CommView® for WiFi

Анализатор беспроводных сетей

Руководство пользователя
Версия 7.1

Содержание

Введение

О программе CommView for WiFi

CommView for WiFi - это специальная версия CommView, созданная для захвата и анализа сетевых пакетов в беспроводных сетях стандарта 802.11 a/b/g/n/ac. Она получает информацию от беспроводного сетевого адаптера и декодирует анализируемые данные.

С помощью CommView for WiFi вы можете видеть список сетевых соединений, IP-статистику и исследовать отдельные пакеты. Пакеты можно расшифровывать с использованием пользовательских ключей WEP или WPA-PSK и декодировать вплоть до самого низкого уровня с полным анализом распространенных протоколов. Предоставляется полный доступ к необработанным данным. Перехваченные пакеты могут быть сохранены в файл для последующего анализа. Гибкая система фильтров позволяет отбрасывать ненужные вам пакеты или перехватывать только те пакеты, которые вы захотите. Настраиваемые предупреждения позволяют сообщать пользователю о важных событиях, таких как подозрительные пакеты, высокая загрузка сети или неизвестные адреса.

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

CommView for WiFi - это полнофункциональный и доступный инструмент для администраторов беспроводных сетей, специалистов в области сетевой безопасности, сетевых программистов или тех, кто хочет видеть всю картину трафика в беспроводной сети. Для работы программы необходим совместимый беспроводной адаптер. Для получения списка адаптеров, которые были проверены на совместимость с CommView for WiFi, перейдите на наш веб-сайт. CommView выгодно отличает наличие современного декодера протоколов, способного анализировать более ста широко распространенных на сегодняшний день протоколов.

Что нового

Версия 7.1

- Быстрые фильтры для закладок «Узлы» и «Каналы»: теперь пакеты можно в один клик отсортировать по узлу, каналу, типу пакета или по скорости передачи данных.
- Поддержка Windows 10.
- Обновленные карта распределения IP-адресов и база данных MAC-адресов для производителей оборудования.

Версия 7.0

- Значительные обновления интерфейса: новые вкладки **Узлы** и **Каналы**, новые диаграммы и статистика.
- Интеграция с Wi-Spy для проведения спектрального анализа.

Версия 6.5

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

Версия 6.3

- Поддержка USB-адаптеров: Ubiquiti SR71-USB (802.11 a/b/g/n), Proxim ORiNOCO 8494 (802.11 a/b/g/n), TP-Link TL-WN821N (802.11 b/g/n), NETGEAR WN111 v2 (802.11 b/g/n).

Версия 6.2

- Поддержка новых адаптеров (для операционных систем Windows Vista и Windows 7): Intel 3945, 4965, 5100, 5150, 5300, 5350.
- Реконструкция UDP-потоков.
- Улучшения в декодере протоколов.

Версия 6.1

- Поддержка новых операционных систем: Windows XP 64-bit Edition, Windows Vista 64-bit Edition, 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).
- Поддержка отображения уровня шума на вкладке "Каналы".
- 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.

Работа с программой

Установка драйвера

CommView for WiFi - это инструмент для мониторинга беспроводных сетей 802.11 a/b/g/n/ac. Для работы с программой вам необходим совместимый беспроводной адаптер. Для активации функции мониторинга вашего беспроводного адаптера вам потребуется специальный драйвер, который включен в данный продукт. Когда CommView for WiFi не запущен, ваш адаптер сможет соединяться с другими беспроводными хостами или точками доступа, как и обычно. Когда CommView for WiFi запущен, ваш адаптер будет работать в пассивном режиме мониторинга, без возможности сетевого соединения.

Перед установкой нового драйвера для вашего беспроводного адаптера убедитесь, что он совместим с данной программой. Список поддерживаемых адаптеров доступен по адресу:

http://www.tamos.ru/products/commwifi/adapterlist1.php

CommView for WiFi может работать и с другими адаптерами. Если вашего адаптера нет в списке, обратитесь к FAQ.

Подробная инструкция доступна в программе через меню **Справка** => **Руководство по установке драйвера**.

Обзор

Интерфейс программы включает несколько вкладок, которые позволят вам просматривать данные и выполнять различные действия с перехваченными пакетами. Функциональность вкладок описана в таблице, приведенной ниже:

Название закладки	Описание
Узлы	Контроль захвата пакетов, показ детальной информации о точках доступа и ассоциированных станциях, статистики использования каналов, а также графическое представление спектра беспроводных сетей.
Каналы	Показ детальной статистики для каждого канала, а также наиболее активных узлов и графиков МБ/сек и Пакетов/сек.
Текущие IP-соединения	Показ детальной информации о текущих IP-соединениях между узлами беспроводной сети. Данная информация доступна, когда анализируемая беспроводная сеть не использует шифрование, или после ввода корректного ключа WPA или WEP.
Пакеты	Список захваченных пакетов; позволяет инспектировать и просматривать содержимое пакетов.
Анализ VoIP	Подробный VoIP-анализ перехваченного трафика. Обратите внимание, что данная вкладка доступна только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.
Log-файлы	Сохранение перехваченных пакетов в файлы в различных форматах, а также настройка автосохранения log-файлов.
Правила	Предоставление доступа к фильтрам пакетов, которые позволяют захватывать/игнорировать пакеты, основываясь на различных критериях, таких как как IP-адрес или номер порта.
Предупреждения	Настройка оповещений, уведомляющих о важных событиях, таких как подозрительные пакеты, повышение загруженности сети, неизвестные адреса и т.п.

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

Главное меню

Пункты меню программы описаны ниже.

Файл

Начать захват/закончить захват – начинает/прекращает сбор пакетов.

Блокировать сбор пакетов/возобновить – остановить/возобновить отображение пакетов в закладке **Пакеты**.

Режим удаленного мониторинга – показывает/скрывает панель инструментов для удаленного мониторинга. Панель позволяет соединяться с удаленными устройствами для захвата пакетов: Remote Agent for WiFi, RPCAP или Aruba remote capture.

Сохранить узлы как – сохранить содержимое закладки **Узлы**.

Сохранить каналы как – сохранить содержимое закладки **Каналы**.

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 узлы – стирает содержимое таблицы в закладке **Узлы**.

Очистить каналы – стирает содержимое таблицы в закладке **Каналы**.

Очистить текущие IP-соединения – стирает содержимое таблицы **Текущие IP-соединения**.

Очистить буфер пакетов – стирает содержимое буфера программы и закладки **Пакеты**.

Очистить данные VoIP – стирает содержимое закладки VoIP.

Производительность – отображает производительность программы: количество успешно перехваченных и непреднамеренно пропущенных драйвером устройства пакетов.

Выход – выход из программы.

Поиск

Найти пакет – вызывает диалог поиска пакета, который позволяет найти пакет, содержащий определенный 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 узлов - показывает/скрывает колонки в закладке **Узлы.**

Колонки каналов - показывает/скрывает колонки в закладке **Каналы.**

Колонки текущих IP-соединений – показывает/скрывает колонки в закладке **Текущие IP-соединения**.

Колонки пакетов – показывает/скрывает колонки в закладке **Пакеты**.

Каналы и спектр – показывает/скрывает панель **Каналы и спектр** в нижней части закладки **Узлы**.

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.

Реассоциация узлов – открывает окно реассоциации узлов.

Настройка

Шрифты – открывает подменю установки шрифтов, используемых в интерфейсе программы.

Ключи WEP/WPA – открывает окно, в котором можно ввести ключи WEP/WPA.

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 for WiFi 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.

Правила

Захватывать data-пакеты – включает/отключает захват пакетов типа "Data".

Захватывать management-пакеты – включает/отключает захват пакетов типа "Management".

Захватывать control-пакеты – включает/отключает захват пакетов типа "Control".

Игнорировать beacon-пакеты - включает/отключает захват пакетов типа "Beacon".

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 for WiFi.

Искать в справке – показывает оглавление файла-справки CommView for WiFi.

Онлайн учебник – открывает в браузере окно с учебником по работе с CommView for WiFi.

Проверить наличие обновлений – открывает мастер обновлений. Для того, чтобы скачать и установить последнее обновление для CommView for WiFi с сайта TamoSoft, следуйте инструкциям.

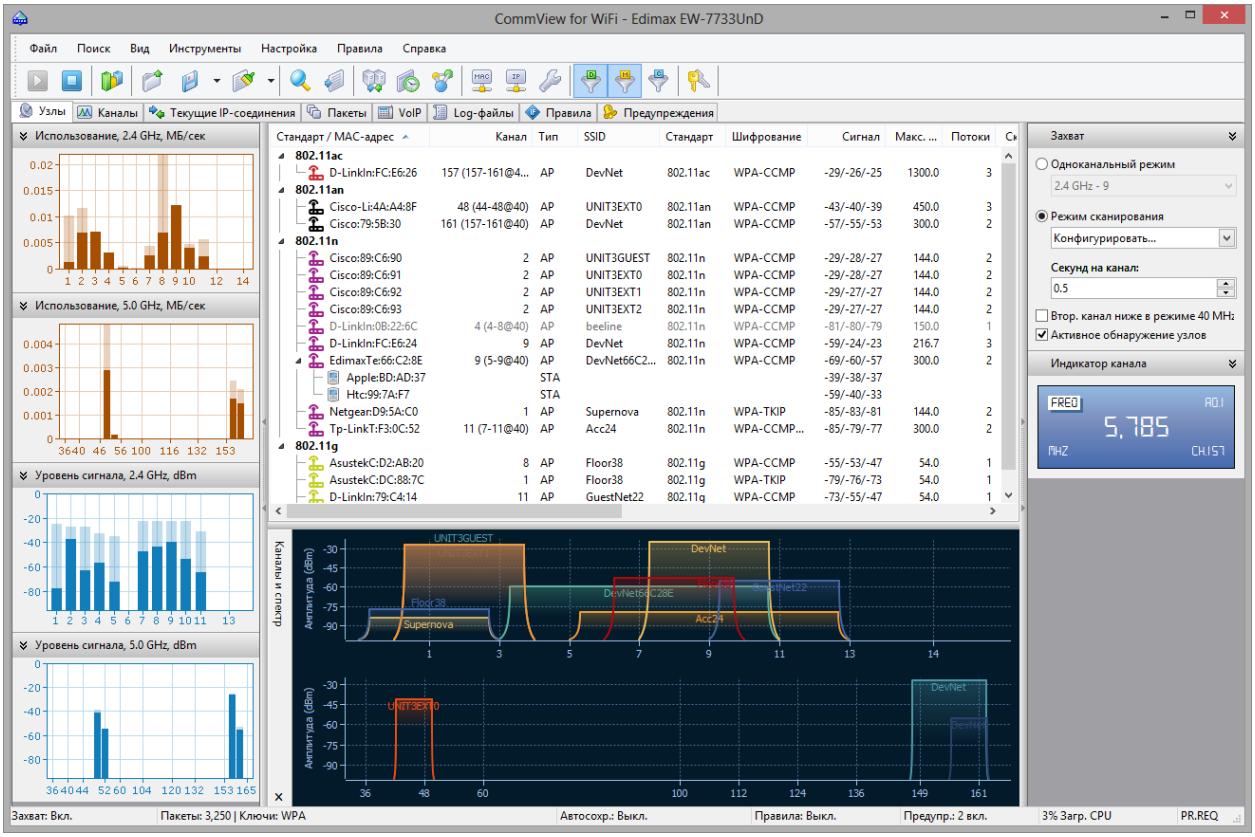
Активация – позволяет активировать вашу копию данного продукта или проверить факт ее активации.

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.

Узлы

Это главная закладка в приложении, которая используется для контроля захвата пакетов, показа детальной информации о точках доступа, ассоциированных станциях, а также статистики использования каналов и графического представления спектра беспроводной сети.



Окно содержит несколько изменяемых по размеру панелей, которые описаны ниже.

Панели «Захват» и «Индикатор канала»

Панель **Захват** позволяет выбрать два режима захвата: **Одноканальный режим** или **Режим сканирования**. Если вы выберете **Одноканальный режим**, приложение будет захватывать пакеты на одном канале (или на нескольких каналах, если вы используете несколько поддерживаемых USB-карт; подробная информация приведена ниже), который вы можете выбрать в выпадающем списке. Если вы выберет **Режим сканирования**, приложение будет проходить через каналы по кругу, т.е. приложение будет проводить захват на первом канале, после этого переключится на следующий канал и так далее, до тех пор, пока не дойдет до последнего канала, после чего начнется новый цикл сканирования. Для того чтобы сконфигурировать набор каналов для сканирования, нажмите кнопку **Конфигурировать** и проставьте флажки, чтобы выбрать или убрать определенные каналы. В зависимости от страны и регулятивного домена, установленного в вашем адаптере, список поддерживаемых каналов может различаться. Данный вопрос детально описан в главе FAQ. Для того чтобы сконфигурировать время, которое приложение тратит на сканирование каждого канала, используйте поле редактирования **Секунд на канал**.

В нижней части панели вы можете видеть две другие опции, которые контролируют захват пакетов. Опция **Втор. канал ниже первичного в режиме 40МГц** определяет позицию вторичного канала, когда используется связывание каналов (channel bonding) в диапазоне 2,4 ГГц. По умолчанию, вторичный канал 40 МГц в сетях 802.11 имеет более высокую частоту, чем первичный канал. Если вы проводите захват пакетов в сетевом окружении, где вторичный канал имеет более низкую частоту, поставьте флажок в этой опции. Флажок не будет иметь эффекта, если вторичный канал не может располагаться ниже первичного; это происходит, например, тогда, когда вы проводите захват с канала 1, 2, 3 или 4 на в диапазоне 2,4 МГц. Данная опция доступна только если ваш адаптер поддерживает захват каналов на частоте 40 МГц. Если включена опция **Активное обнаружение узлов,** приложение периодически посылает пакеты PROBE REQUEST. Такие пакеты облегчают поиск тех точек доступа, которые не транслируют свои SSID. Данная опция доступна только если ваш адаптер поддерживает генерацию пакетов.

После того, как вы сконфигурировали опции захвата, нажмите на кнопку **Начать захват** на панели инструментов. Если вы хотите переключиться на новый канал в то время, как у вас включен режим **Одноканальный режим**, или переключиться в **Режим сканирования**, вы можете сделать это без остановки захвата. Панель **Индикатор канала** отражает текущий канал и частоту в то время, пока приложение проводит захват пакетов.

Использование нескольких адаптеров для захвата нескольких каналов

Если вам нужно захватывать пакеты на нескольких каналах одновременно, вы можете сделать это, используя несколько USB-адаптеров. В таком режиме выпадающий список для выбора каналов предоставляет множественный выбор, что позволяет вам выбрать несколько каналов путем удержания клавиши **Ctrl.** Панель **Индикатор канала** при такой конфигурации отразит несколько индикаторов канал/частота. Обратите внимание, что использование нескольких адаптеров поддерживается только ограниченным числом моделей адаптеров. Подробная информация приведена в главе Многоканальный захват.

Список узлов

После того, как вы начали захват пакетов, программа начинает добавлять обнаруженные беспроводные узлы в список. Механизм анализа пакетов, используемый программой, детектирует и показывает все точки доступа, обнаруженные на просканированных каналах, станции в режиме ad hoc, а также ассоциированные станции в режиме infrastructure. Важно понимать, что радиомодуль беспроводного адаптера может принимать данные только с одного канала в любой момент времени. Поэтому, когда вы выбираете для мониторинга определенный канал, эта таблица будет содержать данные о точках доступа и станциях, ведущих обмен данными в рамках одного выбранного канала. Вы можете выбрать другой канал и повторно запустить процесс захвата в любой момент без сброса данных в таблице, или же включить режим **Сканирования**, чтобы приложение просканировало каналы так, чтобы вы могли увидеть активные узлы на различных каналах.

Значения колонок в таблице описаны ниже:

SSID/Стандарт/Канал – в зависимости от метода группировки, который вы выбрали (доступ осуществляется через контекстное меню **Группировать по**), первая колонка содержит беспроводные узлы, сгруппированные по SSID, стандарту 802.11 или каналу. Каждый

беспроводный узел представлен своими MAC-адресами или псевдонимами. Станции, ассоциированные с точками доступа, показываются как "дочерние" узлы, соединенные с родительскими, которые являются точками доступа.

Канал – канал, на котором работает данная точка доступа. Если точка доступа использует связывание каналов (channel bonding, каналы шириной 40, 80 или 160 МГц), первичный канал указывается первым, затем в скобках следует информация о дополнительных каналах.

Тип – тип узла. Возможные значения: AP (точка доступа), STA (станция в режиме инфраструктуры) и AD HOC (для станций в режиме ad hoc).

SSID – идентификатор сервиса. Уникальная строка, которая отличает одну беспроводную локальную сеть от другой.

Стандарт – стандарт 802.11 для точки доступа. Возможные значения: 802.11a, 802.11b, 802.11g, 802.11n, 802.11an и 802.11ac.

Шифрование – показывает, использует ли узел шифрование WEP или WPA. Для точек доступа в этой колонке будут показаны доступные методы шифрования.

Сигнал – уровень сигнала в формате минимальный/средний/максимальный. Среднее значение вычисляется с того момента, когда содержимое таблицы было сброшено в последний раз. За более подробной информацией обратитесь к главе Об уровне сигнала.

Максимальная скорость – максимальная физическая скорость передачи данных (PHY data rate), которую может предоставить точка доступа.

Потоки – количество пространственных потоков, поддерживаемых точкой доступа.

Скорость (Tx и **Rx)** – скорость передачи данных формате минимальный/средний/максимальный. Среднее значение вычисляется с того момента, когда содержимое таблицы было сброшено в последний раз.

Байт (Tx и **Rx)** –количество байтов, переданных и принятых узлом.

Пакеты (Tx и **Rx)** – количество пакетов, переданных и принятых узлом.

Повтор (Tx и **Rx)** – количество пакетов с выставленным флагом Retry (повтор).

Фрагментированые (Tx и **Rx)** – количество пакетов с выставленным флагом Fragmented (фрагментированные).

Вы можете показать или скрыть отдельные колонки, кликнув правой кнопки мыши на заголовок колонки или использовать меню **Вид**=> **Колонки узлов.** Расположение колонки можно изменить, просто "перетащив" ее на требуемое место. Клик правой кнопкой мыши в списке узлов вызывает меню со следующими командами:

Детали… – показывает окно Детальная информация по точкам доступа и станциям.

Быстрый фильтр – отфильтровывает и показывает в новом окне пакеты, пересылаемые в/из выбранного узла, а также те пакеты, в которых значение MAC-адреса выбранного узла равно значению BSSID-адреса.

Копировать MAC-адрес – копирует MAC-адрес узла в буфер обмена.

Создать псевдоним – открывает окно, где можно назначить легко запоминаемые псевдонимы MAC-адресу.

Сохранить узлы как – позволяет сохранять содержимое закладки Узлы в виде HTML-отчета.

Очистить узлы – очистить таблицу.

Дополнительная статистика – показывает окно со статистикой распределения протоколов и данных.

Группировать по – группирует список по SSID, каналу или стандарту 802.11.

Панели «Использование» и «Уровень сигнала»

Эти панели, расположенные слева в закладке **Узлы**, показывают графики использования каждого канала (два отдельных графика для каналов 2,4 ГГц и 5 ГГц). В дополнение к текущим уровням данные графики также отражают исторические максимумы, которые показываются приглушенным цветом.

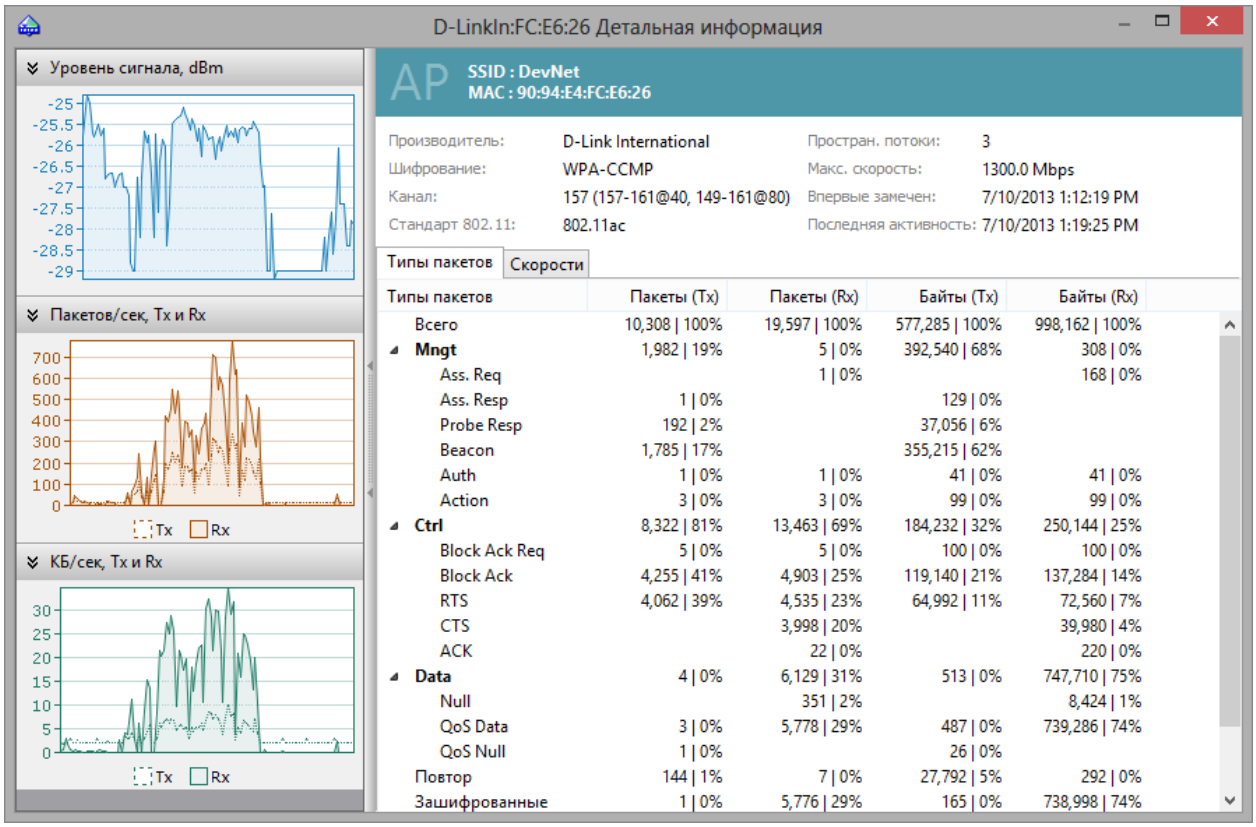
Панель «Каналы и спектр»

Эта панель, расположенная в нижней части закладки **Узлы**, выполняет две функции:

- Содержит графическое представление активных точек доступа, где каждая точка доступа показана с использованием линии, обозначающей ее приблизительную спектральную маску. Ширина маски зависит от ширины канала, поддерживаемой точкой доступа, а высота маски зависит от текущего уровня сигнала.
- Показывает спектральные данные, если подключен спектральный USB-анализатор Wi-Spy от MetaGeek. Спектральный анализатор проводит мониторинг полос частот, используемых беспроводными устройствами Wi-Fi. Поскольку что эти частоты нелицензированные, они часто используются источниками сигнала, использующими стандарты данных, отличных от Wi-Fi, например, такими как беспроводные камеры, микроволновые печи или беспроводные телефоны, что создает помехи. Назначение спектрального анализа – детектировать и идентифицировать источники помех, устранять их и/или идентифицировать каналы беспроводных сетей, где помехи будут минимальны. Информация подробно описана в главе Спектральный анализ.

Детальная информация по точкам доступа и станциям

При двойном клике на имя точки доступа или станции, отражаемых в закладке Узлы, CommView for WiFi выводит детальную информацию по выбранному узлу, как показано ниже.



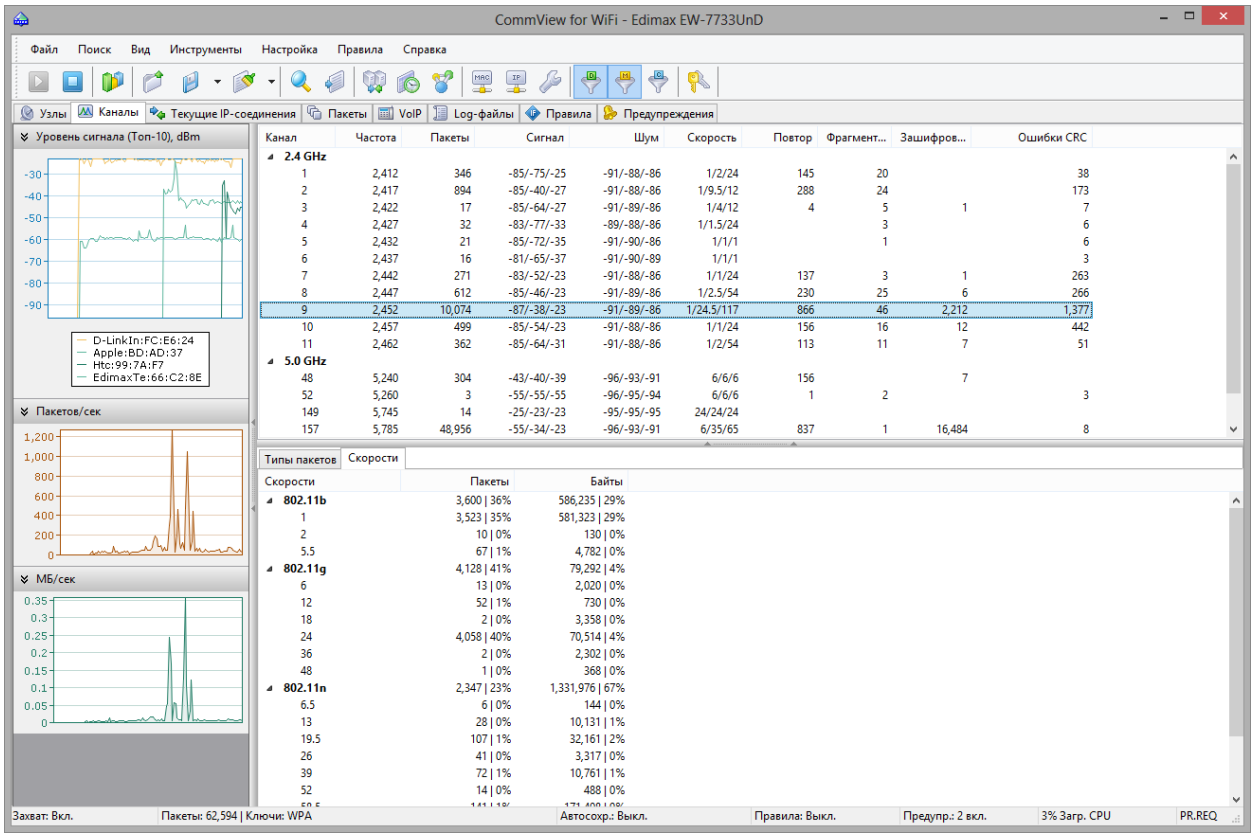
Верхняя панель показывает тип, MAC-адрес и SSID выбранного узла, а также другие ключевые детали, такие как канал, время, когда узел был впервые замечен, время последней активности и т.д. Панель использует тот же цвет, который применяется для показа выбранной точки доступа на панели **Каналы и спектр** в главном окне приложения.

