

# **CommView<sup>®</sup> Remote Agent for WiFi**

**Руководство пользователя**

Copyright © 2001-2009, TamoSoft

## Введение

### О программе CommView Remote Agent for WiFi

Программа CommView Remote Agent for WiFi предназначена для мониторинга трафика в удалённой беспроводной сети. Она позволяет пользователям программы CommView for WiFi перехватывать сетевой трафик на компьютере, где запущен Remote Agent for WiFi, где бы физически этот компьютер ни был расположен. Собирая информацию с множества точек, программа позволяет повысить “прозрачность” беспроводной сети в рамках офиса или здания, а также предоставляет возможности удаленного мониторинга и выявления неисправностей в работе сети без необходимости вашего физического присутствия на наблюдаемом объекте.

После установки и несложной настройки CommView Remote Agent for WiFi готов к приему подключений со стороны CommView for WiFi. После установки соединения и авторизации CommView Remote Agent for WiFi готов к перехвату и последующей передаче пакетов в программу CommView for WiFi. Передаваемые пакеты архивируются с целью экономии трафика и шифруются с целью безопасной передачи по обычным каналам.

Являясь незаменимым инструментом для профессионалов в областях сетевых технологий, программного обеспечения и безопасности, CommView Remote Agent for WiFi предлагает вашему вниманию целый спектр решений, направленных на мониторинг больших беспроводных сетей и на удаленную диагностику программного обеспечения.

Для работы данной программы требуется совместимый беспроводной адаптер. Список поддерживаемых адаптеров вы можете найти на нашем [веб-сайте](#).

## Что нового

### Версия 2.4

- Поддержка новых адаптеров (для операционных систем Windows Vista и Windows 7): Intel 3945, 4965, 5100, 5150, 5300, 5350.

### Версия 2.3

- Поддержка новых операционных систем: Windows XP 64-bit Edition, Windows Vista 64-bit Edition, Windows Server 2008 32-bit и 64-bit Editions.

### Версия 2.2

- Поддержка 802.11n
- Поддержка карт на базе последних чипсетов Atheros

### Версия 2.1

- Поддержка Windows Vista.

### Версия 2.0

- Первый выпуск программы.

