СДЕЛАЕМ ВАШУ СЕТЬ ЛУЧШЕ! Группа компаний ProLAN Inc.

Observer 8.0

Анализатор сетевых протоколов

Средство мониторинга и диагностики локальных и глобальных сетей

OBSERVER®

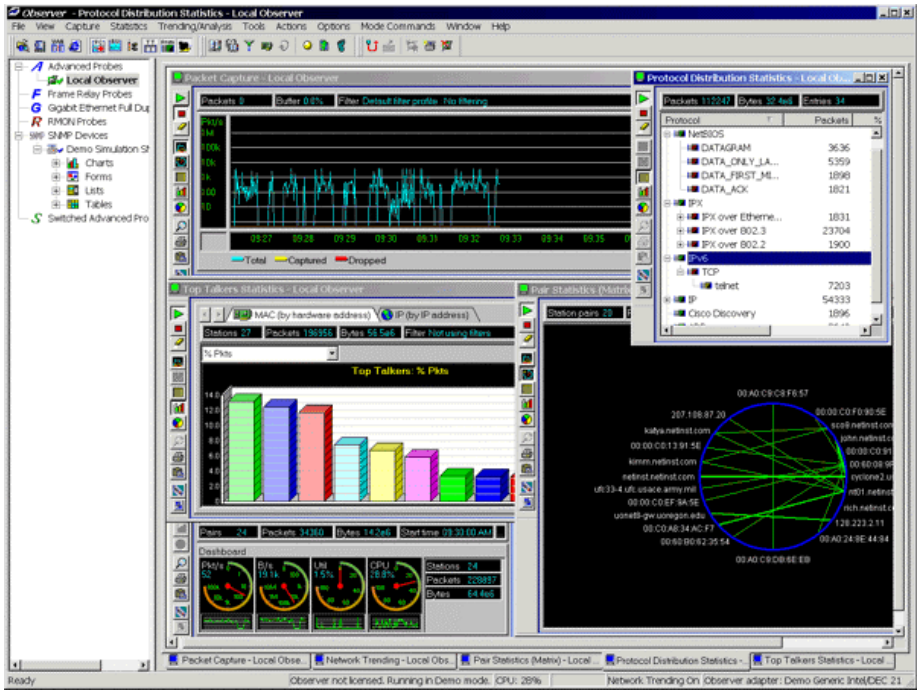
NETWORK INSTRUMENTS®

Содержание

Знакомьтесь - Observer 8.x

Observer 8.x - Анализатор сетевых протоколов и мощное средство для диагностики и мониторинга LAN, WAN, в том числе и коммутируемых сетей

Узнайте о своей сети ...Всё! *Установите пакет* ***Observer 8*** *и Вам станет ясно: исправна ли сеть, почему программы работают медленно, кто и как загружает сеть, где источник ошибок, почему происходят сбои, и многое другое. При этом не важно, какая сетевая ОС:* ***Microsoft, Novell, UNIX, Apple, DEC, IBM*** *используется в вашей сети.*



Observer 8 позволяет в реальном масштабе времени наблюдать за всеми процессами, происходящими в сетях **Ethernet (shared & switched), Fast Ethernet, GigaBIT Ethernet, FDDI, Token Ring**, и на основании полученных данных делать достоверные выводы, как о качестве работы сети, так и о причинах наблюдаемых сбоев.

Отличительной особенностью пакета **Observer 8** является его многофункциональность. С одной стороны - это монитор сети и анализатор сетевых протоколов, с другой стороны - это мощное диагностическое средство, позволяющее быстро выявлять дефекты сети.

Начиная с версии **7.0**, в пакете **Observer** реализована специальная технология (так называемый "**looping**") для диагностики коммутируемых локальный сетей. В настоящее время эта технология является уникальной в мире анализаторов сетевых протоколов. Она позволяет видеть и анализировать трафик одновременно по всем портам коммутатора.

Observer 8 является незаменимым средством для профессионального администрирования и диагностики сетей. Предоставляемая пакетом информация позволяет делать однозначные и достоверные выводы о причинах сбоев в работе сети.

- *Вы сможете измерить текущую и долговременную загрузку (утилизацию) сети. Выявить тенденцию роста загрузки сети в течение рабочего дня, месяца, квартала или даже года. Сравнить загрузку сети за различные промежутки времени.*
- *Специальные встроенные тесты позволяют измерить, как общее число ошибок и коллизий в сети, так и распределение ошибок по рабочим станциям сети; возможность генерации тестового трафика поможет выявить "скрытые" дефекты канального уровня сети.*
- *Функции захвата и декодирования пакетов практически всех известных сетевых протоколов помогут выявить дефекты "верхних" уровней сети. Вы сможете легко определить, почему конкретная станция "не видит" сервера, почему не печатает сетевой принтер, перегружен ли сервер и многое другое.*
- *Вы получите полную информацию об активности рабочих станций сети (кто и как использует сеть), получите распределение трафика по протоколам и субпротоколам, узнаете, какие станции сети взаимодействуют друг с другом и каково при этом время реакции каждой станции (или сервера), получите распределение кадров по длинам кадров и т.п.*
- *Входные фильтры и "триггеры" избавят Вас от необходимости сидеть за экраном монитора для выявления дефектов сети, которые проявляются в непредсказуемые моменты времени. Пакет сам информирует вас, когда в сети произойдет определенное событие (например, сбой). Если вы на своём рабочем месте, то вы будете сразу информированы о наступившем событии. Если вас нет на месте, сообщение может прийти к вам по пейджеру или электронной почте.*
- *Специальные функции наблюдения за WEB-сервером позволят вам определить его загруженность, кто и как часто с ним работает, какова интенсивность этой работы.*
- *Специальные функции наблюдения за маршрутизатором позволят вам, в частности, определить, какова загрузка (утилизация) внешнего канала связи.*

Состав и Комплект поставки Observer 8

Пакет **Observer** является чисто программным средством и представляет собой набор 32-битных приложений и сервисов для **Microsoft Windows (95/98/NT4/2000/XP)**.

Пакет **Observer** поставляется в виде базовой программы и набора расширений (extensions). **Расширения** - это дополнительные программные модули, которые расширяют функциональные возможности базовой программы.

Программа **Observer** устанавливается на обычный компьютер, который подключен к диагностируемому сегменту сети или выделенному порту коммутатора. Принцип работы программы основан на том, что весь сетевой трафик, проходящий по диагностируемому сегменту сети или порту коммутатора "захватывается" программой, расшифровывается и затем анализируется. В результате, Вы получаете абсолютно полную и достоверную информацию о том, какие процессы происходят в сети.

Базовая программа **Observer** предназначена для диагностики ТОЛЬКО одного сегмента сети (**collision domain**) или одного коммутатора. В дополнение к базовой программе **Observer** могут быть приобретены дополнительные программные агенты (**probes**) для диагностики удаленных сегментов сети. Программные агенты устанавливаются на компьютерах удаленных сегментов сети и являются приложениями или сервисами **Windows 95/98/NT4/2000/XP**. Поскольку программный агент потребляет очень мало ресурсов, он практически не мешает работе пользователя, на компьютере которого он установлен. При использовании дополнительных зондов базовая программа **Observer** позволяет проводить диагностику сети, состоящей из большого числа сегментов и/или коммутаторов (до 255).

Расширениями базовой программ являются следующие программные модули.

Expert Extension. Данное расширение является экспертной системой, которая анализирует данные, полученные с помощью программы **Observer** . Экспертная система осуществляет обработку сетевого трафика, как после его "захвата" в буфер анализатора протоколов, так и в реальном времени. Использование экспертной системы существенно упрощает поиск "скрытых дефектов" сети.

SNMP Extension. Данное расширение позволяет наблюдать и управлять любыми SNMP устройствами через интерфейс пакета Observer. Программа включает в себя MIB компилятор для поддержки нестандартных (частных) MIB. Использование данного расширения позволяет использовать программы **Observer** в качестве средства управления активным оборудованием, которое имеет встроенные SNMP-агенты.

RMON Extension. Данное расширение позволяет получать информацию с любых RMON зондов (probes) через интерфейс пакета Observer. Поддерживаются зонды RMON1 и RMON2. Использование данного расширения позволяет использовать программы **Observer** в качестве средства контроля активного оборудования, которое имеет встроенные RMON-зонды.

WEB Extesion. Данное расширение позволяет получать долговременную статистику о работе локальной сети через Internet (с помощью обычного WEB-браузера). Использование данного расширения позволяет осуществлять диагностику и мониторинг удаленных сетей при отсутствии единой корпоративной сети.

Программные RMON зонды. Данное расширение является программной реализацией RMON зондов с полной поддержкой всех групп RMON1 и RMON2. Такие зонды являются недорогой альтернативой дорогостоящим аппаратным зондам и могут использоваться не только с пакетом **Observer**, но и с любой программой на базе SNMP (HP Open View, IBM Tivoly, CA TNG и др.)

Подарок для России от компании Network Instruments

Мы рады сообщить Вам приятное известие. С целью укрепления своих позиций на нашем рынке, Компания Network Instruments LLC (разработчик пакета Observer), сделала подарок своим потенциальным Российским партнерам и конечным пользователям пакета Observer.

Подарок заключается в том, что, начиная с версии 6.2, в Observer включена поддержка русского языка. Пока русифицированы только основные меню. Это называется - "базовый уровень локализации продукта". Однако, недалек тот час, когда будут русифицированы все вспомогательные диалоги и Руководство Пользователя.

Не секрет, что Российский рынок программных средств для диагностики сетей "наводнен" пиратскими программами. Достоверность информации, которую эти программы предоставляют о работе сети, является очень сомнительной. Техническая поддержка отсутствует. Задать интересующие вопросы - некому. Больше всего от этого страдают администраторы небольших сетей (до ~30 компьютеров), для которых обосновать своему руководству необходимость покупки диагностического средства стоимостью $1500-$2000 практически невозможно. "Зачем? Ведь и так вроде всё работает!" или "За что же мы тебе зарплату платим?". Это наиболее типичная реакция подавляющего большинства директоров при постановке вопроса о приобретении диагностического средства.

Тем не менее, многие администраторы сетей уже давно осознали, что эффективно обслуживать сеть, не имея в своем распоряжении хороших диагностических средств очень сложно (если не сказать - невозможно). Очевидно, также, что мало купить диагностическое средство. Надо еще, чтобы кто-то объяснил, как его эффективно использовать для решения конкретных проблем, и чтобы можно было кому-то задать конкретные вопросы, а главное, получить на них правильные ответы.

Хотим сказать без ложной скромности, что **"Теперь есть такое средство и Есть такая компания!"**.

Функциональные возможности

Observer 8.x - Анализатор сетевых протоколов и мощное средство для диагностики, управления и мониторинга LAN, WAN, в том числе и коммутируемых сетей.

Observer - это относительно недорогое, чисто программное средство на базе MS Windows 95/98/NT4/2000/XP для диагностики, управления и мониторинга сетей Ethernet (в том числе Fast Ethernet, GigaBIT Ethernet), Token Ring, FDDI.

Пакет **Observer 8** предоставляет в ваше распоряжение два набора функций:

- Набор функций, которые позволяют наблюдать за работой сети и проводить её диагностику в реальном масштабе времени ("real-time monitoring and troubleshooting").
- Набор функций, которые позволяют анализировать работу сети в течение длительного времени (дни, недели месяцы, годы), выявлять тенденции, сравнивать работу сети за разные промежутки времени ("long term trending and baselining").

Пакет **Observer 8** поставляется в виде базовой программы, дополнительных программных агентов (зондов) и набора расширений (extensions).

Базовая программа **Observer** предназначена для диагностики ТОЛЬКО одного сегмента сети (collision domain) или одного коммутатора. При использовании дополнительных программных зондов (probes), предназначенных для диагностики удаленных сегментов сети, **Observer** позволяет проводить диагностику сети, состоящей из большого числа сегментов и/или коммутаторов (до 255).

Расширения - это дополнительные опциональные программные модули. Так, расширение **Expert Extension** является экспертной системой, которая значительно упрощает поиск "скрытых дефектов" сети. Расширение **SNMP Extension** позволяет наблюдать и управлять любыми SNMP устройствами с помощью пакета **Observer**. Расширение **RMON Extension** позволяет получать информацию с любых RMON1/2 зондов через интерфейс пакета **Observer**. Расширение **WEB Extension** позволяет получать долговременную статистику о работе локальной сети через Internet.

Краткий обзор функциональных возможностей Observer 8

- **Захват пакетов и декодирование протоколов (Packet Capture & Decode)**

  Пакет позволяет декодировать более 500 сетевых протоколов (и субпротоколов) и распознавать более 4000 типов фреймов.