На нижней панели вы можете видеть таблицы **Типы пакетов** и **Скорости**. Эти таблицы отражают детальную статистику по типам и подтипам пакетов, а также по скоростям передачи данных.

В левой панели вы можете увидеть три графика: **Уровень сигнала**, **Пакетов/сек** и **МБ/сек**. График **Уровень сигнала** показывает уровень сигнала для выбранного узла. Графики **Пакетов/сек** и **Мбит/сек** показывают количество пакетов и мегабайт в секунду, отосланных на/с данного узла. Обратите внимание, что данные графики обновляются только тогда, когда приложение проводит захват данных на канале, где работает данный узел. Это означает, что, например, если вы проводите захват данных на канале 5, и выбранная точка доступа также работает на канале 5, то графики будут обновляться постоянно. Однако если вы используете **Режим сканирования**, графики будут обновляться только когда приложение проходит через канал, на котором работает данная точка доступа.

Каналы

В этой закладке показана статистика по всем каналам, которые сканируются в данный момент или сканировались в прошлом. Количество каналов в таблице зависит от режима использования CommView for WiFi. Обычно, если вы наблюдаете только один канал, используемый вашей сетью, таблица будет содержать данные только о выбранном канале, поскольку радиомодуль вашего беспроводного адаптера может работать только с одним каналом одновременно. Если вы выберете для мониторинга другой канал, он сразу добавится в таблице. Если вы выберете режим **Сканирование** в закладке **Узлы**, таблица будет содержать информацию обо всех просканированных каналах, на которых был перехвачен хотя бы один пакет.



Поскольку в стандарте 802.11 используются перекрывающиеся частоты каналов в диапазоне 2,4 ГГц, вы могли заметить, что даже в случае настройки вашей сети на работу только с одним каналом, например 6, вы можете увидеть ненулевые значения для соседних каналов. В отличие от каналов на 2,4 ГГц, каналы на 5 ГГц не перекрываются.

В нижней панели вы можете видеть таблицы **Типы пакетов** и **Скорости**. Эти таблицы отражают детальную статистику по типам и подтипам пакетов, а также по скоростям передачи данных.

В левой панели вы можете увидеть три графика: **Уровень сигнала**, **Пакетов/сек** и **МБ/сек**. График **Уровень сигнала** показывает уровень сигнала для выбранного узла. Графики **Пакетов/сек** и **МБ/сек** показывают количество пакетов и мегабайт в секунду, отосланных на/с выбранного узла. Работая с информацией, приведенной в данных графиках, обратите внимание на следующее:

- Графики отображают данные только для выбранного канала.

- Графики обновляются только тогда, когда приложение проводит захват данных на выбранном канале. Это означает, что, например, если вы проводите захват данных на канале 2 и выбрали канал 2 в списке каналов, то графики будут обновляться постоянно. Если вы выберете канал 3, графики будут "заморожены". Если вы работаете в **Режиме сканирования** и выбираете любой канал, графики будут обновляться каждый раз, когда приложение будет проходить через этот канал.

Колонки таблицы имеют следующие значения:

Канал – номер канала.
Частота – частота канала в МГц.
Пакеты – общее количество захваченных пакетов.
Сигнал – уровень сигнала в формате минимальный/средний/максимальный. Среднее значение вычисляется с того момента, когда содержимое таблицы было сброшено в последний раз. За более подробной информацией обратитесь к главе Об уровне сигнала.
Шум – уровень шума в формате минимальный/средний/максимальный. Среднее значение вычисляется с того момента, когда содержимое таблицы было сброшено в последний раз. Некоторые адаптеры не поддерживают показ информации об уровне шуме, поэтому ваш адаптер не поддерживает эту функцию, эта колонка не будет видна.
Скорость – скорость передачи данных формате минимальный/средний/максимальный. Среднее значение вычисляется с того момента, когда содержимое таблицы было сброшено в последний раз.
Повтор – количество пакетов с выставленным флагом Retry (повтор).
Фрагментированные (Tx и **Rx)** – количество пакетов с выставленным флагом Fragmented (фрагментированные).
Зашифрованные – количество пакетов с выставленным флагом Encrypted (шифрование)
Ошибки CRC – количество пакетов с ошибками CRC. Для более подробной информации см. Об ошибках CRC и ICV.

Отдельные колонки можно показать или спрятать, если кликнуть на заголовок колонки правой кнопкой мыши или через меню **Вид** => **Колонки каналов**. Расположение колонки можно изменить, просто "перетащив" ее на требуемое место. Клик правой кнопкой мыши на название канала вызывает меню со следующими командами:

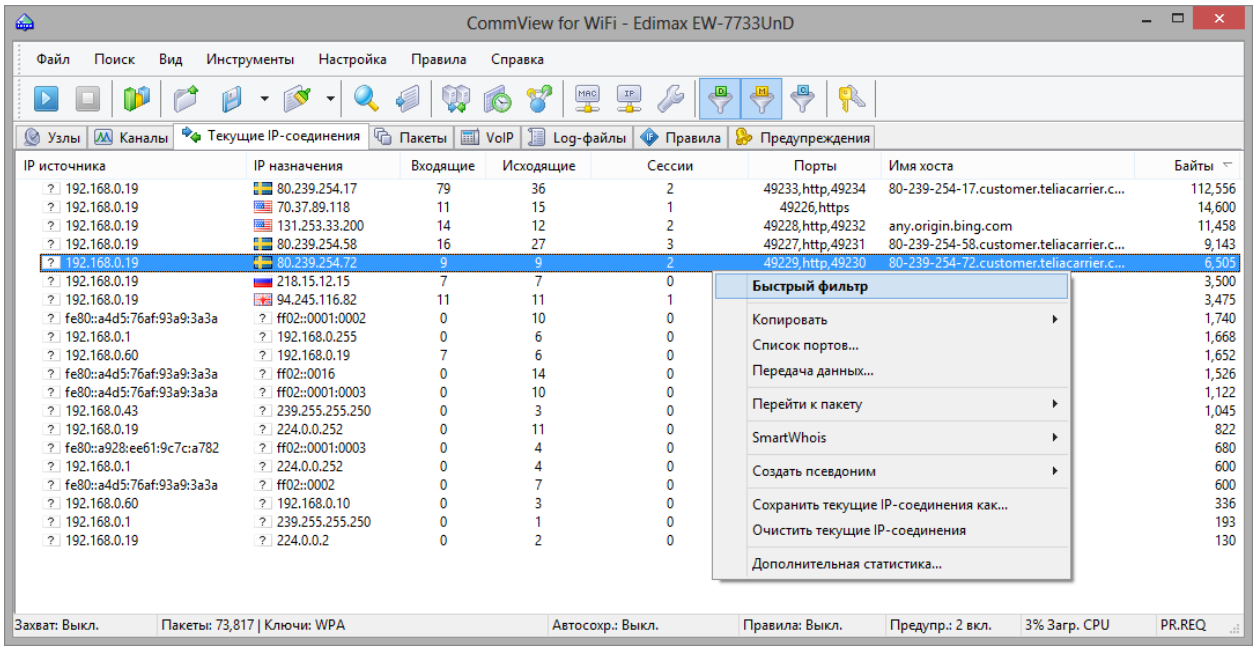
Быстрый фильтр – отфильтровывает и показывает их в отдельном окне пакеты, пересылаемые по выбранному каналу.
Сохранить каналы как – сохранить содержимое закладки каналов в формате HTML-отчета.
Очистить каналы – очистить таблицу.
Дополнительная статистика – показать окно со статистикой распределения протоколов и данных.

Клик правой кнопкой мыши по заголовкам таблиц **Типы пакетов** и **Скорости** вызывает меню со следующей командой:

Быстрый фильтр – отфильтровывает пакеты по выбранному типу или скорости и показывает их в отдельном окне.

Текущие IP-соединения

Эта закладка отображает подробную информацию о беспроводных соединениях вашего компьютера (только для протоколов IP и IPv6). Чтобы начать захват пакетов, выберите **Файл => Начать захват** или нажмите соответствующую кнопку на панели инструментов. Обратите внимание на то, что эта закладка не будет заполняться, если приложение не будет иметь возможности расшифровывать трафик сети, зашифрованный с помощью WEP или WPA. Если сеть использует шифрование WEP или WPA, все пакеты с данными передаются в зашифрованном виде, поэтому невозможно получить IP-адреса до тех пор, пока вы не введете правильный ключ для расшифровывания в меню **Настройка** => **Ключи WEP/WPA**. В случае расшифровывания WPA требуются дополнительные действия, см. главу Расшифровывание WPA.



Ниже описывается назначение колонок таблицы:

IP источника, IP назначения – пара IP-адресов, между которыми пересылаются пакеты. Программа автоматически определяет местонахождение IP-адреса, и в зависимости от ваших установок геолокации, может показывать название страны или флаг. Подробно информация описана в главе Установка опций.

Входящие – показывает число принятых пакетов.

Исходящие – показывает число посланных пакетов.

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. Подробно информация описана в главе Установка опций.

Имя хоста – показывает имя удаленного хоста. Если имя не может быть определено – колонка пуста.

Байт – количество байтов, переданных за сессию.

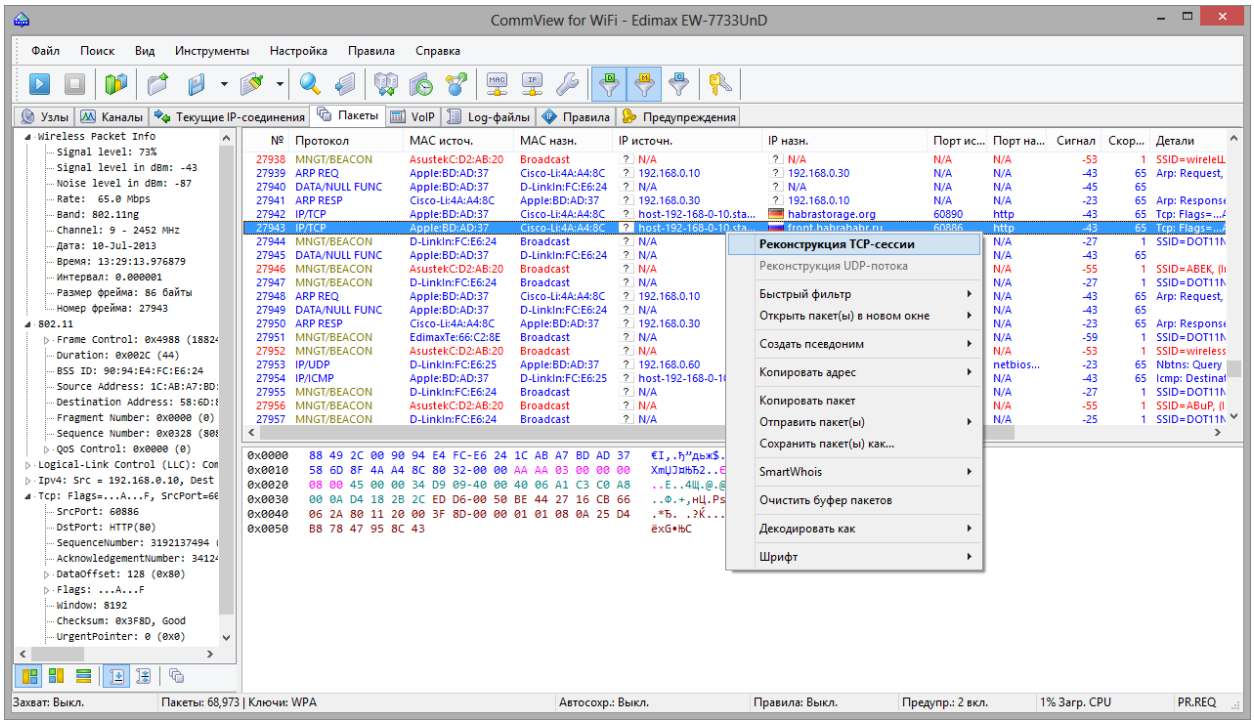
Последний пакет – показывает время, когда в течение сессии был отправлен / получен последний пакет.

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. Клик правой кнопкой мыши на список **Текущие IP-соединения** вызывает контекстное 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, удаленный 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 объеме 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 пакет, соответствующий критерию.
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 имена (алиасы) IP-адресам.
Сохранить текущие IP-соединения как… – позволяет сохранить содержимое закладки **Текущие IP-соединения** как HTML- или CSV-отчет.
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/Интервал – 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.
Сигнал – показывает уровень сигнала в процентах или dBm. За более подробной информацией обратитесь к главе Об уровне сигнала.
Скорость – показывает скорость передачи данных в Мбит/с.
Детали – показывает краткий отчет по пакету.
Ошибки – показывает информацию об ошибках. По умолчанию колонка не показывается.

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 пакетами.

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 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".

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).
Реконструкция UDP-потока – позволяет реконструировать UDP-поток, начиная с выбранного пакета (открывается новое окно, отображающее весь процесс обмена между двумя хостами).
Быстрый фильтр - позволяет 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 имена (алиасы) выбранным MAC- или IP-адресам.
Копировать адрес – копирует локальный MAC- или IP-адрес, удаленный 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) еще 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 for WiFi 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 for WiFi 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 for WiFi сохраняет пакеты в собственном формате с расширением .NCF. Вы всегда можете загрузить и просмотреть эти файлы при помощи утилиты Log viewer или просто загрузить любой NCF-файл, просто дважды кликнув на него. NCF является открытым форматом, детальное описание формата NCF приведено в главе Формат Log-файлов CommView.

Сохранение и Управление

Эта опция используется для сохранения перехваченных пакетов в файл вручную, а также для объединения или разбивки файлов. 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, отображенных 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 файлов .NCF на несколько частей, выберите опцию **Разделить log-файлы**. Следуя указаниям программы, вы можете 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; поэтому можно 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 for WiFi. 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 щелкните 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 for WiFi.

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 for WiFi.
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 определенный 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 сохраненными настройками фильтров в файлах .RLS, а не текущими.

Правила

CommView for WiFi позволяет вам использовать правила двух видов:

1. Первый вид (**беспроводные правила**) позволяют вам фильтровать пакеты по их типу: **Data**, **Management** и **Control**. Для того чтобы включить или выключить захват таких пакетов, используйте команду **Правила** в меню программы или соответствующие кнопки панели инструментов. В дополнение к этому вы можете включить или выключить захват beacon-пакетов, используя команду меню **Игнорировать beacon-пакеты**.
2. Второй вид (**обычные правила**) позволяет вам фильтровать пакеты по множеству критериев. Для установки этих правил перейдите в закладку **Правила** главного окна программы. Если установлено одно или несколько правил, то при отображении пакетов программа будет учитывать всю совокупность правил и покажет только те пакеты, которые подходят под эти правила. Если правило активно, то название соответствующие страницы выделяется жирным шрифтом.

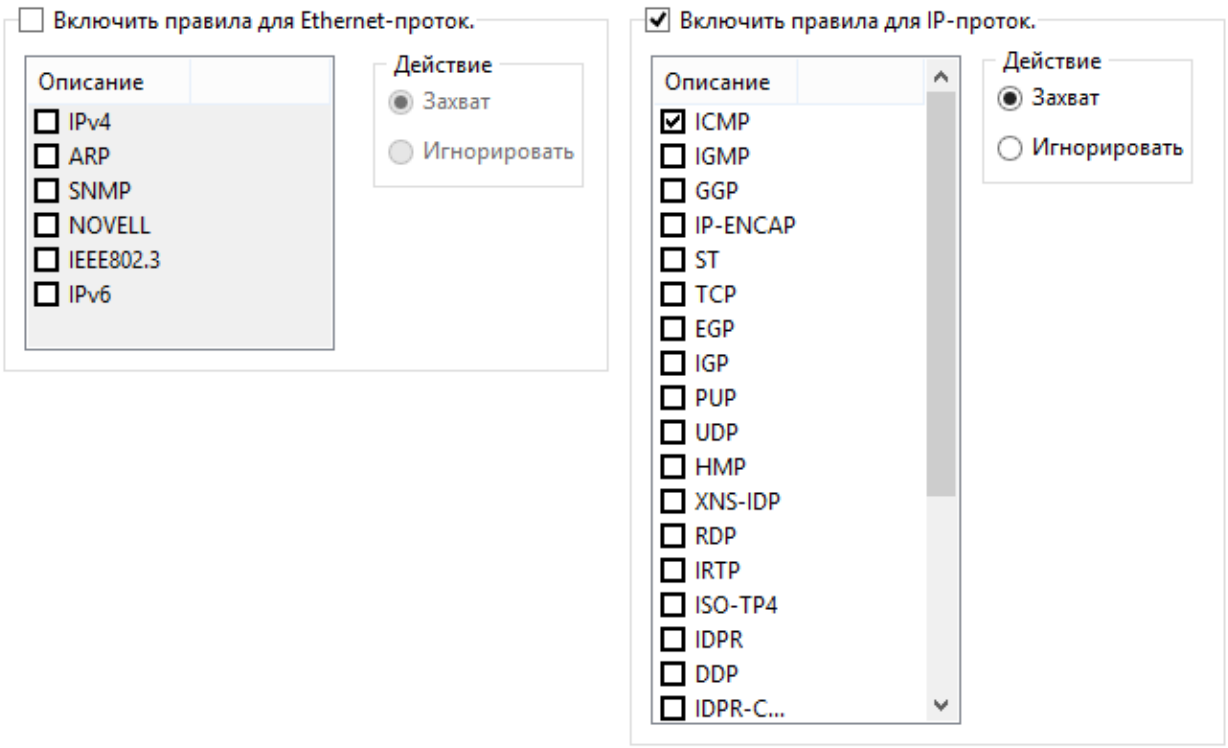
В строке состояния показано количество активных обычных правил. Здесь **не** показано количество активных беспроводных правил, поскольку состояние кнопок на панели инструментов ясно указывает, какое беспроводное правило активно в данный момент. Также помните, что беспроводные правила имеют преимущество перед обычными. Все захваченные пакеты сначала "проходят" через беспроводные правила, и только после этого происходит дальнейшая обработка. Если, к примеру, ни одна из трех кнопок беспроводных правил не нажата, программа не отобразит никаких пакетов.

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

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

Протоколы

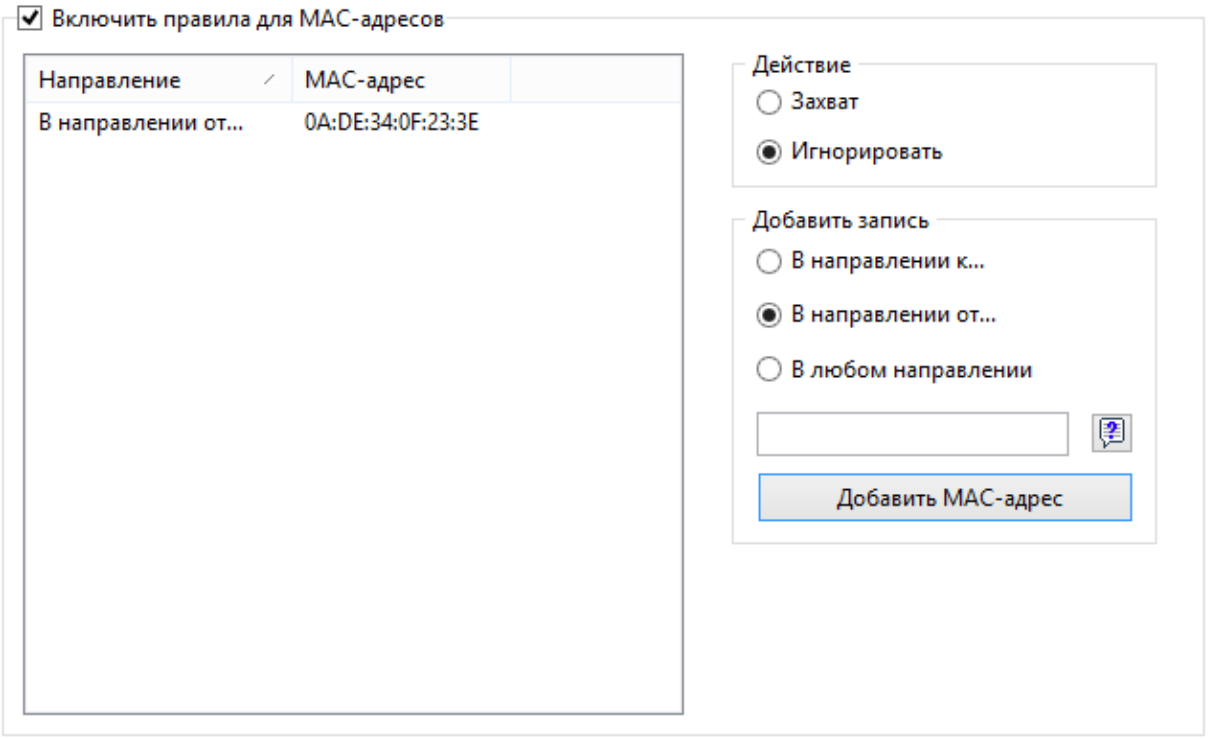
Позволяет игнорировать или перехватывать пакеты, основываясь на протоколах 2-го (Ethernet) и 3-го (IP) уровней, а также на направлениях пакетов.



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

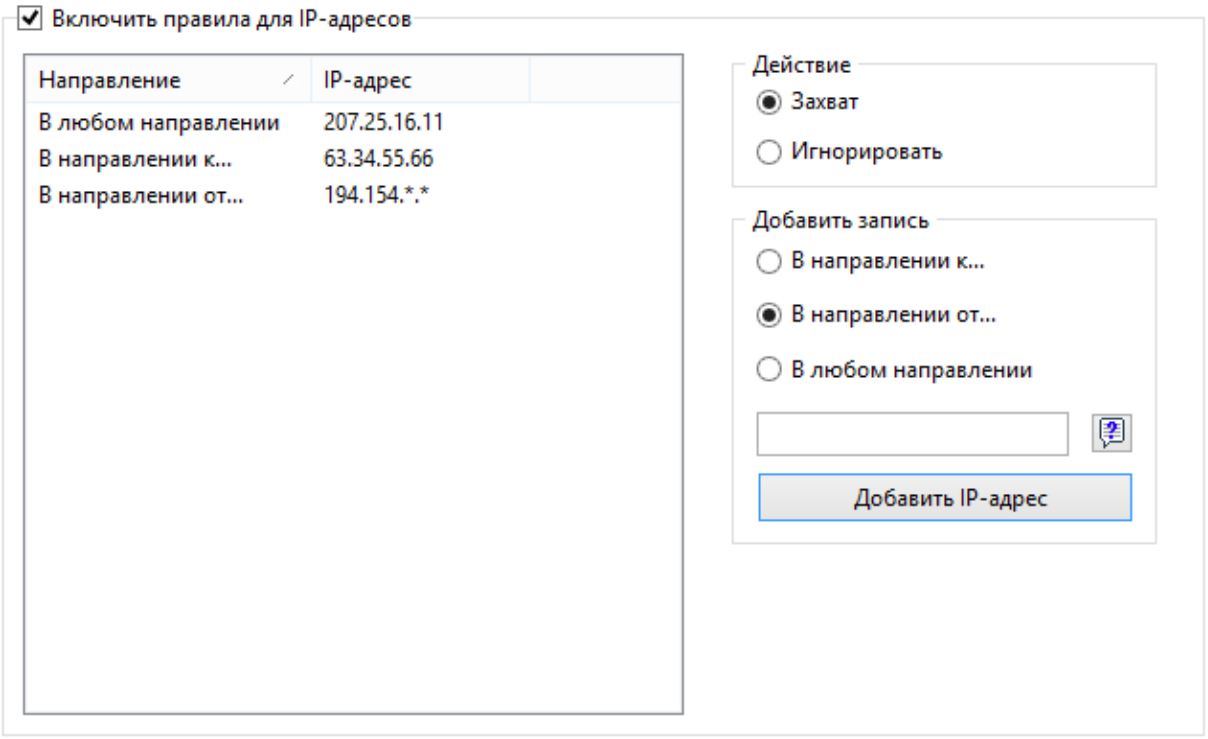
Позволяет игнорировать или перехватывать пакеты, основываясь на аппаратных MAC-адресах. Введите MAC-адрес в поле **Добавить запись**, выберите направление: **В направлении к…**, **В направлении от…** или **В любом направлении.** Затем и нажмите **Добавить MAC-адрес** и новое правило будет отображено. 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**.



