International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2774

(03/2019)

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

Next Generation Networks – Security

Functional requirements of deep packet inspection for future networks

Recommendation ITU-T Y.2774

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, 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
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.2774

Functional requirements of deep packet inspection for future networks

Summary

Recommendation ITU-T Y.2774 specifies the functional requirements of deep packet inspection for future networks (e.g., software defined networks (SDNs), network function virtualization (NFV), etc.). The scope of this Recommendation includes the general requirements of deep packet inspection (DPI) for future networks, DPI functional requirements for SDN, DPI functional requirements for NFV, DPI functional requirements for service function chain (SFC) and DPI as a service, as well as DPI functional requirements for network virtualization and DPI functional requirements for evolving mobile networks.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2774	2019-03-14	13	11.1002/1000/13495

Keywords

Deep packet inspection, functional requirements, future networks.

* 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 not 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.2774

Functional requirements of deep packet inspection for future networks

1 Scope

This Recommendation specifies the functional requirements of deep packet inspection (DPI) for future networks (e.g., software defined networking, network function virtualization, etc.). The scope of this Recommendation includes:

a) General requirements of deep packet inspection for future networks;

b) DPI functional requirements for software defined networking;

c) DPI functional requirements for network function virtualization;

d) DPI functional requirements for service function chain and DPI as a service;

e) DPI functional requirements for network virtualization; and

f) DPI functional requirements for evolving mobile networks.

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

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 X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[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.*

[ITU-T Y.3001] Recommendation ITU-T Y.3001 (2011), *Future networks: Objectives and design goals.*

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 [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 layer 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 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 6-1of [ITU-T Y.2770]).

3.1.3 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), hence, the DPI-NF is functionally equal to the DPI functional entity.

3.1.4 future network (FN) [ITU-T Y.3001]: A network able to provide services, capabilities, and facilities difficult to provide using existing network technologies. A future network is either:

a) A new component network or an enhanced version of an existing one, or

b) A heterogeneous collection of new component networks or of new and existing component networks that is operated as a single network.

3.1.5 service function chain [b-ITU_T Y-Sup.41]: A chain that defines an ordered set of abstract service functions and ordering constraints that must be applied to packets and/or frames and/or flows selected as a result of classification and/or policy.

3.1.6 service function [b-ITU-T Y-Sup.41]: A function, specifically representing network service function, that is responsible for specific treatment of received packets other than the normal, standard functions of an IP router (e.g., IP forwarding and routing functions) on the network path between a source host and destination host.

NOTE – A service function can act at various layers of a protocol stack (e.g., at the network layer or other OSI layers). As a logical component, a service function can be realized as a virtual element or be embedded in a physical network element. One or more service functions can be embedded in the same network element. Multiple occurrences of the service function can exist in the same administrative domain.

3.1.7 service function chaining [b-ITU-T Y-Sup.41]: A mechanism of building service function chains and forwarding packets/frames/flows through them.

3.1.8 metadata [b-IETF RFC 7665]: Provides the ability to exchange context information between classifiers and SFs, and among SFs.

3.1.9 VNF manager [b-ETSI GS NFV-MAN 001]: The lifecycle management of VNF instances; overall coordination and adaptation role for configuration and event reporting between network function virtualization infrastructure (NFVI) and the element management system/network management system (EMS/NMS).

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Program Interface

DPI Deep Packet Inspection

DPI-FE DPI Functional Entity

DPI-PEF DPI Policy Enforcement Function

DPI-PIB DPI Policy Information Base

EMS Element Management System

FN Future Networks

PFF Packet Forwarding Function

GPRS General Packet Radio Service

GTP GPRS Tunnelling Protocol

L-PDF Local Policy Decision Function

MME Mobility Management Entity

NFV Network Function Virtualization

NFVI Network Function Virtualization Infrastructure

NMS Network Management System

P-GW Packet data network Gate Way

PIB Policy Information Base

QoE Quality of Experience

QoS Quality of Service

SDN Software Defined Network

SC Service Chaining

SCTP Stream Control Transmission Protocol

SFC Service Function Chaining

S-GW Service Gateway

RAN Radio Access Network

UDP User Datagram Protocol

VNF Virtual Network Function

vDPI virtual Deep Packet Inspection

5 Conventions

This Recommendation uses the following conventions:

