

Настройка удаленного доступа через модемный пул для различных платформ

Справочное пособие для автоматизаторов (версия 1.0)

Оглавление

1	Настройка модемного пула под ОС семейства Windows	2
	Настройка модемного пула под Windows 2000 Server	2
	Утилита настройки сервера	2
	Настройка удалённого доступа	3
	Мастер настройки удалённого доступа	4
	Редактирование настроек удалённого доступа	10
	Утилита настройки сервера	10
	Настройка удалённого доступа	10
	Настройка входящих модемных соединений	12
	Настройка модемного пула под Windows 2003 Server	17
	Мастер настройки сервера	17
	Мастер настройки удалённого доступа	19
	Редактирование настроек удалённого доступа	24
	Настройка входящих модемных соединений	25
2	Настройка модемного пула под ОС семейства Unix	26
	Конфигурация ядра	27
	Установка и настройка mgetty	27
	Настройка rppd	28
	Распределение IP-адресов	29
	Настройка MASQUERADE	30
3	Приложение. Обзор вариантов организации модемного пула	32
	Проектирование мощности модемного пула	32
	Пример расчета нагрузки на модемный пул	32
	Краткое описание теории расчета количества каналов	33
	Обзор аппаратных решений	33
	Применение многоканального телефона	33
	Аналоговые и цифровые телефонные линии	33
	Решения для аналоговых линий	34
	Решения для цифровых линий E1	35
4	Источники дополнительной информации	37

Глава 1

Настройка модемного пула под ОС семейства Windows

В данной главе описаны инструкции по установке модемного пула под следующими ОС семейства Windows:

- Windows 2000 Server;
- Windows 2003 Server.

Настройка модемного пула под Windows 2000 Server

Утилита настройки сервера

Запустите утилиту настройки сервера с помощью меню **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Configure Your Server Wizard**. На экране появится главное окно утилиты (см. [рис. 1.1](#)).



Рис. 1.1. Главное окно утилиты настройки сервера

Нажмите на раздел **Networking** (Сетевые подключения) и в открывшемся списке выберите параметр **Remote Access** (Удалённый доступ) (см. [рис. 1.2](#)). В окне утилиты содержатся общие сведения об удалённых подключениях, краткие подсказки к действиям в утилите настройки удалённого доступа. Для запуска утилиты настройки удалённого доступа нажмите на ссылку [Open](#).

Если в окне утилиты содержится информация о том, что на компьютере уже установлено ПО удалённого доступа к сети и по своему внешнему виду оно отличается от окна на [рис. 1.2](#) – переходите в раздел **Редактирование настроек удалённого доступа**.

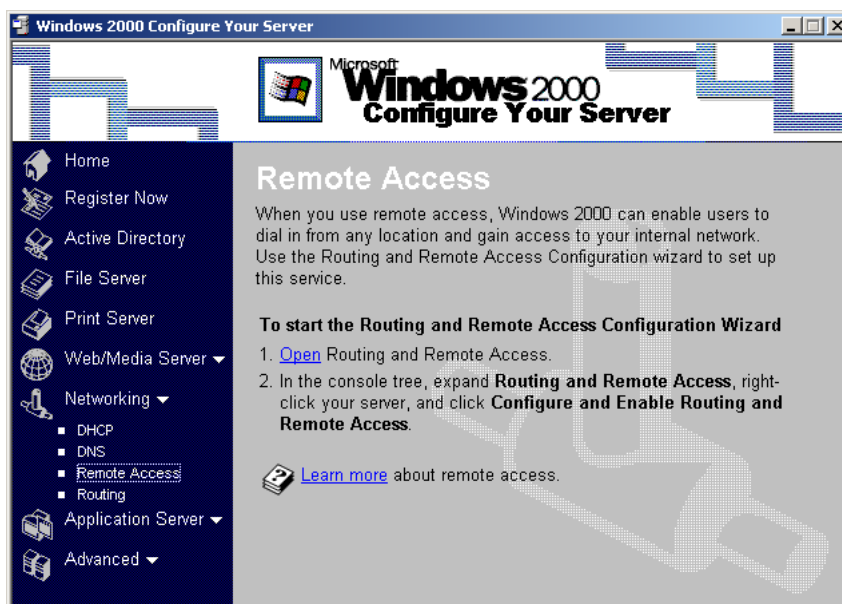



Рис. 1.2. Выбор параметра **Remote Access**

Данное действие запустит утилиту настройки удалённого доступа, главное окно которой представлено на [рис. 1.3](#).

Настройка удалённого доступа

Утилита настройки удалённого доступа помогает установить дополнительное ПО Сервера удалённого доступа, включающее в себя поддержку маршрутизации, удалённого доступа, и VPN. Выберите пункт меню **Actions** → **Add Server** (Действия – Добавить сервер). На экране отобразится следующее окно – [рис. 1.4](#).

В окне добавления сервера выберите пункт **This computer** (Этот компьютер) и нажмите **Ok**. В главном окне утилиты отобразится сетевое имя вашего сервера (см. [рис. 1.5](#)).

Наличие красной точки на иконке сервера напротив наименования вашего компьютера –  означает, что на вашем компьютере не установлено ПО Сервера удалённого доступа. В этом случае выберите указателем мыши ваш компьютер в списке и вызовите контекстное меню. В открывшемся контекстном меню выберите пункт **Configure and Enable Routing and Remote Access** (Настроить и разрешить маршрутизацию и удалённый доступ).

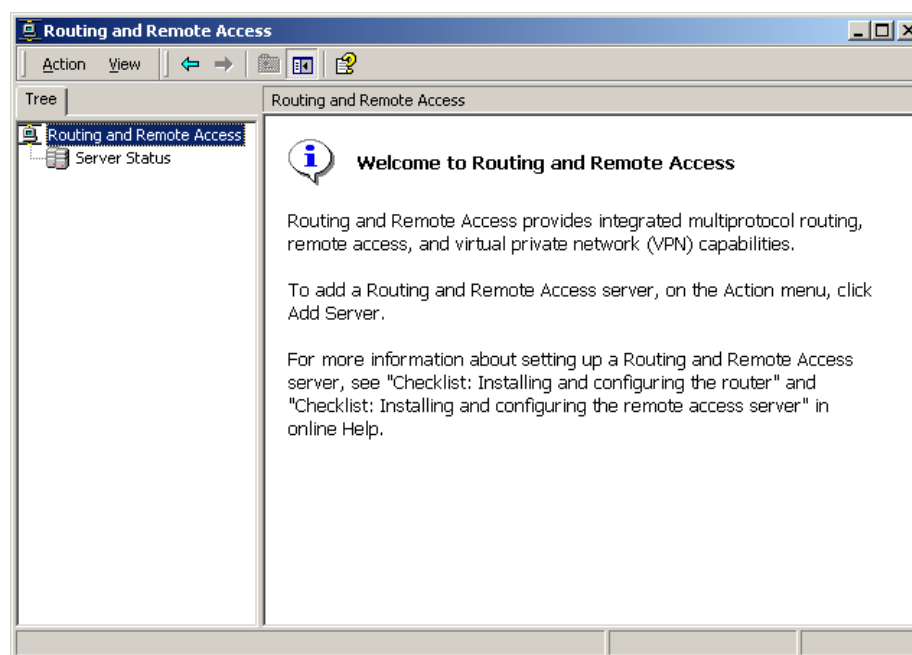


Рис. 1.3. Утилита настройки удалённого доступа

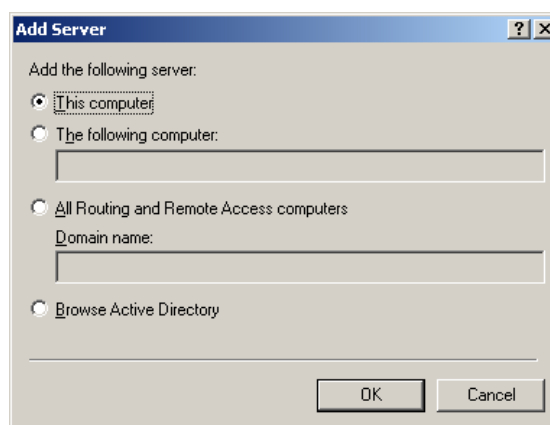


Рис. 1.4. Окно добавления сервера

Мастер настройки удалённого доступа

Выбор пункта контекстного меню **Configure and Enable Routing and Remote Access** запустит Мастер настройки удалённого доступа, первое окно которого представлено на [рис. 1.6](#). Нажмите на кнопку **Next** для перехода в окно выбора желаемого вида конфигурации – [рис. 1.7](#).

Выбор вида конфигурации

В окне выбора вида конфигурации выберите пункт **Remote Access Server** (Сервер удалённого доступа) и нажмите на кнопку **Next**. На экране появится окно со списком необходимых для работы удалённого доступа протоколов ([рис. 1.8](#)).