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

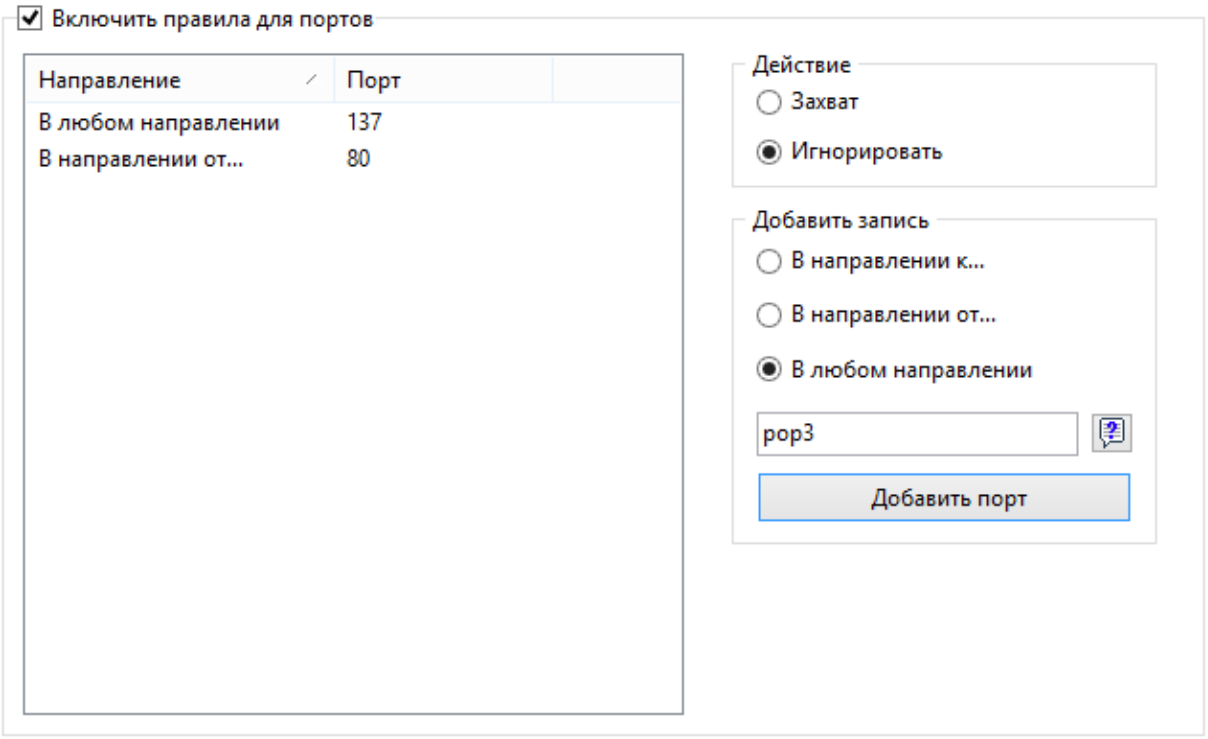
Позволяет игнорировать или перехватывать пакеты, основываясь на IP-адресах. Введите IP- или IPv6-адрес в поле **Добавить запись**, выберите направление: **В направлении к…**, **В направлении от…** или **В любом направлении.** Затем нажмите **Добавить IP-адрес** и новое правило будет отображено. Далее 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

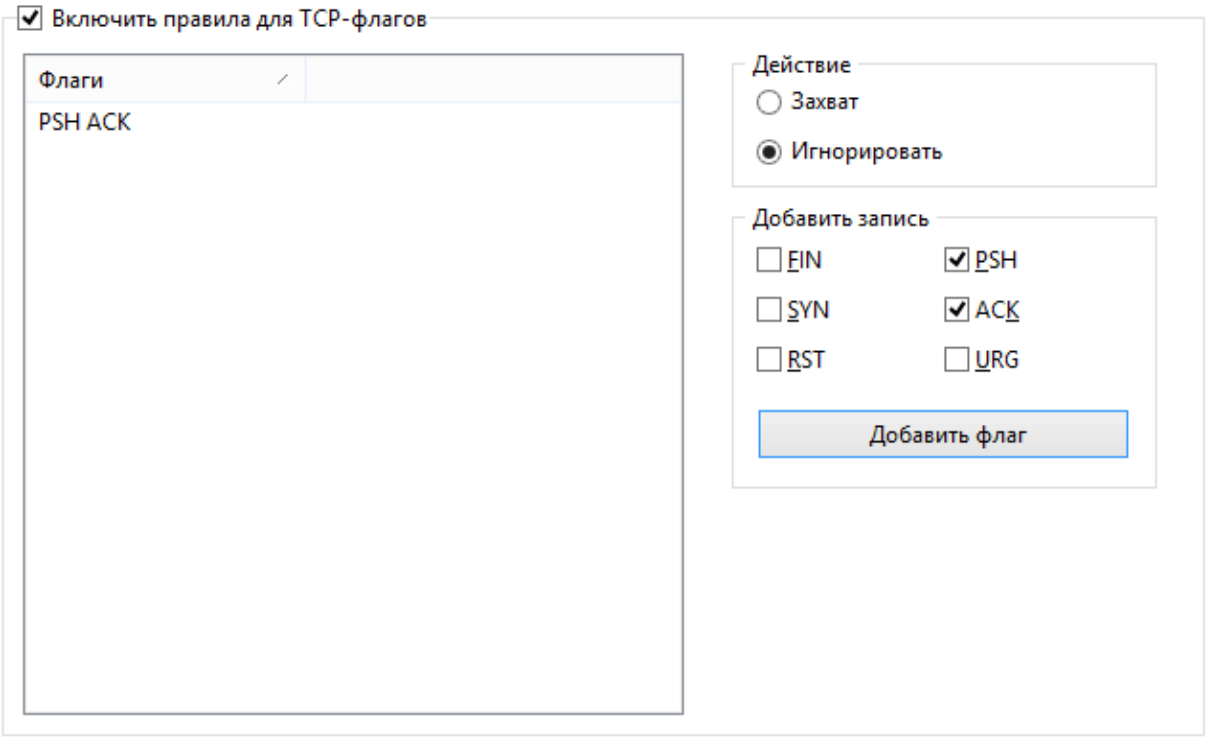
Позволяет игнорировать или перехватывать пакеты, основываясь на номерах портов. Введите номер порта в поле **Добавить запись**, выберите направление: **В направлении к…**, **В направлении от…** или **В любом направлении.** Затем нажмите **Добавить порт** и новое правило будет отображено. Далее следует выбрать действие, которое будет совершено при обработке нового пакета: он может быть либо перехвачен, либо проигнорирован. Чтобы добавить порт в список, дважды щелкните 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 for WiFi игнорировать входящий HTTP-трафик наряду с входящим/исходящим трафиком NetBIOS Name Service. Пакеты, проходящие между портами, будут перехвачены.

TCP-флаги

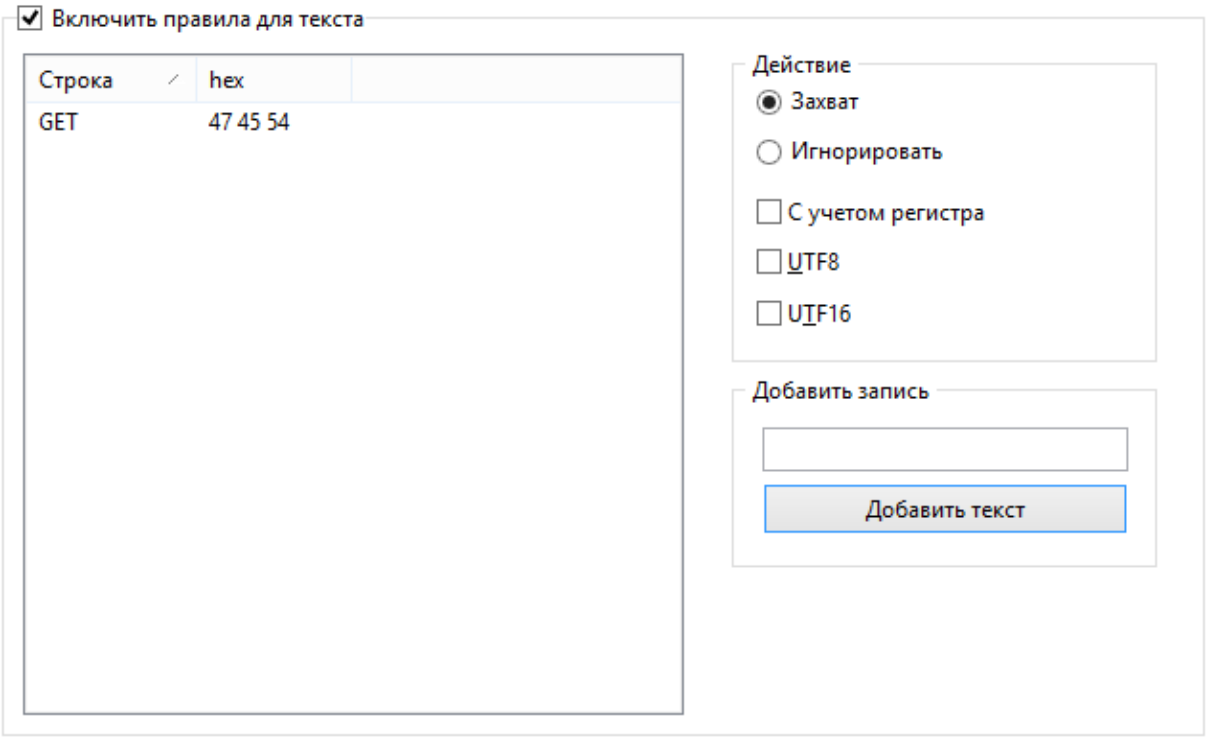
Позволяет игнорировать или перехватывать пакеты, основываясь на TCP-флагах. Выберите флаг или комбинацию флагов в поле **Добавить запись** и нажмите **Добавить флаги.** Новое правило будет отображено. Далее следует выбрать действие, которое будет совершено при обработке нового пакета с TCP-флагом: он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



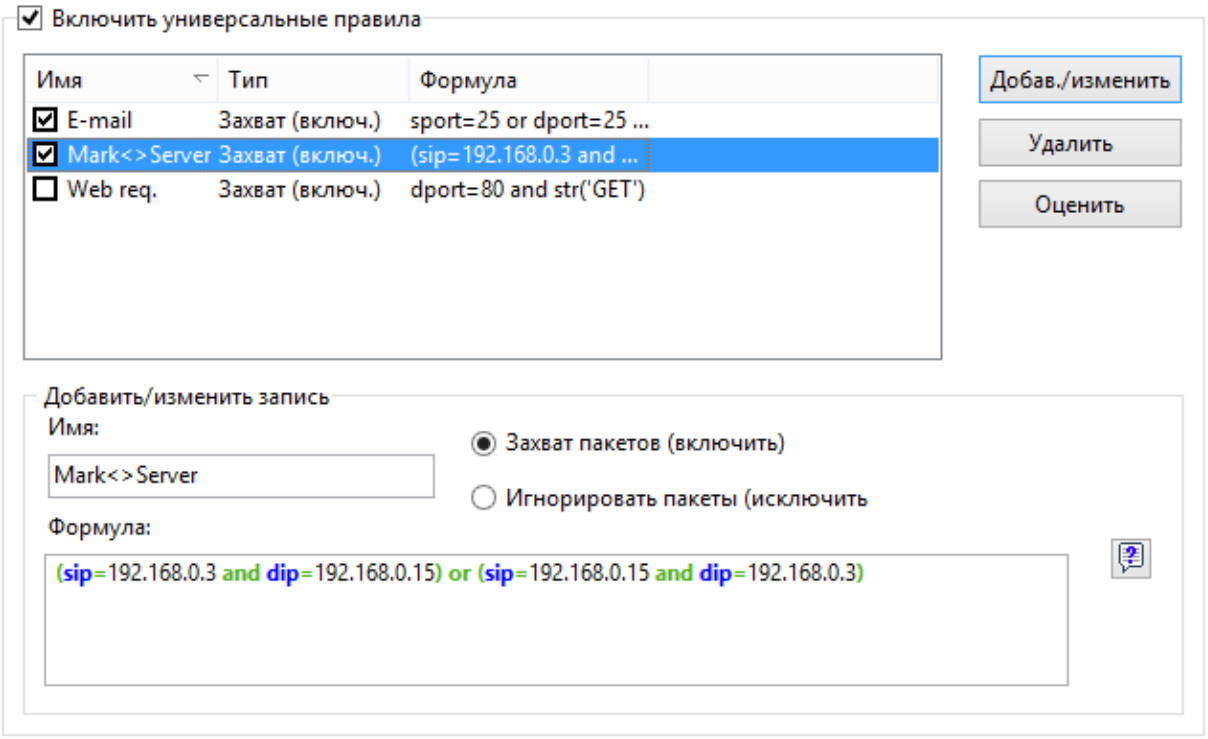
В этом примере показано, как перехватывать только те пакеты, которые содержат текст "GET". При необходимости установите флажок **С учётом регистра**, если вы хотите сделать правила регистрозависимыми. Выберите опции **UTF8** или **UTF16**, если вы хотите, чтобы перехватывались пакеты с текстом только 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.

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 несколько позитивных правил ("Захват") объединяются логическим оператором OR ("ИЛИ"), т.е. для трех активных правил RULE1, RULE2, RULE3, результирующим будет правило RULE1 OR RULE2 OR RULE3. Если вы также используете негативные правила ("Игнорировать"), то они будут добавлены в результирующее правило с логическим оператором AND ("И"), так как результирующее правило с логическим оператором OR ("ИЛИ") не имеет смысла.

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*), IP-адреса с карт-бланшами (то есть, *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 определенное 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 определенную строку. Функция имеет три аргумента: образец поиска, местоположение, чувствительность к регистру. Первый аргумент – строка, например, '*GET*'. Второй аргумент – число, показывающее смещение строки в пакете. Счет 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 учета регистра) или true (с учетом регистра). Второй и третий аргументы необязательны, по умолчанию

имеют значения –1 и false соответственно (искать во всем пакете, без учета регистра). Примеры: *str('GET',-1, false)*, *str('GET',-1)*, *str ('GET')*.

hex - Содержимое пакета. Задает условие, что пакет должен содержать определенный 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. Отсчет ведется с нуля, т. е. первый байт пакета соответствует смещению, равному 0. Чтобы искать во всем пакете, задайте смещение равным –1. Второй аргумент необязателен, по умолчанию имеет значение –1 (искать во всем пакете). Пример: *hex(0x04500, 14)* , *hex(0x4500, 0x0E), hex (0x010101)*.

bit - Содержимое пакета. Задает условие, что пакет должен содержать по указанному смещению определенный бит, имеющий значение 1. В этом случае функция вернет код возврата *true*. Если же искомый бит имеет значение 0 или находится за пределами пакета - функция вернет 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)*.

ToDS, FromDS, MoreFrag, Retry, Power, MoreData, WEP, Order, Ftype, FsubType, Duration, FragNum, SeqNum - позволяют вам использовать значения полей заголовков пакетов стандарта 802.11. Имена параметров полностью соответствуют именам полей заголовков пакетов, описанных в спецификации стандарта 802.11. Допустимыми значениями для полей ToDS, FromDS, MoreFrag, Retry, Power, MoreData, WEP и Order являются 0 или 1. Для полей Ftype, FsubType, Duration, FragNum и SeqNum допустимы также другие числовые значения. Для более подробной информации о смысле этих полей и допустимых значениях, обратитесь к спецификации стандарта 802.11.

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.

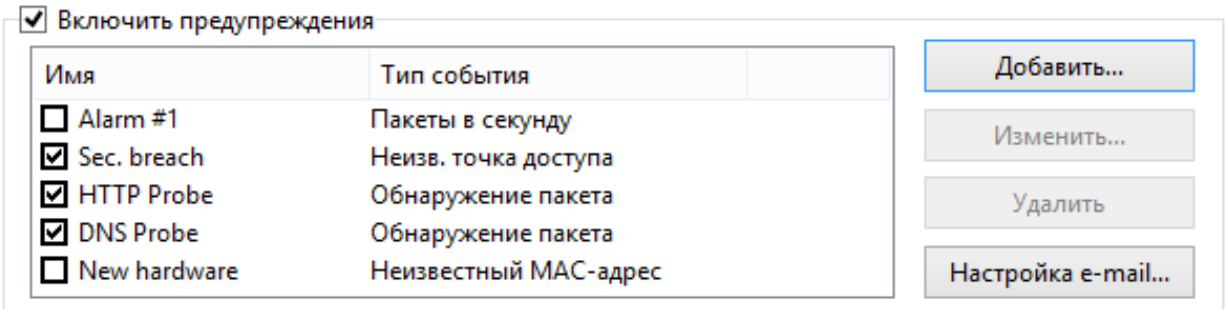
- (smac=00:00:21:0A:13:0E or smac=00:00:21:0A:13:0F) and etherproto=arp // Захватывать пакеты ARP, посылаемые двумя компьютерами с MAC 00:00:21:0A:13:0E и 00:00:21:0A:13:0F.
- ipproto=udp and dport=137 // Захватывать пакеты UDP/IP, посылаемые в порт 137.
- dport=25 and str('RCPT TO:', -1, true) // Захватывать 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".
- not(ftype=0 and fsubtype=8) // Игнорировать management-пакеты типа beacon
- ftype=2 and wep=1 // Перехватывать зашифрованные пакеты данных
- MoreFrag=0 and FragNum=0 // Перехватывать нефрагментированные пакеты

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 определенной последовательности байтов в пакетах, неожиданное подключение новых устройств.

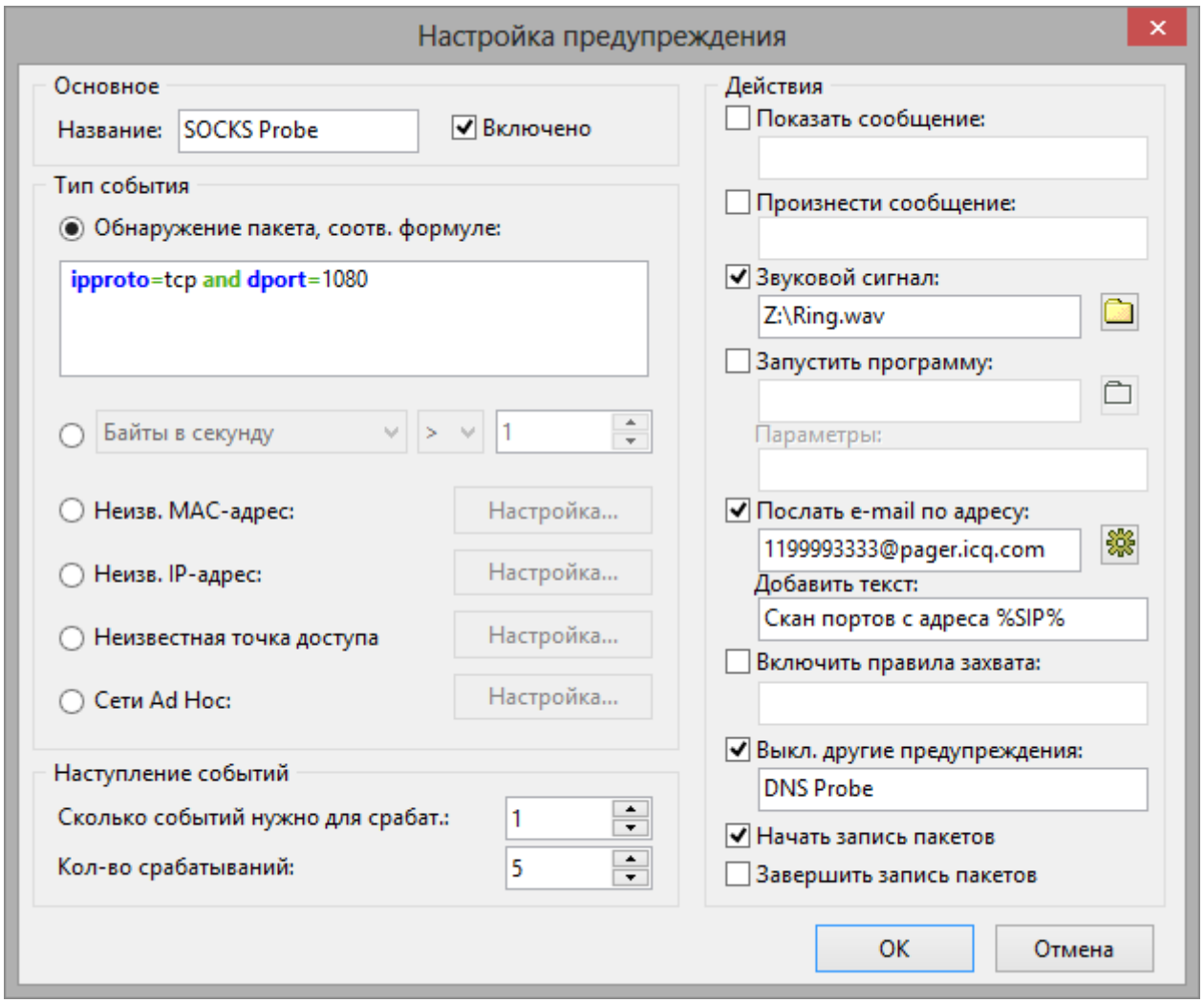
Важно: предупреждения могут показываться только для тех пакетов, которые прошли фильтры программы. Если, например, вы сконфигурировали программу таким образом, что она отсеивает только UDP-пакеты на основе соответствующего правила, в то время, как ваше предупреждение должно показываться при получении UDP-пакета, то такое предупреждение никогда не будет показано.

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 1 Мбайт/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.

- **CRC-ошибки в секунду**: Это предупреждение сработает при превышении указанного уровня частоты возникновения ошибок CRC.
- **Retry-пакеты в секунду**: Это предупреждение сработает при превышении указанного уровня частоты возникновения Retry-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- и 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.
- **Неизвестная точка доступа**: Это предупреждение сработает при получении программой beacon-пакета от неизвестной точки доступа. В Настройках можно задать MAC-адреса известных точек доступа. Это предупреждение может быть полезно для обнаружения неавторизованных точек доступа.
- **Сети Ad Hoc**: Это предупреждение сработает при перехвате программой beacon-пакета от неизвестной Ad Hoc-станции. Опция **Настройка** позволяет задать список известных MAC-адресов Ad Hoc-станций, если они есть. Это предупреждение полезно для обнаружения несанкционированного использования Ad Hoc-сетей.

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 произойдет трижды. При редактировании уже существующего предупреждения происходит обнуление внутреннего счетчика 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 это число, можно настроить CommView for WiFi на многократные срабатывания предупреждений. При редактировании уже существующего предупреждения происходит обнуление внутреннего счетчика 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 приведен 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 замещен 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 for WiFi 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 for WiFi начнет 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.

Ключи WEP/WPA

Для расшифровывания перехваченных пакетов можно ввести ключи в окне **Ключи WEP/WPA**. Без этих ключей программа не сможет расшифровать пакеты данных, передаваемые в вашей локальной беспроводной сети. Поскольку в некоторых сетях используется смешанный режим шифрования, когда идентификация производится по WEP и WPA, вы можете ввести ключ WEP и условную фразу-пароль WPA одновременно.

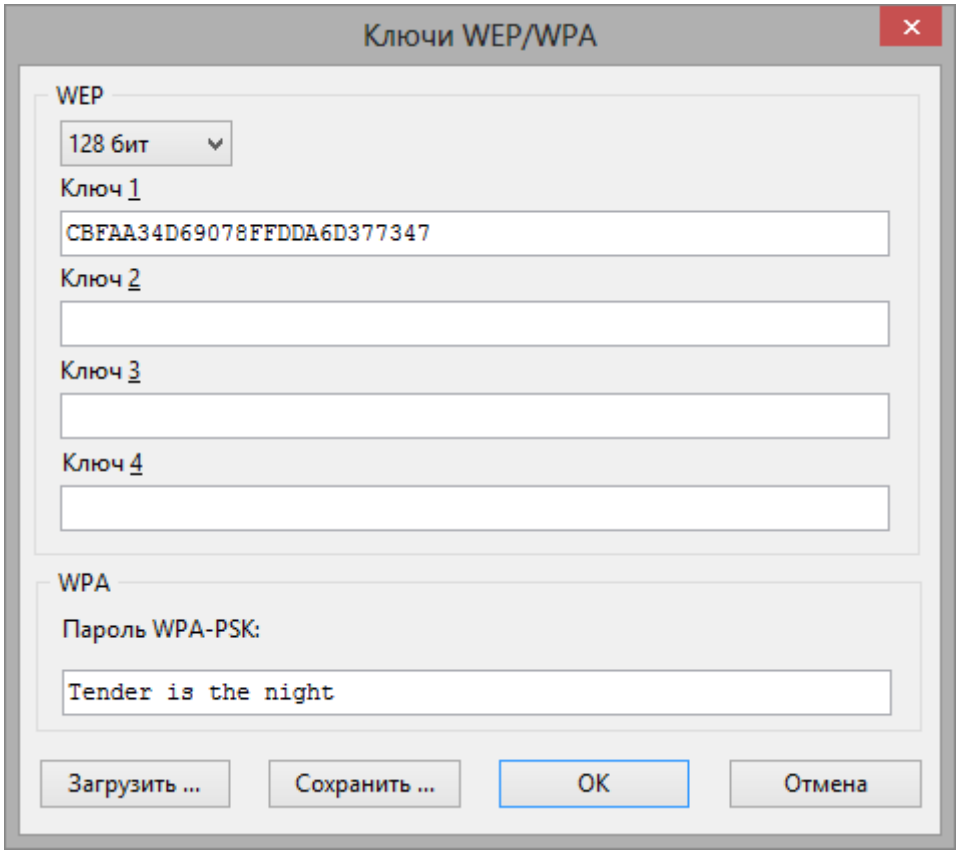
WEP

Стандарт позволяет использовать до четырех ключей WEP, так что вы можете указать один, два, три или четыре ключа. Длину ключа можно выбрать из выпадающего списка. Поддерживаемые значения – 64, 128, 152, и 256 бит, так что вам потребуется ввести шестнадцатеричные строки длиной 10, 26, 32 и 58 соответственно.