The term "is required to" indicates a requirement which must be strictly followed, and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The term "is recommended" indicates a requirement which is recommended, but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 General requirements of deep packet inspection for future networks

Definition of the term future network can be seen in clause 3.1. The definition makes clear that future network does not refer to a specific network architecture. Actually, future networks refers to a network using one or more emerging network architectures and technologies that can provide services, capabilities, and facilities that are difficult to be provided by current networks. In other words, future networks are networks that are designed according to a group of emerging network architectures, adopts a group of emerging network technologies and provides better services. In general, regardless of the kind of architecture or technology that it uses, a future network should have the following features: openness, extendibility, flexibility, security and greenness.

As a basic infra-structure network technology, deep packet inspection (DPI) will play a key role in future networks. In advancing future networks, the following new requirements for deep packet inspection related technologies need to be considered:

- The adoption of DPI functions in future networks is required to maintain the original network architecture.
- In adopting DPI functions in future networks it is recommended to maintain openness, extendibility, flexibility, security and greenness of the target network and not to deteriorate any of these features.

  Openness, extendibility, flexibility, security and greenness are not only features of future networks but are also driving forces to improve the network service. It is therefore beneficial to maintain openness, extendibility, flexibility, security and greenness of the network when adopting a certain technology or method. Nevertheless, it is usually difficult to maintain all the features at the original level, and for that reason the above requirement is recommended.
- Adopting DPI functions in future networks is required to guarantee the performance threshold.

  Adopting DPI functions in future networks is required to match the performance requirements as defined by each network. Specification of performance requirements for each network is out of scope of this Recommendation.

  For example, if the network requires that the end-end latency be less than 50 ms, the end-end latency should be specifically less than 50 ms even if DPI functions are deployed in the network.

In addition, deep packet inspection can enhance the application/service awareness capabilities of the future network and guarantee its quality of service (QoS) and quality of experience (QoE). On the other hand, future networks are service/application centric networks that are based on application/service awareness functionalities, therefore application/service oriented deep packet inspection is beneficial. The following general functional requirements of DPI for future networks should be met:

– DPI for future networks is required to support the unambiguous application identification capability based on DPI. In the past applications were identified by the layer 3 protocol information and layer 4 port information. However, current applications often randomly shift their protocol ports and protocols (e.g., an application using dynamic ports, spams and worms disguised as other well-known SMTP application), and more and more applications are transitioned to web-based services (e.g., applications over web: web page games, web page video with the same port 80). Based on deep packet inspection, applications can be identified by means of an application signature property that enables the DPI application identification capability to be a basic building block for future networks.

– DPI for future networks is required to support application traffic scheduling and optimization based on the actions defined in the DPI policy rules. The actions include, but are not limited to:
  1) accepting and forward the application traffic to the packet forwarding function (PFF) entity;
  2) forwarding application traffic to the DPI policy decision function entity;
  3) processing the application traffic based on the DPI policy [such as restricting spam and other abusive traffic];
  4) redirecting the application traffic to another interface;
  5) mirroring the application traffic to another interface; and
  6) traffic statistics according to the DPI policy rule.
– DPI for future networks is recommended to support the separation of DPI policy decision and the DPI policy enforcement. There is a local policy decision function (L-PDF) and an external DPI policy decision function. Since centralized control is a feature of future networks (e.g., SDN), it is recommended for DPI for future networks to support the separation of DPI policy decision and the DPI policy enforcement.
– DPI for future networks is recommended to support the softwarization capability with respect of DPI based application traffic identification, scheduling and optimization. Applications can initiate and push the DPI policy rules to the DPI policy enforcement entities through the softwarization capability and application program interface (API) provided by the DPI policy decision functional entity.

7 DPI functional requirements for SDN

7.1 Overview of DPI in a SDN context

Generally, SDN architecture is designed as a three-layer structure as follows:

– Resource layer: composed of a group of network devices that carry out data forwarding functions.
– SDN control layer: composed of one or more controllers that control the above network devices.
– Application layer: composed of some software components that access or schedule network resources through the above controllers.

