CommView

Сетевой монитор и анализатор для MS Windows

Руководство пользователя

Введение

О программе CommView

CommView предназначен для мониторинга сетевой активности путём сбора и анализа пакетов любой Ethernet 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 распространённых протоколов. Предоставляется полный доступ к необработанным данным. Перехваченные пакеты могут быть сохранены в файл для последующего анализа, а также экспортированы в другие форматы. Гибкая система фильтров делает возможным отбрасывать ненужные Вам пакеты или перехватывать только те пакеты, которые Вы захотите. Вы можете получать извещения от гибкой системы сигнализации о таких событиях, как наличие в трафике подозрительных пакетов, появление в сети узлов с нештатными адресами или повышение сетевой нагрузки.

CommView - это полезное средство для администраторов локальных сетей, специалистов по безопасности, сетевых программистов, или для любого желающего иметь полную картину трафика, проходящего через его компьютер или сегмент локальной сети. Это приложение разработано для сетей небольших или средних размеров и может быть запущено на любой Windows 95/98/Me/NT/2000/XP системе. Ему необходим сетевой адаптер Ethernet (или Wireless Ethernet) с поддержкой стандарта NDIS 3.0, или стандартный контроллер удалённого доступа (dial-up).

CommView осуществляет полный анализ следующих протоколов: ARP, BCAST, BGP, BMP, CDP, DAYTIME, DDNS, DHCP, DIAG, DNS, EIGRP, FTP, G.723, GRE, H.225, H.261, H.263, H.323, HTTP, HTTPS, ICMP, ICQ, IGMP, IGRP, IPsec, IPv4, IPv6, IPX, HSRP, NCP, NDS, NetBIOS, NFS, NLSP, NTP, OSPF, POP3, PPP, PPPoE, RARP, RADIUS, RDP, RIP, RIPX, RMCP, RPC, RSVP, RTP, RTCP, RTSP, SAP, SER, SMB, SMTP, SNA, SNMP, SNTP, SOCKS, SPX, TCP, TELNET, TFTP, TIME, UDP, VTP, WAP, WDOG, 802.1Q, 802.1X. Список протоколов будет расширен в следующих версиях программы.

Кроме того, новая технология удалённого мониторинга позволяет пользователям CommView наблюдать сетевой трафик компьютера с установленным на нём CommView Remote Agent'ом, где бы такой компьютер ни был физически расположен. Программа CommView Remote Agent является полезным расширением данного анализатора пакетов (CommView).

История версий

Версия 4.0

- Предупреждения: конфигурируемая система сигнализации может извещать о специфических пакетах, неизвестных MAC адресах и т.п.
- Добавлена поддержка протоколов: DAYTIME, DDNS, H.323 (H.225, Q.850, Q.931, Q.932), HTTPS, NTP, RMCP, RTP/RTCP (G.723, H.261, H.263), SNTP, TIME.
- Многоязыковой интерфейс.
- К программе можно подключить пользовательский модуль декодирования протоколов/пакетов.
- Новые параметры командной строки позволяют запускать программу с указываемым набором правил и/или с использованием требуемого адаптера.
- В окне Реконструкции TCP Сессии появилась функция "ПОИСК".
- В Генераторе Пакетов добавлены шаблоны пакетов TCP, UDP и ICMP.
- Функция "Декодировать как…" позволяет декодировать известные протоколы при использовании ими нестандартных портов.
- Расширен список опций конфигурации.

Версия 3.4

- Добавлена поддержка протоколов BGP, EIGRP, IGRP, IPsec, GTP, HSRP, NFS, OSPF, RADIUS, RIP, SNA, VTP, WAP, 802.1Q, 802.1X.
- Добавлена возможность разделять/объединять файлы формата CCF.
- В окне Реконструкции TCP сессий теперь можно переключаться между разными сессиями.
- Новые возможности окна Статистики: выбор отображения интенсивности в бит/сек или байт/сек, индикатор использования пропускной способности, графы распределения IP протоколов и субпротоколов по количеству байтов или пакетов.
- Можно отключать "всеядный" режим (promiscuous mode).
- Импорт файлов в форматах MS NetMon и NAI Sniffer for Windows.
- В окне формул составные правила можно включить подцветку синтаксиса.
- Улучшена поддержка Windows XP themes.
- Исправление ошибки в hex функции составных правил, она неправильно работала с шаблонами, содержащими 0x00.

Версия 3.3

- Добавлена поддержка протоколов FTP, TFTP, SOCKS (v. 4,5), TELNET.
- Используя Булеву логику и легко читаемый синтаксис, можно составлять сложные фильтры.
- Дальнейшее повышение производительности программы.
- Новые возможности в генераторе пакетов: поддержка drag-and-drop для многих форматов пакетов, высокоскоростная генерация пакетов (до 5000 пакетов в секунду), отправка нескольких разных пакетов одним щелчком мышки.
- Отключаемая возможность слияния нескольких log-файлов в один.
- Добавлены новые форматы экспорта: файл с разделителем "точка с запятой", содержащий/не содержащий шестнадцатеричный дамп.
- Сохранение пакетов в форматах CCF, ECN и др., без предварительной загрузки их в утилиту Просмотра Log-файлов.
- Таблицы сетевых узлов расширены до 1000 MAC и IP адресов.
- В списке пакетов добавлена отключаемая колонка Размер Пакетов.
- Описание IP адресов и масок подсети как локальных, для правильного построения статистики.
- Многочисленные улучшения, а также исправления ошибок.

Версия 3.2

- Добавлена поддержка протоколов SNMP (v.1, 2, 3), IPv6, ICQ, GRE, RDP.
- Улучшена производительность при открытии/импорте CCF файлов: файлы загружаются раз в 25 быстрее.
- Снижена загрузка процессора.
- Расширена статистика работы сетевого адаптера – отображаются коллизии, ошибки контрольной суммы.
- В утилите просмотра Log-файлов можно воспользоваться набором правил.
- Улучшен диалог поиска пакетов.

Версия 3.1

- Добавлена поддержка протоколов DHCP, DNS, HTTP, POP3, RTSP, SMTP.
- Технология удаленного мониторинга.
- В диаграмму распределения суб-протоколов IP можно добавлять до четырёх пользовательских протоколов.
- Импорт файлов в формате Tcpdump (libcap).
- Добавлены новые опции в настройки программы.
- Многочисленные улучшения, а также исправления ошибок.

Версия 3.0

- Новый декодер протоколов поддерживает ARP, BCAST, BMP, DIAG, ICMP, IGMP, IPv4, IPX, NCP, NDS, NetBIOS, NLSP, PPP, PPPoE, RARP, RIPX, RSVP, SAP, SER, SMB, SPX, TCP, UDP, WDOG.
- Поддержка Wireless Ethernet (802.11b) адаптера.
- Программа работоспособна под Windows XP (тестирована на RC1)
- При работе под Windows 2000/XP, генератор пакетов может посылать пакеты в адаптер удалённого доступа (dial-up).
- В генератор пакетов добавлены декодер протоколов и корректор контрольной суммы.
- Для наблюдения за трафиком через несколько адаптеров одновременно, можно запускать необходимое число копий программы CommView.
- IP статистику можно включать в Отчёт.
- В окно Статистики добавлена новая таблица LAN хостов по IP адресам.
- В окне Реконструкции TCP сессии можно включать/выключать данные, основываясь на направлении пакетов.
- При фильтрации пакетов теперь можно учитывать TCP флаги.
- Невидимый режим работы программы.
- Используя простой TCP/IP интерфейс, CommView может передавать данные в Вашу прикладную программу.
- Можно выбрать сразу несколько пакетов в закладке Пакеты.

Версия 2.6

- IP адресам можно присваивать имена (алиасы);
- Правила можно применить в окнах Statistics(Статистика) и отчётов;
- Декодирование PPPoE;
- Можно открывать несколько окон TCP Session Reconstruction(Реконструкция TCP сессии) для одновременного просмотра разных сессий;
- Дальнейшее улучшение интерфейса и исправление ошибок.

Версия 2.5

- Поддержка drag-and-drop: мышкой можно перемещать IP Statistics(IP Статистику), пакеты, графы отчётов на десктоп или в любую папку. Аналогично, можно отправлять файлы накопленных пакетов (CCF, ENC, or BFR) в любое внешнее приложение;
- Добавлены Packet Size Distribution chart(Граф распределения размера пакетов) и LAN Hosts Table(Таблица LAN-хостов) в окне Statistics(Статистика);
- Автоматическое или ручное составление отчётов: любые статистические данные можно сохранить в виде HTML или файле отчёта с разделителем-двоеточием [см. закладку Report(Отчёт) в окне Statistics(Статистика)];
- Окно TCP Session Reconstruction(Реконструкция TCP сессии) может отображать данные в виде HTML и EBCDIC в дополнение к ASCII и HEX.

Версия 2.4

- Реконструкция TCP сессии;
- MAC адресам можно присваивать имена (алиасы);
- Определение изготовителя сетевого адаптера по NIC;
- Добавлены новые колонки в закладки IP Statistics(IP Статистика) and Packets(Пакеты);
- Колонки в закладках Packets(Пакеты) и IP Statistics(IP Статистика) можно выключать;
- Декодирование ARP/RARP пакетов;
- Можно использовать маски в правилах IP адресов;
- Режим Both(В обе стороны) добавлен в правила сбора пакетов в дополнение к From(Исход.) и To(Вход.);
- Закладки с включёнными правилами отображаются жирным шрифтом;
- Вывод пакетов можно приостановить/возобновить (suspend/resume);
- Доступны различные формы показа IP Statistics(IP Статистика);
- Некоторые косметические улучшения.

Версия 2.3

- Поддержка Dial-up в Windows 2000.

Версия 2.2

- MAC, IP, и TCP/UDP/ICMP заголовки можно раскрашивать в разные цвета;
- Содержимое закладки IP Statistics(IP Статистика) можно сохранить в файле HTML;
- Добавлена утилита Packet Generator(Генератор пакетов), позволяющая передавать пакеты в сеть;
- Пользовательские настройки правил сбора пакетов можно сохранять и загружать;
- Поиск текста с учётом регистра;
- Улучшен диалог Find Packet Contents(Искать содержимое пакета);
- Исправлена ошибка: запуск драйвера на локализованной Windows 2000 происходит теперь нормально.

Версия 2.1

- Log Viewer(Просмотр Log-файлов): файлы с перехваченными пакетами можно загрузить и исследовать так же, как это делается с перехваченными данными в реальном времени;

- Импорт и экспорт Log-файлов из/в форматы NI Observer или NAI Sniffer;
- Номера портов можно отображать как названия сервисов;
- Новая возможность Jump To(Перейти к): позволяет быстро находить входящие/исходящие пакеты по заданному IP адресу;
- Некоторые улучшения интерфейса;
- Исправлена ошибка: предыдущая версия показывала некорректную контрольную сумму UDP.

Версия 2.01

- Поддержка Windows 2000.

Версия 2.0 Final

- Улучшена производительность под Windows NT;
- Исправлены ошибки, найденные в 2.0 Beta.

Версия 2.0 Beta

- Поддержка Windows NT;
- Доступно больше статистической информации.

Версия 1.0 Final

- Возможности: Find Packet(Найти Пакет) и Go to Packet Number(Перейти к пакету номер…);
- Новые фильтры: перехват/игнорирование пакетов в зависимости от MAC адресов и направления пакета;
- Статистика: гистограммы Packets per second(Количество пакетов в секунду) и Bytes per second(Количество байтов в секунду), графики распределения IP протоколов и суб-протоколов;
- Исправлена ошибка: текстовый фильтр в v.1.0 Beta иногда перехватывал пакеты, не содержащие заданный текст.

Лицензионное соглашение

Пожалуйста, прежде чем использовать это программное обеспечение, внимательно прочтите данные условия. Ваше использование этого программного обеспечения означает Ваше согласие с этим лицензионным соглашением. Если Вы не согласны с условиями этого лицензионного соглашения, Вы должны удалить это программное обеспечение с Вашего устройства хранения и перестать использовать продукт.

Авторское право
Авторские права этого программного обеспечения принадлежат TamoSoft, Inc 1999-2003. CommView – торговая марка TamoSoft, Inc. Использование этого программного обеспечения и авторские права на него охраняются международными договорами об авторском праве. TamoSoft, Inc. владеет всеми правами на это программное обеспечение и документацию, и предоставленная лицензия ни каким образом не уменьшает права на интеллектуальную собственность TamoSoft, Inc. Вы не должны распространять регистрационные коды, предоставляемые на бумаге, в электронном виде, или другой форме.

Демонстрационная Версия
Это не бесплатное программное обеспечение. Настоящим Вам разрешается использовать это программное обеспечение для испытательных целей бесплатно в течение 30 дней. Использование этого программного обеспечения после данного срока является нарушением законов об авторских правах и может закончиться серьезным гражданским и уголовным наказанием.

Зарегистрированная Версия
Одна зарегистрированная копия этого программного обеспечения может или использоваться одним человеком, который лично использует продукт на одном или более компьютерах, или инсталлироваться на одной рабочей станции неодновременно используемой несколькими людьми, но не то и другое вместе. Данное программное обеспечение может быть установлено на сетевом сервере, при условии, что от TamoSoft Inc получены соответствующие отдельные лицензии для каждого терминала, имеющего доступ к данному программному обеспечению.

Отказ от гарантий
Это программное обеспечение предоставляется "как есть" без гарантий любого типа, явных или не явных; включая, но не ограничиваясь, гарантиями коммерческими или пригодности для конкретной цели. Ни в каком случае Tamosoft, inc. не будет нести ответственность перед вами за любой ущерб, включая случайный, или вытекающие ущербы, возникающие при использовании этого программного обеспечения, даже если бы было предупреждено о возможных таких ущербах. Вы подтверждаете, что вы прочитали эту лицензию, понимаете и согласны быть в рамках его условий.

Законодательная поддержка
Данное Соглашение будет рассматриваться в рамках законов Республики Кипр.

Распространение
Это программное обеспечение может свободно распространятся в оригинальной немодифицированной и незарегистрированной форме. Дистрибутив должен включать все файлы его оригинальной поставки. Дитрибьютеры не могут брать деньги за это. Распространяющий это программное обеспечение за любое вознаграждение должен предварительно связаться с нами и получить разрешение.

Другие Ограничения
Вы не можете изменять, переделывать, декомпилировать или дизассемблировать это программное обеспечение любым путём, включая изменение или удаление любых сообщений или окон.

Работа с программой

Краткий обзор

Интерфейс программы состоит из пяти закладок, позволяющих просматривать данные и выполнять различные действия с перехваченными пакетами. Чтобы начать сбор пакетов, выберите сетевое устройство из списка на панели управления и нажмите кнопку **Start Capture(Начать сбор)** или выберите **File(Файл) =>Start Capture(Начать сбор)** из меню. Если в сети есть трафик, проходящий через выбранное устройство, CommView начнёт отображать информацию.

Главное меню

File (Файл)
Start/Stop Capture – начинает/прекращает сбор пакетов.
Suspend/Resume Packet Output – останавливает/возобновляет вывод пакетов в окна 2-й закладки.
Remote Monitoring Mode – добавляет/скрывает дополнительную панель управления удаленным мониторингом.
Save IP Statistics As – позволяет сохранить содержимое закладки **IP Statistics(IP Статистика)** в виде HTML отчёта.
Save Packet Log As – позволяет сохранить содержимое закладки **Packets(Пакеты)** в выбранном формате. Закладка Logging предоставляет на выбор несколько форматов сохранения файлов.
Log Viewer – открывает окно просмотра Log-файлов.
Clear IP Statistics – стирает содержимое закладки **IP Statistics(IP Статистика)**.
Clear Packet Buffer – стирает содержимое буфера программы и 2-й закладки (список пакетов).
Performance Data – отображает производительность программы: количество пакетов успешно захваченных и непреднамеренно пропущенных драйвером устройства. Недоступно под Windows 95/98/Me.
Exit – выход из программы.

Search (Поиск)
Find Packet – вызывает диалог поиска пакета, содержащего определённый текст.
Go to Packet Number - вызывает диалог перехода к пакету с указанным номером.

View (Просмотр)
Statistics – открывает окно со статистикой протоколов и данных.
Port Reference – позволяет посмотреть информацию о портах.
Log Directory – открывает директорию, где по умолчанию сохраняются Log-файлы.
IP Statistics Columns – включает/прячет колонки в закладке **IP Statistics(IP Статистика)**.
Packets Columns – включает/прячет колонки в закладке **Packets(Пакеты)**.

