CommView®

Сетевой монитор и анализатор для Microsoft Windows

Руководство пользователя
Версия 6.5

Содержание

Введение

О программе CommView

Программа CommView предназначена для мониторинга сетевой активности путём сбора и последующего анализа пакетов в любой Ethernet-сети.

С помощью CommView вы можете видеть список сетевых соединений, IP-статистику, а также исследовать отдельные пакеты. IP-пакеты декодируются вплоть до самого низкого уровня с полным анализом распространённых протоколов. Предоставляется полный доступ к необработанным данным. Перехваченные пакеты могут быть сохранены в виде файла для последующего анализа, а также экспортированы в другие форматы. Гибкая система фильтров позволяет отбрасывать ненужные вам пакеты или перехватывать только те из них, которые необходимы. Вы можете получать извещения системы сигнализации о таких событиях, как наличие в трафике подозрительных пакетов, появление в сети узлов с нештатными адресами или повышение сетевой нагрузки.

В состав CommView входит модуль VoIP, предназначенный для углубленного анализа, записи и воспроизведения голосовых коммуникаций стандартов SIP и H.323.

CommView - это полезный инструмент для администраторов локальных сетей, специалистов по безопасности, сетевых программистов или для любого желающего наглядно видеть полную картину трафика, проходящего через его компьютер или сегмент локальной сети. Для работы необходим сетевой Ethernet или Wi-Fi адаптер, или стандартный адаптер удалённого доступа (dial-up). CommView выгодно отличает наличие современного декодера протоколов, способного анализировать более ста широко распространенных на сегодняшний день протоколов.

Кроме того, новая технология удалённого мониторинга позволяет пользователям CommView наблюдать сетевой трафик компьютера с установленным на нём CommView Remote Agent, где бы такой компьютер ни был расположен физически. Программа CommView Remote Agent является весьма полезным дополнением CommView.

Что нового

Версия 6.5

- Полностью переработанный декодер протоколов: добавлена поддержка большого количества новых протоколов. Для каждого пакета теперь показывается краткое содержимое.

Версия 6.1

- Поддержка новых операционных систем: Windows Server 2008 32-bit и 64-bit Editions.
- Оптимизировано использование памяти при работе с VoIP-анализатором. Новая версия программы поддерживает большее количество одновременных звонков, в то время как нагрузка на память стала значительно меньше.
- Настраиваемый буфер джиттера для симуляции и оценки качества звука реальных VoIP-звонков.
- Улучшен диалог "Поиск". Теперь поддерживаются направление поиска и возможность поиска в формате Unicode (UTF-8, UTF-16).
- Более гибкие опции дерева декодера: появилась возможность устанавливать количество раскрываемых узлов.
- Другие улучшения и исправления ошибок.

Версия 6.0

- Модуль VoIP для углубленного анализа, записи и воспроизведения голосовых коммуникаций стандартов SIP и H.323.
- Визуальный анализ сессий TCP с графическим отображением диаграмм сессий.
- Визуальный конструктор пакетов, помогающий при создании пакетов в Генераторе Пакетов.

Версия 5.5

- Полная поддержка IPv6 во всей программе (декодирование, фильтры, поиск, предупреждения).
- Поддержка UTF-8 в реконструкции TCP-сессий.
- Возможность повторной "сборки" фрагментированных IP-пакетов.
- Новый вид предупреждений: программа может воспроизвести сообщения вслух с помощью встроенного в Windows механизма речевого воспроизведения текста.
- Некоторые улучшения и настраиваемые опции в задачах декодирования и реконструкции сессий.
- Устранена проблема с утечкой ресурсов в Windows Vista в случае установки значения DPI от 120 и выше, а также проблема с возможным крахом системы при мониторинге dial-up-подключения.

Версия 5.4

- Поддержка Windows Vista.

Версия 5.3

- В реальном времени показываются страны, соответствующие IP-адресам.

- Для большего удобства работы изменен дизайн колонок в закладках "Пакеты" и "Log-файлы". Порядок расположения закладок в главном окне программы теперь можно изменять.
- Возможность открывать множество новых окон из текущего буфера пакетов, что значительно упрощает работу с пакетами при сильной загрузке сети. С буфером теперь можно работать в разных отдельных окнах без риска потерять старые пакеты и без необходимости искать те пакеты, которые находятся вне видимости.
- Улучшенная система предупреждений позволяет вам настраивать текст оповещений по электронной почте.
- Размер окна "Статистика" можно изменять.
- Доработан диалог "Поиск".
- Для наглядности работы с пакетами добавлена возможность включать/выключать лини сетки.
- Некоторые другие улучшения.

Версия 5.1

- Быстрые фильтры, которые позволяют обнаруживать пакеты, передаваемые между MAC- и IP-адресами, а также портами. Эти пакеты отображаются в новом окне.
- Стала возможной фильтрация по имени процесса.
- Обновлен список MAC-адресов производителей сетевого оборудования.
- Добавлена функция автоматического обновления программы.
- Большое количество других исправлений и улучшений.

Версия 5.0

- Для пакетов отображается название программы их принимающей или передающей (функция доступна в Windows NT/2000/XP/2003).
- Временные отметки повышенной точности (до микросекунд; свойство доступно в Windows NT/2000/XP/2003).
- Новый формат log-файлов, компактный, открытый.
- Графические матрицы, представляющие процесс передачи данных между узлами сети.
- Добавлено декодирование MS SQL, LDAP и YMSG. Улучшено декодирование SMB и ICQ.
- Поддержка Windows XP 64-bit Edition на процессорах AMD Opteron и Athlon64.
- Одновременная работа с несколькими Remote Agent.
- Улучшен генератор пакетов в плане удобства использования шаблонов.
- Отчёты в формате HTML теперь могут содержать графику.
- Новые типы предупреждений.
- Снижена загрузка процессора.

Версия 4.1

- Добавлена возможность анализа трафика через логический адаптер обратной связи, то есть пакеты, посылаемые/получаемые на 127.0.0.1 (функция доступна в Windows NT/2000/XP/2003).
- Ведётся список URL, которые были просмотрены.
- Добавлена поддержка протоколов IMAP, NNTP, SSH, TLS.
- Интерфейс с plug-in, позволяющий выполнять декодирование протоколов собственными методами.

- В окне реконструкции TCP-сессии теперь можно разархивировать сжатые GZIP-данные, а также изображения, которые во время HTTP-сессий.
- Окно реконструкции TCP-сессии теперь позволяет переключаться между сессиями разных хостов (в предыдущих версиях программы можно было переключаться между сессиями только двух изначально выбранных хостов).
- Программа будет сообщать об изменениях в списке сетевых адаптеров.
- Функция перехвата пакетов автоматически возобновляется при выходе компьютера из "спящего" режима и режима ожидания.
- Добавлена поддержка адаптеров Token Ring (доступна в Windows 2000/XP/2003).
- Поддержка увеличенных пакетов Ethernet (Jumbo frames).
- Можно получать статистику на основе данных, собранных ранее (в дополнение к статистике реального времени).
- Улучшена функциональность предупреждений. Возможна передача параметров/переменных уже запущенным программам и предупреждающим сообщениям.
- Некоторые другие улучшения.

Версия 4.0

- Предупреждения: программу можно настроить таким образом, чтобы она сообщала об определенных пакетах, неизвестных MAC-адресах и т. д.
- Добавлена поддержка протоколов: DAYTIME, DDNS, H.323 (H.225, Q.850, Q.931, Q.932), HTTPS, NTP, RMCP, RTP/RTCP (G.723, H.261, H.263), SNTP, TIME.
- Многоязычный интерфейс.
- К программе можно подключить пользовательский модуль декодирования протоколов.
- Новые параметры командной строки позволяют запускать программу с указанным набором правил и/или с использованием требуемого адаптера.
- В окне реконструкции TCP-сессии появилась функция "Поиск".
- В генераторе пакетов добавлены шаблоны пакетов TCP, UDP и ICMP.
- Функция "Декодировать как..." позволяет декодировать известные протоколы с использованием нестандартных портов.
- Добавлено несколько настраиваемых опций.

Работа с программойКраткий обзор

Интерфейс программы состоит из пяти закладок, позволяющих просматривать данные и выполнять различные действия с перехваченными пакетами. Чтобы начать сбор пакетов, выберите сетевое устройство из списка на панели управления и нажмите кнопку **Начать захват** или выберите **Файл => Начать захват** из меню. При прохождении сетевого трафика через выбранное устройство CommView начнёт отображать информацию.

Главное меню

Файл

Начать захват/закончить захват – начинает/прекращает сбор пакетов.
Режим удаленного мониторинга – открывает либо скрывает дополнительную панель управления удаленным мониторингом.
Сохранить текущие IP-соединения как… – позволяет сохранить содержимое закладки "**Текущие IP-соединения**" в форматах HTML или CSV.
Сохранить пакеты как… – позволяет сохранить содержимое закладки "**Пакеты**" в нужном формате. Закладка "Log-файлы" предоставляет на выбор несколько форматов сохранения файлов.
Просмотр Log-файлов – открывает окно просмотра Log-файлов.
Просмотр VoIP log-файлов – открывает новое окно просмотра VoIP log-файлов.
Очистить текущие IP-соединения – стирает содержимое таблицы "**Текущие IP-соединения**" (первая закладка).
Очистить буфер пакетов – стирает содержимое буфера программы и 2-й закладки (список пакетов).
Очистить данные VoIP – стирает содержимое закладки VoIP.
Производительность – отображает производительность программы: количество успешно перехваченных и пропущенных драйвером пакетов.
Выход – выход из программы.

Поиск

Найти пакет – вызывает диалог поиска пакета, который позволяет найти пакет, содержащий определённый текст.
Перейти к пакету с номером… - вызывает диалог, в котором есть возможность перехода к пакету с указанным номером.

Вид

Статистика – открывает окно статистики протоколов и данных.
Информация о портах – позволяет посмотреть информацию о портах.
Каталог log-файлов – открывает директорию, где по умолчанию сохраняются Log-файлы.
Колонки текущих IP-соединений – показывает/скрывает колонки в закладке "**Текущие IP-соединения**".
Колонки пакетов – показывает/скрывает колонки в закладке **"Пакеты"**.

Инструменты

Генератор пакетов – открывает окно генератора пакетов.
Реконструкция TCP-сессии – позволяет реконструировать TCP-сессию, начиная с выбранного пакета (открывается новое окно, отображающее весь процесс обмена между двумя хостами).
Реконструкция UDP-потока – позволяет реконструировать UDP-поток, начиная с выбранного пакета (открывается окно, отображающее весь процесс обмена между двумя хостами).
Определение изготовителя NIC – открывает окно, где можно определить фирму-изготовителя сетевого адаптера по MAC-адресу.
Захват по расписанию – менеджер расписания, добавляет или удаляет из расписания новые работы.

Настройка

Шрифты – открывает подменю установки шрифтов, используемых в интерфейсе программы.
MAC-псевдонимы – вызывает окно, где можно назначить имена (алиасы) MAC-адресам для облегчения обзора трафика сети.
IP-псевдонимы – вызывает окно, где можно назначить легко запоминаемые имена (алиасы) IP-адресам.
Установки – открывает окно, в котором можно определить дополнительные свойства программы.
Языки интерфейса – изменение языка интерфейса (требует перезапуска программы). Инсталляционный пакет CommView может не содержать все доступные файлы языков пользовательского интерфейса. Для загрузки необходимых языков выберите в меню опцию **Другие языки.** Откроется веб-страница с языковыми модулями для данной версии программы.
Установить драйвер Dial-up – устанавливает драйвер для сбора пакетов с адаптеров dial-up. Если драйвер уже установлен – пункт становится невидимым.
Установить драйвер Token Ring – устанавливает драйвер для сбора пакетов с адаптеров Token Ring. Если драйвер уже установлен – пункт становится невидимым.

Правила

Сохранить текущие как… – позволяет сохранить в конфигурационном файле текущие настройки правил сбора пакетов.
Загрузить из… – позволяет загрузить настройки правил сбора пакетов из ранее созданного конфигурационного файла.
Отменить все – отменяет все правила (если таковые были установлены).

Справка

Содержание – открывает файл-справку CommView.
Искать в справке… – показывает оглавление файла-справки CommView.
Онлайн учебник – открывает окно с учебником по работе с CommView в браузере.
Проверить наличие обновлений – открывает мастер обновлений. Для того, чтобы скачать и установить последнее обновление для CommView с сайта TamoSoft, следуйте инструкциям.
Активация – позволяет активировать вашу копию данного продукта или проверить факт ее активации.
О программе – выводит информацию о версии программы.
Практически каждый элемент интерфейса имеет контекстно-зависимое меню, которое можно вызвать нажатием правой кнопки мыши; многие команды доступны только через это меню.

Первая закладка отображает подробную информацию о сетевых соединениях вашего компьютера (только по IP-протоколу). Для более подробной информации обратитесь к главе Текущие IP-соединения.

Вторая закладка используется для просмотра перехваченных сетевых пакетов и отображения детальной информации о выбранном пакете. Для более подробной информации обратитесь к главе Пакеты.

Третья закладка позволяет вам сохранить перехваченные пакеты в файле. Для более подробной информации обратитесь к главе Log-файлы.

Четвёртая закладка позволяет настаивать правила, влияющие на перехват/игнорирование пакетов, основываясь на таких их свойствах, как IP-адрес или номер порта. Для более подробной информации обратитесь к главе Правила.

Пятая закладка настраивает систему оповещения о подозрительных пакетах, повышении загруженности сети, неизвестных адресах и т. п. Для более подробной информации обратитесь к главе Предупреждения.

В шестой закладке реализована возможность работы с модулем анализа VoIP. Эта закладка доступна только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

Вы можете изменять некоторые настройки, такие как шрифты, цвета и размер буфера, пункт меню **Настройка**. Для более подробной информации обратитесь к главе Установка опций.

Выбор сетевого адаптера для работы

Наблюдение за сетевыми соединениями начинаются с выбора сетевого адаптера. Правильный выбор устройства является важным условием получения желаемого результата. Мы постарались сделать CommView как можно более простым и понятным, и всё, что вам нужно сделать - это выбрать требуемый адаптер из выпадающего списка на панели инструментов и нажать кнопку **Начать захват**.

С развитием сетевых технологий на рынке появляются всё новые типы адаптеров - WiFi, xDSL и так далее. Многие из них поддерживаются CommView, однако, каждая разновидность имеет свои характерные особенности, которые необходимо учитывать для получения корректных результатов.

Рассмотрим перечень наиболее известных типов и покажем, как следует настроить CommView для их использования.

Во время установки программы CommView происходит поиск имеющихся на компьютере сетевых адаптеров. В процессе инсталляции вам будет задан вопрос об установке драйвера для адаптера удалённого доступа (dial-up adapter). Следует ответить **Да**, если вы планируете наблюдать трафик на модеме, xDSL-подключении или используете PPPoE/VPN на других видах сетевого доступа. Если в этот момент вы ответите **Нет**, то сможете установить этот драйвер позже. Для этого выберите в меню **Настройка** => **Установить драйвер dial-up.** При установке данного драйвера работа сетевых подключений будет временно приостановлена.

По окончании установки программы запустите CommView и в выпадающем списке на панели инструментов просмотрите имеющиеся адаптеры. Там должен быть логический адаптер обратной связи (Loopback adapter), адаптер локальной сети (если он имеется в компьютере) и адаптер удалённого доступа (если вы ответили **Да** на вопрос об установке соответствующего драйвера).

Рассмотрим, как эти адаптеры соотносятся с реальным оборудованием на вашем компьютере и с типами сетевых подключений.

Если используется обычный **адаптер Ethernet**, можете просто выбрать его и начать работу. CommView поддерживает практически любой тип адаптеров Ethernet - 10, 100, и 1000 Mbit, имеющийся на рынке.

Если для подключения к сети используется модем, выберите **dial-up**. Обратите внимание, что вы увидите только входящие и исходящие пакеты, без транзитных пакетов. Это не является ограничением программы, ведь именно таким образом устроено подключение «точка-точка» - только два узла, ваш и удалённый, участвуют в соединении. Если ваш узел является одновременно шлюзом ICS (совместного использования интернет-подключения), вам будут доступны все пакеты остальных клиентов ICS – входящие и исходящие.

При использовании CommView для наблюдений в беспроводных 802.11 a/b/g/n/ac сетях, выберите для наблюдения ваш **адаптер Wi-Fi**. Универсальные драйверы не могут перевести адаптер Wi-Fi в promiscuous-режим (состояние, в котором сетевой адаптер обнаруживает в сети все пакеты вне зависимости от их конечного адреса). CommView будет отображать входящие и исходящие пакеты, а так же широковещательные и многоадресные пакеты. Заголовки пакетов 802.11 отображаться не будут. Если требуется средство наблюдения трафика беспроводных сетей

в режиме promiscuous - воспользуйтесь CommView для WiFi, который именно для этого и предназначен. Он позволяет наблюдать трафик других беспроводных клиентов и точек доступа. CommView для WiFi можно скачать с веб-сайта TamoSoft.

Если для подключения к сети используется **xDSL-модем** с **интерфейсом USB**, у вас, скорее всего, будет возможность наблюдать трафик с помощью CommView. Официальной поддержки интерфейса USB в CommView нет, но, тем не менее, можно попытаться. В большинстве случаев соединение будет устанавливаться с помощью PPPoE; в этом случае выберите dial-up адаптер, на котором и будет доступно наблюдение всего сетевого трафика.

Если ваш модем **xDSL** оснащён **Ethernet-интерфейсом**, но само подключение осуществляется с помощью PPPoE, выберите dial-up адаптер, на котором будет доступно наблюдение входящего/исходящего трафика вашего узла, а так же широковещательные и многоадресные пакеты. Если для наблюдения выбрать адаптер Ethernet – вы увидите трафик на сегменте локальной сети, но пакеты будут инкапсулированы в соответствии с PPPoE и могут оказаться зашифрованными.

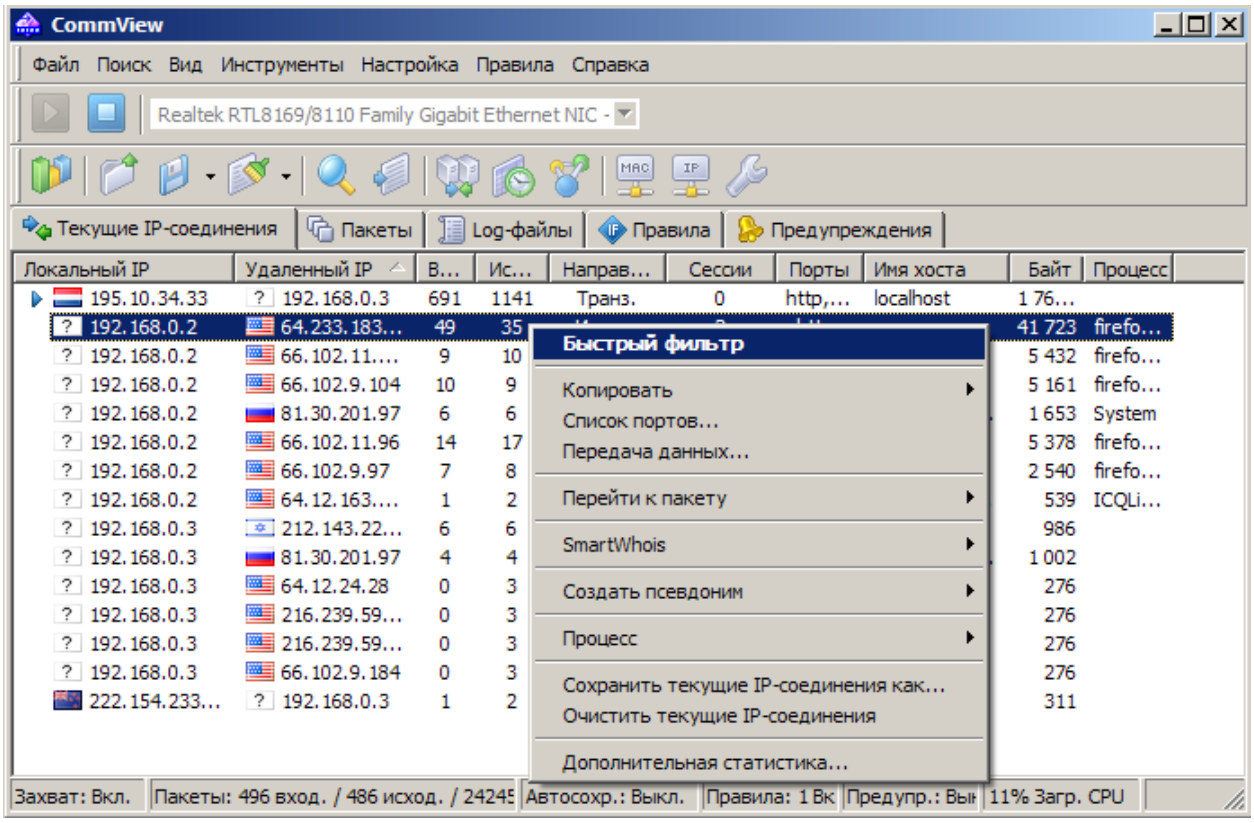
Если ваше подключение к сети защищено с помощью **VPN**, наблюдение на адаптере Ethernet выдаст лишь пакеты в зашифрованном виде. В этом случае следует выбрать dial-up адаптер для получения пакетов в расшифрованном виде.

Если два или более адаптеров объединены в «мост» (**Bridged**), наблюдение на этом «мосту» покажет входящий и исходящий трафик каждого из составляющих его адаптеров, широковещательные и многоадресные пакеты, а также пакеты, переправляемые на остальные адаптеры, включенные в «мост».

Наблюдение на **логическом адаптере обратной связи** (**Loopback)** покажет локальный TCP/IP-трафик, создаваемый программами, работающими на вашем компьютере. Если работающие в данный момент программы такого трафика не создают – вы будете наблюдать полную тишину. Обратите внимание, что генератор пакетов не будет работать с логическим адаптером обратной связи. За подробностями обратитесь к главе Сбор трафика на логическом адаптере обратной связи.

Текущие IP-соединения

Эта закладка отображает подробную информацию о сетевых соединениях вашего компьютера (только для протоколов IP и IPv6). Чтобы начать захват пакетов, выберите **Файл => Начать захват** или нажмите соответствующую кнопку на панели инструментов.



Ниже описывается назначение колонок таблицы:

Локальный IP – показывает локальный IP-адрес. Для входящих пакетов это IP-адрес получателя, для исходящих и транзитных - IP-адрес источника.

Удаленный IP – показывает удалённый IP-адрес. Для входящих пакетов это IP-адрес источника, для исходящих и транзитных – IP-адрес получателя.

Программа автоматически определяет местонахождение любого IP-адреса и, в зависимости от ваших установок геолокации, рядом с IP-адресом может отображать либо название страны, либо ее флаг. Для более подробной информации смотрите главу Установка опций.

Входящие – показывает число принятых пакетов.
Исходящие – показывает число посланных пакетов.
Направление – показывает направление сессии. Направление сессии определяется по направлению первого пакета, принятого от удаленного IP-адреса или отправленного на удалённый IP-адрес.
Сессии – показывает число установленных TCP/IP-сессий. Если соединения по TCP не были установлены (обрыв соединения или работа по протоколам UDP/IP и ICMP/IP) - это значение равно нулю.

Порты - список может быть пустым, если протокол не является TCP/IP. Порты могут быть показаны или как числовые значения, или как соответствующие названия сервисов. Для более подробной информации смотрите главу Установка опций.
Имя хоста – показывает имя удалённого хоста. Если имя не может быть определено – колонка пуста.
Байт – количество байтов, переданных за сессию.
Процесс – показывает имя процесса, посылающего или принимающего пакеты для данной сессии. Установление соответствия между пакетами и процессами вашего компьютера возможно только по отношению к входящим и исходящим пакетам (но не к транзитным), так как CommView не располагает информацией о процессах на других компьютерах, которые могут быть источниками и получателями транзитных процессов. Кроме того, на компьютере может быть несколько процессов, ведущих обмен пакетами по сети, соответственно, закладка **Текущие IP-соединения** показывает имя последнего процесса, обменивавшегося пакетами между данной парой IP-адресов. Чтобы проследить принадлежность конкретного пакета какому-либо процессу, обратитесь к закладке **Пакеты**. Чтобы CommView отображал полный путь к процессу, установите флаг "**Показывать полный путь процессов"** в меню **Настройка** => **Установки**, в закладке **Основн.** Обратите внимание, что в зависимости от используемой вами операционной системы, при первом запуске CommView имена процессов могут не отображаться. Для решения этой проблемы перезагрузите компьютер после первоначальной установки CommView.

Можно показывать или скрывать отдельные колонки таблицы, кликая правой кнопкой мыши по их заголовкам или выбирая соответствующие команды меню **Вид => Колонки текущих IP-соединений**. Расположение колонки можно изменить, просто "перетащив" ее на требуемое место.

Команды контекстного меню

Нажатие правой кнопки мышки на таблице **Текущие IP-соединения** вызывает меню со следующими командами:

Быстрый фильтр – находит пакеты, пересылаемые между выбранными IP-адресами и отображает их в новом окне. Те же действия производятся двойным нажатием мыши.
Копировать – копирует локальный IP-адрес, удалённый IP-адрес или имя хоста в буфер обмена.
Список портов – отображает окно с полным списком портов используемых между выбранной парой IP-адресов. Это удобно, если все используемые порты не помещаются в соответствующей колонке.
Передача данных – отображает окно с информацией об объёме передачи данных между выбранной парой IP-адресов и с временем обработки последнего пакета.
Перейти к пакету – позволяет быстро переходить к первому/последнему пакету с выбранным IP-адресом источника/получателя; программа откроет закладку **Пакеты** и установит курсор на соответствующий пакет.
SmartWhois – отправляет выбранный IP-адрес источника или получателя в SmartWhois, если эта программа установлена на вашем компьютере. SmartWhois - автономное приложение, разработанное нашей компанией, способное собирать информацию о любом IP-адресе или имени хоста по всему миру. Оно автоматически предоставляет информацию, связанную с IP-

адресом, такую как домен, сетевое имя, страну, штат или провинцию, город. Эту программу можно загрузить с нашего веб-сайта.

Создать псевдоним – открывает окно, где можно назначить легко запоминаемые псевдонимы (алиасы) IP-адресам.

Процесс – позволяет получить дополнительную информацию о процессе, принимающем или передающем пакеты в данной сессии, или воздействовать на него. Вы можете **Завершить** процесс, узнать **Свойства файла** или **Показать полный путь** к файлу процесса.

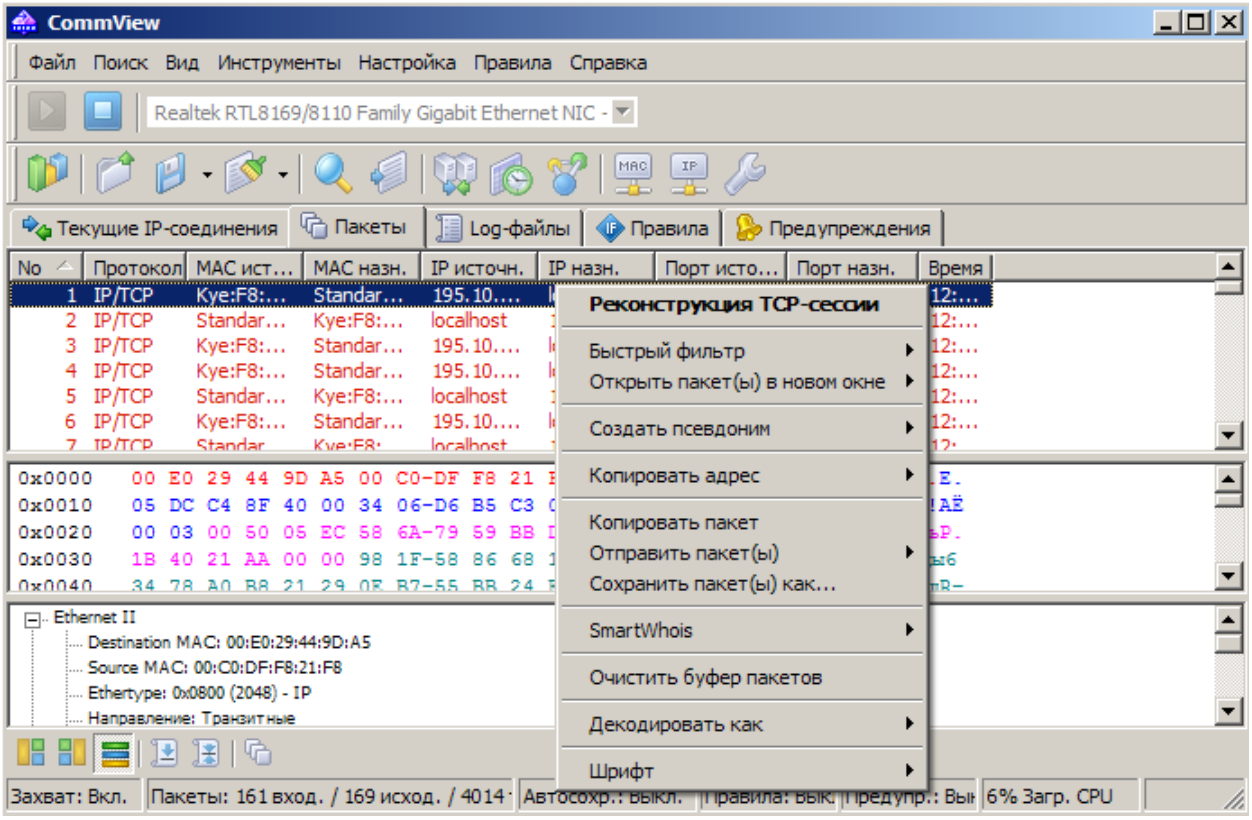
Сохранить текущие IP-соединения как… – позволяет сохранить содержимое закладки **Текущие IP-соединения** как HTML- или CSV-отчёт.

Очистить текущие IP-соединения – очищает таблицу статистики.

Дополнительная статистика… – открывает окно со статистикой протоколов и данных.

Пакеты

Эта закладка используется для показа всех перехваченных сетевых пакетов и отображения подробной информации о выбранном пакете.



