

ПРИМЕНЕНИЕ ПРОБНИКОВ ДЛЯ ОБЕСПЕЧЕНИЯ ОБЪЕКТИВНОСТИ ТЕСТИРОВАНИЯ СЕТЕЙ СВЯЗИ

Р. Я. Пирмагомедов

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Адрес для переписки: prya@spbgut.ru

Аннотация

В настоящей статье описываются архитектура и процедуры сигнализации, которые могут использоваться для удаленного тестирования параметров сети с использованием зондирующих устройств - пробников. Эти процедуры включают в себя непосредственно тестирование, описание профилей тестирования, сохранение результатов измерений и авторизованный доступ пользователей к результатам тестирования. Рассмотренные процедуры позволяют пробнику функционировать по принципу «черного ящика» для записи всех событий на стороне абонента что позволяет обеспечить разрешение споров между различными заинтересованными сторонами. В основе рассмотренной в настоящей статье системы лежат рекомендации, разработанные рабочей группой по тестированию сетей связи, одиннадцатой исследовательской комиссии сектора стандартизации Международного союза электросвязи.

Ключевые слова

ИМТ2020, тестирование сетей, пробники, QoS.

Информация о статье

УДК 004.77

Язык статьи – русский.

Поступила в редакцию 02.07.19, принята к печати 02.09.19.

Ссылка для цитирования: Пирмагомедов Р. Я. Применение пробников для обеспечения объективности тестирования сетей связи // Информационные технологии и телекоммуникации. 2019. Том 7. № 1. С. 52–59. DOI 10.31854/2307-1303-2019-7-1-52-59

APPROACHING TRUSTED TESTING OF NETWORKS WITH THE USE OF PROBES

R. Pirmagomedov

The Bonch-Bruевич Saint-Petersburg University of Telecommunications,
Saint Petersburg, 193232, Russian Federation

Corresponding author: prya@spbgut.ru

Abstract—This paper presents a system-level architecture and signaling procedures of the system enabling trusted testing of telecommunication networks utilizing probes. The described system relies on the ongoing work of Study Group 11 at the International Telecommunication Union. The paper also includes testing profiles description, results storing, and users' access to the results. In a nutshell the considered approach allows for the testing system to operate as a "black box" recording all required network events on the user side. The results of such testing can be further used for resolving disputes between stakeholders. The system discussed in this paper is rely on current work items of Q9/11 of International Telecommunication Union (Standardization sector).

Keywords—IMT2020, network testing, probes, QoS.

Article info

Article in Russian.

Received 02.07.19, accepted 02.09.19.

For citation: Pirmagomedov R.: Approaching trusted testing of networks with the use of probes // Telecom IT. 2019. Vol. 7. Iss. 1. pp. 52–59 (in Russian). DOI 10.31854/2307-1303-2019-7-1-52-59

Введение

В эпоху цифровой экономики, надежная работа сетей связи является необходимым компонентом устойчивого развития. Нарушения в работе сетей связи могут привести к ощутимым издержкам, например в сферах электронной торговли, банковском секторе, или системах контроля и управления. В этой связи особую актуальность приобретают вопросы тестирования и измерения сетевых параметров. В настоящий момент международные организации по стандартизации в области телекоммуникаций ведут активную разработку рекомендаций и стандартов, регламентирующих методы и методики тестирования. В частности, в 11 исследовательской комиссии сектора стандартизации Международного союза электросвязи (ITU-T) разработана рекомендация Q.3960 которая определяет базовые принципы и подходы к тестированию сетей связи [1]. Однако открытым остается вопрос методологии тестирования, обеспечивающей доверие к результатам тестирования со стороны как пользователей, так и операторов.

Большинство операторов имеют частные технические решения для оценки производительности своих сетей, и у пользователей нет альтернативных способов обоснования каких-либо претензий в отношении надлежащего или неадекватного предоставления услуг связи. Решение этой проблемы включает в себя необходимость создание механизма, который может использоваться зондирующими устройствами (пробниками) чтобы их измерения которого могут доверять все заинтересованные стороны как абонент, так и оператор. Использование такого доверенного протокола позволит исключить возможное искажение результатов со стороны заинтересованных сторон и, таким образом, объективность контроля качества предоставляемых услуг.