Tools (Утилиты)
Packet Generator – открывает окно генератора пакетов (кроме Windows 95/98/Me).
Reconstruct TCP Session – позволяет реконструировать TCP сессию, начиная с выбранного пакета; Открывается новое окно, отображающее весь процесс переговоров двух хостов.
NIC Vendor Identifier – открывает окно, где можно определить фирму-изготовителя сетевого адаптера по MAC адресу.
Scheduler – менеджер расписания, добавляет или удаляет из расписания новые работы.

Settings (Настройки)
Fonts – открывает вложенное меню выбора шрифтов в элементах интерфейса программы.
MAC Aliases – вызывает окно, где можно назначить имена (алиасы) MAC адресам для облегчения обзора трафика сети.
IP Aliases – вызывает окно, где можно назначить легко запоминаемые имена (алиасы) IP адресам.
Options – открывает окно **Options(Опции)**, где можно воздействовать на некоторые свойства программы.
Language – позволяет изменить язык интерфейса. Требуется перезапуск программы.

Rules (Правила)
Save Current Rules As – позволяет сохранить в конфигурационном файле текущие настройки Правил сбора пакетов.
Load Rules From – позволяет загрузить, из ранее созданного конфигурационного файла, настройки Правил сбора пакетов.
Reset All – отменяет все правила (если таковые были установлены).

Help (Справка)
Contents – открывает файл-справку CommView.
Search For Help On ... – показывает оглавление файла-справки CommView.
About – выводит информацию о версии программы.

Практически каждый элемент интерфейса имеет контекстно-зависимое меню, которое можно вызвать нажатием правой кнопки мыши, многие команды доступны через это меню.

Первая закладка отображает подробную информацию о сетевых соединениях Вашего компьютера (только по IP протоколу). Для подробной информации смотрите главу IP статистика.

Вторая закладка используется для просмотра перехваченных сетевых пакетов и отображения детальной информации о выделенном пакете. Для подробной информации смотрите главу Пакеты.

Третья закладка позволяет Вам сохранить перехваченные пакеты в файле. Для подробной информации смотрите главу Log-файлы.

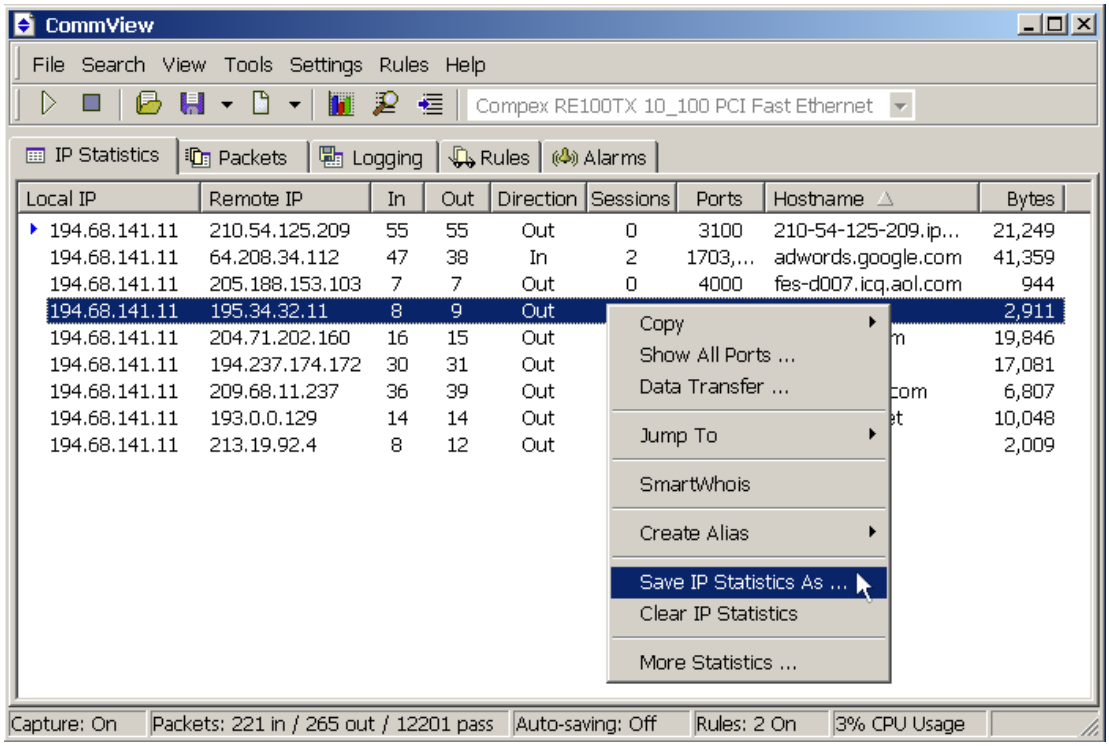
Четвёртая закладка позволяет настаивать правила, влияющие на перехват/игнорирование пакетов, основываясь на таких их свойствах, как IP адрес или номер порта. Для подробной информации смотрите главу Правила.

Пятая закладка настраивает систему извещений о подозрительных пакетах, повышении загруженности сети, нештатных адресах и тому подобном. Для подробной информации смотрите главу Предупреждения.

Вы можете изменять некоторые настройки, такие как шрифты, цвета, и размер буфера, выбирая **Settings(Установки)** из меню. Для подробной информации смотрите главу Установка опций.

IP статистика

Эта закладка отображает подробную информацию о сетевых соединениях Вашего компьютера (только по IP протоколу). Чтобы начать захват пакетов, выберите **File(Файл) =>Start Capture(Начать сбор)** в меню, или нажмите соответствующую кнопку на панели инструментов.



Ниже описывается назначение колонок таблицы:

Local IP – показывает локальный IP адрес. Для входящих пакетов это IP адрес получателя, для исходящих и транзитных - IP адрес источника.
Remote IP – показывает удалённый IP адрес. Для входящих пакетов это IP адрес источника, для исходящих и транзитных - IP адрес получателя.
In – показывает число принятых пакетов.
Out – показывает число посланных пакетов.
Direction – показывает направление сессии. Направление сессии определяется по направлению первого пакета, принятого от или посланного на удалённый IP адрес.
Sessions – 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.
Ports – список портов удалённого компьютера, используемых во время TCP/IP соединения или попытки соединения. Этот список может быть пустым, если протокол не является TCP/IP. Порты могут быть показаны или как числовые значения, или как соответствующие названия сервисов. Для более подробной информации смотрите главу Установка опций.
Hostname – показывает доменное имя удалённого компьютера. Если имя не может быть определено – колонка пуста.
Bytes – количество байтов, переданных за сессию.
Last packet – показывает время последнего принятого/посланного пакета сессии.

Можно выводить/прятать отдельные колонки таблицы, воздействуя на элементы меню **View(Просмотр) =>IP Statistics Columns(Колонки IP статистики)**.

Команды контекстного меню

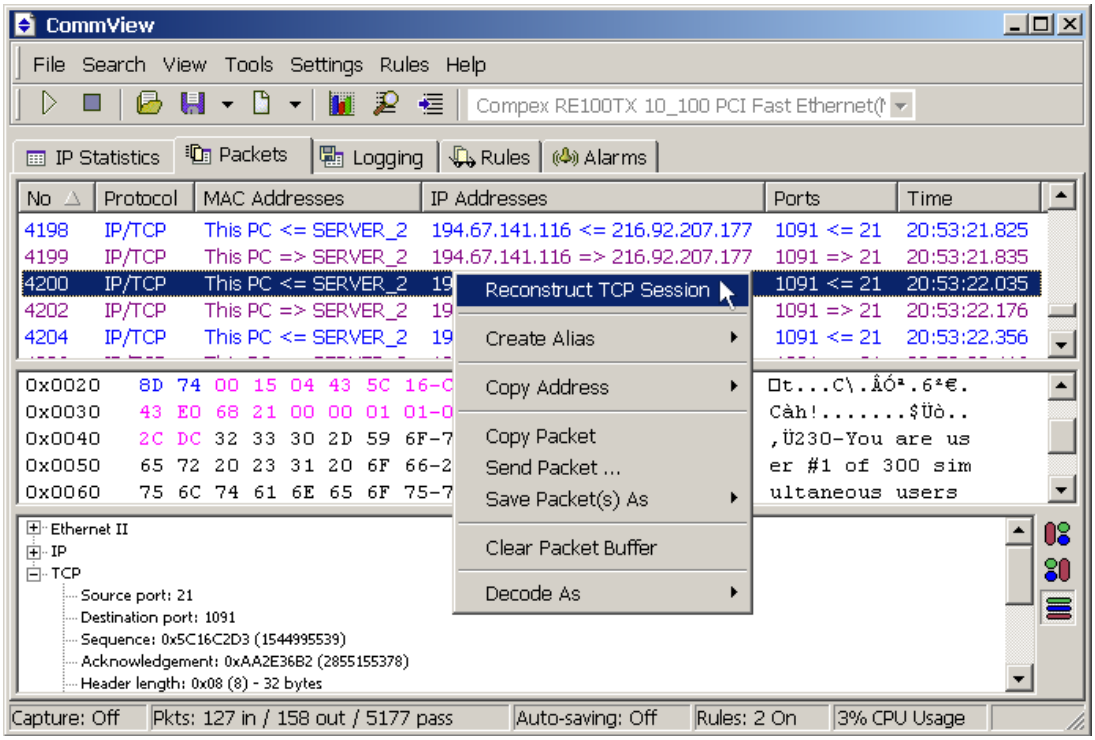
Нажатие правой кнопки мышки на таблице IP Statistics(IP Статистика) вызывает меню со следующими командами:

Copy – копирует локальный IP адрес, удалённый IP адрес или имя хоста в буфер обмена.
Show All Ports – отображает окно с полным списком портов используемых между выбранной парой IP адресов. Это удобно, если все используемые порты не помещаются в соответствующей колонке.
Data Transfer – отображает окно с информацией об объёме передачи данных между выбранной парой IP адресов и с временем приёма/посылки последнего пакета.
Jump To – позволяет быстро переходить к первому/последнему пакету с выбранным IP адресом источника/получателя; программа откроет закладку Packets(Пакеты) и установит курсор на соответствующий пакет.
SmartWhois – отправляет выбранный IP адрес удалённого хоста в SmartWhois, если таковая программа установлена на Вашем компьютере. SmartWhois - это 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.

Create Alias – открывает окно, где можно назначить легко запоминаемые имена (алиасы) IP адресам.
Save IP Statistics As – позволяет сохранить содержимое закладки **IP Statistics(IP Статистика)** как HTML отчёт.
Clear IP Statistics – очищает таблицу статистики.
More Statistics – открывает окно со статистикой протоколов и данных.

Пакеты

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



Верхнее окно содержит список всех перехваченных пакетов. Используйте этот список для выбора пакета, который Вы хотите проанализировать. При выборе пакета нажатием на него, остальные окна показывают информацию о выделенном пакете.

Ниже описывается назначение колонок таблицы:

No – уникальный номер пакета. При настройке CommView с помощью закладки Rules (Правила) на фильтрацию пакетов, некоторые пакеты не будут перехватываться, но будут регистрироваться. Поэтому можно заметить, что пакеты занумерованы не по порядку.
Protocol – показывает протокол пакета.
MAC Addresses – показывает MAC адреса источника и получателя, а также направление пакета.

Пример:

22:22:22:22:22:22 => 33:33:33:33:33:33 исходящий пакет от 22:22:22:22:22:22 к 33:33:33:33:33:33.

22:22:22:22:22:22 <= 33:33:33:33:33:33 входящий пакет от 33:33:33:33:33:33 к 22:22:22:22:22:22.

44:44:44:44:44:44 <=> 55:55:55:55:55:55 транзитный пакет от 44:44:44:44:44:44 к 55:55:55:55:55:55.

55:55:55:55:55:55 <=> 44:44:44:44:44:44 транзитный пакет от 55:55:55:55:55:55 к 44:44:44:44:44:44.

IP Addresses – показывает IP адреса источника и получателя (когда применимо), а также направление пакета.
Ports – показывает порты источника и получателя (когда применимо), а также направление пакета. Порты могут быть отображены или как числовые значения, или как соответствующие названия сервисов. Для более подробной информации смотрите главу Установка опций.
Time / Delta – показывает время появления пакета – абсолютное или как интервал от предыдущего пакета. Переключать режим можно в меню **View(Просмотр) =>Packets Columns(Колонки пакета) =>Show Time As(Показать время как)**.
Size – показывает размер пакета в байтах. По умолчанию, колонка не отображается.

Можно выводить/прятать отдельные колонки таблицы воздействуя на элементы меню **View(Просмотр) =>Packet Columns(Колонки пакета).** Вывод пакетов можно приостановить включив пункт **File(Файл) =>Suspend Packet Output(Приостановить выдачу)**. В этом случае пакеты перехватываются, но не показываются в закладке **Packets(Пакеты)**. Этим можно воспользоваться, когда интересует только статистика, а не сами пакеты. Чтобы восстановить показ пакетов в реальном времени, включите пункт **File(Файл) =>Resume Packet Output(Возобновить выдачу)**.

Среднее окно отображает сырые данные пакета в шестнадцатеричном виде и как текст. В тексте точками заменяются непечатаемые символы.

Нижнее окно показывает декодированную информацию о выбранном пакете. Здесь приводятся ценные сведения для сетевых специалистов. Щелчок правой кнопкой мыши в панели вызывает контекстное меню, позволяющее открывать/закрывать узлы, копировать содержимое выбранного узла или всех узлов. Нажатием на одну из трёх кнопок на краю окна, можно менять его положение (расположить его внизу, справа или слева).

Команды контекстного меню

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

Reconstruct TCP Session – позволяет реконструировать TCP сессию, начиная с выделенного пакета; Открывается новое окно, отображающее весь процесс переговоров двух хостов.
Create Alias -- открывает окно, где можно назначить легко запоминаемые имена (алиасы) выбранным MAC или IP адресам.
Copy Address – копирует локальный MAC или IP адрес, удалённый MAC или IP адрес в буфер обмена.
Copy Packet – копирует сырые данные пакета в буфер обмена.
Send Packet – открывает окно генератора пакетов и позволяет послать выбранный пакет ещё раз. Перед отправкой содержимое пакета можно изменить.
Save Packet(s) As – записывает содержимое выбранного пакета (одного или нескольких) в файл. Формат файла выбирается в выпадающем меню.
Clear Packet Buffer – сбрасывает программный буфер пакетов. Список пакетов очищается, и все накопленные к этому моменту пакеты стираются.
Decode As – (Декодировать как…) действует на TCP и UDP пакеты, позволяет декодировать известные программе протоколы, использующие в данный момент нестандартные номера портов. Например, если сервер SOCKS, вместо 1080, использует порт 333, можно выбрать пакет, принадлежащий сессии SOCKS, и зайдя в это меню, заставить CommView декодировать все пакеты порта 333 как SOCKS. Такое переназначение действует до перезапуска программы. ВНИМАНИЕ! Нельзя переназначить стандартные сочетания порт-протокол, то есть, Вы не сможете заставить CommView декодировать пакеты порта 80 как пакеты TELNET'а.

Кроме того, мышкой можно перемещать пакеты на десктоп или в любую папку.

Ведение Log-файлов

Эта закладка предназначена для записи перехваченных пакетов в файл на диске. CommView сохраняет пакеты в файлы с расширением CCF (CommView Capture Files) в собственном формате. Вы можете в любое время загрузить и просмотреть эти файлы с помощью утилиты Log viewer, или просто дважды щёлкнув мышкой любой CCF файл в папке или на десктопе.

Save Log (Сохранить Log-файл)

Используйте этот фрейм для ручного сохранения накопленных пакетов. Можно или сохранить все пакеты, находящиеся на данный момент в буфере (All packets in buffer), или только часть из них, в заданном диапазоне (Range). Поля From(Начиная от) и To(Вплоть до) устанавливают требуемый диапазон номеров пакетов, отображённых в закладке Packets(Пакеты). Нажмите Save As …(Сохранить Как …) для выбора имени файла.

Auto-saving (Автоматическое сохранение)

Установите этот флажок, чтобы программа автоматически сохраняла перехваченные пакеты, когда они поступают. Используйте поле Maximum directory size (Максимальный объём папки), чтобы ограничить общий размер файлов, находящихся в Папке Log-файлов (Log Directory). Если общий размер файлов превышает предел, программа автоматически удаляет наиболее старые файлы. Чтобы назначить другую Папку Log-файлов (Log Directory), нажмите на поле Save files to (Сохранить файлы в) и выберите другой каталог. Пакеты собираются в блоки по 500 штук в каждом файле. Если требуется, чтобы все файлы данной сессии были объединены в один, установите флаг Concatenate files when capturing is stopped. Программа произведёт объединение файлов после прекращения захвата пакетов.