В верхней таблице содержится список всех перехваченных пакетов. Этот список может быть использован для выбора пакета, который требуется отобразить и проанализировать. Когда какой-либо пакет выбран, остальные окна показывают информацию о нем.

Ниже описывается назначение колонок таблицы:

No – уникальный номер пакета.
Протокол – показывает протокол пакета.
MAC источн./назн. – показывает MAC-адреса источника и получателя.
IP источн./назн. – показывает IP-адреса источника и получателя (когда применимо).
Порты источн./назн. – показывает порты источника и получателя (когда применимо). Порты могут быть отображены или как числовые значения, или как соответствующие названия сервисов. Для более подробной информации смотрите главу Установка опций.
Время – показывает время появления пакета – абсолютное или как интервал от предыдущего пакета. Переключать режим можно в меню **Вид => Колонки пакетов => Показывать время как >**.
Размер – показывает размер пакета в байтах. По умолчанию колонка не отображается.
Детали – показывает краткий отчет по пакету.

Можно показывать или скрывать отдельные колонки таблицы, кликая правой кнопкой мыши по их заголовкам или выбирая соответствующие команды меню **Вид => Колонки пакетов**.

Вывод пакетов можно приостановить, включив пункт **Файл => Блокировать сбор пакетов**. В этом случае пакеты перехватываются, но не показываются в закладке **Пакеты**. Этим можно воспользоваться, когда интересует только статистика, а не сами пакеты. Чтобы восстановить показ пакетов в реальном времени, включите пункт **Файл => Продолжить сбор пакетов**.

В среднем окне показано содержимое пакета в "сыром", необработанном виде. Она представлена как в 16-ричном виде, так и в виде обычного текста. В текстовом отображении непечатаемые символы показаны точками. В случае, когда в верхней таблице выбрано несколько пакетов, в среднем окне будет показано общее количество выбранных пакетов, их суммарный размер, а также временной интервал между первым и последним пакетом.

В нижнем окне показана декодированная информация для выбранного пакета. Эта информация включает в себя существенные данные, которые могут быть использованы профессионалами в области сетевых технологий. Щелкнув правой кнопкой мыши, можно вызвать контекстное меню, которое позволяет открывать/закрывать узлы, копировать содержимое выбранного узла или всех узлов.

В закладке пакетов также есть небольшая панель инструментов:

Вы можете поменять расположение окна декодирования, нажав кликнув на одну из трех кнопок на этой панели (окно может быть выровнено по низу, по левой или правой стороне). Четвертая кнопка выполняет автоматическую прокрутку к последнему принятому пакету. Пятая кнопка позволяет оставить выделенный вами пакет в видимом списке (т. е. он не выйдет за границы видимой области при поступлении новых пакетов). Шестая кнопка открывает содержимое текущего буфера пакетов в новом окне. Это очень полезно при большой загруженности сети, когда список пакетов постоянно прокручивается и изучение пакетов бывает затруднительным, поскольку они быстро исчезают за границей видимости. Нажав на эту кнопку, вы создадите "снимок" буфера пакетов и сможете спокойно изучить его в отдельном окне. Вы можете сделать любое количество таких "снимков".

Команды контекстного меню

Нажатие правой кнопки мыши на списке пакетов вызывает меню со следующими командами:

Реконструкция TCP-сессии – позволяет реконструировать TCP-сессию, начиная с выбранного пакета (открывается новое окно, отображающее весь процесс обмена между двумя хостами).
Быстрый фильтр - позволяют обнаруживать пакеты, передаваемые между MAC- и IP-адресами, а также портами. Эти пакеты отображаются в новом окне.
Открыть пакет(ы) в новом окне – позволяет открыть один или несколько пакетов в отдельном окне.
Создать псевдоним - открывает окно, где можно назначить легко запоминаемые псевдонимы (алиасы) выбранным MAC- или IP-адресам.

Копировать адрес – копирует локальный MAC- или IP-адрес, удалённый MAC- или IP-адрес в буфер обмена.
Копировать пакет – копирует сырые данные пакета в буфер обмена.
Отправить пакет(ы) – открывает окно генератора пакетов и позволяет послать выбранный пакет (один или несколько) ещё раз. Перед отправкой содержимое пакетов можно изменить.
Сохранить пакет(ы) как… – записывает содержимое выбранного пакета (одного или нескольких) в файл. Формат файла выбирается в выпадающем меню.
SmartWhois – отправляет выбранный IP-адрес источника или получателя в SmartWhois, если эта программа установлена на вашем компьютере. SmartWhois - автономное приложение, разработанное нашей компанией, способное собирать информацию о любом IP-адресе или имени хоста по всему миру. Оно автоматически предоставляет информацию, связанную с IP-адресом, такую как домен, сетевое имя, страну, штат или провинцию, город. Эту программу можно загрузить с нашего веб-сайта.
Очистить буфер пакетов – сбрасывает программный буфер пакетов. Список пакетов очищается, и все накопленные к этому моменту пакеты стираются.
Декодировать как… – для TCP- и UDP-пакетов. Позволяет декодировать известные программе протоколы, которые используют нестандартные порты. Например, если сервер SOCKS вместо 1080 использует порт 333, можно выбрать пакет, принадлежащий сессии SOCKS и, зайдя в это меню, заставить CommView декодировать все пакеты порта 333 как SOCKS. Такие переназначения "протокол-порт" не являются перманентными и будут в силе до выхода из программы. Просим заметить, что вы не можете изменить стандартно установленные пары "протокол-порт", т. е. CommView не будет декодировать пакеты с 80-го порта как пакеты TELNET.
Шрифт – позволяет вам изменить шрифт для отображения пакетов без изменения шрифта других элементов программы.

Также есть возможность перемещать пакеты на рабочий стол или в любую папку при помощи мыши.

Log-файлы

Эта закладка предназначена для записи перехваченных пакетов в файл на диск. CommView сохраняет пакеты в собственном формате с расширением NCF. Старый формат CCF (CommView Capture Files) поддерживается нашей программой только для обратной совместимости и недоступен для сохранения новых данных. Вы всегда можете загрузить и просмотреть эти файлы при помощи утилиты Log viewer, а также просто запустив NCF/CCF-файл в папке или на рабочем столе. NCF является открытым форматом, за подробностями обращайтесь к главе Формат Log-файлов CommView.

Сохранение и управление

Эта опция используется для сохранения перехваченных пакетов в файл вручную, а также для объединения или разделения файлов с перехваченной информацией.

Можно или сохранить все пакеты, находящиеся на данный момент в буфере, или только часть из них, в заданном диапазоне. Поля **От** и **До** устанавливают требуемый диапазон номеров пакетов, отображённых в закладке **Пакеты**. Нажмите **Сохранить Как…** для выбора имени файла.

Если требуется вручную объединить нескольких файлов .NCF в один, выберите опцию **Объединить log-файлы…** . Для разделения файла .NCF на несколько частей, выберите опцию **Разделить log-файлы**. Следуя указаниям программы, вы сможете выбрать требуемый размер выходных файлов.

Автосохранение

Установите этот флажок, чтобы программа автоматически сохраняла перехваченные пакеты по мере их поступления. Чтобы ограничить общий размер файлов, находящихся в Папке Log-файлов (Log Directory), введите значение в поле **Максимальный размер каталога, Мбайт**. Если общий размер файлов превышает предел, программа автоматически удаляет наиболее старые файлы. Поле **Средний размер log-файла** устанавливает приблизительный размер файла, при превышении этой величины – автоматически открывается следующий. Чтобы выбрать другую папку для Log-файлов, введите путь в поле **Сохранять log-файлы в:**.

ВАЖНО: Если требуется сохранить файл с перехваченной информацией на долгое время, не держите их в папке для Log-файлов, которая установлена по умолчанию. Существует опасность того, что файл будет автоматически удален по мере того, как будут сохраняться новые файлы. Перенесите необходимый вам файл в другую директорию, чтобы он был в неприкосновенности.

Имейте в виду, что программа не сохраняет автоматически каждый пакет сразу по его прибытии. Это означает, что если вы просматриваете Log-файл в реальном времени, он может не содержать самые последние пакеты. Для того чтобы программа немедленно переслала буфер в файл, нажмите **Закончить захват**, или снимите флажок **Автосохранение.**

Запись доступа к WWW

Установите этот флажок для ведения протоколов сессий HTTP. В поле **Максимальный размер файла, Мбайт** установите требуемое значение для файла протокола. При превышении размера файла, программа автоматически удаляет самые старые записи. Для изменения имени и местоположения файла отредактируйте поле **Сохранять log-файлы в…** Протокол можно вести в формате **HTML** или **TXT**. Кнопка **Конфигурация** позволяет устанавливать параметры протоколирования. Можно изменить номер порта, используемого для доступа к HTTP (значение по умолчанию, равное 80, может не подойти при работе через прокси-сервер), исключить некоторые типы данных (обычно протоколировать что-либо кроме самих страниц HTML нецелесообразно, следует исключить URL изображений из файла протокола).

Просмотр Log-файлов

Утилита предназначена для просмотра и исследования файлов с перехваченными пакетами, которые были созданы с помощью CommView. Этот инструмент также содержит и другие средства для анализа пакетов. Log Viewer имеет ту же функциональность, что и закладка **Пакеты** главного окна программы, и отображает информацию о пакетах из ранее сохраненного файла.

Чтобы запустить утилиту, выберите **Файл => Просмотр Log-файлов** в главном меню программы или дважды щёлкните на любой файл перехваченных пакетов, который вы ранее сохранили. Можно открывать несколько окон просмотра, и каждое из них может быть использовано для просмотра одного или нескольких файлов с перехваченными пакетами.

Этой утилитой можно воспользоваться для исследования Log-файлов, созданных другими анализаторами пакетов и брандмауэрами (файрволлами). Текущая версия программы способна импортировать файлы в форматах Network Instruments Observer®, Network General Sniffer® для DOS/Windows, Microsoft NetMon, WildPackets EtherPeek™ и AiroPeek™, Wireshark/Tcpdump и Wireshark/pcapng. Эти форматы также используются другими приложениями. Утилита способна экспортировать пакеты в файлы форматов Network Instruments Observer®, Network General Sniffer® for DOS/Windows, Microsoft® NetMon, WildPackets EtherPeek™ и AiroPeek™, Wireshark/Tcpdump и Wireshark/pcapng, также как и в собственный формат программы CommView.

Пользование утилитой аналогично работе с закладкой **Пакеты**; за подробной информацией обратитесь сюда.

Команды контекстного меню

Файл

Загрузить log-файлы CommView – открывает и загружает файлы в собственном формате CommView.
Импорт log-файлов – импортирует Log-файлы, созданные другими анализаторами пакетов.
Экспорт log-файлов – экспортирует отображаемые пакеты в Log-файлы нескольких форматов.
Очистить окно – очищает окно со списком пакетов.
Сгенерировать статистику… – получение статистики по пакетам, загруженным в утилиту просмотра Log-файлов. При желании можно сбросить уже имеющиеся значения в окне **Статистика**. Эта функция не покажет распределение пакетов во времени, она ограничена общими сведениями, гистограммами протоколов и таблицами хостов LAN.
Передать в VoIP-анализатор – передает пакеты из текущего окна Log Viewer в окно VoIP-анализатора с целью дальнейшего VoIP-анализа.
Закрыть окно – закрывает окно просмотра.

Поиск

Найти пакет… – вызывает диалог поиска пакета, содержащего определённый текст.
Перейти к пакету с номером… - вызывает диалог перехода к пакету с указанным номером.

Правила

Применить текущие – применить текущий набор правил на пакеты, отображаемые утилитой. В результате, программа удалит пакеты, не отвечающие указанным правилам. Файл на диске при этом не изменяется.

Из файла… – то же, что и по команде **Применить текущие**, но позволяет воспользоваться заранее сохранёнными настройками фильтров в файлах .RLS, а не текущими.

Правила

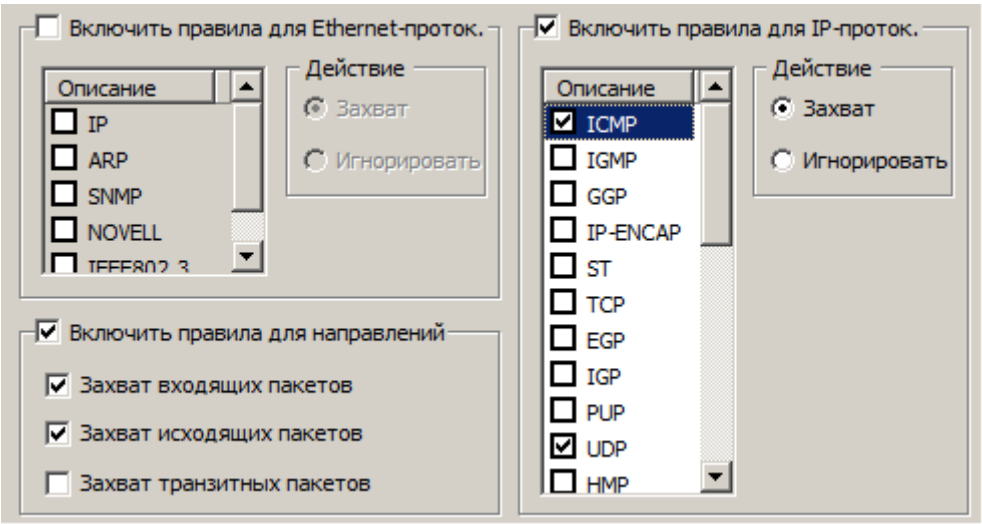
Эта закладка позволяет устанавливать правила перехвата пакетов. Если какие-либо правила установлены, то программа фильтрует пакеты и накапливает только те пакеты, которые соответствуют заданным критериям (правилам). Обратите внимание, CommView не брандмауэр и, когда вы задаёте правила, пакеты продолжают обрабатываться операционной системой, они лишь не отображаются и не сохраняются программой. Если правила установлены, то название соответствующей закладки отображается жирным шрифтом.

Используя команду меню **Правила**, можно сохранять настройки правил в файле и загружать их, когда потребуется.

Так как сетевой трафик часто может создавать большое количество пакетов, рекомендуется использовать правила для фильтрации ненужных пакетов. Это может значительно снизить объём системных ресурсов, используемых программой. Если вы хотите включить/выключить какое-либо правило, выберите соответствующий раздел с левой стороны окна (например, **IP-Адреса Порты**). Затем установите или снимите соответствующий флажок - **Включить правила для IP-адресов** или **Включить правила для портов**. Существует семь типов правил:

Протоколы и Направление

Позволяет игнорировать или перехватывать пакеты, основываясь на протоколах 2-го (Ethernet) и 3-го (IP) уровней, а также на направлениях пакетов.

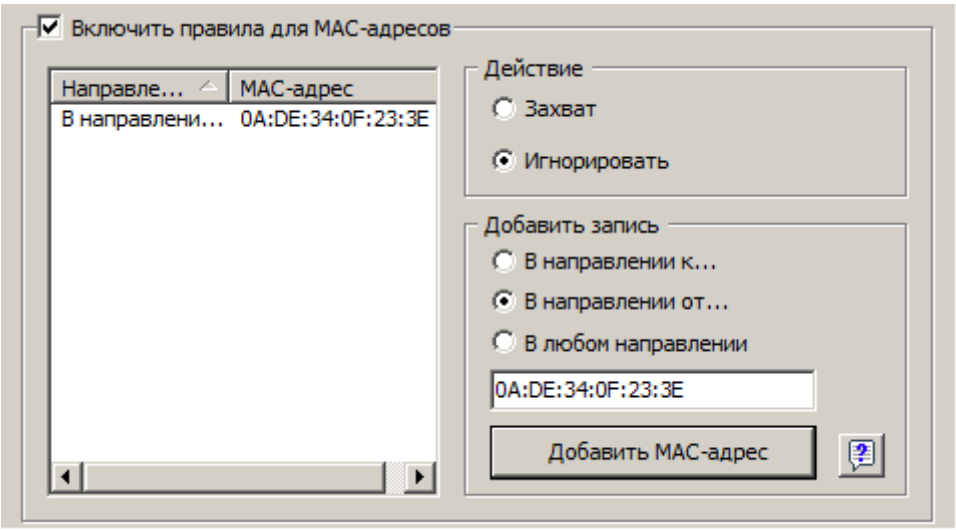


В этом примере показано, как перехватывать только входящие и исходящие пакеты ICMP и UDP. Все остальные пакеты семейства IP, а также транзитные, будут проигнорированы.

MAC-адреса

Позволяет игнорировать или перехватывать пакеты, основываясь на аппаратных MAC-адресах. Введите MAC-адрес в поле **Добавить запись**, выберите направление: **В направлении к…**, **В направлении от…** или **В любом направлении.** Затем и нажмите **Добавить MAC-адрес** и новое правило будет отображено. Далее следует выбрать действие, которое будет совершено при обработке нового пакета: он может быть либо перехвачен, либо проигнорирован.

Список IP-алиасов можно получить, нажав на кнопку **MAC-псевдонимы**. Чтобы показать соответствующий MAC-адрес, следует выбрать нужный IP-алиас из списка.

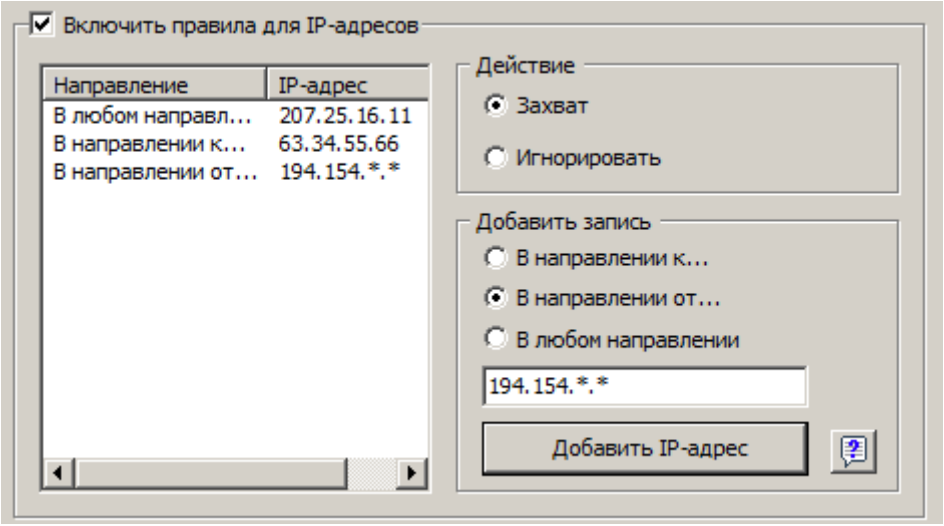


В этом примере показано, как игнорировать пакеты, идущие от 0A:DE:34:0F:23:3E. Пакеты с других MAC-адресов будут перехватываться программой.

IP-адреса

Позволяет игнорировать или перехватывать пакеты, основываясь на IP-адресах. Введите IP- или IPv6-адрес в поле **Добавить запись**, выберите направление: **В направлении к…**, **В направлении от…** или **В любом направлении.** Затем нажмите **Добавить IP-адрес** и новое правило будет отображено. Далее следует выбрать действие, которое будет совершено при обработке нового пакета: он может быть либо перехвачен, либо проигнорирован.

Список IP-алиасов можно получить, нажав на кнопку **MAC-псевдонимы**. Чтобы показать соответствующий MAC-адрес, следует выбрать нужный IP-алиас из списка.

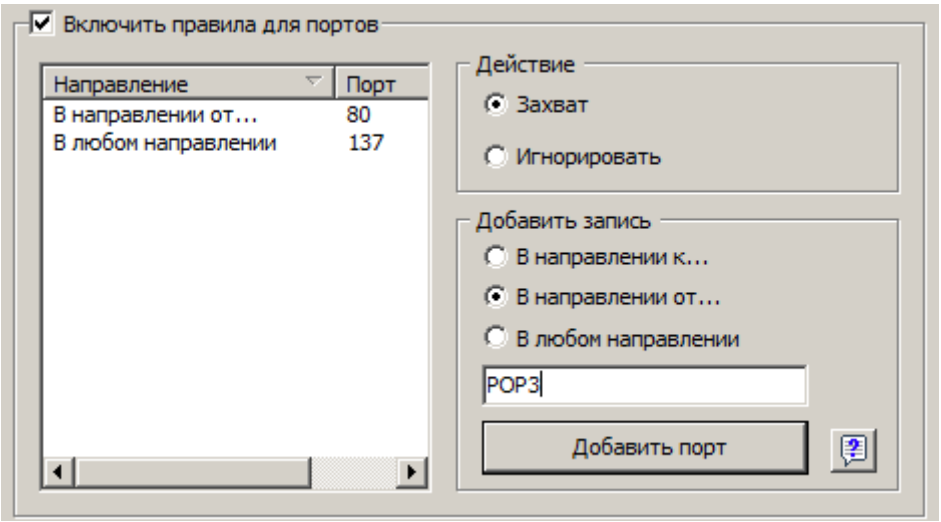


В этом примере показано, как накапливать пакеты, идущие к 63.34.55.66, идущие к/от 207.25.16.11 и идущие со всех адресов в диапазоне 194.154.0.0 -:- 194.154.255.255. Все пакеты, идущие с/на другие адреса будут проигнорированы. Так как IP-адреса используются в IP-протоколе, такая конфигурация заставит программу игнорировать все пакеты, не принадлежащие к IP. Для работы с адресами IPv6 требуется версия Windows XP или выше, а также установленный протокол IPv6.

Порты

Позволяет игнорировать или перехватывать пакеты, основываясь на номерах портов. Введите номер порта в поле **Добавить запись**, выберите направление: **В направлении к…** , **В направлении от…** или **В любом направлении.** Затем нажмите **Добавить порт** и новое правило будет отображено. Далее следует выбрать действие, которое будет совершено при обработке нового пакета: он может быть либо перехвачен, либо проигнорирован.

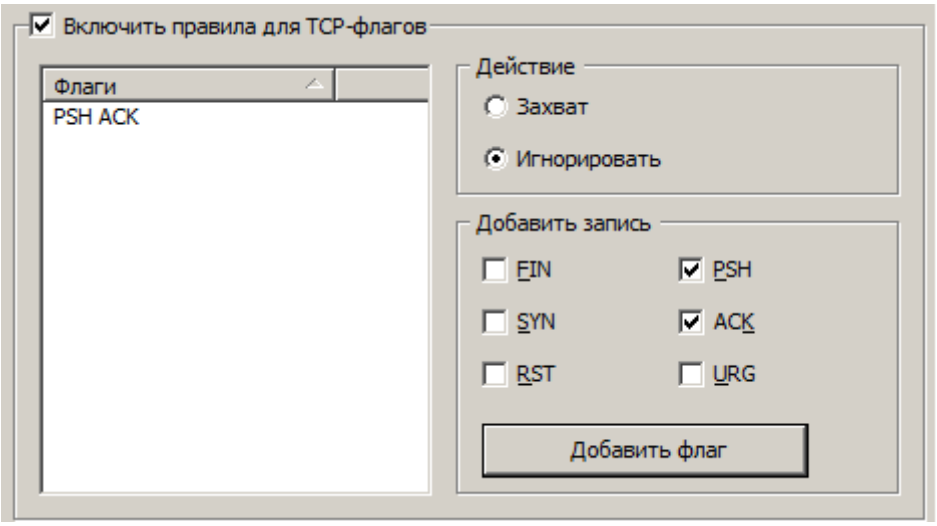
Чтобы добавить порт в список, дважды щёлкните мышью по его номеру. Порты также можно добавлять с использованием из символьных имен, например, http или pop3, а программа затем преобразует введенные значения в численные.



В этом примере показано, как игнорировать пакеты, идущие из порта 80 и идущие из/в порт 137. Это правило позволит CommView игнорировать входящий HTTP-трафик наряду с входящим/исходящим трафиком NetBIOS Name Service. Пакеты, проходящие между портами, будут перехвачены.

TCP-флаги

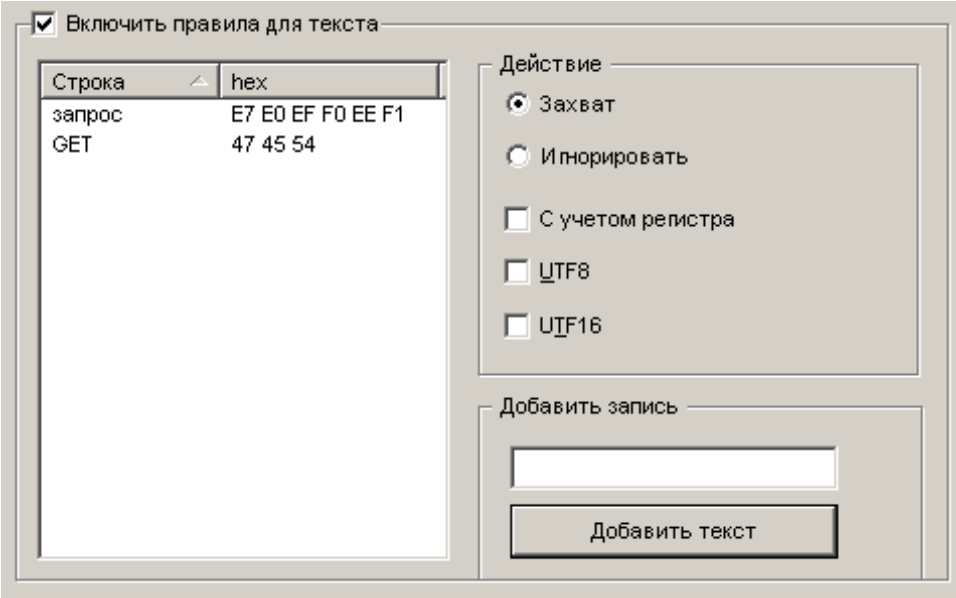
Позволяет игнорировать или перехватывать пакеты, основываясь на TCP-флагах. Выберите флаг или комбинацию флагов в поле **Добавить запись** и нажмите **Добавить флаги.** Новое правило будет отображено. Далее следует выбрать действие, которое будет совершено при обработке нового пакета: он может быть либо перехвачен, либо проигнорирован.



В этом примере показано, как игнорировать TCP-пакеты с установленными флагами PSH и ACK. Пакеты с другими флагами будут перехвачены.

Текст

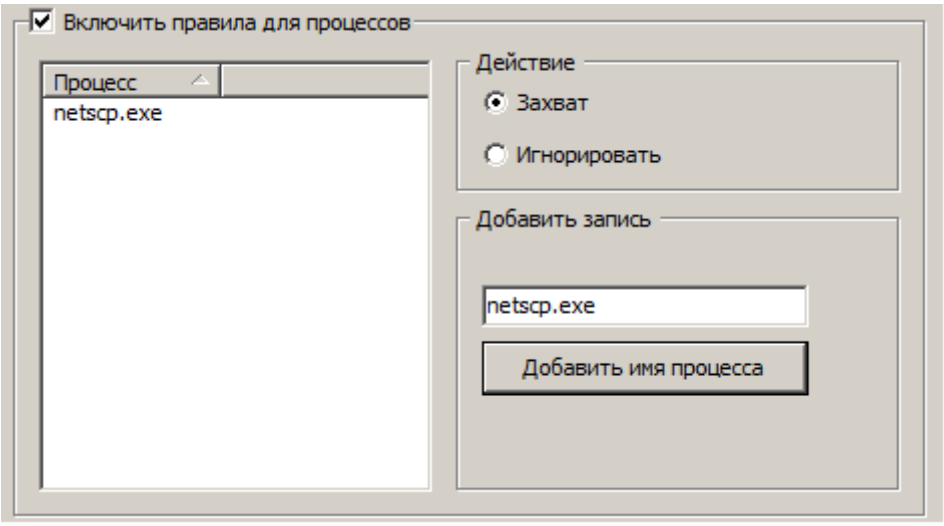
Позволяет перехватывать пакеты, содержащие определённый текст. Введите строку в поле **Добавить запись** и нажмите **Добавить текст.** Новое правило будет отображено. Далее следует выбрать действие, которое будет совершено при обработке нового пакета: он может быть либо перехвачен, либо проигнорирован.



В этом примере показано, как перехватывать только те пакеты, которые содержат текст "GET". При необходимости установите флажок **С учётом регистра**, если вы хотите сделать правила регистрозависимыми. Выберите опции **UTF8** или **UTF16**, если вы хотите, чтобы перехватывались пакеты с текстом только в соответствующей кодировке. Все остальные пакеты, не содержащие вышеуказанного текста, будут игнорированы. Если вы хотите создать правило, основанное на hex-последовательности байтов, когда строку нельзя напечатать (например, 0x010203), используйте Универсальные правила.

Процесс

Позволяет перехватывать пакеты, базируясь на имени процесса. Введите имя процесса в область **Действие** и нажмите **Добавить имя процесса**. Новое правило будет показано. Теперь вы можете выбрать действие, которое будет совершаться при обработке нового пакета: пакет может быть захвачен или пропущен. Вы также можете ввести лишь часть названия процесса, и в правило будет включен каждый процесс, в имени которого будет содержаться такая подстрока. Имена процессов регистронезависимы.



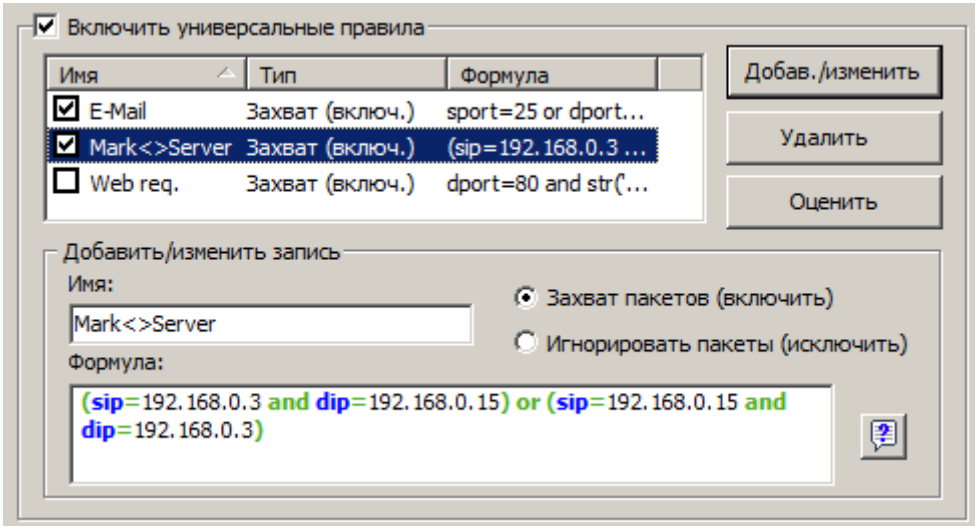
В данном примере показано, как принимать пакеты, принятые или переданные процессом *netscp.exe*. Пакеты, посланные другими процессами, будут пропущены.