  К числу поддерживаемых протоколов (субпротоколов), в частности, относятся:

  - **для сетей NetWare**: IPX, SPX, SAP, RIP, NCP/2, NCP/3, NCP/4, Packet Burst Protocol, NLSP, NDS, Watchdog Protocol, Serialization Protocol, Broadcast Notification Protocol;
  - **для сетей TCP/IP:** IPv4, IPv6, ARP, ICMP, IP, OSPF, RARP, RIP, RIPv2, SNMP, TCP, UDP, NetBios over IP, HTTP, DHCP, DNS, BooTP, FTP, RPC, TELNET, LPD/LPR, TFTP, POP, POP3, IMAP, RCP, NFS, SMTP, SNMPv2, NNTP,PPP.
  - **для сетей Microsoft (NetBios/NetBEUI)**: Full SMB, NON-Session Frames, Session Frames.
  - А также протоколы сетей **DECnet**, **AppleTalk**, **SNA**, **Banyan/Vines**.
  - **Дополнительные протоколы:** MGCP/Megaco, SLP, SQL/TDS, SIP, SDP, RRC 2975 SAP, PPPoE, Xerox XNS/IDP, TNS (Oracle), OSI/CLNP, OSI/Inactive Network, OSI/ISIS, Radius, RSVP, MPLS, CLNS, Frame Relay/Q.931 <Anex D/LMI>, Frame Relay/ISO8885, Frame Relay/Q922, VoIP Codec G729A (Nortel).

  В версии **Observer 8** существенно упрощена процедура старта режима захвата пакетов и декодирования протоколов. Достаточно отметить любую станцию (или пару взаимодействующих станций) в любом режиме наблюдения (например, Pair Statistics) и щелкнуть правой кнопкой мыши, и пакет предложит автоматически запустить режим захвата пакетов именно от выбранной станции (пары взаимодействующих друг с другом станций) .

  - *Функции захвата пакетов и декодирования протоколов незаменимы в тех случаях, когда необходимо быстро определить, почему сеть ведет себя неадекватно. К таким случаям, на пример, относятся: невозможность конкретного пользователя (или группы пользователей) подключиться к сети, медленная работа конкретного пользователя, сбои или невозможность печати на конкретном сетевом принтере и др.*
  - *Функция захвата и декодирования пакетов позволяет хорошо изучить работу сетевых протоколов.*

- **Входные фильтры на захват пакетов (Filters)**

  Пакет позволяет устанавливать большое число разнообразных входных фильтров на захват пакетов. Фильтр называется "входным", т.к. он фильтрует информацию на входе в буфер пакета Observer. (Кроме "входных фильтров" существуют еще и "пост-фильтры", которые фильтруют информацию, которая уже записана в буфер пакета Observer.)

  Входные фильтры могут строиться на основе MAC-адресов станций, IP-адресов станций, имен станций, определяемых в режиме "автоматического обнаружения станций сети" и/или значений данных в кадре сети. Кроме того, имеется возможность осуществлять фильтрацию по конкретным IP-адресам, задавать диапазоны адресов, исключать определенные диапазоны адресов из процесса захвата пакетов, а также использовать групповые символы при определении конфигурации фильтров. Реализована библиотека стандартных фильтров, ориентированных на разные типы протоколов и событий сети. Например, Вы можете установить фильтр, который будет фильтровать, и записывать в буфер только кадры, содержащие ошибки.

  Наряду с использованием библиотеки стандартных фильтров, можно создавать и собственные фильтры, в каждом из которых можно определять тип протокола, значения данных (смещений) в кадре сети, и многое другое.

  В версии **Observer 8** существенно упрощена процедура создания фильтров на основе адресов и имен станций. Достаточно отметить любую станцию (или пару взаимодействующих станций) в любом режиме наблюдения (например, Pair Statistics), щелкнуть правой кнопкой мыши, и пакет вам предложит автоматически создать фильтр, где критериями фильтрации являются адреса выбранных станций.

  - *Наличие входных фильтров существенно упрощает процесс диагностики, т.к. позволяет не записывать на диск компьютера большое число ненужной для анализа информации.*

- **Определение степени загрузки (утилизации) канала связи / коммутатора (Bandwidth Utilization)**

  Пакет измеряет и отображает в графическом и числовом виде текущую, минимальную, среднюю и максимальную утилизацию канала связи сети и/или коммутатора.

  При определении степени загрузки коммутатора, пакет позволяет измерять загрузку не только отдельных портов коммутатора, но и всего коммутатора в целом (по всем портам коммутатора одновременно). Эта возможность является уникальной особенностью пакета **Observer 8.**

  - *Информация об утилизации канала связи/коммутатора необходима, в частности, для определения причин медленной работы сети, вызванной перегруженностью канала связи/коммутатора.*

- **Определение пропускной способности канала связи (Efficiency History)**

  Встроенный в **Observer 8** тест позволяет измерять максимальную пропускную способность сети на канальном уровне. Тест производит периодическую генерацию в канал связи пачек коротких пакетов и одновременно измеряет утилизацию канала связи.

  - *Измеряя пропускную способность сети на канальном уровне после её модификации (изменение топологии, увеличение/уменьшение длины линий связи, модификация активного оборудования), Вы получаете объективную оценку эффективности произведенных изменений.*

- **Сбор статистической информации о наиболее активных станциях сети (Top Talkers)**

  Данный режим позволяет в абсолютных и относительных значениях (процентах) строить рейтинг наиболее активных станций сети. В качестве критерия "активности" станции можно выбрать: общее число обработанных кадров (или байт), число переданных в сеть кадров (или байт), число принятых из сети кадров (или байт), скорость генерации кадров (в пакетах/сек), долю широковещательного и группового трафика, скорость его генерации.

  В версии **Observer 8** в качестве идентификатора станции может выступать как MAC-адрес станции, так и IP-адрес станции.

  - *Статистика о наиболее активных станциях сети позволяет определить, какой пользователь, рабочая станция или приложение потребляет большее, чем положено, количество сетевых ресурсов. Вы сможете увидеть картину загрузки сети, обнаружить неисправные сетевые устройства и определить, какой процент полосы пропускания использует каждое сетевое устройство.*
  - *Если вы используете различные платформы и/или в вашей сети имеется несколько коммутаторов, статистика о наиболее активных станциях сети поможет вам добиться оптимального расположения ваших серверов для достижения максимальной производительности.*
  - *Статистика о наиболее активных станциях сети позволяет определить, насколько архитектура и топология сети соответствуют решаемым в сети задачам. Так, например, вы сможете легко определить, какой пропускной способностью должны обладать конкретные рабочие станции сети. Критерием будет являться объем передаваемых и/или принимаемых ими данных.*

- **Сбор статистической информации по длинам кадров (Size Distribution Statistics)**

  Данный режим позволяет определить какова процентная доля кадров конкретной длины, передаваемых и/или принимаемых каждой станцией сети и всей сети в целом. Другими словами, для каждой станции сети и всей сети в целом строится распределение по процентной доле переданных и принятых кадров различной длины (диапазона длин).

  - *Эта информация позволяет оценить эффективность использования канала связи различными сетевыми приложениями. Чем больше доля коротких кадров, тем менее эффективно используется канал связи сети.*

- **Сбор статистической информации по сетевым протоколам (Protocol Distribution)**

  Данный режим позволяет определить, какая доля трафика приходится на каждый протокол или субпротокол, который работает в сети (поддерживаются более 4000 типов). Другими словами, для каждой станции сети и всей сети в целом строится распределение трафика по используемым сетевым протоколам.

  - *Анализ этой информации позволит Вам определить, на настройку каких сетевых протоколов Вам следует обратить особое внимание.*
  - *Режим Switched Mode дает возможность увидеть интегральную картину протоколов, работающих через ваш коммутатор.*
  - *Вы сможете выяснить, какие рабочие станции создают наибольшую нагрузку на вашу сеть, и какие серверы используются в отдельных сегментах.*
  - *Вы сможете определить, какая доля пропускной способности сети приходится на "случайные" протоколы, которые являются следствием неправильной настройки сетевого оборудования или ПО.*

- **Сбор статистической информации по взаимодействующим парам станций (Network Pair Statistics (Matrix))**

  Пакет отслеживает и отображает все взаимодействующие друг с другом пары станций. Для каждой пары станций отображаются интенсивность и объем сетевого трафика. Кроме этого, собираемая статистика по взаимодействующим парам станций включает в себя время реакции каждой станции сети в каждой паре взаимодействующих друг с другом станций.

  - *Информация о времени реакции каждой станции сети (в качестве которой может выступать и сервер) помогает определить причину замедления работы конкретного прикладного ПО в сети.*

- **Наблюдение за WWW-сервером (Web Observer)**

  Программа позволяет наблюдать входящий и исходящий с WWW-сервера трафик. Отображаются адреса станций, работающих с WWW-сервером, интенсивность работы каждой станции с сервером, процентную долю трафика, который приходится на каждую станцию.

  Встроенные функции "пинга" сервера и функции определения его статуса позволяют получить статистику по времени реакции сервера и числу возникающих ошибок.

- **Наблюдение за маршрутизатором (Router Observer)**

  Данная функция позволяет наблюдать за маршрутизаторами (поддерживается одновременная работа с 8 маршрутизаторами). Цель наблюдения - определить степень загрузки интерфейсов маршрутизаторов. Отображается, в частности, объем и интенсивность трафика, проходящего по каждому интерфейсу (порту) маршрутизатора в каждом направлении (входящий/исходящий трафик), а также процентная величина загрузки интерфейса для каждого направления.

  Определив максимальную пропускную способность канала связи между маршрутизатором и внешним миром (например, канала T1), программа определит утилизацию этого канала связи. Определяется текущая утилизация (с интервалом усреднения 1 минута) и долговременная (с интервалом усреднения 1 час).

  - *Данный режим позволяет определять степень загрузки глобальных каналов связи без использования дорогостоящих аппаратных анализаторов глобальных сетей.*
  - *Информация об объеме и интенсивности трафика, проходящего по портам маршрутизатора, упрощает процесс локализации "узких мест" в глобальной/корпоративной сети.*

- **Индикация активности сети (Network Activity Display)**

  В реальном времени на совмещенном графике, на фоне утилизации канала связи отображается доля широковещательных и групповых пакетов. График меняет свой цвет в зависимости от величины утилизации канала связи и процентной доли широковещательных и групповых пакетов в сетевом трафике.

  - *Достаточно беглого взгляда на график активности сети, чтобы определить, что замедление работы сети является следствием широковещательного или группового "шторма".*

- **Генерация тестового трафика (Traffic Generator)**

  Observer 8 позволяет осуществлять генерацию тестового трафика в процессе наблюдения за работой сети. Вы можете задать размер генерируемых пакетов, интенсивность и период генерации, адрес назначения генерируемых пакетов, адрес источника генерируемых пакетов, число генерируемых пакетов и т.п. Для тестирования конкретных устройств (например, маршрутизаторов) можно задать тип сетевого протокола, который будет инкапсулирован в генерируемые пакеты. Кроме этого, пакет позволяет генерировать в сеть пакеты, которые ранее были захвачены из сети и записаны в буфер.

  - *Генерация тестового трафика в процессе наблюдения за работой сети является важнейшим методическим приемом для выявления "скрытых" дефектов сети. Тестовый трафик, создаваемый анализатором провоцирует проявление "скрытых" дефектов.*

- **Триггеры и сигнализация (Triggers & Alarms)**

  Observer 8 позволяет устанавливать так называемые "триггеры" (trigger) для фиксации конкретных событий в сети. Под "триггерами" в данном случае понимается конкретные условия или события, которые происходят в сети. Примерами таких событий являются, например, факт перегрузки сервера, определенная доля искаженных пакетов в общем числе пакетов, повышенная утилизация канала связи сети, факт наличия дубликатов IP-адресов, внедрение в вашу сеть хакера, и многое другое.

  Можно использовать заранее определенные триггеры, в которых меняются только значения параметров или определить собственные триггеры.

  Пользователь может задать те действия, которые должна выполнять программа при срабатывании триггера, т.е. при фиксации конкретного события в сети. Такое действие называется "сигнализацией" (alarm). В **Observer 8** сигнализацией может быть запись события в лог-файл (журнал ошибок), звуковой сигнал, запуск определенной программы, всплывающее окно, вызов по пейджеру, сообщение по e-mail.

  - *Триггеры и сигнализация освобождают администратора сети от необходимости сидеть за дисплеем и наблюдать за работой сети. Достаточно установить триггеры на интересующие события и программа сообщит Вам, когда эти события наступят.*

- **Сбор долговременной статистической информации о работе сети и построение "трендов" (Network Trending)**

  Функция сбора долговременной статистики (Network Trending) позволяет наблюдать, собирать и анализировать сетевой трафик за длительный временной интервал (дни, недели, месяцы, годы). Observer 8 дает возможность не только получить полную статистическую информацию за интересующий Вас интервал времени, но и сравнить характеристики работы сети за разные периоды времени как по сети в целом, так и по конкретной рабочей станции или порту коммутатора. Таким образом, Вы сможете построить "тренд" использования сети с привязкой к следующим типам данных: 1) По конкретной рабочей станции, 2) По конкретному порту коммутатора, 3) По конкретному SNMP-устройству (эта функция достпна только в Observer Suite).

  - *Анализ информации, характеризующий работу сети за длительный промежуток времени позволяет лучше понять, в какой степени архитектура сети соответствует требованиям пользователей сети.*
  - *Сравнив загруженность сети в начале и конце рабочего дня, в начале и конце месяца, квартала или года, Вы сможете легко определить, как изменяются потребности пользователей сети и когда следует начинать ее модернизацию.*

- **Индикация "здоровья" сети (Network Vital Signs)**

  В реальном времени на совмещенном графике программа показывает число и тип ошибок передачи данных, а также число конфликтов (коллизий) в зависимости от утилизации канала связи сети.

