International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2772

(04/2016)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Next Generation Networks – Security

Mechanisms for the network elements with support of deep packet inspection

Recommendation ITU-T Y.2772

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	**Y.2700–Y.2799**
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2772

Mechanisms for the network elements with support of deep packet inspection

Summary

Recommendation ITU-T Y.2772 provides mechanisms for the network elements supporting deep packet inspection (DPI), including the procedures and methods aspects of deep packet inspection (DPI) with respect to packet based networks. This Recommendation serves to assist in the understanding of DPI related methods, interfaces, protocols, procedures aspects and process aspects of DPI-related products.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2772	2016-04-29	13	11.1002/1000/12709

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.2772

Mechanisms for the network elements with support of deep packet inspection

1 Scope

This Recommendation provides the implementation mechanisms for deep packet inspection (DPI) in packet based networks. The primary purpose of this Recommendation is to describe the application models, related protocols, interface, methods procedure and process of DPI that can be used to identify information flows between DPI functions and other network functions.

The scope of this Recommendation includes:

– definition of DPI mechanism;

– overview of DPI mechanisms in support of application identification;

– procedures and information flows in operational aspect;

– procedures and information flows in management aspect, such as DPI policy management;

– other procedures and information flows for possible DPI functional entity (FE) interfaces.

The following are out of the scope of this Recommendation:

– operational and management aspects that are not specific to DPI entities;

– common network element related management functions, as already specified by the ITU-T M-series and ITU-T X-series Recommendations.

Implementers and users of this Recommendation shall comply with all applicable national and regional laws, regulations and policies. The mechanism described in this Recommendation may not be applicable to international correspondence in order to ensure the secrecy and sovereign national legal requirements placed upon telecommunications providers, as well as the ITU Constitution and Convention.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2011), *Resource and admission control functions in next generation networks*.

[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*.

[ITU-T Y.2771] Recommendation ITU-T Y.2771 (2014), *Framework for deep packet inspection*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 deep packet inspection (DPI) [ITU-T Y.2770]: Analysis, according to the layered protocol architecture OSI-BRM [b-ITU-T X.200], of:

– payload and/or packet properties (see list of potential properties in clause 3.2.11 of [ITU-T Y.2770] deeper than protocol layers 2, 3 or 4 (L2/L3/L4) header information, and

– other packet properties

in order to identify the application unambiguously.

NOTE – The output of the DPI function, along with some extra information such as the flow information, is typically used in subsequent functions such as reporting or actions on the packet.

3.1.2 DPI analyser [ITU-T Y.2771]: A subsequent entity in the DPI processing path (within a DPI policy enforcement function) with focus on comparison functions between the particular packet headers and payloads of preselected packet flows. The primary scope of the DPI analyser is related to the evaluation of DPI policy *conditions* against *preselected* incoming packets.

NOTE – The DPI analyser may be located after a DPI scanner (see clause 3.2.5 of [ITU-T Y.2771]). The DPI analyser may provide the functionality of an intrusion detection system (IDS) analyser.

3.1.3 DPI engine [ITU-T Y.2770]: A subcomponent and central part of the DPI functional entity which performs all packet path processing functions (e.g., packet identification and other packet processing functions in Figure 6-1 of [ITU-T Y.2770]).

3.1.4 DPI node [ITU-T Y.2771]: A network element or device that realizes the DPI related functions. It is thus a generic term used to designate the realization of a DPI physical entity.

NOTE – Functional perspective: the DPI node function (DPI-NF) comprises the DPI policy enforcement function (DPI-PEF) and the (optional) local policy decision function (L-PDF); the DPI-NF is functionally equal to the DPI functional entity.

3.1.5 DPI policy action (action in short) [ITU-T Y.2771]: Definition of what is to be done to enforce a policy rule, when the conditions of the rule are met. Policy actions may result in the execution of one or more operations to affect and/or configure network traffic and network resources (see also [b-IETF RFC 3198]).

3.1.6 DPI policy condition (also known as DPI signature) [ITU-T Y.2770]: A representation of the necessary state and/or prerequisites that identifies an application and define whether a policy rule's actions should be performed. The set of DPI policy conditions associated with a policy rule specifies when the policy rule is applicable (see also [b-IETF RFC 3198]).

A DPI policy condition must contain application level conditions and may contain other options such as state conditions and/or flow level conditions:

1) State condition (optional):
   a) network grade of service conditions (e.g., experienced congestion in packet paths); or
   b) network element status (e.g., local overload condition of the DPI-FE).
2) Flow descriptor/flow level conditions (optional):
   a) packet content (header fields);
   b) characteristics of a packet (e.g., number of MPLS labels);
   c) packet treatment (e.g., output interface of the DPI-FE);
3) Application descriptor/application level conditions:
   a) packet content (application header fields and application payload).

NOTE – The condition relates to the "simple condition" in the formal descriptions of flow level conditions and application level conditions.

3.1.7 DPI scanner (also used as "DPI scan function") [ITU-T Y.2771]: The first entity in the DPI processing path (within a DPI policy enforcement function) which provides a pre-selection (related to the subsequent DPI analyser, see clause 3.2.1 of [ITU-T Y.2771]) by checking *all* DPI policy *conditions* against *all* incoming packets.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BRAS	Broadband Remote Access Server
CLI	Command Line Interface
CMIP	Common Management Information Protocol
DPI	Deep Packet Inspection
DPI-PDFE	DPI Policy Decision Functional Entity
DPI-PIB	DPI Policy Information Base
EMS	Element Management System
GUI	Graphical User Interface
IP	Internet Protocol
IPFIX	IP Flow Information Export
LAN	Local Area Network
L-PDF	Local PDF
NMS	Network Management System
OAM	Operation, Administration and Management
PDF	Policy Decision Function
PIB	Policy Information Base
SNMP	Simple Network Management Protocol
SR	Service Router
TCAM	Ternary Content-Addressable Memory
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

5 Conventions

None.

6 Definition of DPI mechanism

In this Recommendation, the term "mechanism" is considered to include the means, methods, processes and procedures to realize some function or meet some requirement. With this consideration in mind, a DPI mechanism can be described as follows:

- concrete process that can be used to carry out the functions and capabilities defined in [ITU-T Y.2771] and requirements defined in [ITU-T Y.2770];
- detailed procedure that can be adopted to realize the functions and capabilities defined in [ITU-T Y.2771] and requirements defined in [ITU-T Y.2770];
- proper methods that can be made use of to achieve the functions and capabilities defined in [ITU-T Y.2771] and requirements defined in [ITU-T Y.2770];
- specialized tools or means that can be assisted by to achieve the functions and capabilities defined in [ITU-T Y.2771] and requirements defined in [ITU-T Y.2770].

7 Overview of DPI mechanisms in support of application identification

7.1 General aspect of DPI mechanisms

The DPI mechanisms include two main aspects:

- DPI mechanisms relative to the DPI node;
- DPI mechanisms corresponding to the network supporting the DPI functions.

Before specifying these two aspects, it is necessary to introduce the basic structure of the DPI node and the typical network supporting DPI functions.

7.2 Basic structure of a DPI node

The basic structure of a DPI node has been described in Figure 6-1 of [ITU-T Y.2770] and Figure 7-2 of [ITU-T Y.2771]; the realization of a DPI node can be based on the structure.

