АНАЛИЗАТОРЫ ПРОТОКОЛОВ – ДЕТЕКТИВЫ СЕТЕЙ

Э.Рувинова

Сегодня при поддержании сети общего пользования без эффективных средств анализа и имитации сетевого трафика, каковыми являются анализаторы протоколов, просто не обойтись. Анализаторы протоколов широко применяются администраторами сетей для контроля за работой этих сетей и определения их перегруженных участков, отрицательно влияющих на скорость передачи данных. На российском рынке телекоммуникаций представлен ряд анализаторов протоколов зарубежных фирм.

Современные анализаторы протоколов осуществляют захват и анализ пакетов с возможностью фильтрации, анализ распределения потоков данных по заданным оператором критериям, декодирование пакетов для протоколов различных уровней, мониторинг сетевых соединений (ЛВС, WAN, телефония), тестирование сетевых приложений, поиск проблемных мест в сети, обнаружение ошибок в каналах передачи, генерацию потоков с заданными параметрами, тестирование соединений на частоту ошибок по битам (BER). К сожалению, анализаторы используются и злоумышленниками, которые с их помощью способны наладить перехват чужих паролей и другой конфиденциальной информации.

Последнее поколение анализаторов протоколов предоставляет возможность всестороннего слежения как за производительностью и загруженностью всей сети, так и за функционированием отдельного приложения индивидуального пользователя. Анализаторы имеют определенные преимущества перед системами удаленного контроля и управления сетью: анализ и нахождение неисправностей по ходу работы, оценка производительности при планировании сети и решение проблем функционирования сетевых приложений. С помощью анализаторов можно выявлять и устранять проблемы существующей сети, а также упрощать процесс перехода к новой технологии. Эти устройства обеспечивают возможность не только оперативно устранять проблемы по мере их возникновения, но и предупреждать их появление.

Стоимость анализаторов протоколов колеблется от нескольких сотен до десятков тысяч долларов, и для оптимального выбора прибора необходим системный подход. Можно выделить ряд критериев для оценки анализатора протоколов:

- возможность декодирования сетевых протоколов и поддержки сменных интерфейсов;
- качество интерфейса ПО;
- наличие многоканальности;
- возможность интеграции с ПК;
- габариты и масса;
- соотношение цены и предоставляемых услуг.

Поддерживаемые протоколы и возможность подсоединения к различным физическим интерфейсам определяют сферу и широту применения анализаторов. В число традиционно поддерживаемых физических интерфейсов входят V.35, RS-232/V.24, RS-449, RS-530, X.21/V.11, которые обычно включаются в базовый комплект поставки анализатора. Интерфейсы E1, T1, Ethernet, Token Ring – дополнительные и обычно не входят в базовый комплект. Однако благодаря модульной конструкции анализатора его всегда можно оснастить требуемыми физическими интерфейсами. Анализ сетевых протоколов – центральная задача анализаторов, поэтому естественным требованием к ним является поддержка максимального числа протоколов.

Интерфейс программного обеспечения – весьма важный фактор, поскольку чем "дружественнее" оболочка ПО, тем эффективнее работа администратора. Кроме того, графический оконный интерфейс способствует быстрому освоению ПО и позволяет адекватно воспринимать выдаваемую анализатором информацию.

В моделях анализаторов повышенного качества поддержка работы с несколькими каналами обычно подразумевает наличие дополнительной функции имитации. Эта функция в совокупности с многоканальностью позволяет использовать прибор одновременно в качестве генератора тестовых последовательностей и тестирующего оборудования.

Составная часть любого анализатора протоколов – ПК. Существует два принципа взаимодействия анализатора с ПК. Первый состоит в их интеграции на базе единого устройства, второй – в их совместном использовании со строгим разделением функций, выполняемых каждым прибором. Второй подход позволяет проводить независимую модернизацию составных устройств и особенно актуален при существующем развитии компьютерных технологий.

Габариты и масса – важные для анализатора параметры, поскольку проблемы могут возникнуть в любом сегменте сети, и чем компактнее и легче прибор, тем удобнее он будет в эксплуатации.

