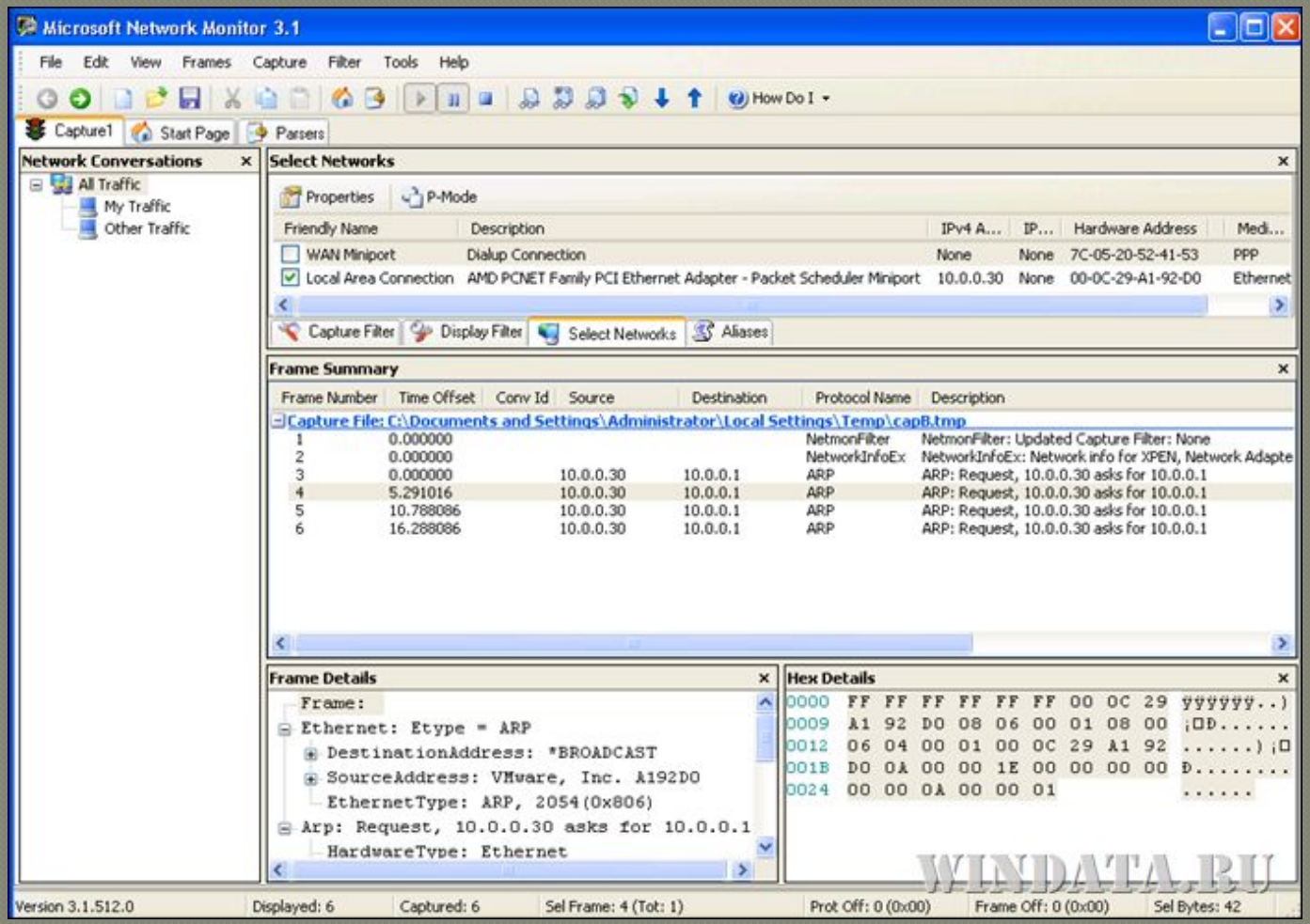
Сетевой монитор

Принцип работы
Триггеры
Фильтрация

Network Monitor (Сетевой монитор) является инструментом, предназначенным для администратора. Утилита ***Network Monitor*** позволяет перехватывать и анализировать сетевые пакеты, а так же просматривать статистику данных, передаваемых в локальной подсети компьютера, на котором выполняется программа.