7.3 Typical network supporting DPI functions

A typical network deployed with DPI nodes is described in Figure 7-1, where, from top to bottom, the five logical layers include: cloud, core layer, aggregate layer, access layer and terminal layer. It should be emphasized that a logical link exists between every DPI node and element management system (EMS) or network management system (NMS), though not all logical links are illustrated in Figure 7-1. All DPI nodes can cooperate with the network entities (such as router, switch and broadband remote access server (BRAS), etc.) and the DPI nodes in Figure 7-1 are independent of the above network entities.

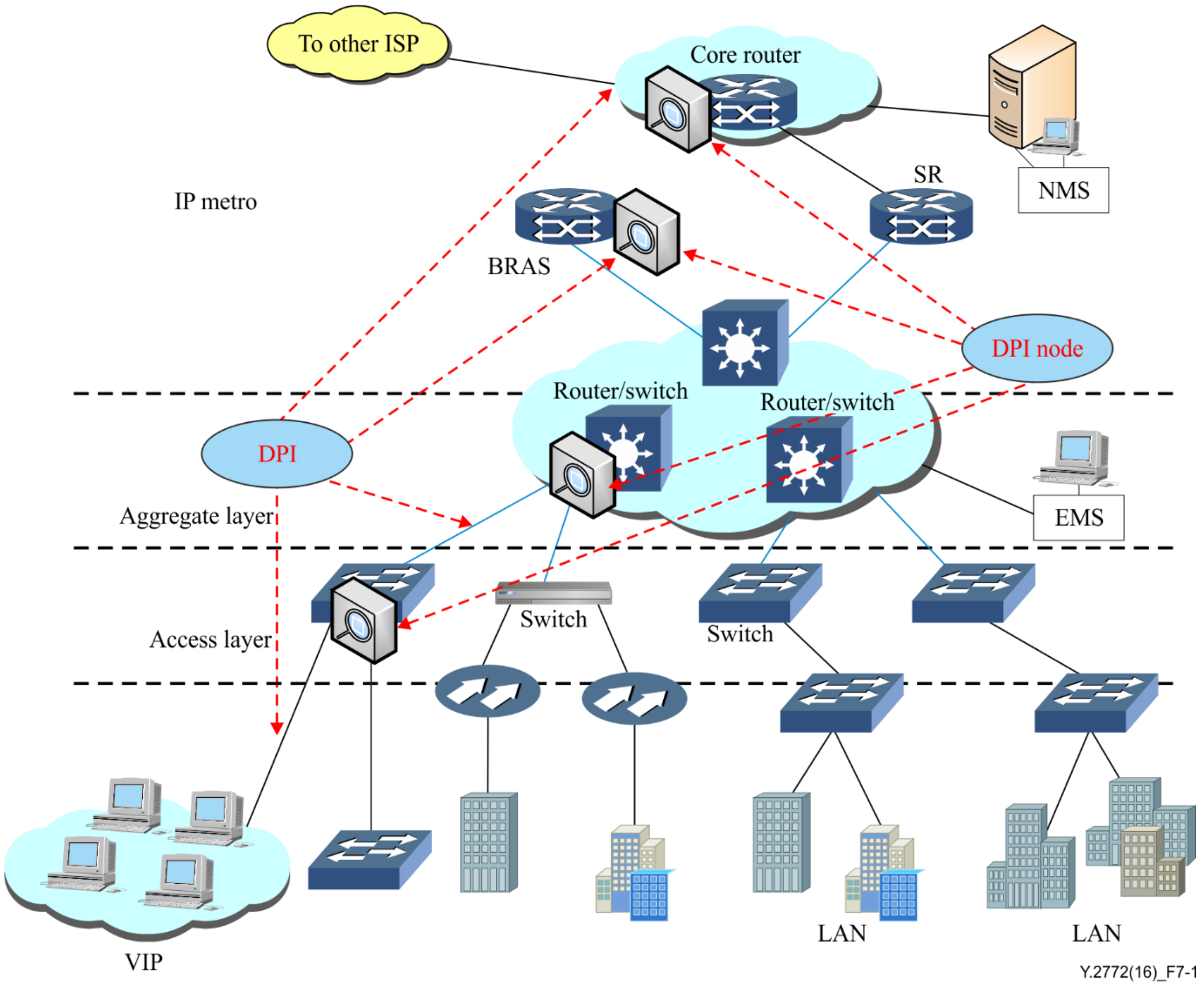


Figure 7-1 – An example network topology deployed with DPI nodes

For more information, see the example DPI applied network given in Figure 6-3 of [b-ITU-T Y-Sup.25].

7.4 DPI mechanism related to the DPI node

The DPI mechanism of the DPI node mainly includes the following three aspects:

1) Information representation method

A network element that supports DPI functions has various kinds of information and data to be represented in the element, for example, the DPI rules. The information representation method is very important to the network element; different representation methods bring about different processing efficiencies.

2) Processing methods and procedures

Processing methods and procedures include instructive methods for the realization of the DPI relative functions and as well as the procedures that a network element executes in supporting these DPI functions.

3) Interface and proper protocol

Interface and proper protocol include the realization of the interfaces that are defined in [ITU-T Y.2770] (e.g., e1, e2) as well as the appropriate protocol used for exchanging information between the above kinds of interface.

7.5 The mechanism of a network deployed with DPI nodes

The mechanism corresponding to the networks supporting DPI functions mainly including the following aspects:

- operation aspects;
- management aspects.

8 Representation methods of the DPI – Policy rule of DPI-PIB

8.1 Overview

The DPI policy rule condition of DPI policy information base (DPI-PIB) is one of the core parts of a DPI node, and almost all actions of the DPI node are based on DPI policy rule conditions. Therefore, it is very important that the DPI policy rule condition is represented effectively and is easy to process. Three DPI policy rule condition representation methods are described: data and mask representation method, regular express representation method and hybrid representation method.

8.2 Data and mask representation method for DPI policy rule conditions

The IP address and mask representation method is usually used in TCP/IP protocol stack and related network devices; the data and mask representation method is similar to the IP address and mask representation method. In the data and mask method, a byte string (data) is used to represent the tagged word that identifies a certain data flow, and a bit string (mask) corresponding to the byte string is used to be decide whether a certain bit of the byte string should be checked or not. Generally, if a mask bit is '1', the corresponding bit of the byte string is not checked. Conversely, if a mask bit is '0', then the corresponding bit of the byte string requires checking.

For the DPI-PIB, it is appropriate to use the data and mask representation method, which has the following advantages:

- simple and easy to understand;
- high efficiency, a single item can be shared by a many data flows;
- matches well with the common used devices such as ternary content-addressable memory (TCAM).

The following two examples illustrate the data and mask representation method:

1) Match the data flows whose TCP source port range from 0x2100 to 0x21ff

In the DPI-PIB, only one item is needed in order to meet the requirement:

Item1: data: 0x2100, mask: 0x00ff

2) Match the data flows whose virtual local area network (VLAN) is in the set 16-63

In the DPI-PIB, two items are needed to meet the requirement:

Item1: data: 0x0010, mask: 0x000f

Item2: data: 0x0020, mask: 0x001f

8.3 Regular expression representation method for DPI policy rule conditions

The data and mask representation method is appropriate to represent a tagged word with a fixed position and determinate value. Generally, layer 2 through layer 4 (L2-L4) protocol headers match this type of request very well.

