

CommView[®] Remote Agent

Руководство пользователя

Copyright © 2001-2008 TamoSoft

Введение

О программе CommView Remote Agent

Программа CommView Remote Agent предназначена для наблюдения трафика в удалённой сети. Она позволяет пользователям программы CommView анализировать сетевой трафик на компьютере, где запущен Remote Agent, где бы физически этот компьютер ни был расположен. Эта новая уникальная технология расширяет ваши возможности, поскольку теперь вы не ограничены только вашим компьютером или сегментом сети. Находясь, например, в Токио, вы можете отлаживать сетевые установки, скажем, в Амстердаме. Запустите CommView Remote Agent на отлаживаемой системе и работайте из своего офиса как бы находясь возле неё!

Достаточно провести установку, несложную конфигурацию и CommView Remote Agent готов принять подключение со стороны CommView. Как только соединение будет установлено и произойдёт успешная проверка пароля, CommView Remote Agent сможет собирать трафик в своём сегменте сети и передавать его на CommView. Передаваемые пакеты "сжимаются" для уменьшения нагрузки на сеть и шифруются для обеспечения безопасной передачи по открытым сетям. Программа CommView оснащена гибким набором фильтров, чтобы отсеивать ненужные пакеты, минимизируя служебный TCP-трафик между CommView и CommView Remote Agent.

CommView Remote Agent незаменим для профессионалов в области сетевых технологий, программирования и безопасности. Программа поможет решить широкий круг задач, таких как наблюдение многосегментных сетей или дистанционная отладка сетевых программ.

Для работы программы потребуется сетевой адаптер Ethernet или Wireless Ethernet с драйвером, соответствующим стандарту NDIS 3.0, или же обычный адаптер удалённого доступа (dial-up adapter).

Что нового

Версия 2.2

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

Версия 2.1

- Поддержка Windows Vista.

Версия 2.0

- Поддержка высокоточных временных отметок (до микросекунд, доступно только в Windows 2000/XP/2003).
- Поддержка Windows XP x64 Edition для процессоров AMD.
- Возможность перехвата loopback-пакетов, посылаемых из/к локальным IP-адресам, т. е. 127.0.0.1 (эта функциональность доступна только в Windows 2000/XP/2003).
- Улучшена производительность.

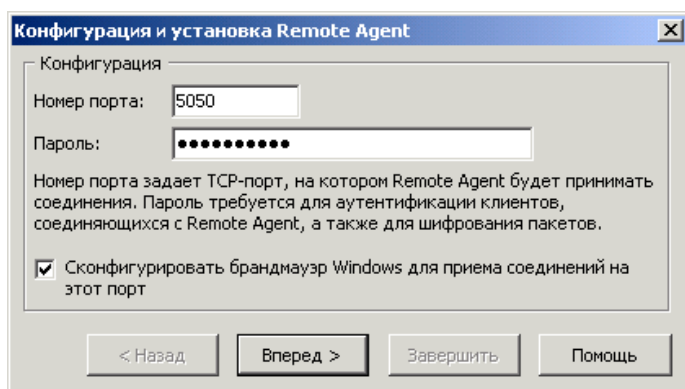
Работа с программой

Установка и настройка

CommView Remote Agent следует устанавливать на компьютер(ах), чей трафик вы намерены отслеживать. Как и CommView, он может захватывать пакеты, проходящие через любой сетевой интерфейс, - сетевой адаптер или адаптер удалённого доступа. CommView Remote Agent можно устанавливать как на подключенные к сети, так и изолированные компьютеры. Для установки программы требуются права администратора, после установки и конфигурирования программы такой уровень привилегий для работы с ней не требуется. Не устанавливайте ОДНОВРЕМЕННО и CommView и CommView Remote Agent на одном и том же компьютере, поскольку это бессмысленно.

Установка

Для установки программы запустите SETUP.EXE и следуйте инструкциям. Когда копирование необходимых файлов завершится, вы увидите окно Установки и Конфигурации (Installation and Configuration), где необходимо указать номер порта TCP и пароль доступа. По умолчанию выбран порт 5050, к нему будет подключаться клиентская программа CommView. Пароль требуется для идентификации клиента и последующей шифрации трафика. Выбирайте **хороший** пароль (достаточно длинный, содержащий буквенно-цифровые комбинации, который трудно угадать), иначе, если кто-либо посторонний узнает пароль, то он получит ПОЛНЫЙ доступ к сетевому трафику данного компьютера.