В этой статье описана система распределенного тестирования сетей связи основанная на текущих разработках Q9/11 ITU-T. Данная система функционирует по принципу черного ящика, обеспечивая объективный контроль и регистрацию сетевых параметров.

Архитектура системы

Система удаленного тестирования параметров сети и услуг связи имеет клиент-серверную архитектуру и включает в себя следующие элементы:

Пробник – клиентская система контроля качества услуг связи, включающая следующие подсистемы:

- Тестовый узел приложения (SMP).
- Интерфейс взаимодействия узла тестирования приложений (SMP CI).

Сервер для удаленного тестирования параметров сетевых и коммуникационных услуг (RTNP-сервер), состоящий из следующих подсистем:

- Подсистема мониторинга (MCS).
- Система сбора, анализа и вывода данных (DCAOS).
- Тестовая база данных (MDB).
- Узел базы данных (PDB).

Архитектура системы изображена на рис. 1.

В зависимости от конкретных особенностей тестируемой сети и стоящих задач, все элементы и подсистемы, рассматриваемой системы, могут использоваться совместно или по отдельности в различных комбинациях.

SMP - программное обеспечение пробника, реализующее тестовые сценарии с использованием тестовых конфигураций, полученных из подсистемы мониторинга, с сохранением и передачей измерений и формированием на основе полученных тестовых конфигураций. выбранный протокол уровня 3-7 в соответствии с моделью OSI.

SMP реализует следующие основные функции:

- получает и передает информацию из / в SMP CI;
- реализует тестовые сценарии в соответствии с тестовыми конфигурациями, полученными из SMP CI;
- генерирует потоки трафика на основе тестовых конфигураций, полученных от CI SMP.

