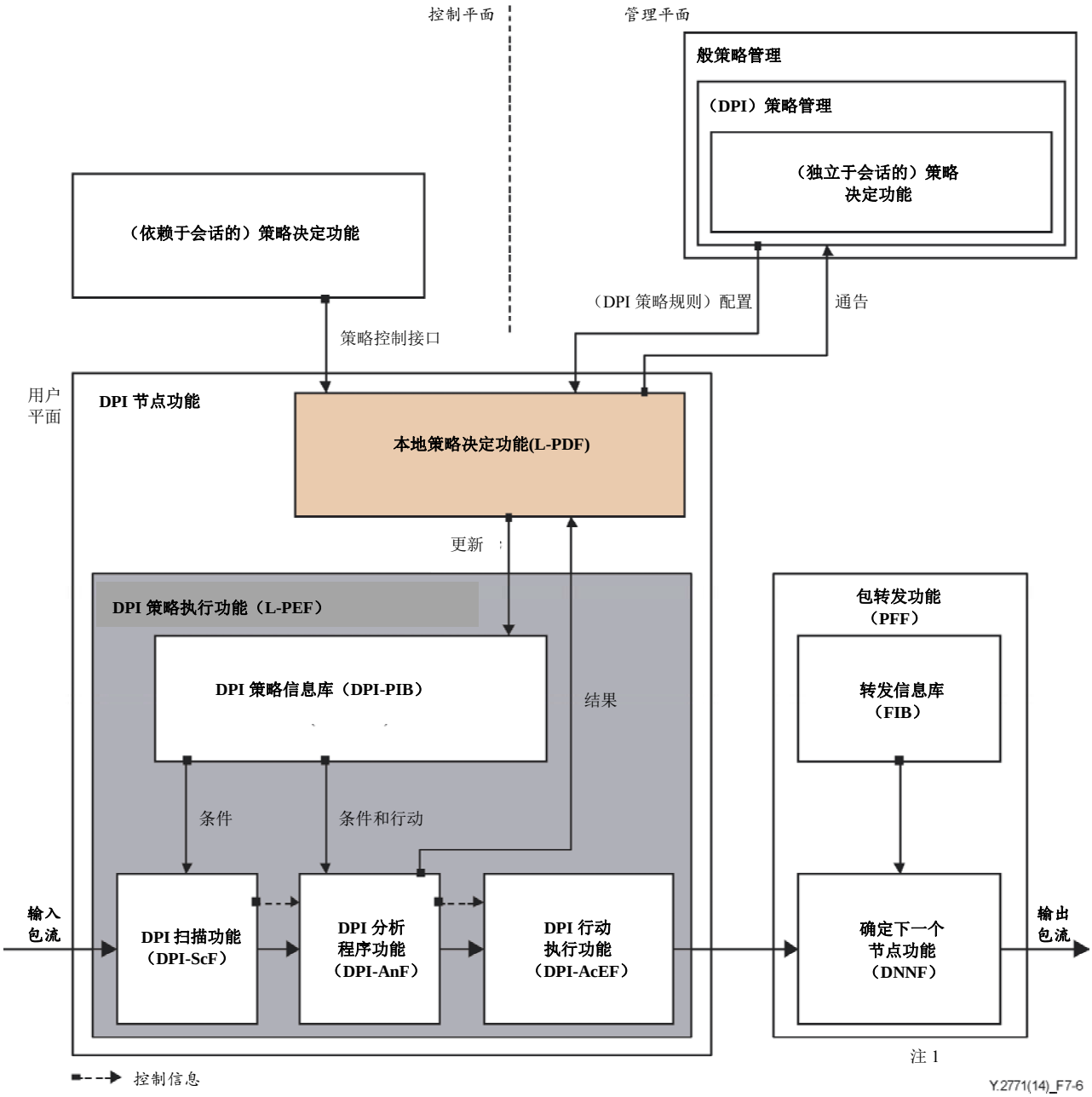
在路径内DPI模式的情况下，每一个成功通过DPI-PEF的包而后都将由常规PFF进行处理（也可参见第7.1.2节）。

7.1.3.3 策略决定：修改DPI策略信息库

DPI-PIB提供一组DPI策略规则$R_{DPI,\ i}$，确定DPI-PEF的实际行为。DPI策略规则由策略决定功能实体（DPI-PDFE）创建。图7-6说明了远程PDF的例子，置于控制平面和管理平面中（图7-7描绘了另一个例子的情形，控制平面无任何（直接的）接入）。控制平面PDF可负责会话相关的DPI策略决定（S_D-PDF）。在第7.1.3.2节中提到了一个可能的会话概念，见注1。[ITU-T H.248.86]定义了这样一个策略控制接口。管理平面PDF可负责图7-6中的、会话独立的DPI策略决定（S_I-PDF）。策略管理可主要定义会话相关的和会话无关的策略规则（如图7-7中的例子）。

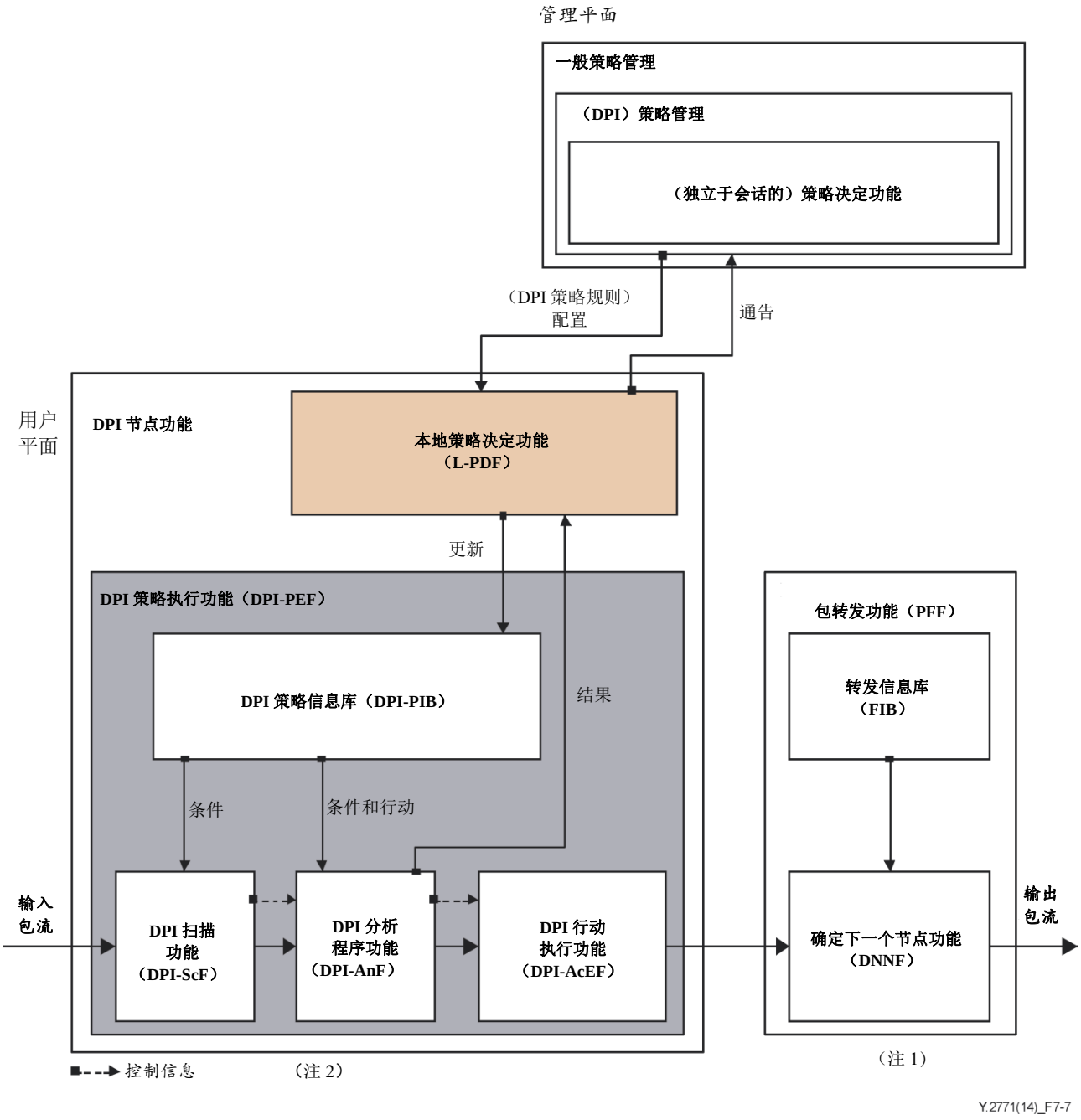
注1 – 例如，会话相关的监管可以具体到某个特定的应用、用户、媒体类型等，会话无关的监管可以涵盖一般安全规则，如每日更新。来自S_D-PDF 和 S_I-PDF的（DPI）策略规则是相辅相成的。图7-4提供的只是网络配置的一个例子。

典型的，DPI策略管理是一般策略管理实体的组成部分，也负责如“传统”浅包检测（SPI）或中等深度包检测（MPI）这样的非DPI策略规则。



注1 – PFF已超出本建议书的讨论范围。
注2 – PTF只出现在路径内DPI模式中。

图7-6 – DPI模型“通过控制和管理平面修正DPI策略信息库”



注1 – PFF已超出本建议书的讨论范围。
注2 – DPI节点可能不与控制平面中的任何其它网络要素相连。
注3 – PTF只出现在路径内DPI模式中。

图7-7 – DPI模型“仅通过管理平面修正DPI策略信息库”
（注：PFF仅出现在路径内DPI模式）

通过针对S_D-PDF的策略控制接口和针对S_I-PDF的策略管理接口，PDF通常置于偏远地区的网络元素中，如图7-6所示（也可参见图7-7）。任何远程的PDF都可暂时停止服务，激活一个额外的、可选的本地PDF（L-PDF），以便优化网络中的DPI服务可用性。

L-PDF与DPI-PEF一起代表DPI节点功能。

注2 – 它涉及[ITU-T Y.2770] 第7.2.1节图7-1中的本地策略决定路径。

L-PDF（如果可用的话）提供与远程PDF的外部通信以及与DPI-PEF的内部接口，以更新DPI-PIB和处理来自DPI分析程序功能（DPI-AnF）的可能结果。L-PDF还可能负责解决DPI策略规则集之间可能存在的规则互动问题。

注3 – 检测和解决规则互动是PDF的一个基本功能。

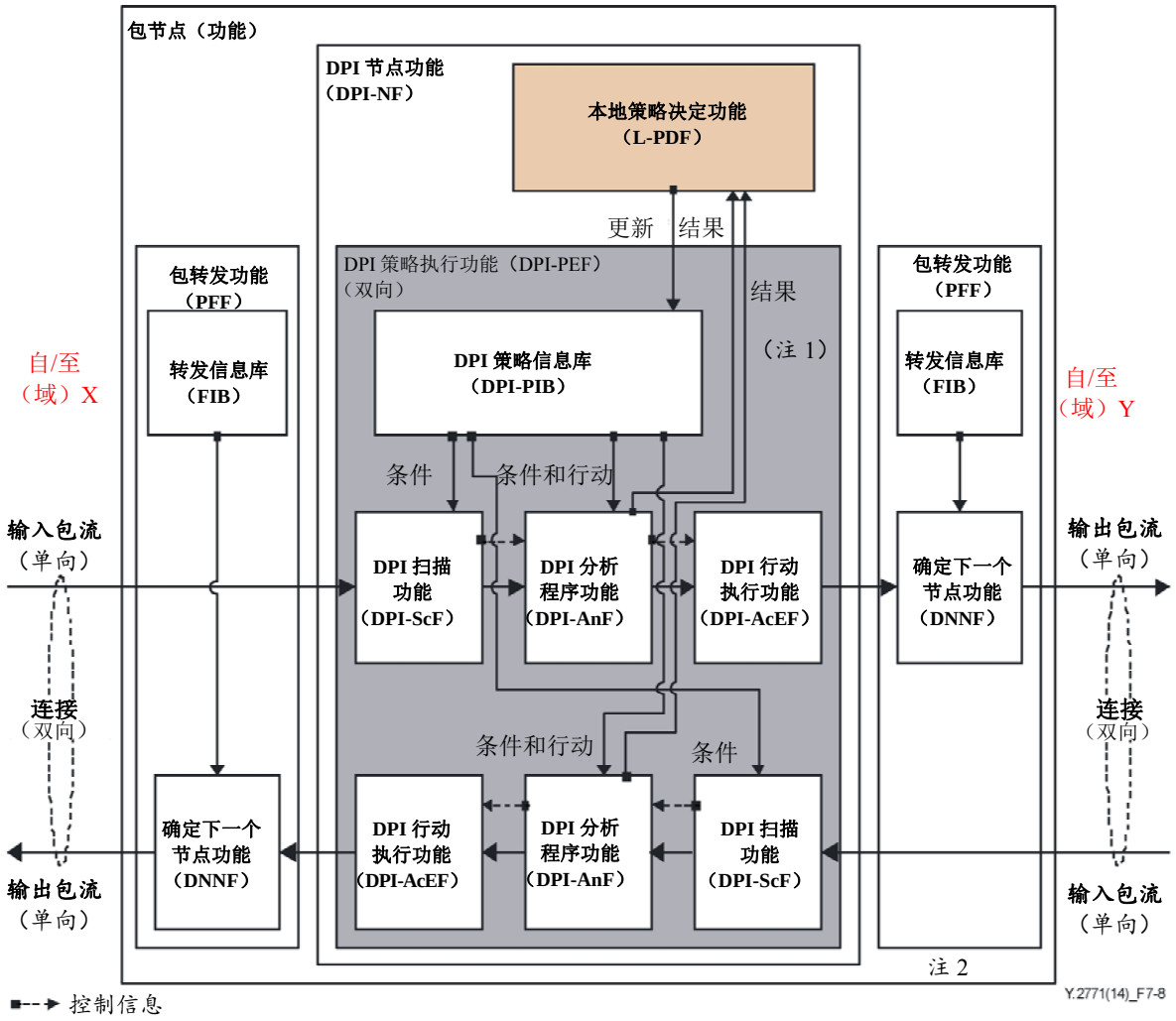
自DPI分析程序功能（DPI-AnF）的反馈可能导致针对策略管理的告警（如通告新的安全威胁）。

基本的策略执行模型是单向的，但可能延伸至双向通信路径，请参见下面章节。

7.1.4 双向DPI

图7-8提供了一个双向DPI模型的例子（定义参见[ITU-T Y.2770]中的第3.2.4节）。

一个双向包连接由两个单向包流组成。从DPI策略执行的角度来看，DPI-PIB是两个流量方向之间的绑定元素。一个“双向”DPI策略规则将提供DPI策略条件或/与涉及两个流量方向的行动。



注1 – DPI-PIB可在依赖于方向的DIP-PIB中内部进行组织，如DPIx-y-PIB and DPIy-x-PIB。
注2 – PFF已超出本建议书的讨论范围。
注3 – PTF只出现在路径内DPI模式中。

图7-8 – DPI模型“双向DPI”

L-PDF负责双向DPI-PEF，并通过来自单向分析程序功能（DPI-ANF）的、可能的后处理结果，来提供一个“中介功能”，而后它可能触发对（本地）策略规则的更新或/与对远程PDF的通告。

