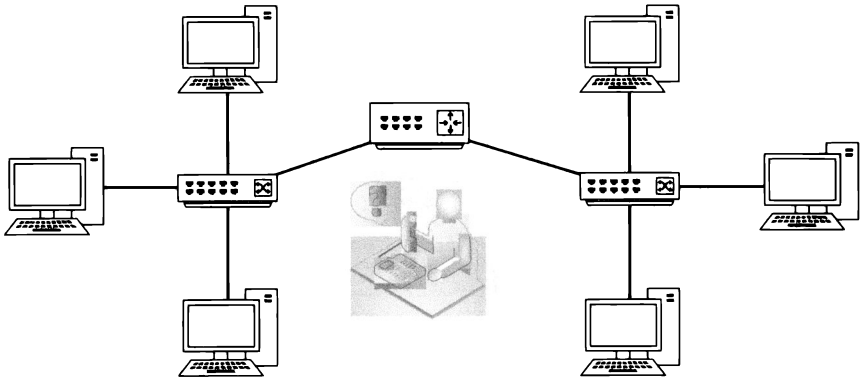

Рис. 2.1. Разместить анализатор пакетов в сети не так-то просто, если в ней имеется немало соединений, поскольку такая ее организация затрудняет получение нужных данных

Прослушивание сети в смешанном режиме

Прежде чем анализировать пакеты в сети, необходимо обзавестись сетевой интерфейсной платой (NIC), иначе называемой сетевым адаптером, с поддержкой драйвера смешанного режима (promiscuous mode) для прослушивания сети. В *смешанном режиме* сетевой адаптер может просматривать все пакеты, проходящие по сети.

Как пояснялось в главе 1, "Анализ пакетов и основы организации сетей", из широковещательного сетевого трафика устройства обычно получают пакеты, которые фактически не предназначены для них. Например, сетевой протокол ARP (Address Resolution Protocol – протокол преобразования адресов) служит крайне важным средством в любой исследуемой сети для определения MAC-адресов, соответствующих конкретному IP-адресу. Чтобы обнаружить подходящий MAC-адрес, устройство посылает широковещательный пакет по сетевому протоколу ARP каждому устройству, находящемуся в его широковещательном домене, в надежде, что нужное устройство отреагирует на данный пакет.

Широковещательный домен (т.е. сетевой сегмент, где любой компьютер может передавать данные непосредственно любому другому компьютеру без помощи маршрутизатора) может состоять из нескольких устройств. Но лишь нужное приемное устройство в этом домене должно быть заинтересовано в получении широковещательного пакета, передаваемого по сетевому протоколу ARP. И было бы совершенно неэффективно, если бы каждое устройство в сети обрабатывало широковещательный пакет, передаваемый по сетевому протоколу ARP. Напротив, если пакет не предназначен для устройства, а сле-

довательно, не нужен ему, то сетевой адаптер данного устройства отбросит пакет вместо того, чтобы передать его на обработку центральному процессору (ЦП).

Отбрасывание пакетов, не предназначенных для принимающего хоста, повышает эффективность обработки данных в сети, но для анализа пакетов этот режим работы сетевой платы совсем не подходит. Специалистам по анализу пакетов, как правило, требуется перехватывать *каждый* пакет, посылаемый по сети, чтобы не пропустить какой-нибудь важный фрагмент информации.

Используя смешанный режим работы сетевого адаптера, можно гарантировать, что будет перехвачен весь сетевой трафик. Когда сетевой адаптер работает в смешанном режиме, он передает каждый обнаруживаемый им пакет процессору хоста независимо от его адреса его получателя. И как только пакет поступит на обработку в ЦП, приложение, анализирующее пакеты, сможет взять его на анализ.

Смешанный режим поддерживается в большинстве современных сетевых адаптеров, и в состав Wireshark входит драйвер libpcap/WinPcap, позволяющий переключить сетевой адаптер непосредственно в смешанный режим из графического интерфейса инструментального средства Wireshark. (Подробнее о драйвере libpcap/WinPcap речь пойдет в главе 3, "Введение в Wireshark".)

ПРИМЕЧАНИЕ *В большинстве операционных систем, включая Windows, не допускается применять сетевой адаптер в смешанном режиме, если только у вас нет расширенных пользовательских полномочий. Если же у вас нет законных оснований получить такие полномочия в своей системе, вам, скорее всего, не удастся провести такого рода анализ пакетов в данной конкретной сети.*

Анализ пакетов через концентраторы

Анализ пакетов в сети, где установлены концентраторы, — мечта любого исследователя пакетов. Как пояснялось в главе 1, "Анализ пакетов и основы организации сетей", сетевой трафик, пропускаемый через концентратор, поступает на каждый порт, подключенный к этому концентратору. Следовательно, чтобы проанализировать трафик, проходящий через компьютер, подключенный к концентратору, достаточно подключить анализатор пакетов к пустому порту концентратора. Это даст возможность просматривать весь обмен данными как с этим компьютером, так и с любыми другими устройствами, подключенными к тому же самому концентратору. Как показано на рис. 2.2, пределы видимости безграничны, когда анализатор пакетов подключен к сети, созданной на основе концентраторов.

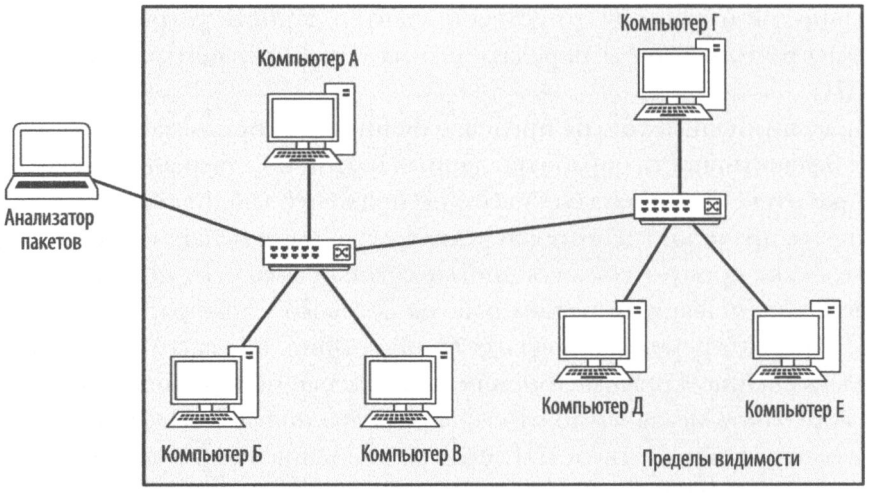

Рис. 2.2. Анализ пакетов в радиально-узловой сети, созданной на основе концентраторов, обеспечивает безграничные пределы видимости

ПРИМЕЧАНИЕ *Как следует из различных блок-схем, приведенных в данной книге, термин пределы видимости охватывает устройства в сети, трафик которых можно просматривать с помощью анализатора пакетов.*

Но теперь, к сожалению, сети очень редко строятся на основе концентраторов, поскольку их администрирование весьма затруднено. В таких сетях лишь одно устройство может одновременно передавать данные через концентратор, и поэтому все подключенные к нему устройства должны конкурировать за право передать данные со всеми остальными устройствами сети. Если данные будут одновременно передавать два или больше устройств, то возникает так называемое явление *коллизии пакетов*, как показано на рис. 2.3. В итоге может произойти потеря пакетов, и для выхода из сложившейся ситуации передающим устройствам нужно будет повторить их передачу, что приводит к падению пропускной способности сети. По мере увеличения уровня трафика и количества коллизий устройствам, возможно, придется повторять передачу пакетов по три или четыре раза, а это в значительной степени снизит производительность сети. Таким образом, нетрудно понять, почему в большинстве современных сетей любых масштабов применяются коммутаторы. Но, несмотря на то что концентраторы редко применяются в современных сетях, иногда они все же встречаются в тех сетях, где поддерживается устаревшее оборудование или специализированные устройства, например, в сетях автоматизированных систем управления производственными процессами (ICS).

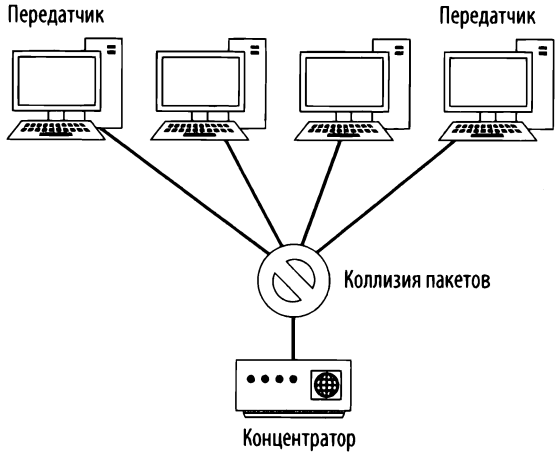

Рис. 2.3. В радиально-узловой сети, созданной на основе концентраторов, может возникнуть коллизия пакетов, когда два или больше устройств будут передавать данные одновременно

Чтобы выяснить наличие концентратора в сети, проще всего заглянуть в серверное помещение или сетевой монтажный шкаф, где большинство концентраторов специально обозначены метками. Если и это не поможет, загляните в самый темный угол серверного помещения, где обычно находится покрытое толстым слоем пыли сетевое оборудование.

Анализ пакетов в коммутируемой среде

В качестве соединительных устройств в современных сетях чаще всего применяются коммутаторы. Они обеспечивают эффективный порядок переноса данных через широковещательный, много- и одноадресатный трафик. Коммутаторы допускают дуплексную передачу данных, а это означает, что машины могут передавать и принимать данные одновременно.

К сожалению, коммутаторы усложняют задачу исследователям пакетов. Подключив свой анализатор пакетов к порту коммутатора, вы сможете просмотреть лишь часть широковещательного трафика, а также трафик, передаваемый и принимаемый тем устройством, на котором установлен анализатор пакетов (рис. 2.4). Чтобы перехватить трафик из целевого устройства в коммутируемой сети, вам придется предпринять дополнительные шаги. Перехватить такой трафик можно следующими четырьмя способами: зеркальное отображение портов (port mirroring), перехват пакетов через концентратор, применение сетевого ответвителя и заражение ARP-кеша.

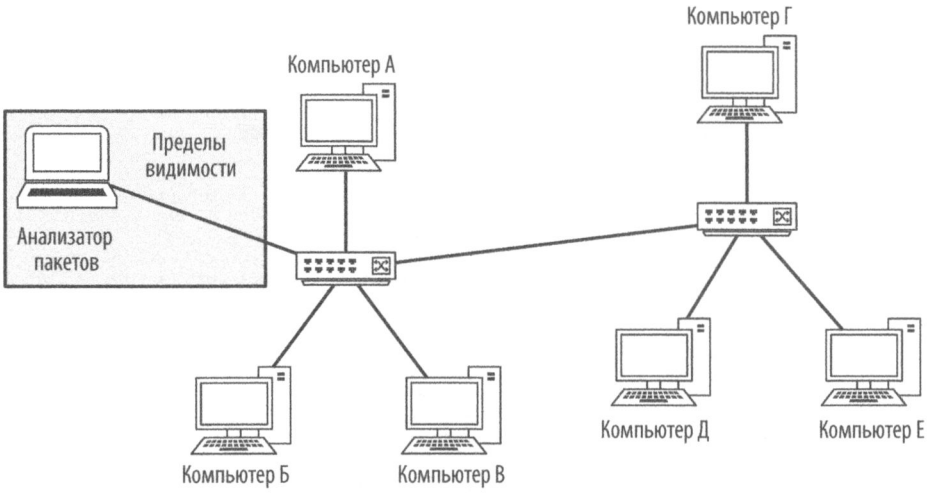

Рис. 2.4. Пределы видимости в коммутируемой сети ограничиваются портом, к которому подключен анализатор пакетов

Зеркальное отображение портов

Зеркальное отображение портов (port mirroring), иначе называемое *расширением портов (port spanning)*, считается едва ли не самым простым способом перехвата сетевого трафика из целевого устройства в коммутируемой сети. Для этого необходимо иметь доступ к интерфейсу командной строки или веб-управления того коммутатора, к которому подключен целевой компьютер. Кроме того, коммутатор должен поддерживать зеркальное отображение портов и иметь пустой порт, к которому можно подключить анализатор пакетов.

Чтобы активизировать зеркальное отображение портов, следует выдать команду, вынуждающую коммутатор копировать весь трафик из одного порта в другой. Например, чтобы перехватить весь трафик, который передает и принимает устройство, подключенное к порту 3 коммутатора, достаточно подключить анализатор пакетов к его порту 4 и зеркально отобразить порт 3 на порт 4. Процесс зеркального отображения портов наглядно показан на рис. 2.5.

Порядок организации зеркального отображения портов зависит от конкретной модели коммутатора. В большинстве промышленных коммутаторов придется пройти регистрацию через интерфейс командной строки и настроить зеркальное отображение портов по специальной команде. Перечень таких команд приведен в табл. 2.1.