WPA

Стандарт WPA (защищенный доступ к WiFi) регламентирует количество режимов идентификации и шифрования. Не все из них поддерживаются программой CommView for WiFi из-за ограничений, связанных с ограничениями базовой модели безопасности. CommView for WiFi поддерживает расшифровывание WPA или WPA2 в режиме PSK с использованием протокола TKIP или AES/CCMP. Вы можете ввести как фразу-пароль, так и шестнадцатеричную строку длиной 64.

Важно: информация о том, как CommView for WiFi обрабатывает трафик, шифрованный WPA, смотрите в главе Расшифровывание WPA. Если вы ввели новый WPA-пароль, вам может понадобится модуль Реассоциации узлов.

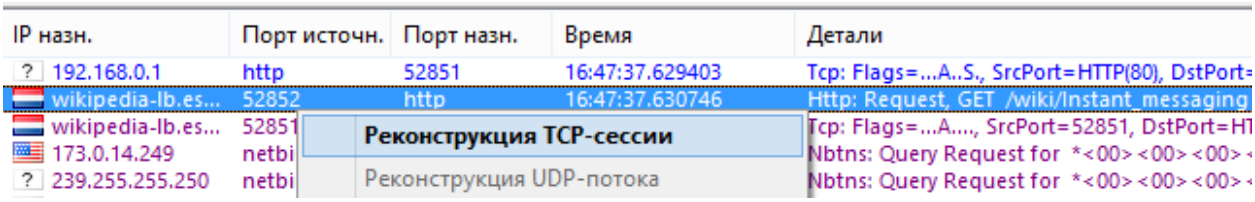


Для сохранения текущего ключа нажмите **Сохранить**. Для загрузки ранее сохраненного ключа нажмите **Загрузить**.

Ключи, загруженные или введенные в этом диалоге будут применены к пакетам, перехваченным в режиме реального времени, а также ко всем NCF-файлам, сохраненным ранее. Когда перехваченные пакеты сохраняются в файл NCF, те пакеты, которые были успешно расшифрованы будут сохранены в расшифрованном виде, а те пакеты, которые не могут быть расшифрованы будут сохранены в исходном виде.

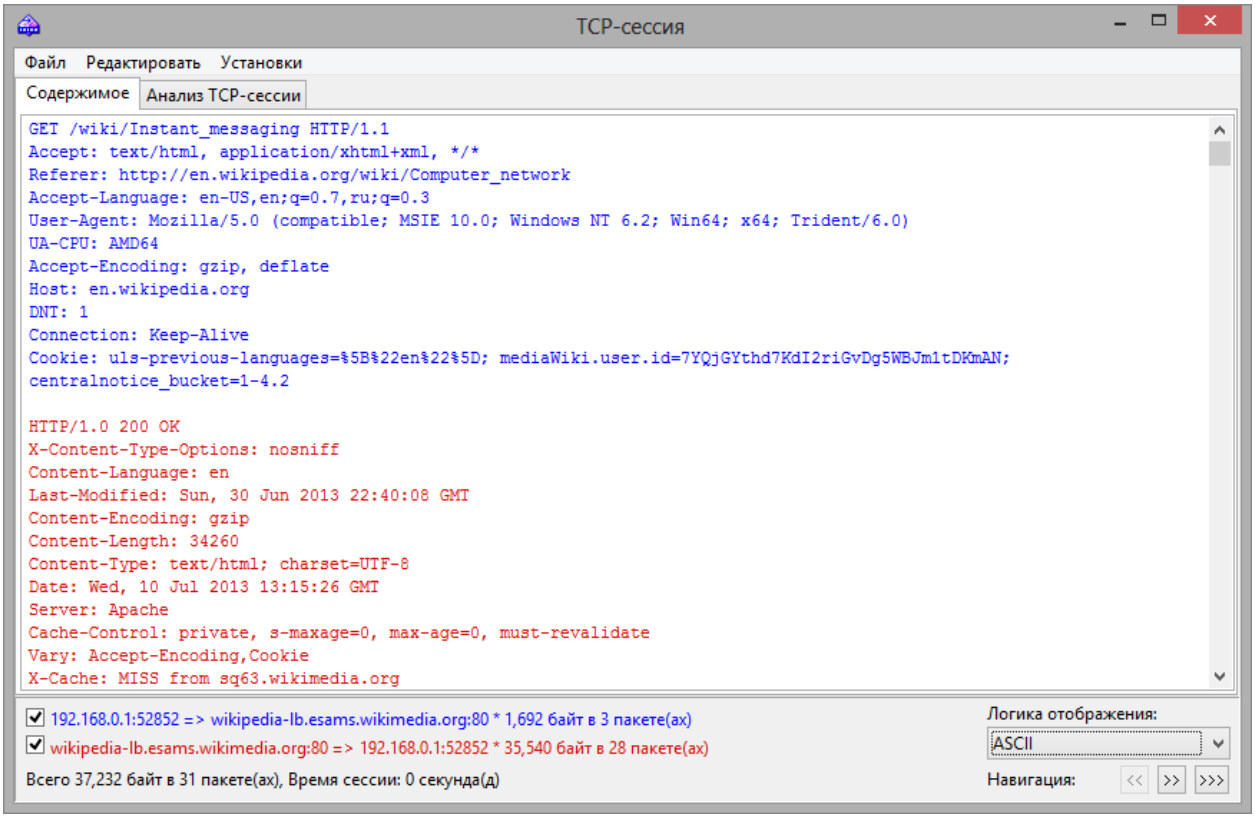
Реконструкция TCP-сессий

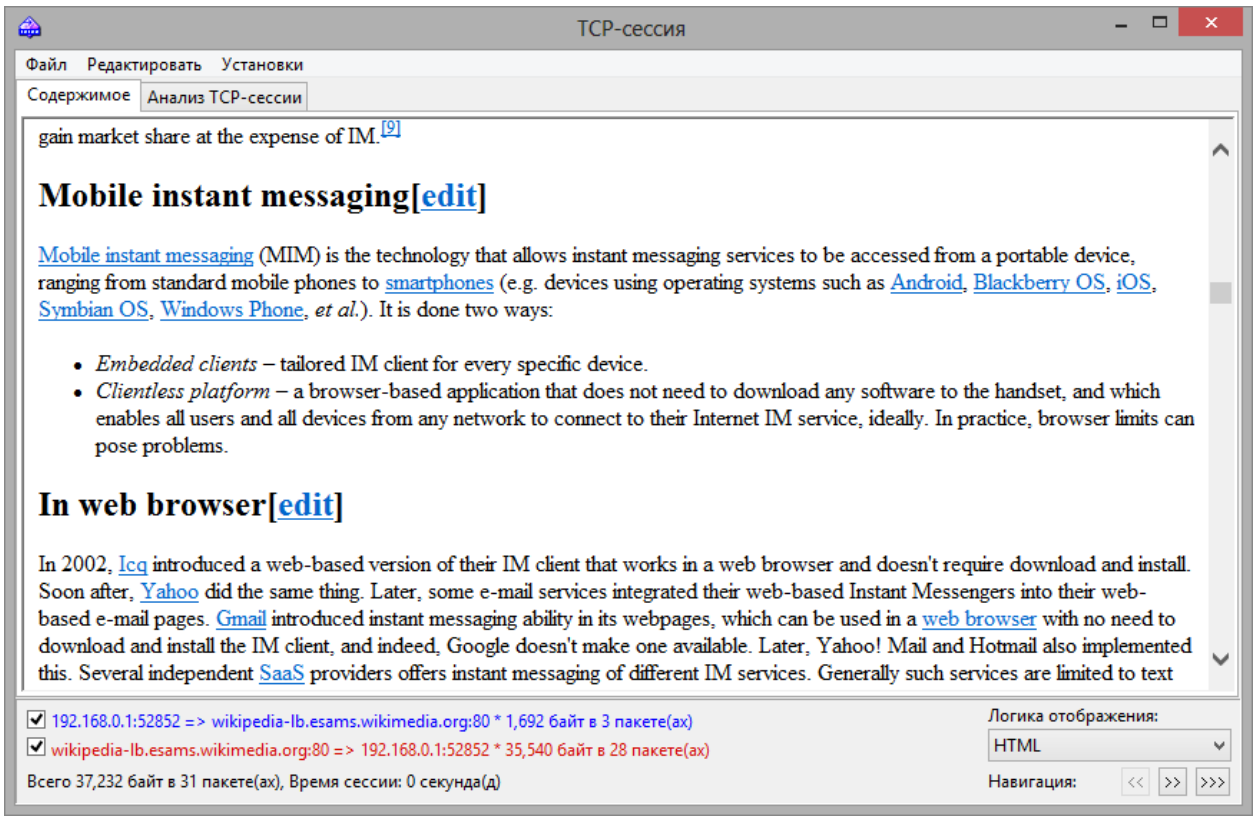
С помощью этой утилиты можно просмотреть процесс обмена между двумя хостами по TCP. Чтобы восстановить TCP- сессию, необходимо сначала выбрать пакет TCP в закладке **Пакеты**. В зависимости от установок (**Искать начало сессии при реконструкции TCP-сессий** в меню **Настройка** => **Установки** => **Декодер**), 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:



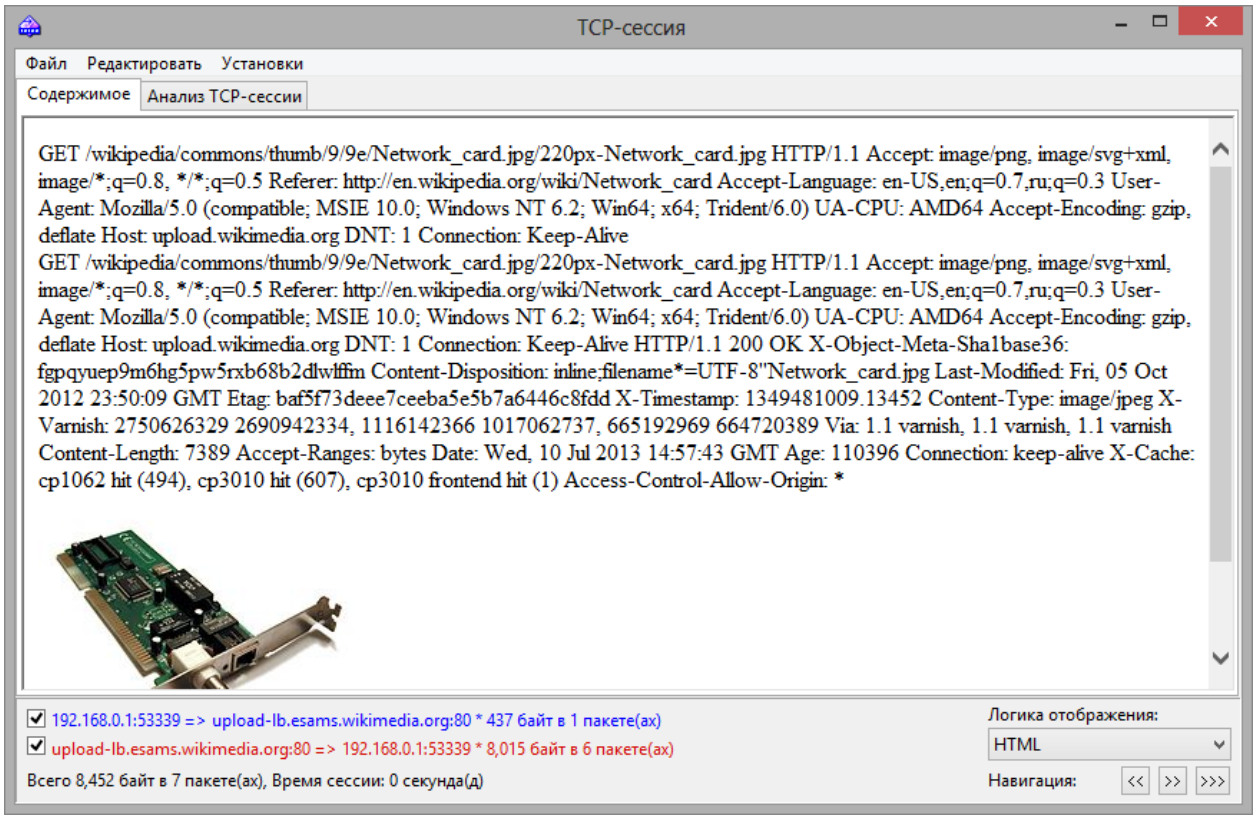
Процесс восстановления лучше всего работает для текстовых протоколов, таких как POP3, Telnet, или HTTP. Возможно также восстановление процесса пересылки большого ZIP-архива, но на обработку нескольких мегабайт данных CommView for WiFi потребуется слишком много времени. Кроме того, в большинстве случаев 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:





В режиме отображения HTML гипертекстовые страницы обычно 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 for WiFi 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, HTML или RTF-формате, выбрав **Файл => Сохранить как…**. При сохранении в текстовом формате, Вы получите файл в кодировке Unicode UTF-16. При сохранении информации в HTML-формате, кодировка выходного файла будет зависеть от значения опции **Логика отображения**. Если выбран режим просмотра HTML, то файл будет иметь формат ANSI; для остальных режимов просмотра – формат Unicode UTF-16. Обратите внимание, что сохраняя HTTP-сессию вместе с изображениями, изображения из HTML-файла сохраняются во временной директории вашего диска, поэтому если вы хотите их оставить, откройте сохраненный файл в вашем браузере и пересохраните файл в формате, который может включать изображения (например, MHT) до того, как закроете CommView for WiFi.

Для поиска строки в пределах текущей сессии, нажмите **Редактировать** => **Найти…**

Анализ сессий

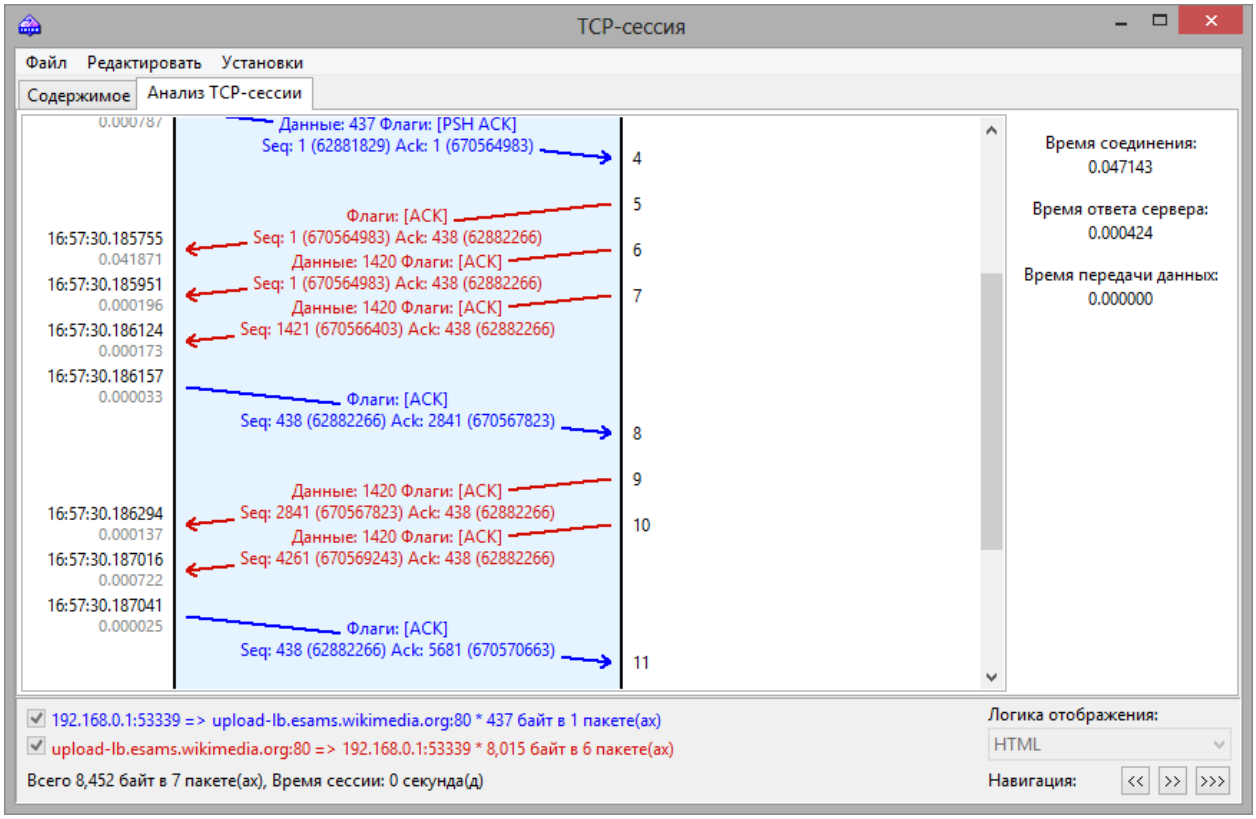
В закладке **Анализ TCP-сессии** окна **TCP-сессия** показывается восстановленная TCP-сессия в графическом виде. Здесь вы увидите потоки данных в этой сессии, ошибки, задержки и факты повторной передачи потерявшейся информации.

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. Однако, поскольку в отличие от протокола TCP, UDP-протокол не требует установления соединения, между реконструкциями TCP-сессий и UDP-потоков есть следующие отличия:

- 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 пакета

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 отчеты

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 подпротоколов. Дважды щелкнув 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 **Отчет**, можно создавать автоматические отчеты в HTML или текстовом формате CSV.

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

Общее

Гистограммы вида "Пакетов в секунду" и "Байт/бит в секунду", индикатор использования пропускной способности (удельный трафик, деленный 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 подсчета: 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 подсчета: 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 ее, 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, щелкните 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.**

Отчет

Закладка позволяет настроить автоматически создаваемые отчеты 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.

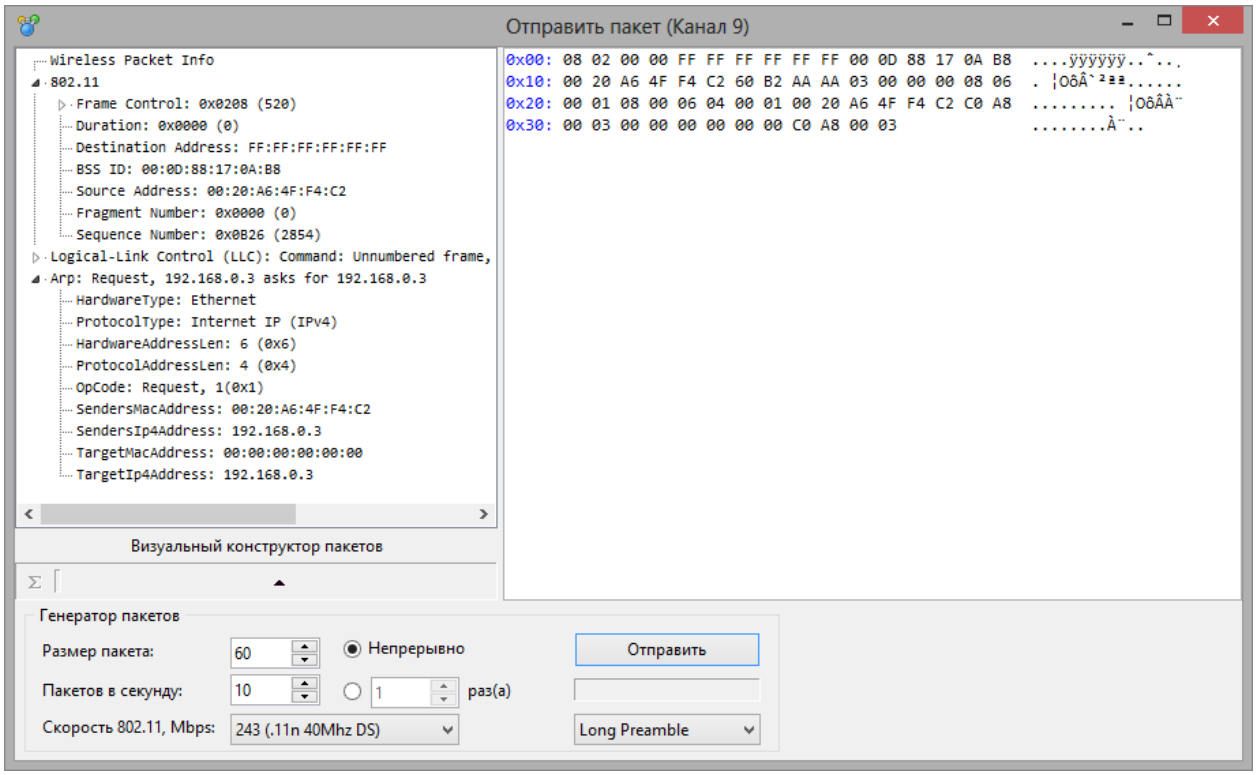
Псевдонимы

CommView for WiFi может подставлять вместо MAC- или IP-адресов легко читаемые и легко запоминаемые имена при отображении пакетов в закладках **Пакеты** и **Статистика**. Например, 00:0F:3D:E9:0D:35 станет AP.

Чтобы создать имя (алиас) для MAC-адреса, щелкните 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 имен можно, щелкнув 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 создается щелчком правой кнопки мыши по пакету, поле имени автоматически заполняется именем хоста (если оно доступно), а затем пользователь может его 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**, щелкните на нем правой кнопкой мыши, а затем выберите команду **Отправить пакет**.



Пожалуйста, прочитайте эту информацию об ограничениях и особенностях работы с Генератором Пакетов и беспроводными адаптерами:

- 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 системный администратор.
- Ваш адаптер может не отправить некоторые пакеты или отправить определенные пакеты много раз. Такое поведение адаптера контролируется только его программным обеспечением и не находится под нашим контролем.
- Прошивка вашего адаптера может не позволить передачу пакетов с произвольной скоростью. Вполне возможно, что когда вы укажете скорость в 1000 пакетов в секунду, прошивка адаптера будет передавать эти пакеты намного медленнее.

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 ручное создание 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 for WiFi 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-ого сетевого адаптера.
Непрерывно – включить режим непрерывной передачи, пока не нажмете **Остановить**.
Количество раз – задать число отправок пакета в сеть.
Скорость 802.11 – задать скорость 802.11 (rate), используемую для отправки пакетов. Возможность использования той или иной скорости зависит от выбранных в настоящий момент диапазона и канала. Например, пакеты 802.11a не могут быть переданы на скорости 2 Mbps.
Long/Short Preamble – установить тип преамбулы для пакетов 802.11b и 802.11g. Неприменимо для 802.11a.
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.

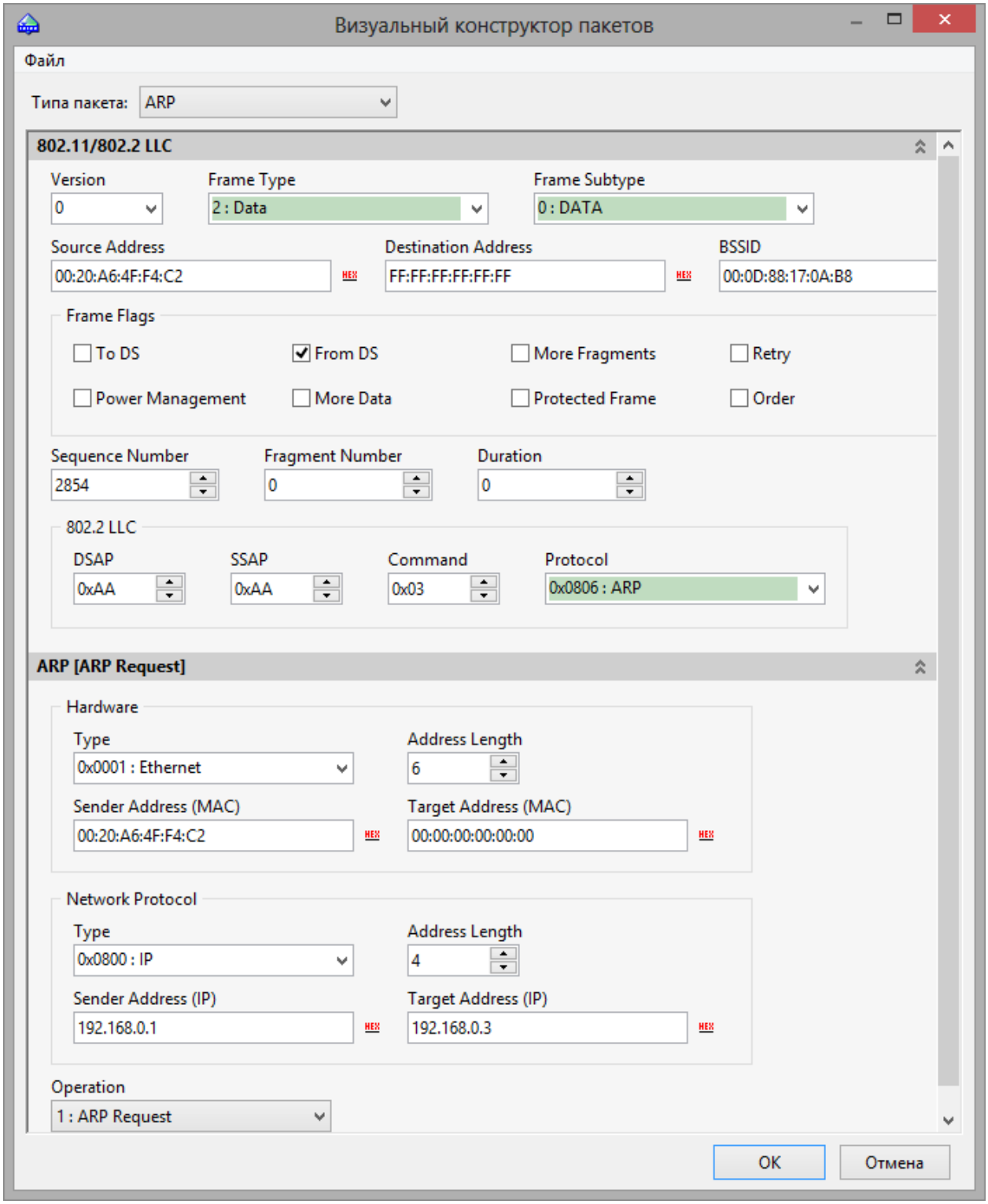
Сохранение отредактированных пакетов

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**.

