Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2772

(04/2016)

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

Сети последующих поколений – Безопасность

Механизмы элементов сети с поддержкой углубленной проверки пакетов

Рекомендация МСЭ-Т Y.2772

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

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 СПП	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
Совершенствование СПП	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.3099
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

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

Рекомендация МСЭ-Т Y.2772

Механизмы элементов сети с поддержкой углубленной проверки пакетов

Резюме

В Рекомендации МСЭ-Т Y.2772 представлены механизмы сетевых элементов, поддерживающие углубленную проверку пакетов, включая аспекты процедур и методов углубленной проверки пакетов (DPI) в отношении пакетных сетей. Эта Рекомендация призвана содействовать пониманию методов, интерфейсов, протоколов и процедур, связанных с DPI, а также механизмов процессов, относящихся к DPI.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т Y.2772	29.04.2016 г.	13-я	11.1002/1000/12709

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите 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 в целях 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 получил извещение 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/.

СОДЕРЖАНИЕ

Стр.

Рекомендация МСЭ-Т Y.2772

Механизмы элементов сети с поддержкой углубленной проверки пакетов

1 Сфера применения

В настоящей Рекомендации описаны механизмы реализации углубленной проверки пакетов (DPI) в пакетных сетях. Основной целью этой Рекомендации является описание прикладных моделей, связанных с ними протоколов, интерфейса, процедур и процессов DPI, которые можно использовать для идентификации информационных потоков между функциями DPI и другими функциями сети.

В сферу применения настоящей Рекомендации входят:

– определение механизма DPI;

– обзор механизмов DPI, поддерживающих идентификацию приложений;

– процедуры и информационные потоки в эксплуатационном аспекте;

– процедуры и информационные потоки в аспекте управления, например управления политикой DPI;

– другие процедуры и информационные потоки возможных интерфейсов функциональных объектов (FE) DPI.

Следующие вопросы не входят в сферу применения настоящей Рекомендации:

– аспекты эксплуатации и управления, неспецифичные для объектов DPI;

– функции управления, связанные с общесетевыми элементами, например уже определенные в Рекомендациях МСЭ-Т серии M и Рекомендациях МСЭ-Т серии X.

Пользователи и специалисты по применению этой Рекомендации МСЭ-Т должны соблюдать все применимые государственные и региональные законы, нормативные акты и политические принципы. Механизм, описанный в настоящей Рекомендации МСЭ-Т, может не применяться в отношении международной корреспонденции в целях обеспечения конфиденциальности и выполнения суверенных национальных юридических требований, касающихся электросвязи, а также соблюдения Устава 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 справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

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

[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.*

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 (DPI) [ITU-T Y.2770]: Проведение в соответствии с базовой эталонной моделью взаимодействия открытых систем (OSI-BRM) [ITU-T X.200], предусматривающей уровневую архитектуру протокола, анализа:

– свойств полезной нагрузки и/или пакетов (см. список возможных свойств в пункте 3.2.11/[ITU-T Y.2770]), более полных, чем информация заголовка на уровнях 2, 3 и 4 (L2/L3/L4) протокола; и

– других свойств пакетов

в целях однозначной идентификации приложения.

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

3.1.2 анализатор DPI (DPI analyser) [ITU-T Y.2771]: Последующий объект в тракте обработки DPI (в рамках функции реализации политики DPI) с упором на функции сравнения между заголовками определенных пакетов и полезными нагрузками предварительно отобранных потоков пакетов. Основная сфера применения анализатора DPI связана с оценкой *условий* политики DPI по сравнению с *предварительно отобранными* входящими пакетами.

ПРИМЕЧАНИЕ. − Анализатор DPI может располагаться после сканера DPI (см. пункт 3.2.5 [ITU-T Y.2771]). Анализатор DPI может обеспечивать функции анализатора системы обнаружения проникновения (IDS).

3.1.3 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, изображенные на рисунке 6-1 [ITU-T Y.2770]).

3.1.4 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. − С функциональной точки зрения 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.

3.1.5 действие в соответствии с политикой DPI (DPI policy action) (сокращенно – действие) [ITU-T Y.2771]: Определение необходимого действия для реализации правила политики при соблюдении условий этого правила. Действия в соответствии с политикой могут привести к тому, что выполнение одной или нескольких операций повлияет на сетевой трафик и сетевые ресурсы и/или изменит их конфигурацию, см. также в [b-IETF RFC 3198].

3.1.6 условие политики DPI (DPI policy condition) (также называемое сигнатурой DPI (DPI signature)) [ITU-T Y.2770]: Представление необходимого состояния и/или предварительных условий, по которым идентифицируется приложение и определяется необходимость выполнения действий, предусмотренное правилом политики. Набор условий политики DPI, связанных с тем или иным правилом политики, определяет случаи применения этого правила политики (см. также [b-IETF RFC 3198]).

Условие политики DPI должно содержать условия прикладного уровня и может содержать другие варианты, например условия состояния и/или условия уровня потока:

1) условие состояния (факультативно):
   a) условия категории обслуживания сетью (например, наличие перегрузки в трактах передачи пакетов); или
   b) статус элементов сети (например, локальное условие переполнения DPI-FE);

2) дескриптор потока/условия уровня потока (факультативно):

a) содержимое пакета (поля заголовка);

b) характеристики пакета (например, число меток MPLS);

c) обработка пакета (например, выходной интерфейс DPI-FE);

3) дескриптор приложения/условия прикладного уровня:

a) содержимое пакета (поля заголовка приложения и полезная нагрузка приложения).

ПРИМЕЧАНИЕ. − Это условие относится к "простому условию" в формальных описаниях условий уровня потока и условий прикладного уровня.

3.1.7 сканер DPI (DPI scanner) (используется также в качестве "функции сканирования DPI") [ITU-T Y.2771]: Первый объект в тракте обработки DPI (в рамках функции реализации политики DPI), обеспечивающий предварительный отбор (для последующего анализатора DPI, см. пункт 3.2.1 [ITU-T Y.2771]) путем выбора *всех условий* политики DPI в отношении *всех* входящих пакетов.

3.2 Термины, определенные в настоящей Рекомендации

Нет.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

BRAS	Broadband Remote Access Server		Широкополосный сервер удаленного доступа
CLI	Command Line Interface		Интерфейс командной строки
CMIP	Common Management Information Protocol	ПОУИ	Протокол передачи общей управляющей информации
DPI	Deep Packet Inspection		Углубленная проверка пакетов
DPI-PDFE	DPI Policy Decision Functional Entity		Функциональный объект решения на основе политики DPI
DPI-PIB	DPI Policy Information Base		Информационная база политики DPI
EMS	Element Management System		Система управления элементами
GUI	Graphical User Interface		Графический интерфейс пользователя
IP	Internet Protocol		Протокол Интернет
IPFIX	IP Flow Information Export		Экспорт информации IP-потока
LAN	Local Area Network		Локальная сеть
L-PDF	Local PDF		Локальная PDF
NMS	Network Management System		Система управления сетью
OAM	Operation, Administration and Management		Эксплуатация, администрирование и управление
PDF	Policy Decision Function		Функция принятия решений в соответствии с политикой
PIB	Policy Information Base		Информационная база политики
SNMP	Simple Network Management Protocol		Простой протокол управления сетью
SR	Service Router		Маршрутизатор службы
TCAM	Ternary Content-Addressable Memory		Троичное ассоциативное запоминающее устройство
TCP	Transmission Control Protocol		Протокол управления передачей
UDP	User Datagram Protocol		Протокол дейтаграмм пользователя
VLAN	Virtual Local Area Network		Виртуальная локальная сеть

5 Условные обозначения и соглашения по терминологии

Отсутствуют.

