

## ТЕСТИРОВАНИЕ СЕТЕВЫХ ПРОТОКОЛОВ НОВОГО ПОКОЛЕНИЯ IPv6

SCHAFF A., НЕМЧЕНКО В.П.

Обосновывается необходимость перехода к сетевым технологиям нового поколения на основе протоколов IPv6. Приводится классификация типов ошибок сетевых протоколов. Показываются методы их тестирования, типы тестов и формы их представления.

Стремительная информатизация современного общества зиждется на широкомасштабном использовании сетевых технологий, в основе которых лежит применение сетевых протоколов. Созданный в 70-х годах стек сетевых протоколов TCP/IP в первой половине 80-х годов стал сетевым стандартом сначала в США, а затем и в других странах и сейчас используется под обобщающим названием IPv4. С тех пор стек протоколов претерпел ряд изменений, но суть его осталась прежней.

Рост масштабов сетей, изменение характера сетевых приложений, усилившиеся требования к информационной безопасности привели к необходимости перехода на новую концепцию в сетевых технологиях. Среди основных, но не единственных недостатков протокола версии IPv4 отметим: недостаточность объема 32-битного адресного пространства; сложность агрегирования маршрутов, разрастание таблиц маршрутизации; сложность массового изменения IP-адресов; отсутствие мер безопасности при пересылке информации по открытым сетям.

Все сказанное выше привело к появлению нового поколения сетевых протоколов, объединенных под общим названием IPng (Internet Protocol Next Generation) или, как его чаще называют, IPv6 [1].

Среди его основных достоинств выделим следующие: расширено адресное пространство — 128 бит; упрощен стандартный заголовок IP-пакета; улучшена поддержка иерархической адресации, агрегирования маршрутов и автоматического конфигурирования адресов; введены механизмы аутентификации и шифрования на уровне IP-пакетов.

Естественно, введение в практику нового поколения сетевых протоколов — процесс достаточно длительный и многоэтапный. На сегодняшний день разработаны и уже внедряются в практику основные идеи IPv6. Сейчас наступил этап проверки созданных протоколов на их соответствие требованиям — этап тестирования протоколов IPv6 [2].

Настоящая статья является в некотором смысле обзорной и не претендует на изложение оригинальных идей, а направлена на ознакомление читателя с состоянием дел в области тестирования сетевых протоколов.

### 1. Модель сетевых протоколов

На сегодняшний день в качестве базовой модели, позволяющей формально описывать поведение сетевых протоколов, в том числе и протоколов версии IPv6, выбрана модель, представленная на рис. 1.

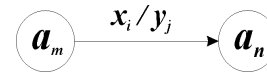


Рис. 1. Графическая модель конечного автомата

В данной модели используются следующие обозначения:  $a$  — состояние протокола в некоторый момент времени;  $x_i$  — входная команда (слово), реализуемая протоколом;  $y_j$  — реакция протокола на входную команду (выходное слово).

Характерно, что существующие другие типы моделей, описывающих протоколы, также могут быть в конечном итоге приведены к данной графической модели. Поэтому целесообразно принять ее в качестве базовой.

### 2. Типы ошибок

Структура всякого сетевого протокола, набор его команд, его поведение всегда строго регламентированы и определяются спецификацией протокола, которая задокументирована и представлена в виде Request for Comments (RFC). Список и сами RFC всех протоколов можно найти в Интернете на странице <http://rfc.net>.

Представив спецификацию некоторого протокола в виде описанной выше графической модели, мы получаем эталонную модель протокола. Предположим, что согласно спецификации некоторый протокол имеет модель, фрагмент которой представлен на рис. 2,а. На рис. 2,б приведена модель, описывающая поведение данного протокола при наличии в нем некоторого множества ошибок.

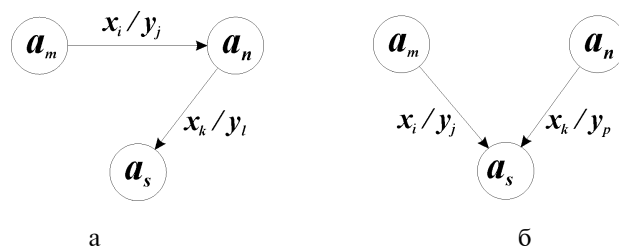


Рис. 2. Графическая модель протокола: а — спецификация протокола; б — протокол с ошибками

Исходя из данной модели, можно дать следующую классификацию возможных ошибок в протоколе, представленном графической моделью конечного автомата (рис. 2).