500 пакетов занимают приблизительно 500 килобайт в файле.

Внимание: Если нужно важный файл сохранить на долгое время, не храните его в Папке Log-файлов, так как есть шанс, что он будет автоматически стёрт по мере записи новых файлов. Переместите файл в другой каталог.

Пожалуйста, имейте в виду, что программа не сохраняет каждый пакет сразу по его прибытию. Пакеты сохраняются по 500 штук за раз. Это означает, что если Вы просматриваете Log-файл в реальном времени, он может не содержать последние 500 пакетов. Для того чтобы программа немедленно переслала буфер в файл, нажмите Stop Capture (Остановить Перехват), или снимите флажок автосохранения (Auto-saving).

Работа с Log-файлами

В поле Log Management, Вы можете вручную объединять несколько файлов CCF в один, нажав на кнопку Concatenate Logs. Кнопка Split Logs позволяет разделить большой файл на несколько меньших. Программа задаст несколько вопросов, и Вы сможете указать желаемый размер результирующих файлов (в мегабайтах).

Просмотр Log-файлов

Утилита просмотра **Log-файлов (Log Viewer)** предназначена для просмотра и исследования файлов перехваченных пакетов, созданных CommView и некоторыми другими анализаторами пакетов. Функционально такая же, как и закладка Packets(Пакеты) главного окна программы, утилита отображает пакеты загруженные из файла, а не перехватываемые в реальном времени.

Выберите **File(Файл) =>Log Viewer(просмотр Log-файлов)** в главном меню программы, или дважды щёлкните на любой файл перехваченных пакетов CommView, который Вы прежде сохранили. Можно открывать несколько окон просмотра, и каждое из них может быть использовано для исследования одного или нескольких файлов.

Этой утилитой можно воспользоваться для исследования Log-файлов, созданных другими анализаторами пакетов и брандмауэрами. Настоящая версия может импортировать файлы в форматах Network Instruments Observer®, Network Associates Sniffer® для DOS/Windows, Microsoft NetMon и Tcpdump (libcap). Эти форматы используются другими приложениями тоже. Утилита способна экспортировать пакеты в файлы форматов Network Instruments Observer® и Network Associates Sniffer® для DOS, также как и в собственный формат программы CommView.

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

Команды контекстного меню

File (Файл)

Load CommView Logs – открывает и загружает файлы в собственном формате CommView.
Import Logs – импортирует Log-файлы, созданные другими анализаторами пакетов.
Export Logs – экспортирует отображаемые пакеты в Log-файлы нескольких форматов.
Clear Window – очищает окно просмотра.
Close Window – закрывает окно просмотра.

Search (Поиск)

Find Packet – вызывает диалог поиска пакета, содержащего определённый текст.
Go to Packet Number - вызывает диалог перехода к пакету с указанным номером.

Rules (Правила)

Apply – накладывает текущий набор правил на пакеты, отображаемые утилитой. В результате, программа отбросит пакеты, не отвечающие указанным условиям. Файл на диске, при этом, не изменяется.
From File ...(Из файла...) – то же, что и по команде **Apply**, но позволяет воспользоваться заранее сохранёнными настройками фильтров в файлах .RLS, а не текущими.

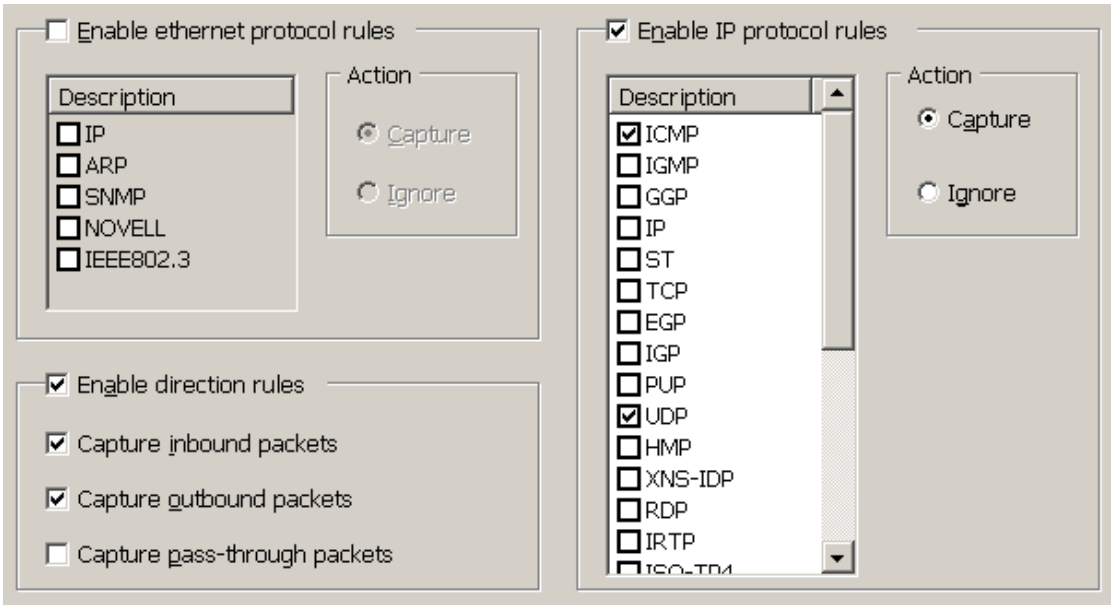
Правила

Эта закладка позволяет устанавливать ограничения на перехват пакетов. Если какие либо правила установлены, то программа фильтрует пакеты и накапливает только те пакеты, которые соответствуют заданным критериям. Обратите внимание, CommView не брандмауэр, и, когда Вы задаёте правила, пакеты продолжают обрабатываться операционной системой, они лишь не отображаются и не сохраняются программой. Название закладки выводится жирным шрифтом, если правила в ней установлены.

Используя команду Rules в меню, можно сохранять профили правил в файле и загружать их.
Так как сетевой трафик часто может создавать большое количество пакетов, рекомендуется использовать ограничения для отсеивания ненужных пакетов. Это может значительно снизить объём системных ресурсов, потребляемых программой. Если Вы хотите включить/выключить какое-либо правило, выберите соответствующую закладку с левой стороны окна [напр. **IP Addresses (IP Адреса)** или **Ports (Порты)**], и установите или снимите соответствующий флажок - **Enable IP Address rules (Включить правило по IP адресу)** или **Enable port rules (Включить правило по портам)**. Существует семь типов правил:

Protocols & Directions (Протоколы и Направления)

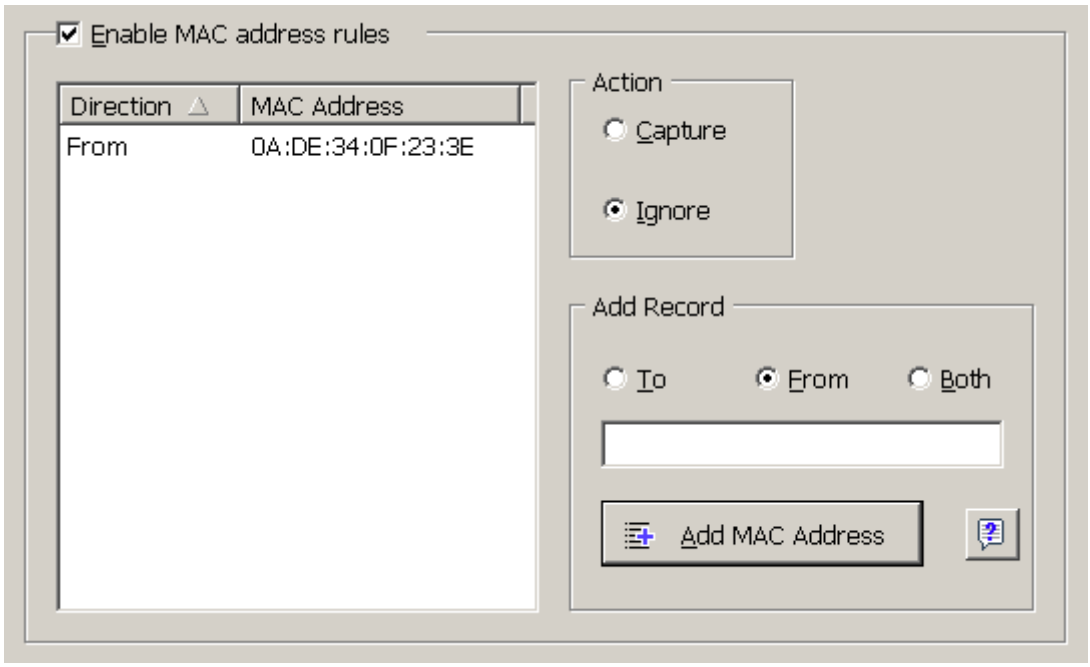
Позволяет игнорировать или перехватывать пакеты, основываясь на Ethernet (Layer 2) и IP (Layer 3) протоколах, а также на направлениях.



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

MAC Addresses (MAC адреса)

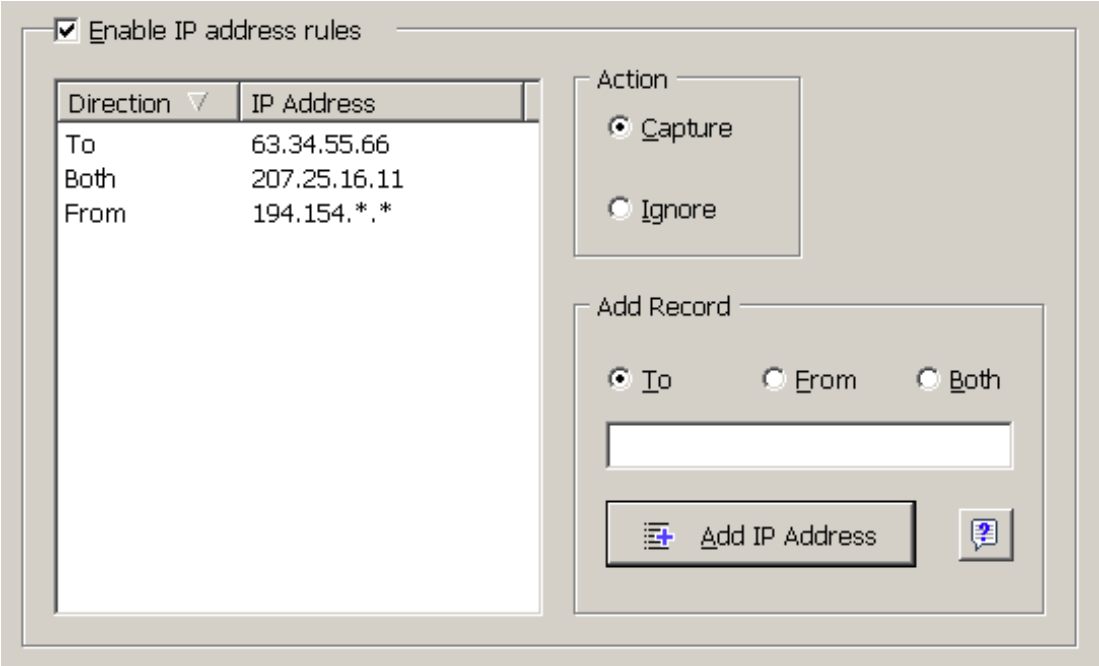
Позволяет игнорировать или перехватывать пакеты, основываясь на MAC (аппаратных) адресах. Введите MAC адрес в поле **Add Record (Добавить запись)**, выберите направление **From (От)**, **To (К)** или **Both (В обе стороны)**, и нажмите **Add MAC Address (Добавить MAC адрес)** и новое правило будет отображено. Теперь надо выбрать действие, которое будет осуществлено, когда будет проходить соответствующий пакет: он может быть или захвачен или игнорирован.
Выбор MAC адреса можно упростить, нажав на кнопку MAC-алиасов. Появится список существующих имён, и, дважды щёлкнув по имени, Вы скопируете нужный адрес в поле ввода.



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

IP Addresses (IP адреса)

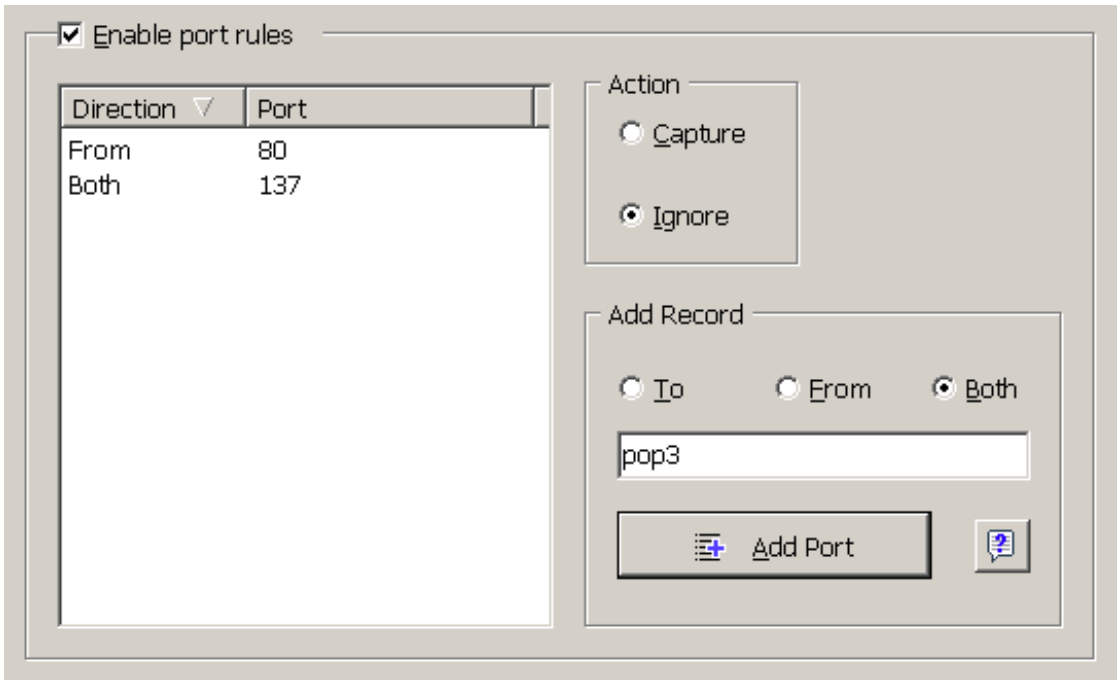
Позволяет игнорировать или перехватывать пакеты, основываясь на IP адресах. Введите IP адрес в поле **Add Record (Добавить запись)**, выберите направление **From (От), To (К)** или **Both (В обе стороны)**, и нажмите A**dd IP Address (Добавить IP адрес)** и новое правило будет отображено. Теперь надо выбрать действие, которое будет осуществлено, когда будет проходить соответствующий пакет: он может быть или захвачен или игнорирован.
Выбор IP адреса можно упростить, нажав на кнопку IP-алиасов. Появится список существующих имён, и, дважды щёлкнув по имени, Вы скопируете нужный адрес в поле ввода.



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, эта конфигурация автоматически заставляет программу игнорировать все не-IP пакеты.

