

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2774

(03/2019)

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ
ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА
ИНТЕРНЕТ, СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ,
ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА

Сети последующих поколений – Безопасность

Функциональные требования углубленной проверки пакетов в будущих сетях

Рекомендация МСЭ-Т Y.2774

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ МЕЖСЕТЕВОГО ПРОТОКОЛА, СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ, ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

Общие положения	Y.100–Y.199
Услуги, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899

АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ

Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
IPTV по NGN	Y.1900–Y.1999

СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности услуг и архитектура услуг	Y.2200–Y.2249
Аспекты обслуживания: взаимодействие услуг и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Пакетные сети	Y.2600–Y.2699

Безопасность Y.2700–Y.2799

Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999

БУДУЩИЕ СЕТИ

	Y.3000–Y.3499
--	---------------

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

	Y.3500–Y.3999
--	---------------

ИНТЕРНЕТ ВЕЩЕЙ И "УМНЫЕ" ГОРОДА И СООБЩЕСТВА

Общие положения	Y.4000–Y.4049
Определения и терминология	Y.4050–Y.4099
Требования и сценарии использования	Y.4100–Y.4249
Инфраструктура, возможность установления соединений и сети	Y.4250–Y.4399
Структуры, архитектуры и протоколы	Y.4400–Y.4549
Услуги, приложения, вычисления и обработка данных	Y.4550–Y.4699
Управление, контроль и рабочие характеристики	Y.4700–Y.4799
Идентификация и безопасность	Y.4800–Y.4899
Анализ и оценка	Y.4900–Y.4999

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Функциональные требования углубленной проверки пакетов в будущих сетях

Резюме

В Рекомендации МСЭ-Т Y.2774 определены функциональные требования углубленной проверки пакетов в будущих сетях (например, сетях с программируемыми параметрами (SDN), сетях с виртуализацией сетевых функций (NFV) и т. д.). В сферу применения настоящей Рекомендации входят общие требования углубленной проверки пакетов (DPI) в будущих сетях, функциональные требования DPI в SDN, функциональные требования DPI в сетях NFV, функциональные требования DPI при создании цепочек функций услуг (SFC) и DPI как услуги, а также функциональные требования DPI при виртуализации сетей и функциональные требования DPI в развивающихся сетях подвижной связи.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Y.2774	14.03.2019 г.	13-я	11.1002/1000/13495

Ключевые слова

Углубленная проверка пакетов, функциональные требования, будущие сети.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: <http://handle.itu.int/>, после которого следует уникальный идентификатор Рекомендации. Например, <http://handle.itu.int/11.1002/1000/11830-en>.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы.

Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: <http://www.itu.int/ITU-T/ipr/>.

© ITU 2019

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

Содержание

		Стр.
1	Сфера применения	1
2	Справочные документы	1
3	Определения	2
	3.1 Термины, определенные в других документах	2
	3.2 Термины, определенные в настоящей Рекомендации	3
4	Сокращения и акронимы	3
5	Соглашения по терминологии	3
6	Общие требования углубленной проверки пакетов в будущих сетях	4
7	Функциональные требования DPI в SDN	5
	7.1 Обзор DPI в контексте SDN	5
	7.2 Функциональные требования DPI в SDN внутри объекта	5
	7.3 Функциональные требования DPI в SDN на уровне объекта	6
	7.4 Функциональные требования DPI в SDN на уровне сети	6
8	Функциональные требования DPI в сетях NFV	7
	8.1 Функциональные требования DPI в сетях NFV внутри объекта	7
	8.2 Функциональные требования DPI в сетях NFV на уровне объекта	7
	8.3 Функциональные требования DPI в сетях NFV на уровне сети	8
9	Функциональные требования DPI при создании цепочек услуг и DPI как услуги	8
	9.1 Обзор создания цепочек услуг и DPI как услуги	8
	9.2 Функциональные требования DPI при DPI как услуге и создании цепочек услуг	9
10	Функциональные требования DPI в контексте виртуализации сети	10
	10.1 Обзор DPI в контексте виртуализации сети	10
	10.2 Функциональные требования к уровню пользователя	10
	10.3 Функциональные требования к уровню управления	11
	10.4 Функциональные требования к уровню администрирования	11
11	Функциональные требования DPI в развивающихся сетях подвижной связи	11
	11.1 Внедрение развивающихся сетей подвижной связи	11
	11.2 Общие требования к развертыванию DPI в развивающихся сетях подвижной связи	11
	11.3 Требования к интерфейсу при развертывании DPI в развивающихся сетях подвижной связи	12
	11.4 Требования к протоколу при развертывании DPI в развивающейся сети подвижной связи	12
12	Вопросы безопасности	13
13	Прочие соображения	13
	Библиография	14

Функциональные требования углубленной проверки пакетов в будущих сетях

1 Сфера применения

В настоящей Рекомендации определены функциональные требования углубленной проверки пакетов (DPI) в будущих сетях (например, сетях с программируемыми параметрами, виртуализацией сетевых функций и т. д.). В сферу применения настоящей Рекомендации входят:

- a) общие требования углубленной проверки пакетов в будущих сетях;
- b) функциональные требования DPI в сетях с программируемыми параметрами;
- c) функциональные требования DPI при виртуализации сетевых функций;
- d) функциональные требования DPI при цепочках функций услуг и DPI как услуге;
- e) функциональные требования DPI при виртуализации сети;
- f) функциональные требования DPI в развивающихся сетях подвижной связи.

