国 际 电 信 联 盟

ITU-T

Y.2772

(04/2016)

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、物联网和智慧城市

下一代网络 – 安全

支持深度包检测的网元机制

ITU-T Y.2772 建议书

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、物联网和智慧城市

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
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
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899
运营商水平的开放环境	Y.2900–Y.2999
未来网络	Y.3000–Y.3499
云计算	Y.3500 -Y.3999
物联网、智慧城市和社区	
综述	Y.4000-Y.4049
定义和术语	Y.4050-Y.4099
要求和应用案例	Y.4100-Y.4249
技术设施、连接和网络	Y.4250-Y.4399
框架、构架和协议	Y.4400-Y.4549
业务、应用、计算和数据处理	Y.4550-Y.4699
管理、控制和性能	Y.4700-Y.4799
识别与安全	Y.4800-Y.4899

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T Y.2772建议书

支持深度包检测的网元机制

摘要

ITU-T Y.2772建议书规定了支持深度包检测的网元机制（DPI），其中包括针对基于数据包的网络深度包检测的程序和方法，目的在于帮助理解DPI产品相关的方法、接口、规程、程序和流程。

历史沿革

版本	建议书	批准	研究组	识别码*
1.0	ITU-T Y.2772	2016-04-29	13	11.1002/1000/12709

* 访问建议书，请在您的Web浏览器地址栏中输入网址http://handle.itu.int/，其次建议书的识别码，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、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）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，国际电联已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

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 3
5 惯例 4
6 DPI机制的定义 4
7 支持应用识别的DPI机制概述 4
7.1 DPI机制的概况 4
7.2 DPI节点的基本结构 4
7.3 支持DPI功能的典型网络 4
7.4 与DPI节点有关的DPI机制 5
7.5 部署DPI节点的网络机制 6
8 DPI-PIB的DPI策略规则的表示方法 6
8.1 概述 6
8.2 适用于DPI策略规则条件的数据和掩码表示方法 6
8.3 DPI策略规则条件的正则表达式表示方法 6
8.4 DPI策略规则条件的混合表示方法 7
9 适用于DPI实体的信息流、处理程序和方法 7
9.1 概述 7
9.2 接口实现 8
9.3 信息流 9
9.4 过程程序 11
9.5 保护方法 12
9.6 数据同步方法 12
10 运行机制描述 13
10.1 概述 13
10.2 运行机制的目标 14
10.3 性能问题或DPI节点部署 14
10.4 当前网络分析 14

页码

10.5 确认网络的DPI要求 15
10.6 选择合适的DPI实体或系统 15
10.7 使用DPI改造当前的网络 15
10.8 监视和管理具有DPI的网络 15
10.9 基于性能监视程序重建具有DPI的网络 16
11 管理机制描述 16
11.1 DPI网络管理概述 16
11.2 管理接口 17
11.3 管理协议和功能 19
12 安全方面的考虑 19
参考资料 20

ITU-T Y.2772建议书

支持深度包检测的网元机制

1 范围

本建议书提供了分组网中深度包检测（DPI）的实现机制，主要目的是描述能够用于识别DPI功能和其它网络功能之间信息流的DPI的应用模型、相关协议、接口、方法程序和过程。

本建议书的范围包括：

– DPI机制的定义；

– 支持应用识别的DPI机制概述；

– 运行方面的程序和信息流；

– 管理方面的程序和信息流，例如DPI策略管理；

– 适用于可能存在的DPI功能实体（FE）接口的其它程序和信息流。

以下内容超出了本建议书的范畴：

– 非DPI实体特有的运行和管理问题；

– ITU-T M系列和X系列建议书已经做出规定的、与管理功能有关的通用网元。

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ITU-T建议书中描述的机制可能并不适用于国际通信，以确保保密和主权国家对电信设置的法律规定，以及国际电联章程和公约。

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 Y.2111] ITU-T Y.2111建议书（2011），下一代网络资源和允许控制功能。

[ITU-T Y.2704] ITU-T Y.2704建议书（2010），下一代网络（NGN）的安全机制和程序。

[ITU-T Y.2770] ITU-T Y.2770建议书（2012），下一代网络深度包检测的要求。

[ITU-T Y.2771] ITU-T Y.2771建议书（2014），深度包检测框架。

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 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 [b-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。

3.1.2 DPI分析程序 DPI analyser [ITU-T Y.2771]：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[ITU-T Y.2771]第3.2.5节）。DPI分析程序可以提供入侵检测系统（IDS）分析程序的功能。

3.1.3 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，包识别功能以及图6-1/[ITU-T Y.2770]中所示的其它包处理功能）。

3.1.4 DPI节点 DPI node [ITU-T Y.2771]：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。

3.1.5 DPI策略行动（简称行动）DPI policy action (action in short) [ITU-T Y.2771]：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 RFC 3198]。

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扫描程序（也被用作“DPI扫描功能”）DPI scanner (also used as “DPI scan function”) [ITU-T Y.2771]：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[ITU-T Y.2771]第3.2.1节）。

3.2 本建议书定义的术语

无。

4 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：

BRAS 宽带远程访问服务器

CLI 命令行接口

CMIP 通用管理接口协议

DPI 深度包检测

DPI-PDFE DP策略决定功能实体

DPI-PIB DPI策略信息库

EMS 网元管理系统

GUI 图形用户接口

IP 互联网协议

IPFIX IP流信息输出

LAN 局域网

L-PDF 本地PDF

NMS 网络管理系统

OAM 操作、管理和维护

PDF 策略决定功能

PIB 策略信息库

SNMP 简单网络管理协议

SR 服务路由器

TCAM 三元按内容寻址存储器

TCP 传输控制协议

UDP 用户数据报协议

VLAN 虚拟局域网

5 惯例

无。

6 DPI机制的定义

在本建议书中，认为术语“机制”包含实现某些功能或满足某些要求的手段、方法、过程和程序，基于此考虑，DPI机制可以描述为：

– 用于实现[ITU-T Y.2771]中规定的功能和能力以及[ITU-T Y.2770]中规定的要求的具体过程；

– 实现[ITU-T Y.2771]中规定的功能和能力以及[ITU-T Y.2770]中规定的要求所采取的详细程序；

– 实现[ITU-T Y.2771]中规定的功能和能力以及[ITU-T Y.2770]中规定的要求所采用的适当方法；

– 有助于实现[ITU-T Y.2771]中规定的功能和能力以及[ITU-T Y.2770]中规定的要求的专用工具或手段。

7 支持应用识别的DPI机制概述

7.1 DPI机制的概况

DPI机制包括两个主要方面：

– 与DPI节点有关的DPI机制；

– 与支持DPI功能的网络相对应的DPI机制。

在详细说明这两个方面之前，有必要介绍DPI节点的基本结构和支持DPI功能的典型网络。

7.2 DPI节点的基本结构

[ITU-T Y.2770]的图6-1和[Y.2771]的图7-2已经描述了DPI节点的基本结构；可以在此结构的基础上实现DPI节点。

7.3 支持DPI功能的典型网络

部署DPI节点的典型网络如图7-1所示，其中从上往下，包含5个逻辑层：云、核心层、汇聚层、接入层和终端层。应该强调的是逻辑链路存在于每一个DPI节点和网元管理系统（EMS）或者网络管理系统（NMS）之间，尽管图7-1中并未画出所有的逻辑链路。所有的DPI节点均能与网络实体（例如，路由器、交换机和宽带远程访问服务器（BRAS）等）协同工作，图7-1中的DPI节点与上层的网络实体无关。