SDN basically has the three following features:

– The control function is separated from the data forwarding function.
– Control functions are logically centralized.
– Open applications.

In an SDN context, it is possible to relate to the entities within all of the three layers to carry out DPI related functions. In addition, DPI deployed in an SDN context also has the above basic features.

7.2 DPI functional requirements for SDN within an entity

– The policy rule table within a DPI functional entity is recommended to support timeout functions, and if one or more policy rule is obsolete, the DPI functional entity should report to the corresponding controllers.
– The policy rule table within a DPI functional entity is recommended to support counting functions, and the counter information can be retrieved by the corresponding controller or the management system.

– The policy rule table within a DPI functional entity is recommended to support setting rule priority functions, meanwhile the priority is relative to the policy rules and can be set by the corresponding controller.
– The L-PDF in the DPI functional entity is required to exchange policy rules data and other data with one or more controllers.
– The DPI policy information base (DPI-PIB) in the DPI functional entity is required to provide policy rules to decide the actions of a DPI policy enforcement function (DPI-PEF) when establishing connections between the DPI functional entity and controller(s).
– When a DPI functional entity is within a SDN context, the local policy decision function within the entity is required not to change the PIB without a command from the corresponding controller, even if the connection between the entity and the controller is interrupted.
– The DPI functional entity is recommended to support multiple policy rule tables. And the policy rule tables are handled in order. Note that the output of handling a policy rule table becomes the input of handling the following policy rule table.

7.3 DPI functional requirements for SDN at entity level

– The DPI functional entity (DPI-FE) is required to support a kind of south-bound interface that is used to exchange policy rules data and other data with one or more controllers.
– The DPI functional entity is required to be able to set up a connection with one or more controllers through the above south-bound interface.
– The DPI functional entity is required to forward all ingress packets when it is used as in-path DPI within a network designed with a SDN architecture, and while the connection between DPI-FE and the corresponding controller is not yet set up.
– The DPI functional entity is required to remain the PIB information when connection between DPI-FE and the controller is broken.
– The DPI functional entity is recommended to support two or more controllers concurrently.

7.4 DPI functional requirements for SDN at the network level

7.4.1 PIB maintenance requirements

– The controller is required to have the capability to maintain the PIB of all the DPI entities that are controlled by the above controller.
– The controller is required to have the capability to recover the PIB of every DPI entity if the PIB of the DPI entity fails.
– If multi-controllers are used to control the same DPI network, the above controllers are required to cooperate in order to maintain the same PIB regardless of the synchronization method that is adopted by the above controllers.

7.4.2 Logical link between a DPI entity and the corresponding controller

– If a logical link between DPI entity A and its corresponding controller needs to go through a DPI entity B, then the DPI entity B is required to have the capability to cooperate with other DPI entities in order to set up the logical link.
– If a logical link between DPI entity A and its corresponding controller includes a DPI entity B, then the DPI entity B is required to have the capability to guarantee that control messages between DPI entity A and its corresponding controller be reliably transported through entity B.

7.4.3 Multi DPI entities cooperation

– If two or more DPI entities are necessary to realize a DPI function, the controller that controls the DPI entities is required to coordinate the above DPI entities to carry out the DPI function.

7.4.4 Bidirectional DPI function realized by two DPI entities

– If a bidirectional DPI function is carried out by two independent DPI entities and the two DPI entities are controlled by a single controller, the above controller is required to coordinate the two DPI entities to carry out the bidirectional DPI functions.

– If a bidirectional DPI function is carried out by two independent DPI entities and the two DPI entities are controlled by two different controllers, the above controllers are required to cooperate in order to coordinate the two DPI entities to carry out the bidirectional DPI functions.

7.4.5 Controller failure

– If a controller fails and the controller is the unique controller to the corresponding DPI network, the DPI entities within the DPI network are required to keep normal status unchanged until the controller is recovered.

– If a DPI network is controlled by multiple controllers and one of the controllers fails, the other controllers are required to have the capability to take over the responsibility of the failed controller.