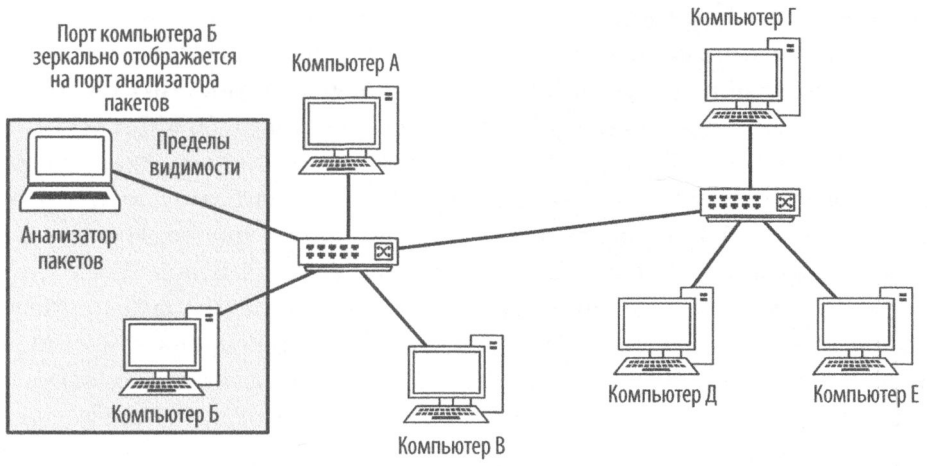

Рис. 2.5. Зеркальное отображение портов позволяет расширить пределы видимости в коммутируемой сети

Таблица 2.1. Команды, применяемые для активизации зеркального отображения

Производитель коммутатора	Команда
Cisco	`set span <порт источника> <порт назначения>`
Enterasys	`set port mirroring create <порт источника> <порт назначения>`
Nortel	`port-mirroring mode mirror-port <порт источника>` `monitor-port <порт назначения>`

ПРИМЕЧАНИЕ *В некоторых промышленных коммутаторах предоставляется веб-ориентированный графический интерфейс, где зеркальное отображение портов не всегда поддерживается, хотя такие коммутаторы нетипичны и не стандартизированы. Но если коммутатор предоставляет эффективный способ настройки зеркального отображения портов через веб-интерфейс, то такой возможностью следует, безусловно, воспользоваться. Кроме того, в коммутаторах для небольших учрежденческих и домашних сетей (SOHO) все чаще начинают предоставляться возможности для зеркального отображения портов, которое, как правило, настраивается через веб-интерфейс.*

Зеркально отображая порты, следует принимать во внимание их пропускную способность. Некоторые производители коммутаторов позволяют зеркально отображать несколько портов на один порт, и такая функция может оказаться полезной при анализе передачи данных между двумя или несколькими устройствами на одном коммутаторе. Рассмотрим, однако, что может при

этом произойти, произведя несложные математические расчеты. Если, например, имеется коммутатор на 24 порта, где 23 порта зеркально отображаются на один порт при дуплексной передаче данных со скоростью 100 Мбит/с, то данные должны поступать в этот порт со скоростью 4600 Мбит/с. Но ведь это выходит далеко за пределы физических возможностей одного порта, а следовательно, может привести к потере пакетов или замедлению работы сети, если сетевой трафик достигнет определенного уровня. Иногда подобная ситуация называется *переподпиской (oversubscription)*. В подобных случаях коммутаторы, как известно, пропускают лишние пакеты или даже нарушается работа внутренних электрических схем, что полностью препятствует передаче данных. Поэтому непременно убедитесь, что, перехватывая пакеты рассматриваемым здесь способом, вы не вызовите подобные осложнения в сети.

Зеркальное отображение портов может оказаться привлекательным, недорогим решением для корпоративных сетей и в тех случаях, когда требуется постоянно контролировать отдельные сегменты сети, например, в ходе текущего контроля сетевой безопасности. Но такая методика, как правило, оказывается недостаточно надежной для подобного применения. Зеркальное отображение портов может давать противоречивые результаты особенно при высоких уровнях трафика в сети, приводя к потере данных, которую трудно проследить. В подобных случаях рекомендуется пользоваться сетевым ответвителем, как поясняется далее в соответствующем разделе.

Перехват пакетов через концентратор

Еще одним способом перехвата трафика, проходящего через целевое устройство в коммутируемой сети, является *перехват пакетов через концентратор*. По этой методике целевое устройство и анализатор пакетов размещаются в одном сегменте коммутируемой сети и подключаются непосредственно к концентратору. Многие считают перехват пакетов через концентратор обманом, но на самом деле это вполне обоснованное решение, когда нельзя выполнить зеркальное отображение портов, но в то же время имеется физический доступ к тому коммутатору, к которому подключено целевое устройство.

Чтобы организовать перехват пакетов через концентратор, достаточно иметь в своем распоряжении сам концентратор и несколько сетевых кабелей. Если у вас имеется такое оборудование, подключите его следующим образом.

1. Найдите коммутатор, к которому подключено целевое устройство, и отключите последнее от сети.
2. Подключите сетевой кабель целевого устройства к своему концентратору.

3. Подключите еще один сетевой кабель, соединяющий ваш анализатор пакетов с концентратором.
4. Подключите сетевой кабель, идущий от концентратора, к сетевому коммутатору, чтобы присоединить концентратор к сети.

Итак, вы разместили целевое устройство и анализатор пакетов в одном широковещательном домене. В итоге весь сетевой трафик от данного устройства будет передаваться в широковещательном режиме. В результате анализатор пакетов может перехватывать из него все пакеты, как показано на рис. 2.6.

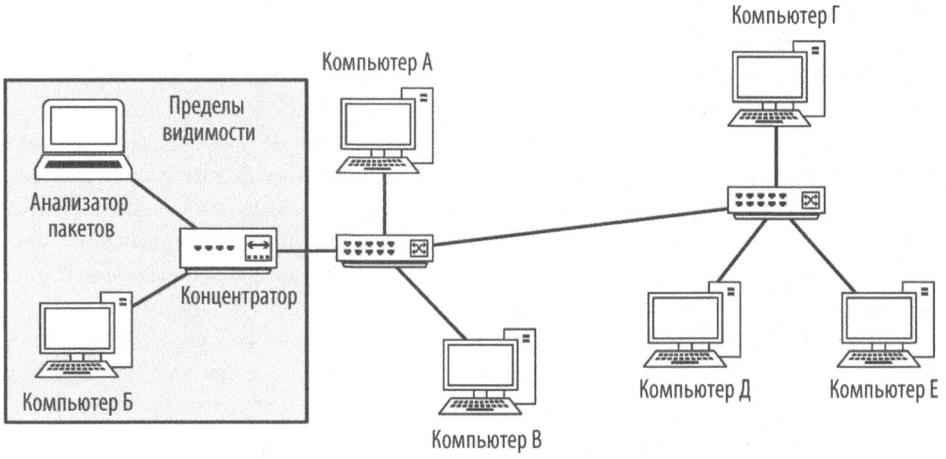

Рис. 2.6. При перехвате пакетов через концентратор целевое устройство и анализатор пакетов изолированы

В большинстве случаев перехват пакетов через концентратор сводит дуплексную (т.е. двунаправленную) передачу данных на целевом устройстве к полудуплексной (т.е. однонаправленной). И хотя эта методика не является самой лучшей для перехвата пакетов, она остается единственно возможной в тех случаях, когда в коммутаторе не поддерживается зеркальное отображение портов. Следует, однако, иметь в виду, что концентратор потребуется также подключить к розетке электросети, которую бывает нелегко найти.

ПРИМЕЧАНИЕ *Не забудьте своевременно предупредить пользователя целевого устройства, что вы собираетесь отключить его от сети, особенно если это большой начальник!*

ВЫБОР "ПРАВИЛЬНЫХ" КОНЦЕНТРАТОРОВ

Чтобы перехватывать пакеты через концентратор, воспользуйтесь настоящим концентратором, а не коммутатором, ложно отнесенным к категории концентраторов. Некоторые производители сетевого оборудования имеют скверную привычку рекламировать и продавать свои устройства как "концентраторы", хотя они на самом деле выполняют функции низкоуровневых коммутаторов. Если вы не пользуетесь проверенным, испытанным концентратором, то сможете просматривать только собственный трафик, а не тот, что проходит через целевое устройство.

Выбирая устройство, которое якобы считается концентратором, убедитесь, что оно отвечает своему назначению. Чтобы выяснить, является ли выбираемое устройство настоящим концентратором, лучше всего подключить к нему пару компьютеров и проверить, можно ли на одном из них анализировать сетевой трафик между вторым и другими устройствами в сети, например, компьютерами или принтерами. Если это можно сделать, значит, вы выбрали именно то, что нужно!

Концентраторы стали теперь настолько редки, что уже не производятся массово. Приобрести имеющийся в продаже настоящий концентратор практически невозможно, и поэтому вам придется проявить творческую инициативу, чтобы найти нужный товар. Отличным местом для поиска концентраторов служит аукцион бывших в употреблении предметов, проводимый в районе местной школы. Государственные школы обязаны попытаться выставить на аукцион бывшие в употреблении предметы, прежде чем избавиться от них, а ведь у них нередко залеживается старое оборудование. Мне не раз приходилось видеть людей, уходивших с таких аукционов с несколькими концентраторами, приобретенными по цене меньше стоимости тарелки фасоли или кукурузного хлеба. Еще одним удобным местом для приобретения концентраторов может служить электронный аукцион eBay, но будьте на чеку, чтобы не приобрести коммутатор, ложно отнесенный к категории концентраторов.

Применение сетевого ответвителя

Всем известно выражение "Зачем мне курица, если я могу съесть бифштекс?" А если вы с юга США, то вам знакомо такое выражение: "Зачем мне ливерный хлеб, если я могу съесть бутерброд с поджаренной болонской колбасой?" Это же относится и к выбору между концентратором и сетевым ответвителем для перехвата и анализа пакетов.

Сетевой *ответвитель* – это оборудование, которое можно установить между двумя точками кабельной разводки сети, чтобы перехватывать пакеты, проходящие между этими точками. И в данном случае, как и при перехвате пакетов через концентратор, в сети устанавливается оборудование, которое позволяет перехватывать нужные для анализа пакеты. Отличие рассматриваемого здесь способа заключается в том, что вместо концентратора в данном

случае применяется оборудование, специально предназначенное для анализа сетевого трафика.

Имеются два основных типа сетевых ответвителей: *агрегированный* и *неагрегированный*. Оба типа сетевых ответвителей устанавливаются между двумя устройствами для анализа обмена данными между ними. Главное отличие неагрегированного сетевого ответвителя от агрегированного заключается в том, что у него имеются четыре порта, как показано на рис. 2.7, и ему требуются отдельные интерфейсы для контроля текущего сетевого трафика в обоих направлениях. А у агрегированного сетевого ответвителя имеются лишь три порта, но он позволяет проводить контроль текущего сетевого трафика в обоих направлениях с помощью единственного интерфейса. Кроме того, сетевые ответвители, как правило, требуется подключать к розетке электросети, хотя некоторые из них работают и от батарей электропитания, допуская краткосрочное проведение анализа пакетов.

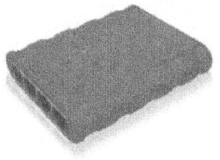

Рис. 2.7. Неагрегированный сетевой ответвитель типа Barracuda

Агрегированные сетевые ответвители

Проще всего пользоваться агрегированным сетевым ответвителем, у которого имеется лишь один физический контрольный порт для анализа двунаправленного сетевого трафика. Чтобы перехватывать с помощью агрегированного сетевого ответвителя весь входящий и исходящий сетевой трафик одного компьютера, подключенного к коммутатору, выполните следующие действия.

1. Отключите компьютер от коммутатора.
2. Подключите один конец первого сетевого кабеля к компьютеру, а другой — к входному порту сетевого ответвителя.
3. Подключите один конец второго сетевого кабеля к выходному порту сетевого ответвителя, а другой — к коммутатору.
4. Подключите один конец третьего сетевого кабеля к контрольному порту сетевого ответвителя, а другой — к компьютеру, выполняющему роль анализатора пакетов.

Агрегированный сетевой ответвитель должен быть подключен к сети так, как показано на рис. 2.8. В итоге анализатор пакетов должен перехватывать весь входящий и исходящий трафик компьютера, подключенного к данному ответвителю.

Рис. 2.8. Применение агрегированного сетевого ответвителя для перехвата сетевого трафика

Неагрегированные сетевые ответвители

Неагрегированный сетевой ответвитель немного сложнее, чем агрегированный. Тем не менее он допускает чуть больше удобств в перехвате сетевого трафика. Вместо единственного контрольного порта, применяемого для прослушивания двунаправленного обмена данными, неагрегированный сетевой ответвитель предоставляет два контрольных порта. Один контрольный порт служит для анализа сетевого трафика в одном направлении (от компьютера, подключенного к сетевому ответвителю), а другой — для анализа сетевого трафика в другом направлении (к компьютеру, подключенному к сетевому ответвителю).

Чтобы перехватывать весь входящий и исходящий сетевой трафик компьютера, подключенного к коммутатору, выполните следующие действия.