7.1.5 无状态和有状态DPI

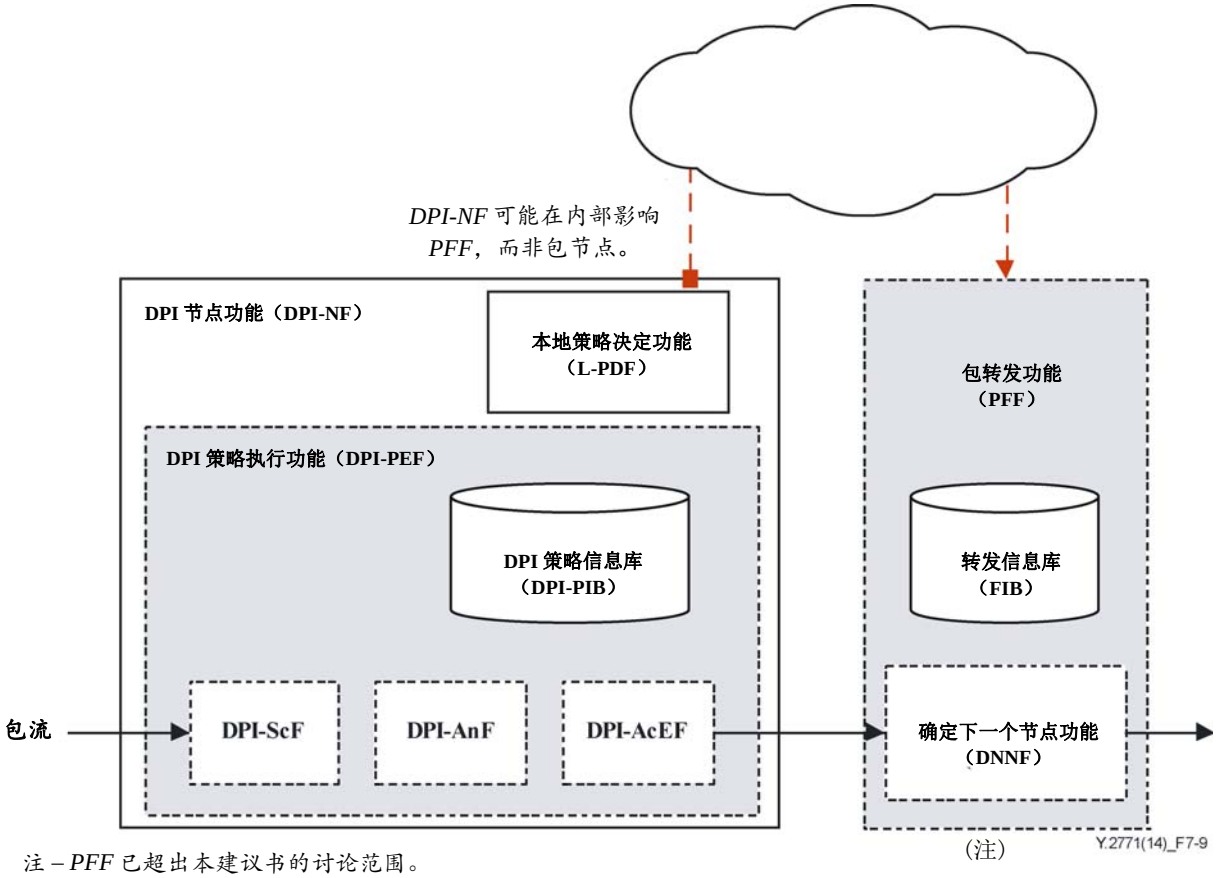
无状态的DPI涉及到在每个包上单独执行的DPI策略规则，无关单向包流或双向包连接中的其它包（参见[ITU-T Y.2770]第3.2.11节中的“状态条件”）。

有状态的DPI指的是这样一种相关性（注），它可通过一个（有限的）状态机来建模。这样一个功能模型将特别针对具体的DPI策略规则，因而超出了本建议书的讨论范围。

注 – 例如，一个带基于TCP的应用数据传输的IP应用。对TCP连接建立阶段，可能有专门的策略条件；对后续的活跃通信阶段，可能有其它的策略条件。

7.1.6 DPI对包转发的影响

在一个PFF是可用的或“非空”PFF条件下（参见第7.1.2节），DPI节点功能可能会影响后续的包转发功能（PFF）。不过，不得授权DPI-NF进行包节点本地PFF修改。这更像是一个选项，它通过包节点外部、远程的网络元素来驱动（参见图7-9）。具体的影响受制于策略决定与/或专用的DPI策略规则，因而超出了本建议书的讨论范围。



注1 – PFF已超出本建议书的讨论。
注2 – PTF只出现在路径内DPI模式中。

图7-9 – 通过远程网络实体、DPI可能对包转发产生的影响

例子：

- 出于与网络拓扑有关的所观测网络性能之故，更新FIB（网络路由信息，也可参见图7-5）；
- 通过阻断某些网络路由，更新FIB（例如，在双向DPI情况下，在相反的方向上）。

应该指出的是，通过DPI-NF驱动以及通过外部网络元素下达的、有关PFF的任何本地修改，在包转发，交换或/与路由概念等方面，都必须与基本的网络大框架保持协调一致（例如，通过一个IPv6 DiffServ域、一个MPLS域、一个L2VPN拓扑等给出）。

7.1.7 基于包的网络和NGN环境中的DPI

DPI节点功能嵌入于一个功能性的、物理的或虚拟的包节点中，其可与基于包的网络中的其它功能进行互动。图7-10提供了一个环境例子。当DPI-PDFE和DPI-FE映射至一个分解的网关模型时，[ITU-T H.248.86]定义一种DPI控制技术。

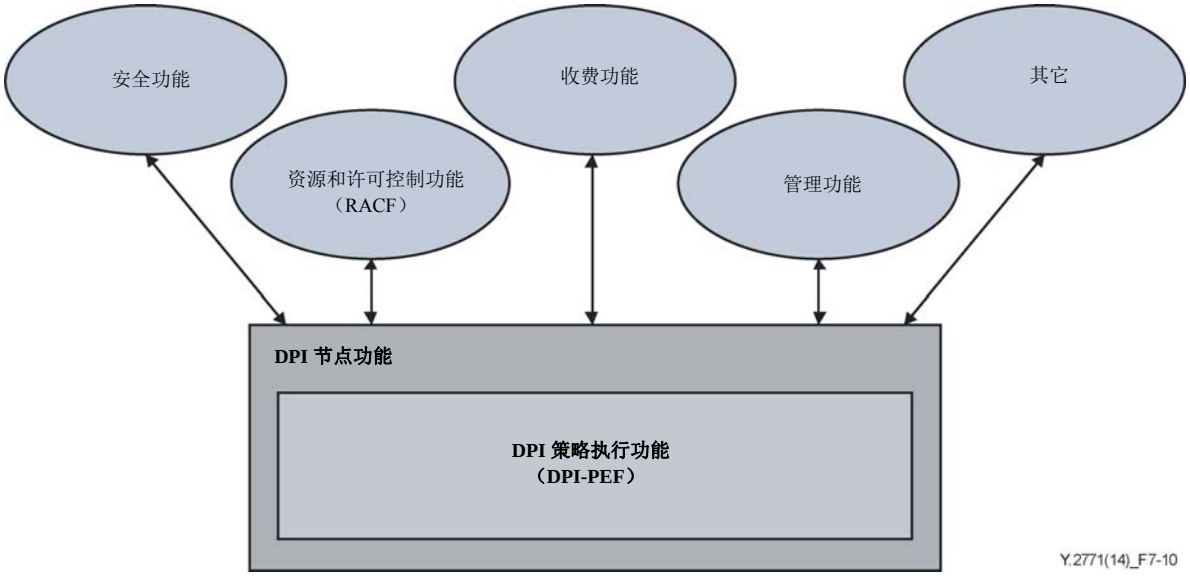


图7-10 – 基于包的网络和NGN环境中的DPI

7.1.8 用于支持IETF流测量的功能模型

7.1.8.1 IETF IPFIX流测量功能的特性

IETF IPFIX流度量功能在[IETF RFC5101]中进行定义（也可参见[ITU-T Y.2770]中的第6.3.3.2节）。根据[ITU-T Y.2770]第3.1.3节和对性能指标度量结果所做的测量，“流”概念指的是一个包流。因此，IPFIX流测量功能一部分与包流识别的策略规则条件整合在一起（基于IPFIX流标识符（参见[ITU-T Y.2770]第3.2.17节）），一部分与度量和报告行动的策略规则行动有关。

7.1.8.2 嵌入式流测量功能

IETF IPFIX流过程可被抽象和描述为DPI策略规则，因此，直接映射至一个DPI-FE。图7-11描述了这样一个嵌入是流测量功能。测量结果的报告可以跨外部接口E2或e1进行通信。

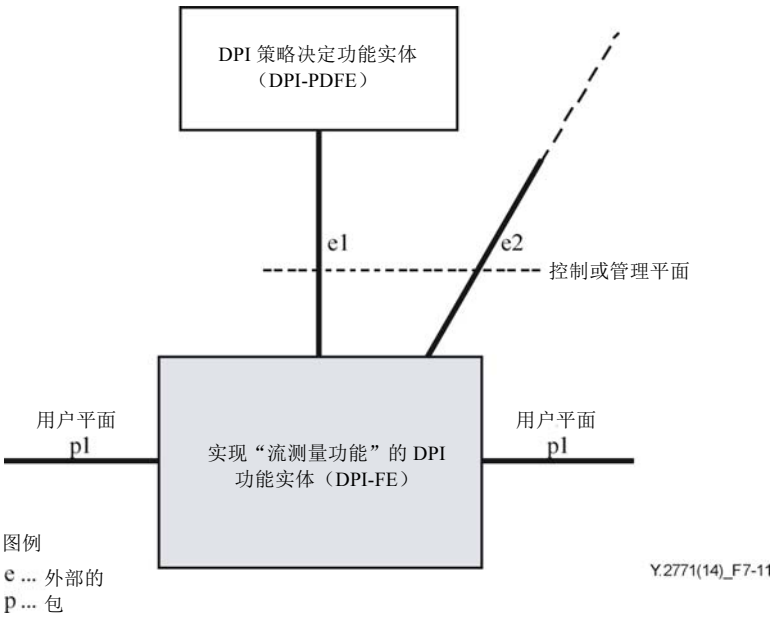


图7-11 – 嵌入式流量测量功能

7.1.8.3 远程流测量功能

流测量功能也可以远程地置于包路径p1中，在DPI-FE之前（参见图7-12）或DPI-FE之后。带远程流测量功能的网络配置可以被激发，例如，当现有的网络提供一个带流度量支持的物理实体并额外部署了一个DPI-PE时。

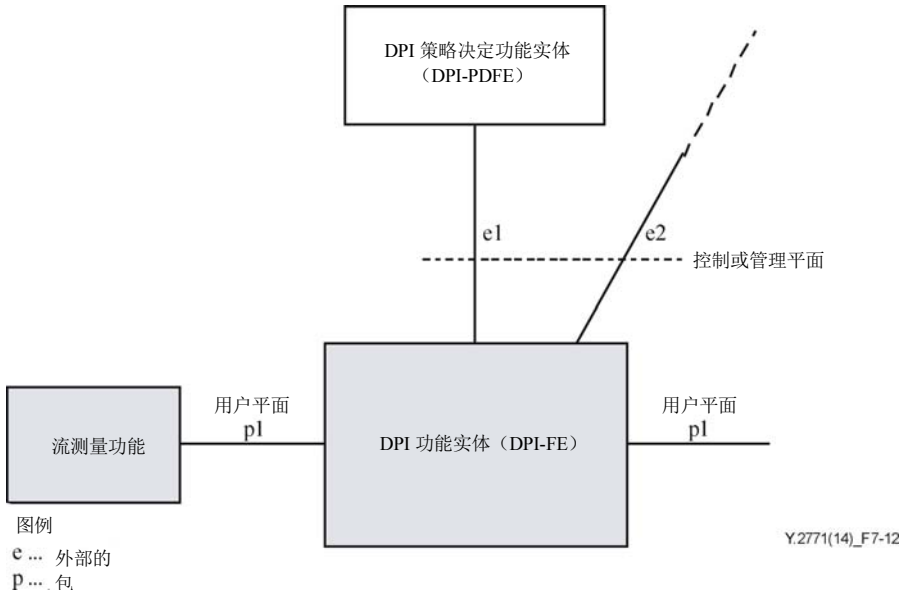


图7-12 – 远程流量测量功能

可将DPI-FE和远程流度量功能看作是一个分布式体系结构，它有两个变体：

1) 解耦体系结构：两个功能实体都只通过p1相连，因而在控制和管理平面中完全解耦。

2) 耦合体系结构：例如，流度量功能的结果也可通过DPI-FE的e2来报告。这样一种功能共享模式将意味着两个功能实体之间的一个额外的、全新的接口（除了p1之外）。

两个变体的用例有待进一步研究。

7.1.9 概率DPI

7.1.9.1 一般性概率DPI

包识别过程内在地可以具有统计性质（而不是确定性的包识别），即识别结果（如一个匹配准则）关联于一个概率。此类包检测被称为概率DPI，也被称为不确定的DPI。

概率DPI与DPI策略规则有关，例如，其条件是：

– 签名集“S”包含签名‘S_1’, ‘S_2’, …, ‘S_N’。根据布尔析取范式（DNF），签名集“S”代表一个组合策略条件，也就是说，一个签名‘S_i’合并为一个基于OR的列表。两个DPI步骤具有以下特征：

  第1步，策略条件的产生基于一个概率过程；以及

  第2步，策略条件的执行导致确定性的匹配结果，因此，整体上导致概率DPI。

概率DPI的主要目标是快速、高效地确定一个包是否与签名集“S”相匹配。具体的匹配信息，即识别的是哪个特定的签名“S_i”是次要的。签名集“S”通常表示有关某个特定应用的识别选项。相关的应用标签，如“带签名集S中签名的包”，可能受制于报告。

7.1.9.2 基于Bloom过滤程序的概率DPI

出于固有的错误率ε_{DPI}之故，一个基于Bloom过滤程序的DPI是概率DPI的一个已知代表 – 依据错误地判为对的错误率$\varepsilon_{f\text{-}p}$（参见第8.2.3.3.1节）– 基本的包检测方法。

考虑一下作为Bloom过滤程序实现的、应用特定的一个例子：

– DPI应用指的是检测“应用x的流量”。应用x的流量通过一个签名集S = {'应用x应用 v1'，'应用x应用 v2'，...，'应用x vk'}来表征，即涉及应用特定之特性的个体签名。而后，可能有那么一个样例DPI策略规则来检测包是否包含“应用x”，使用的是上述签名集，作为复合DPI策略规则条件，当碰到一个匹配时，仅丢弃包，而无需知道确切的应用x版本是什么。

  基于Bloom过滤程序的概率DPI的主要动机是识别精度与识别资源消耗之间的某种权衡（例如，依据CPU时间与/或存储器）。这样一种方法可使DPI处理得到大大简化。

基于Bloom过滤程序概率特性的DPI通过以下过程给出：

– 依据Bloom过滤程序对任何到达包“P”进行比较，它代表整个并行的签名集合“S”,如果一个包“P”匹配集合“S”中的一个或多个签名，那么根据以下公式，结果将是：以概率为PHit, BloomFilter, ’S’的估计信息确定性，“击中”一次。

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

参数值为：

m = Bloom过滤程序以比特计的大小

N = 集合S中的签名数量

k = 用于创建Bloom过滤程序的散列函数数量

“概率”概念与DPI-FE的“识别精度”有关，涉及包识别、流量、应用等，紧密耦合错误率区域的性能指标（参见第8.2节）。对由Bloom过滤程序实现的概率DPI，参见附录1，性能指标“（DPI）错误地判为对的错误率”$\varepsilon_{f\text{-}p}$和性能指标“（DPI）错误地判为错的错误率”$\varepsilon_{f\text{-}n}$等于零。