However, tagged words of high layer applications are usually uncertain and easy to change. Under such circumstance, using the data and mask representation method is hard to implement. In these applications, the regular express representation method is more appropriate for those kinds of tagged words.

A regular expression [b-ITU-T X.680] is a well-known description method in computer science; the detailed presentation and analysis of regular expressions is outside the scope of this Recommendation.

The following two examples illustrate the regular expression representation method:

1) Match the data flow that includes the word "Bittorrent" or "Bitcomment"

In the DPI-PIB, only one item is needed in order to meet the requirement:

Item1: "/Bit(torrent|comment)/"

2) Match the data flow that includes the word "Worm" where the following word is not "v1" or "v2"

In the DPI-PIB, only one item is needed in order to meet the requirement:

Item1: "Worm(?<!v1|v2)"

8.4 Hybrid representation method for DPI policy rule conditions

DPI functions can take effect on layer 2-layer 7. When considering layer 2-layer 4, the uses of the data and mask representation method is a good choice in order to construct the DPI-PIB. On the other hand, when considering the use of tagged words in Layer 7, the regular expression representation method is a better choice for constructing the DPI-PIB.

Therefore, it is useful to combine the above two representation methods for many application environments; this is called the hybrid representation method. In this method, some tagged words are represented through the data and mask representation method while the other tagged words are represented based on the regular expression representation method.

The following example illustrates the hybrid representation method:

1) Match the data flow that includes the word "Bittorrent" or "Bitcomment" and where the VLAN of the data flow is in the set 8-15

In the DPI-PIB, only one item is needed in order to meet the requirement:

Item1: First half: data: 0x0008, mask: 0x0007

Second half: "/Bit(torrent|comment)/"

These two halves can be stored in different memory but they are logically connected to each other.

9 Information flows, processing procedures and methods for a DPI entity

9.1 Overview

A DPI entity includes many necessary functions and the realization of these functions rely on many aspects as follows:

- realization of some necessary interfaces (see clause 9.2);
- design of information flow between function components (see clause 9.3);
- processing procedures of the main function components (see clause 9.4);
- methods to reinforce reliability (see clause 9.5);
- methods to realize information exchange and data synchronization efficiently (see clause 9.6);
- other methods beneficial to the realization of the DPI entity

9.2 Interface realization

9.2.1 Overview of the interface

Several interfaces are defined and illustrated in [ITU-T Y.2770], including external interfaces e1and e2 and internal interfaces i1, i2 and i3. Among these interfaces, external interfaces e1 and e2 are illustrated in Figure 8-1 of [ITU-T Y.2770] and the internal interfaces i1, i2 and i3 are specified in Figure 8-2 of [ITU-T Y.2770]. All of these interfaces should theoretically be carried out within a DPI node.

However, other interfaces should also be realized based on application requirements. For example, under the bidirectional DPI context, the special external interface e3 (see Figure 11-4) may be needed within a DPI node.

9.2.2 Internal interfaces

Internal interfaces (see Figure 8-2 of [ITU-T Y.2770]) are used to exchange information between internal function components within a DPI node. There are three internal interfaces: i1, i2 and i3. The realizations of these internal interfaces are introduced in the following clauses.

9.2.2.1 The i1 interface

The internal interface i1 is an interface between the packet identification function and other packet processing functions within a DPI-FE. Generally, the i1interface is a physical interface realized by hardware in order to guarantee the handling performance of a DPI node. The i1 interface can be realized by various methods, including shared memory, internal parallel communication ports and internal serial communication ports, etc.

9.2.2.2 The i2 interface

The internal interface i2 is an interface between the packet identification function and the local management function within a DPI-FE. The i2 interface is a logical interface realized by software, and there are several methods to design the i2 interface.

If the packet identification function and local management function are executed, controlled or managed by an identical CPU, then the i1 interface can be realized by various methods such as a group of application programming interface (API) functions, shared memory and inter-process communication.

If the packet identification function and local management function are executed, controlled or managed by different CPUs, then the i1 interface can be realized by data communication methods. For example, the above two function components may exchange information through TCP or UDP.

9.2.2.3 The i3 interface

The internal interface i3 is an interface between DPI signature library and local management function within a DPI-FE. The i3 interface is a logical interface realized by software. Generally, the DPI signature library and local management function are designed to be controlled by an identical CPU, and the i3 interface can be realized by a group of API functions.

9.2.3 External interface

External interfaces (see Figure 8-1 of [ITU-T Y.2770]) are used to exchange information between a DPI node and the other functional entities such as NMS. There are also three external interfaces: e1, e2 and e3. The external interfaces e1 and e2 are illustrated in Figure 8-1 of [ITU-T Y.2770] and the external interface e3 is depicted in Figure 11-4 of this Recommendation. The realization of these external interfaces are specified in clauses 9.2.3.1 to 9.2.3.3.

9.2.3.1 The e1 interface

The external interface e1 is an interface between a DPI policy decision functional entity (DPI-PDFE) and a DPI functional entity (DPI-FE). [ITU-T Y.2770] provides a solution to realize the interface: the e1 interface can optionally be an Rw reference point interface as defined in [ITU-T Y.2111]. While Rw is a feasible solution, it is not unique nor mandatory.

No matter which solution is adopted to design the e1 interface, it should be guaranteed that the data transported through the interface can be understood by both the DPI-PDFE and the DPI-FE, even if the DPI-PDFE and the DPI-FE are not designed by an identical vendor.

9.2.3.2 The e2 interface

The external interface e2 is an interface between a DPI-FE and a remote network entity other than the DPI-PDFE (e.g., an NMS). [ITU-T Y.2770] also provides a solution to realize the interface: the e2 interface is recommended to use the IP flow information export (IPFIX, see [b-IETF RFC 5101])-based export protocols. While the IPFIX based export protocols can be used by the e2 interface, information exchanged between a DPI-FE and a remote network entity other than the DPI policy decision functional entity (DPI-PDFE) is also possible with other solutions.

No matter which kind of solution is adopted to design the e2 interface, it should be guaranteed that the information passed through the interface can be understand by both of the remote network entity and the DPI-FE no matter that the remote network entity and the DPI-FE belong to an identical vendor or not.

9.2.3.3 The e3 interface

The external interface e3 is an interface between two independent DPI-FEs when it is necessary to meet bidirectional DPI application requirements. Detailed specification of this interface is given in clause 11.

9.3 Information flow

9.3.1 DPI engine oriented information flow

Figure 9-1 depicts the information flow originated from the DPI engine. The data exchange between the DPI engine and the local policy decision function (L-PDF) is within the DPI entity, meanwhile the data exchange between the L-PDF and the PD-FE is outside the DPI entity.

Data exchange related to DPI should be very reliable. On the other hand, data communication within a DPI entity is more reliable than data communication between two independent entities. Therefore, it is better to use connection-based approaches for data exchange between two independent entities in order to guarantee reliability of data exchange, and data exchange within a DPI entity can be connectionless to reduce system resources and improve the efficiency of data exchange.

Thus, in Figure 9-1, data exchange between DPI-engine and L-PDF is recommended to be designed as connectionless mode because the DPI engine and L-PDF are in a single DPI entity. However, data exchange between L-PDF and PD-EF is recommended to be designed as connection-based mode because PD-FE is not in a single DPI entity.

