XXIX Неделя науки СПбГТУ. Материалы межвузовской научной конференции. Ч.V: С.59-60, 2001.

УДК 681.324

И.М. Шагин (6 курс, каф. АиВТ), В.М. Ицыксон, к.т.н., доц.

РЕАЛИЗАЦИЯ УНИВЕРСАЛЬНОГО ГЕНЕРАТОРА ПАКЕТОВ СРЕДСТВАМИ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА WINDOWS

Задача анализа и диагностики компьютерных сетей появилась одновременно с созданием первой сети, и, естественно, на данный момент существует множество программных и аппаратных ее решений. Важной частью выше обозначенной задачи является анализ сетевого трафика, которая с успехом решается с помощью программ – анализаторов трафика. Надо отметить, что все анализаторы являются пассивными, то есть они принимают данные из сети, но сами не способны формировать возмущающие воздействия на сеть. Это и не является задачей сетевых анализаторов, но для тестирования различных ситуаций, происходящих в сети, зачастую необходимо формировать определенные последовательности пакетов. Существуют специальные программы ‘генераторы пакетов’, которые позволяют посылать произвольные пакеты в сеть, но их немного и обычно они охватывают только узкий круг сетевых протоколов.

Предлагаемое решение ‘универсальный генератор пакетов’ объединяет в себе возможности как генератора, так и анализатора пакетов. С его помощью можно конструировать любые пакеты на всех доступных уровнях сетевой иерархии, посылать эти пакеты в определенной последовательности и с определенной частотой, а также анализировать отклик сети. Для управления логикой работы ‘генератора’ используется специальный язык.

Задача построения такого программного продукта представляется нетривиальной, но, в результате, мы получаем совершенно незаменимый инструмент, который позволяет автоматизировать многие задачи, которые ранее такой автоматизации не поддавались. Область его применения довольно широка – от защиты информации (можно, например, имитировать большинство типовых сетевых атак), до прикладного использования администраторами сетей.

Данная система разрабатывается для операционной системы Windows. Это достаточно необычно для задачи такого рода, так как обычно такие программы разрабатываются для UNIX-подобных ОС. Выбор был обусловлен малой насыщенностью рынка сетевых анализаторов под Windows и широкой распространенностью этой ОС. На данный момент существует лишь несколько серьезных сетевых анализаторов для Windows. Наибольшего уважения заслуживают WinDump (качественный перенос приложения tcpdump с UNIX), и WinEthereal (тоже перенесенный с UNIX). Генераторов же трафика для этой платформы не существует.

Несмотря на очевидные преимущества выбранной платформы, выражающиеся в ее распространенности и наличии мощных интегрированных визуальных средств разработки, имеются и существенные недостатки. Они заключаются в закрытости многих частей системы и меньшей ориентированностью на работу в сети. В частности, для работы с протоколами TCP/IP в операционной системе Windows предполагается использование библиотеки WinSock, функциональность которой ограничена.

Стандартные функции для работы с сетью в Windows построены в соответствии со спецификацией программного интерфейса с сетью для операционных систем Windows*, основанной, в свою очередь, на хорошо знакомой любому UNIX-программисту концепцией сокетов, произрастающей из BSD UNIX. Спецификация включает в себя как стандартные Berkley Style функции, так и набор функций специфичных сугубо для

Windows. На данный момент распространены две базовые версии этой спецификации: WinSock 1 и WinSock 2.

Для реализации функциональности генератора пакетов необходимо иметь возможность посылать произвольные IP-пакеты, то есть пакеты с произвольным заголовком. Далее, на основе таких пакетов можно будет построить любые пакеты протоколов более высокого уровня. Для конструирования произвольных пакетов необходимо использовать так называемые raw sockets (‘сырые’, ‘необработанные’ сокеты), для которых заголовки автоматически не добавляются, что позволяет формировать заголовок из приложения. В стандартной реализации спецификации Windows Sockets поддержка таких сокетов отсутствует. На эту тему было проведено исследование, показавшее, что реализация сокетов в Windows не поддерживает IP и TCP raw sockets. Вместе с тем, ICMP raw sockets поддерживаются, но ICMP – это только один из протоколов, и для поставленной задачи этого не достаточно.

Так как такое ограничение имеет место и в WinSock 1, и в WinSock 2, то, судя по всему, отсутствие поддержки таких сокетов было вполне осознанным актом со стороны Microsoft, вызванным соображениями безопасности.

Недавно появившаяся операционная система Windows 2000 включает в себя новую версию библиотеки WinSock, которая позволяет использовать IP raw sockets. Но, так как эта операционная система еще не очень распространена, то использование специфичных для нее возможностей сильно сузит область применения программы. В таблице приведены возможности различных версий Windows Sockets.

	Winsock 1.1 (все платформы)	Winsock 2 (Windows 9x)	Windows NT 4.0	Windows 2000
Raw ICMP/IGMP	Нет	Да	Да	Да
Raw IP	Нет	Нет	Нет	Да
Raw TCP/UDP	Нет	Нет	Нет	Нет

Для реализации функций анализа сети требуется перевести сетевую карту в специальный ‘прослушивающий’ режим. С помощью стандартных средств Windows сделать это также невозможно.

В результате можно сделать вывод, что возможностей Windows сокетов для решения поставленной задачи недостаточно. Учитывая то, что система должна работать под управлением Windows версии 95 и выше, общаться с сетевой картой напрямую будет невозможно. Вместо этого придется писать драйвер, работающий по соглашениям NDIS (Network Driver Interface Specification). Или, более конкретно, работающий на уровнях TDI (Transport Data Interface) или NDI (Network Driver Interface) сетевой иерархии Windows.Таким образом, задача значительно усложняется – фактически необходимо разработать собственный стек протоколов TCP/IP.

В настоящее время стек протоколов, с помощью которого можно выполнять функции, как анализа сети, так и посылки произвольных пакетов, находится в состоянии разработки.