6 Определение механизма DPI

В настоящей Рекомендации под термином "механизм" понимаются средства, методы, процессы и процедуры, применяемые для реализации той или иной функции или соблюдения определенных требований. С учетом этого механизм DPI можно описать следующим образом:

– конкретный процесс, который можно использовать для реализации функций и возможностей, определенных в [ITU-T Y.2771], и удовлетворения требований, определенных в [ITU-T Y.2770];

– детальная процедура, которую можно применить для реализации функций и возможностей, определенных в [ITU-T Y.2771], и удовлетворения требований, определенных в [ITU-T Y.2770];

– надлежащие методы, которые можно использовать для реализации функций и возможностей, определенных в [ITU-T Y.2771], и удовлетворения требований, определенных в [ITU-T Y.2770];

– специализированные инструменты, которые можно использовать для реализации функций и возможностей, определенных в [ITU-T Y.2771], и удовлетворения требований, определенных в [ITU-T Y.2770].

7 Обзор механизмов DPI для поддержки идентификации приложений

7.1 Общие положения о механизмах DPI

Существуют механизмы DPI двух основных типов:

– механизмы DPI, относящиеся к узлу DPI;

– механизмы DPI, относящиеся к сети, поддерживающей функции DPI.

Прежде чем определять эти разновидности механизмов, необходимо дать определение базовой структуры узла DPI и типичной сети, поддерживающей функции DPI.

7.2 Базовая структура узла DPI

Базовая структура узла DPI показана на рисунке 6-1 [ITU-T Y.2770] и на рисунке 7-2 [ITU-T Y.2771]; на этой структуре может основываться реализация узла DPI.

7.3 Типичная сеть, поддерживающая функции DPI

Типичная сеть, развернутая с узлами DPI, показана на рисунке 7-1. Она состоит из пяти логических уровней (сверху вниз): облака, основного уровня, уровня агрегации, уровня доступа и уровня терминала. Следует подчеркнуть, что существует логическая связь между каждым узлом DPI и системой управления элементами (EMS) или системой управления сетью (NMS), хотя на рисунке 7-1 показаны не все логические связи. Все узлы DPI могут взаимодействовать с сетевыми объектами (такими, как маршрутизатор, коммутатор, сервер широкополосного удаленного доступа (BRAS) и т. д.), поэтому узлы DPI, показанные на рисунке 7-1, не зависят от этих сетевых объектов.

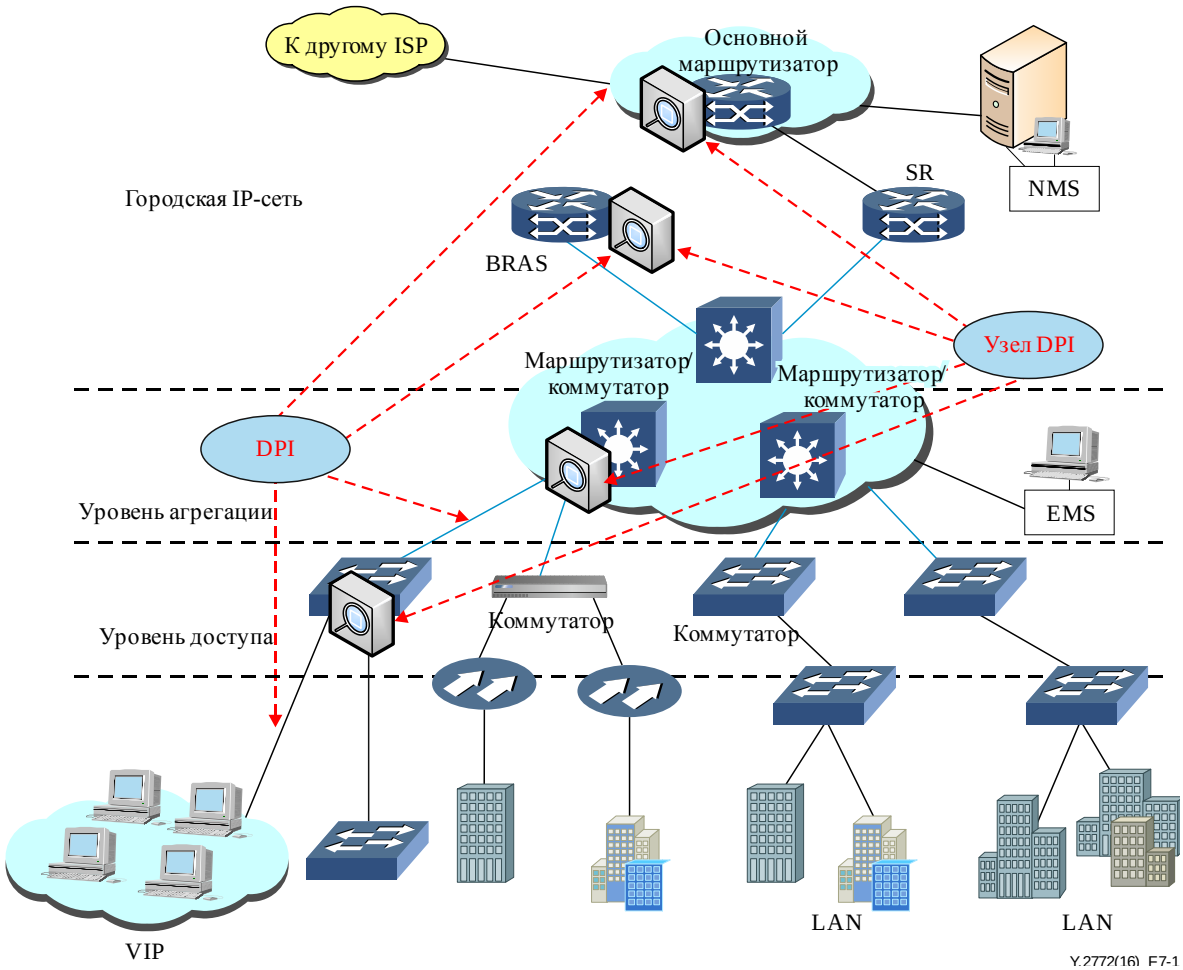

Рисунок 7-1 – Пример топологии сети с узлами DPI

Подробнее см. на рисунке 6-3 [b-ITU-T Y-Sup.25], иллюстрирующем пример сети с применением DPI.

7.4 Механизмы DPI, относящиеся к узлу DPI

Механизм DPI узла DPI в основном состоит из следующих трех элементов.

1) Метод представления информации

Элемент сети, поддерживающий функции DPI, содержит разные виды информации и данных, которые должны быть представлены в этом элементе, например правила DPI. Метод представления информации очень важен для элемента сети; различные методы представления обеспечивают разную эффективность обработки.

2) Методы и процедуры обработки

К методам и процедурам обработки относятся инструктивные методы реализации функций, относящихся к DPI, а также процедуры, выполняемые элементом сети в поддержку этих функций DPI.

3) Интерфейс и соответствующий протокол

Интерфейс и соответствующий протокол – это реализация интерфейсов, определенных в [ITU-T Y.2770] (например, e1, e2), а также соответствующего протокола, используемого для обмена информацией между этими видами интерфейсов.

7.5 Механизм сети с узлами DPI

Механизм, соответствующий сетям, поддерживающим функции DPI, состоит в основном из следующих элементов:

- элементы эксплуатации;
- элементы управления.

8 Методы представления DPI – правило политики DPI-PIB

8.1 Обзор

Условие правил политики DPI в составе информационной базы политики DPI (DPI-PIB) – одна из основных частей узла DPI, и почти все действия узла DPI основаны на условиях правил политики DPI. Поэтому очень важно, чтобы условие правил политики DPI было представлено эффективно и в простой для обработки форме. Описаны три метода представления условия правил политики DPI: метод представления на основе данных и маски, метод представления на основе регулярного выражения и гибридный метод представления.

8.2 Метод представления условий правил политики DPI на основе данных и маски

В пакете протоколов TCP/IP и соответствующих сетевых устройствах обычно используется метод представления на основе IP-адреса и маски; метод представления на основе данных и маски подобен этому методу. В методе на основе данных и маски для представления маркировочного слова, идентифицирующего определенный поток данных, используется последовательность байтов (данных), а для того чтобы решить, следует ли проверять определенный бит последовательности байтов, используется последовательность битов (маска), соответствующая последовательности байтов. Как правило, если бит маски равен "1", то соответствующий бит последовательности байтов не проверяется. И наоборот, если бит маски равен "0", то требуется проверка соответствующего бита последовательности байтов.

