International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y

Supplement 25

(05/2015)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

ITU-T Y.2770 series – Supplement on DPI use cases and application scenarios

ITU-T Y-series Recommendations – Supplement 25

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

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

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

Supplement 25 to ITU-T Y-series Recommendations

ITU-T Y.2770 series – Supplement on DPI use cases and application scenarios

Summary

Supplement 25 to the ITU-T Y.2770 series provides complementary information on deep packet inspection (DPI) use cases and application scenarios in evolving networks. Detailed use cases are specified including application identification and traffic detection, application performance measurements, application specific energy measurements, application statistics reporting, diagnosis and analysis, application traffic optimization and application enrichment, provision of tiered services and parental control. The application scenarios of DPI in next generation networks (NGNs), enterprise networks (ENs) and software-defined networking (SDN) are specified to help guide the deployment of DPI for service/application awareness in evolving networks.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y Suppl. 25	2015-05-01	13	11.1002/1000/12524

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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

Supplement 25 to ITU-T Y-series Recommendations

ITU-T Y.2770 series – Supplement on DPI use cases and application scenarios

1 Scope

This Supplement specifies the use cases and application scenarios of deep packet inspection in support of service/application awareness in evolving networks. The DPI use cases include: application identification and traffic detection, application performance measurements, application specific energy measurements, application statistics reporting, diagnosis and analysis, application traffic optimization and application enrichment, provision of tiered services and parental control. The application scenarios include: DPI applications in NGN, EN and SDN.

2 References

[ITU-T Y.1311] Recommendation ITU-T Y.1311 (2002), *Network-based VPNs – Generic architecture and service requirements*.

[ITU-T Y.1314] Recommendation ITU-T Y.1314 (2005), *Virtual private network functional decomposition.*

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2011), *Resource and admission control functions in Next Generation Networks.*

[ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

[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.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking.*

[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*.

[ETSI TS 123 203] ETSI TS 123 203 (2011), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control architecture (3GPP TS 23.203 version 10..0 Release 10).*

[IETF RFC 2748] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol.*

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term 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.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 application scenario: The environment and context of a system. The application scenario of a system may include one or more use cases.

3.2.2 use case: A use case describes how a user uses a system to accomplish a particular goal.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AAA Authentication, Authorization and Accounting
COPS Common Open Policy Service
DNS Domain Name System
DPI Deep Packet Inspection
DPI-FE DPI Functional Entity
DPI-PDFE DPI Policy Decision Functional Entity
DPI-PEF DPI Policy Enforcement Function
EN Enterprise Networks
GRE Generic Routing Encapsulation
GPRS General Packet Radio Service
ICT Information and Communication Technology
IP Internet Protocol
ISP Internet Service Provider
L2-VPN Layer2 Virtual Private Network
L3-VPN Layer3Virtual Private Network
MPLS Multiple Protocol Label Switching
NAT Network Address Translation
NGCN Next Generation Corporate Network
NGN Next Generation Network
OA Office Automation
OMA Open Mobile Architecture
ONF Open Network Foundation
PCC Policy and Charging Control
PCF Policy Control Framework
PCI Protocol Control Information
PDP Policy Decision Point
PEEM Policy Evaluation, Enforcement and Management
PEP Policy Enforcement Point

QoE Quality of Experience

QoS Quality of Service

RACF Resource and Admission Control Function

SDN Software-Defined Networking

SLA Service Level Agreement

VPN Virtual Private Network

5 Conventions

None.

6 Policy enforcement architecture and common use cases of DPI

6.1 Background and policy enforcement architecture

6.1.1 Background

The network applications' status data, e.g., bandwidth, delay, energy, is a 'Big Data' for network management and control. Internet service providers (ISPs) need to measure the status of network applications and manage the network traffic efficiently to ensure the quality of service (QoS) and quality of experience (QoE). In the past, "over provisioning" of bandwidth was widely used to meet the transport capacity requirements of network applications. With the increase of new Internet applications, e.g., high-bandwidth video, ISPs found it very difficult to build a sustainable evolving network based on "over provisioning". With the current Internet applications shifting their communication ports and protocols randomly, and an increasing number of applications evolving into web-based services. ISPs need to identify and manage network applications unambiguously through protocol, port and application signatures. This kind of fine-grained, long-term traffic management solution aid ISPs in contending with volumes of traffic rising at an exponential rate.

This Supplement specifies application scenarios to guide the deployment of deep packet inspection in support of measurement, reporting, analysis and optimization of network application traffic in evolving networks. These application scenarios should not be considered prescriptive for how to deploy DPI in real networks.

6.1.2 The introduction of converging and evolving networks

With the converging of telecommunication networks, cable TV networks, the Internet and the converging of fixed/mobile broadband networks, the evolving networks are now converging rapidly to IP packet networks (see Figure 6-1). The differences between mobile phones and personal computers is blurring as mobile phones are increasingly being smart and are used to access the Internet freely.

With the emerging of cloud computing and the increasing number of Internet users and applications, packet-based networks are not only used to access information on the World Wide Web and to send email, but also to view television, listen to radio programmes, play games, talk to each other, buy/sell goods and communicate with everyday objects. The Internet traffic is becoming more and more heavy and complex. There is an inevitable urgency for ISPs to work well for all the users and applications. A clear understanding of the current status of the Internet is essential to help diagnose and optimize the network.

Since "over provisioning" of bandwidth is not a sustainable solution for evolving networks, another kind of fine-grained, long-term network awareness and diagnosis solution is required to aid ISPs in contending with volumes of traffic rising at an exponential rate for the evolving intelligent network, e.g., smart pipe, network intelligence capabilities enhancement and smart ubiquitous networks.

