Настройка RRAS – сервер

Потребуется два компьютера(*Computerl и Computer2)* с операционной системой Windows 2003, они должны будут подсоединены к разным телефонным линиям

Создание сервера доступа по телефонной линии с помощью Мастера настройки сервера маршрутизации и удаленного доступа

Вы войдете в систему Computerl и удалите в консоли Маршрутизация и удаленный дос-туп предыдущую конфигурацию. Затем запустите Мастер настройки сервера маршрути-зации и удаленного доступа и настроите на Computerl удаленный доступ по телефонной линии.

1. На Computerl войдите в систему как Администратор (Administrator) в домене Domainl

2. В меню Пуск (Start) выберите Администрирование (Administrative Tools)\Марmрутизация и удаленный доступ (Routing And Remote Access). Откроется консоль Маршру-тизация и удаленный доступ.

3. В дереве консоли щелкните узел COMPUTERl (Local) правой кнопкой и выберите Отключить маршрутизацию и удаленный доступ (Disable Routing And Remote Access).
Если эта команда недоступна, перейдите к п. 4.
Появится информационное окно с предложением подтвердить отключение маршрутизатора. Щелкните Да (Yes). Появится сообщение об остановке службы Маршрути-зация и удаленный доступ.

4. В дереве консоли щелкните узел COMPUTER1 (Local) правой кнопкой и выберите Настроить и включить маршрутизацию и удаленный доступ (Configure and Enable Routing And Remote Access).

5. В окне Мастер настройки сервера маршрутизации и удаленного доступа щелкните Далее (Next).

6. На странице Конфигурация (Configuration) примите вариант по умолчанию Удаленный доступ (VPN или модем) [Remote Access (Dial-Up or VPN)] и щелкните Далее.

7. На странице Удаленный доступ (Remote Access) установите флажок Удаленный доступ (Dial-Up) и щелкните Далее.

8. На странице Выбор сети (Network Selection) выберите вариант по умолчанию Подключение по локальной сети (Local Area Connection) (IP-адрес 192.168.0.1) и щелкните Далее.

.

9. На странице Назначение IP-адресов (IP Address Assignment) выберите вариант по умолчанию Автоматически (Automatically) и щелкните Далее.

10. На странице Управление несколькими серверам и удаленного доступа (Managing Multiple Remote Access Servers) выберите вариант по умолчанию Нет, использовать маршрутизацию и удаленный доступ... (No, use Routing a n d Remote Access...) и щелкните Далее

.

11 На странице Завершение мастера сервера маршрутизации и удаленного доступа (Completing the Routing and Remote Access Server Setup Wizard) щелкните Готово (Finish).

12. Если появится сообщение о необходимости настроить свойства Агента DHCP-ретрансляции (DHCP Relay Agent), щелкните ОК. Появится окно с сообщением об успешном запуске службы Маршрутизация и удаленный доступ, а в

окне консоли Маршрутизация и удаленный доступ под узлом сервера появится структура новой конфигурации.

13. Выйдите из системы Computer 1.

Настройка телефонного подключения к удаленному серверу

Вы настроите телефонное подключение на Computer2. Проследите, чтобы Computerl и Computer2 физически подключались к разным телефонным линиям.

1. На Computer2 войдите в систему как Администратор (Administrator) в домене Domain 1.

2. Откроите окно Сетевые подключения (Network Connections).

3. В меню Файл (File) щелкните Новое подключение (New Connection).

4. В окне Мастер новых подключений (New Connection Wizard) щелкните Далее (Next).

5. На странице Тип сетевого подключения (Network Connection Type) выберите вариант Подключить к сети на рабочем месте (Connect to the network at my workplace) и щелк-ните Далее

.

6. На странице Сетевое подключение (Network Connection) оставьте вариант по умолча-нию Подключение удаленного доступа (Dial-Up Connection) и щелкните Далее.

7. На странице Имя подключения (Connection Name) в поле Организация (Company Name) введите MyCompany и щелкните Далее.

8. На странице Введите номер телефона (Phone Number to Dial) в поле Номер телефона (Phone Number) введите номер телефонной линии, к которой подключен Computerl и щелкните Далее.

9. На странице Доступность подключения (Connection Availability) оставьте вариант по умолчанию — Для всех пользователей (Anyone's Use) и щелкните Далее. Появится страница Завершение работы мастера новых подключений (Completing The New Connection Wizard) .

10. На странице Завершение работы мастера новых подключений (Completing The New Connection Wizard) щелкните Готово(Finish).Откроется окно Подключение к My Company (Connect My Company).

11. Щелкните кнопку Свойства (Properties). Отроется окно MyCompany Свойства (MyCompany Properties).

12. На вкладке Параметры (Options) установите флажок Включать домен входа в Windows (Include Windows Logon Domain).

13. Обратите внимание, что на вкладке Безопасность (Security) по умолчанию выбран вариант Небезопасный пароль (Allow Unsecured Password).

14. Установите переключатель Дополнительные (выборочные параметры) [Advanced (Custom Settings)] и щелкните кнопку Параметры (Settings). Появится окно Дополни-тельные параметры безопасности (Advanced Security Settings). Обратите внимание, что включены протоколы PAP , SPAP , CHAP, MS-CHAP и MS-CHAP v2.

15.Установите переключатель Протокол расширенной проверки подлинности (EAP) [Use Extensible Authentication Protocol (EAP)]. В ставшем доступным поле со списком

вы-бран вариант Смарт-карта или иной сертификат (шифрование включено) [Smart Card Or Other Certificate (Encryption Enabled)]. Он соответствует протоколу EAP-TLS. При-менение смарт-карт по EAP-TLS — это самая безопасная форма аутентификации в сетях Windows Server 2003.

16. Раскройте список Протокол расширенной проверки подлинности (EAP). Обратите внимание, что в списке есть еще только один протокол EAP — MDS-отклик (MD5-Challenge). Это разновидность CHAP, в котором для передачи информации исполь-зуются EAP-сообщения. Он задействован во всех реализациях EAP, но уровень обе-спечиваемой им безопасности считается невысоким.

17. Закройте список и щелкните Отмена (Cancel), чтобы закрыть окно Дополнительные параметры безопасности.

18. На вкладке Безопасность выберите вариант Обычные (рекомендуемые параметры) [Typical (Recommended Settings)]. В списке способе проверки выбран вариант Небезопасный пароль.

19. Щелкните ОК, чтобы закрыть окно MyCompany Свойства.

20.Щелкните Отмена, чтобы закрыть окно Подключение к MyCompany.

21. Выйдите из системы Computer2.

Развертывание системы удаленного доступа

Вы создадите учетную запись пользователя Userl и введете ее в новую глобальную груп-пу безопасности Telecommuters.

1. На Computer! войдите в систему как Администратор (Administrator) в домене

Domainl.

2. В меню Пуск (Start)\Администрирование (Administrative Tools) щелкните Active Directory — пользователи и компьютеры (Active Directory Users a n d Computers). Откро-ется окно консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers).

3. В дереве консоли Active Directory — пользователи и компьютеры щелкните папку Users правой кнопкой и выберите Создать (New)\Пользователь (User).

4. В открывшемся окне Новый объект - Пользователь (New Object - User) в поле Полное имя (Full Name) введите user1.

5. В поле Имя входа пользователя (User Logon Name) введите user 1 .

6. Щелкните Далее (Next). В окне Новый объект - Пользователь появится новый набор параметров.

7. В полях Пароль (Password) и Подтверждение (Confirm Password) введите пароль для учетной записи User1.

8. Снимите флажок Требовать смену пароля при следующем входе в систему (User must change password at next logon).

9. Щелкните Далее (Next), а затем — Готово (Finish).

10. На Computerl из командной строки исполните: net group telecommuters /add /domain
Эта команда создаст в домене глобальную группу безопасности Telecommuters.

Выполните команду net group telecommuters userl /add /domain. Она добавит в группу Telecommuters учетную запись Userl.

11. Когда в дереве консоли Active Directory — пользователи и компьютеры выбрана папка Users, щелкните правой кнопкой свободное место в правой панели и в контекстном меню выберите Обновить (Refresh). В правой панели появится значок новой группы безопасности Telecommuters.

12. В правой панели консоли Active Directory — пользователи и компьютеры двойным щелчком значка Userl откройте окно Userl - свойства (Userl Properties).

13. Перейдите на-вкладку Входящие звонки (Dial-In). В группе Разрешение на удаленный доступ (Remote Access Permissions) доступны только два параметра: Разрешить доступ (Allow Access) и Запретить доступ (Deny Access). Заметьте, что по умолчанию доступ запрещен. Щелкните ОК.

14. В дереве консоли Active Directory — пользователи и компьютеры щелкните значок domain 1.local правой кнопкой и выберите Изменение режима работы домена (Raise Domain Functional Level). Откроется одноименное окно.

15. В списке Выберите режим работы домена (Select an available domain functional level) выберите Windows Server 2003.

16. Щелкните Изменить (Raise). Появится предупреждение о необратимости операции. Щелкните ОК. Появится сообщение об успешном завершении операции.

17. Щелкните ОК и перезапустите Computerl.

18. После перезапуска Computerl вновь войдите в Domainl как Администратор (Administrator).

19. Откройте консоль Active Directory — пользователи и компьютеры.

20. Откройте окно свойств Userl и перейдите на вкладку Входящие звонки (Dial-In). В группе Разрешение на удаленный доступ (Remote Access Permissions) теперь доступен и третий вариант Управление на основе политики удаленного доступа (Control Access Through Remote Access Policy), который и выбран по умолчанию.

21. Закройте консоль Active Directory — пользователи и компьютеры.

Создание политики удаленного доступа для учетной записи Telecommuter

Вы создадите политику удаленного доступа Telecommuters и изучите параметры этой политики.

1. На Computerl войдите в систему как Администратор (Administrator) в домене Domain 1.

2. В дереве консоли Маршрутизация и удаленный доступ (Routing and Remote Access) щелкните узел Политика удаленного доступа (Remote Access Policies) правой кнопкой и выберите Создать политику удаленного доступа (New Remote Access Policy).

3. В окне Мастер создания политики удаленного доступа (New Remote Access Policy Wizard) щелкните Далее (Next).

4. На странице Метод настройки политики (Policy Configuration Method) в поле Имя политики (Policy Name) введите Telecommuters и щелкните Далее.

5. На странице Метод доступа (Access Method) выберите вариант Удаленный доступ (че-рез телефонную сеть) (Dial-Up) и щелкните Далее.

6. На странице Пользователь и л и групп а доступа (User Or Group Access) оставьте выбранный по умолчанию вариант разрешения группы (Group) и щелкните кнопку Добавить (Add).

7. В окне Выбор: « Группы » (Select Groups) в поле Введите имена выбираемых объектов (Enter object names to select) введите telecommuters и щелкните ОК. В поле Имя группы (Group Name) появится запись DOMAIN1\telecommuters. Щелкните Далее.

8. На странице Методы проверки подлинности (Authentication Methods) оставьте выбран-ный по умолчанию протокол MS-CHAPv2 и щелкните Далее.

9. Параметры на странице Уровень шифрования , указанный в политике (Policy Encryption Level) позволяют шифровать только данные подключения, но не пароль. Уровни про-стого, сильного и стойкого шифрования выбраны по умолчанию. Поскольку MS-CHAP v2 поддерживает шифрование по протоколу MPPE, этими параметрами га-рантируется шифрование данных, пересылаемых с Computer2 через подключение MyCompany. Щелкните Далее, оставив параметры по умолчанию.

10. На странице Завершение мастера создания политики удаленного доступа (Completing Th e New Remote Access Policy Wizard) щелкните Готово (Finish). В правой панели консоли Маршрутизация и удаленный доступ видно, что при выборе узла Политики удаленного доступа (Remote Access Policies) первой в списке отобража-ется политика Telecommuters.

11. Дважды щелкните в правой панели значок политики Telecommuters. В открывшемся окне Свойства: Telecommuters (Telecommuters Properties) проверьте

параметры, отобра-жаемые в этом окне. Заметьте, что первое условие политики соответствует всем теле-фонным подключениям, а второе — глобальной группе безопасности DOMAINl\tele-commuters. Обратите также внимание, что выбран переключатель Предоставить право удаленного доступа (Grant Remote Access Permission).

12. Щелкните кнопку Изменить профиль (Edit Profile). В открывшемся окне Изменение
профиля коммутируемых подключений (Edit Dial-In Profile) изучите параметры, определенные на шести вкладках этого окна. Оставьте их без изменений.

13. Щелчком кнопки Отмена (Cancel) закройте окно Изменение профиля коммутируемых подключений.

14. Щелчком кнопки Отмена закройте окно Свойства: Telecommuters.

15. Выйдите из системы Computerl.

Тестирование настройки удаленного доступа

Вы установите телефонное подключение под учетной записью Userl к Computer1 с компьютера Computer2. У каждого компьютера должна быть отдельная телефонная линия. Перед выполнением упражнения подключите компьютеры к соответствующим телефон-ным линиям.

Примечание На время выполнения упражнения отключите локальный кабель, соединяющий оба компьютера, чтобы убедиться, что подключение выполняется по телефон-ной линии.

1. На компьютере Computer2 нажмите Ctrl+Alt+Del, чтобы открыть окно Вход в Windows (Log On To Windows).

2. Установите флажок С использованием удаленного доступа (Log On Using Dial-Up Connection).

3. В поле Пользователь (User Name) введите userl.

4. В поле Пароль (Password) наберите пароль, установленный для пользователя Userl.

5. В списке Вход в (Log On To) выберите DOMAIN! и щелкните ОК. Откроется окно Сетевые подключения (Network Connections).

6. В списке Выберите сетевое подключение (Choose a Network Connection) выберите MyCompany , а затем щелкните Подключит ь (Connect).
Откроется окно Подключение к MyCompany (Connect MyCompany). Поле Пользова-тель (User Name) уже содержит имя userl, поле Пароль (Password)— скрытый па-роль, а поле Домен (Domain) — имя домена DOMAIN 1.

7. Щелкните кнопку Вызов (Dial). В окне Установка связи с MyCompany (Connecting MyCompany) отображается состояние подключения. По завершении набора номера прозвучат два сигнала, и на вызов отве-тит служба Маршрутизация и удаленный доступ (Routing and Remote Access) компьюте-ра Computerl. Проверяется имя пользователя и пароль, после чего компьютер реги-стрируется в сети. Затем окно Установка связи с MyCompany (Connecting MyCompany) закрывается и выполняется вход в домен с соответствующими реквизитами.

8. По завершении операции входа в домен откройте Microsoft Internet Explorer. Не обращайте внимания на получаемые сообщения и предупреждения.

9. В адресной строке введите \\computer1. domain 1. local и нажмите Enter. В окне

браузера появится список общедоступных ресурсов Computerl, подтверждая, что Userl успешно подключился к Computerl по телефонной линии.

10. Закройте браузер и выйдите из системы Computer2.