Для DPI-PIB целесообразно использовать метод представления на основе данных и маски, который имеет следующие преимущества:

- он прост и понятен;
- высокоэффективен; один элемент может использоваться многими потоками данных;
- хорошо сочетается с широко используемыми устройствами, такими как третичные ассоциативные ЗУ (TCAM).

Метод представления на основе данных и маски иллюстрируют следующие два примера.

1) Подбор потоков данных с диапазоном портов источника TCP от 0x2100 до 0x21ff.

Для удовлетворения этого требования в DPI-PIB достаточно одного элемента:

Item1: данные: 0x2100, маска: 0x00ff.

2) Подбор потоков данных, виртуальная локальная сеть (VLAN) которых соответствует диапазону 16–63.

Для удовлетворения этого требования в DPI-PIB нужны два элемента:

Item1: данные: 0x0010, маска: 0x000f

Item2: данные: 0x0020, маска: 0x001f

8.3 Метод представления условий правил политики DPI на основе регулярного выражения

Метод представления на основе данных и маски подходит для представления маркировочного слова с фиксированным положением и определенным значением. Как правило, для запросов этого типа очень хорошо подходят заголовки протоколов уровней 2–4 (L2–L4).

Однако для маркировочных слов высокоуровневых приложений обычно характерна неопределенность, и они могут легко изменяться. В этом случае использование метода представления на основе данных и маски реализовать сложно. Для таких приложений больше подходит метод представления маркировочных слов на основе регулярных выражений.

Регулярное выражение [b-ITU-T X.680] – это метод описания, широко известный в вычислительной технике; подробное представление и анализ регулярных выражений не входит в сферу применения настоящей Рекомендации.

Метод представления на основе регулярных выражений иллюстрируют следующие два примера.

1) Подбор потока данных, содержащего слово "Bittorrent" или "Bitcomment".

Для удовлетворения этого требования в DPI-PIB необходим только один элемент:

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

2) Подбор потока данных, содержащего слово Worm, за которым не следует слово "v1" или "v2". Для удовлетворения этого требования в DPI-PIB необходим только один элемент:

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

8.4 Гибридный метод представления условий правил политики DPI

Функции DPI могут действовать на уровнях 2–7. Для уровней 2–4 в качестве способа построения DPI-PIB хорошо подходит метод представления на основе данных и маски. С другой стороны, при использовании маркировочных слов на уровне 7 для построения DPI-PIB лучше выбрать метод представления на основе регулярных выражений.

Таким образом, во многих приложениях полезно объединить эти два метода представления, что приводит к гибридному методу представления. При этом методе одни маркировочные слова представлены методом на основе данных и маски, а другие – методом на основе регулярных выражений.

Гибридный метод представления иллюстрируют следующие два примера.

1) Обнаружение потока данных, в который входит слово "Bittorrent" или "Bitcomment", причем VLAN этого потока данных находится в диапазоне 8–15.

Для удовлетворения этого требования в DPI-PIB необходим только один элемент:

Item1: первая половина: данные: 0x0008, маска: 0x0007;

вторая половина: "/Bit(torrent|comment)/".

Эти две половины можно хранить в разных областях памяти, но логически они связаны друг с другом.

9 Информационные потоки, процедуры обработки и методы объектов DPI

9.1 Обзор

Объект DPI содержит множество необходимых функций, и реализация этих функций опирается на многие аспекты, в числе которых:

- реализация некоторых необходимых интерфейсов (см. пункт 9.2);
- механизм информационного потока между компонентами функции (см. пункт 9.3);
- процедуры обработки основных компонентов функции (см. пункт 9.4);
- методы повышения надежности (см. пункт 9.5);
- методы эффективного обмена информацией и синхронизации данных (см. пункт 9.6);
- другие методы, полезные для реализации объекта DPI.

9.2 Реализация интерфейса

9.2.1 Обзор интерфейса

В [ITU-T Y.2770] определены и иллюстрируются несколько интерфейсов, включая внешние интерфейсы e1 и e2, а также внутренние интерфейсы i1, i2 и i3. Внешние интерфейсы e1 и e2 показаны на рисунке 8-1 [ITU-T Y.2770], а внутренние интерфейсы i1, i2 и i3 – на рисунке 8-2 [ITU-T Y.2770]. Теоретически в узле DPI должны выполняться все эти интерфейсы.

Однако в зависимости от требований приложения может потребоваться реализация и других интерфейсов. Например, в контексте двунаправленной DPI в узле DPI может потребоваться специальный внешний интерфейс e3 (см. рисунок 11-4).

9.2.2 Внутренние интерфейсы

Внутренние интерфейсы (см. рисунок 8-2 [ITU-T Y.2770]) используются для обмена информацией между внутренними компонентами функции в узле DPI. Существует три внутренних интерфейса: i1, i2 и i3. В следующих пунктах описана реализация этих внутренних интерфейсов.

9.2.2.1 Интерфейс i1

Внутренний интерфейс i1 представляет собой интерфейс между функцией идентификации пакетов и другими функциями обработки пакетов внутри DPI-FE. Как правило, интерфейс i1 – это физический интерфейс, реализованный аппаратными средствами, в целях обеспечения высокопроизводительной работы узла DPI. Интерфейс i1 может быть реализован разными способами, включая общую память, внутренние параллельные порты, внутренние последовательные порты и т. д.

9.2.2.2 Интерфейс i2

Внутренний интерфейс i2 представляет собой интерфейс между функцией идентификации пакетов и локальной функцией управления внутри DPI-FE. Интерфейс i2 – это программно реализуемый логический интерфейс, и существует несколько методов разработки интерфейса i2.

Если выполняются функции идентификации пакетов и локального управления, которыми управляет один и тот же процессор, то интерфейс i1 может быть реализован различными методами, такими как набор функций интерфейса прикладного программирования (API), общая память и взаимодействие между процессами.

Если выполняются функции идентификации пакетов и локального управления, которыми управляют разные процессоры, то интерфейс i1 может быть реализован с помощью методов передачи данных. Например, два вышеупомянутых функциональных компонента могут обмениваться информацией через TCP или UDP.

9.2.2.3 Интерфейс i3

Внутренний интерфейс i3 представляет собой интерфейс между библиотекой сигнатур DPI и локальной функцией управления внутри DPI-FE. Интерфейс i3 – это программно реализуемый логический интерфейс. Как правило, библиотекой сигнатур DPI и функцией локального управления управляет один и тот же процессор, и интерфейс i3 может быть реализован набором функций API.

9.2.3 Внешний интерфейс

Внешние интерфейсы (см. рисунок 8-1 [ITU-T Y.2770]) используются для обмена информацией между узлом DPI и другими функциональными объектами, такими как NMS. Существуют три внешних интерфейса: e1, e2 и e3. Внешние интерфейсы e1 и e2 показаны на рисунке 8-1 [ITU-T Y.2770], а внешний интерфейс e3 – на рисунке 11-4 настоящей Рекомендации. Реализация этих внешних интерфейсов описана в пунктах 9.2.3.1–9.2.3.3.

9.2.3.1 Интерфейс e1

Внешний интерфейс e1 – это интерфейс между функциональным объектом принятия решений в соответствии с политикой DPI (DPI-PDFE) и функциональным объектом DPI (DPI-FE). В [ITU-T Y.2770] приведено решение для реализации данного интерфейса: при необходимости интерфейс e1 может быть интерфейсом с опорной точкой Rw, как указано в [ITU-T Y.2111]. Rw – возможное, но не уникальное и не обязательное решение.

Какое бы решение для проектирования интерфейса e1 ни использовалось, необходимо гарантировать, что данные, передаваемые по интерфейсу, будут понятны как DPI-PDFE, так и DPI-FE, даже если DPI-PDFE и DPI-FE разработаны разными поставщиками.

