А.В. Хмель, О.Ю. Пескова
Россия, г. Таганрог, ТРТУ

ТЕХНОЛОГИЯ УДАЛЕННОГО УПРАВЛЕНИЯ РАБОЧИМИ СТАНЦИЯМИ

Удаленный доступ — очень широкое понятие, которое включает в себя различные типы и варианты взаимодействия компьютеров, сетей и приложений. Существует огромное количество схем взаимодействия, которые можно назвать удаленным доступом, но их объединяет использование глобальных каналов или глобальных сетей при взаимодействии. Кроме того, для удаленного доступа, как правило, характерна несимметричность взаимодействия, то есть с одной стороны имеется центральная крупная сеть или центральный компьютер, а с другой — отдельный удаленный терминал, компьютер или небольшая сеть, которые должны получить доступ к информационным ресурсам центральной сети. За последние год-два количество предприятий, имеющих территориально распределенные корпоративные сети, значительно возросло. Поэтому для современных средств удаленного доступа очень важны хорошая масштабируемость и поддержка большого количества удаленных клиентов.

Еще совсем недавно для удаленного управления корпоративными сетями применялись фирменные решения, отличающиеся использованием собственных протоколов передачи данных по телефонным сетям и собственных методов аутентификации удаленных пользователей, а также оригинальными способами предоставления ресурсов центральной сети. Естественно, это вызывало определенные проблемы и при необходимости «сращивания» двух сетей, имевших прежде различную конфигурацию средств управления сетью, и при подготовке специалистов, и в других ситуациях. Сейчас в системах управления работает все больше стандартных компонентов: протокол передачи данных PPP; «джентльменский набор» средств аутентификации — с помощью систем Kerberos, Novell NDS или MicrosoftDirectoryServices; предоставление информационных ресурсов удаленным пользователям с помощью службы WWW или тех же сервисов, которые работают и в локальной сети. Этот процесс облегчает взаимодействие серверов удаленного доступа с клиентами и сетевыми операционными системами, работающими в локальной сети. Хотя до полной стандартизации еще далеко, за последние несколько лет ситуация изменилась коренным образом.

Одним из наиболее насущных вопросов при разработке программ удаленного управления является вопрос о повышение скорости передачи информации. Основные усилия операторов телекоммуникационных сервисов сегодня направлены на преодоление для массовых пользователей ограничения в 56,2 Кбит/с, накладываемого аналоговыми модемами. Кроме того, передача информации через сеть Интернет является, мягко говоря, небезопасной. Поэтому идеальным вариантом было бы создание виртуальной частной сети — VPN. Подключение корпоративной сети к Internet оправданно в том случае, если вам нужен доступ к соответствующим услугам. Использовать Internet как среду передачи данных стоит только тогда, когда другие способы недоступны и когда финансовые соображения перевешивают требования надежности и безопасности. Одной из наиболее широко обсуждаемых проблем удаленного администрирования является именно безопасность. Если допускается возможность удаленного управления вашей сетью, то какой бы технологией вы ни пользовались, появится ряд проблем, связанных с обеспечением безопасности передающейся по сети информации. Как показывает практика, случаи взлома сети все еще довольно часто встречаются. Частной сети может угрожать ряд опасностей. Прежде всего, это перехват информации при передаче. Здесь мо-

гут помочь средства шифрования, которые решают проблему лишь частично, поскольку применимы в основном к почте и передаче файлов. Решения же, позволяющие с приемлемой скоростью шифровать информацию в реальном времени (например, при непосредственной работе с удаленной базой данных или файл-сервером), пока малодоступны и дороги. Есть, конечно, средство защиты от несанкционированного доступа к сети — Firewall (межсетевой экран). Однако любую защиту можно сломать, особенно если полученная информация окупает стоимость взлома. Таким образом, рекомендовать Internet как основу для систем, в которых требуется надежность и закрытость, можно лишь в крайнем случае и при использовании всех мер защиты, включая межсетевые экраны, шифрование канала и VPN. Кроме того, не стоит забывать и о человеческом факторе — о сотрудниках «внутри» и «снаружи» корпоративной сети.

Для организации удаленного доступа можно использовать технологии X.25 и Frame Relay, которые предоставляют ряд весьма интересных возможностей. Проблема несанкционированного доступа также может достаточно эффективно решаться средствами самой сети. Существует несколько схем удаленного управления сетью, отличающиеся типом взаимодействующих систем: 1 — «терминал-компьютер»; 2 — «компьютер-компьютер»; 3 — «компьютер-сеть»; 4 — «сеть-сеть». Первые три вида удаленного доступа часто объединяют понятием индивидуального доступа, а схемы доступа «сеть-сеть» иногда делят на два класса — ROBO (RegionalOffice/BranchOffice) и SOHO (SmallOffice/HomeOffice). Класс ROBO соответствует случаю подключения к центральной сети сетей средних размеров — сетей региональных подразделений предприятия, а классу SOHO — случаю удаленного доступа сетей небольших офисов и домашних сетей.

