АНАЛИЗАТОРЫ ПРОТОКОЛОВ

АНАЛИЗАТОР ПРОТОКОЛОВ

Анализатор протоколов представляет собой либо специализированное устройство, либо персональный компьютер, обычно переносной, класса Notebook, оснащенный специальной сетевой картой и соответствующим программным обеспечением.

Применяемые сетевая карта и программное обеспечение должны соответствовать технологии сети (Ethernet, Token Ring, FDDI, Fast Ethernet). Анализатор подключается к сети точно так же, как и обычный узел. Отличие состоит в том, что анализатор может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция - только адресованные ей.

Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и программного обеспечения, декодирующего протокол канального уровня, с которым работает сетевой адаптер, а также наиболее распространенные протоколы верхних уровней, например IP, TCP, ftp, telnet, HTTP, IPX, NCP, NetBEUI, DECnet и т.п.

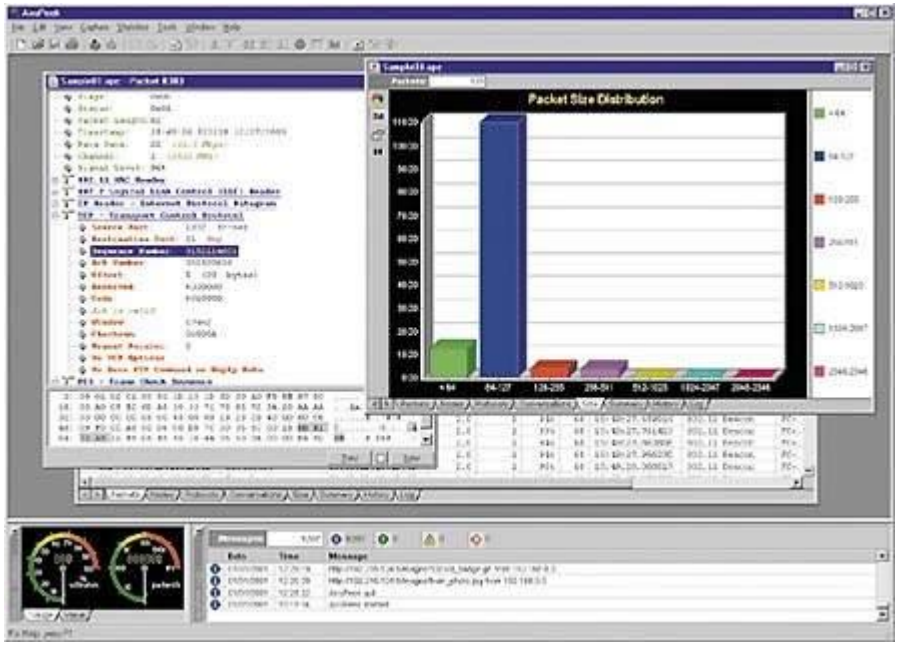
Анализатор сетевых протоколов может использоваться для:

- локализации трудноразрешимых проблем;
- обнаружения и идентификации несанкционированного программного обеспечения;
- получения такой информации, как базовые модели трафика (baseline traffic patterns) и метрики утилизации сети;
- идентификации неиспользуемых протоколов для удаления их из сети;
- генерации трафика для испытания на вторжение (penetration test) с целью проверки системы защиты;
- работы с системами обнаружения вторжений Intrusion Detection System (IDS);
- прослушивания трафика, т. е. локализации несанкционированного трафика с использованием Instant Messaging (IM) или беспроводных точек доступа Access Points — (AP);
- изучения работы сети.

Анализаторы протоколов имеют некоторые общие свойства:

- Возможность (кроме захвата пакетов) измерения среднестатистических показателей трафика в сегменте локальной сети, в котором установлен сетевой адаптер анализатора. Обычно измеряется коэффициент использования сегмента, матрицы перекрестного трафика узлов, количество хороших и плохих кадров, прошедших через сегмент.
- Возможность работы с несколькими агентами, поставляющими захваченные пакеты из разных сегментов локальной сети. Эти агенты чаще всего взаимодействуют с анализатором протоколов по собственному протоколу прикладного уровня, отличному от SNMP или CMIP.
- Наличие развитого графического интерфейса, позволяющего представить результаты декодирования пакетов с разной степенью детализации.
- Фильтрация захватываемых и отображаемых пакетов. Условия фильтрации задаются в зависимости от значения адресов назначения и источника, типа протокола или значения определенных полей пакета. Пакет либо игнорируется, либо записывается в буфер захвата. Использование фильтров значительно ускоряет и упрощает анализ, т.к. исключает захват или просмотр ненужных в данный момент пакетов
- Использование триггеров. Триггеры в данном случае - это задаваемые администратором некоторые условия начала и прекращения процесса захвата данных из сети. Такими условиями могут быть: время суток, продолжительность процесса захвата, появление определенных значений в кадрах данных. Триггеры могут использоваться совместно с фильтрами, позволяя более детально и тонко проводить анализ, а также продуктивнее расходовать ограниченный объем буфера захвата.
- Многоканальность. Некоторые анализаторы протоколов позволяют проводить одновременную запись пакетов от нескольких сетевых адаптеров, что удобно для сопоставления процессов, происходящих в разных сегментах сети.