7.2 信息和数据模型

通信服务的阶段性发展过程[b-ITU-T I.130]区分了“信息”和“数据”的抽象等级（如协议数据单元）。信息模型用在非常高的等级上，以便描述如网络实体之间的信息流（例如，参见[b-ITU-T I.130]、[b-ITU-T X.1036]）。数据模型用在较低的等级上，以便从语法角度描述如一个信息元素（例如，参见[b-ITU-T J.380.1]）。

7.2.1 信息模型（样例框架）

有关DPI策略规则相关信息和信息流建模的任何种类详细规范，都超出了“框架”类型建议书的讨论范围。不过，例如，作为DPI策略规则信息建模的框架，可将[b-IETF RFC 3060]视为一个基线示例。表7-1指明了某些样例信息元素，以便提供某些指南（如何开发一个具体的模型）：

表7-1 – 基于[b-IETF RFC 3060]的样例信息模型

信息要素 （本建议书和[ITU-T Y.2770]）	依据[b-IETF RFC 3060]的一般性策略 核心信息模型
DPI策略规则	可基于“PolicyRule”类
DPI策略规则（组合）条件	可基于“PolicyCondition”抽象类
DPI策略规则（单个）条件	可基于“PolicyCondition”抽象类
DPI策略规则行动	可基于“PolicyAction”抽象类
等等，如对DPI策略规则进行分组和确定DPI策略规则的优先级，诸如规则有效期等特性。	…

7.2.2 数据模型（样例框架）

有关DPI策略规则相关数据对象建模的任何种类详细规范，都超出了“框架”类型建议书的讨论范围（原因是，协议语法制定的领域因此而将被打开）。

不过，[b-IETF RFC 4011]DPI策略规则数据建模可作为基线示例。表7-2指明了某些样例数据对象，以便提供某些指南（如何开发一个具体的模型）：

表7-2 – 基于[b-IETF RFC 4011]的样例数据模型

信息要素 （本建议书和[ITU-T Y.2770]）	作为例子，依据[b-IETF RFC 4011]， 使用基于策略的管理MIB的、一般性数据对象
DPI-PIB	可基于“pmPolicyTable”对象， 它又与“pmPolicyCodeTable”对象关联（注1）
DPI策略规则，即DPI-PIB入口	可基于“pmPolicyEntry”对象
DPI策略规则条件	可基于“pmPolicyCodeEntry”对象（注2）
DPI策略规则行动	可基于“pmPolicyCodeEntry”对象（注2）
等等	等等
注1 – 在两个关联的表中抽象和分离“规则描述”和“规则代码”允许定义一个高效的“DPI-PIB”。 注2 – 即规则条件和规则行动最终可使用相同的数据对象模型（在此例中）。	

网络平面方面：可能需要指出的是，一个一般性数据对象可视为：

- 从DPI管理平面角度来看的被管对象（参见[ITU-T Y.2770] 第8节中的接口e2）；或/与
- 从DPI控制平面角度来看的被控对象（参见[ITU-T Y.2770] 第8节中的接口e1）。

例如，一个特定的DPI策略规则可以通过DPI PD-FE（经由*e1*）来标记，或通过DPI管理系统（经由*e2*）来规定，但在DPI-PIB将导致相同的数据对象“DPI策略规则”入口。

7.3 流量模型

7.3.1 概述

本节的目的是从流量理论角度，对DPI实体的一些有趣的特性进行描述（定义参见[ITU-T Y.2770]第3.2.7节）。派生的内容可能有助于后续的定义，如功能、性能和可用性要求，以及体系结构方面的指标或性能评估。

所描述的流量模型只是例子，并不一定代表一个特定的DPI部件（如DPI-PE、DPI-FE、DPI引擎、DPI签名库等）。

7.3.2 有关包路径处理的基本流量模型

流量以包粒度、DPI-FE的主要功能进行处理，它主要通过嵌入式DPI引擎来实现（定义参见[ITU-T Y.2770]第3.2.6节）。

一个DPI引擎是一个DPI-FE的核心部件，在DPI-FE中起着重要作用。DPI流量由DPI引擎来处理。当一个DPI引擎将作为一个物理部件来实现时，并行处理可能有助于改善DPI引擎的性能。因此在对应一个DPI引擎的物理部件内，可能有多个处理单元。

7.3.2.1 设定DPI引擎范围的DPI-FE基本流量模型

根据[ITU-T Y.2770] 图6-1，图7-13采用了DPI-FE的样例功能模型，以便得出一个典型的流量模型。流量模型仅关注包路径，因而为一个DPI引擎提供一个模型。

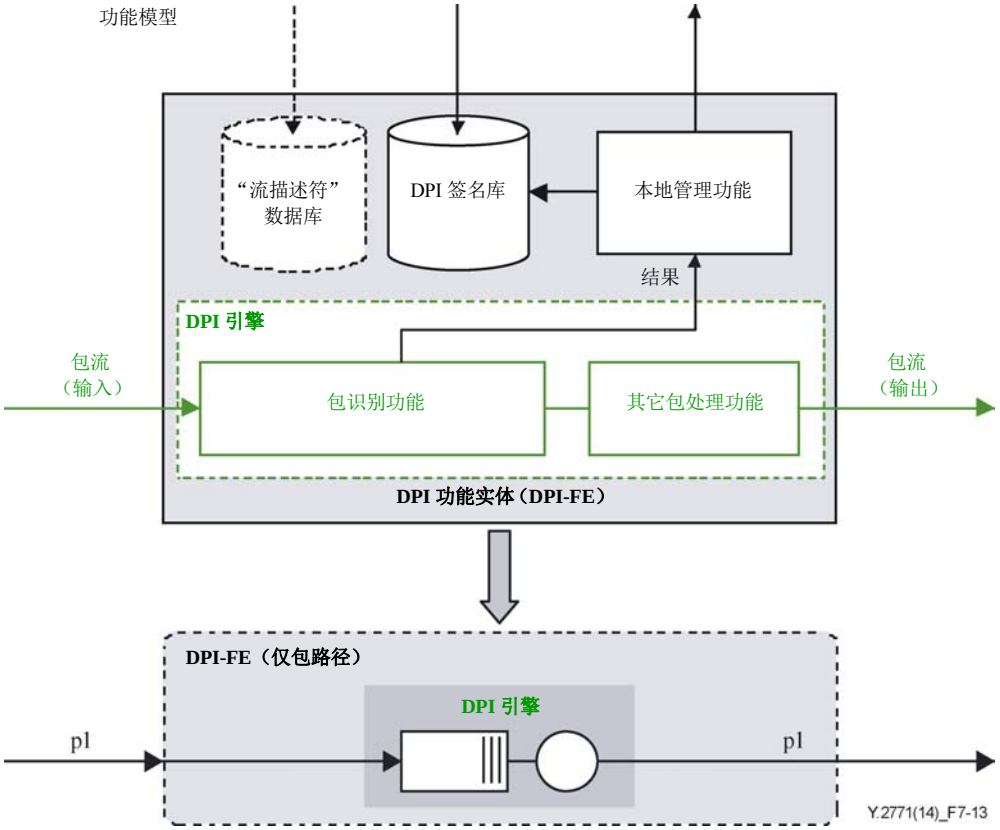


图7-13 – 带DPI引擎范围的DPI-FE基本流量模型

模型通过一个单一的服务器和一个有限的等待队列来表征。因此，服务器处理所有的包路径功能。阶段1服务器模型表示一个单向包流的流量模型。

7.3.2.2 DPI引擎：扩展至多阶段包路径处理

7.3.2.2.1 基于双阶段服务器的DPI引擎

图7-14提供了DPI引擎双阶段流量模型的一个例子。

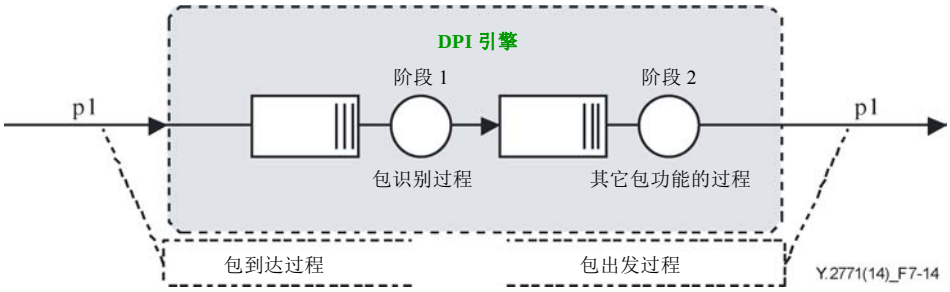


图7-14 – 流量模型DPI引擎：扩展至双阶段包路径

在本例中，第一个服务器负责处理DPI规则条件。

7.3.2.2.2 基于三阶段服务器的DPI引擎

- 一个DPI引擎可以在内部实现，作为分布式系统，例如，作为系列级联处理单元。例如，根据图7-3，样例功能模型表示三个处理阶段，分别称为“DPI扫描、DPI分析和DPI行动执行”，分别缩写为DPI-ScF、DPI-AnF和DPI-AcEF。

图7-15提供了一个相应的流量模型的例子。

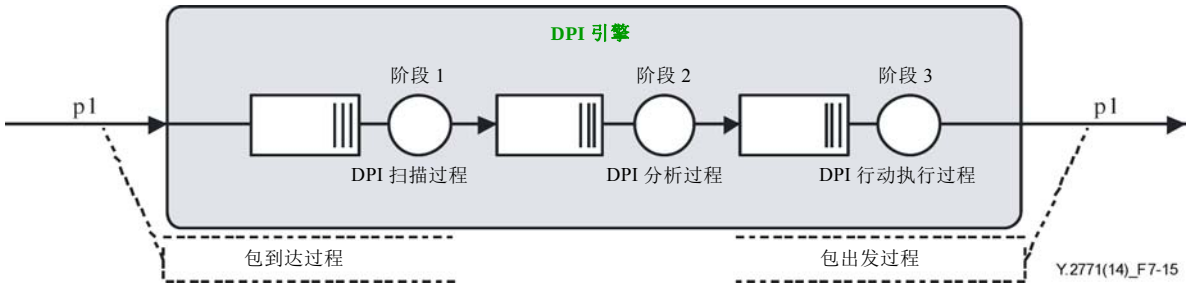


图7-15 – 流量模型DPI引擎：扩展到三阶段包路径

7.3.3 有关DPI引擎的扩展流量模型

7.3.3.1 单外部接口和内部并行

例如：有可能是路径外DPI实体（参见第6.1节），这通过一个单一的网络路由连接至包网络。这样一个DPI实体的目的可能是对大量选中的包流进行离线处理，即可能需要高处理能力。并行可能是实现高处理能力的一个选择方案。图7-16提供了一个在多并行DPI引擎层面上的流量模型例子。

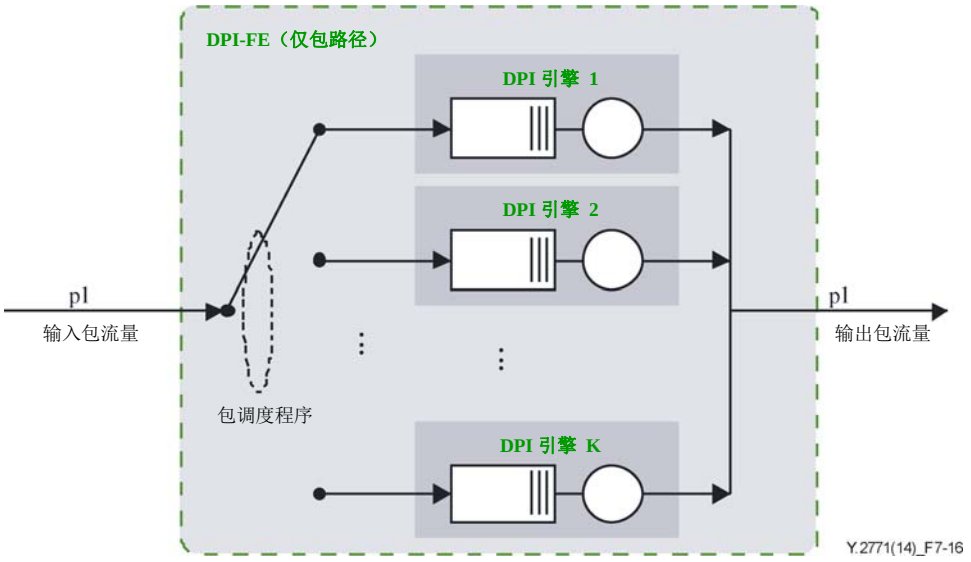


图7-16 – DPI引擎 – 单外部接口和内部并行

流量模型指的是一个*包调度程序功能*，用于将一个输入包指派给一个DPI引擎（服务器）。这样一个功能超出了本建议书的讨论范围。

注 – 例如，包调度程序可以是：

a) 简单的就是一个负载均衡算法（即仅基于DPI引擎服务器的估计负载状态进行调度），这使得实际上只感知无状态的DPI；

b) 基于流描述符信息（以便解决有状态DPI），但从流量建模的观点来看，而后至少会有一个阶段2服务器模型；

c) 任何其它形式的调度方法。

7.3.3.2 多外部接口和内部并行

位于网络核心层中的一个路径内DPI实体（参见第6.1节）通常提供多个物理*p1*接口。多个DPI引擎可并行地为所有的输入包流提供服务（参见图7-17）。通常要求所有的DPI引擎（如*K*）应连接至所有的输入包接口*P*1（如*N*）。因此，为此目的，将需*N-to-K*包交换网络功能。这样一个功能超出了本建议书的讨论范围。