Пользователи Рекомендации и лица, использующие описанные механизмы, должны соблюдать все применимые национальные и региональные законы, нормы и правила. Механизмы, описанные в настоящей Рекомендации, могут не применяться к международной корреспонденции во избежание нарушения секретности и суверенных национальных правовых требований, предъявляемых к электросвязи, но они должны соответствовать Уставу и Конвенции МСЭ.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все рекомендации и другие источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации

- [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] Рекомендация МСЭ-Т Y.2704 (2010 г.), *Механизмы и процедуры безопасности для сетей последующих поколений.*
- [ITU-T Y.2770] Рекомендация МСЭ-Т Y.2770 (2012 г.), *Требования к углубленной проверке пакетов в сетях последующих поколений.*
- [ITU-T Y.2771] Рекомендация МСЭ-Т Y.2771 (2014 г.), *Структура углубленной проверки пакетов.*
- [ITU-T Y.3001] Рекомендация МСЭ-Т Y.3001 (2011 г.), *Будущие сети: целевые установки и цели проектирования.*

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 углубленная проверка пакетов (deep packet inspection (DPI)) [ITU-T Y.2770]: Проводимый в соответствии с базовой эталонной моделью взаимодействия открытых систем (OSI-BRM) [ITU-T X.200], предусматривающей уровневую архитектуру протокола, анализ:

- свойств полезной нагрузки и/или пакетов (см. перечень возможных свойств в пункте 3.2.11 [ITU-T Y.2770]), более глубокий, чем информация заголовка на уровнях 2, 3 или 4 (L2/L3/L4) протокола;
- других свойств пакета в целях однозначного определения приложения.

ПРИМЕЧАНИЕ. – Результат применения функции DPI, наряду с некоторой дополнительной информацией, например информацией о потоке, как правило, используется в последующих функциях, таких как представление отчета, или в действиях в отношении пакета.

3.1.2 ядро DPI (DPI engine) [ITU-T Y.2770]: Подкомпонент и главная часть функционального объекта DPI, которая выполняет все функции обработки в тракте передачи пакета (например, идентификацию пакета и другие функции обработки пакета, показанные на рисунке 6-1 [ITU-T Y.2770]).

3.1.3 узел DPI (DPI node) [ITU-T Y.2771]: Сетевой элемент или устройство, реализующее функции, связанные с DPI. Таким образом, это общий термин, который используется для обозначения реализации физического объекта DPI.

ПРИМЕЧАНИЕ. – Функциональный аспект: функция узла DPI (DPI-NF) включает функцию реализации политики DPI (DPI-PEF) и (факультативно) локальную функцию принятия решений в соответствии с политикой (L-PDF), следовательно, DPI-NF функционально эквивалентна функциональному объекту DPI.

3.1.4 будущая сеть (FN) (future Network (FN)) [ITU-T Y.3001]: Сеть, способная обеспечить услуги, возможности и средства, которые сложно обеспечить с использованием существующих сетевых технологий. Будущей сетью является либо:

- a) новая компонентная сеть или усовершенствованный вариант существующей компонентной сети, либо
- b) разнородная группа новых компонентных сетей или группа, состоящая из новых и существующих компонентных сетей, которая работает как единая сеть.

3.1.5 цепочка функций услуг (service function chain) [b-ITU-T Y-Sup.41]: Цепочка, определяющая упорядоченный набор абстрактных функций услуг и ограничений упорядочения, которые должны применяться к пакетам и/или кадрам и/или потокам, выбранным в результате классификации и/или в соответствии с политикой.

3.1.6 функция услуги (service function) [b-ITU-T Y-Sup.41]: Функция, представляющая конкретную функцию сетевой услуги, которая отвечает за определенную обработку принятых пакетов, и отличающаяся от обычных стандартных функций IP-маршрутизатора (например, функции IP-пересылки и IP-маршрутизации) в сетевом тракте между хостом-источником и хостом-получателем.

ПРИМЕЧАНИЕ. – Функция услуги может действовать на разных уровнях стека протоколов (например, на сетевом уровне или других уровнях ВОС). В качестве логического компонента такая функция может быть реализована как виртуальный элемент или встроена в физический сетевой элемент. В один и тот же сетевой элемент могут быть встроены одна или несколько функций услуги. В одном и том же административном домене может существовать несколько экземпляров функции услуги.

3.1.7 создание цепочек функций услуг (service function chaining) [b-ITU-T Y-Sup.41]: Механизм построения цепочек функций услуг и пересылки пакетов/кадров/потоков между ними.

3.1.8 метаданные (metadata) [b-IETF RFC 7665]: Обеспечивают возможность обмена контекстной информацией между классификаторами и SF и между SF.

3.1.9 администратор VNF (VNF manager) [b-ETSI GS NFV-MAN 001]: Управление жизненным циклом экземпляров VNF; функция общей координации и адаптации конфигурации и составления отчетов о событиях между инфраструктурой виртуализации сетевых функций (NFVI) и системой управления элементами/системой управления сетью (EMS/NMS).