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.

Примечание: 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 for WiFi с перехваченными пакетами (NCF); при этом помните, что если этот файл содержит более одного пакета, то будет загружен лишь первый пакет.

Производитель 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**. Будет показано имя производителя. По умолчанию, в закладке **Пакеты** CommView for WiFi заменяет первые три байта в MAC-адресе на имя производителя адаптера. Такой алгоритм может быть изменен, если деактивировать опцию **Показать названия производителей в MAC-адресах** в диалоговом окне **Опции.** Список производителей находится в файле MACS.TXT в папке CommView for WiFi. Вы можете отредактировать файл 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 for WiFi 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 придется вручную, а остановка произойдет в указанное время.

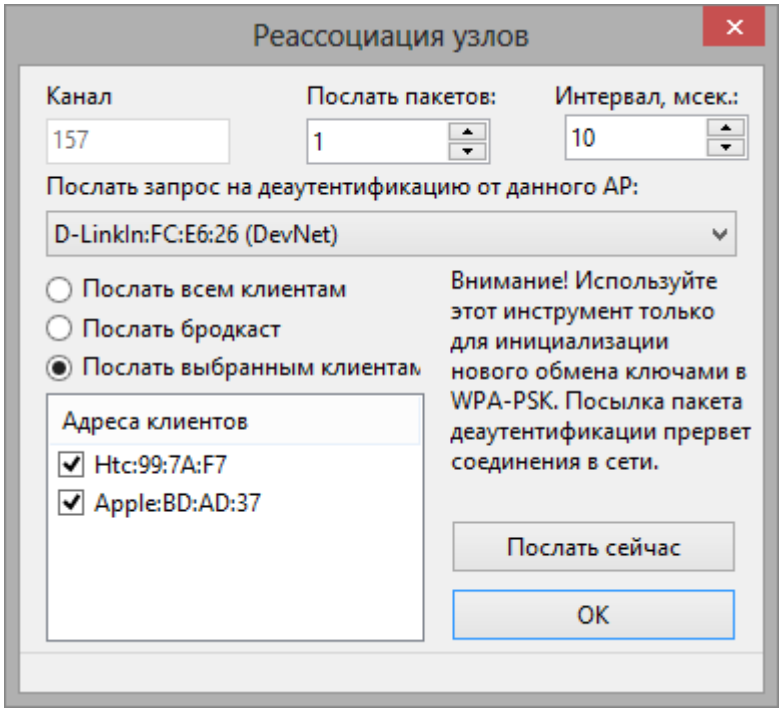
Если CommView for WiFi уже находился в режиме захвата пакетов к моменту начала работы по расписанию, и запланированный адаптер отличается от использованного в тот момент, CommView for WiFi приостановит выполнение текущего задания, переключит адаптер и начнет работу по расписанию.

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

Реассоциация узлов

Поскольку алгоритм шифрования WPA носит динамический характер, знания WPA-пароля недостаточно для расшифровывания трафика сразу после ввода пароля. Для расшифровывания WPA-трафика CommView for WiFi должен работать и перехватывать пакеты во время фазы обмена ключами (эта фаза производится по протоколу EAPOL).

Модуль реассоциации узлов можно использовать для инициирования обмена ключами:



Модуль посылает запрос на деаутентификацию от имени выбранной точки доступа. Этот запрос приводит к реассоциации станции и точки доступа. Процесс реассоциации обычно занимает не более секунды и позволяет программе перехватывать EAPOL-пакеты, необходимые для расшифровывания WPA-PSK. Используйте этот модуль лишь в том случае, если вам требуется расшифровывать трафик WPA-PSK.

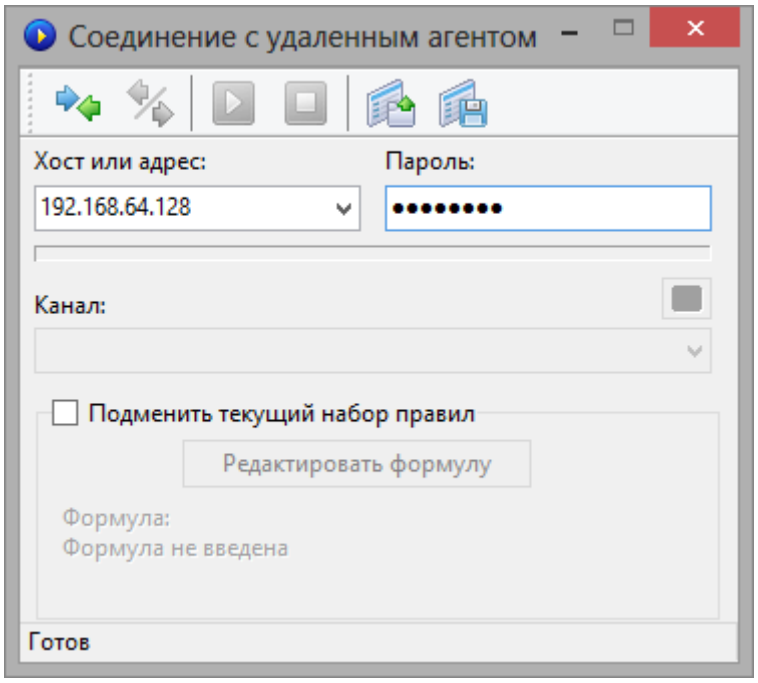
Для начала процесса реассоциации выберите из выпадающего списка точку доступа, выберите станции и нажмите **Послать сейчас**. Опции **Послать всем клиентам** и **Послать выбранным клиентам** позволяют послать unicast-пакеты всем или выбранным клиентам, соответственно. Опция **Послать бродкаст** позволяет послать бродкаст-пакет на адрес FF:FF:FF:FF:FF:FF. Хотя эта опция позволяет покрыть все клиенты, некоторые клиенты могут проигнорировать запрос деаутентификацию, посланный на бродкаст-адрес. Также можно послать несколько пакетов: воспользуйтесь полями **Послать пакетов** и **Интервал**.

Работа с CommView Remote Agent for WiFi

CommView Remote Agent for WiFi – это вспомогательная программа для удаленного мониторинга сетевого трафика. Установите Remote Agent for WiFi на компьютере-объекте наблюдения, затем с помощью CommView for WiFi подключитесь к Remote Agent for WiFi. После подключения и авторизации вы сможете наблюдать трафик удаленного компьютера так, как это был бы ваш локальный компьютер.

Важно: в этой главе объясняется, как использовать CommView for WiFi для связи с CommView Remote Agent for WiFi и для удаленного перехвата трафика. За подробной информацией об установке и настройке Remote Agent обратитесь к его справке. Перед работой с Remote Agent мы настоятельно советуем подробно ознакомиться с его документацией. Программу можно скачать с нашего веб-сайта.

Чтобы включить режим удалённого мониторинга, выберите в меню **Файл** => **Режим удалённого мониторинга**. В CommView for WiFi появится дополнительная панель инструментов рядом с главной. Если вы работаете через брандмауэр (файрволл) или через прокси-сервер, или если вы установили нестандартный номер порта в CommView Remote Agent for WiFi, вам придётся указать порт, нажав кнопку **Дополнительные установки сети** и/или ввести настройки прокси-сервера SOCKS5. В диалоге **Дополнительные установки сети** можно указать, будет ли Remote Agent применять правила фильтрации локально или будет пересылать весь захваченный трафик в CommView for WiFi. Это будет описано ниже в этой главе.

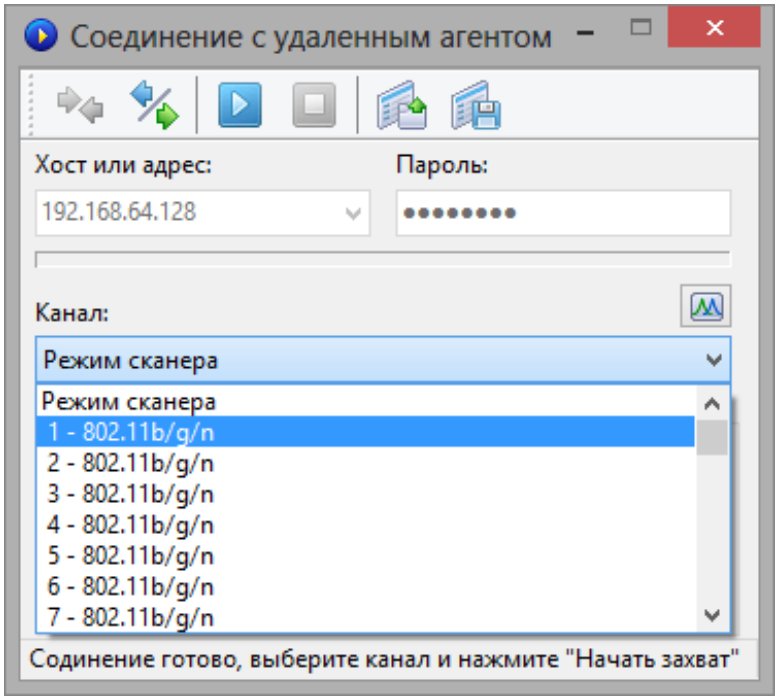


Нажмите кнопку **Новое соединение Удаленного Агента** для установки нового соединения или кнопку **Загрузить профиль Удаленного Агента** для загрузки ранее сохраненного профиля. Ранее сохраненный профиль можно будет загрузить из окна **Соединение с удаленным агентом**.

В появившемся окне **Соединение с удаленным агентом** введите IP-адрес компьютера, на котором запущен CommView Remote Agent for WiFi, пароль подключения и нажмите кнопку **Соединиться**. Если пароль верный, соединение будет установлено. Появится сообщение *Соединение готово*, а в

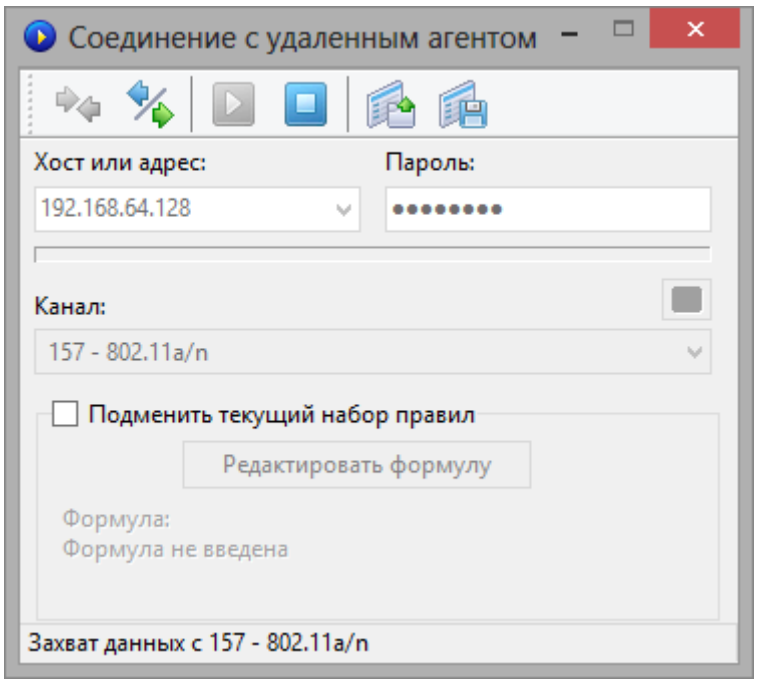
выпадающем списке каналов появятся каналы, поддерживаемые беспроводным адаптером, установленном на удаленном компьютере. Первым в списке каналов будет помещен **Режим сканера**.

Если вы выберите **Режим сканера**, удаленный беспроводной адаптер будет перехватывать данные с каждого канала в течении нескольких секунд, и так по кругу. С помощью небольшой кнопки, расположенной справа над списком каналов, вы сможете настроить работу сканера. Нажав эту кнопку, выберите каналы для мониторинга в режиме сканирования и укажите интервал в секундах на канал.



Теперь можно установить правила перехвата в закладке **Правила** главного окна CommView for WiFi. Вы также можете **подменить текущий набор правил**, отметив соответствующий флажок и нажав кнопку **Редактировать формулу**, после чего в появившееся поле можно ввести формулу, определяющую правила захвата. Синтаксис формулы тот же самый, что и в Универсальных правилах.

Когда вы готовы к началу мониторинга, выберите в списке нужный канал и нажмите кнопку **Начать захват**. CommView for WiFi позволяет сохранить настройки соединения в виде профиля, чтобы бы в будущем его можно было быстро загрузить. Для этого воспользуйтесь кнопкой **Сохранить профиль** и введите имя файла.



CommView for WiFi начнет перехватывать трафик с удаленного адаптера так, как если это был ваш локальный трафик; в удаленной и локальной работе CommView for WiFi нет принципиальной разницы. Чтобы закончить удалённое наблюдение, нажмите кнопку **Закончить захват**. Можно или выбрать другой канал из списка, или отключиться от Remote Agent совсем, нажав кнопку **Разорвать соединение**. Чтобы вернуться в стандартный режим, выберите в меню **Файл** => **Режим удалённого мониторинг** и дополнительная панель управления исчезнет.

CommView for WiFi может работать с несколькими Remote Agent одновременно. Вы можете создавать несколько удаленных подключений, каждое со своими настройками и независимым набором правил, тем самым получая возможность сбора трафика с нескольких локальных беспроводных сетей из одного экземпляра программы CommView for WiFi.

Советы по эффективному использованию CommView Remote Agent for WiFi

Для эффективной работы с Remote Agent необходимо убедиться, что полоса пропускания достаточна для передачи данных между Remote Agent и CommView for WiFi. Как уже говорилось ранее, программа должна быть установлена на компьютере с совместимым беспроводным адаптером (для мониторинга) и Ethernet-адаптером (для связи между программами Remote Agent и CommView for WiFi).

По умолчанию Remote Agent пересылает все захваченные пакеты обратно в CommView for WiFi, независимо от тех правил, которые могут быть настроены в CommView for WiFi. Это делается для шифрования и для предоставления корректной статистической информации, а также для корректной идентификации беспроводных узлов. Поскольку полностью загруженная беспроводная сеть имеет полосу пропускания в 54 Мбит/с (или даже 108 Мбит/с при использовании определенного оборудования), важно, чтобы проводной канал между CommView и CommView for WiFi мог выдержать такую нагрузку. В современных офисах с сетями Gigabit один адаптер Gigabit может с легкостью принимать данные с десятка Remote Agent.

Бывают ситуации, когда быстрая связь – это проблема. Например, в том случае, если вы наблюдаете удаленную беспроводную сеть через Интернет. Даже подключения типа T3 (4.5 Мбит/с) недостаточно для передачи всех пакетов со среднезагруженной беспроводной сети. В таких случаях вы можете изменить начальные установки, настроив Remote Agent на фильтрацию пакетов перед их отправкой в программу CommView for WiFi. С помощью кнопки **Дополнительные установки сети** дополнительной панели инструментов главного окна CommView for WiFi можно включить опцию **Минимизировать загрузку канала**. Когда эта опция включена, текущий набор правил CommView for WiFi периодически пересылается в Remote Agent. Затем этот набор правил применяется локально, так что в CommView for WiFi передаются лишь те пакеты, которые прошли фильтрацию. В этом режиме закладка Узлы может не отображать никаких узлов, а в закладке Каналы не будет показана статистика по отдельным каналам. Поэтому используйте этот режим только тогда, когда вы ограничены в пропускной способности вашего канала и вам требуется доступ к пакетам из удаленной беспроводной сети.

По тем же причинам, связанным с пропускной способностью, мы НЕ рекомендуем использовать беспроводное подключение для передачи данных между Remote Agent и CommView for WiFi. Это неудачная мысль хотя бы потому, что беспроводной адаптер, используемый для мониторинга, будет перехватывать пакеты, отправляемые беспроводным адаптером, который служит для связи между двумя программами, если эти адаптеры работают на одном и том же или близких каналах, что может привести к лавинному эффекту.

Если CommView Remote Agent for WiFi захватит больше данных, чем он способен передать в CommView for WiFi, то Remote Agent задействует свой внутренний буфер для хранения тех пакетов, которые не могут быть переданы немедленно. Размер буфера составляет 5 Мбайт. Индикатор **Использования буфера** в окне Remote Agent отражает текущее состояние буфера. Например, если программа записала в буфер 2.5 Мбайт данных, то буфер задействован на 50%. Если загрузка буфера достигнет 100%, программа перестанет записывать туда данные и перехваченные пакеты будут игнорироваться до тех пор, пока в буфере не освободится место.

Безопасность

CommView Remote Agent for WiFi создавался с учетом требований безопасности. Войти в Remote Agent можно только с помощью пароля, который никогда не передается открытым текстом, а проверяется по схеме "запрос-ответ" с использованием хэш-функции. Если авторизация прошла успешно, весь переданный трафик архивируется и шифруется с помощью этого пароля. Пожалуйста, держите ваш пароль в секрете. Если он станет доступен другому лицу, то этот человек получит обширный доступ к вашей сети и сможет перехватывать сетевой трафик на удаленном компьютере.

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 for WiFi 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**.

Использование Aruba remote capture

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 захвата, обеспечиваемым CommView Remote Agent, CommView for WiFi также позволяет получать поток данных от точек доступа, производимых компанией Aruba Networks Inc.

Для включения режима удаленного захвата выберите в меню **Файл => Режим удаленного мониторинга**. Под основной панелью инструментов CommView for WiFi появится дополнительная панель. Нажмите на кнопку **Новое соединение Aruba remote capture**, чтобы открыть окно нового соединения.

Удаленный захват должен начинаться на стороне точки доступа через интерфейс командной строки. Aruba remote capture имеет следующий синтаксис:

```
pcap start <interface-mac> <target-ipaddr> <target-port> 4 <maxlen>
```

Пример:

```
pcap start 18:64:72:e3:6a:10 192.168.0.2 5000 4 2346
```

После того, как вы настроите удаленный захват пакетов на стороне точки доступа, укажите выбранный вами номер **порта,** и нажмите кнопку **Соединиться,** чтобы начать получение пакетов от точки доступа Aruba.

Информация о портах

Окно (**Вид => Информация о портах**) отражает таблицу номеров портов и соответствующие им имена сервисов. Эта информация берется из файла SERVICES, который установлен Windows. Файл SERVICES располагается в папке **C:\windows\system32\drivers\etc**. Если вы хотите добавить порты/имена сервисов, то можете редактировать этот файл вручную. CommView for WiFi 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 **C:\Windows\system32\drivers\etc**. Вы можете редактировать этот файл вручную, 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 отображен в виде численного значения.

Показывать названия производителей в MAC-адресах – по умолчанию CommView заменяет в закладке **Пакеты** три первых числа в MAC-адресе на имя производителя адаптера. Если вы хотите это изменить, снимите этот флажок.

Показывать поврежденные пакеты – по различным причинам, например, из-за помех в эфире или расстояния, некоторые пакеты, перехваченные вашим адаптером могут оказаться искаженными, т. е. содержать целиком или частично неверную информацию. Установите эту опцию, если вы хотите, чтобы программа перехватывала и показывала такие пакеты. Тут есть свои преимущества и недостатки. Преимущество состоит в том, что если вы физически находитесь далеко от беспроводных станций и/или точек доступа, то возможно большое количество пакетов с искажениями и эта опция даст возможность видеть больше информации, даже если она частично искажена. Недостаток состоит в том, что вы можете видеть некоторые пакеты с некорректной информацией, например, вы можете видеть

пакеты, отправленные на несуществующие IP-адреса. Если эта опция активна, программа попытается расшифровать WEP- или WPA-пакеты, которые не прошли проверку на целостность (ICV), но заголовки которых не повреждены.

Использование памяти

Хранение данных

Максимальное количество пакетов 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 (см. главу Ведение Log-файлов) - это позволит сохранить в все пакеты в log-файле на жестком диске.

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 уровне трафика в беспроводной сети размер буфера некритичен. При высоком уровне трафика в сети может понадобиться увеличить размер буфера, если программа начинает пропускать пакеты. Чтобы узнать, сколько пакетов было пропущено, можно воспользоваться командой **Файл** => **Производительность**.

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 for WiFi не может определить, какие IP-адреса следует считать локальными, и может неверно распределить их по колонкам локальных и удаленных 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**.

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 for WiFi 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 – задает цвета отображения ключевых слов в формулах универсальных правил.

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

Цвет management-пакетов – задает цвета различным типам management-пакетов. Этот цвет используется в колонке **Протокол** закладки **Пакеты**.

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 произойдет 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 for WiFi воспринимает поврежденные 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 подсчет). 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.

Показывать уровень сигнала в dBm – установите этот флаг, если вы хотите, чтобы программа отображала уровень сигнала в dBm, а не в процентах. Возможность отображения уровня сигнала в dBm зависит от типа используемого беспроводного адаптера. За более подробной информацией обратитесь к главе Об уровне сигнала.

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.

Игнорировать поврежденные пакеты в VoIP-анализаторе – при установке этой опции сетевые пакеты беспроводных сетей с неправильной контрольной суммой (CRC) будут отброшены VoIP-анализатором. В случае, если эта опция выключена, такие пакеты не будут отбрасываться, что может привести к созданию ложных сигнальных или медиа-потоков.

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 панели уведомления для восстановления после минимизации.

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 удаленных 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 тяжелого трафика. Это достигается понижением частоты обновлений экрана и выведением на него меньшего объема 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 нажмете на значок в панели уведомления или в панели задач.

Показать линии сетки – программа рисует линии сетки во всех списках пакетов, каналов и точек доступа.

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

Плагины

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

Ответы на 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/commwifi/faq.php.

В. Я подключен к беспроводной сети и хочу мониторить входящий и исходящий трафик своего компьютера. Какой продукт мне нужен, обычная версия CommView или CommView for WiFi?

О. Вам потребуется обычная версия CommView. Она позволит вам мониторить ваш собственный трафик, однако вы не увидите трафик других станций WLAN. В отличие от обычной версии CommView, CommView for WiFi позволяет отслеживать трафик других беспроводных хостов, перехватывать управляющие фреймы, анализировать уровень сигнала и т.п.

В. Потребуется ли специальное оборудование для использования CommView for WiFi?

О. Вам потребуется карта для беспроводной сети, совместимая с CommView for WiFi. Список совместимых карт размещен по адресу http://www.tamos.ru/products/commwifi/. Для активации функции мониторинга вашего беспроводного адаптера вам потребуется специальный драйвер, который включен в данный продукт. Если CommView for WiFi не запущен, ваш адаптер сможет обмениваться данными с другими беспроводными хостами или точками доступа, как будто вы пользуетесь оригинальным драйвером, предоставленным производителем вашей карты. Если CommView for WiFi запущен, то ваш адаптер будет переведен в пассивный режим мониторинга в режиме "promiscuous".

В. Моя беспроводная карта не включена в ваш список поддерживаемого оборудования. Что мне делать?

О. Наш список поддерживаемого оборудования содержит только те карты, которые мы сами проверили в нашей тестовой лаборатории. Конечно же, существуют и другие карты, которые могут быть совместимы с CommView for WiFi. Если вы хотите узнать, совместима ли ваша карта с CommView for WiFi, пожалуйста, скачайте и запустите нашу утилиту Adapter Test Utility. Если у вас установлена совместимая карта, эта утилита отобразит ее название. Перед тем, как вы запустите нашу утилиту, убедитесь, что на вашем компьютере установлены самые последние версии драйверов для вашей сетевой карты. При необходимости скачайте и установите последние версии с веб-сайта соответствующего производителя сетевого оборудования. Это важно, поскольку результаты тестов очень сильно зависят от используемых версий драйверов сетевых карт. Чем новее версия драйвера, тем больше шансов, что карта будет совместима с CommView for WiFi. Вы также можете приобрести совместимую карту, они совсем не дороги, или заказать коробочную версию CommView for WiFi, которая включает совместимый адаптер.