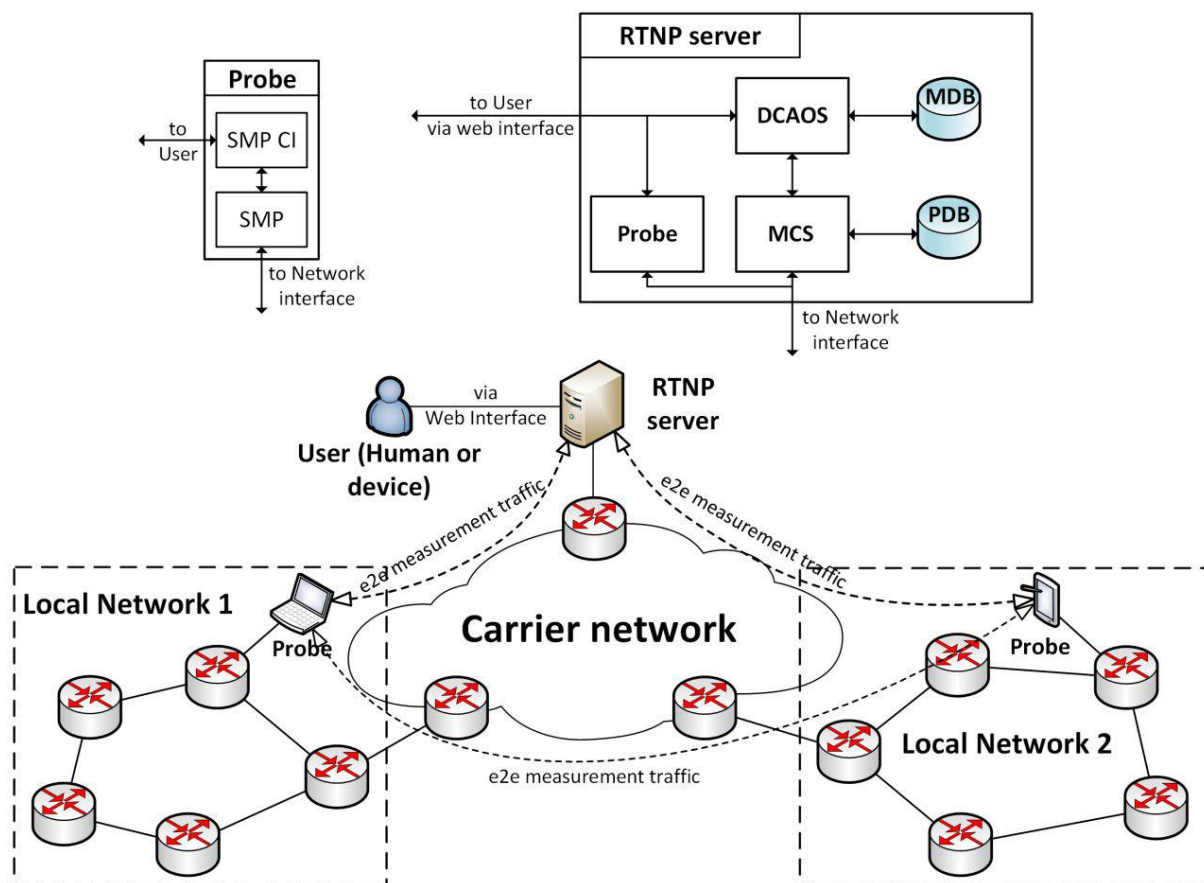


Рис. 1. Архитектура системы удаленного тестирования сети

SMP CI – программное обеспечение, которое обеспечивает взаимодействие пробника с остальными элементами системы. Этот модуль может быть реализован в виде графического интерфейса, консоли, сетевой интерфейса или программного интерфейса (API).

SMP CI выполняет следующие основные функции:

- прием и передача сигнальных сообщений от/к SMP;
- ввод/вывод текущей тестовой конфигурации (тестовые скрипты, PUID, IP-адрес, SMP-порт, MUID и т. д.)
- отправляет промежуточные и финальные результаты тестирования на RTNP сервер;
- обновляет программное обеспечение пробника.

Сервер системы для удаленного тестирования (RTNP) обеспечивает управление сеансами тестирования. Функциональные возможности сервера обеспечиваются подсистемами мониторинга и представления данных.

Подсистема мониторинга – это серверное программное обеспечение, которое контролирует выполнение тестовых сценариев. К основным функциям этой подсистемы относятся:

- регистрация пробников в системе, присвоение уникального номера идентификатора узла (PUID);
- подготовка тестовых конфигураций для пробников, включая уникальный идентификационный номер теста (MUID);
- прием и передача тестовых конфигураций с/на пробник;

- сбор с пробников промежуточных и окончательных результатов тестирования;
- запись и чтение данных о пробниках в базе данных (PDB) с использованием PUID;
- постоянный мониторинг QoS связи с пробниками в процессе тестирования;
- выполняет функции STUN-сервера и TURN-сервера (для реализации сценариев основанных на одноранговых (p2p) технологиях).

Подсистема представления данных - программная подсистема сервера, осуществляющая сбор, анализ и вывод данных, полученных в результате тестирования. К основным функциям этой подсистемы относятся:

- ввод и вывод информации о выполненных тестах;
- анализ информации, полученной по завершенным тестам;
- вывод архивных результатов выполненных тестов с помощью веб-интерфейса.

Кроме того, в состав архитектуры RTNP также входит база данных результатов тестирования, обеспечивающая хранение данных о выполненных тестах (с использованием MUID в качестве индекса), а также база пробников – обеспечивающая хранение данных о зарегистрированных в системе пробниках с использованием (с использованием PUID в качестве индекса).

Процесс тестирования

Общая схема тестирования с использованием пробников приведена на рис. 2. Тестирование сети опирается на распределенную систему зарегистрированных пробников, каждый из которых имеет встроенный аппаратный уникальный идентификатор. Идентификатор основан на уникальных свойствах аппаратного обеспечения и устойчив к взлому программными методами.

После того, как пробники установлены в точках тестирования, сервер RTNP обеспечивает их аутентификацию и авторизацию. Перед запуском теста сервер RTNP может убедиться, что все компоненты, участвующие в тестировании, готовы к запуску.

Процесс тестирования может включать в себя активные и / или пассивные режимы работы пробников. В пассивном режиме пробники измеряют параметры производительности сети с предварительно установленной периодичностью. В этом режиме процесс тестирования не оказывает существенного влияния на текущие операции в сети с заниженной нагрузкой, что позволяет проводить тестирование не прерывая работу сети. В активном режиме, пробники имитируют поток трафика определенного приложения, что может повлиять на характеристики работы сети или даже прерывать текущие процессы.