  Для сетей Ethernet отображаются следующие типы ошибок: CRC, alignment, packets too large/small, collisions. Для сетей Token Ring - все 29 типов ошибок MAC-уровня. Для сетей FDDI - все 183 типа ошибок уровней MAC и SMT. Для сетей Frame Relay отображаются пакеты shows FECN, %FECN, BECN, %BECN, DE и % DE.

  Встроенный в программу тест провоцирует проявление ошибок передачи данных и конфликтов (в сетях Ethernet). Важной функцией режима является то, что график меняет свой цвет в зависимости от величины утилизации канала связи сети и доли ошибок и конфликтов в сетевом трафике. Так, график зеленого цвета свидетельствует об отсутствии проблем в сети, график красного цвета свидетельствует о наличии проблем в сети, график желтого цвета свидетельствует о том, что утилизация канала связи слишком низка, чтобы можно было делать выводы о наличии или отсутствии проблем в сети.

  - *Достаточно беглого взгляда на график индикации "здоровья" сети и Вы определите, что замедление работы сети является следствием повышенного числа ошибок передачи данных или следствием повышенного числа конфликтов в сети.*

- **Сбор статистической информации об ошибках передачи данных (Network Errors-by-Station)**

  Данная функция позволяет определять, какое число ошибок передачи данных (Ethernet, Token Ring, и FDDI) приходится на каждую рабочую станцию сети и сервер. Эта, на первый взгляд, "банальная" функция реализована далеко не во всех анализаторах протоколов. В пакете **Observer 8**, возможность определения числа ошибок передачи данных каждого типа по станциям сети обеспечивается специальными драйверами (ErrorTrack NDIS drivers), входящими в комплект пакета **Observer 8.** При отсутствии специализированных драйверов, в сетях Ethernet достоверную информацию об ошибках передачи данных можно получить только с помощью специализированных сетевых карт.

  Для каждой станции сети программа предоставляет полную статистическую информацию об ошибках передачи данных. Такая информация включает в себя: общее число ошибок передачи данных, число ошибок каждого типа (CRC, короткие кадры, длинные кадры, ошибки выравнивания и др.), скорость возникновения ошибок, долю ошибок каждого типа в общем числе переданных каждой станцией кадров.

  - *Совершенно очевидно, что подобная информация незаменима для выявления дефектов активного и пассивного оборудования сети.*

- **Автоматическое обнаружение сетевых имен (Discover Network Names)**

  Данный режим позволяет автоматически определить все имеющиеся в сети MAC-адреса, поместить их в таблицу настройки фильтров и присвоить соответствующие им имена (auto-alias) для сетей IP или поставить в соответствие IP-адреса или имена DNS. В случае использования NetWare можно "привязать" обнаруженные MAC-адреса к именам пользователей (login name). В сетях Microsoft "привязка" адресов к именам пользователей происходит автоматически. Кроме этого, имена станций можно импортировать, если **Observer 8** используется в сетях Appletalk, SNA, DECnet.

- **Диагностика коммутируемых сетей (Switched Modes)**

  Начиная с версии 6.0, в пакете **Observer** реализована **поддержка коммутируемых сетей**. В настоящее время реализованная в пакете **Observer** технология диагностики коммутируемых сетей является **уникальной**!

Если Ваша сеть построена на основе коммутаторов (свичей), коммутаторы позволяют осуществлять "зеркалирование" портов (port mirroring, spanning или tapping) и имеют telnet-интерфейс, то Вы можете "квази-одновременно" наблюдать за трафиком на всех портах коммутатора. Подключив зонд Observer-а к одному из портов коммутатора, вы сможете автоматически (в цикле) "зеркалировать" все остальные порты коммутатора на подключенный зонд. В результате у вас появится возможность видеть и анализировать трафик не только по каждому отдельно взятому порту коммутатора, но и по всем портам коммутатора сразу. Другими словами, Вы сможете видеть весь трафик, проходящий через коммутатор. Подобная технология позволяет диагностировать 100% коммутируемую сеть таким же образом, как и не коммутируемую (shared).

При этом, естественно, можно анализировать и записывать в буфер пакета **Observer** трафик, проходящий по каждому конкретному порту (портам) коммутатора.

- **Наблюдение за Internet (Internet Observer)**

  Данная функция позволяет определить, как пользователи сети или различные сетевые устройства используют ресурсы Internet. Существуют три возможных режима работы:

  Internet Patrol – позволяет осуществлять сбор информации об использовании ресурсов Internet пользователями сети. Например, можно определить, к каким сайтам обращался конкретный пользователь, когда он начал и закончил сессию и какое количество данных было при этом было передано.

  IP to IP Pairs (Matrix) – отображает ту же информацию, что и Internet Patrol, но с использованием IP-адресов (данный режим может быть полезен для больших сетей, где используются несколько сайтов для одного разделяемого Internet-соединения).

  IP Subprotocols by station – позволяет оценить использование различных сервисов Internet (по субпротоколам) конкретными пользователями.

Зонды и диагностика распределенных сетей

Диагностика распределенных сетей, состоящих из большого числа сегментов, осуществляется с помощью зондов (probes). Обычно в каждом диагностируемом сегменте сети устанавливается один зонд. Установка зондов избавит Вас от необходимости переносить анализатор протоколов, подключая его к разным сегментам распределенной сети. Кроме этого, одновременная диагностика локального и удаленного сегмента незаменима для выявления целого класса "скрытых" дефектов, которые возникают в одном сегменте сети, а проявляются в другом сегменте сети. Зонды могут быть программными, аппаратными или программно-аппаратными (встроенными в активное оборудование).

Консоль пакета **Observer 8** может работать с двумя типами зондов:

- Advanced-зонд;
- RMON-зонд.

Advanced-зонд - это "фирменный", чисто программный зонд, производства компании Network Instruments. Advanced-зонды устанавливаются на компьютерах удаленных сегментов сети, которые вы хотите диагностировать. Эти зонды являются приложениями или сервисами **Windows 95/98/NT4/2000/XP**. Advanced-зонд может производить сбор долговременной статистики о работе сети независимо от консоли пакета **Observer** и передавать информацию консоли только по запросу последней.

Зонды потребляют очень мало системных ресурсов, и практически не мешают работе пользователей, на компьютерах которых они установлены. Их воздействие на сеть, также минимально. При захвате пакетов в буфер (наиболее ресурсоёмкий режим) зонд может захватывать пакеты в свой локальный буфер и передавать их консоли только по запросу последней.

Advanced-зонд обладает большими функциональными возможностями, чем RMON-зонд. Поэтому, при прочих равных условиях, использовать Advanced-зонд более предпочтительно, чем RMON-зонд.

Кроме Advanced-зондов, пакет **Observer 8** может работать с RMON-зондами. В качестве RMON-зондов можно использовать аппаратные RMON-зонды третьих фирм, программно-аппаратные зонды, встроенные в активное оборудование, или чисто программные RMON-зонды, которые, также, производятся компанией Network Instruments.

Программные RMON-зонды производства компании Network Instruments - это зонды, которые поддерживают все 19 групп RMON1 и RMON2 в соответствии с RFC: 1513, 1757, 2021 и 2074 и которые могут поддерживать до 10 одновременных интерфейсов с SNMP/RMON консолями. Эти зонды являются приложениями или сервисами **Windows 95/98/NT4/2000/XP** и могут использоваться как недорогая альтернатива дорогим аппаратным зондам.

Зонды, производимые компанией Network Instruments могут использоваться не только с пакетом **Observer 8**, но и с любой программой на базе SNMP (HP Open View, IBM Tivoly, CA TNG и др.)

Использование с пакетом **Observer 8** RMON-зондов целесообразно только в том случае, если Вы используете активное оборудование, которое уже имеет встроенные RMON-зонды (Вам не надо их покупать дополнительно) и/или в вашей корпоративной сети не должно быть управляющих протоколов, отличных от SNMP.

Какое число зондов необходимо иметь, чтобы одновременно контролировать всю сеть?

Следует помнить, что один программный зонд может контролировать ЛИБО один коллизионный домен сети (хаб или группа хабов), ЛИБО один коммутатор, если все станции подключены непосредственно к коммутатору (без хабов). Таким образом, чтобы иметь возможность контролировать всю сеть, надо иметь число зондов (N), которое вычисляется по следующим формулам.

1. Если сеть построена на основе коммутаторов и концентраторов, и при этом часть рабочих станций подключена непосредственно к коммутаторам, а часть - через концентраторы, то:
N = число коммутаторов + число коллизионных доменов.

2. Если сеть построена только на базе коммутаторов (100% коммутируемая сеть), то:
N = число коммутаторов.

Примечание. Пакет **Observer** позволяет контролировать только такие коммутаторы, которые имеют встроенную технологию "зеркалирования" портов и допускают управление по протоколу telnet (HP, Cisco, Bay Networks).

Системные требования

Минимально: Windows 98, поддерживаемый сетевой адаптер (**НЕ ЛЮБОЙ, если вы хотите иметь возможность видеть распределение ошибок передачи данных по станциям**), мышь, монитор VGA при разрешении не ниже 800x600.

Рекомендуется: Windows 2000, 16-битный сетевой адаптер (**НЕ ЛЮБОЙ, если вы хотите иметь возможность видеть распределение ошибок передачи данных по станциям**), 16-битный графический адаптер, монитор SVGA при разрешении не ниже 1024x768.

Требования к процессору и оперативной памяти:

	МИНИМАЛЬНО		РЕКОМЕНДУЕТСЯ	
	Windows 98/ME	**NT/2000/XP**	**Windows 98/ME**	**NT/2000/XP**
10MB Ethernet	Pentium 266 /64MB RAM	Pentium 266 /128MB RAM	Pentium 400 /128MB RAM	Pentium 400 /128MB RAM
100MB Ethernet	Pentium 400 /128MB RAM	Pentium 400 /128MB RAM	Pentium III 900 /128MB RAM	Pentium III 900 /256MB RAM
4MB Token Ring	Pentium 266 /64MB RAM	Pentium 266 /128MB RAM	Pentium 400 /128MB RAM	Pentium 400 /128MB RAM
16MB Token Ring	Pentium 266 /128MB RAM	Pentium 266 /128MB RAM	Pentium 400 /128MB RAM	Pentium 400 /128MB RAM
FDDI	Pentium 400 /128MB RAM	Pentium 400 /128MB RAM	Pentium II 600 /256MB RAM	Pentium III 600 /256MB RAM
Gigabit	Pentium III 600 /128MB RAM	Pentium III 800 /128MB RAM	Pentium 1.4Ghz /256MB RAM	Pentium III 1.4Ghz /512MB RAM

Поддерживаемые сетевые адаптеры: Любые сетевые адаптеры с драйверами NDIS 3.0/3.1 (или более поздними), поддерживающие режим PROMISCUOUS MODE (Режим, в котором сетевой адаптер обнаруживает в сети все фреймы вне зависимости от их конечного адреса). Для диагностики сетей Fast Ethernet рекомендуется использовать сетевые адаптеры стандарта PCI.

Требования к коммутаторам: Для использования функции LOOPING в зондов (probes) Observer 8 коммутаторы должны поддерживать технологию "зеркалирования портов" и иметь возможность управления через SNMP (предпочтительно) или по протоколу Telnet.

Для использования функции "Сбор статистики рабочей станции Ethernet" (Ethernet Station Error Statistics): в настоящее время компания Network Instruments поставляет драйвер для сетевых адаптеров с чипсетом Intel/DEC 21143 (PCMCIA, ISA или PCI).

Поддерживаемые платформы: Microsoft Windows 98/ME и Windows NT 4.x/2000/XP.

Поддерживаемые топологии: Ethernet (10/100/Gigabit), Token Ring (4/16Mb), FDDI и Frame Relay.

Expert Extension – Экспертная система для диагностики сети

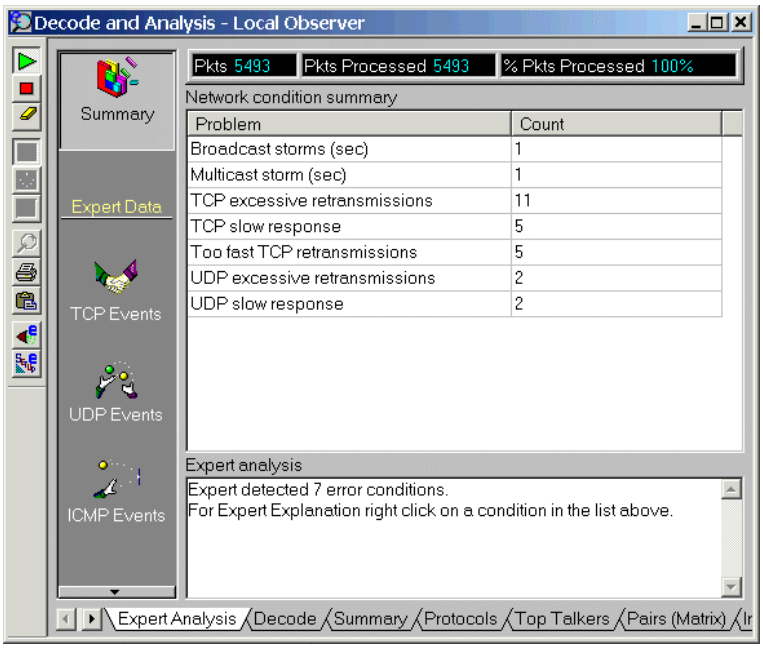
Во многих случаях базовых возможностей пакета Observer недостаточно для поиска неисправностей в сети. Например, для выявления нежелательных событий в работе протоколов транспортного и прикладного уровней, являющихся признаками наличия дефекта или узкого места в сети (повторных передач на транспортном уровне, больших задержек при передаче пакетов и др.) надо проанализировать сотни и тысячи сетевых пакетов. В таких ситуациях значительную помощь оказывают экспертные системы, анализирующие информацию, содержащуюся в трассе захваченных пакетов, и, на основе заложенных в них эвристических правил, делающие выводы о тех или иных дефектах сети. Такой экспертной системой в пакете Observer является Expert Extension.

