

# Удаленный доступ

Лаштанов И.Г.



# Общие сведения о RRAS

Служба **RRAS** в Windows 2000 Server позволяет удаленным пользователям подключаться по телефонным линиям к корпоративной сети и обращаться к ее ресурсам, как если бы они были подключены к этой сети напрямую. RRAS также содержит службы VPN, позволяющие предоставлять доступ к корпоративным сетям через Интернет.

Служба RRAS в Windows 2000 Server обрабатывает подключения удаленных пользователей. В итоге они работают так, как если бы их компьютеры были физически соединены с сетью. Пользователи (или клиенты) запускают ПО удаленного доступа для подключения к серверу удаленного доступа — компьютеру с Windows 2000 Server и службой RRAS. Он идентифицирует пользователей и обслуживает подключения до их завершения. При удаленном подключении клиентам доступны те же службы, что и пользователям ЛВС, в том числе службы доступа к файлам и принтерам, доступ к Web-серверам и обмен сообщениями.

Клиенты удаленного доступа применяют стандартные средства для доступа к сетевым ресурсам. Поскольку RRAS полностью поддерживает буквы дисков и имена UNC, большинство приложений не требуют модификации для работы с удаленным доступом. Сервер Windows 2000 обслуживает два типа удаленных подключений:

- **Подключение по коммутируемой (телефонной) линии.**
- **Виртуальная частная сеть (VPN).**

# Типы удаленных подключений

**Подключение по коммутируемой (телефонной) линии.** Клиент удаленного доступа может установить временное телефонное подключение с физическим портом на сервере удаленного доступа, пользуясь услугами поставщика телекоммуникаций, по аналоговой линии, линиям ISDN или X.25. Типичный пример такого подключения — клиент, набирающий телефонный номер одного из портов сервера удаленного доступа. Удаленное подключение по аналоговой линии или **ISDN** — прямое физическое соединение клиента и сервера. Передаваемые по такому каналу данные можно шифровать, хотя это и не обязательно.

**Виртуальная частная сеть (VPN).** Это реализация защищенных соединений типа «точка-точка» через частную или общедоступную сеть, например Интернет. Для вызова порта на сервере VPN клиент использует специальные протоколы, основанные на TCP/IP, называемые туннельными. Типичный пример VPN — подключение клиента по телефону через Интернет к серверу корпоративной сети. Сервер удаленного доступа отвечает на виртуальный вызов, идентифицирует вызывающего и передает данные между клиентом VPN и корпоративной сетью.

В отличие от прямого подключения по телефону работа через VPN — это логическое (а не физическое) соединение между клиентом и сервером. Для гарантии безопасности рекомендуется шифровать данные, передаваемые по VPN-подключению.

# Функции RRAS

Служба RRAS включает функции преобразования сетевых адресов (Network Address Translation NAT), мультипротокольной маршрутизации, протокол туннелирования канального уровня (Layer Two Tunneling Protocol, L2TP), службу проверки подлинности в Интернете (Internet Authentication Service, IAS) и политики удаленного доступа (Remote Access Policies, RAP). В конце этого занятия рассказано о фильтрах подключения по запросу, настройке времени подключения и свойств удаленного доступа для объекта пользователя, применении серверов имен и DHCP, протоколе VAP и мониторинге удаленного доступа.

# NAT и многоадресная маршрутизация

**NAT.** это стандарт, определенный в RFC 1631. NAT — маршрутизатор, преобразующий IP-адреса интрасети или домашней ЛВС в действительные адреса Интернета. NAT позволяет подключаться к Интернету с любого компьютера частной сети через один IP-адрес. Windows 2000 Server включает полную реализацию NAT, называемую Connection Sharing (Общее подключение), и не конфигурируемую версию — Shared Access (Общий доступ).

**Многоадресная маршрутизация.** Windows 2000 Server реализует ограниченную форму многоадресной маршрутизации, используя многоадресный прокси-узел для расширения многоадресной поддержки до полноценного многоадресного маршрутизатора. Лучше всего использовать многоадресный прокси-узел для многоадресной рассылки среди удаленных пользователей или в одной ЛВС, подключенной к Интернету. На одном или нескольких интерфейсах Windows 2000 играет роль многоадресного маршрутизатора, обеспечивая многоадресную рассылку для локальных клиентов. На интерфейсе, который имеет прямой доступ к настоящему многоадресному маршрутизатору. Windows 2000 выполняет функции многоадресного клиента, перенаправляющего трафик со стороны локальных клиентов.