Нажмите **Вперед**, чтобы продолжить, программа установит необходимые драйверы и произведёт первый запуск CommView Remote Agent.

Установка в пакетном режиме

Установку в пакетном режиме удобно применять при массовой установке CommView Remote Agent на большое количество компьютеров. В таком режиме требуемые параметры установки передаются через параметры командной строки, а сам процесс установки происходит автоматически, без вмешательства пользователя. Для установки в пакетном режиме требуется запустить файл SETUP.EXE со следующими аргументами:

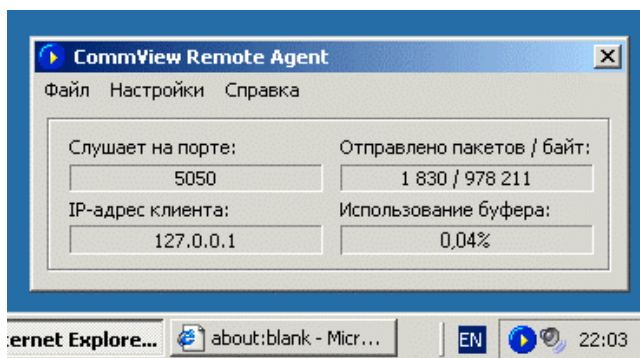
```
/s – "тихая" установка, без взаимодействия с пользователем. Аргумент обязателен.  
/port=xxx – номер порта, где xxx – любое число в диапазоне от 1 до 65536. Аргумент обязателен.  
/pass="xxx" – пароль, где xxx – строка с паролем. Строка должна быть в кавычках. Аргумент обязателен.  
/du – устанавливает драйвер для мониторинга адаптера удалённого доступа (dial-up adapter) в дополнение к стандартному набору драйверов. Аргумент необязателен. Не используйте этот аргумент если у вас нет нужды перехватывать данные от адаптера удалённого доступа. Обратите внимание, что в зависимости от политики в отношении установки драйверов на системе, на которой вы устанавливаете приложение, в процессе инсталляции может возникнуть нужда подтвердить установку драйвер, и в этом случае потребуются взаимодействие с пользователем.  
/lb – устанавливает драйвер для перехвата loopback-пакетов, посылаемых из/к локальным IP-адресам, напр. 127.0.0.1. Аргумент необязателен. Не используйте этот аргумент если у вас нет нужды перехватывать loopback-пакеты.
```

Пример использования:

```
SETUP.EXE /s /port=5050 /pass="ZdU34 ! Hny536" /lb
```

Интерфейс

После завершения установки и конфигурации иконка программы появится в панели уведомлений, как показано на рисунке внизу. Щелчок на иконке вызовет окно, которое будет показывать статус приложения: порт, на котором CommView Remote Agent принимает подключения, IP-адрес клиента, статистику по переданным пакетам и байтам и использование 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 не позволяет одновременно установить более одного клиентского соединения.

Управление программой

CommView Remote Agent 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 службой можно осуществлять через меню **Файл** консоли, описанное выше. Как и с любым другим сервисом, возможно управление через Панель управления => Администрирование => Службы. Там же можно установить режим запуска (автоматический/ручной).

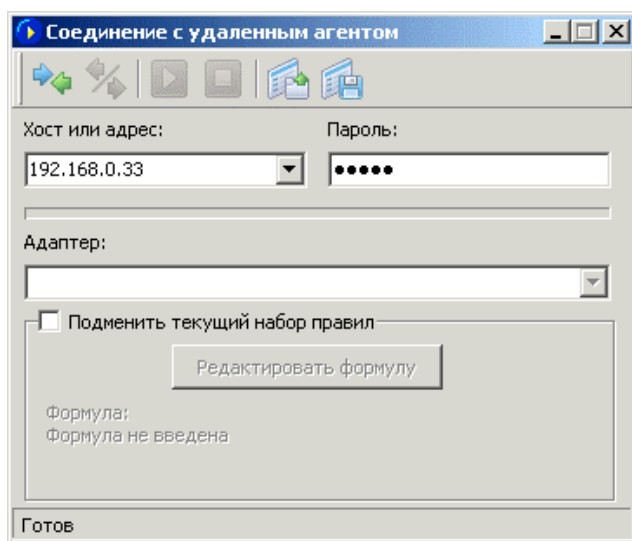
Наблюдение за трафиком

В этой главе объясняется, как использовать CommView для связи с CommView Remote Agent и наблюдения удалённого трафика. Для работы вам необходим CommView на вашем компьютере и CommView Remote Agent, запущенный на удалённом компьютере. Считаем, что Remote Agent уже успешно установлен и работает (подробности в предыдущей главе), и что вы знакомы с CommView. Если у вас нет копии программы CommView, возьмите её [здесь](#) и ознакомьтесь с ней перед использованием CommView Remote Agent.