1. Отключите компьютер от коммутатора.
2. Подключите один конец первого сетевого кабеля к компьютеру, а другой — к входному порту сетевого ответвителя.
3. Подключите один конец второго сетевого кабеля к выходному порту сетевого ответвителя, а другой — к коммутатору.
4. Подключите один конец третьего сетевого кабеля к контрольному порту A сетевого ответвителя, а другой его конец — к одному сетевому адаптеру на компьютере, выполняющем роль анализатора пакетов.

5. Подключите один конец четвертого сетевого кабеля к контрольному порту B сетевого ответвителя, а другой – к другому сетевому адаптеру на компьютере, выполняющем роль анализатора пакетов.

В итоге неагрегированный сетевой ответвитель должен быть подключен к сети так, как показано на рис. 2.9.

Рис. 2.9. Применение неагрегированного сетевого ответвителя для перехвата сетевого трафика

Приведенные выше примеры могут навести на мысль, что с помощью сетевого ответвителя можно контролировать только одно устройство. Но на самом деле контролировать можно многие устройства, проявив творческий подход к размещению сетевого ответвителя. Так, если требуется полностью контролировать обмен данными между целым сегментом сети и Интернетом, сетевой ответвитель можно установить между коммутатором, к которому подключены все остальные устройства, и маршрутизатором восходящего потока данных в сети. Такое расположение в узком месте сети позволяет собирать требующийся сетевой трафик. Подобная стратегия обычно применяется при текущем контроле сетевой безопасности.

Выбор сетевого ответвителя

Какой же тип сетевого ответвителя лучше? Как правило, предпочтение следует отдавать агрегированным сетевым ответвителям, поскольку для них требуется меньше кабельной разводки и не нужно устанавливать два сетевых адаптера на компьютере анализатора пакетов. Но если требуется перехватывать большие объемы сетевого трафик или контролировать трафик, проходящий только в одном направлении, то лучше выбрать неагрегированный сетевой ответвитель.

Приобрести можно сетевые ответвители всех размеров: от простых ответвителей сети Ethernet за 150 долл. до оптоволоконных ответвителей корпоративного уровня, цена которых обозначается шестизначными цифрами. Мне лично приходилось пользоваться сетевыми ответвителями корпоративного уровня от компаний Ixia (бывшей Net Optics), Dualcomm и Fluke Networks, и я был ими очень доволен, хотя имеется много других замечательных сетевых ответвителей. Если вы предполагаете применять сетевой ответвитель на корпоративном уровне, убедитесь в достаточной его отказоустойчивости. Это означает, что если сетевой ответвитель неверно функционирует или выходит из строя, то он должен все равно пропускать пакеты, не нарушая связность сети на ее ответвляемом участке.

Заражение ARP-кеша

К числу наиболее предпочитаемых мною методик перехвата сетевого трафика относится заражение ARP-кеша. Более подробно сетевой протокол ARP будет рассматриваться в главе 7, "Протоколы сетевого уровня", а здесь приводится лишь краткое его описание, необходимое для понимания особенностей данной методики.

ARP-процесс

Как упоминалось в главе 1, "Анализ пакетов и основы организации сетей", в модели OSI адресация пакетов может осуществляться на двух уровнях — втором и третьем. Адреса второго уровня или MAC-адреса применяются вместе с выбранной вами системой адресации третьего уровня. В данной книге система адресации третьего уровня обозначается как *система IP-адресации* в соответствии с принятой в данной отрасли стандартной терминологией.

Все устройства в сети связываются вместе по IP-адресам на третьем уровне модели OSI. А поскольку коммутаторы действуют на втором уровне данной модели, то они осведомлены только о MAC-адресах второго уровня. Следовательно, для обмена пакетами между собой устройства должны включать в них информацию о MAC-адресах. Если же MAC-адрес неизвестен, он должен быть получен из известного IP-адреса третьего уровня, чтобы можно было пересылать сетевой трафик соответствующему устройству. И такой процесс преобразования адресов выполняется с помощью сетевого протокола ARP на втором уровне модели OSI.

Для компьютеров, подключенных к сетям Ethernet, ARP-процесс начинается в тот момент, когда одному компьютеру требуется связаться с другим. Сначала передающий компьютер проверяет свой ARP-кеш, чтобы выяснить, имеется ли в нем уже MAC-адрес, связанный с IP-адресом компьютера-получателя. Если такой адрес отсутствует, передающий компьютер посылает ARP-запрос

по широковещательному адресу `ff:ff:ff:ff:ff:ff` канального уровня, в котором указывает IP-адрес получателя, как пояснялось в главе 1, "Анализ пакетов и основы организации сетей". Формируемый в итоге широковещательный пакет принимается всеми компьютерами в данном конкретном сегменте сети Ethernet. По существу, этот пакет содержит такой запрос: "Какой MAC-адрес имеет компьютер с указанным IP-адресом?"

Те устройства, которые не соответствуют указанному в запросе IP-адресу получателя, просто игнорируют данный ARP-запрос. А компьютер, IP-адрес которого совпал с указанным в ARP-запросе, формирует ответный ARP-пакет, в котором указывает свой MAC-адрес. Таким образом, исходный передающий компьютер получает информацию об адресации канального уровня, которая требуется ему для связывания с удаленным компьютером. И эту информацию он сохраняет в своем ARP-кеше для быстрого ее извлечения.

Принцип действия заражения ARP-кеша

Заражение ARP-кеша, иногда еще называемое *ARP-подменой*, является усовершенствованной формой подключения к коммутируемой сети с целью ее прослушивания. Принцип его действия состоит в том, чтобы посылать ARP-сообщения коммутатору или маршрутизатору сети Ethernet с поддельными MAC-адресами (второго уровня) для перехвата сетевого трафика другого компьютера, как наглядно показано на рис. 2.10.

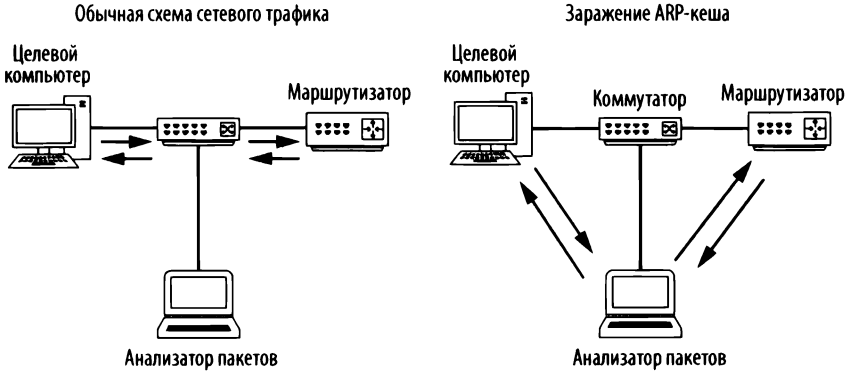

Рис. 2.10. Заражение ARP-кеша позволяет перехватывать сетевой трафик целевого компьютера

Такая методика обычно применяется атакующими злоумышленниками для посылки ложно адресуемых пакетов клиентским системам, чтобы перехватить определенный сетевой трафик или вызвать атаку типа отказа в обслуживании (DoS) на целевой компьютер. Но данную методику можно применять и вполне законно для перехвата пакетов целевого компьютера в коммутируемой сети.

Применение Cain & Abel

Прежде чем пытаться применить заражение ARP-кеша, следует приобрести необходимые инструментальные средства и собрать некоторую информацию. В целях демонстрации данной методики воспользуемся распространенным инструментальным средством защиты Cain & Abel от компании oxid.it (`http://www.oxid.it/`), которое поддерживает операционные системы Windows. Загрузите и установите это инструментальное средство, следуя инструкциям на веб-сайте по указанному выше адресу.

ПРИМЕЧАНИЕ *При попытке загрузить инструментальное средство Cain & Abel, вероятнее всего, антивирусная программа или браузер отметит его как зловредное программное обеспечение или "хакерское инструментальное средство". Оно действительно находит самое разное применение, включая и злонамеренное. Но для рассматриваемых здесь целей оно не представляет никакой угрозы вашей системе.*

Прежде чем воспользоваться Cain & Abel, вам придется собрать определенную информацию, включая IP-адрес вашей анализирующей пакеты системы, удаленной системы, откуда вы хотели бы перехватывать сетевой трафик, а также маршрутизатора, от которого удаленная система получает нисходящий поток данных.

Открыв Cain & Abel в первый раз, вы заметите ряд вкладок у верхнего края главного окна. Ведь заражение ARP-кеша — это лишь одна из функциональных возможностей Cain & Abel. Для рассматриваемых здесь целей выберите вкладку **Sniffer** (Анализатор пакетов). Щелкнув на этой вкладке, вы должны увидеть пустую таблицу (рис. 2.11).

Чтобы заполнить эту таблицу, вам придется активизировать встроенный в Cain & Abel анализатор пакетов и просканировать хосты в своей сети. С этой целью выполните следующие действия.

1. Щелкните на второй слева пиктограмме с изображением сетевого адаптера на панели инструментов.
2. Вам будет предложено выбрать интерфейс для анализа пакетов. Выберите интерфейс, подключенный к той сети, где вы будете выполнять заражение ARP-кеша. Если это ваша первая попытка воспользоваться средствами Cain & Abel, выберите этот интерфейс и щелкните на кнопке **OK**. А если вы выбирали интерфейс в Cain & Abel прежде, то результат вашего выбора был сохранен, и вам нужно лишь щелкнуть на пиктограмме с изображением сетевого адаптера еще раз, чтобы выбрать подходящий интерфейс. (Убедитесь, что кнопка с этой пиктограммой находится в нажатом состоянии, чтобы активизировать встроенный в Cain & Abel анализатор пакетов.)

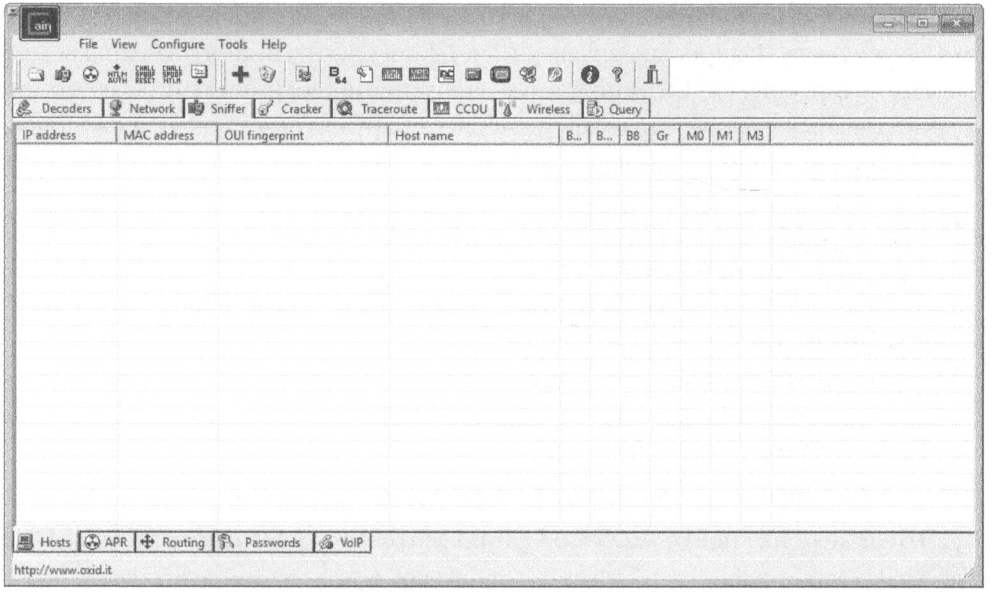

Рис. 2.11. Вкладка Sniffer *в главном окне Cain & Abel*

3. Чтобы составить список хостов, имеющихся в вашей сети, щелкните на кнопке со знаком "плюс" (+). Откроется диалоговое окно MAC Address Scanner (Сканер MAC-адресов), как показано на рис. 2.12. В этом окне должен быть выбран переключатель All hosts in my subnet (Все хосты в подсети), либо вы можете указать диапазон адресов. Щелкните на кнопке OK, чтобы продолжить дальше.

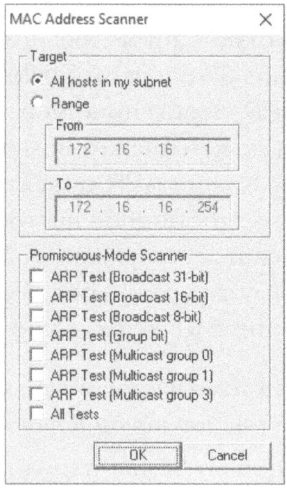

Рис. 2.12. Сканирование MAC-адресов средствами Cain & Abel для обнаружения узлов сети

Некоторые пользователи Windows 10 жалуются, что Cain & Abel не в состоянии определить IP-адрес их сетевых интерфейсов, что препятствует завершению данного процесса. Если подобное затруднение возникнет и у вас, то при настройке своих сетевых интерфейсов вы обнаружите, что их IP-адрес равен `0.0.0.0`. Чтобы выйти из этого затруднения, выполните следующие действия.

