国 际 电 信 联 盟

ITU-T

Y.2770

(11/2012)

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

下一代网络的移动安全框架

ITU-T Y.2770 建议书

ITU-T

国际电信联盟

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.2770 建议书

下一代网络深度包检测的要求

摘要

本建议书规定了下一代网络（NGN）深度包检测（DPI）的要求。此建议书主要规定NGN、寻址中的深度包检测（DPI）实体的要求，特别是应用识别、流量识别、检测的业务类型、签名管理、向网络管理系统（NMS）报告以及与决策功能实体的互动等。尽管针对NGN，但这些要求也可适用于其他类型的网络。本建议书也在附录中包含了使用案例和其他补充信息。

历史沿革

版本	建议书	批准日期	研究组
1.0	ITU-T Y.2770	2012-11-20	13

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/。

目录

ITU-T Y.2770 建议书

下一代网络深度包检测的要求

1 范围

此建议书主要规定NGN、寻址中的深度包检测（DPI）实体的要求，特别是应用识别、流量识别、检测的业务类型、签名管理、向网络管理系统（NMS）报告以及与决策功能实体的互动等。

此建议书也确定了非原生编码格式业务（如加密业务、压缩数据和转码信息）DPI的要求。

任何DPI功能可通过政策规则（见第1.2节）给予一般性描述。附录中给出了DPI应用情景和补充信息，如包识别的政策规则、政策执行过程、政策规定语言、分层协议架构中的DPI以及术语定义。

所述方法的执行者和使用者须遵守所有可适用的国内和区域性法律、法规和政策。

该建议书并未涉及落实分布式DPI功能的具体影响。要求主要涉及DPI的功能方面，但也涵盖了物理方面。在功能至物理映射情形下，只有DPI-FE和DPI-PE之间的1对1映射和N对1映射属于本建议书的范围。也就是说，没有要求涵盖分布式DPI-PE。

1.1 适用性

此建议书适用于图1-1所确定的情形：

		分组网络类型	
		NGN	非NGN
包载体技术	IP	适用	可适用
	非IP	可适用	可适用

Y.2770(12)_F1-1

图1-1 – 本建议书的适用性

“非IP”的提法指没有IP协议层的包载体的包协议堆栈（[IETF RFC 791]和[IETF RFC 2460]）。

尽管本建议书主要涉及NGN的DPI要求，这些要求可适用于其他类型的网络。这种进一步的适用性需进一步研究。

1.2 政策规则

本建议书假定政策规则采用一般高级格式。如图1-2所示，这种高级格式适用于DPI规则。格式区分三种基本块：

i) 规则标识符/名称（附有因可能存在多个规则而产生的等级/顺序）；

ii) DPI签名/条件；

iii) 行动。

行动和条件之间存在逻辑绑定关系，见第3.1.2节。

图 1-2 – DPI政策规则的一般格式

应注意到，以下问题属于范围之内：

- 与DPI签名有关的要求规范（即用于应用识别和流量识别的DPI签名）；
- 与DPI政策规则识别和命名有关的要求规范；以及
- 涉及政策行动，作为评估DPI签名之后潜在后续行动的可能情形的识别。

与此相反，以下问题不属于范围之内：

- 与涉及修改已检测包行动有关的要求规范；
- 行动和条件之间明确绑定关系的规范（注）；
- DIP完整政策规则的规范；
- DPI签名语言的规范；以及
- 明确的DPI政策条件的规范（例如行为或统计功能）。

注 – 例如，可能存在丢弃包行为的规范以及搜索包签名的条件，但不存在与将单个行动关联到实际条件的规范。

2 参考文献

下列ITU-T建议书和其它参考文献的条款，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。所有建议书和其它参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T E.107] ITU-T E.107建议书（2007年），应急电信服务（ETS）和ETS国家级实施方案（ENI）的互连框架。

[ITU-T X.200] ITU-T X.200建议书（1994年）|ISO/IEC 7498-1:1994，信息技术。开放系统互联。基本参考模型：基本模型。

[ITU-T X.731] ITU-T X.731建议书（1992年）|ISO/IEC 10164-2:1993，信息技术—开放系统互联—系统管理：状态管理功能。

[ITU-T Y.1221] ITU-T X.1221建议书（2010年），IP网络中的业务控制和拥塞控制。

[ITU-T Y.2111] ITU-T Y.2111建议书（2008年），下一代网络的资源和接纳控制功能。

[ITU-T Y.2205] ITU-T Y.2205建议书（2011年），下一代网络—应急通信—技术考虑。

[ITU-T Y.2701] ITU-T Y.2701建议书（2007年），NGN发布1的安全要求。

[ITU-T Y.2704] ITU-T Y.2704建议书（2010年），NGN的安全机制和程序。

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.

[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 其他文件定义的术语

本建议书采用了以下其他文件定义的术语：

3.1.1 filter 过滤 [b-IETF RFC 3198]：一系列用于分离和分类的术语和/或标准。通过业务字头和/或载荷数据的单或多字段匹配实现。“过滤”常在网络运营和政策中使用。例如，包过滤规定匹配某个模式的标准（如IP或802标准），以区分可分离的业务类别。

注 – 本建议书中，“业务字头”一词相当于“包字头”。

3.1.2 filter/policy rule 过滤/政策规则 [b-IETF RFC 3198]：基于政策系统的基本构成块。它是一系列行动和条件的绑定，其中对条件进行评估，以判定是否采取了行动。

注 – 本建议书中，过滤政策是一项带有分离业务的具体政策，如主类别中的“接受”和“不接受”。

3.1.3 flow 流量 [IETF RFC 5101]：网络中在某一时间间隔通过观测点的一系列 IP 包。属于某个特定流量的所有包具有一系列相同的属性。每种属性定义为将函数应用于以下数值后获得的结果：

1) 一个或多个包字头字段（如目的地IP地址）、传输字头字段（如目的地端口号）或应用字头字段（如RTP字头字段[b-IETF RFC 3550]）。

2) 一个或多个包自身的特性（如MPLS 标签的号码等）。

3) 一个或多个从包处理中获得的字段（如下一跳IP地址、输出接口）。

如果包完全满足流量的所有定义特性，则包定义为属于此流量。

此定义涵盖在从某个网络接口观测到的、包含所有包的流量到两个应用之间仅包含一个单一包的流量的范围。它包括取样机制选择的包。

注 – 上述编号列出的项目显示了(1)包“协议控制信息（PCI）”，(2)“包协议数据单元（PDU）属性”以及(3)“本地包前向信息”类别的流量属性。

3.1.4 policy 政策 [b-IETF RFC 3198]：一系列管理和控制网络资源获取的规则。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 application 应用：以下情形之一的名称

- 应用协议类型（如IP应用协议H.264（视频）或SIP）；
- 应用的服务用户实例（如VoIP、VoLTE、VoIMS、VoNGN和 VoP2P），如“分组话音应用”；
- 分组话音的“与提供商相关的应用”（如3GPP 提供商VoIP、Skype VoIP）；以及
- 嵌入另一个应用的应用（如SIP或HTTP信息正文中的应用内容）。

可用特定的标识符（如通过位字段、模式、签名或“应用等级条件”等常规表达式，亦参见第3.2.2节）。

3.2.2 application-descriptor (also known as application-level conditions) 应用 – 描述符（也称为应用 – 等级条件）：（根据第3.2.1节）识别应用的一系列规则条件。

