Тестирование телекоммуникационных протоколов: проблемы и подходы

Б.С.Гольдштейн, И.М.Ехриель, Р.Д.Рерле

Задача тестирования телекоммуникационных протоколов имеет почти такой же возраст, как и сами телекоммуникации и связанными с ними проблемы взаимодействия разнородных сетей с разнообразными протоколами. В нынешних условиях конвергенции сетей и услуг связи эта задача становится все более важной. Многообразие сетей и быстро растущее число соединений между ними обусловлены как увеличением числа операторов связи, предлагающих одинаковый набор услуг, так и появлением целого ряда принципиально новых сетей (ISDN, GSM, IN, VoIP и др.), которым необходимо взаимодействие с существующими сетями.

Усложнение архитектуры, взаимодействие нескольких разнородных сетей и разнообразие операторов и сервис-провайдеров создающейся прямо на глазах мультисервисной сети связи следующего поколения многократно увеличивают число интерфейсов, подлежащих тестированию в процессе пуско-наладочных работ, в случае возникновения неисправностей или при проведении регулярных испытаний. Взаимоотношения между операторами тоже становятся более сложными, что особенно критично для новых игроков на телекоммуникационном рынке, поскольку качество обслуживания, предоставляемое абоненту, зависит, в первую очередь, от качества межсетевого взаимодействия. К этому следует добавить необходимость обеспечить бесшовный доступ к услугам, который нужен любому сервис-провайдеру. И наконец, в связи с постоянным введением в сеть все новых и новых протоколов и услуг, усложняется и их внутренняя структура.

Наука и искусство тестирования протоколов

О том, что тестирование -- это больше искусство, чем наука, авторы уже писали не раз. Книга "Искусство тестирования программ" была почти так же популярна среди программистов старшего поколения, как и три культовых тома "Искусства программирования". И все же наука и даже техника тестирования и мониторинга протоколов сигнализации являются ключевыми элементами конвергенции сетей связи. Трудности научных и технических подходов к тестированию протоколов и получению необходимых количественных оценок часто связаны со сложностью оценки необходимого объема тестирования -- попробуйте ответить, например, на такой вопрос: насколько больше ошибок можно выявить, увеличив число тестов на 20%?

К этому можно добавить отечественную эксплуатационную прагматику, когда вкладывать деньги в тестирование не любят, так как оно не добавляет возможностей к уже закупленному оборудованию. Считается, что такое оборудование должно функционировать безошибочно, если его разработка выполнена корректно (полностью в соответствии со спецификациями заказчика).

Если уж что и можно противопоставить такой сложившейся практике, то только научно обоснованные методы тестирования. К ним относятся:

* тестирование соответствия (аттестационное);

* тестирование производительности;

* тестирование совместного функционирования;

* тестирования взаимодействия;

* тестирование функциональности;

* мониторинг.

Далее в данной статье мы рассмотрим эти методы, но сначала несколько слов о самом объекте тестирования.

Телекоммуникационные протоколы

Появившись задолго до зарождения сетей мобильной связи и IP-сетей, коммутируемая телефонная сеть общего пользования (ТфОП) существует уже многие десятилетия. Пока идея конвергенции сетей, согласно которой речь и данные должны передаваться одной и той же средой, постепенно пробивает себе дорогу, традиционная ТфОП живет и развивается в новых условиях. Современные узлы и станции ТфОП обычно используют один из трех стеков протоколов сигнализации: систему общеканальной сигнализации ОКС7, протокол DSS1 первичного доступа PRI и универсальный интерфейс сети доступа V5.2.

Система ОКС7 используется внутри ТфОП для сигнализации между транзитными коммутационными узлами и оконечными станциями, для доступа узлов и станций к сетевым базам данных, а также для

взаимодействия с пакетными сетями. ОКС7 можно рассматривать как особый тип передачи данных, специализированный для пересылки сигнализации и информационного обмена между процессорами узлов связи различного назначения. Эта система сигнализации является универсальной в том смысле, что она ориентирована на использование в разных сетях: телефонных, интеллектуальных, подвижной связи, передачи данных, а также на стыках тех и других сетей с ISDN и в самой ISDN.