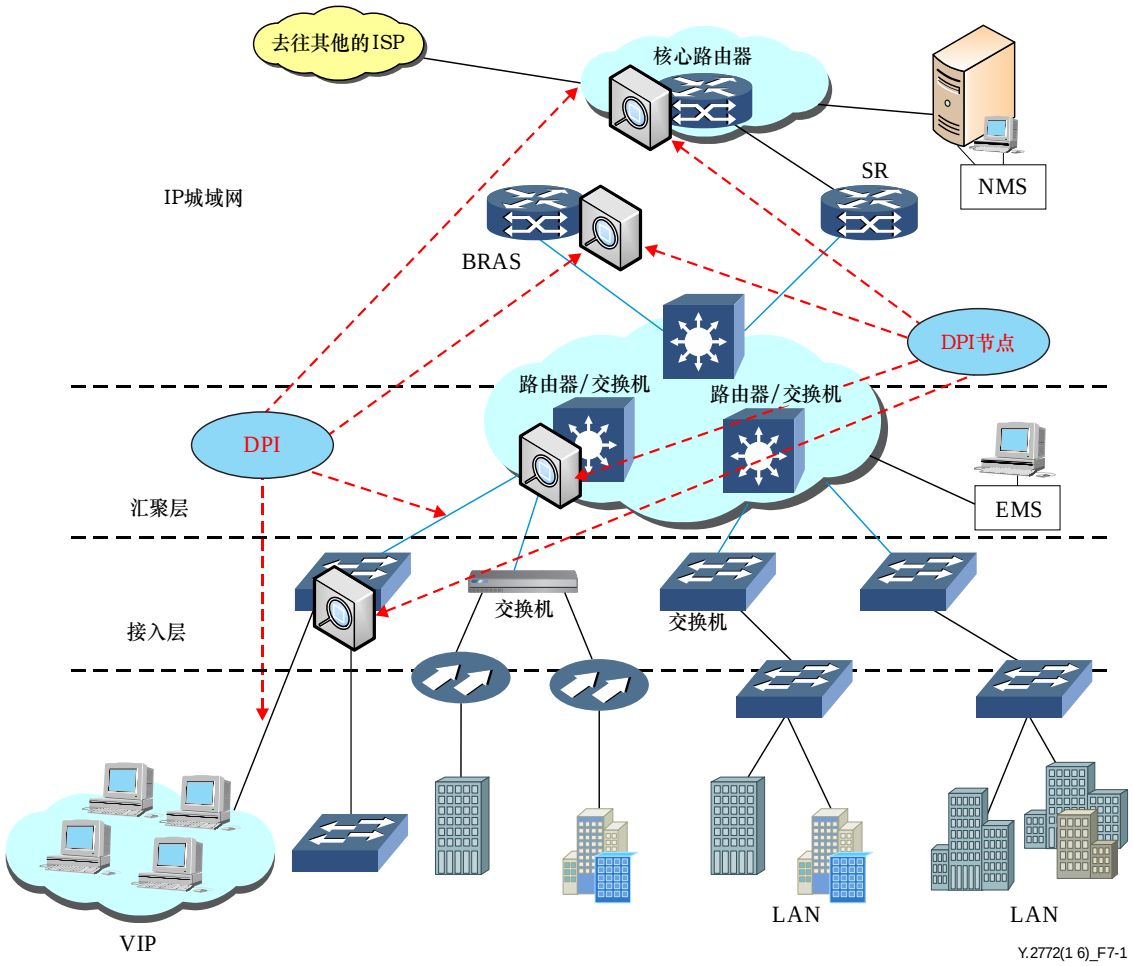

图7-1 – 部署DPI节点的网络拓扑示例

更多信息见[b-ITU-T Y.sup25]图6-3给出的DPI应用网络示例。

7.4 与DPI节点有关的DPI机制

DPI节点的DPI机制主要包括以下三个方面：

1) 信息表示方法

支持DPI功能的网元需要表示其中各种各样的信息和数据，例如，DPI规则。信息表示方法对于网元非常重要；不同的表示方法会产生不同的处理效率。

2) 处理方法和程序

处理方法和程序包括实现DPI相关功能的指导性方法，以及网元在支持这些DPI功能时所执行的程序。

3) 接口和适合的协议

接口和适合的协议包括实现[ITU-T Y.2770]中规定的接口（例如e1、e2）以及用于在上述各种接口之间交换信息的适合的协议。

7.5 部署DPI节点的网络机制

与支持DPI功能的网络相对应的机制包括以下方面：

- 操作方面；
- 管理方面。

8 DPI-PIB的DPI策略规则的表示方法

8.1 概述

DPI策略信息库（DPI-PIB）的DPI策略规则条件是一个DPI节点的核心部分之一，DPI节点几乎所有的行动均以DPI策略规则条件为基础。因此，有效地表示并且容易处理DPI策略规则条件是非常重要的。描述了三种DPI策略规则表示方法：数据和掩码表示方法、正则表达式表示方法和混合表示方法。

8.2 适用于DPI策略规则条件的数据和掩码表示方法

IP地址和掩码表示方法通常用于TCP/IP协议栈和相关的网络设备；数据和掩码表示方法与IP地址和掩码表示方法类似。在数据和掩码方法中，字节串（数据）用于表示标识一个特定数据流的标记字，字节串相对应的位串（掩码）用于决定是否检查字节串的某一个比特。通常，如果掩码位为“1”，则不检查该字节串对应的位，相反地，如果掩码位为“0”，则需要检查该字节串对应的位。

对于DPI-PIB，适合采用数据和掩码表示方法，该方法具有以下优点：

- 简单且易于理解；
- 高效，单个数据项可以被多个数据流共享；
- 与通用设备很好地匹配，例如三元内容可寻址存储器（TCAM）。

下面的两个例子说明了数据和掩码表示方法：

1) 匹配其TCP源端口范围从0x2100到0x21ff的数据流

在DPI-PIB中，为了满足该要求只需要一个数据项：

Item1: 数据: 0x2100, 掩码: 0x00ff

2) 匹配其虚拟局域网（VLAN）在集合16-63内的数据流

在DPI-PIB中，满足该要求需要两个数据项：

Item1: 数据: 0x0010, 掩码: 0x000f

Item2: 数据: 0x0020, 掩码: 0x001f

8.3 DPI策略规则条件的正则表达式表示方法

数据和掩码表示方法适用于表示具有固定位置和确定数值的标记字，通常，第2层到第4层（L2-L4）协议报头很符合这类要求。

然而，高层应用的标记字通常不确定并且容易改变，在这种情况下，采用数据和掩码表示方法难以实现。在这些应用中，正则表达式表示方法更适合于那些类型的标记字。

正则表达式[b-ITU-T X.680]是计算机科学中一个众所周知的描述方法；正则表达式的详细介绍和分析超出了本建议书的范畴。

下面的两个例子说明了正则表达式表示方法：

1) 匹配包含字“Bittorrent”或“Bitcomment”的数据流

在DPI-PIB中，为了满足该要求只需要一个数据项：

Item1: “/Bit(torrent|comment)/”