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

3.2.3 application tag 应用标签：用来表示应用语义唯一名称，通常用于报告情形。

图3-1简要描述了应用标签和应用描述符之间的关系。

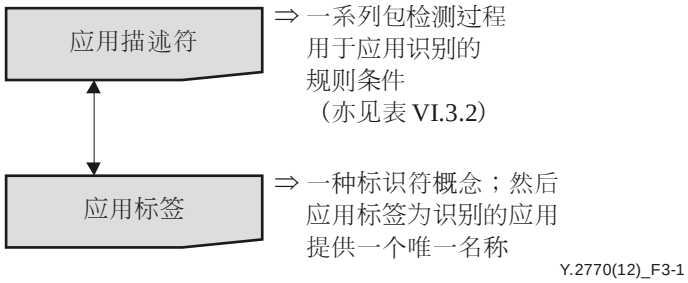


图3-1 – 应用标签和应用描述符之间的关系

3.2.4 bidirectional DPI 双向DPI：涉及业务双方向政策条件的DPI。

注 – 也参见VI.3.2节中应用描述符的正式定义：政策条件与简单条件有关。对于双向DPI的情况，每个业务方向至少有一个简单条件。

3.2.5 deep packet inspection 深度包检测：根据分层协议架构OSI-BRM [ITU-T X.200]来分析：

- 载荷和/或包属性（深于协议层2、3、4（（L2/L3/L4）字头信息的潜在属性的清单，见第3.2.11节），以及
- 其他包属性

以便明确地识别应用。

注 – DPI功能的输出以及流量信息等一些额外信息通常用于报告或对包采取行动等后续功能中。

3.2.6 DPI engine DPI引擎：DPI功能实体的一个子部分和中心部分，该部分执行所有的包路径处理功能（如包识别及图6-1中的其他包处理功能）。

3.2.7 DPI entity DPI实体：DPI实体或者是DPI功能实体，或者是DPI物理实体。

3.2.8 DPI functional entity (DPI-FE) DPI功能实体：执行深度包检测的功能实体。

3.2.9 DPI physical entity (DPI-PE) DPI物理实体：DPI功能实体的实施示例。

3.2.10 DPI policy DPI政策：如在[b-IETF RFC 3198] 中定义（见3.1.4节）并在DPI实体中执行的政策。

3.2.11 DPI policy condition DPI政策条件（也称为DPI签名）：识别应用并定义政策规则的行动是否应执行的必要状态和/或前提条件的表示。与政策规则有关的一系列DPI政策条件规定何时政策规则应适用（亦参见[b-IETF RFC 3198]）。

DPI政策条件必须包含应用等级条件并可能包含状态条件和/或流量等级条件等其他选项：

1 状态条件（可选）：

a) 网络服务等级条件（如包路径中遇到的拥塞）或

b) 网络元素状态（如DPI-FE局部过载条件）。

2 流量描述符/流量等级条件（可选）：

a) 包内容（字头字段）；

b) 包的特性（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/应用等级条件：

a) 包内容（应用字头字段和应用载荷）。

注 – 条件涉及流量等级条件和应用等级条件的正式描述中的“简单条件”（亦参见表VI.3.1和VI.3.2）。

3.2.12 DPI policy decision functional entity (DPI-PDFE) DPI政策决定功能实体：远离DPI-FE、决定DPI-FE中应执行的签名规则的功能。一些控制和/或管理功能不一定远离DPI-FE。

3.2.13 DPI policy rule DPI政策规则：与DPI有关的政策规则（亦参见3.1.2节）。本建议书中，DPI政策规则仅指规则。

3.2.14 DPI signature DPI签名：DPI政策条件的同义词（参见节3.2.11）。

3.2.15 DPI signature library DPI签名库：包哈一系列DPI签名的数据库。也称为DPI协议库，因为签名通常用于协议识别。

3.2.16 flow descriptor 流量描述符（也称为流量等级条件）：用来在检测流量中（根据3.1.3节）识别特定类型流量的一系列规则条件。

注1 – 流量描述符的该定义比[b-ITU-T Y.2121]的定义增加了第3节所述的内容。

注2 – 有关本建议书中流量描述符的进一步规范讨论，见附件A。

3.2.17 IPFIX flow ID IPFIX流量标识符：与流量描述符共同使用，用于识别特定流量的一系列IPFIX流量键值。

3.2.18 IPFIX flow key IPFIX流量键：在IPFIX流量识别过程中（根据[IETF RFC 5101]）采用的流量描述符的每个信息元素。

注 – IPFIX流量键定义在语义上符合IPFIX [IETF RFC5101]规定的流量键定义。两个术语唯一的区别是本文件中的定义限于流量描述符的范围。

3.2.19 L3,4 header inspection L3,4字头检测（$L_{3,4}$HI）：根据只涉及网络层和/或传输层协议控制信息（PCI）要素的政策条件处理政策规则。

3.2.20 L4+ header inspection L4+字头检测（L_{4+}HI）：根据只涉及传输层以上协议控制信息（PCI）要素处理政策规则。

3.2.21 L4 payload inspection L4 载荷检测（L_4PI）：根据只涉及传输载荷（可能是用于某种应用协议（如SIP）的“应用数据”）处理政策规则。

注 – L_4PI与L_{4+}HI和L_7PI政策条件的合并有关。

3.2.22 L7 payload inspection L7载荷检测（L_7PI）：根据基于应用数据的政策条件处理政策规则。

3.2.23 payload 载荷：包中位于字头元素之后的数据单位，不包括包末尾的可选项（如补白、报尾、校验和元素等）。

注1 – 因此，载荷的提法与OSI-BRM [ITU-T X.200]中的业务数据单元（SDU）是同义词，包是协议数据单元（PDU）的同义词，且协议控制信息（PCI）涵盖所有的字头和报尾元素。归纳起来，“PDU = PCI + SDU”。

注2 – 载荷的提法只与特定协议层有关（即Lx-Payload指协议层x的载荷）。Lx-SDU、Lx-PDU和Lx-PCI同上。

4 缩写和首字母缩略语

本建议书采用下列缩写和首字母缩略语：

AH	认证头
BRM	基本参考模型
DCCP	数据报拥塞控制协议
DPI	深度包检测
DPI-FE	DPI功能实体
DPI-PDFE	DPI政策决定功能实体
DPI-PE	DPI物理实体
DPI-PIB	DPI政策信息库
ESP	封装安全载荷
ET	应急电信
FPA	全载荷区域分析
FSL	过滤规范语言
HTTP	超文本传输协议
IANA	互联网号码分配机构
IE	信息元素
IP	互联网协议
IPFIX	IP流量信息输出
IS	服务状态
L-PDF	本地PDF
MPLS	多协议标签交换
NGN	下一代网络
NMS	网络管理系统
OGP	开放游戏协议
OoS	非服务状态
OSI-BRM	开放系统互连 — 基本参考模型
P2P	端到端
PCC	政策和计费控制
PCI	协议控制信息
PDF	政策决定功能
PDU	协议数据单元
PEL	政策表述语言
PFF	包转发功能
PIB	政策信息库
PPA	载荷区域分析
PSAMP	包取样

PSL 政策规范语言
RACF 资源和接纳控制功能
RACS 资源和接纳控制子系统
R-PDF 远程PDF（即从DPI节点来看，PDF距离较远）
RTP 实时传输协议
SA 安全协会（IPsec）
SCTP 流控制传输协议
SDU 业务数据单元
SigComp 信令压缩
SIP 会话启动协议
SPI 安全参数索引（IPsec）
TCP 传输控制协议
TISPAN 电信和互联网融合业务及高级网络协议
UDP 用户数据报协议

5 惯例

本文将提供了一系列标示为*R-x/y*的名目，其中x指章节号，而y指该节内的一个号码。此类名目采用下列关键词，其含义如下：

关键词“须”指必须严格遵守的要求，如果要宣称符合本文件，就不得违反。

关键词“禁止”指必须严格遵守的要求，如果要宣称符合本文件，就不得违反。

关键词“建议”指建议但并非需要绝对遵守的要求。因此宣称符合本文件不需要说明已满足此要求。

关键词“可作为选项”指允许可选的、但并非建议遵守的要求。该术语并非旨在暗示销售商的实施必须提供该选项且该功能部件可作为选项由网络运营商/业务提供商激活，而是指销售商可作为选项提供该功能部件并仍根据规范宣称符合本文件。

在本文件正文及其附件中，有时会出现“须”、“不得”、“应”、“可”等词语。在这些情况下，这些词语应分别理解为“需”、“禁止”、“建议”和“可作为选项”。在附录或明确标为信息参考的资料中出现这些短语和关键词应理解为并非出于规范性的意向。

6 DPI功能实体要求

6.1 流量和应用识别

R-6.1/1：需要DPI功能实体执行应用识别。

R-6.1/2：需要DPI功能实体支持各种DPI政策规则。

R-6.1/3：需要DPI-FE，通过检测应用载荷来识别一个应用。

R-6.1/4：对于所有单向应用，在单向业务（单向DPI）基础上以及对于双向应用，在一种业务方向可进行明确识别的条件下，需要DPI应用等级条件（以及可选的流量等级条件）进行应用识别。

R-6.1/5：DPI应用等级条件以及（可选的流量等级条件）可作为可选项，允许在双向业务（双向DPI）的基础上进行识别。

R-6.1/6：建议在流量等级条件中的信息元素符合[b-IETF RFC 5102]，按照IANA [b-IETF IANA IPFIX]进行注册。在这种情况下，建议信息元素根据IETF基本分层协议架构，包括与连接（L2）、网络（L3）和传输（L4）协议层有关的IPFIX信息元素。