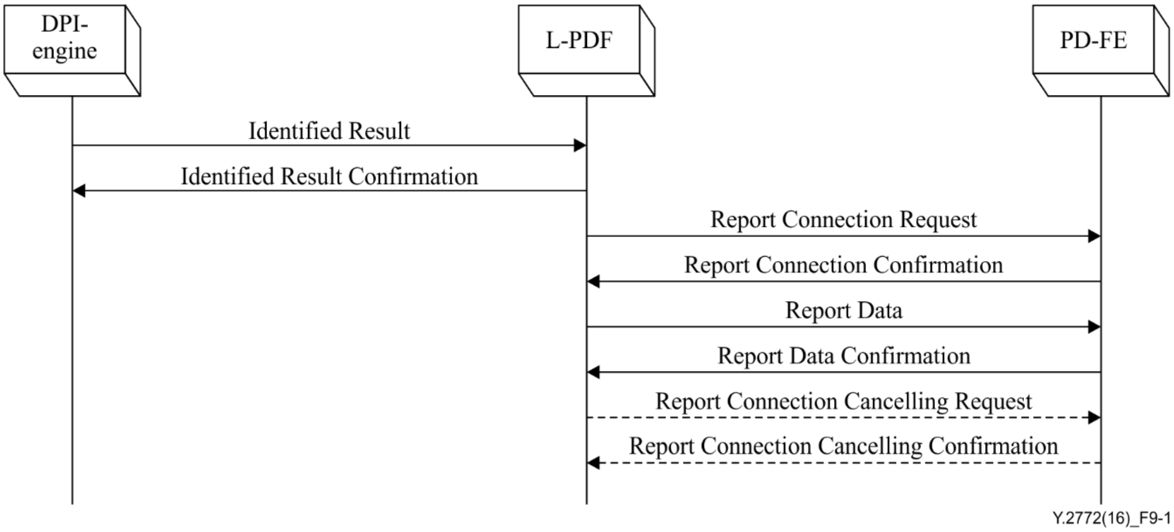

DPI-engine
L-PDF
PD-FE
Identified Result
Identified Result Confirmation
Report Connection Request
Report Connection Confirmation
Report Data
Report Data Confirmation
Report Connection Cancelling Request
Report Connection Cancelling Confirmation
Y.2772(16)_F9-1

Figure 9-1 – DPI-engine oriented information flow

In Figure 9-1, the primitive "Identified Result" is used to transport data generated by a DPI-engine, and the primitive "Identified Result Confirmation" is used to tell the DPI-engine that the above data have been received. The primitive couple "Report Connection Request" and "Report Connection Confirmation" is used to establish a connection, and the primitive couple "Report Data" and "Report Data Confirmation" are used to transport reported data. After finishing the exchange of all reported data, the primitive couple "Report Connection Cancelling Request" and "Report Connection Cancelling Confirmation" is optionally used to remove the connection (represented by dashed line in Figure 9-1).

9.3.2 DPI-PIB oriented information flow

Figure 9-2 depicts the information flow based on DPI-PIB. The data exchange between the DPI-PIB and the L-PDF is within the DPI entity, and the data exchange between the L-PDF and the PD-FE is beyond the DPI entity.

In Figure 9-2, data exchange between DPI-PIB and L-PDF is recommended to be designed as connectionless mode, and data exchange between L-PDF and PD-EF is recommended to be designed as connection-based mode.

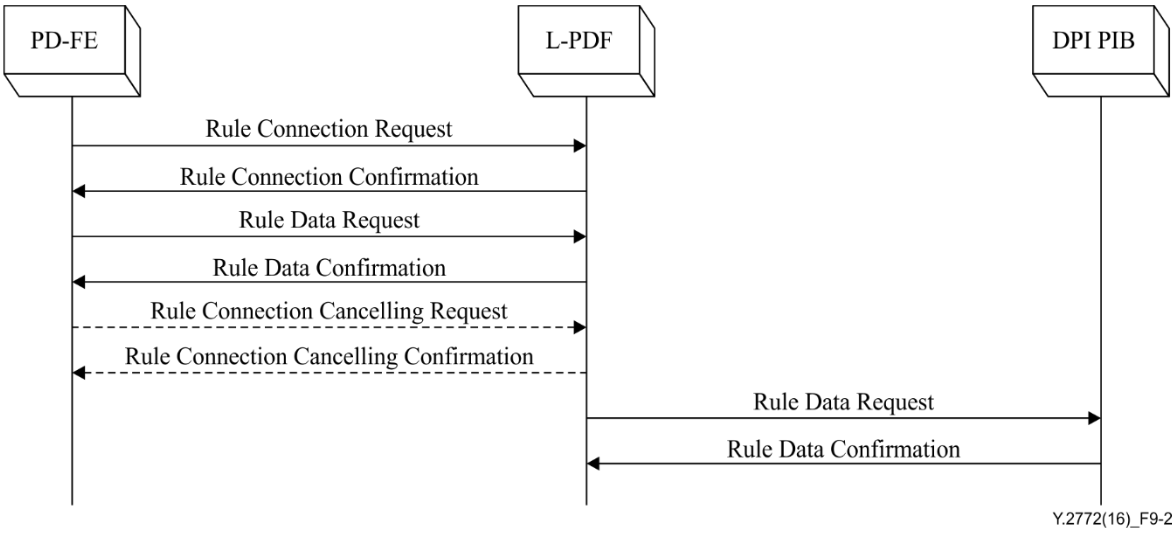


Figure 9-2 – DPI-PIB oriented information flow

In Figure 9-2, the primitive couple "Rule Connection Request" and "Rule Connection Confirmation" is used to establish a connection, and another primitive couple "Rule Data Request" and "Rule Data Confirmation" is used to transport rule data. After finishing the exchange of all rule data, the primitive couple "Rule Connection Cancelling Request" and "Rule Connection Cancelling Confirmation" is optionally used to remove the connection (represented by a dashed line in Figure 9-2).

9.3.3 DPI L-PDF oriented information flow

Figure 9-3 depicts the DPI L-PDF oriented information flow. Both the data exchange between the L-PDF and the PD-FE and the data exchange between the L-PDF and the Management Entity are outside the DPI entity.

In Figure 9-3, among the three functional components including PD-FE, L-PDF and Management Entity, no two components belong to a single entity. Therefore, mutual data exchange is recommended to be designed as connection-based mode.

In Figure 9-3, four primitive couples (including "Rule Connection Request" and "Rule Connection Confirmation", "Rule Synchronization Connection Request" and "Rule synchronization Connection Confirmation", "Report Connection Request" and "Report Connection Confirmation", and "Config Connection Request" and "Config Connection Confirmation") are used to establish a corresponding connection. Meanwhile, four other primitive couples (including "Rule Data Request" and "Rule Data Confirmation", "Rule Data Request" and "Rule data Confirmation", "Report Data Request" and "Report Data Confirmation", "Config Data Request" and "Config Data Confirmation") are used to transport corresponding data. In addition, corresponding to every type of connection, after finishing the exchange of all corresponding data, the primitive couple "… Connection Cancelling Request" and "… Connection Cancelling Confirmation" is optionally used to remove the connection. These last-mentioned primitive couples are not depicted in Figure 9-3 to reduce complication and avoid confusion in the figure, however, they have similar functions as the primitive couple "Rule Connection Cancelling Request" and "Rule Connection Cancelling Confirmation".