2) 匹配包含字“Worm”的数据流，其中下列字不是“v1”或“v2”

在DPI-PIB中，为了满足该要求只需要一个数据项：

Item1: “Worm(?<!v1|v2)”

8.4 DPI策略规则条件的混合表示方法

DPI功能能够对第2层-第7层起作用，当考虑第2层-第4层时，为了建立DPI-PIB，采用数据和掩码表示方法是很好的选择。另一方面，当考虑在第7层使用标记字时，正则表达式表示方法对于建立DPI-PIB是更好的选择。

因此，对于很多应用环境，组合上述两种表示方法是有用的；这被称为混合表示方法。在这种方法中，一些标记字采用数据和掩码表示方法表示，而其余的标记字采用基于正则表达式表示方法来表示。

下面的例子说明了混合表示方法：

1) 匹配包含字“Bittorrent”或“Bitcomment”的数据流，其中数据流的VLAN在集合8-15内

在DPI-PIB中，为了满足该要求只需要一个数据项：

Item1: 前一半: 数据: 0x0008, 掩码: 0x0007

后一半: “/Bit(torrent|comment)/”

这两半可以存储在不同的存储器内，但它们相互之间是逻辑连接的。

9 适用于DPI实体的信息流、处理程序和方法

9.1 概述

DPI实体包括许多必需的功能，这些功能的实现依靠下列诸多方面：

– 一些必需接口的实现（见第9.2节）；
– 功能部件之间信息流的设计（见第9.3节）；
– 主功能部件的处理程序（见第9.4节）；
– 增强可靠性的方法（见第9.5节）；
– 有效实现信息交换和数据同步的方法（见第9.6节）；
– 有益于实现DPI实体的其它方法。

9.2 接口实现

9.2.1 接口概述

[ITU-T Y.2770]规定并说明了一些接口，包括外部接口e1、e2和内部接口i1、i2、i3。在这些接口中，外部接口e1和e2的描述见[ITU-T Y.2770]的图8-1，[ITU-T Y.2770]的图8-2规定了内部接口i1、i2和i3。理论上，所有这些接口都应该在一个DPI节点内实现。

然而，也应基于应用要求实现其它的接口，例如，在双向DPI环境下，在一个DPI节点内可能需要特殊的外部接口e3（见图11-4）。

9.2.2 内部接口

内部接口（见[ITU-T Y.2770]的图8-2）用于一个DPI节点内的内部功能部件之间交换信息，内部接口有三个：i1、i2和i3。下面小节介绍了这些内部接口的实现。

9.2.2.1 i1接口

内部接口i1是在DPI-FE的内部包识别功能和其它包处理功能之间的接口，通常，i1接口是一个采用硬件实现的物理接口，以确保DPI节点的处理性能。i1接口可采取多种方法实现，包括共享存储器、内部并行通信端口和内部串行通信端口等。

9.2.2.2 i2接口

内部接口i2是在DPI-FE的内部包识别功能和本地管理功能之间的一个接口，i2接口是采用软件实现的一个逻辑接口，有多种方法来设计i2接口。

如果由同样的CPU来执行、控制或管理包识别功能和本地管理功能，则i1接口可以采取多种方法实现，例如一组应用程序接口（API）功能、共享的存储器和进程间通信。

如果由不同的CPU来执行、控制或管理包识别功能和本地管理功能，则可采用数据通信方法来实现i1接口。例如，上述两个功能部件可以通过TCP或UDP来交换信息。

9.2.2.3 i3接口

内部接口i3是在DPI-FE的内部DPI签名库和本地管理功能之间的一个接口，i3接口是一个采用软件实现的逻辑接口，通常，DPI签名库和本地管理功能被设计成由同样的CPU控制，i3接口可以用一组API功能来实现。

9.2.3 外部接口

外部接口（见[ITU-T Y.2770]图8-1）用于DPI节点和其它功能实体例如NMS之间交换信息，外部接口也有三个：e1、e2和e3，外部接口e1和e2如[ITU-T Y.2770]的图8-1所示，外部接口e3的描述见本建议书的图11-4。第9.2.3.1节至第9.2.3.3节规定了这些外部接口的实现。

9.2.3.1 e1接口

外部接口e1是DPI策略决定功能实体（DPI-PDFE）和DPI功能实体（DPI-FE）之间的一个接口，[ITU-T Y.2770]提供了实现该接口的一个解决方案：按照[ITU-T Y.2111]的规定，e1接口可以随意地为一个Rw参考点。尽管Rw是一个可行的解决方案，但它不是唯一的，也不是强制性的。

无论采用哪个解决方案来设计e1接口，应确保经过该接口传输的数据能被DPI-PDFE和DPI-FE理解，即便DPI-PDFE和DPI-FE不是由同一个供货商设计的。

9.2.3.2 e2接口

外部接口e2是DPI-FE和除了 DPI-PDFE之外的远程网络实体（例如，NMS）之间的一个接口。[ITU-T Y.2770]还提供了实现该接口的一种解决方案：建议e2接口采用基于IP流信息输出（IPFIX，见[b-IETF RFC 5101]）的输出协议。虽然e2接口可以使用基于IPFIX的输出协议，但DPI-FE和除了DPI策略决定功能实体（DPI-PDFE）之外的远程网络实体之间的信息交换也可能采用其它解决方案。

无论采用哪种解决方案来设计e2接口，应确保经过该接口传送的信息能被远程网络实体和DPI-FE所理解，而不管远程网络实体和DPI-FE是否属于同一个供货商。

9.2.3.3 e3接口

外部接口e3是两个独立的DPI-FE之间的、在必须满足双向DPI应用要求时的一个接口。第11节给出了对该接口的详细技术要求。

9.3 信息流

9.3.1 面向DPI引擎的信息流

图9-1描述的是源自DPI引擎的信息流，DPI引擎和本地策略决定功能（L-PDF）之间的数据交换在DPI实体内，同时，L-PDF和PD-FE之间的数据交换在DPI实体外。

与DPI有关的数据交换应该是非常可靠的，另一方面，DPI实体内的数据通信比两个独立实体之间的数据通信更为可靠，因此，为了确保数据交换的可靠性，两个独立实体之间的数据交换最好采用基于连接的方法，一个DPI实体内的数据交换可以是无连接的，以便降低系统资源并提高数据交换的效率。

因此，在图9-1中，建议将DPI-引擎和L-PDF之间的数据交换设计成无连接模式，原因是DPI引擎和L-PDF在单一的DPI实体内，然而，建议将L-PDF和PD-EF之间的数据交换设计成基于连接的模式，原因是PD-FE不在单一的DPI实体内。