注 – IANA的IPFIX信息元素注册可予以增强，包括额外的（IETF）要素。当前的IANA注册（截至2011年底）除了UDP和TCP以外，还缺少L4协议的信息元素（如对于SCTP和DCCP）。

R-6.1/7：信息元素可以是IPFIX注册以外的其他L2、L3或L4相关信息元素（称为IPFIX协议[IETF RFC5101]中的企业特定信息元素。

6.2 DPI签名管理

本节定义了与DPI签名库的运作有关的要求。此类运作可在本地由DPI-FE启动，或由远程网络实体启动（见图6-1）。所有类型的远程网络实体可抽象地归纳为决定DPI-FE将要执行的签名规则的DPI政策决定功能实体。

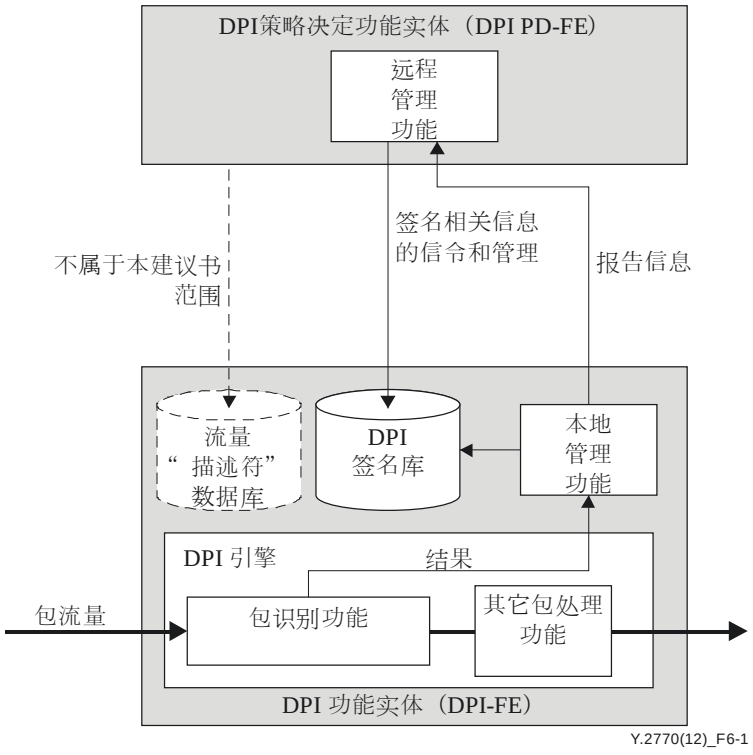


图6-1 – 示例性DPI功能实体架构范围内的DPI签名管理
（亦见与内部接口有关的图8-2）

DPI政策决定功能实体将与RACF（对于NGN的情况，则与RACF）有关，但其指标不属于本建议书的范围。将其包括在图6.1中是因为它包含了DPI-FE 的远程管理功能。

6.2.1 一般签名要求

R-6.2.1/1：须在DPI签名库中存储DPI签名，DPI签名库是DPI-FE的一个子实体。

注 – DPI签名库的逻辑依据是包识别功能要求立即访问数据库内容。

DPI签名可用于

- 近似识别（如行为、探索法识别等）及
- 精确识别（如精确匹配规则）。

用于规定本库中DPI政策规则的语言（正式或行为的）以及匹配规则自身不属于本建议书的范围。本建议书仅规定DPI签名库存在，什么是DPI签名以及库的管理功能。

R-6.2.1/2：DPI签名库须安全地予以维护并不得向非授权用户开放。

6.2.2 管理DPI签名库

本节定义DPI签名库的管理要求。

6.2.2.1 增加新签名

R-6.2.2.1/1：须可以向DPI签名库中增加新DPI签名。

6.2.2.2 操作现有的签名

R-6.2.2.2/1：须可以修改（更新）DPI签名库中的现有签名。

R-6.2.2.2/2：须可以激活或禁止DPI签名库中的特定DPI签名。

R-6.2.2.2/3：须可以删除（移除）DPI签名库中的特定DPI签名。

6.2.2.3 经由外部接口的规则格式交换

R-6.2.2.3/1：用于应用识别的、通过外部接口（如图8-1中的e1和e2）交换的DPI签名，可任意地采用规则格式（亦参见1.2节）。

6.2.3 位置管理功能

R-6.2.3/1：须本地从DPI功能实体或远程，或同时以两种方式进行6.2.2节规定的DPI签名管理行动（见图6-1）。

6.2.4 管理行动的开始

R-6.2.4/1：当（如由图6-1中的DPI-PDFE）开始远程操作时，须支持与DPI签名操作有关的推送模式。

R-6.2.4/2：当（如由图6-1中的DPI-FE）开始远程操作时，须支持与DPI签名操作有关的“提拉”（pull）模式。“提拉”的提法指DPI-FE本地管理功能要求DPI-PDFE在一个新的或现有的签名上执行一个管理行动。

DPI-FE如何启动要求不属于本建议书的范围。

6.3 业务检查方面

本节涉及DPI的业务类型问题。

6.3.1 流量识别方面

R-6.3.1/1：建议DPI功能实体支持识别应用，没有流量等级检查（亦参见图VII-7）。

R-6.3.1/2：任何DPI情形均可在开始时独立于流量，即向DPI-FE提供的DPI政策规则不会包含流量描述符。但是，规则可要求收集感兴趣的流量信息。

R-6.3.1/3：须请求提供IPFIX流量键并可完成缺少的流量信息。

R-6.3.1/4：DPI功能实体可要求在给定的IPFIX流量键基础上完成IPFIX流量标识符的识别以及多个后续包的检查。

R-6.3.1/5：DPI-FE向远程网络实体的完整或不完整IPFIX流量标识符的报告行动可以是受制约的（如事件驱动、定时器控制等）。

6.3.2 协议-堆栈已知和协议-堆栈未知的DPI问题

DPI识别功能（DPI-FE内）负责应用识别并涉及到在DPI签名基础上，根据新包（PDU）进行比较和搜索操作。有两种选项：DPI-FE或者知道内部PDU结构（如“协议-堆栈已知的DPI-FE”）或不知道结构（“协议-堆栈未知的DPI-FE”）。

两种选项均可提供相同的识别结果且在功能上是等效的。主要的区别是协议-堆栈已知识别逻辑可能更加有效。

区分以下两种与操作效率有关的分析类型（即应用识别和可选的流量识别）是有益的：

a) 预订载荷区域分析（PPA）：当包（流量）根据一个明确定义的载荷结构对应于一个已知的应用时，DPI-FE可检查载荷的固定预定位置（即协议-堆栈已知包检查模式）。

b) 全载荷区域分析（FPA）：当包（流量）不对应于一个已知的应用或应用载荷的结构未明确定义或已知时，DPI-FE可检查“载荷的整个区域”（即协议-堆栈未知包检查模式）。

PPA和FPA均可应用于相同的业务流量。

R-6.3.2/1：建议DPI-FE支持协议-堆栈已知的应用识别。

R-6.3.2/2：建议DPI-FE支持协议-堆栈未知的应用识别。

R-6.3.2/3：DPI-FE须识别IPv4和IPv6协议堆栈上的应用并作为选项可识别其他基础协议堆栈上的应用。

R-6.3.2/4：建议识别嵌套业务中的应用（如封装或埋入式业务）。

6.3.3 DPI政策规则行动方面

6.3.3.1 背景情况

DPI政策行动可在不同等级上（如DPI-FE、本地和远程PDF）进行，并可包括以下内容：

1) 包路径等级行动（由DPI-FE实施）：
   a) 接受包并将其转给包转发功能（PFF）（对于仅In-Path DPI模式，为受制约行动）；
   b) 丢弃包（静默地或其他方式）；
   c) 将包改发给其他输出接口；
   d) 复制/镜像包至其他输出接口；
   e) 衡量数据的业务分类、位置测量和报告；
   f) 单个包的确定优先次序、修整和进度安排法。
2) 节点等级行动（通过（L-PDF）本地政策决定功能的参与）；
   a) 新DPI政策规则的动态构建和/或（存储在DPI政策信息库（DPI-PIB）中的）现有规则的修订；
   b) 生成日志/跟踪数据并向政策管理报告（见[b-IETF RFC 3871]的第2.11.2节）；
   c) 发现并报告不可识别的应用；
   d) 入侵探测系统的通知（如通过报告业务样本、可疑包等）；
3) 网络等级行动（通过远程政策决定功能（R-PDF））：
   a) 资源管理、接纳控制和高级过滤（在网络分系统层面（如ITU-T RACF [ITU-T Y.2111]、ETSI TISPAN RACS [b-ETSI ES 282 003]和3GPP PCC [b-ETSI TS 123 203]等建议书所述））；
   b) 根据用户应用类型的内容收费（如IETF RADIUS或Diameter）。

