Лекция 12.

СРЕДСТВА УДАЛЕННОГО ДОСТУПА В ИВС.

Удаленный доступ - *это частный случай соединения компьютеров через глобальные связи.* От обычных вариантов с использованием мостов и маршрутизаторов удаленный доступ отличается тем, что одной из взаимодействующих сторон является не локальная сеть, а отдельный компьютер без сетевого адаптера. Кроме того, удаленный доступ обычно использует низкоскоростные соединения по коммутируемым телефонным аналоговым сетям. Реже используются сети ISDN или X.25.

12.1. Компоненты удаленного доступа

Большинство решений для удаленного доступа базируются на тех же основных компонентах, что и обычные локальные сети:

• некоторое количество машин, работающих в качестве информационных серверов,

• большое количество клиентских машин или ноутбуков, имеющих доступ к разделяемым данным, хранящимся на серверах,

• программная и аппаратная инфраструктура, обеспечивающая взаимодействие серверных и клиентских машин.

Однако в то время, как в локальных сетях инфраструктура передачи данных обычно состоит из сетевых адаптеров, кабелей и маршрутизаторов, системы удаленного доступа добавляют к ним *модемы, телефонные линии,* возможно, некоторое количество *выделенных линий,* а также *специальное программное и аппаратное обеспечение удаленного доступа.*

Очевидно, что для экономии модемов можно не ставить на каждую телефонную линию отдельный модем, а организовать общий *пуп модемов* и сделать его разделяемым ресурсом как для звонков из локальной сети, так и для звонков извне. Действительно, если каждому пользователю выделить персональный модем (и персональную линию связи). то, как правило, большую часть времени он будет простаивать, поэтому гораздо эффективнее использовать то число модемов (и линий), которое реально необходимо.

Разделяемый пул модемов создается с помощью так называемого *коммуникационного сервера (communication server).* Коммуникационный сервер - это обычный компьютер или специализированное устройство, предоставляющее пользователям локальной сети прозрачный доступ к последовательным портам ввода-вывода, к которым подключены разделяемые модемы. Пользователь, подключившийся к коммуникационному серверу, может работать с одним из подключенных к нему модемов точно также, как если бы этот модем был подключен непосредственно к компьютеру пользователя,

Более сложные функции, связанные с обработкой передаваемой информации в системах удаленного доступа, выполняют *серверы доступа (access server).* Серверы доступа могут быть реализованы самыми различными способами, на которых мы остановимся позже.

12.2. Различные варианты удаленного доступа

В зависимости от потребностей пользователей и возможностей программно-аппаратного обеспечения удаленный доступ может осуществляться в соответствии с различными схемами; характеристика пяти наиболее распространенных из них приведена ниже.

1. Первый вариант - это **режим удаленного узла (remote node).** Программное обеспечение удаленного узла на клиентской машине позволяет последовательному порту и модему (или интерфейсу ISDN) стать медленным узлом канального уровня, взаимодействующим обычным способом с редиректором операционной системы. В локальной сети должен быть установлен сервер удаленного узла, который умеет транслировать приходящие низкоскоростные кадры в кадры протоколов Ethernet, Token Ring и других протоколов, используемых в локальной сети.

Серверы, работающие в режиме удаленного узла, представляют собой функциональный эквивалент маршрутизаторов или мостов с WAN-портами для последовательных или ISDN-линий. Клиенты, работающие в режиме удаленного узла, могут логически войти в сеть таким же образом, как если бы они были локальными пользователями, отображать сетевые диски и даже загружать программы через удаленную связь. Но загрузка больших программ не разумна, так как самый скоростной модем - (28.8 Кб/с) работает со скоростью, составляющей только 3% от скорости сегмента Ethernet, и программа, которая в локальной сети загружается за 30 сек, будет загружаться по удаленной связи в течение 15-20 минут. Поэтому в режиме удаленного узла следует использовать преимущественно локальные копии программ.