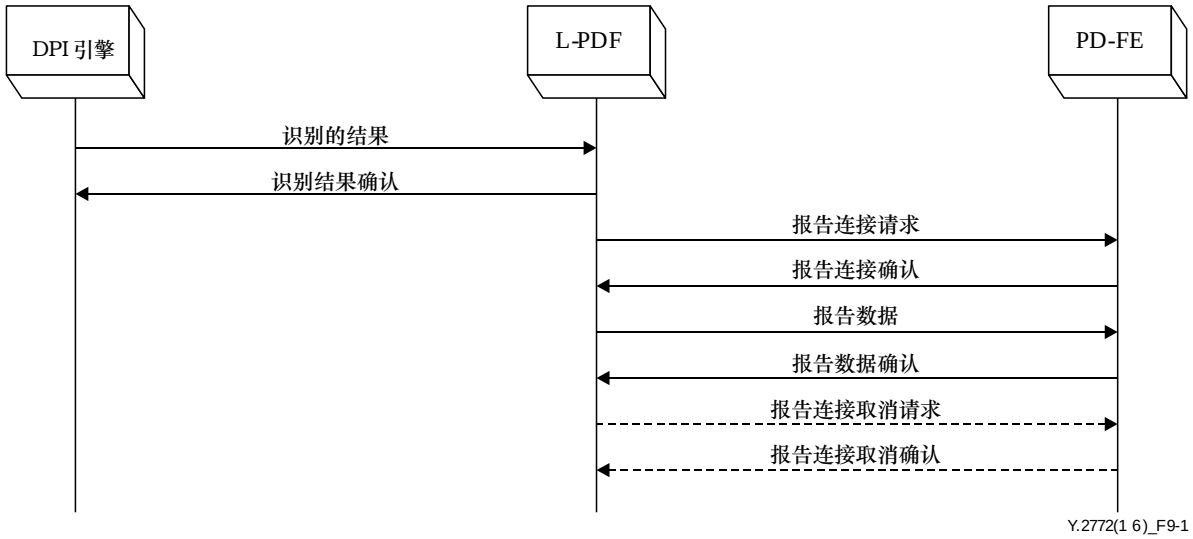

图9-1 – 面向DPI-引擎的信息流

在图9-1中，原语“识别的结果”用于传输由DPI-引擎产生的数据，原语“识别结果确认”用于告知DPI引擎上述数据已经收到。原语对“报告连接请求”和“报告连接确认”用于建立一个连接，原语对“报告数据”和“报告数据确认”用于传输报告的数据。在完成了所有的报告数据交换之后，原语对“报告连接取消请求”和“报告连接取消确认”可选地用于删除该连接（用图9-1中的虚线表示）。

9.3.2 面向DPI-PIB的信息流

图9-2描述的是基于DPI-PIB的信息流。DPI-PIB和L-PDF之间的数据交换在DPI实体内部，而L-PDF和PD-FE之间的数据交换在DPI实体之外。

在图9-2中，建议将DPI-PIB和L-PDF之间的数据交换设计成无连接模式，建议将L-PDF和PD-EF之间的数据交换设计成基于连接的模式。

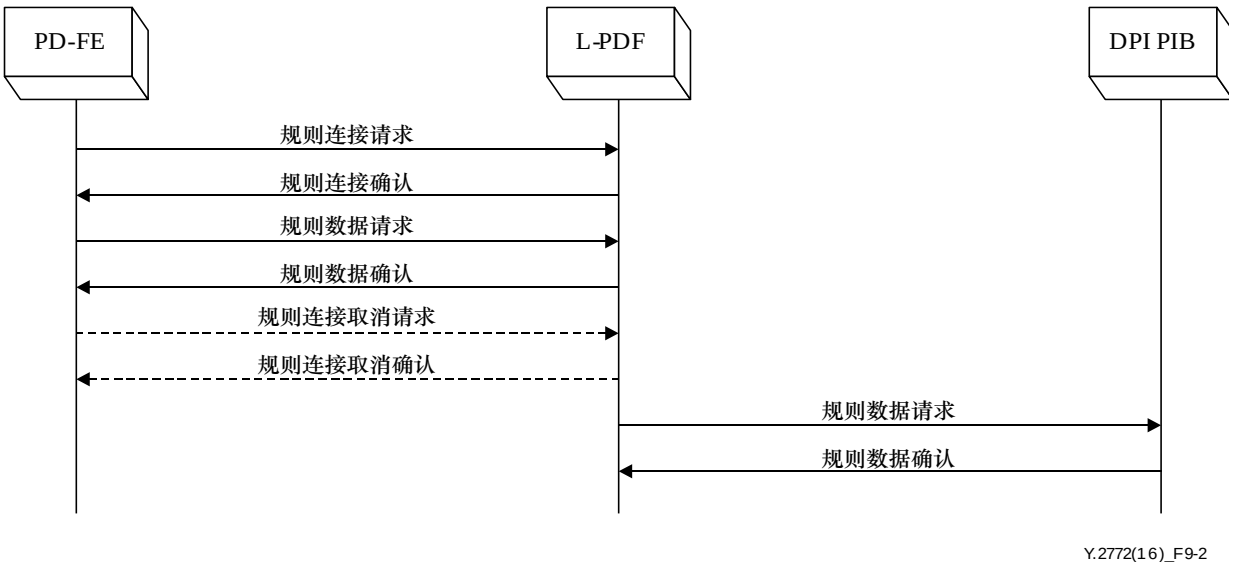

图9-2 – 面向DPI-PIB的信息流

在图9-2中，原语对“规则连接请求”和“规则连接确认”用于建立一个连接，另一个原语对“规则数据请求”和“规则数据确认”用于传输规则数据。在完成了所有规则数据交换之后，原语对“规则连接取消请求”和“规则连接取消确认”可选地用于删除该连接（用图9-2中的虚线表示）。

9.3.3 面向DPI L-PDF的信息流

图9-3描述的是面向DPIL-PDF的信息流，L-PDF和PD-FE之间的数据交换以及L-PDF和管理实体之间的数据交换均在DPI实体的外部。

在图9-3中，PD-FE、L-PDF和管理实体这三个功能部件之中，没有两个部件属于单一的实体，因此，建议将相互的数据交换设计成基于连接的模式。

在图9-3中，四个原语对（包括“规则连接请求”和“规则连接确认”，“规则同步连接请求”和“规则同步连接确认”、“报告连接请求”和“报告连接确认”，以及“配置连接请求”和“配置连接确认”）用于建立一个相应的连接。同时，另外四个原语对（包括“规则数据请求”和“规则数据确认”，“规则数据请求”和“规则数据确认”，“报告数据请求”和“报告数据确认”、“配置数据请求”和“配置数据确认”）用于传输相应的数据。此外，与每一类连接相对应，在完成了全部相应数据交换之后，原语对“…连接取消请

求”和“…连接取消确认”可选地用于删除该连接。为了降低复杂度并避免混淆，图9-3并没有画出最后提到的这些原语，然而它们具有与原语对“规则连接取消请求”和“规则连接取消确认”类似的功能。