Ports (Порты)

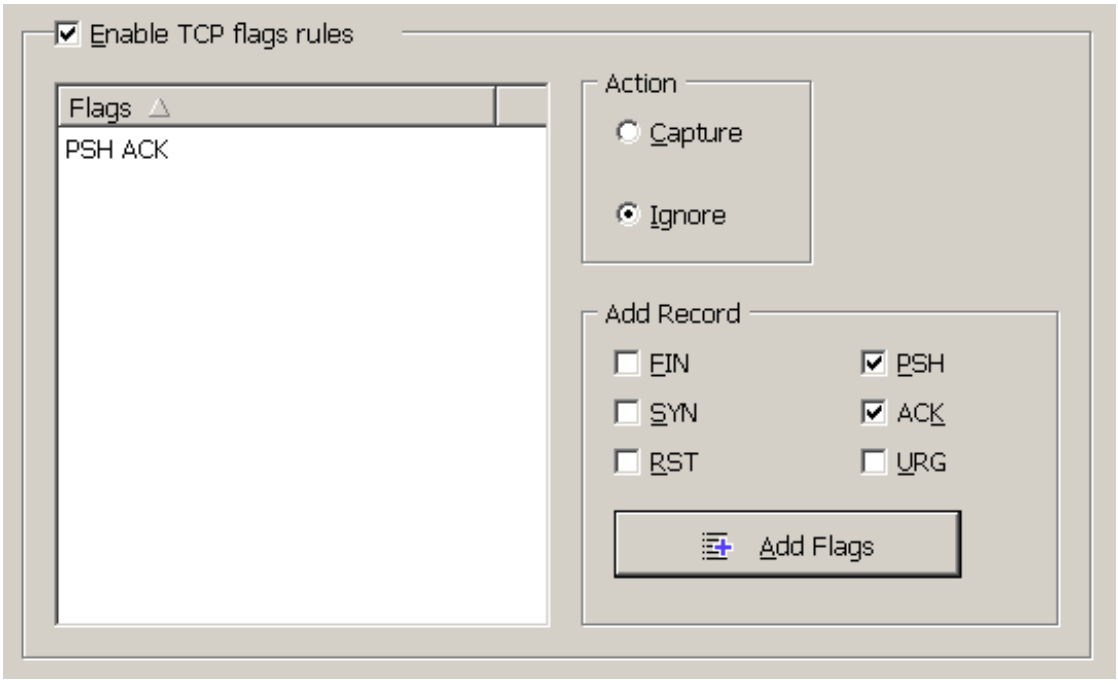
Позволяет игнорировать или перехватывать пакеты, основываясь на номерах портов. Введите номер порта в поле **Add Record (Добавить запись)**, выберите направление **From (От), To (К)** или **Both (В обе стороны)**, и нажмите **Add Port (Добавить порт)** и новое правило будет отображено. Теперь надо выбрать действие, которое будет осуществлено, когда будет проходить соответствующий пакет: он может быть или захвачен или игнорирован.
Нажав на кнопку **Port reference**, можно увидеть список всех известных портов; дважды щёлкнув по порту мышкой, Вы добавите его в запись. Порты можно вводить по имени, например, http или pop3, и программа подставит его номер.



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

TCP Flags (TCP флаги)

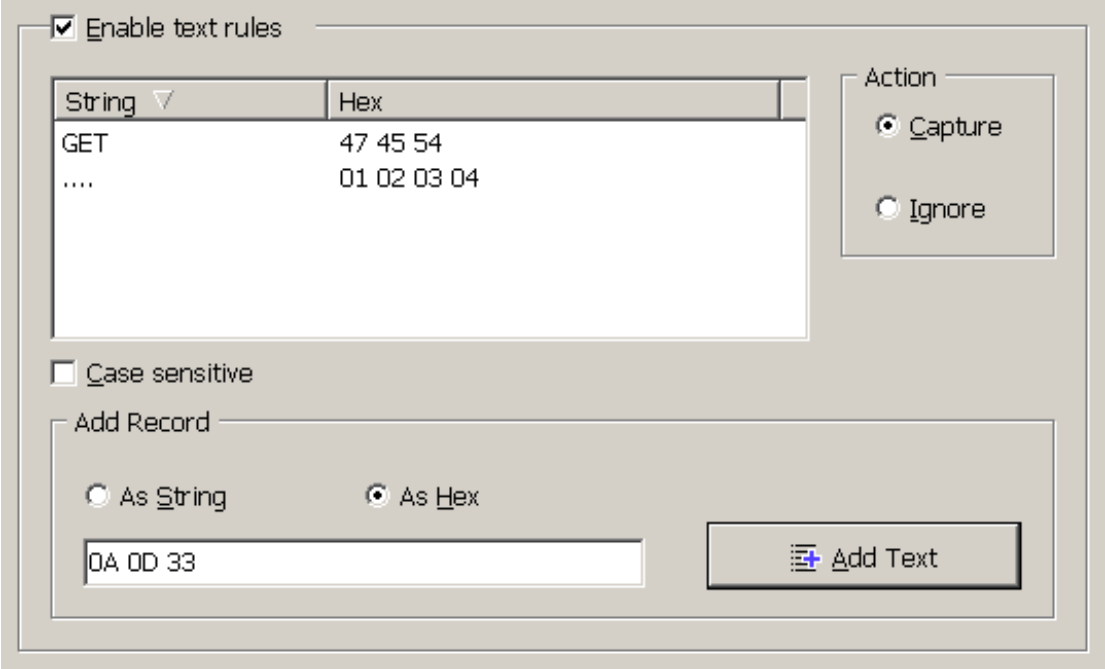
Позволяет игнорировать или перехватывать пакеты, основываясь на TCP флагах. Выберите флаг или комбинацию флагов в поле **Add Record (Добавить запись)**, и нажмите **Add Flags (Добавить флаги)** и новое правило будет отображено. Теперь надо выбрать действие, которое будет осуществлено, когда будет проходить пакет с соответствующим(и) флагом(ами): он может быть или захвачен или игнорирован.



В этом примере показано, как игнорировать TCP пакеты с установленным PSH ACK флагом. Пакеты с другими флагами будут накапливаться.

Text (Текст)

Позволяет ловить пакеты, содержащие определённый текст. Введите строку в поле **Add Record (Добавить запись)**, выберите тип **As String (Как текст)** или **As Hex (Шестнадцатеричная величина)**, и нажмите **Add Text (Добавить текст)** и новое правило будет отображено. Теперь надо выбрать действие, которое будет осуществлено, когда будет проходить соответствующий пакет: он может быть или захвачен или игнорирован. Шестнадцатеричные величины разделять в образце пробелами.



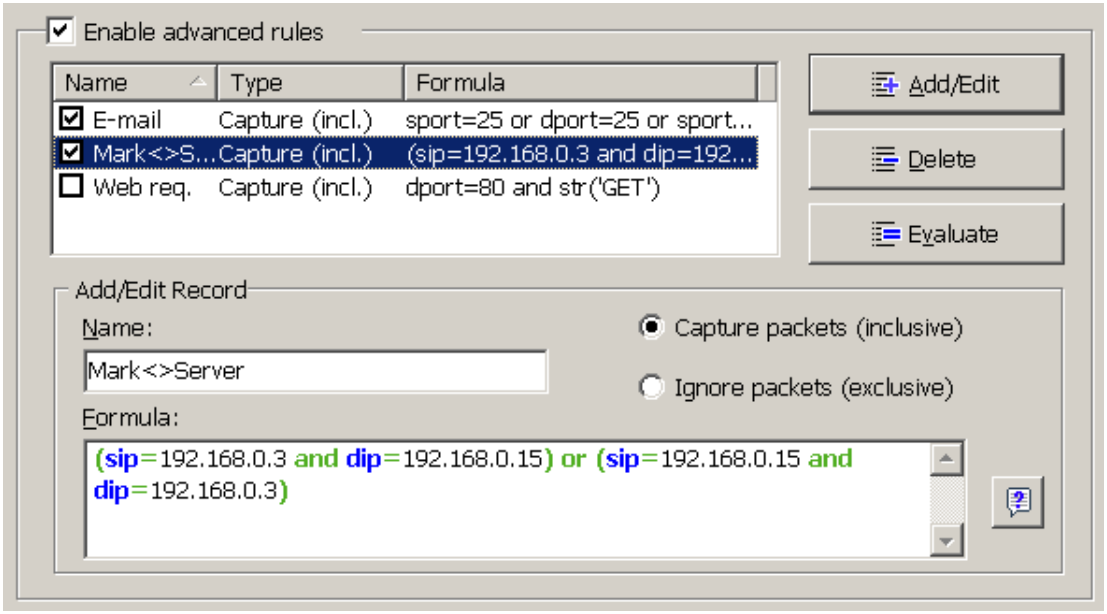
В этом примере показано, как собирать только пакеты, содержащие или текст "GET" или 01 02 03 04 шестнадцатеричные данные. При необходимости, установите флажок **Case sensitive** (С учётом регистра).

Advanced (Составные)

Составные правила являются мощным и гибким механизмом создания фильтров с помощью Булевой логики.

Составные правила

Составные правила являются мощным и гибким механизмом создания фильтров с помощью Булевой логики. Синтаксис правил несложен для понимания.



Обзор

Чтобы создать новое правило, задайте ему имя в поле **Name**, выберите действие **(Capture(Сбор)/Ignore(Пропуск))**, в поле **Formula** задайте формулу, пользуясь синтаксисом, описанным ниже, и нажмите **Add(Добавить)/Edit(Редактировать)**. Новое правило будет добавлено и немедленно активизировано. Неограниченное количество правил может быть задано, но активизированы только те из них, которые помечены галочкой в колонке имён. Любое правило можно включить/выключить, воздействуя на соответствующий флажок, или совсем удалить с помощью кнопки **Delete**. Если включены сразу несколько правил, их совместное ограничение можно оценить, нажав на кнопку **Evaluate**. Обратите внимание, что отдельные правила объединяются в составное логическим оператором ИЛИ.

Можно пользоваться составными правилами совместно с обычными, описанными в предыдущей главе, однако, если Вы владеете Булевой логикой, рекомендуем пользоваться в основном составными, так как они более гибки. Обычные правила объединяются с составными по логическому оператору И.

Описание синтаксиса

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

etherproto – Протокол Ethernet (13й и 14й 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 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), 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.

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 **View(Просмотр) => Port Reference(Список портов)**.

dport – Порт-получатель пакетов TCP или UDP.

flag – Флаги 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), and U (URG), или ключевое слово has, означающее, что флаг содержит определённое значение. Например: flag=0x18, flag=SA, flag has F.

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

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

hex - Содержимое пакета. Используйте эту функцию, чтобы задать условие, что пакет должен содержать определённую последовательность байтов. Функция имеет два аргумента: образец поиска и местоположение. Первый аргумент – шестнадцатеричная величина, например, 0x4500. Второй аргумент – число, показывающее смешение в пакете. Счёт начинается с нуля – первый байт пакета надо искать, задавая смещение равное 0. Чтобы искать во всём пакете, задайте смещение равным –1. Второй аргумент необязателен, по умолчанию имеет значение –1 (искать во всём пакете). Пример: hex(0x04500, 14) , hex(0x4500, 0x0E), hex (0x010101).

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

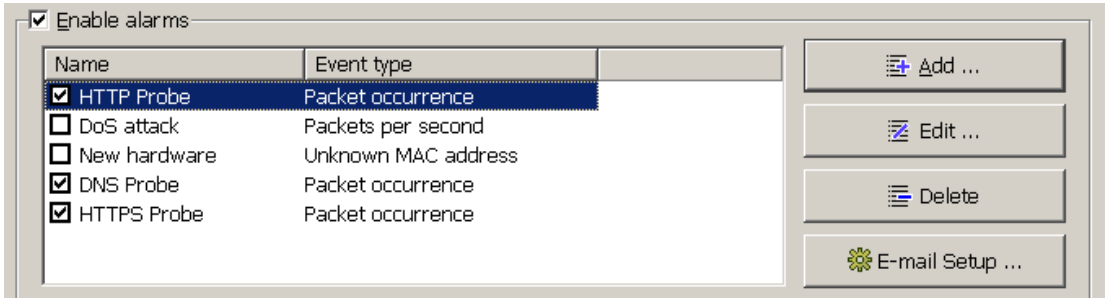
Ниже приведены несколько примеров, поясняющих синтаксис правил. К каждому правилу, напечатанному красным, даны комментарии, отделяемые двойной косой чертой.

- 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, при чём IP адреса получателей находятся в сегменте 192.168.1.0/255.255.255.240, и имеющие TCP флаг PSH ACK.
- Hex(0x0203, 89) and (dir<>in) // Захватывать пакеты, содержащие 0x0203 в смещении 89, при этом, направление пакета не "входящий".

Предупреждения

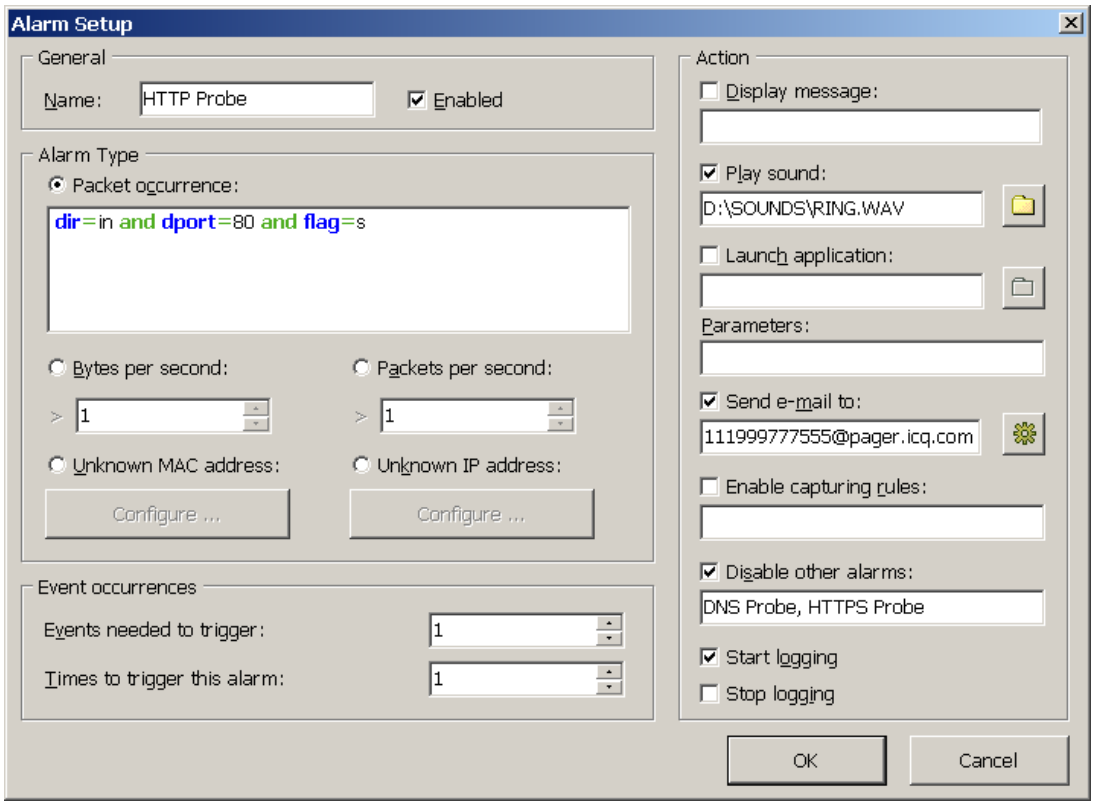
В этой закладке можно создавать систему сообщений о существенных событиях в сети, таких как появление подозрительных пакетов, повышение сетевой нагрузки, нештатные адреса и так далее… Предупреждения могут очень помочь в случае если Вам надо отслеживать такие события в сети, как сканирование портов, появление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

Управление предупреждениями осуществляется с помощью показанного ниже списка:



Каждая строка описывает отдельное предупреждение, а флажок рядом с названием – отмечает состояние включено/выключено. Когда предупреждение срабатывает, флажок сбрасывается. Чтобы вторично активизировать ожидание сработавшего предупреждения, установите флажок возле его имени. Для отключения всех предупреждений – сбросьте флажок **Enable alarms(Включить предупреждения)**. Чтобы добавить новое или редактировать/удалить имеющееся предупреждение, воспользуйтесь кнопками справа от списка. Если планируется использовать почтовое извещение, нажав кнопку **E-mail Setup(Настройка e-mail)** введите настройки SMTP сервера (см. ниже).

Ниже показано окно настройки предупреждений:



В поле **Name(Имя)** описывается назначение текущей функции предупреждения. Если вы хотите, чтобы предупреждение было активировано по окончанию его настройки/создания, установите флажок **Enabled**. Этот флажок совпадает со значением в соответствующей колонкой в списке предупреждений. В поле **Alarm Type** можно выбрать один из пяти типов событий:

- **Packet occurrence(Обнаружение пакета)**: Это предупреждение сработает при обнаружении пакета, соответствующего указанной формуле. Синтаксис формул совпадает с синтаксисом составных правил и подробно описан в главе Составные правила.

- **Bytes per second(Байты в секунду)**: Это предупреждение сработает при превышении указанного уровня загрузки сети. Значение надо указывать в байтах, например, если требуется срабатывание при превышении уровня трафика в 1Mbyte/сек, укажите порог, равный 1000000.