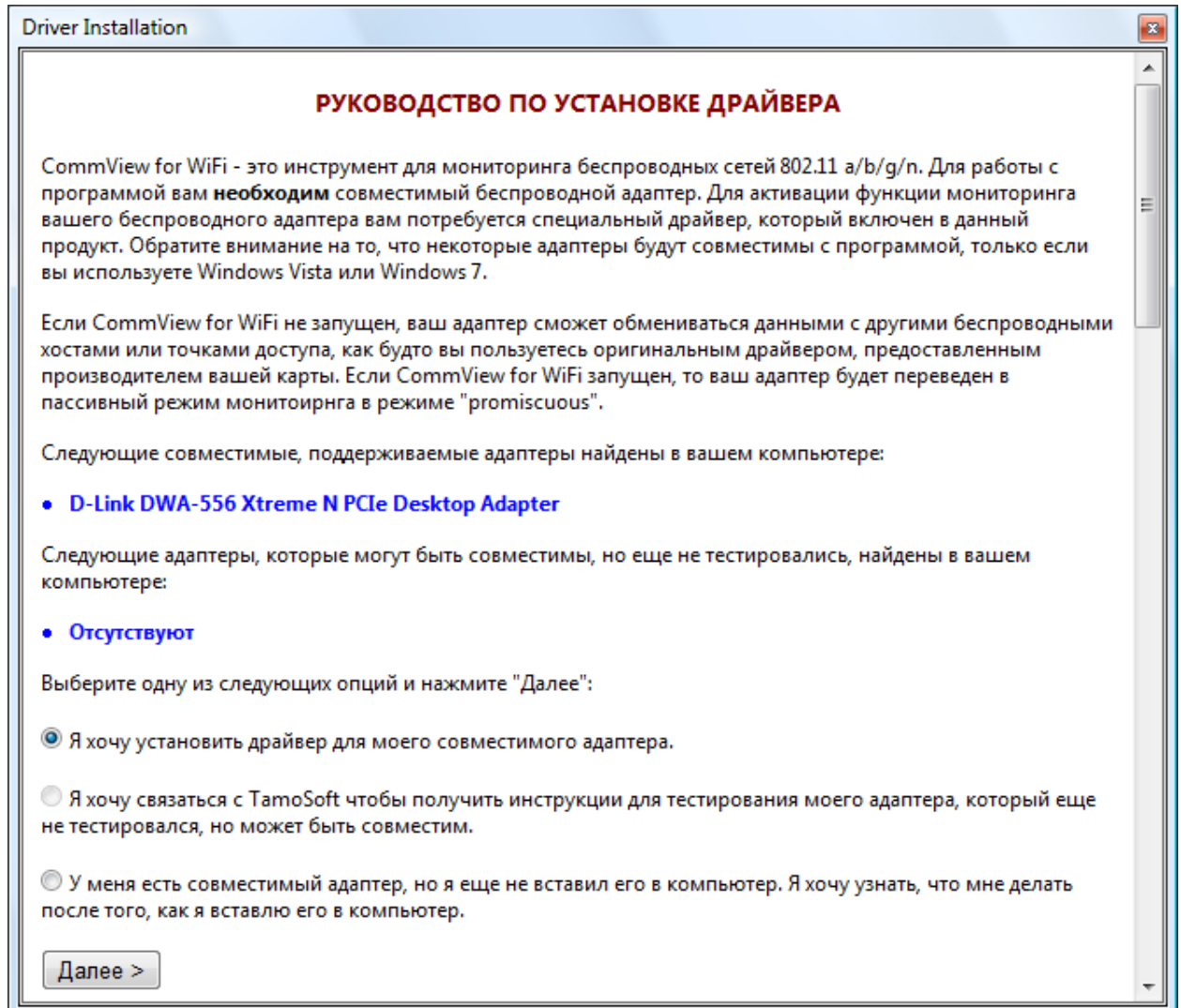
## Работа с программой

### Установка и настройка

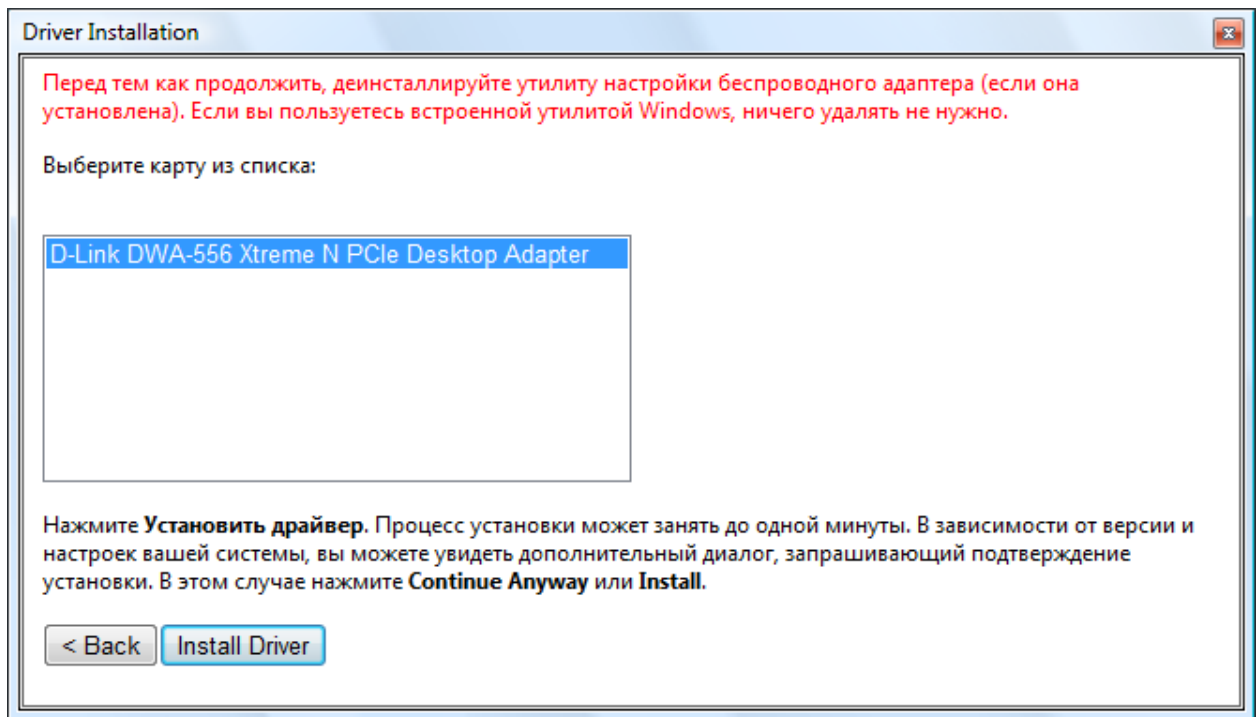
Программа должна быть установлена на компьютере с совместимым беспроводным адаптером (он используется для мониторинга) и Ethernet-адаптером (для связи между программами Remote Agent и CommView for WiFi). Для установки программы вам потребуются административные права, но после первоначальной установки и настройки они вам не потребуются. НЕ СЛЕДУЕТ устанавливать CommView for WiFi и CommView Remote Agent for WiFi на одном компьютере.