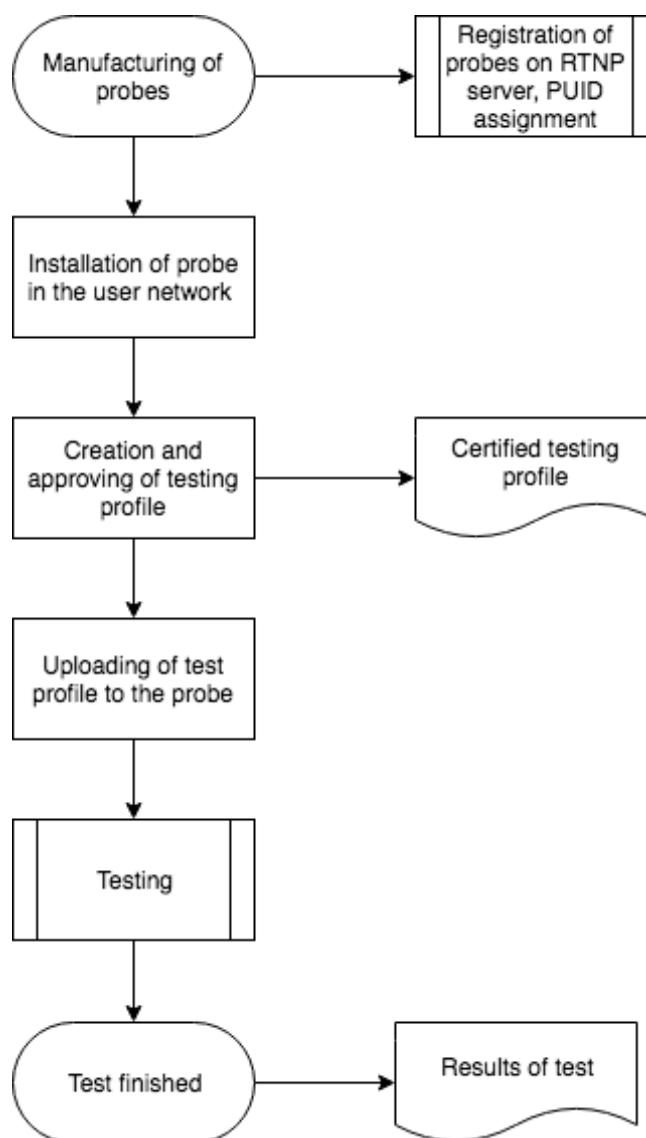


Рис. 2. Тестирование сети при помощи пробников

По окончании теста результаты сохраняются в соответствии с политикой, принятой пользователем и доступной через веб-интерфейс на сервере RTNP.

Профили тестирования

Следует учитывать, что результат тестирования может в значительной степени зависеть от установленных параметров теста [2, 3], и требует индивидуального подбора. Параметры теста хранятся в профиле тестирования. Перед тестированием, используемый профиль должен быть согласован заинтересованными сторонами – пользователем и поставщиком телекоммуникационных услуг. Профиль теста не может быть изменен в одностороннем порядке. Структура тестового профиля зависит от режима работы пробника.

Профиль тестирования для пассивного режима включает в себя набор параметров, которые должны контролироваться во время теста, частоту измерений и методологию измерения. Список параметров, подлежащих мониторингу, может включать, но не ограничивается:

- задержка, мс;
- джиттер, мс;
- коэффициент потери пакетов, отношение потерянных пакетов и полученных пакетов;
- измерение скорости соединения, Мбит/с.

Профили тестирования для активного режима в дополнение к параметрам, измеренным в пассивном режиме, включают в себя сценарии, описывающие модель трафика для приложения [4, 5]. Используя эти сценарии, зонды эмулируют работу приложений, используя похожие шаблоны трафика. Основные параметры, определенные сценарием:

- используемые протоколы прикладного уровня;
- используемые порты;
- распределение трафика между IP-адресами;
- соотношение скоростей восходящего и нисходящего потока;
- средний размер пакета, байт;
- средняя скорость передачи пакетов, пакетов / сек.

Заключение

Рассмотренная в настоящей статье система призвана обеспечить надежное и объективное тестирование сетевых параметров. Подобные системы могут быть особенно актуальными в системах, где сети связи являются критической инфраструктурой [6, 7]. Количество которых возрастает при полномасштабном внедрении сетей IMT2020. В настоящий момент в ITU-T завершается работа по подготовке рекомендации, описывающей подобную систему. Ожидается что выпуск этой рекомендации будет способствовать улучшению надежности сетей и услуг связи.