9.2.3.2 Интерфейс e2

Внешний интерфейс e2 представляет собой интерфейс между DPI-FE и удаленной сетью, отличной от DPI-PDFE (например, NMS). В [ITU-T Y.2770] также приведено решение для реализации этого интерфейса: для интерфейса e2 рекомендуется использовать протоколы экспорта на основе экспорта информации IP-потока (IPFIX, см. [b-IETF RFC 5101]). Хотя для интерфейса e2 можно использовать протоколы экспорта на основе IPFIX, возможны и другие решения для обмена информацией между DPI-FE и объектом удаленной сети, отличным от функционального объекта принятия решений в соответствии с политикой DPI (DPI-PDFE).

Каким бы ни было решение, выбранное для проектирования интерфейса e2, необходимо гарантировать, что информация, передаваемая по этому интерфейсу, будет понятна как удаленному объекту сети, так и DPI-FE, независимо от удаленного объекта сети и от того, разработан ли DPI-FE одним и тем же поставщиком.

9.2.3.3 Интерфейс e3

Внешний интерфейс e3 представляет собой интерфейс между двумя независимыми DPI-FE, когда необходимо соблюдать требования двунаправленного приложения DPI. Подробное описание этого интерфейса приведено в разделе 11.

9.3 Поток информации

9.3.1 Поток информации, ориентированный на ядро DPI

На рисунке 9-1 изображен поток информации, создаваемый ядром DPI. Обмен данными между ядром DPI и локальной функцией принятия решений в соответствии с политикой (L-PDF) осуществляется в пределах объекта DPI, а обмен данными между L-PDF и PD-FE – вне объекта DPI.

Обмен данными, связанными с DPI, должен быть очень надежным. С другой стороны, передача данных внутри DPI надежнее, чем передача данных между двумя независимыми объектами. Таким образом, для обмена данными между двумя независимыми объектами лучше использовать подходы, основанные на соединениях, с тем чтобы гарантировать надежность обмена данными, а обмен данными в пределах объекта DPI может осуществляться без установления соединения для экономии системных ресурсов и повышения эффективности обмена данными.

Таким образом, как показано на рисунке 9-1, рекомендуется проектировать обмен данными между ядром DPI и L-PDF в режиме без установления соединения, так как ядро DPI и L-PDF находятся в одном и том же объекте DPI. Однако обмен данными между L-PDF и PD-EF рекомендуется проектировать на основе режима с установлением соединения, так как PD-FE не находится в том же объекте DPI.

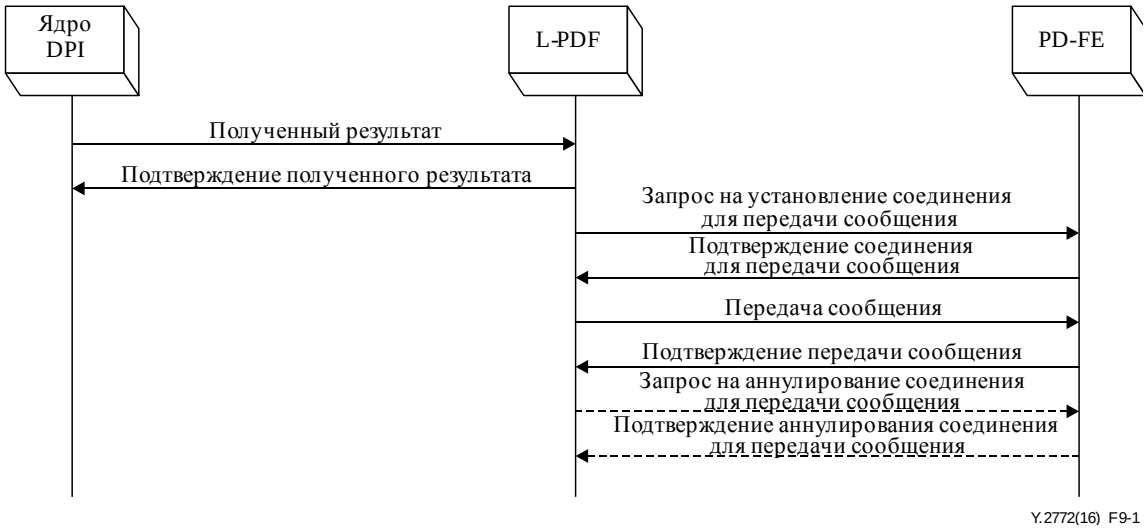

Рисунок 9-1 − Поток информации, ориентированный на ядро DPI

На рисунке 9-1 элемент "Полученный результат" используется для передачи данных, созданных ядром DPI, а элемент "Подтверждение полученного результата" – для сообщения ядру DPI о том, что указанные данные получены. Пара элементов "Запрос на установление соединения для передачи сообщения" и "Подтверждение соединения для передачи сообщения" используется для установления соединения, а пара элементов "Передача сообщения" и "Подтверждение передачи сообщения" – для передачи данных сообщения. По окончании передачи всех данных сообщения можно использовать пару элементов "Запрос на аннулирование соединения для передачи сообщения" и "Подтверждение аннулирования соединения для передачи сообщения" для аннулирования соединения (пунктирная линия на рисунке 9-1).

9.3.2 Поток информации, ориентированный на DPI-PIB

Рисунок 9-2 иллюстрирует поток информации, основанный на DPI-PIB. Обмен данными между DPI-PIB и L-PDF осуществляется в пределах объекта DPI, а обмен данными между L-PDF и PD-FE – вне объекта DPI.

Как показано на рисунке 9-2, обмен данными между DPI-PIB и L-PDF рекомендуется проектировать как режим без установления соединения, а обмен данными между L-PDF и PD-EF – как режим с установлением соединения.

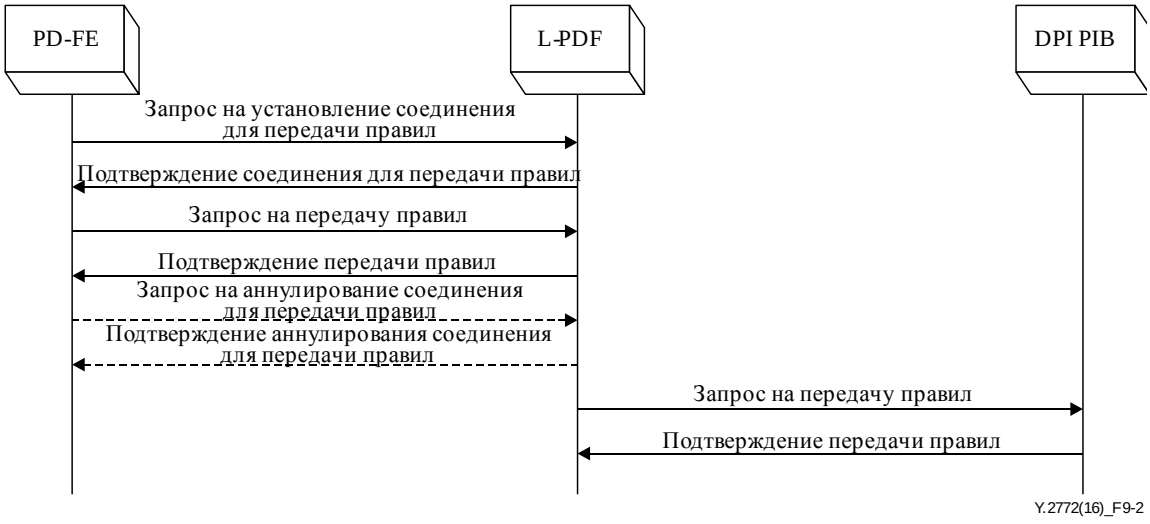

Рисунок 9-2 − Поток информации, ориентированный на DPI-PIB

На рисунке 9-2 простейшая пара элементов "Запрос на установление соединения для передачи правил" и "Подтверждение соединения для передачи правил" используется для установления соединения, а пара элементов "Запрос на передачу правил" и "Подтверждение передачи правил" – для передачи информации правил. По окончании передачи всех данных правил можно использовать пару элементов "Запрос на аннулирование соединения для передачи правил" и "Подтверждение аннулирования соединения для передачи правил" для аннулирования соединения (пунктирная линия на рисунке 9-2).