1. Если инструментальное средство Cain & Abel открыто, закройте его.
2. Введите **`ncpa.cpl`** в строке поиска на рабочем столе операционной системы, чтобы открыть диалоговое окно Network Connections (Сетевые подключения).
3. Щелкните сначала правой кнопкой мыши на сетевом интерфейсе, из которого вы собираетесь выполнять анализ пакетов, а затем на кнопке Properties (Свойства).
4. Дважды щелкните на опции Internet Protocol Version 4 (TCP/IPv4).
5. Щелкните на кнопке Advanced (Дополнительно) и выберите вкладку DNS.
6. Установите флажок рядом с меткой Use this connection's DNS suffix in DNS registration (Использовать DNS-суффикс для подключения при регистрации в DNS), чтобы активизировать соответствующий режим.
7. Щелкните на кнопке OK, чтобы выйти из открытых диалоговых окон, а затем перезапустите Cain & Abel.

В итоге таблица должна заполниться списком всех хостов, подключенных к вашей сети, наряду с их MAC-адресами, IP-адресами и сведениями о производителях. Именно с этим списком вам придется работать при настройке заражения ARP-кеша.

У нижнего края рабочего окна Cain & Abel должен появиться ряд вкладок для перехода в другие окна под заголовком Sniffer. Итак, составив список хостов, перейдите на вкладку APR, чтобы приступить к работе по методике заражения ARP-кеша в соответствующем диалоговом окне.

В открывшемся диалоговом окне APR появятся две пустые таблицы. По окончании приведенных ниже действий по настройке в верхней таблице появятся устройства, задействованные в заражении ARP-кеша, а в нижней таблице – весь обмен данными между зараженными вами машинами.

Чтобы настроить заражение ARP-кеша, выполните следующие действия.

1. Щелкните сначала на пустом участке в верхней части экрана, а затем на кнопке со знаком "плюс" (+) стандартной панели инструментов Cain & Abel.
2. В открывшемся окне появятся две панели выбора. Слева вы увидите список всех хостов, имеющихся в вашей сети. Если вы щелкнете на IP-адресе целевого компьютера, то в панели справа появится список

всех хостов в вашей сети, кроме хоста, имеющего IP-адрес целевого компьютера.

3. Щелкните сначала в правой панели на IP-адресе маршрутизатора, непосредственно направляющего поток данных, исходящий из целевого компьютера (рис. 2.13), а затем на кнопке OK. В итоге IP-адреса обоих устройств должны появиться в верхней таблице в главном окне прикладной программы.
4. Чтобы завершить процесс, щелкните на черно-желтом знаке радиации, что на стандартной панели инструментов. Это приведет к активизации средств Cain & Abel для заражения ARP-кеша и позволит вашей анализирующей пакеты системе стать посредником во всех обменах данными между целевой системой и маршрутизатором восходящего потока.

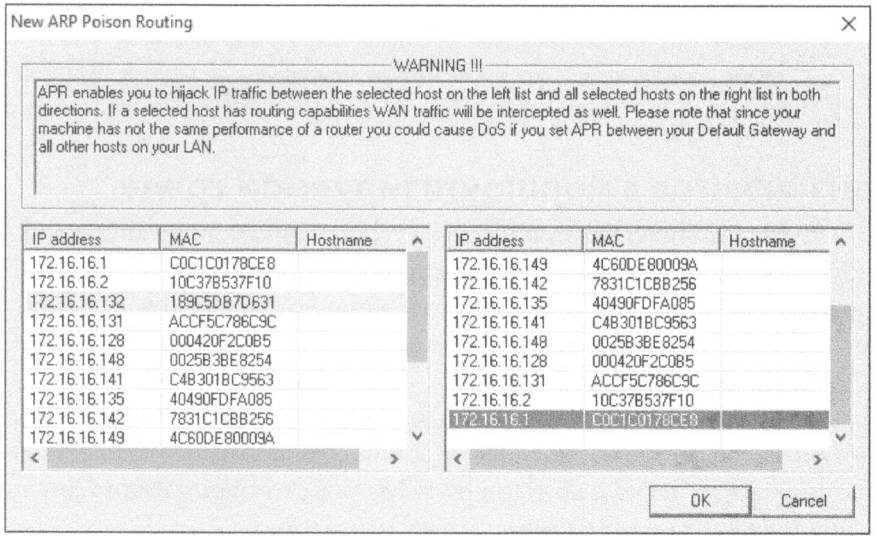

Рис. 2.13. Выбор устройств, для которых требуется активизировать заражение ARP-кеша

Теперь вы сможете запустить свой анализатор пакетов и приступить к процессу их анализа. Завершив перехват сетевого трафика, щелкните еще раз на черно-желтом знаке радиации, чтобы прекратить заражение ARP-кеша.

Предупреждение о заражении ARP-кеша

В качестве заключительного замечания по поводу заражения ARP-кеша хочется сказать, что вы должны учитывать назначение тех систем, для которых реализуется данный процесс. Данную методику не следует, в частности, применять для устройств с очень высокой степенью использования в сети.

Примером тому служит файловый сервер, имеющий канал связи с сетью на скорости 1 Гбит/с, особенно когда система анализа пакетов подключена на скорости только 100 Мбит/с.

Когда сетевой трафик перенаправляется по методике, представленной в данном примере, весь трафик, передаваемый и получаемый целевой системой, должен сначала пройти через систему анализа пакетов, а следовательно, она станет узким местом в процессе обмена данными. Такая перемаршрутизация может иметь эффект вроде отказа в обслуживании на анализируемой машине, что в конечном счете приведет к снижению производительности сети и получению ложных данных анализа. Перегрузка по трафику может также воспрепятствовать нормальному обмену данными по сетевому протоколу SSL.

ПРИМЕЧАНИЕ *Чтобы исключить прохождение всего сетевого трафика через вашу систему анализа пакетов, воспользуйтесь таким средством, как асимметричная маршрутизация. Подробнее с этой методикой можно ознакомиться в разделе APR руководства пользователя Cain & Abel (*`http://www.oxid.it/ca_um/topics/apr.htm`*).*

Анализ пакетов в маршрутизируемой среде

Все методики подключения к коммутируемым сетям доступны и для маршрутизируемых сетей. Для работы в маршрутизируемых средах следует лишь обращать особое внимание на местоположение анализатора пакетов, когда устраняются неполадки, охватывающие несколько сегментов сети.

Как вам должно быть уже известно, широковещательный домен целевого устройства простирается вплоть до маршрутизатора, где сетевой трафик передается следующему маршрутизатору восходящего потока. Если данные должны проходить несколько маршрутизаторов, то очень важно анализировать сетевой трафик со всех сторон маршрутизатора.

В качестве примера рассмотрим затруднение, которое может возникнуть в сети с несколькими сегментами, соединенными через ряд маршрутизаторов. В такой сети каждый сегмент связывается с восходящим сегментом для сохранения и извлечения данных. Затруднение, которое мы пытаемся разрешить, состоит в том, что нисходящая подсеть (т.е. сеть Г на рис. 2.14) не может связаться ни с одним из устройств в сети А.

Если проанализировать трафик устройства в сети Г, испытывающего трудности связывания с устройствами в других сетях, можно явно обнаружить данные, передаваемые в другой сегмент сети, но не обнаружить данные, поступающие обратно. Если же изменить положение анализатора пакетов и приступить к анализу сетевого трафика в следующем восходящем сегменте сети (т.е. в сети Б), то можно обнаружить, что сетевой трафик пропускается или

неверно направляется маршрутизатором сети Б. В конечном итоге это приведет к проблеме настройки маршрутизатора, разрешив которую можно разрешить и более крупную дилемму. И хотя рассматриваемый здесь случай выглядит несколько общим, из него можно сделать следующий важный вывод: когда приходится иметь дело с несколькими маршрутизаторами и сетевыми сегментами, анализатор пакетов придется устанавливать в разных местах сети, чтобы получить полную картину происходящего и точно определить возникшее в ней затруднение.

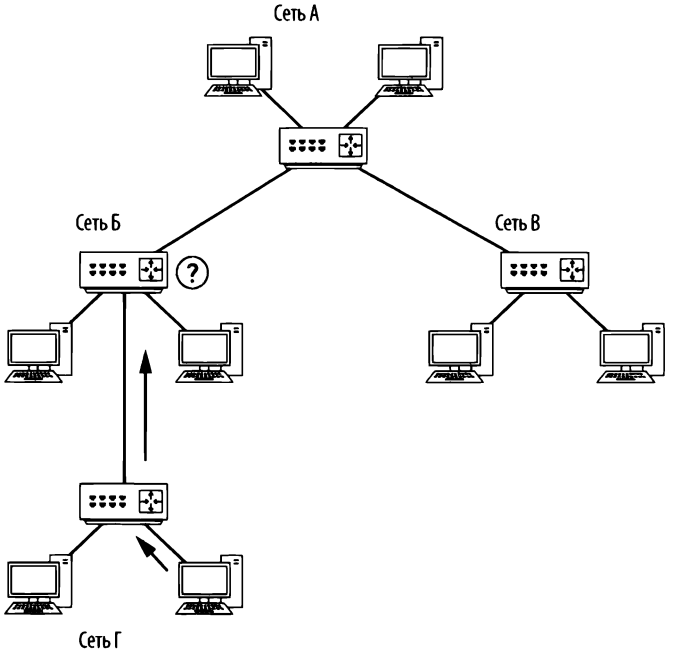

Рис. 2.14. Компьютер в сети Г не может связаться с компьютерами в сети А

КАРТЫ СЕТИ

Обсуждая расположение анализатора пакетов в сети, мы исследовали несколько так называемых карт сети. *Карта*, или *схема*, сети показывает все технические ресурсы в сети и порядок их соединения.

Чтобы определить место для расположения анализатора пакетов в сети, лучше всего представить ее наглядно. Если у вас имеется карта сети, держите ее под рукой, поскольку она является весьма ценным ресурсом для процесса диагностики и анализа. Для этого вам, возможно даже, придется составить подробную карту своей сети. Помните, что иногда половину дела в устранении неисправностей обеспечивает сбор надлежащих данных.

Размещение анализатора пакетов на практике

Мы рассмотрели четыре способа перехвата сетевого трафика в коммутируемой среде. К ним можно добавить еще один, для чего достаточно рассмотреть установку приложения для анализа пакетов на одном устройстве, из которого требуется перехватывать сетевой трафик (такая методика называется *прямой установкой*). Из этих пяти способов не так-то просто выбрать наиболее подходящий. Поэтому в табл. 2.2 сведены основные положения по каждому способу и соответствующей методике анализа пакетов.

Исследователям пакетов необходимо действовать как можно более скрытно. В идеальном случае требующиеся данные следует собирать, не оставляя следов. Подобно тому, как следователи-криминалисты не должны портить место преступления, так и аналитикам пакетов не следует портить перехватываемый сетевой трафик.

Таблица 2.2. Основные положения по анализу пакетов в коммутируемой среде

Методика	Основные положения
Зеркальное отображение портов	• Не оставляет следы и не формирует дополнительные пакеты • Можно настроить, не отключая клиента от сети, что удобно при зеркальном отображении портов маршрутизатора или сервера • Задействует ресурсы коммутатора для целей обработки и может быть неприемлемой при высоком трафике
Перехват пакетов через концентратор	• Подходит в тех случаях, когда хост можно безболезненно отключить от сети • Не дает желаемого эффекта, когда требуется перехватить сетевой трафик из нескольких хостов, поскольку в этом случае вполне возможны коллизии и потеря пакетов • Может привести к потере пакетов в современных хостах, работающих на скорости 100–1000 Мбит/с, поскольку большинство настоящих концентраторов работают на скорости лишь 10 Мбит/с
Применение сетевого ответвителя	• Идеально подходит в том случае, если хост можно безболезненно отключить от сети • Единственная возможность, когда требуется проанализировать сетевой трафик по оптоволоконному соединению • Наиболее предпочтительное решение для перехвата пакетов и непрерывного контроля сети в корпоративной среде, поскольку сетевые ответвители весьма надежны и допускают наращивание до масштабов каналов связи с высокой пропускной способностью • Сетевые ответвители предназначены для решения насущных задач и вполне соответствуют уровням скоростей в современных сетях, что выгодно отличает данную методику от перехвата пакетов через концентратор • Может обойтись недешево, особенно в крупных масштабах, а следовательно, применять данную методику невыгодно

Окончание табл. 2.2

Методика	Основные положения
Заражение ARP-кеша	• Считается весьма нестабильной методикой, поскольку требует внедрения пакетов в сеть с целью перенаправить сетевой трафик через анализатор пакетов • Если зеркальное отображение портов невозможно, то может оказаться эффективной методикой для быстрого перехвата сетевого трафика из целевого устройства, не отключая его от сети • Требует особой аккуратности, чтобы не оказывать влияния на функционирование сети
Прямая установка	• Обычно не рекомендуется, ведь если возникнут трудности в работе хоста, они могут привести к потере пакетов или такому манипулированию ими, что они не будут представлены точно • От сетевого адаптера хоста не требуется поддержки смешанного режима работы • Лучше всего подходит для тестовых сред, исследования или сравнения с исходными характеристиками производительности, анализа файлов перехвата, создаваемых в других местах сети

Перейдя к практическим сценариям в последующих главах, мы обсудим наилучшие способы перехвата требующихся данных в каждом конкретном случае. А пока обратите внимание на рис. 2.15, на котором приведена блок-схема, призванная помочь вам выбрать наилучшую методику для перехвата сетевого трафика в конкретной ситуации. На этой блок-схеме во внимание приняты самые разные факторы, начиная с места для перехвата пакетов: дома или на работе, но она служит лишь в качестве общей справки и не охватывает все возможные сценарии подключения к сети с целью прослушивания и анализа пакетов.