Анализаторы протоколов могут поставляться в виде ПО или комбинации программных и аппаратных средств. Аппаратный анализатор протокола – это автономный модуль. Анализаторы протоколов используются на рабочей станции сети и выполняют обычно следующие задачи:

- выводят на экран информацию о типах пакетов, передаваемых по сети, благодаря чему можно определить точность передачи;
- опрашивают все узлы и выполняют тестирование передачи данных от точки к точке между любыми узлами;
- определяют конфигурацию всей сети;
- анализируют критические данные от одного или всех узлов и на основе заданных пользователем пороговых значений сообщают только о необычной активности;
- выводят данные о производительности, такие как объем трафика и обслуживание пакетов;

- обеспечивают дополнительную информацию об эффективности сети, ее производительности, возможных аппаратных ошибках, проблемах, связанных с шумами, и проблемах в прикладном ПО.

КОМПАНИЯ RADCOM

Для организации и поддержки современных скоростных сетей с передачей голоса и данных требуются высокоскоростные и мощные средства тестирования. К таким средствам относятся анализаторы протоколов для сетей WAN/Fast LAN/Telecom **серии RC** компании RADCOM. Это портативные и легкие приборы, позволяющие тестировать сети в процессе их использования. Они обеспечивают одновременно двухканальный мониторинг и моделирование WAN, LAN и fast LAN и поддерживают свыше 300 протоколов этих сетей.

Конструктивно каждый анализатор выполнен в одном блоке (рис.1), портативном и легком (менее 2 кг). Имеет RISC-процессор (i960), ОЗУ (8 Мбайт). Может соединяться с любым ПК, в том числе ноутбуком. Два независимых WAN-порта, каждый из которых дает возможность проводить двухканальный мониторинг и моделирование. Два RJ-45 fast LAN-порта с возможностью дуплексного режима при скорости 10 и 100 Мбит/с. Графический интерфейс на базе MS-Windows.

Рис.1. Анализатор RC-100WL

Анализаторы серии RC осуществляют процессы: захват, определение статистических данных, фоновую запись, анализ, моделирование кадров, моделирование пакетов, моделирование протоколов, определение статуса линии, BER-тестирование.

Поддерживаемые протоколы в сетях:

WAN – HDLC, SDLC, LAPB, LAPD, Frame Relay, X.25, SNA, ISDN, Cisco routers, RND routers, PPP suite, Wellfleet routers, Async, Timeplex, SMDS/DXI, MLPPP, FUNI, ATM/DXI;

ЛВС – LAN/Encapsulated – Ethernet 10/100/1000, Token Ring, IGRP, EIGRP, TCP/IP suite, FDDI, ISO/OSI, DecNet, XNS, Novell/IPX, Banyan Vines, 3Com, AppleTalk, Sun, LanManager, DLSw, NetBios, IPv6, NHRP, DSVPV, Jacobson;

VoIP (голосовая связь по сетям передачи данных) – H.323 suite, MGLP, SGLP, SIP, SAP, T.38;

Cellular (сотовая сеть) – GSM suite, CDMA suite, GPRS suite, CDPD;

SS7 – MTP2, MTP3, ISUP, SCCP, TCAP, MAP.

Возможности тестирования и рабочие характеристики моделей серии RC следующие. **RC-88W** – WAN/Telecom анализатор, работающий вплоть до 256 Кбит/с; **RC-88WL** – WAN/LAN/Telecom анализатор, работающий вплоть до 256 Кбит/с в глобальных сетях и при 10 или 4/10 Мбит/с в ЛВС. **RC-88WFL** – WAN/Fast LAN/Telecom анализатор, работающий вплоть до 256 Кбит/с в глобальных сетях и при 10/100 Мбит/с в скоростных ЛВС. **RC-100W** – высококачественный WAN/Telecom анализатор, работающий вплоть до 2 Мбит/с. **RC-100WL** – высококачественный WAN/LAN/Telecom анализатор, работающий вплоть до 2 Мбит/с в глобальных сетях и при 10 или 4/16 Мбит/с в ЛВС. **RC-100WFL** – высококачественный WAN/Fast LAN/Telecom анализатор, работающий вплоть до 2 Мбит/с в глобальных сетях и при 10/100 Мбит/с в скоростных ЛВС.