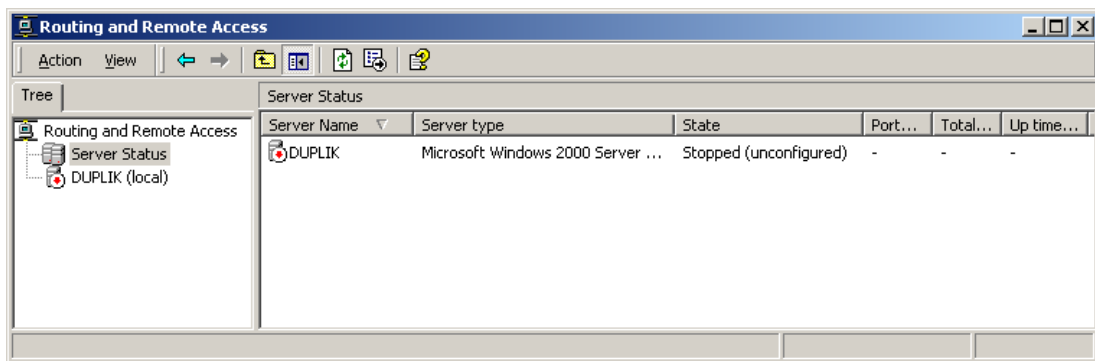


Рис. 1.5. Добавленный сервер в утилите настройки удалённого доступа

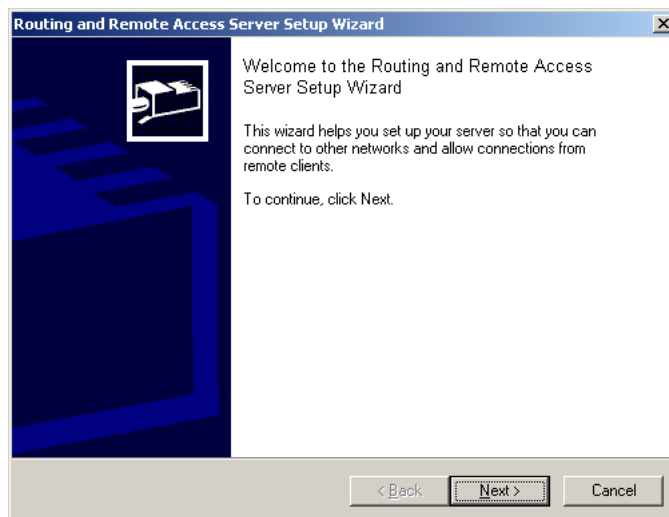


Рис. 1.6. Первое окно Мастера настройки удаленного доступа

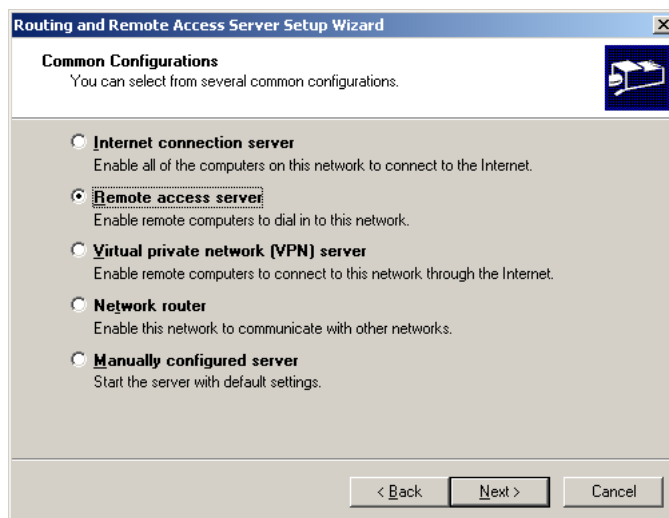


Рис. 1.7. Окно выбора вида конфигурации

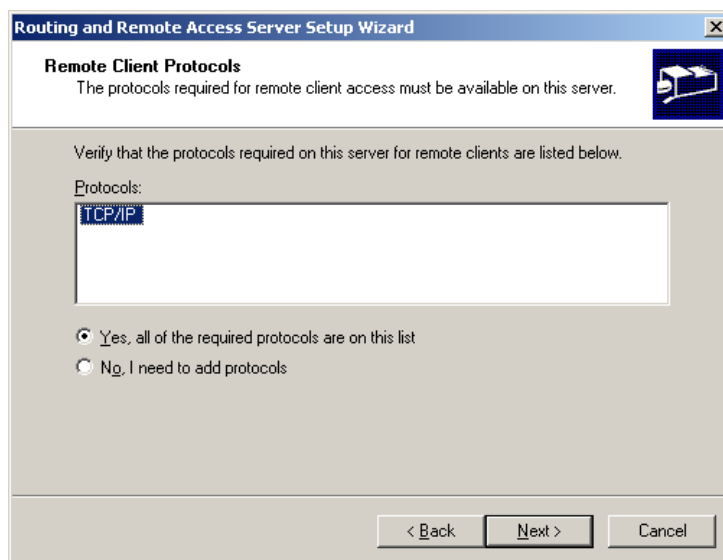


Рис. 1.8. Окно списка протоколов

Проверка установленных протоколов

Для организации удалённого доступа клиентов с помощью модемного пула необходимо наличие установленного протокола TCP/IP. Убедитесь, что данный протокол присутствует в списке. В противном случае установите этот протокол на вашем компьютере. Нажмите на кнопку **Next** для перехода к следующему окну.

Выбор локальной сети

В появившемся окне (рис. 1.9) необходимо выбрать сеть, к которой будут подключаться модемы клиентов банка. Выберите необходимую сеть и нажмите **Next**.

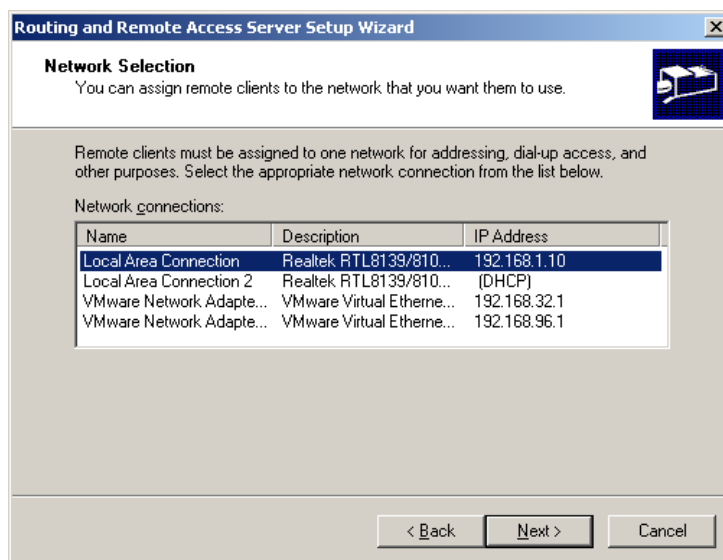


Рис. 1.9. Окно выбора сети

Выбор принципа назначения IP-адресов

В открывшемся окне следует указать принцип назначения IP-адресов клиентам, подключающимся с помощью модема (рис. 1.10). В целях безопасности необходимо назначать IP-адреса, отличные от используемых компьютерами в локальной сети банка. Для этого выберите опцию **From a specified range of addresses** (Из определённого диапазона адресов) и нажмите **Next** для перехода к окну управления диапазонами адресов.

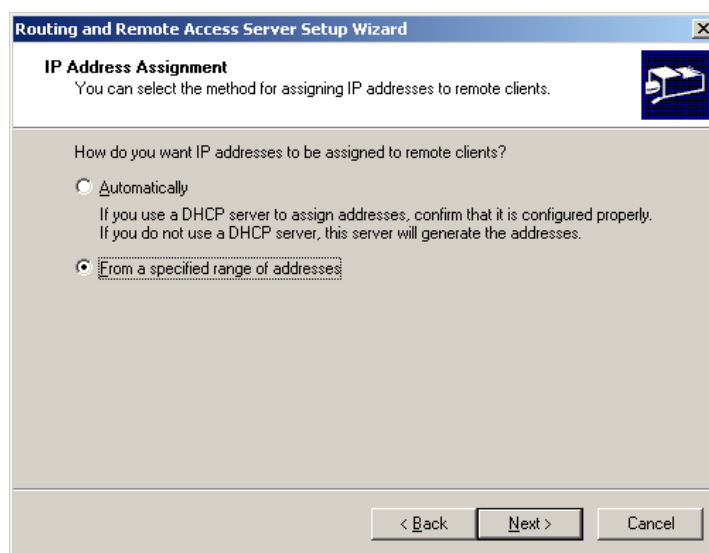


Рис. 1.10. Выбор принципа назначения IP-адресов

Выделение диапазонов адресов

Внутренняя сеть банка должна быть сконфигурирована таким образом, чтобы Сервер Приложения iBank 2 UA находился в том же сегменте сети, что и компьютер, обеспечивающий связь с модемным пулом. Остальные сегменты внутренней сети банка должны быть закрыты для выделенных клиентам диапазонов IP-адресов. Из этих соображений вопрос выбора диапазонов IP-адресов должен быть предварительно согласован с системным администратором банка. Общее количество задаваемых IP-адресов должно на 1 превышать количество подключенных линий. Адреса должны выбираться из диапазона, не пересекающегося с диапазонами адресов, реально используемых в сети (т.н. «серые» адреса).

О том, как машине клиента можно присвоить её собственный IP-адрес, отличный от адресов из разрешённого диапазона, смотрите в подразделе [Дополнительные правила для IP-адресов](#).

Окно управления диапазонами IP-адресов представлено на рис. 1.11. Нажмите на кнопку **New...** для вызова окна добавления диапазона IP-адресов (рис. 1.12).

В открывшемся окне **New Address Range** выполните следующие действия:

1. В поле **Start IP address** введите начальный IP-адрес диапазона, из которого будут выдаваться адреса клиентам;
2. В поле **End IP address** введите конечный IP-адрес диапазона, из которого будут выдаваться адреса клиентам;

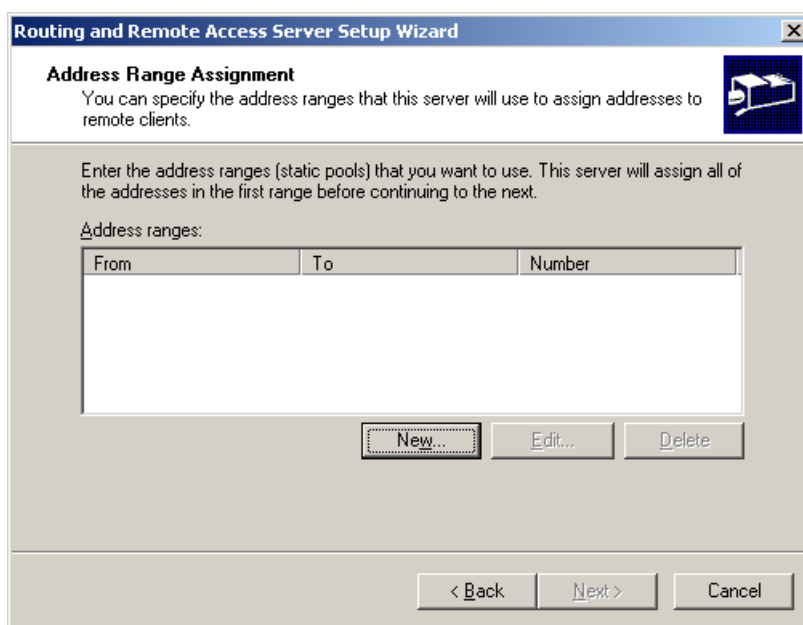
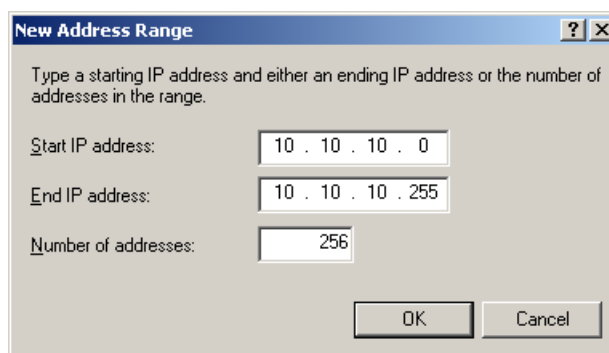


Рис. 1.11. Окно управления диапазонами IP-адресов

Рис. 1.12. Окно **New Address Range** (добавление адресов)

3. Нажмите кнопку **ОК**.

При необходимости, отредактируйте или удалите введённый диапазон (кнопки **Edit...** и **Delete** соответственно); добавьте дополнительные диапазоны IP-адресов в окне управления диапазонами адресов.

Окончив редактирование диапазонов адресов, нажмите **Next** для перехода к следующему окну.

Выбор типа аутентификации клиентов

На [рис. 1.13](#) изображено окно настройки аутентификации для клиентов, подключающихся через модемное соединение.

В нём необходимо выбрать опцию **No, I don't want to set up this server to use RADIUS now.** (запрет на использование сервера RADIUS для аутентификации клиентов) и нажмите **Next** для перехода к последнему окну Мастера настройки удалённого доступа.