# Протокол L2TP и Служба IAS

**Протокол L2TP.** Его считают следующей версией протокола PPTP. Работа L2TP напоминает PPTP, однако первый включает технологию перенаправления Layer 2 Forwarding (L2F), разработанную Cisco. Вскоре протокол L2TP будет принят в качестве индустриального стандарта и опубликован в RFC. Протокол L2TP соответствует канальному уровню модели OSI и применяется для VPN.

**Служба IAS.** Это сервер Remote Authentication Dial-In User Service (RADIUS). Сетевой протокол RADIUS позволяет проводить удаленную аутентификацию, авторизацию и учет удаленных пользователей, которые подключаются к серверу доступа к сети (Network Access Server, NAS). NAS (например, сервер RRAS в Windows 2000) может быть клиентом или сервером RADIUS.

# Политики удаленного доступа

В Windows NT 3.5 и более поздних версиях удаленный доступ предоставлялся в зависимости от значения параметра Grant Dial-in Permission To User для объекта пользователя или средствами утилиты Remote Access Admin. Параметры обратного вызова также задавались индивидуально для каждого пользователя.

В Windows 2000 удаленный доступ предоставляется на основе свойств объекта пользователя и соответствующей политики — набора условий и параметров подключения, позволяющих сетевым администраторам более гибко настраивать разрешения удаленного доступа. Примеры таких условий — дата, принадлежность к группе или тип подключения (телефонное или VPN). Примеры параметров подключения: требования аутентификации и шифрования, использование многоканальных линий связи и длительность подключений. Одним из достоинств такого дополнительного контроля является требование шифрования при VPN-соединениях и отказ от шифрования при подключении по модему.

Политики удаленного доступа хранятся на локальном компьютере и совместно используются оснасткой Routing and Remote Access (Маршрутизация и удаленный доступ) и службой IAS. Политики удаленного доступа, настраиваются из оснасток Internet Authentication Service (Служба проверки подлинности в Интернете) и Routing and Remote Access.

# Настройка сервера RRAS. Включение входящих подключений

После включения RRAS вы можете настроить обслуживание входящих подключений, ограничить удаленный доступ средствами политики, добавить профили удаленных пользователей и контролировать доступ с помощью протокола ВАР.

При первом запуске RRAS автоматически создаются 5 портов PPTP и 5 портов L2TP. Число доступных любому удаленному серверу VPN-портов не ограничено. Вы вправе настроить порты в папке Ports (Порты) и дереве консоли оснастки Routing and Remote Access (Маршрутизация и удаленный доступ).

В папку Ports также можно добавить параллельный порт. Последовательные коммуникационные порты будут отображаться только после установки модема. Оба типа портов способны обрабатывать входящие и исходящие подключения.



# Создание политики удаленного доступа

Политика удаленного доступа — это именованный набор условий (рис. 11-4), определяющий пользователей, которым разрешен удаленный доступ к сети, и характеристики этого подключения. Принятие или отклонение подключения зависит от разных параметров:

даты и времени подключения, членства в группе, типа службы и т. п. Например, вы можете разрешить подключение по ISDN длительностью не более 30 минут без передачи пакетов HTTP.

Средствами оснастки RRAS политики можно создавать, удалять, переименовывать и упорядочивать. Заметьте, что команда Save при этом недоступна, так что сохранить копию на дискету невозможно. Порядок политик важен, поскольку подключение отклоняется или принимается после прохождения первой подходящей политики.

# Условия политики

На основе этой блок-схемы можно предсказать результат запроса подключения в любой ситуации. Например, для объекта пользователя задан параметр Control Access Through Remote Access Policy, а в политике указано Allow Access If Dial-In Permission Is Enabled (Разрешить доступ, если разрешены входящие подключения). Согласно блок-схеме пользователю будет отказано в подключении.