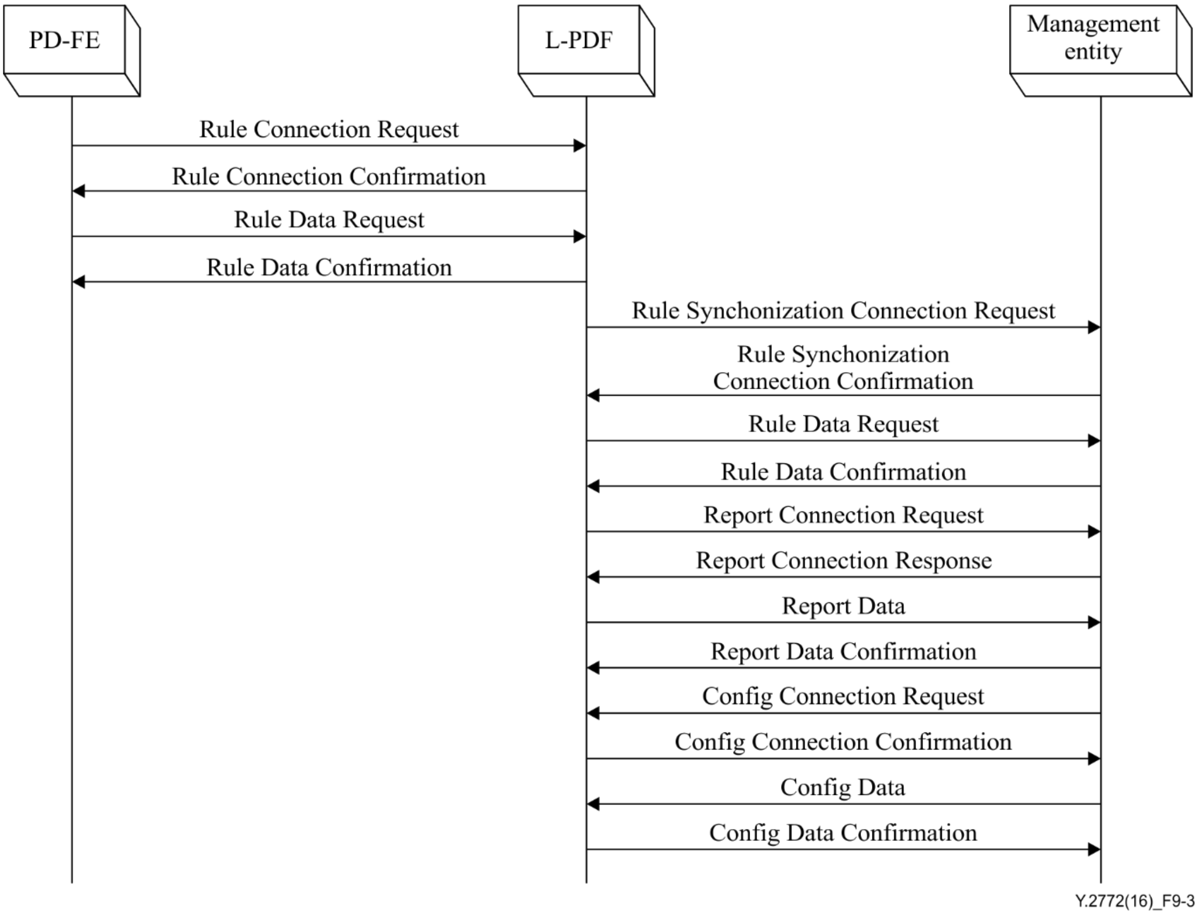

PD-FE
L-PDF
Management entity
Rule Connection Request
Rule Connection Confirmation
Rule Data Request
Rule Data Confirmation
Rule Synchonization Connection Request
Rule Synchonization Connection Confirmation
Rule Data Request
Rule Data Confirmation
Report Connection Request
Report Connection Response
Report Data
Report Data Confirmation
Config Connection Request
Config Connection Confirmation
Config Data
Config Data Confirmation
Y.2772(16)_F9-3

Figure 9-3 – L-PDF oriented information flow

9.4 Process procedure

9.4.1 DPI-engine process procedure

When a packet enters into the DPI-engine, the DPI-engine scans and identifies the packet according the policy rule defined in DPI-PIB. Then analyser of DPI-engine analyses the identified packet, and records the analysed result. After that, the policy action will be executed according the identified result.

If the packet is not identified, the 'non-identified' action will be performed. If the packet is identified, DPI-engine will execute the corresponding action according to the policy rule defined in DPI-PIB.

Meanwhile, DPI-engine records the identified result of each packet, and caches several similar results. It reports the results to the management entity periodically. The report period is specific to realization, and is outside of the scope of this Recommendation.

9.4.2 DPI-PIB process procedure

DPI-PIB contains a set of one or multiple DPI policy rule entries. DPI-PIB receives rule data from L-PDF after L-PDF received rule data from PD-FE.

9.4.3 L-PDF process procedure

The L-PDF updates the rule entries for the DPI-PIB when it receives rule data from remote policy decision function(s) (PDF(s)). The L-PDF send identified result to remote PDF(s) when it receives identified result from DPI-engine. The L-PDF may be also responsible for resolving possible rule interaction problems between the set of DPI policy rules.

9.5 Protection method

[ITU-T Y.2771] has defined "1+N" redundancy group to realize the fault tolerance. There are two distinct protection models: the "1+1" (N=1) model and the "1+N" (N>1) model. The "1+1" model is used for one active component and one standby component, while the "1+N" (N>1) model is used for one active component and N standby components.

9.5.1 "1+1" model

The "1+1" model is also called the active/standby model and represents a kind of failover model where, in case of a failure, an idle standby component takes over for the failed component. In this model, the standby component uses a heartbeat mechanism to detect the failure of the active component. The level of high-availability depends on the replication strategy for component status. For an active/standby model, the hot-standby solution is recommended to be used. A hot-standby solution provides hardware redundancy as well as software redundancy. However, the status of the active component is replicated to the standby component on any change, i.e., the status of the standby component is always up-to-date. In case of a failure of the active component, the standby component replaces the failed component and continues to operate based on the current status.

Component status is copied using active replication. A commit protocol is used to announce status changes to the standby component before they are executed at the active component. Once executed, the standby component receives a second message to commit the status change. Any uncommitted status changes are executed by the standby component upon failover. The commit protocol is specific to realization, and is outside of the scope of this Recommendation.

The active/hot-standby model offers continuous availability without any interruption of service.

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

The "1+N" (N>1) model is based on multiple redundant component, and more than two DPI components (in other words, a DPI "1+N" redundancy group of which the DPI components are the functional components) are designed within a DPI node, and one DPI component works as the active component while the other DPI components operate as backup components.

The process procedures of this mode is similar to the "1+1" model. The backup components use heartbeat messages to detect the failure of active component. When the active component has failed, one of backup components takes over the failed component.

9.6 Data synchronization method

Data synchronization needs to be considered in case protection switchover occurs. The active functional components and the backup functional components are recommended to keep totally identical information such as policy information base (PIB) through a data synchronization method.

9.6.1 Data synchronization in "1+1" mode

In case of the active component (including DPI-node, DPI-engine and DPI-FE) failure, the backup component takes over the work of the active component. The backup component needs to send 'Rule Synchronization Request' to the management entity. The management entity will send the rule data to the backup component.