Универсальные правила

Универсальные правила являются мощным и гибким механизмом создания фильтров с помощью булевой логики.

Универсальные правила

Универсальные правила являются мощным и гибким механизмом создания фильтров с помощью булевой логики. Требуются лишь элементарные знания математики и логики; синтаксис правил несложен для понимания.



Обзор

Чтобы создать новое правило, задайте ему произвольное имя в поле Имя, выберите действие (Захват пакетов/Игнорировать пакеты), в поле Формула задайте формулу, пользуясь синтаксисом, описанным ниже, и нажмите Добавить/Изменить. Новое правило будет добавлено в список и немедленно активизировано. Вы можете задать неограниченное количество правил, но активными из них буду лишь те, возле которых будет установлена метка. Любое правило можно включить/выключить, изменяя соответствующий флажок, либо совсем удалить правило с помощью кнопки Удалить. Если активны сразу несколько правил, вы можете выполнить комбинированное правило, нажав на кнопку Оценить. Обратите внимание, что отдельные правила объединяются логическим оператором OR ("ИЛИ"). Пример: для трех активных правил RULE1, RULE2, RULE3, результирующим будет правило RULE1 OR RULE2 OR RULE3.

Можно пользоваться составными правилами совместно с обычными, описанными в предыдущей главе. Однако, если вы владеете булевой логикой, рекомендуем пользоваться только составными, так как они более гибки. Обычные правила объединяются с составными с помощью логического оператора AND ("И").

Описание синтаксиса

dir – Направление пакета. Возможные значения - in (входящий), out (исходящий) и pass (транзитный).

etherproto – Протокол Ethernet (13-й и 14-й байты пакета). Допустимыми значениями являются числа (например, *etherproto=0x0800* соответствует протоколу IP) или известные аббревиатуры (например, *etherproto=ARP*, что соответствует 0x0806).

ipproto – Протокол IP. Допустимыми значениями являются числа (например, *ipproto!=0x06* соответствует протоколу TCP) или известные аббревиатуры (например, *ipproto=UDP*, что соответствует 0x11).

smac – MAC источника. Допустимыми значениями являются MAC-адреса источников в шестнадцатеричном виде (например, *smac=00:00:21:0A:13:0F*) или алиасы.

dmac – MAC получателя.

sip – IP- или IPv6-адрес источника. Допустимыми значениями являются IP-адреса, записанные через точку (например, *sip=192.168.0.1* или *sip= fe80::02c0:26ff:fe2d:edb5*), IP-адреса с карт-бланшами (например, ***sip!=*.*.*.255***, кроме адресов IPv6), сетевые адреса с масками подсетей (например, *sip=192.168.0.4/255.255.255.240* или *sip=192.168.0.5/28*), диапазоны IP-адресов (то есть, *sip from 192.168.0.15 to 192.168.0.18* или *sip in 192.168.0.15 ... 192.168.0.18*) или алиасы. Для работы с адресами IPv6 требуется версия Windows XP или выше, а также установленный протокол IPv6.

dip - IP-адрес получателя.

sport – Номер порта-источника пакета TCP или UDP. Допустимыми значениями являются числа (например, *sport=80* соответствует HTTP), диапазоны (то есть, *sport from 20 to 50* или *sport in 20..50* для любых портов в диапазоне от 20 до 50) или алиасы, известные операционной системе (например, *sport=ftp*, что соответствует порту 21). Проверить список алиасов, известных ОС, можно нажав **Вид => Информация о портах**.

dport – Порт-получатель пакетов TCP или UDP.

flag – Флаг TCP. Допустимыми значениями являются числа (например, *0x18* соответствует PSH ACK), одна или несколько букв из следующего списка: *F* (FIN), *S* (SYN), *R* (RST), *P* (PSH), *A* (ACK) и *U* (URG) или ключевое слово has, означающее, что флаг содержит определённое значение. Например: *flag=0x18, flag=SA, flag has F*.

size – Размер пакета. Допустимыми значениями являются числа (например, *size=1514*) или диапазоны (*size from 64 to 84* или *size in 64..84* для размеров с 64 до 84 байтов).

str – Содержимое пакета. Задает условие, что пакет должен содержать определённую строку. Функция имеет три аргумента: образец поиска, местоположение, чувствительность к регистру. Первый аргумент – строка, например, *'GET'*. Второй аргумент – число, показывающее смешение строки в пакете. Счёт начинается с нуля – первый байт пакета надо искать, задавая смещение равное *0*. Чтобы искать строку в любом месте пакета, задайте смещение равным *–1*. Третий аргумент устанавливает чувствительность к регистру и может принимать значения *false* (без учёта регистра) или *true* (с учётом регистра). Второй и третий аргументы необязательны, по умолчанию имеют значения –1 и false соответственно (искать во всём пакете, без учёта регистра). Примеры: *str('GET',-1,false)*, *str('GET',-1)*, *str ('GET')*.

hex - Содержимое пакета. Задает условие, что пакет должен содержать определённый 16-ричный набор. Функция имеет два аргумента: образец поиска и местоположение. Первый аргумент – 16-ричная величина, например, *0x4500*. Второй аргумент – число, задающее смещение внутри пакета. Отсчёт ведется с нуля, т. е. первый байт пакета соответствует смещению, равному *0*. Чтобы искать во всём пакете, задайте смещение равным *–1*. Второй аргумент необязателен, по умолчанию имеет значение *–1* (искать во всём пакете). Пример: *hex(0x04500, 14) , hex(0x4500, 0x0E), hex (0x010101)*.

bit - Содержимое пакета. Задает условие, что пакет должен содержать по указанному смещению определённый бит, имеющий значение 1. В этом случае функция вернёт код возврата *true*. Если же искомый бит имеет значение 0 или находится за пределами пакета - функция вернёт код возврата *false*. Первый аргумент – номер бита в байте, начиная с нуля; допустимые значения 0-7. Таким образом, если вы ищете восьмой бит, установите номер равным семи. Второй аргумент – число, обозначающее смещение байта в пакете, начиная с нуля, то есть, если нужен первый байт пакета – смещение должно быть равно *0*. Оба аргумента обязательны, например: *bit(0, 14)* , *bit(5, 1)*.

Вышеописанные ключевые слова можно использовать со следующими операторами:

and - конъюнкция, булево И.
or - дизъюнкция, булево ИЛИ.
not - булево отрицание.
= - Арифметическое равенство.
!= - Арифметическое неравенство.
<> - Арифметическое неравенство.
> - Арифметическое условие "больше, чем".
< - Арифметическое условие "меньше, чем".
( ) – скобки, управляющие порядком вычисления правил.

Числа могут быть в десятичной или шестнадцатеричной системе. Для указания на шестнадцатеричную нотацию, используйте 0x перед значением, например, 15 и 0x0F задают одно и тоже число.

Примеры

Ниже приведены несколько примеров, поясняющих синтаксис правил. К каждому правилу даны комментарии, отделяемые двойной косой чертой.

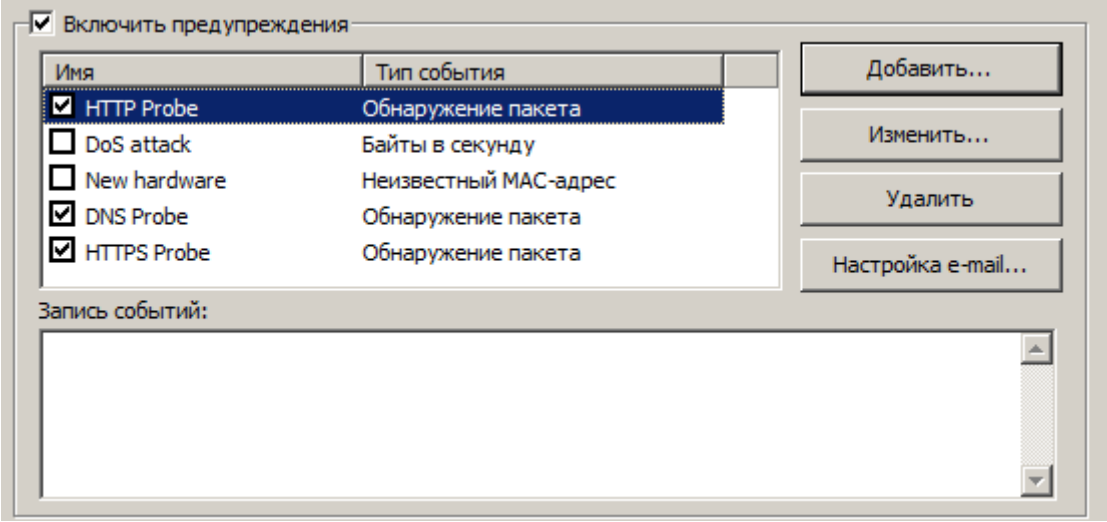
- dir!=pass // Захватывать только входящие и исходящие пакеты. Транзитные пакеты игнорируются.
- (smac=00:00:21:0A:13:0E or smac=00:00:21:0A:13:0F) and etherproto=arp // Захватывать пакеты ARP, посылаемые двумя компьютерами с MAC 00:00:21:0A:13:0E и 00:00:21:0A:13:0F.
- ipproto=udp and dport=137 // Захватывать пакеты UDP/IP, посылаемые в порт 137.
- dport=25 and str('RCPT TO:', -1, true) // Захватывать пакеты TCP/IP или UDP/IP, содержащие строку "RCPT TO:" и направляемые в порт 25.

- not (sport>110) // Захватывать все пакеты, кроме тех, что имеют порт-источник с номером выше 110.
- (sip=192.168.0.3 and dip=192.168.0.15) or (sip=192.168.0.15 and dip=192.168.0.3) // Захватывать только IP-пакеты, следующие между двумя хостами, 192.168.0.3 и 192.168.0.15. Все остальные игнорируются.
- ((sip from 192.168.0.3 to 192.168.0.7) and (dip = 192.168.1.0/28)) and (flag=PA) and (size in 200..600) // Захватывать TCP-пакеты, размер которых лежит в диапазоне от 200 до 600 байтов, приходящие с IP-адресов в диапазоне 192.168.0.3 - 192.168.0.7, причем IP-адреса получателей находятся в сегменте 192.168.1.0/255.255.255.240, и имеющие TCP-флаг PSH ACK.
- Hex(0x0203, 89) and (dir<>in) // Захватывать пакеты, содержащие 0x0203 в смещении 89, при этом направление пакета - не "входящий".

Предупреждения

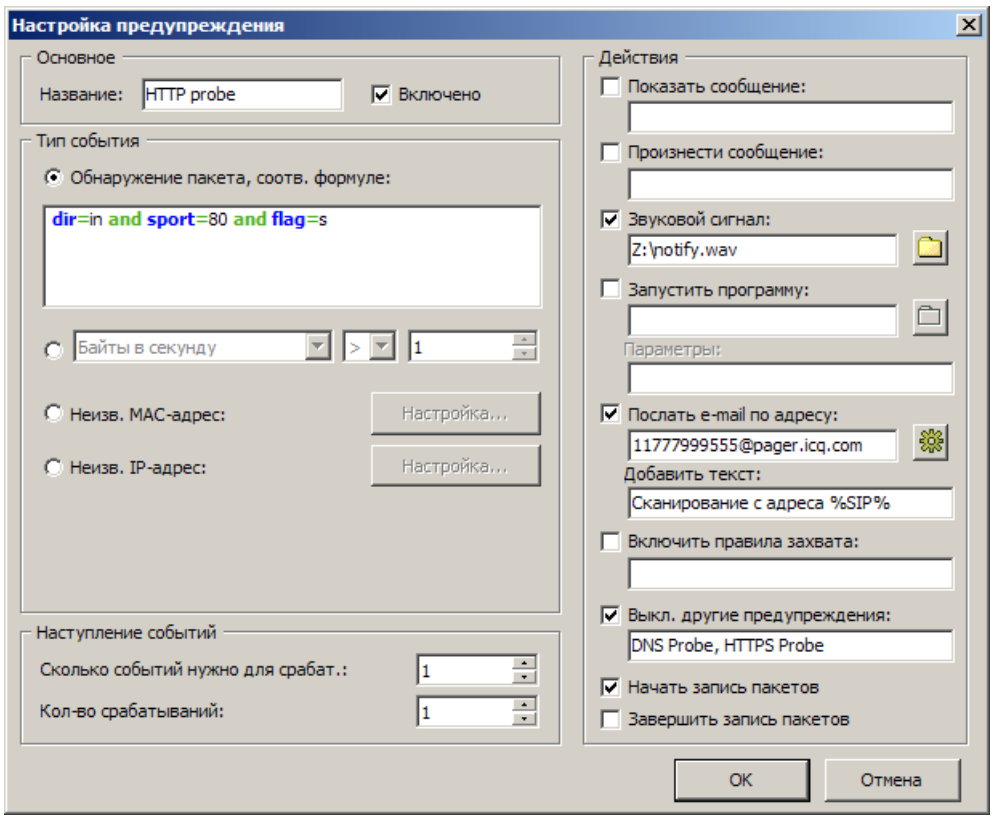
В этой закладке можно создавать систему предупреждений о существенных событиях в сети, таких как появление подозрительных пакетов, повышение сетевой нагрузки, нештатные адреса и так далее. Предупреждения могут очень помочь, если вам надо отслеживать такие события в сети, как сканирование портов, появление определённой последовательности байтов в пакетах, неожиданное подключение новых устройств.

Управление предупреждениями осуществляется с помощью показанного ниже списка:



В каждой строке показано отдельное предупреждение, а флажок рядом с названием предупреждения показывает, активно оно или нет. При срабатывании предупреждения флажок сбрасывается. Чтобы повторно активизировать ожидание сработавшего предупреждения, установите флажок возле его имени. Для отключения всех предупреждений – сбросьте флажок **Включить предупреждения**. Чтобы добавить новое, отредактировать или удалить какое-либо предупреждение, воспользуйтесь кнопками справа от списка. Если вы хотите использовать оповещение по E-mail, то посредством опции **Настройка E-mail** введите настройки вашего SMTP-сервера (см. ниже).

Ниже показано окно настройки предупреждений:



В поле **Имя** описывается назначение текущей функции предупреждения. Установите флажок **Включено**, если требуется активировать предупреждение, которое вы в данный момент редактируете. Этот флажок совпадает со значением соответствующей колонки в списке предупреждений. В поле **Тип события** можно выбрать один из семи типов событий:

- **Обнаружение пакета**: Это предупреждение сработает при обнаружении пакета, соответствующего указанной формуле. Синтаксис формул совпадает с синтаксисом составных правил и подробно описан в главе Универсальные правила.
- **Байты в секунду**: Это предупреждение сработает при превышении указанного уровня загрузки сети. Значение следует указывать в байтах. Например, если требуется срабатывание при превышении уровня трафика в 1Mbyte/сек, укажите порог, равный 1000000.
- **Пакеты в секунду**: Это предупреждение сработает при превышении заданного уровня частоты передачи пакетов.
- **Бродкасты в секунду**: Это предупреждение сработает при превышении указанного уровня частоты передачи широковещательных пакетов.
- **Мультикасты в секунду**: Это предупреждение сработает при превышении указанного уровня частоты передачи многоадресных пакетов.
- **Неизвестный MAC-адрес**: Это предупреждение сработает при перехвате программой пакетов с неизвестными MAC-адресами отправителя либо получателя. Опция **Настройка** позволяет задать список известных адресов. Это предупреждение можно использовать для обнаружения подключений нового или несанкционированного оборудования в сеть.

- **Неизвестный IP-адрес**: Это предупреждение сработает при перехвате программой пакетов с неизвестными IP- или IPv6-адресами отправителя либо получателя. Опция **Настройка** позволяет задать список известных адресов. Это предупреждение можно использовать для обнаружения несанкционированных подключений через корпоративный брандмауэр. Для работы с адресами IPv6 требуется версия Windows XP или выше, а также установленный протокол IPv6.

Поле **Сколько событий нужно для срабатывания** позволяет установить количество событий, которое должно произойти, чтобы сработало предупреждение. Например, если установить уровень равный 3, предупреждение не сработает, пока событие не произойдёт трижды. При редактировании уже существующего предупреждения происходит обнуление внутреннего счётчика событий.

Поле **Кол-во срабатываний** определяет, сколько раз может срабатывать предупреждение, прежде чем станет неактивным. По умолчанию, эта величина равна 1, и предупреждение отключится после первого же срабатывания. Увеличив количество, можно настроить CommView на многократные срабатывания предупреждений. При редактировании уже существующего предупреждения происходит обнуление внутреннего счётчика событий.

В поле **Действия** можно выбрать действие, которое будет исполнено при срабатывании предупреждения. Список возможных действий имеет следующий вид:

- **Показать сообщение**: появляется сообщение (в немодальном окне) с предварительно записанным сообщением. Данное действие позволяет использовать переменные, в которые будут записаны данные из пакета, вызвавшего срабатывание предупреждения. Ниже приведён список переменных:

  %SMAC% -- MAC-адрес источника.
  %DMAC% -- MAC-адрес получателя.
  %SIP% -- IP-адрес источника.
  %DIP% -- IP-адрес получателя.
  %SPORT% -- порт-источник.
  %DPORT% -- порт-получатель.
  %ETHERPROTO% -- имя Ethernet-протокола.
  %IPPROTO% -- имя IP-протокола.
  %SIZE% -- размер пакета.
  %FILE% -- путь к временному файлу, содержащему захваченный пакет.

  Например, в сообщении "SYN-пакет получен от %SIP%", в появившемся окне текст %SIP% будет замещён на IP- адрес источника пакета, вызвавшего срабатывание. Если использовать переменную %FILE%, в папке временных файлов будет создан файл .NCF, удаление данного файла – ответственность вашего обработчика данных. Не используйте переменные в предупреждениях, срабатывающих по значению **Байт в секунду** или **Пакетов в секунду**, так как они не вызываются каким-либо конкретным пакетом.

- **Произнести сообщение:** дать Windows команду произнести сообщение вслух с помощью встроенного механизма речевого воспроизведения текста. Если в вашей версии Windows нет этого механизма, то данная опция будет недоступна. По умолчанию в состав Windows включен лишь англоязычный речевой модуль, так что Windows может оказаться не в состоянии корректно воспроизвести сообщения, введенные не на английском языке. В тексте сообщения вы можете использовать переменные, описанные выше для опции **Показать сообщение**.

- **Звуковой сигнал**: Проигрывает указанный WAV-файл.

- **Запустить программу**: Запускает указанный EXE- или COM-файл. В поле **Параметры** можно задать параметры командной строки, если они требуются для запуска приложения. Можно использовать переменные, описанные в пункте **Показать сообщение**, чтобы передать программе информацию о пакете, вызвавшем срабатывание предупреждения.

- **Послать E-mail по адресу**: Отправляет E-mail по указанному адресу. ОБЯЗАТЕЛЬНО укажите SMTP-сервер, которым должен пользоваться CommView при отправке. Для этого нажмите кнопку **Настройка E-mail,** задайте установки SMTP-сервера и отправьте пробное письмо. Зачастую, оповещения по электронной почте можно использовать для отправки сообщений на пейджер, в виде SMS на мобильный телефон или пейджер. Например, чтобы послать сообщение абоненту ICQ, укажите адрес E-mail в виде ICQ_USER_UIN@pager.icq.com, где ICQ_USER_UIN ваш номер в системе ICQ, а в свойствах ICQ установите "Разрешить EmailExpress messages". Подробнее о настройках службы SMS вы можете узнать у своего сотового оператора. В поле **Добавить текст** можно ввести произвольное сообщения для E-Mail. Вы можете использовать переменные, описанные в секции **Показать сообщение**.

- **Включить правила захвата**: Включает Универсальные правила; укажите названия правил, если требуется несколько правил, перечислите их названия через запятую (или точку с запятой).

- **Выключить другие предупреждения**: Выключает ненужные предупреждения; укажите название предупреждения. Если требуется отключить несколько предупреждений, перечислите их названия через запятую (или точку с запятой).

- **Начать запись пакетов**: Включает автосохранение (смотрите главу Ведение Log-файлов); CommView начнёт запись перехваченных пакетов на диск.

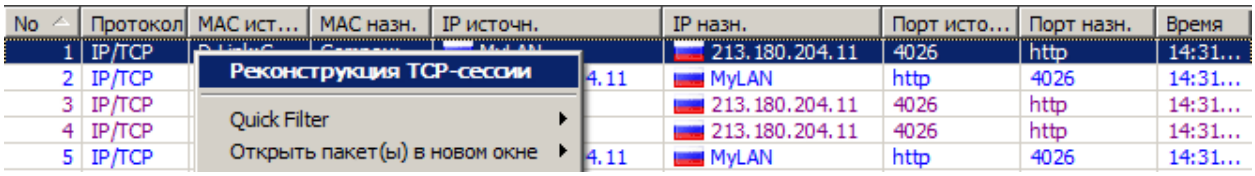
- **Завершить запись пакетов**: Выключает автосохранение.

Нажмите **OK**, чтобы сохранить настройки и закрыть диалог настройки предупреждений.

Все события, и относящиеся к ним действия, перечисляются в поле **Запись Событий**, которое находится под списком предупреждений.

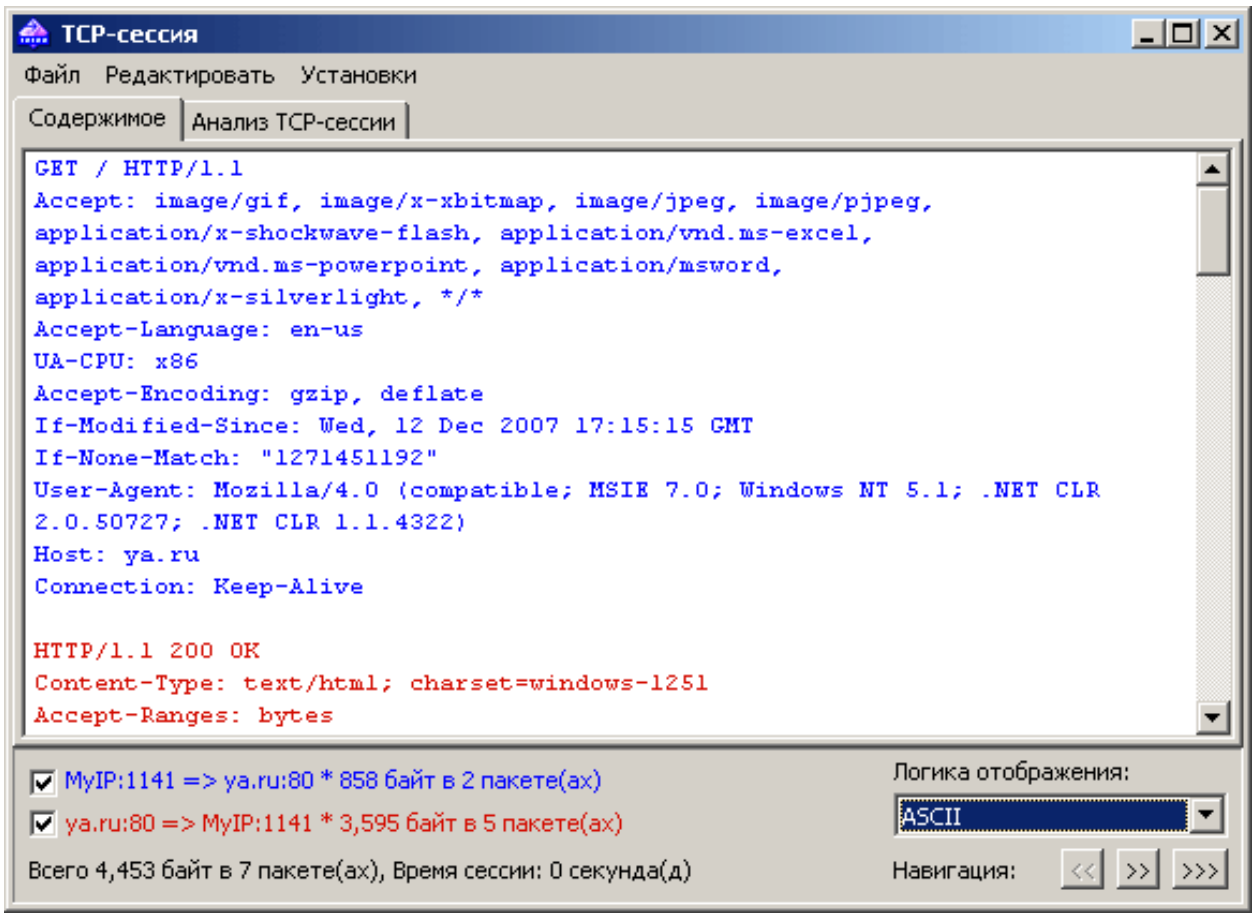
Реконструкция TCP-сессий

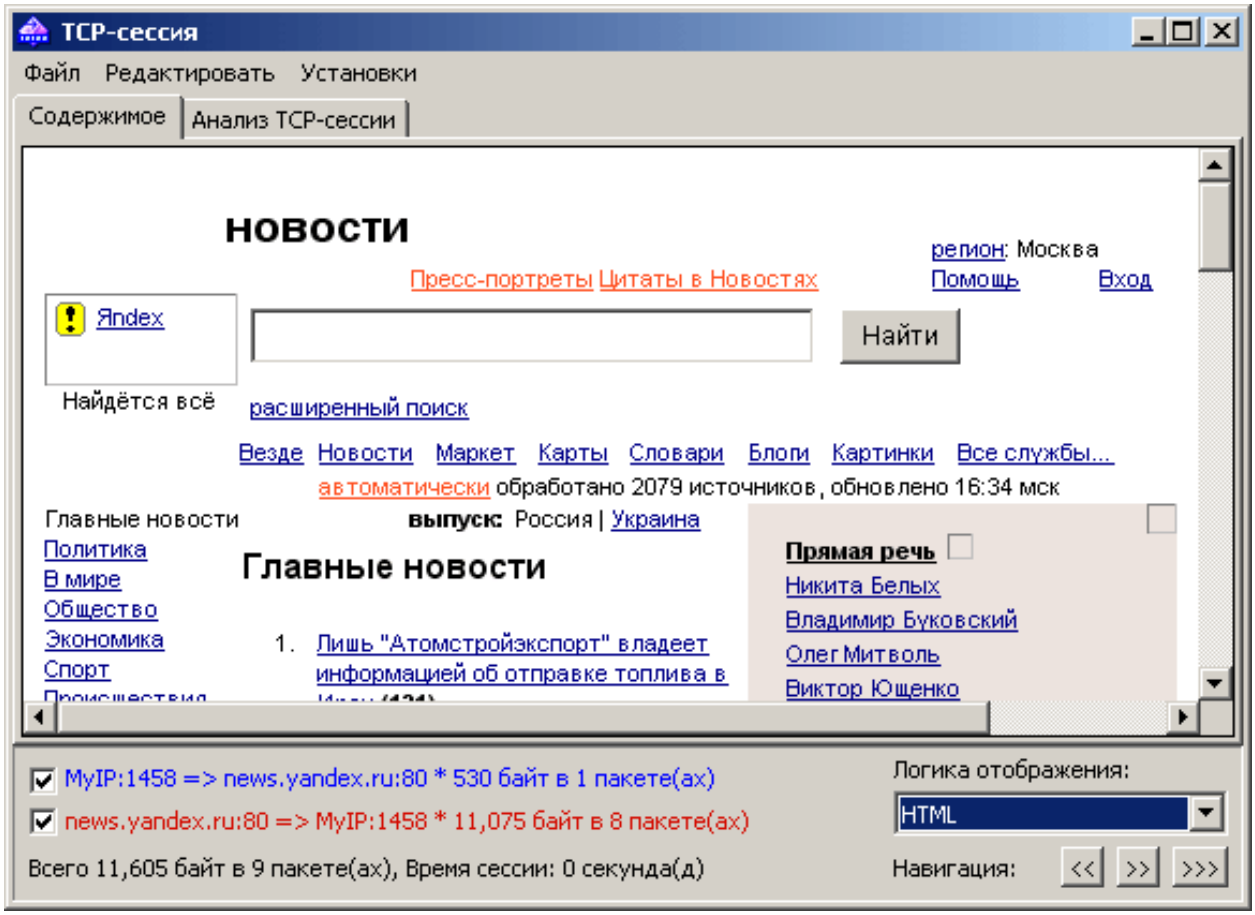
С помощью этой утилиты можно просмотреть процесс обмена между двумя хостами по TCP. Чтобы восстановить TCP- сессию, необходимо сначала выбрать пакет TCP в закладке **Пакеты**. В зависимости от установок (**Искать начало сессии при реконструкции TCP-сессий** в меню **Настройка** => **Установки** => **Декодер**), сессия будет восстановлена начиная с выбранного пакета, который может оказаться в середине сессии, либо с ее начала. Найдя и выбрав нужный пакет, щёлкните правой кнопкой мышки на нём, в появившемся меню выберите **Реконструкция TCP-сессии**, как показано здесь:



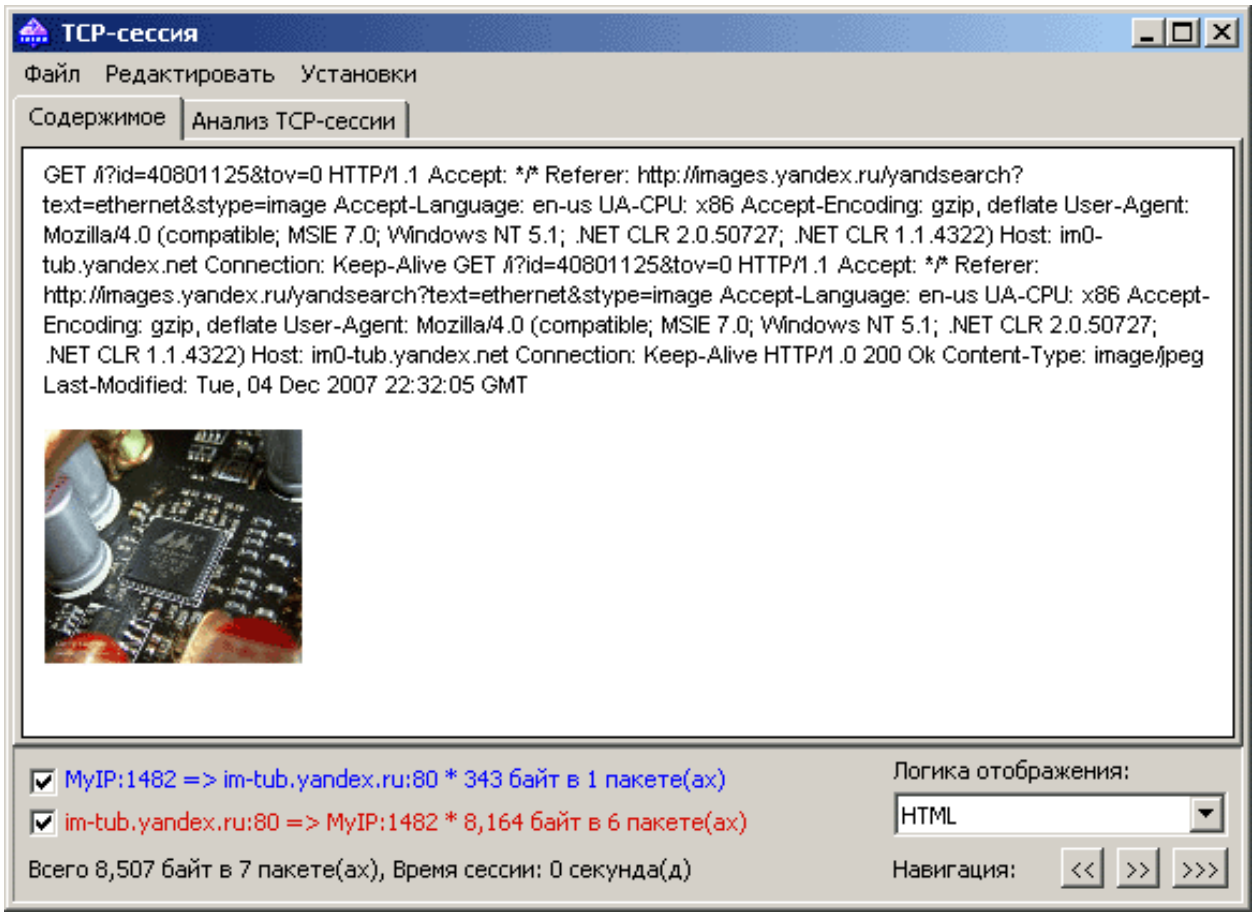
Процесс восстановления лучше всего работает для текстовых протоколов, таких как POP3, Telnet, или HTTP. Возможно также восстановление процесса пересылки большого ZIP-архива, но на обработку нескольких мегабайт данных CommView потребуется слишком много времени. Кроме того, в большинстве случаев полученная информация будет бесполезна. В закладке **Содержимое** показаны фактические данные по сессии, а в закладке **Анализ TCP-сессии** показан поток реконструированной TCP-сессии.