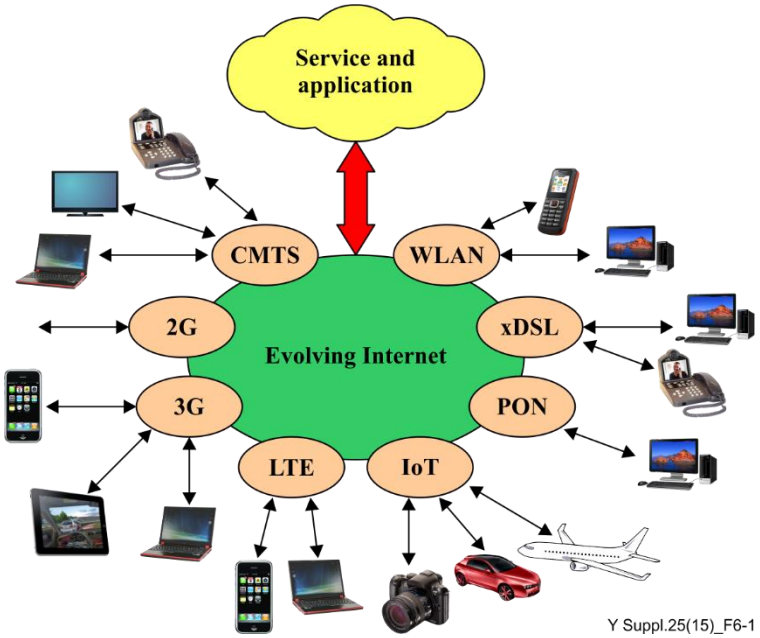

Figure 6-1 – The converging and evolving networks

Example common use cases include application identification and traffic detection, performance metrics measurement, energy metrics measurement, statistics reporting, diagnosis and analysis, traffic optimization and content enrichment, provision of tiered services, parental control, etc. Figure 6-2 illustrates a common use case where DPI policy enforcement points (PEPs) are distributed in the network as an Internet sensor to measure and perceive the network status and report to the policy decision point (PDP) (also known as Intelligence controller). After intelligent analysis of network status data, The PDP can schedule the network resource to optimize the network performance.

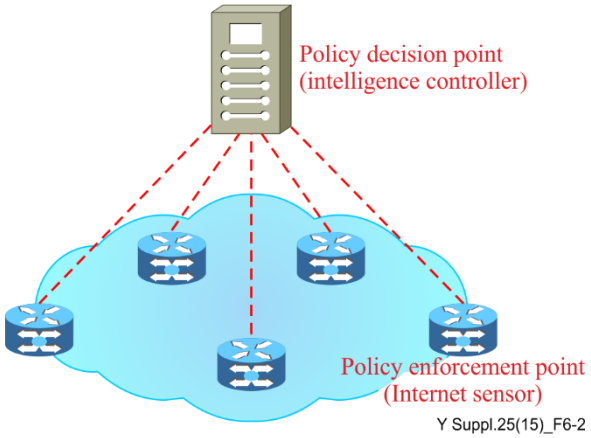

Figure 6-2 – Common policy enforcement architecture

6.1.3 DPI-PE deployment modes

The DPI physical entity (DPI-PE) is a physical instance that represents an implementation of a DPI functional entity [ITU-T Y.2770]. There are multiple network scenarios according to clause 6.1 of [ITU-T Y.2771]. For instance, there are two realizations:

– Integrated DPI-PE (known as "integral DPI" at the functional level (see clause 6.1 in [ITU-T Y.2771])): the DPI functional entity (DPI-FE) is embedded in another network element, e.g., integrated into a legacy packet processing device, such as an IP router or a (Ethernet, MPLS) switch;

– Standalone DPI-PE: the DPI-FE is realized as a self-contained network element (also known as standalone device).

There are two DPI deployment scenarios, from the perspective of the end-to-end communication path:

– Inline mode (known as "In-Path DPI" in [ITU-T Y.2771]): DPI-PE is deployed in a serial manner, the network traffic transverses entirely the DPI-PE, see Figure 6-3.a;

– Bypass mode (known as "Out-of-Path DPI" in [ITU-T Y.2771]): DPI-PE is deployed in parallel to the packet path, which implies that the network traffic needs to be duplicated and directed to DPI-PE, see Figure 6-3.b.

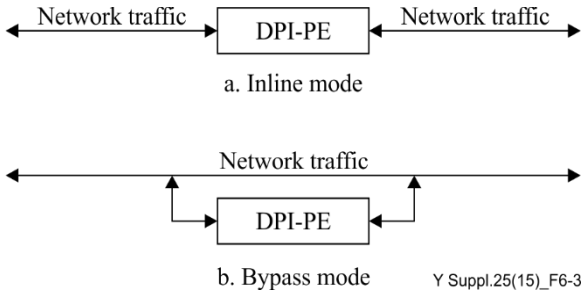

Figure 6-3 – DPI-PE location scenarios from the packet path perspective

6.1.4 Different policy enforcement architectures

Policy and traffic management architectures have been standardized in the past by many important international telecommunication standards organizations [b-Graham]. These include resource and admission control functions (RACF) in ITU-T [ITU-T Y.2111], policy and charging control (PCC) in 3GPP [ETSI TS 123 203], packet cable multimedia (PCMM) in CableLabs [b-PCMM], policy evaluation, enforcement & management (PEEM) in OMA [b-PEEM], policy control framework (PCF) in Broadband Forum [b-BBF BPCF], AAA standards and common open policy service (COPS) in [IETF RFC 2748].

DPI-PEs are deployed as policy enforcement point (PEP) under these architectures in fixed/mobile broadband networks.

Table 6-1 – Policy management architectures

Organization	Policy management architectures
ITU-T	Resource and admission control functions (RACF)
3GPP	Policy and charging control (PCC)
CableLabs	Packet cable multimedia (PCMM) architecture with CMTS acts as PEP
OMA	Policy evaluation, enforcement & management (PEEM)
Broadband Forum	Broad policy control framework (PCF)
IETF	AAA standards and common open policy service (COPS)
SDN	DPI policy based on software-defined network (SDN) architecture