SNIFFER WIRELESS



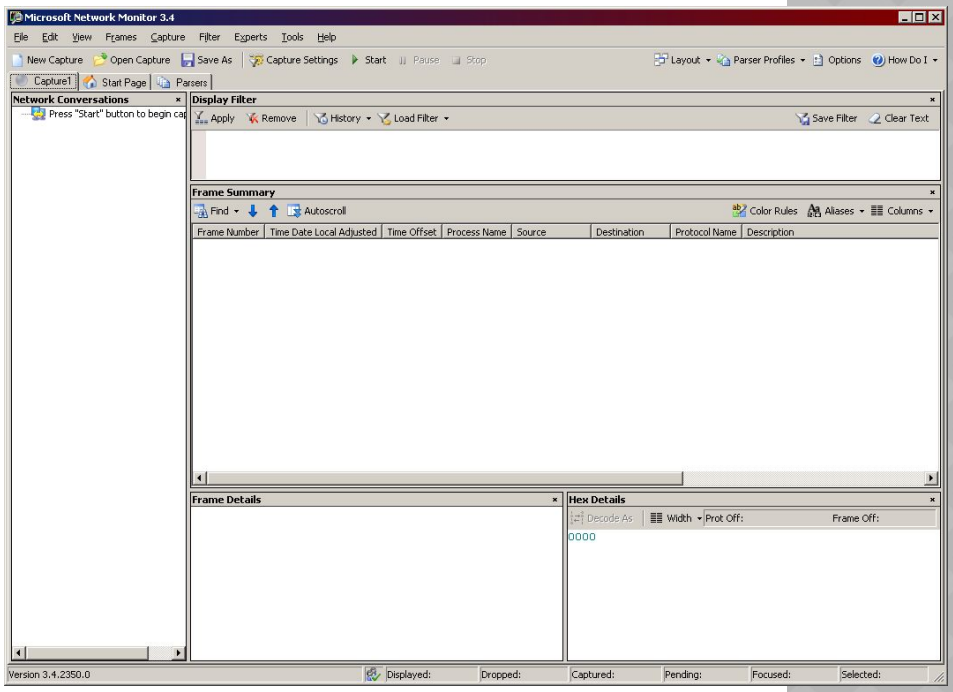
Версия известного анализатора кабельных локальных сетей, устанавливается на компьютер под управлением ОС Windows, оборудованный адаптером беспроводной сети производства Agere Systems, Cisco Systems или Symbol Technologies.

С помощью этого анализатора администратор сети может следить за тем, кто входит в сеть, контролировать уровень радиосигнала во всех точках доступа (также называемых базовыми станциями) локальной сети, наблюдать за изменением рабочих характеристик сети по мере нарастания трафика и проверять, как взаимодействуют между собой различные продукты и приложения беспроводной среды

NETWORK MONITOR

С распространением серверов Windows NT все более популярным становится анализатор Network Monitor фирмы Microsoft. Он является частью сервера управления системой SMS, а также входит в стандартную поставку Windows NT Server, начиная с вервии 4.0. Network Monitor в версии SMS является многоканальным анализатором протоколов, поскольку может получать данные от нескольких агентов Network Monitor Agent, работающих в среде Windows NT Server, однако в каждый момент времени анализатор может работать только с одним агентом, так что сопоставить данные разных каналов с его помощью не удастся.