Другая проблема связана со способом работы сетевых операционных систем. Серверы часто рассылают широковещательные сообщения всем узлам сети для проверки подключенных и работающих клиентов. Такие широковещательные рассылки могут заблокировать удаленный доступ, если они не фильтруются перед отправкой по удаленным связям. Поэтому перед приобретением любого продукта необходимо проверить по его описаниям, может ли он работать в режиме удаленного доступа.

Удаленное сетевое соединение (remote network connection) или, что то же самое, удаленный узел, наиболее эффективно работает с системами клиент-сервер, такими как СУБД, файл- и принт-серверы, а также с мейнфреймами.

Операционные системы Mac OS, OS/2, Windows 95 и Windows NT Workstation включают в стандартной поставке клиентскую часть программного обеспечения удаленного узла. В настоящее время имеется явная тенденция использования клиентами удаленного узла протокола PPP. В результате достигается совместимость клиентских и серверных частей систем, работающих в режиме удаленного узла, различных производителей.

2. Другим распространенным вариантом удавленного доступа является так называемое **удаленное управление (remote control).** При этом способе удаленный компьютер становится, в сущности, виртуальным терминалом компьютера-хоста, который может быть, а может и не быть подключен к сети. Этот вариант позволяет запустить любое приложение на компьютере-хосте, а также получить доступ к любым данным этого хоста. Удаленное управление нужно использовать тогда, когда вы работаете с приложениями, не оптимизированными для работы в сети, например с традиционными СУБД персональных компьютеров, например, dBase, Paradox или Access. Когда приложение находится на одном компьютере, а файлы баз данных - на другом, то в сети создается большой график.

Протоколы, используемые программами удаленного управления для передачи информации об обновлении экрана, нажатиях клавиш и перемещениях мыши, являются нестандартными - пользователи Norton pc Anywhera не смогут дозвониться до хоста, работающего под управлением программ ReachOut, LapLink for Windows, Carbon Copy, Remotely Possible или Close-Up.

3. **Почта** является еще одним видом удаленного доступа. **Почтовые шлюзы** доступные по коммутируемым телефонным линиям, и клиентское почтовое обеспечение удаленного доступа могут быть достаточными доя обеспечения потребностей многих обычных пользователей. Такие почтовые шлюзы позволяют удаленным пользователям или даже удаленным офисам звонить в почтовую систему центрального отделения, обмениваться входящими и исходящими сообщениями и файлами, а затем отключаться.

Продукты, предназначенные для этих целей, варьируются от клиентских программ для одного пользователя, таких как cc:mail Mobile фирмы Lotus, до полномасштабных шлюзов, которые организуют почтовый обмен между удаленными серверами и корпоративной локальной сетью.

Почтовые шлюзы могут быть полезны в случае, когда количество данных, которыми обмениваются удаленные пользователи с центральным офисом, невелико. Из-за того, что среднее время сессии пользователь-шлюз сравнительно невелико, шлюз центральной сети не должен поддерживать большое количество

телефонных линий. Обычно почтовое соединение легко устанавливается, а стоимость программного обеспечения шлюза невелика,

Шлюзы работают в автоматическом режиме без вмешательства человека. Если в удаленном офисе работают один или два сотрудника, и им не нужен доступ к корпоративным данным в реальном масштабе времени, то почтовый шлюз может быть хорошим решением. Почтовый шлюз может быть всегда модифицирован в стандартное сетевое соединение, если количество пользователей и их потребности возросли.

Не только почта, но и другие приложения, написанные для использования в локальной вычислительной сети, могут иметь специфические программные модули, предназначенные для удаленных соединений. Такие программы устанавливают соединения между собой с помощью нестандартных протоколов и часто максимизируют использование времени соединения за счет специальных приемов, например, путем передачи только обновлений между удаленным компьютером и хостом. Примером продуктов этого класса являются программные системы коллективной работы.