6.1.5 Different deployment sites

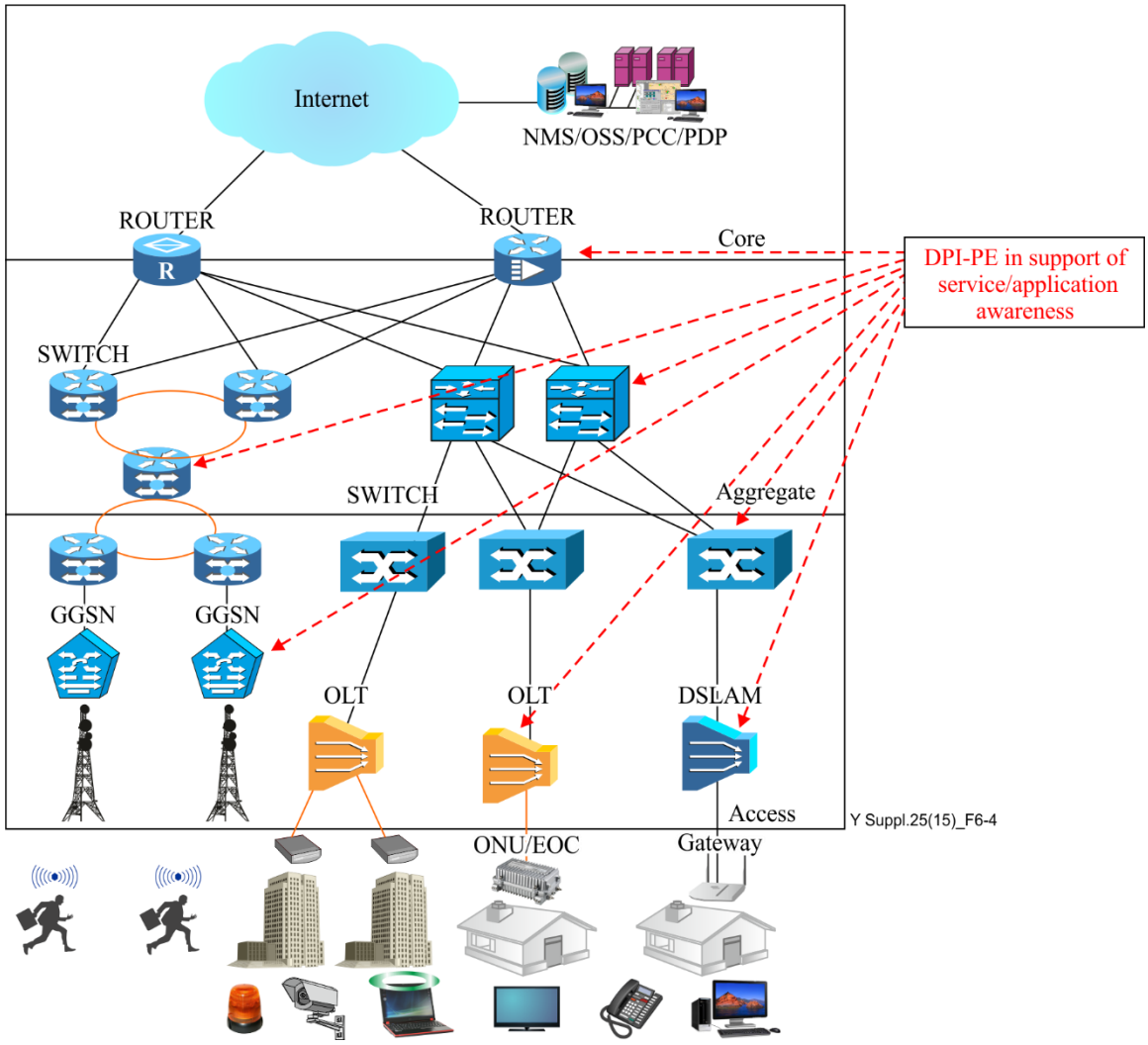

Figure 6-4 – DPI-PE deployment in fixed/mobile broadband networks

6.2 Common use cases of DPI

6.2.1 Use case 1: Application identification and traffic detection

The number of applications and the volume of traffic are increasing rapidly in fixed/mobile broadband networks. In order to prevent a small number of users or applications from clogging up access to the Internet by using a disproportionate share of the available bandwidth, ISPs need to identify applications and manage traffic efficiently to allocate available resources to attain optimum performance for diverse classes of users across their network. DPI-FEs play a key role within all traffic management measures to identify applications unambiguously and for the proper functioning of the Internet. In this situation, ISPs should avoid unfair access or use of the Internet when deploying DPI-FEs for application identification and traffic detection.

6.2.2 Use case 2: Performance measurements

Remote monitoring of network performance (such as grade-of-service-related metrics) is a well-known method in packet networks (see e.g., activities and products by former IETF working group RMON (remote monitoring), see [b-IETF RFC 3577]).

A DPI specific use case could be e.g., derived from the framework of IETF working group RAQMON (Real-time Application QoS Monitoring), an activity related to "real-time application Quality-of-Service monitoring", see [b-IETF RFC 4710]:

– Typical performance indicators of interest: See e.g., the ones defined (with scope on transport level metrics) by [b-IETF RFC 2330], [b-IETF RFC 2678], [b-IETF RFC 2679], [b-IETF RFC 2680] and [b-IETF RFC 2681].
– Necessity of DPI: In order to correlate above performance indicators with "specific packet traffic" (given by the granularity of DPI flow and application descriptors).
– A DPI entity would be then used as a measurement device.

6.2.3 Use case 3: Application specific energy measurements

Energy saving in the information and communication technology (ICT) field is an important issue, as has been identified in designing future networks [ITU-T Y.3012]. One of the basic objectives of the development of future networks is demonstrating environmental awareness, which may be realized via energy-saving technologies. Historically, energy saving has been studied for increasing benefits to the user or company, such as reduced energy costs and temperature management for stable machine operation.

The importance of these issues is increasing due to the more widespread implementation of network equipment and the greater energy consumption that this requires. It is also becoming increasingly important from a social aspect to support the reduction of greenhouse gas (GHG) emissions. These issues will gain more importance in the future. This Supplement therefore studies potential technologies and their coordinated operation, which will contribute to saving energy and to various other objectives.

It is possible for a DPI-FE to measure energy consumption and report to the PDP.

6.2.4 Use case 4: Application specific statistics reporting

Reporting concerns the notification (e.g., due to a particular event detected by the DPI-FE) to another functional entity, which is typically located in a remote network element (in the user, control or management plane). The DPI-FE may provide multiple reporting interfaces in support of the "different types of events".

According to the policy and traffic management architectures, all identified applications, traffic, performance and energy metrics can be reported to the RACF, PCC, PCMM, PEEM, PCF or COPS.

6.2.5 Use case 5: Application diagnosis and analysis

Network management needs an agreed-upon standard to reflect the level of satisfaction of the end-user for their experience with everyday applications. One of the emerging terms to describe this is Quality of Experience or QoE. Network operators can diagnose and analyse the network and application status after all the network and application metrics are received.

