2) изучить содержимое окон Frame Summary и Frame Details, объяснить и сохранить полученные результаты;

3) повторить эксперимент с передачей файла, содержащего «1», объяснить полученный результат.

Этап 5. Возобновление обычного режима связи между компьютерами

1. На обоих компьютерах в консоли mmc, вызвав контекстное меню, снять ранее назначенные политики IPSec.

2. Закрыть окна программ mmc.exe, cmd.exe, MS Network Monitor.

3. Возобновить первоначальные значения настроек сетевого интерфейса.

4. Выйти из системы, завершив сеанс работы от имени администратора.

Требования к содержанию отчета

Отчет должен включать:

- номер, тема и цель работы;
- краткие теоретические сведения по работе;
- ход выполнения работы со скриншотами основных окон настроек;
- распечатки результатов экспериментов с комментариями к ним;
- выводы по работе.

Контрольные вопросы

1. Какие три протокола представляют ядро IPSec и какое назначение каждого из них?

2. Какова последовательность работы протокола IPSec?

3. Какая структура IP-пакета после применения протокола AH в транспортном и туннельном режимах?

4. Какая структура IP-пакета после применения протокола ESP в транспортном и туннельном режимах?

5. Чем отличаются транспортный и туннельный режимы работы IPSec?

6. Какие методы проверки подлинности (IKE) обеспечиваются ОС Windows? Опишите их отличительные особенности.

7. Назовите алгоритмы проверки целостности и шифрования используемые в ОС Windows для обеспечения безопасности при обмене ключами и передачи данных.

8. Из каких полей состоят заголовки AH и ESP?

9. Структура IKE-сообщения.

1.7 Удаленный доступ к сети с использованием виртуального защищенного соединения PPTP и L2TP

Цель и задачи работы

1. Изучить протоколы туннелирования PPTP и L2TP.
2. В лабораторных условиях ознакомиться с процессом организации удаленного доступа к сети с использованием виртуального защищенного соединения.
3. Провести эксперименты для проверки работы протоколов.

Подготовка к лабораторной работе

При подготовке к лабораторной работе необходимо:
- ознакомиться с целью и задачами исследования;
- изучить теоретический материал, приведенный в учебном пособии;
- бесплатно скачать с официального сайта: http://www.microsoft.com/en-us/download/details.aspx?id=4865 утилиту Microsoft Network Monitor 3.4, инсталлировать ее на компьютерах лаборатории, ознакомиться с правилами ее использования.

Теоретический материал

Средства VPN, применяемые на канальном уровне модели OSI, позволяют обеспечить инкапсуляцию различных видов трафика третьего уровня (и выше) и построение виртуальных туннелей типа «точка-точка» (от маршрутизатора к маршрутизатору или от персонального компьютера к шлюзу ЛС) (рис. 1). Туннелирование само по себе не решает задачи обеспечения безопасности передачи данных. Специальные пакеты предназначены всего лишь для маршрутизации данных в точку назначения.

Протоколы PPTP (Point-to-Point Tunneling Protocol) и L2TP (Layer-2 Tunneling Protocol) – это протоколы туннелирования канального уровня модели OSI. Протокол PPTP осуществляет туннелирование и шифрование передаваемых данных. Протокол L2TP поддерживает только функцию туннелирования, поэтому для защиты данных необходимо использовать дополнительный протокол IPSec.

Протоколы PPTP и L2TP основываются на стандартном протоколе канального уровня PPP (Point-to-Point Protocol) и являются его расширениями.