- **Packets per second(Пакеты в секунду)**: Это предупреждение сработает при превышении указанного уровня частоты передачи пакетов.

- **Unknown MAC address(Неизвестный MAC)**: Это предупреждение сработает при обнаружении программой пакетов с неизвестными MAC-адресами отправителя и/или получателя. Кнопка **Configure** позволяет создать список известных адресов. Это предупреждение можно использовать для обнаружения подключений нового или несанкционированного оборудования в сеть.

- **Unknown IP address(Неизвестный IP)**: Это предупреждение сработает при обнаружении программой пакетов с неизвестными IP-адресами отправителя и/или получателя. Кнопка **Configure** позволяет создать список известных адресов. Это предупреждение можно использовать для обнаружения несанкционированных подключений через корпоративный брандмауэр.

Поле **Events needed to trigger(Порог чувствительности)** устанавливает количество событий, которое должно произойти, чтобы сработало предупреждение. Например, если установить уровень равный 3, предупреждение не сработает, пока событие не произойдёт трижды. При редактировании уже существующего предупреждения происходит обнуление внутреннего счётчика событий.

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

Поле **Action(Действия)** выбирает исполняемое при срабатывании предупреждения действие. Доступны следующие варианты:

- **Display message(Показать сообщение)**: Появляется окно с предварительно записанным сообщением.

- **Play sound(Звуковой сигнал)**: Проигрывает указанный WAV-файл.

- **Launch application(Запустить программу)**: Запускает указанный EXE- или COM-файл. В поле **Parameters(Параметры)** можно задать необходимые запускаемому приложению параметры командной строки.

- **Send e-mail to(Отправить e-mail...)**: Отправляет e-mail по указанному адресу. ОБЯЗАТЕЛЬНО укажите SMTP сервер, которым должен пользоваться CommView при отправке. Для этого нажмите кнопку **E-mail Setup(Настройка почты)**, задайте установки SMTP сервера и отправьте пробное письмо. Удобно настроить отправку сообщений на пейджер, в виде SMS на мобильный телефон или же в программы персональной коммуникации. 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 узнайте у своего сотового оператора.

- **Enable capturing rules(Включить правила сбора)**: Включает Составные правила; укажите названия правил, если требуется несколько правил, перечислите их названия через запятую или точку_с_запятой.

- **Disable other alarms(Выключить другие предупреждения)**: Выключает ненужные предупреждения; укажите название предупреждения, если требуется отключить несколько предупреждений, перечислите их названия через запятую или точку_с_запятой.

- **Start logging(Начать ведение log-файлов)**: Включает автосохранение (смотри главу Ведение Log-файлов); CommView начнёт запись захваченных пакетов на диск.

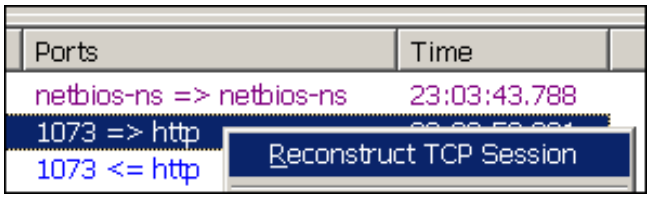
- **Stop logging(Прекратить ведение log-файлов)**: Выключает автосохранение.

Нажав **OK** вы сохраните настройки и закроете данный диалог.

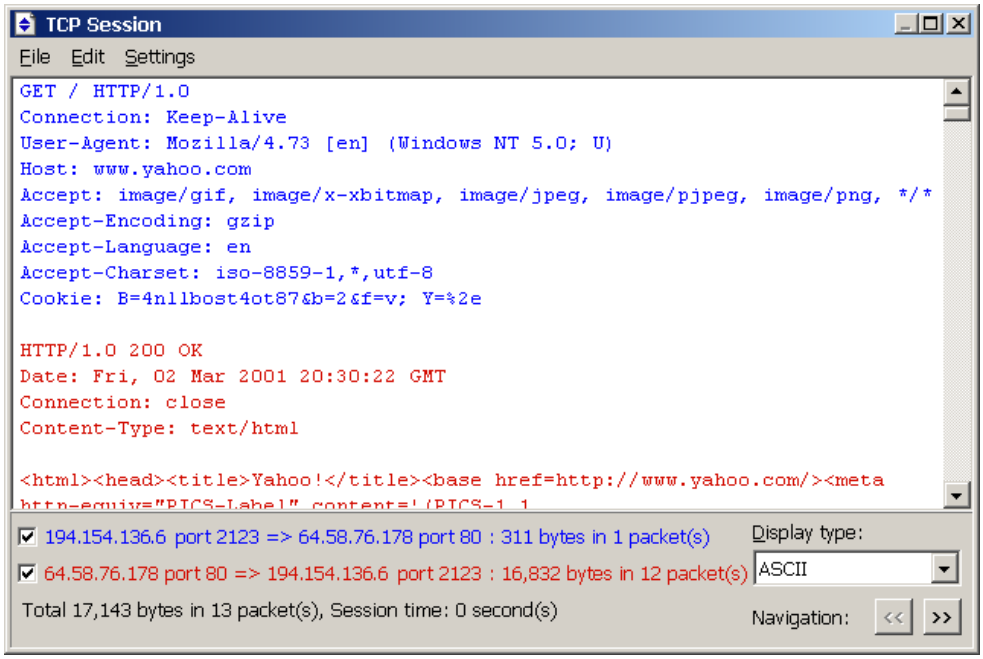
Все события, и относящиеся к ним действия, перечисляются в окне **Event Log**, находящемся под списком предупреждений.

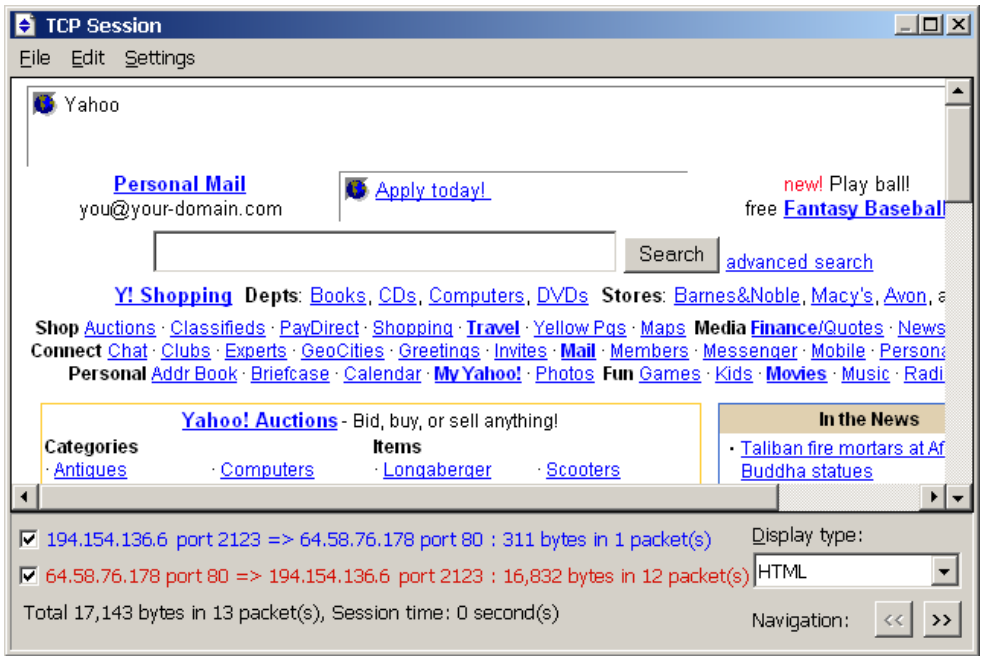
Реконструкция TCP сессий

С помощью этой утилиты можно просмотреть процесс общения двух хостов по TCP. Чтобы восстановить TCP сессию, необходимо сначала выбрать пакет TCP в закладке **Packets(Пакеты)**. Если Вы хотите восстановить сессию целиком, целесообразно выбрать первый пакет этой сессии, иначе реконструкция может начаться с середины. Найдя и выбрав нужный пакет, щёлкните правой кнопкой мышки на нём, в появившемся меню выберите **Reconstruct TCP Session(Реконструкция TCP сессии)**, как показано здесь:



Эта утилита нагляднее всего работает на текстовых протоколах - POP3, Telnet, или HTTP. Возможна также и реконструкция процесса пересылки, например "зазипованного" архива, но на восстановление нескольких мегабайтов данных CommView потребуется слишком много времени, да и в большинстве случаев полученная информация будет совершенно бесполезна. Ниже показан пример реконструкции HTTP сессии в режимах ASCII и HTML соответственно:





Можно игнорировать данные, следовавшие в выбранном направлении, установив/сняв флажок в нижней части окна. Для удобства входящие и исходящие данные помечены разным цветом. Если Вы хотите изменить цвет отображения, выберите **Settings(Установки) =>Colors(Цвет)** и воспользуйтесь палитрой. Можно включить или выключить перенос слов пунктом **Word Wrap(Перенос слов)** в меню **Settings(Установки)**.

Выпадающее меню **Display type (Тип отображения)** позволяет выбрать **ASCII (обычный текст)**, **HEX (шестнадцатеричные данные), HTML (web-документы)** и **EBCDIC (IBM mainframes' data encoding)** режимы просмотра. Данные в режиме HTML могут выглядеть несколько иначе, чем при просмотре настоящим браузером (Вы не увидите графические объекты и т.п.), однако вполне можно понять, как выглядела данная страница на самом деле.

Кнопки перемещения Navigation позволяют перескакивать к следующей или предыдущей сессиям, имеющимся в буфере. Если в буфере несколько сессий, рекомендуется начинать реконструкцию с самой первой, так как кнопка возврата **[<<]** не может перейти на сессию раньше той, с которой началась реконструкция.

Полученные данные Вы можете записать на диск в двоичном виде, в текстовом или RTF формате, выбрав **File(Файл) =>Save As...(Сохранить как...)**. Кроме того, нажав **Edit(Редактировать)** => **Find...(Найти...)** можно искать строку в пределах сессии.

Статистика и отчёты

Выбрав в меню **View(Просмотр) =>Statistics(Статистика)**, можно ознакомиться с такими параметрами сетевой статистики сегмента LAN или Вашего компьютера, как количество пакетов в секунду, байтов в секунду, или распределение протоколов и суб-протоколов. Дважды щёлкнув по графам, их можно скопировать в буфер обмена. Для удобства просмотра круговых графов, их можно вращать с помощью двух кнопок в правом нижнем углу.

Данные каждой закладки можно сохранить или в формате bitmap или в текстовом файле с разделителем "точка_с_запятой". Для этого воспользуйтесь контекстным меню или просто перетащите объект мышкой. Закладка **Report (Отчёт)** создаёт автоматические отчёты в HTML или текстовом формате с разделителем "точка_с_запятой".

Сетевая статистика может строиться на базе всех пакетов, проходящих через адаптер, или с учётом текущих правил на захват пакетов. Воспользуйтесь флажком **Apply current rules (С учётом ограничений)**, чтобы последние повлияли на построение статистической картины.

General (Общая)
Гистограммы "Пакеты в секунду" и "Байты в секунду", индикатор использования пропускной способности (удельный трафик, делённый на номинальную скорость сетевого адаптера или модемного соединения), а также общее количество пакетов и байтов.

IP Protocols (IP Протоколы)
Распределение основных IP протоколов: TCP, UDP и ICMP. Выпадающее меню **Chart by (Выстроить по...)** переключает методы подсчёта: по количеству пакетов или по количеству байтов.

IP Sub-protocols (Субпротоколы IP)
Распределение основных IP субпротоколов уровня приложений: HTTP, FTP, POP3, SMTP, Telnet, NNTP, NetBIOS, HTTPS, и DNS. Чтобы добавить собственные протоколы, нажмите кнопку **Customize (Подстройка)**. Можно доопределить до восьми протоколов, введя название, IP тип протокола (TCP/UDP) и номер порта. Выпадающее меню **Chart by (Выстроить по...)** переключает методы подсчёта: по количеству пакетов или по количеству байтов.

Sizes (Размер пакетов)
Распределение размера пакетов.

LAN Hosts (MAC)
Список активных LAN хостов по адресам MAC, со статистикой передачи данных. MAC адресам можно присвоить имена (алиасы).

LAN Hosts (IP)
Список активных LAN хостов по IP адресам, со статистикой передачи данных. Поскольку IP пакеты, накапливаемые программой, могут приходить с неограниченного числа IP адресов (и внутрисетевых и внешних), по умолчанию, данная закладка не отображает никакой статистики. Чтобы получить её, необходимо задать диапазон IP адресов в Add/Set Ranges. Обычно, диапазон должен принадлежать Вашей сети. Можно задать несколько диапазонов, но общее число IP адресов не может превышать 1000. Чтобы удалить диапазон, щёлкните правой кнопкой мыши по нему и выберите соответствующую команду **(Delete Range – удалить выбранный, Delete All Ranges – удалить все)**. IP адресам можно присвоить имена (алиасы).

Errors (Ошибки)
Отображает сведения об ошибках Ethernet'а, получаемые непосредственно из адаптера. В их числе:

Rx CRS Errors
Количество кадров, принятых с ошибками контрольной суммы (CRC) или проверки последовательности кадров (FCS).
Rx Alignment Errors
Количество кадров, принятых с ошибками выравнивания.
Rx Overrun
Количество кадров, не принятых из-за ошибок переполнения адаптера.
Tx One Collision
Количество кадров, переданных успешно после единственной коллизии.
Tx More Collisions
Количество кадров, переданных успешно после нескольких коллизий.
Tx Deferred
Количество кадров, переданных успешно после того, как адаптер отложил передачу хотя бы один раз.
Tx Max Collisions
Количество кадров, не переданных из-за многочисленных коллизий.
Tx Underrun
Количество кадров, не переданных из-за несвоевременной загрузки адаптера данными.
Tx Heartbeat Failure
Количество кадров, переданных успешно, без обнаружения коллизий.
Tx Times CRS Lost
Количество пропаданий сигнала контрольной суммы во время передачи пакета.
Tx Late Collisions
Количество коллизий, обнаруженных за пределами окна.
Rx Frames w/Errors
Количество кадров, принятых адаптером, но не переданных протоколам из-за ошибок.

Rx Frames w/o Errors
Количество кадров, успешно принятых адаптером и переданных соответствующим протоколам.
Tx Frames w/Errors
Количество кадров, не переданных по каким-либо причинам.
Tx Frames w/o Errors
Количество успешно переданных кадров.

Замечание:

- Dial-up адаптеры не поддерживаются, только аппаратные Ethernet адаптеры.
- Не все адаптеры способны сообщать все эти значения, зависит от изготовителя.
- В отличии от остальных данных окна **Statistics (Статистика)**, счётчики закладки **Errors (Ошибки)** не сбрасываются при нажатии кнопки **Reset (Сброс)**. Счётчики инициализируются при каждой перезагрузке компьютера.

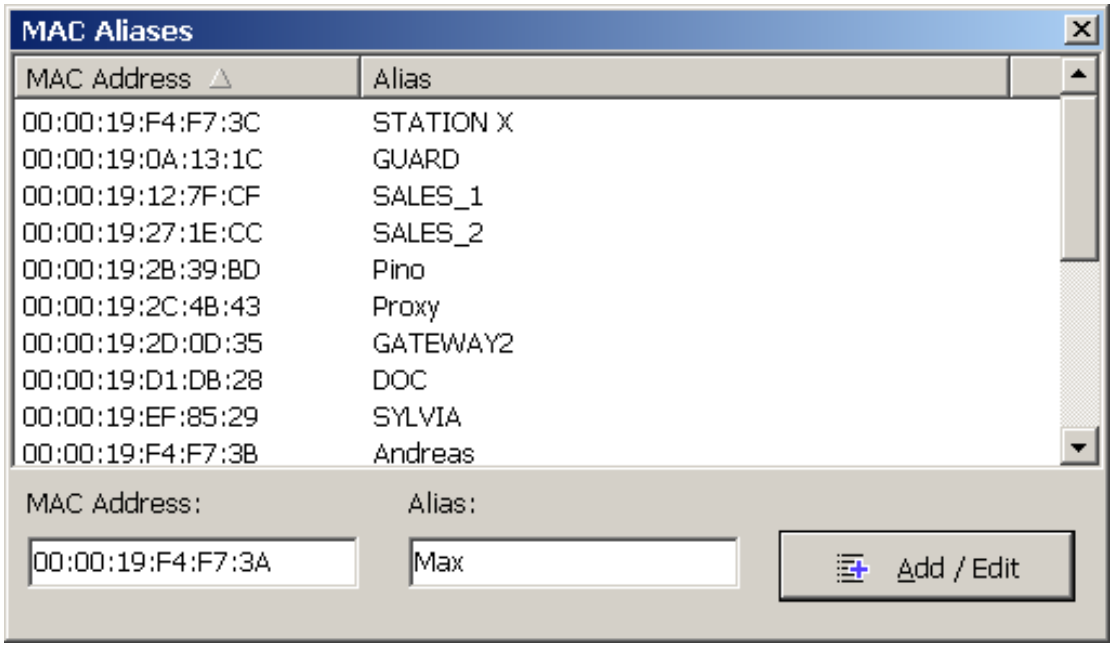
Данная закладка недоступна под Windows 95.