Функциональная архитектура системы является многоуровневой, причем функции нижних уровней, которые вместе обеспечивают перенос сигнальных сообщений от станции-отправителя до станции-получателя, образуют единую платформу, необходимую во всех вариантах использования системы, в то время как функции более высоких уровней в каждом таком варианте специфические и выполняются соответствующими подсистемами -- пользователями этой платформы. В частности, при применении в ТФОП и ISDN названная платформа дополняется “сверху” подсистемой ISDN-UP (сокращенно ISUP), а также (в случае необходимости) -- подсистемой управления сигнальными соединениями SCCP, которая необходима для образования в сети ОКС виртуальных соединений для переноса через нее информации (вообще говоря, не только сигнальной).

Разные прикладные подсистемы, встраиваемые в систему ОКС7 (TCAP, OMAP, INAP и MAP и другие), позволяют решать задачи эксплуатационного управления сетью ОКС, обмена служебной информацией между узлами управления и узлами коммутации услуг Интеллектуальной сети, роуминга в сетях GSM и т. п.

В отличие от системы сигнализации DSS1, протоколы, используемые на интерфейсе V5, известны не так широко. Интерфейс V5.2 применяется для подключения оборудования сетей доступа к оконечным коммутационным станциям ТфОП. В недавнем прошлом внутренние интерфейсы между выносными абонентскими концентраторами и модулями подключения к оборудованию АТС не подлежали международной стандартизации. Расширение номенклатуры средств сети абонентского доступа вызвало потребность в стандартном интерфейсе, который позволил бы совмещать в одной сети оборудование разных производителей, и как следствие, создание универсального интерфейса V5 в двух модификациях: V5.1 и V5.2.

Через интерфейс V5.2 можно подключить оборудование по 16 трактам E1. Интерфейс является асимметричным. На одной стороне интерфейса находится местная телефонная станция (LE, Local Exchange), на другой -- сеть доступа (AN, Access network). Стек V5.2 содержит несколько протоколов, при этом наибольшей спецификой обладают протоколы сетевого уровня. Это протоколы передачи телефонной (ТфОП) сигнализации, управления (включает в себя протокол управления пользовательскими портами и протокол общего управления), размещения несущих каналов, управления трактами, защиты.

В конце статьи будет кратко рассмотрен необходимый инструментарий для функционального тестирования и тестирования производительности всех трех вышеупомянутых стеков протоколов ТФОП. Используя систему типа SNT-7531, можно также эмулировать работу ТфОП для мультисервисной сети следующего поколения (Next Generation Network -- NGN), как это показано на рис. 1.

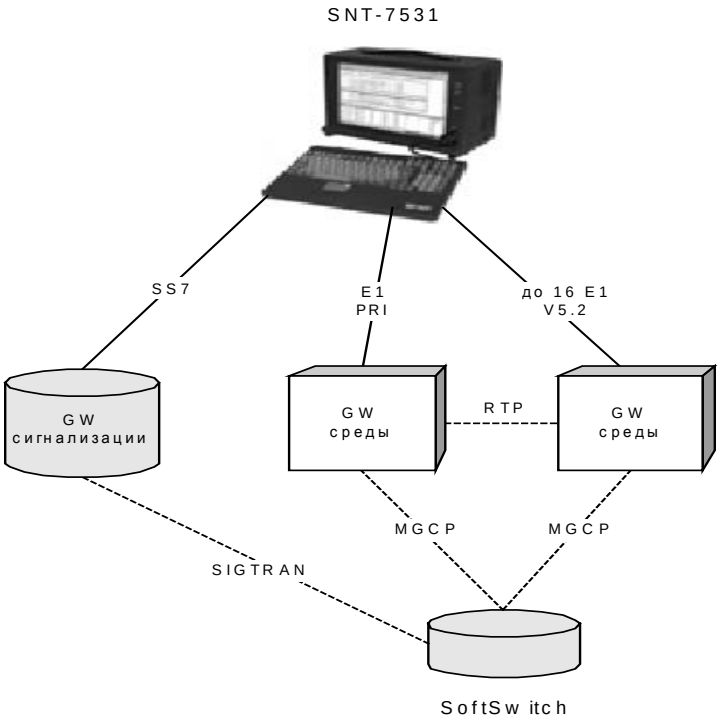

Рис.1. Тестирование медиа-шлюзов сетей NGN (GW -- шлюз)

