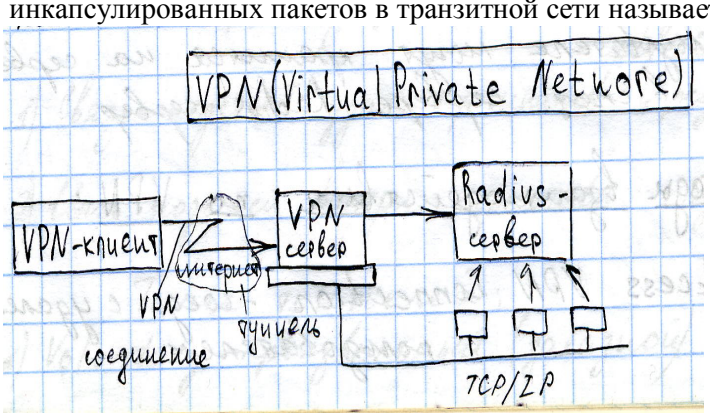
40. Удаленный доступ через промежуточные сети.

Раньше удаленный международный или междугородный доступ отдельных пользователей всегда реализовывался по схеме, основанной на использовании международной или междугородной телефонной связи. Публичные территориальные сети с коммутацией пакетов (в основном — сети X.25) не были так распространены, чтобы, находясь в любом городе, посланный в командировку сотрудник мог получить доступ к этой сети, а через нее — к маршрутизатору или серверу удаленного доступа своего предприятия. Поэтому удаленные пользователи непосредственно звонили по телефонной сети на сервер удаленного доступа своего предприятия, не считаясь с затратами на международные или междугородные переговоры.
Однако сегодня очень часто служба международной сети с коммутацией пакетов имеется во многих городах, и чаще всего это служба Internet. По мере развития услуг сетей frame relay возможно, что и эта технология получит такое же массовое распространение. Поэтому стала возможной двухступенчатая связь удаленного пользователя со своей корпоративной сетью — сначала выполняется доступ по городской телефонной сети к местному поставщику услуг Internet, а затем через Internet пользователь соединяется со своей корпоративной сетью.
Такой вариант может значительно удешевить доступ по сравнению с непосредственным подключением через междугородные АТС.
Центральная сеть предприятия, используя выделенный канал, обычно непосредственно подключается к той же сети с коммутацией пакетов, что и удаленные пользователи в других городах.
Стандартизация клиентов удаленного доступа на основе протоколов PPP и SLIP упрощает проблемы обслуживания разнородных пользователей одним поставщиком услуг при использовании Internet в качестве промежуточной сети. Для сетей X.25 протоколы взаимодействия сети офиса с сетью поставщика услуг также вполне определены, хотя иногда наблюдаются случаи различной настройки одного и того же протокола в оборудовании и программном обеспечении клиента и поставщика услуг.

Технология VPN.

VPN расшифровывается как Virtual Private Network – “виртуальная частная сеть”. Суть этой технологии в том, что при подключении к VPN серверу при помощи специального программного обеспечения поверх общедоступной сети в уже установленном соединении организуется зашифрованный канал, обеспечивающий высокую защиту передаваемой по этому каналу информации за счёт применения специальных алгоритмов шифрования.
В общем случае VPN - это объединение локальных сетей или отдельных машин, подключенных к сети общего пользования, в единую виртуальную (наложенную) сеть, обеспечивающую секретность и целостность передаваемой по ней информации (прозрачно для пользователей).
Для того чтобы была возможность создания VPN на базе оборудования и программного обеспечения от различных производителей необходим некоторый стандартный механизм. Таким механизмом построения VPN является протокол Internet Protocol Security (IPSec). IPSec описывает все стандартные методы VPN. Этот протокол определяет методы идентификации при инициализации туннеля, методы шифрования, используемые конечными точками туннеля и механизмы обмена и управления ключами шифрования между этими точками. Из недостатков этого протокола можно отметить то, что он ориентирован на IP. Другими протоколами построения VPN являются протоколы PPTP (Point-to-Point Tunneling Protocol), , объединивший оба вышеназванных протокола. Однако эти протоколы, в отличие от IPSec, не являются полнофункциональными (например, PPTP не определяет метод шифрования).Говоря об IPSec, нельзя забывать о протоколе IKE (Internet Key Exchange), позволяющем обеспечить передачу информации по туннелю, исключая вмешательство извне. Этот протокол решает задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами, в то время, как IPSec кодирует и подписывает пакеты. IKE автоматизирует процесс передачи ключей, используя механизм шифрования открытым ключом, для установления безопасного соединения. Помимо этого, IKE позволяет производить изменение ключа для уже установленного соединения, что значительно повышает конфиденциальность передаваемой информации.
Протокол, сочетающий в себе функции обслуживания туннеля и передачи данных, называется *протоколом туннелирования* (tunneling protocol). Для формирования туннеля клиент
и сервер туннелирования должны использовать одинаковый протокол.
Туннелирование (tunneling), или *инкапсуляция* (encapsulation), — это способ передачи информации через транзитную сеть. Такой информацией могут быть кадры (или пакеты) другого протокола. При инкапсуляции кадр не передается в сгенерированном узлом-отправителем виде, а снабжается дополнительным заголовком, содержащим информацию о маршруте, позволяющую инкапсулированным пакетам проходить через промежуточную сеть. На конце туннеля кадры деинкапсулируются и передаются получателю. Этот процесс

(включающий инкапсуляцию и передачу пакетов) и есть туннелирование. Логический путь передвижения инкапсулированных пакетов в транзитной сети называется *туннелем* (tunnel).