6.2.6 Use case 6: Traffic and application delivery optimization

The following techniques, when applied to network traffic, can dramatically improve application performance and availability/reliability, decrease latency and improve bandwidth utilization:

– Domain name system (DNS) optimization – Identifying DNS application through DNS policy rules, redirecting DNS lookups to the fastest DNS server and accelerating DNS lookups help to ensure speedy application delivery.
– Traffic path optimization – Networked applications are matched against the DPI policy rules, the actions may be different applications may take different policy routing (e.g., redirect the packet to other output interfaces).
– Server optimization – Reduces server workload by using techniques such as server load balancing (SLB) and connection management.

6.2.7 Use case 7: Provision of tiered services

ISPs can provide tiered services based on traffic type/class. These tiered services can also be provided based on specific customers' SLAs, see example tiered services in Table 6-2.

Table 6-2 – Tiered services examples based on traffic/class

Traffic type	Traffic class	Priority
Bulk transfers, games	Background	1
Less than 10 millisecond delay	Voice	2
Less than 100 millisecond delay	Video	3
Important application	Controlled load	4
Best effort	Excellent effort	5
Ordinary priority	Best effort	6
Signalling and OAM	Network control	7

6.2.8 Use case 8: Parental and network-based control

It is a very good idea where there are children in a house to deploy a DPI-FE to implement parental control. They allow adults to restrict children's access to various sites by type i.e., adult or over 18 sites, or specific sites by domain name.

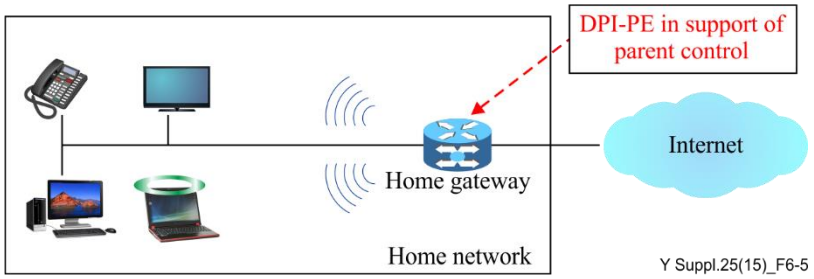

Figure 6-5 – DPI-PE deployment in enterprise networks

6.3 DPI use case: Network-oriented versus link-oriented DPI

6.3.1 Overview

The DPI signatures (of DPI policy rules) may cover protocol layer 3 and upwards or start already with protocol layer 2 (see [ITU-T Y.2770]), which may be distinguished in network-oriented DPI and link-oriented DPI, see Figure 6-6. The crucial point relates to the fact that layer 2 information is limited, either to a point-to-point link or to the borders of layer 2 network domain.

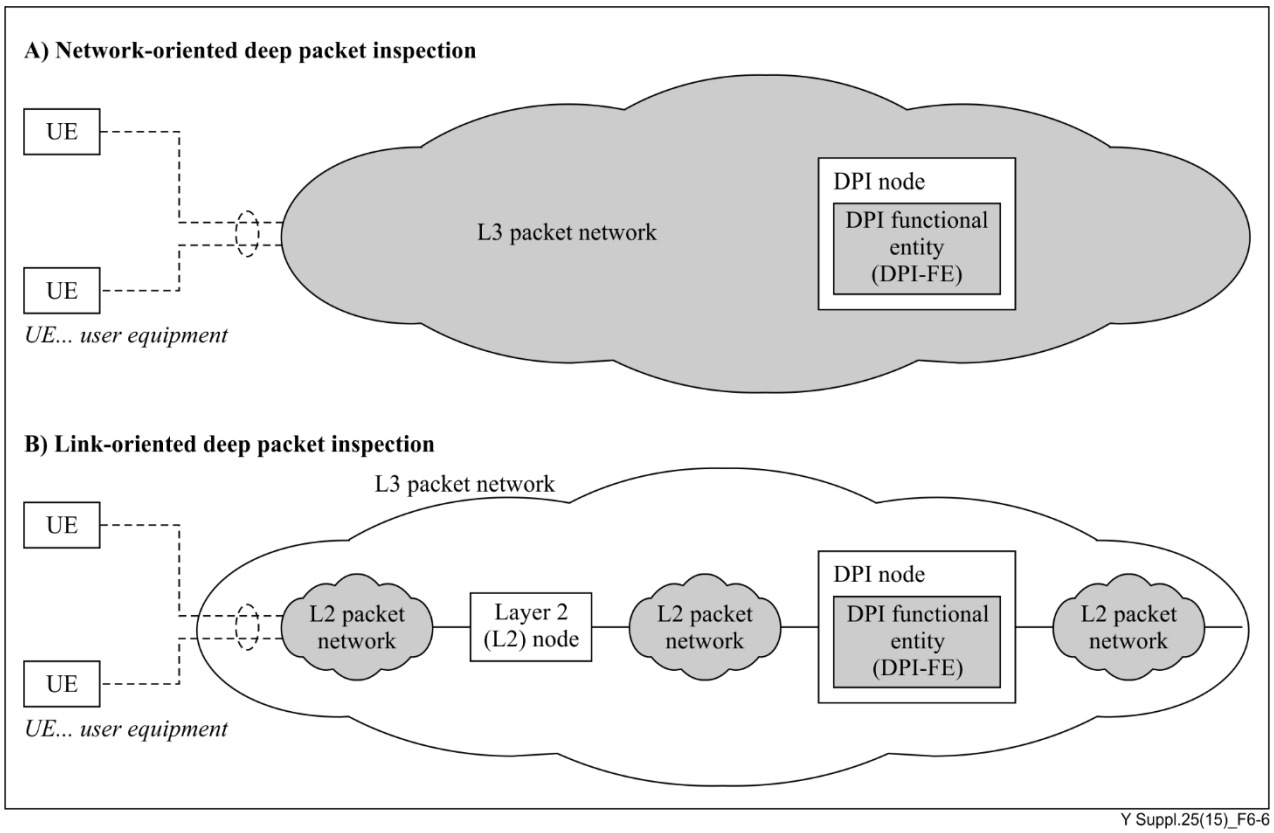

Figure 6-6 – Network-oriented versus link-oriented DPI

6.3.2 Link-oriented DPI

Link layer protocol control information (PCI) is limited to a layer 2 (L2) network domain, and may consequently change in the end-to-end communication path. Usage of L2-PCI (e.g., ATM VCI, Ethernet destination address) as part of DPI signatures may thus question the applicability of such DPI policy rules. The policy decision entity must also be aware of the underlying layer 2 network infrastructure.