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

API	Application Program Interface	Интерфейс прикладных программ
DPI	Deep Packet Inspection	Углубленная проверка пакетов
DPI-FE	DPI Functional Entity	Функциональный объект DPI
DPI-PEF	DPI Policy Enforcement Function	Функция реализации политики DPI
DPI-PIB	DPI Policy Information Base	Информационная база политики DPI
EMS	Element Management System	Система управления элементами
FN	Future Networks	Будущие сети
PFF	Packet Forwarding Function	Функция пересылки пакетов
GPRS	General Packet Radio Service	Служба пакетной радиосвязи общего пользования
GTP	GPRS Tunnelling Protocol	Протокол туннелирования GPRS
L-PDF	Local Policy Decision Function	Локальная функция принятия решений в соответствии с политикой
MME	Mobility Management Entity	Объект управления мобильностью
NFV	Network Function Virtualization	Виртуализация сетевых функций
NFVI	Network Function Virtualization Infrastructure	Инфраструктура виртуализации сетевых функций
NMS	Network Management System	Система управления сетью
P-GW	Packet data network Gate Way	Шлюз сети пакетной передачи данных
PIB	Policy Information Base	Информационная база политики
QoE	Quality of Experience	Оценка качества услуг пользователем
QoS	Quality of Service	Качество обслуживания
RAN	Radio Access Network	Сеть радиодоступа
SDN	Software Defined Network	Сеть с программируемыми параметрами
SC	Service Chaining	Создание цепочек услуг
SCTP	Stream Control Transmission Protocol	Протокол передачи с управлением потоком
SFC	Service Function Chaining	Создание цепочек функций услуг
S-GW	Service Gateway	Служебный шлюз
UDP	User Datagram Protocol	Протокол дейтаграмм пользователя
VNF	Virtual Network Function	Функция виртуальной сети
vDPI	virtual Deep Packet Inspection	Виртуальная углубленная проверка пакетов

5 Соглашения по терминологии

В настоящей Рекомендации используются следующие соглашения по терминологии.

Термин "требуется" или "должен" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

Термин "рекомендуется" означает требование, которое рекомендуется к соблюдению, но не является абсолютно необходимым. Таким образом, для заявления о соответствии настоящему документу данное требование не является обязательным.

6 Общие требования углубленной проверки пакетов в будущих сетях

Определение термина "будущая сеть" приведено в пункте 3.1. Из этого определения однозначно следует, что "будущая сеть" не означает конкретную сетевую архитектуру. По существу, под будущими сетями подразумевается созданная с использованием одной или нескольких новых сетевых архитектур и технологий сеть, способная обеспечить услуги, возможности и средства, которые сложно обеспечить в современных сетях. Иными словами, будущие сети – это сети, которые разработаны в соответствии с группой передовых сетевых архитектур, используют группу передовых сетевых технологий и предоставляют более качественные услуги. В целом будущая сеть, независимо от используемой архитектуры или технологии, должна обладать следующими свойствами: открытость, расширяемость, гибкость, безопасность и экологичность.

Углубленная проверка пакетов (DPI) будет играть ключевую роль в будущих сетях в качестве технологии сети базовой инфраструктуры. При создании будущих сетей необходимо учитывать следующие новые требования к технологиям, связанным с углубленной проверкой пакетов.

- При внедрении функций DPI в будущих сетях требуется сохранять исходную сетевую архитектуру.
- При внедрении функций DPI в будущих сетях рекомендуется сохранять свойства открытости, расширяемости, гибкости, безопасности и экологичности целевой сети, не ухудшая ни одно из этих свойств.

Открытость, расширяемость, гибкость, безопасность и экологичность – это не только свойства будущих сетей, но и движущие силы повышения качества сетевых услуг. Следовательно, в случае внедрения определенной технологии или метода полезно сохранять открытость, расширяемость, гибкость, безопасность и экологичность. Вместе с тем, как правило, сложно сохранить все функции на первоначальном уровне, и именно по этой причине указанное выше требование носит рекомендательный характер.

- При внедрении функций DPI в будущих сетях требуется гарантировать соблюдение пороговых значений характеристик.

При внедрении функций DPI в будущих сетях требуется обеспечивать соответствие эксплуатационным требованиям, определяемым каждой сетью. Спецификация эксплуатационных требований для каждой сети не входит в сферу применения настоящей Рекомендации.

Например, если сеть требует, чтобы сквозная задержка не превышала 50 мс, то такая задержка должна оставаться на уровне менее 50 мс даже в случае развертывания в этой сети функций DPI.

Кроме того, углубленная проверка пакетов может расширить возможности по обеспечению осведомленности о приложениях/услугах в будущей сети, а также гарантировать высокое качество обслуживания (QoS) и оценку качества услуг пользователями (QoE). С другой стороны, будущие сети являются ориентированными на услуги/приложения сетями, основанными на функции осведомленности о приложениях/услугах, поэтому целесообразна углубленная проверка пакетов, ориентированная на приложения/услуги. В будущих сетях необходимо выполнять следующие общие функциональные требования DPI.

- Требуется, чтобы DPI в будущих сетях поддерживала возможность однозначной идентификации приложений на основе DPI. В прошлом приложения идентифицировались по информации протокола уровня 3 и информации порта уровня 4. Однако современные приложения часто произвольным образом изменяют свои порты протокола и протоколы (например, приложение с использованием динамических портов; спам и черви, маскирующиеся под другое хорошо известное SMTP-приложение), и все больше приложений переводится на веб-услуги (например, приложения, работающие через веб-страницы: игры на веб-странице, видео на веб-странице с тем же портом 80). При углубленной проверке пакетов приложения можно идентифицировать с помощью свойства подписи приложения, что позволяет сделать функцию DPI-идентификации приложений основным конструктивным блоком для будущих сетей.