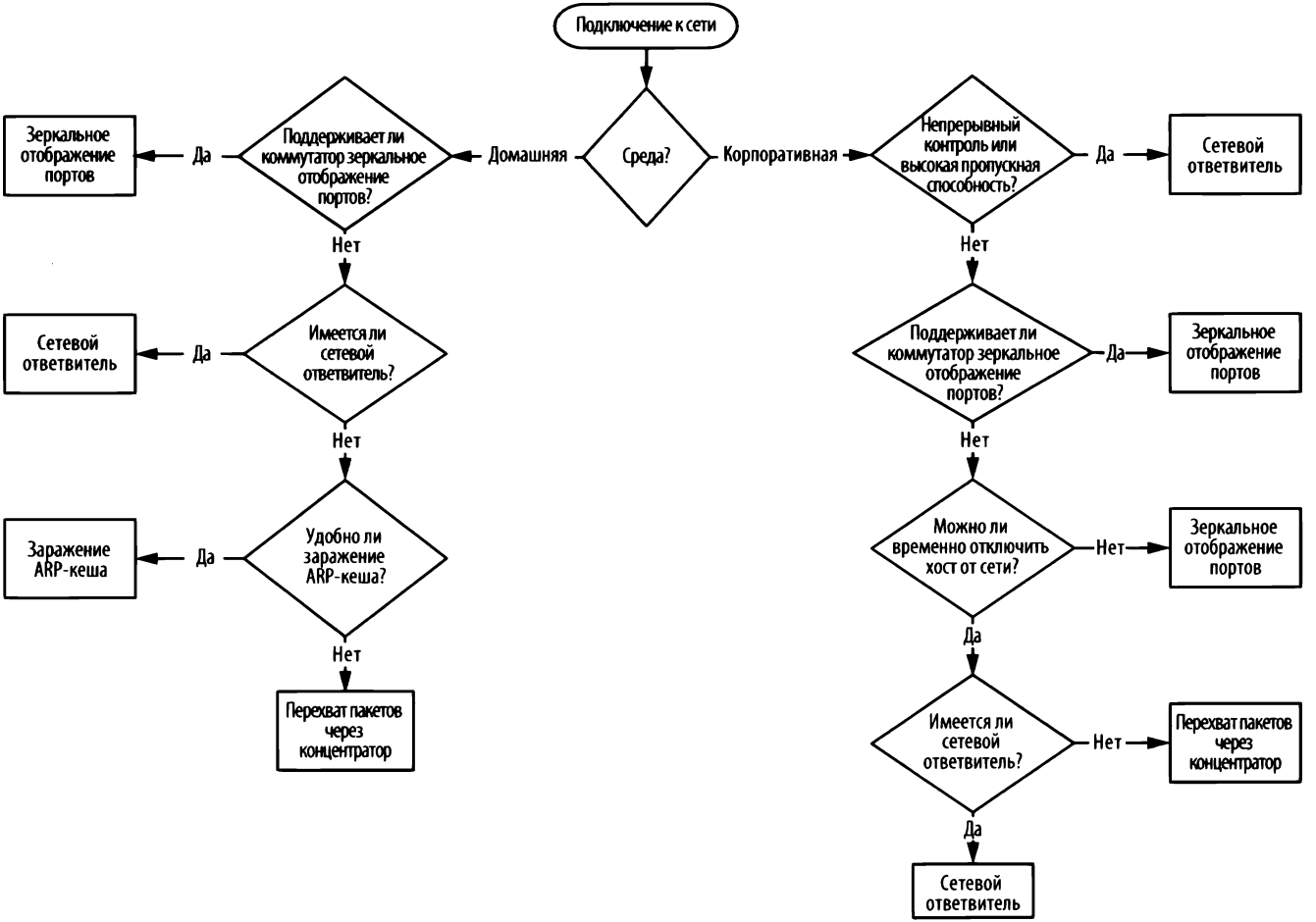

Рис. 2.15. Блок-схема, оказывающая помощь в выборе наилучшей методики для подключения к сети с целью прослушивания и анализа пакетов

3

ВВЕДЕНИЕ В WIRESHARK

Как упоминалось в главе 1, "Анализ пакетов и основы организации сетей", для анализа сетевых пакетов имеется несколько приложений, но в этой книге основное внимание уделяется приложению Wireshark. А в этой главе представлено введение в Wireshark.

Краткая история создания Wireshark

У приложения Wireshark очень богатая история. Джеральд Комбс (Gerald Combs), окончивший курс вычислительной техники в университете штата Миссури, расположенном в Канзас-Сити, разработал это приложение по необходимости. Первая версия его приложения была выпущена под названием Ethereal в 1998 году по универсальной общедоступной лицензии GNU (GPL).

Через восемь лет после выпуска версии Ethereal Комбс оставил свою работу в поисках других карьерных возможностей. К сожалению, у его тогдашнего работодателя остались все права на торговую марку Ethereal, и поэтому Комбсу не удалось добиться согласия на получение контроля над фирменным названием Ethereal. Поэтому Комбс и остальные члены команды разработчиков переименовали свой проект на *Wireshark* в середине 2006 года.

Ныне популярность приложения Wireshark существенно возросла, а в его разработке приняло участие более 500 специалистов. В то же время приложение, существующее под названием Ethereal, больше не разрабатывается.

Преимущества Wireshark

Приложение Wireshark дает ряд преимуществ, благодаря которым оно оказывается весьма привлекательным для повседневного применения. Оно рассчитано на разные категории аналитиков пакетов: от начинающих до опытных, предоставляя заманчивые возможности как для тех, так и для других. Итак, исследуем возможности Wireshark по критериям, определенным в главе 1, "Анализ пакетов и основы организации сетей", для выбора инструментальных средств анализа пакетов.

- **Поддержка сетевых протоколов.** Wireshark отличается поддержкой целого ряда сетевых протоколов – на момент написания этой книги их насчитывалось около 1000. К числу поддерживаемых сетевых протоколов относятся как общеупотребительные протоколы вроде IP и DHCP, так и более развитые специализированные протоколы вроде DNP3 и BitTorrent. А поскольку приложение Wireshark разработано по модели открытого исходного кода, то при каждом его обновлении вводится поддержка нового сетевого протокола.

ПРИМЕЧАНИЕ *В том маловероятном случае, если требующийся вам сетевой протокол не поддерживается в Wireshark, можете запрограммировать его поддержку сами. После этого передайте свой исходный код разработчикам Wireshark на рассмотрение, чтобы включить его в данное приложение. Узнать о том, что требуется для участия со своим исходным кодом в проекте Wireshark, можно по адресу* `https://www.wireshark.org/develop.html`.

- **Удобство для пользователей.** Интерфейс Wireshark – самый простой для усвоения среди всех приложений для анализа пакетов. Он создан на основе графического интерфейса с ясно составленными контекстными меню и простой компоновкой. Кроме того, в нем предоставляется ряд средств, предназначенных для повышения удобства его практического применения, в том числе выделение сетевых протоколов разным цветом и подробное графическое представление исходных данных. В отличие от некоторых более сложных приложений, работающих в режиме командной строки (например, утилиты `tcpdump`), интерфейс приложения Wireshark вполне доступен тем, кто делает только первые шаги в области анализа пакетов.
- **Стоимость.** Приложение Wireshark совершенно бесплатно, поскольку оно выпущено по универсальной общедоступной лицензии GNU (GPL). Его можно свободно загрузить и применять в любых целях: как в личных, так и в коммерческих.

ПРИМЕЧАНИЕ *Несмотря на то что приложение Wireshark может быть получено бесплатно, некоторые по ошибке внесли за него плату. Если вы ищете анализаторы пакетов на электронном аукционе eBay, вас может удивить, сколько людей готовы продать "профессиональную корпоративную лицензию" на Wireshark всего лишь за 39,95 долларов. Если вы действительно решите приобрести такую лицензию, свяжитесь со мной, и мы сможем обсудить выгодные варианты приобретения недвижимости с видом на океан, которые я мог бы предложить вам у себя в Кентукки!*

- **Поддержка программы.** Уровень поддержки программного обеспечения может решить его судьбу. Свободно распространяемое программное обеспечение вроде Wireshark может и не иметь никакой формальной поддержки. Поэтому сообщество разработчиков программного обеспечения с открытым исходным кодом нередко опирается на свою базу пользователей для оказания помощи. К счастью для нас, сообщество разработчиков Wireshark относится к числу самых активных. В частности, ссылки на веб-сайте, посвященном приложению Wireshark, направляют непосредственно к нескольким формам поддержки, включая оперативно доступную документацию, вики-страницы, часто задаваемые вопросы и место для подписки на список рассылки, который контролируется большинством главных разработчиков Wireshark. Имеется также платная поддержка Wireshark со стороны компании Riverbed Technology.
- **Доступ к исходному коду.** Wireshark относится к категории программного обеспечения с открытым исходным кодом, который доступен в любой момент. Это может оказаться удобным для поиска и устранения неисправностей в данном приложении, понимании принципа действия дешифраторов сетевых протоколов или внесения своего вклада в разработку Wireshark.
- **Поддержка операционных систем.** В приложении Wireshark поддерживаются все основные современные операционные системы, включая Windows, Linux и Mac OS X. Полный перечень поддерживаемых операционных систем можно посмотреть на начальной странице веб-сайта, посвященного приложению Wireshark.

Установка Wireshark

Процесс установки Wireshark удивительно прост. Но прежде чем установить Wireshark, убедитесь, что ваша система отвечает следующим требованиям.

- Любой современный 32- или 64-разрядный ЦП типа x86.
- 400 Мбайт доступной оперативной памяти, хотя для крупных файлов перехвата потребуется больший объем памяти.
- Не меньше 300 Мбайт на жестком диске плюс место для файлов перехвата.
- Сетевой адаптер, поддерживающий комбинированный (promiscuous mode) режим работы.
- Драйвер перехвата WinPcap/libpcap.

Драйвер перехвата WinPcap является реализованным в Windows вариантом pcap — интерфейса API для перехвата пакетов. Проще говоря, этот драйвер взаимодействует с операционной системой для перехвата исходных данных пакета, применения фильтров и переключения сетевого адаптера в комбинированный режим, и обратно.

Несмотря на то что драйвер WinPcap можно загрузить отдельно (по адресу `http://www.winpcap.org/`), его, как правило, лучше устанавливать из дистрибутивного пакета Wireshark, поскольку версия драйвера WinPcap, входящая в этот пакет, уже проверена на работоспособность вместе с Wireshark.

Установка в системах Windows

Текущая версия Wireshark проверена на работоспособность в разных версиях ОС Windows, которые поддерживаются до сих пор их производителем. На момент написания этой книги к поддерживаемым относились версии Windows Vista, Windows 7, Windows 8, Windows 10, а также Windows Server 2003, 2008 и 2012. И хотя Wireshark зачастую будет работать и в других версиях Windows (вроде Windows XP), официально эти версии не поддерживаются.

Для установки Wireshark в ОС Windows прежде всего необходимо получить последнюю версию сборки установочного пакета с официального веб-сайта Wireshark по адресу `http://www.wireshark.org/`. С этой целью перейдите в раздел **Download** (Загрузки) этого веб-сайта и выберите нужный вариант установочного пакета в зависимости от применяемой версии Windows. А после загрузки установочного пакета выполните следующие действия.

1. Дважды щелкните на файле с расширением **.exe**, чтобы начать установку, а затем щелкните на кнопке Next (Далее) во вступительном окне.
2. Прочитайте лицензионное соглашение и, если согласны с ним, щелкните на кнопке I Agree (Соглашаюсь).
3. Выберите компоненты Wireshark, которые требуется установить, как показано на рис. 3.1. Для своих целей можете принять выбранные по умолчанию компоненты и щелкнуть на кнопке Next.