Тестирование соответсвия

Тестирование на соответствие заданной спецификации (рис. 2) является наиболее стандартизированным и широко распространенным методом проверки корректности реализации протокола. Инструментальным средством для такого тестирования весьма удачно служит специализированный язык написания тестов TTCN.

Стандартизация тестирования на соответствие осуществляется международными организациями ETSI, ITU-T и ISO. Основным документом является стандарт ISO 9646, главная идея которого состоит в том, что спецификации каждого протокола должны содержать комплект тестовых сценариев его проверки. Вследствие своей узкоспециальной направленности эти комплекты не являются общедоступными и, как правило, бесплатно не распространяются. Такой тестовый комплект состоит их отдельных тестовых сценариев, каждый из которых проверяет определенную функцию из спецификации протокола. Результат выполнения сценария получает одно из трех значений: успешное (passed), неубедительное (inconclusive) или неудачное (failed).

Для процесса проведения тестирования стандартом ISO 9646 определяются следующие документы:

* проформа PICS,

* проформа PIXIT,

* структура комплекта ATS и перечень целей тестирования TSS&TP,

* комплект сценариев ATS на языке TTCN.

Проформа PICS отражает набор действительно реализованных сценариев и делается производителем оборудования, которое подвергается проверке. Поскольку стандарт любого протокола содержит обязательные и необязательные части, то в зависимости от действительно реализованных функций из всего комплекта выбираются лишь необходимые сценарии. Заполненная производителем оборудования проформа PICS показывает, в какой степени реализованы требования соответствующего стандарта (в основном, необязательной его части). Эта проформа используется для статической оценки соответствия и выбора из комплекта ATS тех тестовых сценариев, которые необходимы для проверки заявленной в PICS функциональности.

Полезность формы PIXIT обусловлена тем, что для тестирования реальной системы требуется дополнительная информация, описывающая зависящие от тестируемой системы (System Under Test -- SUT) данные. К этим данным относятся, например, информация о маршрутизации или данные, уточняющие информацию PICS (скажем, в части указания диапазона поддерживаемых значений

параметров). Эти данные группируются в специальной форме, которая и называется PIXIT, она заполняется в лаборатории, производящей тестирование системы по заявке ее производителя.

Язык TTCN является абстрактной нотацией для написания тестовых сценариев и стандартизирован организациями ETSI и ISO, как часть стандарта ISO 9646. Для получения исполняемого файла с тестовым сценарием требуется специальный компилятор, который зависит от типа прибора (т. е. компилятор TTCN одной системы тестирования не совместим ни с какими другими системами).

Наиболее известны и широко применяются комплекты ATS для тестирования подсистемы пользователя ISUP и прикладного протокола INAP системы сигнализации ОКС7, уровней 2 и 3 системы сигнализации DSS1, протоколов уровня 3 интерфейсов V5.1 и V5.2, о которых говорилось выше.

Рис.2. Модель тестирования соответствия

Тестирование производительности

В рамках рассмотренного выше тестирования соответствия выполняется комплект сценариев для проверки правильности реализации протокола. В случае успешного прохождения всех сценариев, считается, что протокол реализован правильно. Однако, одно лишь тестирование на соответствие не может гарантировать корректность реализации полностью, так как не предполагает проведение тестирования под нагрузкой и проверку поведения системы во всем диапазоне возможных значений параметров спецификации.

Модель тестирования производительности представлена на рис. 3. В ходе этого процесса измеряются такие параметры системы SUT, которые зависят от поступающей на систему нагрузки, и производится их сравнение с допустимыми значениями. Например, для ТфОП измеряется интенсивность потерь вызовов, и она сравнивается с нормами в промилях для конкретного типа узла коммутации. В более общем виде тестирование производительности сводится к измерению параметров качества обслуживания QoS (Quality of Service) или производительности сети NP (Network Performance) при различных значениях параметров поступающей нагрузки.