- Требуется, чтобы DPI в будущих сетях поддерживала планирование и оптимизацию трафика приложений на основе действий, определенных в правилах политики DPI. К этим действиям, в частности, относятся:
 - 1) прием и пересылка трафика приложений в объект функции пересылки пакетов (PFF);
 - 2) пересылка трафика приложений в объект функции принятия решения в соответствии с политикой DPI;
 - 3) обработка трафика приложений в соответствии с политикой DPI [например, ограничение спама и другого неправомерного трафика];
 - 4) перенаправление трафика приложений на другой интерфейс;
 - 5) зеркальное отображение трафика приложений на другой интерфейс;
 - 6) учет статистики трафика в соответствии с правилом политики DPI.
- Рекомендуется, чтобы DPI в будущих сетях поддерживала разделение функций принятия решений в соответствии с политикой DPI и реализации политики DPI. Существует локальная функция принятия решений в соответствии с политикой (L-PDF) и внешняя функция принятия решений в соответствии с политикой DPI. Поскольку для будущих сетей (например, SDN) характерно централизованное управление, рекомендуется, чтобы DPI в будущих сетях поддерживала разделение таких функций, как принятие решений в соответствии с политикой DPI и реализация политики DPI.
- Рекомендуется, чтобы DPI в будущих сетях поддерживала возможность программизации в отношении идентификации, планирования и оптимизации трафика приложений на основе DPI. Приложения могут инициировать и передавать правила политики DPI в объекты реализации политики DPI благодаря возможности программизации и интерфейсу прикладных программ (API), предоставляемому функциональным объектом принятия решений в соответствии с политикой DPI.

7 Функциональные требования DPI в SDN

7.1 Обзор DPI в контексте SDN

Архитектура SDN, как правило, разрабатывается как трехуровневая структура следующим образом.

- Уровень ресурсов – состоит из группы сетевых устройств, которые выполняют функции пересылки данных.
- Уровень управления SDN – состоит из одного или нескольких контроллеров, управляющих вышеупомянутыми сетевыми устройствами.
- Уровень приложения – состоит из определенных программных компонентов, которые получают доступ к сетевым ресурсам или планируют их с помощью вышеупомянутых контроллеров.

SDN обладает следующими тремя основными свойствами:

- функция управления изолирована от функции пересылки данных;
- функции управления логически централизованы;
- применяются открытые приложения.

В контексте SDN для выполнения функций, связанных с DPI, можно опираться на объекты всех трех уровней. Кроме того, DPI, развернутая в контексте SDN, также обладает вышеуказанными основными свойствами.

7.2 Функциональные требования DPI в SDN внутри объекта

- Рекомендуется, чтобы таблица правил политики в функциональном объекте DPI поддерживала функции тайм-аута, и при истечении срока действия одного или нескольких правил политики данный функциональный объект DPI должен сообщать об этом соответствующим контроллерам.
- Рекомендуется, чтобы таблица правил политики в функциональном объекте DPI поддерживала функции счета и чтобы данные счетчика могли извлекаться соответствующим контроллером или системой управления.

- Рекомендуется, чтобы таблица правил политики в функциональном объекте DPI поддерживала функции установления приоритетности правил, тем временем приоритет, относящийся к правилам политики, может устанавливаться соответствующим контроллером.
- Требуется, чтобы L-PDF в функциональном объекте DPI обменивалась данными правил политики и другими данными с одним или несколькими контроллерами.
- Требуется, чтобы информационная база политики DPI (DPI-PIB) в функциональном объекте DPI предоставляла правила политики для принятия решений о действиях функции реализации политики DPI (DPI-PEF) при установлении соединений между этим функциональным объектом DPI и контроллером (контроллерами).
- Когда функциональный объект DPI находится в контексте SDN, требуется, чтобы локальная функция принятия решений на основе политики в этом объекте не изменяла PIB без команды соответствующего контроллера, даже если соединение между данным объектом и контроллером прерывается.
- Рекомендуется, чтобы функциональный объект DPI поддерживал несколько таблиц правил политики. Таблицы правил политики обрабатываются по порядку. Следует отметить, что результаты обработки таблицы правил политики служат входными данными для обработки следующей таблицы правил политики.

7.3 Функциональные требования DPI в SDN на уровне объекта

- Требуется, чтобы функциональный объект DPI (DPI-FE) поддерживал некоторый нисходящий (так называемый южный) интерфейс, используемый для обмена данными правил политики и другими данными с одним или несколькими контроллерами.
- Требуется, чтобы функциональный объект DPI имел возможность устанавливать соединение с одним или несколькими контроллерами через вышеупомянутый нисходящий интерфейс.
- Требуется, чтобы функциональный объект DPI пересылал все входящие пакеты, когда он используется в качестве узла DPI в тракте сети с архитектурой SDN, пока не установлено соединение между DPI-FE и соответствующим контроллером.
- Требуется, чтобы функциональный объект DPI сохранял информацию PIB при нарушении связи между DPI-FE и контроллером.
- Рекомендуется, чтобы функциональный объект DPI поддерживал одновременно два или несколько контроллеров.

7.4 Функциональные требования DPI в SDN на уровне сети

7.4.1 Требования к обслуживанию PIB

- Требуется, чтобы контроллер имел возможность поддерживать PIB всех объектов DPI, управляемых этим контроллером.
- Требуется, чтобы контроллер имел возможность восстанавливать PIB каждого объекта DPI в случае отказа PIB этого объекта.
- Если для управления одной и той же сетью DPI используются несколько контроллеров, то требуется, чтобы эти контроллеры взаимодействовали в целях поддержки одной и той же PIB, независимо от принятого в них метода синхронизации.

7.4.2 Логический канал связи между объектом DPI и соответствующим контроллером

- Если необходимо, чтобы логический канал связи между объектом DPI A и соответствующим контроллером проходил через объект DPI B, объект DPI B должен иметь возможность взаимодействия с другими объектами DPI для установления такого логического канала связи.
- Если логический канал связи между объектом DPI A и соответствующим контроллером включает объект DPI B, объект DPI B должен иметь возможность обеспечить надежное прохождение через него управляющих сообщений, передаваемых между объектом DPI A и соответствующим контроллером.