Особое место среди всех видов удаленного доступа к компьютеру занимает способ, при котором пользователь получает возможность удаленно работать с компьютером так же, как если бы он управлял им с помощью локально подключенного терминала. В этом режиме он может запускать программы на удаленном компьютере и видеть результаты их выполнения. При этом такой способ доступа принято разделять на терминальный доступ и на удаленное управление. Хотя это близкие режимы работы, но в описании продуктов удаленного доступа их не принято объединять в один класс. Обычно под терминальным доступом понимают символьный режим работы пользователя с удаленными многопользовательскими ОС — UNIX, VAXVMS, ОС мэйнфреймов IBM. В класс удаленного управления включают программы эмуляции графического экрана ОС персональных компьютеров — в первую очередь разных версий Windows, а в последнее время к этому классу можно отнести Linux-системы, Solaris и др.

Многие производители операционных систем предусмотрели в своих стеках протоколов средства терминального доступа пользователей к компьютерам по сети. Эти средства позволяют пользователю, работающему за компьютером, подключенным к сети, превратить экран своего монитора в эмулятор терминала другого компьютера, также подключенного к сети. Наиболее популярным средством такого типа является протокол telnet стека TCP/IP, появившегося в рамках операционной системы UNIX и с тех пор неразрывно с нею связанного.

В отличие от систем терминального доступа, превращающих компьютер пользователя в эмулятор экрана центрального компьютера, средства поддержки режима удаленного узла (remote node) делают вызывающую машину полноправным звеном локальной сети. Это достигается за счет того, что на удаленном компьютере работает тот же стек протоколов, что и в компьютерах центральной локальной сети, за исключением протоколов канального и физического уровня. На этом уровне вместо традиционных протоколов Ethernet или Token Ring работают

модемные протоколы (физический уровень) и канальные протоколы соединений «точка-точка», такие как SLIP, HDLC и PPP. Эти протоколы используются для передачи по телефонным сетям пакетов сетевого и других протоколов верхних уровней. Таким образом, осуществляется полноценная связь удаленного узла с остальными узлами сети. Сервис удаленного узла обеспечивает ему транспортное соединение с локальной сетью, поэтому на удаленном узле могут использоваться все сервисы, которые доступны локальным клиентам сети, например файл-сервис NetWare, сервис telnet или X-Window ОС UNIX, администрирование Windows NT.

Наибольшие сложности вызывает удаленное управление популярными настольными операционными системами семейства Windows, OS/2 и т.п. Это связано с тем, что для данных систем нет стандартного протокола эмуляции терминала, подобного telnet или X-Window для UNIX или LAT для VAXVMS. Кроме того, эти операционные системы наиболее знакомы конечному пользователю, и ему было бы очень удобно использовать привычный графический интерфейс Windows при управлении удаленным хостом. Поэтому именно разработка средств удаленного управления для ОС семейства Windows стала основной целью данного проекта.

В рамках проекта по созданию системы удаленного управления рабочими станциями реализован программный комплекс, содержащий два модуля – «Сервер» (устанавливается на удаленном персональном компьютере) и «Клиент» (устанавливается на рабочей станции администратора сети), задачами которых является передача защищенной информации между удаленными компьютерами с наименьшими потерями во времени. Эта программа позволяет работать с файлами на удаленном компьютере (операции сетевого и локального копирования и перемещения, локального переименования и удаления файлов, открытие файлов в соответствии с файловыми ассоциациями), осуществлять доступ к реестру и редактирование его параметров, выполнять просмотр списка работающих процессов и программ на удаленном компьютере с возможностью запуска и останова процессов, блокировать и завершать работу удаленного пользователя или компьютера, а также получать доступ к средствам ввода/вывода удаленной станции.

Работа поддержана грантом РФФИ №03-07-90075.

Е.В. Хандыго, О.Ю. Пескова
Россия, г. Таганрог, ТРТУ

ТЕХНОЛОГИЯ ЗАХВАТА СЕТЕВОГО ТРАФИКА

В настоящее время аппаратная архитектура Ethernet завоевала большую часть рынка локальных сетей. Из-за особенностей ее построения пакет, отправленный в широковещательной сети одним из узлов, принимается всеми находящимися в этом сегменте сети машинами, но только узел назначения, указанный в заголовке пакета, "смотрит" на него и начинает его обработку. Благодаря этому свойству существует большой класс программ, предназначенных для перехвата всех сетевых пакетов и дальнейшего их анализа – так называемых снифферов. Такие средства используются как для мониторинга сетей, так и для перехвата секретной информации. Алгоритм работы снифферов несложен. В локальной сети, организованной на основе хабов, можно перехватывать все отправляемые пакеты со всех машин, так как там практикуется широковещание. По умолчанию сетевой интерфейс “видит” пакеты, предназначенные только для него. Однако анализаторы устанавливают его в режим приема всех пакетов – promiscuous mode, прослушивают сеть и заставляют сетевой интерфейс принимать все фреймы, вне зависимости от того, кому они адресованы в сети. После этого происходит непосредственно ана-