8 DPI functional requirements for NFV

8.1 DPI functional requirements for NFV within an entity

A DPI functional entity in a NFV context is called a NFV DPI functional entity that is carried out by one or more virtual network functions (VNFs), for example, a NFV DPI functional entity is composed of three VNFs. The first VNF carries out the DPI engine functions, the second one undertakes the L-PDF functions and the third one is responsible for the DPI PIB.

The following requirements are related to the NFV DPI functional entity.

– It is required that a NFV DPI functional entity includes a DPI-engine, a DPI-PIB and an L-PDF as well as some internal or external interfaces.

– If a NFV DPI functional entity is implemented by a single VNF, it is required that the VNF implements all components (including DPI-engine, DPI-PIB, L-PDF, etc.) of a DPI functional entity.

– If a NFV DPI functional entity includes two or more VNFs, it is recommended that all VNFs have equivalent performance in case that one lower-performance VNF influences the higher-performance VNF.

– If a NFV DPI functional entity includes two or more VNFs, it is required that the resources allocated to the data exchange between VNFs are enough to guarantee that the data exchange is reliable and timely.

– If a VNF is scheduled to carry out the DPI functions, it is required that the VNF only performs DPI functions and that the VNF is independent from other VNFs.

8.2 DPI functional requirements for NFV at the entity level

– The NFV DPI functional entity is required to support a kind of interface that is used to exchange policy control data and other data with one or more VNF managers.

– The NFV DPI functional entity is required to have the capability to set up a connection with one or more VNF managers through the above interface.

– The NFV DPI functional entity is required to exchange ingress packets with the NFV infrastructure when it is used in a NFV network context.
– The NFV DPI functional entity is required to remain the policy control information when the connection between entity and the VNF manager is interrupted or when the VNF manager is out of order.
– The NFV DPI functional entity is recommended to support two or more VNF managers concurrently.

8.3 DPI functional requirements for NFV at the network level

– If a DPI function needs two or more NFV DPI functional entities to operate, the VNF managers that manage the VNFs (the VNFs implement the above NFV DPI functional entities) are required to coordinate the VNFs to carry out the functions.
– If a bidirectional DPI function is carried out by two independent NFV DPI functional entities, and the two NFV DPI functional entities are managed by a single VNF manager, the above VNF manager is required to coordinate the two NFV DPI functional entities to carry out the bidirectional DPI functions.
– If a bidirectional DPI function is carried out by two independent NFV DPI functional entities, and the two NFV DPI functional entities are managed by two different VNF managers, the VNF managers are required to cooperate in order to coordinate the two NFV DPI functional entities to carry out the bidirectional DPI functions.

9 DPI functional requirements for service chaining and DPI as a service

9.1 Overview of service chaining and DPI as a service

Service function chaining (SFC) is a new architecture under development in IETF [b-IETF RFC 7665]. Service chaining (SC) is an emerging set of technologies and processes that enables operators to configure network services dynamically in software without having to make changes to the network at the hardware level.

DPI functions can also be designed as common functions to almost all service functions in the service chain that deal with L2-L7 protocols. In other words, DPI is deployed based on the architecture of DPI as a service. Figure 9-1 illustrates the architecture of DPI as a service or DPI functions for the service chain. In Figure 9-1, the left DPI service node or the right DPI service node provides DPI function for service function node 1, service function node 2, service function node 3, etc.

DPI as a service means that DPI functions are provided in the network to other network modules as a service function. Therefore, in the architecture of DPI as a service the DPI function can be shared by different network modules. The traffic needs to be scanned only once and this one-time scanning can handle the data of all service functions in the service chain. The DPI service then passes the scan results to the appropriate service function instances. Deploying DPI functions based on the architecture of DPI as a service has significant advantages in performance, scalability, robustness.