# Протокол ВАР

Протоколы Bandwidth Allocation Protocol (ВАР) и Bandwidth Allocation Control Protocol (ВАСР) повышают эффективность многоканальных подключений путем динамического добавления и отключения линий связи. Оба протокола являются управляющими протоколами PPP и работают совместно для предоставления полосы пропускания по запросу.

Функции динамического перераспределения полосы пропускания реализуются посредством компонентов, описанных ниже.

- **Link Discriminator** — новая функция протокола управления связью (Link Control Protocol, LCP), используемая для уникальной идентификации каждой линии связи в многоканальном пучке.
- **Протокол ВАСР** — использует LCP-согласования для определения предпочтительного узла, если узлы одновременно передают один и тот же запрос ВАСР.
- **Протокол ВАР** — предоставляет механизм для управления каналом и полосой пропускания. Управление каналом позволяет добавлять и отключать дополнительные каналы связи при необходимости. Управление полосой пропускания решает, когда добавить или отключить канал, в зависимости от текущей нагрузки на каналы связи.

# Внедрение виртуальных частных сетей

VPN обладает свойствами выделенной частной сети и позволяет передавать данные между двумя компьютерами через промежуточную сеть. Дома или в пути пользователи могут, применяя VPN-одключения, соединиться с сервером организации через инфраструктуру общедоступной сети (например Интернета). С точки зрения пользователя, VPN-подключение выглядит как прямое соединение «точка-точка» между его компьютером (клиентом VPN) и сервером организации (сервером VPN). Конкретная инфраструктура общедоступной сети значения не имеет, так как логически данные передаются через выделенное частное подключение.

Организации через VPN-подключения осуществляют соединения между географически удаленными подразделениями или подключаются к серверам других организаций через общедоступные сети (например Интернет) с поддержкой безопасной связи. VPN-подключения через Интернет логически выглядят как выделенные подключения через ГВС.

Интерфейс виртуальной сети предоставляет пользователю защищенное подключение к частной сети через общедоступную.

# Схема виртуальной частной сети



# Основы туннелирования

*Туннелирование* (tunneling), или *инкапсуляция* (encapsulation), — это способ передачи полезной информации через промежуточную 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).



# Протоколы VPN

Для формирования VPN в Windows 2000 используются протоколы PPTP, L2TP, IPSEC и IP-IP.

- Протокол PPTP — позволяет инкапсулировать IP-, IPX- и NetBEUI-трафик в заголовки IP для передачи по IP-сети, например Интернету;
- Протокол L2TP — позволяет шифровать и передавать IP-трафик с использованием любых протоколов, поддерживающих режим «точка-точка» доставки дейтаграммам. Например, к ним относятся протокол IP, ретрансляция кадров и асинхронный режим передачи (ATM);
- Протокол IPSec — позволяет шифровать и инкапсулировать полезную информацию протокола IP в заголовки IP для передачи по IP-сетям, например Интернету;
- Протокол IP-IP — IP-дейтаграмма инкапсулируется с помощью дополнительного заголовка IP. Главное назначение IP-IP — туннелирование многоадресного трафика и частях сети, не поддерживающих многоадресную маршрутизацию.

# Поддержка многоканальных подключений

Протокол Point-to-Point Protocol (PPP) разработан для передачи данных по телефонным линиям и выделенным соединениям точка-точка. PPP инкапсулирует пакеты IP, IPX и NetBIOS и кадры PPP и передает их по каналу точка-точка. Протокол PPP может использоваться маршрутизаторами, соединенными выделенным каналом, или клиентом и сервером RAS, соединенными удаленным подключением.

Многоканальные подключения, впервые реализованные в службе RAS Windows NT 4.0, позволяют объединять несколько физических соединений в один логический канал. Обычно объединяют две и более ISDN-линии или модемных подключения для расширения полосы пропускания. Поддержка многоканальности стала возможной благодаря:

- **новому параметру LCP** — во время фазы LCP протокола PPP определяется, можно ли создать многоканальное подключение;
- **новому протоколу PPP** — он называется MP (Multilink PPP) и для PPP выглядит как стандартная полезная информация. MP изменяет последовательность и содержимое пакетов перед тем, как передать их транспортному протоколу, например TCP/IP.