#### Установка

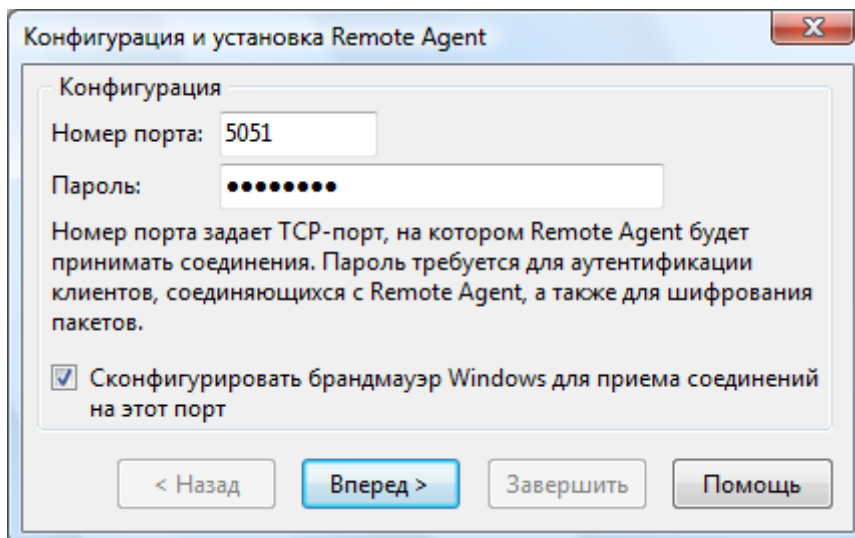
Для установки программы запустите SETUP.EXE и следуйте инструкциям. Первый шаг – это установка специализированного драйвера для вашего совместимого беспроводного адаптера. Перейдите вниз по странице и нажмите кнопку **Далее**.



Если в вашей системе был обнаружен совместимый беспроводной адаптер, то на последней странице вы сможете установить для него драйвер:



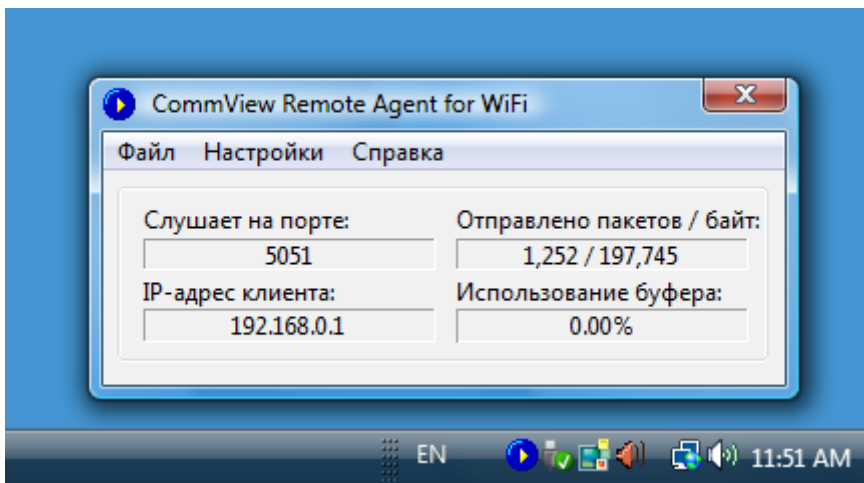
Если установка драйвера прошла успешно, то вы увидите окно Конфигурации и установки Remote Agent, где вы сможете задать начальную конфигурацию. Выберите номер TCP-порта и пароль. TCP-порт (по умолчанию 5051) будет использован программой для приема входящих подключений со стороны клиента (CommView for WiFi). Пароль требуется для авторизации клиента и последующего шифрования пакетов. Старайтесь выбирать длинный, трудно угадываемый пароль с использованием цифр и букв разных регистров. Если кто-то завладеет вашим паролем, то он/она получит доступ к перехваченному трафику на том компьютере, где вы установили CommView Remote Agent for WiFi.



Нажмите Далее. Программа установит оставшиеся компоненты и CommView Remote Agent for WiFi будет запущен первый раз.

### Интерфейс

После установки и начальной конфигурации иконка программы появится в системной области (см. ниже). Нажатие на иконку вызовет окно, в котором будет показано состояние программы – номер порта, который “слушает” CommView Remote Agent for WiFi, IP-адрес клиента, который в данный момент подключен к Remote Agent, статистика передачи пакетов и использования буфера.



## Главное меню

### Файл

**Запустить/продолжить работу сервиса** – запускает сервис CommView Remote Agent или продолжает его работу (resume), если он был в состоянии паузы.

**Остановить сервис** – останавливает сервис.

**Приостановить сервис** – переводит сервис в режим паузы.

**Выход** – закрывает консоль CommView Remote Agent console. Обратите внимание на то, что сервис Remote Agent будет при этом продолжать работу и принимать соединения от CommView.

### Настройки

**Сменить порт** – позволяет сменить номер порта, на котором приложение принимает соединения от CommView.

**Сменить пароль** – позволяет сменить пароль.

**Language** – позволяет переключить язык интерфейса программы.

### Справка

**Содержание** – вызывает файл справки.

**О программе** – показывает общие сведения о программе.

CommView Remote Agent for WiFi не позволяет одновременно установить более одного клиентского соединения.

## Управление программой

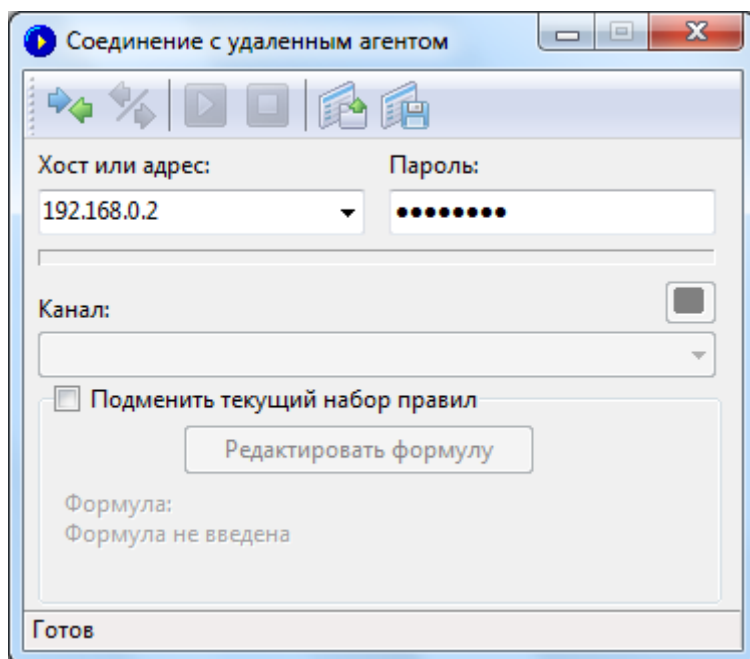
CommView Remote Agent for WiFi является **сервисным приложением (service application)**. Это означает, что программа запускается и начинает работать автоматически при загрузке компьютера, даже если ни один из пользователей не вошел в систему. Управление сервисом можно осуществлять через меню **Файл**, описанное выше. Как и с любым другим сервисом, возможно управление через Панель управления => Администрирование => Службы. Там же можно установить режим запуска (автоматический/ручной).