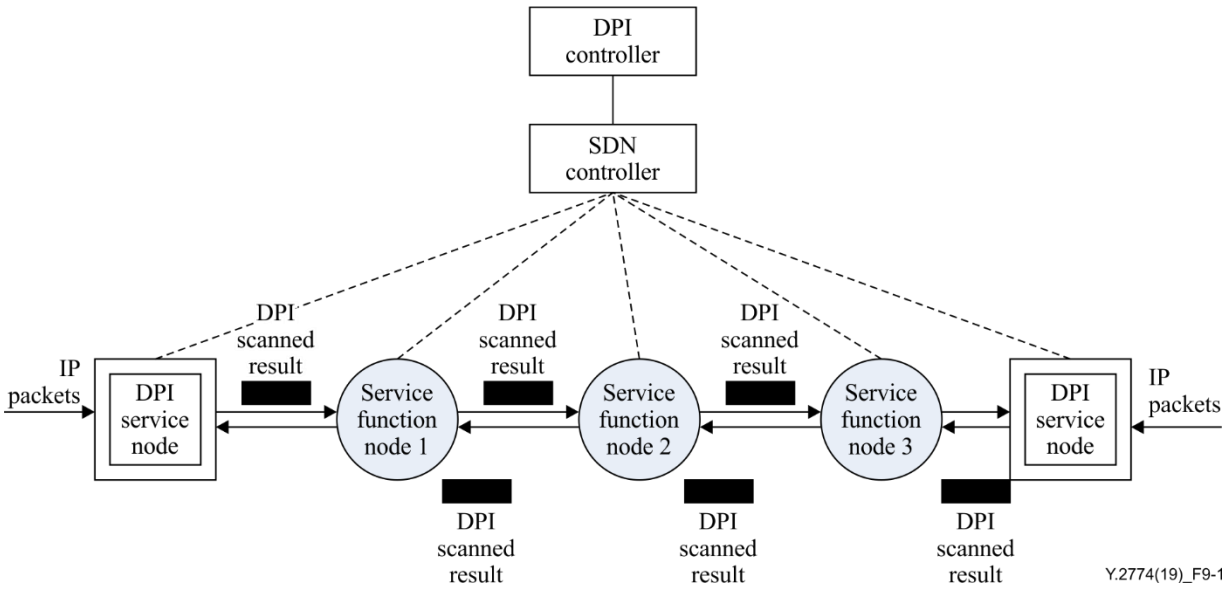

Figure 9-1 – DPI service in service chaining

9.2 DPI functional requirements for DPI as a service and service chaining

9.2.1 Classification requirements for DPI as a service

– The DPI functional entity is required to support a kind of interface that is used to exchange classification rules data and other data with one or more controllers.

– The DPI functional entity is required to be able to set up a connection with one or more controllers through the interface that is used to exchange classification rules data and other data with one or more controllers.

– The DPI functional entity is required to have the capability to keep PIB unchanged when the connection between the above DPI functional entity and the corresponding controllers is interrupted.

– The DPI functional entity is required to be able to provide the classification function according to the L2-L7 fields of packets.

– The DPI functional entity is recommended to support two or more controllers concurrently.

– The DPI functional entity is recommended to support full application classification and metadata extraction.

9.2.2 General functional requirements for DPI as a service

– The DPI functional entity is required to be prior to any other service functions that require DPI functions.

– The DPI functional entity is recommended to scan the packets and logs for all detected patterns as metadata to the packets.

– The DPI controller is recommended to be designed as a logically centralized entity whose role is to control the DPI process across the network and to also communicate with the SDN controller.

– The service functions that use DPI services are required to register their pattern set with the DPI controller.

– The DPI controller is recommended to have the ability to process DPI nodes registration and manage DPI nodes.

– The DPI controller is required to have the capability to initialize DPI service instances and to deploy different DPI service instances across the network.

– The DPI controller is required to have the capability to manage the DPI instance resources, to allocate instances, to remove service instances and to migrate flows between instances.
– It is required that passing the pattern matches results to the service function node does not interfere with forwarding the packet through the chain of service function nodes and then to its destination.
– It is required that the process to pass the pattern matches results to the service function node is compatible in the following scenarios:
    1) The meta-data size is variable
    2) The number of match results is variable
    3) The above size and number is not known in advance
– It is required that the process to pass the pattern matching results to the service function nodes should be oblivious to the service function nodes that are not aware of the DPI service.

10 DPI functional requirements in the network virtualization context

10.1 Overview for DPI in the network virtualization context

A basic feature of network virtualization is that a physical network can be virtualized to one or more logical networks. In other words, although only a physical network exists in reality, from the different perspectives of different users or different services, the physical network can be thought of as one or more independent logical networks. For example, a physical local area network can be virtualized to up to 4096 virtual local area networks. Network virtualization also means that the physical resources within the physical network have the capability to be virtualized to logical or virtual resources.