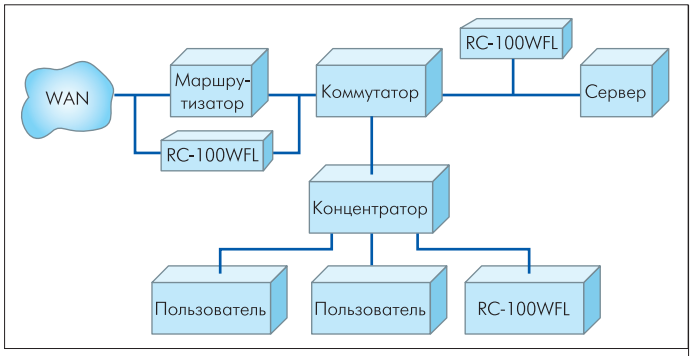

Рис.2. Схема применения анализатора протоколов RC-100WFL

Применение анализаторов протоколов серии RC (рис.2) охватывает контроль за работой сети с анализом трафика на важных, полнодуплексных соединениях со скоростью 100 Мбит/с; настройку или модернизацию сетей с высокопроизводительными коммутаторами и маршрутизаторами, при этом анализатор позволяет также обнаруживать ошибки конфигурации до того, как они начнут оказывать вредное влияние на работу сети. Анализатор можно использовать для разработки сетевых приложений нового поколения, обеспечивающих интеграцию голоса и данных, поддержку многопротокольных маршрутизаторов и шлюзов, возможность соединения компьютерных и традиционных телефонных сетей, реализацию IP-телефонии и т.п.

Для быстрого и эффективного решения проблем на стыках сетевых технологий необходимы инструменты для одновременного тестирования нескольких технологий, и компания RADCOM выпускает два варианта интегрированных анализаторов WAN, ЛВС и АТМ:

Prism200 – настольный анализатор, обеспечивающий идеальное решение для разработчиков и сетевых администраторов;

PrismLite – универсальный переносной анализатор с поддержкой нескольких сетевых технологий в компактном автономном исполнении.

Рис.3. Анализатор PrismLite

Эти приборы поддерживают все приложения, интерфейсные модули и протоколы, которые могут потребоваться для решения проблем, связанных с межсетевым взаимодействием. Они выпускаются с 18 различными типами линейных интерфейсов, что обеспечивает их подключение практически ко всем типам линий. Набор дополнительных программ позволяет настраивать и оптимизировать работу самых сложных сетей.

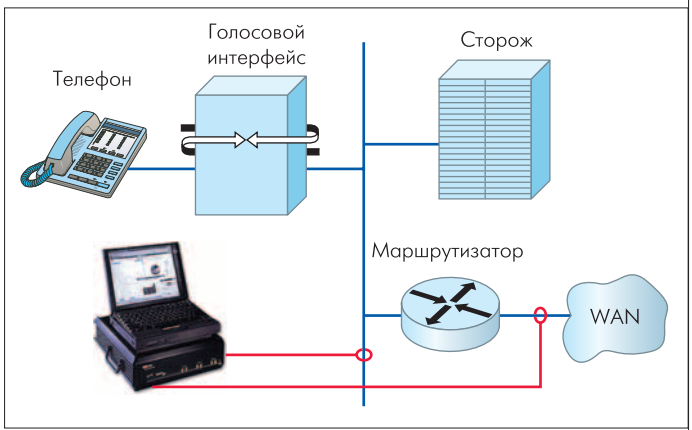

Рис.4. Анализатор PrismLite в сети VoIP

Анализатор PrismLite (рис.3) декодирует свыше 450 протоколов. Осуществляет тестирование и настройку ATM-сетей: имитация сигнальной информации, генерация нагрузки (трафика), BER-тестирование, вставка ошибок, проверка состояния физических линий. Его применение в ЛВС с 10/100 Мбит/с – это имитация Ethernet, проверка состояния физических линий, анализ наиболее "разговорчивых узлов", распределение протоколов, вставка ошибок. В глобальных сетях: имитация Frame Relay, ISDN, X.25, автоматическое распознавание ошибок Frame Relay, BER-тестирование.