Литература

1. Губская О. А., Алисевиц Е. А., Кулик В. А., Киричек Р. В., Бородин А. С. Программно-аппаратный комплекс для тестирования качества услуг связи на базе Рекомендации МСЭ-Т Q. 3960 // Электросвязь. 2017. № 8. С. 25–32.
2. Pirmagomedov, R., Hudoev, I., Shangina, D. Simulation of Medical Sensor Nanonetwork Applications Traffic // Communications in Computer and Information Science. 2016. Vol. 678. pp. 430–441.
3. Kulik, V., Muthanna, A., Pham, V., Hakimov, A., Kirichek, R. V., Pirmagomedov, R. Ya. The Study of Semantic Gateway Performance // Электросвязь. 2017. № 6. С. 69–73.
4. Блинников М. А., Пирмагомедов Р. Я. Оптимизация нагрузки на сети связи общего пользования, вызванной трафиком медицинских наносетевых приложений // Информационные технологии и телекоммуникации. 2016. Т. 4. №. 3. С. 22.
5. Борисова М. В., Парамонов А. И., Пирмагомедов Р. Я. Анализ свойств трафика машина-машина и его влияния на качество обслуживания // Девятнадцатая Международная научная конференция «Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь» (DCCN). 2016. С. 36–43.
6. Volkov, A., Muhathanna, A., Pirmagomedov, R., Kirichek, R. SDN Approach to Control Internet of Thing Medical Applications Traffic // Communications in Computer and Information Science. 2017. Vol. 700. pp. 467–476.
7. Pirmagomedov, R., Moltchanov, D., Ustinov, V., Saqib, Md N., Andreev, A. Performance of mmWave-Based Mesh Networks in Indoor Environments with Dynamic Blockage // Lecture Notes in Computer Science. 2019. Vol. 11618. pp. 129–140.

References

1. Gubskaya, O. A., Alisevich, E. A., Kulik, V. A., Kirichek, R. V., Borodin, A. S. Software-Hardware Complex for Communication Quality Testing on the Basis of ITU-T Q.3960 Recommendation // *Elektrosvyaz'*. 2017. No. 8. pp. 25–32.
2. Pirmagomedov, R., Hudoev, I., Shangina, D. Simulation of Medical Sensor Nanonetwork Applications Traffic // *Communications in Computer and Information Science*. 2016. Vol. 678. pp. 430–441.
3. Kulik, V. A., Muthanna, A., Pham, V., Hakimov, A., Kirichek, R. V., Pirmagomedov, R. Ya. The Study of Semantic Gateway Performance // *Elektrosvyaz'*. 2017. No. 6. pp. 69–73.
4. Blinnikov, M., Pirmagomedov, R. Optimization of the Load on the Public Telecommunications Network, the Traffic Caused Medical Nanonetwork Application // *Telecom IT*. 2016. Vol. 4. Iss. 3. pp. 22–30 (in Russian).
5. Borisova, M. V., Paramonov, A. I., Pirmagomedov, R. Ya. Machine-to-Machine Traffic Analysis And Its Impact on Quality of Service // Nineteenth International Scientific Conference "Distributed Computer and Communication Networks: Control, Computation, Communications" (DCCN). 2016. pp. 36–43.
6. Volkov, A., Muhathanna, A., Pirmagomedov, R., Kirichek, R. SDN Approach to Control Internet of Thing Medical Applications Traffic // *Communications in Computer and Information Science*. 2017. Vol. 700. pp. 467–476.
7. Pirmagomedov, R., Moltchanov, D., Ustinov, V., Saqib, Md N., Andreev, A. Performance of mmWave-Based Mesh Networks in Indoor Environments with Dynamic Blockage // *Lecture Notes in Computer Science*. 2019. Vol. 11618. pp. 129–140.

Пирмагомедов

Рустам Ярахмедович

– кандидат технических наук, доцент, СПбГУТ,
Санкт-Петербург, 193232, Российская Федерация,
prya@spbgut.ru

Pirmagomedov Rustam

– Candidate of Engineering Sciences, Associate Professor, SUT,
St. Petersburg, 193232, Russian Federation,
prya@spbgut.ru