4. Четвертый вариант удаленного доступа - это **доступ по коммерческим сервисам реального времени** или по сети Internet. Все сервисы реального времени и практически все провайдеры Internet'a поддерживают электронную почту и некоторые формы передачи файлов. Для подключения к таким сервисам в этом варианте, как правило, достаточно местных телефонных звонков (в отличие от первых трех схем удаленного доступа, для которых в общем случае необходимы более дорогостоящие междугородние вызовы). Сервисы реального времени имеют свое собственное программное обеспечение *идя* доступа, хотя к ним можно получить доступ и с помощью обычных программ эмуляции терминала. Сегодня, когда Mac OS, OS/2, Windows 95, Windows NT Workstation и практически любой вариант Unix'a включают стек TCP/IP, несколько популярных программ для доступа в Internet и программу электронной почты, технические барьеры на пути к Internet'y значительно снизились.

5. Пятый сценарий - наиболее простая форма удаленных коммуникаций - состоит в **соединении точка-точка и обеспечивает передачу файлов, эмуляцию терминалов и досок объявлений BBS.** Доски объявлений, а также программы мейнфреймов и миникомпьютеров обычно находятся в автоматическом режиме ожидания звонков, в то время как связи ПК-ПК устанавливаются обычно от случая к случаю. Удаленному пользователю *для* работы по этому сценарию необходимо некоторое оборудование для соединения по последовательной линии и программа эмуляции терминала. Рисунок 12.1 показывает некоторые конфигурации, используемые для удавленного доступа. Необходимо также упомянуть о передаче факсов. Если удаленный ПК оборудован факс-модемом и соответствующим программным обеспечением, то он может принимать факсы от любого факс-аппарата, установленного в любой точке земного шара.

Использование того или иного варианта удаленного доступа во многом определяется потребностями пользователей. Все множество пользователей, которым может потребоваться удаленный доступ, может быть разделено на несколько групп.

• Пользователи, которые работают дома только от случая к случаю (home-based worker). Они обычно используют режим удаленного управления своей собственной PC, которую они оставили в офисе.

• Мобильные пользователи (Mobile users). Обычно это сотрудники, которые по долгу службы проводят рабочий день не в собственном офисе, а непосредственно на местах работы клиентов. Кроме того, к этой группе относятся руководители, находящиеся в отпуске или в командировке. Типичное "снаряжение" этой категории пользователей - переносной компьютер с модемом. Сеанс связи с ЛВС офисов более высоких уровней обычно бывает непродолжительным и может происходить в любое, заранее не запланированное