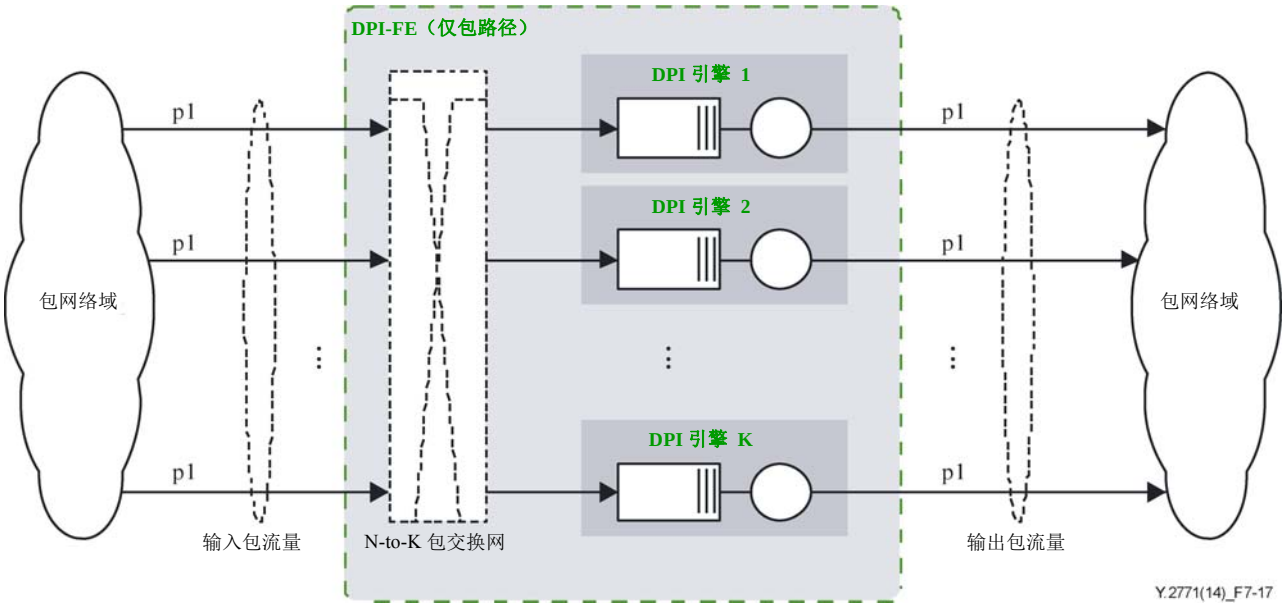


图7-17 – 多外部接口和内部并行

7.3.3.3 基于三阶段服务器模型的并行DPI引擎

基于一个阶段3DPI引擎模型（第7.3.2.2.2节）和DPI引擎层面并行性（第7.3.3.1节）的组合，图7-18和7-19描绘了一个扩展模型。

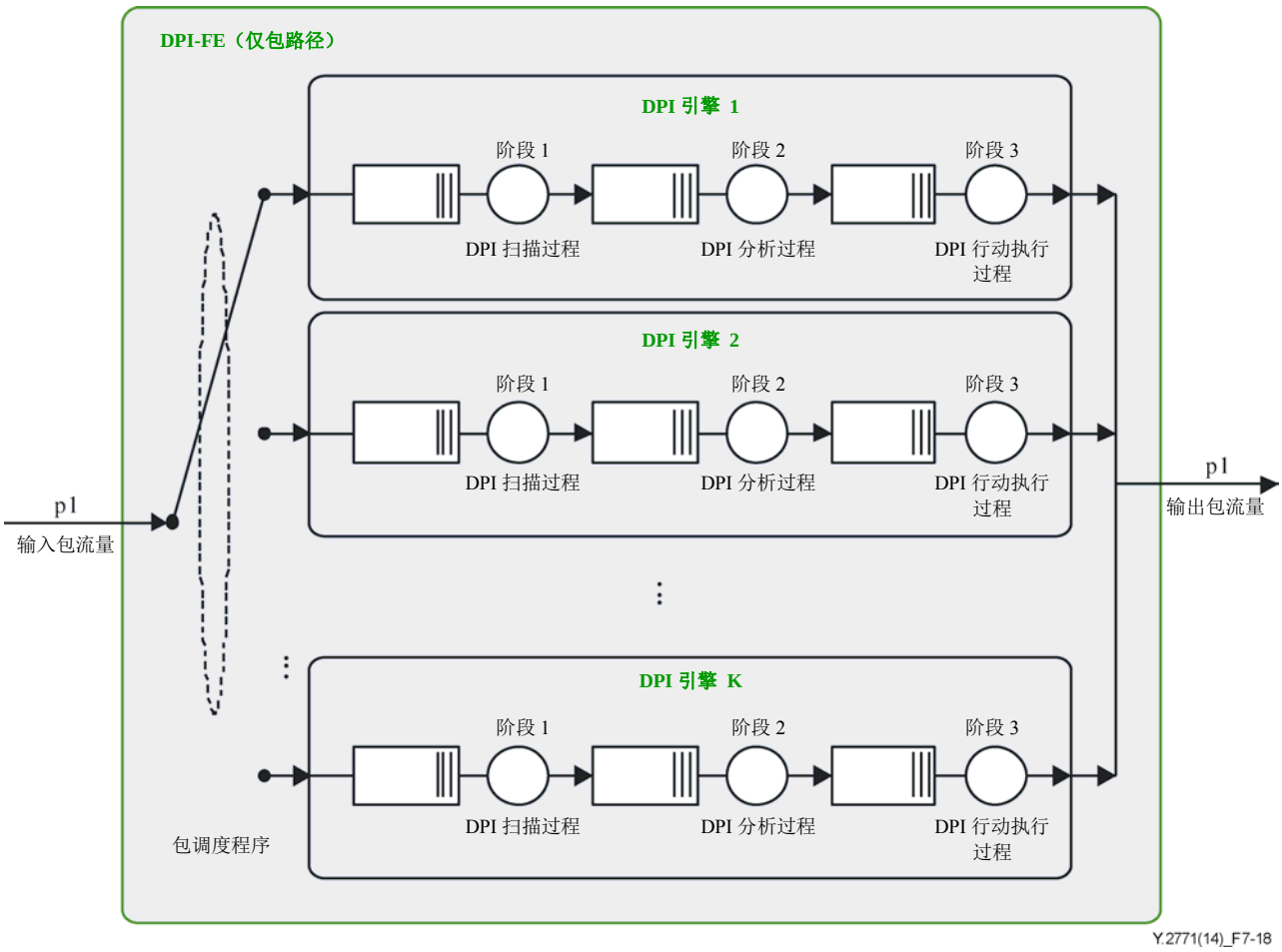


图7-18 – 基于三阶段服务器模型的并行DPI引擎（单外部接口）

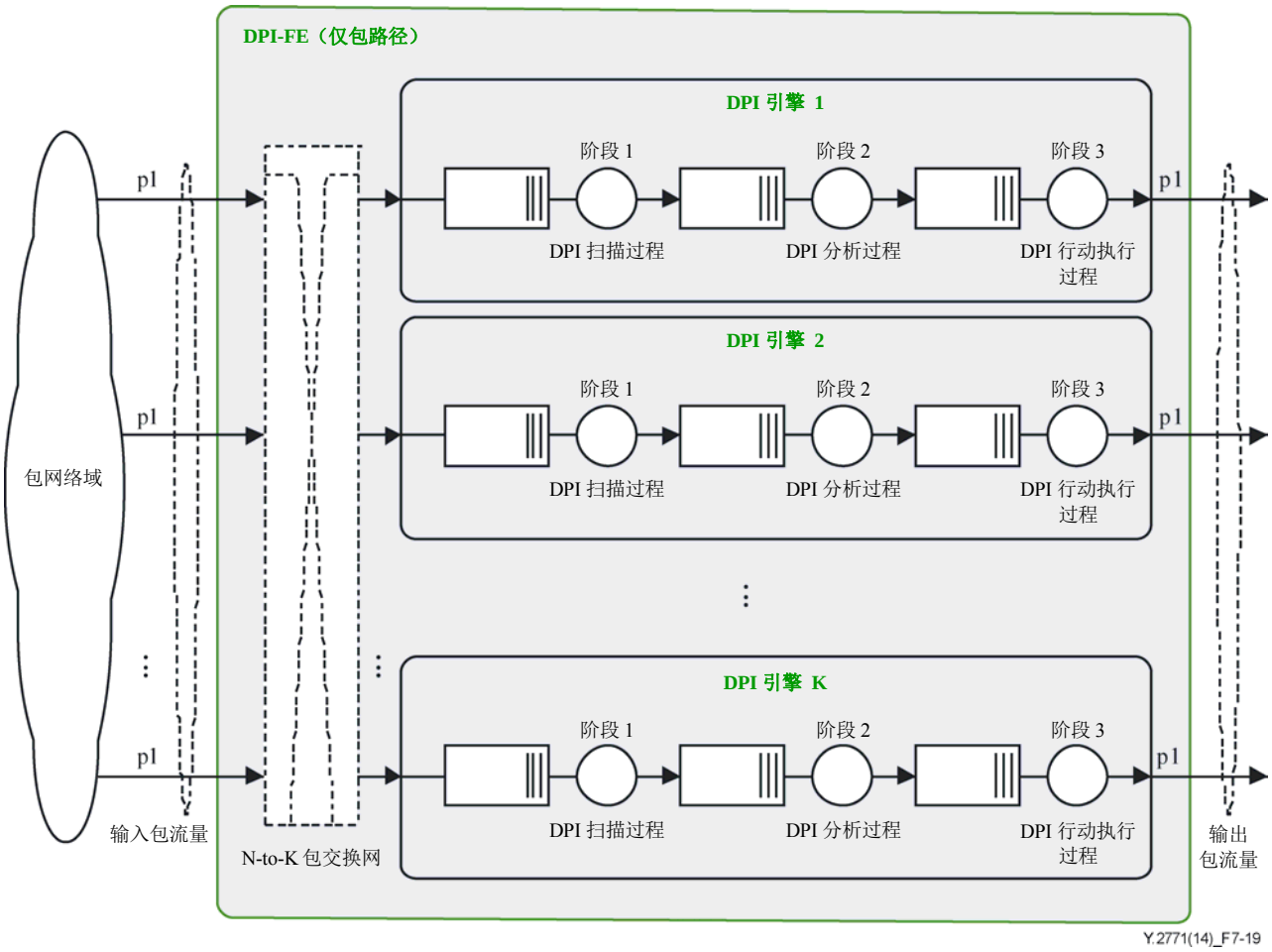


图7-19 – 基于三阶段服务器模型的并行DPI引擎（多外部接口）

流量模型通过完全并发运行的并行DPI引擎来表征，也就是说，DPI引擎之间没有任何相关性。这样一个DPI-PE体系结构，其最大性能将在所有服务器都被“最佳加载”（即没有任何服务器过载或欠载）时实现，这意味着在流量模型的两个维度上负载均匀地分布。设计这样一种体系结构相当富有挑战性，就提供的包负载而言，可能仅针对某些特定的流量分布。

这样一个背景可能会导致不同的体系结构，如在后续章节中所考虑的那样。

7.3.3.4 基于三阶段和内部并行的单DPI引擎

图7-20和图7-21描绘了一个关于单一DPI引擎的例子，它基于三个处理阶段以及每个阶段的并行性。各阶段并行水平不同，即每个阶段可能有不同数量的服务器（即K1、K2、K3有不同的值）。

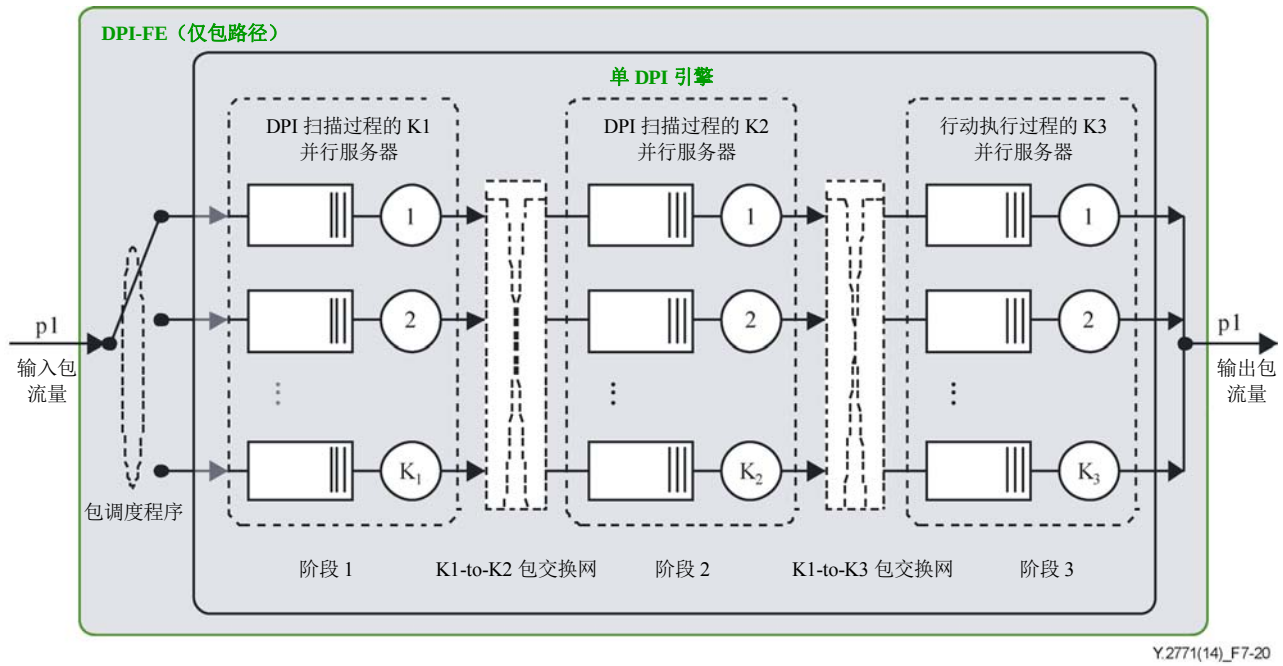


图7-20 – 基于三阶段和内部并行的单DPI引擎（单外部接口）

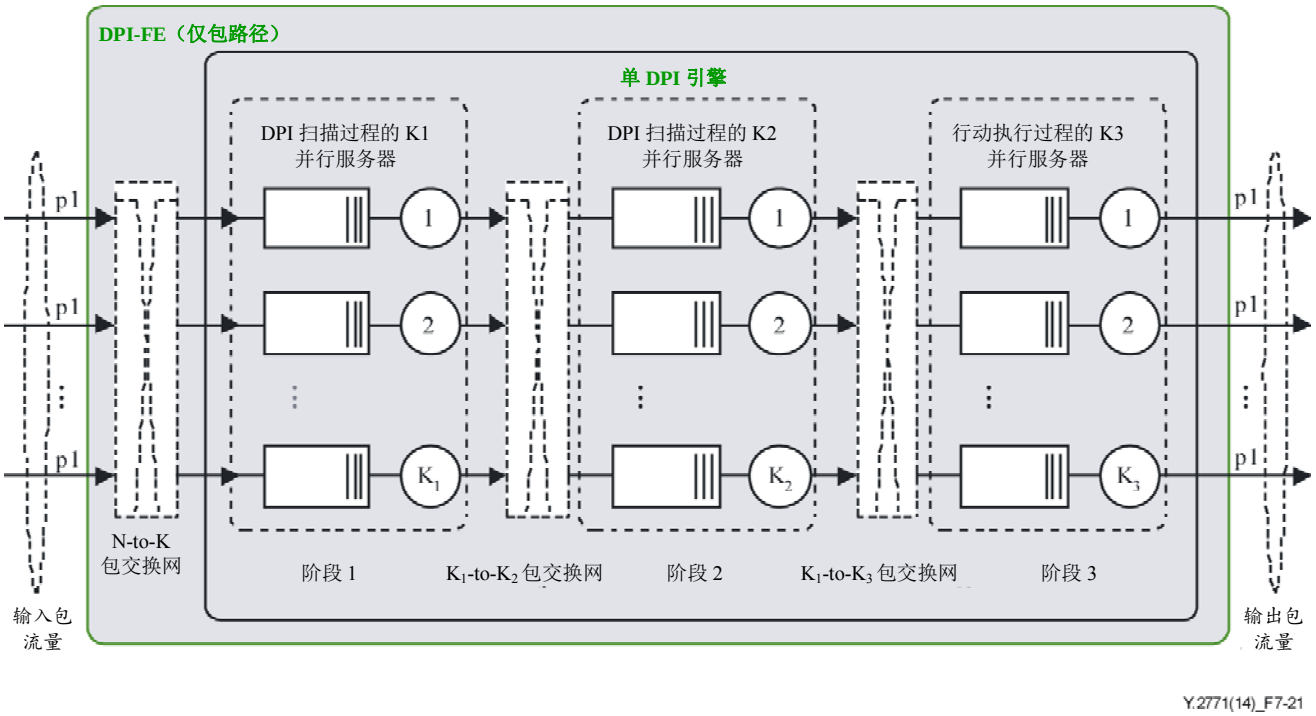


图7-21 – 基于三阶段和内部并行的单DPI引擎（多外部接口）

当DPI引擎需支持有状态的DPI时，出于本地“状态信息”之故，对同一流的所有包，都可能需要跨越各服务器的相同路径进行路由。该问题超出了上述流量模型的讨论范围。

7.4 可能之DPI-FE子部件的识别

对一个DPI-FE，可被划分为功能子部件，在之前的各节中已通过样例功能模型做了说明。表7-3概括了DPI-FE内典型的功能子部件。后续各节部分地提到了这些部件（例如，在讨论性能方面的问题、可能的功能或工作要求时，等等）。