Expert Extension позволяет осуществлять экспертный анализ не только **на основе предварительно записанной канальной трассы** (информации, проходящей по сети и собираемой анализатором протоколов), но и в процессе захвата пакетов. Организовав циклический режим заполнения буфера захвата пакетов, вы сможете осуществлять экспертный анализ сетевого трафика **в реальном времени**. Все выявленные проблемы отображаются в одном окне - в виде списка, из которого по контекстному меню можно перейти к режиму более детального анализа данной проблемы, а также вывести справочную информацию о возможных причинах и путях устранения обнаруженной проблемы.

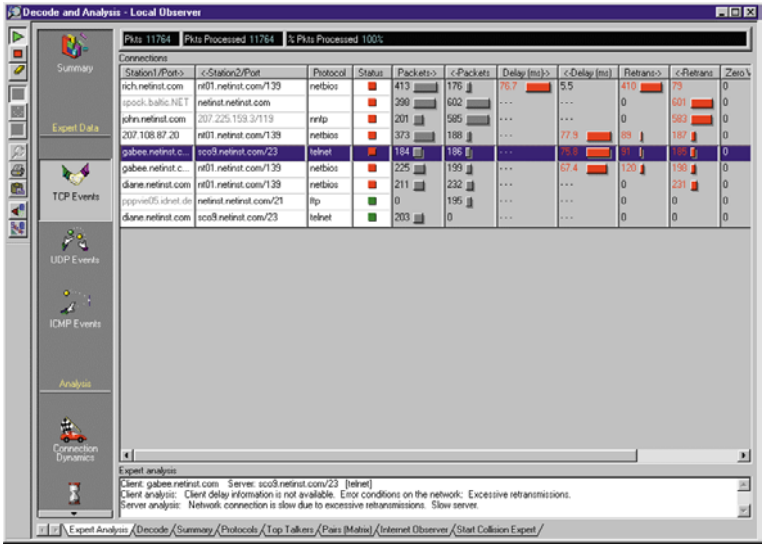
В версии Observer 8.0 экспертный анализ осуществляется, в основном, для IP-трафика. В следующих версиях планируется также поддержка протоколов IPX/SPX, NetBEUI/NetBIOS.

Некоторые из возможностей Expert Extension приведены ниже.

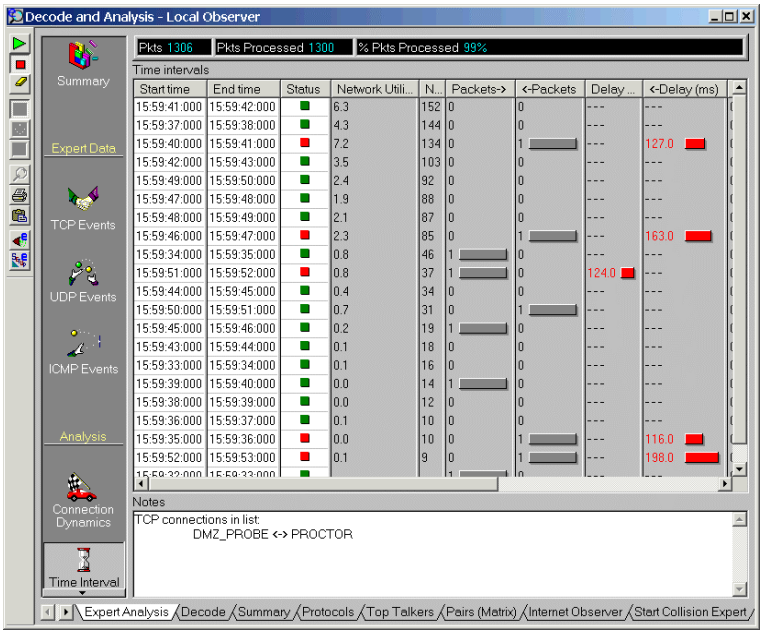
Сводный анализ проблем (Expert Summary Problem Analysis) отображает краткую информацию об ошибках. Данная функция позволяет отображать экспертную информацию для TCP/UDP/ICMP, IPX/SPX, NetBIOS/NetBEUI, SQL и Frame Relay.



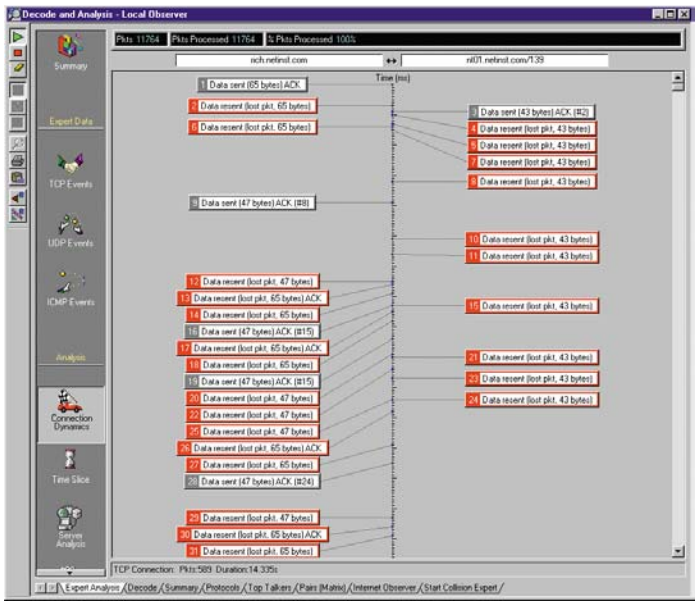
Эксперты TCP/UDP/ICMP, IPX/SPX и NetBIOS/NetBEUI позволяют выявлять и отображать в режиме реального времени проблемы, возникающие в стеке протоколов и в базирующихся на этих протоколах приложениях. При анализе трафика локальных и глобальных сетей используются различные критерии, учитывающие специфику этих сетей. Отслеживается время установления соединения, время отклика для всех основных служб, базирующихся на использовании TCP/UDP-портов.



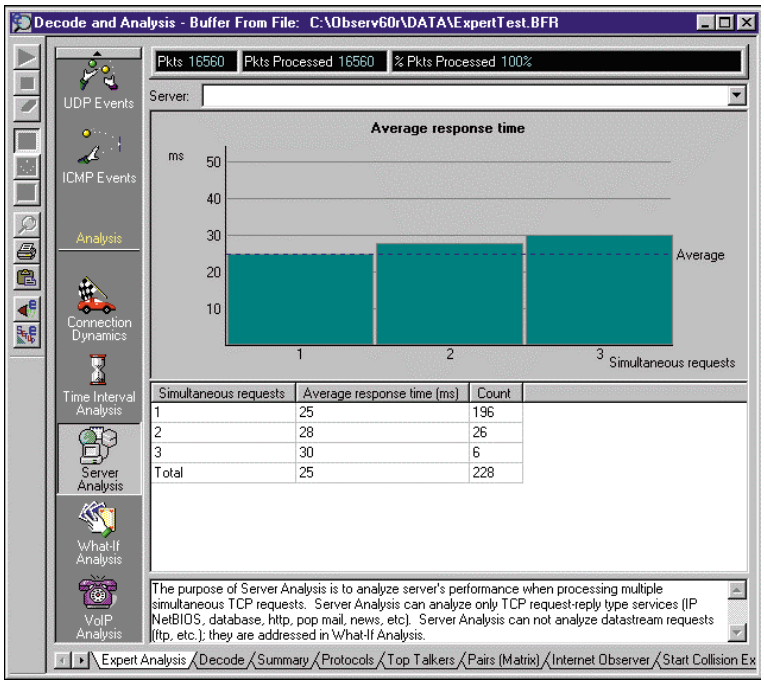
Анализ временных интервалов (Time Interval Analysis) можно провести для любого соединения, показываемого в окнах Экспертов TCP/UDP/ICMP. Информация по выбранному соединению разбивается по последовательным интервалам времени. Такое представление позволяет, в частности, понять, проявляется ли та или иная информация постоянно, или она имела место лишь на определенном интервале времени. Чтобы можно было определить, не связана ли наблюдаемая проблема с загруженностью сети, для каждого интервала времени выводится значение утилизации сети.



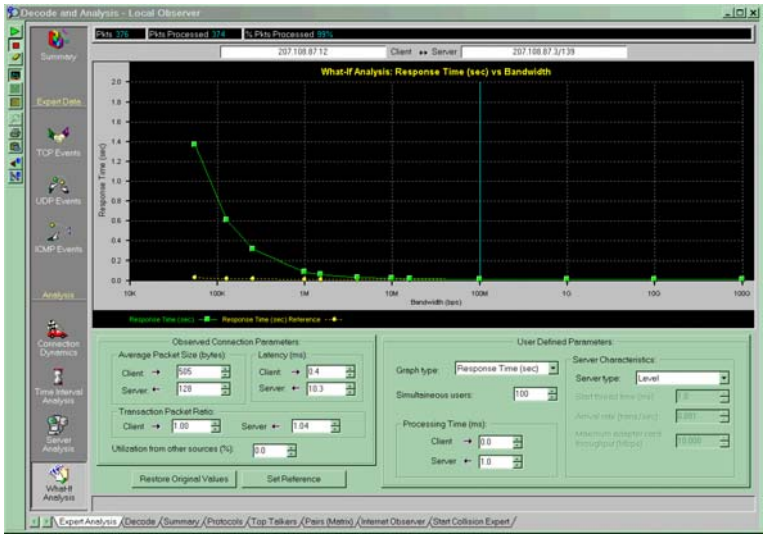
Динамика соединений (Connection Dynamics) позволяет отобразить процесс обмена пакетами между выбранными узлами сети в виде диаграммы. Визуальное отображение интервалов времени между пакетами позволяет быстро выявлять длительные задержки и низкое время реакции. Повторно переданные или пропущенные пакеты выделяются на диаграмме другим цветом. Любой отображаемый пакет можно декодировать одним нажатием мыши.



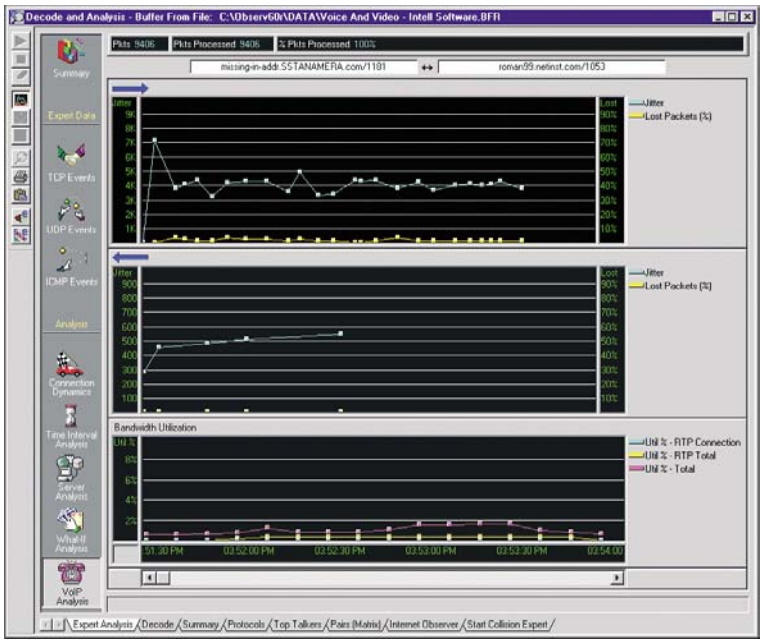
Анализ сервера (Server Analysis) позволяет исследовать зависимость времени отклика сервера, выбранного из списка обнаруженных в трассе узлов, от количества одновременных запросов к нему. Диапазон значений числа запросов определяется данными, содержащимися в анализируемой трассе.



