® Hewlett-Packard

Сеть часто напоминает цифровой мир — в ней живет информация, которую бывает полезно не просто копировать себе на винчестер, но и знать, как она движется по сети. Неплохо также выяснить, кто из «соседей» заходил в гости на ваш ПК или сколько трафика «пожирает» программа. В этом поможет специальное ПО

Увидеть сеть на мониторе

Евгений Барилюк, barilyuk@softpress.com.ua

Постоянный контроль за работой локальной сети необходим для поддержания ее работоспособности. Для этих целей существуют специальные аппаратные средства — мониторы. Однако их установка не оправдывает себя в малых сетях, в этом случае пригодятся программные сетевые мониторы.

Сетевой монитор — это программа диагностики сетей, которая используется для контроля над локальной ее частью и отображения статистики в графическом виде. Эта статистика необходима при решении текущих проблем, например, при определении наиболее активного пользователя или при повышенном расходе трафика. Монитор собирает информацию из сетевого потока данных на сетевом адаптере того ПК, на котором он установлен, и отображает полученные сведения о сети.

Существуют и другие задачи, решить которые помогает анализ трафика. Например защита от троянов — с помощью сетевого монитора вы увидите неизвестное приложение, передающее данные в Интернет, и сможете его удалить даже когда антивирус ничего не находит. Также мониторы оказываются полезными при необходимости проанализировать объемы переданного и принятого трафика.

Как это работает?

Зная название ПК, где хранятся требуемые данные, вы не тратите время на поиск информации на каждой из представленных в сетевом окружении машин.

Примерно также общаются и компьютеры между собой. Любой компьютер в сети получает свой IP-адрес, который назначается DHCP-сервером или вручную. Очевидно, что в первом случае IP-адрес не может быть постоянным — такое часто используется при dial-up-подключении, когда пользователь сам не знает время следующего соединения с сетью. Кроме того, каждый Ethernet-адаптер имеет собственный уникальный MAC-адрес, который назначается изготовителем устройства на заводе.

Двое на одного

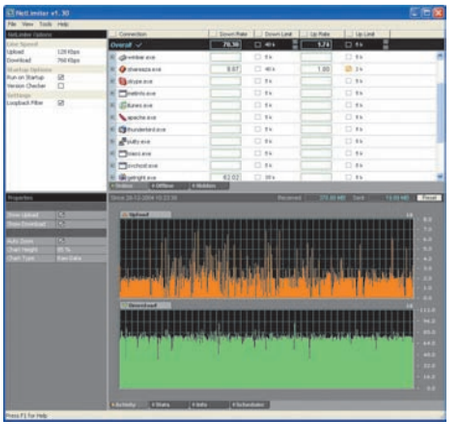
Эти два адреса используются для идентификации компьютера в сети. Естественно, человеку запомнить наборы цифр довольно трудно, поэтому существуют специальные DNS-серверы, осуществляющие трансляцию цифровых адресов в обычные имена. Например, сайт *www.google.com* имеет множество IP-адресов (узнать их можно с помощью сервиса *dns-tools.domaintools.com)*. Чтобы «общаться» между собой, компьютеры также используют специальные протоколы (TCP, UDP), по которым передается информация, и порты — выделенные «окна» для связи (например, протокол HTTP использует TCP 80).

Поэтому программы анализа и мониторинга сетевого трафика, как правило, следят и выдают данные о перечисленных выше параметрах (IP- и MAC-адреса, DNS-имя, названия приложений и номера открытых ими портов). К примеру, если к вашему ПК кто-то подключился, то сетевой монитор укажет IP-адрес посетителя, DNS-имя его хоста, название используемого ПО, а также статистику трафика. Причем программы зачастую способны подсчитать весь трафик (как для отдельного приложения, так и для всех вместе) за определенный период времени. А владея такой информацией, можно оптимизировать свои расходы на Интернет, узнать кто заходил к вам в гости, а также вычислить вредоносное и рекламное ПО, которое не всегда детектируется антивирусами.

Далее мы подробно рассмотрим некоторые наиболее удачные средства сетевого мониторинга. Больше программ и описания к ним ищите на hi-Tech DVD.

Мал, да удал

Netlimiter



Разработчик: . . . . . Locktime Software
Ссылка: . . . . . www.netlimiter.com
Цена: $30

Оценка

- ⊕ удобный интерфейс
- ⊕ наличие планировщика процессов
- ⊖ высокая стоимость

Утилита не только покажет, кто сколько трафика потребляет, но и распределит интернет-канал при необходимости

■ Программа Netlimiter — удобное средство контроля за приложениями, использующими Интернет. Главное достоинство этой утилиты — фантастически малый размер: всего лишь 500 КБ. Но при этом она позволяет следить за всеми приложениями, которые имеют статус «online» (использующие в данный момент сетевое соединение), «offline» (были запущены ранее, но сейчас неактивны) и «hidden» (скрытые приложения, за которыми может скрываться и шпионское ПО).

С помощью удобного графического интерфейса программа **Netlimiter позволяет легко отслеживать количество переданного и принятого трафика** (как в отдельности для каждой программы, так и для всего используемого ПО).