Инструментальными средствами для измерения значений параметров QoS и NP являются генераторы сигнального трафика, создающие нагрузку определенного вида на тестируемую систему посредством генерации последовательностей сообщений определенного протокола и измеряющие значения интенсивности появления ошибок протокола, интервалы времени между передачей и приемом сообщений (таймеры), интенсивность потерь вызовов (для протоколов ТфОП) и т. п.

Сетевой элемент разрабатывается из расчета обслуживания определенного объема реального трафика в час наибольшей нагрузки. Поэтому тесты производительности должны имитировать близкий к реальному трафик по таким параметрам, как длительность вызова и количество попыток вызова. Чтобы получить близкий к реальному трафик требуется большое количество генераторов, которые подсоединены к каждой абонентской или соединительной линии, генерируют на каждой из них нужный объем трафика и удерживают линию/канал на время, соответствующее средней длительности разговора. Кроме того, для генерации пуассоновского потока такие генераторы используют экспоненциальное случайное распределение между моментами посылки вызовов.

Непосредственная подача нагрузки на все входы системы при тестировании производительности удовольствие, как правило, дорогое, поэтому при измерениях приходится идти на компромиссы,

заключающиеся в зацикливании трафика, создании заведомо удлиненных и усложненных маршрутов, а также в уменьшении количества входов, по которым тестирующая система воздействует на тестируемую. Для того чтобы по меньшему количеству входов подать на тестируемую систему нагрузку, соответствующую реальной, увеличивают интенсивность вызовов на каждом из входов, пропорционально уменьшая их длительность. Возможно также измерение текущих параметров QoS и NP при наблюдении за работающим оборудованием в реальной сети.

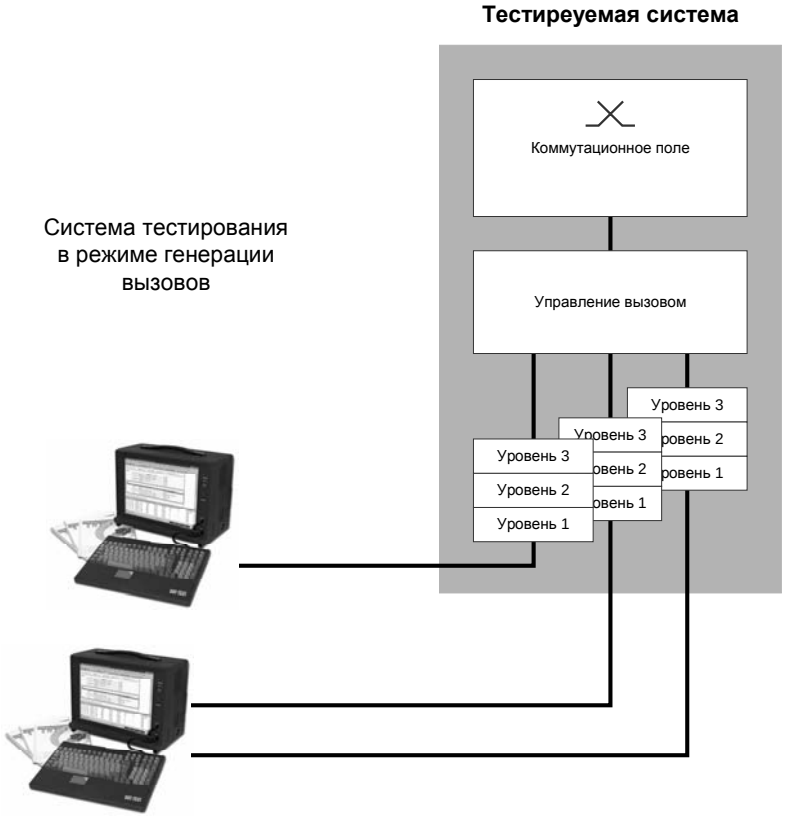

Рис.3. Модель тестирования производительности

Тестирование совместного функционирования

Практически все спецификации протоколов в той или иной степени содержат разделы, допускающие различную интерпретацию разработчиками и, следовательно, различную реализацию. Это, например, опциональные процедуры и параметры, разные значения параметров и величины таймеров. Неоднозначность спецификации приводит к тому, что реализации протоколов разных фирм-производителей не работают совместно, даже если каждая реализация успешно прошла предварительное тестирование на соответствие.