9.3.3 Поток информации, ориентированный на DPI L-PDF

Рисунок 9-3 иллюстрирует поток информации, ориентированный на DPI L-PDF. Обмен данными как между L-PDF и PD-FE, так и между L-PDF и объектом управления осуществляется вне объекта DPI.

Как показано на рисунке 9-3, никакие два из трех функциональных элементов – PD-FE, L-PDF и объект управления – не относятся к одному и тому же объекту. Поэтому рекомендуется проектировать обмен данными на основе режима с установлением соединения.

Как показано на рисунке 9-3, для установления соответствующего соединения используются четыре простейшие пары элементов ("Запрос на установление соединения для передачи правил" и "Подтверждение соединения для передачи правил", "Запрос на установление соединения для синхронизации правил" и "Подтверждение соединения для синхронизации правил", "Запрос на установление соединения для передачи сообщения" и "Подтверждение соединения для передачи сообщения", "Запрос на установление соединения для передачи конфигурации" и "Подтверждение соединения для передачи конфигурации"). Четыре других пары элементов используются для передачи соответствующих данных ("Запрос на передачу правил" и "Подтверждение передачи правил", "Запрос на передачу правил" и "Подтверждение передачи правил", "Запрос на передачу сообщения" и "Подтверждение передачи сообщения", "Запрос на передачи конфигурации" и "Подтверждение передачи конфигурации"). Кроме того, в соответствии с каждым типом соединения после окончания обмена всеми соответствующими данными может использоваться пара элементов "Запрос на аннулирование соединения" и "Подтверждение аннулирования соединения" для аннулирования соединения. Эти последние пары элементов не изображены на рисунке 9-3 для его упрощения и во избежание путаницы, однако они выполняют те же функции, что и пара "Запрос на аннулирование соединения для передачи правил" и "Подтверждение аннулирования соединения для передачи правил".

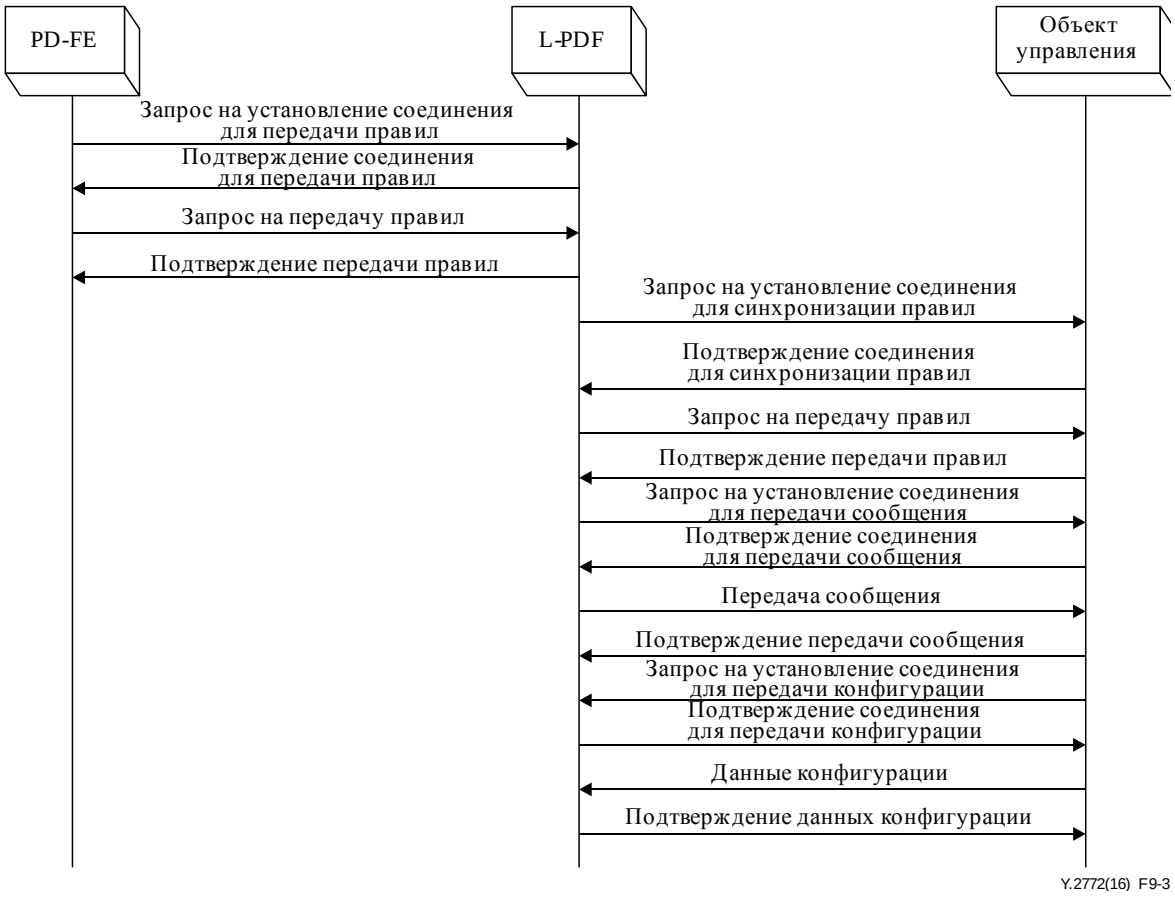

Рисунок 9-3 − Поток информации, ориентированный на L-PDF

9.4 Процедура обработки

9.4.1 Процедура обработки ядра DPI

Когда пакет поступает в ядро DPI, которое сканирует и идентифицирует этот пакет согласно правилу политики, определенному в DPI-PIB. Затем анализатор ядра DPI анализирует идентифицированный пакет и записывает результаты анализа. После этого выполняется действие политики, соответствующее полученному результату.

Если пакет не идентифицирован, выполняется действие "не идентифицирован". Если пакет идентифицирован, ядро DPI выполняет действие, соответствующее правилу политики, определенному в DPI-PIB.

Тем временем ядро DPI записывает полученный результат для каждого пакета и сохраняет несколько аналогичных результатов в буферной памяти. Периодически он сообщает о результатах в объект управления. Период передачи сообщений зависит от реализации и не входит в сферу применения настоящей Рекомендации.

9.4.2 Процедура обработки DPI-PIB

DPI-PIB содержит одну или несколько записей правил политики DPI. DPI-PIB получает информацию о правилах от L-PDF после того, как L-PDF получит информацию о правилах от PD-FE.

9.4.3 Процедура обработки L-PDF

L-PDF обновляет записи правил DPI-PIB, когда получает информацию о правилах от одной или нескольких удаленных функций принятия решений в соответствии с политикой (PDF). Когда L-PDF получает определенный результат от ядра DPI, она передает его одной или нескольким удаленным PDF. Функция L-PDF может также отвечать за решение потенциальных проблем взаимодействия правил, возникающих в наборе правил политики DPI.

9.5 Метод защиты

В [ITU-T Y.2771] определена группа избыточности "1 + N" для реализации отказоустойчивости. Существуют две различные модели защиты: модель "1 + 1" (N = 1) и модель "1 + N" (N > 1). Модель "1 + 1" используется для одного активного и одного резервного компонента, а модель "1 + N" (N > 1) – для одного активного и N резервных компонентов.

9.5.1 Модель "1 + 1"

Модель "1 + 1" также называется моделью "активный/резервный" и представляет собой разновидность модели отказоустойчивости, когда в случае отказа резервный компонент, находящийся в режиме ожидания, берет на себя функции отказавшего компонента. В этой модели резервный компонент использует для обнаружения отказа активного компонента механизм периодических контрольных сообщений. Уровень высокой готовности зависит от стратегии репликации состояния компонента. Для модели "активный/резервный" рекомендуется использовать решение с горячим резервом. Решение с горячим резервом обеспечивает резервирование как аппаратуры, так и программного обеспечения. Однако состояние активного компонента реплицируется в резервный компонент при любых изменениях, то есть резервный компонент постоянно находится в состоянии готовности. В случае отказа активного компонента резервный компонент заменяет неисправный компонент и продолжает действовать в соответствии с текущим состоянием.