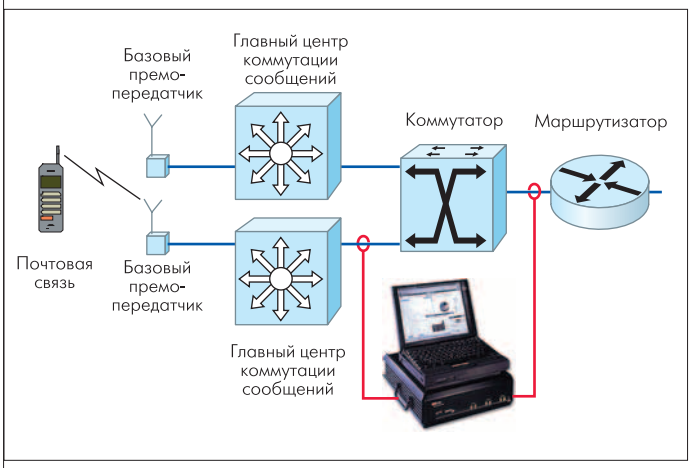

Рис.5. Анализатор PrismLite в сотовой сети

Кроме того, анализатор PrismLite обеспечивает поиск неисправностей в системах голосовой связи по сетям передачи (рис.4), а также всестороннюю поддержку протоколов 2/2.5/3G (GPRRSSS/UUMTS/CDMA2000) и непрерывное обновление поддержки для новых сотовых протоколов (рис.5).

Рис.6. Анализатор Prism UltraLite

Компания выпускает также легкий и портативный анализатор **Prism UltraLite** (рис.6), который тестирует VoIP, сотовые и традиционные сети. Прибор анализирует и имитирует поведение сети и поддерживает широкий диапазон коммуникационных протоколов. Идеальное устройство в условиях эксплуатации сетей.

Последний анализатор протоколов, выпущенный компанией RADCOM, – анализатор с высокими параметрами марки Performer. Это универсальный прибор для НИОКР, лабораторных исследований и при эксплуатации сети. Обеспечивает мониторинг и поиск неисправностей WAN/LAN/ATM/PoS/Metro-сетей на всех семи слоях.

ФИРМА AGILENT TECHNOLOGIES

На мировом рынке самым мощным считается анализатор **J2300E** фирмы Agilent Technologies (рис.7). Это универсальный анализатор протоколов локальных и глобальных сетей, универсальное решение для анализа WAN, ЛВС, АТМ. Позволяет осуществлять мониторинг всех основных коммуникационных протоколов WAN от 50 бит/с до

Рис.7. Анализатор J2300E

622 Мбит/с: SONET/SDH, Frame Relay, ISDN, X.25, HDLC, SDLC, SNA, синхронных/асинхронных двухточечных линий, ATM-DXI и инкапсулированных ЛВС-протоколов. Возможна эмуляция протоколов X. 25, Frame Relay и ISDN до 2,048 Мбит/с, BER-тестирование. Встроенная экспертная система позволяет провести сканирование сети на наличие в ней неисправностей и анализ причин их возникновения.

Интерфейсы V-серии, такие как RS232C/V.24, RS-449/422/423, V.10/V.11 и V.35, уже встроены в платформу. Для высокоскоростных V-интерфейсов (до 8,192 Мбит/с) предусмотрены вставляемые модули, которые добавляют тестовую способность для сетей ISDN BRI и PRI, T1, J2, E1, E3, T3, STM-1e, ATM25 и UTP155. Дополнительные, подстыковываемые снизу модули также добавляют тестовые возможности для ATM, Ethernet, коммутируемой Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI и STM-4 (622 Мбит/с ATM), ЛВС на основе Token Voice Quality по аналоговым интерфейсам FXO и E&M.

Анализатор J2300E быстро изолирует и идентифицирует сетевые проблемы по нажатию лишь одной клавиши.

Характеристики анализатора:

- ОП – Windows 98;
- предварительно написанные тесты для основных протоколов;
- позволяет отвечать на сообщения, создавать отчеты, документировать результаты испытаний или выполнять любое стандартное приложение DOS или MS WINDOWS;
- процессор Pentium, 400 МГц, память 256 Мбайт;
- жесткий диск 6 Гбайт.

Анализаторы J2300E поставляются с полным ПО, куда включены тестовые сценарии.

ФИРМА TEKTRONIX

Это крупный поставщик решений в области тестирования, измерений и мониторинга для производителей оборудования и операторов сотовой связи. Анализатор протоколов **Tektronix K1297-G20** версии 2.60 (V2.60) позволяет осуществлять тестирование оборудования на соответствие универсальной мобильной телекоммуникационной системы 5-го выпуска (UMTS R5) с помощью платформы, которая может обслуживать более тысячи протоколов.