图6-2通过详细的一般性政策规则格式（相对于第1.2节所介绍的格式）进一步解释了上述结构原则：

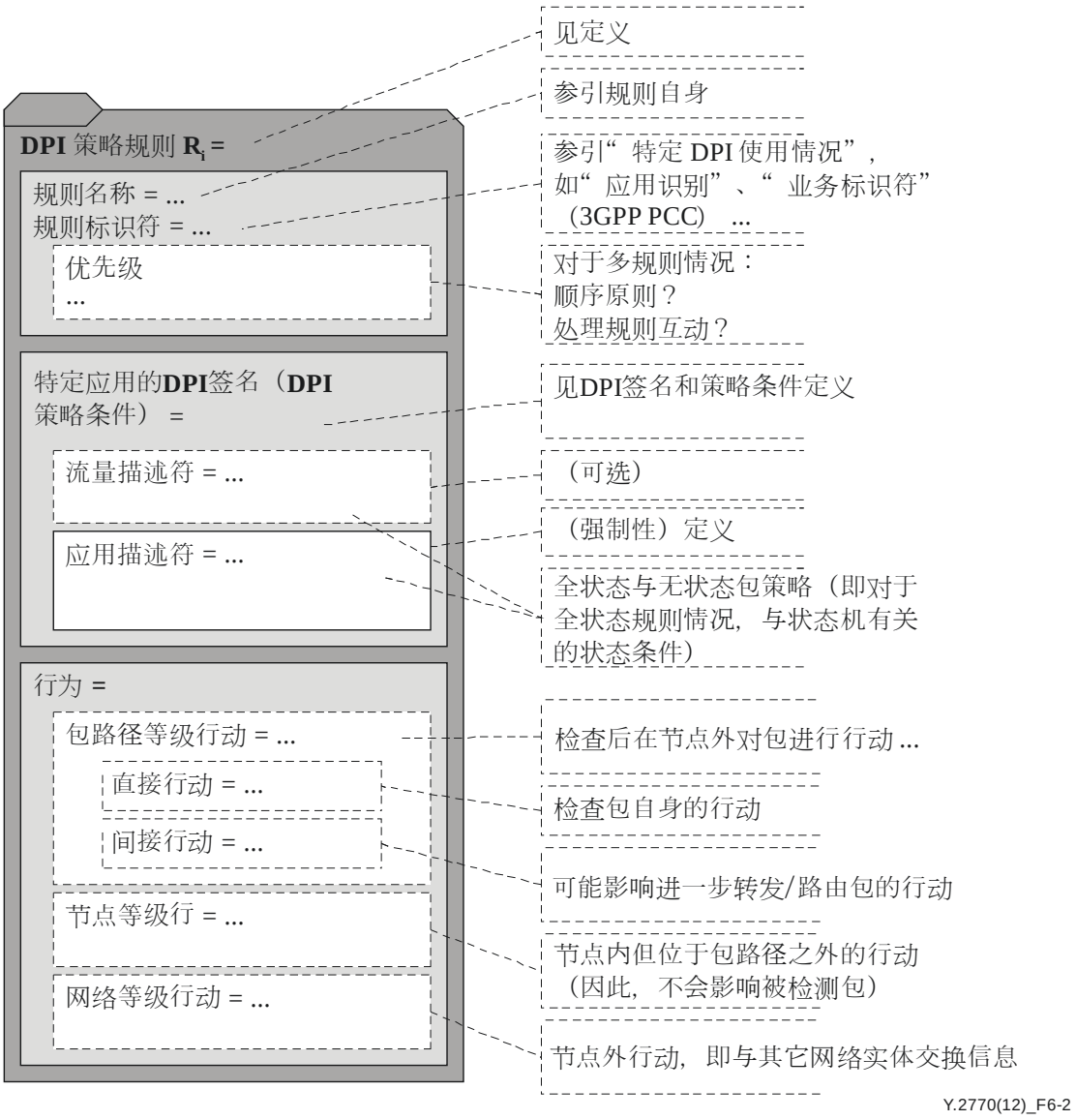


图6-2 – 详细政策规则格式的示例
（与图1-2相比）

特定行动与条件的映射关系不属于本建议书范围。

6.3.3.2 要求

R-6.3.3.2/1：一旦DPI-FE识别了某种应用，可随意提取应用的具体信息。

例如，HTTP 中的URL、实时传输协议（RTP）中的媒体格式（编解码器类型）或RTP会话标识符（如RTP源端点的SSRC）。

R-6.3.3.2/2：DPI-FE可与流量计功能（如IPFIX计量过程[IETF RFC 5101]）和一些过滤功能（如[b-IETF RFC 5476]）一同工作。

注 – 此计量过程通常位于以下IPFIX信息元素（作为流量键）：sourceIPv6Address和destinationIPv6Address、sourceIPv4Address和destinationIPv4Address、protocolIdentifier、sourceTransportPort、destinationTransportPort等。但是，由DPI-FE负责输入应用标签和完成IPFIX流量标识符（根据给定的IPFIX流量键，亦参见图A.1）。

6.4 报告能力

报告涉及到通知（如由于DPI-FE探测到某个特定的事件）另一个功能实体，此功能实体通常位于某个远程网络要素（位于用户、控制或管理平面）中。DPI-FE可提供多个支持“不同事件类型”的报告接口。

6.4.1 向网络管理系统（NMS）报告

6.4.1.1 报告的接口和协议

R-6.4.1.1/1：建议输出协议遵循IPFIX规范[IETF RFC 5101]并可遵循IPFIX的扩展。

R-6.4.1.1/2：对于双方向流量，输出协议可遵循IPFIX规范[b-IETF RFC 5103]。

R-6.4.1.1/3：建议IPFIX输出协议采用外部接口e2（见图8.1）。

6.4.1.2 报告的信息

R-6.4.1.2/1：DPI-FE须向DPI管理平面报告检查结果（如应用标签和可能与应用有关的具体信息元素）以及与流量有关的具体信息。本地更新的流量键值（包括流量计量功能的典型字段）可输出到政策决定功能（如[ITU-T Y.2111]中定义的PD-FE）。

R-6.4.1.2/2：建议所报告的信息重复使用IPFIX信息元素（[b-IETF IANA IPFIX]），这些元素起初规定在IPFIX信息模型[b-IETF RFC 5102]中。

与流量有关的具体信息规定在IPFIX信息模型[b-IETF RFC 5102]中，例如：

1) 与应用有关的信息：
   - 应用标签；以及
   - RTP媒体格式和RTP SSRC等提取的字段。
2) 对应着IP地址、L4端口（如TCP或UDP，注1）以及协议类型的L3/L4字头字段；
3) 性能信息（如规格、统计数字）字节计数、包计数、最大包长度（注2）；
4) 时间信息：流量开始时间、流量结束时间；
5) 包相关信息：下一跳和包长度（注3）；

注1 – 一些列出的信息元素不是互联网号码分配机构（IANA）IPFIX注册的一部分，但在本建议书中是有效的。

注2 – 与流量有关的特定信息可由包采样（PSAMP）机制生成，但当向NMS输出这些结果时，建议增加与应用有关的信息。

注3 – 新信息元素可能应根据[b-IETF RFC 5102]第7节“IANA的考虑”在IPFIX IANA注册。

6.4.2 报告新应用、未知应用或错误应用

6.4.2.1 此类业务的特性

这些业务类型略有差别。其特点在于其探测所获得不同应用等级条件结果的以下特定属性：

– 新应用：如应用的新版本、一个与应用有关的特定信息元素的新版本（如OGP内的新游戏版本）或一个新的协议版本；可注意到，“新”的提法基于DPI业务的角度（可能基于以往DPI业务的历史）；