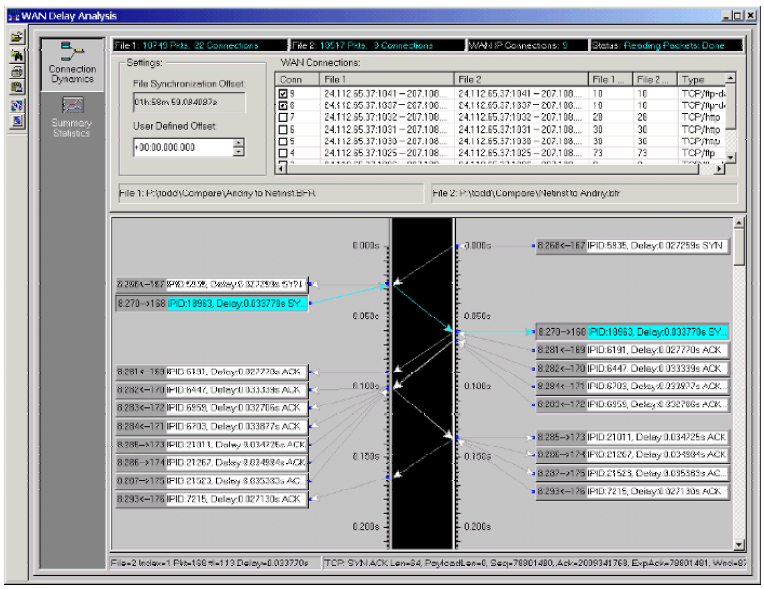
Режим моделирования "What If" ("What if" Modeling) использует информацию, полученную из реального сеанса обмена сообщениями между станциями, для того, чтобы предсказать, как изменятся характеристики сети (утилизация, времена отклика) при изменении скорости передачи данных (например, с 10 Мб/с до 100 Мб/с), среднего размера пакетов, отношения числа переданных пакетов к числу принятых, загрузки сервера, числа пользователей и т.д. Используя этот режим можно моделировать последствия изменений в архитектуре сети и в настройке параметров прикладного ПО.



Эксперт VoIP графически отображает и анализирует потоки данных, использующих протоколы группы VoIP (H.323). На трех отдельных дисплеях отображаются: процент потерянных пакетов и дрожание (jitter) при передаче данных в обоих направлениях; утилизация, создаваемая передаваемыми данными; полная утилизация сети. Данный режим помогает понять, чем вызваны проблемы передачи данных или, наоборот, при какой загрузке сети передача данных будет осуществляться с приемлемым уровнем качества.



Анализ задержек в глобальных сетях связи (WAN Delay Analysis) при помощи функции **WAN compare capture**, основанной на технологии временной синхронизации позволяет определить причины задержек, возникающих в глобальных сетях связи. Expert Observer (и удаленный зонд (Probe)) дает возможность осуществлять захват пакетов на обоих концах глобальной линии связи и определять время отклика (Response Time).



Системные требования, предъявляемые Expert Extension

Минимально: Pentium 400 с объемом оперативной памяти 128 Мб, Windows 98 или более поздняя версия, поддерживаемый сетевой адаптер, мышь, монитор SVGA при разрешении не ниже 1024x768; лицензионная версия Observer 8.0.

Рекомендуется: Pentium 600 или более мощный с объемом оперативной памяти 256 Мб, Windows 2000/XP, поддерживаемый сетевой адаптер, мышь, 16-битный графический адаптер, монитор SVGA при разрешении 1280x1024; лицензионная версия Observer 8.0.

RMON Extension (RMON-Расширение)

Область применения пакета Observer 8.x может быть существенно расширена, если одновременно с этим пакетом установить его специальное расширение, которое называется RMON Extension (далее RMON-Расширение).

Установка RMON-Расширения позволяет использовать для диагностики сети не только фирменные зонды производства компании Network Instruments, но и ВСЕ стандартные RMON-зонды, встроенные в активное сетевое оборудование или установленные автономно. Это означает, что, имея пакет Observer 8.x и RMON-Расширение, Вы получаете возможность контроля всего активного оборудования вашей сети и, плюс к этому, возможность анализа сетевых протоколов.

Уникальность же предлагаемого решения заключается в том, что вся информация, которая собирается стандартными RMON-зондами и обычно отображается в виде сложных для восприятия таблиц, теперь воспроизводится с помощью тех же графических экранов, которые используются программой Observer для отображения состояния сети. Это означает, что непосредственно из оболочки пакета Observer Вы сможете не только анализировать сетевой трафик, но и осуществлять сбор данных и управлять активным сетевым оборудованием, если последнее оснащено встроенными RMON-зондами.

RMON-Расширение дополняет функциональность пакета Observer всеми возможностями, которые предоставляются RMON - технологиями. RMON-Расширение позволит Вам диагностировать любой сегмент сети, коммутатор или какое-то другое устройство, - достаточно лишь, чтобы в этом сегменте или устройстве был установлен RMON-зонд.

Таким образом, если встроенные в оборудование вашей сети RMON-зонды, обладают достаточной для полноценной диагностики функциональностью, то для диагностики распределенной сети Вам не нужно приобретать дополнительных фирменных зондов к программе Observer 8.x. Эти функции возьмут на себя RMON-зонды, встроенные в сетевое оборудование.

Дополнив пакет Observer одним только RMON-Расширением, Вы, фактически, получаете несколько инструментов:

- Консоль управления, полностью соответствующую промышленному стандарту RMON.
- Систему отображения данных, получаемых с удаленных зондов, поддерживающих стандарты RMON1 и/или RMON2.
- Единое средство управления сетями, в которых используется оборудование различных производителей.
- Удаленную консоль для RMON-устройств, расположенных в любом месте Вашей локальной или глобальной сети, либо подключаемых через Internet.
- Эффективное с точки зрения цена/производительность решение для RMON-анализа.

Зачем нужно использовать RMON?

RMON (Remote Network Monitoring - Удаленный Сетевой Мониторинг) в настоящее время очень быстро становится промышленным стандартом для управления трафиком и сбора данных на уровне пакетов для многосегментных локальных и глобальных сетей. Использование RMON в качестве стандарта Вашей сети, позволяет осуществлять анализ трафика во всех сетевых сегментах и коммутаторах, используя единую консоль управления - программу Observer с RMON-Расширением.

Управление на основе RMON

RMON предоставляет стандартную информацию, которую администратор сети может использовать для мониторинга, анализа и поиска неисправностей в распределенных локальных сетях и в связанных между собой глобальных сетях с одного (центрального) рабочего места.

RMON-Расширение может работать как с аппаратными зондами (например, встроенными в коммутаторы или маршрутизаторы), так и с программными зондами (например, с RMON-зондами компании Network Instruments, которые работают в среде Windows 95/98/NT/2000/XP). RMON-Расширение предоставляет администратору сети детальную информацию со всех RMON-зондов, независимо от того, где они физически расположены.

Во многих коммутаторах, устанавливаемых в локальных сетях, уже имеются встроенные зонды, которые могут отслеживать RMON-информацию, касающуюся трафика, проходящего через эти устройства. Такие аппаратные RMON-зонды могут использоваться администратором сети для сбора информации, характеризующей работу сетевых устройств и подключенных к этим устройствам сегментов сети . Чтобы получать информацию со встроенных в оборудование RMON-зондов, необходима RMON-консоль. Используя RMON-Расширение, Вы получаете возможность собирать информацию с RMON-зондов и отображать её в удобном для восприятия и анализа виде - с помощью графического интерфейса пакета Observer.

Если оборудование вашей сети не имеет встроенных RMON-зондов, но вы хотите использовать RMON-технологии, то вам необходимо приобрести либо автономные аппаратные RMON-зонды, либо программные RMON-зонды. Компания Network Instruments предлагает в качестве альтернативы дорогим аппаратным зондам, существенно менее дорогие программные RMON-зонды, которые можно установить на серверах или рабочих станциях в тех сегментах сети, которые нужно контролировать или диагностировать. Эти программные RMON-зонды также будут собирать RMON - данные для последующего их графического представления пакетом Observer с RMON-Расширением.

Примечание. *Поскольку программные RMON - зонды компании Network Instruments реализованы в соответствии с международными стандартами, их можно использовать с любой стандартной системой управления сетью, например HP Open View, CA Unicenter и др.*

RMON-зонды могут собирать до 19-ти типов информации, известных как RMON-группы в полном соответствии с RFC 1513, 1757, 2021 и 2074: 9 групп составляют стандарт RMON1 , а следующие 10 групп - стандарт RMON2. Использование RMON-технологии позволяет получать информацию о числе переданных пакетов или байт, числе пропущенных пакетов, статистику по хостам, статистику по обмену данными между парами адресов, а также получать сообщения об определенных событиях, происходящих в сети. Такого рода информация может помочь администратору сети определить, в какой степени каждый пользователь загружает сеть, какие сетевые ошибки имели место и т.д. Конфигурирование RMON-зондов на выдачу предупреждений (Alarms), сигнализирующих о том, что в сети происходят определенные события, позволяет использовать данные зонды в качестве индикаторов надвигающихся проблем.

RMON-зонд представляет собой программное обеспечение, которое выполняется на стандартном не выделенном компьютере под управлением Windows 98/Me/NT/2000/XP и не требует установки каких-либо дополнительных аппаратных средств. (Для сетей Ethernet установка поддерживаемых сетевых адаптеров и специальных драйверов ErrorTrack компании Network Instruments позволит получать более подробную информацию о возникающих в сети ошибках. Эта дополнительная возможность не является обязательной для правильного функционирования RMON зондов). RMON-зонд в процессе своей работы отображает на дисплее текущую информацию о состоянии сети.

Для обеспечения возможности сбора информации о работе удаленных сегментов сети в каждом из них должен быть установлен RMON-зонд.

RMON-зонд поддерживает отсылку результатов измерений на одновременно несколько управляющих компьютеров, количество которых ограничивается только объемом оперативной памяти на рабочей станции с установленным RMON-зондом. RMON-зонд может отсылать результаты измерений на любую управляющую SNMP- или RMON-консоль, на которой сконфигурированы необходимые права доступа. Настройки безопасности RMON-зонда поддерживают возможность задания отдельных имен сообществ (Community String) на чтение и на запись, а также задание конкретных IP-адресов (диапазонов IP-адресов) управляющих компьютеров.

RMON-зонд может работать одновременно с 10 интерфейсами. При этом топологии данных интерфейсов могут быть смешанными, например возможна одновременная работа с интерфейсами Ethernet и Token Ring.

RMON-зонд можно сконфигурировать для отправки SNMP-трапов на один или несколько управляющих компьютеров.

Внимание! При всех своих достоинствах, любые стандартные RMON-зонды (в том числе и программные RMON-зонды производства компании Network Instruments) уступают по функциональности фирменным зондам компании Network Instruments, которые называются "Advanced Probes" (Advanced-зонды) и используются в пакете Observer наряду с RMON-зондами. "Advanced Probes" не являются RMON-зондами и имеют ряд дополнительных функций, не предусмотренных стандартами RMON1 и RMON2.

Удобное представление RMON-данных

RMON-Расширение для пакета Observer отображает, как данные RMON1, так и данные RMON2, используя единый графический интерфейс пакета Observer. Благодаря этому, любой администратор сети может просматривать и анализировать RMON-данные, не вникая в сложности их представления в соответствующих RMON-таблицах. Администраторы и консультанты, знакомые с программой Observer, могут сразу же, без дополнительной подготовки приступать к диагностике сети с помощью RMON-Расширения.

Управление RMON-зондом

RMON-Расширение позволит Вам не только анализировать данные, собираемые RMON-зондами, но и управлять ими, т.е. конфигурировать различные RMON-таблицы и RMON-переменные. Большой объем информации, собираемый RMON- зондами, позволяет контролировать фактически весь сетевой трафик. При этом RMON-Расширение содержит все необходимые средства для того, чтобы с легкостью управлять всей информацией, собираемой RMON-зондами в каждом сегменте сети. Более того , RMON-Расширение проверит Ваш RMON-зонд и сообщит Вам о его возможностях (в частности, о его соответствии стандартам RMON1 и/или RMON2).

Экраны, используемые для отображения RMON-данных

Чтобы облегчить визуальное восприятие, а следовательно и анализ RMON-данных, RMON-Расширение отображает RMON-данные с помощью тех же самых экранов, которые используются для отображения данных в программе Observer. Кроме этого, RMON-Расширение позволяет отображать RMON-данные (все 19 групп информации со своими значениями) непосредственно в виде RMON-таблиц. В зависимости от того, какую версию RMON поддерживает Ваш зонд, RMON-Расширение может использовать для отображения RMON-данных различные экраны пакета Observer.

Экраны пакета Observer, на которых отображаются данные, собираемые RMON1-зондами

Bandwidth Utilisation (Текущая загрузка сети) - показывает текущее значение утилизации сети или коммутатора.

Utilisation History (Долговременная загрузка сети) - показывает минимальное, среднее и максимальное значение утилизации сети для заданного периода времени в графическом и цифровом виде.

Utilization Thermometer ("Термометр" Утилизации) - показывает текущее значение утилизации сети, а также усредненные за 1 и за 5 мин значения утилизации на индикаторе в виде термометра.

Top Talkers (Наиболее активные станции сети) - показывает распределение трафика по станциям сети. Для каждой станции индицируется процент используемой полосы пропускания сети, полный трафик (число пакетов, пакетов/с, байт, байт/с), трафик, который каждая станция принимает из сети или передает в сеть (число пакетов, байт), широковещательный и групповой трафик (число пакетов, пакетов/с).

Pair Statistics (Matrix) (Статистика по Парам станций) - отслеживает все взаимодействующие друг с другом пары станций. При отображении информации в виде Графической Матрицы (Graphical Matrix), обмен данными между взаимодействующими станциями отображается на диаграмме линиями, толщина которых отражает объем трафика, проходящего между взаимодействующими станциями.

Network Activity Display (Экран Сетевой Активности) - отображается информация о текущем числе широковещательных и групповых пакетов в общем сетевом трафике, а также информация о текущей утилизации сети. Этот экран может моментально показать Вам "здоровье" сети и предупредить о возможных замедлениях в её работе, вследствие широковещательного или группового шторма. Для большей наглядности при отображении информации используется цветовое кодирование графиков.