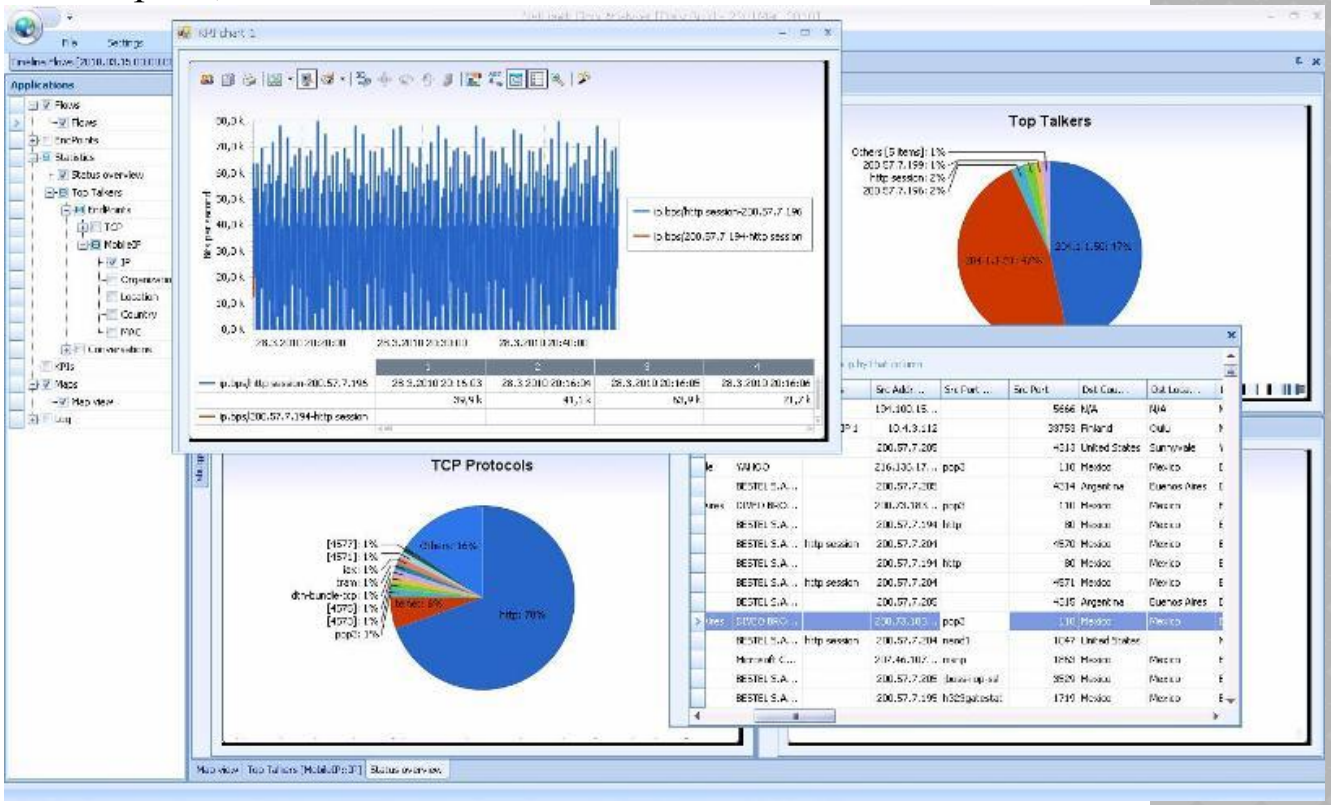
Network Monitor поддерживает фильтры захвата (достаточно простые) и дисплейные фильтры, отображающие нужные кадры после захвата (более сложные). Экспертной системой Network Monitor не располагает.



АНАЛИЗАТОР ПРОТОКОЛОВ NETHAWK M5

NetHawk M5 позволяет в реальном времени производить трассировку звонков, осуществлять сквозную корреляцию сессий для звонков осуществляемых с применением различных технологий (GSM, UTRAN, LTE, IMS, CS Core, PS Core, SS7), формировать более 100 различных KPI, измерять QoS и MOS. Для передачи данных в IP сетях NetHawk M5 позволяет выделять отдельные сессии на основании IP и MAC адресов, номеров протоколов и портов, меткам VLAN и MPLS.

Для каждой сессии определяются пропускная способность и объем переданных данных. Все полученные результаты могут быть сохранены в базе данных для проведения дальнейшего статистического анализа. Для детализированного анализа протоколов M5 использует подключаемые декодирующие модули.



R&S CRTU ПЛАТФОРМА ТЕСТИРОВАНИЯ ПРОТОКОЛОВ

- Анализатор протоколов и платформа системного моделирования для протоколов (E)GPRS, GSM, HSDPA, HSUPA, WCDMA FDD, GAN, Application Testing и других
- Утвержденная GCF / PTCRB тестовая платформа для проведения сертификационных испытаний и испытаний на соответствие стандартам и техническим условиям
- Создание тестовых сценариев для НИОКР с помощью простых и мощных в использовании интерфейсов (API и технология "перетаскивания" drag-and-drop)
- Испытание модулей реализации приложений Application Enabler (MMS, PoC, видеотелефония, просмотр информации в сети)
- Автоматизация последовательностей испытаний для экономически эффективного автоматического тестирования

СЕТЕВОЙ АНАЛИЗАТОР LANEXPERT

- диагностика сетей Ethernet (10/100/1000Мбит/с)
- получение подробной информации о сети и сетевом устройстве: конфигурация, адресация, статус
- измерение производительности сети по методике RFC2544
- захват трафика (до 10,000 пакетов) для дальнейшего анализа
- поддержка таких технологий, как VLAN, IPv6 и PoE (Power over Ethernet)
- мониторинг состояния сети - отображение количества переданных кадров, загрузки сети, уровень трафика, ошибок, коллизий и т.д.
- система регистрации ошибок в сети, таких как: дублирующиеся IP-адреса, оставшиеся без ответа DNS-запросы, нежелательные протоколы и ошибки при передачи данных
- идентификация соединения: определение возможной и текущей скорости соединения (10/100/1000 Мбит/с) и настроек дуплекса (full/half)
- тестирование VoIP - мониторинг работы IP-телефонии и обмена данными VoIP, измерение ключевых параметров QoS
- возможность подключения к ВОЛС (SM/MM) с помощью оптических SFP модулей (для LE85M/S)
- **базовое тестирование кабеля (только LE80):** измерение длины кабеля и расстояния до повреждения; идентификация коротких замыканий, обрывов, выявление ошибок разводки