Тестирование совместного функционирования (рис. 4) является ключевым моментом для сетевых операторов, эксплуатирующих оборудование разных производителей. Очевидно, что сетевые элементы одного производителя должны корректно работать с сетевыми элементами другого производителя. Проверка этой возможностей может проводиться в лабораторных условиях или непосредственно в сети оператора.

На этапе тестирования совместного функционирования проверяется, в какой степени и при каких условиях разные реализации одного и того же протокола могут совместно работать, выдавая ожидаемый результат. Тесты этого вида можно применять как ко всем протоколам стека, используемого на интерфейсе, так и к какому-либо одному выбранному протоколу.

Тестирование совместного функционирования производится с применением эталонной системы (что не всегда возможно и дорого) или с использованием системы тестирования, имитирующей эталонную. Для имитации эталонной системы, с которой должно стыковаться тестируемое оборудование, служат симуляторы протоколов и генераторы вызовов. При использовании реальной системы в качестве эталонной применяются анализаторы протоколов, которые осуществляют мониторинг интерфейса, соединяющего тестируемую систему с эталонной.

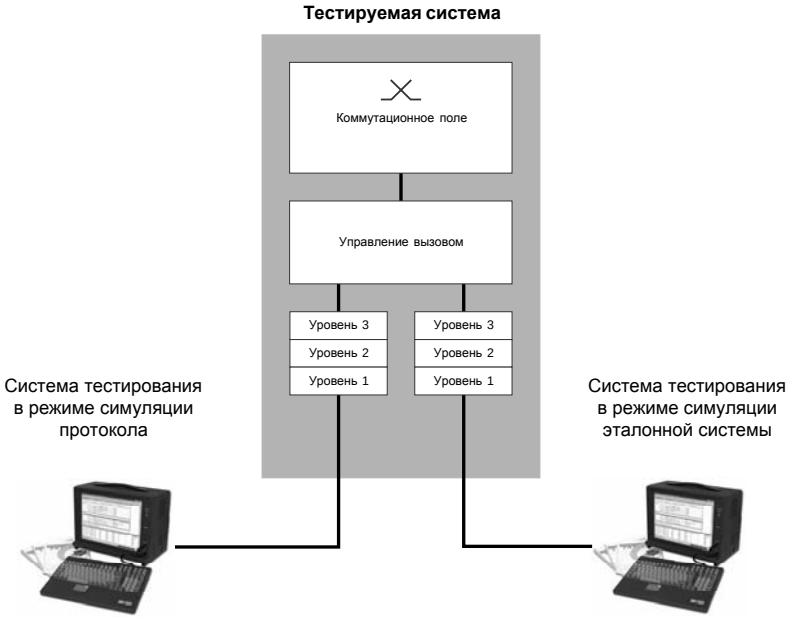

Рис.4. Модель тестирования совместного функционирования

Тестирование взаимодействия

Тестирование взаимодействия разных протоколов и систем сигнализации (рис. 5) приобретает важное значение для современных мультисервисных телекоммуникационных сетей благодаря уже упоминавшемуся в статье процессу конвергенции. Именно этот вид тестирования является основным для представленного на рис. 1 программного коммутатора Softswitch.