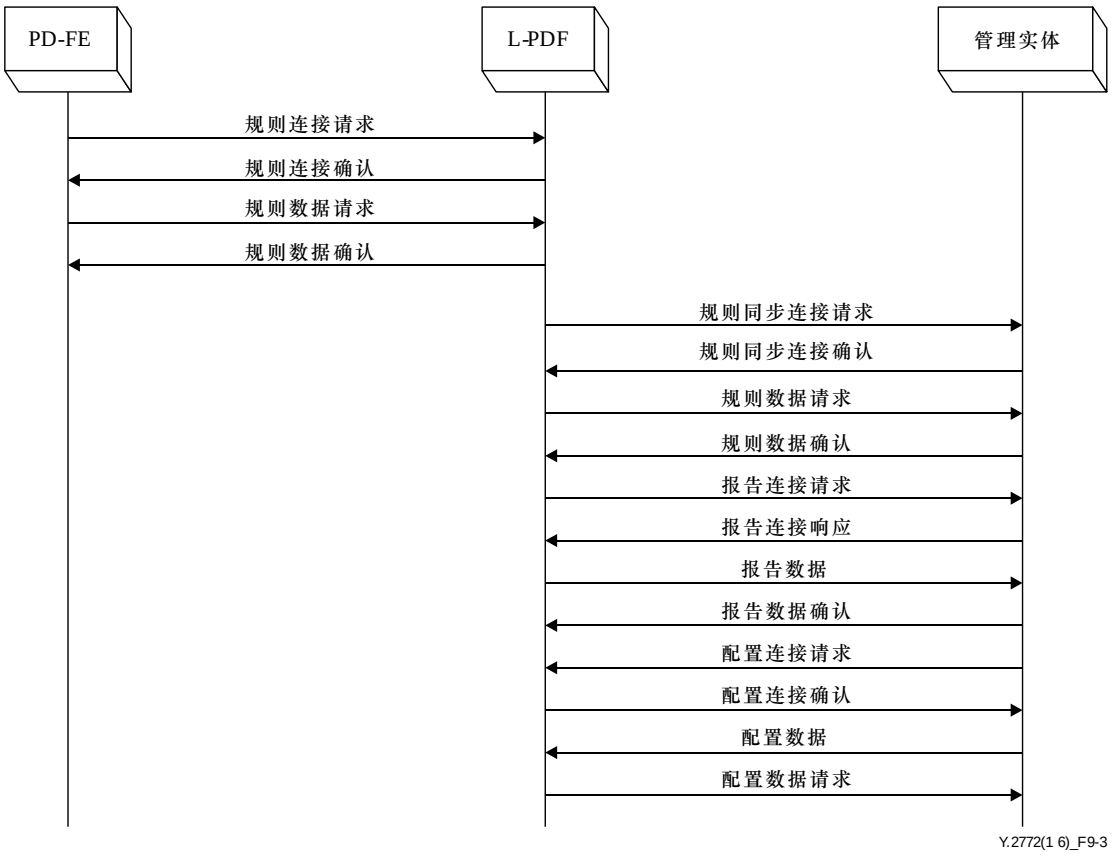

图9-3 – 面向L-PDF的信息流

9.4 过程程序

9.4.1 DPI-引擎过程程序

当一个数据包进入DPI引擎时，DPI引擎会按照DPI-PIB中规定的策略扫描并识别数据包，然后DPI引擎的分析程序对识别的数据包进行分析，并记录分析的结果。此后，将按照识别的结果执行策略行动。

如果数据包不能被识别，则实施‘不能被识别’行动。如果数据包被识别，DPI引擎将会按照DPI-PIB中规定的策略规则执行相应的行动。

同时，DPI引擎记录每个数据包的识别结果，缓存多个类似的结果，定期向管理实体报告该结果。报告的周期是实现所特有的，超出了本建议书的范畴。

9.4.2 DPI-PIB过程程序

DPI-PIB包含一条或多条DPI策略规则记录的集合，在L-PDF收到来自PD-FE的规则数据之后，DPI-PIB才会接收到来自L-PDF的规则数据。

9.4.3 L-PDF过程程序

L-PDF收到来自远程策略决定功能（PDF）的规则数据时，会更新DPI-PIB的规则记录。当L-PDF收到来自DPI引擎的识别结果时，会将识别的结果发送给远程PDF。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。

9.5 保护方法

[ITU-T Y.2771]已经规定了“1+N”冗余组来实现容错，有两种截然不同的保护模型：“1+1”（N=1）模型和“1+N”（N>1）模型。“1+1”模型用于一个活跃部件和一个备用部件，而“1+1”（N>1）模型用于一个活跃部件和N个备用部件。

9.5.1 “1+1”模型

“1+1”模型也被称为活跃/备用模型，代表一种故障切换模型，即当出现故障时，空闲的备用部件接替失效的部件。在该模型中，备用部件采用心跳机制检测活跃部件的失效。高可用性的程度取决于部件状态的复制策略。对于活跃/备用模型，建议采用热备解决方案。热备解决方案既提供硬件冗余，也提供软件冗余。然而，活跃部件状态的任何变化均被复制到备用部件，即备用部件的状态总是最新的。在活跃部件失效的情况下，备用部件取代失效的部件，并根据当前的状态继续工作。

部件状态采用活跃复制进行拷贝，在活跃部件执行状态变化之前，采用提交协议将状态变化告知备用部件。只要活跃部件执行了状态变化，备用部件就会收到第二个报文来提交该状态变化。一旦故障切换，备用部件就能执行所有未提交的状态变化。提交协议是实现所特有的，超出了本建议书的范畴。

活跃/热备模型提供了在不中断服务情况下的连续可用性。

9.5.2 “1+N”（N>1）模型

“1+N”（N>1）模型是基于在一个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。

该模式的过程程序与“1+1”模型类似，备份部件采用心跳报文来检测活跃部件的失效，当活跃部件已经失效时，其中一个备份部件会接替该失效的部件。

9.6 数据同步方法

在保护切换出现的情况下，需要考虑数据同步。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，如策略信息库（PIB）。

9.6.1 “1+1”模式下的数据同步

在活跃部件（包括DPI节点、DPI引擎和DPI-FE）失效的情况下，备份部件会接替活跃部件的工作，备份部件需要发送‘规则同步请求’给管理实体。管理实体将发送规则数据给备份部件。

9.6.2 部件级“1+N”（N>1）模式下的数据同步

部件级“1+N”模式的数据同步与“1+1”模式类似。在活跃部件（包括DPI节点、DPI引擎和DPI-FE）失效的情况下，备份部件接替活跃部件的工作。备份部件需要发送‘规则同步请求’给管理实体，管理实体将发送规则数据给该备份部件。

9.6.3 节点级“1+N”（N>1）模式下的数据同步

节点级“1+N”（N>1）模式采用集群模式实现，在集群模式下，如果主节点失效，则备份节点接替主节点的工作，备份节点将会与来自管理实体的规则数据同步。

在从节点失效的情况下，经过失效节点的业务将由上游路由器根据负载均衡算法重新分配到其它的从节点。这些从节点将会被触发与来自管理实体的新规则同步。

10 运行机制描述

10.1 概述

本节描述了DPI技术的运行情况，包括以下方面：

- 所采用的DPI技术的目标；
- DPI系统部署的性能情况；
- 分析没有DPI的当前网络；
- DPI物理实体的部署以及建立相关的网络；
- DPI相关网络的操作、管理和维护；
- 根据对当前网络性能的监视，改变和改进当前的网络。