Использование сетевого монитора позволяет собирать сведения, обеспечивающие бесперебойную работу, начиная от определения шаблона до предотвращения и устранения неполадок. Сетевой монитор предоставляет сведения о трафике сетевого адаптера того компьютера, на котором он установлен. Сбор и анализ этих сведений позволяет предотвращать, диагностировать и устранять сетевые неполадки различных типов.

Можно настроить сетевой монитор для предоставления конкретных наиболее важных сведений. Например, можно так установить триггеры, что сетевой монитор будет начинать и завершать сбор сведений при соблюдении определенного условия или набора условий. Также можно установить фильтры для контроля за типом собираемых и отображаемых сетевым монитором сведений. Для облегчения анализа сведений можно изменить способ отображения данных на экране, а также сохранить или распечатать данные, чтобы просмотреть их позднее.

С помощью компонента Сетевой монитор, включенного в операционные системы ***Microsoft Windows Server 2003***, можно собирать данные, отправленные или полученные с компьютера, на котором установлен сетевой монитор. Для сбора данных, посылаемых или получаемых с удаленного компьютера, необходимо использовать компонент Сетевой монитор, входящий в ***Microsoft Systems Management Server (SMS)***, с помощью которого можно собирать данные, посылаемые или получаемые с любого компьютера, на котором установлен драйвер сетевого монитора.

Принцип работы

Данные, пересылаемые по сети, делятся на кадры. В каждом таком кадре содержатся следующие сведения:

- Адрес источника. Адрес сетевого адаптера, с которого поступил кадр.
- Адрес назначения. Адрес сетевого адаптера, которому предназначался кадр. Этот адрес может также определять группу сетевых адаптеров.
- Данные заголовка. Данные для каждого протокола, используемого при передаче кадра.
- Данные. Передаваемые данные (или часть данных).

Каждый компьютер сегмента сети получает кадры, отправленные данному сегменту. Сетевой адаптер каждого компьютера сохраняет и обрабатывает только адресованные данному адаптеру кадры. Остальные кадры отбрасываются и больше не обрабатываются. Сетевой адаптер также сохраняет широковещательные (и, потенциально, многоадресные) кадры.

Принцип работы

После установки программы сетевого монитора можно записать в файл все кадры, отправленные сетевому адаптеру данного компьютера, или сохраненные им. Записанные кадры можно просмотреть или сохранить для дальнейшего анализа. Программа позволяет задать фильтр записи, разрешающий запись только определенных кадров. В этом случае запись кадров будет производиться на таких условиях, как адрес источника, адрес назначения или протокол. Сетевой монитор также дает возможность пользователям разработать триггер записи для запуска определенных действий при обнаружении им в сети конкретного набора условий. Такими действиями могут быть запуск записи, конец записи или запуск программы.

По умолчанию размер буфера записи равен 1 МБ. Размер данных можно уменьшить, уменьшив размер буфера записи.

Запись данных

Процесс копирования пакетов сетевым монитором называется записью. Можно записывать как весь сетевой трафик локального сетевого адаптера, так и отдельные наборы пакетов с помощью фильтров записи. Можно также задать набор условий для триггеров событий. После создания триггеров сетевой монитор может отвечать на события в сети. Например, операционная система может запустить исполняемый файл, если сетевой монитор обнаруживает в сети выполнение определенного набора условий. После записи данных их можно просмотреть. Сетевой монитор преобразует исходные данные в соответствии с логической структурой пакета.

Сетевой монитор копирует передаваемые по сети пакеты с требуемыми характеристиками в буфер записи с помощью спецификации NDIS.

Запись данных

При записи кадров сетевым монитором сведения о кадрах отображаются в окне записи данных, разделенном на четыре панели.

Панель	Значение
График	Графическое представление кадров, отправленных на локальный компьютер или с локального компьютера.
Статистика сеанса	Сведения о каждом отдельном сеансе.
Статистика станции	Сведения о кадрах, отправленных на локальный компьютер или с локального компьютера, на котором запущен сетевой монитор.
Общая статистика	Обобщенные сведения о кадрах, отправленных на локальный компьютер или с локального компьютера после начала процесса записи.

Фильтры записи
Создание фильтров записи

Фильтр записи работает как запрос базы данных, который используется для указания типов пакетов, передаваемых по сети, которые планируется записывать для последующего анализа. Например, для сбора данных, относящихся к определенному подмножеству компьютеров или протоколов, следует подготовить базу данных адресов, использовать эту базу для создания фильтра записи, а затем сохранить этот фильтр в файле. В дальнейшем при необходимости этот файл можно загружать для работы с фильтром. Использование фильтра позволяет сэкономить время и память буфера записи.