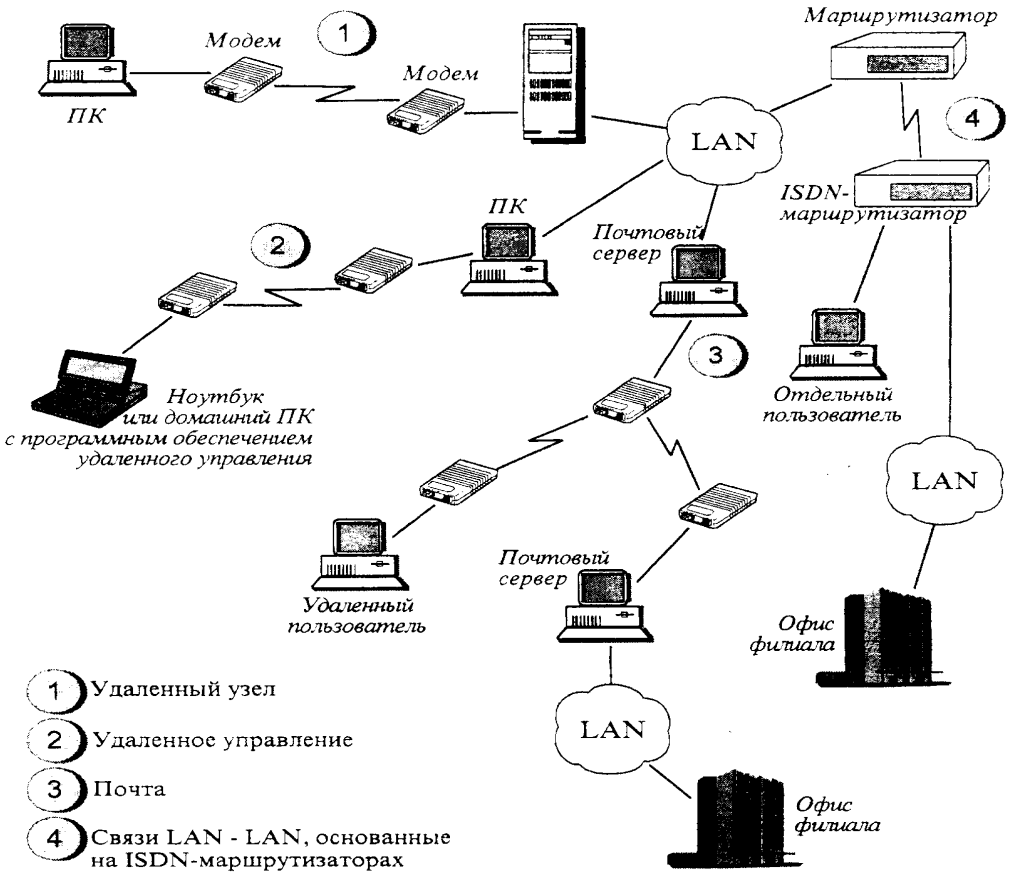

Рис. 12.1. Некоторые схемы удаленного доступа

время. Они обычно используют те способы связи. которые они могут найти в тех местах, где они остановились, Поэтому компьютер мобильного пользователя должен быть оснащен разнообразными средствами удаленного доступа.

• Филиалы или пользователи с одним компьютером *(telecommuters,* буквально - жители пригорода, работающие в городе). К этой группе относятся малые филиалы с одним компьютером, сотрудники, работающие на дому (например, разработчики программного обеспечения), и представители компании в другой компании. Обычно эти люди используют в своей деятельности персональный компьютер или UNIX-терминал. Связь с офисами более высоких уровней в течение дня должна поддерживаться достаточно продолжительное время. Телекомпьютеры - пользователи, рабочее место которых постоянно находится дома, но которым постоянно требуется информация центрального офиса. Для таких пользователей больше всего подходит режим удаленного узла.

• Сотрудники небольших удаленных офисов, имеющие собственные локальные сети. Они обычно подключаются к сети центрального офиса с помощью маршрутизаторов через коммутируемые телефонные линии, ISDN или выделенные линии.

Удаленному пользователю может понадобиться любая комбинация описанных сценариев. Если один из режимов удаленного доступа становится ненадежным или недоступным. то вместо него можно использовать другой.

Например, путешественник обычно имеет немного времени для удаленной работы. Поэтому, если линия электронной почты занята, то он может попытаться установить сессию удаленного управления по другому номеру и войти в почтовую систему "локально ", если же сессия удаленного управления разрывается, то он

может позвонить в Internet и отправить сообщение по его электронной почте.

12.3. Режимы Dial-in и Dial-out

Удаленный доступ может быть реализован по-разному, в зависимости от направления предоставляемого доступа.

Dial-in - режим, который позволяет пользователю, работающему на отдельном компьютере, обращаться с запросами в удаленную сеть. Именно это является основной задачей систем удаленного доступа. С этой точки зрения удаленный доступ можно определить как эффективный способ разделения ресурсов централизованных серверов между удаленными клиентами.

Однако иногда пользователям или процессам центральной сети может потребоваться обратиться к отдельным удаленным компьютерам.

Dial-out - режим, который предоставляет пользователям локальной сети доступ к отдельно стоящим удаленным компьютерам.

Удаленный пользователь часто требует помощи от профессионала, но затрудняется рассказать ему о своих проблемах, сообщить значения системных инсталляционных параметров и переменных. Поэтому хорошим средством оказания помощи этим пользователям является работа в режиме dial-out. Обслуживающий персонал подключается к компьютерам таких пользователей с помощью программного обеспечения удаленного управления. В результате профессионал из офиса получает полный контроль над компьютером удаленного пользователя.