表7-3 – 典型的DPI-FE子部件

部件	描述
DPI策略执行功能（DPI-PEF）：	有关DPI策略规则执行的一个功能元素，包括至少一个DPI策略信息库、一个DPI包识别功能和一个DPI行动执行功能。
进一步细化DPI-PEF： 1) 包处理路径	
1.1) DPI包识别功能（DPI-PIF）样例功能分解：	依据输入包流，负责DPI策略条件处理的功能元素。
1.1.1) DPI扫描功能（DPI-ScF）：	用于执行初始比较功能的一个功能元素（DPI-PIF的组成部分），由DPI策略规则条件决定。
1.1.2) DPI分析程序功能（DPI-AnF）：	用于执行后续比较功能的一个功能元素（DPI-PIF的组成部分），也由DPI策略规则条件决定（例如，与包头元素或内容（在包负载中）有关）。
1.2) DPI行动执行功能（DPI-AcEF）：	依据确定的DPI策略规则行动，用于对所涉之包执行操作的一个功能元素。
2) DPI策略信息库（DPI-PIB；注1）功能：	代表数据库的一个功能元素，包含一个有一个或多个DPI策略规则入口的集合（如下所示）。
a) DPI策略规则入口：	表的入口，包含一个DPI策略规则（注2）。
i) DPI策略规则条件（简称“规则条件”）：	一个表达式（典型地为布尔类型）。一个条件也称为一个匹配准则（例如，出于代表部分匹配、完全匹配、前缀匹配、最长前缀匹配等的条件类型之故）。
ii) DPI策略规则行动（简称“规则行动”）：	一个行动，在对所有规则特定的策略条件和行动的执行结果进行评估后执行。
注1 – 也称为：*规则表、策略签名库，或者就称为：签名库*。 注2 – 可执行一个或多个规则。此类规则可静态地预定义（通过包节点的配置管理，称为DPI策略管理），或者标记（通过一个策略控制接口），或者动态地在本地生成（通过一个本地PDF）。DPI策略规则用一系列条件来比较协议控制信息（PCI，即包头元素）或者包流的负载/内容，以确定字符串匹配是否成功。	

7.5 容错模型

网络节点（如DPI节点）的可靠性和可用性对网络节点所在的网络而言至关重要。当网络节点停止工作时（例如，参见ITU-T X.731]中的工作状态模型），可能导致网络灾难，可使所有网络用户被迫进入脱机状态，致使大量有价值的信息丢失。因此，追求网络节点的高可靠性和高可用性至关重要。作为一种网络节点的DPIc节点，也应支持高可靠性和可用性。

使用故障容差法，DPI“1 + N”冗余组旨在提高利用DPI节点部署之网络的可靠性和可用性。

DPI“1 + N”冗余组可靠性可通过以下参数来计算：

1) MTBF：平均无故障时间，是DPI“1 + N”冗余组故障之间的平均时间。

2) MTTR：平均修复时间，是采取措施使出现故障的DPI“1 + N”冗余组恢复正常工作所需的时间。

DPI“1 + N”冗余组的可用性可通过如下公式来计算（参见[ITU-T G.602]）：

3) 可用性 = 运行时间/（停机时间 + 运行时间）或者

4) 可用性 = MTBF/（MTBF + MTTR）。

5) 在一个DPI“1 + N”组冗余内，冗余功能部件的数量取决于特殊的实现，它超出了本建议书的讨论范围。在一个冗余组内工作于活跃/备份模式的功能部件，只有一个功能部件可以作为活跃的功能部件，其它的功能部件则作为备份功能部件。当活跃的功能部件停止工作时，一个且只有一个备份的功能部件将变成为新的、活跃的功能部件，之前的、活跃的功能部件将变成为一个备份的功能部件。

6) 活跃功能部件与备份功能部件之间的接口，用于活跃与备份功能部件之间的切换，它独立于DPI以及具体的实施方案，因而超出了本建议书的讨论 范围。

7) 提出多种容错模型，用于说明DPI节点级容错模式（第7.5.1节）、DPI PEF级容错模式（第7.5.2节）、DPI PIB级容错模型（第7.5.3节）和DPI引擎级容错模式（第7.5.4节）。

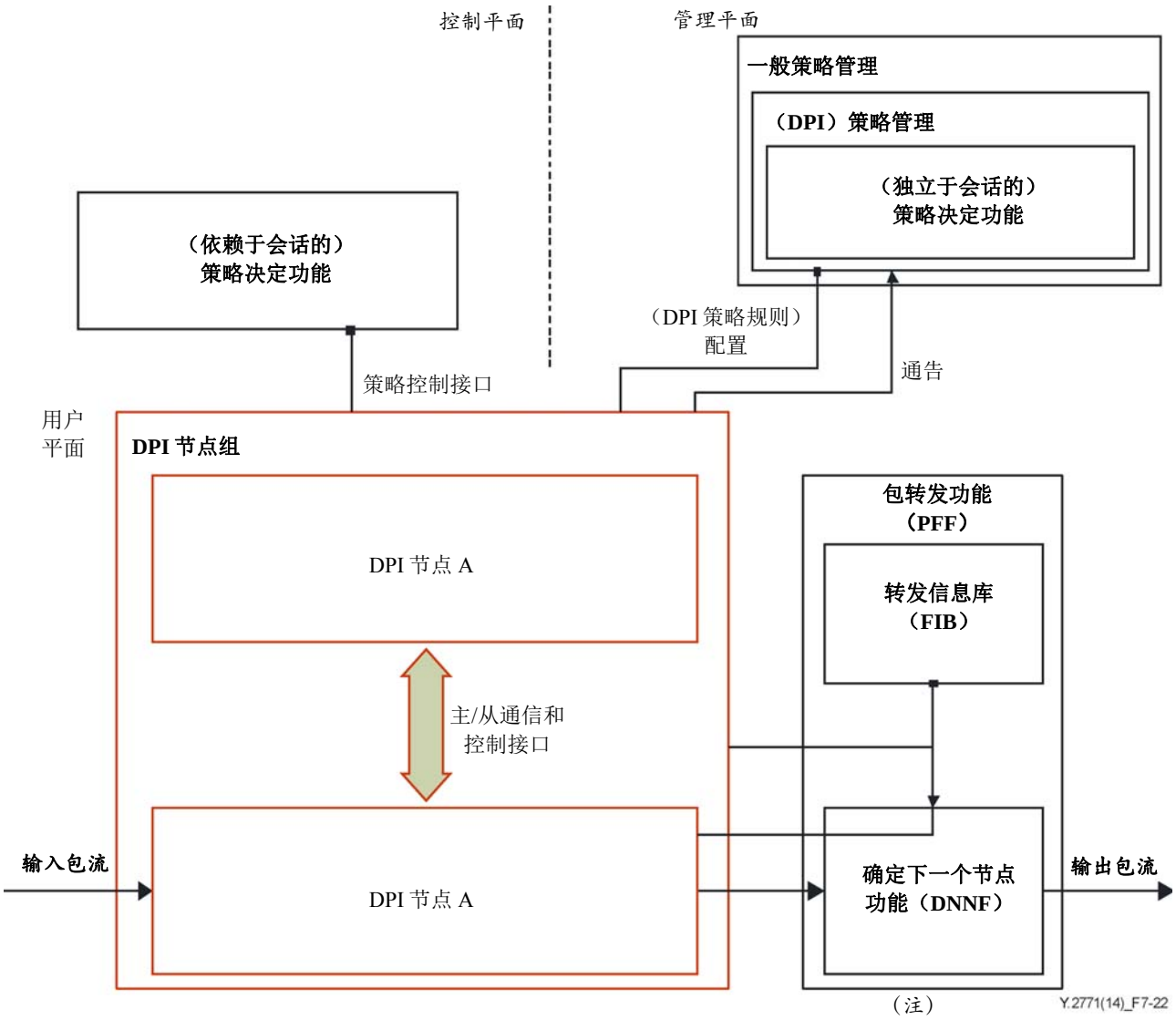
8) 所有容错模型都基于DPI“1 + N”冗余组（换言之，该功能部件的冗余性，例如，在图7-22中的DPI节点）。

9) 活跃功能部件和备份功能部件应通过数据同步方法保持完全一致的信息，如PIB。数据同步方法依赖于特殊的实现，它超出了本建议书的讨论范围。

7.5.1 DPI节点级容错模型

图7-22描绘了带DPI节点级可靠性保证的DPI模型，两个或更多个DPI节点被部署在一起，以形成一个DPI节点组（一个DPI“1 + N”冗余组，DPI节点为功能部件），一个DPI节点作为活跃DPI节点，其它作为备份节点DPI。此外，根据正常操作要求，活跃和备份DPI节点必须复制内部信息。一旦活跃DPI节点停止服务，备份DPI节点之一将自动成为活跃DPI节点。

虽然在图7-22中只描绘了两个DPI节点，但在有两个以上DPI节点的情况下，容错模型是类似的（出于“1 + N”冗余概念之故）。



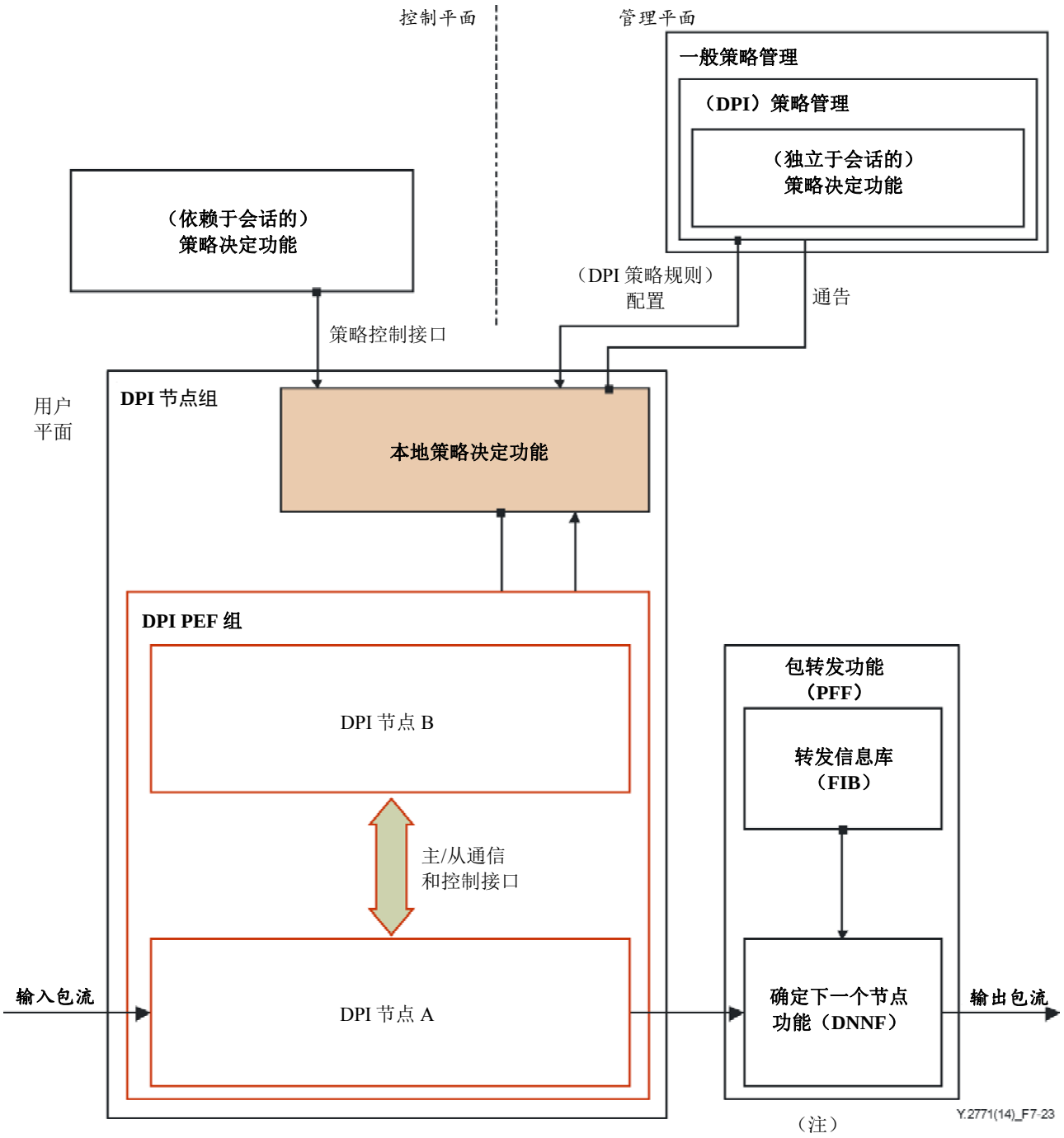
注 – PFF已超出本建议书的讨论范围。

图7-22 – 带DPI节点级可靠性保证的DPI模型

7.5.2 DPI PEF级容错模型

图7-23描绘了带DPI PEF级可靠性支持的DPI模型，在一个DPI节点内设计了两个或更多个DPI PEF部件（换言之，一个DPI“1 + N”冗余组，DPI PEF部件为其中的功能部件），一个DPI PEF部件作为活跃部件，其它DPI PEF部件作为备份部件。在出现故障的情况下，切换过程类似节点级可靠性支持的情形（参见第7.5.1节）。

虽然在图7-23中只描绘了两个PEF部件，但在有两个以上PEF部件的情况下，容错模型是类似的。



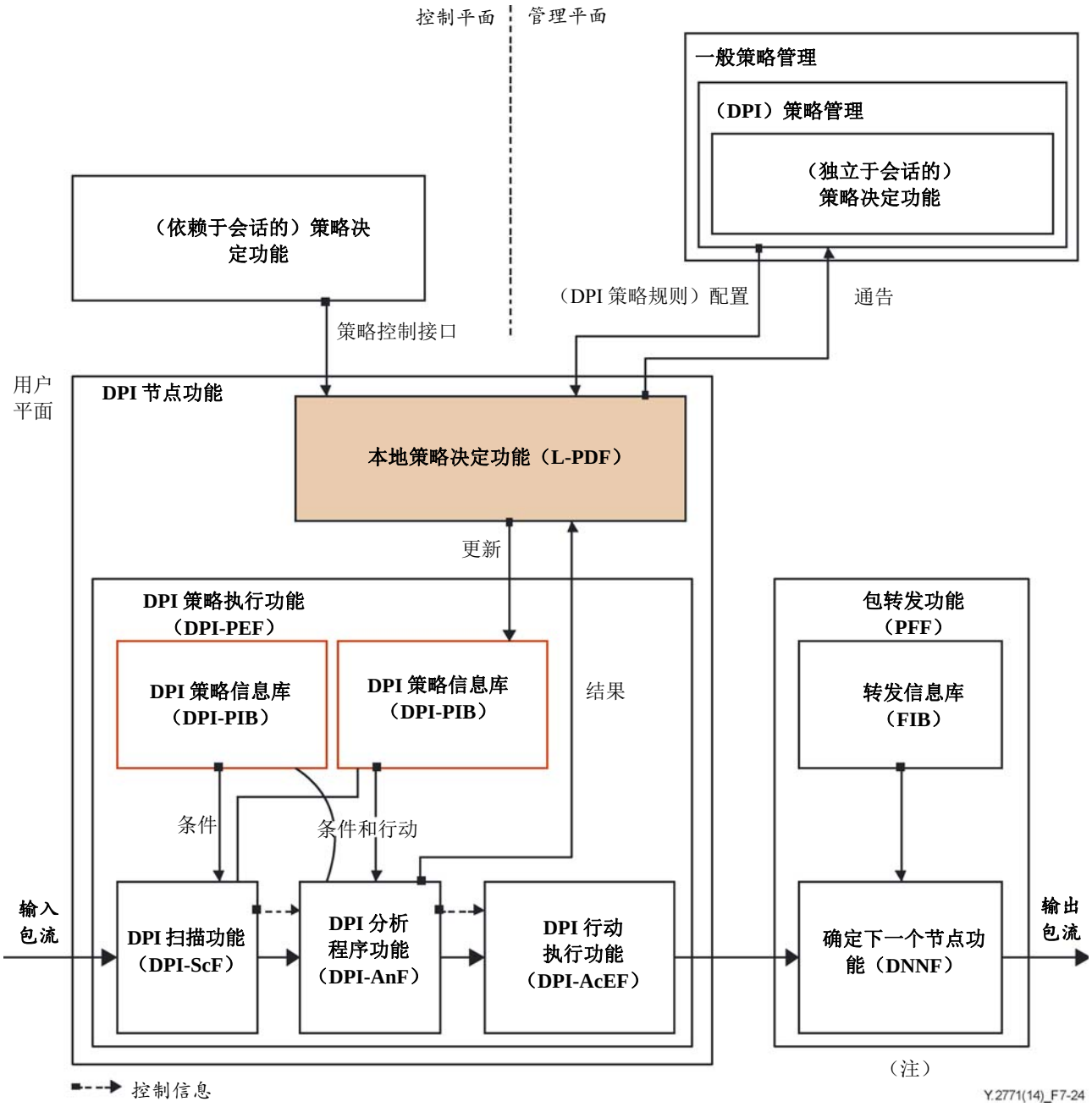
注 – PFF已超出本建议书的讨论范围。

图7-23 – 带DPI PEF级可靠性支持的DPI模型

7.5.3 DPI-PIB级容错模型

图7-24描绘了带DPI PIB级可靠性支持的DPI模型，在一个DPI节点内有两个或更多个DPI PIB的拷贝（换言之，一个DPI“1 + N”冗余组由两个或更多个DPI PIB的拷贝构成），所有的DPI PIB均保持同步，因此包含相同的信息。一个DPI PIB作为活跃PIB，其它PIB作为备份PIB。在活跃PIB出现故障的情况下，备份PIB之一将自动变为活跃PIB。