– 未知的应用：如未知包类型、未知协议、未知“应用”；

– 错误应用：如携带错误协议语法的包（注）等。

注 – 错误的协议句法可被用于安全攻击。受影响的协议通常为在用户设备（如信令协议）中终接的那些协议。

6.4.2.2 报告要求

R-6.4.2.2/1：DPI-FE可支持在检查业务时报告新应用、未知应用或错误应用。

6.4.3 报告异常业务

R-6.4.3/1：DPI-FE可提供与在检查此类业务时与发现异常业务有关的报告能力。

异常业务定义为与正常业务类别（见第1.6节）无关的业务。正常业务类别为与明确定义应用的现有统计属性（如包到达间隔时间、到达顺序、特定协议层PDU的大小、载荷的大小或（在某个协议层的）业务量）相对应的一系列业务。

6.4.4 向DPI-PE报告相关事件

本节描述了涉及DPI实体操作状态的事件及相关报告要求。

6.4.4.1 与DPI-PE不正确行为有关的失败事件

描述DPI-PE管理状态的最简单方法是从两种状态：“正常运转”（IS）和“服务中止”（OoS）。

R-6.4.4.1/1：建议DPI管理基于现有技术水平（如[ITU-T X.731]和[b-IETF RFC 4268]）并建议至少支持IS和OoS的管理状态。

R-6.4.4.1/2：DPI-PE的任何故障，如果未按照冗余方式设计，可引起“IS至OoS”状态转换。建议报告此类事件。

6.4.4.2 与DPI-PE错误管理有关的事件

DPI-PE提供进出业务的网络接口。错误可能会在这些接口出现。

R-6.4.4.2/1：建议DPI-PE支持如[b-ITU-T X.734]中定义的告警报告功能。

6.4.4.3 与DPI功能实体日志有关的事件

R-6.4.4.3/1：DPI功能实体可根据Syslog [b-IETF RFC 5424]等支持系统日志能力。在这种情况下，DPI功能实体为*系统日志信息*（Syslog message）的始发点。

应注意到，当被检查包流量携载日志业务时，DPI功能实体既不是一个日志信息的始发点，也不是终点。也就是说，此类包流量的查阅键可能基于*应用描述符*（与*系统日志应用层*有关）和IPFIX*流量描述符*（与选定的*系统日志传输*模式有关）。进一步信息可查阅[b-IETF RFC 5424]和[b-IETF RFC 5426]。

6.4.4.4 与DPI物理实体的载入状态和资源消耗有关的事件

DPI-PE用于DPI处理的资源有限。资源详情取决于落实且不属于本建议书范围。

R-6.4.4.4/1：建议DPI物理实体支持向管理平面报告DPI资源组成部分的负载水平。

例如，在应急通信业务的网络中（见第7.1.1节），DPI过程必须可通过拥塞的网络节点转发应急通信业务；因此，网络管理系统需要了解负载水平。

6.5 与政策决定功能的互动

R-6.5/1：根据[ITU-T Y.2111]的规定，DPI-FE可作为政策执行功能实体的一部分，提供相关传输功能。

R-6.5/2：根据[ITU-T Y.2111]的规定，DPI-FE和RACF之间的接口可为Rw。

R-6.5/3：根据具体DPI使用情况的不同，DPI-FE和RACF PD-FE之间的信息可通过*现有*（如Rw接口）或*新的*RACF接口交换。

注 – 在这种情况下，需增强RACF，以涵盖DPI信息（如DPI政策规则内的协议签名）；[ITU-T Y.2111]中定义的RACF主要支持基于流量识别的政策规则。具体的RACF参考点将取决于具体的DPI使用情况。

6.6 业务控制

I.5节提供了与业务控制情形下涉及DPI功能的一些高端使用情况。可得出以下高级要求：

R-6.6/1：DPI功能实体可涉及网络情形中，其宗旨是业务控制（如[ITU-T Y.1221]定义的业务控制功能）或附录I中所述的“带宽优化”，或业务重路由）。建议DPI-FE支持相应的业务控制能力。

R-6.6/2：DPI-FE可支持原生的业务控制。尽管如此，业务控制的详细功能要求不属于本建议书范围。

R-6.6/3：DPI-FE可支持与外部业务控制功能的互动。相关的功能要求不属于本建议书范围。

6.7 会话标识

本建议书中有很多与会话相关的术语。DPI-FE可以清楚地确定会话的所有流量，因为，“会话描述符”或相当于流和/或应用描述符或为其子集。

6.7.1 会话标识要求

R-6.7.1/1：要求DPI-FE可以分析会话（如RTP会话、HTTP会话、IM会话、VoIP SIP会话）行为。

R-6.7.1/2：要求DPI-FE可以跟踪会话状态。

6.7.2 “会话层”的DPI行动

R-6.7.2/1：DPI-FE可选择在会话层提取或生成测量数据（如用于监测有关用户体验质量的性能指标）。

6.8 加密流量的检查

通常认为，DPI签名仅可用于非加密流量。然而，DPI签名可根据以下情况适用于加密流量：

- 加密水平（见第6.8.1段）；
- 解密密钥的本地可用性（见第6.8.2段）；
- 基于加密信息的检查条件（见第6.8.3段）。

6.8.1 加密程度

作为协议数据单元（PDU）的任何“包”包含不同协议层的协议控制信息（PCI）和数据单元（SDU）。当加密用于被检查通信路径时，加密可用于：

- 整个协议堆或仅仅协议堆的一部分（注1），以及
- 在协议层内，x（Lx）层的PDU（即完整的Lx-PDU）或部分（如仅仅是Lx-PCI或Lx-SDU部分）。

注1 – 举例：IP之上的RTP包服务可在以下情况下提供加密：

a) 网络层（如通过IPsec传送模式或IPsec隧道模式）；

b) 传送层（如，通过DTLS）；或/和

c) 应用层（如，通过SRTP）。

DPI可在包的任何非加密部分进行。

R-6.8.1/1：对加密流量的认识（从DPI签名角度）：DPI根据加密范围可选择在所有被检查流量的非加密信息元素上进行（注2）。

注2 – 举例：如仅有RTP SDU（包含IP应用数据）加密的话，IP之上的SRTP包流在DPI签名的情况下仍可基于有关RTP PCI（“RTP字头”）UDP PCI （“UDP字头”）、IP PCI（“IP字头”）等信息元素得到检查。

R-6.8.1/2：对加密流量的无知（从DPI签名角度）：DPI可选择作为部分DPI进行（因为，部分DPI签名可与非加密的包信息元素相关）。

有关加密流量的“部分DPI”可能导致“有限的DPI服务”（如附录1所述），但已能满足具体使用情况（如“应用或协议”的“粗颗粒”识别够用的话）。

6.8.2 解密密钥的可用性

R-6.8.2/1：DPI可选择用于本地提供已使用的加密密钥的情况。任何DPI执行均意味着对被检查包（本地副本）的初步解密。

6.8.3 基于加密信息的检查条件

R-6.8.3/1：当政策条件适用于基于加密信息检查的情况下，DPI可选择在加密流量上得到支持（注3）。

注 – 举例：比特模式（清楚地确定具体的包流）可通过观察（检查）部分加密的流量（见第6.8.1段）。比特模式作为之后DPI签名的组成部分在此时用于加密编码。

6.8.4 IPsec特定的DPI要求

第6.8.1至第6.8.4分段所述要求亦适用于IPsec加密包。该建议书侧重于IPsec加密流量的流标识方面。与应用标识相关的方面待进一步研究。

6.8.4.1 一般性要求

R-6.8.4.1/1：DPI-FE可选择至少支持IPsec加密流量的流标识。相应的流描述符n-tuple可选择仅限于基于L2和L3的元素。

R-6.8.4.1/2：流可选择对应于单一IPsec安全关联（SA）流量或选择横跨多个SA。

R-6.8.4.1/3：基于SA的流标识意味着，32比特IPsec安全参数指标（SPI）可选择作为流描述符的组成部分。

6.8.4.2 IPsec隧道和传送模式

IPsec协议（AH和ESP，见下文）可用来保护整个IP载荷（即隧道模式）或IP载荷的上层协议（即传送模式）。

R-6.8.4.2/1：DPI-FE可选择得以在隧道模式中检测IPsec加密流量。

R-6.8.4.2/2：DPI-FE可选择得以在传送模式检测IPsec加密流量。

6.8.4.3 IPsec AH保护的流量

认证字头（AH）提供数据完整性、数据来源认证和有限的可选防重播服务。

R-6.8.4.3/1：DPI-FE可选择可以基于相应的IP协议号检测AH保护的流量。

6.8.4.4 IPsec ESP保护的流量

封装安全载荷（ESP）提供附加保密性。

R-6.8.4.4/1：DPI-FE可选择得以基于相应的IP协议号检测ESP保护的流量。

6.9 压缩流量的检查

压缩的目的是减少流量数量，举例而言：

- 基于“ZIP”的压缩缩小了文件尺寸（与TCP/IP之上的FTP流相关）；
- 基于“SigComp”的压缩[b-IETF RFC 3320]缩小SIP消息尺寸（与L4/IP之上的SIP流相关）。