However, there are use cases for a link-oriented DPI, like for instance:

– end-to-end network related to a single layer 2 network; or

– L2-VPN (layer2 virtual private network) with L2-VPN dedicated DPI policy decisions.

L2 network domain specific DPI should be thus supported by DPI functional entities.

6.3.3 Network-oriented DPI

Network-oriented DPI is related to DPI signatures which cover protocol information on network layer (L3) and higher. The L2 PCI (e.g., L2 header, padding) is removed before the DPI-FE. Network-oriented DPI represents a common case for DPI due to the "end-to-end" relevance of the network layer. Which means that there would not be any dependency on the location of the DPI-FE within the end-to-end packet path, and the results would be the same.

NOTE 1 – There are scenarios with L3-PCI modifications between end nodes, e.g., the application of topology hiding implies changes of L3 topology information (e.g., NAT (network address translation) in IPv4 networks), L3-VPN (layer 3 virtual private network).

NOTE 2 – The model in clause 6.2 of [ITU-T Y.2771] considers the simplest case of a flat protocol stack. There might be however hierarchical (nested) protocol stacks in real networks like tunnelling methods (e.g., MPLS, IPv4-over-IPv6, Generic Routing Encapsulation (GRE, [b-IETF RFC2784]), GPRS tunnelling in mobile access networks), which may lead to "L3-over-L3" packet types. Such protocol encapsulation is principally covered by the DPI definition (according to [ITU-T Y.2770]), but not further detailed in the Recommendation.

7 Application scenarios in next generation networks

Currently there are few NGN deployments around the world. Only some of its possible application scenarios can be deduced based on its already defined 2-stratum architecture ([b-ITU-T Y.2012]).

Figure 7-1 illustrates an example of how DPI can be deployed in an NGN context. The functional blocks included in the dashed box are components that are closely related to the process of both DPI and packet forwarding: the blocks of policy control consists of subscriber policy control and its corresponding policy repository; the block of resource admission control subsystem is responsible for subscriber authentication/admission and resource allocation while the block of DPI will carry out all the functions of packet header analysis and content scanning.

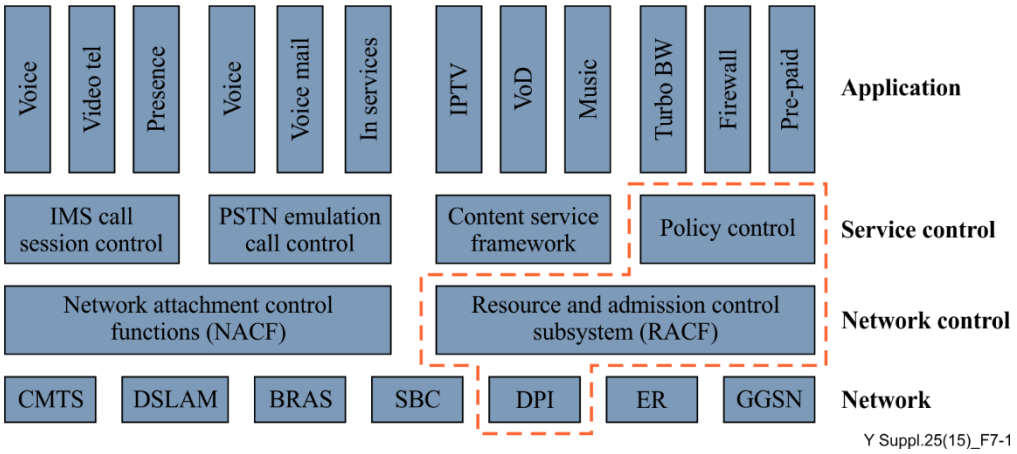

Figure 7-1 – Example of DPI's application scenario within the context of NGN

Figure 7-1 illustrates NGN as a layered architecture. The DPI-PDFE (DPI policy decision functional entity) resides in RACF and the DPI policy enforcement function (DPI-PEF) resides in the packet forwarding plane, while resource and admission control is a basic function of control plane, with policies being stored in the policy repository. Whenever a new application is detected, DPI will generate a request for resource demand and will deliver it to the control plane for resource allocation. In some cases, DPI can even be used to reroute the packets to satisfy SLA requirements.

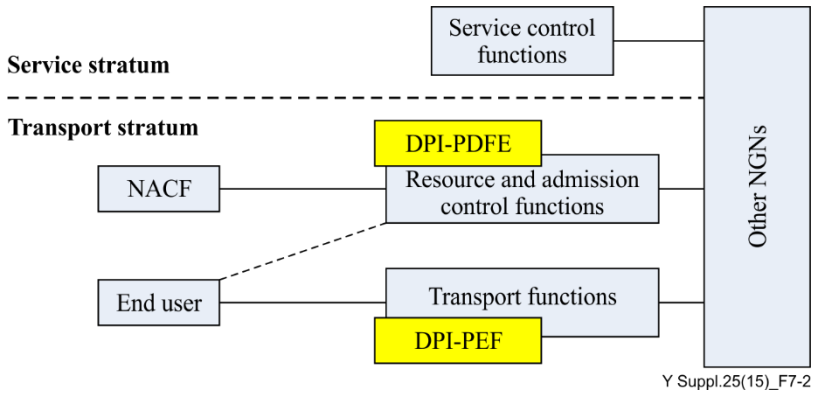

Figure 7-2 – Example of DPI's operation within the context of layered NGN architecture

Figure 7-2 illustrates example locations of DPI policy rule enforcement, e.g., customer premises equipment (CPE) – or host-based on customer premises or network based DPI.

In the scenario above, when DPI is used in the scenario for resource allocation, there are some standardized interfaces within the network architecture. Resource reservation requests originated from DPI will be generated whenever a new service is identified. For example, bandwidth allocation and QoS guarantee for a real-time VoIP application. Under such circumstances, DPI is deployed to fulfil the following goals:

1) Monitor network and bandwidth usage. DPI is applied to automatically discover the application and determine the protocol that might affect the network performance and bandwidth usage.

2) Define the policies in accordance with the identified application. Policies can be seen as the tie between application and resource requirements, which in turn determines the QoS attributes of applications. Among these are minimum and maximum bandwidth, and traffic prioritization.

3) Enforce the policy and update the policy repository at any time.

From the perspective of NGN, DPI is applied to identify the application and generate the raw resource demand. All the remaining processing, including message triggering, delivery and processing will follow the procedures as defined in clause 9 of [ITU-T Y.2111].