Тестирование взаимодействия необходимо и внутри ТфОП: между общеканальными системами сигнализации и интерфейсами (ОКС7, DSS1, V5) и системами сигнализации по выделенным каналам (2ВСК, 1ВСК, R2) с разными способами передачи регистровой информации (многочастотный импульсный челнок, пакет, MFC R2, DTMF). Чаще всего процедуры взаимодействия осуществляются элементами сети ТФОП, например, в тех случаях, когда аналоговый абонент звонит абоненту ISDN, используя в качестве межстанционной сигнализации подсистему ISUP ОКС7. Тесты взаимодействия проводят с помощью стандартных функций симуляции протоколов, дополненных графическими редакторами тестовых сценариев и конструкторами сообщений. Отечественные средства тестирования взаимодействия протоколов ВСС РФ рассматриваются в конце статьи.

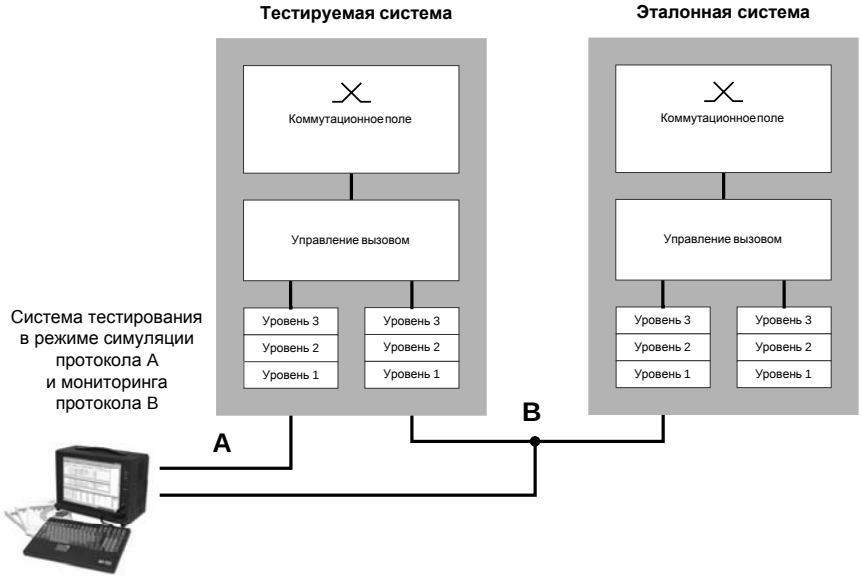

Рис.5. Модель тестирования взаимодействия

Функциональное тестирование

Сложность современных инфокоммуникационных систем обусловливает наличие огромного числа функций, для полной проверки которых требуются месяцы и годы проведения тысяч разных тестов. Поэтому с увеличением сложности телекоммуникационной инфраструктуры процесс тестирования осуществляется все более систематизированным образом. В частности, спецификации тестов для предыдущих версий оборудования используются для выборочной проверки того, что в новом оборудовании прежние функции (проверенные при тестировании старой версии) по-прежнему работают правильно. Эти проверки называются регрессионным тестированием. Только после регрессионного тестирования проверяются новые функции. Такой порядок тестирования называется функциональным. При его проведении основной акцент делается на проверку системы в условиях некорректной работы встречной стороны (с помощью симуляторов).

Мониторинг

Мониторинг телекоммуникационных протоколов является не только последней фазой тестирования протоколов, но и самой длительной и, пожалуй, самой важной. Именно поэтому он заслуживает отдельной статьи. Здесь же отметим лишь несколько причин, говорящих в пользу проведения периодического или постоянного мониторинга интерфейса между находящимися в эксплуатации сетевыми элементами. Такой мониторинг обеспечит:

* выявление ошибок при взаимодействии протоколов, не обнаруженных на других этапах тестирования;

* обнаружение несанкционированного доступа к ресурсам со стороны отдельных абонентов;

* сбор информации о вызовах (CDR) и транзакциях (TDR);

* трассировку вызовов;

* обнаружение зацикливания сообщений;

* контроль источников и маршрутов прохождения трафика.