Report (Отчёт)
Закладка позволяет настроить автоматически создаваемые отчёты в форматах HTML или текстовом, с разделителем "точка_с_запятой".

Использование имён (алиасов)

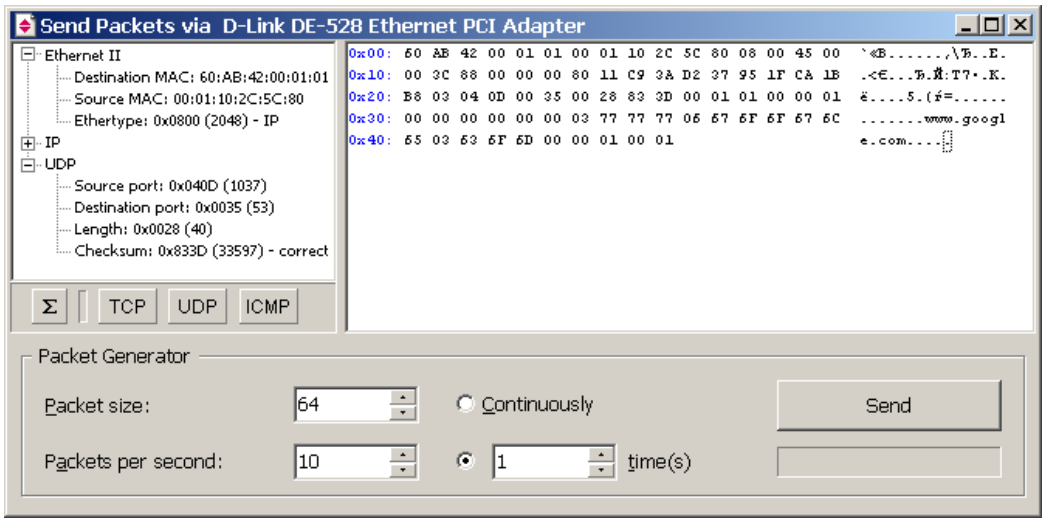
CommView может подставлять вместо MAC или IP адресов более "осмысленные" имена при отображении пакетов в закладках **Packets (Пакеты)** и **Statistics (Статистика)**. Например, 00:00:19:2D:0D:35 станет GATEWAY2, а ns1.earthlink.com превратится в MyDNS.

Чтобы создать имя (алиас) для MAC адреса, щёлкните правой кнопкой мышки на пакете и выберите в контекстном меню **Create Alias Using Source MAC (Дать имя MAC источника)** или **Using Destination MAC (Дать имя MAC получателя).** Появится окно, с уже заполненным полем MAC адреса, теперь можно ввести подходящее имя. Другой способ: выберите в меню **Tools(Утилиты) =>Aliases(Имена)** и заполните поля вручную. Удалить имя или стереть весь список имён можно щёлкнув правой кнопкой мышки в окне **Aliases** и выбрав **Delete Record (Удалить запись)** или **Clear All (Стереть всё)**. Точно так же происходит работа над IP адресами. Если новая запись IP-имени создаётся щелчком правой кнопки мыши по пакету, поле имени автоматически заполняется именем хоста (если оно доступно), и его можно редактировать.



Генератор пакетов

Эта утилита позволяет создавать и передавать пакеты через сетевой адаптер. Утилита доступна только под Windows NT, Windows 2000 и Windows XP. Выберите в меню **View(Просмотр) =>Packet Generator(Генератор пакетов)**, или выбрав пакет в закладке **Packets(Пакеты)**, щёлкните правой кнопкой мышки на нём, а затем выберите команду **Send Packet(Передать пакет)**.



Генератор пакетов позволяет задавать содержимое пакета любого типа и декодировать его в левом окне по мере редактирования. Для пакетов IP, TCP, UDP и ICMP контрольная сумма автоматически обновляется при нажатии на кнопку "сигма". Воспользуйтесь кнопками **TCP**, **UDP** и **ICMP** для быстрой загрузки готовых шаблонов пакетов. В шаблонах TCP, UDP и ICMP пакетов вам потребуется изменить на нужные значения такие поля, как MAC и IP адреса, номера портов, SEQ и ACK номера, и так далее. Можно создать собственные шаблоны, загрузив файлы в формате CCF в директорию программы. Имена файлов шаблонов должны быть "template_tcp.ccf", "template_udp.ccf" и "template_icmp.ccf". Если в директории CommView есть хоть один такой файл, нажатие на кнопку шаблонов будет загружать из него соответствующий пакет. Хотя в файле-шаблоне может быть и несколько пакетов, CommView загрузит только первый.

Ниже приведены доступные параметры передачи:

Packet Size – изменяет размер пакета.
Packets Per Second – устанавливает частоту передачи пакетов. Будьте осторожны, чтобы не превысить пропускную способность соединения. Попытка посылать 5000 раз в секунду пакеты длиной в 1000 байтов превысит возможности 10Mbit-ного сетевого адаптера.
Continuously – (Непрерывно) – включает режим непрерывной передачи, пока не нажмёте **Stop**.
Time(s) – (Количество) – задаёт число отправок пакета в сеть.
Send/Stop – (Старт/Стоп) – включает/выключает режим передачи пакета.

Работа с несколькими пакетами одновременно

Генератор пакетов может передавать несколько пакетов одновременно. Выберите нужные Вам пакеты из списка и, правым щелчком мышки, 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 отредактированного пакета

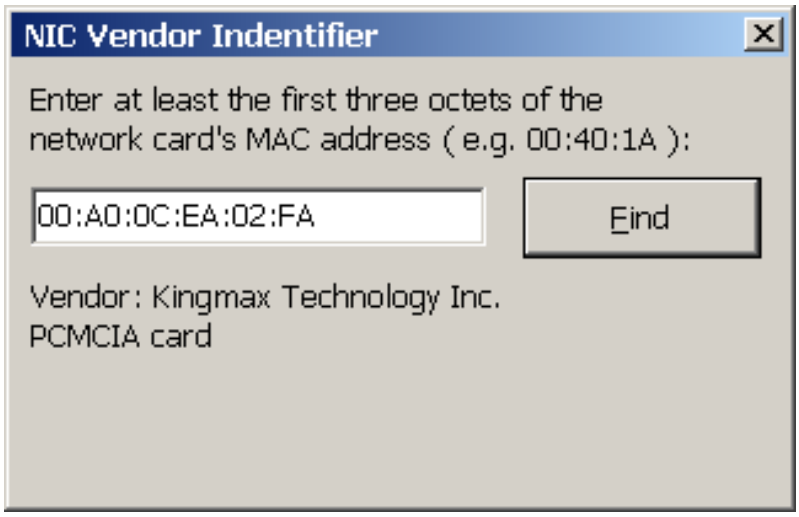
Если Вы отредактировали пакет и хотите его сохранить, просто перетащите мышкой дерево декодера на десктоп или в любую папку. Будет создан новый файл в формате CCF с именем PACKET.CCF.

ВНИМАНИЕ:

1. Не пользуйтесь этой утилитой для баловства! Передача пакетов в сеть может привести к непредсказуемым результатам. Используйте её только если Вы знаете, чего хотите добиться.
2. Утилита не работает с RAS/Dial-up адаптером под Windows NT.
3. Кроме Вашего, в сети должен быть хотя бы ещё один работающий компьютер, иначе в передаче пакетов возникнут значительные задержки.

Определение изготовителя сетевого адаптера (NIC)

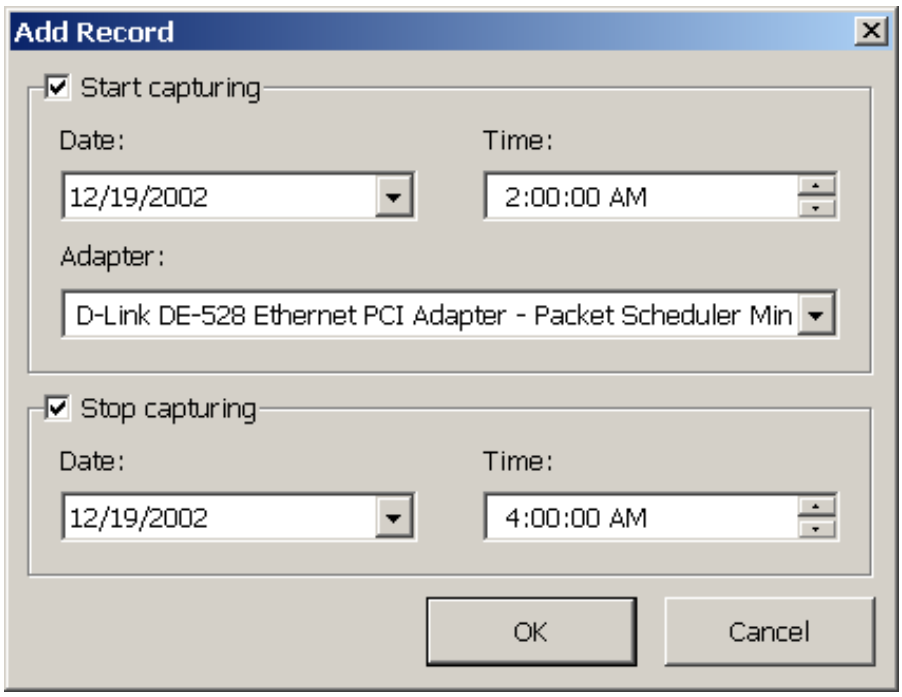
Первые 24 бита MAC адреса сетевого адаптера однозначно указывают фирму-изготовителя. Этот 24-битовый номер называется **OUI ->"Organizationally Unique Identifier" (Организационно-уникальный Идентификатор)**. Чтобы узнать фирму, выберите **Tools(Утилиты) =>NIC Vendor Identifier(Определитель фирмы)**, введите MAC адрес и нажмите **Find(Поиск)**.



Список фирм находится в файле MACS.TXT, расположенном в программной папке CommView. Файл можно редактировать, чтобы добавлять/изменять информацию.

Планировщик

Утилита планировщика позволяет управлять сбором пакетов по расписанию. Этой утилитой удобно пользоваться, когда необходимо начинать/прекращать сбор пакетов в ваше отсутствие, например, в выходные или ночью. Чтобы добавить новое задание в расписание работы, зайдите в **Tools** => **Scheduler**, и нажмите кнопку **Add(Добавить)**.



В поле **Start capturing(Начать сбор)** укажите дату/время, когда CommView должен начать захват. В выпадающем списке **Adapter(Адаптер)** выберите требуемый адаптер. В поле **Stop capturing(Остановить сбор)** укажите момент окончания захвата пакетов. Заполнять оба поля **Start capturing** и **Stop capturing** не обязательно. Если вы заполните только первое поле, начавшийся захват будет идти, пока его не остановят вручную. Если вы заполните только второе поле, начать захват придётся вручную, а прекратится он в указанное время.

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

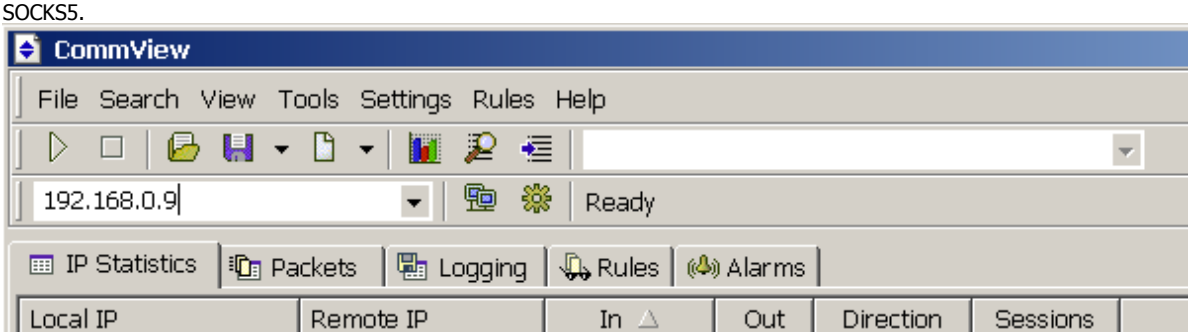
Внимание: CommView выполняет расписание ТОЛЬКО если он запущен.

Мониторинг на расстоянии

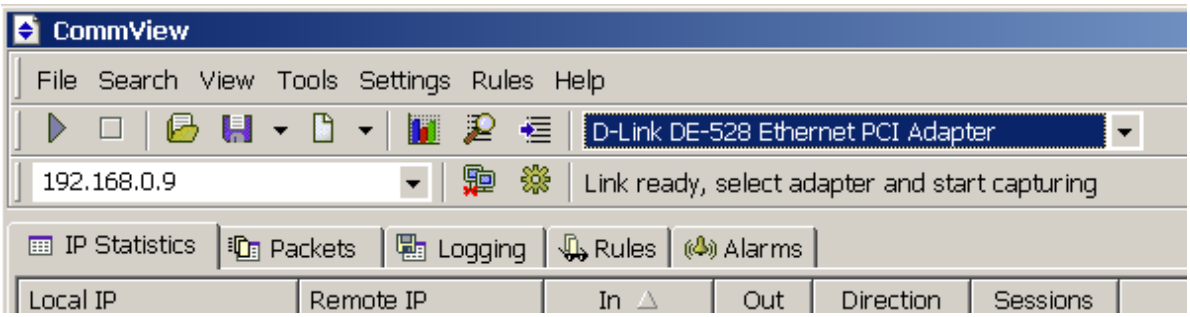
Программа **CommView Remote Agent**, являясь дополнительным продуктом, позволяет пользователям **CommView** наблюдать трафик в удалённых сетях. Необходимо установить **Remote Agent** на компьютер в интересующей Вас сети и включить в **CommView** управление сервисом, предоставляемым Remote Agent'ом. Подключившись и введя пароль доступа, можно начинать сбор сетевой информации, как если бы Ваш компьютер непосредственно находился в той сети.

Внимание: Данная глава описывает использование CommView для подключения к Remote Agent и наблюдение трафика на расстоянии. Подробное описание установки и настройки программы Remote Agent находится в документации, поставляемой вместе с ней. Внимательно ознакомьтесь с описанием прежде чем использовать программу. CommView Remote Agent можно скачать здесь.

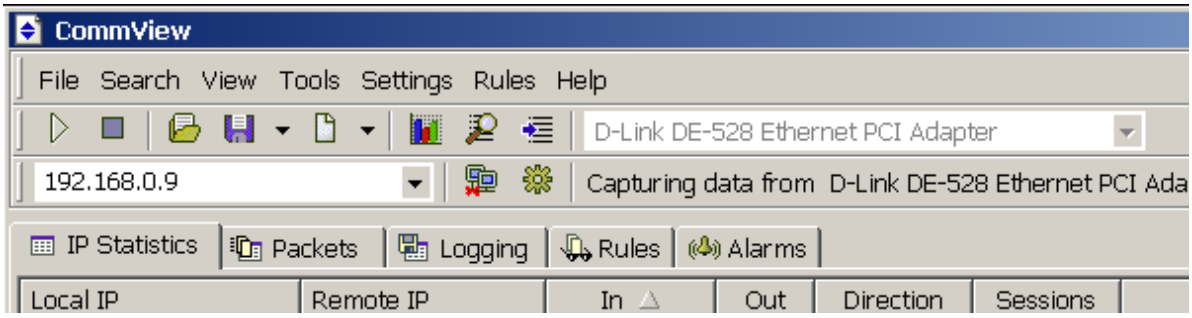
Для включения режима работы на расстоянии, выберите в меню File(Файл) =>Remote Monitoring Mode(Режим работы на расстоянии). Под основной панелью инструментов CommView появится дополнительное поле. В окне адреса укажите IP адрес компьютера, на котором запущен CommView Remote Agent, нажмите кнопку Connect(Установить связь). Если Вы работаете через брандмауэр или прокси-сервер, а также, если в Remote Agent выбран нестандартный номер порта, нажав кнопку Network Settings(Сетевые настройки), укажите используемый порт и/или задайте параметры прокси-сервера SOCKS5.