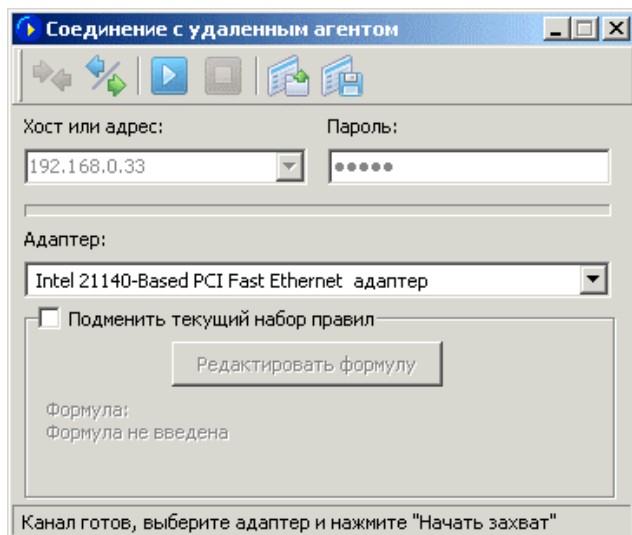
Подключение CommView к CommView Remote Agent

Чтобы включить режим удалённого мониторинга, выберите в меню **Файл => Режим удалённого мониторинга**. В CommView появится дополнительная панель инструментов рядом с главной. Если вы работаете за брандмауэром (файрволом) или через прокси-сервер, или если вы установили нестандартный номер порта в CommView Remote Agent, вам придётся, нажав кнопку **Дополнительные установки сети**, указать порт и/или ввести настройки прокси-сервера SOCKS5.

Нажмите кнопку **Новое соединение Удаленного Агента** для установки нового соединения или кнопку **Загрузить профиль Удаленного Агента** чтобы загрузить предварительно сохраненный профиль (его также можно будет загрузить уже после открытия нового окна).

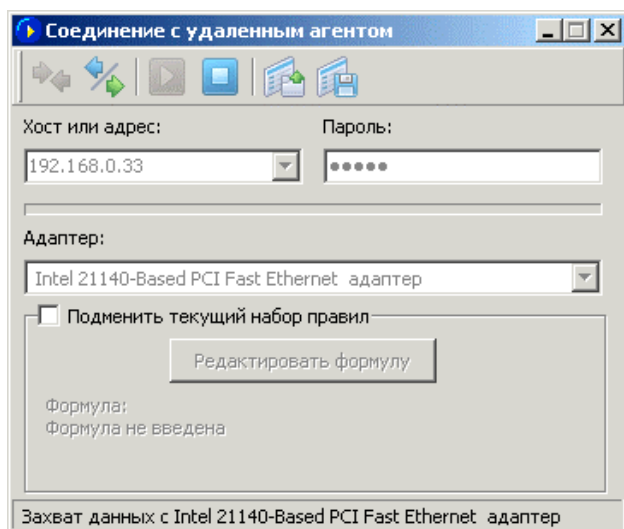


В появившемся окне введите IP-адрес компьютера, на котором установлен CommView Remote Agent, а также пароль, и нажмите кнопку **Соединиться**. Если пароль верный, соединение будет сразу же установлено. Появится сообщение *Канал готов*, а в списке доступных адаптеров появятся все имеющиеся на удалённом компьютере адаптеры.



Теперь необходимо установить правила в закладке **Правила** главного окна CommView. Важно настроить их так, чтобы не превысить пропускную способность канала связи между Remote Agent и CommView, иначе вы заметите существенное замедление реакции системы. Обязательно отфильтровывайте не интересующие вас пакеты (читайте об этом ниже). 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. Синтакс формулы описано в главе **Универсальные правила** файла справки CommView.

Когда всё готово, выберите в списке нужный адаптер и нажмите кнопку **Начать захват**. CommView позволяет сохранить настройки соединения в виде профиля, чтобы бы в будущем его можно было быстро загрузить. Для этого воспользуйтесь кнопкой **Сохранить профиль**.