## Наблюдение за трафиком

В этой главе объясняется, как использовать CommView for WiFi для связи с CommView Remote Agent for WiFi и для удаленного перехвата трафика. Чтобы осуществлять мониторинг трафика беспроводной сети с использованием удаленных компьютеров, вам потребуется CommView Remote Agent for WiFi, запущенный на удаленном хосте и CommView for WiFi, запущенный на вашем компьютере. Предполагается, что Remote Agent уже установлен и запущен (см. предыдущую главу) и вы знакомы с программой CommView for WiFi. Если у вас нет программы CommView for WiFi, скачайте её [здесь](#) и ознакомьтесь с ней перед использованием CommView Remote Agent WiFi.

### Подключение CommView for WiFi к CommView Remote Agent for WiFi

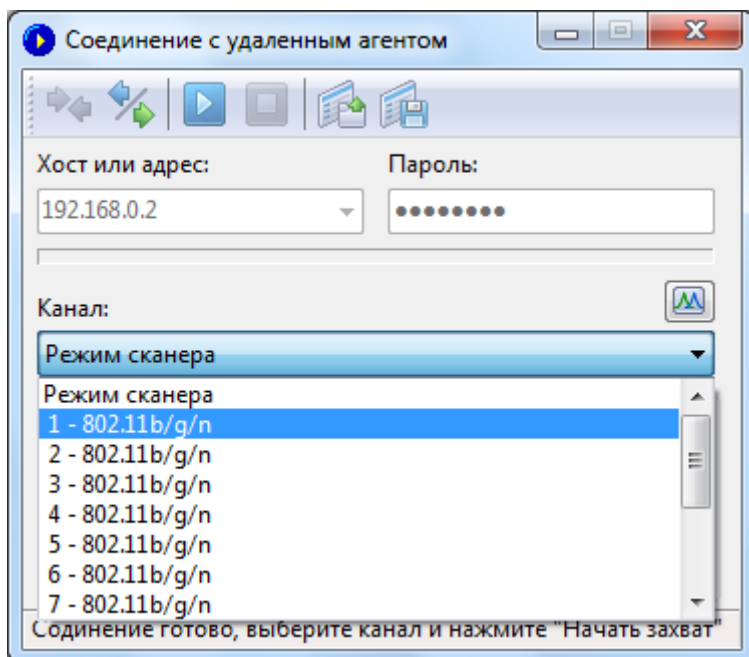
Чтобы включить режим удалённого мониторинга, выберите в меню **Файл => Режим удалённого мониторинга**. В CommView появится дополнительная панель инструментов рядом с главной. Если вы работаете через брандмауэр (файрволл) или через прокси-сервер, или если вы установили нестандартный номер порта в CommView 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**.