虽然在图7-24中只描绘了两个DPI PIB，但在有两个以上DPI PIB的情况下，容错模型是类似的。



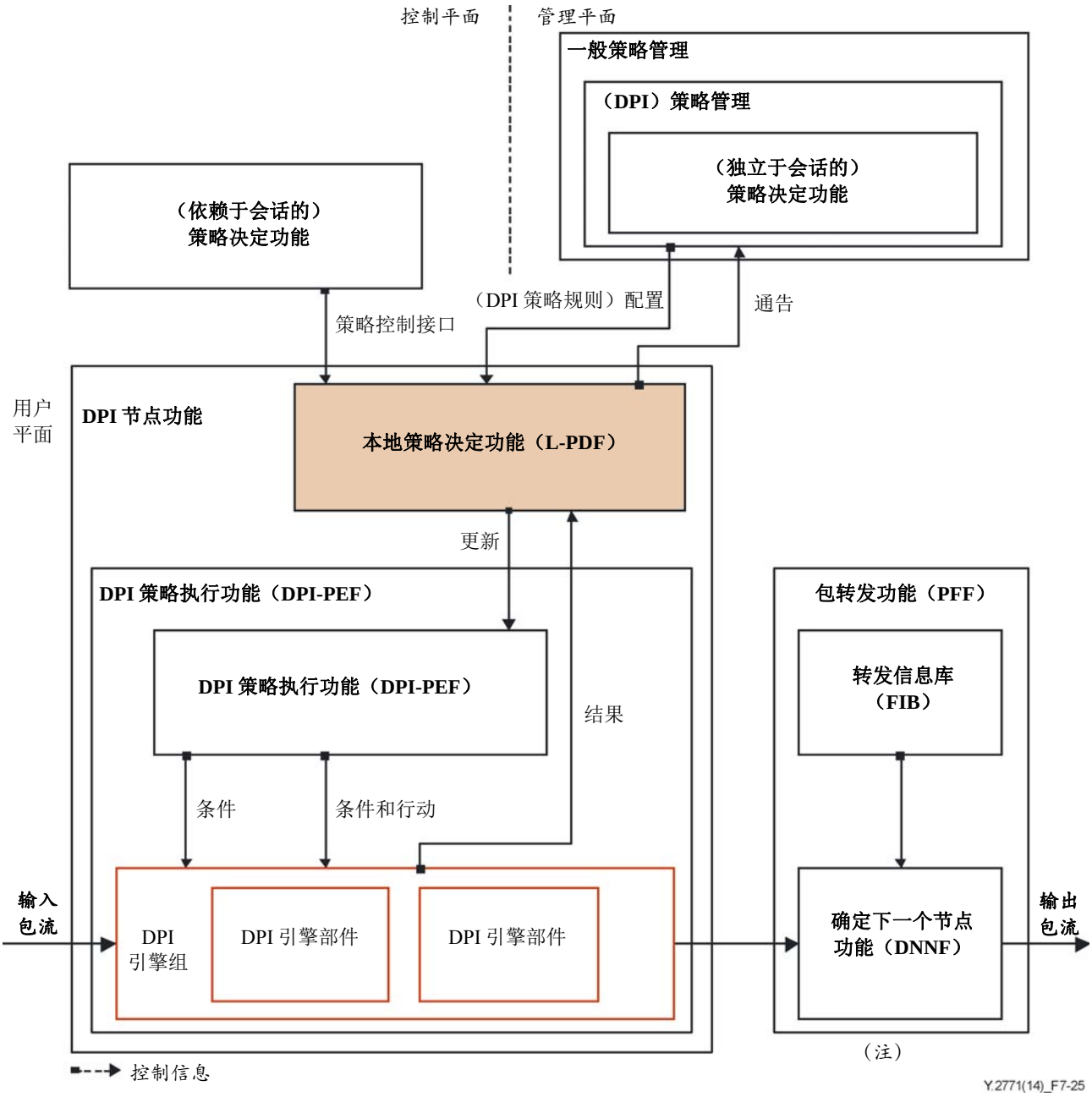
注 – PFF已超出本建议书的讨论范围。

图7-24 – 带DPI PIB级可靠性保证的DPI模型

7.5.4 DPI引擎级容错模型

图7-25描绘了带DPI引擎级可靠性支持的DPI模型。容错原则等同之前所述的、更高级别上的容错原则。

虽然在图7-25中只描绘了两个DPI引擎部件，但在有两个以上DPI引擎部件的情况下，容错模型是类似的。



注 – PFF已超出本建议书的讨论范围。

图7-25 – 带DPI引擎级可靠性保证的DPI模型

8 性能框架

8.1 目的和性能方面的考虑范围

本节描述一个框架以及确定和设计DPI相关性能指标的程序。这些性能指标可用来表征DPI实体的行为。

性能框架基本上涵盖的领域：

1) 性能指标：

一个DPI实体的容量、可用性和性能可通过性能指标来表征。主要目的是：

a) 明确是否存在，非DPI性能指标可重复使用；

b) 认识DPI特定的性能指标，已由致力于DPI的其它组织引入；

c) 确定新的DPI特定的性能指标，指的是这样一个指标的定义；以及

d) 将指标集划分为关键性能指标（KPI）等。

2) 性能需求:

此类DPI需求关联到特定的性能指标。实现相关的性能需求超出了范围。因此，基本上有望得出定性的或相对的性能需求。额外的定量或绝对的性能需求规范只可能提供给一些有限的领域（例如，如果最大节点传送延迟预算将受制于总的端到端网络方面的考虑...）。

3) 性能基准:

相对识别和规范公认的、有意义的基准情形而言，确定基准是一个相当有挑战性的领域。DPI性能基准的定义基本上超出了范围。不过，在尝试指定DPI实体的性能基准时，本建议书可以提供有关审议方面的信息和指导。

新的性能度量类型（也称为性能指标）的定义应基本上遵循[b-IETF RFC6390]的指南，因此，原则上，至少应融入：

- 度量名称和度量描述；
- 测量或计算方法；
- 测量单元；以及
- 性能指标定义不应受制于统计参数，如最小值、最大值、平均值、PDF、方差等。这些方面更应受制于需求规范。

8.2 性能测量

8.2.1 概述 – DPI节点的性能指标

性能要求与性能指标有关。关键指标类型被称为关键性能指标（KPI），代表总的指标集合的一个子集。

8.2.1.1 将DPI相关性能度量作为KPI的指南

本建议书采用下列KPI定义（注1-源自[ETSI TS132.410]）：

- **通常的关键性能指标（KPI）：**

  是用来评估过程性能的主要指标，作为网络要素核心功能的指标。

- **DPI实体的关键性能指标（KPI_{DPI}）：**

  KPI_{DPI} – 在本建议书范围内－因此用于表征DPI引擎的性能（参见[ITU-T Y.2770] 第3.2.6节，也称为DPI包处理路径）。

注2 – 性能指标（PI）的概念等同于本建议书中的性能度量。

为了将DPI性能指标分类为关键性能指标或非关键性能指标，应考虑到以下准则。DPI实体的关键性能指标应满足下列条件：

1) 性能指标应受制于包处理路径本身，其中，DPI策略规则在包对象上予以执行（因此，不是DPI包路径之外的任何其它DPI功能）；以及

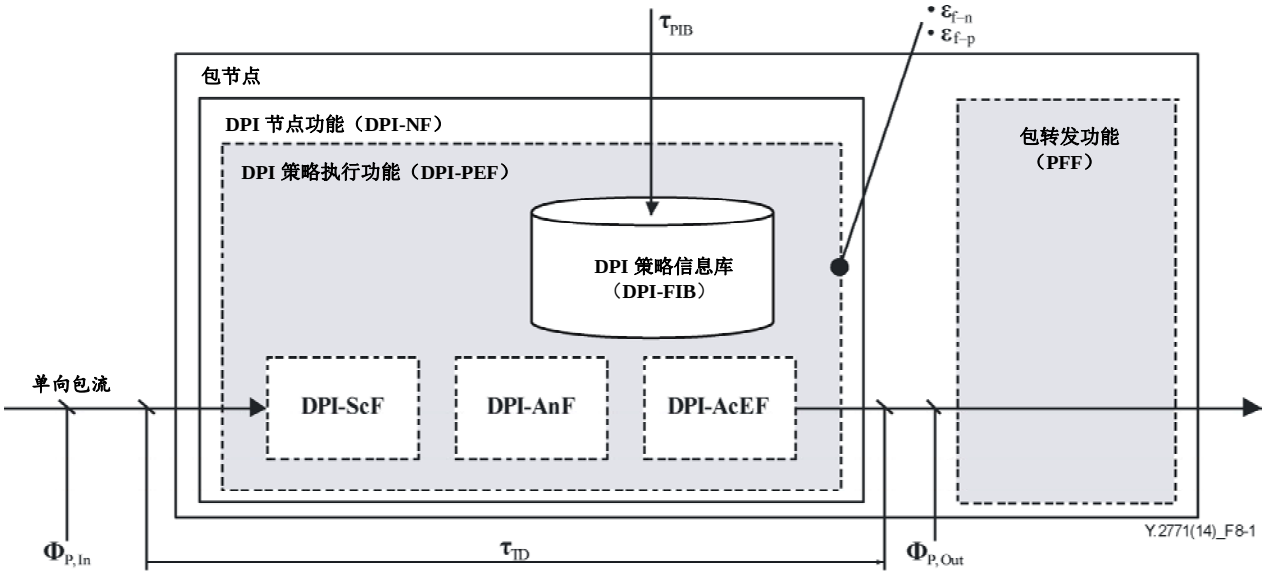
2) 性能指标应独立于DPI用例（因此，不是特别针对特殊DPI服务的应用）；以及

3) 性能指标应独立于IP层之下和之上的特定协议（因此，例如，不是特别针对某个特殊的IP传输协议（如TCP）、IP应用协议等）；以及

4) 性能指标应独立于DPI实体的物理实现（因此，与实施方案特定的问题无关，如能耗问题、功耗问题、先进处理部件等）。

8.2.1.2 DPI节点的典型关键性能指标

图8-1说明了一些众所周知的、有关DPI节点的KPI例子（KPI_{DPI}清单并不详尽）。KPI_{DPI}类型列于下图。相应的性能需求（如果有的话）在各节中予以描述。



注1 – 包节点和PFF涉及性能度量指标的明确规范，但这两个实体均超出本建议书的讨论范围。
注2 – PFF只出现在路径内DPI模式中。

图8-1 – 概述 – 有关DPI节点的关键性能指标

典型地，主要的性能度量指标是：

- KPI“（DPI）**节点内部传送延迟**”τ_{TD} [μs]：参见第8.2.3.1节。
- KPI“（DPI）**包处理速率**”$\phi_{P,\,In}[s^{-1}]$：参见第8.2.3.2节。
- KPI“（DPI）**错误率**”ε_{DPI}：参见第8.2.3.3节。
  - KPI“（DPI）**错误地判为对的错误率**”$\varepsilon_{f\text{-}p}$。
  - KPI“（DPI）**错误地判为错的错误率**”$\varepsilon_{f\text{-}n}$。
- KPI“（DPI）**包成功识别率**”$\phi_{P,\,Identified}[s^{-1}]$：参见第8.2.3.4节。

8.2.2 有关性能测量定义的正式模板

本建议书中的性能测量定义（使用依照表8-1的模板），本身源自IETF模板（依照[b-IETF RFC6390] 第5.4.4节“性能度量定义模板”）。

表8-1 – 有关性能测量定义的正式模板

测量名称：	N	
符号：	I	
测量描述：	N	
度量或计算方法：	N	
度量单位：	N	
有潜在度量域的度量点：	N	
度量时序：	N	
实施：	I	
验证：	I	
使用和应用：	I	如“实时DPI”、“非实时DPI”
报告模型：	I	
类型“KPI”：是/否？	I	即“KPI”、“非KPI”或“未分类”
注 – 规范性（N）和说明性（I）描述要素。		

使用模板，以便确保本建议书引入的指标能满足一定的最低要求质量。不过，因本建议书的“框架字符”，将主要提供规范性的描述元素。空（说明性的）描述元素是一个指标，在实际的性能指标中使用这样一个指标将首先需要做进一步的规范工作，以便得到完整的、适用的指标。例如，“实施方案”条目的描述已超出“框架”建议书的范围，或者无“核实”条目信息的指标定义是无用的（原因是，例如，需要校准测量功能）。

8.2.3 有关DPI实体的通用性能测量定义

8.2.3.1 DPI测量“节点内部传送延迟”

DPI相关的策略规则应用于特定包流的每一个包上。此类政策执行基本上在带“DPI引擎”支持（即提供DPI的一个策略执行点（PEP））的、包节点的包转发路径（如一个IP跳）中引入额外的服务和等待时间。性能指标节点内部传送延迟表示通过网络元素本身的包传送延迟。

表8-2提供了测量定义。

表8-2 – DPI测量“节点内部传送延迟”

测量名称：	N	节点内部传送延迟
符号：	I	τ_{TD}
测量描述：	N	通过一个DPI节点的包累积等待和服务时间。
度量或计算方法：	N	通过测量DPI节点功能物理或逻辑表示之包接 口处的单个包进和出时间（$T_{in,\,i}$和$T_{out,\,i}$），来计算该值。 前提条件：测量实体必须能够识别单个的包。 警告：该指标通常取决于负载，原因是，节点内部传送延迟由节点内部服务和等候时间构成。负载，或者更精确地为DPI提供的负载$A_{DPI\text{-}NF}$，由输入包速率$\phi_{P,\,In}$和每个包的平均服务时间$T_{H,\,Packet}$给出，根据以下公式： $A_{DPI-NF} = \phi_{P,In} \cdot T_{H,Packet}$ 主要负载依赖性（参见第8.3节）： $\tau_{TD} = f(A_{DPI\text{-}NF})$
度量单位：	N	ns
有潜在度量域的度量点：	N	参见图8-1（流量模型）。
度量时序：	N	该度量可在很宽的时间间隔上使用。
实施：	I	–
验证：	I	–
使用和应用：	I	“实时DPI”
报告模型：	I	典型地，将作为性能管理的一部分。
类型“KPI”：是/否？	I	“KPI”
注 – N：规范性描述要素；I：说明性描述要素		