Ниже показан пример реконструкции HTTP-сессии, содержащей данные HTML, в режимах ASCII и HTML соответственно:


TCP-сессия
Файл Редактировать Установки
Содержимое Анализ TCP-сессии
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword,
application/x-silverlight, */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
If-Modified-Since: Wed, 12 Dec 2007 17:15:15 GMT
If-None-Match: "1271451192"
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR
2.0.50727; .NET CLR 1.1.4322)
Host: ya.ru
Connection: Keep-Alive
HTTP/1.1 200 OK
Content-Type: text/html; charset=windows-1251
Accept-Ranges: bytes
MyIP:1141 => ya.ru:80 * 858 байт в 2 пакете(ах)
ya.ru:80 => MyIP:1141 * 3,595 байт в 5 пакете(ах)
Всего 4,453 байт в 7 пакете(ах), Время сессии: 0 секунда(д)
Логика отображения:
ASCII
Навигация:
<< >> >>>


TCP-сессия
Файл Редактировать Установки
Содержимое Анализ TCP-сессии
НОВОСТИ
регион: Москва
Пресс-портреты Цитаты в Новостях
Помощь Вход
Яndex
Найти
Найдётся всё
расширенный поиск
Везде Новости Маркет Карты Словари Блоги Картинки Все службы...
автоматически обработано 2079 источников, обновлено 16:34 мск
Главные новости
выпуск: Россия | Украина
Политика
В мире
Общество
Экономика
Спорт
Главные новости
1. Лишь "Атомстройэкспорт" владеет информацией об отправке топлива в
Прямая речь
Никита Белых
Владимир Буковский
Олег Митволь
Виктор Ющенко
MyIP:1458 => news.yandex.ru:80 * 530 байт в 1 пакете(ах)
news.yandex.ru:80 => MyIP:1458 * 11,075 байт в 8 пакете(ах)
Всего 11,605 байт в 9 пакете(ах), Время сессии: 0 секунда(д)
Логика отображения:
HTML
Навигация:
<< >> >>>

В режиме отображения HTML гипертекстовые страницы не содержат графических объектов, поскольку в рамках протокола HTTP изображения передаются отдельно. Для просмотра изображений обычно требуется перейти к следующей TCP-сессии. Ниже приведён пример HTTP-сессии, содержащей графические объекты, которые отображаются гипертекстовом режиме:



По умолчанию, CommView разархивирует web-трафик, сжатый с помощью GZIP, и восстанавливает изображения из бинарных потоков данных. Чтобы выключить эти опции, воспользуйтесь закладкой **Декодер.**

Можно игнорировать данные из определенного источника, установив соответствующий флажок в нижней части окна. Для удобства входящие и исходящие данные помечены разным цветом. Если вы хотите изменить цветовую гамму, выберите **Установки => Цвета** и воспользуйтесь палитрой. Можно включить или выключить перенос слов: **Установки => Перенос по словам**.

Выпадающее меню **Логика отображения** позволяет просматривать выбрать режимы просмотра **ASCII** (обычный текст), **HEX** (шестнадцатеричные данные), **HTML** (web-документы и картинки), **EBCDIC** (кодировка, используемая в мейнфреймах IBM) и **UTF-8** (юникод). Учтите, что результаты просмотра данных в режиме HTML могут выглядеть несколько иначе, чем при просмотре настоящим браузером (вы не увидите графические объекты и т. п.), однако вполне можно представить, как выглядела данная страница на самом деле.

Выбрать вид отображения по умолчанию можно в закладке **Декодер.**

Кнопки навигации позволяют осуществлять переход между предыдущей и последующей TCP-сессиями. Первая кнопка "вперёд" **[>>]** перейдёт к следующей сессии между теми же хостами, что и при первом вызове реконструкции. Вторая кнопка "вперёд" **[>>>]** перейдёт к следующей сессии между любыми двумя хостами. Если в буфере несколько сессий, рекомендуется начинать реконструкцию с самой первой, так как кнопка возврата **[<<]** не сможет перейти на сессию, предшествующую той, с которой началась реконструкция.

Полученные данные вы можете записать на диск в двоичном виде, в текстовом или RTF-формате, выбрав **Файл => Сохранить как…**. Кроме того, выбрав **Редактировать** => **Найти…**, можно выполнить поиск строки в пределах текущей сессии.

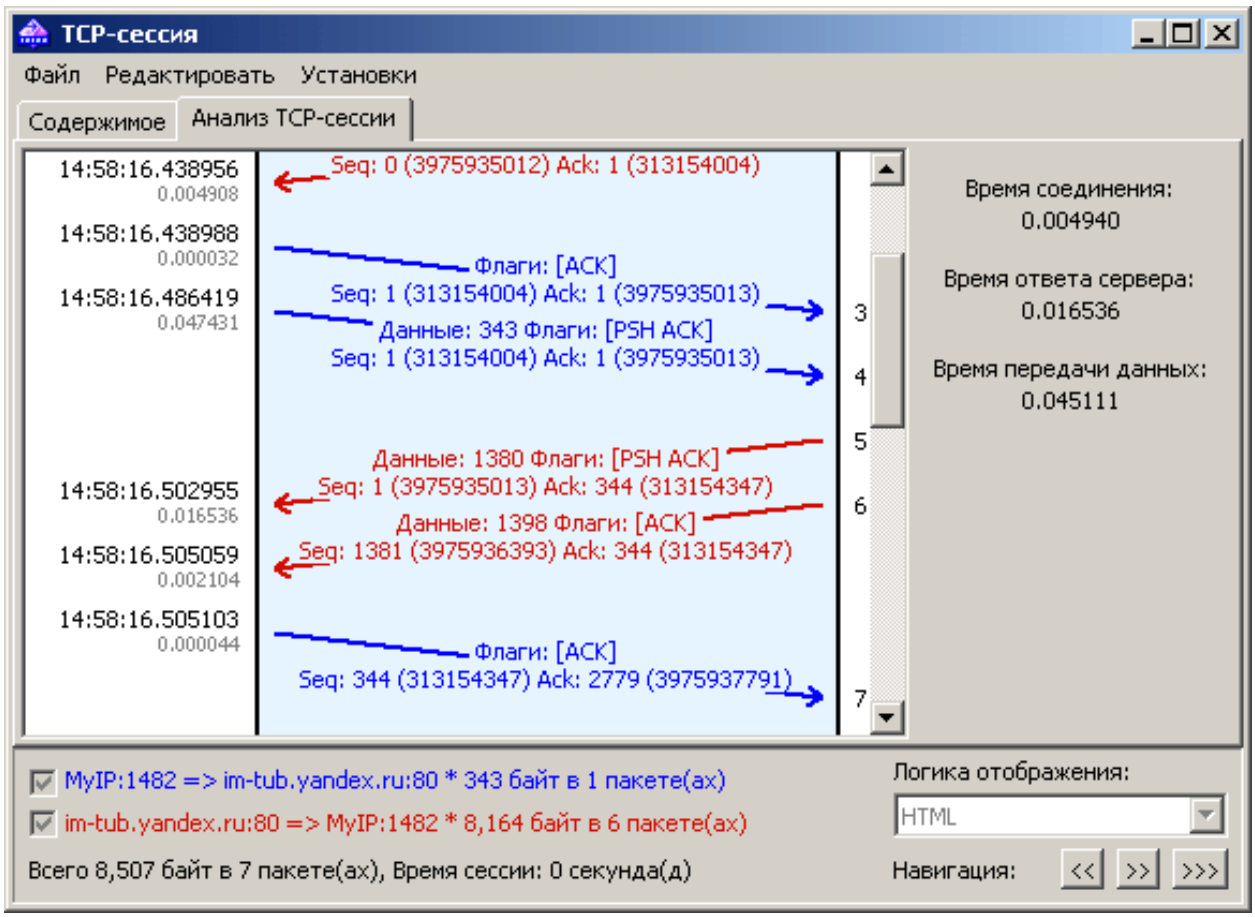
Анализ сессий

В закладке **Анализ TCP-сессии** окна **TCP-сессия** показывается восстановленная TCP-сессия в графическом виде. Здесь вы увидите потоки данных в этой сессии, ошибки, задержки и факты повторной передачи потерявшейся информации.

Для каждого пакета сессии показана следующая информация:

- Флаги TCP.
- Абсолютные и относительные значения SEQ и ACK.
- Время прибытия пакета.
- Временной интервал между текущим и предыдущим пакетами.
- Номер пакета в восстановленной сессии.

Если пакет содержит ошибки, то будет показано текстовое описание этих ошибок справа от картинки. Когда вы наведете курсор мыши на пакет, во всплывающем окне будет показано его содержимое при условии, что пакет содержит данные. Помните, что в поле **Логика отображения** задается способ декодирования данных во всплывающем окне. Пример окна анализа TCP-сессии показан ниже.



В правой панели показана основная статистика для данной сессии:

Время соединения – время, затраченное на установление TCP-соединения. Иными словами, это время трехстороннего обмена по TCP (SYN => SYN ACK => ACK).

Время ответа сервера – время с момента начального запроса клиента до первого отклика сервера.

Время передачи данных – время между первым и последним ответом сервера (0 в том случае, если был всего один ответ от сервера).

Вы можете сохранить графическое представление восстановленной TCP-сессии в файлы BMP, GIF или PNG, кликнув по рисунку правой кнопкой мыши и выбрав в контекстном меню **Сохранить изображение как…** . Сессия с большим количеством пакетов будет разбита на несколько файлов.

Реконструкция UDP-потоков

Этот инструмент во многом схож с аналогичным инструментом для реконструкции TCP-сессий, описанным в предыдущей главе; вы можете найти в ней подробную информацию. Пожалуйста, обратитесь к ней в случае каких-либо вопросов. Однако, поскольку в отличие от протокола TCP, UDP-протокол не требует установления соединения, между реконструкциями TCP-сессий и UDP-потоков есть следующие различия:

- Отсутствует вкладка **Анализ TCP-сессии**, поскольку UDP не предусматривает наличия сессий, SEQ или ACK.
- Поскольку в UDP отсутствуют SYN или FIN, все пакеты между IP-адресами и соответствующими портами считаются принадлежащими одному потоку.

Поиск пакетов

Для поиска пакетов, в которых содержится определенный текст или адрес, используйте диалог поиска (**Поиск => Найти пакет)**. Введите подстроку для поиска, выберите тип данных (**Строка** или **Hex**) и нажмите **Найти далее**. Программа найдет пакеты, удовлетворяющие критерию поиска и покажет их в закладке **Пакеты**.

Текст можно ввести как строку, шестнадцатеричное значение, MAC- или IP-адрес. Поиск текстовых строк будет осуществлен как в ASCII, так и в формате Unicode (UTF-8 и UTF-16). Hex-строка используется для ввода непечатаемых символов: просто введите шестнадцатеричную строку, например, AD0A027804.

Для регистрозависимого поиска установите флаг **С учетом регистра**. Для поиска строки, которая начинается с определенного смещения, установите флаг **Со смещения (hex)**. Помните, что смещение шестнадцатеричное и начинается с нуля (если вы ищите первый байт пакета, то значение смещения равно 0). Также вы можете выбрать направление поиска: **Вверх** или **Вниз**.

Статистика и отчёты

Выбрав в меню **Вид => Статистика**, можно ознакомиться с такими параметрами сетевой статистики сегмента LAN или вашего компьютера, как количество пакетов в секунду, байтов в секунду, или распределение протоколов Ethernet, IP и субпротоколов. Дважды щёлкнув по диаграммам, их можно скопировать в буфер обмена. Для удобства просмотра секторных диаграмм, их можно вращать с помощью двух небольших кнопок в правом нижнем углу.

Данные каждой страницы можно сохранить или в формате bitmap или в текстовом файле CSV. Для этого воспользуйтесь контекстным меню или просто перетащите объект мышкой. Выбрав пункт меню **Отчёт**, можно создавать автоматические отчёты в HTML или текстовом формате CSV.

Сетевая статистика может строиться на базе всех пакетов, проходящих через адаптер, или с учётом правил, установленных на данный момент. Если требуется, чтобы в статистике учитывались лишь текущие правила, следует отметить флаг **Apply current rules (С учётом действующих правил)**.

Общее

Гистограммы вида "Пакетов в секунду" и "Байт/бит в секунду", индикатор использования пропускной способности (удельный трафик, делённый на номинальную скорость сетевого адаптера или модемного соединения), а также общее количество пакетов и байт.

Протоколы

Распределение Ethernet-протоколов: ARP, IP, SNAP, SPX и т. д. Выпадающее меню **Построить по…** позволяет выбрать методы: по числу пакетов или числу байт.

IP-протоколы

Распределение IP-протоколов. Выпадающее меню **Построить по…** переключает методы подсчёта: по количеству пакетов или по количеству байт.

IP-подпротоколы

Распределение основных IP-протоколов уровня приложения: HTTP, FTP, POP3, SMTP, Telnet, NNTP, NetBIOS, HTTPS и DNS. Чтобы добавить собственные протоколы нажмите кнопку **Настройка**. Можно задать до восьми протоколов, введя название, тип IP-протокола (TCP/UDP) и номер порта. Выпадающее меню **Построить по…** переключает методы подсчёта: по количеству пакетов или по количеству байт.

Размеры

Распределение размера пакетов.

Хосты по MAC-адресу

Список активных LAN-хостов по MAC-адресам, со статистикой передачи данных. MAC-адресам можно присвоить псевдонимы (алиасы). Если в вашей сети очень много multicast-пакетов и таблица Hosts by MAC слишком перегружена данными – можно сгруппировать их в одну строку GroupedMulticast. Эта опция включается флажком **Группировать мультикаст-адреса.** Обратите

внимание: группироваться будут только вновь получаемые пакеты. Данные, полученные до момента включения данной опции, не будут группироваться.

Хосты по IP-адресу

Список активных LAN-хостов по IP-адресам, со статистикой передачи данных. Поскольку IP-пакеты, накапливаемые программой, могут приходить с неограниченного числа IP-адресов (как внутренних, так и внешних), по умолчанию данная закладка не отображает никакой статистики. Чтобы получить её, необходимо задать диапазон IP-адресов в соответствующем поле. Задаваемый диапазон должен принадлежать вашей сети. Можно задать несколько диапазонов, но общее число IP-адресов не может превышать 1000. Чтобы удалить диапазон, щёлкните по нему правой кнопкой мыши и выберите соответствующую команду (**Удалить диапазон, Удалить все диапазоны)**. IP-адресам можно присвоить псевдонимы (алиасы).

Матрица по MAC-адресу

Эта страница показывает общение узлов сети в графической форме, опираясь на значения MAC-адресов. Компьютеры, представленные их MAC-адресами, расположены по кругу, а сессии между ними показаны линиями, соединяющими соответствующие узлы. Подведя мышку к узлу, вы увидите все сессии, имевшиеся у данного компьютера с остальными. Меняя значение поля **Самые активные пары**, вы можете управлять количеством отображаемых связей в матрице. Меняя значение поля **Считать последних пар**, вы можете управлять числом пар адресов, отслеживаемых программой для построения матрицы. Если в вашем сегменте наблюдается слишком много широковещательных или multicast пакетов, переполняющих матрицу – вы можете игнорировать такие пакеты, установив соответствующий флажок: **Игнорировать бродкасты** или **Игнорировать мультикасты.**

Матрица по IP-адресу

На этой странице показана графическая матрица обмена узлами сети со своими IP-адресами. Узлы сети (их IP-адреса) расположены по кругу, а сессии между ними показаны линиями, соединяющими соответствующие узлы. Подведя мышь к узлу, вы увидите все сессии, происходившие у данного между данным узлом и остальными. Меняя значение поля **Самые активные пары**, вы можете управлять количеством отображаемых связей в матрице. Меняя значение поля **Считать последних пар**, вы можете управлять числом пар адресов, отслеживаемых программой для построения матрицы. Если в вашем сегменте наблюдается слишком много широковещательных или multicast пакетов, излишне перегружающих матрицу – вы можете игнорировать такие пакеты, установив соответствующий флажок: **Игнорировать бродкасты** или **Игнорировать мультикасты.**

Ошибки

Отображает сведения об ошибках Ethernet, получаемые непосредственно из адаптера. В их числе такие типы ошибок:

Rx CRS Errors

Количество кадров, принятых с ошибками контрольной суммы (CRC) или проверки последовательности кадров (FCS).

Rx Alignment Errors

Количество кадров, принятых с ошибками выравнивания.

Rx Overrun

Количество кадров, не принятых из-за ошибок переполнения адаптера.

Tx One Collision

Количество кадров, переданных успешно после единственной коллизии.

Tx More Collisions

Количество кадров, переданных успешно после нескольких коллизий.

Tx Deferred

Количество кадров, переданных успешно после того, как адаптер отложил передачу хотя бы один раз.

Tx Max Collisions

Количество кадров, не переданных из-за многочисленных коллизий.

Tx Underrun

Количество кадров, не переданных из-за несвоевременной загрузки адаптера данными.

Tx Heartbeat Failure

Количество кадров, переданных успешно, без обнаружения SQE (нарушений качества сигнала).

Tx Times CRS Lost

Количество пропаданий сигнала контрольной суммы во время передачи пакета.

Tx Late Collisions

Количество коллизий, обнаруженных за пределами окна.

Rx Frames w/Errors

Количество кадров, принятых адаптером, но не переданных протоколам из-за ошибок.

Rx Frames w/o Errors

Количество кадров, успешно принятых адаптером и переданных соответствующим протоколам.

Tx Frames w/Errors

Количество кадров, не переданных по каким-либо причинам.

Tx Frames w/o Errors

Количество успешно переданных кадров.

Замечания:

- Dial-up-адаптеры не поддерживаются, только карты Ethernet.
- Ваш адаптер может не поддерживать все вышеперечисленные поля. Некоторые производители выпускают карты, из которых можно получить всю необходимую информацию, но некоторые – нет.
- В отличие от остальных данных в окне **Статистика**, данные закладки **Ошибки** не сбрасываются при нажатии кнопки **Сброс**. Счётчик сбрасывается при каждой перезагрузке компьютера.

Отчёт

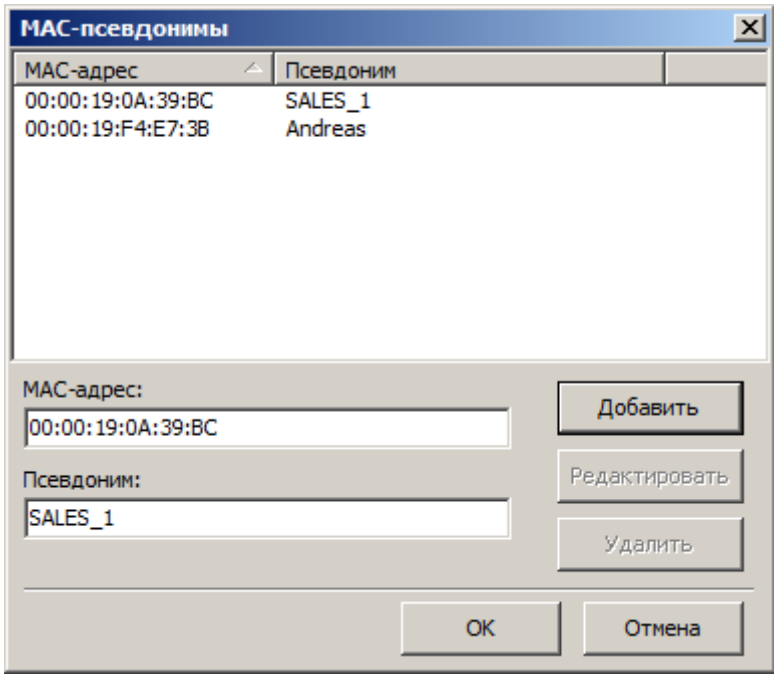
Закладка позволяет настроить автоматически создаваемые отчёты в форматах HTML (с графическим представлением гистограмм) или в формате CSV.

Возможно получение статистики по ранее собранным пакетам. Для этого загрузите файл в утилиту просмотра Log-файлов и выберите **Файл** => **Получить статистику**. При желании можно сбросить уже имеющиеся значения в окне **Статистика**. Эта функция не покажет распределение пакетов во времени, она ограничена общими сведениями, гистограммами протоколов и таблицами хостов LAN.

Использование псевдонимов (алиасов)

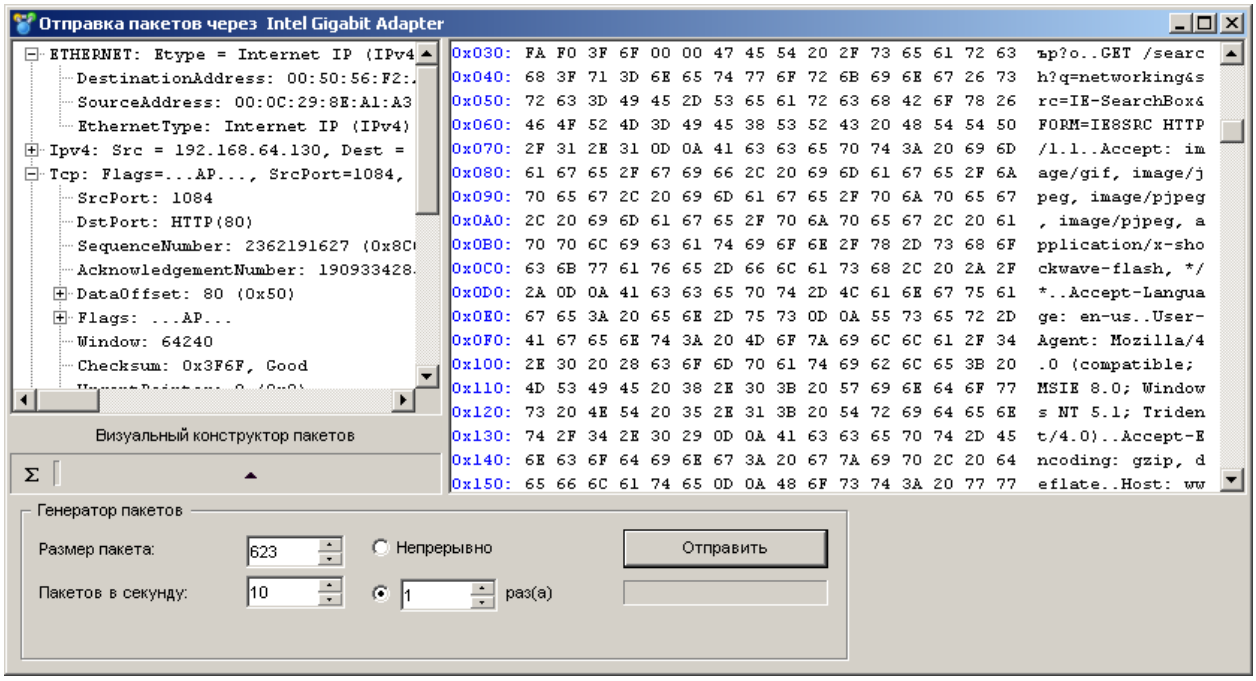
CommView может подставлять вместо MAC- или IP-адресов легко читаемые и легко запоминаемые имена при отображении пакетов в закладках **Пакеты** и **Статистика**. Например, 00:00:19:2D:0D:35 станет GATEWAY2, а ns1.earthlink.com превратится в MyDNS.

Чтобы создать имя (алиас) для MAC-адреса, щёлкните правой кнопкой мыши на пакете и выберите в контекстном меню **Создать псевдоним > используя MAC источника** или **используя MAC получателя.** Появится окно с уже заполненным полем MAC-адреса, теперь можно ввести подходящее имя. Другой способ: выберите в меню **Настройка => Псевдонимы** и заполните поля вручную. Удалить имя или стереть весь список имён можно, щёлкнув правой кнопкой мыши в окне **Псевдонимы** и выбрав **Удалить запись** или **Очистить все**. Точно так же происходит работа с IP-адресами. Если новая запись IP-имени создаётся щелчком правой кнопки мыши по пакету, поле имени автоматически заполняется именем хоста (если оно доступно) и его можно редактировать.



Генератор пакетов

Эта утилита позволяет создавать и передавать пакеты через сетевой адаптер. Выберите в меню **Инструменты => Генератор пакетов**. Или, выбрав пакет в закладке **Пакеты**, щёлкните на нем правой кнопкой мыши, а затем выберите команду **Отправить пакет**.



Обратите внимание на то, что **Генератор Пакетов** не может и не должен быть использован для посылки пакетов с уровня приложений, то есть он **не** следит за инкрементом значений SEQ, ACK, значениями контрольных сумм, размерами пакетов и т. д. Если требуется переслать поток TCP, следует воспользоваться Winsock-приложением. **Генератор Пакетов** предназначен для воспроизведения уже захваченного трафика, тестирования брандмауэров и систем обнаружения вторжения, а так же для других целей, где требуется ручная обработка пакетов.

Генератор пакетов позволяет изменять содержимое пакета и одновременно показывать его в декодированном виде в левом окне. Можно создавать любые виды пактов, получая полный контроль над их содержимым. Для пакетов IP, TCP, UDP и ICMP контрольная сумма автоматически корректируется при нажатии на кнопку "сигма". Для помощи в редактировании пакета предусмотрен специальный модуль - Визуальный конструктор пакетов; его можно вызвать, нажав на соответствующую кнопку.

Воспользуйтесь кнопкой (с изображенной на ней стрелкой) для получения списка доступных шаблонов пакетов. В программе есть шаблоны **TCP**, **UDP** и **ICMP** пакетов; их использование зачастую оказывается удобнее, чем ввод 16-ричных значений в окне редактора. Возможно, в шаблонах TCP-, UDP- и ICMP-пакетов вам потребуется изменить поля MAC- и IP- адреса, номера портов, SEQ- и ACK-номера и т. д. Вместо встроенных шаблонов можно использовать собственные, переместив пакет из закладки **Пакеты** в окно шаблона в **Генераторе Пакетов**. В случае переноса нескольких пакетов, только первый из них будет использован в качестве шаблона. В списке файлов шаблонов появится новый файл – New Template, который можно переименовать по

правому щелчку мыши, выбрав **Rename** или удалить, выбрав **Delete**. После выбора шаблона, он будет загружен в окно редактора, где можно изменить содержимое пакета перед его отправкой.

Кроме того, можно скопировать произвольные файлы NCF в поддиректорию TEMPLATES. CommView будет отображать в списке шаблонов файл(ы) NCF, обнаруженные в поддиректории TEMPLATES. Если в файле NCF будет больше одного пакета – в качестве шаблона будет использован только первый пакет.

Ниже приведены параметры передачи:

Размер пакета – задать размер пакета.
Пакетов в секунду – установить частоту передачи пакетов. Будьте осторожны и не превышайте пропускную способность соединения! Попытка переслать 5000 раз в секунду пакеты длиной в 1000 байт превысит возможности 10Mbit-ного сетевого адаптера.
Непрерывно – включить режим непрерывной передачи, пока не нажмёте **Остановить**.
Количество раз – задать число отправок пакета в сеть.
Отправить/Остановить – возобновить/остановить передачу пакета.