Типы туннелей. Существует два основных типа туннелей: *заказные* (voluntary) и *принудительные* (compulsory).В зависимости от конфигурации клиента принудительные туннели могут быть *статическими* (static) и *динамическими* (dynamic).
Заказные туннели. Устанавливаются и настраиваются пользователем — клиентом туннеля. Компьютер пользователя является одним из концов туннеля и играет роль клиента. Заказные туннели создаются, когда рабочая станция клиента запрашивает туннель у сервера туннелирования. Так как компьютер клиента берет на себя функции клиента туннеля, на нем должен быть установлен соответствующий протокол туннелирования. Заказные туннели применяются в одном из следующих случаев.
• Клиент уже имеет доступ к транзитной сети, способной маршрутизировать инкапсулированные данные между клиентом и сервером туннелирования.
• Наиболее распространенный вариант. Клиент должен установить удаленное подключение (по коммутируемому каналу) с транзитной сетью до настройки туннеля. Типичным пример — пользователь, имеющий доступ в Интернет по коммутируемой линии. Набрав
телефон своего ISP, он получает доступ в Интернет, и может организовать туннель.
Принудительные туннели. Создаются и настраиваются автоматически. При этом функции клиента туннеля выполняет не компьютер пользователя, а другое промежуточное устройство.
Туннель может быть создан, даже если на клиентском компьютере не установлен протокол туннелирования. При этом от имени клиентского компьютера может выступать другой компьютер или сетевое устройство — *концентратор доступа* (access concentrator). Концентратор доступа должен иметь протокол туннелирования и уметь создавать туннель при подключении к нему клиентского компьютера.
Статические принудительные туннели. Конфигурация со статическими туннелями требует оборудования, предоставляющего доступ по выделенной линии (автоматические туннели), либо ручной настройки (туннелина основе сферы).При автоматическом туннелировании каждому клиенту удаленного доступа назначается определенный сервер туннелирования, на который он будет автоматически направляться при соединении с концентратором доступа. Для этого нужны выделенные линии локального доступа и оборудование для сетевого доступа (это стоит недешево). Для каждого сервера туннелирования можно назначить определенный номер, набрав который, пользователь через концентратор доступа установит с ним туннель.
Динамические принудительные туннели. Адрес назначения выбирается в момент подключения пользователя к концентратору доступа. Так как этот выбор может быть основан на самых разных параметрах (имени или адресе пользователя, номере телефона пользователя или концентратора доступа, отделе или даже времени дня), пользователи из одной сферы могут быть направлены на разные
серверы туннелирования. Это делает динамическое туннелирование самым гибким мето дом принудительного туннелирования.
Управление пользователями. Так как размещать учетные записи одного пользователя на разных серверах непрактично,
большинство администраторов создают главную БД учетных записей на контроллере домена или сервере RADIUS. Это позволяет серверу VPN отправлять сведения об аутентификации на центральное устройство аутентификации. Для удаленного доступа через ком-
мутируемое или VPN-подключение применяются одни и те же учетные записи.
Управление аутентификацией. В качестве поставщика служб проверки подлинности для сервера VPN можно выбрать как
Windows, так и RADIUS. В первом случае пользователи, пытающиеся установить VPN-соединение, аутентифицируются средствами Windows и политики удаленного доступа, настраиваемой из оснастки Routing And Remote Access.Во втором случае реквизиты пользователей и параметры запрашиваемого подключения направляются на сервер RADIUS. Получив сообщение о запросе пользователя на подключение к серверу VPN, сервер RADIUS проверяет пользователя по своей БД аутентификации. В центральной БД сервера RADIUS могут храниться параметры пользователя, поэтому, кроме положительного или отрицательного ответа на запрос об аутентификации, сервер RADIUS может сообщать серверу VPN и другие параметры подключения, например максимальное время сеанса, выделяемые пользователям статические IP-адреса и др. Сервер IAS RADIUS хранит сведения о профиле удаленного доступа для клиентов, использующих сервер RADIUS в

качестве поставщика проверки подлинности. Если сервер RAS использует аутентификацию RADIUS, то в дереве консоли оснастки Routing And Remote Access не отображается узел Remote Access Policies. При этом для настройки политики удаленного доступа надо использовать IAS.Для ответов на запросы об аутентификации RADIUS может использовать или другой сервер БД, например ODBC-источник, или контроллер домена Windows 2000. Последний может располагаться как на том же компьютере, что и сервер RADIUS, так и в другом месте. Кроме того, сервер RADIUS может играть роль прокси-клиента для удаленного сервера RADIUS.

Резюме.VPN обладает свойствами выделенной частной сети, поддерживая передачу данных между двумя компьютерами через транзитную сеть, например Интернет. Для соединения с сетью организации через Интернет подразделение организации может использовать как выделенные, так и коммутируемые линии. VPN передает информацию с помощью туннелирования-метода передачи через транзитную сеть. Протокол туннелирования состоит из протокола поддержки туннеля и протокола передачи данных через туннель. Существует два основных типа туннелей-заказные и принудительные. Для соединений VPN в Windows 2000 используются протоколы PPTP, L2TP, IPSec и IP-IP. Управление VPN включает в себя управление пользователями, адресами и серверами имен, доступом, аутентификацией и шифрованием. Проблемы, возникающие при работе с VPN, могут быть связаны с IP-соединениями, установление vf подключений удаленного доступа, маршрутизацией и IPSec.