В появившемся окне введите пароль доступа к Remote Agent, если пароль указан правильно – будет установлено соединение. Об этом будет свидетельствовать сообщение Link Ready(Связь установлена), а в окне выбора адаптеров появится список имеющихся на удалённом компьютере сетевых адаптеров.



Теперь необходимо установить фильтрацию пакетов в закладке **Rules(Правила)**. Важно сконфигурировать фильтры так, чтобы трафик между Remote Agent'ом и CommView не превысил пропускную способность линии связи, иначе возникнут заметные задержки и запаздывания. Все не интересующие Вас пакеты должны игнорироваться, подробнее о настройке фильтров смотрите здесь. Окончив настройку, выберите адаптер из списка и нажмите кнопку **Start Capture (Начать сбор)**.



CommView начнёт сбор трафика удалённого компьютера, как если бы дело происходило в Вашем сегменте локальной сети. Для окончания мониторинга нажмите кнопку **Stop Capture (Прекратить сбор)**. Можно или выбрать другой адаптер или отключиться от Remote Agent'а, нажав кнопку **Disconnect(Разорвать связь)**. Снимите флажок в меню **File(Файл) =>Remote Monitoring Mode(Режим работы на расстоянии)**, и, CommView вернётся в местный режим работы.

Установка опций

Выбрав в меню пункт **Settings(Настройки)**, можно менять настройки программы.

Fonts (Шрифты)

Используйте это меню для установки шрифтов пользовательского интерфейса и текста пакетов. Чтобы изменить цвет текста пакетов, используйте меню **Options (Опции)**, см. ниже.

Options (Опции)

General (Общие)

Auto-start capturing – установите этот флажок, если Вы хотите чтобы CommView начал перехват пакетов сразу же после запуска программы. Для систем с несколькими устройствами, следует выбрать из списка устройство, которое будет при этом использоваться.

Network (Сеть)

Disable DNS resolving – установите этот флажок, если Вы не хотите, чтобы CommView делал обратный DNS поиск IP адресов. Если флажок установлен, то колонка **Hostname (Имя хоста)** закладки **IP Statistics (IP Статистика)** будет пустой.

Convert numeric port values to service names – установите этот флажок, 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 числовые значения, в названия сервисов используя файл SERVICES инсталлированный с Windows. В зависимости от версии Windows, файл SERVICES может находиться в разных каталогах: в Windows 95/98/Me он в каталоге \Windows, а в Windows NT/2000/XP - в каталоге \Winnt\system32\drivers\etc. Вы можете вручную редактировать этот файл, если Вы хотите добавить другие названия портов/сервисов.

Convert MAC addresses to aliases – заменять MAC адреса пакетов в закладке **Packets (Пакеты)**. Создавать алиасы можно командой меню **Settings(Установки) =>MAC Aliases(MAC имена)**.

Convert IP addresses to aliases – заменять IP адреса пакетов в закладках **Packets (Пакеты)** и **Statistics (Статистика)**. Создавать алиасы можно командой меню **Settings(Установки) =>IP Aliases(IP имена)**.

Convert IP addresses to hostnames in the "Packets" tab – установите этот флажок, если Вы хотите, чтобы CommView отображал имена хостов вместо их IP адресов в закладке **Packets(Пакеты)**. Если этот флажок установлен, CommView сперва попробует найти алиас данному адресу. Если алиаса нет, или не установлен флажок (**Convert IP addresses to aliases**), CommView запросит внутренний кэш DNS. Если запрос не будет удовлетворён и имя не будет найдено, IP адрес будет отображён в цифровом виде.

Use non-promiscuous mode – по умолчанию, CommView переводит сетевой адаптер во "всеядный" режим (promiscuous mode), что позволяет программе видеть весь трафик в локальном сегменте сети. Установка этого флажка переводит сетевой адаптер в нормальный режим аппаратной фильтрации пакетов. Воспользуйтесь им в случае, если дисциплина сетевой безопасности Вашей компании не разрешает тотальный мониторинг; если Вы хотите снизить загрузку процессора при исследованиях только собственных входящих/исходящих пакетов, отфильтровывая все транзитные.

Memory Usage (Использование памяти)

Display (Отображение)

Maximum packets in buffer – 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 компьютера использует программа. Если Вы хотите иметь доступ к большему количеству пакетов, рекомендуется использовать автосохранение - это позволит сохранить в файле все пакеты. Подробности в главе Ведение Log-файлов

Maximum IP statistics lines - устанавливает количество строк в закладке **IP Statistics (IP Статистика)**. Когда количество соединений превышает указанный предел, самые старые соединения в списке удаляются из него.

Driver Buffer (Windows NT/2000/XP only) - устанавливает размер буфера драйвера (только под Windows NT/2000/XP). Эта установка влияет на производительность программы: чем больше памяти выделено, тем меньше программа теряет пакетов. При низком трафике локальной сети или dial-up соединении размер буфера некритичен. При высоком трафике локальной сети, может понадобиться увеличить размер буфера, если программа теряет пакеты. Используя команду меню **File(Файл) =>Performance Data(Сведения о производительности)**, в процессе перехвата пакетов можно проверить количество потерянных пакетов,.

IP Statistics (IP Статистика)

Display Logic – выбирает раскладку отображения IP Statistics (IP Статистика). Рекомендуем пользоваться режимом Smart logic.

Define Local IP Addresses – указание IP адресов, как местных. Этим окном рекомендуется пользоваться при наблюдении трафика с большим числом транзитных пакетов и наличии совокупности внешних и внутренних IP адресов. В этом случае CommView не может определить, какие IP адреса следует считать локальными, и может перепутывать их в колонках Локальных и Удалённых IP адресов. В этом окне можно явно указать локальные сетевые адреса и маски подсети, чтобы окно IP Statistics (IP Статистика) работало правильно. Требуется, чтобы был включен режим отображения Smart logic.

Colors (Цвета)

Packet color – устанавливает цвет отображения пакетов в закладке **Packets (Пакеты)** в зависимости от направления (входящий, исходящий, транзитный). Чтобы изменить цвет, выберите направление пакета из списка и нажмите на цветной прямоугольник.

Colorize Packet Headers – установите этот флажок, если хотите, чтобы CommView раскрашивал содержимое пакетов. Если флажок установлен, программа отображает первые четыре уровня пакета, используя различные цвета. Чтобы изменить цвет, выберите тип заголовка, для которого Вы хотите изменить цвет и нажмите на цветной прямоугольник.

Formula syntax highlighting – задаёт цвета отображения ключевых слов в формулах составных правил.

Selected byte sequence color – задаёт цвета отображения последовательности байтов, выбранных в дереве декодера. Например, если выбрать узел "TCP" в декодере, соответствующая часть пакета будет выделена данным цветом.

Decoding (Декодирование)

Always fully expand all nodes in the decoder window – установите этот флажок, если Вы хотите, чтобы при выборе пакета все узлы в окне декодера автоматически разворачивались.

Decode up to the first level only in ASCII export – этот флажок устанавливает формат, используемый при экспорте лог-файла или отдельного пакета в текстовом виде с декодированием. Если флаг установлен, экспортируются только узлы верхнего уровня. Например, при снятом флаге, экспорт TCP/IP пакета произойдёт с записью всех узлов "Тип сервиса". При установленном флаге – эти узлы не экспортируются. Таким образом, можно получать менее детальные, но более короткие файлы.

Ignore incorrect checksums when reconstructing TCP sessions – эта опция воздействует на то, как CommView воспринимает повреждённые TCP/IP пакеты при реконструкции TCP сессии. По умолчанию, эта опция включена, и пакеты со сбойной контрольной суммой не отбрасываются при реконструкции. Если опцию выключить, пакеты со сбойной контрольной суммой будут отброшены и не попадут в окно реконструкции. Вниманию пользователей сетевых адаптеров Gigabit: все Ваши исходящие пакеты будут содержать неправильную контрольную сумму, если на адаптере присутствует свойство/фича "checksum offload"(аппаратный подсчёт). Если Вы выключите эту опцию, Вы увидите только половину реконструированной TCP сессии.

Miscellaneous (Разное)

Hide from the taskbar on minimization - установите этот флажок, если не хотите видеть кнопку программы в панели задач Windows когда Вы минимизируете CommView. Если этот флажок установлен, используйте значок программы в панели уведомления для восстановления после минимизации.

Allow multiple application instances - установите этот флажок, если нужно запускать несколько копий программы для наблюдения за несколькими адаптерами одновременно. Не работает под Windows 95.

Prompt for confirmation when exiting the application – установите этот флажок, если хотите, чтобы программа запрашивала подтверждение при выходе из неё.

Auto-scroll packet data window - если этот флажок установлен, программа автоматически прокручивает текст в окне данных пакетов, (если только текст не помещается в окно). Это полезно, когда Вы хотите видеть содержимое большого пакета без ручного прокручивания окна.

Auto-sort new records in IP statistics - если этот флажок установлен, программа автоматически сортирует новые записи в закладке IP Statistics (IP Статистика) в соответствии с заданными правилами сортировки (например, в возрастающем порядке удалённых IP адресов).

Auto-scroll packet list to the last packet - если этот флажок установлен, программа автоматически прокручивает пакеты в списке закладки **Packets(Пакеты)** вниз, до последнего принятого.

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

Run on Windows startup - если этот флажок установлен, программа автоматически запускается при загрузке Windows.

Run minimized - если этот флажок установлен, программа запускается минимизированной, и главное окно не отображается, пока Вы не нажмёте на значок в панели уведомления или в панели задач.

Поиск пакета

Диалог **Search(Поиск) =>Find Packet(Найти пакет)** позволяет находить пакеты, содержащие определённый текст. Введите строку для поиска, выберите тип введенной информации **String (Строка)** или **Hex (Шестнадцатеричное значение)**, и нажмите **Find Next (Найти далее)**. Программа будет искать пакеты, которые соответствуют запросу и отображать их в закладке **Packets (Пакеты)**.

Можно ввести образец как строку, как IP адрес или шестнадцатеричное значение. Последний способ может быть использован, когда надо ввести непечатаемые символы: для этого введите их шестнадцатеричные коды, разделённые пробелом, например, AD 0A 02 78 04.

Установите флаг **Match Case (С учётом регистра)** для поиска с соблюдением регистра. Установите флаг **At offset (Со смещением)** для поиска строки, которая начинается с некоторого смещения. Смещение задаётся в шестнадцатеричном виде.

Справочник по портам

Это окно отображает список номеров портов и соответствующих названий сервисов. Эта справка создается по файлу SERVICES инсталлированного с Windows. В зависимости от Вашей версии Windows, файл SERVICES находится в различных каталогах: В Windows 95/98/Me он в каталоге \Windows, а в Windows NT/2000/XP в каталоге \Winnt\system32\drivers\etc. Вы можете вручную редактировать этот файл, если хотите добавить больше названий портов/сервисов. CommView читает этот файл при загрузке, поэтому Ваши изменения в файле будут отображены только после рестарта программы.

Устранение неполадок

ЧаВо (FAQ)

В этой главе Вы можете найти ответы на некоторые из наиболее Часто задаваемых Вопросов. Свежий FAQ всегда доступен на http://www.tamos.com/products/commview/faq.php

? : Может ли CommView быть использован для перехвата dial-up (RAS) трафика?
! : Да, под Windows 95/98/Me/NT/2000/XP.

? : При наблюдении dial-up соединения, я не вижу пакетов PPP во время установления связи (CHAP, LCP, и т.п.). Это нормально?
! : Пакеты PPP захватываются только под Windows 95/98/NT/ME, они не доступны CommView под Windows 2000/XP.

? : Что конкретно "видит" CommView, инсталлированный на компьютер, который подключен к локальной сети?
! : CommView переводит сетевой адаптер во "всеядный" режим, и тот может перехватывать весь трафик в локальном сегменте сети. Другими словами, он перехватывает и анализирует пакеты адресованные любому компьютеру сегмента, а не только к компьютеру, на котором запущена программа. Есть ограничения при использовании с Wireless Ethernet адаптером (CommView будет перехватывать только входящие и исходящие пакеты с Вашего компьютера, т.е. транзитные пакеты отображаться не будут), и при работе через switch (см. вопрос о switch ниже в FAQ) .

? : Я подключен к LAN через switch, и, когда я запускаю CommView, он ловит только пакеты, идущие к/от меня, я не вижу трафика других машин. Почему?
! : В отличие от hub-ов, switch препятствует подслушиванию. В такой ситуации CommView (как и любой другой анализатор) ограничен приёмом broadcast и multicast пакетов, а также трафика того компьютера, на котором он запущен. Однако, современные switch-и имеют функцию "port mirroring", что позволяет сконфигурировать их так, чтобы они перенаправляли трафик на некоторых или всех портах, на специальный мониторный порт. Это позволит увидеть трафик всего сегмента сети. Обратитесь к документации на Ваш switch. В документации разных производителей, данная функция называется по разному.

Производитель	**Наименование функции port mirroring в документации**	**Модели, имеющие данную функцию**
Cisco	Port spanning	Cisco Catalyst 1900 Series Switches Cisco Catalyst 6000 Family Switches
3COM	Roving analysis port (RAP)	3Com SuperStack 3 Switch 4400
Intel	Port mirroring	Intel Express 460T Intel Express 480T

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

? : Может ли CommView собирать данные на адаптере, которому не выделен IP адрес?
! : Да. Сетевой адаптер может быть даже не привязан ни к TCP/IP, ни к какому либо другому протоколу. При отладке сети, Вам может понадобиться подключить компьютер с CommView в свободный порт хаба. В этом случае Вам не обязательно знать, какие IP адреса свободны в данном сегменте, просто снимите привязку адаптера к протоколу TCP/IP и начните обычную работу. В Windows 2000/XP зайдите в Control Panel => Network Connections, щёлкните правой кнопкой на иконке соединения, выберите Properties, и снимите флажки с соответствующих протоколов. В Windows 9x зайдите в Control Panel => Network, выберите TCP/IP привязанный к сетевому адаптеру, щёлкните Remove(Удалить) и перезагрузитесь.

? : Я запустил программу и нажал "Start Capture", но пакеты не отображаются. Почему?
! : Возможны две причины: Вы выбрали неактивное сетевое устройство, или ошиблись, устанавливая правила перехвата. Попробуйте выключить правила и посмотрите, что происходит. В любом случае, даже когда они включены, строка состояния программы будет отображать общее количество пакетов, посмотрите туда прежде, чем паниковать.

? : Я заметил, что контрольные суммы исходящих пакетов IP/TCP/UDP сбойные. Почему?
! : Gigabit-овые сетевые адаптеры имеют способность, называемую TCP/UDP/IP "checksum offload", она позволяет адаптеру вычислять контрольную сумму аппаратно, разгружая от этой работы процессор. Так как CommView перехватывает пакеты до того, как они попадают в адаптер, он обнаруживает неверную контрольную сумму. Это совершенно нормально и затрагивает только процесс реконструкции TCP сессии И ТОЛЬКО ЕСЛИ выключена опция "Ignore incorrect checksums". (Подробнее смотрите здесь)

? : Работает ли CommView на многопроцессорных системах?
! : Да.

? : Я подключен к сети через cable/xDSL модем. Будет ли CommView работать с ним?

! : Если у модема интерфейс USB/Ethernet, и Вы можете подключить его к сетевому адаптеру Ethernet, CommView сможет наблюдать сетевой трафик. Если на модеме только USB интерфейс, остаётся попробовать…

? : Мой брандмауэр, когда я пользуюсь CommView, сообщает, что CommView "пытается получить доступ в Internet". Я знаю, что некоторые фирмы могут отслеживать действия пользователей, собирая информацию, посылаемую их программами на сайт фирмы через Internet. Зачем CommView пытается получить доступ в Internet?
! : Брандмауэр (firewall) реагирует на попытки преобразовать IP адрес в имя хоста. Так как CommView должен послать DNS запрос на DNS сервер, срабатывает тревога. Можно выключить данный сервис (**Settings => Options => Disable DNS resolving**), но в этом случае, в закладке **IP Statistics(IP Статистика)** не будут показаны имена хостов. DNS запросы - единственный тип соединений, который может установить CommView. Никакой другой (тайной) сетевой активности нет. Мы не продаём Троянов (spyware).