Vital Sign Display (Жизненно-важные показатели работы сети) - отображается число ошибок для сетей типа Ethernet или Token Ring.

Ethernet - отображаются ошибки CRC, ошибки выравнивания, слишком большие и слишком маленькие пакеты, коллизии.

Token Ring - отображаются 28 ошибок MAC-уровня (ошибки монитора при использовании технологии RMON не поддерживаются).

Экраны пакета Observer, на которых отображаются данные, собираемые RMON2-зондами

Packet Capture & Decode (Захват и декодирование пакетов) - декодирует все основные протоколы и субпротоколы (поддерживаются более 300 протоколов).

Filters (Фильтры) - предоставляется доступ к библиотеке фильтров по протоколам и смещениям; возможно задание смещений пользователем с установкой до 20 смещений одновременно.

Protocol Statistics (Распределение трафика по протоколам) - предоставляется информация о распределении трафика по различным протоколами и субпротоколами в табличном или графическом формате. Показывается, как используется полоса пропускания Вашей сети. Выделяются "неожиданные" протоколы, обусловленные неправильной конфигурацией системы.

Web Observer (Наблюдения за Web-сервером) - отображается трафик, идущий к WWW-серверу и от него. Отображаются адреса станций сети, которые обращаются к WWW- серверу, объем трафика (в % от общего объема), генерируемый каждой станцией сети.

Router Observer (Наблюдения за маршрутизатором) - позволяет Вам наблюдать на трафиком какого-то конкретного устройства сети (обычно маршрутизатора). Этот режим позволяет Вам увидеть, как используется данное устройство, какова утилизация его внешнего интерфейса (например, T1-соединения). На стрелочных индикаторах выдается информация о трафике, выраженная в пакетах/сек. и в бит/сек., а также утилизация внешнего интерфейса в %. Кроме текущей утилизации интерфейса, индицируется ее усредненное значение за 1 мин и 1 час.

Triggers & Alarms (Триггеры и предупреждения) - позволяет автоматически зафиксировать возникновение конкретных ситуаций в сети и информировать об этих ситуациях администратора. Возможно использование как предопределенных, так и определяемых пользователем триггеров. Каждый триггер может вызывать связанное с ним действие: выпадающие окна сообщений, запись/добавление записи в журнал, печать сообщения о срабатывания триггера (printing trouble tickets), выполнение внешней программы, посылка сообщения по электронной почте или пейджеру.

Discover Network Names (Поиск сетевых имен) - находит все сетевые MAC- адреса, хранит их в таблице и автоматически присваивает им псевдонимы, в качестве которых используются адреса IP, имена DNS. Возможен также ввод имен из SNA, AppleTalk, DECnet и др.

RMON Table (Таблица RMON) - отображаются все данные RMON1/2 в табличном формате, - точно так, как они хранятся в RMON-зонде.

Поддержка RFC

RMON-Расширение для пакета Observer полностью поддерживает рекомендации RMON RFC, включая RFC 1757 (RMON1 Draft Standart - Ethernet), RFC 1513 (Token Ring RMON Extensions), RFC 2021 (RMON2) и RFC 2074 (Protocol Identifiers).

Системные требования, предъявляемые RMON-расширением

***Минимально**:* Pentium 400 с объемом оперативной памяти 128 Мб, Windows 98 или более поздняя версия, поддерживаемый сетевой адаптер, мышь, монитор SVGA при разрешении не ниже 1024x768; лицензионная версия Observer 8.0.

Рекомендуется: Pentium 600 с объемом оперативной памяти 256 Мб, Windows 2000/XP, поддерживаемый сетевой адаптер, мышь, монитор SVGA при разрешении не ниже 1280x1024; лицензионная версия Observer 8.0.

Лицензирование: действие лицензии на RMON-Расширение распространяется только на один компьютер с установленным пакетом Observer, расположенный в одном месте одной локальной сети. Если RMON-Расширение требуется устанавливать на ноутбуке с установленным пакетом Observer, то для каждого ноутбука требуется отдельная лицензия на RMON-Расширение и Observer

Системные требования, предъявляемые Advanced- и RMON-зондами

***Минимально**:* Pentium 166 с объемом оперативной памяти 64 Мб, Windows 98 и поддерживаемый сетевой адаптер.

Поддерживаемые платформы: Windows 98/ME и Windows NT 4.x (Server или Workstation) или Windows 2000/XP.

Поддерживаемые топологии: Ethernet (10/100) и Token Ring (4/16).

Требования к коммутаторам (только для Advanced-зондов): коммутаторы должны поддерживать "зеркалирование" портов (Port Mirroring), а также должны иметь управляющий Telnet- или SNMP-интерфейс для контроля за "зеркалированием" портов.

Поддерживаемые сетевые адаптеры: Любые сетевые адаптеры с драйверами NDIS 5.x/4.x/3.x, поддерживающие режим PROMISCUOUS MODE (Режим, в котором сетевой адаптер обнаруживает в сети все фреймы вне зависимости от их конечного адреса).

Лицензирование: действие лицензии на RMON-зонд распространяется только на один компьютер, расположенный в одном месте одной локальной сети. Если RMON-зонд требуется устанавливать на ноутбуке, то для каждого ноутбука требуется отдельная лицензия на RMON-зонд.

SNMP Extension (SNMP-Расширение)

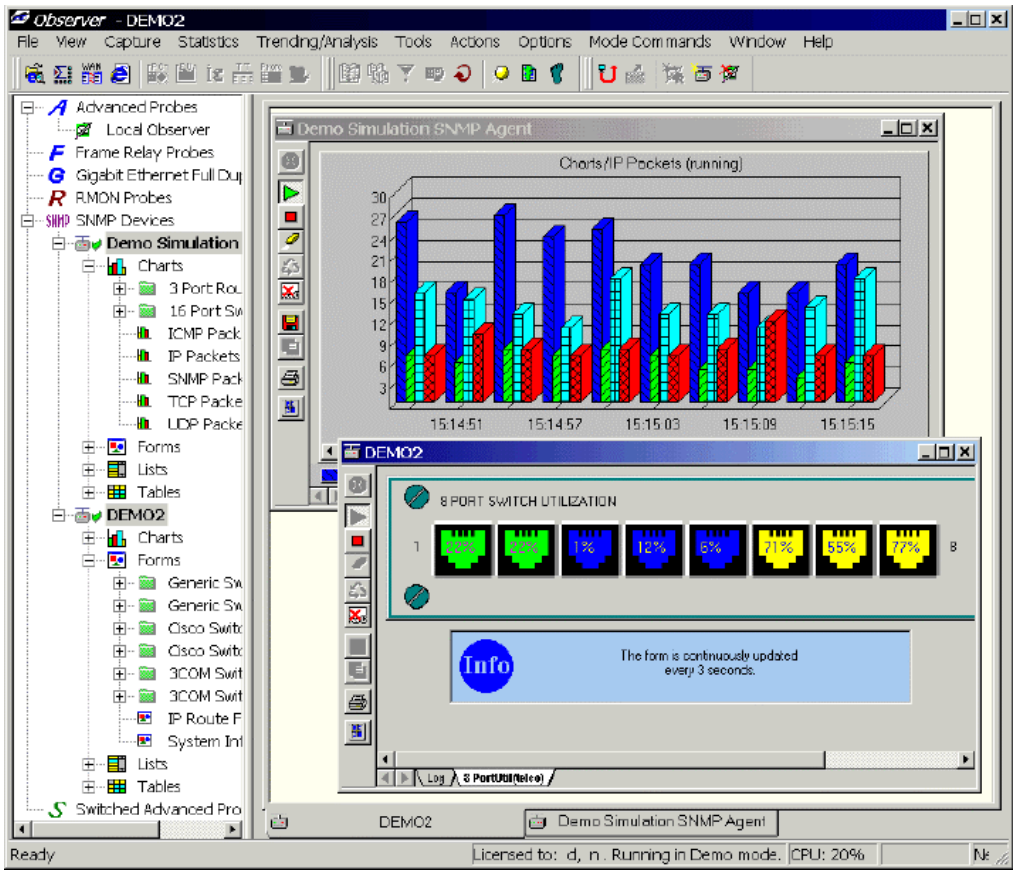
Исторически существуют две технологии для диагностики и управления сетями. Первая - это анализаторы сетевых протоколов. Вторая - это системы управления оборудованием на базе протокола SNMP. Каждая из этих технологий имеет свои достоинства и недостатки.

Теперь Вам больше не нужно выбирать между этими альтернативными технологиями. Вы можете получить в свое распоряжение одно средство, которое сочетает в себе функциональность анализатора сетевых протоколов и системы мониторинга и управления сетевыми устройствами на базе SNMP. Это средство, которое уникально по сочетанию своих функциональных возможностей и легкости в использовании, называется - пакет Observer с SNMP-Расширением.

SNMP-Расширение дополняет функциональные возможности пакета Observer всеми возможностями, предоставляемыми SNMP-технологиями. При наличии данного расширения, становятся доступны все возможности протокола SNMP по управлению и анализу работы активного сетевого оборудования. При этом вся работа с SNMP-устройствами осуществляется с помощью интерфейса пакета Observer.

Дополнив пакет Observer SNMP-Расширением Вы, фактически, получаете несколько инструментов:

- Полноценную консоль SNMP-управления.
- Полноценную утилиту для конфигурирования маршрутизаторов, коммутаторов или любых других устройств, совместимых с SNMP.
- Единое средство управления сетями, в которых используется оборудование от различных производителей.
- Удаленную консоль для SNMP-устройств, расположенных в любом месте Вашей локальной или глобальной сети, либо подключаемых через Internet.
- Консоль "трап-сообщений" для отслеживания критических событий на SNMP-устройствах.
- Компилятор MIB, позволяющий поддерживать любые SNMP-устройства.



Исторически анализаторы протоколов, в том числе и Observer, разрабатывались с целью мониторинга сетевого трафика. В то же время протокол SNMP стал стандартом для мониторинга сетевых устройств. Протокол SNMP позволяет гибко и эффективно собирать и представлять информацию, требуемую для оптимизации работы сетевых устройств. Использование пакета Observer с SNMP-Расширением позволяет решать обе эти задачи.

SNMP-Расширение позволяет не только считывать значения SNMP-объектов, но и присваивать им новые значения (при условии, что они доступны для записи). Благодаря этому, администратор может контролировать состояние устройств, изменять параметры их настройки.

SNMP является промышленным стандартом, что дает администратору сети, использующему Observer и SNMP-Расширением, уверенность в том, что данное техническое решение будет совместимо с современными и будущими средствами управления сетями.

SNMP-Расширение предлагает широкий выбор средств генерации отчетов: разнообразные диаграммы, таблицы, списки и графические объекты (формы). Полностью поддерживаются сообщения о ловушках (трап-сообщения) с различными вариантами реакций (действий, которые будет выполнять программа при поступлении трап-сообщения). В комплект поставки входит компилятор MIB, позволяющий работать с MIB различных производителей. При этом поддерживается, как SNMPv1, так и SNMPv2.

Зачем нужно использовать SNMP?

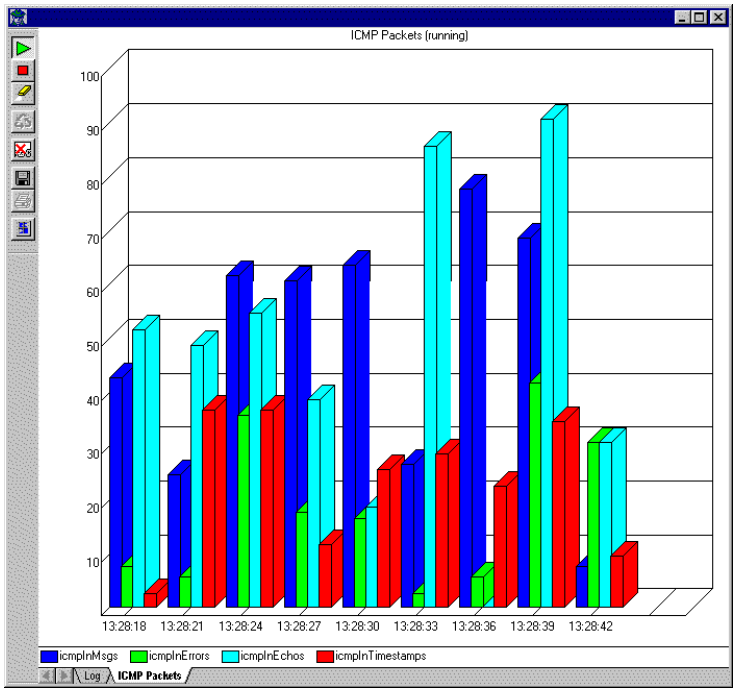
SNMP позволяет администратору сети получать такие данные о сетевых устройствах, которые невозможно получить другими средствами. SNMP-данные, обычно, специфичны для каждого типа устройства. Например, для маршрутизатора важными контролируемыми параметрами являются данные о сетевом трафике: число и тип пакетов, переданных из одной сети в другую, утилизация каждого интерфейса, число ошибок передачи данных. Для сетевого принтера важной является совершенно другая информация, например, информация о числе заданий на печать, состоянии принтера ("нет бумаги", "загрузка данных" и т.д.).