When a DPI node is deployed in a network virtualization context, it is possible that the DPI node or components (e.g., DPI engine) within the DPI node need to be virtualized to logical/virtual DPI nodes or logical/virtual components.

10.2 User layer functional requirements

– The DPI engine, DPI-PIB and DPI node are recommended to have the capability to be virtualized respectively as one or more virtual deep packet inspection (v-DPI) engines, virtual DPI PIBs and virtual DPI nodes.
– If a physical DPI component (DPI node, DPI engine or DPI PIB, etc.) is virtualized to be two or more logical DPI components, the logical DPI components are required to be logically independent and separated from each other.
– If a virtual DPI node, a virtual DPI engine or a virtual PIB is logically deployed in a virtual network, the virtual DPI node, the virtual DPI engine or the virtual PIB is required to have the same DPI capability as that of a physical DPI node, a physical DPI engine or a physical DPI PIB.
– If a virtual DPI node, a virtual DPI engine or a virtual PIB is logically deployed in a virtual network, the virtual DPI node, virtual DPI engine or virtual PIB is required not to worsen the performance of the virtual network.
– The mapping mode between physical DPI components (DPI node, DPI engine or DPI PIB, etc.) and virtual DPI components is recommended to be 1:n, m:1 or m:n (m and n are positive integers, and $m > 1$, $n > 1$).

10.3 Control layer functional requirements

– Every logical/virtual DPI component is required to have one or more corresponding control entities that control the logical/virtual DPI component.

– The control entity is recommended to have the capability to configure mapping physical DPI components (DPI node, DPI engine or DPI PIB, etc.) to the corresponding logical/virtual DPI components.
– The control entity is recommended to have the capability to guarantee that the different logical/virtual DPI components are independent and separated from each other.
– When a logical/virtual DPI component is controlled by two or more control entities, it is required that the control entities guarantee information conformance related to the controlled logical/virtual component.

10.4 Management layer functional requirements

– The management entity is required to have the capability to manage the physical DPI components (DPI node, DPI engine or DPI PIB, etc.) that are virtualized to some logical/virtual DPI components.
– The management entity is recommended to have the capability to manage logical/virtual DPI components.
– If a physical DPI component (DPI node, DPI engine or DPI PIB, etc.) and its corresponding logical/virtual DPI component are managed by an identical management entity, the management entity is required to guarantee the independence of the management information related to the above physical DPI component and its corresponding logical/virtual DPI component.

11 DPI functional requirements for evolving mobile networks

11.1 Introduction of evolving mobile networks

The evolution of mobile networks refers to the process of mobile networks being updated to new generation networks. Note, for example, when the 2G mobile network is updated to the 3G mobile network.

Therefore, evolving mobile networks are mobile networks that are developing to a new-generation mobile network with the development of related technologies. For example, current mobile networks have been evolving to 4G mobile networks and will evolve to 5G, etc., in the future.

11.2 General requirements for DPI deployed in evolving mobile networks

– The following general requirements are to be taken into consideration when a DPI is deployed in an evolving mobile network: When the mobile network is upgraded to next generation technology, the DPI function is required to have the capability to work normally or be easily upgraded to the available status.
– The DPI function is required to sustain and not to worsen the original capability and performance of the evolving mobile network no matter if it is deployed within radio access network (RAN), at the access edge of packet based core network, within packet based core network or at the uplink edge of packet based core network.
– The DPI function is required to have the capability to guarantee that the evolving mobile network can work normally if the component or node that performs the functions of the DPI is out of order.

11.3 Interface requirements for DPI deployed in evolving mobile networks

– Regardless of the position where the DPI functions are deployed (within RAN, at the access edge of packet based core network, within packet based core network or at the uplink edge of packet based core network) the component or node that performs the DPI functions is

required to have the interfaces that can connect with a corresponding entity within the evolving mobile network.

For example, when deploying DPI functions for 4G networks between a service gateway (S-GW) and a packet data network gateway (P-GW), the component or node should have proper interfaces that can connect with S-GW and P-GW.