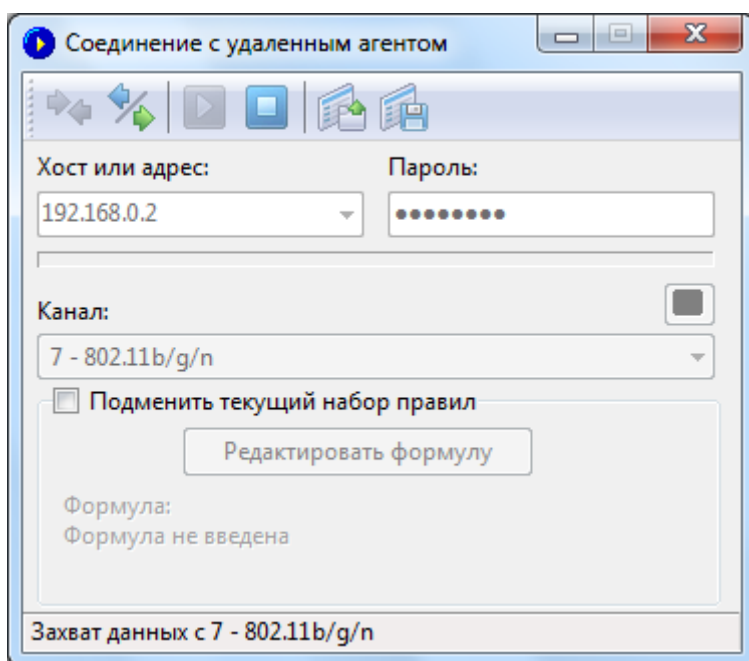
В появившемся окне **Соединение с удаленным агентом** введите IP-адрес компьютера, на котором запущен CommView Remote Agent for WiFi, пароль подключения и нажмите кнопку **Соединиться**. Если пароль верный, соединение будет установлено. Появится сообщение *Соединение готово*, а в выпадающем списке каналов появятся каналы, поддерживаемые беспроводным адаптером, установленном на удаленном компьютере. Первым в списке каналов будет помещен **Режим сканера**.

Если вы выберете **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. По техническим причинам для беспроводных адаптеров Intel этот интервал не может быть менее 4 секунд.



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 мониторинга** 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 300 Мбит/с при использовании 802.11n-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.

## Информация

### Как приобрести CommView Remote Agent for WiFi

Демо-версия имеет 30-дневный ознакомительный период. Посетите [наш сайт](#) для получения последней информации ценах и покупке.

#### Как зарегистрированный пользователь вы получите:

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

Мы принимаем к оплате: кредитные карты, чеки, почтовые переводы и другие виды платежей. Цены и лицензионное соглашение могут быть изменены без предупреждения. Пожалуйста, посетите наш сайт для получения последней информации о продуктах:

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

## Как с нами связаться

У вас есть вопросы, предложения? Пожалуйста, свяжитесь с нами.

<http://www.tamos.ru/>

Описывая вашу проблему, постарайтесь быть как можно точнее. Детальное описание вопроса поможет нам быстрее в нем разобраться. Пожалуйста, не забудьте указать версию операционной системы, версию программы (**Справка => О программе**), тип адаптера и другие важные подробности.

## Другие продукты компании Тамософт

### CommView

CommView - это программа для проведения мониторинга сетевой активности, способная захватывать и анализировать пакеты сети Ethernet. CommView собирает информацию о данных проходящих через LAN и декодирует проанализированные данные. С программой CommView вы сможете увидеть лист сетевых соединений, живую IP-статистику и протестировать индивидуальные пакеты. IP-пакеты декодируются вплоть до самого низкого уровня с полным анализом основных протоколов IP: TCP, UDP, и ICMP. Также предусмотрен полный доступ к исходным данным. Захваченные пакеты могут быть сохранены, чтобы в будущем провести полный анализ, а также экспортироваться в другие форматы. Гибкая система фильтров делает возможным сбрасывать пакеты, которые вам не нужны или собирать только те пакеты, которые вы хотите захватить.