SNMP был разработан для того, чтобы собирать информацию от SNMP-агентов, представлять эту информацию в упорядоченном виде и передавать ее управляющей станции по протоколу SNMP. SNMP-Расширение позволяет эффективно собирать SNMP-данные и отображать их в графическом виде, причем процесс сбора и отображения данных интегрирован со стандартными функциями пакета Observer.

Управление сетью на основе SNMP

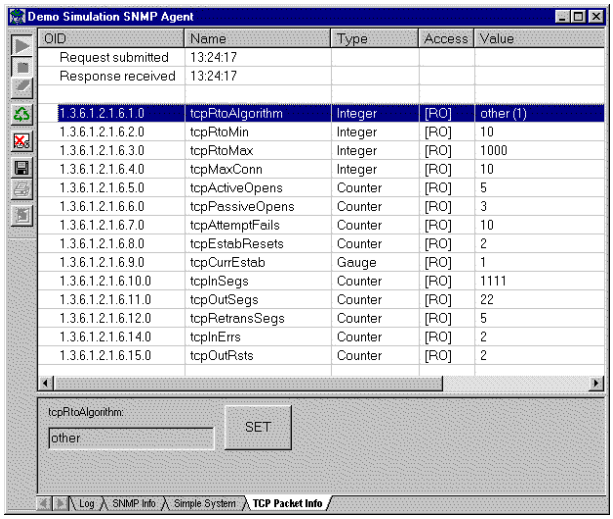
SNMP-Расширение не только позволит Вам собирать информацию с SNMP-агентов, размещенных на различных сетевых устройствах, но и предоставит возможность устанавливать новые значения SNMP-объектам (если они доступны для записи). Это позволит Вам изменять конфигурацию сетевых устройств непосредственно из оболочки пакета Observer. Благодаря данной возможности, Вы легко сможете, например, изменить направление подачи бумаги в сетевом принтере, значение таймаута в Вашем коммутаторе и т.д.

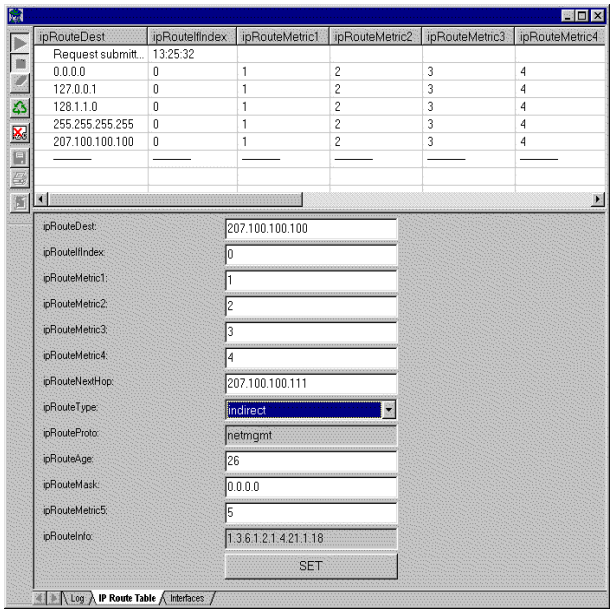
SNMP - диаграммы



SNMP-диаграммы предназначены для визуализации данных, которые интересно наблюдать "во времени". В этом режиме графически отображаются приращения значений SNMP-объектов относительно их предыдущего значения. Конфигурирование диаграмм осуществляется очень просто - путем "перетаскивания" SNMP-объекта из таблицы MIB на панель запросов диаграммы. Диаграммы можно отображать в двухмерном или трехмерном виде, в виде круговой или линейной диаграммы. Диаграммы можно распечатывать в том виде, в каком они отображаются на мониторе или сохранять в файле формате CSV, (значения, разделяемые запятыми). Период обновления информации на диаграмме можно изменять.

SNMP - списки и таблицы



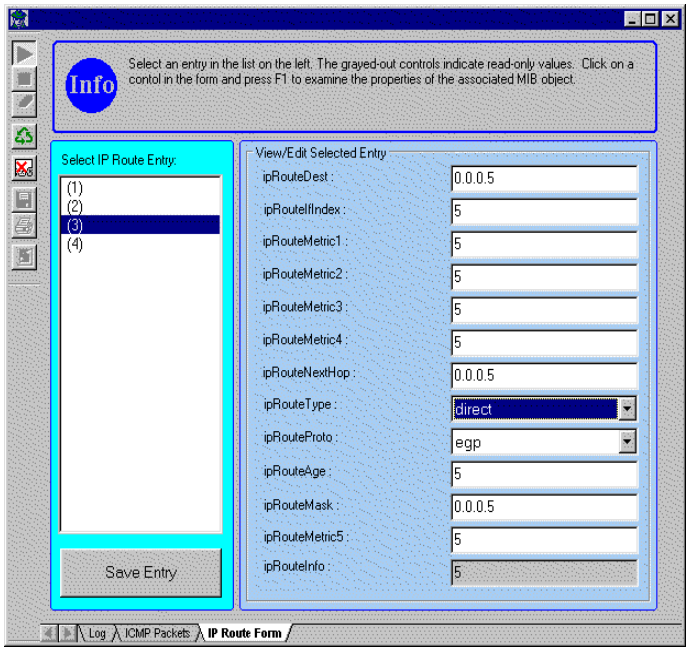


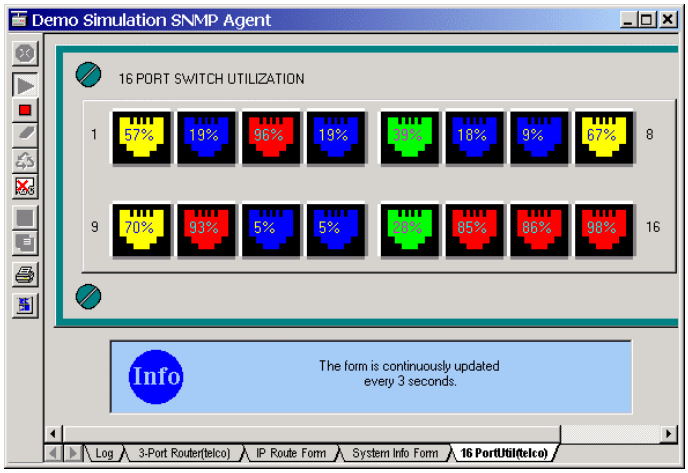
Для просмотра статических, т.е. не зависящих от времени данных, в SNMP-Расширении предусмотрены SNMP-списки и SNMP-таблицы.

В виде списков удобно отображать информацию об устройстве, которая характеризуется зависимостью: "метка" - "значение". Пример такого рода информации: метка - "IP-адрес", значение "200.200.200.10". В виде таблиц удобнее отображать информацию, которая характеризуется зависимостью "метка" - "совокупность значений". Пример такого рода информации: метка - "Текущие соединения", совокупность значений - "Список текущих соединений".

В каждом из этих двух представлений можно изменять значения тех SNMP-объектов, которые доступны для записи. Для этого Вам нужно лишь выделить данный объект и ввести или выбрать из списка его новое значение.

SNMP - формы





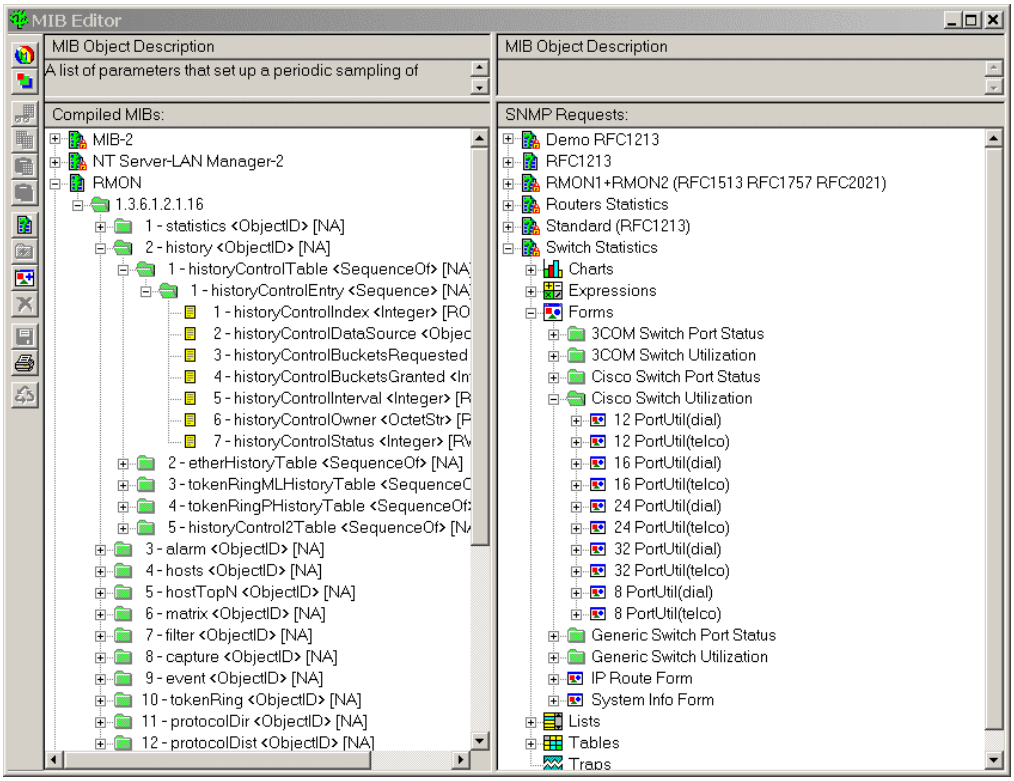
SNMP-Расширение предоставляет возможность отобразить SNMP-данные в графическом виде. При этом графические возможности по отображению данных ограничены лишь Вашим воображением. В программу уже встроены разнообразные изображения маршрутизаторов, коммутаторов и концентраторов, так что Вы можете, например, отображать состояние портов (включен/выключен) различных устройств конкретным цветом.

Для изменения таблиц маршрутизации или статуса соединения с web-сервером предусмотрены простые формы с многовариантным выбором. Благодаря встроенным инструментам для рисования и манипуляции растровыми изображениями, возможности отображения информации в SNMP-формах становятся практически безграничными. Так же, как в случае списков и таблиц, в SNMP-формах Вы можете изменять значения объектов.

SNMP - ловушки

SNMP-Расширение предоставляет все возможности для работы с, так называемыми SNMP-ловушками (трап-сообщениями). Типы ловушек выбираются из MIB контролируемого устройства или сервера, а связанные с ними действия определяются в процессе конфигурирования SNMP-ловушки. Такими действиями могут быть: запись сообщения в журнал событий, вывод информации во всплывающем окне, вывод сообщения на печать, отправка сообщения или даже всего журнала событий по электронной почте, отправка сообщения по пейджеру, пересылка трап-сообщения на другую станцию управления.

Поддержка MIB



В SNMP-Расширение уже встроена поддержка MIB-2 (RFC1213) и SNMP-агентов, инсталлируемых на большинстве систем и устройств, работающих под управлением UNIX, NT и NetWare. Кроме того, SNMP-Расширение позволяет Вам инсталлировать и компилировать определения частных MIB для SNMP-агентов различных производителей. Процесс компиляции MIB и построения запросов к устройствам осуществляется с помощью простого в использовании интерфейса на основе "перетаскивания" объектов (drag and drop). SNMP-запросы (диаграммы, списки, таблицы, формы, ловушки) имеют файловую структуру, поэтому они могут использоваться совместно несколькими пользователями SNMP-Расширения.

Системные требования, предъявляемые SNMP-Расширением

***Минимально**:* Pentium 400 с объемом оперативной памяти 128 Мб, Windows 98 или более поздняя версия, поддерживаемый сетевой адаптер, мышь, монитор SVGA при разрешении не ниже 1024x768; лицензионная версия Observer 8.0.

Рекомендуется: Pentium 600 с объемом оперативной памяти 256 Мб, Windows 2000/XP, поддерживаемый сетевой адаптер, мышь, монитор SVGA при разрешении не ниже 1280x1024; лицензионная версия Observer 8.0.

Лицензирование: действие лицензии на RMON-Расширение распространяется только на один компьютер с установленным пакетом Observer, расположенный в одном месте одной локальной сети. Если RMON-Расширение требуется устанавливать на ноутбуке с установленным пакетом Observer, то для каждого ноутбука требуется отдельная лицензия на RMON-Расширение и Observer.

WEB Extension (WEB-Расширение)

Вы администратор сети и в любой момент времени, где бы Вы ни находились (дома, в командировке или даже в отпуске), должны знать, как работает ваша сеть. Теперь у Вас есть такая возможность. К функциональности анализатора сетевых протоколов и монитора сети **Observer** добавлены новые возможности для работы с Internet-технологиями! Эти возможности предоставляет WEB-Расширение пакета Observer.