9.6.2 Data synchronization in component level "1+N" (N>1) mode

The data synchronization in component level "1+N" mode is similar with "1+1" mode. In case of active component (including DPI-node, DPI-engine and DPI-FE) failure, the backup component takes over the work of active component. The backup component needs to send 'Rule Synchronization Request' to the management entity. The management entity will send the rule data to the backup component.

9.6.3 Data synchronization in node level "1+N" (N>1) mode

The node level "1+N" (N>1) mode is realized using cluster mode. In cluster mode, if the master node fails, the backup node takes over the work of master node. The backup node will synchronize the rule data from management entity.

In case of slave node failure, the traffic passed to the failed node will redistribute to the other slave nodes by upstream routers according the load balance algorithm. These slave nodes will be triggered to synchronize the new rules from the management entity.

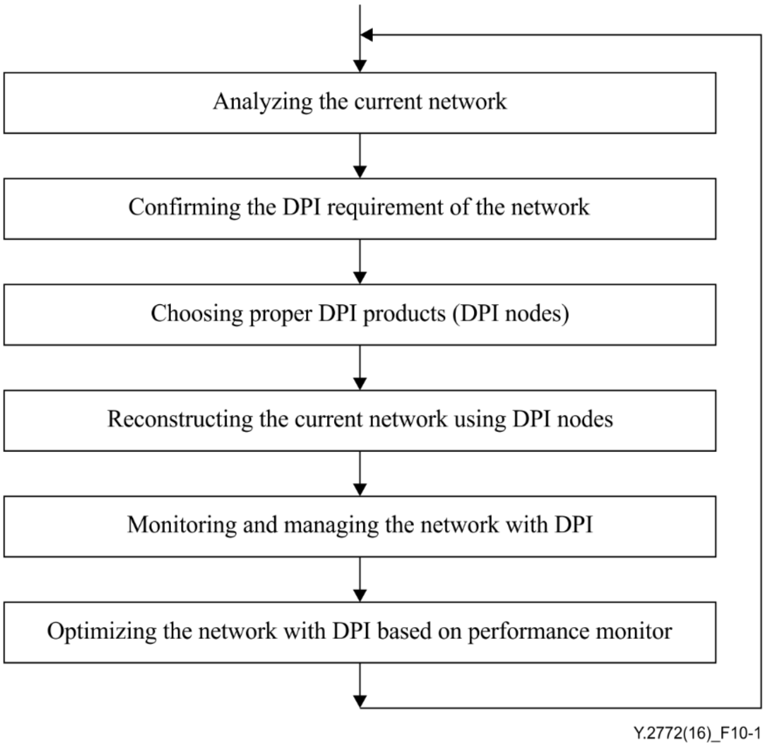
10 Operational mechanism specification

10.1 Overview

This clause depicts operational aspects of DPI technologies, including the following aspects:

- goals of adopted DPI technology;
- performance aspect of DPI system deployment;
- analysis of the current networks without DPI;
- deployment of DPI physical entities and setting up relative networks;
- operation, administration and maintenance of the DPI relative networks;
- changing and improving current networks based on monitoring performance of the current networks.

The general process to build and operate a network with DPI nodes is depicted in Figure 10-1. The functions of the six steps depicted in the figure are described in clauses 10.3 to 10.8.



Analyzing the current network

Confirming the DPI requirement of the network

Choosing proper DPI products (DPI nodes)

Reconstructing the current network using DPI nodes

Monitoring and managing the network with DPI

Optimizing the network with DPI based on performance monitor

Figure 10-1 – Illustrating the process to build and operate a network with DPI nodes

10.2 Objectives of the operation mechanism

10.2.1 Overall objective

The general objectives for applying DPI relative technologies include the following three aspects:

1) monitoring the status of the current network;
2) instructing operators to rebuild and optimize network;
3) improving the network performance.

10.2.2 Specific objectives

The specific objectives of operation mechanism can be listed as follows:

- deploying DPI nodes without influencing current on-line service;
- monitoring all kinds of traffic of the active network;
- identifying the invalid traffic defined in policy rules;
- analysing the status of the network based on detail network performance monitoring;
- reallocating network resources based on network status analysing;
- rebuilding and improving network based network status;
- improving the satisfaction level of network users.

10.3 Performance aspect or DPI nodes deployment

In principle, the deployment of DPI nodes should not interrupt the current network services and applications. However, in practice there may be some negative effects on network services and applications while a DPI node is being installed into the network. After installation, the negative influence introduced by DPI node deployments should meet special requirements.

10.3.1 Out-of-path DPI nodes deployment specification

While an out-of-path DPI node is being inserted into a network, services and applications interrupt time of the current network should be less than 50 milliseconds. Theoretically, deploying out-of-path DPI nodes can be carried out without interrupting services and applications.

10.3.2 In-path DPI nodes deployment specification

While an in-path DPI node is being inserted into a network, services and applications interrupt time of the current network should be less than50 milliseconds. By using auxiliary methods or instruments, the 50 milliseconds target can be achieved. For example, use a redundant link first before deploying the in-path DPI node, then remove the redundant link when the in-path DPI node can work normally.

10.4 Analysis of current networks

Before deploying a DPI node, some information about the current network need to be achieved, e.g., the maximum bandwidth of all network segments, active average traffic of the network segments, traffic distribution of the network segments according to date and time, influence degree while deploying a DPI node. Typically, this information can be collected by the NMS of the present network.

Through analysing this information, the design scheme of building a network with DPI functions can be achieved.

10.5 Confirming the DPI requirement of the network

Collect and confirm the requirement of DPI node based on the above analysis of the current network.

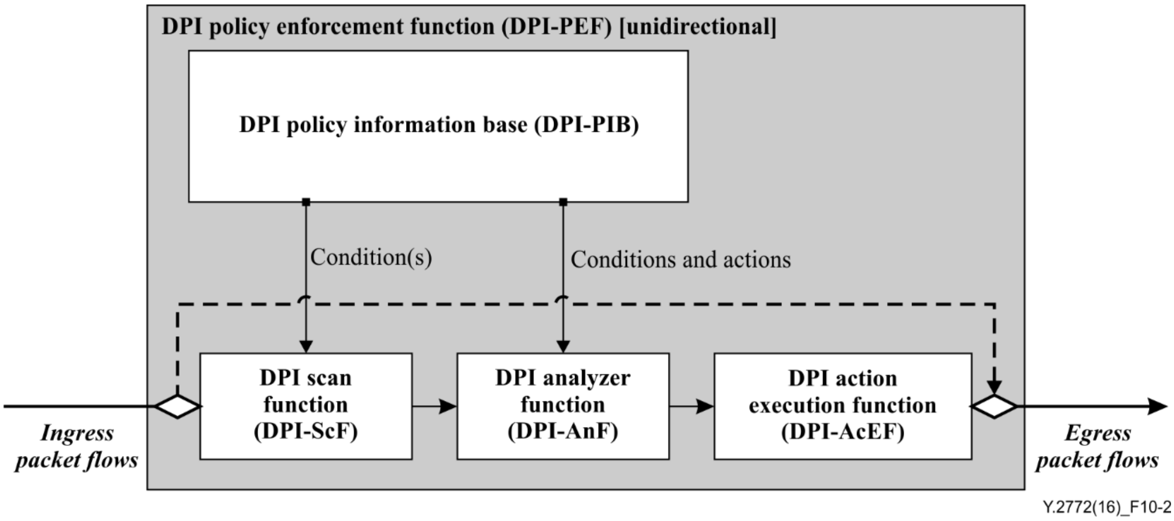
10.6 Choosing proper DPI entities or systems

DPI entities used to construct the network with DPI functions should meet the requirement described in clause 10.4.