Работа с несколькими пакетами одновременно

Генератор пакетов может передавать несколько пакетов одновременно. Выберите нужные вам пакеты из списка и правым щелчком мыши вызовите **Генератор Пакетов**. Кроме того, можно просто перетащить файл с пакетами (в любом поддерживаемом формате) в окно **Генератора Пакетов**. При работе в этом режиме декодер и редактор пакетов отключаются.

Сохранение отредактированных пакетов

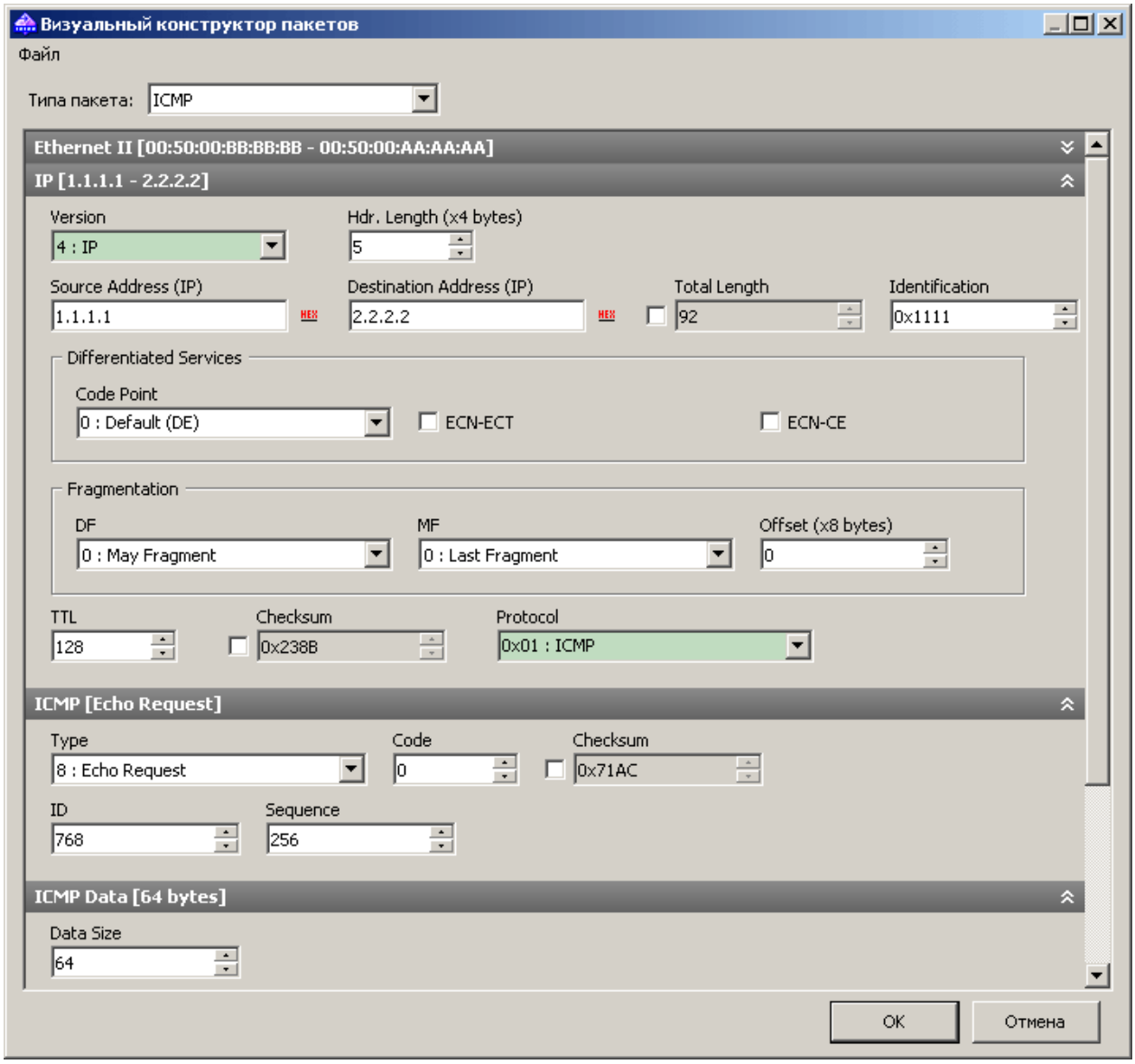
Если вы отредактировали пакет и хотите его сохранить, просто перетащите мышью дерево декодера на рабочий стол или в любую папку. Будет создан новый файл в формате NCF с именем PACKET.NCF. Если требуется редактировать и посылать несколько пакетов – делайте это по очереди, вынося каждый пакет на рабочий стол и задавая ему новое имя. Затем откройте окно **Просмотра Log-файлов**, внесите в него отредактированные пакеты, выберите их и, удерживая клавишу Shift, активизируйте из контекстного меню **Генератор Пакетов**.

ВНИМАНИЕ:

1. Пользуйтесь генератором пакетов только в том случае, если вы точно знаете, какова ваша цель. Передача пакетов в сеть может привести к непредсказуемым последствиям. Советуем пользоваться этим инструментом лишь в том случае, если вы опытный системый администратор.
2. Чтобы избежать значительных задержек при передаче, убедитесь, что кроме вашаго компьютера в сети есть еще по крайней мере один.

Визуальный конструктор пакетов

Визуальный конструктора пакетов – это модуль, предназначенный для редактирования пакетов и их генерации в Генераторе пакетов. С помощью конструктора вы сможете быстро и безошибочно создать новый пакет либо редактировать существующий, используя при этом готовые шаблоны. После создания или редактирования пакет можно отправить в сеть с помощью Генератора пакетов.



Поддерживается генерация пакетов TCP, UDP, ICMP (на основе версий 4 и 6 протокола IP), а также пакетов ARP. Для создания пакета выберите его вид в выпадающем списке **Тип пакета**. Все значения по умолчанию полей пакета будут заполнены автоматически, но могут быть впоследствии отредактированы.

Пакеты ICMP, TCP, UDP и ARP состоят из нескольких отдельных слоев; интерфейс Визуального конструктора пакетов создан по такому же принципу. Опции, имеющие отношение к одно и тому же слою, расположены на отдельной панели. К примеру, пакет TCP состоит из 4 слоев; поля

адресов **Source MAC** и **Destination MAC** расположены в панели **Ethernet II** (канальный уровень); поля **Scr Port** и **Dst Port** находятся в панели **TCP** (транспортный уровень). Если вы хотите скрыть панель, нажмите кнопку Свернуть/Развернуть, расположенную в правой верхней части панели.

Помните, что некоторые значения в "родительском" уровне могут влиять на тип пакета в низших уровнях, поэтому изменения в верхних уровнях могут привести к перестройке более низких уровней пакета. Таким образом, если вы измените тип протокола в панели Ethernet II (канальный уровень), то это приведет к перестройке всего пакета. Учтите также, что значения одних полей и низших уровней могут зависеть от значений других полей. Примеры таких полей: контрольные суммы и длины заголовков и/или данные с низших уровней. Визуальный конструктор пакетов вычисляет эти значения автоматически. Тем не менее, вы можете создавать и нестандартные пакеты. Для этого выберите опцию **Установить свои значения вместо используемых по умолчанию** и введите требуемые значения.

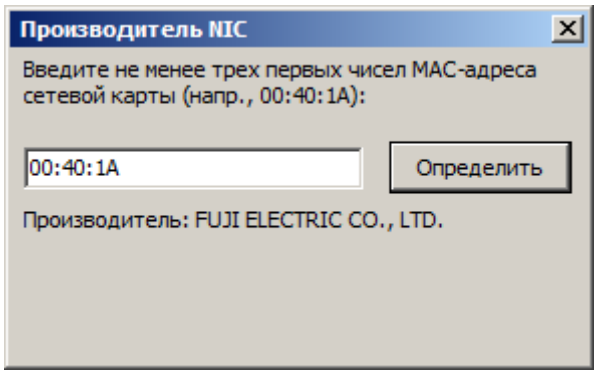
Замечание: визуальный конструктор пакетов помогает вам отслеживать корректность созданного пакета путем подсветки неверных или нестандартных значений красным цветом.

Несмотря на то, что в конструкторе пакетов предусмотрена поддержка только для протоколов TCP, UDP, ICMP и ARP, вы можете использовать его для редактирования пакетов других протоколов. В этом случае следует использовать шестнадцатеричный редактор.

После создания пакета вы можете его сохранить и потом снова загрузить в конструктор. Для этого используйте соответствующие команды меню **Файл**. Вы можете загрузить любой файл CommView с перехваченными пакетами (NCF); при этом помните, что если этот файл содержит более одного пакета, то будет загружен лишь первый пакет.

Определение изготовителя NIC

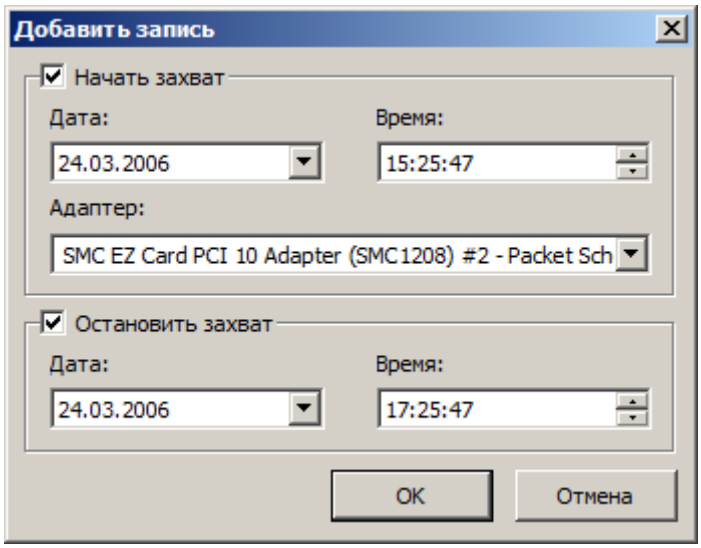
Первые 24 бита MAC-адреса сетевого адаптера позволяют однозначно определить имя фирмы-изготовителя. Этот 24-битный код имеет название OUI (Organizationally Unique Identifier). Чтобы определить название производителя, выберите **Инструменты => Определение изготовителя NIC**, введите MAC-адрес и нажмите **Определить**.



Список фирм находится в файле MACS.TXT, расположенном в папке CommView. Файл можно редактировать вручную.

Захват по расписанию

Утилита-планировщик позволяет задавать расписание сбора пакетов. Этой утилитой удобно пользоваться, когда требуется начать либо остановить сбор пакетов без постороннего наблюдения, например, в выходные или ночью. Чтобы добавить новое задание в расписание работы, зайдите в **Инструменты** => **Захват по расписанию**, и нажмите кнопку **Добавить**.



В поле **Начать захват** укажите дату и время, когда CommView должен начать перехват пакетов. В выпадающем списке **Адаптер** выберите требуемый адаптер. В поле **Остановить захват** укажите момент окончания перехвата пакетов. Заполнять оба поля **Начать захват** и **Остановить захват** необязательно. Если вы заполните только первое поле, перехват начнется, и будет продолжаться до момента остановки пользователем. Если вы заполните только второе поле, начать перехват придётся вручную, а остановка произойдет в указанное время.

Если CommView уже находился в режиме захвата пакетов к моменту начала работы по расписанию, и запланированный адаптер отличается от использованного в тот момент, CommView приостановит выполнение текущего задания, переключит адаптер и начнёт работу по расписанию.

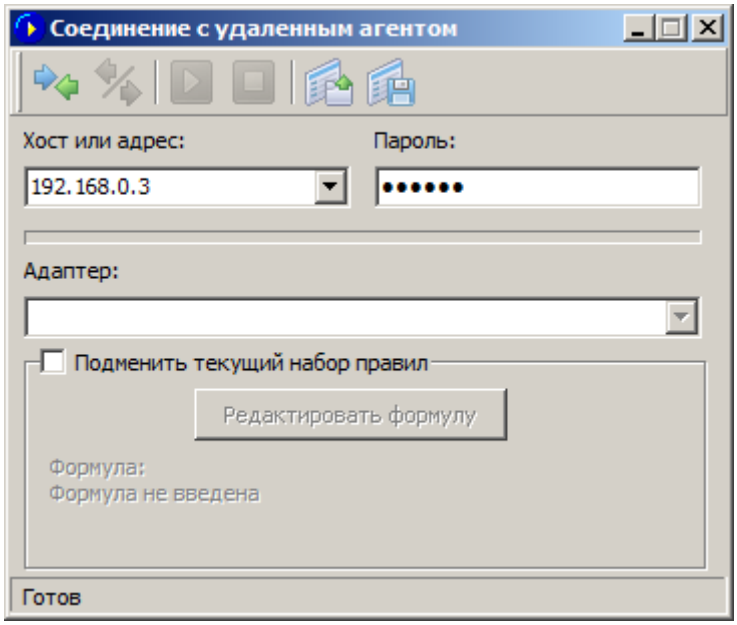
Важно: CommView выполняет работу по расписанию лишь в том случае, если он запущен.

Удаленный мониторинг (Remote Agent)

Программа **CommView Remote Agent**, являясь вспомогательным продуктом, позволяет пользователям **CommView** наблюдать трафик в удалённых сетях. Необходимо установить **Remote Agent** на компьютер в интересующей вас сети и затем использовать **CommView** для подключения к **Remote Agent**. Подключившись и введя пароль доступа, можно начинать сбор сетевой информации, как если бы ваш компьютер непосредственно находился в нужной сети.

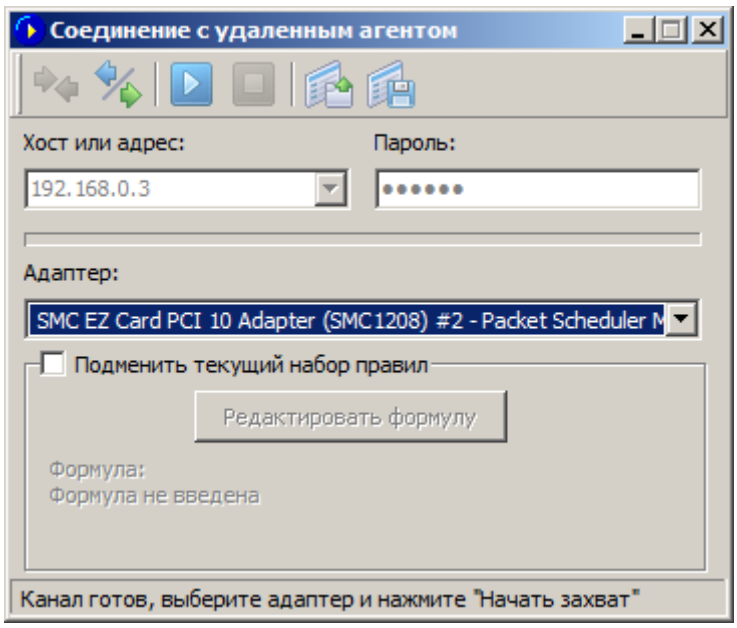
Важно: В данной главе описывается, каким образом использовать CommView для подключения к Remote Agent и как наблюдать за трафиком удаленно. Подробное описание установки и настройки программы Remote Agent находится в документации, поставляемой вместе с ней. Внимательно ознакомьтесь с описанием, прежде чем использовать программу. CommView Remote Agent можно скачать здесь.

Для включения режима удаленной выберите в меню **Файл => Режим удаленного мониторинга**. Под основной панелью инструментов CommView появится дополнительное поле. В окне адреса укажите IP-адрес компьютера, на котором запущен CommView Remote Agent, нажмите кнопку **Соединиться**. Если вы работаете через брандмауэр или прокси-сервер, а также, если в Remote Agent выбран нестандартный номер порта, нажав кнопку **Дополнительные установки сети**, укажите используемый порт и/или задайте параметры прокси-сервера SOCKS5.

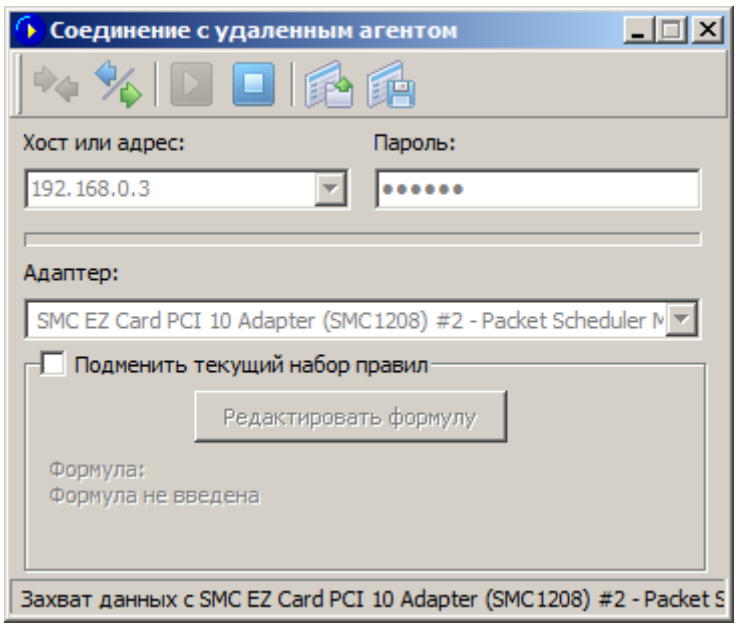


Чтобы установить новое соединение, нажмите на кнопку **Новое соединение Удаленного Агента** или загрузите ранее сохраненный профиль, нажав на **Загрузить профиль удаленного агента.**

В появившемся окне введите пароль доступа к Remote Agent и IP-адрес – будет установлено соединение. Об этом будет свидетельствовать сообщение "Связь установлена", а в окне выбора адаптеров появится список имеющихся на удалённом компьютере сетевых адаптеров.



Теперь необходимо установить фильтрацию пакетов в закладке **Правила**. Важно сконфигурировать фильтры так, чтобы трафик между Удаленным Агентом и CommView не превысил пропускную способность канала, иначе возникнут существенные задержки. Убедитесь, что установлены соответствующие фильтры на пакеты, которые не представляют интереса. Вы также можете самостоятельно задать правила перехвата для данного соединения и тем самым обойти текущую настройку правил CommView. Для этого установите флаг **Подменить текущий набор правил**, нажмите кнопку **Редактировать формулу** и введите новую формулу в соответствующее поле. Синтаксис формул такой же, как и в универсальных правилах. Завершив настройку, выберите адаптер из списка и нажмите кнопку **Начать захват**. Для быстрого и удобного использования в будущем CommView предлагает вам сохранить настройки текущего соединения. Для этого нажмите на кнопку **Сохранить профиль** и введите имя файла.



CommView начнёт перехват трафика удалённого компьютера. Для окончания мониторинга нажмите кнопку **Закончить захват**. Можно либо выбрать другой адаптер, либо отключиться от

Remote Agent, нажав кнопку **Разорвать связь**. Снимите флажок в меню **Файл => Режим удаленного мониторинга**, и CommView вернётся в местный режим работы.

Имейте в виду, что CommView может работать с несколькими Удаленными Агентами одновременно. Вы можете открыть несколько удаленных соединений (каждое со своими настройками и набором правил) и осуществлять перехват трафика с удаленных сегментов сети в рамках одного приложения CommView.

Использование RPCAP

Важно: В данной главе описывается функциональность, которая может не работать в соответствии с описанием в зависимости от того, как она реализована в программном обеспечении или оборудовании других производителей. Техническая поддержка по описываемым ниже функциям не оказывается.

В дополнение к возможностям удаленного мониторинга, обеспечиваемым CommView Remote Agent, CommView также позволяет получать трафик с удаленных хостов по протоколу RPCAP (Remote Packet Capture). Этот протокол поддерживается некоторыми типами оборудования (напр. точками доступа Aerohive) и программного обеспечения (напр. WinPcap).

Для включения режима удаленной работы выберите в меню **Файл => Режим удаленного мониторинга**. Под основной панелью инструментов CommView появится дополнительная панель. Нажмите на кнопку **Новое RPCAP-соединение,** чтобы открыть окно нового соединения.

Для соединения с удаленным устройством введите его **хост или IP-адрес**, укажите **порт** (по умолчанию RPCAP использует порт 2002), поставьте флаг **Авторизация пользователя** и введите имя **пользователя** и **пароль**, если это требуется, и поставьте флаг **Режим promiscuous**, если хотите осуществлять мониторинг в этом режиме. Нажмите кнопку **Соединиться** для установки соединения. После установки соединения вы увидите список доступных сетевых интерфейсов в выпадающем списке **Адаптер**. Выберите интерфейс и нажмите кнопку **Начать захват.**

Сбор трафика на логическом адаптере обратной связи (loopback)

CommView позволяет осуществлять перехват трафика с интерфейса обратной связи. В данном случае обмен пакетов с сетью происходит без участия сетевого адаптера. Дополнительный адаптер "Loopback" будет показан в выпадающем списке адаптеров.

Пакеты в логическом адаптере обратной связи посылаются и принимаются внутри данного компьютера, то есть адресуются сами себе. Обычно локального трафика практически нет, однако, он широко используется разработчиками сетевого ПО для отладки сетевых приложений. Данная функция в CommView создана именно для разработчиков сетевого ПО.

Сбор трафика на логическом адаптере ничем не отличается от реального, за исключением того факта, что для пакетов не вычисляются контрольные суммы. Обратите внимание на следующие особенности данного режима работы:

- CommView собирает пакеты со всех локальных IP-адресов. Сюда относятся адреса 127.0.0.1/255.0.0.0, но иногда может попадать и локальный адрес сетевого адаптера, например, 192.168.0.1.
- Перехватываются пакеты всех протоколов (TCP, UDP и т. д.), за исключением ICMP.
- Захватываются только успешно посланные/принятые пакеты. Например, вы не увидите пакетов SYN/RST, если соединение не состоялось из-за того, что порт-получатель закрыт.
- Сессии завершаются без уведомления; пакеты FIN не перехватываются.

Информация о портах

На этой странице (**Вид => Информация о портах**) показана таблица номеров портов и соответствующие им имена сервисов. Эта информация берется из файла SERVICES, который установлен Windows. Файл SERVICE располагается в директории **\system32\drivers\etc**. Если вы хотите добавить порты/имена сервисов, то можете редактировать этот файл вручную. CommView загружает этот файл при запуске, так что ваши изменения будут видны лишь после перезапуска программы.

Установка опций

В меню **Настройка => Установки** вы можете настроить некоторые опции программы.

Основные

Автозапуск захвата – установите этот флажок, если вы хотите, чтобы CommView начал перехват пакетов непосредственно после запуска программы. Если в системе несколько устройств, выберите из выпадающего списка то устройство, которое будет при этом использоваться.

Отключить распознавание DNS – установите этот флаг, если вы не хотите, чтобы CommView делал обратный DNS поиск IP-адресов. Если флажок установлен, то колонка **Имя хоста** закладки **Последние IP-соединения** будет пустой.

Преобразовывать номера портов в имена служб – установите этот флаг, если вы хотите, чтобы CommView отображал названия сервисов вместо номеров портов. Например, если этот флажок установлен, порт 21 показывается как ftp, а порт 23 как telnet. Программа преобразует численные значения в названия сервисов, используя файл SERVICES, инсталлированный системой. Файл SERVICES находится в каталоге \Winnt\system32\drivers\etc. Вы можете вручную редактировать этот файл, если хотите добавить другие названия портов/сервисов.

Преобразовывать MAC-адреса в псевдонимы – заменять MAC-адреса пакетов в закладке **Пакеты**. Создавать алиасы можно командой меню **Настройка => MAC-псевдонимы**.

Преобразовывать IP-адреса в псевдонимы– заменять IP-адреса пакетов в закладках **Пакеты** и **Статистика**. Создавать алиасы можно командой меню **Настройка => IP-псевдонимы**.

Преобразовывать IP-адреса в имена хостов в закладке "Пакеты" – установите этот флаг, если вы хотите, чтобы CommView отображал имена хостов вместо их IP-адресов в закладке **Пакеты**. Если этот флаг установлен, CommView сначала попробует найти алиас для данного адреса. Если алиаса нет, или не установлен флаг **Преобразовывать IP-адреса в псевдонимы**, CommView запросит внутренний кэш DNS. Если имя хоста не будет найдено, IP-адрес будет отображён в виде численного значения.

Использовать non-promiscuous режим – по умолчанию, CommView переводит сетевой адаптер в "беспорядочный" режим (promiscuous mode), состояние, в котором сетевой адаптер обнаруживает в сети все пакеты вне зависимости от их конечного адреса. Установка этого флага переводит сетевой адаптер в нормальный режим фильтрации пакетов. Воспользуйтесь им в случае, если политика сетевой безопасности вашей компании не разрешает тотальный мониторинг. Также используйте этот режим, если вы хотите снизить нагрузку на процессор при мониторинге лишь собственных входящих/исходящих пакетов, игнорируя при этом все транзитные.

Извещать об изменении списка адаптеров – установите этот флаг, если вы хотите, чтобы CommView показывал всплывающее сообщение при изменении числа активных сетевых адаптеров.

Показывать полный путь процессов – установите этот флаг, если требуется показать полный путь к процессу, который отсылает/принимает пакеты (вкладка **Последние IP-соединения** и дерево декодированных пакетов во вкладке **Пакеты**. Например, "C:\Files\Program.exe" - полный путь, а "Program.exe" - короткий).

Показывать упрощенные имена адаптеров– установите этот флаг, если требуется показать названия адаптеров в выпадающем списке таким же образом, как они показаны в Windows Network Connections.

Показывать сетку – показать линии сетки во всех списках пакетов.

Использование памяти

Хранение данных

Максимальное количество пактов в буфере – устанавливает максимальное количество пакетов, сохраняемых в памяти и которое можно отобразить в списке пакетов (вторая закладка). Например, если вы устанавливаете это значение равным 3000, только последние 3000 пакетов будут храниться в памяти и списке пакетов. Чем выше это значение, тем больше ресурсов потребляется программой. Если вы хотите иметь доступ к большему количеству пакетов, рекомендуем воспользоваться функцией автоматического сохранения - это позволит сохранить в файле все пакеты. Подробности в главе Ведение Log-файлов.

Максимальное количество строк в текущих IP-соединениях - устанавливает количество строк в закладке **Статистика**. Когда количество соединений превышает указанный предел, самые старые из неактивных соединений удаляются из списка.

Буфер драйвера - устанавливает размер буфера драйвера. Эта установка влияет на производительность программы: чем больше памяти выделено, тем меньше программа теряет пакетов. При низком трафике локальной сети или dial-up соединении размер буфера некритичен. При высоком уровне трафика в локальной сети, может понадобиться увеличить размер буфера, если программа начинает пропускать пакеты.

Текущие IP-соединения

Тип отображения – опция позволяет выбрать способ отображения последних соединений. В выпадающем списке будет показано описание выбранного способа отображения. В большинстве случаев рекомендуется пользоваться режимом **Smart**.

Задание локальных IP-адресов – это требуется сделать, если наблюдаемый LAN-трафик содержит множество транзитных пакетов, и в обмене участвуют как внешние, так и внутренние IP-адреса. В этом случае CommView не может определить, какие IP-адреса следует считать локальными, и может неверно распределить их по колонкам локальных и удалённых IP-адресов. В этом окне можно явно задать локальные сетевые адреса и маски подсети, чтобы в окне статистики содержалась достоверная информация. Все вышеописанное будет работать только при включенном режиме отображения **Smart**.

Добавлять цифровой PID к имени процесса – установите эту метку, если требуется показывать численные идентификаторы процессов после их названия в колонке **Процессы**.

Цвета

Цвета пакетов – устанавливает цвет отображения пакетов в закладке **Пакеты** в зависимости от направления (входящий, исходящий, транзитный). Чтобы изменить цвет, выберите направление пакета из списка и нажмите на прямоугольник с нужным цветом.

Расцветка заголовков пакета – установите этот флаг, если хотите, чтобы CommView задавал цвета содержимому пакетов. Если флаг установлен, программа отображает первые 8 уровней пакета, используя различные цвета. Чтобы изменить цвет, выберите тип заголовка, для которого вы хотите изменить цвет и нажмите на прямоугольник с нужным цветом.

Подсветка синтаксиса формул – задаёт цвета отображения ключевых слов в формулах составных правил.

Цвет выделенной части пакета – задаёт цвета отображения последовательности байт, выбранных в дереве декодирования. Например, если выбрать узел "TCP" в декодере, соответствующая часть пакета будет выделена данным цветом.

Декодер

Полностью разворачивать все узлы в окне декодера – установите этот флаг, если вы хотите, чтобы при выборе пакета все узлы в окне декодера автоматически разворачивались.

Разворачивать последние узлы – установите этот флаг и укажите количество узлов, если вы хотите, чтобы при выборе нового пакета из списка автоматически раскрывались последние узлы окна декодирования, в соответствие с установленным вами значением. По умолчанию раскрывается первый узел окна декодирования. Если установлен флаг **Полностью разворачивать все узлы в окне декодера**, то эта опция не имеет значения.

Уровень развертывания – установите число разворачиваемых уровней. Этот параметр указывает "глубину" развертывания узлов дерева.

Декодировать до первого уровня в ASCII-экспорте – этот флаг устанавливает формат, используемый при экспорте лог-файла или отдельного пакета в виде текстового файла с декодированием. Если флаг установлен, экспортируются только узлы верхнего уровня. Например, при снятом флаге, экспорт TCP/IP-пакета произойдёт с записью всех узлов "Тип сервиса". При установленном флаге эти узлы не экспортируются. Таким образом, можно получать менее детальные, но более компактные файлы.

Игнорировать неверные контрольные суммы при реконструкции TCP-сессий – эта опция воздействует на то, как CommView воспринимает повреждённые TCP/IP-пакеты при реконструкции TCP-сессии. По умолчанию эта опция включена, и пакеты со сбойной контрольной суммой не отбрасываются при реконструкции. Если опцию выключить, пакеты со сбойной контрольной суммой будут отброшены и не попадут в окно реконструкции. Вниманию пользователей сетевых адаптеров Gigabit: все ваши исходящие пакеты будут содержать неправильную контрольную сумму, если на адаптере присутствует свойство "checksum offload" (аппаратный подсчёт). Если вы выключите эту опцию, вы увидите только половину реконструированной TCP-сессии. То же самое относится и к реконструкции локальных (loopback) сессий, так как эти пакеты содержат нулевую контрольную сумму.