7.4.3 Взаимодействие нескольких объектов DPI

- Если для реализации функции DPI необходимы два или более объектов DPI, управляющий ими контроллер должен координировать выполнение вышеуказанными объектами функции DPI.

7.4.4 Функция двунаправленной DPI, реализованная двумя объектами DPI

- Если функция двунаправленной DPI выполняется двумя независимыми объектами DPI и оба этих объекта управляются одним и тем же контроллером, такой контроллер должен координировать выполнение функций двунаправленной DPI двумя объектами DPI.
- Если функция двунаправленной DPI выполняется двумя независимыми объектами DPI и эти объекты управляются двумя разными контроллерами, такие контроллеры должны взаимодействовать для координации выполнения функций двунаправленной DPI двумя объектами DPI.

7.4.5 Отказ контроллера

- При выходе из строя контроллера, который является единственным контроллером в соответствующей сети DPI, требуется, чтобы объекты DPI в этой сети сохраняли обычное состояние без изменений до восстановления контроллера.
- Если сеть DPI управляют несколько контроллеров и один из них выходит из строя, требуется, чтобы другие контроллеры имели возможность взять на себя функции отказавшего контроллера.

8 Функциональные требования DPI в сетях NFV

8.1 Функциональные требования DPI в сетях NFV внутри объекта

Функциональный объект DPI в контексте NFV называется функциональным объектом DPI NFV, реализуемым одной или несколькими функциями виртуальной сети (VNF), например функциональный объект DPI NFV, который состоит из трех VNF. Первая VNF выполняет функции ядра DPI, вторая – функции L-PDF, а третья отвечает за PIB DPI.

К функциональному объекту DPI NFV относятся следующие требования.

- Требуется, чтобы функциональный объект DPI NFV включал в себя ядро DPI, DPI-PIB и L-PDF, а также некоторые внутренние или внешние интерфейсы.
- Если функциональный объект DPI NFV реализуется одной VNF, требуется, чтобы эта VNF реализовывала все компоненты функционального объекта DPI (ядро DPI, DPI-PIB, L-PDF и т. д.).
- Если функциональный объект DPI NFV состоит из двух или более VNF, рекомендуется, чтобы все VNF имели равную производительность в том случае, когда одна VNF с более низкой производительностью влияет на VNF с более высокой производительностью.
- Если функциональный объект DPI NFV состоит из двух или более VNF, требуется, чтобы ему выделялись достаточные ресурсы для надежного и своевременного обмена данными между этими NFV.
- Если планируется, что VNF должна выполнять функции DPI, требуется, чтобы она выполняла только функции DPI и не зависела от других VNF.

8.2 Функциональные требования DPI в сетях NFV на уровне объекта

- Требуется, чтобы функциональный объект DPI NFV поддерживал некоторый интерфейс, используемый для обмена данными по управлению политикой и другими данными с одним или несколькими администраторами NFV.
- Требуется, чтобы функциональный объект DPI NFV имел возможность устанавливать соединение с одним или несколькими администраторами NFV через вышеупомянутый интерфейс.
- Требуется, чтобы функциональный объект DPI NFV, когда он используется в контексте сети NFV, обменивался входящими пакетами с инфраструктурой NFV.

- Требуется, чтобы функциональный объект DPI NFV сохранял информацию по управлению политикой, когда соединение между этим объектом и администратором VNF прерывается или когда администратор VNF выходит из строя.
- Рекомендуется, чтобы функциональный объект DPI NFV поддерживал одновременно два или несколько администраторов NFV.

8.3 Функциональные требования DPI в сетях NFV на уровне сети

- Если для работы функции DPI требуются два или более функциональных объекта DPI NFV, требуется, чтобы администраторы VNF, осуществляющие управление VNF (эти VNF реализуют вышеупомянутые функциональные объекты DPI NFV), координировали выполнение VNF этих функций.
- Если функция двунаправленной DPI выполняется двумя независимыми функциональными объектами DPI NFV и оба эти объекта управляются одним и тем же администратором NFV, требуется, чтобы такой администратор координировал выполнение функций двунаправленной DPI двумя функциональными объектами DPI NFV.
- Если функция двунаправленной DPI выполняется двумя независимыми функциональными объектами DPI NFV и эти два объекта управляются двумя разными администраторами NFV, требуется, чтобы такие администраторы взаимодействовали для координации выполнения функций двунаправленной DPI двумя функциональными объектами DPI NFV.

9 Функциональные требования DPI при создании цепочек услуг и DPI как услуги

9.1 Обзор создания цепочек услуг и DPI как услуги

Создание цепочек функций услуг (SFC) – это новая архитектура, разрабатываемая в IETF [b IETF RFC 7665]. Создание цепочек услуг (SC) – это новый набор технологий и процессов, которые позволяют операторам динамически настраивать сетевые услуги в программном обеспечении без необходимости внесения изменений в сеть на аппаратном уровне.

Функции DPI также могут разрабатываться как общие функции почти для всех функций услуг в цепочке услуг, работающей с протоколами L2–L7. Иными словами, DPI развертывается на основе архитектуры DPI как услуги. На рисунке 9-1 показана архитектура DPI как услуги или функции DPI для цепочки услуг. На рисунке 9-1 функцию DPI для узла функции услуги 1, узла функции услуги 2, узла функции услуги 3 и т. д. обеспечивает левый или правый узел услуги DPI.