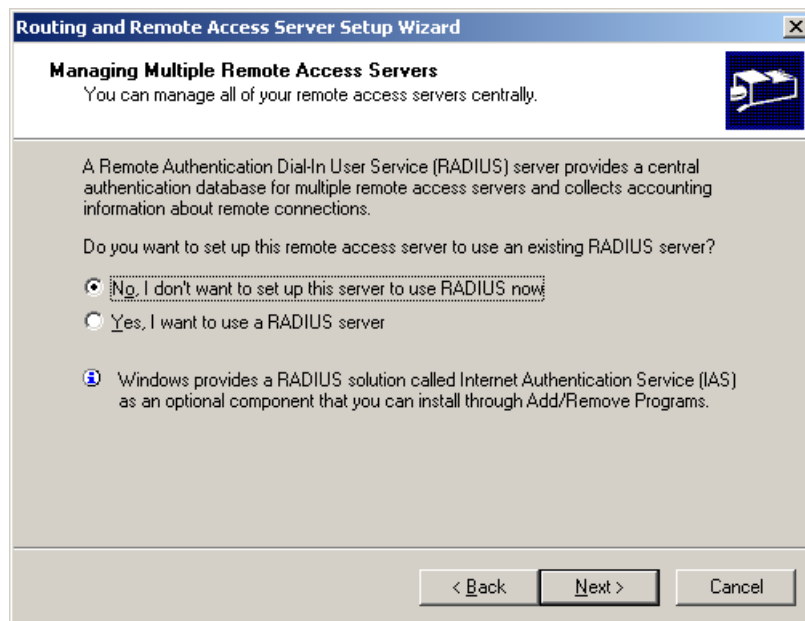


Рис. 1.13. Окно настройки аутентификации клиентов

Выход из Мастера настройки удалённого доступа

В последнем окне Мастера (рис. 1.14) нажмите **Finish** для выхода.

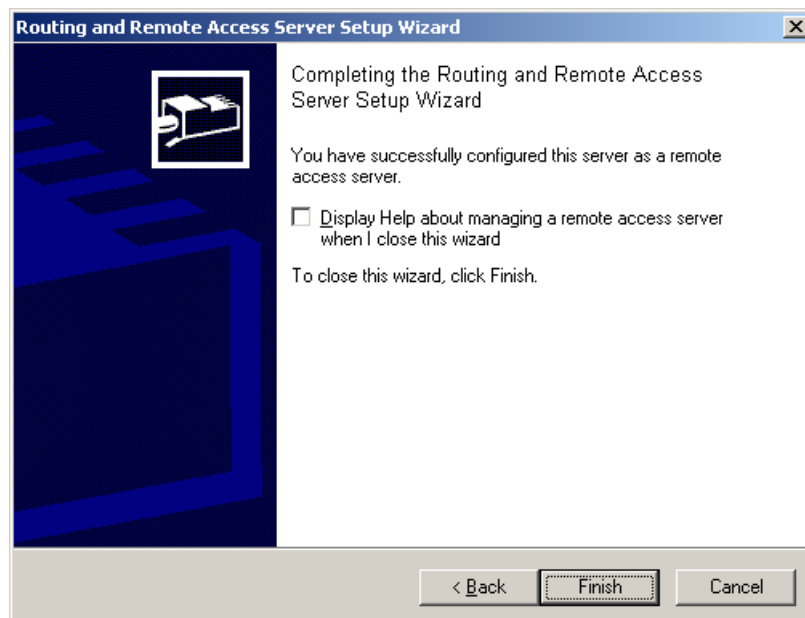


Рис. 1.14. Последнее окно Мастера настройки удалённого доступа

Редактирование настроек удалённого доступа

Утилита настройки сервера

Для проверки или редактирования настроек удалённого доступа запустите мастер настройки сервера с помощью меню **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Configure Your Server Wizard**. На экране появится стартовое окно мастера (см. [рис. 1.1](#)).

Нажмите на раздел **Networking** (Сетевые подключения) и в открывшемся списке выберите параметр **Remote Access** (Удалённый доступ) (см. [рис. 1.15](#)). В окне утилиты содержатся общие сведения об удалённых подключениях, краткие подсказки к действиям в утилите настройки удалённого доступа. Для запуска утилиты настройки удалённого доступа нажмите на ссылку [Manage](#) (Настройка).



Рис. 1.15. Окно запуска утилиты настройки удалённого доступа

Настройка удалённого доступа

Данное действие запустит утилиту настройки удалённого доступа, главное окно которой представлено на [рис. 1.16](#).

Указателем мыши выберите наименование сервера и щелчком правой мыши по нему вызовите контекстное меню. В открывшемся контекстном меню выберите пункт **Properties** (Свойства). В результате этого на экране откроется окно параметров сервера, изображённое на [рис. 1.17](#). Перейдите на вкладку **IP** (Настройка протокола TCP/IP), внешний вид которого представлен на [рис. 1.18](#) и выполните следующее:

1. Проверьте наличие галочек в опциях **Enable IP routing** (Разрешить маршрутизацию IP) и **Allow IP-based remote access and demand-dial connections** (Разрешить удалённый доступ на базе TCP/IP и модемные подключения методом Dial-up).

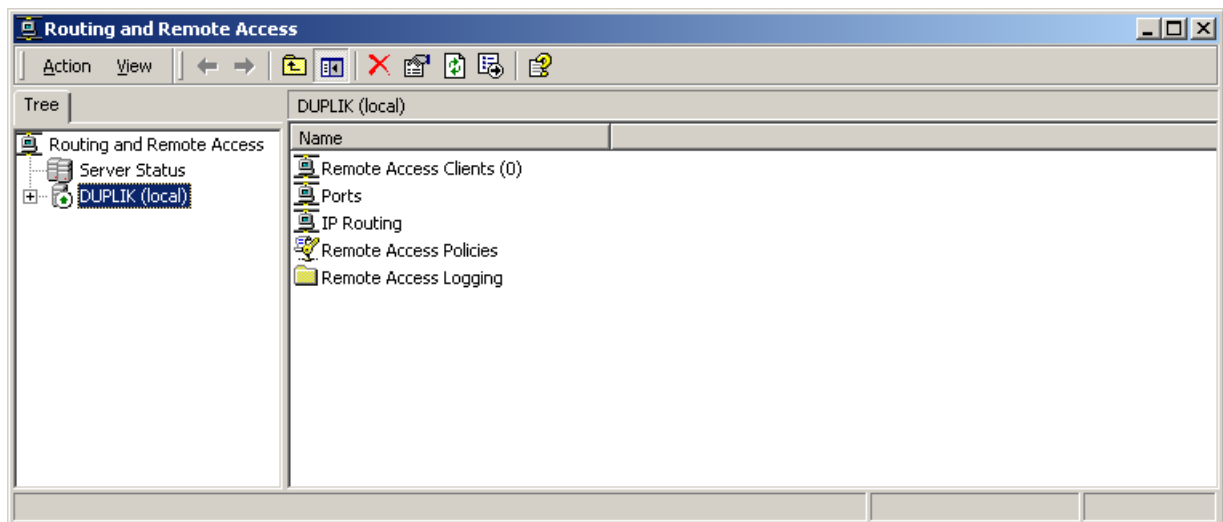
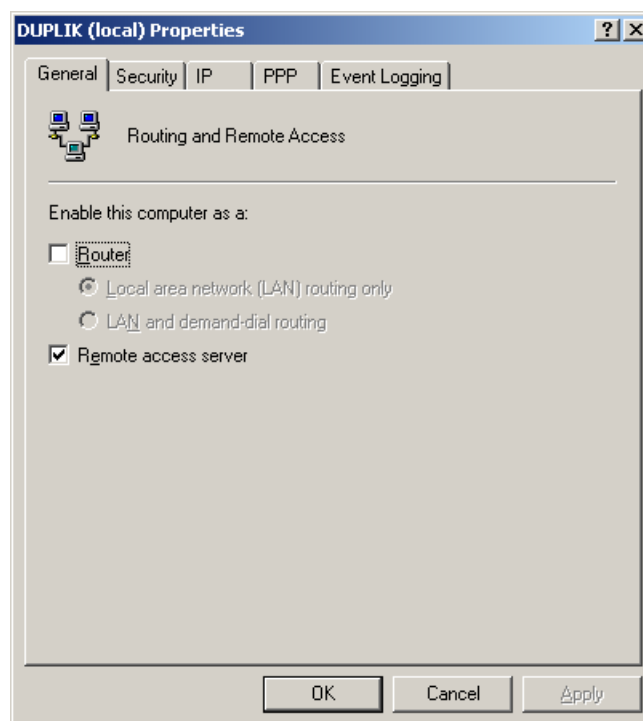


Рис. 1.16. Утилита настройки удалённого доступа

Рис. 1.17. Окно параметров сервера, вкладка **General** (Общие)

2. В секции **IP address assignment** (Назначение IP-адресов) галочка должна быть поставлена в поле **Static address pool** (Массив статических адресов). В таблице ниже отображается список диапазонов назначенных IP-адресов. При необходимости в него можно добавить новые диапазоны адресов кнопкой **Add** или отредактировать существующие кнопкой **Edit**.

Нажмите **Ok** для сохранения введённых настроек.

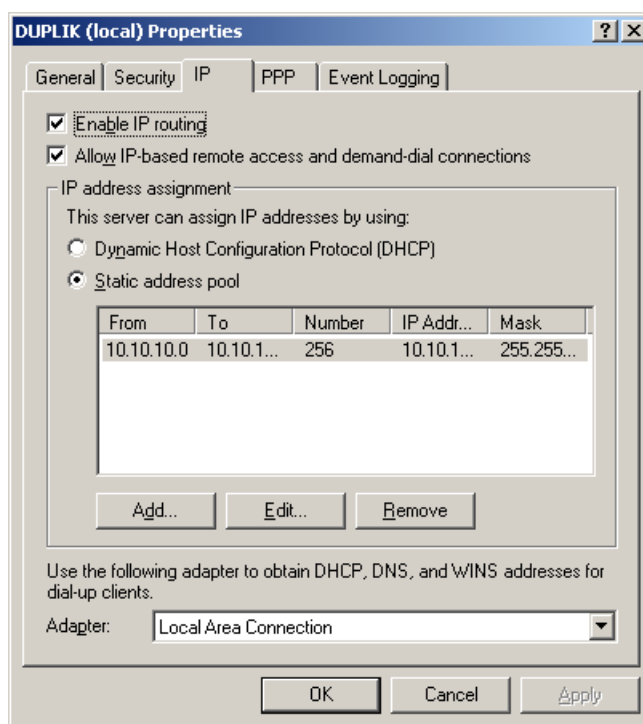


Рис. 1.18. Окно параметров сервера, вкладка **IP** (Настройка протокола TCP/IP)

Настройка входящих модемных соединений

Настройка входящих модемных соединений включает в себя два этапа:

1. Настройку авторизации входящих соединений (обязательный этап);
2. Настройку дополнительных правил распределения IP-адресов (необязательный этап).