As part of the application scenario, how DPI nodes are installed in the network is a big concern. Whether it is deployed as in-path mode or out-of-path mode, and what functions DPI can fulfil are something that also should be mentioned.

8 Application scenarios in enterprise networks

Enterprise communication (see clause 3.2.7 of [ITU-T Y.2201]) belongs to the category of private networks (such as enterprise, corporate, home networks, etc.), which contrast with public networks (such as NGN). The enterprise network considered here might be for instance a next generation corporate network (NGCN), see clause 3.2.10 of [ITU-T Y.2201].

Compared to public networks, private networks provide some specific characteristics which are outlined for instance in clause 17.3 of [ITU-T Y.2201]. On the one hand, an enterprise network is to some extent close and independent from the external network. On the other hand, an enterprise network cannot be completely separated from the external network. With the development of the public network and the increase in size of the enterprise network, the enterprise network is more easily influenced by the public network. Figure 8-1 illustrates a typical example of an enterprise network.

The main differences between private and public networks, from the DPI perspective, are:

– network topology: multiple NGCN sites may be interconnected, i.e., besides the traffic between public and private networks there is intra-private network traffic "tunneled" through the public network;

– virtualization: private network solutions could be realized as virtual private networks (VPNs), see [ITU-T Y.1311], [ITU-T Y.1314];

– location of DPI entities (e.g., at private network site(s), or/and public network);

– applications (e.g., dedicated requirements with regard to privacy, integrity and confidentiality);

– others.

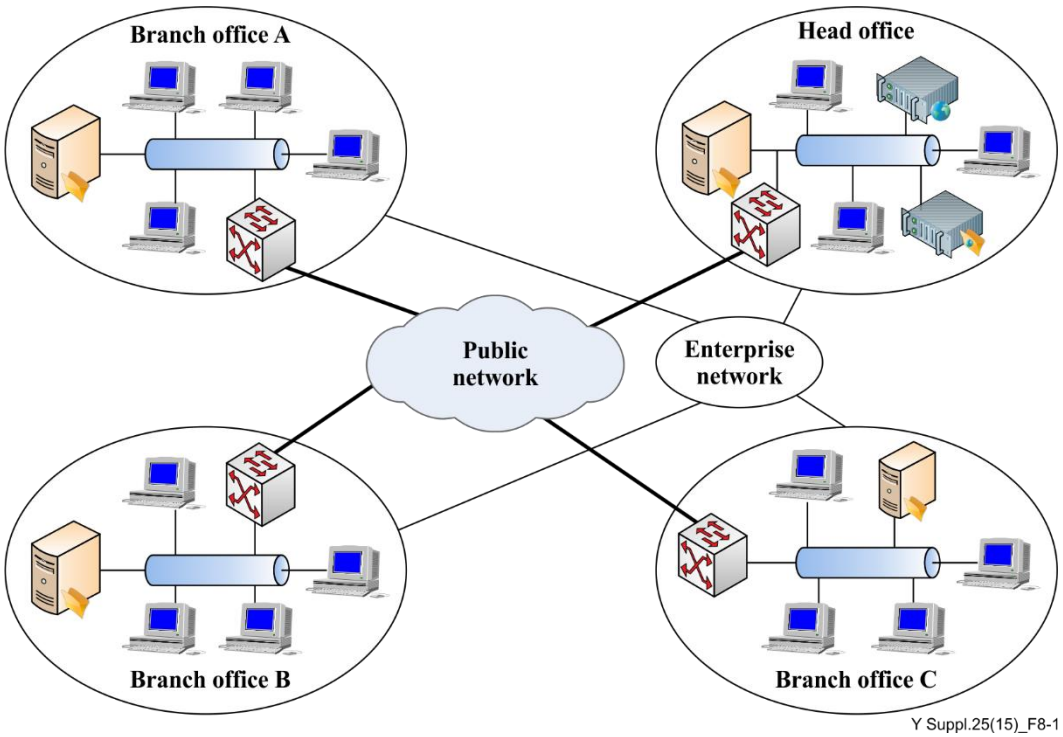

Figure 8-1 – Example of general enterprise network without DPI support

In Figure 8-1, the enterprise (corporation or factory) has several branch offices and a head office (e.g., so called NGCN sites, see [ITU-T Y.2201]) that are located in different place. In other words, the head office and branch offices are geographically separated. The sub-networks of the offices are connected through the public network.

Because of the influence from the external network, control and management of the enterprise network became more important. On the one hand, external bad information can possibly enter the enterprise internal network; on the other hand, precious enterprise data can be leaked outside the enterprise. Furthermore, the internal network resources utility should be optimized through a special method or measure. Additionally, internal office automation (OA) can be more effective by using a certain method.

This means that the use of effective technologies such as DPI to manage and control the enterprise network is highly desired.

8.1 Use DPI to guarantee the information security of the enterprise network

DPI technology used in the scenario is depicted in Figure 8-2. DPI entities are deployed between a part of enterprise network and the public network, so that harmful information from the public network and useful data from the enterprise network will be identified by the DPI entities. With the help of the DPI policy enforcement function, the harmful external information will not enter the enterprise network, and the useful enterprise data will not flow outside.

