

**Министерство образования и науки Российской Федерации  
Федеральное агентство по образованию**

**Московский Государственный Технический Университет им. Н.Э.  
Баумана**

**Факультет «Информатика и системы управления»  
Кафедра «Компьютерные системы и сети»**

Сурков Л.В.

Методические указания к лабораторной работе  
по дисциплине  
Корпоративные сети

Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003

ВВЕДЕНИЕ .....	3
ЭЛЕМЕНТЫ VPN-СОЕДИНЕНИЯ .....	4
VPN-соединения .....	4
VPN-соединение удаленного доступа .....	5
VPN-соединение между маршрутизаторами .....	5
VPN-соединения через Интернет или интрасети .....	5
VPN-соединения через Интернет .....	5
VPN-соединения через интрасети .....	6
Комбинированные VPN-соединения через Интернет и интрасети .....	8
УПРАВЛЕНИЕ ВИРТУАЛЬНЫМИ ЧАСТНЫМИ СЕТЯМИ .....	9
ТУННЕЛЬНЫЕ ПРОТОКОЛЫ .....	10
PPTP .....	10
Поддержание туннеля с помощью управляющего PPTP-соединения .....	10
Туннелирование данных средствами PPTP .....	11
PPTP-пакеты и сетевая архитектура Windows 2008 .....	12
L2TP .....	13
Поддержание туннеля с помощью управляющих L2TP-сообщений .....	14
Туннелирование данных средствами L2TP .....	15
Пакеты L2TP поверх IPSec и сетевая архитектура Windows 2008 .....	17
ЗАЩИТА ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ .....	18
АДРЕСАЦИЯ И МАРШРУТИЗАЦИЯ ПРИ ИСПОЛЬЗОВАНИИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ .....	20
VPN-соединения удаленного доступа .....	20
VPN-соединения между маршрутизаторами .....	24
Временные и постоянные VPN-соединения между маршрутизаторами .....	25
VPN-соединения через подключение удаленного доступа с ISP .....	25
Статическая и динамическая маршрутизация .....	27
Аутентификация на основе общего ключа при использовании L2TP поверх IPSec для VPN-соединений между маршрутизаторами .....	27
ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ И БРАНДМАУЭРЫ .....	30
Конфигурации VPN-сервера и брандмауэра .....	30
VPN-сервер перед брандмауэром .....	30
VPN-сервер за брандмауэром .....	31
ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ И NAT .....	34
PPTP-трафик .....	34
Трафик L2TP поверх IPSec .....	34
СКВОЗНЫЕ VPN-СОЕДИНЕНИЯ .....	36
Конфигурирование VPN-сервера компании А .....	37
Конфигурирование VPN-сервера компании В .....	37
Настройка компьютера VPN-клиента на использование сквозной VPN .....	38
ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ ПРОБЛЕМ .....	40
Наиболее распространенные проблемы с VPN .....	40
Средства диагностики .....	44
ПРАКТИЧЕСКАЯ ЧАСТЬ .....	46
ЛАВ 1. VPN-соединение удаленного доступа .....	46
ЛАВ 2.1 Установка маршрута по умолчанию .....	53
ЛАВ 2.2 Установка маршрута по умолчанию .....	56
ЛАВ 3. VPN-Соединение между маршрутизаторами по требованию .....	71
ЛАВ 4. Сквозное VPN-соединение .....	88

## Введение

Виртуальная частная сеть (virtual private network, VPN) — это расширение частной сети, включающей соединения через общедоступные сети, обычно Интернет. VPN позволяет передавать данные между двумя компьютерами по общедоступным сетям, эмулируя свойства частного канала связи типа «точка-точка». Для эмуляции канала связи «точка-точка» данные инкапсулируются в пакет с заголовком, который содержит информацию о маршрутах, необходимую для пересылки этого пакета в конечную точку по общедоступным сетям. Кроме того, передаваемые данные зашифровываются (можно зашифровать). Канал связи, при использовании которого частные данные инкапсулируются и зашифровываются, называется VPN-соединением. VPN-соединения также позволяют организациям создавать маршрутизируемые подключения к территориально удаленным офисам и другим организациям по общедоступным сетям типа Интернета, в то же время, обеспечивая защиту коммуникационных связей. Маршрутизируемое VPN-соединение (routed VPN connection) через Интернет на логическом уровне обрабатывается как выделенный WAN-канал. Обладая свойствами как удаленных, так и маршрутизируемых соединений, VPN-соединения позволяют организации заменить междугородные выделенные или коммутируемые линии удаленного доступа на локальные выделенные линии или удаленный доступ по коммутируемой линии к местному провайдеру Интернет-услуг (Internet service provider, ISP).

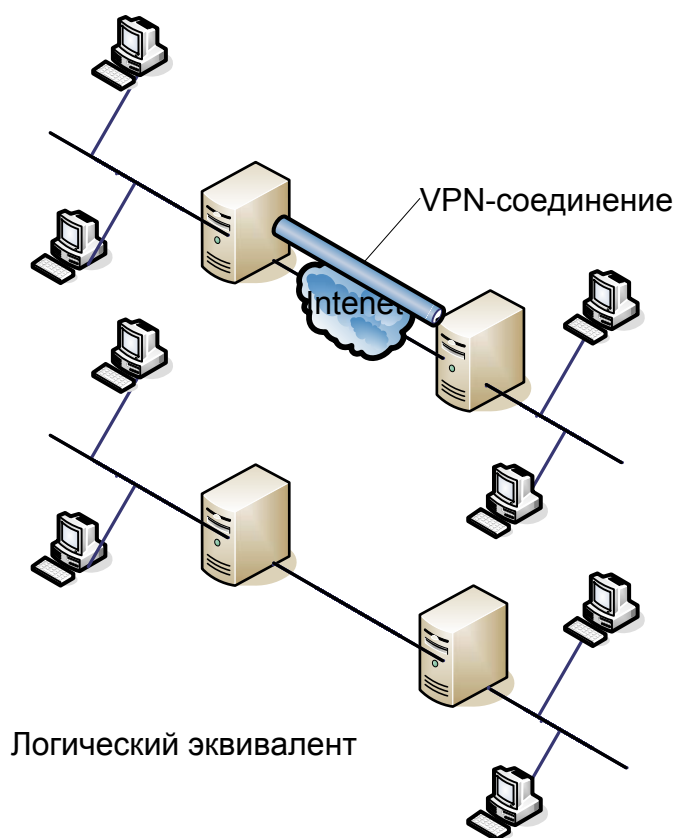


Рисунок 1

## Элементы VPN-соединения

*VPN-сервер.* Компьютер, принимающий запросы на VPN-соединения от VPN-клиентов. VPN-сервер поддерживает VPN-соединения удаленного доступа и VPN-соединения между маршрутизаторами.

*VPN-клиент.* Компьютер, инициирующий VPN-соединение с VPN-сервером. VPN-клиент может быть автономным компьютером, используемым для удаленного доступа, или маршрутизатором, принимающим межмаршрутизаторные VPN-соединения.

*Туннель.* Часть соединения, по которой данные передаются в инкапсулированном виде.

*VPN-соединение.* Часть соединения, по которой данные передаются в зашифрованном виде. В случае безопасных VPN-соединений данные зашифровываются и инкапсулируются на одной и той же части соединения.

*Протоколы туннелирования* (туннелирующие протоколы). Коммуникационные стандарты, применяемые для управления туннелями и инкапсуляции конфиденциальных данных. Windows 2008 включает протоколы туннелирования PPTP и L2TP.

*Туннелированные данные.* Данные, которые обычно передаются по частному каналу связи типа «точка-точка».

*Транзитная межсетевая среда.* Открытая или общедоступная межсетевая среда, через которую передаются инкапсулированные данные. В случае Windows 2008 транзитной всегда является межсетевая IP-среда. Транзитной межсетевой средой может быть Интернет или частная IP-интрасеть.

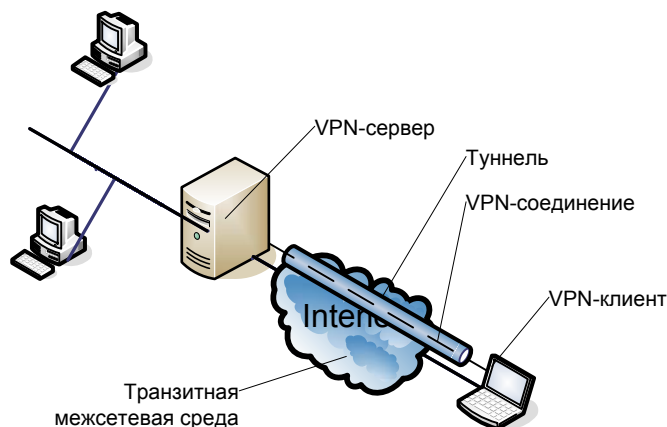


Рисунок 2

## VPN-соединения

Создание VPN-соединения во многом аналогично установлению соединения типа «точка-точка» по коммутируемой линии или при маршрутизации с соединением по требованию. Существует два типа VPN-соединений: VPN-соединение удаленного доступа (remote access VPN connection) и VPN-соединение между маршрутизаторами (router-to-router VPN connection).

## VPN-соединение удаленного доступа

Такое соединение инициируется клиентом удаленного доступа (компьютером индивидуального пользователя), который подключается к частной сети. VPN-сервер предоставляет доступ к своим ресурсам или ко всей сети, с которой он связан. Пакеты, передаваемые по VPN-соединению, генерируются клиентом удаленного доступа.

Клиент удаленного доступа (VPN-клиент) аутентифицируется на сервере удаленного доступа (VPN-сервере), а тот — на клиенте (в случае взаимной аутентификации).

## VPN-соединение между маршрутизаторами

Данное VPN-соединение инициируется маршрутизатором и связывает два фрагмента частной сети. VPN-сервер предоставляет маршрутизируемое соединение с сетью, к которой он подключен. При VPN-соединении между маршрутизаторами пакеты передаются одним из них и обычно генерируются другими компьютерами.

Вызывающий маршрутизатор (VPN-клиент) аутентифицируется на отвечающем (VPN-сервере), а отвечающий — на вызывающем (в случае взаимной аутентификации).

## VPN-соединения через Интернет или интрасети

### VPN-соединения через Интернет

Используя такие соединения, Вы избегаете расходов на междугородную и/или международную телефонную связь и в то же время получаете все преимущества глобальных Интернет-коммуникаций.

#### Удаленный доступ через Интернет

Клиент удаленного доступа — вместо того чтобы связываться с корпоративным или аутсорсинговым сервером доступа в сеть по междугородной связи — звонит местному ISP. Установив физическое соединение с местным ISP, клиент удаленного доступа инициирует VPN-соединение через Интернет с VPN-сервером своей организации. После создания VPN-соединения клиент удаленного доступа может обращаться к ресурсам частной интрасети. Схема удаленного доступа через Интернет показана на рисунке 3.

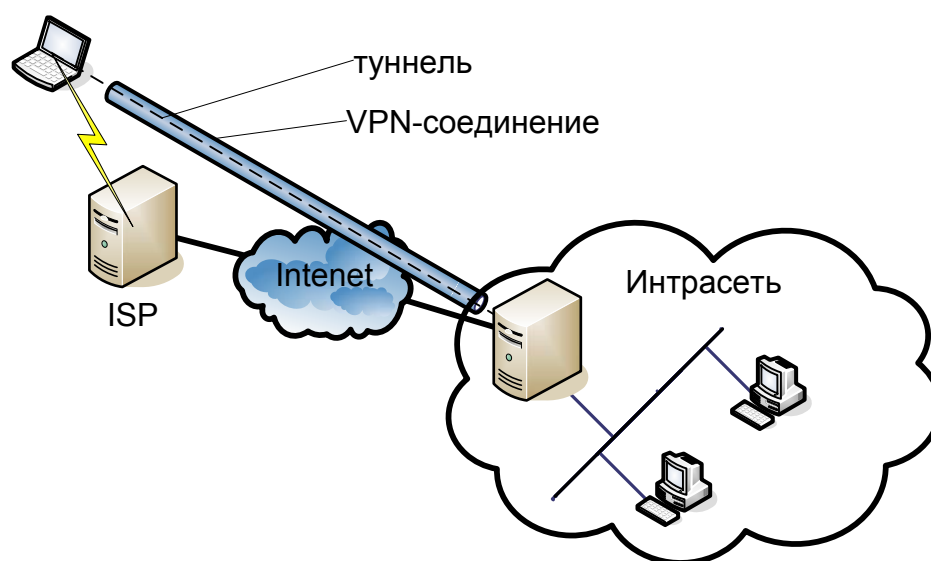


Рисунок 3

### Соединение сетей через Интернет

Когда сети соединяются через Интернет (рисунок 4) один маршрутизатор пересылает пакеты другому по VPN-соединению. С точки зрения маршрутизаторов, VPN действует как каналный уровень сети.

#### **Соединение сетей с использованием выделенных WAN-каналов.**

Маршрутизаторы офисов подключаются не через дорогостоящий междугородный выделенный WAN-канал, а через Интернет с использованием локальных выделенных WAN-каналов связи с местными ISP. VPN-соединение инициируется одним из маршрутизаторов. После соединения маршрутизаторы могут пересылать друг другу любой трафик.

#### **Соединение сетей с использованием коммутируемых WAN-каналов.**

Маршрутизатор филиала — вместо того чтобы связываться с корпоративным или аутсорсинговым сервером доступа в сеть (NAS) по междугородной или международной телефонной линии — звонит местному ISP. Используя соединение с местным ISP, маршрутизатор филиала инициирует межмаршрутизаторное VPN-соединение с корпоративным маршрутизатором-концентратором через Интернет. Корпоративный маршрутизатор-концентратор, выступающий в роли VPN-сервера, должен быть подключен к местному ISP по выделенному WAN-каналу. Подробнее о настройке VPN-соединений, создаваемых на коммутируемом подключении с местным ISP, см. раздел «Адресация и маршрутизация при использовании виртуальных частных сетей» далее в этой главе. Оба офиса можно подключить к Интернету по коммутируемым WAN-каналам, но это реально, только если ISP поддерживает для своих заказчиков маршрутизацию с соединением по требованию; в этом случае ISP, получив IP-дейтаграмму, которую нужно доставить заказчику, вызывает его маршрутизатор. Такой сервис предоставляют лишь отдельные ISP.

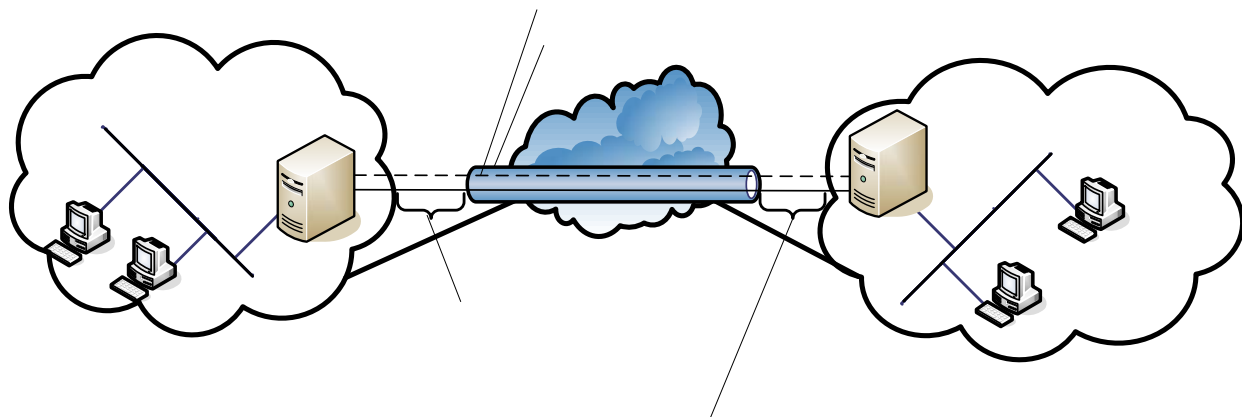


Рисунок 4

### **VPN-соединения через интрасети**

Такое VPN-соединение использует преимущества поддержки IP-соединений в интрасети организации.

#### **Удаленный доступ через интрасеть**

В некоторых интрасетях информация, принадлежащая какому-либо отделу, например отделу кадров, настолько конфиденциальна, что соответствующий сегмент сети физически отключается от остальной части интрасети организации. Хотя этот способ надежно защищает конфиденциальную информацию, он создает проблемы с доступом к ней для пользователей, не подключенных к отделенному сегменту сети. Применение VPN-

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

соединений позволяет физически подключить сегмент сети отдела, имеющего дело с конфиденциальной информацией, к интрасети организации, но отделить его VPN-сервером, который не обеспечивает прямое маршрутизируемое соединение между корпоративной интрасетью и отделенным сегментом сети. Пользователи корпоративной интрасети с соответствующими разрешениями могут устанавливать с VPN-сервером VPN-соединения удаленного доступа и обращаться к защищенным ресурсам. Кроме того, все данные, передаваемые по VPN-соединению, зашифровываются для обеспечения их конфиденциальности. Пользователям, не имеющим прав на установление такого VPN-соединения, отделенный сегмент сети просто не виден.

Схема удаленного доступа через интрасеть показана на рисунке 5.

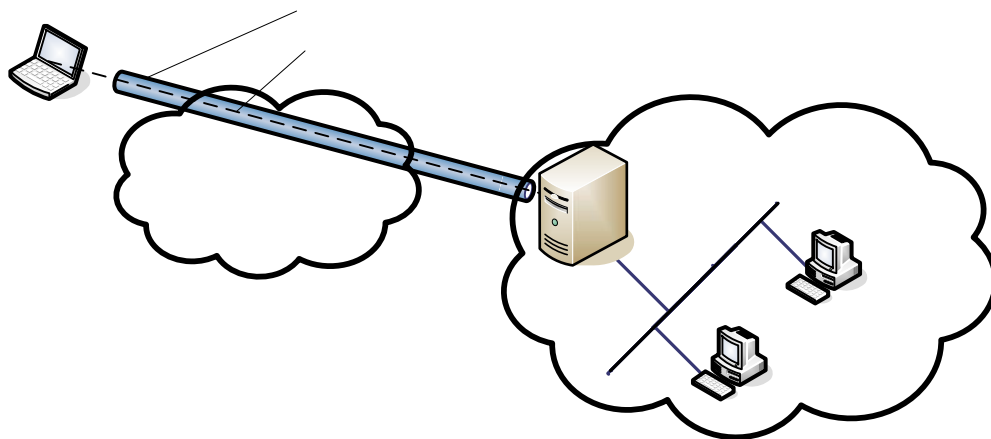


Рисунок 5

### Соединение сетей через интрасеть

Используя VPN-соединение между маршрутизаторами, Вы можете связать две сети через интрасеть. VPN-соединение этого типа очень удобно для организации коммуникационного взаимодействия между двумя отделами, которые находятся в разных географических точках и имеют дело с конфиденциальной информацией, например, бухгалтерия могла обмениваться с отделом кадров сведениями о заработной плате сотрудников организации.

Бухгалтерия и отдел кадров подключаются к общей интрасети через компьютеры, работающие в качестве VPN-клиентов или серверов. Как только VPN-соединение установлено, пользователи любой из двух сетей могут обмениваться конфиденциальной информацией через корпоративную интрасеть.

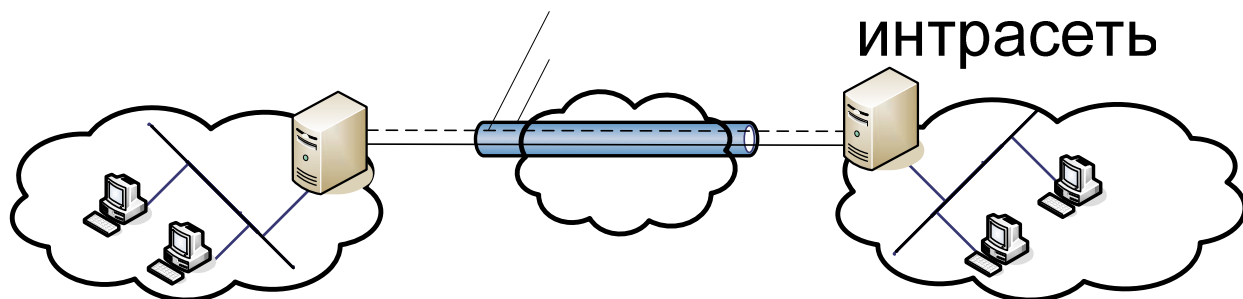


Рисунок 6

## Комбинированные VPN-соединения через Интернет и интрасети

VPN-соединения — гибкое средство для создания защищенных подключений типа «точка-точка». Менее распространены комбинированные VPN-соединения, также называемые сквозными (pass-through VPN connection) (рисунок 7). Такое соединение позволяет удаленному клиенту, подключенному к интрасети одной компании, получить доступ через Интернет к ресурсам интрасети другой компании. В этом варианте VPN-соединение удаленного доступа достигает интрасети назначения через другую интрасеть и Интернет. Подробнее о сквозных VPN-соединениях см. раздел «Сквозные VPN-соединения» далее в этой главе.

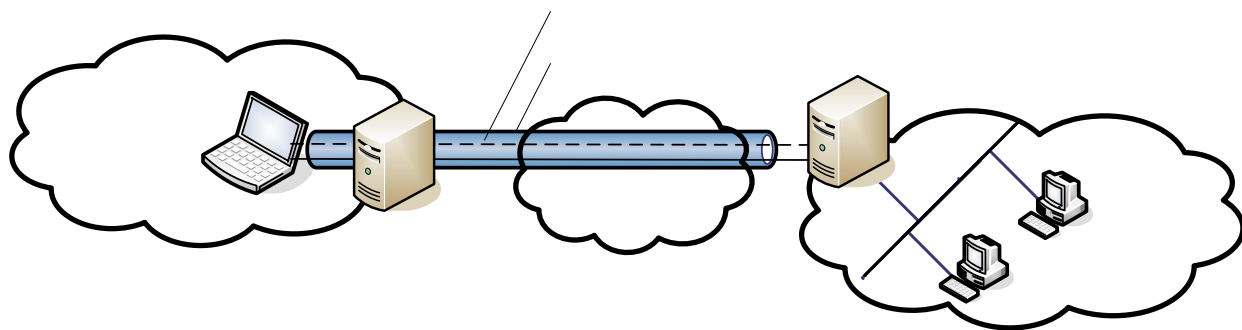


Рисунок 7

Интрасеть

VPN-server



## Управление виртуальными частными сетями

Управление виртуальными частными сетями ничем не отличается от управления любыми другими сетевыми ресурсами, и при использовании VPN-соединений (особенно через Интернет) следует тщательно продумать систему безопасности. Ответьте себе на следующие вопросы.

1. Где должны храниться учетные данные пользователей?

- Первичном контроллере домена
- На сервере RADIUS

2. Как будут назначаться адреса VPN-клиентам?

- DHCP
- Заданный пул IP-адресов, DNS, WINS

3. Кому разрешено создавать VPN-соединения?

Для управления удаленным доступом следует настроить параметры входящих звонков в свойствах пользовательских учетных записей и в соответствующих политиках удаленного доступа.

- Доступ по пользовательской учетной записи
- Доступ по принадлежности к группам

4. Как VPN-сервер будет аутентифицировать пользователя, пытающегося установить VPN-соединение?

- Windows-аутентификация
- RADIUS-аутентификация

5. Как VPN-сервер будет регистрировать активность, связанную с VPN?

- Средства Windows
- Средства RADIUS (файл/БД)

6. Как добиться того, чтобы VPN-сервером можно было управлять на основе стандартных протоколов и инфраструктуры сетевого администрирования?

Если на компьютер с Windows 2008, работающий в качестве VPN-сервера, установить службу SNMP, он сможет действовать в среде SNMP (Simple Network Management Protocol) как агент SNMP. VPN-сервер регистрирует управляющую информацию в различных идентификаторах объектов MIB II (Management Information Base), которые устанавливаются со службой SNMP.

## Туннельные протоколы

### ***PPTP***

PPTP (Point-to-Point Tunneling Protocol) инкапсулирует кадры PPP (Point-to-Point Protocol) в IP-дейтаграммы для передачи через межсетевую IP-среду, например Интернет или частную интрасеть. PPTP документирован в RFC 2637. Для создания, поддержания и закрытия туннеля протокол PPTP использует TCP-соединение, известное под названием «управляющее PPTP-соединение» (PPTP control connection), а для инкапсуляции PPP-кадров как туннелированных данных — модифицированную версию GRE (Generic Routing Encapsulation). Собственно данные инкапсулированных PPP-кадров можно шифровать и/или сжимать. PPTP требует наличия межсетевой IP-среды между PPTP-клиентом и PPTP-сервером. PPTP-клиент может быть уже подключен к межсетевой IP-среде, через которую достигим PPTP-сервер, либо он может дозваниваться до сервера доступа в сеть (NAS) и устанавливать IP-соединение — так же, как и пользователь, получающий доступ в Интернет по коммутируемой линии. Аутентификация, выполняемая при создании VPN-соединения на основе PPTP, осуществляется с применением тех же механизмов, что и при установлении PPP-соединений, — например, EAP (Extensible Authentication Protocol), MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), CHAP, SPAP (Shiva Password Authentication Protocol) и PAP (Password Authentication Protocol). PPTP наследует методы шифрования и/или сжатия полезных данных PPP от протокола PPP. В случае Windows 2008 для шифрования этих данных по методу MPPE (Microsoft Point-to-Point Encryption) следует использовать либо EAP-TLS (SAP-Transport Level Security), либо MS-CHAP.

MPPE обеспечивает шифрование не на всем пути передачи данных (между клиентским приложением и сервером, на котором размещен ресурс или сервис, используемый этим приложением), а лишь при их прохождении по каналу. Для шифрования на всем пути передачи данных нужно использовать IPsec, который будет шифровать IP-трафик после создания PPTP-туннеля.

PPTP-сервер на основе Интернет-стандартов представляет собой VPN-сервер с поддержкой PPTP; при этом один из его интерфейсов подключен к Интернету, а другой — к интрасети.

### **Поддержание туннеля с помощью управляющего PPTP-соединения**

Управляющее PPTP-соединение устанавливается между динамически назначаемым TCP-портом PPTP-клиента и зарезервированным TCP-портом 1723 PPTP-сервера. По этому соединению PPTP управляет вызовами и передает управляющие сообщения, используемые для поддержания PPTP-туннеля. К ним относятся PPTP-сообщения Echo-Request и Echo-Reply, позволяющие распознавать обрыв связи между PPTP-клиентом и сервером. Пакет, передаваемый по управляющему PPTP-соединению состоит из IP- и TCP-заголовков, управляющего PPTP-сообщения, а также заголовка и концевой части канального уровня (рисунок 8).



Рисунок 8

В таблице 1 перечислены основные управляющие PPTP-сообщения, передаваемые по управляющему PPTP-соединению. Конкретный PPTP-туннель для всех управляющих PPTP-сообщений идентифицируется по TCP-соединению.

Таблица 1. Основные управляющие PPTP-сообщения

Start-Control-Connection-Request	Посылается PPTP-клиентом для установления управляющего соединения. До передачи любых других PPTP сообщений для каждого PPTP-туннеля нужно создать свое управляющее соединение.
Start-Control-Connection-Reply	Посылается PPTP-сервером в ответ на сообщение Start-Control-Connection-Request.
Outgoing-Call-Request	Посылается PPTP-клиентом для создания PPTP-туннеля. В это сообщение включается идентификатор вызова (Call ID), используемый в GRE-заголовке для определения туннелируемого трафика, передаваемого по конкретному туннелю.
Outgoing-Call-Reply	Посылается PPTP-сервером в ответ на сообщение Outgoing-Call-Request.
Echo-Request	Посылается PPTP-клиентом или сервером для проверки активности соединения. Если ответ на это сообщение не поступает, PPTP-туннель через определенное время закрывается.
Echo-Reply	Ответ на сообщение Echo-Request. Примечание: PPTP-сообщения Echo-Request и Echo-Reply не имеют никакого отношения к ICMP-сообщениям Echo Request (Эхо-запрос) и Echo Reply (Эхо-ответ),
WAN-Error-Notify	Посылается PPTP-сервером всем VPN-клиентам, чтобы сообщить о какой-либо ошибке, возникшей на PPP-интерфейсе PPTP-сервера.
Set-Link-Info	Посылается PPTP-клиентом или сервером для установки согласованных PPP-параметров.
Call-Clear-Request	Посылается PPTP-клиентом для закрытия туннеля.
Call-Disconnect-Notify	Посылается PPTP-сервером в ответ на сообщение Call-Clear-Request или по другим причинам. Указывает, что туннель должен быть закрыт.
Stop-Control-Connection-Request	Посылается PPTP-клиентом или сервером для уведомления другой стороны о закрытии управляющего соединения.
Stop-Control-Connection-Reply	Ответ на сообщение Stop-Control-Connection-Request.

## Туннелирование данных средствами PPTP

Такое туннелирование осуществляется путем многоуровневого инкапсулирования. Структура данных, туннелирования средствами PPTP, показана на рисунке 9.



Рисунок 9

### **Инкапсуляция PPP-кадра**

Исходные полезные данные PPP зашифровываются и инкапсулируются в кадр с PPP-заголовком (PPP-кадр). Затем этот кадр инкапсулируется в пакет с модифицированным GRE-заголовком. GRE документирован в RFC 1701 и 1702, и изначально был разработан в качестве простого универсального механизма инкапсуляции данных, передаваемых через межсетевые IP-среды. GRE является клиентским протоколом IP и использует идентификатор IP-протокола 47.

GRE-заголовок модифицируется для PPTP следующим образом:

- Бит подтверждения указывает на наличие 32-битного поля подтверждения;
- Поле ключа заменяется 16-битными полями длины полезных данных и идентификатора вызова. Последнее устанавливается PPTP-клиентом при создании PPTP-туннеля;
- Добавляется 32-битное поле подтверждения.

Внутри GRE-заголовка в поле типа протокола записывается значение 0x880B, используемое как значение EtherType для PPP-кадра.

### **Инкапсуляция GRE-пакета**

GRE-пакет далее инкапсулируется в пакет с IP-заголовком, в котором указываются IP-адреса отправителя и получателя (в роли которых выступают PPTP-клиент и сервер).

### **Инкапсуляция канального уровня**

Для передачи по локальной сети (LAN) или WAN-каналу созданная на предыдущем этапе IP-дейтаграмма инкапсулируется в пакет с заголовком и концевой частью канального уровня, применяемого на данном физическом интерфейсе. Например, при передаче через Ethernet-интерфейс IP-дейтаграмма инкапсулируется в пакет с Ethernet-заголовком и концевой частью, а при передаче по WAN-каналу типа «точка-точка» (аналоговой телефонной линии или ISDN) — в пакет с PPP-заголовком и концевой частью.

GRE иногда используется ISP для пересылки информации о маршрутизации внутри своих сетей. Чтобы эта информация не пересылалась на маршрутизаторы Интернет-магистралей (Internet backbone routers), ISP отфильтровывают GRE-трафик на периферии. В результате можно только создавать PPTP-туннели, но не пересылать туннелированные данные.

## **PPTP-пакеты и сетевая архитектура Windows 2008**

Рисунок 10 иллюстрирует путь, который проходят туннелированные данные (от VPN-клиента по VPN-соединению удаленного доступа, установленному с помощью аналогового модема) через компоненты сетевой архитектуры Windows 2008.

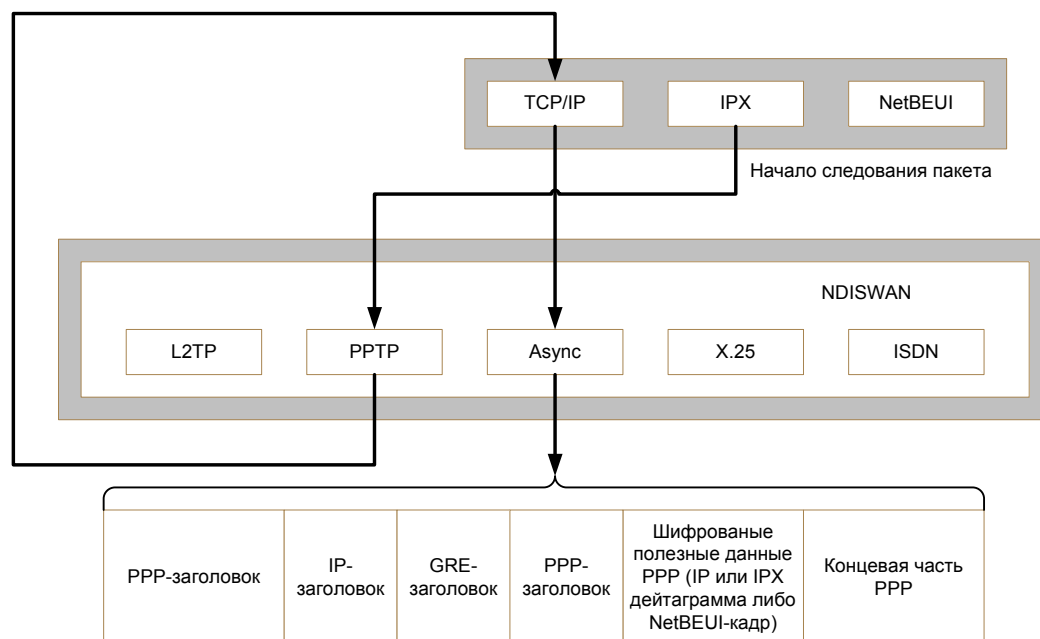


Рисунок 10

1. IP- или IPX-дейтаграмма либо NetBEUI-кадр передается соответствующим протоколом через NDIS (Network Driver Interface Specification) на виртуальный интерфейс, представляющий VPN-соединение;
2. NDIS передает пакет NDISWAN, который расшифровывает и/или декомпрессирует данные и предоставляет PPP-заголовок, включающий только поле идентификатора PPP-протокола. Поля флагов и FCS (Frame Check Sequence) не добавляются. Это предполагает, что на LCP-этапе процесса установления PPP-соединения было согласовано сжатие полей адреса и управления;
3. NDISWAN передает данные драйверу протокола PPTP, который инкапсулирует PPP-кадр в пакет с GRE-заголовком. В поле идентификатора вызова в GRE-заголовке записывается значение, идентифицирующее туннель;
4. Полученный пакет драйвер протокола PPTP передает драйверу протоколов TCP/IP;
5. Этот драйвер инкапсулирует туннелированные средствами PPTP данные в пакет с IP-заголовком и передает его через NDIS интерфейсу, представляющему соединение удаленного доступа с местным ISP;
6. NDIS передает пакет NDISWAN, который добавляет PPP-заголовок и концевую часть.
7. NDISWAN передает полученный PPP-кадр минипорт-драйверу WAN, представляющему аппаратные средства удаленного доступа, например асинхронный порт (в случае модемного соединения).

Можно согласовать использование шифруемого PPP-соединения по коммутируемому соединению с ISP. Но следует помнить, что туннелированные данные уже зашифрованы.

## L2TP

L2TP (Layer Two Tunneling Protocol) — это комбинация PPTP и L2F (Layer 2 Forwarding), технологии, предложенной компанией Cisco Systems Inc. Чтобы два несовместимых протокола туннелирования не конкурировали на рынке и не запутывали заказчиков, IETF распорядился скомбинировать эти две технологии в один протокол туннелирования, который сочетал бы в себе лучшие качества PPTP и L2F.

L2TP документирован в RFC 2661. L2TP инкапсулирует PPP-кадры, передаваемые по сетям IP, X.25, Frame Relay или ATM. В настоящее время определен стандарт только на L2TP поверх IP. При передаче по межсетевой IP-среде L2TP-кадры инкапсулируются как UDP-сообщения. L2TP — протокол туннелирования, пригодный для применения как в Интернете, так и в частных интрасетях.

L2TP использует UDP-сообщения в межсетевых IP-средах для управления туннелями и передачи туннелированных данных. Полезные данные инкапсулированных PPP-кадров могут быть зашифрованы и/или сжаты; однако L2TP-клиенты под управлением Windows 2008 не могут использовать MPPE для L2TP-соединения. Поэтому шифрование для таких соединений реализуется за счет IPSec-протокола ESP.

Windows 2008 позволяет создавать L2TP-соединения, не шифруемые с помощью IPSec (IP-безопасность). Но в таком случае Вы не получите VPN-соединение, несколько конфиденциальные данные, инкапсулируемые L2TP, окажутся незашифрованными. Нешифруемые L2TP-соединения можно использовать в качестве временной меры при устранении каких-либо проблем с поддержкой соединения L2TP поверх IPSec; при этом исключаются IPSec-процессы аутентификации и согласования.

L2TP требует наличия межсетевой IP-среды между L2TP-клиентом (VPN-клиентом, использующим протокол туннелирования L2TP и IPSec) и L2TP-сервером (VPN-сервером, использующим тот же протокол и IPSec). L2TP-клиент может быть уже подключен к межсетевой IP-среде, через которую достигим L2TP-сервер, либо он может дозваниваться до сервера NAS и устанавливать IP-соединение — так же как и пользователь, получающий доступ в Интернет по коммутируемой линии. Аутентификация, выполняемая при создании L2TP-туннелей, осуществляется с применением тех же механизмов, что и при установлении PPP-соединений, — например, EAP, MS-CHAP, CHAP, SPAP и PAP.

L2TP-сервер на основе Интернет-стандартов представляет собой сервер удаленного доступа с поддержкой L2TP; при этом один из его интерфейсов подключен к Интернету, а другой — к интрасети. Пакеты с информацией, управляющей L2TP-туннелем, и туннелированными данными имеют одинаковую структуру.

### Поддержание туннеля с помощью управляющих L2TP-сообщений

L2TP — в отличие от PPTP — не требует для поддержания туннеля отдельного TCP-соединения. L2TP-трафик передается между L2TP-клиентом и сервером в виде UDP-сообщений. В Windows 2008 для этого используется UDP-порт 1701. Управляющие сообщения L2TP поверх IP посылаются как UDP-дейтаграммы. В варианте, реализованном в Windows 2008, эти UDP-дейтаграммы передаются в виде зашифрованных полезных данных IPSec-протокола ESP (рисунок 11).



Рисунок 11

Поскольку TCP-соединение не используется, L2TP — чтобы гарантировать доставку L2TP-сообщений — применяет их упорядочение (message sequencing). Поля Next-Received (по аналогии с TCP-полем подтверждения) и Next-Sent (по аналогии с TCP-полем номера

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

последовательности) внутри управляющего L2TP-сообщения предназначены для слежения за последовательностью сообщений. Пакеты, выпадающие из должной последовательности, отбрасываются. Поля Next-Sent и Next-Received могут также использоваться для упорядоченной доставки и управления потоком туннелированных данных.

L2TP поддерживает по несколько вызовов на каждом туннеле. С этой целью в управляющем L2TP-сообщении в L2TP-заголовке туннелированных данных присутствуют поля идентификатора туннеля и идентификатора вызова (для данного туннеля).

Основные управляющие L2TP-сообщения перечислены в таблице 2.

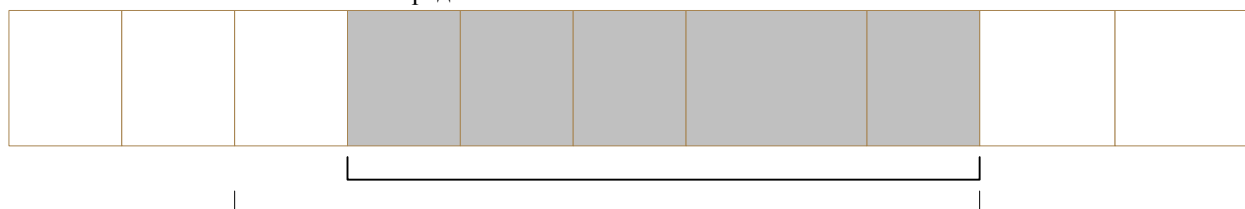
Таблица 2

Start-Control-Connection-Request	Посылается L2TP-клиентом для установления управляющего соединения. До передачи любых других L2TP-сообщений для каждого L2TP-туннеля нужно создать свое управляющее соединение.
Start-Control-Connection-Reply	Посылается L2TP-сервером в ответ на сообщение Start-Control-Connection-Request (см. Также ниже).
Start-Control-Connection-Connected	Посылается L2TP-клиентом в ответ на сообщение Start-Control-Connection-Reply.
Outgoing-Call-Request	Посылается L2TP-клиентом для создания L2TP-туннеля. В это сообщение включается назначенный идентификатор вызова (Assigned Call ID), определяющий конкретный вызов по данному туннелю.
Outgoing-Call-Reply	Посылается L2TP-сервером в ответ на сообщение Outgoing-Call-Request.
Start-Control-Connection-Connected	Посылается L2TP-клиентом в ответ на сообщение Outgoing-Call-Reply.
Hello	Посылается L2TP-клиентом или сервером для проверки активности соединения. Если прием этого сообщения не подтверждается, L2TP-туннель через определенное время закрывается.
WAN-Error-Notify	Посылается L2TP-сервером всем VPN-клиентам, чтобы сообщить о какой-либо ошибке, возникшей на PPP-интерфейсе L2TP-сервера.
Set-Link-Info	Посылается L2TP-клиентом или сервером для установки согласованных PPP-параметров.
Call-Disconnect-Notify	Посылается L2TP-сервером или клиентом для уведомления другой стороны о том, что данный вызов в данном туннеле должен быть завершен.
Stop-Control-Connection-Notification	Посылается L2TP-сервером или клиентом для уведомления другой стороны о том, что туннель должен быть закрыт.

## Туннелирование данных средствами L2TP

Такое туннелирование осуществляется путем многоуровневого инкапсулирования.

Структура данных, туннелированных средствами L2TP, показана на рисунке 12.



Заголовок  
канального  
уровня

IP-  
заголовок

ESP-  
заголовок

UDP-  
заголовок

заг

### Инкапсуляция L2TP

Изначальные полезные данные PPP инкапсулируются с использованием PPP- и L2TP-заголовков.

### Инкапсуляция UDP

Пакет, инкапсулированный L2TP, инкапсулируется в сообщение с UDP-заголовком, а порты отправителя и получателя устанавливаются как 1701.

Подписывается дл

### Инкапсуляция IPsec

UDP-сообщение зашифровывается на основе политики IP-безопасности и инкапсулируется в пакет с заголовком и концевой частью ESP (Encapsulating Security

Payload); кроме того, добавляется концевая часть ESP Authentication, необходимая для аутентификации по IPsec-протоколу ESP.

### Инкапсуляция IP

IPsec-пакет инкапсулируется в IP-дейтаграмму с IP-заголовком, который содержит IP-адреса отправителя и получателя, соответствующие VPN-клиенту и серверу.

### Инкапсуляция канального уровня

Для передачи по локальной сети или WAN-каналу созданная на предыдущем этапе

IP-дейтаграмма инкапсулируется в пакет с заголовком и концевой частью канального уровня, применяемого на данном физическом интерфейсе. Например, при передаче через Ethernet-интерфейс IP-дейтаграмма инкапсулируется в пакет с Ethernet-заголовком и концевой частью, а при передаче по WAN-каналу типа «точка-точка» (аналоговой телефонной линии или ISDN) — в пакет с PPP-заголовком и концевой частью.

### Обработка данных, туннелированных L2TP поверх IPsec

Получив данные, туннелированные средствами L2TP поверх IPsec, L2TP-клиент или сервер выполняет следующие операции:

1. Обрабатывает и удаляет заголовок и концевую часть канального уровня;
2. Обрабатывает и удаляет IP-заголовок;
3. Используя концевую часть ESP Authentication, проверяет подлинность полезных данных IP и ESP-заголовка;
4. Используя ESP-заголовок, расшифровывает зашифрованную часть пакета;
5. Обрабатывает UDP-заголовок и передает L2TP-пакет протоколу L2TP;
6. L2TP считывает содержимое полей идентификатора туннеля и идентификатора вызова в L2TP-заголовке, чтобы определить конкретный L2TP-туннель;
7. Идентифицирует по PPP-заголовку полезные данные PPP и передает их драйверу соответствующего протокола для обработки.



**Пакеты L2TP поверх IPsec и сетевая архитектура Windows 2008**

Рисунок 13 иллюстрирует путь, который проходят туннелированные данные (от VPN-клиента по VPN-соединению удаленного доступа, установленному с помощью аналогового модема) через компоненты сетевой архитектуры Windows 2008.

1. IP- или IPX-дейтаграмма либо NetBEUI-кадр передается соответствующим протоколом через NDIS на виртуальный интерфейс, представляющий VPNсоединение;
2. NDIS передает пакет NDISWAN, который декомпрессирует данные (при необходимости) и предоставляет PPP-заголовок, включающий только поле идентификатора PPP-протокола. Поля флагов и FCS не добавляются;
3. NDISWAN передает PPP-кадр драйверу протокола L2TP, который инкапсулирует этот кадр в пакет с L2TP-заголовком. В поля идентификаторов туннеля и вызова в L2TP-заголовке записываются значения, идентифицирующие туннель и вызов;
4. Полученный пакет драйвер протокола L2TP передает драйверу протоколов TCP/IP и уведомляет его о том, что данный L2TP-пакет следует отправить как UDP-сообщение с UDP-порта 1701 клиента в UDP-порт 1701 сервера (при этом указываются IP-адреса клиента и сервера);
5. Драйвер протоколов TCP/IP формирует IP-пакет, добавляя необходимые IP- и UDP-заголовки. Далее этот IP-пакет анализируется IPsec и приводится в соответствие с текущей политикой IP-безопасности. В зависимости от параметров политики IPsec шифрует UDP-часть IP-пакета и добавляет требуемые заголовки и концевые части ESP. Перед началом ESP-пакета добавляется исходный IP-заголовок со значением в поле протокола, равным 50. Затем драйвер протоколов TCP/IP передает полученный пакет через NDIS интерфейсу, представляющему соединение удаленного доступа с местным ISP;
6. NDIS передает пакет NDISWAN, который добавляет PPP-заголовок и концевую часть;
7. NDISWAN передает полученный PPP-кадр минипорт-драйверу WAN, представляющему аппаратные средства удаленного доступа.

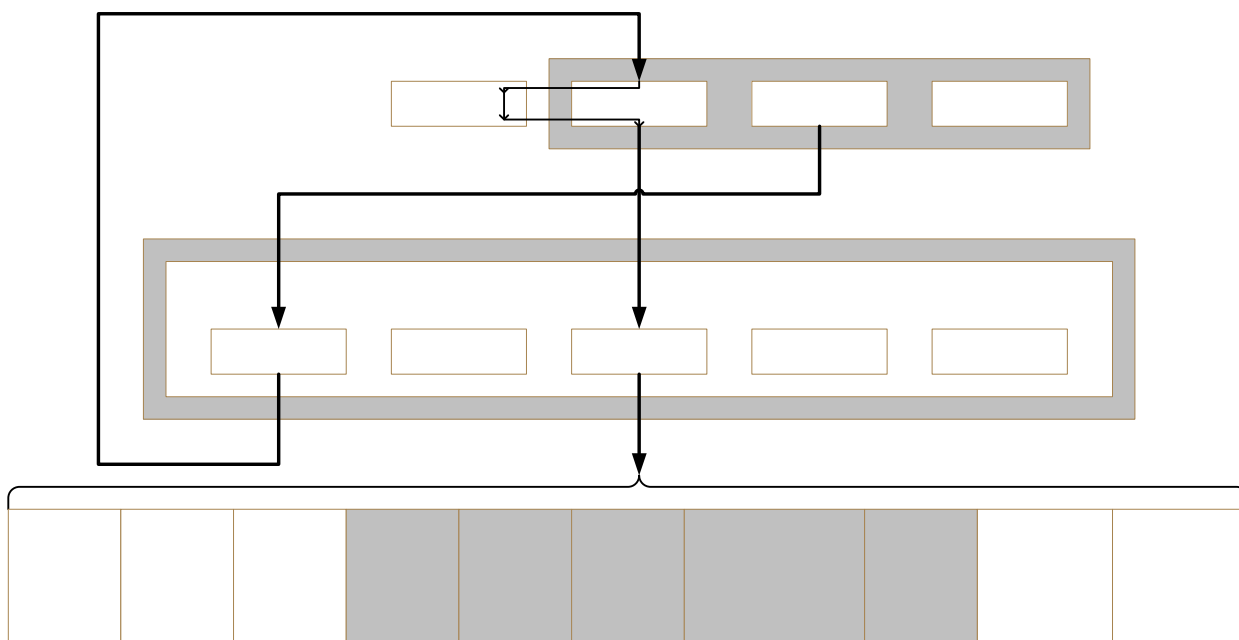


Рисунок 13

Можно согласовать использование шифруемого PPP-соединения по коммутируемому соединению с ISP. Но следует помнить, что туннелированные данные уже зашифрованы.

## Защита виртуальных частных сетей

Защита — важный элемент VPN. Далее описываются средства защиты, поддерживаемые PPTP и L2TP поверх IPSec для VPN-соединений.

PPTP обеспечивает:

- аутентификацию пользователей;
- шифрование данных.

«L2TP поверх IPSec» обеспечивает:

- аутентификацию пользователей;
- взаимную аутентификацию компьютеров;
- шифрование данных;
- аутентификацию данных и проверку их целостности.

	<b>РРТР-соединения</b>	<b>Соединения L2TP поверх IPSec</b>
А У Т е н т и ф и к а ц и я	<p>Пользователь, запрашивающий РРТР-соединение, аутентифицируется по одному из РРР-протоколов аутентификации: EAP, MS-CHAP, CHAP, SPAP или PAP. Для РРТР-соединений настоятельно рекомендуется использовать EAP-TLS в сочетании со смарт-картами либо MS-CHAPv2, поскольку они поддерживают взаимную аутентификацию и являются самыми безопасными методами обмена удостоверениями.</p>	<p>Аутентификация VPN-клиента осуществляется на двух уровнях: сначала проверяется подлинность компьютера, затем - пользователя</p> <p><u>IPSec аутентификация компьютеров</u></p> <p>Взаимная аутентификация выполняется путем обмена машинными сертификатами при создании IPSec-протоколом ESP сопоставления безопасности (security association, SA). IPSec SA устанавливается на втором этапе процесса IPSec-согласования; к этому времени стороны также выбирают алгоритмы шифрования и хэширования и договариваются о шифровальных ключах. Для использования L2TP поверх IPSec у VPN-клиента и сервера должны быть машинные сертификаты. Получать их можно автоматически (в Group Policy галка автоматический запрос сертификатов) или, или вручную - через оснастку Certificates (Сертификаты).</p> <p><u>L2TP-аутентификация на уровне пользователей</u></p> <p>Пользователь, запрашивающий L2TP -соединение, аутентифицируется по одному из РРР-протоколов аутентификации: EAP, MS-CHAP, CHAP, SPAP или PAP. Поскольку процесс установления РРР-соединения защищается средствами шифрования IPSec, можно использовать любой метод РРР-аутентификации. Взаимная аутентификация на уровне пользователей возможна только при выборе MS-CHAPv2 или EAP-TLS.</p> <p><u>Аутентификация L2TP -туннеля</u></p> <p>В процессе установления L2TP-туннеля протокол L2TP позволяет аутентифицировать конечные точки этого туннеля. По умолчанию Windows 2008 ее не выполняет.</p> <p><u>Аутентификация и проверка целостности данных</u> реализуется одним из следующих алгоритмов:</p> <ul style="list-style-type: none"> <li>• HMAC (Hash Message Authentication Code) MD5 (Message Digest 5) - генерирует 128-битный хэш аутентифицированных полезных данных;</li> <li>• HMAC SHA (Secure Hash Algorithm) - генерирует 160-битный хэш аутентифицированных полезных данных.</li> </ul>
	<b>РРТР-соединение</b>	<b>Соединения L2TP поверх IPSec</b>
Ш	РРТР поддерживает шифрование методом MPPE, который основан на алгоритме RSA (Rivest-Shamir-Adleman) RC4. MPPE доступен только при	Метод шифрования выбирается при установлении IPSec SA. Доступные методы

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

и ф р о в а н и е	<p>использовании EAP-TLS или MS-CHAP (версии 1 или 2). MPPE оперирует с 40-, 56- или 128-битными шифровальными ключами. По умолчанию VPN-клиент и сервер договариваются о применении самого стойкого ключа из числа поддерживаемых. Если VPN-сервер требует более стойкого ключа, не поддерживаемого VPN-клиентом, запрос на соединение отклоняется. MPPE для VPN-соединения использует отдельный шифровальный ключ для каждого пакета. В MPPE-заголовок включается номер последовательности. Шифровальные ключи меняются в соответствии с этим номером последовательности.</p>	<p>шифрования включают:</p> <ul style="list-style-type: none"> <li>• DES с 56-битным ключом;</li> <li>• 3DES (Triple DES),</li> </ul> <p>Каждый IPSec-пакет зашифровывается независимо от других IP Sec-пакетов.</p> <p>Исходные шифровальные ключи генерируются в процессе IPsec-аутентификации. При соединениях с шифрованием по методу DES новые шифровальные ключи генерируются через каждые 5 мин/250 Мб, а по методу 3DES — каждый 1 час/2 Гб переданной информации. Для соединений, защищаемых AH, новые хэш-ключи генерируются каждый 1 час/2 Гб.</p>
Ф и л ь т р а ц и я п а к е т о в	<p>VPN-сервер на основе PPTP обычно снабжен двумя физическими интерфейсами: один подключен к общедоступной сети (например, к Интернету), другой — к частной интрасети. Кроме того, у него имеется виртуальный интерфейс, соединяющий его со всеми VPN-клиентами. Чтобы VPN-сервер мог пересылать трафик между VPN-клиентами, на всех его интерфейсах нужно включить поддержку IP-пересылки. Однако включение поддержки пересылки между двумя физическими интерфейсами приводит к тому, что VPN-сервер перенаправляет весь IP-трафик из общедоступной сети в интрасеть. Для защиты интрасети от постороннего трафика Вы должны настроить фильтрацию пакетов в PPTP так, чтобы VPN-сервер передавал данные только между VPN-клиентами и интрасетью и блокировал обмен пакетами между интрасетью и потенциально опасными пользователями общедоступной сети. Фильтрацию пакетов средствами PPTP можно настроить либо на VPN-сервере, либо на промежуточном брандмауэре.</p>	<p>Как и в случае VPN-соединений на основе PPTP, включение поддержки пересылки между интерфейсами общедоступной сети и интрасети приводит к тому, что VPN-сервер перенаправляет весь IP-трафик из общедоступной сети в интрасеть. Для защиты интрасети от постороннего трафика Вы должны настроить фильтрацию пакетов средствами L2TP поверх IPSec так, чтобы VPN-сервер передавал данные только между VPN-клиентами и интрасетью и блокировал обмен пакетами между интрасетью и потенциально опасными пользователями общедоступной сети. Фильтрацию пакетов средствами L2TP поверх IPSec можно настроить либо на VPN-сервере, либо на промежуточном брандмауэре.</p>

## Адресация и маршрутизация при использовании виртуальных частных сетей

VPN-соединение образует виртуальный интерфейс, которому нужно назначить соответствующий IP-адрес; кроме того, следует изменить или добавить маршруты, чтобы требуемый трафик передавался по защищенному VPN-соединению, а не по транзитной межсетевой среде.

### VPN-соединения удаленного доступа

При VPN-соединении удаленного доступа компьютер подключается к VPN-серверу. В процессе установления соединения VPN-сервер назначает VPN-клиенту IP-адрес и изменяет маршрут по умолчанию на удаленном клиенте, чтобы соответствующий трафик передавался по виртуальному интерфейсу.

VPN-клиент удаленного доступа перед созданием VPN-соединения с VPN-сервером сначала подключается к Интернету и из-за этого получает два IP-адреса:

- при установлении PPP-соединения NAS-сервер ISP присваивает клиенту общий IP-адрес (в IPSP-процессе согласования);
- при создании VPN-соединения VPN-сервер (в IPSP-процессе согласования) назначает клиенту IP-адрес из диапазона адресов своей интрасети. Этот IP-адрес может быть общим (видимым в Интернете) или частным (невидимым в Интернете) в зависимости от того, какие адреса используются в данной интрасети — общие или частные.

В любом случае IP-адрес, выделенный VPN-клиенту, должен быть достижим для хостов в интрасети и наоборот. В таблице маршрутизации на VPN-сервере должны быть записи, позволяющие связаться с любыми хостами в интрасети, а в аналогичных таблицах на маршрутизаторах — записи, необходимые для взаимодействия с VPN-клиентами.

В IP-заголовке туннелированных данных, посылаемых через VPN, указываются адрес, выделенный клиенту VPN-сервером, и адрес интрасети, а во внешнем IP-заголовке — IP-адрес, выделенный клиенту провайдером, и общий адрес VPN-сервера. Поскольку маршрутизаторы в Интернете обрабатывают только внешние IP-заголовки, они пересылают туннелированные данные на общий IP-адрес VPN-сервера.

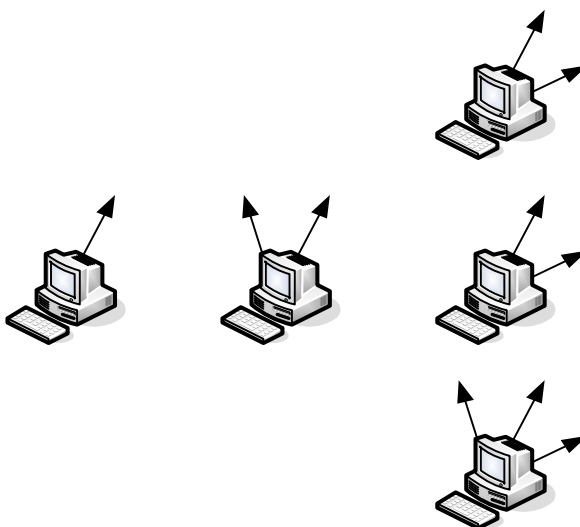


Рисунок 14

Случай а):

Клиент дозванивается до ISP и получает (обычно) общий IP-адрес. При этом адрес основного шлюза в IPSP-процессе не назначается. Маршрут по умолчанию необходимо добавить в таблицу маршрутизации.

Случай б):

Клиент имеет соединение с intranet (или просто имеет иной TCP/IP интерфейс) и дозванивается до ISP. В этом случае клиент получает от ISP IP-адрес и новый шлюз по умолчанию. Причем предыдущий шлюз по умолчанию получает значение более высокой метрики (т.е. становится менее приоритетным) по сравнению с новым шлюзом. Т.о. адреса в интрасети, находящиеся вне сети, к которой клиент удаленного доступа подключен напрямую.

Новый шлюз назначается автоматически (по умолчанию).

Чтобы запретить создание маршрута по умолчанию:

В свойствах TCP/IP объекта соединения удаленного доступа откройте диалоговое окно Advanced TCP/IP Settings, перейдите на вкладку General и сбросьте флажок Use default gateway on remote network.

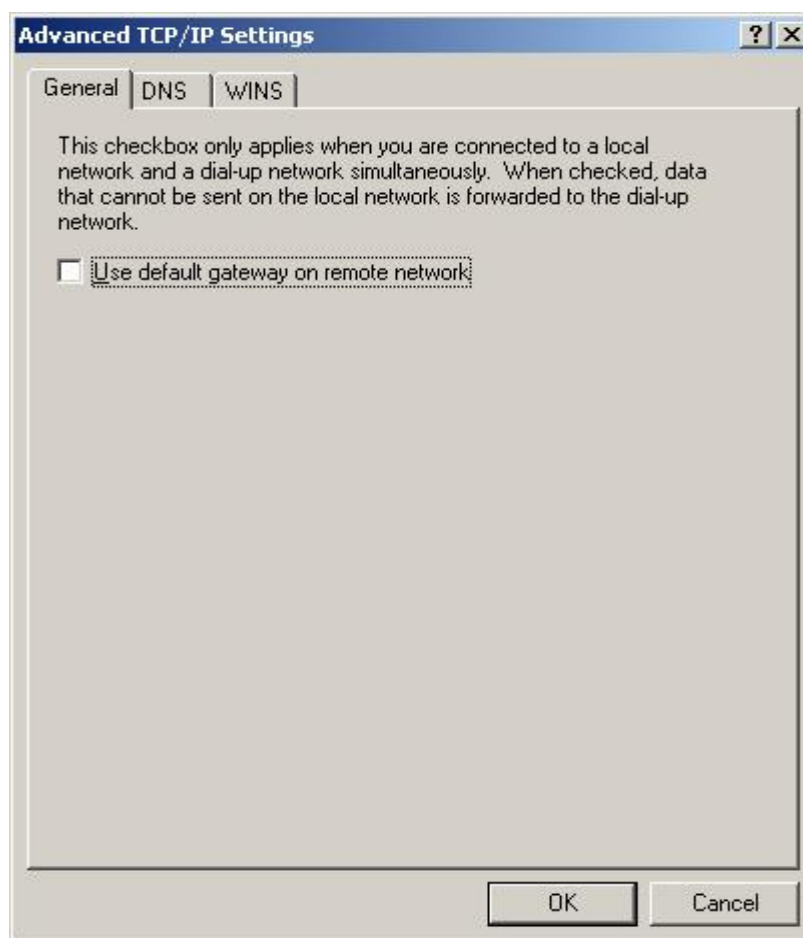


Рисунок 15

Чтобы обеспечить связь как с адресами в интрасети, так и с адресами в Интернете, пока активно соединение с ISP, не сбрасывайте флажок Use default gateway on remote network, а в таблицу маршрутизации на клиенте удаленного доступа добавьте маршруты к интрасети. Эти маршруты можно добавить как статические (командой route) или, если в интрасети используется протокол маршрутизации RIP Версии 1, воспользоваться службой

Route Listening Service для прослушивания трафика RiP v1 и динамического добавления нужных маршрутов. Тогда после соединения с ISP все адреса в интрасети будут достижимы через маршруты к интрасети, а все адреса в Интернете — через маршрут по умолчанию.

Случай в):

Клиент уже имеет соединения с intranet либо ISP или оба вместе, и пытается установить VPN. Стоит отметить, что ситуация аналогична предыдущей.

Когда VPN-клиент создает VPN-соединение, в его таблицу маршрутизации добавляются еще один маршрут по умолчанию и маршрут к VPN-серверу (рисунок 16). Прежний маршрут по умолчанию сохраняется, но его метрика увеличивается. Добавление нового маршрута по умолчанию означает, что все адреса в Интернете, кроме IP-адреса сервера туннелирования, недостижимы до закрытия VPN-соединения.

Как и в случае клиента удаленного доступа, подключающегося к Интернету, создание VPN-клиентом удаленного доступа VPN-соединения с частной интрасетью через Интернет влечет за собой одно из следующих последствий:

- пока VPN-соединение неактивно, адреса в Интернете достижимы, а в интрасети через интернет— нет;
- пока VPN-соединение активно, адреса в интрасети через Интернет достижимы, а в Интернете —нет.

Для большинства VPN-клиентов, подключенных к Интернету, такая схема не создает никаких проблем, потому что они, как правило, поддерживают коммуникационную связь либо с интрасетью, либо с Интернетом, но не то и другое одновременно.

А что касается VPN-клиентов, которым после установления VPN-соединения нужен одновременный доступ и к интрасети, и к Интернету, то конкретное решение зависит от типа адресации в интрасети. Но в любом случае объект VPN-соединения следует настроить так, чтобы новый основной шлюз не добавлялся. Тогда после создания VPN-соединения маршрут по умолчанию будет по-прежнему указывать адрес NAS-сервера ISP, что позволит обращаться по любым адресам в Интернете.

Исходя из типа адресации в интрасети одновременный доступ к ресурсам интрасети и Интернета реализуется следующим образом.

**Общие адреса.** Добавьте статические постоянные маршруты к общим адресам интрасети с использованием IP-адреса виртуального интерфейса VPN-сервера в качестве IP-адреса шлюза.

**Частные адреса.** Добавьте статические постоянные маршруты к частным адресам интрасети с использованием IP-адреса виртуального интерфейса VPN-сервера в качестве IP-адреса шлюза.

**Перекрывающиеся или недопустимые адреса.** Если в интрасети используются перекрывающиеся (overlapping) или недопустимые (illegal) адреса (идентификаторы IP-сетей, которые не являются частными и либо не зарегистрированы в InterNIC, либо получены от ISP), эти IP-адреса могут дублировать общие адреса в Интернете. Если в таблицу маршрутизации на VPN-клиенте добавляются статические постоянные маршруты с перекрывающимися адресами, то совпадающие: с ними адреса в Интернете недостижимы.

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

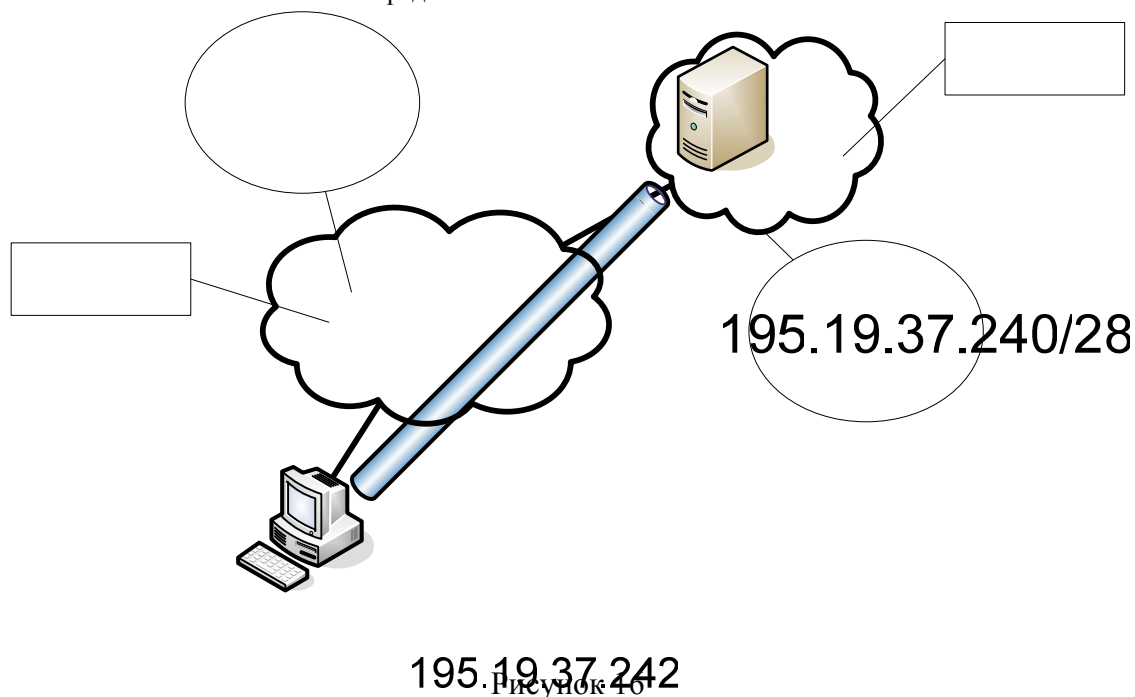


Рисунок 4

В каждом из этих случаев в таблице маршрутизации на VPN-клиенте нужно добавлять статические постоянные маршруты к идентификаторам сетей, используемых в интрасети.

Каждый маршрут добавляется следующей командой:

**ROUTE ADD** <идентификатор сети для интрасети> **MASK** <маска сети> <IP-адрес виртуального интерфейса VPN-сервера> **-p**

IP-адрес шлюза в командах route для каждого маршрута интрасети — это IP-адрес виртуального интерфейса VPN-сервера, а не его Интернет-интерфейса.

Вы можете определить IP-адрес виртуального интерфейса VPN-сервера по IP-адресу интерфейса Internal (Внутренний), раскрыв в оснастке Routing and Remote Access узлы IP Routing и General (Общие).

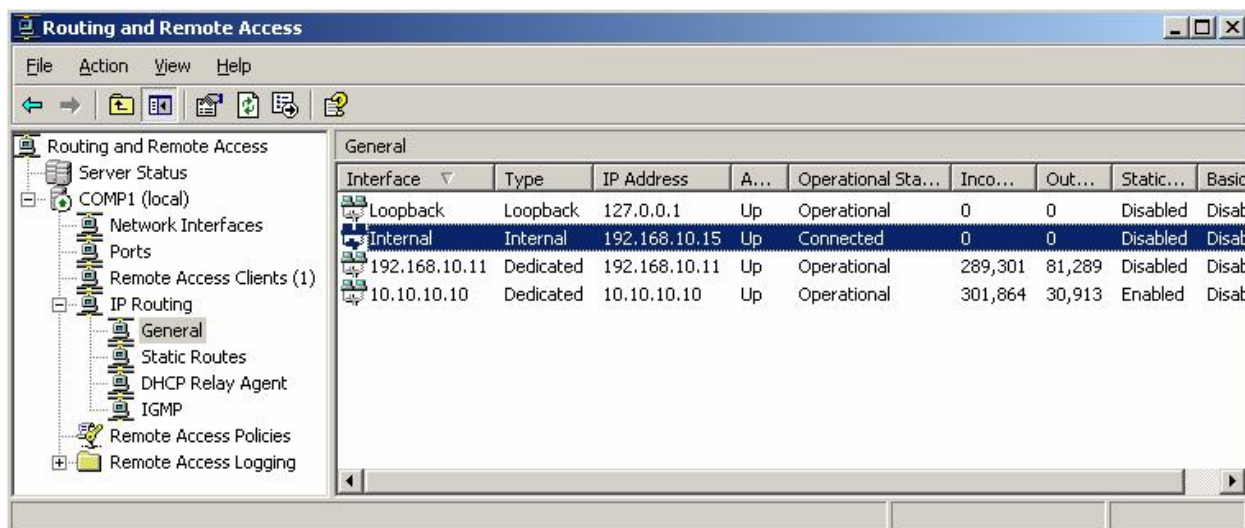


Рисунок 17

Если IP-адреса для VPN-клиентов и удаленного доступа к сетям выделяются через DHCP, то IP-адрес виртуального интерфейса VPN-сервера является первым IP-адресом, полученным от DHCP.

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

Если Вы сконфигурировали статический пул IP-адресов, то IP-адрес виртуального интерфейса VPN-сервера – первый IP-адрес из этого пула.

Вы можете выяснить IP-адрес виртуального интерфейса VPN-сервера и таким способом: дважды щелкните объект активного VPN-соединения и в диалоговом окне Status перейдите на вкладку Details.

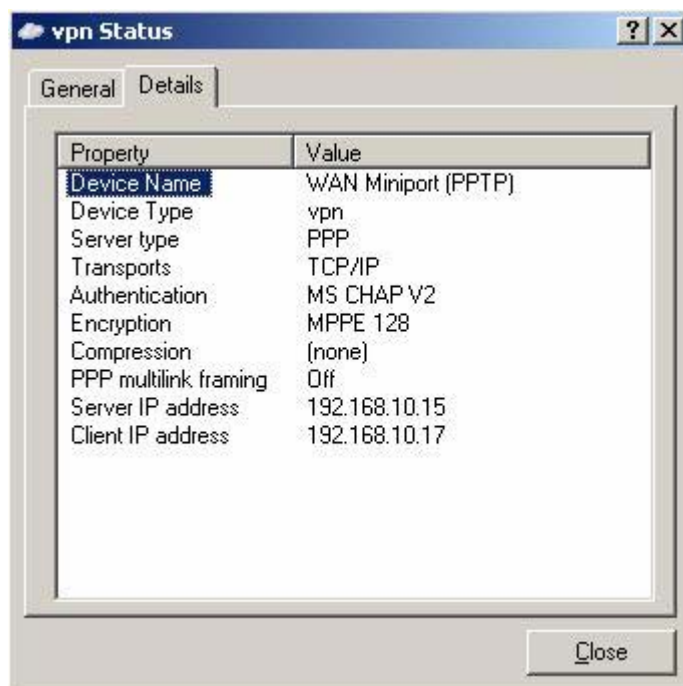


Рисунок 18

Необходимо быть очень осторожным при добавлении маршрутов, чтобы гарантировать передачу трафика, связанного с интрасетью, по VPN-, а не по PPP-соединению с ISP. Если Вы добавите неправильные маршруты, то трафик, который должен был бы пересылаться через VPN в зашифрованном виде, будет передаваться через Интернет открытым текстом.

### **VPN-соединения между маршрутизаторами**

В случае VPN-соединений между маршрутизаторами пересылка пакетов осуществляется через интерфейс соединения по требованию (demand-dial interface), настраиваемый следующим образом.

- На вкладке General (Общие) введите хост-имя или IP-адрес VPN-сервера.
- На вкладке Security (Безопасность) выберите либо шифрование пароля и данных, либо переключатель Custom (Дополнительные (особые параметры)]. Выбрав Custom. Вы должны указать подходящие параметры шифрования и аутентификации.
- На вкладке Networking (Сеть) укажите нужный тип сервера и протоколы, подлежащие маршрутизации. Если в качестве типа сервера Вы выбрали вариант Automatic (Автоматически), то сначала предпринимается попытка установить соединение L2TP поверх IPSec, затем PPTP-соединение.
- В окне Interface Credentials (Учетные данные для интерфейса) введите имя пользователя, пароль и имя домена, применяемые для проверки вызывающей» маршрутизатора.



В создании интерфейсов соединения по требованию помогает Demand-Dial Interface Wizard (Мастер интерфейса вызова по требованию). Имя такого интерфейса на отвечающем маршрутизаторе должно совпадать с именем пользователя в удостоверениях (учетных данных) вызывающего маршрутизатора и наоборот — иначе Вам не удастся установить VPN-соединение между маршрутизаторами.

## Временные и постоянные VPN-соединения между маршрутизаторами

VPN-соединения между маршрутизаторами могут быть временными или постоянными.

- Временные соединения создаются для пересылки пакетов через VPN-интерфейс соединения по требованию и закрываются по истечении определенного времени простоя. Этот интервал задается как на VPN-клиенте (вызывающем маршрутизаторе), так и на VPN-сервере (вызываемом маршрутизаторе). По умолчанию время простоя для интерфейсов соединения по требованию на VPN-клиенте не ограничено, а на VPN-сервере — составляет 20 минут. Эти интервалы можно изменить по своему усмотрению. Временные VPN-соединения между маршрутизаторами рекомендуется использовать в филиалах, сначала подключающихся к Интернету через местных провайдеров.
- Постоянные соединения создаются при запуске маршрутизатора и существуют независимо от того, пересылается по ним трафик или нет. Если VPN-соединение закрывается, оно автоматически восстанавливается. Используйте постоянные VPN-соединения между маршрутизаторами в офисах, располагающих постоянными подключениями к Интернету.

Чтобы сделать соединение временным или постоянным:

1. В оснастке Routing and Remote Access выберите Routing Interfaces.
2. Щелкните правой кнопкой мыши нужный интерфейс соединения по требованию и выберите команду Properties.
3. На вкладке Options в разделе Connection Type выберите один из переключателей: либо Demand dial, либо Persistent.

## VPN-соединения через подключение удаленного доступа с ISP

Если VPN-сервер и VPN-клиент напрямую подключены к Интернету по постоянному WAN-каналу типа T1 или Frame Relay, то VPN-соединение может быть постоянным и действовать круглосуточно. Однако, если нет возможности использовать постоянный WAN-канал или если его применение нерентабельно, то можно сконфигурировать VPN-соединение между маршрутизаторами, устанавливаемое по требованию и использующее подключение удаленного доступа к ISP. Для этого VPN-соединения нужно два интерфейса соединения по требованию: один обеспечивает подключение к местному ISP, другой — создание VPN-соединения между маршрутизаторами. Временное VPN-соединение между маршрутизаторами устанавливается автоматически, когда маршрутизатор филиала принимает трафик, подлежащий пересылке по VPN-соединению. Например, получив пакет, который нужно переслать в центральный офис, маршрутизатор филиала сначала связывается с местным ISP по коммутируемой линии. Подключившись к Интернету, маршрутизатор филиала (VPN-клиент) создает межмаршрутизаторное VPN-соединение с маршрутизатором центрального офиса (VPN-сервером).

**Чтобы настроить маршрутизатор филиала:**

1. Добавьте интерфейс соединения по требованию для подключения к Интернету и настройте его на использование нужного оборудования (модема или ISDN-устройства). Затем укажите телефонный номер местного ISP, имя и пароль пользователя, необходимые для получения доступа в Интернет.
2. Добавьте интерфейс соединения по требованию для межмаршрутизаторного VPN-соединения с маршрутизатором центрального офиса и настройте его на использование PPTP или L2TP. Затем укажите IP-адрес или хост-имя Интернет-интерфейса VPN-сервера центрального офиса, а также имя и пароль пользователя, которые сможет проверить VPN-сервер. Имя пользователя должно совпадать с именем интерфейса соединения по требованию на VPN-сервере центрального офиса.
3. Создайте статический маршрут к хосту для IP-адреса Интернет-интерфейса VPN-сервера; этот маршрут должен использовать интерфейс соединения по требованию, через который маршрутизатор филиала связывается с местным ISP.
4. Создайте статический маршрут или маршруты для идентификаторов сетей в корпоративной интрасети; эти маршруты должны использовать VPN-интерфейс соединения по требованию.

**Чтобы настроить маршрутизатор центрального офиса:**

1. Добавьте интерфейс соединения по требованию для VPN-соединения с маршрутизатором филиала и настройте его на использование VPN-устройства (PPTP-или L2TP-порта). Имя интерфейса соединения по требованию должно совпадать с именем пользователя в аутентификационных удостоверениях маршрутизатора филиала.
2. Создайте статический маршрут или маршруты для идентификаторов сетей в интрасети филиала; эти маршруты должны использовать VPN-интерфейс соединения по требованию.

VPN-соединение между маршрутизаторами автоматически инициируется маршрутизатором филиала, и вот что при этом происходит.

1. Пакеты, передаваемые в корпоративную сеть от пользователя в сети филиала, пересылаются клиентским компьютером этого пользователя на маршрутизатор филиала.
2. Маршрутизатор филиала просматривает свою таблицу маршрутизации и находит нужный маршрут, использующий VPN-интерфейс соединения по требованию.
3. Маршрутизатор филиала проверяет VPN-интерфейс соединения по требованию и обнаруживает, что он находится в отключенном состоянии.
4. Маршрутизатор филиала считывает конфигурационные параметры этого интерфейса.
5. На основе полученных параметров маршрутизатор филиала пытается инициализировать VPN-соединение между маршрутизаторами, используя IP-адрес VPN-сервера в Интернете.
6. Для создания VPN-соединения нужно либо установить TCP-соединение (при использовании PPTP), либо выполнить процесс согласования IPSec с VPN-сервером. С этой целью генерируется пакет запроса на VPN-соединение.
7. Чтобы переслать этот пакет маршрутизатору центрального офиса, маршрутизатор филиала отыскивает в своей таблице маршрутизации маршрут к хосту, указывающий на ISP-интерфейс соединения по требованию.
8. Маршрутизатор филиала проверяет ISP-интерфейс соединения по требованию и обнаруживает, что он находится в отключенном состоянии.

9. Маршрутизатор филиала считывает конфигурационные параметры этого интерфейса.
10. На основе полученных параметров маршрутизатор филиала устанавливает соединение с местным ISP по модему или через ISDN-адаптер.
11. Установив соединение с ISP, маршрутизатор филиала посылает маршрутизатору центрального офиса пакет запроса на VPN-соединение.
12. После этого оба маршрутизатора согласуют параметры VPN-соединения. В процессе согласования маршрутизатор филиала посылает аутентификационные удостоверения, проверяемые маршрутизатором центрального офиса.
13. Маршрутизатор центрального офиса проверяет свои интерфейсы соединения по требованию и выбирает тот, чье имя совпадает с именем пользователя, указанным при аутентификации. Затем этот интерфейс переводится в подключенное состояние.
14. Маршрутизатор филиала отправляет пакеты по VPN-соединению, а VPN-сервер пересылает их на соответствующий адрес в корпоративной сети.

### **Статическая и динамическая маршрутизация**

Создав интерфейсы соединения по требованию и сделав выбор между временными и постоянными соединениями, Вы должны решить, каким способом следует добавлять информацию о маршрутах в таблицу маршрутизации.

1. В случае временных соединений Вы можете вручную добавить нужные статические маршруты, позволяющие достичь адресов в сетях других офисов. Этот вариант подходит для малых межсетевых сред с небольшим числом маршрутов.
2. В случае временных соединений Вы можете использовать механизм автостатических обновлений для периодического обновления статических маршрутов, обеспечивающих передачу пакетов по VPN-соединению между маршрутизаторами. Этот вариант хорошо работает в крупных межсетевых средах с большим количеством маршрутов.
3. В случае постоянных соединений разрешите функционирование нужных протоколов маршрутизации через VPN-соединение между маршрутизаторами. Протоколы будут считать это VPN-соединение каналом связи типа «точка-точка».

В отличие от маршрутизации с соединением по требованию на основе прямых физических подключений в данном случае IP-маршрут по умолчанию, созданный для VPN-интерфейса соединения по требованию, не годится для суммирования всех маршрутов интрасети, доступных через VPN. Поскольку маршрутизатор подключен к Интернету, маршрут по умолчанию должен суммировать все маршруты Интернета, и Вы должны настроить его на использование Интернет-интерфейса.

### **Аутентификация на основе общего ключа при использовании L2TP поверх IPSec для VPN-соединений между маршрутизаторами**

По умолчанию L2TP-клиент и L2TP-сервер Windows 2008 настраиваются на IPSec-аутентификацию на основе сертификатов. Когда Вы устанавливаете соединение L2TP поверх IPSec, автоматически создается политика IP-безопасности, заставляющая IKE (Internet Key Exchange) в процессе согласования параметров защиты для L2TP использовать аутентификацию на основе сертификатов. Это означает, что у L2TP-клиента и сервера должны быть машинные сертификаты. Они могут быть получены от центра сертификации (certificate authority, CA), либо на каждом компьютере должна быть установлена копия корневого сертификата CA другой стороны, полученная из хранилища доверенного корневого центра сертификации.

Иногда IPSec-аутентификация на основе сертификатов для VPN-соединений между маршрутизаторами с использованием L2TP нежелательна — например, когда у Вас небольшая организация и Вы не хотите развертывать инфраструктуру сертификации или

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

когда Вы подключаетесь к маршрутизаторам, не поддерживающим такой вид IPSec-аутентификации. В таких случаях Вы можете вручную создать политику IP-безопасности, заставляющую при установлении VPN-соединений между маршрутизаторами использовать общие ключи (pre-shared keys). Подобный ключ действует как простой пароль в IKE-процессе согласования: если обе стороны подтверждают, что им известен этот пароль, значит, они доверяют друг другу и могут продолжить согласование закрытых ключей симметричного шифрования и специфических параметров защиты L2TP-трафика.

Общий ключ IKE считается менее надежным, чем сертификаты, поскольку IKE-аутентификация (и неявное доверие) зависит лишь от одного ключа, значение которого хранится в политике IP-безопасности открытым текстом. Любой человек, просмотрев параметры этой политики, узнает значение общего ключа. Получив этот ключ, злоумышленник мог бы сконфигурировать свою систему в соответствии с параметрами IPSec Вашей системы. Однако L2TP-соединение требует проверки подлинности на уровне пользователя с применением одного из PPP-протоколов аутентификации. Поэтому для успешного установления соединения L2TP поверх IPSec одного общего ключа мало — нужно знать еще и учетные данные.

Для перехода на аутентификацию на основе общего ключа применительно к межмаршрутизаторным VPN-соединениям L2TP поверх IPSec нужно модифицировать реестр и соответственно настроить параметры политики IP-безопасности.

Чтобы запретить службе маршрутизации и удаленного доступа автоматически создавать политику IP-безопасности для L2TP-трафика, присвойте параметру ProhibitIPSec в разделе реестра HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\RasMan\Parameters значение 1. По умолчанию ProhibitIPSec равен 0.

Когда Вы меняете значение ProhibitIPSec на 1, параметры шифрования для интерфейса соединения по требованию на вызывающем маршрутизаторе замещаются параметрами шифрования из созданной Вами политики IP-безопасности. Перезагрузите компьютер, чтобы эти изменения вступили в силу.

Настройка IPSec зависит от следующего.

- Если VPN-сервер является автономным или входит в домен Windows NT 4.0, Вы должны настроить локальную политику IP-безопасности.
- Если VPN-сервер входит в домен Windows 2008, локальные политики IP-безопасности замещаются политиками IP-безопасности данного домена. Чтобы сформировать политику IP-безопасности, применяемую только к Вашему VPN-серверу, создайте в службе каталогов Active Directory организационную единицу (OU), включите в нее учетную запись компьютера VPN-сервера и используйте групповую политику для создания и назначения политик IP-безопасности для OU, в которую входит VPN-сервер. Тогда эти политики будут распространены на Ваш VPN-сервер.

Прежде чем создавать политику IP-безопасности, Вы должны решить, будут ли все подключаемые сайты использовать одинаковый общий ключ или для каждого соединения потребуется свой общий ключ. От этого решения зависит характер настройки списка фильтров IPSec и политики.

Одинаковый общий ключ приемлем, если обе конечные точки L2TP-туннеля контролируются одним администратором. Если же L2TP-туннели создаются между системами, управляемыми разными администраторами, желательно использовать отдельный общий ключ на каждое VPN-соединение. Так, единственный VPN-сервер Windows 2008 может быть настроен на коммуникационную связь с шестью бизнес партнерами, каждому из которых для L2TP-соединений понадобится свой общий ключ.

**Примечание** Если Ваш VPN-сервер Windows 2008 взаимодействует с другими L2TP-клиентами или серверами, используя IPSec-аутентификацию на основе сертификатов (она предлагается по умолчанию), но для одного из L2TP/IPSec-туннелей Вам нужна IP Sec-аутентификация на основе общего ключа, тогда Вы должны включить в политику IP-безопасности и правило для аутентификации на основе общего ключа, и правила для аутентификации на основе сертификатов (предназначенные для остальных систем).

## Виртуальные частные сети и брандмауэры

Брандмауэр (firewall) применяет фильтры пакетов, разрешая или запрещая передачу определенных видов сетевого трафика. Механизм фильтрации IP-пакетов позволяет точно определять, какой IP-трафик может проходить через брандмауэр. Фильтрация IP-пакетов очень важна при подключении частных интрасетей к общедоступным сетям вроде Интернета.

### Конфигурации VPN-сервера и брандмауэра

Существует два подхода к использованию брандмауэра в сочетании с VPN-сервером:

- VPN-сервер подключается к Интернету, а брандмауэр размещается между VPN-сервером и интрасетью;
- брандмауэр подключается к Интернету, а VPN-сервер размещается между брандмауэром и интрасетью.

### VPN-сервер перед брандмауэром

При размещении VPN-сервера перед брандмауэром, подключенным к Интернету (рисунок 19). Вы должны создать фильтры пакетов на Интернет-интерфейсе VPN-сервера, разрешающие передачу и прием только VPN-трафика.

Туннелированные данные входящего трафика расшифровываются VPN-сервером и пересылаются брандмауэру, и тот применяет к ним свои фильтры, пропуская в интрасеть лишь разрешенный трафик. Поскольку через VPN-сервер проходит только трафик, создаваемый аутентифицированными VPN-клиентами, брандмауэр в данном варианте используется исключительно для того, чтобы VPN-клиенты не могли обращаться к определенным ресурсам в интрасети. Так как единственный Интернет-трафик, разрешенный в интрасети, сначала проходит через VPN-сервер, в этом варианте блокируется и возможность доступа посторонних пользователей к FTP- или Web-ресурсам интрасети. Если Вы выбрали именно этот вариант, то должны сконфигурировать для Интернет-интерфейса VPN-сервера следующие входные и выходные фильтры. С этой целью используйте оснастку Routing and Remote Access.

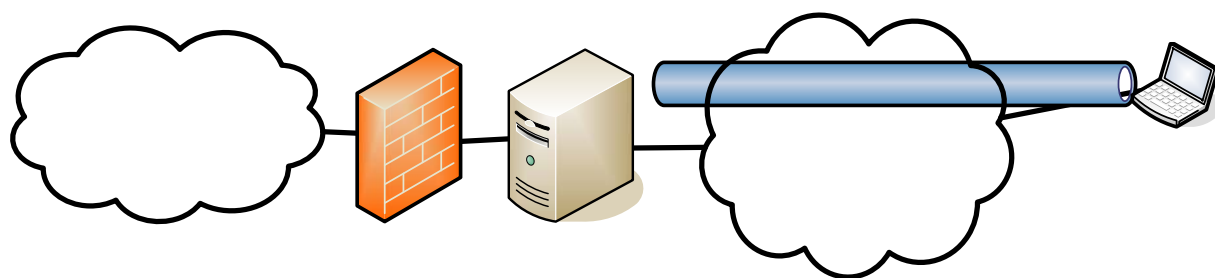


Рисунок 19

Настройка фильтров, в которых действие фильтра определено как Drop all packets except those that meet the criteria below.

	<b>Фильтрация пакетов для PPTP</b>	<b>Фильтры пакетов для L2TP поверх IPsec</b>
in	<ul style="list-style-type: none"> <li>• IP-адрес сети назначения для Интернет-интерфейса VPN-сервера, маска подсети - 255.255.255.255 и TCP-порт назначения - 1723 (0x06BB).</li> </ul> <p>Этот фильтр разрешает передачу управляющего PPTP-туннелями трафика от PPTP-клиента PPTP-серверу.</p> <ul style="list-style-type: none"> <li>• IP-адрес сети назначения для Интернет-интерфейса VPN-сервера, маска подсети — 255.255.255.255 и идентификатор IP-протокола — 47 (0x2F).</li> </ul> <p>Этот фильтр разрешает передачу данных, туннелированных средствами PPTP, от PPTP-клиента PPTP-серверу.</p> <ul style="list-style-type: none"> <li>• IP-адрес сети назначения для Интернет-интерфейса VPN-сервера, маска подсети — 255.255.255.255 и TCP-порт источника — 1723 (0x06BB); Вы должны выбрать вариант TCP [established] (TCP (установлено)).</li> </ul>	<ul style="list-style-type: none"> <li>• IP-адрес сети назначения для Интернет-интерфейса VPN-сервера, маска подсети - 255.255.255.255 и UDP-порт назначения - 500 (0x01F4).</li> </ul> <p>Этот фильтр разрешает передачу трафика IKE (Internet Key Exchange) на VPN-сервер.</p> <ul style="list-style-type: none"> <li>• IP-адрес сети назначения для Интернет-интерфейса VPN-сервера, маска подсети - 255.255.255.255 и UDP-порт назначения - 1701 (0x6A5).</li> </ul> <p>Этот фильтр разрешает передачу L2TP-трафика от VPN-клиента VPN-серверу.</p>
out	<ul style="list-style-type: none"> <li>• IP-адрес исходной сети для Интернет-интерфейса VPN-сервера, маска подсети - 255.255.255.255 и TCP-порт источника - 1723 (0x06BB).</li> </ul> <p>Этот фильтр разрешает передачу управляющего PPTP-туннелями трафика от PPTP-сервера PPTP-клиенту.</p> <ul style="list-style-type: none"> <li>• IP-адрес исходной сети для Интернет-интерфейса VPN-сервера, маска подсети — 255.255.255.255 и идентификатор IP-протокола — 47 (0x2F).</li> </ul> <p>Этот фильтр разрешает передачу данных, туннелированных средствами PPTP, от PPTP-сервера PPTP-клиенту.</p> <ul style="list-style-type: none"> <li>• IP-адрес исходной сети для Интернет-интерфейса VPN-сервера, маска подсети — 255.255.255.255 и TCP-порт назначения — 1723 (0x06BB); Вы должны выбрать вариант TCP [established].</li> </ul>	<ul style="list-style-type: none"> <li>• IP-адрес исходной сети для Интернет-интерфейса VPN-сервера, маска подсети - 255.255.255.255 и UDP-порт источника - 500 (0x01F4).</li> </ul> <p>Этот фильтр разрешает передачу трафика IKE от VPN-сервера.</p> <ul style="list-style-type: none"> <li>• IP-адрес исходной сети для Интернет-интерфейса VPN-сервера, маска подсети - 255.255.255.255 и UDP-порт источника - 1701 (0x6A5).</li> </ul> <p>Этот фильтр разрешает передачу L2TP-трафика от VPN-сервера VPN-клиенту.</p> <p>Для ESP-трафика применительно к IP-протоколу 50 никаких фильтров не требуется. После того как из пакета удаляется ESP-заголовок (модулем IPsec в TCP/IP), применяются фильтры службы маршрутизации и удаленного доступа.</p>

Этот фильтр нужен, только если VPN-сервер выступает в роли VPN-клиента (вызывающего маршрутизатора) при VPN-соединении между маршрутизаторами. Когда выбираете TCP [established], трафик принимается лишь в том случае, если VPN-сервер инициирует TCP-соединение,

## VPN-сервер за брандмауэром

В более распространенной конфигурации (рисунок 20) брандмауэр подключается непосредственно к Интернету, а VPN-сервер является одним из ресурсов интрасети в демилитаризованной зоне (demilitarized zone, DMZ). DMZ — это сегмент IP-сети, в котором обычно находятся ресурсы, доступные пользователям Интернета, например Web- и FTP-сервисы. Один из интерфейсов VPN-сервера подключается к DMZ, а другой — к интрасети.

При таком подходе для Интернет-интерфейса брандмауэра нужно создать входные и выходные фильтры, которые пропускают к VPN-серверу трафик, управляющий туннелями, и туннелированные данные. Дополнительные фильтры могут разрешать пропуск трафика к Web- и FTP-серверам, а также другим типам серверов и DMZ.

Поскольку у брандмауэра нет шифровальных ключей для VPN-соединений, он может осуществлять фильтрацию только па основе незашифрованных заголовков туннелированных данных, а значит, все туннелированные данные свободно проходят через брандмауэр. Однако это не создает проблем с безопасностью, так как VPN-соединения требуют аутентификации, которая блокирует попытки несанкционированного доступа.

Для Интернет-интерфейса брандмауэра нужно создать следующие входные и выходные фильтры (при этом используется программное обеспечение брандмауэра).

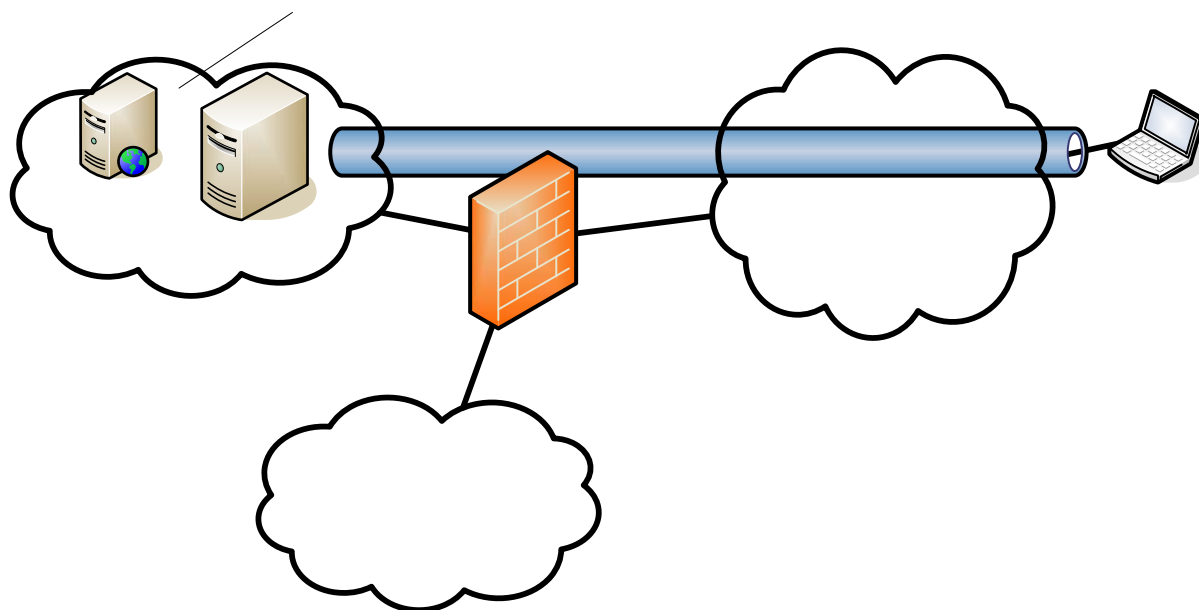


Рисунок 20

**DMZ**

Настройте фильтры, в которых действие фильтра определено как **Drop all packets except those that meet the criteria below.**

	Фильтрация пакетов для PPTP	Фильтры пакетов для L2TP поверх IPsec
in	<p>IP-адрес сети назначения для DMZ-интерфейса VPN-сервера и TCP-порт назначения - 1723. Этот фильтр разрешает передачу управляющего PPTP-туннелем трафика от PPTP-клиента PPTP-серверу.</p> <p>IP-адрес сети назначения для DMZ-интерфейса VPN-сервера и идентификатор IP-протокола — 47. Этот фильтр разрешает передачу данных, туннелированных средствами PPTP, от PPTP-клиента PPTP-серверу.</p> <p>IP-адрес сети назначения для DMZ-</p>	<p>IP-адрес сети назначения для DMZ-интерфейса VPN-сервера и UDP-порт назначения – 500.</p> <p>Этот фильтр разрешает передачу трафика IKE на VPN-сервер.</p> <p>IP-адрес сети назначения для DMZ-интерфейса VPN-сервера и идентификатор IP-протокола — 50.</p> <p>Этот фильтр разрешает передачу ESP-трафика от PPTP-клиента PPTP – серверу.</p>

**WEB-server**

**VPN-server**



Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

	интерфейса VPN-сервера и TCP-порт источника — 1723; Вы должны выбрать вариант TCP [established] (TCP[установлено]).	
out	<p>IP-адрес исходной сети для DMZ-интерфейса VPN-сервера и TCP-порт источника - 1723.</p> <p>Этот фильтр разрешает передачу управляющего PPTP-туннелями трафика от PPTP-сервера PPTP-клиенту.</p> <p>IP-адрес исходной сети для DMZ-интерфейса VPN-сервера и идентификатор IP-протокола — 47.</p> <p>Этот фильтр разрешает передачу данных, туннелированных средствами PPTP, от PPTP-сервера PPTP-клиенту.</p> <p>IP-адрес исходной сети для DMZ-интерфейса VPN-сервера и TCP-порт назначения - 1723; Вы должны выбрать вариант TCP [established].</p>	<p>IP-адрес исходной сети для DMZ-интерфейса VPN-сервера и UDP-порт источника - 500.</p> <p>Этот фильтр разрешает передачу трафика IKE от VPN-сервера.</p> <p>IP-адрес исходной сети для DMZ-интерфейса VPN-сервера и идентификатор IP-протокола-50.</p> <p>Этот фильтр разрешает передачу ESP-трафика от VPN-сервера VPN-клиенту.</p> <p>Для L2TP-трафика, направляемого в UDP-порт 1701, никаких фильтров не требуется. На брандмауэре весь L2TP-трафик, в том числе управляющий туннелями и туннелированные данные, зашифровывается как полезная нагрузка IPSec-протокола ESP</p>

## Виртуальные частные сети и NAT

Транслятор сетевых адресов (network address translator. NAT) — это IP-маршрутизатор, способный транслировать IP-адреса и номера TCP/UDP-портов в пересылаемых пакетах.

По умолчанию NAT транслирует IP-адреса и TCP/UDP-порты. Если информация об IP-адресе и портах содержится только в IP- и TCP/UDP-заголовках, никаких проблем трансляция не вызывает. Пример - HTTP-трафик в Web. Однако некоторые приложения и протоколы хранят информацию об IP-адресах и TCP/UDP-портах в собственных заголовках. FTP, например, записывает точечное десятичное представление IP-адресов в FTP-заголовке для использования командой FTP port. Если NAT неправильно преобразует IP-адрес в FTP-заголовке, может возникнуть проблема с поддержкой соединений. Более того, некоторые протоколы для идентификации потоков данных используют не TCP- или UDP-заголовки, а поля в других заголовках. Когда компоненту NAT приходится выполнять дополнительные преобразования и учитывать полезные данные не только в IP-, TCP- и UDP-заголовках, нужен NAT-редактор. Этот редактор так модифицирует иначе не транслируемые данные, чтобы NAT мог пересылать их на правильные адреса.

Чтобы туннели PPTP и L2TP поверх IPSec могли работать через NAT, последний должен корректно обрабатывать множество потоков данных, поступающих на единственный IP-адрес или передаваемых с него.

### ***PPTP-трафик***

PPTP-трафик связан с TCP-соединением, используемым для управления туннелем, и с инкапсуляцией туннелированных данных в GRE-пакеты. Первая часть PPTP-трафика корректно транслируется самим NAT, а вторая часть — только в комбинации со специфическим NAT-редактором. В туннелированных данных конкретный туннель определяется по IP-адресу источника и полю идентификатора вызова в GRE-заголовке. Когда к одному PPTP-серверу обращается несколько PPTP-клиентов, расположенных в частной сети за NAT, весь туннелированный трафик имеет один и тот же IP-адрес источника. Кроме того, поскольку PPTP-клиенты ничего не знают о трансляции адресов, они могут выбрать одинаковые идентификаторы вызова при создании PPTP-туннеля. Во избежание этой проблемы NAT-редактор для PPTP должен отслеживать формирование PPTP-туннелей и создавать отдельные сопоставления частных IP-адресов и идентификаторов вызова, используемых PPTP-клиентами, с общим IP-адресом и уникальными идентификаторами вызова, принимаемыми PPTP-сервером в Интернете. Протокол маршрутизации NAT, поддерживаемый службой маршрутизации и удаленного доступа, предоставляет NAT-редактор для PPTP, который преобразует GRE-поля идентификаторов вызова, и это позволяет различать PPTP-туннели, создаваемые клиентами частной сети за NAT.

### ***Трафик L2TP поверх IPSec***

Этот трафик не обрабатывается NAT, потому что номер UDP-порта в нем зашифрован и его значение защищено криптографической контрольной суммой. Трафик L2TP поверх IPSec не транслируется даже с помощью NAT-редактора по причинам, изложенным ниже.

### **Нельзя различить потоки данных IPSec-протокола ESP**

ESP-заголовок содержит поле индекса параметров безопасности (security parameters index, SPI). SPI используется — в сочетании с IP-адресом назначения в незашифрованных IP-заголовке и заголовке одного из IPSec-протоколов (ESP или AH) — для идентификации IPSec-сопоставления безопасности (SA).

В исходящем от NAT трафике IP-адрес назначения не изменяется, а во входящем в NAT трафике этот адрес должен быть преобразован в частный. Как и в случае нескольких PPTP-клиентов в частной сети за NAT, IP-адрес назначения в нескольких входящих потоках данных IPSec-протокола ESP тоже одинаков. Чтобы отличить один поток от другого, исходные IP-адрес назначения и SPI следовало бы транслировать в частные IP-адрес назначения и SPI. Однако из-за того, что в концевой части ESP Authentication содержится криптографическая контрольная сумма, удостоверяющая подлинность ESP-заголовка и полезных данных, изменять SPI нельзя - иначе эта контрольная сумма будет модифицирована.

### **Нельзя модифицировать контрольные суммы TCP и UDP**

В пакетах «L2TP поверх IPSec» каждый UDP- и TCP-заголовок содержит контрольную сумму, включающую IP-адреса источника и назначения, взятые из незашифрованного IP-заголовка. Это означает, что Вы не можете изменить адреса в незашифрованном IP-заголовке, не изменив контрольные суммы в TCP- и UDP-заголовках. А обновлять эти контрольные суммы нельзя, потому что они входят в зашифрованную часть полезных данных ESP.

## Сквозные VPN-соединения

Сквозная VPN (pass-through VPN) позволяет клиенту удаленного доступа, подключенному к интрасети одной компании, обращаться через Интернет к ресурсам в интрасети другой компании. VPN-соединение удаленного доступа к одной интрасети проходит через другую интрасеть и Интернет.

В типичном случае компании А и В являются бизнес-партнерами, и сотрудники компании А посещают сетевые ресурсы компании В. Когда сотрудник компании А, участвующий в совместном совещании, подключает свой портативный компьютер к интрасети компании В, его система получает информацию о конфигурации IP-адресов в этой интрасети. Если этому сотруднику нужно подключиться к интрасети своей компании, это делается одним из двух способов.

- По телефонной линии в комнате совещаний сотрудник компании А может либо напрямую подключиться к серверу удаленного доступа этой компании и установить соединение удаленного доступа с ее интрасетью, либо связаться с местным ISP и создать VPN-соединение с интрасетью компании А.
- Как показано на рисунке 21, технология VPN и соответствующая инфраструктура позволяют сотруднику компании А создать туннель через интрасеть компании В в Интернет, а затем создать другой туннель — через интрасеть компании В и Интернет в интрасеть компании А.

При втором способе VPN-соединение с интрасетью компании А создается за счет активизации двух объектов подключения и использования существующего локального физического сетевого соединения. Заметьте, что второй туннель формируется внутри первого.

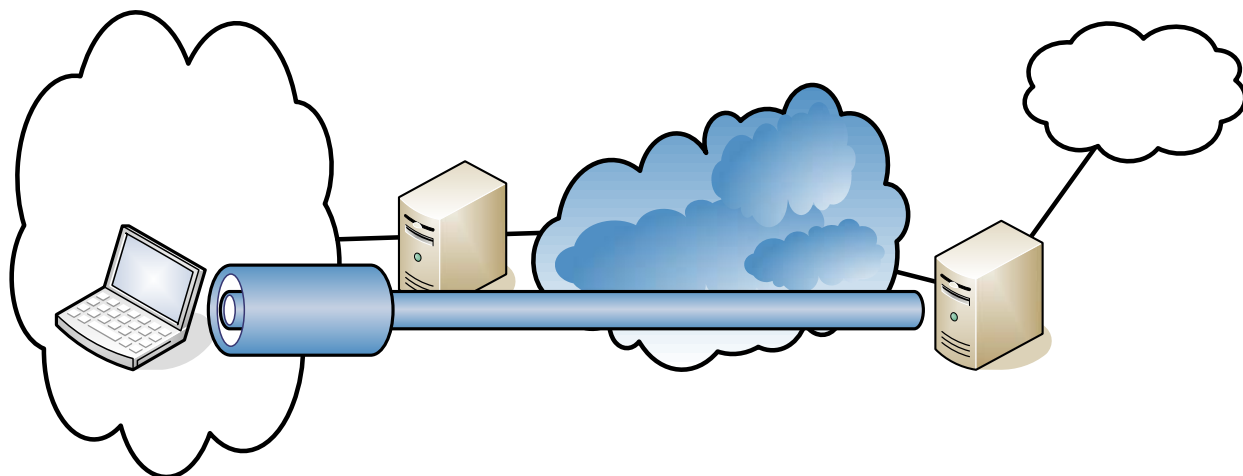


Рисунок 21

Как только будет установлено сквозное VPN-соединение сотрудник компании А сможет обращаться к любому сетевому ресурсу своей компании.

Чтобы создать сквозное соединение:

Данная процедура предназначена для сотрудника компании А, который создает сквозное VPN-соединение с VPN-сервером компании А, подключенным к Интернету.

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

1. Дважды щелкните объект соединения, создающий туннель с VPN-сервером компании В в ее интрасети.
2. Когда появится приглашение, введите учетные данные, которые соответствуют специальной пользовательской учетной записи, созданной в компании В.
3. Дважды щелкните объект соединения, создающий VPN с VPN-сервером компании А в Интернете.
4. Когда появится приглашение, введите учетные данные, которые соответствуют Вашей пользовательской учетной записи, имеющейся в компании А.

### **Конфигурирование VPN-сервера компании А**

Настройте VPN-сервер компании А на прием VPN-соединений удаленного доступа от клиентов через Интернет и создайте политики удаленного доступа, требующие наиболее защищенные типы аутентификации и шифрования.

### **Конфигурирование VPN-сервера компании В**

Настройте VPN-сервер компании В следующим образом.

1. Сконфигурируйте этот VPN-сервер на прием VPN-соединений удаленного доступа.
2. Создайте ручную пул общих IP-адресов.
3. Создайте группу Windows 2008 для пользовательских учетных записей сотрудников другой компании, устанавливающих сквозные VPN-соединения, например, группу VPN\_PassThrough.
4. Создайте пользовательские учетные записи для сотрудников компании А.

Если сквозные VPN-соединения сотрудников из других компаний обслуживаются только этим VPN-сервером, удалите политику по умолчанию **Allow access if dialin permission is enabled** и создайте свою, назвав ее, например, VPN PassThrough for Business Partners. В этой политике нужно установить разрешение на удаленный доступ как **Grant remote access permission**. Потом задайте условия и параметры профиля, как показано в таблицах 3 и 4. Параметры политики удаленного доступа, перечисленные в таблицах 3 и 4, предполагают управление удаленным доступом на основе групп. С этой целью во всех пользовательских учетных записях нужно установить разрешение на удаленный доступ как **Control access through Remote Access Policy**.

Таблица 3, Условия политики удаленного доступа для VPN-сервера компании В

NAS-Port- Type	Virtual (VPN)
Called- Station-ID	IP-адрес интерфейса VPN-сервера, принимающего VPN-соединения
Windows- Groups	Например, VPN_PassThrough

Таблица 4. Параметры профиля политики удаленного доступа для VPN-сервера компании В

Authentication	Установите флажок Microsoft Encrypted Authentication (MS-CHAP)
Encryption	Выберите Basic, Strong или No encryption

Шифрование первого туннеля (от сотрудника компании А до VPN-сервера компании В) излишне и может отрицательно повлиять на производительность.

### Настройка фильтрации

Drop all packets except those that meet the criteria below

	Фильтрация пакетов для PPTP	Фильтры пакетов для L2TP поверх IPsec
in	<p><u>Интерфейс интрасети</u> IP-адрес сети назначения, маска подсети 32 и TCP-порт назначения - 1723. IP-адрес сети назначения, маска подсети 32 и идентификатор IP-протокола - 47.</p> <p><u>Интернет-интерфейс</u></p> <ul style="list-style-type: none"> <li>• IP-адрес сети назначения и маску подсети для пула общих IP-адресов, а также TCP-порт источника - 1723.</li> <li>• IP-адрес сети назначения и маску подсети для пула общих IP-адресов, а также идентификатор IP-протокола - 47.</li> </ul>	<p><u>Интерфейс интрасети</u> IP-адрес сети назначения, маска подсети - 32 и UDP-порт назначения - 1701. IP-адрес сети назначения, маска подсети - 32 и UDP-порт назначения - 500.</p> <p><u>Интернет-интерфейс</u> IP-адрес сети назначения и маску подсети для пула общих IP-адресов, а также идентификатор IP-протокола - 50. IP-адрес сети назначения и маску подсети для пула общих IP-адресов, а также UDP-порт источника - 500.</p>
out	<p><u>Интерфейс интрасети</u> IP-адрес исходной сети, маска подсети - 32 и TCP-порт источника - 1723. IP-адрес исходной сети, маска подсети - 32 и идентификатор IP-протокола - 47.</p> <p><u>Интернет-интерфейс</u> IP-адрес исходной сети и маску подсети для пула общих IP-адресов, а также TCP-порт назначения - 1723. IP-адрес исходной сети и маску подсети для пула общих IP-адресов, а также идентификатор IP-протокола - 47.</p>	<p><u>Интерфейс интрасети</u> IP-адрес исходной сети, маска подсети - 32 и UDP-порт источника - 1701. IP-адрес исходной сети, маска подсети - 32 и UDP-порт источника - 500.</p> <p><u>Интернет-интерфейс</u> IP-адрес исходной сети и маску подсети для пула общих IP-адресов, а также идентификатор IP-протокола - 50. IP-адрес исходной сети и маску подсети для пула общих IP-адресов, а также UDP-порт назначения - 500.</p>

### Настройка компьютера VPN-клиента на использование сквозной VPN

	Чтобы настроить PPTP-соединение:	Чтобы настроить соединение L2TP поверх IPsec:
1	<p>Создать объект VPN-соединения, подключающий сотрудника компании А к VPN-серверу комп. В:</p> <ul style="list-style-type: none"> <li>• на вкладке <b>General</b> введите хост имя или IP-адрес интерфейса интрасети VPN-сервера компании В;</li> <li>• на вкладке <b>Security</b> выберите шифрование только пароля;</li> <li>• на вкладке <b>Networking</b> выберите в качестве типа сервера <b>Point-to-Point Tunneling</b></li> </ul>	<p>Создать объект VPN-соединения, подключающий сотрудника компании А к VPN-серверу комп. В:</p> <ul style="list-style-type: none"> <li>• на вкладке <b>General</b> введите хост-имя или IP-адрес интерфейса интрасети VPN-сервера компании В;</li> <li>• на вкладке <b>Security</b> выберите шифрование только пароля;</li> <li>• на вкладке <b>Networking</b> выберите в качестве типа сервера <b>Layer-2 Tunneling</b></li> </ul>

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

	<b>Protocol (PPTP).</b>	<b>Protocol (L2TP).</b>
2	<p>Создать объект VPN-соединения, подключающий сотрудника компании А к VPN-серверу комп. А:</p> <ul style="list-style-type: none"> <li>• на вкладке <b>General</b> введите хост-имя или IP-адрес Интернет-интерфейса VPN-сервера компании А;</li> <li>• на вкладке <b>Security</b> выберите либо шифрование пароля и данных, либо переключатель <b>Custom</b>. Выбрав <b>Custom</b>, необходимо указать подходящие параметры шифрования и аутентификации;</li> <li>• на вкладке <b>Networking</b> выберите в качестве типа сервера <b>Point-to-Point Tunneling Protocol (PPTP)</b>.</li> </ul>	<p>Создать объект VPN-соединения, подключающий сотрудника компании А к VPN-серверу комп. А:</p> <ul style="list-style-type: none"> <li>• на вкладке <b>General</b> введите хост-имя или IP-адрес Интернет-интерфейса VPN-сервера компании А;</li> <li>• на вкладке <b>Security</b> выберите либо шифрование пароля и данных, либо переключатель <b>Custom</b>. Выбрав <b>Custom</b>, Вы должны указать подходящие параметры шифрования и аутентификации;</li> <li>• на вкладке <b>Networking</b> выберите в качестве типа сервера <b>Layer-2 Tunneling Protocol (L2TP)</b>.</li> </ul>

## Выявление и устранение проблем

Устанавливая причины проблем с виртуальными частными сетями, необходимо проверить поддержку IP-соединений, процессы установления соединений по требованию и удаленного доступа, маршрутизацию и IPSec.

### Наиболее распространенные проблемы с VPN

Проблемы с VPN, как правило, делятся на несколько категорий:

- запрос на соединение отклоняется, хотя должен быть принят;
- запрос на соединение принимается, хотя должен быть отклонен;
- адреса за VPN-сервером недостижимы;
- не удается создать туннель.

Ниже даются рекомендации по устранению ошибок в конфигурации или инфраструктуре, вызывающих эти проблемы с VPN.

#### Запрос на соединение отклоняется, хотя должен быть принят

1. Используя команду `ping`, проверьте, возможно ли соединение с VPN-сервером по его хост-имени или IP-адресу. Если Вы имеете дело с хост-именем, проверьте, правильно ли оно разрешается в IP-адрес. Если выполнение команды `ping` заканчивается неудачей, то, возможно, фильтрация пакетов препятствует передаче ICMP-сообщений на VPN-сервер или от него;
2. Убедитесь, что на VPN-сервере работает служба маршрутизации и удаленного доступа;
3. В случае VPN-соединений удаленного доступа убедитесь, что на VPN-сервере разрешен удаленный доступ. В случае VPN-соединений между маршрутизаторами проверьте, настроен ли VPN-сервер на маршрутизацию с соединением по требованию;
4. В случае VPN-соединений удаленного доступа убедитесь, что PPTP- и L2TP-порты настроены на прием входящих соединений удаленного доступа. В случае VPN-соединений между маршрутизаторами проверьте, настроены ли PPTP- и L2TP-порты на входящие и исходящие соединения по требованию. Убедитесь, что VPN-клиент и сервер, на котором действует политика удаленного доступа, используют хотя бы один общий метод аутентификации и/или шифрования;
5. Убедитесь, что параметры запроса на соединение согласуются с параметрами политик удаленного доступа;

Для успешного установления соединения параметры в запросе на соединение должны:

- соответствовать всем условиям но крайней мере одной политики удаленного доступа;
  - предоставлять право на удаленный доступ либо через **Allow access** в пользовательской учетной записи, либо через **Control access through Remote Access Policy** в пользовательской учетной записи и **Grant remote access permission** в политике удаленного доступа;
  - соответствовать всем параметрам профиля;
  - соответствовать всем параметрам входящих звонков в свойствах пользовательской учетной записи;
6. Убедитесь, что настройки в профиле политики удаленного доступа не конфликтуют со свойствами VPN-сервера. Профиль политики удаленного доступа и свойства VPN-сервера предусматривают настройки для:



Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

- многоканальных подключений;
- протокола VAP;
- протоколов аутентификации.

Если настройки в профиле соответствующей политики удаленного доступа конфликтуют со свойствами VPN-сервера, запрос на соединение будет отклонен. Например, если в профиле указан протокол аутентификации EAP-TLS, по этот протокол в свойствах VPN-сервера не включен, последний будет отклонять запросы на соединение;

7. Если VPN-сервер является рядовым сервером в домене Windows 2008, который работает в смешанном или основном режиме и сконфигурирован на аутентификацию через Windows 2008, убедитесь, что:
  - в службе каталогов Active Directory имеется группа безопасности RAS and IAS Servers (Серверы RAS и IAS). Если этой группы нет, создайте ее, указав тип Security и область действия Domain local;
  - у группы безопасности RAS and IAS Servers имеется разрешение на чтение объекта RAS and IAS Servers Access Check;
  - учетная запись компьютера VPN-сервера включена в группу безопасности RAS and IAS Servers. Для просмотра текущих регистраций используйте команду *netsh ras show registeredserver*, а для регистрации сервера в определенном домене — команду *netsh ras add registeredserver*;
  - Если Вы добавляете компьютер VPN-сервера в группу безопасности RAS and IAS Servers или удаляете из нее, изменения не вступают в силу немедленно (из-за особенностей кэширования информации службы каталогов Active Directory в Windows 2008). Чтобы изменения немедленно вступили в силу, перезагрузите этот компьютер.
8. В случае VPN-соединений удаленного доступа убедитесь, что LAN-протоколы, используемые VPN-клиентами, настроены на удаленный доступ;
9. Убедитесь, что на VPN-сервере есть свободные PPTP- или L2TP-порты. При необходимости увеличьте количество этих портов;
10. Проверьте, поддерживается ли VPN-сервером протокол туннелирования, используемый VPN-клиентом.

По умолчанию VPN-клиенты удаленного доступа Windows 2008 настроены на автоматический выбор типа сервера, т. е. сначала они пытаются установить VPN-соединение на основе L2TP поверх IPSec, а затем, если первое не удастся - VPN-соединение на основе PPTP. Если на VPN-клиенте тип сервера выбран как Point-to-Point Tunneling Protocol (PPTP) или Layer-2 Tunneling Protocol (L2TP), проверьте, поддерживается ли VPN-сервером выбранный протокол туннелирования.

По умолчанию компьютер под управлением Windows 2008 Server и службы маршрутизации и удаленного доступа является PPTP- и L2TP-сервером с пятью L2TP-портами и пятью PPTP-портами. Чтобы создать только PPTP-сервер, укажите, что число L2TP-портов равно 0. А чтобы создать только L2TP-сервер, укажите, что число PPTP-портов равно 0;

11. В случае VPN-соединений удаленного доступа на основе L2TP поверх IPSec убедитесь, что на VPN-клиенте и сервере установлены сертификаты компьютеров, также называемые машинными сертификатами;
12. Проверьте в удостоверениях (учетных данных) VPN-клиента правильность имени и пароля пользователя, а также имени домена и убедитесь, что они могут быть проверены VPN-сервером;

13. Если VPN-сервер настроен на использование статического пула IP-адресов, проверьте, достаточно ли адресов в пуле. Если все адреса из статического пула уже выделены VPN-клиентам, VPN-сервер не сможет назначить очередной IP-адрес. Если VPN-клиент сконфигурирован на использование только TCP/IP, запрос на соединение будет отклонен;
14. Если VPN-клиент требует выделить ему определенный номер IPX-узла, убедитесь, что VPN-сервер разрешает это делать;
15. Если VPN-сервер удаленного доступа настроен на диапазон номеров IPX-сетей, убедитесь, что эти номера не используются где-нибудь в другой части межсетевой IPX-среды;
16. Проверьте конфигурацию службы аутентификации. VPN-сервер может быть настроен на аутентификацию удостоверений VPN-клиентов либо через Windows, либо через RADIUS;
17. Если VPN-сервер является рядовым сервером в домене Windows 2008 основного режима, убедитесь, что он присоединился к домену;
18. Если VPN-сервер под управлением Windows NT 4.0 с Service Pack 4 и выше является членом домена Windows 2008 смешанного режима или если VPN-сервер под управлением Windows 2008 включен в домен Windows NT 4.0, считывающий параметры пользовательских учетных записей из доверяемого домена Windows 2008, проверьте, включена ли группа Everyone (Все) в группу Pre-Windows 2000 Compatible Access. Для этого воспользуйтесь командой net localgroup «Pre-Windows 2000 Compatible Access». В случае отрицательного результата введите команду net localgroup «Pre-Windows 2000 Compatible Access» everyone /add на контроллере домена и перезагрузите его;
19. Если VPN-сервер под управлением Windows NT 4.0 с Service Pack 3 и ниже является членом домена Windows 2008 смешанного режима, убедитесь, что группе Everyone предоставлены права на перечисление содержимого (list contents), чтение всех свойств (read all properties) и чтение (read) до корневого узла Вашего домена и всех подобъектов (sub-objects) корневого домена;
20. В случае аутентификации через RADIUS проверьте, взаимодействует ли компьютер VPN-сервера с сервером RADIUS;
21. В случае PPTP-соединения с использованием MS-CHAP v1 и MPPE с 40-битным ключом убедитесь, что длина пароля не превышает 14 символов.

#### **Запрос на соединение принимается, хотя должен быть отклонен**

1. Убедитесь, что данные параметры соединения запрещены в политиках удаленного доступа. Чтобы запрос на соединение отклонялся, его параметры должны быть запрещены одним из двух способов: в свойствах учетной записи выберите переключатель либо Deny access, либо Control access through Remote Access Policy. Но в последнем случае разрешение на удаленный доступ в первой политике удаленного доступа, соответствующей параметрам запроса на соединение, укажите как Deny remote access permission.

#### **Адреса за VPN-сервером недостижимы**

1. Убедитесь, что LAN-протоколы, используемые VPN-клиентами, либо поддерживают маршрутизацию, либо позволяют обращаться к сети, к которой подключен VPN-сервер.
2. Проверьте настройки распределения IP-адресов VPN-сервером.

Если VPN-сервер настроен на использование статического пула IP-адресов, проверьте, достижимы ли адреса из этого пула хостами и маршрутизаторами

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

интрасети. Если нет, добавьте на маршрутизаторы интрасети IP-маршрут, соответствующий статическому пулу IP-адресов VPN-сервера (пул определяется по IP-адресу и маске диапазона), или включите на VPN-сервере подходящий протокол маршрутизации. Если маршруты к подсетям VPN-клиентов удаленного доступа отсутствуют, эти клиенты не смогут получать трафик из интрасети. Маршруты к подсетям указываются либо статически, либо определяются протоколом маршрутизации (OSPF или IP).

Если VPN-сервер настроен на выделение IP-адресов через DHCP, а DHCP-сервер недоступен, VPN-сервер выделяет адреса из диапазона 169.254.0.1-169.254.255.254, зарезервированного для автоматического назначения частных IP-адресов (APIPA). Функция APIPA применима к VPN-клиентам удаленного доступа только в том случае, если в сети, к которой подключен VPN-сервер, тоже используются адреса, назначаемые APIPA.

Если VPN-сервер использует APIPA при доступном DHCP-сервере, проверьте, правильно ли выбран адаптер для получения IP-адресов от DHCP-сервера. По умолчанию VPN-сервер выбирает такой адаптер случайным образом. Если на компьютере имеется несколько сетевых адаптеров, служба маршрутизации и удаленного доступа может выбрать сетевой адаптер, через который DHCP-сервер недоступен. Вы можете сами выбрать подходящий сетевой адаптер на вкладке IP в окне свойств сервера удаленного доступа (через оснастку Routing and Remote Access). Если диапазон IP-адресов статического пула является подмножеством диапазона IP-адресов сети, к которой подключен VPN-сервер, убедитесь, что диапазоны IP-адресов из статического пула не назначаются другим TCP/IP-хостам ни статически, ни через DHCP.

3. В случае VPN-соединений между маршрутизаторами убедитесь, что на обеих сторонах такого VPN-соединения имеются маршруты, обеспечивающие двухсторонний обмен трафиком.

В отличие от VPN-соединения удаленного доступа VPN-соединение между маршрутизаторами не приводит к автоматическому созданию маршрута по умолчанию. Вы должны сами создать соответствующие маршруты на обеих сторонах VPN-соединения между маршрутизаторами, чтобы можно было перенаправлять трафик, передаваемый другой стороне соединения или принимаемый от нее.

Вы можете добавлять статические маршруты в таблицу маршрутизации либо вручную, либо через протоколы маршрутизации. В последнем случае для постоянных VPN-соединений можно использовать OSPF или RIP, а для VPN-соединений по требованию — механизм автостатических обновлений.

4. В случае VPN-соединения между маршрутизаторами, инициируемого любой из сторон (two-way initiated router-to-router VPN connection), убедитесь, что оно не воспринимается VPN-сервером как соединение удаленного доступа.

Если имя пользователя из удостоверений вызывающего маршрутизатора появляется в папке Remote Access Clients (Клиенты удаленного доступа) оснастки Routing and Remote Access, значит, VPN-сервер считает вызывающий маршрутизатор клиентом удаленного доступа. Убедитесь, что имя пользователя в удостоверениях вызывающего маршрутизатора совпадает с именем интерфейса соединения по требованию на VPN-сервере.

5. В случае межмаршрутизаторного VPN-соединения по требованию, инициируемого только одной из сторон (one-way initiated router-to-router VPN connection), убедитесь, что маршруты интрасети вызывающего маршрутизатора сконфигурированы как статические (в параметрах входящих звонков в свойствах пользовательской учетной записи, применяемой этим маршрутизатором).

6. Убедитесь, что фильтры TCP/IP-пакетов в профиле политики удаленного доступа на VPN-сервере не препятствуют передаче или приему необходимого TCP/IP-трафика. Учтите, что эти фильтры могут быть сконфигурированы на сервере RADIUS, если используется служба проверки подлинности в Интернете (IAS).
7. В случае VPN-соединений по требованию проверьте, не установлены ли на интерфейсах соединений по требованию вызывающего и отвечающего маршрутизаторы фильтры пакетов, препятствующие передаче или приему нужного трафика.

### Не удается создать туннель

1. Убедитесь, что фильтрация пакетов на интерфейсе маршрутизатора между VPN-клиентом и сервером не препятствует пересылке трафика протокола туннелирования.

На VPN-сервере Windows 2008 фильтрация IP-пакетов настраивается в окне дополнительных параметров TCP/IP и в оснастке Routing and Remote Access. Проверьте оба этих места — возможно, какие-то фильтры блокируют трафик VPN-соединения.

2. Убедитесь, что на VPN-клиенте не работает клиент Winsock Proxy. Если он активен, вызовы API-функций Winsock, используемые, в частности, для создания туннелей и передачи туннелированных данных, перехватываются и перенаправляются сконфигурированному прокси-серверу. Компьютер с прокси-сервером позволяет организации получать доступ к специфическим типам Интернет-ресурсов (обычно Web и FTP) без прямого подключения к Интернету. При этом организация использует выделяемые InterNIC идентификаторы частных сетей (например, 10.0.0.0/8).

Прокси-серверы обычно применяются для того, чтобы пользователи внутри организации могли обращаться к общедоступным Интернет-ресурсам так, будто они напрямую подсоединены к Интернету. В то же время VPN-соединения, как правило, предназначены для того, чтобы авторизованные пользователи из Интернета могли обращаться к ресурсам частной сети организации так, будто они напрямую подключены к этой сети. Единственный компьютер может выступать и в роли прокси-сервера (для пользователей частной сети), и в роли VPN-сервера (для авторизованных пользователей из Интернета).

## Средства диагностики

С Windows 2008 поставляются средства диагностики, позволяющие собирать дополнительную информацию об источниках проблем с VPN.

### Причина недоступности

Если установить соединение по требованию не удастся, интерфейс соединения по требованию остается в недостижимом состоянии. Служба маршрутизации и удаленного доступа Windows 2008 регистрирует причину, по которой не удалось установить соединение, в параметре **Unreachability reason** (Причина недоступности).

Информация, указанная в этом параметре, поможет Вам локализовать источник проблем.

### Протоколирование событий

На вкладке **Event logging** (Журнал событий) окна свойств VPN-сервера предлагается четыре уровня протоколирования. Выберите переключатель **Log the maximum amount of information** (Вести журнал всех событий) и повторите попытку соединения. Как только попытка закончится неудачей, проверьте, какие события были зарегистрированы в

системном журнале при попытке соединения. Просмотрев события, выберите на вкладке Event logging переключатель **Log errors and warnings** (Вести журнал ошибок и предупреждений).

### **Трассировка**

Средства трассировки записывают последовательность вызываемых функций в файл. Разрешите применение трассировки для записи детальной информации о процессах, выполняемых при установлении соединений удаленного доступа и компонентами VPN.

Закончив трассировку и просмотрев нужную информацию, верните параметрам трассировки исходные значения.

Трассировочная информация может оказаться сложной и очень летальной. Часть ее полезна только инженерам службы технической поддержки Microsoft или сетевым администраторам, имеющим большой опыт работы со службой маршрутизации и удаленного доступа. Трассировочную информацию можно сохранить в виде

файлов и послать в службу технической поддержки Microsoft для анализа.

### **Network Monitor**

Network Monitor (Сетевой монитор) — это программа для захвата пакетов и их анализа, которая позволяет наблюдать за трафиком, передаваемым между VPN-сервером и VPN-клиентом в процессе установления VPN-соединения и при передаче данных. Network Monitor не анализирует зашифрованную часть VPN-трафика.

Правильная интерпретация связанного с VPN и удаленным доступом трафика требует глубокого понимания PPP, PPTP IPSec и других протоколов. Информацию, захваченную Network Monitor, можно сохранить в виде файлов для дальнейшего анализа.

## Практическая часть

### LAB 1. VPN-соединение удаленного доступа

#### Задание:

Установим VPN-соединение удаленного доступа на примере сети, показанной на рисунке 22.

VPN-сервер отделяет частную сеть с адресным пространством 192.168.x.x/24 от Интернета (195.19.x.x/24).

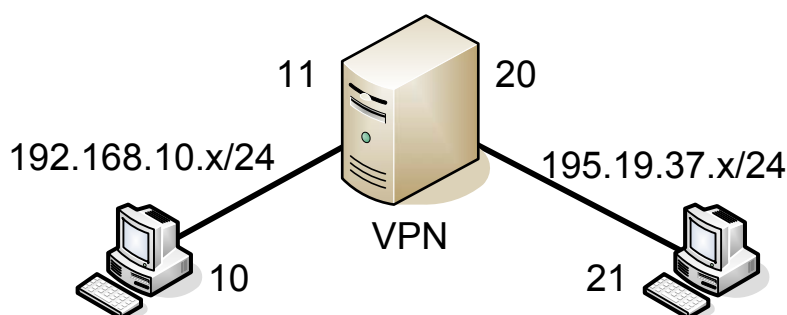


Рисунок 22

#### План выполнения работы:

- Выполним сетевые настройки: 2 адаптера одной сети, 2 – другой.
- Убедимся в работоспособности сети с компа 2:
- Установим сервер VPN.
- Добавим специальную учетную запись remote (password: 1) на сервере.
- Настроим клиента на VPN-сервере
- Итоги, изучение результата

Для идентификации машин выделим им псевдоимена, имеющие свое действие исключительно для сопоставления настроек определенной машине, рисунок 23.

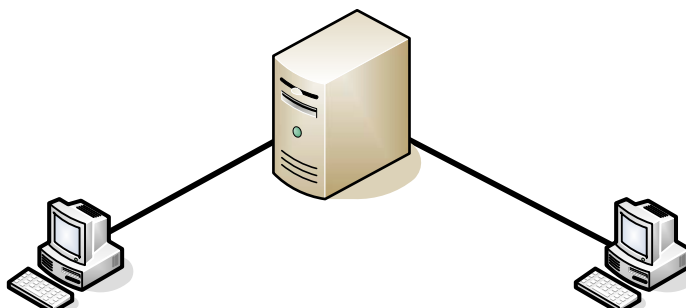


Рисунок 23

Ниже приведено визуальное исполнение лабораторной работы.

### Сетевые настройки.

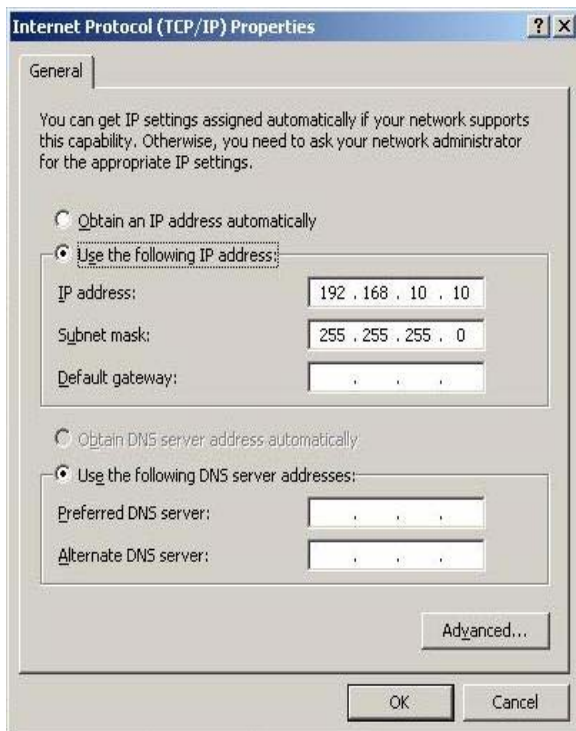


Рисунок 24. IP-адреса Comp1

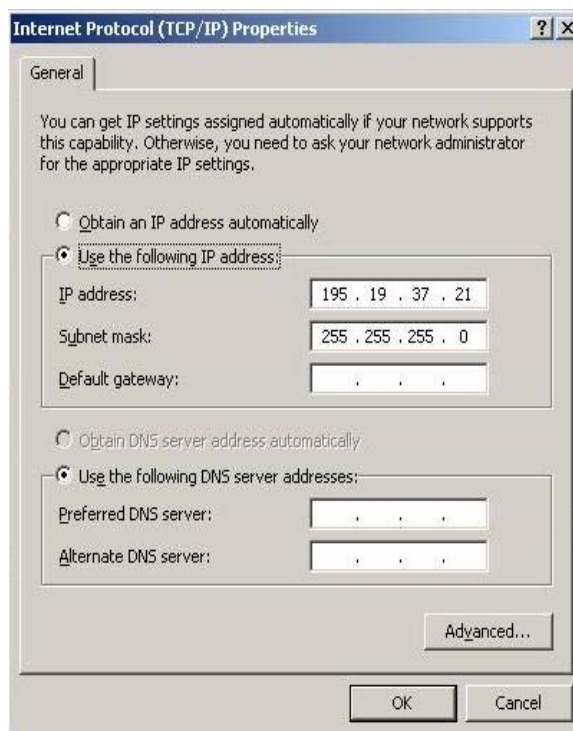


Рисунок 25. IP-адреса Comp3

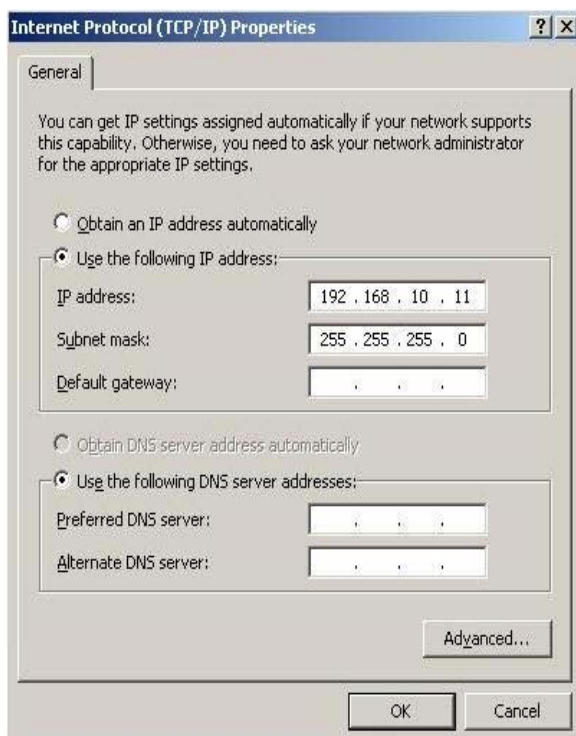


Рисунок 26. IP-адреса Comp2

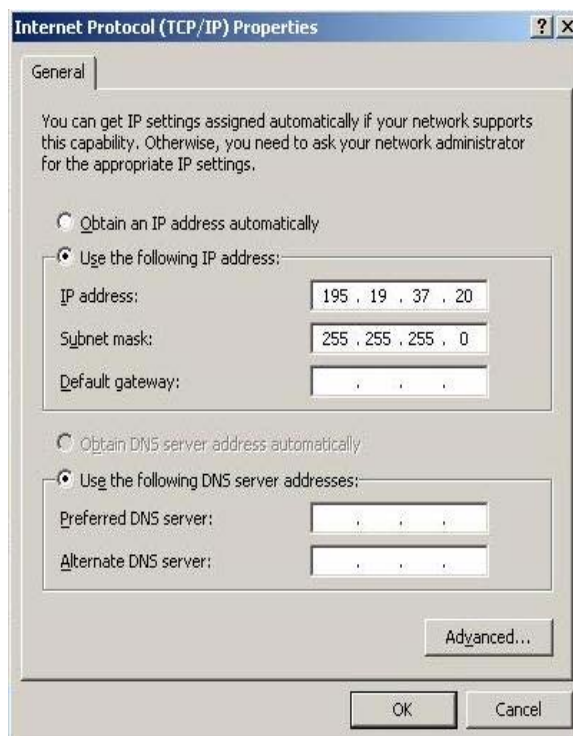
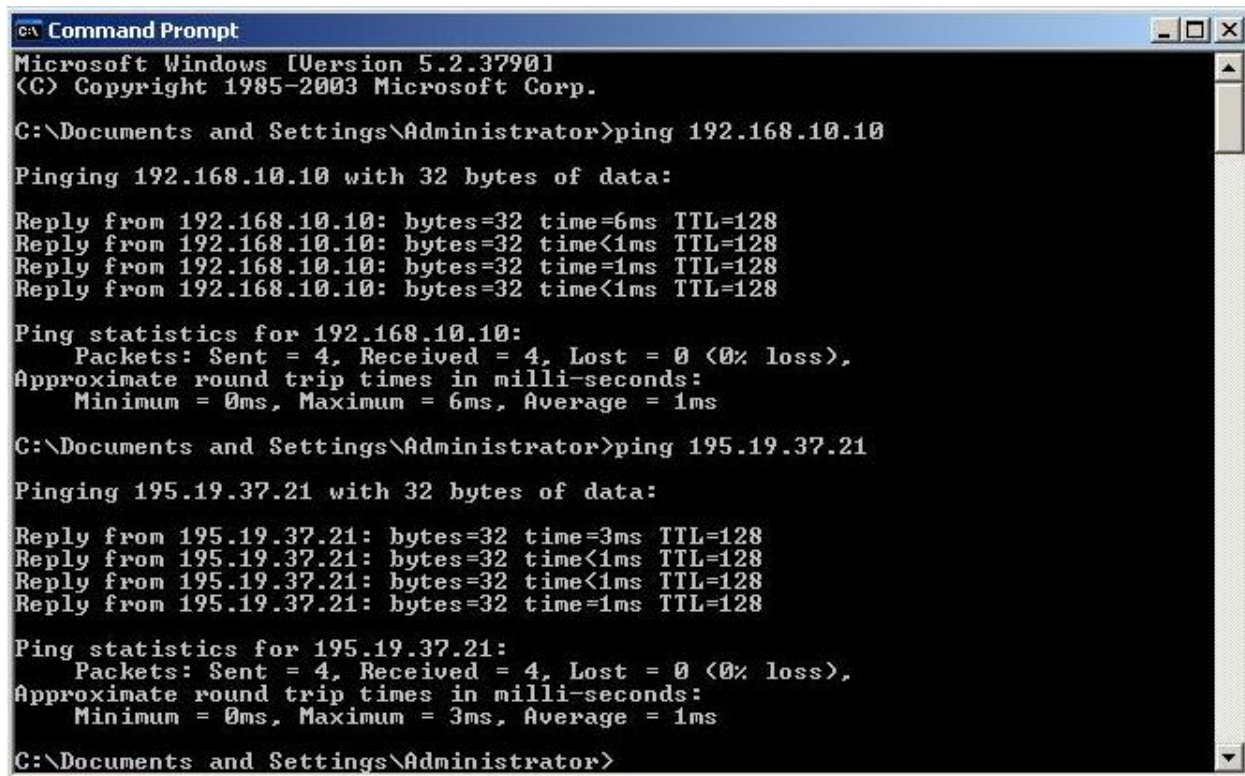


Рисунок 27. IP-адреса Comp2

## Проверка работоспособности с COMP2



```
ca\ Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=6ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time=1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\Documents and Settings\Administrator>ping 195.19.37.21

Pinging 195.19.37.21 with 32 bytes of data:

Reply from 195.19.37.21: bytes=32 time=3ms TTL=128
Reply from 195.19.37.21: bytes=32 time<1ms TTL=128
Reply from 195.19.37.21: bytes=32 time<1ms TTL=128
Reply from 195.19.37.21: bytes=32 time=1ms TTL=128

Ping statistics for 195.19.37.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\Documents and Settings\Administrator>
```

Рисунок 28

## Установим VPN-сервер

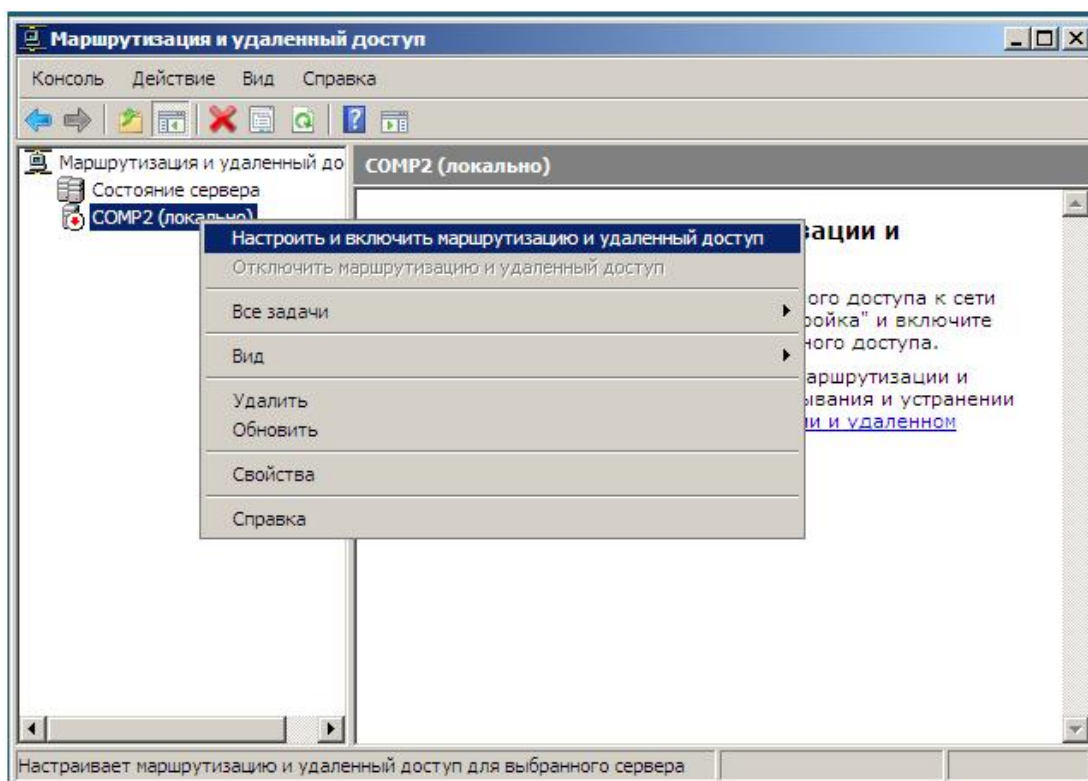


Рисунок 29



Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

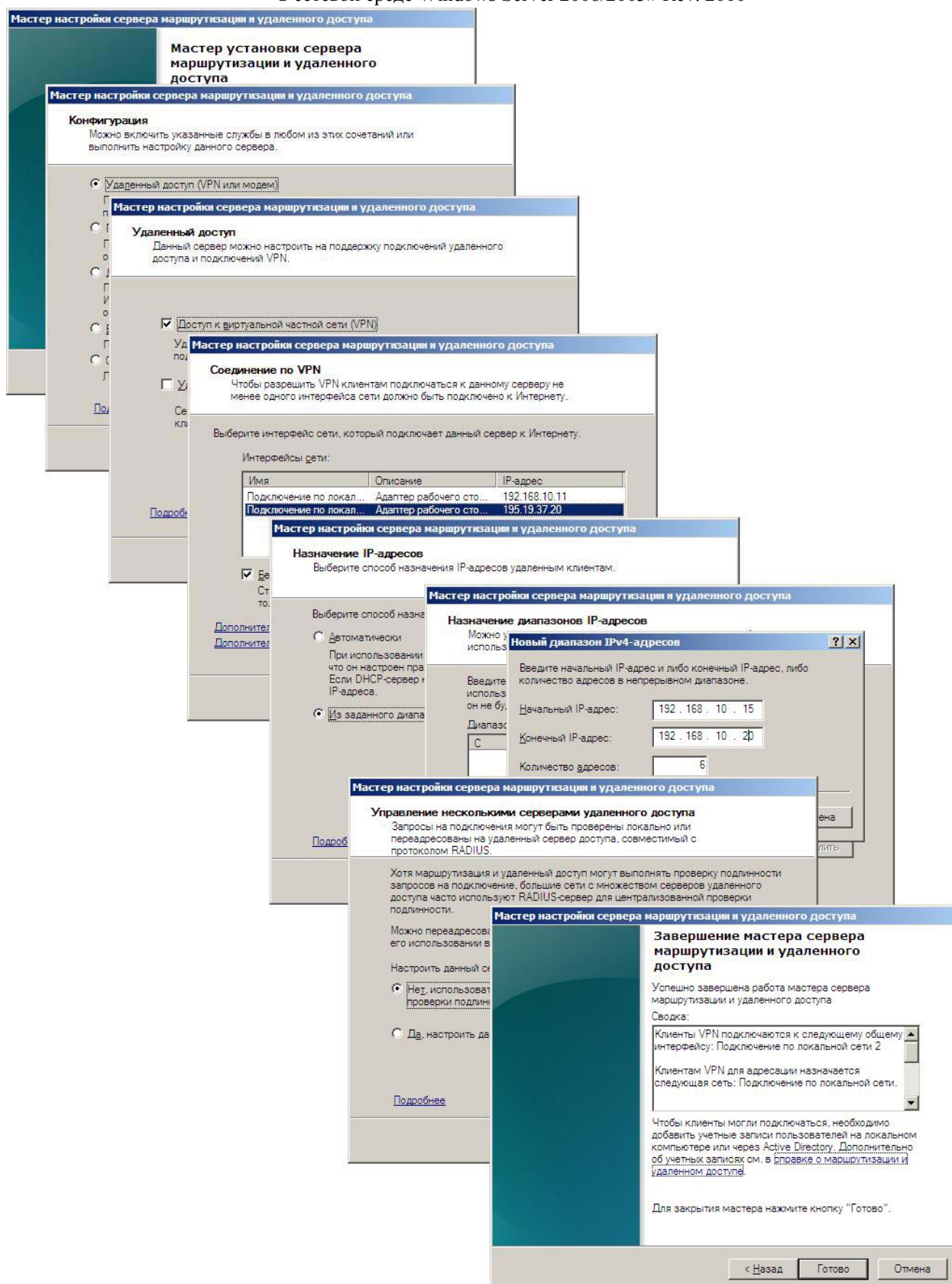


Рисунок 30

Поясним установку VPN-сервера:

Оснастку **Routing and Remote Access** можно вызвать через **Administrative Tools**.

Мастер вызывается выбором пункта меню **Configure and Enable Routing and Remote Access**.

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

Четвертое окно мастера предлагает указать интерфейс, который подсоединен к Интернету. Следует отчетливо представлять, если использование VPN-туннеля предполагается во внутренней сети, то внутренний пользователь подсоединяется к внутренней сети, то указать следует интерфейс, к которому будут подключаться пользователи.

Выбор **Enable security on selected interface** позволяет установить на этот интерфейс фильтры, пропускающие исключительно трафик, связанный с VPN-туннелями.

Разрешить **ping** (этого интерфейса и всех интерфейсов за VPN-севером) необходимо соответствующим новым фильтром.

Т.к. DHCP не используется, то назначение IP-адресов вновь подсоединенных пользователей происходит из назначенного диапазона, очевидно диапазон должен быть из пространства адресов за VPN-сервером.

Сервер RADIUS не используется.

### Добавим специальный аккаунт на сервере

Т.к. Active Directory не применяется, то учетные данные для удаленного доступа будут храниться на VPN-сервере. Учетную запись можно завести с помощью оснастки Computer Manager.

Учетная запись: user#: remote; password: #

После создания записи, необходимо дать разрешение удаленного доступа (Allow access)

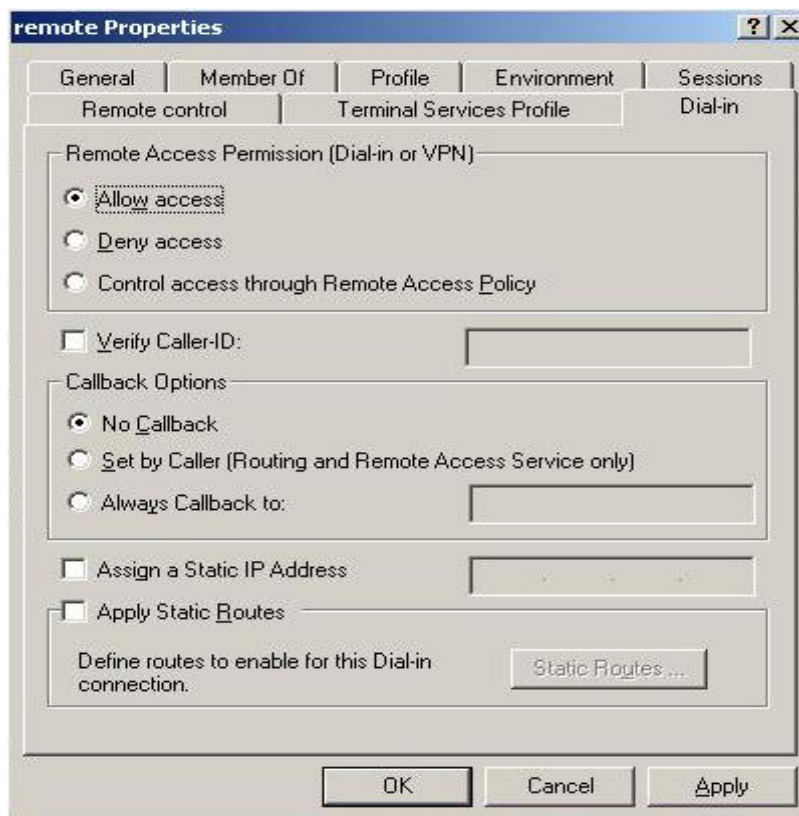


Рисунок 31

### Настройка VPN-клиента.

Никаких трудностей в настройке VPN-клиента возникнуть не должно.

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

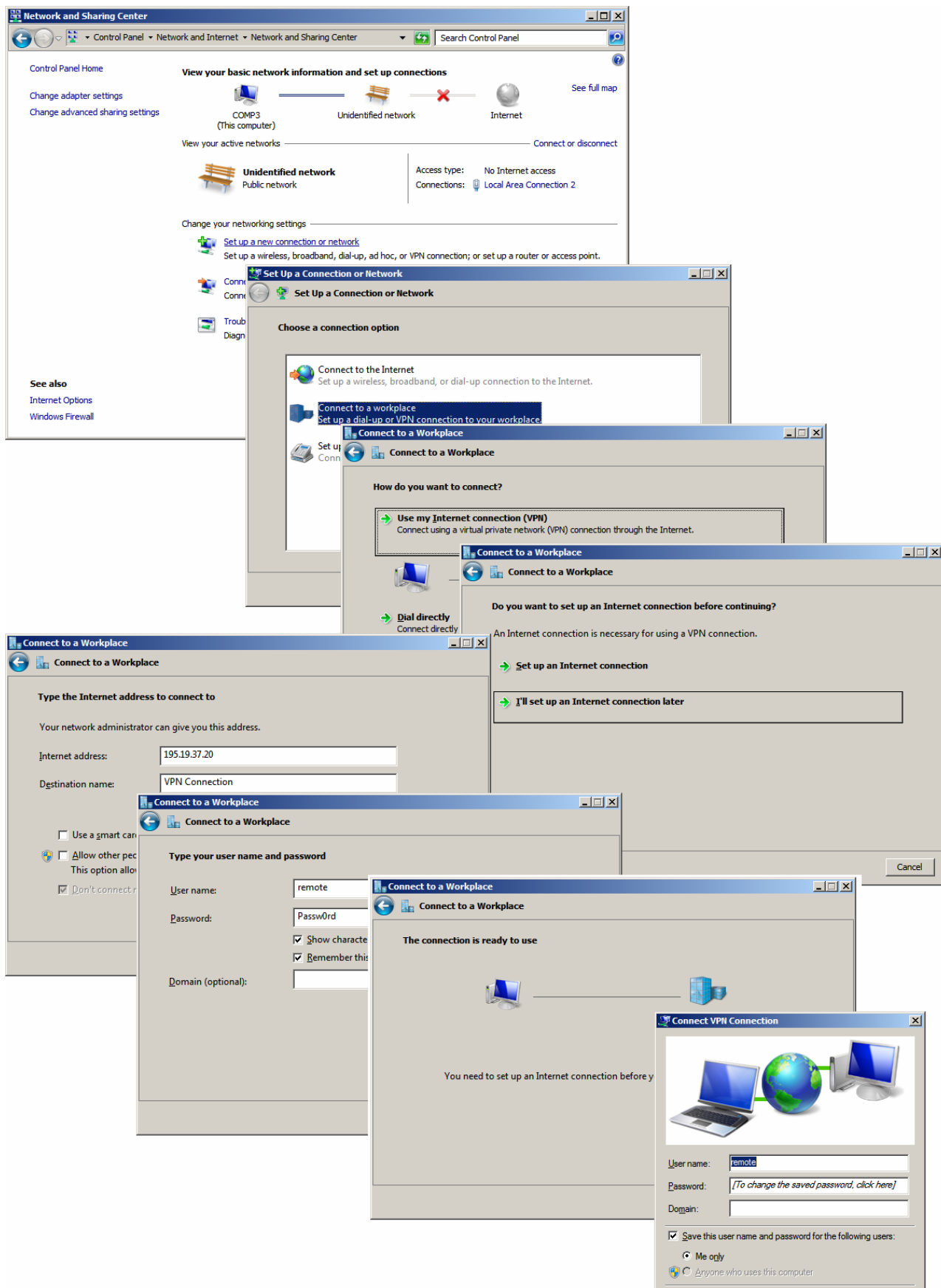


Рисунок 32

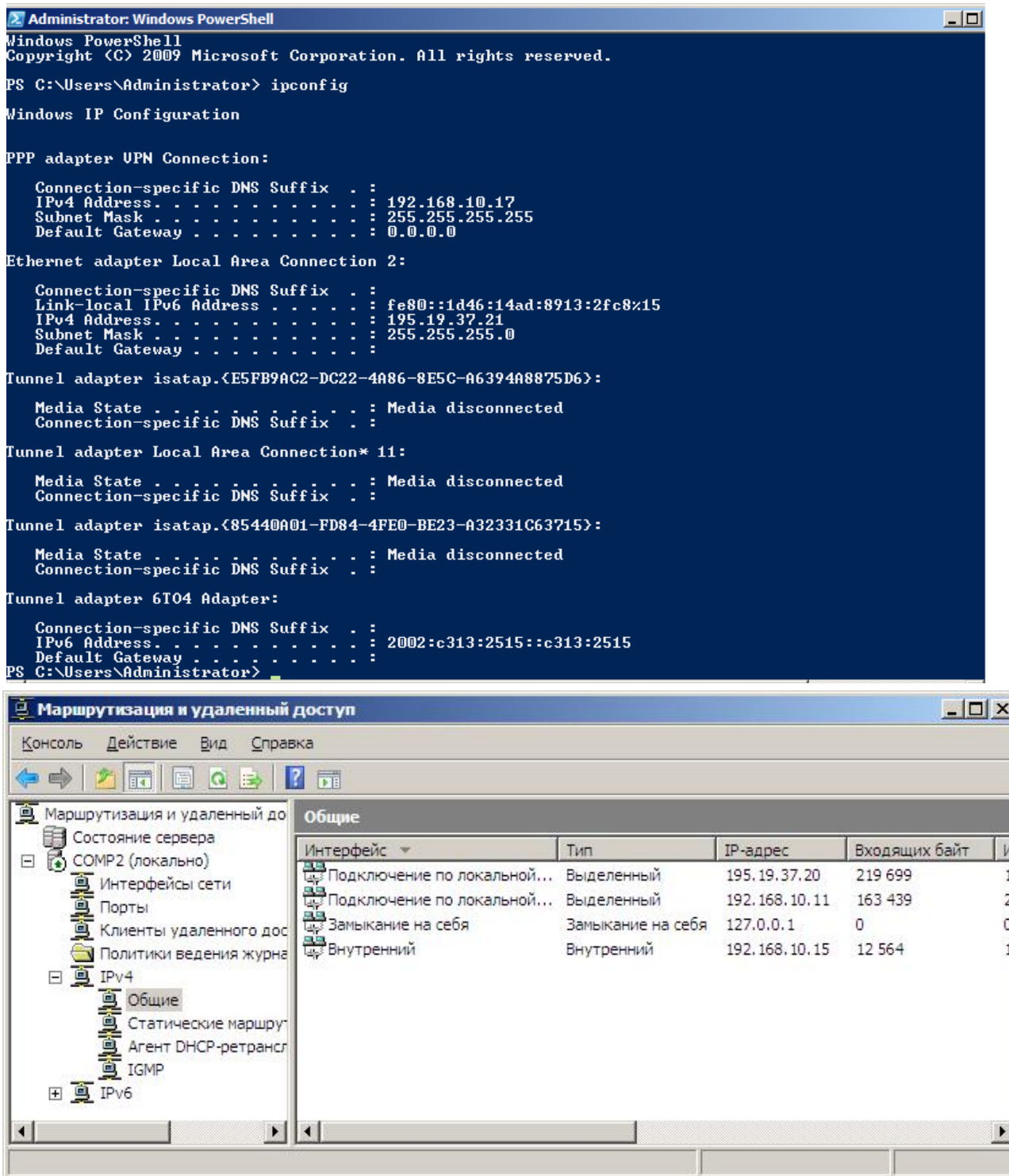
**Результат.**

Рисунок 33

При настройке VPN-сервер выделяет сам себе IP-адрес (Internal: 192.168.10.11). Этот адрес самый первый из предоставленного диапазона. Если же используется DHCP, то VPN-сервер получает адрес первый.

Следует отметить, что команда *ping 192.168.10.10* с COMPT3 без установленного VPN-соединения закончится неуспешно, т.к. ICMP не разрешен фильтрами VPN-сервера.

**LAB 2.1 Установка маршрута по умолчанию**Задание А:

На основе предыдущей лабораторной работы проверить применение маршрута по умолчанию, выделяемого VPN-сервером.

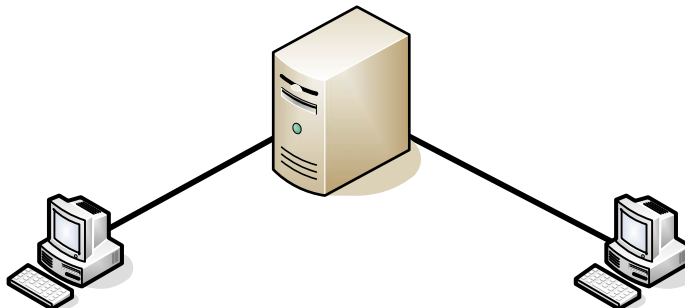


Рисунок 34

План выполнения работы:

- Исследуем таблицу маршрутизации VPN-клиента.
- Запретим использование маршрута по умолчанию VPN-клиенту.
- Исследуем таблицу маршрутизации VPN-клиента.

**Исследуем таблицу маршрутизации VPN-клиента**

```

Select Administrator: Windows PowerShell
C:\Users\Administrator> route print
=====
Interface List
22.....VPN Connection
15...08 00 27 0f 33 93 .....Intel(R) PRO/1000 MT Desktop Adapter #2
1.....Software Loopback Interface 1
12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
13...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
14...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
16...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
0.0.0.0                    0.0.0.0          On-link          192.168.10.18    11
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        4531
127.0.0.1                  255.255.255.255 On-link          127.0.0.1        4531
127.255.255.255           255.255.255.255 On-link          127.0.0.1        4531
192.168.10.18             255.255.255.255 On-link          192.168.10.18    266
195.19.37.0               255.255.255.0   On-link          195.19.37.21    4491
195.19.37.20              255.255.255.255 On-link          195.19.37.21    4236
195.19.37.21              255.255.255.255 On-link          195.19.37.21    4491
195.19.37.255            255.255.255.255 On-link          195.19.37.21    4491
224.0.0.0                 240.0.0.0        On-link          127.0.0.1        4531
224.0.0.0                 240.0.0.0        On-link          195.19.37.21    4492
224.0.0.0                 240.0.0.0        On-link          192.168.10.18    11
255.255.255.255           255.255.255.255 On-link          127.0.0.1        4531
255.255.255.255           255.255.255.255 On-link          195.19.37.21    4491
255.255.255.255           255.255.255.255 On-link          192.168.10.18    266
=====

Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
16 306 ::1/128 On-link
16 1010 2002::/16 On-link
16 266 2002:c313:2515::c313:2515/128 On-link
15 266 fe80::/64 On-link

```

Рисунок 35

После установления VPN-соединения, VPN-сервер выделяет VPN-клиенту IP-адрес, а клиент устанавливает шлюз по умолчанию 192.168.10.16.

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

У вас не вызывает удивление в совпадении IP-адреса и шлюза?.

В нашем случае клиент не использовал шлюз до установления VPN-соединения. Поэтому механизм перенастройки шлюзов может остаться до конца не ясным. Более подробно этот механизм показан в следующей лабораторной работе.

### Запретим использования маршрута по умолчанию VPN-клиенту

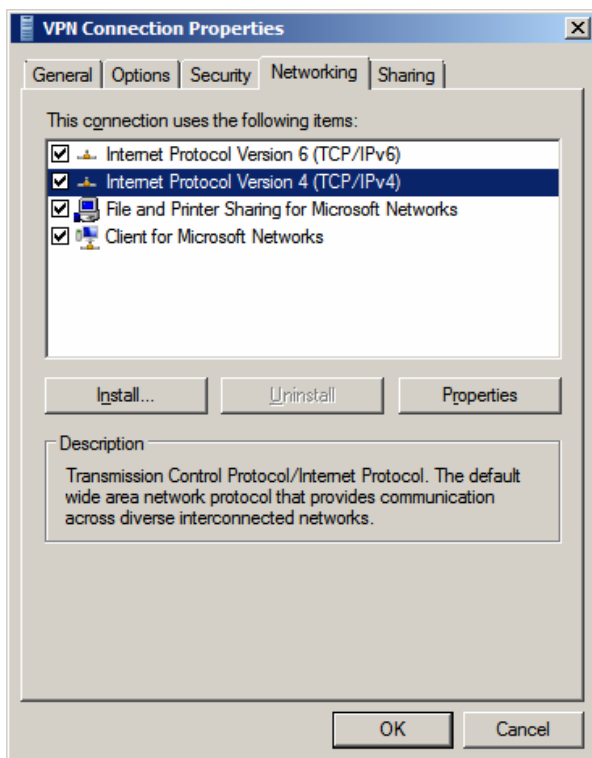


Рисунок 36

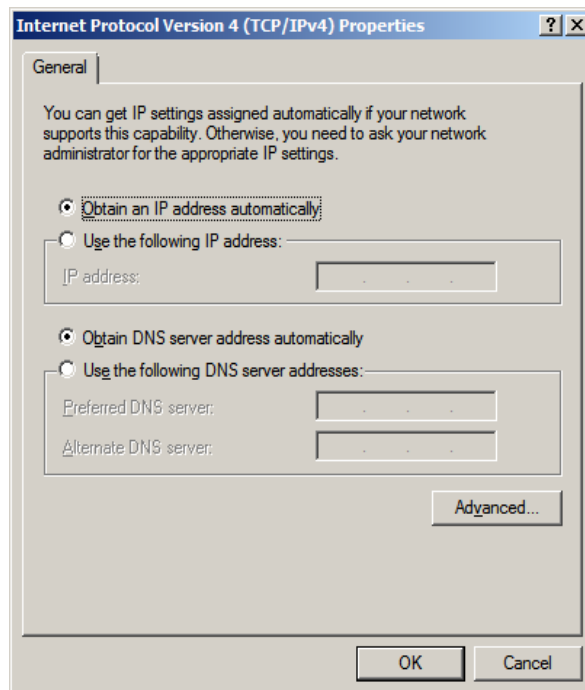


Рисунок 37

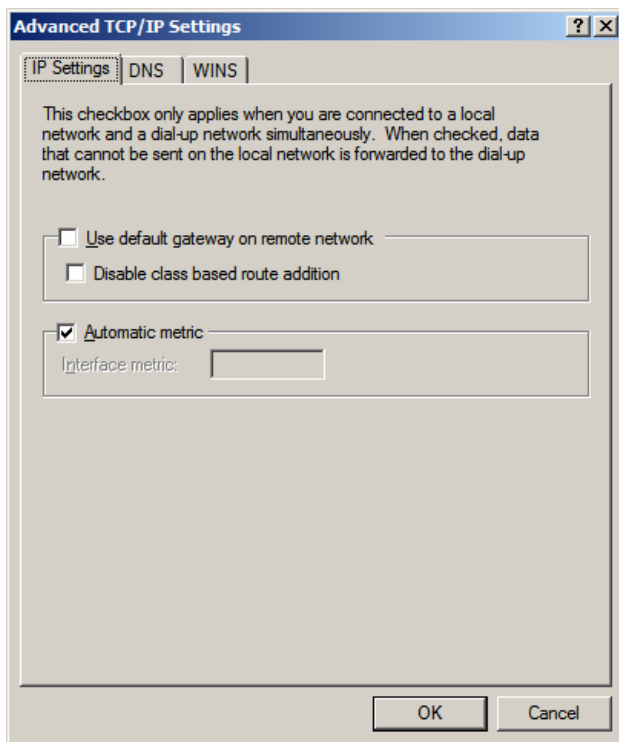


Рисунок 38

Уберем флажок Use default gateway on remote network.

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

Изменение этого параметра и применение его возможно только после создания нового подключения.

### Исследуем таблицу маршрутизации VPN-клиента

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> route print
=====
Interface List
22.....UPN Connection
15...08 00 27 0f 33 93 .....Intel(R) PRO/1000 MT Desktop Adapter #2
1.....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
14...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
16...00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
-----
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link          127.0.0.1        306
127.255.255.255           255.255.255.255 On-link          127.0.0.1        306
192.168.10.0              255.255.255.0   192.168.10.15   192.168.10.19   11
192.168.10.19             255.255.255.255 On-link          192.168.10.19   266
195.19.37.0               255.255.255.0   On-link          195.19.37.21    266
195.19.37.20              255.255.255.255 On-link          195.19.37.21    11
195.19.37.21              255.255.255.255 On-link          195.19.37.21    266
195.19.37.255            255.255.255.255 On-link          195.19.37.21    266
224.0.0.0                 240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                 240.0.0.0        On-link          195.19.37.21    266
255.255.255.255           255.255.255.255 On-link          127.0.0.1        306
255.255.255.255           255.255.255.255 On-link          195.19.37.21    266
255.255.255.255           255.255.255.255 On-link          192.168.10.19   266
=====

Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
-----
1      306   ::1/128                On-link
16     1010  2002::/16              On-link
16     266   2002:c313:2515::c313:2515/128
On-link
15     266   fe80::/64              On-link
15     266   fe80::1d46:14ad:8913:2fc8/128

```

Рисунок 39

Шлюз по умолчанию назначен не был.

**LAB 2.2 Установка маршрута по умолчанию**Задание В:

Проверить применение маршрута по умолчанию, выделяемого VPN-сервером на основе сети, рисунок 40

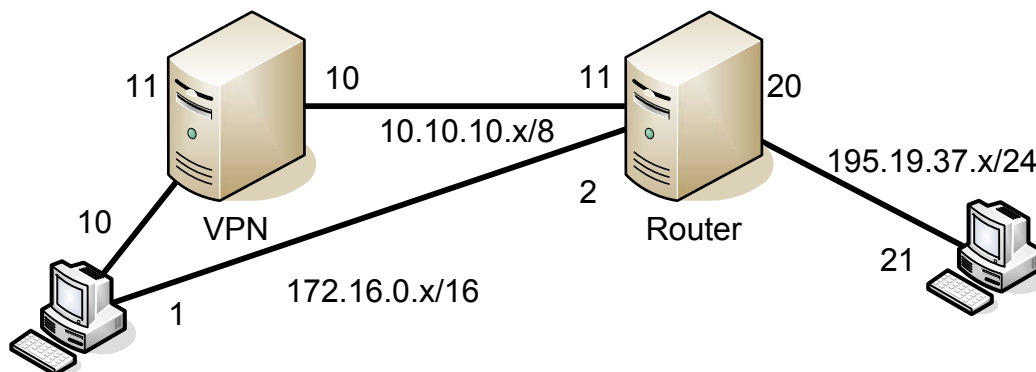


Рисунок 40.

План выполнения работы:

- Сетевые настройки: три пары адаптеров трех сетей + 1 адаптер + 2 шлюза
- Настройка Роутинга на Router
- Настройка VPN-сервера
- Разрешить ICMP на внешнем интерфейсе VPN-сервера
- Проверка работоспособности сети
- Добавление учетной записи (вход по политике)
- Настройка политики удаленного доступа на разрешение всех VPN-соединений
- Настройка VPN-клиента
- Исследование поведения таблицы маршрутизации (иначе роутинга) VPN-клиента с использованием шлюза по умолчанию и без него.

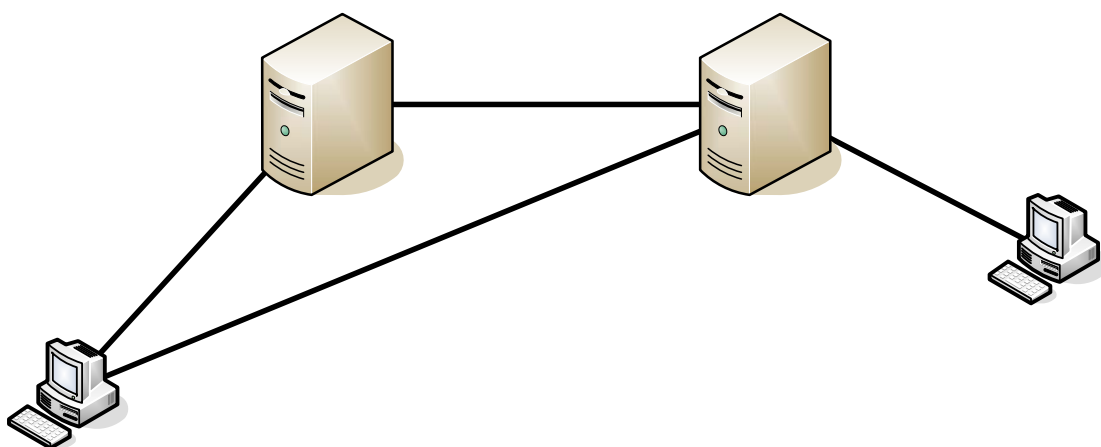


Рисунок 41.

**Сетевые настройки**



Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

Сервер	Интерфейс	IP-address	Subnet mask	Default gateway
Comp1	interface1	192.168.10.11	255.255.255.0	
	interface2	10.10.10.10	255.0.0.0	
Comp2	interface1	10.10.10.11	255.0.0.0	
	interface2	195.19.37.20	255.255.255.0	
	interface3	172.16.0.2	255.255.0.0	
Comp3	interface1	195.19.37.21	255.255.255.0	195.19.37.20
Comp4	interface1	192.168.10.10	255.255.255.0	192.168.10.11
	Interface2	172.16.0.1	255.255.0.0	172.16.0.2

```

Administrator: Windows PowerShell

IPv4 Route Table
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
-----
0.0.0.0                0.0.0.0         192.168.10.11   192.168.10.10    266
0.0.0.0                0.0.0.0         172.16.0.2     172.16.0.1       266
127.0.0.0              255.0.0.0       On-link        127.0.0.1        306
127.0.0.1              255.255.255.255 On-link        127.0.0.1        306
127.255.255.255        255.255.255.255 On-link        127.0.0.1        306
172.16.0.0             255.255.0.0     On-link        172.16.0.1       266
172.16.0.1             255.255.255.255 On-link        172.16.0.1       266
172.16.255.255         255.255.255.255 On-link        172.16.0.1       266
192.168.10.0           255.255.255.0   On-link        192.168.10.10    266
192.168.10.10         255.255.255.255 On-link        192.168.10.10    266
192.168.10.255        255.255.255.255 On-link        192.168.10.10    266
224.0.0.0              240.0.0.0       On-link        127.0.0.1        306
224.0.0.0              240.0.0.0       On-link        192.168.10.10    266
224.0.0.0              240.0.0.0       On-link        172.16.0.1       266
255.255.255.255        255.255.255.255 On-link        127.0.0.1        306
255.255.255.255        255.255.255.255 On-link        192.168.10.10    266
255.255.255.255        255.255.255.255 On-link        172.16.0.1       266
=====

Persistent Routes:
Network Address        Netmask          Gateway Address  Metric
-----
0.0.0.0                0.0.0.0         192.168.10.11   Default
0.0.0.0                0.0.0.0         172.16.0.2     Default
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination    Gateway
-----
1      306  ::1/128           On-link
11     266  fe80::/64         On-link
19     266  fe80::/64         On-link
19     266  fe80::94df:90e9:a86c:fb/128
                                On-link
11     266  fe80::e913:9d17:671c:d913/128
                                On-link
1      306  ff00::/8          On-link
11     266  ff00::/8          On-link
=====

Administrator: Windows PowerShell
PS C:\Users\Administrator> route add 195.19.37.0 mask 255.255.255.0 172.16.0.2 -p
OK!
PS C:\Users\Administrator>

```

Рисунок 42. Добавление маршрута на СОМР4 до сети 195.19.37.0/24

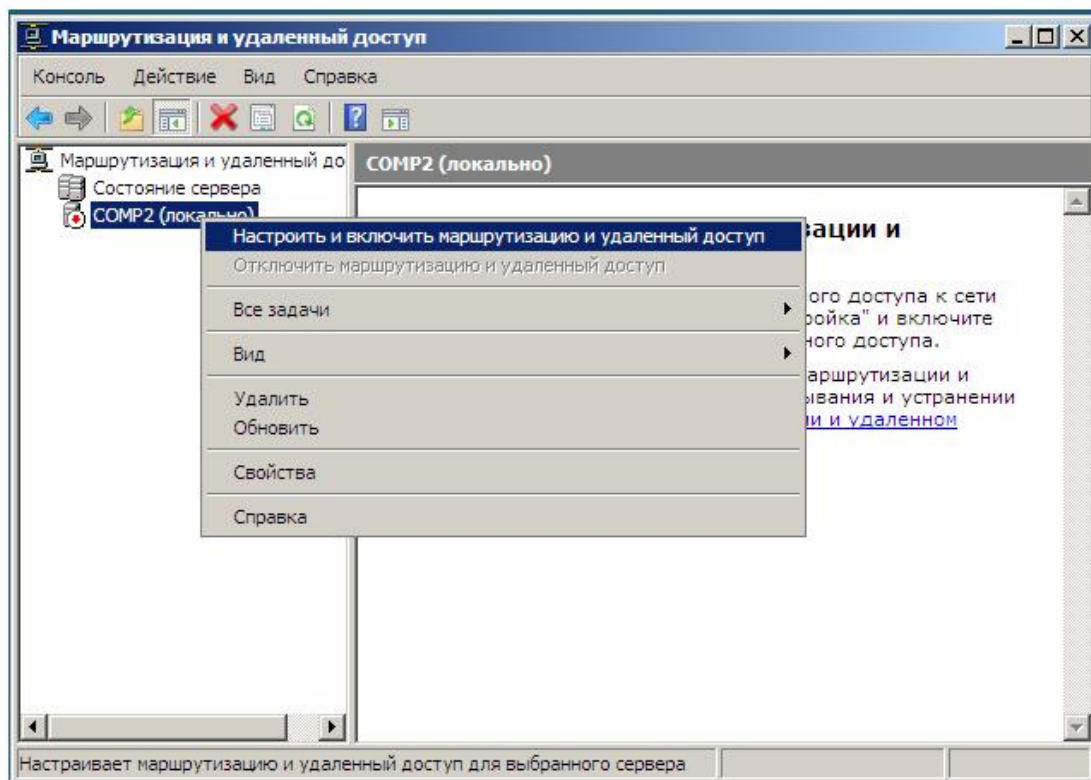
**Настройка Роутинга**

Рисунок 43

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

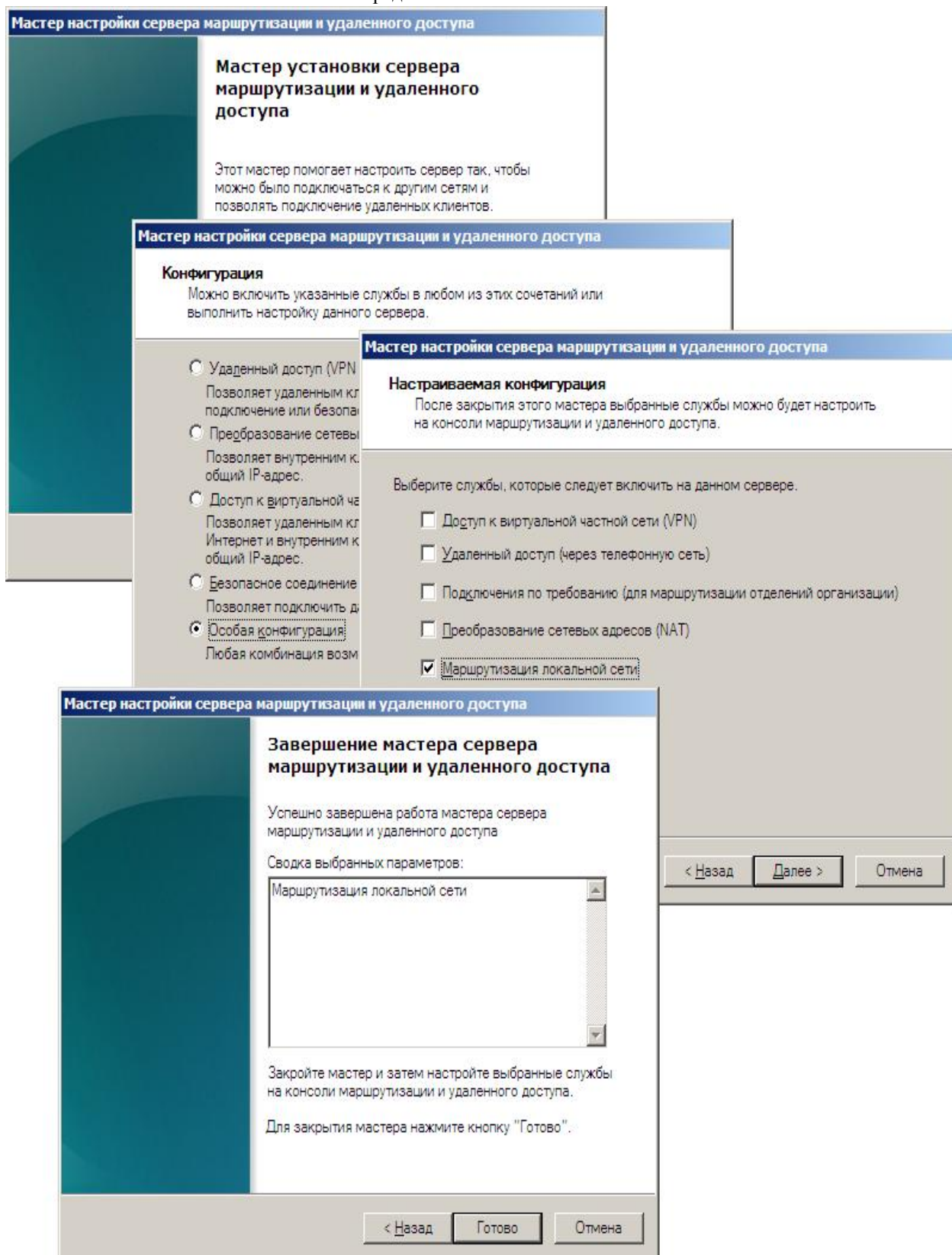


Рисунок 44

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

```

Администратор: Командная строка
C:\Users\Администратор>route print
=====
Список интерфейсов
 22 ...08 00 27 07 ab ef ..... 12 ...08 00 27 ae 78 63 ..... 10 ...08 00 27
d2 9e 83 ..... 1 ..... Software Loopback Interface 1
 14 ...00 00 00 00 00 00 e0 isatap.<4560DA01-0799-4938-B553-4148EEF36B3A>
 11 ...02 00 54 55 4e 01 ..... Teredo Tunneling Pseudo-Interface
 13 ...00 00 00 00 00 00 e0 isatap.<5AD2368C-D1CE-408E-A28C-1E210CF6E51F>
 15 ...00 00 00 00 00 00 e0 6T04 Adapter
 16 ...00 00 00 00 00 00 e0 =====

IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес          Маска сети          Адрес шлюза          Интерфейс          Метрика
10.0.0.0                255.0.0.0           On-link              10.10.10.11        266
10.10.10.11             255.255.255.255    On-link              10.10.10.11        266
10.255.255.255          255.255.255.255    On-link              10.10.10.11        266
127.0.0.0               255.0.0.0           On-link              127.0.0.1          306
127.0.0.1               255.255.255.255    On-link              127.0.0.1          306
127.255.255.255        255.255.255.255    On-link              127.0.0.1          306
172.16.0.0              255.255.0.0         On-link              172.16.0.2         266
172.16.0.2              255.255.255.255    On-link              172.16.0.2         266
172.16.255.255         255.255.255.255    On-link              172.16.0.2         266
195.19.37.0            255.255.255.0       On-link              195.19.37.20       266
195.19.37.20           255.255.255.255    On-link              195.19.37.20       266
195.19.37.255          255.255.255.255    On-link              195.19.37.20       266
224.0.0.0               240.0.0.0           On-link              127.0.0.1          306
224.0.0.0               240.0.0.0           On-link              195.19.37.20       266
224.0.0.0               240.0.0.0           On-link              10.10.10.11        266
224.0.0.0               240.0.0.0           On-link              172.16.0.2         266
255.255.255.255         255.255.255.255    On-link              127.0.0.1          306
255.255.255.255         255.255.255.255    On-link              195.19.37.20       266
255.255.255.255         255.255.255.255    On-link              10.10.10.11        266
255.255.255.255         255.255.255.255    On-link              172.16.0.2         266
=====
Постоянные маршруты:
Отсутствует

IPv6 таблица маршрута
=====
Активные маршруты:
Метрика   Сетевой адрес          Шлюз
1          306 ::1/128              On-link
15         1010 2002::/16         On-link
15         266 2002:c313:2514::c313:2514/128
On-link
12         266 fe80::/64            On-link
10         266 fe80::/64            On-link
22         266 fe80::/64            On-link
10         266 fe80::352b:e747:3f5c:573a/128
On-link
22         266 fe80::ac42:9a7:830:caa1/128
On-link
12         266 fe80::c8d3:cc02:697e:67b/128
On-link
1          306 ff00::/8              On-link
12         266 ff00::/8              On-link
10         266 ff00::/8              On-link
22         266 ff00::/8              On-link
=====
Постоянные маршруты:
Отсутствует

C:\Users\Администратор>route add 192.168.10.0 mask 255.255.255.0 10.10.10.10 -p
OK
C:\Users\Администратор>

```

Рисунок 45. Добавление маршрута на COM2

## Настройка VPN-сервера

В мастере выбираем:

Интерфейс подсоединенный к Интернету: 10.10.10.10

Установить флажок: Enable security

Диапазон выделенных IP-адресов: 192.168.10.15.. 192.168.10.20

Отказываемся от RADIUS.

Настройка VPN возможна и с частичным прохождением мастера настройки:

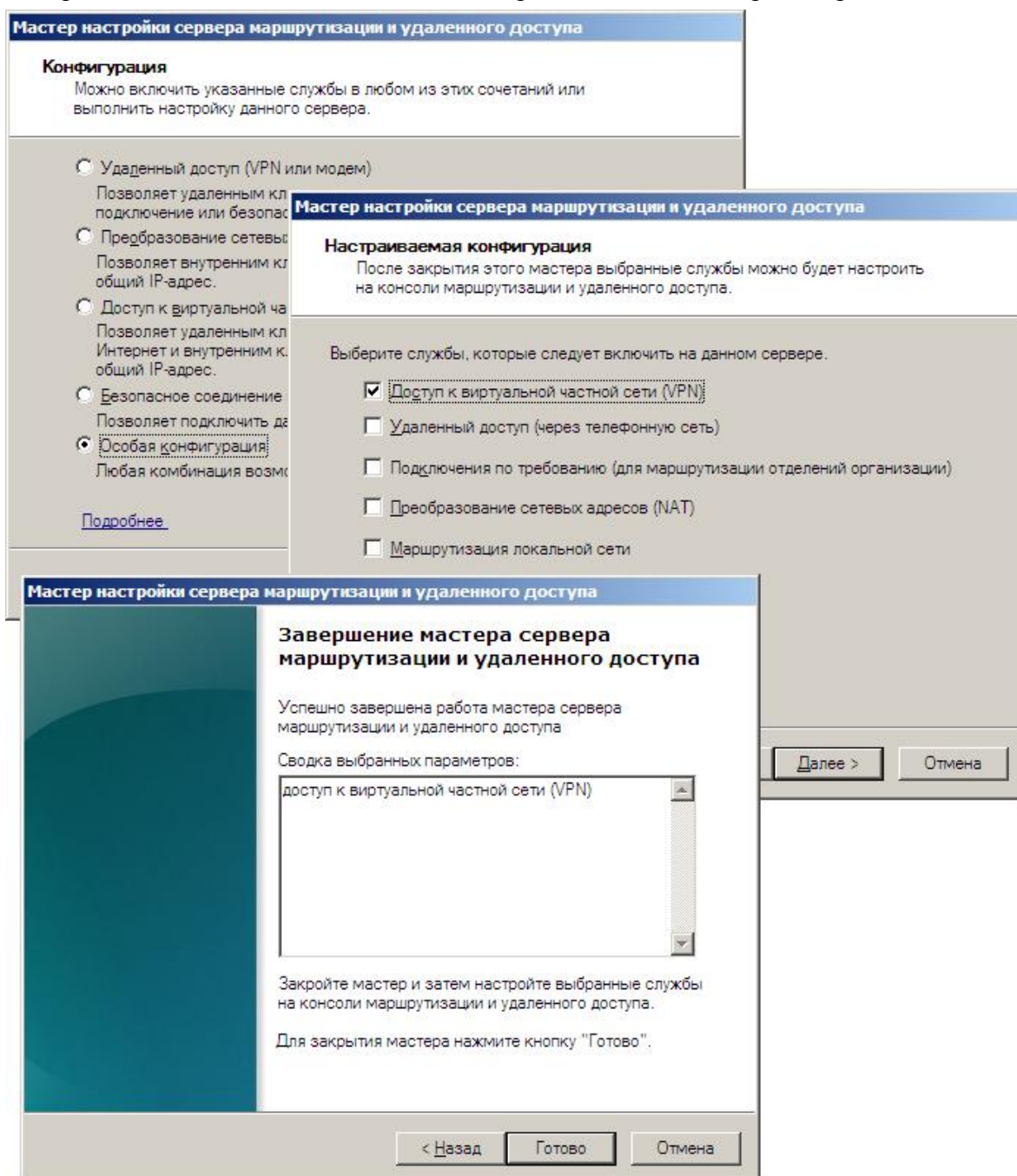


Рисунок 46

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

Для этого выбирается пункт Custom configuration и устанавливается галка VPN-access.

В данном случае необходимо после работы мастера на VPN-сервере указать диапазон выделенных IP-адресов и настроить фильтр на интерфейсе 10.10.10.10 на прием и отправку только пакетов имеющих отношение к VPN.

Поэтому рекомендуется воспользоваться полным мастером настройки.

```

Администратор: Командная строка
C:\Users\Администратор>route add 195.19.37.0 mask 255.255.255.0 10.10.10.11 -p
OK

C:\Users\Администратор>
C:\Users\Администратор>route print
=====
Список интерфейсов
17 ...08 00 27 ef d7 4a ..... 10 ...08 00 27 d0 dd ca ..... 1 .....
..... Software Loopback Interface 1
19 ...00 00 00 00 00 00 e0 11 ...02 00 54 55 4e 01 ..... Teredo Tunneling
Pseudo-Interface
12 ...00 00 00 00 00 00 e0 =====

IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
10.0.0.0            255.0.0.0      On-link          10.10.10.10    266
10.10.10.10        255.255.255.255 On-link          10.10.10.10    266
10.255.255.255     255.255.255.255 On-link          10.10.10.10    266
127.0.0.0          255.0.0.0      On-link          127.0.0.1      306
127.0.0.1          255.255.255.255 On-link          127.0.0.1      306
127.255.255.255    255.255.255.255 On-link          127.0.0.1      306
192.168.10.0       255.255.255.0  On-link          192.168.10.11  266
192.168.10.11     255.255.255.255 On-link          192.168.10.11  266
192.168.10.255    255.255.255.255 On-link          192.168.10.11  266
195.19.37.0        255.255.255.0  10.10.10.11     10.10.10.10    11
224.0.0.0          240.0.0.0      On-link          127.0.0.1      306
224.0.0.0          240.0.0.0      On-link          10.10.10.10    266
224.0.0.0          240.0.0.0      On-link          192.168.10.11  266
255.255.255.255    255.255.255.255 On-link          127.0.0.1      306
255.255.255.255    255.255.255.255 On-link          10.10.10.10    266
255.255.255.255    255.255.255.255 On-link          192.168.10.11  266
=====
Постоянные маршруты:
Сетевой адрес      Маска      Адрес шлюза      Метрика
195.19.37.0        255.255.255.0  10.10.10.11     1
=====

```

Рисунок 47. Добавление маршрута на COM1

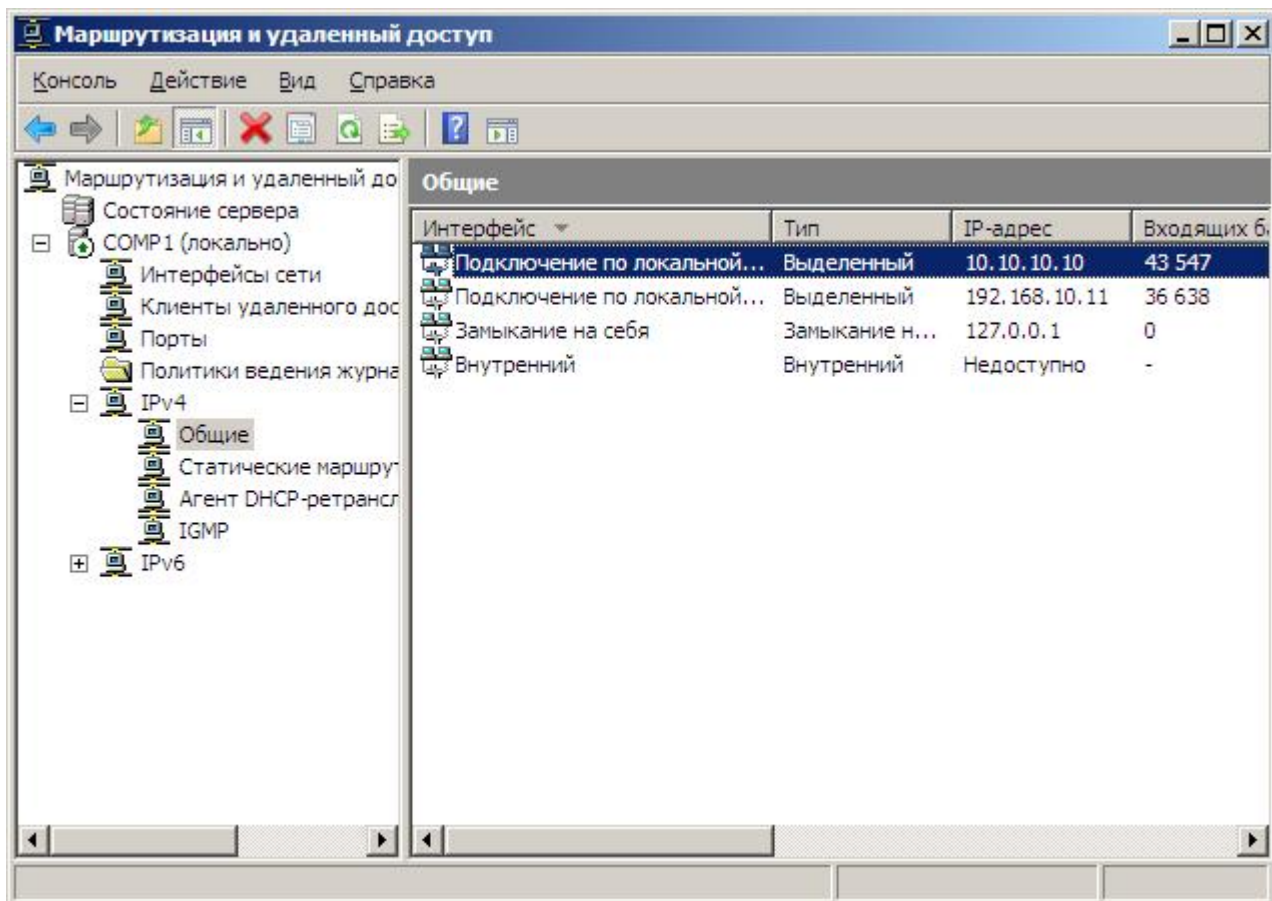
**Разрешение ICMP на внешнем интерфейсе VPN-сервера**

Рисунок 48

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

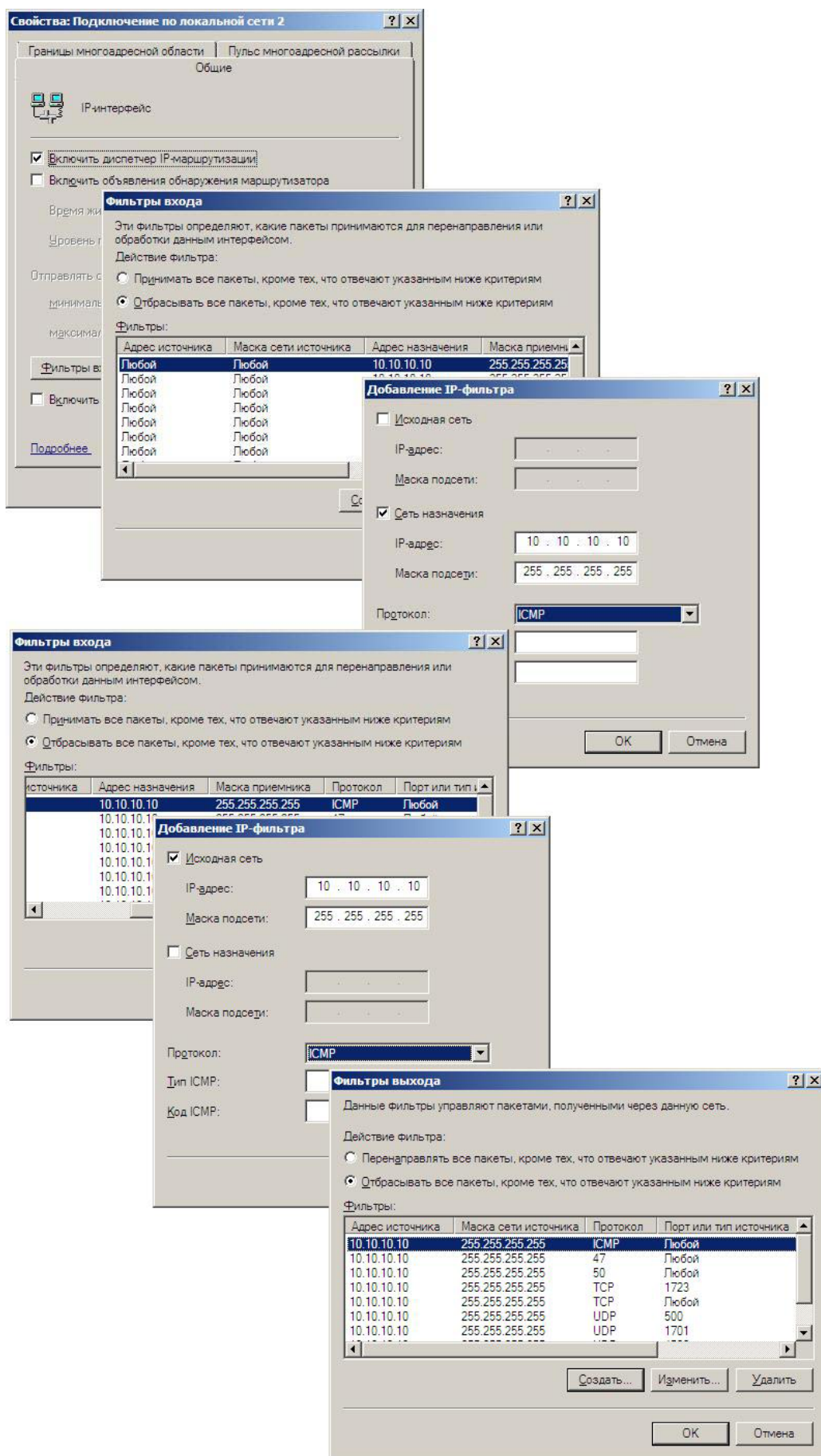


Рисунок 49



## Добавление учетной записи

Учетная запись добавляется на VPN-сервере.

Удаленный доступ для данной учетной записи оставим: согласно политике.

User: remote

Password: Passw0rd

## Настройка политики удаленного доступа

Откройте оснастку «Сервер Политики Сети(NPS)» и создайте новую политику запросов на подключение.

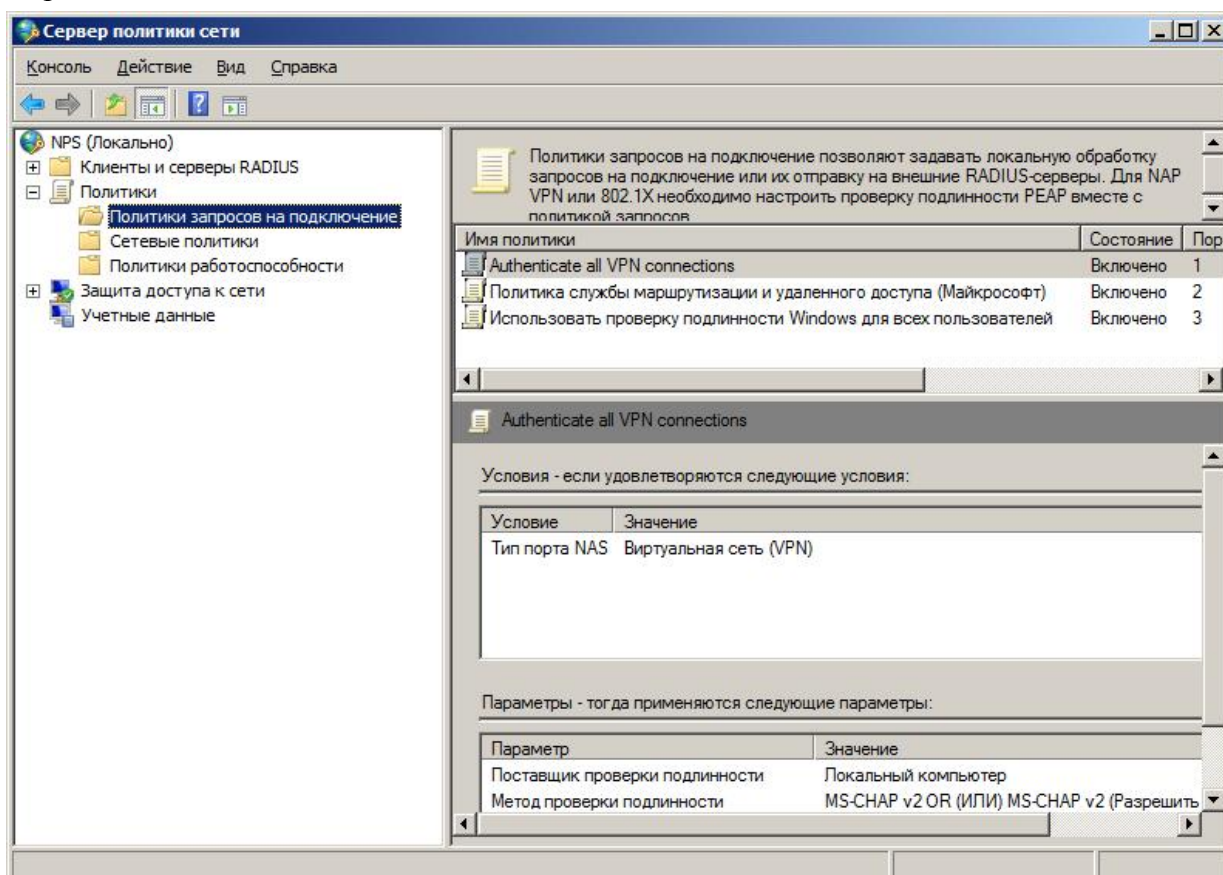


Рисунок 50

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

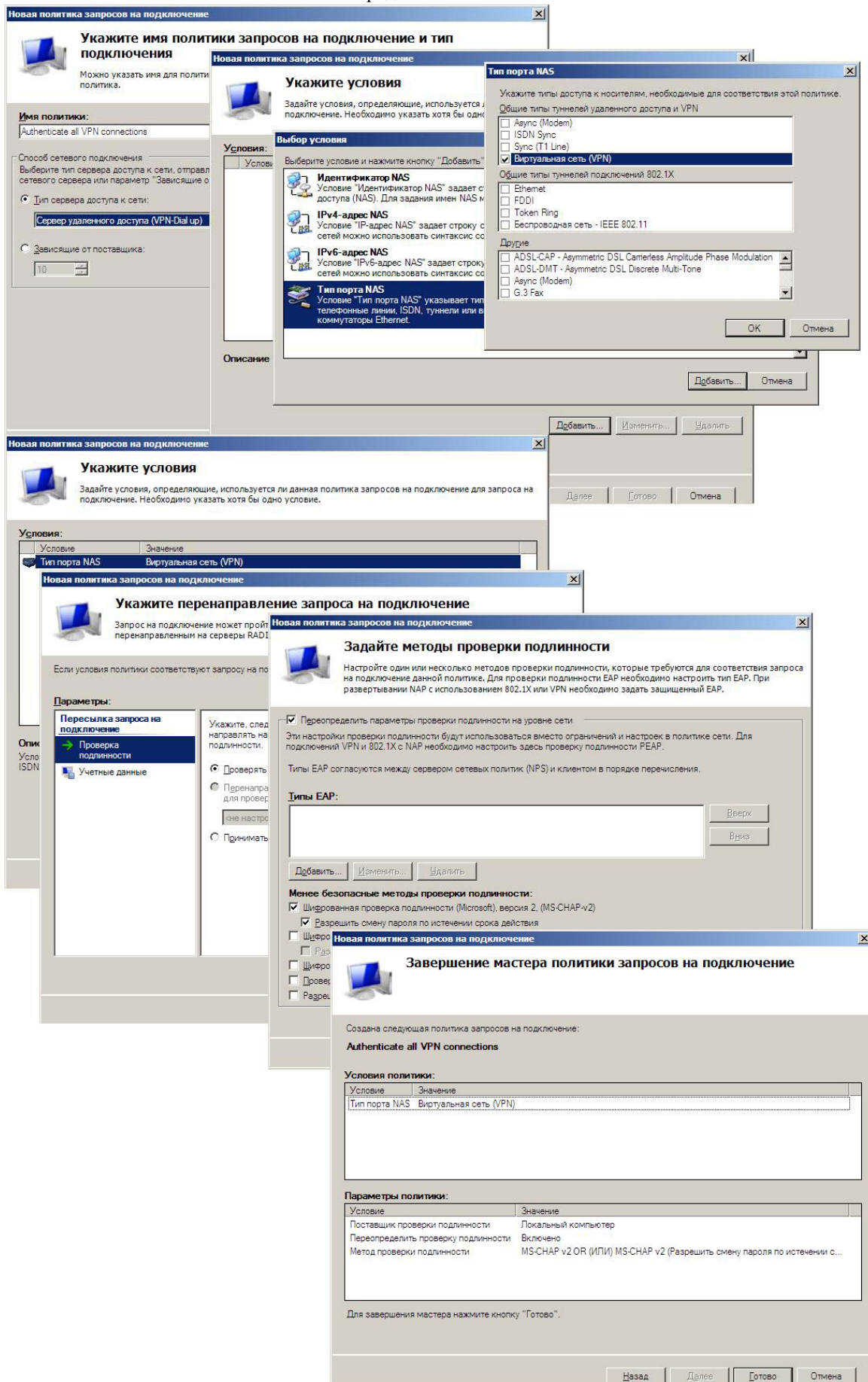


Рисунок 51

**Настройка VPN-клиента**

В мастере указать:

VPN connection name: vpn

IP-address VPN: 10.10.10.10

**Исследование таблицы маршрутизации**

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> route print
=====
Interface List
11...08 00 27 b7 b2 34 .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
16...00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
-----
0.0.0.0                    0.0.0.0          195.19.37.20     195.19.37.21     266
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link          127.0.0.1        306
127.255.255.255           255.255.255.255 On-link          127.0.0.1        306
195.19.37.0                255.255.255.0   On-link          195.19.37.21     266
195.19.37.21              255.255.255.255 On-link          195.19.37.21     266
195.19.37.255             255.255.255.255 On-link          195.19.37.21     266
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          195.19.37.21     266
255.255.255.255           255.255.255.255 On-link          127.0.0.1        306
255.255.255.255           255.255.255.255 On-link          195.19.37.21     266
=====

Persistent Routes:
Network Address            Netmask          Gateway Address  Metric
-----
0.0.0.0                    0.0.0.0          195.19.37.20     Default
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
-----
1      306   ::1/128                    On-link
16     1010  2002::/16                  On-link
16     266   2002:c313:2515::c313:2515/128
On-link
11     266   fe80::/64                  On-link
11     266   fe80::89a:8f70:3c9d:519b/128
On-link
1      306   ff00::/8                   On-link
11     266   ff00::/8                   On-link
=====

Persistent Routes:
None
PS C:\Users\Administrator>

```

Рисунок 54. Таблица маршрутизации без VPN

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> ping -n 1 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:
Reply from 172.16.0.2: bytes=32 time=14ms TTL=127

Ping statistics for 172.16.0.2:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 14ms, Average = 14ms
PS C:\Users\Administrator> ping -n 1 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=7ms TTL=127

Ping statistics for 10.10.10.10:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 7ms, Average = 7ms
PS C:\Users\Administrator> ping -n 1 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.10.10:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
PS C:\Users\Administrator>

```

Рисунок 55. Достижимость узлов без VPN.

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> route print
=====
Interface List
22.....UPN
11...08 00 27 b7 b2 34 .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
14...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
16...00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          195.19.37.20     195.19.37.21     4491
0.0.0.0                    0.0.0.0          On-link         192.168.10.17     11
10.10.10.10                255.255.255.255 195.19.37.20     195.19.37.21     4236
127.0.0.0                  255.0.0.0       On-link         127.0.0.1         4531
127.0.0.1                  255.255.255.255 On-link         127.0.0.1         4531
127.255.255.255           255.255.255.255 On-link         127.0.0.1         4531
192.168.10.17             255.255.255.255 On-link         192.168.10.17     266
195.19.37.0               255.255.255.0   On-link         195.19.37.21     4491
195.19.37.21              255.255.255.255 On-link         195.19.37.21     4491
195.19.37.255             255.255.255.255 On-link         195.19.37.21     4491
224.0.0.0                 240.0.0.0       On-link         127.0.0.1         4531
224.0.0.0                 240.0.0.0       On-link         195.19.37.21     4492
224.0.0.0                 240.0.0.0       On-link         192.168.10.17     11
255.255.255.255           255.255.255.255 On-link         127.0.0.1         4531
255.255.255.255           255.255.255.255 On-link         195.19.37.21     4491
255.255.255.255           255.255.255.255 On-link         192.168.10.17     266
=====

Persistent Routes:
Network Address            Netmask          Gateway Address  Metric
0.0.0.0                    0.0.0.0          195.19.37.20     Default
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1       306   ::1/128                On-link
16      1010  2002::/16              On-link
16      266   2002:c313:2515::c313:2515/128
                                           On-link
11      266   fe80::/64              On-link
11      266   fe80::89a:8f70:3c9d:519b/128
                                           On-link
1       306   ff00::/8               On-link
11      266   ff00::/8               On-link
=====

Persistent Routes:
None
PS C:\Users\Administrator> _

```

Рисунок 56. Таблица маршрутизации с VPN (со шлюзом по умолчанию)

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> ping -n 1 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:
Reply from 192.168.10.15: Destination net unreachable.

Ping statistics for 172.16.0.2:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
PS C:\Users\Administrator> ping -n 1 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=2ms TTL=127

Ping statistics for 10.10.10.10:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
PS C:\Users\Administrator> ping -n 1 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time=7ms TTL=127

Ping statistics for 192.168.10.10:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 7ms, Average = 7ms
PS C:\Users\Administrator> _

```

Рисунок 57. Достижимость узлов с VPN (со шлюзом по умолчанию)

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> route print
=====
Interface List
22.....UPN
11..08 00 27 b7 b2 34 .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
13...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
14...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
16...00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
=====

IPv4 Route Table
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0          195.19.37.20    195.19.37.21     266
10.10.10.10           255.255.255.255 195.19.37.20    195.19.37.21     11
127.0.0.0              255.0.0.0        On-link         127.0.0.1        306
127.0.0.1              255.255.255.255 On-link         127.0.0.1        306
127.255.255.255       255.255.255.255 On-link         127.0.0.1        306
192.168.10.0           255.255.255.0    192.168.10.15   192.168.10.19    11
192.168.10.19         255.255.255.255 On-link         192.168.10.19    266
195.19.37.0            255.255.255.0    On-link         195.19.37.21    266
195.19.37.21          255.255.255.255 On-link         195.19.37.21    266
195.19.37.255         255.255.255.255 On-link         195.19.37.21    266
224.0.0.0              240.0.0.0        On-link         127.0.0.1        306
224.0.0.0              240.0.0.0        On-link         195.19.37.21    266
255.255.255.255       255.255.255.255 On-link         127.0.0.1        306
255.255.255.255       255.255.255.255 On-link         195.19.37.21    266
255.255.255.255       255.255.255.255 On-link         192.168.10.19    266
=====

Persistent Routes:
Network Address        Netmask          Gateway Address  Metric
0.0.0.0                0.0.0.0          195.19.37.20    Default
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1       306   ::1/128                On-link
16      1010  2002::/16              On-link
16      266   2002:c313:2515::c313:2515/128
On-link
11      266   fe80::/64              On-link
11      266   fe80::89a:8f70:3c9d:519b/128
On-link
1       306   ff00::/8               On-link
11      266   ff00::/8               On-link
=====

Persistent Routes:
None
PS C:\Users\Administrator>

```

Рисунок 58. Таблица маршрутизации с VPN (без шлюза по умолчанию)

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> ping -n 1 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:
Reply from 172.16.0.2: bytes=32 time=3ms TTL=127

Ping statistics for 172.16.0.2:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 3ms, Average = 3ms
PS C:\Users\Administrator> ping -n 1 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=4ms TTL=127

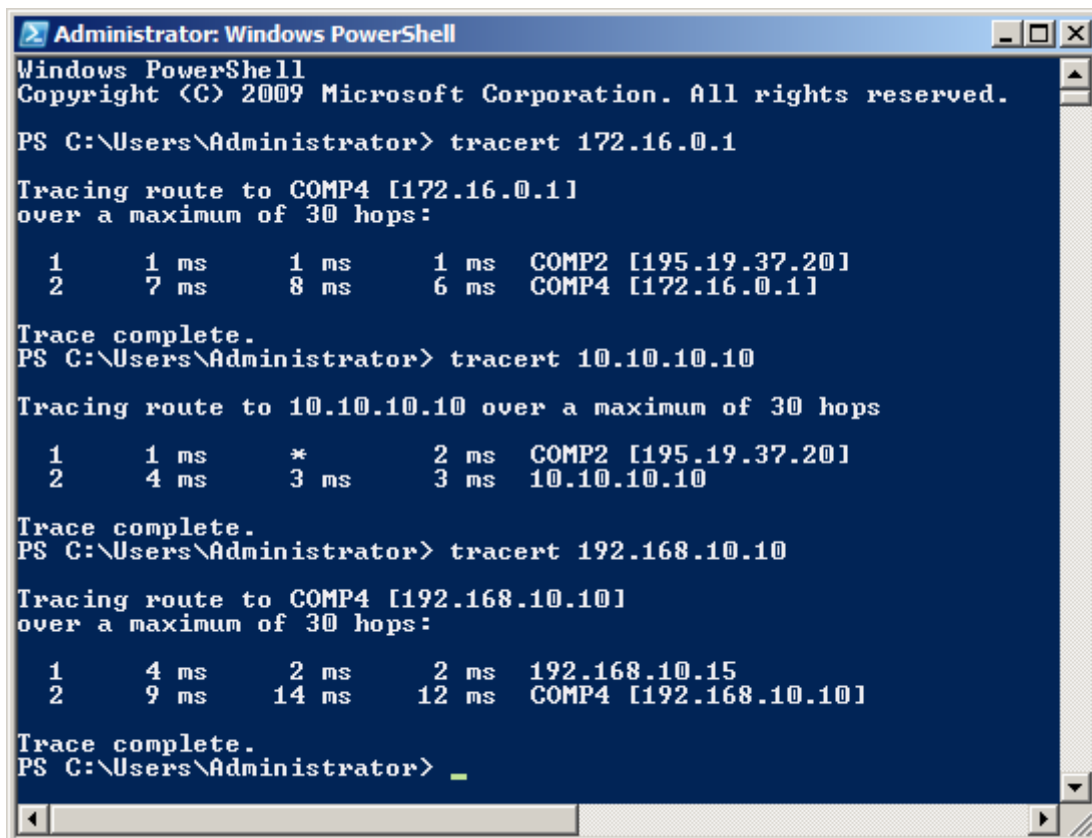
Ping statistics for 10.10.10.10:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms
PS C:\Users\Administrator> ping -n 1 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time=33ms TTL=127

Ping statistics for 192.168.10.10:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 33ms, Average = 33ms
PS C:\Users\Administrator>

```

Рисунок 59. Достижимость узлов с VPN (без шлюза по умолчанию)



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> tracert 172.16.0.1

Tracing route to COMP4 [172.16.0.1]
over a maximum of 30 hops:

  1      1 ms      1 ms      1 ms    COMP2 [195.19.37.20]
  2      7 ms      8 ms      6 ms    COMP4 [172.16.0.1]

Trace complete.
PS C:\Users\Administrator> tracert 10.10.10.10

Tracing route to 10.10.10.10 over a maximum of 30 hops

  1      1 ms      *         2 ms    COMP2 [195.19.37.20]
  2      4 ms      3 ms      3 ms    10.10.10.10

Trace complete.
PS C:\Users\Administrator> tracert 192.168.10.10

Tracing route to COMP4 [192.168.10.10]
over a maximum of 30 hops:

  1      4 ms      2 ms      2 ms    192.168.10.15
  2      9 ms     14 ms     12 ms    COMP4 [192.168.10.10]

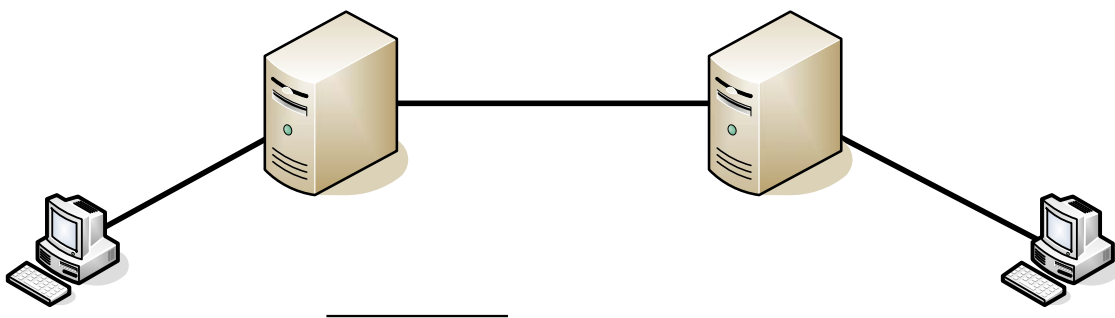
Trace complete.
PS C:\Users\Administrator> _
```

Рисунок 60

### LAB 3. VPN-Соединение между маршрутизаторами по требованию

Задание:

Установить VPN-Соединение между маршрутизаторами филиала и головного офиса. Сеть представлена на рисунке 61.



Филиал

Рисунок 61

План выполнения лабораторной:

- Настройка сетевых адаптеров: три пары адаптеров + 2 шлюза по умолчанию
- Настройка двух VPN-серверов
- Создание двух интерфейсов по требованию
- Проверка работоспособности.

**Настройка сетевых адаптеров**

Сервер	Интерфейс	IP-адрес	Subnet mask	Default gateway
Comp1	interface1	192.168.10.11	255.255.255.0	Demand-Dial
	interface2	10.10.10.10	255.0.0.0	
Comp2	interface1	10.10.10.11	255.0.0.0	Dial in:
	interface2	195.19.37.20	255.255.255.0	
Comp3	interface1	195.19.37.21	255.255.255.0	195.19.37.20
Comp4	interface1	192.168.10.10	255.255.255.0	192.168.10.11

**Настройка двух VPN-серверов**

Рекомендую настраивать сервера с помощью мастера.

Dial out:  
user intcomp  
pass 2 71

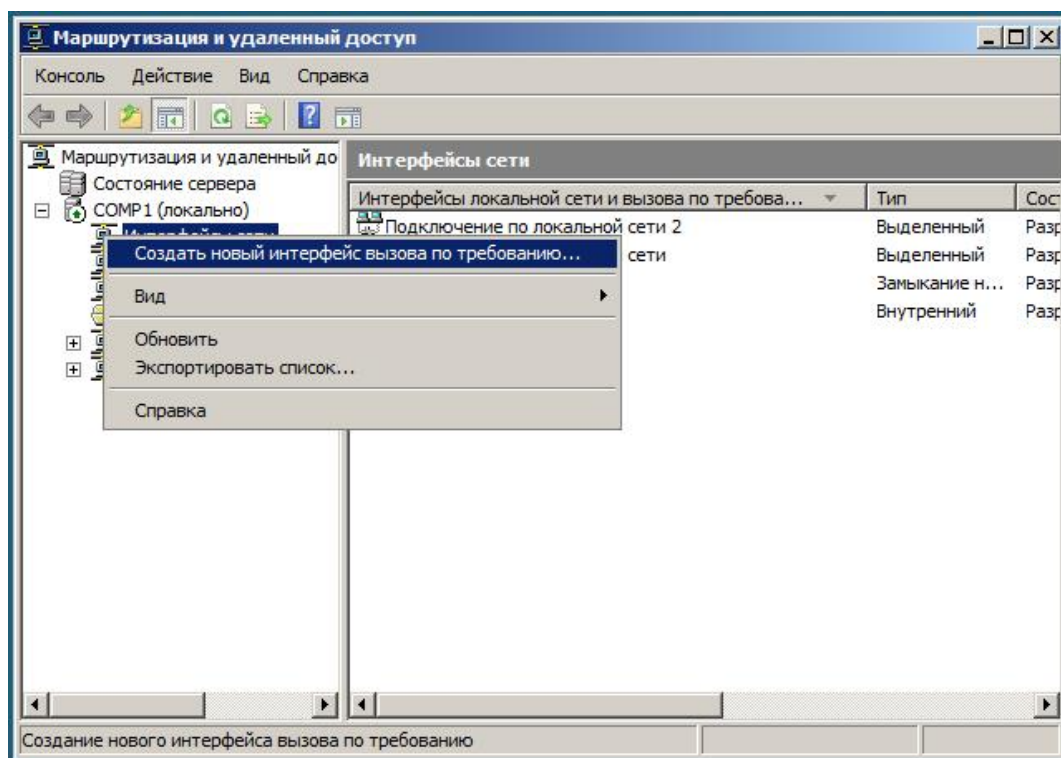
**Создание двух интерфейсов по требованию**

Рисунок 62

При создании интерфейса мастер предложит ввести имя интерфейса, тип соединения, тип VPN, адрес удаленного VPN-сервера.

Если же настраивается сервер филиала (по логике головному офису нет необходимости обращаться за ресурсами в сети филиала – поэтому инициатором соединения выступает сервер филиала), то создавать учетную запись для входящих VPN нет необходимости.

Необходимо указать статический маршрут до удаленной сети, а так же исходящую учетную запись – учетную запись, с которой сервер будет пытаться авторизоваться у другого сервера.

user: IntComp#

password: #

При настройке VPN-сервера головного офиса в мастере следует установить флажок Add a user account so a remote router can dial in.



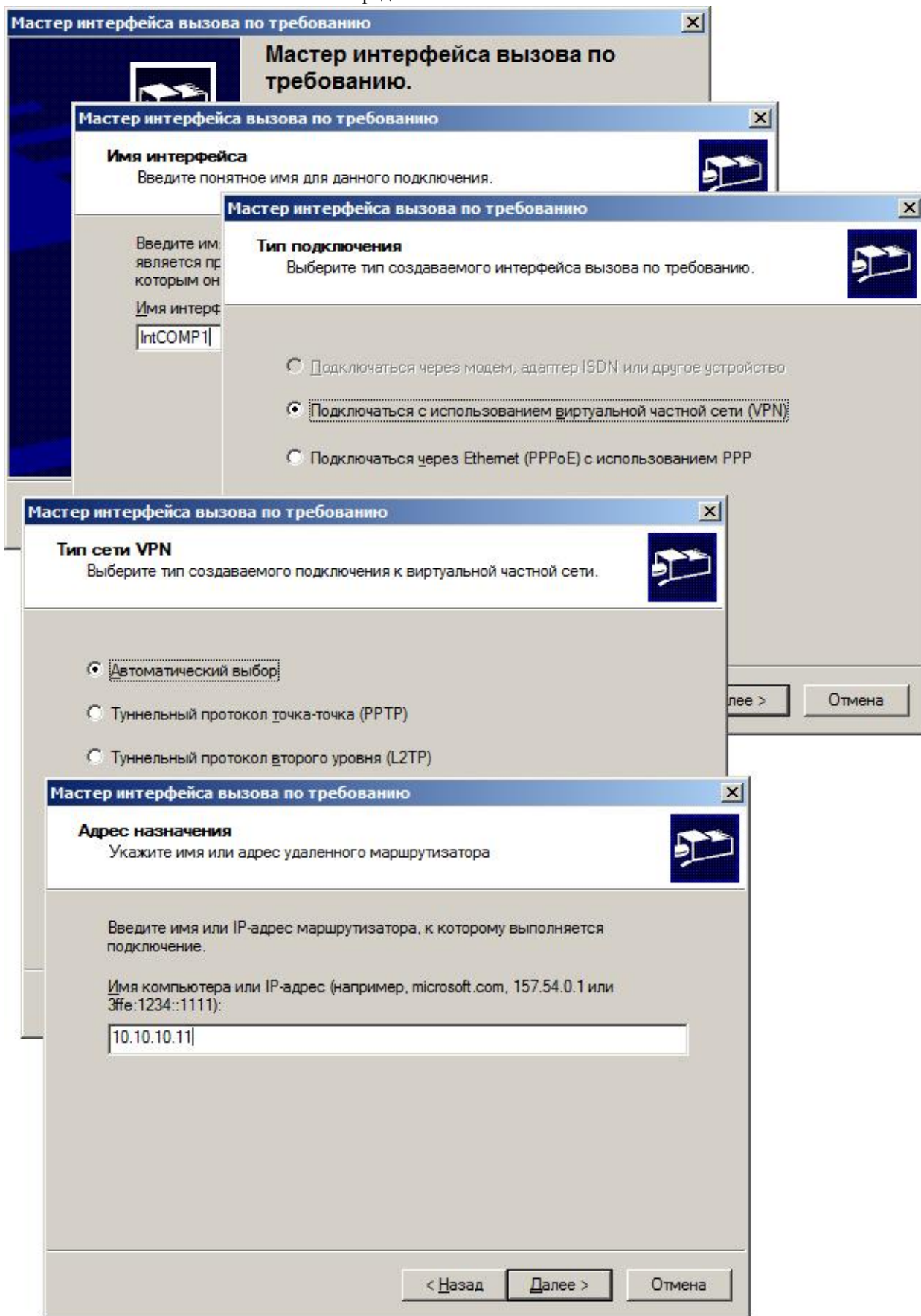


Рисунок 63. Настройка интерфейса по требованию на VPN-сервере филиала

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

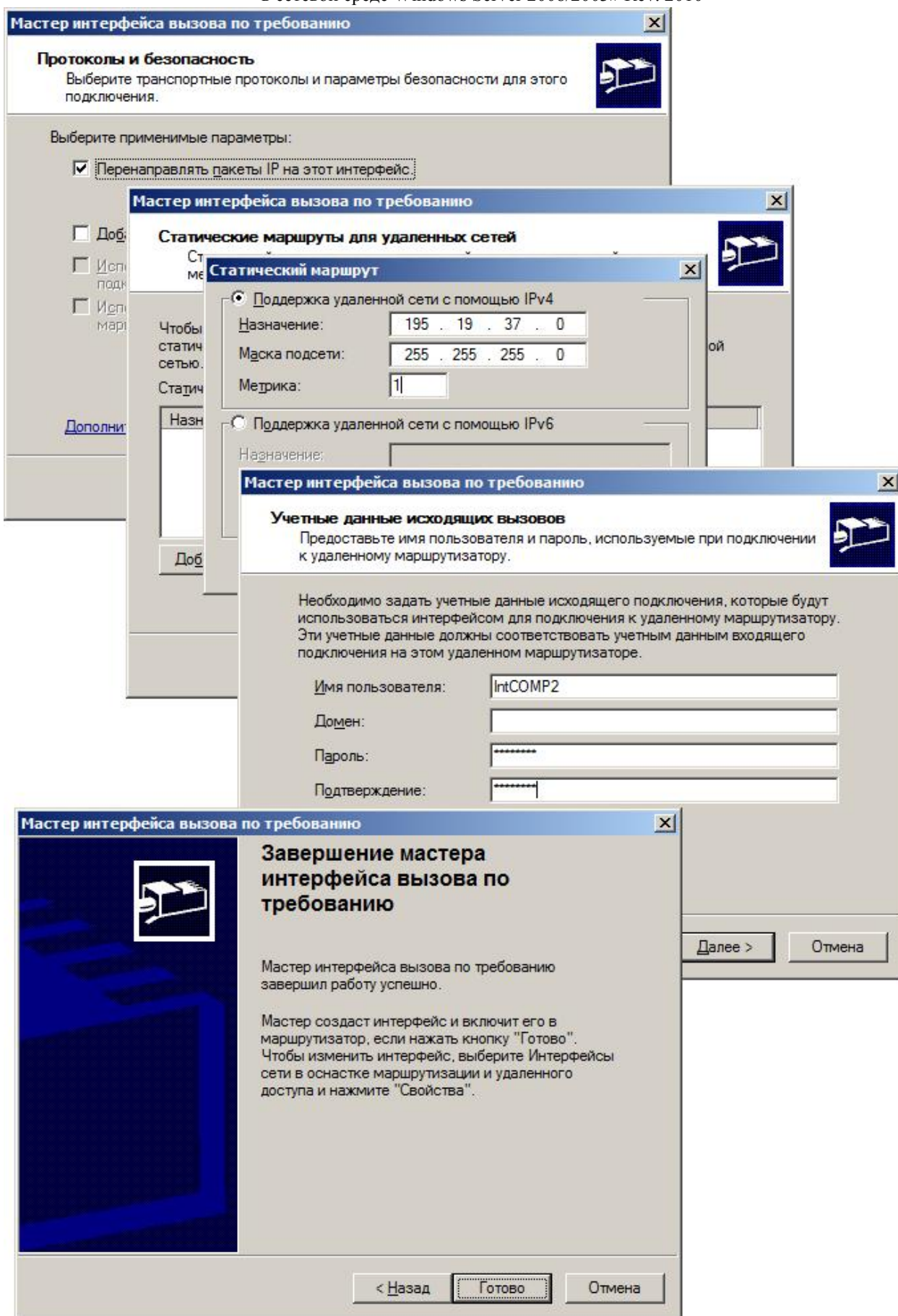


Рисунок 64. Продолжение настройки VPN-сервера филиала

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

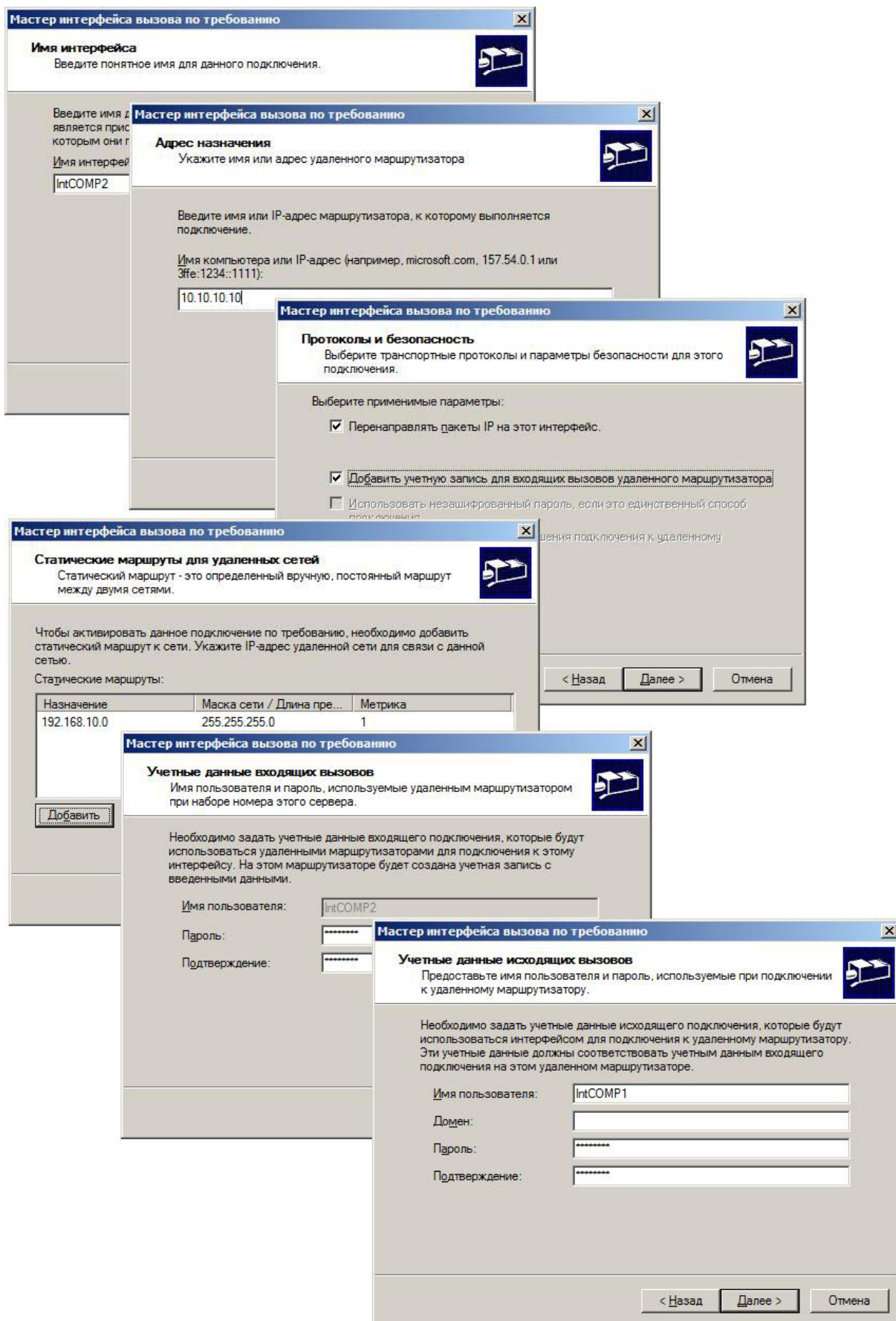


Рисунок 65. Настройка интерфейса по требованию VPN-сервера головного офиса

## Проверка работоспособности

Проверим на наличие в Computer Manager новую учетную запись: IntComp#.

Просмотрим изменения в интерфейсах и таблицах маршрутизации VPN-серверов.

```
Администратор: Командная строка
C:\Users\Администратор>ipconfig

Настройка протокола IP для Windows

Ethernet adapter Подключение по локальной сети 2:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::7158:ede6:624:bc1a%12
    IPv4-адрес . . . . . : 10.10.10.10
    Маска подсети . . . . . : 255.0.0.0
    Основной шлюз . . . . . :

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::85b5:b6da:11f7:427d%10
    IPv4-адрес . . . . . : 192.168.10.11
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . :

Адаптер PPP RAS (Dial In) Interface:

    DNS-суффикс подключения . . . . . :
    IPv4-адрес . . . . . : 192.168.10.15
    Маска подсети . . . . . : 255.255.255.255
    Основной шлюз . . . . . :

Туннельный адаптер Подключение по локальной сети*:

    Состояние носителя . . . . . : Носитель отключен
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 8:

    Состояние носителя . . . . . : Носитель отключен
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 9:

    Состояние носителя . . . . . : Носитель отключен
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 11:

    Состояние носителя . . . . . : Носитель отключен
    DNS-суффикс подключения . . . . . :
```

Рисунок 66. Интерфейсы COMP1

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

```
Администратор: Командная строка
C:\Users\Администратор>ipconfig

Настройка протокола IP для Windows

Ethernet adapter Подключение по локальной сети 2:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::c8d3:cc02:697e:67b%12
    IPv4-адрес. . . . . : 195.19.37.20
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . :

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::352b:e747:3f5c:573a%10
    IPv4-адрес. . . . . : 10.10.10.11
    Маска подсети . . . . . : 255.0.0.0
    Основной шлюз. . . . . :

Адаптер PPP Аа??:

    DNS-суффикс подключения . . . . . :
    IPv4-адрес. . . . . : 195.19.37.25
    Маска подсети . . . . . : 255.255.255.255
    Основной шлюз. . . . . :

Туннельный адаптер Подключение по локальной сети*:

    Состояние носителя. . . . . : Носитель отключен
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 8:

    Состояние носителя. . . . . : Носитель отключен
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 9:

    Состояние носителя. . . . . : Носитель отключен
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 11:

    DNS-суффикс подключения . . . . . :
    IPv6-адрес. . . . . : 2002:c313:2514::c313:2514
    IPv6-адрес. . . . . : 2002:c313:2519::c313:2519
```

Рисунок 67. Интерфейсы COM2

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

```

Администратор: Командная строка
C:\Users\Администратор>route print
=====
Список интерфейсов
12 ...08 00 27 ef d7 4a ..... 10 ...08 00 27 d0 dd ca ..... 15 .....
..... RAS (Dial In) Interface
1 ..... Software Loopback Interface 1
13 ...00 00 00 00 00 00 00 e0 isatap.<B536AD90-1A93-417D-93DC-D0BB41489C2C>
11 ...02 00 54 55 4e 01 ..... Teredo Tunneling Pseudo-Interface
14 ...00 00 00 00 00 00 00 e0 isatap.<8823B1D3-8986-410E-AD73-578E00A08A95>
23 ...00 00 00 00 00 00 00 e0 .....
=====

IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес          Маска сети          Адрес шлюза          Интерфейс          Метрика
10.0.0.0                255.0.0.0           On-link              10.10.10.10        266
10.10.10.10             255.255.255.255    On-link              10.10.10.10        266
10.255.255.255          255.255.255.255    On-link              10.10.10.10        266
127.0.0.0               255.0.0.0           On-link              127.0.0.1          306
127.0.0.1               255.255.255.255    On-link              127.0.0.1          306
127.255.255.255         255.255.255.255    On-link              127.0.0.1          306
192.168.10.0            255.255.255.0      On-link              192.168.10.11     266
192.168.10.11           255.255.255.255    On-link              192.168.10.11     266
192.168.10.15           255.255.255.255    On-link              192.168.10.15     306
192.168.10.255         255.255.255.255    On-link              192.168.10.11     266
195.19.37.0             255.255.255.0      On-link              127.0.0.1          51
195.19.37.255          255.255.255.255    On-link              127.0.0.1          306
224.0.0.0               240.0.0.0           On-link              127.0.0.1          306
224.0.0.0               240.0.0.0           On-link              10.10.10.10        266
224.0.0.0               240.0.0.0           On-link              192.168.10.11     266
224.0.0.0               240.0.0.0           On-link              192.168.10.15     306
255.255.255.255         255.255.255.255    On-link              127.0.0.1          306
255.255.255.255         255.255.255.255    On-link              10.10.10.10        266
255.255.255.255         255.255.255.255    On-link              192.168.10.11     266
255.255.255.255         255.255.255.255    On-link              192.168.10.15     306
=====
Постоянные маршруты:
Отсутствует

IPv6 таблица маршрута
=====
Активные маршруты:
Метрика    Сетевой адрес          Шлюз
1          306    ::1/128                On-link
12         266    fe80::/64              On-link
10         266    fe80::/64              On-link
12         266    fe80::7158:ede6:624:bc1a/128

```

Рисунок 68. Таблица маршрутизации COMPT.

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

```

Администратор: Командная строка
C:\Users\Администратор>route print
=====
Список интерфейсов
12 ...08 00 27 ae 78 63 ..... 10 ...08 00 27 d2 9e 83 ..... 17 .....
14 ...00 00 00 00 00 00 00 e0 ..... Software Loopback Interface 1
11 ...02 00 54 55 4e 01 ..... Teredo Tunneling Pseudo-Interface
13 ...00 00 00 00 00 00 00 e0 ..... isatap.{5AD2368C-D1CE-408E-A28C-1E210CF6E51F}
15 ...00 00 00 00 00 00 00 e0 ..... 6T04 Adapter
24 ...00 00 00 00 00 00 00 e0 .....
=====

IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес          Маска сети          Адрес шлюза          Интерфейс          Метрика
10.0.0.0                255.0.0.0           On-link              10.10.10.11        266
10.10.10.11            255.255.255.255    On-link              10.10.10.11        266
10.255.255.255         255.255.255.255    On-link              10.10.10.11        266
127.0.0.0              255.0.0.0           On-link              127.0.0.1          306
127.0.0.1              255.255.255.255    On-link              127.0.0.1          306
127.255.255.255        255.255.255.255    On-link              127.0.0.1          306
192.168.10.0           255.255.255.0      On-link              127.0.0.1          51
192.168.10.255         255.255.255.255    On-link              127.0.0.1          306
195.19.37.0            255.255.255.0      On-link              195.19.37.20       266
195.19.37.20           255.255.255.255    On-link              195.19.37.20       266
195.19.37.25           255.255.255.255    On-link              195.19.37.25       306
195.19.37.255          255.255.255.255    On-link              195.19.37.20       266
224.0.0.0              240.0.0.0           On-link              127.0.0.1          306
224.0.0.0              240.0.0.0           On-link              195.19.37.20       266
224.0.0.0              240.0.0.0           On-link              10.10.10.11        266
224.0.0.0              240.0.0.0           On-link              195.19.37.25       306
255.255.255.255        255.255.255.255    On-link              127.0.0.1          306
255.255.255.255        255.255.255.255    On-link              195.19.37.20       266
255.255.255.255        255.255.255.255    On-link              10.10.10.11        266
255.255.255.255        255.255.255.255    On-link              195.19.37.25       306
=====
Постоянные маршруты:
Отсутствует

IPv6 таблица маршрута
=====
Активные маршруты:
Метрика  Сетевой адрес          Шлюз
1         306  ::1/128                On-link
15        1010 2002::/16              On-link
15        266  2002:c313:2514::c313:2514/128
On-link

```

Рисунок 69. Таблица маршрутизации COMPT.

В свойствах интерфейсах по требованию установим время простоя до разрыва соединения в 1 минуту.

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

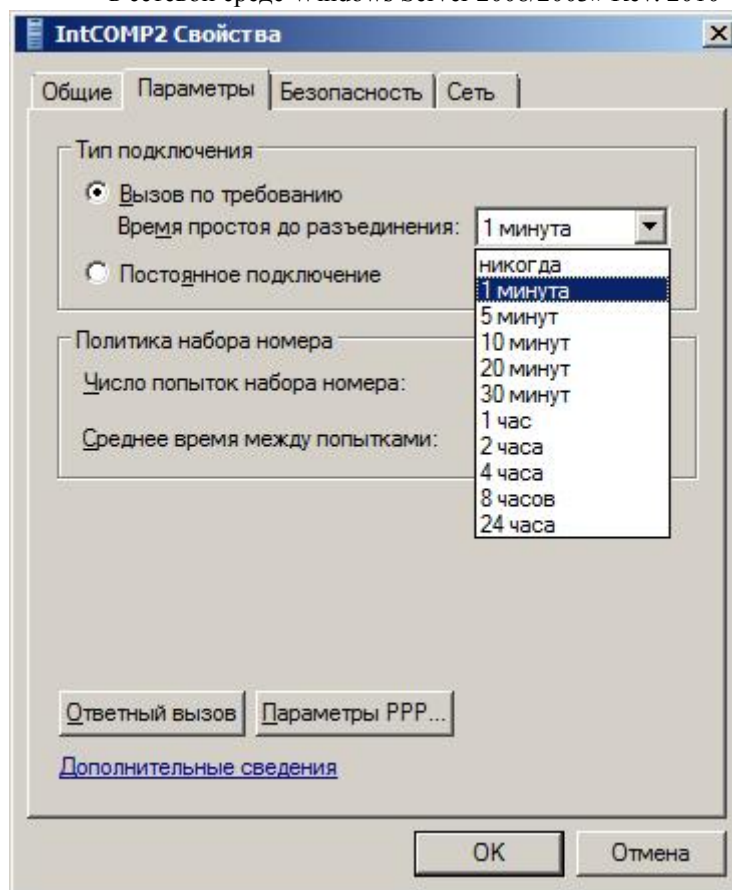


Рисунок 70

Убедимся, что интерфейсы «лежат» (или хотя бы один).

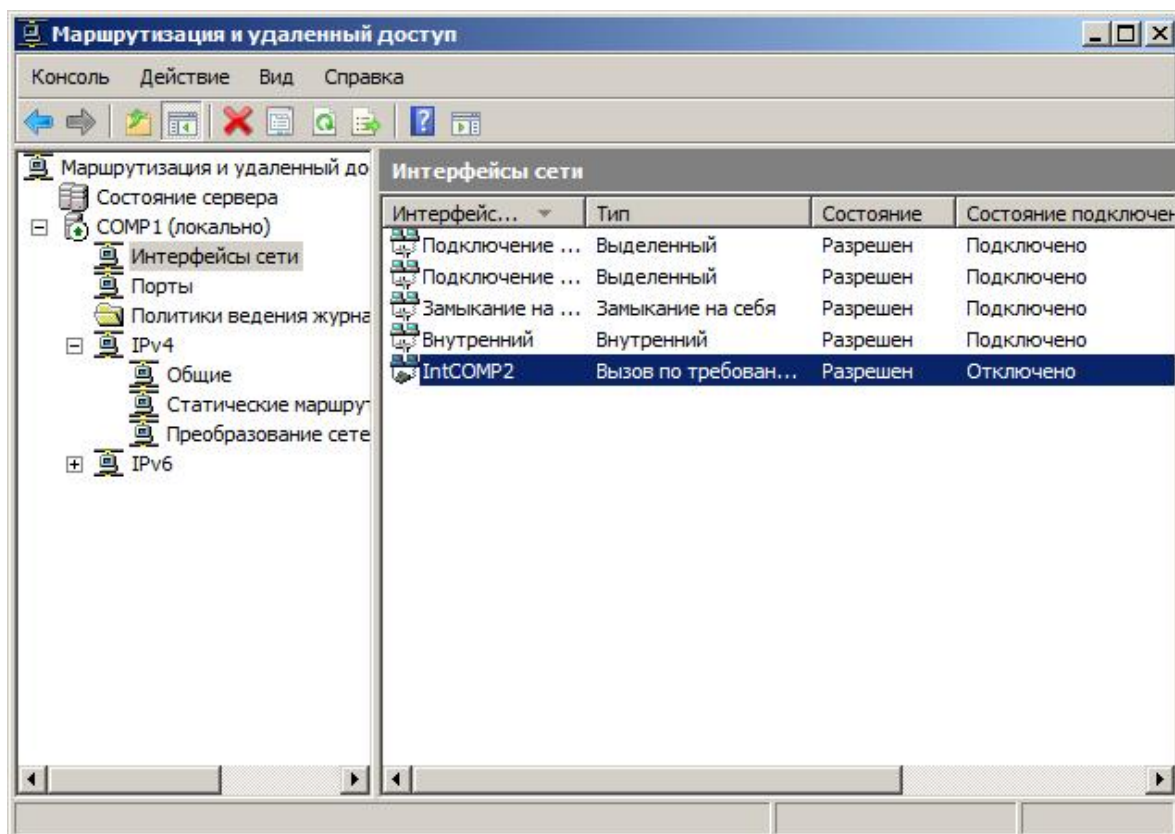
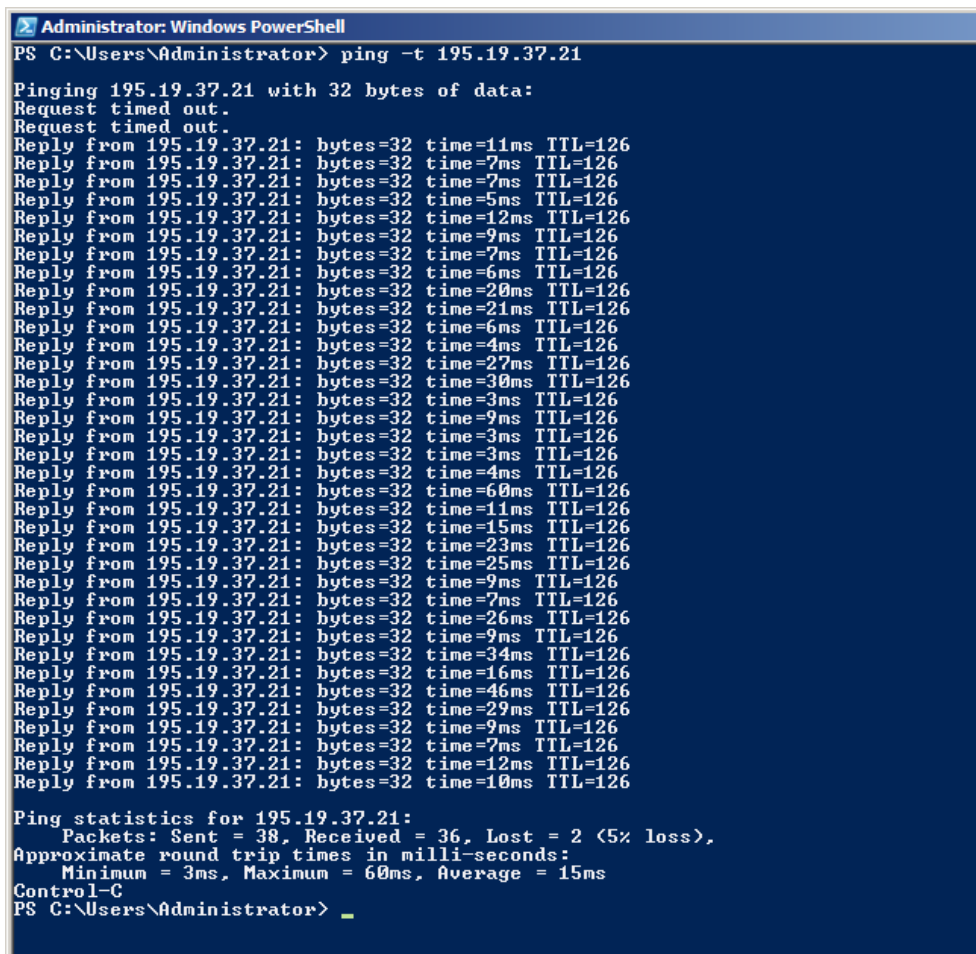


Рисунок 71



Запустим команду ping с параметром `-t` на адрес 195.19.37.21 с COM4 (Из филиала в головной офис):



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ping -t 195.19.37.21

Pinging 195.19.37.21 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 195.19.37.21: bytes=32 time=11ms TTL=126
Reply from 195.19.37.21: bytes=32 time=7ms TTL=126
Reply from 195.19.37.21: bytes=32 time=7ms TTL=126
Reply from 195.19.37.21: bytes=32 time=5ms TTL=126
Reply from 195.19.37.21: bytes=32 time=12ms TTL=126
Reply from 195.19.37.21: bytes=32 time=9ms TTL=126
Reply from 195.19.37.21: bytes=32 time=7ms TTL=126
Reply from 195.19.37.21: bytes=32 time=6ms TTL=126
Reply from 195.19.37.21: bytes=32 time=20ms TTL=126
Reply from 195.19.37.21: bytes=32 time=21ms TTL=126
Reply from 195.19.37.21: bytes=32 time=6ms TTL=126
Reply from 195.19.37.21: bytes=32 time=4ms TTL=126
Reply from 195.19.37.21: bytes=32 time=27ms TTL=126
Reply from 195.19.37.21: bytes=32 time=30ms TTL=126
Reply from 195.19.37.21: bytes=32 time=3ms TTL=126
Reply from 195.19.37.21: bytes=32 time=9ms TTL=126
Reply from 195.19.37.21: bytes=32 time=3ms TTL=126
Reply from 195.19.37.21: bytes=32 time=3ms TTL=126
Reply from 195.19.37.21: bytes=32 time=4ms TTL=126
Reply from 195.19.37.21: bytes=32 time=60ms TTL=126
Reply from 195.19.37.21: bytes=32 time=11ms TTL=126
Reply from 195.19.37.21: bytes=32 time=15ms TTL=126
Reply from 195.19.37.21: bytes=32 time=23ms TTL=126
Reply from 195.19.37.21: bytes=32 time=25ms TTL=126
Reply from 195.19.37.21: bytes=32 time=9ms TTL=126
Reply from 195.19.37.21: bytes=32 time=7ms TTL=126
Reply from 195.19.37.21: bytes=32 time=26ms TTL=126
Reply from 195.19.37.21: bytes=32 time=9ms TTL=126
Reply from 195.19.37.21: bytes=32 time=34ms TTL=126
Reply from 195.19.37.21: bytes=32 time=16ms TTL=126
Reply from 195.19.37.21: bytes=32 time=46ms TTL=126
Reply from 195.19.37.21: bytes=32 time=29ms TTL=126
Reply from 195.19.37.21: bytes=32 time=9ms TTL=126
Reply from 195.19.37.21: bytes=32 time=7ms TTL=126
Reply from 195.19.37.21: bytes=32 time=12ms TTL=126
Reply from 195.19.37.21: bytes=32 time=10ms TTL=126

Ping statistics for 195.19.37.21:
    Packets: Sent = 38, Received = 36, Lost = 2 (5% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 60ms, Average = 15ms
Control-C
PS C:\Users\Administrator> _
```

Рисунок 72

Из предыдущего рисунка видно, что соединение установилось спустя некоторое время. Это время тратится на установление туннеля, аутентификацию, авторизацию.

Убедимся, что интерфейсы подняты (или хотя бы один поднят).

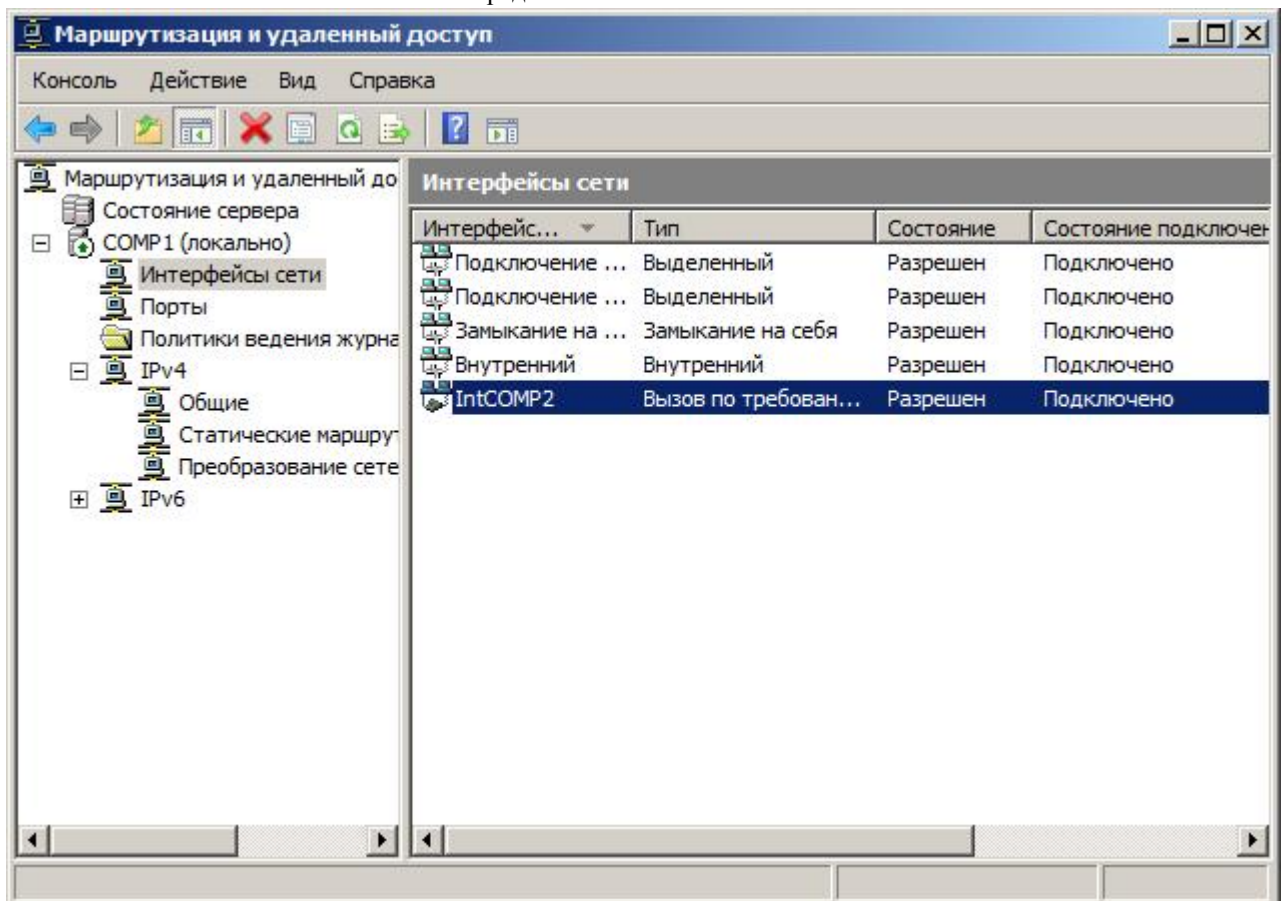
Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

Рисунок 73

Теперь подождем 1 минуту, пакеты при этом между серверами не должны ходить. И убедимся, что туннель исчез. В этом можно убедиться проверив интерфейсы.

Если же предсказанного с интерфейсами не произошло, то необходимо выполнить Refresh.

Если требуется установить постоянное соединение между VPN-серверами, то необходимо в свойствах обоих серверов указать Persistent connection.

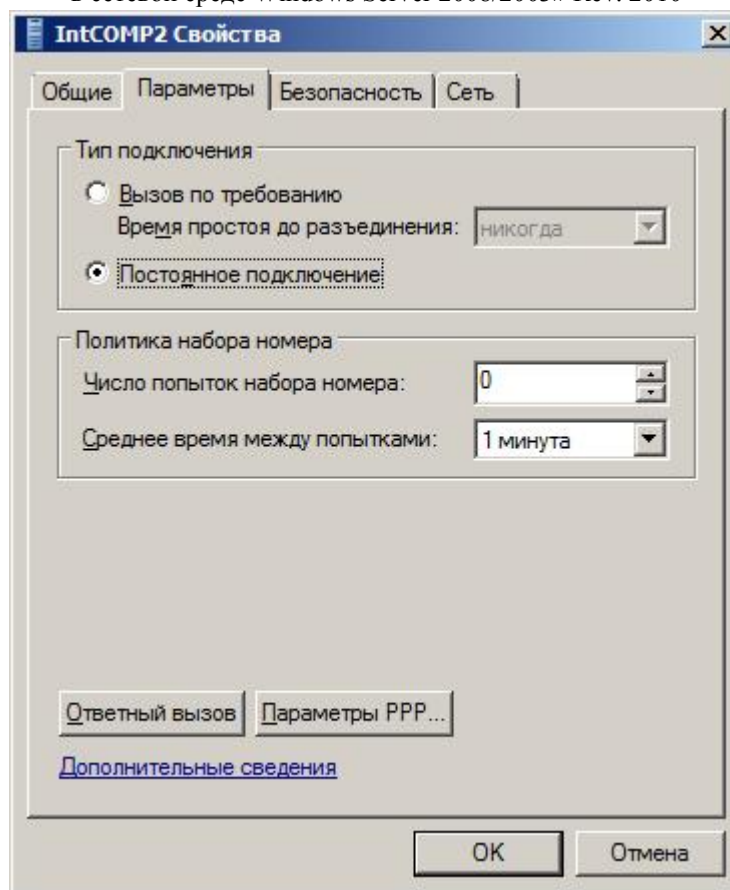
Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

Рисунок 74

Просмотрим интерфейсы и таблицы маршрутизации VPN-серверов в состоянии включенного туннеля.

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

```
Администратор: Командная строка
C:\Users\Администратор>ipconfig

Настройка протокола IP для Windows

Адаптер PPP IntCOMP2:

    DNS-суффикс подключения . . . . . :
    IPv4-адрес . . . . . : 195.19.37.28
    Маска подсети . . . . . : 255.255.255.255
    Основной шлюз . . . . . :

Ethernet adapter Подключение по локальной сети 2:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::7158:ede6:624:bc1a%12
    IPv4-адрес . . . . . : 10.10.10.10
    Маска подсети . . . . . : 255.0.0.0
    Основной шлюз . . . . . :

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::85b5:b6da:11f7:427d%10
    IPv4-адрес . . . . . : 192.168.10.11
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . :

Адаптер PPP RAS (Dial In) Interface:

    DNS-суффикс подключения . . . . . :
    IPv4-адрес . . . . . : 192.168.10.15
    Маска подсети . . . . . : 255.255.255.255
    Основной шлюз . . . . . :

Туннельный адаптер Подключение по локальной сети*:

    Состояние носителя . . . . . : Носитель отключен
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 8:

    Состояние носителя . . . . . : Носитель отключен
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 9:

    Состояние носителя . . . . . : Носитель отключен
```

Рисунок 75. COMP1

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

```
Администратор: Командная строка
C:\Users\Администратор>ipconfig

Настройка протокола IP для Windows

Адаптер PPP Int2:

    DNS-суффикс подключения . . . . . :
    IPv4-адрес . . . . . : 192.168.10.18
    Маска подсети . . . . . : 255.255.255.255
    Основной шлюз . . . . . :

Ethernet adapter Подключение по локальной сети 2:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::c8d3:cc02:697e:67b12
    IPv4-адрес . . . . . : 195.19.37.20
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . :

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::352b:e747:3f5c:573a10
    IPv4-адрес . . . . . : 10.10.10.11
    Маска подсети . . . . . : 255.0.0.0
    Основной шлюз . . . . . :

Адаптер PPP Аа??:

    DNS-суффикс подключения . . . . . :
    IPv4-адрес . . . . . : 195.19.37.25
    Маска подсети . . . . . : 255.255.255.255
    Основной шлюз . . . . . :

Туннельный адаптер Подключение по локальной сети*:

    Состояние носителя . . . . . : Носитель отключен
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 8:

    Состояние носителя . . . . . : Носитель отключен
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 9:

    Состояние носителя . . . . . : Носитель отключен
```

Рисунок 76. COMP2

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

```

C:\Users\Администратор>route print
=====
Список интерфейсов
21 ..... IntCOMP2
12 ..08 00 27 ef d7 4a ..... 10 ..08 00 27 d0 dd ca ..... 15 .....
..... RAS (Dial In) Interface
1 ..... Software Loopback Interface 1
13 ..00 00 00 00 00 00 e0 isatap.<B536AD90-1A93-417D-93DC-D0BB41489C2C>
11 ..02 00 54 55 4e 01 ..... Teredo Tunneling Pseudo-Interface
14 ..00 00 00 00 00 00 e0 isatap.<8823B1D3-8986-410E-AD73-578E00A08A95>
23 ..00 00 00 00 00 00 e0 22 ..00 00 00 00 00 00 e0 24 ..00 00 00
00 00 00 00 e0
=====

IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес          Маска сети          Адрес шлюза          Интерфейс          Метрика
10.0.0.0                255.0.0.0           On-link              10.10.10.10        266
10.10.10.10             255.255.255.255    On-link              10.10.10.10        266
10.10.10.11             255.255.255.255    On-link              10.10.10.10        11
10.255.255.255          255.255.255.255    On-link              10.10.10.10        266
127.0.0.0               255.0.0.0           On-link              127.0.0.1          306
127.0.0.1               255.255.255.255    On-link              127.0.0.1          306
127.255.255.255         255.255.255.255    On-link              127.0.0.1          306
192.168.10.0            255.255.255.0      On-link              192.168.10.11      266
192.168.10.11           255.255.255.255    On-link              192.168.10.11      266
192.168.10.15           255.255.255.255    On-link              192.168.10.15      306
192.168.10.255          255.255.255.255    On-link              192.168.10.11      266
195.19.37.0             255.255.255.0      192.168.10.18       195.19.37.28       11
195.19.37.28            255.255.255.255    On-link              195.19.37.28       266
224.0.0.0               240.0.0.0           On-link              127.0.0.1          306
224.0.0.0               240.0.0.0           On-link              10.10.10.10        266
224.0.0.0               240.0.0.0           On-link              192.168.10.11      266
224.0.0.0               240.0.0.0           On-link              192.168.10.15      306
255.255.255.255         255.255.255.255    On-link              127.0.0.1          306
255.255.255.255         255.255.255.255    On-link              10.10.10.10        266
255.255.255.255         255.255.255.255    On-link              192.168.10.11      266
255.255.255.255         255.255.255.255    On-link              192.168.10.15      306
255.255.255.255         255.255.255.255    On-link              195.19.37.28       266
=====
Постоянные маршруты:
Отсутствует

IPv6 таблица маршрута
=====
Активные маршруты:
Метрика  Сетевой адрес          Шлюз

```

Рисунок 77. COMP1

Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

```

Администратор: Командная строка
C:\Users\Administrator>route print
=====
Список интерфейсов
21 ..... Int2
12 ...08 00 27 ae 78 63 ..... 10 ...08 00 27 d2 9e 83 ..... 17 .....
..... 1 ..... Software Loopback Interface 1
14 ...00 00 00 00 00 00 e0 isatap.<4560DA01-0799-4938-B553-4148EEF36B3A>
11 ...02 00 54 55 4e 01 ..... Teredo Tunneling Pseudo-Interface
13 ...00 00 00 00 00 00 e0 isatap.<5AD2368C-D1CE-408E-A28C-1E210CF6E51F>
15 ...00 00 00 00 00 00 e0 6T04 Adapter
24 ...00 00 00 00 00 00 e0 25 ...00 00 00 00 00 00 e0 =====

IPv4 таблица маршрута
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
10.0.0.0           255.0.0.0      On-link          10.10.10.11    266
10.10.10.11       255.255.255.255 On-link          10.10.10.11    266
10.255.255.255    255.255.255.255 On-link          10.10.10.11    266
127.0.0.0         255.0.0.0      On-link          127.0.0.1      306
127.0.0.1         255.255.255.255 On-link          127.0.0.1      306
127.255.255.255  255.255.255.255 On-link          127.0.0.1      306
192.168.10.0      255.255.255.0  195.19.37.28    192.168.10.18  11
192.168.10.18    255.255.255.255 On-link          192.168.10.18  266
195.19.37.0      255.255.255.0  On-link          195.19.37.20   266
195.19.37.20     255.255.255.255 On-link          195.19.37.20   266
195.19.37.25     255.255.255.255 On-link          195.19.37.25   306
195.19.37.255   255.255.255.255 On-link          195.19.37.20   266
224.0.0.0        240.0.0.0      On-link          127.0.0.1      306
224.0.0.0        240.0.0.0      On-link          195.19.37.20   266
224.0.0.0        240.0.0.0      On-link          10.10.10.11     266
224.0.0.0        240.0.0.0      On-link          195.19.37.25   306
255.255.255.255  255.255.255.255 On-link          127.0.0.1      306
255.255.255.255  255.255.255.255 On-link          195.19.37.20   266
255.255.255.255  255.255.255.255 On-link          10.10.10.11     266
255.255.255.255  255.255.255.255 On-link          195.19.37.25   306
255.255.255.255  255.255.255.255 On-link          192.168.10.18   266
=====
Постоянные маршруты:
Отсутствует

IPv6 таблица маршрута
=====
Активные маршруты:
Метрика  Сетевой адрес      Шлюз
1         306  ::1/128             On-link
15        1010 2002::/16         On-link

```

Рисунок 78. COMP2

Выполним трассировку с машины из филиала до машины из офиса.

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> tracert 195.19.37.21

Tracing route to COMP3 [195.19.37.21]
over a maximum of 30 hops:

  1      1 ms      1 ms      1 ms  COMP1 [192.168.10.11]
  2      8 ms      *         3 ms  192.168.10.18
  3      9 ms      7 ms     23 ms  COMP3 [195.19.37.21]

Trace complete.
PS C:\Users\Administrator>

```

Рисунок 79

**LAB 4. Сквозное VPN-соединение**Задание:

Клиент из сети 192.168.10.x/24 устанавливает VPN-соединение с сетью 172.16.0.x/16 через Интернет. При настройке туннеля необходимо настроить фильтры, отбрасывающие весь трафик не связанный с данным туннелем.

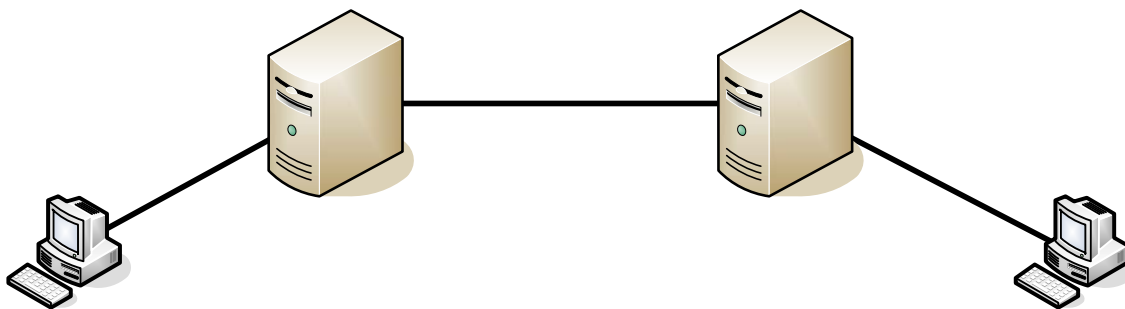


Рисунок 80.

План выполнения работы:

- Настройка сетевых адаптеров
- Настройка VPN-сервера А с полным мастером
- Настройка VPN-сервера В без мастера.
- Заведение группы VPNPassThrouhg для сервера В и учетных записей
- Заведение политики доступа для сервера А – доступ для всех VPN-соединений
- Заведение политики доступа для сервера В – доступ для группы VPNPassThrouhg
- Настройка фильтров на сервере В
- Установление соединения с сервером В, сервером А
- Проверка результата работы

**B**

20

11

195

**Настройка сетевых адаптеров****VPN**

Сервер	Интерфейс	IP-address	Subnet mask	Default gateway
Comp1	interface1	192.168.10.10	255.255.255.0	
Comp2	interface1	192.168.10.11	255.255.255.0	
	interface2	195.19.37.20	255.255.255.0	
Comp3	interface1	195.19.37.21	255.255.255.0	
	interface2	172.16.0.11	255.255.0.0	
Comp4	interface1	172.16.0.10	255.255.0.0	



## **Настройка VPN-сервера А**

В мастере выбираем:

Интерфейс подсоединенный к Интернету: 195.19.37.21

Установить флажок: Enable security

Диапазон выделенных IP-адресов: 172.16.0.15.. 172.16.0.20

Отказываемся от RADIUS.

## **Настройка VPN-сервера В**

В мастере выбираем:

Интерфейс подсоединенный к Интернету: 195.19.37.20

Сбросить флажок: Enable security

Диапазон выделенных IP-адресов: 195.19.37.25..195.19.37.30

Отказываемся от RADIUS.

## **Создание группы VPNPassThrouhg для сервера В и учетных записей**

На сервере В заведем группу VPNPassThrouhg.

На сервере А заведем учетную запись: remoteA, a.

На сервере В заведем учетную запись: remoteB, b.

## **Создание политики доступа для сервера А – доступ для всех VPN-соединений**

## **Создание политики доступа для сервера В – доступ для группы VPNPassThrouhg**

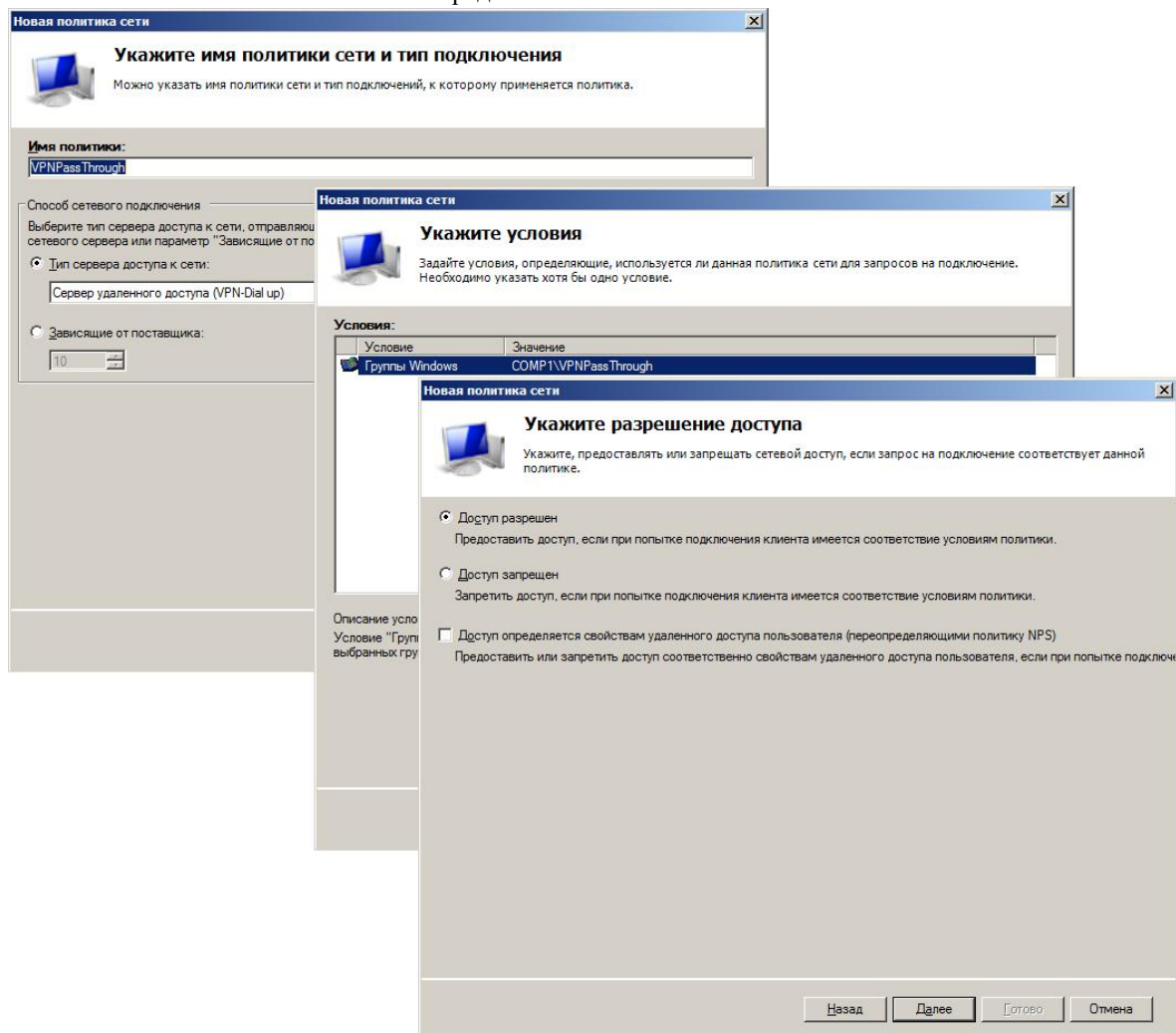
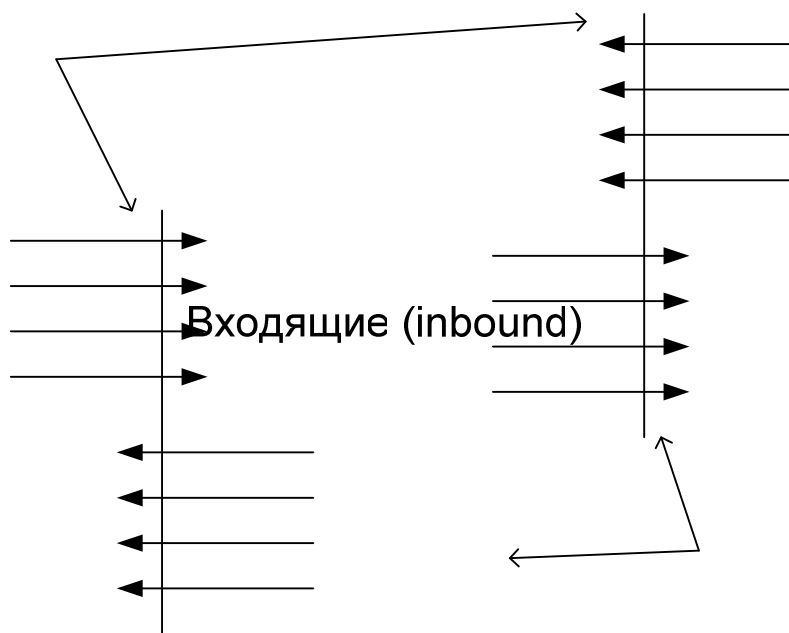
Практикум «Построение виртуальных частных сетей VPN  
в сетевой среде Windows Server 2008/2003» Rev. 2010

Рисунок 81

**Настройка фильтров на сервере В**

# VPN-сервер В



На 192.168.10.11/32, protocol 47

Рисунок 82

На 192.168.10.11/32 на tcp 1723

C 195.19.

C 195.19.

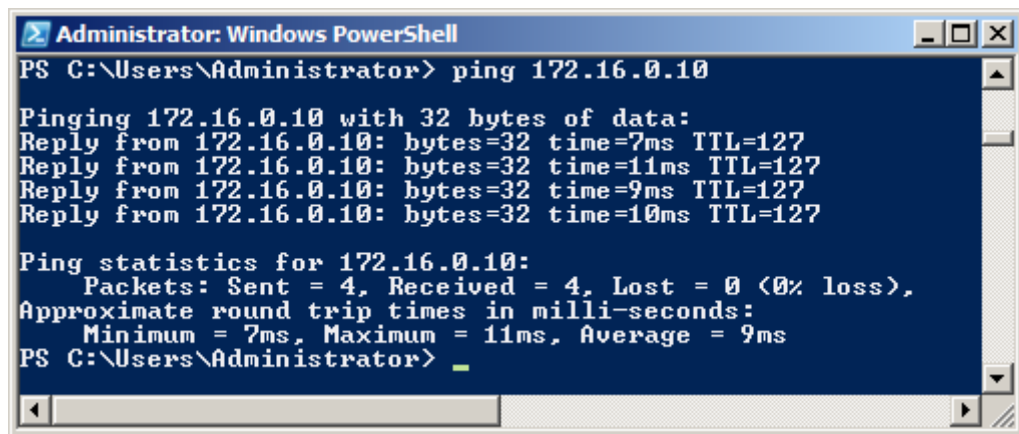
## Установка соединения с сервером В, сервером А

Property	Value
Device Name	WAN Miniport (PPTP)
Device Type	vpn
Authentication	MS CHAP V2
Encryption	MPPE 128
Compression	(none)
PPP multilink framing	Off
Client IPv4 address	195.19.37.29
Server IPv4 address	195.19.37.25
NAP State	Not NAP-capable
Origin address	(unknown)
Destination address	192.168.10.11

Property	Value
Device Name	WAN Miniport (PPTP)
Device Type	vpn
Authentication	MS CHAP V2
Encryption	MPPE 128
Compression	(none)
PPP multilink framing	Off
Client IPv4 address	172.16.0.17
Server IPv4 address	172.16.0.15
NAP State	Not NAP-capable
Origin address	(unknown)
Destination address	195.19.37.21

Рисунок 83

**Проверка результата работы**A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window shows the execution of a ping command to the IP address 172.16.0.10. The output indicates that all four packets were received successfully with 0% loss. The round trip times are listed as follows: Minimum = 7ms, Maximum = 11ms, and Average = 9ms.

```
PS C:\Users\Administrator> ping 172.16.0.10

Pinging 172.16.0.10 with 32 bytes of data:
Reply from 172.16.0.10: bytes=32 time=7ms TTL=127
Reply from 172.16.0.10: bytes=32 time=11ms TTL=127
Reply from 172.16.0.10: bytes=32 time=9ms TTL=127
Reply from 172.16.0.10: bytes=32 time=10ms TTL=127

Ping statistics for 172.16.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 11ms, Average = 9ms
PS C:\Users\Administrator>
```

Рисунок 84

Похвально! Вы успешно выполнили конфигурирование непрямых VPN – подключений. Не забывайте документировать скриншотами трассировку пройденных этапов работы. Оформленные скриншоты являются документальным отчетом выполненной лабораторной работы.