6.9.1 对压缩方法的认识

R-6.9.1/1：DPI在可获得有关应用压缩方案的本地信息时可选择得到支持（如DPI节点认识到，被检查的SIP信令路径符合[b-ETSI TS 124 229]第8段的编码）。任何DPI的执行则都意味着对被检查包（本地副本）的初步解压缩。

R-6.9.1/2：如果可以从被检查业务流中提取所使用的压缩方案时，DPI可选择亦得到支持（即，具体的zip压缩方法可选择从文件字头信息元素中推导）。

6.10 非正常流量的检测

6.10.1 检测非正常流量的要求

R-6.10.1/1：要求DPI-FE得以支持对非正常流量的检测。也就是说，DPI签名被要求得以确定正常和非正常流量的特点（如作为黑或白清单）。

注 – DPI政策规则方面：该能力可意味着检查流量和/或包特性的多种指标以及为就正常或非正常流量类型达成最终结论保持决策树的可能性。

7 从网络角度看功能要求

7.1 一般性要求

7.1.1 应急通信

DPI功能的总体设计、实施、部署和使用必须包含适当的测量，以防止对应急通信（ET）性能和安全造成不良影响。ET [ITU-T Y.2205]意味着任何相对于其它服务而言需要特殊处理的应急服务（即超越普通业务的优先处理）。这包括政府授权的应急服务，如应急通信服务[ITU-T E.107]和公共安全服务。

该建议书基于使用应用标签广泛确定不同应用语义（如应用协议类型（如H.264视频或SIP作为IP应用协议例子））。相同应用类型（如SIP）用来支持普通服务和应急通信应用服务。然而，本建议书未规定任何用来识别应急通信应用服务的专门应用标签。因此，为防止对应急通信应用服务造成不良影响，有必要采取适当的谨慎措施。

R-7.1/1：不得干预对应急通信应用服务流量提供的超越于普通服务的优先处理。

R-7.1/2：要求DPI功能的总体设计、应用、部署和使用包括适当的措施，以防止对应急通信应用服务的性能产生不良影响（如引入不必要的延迟）。

R-7.1/3：要求DPI功能的总体设计、实施、部署和使用包括适当的测量，以防止对应急通信/会话的完整性、保密性或可用性引发安全隐患。

注 – 本建议书不提供任何有关如何满足以上要求的规定。要求可通过使用功能性能力、操作测量或二者的结合加以实现。

7.2 DPI节点中的数据平面、控制平面和管理平面

7.2.1 从DPI节点角度看流量平面和流量类型

根据用户、控制和管理平面网络模型（见[b-ITU-T Y.2011]），DPI节点涉及数据路径和本地决策路径（见图7-1）。数据路径可在单向或双向模式内运行。

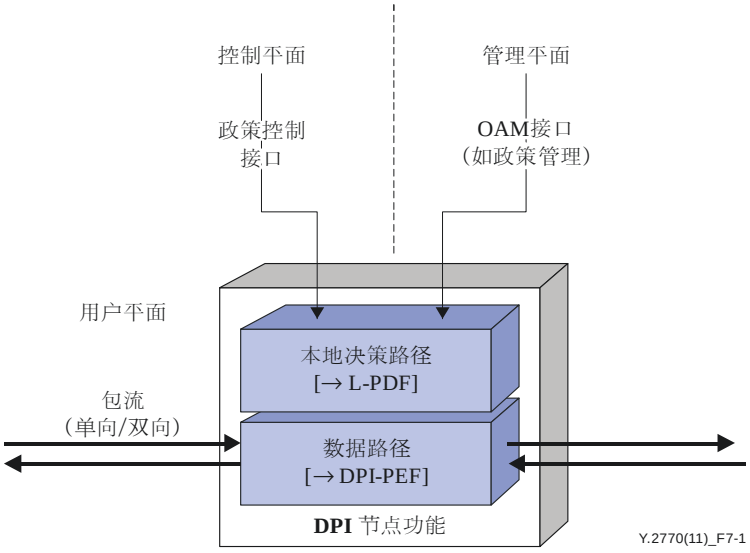


图7-1 – DPI节点的外部和内部流量平面

注1 – 包流在包路径上被选择路由/交换。这些路径在IP网络中通常被称为数据路径（见[b-IETF RFC 4778]），因此，数据平面一词与用户平面为同义词。

注2 – 在IP应用数据流量中，IP数据路径亦称为IP媒体路径（或承载路径），在IP应用控制流量中，或称为IP信令路径[b-ITU-T X.1141]。

R-7.2.1/1：要求DPI节点支持用于政策管理的管理平面接口并可选择支持用于政策控制的控制平面接口。

本地决策路径实体提供节点内控制和管理能力。

R-7.2.1/2：要求DPI节点识别两种包（见图7-2）：

a) 数据包，属于客户并承载客户流量（称为“THROUGH”流量，见[b-IETF opsec]）；

b) 控制和管理包，属于网络提供商，与网络操作相关（称为“TO”流量，见[b-IETF opsec]）。

两种包穿越“共同通道”（或“在带内”）或穿越在逻辑上将数据从“带外”控制包中分离出来的不同信道（亦见[b-IETF RFC 4778]有关管理流量示例的第2.2段）。

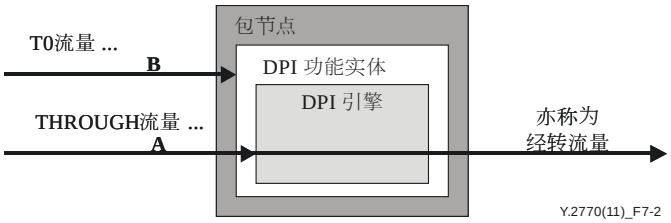


图7-2 – DPI节点的THROUGH(A)和TO(B)流量

7.2.2 有关管理平面的要求

R-7.2.2/1：要求DPI-FE支持用于DPI政策规则配置管理的管理协议。

R-7.2.2/2：建议DPI-FE支持用户身份信息和用户与用户应用之间关系的管理。

R-7.2.2/3：建议DPI-FE支持应用和服务的管理

- 生成、修改和公布应用模板；
- 维护应用和战略之间的关系并
- 提供并管理用户服务预留；

R-7.2.2/4：建议DPI-FE支持预先定义的或动态生成的战略的管理。（这些战略可选择与应用标识、应用控制和用户管理相关）

R-7.1.2/5：建议DPI-FE支持行政机构的管理。为支持分层的管理，不同管理人员具有不同的管理权限。

7.2.3 有关控制平面的要求

R-7.2.3/1：DPI-FE可选择支持政策控制协议（如用于[ITU-T Y.2111]针对DPI政策规则的控制和信令所定义的ITU-T *Rw*参考点的[b-ITU-T H.248.1]）。

7.2.4 有关用户（数据）平面的要求

数据（用户）平面满足以下可选要求：

R-7.2.4/1：DPI-FE可选择支持不同包技术（如xDSL、UMTS、CDMA2000、有线电视、LAN、WLAN、以太网、MPLS、IP、ATM）。

7.2.5 跨平面要求

R-7.2.5/1：DPI-FE可选择支持有关DPI政策规则规范的统一协议语法。政策控制接口（控制平面）和政策管理接口（管理平面）使用的句法最好相同。这并不意味着使用相同的协议，但涉及（DPI）政策规则的规范语言（通常称为过滤规范语言（FSL）或政策规范语言（PSL），见注1）。