В. Какой адаптер вы рекомендуете использовать для работы с вашей программой?

О. Ознакомьтесь с нашим списком совместимого оборудования по адресу http://www.tamos.ru/products/commwifi/adapterlist1.php . В этом списке вы сможете найти адаптер, наиболее полно отвечающий вашим требованиям к его форм-фактору (USB, встроенный, и т.д.), чувствительности, частотным 802.11-стандартам и поддерживаемым Windows. На наш взгляд наилучшим выбором был бы 802.11ac-совместимый USB-адаптер.

В. У каких поддерживаемых адаптеров есть внешние антенные разъемы?

О. К сожалению, сейчас таких адаптеров существует не так много. Если говорить об устаревших устройствах, поддерживающих стандарт 802.11n, то внешние антенные разъемы имеют все адаптеры Ubiquiti Networks (SR71C, SR71X, SR71-USB и SRC), а также CACE Technologies AirPcap (Ex и NX). Что касается адаптеров, поддерживающих стандарт 802.11ac, вы можете попробовать Amped Wireless ACA1, но наши тесты показали, что качество приема у этого адаптера достаточно низкое.

В. Возможен ли одновременный захват данных с нескольких каналов?

О. Да, если вы используете два и более совместимых USB-адаптеров. Более подробная информация доступна в главе Многоканальный захват настоящего руководства.

В. Я установил драйвер для моего адаптера, и теперь он не может соединиться с беспроводной сетью после закрытия CommView for WiFi. В чем может быть проблема?

О. Когда вы переустанавливаете драйвер вашего адаптера, настройки конфигурации (включая настройки выбранных беспроводных сетей, паролей и т.д.) могут быть утеряны, поэтому вам, возможно, потребуется настроить адаптер заново. Если ваш адаптер настроен, и вы все еще не можете соединиться, попробуйте отключить, а затем снова включить адаптер в Диспетчере Устройств, после чего связь должна восстановиться.

В. Некоторые каналы в Сканере недоступны для выбора. Это нормально? Как быть, если я хочу работать с этими каналами?

О. В зависимости от страны ваш адаптер может не поддерживать все каналы, указанные в окне Сканера. Для каждой страны набор каналов разный – это регламентируется законодательством. Например, в США, правила FCC (Федеральное агентство по связи) разрешают использовать только каналы с 1 по 11 на частоте 2,4 ГГц. Встроенное программное обеспечение беспроводных адаптеров, которое продается в США, обычно конфигурируется таким образом, чтобы отсечь каналы 12 и 13. Это не всегда удобно, поскольку во время поездок в разные точки мира вам может понадобиться мониторинг каналов, разрешенных в данной стране. Вы можете купить адаптер на месте, но также можете использовать специальную утилиту, которая позволяет изменить регуляторную область (regulatory domain) и код страны в некоторых адаптерах. Перед тем, как скачать утилиту, имейте в виду, что:

- Изменение regulatory domain может привести к его повреждению. Действуйте на свой страх и риск.
- Изменение regulatory domain может быть незаконным в вашей стране, поэтому сначала проконсультируйтесь с юристом.
- Мы не осуществляем технической поддержки для данной утилиты.
- До использования данной утилиты вы должны установить драйверы, идущие в поставке с CommView for WiFi.
- Утилита работает ТОЛЬКО с адаптерами на базе чипсетов Atheros.
- Эта утилита не поддерживает работу с USB-адаптерами. При работе CommView for WiFi с USB-адаптерами доступны все поддерживаемые ими каналы, поэтому в изменении regulatory domain нет необходимости.

Нажмите здесь, чтобы скачать утилиту. Для адаптеров, выполненных не на чипсете Atheros, возможно включение 12-го и 13-го каналов посредством изменения некоторых настроек. Свяжитесь с нами, если вам нужна помощь.

В. Могу ли я быть уверенным, что программа перехватит каждый отправленный или полученный пакет во время мониторинга беспроводной сети?

О. Нет, и вот в чем причина. Когда беспроводная станция подключилась к сети и авторизовалась, станция и беспроводной коммутатор(ы) используют механизм, позволяющий им пересылать пакеты, которые по какой-либо причине (например, радиопомехи) не были получены другой стороной или были повреждены. В случае с CommView for WiFi беспроводной адаптер переходит в пассивный режим мониторинга. Таким образом, адаптер не может отправить запросы на повторную отправку пакетов и он также не может подтвердить успешное получение пакетов. В результате этого возникают потери пакетов. Доля потерянных пакетов может изменяться. В целом, чем ближе вы находитесь к другим станциям или беспроводным коммутаторам, тем меньше пакетов будет потеряно.

В. Может ли программа расшифровывать пакеты, зашифрованные при помощи WPA/WPA2?

О. Да, в режиме WPA-PSK. Поддерживаются как TKIP (WPA), так и AES/CCMP (WPA2).

В. Я работаю в беспроводной 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, выбрал канал и начал мониторинг, однако пакеты не отображаются. Пожалуйста, помогите!

О. Во-первых, перейдите на закладку **Пакеты**. Закладка **IP-статистика** может быть пустой, если сеть использует шифрование WEP или WPA. Если закладка **Пакеты** также пуста, посмотрите на строку состояния программы (status bar). Если счетчик пакетов увеличивается, это означает, что у вас активированы правила, которые не позволяют программе отображать пакеты. Выберите **Правила => Сбросить все**, затем нажмите три кнопки на панели инструментов: **Захватывать data-пакеты**, **Захватывать management-пакеты** и **Захватывать control-пакеты**. Если счетчик пакетов в строке состояния не увеличивается, скорее всего программа не обнаружила активные точки доступа. Если вы абсолютно уверены, что в зоне охвата находятся активные точки доступа, сообщите нам об этой проблеме.

В. Может ли CommView for WiFi читать файлы формата NCF, созданные обычной версией CommView? А наоборот?

О. Да, CommView for WiFi может читать файлы формата NCF, созданные обычной версией CommView. Обычная версия CommView может читать файлы формата NCF, созданные CommView for WiFi, но (а) вам потребуется CommView 4.0 сборка 296 или выше, и (б) вы не увидите колонки, относящиеся к беспроводным сетям, такие как сила сигнала или номер канала.

В. Работает ли CommView for WiFi 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 закладке **Log-файлы**. Таким образом, программа будет непрерывно записывать в файл(ы) все перехваченные пакеты, и вы сможете установить любое ограничение на объем перехваченных данных.

В. Во время использования CommView for WiFi мой брандмауэр сообщает, что программа "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 for WiFi. 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 for WiFi 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 for WiFi автоматически запускается с повышенными правами.

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. Мне непонятны типы лицензий для CommView for WiFi. Не могли бы Вы объяснить разницу между ними?

О. В настоящее время для CommView for WiFi есть два вида лицензий: стандартная лицензия и VoIP-лицензия. Наиболее дорогая **VoIP License** активизирует все функции программы, включая анализатор VoIP, в то время как стандартная лицензия не имеет функции анализатора VoIP.

Более подробная информация о лицензировании доступна в лицензионном соглашении, сопровождающем продукт.

В. Поддерживает ли 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

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

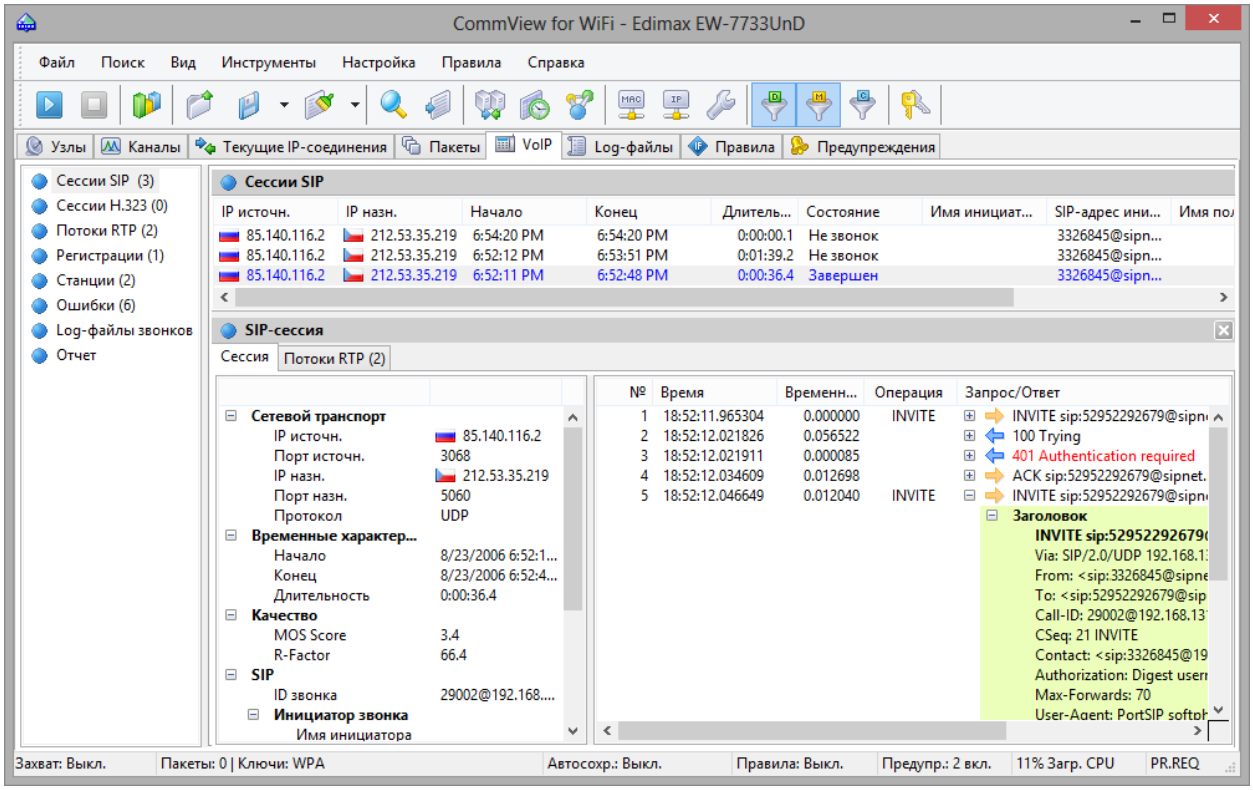
Анализатор VoIP – это встроенный в CommView модуль, предназначенный для перехвата и анализа в режиме реального времени таких событий Интернет-телефонии (VoIP), как звонки, сессии, регистрации, потоки данных, ошибки и т. д. Представляя данные в графическом виде и оценивает качество голосовой передачи, 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.).

Если в вашей беспроводной сети используется WEP- или WPA-шифрование, то вам следует правильно ввести ключи WEP или WPA. В противном случае анализ VoIP будет невозможен. За более подробной информацией обратитесь к главам Ключи WEP/WPA и Расшифровывание WPA.

Работа с анализатором VoIP

Примечание: 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:

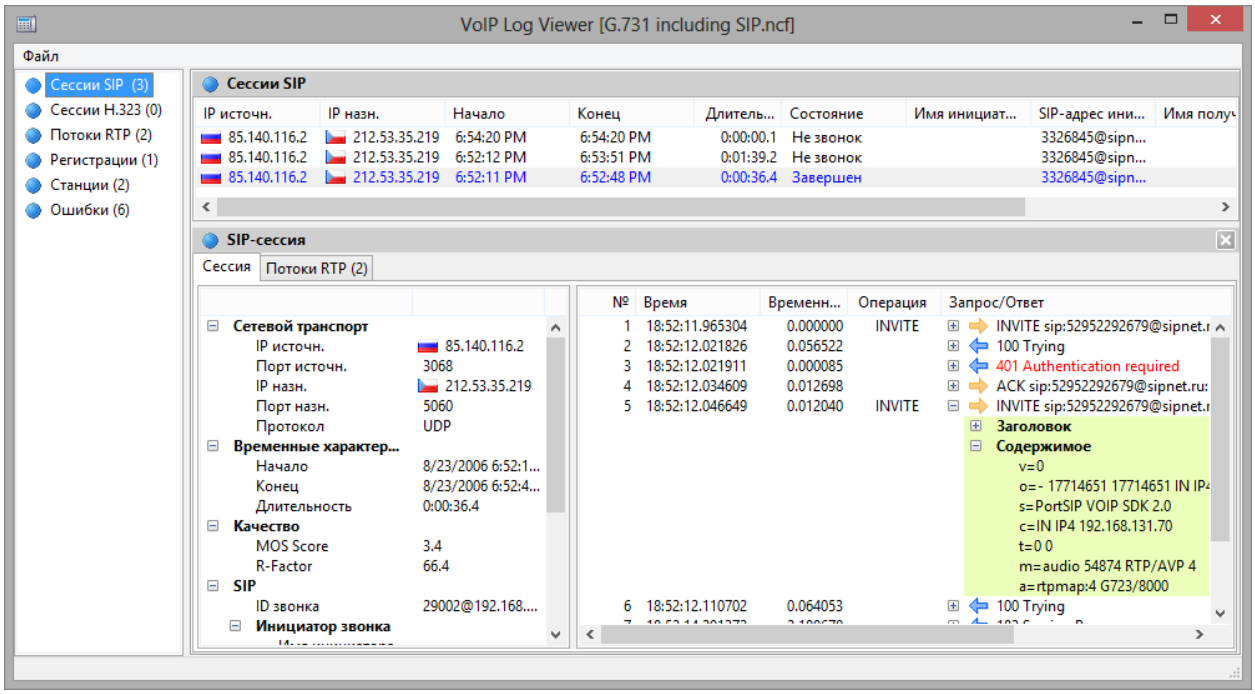
Сессии SIP – список перехваченных сессий SIP 2.0.
Сессии H.323 – список перехваченных сессий H.323.
Потоки RTP – список перехваченных потоков RTP.
Регистрации – список клиентов, зарегистрированных на сервере и история регистраций клиентов.
Станции – список рабочих станций, участвующих в обмене VoIP-данными.
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.

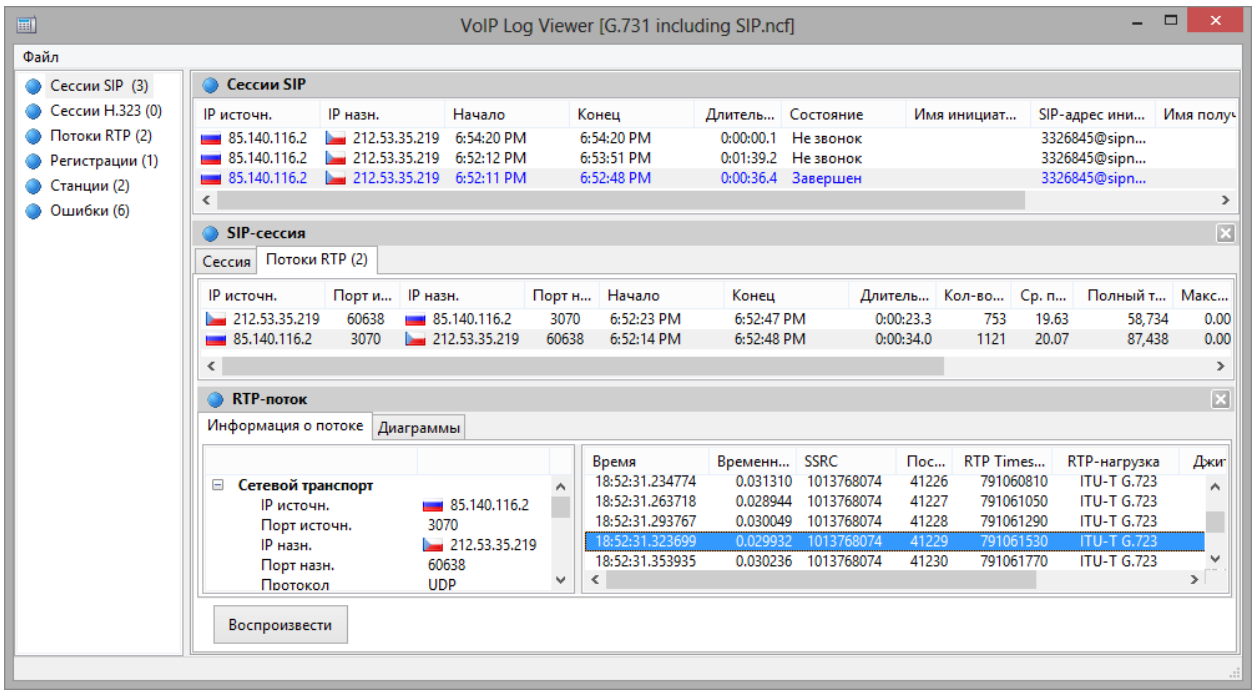
Сессии SIP and H.323

Примечание: 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:

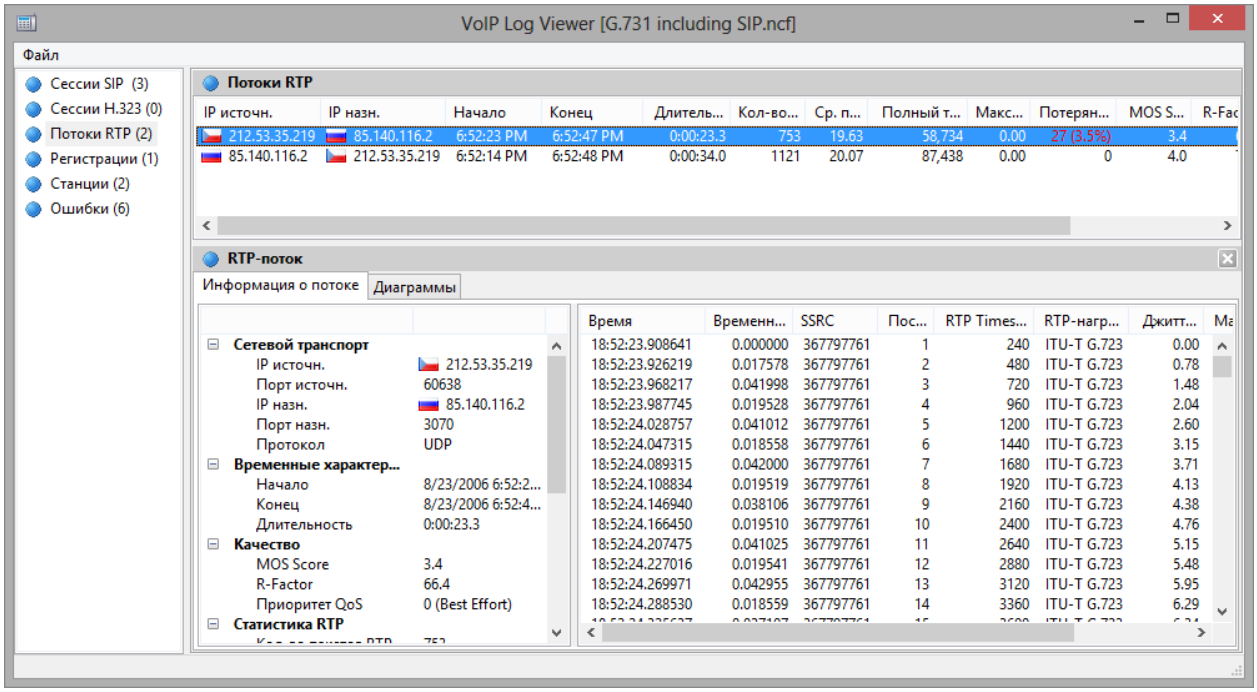
Работа со списками в анализаторе VoIP
Воспроизведение звонка
Файлы NVF

Потоки RTP

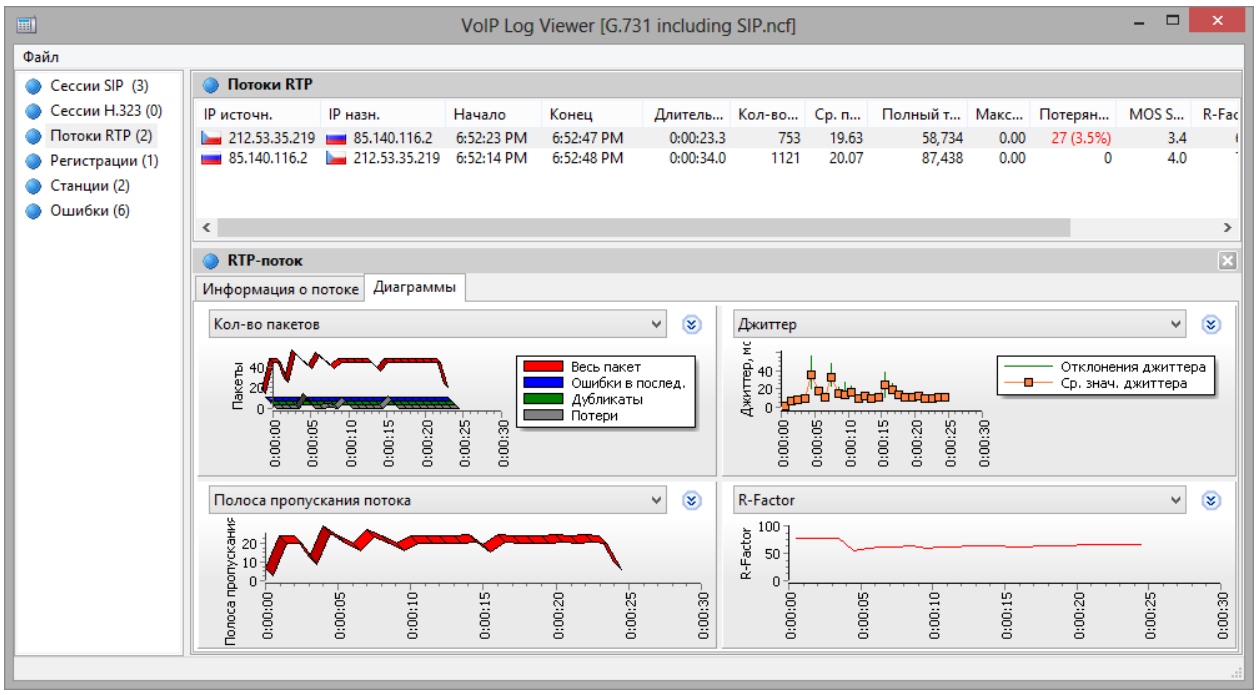
Примечание: модуль анализа VoIP доступен только обладателям лицензии VoIP или пользователям, работающим с ознакомительной версией с выбранной при установке опцией VoIP.

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, станции, ошибки

Примечание: 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 анализатора VoIP 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.

Для просмотра списка рабочих станций, задействованных в обмене данных VoIP, включая статистические данные и список наиболее часто звонящих, выберите пункт **Станции** в левой части панели в окне анализатора VoIP. Полный список станций представлен в верхней части панели. При выборе станции в нижней части панели будут показаны входящие и исходящие звонки от выбранного компьютера или устройства.

Для просмотра списка последних ошибок, зарегистрированных при обмене данными между клиентами VoIP и серверами, выберите пункт **Ошибки** в левой панели в окне анализатора VoIP. Список последних ошибок показан в верхней части панели. При выборе записи в нижней части панели будет показана информация о соответствующем звонке.

Log-файлы звонков и отчеты

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

Панель **Log-файлы звонков** 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.

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 генерацией отчетов. Новые отчеты могут как замещать старые, так и дописываться к ним.

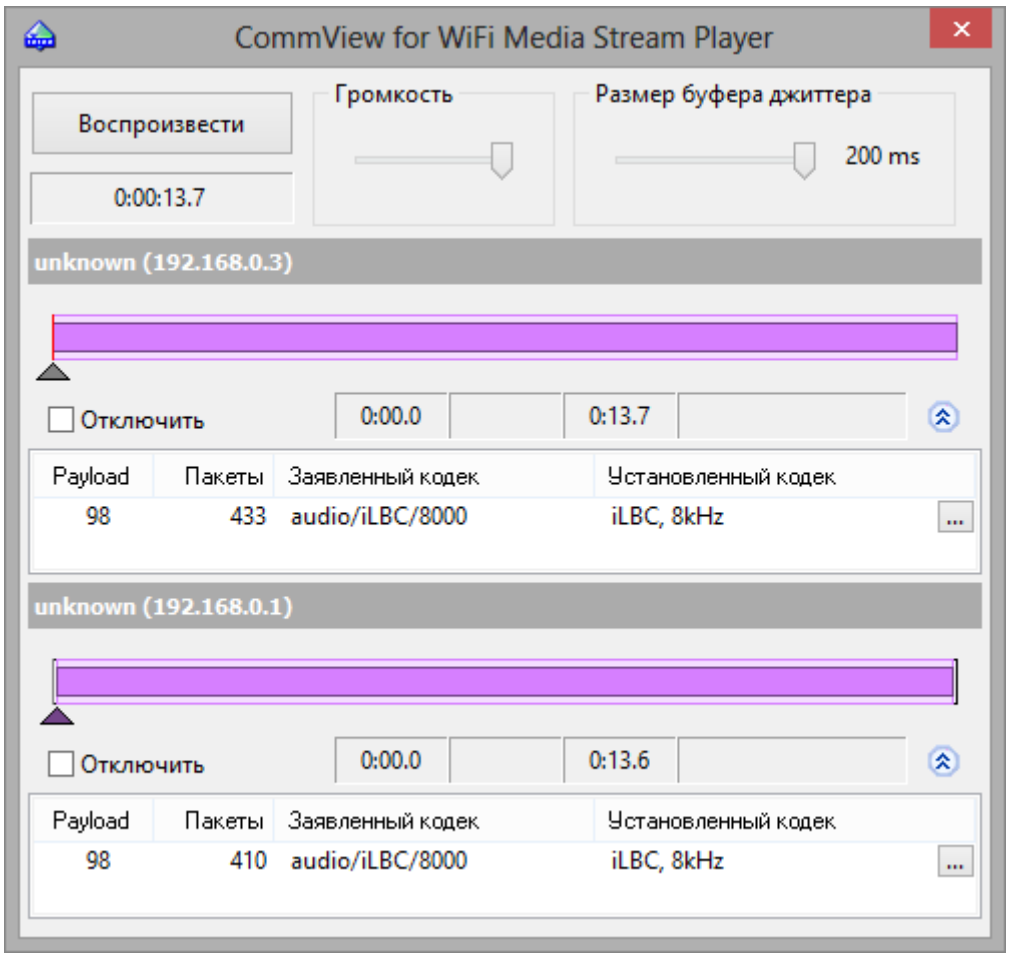
Воспроизведение звонка

Примечание: 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).