**Ошибка выхода:** на переходе  $a_n$  а  $a_s$  под воздействием входного слова  $x_k$  вырабатывается выходное слово  $y_p$  вместо заданного  $y_l$ .

**Ошибка перехода:** вместо перехода  $a_m$  а  $a_n$  реализуется ошибочный переход  $a_m$  а  $a_s$ .

*Ошибка состояния*: количество состояний в спецификации протокола и в его реализации не совпадает.

Отметим, что на практике часто имеет место одновременное присутствие ошибок разного типа.

### 3. Типы тестовых последовательностей

Рассмотрим классификацию тестовых последовательностей для проверки сетевых протоколов.

1. *Тесты соответствия* проверяют соответствие поведения проверяемого протокола поведению, предусмотренному спецификацией протокола.

Приведем несколько причин, по которым может возникать несоответствие протокола его спецификации. Прежде всего, это ошибки, связанные с неправильным выполнением некоторой операции, т.е. ошибки выхода. Кроме того, это ошибки перехода, связанные с осуществлением неправильного перехода из одного состояния протокола в другое. Все эти типы ошибок были рассмотрены выше (см. рис. 2,б).

Анализ показывает, что все множество тестов соответствия может быть разбито на четыре группы:

1.1. *Тесты базового взаимодействия* проверяют элементарное поведение протокола при выполнении таких базовых команд как “открыть / закрыть связь”, “передать данные” и т. п.

1.2. *Тесты производительности протокола* проверяют корректность отнесения протокола к заданному классу.

1.3. *Тесты динамического поведения протокола* проверяют возможности протокола выполнять такие действия как управление потоками информации, мультиплексирование, сегментирование и т. п. Естественно, что таких тестов может быть достаточно много и поэтому задача их генерирования в основном ложится на плечи экспертов — специалистов, формирующих тестовые последовательности опытным путем.

1.4. *Тесты проверки характеристик протокола* направлены на проверку конкретных наперед заданных параметров протокола и определяются каждый раз исходя из реальной задачи проверки.

2. *Тесты устойчивости протокола* проверяют поведение протокола в “экстремальных” условиях при задании некоторых граничных параметров, не предусмотренных спецификацией протокола.

3. *Тесты параметров протокола* проверяют такие возможности протокола, как поддерживать максимальное количество параллельных подсоединений, максимальную пропускную способность и т. п.

4. *Тесты взаимодействия* проверяют возможности взаимодействия как минимум двух протоколов в реальных условиях.

### 4. Полнота тестов

Использование графической модели конечного автомата в качестве базовой позволяет свести задачу определения полноты генерируемой тестовой по-

следовательности к задаче оптимального покрытия графа, задающего функционирование некоторого сетевого протокола. Другими словами, требуется обойти все вершины графа и пройти по всем его дугам так, чтобы побывать в каждой вершине и пройти по каждой дуге минимальное количество раз. Здесь мы приходим к классической задаче, называемой в отечественной литературе “задачей коммивояжера”, а в зарубежной — “задачей китайского почтальона” (Chinese Postman Problem), описанной швейцарским математиком Эйлером еще в 1736 году. Не вдаваясь в подробности, напомним только, что задача в целом является переборной и имеет эвристические решения, позволяющие получить достаточно оптимальные результаты.

С другой стороны, вопрос полноты генерируемых тестов может быть сформулирован также в плоскости определения, насколько полно полученная тестовая последовательность покрывает спецификацию протокола. Теоретические выкладки этого аспекта полноты тестов выходят за рамки данной статьи. Подробнее с ними можно ознакомиться в [2].

### 5. Представление тестовых последовательностей

Необходимость выработки единых требований к способу представления тестовых последовательностей для сетевых протоколов привела к созданию международного стандарта (ISO 9646, part 3) представления тестов в табличном виде TTCN (Tree and Tabular Combined Notation). Это представление дает описание тестовых последовательностей, независимое от архитектуры тестов.

TTCN имеет два основных элемента: декларирующую часть и динамическую часть. В декларирующей части декларируются так называемые точки доступа к сервисам (Service Access Points), параметры UDP / UDS и некоторые другие параметры. Динамическая часть определяет таблицу, описывающую тестовую последовательность в форме дерева. Общий вид TTCN приведен на рис. 3.

Test reference identifier	Defaults	Purpose	Page
Behaviour description	Label	UDS / UDP	Results
	event A		
	event B		
	event C		
	event D		
	event E		

Рис. 3. Представление тестов в виде TTCN

Здесь *Event* представляют собой действие тестера, который находится либо в состоянии ожидания входного сообщения (в реальной TTCN обозначается знаком ?), либо в состоянии выработки выходного воздействия, команды (обозначается знаком !).