Чтобы создать фильтр записи, следует выбрать критерии фильтрации в диалоговом окне Фильтр записи. В этом диалоговом окне отображается дерево критериев, которое является графическим представлением логики фильтра. При каждом добавлении или исключении компонентов спецификации записи эти изменения отражаются в дереве критериев.

Фильтры записи
Фильтрация на основе протоколов

Для записи пакетов, передаваемых по сети с использованием конкретного протокола, необходимо указать этот протокол в строке ***SAP/ETYPE=*** дерева критериев. Например, для работы только с пакетами протокола IP сначала следует запретить все протоколы, а после этого разрешить ***IP ETYPE 0x800*** и ***IP SAP 0x6***. По умолчанию все поддерживаемые сетевым монитором протоколы разрешены. Протокол можно указать только с помощью ***ETYPE*** или ***SAP***.

Фильтры записи
Фильтрация на основе адресов

Задайте одну или несколько пар адресов в фильтре записи для сбора данных, посылаемых или получаемых с конкретного компьютера сети. Допускается одновременное наблюдение за четырьмя адресными парами.

Адресная пара состоит из:

- адресов двух компьютеров, за трафиком между которыми ведется наблюдение;
- стрелок, указывающих интересующее направление передачи данных;
- ключевого слова ***INCLUDE*** или ***EXCLUDE***, которое определяет, будет ли сетевой монитор захватывать или игнорировать соответствующие пакеты данных.

Независимо от того, в каком порядке располагаются адресные пары в диалоговом окне Фильтр записи, инструкции ***EXCLUDE*** обрабатываются первыми. Поэтому, если пакет удовлетворяет критериям, указанным в инструкции ***EXCLUDE***, он будет игнорирован независимо от того, присутствует ли в спецификации фильтра инструкции ***INCLUDE*** и ***EXCLUDE***. Сетевой монитор не проверяет, удовлетворяет ли этот пакет условиям инструкций ***INCLUDE***.

Фильтры записи

Фильтрация на основе соответствия шаблону

Указывая шаблон для соответствия в фильтре записи, имеется возможность:

- ограничить запись подмножеством кадров, которые содержат указанный шаблон (его можно задавать в текстовом или шестнадцатеричном виде);
- определить, на каком расстоянии (смещение) от начала или конца кадра должен начаться поиск.

При задании фильтра соответствия шаблону необходимо указать место в кадре, откуда должен начаться поиск соответствия шаблону. Эти настройки определяют расстояние в байтах от начала кадра или от конца заголовка топологии до места совпадения шаблона. Если пакеты не имеют постоянной длины (например пакеты протокола ***MAC*** в сетях ***Ethernet*** или ***Token Ring***), следует указывать смещение от конца заголовка пакета соответствующей топологии.

Триггеры записи
Типы триггеров

После создания триггеров записи сетевой монитор может отвечать на события в сети. По умолчанию условия включения триггера не установлены.

С помощью сетевого монитора можно определить степень заполнения буфера записи и наличие определенного шаблона данных в записанном кадре. Можно создавать триггеры записи на основе одного из этих условий или на основе обоих условий.

Если триггер задан на основе определенного шаблона данных в записанном кадре, то сетевой монитор выполнит определенное действие при обнаружении кадра с нужным шаблоном. Шаблон может быть задан шестнадцатеричной строкой или строкой ASCII. Можно задать триггер на основе определенного шаблона данных в записанном кадре и определенного процента заполнения буфера записи. Также можно задать начало поиска для сетевого монитора: с начала каждого кадра, после заголовка каждого кадра или через несколько байт после любого из этих положений. По умолчанию сетевой монитор выполняет поиск по шаблону для всего кадра.

Триггеры записи
Действия триггера

Можно выбрать одно из следующих действий триггера, которое будет исполняться при выполнении условий триггера.

- Компьютер издает звуковой сигнал.
- Сетевой монитор прекращает запись кадров.
- Выполняется выбранная команда.

Чтобы задать команду, которая запускает программу, введите имя и путь к файлу программы, или нажмите кнопку Обзор и найдите файл программы. Для использования команды MS-DOS, такой как copy, введите CMD /K и затем введите команду.

Спасибо за просмотр

Работу выполнил студент группы 22-КС

Меркулов С.В.