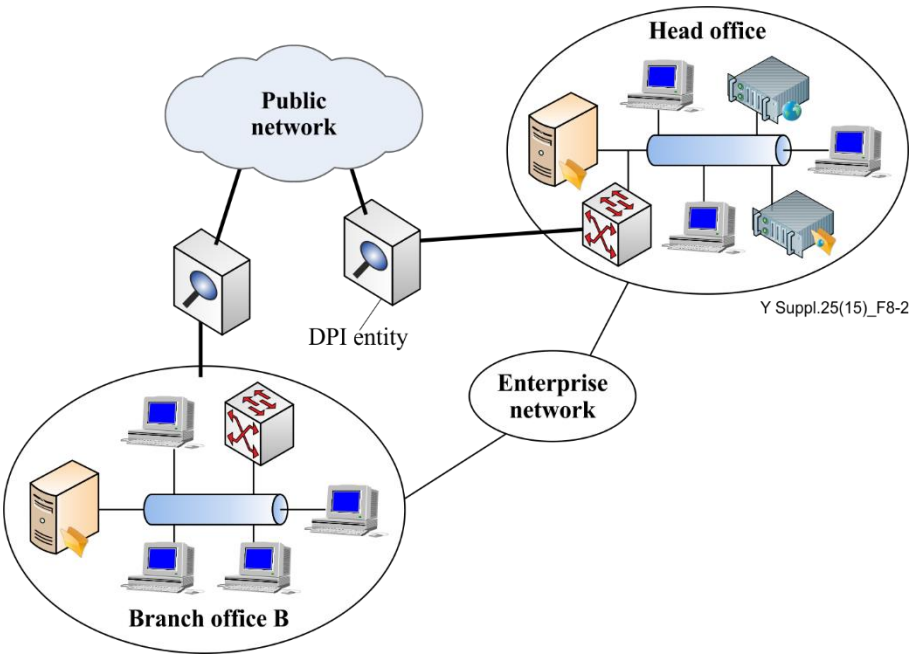

Figure 8-2 – Example of DPI and enterprise information security

8.2 Use DPI to improve internal resources utility of the enterprise network

Figure 8-3 illustrates the case in which DPI technology assists the scheduling of internal resources. DPI entities are deployed between edge routers and internal network segments. Then every flow coming from the internal network is identified by DPI entities, and network resources are allocated based on the results identified.

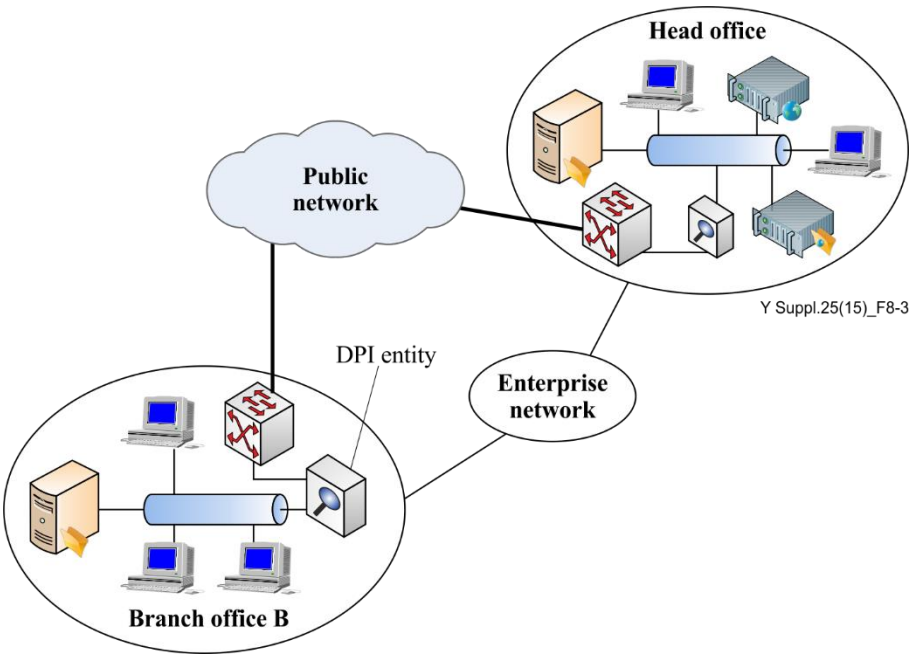

Figure 8-3 – Example of DPI and resource use improvement

8.3 Enterprise internal management optimization

DPI technology can also be used to make the enterprise office automation more effective. Figure 8-4 describes an example of such application scenario. DPI entities can be placed between an internal application server and the network devices (switch, router, etc.) to identify the data flow accessing the application server. The internal workflow can then be analysed based on the results identified.

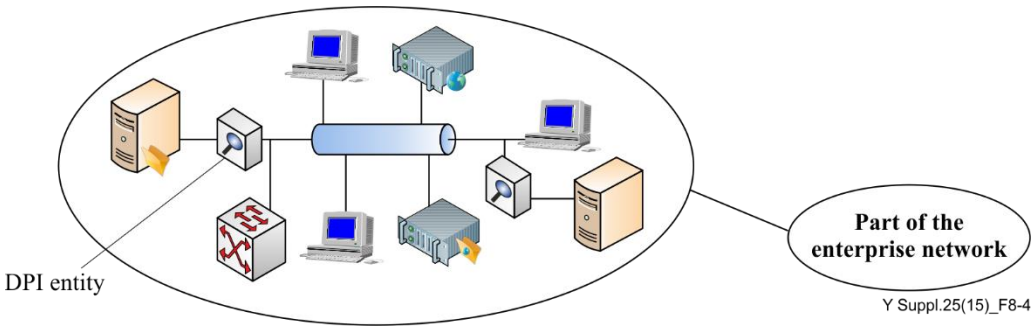

Figure 8-4 – Example of DPI and office automation optimization

9 Application scenario of deep packet inspection in SDN

9.1 SDN defined by ITU-T and ONF

ITU-T SDN is defined in [ITU-T Y.3300]:

"**software-defined networking**: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner."

9.2 SDN defined by ONF

ONF SDN is defined in [b-ONF SDN]:

"Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services."

According to [ITU-T Y.2770], DPI is used to identify the application unambiguously. As described above, DPI is deployed in evolving networks for application identification, reporting, measurements and traffic optimization, which means DPI is seeking to make the network application-aware (e.g., application identification, application measurement, application optimization, etc.).

On the contrary, software-defined networking is aiming at separating network control functions from physical network elements (related to packet processing only) and enable the network to be treated as programmable resource to applications, which means SDN is seeking to make the application network-aware.

The example application scenario of deep packet inspection in extended ONF SDN is shown in Figure 9-1, which is based on ONF SDN architecture [b-ONF SDN] with DPI extension. Application requirements such as application signature, end-to-end transport capacity, packet transfer delay, packet delay variation, packet loss rate, etc., are transferred to the control layer by API interfaces. Based on the current network resource status and route generating methods, network services with DPI PD-FE distribute ONF flow tables with flow layer information and application layer information to the network devices located in infrastructure layer through the control/data plane interfaces. The ONF flow table consists of flow entries [b-OpenFlow]. Each flow table entry of ONF contains:

– match fields: to match against packets. These consist of the ingress port and packet headers, and optionally metadata specified by a previous table.
– priority: matching precedence of the flow entry.
– counters: updated when packets are matched.
– instructions: to modify the action set or pipeline processing.

– timeouts: maximum amount of time or idle time before flow is expired by the switch.