建立和运营一个具有DPI节点的网络的一般过程如图10-1所示。该图所示的6个步骤的功能见第10.3节至第10.8节的描述。

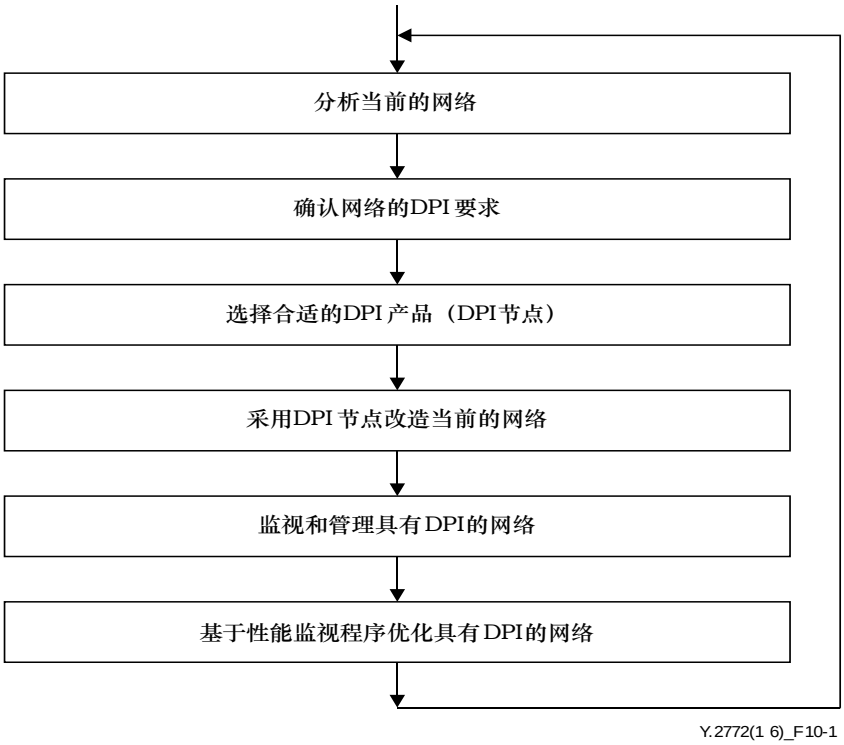

图10-1 – 图解建立和运营一个具有DPI节点的网络的过程

10.2 运行机制的目标

10.2.1 总体目标

采用DPI相关技术的总的目标包括以下三个方面：

1) 监视当前网络的状态；
2) 指导运营商改建和优化网络；
3) 提高网络性能。

10.2.2 具体目标

运行机制的具体目标可列举如下：

- 在不影响当前在线业务的情况下部署DPI节点；
- 监视活跃网络的所有类型的业务；
- 识别策略规则中规定的无效业务；
- 基于详细的网络性能监视来分析网络的状态；
- 基于网络状态分析重新分配网络资源；
- 基于网络状态改建并改进网络；
- 提高网络用户的满意度。

10.3 性能问题或DPI节点部署

原则上，DPI节点的部署不应中断当前的网络服务和应用，然而，当将DPI节点安装到网络中的时候，实际上可能会对网络服务和应用产生一些负面的影响。在安装之后，由DPI节点部署引入的负面影响应满足特定的要求。

10.3.1 路径外DPI节点部署技术要求

当将路径外的DPI节点插入到网络中时，当前网络服务和应用的中断时间应小于50毫秒，从理论上讲，可以在不中断服务和应用的情况下完成路径外DPI节点的部署。

10.3.2 路径上DPI节点部署技术要求

当将路径上的DPI节点插入到网络中时，当前网络服务和应用的中断时间应小于50毫秒，通过采用辅助的方法或者工具，可以达到50毫秒的目标。例如，在部署路径上DPI节点之前首先使用一条冗余链路，当路径上DPI节点能够正常工作时去掉该冗余链路。

10.4 当前网络分析

在部署一个DPI节点之前，需要获得关于当前网络的一些信息，例如，所有网络段的最大带宽，网络段活跃的平均业务量，网络段按日期和时间的业务量分布，部署一个DPI节点的影响程度。典型地，这些信息可以通过当前网络的NMS来采集。

通过分析该信息，可以获得构建具有DPI功能的网络的设计方案。

10.5 确认网络的DPI要求

基于以上对当前网络的分析，收集并确认对DPI节点的要求。

10.6 选择合适的DPI实体或系统

用于构建具有DPI功能的网络的DPI实体应满足第10.4节描述的要求。

10.7 使用DPI改造当前的网络

部署DPI设备不应降低当前网络的性能，尤其是不能影响在线业务。相比路径上的DPI物理实体，路径外的DPI物理实体能够更加方便地被设立，然而不合适的操作可能会影响业务。因此，应选择合适的时间和位置以使得上述的影响最小，时间和位置的选择应取决于网络在线业务。

需要强调一点，当将DPI节点部署在网络中并作为路径上的DPI节点工作时，它应支持内部旁路功能，图10-2描述的内部旁路功能，虚线表示旁路。当数据包流在旁路上传输时，相当于该DPI节点不在该网络中。换言之，对于数据包流，看来似乎是DPI节点之前的网络设备与该DPI节点之后的网络设备直接相连。