Системы мониторинга и анализа сигнализации декодируют принимаемые от многочисленных каналов сети сигнализации сообщения и сигналы, проверяют их на предмет соответствия заданной спецификации, выделяют (как правило, красным цветом) сообщения или их отдельные параметры, не соответствующие спецификации, точно таким же образом они отображают перегрузки, аварийные ситуации и многое другое. Анализаторы не стоит путать с приборами, осуществляющими лишь простейшие функции мониторинга, когда вся принимаемая с линии информация декодируется произвольным образом без выделения ошибочных сообщений или параметров. Профессиональные анализаторы обладают развитой системой фильтрации по различным критериям. Фильтры позволяют из общей массы сообщений (нескольких десятков тысяч), накопленных, например, за сутки наблюдения, выделить только интересующую пользователя информацию.

Варианты реализации

В качестве иллюстрации реализации изложенного выше подхода кратко рассмотрим различные отечественные приборы тестирования: компактный анализатор SNTlite, многопортовый анализатор/симулятор общеканальных систем сигнализации SNT-7531, анализатор/симулятор систем сигнализации по выделенным сигнальным каналам UST-4268, специализированный тестер ТОР-2 и систему распределенного мониторинга и анализа сетей ОКС7 SpiderNM («Спайдер»). В совокупности они реализуют все описанные типы тестирования. Характеристики этих приборов по тестированию протоколов сигнализации ВСС РФ представлены в таблице.

Компактный анализатор SNTlite предназначен для оперативной диагностики проблем, возникающих в процессе эксплуатации коммутационных систем и требующих выезда специалиста на место установки оконечного коммутационного оборудования (РАТС, концентраторов, учрежденческих АТС или оборудования беспроводного доступа и др.). Он выполнен на базе ноутбука и малогабаритного внешнего интерфейсного модуля для подсоединения к первичному тракту ИКМ. Прибор поддерживает протоколы российских версий систем сигнализаций ОКС7, ISDN PRI, V5.1/V5.2 и 2ВСК, определяет состояние и проверяет качество тракта ИКМ (BERT).

Переносимый многопортовый анализатор/симулятор SNT-7531 предназначен для проведения всех видов профессионального тестирования телекоммуникационного оборудования ТфОП/ISDN, сетей GSM, региональных сетей передачи данных WAN, ЛВС, выделенных и частных сетей. Прибор выполняет мультипротокольный полнодуплексный мониторинг и анализ восьми трактов ИКМ, симуляцию и генерацию вызовов по 16 трактам ИКМ для проверки их на предмет соответствия российским спецификациям, рекомендациям ITU-T и стандартам ETSI. В SNT-7531 реализована поддержка стеков протоколов ОКС7, ISDN PRI/BRI, GSM/GPRS, IN, CAMEL, V5.1 и V5.2, QSIG, TCP/IP,

Frame Relay, X.25, H.323, а также сигнализации по 2ВСК. Он используется для решения задач, требующих одновременного мониторинга нескольких направлений и/или протоколов и анализа их взаимодействия, например, на крупных коммутационных узлах и АМТС ТфОП. Прибор обладает уникальной функцией мониторинга и анализа взаимодействия между протоколами 2ВСК и ISUP, 2ВСК и DSS1 для СЛ, ЗСЛ, СЛМ и МГК ВСС РФ. Наличие эмуляторов протоколов нижних уровней и симуляторов пользовательских и прикладных протоколов ISUP, INAP, DSS1 L3, V5.2 позволяет полностью реализовать все упомянутые выше виды тестирования в лабораториях при разработке и отладке оборудования, а также при проведении заводских испытаний.

Другая модификация этого же прибора -- UST-4268 -- специализирована для анализа систем сигнализации ТфОП по выделенным сигнальным каналам и осуществляет мониторинг и декодирование линейных и регистровых сигналов всех применяемых в России систем межстанционной сигнализации по 2ВСК и 1ВСК, многочастотной сигнализации методами "импульсный челнок", "импульсный пакет" и "безынтервальный пакет", сигнализации методами "норка" и индуктивным кодом, одночастотной сигнализации 2600, а также сигнализации R2 MFC и R2 DTMF. Прибор поддерживает режим симуляции протоколов по ВСК и режим осциллографа для проведения детального частотного анализа.