[Подробнее](#)

### CommView для WiFi

CommView для WiFi - это мощный инструмент для мониторинга и анализа беспроводных сетей 802.11 a/b/g. В программе сочетаются большой набор функций и простота их использования. CommView для WiFi перехватывает из эфира каждый пакет и сообщает такую информацию, как списки точек доступа и станций, статистику по узлам и каналам, уровень сигнала, списки пакетов и сетевых подключений, диаграммы распределения протоколов и т. д. Владея этой информацией, вы сможете анализировать пакеты, идентифицировать проблемы в сетях, на сайтах, в программном и аппаратном обеспечении.

[Подробнее](#)

### NetResident

NetResident - это продвинутая программа мониторинга сетевого трафика, предназначенная для перехвата, сохранения, анализа и восстановления различных событий в сети: сообщений электронной почты, веб-страниц, загруженных файлов и сообщений коммуникационных программ (ICQ/AIM, MSN). Программа перехватывает информацию из сети, записывает ее в базу данных, воссоздает эту информацию и отображает ее в простой и понятной форме. Во многих аспектах NetResident похож на сетевой анализатор, но данную программу отличает ориентация на высокоуровневые протоколы, использующиеся для передачи данных через Интернет или локальную сеть. Работая с программой, вам не потребуются глубоких знаний в области сетевых технологий, не придется пользоваться сложными программами для перехвата и анализа пакетов, а также изучать пакеты в попытке восстановить их содержимое – NetResident сделает все это за вас и предоставит по вашему запросу только веб-страницы, сообщения электронной почты и коммуникационных программ или загруженные файлы. Программа используется сетевыми администраторами для безопасности, родителями для наблюдением за своими детьми и судебными экспертами для сбора необходимой информации.

[Подробнее](#)

### SmartWhois

Удобная утилита для сбора информации о любом IP-адресе или имени хоста. В отличие от стандартной Whois-утилиты, SmartWhois автоматически предоставляет информацию, связанную с IP-адресом вне зависимости от географического места его регистрации. За несколько секунд вы можете узнать всё, что вы хотите знать о пользователе: домен, сетевое имя, страну, штат или провинцию, город. Даже если по IP-адресу не может быть определено имя хоста, SmartWhois будет работать.

[Подробнее](#)

### CountryWhois

CountryWhois – это утилита для определения географического местоположения IP-адреса. Утилита может быть использована для анализа лог-файлов сервера, проверки заголовков электронных писем, обнаружения фактов мошенничества с помощью кредитных карт и во многих других случаях, когда требуется быстро и точно определить страну по IP-адресу.

[Подробнее](#)

### Essential NetTools

Полезный пакет для диагностики сетей и слежения за сетевыми соединениями вашего компьютера. Он включает быстрый, многопоточный NetBIOS-сканер, оболочку для NetBIOS Auditing Tool (NAT), утилиту netstat, которая отображает все сетевые соединения компьютера, монитор для слежения за внешними соединениями к открытым ресурсам вашего компьютера, удобную утилиту для быстрого соединения к удалённым ресурсам, которая даёт пользователям Windows 95/98 возможности

Windows NT при подключении на уровне пользователей, удобный редактор файла LMHosts и другие полезные утилиты. Программа легка в использовании и является заменой таких Windows-утилит, как nbtstat, netstat, NetWatcher. Она имеет много дополнительных возможностей, чем стандартные утилиты Windows похвастать не могут.

[Подробнее](#)

### **CommTraffic**

CommTraffic – утилита для получения статистики использования сети, включая локальную сеть и удалённый доступ. Статистика отображается по каждому узлу сети. Программа оснащена гибким, привлекательным интерфейсом, иконкой в панели извещений, показывающей общую сетевую статистику. Можно получать отчёты, отражающие объём сетевого трафика и стоимость подключения к интернет (опция). CommTraffic можно настроить практически на любые особенности тарифных планов интернет-провайдеров, такие как время активности, объём трафика, время суток и тому подобное. Есть настраиваемые предупреждения, срабатывающие по таким критериям, как достижение лимита по сумме оплаты или объёму трафика. Мастер настройки поможет установить программу, автоматически распознает сетевую конфигурацию и параметры подключения.

[Подробнее](#)