? : В Windows 2000/XP я регистрируюсь, как пользователь без прав администратора. Чтобы пользоваться CommView, надо ли мне каждый раз выходить и перерегистрироваться администратором?
! : Нет, откройте папку с CommView, удерживая нажатой клавишу Shift, щелкните правой кнопкой мышки на CV.exe и выберите в меню пункт "Run As". Введите учётную запись администратора, нажмите OK, и программа запустится.

? : У меня Windows NT, и я вижу несколько "Remote Access WAN Wrapper" в списке устройств. Который мне выбрать, чтобы CommView перехватывал RAS пакеты?
! : Это зависит от Вашей системы. Прежде всего, попробуйте их один за другим, и в большинстве случаев один из них будет работать. С одним из Remote Access WAN Wrapper устройств, Вы можете столкнуться с нежелательным эффектом: CommView перехватывает и отображает пакеты, но пакеты не доходят до Ваших сетевых приложений (т.е. время ожидания истекло и т.д.). Если у Вас эта проблема, то остановите перехват и выберите другой Remote Access WAN Wrapper из списка.

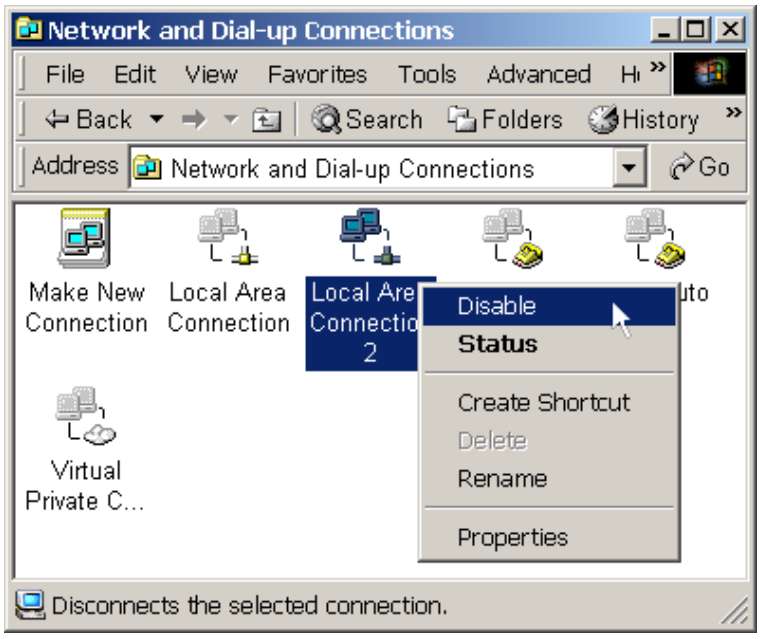
? : У меня Windows 95, и я не вижу вертикальные закладки, как показано в скриншотах. Кроме того, я не вижу флажки рядом с названиями протоколов на закладке "Rules". В чём дело?
! : Это означает, что у Вас очень старые системные файлы, в частности COMCTL32.DLL. Один из способов обновить их - инсталлировать последнюю версию Microsoft Internet Explorer. Это и будет решением данной проблемы. (И создаст много новых, в частности, проблемы безопасности [VBscipt вирусы, JavaScript вирусы, spyware]. Лучше – просто обновить устаревшие файлы, скачав 50COMUPD.EXE (~500 Kb), а пользоваться браузером Opera (~3200 Kb).– прим. перев.)

? : У меня Windows 95 и dial-up подключение. Каждый раз, как я нажимаю "Stop Capture", модем разрывает соединение. Что можно с этим сделать?
! : Вам следует установить обновления winsock и dial-up networking для Windows 95, и это решит проблему. Важен порядок установки обновлений, сперва Windows Socket 2 Update, а потом Dial Up Networking 1.4 Performance & Security Update.

Windows Socket 2 Update

Dial Up Networking 1.4 Performance & Security Update

? : У меня Windows 2000, при удалении программы появляется сообщение: "CommView will now uninstall the drivers. Click "OK" to continue. This can take between 10 and 60 seconds." Но, ничего не происходит!
! : Это может случиться, если есть активное сетевое подключение в момент удаления программы. Следует временно выключить сетевое подключение, как показано здесь:



Как только сеть отключится, CommView продолжит процесс удаления, после его завершения можно возобновить сетевое подключение.

? : У меня Windows 2000 Terminal Server, и я не могу запустить CommView с удалённой консоли.

! : Выход из положения зависит от версии CommView:
CommView 3.0 и выше: перезагрузите сервер, чтобы запустить CommView через Terminal Services client.
CommView 2.4-2.6: скачайте обновлённый CV2K.DLL, замените им старый DLL в папке программы, включите и выключите захват пакетов как локальный пользователь, и перезагрузите компьютер. Теперь проблем с запуском CommView через Terminal Services Client быть не должно.
Единственное ограничение заключается в том, что каждый адаптер доступен только одному пользователю. Другими словами, два пользователя (местный и удалённый) не могут собирать трафик с одного и того же адаптера, запустив две копии CommView на одном сервере.

? : Я работаю в сильно загруженной локальной сети и замечаю, что CommView увеличивает загрузку процессора и/или начинает медленнее отвечать на запросы. Что можно с этим сделать?
! : Самый лучший способ оптимизировать работу программы это использование фильтрации пакетов, которые Вам не нужны. Например, копирование файла размером 50 мегабайт между двумя машинами может порождать около 40 000 пакетов NetBIOS со скоростью 1 Мегабайт в секунду, что может быть значительной нагрузкой для приложения. Обычно, нет необходимости просматривать каждый пакет NetBIOS, по этому Вы можете сконфигурировать CommView для перехвата только IP пакетов. CommView имеет гибкую систему фильтров, которые позволяют произвести тонкую настройку только на те пакеты, которые Вам действительно необходимы. Если Вы заинтересованы в получении только статистической информации (гистограммы и круговые графы) – включите "Suspend packet output", Вы получите верные результаты в диаграмме протоколов. См. также главу Работа в сильно загруженной сети.

? : Поддерживает ли CommView не-Ethernet network адаптеры, например TokenRing?
! : К сожалению, пока нет.

? : Можно ли менять PC-карты в ноутбуке, когда запущен CommView?
! : Нет, лучше выйти из CommView, сменить адаптер и запустить программу снова. Список адаптеров автоматически обновится.

? : Иногда, при запуске CommView, появляются "песочные часы", а программа не включается. Почему?
! : Проверьте, не открыто ли окно свойств сети или удалённого соединения. Как только Вы его закроете, CommView запустится.

? : Известны ли конфликты с другими программами?
! : В данный момент мы знаем о конфликтах со следующими программами:

- SoftIce by Numega: возможен крах системы.
- PGPNet 7.0 by NAI: низкоуровневый конфликт драйвера, приводящий к BSoD под Windows 2000, если PGPNet привязан к dial-up адаптеру.
- Sygate Personal Firewall: конфликт драйвера, приводящий к BSoD под Windows 2000/XP, если Вы пытаетесь наблюдать за dial-up адаптером с помощью CommView 3.3 или старее. Проблема не возникает при наблюдении сетевого адаптера Ethernet. Исправлено в CommView 3.4.
- Kerio Personal Firewall v2.x: Несовместимость с драйвером KPF, приводящая к BSoD в Windows XP при наблюдении трафика на адаптере удалённого доступа. Наступает при условии, что CommView был установлен после KPF. Если наблюдать за Ethernet адаптером, BSoD не случается. Устранён в KPF v3.0; ждите официального релиза.

Если Вы думаете, что обнаружили конфликт с приложением, которого нет в списке, мы будем Вам благодарны за сообщение.

? : Должен ли я быть профессионалом, чтобы использовать эту программу?
! : Нет. Мы надеемся, что даже неопытные пользователи сочтут эту программу полезной. Вы можете не использовать все её возможности. Например, даже начинающим может быть интересно получить полную картину сетевых соединений их компьютеров, или выяснить, что установленная вчера программа на самом деле - Троян, отправляющий их dial-up пароли на чужой e-mail адрес.

? : Где найти подробную информацию о захвате пакетов и анализе протоколов?
! : Зайдите на эти сайты:

Sniffing (network wiretap, sniffer) FAQ

Protocols.com

Работа в сильно загруженной сети

При сборе пакетов на большом или сильно загруженном сегменте сети, обработка тысяч пакетов в секунду может существенно нагрузить процессор и снизить скорость реакции программы. Повысить же производительность программы можно используя правила для фильтрации ненужных Вам пакетов. Пересылка 50 Мб файла между двумя машинами порождает около 40000 NetBIOS пакетов со скоростью 1 мегабайт в секунду, что может оказаться тяжёлой задачей для CommView на Вашей машине. Однако, часто не требуется анализ каждого из пакетов NetBIOS, и, можно сконфигурировать CommView так, что он будет принимать только пакеты IP. В CommView есть развитая система фильтров, позволяющая принимать только те пакеты, которые Вам действительно интересны. Если нужна лишь статистическая информация (гистограммы, таблицы хостов), можно воспользоваться командой "Suspend packet output" в меню, отображение пакетов будет выключено, нагрузка на ресурсы машины снижена, а требуемая информация будет получена.

Факторы, улучшающие производительность программы:

- Быстрый процессор (Pentium III или выше)
- Большая память (128 Мб и больше)
- Операционная система, построенная на основе технологии NT (рекомендуем Windows 2000/XP)
- Использование фильтров для игнорирования ненужного трафика
- Использование режима "Suspend packet output"

Факторы, ухудшающие производительность программы:

- Медленный процессор или малое ОЗУ
- Использование алиасов для MAC и IP, особенно, если их много
- Использование преобразования номера порта в имя сервиса

Запуск нескольких копий программы

CommView может захватывать пакеты на нескольких сетевых адаптерах одновременно (недоступно под Windows 95). Эта возможность включается флажком **Allow Multiple Application Instances** в **Settings(Настройки) =>Options(Опции) => Miscellaneous(Разное)**. Однако, один и тот же адаптер нельзя открыть двумя копиями программы. Такое же ограничение существует для Terminal Server: два пользователя (местный и удалённый) не могут наблюдать трафик одним и тем же адаптером, запустив две копии CommView на одном и том же сервере.

Невидимый режим

Есть два способа скрыть работающий CommView:

1. Запустить CommView с ключём "hidden":

   CV.EXE hidden

2. Если CommView уже запущен, Вы можете прятать/вызывать (hide/unhide) 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. Когда CommView спрятан, его нет в списке задач (в том, что вызывается по ALT+CTRL+DEL) Windows 95/98/Me, но любая утилита, показывающая работающие процессы, обнаружит CommView. В Windows NT/2000/XP такой утилитой является Task Manager.

Параметры командной строки

При запуске программы доступны следующие параметры командной строки:

- Загрузить из файла и включить правила. Используйте ключ "/ruleset", за которым следует имя и полный путь к файлу, например:

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

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

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

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

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

При необходимости, можно использовать оба ключа одновременно.

Передача данных во внешнее приложение

Начиная с версии 3.0, CommView предоставляет простой TCP/IP интерфейс передачи захватываемых пакетов в Ваше приложение для обработки их в реальном времени.

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

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

Когда CommView запущен подобным образом, он пытается установить TCP соединение с указанным IP адресом по указанному номеру порта. Это означает, что Ваше приложение уже должно быть запущено и "слушать" по указанному порту. Если CommView не может установить соединение, он будет делать повторные попытки каждые 15 секунд. То же самое будет происходить при разрыве соединения: каждые 15 секунд CommView будет пытаться восстановить его. Если соединение успешно установлено, CommView будет передавать захватываемые пакеты по мере их прихода.

Формат данных
Так как пакеты передаются в виде потока, Вам надо уметь разделять его, CommView использует простые заголовки для "нарезки" потока на исходные пакеты. Перед каждым пакетом передаётся трёхбайтовый заголовок. Первые два байта – длина пакета, не считая данный заголовок. Байты передаются, начиная с младшего, т.е. 0x0200 соответствует 2, а 0x0002 представляет 512. Третий байт кодирует направление пакета:

0x00 - транзитный
0x01 - входящий
0x02 – исходящий

Например:
0xE80000 – транзитный пакет длиной 232 байта
0xB10102 – исходящий пакет длиной 433 байта

Пользуясь данным описанием можно создать собственный обработчик потока и выделять дублируемые CommView пакеты.

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

- http://www.tamos.com/products/commview/samp_mirr_c.zip. Проект в Visual Studio с исходным текстом на C++.
- http://www.tamos.com/products/commview/samp_mirr_d.zip. Проект на Delphi с исходником на Pascal. Для компиляции проекта Вам понадобятся ICS компоненты от Francois Piette, которые доступны на http://overbyte.delphicenter.com/frame_index.html

Пропускная способность (Bandwidth)
При копировании данных на удалённый компьютер, удостоверьтесь, что линия связи между ними достаточно широкополосна, чтобы пропустить все захватываемые данные. Если CommView собирает данные с интенсивностью 500 kB/sec, а линия связи способна передавать только 50kB/sec, неизбежно возникнут "пробки на дорогах", приводящие к разным неприятностям (например, в зависимости от версии Windows, winsock может прекратить передавать данные вообще). Если Вам требуется более гибкое решение, использующее буферизацию и дистанционное управление – попробуйте воспользоваться CommView Remote Agent.

Пользовательский модуль декодирования

Начиная с версии 4.0, CommView позволяет подключить пользовательский модуль декодирования. Если таковой имеется, он будет отображён в дополнительной колонке закладки **Packets(Пакеты)**. Пользовательский декодер должен быть 32-bit DLL с именем файла "Custom.dll" и экспортировать единственную процедуру - "Decode". Ниже показан её прототип на языках C и Pascal:

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

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

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

Перед тем как отобразить новый пакет, CommView вызывает процедуру "Decode" и передаёт ей содержимое пакета. Процедура "Decode", обработав пакет, должна вернуть результат в соответствующем буфере. Первый аргумент - указатель на данные пакета, второй - их длина, третий аргумент - указатель на буфер для результата обработки, четвёртый аргумент - размер буфера (в данной версии - всегда 1024 байта). Буфер выделяется и освобождается самой программой CommView, не пытайтесь манипулировать его освобождением. Содержимое буфера будет отображено в виде сроки в колонке "Custom".

Быстродействие кода процедуры должно позволять обработку тысяч пакетов в секунду; в противном случае снизится производительность программы. Обязательно соблюдайте соглашения STDCALL при вызове.

Образцы проектов

Две демонстрационных DLL приведены для примера. Они выполняют примитивные действия: "результатом" работы функции "Decode" является шестнадцатеричный код последнего байта пакета. Пользовательский декодер может выполнять любые мыслимые преобразования.

- 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.

Информация

Где купить CommView

Демо-версия имеет 30-дневный период. Ниже приведены цены на зарегистрированную, полнофункциональную версию программы:

Тип лицензии	Цена, USD
CommView Home License 1 user (для частного, некоммерческого использования)	129.00
CommView Enterprise License 1 user (для профессионального, коммерческого использования)	249.00

Два типа лицензий:

- Более дорогая Enterprise License даёт право на коммерческое и некоммерческое использование программы.
- Менее дорогостоящая Home License даёт Вам право пользоваться программой дома на некоммерческой основе, количество хостов, доступных для наблюдения в Вашей домашней сети, ограничивается пятью.

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.

Покупатели из России могут приобрести программу за рубли у нашего российского дилера, компании Softkey:

http://www.softkey.ru/catalog/company.php?ID=16905

Покупатели из других стран могут заказать программу через наш веб сайт:

http://www.tamos.com/order/

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.

Как связаться с TamoSoft Inc.?

Web

http://www.tamos.ru/

E-mail

sales@tamos.ru (По вопросам продаж)
support@tamos.ru (По прочим вопросам)

Почта и факс

Почтовый адрес:

PO Box 1385
Christchurch 8015
New Zealand

Факс: +64 3 359 0392 (New Zealand)
Факс: +1 503 213-7764 (USA)

Другие продукты компании TamoSoft

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..

Essential NetTools

Полезный пакет для диагностики сетей и слежения за сетевыми соединениями Вашего компьютера. Он включает быстрый многопотоковый 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 шифрованных архивов, самораспаковывающихся EXE-файлов. В DigiSecret есть и средства сжатия файлов; Вам больше не потребуется zip-овать 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..