Включать номера пакетов при реконструкции TCP-сессий – установите этот флаг, если требуется, чтобы фрагментам данных в окне реконструкции TCP-сессий предшествовали номера пакетов, соответствующие этим фрагментам.

Искать начало сессии при реконструкции TCP-сессий – если данный флаг установлен, программа попытается найти начало восстанавливаемой TCP-сессии. Если флаг не установлен, то сессия будет воссоздана только с выбранного пакета, т.е. все предшествующие пакеты будут проигнорированы.

Декомпрессировать данные в формате GZIP - установите этот флаг, если требуется распаковывать GZIP-содержимое HTTP-трафика и выводить его в читаемом виде. Распаковка GZIP происходит, только если в окне реконструкции выбран режим просмотра "ASCII".

Реконструировать изображения – установите этот флаг, если требуется, чтобы CommView конвертировал двоичные данные HTTP-потоков, представляющие изображения, в сами изображения в форматах JPG, BMP, PNG, и GIF в окне реконструкции. Картинки отображаются, только если в окне реконструкции выбран режим просмотра "HTML". Картинки **не** показываются в реконструируемых страницах HTML, так как они передаются сервером в независимых HTTP-сессиях.

Использовать нотацию IPv4 в окончаниях IPv6-адресов – если флаг не установлен, то IPv6-адреса будут показываться только в шестнадцатеричном формате, например, fe80::02c0:26ff:fe2d:edb5. Если флаг установлен, то последние 4 байта в IPv6-адресе отображаются с использованием нотации IPv4, с точками: fe80::02c0:26ff:254.45.237.181.

Пересобирать фрагментированные IP-пакеты – установите этот флаг, если вы хотите, чтобы программа пересобрала фрагментированные IP-пакеты. По умолчанию, фрагментированные IP-пакеты отображаются в их исходном виде, как они были получены. Если эта опция включена, программа будет использовать внутренний буфер для хранения фрагментов и попытается "склеить" их. Отображаться будут только результаты успешной сборки.

Пытаться соотнести входящие UDP-пакеты с процессом – поскольку природа отображения входящих пакетов на процесс-собственник носит вероятностный характер, то, по умолчанию, система отображения программы не будет пытаться делать этого.

Логика изображения по умолчанию - выберите режим отображения из выпадающего списка. Этот режим будет установлен как "режим по умолчанию" для функции восстановления TCP-сессий. Возможные значения - ASCII, HEX, HTML, EBCDIC.

VoIP

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

Отключить анализ VoIP-данных – отключить перехват и анализ данных VoIP. Выберите эту опцию, если вы не планируете работать с VoIP и хотите минимизировать потребление ресурсов компьютера.

Максимальное кол-во записей в списке – ограничить количество отображаемых и обрабатываемых событий VoIP. Когда количество записей превысит указанный лимит, более старые записи будут удалены из списка.

Игнорировать потоки без сессии – если опция активна, то анализатор VoIP будет игнорировать перехваченные потоки RTP, у которых не будет "родительской" сессии. Потоки RTP без сессии обычно возникают в том случае, если перехват пакетов был включен уже в процессе звонка, сигнализирующий протокол неизвестен приложению (т.е. это не SIP и не H.323) или передача была произведена нестандартным образом (в зашифрованном виде или как часть другой сессии). Такие потоки можно анализировать, а иногда даже воспроизводить. За более подробной информацией о проигрывании звонков VoIP обратитесь к главе Воспроизведение звонка. Если потоки без сессии вам не интересны, и вы хотите сэкономить ресурсы компьютера – отключите эту опцию. Помните, что если потоки без сессии не игнорируются, анализатор VoIP может ошибочно принять данные, переданные по протоколу UDP за потоки RTP. В целом это не является ошибкой, поскольку пакеты RTP не имеют единой стандартной структуры, так что ложные срабатывания в данном случае – нормальное явление.

Геолокация

Геолокация – это определение страны по IP-адресу. Если опция включена, CommView извлечет из внутренней базы данных информацию о том, к какой стране принадлежит IP-адрес. Рядом с каждым IP-адресом вы можете показывать **ISO-код страны**, **Название страны** или **Флаг страны**. Вы также можете отключить геолокацию. Для некоторых IP-адресов (например, зарезервированных

вида 192.168.*.* или 10.*.*.*) информация о стране предоставлена не будет. В этом случае имя страны показано не будет, а если вы установили опцию **Показывать флаг страны**, будет показан флаг со знаком вопроса.

Поскольку местонахождение IP-адресов постоянно меняется, важно, чтобы у вас всегда была последняя версия CommView. Обновления базы данных включаются в каждую сборку CommView. Последняя версия базы данных имеет точность порядка 98%. Без обновлений показатель точности падает примерно на 15% каждый год.

Разное

Убирать кнопку программы с панели задач при сворачивании - установите этот флаг, если не хотите видеть кнопку программы в панели задач Windows, когда вы минимизируете CommView. Если этот флаг установлен, используйте значок программы в панеле уведомления для восстановления после минимизации.

Разрешить запуск нескольких копий программы - установите этот флаг, если нужно запускать несколько копий программы для наблюдения за несколькими адаптерами одновременно.

Спрашивать подтверждение при выходе из программы – установите этот флаг, если хотите, чтобы программа запрашивала подтверждение при выходе.

Автоматическая прокрутка окна данных пакета - если этот флаг установлен, программа автоматически прокручивает текст в окне данных пакетов (если только текст не помещается в окне). Это полезно, когда вы хотите видеть содержимое большого пакета без ручного прокручивания окна.

Автоматическая прокрутка списка пакетов до последнего пакета - если этот флаг установлен, программа автоматически сортирует новые записи в закладке **IP-статистика** в соответствии с заданными правилами сортировки (например, в возрастающем порядке удалённых IP-адресов).

Автосортировка записей в текущих IP-соединениях - если этот флаг установлен, программа автоматически прокручивает пакеты в списке закладки **Пакеты** вниз, до последнего принятого.

Контроль загрузки CPU – если флаг установлен, программа пытается снизить загрузку процессора при обработке тяжёлого трафика. Это достигается понижением частоты обновлений экрана и выведением на него меньшего объёма информации.

Запуск программы при старте Windows - если этот флаг установлен, программа автоматически запускается при загрузке Windows. При работе под системами Windows Vista и старше, установка этого флага не будет иметь эффекта, если в системе включен User Account Control (UAC). Это ограничение Windows Vista и более новых версий Windows, которое препятствует запуску приложений с повышенными правами при загрузке ОС. Если опция запуска приложения при старте Windows для вас важна, отключите UAC.

Запуск в свернутом состоянии - если этот флаг установлен, программа запускается минимизированной, и главное окно не отображается, пока вы не нажмёте на значок в панеле уведомления или в панели задач.

Включить автоматическую проверку обновлений – требуется задать интервал между проверками в днях.

Плагины

Эта закладка используется сторонними модулями для задания конфигурации. Подробнее...

Часто задаваемые вопросы (FAQ)

В этой главе вы можете найти ответы на некоторые из наиболее часто задаваемых вопросов. Свежий FAQ всегда доступен на http://www.tamos.ru/products/commview/faq.php

В. Может ли CommView быть использован для перехвата dial-up (RAS) трафика?
О. Да.

В. Что может "видеть" CommView, которая инсталлирована на компьютер с локальной сетью?
О. CommView переводит сетевой адаптер во "всеядный" (promiscuous) режим, что позволяет перехватывать весь трафик в локальном сегменте сети. Другими словами, он перехватывает и анализирует пакеты, адресованные любому компьютеру сегмента, а не только к компьютеру, на котором запущена программа. Есть ограничения при использовании с Wireless Ethernet-адаптером (CommView будет перехватывать только входящие и исходящие пакеты с вашего компьютера, т. е. транзитные пакеты отображаться не будут), и при работе через switch (см. вопрос о switch ниже в FAQ).

В. Я подключен к LAN через switch и, когда я запускаю CommView, он ловит только пакеты, идущие к/от меня, я не вижу трафика других машин. Почему?
О. В отличие от hub-ов, switch препятствует подслушиванию. В такой ситуации CommView (как и любой другой анализатор) ограничен приёмом broadcast и multicast пакетов, а также трафика того компьютера, на котором он запущен. Однако современные switch имеют функцию "port mirroring", что позволяет сконфигурировать их так, чтобы они перенаправляли трафик на некоторых или всех портах на специальный мониторный порт. Это позволит наблюдать трафик всего сегмента сети. На сайте доступна статья, в которой этот вопрос раскрыт подробно.

В. Я подключен к сети через hub, но не вижу чужого трафика, как если бы это был switch. Почему?
О. Возможны две причины: или это действительно switch, маркированный как hub (некоторые изготовители, например, Linksys иногда так поступают), или у вас многоскоростной hub, в этом случае вы не увидите трафик других станций, работающих на скоростях, отличающихся от скорости вашего адаптера (то есть, если у вас 10 Mbit-адаптер, вы не сможете увидеть трафик машин со 100 Mbit-адаптерами).

В. Моя домашняя сеть подключена к интернету через широкополосный маршрутизатор, и я вижу только свой собственный трафик. Можно ли наблюдать трафик остальных машин моей сети?
О. Да. Существует несколько способов решить эту задачу. За более подробной информацией и примерами конфигурации сети обратитесь к нашей статье.

В. Может ли CommView собирать данные на адаптере, который не имеет своего IP-адреса?
О. Да. Фактически, сетевой адаптер может быть даже не привязан ни к TCP/IP, ни к какому либо другому протоколу. При отладке сети вам может понадобиться подключить компьютер с CommView в свободный порт хаба. В этом случае вам необязательно знать, какие IP-адреса свободны в данном сегменте, просто снимите привязку адаптера к протоколу TCP/IP и начните перехват пакетов. В Control Panel => Network Connections щёлкните правой кнопкой на иконке

соединения, выберите Properties и снимите метки с соответствующих протоколов, которые вы не хотите "привязывать" к NIC.

В. Я работаю в локальной сети с большим объемом трафика, и поэтому мне сложно изучать отдельные пакеты, когда программа принимает сотни и тысячи пакетов в секунду, и старые пакеты быстро исчезают из циркулярного буфера. Можно с этим что-нибудь сделать?
О. Да, нажмите кнопку **Открыть текущий буфер в новом окне** в нижней панели инструментов в закладке **Пакеты**. Таким образом вы сможете создавать копии окна в любой момент времени, с любым интервалом и изучать пакеты не торопясь.

В. Я запустил программу и нажал "Начать захват", но пакеты не отображаются. Почему?
О. Возможны две причины: вы выбрали неактивное сетевое устройство или ошиблись, устанавливая правила перехвата. Попробуйте выключить правила и посмотрите, что происходит. В любом случае, даже когда они включены, строка состояния программы будет отображать общее количество пакетов, так что посмотрите сначала туда.

В. Я заметил, что контрольные суммы исходящих пакетов IP/TCP/UDP неверные. Почему?
О. Gigabit-овые сетевые адаптеры имеют способность, называемую TCP/UDP/IP "checksum offload", она позволяет адаптеру вычислять контрольную сумму аппаратно, освобождая от этой работы процессор. CommView перехватывает пакеты до того, как они попадают в адаптер, поэтому он выдает неверную контрольную сумму. Это нормальное явление и может повлиять только на процесс реконструкции TCP-сессии, причем только в том случае, если выключена опция "Ignore incorrect checksums". (Подробнее смотрите здесь)

В. Работает ли CommView на многопроцессорных системах?
О. Да.

В. Похоже, невозможно сохранить более 5000 пакетов из пакетного буфера. Есть ли способ решить эту проблему?
О. На самом деле такого ограничения нет. Для сохранения перехваченных пакетов в программе используется кольцевой (циркулярный) буфер. По умолчанию в буфере может содержаться до 5000 пакетов, но это значение можно поменять в окне **Установки**. Максимальный размер буфера составляет 20000 пакетов (буфер не может быть бесконечным по очевидным причинам – объем оперативной памяти на вашем компьютере тоже не бесконечен). Вы можете записать содержимое буфера в файл из закладки **Log-файлы**. Тем не менее, данное ограничение на размер буфера ни коим образом не ограничивает ваши возможности по сохранению любого количества пакетов. Вам всего лишь следует включить опцию автосохранения на данной закладке. Таким образом, программа будет непрерывно записывать в файл(ы) все перехваченные пакеты, и вы сможете установить любое ограничение на объем перехваченных данных.

В. Я подключен к сети через cable/xDSL-модем. Будет ли CommView осуществлять мониторинг трафика в этом случае?
О. Если модем поддерживает оба интерфейса USB и Ethernet, и вы можете подключить его к сетевому адаптеру Ethernet, CommView сможет наблюдать сетевой трафик. Если на модеме есть только USB-интерфейс, то можно, по крайней мере, попробовать.

В. Во время использования CommView мой файрволл сообщает, что CommView "пытается получить доступ в Internet". Я знаю, что некоторые сайты способны отслеживать пользователей, собирая информацию, посылаемую их программами через интернет. Зачем CommView пытается получить доступ в интернет?

О. Ваш файрволл могут заставить сработать 3 события. Во-первых, может иметь место попытка преобразования IP-адресов в имена хостов. Поскольку CommView обращается к вашим DNS-серверам для выполнения DNS-запроса, неизбежно возникнет предупреждение со стороны файрволла. Вы можете это отключить (**Настройка=>Установки=>Отключить распознавание DNS**), но в этом случае в окне последних соединений не будут показаны имена хостов. Во-вторых, вы могли настроить программу таким образом, что она автоматически проверяет наличие обновлений или новых версий. Для этого CommView соединяется с сайтом www.tamos.com. Вы можете это отключить (**Настройка=>Установки=>Разное=>Включить автоматическую проверку обновлений**). В-третьих, после покупки программы требуется ее активация. Если вы выберете онлайн-активацию, то программа сама подключится к www.tamos.com. Этого можно избежать, выбрав активацию вручную. Это единственные виды соединений, которые может устанавливать CommView. Программа не ведет никакого скрытого обмена данными – мы не продаем spyware.

В. Зачастую я вхожу как пользователь без административных прав. Следует ли мне каждый раз выходить и заходить вновь уже как администратор?

О. Нет. Откройте папку с CommView и, удерживая нажатой клавишу Shift, щелкните правой кнопкой мышки на CV.exe и выберите в меню пункт "Запустить как". Введите административные логин/пароль и нажмите OK для запуска программы. Под операционными системами Windows Vista и старше CommView автоматически запускается с повышенными правами.

В. Может ли CommView работать с сетевым адаптером, если CommView запущен под Microsoft Virtual PC?

О. Да. Единственным ограничением является то, что для виртуальных адаптеров недоступен "всеядный" режим, так что вы будете ограничены возможностью перехвата только собственных пакетов и пакетов, которые адресованы всем.

В. Во время dial-up соединения я не вижу PPP-пакетов. Это нормально?

О. К сожалению, пакеты согласования PPP не могут быть перехвачены. Заметим, что те PPP-пакеты, которые следуют непосредственно после пакетов согласования, перехватываются успешно.

В. Я работаю с WireShark и заметил, что после установки CommView больше не могу перехватывать пакеты.

О. Это известный конфликт между WinPcap (драйвером, который используется в WireShark и многих других сходных продуктах) и драйвером, используемым в CommView. Есть простое решение проблемы: начинайте перехват пакетов с помощью WireShank до того, как начнете перехват с помощью CommView. В этом случае обе программы будут осуществлять захват данных одновременно. Если же вы начнете перехват из CommView раньше, то по неизвестной нам причине WinPcap не сможет перехватывать пакеты.

В. Я реконструировал TCP-сессию, содержащую HTML-страницы на японском или китайском языке, но я не вижу текста!

О. Для того чтобы иметь возможность просматривания восточных языков, вам нужно установить соответствующие шрифты. Откройте Панель управления => Язык и региональные стандарты, выберите пункт "Языки" и включите опцию "Установить поддержку языков с письмом иероглифами".

В. Поддерживает или анализатор VoIP экспорт аудио-информации в WAV или MP3?

О. Напрямую – нет, но на рынке представлено достаточное количество программ, которые могут решить эту задачу. Фактически, вам нужен "виртуальный аудио-кабель", т.е. возможность сохранения в файл всего, что проигрывается через вашу аудио-карту. К примеру, вы можете использовать программу Xilisoft Sound Recorder (используйте режим "What you hear").

Анализ VoIP

Введение

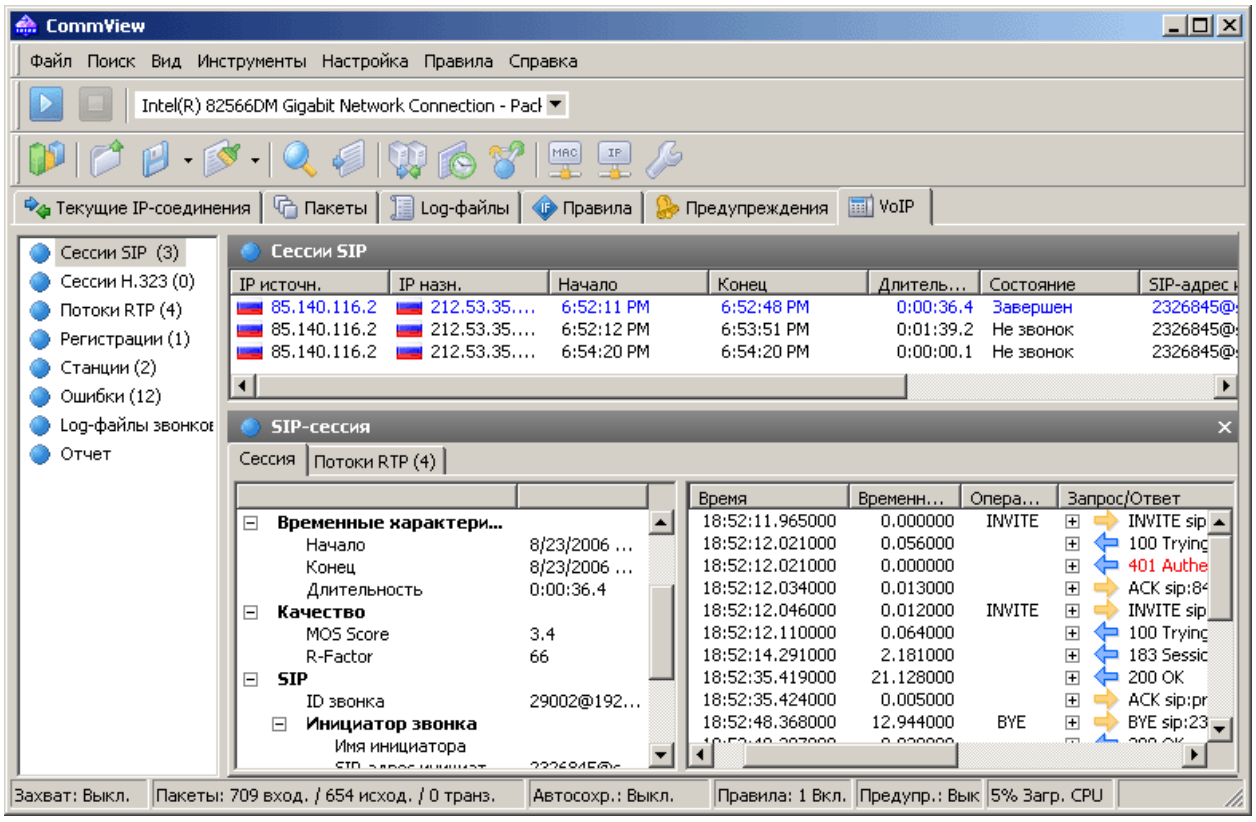
Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

Анализатор VoIP – это встроенный в CommView модуль, предназначенный для перехвата и анализа в режиме реального времени таких событий Интернет-телефонии (VoIP), как звонки, сессии, регистрации, потоки данных, ошибки и т. д. Представляя данные в графическом виде и оценивает качество голосовой передачи, этот модуль поможет вам повысить эффективность отладки VoIP-сетей, программного и аппаратного обеспечения. Анализатор VoIP поддерживает сигнальные протоколы SIP 2.0 и H.323, медийные потоки данных RTP 2.0 и множество распространенных кодеков. Помимо анализа в режиме реального времени, существует возможность импорта и исследования уже перехваченных данных в разных форматах (например, Tcpdump, EtherPeek и т. д.).

Работа с анализатором VoIP

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

Анализатор VoIP доступен из закладки **VoIP** главного окна программы. В этой закладке производится анализ перехваченных пакетов в режиме реального времени. Анализатор также доступен из окна Просмотра VoIP Log-файлов, в котором вы можете изучать ранее перехваченные данные, содержащиеся в log-файлах. Анализатор VoIP работает параллельно с перехватом пакетов и показывает результаты в реальном времени:



Информация распределена по нескольким категориям. Список категорий расположен на панели, где можно выбрать любую из категорий. Подробная статистика будет представлена в правой части окна. Список категорий имеет следующий вид:

Сессии SIP – список перехваченных сессий SIP 2.0.
Сессии H.323 – список перехваченных сессий H.323.
Потоки RTP – список перехваченных потоков RTP.
Регистрации – список клиентов, зарегистрированных на сервере и история регистраций клиентов.
Станции – список рабочих станций, участвующих в обмене VoIP-данными.
Ошибки – список ошибок, зарегистрированных при обмене данными по VoIP.
Log-файлы звонков – настройка опций сохранения log-файлов для перехваченной информации VoIP.

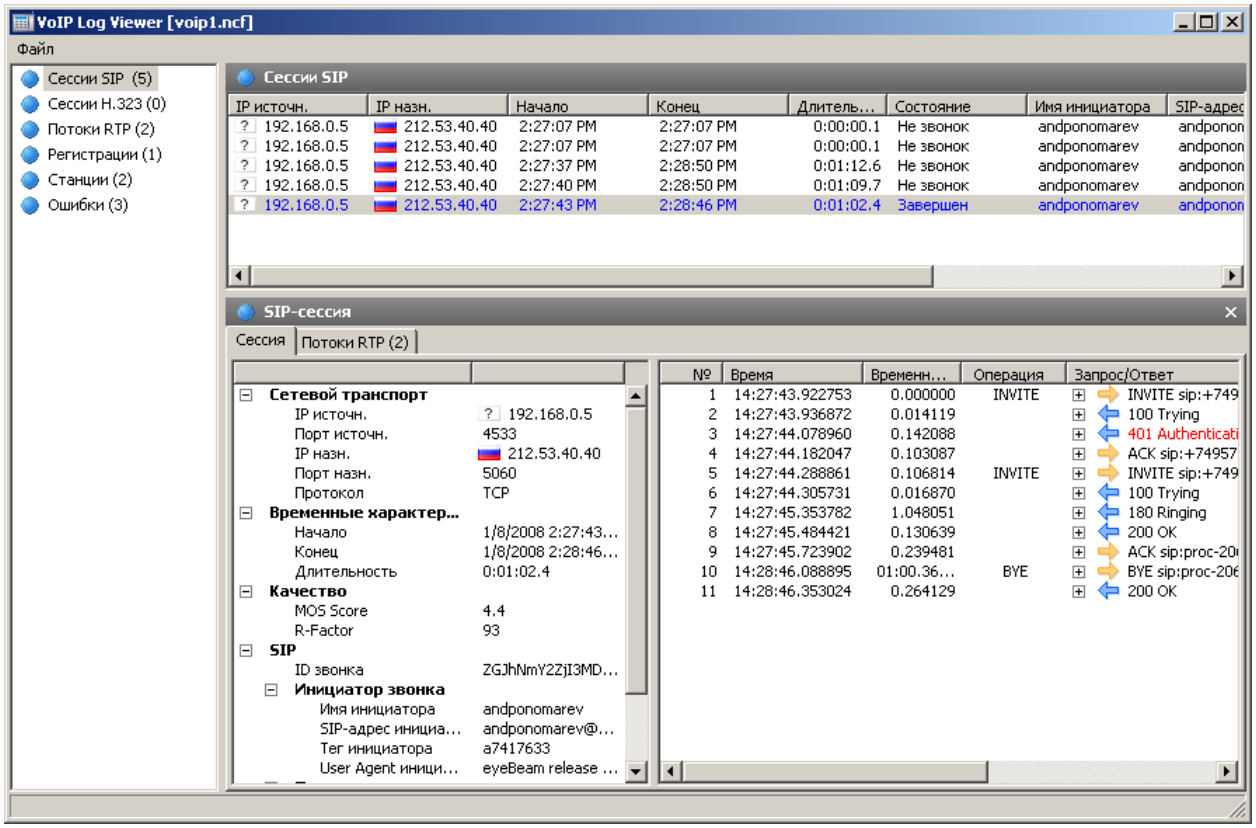
Отчет – настройка генерации отчетов, включая автоматический режим.

За более подробной информацией о том, как организованы данные в анализаторе VoIP обратитесь к главе Работа со списками в анализаторе VoIP.

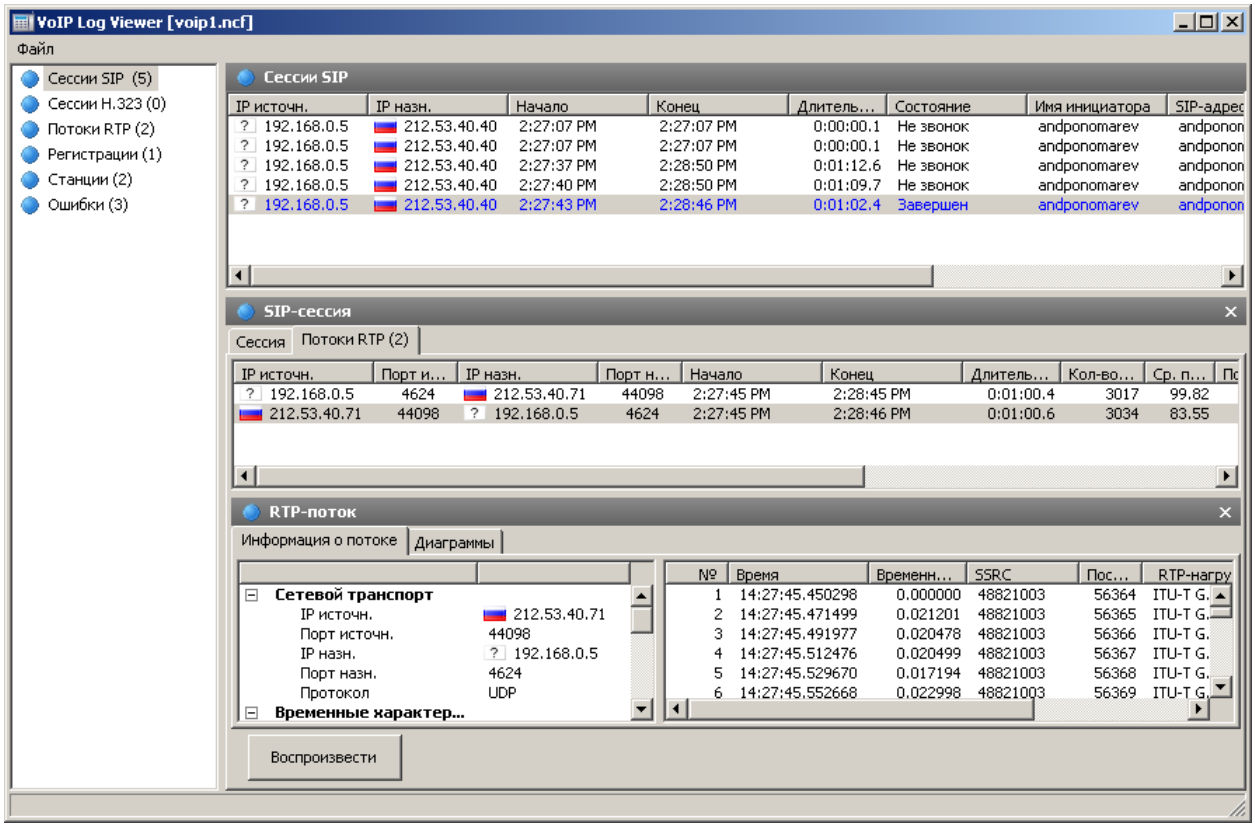
Сессии SIP and H.323

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

В настоящее время анализатор VoIP поддерживает два вида сигнальных протоколов – SIP и H.323. Сессии SIP и H.323 представлены на панели слева как две отдельные записи. Выбрав одну из них, вы увидите соответствующие сессии, перехваченные программой, а также подробную информацию по каждой сессии в отдельности:



На верхней панели показан полный список перехваченных сессий SIP и H.323. При выборе в списке сессии SIP/H.323 на нижней панели будет показана подробная информация о данной сессии, включая подробный журнал сеансов, общую и статистическую информацию и потоки RTP, относящиеся к выбранной сессии:



Если для выбранных сессий доступны RTP-потоки, то появляется возможность воспроизведения звонка нажатием на кнопку **Воспроизвести**.