Подробнее об этом читайте ниже.

Настройка авторизации

Для настройки модемного пула необходимо создать учётную запись пользователя для входящих модемных соединений. Логин и пароль этого пользователя, а также номер телефона, на котором размещается модемный пул, будут использоваться клиентами банка как параметры настройки Dial-up подключения для PC — Банкинга.

Для создания учётной записи пользователя входящих модемных соединений выполните следующие действия:

1. Зайдите в меню **Start** → **Settings** → **Network and Dial-up Connections** → **Incoming Connections** (Пуск → Настройки → Сетевые и модемные подключения → Входящие соединения).
2. В появившемся окне свойств **Incoming Connections Properties** (Свойства входящих соединений) выберите вкладку **Users** (Пользователи) (рис. 1.19).

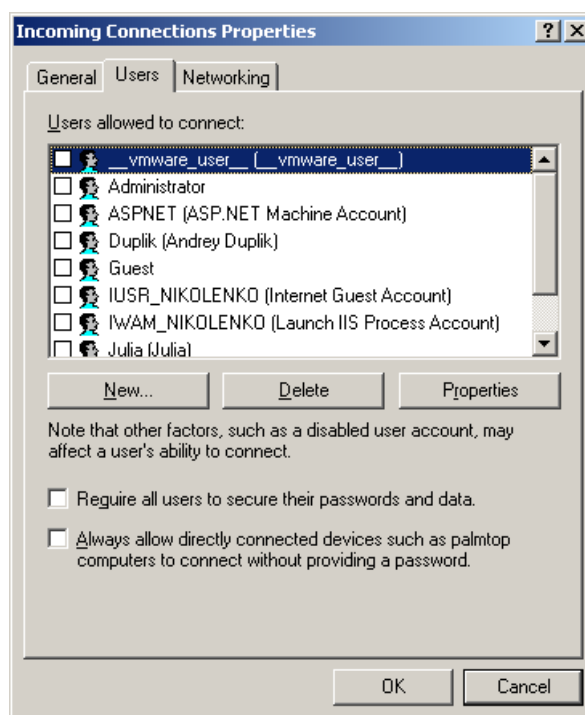


Рис. 1.19. Окно **Incoming Connections Properties**, вкладка **Users**

3. Нажмите на кнопку **New** (Новый) и в открывшемся окне **New User** (Новый пользователь) введите в поля **User name** и **Full name** логин учётной записи и в поля **Password** и **Confirm password** пароль учётной записи. Нажмите **Ok** для сохранения ввода.
4. Добавленный пользователь отобразится в списке учётных записей пользователей, зарегистрированных на данном компьютере. Наличие галочки напротив имени пользователя означает, что данная учётная запись активна для установки входящих модемных соединений (см. [рис. 1.20](#)).

Для удаления учётной записи выберите имя требуемого пользователя и нажмите **Delete**.

Нажатие на кнопку **Properties** (Свойства) открывает окно свойств (<наименование учётной записи> **Properties**) ([рис. 1.21](#)). В данном окне в закладке **General** (Общие) можно изменить пароль учётной записи. Настройка параметров Callback осуществляется на одноимённой вкладке окна свойств.

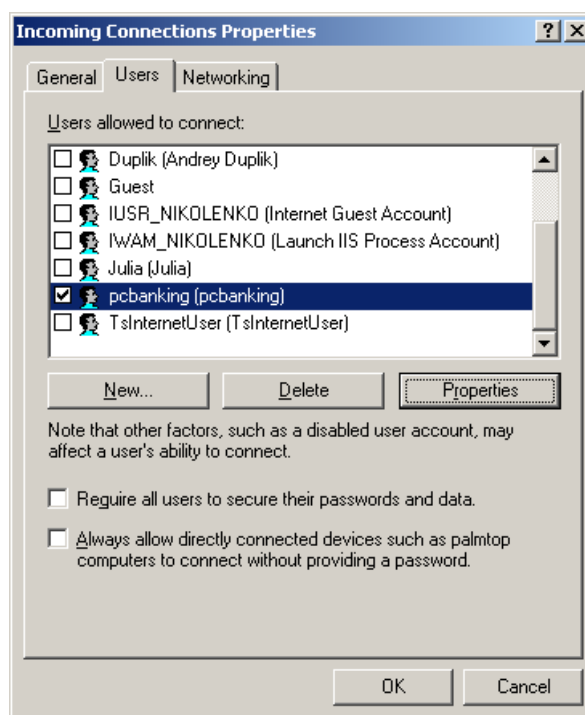
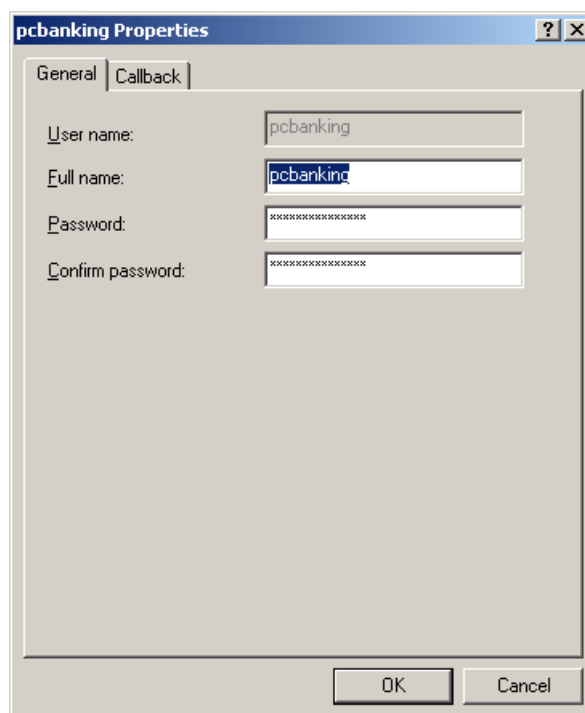


Рис. 1.20. Добавленная учётная запись в списке пользователей

Рис. 1.21. Вкладка **General** (Общие) окна свойств учётной записи

Дополнительные правила для IP-адресов

На вкладке **Networking** (Сеть) (см. [рис. 1.22](#)) окна **Incoming Connections Properties** осуществляется управление сетевыми протоколами для входящих соединений. В частности, на

этой вкладке настраиваются дополнительные правила распределения IP-адресов для машин клиентов. В случае, если для клиента настроена IP-фильтрация на Сервере Приложения, необходимо, чтобы при установке входящего модемного соединения машине клиента присваивался IP-адрес не из общего диапазона адресов, настроенного на шаге 2 на стр. 11, а тот IP-адрес, который установлен на его машине. Для установки этой опции выполните следующее:

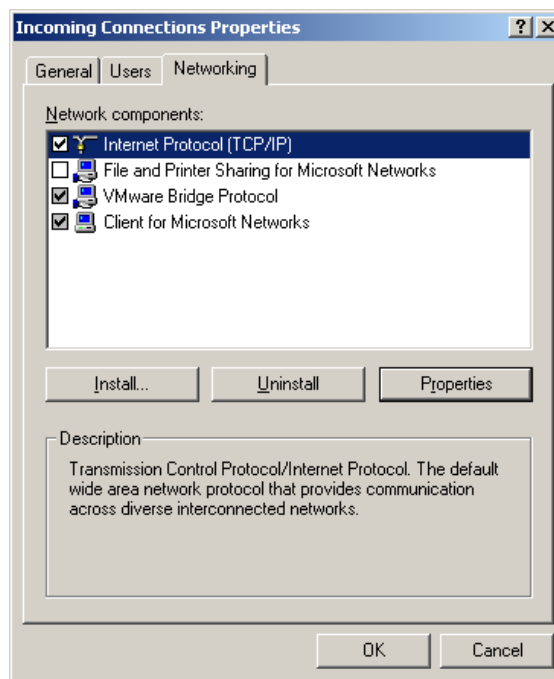


Рис. 1.22. Вкладка **Networking** окна свойств входящих соединений

1. Проверьте в списке присутствие протокола TCP/IP. Если он отсутствует, нажмите на кнопку **Install...**, выберите в появившемся окне — **Protocol** (Протокол), нажмите кнопку **Add...** (Добавить). Из списка протоколов выберите **TCP/IP** и нажмите **Ok**.

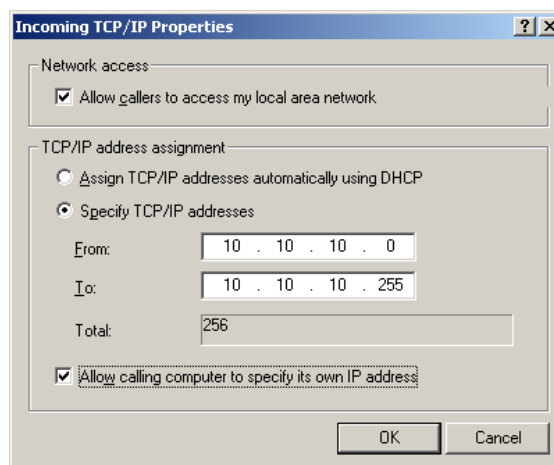


Рис. 1.23. Окно **Incoming TCP/IP Properties**

2. В окне вкладки **Networking** выберите протокол TCP/IP и нажмите на кнопку **Properties** (Свойства). На экране отобразится окно **Incoming TCP/IP Properties** (Свойства протокола TCP/IP для входящих соединений) (рис. 1.23). В нём отметьте поле **Allow calling computer to specify its own IP address** (Разрешить компьютеру указывать свой собственный IP-адрес) и нажмите **Ок**.

О разрешении проблемных ситуаций с IP-адресами смотрите в подразделе [Разрешение конфликтов IP-адресов](#).

Настройка модемного пула под Windows 2003 Server

Мастер настройки сервера

Запустите мастер настройки сервера с помощью меню **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Configure Your Server Wizard**. На экране появится стартовое окно мастера (см. рис. 1.24). Нажмите **Next** (Далее) для перехода к окну предварительной настройки.



Рис. 1.24. Стартовое окно мастера настройки сервера

В следующем окне нажмите **Next** (см. рис. 1.25).

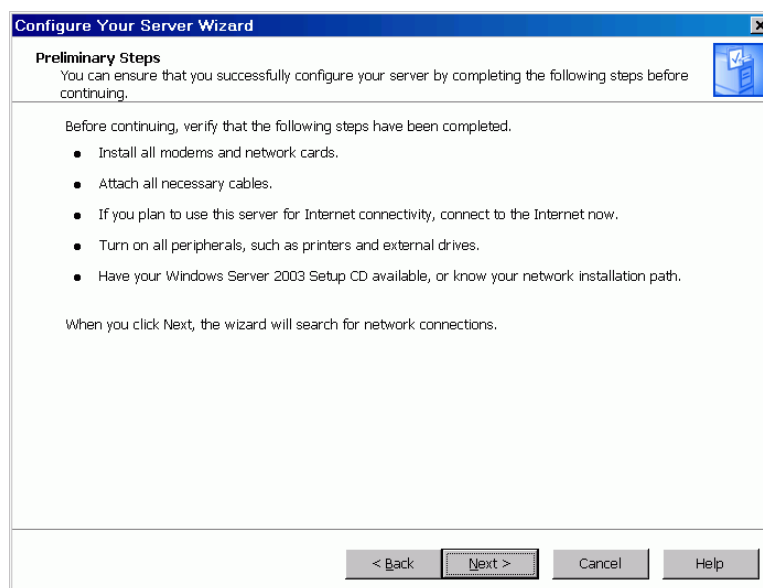


Рис. 1.25. Окно предварительной подготовки мастера настройки сервера

Выбор вида конфигурации

Выберите в списке пункт **Remote access/VPN Server** и нажмите **Next** (см. рис. 1.26).

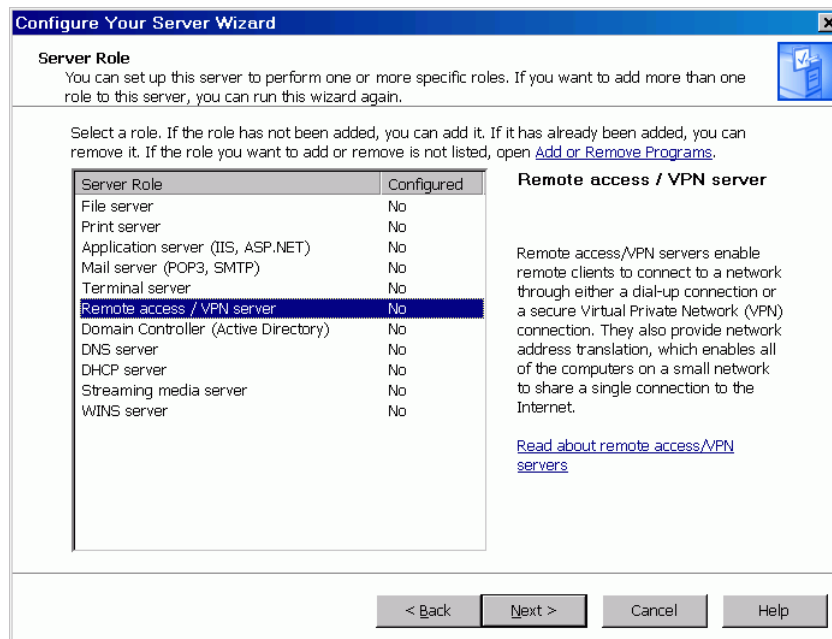


Рис. 1.26. Выбор роли сервера

В следующем окне отображается информация о выбранных ролях. Убедитесь, что роли выбраны правильно (Routing and VPN). Нажмите **Next** (см. рис. 1.27).

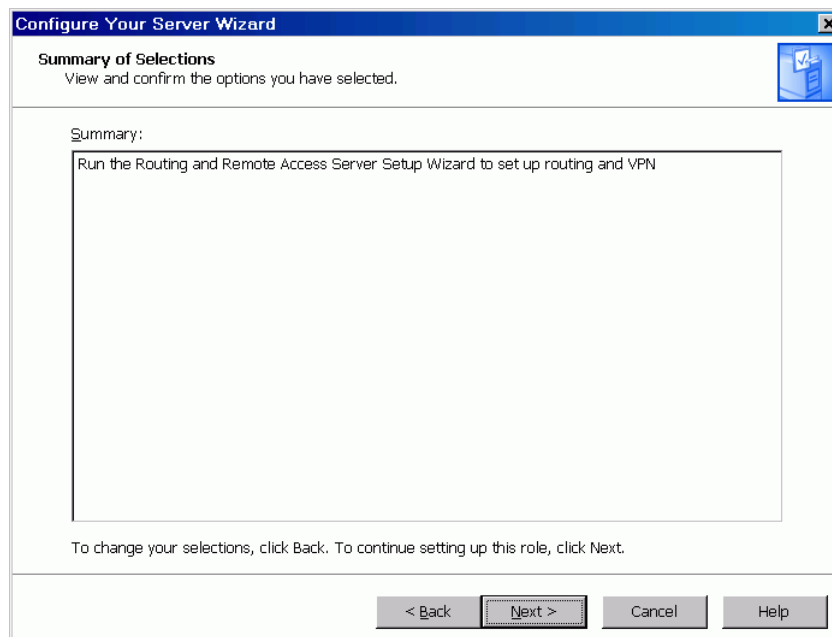


Рис. 1.27. Просмотр списка выбранных ролей сервера

Мастер настройки удалённого доступа

На экране появится стартовое окно мастера настройки сервера удаленного доступа. Нажмите **Next** (см. рис. 1.28).

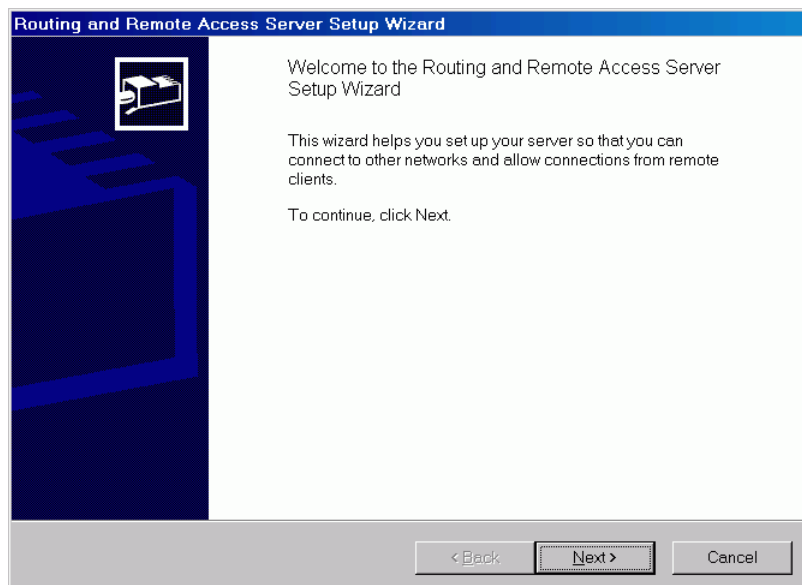


Рис. 1.28. Первое окно мастера настройки сервера удаленного доступа

В следующем окне поставьте флаг в поле **Remote access (dial-up or VPN)**. Нажмите **Next** (см. рис. 1.29).

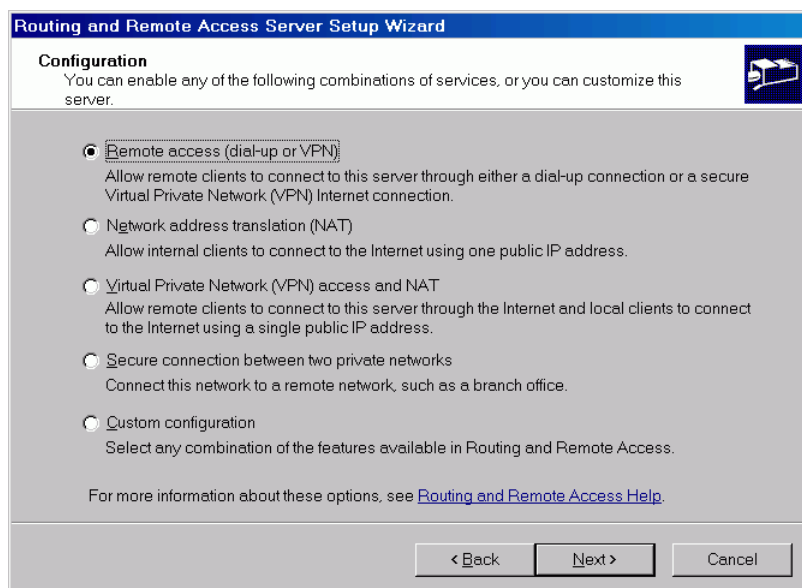


Рис. 1.29. Выбор конфигурации сервера удаленного доступа

Для настройки работы сервера удаленного доступа с модемными соединениями поставьте метку в поле **Dial-up** и нажмите **Next** (см. рис. 1.30).

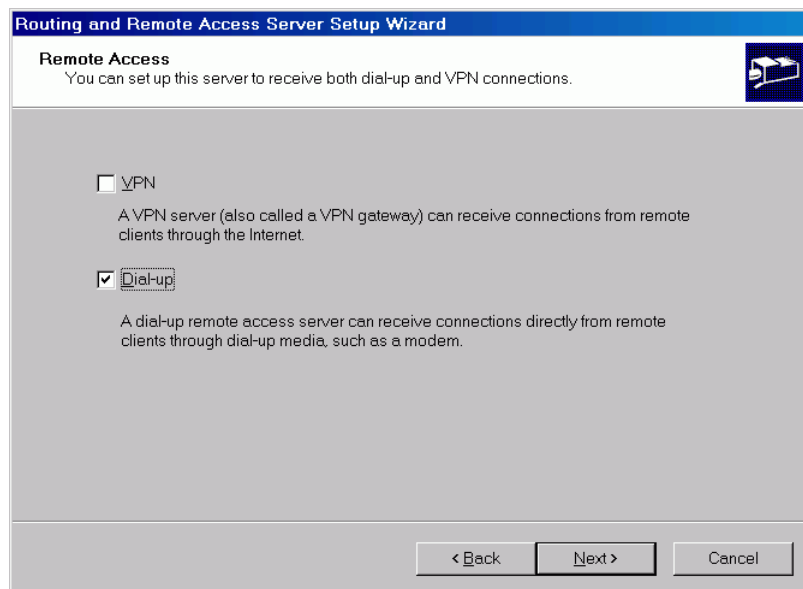


Рис. 1.30. Настройка сервера удаленного доступа для работы с dial-up

Выбор принципа назначения IP-адресов

В следующем окне проставьте флаг в поле **From a specified range of addresses** для задания диапазона IP-адресов, присваиваемых подключающимся клиентам. Нажмите **Next** (см. [рис. 1.31](#)).

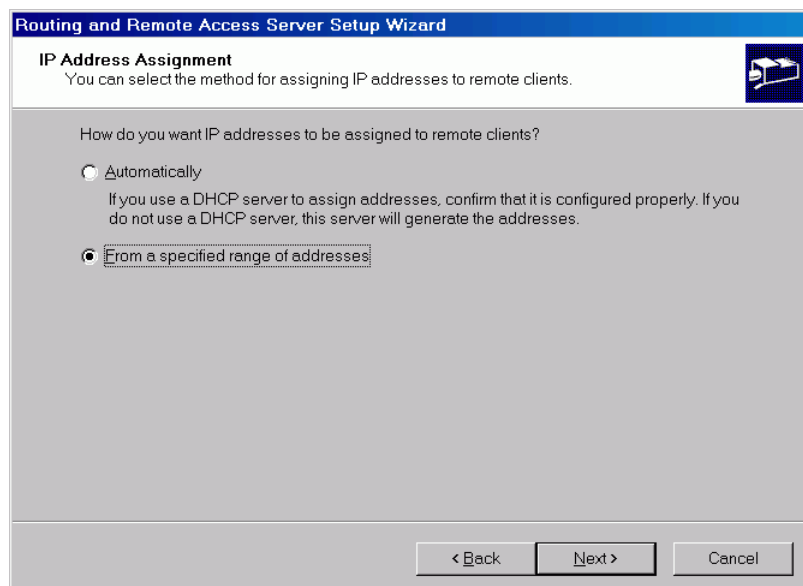


Рис. 1.31. Выбор способа задания IP-адресов

Выделение диапазонов адресов

Внутренняя сеть банка должна быть сконфигурирована таким образом, чтобы Сервер Приложения iBank 2 UA находился в том же сегменте сети, что и компьютер, обеспечивающий связь с модемным пулом. Остальные сегменты внутренней сети банка должны быть закрыты для

выделенных клиентам диапазонов IP-адресов. Из этих соображений вопрос выбора диапазонов IP-адресов должен быть предварительно согласован с системным администратором банка. Общее количество задаваемых IP-адресов должно на 1 превышать количество подключенных линий. Адреса должны выбираться из диапазона, не пересекающегося с диапазонами адресов, реально используемых в сети (т.н. «серые» адреса).

О том, как машине клиента можно присвоить её собственный IP-адрес, отличный от адресов из разрешённого диапазона, смотрите в подразделе [Дополнительные правила для IP-адресов](#).

В следующем окне нажмите кнопку **New** (см. [рис. 1.32](#)). В открывшемся окне **New Address Range** выполните следующие действия:

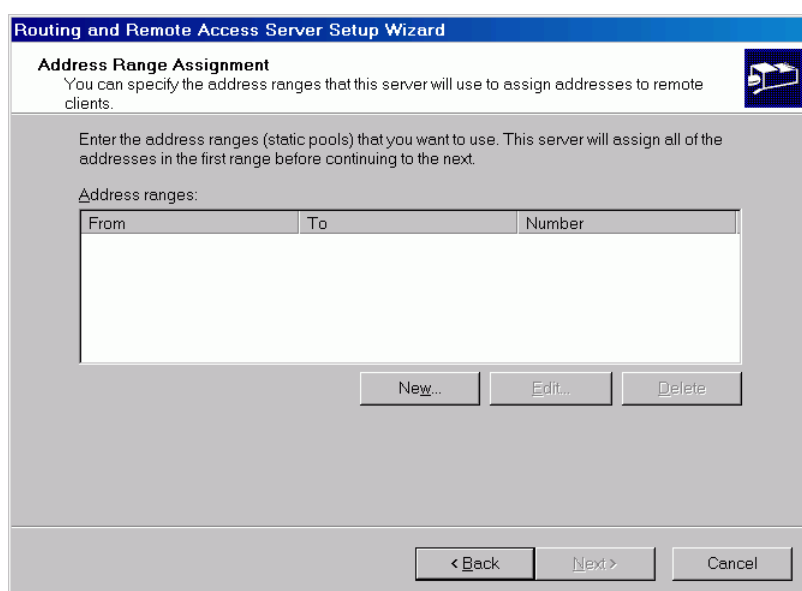


Рис. 1.32. Окно задания диапазона IP-адресов

- В поле **Start IP address** введите начальный IP-адрес диапазона, из которого будут выдаваться адреса клиентам.
- В поле **End IP address** введите конечный IP-адрес диапазона, из которого будут выдаваться адреса клиентам.
- Нажмите кнопку **OK** (см. [рис. 1.33](#)).

При необходимости задать несколько диапазонов IP-адресов повторите данные действия требуемое количество раз. После окончания нажмите кнопку **Next**.

Выбор типа аутентификации клиентов

В следующем окне проставьте флаг в поле **No, use Routing and Remote Access to authenticate connection requests** для запрета использования сервера RADIUS для аутентификации подключений. Нажмите **Next** (см. [рис. 1.34](#)).

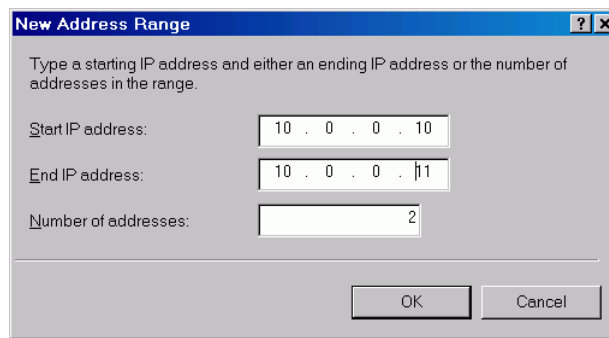


Рис. 1.33. Ввод IP-адресов

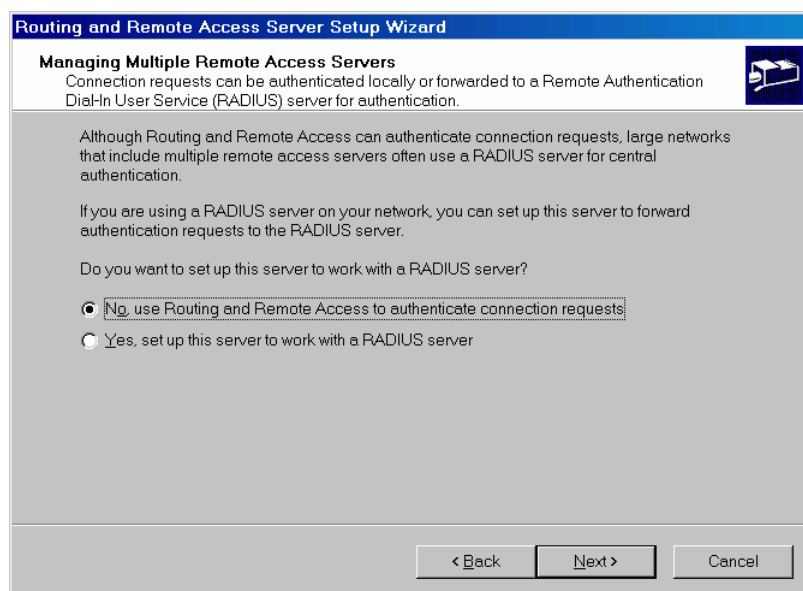


Рис. 1.34. Выбор способа аутентификации подключений

Выход из Мастера настройки удалённого доступа

В последнем окне Мастера настройки удаленного доступа нажмите **Finish** (см. [рис. 1.35](#)).

Для завершения работы мастера настройки сервера нажмите **Finish** (см. [рис. 1.36](#)).

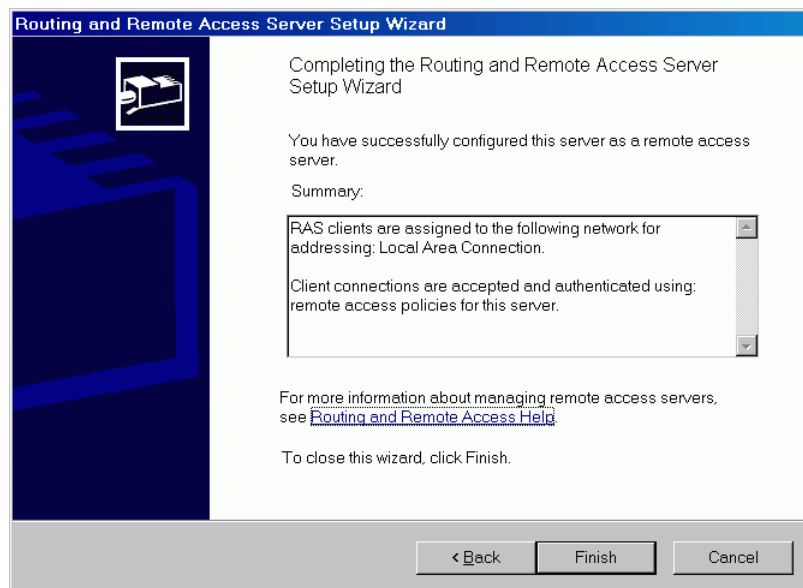


Рис. 1.35. Финальное окно мастера настройки удаленного доступа



Рис. 1.36. Финальное окно мастера настройки сервера

Редактирование настроек удалённого доступа

В случае, если на сервере уже настроен удаленный доступ, необходимо проверить его настройки и, при необходимости, отредактировать. Для этого вызовите управление компьютером **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Computer Management**, выберите в дереве пункт **Routing and Remote Access**, правой кнопкой мыши вызовите контекстное меню и выберите в нем пункт **Properties** (см. [рис. 1.37](#)).

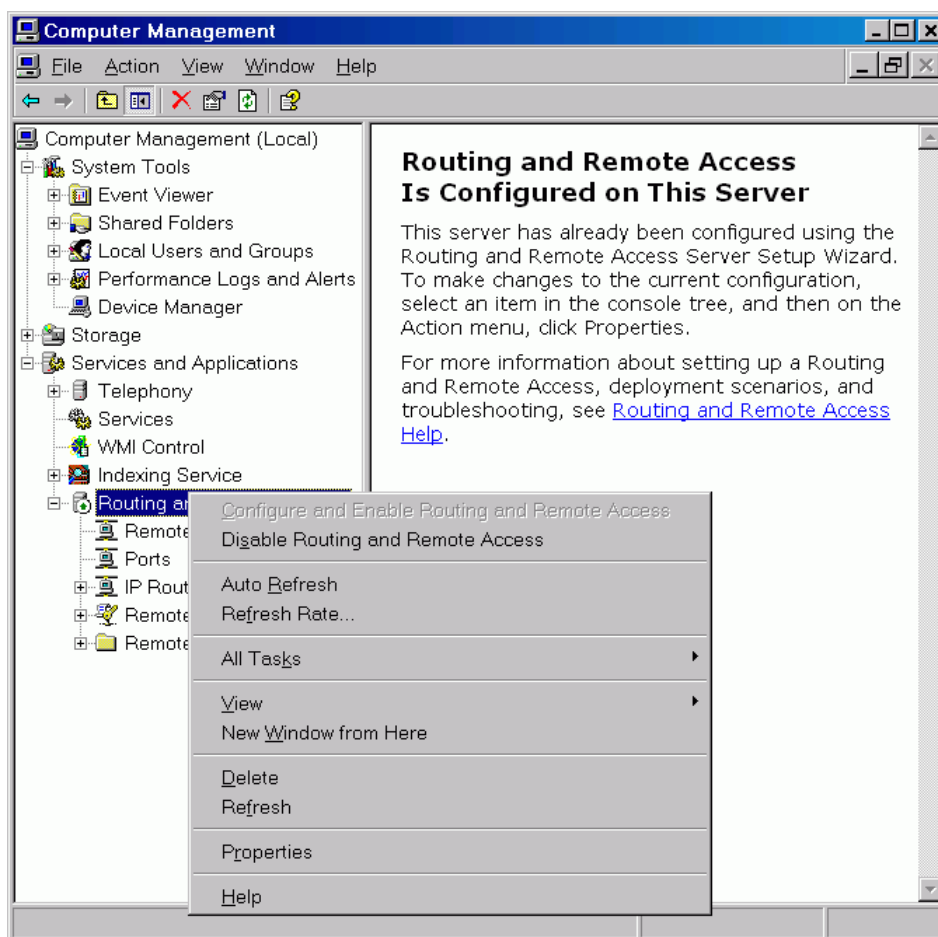


Рис. 1.37. Вызов настроек удаленного доступа

В открывшемся окне настроек удаленного доступа выполните следующие действия:

1. Проверьте наличие галочек в опциях **Enable IP routing** (Разрешить маршрутизацию IP) и **Allow IP-based remote access and demand-dial connections** (Разрешить удаленный доступ на базе TCP/IP и модемные подключения методом Dial-up).
2. В секции **IP address assignment** (Назначение IP-адресов) галочка должна быть поставлена в поле **Static address pool** (Массив статических адресов). В таблице ниже отображается список диапазонов назначенных IP-адресов. При необходимости в него можно добавить новые диапазоны адресов кнопкой **Add** или отредактировать существующие кнопкой **Edit**.
3. Проверьте наличие галочки в опции **Enable broadcast name resolution**.

Настройка входящих модемных соединений

Настройка входящих модемных соединений включает в себя два этапа:

1. Настройку авторизации входящих соединений (обязательный этап);
2. Настройку дополнительных правил распределения IP-адресов (необязательный этап).

О настройке дополнительных правил распределения IP-адресов смотрите в подразделе [Дополнительные правила для IP-адресов](#) по аналогии с ОС Windows 2000 Server.

Настройка авторизации

Для окончательной настройки модемного пула необходимо создать учётную запись пользователя для входящих модемных соединений. Логин и пароль этого пользователя, а также номер телефона, на котором размещается модемный пул, будут использоваться клиентами банка как параметры настройки Dial-up подключения для PC — Банкинга.

Для создания учётной записи пользователя входящих модемных соединений выполните следующие действия:

1. Зайдите в меню **Start** → **Settings** → **Network and Dial-up Connections**;
2. В открывшемся окне дважды щёлкните по значку **Incoming Connections**.

Дальнейшие действия аналогичны рекомендациям для ОС Windows 2000 Server, начиная с [шага 2](#).

Глава 2

Настройка модемного пула под ОС семейства Unix

Принцип работы модемного пула под ОС семейства Unix

Обработка входящего звонка на модемный пул осуществляется следующим образом:

1. Клиент звонит на модемный пул, и модем устанавливает соединение.
2. Процесс `mgetty` определяет тип соединения, запускает процесс `pppd` и завершает свою работу.
3. Процесс `pppd` осуществляет авторизацию пользователя по системной базе и создает IP-интерфейс в соответствии с заданной конфигурацией.
4. IP-интерфейс с использованием маршрутизации с применением `MASQUERADE` обеспечивает работу клиента с системой.
5. В случае разрыва соединения (намеренного или непредвиденного) обслуживающий его процесс `pppd` запускает финальные скрипты и завершает свою работу.
6. `init` порождает процесс `mgetty`, готовый к обслуживанию освободившейся линии, после чего система вновь готова принять входящий звонок.

Таким образом, для успешной организации удаленного доступа необходимо выполнить следующие шаги:

1. Конфигурация ядра с целью настройки поддержки PPP (в версии 2.4 и позднее ядро по умолчанию имеет встроенную поддержку PPP).
2. Установка и настройка `mgetty`.
3. Настройка `pppd`.
4. Настройка маршрутизации с помощью `iptables` и `MASQUERADE`.

Данные шаги подробно описаны ниже.

Конфигурация ядра

Соберите ядро с поддержкой PPP (Point to Point Protocol), поддержкой асинхронных последовательных линий и поддержкой алгоритмов компрессии для PPP соединений. При сборке ядра укажите следующие настройки:

- Секция `Network device support`:

```
CONFIG_PPP=y # PPP (point-to-point protocol) support
CONFIG_PPP_ASYNC=y # PPP support for async serial ports
CONFIG_PPP_DEFLATE=y # PPP Deflate compression
CONFIG_PPP_BSDCOMP=y # PPP BSD-Compress compression
```

- Секция `Networking options`:

```
CONFIG_NETFILTER=y # Network packet filtering (replaces ipchains)
CONFIG_INET=y # TCP/IP networking
```

- Секция `IP: Netfilter Configuration`:

```
CONFIG_IP_NF_CONNTRACK=y # Connection tracking (required for masq/NAT)
CONFIG_IP_NF_IPTABLES=y # IP tables support (required for filtering/masq/NAT)
CONFIG_IP_NF_NAT=y # Full NAT
CONFIG_IP_NF_TARGET_MASQUERADE=y # MASQUERADE target support
```

Установка и настройка mgetty

Для настройки удаленного доступа необходимо скачать программу mgetty версии 1.1.28 (сайт разработчика <http://alpha.greenie.net/mgetty/>). Данная программа служит для обработки модемных соединений.

Распакуйте архив с программой с помощью следующих команд:

```
% tar zxvf ./mgetty1.1.28-Jan10.tar.gz
% cd ./mgetty-1.1.28
```

Скопируйте конфигурационный файл `policy.h`:

```
% cp ./policy.h-dist ./policy.h
```

Внесите в файл `policy.h` следующие изменения:

```
#define CONSOLE "/dev/null"
```

Отредактируйте файл `Makefile`:

```
CFLAGS= -DAUTO_PPP
prefix=
```

Откомпилируйте и установите mgetty следующими командами:

```
% make
% make install
```

Отредактируйте файл `/etc/mgetty+sendfax/login.config`, добавив туда следующую строку:

```
/AutoPPP/ -      a_ppp  /usr/sbin/pppd file /etc/ppp/options
```

Отредактируйте файл `/etc/mgetty+sendfax/mgetty.config`, изменив описание портов аналогично приведенному ниже:

```
port ttyS0
  debug 3
  data-only y
```

Добавьте в файл `/etc/inittab` следующую строку, позволяющую осуществлять запуск `mgetty` с помощью `init`:

```
d0:23:respawn:/sbin/mgetty ttyS0
```

Перезапустите `init` следующей командой:

```
% kill -1 1
```

Настройка pppd

Для того чтобы пользователи модемного пула имели доступ к Серверу Приложения, последний должен находиться в той же подсети, что и компьютер, к которому подсоединён модемный пул. Также необходимо выделить диапазон свободных IP-адресов в этой подсети. Для корректного распределения адресов и авторизации пользователей необходимо настроить демон `pppd`.

- В файле `/etc/ppp/ppp.conf` необходимо указать параметр `enable proxy`, в файле `/etc/rc.conf` необходимо проверить наличие строки:

```
gateway_enable="YES"
```

- Необходимо внести приведенные ниже изменения в файл `/etc/ppp/options` (более подробная информация о данных настройках содержится в документации по `pppd`). В указанном примере `ms-dns` — адрес DNS-сервера, `netmask` — сетевая маска (необязательный параметр), `name modem.bankname.ua` — определение доменного имени сервера, к которому подключён модемный пул, как `modem.bankname.ua`.

```
modem
crtscts
name modem.bankname.ua
-detach
mru 1500
mtu 1500
auth
+pap
ms-dns 192.168.100.1
netmask 255.255.255.0
```

- Для каждого порта создайте файл `/etc/ppp/options.ttySX` (`options.ttyS0`, `options.ttyS1` и т.д.). В нем прописывается комбинация шлюз:адрес. Указанные адреса будут назначаться клиентским машинам при установке PPP-соединения, например:

```
192.168.0.1:192.168.0.10
```

- Создайте в системе пользователя модема, в качестве оболочки указав ему `/usr/sbin/pppd`. В файле `/etc/ppp/ppp-secrets` необходимо определить логин, пароль и параметры IP-соединения для пользователя.

Распределение IP-адресов

При настройке модемного пула необходимо учитывать использование IP-фильтрации на Сервере Приложения. Если для некоторых клиентов настроена IP-фильтрация, то необходимо, чтобы IP-адрес машины такого клиента сохранялся при подключении к банковскому серверу через модемный пул. При использовании машинами клиентов собственных IP-адресов локальная сеть банка должна быть настроена таким образом, чтобы IP-адреса клиентов не конфликтовали с IP-адресами того сегмента сети, в котором расположен Сервер Приложения iBank 2 UA.

Для каждой из двух категорий клиентов необходимо создать и настроить отдельную учётную запись.

Параметры учётной записи для клиентов с собственными IP-адресами

Для того чтобы машины клиентов использовали свои IP-адреса, в файле `/etc/ppp/ppp-secrets` должна быть строка с такими значениями:

`<имя учётной записи> <доменное имя сервера> <пароль учётной записи> *`, где знак `*` — разрешение использовать машинам клиентов свои собственные IP-адреса.

Например:

```
login modem.bankname.ua password *
```

В этом случае учётная запись с логином/паролем `login/password` должна использоваться теми клиентами, которым требуется сохранение их собственного IP-адреса для корректной работы в условиях IP-фильтра на Сервере Приложения.

Разрешение конфликтов IP-адресов

При возникновении конфликтов IP-адресов компьютеров клиентов и компьютеров в сети банка, для обеспечения политики IP-безопасности можно дополнительно настроить параметры IP-фильтрации для отдельных клиентов, чтобы они могли подключаться через модемный пул. В этом случае клиент с конфликтующим IP-адресом сможет успешно работать с Сервером Приложения, используя учётную запись с автоматическим назначением IP-адресов (см. подраздел [Параметры учётной записи для клиентов с назначаемыми IP-адресами](#)).

Параметры учётной записи для клиентов с назначаемыми IP-адресами

Для тех клиентов, которым не требуется использование их собственного IP-адреса, pppd выделяет адреса из диапазонов, настроенных в файл `/etc/ppp/options`.

Чтобы настроить такую учётную запись в файле `/etc/ppp/ppp-secrets` должна быть строка со следующими значениями:

<имя учётной записи> <доменное имя сервера> <пароль учётной записи> <диапазон IP-адресов>

Например:

```
login1 modem.bankname.ua password1 192.168.0.1/50 ,
```

где значение `192.168.0.1/50` означает, что клиентским машинам будут выделяться адреса из диапазона `192.168.0.1 — 192.168.0.50`. Учётная запись с логином/паролем `login1/password1` должна использоваться теми клиентами РС — Банкинга, которым не нужен определённый IP-адрес для соблюдения условий IP-фильтрации.

Если необходимо производить учет и ограничение доступа (`accounting/billing`) пользователей к модемному пулу (например, установить им временной лимит использования пула), можно для этих целей воспользоваться скриптами `/etc/ppp/auth-up`, `/etc/ppp/ip-up`, `/etc/ppp/ip-down`, `/etc/ppp/auth-down`, которые исполняются при установлении и окончании соединения соответственно.

Настройка MASQUERADE

Использование `MASQUERADE` означает, что связь клиентов модемного пула будет осуществляться с применением NAT-ретрансляции IP-адресов. Для клиентов, использующих учётную запись доступа к модемному пулу с сохранением их IP-адреса, маршрутизация с помощью `MASQUERADE` невозможна. Для них должны быть настроены дополнительные правила маршрутизации. Подробное руководство на русском языке для `iptables` доступно по адресу http://ru.gentoo-wiki.com/Подробная_настройка_iptables.

Убедитесь, что в системе установлен `iptables`.

Правило маршрутизации добавляется по такому образцу:

```
iptables -t nat -A POSTROUTING -i <интерфейс_модемного_подключения> ==>
```

```
==> -s <адрес_локальной_сети> -j MASQUERADE , где:
```

- `интерфейс_модемного_подключения` — это название сетевого интерфейса подключения модемного пула, к примеру, `ppp+`;
- `адрес_локальной_сети` — это выделенный для модемного пула диапазон IP-адресов, задаваемый как адрес сети и маска. Для выделенного диапазона в примерах выше это значение для диапазона `192.168.0.1 — 192.168.0.50` должно быть `192.168.0.0/24`.

Например:

```
iptables -t nat -A POSTROUTING -i ppp+ -s 192.168.0.0/24 -j MASQUERADE
```

Это или любое другое правило маршрутизации также может быть выполнена как команда:

```
/usr/sbin/iptables -t nat -A POSTROUTING -i ppp+ -s 192.168.0.0/24 -j MASQUERADE
```

При наличии нескольких диапазонов адресов правило маршрутизации должно быть прописано для каждого из них.

Изменения в маршрутизации сохраняются командой `/etc/init.d/iptables save`. Сам `iptables` необходимо прописать в `rc-update` командой `rc-update add iptables default`.

Для включения маршрутизации пропишите в файле `/etc/sysctl.conf` строку

```
net.ipv4.ip_forward = 1
```

и выполните команду:

```
sysctl -w net.ipv4.ip_forward=1
```

Глава 3

Приложение. Обзор вариантов организации модемного пула

Ниже приводится краткий обзор вариантов организации модемного пула в банке. Описанные решения начинаются с решений для небольших банков и заканчиваются промышленными решениями высочайшего класса. Приводятся рекомендации и описание методологии выбора конкретного решения.

Проектирование мощности модемного пула

При проектировании мощности модемного пула банку необходимо учитывать следующие факторы:

- количество клиентов РС — Банкинга;
- динамику роста количества клиентов РС — Банкинга;
- количество документов в день, проходящих через РС — Банкинг;
- время пребывания клиента на линии;
- допустимое время ожидания свободной линии.

Пример расчета нагрузки на модемный пул

Принимая допустимую вероятность отказа клиенту в соединении равной 1% (из ста клиентов, звонящих на модемный пул в момент пиковой нагрузки, один не сможет дозвониться) и считая время пребывания клиента на линии равным 60 секунд (среднее время синхронизации, необходимое для загрузки 50 документов), получаем зависимость максимального числа клиентов от числа телефонных линий, приведенную в таблице ниже¹:

Количество телефонных линий	Число клиентов
4	50
8	180
16	530
30	1220

¹ Данные получены с использованием таблиц Эрланга.

60	2810
120	6170

Краткое описание теории расчета количества каналов

Расчет количества каналов осуществляется в соответствии с теорией телетрафика. Используются следующие основные понятия:

- Вероятность блокировки (отказа) — средняя вероятность того, что клиент не сможет дозвониться на модемный пул из-за занятости всех линий.
- Нагрузка — показатель занятости линий связи. Нагрузка выражается в Эрлангах (Эрл). 1 Эрл представляет собой единицу нагрузки, используемую для выражения величины нагрузки, требуемой для поддержания занятости одного устройства в течение одного часа. 1 Эрл равен 3600 секунд вызывного времени.
- Среднее время пребывания клиента на линии.

В качестве основного источника используются таблицы Эрланга В. Данные таблицы позволяют определять нагрузку в Эрл по заданному количеству каналов и вероятности блокировки.

Средняя нагрузка вычисляется следующим образом:

$$A = n_{cl} \frac{t}{3600}$$

где A — средняя нагрузка, n_{cl} — количество абонентов, t — среднее время пребывания клиента на линии.

Обзор аппаратных решений

Применение многоканального телефона

Первое и основное требование к модемному пулу — использование многоканального телефона. Использование нескольких одноканальных телефонов возможно в виде исключения для небольших модемных пулов (до 4 телефонных номеров). Однако при этом необходимо четко осознавать недостатки такого решения:

- Использование нескольких телефонных номеров снижает производительность системы;
- С точки зрения клиентов звонок на несколько телефонных номеров (особенно в часы пиковой нагрузки, когда существенная их часть занята) представляется крайне неудобным.

Аналоговые и цифровые телефонные линии

В качестве линии для приема телефонного сигнала можно использовать либо обычные аналоговые линии, либо цифровую телефонную линию стандарта Е1. Цифровая линия Е1 включает в себя 30 телефонных каналов и способна заменить до 30 обычных аналоговых линий. С точки зрения простоты архитектуры и надежности модемного пула линия Е1 является предпочтительной. Поэтому аналоговые линии допустимо использовать только в небольших решениях для модемного пула, не предусматривающих существенного расширения системы.

Решения для аналоговых линий

Решение на основе отдельного компьютера и платы MOXA C168H/PCI

В качестве наиболее простого решения для аналоговой телефонной линии можно использовать отдельный компьютер с установленной специализированной платой MOXA C168H/PCI (производитель — MOXA Technologies Inc.). Это 8-портовая асинхронная плата, предназначенная для небольших систем. Данная плата имеет восемь COM-портов (RS-232) для подключения внешних модемов. В состав данной конфигурации входят:

- Компьютер (минимальная конфигурация Pentium3/RAM 128Mb/HDD 10Gb);
- MOXA C168H/PCI — рекомендованная цена 170 \$;
- 8 внешних аналоговых модемов (ZyXEL, U.S.Robotics Courier, Motorola).

Компьютер может работать под следующими ОС: Windows 2000/XP/2003, Windows NT, Windows 95/98/ME, Windows XP Embedded, DOS, FreeBSD 4.x, Linux 2.2.x (Alpha), Linux Base, SCO Open Server 5, SCO UnixWare 2.1.x, SCO UnixWare 7.

Более современными аналогами платы MOXA C168H/PCI являются следующие продукты:

- 8-портовая плата расширения PCI-X — RS-232: **CP-168EL** — \$ 260;
- 4-портовый концентратор USB — RS-232: **NPort 1240 w/ DK35B** — \$ 230.

Самую актуальную информацию о продукции MOXA в Украине вы можете найти на сайте <http://www.moxa.com.ua/>.

Недостатком данного решения является *низкая надежность* из-за наличия дополнительного компьютера, который может привести к отказу всей системы в случае сбоя. Более предпочтительными являются системы, в которых прием цифрового сигнала, его обработку и дальнейшую передачу осуществляет единое специализированное устройство.

Решение на основе маршрутизатора CISCO 2511

Данный маршрутизатор способен принимать сигнал до 16 внешних модемов. Возможно использование как отдельных модемов, так и единого сервера доступа. В качестве сервера доступа рекомендуется USR Total Control NETServer 16 i-modem Plus (объединенные в одном устройстве 16 аналоговых модемов). *Основным недостатком* данного варианта является то, что в настоящее время компания Cisco Systems не выпускает маршрутизаторы серии 2500, поэтому в рамках данного решения необходимо будет приобрести поддержанное оборудование. В состав данного решения входят:

- CISCO 2511-CN (поддержанный) — рекомендованная цена от 3 300 \$;
- 16 внешних аналоговых модемов (ZyXEL, U.S.Robotics Courier, Motorola);
- USR Total Control NETServer 16 i-modem Plus — 1 200 \$.

Решение на основе маршрутизатора CISCO 2611XM

Наиболее передовое решение на основе обычных аналоговых линий — это использование маршрутизатора CISCO 2611XM со встроенным модулем NM-16AM-V2. Модуль NM-16AM-V2 имеет 16 встроенных аналоговых модемов, к которым подключаются телефонные линии. Стоимость такого решения:

- CISCO 2611XM — рекомендованная цена 1 625 \$;
- NM-16AM-V2 — рекомендованная цена 3 400 \$.

Итого: 5 025 \$.

Решения для цифровых линий E1

Промышленные решения предполагают использование цифровой телефонной линии E1. Данная линия объединяет 30 каналов с пропускной способностью 2 мегабита. Таким образом, одна телефонная линия E1 способна заменить до 30 обычных аналоговых линий. При использовании такого решения можно оказывать услуги работы в РС – Банкинге максимальному числу клиентов.

Решение на основе маршрутизатора CISCO и модуля NM-HDV-2E1-60

Простейший вариант такого решения — использование уже имеющегося в банке маршрутизатора CISCO (серии 2600XM и выше). Для обработки сигнала, поступившего по телефонной линии, используется модуль CISCO NM-HDV-2E1-60. Данный модуль имеет 2 порта E1 и поддерживает 60 каналов. Стоимость такого решения:

- NM-HDV-2E1-60 — ориентировочная цена 8 500 \$.

Решение на основе универсального сервера доступа серии CISCO AS53XX

Наиболее профессиональное и высококлассное решение — использование единого пакета оборудования, специально предназначенного для организации модемного пула. Таким решением является универсальный сервер доступа CISCO AS5350. Сервер доступа CISCO AS5350 имеет 2, 4 или 8 портов E1 и может включать до 210 встроенных модемов для обработки сигнала. Стоимость такого сервера:

- Cisco AS5300-8E1-240-AC — ориентировочная цена 4 200 \$;
- CISCO AS5350-2E1-60 — ориентировочная цена 9 165 \$;
- CISCO AS5350-4E1-120 — ориентировочная цена 16 965 \$;
- CISCO AS5350-8E1-210 — ориентировочная цена 27 300 \$.

Универсальное решение масштаба банка

Универсальный сервер доступа и медиа-шлюз Cisco AS5350XM является более усовершенствованным вариантом описанного выше Cisco AS5350. На базе этого устройства банк может организовать не только высокопроизводительный и надёжный модемный пул, но и такие сервисы общепанковского масштаба как:

- Call-центр;

- Интерактивный автоответчик (IVR);
- IP-телефонию;
- Корпоративную VPN.

При ориентировочной цене 8Е1-портовой конфигурации Cisco AS5350ХМ в 28 300 \$ применение единого внутрибанковского решения многоцелевого применения позволит снизить общую стоимость ИТ-инфраструктуры банка.

Более мощным решением, включающим в себя ряд опциональных модулей, является Cisco AS5850 — 24 порта Е1.

Глава 4

Источники дополнительной информации

С дополнительной информацией по данной тематике можно ознакомиться в документах:

- *Общая информация о системе iBank 2 UA*
- *Механизмы безопасности в системе iBank 2 UA*
- *Установка системы iBank 2 UA под ОС Windows/Unix*
- *Файловая структура Сервера Приложения iBank 2 UA*

Примечание: _____

Со всеми предложениями и пожеланиями по документации обращайтесь по электронному адресу support@bifit.com.ua