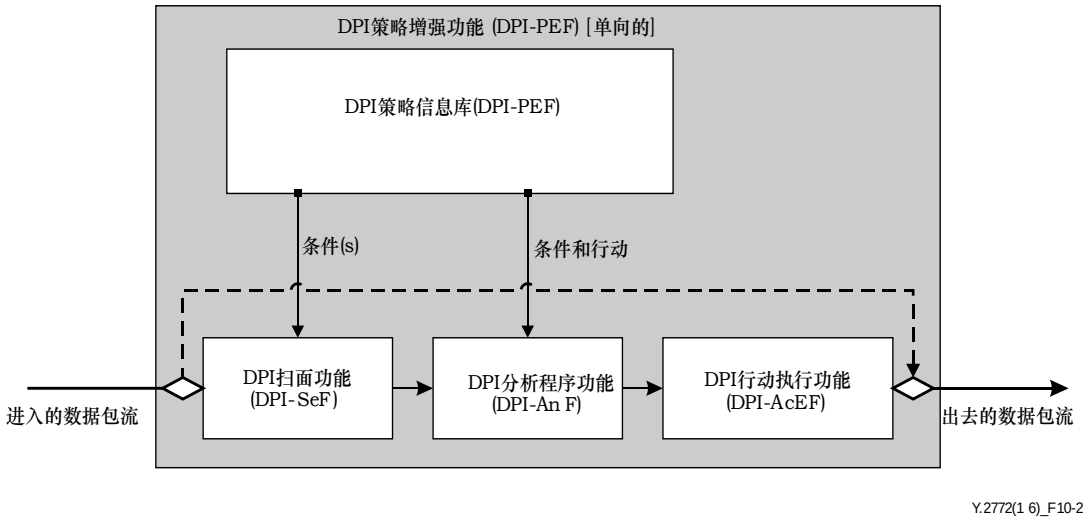

图10-2 – DPI节点的内部旁路功能

10.8 监视和管理具有DPI的网络

通常，包含了DPI功能的网络比没有DPI功能的网络更为复杂。因此，DPI网络应经常使用操作、管理和维护（OAM），即应该对DPI节点及其PIB进行维护和管理。

10.9 基于性能监视程序重建具有DPI的网络

通常，重建一个包括DPI功能的网络是一个自适应的过程。应基于网络性能状态的变化逐步地调整网络结构。监视网络状态取决于适当的数据和统计分析。

11 管理机制描述

11.1 DPI网络管理概述

正如任何一个典型的网元一样，DPI节点应支持配置、故障、性能和安全管理功能。这些管理功能已经在另外的建议书中进行了规定，超出了本建议书的范畴。然而，在这里确定了DPI网络管理应采取的一些特殊的考虑。

在双向DPI应用环境下，可以通过单一DPI节点（单一节点模式，见图11-1）或者一对DPI节点（双节点模式，见图11-2）来实现双向DPI功能，在一些情况下，双向节点模式比单一节点模式更为有利，例如，当需要对某些特殊的业务进行阻断时，使用双节点模式会更加容易阻断上述的特殊业务。

由于有可能两个相关的DPI节点在物理上是独立部署的，并且这些DPI节点的管理需要统一，因此管理将会更加复杂，原因是在这样的情况下网络管理应是子网级的，而不是节点级的。

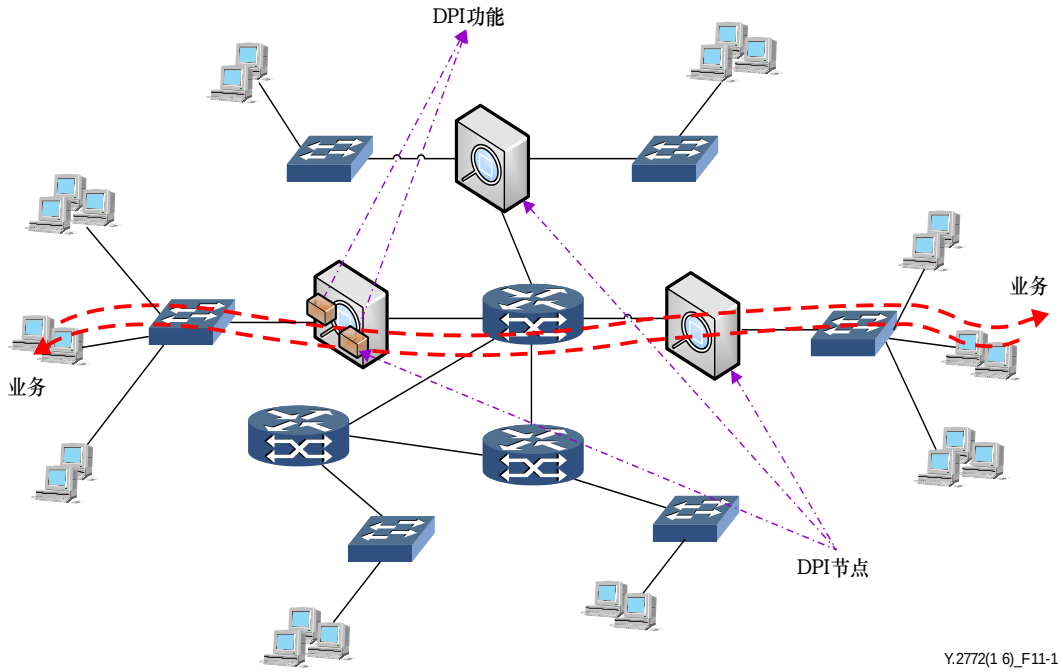

图11-1 – 由单个DPI节点（单一节点模式）实现双向DPI功能

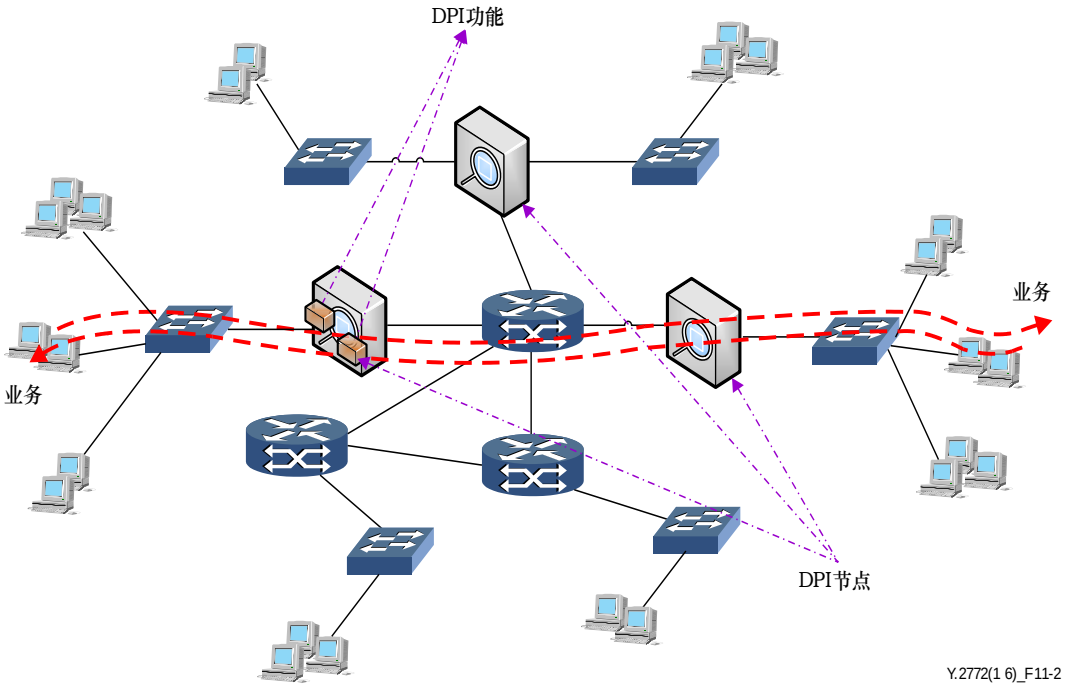

图11-2 – 由一对DPI节点（双节点模式）实现双向DPI功能

11.2 管理接口

11.2.1 单向DPI管理接口

单向DPI的一般管理如图11-3所示，其中DPI节点和网络管理系统（NMS）之间的连接不是一个物理上的直接连接，而是一个经过子网的逻辑连接。DPI节点和NMS之间的链路用该图中的虚线表示，在逻辑上，DPI节点和NMS之间的管理接口可以描述如下：