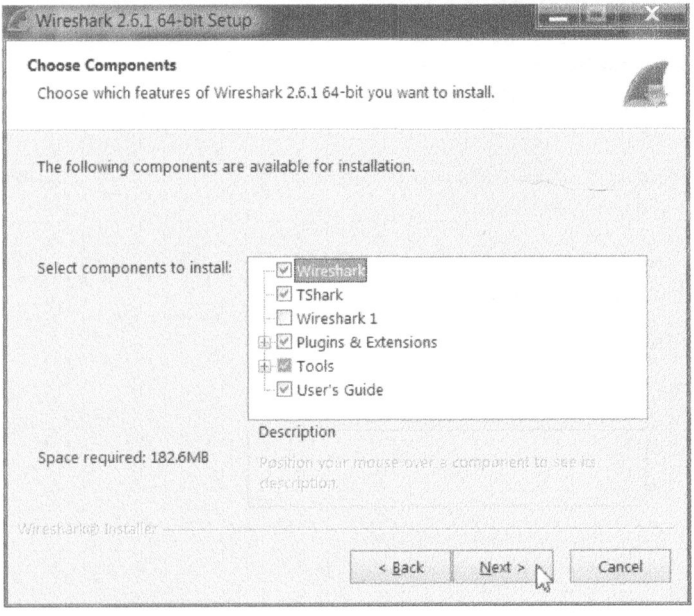

Рис. 3.1. Выберите компоненты Wireshark, которые требуется установить

4. Щелкните на кнопке Next в открывшемся окне Select Additional Tasks (Выбор дополнительных задач).
5. Выберите место для установки Wireshark и щелкните на кнопке Next.
6. Когда появится диалоговое окно, в котором запрашивается установка драйвера WinPcap, установите сначала флажок Install WinPcap (Установить драйвер WinPcap), как показано на рис. 3.2, а затем щелкните на кнопке Install. В итоге должен начаться процесс установки.
7. Далее вам представится возможность установить USBPcap — утилиту для сбора данных из USB-устройств. Установите соответствующий флажок, если желаете установить эту утилиту, а затем щелкните на кнопке Next.
8. Где-то посредине процесса установки Wireshark должна начаться установка драйвера WinPcap. И как только это произойдет, щелкните на кнопке Next во вступительном окне, прочитайте лицензионное соглашение и, если согласны с ним, щелкните на кнопке I Agree.
9. В итоге выбранный драйвер WinPcap и утилита USBPcap должны быть установлены на вашем компьютере. По окончании данной установки щелкните на кнопке Finish (Готово).
10. На этом установка Wireshark должна быть завершена. И как только это произойдет, щелкните на кнопке Next.
11. Щелкните на кнопке Finish в открывшемся окне подтверждения установки Wireshark.

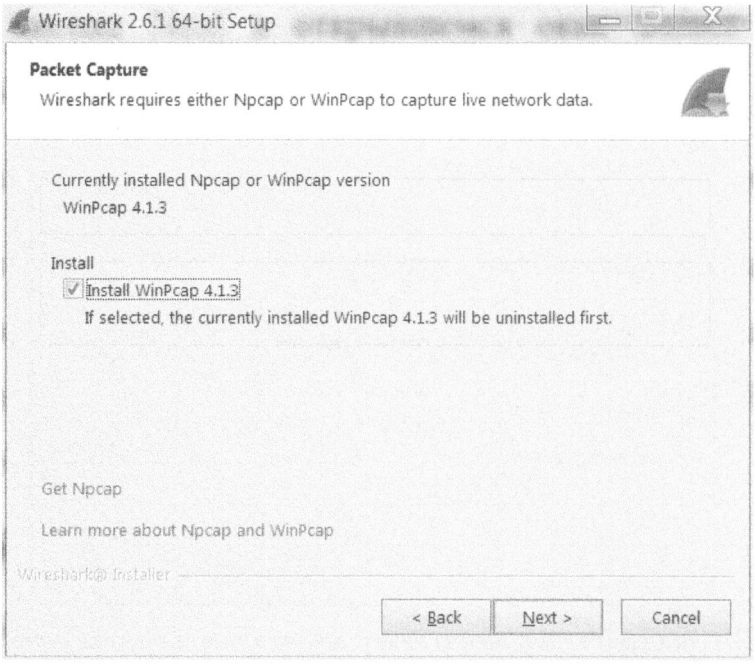

Рис. 3.2. Выбор варианта установки драйвера WinPcap

Установка в системах Linux

Приложение Wireshark работает на большинстве современных платформ, построенных на основе ОС Unix. Его можно установить с помощью одного из диспетчеров дистрибутивных пакетов или же загрузив и установив дистрибутивный пакет, подходящий для вашей операционной системы. Было бы нереально охватить все процедуры установки в каждой версии ОС Linux, поэтому рассмотрим лишь некоторые из них.

Как правило, для установки системного программного обеспечения в ОС Unix требуется права доступа суперпользователя (`root`). Но для установки локальных версий программного обеспечения, скомпилированных из исходного кода, права суперпользователя не требуется.

Системы на основе RPM-пакетов

Если вы пользуетесь версией Red Hat Linux или основанным на ней дистрибутивом вроде CentOS, то в этой ОС, скорее всего, имеется устанавливаемое по умолчанию инструментальное средство Yum для управления пакетами. В таком случае для быстрой установки приложения Wireshark вам достаточно извлечь его из хранилища дистрибутивного программного обеспечения. С этой целью откройте окно терминала и введите в нем следующую команду:

```
$ sudo yum install wireshark
```

Если потребуются какие-нибудь дополнительные зависимости, вам будет предложено установить и их. Если же все пройдет удачно, вы сможете запустить приложение Wireshark на выполнение из командой строки и получить к нему доступ через графический интерфейс.

Системы на основе DEB-пакетов

В состав большинства дистрибутивов на основе DEB-пакетов, например Debian или Ubuntu, входит инструментальное средство APT для управления пакетами. Оно позволяет установить Wireshark из хранилища программного обеспечения ОС. Чтобы установить Wireshark с помощью этого инструментального средства, откройте окно терминала и введите в нем следующую команду:

```
$ sudo apt-get install wireshark wireshark-qt
```

И в этом случае вам будет предложено установить любые зависимости, чтобы завершить процесс установки.

Компиляция исходного кода Wireshark

В силу изменений в архитектуре операционной системы и функциональных средствах Wireshark инструкции по компиляции исходного кода Wireshark могут со временем меняться. И это одна из причин, по которым рекомендуется пользоваться диспетчером пакетов операционной системы для установки данного приложения. Но если в вашем дистрибутиве Linux не применяется программное обеспечение для автоматического управления пакетами или вам требуется специальная установка Wireshark, то у вас есть возможность установить данное приложение вручную, скомпилировав его исходный код. С этой целью выполните следующие действия.

1. Загрузите исходный пакет с соответствующей страницы веб-сайта, посвященного Wireshark по указанному ранее адресу.
2. Извлеките архив, введя следующую команду и подставив в ней соответствующее имя файла загруженного пакета:

```
$ tar -jxvf <укажите здесь имя файла пакета>.tar.bz2
```

3. Прежде чем выбирать конфигурацию и устанавливать Wireshark, возможно, придется установить ряд дополнительных пакетов в зависимости от выбранной вами версии Linux. Например, в Ubuntu 14.04 требуется установить ряд дополнительных пакетов для нормальной работы

Wireshark. И это можно сделать по приведенной ниже команде. Но для этого потребуются права доступа суперпользователя, а иначе придется сначала ввести команду **sudo**.

```
$ sudo apt-get install pkg-config bison flex qt5-default libgtk-3-dev
  libpcap-dev qttools5-dev-tools
```

4. Установив требуемые дополнительные пакеты, перейдите к тому каталогу, в который были извлечены исходные файлы Wireshark.
5. Настройте исходный код на правильную его сборку в вашем дистрибутиве Linux по команде **./configure**. Если вы желаете изменить стандартные параметры установки, укажите их на данной стадии установки. Если же какие-нибудь зависимости (т.е. дополнительные пакеты) отсутствуют, то компиляция исходного кода, скорее всего, завершится с ошибкой. Поэтому установите и настройте отсутствующие зависимости, прежде чем продолжить дальше. И если настройка пройдет удачно, вы увидите сообщение, извещающее об этом, как показано на рис. 3.3.

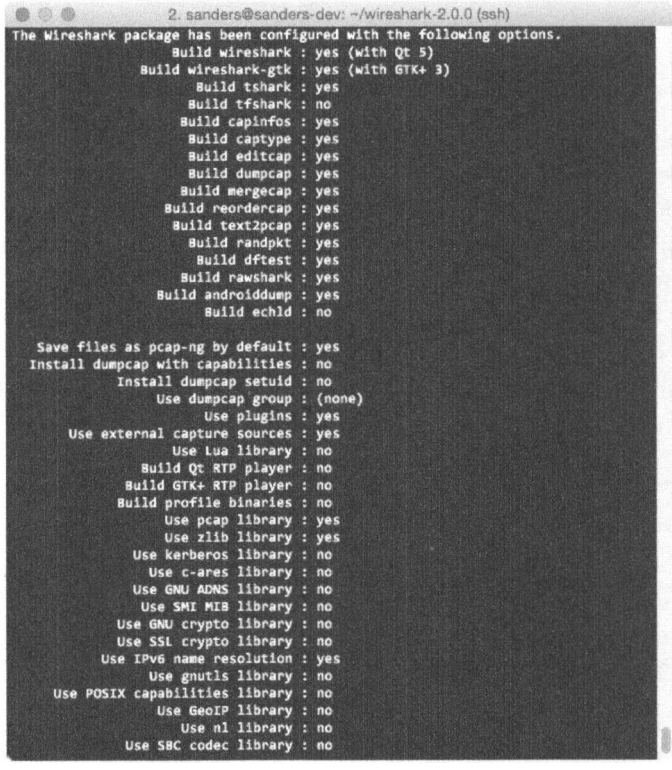

*Рис. 3.3. При удачном завершении команды **./configure** появится приведенное здесь сообщение с выбранными настройками*

6. Введите команду **make**, чтобы скомпилировать исходный код и собрать двоичный исполняемый файл.
7. Запустите завершающую стадию установки по команде **sudo make install**.
8. Выполните команду **sudo /sbin/ldconfig**, чтобы завершить процесс установки.

ПРИМЕЧАНИЕ *Если при выполнении описанных выше действий возникнут какие-нибудь ошибки, возможно, придется установить еще один дополнительный пакет.*

Установка в системах Mac OS X

Чтобы установить Wireshark в одной из систем Mac OS X, выполните следующие действия.

1. Загрузите установочный пакет для Mac OS X с соответствующей страницы веб-сайта, посвященного Wireshark по указанному ранее адресу.
2. Запустите на выполнение утилиту в виде мастера установки и далее следуйте указанным в нем инструкциям. Приняв условия лицензии конечного пользователя, выберите место для установки Wireshark.
3. Завершите процесс установки в соответствующем мастере.

Основы работы в Wireshark

Установив успешно приложение Wireshark в своей системе, можете приступить к его изучению. Открыв полностью функционирующий анализатор пакетов, вы не увидите в нем практически ничего интересного! А дело в том, что для анализа пакетов Wireshark требуются какие-нибудь данные.

Первый перехват пакетов

Чтобы ввести данные пакетов в Wireshark, вам придется сделать свой первый перехват пакетов. И здесь у вас может возникнуть следующий вопрос: "Как же мне перехватывать пакеты, если в моей сети все в порядке?"

Во-первых, в сети *всегда* что-нибудь да не так. Если не верите, пошлите сообщение по электронной почте всем пользователям своей сети, известив их, что все работает идеально. Во-вторых, для анализа пакетов совсем не обязательно, чтобы в сети было что-нибудь не так. На самом деле аналитики пакетов большую часть своего рабочего времени тратят на анализ исправного, а не проблемного сетевого трафика. Ведь нужно же иметь какое-то исходное основание для сравнения, чтобы эффективно исправить сетевой трафик. Так,

если вы надеетесь разрешить затруднение, связанное с сетевым протоколом DHCP, проанализировав его трафик, то должны знать, каким образом выглядит поток рабочего трафика по протоколу DHCP.

В более широком смысле, чтобы найти аномалии в повседневной работе сети, необходимо знать, каким образом выглядит эта повседневная работа. Если ваша сеть работает бесперебойно, то ваши наблюдения за ней послужат исходным основанием для представления сетевого трафика в его нормальном состоянии.

Итак, перехватите немного пакетов, выполнив следующие действия:

1. Откройте Wireshark.
2. Выберите команду Capture⇨Options (Перехват⇨Параметры) из главного меню. В итоге должно появиться диалоговое окно, где перечислены различные сетевые интерфейсы, которые могут быть использованы для перехвата пакетов, а также самые основные сведения о каждом из них (рис. 3.4). Обратите внимание на столбец Traffic, в котором приведен линейный график, наглядно показывающий объем сетевого трафика, проходящего в настоящий момент через данный интерфейс. Пиковые точки на этом графике фактически указывают на перехват пакетов. Если они отсутствуют, линейный график должен быть плоским. Кроме того, каждый интерфейс можно расширить, щелкнув на стрелке слева от него, чтобы увидеть связанную с ним информацию об адресации, например, MAC-адрес или IP-адрес.

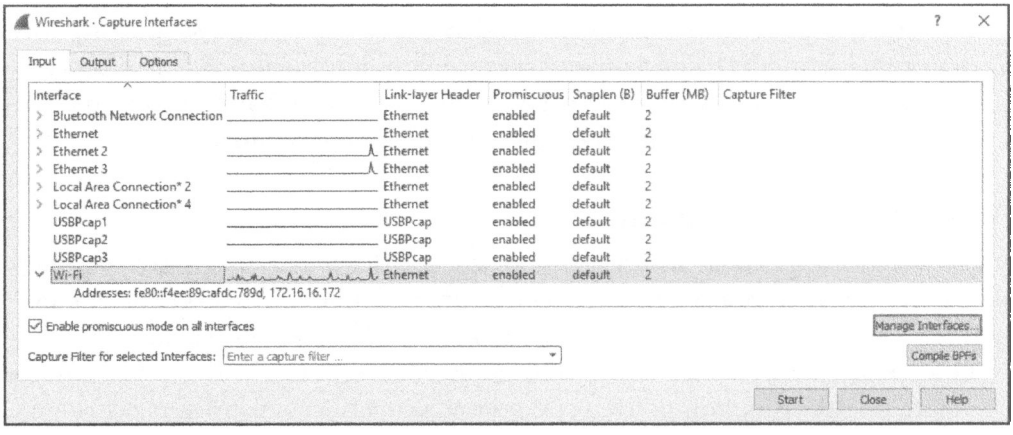

Рис. 3.4. Выбор сетевого интерфейса для перехвата пакетов

3. Щелкните сначала на том сетевом интерфейсе, которым вы хотели бы воспользоваться, а затем на кнопке Start (Пуск). Текущее окно должно заполниться перехватываемыми данными.