12.4. Многопротокольность серверов удаленного доступа

В прошлом удаленный клиент почти всегда представлял собой тупой терминал (или ПК, работающий в режиме тупого терминала), присоединенный к модему и телефонной линии. Пользователь мог посылать команды модему, которые инициировали телефонный звонок и подключение к удаленному компьютеру. После процедуры логического входа с помощью пароля пользователь обычно получал доступ к UNIX-хосту, миникомпьютеру VAX/VMS или к мейнфрейму IBM. Объем передаваемых по телефонным линиям данных был очень небольшим и не предъявлял высоких требований к пропускной способности линий. Коды нажимаемых пользователем клавиш обычно сопровождались небольшим текстовым ответом от хоста, а вся вычислительная работа выполнялась централизовано серверами.

Сегодня картина существенно изменилась. Клиентские машины, например, IBM PC и Macintosh отнюдь не являются тупыми терминалами, напротив, часто они близки по мощности к серверам, с которыми они взаимодействуют удаленно. По одному и тому же удаленному соединению могут передаваться мегабайты трафика электронной почты, данные разделяемых файлов, сетевые новости и гипертекст серверов WWW, что требует значительно большей пропускной способности доя удовлетворения потребностей современного пользователя.

Простая терминальная сессия теперь заменена сетевыми протоколами как средством передачи данных между удаленными компьютерами. Однако последовательные линии, такие как коммутируемые телефонные линии, способны только передавать потоки битов без их деления на информационные пакеты. Поэтому для имитации работы удаленного пользователя в сети необходимо соответствующее программное или аппаратное обеспечение, которое должно преобразовывать битовый поток в последовательность пакетов. Для этих целей должны быть разработаны протоколы последовательных линий, которые могут быть использованы сетевым программным обеспечением для организации удаленных соединений.

Подобно тому, как для работы нескольких сетевых протоколов через один сетевой адаптер было разработано соответствующее мультиплексирующее программное обеспечение, для последовательных линий также должно быть разработано решение, обеспечивающее использование более чем одного протокола на одной последовательной линии. Большинство существовавших ранее протоколов удаленного доступа были разработаны для поддержки одного сетевого протокола, и поэтому их трудно приспособить для поддержки сразу нескольких сетевых

протоколов. Кроме того, протоколы сетевого уровня локальных сетей, такие как IPX и AppleTalk, были разработаны без учета возможности работы на медленных последовательных линиях. Они применяют небольшие времена тайм-аутов, частую рассылку широковещательных пакетов и имеют другие особенности, которые резко снижают производительность при использовании их для удаленного доступа.

Существует несколько важных факторов, которые нужно принимать во внимание при организации удаленного доступа в многопротокольной среде. Прежде всего - это поддержка множества сетевых протоколов через набор удаленных связей. Пользователи, звонящие в сеть и из сети, должны быть в состоянии подсоединиться к любой линии из группы телефонных каналов и использовать на ней протокол, наиболее соответствующий их потребностям. Для того, чтобы обеспечить такую возможность, сервер удаленного доступа должен поддерживать все распространенные протоколы последовательных линий - SLIP, CSLIP, PPP и ARAP (их краткая характеристика дается в таблице 12.1) - и быть в состоянии автоматически распознавать предпочтительный протокол или же давать возможность пользователю указать его.

Таблица 12.1.

Аббревиатура	Название	Описание
UUCP	Unix-to-Unix Copy Protocol	Разработан в Bell Labs в 1978 году. Обеспечивает пересылку одним сообщением файлов электронной почты, обычных файлов или командных файлов доя последующего выполнения
SLIP	Serial Line IP	Добавлен в начале 80-х к Berkeley Unix. Обеспечивает очень простую схему поддержки кадров данных для протоколов TCP/IP
CSLIP	Compressed SLIP	Усовершенствованный в 1988 г. SLIP. компрессирует 20-байтный заголовок IP пакета в заголовок из 3 байт
PPP	Point-to-Point Protocol	Впервые предложен в 1989 году как основное улучшение SLIP, позволяющее нескольким протоколам сетевого уровня разделять одну последовательную линию. Опубликовано большое количество стандартов для использования таких протоколов как IP, IPX, AppleTalk, NetBIOS, XNS и других поверх PPP.
ARAP	AppleTalk Remote Access Protocol	Введенный в 1991 году компанией Apple, ARAP обеспечивает схему кадрирования для протокола AppleTalk на последовательных линиях, а также стандартизует инкапсуляцию IP в пакеты Apple-Talk
AsyBEUI	Asynchronous NetBEUI	Частный протокол компании Microsoft, первоначально разработан для удаленного доступа к серверам LAN Manager