Система UMTS R5 представляет собой завершающий шаг в процессе перехода к полному внедрению сетей UMTS третьего поколения. Эти сети функционируют во многих частях света, и производители сотового оборудования, чтобы удовлетворить спрос, испытывают особую потребность в тестировании своих продуктов на соответствие последним стандартам. Tektronix K1297-G20 (рис.8) поддерживает многоканальный и мультипортовый анализ протоколов и содержит широкий набор тестов. Устройство способно одновременно производить мониторинг и обеспечивать совместимость элементов сетей GSM, GPRS и UMTS. Прибор V2.60 кодирует содержание сообщения перед его отправкой в сеть. Это позволяет создавать специальные тестовые сообщения и последовательности сообщений, обеспечивая имитацию специфических нормальных и аномальных состояний сети. В результате пользователь может убедиться в том, что реализация протокола соответствует стандарту.

Рис.8. Анализатор K1297-G20

V2.60 декодирует информацию, полученную от сети, и обеспечивает доступ к содержанию всех сообщений, которыми обменивались элементы сети. Таким образом, пользователь имеет возможность контролировать поведение тестируемой сети, точно определяя местонахождение источника потенциальных проблем и основную причину отказа.

ФИРМА YOKOGAWA ELECTRIC

Эта фирма еще на выставке WPC EXPO 2002 продемонстрировала анализатор протокола IEEE 1394b – IP1200. Спецификация нового стандарта IEEE 1394b предусматривает передачу данных с быстродействием до 1 Гбит/с. Анализатор подключается к локальной сети и выступает в качестве сетевого сервера, управляемого при помощи специального ПО, поставляемого фирмой Yokogawa. Устройство позволяет проводить анализ протокола IEEE 1394b через браузер на любом ПК, подключенном к локальной сети. Сам анализатор изготовлен на основе PC/AT-совместимого компьютера и не имеет монитора. К прибору можно подключить клавиатуру, и он будет работать как автономное устройство.

Наибольшей функциональной полнотой в работе с сетевыми протоколами отличаются модели фирм Agilent и RADCOM.

АНАЛИЗАТОРЫ ПРОТОКОЛОВ ДЛЯ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

При эксплуатации беспроводных локальных сетей совершенно необходимо применять специальные средства мониторинга и анализа их работы. Анализаторы протоколов беспроводных сетей, как правило, состоят из тех же компонентов, что входят в само беспроводное оборудование. Для беспроводных сетей стандарта IEEE 802.11b это широко распространенные сетевые радиокарты 802.11, устанавливаемые в ноутбуки, карманные ПК или патентованные устройства нестандартных размеров. Явно сфокусированы

Рис.9. Карманный анализатор фирмы AirMagnet

на специфике беспроводных сетей анализаторы протоколов фирм AirMagnet и Sniffer.

В первую очередь следует отметить карманный анализатор фирмы **AirMagnet** (рис.9), созданный на базе ПК iPAQ компании Hewlett-Packard. Благодаря пиктограммам, обеспечивающим быструю смену контекста и наборов доступных функций, он позволяет оперативно обнаруживать проблемы в тестовой среде и просматривать результаты мониторинга сети. ПО анализатора поддерживает два режима – экспертный и обзорный. Последний позволяет выяснить, какие устройства работают в эфире, а экспертный – провести специальный анализ их функционирования.

Как известно, стандарт 802.11b предусматривает организацию до 14 радиоканалов, и анализатор должен уметь сканировать все 14 каналов. Портативный прибор фирмы AirMagnet, в котором реализована функция сканирования всего рабочего спектра, выдает точные значения интенсивностей сигнала и шума для устройств, установленных в сети 802.11b. Он позволяет анализировать потенциально опасные ситуации, например передачу точкой доступа в эфир идентификатора SSID или отключение поддержки протокола WEP. Анализатор выдает и сведения, связанные с производительностью сети, скажем, сигнализирует о передаче клиентским устройством необычно большого числа низкоскоростных пакетов или о появлении чрезмерного количества опознавательных сигналов, которые указывают на возможные проблемы в радиоэфире. Наконец, анализатор имеет легко вызываемые функции управления командами ping, обнаружения устройств и присвоения адресов по механизму DHCP.