4. Подождите около минуты, и как только будете готовы остановить перехват и просмотреть полученные данные, щелкните на кнопке Stop (Остановка), выбираемой из раскрывающегося меню Capture.

Как только вы выполните описанные выше действия, завершив процесс перехвата, главное окно Wireshark должно заполниться полученными в итоге данными. В действительности объем этих данных может вас ошеломить, но они быстро обретут для вас определенный смысл, стоит вам научиться разбирать содержимое главного окна Wireshark по частям.

Главное окно Wireshark

Большую часть времени вам придется работать в главном окне Wireshark. Именно здесь перехватываемые пакеты отображаются и преобразуются в более удобный для анализа формат. Итак, рассмотрим содержимое главного окна Wireshark, используя сделанный только что перехват, как показано на рис. 3.5.

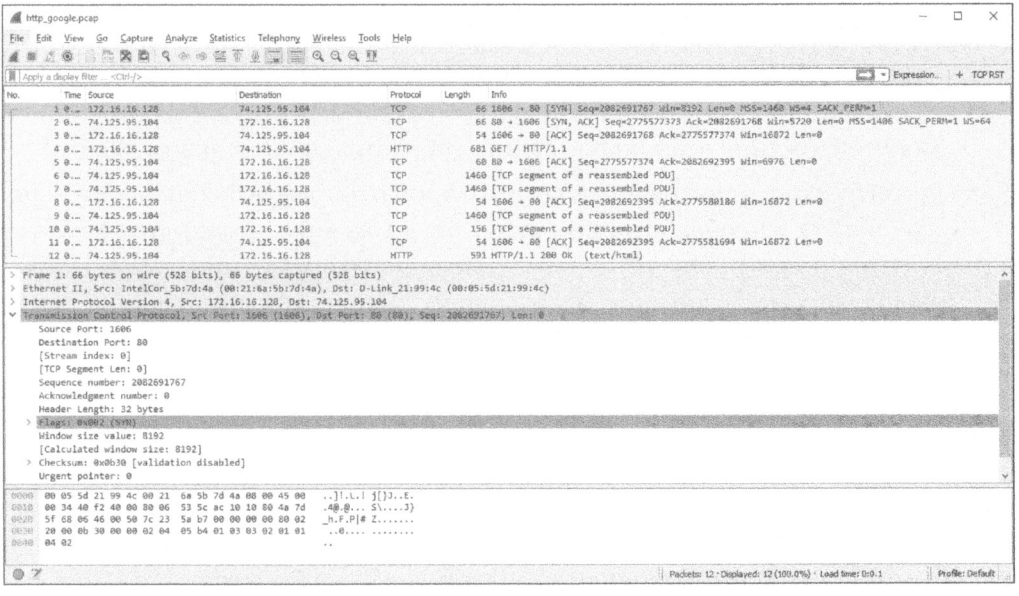

Рис. 3.5. Вид главного окна Wireshark, состоящего из трех панелей

Главное окно Wireshark состоит из панелей Packet List (Список пакетов), Packet Details (Подробные сведения о пакете) и Packet Bytes (Байты из пакетов), которые располагаются сверху вниз и зависят друг от друга. Чтобы просмотреть подробные сведения об отдельном пакете в панели Packet Details, необходимо сначала выбрать этот пакет в панели Packet List. Если же выбрать часть пакета в панели Packet Details, то в панели Packet Bytes появятся отдельные байты, соответствующие данной части пакета.

ПРИМЕЧАНИЕ *На рис. 3.5 обратите внимание на то, что в панели* Packet List *перечислены разные сетевые протоколы. Здесь отсутствует визуальное разделение протоколов на разные уровни, кроме их выделения разным цветом. А все пакеты показаны в том порядке, в каком они получены по сети.*

Ниже приведено краткое описание каждой панели.

- Packet List. Это верхняя панель, в которой отображается таблица, содержащая все пакеты из текущего файла перехвата. Она состоит из столбцов, содержащих номер пакета, относительное время перехвата пакета, адреса источника и получателя пакета, тип сетевого протокола пакета, а также некоторые общие сведения, находящиеся в пакете.

ПРИМЕЧАНИЕ *Здесь и далее под сетевым трафиком подразумеваются все пакеты, отображаемые в панели* Packet List. *А если речь идет только о трафике DNS, то имеются в виду пакеты по протоколу DNS (служба доменных имен), отображаемые в той же самой панели.*

- Packet Details. Это средняя панель, где в иерархическом виде отображаются сведения об одном пакете. Она может быть свернута или развернута для отображения всей информации, собранной об отдельном пакете.
- Packet Bytes. Это нижняя панель, в которой отображаются исходные данные пакета в необработанном виде, т.е. в том виде, в каком пакет переносится по сети. Эти исходные данные не содержат ничего, что упрощало бы их отслеживание. Методики их интерпретации подробнее рассматриваются в приложении Б, "Интерпретация пакетов", к этой книге.

Глобальные параметры настройки Wireshark

Имеется несколько глобальных параметров Wireshark, которые можно настроить под свои нужды. Чтобы получить доступ к глобальным параметрам настройки Wireshark, выберите команду Edit⇨Preferences (Правка⇨Параметры) из главного меню. В итоге откроется диалоговое окно Preferences с несколькими специально настраиваемыми параметрами, как показано на рис. 3.6.

Глобальные параметры настройки Wireshark разбиты на шесть основных разделов и дополнительный раздел Advanced. Ниже приведено краткое описание этих разделов.

- **Appearance (Представление).** В этом разделе находятся глобальные параметры, которые определяют порядок представления данных в Wireshark. Большую часть этих параметров можно изменить, исходя из своих личных предпочтений, включая необходимость сохранять

положение окон, компоновку трех основных панелей, расположение полосы прокрутки и столбцов в панели Packet List, шрифты, которыми выделяются перехваченные данные, а также цвета фона и символов шрифта.

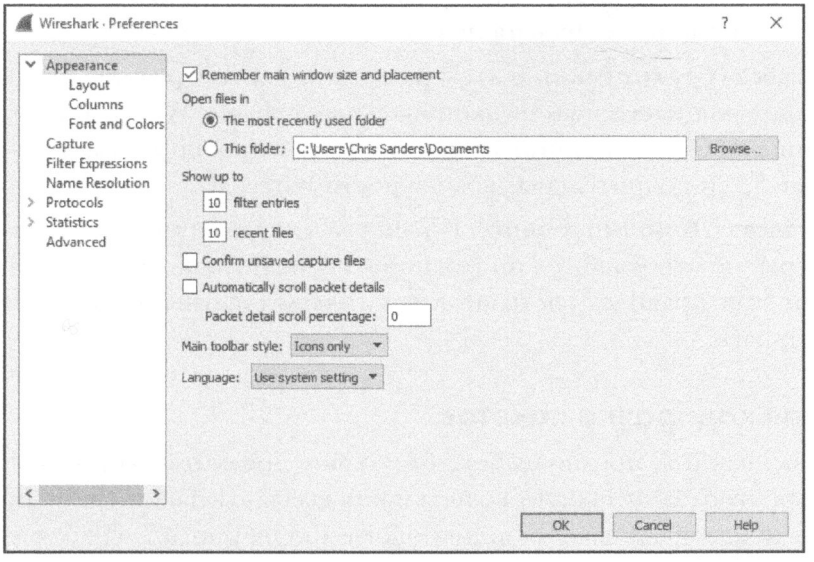

Рис. 3.6. В диалоговом окне Preferences можно специально настроить глобальные параметры Wireshark

- **Capture (Перехват).** В этом разделе находятся глобальные параметры, которые определяют порядок перехвата пакетов, включая стандартный интерфейс для перехвата, необходимость перехода в комбинированный режим по умолчанию и обновления панели Packet List в реальном времени.
- **Filter Expressions (Фильтрующие выражения).** В дальнейшем мы обсудим, каким образом в Wireshark можно фильтровать сетевой трафик по отдельным критериям. А в этом разделе находятся глобальные параметры, которые позволяют создавать фильтры сетевого трафика и манипулировать ими.
- **Name Resolution (Преобразование имен).** С помощью глобальных параметров из этого раздела можно активизировать функциональные средства Wireshark, позволяющие преобразовывать адреса в их более удобные для различения имена, в том числе адреса канального, сетевого и транспортного уровня, а также указывать максимальное количество параллельных запросов на преобразование имен.
- **Protocols (Протоколы).** В этом разделе находятся глобальные параметры, имеющие отношение к перехвату и отображению различных

пакетов, которые Wireshark в состоянии декодировать. Настраиваемые глобальные параметры имеются не для всех сетевых протоколов, но параметры некоторых из них все же можно изменить. Впрочем, эти параметры лучше оставить установленными по умолчанию, если только нет особых причин для их изменения.

- **Statistics (Статистика).** В этом разделе находится ряд глобальных параметров для настройки функциональных средств Wireshark, предназначенных для ведения статистики и более подробно рассматриваемых в главе 5, "Дополнительные возможности Wireshark".
- **Advanced (Дополнительно).** В этом разделе находятся глобальные параметры, не относящиеся ни к одной из перечисленных выше категорий. Они, как правило, настраиваются только опытными пользователями Wireshark.

Цветовая кодировка пакетов

Если вы, как и я, предпочитаете блестящие предметы и приятные цвета, то вас, вероятно, заинтересует возможность выделять пакеты разными цветами в панели Packet List, как, например, показано на рис. 3.7. И хотя это всего лишь черно-белый рисунок в печатном издании, тем не менее, разные оттенки серого на нем дают общее представление о цветовой кодировке пакетов. На первый взгляд может показаться, что пакеты выделяются цветами произвольно, но на самом деле это не так.

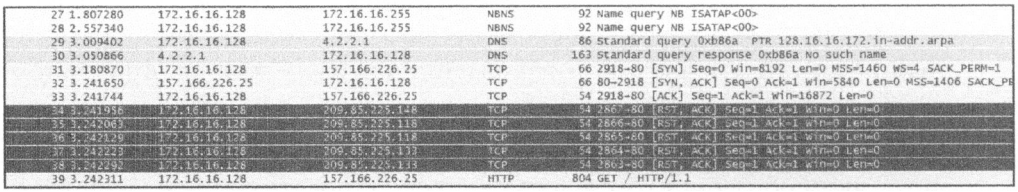

Рис. 3.7. Цветовая кодировка пакетов в Wireshark позволяет быстро распознавать сетевые протоколы

Каждый пакет отображается отдельным цветом по весьма веской причине: цвет может отражать сетевой протокол и значения в отдельных полях пакета. Например, весь трафик по сетевому протоколу UDP выделяется по умолчанию голубым цветом, а весь трафик по сетевому протоколу HTTP – салатовым. Такая цветовая кодировка позволяет быстро распознавать различные сетевые протоколы, не обращаясь к полю протокола в каждом пакете, отображаемом в панели Packet List. Со временем вы сами убедитесь, насколько это экономит время, затрачиваемое на просмотр крупных файлов перехвата.

Цвета, назначенные для каждого сетевого протокола, нетрудно изменить в диалоговом окне Coloring Rules (Правила выделения цветом), как показано на рис. 3.8. Чтобы открыть это окно, выберите команду View⇨Coloring Rules (Вид⇨ Цветовые правила) из главного меню.