Горизонтальная ось таблицы говорит о временной очередности событий. События, находящиеся на одной вертикальной оси, реализуются в один и тот

же момент времени. Остальные события наступают либо раньше, либо позже данного события в зависимости от их месторасположения по отношению к вертикальной оси. Вертикальная ось таблицы дает представление о наборе команд тестовой последовательности.

Возможны три исхода тестовой проверки протокола: *тест пройден (Passed)* – проверка говорит о том, что проверяемый протокол соответствует своей спецификации; *ошибка (Fail)* – говорит о том, что тест не соответствует своей спецификации; *неопределенность (Inconclusive)* – по результатам проверки нельзя сделать конкретное заключение.

Таким образом, тест протокола, записанный в виде TTCN, представляет собой некоторую последовательность команд проверяемого протокола и ожидаемых ответов на них. По совпадению или несовпадению реальных ответов на подаваемые команды делается заключение о работоспособности проверяемого протокола, о его соответствии спецификации или конкретным параметрам.

## 6. Применение тестовых последовательностей

Разработка нового сетевого программного обеспечения требует его проверки перед внедрением в практику. В полной мере это можно отнести к созданию и внедрению новых сетевых технологий и протоколов, таких как IPv6. Другими словами, речь идет об использовании методов тестирования сетевых протоколов.

Можно выделить два этапа в тестировании протоколов.

На первом этапе требуется осуществлять тестирование сетевых протоколов на их соответствие спецификациям. Для этого используются *тесты соответствия*.

На втором этапе используются *тесты взаимодействия* для проверки возможностей взаимодействия новых протоколов с уже существующими протоколами и с другим программным обеспечением.

Вопросы, связанные с разработкой и использованием *тестов соответствия*, рассмотрены выше. Сделаем несколько замечаний, связанных с использованием *тестов взаимодействия*.

Необходимость в применении тестов взаимодействия возникает в связи с использованием различными протоколами общих входных значений, общих баз данных, в связи с выработкой выходных данных в заданном формате, а также исходя из необходимости проведения в жизнь общей “политики” для всех разрабатываемых и уже существующих протоколов.

Следует отметить, что существующая в настоящее время международная программа “bone” по поэтапному внедрению нового семейства протоколов IPv6 в практику, в которой участвуют страны северной Америки, Европы и Японии, предполагает широкое использование методов тестирования сетевых протоколов. Сегодня уже существует ряд программ, позволяющих строить тестовые последовательности для разрабатываемых протоколов.

Вместе с тем, потребность в новых разработках существует и требует все новых исследований и практических реализаций в данной области.

В заключение отметим, что настоящая статья появилась в результате сотрудничества кафедры АПВТ Харьковского технического университета радиотехники (Украина) и группы RESEDAS INRIA Lorraine при университете Nancy-1 (Франция) и предполагает продолжение совместных исследований в данной области [3].

## Summary

The present article is the survey paper and does not claim for the original ideas presentation and is destined on acquaintance of the reader with a state of businesses in the network protocol testing field. Now, there is a transition from a usage of the IPv4 protocols to the application of the new IPv6 protocol set. The necessity for development of the new network protocol testing methods is appeared. In this article the usage of a graphic representation of the protocol models is exhibited and also the possible types of errors on an example of the protocol model are parsed. The classification of the test sequences for the check of the network protocols is indicated. The tabular form of the tests presentation – TTCN (Tree and Tabular Combined Notation) is circumscribed. The usage of the some types of the test sequences is exhibited also.

**Литература:** 1. Cizolt G. IPv6. Editions O’Peilly. Paris. 1998. 2. Castanet R. Test de protocoles de communication. Réseaux de Communication et Techniques Formelles. Paris – septembre 1994. 3. Nemchenko V. Génération des séquences de test pour les protocoles IPv6. Sécurité dans IPv6. Rapport de Recherche. INRIA Lorraine. Nancy. Décembre 2000.

Поступила в редколлегию 19.12.2000

**Рецензент:** д-р техн. наук, проф. Кривуля Г.Ф.



**Schaff Andre**, д-р философии, профессор Университета-1 Анри Пуанкаре г. Нанси (Франция). Научные интересы: сетевые протоколы и безопасность. Увлечения и хобби: литература. Адрес: 615 rue du Jardin Botanique, 54600 Villers les Nancy; tel.: 83592011.

**Немченко Владимир Петрович**, канд. техн. наук, профессор ХТУРЭ. Научные интересы: техническая диагностика, сетевые технологии. Увлечения и хобби: иностранные языки. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-94-17.