11.4 Protocol requirements for DPI deployed in evolving mobile network

Regardless of the place where the DPI functions are deployed (within RAN, at the access edge of packet based core network, within packet based core network or at the uplink edge of packet based core network) the component or node that performs the DPI functions is required to have the capability to handle the protocol that is used by a corresponding entity within the mobile network. For example, in the case of 4G networks. Figure 11-1 describes the protocol stack related to the interface of S-GW and P-GW (interface s5 or s8), if DPI functions are deployed between S-GW and P-GW, then the component or node that performs the above DPI functions should have the ability to handle the general packet radio service (GPRS) tunnelling protocol (GTP).

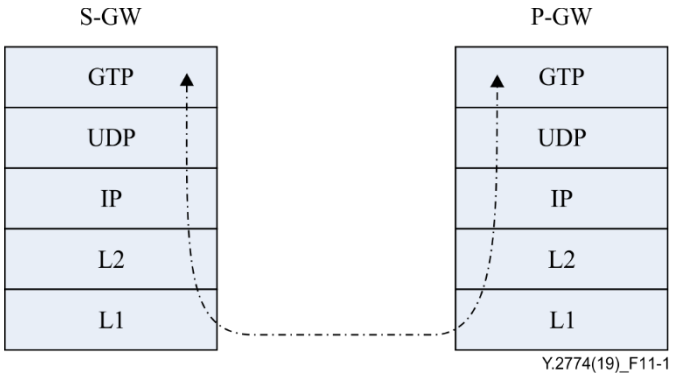

Figure 11-1 – An example protocol stack between S-GW and P-GW

In an additional example, Figure 11-2 describes the protocol stack between eNodeB and mobility management entity (MME), if DPI functions are deployed between eNodeB and MME, then the component or node that implements the above DPI functions should have the ability to handle the stream control transmission protocol (SCTP).

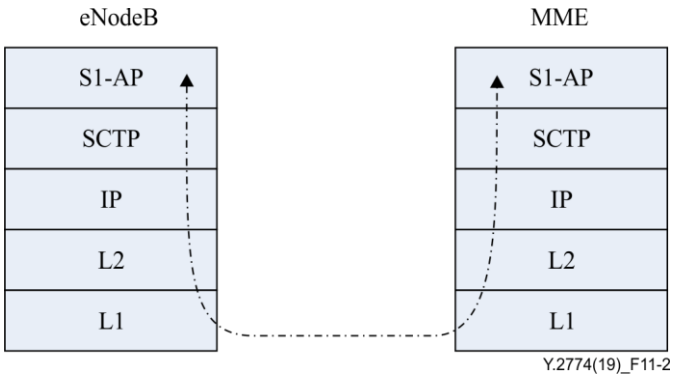

Figure 11-2 – An example protocol stack between eNodeB and MME

– When the DPI functions are deployed within the packet based core network, the DPI functions are required to have the capability to handle packets of multiple protocols.

For example, if the component or node that implements the above DPI function is deployed between S-GW and P-GW in an evolving mobile network, the protocols such as SCTP, user datagram protocol (UDP) and GTP-U, etc., should be supported by the component or node.

– When the DPI functions are deployed within the packet based core network, the policy rules in DPI PIB are recommended to be effective to multiple protocols concurrently.

For example, if a policy rule is laid out with an application tag A, then packets with an application tag A corresponding to the protocols such as UDP, GTP (see Figure 11-1) and SCTP (see Figure 11-2) etc., should be matched by the policy rule.

12 Security considerations

This Recommendation has the same security requirements as [ITU-T Y.2770].

13 Other considerations

Regulation, and privacy 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.

Bibliography

[b-ITU-T Y-Sup.41] ITU-T Y-series Recommendations – Supplement 41 (2016), *ITU-T Y.2200-series – Deployment models of service function chaining*.

[b-ETSI GS NFV-MAN 001] ETSI GS NFV-MAN 001 (2014), *Network Functions Virtualisation (NFV); Management and Orchestration: V1.1.1*.

[b-IETF RFC 7665] IETF RFC 7665 (2015), *Service Function Chaining (SFC) Architecture*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019