10.7 Reconstructing the current network using DPI

Deploying DPI devices should not reduce the performance of the current network, and especially the on-line service should not be impacted. Out-of-path DPI physical entities can be set up more conveniently than in-path DPI physical entities, however improper operations are possible to influence the service. Therefore, the proper time and location should be selected to minimize the above influence, and the time and location selection should be dependent on the network on-line traffic.

As a point of emphasis, a DPI node should support an internal bypass function when it is deployed in the network and it works as in-path DPI node. Figure 10-2 depicts the internal bypass function, and the dashed line represents the bypass. When the packet flows are carried on the bypass, it is equivalent to the DPI node not being in the network. In other words, it appears to the packet flows that the network device prior to the DPI node connects with the network device following the DPI node directly.



DPI policy enforcement function (DPI-PEF) [unidirectional]
DPI policy information base (DPI-PIB)
Condition(s)
Conditions and actions
DPI scan function (DPI-ScF)
DPI analyzer function (DPI-AnF)
DPI action execution function (DPI-AcEF)
Ingress packet flows
Egress packet flows
Y.2772(16)_F10-2

Figure 10-2 – Internal bypass function of a DPI node

10.8 Monitoring and managing the network with DPI

In general, networks that incorporate DPI functions are more complex than networks without DPI functions. Therefore, a DPI network should always use operation, administration and maintenance (OAM). That is, the DPI nodes and their PIB should be maintained and managed.

10.9 Rebuilding the network with DPI based on performance monitor

In general, building a network that incorporates DPI functions is an adaptive process. The network structure should be adjusted gradually based on network performance status changes. Monitoring network status depends on appropriate data and statistical analyses.

11 Specification of management mechanism

11.1 Overview of DPI network management

Just like any typical network element, a DPI node should support configuration, fault, performance and security management functions. These management functions have been defined in the other

Recommendations and are outside of the scope of this Recommendation. However, some special considerations to be taken on management of DPI networks are identified here.

Under bidirectional DPI application environments, the bidirectional DPI functions can be realized by either a single DPI node (single node mode, see Figure 11-1) or by a pair of DPI nodes (double nodes mode, see Figure 11-2). Under many circumstances, double nodes mode is more advantageous than single node mode. For example, when some special traffic needs to be blocked, then the above special traffic can be blocked earlier when using double nodes mode.

Because it is possible that the two related DPI nodes are deployed physically independent, and the management of these DPI nodes needs to be unified, the management will be more complex because under such circumstances network management should be in sub-network level rather than at the node level.

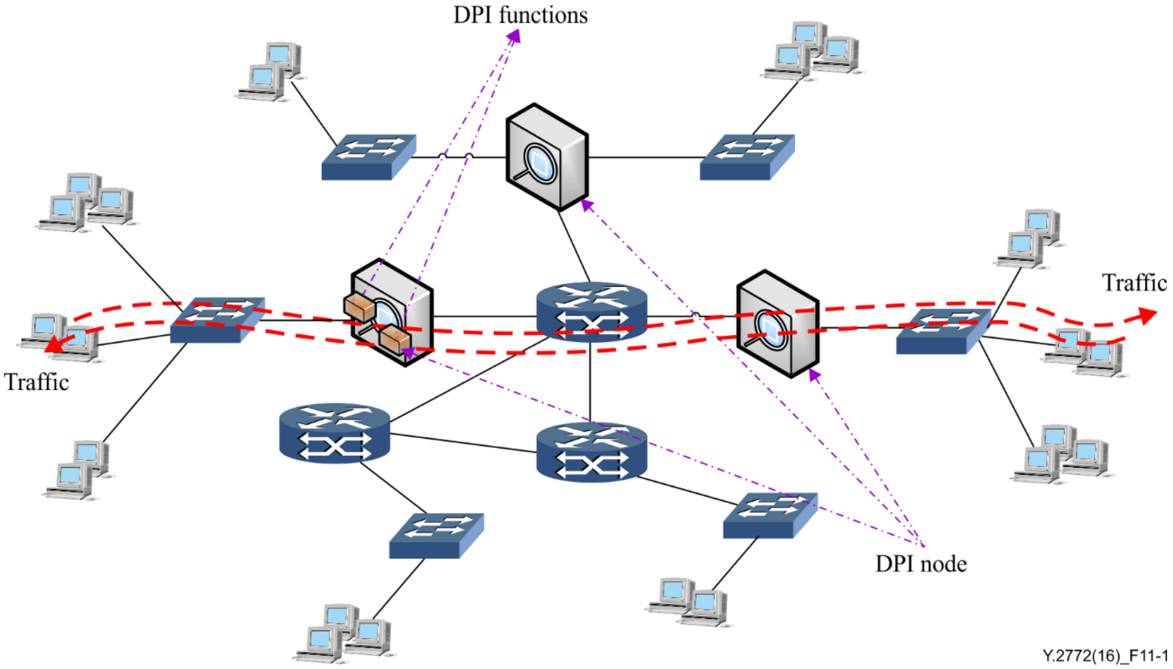


Figure 11-1 – Bidirectional DPI functions carried out by a single DPI node (single node mode)

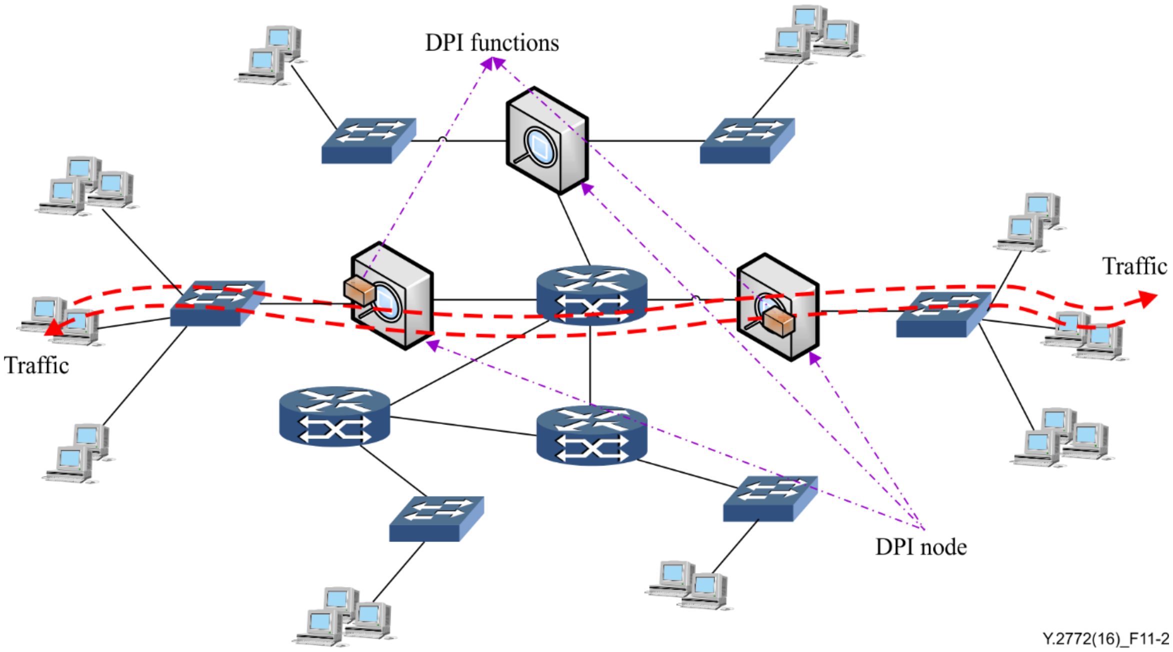


Figure 11-2 – Bidirectional DPI functions carried out by a pair of DPI nodes (double nodes mode)