Примечание: 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 for WiFi.

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

Примечание: 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 CommView (NVF).

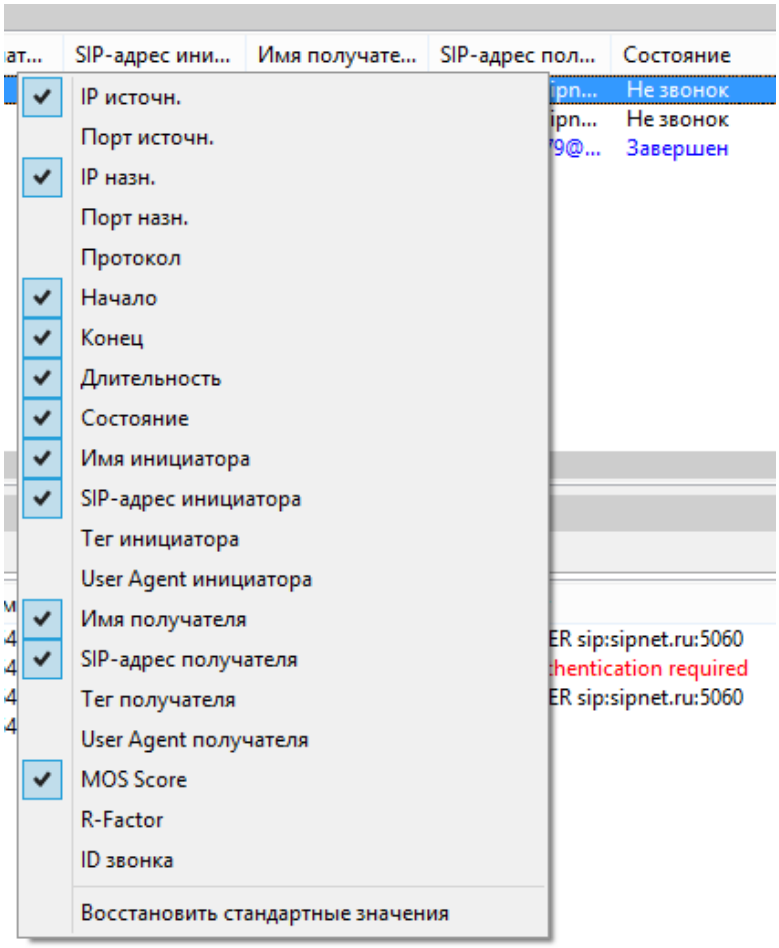
Меню модуля просмотра VoIP log-файлов

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.

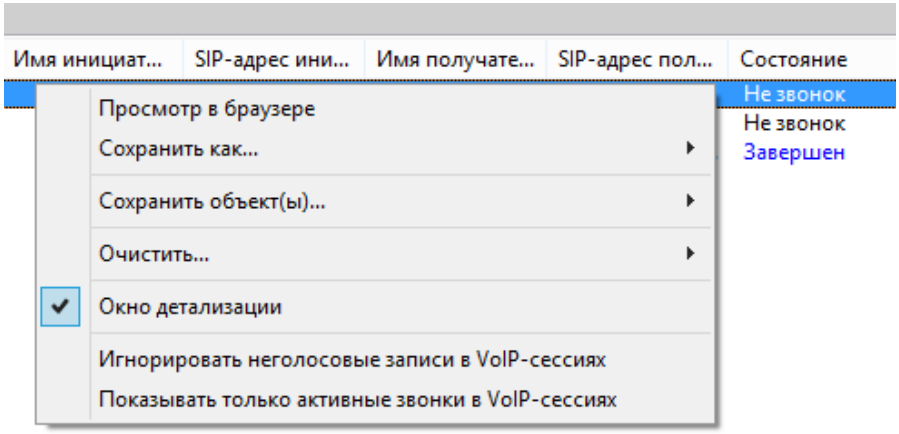
Работа со списками в анализаторе VoIP

Примечание: 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:



Просмотр в браузере – открыть текущий вил в виде HTML-файла в веб-браузере.
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.
Игнорировать записи неголосовые записи в VoIP-сессиях – скрыть все записи, которые не являются голосовыми звонками.
Показывать только активные звонки в VoIP-сессиях – скрыть все записи, которые больше не являются активными.

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

Мониторинг сетей 802.11n и 802.11ac

Несмотря на схожесть технологий 802.11 a/b/g и 802.11n/ac, в сетях 802.11n/ac есть некоторые особенности, которые нужно учитывать при мониторинге. Без углубления в технические аспекты стандартов (они доступны для ознакомления в Интернете), эта глава рассматривает наиболее эффективные способы мониторинга и требования к оборудованию для сетей 802.11n и 802.11ac.

Совместимость адаптеров

Захват пакетов стандарта 802.11n требует наличие адаптера стандарта 802.11n или 802.11ac. Захват пакетов стандарта 802.11ac требует наличие адаптера 802.11ac. Вы не можете производить захват пакетов стандарта 802.11n, используя адаптер стандарта 802.11 a/b/g, и вы не можете производить захват пакетов стандарта 802.11ac, используя адаптер 802.11 a/b/g или 802.11n. Список совместимых адаптеров стандарта 802.11n и 802.11ac можно найти на странице загрузки CommView for WiFi на нашем веб-сайте. В зависимости от конфигурации анализируемой беспроводной сети 802.11n или 802.11ac, к адаптеру могут быть применимы дополнительные требования. Такие требования подробно описаны ниже.

MIMO, пространственные потоки и Transmit Beamforming

Использование MIMO и технологии Transmit Beamforming (формирование диаграммы направленности) в сетях 802.11n и 802.11ac – серьезные испытания для беспроводных анализаторов. Сети 802.11n и 802.11ac создают очень сложную адаптивную диаграмму мощности сигнала с уклонами и подъемами, иногда составляющими всего несколько сантиметров в объеме. Так как устройство мониторинга пассивно, беспроводная сеть никаким образом не адаптирует сигнал, поскольку просто "не видит" устройство, которое ведет мониторинг. Кроме того, сигнал, передаваемый несколькими антеннами на высокой скорости (на текущий момент до 867 Мбит/с), сложно перехватить без ошибок CRC. Вышесказанное означает, что, как правило, вам следует быть готовым к значительно большему количеству (в процентном соотношении) ошибочных фреймов в 802.11n и 802.11ac сетях по сравнению с более старыми сетями 802.11 a/b/g. Это не будет являться проблемой при общем контроле работы беспроводной сети или измерении силы сигнала отдельных устройств, однако если вы анализируете отдельные TCP-потоки или занимаетесь низкоуровневыми проблемами (на уровне пакетов), это может быть затруднительным при значительном количестве поврежденных фреймов.

Для уменьшения влияния этих факторов, специфичных для 802.11n/ac сетей, рассмотрите следующие варианты:

- Найдите наилучшее местоположение ноутбука с запущенной программой CommView for WiFi. Поворачивая или передвигая ноутбук даже на небольшое расстояние (несколько сантиметров), можно очень сильно улучшить или ухудшить качество принимаемого сигнала. Более того, даже положение вашего тела или поднятая рука могут влиять на количество CRC-ошибок.
- Убедитесь, что беспроводные устройства работают не на максимальной скорости. Успешный перехват пакетов на скоростях 100Мб/с и ниже намного более вероятен, нежели

при максимальной скорости передачи данных. Хотя на первый взгляд это противоречит интуиции, если ваш ноутбук для мониторинга находится рядом с точкой доступа, удаление клиентов от точки доступа на несколько метров улучшит, а не ухудшит качество мониторинга. Клиент стандарта 802.11n, расположенный на расстоянии метра или двух от точки доступа, скорее всего, будет передавать и получать пакеты на скорости 300 или 270 Мбит/с, в то время как тот же клиент, удаленный на пять метров, снизит скорость до 130 или 108 Мбит/с, что, с точки зрения мониторинга, гораздо лучше.

Важно помнить о том, что возможности вашего адаптера в плане количества поддерживаемых пространственных потоков должны превышать или соответствовать возможностям анализируемой беспроводной сети. Другими словами, вы не сможете перехватить пакеты, посылаемые трехпоточной точкой доступа трехпоточному клиенту, используя адаптер, который поддерживает только один или два пространственных потока (но вы можете перехватывать, например, пакеты, посылаемые от двухпоточной точки доступа к двухпоточному клиенту, используя трехпоточный адаптер). Число поддерживаемых пространственных потоков легко определить, если просмотреть спецификацию адаптера: для устройств стандарта 802.11n максимальная поддерживаемая скорость 150 Мбит/с означает однопототочный адаптер, 300 Мбит/с означает двухпототочный адаптер, 450 Мбит/с означает трехпототочный адаптер. Для устройств стандарта 802.11ac, максимальная поддерживаемая скорость 433 Мбит/с означает однопототочный адаптер, 876 Мбит/с означает двухпототочный адаптер, 1300 Мбит/с означает трехпототочный адаптер.

Технология Channel Bonding (связывание каналов) в диапазоне 2,4 ГГц

В беспроводных сетях стандарта 802.11n скорость передачи данных может быть опционально увеличена путем связки двух 20 МГц-каналов за счет технологии Channel Bonding (связки каналов), что дает возможность работы в режиме 40 МГц, т.е. этот режим использует более широкие полосы частот (в сравнении с 20 МГц-режимом 802.11a/b/g сетей). И хотя технически одновременный перехват двух каналов не является проблемой для сетевого анализатора, оборудованного адаптером 802.11n, важно обратить внимание на регуляторную область (regulatory domain) используемого оборудования, который накладывает ограничения на использование частот.

Вкратце, при режиме работы в 40 МГц, частота вторичного канала зависит от частоты первичного. Например, выбор канала №1 означает, что первичный 20-мегагерцовый канал будет работать на частоте канала №1, а вторичный 20-мегагерцовый канал будет работать на частоте канала, расположенного на четыре уровня выше первичного, т.е. на частоте пятого канала. При работе с "высокими" каналами, например 10, или 11, добавление четверки к номеру канала будет означать, что частота вторичного канала выйдет за пределы: в США, например, наибольший номер канала в 2,4 ГГц-диапазоне - 11; в большинстве европейских стран - 13. В этих случаях вторичный канал использует частоту, которая находится в нижнем диапазоне по сравнению с частотой первичного канала. Например, выбор канала №10 на вашем оборудовании будет означать, что первичный 20Мгц-канал будет работать на частоте десятого канала, а вторичный 20-мегагерцовый канал будет работать на частоте канала, который меньше первичного на 4 позиции, т.е. на частоте шестого канала.

Инженер по беспроводным сетям, работающий в различных регионах мира, может столкнуться с проблемой, когда региональные ограничения его оборудования могут не совпасть с ограничениями беспроводной сети, которую нужно проанализировать. Например, беспроводная сеть 802.11n, расположенная на территории Германии и работающая на канале №9, будет

использовать "связку" каналов №9 и №13. В то же время, для адаптера беспроводной сети, купленного в Канаде, вторичным каналом в этой ситуации должен быть канал №5. По этой причине при мониторинге вышеуказанной сети адаптер просто "не увидит" 40-мегагерцовые потоки данных в беспроводном анализаторе. Для разрешения этой ситуации мы рекомендуем приобретать оборудование с идентичными ограничениями, либо же включить **Втор. канал ниже первичного в режиме 40 МГц** на панели **Захват** в главном окне программы. Когда эта настройка включена, частота вторичного канала, используемая адаптером, будет ниже частоты первичного канала, даже если это не требуют региональные установки адаптера.

Обратите внимание, что некоторые адаптеры, поддерживаемые CommView for WiFi, такие как адаптеры на основе чипсетов Intel или Broadcom, не поддерживают связывание каналов и могут перехватывать пакеты только на каналах 20 МГц. Подробно об этом можно прочитать в Технической информации. Мы рекомендуем выбирать один из адаптеров с пометкой "Рекомендуем к использованию", указанных на странице загрузки. Эти адаптеры поддерживают технологию связывания каналов.

Технология Channel Bonding в диапазоне 5 ГГц

Технология Channel Bonding в диапазоне 5 ГГц похожа на Channel Bonding в диапазоне 2,4 ГГц, но число связываемых каналов может доходить до восьми в сетях 802.11ac, что означает, что ширина канала может достигать 160 МГц. В отличие от диапазона 2,4 ГГц, наборы связываемых каналов в диапазоне 5 ГГц строго ограничены стандартом. Например, при режиме работы в 40 МГц канал №52 всегда связан с каналом №56 и не может быть связан с каналом №48. По этой причине опция **Втор. канал ниже первичного в режиме 40 МГц** игнорируется, когда вы проводите захват каналов в диапазоне 5 ГГц с помощью рекомендованного адаптера стандарта 802.11ac; адаптер автоматически выбирает корректный набор каналов. Например, если вы выбираете канал №36, адаптер будет проводить захват на 80-мегагарцевом канале (каналы с 36 по 48). При этом, в данном примере пакеты, пересылаемые с использованием 20-мегагерцевого канала, будут видны только если они пересылаются по каналу №36. Иными словами, если вы проводите мониторинг точки доступа 802.11ac, которая сконфигурирована таким образом, чтобы использовать каналы с 36 по 48, при этом первичным каналом является канал №36, вы увидите beacon-пакеты и пересылаемые 80-мегагерцевые потоки данных, если вы проводите захват данных на канале №36; но если вы проводите захват данных на каналах №40, №44 или №48, вы увидите только 80-мегагерцевые потоки данных (и никаких beacon-пакетов).

Кодирование BCC и LDPC

На уровне аппаратного обеспечения пакеты стандарта 802.11n кодируются с применением технологий BCC (Binary Convolutional Code - двоичный сверточный код) или LDPC (Low Density Parity Check - код малой плотности с контролем по чётности). BCC является методом кодирования по умолчанию, который использует большинство устройств стандарта 802.11n. LDPC является опциональным методом кодирования, который поддерживают некоторые устройства стандарта 802.11n. Когда устройство ассоциируется с точкой доступа, элемент **HT Capabilities Info** в пакетах association request и association response определяет использование одного из двух методов кодирования. Например, если используется дефолтный метод BBC, **HT Capabilities Info** содержит поле "**HT LDPC coding capability: Transmitter does not support receiving LDPC coded packets**". Если анализируемая беспроводная сеть использует кодирование LDPC, ваш адаптер должен также

поддерживать этот метод кодирования, иначе пакет, передаваемый HT-рейтах в одном или обоих направлениях, будет утерян или поврежден. Захват пакетов с кодированием LDPC поддерживается последними моделями 802.11n адаптеров mPCIe на основе Atheros, такими как AR93xx, AR94xx и AR95xx, а также всеми рекомендованными нами моделями адаптеров стандарта 802.11ac.

Ошибки CRC и ICV

Ошибки CRC

Каждый пакет беспроводной сети состоит из следующих компонент:

- MAC-заголовок, в который включена информация о длительности, адресе и контроле последовательности.
- Тело пакета переменной длины, где содержится информация для данного типа пакета.
- Контроль последовательности (FCS), содержащий 4-байтовый циклический избыточный код (CRC).

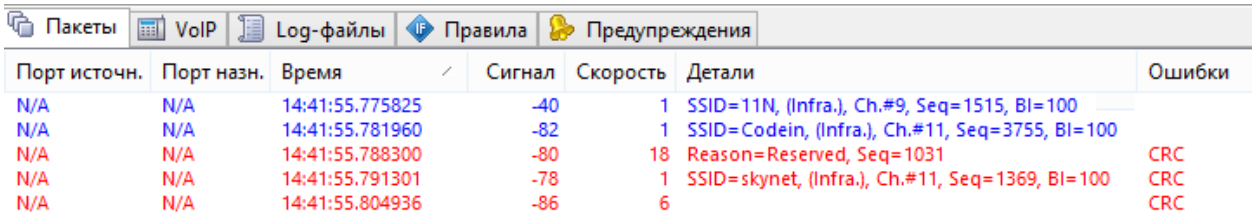
Последний компонент, FCS, используется на принимающей стороне для проверки целостности пакета. Принимающий компьютер вычисляет значение CRC из принятого пакета и сравнивает его со значением, указанным в последних четырех байтах принятого пакета. Если значения не совпадают, пакет считается поврежденным.

Правила управления поврежденными пакетами задаются пользователем. По умолчанию такие пакеты игнорируются программой, за следующими исключениями:

- Они увеличивают счетчики пакетов и байтов.
- Они увеличивают счетчики ошибок CRC в закладке **Каналы**.
- Они включены в график размера пакетов окна **Статистики**.

Поврежденные пакеты не учитываются в других частях программы и таблицах по очевидной причине: ни одна часть пакета с неверным значением CRC не может считаться достоверной. Такой пакет может содержать совершенно неверный IP-адрес, искаженные данные и т. д., хотя в реальных ситуациях такие пакеты часто довольно близки по содержимому к оригиналу. По этой же причине ошибки CRC не могут быть привязаны к конкретным беспроводным точкам доступа или станциям, поскольку невозможно определить реальный MAC-адрес отправителя.

Несмотря на это, пользователь может включить опцию **Показывать поврежденные пакеты** в установках программы – в этом случае поврежденные пакеты будут показаны в списке пакетов. По умолчанию такие пакеты отмечены красным и в колонке **Ошибки** закладки **Пакеты** указан тип ошибки – CRC.



Важно понимать, что пакет с ошибкой CRC, принятый CommView for WiFi, мог быть принят узлом назначения без ошибки. Несмотря на то, что полагается игнорировать поврежденные пакеты узлом назначения, CommView for WiFi попытается декодировать и даже расшифровать такие пакеты.

Не все беспроводные адаптеры способны передавать поврежденные пакеты на уровень приложения. Такая функция гарантируется только для рекомендованных нами адаптеров, поддерживаемых CommView for WiFi.

Ошибки ICV

Значение контроля целостности (ICV) – это четырехбайтовая контрольная сумма, используемая в WEP- и WPA-шифрованных пакетах для сверки результата расшифровывания. Принимающая сторона вычисляет значение ICV исходя из фрагмента данных принятого пакета и сравнивает вычисленное значение с последними 4 байтами. Если значения не совпадают, расшифровывание считается неудавшимся.

Если пользователь ввел корректные ключи WEP/WPA, CommView for WiFi сможет выполнять расшифровывание WEP и WPA "на лету". Информация, связанная с ICV, показывается в колонке **Ошибки** закладки **Пакеты**. Учет программой ошибок ICV зависит от введенного ключа, а также от его правильности. Возможны три случая:

1. Введенный ключ является верным для данной беспроводной сети.
2. Введенный ключ не является верным для данной беспроводной сети.
3. Ключ не введен.

В первом случае программа сообщит об очень небольшом количестве ошибок. Во втором случае все перехваченные пакеты будут идти с признаком ошибки ICV, поскольку в случае ввода неверного ключа вычисленные и фактические значения ICV не совпадут. В третьем случае ошибок ICV не будет, поскольку программа даже не попытается расшифровывать пакеты.

Как уже объяснялось выше, в отличии от "аппаратных" ошибок CRC, ICV-ошибки являются "программными", т.к. зависят от ключа для расшифровывания. Ваша беспроводная сеть может работать совершенно нормально, но если в программе вы ввели неверный WEP-ключ, вы увидите множество ошибок ICV. Пакеты с ошибками ICV будут показаны тем же цветом, что и другие пакеты. Цвет можно всегда изменить в настройках программы.

Если в пакете обнаружена ошибка CRC, то обнаружение ошибки ICV не имеет смысла. Поэтому CommView for WiFi никогда не устанавливает флаг ошибки ICV, если до этого была найдена ошибка CRC.

Расшифровывание WPA

Как уже упоминалось в данной справке, CommView for WiFi может расшифровывать WEP- и WPA/WPA2-трафик "на лету". Чтобы воспользоваться этими функциями, вам потребуется хорошее понимание принципов криптографии.

WEP (**Wired Equivalent Privacy**) – это механизм, используемый для обеспечения защиты данных в беспроводных сетях. WEP дает возможность администратору определять набор ключей (или один ключ) для беспроводной локальной сети. Эти ключи распределяются между клиентами и точками доступа и используются для шифрования данных до их передачи. Если у клиента нет нужного ключа WEP, то он не сможет расшифровать принятые пакеты, а также не сможет отправить данные другим клиентам. Такой подход служит для предотвращения несанкционированного доступа к сети и подслушивания. Если у вас есть нужный ключ, то расшифровывание WEP – процесс простой. WEP является статической системой без изменения состояния. Это означает, что если вы ввели правильный ключ в диалоге ключей WEP/WPA, CommView for WiFi сможет сразу начать расшифровывать пакеты.

WPA (Wi-Fi Protected Access) создан как замена менее безопасному стандарту WEP. В WPA исправлены много "дыр" в безопасности, найденных в WEP: уровень защиты данных и контроль доступа к беспроводным сетям существенно улучшены. В отличии от WEP, WPA является динамической системой с периодическим обновлением ключей, уникальными ключами для каждой станции и другими мерами повышения безопасности. WPA включает в себя два режима – PSK и Enterprise, которые отличаются между собой по нескольким параметрам. CommView поддерживает расшифровывание WPA и WPA2 в режиме PSK.

Из-за динамической сущности процесса WPA-шифрования знания одного лишь пароля WPA недостаточно для мгновенного начала захвата пакетов сразу после ввода пароля. Для расшифровывания WPA-трафика CommView должен принимать пакеты во время фазы обмена ключами (обмен ключами осуществляется по протоколу EAPOL). Очень важно, чтобы все пакеты EAPOL были успешно перехвачены. Если пакет EAPOL будет отсутствовать или будет поврежден, CommView for WiFi не сможет расшифровать принимаемые/отправляемые пакеты и может потребоваться перехват следующей сессии между точкой доступа и станцией. Это является важным отличием в процессе расшифровывания WEP и WPA.

Вышеописанные принципы означают, что когда вы ввели пароль WPA, закрыли диалог ввода ключей WEP/WPA и начали перехват пакетов, вам нужно будет подождать следующего обмена ключами, прежде чем программа сможет расшифровывать пакеты. Вполне типична ситуация, когда программа может расшифровать принятые/переданные пакеты от одного клиента, но не может от другого, поскольку программа еще не перехватила EAPOL-пакеты для всех клиентов.

Реассоциация клиента может быть выполнена с помощью модуля Реассоциации узлов, либо перезапуском точки доступа (реассоциация для всех авторизованных станций), либо переподключением к сети (реассоциации для одного клиента).

Об уровне сигнала

Уровень радиосигнала обычно измеряется в процентах или в dBm (мощность в децибелах, отнесенная к одному милливатту). По умолчанию CommView for WiFi показывает уровень сигнала в dBm. Показатель в 100% соответствует уровню сигнала в -35 dBm и выше, т. е. -25 dBm и –15 dBm будут показаны как 100%, поскольку уровень сигнала очень высок. Показатель в 1% соответствует уровню сигнала в -95 dBm. В интервале от -95 dBm до -35 dBm процентная шкала является линейной, т. е. 50% соответствует -65 dBm.

Если вы предпочитаете показания в процентах, то вы можете задать это через опцию **Показывать уровень сигнала в dBm** в меню **Настройка** => **Установки** => **Декодер**. Когда включена опция **Показывать уровень сигнала в dBm**, уровень сигнала в закладках **Узлы**, **Каналы** и **Пакеты**. В дереве декодирования пакетов уровень всегда показан как в процентах, так и в dBm.

Захват пакетов A-MPDU и A-MSDU

Стандарты 802.11n и 802.11ac позволяют осуществлять одномоментную посылку двух и более фреймов (кадров) путем объединения фреймов в один большой кадр. Существуют две формы агрегации фреймов: Aggregated Mac Protocol Data Unit (A-MPDU) и Aggregated Mac Service Data Unit (A-MSDU). CommView for WiFi поддерживает оба типа агрегированных пакетов, более подробно о которых рассказано ниже.

Принятые фреймы A-MPDU разделяются на отдельные пакеты на уровне "железа". Размеры таких фреймов могут достигать 64 Кбайт. При захвате фрейма A-MPDU он передается на уровень приложения как набор дезагрегированных пакетов, которые выглядят как любые другие пакеты и никаким образом дополнительно не выделяются в интерфейсе CommView for WiFi. Поддержка A-MPDU обязательна для стандартов 802.11n и 802.11ac, и они получили широкое распространение в устройствах 802.11n и 802.11ac. Захват фреймов A-MPDU возможен при использовании любых 802.11n- или 802.11ac-адаптеров, поддерживаемых CommView for WiFi.