CommView начнёт сбор трафика удалённого компьютера, как если бы это был ваш локальный трафик. Между этими двумя режимами работы CommView практически нет разницы. Чтобы закончить удалённое наблюдение, нажмите кнопку **Закончить захват**. Можно или выбрать другой адаптер 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 может работать с несколькими соединениями с CommView Remote Agent одновременно, т.е. можно создавать много соединений, каждое со своими независимыми настройками и набором правил, давая возможность мониторинга нескольких сегментов сети.

Советы по эффективному использованию CommView Remote Agent

Настоятельно рекомендуем обратить самое пристальное внимание на установки правил сбора пакетов (в закладке **Правила** главного окна CommView), чтобы они соответствовали целям ваших исследований. Пропускная способность канала связи между вашим и исследуемым компьютером неограничена; чаще всего, если CommView Remote Agent установлен в сети с интенсивным трафиком, **вся** ёмкость канала будет занята попытками передавать **все** пакеты на ваш CommView. Если правила установлены так, что они не отбрасывают все нежелательные пакеты, весьма вероятно перегрузка канала связи CommView с CommView Remote Agent. Даже если вы связаны с CommView Remote Agent через каналы T1 или T3 (1.5 или 4.5 Mb/сек соответственно), удалённый компьютер может находиться в 100 Mb/сек сети; таким образом, при высокой сетевой активности, ваша линия связи может оказаться совершенно не соответствующей объёму подлежащего передаче трафика

Если CommView Remote Agent захватывает данных больше, чем можно передать в сторону CommView, он использует буфер для пакетов, которые невозможно отправить немедленно. Размер буфера 5 Mb. Индикатор **Использование буфера** в окне Remote Agent отображает текущее состояние буфера. Например, если в буфере находится 2.5 Mb данных, использование буфера составит 50%. При достижении уровня занятости буфера в 100%, программа прекращает добавлять туда новые данные и отбрасывает захватываемые пакеты до тех пор, пока в буфере не появится свободное место. Не допустить потери данных можно, установив правила сбора пакетов так, чтобы буфер не переполнялся.

Безопасность

CommView Remote Agent разрабатывался с учётом требований сетевой безопасности. Доступ предоставляется только по паролю, который открытым текстом по сети НЕ передаётся, а проверяется по схеме "запрос-ответ" с использованием хэш-функции. Если проверка пароля прошла успешно, весь передаваемый трафик компрессируется и шифруется этим же паролем. Храните пароль в строгой секретности. Если пароль попадёт в руки к посторонним, они смогут получить широкие возможности по изучению вашей сети и перехвату сетевого трафика.

Информация

Как приобрести CommView Remote Agent

Демо-версия имеет 30-дневный ознакомительный период. Для получения информации о ценах и покупке перейдите на наш [веб-сайт](#).

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

Web

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

E-mail

sales@tamos.com (вопросы, связанные с продажами)

support@tamos.com (по всем остальным вопросам)

Почта и факс

Почтовый адрес:

TamoSoft
PO Box 1385
Christchurch 8140
New Zealand

Факс: +64 3 359 0392 (Новая Зеландия)

Факс: +1 971 591-6567 (США)

Другие продукты компании Тамософт

CommView

CommView - это полезный инструмент для администраторов локальных сетей, специалистов по безопасности, сетевых программистов или для любого желающего наглядно видеть полную картину трафика, проходящего через его компьютер или сегмент локальной сети. С помощью CommView вы можете видеть список сетевых соединений, IP-статистику и исследовать отдельные пакеты. IP-пакеты декодируются вплоть до самого низкого уровня с полным анализом распространенных протоколов. Предоставляется полный доступ к низкоуровневым 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.

[Подробнее](#)

CommView для WiFi

CommView для WiFi - это мощный инструмент для мониторинга и анализа беспроводных сетей 802.11 a/b/g/n. 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](#)

DigiSecret

DigiSecret – простая, надёжная и мощная программа шифрования. В ней используется проверенный временем мощный алгоритм кодирования для создания зашифрованных архивов, самораспаковывающихся EXE-файлов. В DigiSecret есть и средства сжатия файлов; вам больше не потребуется "сжимать" файлы, вы сможете за один раз и зашифровать и заархивировать их в DigiSecret. Программа интегрируется в оболочку Windows, все операции доступны по щелчку правой кнопкой мышки по файлам. Поддерживается drag-and-drop работа с файлами.

[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](#)