11.2 Management interface

11.2.1 Unidirectional DPI management interface

The general management of the unidirectional DPI can be as depicted in Figure 11-3, where the connection between a DPI node and the network management system (NMS) is not a physically direct connection, but rather a logical connection through a sub-network. This link between a DPI node and an NMS is represented by a dashed line in the figure. Logically, the management interface between the DPI node and the NMS can be described as follows:

Command line interface (CLI): the NMS manages and controls the DPI node through a serial port, and management action takes effect through a series of single-line commands. The NMS can manage only one online DPI node at a time.

Graphical user interface (GUI): the NMS manages and controls the DPI node through an Ethernet port or the other kind of physical port, and management action takes effect through exchanging a group of protocol packets between the DPI node and the NMS. The NMS can manage one or more online DPI node concurrently.

Telnet interface: the NMS manages and controls the DPI node through an Ethernet port or the other kind of physical port, and management action takes effect through a series of single-line commands. The NMS can manage only one online DPI node at a time.

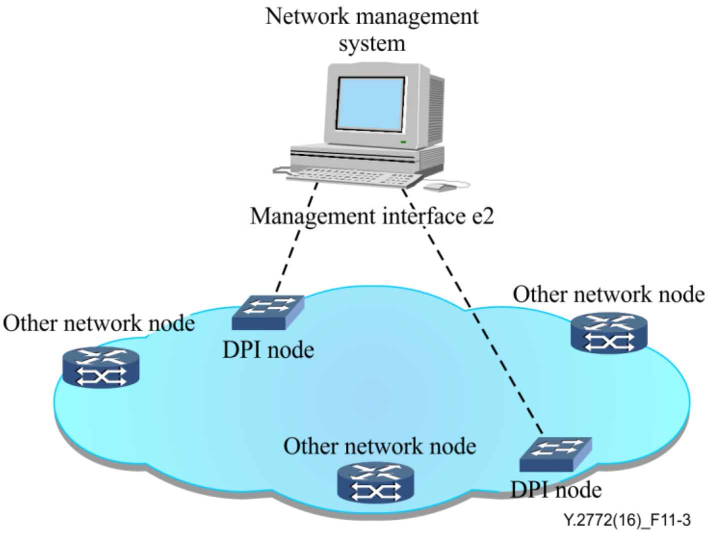


Figure 11-3 – Network management of unidirectional DPI

11.2.2 Bidirectional DPI management interface

The management of the bidirectional DPI can be as depicted in Figure 11-4. Compared with unidirectional DPI management, bidirectional DPI (see the above Figures 11-1 and 11-2) may be more complex because the two or more DPI nodes are inter-dependent. Thus, some connections between two DPI nodes should be set up, certainly. These connections is not necessarily physically direct connections, but can be connections through a sub network or through an NMS. These links are represented by the dashed lines in Figure 11-4. In addition to the unidirectional DPI management interface, the following management interface should be used in bidirectional DPI management:

Interface e3 (see Figure 11-2): the interface between two relative DPI nodes that is used to guarantee the information unity of the two DPI nodes and keep the logically connection between two relative DPI nodes.

In bidirectional DPI application scenarios, it is more efficient and economical to realise bidirectional DPI functions based on cooperation between a pair of DPI nodes with one DPI node being responsible for the DPI function of one direction and the other DPI node being in charge of the DPI function of the counter direction. Therefore, PIBs in the two DPI nodes should be correlative; changes of PIB in one DPI node should cause associated modification of PIB in another DPI node.

For example, if bidirectional DPI functions on the traffic between network device A and B are required to be carried out, then the policy control rule relative to a flow from A to B should be set up in one DPI node, while the policy control rule relative to data flow from B to A should be configured in another DPI node. Note that the network management system need only inform the DPI nodes that they are required to realize bidirectional DPI function on traffic between A and B. PIB configuration in the two DPI nodes should be completed automatically by the DPI nodes and thus, information exchanging between the DPI nodes is necessary and is carried out though interface e3.

Moreover, in order to exchange information between the DPI nodes, some protocol should be used to make the DPI nodes connective and the protocol data packets are also communicated through interface e3.

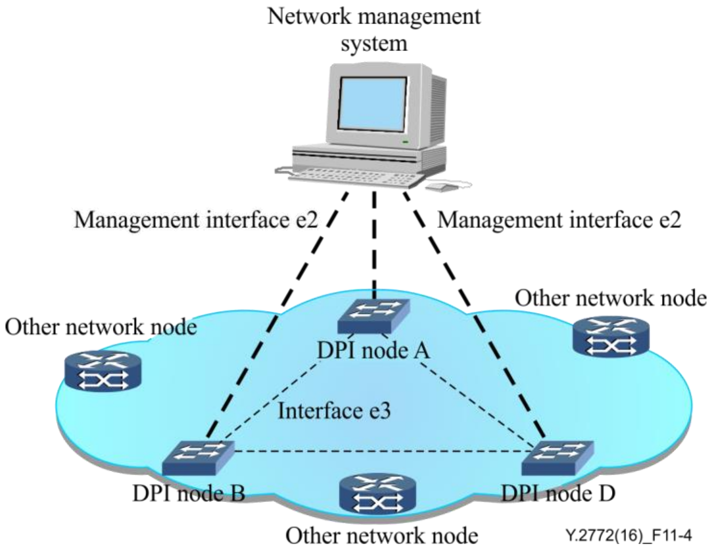


Figure 11-4 – Network management of bidirectional DPI

11.3 Management protocol and functions

The management protocol between the NMS and the DPI node or the DPI subnetwork may be simple network management protocol (SNMP), common management information protocol (CMIP) or any other management protocol.

The management functions include traditional configuration management, alarm management and performance management. In addition, bidirectional DPI subnetwork PIB maintain function should be adopted in the NMS.

12 Security consideration

Regulation, privacy, security application aspects of DPI are outside the scope of this Recommendation. Vendors, operators and service providers are required to take into account national regulatory and policy requirements when implementing this Recommendation.

According to [ITU-T Y.2770], the DPI-FE and the information pertaining to DPI operations should be under protection against threats. The mechanisms specified in [ITU-T Y.2704] address the security requirements of [ITU-T Y.2770].

Bibliography

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

[b-ITU-T X.680] Recommendation ITU-T X.680 (2015), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[b- ITU-T Y-Sup.25] ITU-T Y.2770-series Recommendations – Supplement 25 (2015), *Supplement on DPI use cases and application scenarios*.

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

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016