Система мониторинга и анализа сетей сигнализации "Спайдер" предназначена для постоянного наблюдения за состоянием элементов сети, контроля качества связи, сбора информации о возникающих в сети событиях, архивирования и статистической обработки информации по различным критериям, трассировки вызовов в пределах сети, генерации CDR, а также удаленного мониторинга и анализа протоколов ОКС7, применяемых в сетях ТФОП/ISDN/IN и GSM/GPRS. Система состоит из нескольких удаленных модулей SpiderNM/RU и одного или нескольких (по числу операторов) центров наблюдения SpiderNM/CU, соединенных между собой по выделенной технологической сети передачи данных.

Из таблицы видно, что профессиональные анализаторы редко могут предоставить одинаковые по качественному уровню функции в части анализа общеканальных систем сигнализации (ОКС) и сигнализации по выделенным каналам (ВСК). Это связано с диаметрально противоположными требованиями, предъявляемыми к программно-аппаратной платформе таких анализаторов. Так, анализаторы общеканальных протоколов должны принимать огромное количество сообщений, передаваемых по линии связи в цифровом виде с высокой скоростью по одному временному интервалу, в то время как анализаторы систем сигнализации по выделенным каналам должны производить частотный анализ в каждом временном интервале разговорного пучка.

Таблица: Функциональные характеристики и виды тестирования

Платформа тестирования SNT			Элементы			
Характеристики и функциональные возможности			**SNT-7531**	**SNTlite**	**SpiderNM**	**UST-4268**
Тип тестирования	На соответствие		+	-	-	+
	Производительности		+	-	-	-
	Совместной работы		+	+	+	+
	Взаимодействия		+	-	+	+
	Функциональное		+	+	+	+
	Автономный мониторинг		+	+	+	+
	Распределенный мониторинг		-	-	+	-
Режим работы	Мониторинг		+	+	+	+
	Симуляция		+	-	-	+
	Генерация нагрузки		+	-	-	-
Тип, количество физических интерфейсов/ звеньев данных	E1: ОКС-7, ISDN PRI, V5	Мониторинг	8/16	1/1	16/32 x N	1
		Симуляция/генерация	16/1	-	-	1
	ISDN BRI	Мониторинг	1/1	-	-	-
		Симуляция	2/2	-	-	-
	Ethernet	Мониторинг	2	-	-	-
Сети/ протоколы	ОКС-7	MTP2, MTP3, ISUP	+	+	+	-
		SCCP, TCAP	+	-	+	-
	ISDN	LAPD, DSS1 L3	+	+	+	-
	IN	INAP, CAMEL	+	-	+	-
	V5.x	LAPV5, PSTN, CC, BCC, LC, PROTECTION	+	+	+	-
	GSM	MAP, A-bis RSL, BSSMAP, DTAP	+	-	+	-
	GPRS	NS/FR, LLC, SNDCP, BSSGP, IP, TCP, UDP, GTP	+	-	-	-
	ТФОП	2ВСК-R1.5,АОН,челнок,R2	+	+	-	+
		1ВСК,«норка»,индукт.код, одночаст.2600Гц, 3-пров.	-	-	-	+
	WAN	LAPB, LAPD, Q.922, FRF1.1, X.25, Q.931, Q.933	+	-	-	-
	LAN	Ethernet 10 Base-T, TCP, IP, UDP, IPv6	+	-	-	-
	VoIP	H.323v2 (H.225.0, H.245)	+	-	-	-

Вместо заключения

Из вышеизложенного видно, что сегодня при переходе к NGN для тестирования протоколов просто обязательно следовать девизу: *трудные задачи выполняем немедленно, невозможные -- чуть погодя*. Более того, новые опции в тестерах должны появляться (и появляются!) еще до окончательного утверждения соответствующих спецификаций новых протоколов. Так, в частности, было с российской версией ISUP, называемой иногда ISUP-R, с протоколами интерфейса V5 и другими опциями приведенных в таблице тестеров, а также не попавших туда предыдущих модификаций: STA-7, ANT-5, MAS-8. Такое же происходит сегодня с заложенными в SNT-7531 спецификациями протоколов IP-телефонии H.323, SIP и MGCP, интеллектуальной сети INAP-R CS-2 и CAMEL.