注 – 脚本语言示例为SIEVE [b-IETF RFC 5228]或PERL、或XML或XACML（eXtensible接入控制标记语言）

统一的协议语法可在DPI节点中的政策执行路径内使用通用数据/对象模型，这是高效和快速执行规则以及在DPI签名库中无中断更新操作的前提。

8 DPI功能实体接口

上述各段描述的要求包含以下接口：

- DPI-FE和远端网络实体之间（见第8.1段）；
- DPI-FE内部组件之间（见第8.2段）。

8.1 外部DPI-FE接口

图8-1描述了DPI-FE的外部接口：

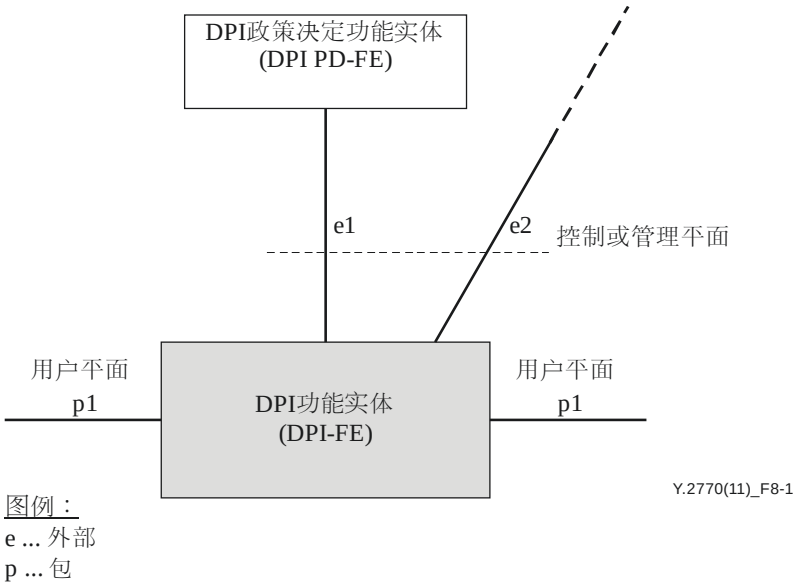


图8-1 – 外部DPI-FE接口

8.1.1 经检查的流量（p1）

DPI-FE与远端包节点通过p1交换包。包路径拓扑对于工作在路径内DPI模式中的DPI-FE来说为点对点。不支持多点拓扑。接口p1涵盖双向包路径。

工作在带外DPI模式中的DPI-FE的包路径拓扑与一个端点相关。

8.1.2 流量检查的控制/管理（e1）

DPI政策决定功能实体（DPI-PDFE）旨在控制或管理DPI-FE。通过e1交流的信息由此涉及控制/配置DPI-FE包处理行为的指令。这些指令可用DPI政策加以描述。

接口e1还从DPI-FE到DPI-PDFE的报告和通知。

8.1.3 向其它网络实体报告（e2）

接口e2包括与除DPI-PDFE以外的远端网络实体的所有可能的通信接口。该接口主要支持报告。

8.2 内部DPI-FE接口

图8-2基于DPI要求显示了可能的内部接口：

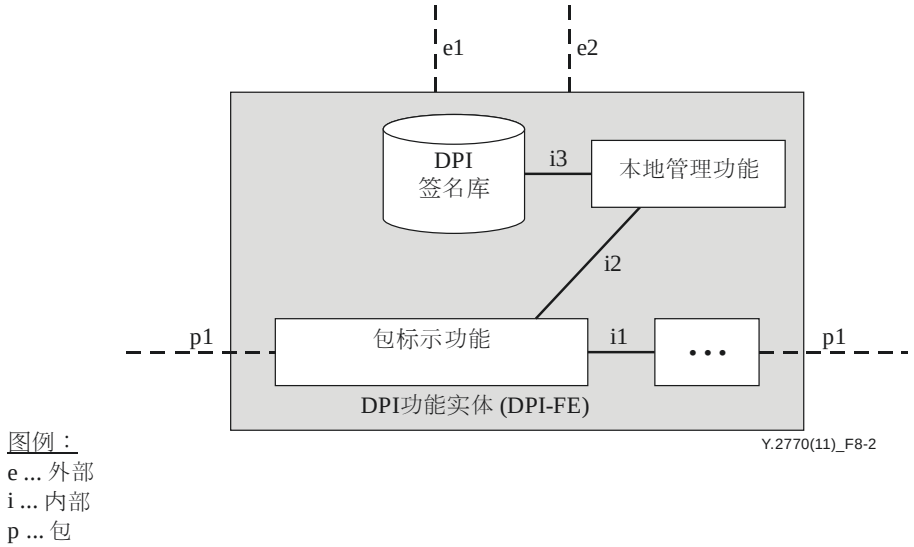


图8-2 – 内部DPI-FE接口

可能还有更多的DPI-FE内部功能组件和内部接口。内部接口有待进一步研究。

8.3 接口要求

R-8.3/1：建议接口e1符合第6.5段的要求。

R-8.3/2：建议接口e2符合第6.4.1段的要求。

9 安全考虑和要求

该段描述了NGN中DPI实体的安全威胁并定义了安全要求。

9.1 针对DPI实体的安全威胁

与DPI相关的功能实体一般位于ITU-T Y.2701建议书[ITU-T Y.2701]所定义的NGN运营商内部的可信赖区域或可信赖但易受影响区域。该建议书确定了对NGN的安全威胁并规定了防止这些威胁的要求。由于DPI相关实体是NGN的组成部分，[ITU-T Y.2701]的结论适用于这些实体。基于[ITU-T Y.2701]，与DPI实体相关的安全威胁确定如下：

- 对DPI相关信息的破坏；
- 对DPI相关信息的损坏或修改；
- DPI相关信息的盗用、取消或丢失；
- DPI相关信息的披露；
- 服务中断

有关DPI操作的信息包括DPI有关签名和DPI输出流及应用信息的政策。对这类信息的破坏、损坏或修改、盗用、取消或丢失可能使DPI操作无法使用这些信息。很多国家建议按照国家监管和政策要求对待这类信息，不得予以披露。

服务中断可能是DoS攻击的结果。任何接收数据的实体均可成为DoS的攻击对象。举例而言，攻击者可直接用大量流量冲毁DPI实体，造成合法用户DPI服务的质量下降或中断。

9.2 DPI实体的安全要求

DPI实体的主要安全要求包括：

R-9.2/1：必须保护DPI实体内的DPI相关信息。

R-9.2/2：如果在NGN运营商可信赖区域之外交流信息，应在DPI实体和远端功能实体（如DPI PD-FE、NMS）之间保护DPI相关信息。

R-9.2/3：可选择要求建立缓解对DPI FE破坏性攻击的机制。

R-9.2/4：要求厂商、运营商和服务提供商在实施本建议书时考虑到国家监管和政策要求。

R-9.2/5：建议实施者利用现有经反复测试的机制来满足本建议书的安全要求，如ITU-T Y.2704 [ITU-T Y.2704]建议书的规定。

附件A

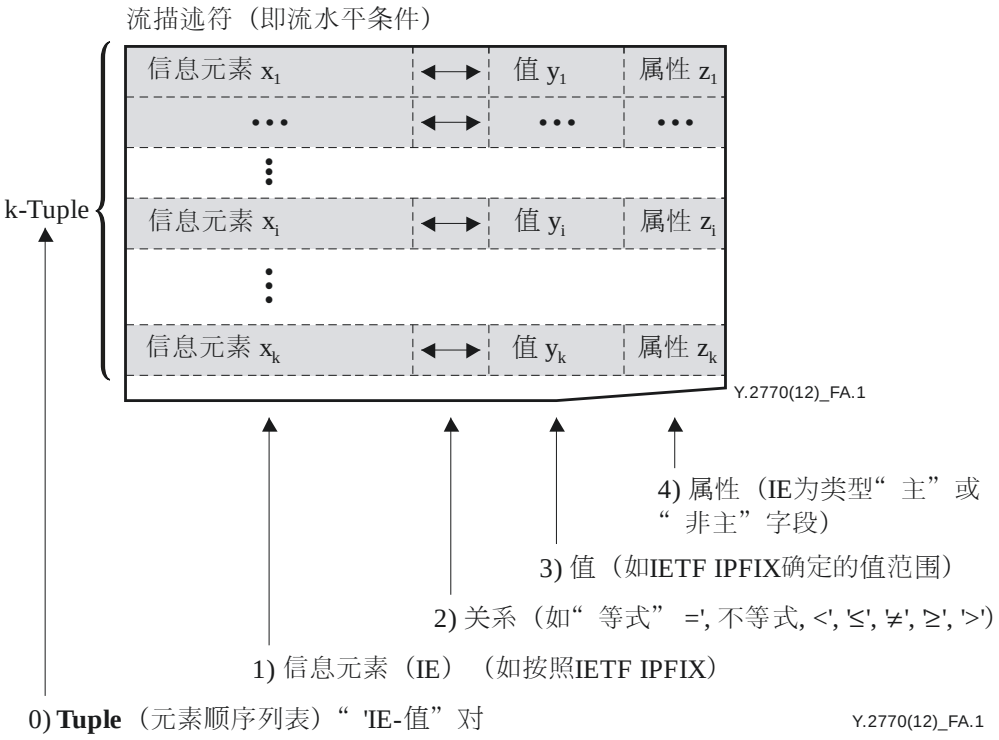
流描述符规范

（本附件是本建议书的组成部分）

A.1 协议句法问题

流描述符涉及数据结构（数据对象）。该数据对象可作为k-Tuple建模（见图A.1）。数据结构包含k信息元素（IE）（注1）。k值为变量并大于零[1]，但针对具体流而言为常数。信息元素是包含在IANA IPFIX寄存器中的1。每个信息元素都有一个相关的值。这种关联一般用数学等式（'='）表示，但并不排斥其它数学关系。