См. также:

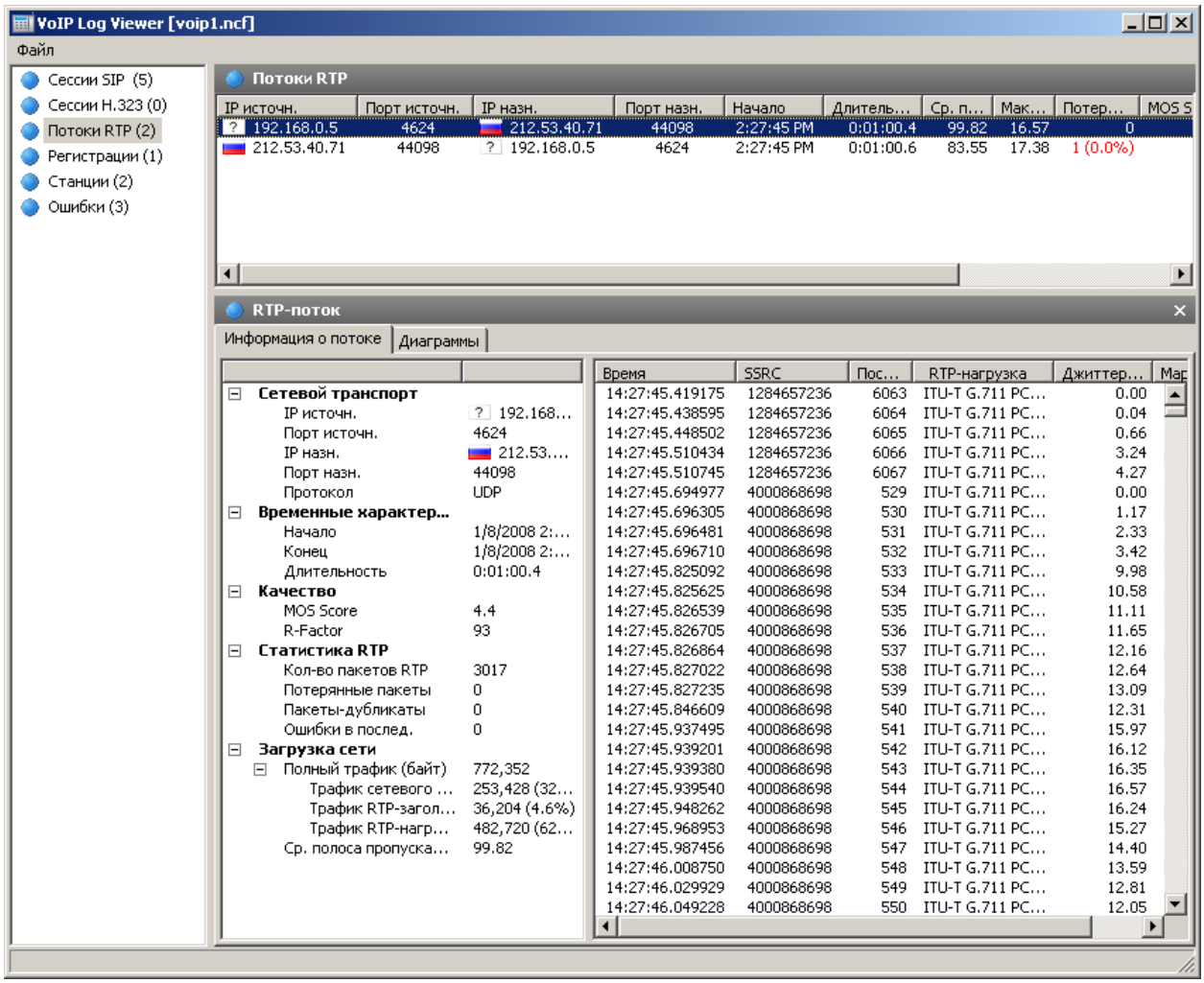
Работа со списками в анализаторе VoIP
Воспроизведение звонка
Файлы NVF

Потоки RTP

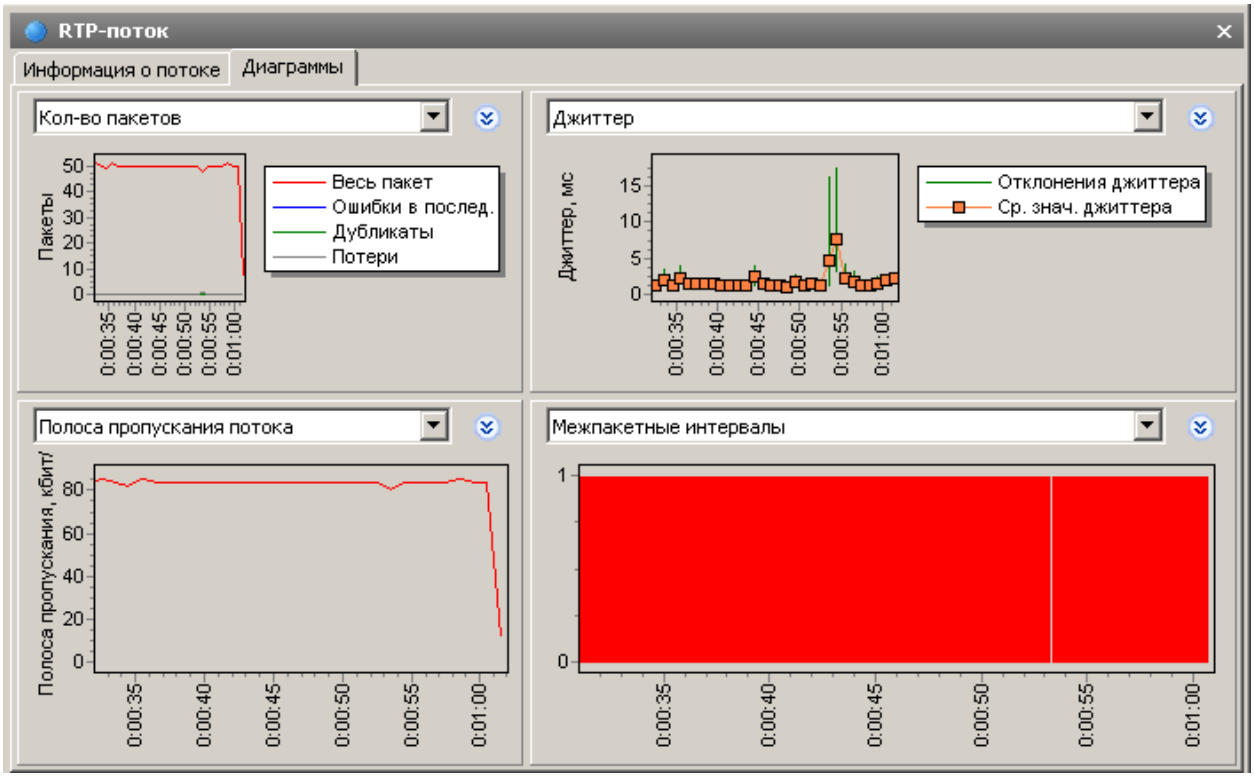
Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

В протоколе обработки данных в реальном времени (RTP) определен стандартный формат пакета для передачи аудио- и видео-информации в сети Интернет. Если протоколы SIP и H.323 используются для управления процессом звонка (например, подключения, дозвона, разъединения и т. п.), то RTP служит для надежной передачи пакетов данных и поддержания надлежащего Качества Сервиса (Quality of Service). Другими словами, в потоках RTP содержится реальная голосовая информация, закодированная с помощью одно из кодеков. Анализ данных RTP дает ценную информацию о качестве звонка и для отладки сетей VoIP.

Для просмотра перехваченных программой потоков RTP выберите **Потоки RTP** в левой панели окна анализатора VoIP:



В верхней части показан полный список потоков RTP. При выборе потока RTP из списка на нижней панели будет показана подробная информация о данном потоке, включая полный список пакетов RTP, общая и статистическая информация и графики:



Для выбранного потока можно показать до 4 графиков одновременно, с интервалом от 5 до 60 секунд. Изображение можно прокрутить направо или налево, кликнув по нему правой кнопкой мыши и перетащив. Доступны следующие виды графиков:

Кол-во пакетов – количество пакетов RTP в секунду включая повторные, потерянные и "искаженные" пакеты.
Полоса пропускания потока – скорость потока в Кбит/с.
Размеры пакета – средние размеры пакетов RTP в виде четырех диаграмм (весь пакет, RTP-нагрузка, RTP-заголовок, сетевой заголовок).
Джиттер – джиттер потока.
R-Factor, MOS Score – оценка качества потока.
Межпакетные интервалы – временное распределение пакетов RTP в потоке.

В списке потоков RTP содержатся все перехваченные потоки RTP, которые принадлежат сессиям SIP и H.323, а также те потоки, для которых сессии не были определены (т. н. "потоки без сессий", не принадлежащие ни к одной "родительской" сессии). За более подробной информацией об исключении потоков RTP без соответствующих сессий обратитесь к главе Установка опций.

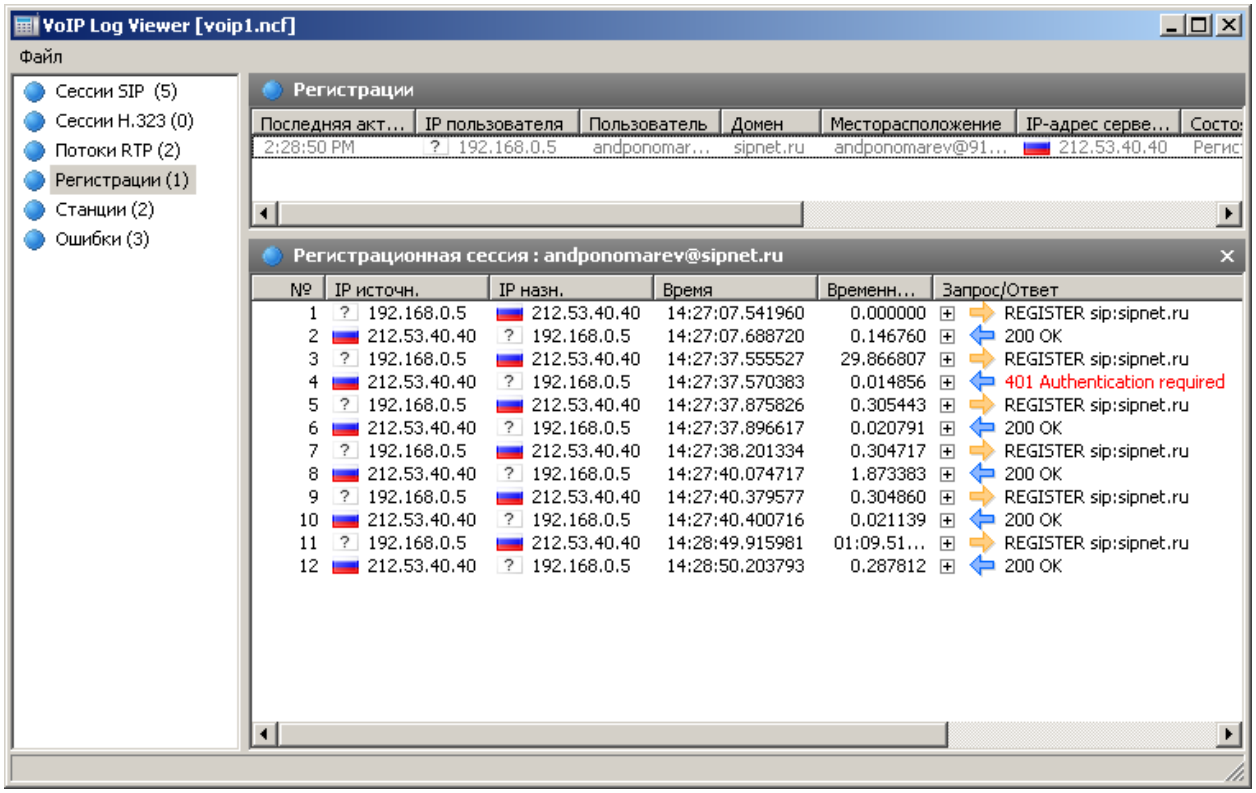
См. также:

Работа со списками в анализаторе VoIP
Воспроизведение звонка
Файлы NVF

Регистрации

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

Для просмотра клиентов VoIP, зарегистрированных на серверах, выберите на панели слева пункт **Регистрации**:

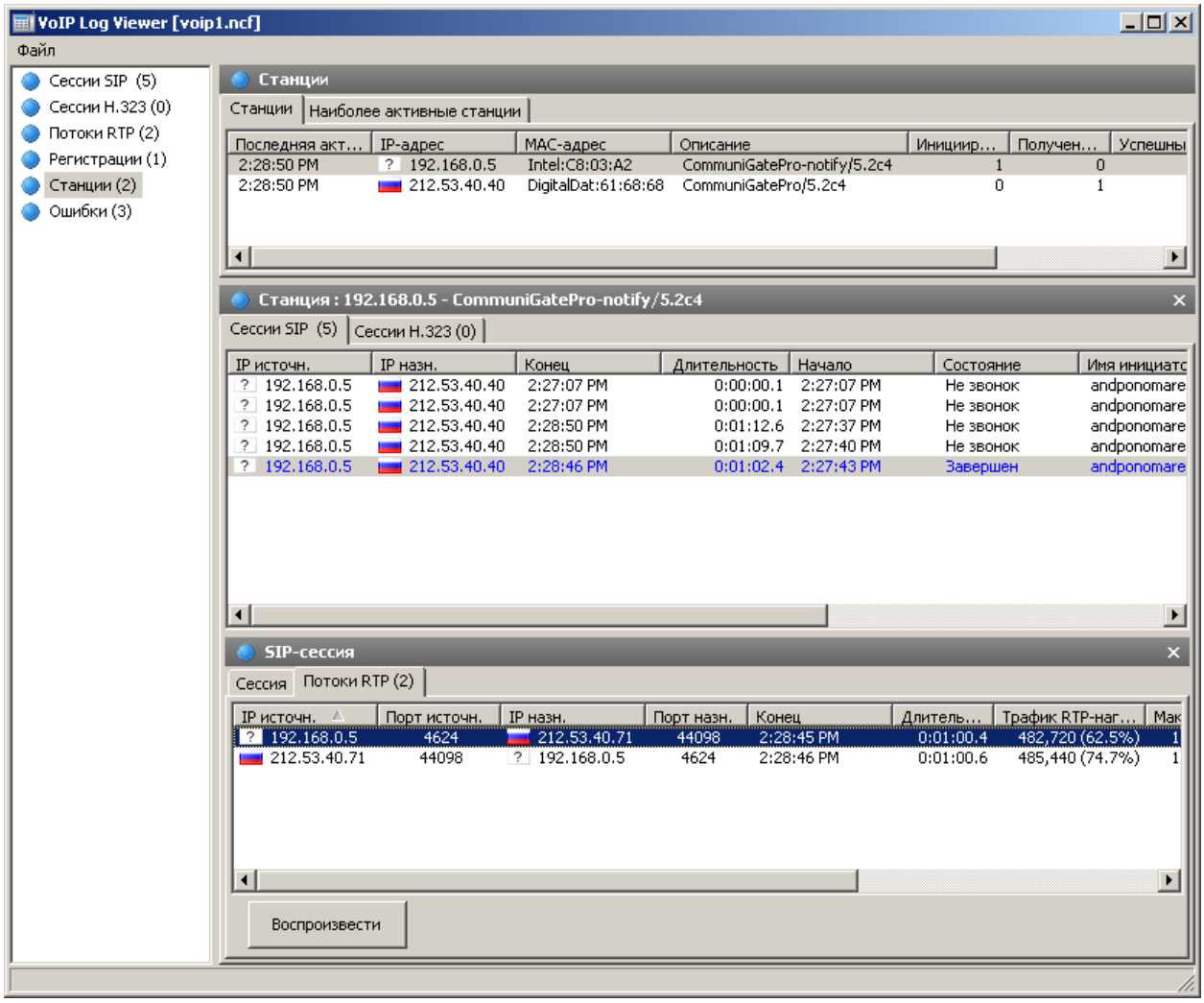


В верхней части правой панели приведен полный список всех регистраций, включая текущий статус регистрации клиентов VoIP. При выборе записи регистрации будет показан список сообщений VoIP-клиента, отправленных серверу регистрации или полученных от него.

Станции

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

На данной панели показан список станций, участвующих в обмене VoIP-данными, включая статистическую информацию и список станций, на которые приходится наибольшее число звонков.

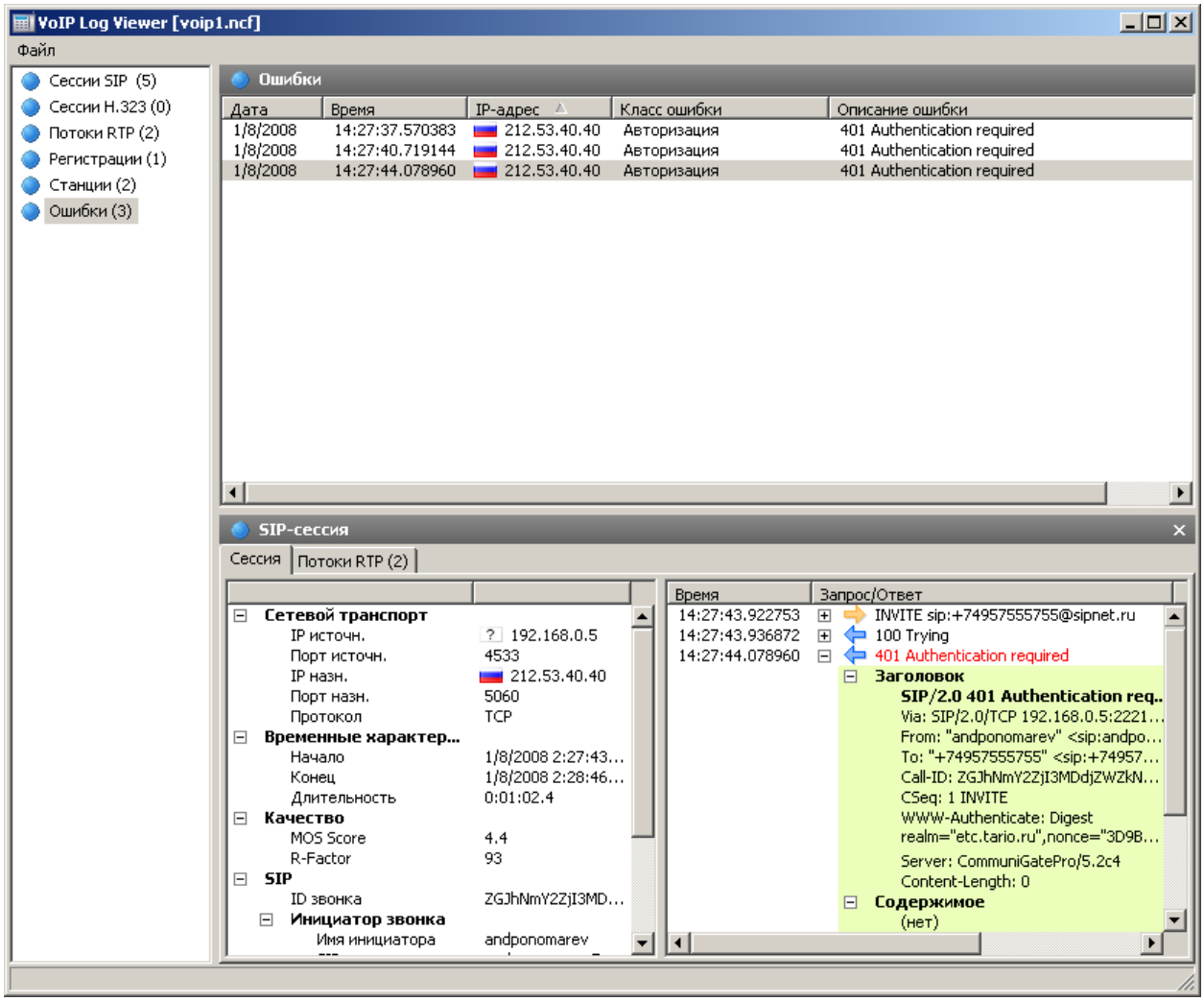


Полный список рабочих станций представлен в верхней части панели. При выборе станции в нижней части панели будут показаны входящие и исходящие звонки от выбранного компьютера или устройства.

Ошибки

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

На данной панели показан список последних ошибок, зарегистрированных при обмене данными между клиентами VoIP и серверами:

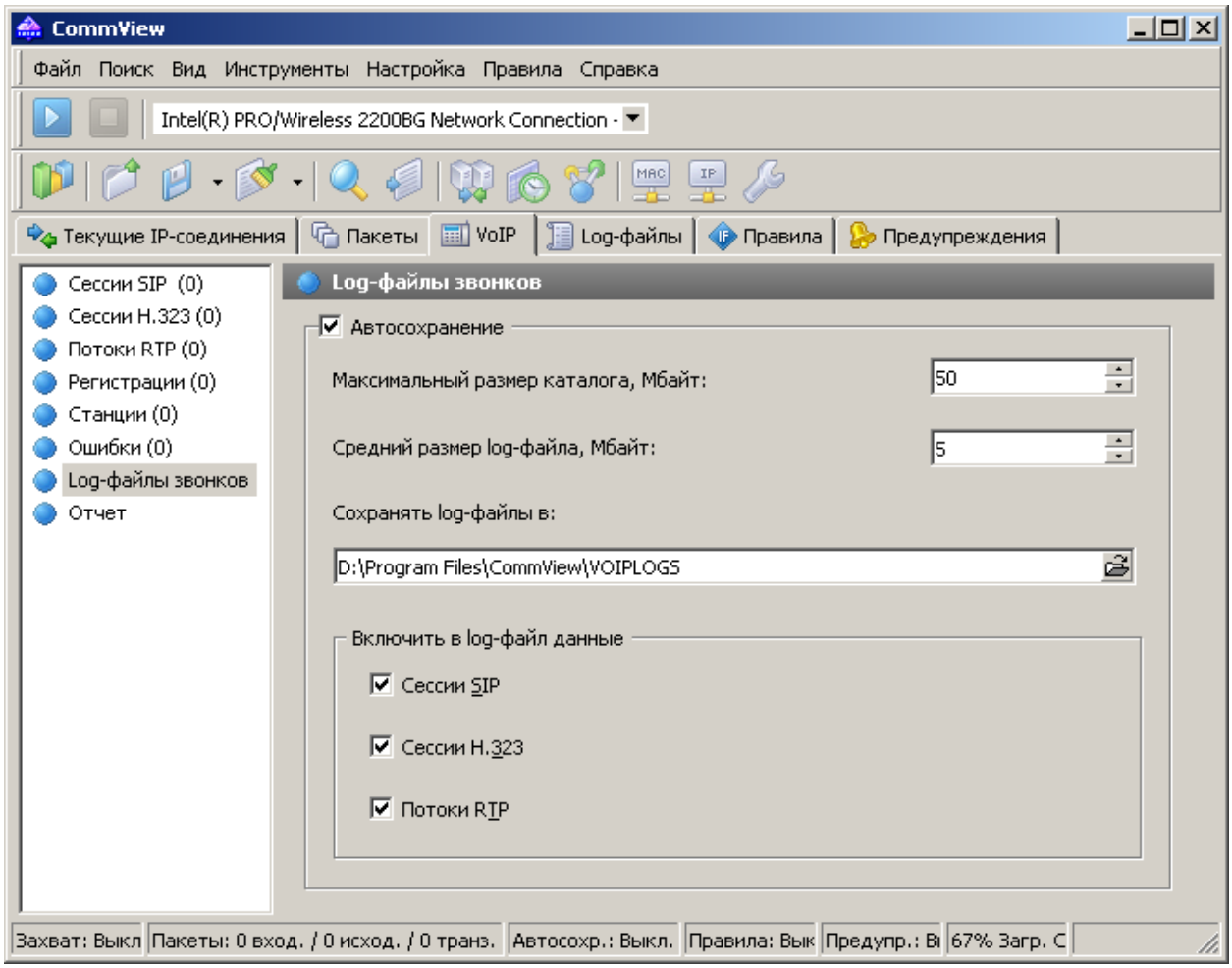


Список последних ошибок показан в верхней части панели. При выборе записи в нижней части панели будет показана информация о соответствующем звонке.

Log-файлы звонков

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

Программа дает возможность автоматической записи всех VoIP-пакетов в log-файлы CommView:

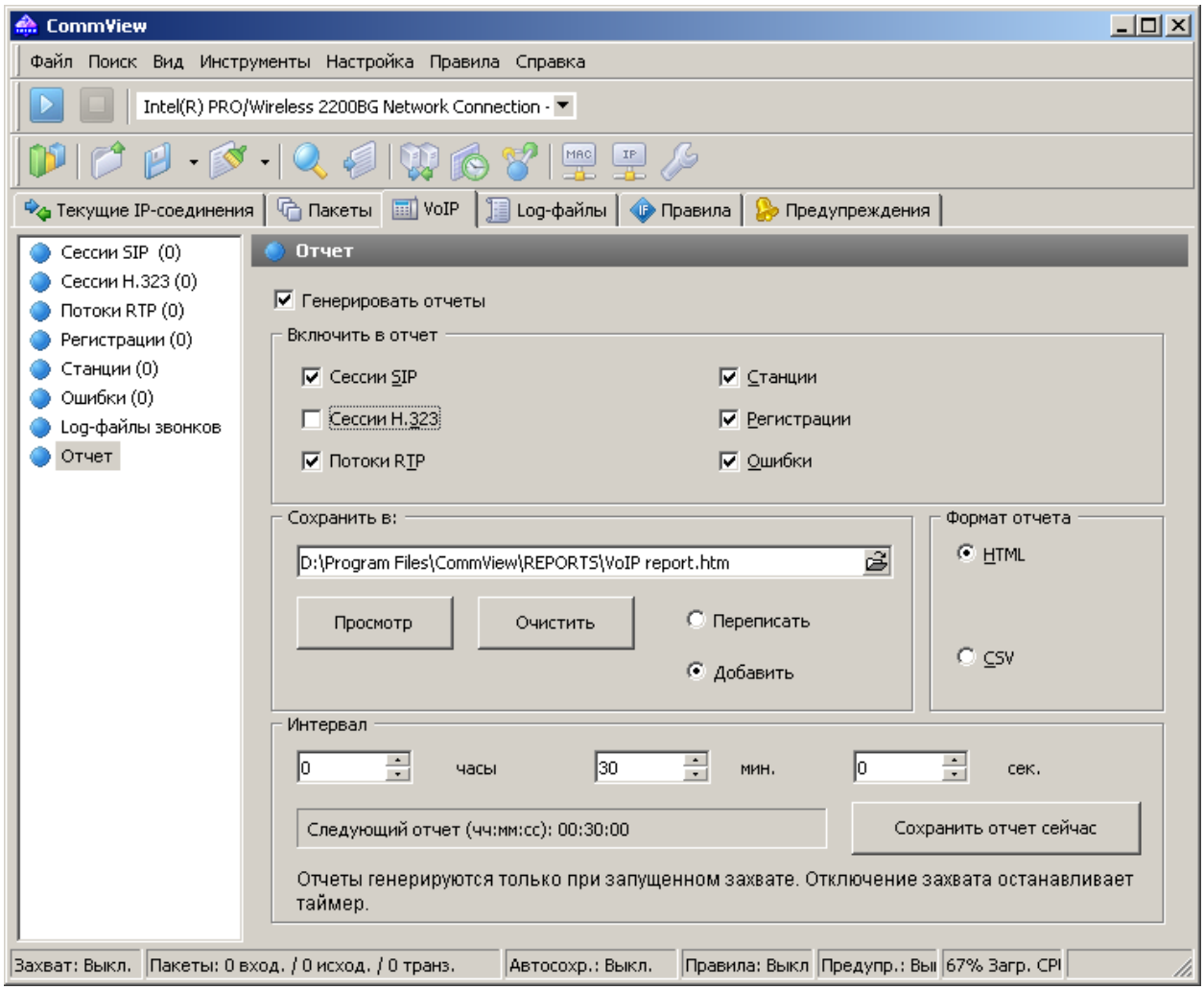


Выберите опцию **Автосохранение** и укажите данные, которые требуется сохранять в log-файл. В области **Включить в log-файл данные** укажите виды пакетов, которые следует сохранять.

Отчет

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

Панель **Отчет** предназначена для автоматического создания отчетов по VoIP:

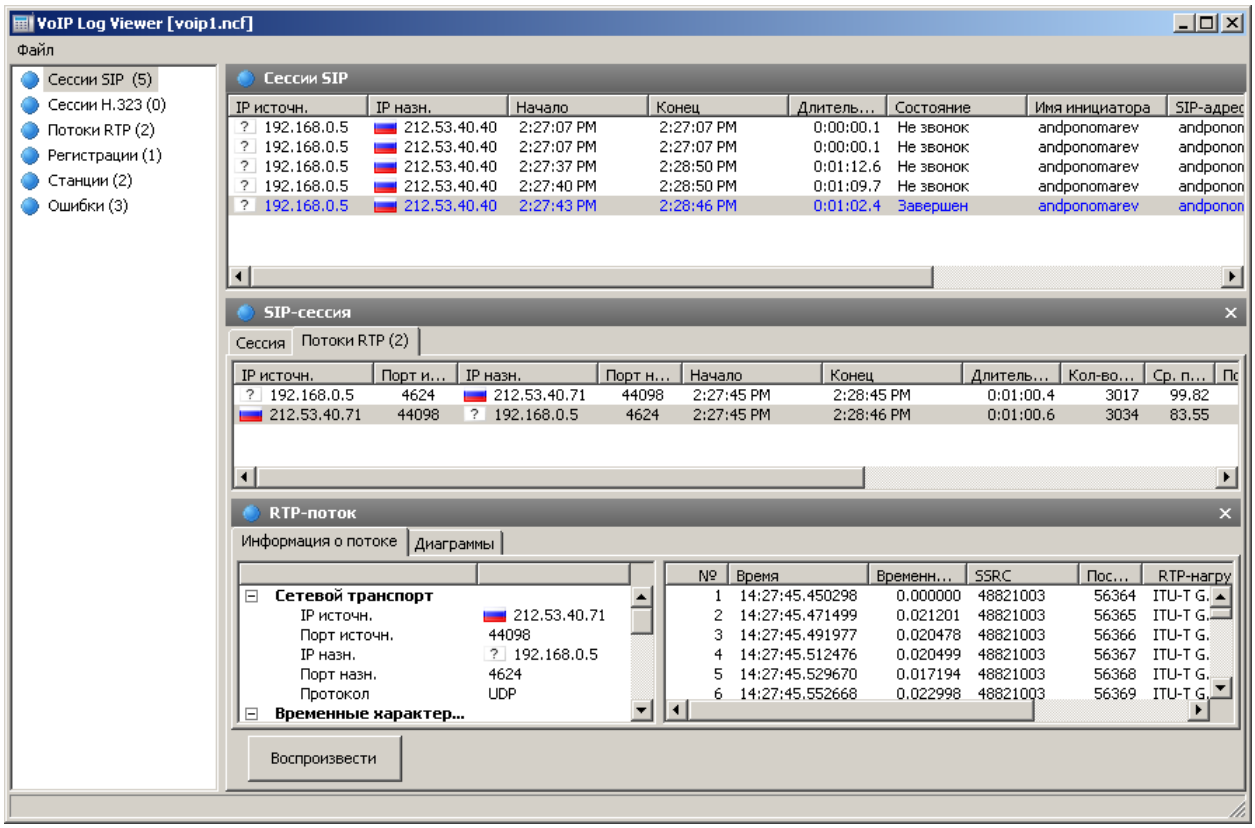


Для включения генерации отчетов выберите опцию **Генерировать отчеты**. В области **Включить в отчет** вы можете указать, какие данные вы хотите в нем увидеть. Помимо этого есть возможность указать формат отчета (CSV или HTML), а также задать временной промежуток между отчетами. Новые отчеты могут как замещать старые, так и дописываться к ним.