DPI как услуга означает, что функции DPI предоставляются в сети другими сетевыми модулями в качестве функции услуги. Поэтому в архитектуре DPI как услуги функция DPI может совместно использоваться различными сетевыми модулями. Трафик должен сканироваться только один раз, и при этом одноразовом сканировании могут обрабатываться данные всех функций услуг в цепочке услуг. Затем услуга DPI передает результаты сканирования соответствующим экземплярам функции услуги. Развертывание функций DPI на основе архитектуры DPI как услуги имеет значительные преимущества в части производительности, масштабируемости, надежности.

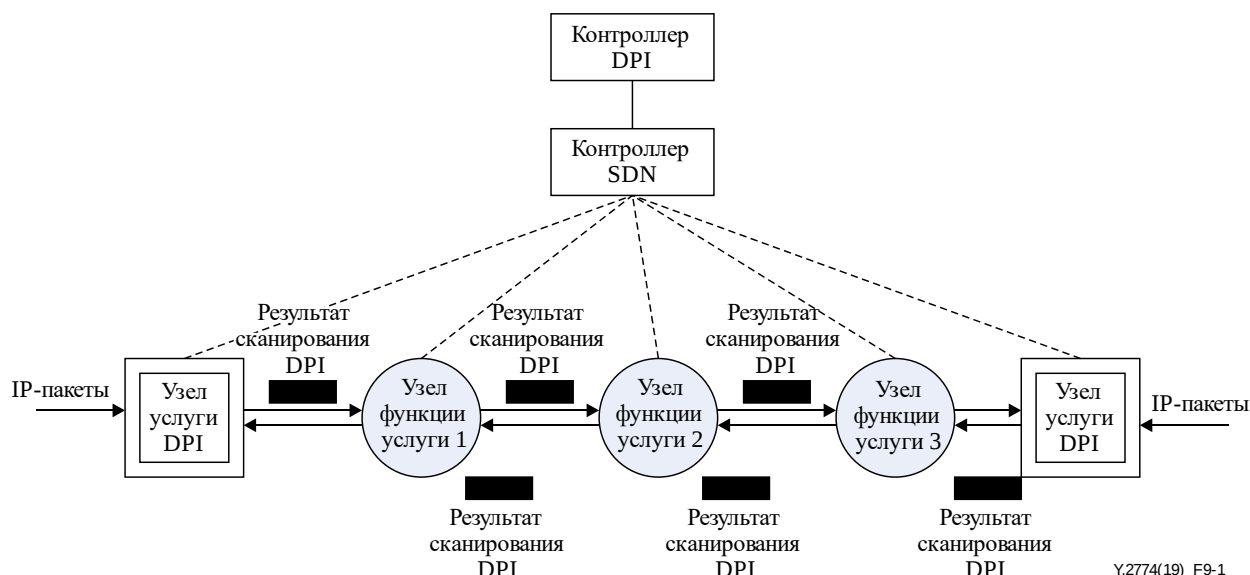


Рисунок 0-1 – Услуга DPI в цепочке услуг

9.2 Функциональные требования DPI при DPI как услуге и создании цепочек услуг

9.2.1 Требования классификации при DPI как услуге

- Требуется, чтобы функциональный объект DPI поддерживал некоторый интерфейс, используемый для обмена данными правил классификации и другими данными с одним или несколькими контроллерами.
- Требуется, чтобы функциональный объект DPI имел возможность устанавливать соединение с одним или несколькими контроллерами через интерфейс, используемый для обмена данными правил классификации и другими данными.
- Требуется, чтобы функциональный объект DPI имел возможность сохранять PIV без изменений, когда соединение между вышеуказанным объектом и соответствующими контроллерами прерывается.
- Требуется, чтобы функциональный объект DPI имел возможность обеспечивать функцию классификации в соответствии с полями L2–L7 пакетов.
- Рекомендуется, чтобы функциональный объект DPI поддерживал одновременно два или несколько контроллеров.
- Рекомендуется, чтобы функциональный объект DPI поддерживал полную классификацию приложений и извлечение метаданных.

9.2.2 Общие функциональные требования к DPI как услуге

- Требуется, чтобы функциональный объект DPI предшествовал любым другим функциям услуг, для которых требуются функции DPI.
- Рекомендуется, чтобы функциональный объект DPI сканировал пакеты и журналы всех обнаруженных шаблонов в виде метаданных к пакетам.
- Рекомендуется, чтобы контроллер DPI представлял собой логически централизованный объект, роль которого заключается в управлении процессом DPI по всей сети, а также в поддержании связи с контроллером SDN.
- Требуется, чтобы функции услуг, использующие услуги DPI, регистрировали свой набор шаблонов в контроллере DPI.
- Рекомендуется, чтобы контроллер DPI имел возможность производить регистрацию узлов DPI и управлять узлами DPI.

- Требуется, чтобы контроллер DPI имел возможность инициализировать экземпляры услуги DPI и развертывать другие экземпляры услуги DPI в сети.
- Требуется, чтобы контроллер DPI имел возможность управлять ресурсами экземпляров DPI, распределять экземпляры, удалять экземпляры услуг и переносить потоки между экземплярами.
- Передача результатов сопоставления с шаблоном узлу функции услуги не должна мешать пересылке пакета по цепочке узлов функции услуги, а затем в пункт назначения.
- Процесс передачи результатов сопоставления с шаблоном узлу функции услуги должен соответствовать следующим сценариям:
 - 1) переменный размер метаданных;
 - 2) переменное число результатов сопоставления;
 - 3) неизвестные заранее значения вышеуказанных размера и числа.
- Процесс передачи результатов сопоставления с шаблоном узлам функции услуги не должен зависеть от узлов функции услуги, не имеющих отношения к услуге DPI.