Состояние компонента копируется с помощью активной репликации. Для сообщения резервному компоненту об изменениях состояния перед их отработкой активным компонентом используется протокол фиксации. После отработки резервный компонент получает второе сообщение для фиксации изменения состояния. Любые незафиксированные изменения состояния отрабатываются резервным компонентом после обработки отказа. Протокол фиксации зависит от реализации и не входит в сферу применения настоящей Рекомендации.

Модель "активный/горячий резерв" обеспечивает непрерывную готовность без каких бы то ни было прерываний обслуживания.

9.5.2 Модель "1 + N" (N > 1)

Модель "1 + N" (N > 1) основывается на нескольких избыточных компонентах, причем более двух компонентов DPI (иными словами, группа избыточности "1 + N", DPI-компонентами которой являются функциональные компоненты) находятся в узле DPI и один DPI компонент играет роль активного компонента, в то время как другие DPI-компоненты действуют как резервные.

Процедуры обработки этого режима аналогичны процедурам обработки модели "1 + 1". Для обнаружения отказа активного компонента резервные компоненты используют периодические контрольные сообщения. В случае отказа активного компонента один из резервных компонентов берет на себя роль неисправного компонента.

9.6 Метод синхронизации данных

В случае защитного переключения необходимо обеспечить синхронизацию данных. Рекомендуется, чтобы активные и резервные функциональные компоненты содержали полностью идентичную информацию, такую как информационная база политики (PIB), для чего используется метод синхронизации данных.

9.6.1 Синхронизация данных в режиме "1 + 1"

В случае отказа активного компонента (включая DPI-узел, ядро DPI и DPI-FE) резервный компонент берет на себя работу активного компонента. Резервный компонент посылает в объект управления "Запрос синхронизации правил". Объект управления посылает резервному компоненту информацию правил.

9.6.2 Синхронизация данных в режиме "1 + N" (N > 1) на уровне компонента

Синхронизация данных в режиме "1 + N" на уровне компонента осуществляется так же, как и в режиме "1 + 1". В случае отказа активного компонента (включая DPI-узел, ядро DPI и DPI-FE) резервный компонент берет на себя работу активного компонента. Резервный компонент посылает в объект управления "Запрос синхронизации правил". Объект управления посылает резервному компоненту информацию правил.

9.6.3 Синхронизация данных в режиме "1 + N" (N > 1) на уровне узла

Режим "1 + N" (N > 1) на уровне узла реализуется с помощью режима кластера. В режиме кластера в случае отказа ведущего узла его работу берет на себя резервный узел. Резервный узел синхронизирует данные правил с объектом управления.

В случае отказа ведомого узла предшествующие маршрутизаторы переадресовывают трафик, передаваемый в неисправный узел, в другие ведомые узлы в соответствии с алгоритмом выравнивания нагрузки. В этих ведомых узлах запускается синхронизация с новыми правилами из объекта управления.

10 Спецификация механизма эксплуатации

10.1 Обзор

В данном разделе рассматриваются эксплуатационные аспекты технологий DPI, в том числе:

- цели принятой технологии DPI;
- аспект характеристик сети при развертывании системы DPI;
- анализ существующих сетей без DPI;
- развертывание физических объектов DPI и создание соответствующих сетей;
- эксплуатация, администрирование и техническое обслуживание сетей с DPI;
- изменение и совершенствование существующих сетей на основе контроля характеристик сети.

Общий процесс создания и эксплуатации сети с DPI-узлами показан на рисунке 10-1. Шесть шагов, показанные на рисунке, описаны в пунктах 10.3–10.8.

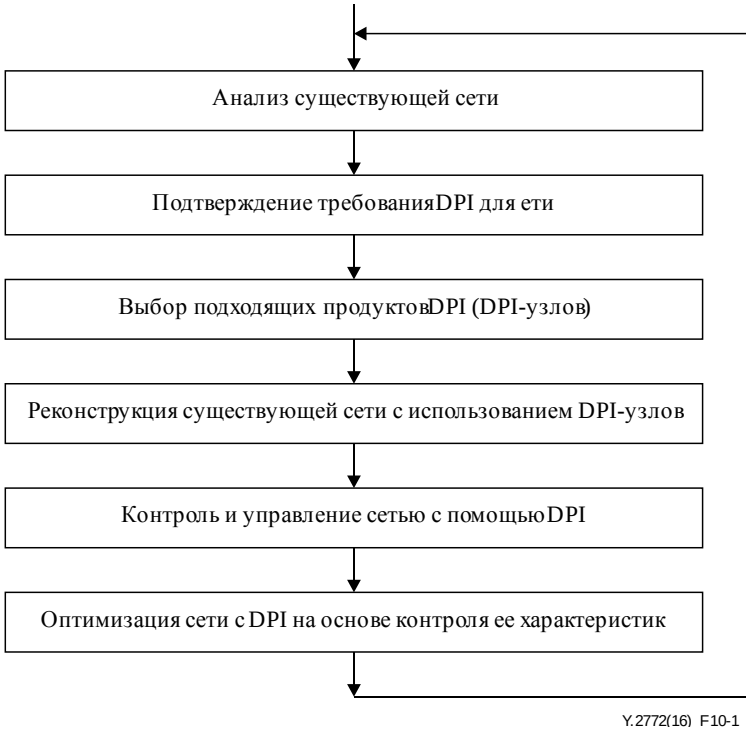

Рисунок 10-1 − Иллюстрация процесса создания и эксплуатации сети с DPI-узлами

10.2 Цели механизма эксплуатации

10.2.1 Общая цель

Общие цели применения DPI-технологий связаны со следующими тремя аспектами:

1) контроль состояния существующей сети;
2) инструктаж операторов по восстановлению и оптимизации сети;
3) улучшение характеристик сети.

10.2.2 Конкретные цели

Механизм эксплуатации преследует следующие конкретные цели:

– развертывание узлов DPI без влияния на существующие онлайновые службы;
– мониторинг всех видов трафика активной сети;
– выявление трафика, не соответствующего установленным правилам политики;
– анализ состояния сети на основе детального контроля ее характеристик;
– перераспределение ресурсов сети на основе анализа ее состояния;
– реконструкция и совершенствование сети на основе ее состояния;
– повышение уровня удовлетворенности пользователей сети.

10.3 Аспект характеристик сети при развертывании узлов DPI

В принципе, развертывание узлов DPI не должно приводить к прерыванию работы существующих сетевых служб и приложений. Однако на практике, когда в сеть устанавливается узел DPI, могут иметь место некоторые негативные последствия для сетевых служб и приложений. Негативное влияние развертывания узлов DPI после установки должно соответствовать особым требованиям.

10.3.1 Спецификация развертывания узлов DPI вне тракта

Когда в сеть вводится узел DPI вне тракта, время прерывания работы существующих служб и приложения должно быть меньше 50 мс. Теоретически развертывание узлов DPI вне тракта может осуществляться без прерывания работы служб и приложений.

10.3.2 Спецификация развертывания узлов DPI в тракте

Когда в сеть вводится узел DPI в тракте, время прерывания работы существующих служб и приложения должно быть меньше 50 мс. Цель в 50 мс может быть достигнута с помощью вспомогательных методов или инструментов. Например, перед развертыванием узла DPI в тракте можно сначала использовать резервную линию, а затем удалить ее, когда узел DPI в тракте сможет работать нормально.

10.4 Анализ существующих сетей

Перед развертыванием узла DPI необходимо получить некоторую информацию о существующей сети, например максимальную пропускную способность всех сегментов сети, активный средний трафик сегментов сети, распределение трафика сегментов сети по датам и времени, степень влияния при развертывании узла DPI. Как правило, эту информацию можно собирать с помощью NMS существующей сети.

Анализируя эту информацию, можно спроектировать схему построения сети с функциями DPI.