Воспроизведение звонка

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

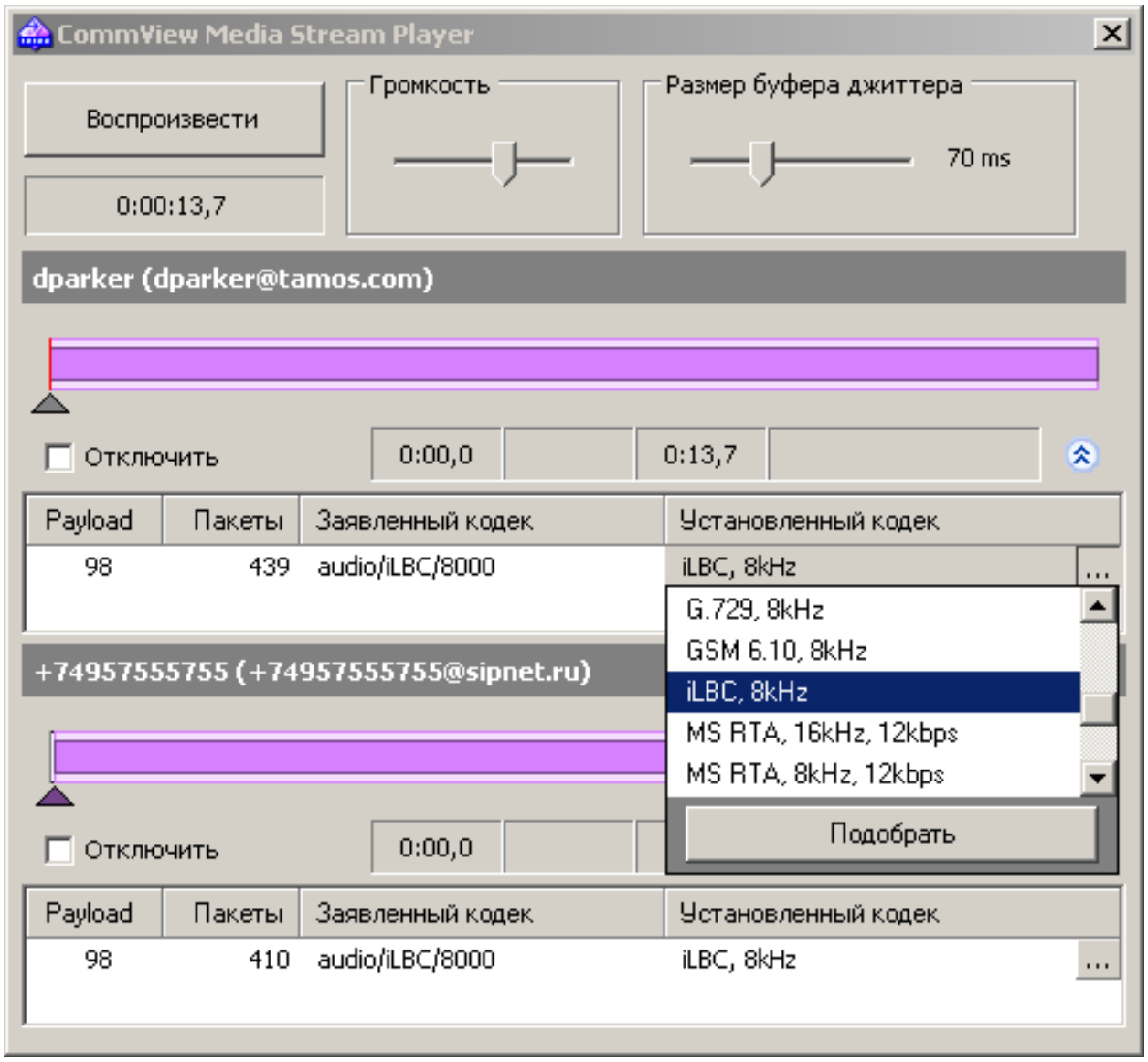
Функция воспроизведения звонка может быть использована для оценки качества звука, проходящего между сторонами, участвующими в звонке VoIP. В большинстве случаев анализатор VoIP даст вам возможность воспроизвести перехваченные звонки (это зависит от наличия поддержки для определенных кодеков, используемых в данном VoIP-звонке). Для воспроизведения выберите запись в окне анализатора VoIP, перейдите в закладку **Потоки RTP** и нажмите кнопку **Воспроизвести**.



Помимо этого, вы можете выбрать любую запись на панели справа, где находится список потоков RTP (например, категория Потоки RTP), затем указать один или несколько потоков, кликнуть по ним правой кнопкой мыши и выбрать пункт меню **Воспроизвести выбранное**. Таким образом, можно установить взаимосвязь и воспроизвести потоки, для которых сессия либо отсутствует, либо не поддерживается сигнальный протокол (т.е. протокол не является SIP или H.323).

Замечание: одновременное воспроизведение потоков RTP, принадлежащих **разным звонкам**, начатым в разное время, как правило, не сработает. Основной проблемой является существенный сдвиг по времени между потоками, принадлежащими разным VoIP-звонкам. Кроме того, прослушивание аудио-фрагмента, состоящего из несвязанных между собой частей разных звонков не имеет никакого смысла. Возможность выбора произвольных потоков RTP для последующего воспроизведения дается лишь для ручного восстановления звонка из нескольких потоков в тех случаях, когда "родительские" сессии SIP/H.323 недоступны.

После нажатия кнопки **Воспроизвести** откроется окно Media Stream Player:



Чтобы показать более подробную информации об аудио-потоках и получить доступ к ручному выбору кодека нажмите кнопку с двойной стрелкой. Для каждого потока RTP вы можете:

- Вручную синхронизировать поток по времени, т. е. привязать время начала воспроизведения к другим потокам. Для этого переместите небольшой треугольник налево или направо.

- Выбрать правильный кодек для каждого потока RTP. В большинстве случаев Media Stream Player выберет нужный кодек автоматически. Несмотря на это, при работе с потоками RTP без сессии SIP/H.323 и, следовательно, без всякой информации о необходимом кодеке вам придется самостоятельно выбрать кодек из выпадающего списка. Если вы затрудняетесь в выборе кодека, нажмите кнопку **Подобрать,** и плеер сам попытается выбрать правильный кодек.

Имейте в виду, что иногда не будет возможности воспроизвести звук из потоков RTP, поскольку сами потоки могут быть зашифрованы или работать с проприетарными кодеками или кодеками, которые не поддерживаются в CommView.

С помощью ползунка **Громкость** вы можете соответствующим образом настроить громкость звука при воспроизведении. С помощью ползунка **Размер буфера джиттера** можно симулировать буфер джиттера, который используется VoIP-станциями при реальных VoIP-разговорах. Обычно размер буфер джиттера составляет от 30 до 50 мс. Увеличение размера буфера ведет за собой улучшение качества звука, но вместе с тем и увеличение задержки.

Просмотр VoIP log-файлов

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

Модуль просмотра VoIP log-файлов предназначен для отображения и анализа файлов с перехваченными пакетами, созданных CommView и некоторыми другими сетевыми анализаторами. Выполняемые функции сходны с функциями анализатора VoIP, который является частью главного окна программы. Отличие состоит в том, что модуль просмотра служит для изучения данных после их перехвата, т. е. для работы с файлами, а не с пакетами в реальном времени. За более подробной информацией обратитесь к главе Работа с анализатором VoIP.

Для запуска функции просмотра log-файлов выберите в главном меню **Файл** => **Просмотр VoIP log-файлов**. Вы можете открыть любое количество окон для просмотра, при этом в каждом из окон можно проводить анализ одного или нескольких файлов с перехваченной информацией.

Модуль просмотра можно использовать для загрузки файлов перехвата CommView в формате NCF и других форматах. Кроме этого в данный модуль можно загрузить VoIP-файлы CCommView (NVF).

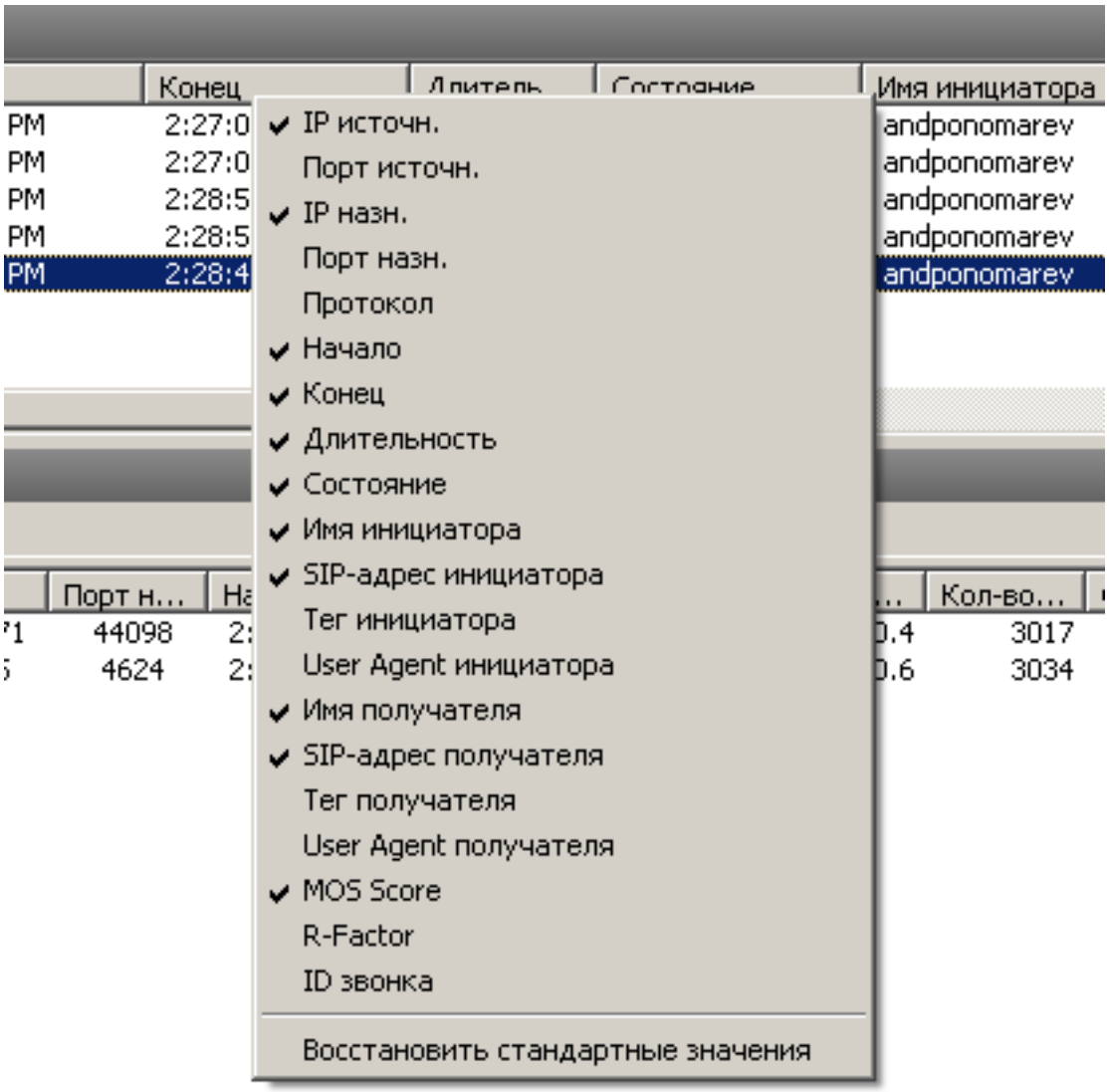
Меню модуля просмотра VoIP log-файлов

Загрузить log-файлы CommView – открыть и загрузить один или несколько файлов перехвата CommView.
Импорт log-файлов – импортировать файлы перехвата, созданные другими сетевыми анализаторами.
Сгенерировать отчет – создать сводный отчет по данным, загруженным в модуль просмотра и сохранить этот отчет на диск. При создании отчета используются настройки панели отчетов, расположенной в главном окне анализатора VoIP.
Очистить данные VoIP – очистить данные в текущем окне
Закрыть окно – закрыть окно.

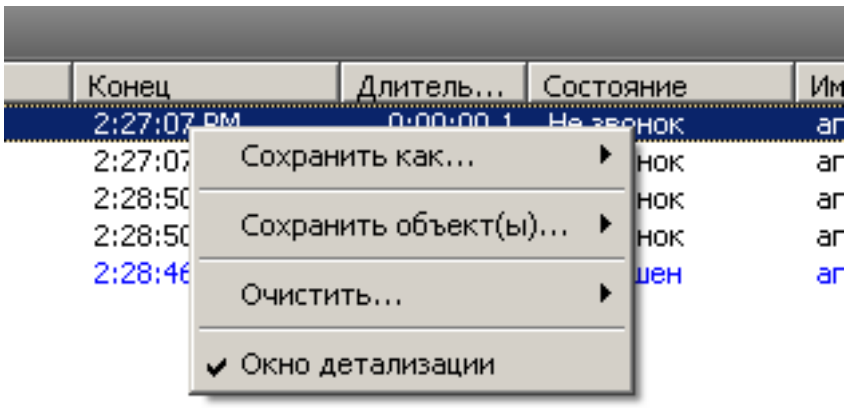
Работа со списками в анализаторе VoIP

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

Хотя данные в списках анализатора VoIP представлены в разных формах, описанные ниже принципы отображения информации являются общими для всех списков. По умолчанию в состав этих списков включены только наиболее часто используемые поля данных, а остальные поля скрыты. Для показа требуемых полей кликните по заголовку списка правой кнопкой мыши и включите/выключите соответствующие опции. Вы также можете изменить ширину и порядок расположения полей, перетащив их мышью.



Нажатие правой кнопки мыши вызовет контекстное меню со следующими пунктами:



Сохранить как – экспортировать все или выбранные записи в текстовый файл.
Сохранить объект(ы) – сохранить все или выбранные объекты в NVF-файл. За более подробной информацией по NVF-файлам обратитесь к главе Файлы NVF.
Очистить – очистить все или выбранные объекты либо списки. Удаление родительских объектов повлечет за собой удаление дочерних объектов; например, удалив звонок SIP, вы также удалите принадлежащие этому звонку потоки RTP из списка **Потоков RTP**.
Окно детализации – если вы работаете с главным списком, т. е. к выбранному объекту относится некоторое количество дополнительной информации, включение/отключение этой опции повлечет за собой отображение/скрывание соответствующих деталей объекта. Например, при включении **Окно детализации** в списке **Сессий SIP** программа отобразит/скроет подробную информацию о выбранной сессии SIP. К детализации относятся общая информация о звонке и связанных с ним потоков RTP.

Файлы NVF

Замечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

Анализатор VoIP дает вам возможность сохранить один или несколько объектов данных VoIP в файле-контейнере формата NVF. В отличие от других файлов перехвата, NVF-файл не содержит захваченных пакетов. Он представляет собой набор объектов, хранимых в едином файле. NVF-файлы могут пригодиться, если вы захотите сохранить звонок VoIP со всеми относящимися к нему потоками для последующего анализа.

Виды объектов, которые можно сохранить в NVF-файлы:

- **Сессии SIP**
- **Сессии H.323**
- **Потоки RTP**

Для сохранения объекта в файл NVF, выберите один или несколько объектов из списков анализатора VoIP, откройте контекстное меню правой кнопкой мыши и выберите пункт **Сохранить объект(ы)**. Сессии SIP/H.323 и соответствующие потоки RTP (при их наличии) будут сохранены в файл. Однако, если вы решите сохранить поток RTP, то соответствующие родительские сессии SIP/H.323 сохранены не будут.

Сохраненные файлы NVF можно загрузить в окне Просмотр VoIP log-файлов.

Дополнительные главы

Перехват больших объемов трафика

При сборе пакетов на большом или сильно загруженном сегменте сети, следует учесть, что обработка тысяч пакетов в секунду может существенно загрузить процессор и привести к "повисанию" программы. Повысить же производительность программы можно, используя правила для фильтрации ненужных вам пакетов. Пересылка файла объемом 50 Мб между двумя машинами порождает около 40000 NetBIOS-пакетов со скоростью передачи 10 мегабайт в секунду, что может оказаться трудновыполнимой задачей для программы. Однако часто не требуется анализ каждого пакета NetBIOS. Можно настроить CommView таким образом, что он будет принимать только пакеты IP. В CommView есть гибкая система фильтров, позволяющая принимать только те пакеты, которые вам действительно интересны. Если нужна лишь статистическая информация (гистограммы, таблицы хостов), можно воспользоваться командой "Блокировать сбор пакетов" в меню. В этом случае отображение пакетов в реальном времени будет приостановлено, а статистические данные будут продолжать собираться и показываться.

Факторы, улучшающие производительность программы:

- Быстрый процессор (рекомендуется Intel Core i7)
- Объем оперативной памяти (рекомендуется 2Гб и больше)
- Использование правил для фильтрации ненужного трафика

Запуск нескольких копий программы

CommView может перехватывать пакеты с нескольких сетевых адаптеров одновременно. Эта возможность включается меткой **Разрешить запуск нескольких копий программы** в меню **Настройка => Установки => Разное**. Имейте в виду, что один и тот же адаптер нельзя открыть из двух запущенных экземпляров программы. Такое же ограничение существует для Terminal Server: два пользователя (локальный и удалённый) не могут осуществлять перехват трафика с одного адаптера, запустив две копии CommView на одном и том же сервере.

Невидимый режим

Есть два способа запустить CommView как невидимый процесс:

1. Запустить CommView с ключом "hidden":

   CV.EXE hidden

2. Если CommView уже запущен, вы можете прятать или вызывать его "горячими" клавишами. Чтобы спрятать, нажмите ALT+SHIFT+h. Чтобы отменить невидимость, нажмите ALT+SHIFT+u.

Помните, однако, что полностью скрыть работу приложений в Windows нельзя. При работе в невидимом режиме процесс CommView будет виден в Панели Задач.

Параметры командной строки

При запуске программы доступны следующие параметры командной строки:

- Загрузить и активизировать набор правил из файла. Используйте ключ "/ruleset" между CV.EXE и полным путем к файлу правил:

  CV.EXE /ruleset "C:\Program Files\CommView\Rules\POP3Rules.rls"

  Если имя файла или путь включает символы пробела - заключите их в кавычки (" ").

- Выбрать адаптер и начать сбор пакетов. Используйте ключ "/adapter", за которым следует название адаптера, например:

  CV.EXE /adapter "Intel(R) PRO/1000 T Desktop Adapter"

  Название адаптера должно находиться в кавычках (" "). Поскольку названия обычно достаточно длинные, воспользуйтесь комбинацией Ctrl-C Ctrl-V для переноса имени из списка доступных адаптеров.

- Использовать специальный каталог для хранения log-файлов. Используйте ключ /logdir:

  CV.EXE /logdir "C:\Program Files\CommView\Logs"

Все эти опции можно использовать одновременно.

Обмен данными с вашим приложением

В CommView реализован простой и понятный интерфейс доступа к TCP/IP. Он позволяет вашему приложению в режиме реального времени обрабатывать пакеты, принятые с помощью CommView. Начиная с версии 5.0 есть возможность передавать пакеты аналогично тому, как это делает Packet Generator (генератор пакетов).

Принцип работы

Вам следует запустить CommView, задав ему в командной строке специальный ключ MIRROR, указывающий программе на какой IP-адрес и в какой TCP-порт дублировать захватываемые пакеты.

Примеры:
CV.EXE mirror:127.0.0.1:5555 // дублирует пакеты на loopback, в TCP-порт 5555
CV.EXE mirror:192.169.0.2:10200 // дублирует пакеты на 192.169.0.2, в TCP-порт 10200

Когда CommView запущен с этим ключом, он пытается установить TCP-соединение с указанным IP-адресом по указанному номеру порта. Это означает, что ваше приложение уже должно быть запущено и должно быть готовым к приему по указанному порту. Если CommView не может установить соединение, он будет делать повторные попытки каждые 15 секунд. То же самое будет происходить при разрыве соединения: каждые 15 секунд CommView будет пытаться восстановить его. Если соединение успешно установлено, CommView будет передавать захватываемые пакеты по мере их прихода, в режиме реального времени.

Формат данных

Данные передаются в формате NCF. Описание формата смотрите в последней главе данного раздела.

Передача пакетов

Ваше приложение может не только принимать пакеты, но и посылать их, аналогично генератору пакетов. Данные могут быть переданы в CommView с помощью все того же TCP-соединения, через которое происходил прием. Формат данных прост – двухбайтовое беззнаковое целое число, затем сам пакет. Если адаптер не открыт или он не поддерживает прием пакетов, пакет отбрасывается без уведомления.

Примеры проектов

Ниже приведены два простых примера программ, ожидающих входящих соединений, выделяющих пакеты из потока и отображающих "сырые" данные.

- http://www.tamos.com/products/commview/samp_mirr_c5.zip. Проект в Visual Studio с исходным текстом на C++.

- http://www.tamos.com/products/commview/samp_mirr_d5.zip. Проект на Delphi с исходником на Pascal. Для компиляции проекта вам понадобятся ICS-компоненты от Francois Piette, которые доступны на http://www.overbyte.be

Пропускная способность (Bandwidth)

При пересылке данных на удалённый компьютер, убедитесь, что линия связи между ними имеет достаточную пропускную способность, чтобы передать все перехваченные данные. Если CommView собирает данные с интенсивностью 500 кб/сек, а линия связи способна передавать только 50кб/сек, неизбежно возникнут "заторы", приводящие к разным неприятностям (например, в зависимости от версии Windows, winsock может прекратить передавать данные вообще). Если вам требуется более гибкое решение, использующее буферизацию и дистанционное управление – попробуйте воспользоваться CommView Remote Agent.

Пользовательский модуль декодирования

CommView позволяет подключить два типа пользовательских модулей декодирования.

Простой декодер

Если он используется, то результаты его работы будут показаны в дополнительной колонке закладки **Пакеты**. Пользовательский декодер должен быть 32-bit DLL с именем файла "Custom.dll" и экспортировать единственную процедуру - "Decode". Ниже показан её прототип на языках C и Pascal:

```
extern "C" {
void __stdcall Decode(unsigned char *PacketData, int PacketLen, char *Buffer, int BufferLen);
}

procedure Decode (PacketData: PChar; PacketLen: integer; Buffer: PChar; BufferLen: integer); stdcall;
```

Данная DLL должна располагаться в той же директории, что и CommView. При запуске CommView ищет файл с именем "Custom.dll" и загружает его в память. Если в нем найдена точка входа "Decode" - CommView добавляет новую колонку с именем "Custom" в списке пакетов.

Перед тем как отобразить новый пакет, CommView вызывает процедуру "Decode" и передаёт содержимое пакета в DLL. Процедура "Decode" должна обработать пакет и записать его в буфер. Первый аргумент - указатель на содержимое пакета, второй - длина, третий аргумент - указатель на буфер, в котором хранится результат обработки, четвёртый аргумент - размер буфера (в данной версии - всегда 1024 байта). Буфер выделяется и освобождается самой программой CommView, так что не следует управлять распределением памяти под этот буфер самостоятельно. Содержимое буфера будет отображено в виде строки в колонке "Custom".
Ваша процедура должно быть достаточно быстрой и обрабатывать тысячи пакетов в секунду; в противном случае снизится производительность программы. Не забывайте использовать STDCALL при вызове.

Две DLL представлены как пример. Они выполняют простейшие операции: "результатом" работы функции "Decode" является шестнадцатеричный код последнего байта пакета. Пользовательский декодер может быть сколь угодно сложным.

- http://www.tamos.com/products/commview/cust_decoder_c.zip. Проект Visual Studio с исходниками на C++.
- http://www.tamos.com/products/commview/cust_decoder_d.zip. Проект Delphi с исходниками на Pascal.

Сложный декодер

При реализации этого типа декодера, результат будет отображаться, как дополнительные элементы основного дерева декодера в окне пакетов. Подробное руководство по созданию такого декодера можно получить здесь:

http://www.tamos.com/products/commview/complex_decoder_c7.zip

Сложный декодер может быть написан только на Microsoft Visual C++, так как он основан на классах C++.

Техническая поддержка

Техническая поддержка пользовательских декодеров осуществляется "по мере сил", но мы не всегда сможем оказаться в состоянии разрешить любую вашу проблему.

Формат Log-файлов CommView

Для записи перехваченных пакетов в файлы .NCF CommView и CommView для WiFi используют формат данных, описанный ниже. Это открытый формат, который можно использовать в собственных приложениях для обработки log-файлов, созданных CommView. Этот формат также можно использовать для прямого обмена данными между CommView и пользовательским приложением. Пакеты идут последовательно. Перед каждым пакетом идет 24-байтовый заголовок, структура которого описана ниже. Все поля заголовка, размер которых превышает 1 байт, используют формат с прямым порядком байтов.

Суммарная длина заголовка составляет 24 байта. Если пакеты находятся в сжатом виде, поле **Объем данных** содержит объем разархивированных данных. Поле **Объем исходных данных**, в свою очередь, содержит объем исходных данных. Если пакет не был сжат, оба поля одинаковы.

<table>
<tr><th>Название поля</th><th>Длина (байты)</th><th>Описание</th></tr>
<tr><td>Объем данных</td><td>2</td><td>Длина тела пакета, который идет следом за заголовком</td></tr>
<tr><td>Объем исходных данных</td><td>2</td><td>Исходная длина тела пакета, без компрессии. Если компрессия не применялась, то это поле равно предыдущему</td></tr>
<tr><td>Версия</td><td>1</td><td>Версия формата пакета (текущая – 0)</td></tr>
<tr><td>Год</td><td>2</td><td>Дата создания пакета (год)</td></tr>
<tr><td>Месяц</td><td>1</td><td>Дата создания пакета (месяц)</td></tr>
<tr><td>День</td><td>1</td><td>Дата создания пакета (день)</td></tr>
<tr><td>Часы</td><td>1</td><td>Время создания пакета (часы)</td></tr>
<tr><td>Минуты</td><td>1</td><td>Время создания пакета (минуты)</td></tr>
<tr><td>Секунды</td><td>1</td><td>Время создания пакета (секунды)</td></tr>
<tr><td>Микросекунды</td><td>4</td><td>Время создания пакета (микросекунды)</td></tr>
<tr><td>Флаги</td><td>1</td><td>Битовые флаги:
<table>
<tr><td>Среда передачи</td><td>0...3</td><td>Тип пакета (0 - Ethernet, 1 - WiFi, 2 - Token Ring)</td></tr>
<tr><td>Расшифрован</td><td>4</td><td>Пакет был расшифрован (только для пакетов WiFi)</td></tr>
<tr><td>Поврежден</td><td>5</td><td>Пакет был искажен, т. е. имел некорректную контрольную сумму (только для пакетов WiFi)</td></tr>
<tr><td>Сжатие</td><td>6</td><td>Пакет хранится в сжатом виде</td></tr>
<tr><td>Зарезервировано</td><td>7</td><td>Резерв</td></tr>
</table></td></tr>
</table>

Уровень сигнала	1	Уровень сигнала в процентах (только для пакетов WiFi)
Скорость передачи	1	Скорость передачи данных в Мбит/с, умноженная на 2 (только для пакетов WiFi)
Диапазон	1	Диапазон передачи. 0x01 для 802.11a, 0x02 для 802.11b, 0x04 для 802.11g, 0x08 для 802.11a-turbo, 0x10 для 802.11 SuperG, 0x20 для 4.9 GHz Public Safety, 0x40 для 5 GHz 802.11n, 0x80 для 2.4 GHz 802.11n. (только для пакетов WiFi)
Канал	1	Номер канала (только для пакетов WiFi)
Направление	1	Для проводных пакетов - направление пакета. 0x00 для транзитных, 0x01 для входящих, 0x02 для исходящих. Для пакетов WiFi – старший байт для поля Скорость передачи, для тех случаев, когда однобайтное поле Скорость передачи недостаточно для хранения значения переменной (т.е. если значение превышает 255).
Уровень сигнала (dBm)	1	Уровень сигнала в dBm (для пакетов WiFi)
Уровень шума (dBm)	1	Уровень шума в dBm (для пакетов WiFi)
Данные	...	Тело пакета (без изменений, в исходном виде). Если установлен флаг компрессии, данные сжимаются с помощью свободно распространяемой библиотеки Zlib 1.1.4. Длина записывается в поле Data Length.

Покупка и поддержка

Работа демо-версии ограничена 30 днями. Вы можете приобрести полнофункциональную версию программы, перейдя на наш веб-сайт. Сейчас для CommView доступны два типа лицензий: **Standard** и **VoIP**. Наиболее дорогая лицензия **VoIP** активизирует все функции программы, включая анализатор VoIP, в то время как лицензия **Standard** не включает анализатор VoIP.

Одна зарегистрированная копия CommView может использоваться одним лицом для установки на одном компьютере и, дополнительно, на одном портативном компьютере. Более подробная информация о лицензировании доступна в лицензионном соглашении, сопровождающем продукт.

Как зарегистрированный пользователь, вы получаете:

- Полностью функциональную неограниченную временем использования копию программы.
- Бесплатные обновления, которые будут выпускаться в течение одного года со дня приобретения.
- Информацию об обновлениях и новых продуктах.
- Бесплатную техническую поддержку.

Заказать программу можно через наш веб-сайт:

http://www.tamos.ru/order/

Цены и лицензионное соглашение могут быть изменены нами в одностороннем порядке. Пожалуйста, посетите наш сайт для получения последней информации о продуктах.

Чтобы связаться со службой технической поддержки, посетите страницу:
http://www.tamos.ru/support/