10 Функциональные требования DPI в контексте виртуализации сети

10.1 Обзор DPI в контексте виртуализации сети

Одной из основных особенностей виртуализации сети является то, что физическая сеть может быть виртуализирована в одну или несколько логических сетей. Другими словами, при том что реально существует только определенная физическая сеть, с разных точек зрения разных пользователей или разных услуг она может рассматриваться как одна или несколько независимых логических сетей. Например, физическая локальная сеть может быть виртуализирована в 4096 виртуальных локальных сетей. Виртуализация сети также означает, что физические ресурсы в физической сети могут виртуализироваться в логические или виртуальные ресурсы.

Когда узел DPI развертывается в контексте виртуализации сети, возможно, что узел или компоненты DPI (например, ядро DPI) внутри узла DPI должны быть виртуализированы в логические/виртуальные узлы DPI или логические/виртуальные компоненты.

10.2 Функциональные требования к уровню пользователя

- Рекомендуется, чтобы ядро DPI, DPI-PIB и узел DPI обладали возможностью виртуализироваться соответственно в одно или более виртуальных ядер углубленной проверки пакетов (vDPI), виртуальных PIB DPI и виртуальных узлов DPI.
- Если физический компонент DPI (узел DPI, ядро DPI или PIB DPI и т. д.) виртуализирован в два или более логических компонента DPI, требуется, чтобы такие логические компоненты были логически независимы и отделены друг от друга.
- Если виртуальный узел DPI, виртуальное ядро DPI или виртуальная PIB логически развернуты в виртуальной сети, требуется, чтобы такие виртуальный узел DPI, виртуальное ядро DPI или виртуальная PIB обладали теми же возможностями DPI, что и физический узел DPI, физическое ядро DPI или физическая PIB DPI.
- Если виртуальный узел DPI, виртуальное ядро DPI или виртуальная PIB логически развернуты в виртуальной сети, требуется, чтобы такой виртуальный узел DPI, виртуальное ядро DPI или виртуальная PIB не ухудшали характеристики виртуальной сети.
- Рекомендуется использовать преобразование между физическими и виртуальными компонентами DPI (узлы DPI, ядра DPI, PIB DPI и т. д.), при котором соотношение между этими компонентами составляет $1: n$, $m: 1$ или $m: n$ (где m и n – целые положительные числа и $m > 1$, $n > 1$).

10.3 Функциональные требования к уровню управления

- Требуется, чтобы каждый логический/виртуальный компонент DPI имел один или несколько соответствующих объектов управления, которые управляют этим логическим/виртуальным компонентом.
- Рекомендуется, чтобы объект управления был способен настраивать преобразование физических компонентов DPI (узлы DPI, ядра DPI, PIB DPI и т. д.) в соответствующие логические/виртуальные компоненты DPI.
- Рекомендуется, чтобы объект управления мог гарантировать, что разные логические/виртуальные компоненты DPI независимы и отделены друг от друга.
- Когда логическим/виртуальным компонентом DPI управляют два или более объекта управления, требуется, чтобы эти объекты гарантировали согласованность информации, относящейся к управляемому логическому/виртуальному компоненту.

10.4 Функциональные требования к уровню администрирования

- Требуется, чтобы объект администрирования имел возможность управлять физическими компонентами DPI (узлы DPI, ядра DPI, PIB DPI и т. д.), виртуализированными в логические/виртуальные компоненты DPI.
- Рекомендуется, чтобы объект администрирования имел возможность управлять логическими/виртуальными компонентами DPI.
- Если физический компонент DPI (узел DPI, ядро DPI, PIB DPI и т. д.) и соответствующий ему логический/виртуальный компонент DPI управляются одним и тем же объектом администрирования, требуется, чтобы этот объект гарантировал независимость информации управления, относящейся к вышеупомянутому физическому компоненту DPI и к соответствующему ему логическому/виртуальному компоненту.

11 Функциональные требования DPI в развивающихся сетях подвижной связи

11.1 Внедрение развивающихся сетей подвижной связи

Развитие сетей подвижной связи – это процесс модернизации (обновления) сетей подвижной связи с переходом к сетям нового поколения. Следует отметить, например, что обновление сети подвижной связи 2G приводит к ее замене сетью подвижной связи 3G.

Таким образом, развивающиеся сети подвижной связи – это сети подвижной связи, которые с развитием соответствующих технологий преобразуются в сети новых поколений. Например, современные сети подвижной связи развиваются в сети подвижной связи 4G, а в будущем будут развиваться в сети 5G и т. д.

11.2 Общие требования к развертыванию DPI в развивающихся сетях подвижной связи

- Ниже приводятся общие требования, которые необходимо учитывать при развертывании DPI в развивающихся сетях подвижной связи. Когда подвижная сеть модернизируется с использованием технологии следующего поколения, требуется, чтобы функция DPI имела возможность нормально работать или легко обновляться до достижимого состояния.
- Требуется, чтобы функция DPI сохраняла и не ухудшала первоначальные возможности и характеристики развивающейся сети подвижной связи независимо от того, развернута ли она в сети радиодоступа (RAN), на границе доступа базовой сети с коммутацией пакетов, в базовой сети с коммутацией пакетов или на границе восходящей линии базовой сети с коммутацией пакетов.
- Требуется, чтобы функция DPI имела возможность гарантировать, что развивающаяся сеть подвижной связи сможет нормально работать в случае отказа компонента или узла, выполняющего функции DPI.