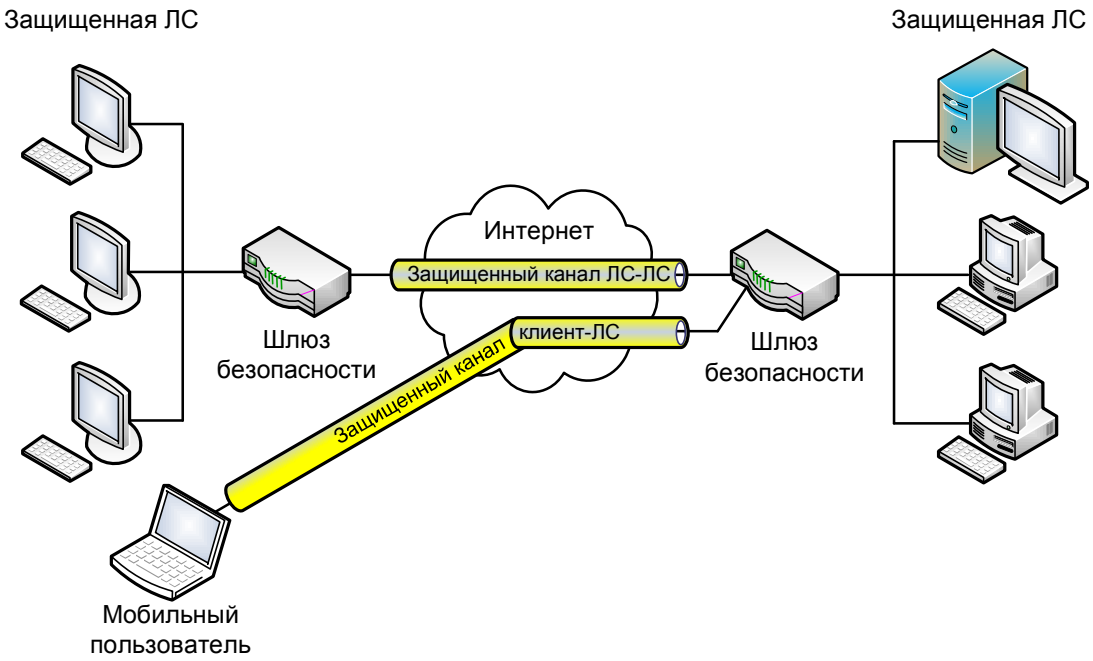

Рис. 1. Виртуальные защищенные каналы типа ЛС-ЛС и клиент-ЛС

В набор PPP входят протокол управления соединением LCP (Link Control Protocol), ответственный за конфигурацию, установку, работу и завершение соединения «точка-точка», и протокол управления сетью NCP (Network Control Protocol), способный инкапсулировать в PPP протоколы сетевого уровня для транспортировки через соединение «точка-точка».

Процесс доставки конфиденциальных данных:

1) инкапсуляция данных с помощью протокола PPP;

2) шифрование и собственная инкапсуляция протоколами PPTP и L2TP;

3) упаковка в протокол IP;

4) продвижение пакета в сетях TCP/IP из начальной точки в конечную;

5) проверка и деинкапсуляция пакетов в точке приема.

Пакеты, передаваемые в рамках сессии PPTP, имеют структуру показанную на рис. 2.

Заголовок кадра передачи	IP-заголовок	GRE-заголовок маршрутизации	PPP-заголовок	Данные PPP	Концевик кадра передачи

Рис. 2. Структура пакета для пересылки по туннелю PPTP

По протоколу PPTP при создании защищенного виртуального канала производится аутентификация удаленного пользователя и шифрование передаваемых данных (рис. 3).

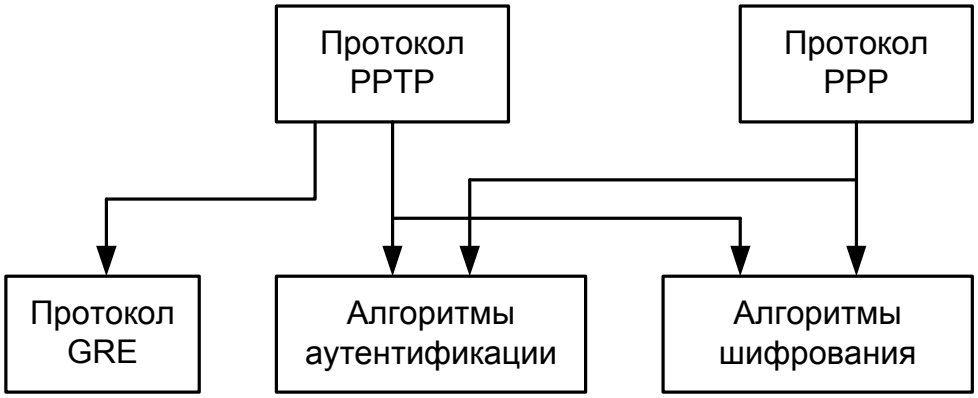

Рис. 3. Архитектура протокола PPTP

Для аутентификации может использоваться один из перечисленных протоколов: распознавание по паролю PAP (Password Authentication Protocol), распознавание при рукопожатии MSCHAP (Microsoft Challenge-Handshaking Authentication Protocol) и распознавание EAP-TLS (Extensible Authentication Protocol – Transport Layer Security).

Для шифрования используется протокол MPPE (Microsoft Point-to-Point Encryption), который совместим только с MSCHAP (версии 1 и 2) и EAP-TLS. Протокол MPPE поддерживает работу с ключами длиной 40, 56 и 128 бит, он изменяет значение ключа шифрования после каждого принятого пакета.