К сожалению, большая часть клиентского программного обеспечения для удаленного доступа, имеющегося сегодня на рынке, использует реализацию протокола PPP. поддерживающую только один сетевой протокол, например, IP.

Другим важным фактором, который нужно принимать во внимание, является различие в пропускной способности и эффективности использования последовательных линий удаленного доступа и кабельных связей локальных сетей. Протоколы локальных сетей используют многоуровневую вложенность, при которой каждый пакет содержит заголовки пакетов более верхних уровней, например, пакет IPX содержит заголовок пакета NCP. Для увеличения эффективности использования линий связи заголовки пакетов должны быть как можно меньше по сравнению с общей длиной пакета. В связи с этим, для удаленного доступа следует отдавать предпочтение протоколам с небольшими заголовками и большой длиной пакета. К сожалению, многие популярные протоколы локальных сетей демонстрируют прямо противоположные свойства (таблица 12.2).

По умолчанию стек TCP/IP поддерживает пакеты большой длины, что делает его более привлекательным при работе на глобальных связях. CSLIP включает сложный алгоритм сжатия IP-заголовков TCP-пакетов. Протокол PPP имеет возможность сжимать как заголовок, так и весь пакет. Протокол ARAP также может сжимать весь пакет.

Удаленные соединения, обычно использующие медленные соединения со скоростями 14.4 или 28.8 Кб/с, могут вызвать большие задержки принимаемых пакетов подтверждения. Для эффективного использования пропускной способности медленной линии протокол. используемый для передачи больших объемов данных, должен поддерживать алгоритм скользящего окна, который разрешает отправлять некоторое количество пакетов до получения подтверждения.

Таблица 12.2.

протокол	длина заголовка	длина пакета	сжатие
CSLIP	от 3 до 8	1500	нет
IP	20	1500	нет
TCP поверх IP	40	1500	да
UDP поверх IP	28	1500	нет
IPX	30	576	нет
SPX поверх IPX	42	576	да
NCP поверх IPX	38	576	нет
ARAP	*)	604	нет

*) Размер пакета ARAP определяется параметром MTU (максимальный блок передачи) протокола AppleTalk.

Методические рекомендации для преподавателей.

Для проведения данного занятия рекомендуется следующий расчет времени и методика его проведения.

I. Вводная часть - 5 мин.

- проверка наличия обучаемых;
- объявление темы, цели занятия, перечня учебных пособий и учебных вопросов.

II. Основная часть – 120 мин.

1. Введение - 5 мин.

Дать определение удаленного доступа.

2.Компоненты удаленного доступа - 20 мин.

Рассмотреть основные компоненты удаленного доступа.

3. Варианты удаленного доступа - 50 мин.

Рассмотреть различные варианты удаленного доступа, их характеристики и способы реализации, используя рис. 12.1.

4. Режимы Dial-in и Dial-out – 10 мин.

Провести краткое сравнение режимов удаленного доступа Dial-in и Dial-out по назначению и применению.

5. Многопротокольность серверов удаленного доступа – 35 мин.

Рассмотреть основные тенденции в развитии ПК в направлении к многопротокольным многофункциональным серверам, используя в качестве иллюстративного материала таблицы 12.1….12.2.

III. Заключительная часть – 10 мин.

- контрольный опрос
- ответы на вопросы обучаемых;
- подведение итогов занятия;
- задание на самоподготовку.