8.2.3.1.1 进一步的讨论

a) DPI对非DPI节点：

IP节点的例子：一个DPI节点的传送延迟可能会从根本上比一个传统IP节点的传送延迟要大（依据[IETF RFC1812]，即是一个IP跳或路由器），出于本地IP转发功能顶层的额外服务功能之故。

b) 典型的关系：

节点内部传送延迟τ_{TD}也可依赖于（因为是实施方案特定的）以下参数：

- DPI策略规则的数量N_{db}（例如，当串行处理多个DPI策略规则时，增加的服务时间），
- 包大小Sp[位]（例如，增加的搜索或比较时间，作为DPI策略条件验证的一部分），包大小Sp可能与通过[b-IETF RFC2544]给出的L2帧大小值有关，以及

– DPI引擎数量N_{DPIeng}（例如，考虑内部的并行性，参见第7.3.3节）。

因此，在这个例子中，τ_{TD}是参数*Ndb, Sp*和N_{DPIeng}的一个函数，即：

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

这三个参数因此影响每个包的平均服务时间$T_{H, Packet}$（在表8-3中引入）：前两个参数为增加的因素，而第三个参数会导致降低的平均服务时间。

c) 定性的性能要求：

传送延迟（出于DPI处理之故，含额外的服务时间）不应超过总的通信服务相关的任何端到端实时要求。

注1 – 这样一种包转发能力也通俗地被称为“线速处理”。

注2 – 这样一种性能目标可限定每个包所执行的策略规则数量（只是出于有限的服务时间预算之故）。

8.2.3.2 DPI测量“包处理速率”

表8-3提供了测量定义。

表8-3 – DPI测量“包处理速率”

测量名称：	N	包处理速率
符号：	I	$\phi_{P, In}$
测量描述：	N	DPI-PEF的包处理速率。 这是输入包速率，原因是，对每一个输入包都执行DPI策略规则。输出速率等于或小于输入速率（由于可能的包丢弃行动）， $\phi_{P,In} \le \phi_{P,Out}$
度量或计算方法：	N	对一段时间内、在输入接口*p1*处观测到的所有包进行计算。而后，该值除以此段时间内观测到的数量。
度量单位：	N	s^{-1}
有潜在度量域的度量点：	N	参见图8-1（流量模型）。
度量时序：	N	该度量可在很宽的时间间隔上使用。典型地，时间尺度在秒级水平上。
实施：	I	–
验证：	I	–
使用和应用：	I	“实时DPI”
报告模型：	I	典型地作为性能管理的一部分。
类型“KPI”：是/否？	I	“KPI”
注 – N：规范性描述要素；I：说明性描述要素		

DPI包处理速率ϕ_P取决于许多参数，如以下参数的组合：

– DPI策略规则的数量，或者DPI PIB的大*Ndb*；

– 包的大小*Sp*，包的大小*Sp*可与由[b-IETF RFC2544]给出的、L2帧的大小相关；以及

– 可能的其它参数。

例子：当$(\phi_P, N_{db}, Sp) = (200, 1000, 64)$时，当策略规则数目小于1000且包大小为64时，处理速率至少为200包/秒。

定性行为在第8.3节中予以描述。通过添加新的DPI策略规则、修改现有的DPI策略规则或删除DPI策略规则来升级DPI-PIB，不应影响标称的DPI包处理速率ϕ_P（ϕ_P等于$\phi_{P,In}$）。

8.2.3.3 DPI测量“错误率”

*错误地判为错*和*错误地判为对*的总和与DPI节点的错误率有关。这些性能指标仅关系到DPI节点的统计决策（如果有的话）。DPI-PEF将为众多DPI策略规则提供一个确定性的行为，不过，可能存在带统计策略条件的DPI策略规则或者带统计流量信息的包流，它们可导致不正确的DPI-PEF决策。

表8-4提供了测量定义。

表8-4 – DPI测量“错误率”

测量名称：	N	错误率
符号：	I	ε_{DPI}
测量描述：	N	*错误地判为错*（参见第8.2.3.3.2节）和错误地判为对（见第8.2.3.3.1）的总和形成DPI节点的结果。
度量或计算方法：	N	直接测量：不可能（注2） 间接测量（计算）： $\varepsilon_{DPI} = \varepsilon_{f-n} + \varepsilon_{f-p}$
度量单位：	N	–
有潜在度量域的度量点：	N	参见图8-1（流量模型）。
度量时序：	N	从被服务用户实例的角度来看，测量时间间隔依赖于时间尺度。 （注3）
实施：	I	–
验证：	I	–
使用和应用：	I	“实时DPI”
报告模型：	I	典型地，将作为性能管理的一部分。
类型“KPI”：是/否？	I	“KPI”

注1 – N：规范性描述要素；I：说明性描述要素。

注2 – 该性能指标就是所谓的组合指标，也就是说，它可能无法直接测量，但可以从已测得的基础指标来组成（参见[b-IETF RFC6390] 第5.3.1节）。

注3 – 通常的被服务用户实例代表一个远程实体（以下简称“用户”），兴趣在测量。例如：性能管理体系，DPI PD-FE。

8.2.3.3.1 DPI测量“错误地判为对的错误率”

表8-5提供了测量定义。

表8-5 – DPI测量“错误地判为对的错误率”

测量名称：	N	错误地判为对的错误率
符号：	I	$\varepsilon_{f\text{-}p}$
测量描述：	N	被错误地判为对而实际为错的实例所占的比例。
度量或计算方法：	N	该指标的测量本质上具有挑战性，因此，本建议书给出只能给出示值： 典型地，一个足够大包序列的已知样式将被发送给DPI实体。预期结果（由所用的DPI策略规则给出）将与从DPI过程中得到的测量结果进行比较。 测量可在侵入式和非侵入式的测试类型中进行。
度量单位：	N	–
有潜在度量域的度量点：	N	参见图8-1（流量模型）。
度量时序：	N	从被服务用户实例的角度来看，测量时间间隔依赖于时间尺度。
实施：	I	–
验证：	I	–
使用和应用：	I	“实时DPI”
报告模型：	I	典型地，将作为性能管理的一部分。
类型“KPI”：是/否？	I	是
注 – N：规范性描述要素；I：说明性描述要素。		

例子1：

DPI策略条件C_i指的是识别“应用类型*X*”以及包识别功能（DPI-PIF）将“应用类型*Y*”的包判为“应用类型*X*”，这是一个错误地判为对的结果。

例子2：

该指标的计算对基于Bloom过滤程序的概率DPI是可能的（参见附录1），参数值如下：

- m = Bloom过滤程序以比特计的大小
- n = 结合S中的签名数量
- k = 用于生成Bloom过滤程序的散列函数数量

错误地判为对的错误率$\varepsilon_{f\text{-}p}$由以下方程式给出：

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

计算的和预期的结果而后可以通过测量来校验。

8.2.3.3.2 DPI测量“错误地判为错的错误率”

表8-6提供了测量定义。

表8-6 – DPI测量“错误地判为错的错误率”

测量名称：	N	错误地判为错的错误率
符号：	I	$\varepsilon_{f\text{-}n}$
测量描述：	N	被错误地判为错而实际为对的实例所占的比例。
度量或计算方法：	N	参见表8-5中相应的入口。
度量单位：	N	–
有潜在度量域的度量点：	N	参见图8-1（流量模型）。
度量时序：	N	从被服务用户实例的角度来看，测量时间间隔依赖于时间尺度。
实施：	I	–
验证：	I	–
使用和应用：	I	“实时DPI”
报告模型：	I	典型地，将作为性能管理的一部分。
类型“KPI”：是/否？	I	是
注 – N：规范性描述要素；I：说明性描述要素		

例子：

DPI策略条件C_i指的是识别“应用类型*X*”以及DPI包识别功能（DPI-PIF）未将“应用类型*X*”的包判为“应用类型*X*”，这是一个错误地判为错的结果。

8.2.3.3.3 与运行时间错误的关系

作为执行DPI策略规则的运行时间环境的DPI引擎，在本质上是没有错误的。不过，运行时间错误率和DPI指标“错误率”代表不同的性能指标。

背景信息：

例如：根据[b-IETF RFC4011] 第4.1节的运行时间异常事件，提供了关于运行时错误概念的信息：

> [...]运行时间异常（RTE） – 一个运行时间异常指的是在语言或函数处理过程中引起的一个致命错误。如果在一个脚本调用过程中，出现运行时间异常，那么将立即终止该脚本的执行。如果在处理一个元素时，一个策略条件遇到一个运行时间异常，那么该元素不匹配条件，相关的动作将不会在该元素上予以运行。[...]

8.2.3.4 DPI测量“包成功识别率”

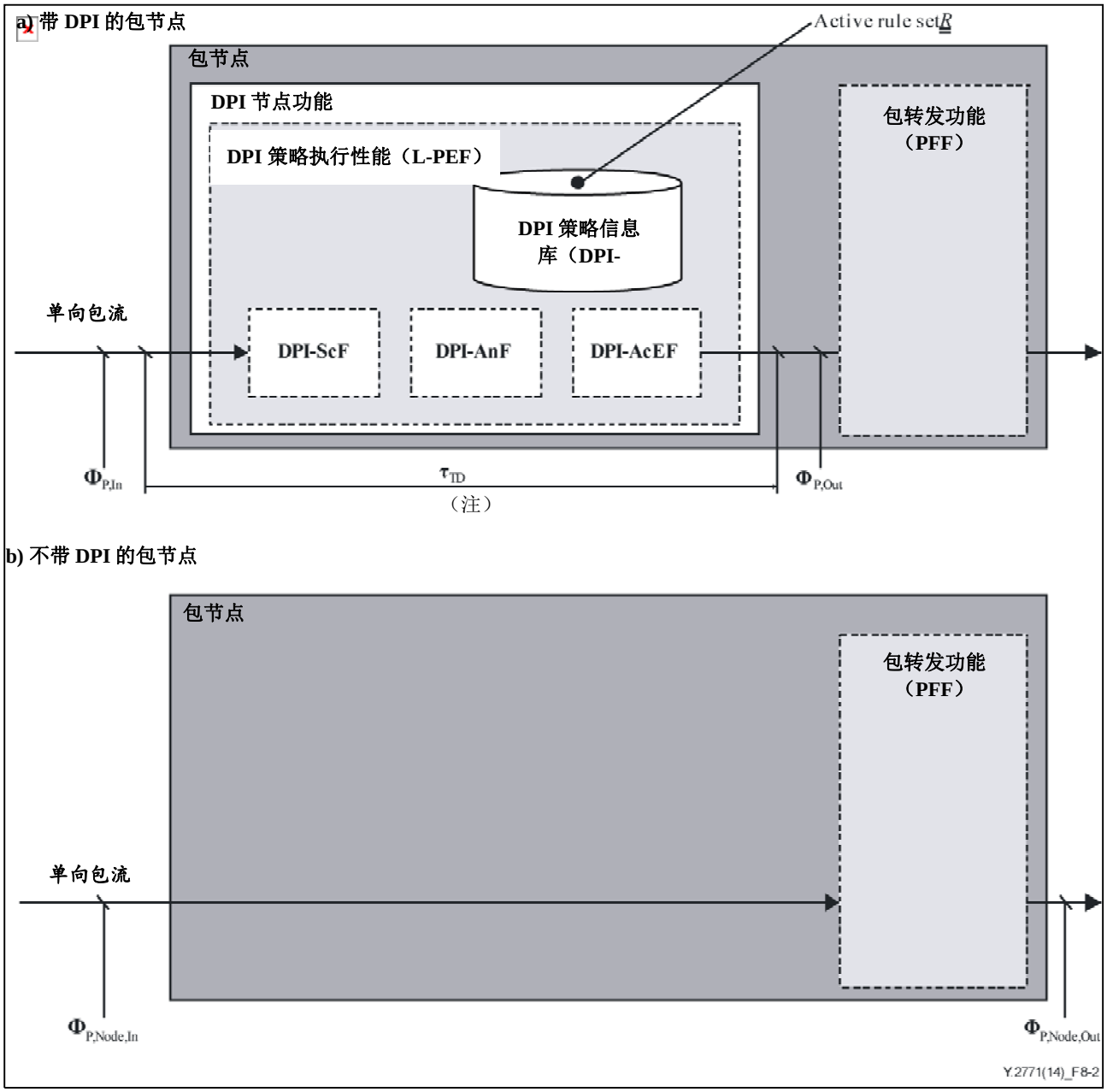
表8-7提供了测量定义。

表8-7 – DPI测量“包成功识别率”

测量名称：	N	包成功识别率
符号：	I	$\phi_{P,\ Identified}$
测量描述：	N	当DPI策略规则条件（来自至少一个DPI策略规则）“匹配”所检测的包时，输入包将被“成功识别”（通过包识别功能）。 对“匹配”类型（如完全匹配、部分匹配、确定匹配、可能匹配...等）不做进一步限定。 “速率”涉及每个时间单位内成功识别的包数量。
度量或计算方法：	N	1．直接测量： 例如：执行一个已知的DPI策略规则以及产生一个具有已知特性的包流（即流量比例应匹配（或不匹配）事先是知道的）。而后，测量值与标称值进行比较。 2．间接测量（计算） $\phi_{P,Identified} = \phi_{P,In} \cdot (1 - \varepsilon_{DPI})$
度量单位：	N	s^{-1}
有潜在度量域的度量点：	N	参见图8-1（流量模型）。
度量时序：	N	从被服务用户实例的角度来看，测量时间间隔依赖于时间尺度。
实施：	I	–
验证：	I	参见上述方法“直接测量”。
使用和应用：	I	“实时DPI”
报告模型：	I	典型地，将作为性能管理的一部分。
类型KПI：是/否？	I	“KPI”
注 – N：规范性描述要素；I：说明性描述要素		

8.3 策略执行点的性能、定性性能行为的估计

本节的目的是为协议层相关策略的执行提供有关定性性能估计的补充信息。图8-2显示了带DPI节点功能的包节点（a）以及没有任何执行之DPI的包节点（b）。此处考虑的关键性能指标是包节点吞吐量$_{P,\ Node,\ Out}$。



注 – 包节点和PFF涉及性能度量指标的明确规范，但这两个实体均超出本建议书的讨论范围。

图8-2 – 策略执行性能 – 包节点吞吐量$\phi_{P, Node, Out}$是每个包执行之策略规则R的一个函数

图8-3描绘了一些主要的吞吐量曲线。具体的策略执行功能（y轴）通过每个包的策略规则数量R以及规则互动方面的因素来表征。执行一个特定的策略规则将消耗一定数量的包路径资源，如处理时间、包存储器、TCAM/CAM存储器、策略数据库等。