Sniffer Wireless – "беспроводная" версия анализатора фирмы Sniffer. Созданное на базе все того же iPAQ, устройство в первую очередь предназначено для выявления проблем функционирования сети. Главное достоинство данной модели – функции декодирования пакетов и экспертного анализа, оперативно обеспечивающие представление о происходящем в сети. Устройство поддерживает сканирование всех 14 каналов сети 802.11b и, подобно изделию AirMagnet, имеет высокую радиочувствительность.

С помощью этого анализатора администратор сети может следить за тем, кто входит в сеть, контролировать уровень радиосигнала во всех точках доступа беспроводной сети, наблюдать за изменением рабочих характеристик сети по мере нарастания трафика и проверять, как взаимодействуют между собой различные продукты и приложения беспроводной сети. В состав анализатора входит приложение, которое регистрирует предупреждающие сигналы и выдвигает возможные причины неполадок. Это же приложение умеет автоматически идентифицировать различные проблемы, например некорректно сконфигурированные маршрутизаторы, повторяющиеся сетевые адреса и узкие места сетевой инфраструктуры, влияющие на производительность.

Беспроводная версия **OptiView компании Fluke** (рис.10) представляет собой портативный ПК с сенсорным экраном и интегрированными адаптерами – от двухскоростного 10/100-мегабитного до гигабитного Ethernet. Сенсорный экран очень удобен в работе, а в качестве электронного пера можно воспользоваться собственным ногтем. В беспроводную версию входит ПО Fluke Wireless Analyzer и сетевой адаптер фирмы Fluke для сетей 802.11b.

Рис.10. Беспроводная версия анализатора OptiView

Функциональность ПО сконцентрирована на характеристиках точек доступа и связанных с ними клиентских устройств. В отличие от приложения OptiView для проводных сетей, здесь нет встроенной экспертной системы или функции анализа проблем в беспроводных локальных сетях. Версии ПО для беспроводных и проводных сетей могут работать одновременно, но при высоких нагрузках в той или иной среде производительность одной из них заметно падает. Беспроводной анализатор Fluke способен захватывать и декодировать пакеты в формате фирмы Sniffer.

Функция локализации обеспечивает выдачу звукового сигнала при приближении к желаемому устройству, причем даже в том случае, когда две близко расположенные точки доступа используют один и тот же радиоканал. Поворачивая анализатор вокруг оси на 360°, можно определить направленность излучения. Масса прибора – 2 кг, габариты – 26x23x6 см.

Анализатор **Surveyor Wireless V1.10.95 фирмы Finisar** предназначен для работы только в сетях стандарта 802.11b. Мониторинг каналов проводится последовательно; переход с одного на другой выполняется через задаваемый пользователем временной интервал. Статистические данные, накопленные за время сканирования канала, выводятся на экран в виде гистограммы, а степень использования полосы пропускания канала, уровень сигнала и количество ошибок в секунду кодируются цветом. Предусмотрены два режима (мониторинг и захват пакетов), которые могут быть активированы по очереди или одновременно, однако ни в одном из них не доступны статистические данные, накопленные для отдельных каналов.

Предусмотренный разработчиками экранный интерфейс Detailed View позволяет отображать в отдельных окнах различные взаимосвязи между ресурсами. Кроме того, в них выводятся гистограммы и таблицы накопленных данных для характеристик, являющихся специфическими для сетей 802.11b и проводных сетей. Экспертная система в продукте не предусмотрена, но возможна установка триггеров и порогов для выдачи предупреждающих сообщений при возникновении тех или иных условий (избыточное число низкоскоростных пакетов, высокий уровень ошибок или управляющих фреймов и др.).

Сильная сторона анализатора Surveyor Wireless – многообразие удобных средств визуализации данных. А его основной недостаток – отсутствие инструментария для поддержания инфраструктуры беспроводной сети в надлежащем состоянии, такого как функции оперативного выявления связей между клиентами и точками доступа в сети 802.11, защиты данных в соответствии со стандартом 802.1x или настройки/тестирования соединений между точками доступа.

www.bnti.ru/
www.ksaa.edu.ru:
www.bilim.com/koi8/radcom/
www.radcom.com/
www.agilent.com/
www.miks.ru/
www.tek.com/
www.tlsgroup.ru/
arcw.comptek.ru/
www.compulenta.ru/