– cookie: opaque data value chosen by the controller. May be used by the controller to filter flow statistics, flow modification and flow deletion. Not used when processing packets.

It can be seen that the ONF flow table entry is similar to the DPI policy rule defined in clause 3.2.13 of [ITU-T Y.2770], e.g., the match fields are similar to the DPI policy conditions and the instructions are similar to the DPI actions. The arriving packets are matched against the ONF flow table (see clause 5 of [b-OpenFlow]) with packet header information and application descriptor information by DPI FE, and the corresponding matched packets are forwarded to the appropriate next hop. Flow and application tag (see clause 3.2.3 in [ITU-T Y.2770]) will also be reported to the control layer and application layer for further decision and scheduling.

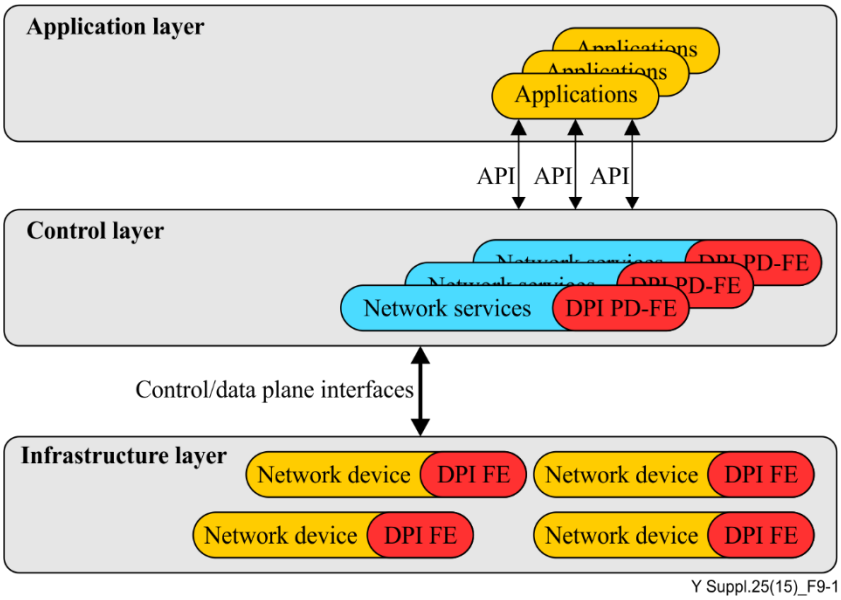

Figure 9-1 – Example application scenario of deep packet inspection in extended ONF SDN

The match fields of ONF SDN flow table defined in [b-OpenFlow] need to been extended to include application payload conditions except L2-L4 header information. An example ONF SDN flow table extension is shown in Figure 9-2.

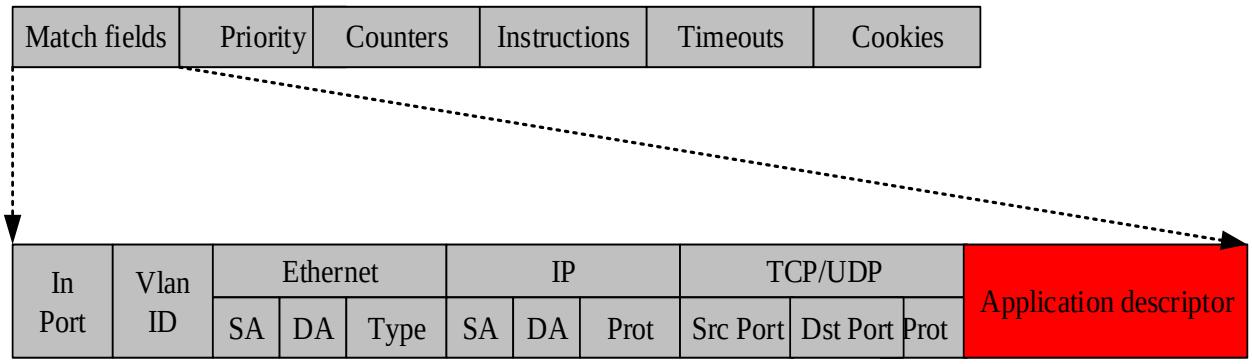

Figure 9-2 – Example ONF SDN flow table extension with application descriptor

10 Security considerations

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

According to [ITU-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 Y.2012] Recommendation ITU-T Y.2012 (2004), *Functional requirements and architecture of the NGN*.

[b-ITU-T Y.3021] Recommendation ITU-T Y.3021 (2012), *Framework of energy saving for future networks*.

[b-BBF BPCF] Broadband Forum TR-134 (2012), *Broadband Policy Control Framework (BPCF), Issue: 1*.

[b-IETF RFC 2330] IETF RFC 2330 (1998), *Framework for IP Performance Metrics*.

[b-IETF RFC 2678] IETF RFC 2678 (1999), *IPPM Metrics for Measuring Connectivity*.

[b-IETF RFC 2679] IETF RFC 2679 (1999), *A One-way Delay Metric for IPPM*.

[b-IETF RFC 2680] IETF RFC 2680 (1999), *A One-way Packet Loss Metric for IPPM*.

[b-IETF RFC 2681] IETF RFC 2681 (1999), *A Round-trip Delay Metric for IPPM*.

[b-IETF RFC 2784] IETF RFC 2784 (2000), *Generic Routing Encapsulation (GRE)*.

[b-IETF RFC 3577] IETF RFC 3577 (2003), *Introduction to the Remote Monitoring (RMON) Family of MIB Modules*.

[b-IETF RFC 4710] IETF RFC 4710 (2006), *Real-time Application Quality-of-Service Monitoring (RAQMON) Framework*.

[b-ONF SDN] The ONF SDN Defined.
<https://www.opennetworking.org/sdn-resources/sdn-definition>

[b-OpenFlow] OpenFlow Switch Specification Version 1.3.1.
<https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.1.pdf>

[b-Graham] CRTC 2009, *Graham, F., ISP Traffic Management Technologies: The State of the Art, January 2009*.

[b-PCMM] CableLabsPKT-SP-MM-I05-091029 (2009), *Multimedia Specification, I05* – Released October 29, 2009.

[b-PEEM] Open Mobile Alliance, PEEM (2008), *Policy Evaluation, Enforcement and Management Architecture,* Candidate Version 1.0-05 Aug 2008.

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	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**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015