10.5 Подтверждение требования DPI для сети

Собрать информацию и подтвердить требование узла DPI на основе описанного выше анализа существующей сети.

10.6 Выбор надлежащих объектов или систем DPI

Объекты DPI, используемые для построения сети с функциями DPI, должны отвечать требованиям, описанным в пункте 10.4.

10.7 Реконструкция существующей сети с использованием DPI

Развертывание устройств DPI не должно приводить к ухудшению характеристик существующей сети; особенно важно, чтобы не были затронуты онлайновые службы. Создавать физические объекты DPI вне тракта удобнее, чем физические объекты DPI в тракте, однако при неправильной работе они могут повлиять на обслуживание. Поэтому необходимо правильно выбрать время и место, чтобы свести влияние к минимуму, причем этот выбор времени и места должен определяться онлайновым трафиком сети.

Важно, чтобы узел DPI поддерживал функцию внутреннего обходного пути, когда он развернут в сети и работает как узел DPI в тракте. Рисунок 10-2 иллюстрирует функцию внутреннего обходного пути, который показан пунктирной линией. Когда потоки пакетов следуют по обходному пути, это эквивалентно отсутствию узла DPI в сети. Другими словами, с точки зрения потоков пакетов сетевое устройство, предшествующее узлу DPI, непосредственно соединено с сетевым устройством, расположенным после узла DPI.

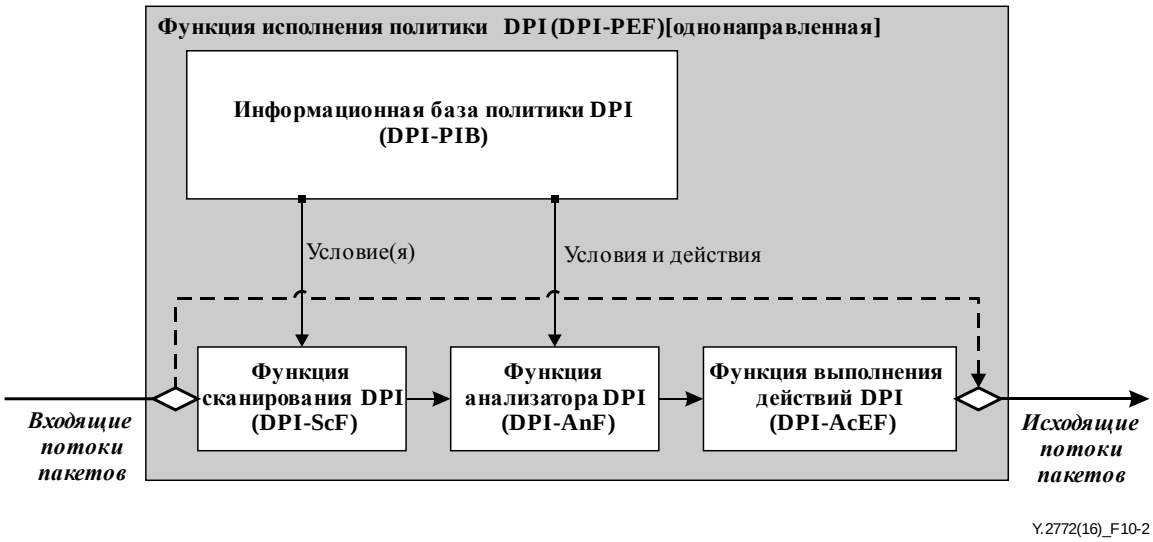

Рисунок 10-2 − Функция внутреннего обходного пути узла DPI

10.8 Контроль и управление сетью с помощью DPI

В общем случае сети с функциями DPI сложнее сетей без функций DPI. Поэтому в сети с DPI всегда следует использовать уровень эксплуатации, администрирования и технического обслуживания (OAM). То есть узлы DPI и их PIB нужно поддерживать и администрировать.

10.9 Реконструкция сети с DPI на основе контроля характеристик

В общем случае реконструкция сети с функциями DPI представляет собой адаптивный процесс. Структура сети постепенно корректируется в зависимости от изменения характеристик ее состояния. Мониторинг состояния сети зависит от соответствующих данных и статистического анализа.

11 Спецификация механизма управления

11.1 Обзор управления сетью DPI

Как и любой типичный сетевой элемент, узел DPI должен поддерживать функции управления конфигурацией, отказами, характеристиками и мерами безопасности. Эти функции управления определены в других Рекомендациях и не входят в сферу применения настоящей Рекомендации. Однако некоторые специальные соображения по управлению сетями DPI приведены в этом разделе.

В средах с двунаправленной DPI функции двунаправленной DPI могут быть реализованы либо одним узлом DPI (режим одного узла, см. рисунок 11-1), либо парой узлов DPI (режим с двумя узлами, см. рисунок 11-2). Во многих случаях режим с двумя узлами выгоднее режима одного узла. Например, когда нужно заблокировать определенный трафик, использование режима с двумя узлами позволяет заблокировать этот трафик раньше.

Тот факт, что два взаимодействующих узла DPI могут быть развернуты физически независимо друг от друга и управление этими узлами DPI должно быть унифицированным, усложняет управление, поскольку в таких условиях управление сетью должно осуществляться на уровне подсети, а не на уровне узла.

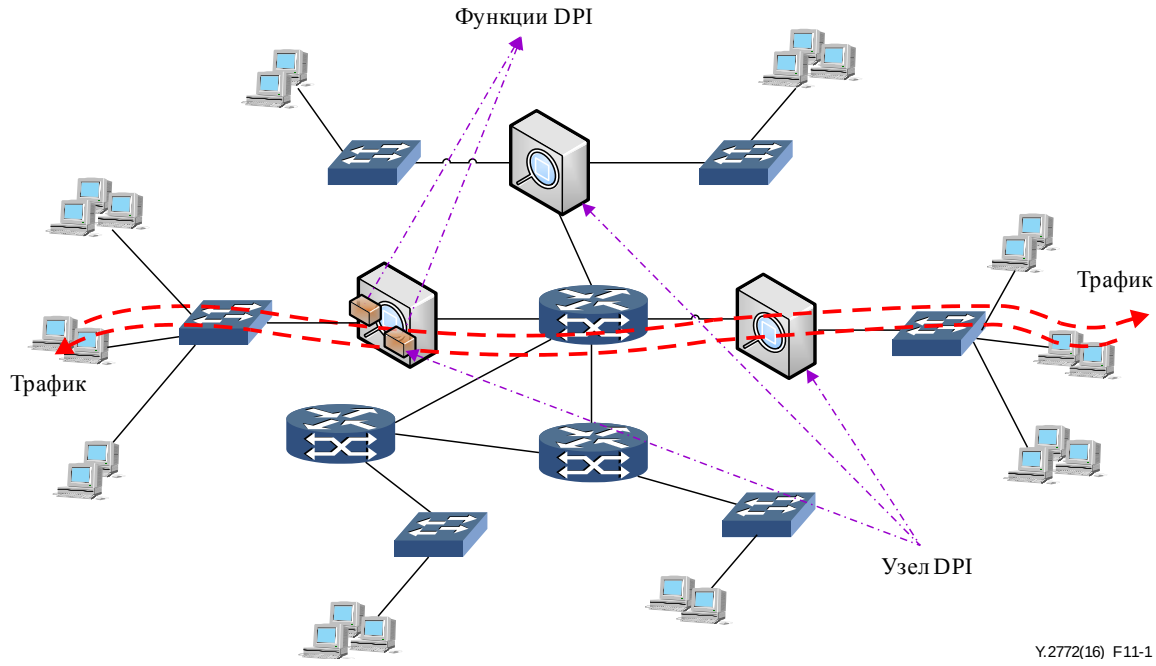

Рисунок 11-1 − Функции двунаправленной DPI, осуществляемые одним узлом DPI (режим одного узла)