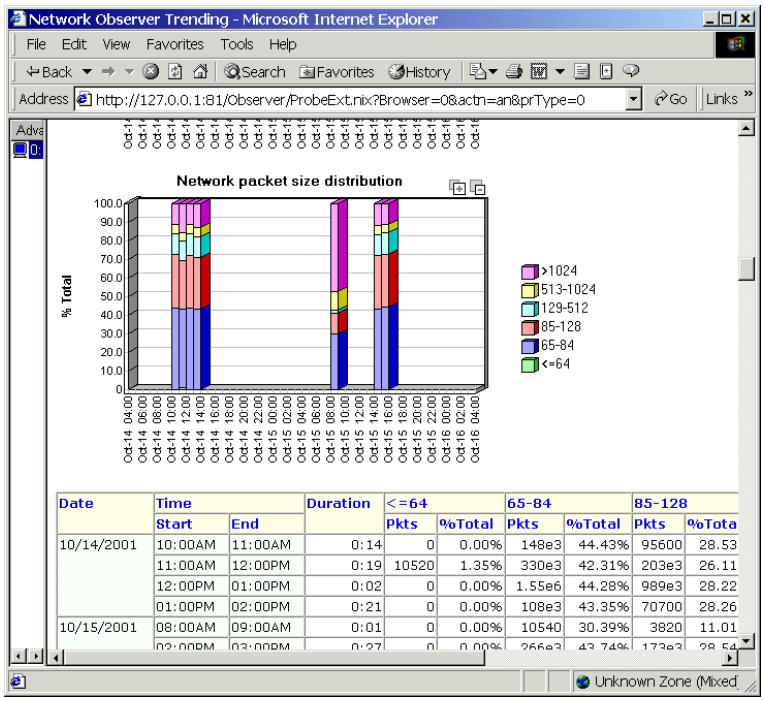
Сочетая функциональность пакета Observer с доступностью Internet, WEB-Расширение является идеальным дополнением для пакета Observer. Если в вашей организации несколько локальных сетей, но отсутствуют специальные корпоративные каналы связи между ними, то с помощью WEB-Расширения вы можете контролировать работу каждой локальной сети через Internet.

WEB-Расширение пакета Observer позволяет контролировать работу сети с помощью WEB-браузера. Теперь статистика о работе Вашей сети может быть доступна с любого компьютера, на котором установлен WEB-браузер. Все, что Вам для этого необходимо - это соединение с Internet или Intranet-сетью Вашей компании.

WEB-Расширение функционирует во взаимодействии с пакетом Observer. Для его функционирования не требуется наличие WEB-серверов, так как уже имеется встроенный WEB-сервер.

При наличии пакета Observer и WEB-Расширения Вы сможете:

- Создавать отчеты об использовании сетевых ресурсов Вашей корпоративной сети (типа Intranet/Extranet).
- Предоставлять пользователям, не имеющим доступа к пакету Observer, контролируемый доступ к основным данным, о функционировании Вашей локальной или глобальной сети.
- Иметь доступ к информации о работе сети из любого места (например, из дома), с помощью любого WEB - браузера.
- Просматривать статистику в реальном времени с дискретностью в 1 минуту и более.
- Устанавливать уровни безопасности при доступе к информации, при многоуровневой системе защиты.



Date	Time		Duration	<=64		65-84		85-128	
	Start	End		Pkts	%Total	Pkts	%Total	Pkts	%Tota
10/14/2001	10:00AM	11:00AM	0:14	0	0.00%	148e3	44.43%	95600	28.53
	11:00AM	12:00PM	0:19	10520	1.35%	330e3	42.31%	203e3	26.11
	12:00PM	01:00PM	0:02	0	0.00%	1.55e6	44.28%	989e3	28.22
	01:00PM	02:00PM	0:21	0	0.00%	108e3	43.35%	70700	28.26
10/15/2001	08:00AM	09:00AM	0:01	0	0.00%	10540	30.39%	3820	11.01

Обзор возможностей

Установив WEB-Расширение, вы сможете получить доступ к полному набору данных, необходимых для анализа производительности и исправности сети, с любой платформы, поддерживающей Web-браузер. Данная информация собирается пакетом Observer, а отчеты генерируются динамически по запросам любого WEB-браузера. Информация представляется в наглядной форме с использованием графиков, диаграмм и текстовой информации. Вы сами можете настраивать частоту обновления информации, при этом минимальный интервал может составлять одну минуту. Вы можете просматривать данные, усредненные по времени, по станциям, а также по тому и другому одновременно.

Можно установить опции просмотра такими, чтобы просматривать статистику о работе сети за один день, несколько дней, недель, месяцев и более.

Можно получать информацию о работе конкретных станций или серверов сети с целью определения того, как они работают сейчас и как они работают в течение длительного периода времени. Собранную статистическую информацию можно сравнивать с информацией, которая получена ранее за такой же промежуток времени. Например, Вы можете сравнить загрузку сети и число ошибок в сети за январь и декабрь прошлого года. Это позволит выявить тенденцию (тренд) увеличения загруженности сети, тенденцию увеличения числа ошибок в сети и т.п.

Администратор сети полностью контролирует доступ к информации о работе сети. Администратор может задавать, какие именно отчеты и типы статистики разрешено предоставлять для внешнего просмотра. Кроме этого, он может устанавливать пароли на доступ к информации. Такая гибкая система безопасности позволяет администратору сети, разрешать, например, внешнему консультанту просматривать сетевой трафик и информацию об ошибках, не допуская при этом консультанта к возможностям захвата и декодирования пакетов, чтобы сохранить в тайне важную для компании информацию (пароли, имена пользователей, информацию о счетах и т.д.).

Доступные типы статистики

Приведенные ниже типы статистики можно получать, как по конкретным станциям сети, так и по всей сети в целом. Поддерживаются сети Ethernet, Token Ring, FDDI; данные отображаются по каждому сегменту сети, где установлен Зонд.

Вы сможете организовать автоматический сбор данных с Зондов, установленных в различных сегментах сети на WEB-консоль пакета Observer, в заданные интервалы времени. Это позволяет получать информацию о функционировании различных сегментов сети (собираемую Зондами) из любого места Вашей локальной или глобальной сети, где имеется WEB-браузер.

Обзор доступных типов статистики:

Network Activity Summary (Активность сети) - показывает, кто в настоящий момент подключен к данной локальной сети, а также время первого и последнего подключения каждого пользователя к сети.

Network Top Talkers (Наиболее активные станции сети) - предоставляет информацию о пользователях, наиболее активно использующих ресурсы сети. Дает информацию по всем станциям сети, или только по наиболее активным "XX" станциям сети.

Network Packet Size Distribution (Распределение пакетов в сети по размерам) - статистика распределения пакетов по размерам.

Network Protocol Distribution (Распределение пакетов в сети по протоколам) - статистика распределения пакетов по протоколам.

Network IP Group Protocol Distribution (Распределение пакетов в сети по IP-субпротоколам) - статистика распределения пакетов по основным IP-субпротоколам (TCP, UDP, ICMP, ARP, RARP, IP и др.).

Network IP Application Protocol Distribution (Распределение пакетов в сети по IP-приложениям) - статистика распределения пакетов по основным IP-приложениям (Telnet, POP, HTTP и др.). Могут быть добавлены и другие, определяемые пользователями, приложения.

Network IPX Subprotocol Distribution (Распределение пакетов в сети по IPX-субпротоколам) - статистика распределения пакетов по основным IPX-субпротоколам.

Network Error Distribution (Распределение ошибок в сети) - статистика распределения ошибок в сети по типам.

Station Error Distribution (Распределение ошибок в сети по станциям) - статистика распределения ошибок в сети по станциям.

Router Statistics (Статистика маршрутизатора) -статистика загруженности маршрутизатора.

Системные требования, предъявляемые WEB-Расширением

Минимально: Pentium 400 с объемом оперативной памяти 128 Мб, Windows 98 или более поздняя версия, поддерживаемый сетевой адаптер, мышь, монитор SVGA при разрешении не ниже 1024x768; лицензионная версия Observer 8.0.

Рекомендуется: Pentium 600 с объемом оперативной памяти 256 Мб, Windows 2000/XP, поддерживаемый сетевой адаптер, мышь, монитор SVGA при разрешении не ниже 1280x1024; лицензионная версия Observer 8.0.

Лицензирование: действие лицензии на WEB-Расширение распространяется только на один компьютер с установленным пакетом Observer, расположенный в одном месте одной локальной сети. Число клиентов, обращающихся к серверу, на котором установлено WEB-Расширение, не ограничено.

Добавьте к функциональности Observer широкие возможности Internet / Intranet технологий!

Новые возможности

Новые возможности Observer

Пакет Observer 8 включает в себя следующие новые возможности.

- Совместимость с Windows XP
- Новое интуитивно понятное меню с функциональным разделением – основные пункты меню теперь сгруппированы исходя из удобства решения наиболее часто встречающихся задач.
- Увеличена область просмотра. Для улучшения условий просмотра и доступа к информации кнопки на боковом меню заменены на закладки в стиле папок.
- Новое графическое представление данных в виде трехмерных графиков и трехмерных секторных диаграмм с возможностью детализации информации по ключевым показателям.
- Распределение по Протоколам (Protocol Distribution) представлено в виде иерархической структуры с возможностью динамического добавления различных типов протоколов.
- Новые возможности фильтрации пакетов:
  - Комбинированные фильтры первого (MAC) и третьего (IP) уровней;
  - Фильтрация IPv6;
  - Разным типам фильтров теперь соответствуют разные иконки;
  - Фильтрация по IP-адресам с возможностью задания диапазонов адресов, исключения определенных диапазонов адресов и использования групповых символов;
  - Количество одновременно используемых фильтров адресов увеличено с 5 до 10;
  - Фильтры адресов Frame Relay.
- Новый модуль просмотра отчетов с Web-интерфейсом, позволяющий быстро изменять масштаб для отображения данных на больших и малых интервалах времени.
- Новые современные средства отображения трехмерных графиков.
- Многоуровневые всплывающие подсказки, обеспечивающие более подробные пояснения к различным элементам интерфейса.
- Дерево Зондов/Агентов (Probe/Agent Tree), отображающее Зонды и SNMP-агенты в виде стандартной для Windows древовидной структуры.
- Настраиваемый порядок столбцов и различные настройки отображения в окнах декодирования.

- Модуль Захвата Пакетов (Packet Capture) теперь дает возможность устанавливать относительные временные отметки.
- Ярлыки "быстрой" навигации по окну декодирования.
- Новые усовершенствованные круговые индикаторы.
- Поддержка декодирования большого количества дополнительных протоколов, включая: MGCP/Megaco, SLP, SQL/TDS, SIP, SDP, RRC 2975 SAP, PPPoE, Xerox XNS/IDP, TNS (Oracle), OSI/CLNP, OSI/Inactive Network, OSI/ISIS, Radius, RSVP, MPLS, CLNS, Frame Relay/Q.931 <Anex D/LMI>, Frame Relay/ISO8885, Frame Relay/Q922, VoIP Codec G729A (Nortel) и многих других. Помимо этого, теперь есть возможность распознавания более 4000 типов фреймов.
- Полное декодирование трафика баз данных SQL.
- Описания, имеющиеся в скомпилированных MIB, теперь отображаются в окне декодирования. Компакт-диск Observer содержит большую библиотеку скомпилированных MIB.
- Возможность чтения и сохранения данных в формате Sniffer (файлы *.cap).
- Функция Protocol Forcing позволяет осуществлять выбор стартовых точек декодирования в заголовках пакетов (могут быть установлены до 8 стартовых точек).
- Сохраненные файлы результатов работы модуля захвата пакетов теперь проассоциированы с приложением Observer, что позволяет открывать их двойным щелчком мыши.
- Компонент Router Observer теперь может наблюдать одновременно за 8 маршрутизаторами (в предыдущих версиях – только за 1).
- Компонент Web Observer теперь может наблюдать одновременно за 8 Web-серверами (в предыдущих версиях – только за 1).
- Анализ тенденций (Trending) теперь поддерживает 8 маршрутизаторов и 8 Web-серверов.
- Тесная интеграция с XML.

Новые возможности Expert Observer

Expert Observer помимо перечисленных выше новых функций Observer, включает в себя следующие возможности:

- Новая функция отображения событий и проблемных ситуаций для IPX/SPX, NetBIOS/NetBEUI, Frame Relay и SQL.
- Количество событий, идентифицирующих сетевые проблемы увеличилось более чем на 30%.
- Функция WAN compare capture, используя технологию временной синхронизации, позволяет определять причины задержек, возникающих в глобальных сетях связи. Expert Observer теперь позволяет осуществлять захват на обоих концах глобальной линии связи и определять время отклика (Response Time). Измерение времени прохождения транзакции между рабочей станцией и сервером производится с помощью эксклюзивного метода синхронизированных захватов (Synchronizing Captures) компании Network Instruments. Данная функция может пригодиться в первую очередь большим компаниям, а также сетевым специалистам, обеспечивающим функционирование большого количества глобальных линий связи, которые раннее для этой цели были вынуждены приобретать чрезвычайно дорогостоящее синхронизирующее оборудование. Например, крупная компания, имеющая сеть розничной торговли, может использовать данную функцию для отслеживания и анализа времени прохождения транзакций между торговыми филиалами и сервером в центральном офисе.

Новые возможности Observer Suite

Observer Suite помимо перечисленных выше новых функций Expert Observer, включает в себя следующие возможности:

- Средства отображения SNMP отчетов с Web-интерфейсом, включающие в себя временные шкалы с удобными средствами масштабирования.
- Новые трехмерные средства отображения SNMP трендов.
- Линии привязок к шкале времени на всех SNMP графиках, позволяющие точно определить время возникновения каждого события.
- Новая функция RMON get-multiple.