Принятые фреймы A-MSDU разделяются на отдельные пакеты на уровне программы. Размеры таких фреймов могут достигать 7935 байт. При захвате фрейма A-MSDU он передается на уровень приложения как единый агрегированный пакет, т.е. в своей изначальной форме. Если агрегированный пакет не поврежден и может быть расшифрован (если расшифровывание требуется), CommView for WiFi дезагрегирует A-MSDU и отображает отдельные пакеты в списке пакетов. Такие пакеты будут обозначены как "Subframe #... of A-MSDU #..." в колонке "Детали". Кроме подкадров будет отображен и оригинальный A-MSDU, обозначаемый как "A-MSDU #....". Если же агрегированный пакет поврежден или зашифрован, то будет показан только оригинальный A-MSDU. Поддержка A-MSDU необязательна для стандарта 802.11n. Такие фреймы достаточно редко используются в 802.11n-устройствах. Захват фреймов A-MSDU возможен при использовании следующих сетевых адаптеров, совместимых с CommView for WiFi:

- Любые рекомендованные 802.11n PC Card, ExpressCard, PCI или PCIe-адаптеры на чипсете Atheros, а также 802.11n USB-адаптеры на чипсетах Ralink. Поддерживаются фреймы A-MSDU размером до 3839 байт.
- Любые рекомендованные 802.11n USB-адаптеры на чипсетах Atheros, а также адаптеры CACE Technologies AirPcap. Поддерживаются фреймы A-MSDU размером до 7935 байт.
- Любые рекомендованные 802.11ac USB-адаптеры на чипсетах Realtek. Поддерживаются фреймы A-MSDU размером до 7935 байт.

Обращаем внимание, что большие пакеты, такие как A-MSDU, часто бывают повреждены, особенно если их посылка осуществляется на высокой скорости передачи данных.

Использование CommView For WiFi на виртуальной машине

Вы можете установить и использовать CommView for WiFi в виртуализированной операционной системе Windows, которая работает в качестве гостевой операционной системы на устройствах Mac (или PC, если вы по каким-то причинам предпочитаете использовать виртуальную среду). Для того, чтобы это сделать, вам понадобится ПО для виртуализации, например, **VMWare**, **Parallels Desktop for Mac** или **Virtual Box**.

Гостевая операционная система

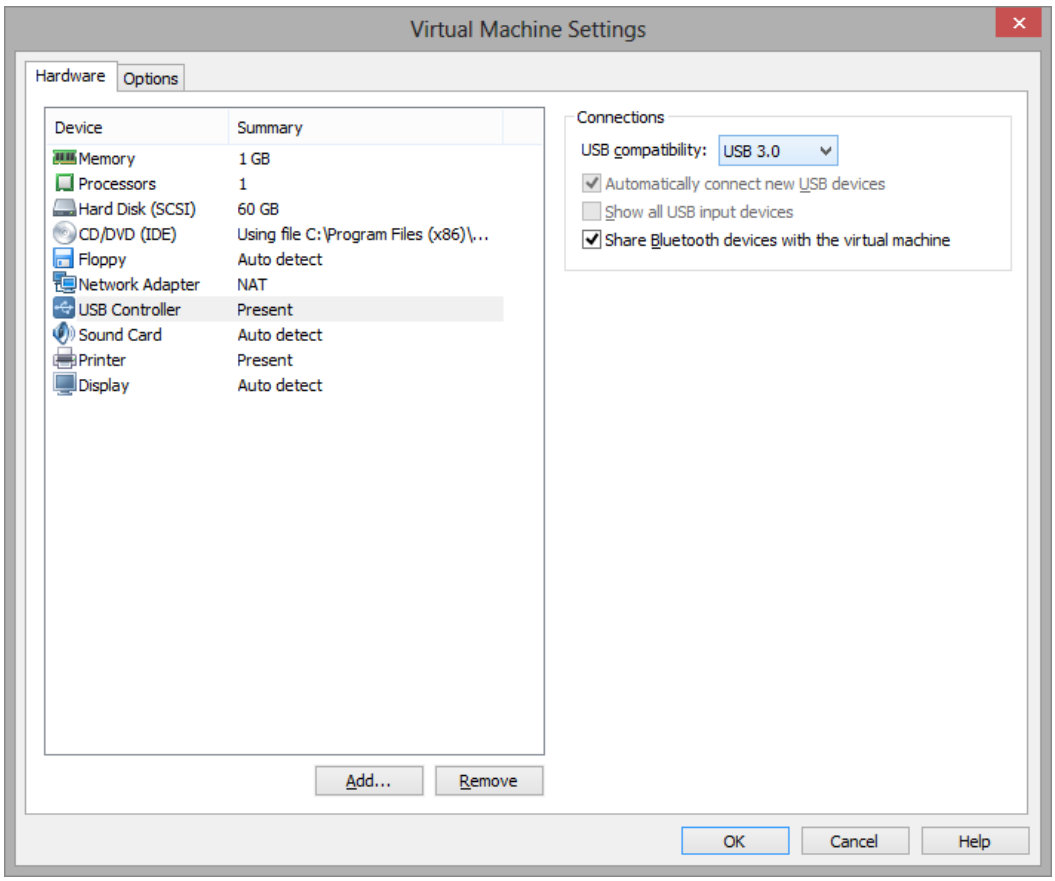
В качестве гостевой операционной системы Windows вы можете использовать Windows 10, 8,1, 8 или 7, хотя мы рекомендуем Windows 10, 8.1 или 8 по причинам, изложенным ниже.

Аппаратное обеспечение

Для того чтобы использовать CommView for WiFi для пассивных инспектирований, вам понадобится совместимый адаптер. Когда вы запускаете наше ПО на ноутбуке с операционной системой Windows, вы можете использовать любой из совместимых адаптеров в различных форм-факторах. Список совместимых адаптеров можно посмотреть здесь. Когда вы запускаете CommView for WiFi на виртуальной Windows-машине, вы можете использовать **только USB-адаптеры**. Пожалуйста, обратитесь к списку адаптеров, чтобы найти тот, который вы собираетесь использовать. Мы настоятельно рекомендуем выбирать адаптеры, отмеченные как "Рекомендуем к использованию". Вы также можете приобрести адаптер у нас, если Вы приобретаете коробочную версию.

Конфигурация программного обеспечения для виртуализации

Если ваше программное обеспечение для виртуализации поддерживает эмуляцию USB 3.0 (как, например, в случае, если вы используете VMWare или Parallels Desktop for Mac), то используйте эмуляцию USB 3.0, а не USB 2.0, даже если порт и беспроводной адаптер, которые вы планируете использовать, являются устройствами USB 2.0. Поддержка USB 3.0 требует по меньшей мере Windows 8 в качестве гостевой операционной системы. Конфигурация USB в среде VMWare показана на иллюстрации ниже.



Эмуляция USB 3.0 предпочтительна, так как существенно увеличивает скорость передачи данных между беспроводным адаптером и гостевой ОС. Например, в некоторых адаптерах переключение канала Wi-Fi может длиться 500 или даже 1000 миллисекунд, если вы используете USB 2.0, и только 100 миллисекунд, если вы используете эмуляцию USB 3.0. Учитывая тот факт, что CommView for WiFi может переключать каналы каждые 250 миллисекунд, разница будет существенной. Использование эмуляции USB 2.0 может значительно замедлить работу приложения.

По этой причине **мы не рекомендуем использовать VirtualBox** в качестве ПО для виртуализации. В настоящее время VirtualBox не имеет поддержки USB 3.0. Если вы, тем не менее, хотите использовать VirtualBox, то, как минимум, включите опцию **Enable USB 2.0 (EHCI) Controller**. В противном случае ваш адаптер Wi-Fi вообще не будет работать в виртуальной среде.

Установка адаптера

Вставьте USB адаптер в ваш компьютер. После того, как адаптер вставлен, вам нужно сконфигурировать ПО для виртуализации, чтобы использовать обнаруженное USB-устройство, то есть отсоединить его от главной ОС и подсоединить к гостевой ОС. Метод конфигурации зависит от конкретного ПО для виртуализации, которое вы используете. Пожалуйста, обратитесь к соответствующей документации. После того, как виртуальная машина получит контроль над адаптером, Windows уведомит вас, что обнаружено новое USB-устройство, и попытается найти драйвер для устройства. Выберите **Справка => Руководство по установке драйверов** в окне CommView for WiFi, чтобы прочитать инструкции по установке нашего специального драйвера для захвата пакетов. После того, как драйвер установлен, вы можете перезапустить приложение и начать его использовать.

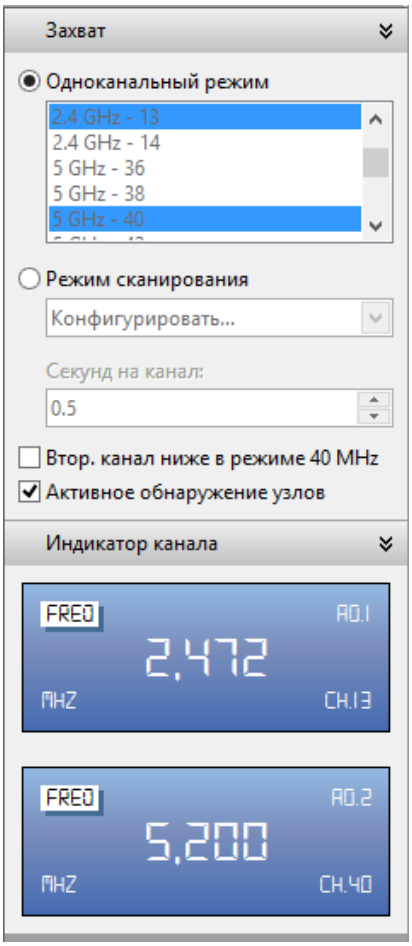
Многоканальный захват

CommView for WiFi позволяет осуществлять одновременный захват данных с нескольких каналов (при использовании нескольких совместимых USB-адаптеров). Следующие 802.11n USB-адаптеры могут быть использованы для многоканального захвата данных: D-Link DWA-160 v.A1, v.A2, v.B2, и v.C1, Edimax EW-7733UnD, Linksys AE3000, NETGEAR WN111 v2, NETGEAR WNDA3100 v1, Proxim ORiNOCO 8494, SMC Networks SMCWUSB-N2, Sony UWA-BR100, TP-Link TL-WDN3200, TP-Link TL-WN721N, TP-Link TL- WN722N, TP-Link TL-WN821N v1, v2 и v3, TP-Link TL-WN822N v1 и v2, Ubiquiti SR71-USB, CACE Technologies AirPcap Ex или NX. Следующие 802.11ac USB-адаптеры могут быть использованы для многоканального захвата данных: Belkin F9L1109 v1, D-Link DWA-180 rev A1, D-Link DWA-182 rev C1, Edimax EW-7822UAC, EnGenius EUB1200AC, Linksys WUSB6300, TP-LINK Archer T4U, TRENDnet TEW-805UB, ZyXEL AC240.

Обращаем ваше внимание, что используемые в работе адаптеры должны быть одной и той же модели. При одновременном подключении нескольких сетевых адаптеров меняются следующие пункты интерфейса:

- Окно выбора каналов в панели **Захват** позволяет выделить несколько каналов. Вы можете выделить несколько каналов, удерживая клавишу **Ctrl**. Число каналов, которые вы выберете, не может превышать число подсоединенных USB-адаптеров.
- Панель **Индикатор канала** отражает несколько индикаторов, число которых соответствует числу подсоединенных USB-адаптеров.

Это показано на иллюстрации ниже.



Когда вы используете несколько адаптеров, пожалуйста, учитывайте следующие факторы:

1. Потребление энергии. Один адаптер может потреблять до 450 мА. Один порт USB 2.0 может обеспечить до 500 мА. Один порт USB 3.0 может обеспечить до 900 мА. Типичный современный ноутбук имеет два порта USB 3.0, то есть, вы должны использовать либо один адаптер на порт, или вы можете использовать USB-хаб (разветвитель); при этом, если вы будете использовать три адаптера в хабе для USB 3.0, вы превысите лимит 900 мА, что может привести к нежелательным последствиям, например, адаптеры без предупреждения перестанут захватывать пакеты.

2. Время переключения каналов. Когда CommView for WiFi работает в режиме сканирования, переключение каналов может занимать какое-то время, от 20 до 80 миллисекунда для каждого адаптера. Рассмотрим ситуацию, когда нужно просканировать 12 каналов с интервалом сканирования 250 мс для каждого канала, а переключение между каналами, скажем, 60 мс. Общее время сканирования получается (250 + 60) x 12 = 3,72 секунды, если вы используете один адаптер. Если вы используете три адаптера, общее время сканирования будет (250 + 60 x3) x 4 = 1,72 секунды.

Получается быстрее в 2,16 раза, а не в 3. Таким образом, добавление адаптеров ведет к увеличению времени при переключении каналов. Если вы используете 12 адаптеров, что теоретически возможно, сканирование 12 каналов займет 250 + 60 x 12 = 0.97 секунды, то есть, вы не сильно выиграете.

Принимая во внимание вышесказанное, мы не рекомендуем использовать более двух или трех адаптеров.

Спектральный анализ

Спектральный анализ включает в себя использование специального радиооборудования, предназначенного для мониторинга полос частот, используемых беспроводными устройствами Wi-Fi. Поскольку что эти частоты нелицензированные, они часто используются источниками сигнала, использующими стандарты данных, отличных от Wi-Fi, например, такими как беспроводные камеры, микроволновые печи или беспроводные телефоны, что создает помехи. Назначение спектрального анализа – детектировать и идентифицировать источники помех, устранять их и/или идентифицировать каналы беспроводных сетей, где помехи будут минимальны.

Системные требования

CommView for WiFi позволяет проводить спектральный анализ с использованием USB-анализатора спектра Wi-Spy. Wi-Spy можно приобрести у компании TamoSoft или напрямую у компании MetaGeek.

CommView for WiFi поддерживает следующие модели Wi-Spy:

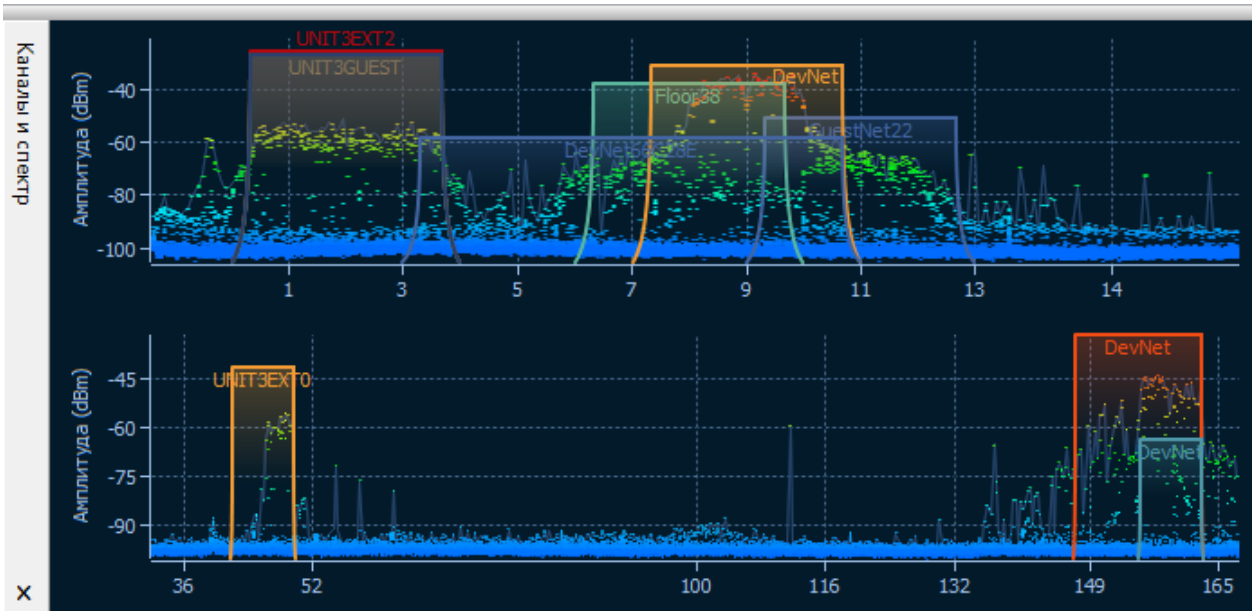
- Wi-Spy DBx (двухдиапазонная, 2,4 ГГц и 5 ГГц)
- Wi-Spy 2.4x (однодиапазонная, 2,4 ГГц)
- Wi-Spy 2.4i (однодиапазонная, 2,4 ГГц)

Обратите внимание, что CommView for WiFi НЕ ПОДДЕРЖИВАЕТ самую старую модель Wi-Spy ("Wi-Spy original" с зеленым логотипом) и модели 900x.

Двухдиапазонная модель Wi-Spy DBx может сканировать оба диапазона по очереди, постоянно переключаясь между ними во время работы. Использование двух устройств Wi-Spy DBx одновременно может улучшить качество данных, поскольку в этом случае CommView for WiFi будет использовать по одному устройству на диапазон.

Диаграммы спектральных данных

Когда Wi-Spy подключен к компьютеру, картина спектра в реальном режиме времени показывается в панели **Каналы и Спектр** главного окна CommView for WiFi, как показано ниже.



Спектральная панель аналогична соответствующей панели *Chanalyzer* – программы для спектрального анализа фирмы MetaGeek, идущей в комплекте с Wi-Spy. По умолчанию спектральная панель отображает один или два планарных графика для одно- и двухдиапазонных моделей Wi-Spy соответственно.

Вид графиков настраивается через контекстное меню. Выберите **2,4 ГГц**, **5,0 ГГц** или **Двойной** для того, чтобы на спектральной панели отображался один диапазон частот или два диапазона одновременно (опции **5,0 ГГц** и **Двойной** доступны только для двухдиапазонной модели Wi-Spy). Выберите **Текущий уровень** для отображения линии, показывающей текущую амплитуду сигнала; выберите **Максимальный уровень** для отображения линии, показывающей максимальную амплитуду сигнала. С помощью опции **Ось X** можно указать единицы измерения для горизонтальной оси: вы можете выбрать между **Частотой** в МГц и номерами **Каналов**. При включении вида **Водопад** приложение отобразит изменение амплитуды во времени. Выберите **1/3**, **1/2** или **2/3 размера окна** для настройки области окна, занятой водопадным графиком. Спектральная панель может быть отделена от главного окна приложения и отображаться как отдельное плавающее окно. Используйте команды **Отделить окно** и **Прикрепить окно** для выполнения соответствующих операций. Вы также можете спрятать панель **Каналы и Спектр** с помощью пункта **Вид => Каналы и Спектр** в главном окне приложения.

Обратите внимание: если программа Chanalyzer запущена, то чтобы иметь возможность видеть спектральные данные в CommView for WiFi, вы должны закрыть ее, поскольку Wi-Spy нельзя использовать несколькими приложениями одновременно.

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. Самым лучшим решением для оптимизации работы программы является использование правил для фильтрации пакетов, которые вы планируете наблюдать. Например, пересылка файла объемом 50 Мб между двумя машинами порождает около 40000 NetBIOS-пакетов со скоростью передачи 5 мегабайт в секунду, что может оказаться трудновыполнимой задачей для программы. Однако обычно не требуется анализ каждого пакета NetBIOS. Можно настроить CommView for WiFi таким образом, что он будет принимать только пакеты IP. В CommView for WiFi есть гибкая система фильтров, позволяющая принимать только те пакеты, которые вам действительно интересны. В дополнение, 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

Невидимый режим

Есть два способа запустить CommView for WiFi как невидимый процесс:

1. Запустить CommView for WiFi с ключом "hidden":

   CV.EXE hidden

2. Если CommView for WiFi 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 for WiFi 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\CommViewWiFi\Rules\POP3Rules.rls"

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

- Выбрать и активировать набор ключей WEP/WPA из файла. Используйте ключ "/keyset" между CV.EXE и полным путем к файлу:

  CV.EXE /keyset "C:\Program Files\CommViewWiFi\WLAN3Keys.wep"

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

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

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

- Запустить приложение без предложения об установке драйвера. Этот параметр полезен, если вы используете CommView for WiFi для обработки лог-файлов, собранных на других компьютерах или соединяетесь с удаленными агентами (CommView Remote Agent for WiFi). Используйте ключ /noprompt:

  CV.EXE /noprompt

- Соединиться с одним или несколькими удаленными агентами. Используйте ключ "/ra" с последующим указанием IP-адреса или имени хоста удаленного агента с которым вы соединяетесь, паролем, заключенным в кавычки, и номером канала за которым должно вестись наблюдение (номера каналов начинаются с "1", т.е. работы программы в режиме сканера укажите "1", если вам нужно наблюдать за первым каналом, укажите "2" и так далее), например:

  CV.exe /ra 192.168.0.5 "MyPassword" 2

- Для того чтобы соединиться с несколькими удаленными агентами работающими с одной копией CommView for WiFi, используйте следующий командный (.BAT) файл:

```
START "CV" "C:\Program Files\CommViewWiFi\CV.exe" /noprompt
PING 1.1.1.1 -n 1 -w 5000 >NUL
START "CV" "C:\Program Files\CommViewWiFi\CV.exe" /ra 192.168.0.1 "pwd1" 5
PING 1.1.1.1 -n 1 -w 1000 >NUL
START "CV" "C:\Program Files\CommViewWiFi\CV.exe" /ra 192.168.0.2 "pwd2" 5
PING 1.1.1.1 -n 1 -w 1000 >NUL
START "CV" "C:\Program Files\CommViewWiFi\CV.exe" /ra 192.168.0.3 "pwd3" 5
PING 1.1.1.1 -n 1 -w 1000 >NUL
```

Этот скрипт запускает CommView for WiFi, ждет 5 секунд, чтобы убедиться, что приложение загружено (для задержек используется команда PING, поскольку язык скрипта не предполагает какой-либо команды для инициирования задержек), затем мы предоставляем программе IP-адреса, пароли и номера адаптеров трех удаленных агентов (с паузой в одну секунду).

Одновременно возможно использование всех ключей за исключением последнего.

Обмен данными с вашим приложением

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

Принцип работы

Вам следует запустить CommView for WiFi, 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 for WiFi 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 for WiFi не может установить соединение, он будет делать повторные попытки каждые 15 секунд. То же самое будет происходить при разрыве соединения: каждые 15 секунд CommView for WiFi будет пытаться восстановить его. Если соединение успешно установлено, CommView for WiFi 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 for WiFi с помощью все того же TCP-соединения, через которое происходит прием. Формат данных прост: нужно указать длину пакета (двухбайтовое беззнаковое целое число со стандартным порядком следования байтов начиная с младшего, т.е. little-endian), затем индекс скорости передачи данных (двухбайтовое беззнаковое целое число со стандартным порядком следования байтов начиная с младшего, т.е. little-endian), затем сам пакет. Длина пакета не включает те четыре байта, которые ставятся перед содержимым пакета. Индекс скорости передачи данных отсчитывается с нуля; он должен содержать индекс скорости (т.е. рейта), показанный в Генераторе пакетов. Обратите внимание на следующий пример:

Строка, которая должна быть отослана, в шестнадцатеричном формате (hex): D4 00 00 00 80 1F 02 66 C2 8E. Длина строки составляет 10 байтов.
Используемая скорость: 5,5 Mbps Это третий пункт выпадающего списка "скорость передачи 802.11" в окне Генератора пакетов.
Итоговое значение в буфере, которое должно быть отослано: 0A 00 02 00 D4 00 00 00 80 1F 02 66 C2 8E.

Если адаптер не открыт или не поддерживает генерацию пакетов, пакет будет сброшен 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/commwifi/samp_mirr_c7.zip. Проект в Visual Studio с исходным текстом на C++.
- http://www.tamos.com/products/commwifi/samp_mirr_d7.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 удаленный компьютер, убедитесь, что линия связи между ними имеет достаточную пропускную способность, чтобы передать все перехваченные данные. Если CommView for WiFi 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).

Пользовательский модуль декодирования

CommView for WiFi 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 ее 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 for WiFi. При запуске CommView for WiFi ищет файл с именем "Custom.dll" и загружает его в память. Если в нем найдена точка входа "Decode" - CommView for WiFi добавляет новую колонку с именем "Custom" в списке пакетов.

Перед тем как отобразить новый пакет, CommView for WiFi вызывает процедуру "Decode" и передает 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, четвертый аргумент - размер буфера (в данной версии - всегда 1024 байта). Буфер выделяется и освобождается самой программой CommView for WiFi, так что не следует управлять распределением памяти под этот буфер самостоятельно. Содержимое буфера будет отображено в виде строки в колонке "Custom".

Ваша процедура должна 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 for WiFi. Этот формат также можно использовать для прямого обмена данными между CommView for WiFi 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>
<tr><td>Уровень сигнала</td><td>1</td><td>Уровень сигнала в процентах (только для пакетов WiFi)</td></tr>
</table>

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/ac, 0x80 для 2.4 GHz 802.11n/ac (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.

Информация

Как купить CommView for WiFi

Работа демо-версии ограничена 30 днями. Посетив наш веб-сайт, вы можете приобрести полнофункциональную версию программы. В настоящее время для CommView for WiFi доступны два вида лицензий: **Standard license** и **VoIP license**. Более дорогая **VoIP license** активизирует все функции программы, включая анализатор VoIP. **Standard license** включает в себя все функции, кроме анализатора VoIP.

Для информации по ценам на одно- и многопользовательские лицензии посетите наш веб-сайт. Одна зарегистрированная копия CommView for WiFi может использоваться одним лицом для установки на одном компьютере и, дополнительно, на одном портативном компьютере. Более подробная информация о лицензировании доступна в лицензионном соглашении, сопровождающим продукт.

Как зарегистрированный пользователь, вы получите:

- 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.

Цены и лицензионное соглашение могут быть изменены без предварительного оповещения. Пожалуйста, посетите наш сайт для получения последней информации о продуктах и ценах.

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