命令行接口（CLI）：NMS通过一个串口管理和控制DPI节点，通过一系列单行命令来实施管理行动。NMS只能同时管理一个在线DPI节点。

图形用户接口（GUI）：NMS通过以太网端口或者其它类型的物理端口管理和控制DPI节点，通过在DPI节点和该NMS之间交换一组协议数据包来实施管理行动。NMS能够同时管理一个或多个在线的DPI节点。

Telnet接口：NMS通过以太网端口或者其它类型的物理接口管理和控制DPI节点，通过一系列单行命令来实施管理行动。NMS只能同时管理一个在线DPI节点。

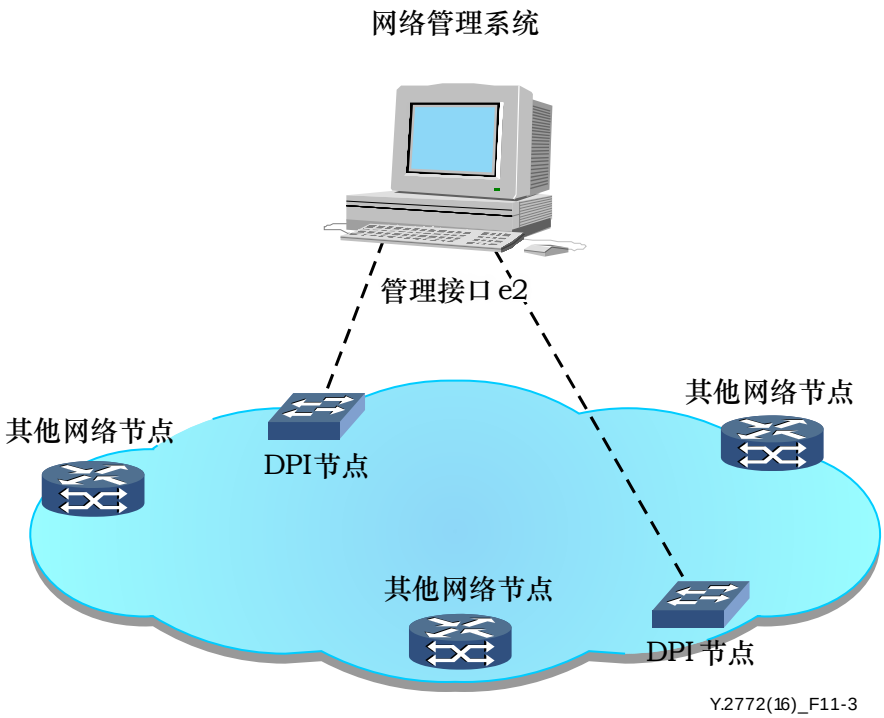

图11-3 – 单向DPI的网络管理

11.2.2 双向DPI管理接口

双向DPI的管理如图11-4所示。与单向DPI管理相比，双向DPI（见上面的图11-1和11-2）可能会更加复杂，原因是两个或多个DPI节点是相互依赖的。因此，无疑应该建立两个DPI节点之间的某些连接，这些连接不一定是物理上的直接连接，但可以是通过子网或者通过NMS的连接。这些链路用图11-4中的虚线表示，除了单向DPI管理接口以外，双向DPI管理中应使用以下管理接口：

接口e3（见图11-2）：两个相关DPI节点之间的、用于确保这两个DPI节点之间信息一致性并且保持这两个相关节点之间逻辑连接的接口。

在双向DPI应用情况下，基于一对DPI节点的协作实现双向DPI功能更为高效和经济，其中一个DPI节点负责一个方向的DPI功能，另一个节点负责相反方向的DPI功能。因此，两个DPI节点中的PIB应是相关的；一个DPI节点中PIB的变化应引起另一个DPI节点中PIB的相关改变。

例如，如果需要对网络设备A和B之间的业务实施双向DPI功能，则应在某一个DPI节点上设置与从A到B的数据流有关的策略控制规则，而在另一个DPI节点上配置与从B到A的数据流有关的策略控制规则。注意到网络管理系统只需要通知DPI节点，需要它们在A到B之间的业务上实现双向的DPI功能。这两个DPI节点上的PIB配置应由DPI节点自动地完成，因此，DPI节点之间的信息交换是必不可少的，并且是通过接口e3完成的。

此外，为了在DPI节点之间交换信息，应采用一些协议让DPI节点连接起来，并且还通过接口e3传送协议数据包。

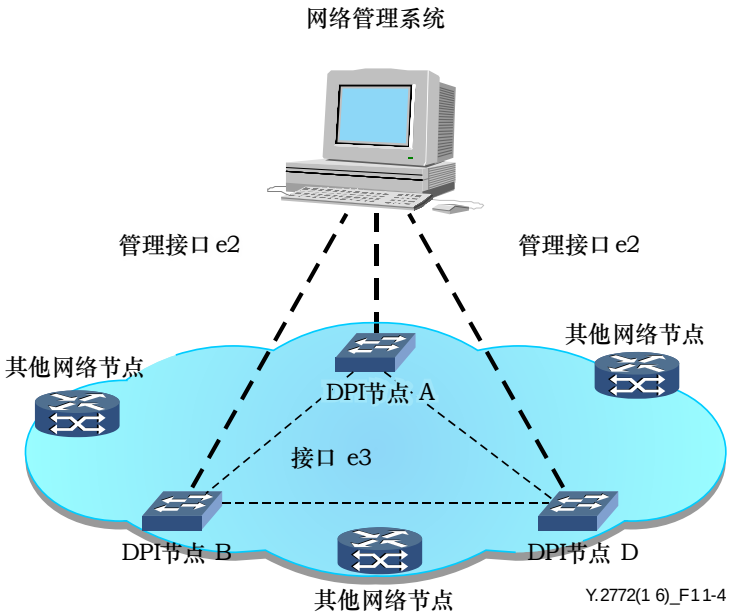

图11-4 – 双向DPI的网络管理

11.3 管理协议和功能

NMS和DPI节点或者DPI子网之间的管理协议可能是简单网络管理协议（SNMP）、通用管理信息协议（CMIP）或者任何其他的管理协议。

管理功能包括传统的配置管理、告警管理和性能管理，此外，NMS应采用双向的DPI子网PIB维护功能。

12 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。

参考资料

[b-ITU-T X.200] ITU-T X.200建议书 (07/1994)，信息技术 – 开放系统互连 – 基本参考模型：基本模型。

[b-ITU-T X.680] ITU-T X.680建议书 (08/2015)，信息技术 – 抽象语法标记1(ASN.1):基本标记的规范。

[b- ITU-T Y.sup25] ITU-T Y.sup25增补 (2015)，关于DPI用例和应用情况的增补。

[b-IETF RFC 3198] IETF RFC 3198 (2001), 基于策略的管理所用术语。

[b-IETF RFC 5101] IETF RFC 5101 (2008), IP业务流信息交换的IP流信息导出（*IPFIX*）协议的规范。

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	视听和多媒体系统
I系列	综合业务数字网
J系列	有线网和电视、声音节目和其他多媒体信号的传输
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
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	测量设备技术规程
P系列	电话传输质量、电话装置、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	数据网和开放系统通信及安全
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**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2016年，日内瓦