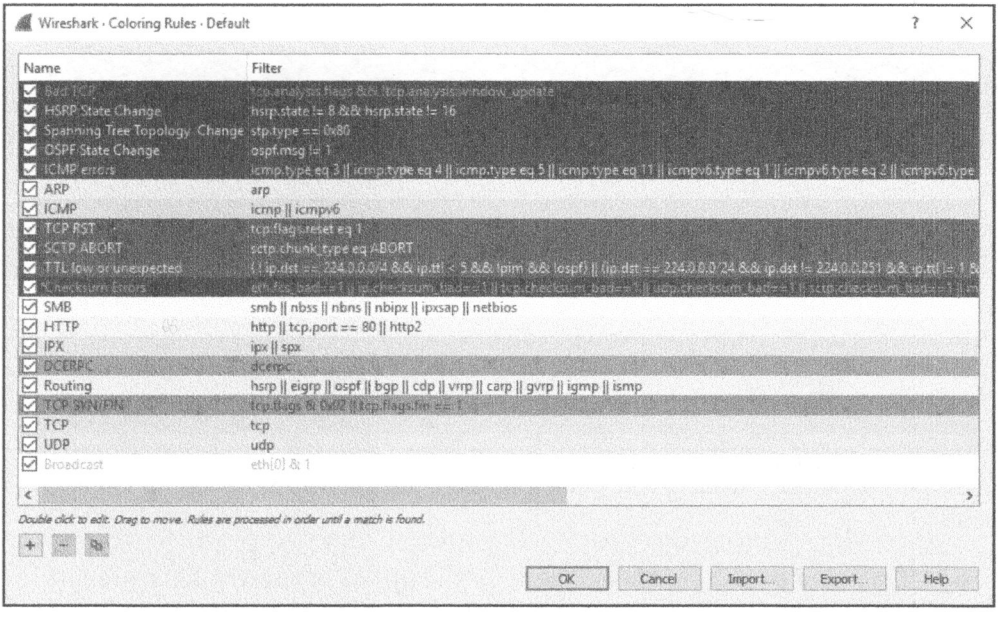

Рис. 3.8. В диалоговом окне Coloring Rules можно просматривать и изменять порядок выделения пакетов разными цветами

Правила выделения цветом основываются на фильтрах, применяемых в Wireshark и подробнее рассматриваемых в главе 4, "Обработка перехваченных пакетов". С помощью этих фильтров можно определить собственные правила выделения цветом или изменить уже существующие. Например, чтобы изменить с салатового на бледно-лиловый цвет фона, которым выделяется сетевой трафик по протоколу HTTP, выполните следующие действия.

1. Откройте Wireshark, а затем диалоговое окно Coloring Rules (по команде View⇨Coloring Rules).
2. Найдите правило выделения цветом сетевого протокола HTTP в списке подобных правил и выберите его, щелкнув на нем кнопкой мыши.
3. В нижней части экрана появятся кнопки выбора цветов символов и фона, как показано на рис. 3.9.
4. Щелкните на кнопке Background (Фон).
5. Выберите требующийся цвет на палитре цветов и щелкните на кнопке OK.

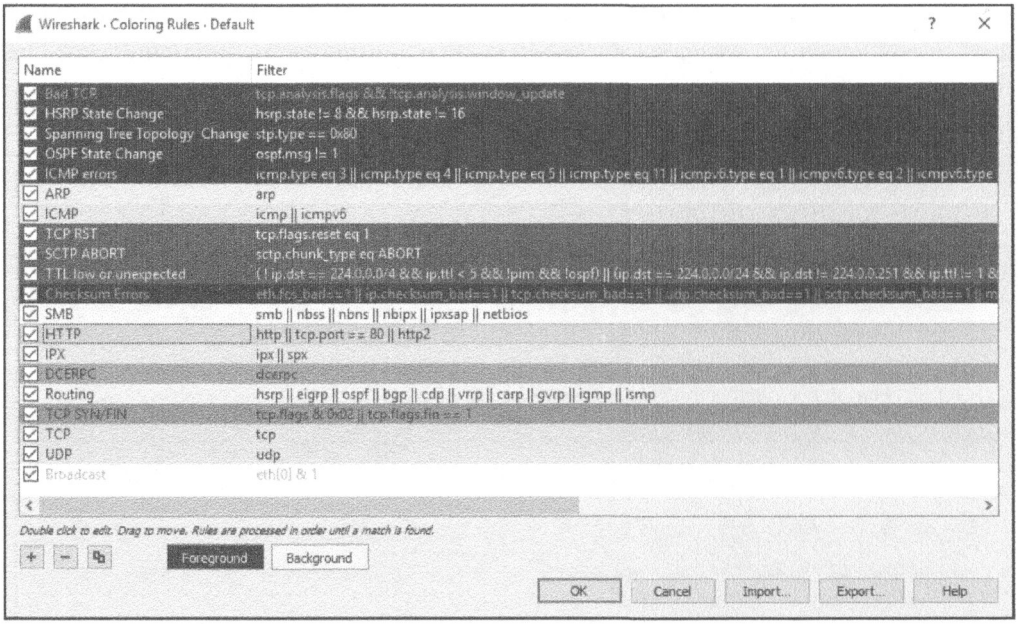

Рис. 3.9. Редактируя фильтр выделения цветом, можно изменить цвета символов и фона

6. Щелкните на кнопке OK еще раз, чтобы принять внесенные изменения и вернуться в главное окно. В итоге пользовательский интерфейс должен перезагрузиться, чтобы отразить обновленную цветовую схему.

В ходе работы со своей сетью в Wireshark вы постепенно начнете замечать, что с одними сетевыми протоколами вам приходится иметь дело чаще, чем с другими. Именно здесь и приходит на помощь цветовая кодировка пакетов, упрощающая их анализ. Так, если вы считаете, что в вашей сети имеется непослушный DHCP-сервер, самовольно назначающий IP-адреса, можете изменить правила выделения цветом сетевого протокола DHCP таким образом, чтобы отображать соответствующие пакеты светло-желтым или любым другим легко различаемым цветом. Это даст вам возможность намного быстрее различать весь сетевой трафик по протоколу DHCP, а следовательно, повысить эффективность анализа пакетов.

ПРИМЕЧАНИЕ *Не так давно мне пришлось обсуждать принятые в Wireshark правила выделения цветом в ходе презентации для группы местных учащихся. Один из учащихся признался, что ему удалось изменить установленные по умолчанию правила выделения цветом, поскольку он не может различать некоторые цвета. Такое изменение правил выделения пакетов разным цветом лишь расширяет специальные возможности пользователей Wireshark.*

Файлы конфигурации

Полезно знать, где именно Wireshark сохраняет настройки своей конфигурации, на тот случай, если потребуется внести в них непосредственные коррективы. Чтобы найти местоположение файлов конфигурации Wireshark, достаточно выбрать сначала команду Help⇨About Wireshark (Сцравка⇨О программе Wireshark), а затем вкладку Folders (Папки). Диалоговое окно с этой развернутой вкладкой приведено на рис. 3.10.

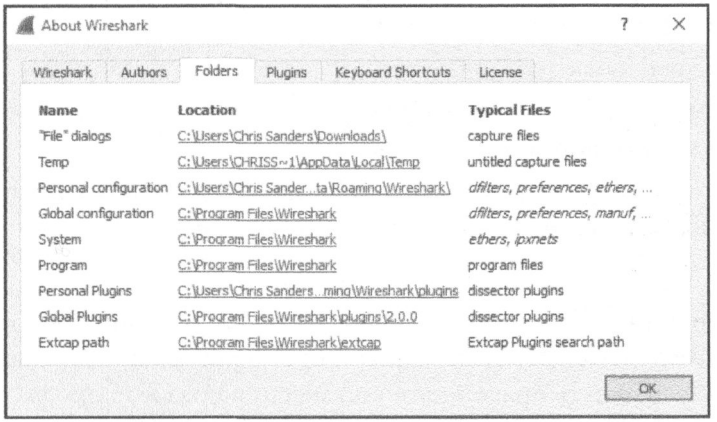

Рис. 3.10. Местоположение файлов конфигурации Wireshark

Что касается специальной настройки Wireshark, то двумя самыми важными местами для ее проведения служат каталоги личной и глобальной конфигурации. Так, в каталоге глобальной конфигурации содержатся все устанавливаемые и сохраняемые по умолчанию настройки и профили Wireshark, а в каталоге личной конфигурации — специальные настройки и профили, характерные для вашей учетной записи. Любые новые файлы, которые вы создаете, будут сохраняться в подкаталоге, расположенном в каталоге личной конфигурации по указанным вами именам. Различать каталоги личной и глобальной конфигурации важно потому, что любые изменения в файлах глобальной конфигурации окажут влияние на каждого пользователя Wireshark в системе.

Профили конфигурации

После ознакомления с глобальными параметрами настройки Wireshark у вас может порой возникнуть потребность воспользоваться сначала одним рядом этих параметров, а затем быстро перейти к другим глобальным параметрам, чтобы учесть изменившуюся ситуацию. Но вместо того чтобы перенастраивать глобальные параметры каждый раз, когда в этом возникает потребность, можно воспользоваться внедренными в Wireshark профилями

конфигурации, дающими пользователям возможность создавать и сохранять определенный ряд глобальных параметров.

В профиле конфигурации хранится следующее.

- Глобальные параметры настройки
- Фильтры перехвата
- Фильтры отображения
- Правила выделения цветом
- Запрещенные сетевые протоколы
- Принудительные расшифровки
- Недавние установки, в том числе размеры панелей, настройки представления меню и ширина столбцов
- Характерные для протоколов таблицы, содержащие, например, перечень пользователей сетевого протокола SNMP и специальные HTTP-заголовки

Чтобы просмотреть список профилей конфигурации, выберите команду Edit⇨Configuration Profiles (Правка⇨Профили конфигурации) из главного меню. Можно также щелкнуть правой кнопкой мыши на разделе профилей в правом нижнем углу окна и выбрать команду Manage Profiles (Управлять профилями) из контекстного меню. В открывшемся окне Configuration Profiles вы обнаружите ряд стандартных профилей Wireshark, включая следующие: **`Default`** (Стандартный), **`Bluetooth`** (Беспроводная персональная сеть Bluetooth) и **`Classic`** (Классический). Здесь же находится специально созданный автором книги профиль **`Latency Investigation`** (Исследование сетевой задержки), который выделяется простым текстом, тогда как остальные профили — курсивом, как показано на рис. 3.11.

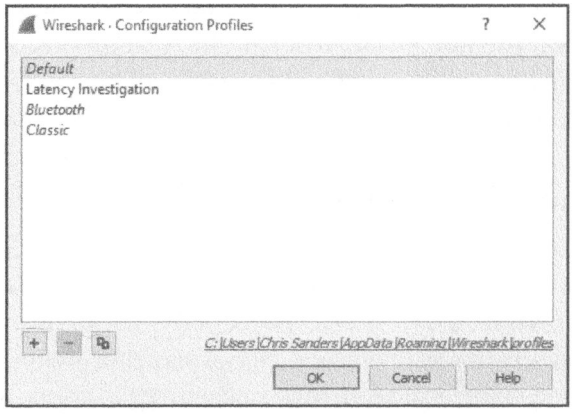

Рис. 3.11. Просмотр профилей конфигурации

В окне Configuration Profiles можно создавать, копировать, удалять и применять профили конфигурации. Процесс создания нового профиля довольно прост. Для этого достаточно выполнить следующие действия.

1. Настройте конфигурацию Wireshark с установками, которые требуется сохранить в отдельном профиле.
2. Перейдите в окно Configuration Profiles, выбрав команду Edit⇨Configuration Profiles из главного меню.
3. Щелкните на кнопке со знаком "плюс" (+) и присвойте описательное имя новому профилю конфигурации.
4. Щелкните на кнопке OK.

Когда у вас возникнет потребность сменить профиль конфигурации, перейдите в окно Configuration Profiles, щелкните сначала на имени нужного профиля, а затем на кнопке OK. Эту операцию можно ускорить, щелкнув правой кнопкой мыши в правом нижнем углу окна Wireshark на заголовке **Profile** и выбрав нужный профиль, как показано на рис. 3.12.

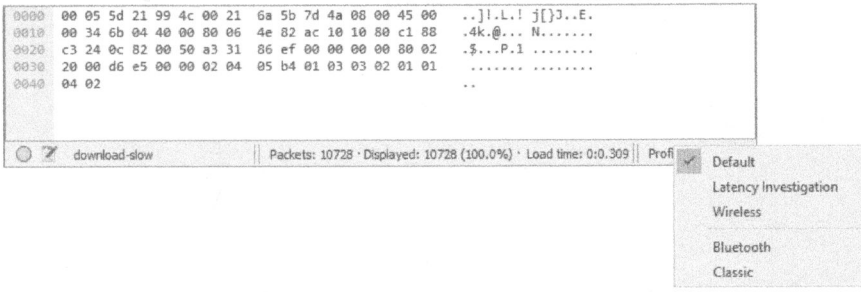

Рис. 3.12. Быстрая смена профиля конфигурации через заголовок ***Profile***

К числу самых полезных свойств профилей конфигурации относится возможность сохранять их в отдельном каталоге вместе с целым рядом файлов конфигурации. Это означает, что можно создавать резервные копии профилей, а затем обмениваться ими с другими пользователями. На вкладке Folders, приведенной на рис. 3.10, указаны пути к каталогам с файлами личной и глобальной конфигурации. Чтобы обменяться профилем с пользователем на другом компьютере, достаточно скопировать папку, совпадающую с именем обмениваемого профиля, и вставить ее в тот же самый каталог для соответствующего пользователя на другом компьютере.

По ходу чтения этой книги у вас может возникнуть потребность создать несколько профилей высокого уровня для общей диагностики сети, выявления источника сетевой задержки и исследования вопросов безопасности. Не бойтесь свободно пользоваться профилями. Они действительно экономят время,

когда требуется быстро сменить ряд глобальных параметров настройки. Мне известны пользователи Wireshark, которые употребляли десятки профилей для успешного разрешения самых разных ситуаций в сети.

Итак, установив и настроив Wireshark, вы готовы приступить к анализу пакетов. В главе 4, "Обработка перехваченных пакетов", поясняется, как обрабатывать перехваченные пакеты.