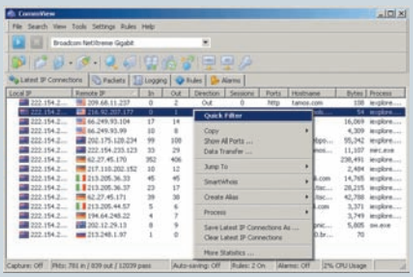
Если же перевести экран в режим статистики (Stats), то вы получите подробную информацию о сетевой активности любого приложения. Здесь представлена статистика в байтах о переданном (Upload) и загруженном (Download) из Сети трафике за текущий час, день или даже год. Во вкладке Info пользователь может также получить информацию о дате инсталляции приложения и его местонахождении.

Изюминка Netlimiter — встроенный планировщик. С его помощью вы можете назначить сетевую активность для конкретного приложения (например, ограничить трафик или вовсе запретить программе использовать сеть в определенное время). Подобная возможность очень пригодится, если компьютер используется несколькими пользователями.

Кроме того, Netlimiter позволяет выставить ограничение на прием и передачу трафика как для всего интернет-канала, так и для любого приложения в отдельности. Плюс у программы есть одновременно две версии — для 32- и 64-битовых ОС.

Глубокий анализ

Commview



Разработчик: TamoSoft
Ссылка: www.tamos.ru
Цена: 760 грн

Оценка

- ⊕ есть графический интерфейс и командная строка
- ⊕ многоязычный интерфейс
- ⊖ сложный для новичка интерфейс
- ⊖ высокая цена

Commview позволяет не толко узнать расход трафика, но и проанализировать его

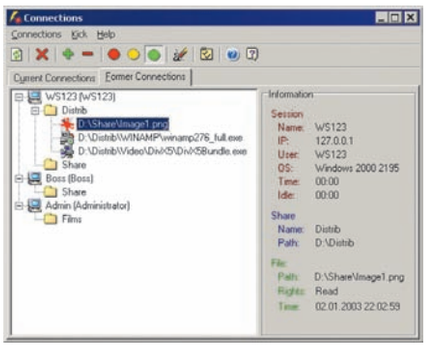
■ Самую полную картину, происходящую с трафиком в локальной сети или на определенном сетевом адаптере компьютера, покажут программы-анализаторы. Например, программа Commview. Она **позволяет не только производить мониторинг, но и обеспечивать глубокий анализ передаваемых пакетов данных**. По сути, Commview собирает все пакеты, проходящие через модем или сетевую карту, и выдает о них подробную информацию: флаг пакета, его размер и содержимое.

Commview умеет также фиксировать список сетевых соединений (IP-, MAC-адреса, порты, сессии) и исследовать отдельные пакеты. При этом IP-пакеты можно разбирать вплоть до самого низкого уровня, анализируя данные распространенных протоколов. А функция фильтрации позволяет отбрасывать ненужные пакеты, анализируя только выбранные. При обнаружении определенного пакета программа позволит отослать предупреждения по электронной почте, записать данные в лог-файл или сообщить о находке всплывающим окошком.

Commview работает на платформах ОС Windows 95/98/Me/NT/2000/XP и поддерживает как графический интерфейс, так и режим командной строки. Программа также поддерживает работу ПК с беспроводным Wi-Fi-адаптером. Правда, в этом случае анализируются только пакеты, сгенерированные вашим компьютером, и пакеты, адресованные непосредственно ему. Для мониторинга всех пакетов в Wi-Fi-сети следует использовать версию Commview Wi-Fi.

Личный следопыт

Friendly Net Watcher



Разработчик: . . . . . Андрей Килиевич
Ссылка: . . . . . www.kilievich.com
Цена: . . . . . бесплатно

Оценка

- ⊕ поддержка русского языка
- ⊕ подробная документация всех событий
- ⊖ недостаточная функциональность

«Дружественный сетевой монитор» берет своей простотой использования

■ Если вам необходимо эффективно отследить, кто из сетевого окружения посещает «расшаренные» папки на вашем ПК, то обратите внимание на Friendly Net Watcher.

В меню данной утилиты присутствуют две основные вкладки — *Текущее соединение* и *История*. Заглянув в первую, можно увидеть, кто в данный момент подключился к ПК. Причем отображается как само название файла или приложения, так и полный путь к нему. **В отличие от аналогичных средств Windows XP, эта программа выдает более подробную статистику о посетителе** (DNS-имя, IP-адрес, время установления соединения и использования файла, ОС подключенного ПК). Кроме того, пользователи Friendly Net Watcher могут поместить надоедливых соседей в черный список под названием kicklist. При этом компьютеры из этого списка при попытке установить соединения будут сразу же разъединены.

В ПО также предусмотрен режим оповещения в виде звукового сигнала из WAV-файла. Программа может оповещать вас о следующих событиях: установленное соединение, первый открытый ресурс или файл, а также о любом открываемом файле или ресурсе.

Больше программ для мониторинга сети и описания к ним смотрите на hi-Tech DVD