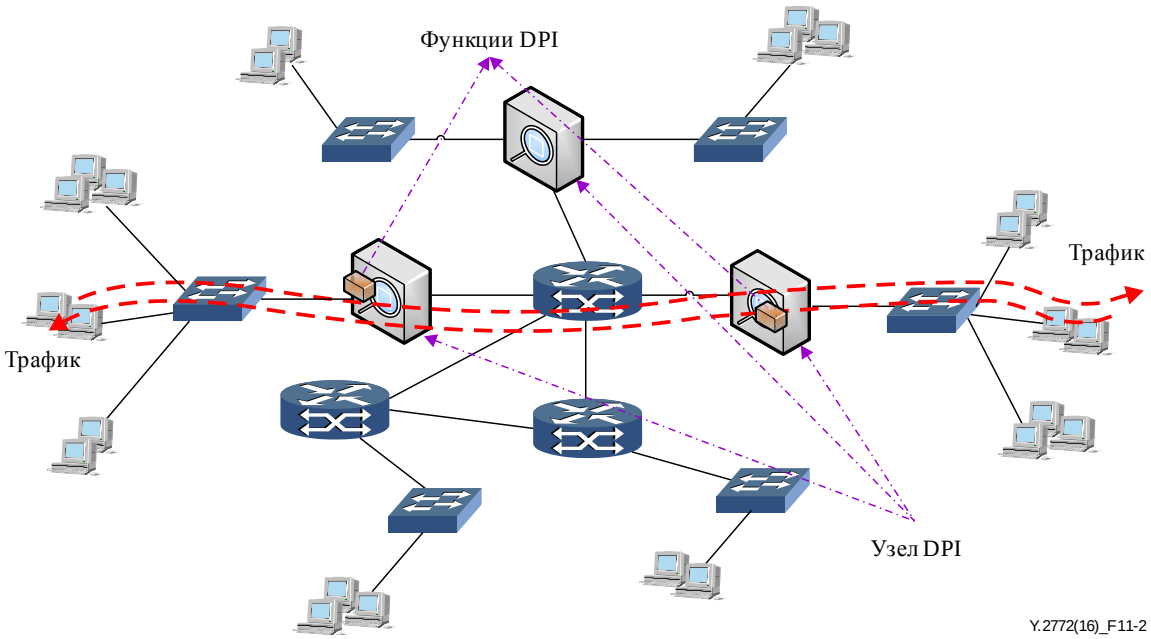

Рисунок 11-2 − Функции двунаправленной DPI, осуществляемые парой узлов DPI (режим двух узлов)

11.2 Интерфейс управления

11.2.1 Интерфейс управления однонаправленной DPI

Общее управление однонаправленной DPI может осуществляться, как показано на рисунке 11-3, где связь между узлом DPI и системой управления сетью (NMS) представляет собой не прямое физическое соединение, а, скорее, логическое соединение через подсеть. На рисунке эта связь между узлом DPI и NMS показана пунктирной линией. Логически интерфейс управления между узлом DPI и NMS можно описать следующим образом.

Интерфейс командной строки (CLI) – NMS управляет узлом DPI и контролирует его через последовательный порт, а действия по управлению осуществляются посредством набора однострочных команд. В каждый момент времени NMS может управлять только одним действующим узлом DPI.

Графический интерфейс пользователя (GUI) – NMS управляет узлом DPI и контролирует его через порт Ethernet или другой физический порт, а действия по управлению осуществляются посредством обмена группой пакетов протокола между узлом DPI и NMS. NMS может управлять одним или несколькими действующими узлами DPI одновременно.

Интерфейс Telnet – NMS управляет узлом DPI и контролирует его через порт Ethernet или другой физический порт, а действия по управлению осуществляются посредством набора однострочных команд. В каждый момент времени NMS может управлять только одним действующим узлом DPI.

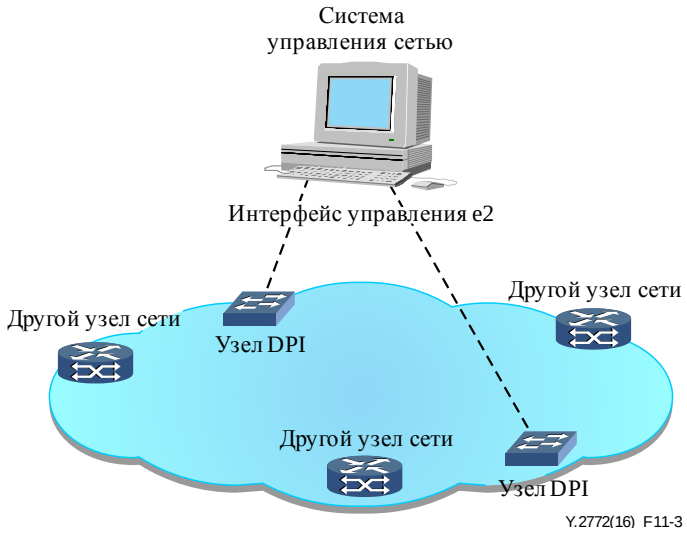

Рисунок 11-3 − Управление сетью с однонаправленной DPI

11.2.2 Интерфейс управления двунаправленной DPI

Управление двунаправленной DPI может осуществляться, как показано на рисунке 11-4. По сравнению с управлением однонаправленной DPI, управление двунаправленной DPI (см. рисунки 11-1 и 11-2) может оказаться сложнее, поскольку два или более узлов DPI взаимозависимы. Поэтому между двумя узлами DPI, конечно, необходимо установить те или иные соединения. Это не обязательно должны быть прямые физические соединения; они могут проходить через подсеть или NMS. На рисунке 11-4 эти соединения показаны пунктирными линиями. В дополнение к интерфейсу управления однонаправленной DPI для управления двунаправленной DPI должен использоваться следующий интерфейс управления.

Интерфейс e3 (см. рисунок 11-2) – интерфейс между двумя взаимодействующими узлами DPI, который гарантирует совместимость информации двух узлов DPI и обеспечивает логическое соединение между двумя взаимодействующими узлами DPI.

В сценариях применения двунаправленной DPI эффективнее и экономичнее реализовать функции двунаправленной DPI на основе взаимодействия пары узлов DPI, когда один узел DPI, отвечает за функцию DPI одного направления, а другой – за функцию DPI противоположного направления. Таким образом, PIB в двух узлах DPI должны совпадать; изменения PIB одного узла DPI должны вызвать соответствующие изменения в PIB другого узла DPI.

Например, если функции двунаправленной DPI должны выполняться применительно к трафику между сетевыми устройствами A и B, то в одном узле DPI должно быть настроено правило управления политикой, применяемое к потоку данных из A в B, а в другом – правило управления политикой, применяемое к потоку данных из B в A. Следует отметить, что система управления сетью должна информировать узлы DPI лишь о том, что от них требуется реализация функции двунаправленной DPI по отношению к трафику между A и B. Настройка PIB в двух узлах DPI должна выполняться автоматически узлами DPI, и, таким образом, необходим обмен информацией между узлами DPI, осуществляемый через интерфейс e3.

Кроме того, для обмена информацией должен использоваться тот или иной протокол для реализации взаимодействия между узлами DPI, и пакеты данных этого протокола также передаются через интерфейс e3.

Рисунок 11-4 − Управление сетью с двунаправленной DPI

11.3 Протокол и функции управления

В качестве протокола управления между NMS и узлом DPI или подсетью DPI можно использовать простой протокол управления сетью (SNMP), протокол передачи общей управляющей информации (ПОУИ) или любой другой протокол управления.

В число функций управления входят традиционное управление конфигурацией, управление сигнализацией и управление характеристиками. Кроме того, функция поддержки PIB подсети двунаправленной DPI должна быть адаптирована к NMS.

12 Вопросы безопасности

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

Согласно [ITU-T Y.2770], объект DPI-FE и информация, относящаяся к работе DPI, должны быть защищены от возможных неблагоприятных воздействий. Соблюдение требований безопасности, установленных в [ITU-T Y.2770], обеспечивают механизмы, описанные в [ITU-T Y.2704].

Библиография

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

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

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

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

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

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
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	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
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

Отпечатано в Швейцарии
Женева, 2016 г.