经简化的经验法则：“每个包的规则越多，策略执行所需的资源就越多”。

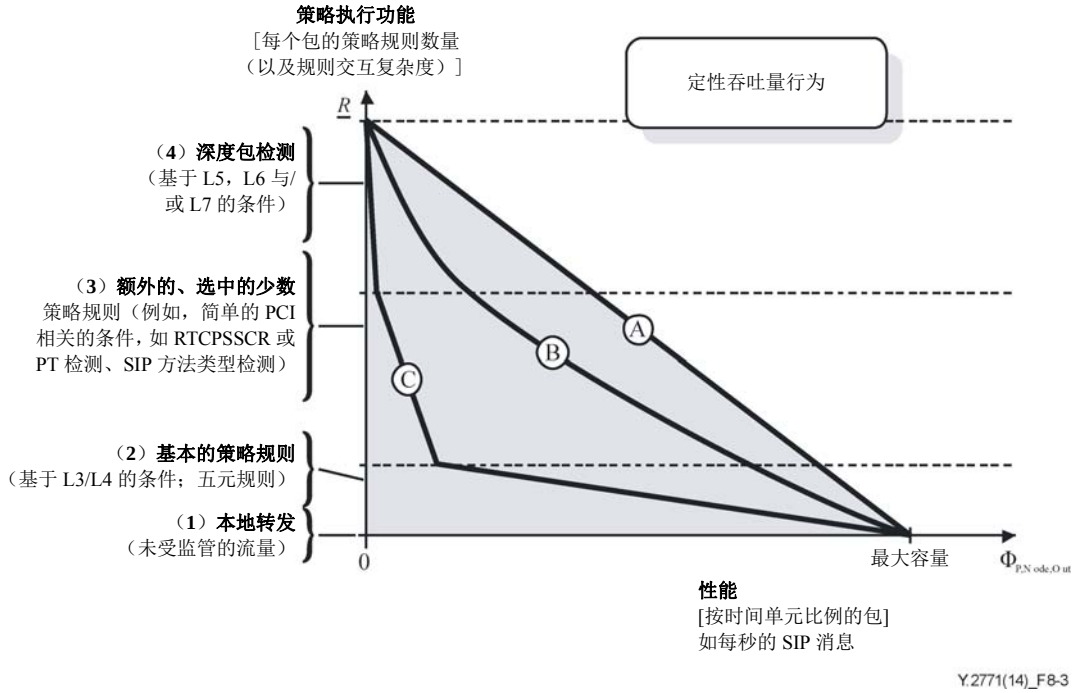


图8-3 – 策略执行性能 – 定性吞吐量行为

一个理想的实施方案可以实现一个像A那样的“线性”行为。一个更现实的和成本效益更高的模型将更倾向于曲线*C*。

行为*C*的技术（和商业）挑战在相当程度上是非线性关系，参见图8-4，这使得设计标称负载点或/与显得非常重要，以达成所需的均衡，限制所执行策略规则集。

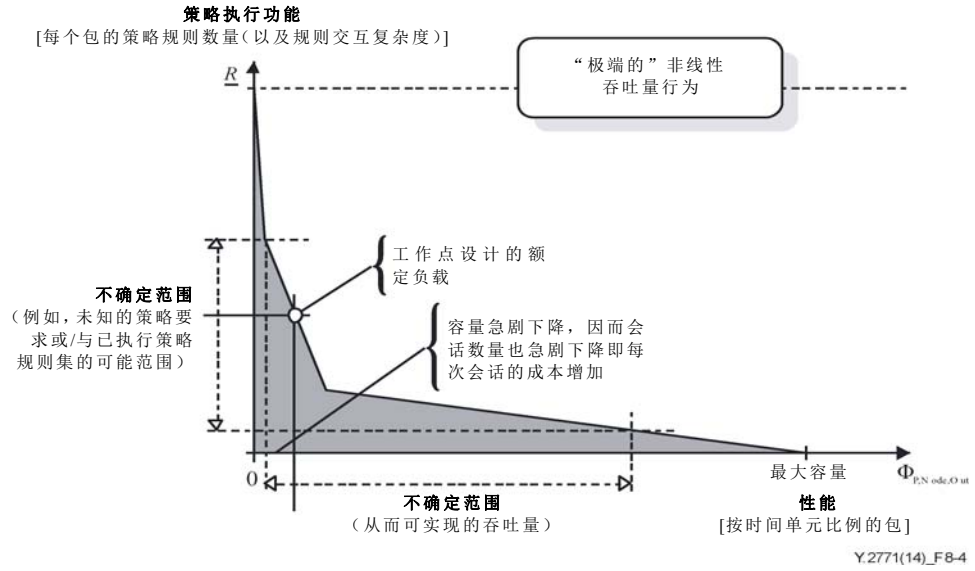


图8-4 – 策略执行性能 – 使用案例C作为最坏案例情形的例子

9 DPI功能实体的分类

根据[ITU-T Y.2770]，一个DPI实体通常不支持DPI要求的全集，而仅仅支持由目标用例给定的子集。因此可能识别不同类型的DPI-FE。

9.1 分类原则

每个可识别的DPI实体能力，基本上都可与DPI要求关联，如[ITU-T Y.2770]规定的那样。在较高层上有：

- 在条件处理方面的能力；
- 在动作处理方面的能力；以及
- 可能的其它能力。

对特定DPI-FE类型的识别，典型的准则是部署方案（DPI用例）、处理逻辑的复杂度、成本因素等。

9.2 依据条件处理的能力

条件处理能力可分为两类：L4 PI（具有L4负载检测能力）和非L4 PI（没有负载检测能力）。

9.3 依据行动处理的能力

参见[ITU-T Y.2770]中有关行动和样例层次的第6.3.3.1节。

9.4 DPI-FE类型

表9-1使用第9.2节和第9.3节中的分类原则，并对三个相关类型做了概述：

表9-1 – DPI-FE类型分类

<table>
<tr><td colspan="3" rowspan="3">DPI-FE类型</td><td colspan="2">依据行动处理的能力</td></tr>
<tr><td colspan="2">支持DPI-AcEF</td></tr>
<tr><td>否</td><td>是</td></tr>
<tr><td rowspan="2">依据条件处理的能力</td><td rowspan="2">支持L4负载检测</td><td>否</td><td colspan="2">类型1</td></tr>
<tr><td>是</td><td>类型2</td><td>类型3</td></tr>
</table>

根据某个DPI-FE的DPI功能能力，可将DPI-FE分类如下（表9-2）：

表9-2 – 三种类型详述

类型	规则处理
1	无L4负载检测能力的FE（$L_4PI = L_{4+}HI \cup L_7PI$）， 即非DPI-FE类型（如SPI-FE）
2	无行动执行能力（DPI-AcFE）的DPI-FE， 但有L4负载检测能力（$L_4PI = L_{4+}HI \cup L_7PI$）。
3	有行动执行能力（DPI-AcFE）以及有L4负载检测能力（$L_4PI = L_{4+}HI \cup L_7PI$） 的DPI-FE。

DPI FE类型可以是以下因素的结果：

1) 可用资源数量：一个特定DPI物理实体（DPI-PE）的能力（如硬件（HW）或软件（SW）部件）或者

2) 为DPI处理而分配/启用的资源数量：通过配置管理（如通过提供一个专用的功能集、通过策略管理实体（参见第7节））。

需要注意的是：一个特定*n*类型的DIP FE可通过其管理实体被配置为一个*m*类型（n>m）的DIP FE。（出于以下事实之故，例如，“类型3的DPI能力集”是关于其它类型的一个超集）。

DPI FE应能向相关的功能实体（如RACF）报告其类型。

根据DPI-FE的DPI功能能力，类型3的DPI-FE可被进一步细分为（表9-3）：

表9-3 – 类型3的子变体

类型	规则处理
3.1	有信息收集和报告能力的DPI-FE
3.2	类型3.1以及有流量控制能力，但无包内容修正能力
3.3	类型3.2以及有包内容修正在能力

10 安全方面的考虑

DPI的监管、隐私和安全应用问题超出了本建议书的范围。在实施本建议书时，要求供货商、运营商和服务提供商考虑到国家监管和政策要求。

依据ITU-T Y.2770建议书，应保护好DPI-FE以及与DPI操作有关的信息，使之免遭威胁。[ITU-T Y.2704]建议书中规定的机制旨在解决[ITU-T Y.2770]建议书中所提的要求。

附录I

基于Bloom过滤程序的、概率DPI的样例功能体系结构

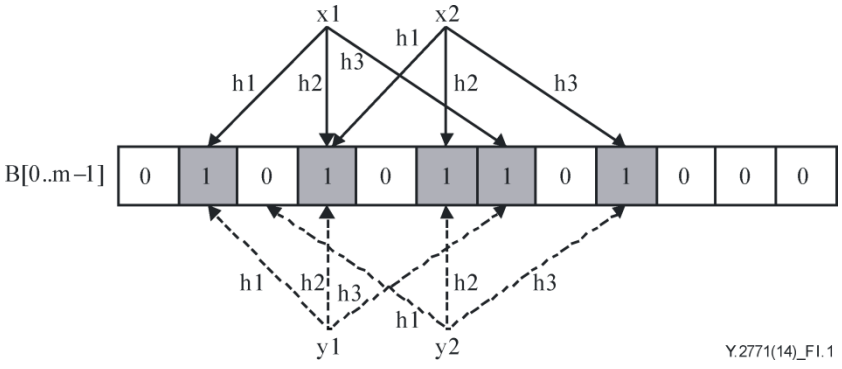
（本附录非本建议书的有机组成部分）

I.1 概述

Bloom过滤程序在[b-Bloomfilter]中阐述：

“Bloom过滤程序使用一种随机技术来测试成员对一个字符串集合的查询情况。给定一个字符串，Bloom过滤程序将计算在其上产生1～m散列值的散列函数（参见图I-1）。而后，对应*k*个散列值，它在各地址上、在一个m位长的向量中设置k比特，其中，*k*不大于m（也可参见方程式[7-1]）。对该集合的所有成员，重复相同的过程。该过程被称为过滤程序的“编程”。查询过程类似于编程，其中一个字符串其成员待验证，将输入到过滤程序中。使用相同的散列函数，Bloom过滤程序产生*k*个散列值，它用之来对过滤程序进行编程。查询对应*k*个散列值的、各位置上m位长向量中的各比特。如果发现这些位中至少有1比特未设置，那么宣布该字符串不是集合的一个成员。如果发现所有的位都设置了，那么认为该字符串在一定概率上属于集合的一个成员。成员的这种不确定性来自这样的事实，即m位长向量中的这些*k*比特可以由任何成员来设置。因此，寻找一个比特设置并不一定意味着它要由被查询的特定字符串来设置。不过，寻找一个未设置的比特一定意味着该字符串不属于该集合，原因是，如果这么做，那么在利用该字符串对Bloom过滤程序进行编程时，所有的*k*比特都将肯定会被设置。这就解释了为什么在该方案中会出现错误地判为对的情况，而不会出现错误地判为错的情况。”

例如，在图I-1中，Bloom过滤程序BF（B[0 .. M-1]）由3个散列函数（即h1、h2、h3）在字符串x1和x2上产生，其中，在基于DPI的Bloom过滤程序中，字符串x1和x2为DPI签名。依据Bloom过滤程序BF（通过位向量B[0 .. M-1]给出），在字符串y1和y2上，通过3个散列函数h1、h2和h3，对字符串y1和y2进行验证，其中，在基于DPI的Bloom过滤程序中，字符串y1和y2表示被检测的数据结构，例如，通过输入包的负载给出。



图I-1 – Bloom过滤程序编程和查询（BF相当于比特向量B[0..m-1]）

错误地判为对的错误率$\varepsilon_{f\text{-}p}$通过方程式（I-1）来表示：

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

其中，*n*是编入Bloom过滤程序中的字符串数量。针对成员集合*n*的给定大小，可以通过选择适当的*m*和*k*值，来降低$\varepsilon_{f\text{-}p}$的值。

I.2 基于Bloom过滤程序的、概率DPI的功能模型

基于概率DPI的Bloom过滤程序的功能模型在图I-2中进行描述。概率DPI的策略规则可以是：

如果包“P”包含来自DPI签名集合“*S*”（作为策略条件）的签名，其中，签名集合由“*S*”={“*S1*”，“*S2*”，...，“*Sm*”}给出，那么丢弃该包（作为政策行动）。

有关签名集合S的Bloom过滤程序BF由一组散列函数H_1, H_2, …, H_k产生，策略规则转换为：

如果H_1(‘P’), H_2(‘P’),…, H_k(‘P’)匹配BF，那么丢弃。

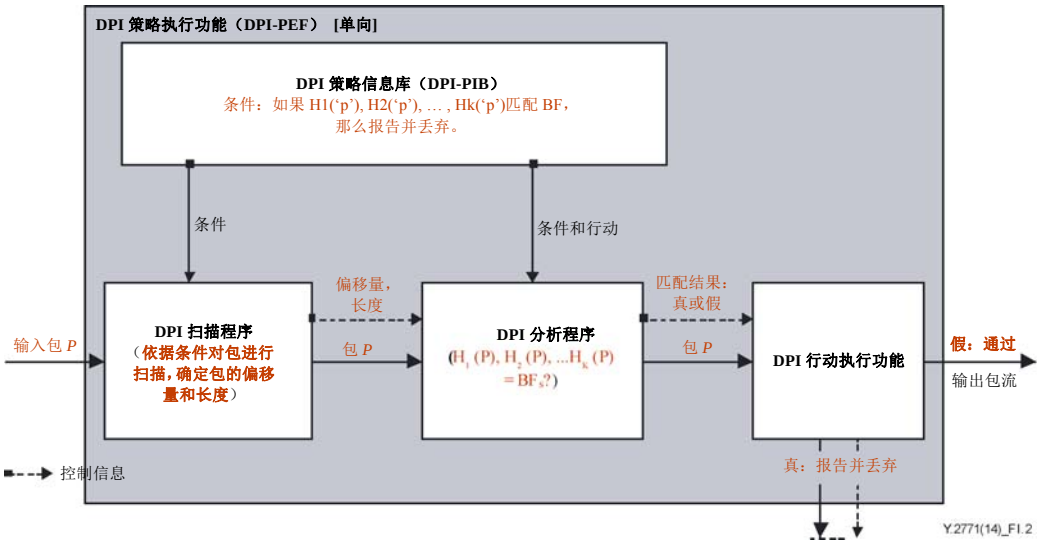
在依据该DPI策略规则条件，对DPI分析程序与到达包进行比较前，DPI扫描程序需要确定到达包中的偏移量和长度，依据DPI策略规则条件，用之来匹配。

有两种基本选择：

1) 在协议栈知道DPI规则条件的情况下，集合“S”中的偏移量和签名长度是已知的，扫描程序直接向DPI分析程序报告偏移量和长度信息。

2) 在协议不知道DPI规则条件的情况下，DPI扫描程序需要进行扫描，并确定偏移量和长度。DPI扫描程序向DPI分析程序报告该信息。

DPI分析程序利用H_1, H_2, …, H_k产生包P的散列结果，利用BF匹配结果，向DPI行动执行功能报告匹配结果。DPI行动执行功能报告匹配结果（“真”或“假”），并在估计匹配结果为“真”时丢弃包，否则将包传给包转发功能。如果生成的匹配结果不匹配BF，那么DPI扫描程序需要从“偏移量+1“字节（偏移量=偏移量+1）开始进行扫描，该过程将一直持续到包的末尾。



图I-2 – 基于概率DPI的Bloom过滤程序功能模型

可以看到，DPI分析程序的匹配结果是布尔类型，即“真”（True）或“假”（False），而非任何概率值，如“*正确匹配概率为**p***（p在0%与100%之间）”。不过，由于内在的、错误地判为对的错误率$\varepsilon_{f\text{-}p}$是DPI策略条件的一部分，因此，如上所述的整个DPI包处理路径阶段将导致概率性的DPI结果。

参考资料

[b-ITU-T H.248.53] Recommendation ITU-T H.248.53 (2009), *Gateway control protocol: Traffic management packages.*

[b-ITU-T I.130] Recommendation ITU-T I.130 (1988), *Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN.*

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

[b-ITU-T X.1036] Recommendation ITU-T X.1036 (2007), *Framework for creation, storage, distribution and enforcement of policies for network security.*

[b-ITU-T Y.1221] Recommendation ITU-T X.1221 (2010), *Traffic control and congestion control in IP based networks.*

[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-T 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. Haberman.*

[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*.

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	**全球信息基础设施、互联网协议问题和下一代网络**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2015年，日内瓦