11.3 Требования к интерфейсу при развертывании DPI в развивающихся сетях подвижной связи

- Требуется, независимо от места развертывания функции DPI (в RAN, на границе доступа базовой сети с коммутацией пакетов, в базовой сети с коммутацией пакетов или на границе восходящей линии базовой сети с коммутацией пакетов), чтобы компонент или узел, выполняющий функции DPI, имел интерфейсы, которые могут обеспечить связь с соответствующими объектами в развивающейся сети подвижной связи.

Например, при развертывании функций DPI в сетях 4G между служебным шлюзом (S-GW) и шлюзом сети пакетной передачи данных (P-GW) требуется, чтобы компонент или узел имели надлежащие интерфейсы, обеспечивающие связь с S-GW и P-GW.

11.4 Требования к протоколу при развертывании DPI в развивающейся сети подвижной связи

Требуется, независимо от места развертывания функции DPI (в RAN, на границе доступа базовой сети с коммутацией пакетов, в базовой сети с коммутацией пакетов или на границе восходящей линии базовой сети с коммутацией пакетов), чтобы компонент или узел, выполняющий функции DPI, имел возможность обрабатывать протокол, используемый соответствующим объектом в сети подвижной связи. Например, для случая сетей 4G на рисунке 11-1 описан стек протоколов, относящийся к интерфейсу S-GW и P-GW (интерфейс s5 или s8), и если функции DPI развернуты между S-GW и P-GW, то компонент или узел, выполняющий вышеуказанные функции DPI, должен иметь возможность обрабатывать протокол туннелирования (GTP) службы пакетной радиосвязи общего пользования (GPRS).

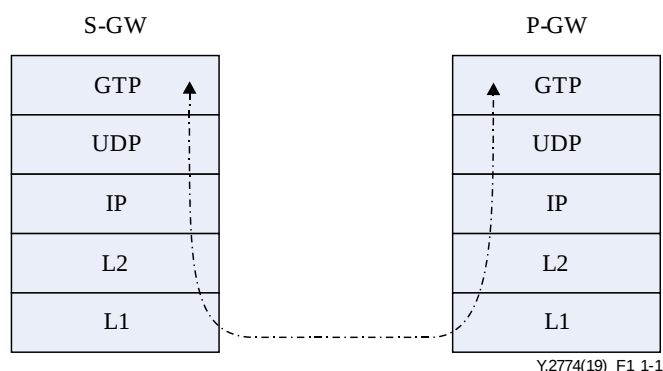


Рисунок 11-1 – Пример стека протоколов связи между S-GW и P-GW

В другом примере, представленном на рисунке 11-2, описан стек протоколов связи между eNodeB и объектом управления мобильностью (MME), и если функции DPI развернуты между eNodeB и MME, компонент или узел, реализующий эти функции DPI, должен иметь возможность обрабатывать протокол передачи с управлением потоком (SCTP).

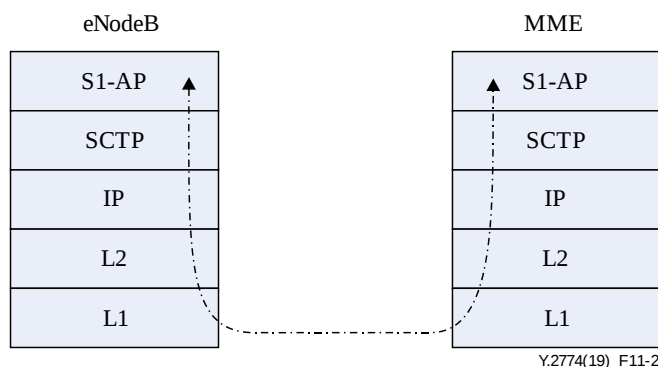


Рисунок 11-2 – Пример стека протокола связи между eNodeB и MME

- Когда функции DPI развернуты в базовой сети с коммутацией пакетов, требуется, чтобы функции DPI имели возможность обрабатывать пакеты нескольких протоколов.

Например, в случае развертывания компонента или узла, реализующего вышеуказанную функцию DPI, между S-GW и P-GW в развивающейся сети подвижной связи этот компонент или узел должны поддерживать такие протоколы, как SCTP, протокол дейтаграмм пользователя (UDP) и GTP-U и т. д.

- Когда функции DPI развернуты в базовой сети с коммутацией пакетов, рекомендуется, чтобы правила политики в PIV DPI выполнялись для нескольких протоколов одновременно.

Например, если имеется правило политики с тегом приложения А, то пакеты с тегом приложения А, соответствующие таким протоколам, как UDP, GTP (см. рисунок 11-1), SCTP (см. рисунок 11-2) и т. д., должны соответствовать этому правилу политики.

12 Вопросы безопасности

В настоящей Рекомендации содержатся те же требования безопасности, что и в [ITU-T Y.2770].

13 Прочие соображения

Аспекты регулирования и конфиденциальности приложений безопасности не входят в сферу применения настоящей Рекомендации. При реализации настоящей Рекомендации поставщики оборудования, операторы сетей и поставщики услуг должны учитывать национальные регуляторные требования и требования политики.

Библиография

- | | |
|-------------------------|--|
| [b-ITU-T Y-Sup.41] | ITU-T Y-series Recommendations – Supplement 41 (2016), <i>ITU-T Y.2200-series – Deployment models of service function chaining</i> . |
| [b-ETSI GS NFV-MAN 001] | ETSI GS NFV-MAN 001 (2014-12), <i>Network Functions Virtualisation (NFV); Management and Orchestration:V1.1.1</i> |
| [b-IETF RFC 7665] | IETF RFC 7665 (2015), <i>Service Function Chaining (SFC) Architecture</i> |

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи