Содержание

Введение .........................................................................................................

1 Методы и средства удаленного доступа .......................................

1.1 Удаленный доступ. Варианты классификации методов удаленного доступа ...

1.2 Терминальные доступ .................................................................................. 1.3 Удаленный узел ............................................................................................

1.4 Удаленное управление .................................................................................

1.5 Виртуальные частные сети .......................................................................... 1.6 Удаленный доступ к Exchange 2003 по каналам HTTP

2 Протоколы удаленного доступа ....................................................................

2.1 Протокол SLIP .............................................................................................. 2.2 Протокол PPP ...............................................................................................

2.3 Протоколы защищенных каналов SSL, PPTP, IPSec ................................

2.4 Усугубление проблем безопасности при удаленном доступе.

2.5 Проверка подлинности Windows.......................................................

Заключение .........

**Введение**

В настоящее время эффективная работа, связанная с анализом и обработкой информации, невозможна без использования компьютерных сетей. Частные сети фирм сеть Интернет предоставляют доступ к базам данных и новостям (RSS). Кроме того, пользователь получает возможность коллективной работы и оперативных консультаций с коллегами и экспертами. Подобные услуги оказываются необходимыми для бизнесменов, врачей, учителей, госчиновников, журналистов и т.п. Для обеспечения такого рода работы в рамках некоторой структуры, например, фирмы, используют локальные сети.

Однако физическая реализация локальной сети не всегда возможна и/или удобна. Часто складывается ситуация, когда подразделения фирмы географически удалены друг от друга или работники находятся не в помещение офиса, а работают с клиентами на местах, выезжают в командировки. В этом случае важно организовать работу таким образом, чтобы, находясь в отдалении от локальной сети фирмы, они, тем не менее, могли подключиться к ней.

Для того чтобы обеспечить доступ к услугам локальной сети при отсутствии непосредственного подключения к ней, служат средства удаленного доступа к сети. Эти средства использую для связи удаленного (то есть не имеющего непосредственного подключении к локальной сети) компьютера с сетью коммутированные линии телефонных сетей общего пользования, аналоговые выделенные линии, цифровые линии сети ISDN (Integrated Services Network - цифровая сеть с интеграцией служб), сети коммутации пакетов общего пользования. Они обеспечивают передачу данных на любые расстояния.

Безусловным преимуществом таких систем является снижение затрат на обслуживание данной категории пользователей. Во-первых, пропадает необходимость выделения офисного пространства выездным или надомным работникам (например, менеджерам по продажам, программистам, дизайнерам, журналистам, переводчикам). Во-вторых, не нужно приобретать дополнительно мебель, компьютер и т.д. В-третьих, увеличивается эффективность работы компании ее филиалов, что достигается за счет автоматизации многих бизнес-процессов. Таким образом, удаленный доступ - это не роскошь, а еще один компонент успешного ведения современного бизнеса.

Естественно, организация системы удаленного доступа - задача не из легких. Конечно, можно обойтись и телефонным переговорами, отвлекая остальных сотрудников и руководство от выполнения их собственной работы. А время, как известно деньги: что не успел ты - успели твои конкуренты. Получить необходимые данные вовремя и быстро принять решение - значит успешно вести свой бизнес.

Универсального рецепта построения, который подходил бы абсолютно всем клиентам от небольшой фирмы, в которой требуется организовать доступ для нескольких человек, до крупной корпорации, где удаленно работают несколько тысяч сотрудников, не существует. Сколько пользователей - столько и решений. Основным фактором, влияющим на выбор, следует назвать размер компании. Исходя из ее потребностей и возможностей, определяется «прожиточный минимум» удаленного пользователя, то есть пакет необходимых ему программно-аппаратных средств. Теперь дело за малым: «подобрать» такое оборудование и методику организации удаленного доступа, которые решали бы данные задачи, а главное без переплаты за массу других ненужных функций.

В то же время не следует забывать о том, что данные в подобных системах передаются на большое расстояние и, часто, по сетям общего пользования, доступ к которым не ограничен.

Актуальность, безопасности передаваемых данных и их защиты от несанкционированного доступа в системах удаленного доступа требует особенно пристального внимания и применения специальных методик, которые гарантировали бы достаточную конфиденциальность и достоверность данных. В противном случае, хакер, подключившийся в качестве удаленного клиента или перехватывая трафик реально существующего клиента, сможет украсть данные являющееся коммерческой тайной или фальсифицировать их.

Задача, решаемая данной работой связана с решением обозначенной выше проблемы и может быть сформулирована следующим образом: Проанализировать и исследовать существующие способы обеспечения безопасности работы в системах удаленного доступа и выработать рекомендации по выбору конкретного способа.

1. **Методы и средства удаленного доступа.**

Под средствами удаленного доступа понимаются средства, необходимые для связи небольших локальных сетей и даже удаленных отдельных компьютеров с центральной локальной сетью предприятия. В качестве отдельных удаленных узлов могут также выступать банкоматы или кассовые аппараты, требующие доступ к центральной базе данных о легальных клиентах банка, пластиковые карточки которых необходимо авторизовать на месте. Банкоматы или кассовые аппараты обычно рассчитаны на взаимодействие с центральным компьютером по сети Х.25, которая в свое время специально разрабатывалась как сеть для удаленного доступа неинтеллектуального терминального оборудования к центральному компьютеру.

Методы удаленного доступа.

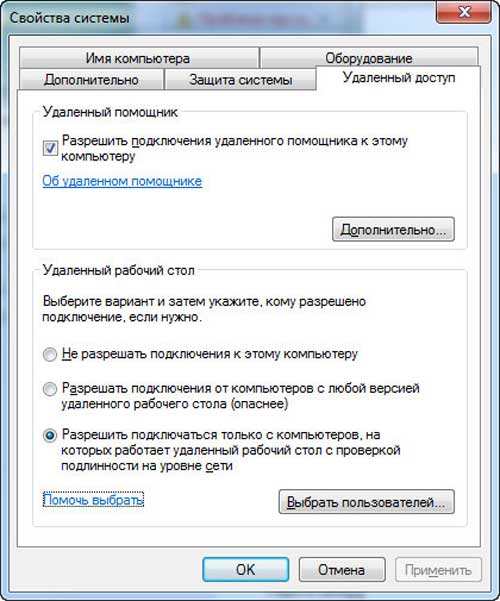
Метод удаленного доступа – это метод, при котором пользователь удаленного терминала с помощью специального программного обеспечения подключается по глобальной сети к другому компьютеру, как локальный узел. Этот способ часто используется на мини-компьютерах, но мало распространен в ЛВС. Удаленной управление (remote control) – это метод, который позволяет удаленному пользователю получить контроль над локальными ПК в ЛВС корпорации (т. е. управлять одним из ПК в ЛВС). Скорость проведения сеанса и его возможности зависят от характеристик управляемого ПК, т. к. именно на нем выполняется обработка всех сетевых команд. Коды клавиш, нажимаемых на удаленном ПК, посылаются в управляемый ПК, а все изменения на экране управляемого выводятся на экран удаленного ПК Удаленное управление Используемые файлы и прикладные программы не загружаются в удаленный ПК. Передача через модем со скоростью 2400 – 57600 бит/с. Недостаток метода: для выполнения одной работы задействованы два ПК. Метод удаленного узла (remote node) основан на использовании сервера удаленного доступа, который служит своего рода «регулировщиком» и позволяет отдельному удаленному ПК или ЛВС связываться с центральной ЛВС. Программное обеспечение удаленного ПК, реализующее функции удаленного узла, позволяет ему функционировать как полноценному пользователю ЛВС. Таким программным обеспечением может быть Windows 98, NT Work Station. Как только связь установлена, телефонные линии становятся «прозрачными» и пользователь может работать со всеми ресурсами сети, как будто он сидит за ПК, непосредственно подключенным к ЛВС. Сервер удаленного доступа может быть реализован: в виде модема со встроенным специальным ПО; либо быть сервером ЛВС, на котором выполняются программы удаленного узла желательно, чтобы на удаленном ПК помимо сетевого системного ПО находилось все прикладное ПО, необходимое для сеанса связи: все выполняемые (\*.exe) файлы; необходимые Windows-приложения. В противном случае их необходимо будет передавать с сетевого сервера на канал связи. Т. к. они имеют, как правило, большие объемы данных, то это потребует значительных затрат времени. Удаленный узел как каждый полноценный пользователь ЛВС, удаленный узел имеет свой сетевой адрес. Сетевая операционная система преобразует сетевые пакеты, которые нужно передать через модем, из формата протокола IP или IPX в формат, совместимый со стандартом последовательной передачи. С появлением все большего количества программ, поддерживающих архитектуру «клиент - сервер», усиливается тенденция на программное обеспечение для удаленных узлов, т. к. такие программы позволяют обрабатывать большие файлы данных на серверах ЛВС, а на удаленный ПК передать только результаты обработки.

**1.1 Удаленный доступ. Варианты классификации методов удаленного доступа.**

Нередко встречаются ситуации, когда появляется необходимость получить доступ к удаленному компьютеру - к его рабочему столу. Чаще всего это происходит тогда, когда вам нужно помочь кому-то из родственников или друзей в освоении всяких компьютерных премудростей.

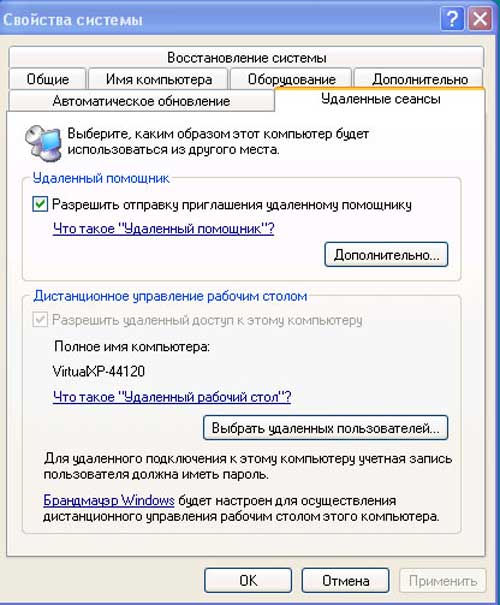
Например, звонит вам матушка и говорит: "Слушай, а почему у меня на компьютере выдается какое-то страшное сообщение, которое я не могу прочитать? Они просят нажать какую-то кнопочку - мне нажимать?" В этом случае, конечно, вам лучше всего своими глазами увидеть, что именно там спрашивается и какие кнопочки предлагаются на выбор, а то мало ли что...

Кроме того, удаленный доступ бывает очень полезен, когда на компьютере, находящемся далеко, нужно установить или настроить какое-нибудь программное обеспечение. Да и к своему компьютеру иногда бывает нужен доступ на расстоянии - всякие случаи бывают. Как и с помощью чего это все делается? В операционной системе Windows удаленный доступ можно осуществлять средствами самой системы. Откройте "Панель управления - Система - Удаленный доступ". Там нужно включить опцию разрешения подключения удаленного помощника и удаленного рабочего стола.



Настройки удаленного доступа в Windows 7

Если на вашем и на удаленном компьютере установлена Windows 7, тогда среди опций удаленного рабочего стола выбирайте третий вариант - подключаться к удаленному рабочему столу с проверкой подлинности на уровне сети. Если планируется подключаться к Windows XP, тогда надо выбрать второй вариант.



Включение удаленного помощника в Windows XP

Windows 7 поддерживает два разных режима:

- подключение удаленного помощника;

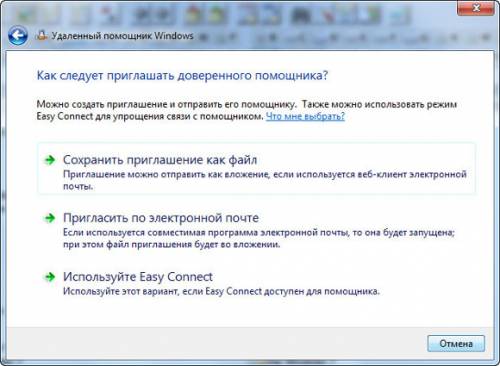
- дистанционное управление рабочим столом.

Удаленный помощник работает во всех версиях Windows от XP до Windows7. При этом вы будете видеть рабочий стол вашего абонента и сможете обмениваться с ним сообщениями в чате (мало ли, может, у вас нет возможности одновременно разговаривать с ним по телефону), также он может дать вам доступ к управлению компьютером: вы получите возможность своей мышью и клавиатурой совершать различные действия на его компьютере.

Дистанционное управление рабочим столом поддерживается только в Windows 7, причем кроме версий "Начальная", "Домашняя базовая" или "Домашняя расширенная". При дистанционном управлении ваш абонент будет видеть экран блокировки, а вы сможете зайти на его компьютер под определенным пользователем и работать так же, как будто вы сидите за этим компьютером.

Подключение удаленного помощника

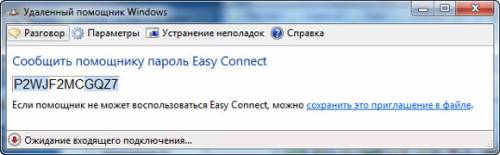
На обоих компьютерах запустите программу "Удаленный помощник Windows". На вызываемом компьютере щелкните "Пригласить того, кому вы доверяете для оказания помощи". Далее может быть три варианта: сохранить приглашение в виде файла, отправить приглашение по электронной почте, использовать Easy Connect.

[](http://umeha.3dn.ru/_pu/59/49563386.jpg)

Вид приглашения

Первый вариант - создается специальный файл приглашений, после чего его надо как-то передать абоненту - например, через мессенджер. Второй вариант - практически то же самое, только этот файл отправляется абоненту через электронную почту. Третий вариант, который может быть недоступным, - отправка приглашения через специальный сервис Easy Connect.

После того как вы выберете любой из вариантов, у вас на экране возникнет пароль, который должен будет ввести ваш абонент для доступа к вашему компьютеру.

[](http://umeha.3dn.ru/_pu/59/56031404.jpg)

Пароль

Если абонент получил файл приглашения, он его должен запустить - появится запрос пароля. При использовании Easy Connect у него появится этот запрос без всяких файлов.

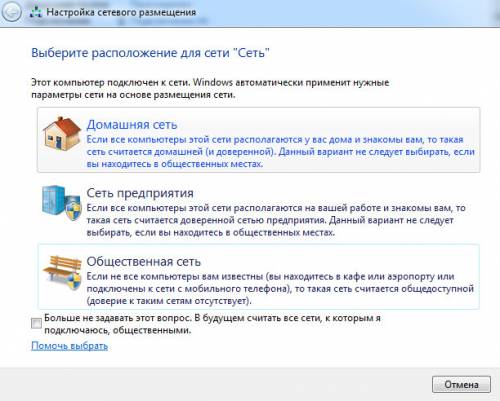
После ввода пароля компьютеры попробуют установить соединение и, если все получилось, у вас появится запрос на подтверждение подключения удаленного помощника. После подтверждения у абонента на компьютере появится ваш рабочий стол.

Удаленный рабочий стол

В окне удаленного помощника вызывающего абонента есть опция "Запросить управление". Если он ее нажмет, то у вас появится запрос на разрешение удаленному помощнику управлять вашим рабочим столом. При подтверждении удаленный помощник сможет производить действия на вашем компьютере.

Надо сказать, что далеко не во всех случаях удается установить режим подключения удаленного помощника. Это подключение может блокироваться брандмауэрами (они же файрволы, они же сетевые экраны), комплексными средствами защиты (например, Kaspersky Internet Security). Для Windows XP и Windows Server 2003 роутер (маршрутизатор) должен поддерживать сетевую технологию UPnP.

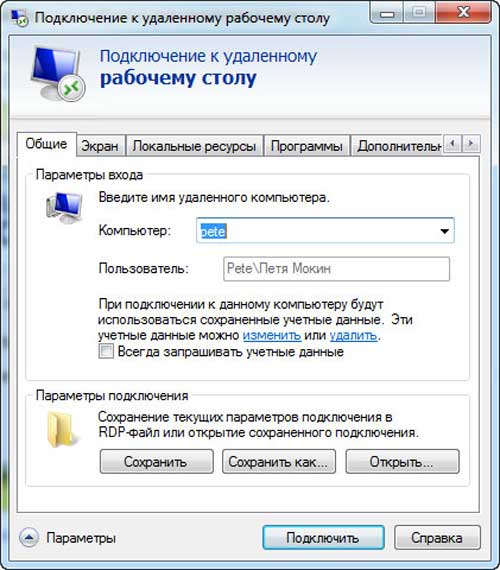
Также домашние сети обоих компьютеров в Windows Vista или Windows 7 должны быть в режиме "Домашняя сеть" или "Сеть предприятия", но не "Общественная сеть".

[](http://umeha.3dn.ru/_pu/59/85091029.jpg)

Параметры сети

Дистанционное управление рабочим столом

Запускаете программу "Подключение к удаленному рабочему столу". Там делаете нужные вам настройки (параметры экрана, звука и так далее), вводите имя компьютера и имя пользователя, под которым вы должны зайти.



Настройки подключения

Нажимаете кнопку "Подключить", после чего, если компьютер будет найден и подключение возможно, у вас запросят пароль пользователя. Эти данные можно сохранить, чтобы в следующий раз подключаться без ввода пароля.

После установления соединения перед вами возникнет рабочий стол удаленного компьютера, на котором вы сможете работать так, как будто вы сидите прямо за ним. На самом удаленном компьютере в этот момент завершится сеанс работы и появится экран выбора пользователей. Если пользователь удаленного компьютера снова выполнит вход - ваш сеанс подключения к удаленному рабочему столу завершится.

[](http://umeha.3dn.ru/_pu/59/03953099.jpg)

Рабочий стол удаленного компьютера поверх обычного рабочего стола

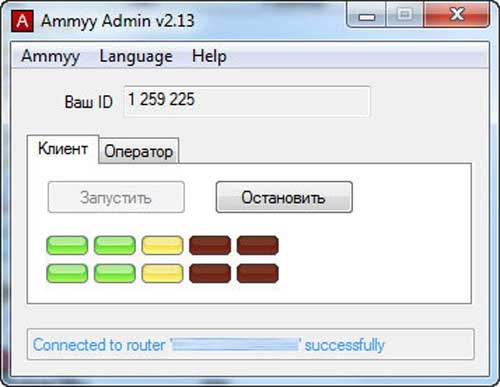
Безопасность

Для безопасности рекомендуется включать возможность удаленного доступа только непосредственно перед планируемым сеансом. После того как все будет сделано, возможность удаленного доступа (что помощника, что управления рабочим столом) следует отключить.

Другие способы. Есть и другие способы удаленного подключения. Существует не один десяток соответствующих программ, которые реализуют подобную возможность.

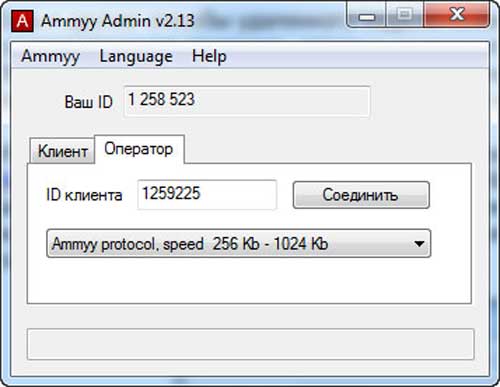
Эти программы бывают как сложные и продвинутые вроде [RAdmin](http://www.radmin.ru/), так и простенькие, которые практически не требуют никаких настроек.

Из несложных и эффективных могу порекомендовать бесплатную утилиту Ammyy Admin ([скачать](http://www.ammyy.com/AMMYY_Admin.exe)). Она предельно простая и удобная. Скачиваете программу, запускаете ее на своем и удаленном компьютере. На удаленном компьютере нужно выбрать закладку "Клиент" и нажать кнопку "Запустить". Программа сообщит свой идентификационный номер - ID.



Запущенный клиент

На своем компьютере нужно открыть закладку "Оператор", там вписать ID клиента (цифры запомнятся на будущее) и нажать кнопку "Соединить".



Запущенный оператор

После этого запустится удаленный рабочий стол, которым вы сможете управлять с помощью мыши и клавиатуры.

Удаленный рабочий стол

Как видите, все предельно просто и понятно. Правда, в отличие от базовых средств Windows 7 управление удаленным рабочим столом заметно подтормаживает, но обычно такой вид доступа нужен для того, чтобы произвести несколько несложных действий или даже просто посмотреть, что там происходит на экране, поэтому данный способ вполне можно использовать.

**1.2 Терминальный доступ.**

Терминальный доступ — доступ к [информационной системе](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) (ИС), организованный так, что локальная [машина-терминал](http://ru.wikipedia.org/w/index.php?title=%D0%9C%D0%B0%D1%88%D0%B8%D0%BD%D0%B0-%D1%82%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB&action=edit&redlink=1) не выполняет вычислительной работы, а лишь осуществляет перенаправление ввода информации (от [мыши](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%BC%D1%8B%D1%88%D1%8C) и [клавиатуры](http://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D0%B2%D0%B8%D0%B0%D1%82%D1%83%D1%80%D0%B0)) на центральную машину ([терминальный сервер](http://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80)) и отображает графическую информацию на [монитор](http://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%BD%D0%B8%D1%82%D0%BE%D1%80_(%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%BE)). Причем вся вычислительная работа в [терминальной системе](http://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) выполняется на центральной машине.

В более широком смысле под терминальным доступом подразумевается такая организация работы, когда информация хранится и обрабатывается на некотором удалённом сервере, а оборудование пользователя выполняет лишь функцию ввода и вывода. Пример: терминалы для оплаты покупок банковскими картами. Терминал считывает с карты, данные для [аутентификации](http://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) покупателя. Далее сама аутентификация и транзакция производятся на сервере банка. Результат операции — списание средств или отказ — передаются обратно на терминал.

Исторически терминальный доступ впервые был организован на компьютерах, способных одновременно обслуживать несколько вычислительных процессов. Это позволило более рационально распределять вычислительные ресурсы между пользователями первых очень дорогих вычислительных машин. С появлением дешевых [персональных компьютеров](http://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) (ПК) роль терминального доступа стала несколько снижаться, так как сложилось мнение, что достаточную производительность ИС можно получить на рабочем столе каждого пользователя ПК.

Однако в дальнейшем стало очевидным, что дешевизна ПК не в состоянии компенсировать ежедневные затраты на сопровождение большого количества рабочих пользователей, обладающих якобы преимуществами из-за возможности персонализации настроек [операционных систем](http://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) (ОС) и [ПО](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5). Реально (в крупных организациях), наличие большого количества «разношерстного» оборудования вместо достоинств создает дополнительные сложности пользователям и [системным администраторам](http://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80). Вопросы обеспечения безопасности ИС, также потребовали пересмотра взглядов и возврата к терминальному доступу, как более унифицированному и экономически оправданному.

Так же с точки зрения обеспечения информационной безопасности и препятствия изъятия данных с рабочих станций все чаще и чаще крупные компании используют терминальный доступ к чувствительным ресурсам компании, таким как Бухгалтерские, Юридические, АБС и многие другие.

**1.3 Удаленный узел.**

Одним из вариантов удаленного доступа типа компьютер - сеть является режим удаленного узла (remote node). Программное обеспечение удаленного узла на клиентской машине позволяет последовательному порту и модему (или терминальному адаптеру ISDN) стать медленным узлом удаленной локальной сети, взаимодействующим обычным способом с сетевыми операционными системами при разделении их ресурсов. В локальной сети должен быть установлен сервер удаленного доступа, поддерживающий режим удаленного узла. Это означает, что сервер должен поддерживать один из протоколов канального уровня, используемых на глобальном канале. Протокол канального уровня необходим для связи удаленного компьютера с центральной локальной сетью. Так как чаще всего этот канал является коммутируемым каналом телефонной сети или ISDN, то сервер удаленного доступа должен поддерживать протоколы РРР и SLIP, используемые на этих каналах. В сети Х.25 или frame relay сервер удаленного доступа должен поддерживать протоколы этих сетей, то есть протоколы LAP-B и Х.25/3 для первого случая и LAP-F для второго (если сеть frame relay поддерживает только постоянные виртуальные каналы). При получении по глобальному каналу кадров соответствующего протокола, сервер, работающий в режиме удаленного узла, извлекает из кадра, например, РРР, пакеты тех общих протоколов сетевого уровня, по которым работают удаленный компьютер и компьютеры локальной сети. Такими протоколами могут быть протоколы IP, IPX или немаршрутизируемый протокол NetBEUI. Далее вступают в работу протоколы верхних уровней, и пользователь получает такой же доступ, как если бы его компьютер находился непосредственно в локальной сети, но с небольшим исключением — скорость обмена его компьютера с остальными компьютерами удаленной сети зависит от пропускной способности глобального канала связи.

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 удаленная загрузка больших программ неразумна, так как самый скоростной модем 33,6 Кбит/с работает со скоростью, составляющей только 3 % от скорости сегмента Ethernet, и программа, которая в локальной сети загружается за 30 с, будет загружаться по удаленной связи в течение 15-20 минут. Поэтому в режиме удаленного узла локальные копии программ, как правило, эффективнее.

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.

Компьютер, использующий режим удаленного узла, наиболее эффективно работает с системами клиент-сервер, так как в этом случае трафик по глобальному каналу обычно передается не очень интенсивный — запрос клиента обрабатывается на сервере, а по глобальному каналу передается только ответ. В режиме клиент-сервер работают многие корпоративные СУБД (например, Oracle, Informix, Microsoft SQL Server), а также приложения, ориентированные на эту архитектуру. Многие административные утилиты современных операционных систем поддерживают такой режим, например, User Manager for Domains Windows NT.

Серверы, работающие в режиме удаленного узла, выполняют свои функции различным образом.

Первый вариант — это реализация в сервере удаленного узла функционального эквивалента маршрутизатора с WAN-портами для асинхронных модемов, ISDN-линий или асинхронного доступа к PAD X.25. Этот вариант универсален, так как обеспечивает доступ как отдельных компьютеров, так и локальных сетей. Однако данный вариант при подключении отдельного компьютера избыточен, поскольку требует выделения отдельного номера сети каждому подключившемуся к сети пользователю.

Второй вариант основан на работе сервера удаленного узла в режиме шлюза. Если удаленные клиенты и локальная сеть работают на протоколе IP, то всем удаленным компьютерам присваивается один и тот же номер IP-сети, совпадающий с номером локальной сети, к которой они получают доступ. В этом случае сервер выполняет функции посредника по протоколу ARP (говорят, что он поддерживает режим proxy ARP), отвечая компьютерам локальной сети своим МАС - адресом на запросы о IP-адресах, принадлежащих удаленным подключившимся узлам. Для протокола NetBIOS работа сервера в режиме шлюза — это единственно возможный режим работы, так как этот протокол не может маршрутизироваться.

В сервере удаленного узла могут быть реализованы оба варианта работы, которые выбираются в зависимости от типа клиента (компьютер или сеть), а также протокола.

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

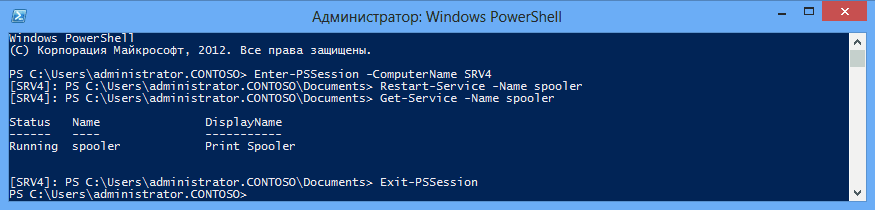
**1.4 Удаленное управление.**

Самый простой способ удаленного управления — интерактивно открыть удаленную сессию и в ней выполнить нужные действия. Например, откроем сессию на компьютер SRV4 и рестартуем на нем сервис печати:

Enter-PSSession -ComputerName SRV4 Restart-Service -Name spooler

Посмотрим состояние сервиса и закроем удаленную сессию:

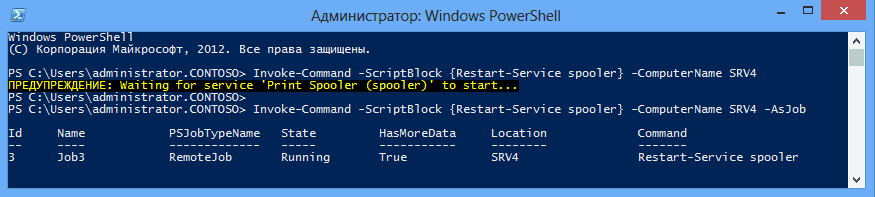
Get-Service –Name spooler Exit-PSSession

[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr1.png)

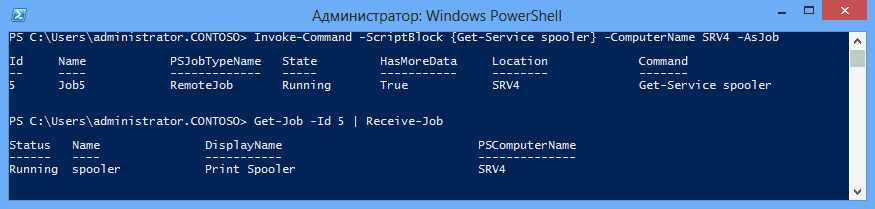
Интерактивная работа подходит для решения несложных задач удаленного администрирования. Если же надо автоматизировать процесс, то лучше воспользоваться командлетом Invoke-Command. Вот так с его помощью можно сделать то же самое действие:

Invoke-Command -ScriptBlock {Restart-Service spooler} -ComputerName SRV4

Эта команда откроет удаленную сессию на SRV4, выполнит блок команд, указанный в параметре -ScriptBlock, и закроет сессию. А чтобы задание выполнялось в фоновом режиме, дополнительно можно указать параметр -AsJob.

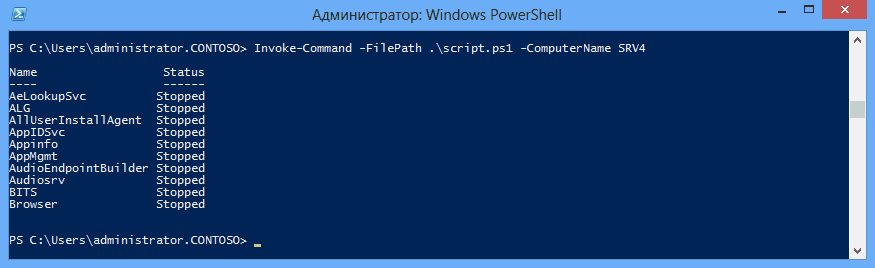
[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr2.png)

Следует помнить о том, что при работе в фоновом режиме PowerShell не возвращает результат. Для его получения придётся воспользоваться командлетом Receive-Job.

[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr3.png)

Для того, чтобы выполнить не пару-тройку команд, а какой-либо скрипт, у Invoke-Command есть параметр –FilePath, который можно использовать вместо –ScriptBlock для определения файла сценария. Для примера я создал скрипт, который выводит список остановленных служб и запустил его на удаленной машине SRV4:

Invoke-Command -FilePath .\script.ps1 -ComputerName SRV4

[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr4.png)

Управление «один ко многим»

Довольно часть возникает необходимость параллельно выполнить одну задачу на нескольких компьютерах. Это довольно легко можно сделать с помощью того же Invoke-Command. Например, имена компьютеров можно просто перечислить через запятую:

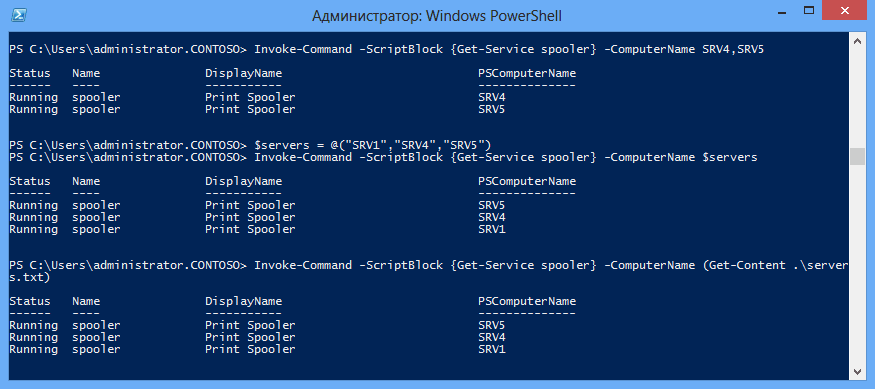
Invoke-Command -ScriptBlock {Restart-Service spooler} -ComputerName SRV4, SRV5

Поместить в переменную:

$servers = @ (″SRV1″, ″SRV2″, ″SRV3″) Invoke-Command -ScriptBlock {Restart-Service spooler} -ComputerName $servers

Или взять из файла:

Invoke-Command -ScriptBlock {Restart-Service spooler} -ComputerName` (Get-Content .\servers.txt)

[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr5.png)

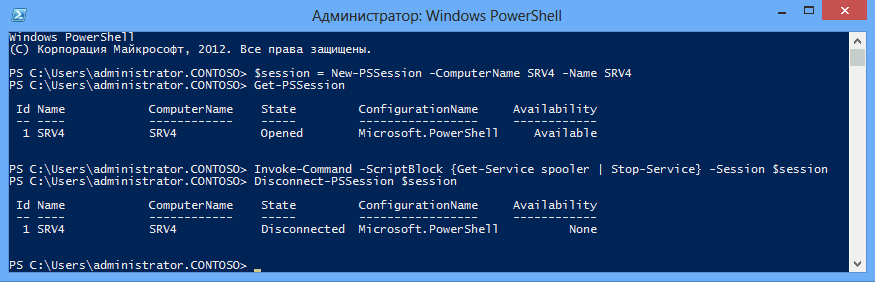
Примечание: у Invoke-Command есть параметр ThrottleLimit, ограничивающий максимальное количество компьютеров, которыми можно управлять одновременно. По умолчанию этот параметр равен 32. При необходимости его можно изменить, но учтите, что повышение этого параметра увеличит нагрузку на процессор и память вашего компьютера, поэтому эту операцию нужно выполнять с большой осторожностью.

Сессии

Каждый раз при выполнении Invoke-Command создается новая сессия, на создание которой тратится время и ресурсы. Чтобы этого избежать мы можем открыть одну сессию, в которой и выполнять все команды. Например, откроем сессию с именем SRV4 на компьютер SRV4 и поместим ее в переменную $session, а затем этой сессии выполним нашу задачу (остановим многострадальный spooler):

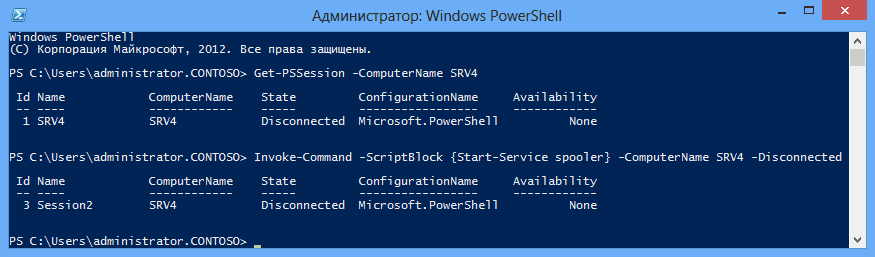
$session = New-PSSession -ComputerName SRV4 -Name SRV4  
Invoke-Command -ScriptBlock {Get-Service spooler | Stop-Service} ` -Session $session

Сессия будет активна до того момента, пока мы не выйдем из консоли PowerShell. Также сессию можно закрыть - Disconnect-PSSession или удалить - Remove-PSSession.

[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr6.png)

А теперь несколько интересных возможностей, появившихся в PowerShell 3.0. Если раньше при выходе из сессии или закрытии консоли сессия удалялась, то в PS 3.0 при закрытии сессия переходит в состояние disconnected. Мы можем открыть новый сеанс на этом же (или любом другом) компьютере и выполнить команду прямо в этой отключенной сессии. В качестве примера стартуем на компьютере SRV4 сервис печати, остановленный в прошлый раз:

Invoke-Command -ScriptBlock {Start-Service spooler} ` -ComputerName SRV4 -Disconnected

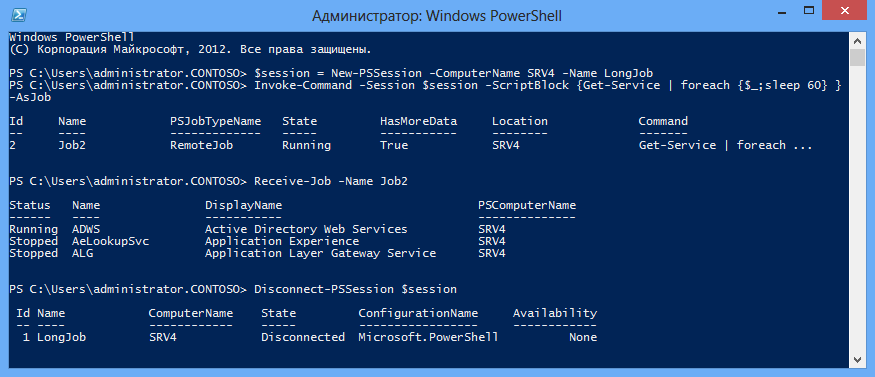
[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr7.png)

Еще один вариант использования отключенных сессий — запуск длительных по времени задач. Для примера откроем сессию c именем LongJob на SRV4 и запустим в ней фоновое задание, которое будет выводить список сервисов с интервалом в 1 минуту:

$session = New-PSSession -ComputerName SRV4 -Name LongJob  
Invoke-Command -Session $session -ScriptBlock` {Get-Service | foreach {$\_; sleep 60}} -AsJob

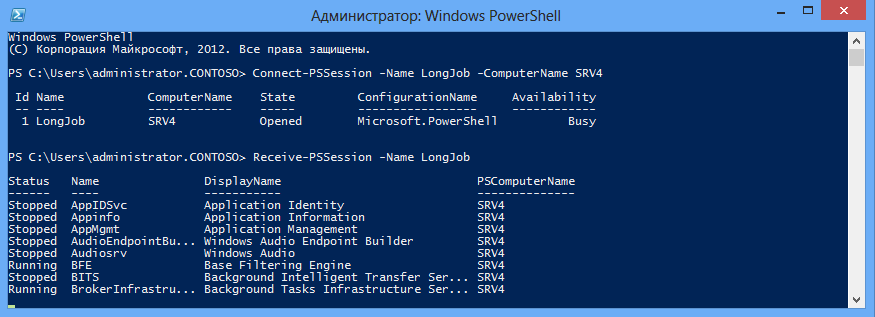
Посмотрим, как выполняется задача и закроем сессию:

Receive-Job -Name Job2 Disconnect-PSSession $session

[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr8.png)

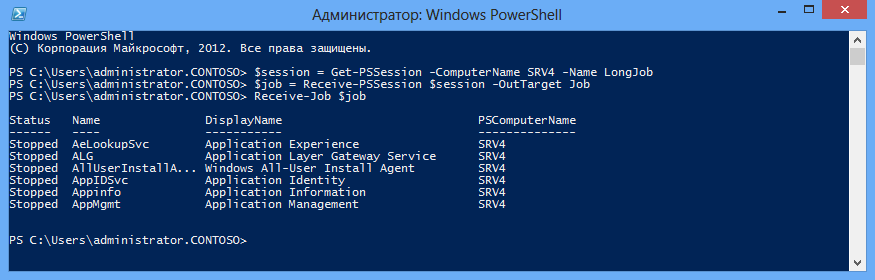
Идем на другой компьютер и открываем консоль, подключаемся к сессии LongJob и с помощью командлета Receive-PSSession получаем результат выполнения задания:

Connect-PSSession -Name LongJob -ComputerName SRV4  
Receive-PSSession -Name LongJob

[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr9.png)

Или еще вариант, без явного подключения к сессии с помощью Connect-PSSession:

$session = Get-PSSession -Name LongJob - ComputerName SRV4  $job = Receive-PSSession $session -OutTarget Job Receive-Job $job

[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr10.png)

Примечание: для того, чтобы результат остался в системе, Receive-Job надо использовать с параметром - Keep.

Неявное удаленное управление. Ещё один, довольно нестандартный способ удаленного управления — неявное удаленное управление (Implicit remoting). Используя его можно, не создавая удаленной сессии, локально выполнять командлеты, находящиеся на удаленном компьютере.

Для примера берем обычную рабочую станцию, без установленных средств удаленного администрирования. Создаем удаленную сессию с контроллером домена SRV4 и импортируем в эту сессию модуль Active Directory:

$session = New-PSSession -ComputerName SRV4 Invoke-Command {Import-Module Active Directory} -Session $session

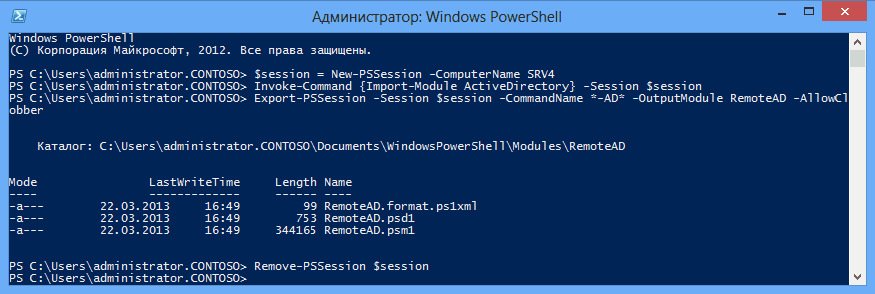
Затем экспортируем из удаленной сессии командлеты Active Directory и помещаем их в локальный модуль RemoteAD:

Export-PSSession -Session $session -CommandName \*-AD\* -OutputModule RemoteAD`-AllowClobber

Эта команда создаст в папке WindowsPowerShell\Modules\RemoteAD новый модуль PowerShell.

Загружены будут только командлеты с именами, соответствующими шаблону \*-AD\*. При этом сами командлеты не копируются на локальный компьютер. Локальный модуль служит своего рода ярлыком, а сами команды будут выполняться на удаленном контроллере домена.

После создания модуля удаленную сессию можно закрыть, она больше не понадобится.

[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr11.png)

Импортируем новый модуль в текущий сеанс (в PS 3.0 можно этот шаг пропустить):

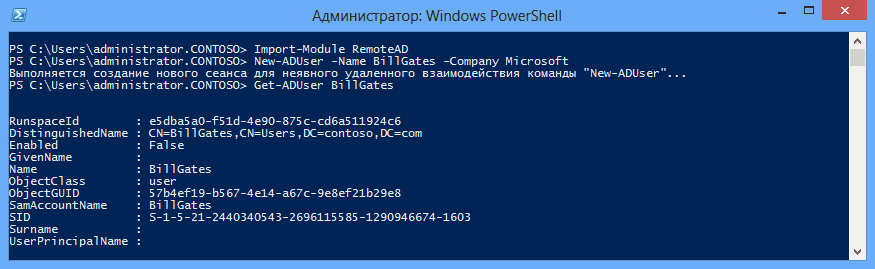
Import-Module RemoteAD

А теперь внимание — мы не открываем удаленную сессию с контроллером домена, где расположены командлеты. Не нужно явно запускать этот сеанс — это можно сделать неявно, попытавшись выполнить удаленные командлеты:

New-ADUser -Name BillGates -Company Microsoft Get-ADUser BillGates

При этом будет восстановлено удаленное подключение к контроллеру домена, после чего команда будет передана на контроллер домена и там выполнена. Результат выполнения будет сериализован в XML и передан по сети на локальный компьютер, где будет выполнена десериализация в объекты, с которыми может работать PowerShell.

Удаленный сеанс будет активным до тех пор, пока вы не закроете консоль или не удалите модуль RemoteAD.

[](http://windowsnotes.ru/wp-content/uploads/2013/03/psr12.png)

Неявное удаленное управление позволяет работать с командлетами на удаленном компьютере практически так же, как если бы они были установлены на локальной машине. При этом все необходимые командлеты всегда под рукой, что довольно удобно.

В заключение скажу, что на данный момент PowerShell Remoting является основным инструментом для удаленного управления операционными системами Windows. Поэтому знать о его возможностях и уметь ими пользоваться просто необходимо любому Windows-администратору.

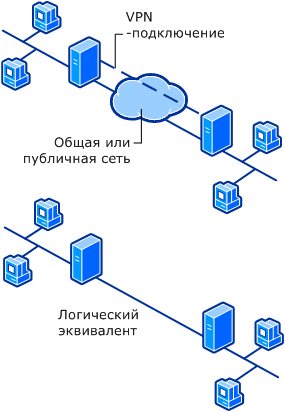
**1.5 Виртуальные частные сети.**

Виртуальная частная сеть (VPN) представляет собой подключение типа «точка-точка» в частной или общедоступной сети, например, в Интернете. VPN-клиенты используют специальные TCP/IP-протоколы, называемые туннельными протоколами, обеспечивающие установление защищенного канала обмена данными между двумя компьютерами. С точки зрения взаимодействующих компьютеров между ними организуется выделенный канал типа «точка-точка», хотя в действительности, соответствующие данные передаются через Интернет, как и любые другие пакеты. При обычной реализации VPN клиент инициирует виртуальное подключение типа «точка-точка» к серверу удаленного доступа через Интернет. Сервер удаленного доступа отвечает на вызов, выполняет проверку подлинности вызывающей стороны и передает данные между VPN-клиентом и частной сетью организации.

Для эмуляции канала типа «точка-точка» к данным добавляется заголовок (выполняется инкапсуляция). Этот заголовок содержит сведения о маршрутизации, которые обеспечивают прохождение данных по общей или публичной сети до конечной точки. Для эмуляции частного канала и сохранения конфиденциальности передаваемые данные шифруются. Дополнительные сведения о туннельных протоколах, поддерживаемых в этой версии Windows, см. на странице Туннельные протоколы VPN (страница может быть на английском языке).

Требования к установке см. в разделе Требования для установки RRAS в качестве VPN-сервера.

VPN-подключение



Существует два типа VPN-подключений.

VPN-подключение удаленного доступа

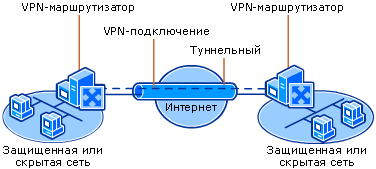
VPN-подключение удаленного доступа дает пользователям возможность работать дома или в дороге, получая доступ к серверу частной сети посредством инфраструктуры общедоступной сети, например Интернета. С точки зрения пользователя VPN-подключение представляет собой подключение типа «точка-точка» между клиентским компьютером и сервером организации. Реальная инфраструктура общей или публичной сети не имеет значения, поскольку данные передаются подобно тому, как если бы они передавались по выделенному частному каналу.

VPN-подключение типа «сеть-сеть»

VPN-подключение типа «сеть-сеть» (иногда называется VPN-подключением типа «маршрутизатор-маршрутизатор») предназначено для маршрутизации подключений между различными филиалами организации, а также между организациями через общедоступную сеть, обеспечивая при этом защиту подключений. Если сети соединены через Интернет, как показано на следующем рисунке, маршрутизатор с поддержкой VPN пересылает пакеты другому такому маршрутизатору через VPN-подключение. С точки зрения маршрутизаторов VPN-подключение на логическом уровне функционирует как выделенный канал уровня передачи данных.

С помощью VPN-подключений можно соединить две частные сети. VPN-сервер обеспечивает маршрутизируемое подключение к сети, к которой присоединен VPN-сервер. Вызывающий маршрутизатор проходит проверку подлинности на отвечающем маршрутизаторе, и в целях взаимной проверки подлинности отвечающий маршрутизатор проходит проверку подлинности на вызывающем маршрутизаторе. При VPN-подключении типа «сеть-сеть» пакеты, отправляемые с любого из маршрутизаторов через VPN-подключение, обычно формируются не на маршрутизаторах.

VPN-подключение между двумя удаленными сайтами через Интернет



Свойства VPN-подключений

Инкапсуляция. Обеспечивается инкапсуляция частных данных с использованием заголовка, содержащего сведения о маршрутизации для передачи этих данных по транзитной сети. Примеры инкапсуляции см. на странице [Туннельные протоколы VPN (страница может быть на английском языке)](http://go.microsoft.com/fwlink/?linkid=140602) (<http://go.microsoft.com/fwlink/?linkid=140602>).

Проверка подлинности. Существует три различные формы проверки подлинности для VPN-подключений:

Проверка подлинности на уровне пользователя по протоколу PPP. Для установления VPN-подключения VPN-сервер выполняет проверку подлинности VPN-клиента, пытающегося установить подключение, на уровне пользователя по протоколу PPP и проверяет, имеет ли VPN-клиент соответствующие разрешения на доступ. При взаимной проверке подлинности VPN-клиент также выполняет проверку подлинности VPN-сервера, что гарантирует защиту от компьютеров, выдающих себя за VPN-серверы.

Проверка подлинности на уровне компьютера по протоколу IKE. Чтобы установить сопоставление безопасности IPSec, VPN-клиент и VPN-сервер используют протокол IKE для обмена сертификатами компьютеров или предварительным ключом. В обоих случая VPN-клиент и VPN-сервер выполняют взаимную проверку подлинности на уровне компьютера. Проверка подлинности на основе сертификата компьютера является одним из самых надежных способов и рекомендуется к применению. При проверке подлинности на уровне компьютера используются подключения по протоколам L2TP/IPSec или IKE версии 2.

Проверка подлинности источника данных и обеспечение целостности данных. Чтобы убедиться в том, что источником отправленных по VPN-подключению данных является другая сторона VPN-подключения и что они переданы в неизмененном виде, в данные включается контрольная сумма шифрования, основанная на ключе шифрования, который известен только отправителю и получателю. Функции проверки подлинности источника данных и обеспечения целостности данных доступны для подключений по протоколам L2TP/IPSec и IKE версии 2.

Шифрование данных. Для обеспечения конфиденциальности данных при передаче по общей или публичной транзитной сети они шифруются отправителем и расшифровываются получателем. Успешность процессов шифрования и расшифровки гарантируется в том случае, когда отправитель и получатель используют общий ключ шифрования.

Содержание перехваченных пакетов, отправленных по VPN-подключению в транзитной сети, понятно только владельцам общего ключа. Одним из важнейших параметров безопасности является длина ключа шифрования. Для определения ключа шифрования можно использовать различные методики вычислений. Однако при возрастании размера ключа шифрования использование подобных методик требует большей вычислительной мощности и большего времени для выполнения этих вычислений. Поэтому для обеспечения конфиденциальности данных рекомендуется использовать ключ максимально возможной длины.

**1.6 Удаленный доступ к Exchange 2003 по каналам HTTP**.

Использование Outlook 2003 для доступа к почтовому ящику Exchange.

Новая возможность Outlook 2003 для доступа к почтовому ящику Exchange. Благодаря сочетанию Microsoft Outlook 2003, Windows Server 2003 и Microsoft Exchange Server 2003 открываются новые возможности для подключения клиента Outlook 2003 к Exchange 2003 по каналам HTTP. Соединение не просто использует HTTP: Outlook заключает вызов удаленных процедур (RPC) к Exchange 2003 в оболочку HTTP, обеспечивая соединение локального клиента Outlook 2003 с удаленным сервером Exchange 2003 с любой машины, располагающей Web-браузером. Это полезный метод, особенно если учесть недостатки других способов: Outlook Web Access (OWA), который совершенствуется, но по-прежнему уступает полноценному клиенту Outlook, или доступ к Outlook через соединение VPN, которое часто блокируется сетевыми провайдерами. Чтобы использовать RPC over HTTP, необходимо понимать механизм и требования к конфигурациям как клиента, так и сервера.

Взаимодействие Outlook и Exchange

Во всех версиях Outlook для взаимодействия с любой версией Exchange Server применяется интерфейс Messaging API (MAPI) и вызовы удаленных процедур (RPC) для обработки вызовов MAPI. Протокол RPC не располагает встроенными функциями повышения надежности, это свойство определяется базовым транспортным протоколом, таким как TCP/IP. При использовании менее надежного транспортного средства, например, UDP, приложение на базе RPC должно обеспечить функции тайм-аута и повторной пересылки.

RPC-соединения Outlook-Exchange начинаются с процедуры квитирования между клиентом Outlook и сервером Exchange через хорошо известный порт (например, UDP-порт 135 — порт подключения конечных точек RPC) с последующей организацией канала связи через динамически назначаемый порт (обычно в диапазоне от 1024 до 1100). Назначать порты можно с помощью параметров реестра, но обычно администраторы сетей и брандмауэров не разрешают организовывать соединения RPC через общедоступные сети TCP/IP. Кроме того, из-за серьезных проблем с безопасностью RPC-службы Windows NT в прошлом большинство сетевых администраторов блокируют порты 135, 137, 139 и 445, чтобы помешать проходу внешних тестовых сообщений RPC через брандмауэр. Эти ограничения приводят к тому, что нельзя использовать Outlook в сети одной компании, чтобы установить соединение через Internet с сервером Exchange в сети другой компании. Вместо того чтобы возложить согласование RPC по каналам TCP/IP на администраторов сетей и брандмауэров, разработчики Microsoft модернизировали механизм RPC в Outlook и Exchange, обеспечив связь поверх протокола HTTP.

Благодаря новым функциям можно установить возвратный proxy-сервер (reverse proxy server) HTTP и использовать протокол HTTP для внешних соединений. Как правило, для связи применяется стандартный порт 80 или какая-нибудь его разновидность (например, 8080 или 8088). После настройки браузера Microsoft Internet Explorer (IE) на клиентском компьютере для работы с proxy-сервером любое приложение может задействовать протокол HTTP для соединений клиент/сервер. Протокол Secure HTTP (HTTPS) также обычно доступен через порт 443.

Требования RPC over HTTP

Для соединения RPC over HTTP между Outlook и Exchange необходимо, чтобы на клиентском компьютере были установлены Windows XP Service Pack 1 (SP1) и исправление, описанное в статье Microsoft «Outlook 11 Performs Slowly or Stops Responding When Connected to Exchange Server 2003 Through HTTP» На клиенте должен работать Outlook 2003 (при подготовке данной статьи использовалась вторая бета-версия, сборка 4920).

На сервере должна быть установлена Windows 2003, чтобы использовать службу Microsoft Internet Information Services (IIS) 6.0 в режиме Worker Process Isolation Mode. Windows 2003 должна работать на всех системах, устанавливающих связь с клиентом Outlook 2003, в том числе серверах Exchange, серверах глобального каталога (Global Catalog, GC) и контроллерах домена (DC).

Архитектура RPC over HTTP

Архитектура RPC over HTTP напоминает модель внешний/внутренний сервер (front end/back end server), впервые примененную Microsoft в Exchange 2000 Server и используемую в OWA, IMAP и POP3. Outlook 2003 связывается через протокол 2003 с proxy-сервером RPC, также известным как внешний proxy-сервер RPC. Proxy-сервер RPC действует от имени клиента, устанавливая RPC-соединения с внутренним сервером, на котором размещается почтовый ящик клиента. Соединения показаны на рисунке 1.

|  |
| --- |
| http://www.osp.ru/data/255/528/1234/062_1.jpg |
| Рисунок 1. Архитектура RPC over HTTP для Outlook и Exchange |

Следует отметить важные особенности архитектуры. Во-первых, RPC-посредник не обязательно должен быть системой Exchange 2003, так как proxy-сервер не использует в своей работе компонентов Exchange. Функции посредника возлагаются на фильтр Internet Server API (ISAPI) в IIS 6.0, поэтому единственное требование к системе — наличие Windows 2003. Во-вторых, proxy-сервер RPC — простая функция IIS 6.0, поэтому его можно разместить на системе Exchange 2003. И в-третьих, на системе Exchange 2003 можно разместить и GC-сервер, хотя делать этого не рекомендуется, чтобы не снижалась производительность и сохранялась корректность технических решений. Поэтому все серверные компоненты, показанные на рисунке 1, могут сосуществовать на одной серверной машине.

Следует также рассмотреть возможность размещения сервера относительно внутренних и внешних брандмауэров и образуемой в результате демилитаризованной зоны (DMZ). Proxy-сервер RPC можно разместить в DMZ, а серверы Exchange и другие серверы Active Directory (AD) — во внутренней части сети (рисунок 2). Но поскольку во внутреннем брандмауэре требуется открыть больше портов, данная конфигурация связана с излишним риском и использовать ее обычно не рекомендуется. Риск особенно высок при динамическом назначении портов, которые открываются для RPC-соединений между proxy-сервером RPC и почтовым сервером Exchange 2003. Теоретически эти порты лежат в диапазоне от 1024 до 65535, но в процессе реализации RPC over HTTP требуется определить более узкий диапазон (от порта 6001 до порта 6004). Диапазон задается с помощью параметров реестра, которые будут рассмотрены в следующем разделе. В дополнение к портам, показанным на рисунке 2, proxy-сервер RPC может затребовать порт 88 (UDP/TCP) для служб Kerberos, порт 53 (UDP/TCP) для запросов DNS, порт 445 для Server Message Block (SMB) службы NetLogon и порты для любых других протоколов, необходимых для управления и мониторинга служб.

|  |
| --- |
| http://www.osp.ru/data/253/528/1234/062_2.gif |
| Рисунок 2. Proxy-сервер RPC, расположенный внутри DMZ. |

Лучше разместить proxy-сервер RPC во внутренней части сети и использовать универсальный ретранслятор HTTP в DMZ (рисунок 3). В данной конфигурации предусматривается лишь одно соединение от ретранслятора HTTP в DMZ (в данном случае Microsoft Internet Security и Acceleration-ISA-server) к proxy-серверу RPC во внутренней сети. Данное соединение может быть установлено через базовый протокол HTTP (порт 80) или зашифровано с использованием SSL (Secure Sockets Layer — порт 443). Можно также задействовать функции шифрования RPC over HTTP программы Outlook 2003. При использовании данного подхода можно применять несколько способов защиты соединений. Самый обычный метод — завершить SSL-соединение на proxy-сервере ретрансляции HTTP и установить простое соединение HTTP с RPC-посредником. Этот подход широко распространен, так как подобные proxy-серверы HTTP обычно оснащены аппаратными акселераторами шифрования SSL. Альтернативный подход — провести туннель для входящего SSL-соединения через proxy-сервер HTTP и возложить задачу SSL-шифрования на proxy-сервер RPC. Или же proxy-сервер HTTP может завершить исходящий сеанс SSL и установить новый сеанс SSL с proxy-сервером RPC.

|  |
| --- |
| http://www.osp.ru/data/227/528/1234/062_3.gif |
| Рисунок 3. Proxy-сервер RPC, расположенный во внутренней сети |

Конфигурирование RPC over HTTP на серверах

Для реализации RPC over HTTP необходимо выполнить на серверах несколько изменений. Прежде всего нужно убедиться, что на сервере, применяемом в качестве сервера-посредника RPC, установлена служба RPC over HTTP Proxy. Для этого следует открыть утилиту Add/Remove Programs панели управления и щелкнуть на вкладке Add/Remove Windows Components. Затем нужно отметить пункт Networking Services, убедиться, что выбрана служба RPC over HTTP (экран 1) и щелкнуть на кнопке OK, чтобы развернуть службу.

|  |
| --- |
| http://www.osp.ru/data/225/528/1234/062_4.gif |
| Экран 1. Установка службы RPC over HTTP Proxy |

После установки службы RPC over HTTP Proxy необходимо перейти к объекту Web SitesDefault Web SiteRPC Virtual Directory в оснастке IIS Manager консоли управления Microsoft Management Console (MMC) и открыть диалоговое окно Properties объекта ([экран 2](http://www.osp.ru/win2000/2003/07/176435/062_1v.htm)). Следует перейти к вкладке Directory Security, выбрать раздел Authentication and access control, а затем запретить Anonymous access и разрешить режим Integrated Windows Authentication или, если используется SSL, режим Basic authentication. Если выбран режим Basic authentication, то мандат передается открытым текстом, но соединение защищено благодаря SSL, поэтому такой подход вполне приемлем.

Далее требуется настроить конфигурацию сервера для работы в качестве посредника RPC. Для этого необходимо открыть редактор реестра, перейти в раздел реестра HKEY\_LOCAL\_MACHINESOFTWAREMicrosoftRpc RpcProxy и присвоить параметру ValidPorts значение с типом данных REG\_SZ.

Устанавливая значение ValidPorts, необходимо указать каждый сервер, с которым может установить связь proxy-сервер RPC, в том числе все почтовые серверы Exchange 2003 и любые DC и GC, и назначить порт 593 для каждого сервера. Служба RPC over HTTP Endpoint Mapper использует порт 593 для организации соединения путем квитирования. В строке параметров также указывается диапазон портов для соединений. На [экране 3](http://www.osp.ru/win2000/2003/07/176435/062_2v.htm) показан пример такой строки для сервера с именем osbex01. В зависимости от конкретной среды, расположения сервера и способа разрешения имен, иногда следует указать Fully Qualified Domain Name (FQDN) серверов в элементе реестра ValidPorts (если имена в сокращенном формате не обеспечивают корректного преобразования). На экране 6 видно, что в дополнение к параметрам для osbex01 указаны и соответствующие параметры для osbex01.osb.cantaz.net. Если роль GC-сервера выполняет тот же сервер, на котором работает Exchange 2003, то нет необходимости указывать GC отдельно от системы Exchange.

Очевидно, что при наличии десятков или сотен почтовых и GC-серверов обновление параметров ValidPorts реестра с указанием значений для каждого сервера — труднейшая задача. Поэтому мы надеемся, что Microsoft дополнит пакет Exchange 2003 утилитой, которая будет анализировать среду Exchange и автоматически обновлять данный параметр реестра.

Ограничение соединений RPC-посредника

Диапазон портов proxy-сервера RPC определяет область функционирования RPC over HTTP. Однако можно явно назначить порты, которые будут использоваться каждым сервером — участником соединений RPC over HTTP. Следует обратить внимание, что в бета-версиях Exchange 2003 в разделе реестра ValidPorts можно указать принимаемый по умолчанию диапазон 1024-65535, и любые внутренние серверы или GC будут динамически выбирать рабочие порты в этом диапазоне без дополнительной настройки. Из версии Release Candidate 0 эта функция удалена.

Самые существенные изменения требуется внести во внутренние почтовые серверы. Во-первых, необходимо определить порт, через который внутренний сервер устанавливает соединения RPC over HTTP с хранилищем Exchange Store. Для этого нужно присвоить параметру реестра HKEY\_LOCAL\_MACHINESYSTEMCurrentControlSet ServicesMSExchangeISParametersSystemRPC/HTTP Port значение 6001 типа REG\_DWORD.

Затем следует настроить внутренний сервер для перенаправления Directory Service (DS) Referral, присвоив параметру реестра HKEY\_LOCAL\_MACHINESYSTEMCurrentControlSet ServicesMSExchangeSAParametersHTTP Port значение 6002 типа REG\_DWORD. Затем внутренний сервер настраивается для доступа DS Proxy. Для этого параметру HKEY\_LOCAL\_MACHINESYSTEMCurrentControlSet ServicesMSExchangeISParametersSystemRPC/HTTP NSPI Port присваивается значение 6003 типа REG\_DWORD. Эти изменения должны быть выполнены на всех внутренних серверах Exchange 2003, которые могут устанавливать соединения с proxy-сервером RPC.

Кроме того, необходимо настроить любые DC и GC, указанные в разделе реестра ValidPorts proxy-сервера RPC, для связи с proxy-сервером RPC через порты ограниченного диапазона. Следует перейти к элементу HKEY\_LOCAL\_MACHINESYSTEMCurrentControlSet ServicesNTDSParametersNSPI interface protocol sequences реестра DC или GC-сервера и присвоить этому параметру значение ncacn\_http:6004 типа REG\_SZ.

Безопасные соединения

Соединения RPC over HTTP желательно устанавливать по каналам SSL, избегая незащищенных линий. В рекомендуемой конфигурации (см. рисунок 3) ретрансляционный proxy-сервер HTTP (ISA Server) завершает любые клиентские SSL-соединения и устанавливает отличные от SSL соединения с proxy-сервером RPC. Для этого необходимо установить серверный сертификат на ретрансляционном посреднике HTTP. Соответствующие сертификаты можно получить из коммерческой организации Certificate Authority (CA), такой как VeriSign или Thawte, либо использовать службу Microsoft Certificate Services для создания собственных сертификатов.

Раздел реестра HKEY\_LOCAL\_MACHINESOFTWAREMicrosoftRpc RpcProxyAllowAnonymous управляет работой proxy-сервера RPC с соединениями, отличными от SSL. Если данного раздела не существует или значение его параметра равно 0, то proxy-сервер RPC отвергает все отличные от SSL и неаутентифицированные соединения. Когда ретранслятор HTTP завершает SSL-соединение, последующее соединение с посредником RPC обычно не защищено SSL и поэтому будет отвергнуто. В данном случае можно присвоить параметру реестра значение 1-го типа REG\_DWORD. Изменение вступает в силу после перезапуска службы IIS на proxy-сервере RPC.

В целях безопасности в текущей документации Microsoft такие изменения рекомендуется вносить только на непроизводственных системах. Однако во многих рабочих средах необходима следующая конфигурация: SSL-соединение завершается на proxy-серверах HTTP, а с proxy-сервером RPC устанавливаются отличные от SSL соединения. Необходимо взвесить все за и против и выбрать оптимальную конфигурацию для конкретной среды.

Настройка клиента

Некоторые изменения требуется внести и в профиль Messaging API (MAPI), чтобы позволить клиенту Outlook 2003 установить связь с сервером по HTTP. Если у пользователя уже имеется профиль MAPI, то доступ к его свойствам можно получить, выбрав соответствующий профиль MAPI в утилите Mail панели управления. Нужно выбрать пункты Change, More Settings, а затем перейти к вкладке Connection. Затем следует установить флажок Connect to my Exchange mailbox using HTTP и щелкнуть на кнопке Exchange Proxy Settings, чтобы завершить настройку конфигурации. В диалоговом окне (экран 4) требуется ввести URL, чтобы направить клиента на proxy-сервер RPC. Этот URL может быть значением, объявляемым ретрансляционным proxy-сервером HTTP (для последующего перенаправления пакетов в proxy-сервер RPC). В режиме Basic Authentication префикс URL автоматически изменяется с http на https, поэтому может использоваться только безопасное соединение. Если режим с подключением через протокол HTTP отключен, необходимо убедиться, что установлены XP SP1 и упомянутая выше программа коррекции. Можно установить флажок Mutually authenticate the session when connecting with SSL. В результате proxy-сервер RPC (или ретрансляционный proxy-сервер HTTP) аутентифицирует подключающегося клиента с помощью как клиентского, так и серверного сертификата. В этом режиме клиент должен передать в модуль Security Support Provider (SSP) сервера ожидаемое имя сервера Principal name. Согласно стандартным синтаксическим правилам Microsoft, за префиксом msstd: следует FQDN proxy-сервера RPC (экран 4).

|  |
| --- |
| http://www.osp.ru/data/231/528/1234/062_7.gif |
| Экран 4. Настройка конфигурации клиента RPC over HTTP. |

И наконец, чтобы использовать для соединения протокол HTTP, необходимо установить флажок Connect using HTTP first, then connect using my Local Area Network (LAN). Как правило, Outlook 2003 сначала пытается установить связь с сервером Exchange через TCP/IP. Если попытка не удается, Outlook пробует соединиться через HTTP. После установки этого флажка Outlook делает попытку сначала соединиться через HTTP, что позволит избежать задержки, связанной с тайм-аутом протокола.

При обсуждении смены профиля MAPI предполагалось, что профиль на клиентском компьютере уже существует. Если требуется создать профиль, следует помнить, что для этого необходим прямой RCP-доступ к серверу Exchange через TCP/IP. Если нужно создать профили MAPI для удаленных пользователей (т. е. прямой TCP/IP-доступ к серверу Exchange отсутствует), следует задействовать утилиту генерации профиля MAPI, такую как profgen.exe — инструмент из набора ресурсов Microsoft Office 2003 Resource Kit. В идеале для управления системами необходимо автоматизировать все изменения в MAPI-профилях пользователей, чтобы значительно снизить вероятность возникновения пользовательских ошибок.

Применение RPC over HTTP для подключения клиентов Outlook 2003 к почтовым серверам представляет собой гибкий способ обращения к домашним почтовым ящикам пользователей без ограничений туннелирования или громоздкого клиента на базе Web. Однако в стандартной конфигурации эта функция не работает. Ее запуск требует планирования и настройки конфигурации со стороны администратора систем отправки сообщений. Прежде чем внедрять службу RPC over HTTP на всем предприятии, следует выполнить пилотный проект, чтобы исследовать влияние данной службы на инфраструктуру.

Протокол получения информации о пользователях - Finger.

Протокол Finger возвращает информацию об одном или нескольких пользователях на указанном хосте. Это приложение обычно используется, для того чтобы посмотреть, находится ли конкретный пользователь в настоящее время в системе, или чтобы получить имя какого-либо пользователя, чтобы послать ему почту. Сервер Finger использует заранее известный порт 79. Клиент осуществляет активное открытие на этот порт и отправляет запрос длиной в 1 строку. Сервер обрабатывает запрос, посылает назад вывод и закрывает соединение. Запрос и отклик в формате NVT ASCII, почти так же как мы видели в случае FTP и SMTP.

1. **Протоколы удаленного доступа**

Протокол Telnet

Протокол Telnet (TELNET) предназначен для взаимодействия устройств и процессов терминала. TELNET часто применяется программами эмуляции терминала для входа в удаленную систему. TELNET также обеспечивает взаимодействия терминал-терминал и взаимодействия между процессами. Кроме того, TELNET применяется другими протоколами (например, FTP) для создания управляющего канала протокола.

Протокол пересылки файлов FTP.

Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлу. Он может использоваться приложениями и пользователями для передачи файлов по сети. Для того, чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений - TCP. Однако, кроме пересылки файлов, протокол FTP предлагает и другие услуги. Так, пользователю предоставляется возможность интерактивной работы с удаленной машиной, например, он может распечатать содержимое ее каталогов. Кроме того, FTP позволяет пользователю указывать тип и формат запоминаемых данных. Наконец, FTP выполняет аутентификацию пользователей.

Протокол пересылки файлов FTP (File Transfer Protocol) реализует удаленный доступ к файлу. Он может использоваться приложениями и пользователями для передачи файлов по сети. Для того, чтобы обеспечить надежную передачу, FTP использует в качестве транспорта протокол с установлением соединений - TCP. Однако, кроме пересылки файлов, протокол FTP предлагает и другие услуги. Так, пользователю предоставляется возможность интерактивной работы с удаленной машиной, например, он может распечатать содержимое ее каталогов. Кроме того, FTP позволяет пользователю указывать тип и формат запоминаемых данных. Наконец, FTP выполняет аутентификацию пользователей. FTP обеспечивает защиту данных при передаче, отправляя внешнему хосту пароль пользователя и учетного файла пользователя

Протокол TFTP.

Упрощенный протокол передачи файлов (TFTP) предназначен для обмена файлами с внешними хостами. Для передачи файлов TFTP применяет ненадежный Протокол пользовательских дейтаграмм, поэтому обычно он работает быстрее, чем FTP. Как и FTP, TFTP поддерживает передачу файлов в формате NETASCII и в 8-разрядном двоичном формате. В отличие от FTP, TFTP не поддерживает просмотр каталогов или переход в другой каталог внешнего хоста. В нем также не предусмотрена защита с помощью пароля. Кроме того, TFTP работает только с общими каталогами.

Протокол SMTP.

Для передачи электронной почты в Internet разработан специальный протокол Simple Mail Transfer Protocol (SMTP), который является протоколом прикладного уровня и использует транспортный протокол TCP. при использовании протокола SMTP sendmail пытается найти машину-получателя почты и установить с ней взаимодействие в режиме on-line для того, чтобы передать почту в ее почтовый ящик. совместно с этим протоколом используется и Unix-Unix-Copy (UUCP) протокол. UUCP почта передается по принципу "stop-go"(off-line), т. е. почтовое сообщение передается по цепочке почтовых серверов от одной машины к другой, пока не достигнет машины-получателя или не будет отвергнуто по причине отсутствия абонента-получателя.

Протокол IMAP.

С ростом популярности E-mail и multimedia возникла необходимость в одном сообщении передавать данные различных типов:

текстовую информацию на различных языках,

графические изображения,

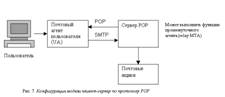
видео, аудио и просто, бинарные файлы;

Это послужило толчком к созданию унифицированного интерфейса (стандарта), который бы интерпретировался всеми почтовыми системами одинаково.

Протокол MIME.

Стандарт MIME (Multipurpose Internet Mail Extention, многоцелевое расшироение интернет почты) представляет такой удобный интерфейс. Он не заменяет, а расширяет существующий способ формирования электронных сообщений. MIME - новый формат представления данных, представляющий почтовому клиенту гибкий интерфейс для работы с E-mail.

Протокол POP3.

Post Office Protocol (POP) - протокол доставки почты пользователю из почтового ящика почтового сервера РОР.

Конструкция протокола РОРЗ обеспечивает возможность пользователю обратиться к своему почтовому серверу и изъять накопившуюся для него почту. Пользователь может получить доступ к РОР-серверу из любой точки доступа к Интернет. При этом он должен запустить специальный почтовый агент (UA), работающий по протоколу РОРЗ, и настроить его для работы со своим почтовым сервером. В протоколе РОРЗ оговорены три стадии процесса получения почты: авторизация, транзакция и обновление.

Сервер новостей должен заниматься сбором новостей и созданием необходимых индексных файлов.

Серверы почты и почтовые клиенты.

Схема передачи/приёма писем.

Работа с почтой в режимах online и offline.

Протокол новостей NNTP.

NNTP представляет собой протокол для рассылки, подписки, поиска и доставки новостей на основе надежного протокола поточного типа (например, TCP) с использованием схемы клиент-сервер. NNTP сконструирован так, что статья, записанная в одном из серверов. Сервер является единственным интерфейсом между программами и базами данных, хранящими новости. Он не выполняет взаимодействия с пользователем или каких-либо операций презентационного уровня. Эти функции передаются программам клиента, которые имеют исчерпывающую информацию о среде. При работе через Интернет в рамках протокола TCP используется порт 119. На команды, посылаемые клиентом, предусмотрены текстовые и статусные отклики. Всякая сессия начинается с процедуры установления соединения между клиентом и сервером по инициативе клиента (например, с использованием протокола TCP). становится доступной для всех подписчиков-клиентов.становится доступной для всех подписчиков-клиентов. Единицей хранения на сервере является статья.

Работа с сервером новостей.

Альтернативные системы рассылки (subscribe.ru).

Сетевой протокол времени NTP

Сетевой протокол задания времени NTP лужит для осуществления синхронизации работы различных процессов в серверах и программах клиента. Протокол NTP обеспечивает механизмы синхронизации с точностью до наносекунд. Протокол предлагает средства для определения характеристик и оценки ошибок локальных часов и временного сервера, который осуществляет синхронизацию. Предусмотрены возможности работы с иерархически распределенными первичными эталонами, такими как синхронизуемые радио-часы

**2.1 Протокол SLIP.**

SLIP (Serial Line Internet Protocol) — устаревший [сетевой протокол](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) [канального уровня](http://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C) [эталонной сетевой модели OSI](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI) для доступа к сетям [стека TCP/IP](http://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%BA_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%BE%D0%B2_TCP/IP)через низкоскоростные линии связи путём простой [инкапсуляции](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D0%BA%D0%B0%D0%BF%D1%81%D1%83%D0%BB%D1%8F%D1%86%D0%B8%D1%8F_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8)) [IP-пакетов](http://ru.wikipedia.org/wiki/IP#IP-.D0.BF.D0.B0.D0.BA.D0.B5.D1.82). Используются [коммутируемые соединения](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B8%D1%80%D1%83%D0%B5%D0%BC%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF) через [последовательные порты](http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BF%D0%BE%D1%80%D1%82)для соединений клиент-сервер типа [точка-точка](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D1%8C_%D1%82%D0%BE%D1%87%D0%BA%D0%B0-%D1%82%D0%BE%D1%87%D0%BA%D0%B0). В настоящее время вместо него используют более совершенный протокол [PPP](http://ru.wikipedia.org/wiki/Point-to-Point_Protocol). SLIP был разработан в начале [80-х](http://ru.wikipedia.org/wiki/1980-%D0%B5) компанией [3COM](http://ru.wikipedia.org/w/index.php?title=3COM&action=edit&redlink=1). Протокол начал быстро распространяться после включения в [ОС](http://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) [Berkeley](http://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BB%D0%B8%D1%84%D0%BE%D1%80%D0%BD%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%83%D0%BD%D0%B8%D0%B2%D0%B5%D1%80%D1%81%D0%B8%D1%82%D0%B5%D1%82_%D0%B2_%D0%91%D0%B5%D1%80%D0%BA%D0%BB%D0%B8) [Unix](http://ru.wikipedia.org/wiki/Unix) 4.2 Риком Адамсом (Rick Adams) в [1984](http://ru.wikipedia.org/wiki/1984_%D0%B3%D0%BE%D0%B4), так как благодаря ему стало возможным подключение к [Интернет](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) через последовательный [COM-порт](http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BF%D0%BE%D1%80%D1%82), имевшийся на большинстве компьютеров. Ввиду своей простоты сейчас используется в [микроконтроллерах](http://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BA%D1%80%D0%BE%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D0%BB%D0%B5%D1%80). Собственно SLIP и PPP - это протоколы, адаптирующие IP для работы на последовательных линиях. Они представляют собой некую прокладку между IP и модемными протоколами. SLIP и PPP имеет смысл использовать вкупе со скоростными модемами на достаточно скоростных линиях.

**2.2 Протокол PPP.**

Основная функция программного обеспечения SLIP/PPP - организовать пересылку IP -пакетов по последовательной линии, которая не предусматривает деления пересылаемой информации на какие-либо отдельные блоки и пересылает все данные единым непрерывным потоком. SLIP/PPP как раз и занимается организацией такой пересылки, чтобы на другом конце можно было этот сплошной и непрерывный поток данных разделить на составляющие его IP -пакеты, выделить их и передать дальше уже как IP -пакеты.

SLIP/PPP очень удобен для подключения домашнего компьютера к локальной сети, которая, в свою очередь, входит в Internet. Например, можно воспользоваться PPP , чтобы подключить свою домашнюю персоналку к сети вашей организации. И тогда ваш компьютер будет иметь такие же возможности работы в Internet, как и любой другой компьютер вашей организации, подключённый к Сети через Ethernet.

SLIP/PPP подходят и для подключения домашнего компьютера (или очень маленькой локальной сети) к собственно првайдеру, который может предоставить непосредственный доступ в Internet.

Однако следует понимать, что эти протоколы, вообще-то, совсем не предназначены для подключения к Internet сетей средней величины или больших сетей: они не предназначены для работы на высокоскоростных линиях, которые требуются для обслуживания большого количество пользователей.

Для того, чтобы организовать связь через канал связи с непосредственным соединением, инициирующий РРР сначала отправляет пакеты LCР для выбора конфигурации и (факультативно) проверки канала передачи данных. После того, как канал установлен и пакетом LCР проведенo необходимое согласование факультативных средств, инициирующий РРР отправляет пакеты NCP, чтобы выбрать и определить конфигурацию одного или более протоколов сетевого уровня. Как только конфигурация каждого выбранного протокола оперделена, дейтаграммы из каждого протокола сетевого уровня могут быть отправлены через данный канал. Канал сохраняет свою конфигурацию для связи до тех пор, пока явно выраженные пакеты LCP или NCP не закроют этот канал, или пока не произойдет какое-нибудь внешнее событие (например, истечет срок бездействия таймера или вмешается какой-нибудь пользователь).

**2.3 Протоколы защищенных каналов SSL, PPTP, IPSec**

Протокол PPTP (Point-to-Point Tunneling Protocol) разработан компанией Microsoft совместно с компаниями Ascend Communications, 3Com/Primary Access, ECI-Telematics и US Robotics. Этот протокол был представлен в рабочую группу "PPP Extentions" IETF в качестве претендента на стандартный протокол создания защищенного канала при доступе удаленных пользователей через публичные сети (в первую очередь Internet) к корпоративным сетям. Этот протокол получил статус проекта стандарта Internet, однако, в качестве стандарта так и не был утвержден. Сейчас рабочая группа IETF рассматривает возможность принятия в качестве стандарта протокол L2TP (Layer 2 Tunneling Protocol), который должен объединить лучшие стороны протокола PPTP с протоколом аналогичного назначения L2F (Layer 2 Forwarding), предложенного компанией Cisco.

Протокол PPTP позволяет создавать защищенные каналы для обмена данными по различным сетевым протоколам — IP, IPX или NetBEUI. Данные этих протоколов инкапсулируются с помощью протокола PPTP в пакеты протокола IP, с помощью которого переносятся в зашифрованном виде через любую сеть TCP/IP. Инкапсулируется исходный кадр РРР, поэтому протокол PPTP можно отнести к классу протоколов инкапсуляции канального уровня в сетевой.

Многопротокольность — основное преимущество инкапсулирующих протоколов канального уровня, к которым относится протокол PPTP. Протокол SSL, например, ориентируется на один протокол сетевого уровня — IP. К тому же размещение протокола защищенного канала непосредственно под прикладным уровнем требует переписи приложений, если они хотят воспользоваться возможностями защиты. Защиты данных на канальном уровне делает средства защиты прозрачными как для протоколов прикладного уровня, так и для протоколов сетевого уровня.

Существуют также и варианты встраивания средств создания защищенного канала на сетевом уровне. Имеется несколько протоколов этого типа, использующих шифрацию и инкапсуляцию протокола сетевого уровня в сетевой. Для защиты данных в IP-сетях разработана защищенная версия протокола IP, которую чаще всего называют IPSec (подробнее о нем поговорим о нем в следующей части статьи). Эта версия поддерживает аутентификацию на сетевом уровне, а также может выполнять шифрацию пользовательских данных. IPSec — это набор стандартов, часть из которых существует в виде проектов, а часть еще находится в стадии разработки. Протокол IPSec не определяет жестко, какие методы шифрации должны использоваться для аутентификации и создания защищенного канала, хотя для первых реализаций определен вариант IPSec, использующий дайджест-функцию MD5 для аутентификации и алгоритм шифрования DES для образования защищенного канала. Недостатком протокола IPSec является то, что он работает только в IP-сетях и не определяет способа защищенной транспортировки пакетов других протоколов. Этот недостаток устраняют такие протоколы, как PPTP или L2F.принцип работы PPTP.

Сетевые протоколы функционируют путем обмена порциями данных, называемыми пакетами. Пакет состоит из управляющей информации, специфичной для протокола, и собственно данных, которые должны быть переданы; их часто называют полезной нагрузкой. До тех пор, пока обмен данными происходит достаточно быстро и без ошибок, нас не волнует, какую управляющую информацию добавляет протокол для своих целей. Но она жизненно важна и должна сохраняться неизменной, если два компьютера собираются обмениваться данными, вне зависимости от среды соединения.  
PPTP работает путем инкапсуляции "родных" пакетов локальной сети — например, пакетов IPX — внутрь пакетов TCP/IP. Весь пакет IPX, включая его управляющую информацию, становится полезной нагрузкой для пакета TCP/IP, который затем можно передавать по Internet. Программные средства на другом конце линии связи извлекают пакет IPX и направляют его для нормальной обработки в соответствии с его собственным протоколом. Этот процесс называется туннелированием, вероятно, потому, что создается коридор в Internet, соединяющий два узла.

Туннелирование позволяет не только экономить на стоимости дальних звонков, но и повышать степень защиты данных. Поскольку туннель соединяет два совместимых протокола с сетью Windows NT/2000, операционная система может выполнять всеобъемлющие проверки надежности защиты, которые она проводит в самой локальной сети. Таким путем соединение может обеспечить принятую в Windows NT/2000 аутентификацию пользователей по протоколам PAP (Password Authentication Protocol) или CHAP (Challenge Handshake Authentication Protocol). Более того, PPTP позволяет передавать данные, зашифрованные RSA-методами RC-4 или DES. Если безопасность подключения к сети VPN является критическим фактором, администратор сервера может указать, что сервер будет принимать посредством дистанционного соединения только пакеты PPTP, но это предотвратит использование сервера в режиме открытого доступа по HTTP или FTP. Однако, если имеется более одного сервера и если нужно обеспечить наивысшую защиту, такое решение — вполне приемлемый вариант.

Но даже при всех подобных мерах безопасности единственным специальным программным обеспечением для клиента служит сам протокол PPTP плюс программа связи по модему, которая может соединить с сетью VPN. И даже это не является необходимым, если у поставщика услуг Internet есть средства работы с PPTP, позволяющие безопасно передавать любые данные по стандартному протоколу PPP (Point-to-Point Protocol, протокол соединения "точка-точка"). процесс связи по протоколу PPTP .

Поскольку вся идея дистанционного доступа состоит в разрешении машине клиента подключаться по телефонной линии к машине сервера, соединение PPTP инициируется клиентом, который использует служебное средство Windows NT — Remote Access Service (RAS) — для установления PPP-соединения с поставщиком услуг Internet. Затем при активизированном соединении PPP с помощью сервера, подключенного к Internet и действующего как сервер RAS, клиент применяет RAS для выполнения второго соединения. На этот раз в поле номера телефона указывается IP-адрес (или доменное имя), и клиент, для того чтобы осуществить соединение, вместо COM-порта использует VPN-порт (VPN-порты конфигурируются на машинах клиента и сервера в процессе инсталляции PPTP).

Ввод IP-адреса инициирует передачу запроса серверу на начало сеанса. Клиент ожидает от сервера подтверждения имени пользователя и пароля и ответа сообщением, что соединение установлено. В этот момент начинает свою работу канал PPTP, и клиент может приступить к туннелированию пакетов серверу. Поскольку они могут быть пакетами IPX и NetBEUI, сервер может выполнять с ними свои обычные процедуры обеспечения защиты.

В основе обмена данными по протоколу PPTP лежит управляющее соединение PPTP — последовательность управляющих сообщений, которые устанавливают и обслуживают туннель. Полное соединение PPTP состоит только из одного соединения TCP/IP, которое требует передачи эхо-команд для поддержания его открытым, пока выполняются транзакции. В таблице 1 показаны эти сообщения и их функциональное назначение.

|  |  |
| --- | --- |
| Управляющее сообщение | Функция |
| Start-Control-Connection-Request | Запрос на установление управляющего соединения |
| Start-Control-Connection-Replay | Ответ на сообщение Start-Control-Connection-Request |
| Echo-Request | Сообщение "Keep-alive" ("все живы") для управляющего соединения |
| Echo-Replay | Ответ на сообщение Echo-Request |
| Set-Link-Info | Посылается сервером сети для задания PPP-параметров переговоров |
| Stop-Control-Connection-Request | Команда завершить управляющее соединение |
| Stop-Control-Connection-Replay | Ответ на сообщение Stop-Control-Connection-Request |

Табл. 1. Управляющие сообщения PPTP

Схемы применения протокола PPTP.

В протоколе PPTP определено две схемы его применения.  
Первая схема рассчитана на поддержание защищенного канала между сервером удаленного доступа ISP и пограничным маршрутизатором корпоративной сети (рис.1).

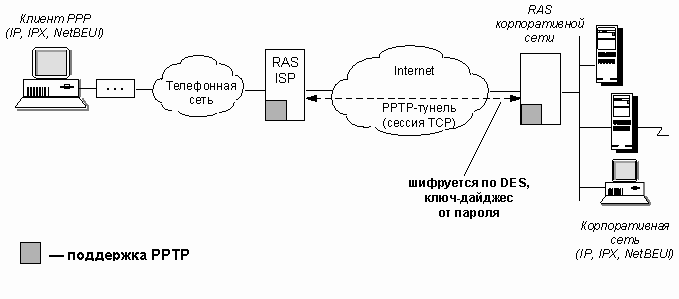


Рис.1. Защищенный канал "провайдер–маршрутизатор корпоративной сети" на основе протокола PPTP.

В этом варианте компьютер удаленного пользователя не должен поддерживать протокол PPTP. Он связывается с сервером удаленного доступа RAS, установленного у ISP, с помощью стандартного протокола PPP и проходит первую аутентификацию у провайдера. RAS ISP должен поддерживать протокол PPTP. По имени пользователя RAS ISP должен найти в базе учетных данных пользователей IP-адрес маршрутизатора, являющегося пограничным маршрутизатором корпоративной сети данного пользователя. С этим маршрутизатором RAS ISP устанавливает сессию по протоколу PPTP. Протокол PPTP определяет некоторое количество служебных сообщений, которыми обмениваются взаимодействующие стороны, служебные сообщения передаются по протоколу TCP. RAS ISP передает маршрутизатору корпоративной сети идентификатор пользователя, по которому маршрутизатор снова аутентифицирует пользователя по протоколу CHAP. Если пользователь прошел вторичную аутентификацию (она для него прозрачна), то RAS ISP посылает ему сообщение об этом по протоколу РРР и пользователь начинает посылать свои данные в RAS ISP по протоколу IP, IPX или NetBIOS, упаковывая их в кадры РРР. RAS ISP осуществляет инкапсуляцию кадров РРР в пакеты IP, указывая в качестве адреса назначения адрес пограничного маршрутизатора, а в качестве адреса источника — свой собственный IP-адрес. Пакеты РРР шифруются с помощью секретного ключа, в качестве которого используется дайджест от пароля пользователя, который хранится в базе учетных данных RAS ISP для аутентификации по протоколу CHAP.

Пакеты, циркулирующие в рамках сессии PPTP, имеют следующий вид:

- заголовок канального уровня, используемого внутри Internet (PPP,  SLIP, Ethernet); -заголовок-IP; -заголовок-GRE; - исходный пакет PPP, включающий пакет IP, IPX или NetBEUI. Для указания сведений отом, что внутри пакета IP находится инкапсулированный пакет РРР, используется стандартный для Internet заголовок GRE v.2 (RFC 1701 и 1702), используемый при инкапсуляции различного типа. Внутренние серверы корпоративной сети также не должны поддерживать протокол PPTP, так как пограничный маршрутизатор извлекает кадры РРР из пакетов IP и посылает их по сети в необходимом формате —IP, IPX или NetBIOS. Microsoft предложила также и другую схему использования протокола PPTP, с помощью которой образуется защищенный канал между компьютером удаленного пользователя и пограничным маршрутизатором корпоративной сети, в качестве которого должен использоваться RAS Windows NT/2000. Эта схема приведена на рисунке 2.

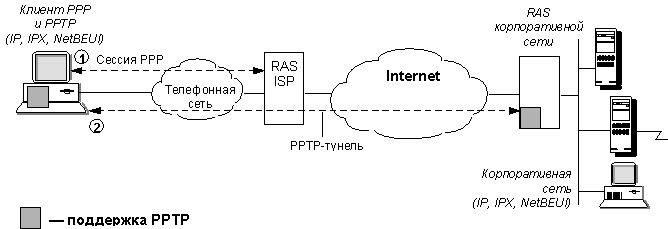


Рис.2. Защищенный канал "клиент - маршрутизатор" корпоративной сети на основе протокола PPTP В первый раз клиент звонит на сервер RAS ISP и устанавливает с ним связь по протоколу PPP, проходя аутентификацию одним из способов, поддерживаемых провайдером — по протоколам PAP, CHAP или с помощью терминального диалога.

После аутентификации у провайдера, пользователь вторично "звонит", на этот раз в сервер удаленного доступа корпоративной сети. Этот "звонок" отличается от обычного тем, что вместо телефонного номера указывается IP-адрес RAS Windows NT, подключенного к Internet со стороны корпоративной сети. При этом устанавливается сессия по протоколу PPTP между клиентским компьютером и RAS корпоративной сети. Клиент еще раз аутентифицируется, теперь на сервере RAS его сети, а затем начинается передача данных, как и в первом варианте.

**2.4 Усугубление проблем безопасности при удаленном доступе.**

Обеспечение безопасности данных при удаленном доступе - проблема если и не номер один, то, по крайней мере, номер два, после проблемы обеспечения приемлемой для пользователей пропускной способности. А при активном использовании транспорта Internet она становится проблемой номер один.

Неотъемлемым свойством систем удаленного доступа является наличие глобальных связей. По своей природе глобальные связи, простирающиеся на много десятков и тысяч километров, не позволяют воспрепятствовать злонамеренному доступу к передаваемым по этим линиям данным. Нельзя дать никаких гарантий, что в некоторой, недоступной для контроля точке пространства, некто, используя, например, анализатор протокола, не подключится к передающей среде для захвата и последующего декодирования пакетов данных. Такая опасность одинаково присуща всем видам территориальных каналов связи и не связана с тем, используются ли собственные, арендуемые каналы связи или услуги общедоступных территориальных сетей, подобные Internet.

Однако использование общественных сетей (речь в основном идет об Internet) еще более усугубляет ситуацию, хотя бы потому, что в такой сети для доступа к корпоративным данным в распоряжении злоумышленника имеются более разнообразные и удобные средства, чем выход в чистое поле с анализатором протоколов. Кроме того, огромное число пользователей увеличивает вероятность попыток несанкционированного доступа.

Безопасная система - это система, которая, во-первых, надежно хранит информацию и всегда готова предоставить ее своим пользователям, а во-вторых, система, которая защищает эти данные от несанкционированного доступа.

Межсетевой экран (firewall, брандмауэр) - это устройство, как правило, представляющее собой универсальный компьютер с установленным на нем специальным программным обеспечением, который размещается между защищаемой (внутренней) сетью и внешними сетями, потенциальными источниками опасности. Межсетевой экран контролирует все информационные потоки между внутренней и внешними сетями, пропуская данные, в соответствии с заранее установленными правилами. Эти правила являются формализованным выражением политики безопасности, принятой на данном предприятии. Межсетевые экраны базируются на двух основных приемах защиты:

пакетной фильтрации;

сервисах-посредниках (proxy-services).

Эти две функции можно использовать как по отдельности, так и в комбинации.

Пакетная фильтрация. Использование маршрутизаторов в качестве firewall

Фильтрация осуществляется на транспортном уровне: все проходящие через межсетевой экран пакеты или кадры данных анализируются, и те из них, которые имеют в определенных полях заданные ("неразрешенные") значения, отбрасываются.

Пропуск во внутреннюю сеть пакетов сетевого уровня или кадров канального уровня по адресам (MAC-адреса, IP-адреса, IPX-адреса) или номерам портов TCP, соответствующих приложениям. Например, для того, чтобы трафик telnet не пересекал границу внутренней сети, межсетевой экран должен отфильтровывать все пакеты, в заголовке TCP которых указан адрес порта процесса-получателя, равный 23 (этот номер зарезервирован за сервисом telnet). Сложнее отслеживать трафик FTP, который работает с большим диапазоном возможных номеров портов, что требует задания более сложных правил фильтрации.

Конечно, для фильтрации пакетов может быть использован и обычный маршрутизатор, и действительно, в Internet 80% пакетных фильтров работают на базе маршрутизаторов. Однако маршрутизаторы не могут обеспечить ту степень защиты данных, которую гарантируют межсетевые экраны.

Главные преимущества фильтрации межсетевым экраном по сравнению с фильтрацией маршрутизатором состоят в следующем:

межсетевой экран обладает гораздо более развитыми логическими способностями, поэтому он в отличие от маршрутизатора легко может, например, обнаружить обман по IP-адресу;

у межсетевого экрана большие возможности аудита всех событий, связанных с безопасностью.

Сервисы - посредники (Proxy-services) Сервисы-посредники не допускают возможности непосредственной передачи трафика между внутренней и внешней сетями. Для того, чтобы обратиться к удаленному сервису, клиент-пользователь внутренней сети устанавливает логическое соединение с сервисом-посредником, работающим на межсетевом экране. Сервис-посредник устанавливает отдельное соединение с "настоящим" сервисом, работающим на сервере внешней сети, получает от него ответ и передает по назначению клиенту - пользователю защищенной сети.

Для каждого сервиса необходима специальная программа: сервис-посредник. Обычно, защитный экран включает сервисы-посредники для FTP, HTTP, telnet. Многие защитные экраны имеют средства для создания программ-посредников для других сервисов. Некоторые реализации сервисов-посредников требуют наличия на клиенте специального программного обеспечения. Пример: Sock - широко применяемый набор инструментальных средств для создания программ-посредников.

Сервисы-посредники не только пересылают запросы на услуги, например, разработанный CERN сервис-посредник, работающий по протоколу HTTP, может накапливать данные в кэше межсетевого экрана, так что пользователи внутренней сети могут получать данные с гораздо меньшим временем доступа.

Журналы событий, поддерживаемые сервисами-посредниками, могут помочь предупредить вторжение на основании записей о регулярных неудачных попытках. Еще одним важным свойством сервисов-посредников, положительно сказывающимся на безопасности системы, является то, что при отказе межсетевого экрана защищаемый посредником сервис-оригинал остается недоступным.

Трансляция сетевых адресов - новый вид сервиса-посредника. Трансляторы адресов заменяют "внешние" IP-адреса серверов своих сетей на "внутренние". При таком подходе топология внутренней сети скрыта от внешних пользователей, вся сеть может быть представлена для них одним-единственным IP-адресом. Такая непрозрачность сети усложняет задачу несанкционированного доступа. Кроме этого, трансляция адресов дает еще одно преимущество - позволяет иметь внутри сети собственную систему адресации, не согласованную с Internet, что снимает проблему дефицита IP-адресов.

Сервисы-посредники намного надежнее фильтров, однако они снижают производительность обмена данными между внутренней и внешней сетями, они также не обладают той степенью прозрачности для приложений и конечных пользователей, которая характерна для фильтров.

Технология защищенного канала призвана обеспечивать безопасность передачи данных по открытой транспортной сети, например, по сети Internet. Защищенный канал включает в себя выполнение трех основных функций:

взаимная аутентификация абонентов;

защита передаваемых по каналу сообщений от несанкционированного доступа;

подтверждение целостности поступающих по каналу сообщений.

Взаимная аутентификация обеих сторон при установлении соединения может быть выполнена, например, путем обмена сертификатами.

Секретность может быть обеспечена каким-либо методом шифрации, например, передаваемые сообщения шифруются с использованием симметричных сессионных ключей, которыми стороны обмениваются при установлении соединения. Сессионные ключи передаются также в зашифрованном виде, при этом они шифруются с помощью открытых ключей. Использование для защиты сообщений симметричных ключей связано с тем, что скорость процессов шифрации и дешифрации на основе симметричного ключа существенно выше, чем при использовании несимметричных ключей.

Целостность передаваемых сообщений достигается за счет того, что к сообщению (еще до его шифрации сессионным ключом) добавляется дайджест, полученный в результате применения односторонней функции к тексту сообщения.

Защищенный канал в публичной сети часто называют также виртуальной частной сетью - VirtualPrivateNetwork, VPN. Существует два способа образования VPN (рисунок 4.1):

с помощью специального программного обеспечения конечных узлов;

с помощью специального программного обеспечения шлюзов, стоящих на границе между частной и публичной сетями.

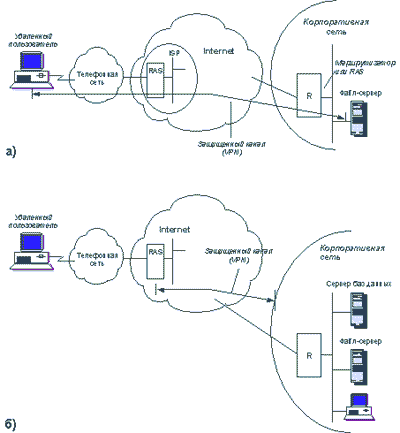


Рис. 4.1. VPN - частные виртуальные сети

В первом случае (рисунок 4.1, a) программное обеспечение, установленное на компьютере удаленного клиента, устанавливает защищенный канал с сервером корпоративной сети, к ресурсам которого клиент обращается. Преимуществом этого подхода является полная защищенность канала вдоль всего пути следования, а также возможность использования любых протоколов создания защищенных каналов, лишь бы на конечных точках канала поддерживался один и тот же протокол. Недостатки заключаются в избыточности и децентрализованности решения.

Избыточность состоит в том, что уязвимыми для злоумышленников обычно являются сети с коммутацией пакетов, а не каналы телефонной сети или выделенные каналы. Поэтому установка специального программного обеспечения на каждый клиентский компьютер и каждый сервер корпоративной сети не является необходимой. Децентрализация процедур создания защищенных каналов не позволяет вести централизованное управление доступом к ресурсам сети. В большой сети необходимость отдельного администрирования каждого сервера и каждого клиентского компьютера с целью конфигурирования в них средств защиты данных - это трудоемкая процедура. Во втором случае клиенты и серверы не участвуют в создании защищенного канала - он прокладывается только внутри публичной сети с коммутацией пакетов, например, внутри Internet. Канал создается между сервером удаленного доступа провайдера услуг публичной сети и пограничным маршрутизатором корпоративной сети. Это хорошо масштабируемое решение, управляемого централизованно как администратором корпоративной сети, так и администратором сети провайдера. Для клиентских компьютеров и серверов корпоративной сети канал прозрачен - программное обеспечение этих конечных узлов остается без изменений. Реализация этого подхода сложнее - нужен стандартный протокол образования защищенного канала, требуется установка программного обеспечения, поддерживающего такой протокол, у всех провайдеров, необходима поддержка протокола производителями серверов удаленного доступа и маршрутизаторов.

Протоколы аутентификации удаленных пользователей.

Контроль доступа пользователей к ресурсам корпоративной сети должен осуществляться в соответствии с политикой безопасности организации, которой принадлежит данная сеть. Эффективное разграничение доступа к сетевым ресурсам может быть обеспечено только при надежной аутентификации пользователей. Требования к надежности аутентификации удаленных пользователей должны быть особенно высокими, так как при взаимодействии с физически удаленными пользователями значительно сложнее обеспечить доступ к сетевым ресурсам. В отличие от локальных пользователей удаленные пользователи не проходят процедуру физического контроля при допуске на территорию организации.

При удаленном взаимодействии важна аутентификация не только пользователей, но и оборудования, поскольку подмена пользователя или маршрутизатора приводит к одним и тем же последствиям — данные из корпоративной сети передаются не тем лицам, которым они предназначены.

Для обеспечения надежной аутентификации удаленных пользователей необходимо выполнение следующих требований:

• проведение аутентификации обеих взаимодействующих сторон — как удаленного пользователя, так и сервера удаленного доступа — для исключения маскировки злоумышленников;

• оперативное согласование используемых протоколов аутентификации;

• осуществление динамической аутентификации взаимодействующих сторон в процессе работы удаленного соединения;

• применение криптозащиты передаваемых секретных паролей либо механизма одноразовых паролей для исключения перехвата и несанкционированного использования аутен-тифицирующей информации.

Протокол РРР имеет встроенные средства, которые могут быть использованы для организации аутентификации при удаленном взаимодействии. В стандарте RFC 1334 определены два протокола аутентификации:

• по паролю — PAP (Password Authentication Protocol);

• по рукопожатию — CHAP (Challenge Handshake Authentication Protocol).

В процессе установления удаленного соединения каждая из взаимодействующих сторон может предложить для применения один из стандартных протоколов аутентификации — РАР или CHAP.

Иногда компании создают собственные протоколы аутентификации удаленного доступа, работающие вместе с протоколом РРР. Эти фирменные протоколы обычно являются модификациями протоколов РАР и CHAP.

Широкое применение для аутентификации по одноразовым паролям получил протокол S/Key. В программных продуктах, обеспечивающих связь по протоколу РРР, протоколы РАР и CHAP, как правило, поддерживаются в первую очередь.

Протокол РАР.

Суть работы протокола РАР довольно проста. В процессе аутентификации участвуют две стороны — проверяемая и проверяющая. Протокол РАР использует для аутентификации передачу проверяемой стороной идентификатора и пароля в виде открытого текста. Если проверяющая сторона обнаруживает совпадение идентификатора и пароля с записью, имеющейся у него в БД легальных пользователей, то процесс аутентификации считается успешно завершенным, после чего проверяемой стороне посылается соответствующее сообщение. В качестве стороны, чья подлинность проверяется, как правило, выступает удаленный пользователь, а в качестве проверяющей стороны — сервер удаленного доступа.

Для инициализации процесса аутентификации на базе протокола РАР сервер удаленного доступа после установления сеанса связи высылает удаленному компьютеру пакет LCP (Link Control Protocol) — протокол управления каналом, указывающий на необходимость применения протокола РАР. Далее осуществляется обмен пакетами РАР. Удаленный компьютер передает по каналу связи проверяющей стороне идентификатор и пароль, введенные удаленным пользователем. Сервер удаленного доступа по полученному идентификатору пользователя выбирает эталонный пароль из БД системы защиты и сравнивает его с полученным паролем. Если они совпадают, то аутентификация считается успешной, что сообщается удаленному пользователю.

Следует особо отметить, что протокол аутентификации РАР, согласно которому идентификаторы и пароли передаются по линии связи в незашифрованном виде, целесообразно применять только совместно с протоколом, ориентированным на аутентификацию по одноразовым паролям, например, совместно с протоколом S/Key. В противном случае пароль, передаваемый по каналу связи, может быть перехвачен злоумышленником и использован повторно в целях маскировки под санкционированного удаленного пользователя.

Протокол CHAP.

В протоколе CHAP используется секретный статический пароль. В отличие от протокола РАР, в протоколе CHAP пароль каждого пользователя для передачи по линии связи шифруется на основе случайного числа, полученного от сервера. Такая технология обеспечивает не только защиту пароля от хищения, но и защиту от повторного использования злоумышленником перехваченных пакетов с зашифрованным паролем. Протокол CHAP применяется в современных сетях гораздо чаще, чем РАР, так как он использует передачу пароля по сети в защищенной форме, и, следовательно, гораздо безопаснее.

Шифрование пароля в соответствии с протоколом CHAP выполняется с помощью криптографического алгоритма хэширования и поэтому является необратимым. В стандарте RFC 1334 для протокола CHAP в качестве хэш-функции определен алгоритм MD5, вырабатывающий из входной последовательности любой длины 16-байтовое значение. Хотя минимальной длиной секрета является 1 байт, для повышения криптостойкости рекомендуется использовать секрет длиной не менее 16 байт. Спецификация CHAP не исключает возможность использования других алгоритмов вычисления хэш-функций.

Для инициализации процесса аутентификации по протоколу CHAP сервер удаленного доступа после установления сеанса связи должен выслать удаленному компьютеру пакет LCP, указывающий на необходимость применения протокола CHAP, а также требуемого алгоритма хэширования. Если удаленный компьютер поддерживает предложенный алгоритм хэширования, то он должен ответить пакетом LCP о согласии с предложенными параметрами. В противном случае выполняется обмен пакетами LCP для согласования алгоритма хэширования.

После этого начинается аутентификация на основе обмена пакетами протокола CHAP.

В протоколе CHAP определены пакеты четырех типов:

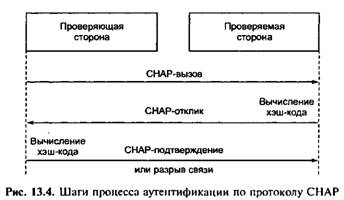
• Вызов (Challenge);

• Отклик (Response);

• Подтверждение (Success);

• Отказ (Failure).

Протокол CHAP использует для аутентификации удаленного пользователя результат шифрования произвольного слова-вызова с помощью уникального секрета. Этот секрет имеется как у проверяющей, так и у проверяемой стороны. Процедура аутентификации начинается с отправки сервером удаленного доступа пакета Вызов.

[](http://ypn.ru/wp-content/uploads/2010/09/13.4.jpg)

Удаленный компьютер, получив пакет Вызов, зашифровывает его с помощью односторонней функции и известного ему секрета, получая в результате дайджест. Дайджест возвращается проверяющей стороне в виде пакета Отклик.

Так как используется односторонняя хэш-функция, то по перехваченным пакетам Вызов и Отклик вычислить пароль удаленного пользователя практически невозможно.

Получив пакет Отклик, сервер удаленного доступа сравнивает содержимое результата из полученного пакета Отклик с результатом, вычисленным самостоятельно. Если эти результаты совпадают, то аутентификация считается успешной и сервер высылает удаленному компьютеру пакет Подтверждение.

В противном случае сервер удаленного доступа высылает пакет Отказ и разрывает сеанс связи.

Пакет Вызов должен быть отправлен сервером повторно, если в ответ на него не был получен пакет Отклик. Кроме того, пакет Вызов может отправляться периодически в течение сеанса удаленной связи для проведения динамической аутентификации, чтобы убедиться, что противоположная сторона не была подменена. Соответственно пакет Отклик должен отправляться проверяемой стороной в ответ на каждый принятый пакет Вызов.

Протокол S/Key.

Одним из наиболее распространенных протоколов аутентификации на основе одноразовых паролей является стандартизованный в Интернете протокол S/Key (RFC 1760). Этот протокол реализован во многих системах, требующих проверки подлинности удаленных пользователей, в частности в системе TACACS+ компании Cisco.

Перехват одноразового пароля, передаваемого по сети в процессе аутентификации, не предоставляет злоумышленнику возможности повторно использовать этот пароль, так как при следующей проверке подлинности необходимо предъявлять уже другой пароль. Поэтому схема аутентификации на основе одноразовых паролей, в частности S/Key, позволяет передавать по сети одноразовый пароль в открытом виде и, таким образом, компенсирует основной недостаток протокола аутентификации РАР.

Однако следует отметить, что протокол S/Key не исключает необходимость задания секретного пароля для каждого пользователя. Этот секретный пароль используется только для генерации одноразовых паролей. Для того чтобы злоумышленник не смог по перехваченному одноразовому паролю вычислить секретный исходный пароль, генерация одноразовых паролей выполняется с помощью односторонней, т. е. необратимой, функции. В качестве такой односторонней функции в спецификации протокола S/Key определен алгоритм хэширования MD4 (Message Digest Algorithm 4). Некоторые реализации протокола S/Key в качестве односторонней функции используют алгоритм хэширования MD5 (Message Digest Algorithm 5).

Иногда желательно, чтобы пользователь имел возможность сам назначать секретный постоянный пароль. Для осуществления такой возможности спецификация S/Key предусматривает режим вычисления одноразовых паролей не только на основе секретного пароля, но и на основе генерируемого проверяющей стороной случайного числа. Таким образом, в соответствии с протоколом S/Key за каждым пользователем закрепляется идентификатор и секретный постоянный пароль.

Перед тем как проходить аутентификацию, каждый пользователь должен сначала пройти процедуру инициализации очередного списка одноразовых паролей, т. е. фазу парольной инициализации. Данная фаза выполняется по запросу пользователя на сервере удаленного доступа.

Для ускорения процедуры аутентификации определенное число одноразовых паролей, например, несколько десятков, может быть вычислено заранее и храниться на удаленном компьютере в зашифрованном виде.

Протокол аутентификации на основе одноразовых паролей S/Key применяют, в частности, для улучшения характеристик протоколов централизованного контроля доступа к сети удаленных пользователей TACACS и RADIUS.

Централизованный контроль удаленного доступа.

Для управления удаленными соединениями небольшой локальной сети вполне достаточно одного сервера удаленного доступа. Однако если локальная сеть объединяет относительно большие сегменты и число удаленных пользователей существенно возрастает, то одного сервера удаленного доступа недостаточно.

При использовании в одной локальной сети нескольких серверов удаленного доступа требуется централизованный контроль доступа к компьютерным ресурсам.

Рассмотрим, как решается задача контроля доступа к сети удаленных пользователей в соответствии с обычной схемой, когда удаленные пользователи пытаются получить доступ к сетевым ресурсам, которые находятся под управлением нескольких разных ОС. Пользователь дозванивается до своего сервера удаленного доступа, и RAS выполняет для него процедуру аутентификации, например, по протоколу CHAP. Пользователь логически входит в сеть и обращается к нужному серверу, где снова проходит аутентификацию и авторизацию, в результате чего получает или не получает разрешение на выполнение запрошенной операции.

Нетрудно заметить, что такая схема неудобна пользователю, поскольку ему приходится несколько раз выполнять аутентификацию — при входе в сеть на сервере удаленного доступа, а потом еще каждый раз при обращении к каждому ресурсному серверу сети. Пользователь вынужден запоминать несколько разных паролей. Кроме того, он должен знать порядок прохождения разных процедур аутентификации в разных ОС. Возникают также трудности с администрированием такой сети. Администратор должен заводить учетную информацию о каждом пользователе на каждом сервере. Эти разрозненные БД трудно поддерживать в корректном состоянии. При увольнении сотрудника сложно исключить его из всех списков. Возникают проблемы при назначении паролей, существенно затрудняется аудит.

Отмеченные трудности преодолеваются при установке в сети централизованной службы аутентификации и авторизации. Для централизованного контроля доступа выделяется отдельный сервер, называемый сервером аутентификации. Этот сервер служит для проверки подлинности удаленных пользователей, определения их полномочий, а также фиксации и накопления регистрационной информации, связанной с удаленным доступом. Надежность защиты повышается, если сервер удаленного доступа запрашивает необходимую для аутентификации информацию непосредственно у сервера, на котором хранится общая БД системы защиты компьютерной сети.

Однако в большинстве случаев серверы удаленного доступа нуждаются в посреднике для взаимодействия с центральной БД системы защиты, например, со службой каталогов.

Большинство сетевых ОС и служб каталогов сохраняют эталонные пароли пользователей с использованием одностороннего хэширования, что не позволяет серверам удаленного доступа, стандартно реализующим протоколы РАР и CHAP, извлечь открытый эталонный пароль для проверки ответа.

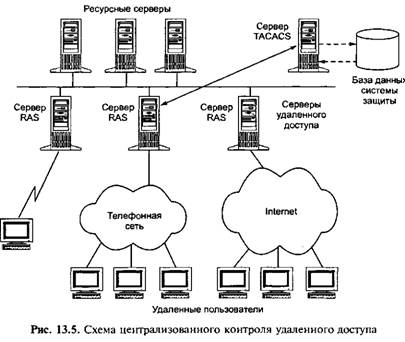
Роль посредника во взаимодействии между серверами удаленного доступа и центральной БД системы защиты может быть возложена на сервер аутентификации. Централизованный контроль удаленного доступа к компьютерным ресурсам с помощью сервера аутентификации выполняется на основе специализированных протоколов. Эти протоколы позволяют объединять используемые серверы удаленного доступа и сервер аутентификации в одну подсистему, выполняющую все функции контроля удаленных соединений на основе взаимодействия с центральной БД системы защиты. Сервер аутентификации создает единую точку наблюдения и проверки всех удаленных пользователей и контролирует доступ к компьютерным ресурсам в соответствии с установленными правилами.

К наиболее популярным протоколам централизованного контроля доступа к сети удаленных пользователей относятся протоколы TACACS (Terminal Access Controller Access Control System) и RADIUS (Remote Authentication Dial-In User Service). Они предназначены в первую очередь для организаций, в центральной сети которых используется несколько серверов удаленного доступа. В этих системах администратор может управлять БД идентификаторов и паролей пользователей, предоставлять им привилегии доступа и вести учет обращений к системным ресурсам.

Протоколы TACACS и RADIUS требуют применения отдельного сервера аутентификации, который для проверки подлинности пользователей и определения их полномочий может использовать не только собственную БД, но и взаимодействовать с современными службами каталогов, например, с NDS (Novell Directory Services) и Microsoft Windows NT Directory Service.

Серверы TACACS и RADIUS выступают в качестве посредников между серверами удаленного доступа, принимающими звонки от пользователей, с одной стороны, и сетевыми ресурсными серверами — с другой. Реализации TACACS и RADIUS могут также служить посредниками для внешних систем аутентификации.

Рассмотрим особенности централизованного контроля удаленного доступа на примере протокола TACACS.

[](http://ypn.ru/wp-content/uploads/2010/09/13.5.jpg)

Система TACACS выполнена в архитектуре клиент-сервер. В компьютерной сети, включающей несколько серверов удаленного доступа, устанавливается один сервер аутентификации, который называют сервером TACACS (обычно это программа, работающая в среде универсальной ОС, чаще всего Unix).

На сервере TACACS формируется центральная база учетной информации об удаленных пользователях, включающая их имена, пароли и полномочия. В полномочиях каждого пользователя задаются подсети, компьютеры и сервисы, с которыми он может

работать, а также различные виды ограничений, например, временные ограничения. На этом сервере ведется БД аудита, в которой накапливается регистрационная информация о каждом логическом входе, продолжительности сессии, а также времени использования ресурсов сети.

Клиентами сервера TACACS являются серверы удаленного доступа, принимающие запросы на доступ к ресурсам сети от удаленных пользователей. В каждый такой сервер встроено ПО, реализующее стандартный протокол, по которому они взаимодействуют с сервером TACACS. Этот протокол также называется TACACS.

**2.5 Проверка подлинности Windows**

Проверка — это выполняемый в Интернете процесс, в ходе которого проверяется подлинность копии Windows, а также наличие и целостность важных лицензионных файлов Windows. Эта процедура длится всего несколько секунд и позволяет корпорации Майкрософт сопоставить профиль оборудования компьютера с 25-символьным ключом продукта, который обычно указывается в [сертификате подлинности](http://windows.microsoft.com/ru-ru/windows/genuine/what-to-look-for). Это сопоставление анонимно архивируется для использования при дальнейших попытках активации и проверки, позволяя гарантировать, что установленный на компьютере ключ продукта Windows соответствует оригинальному ключу продукта Windows, который был приобретен. Таким образом проверка гарантирует, что ключ продукта не используется другими лицами в злоумышленных целях, например, для активации нелицензионных или контрафактных копий Windows. Корпорация Майкрософт может попросить выполнить проверку после активации Windows, в случае запроса загрузки подлинной операционной системы Windows из Центра загрузки Майкрософт или запроса не относящейся к безопасности загрузки из Центра обновления Windows. Во время проверки никакие персональные данные не собираются.

После завершения проверки отобразится веб-страница с объяснением результатов. Например, если подлинность установленной на компьютере операционной системы Windows подтверждена, отобразится веб-страница с сообщением об успешном завершении проверки и подтверждением подлинности Windows. Однако если окажется, что на компьютере используется контрафактная операционная система Windows, на отображенной веб-странице будут содержаться сведения о проблеме, которая привела к невозможности подтверждения, включая предполагаемые причины ее возникновения и рекомендации по ее устранению. Также отобразятся специальные предложения корпорации Майкрософт по покупке подлинной операционной системы Windows, если на компьютере установлена контрафактная система Windows.

Кроме того, если установленная операционная система Windows — нелицензионная, конфигурация операционной системы вашего компьютера может быть изменена. Если Windows XP не смогла пройти проверку, на рабочем столе будет отображаться напоминание о том, что операционная система Windows может быть контрафактной. Напоминания также будут отображаться при каждом входе в систему и периодически во время использования Windows, а фоновый рисунок рабочего стола изменится на черный фон. Можно изменить цвет или установить любимый фон рабочего стола, но он все равно будет меняться на черный фон каждые 60 минут. Кроме того, вы не сможете получать обновления из Центра обновления Windows за исключением обновлений безопасности системы. Эти изменения будут сохранять силу, пока операционная система Windows не станет подлинной. Если проверка Windows уже была выполнена ранее, но вам необходимо повторно просмотреть рекомендации по решению проблемы или специальные предложения от корпорации Майкрософт по приобретению лицензионной операционной системы Windows, можно в любой момент нажать кнопку выполнить проверку сейчас.