注1 – IETF IPFIX信息元素可被定为"主字段"或"非主字段"。



图A.1 – 从协议句法角度看流描述符（流层面条件）

流水平描述符k元组一直代表"名称值对"（NVP）的k清单；在此为"<IE ↔值>"对)[2]的序列。

A.2 规定信息元素值

在流水平条件中，IE的值可为：

- 全规定值
  全规定值代表名称值的全面设置的情况。

---

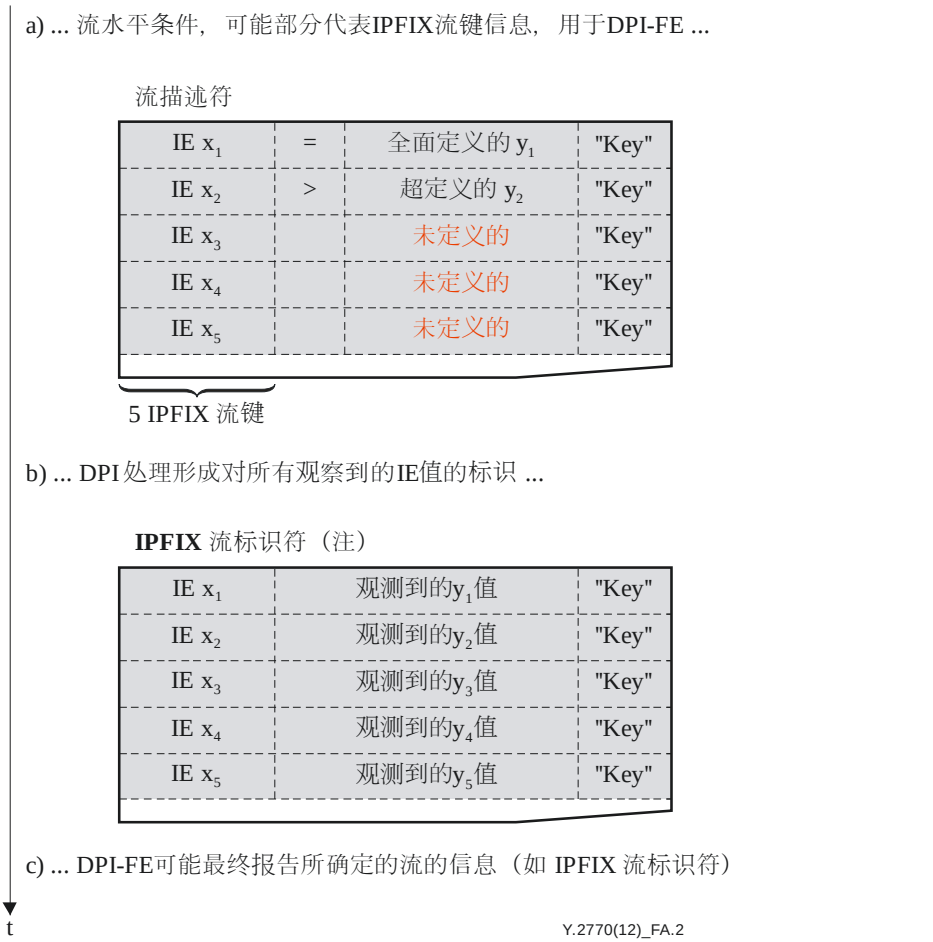
[1] 注：N = 0表明"独立于流"。

[2] 与AVP（<属性名称、值>）等其它结构、参数值对（<parm=value>）等相似。

- 无规定
  “无规定”代表尚未对IE分配任何值的情况。
- 过度规定或
  过度规定表示一个IE可能有多个值。
- 规定不足
  规定不足表示未知因素（如，所有可能的值或选择值）。

A.3 流描述符、IPFIX流标识符和IPFIX流键之间的关系

图A.2中的示例提供了一个5元组流描述符，包含5个IFPIX流键。为确定具体的流，流描述符按照第A.2款的规定施对这些流键加了一些条件：第一个流键IE x_1为“全规定值”，第二个流键IE x_2为“过度规定值”，而其它IE为“无规定”，如图A.2 a)部分所示。



注 – IPFIX流标识符是从流描述符中推导得出的对象，因此，不影响流描述符的内容。

图A.2 – 流描述符、IPFIX流标识符和IPFIX流键示例

请注意流描述符不仅对IPFIX流键施加条件：的确，在一些情况下，流描述符可能需要对非流键施加条件，举例而言，当需要流第一个包的TCP旗语时。流描述符和IPFIX流标识符在图A.2示例中的主要差别在于，流描述符包含一个有关IE x_2的“大于”条件（“IE x_2 > value y_2”），而IPFIX流标识符包含IE x_2的观测值，即值yy_2。当DPI功能实体处理了数据包并将其归类入流后，IPFIX流标识符由一套流键的观测值构成。

请注意，如输出信息（如，通过IPFIX流记录）包含除相关观测值以外的各IE，无论IE是否为IPFIX流值，没有必要分配具体的IPFIX流标识符，因为IPFIX流标识符是所有这一信息的集合。

参考资料

[b-ITU-T H.248.1] Recommendation ITU-T H.248.1 v3 (2005), *Gateway Control Protocol: Version 3*.

[b-ITU-T X.734] Recommendation ITU-T X.734 (1992), *Information technology – Open Systems Interconnection – Systems Management: Event report management function*.

[b-ITU-T X.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.

[b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation 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-ETSI ES 282 003] ETSI ES 282 003 (2011), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture*.

[b-ETSI TS 123 203] ETSI TS 123 203 (2011), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control architecture (3GPP TS 23.203 version 10.4.0 Release 10)*.

[b-ETSI TS 124 229] ETSI TS 124 229 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE;IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 version 9.4.0 Release 9)*.

[b-IETF IANA IPFIX] IETF IANA IPFIX (2007), IP Flow Information Export (IPFIX) Entities.
<http://www.iana.org/assignments/ipfix/ipfix.xhtml>

[b-IETF opsec] IETF draft-ietf-opsec-filter-caps (2007), *Filtering and Rate Limiting Capabilities for IP Network Infrastructure*.
<http://tools.ietf.org/html/draft-ietf-opsec-filter-caps-09>

[b-IETF RFC 1950] IETF RFC 1950 (1996), *ZLIB Compressed Data Format Specification version 3.3*.

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

[b-IETF RFC 3320] IETF RFC 3320 (2003), *Signaling Compression (SigComp)*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[b-IETF RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*.

[b-IETF RFC 4268] IETF RFC 4268 (2005), *Entity State MIB*.

[b-IETF RFC 4778] IETF RFC 4778 (2007), *Operational Security Current Practices in Internet Service Provider Environments*.

[b-IETF RFC 4867] IETF RFC 4867 (2007), *RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs.*

[b-IETF RFC 5102] IETF RFC 5102 (2008), *Information Model for IP Flow Information Export*.

[b-IETF RFC 5103] IETF RFC 5103 (2008), *Bidirectional Flow Export Using IP Flow Information Export (IPFIX).*

[b-IETF RFC 5228] IETF RFC 5228 (2008), *Sieve: An Email Filtering Language.*

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol*.

[b-IETF RFC 5426] IETF RFC 5426 (2009), *Transmission of Syslog Messages over UDP*.

[b-IETF RFC 5476] IETF RFC 5476 (2009), *Packet Sampling (PSAMP) Protocol Specifications*.

[b-PacketTypes] McCann, P.J., and Chandra S. (2000), *Packet Types: Abstract Specification of Network Protocol Messages*; in SIGCOMM '00: Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp. 321-333, ACM Press, New York.

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
2014年，日内瓦