Для установления соединения по протоколу PPTP между удаленным пользователем и локальной сетью необходимо наличие:

- на компьютере пользователя – установленная клиентская часть сервиса удаленного доступа RAS (Remote Access Service) и драйвер PPTP, которые входят в состав ОС Windows;
- на сервере удаленного доступа локальной сети (функции которого может выполнять пограничный маршрутизатор с поддержкой используемых протоколов или компьютер с ОС Windows Server) – сервер RAS и драйвер PPTP.

Недостатки протокола PPTP:

- возможность создания туннеля только поверх TCP/IP сетей;
- уязвимости протоколов аутентификации;
- слабая аутентификация пользователя (по паролю) и отсутствие аутентификации компьютера;

- протокол шифрования MPPE не поддерживается большинством сетевого оборудования.

Протокол L2TP разработан в организации IETF (Internet Engineering Task Force) при поддержке компаний CISCO Systems и Microsoft, как альтернатива протоколу PPTP.

В отличие от PPTP, протокол L2TP не привязан к протоколу IP, поэтому он может быть использован в сетях с коммутацией пакетов (например ATM) или в сетях с ретрансляцией кадров (Frame Relay). Кроме того, в протокол L2TP добавлена функция управления потоками данных и дополнительных функций защиты, в частности, включена возможность работы с протоколами AH и ESP стека протоколов IPSec (рис. 4).

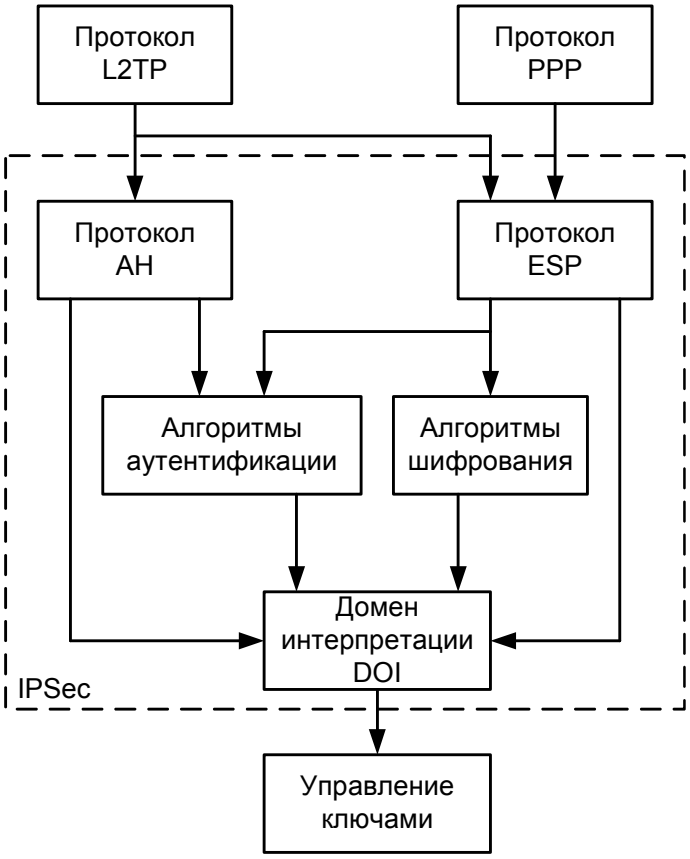

Рис. 4. Архитектура протокола L2TP

Протокол L2TP (поверх IPSec) выполняет аутентификацию на уровнях «компьютер» и «пользователь», а также шифрование данных надежнее, чем PPTP. В отличие от протокола PPTP, L2TP предоставляет возможность открывать между конечными абонентами сразу несколько туннелей, каждый из которых может быть выделен для отдельного приложения.

Согласно спецификации протокола L2TP роль сервера удаленного доступа выполняет концентратор LAC (L2TP Access Concentrator), который обеспечивает удаленному пользователю доступ к его ЛС через Интернет. В качестве сервера удаленного доступа ЛС выступает сетевой сервер LNS (L2TP Network Server), функционирующий на совместимых с протоколом PPP платформах.

Три этапа формирования VPN-канала:

1) установление соединение с сервером удаленного доступа ЛС;
2) аутентификация пользователя;
3) конфигурирование защищенного туннеля.

Недостатки протокола L2TP:

- для его реализации необходима поддержка Интернет-провайдеров;
- ограничивает трафик рамками выбранного туннеля и лишает пользователей доступа к другим частям Интернета;
- спецификация обеспечивает шифрование только в IP-сетях с IPSec.

Этапы выполнения работы

1. Настройка VPN-сервера с ОС Windows Server 2008 R2.
2. Настройка VPN-клиента с ОС Windows XP.
3. Настройка компьютера в локальной сети.
4. Тестирование виртуального защищенного соединения.
5. Восстановление начального состояния компьютеров.

Для выполнения лабораторной работы необходимо наличие трех компьютеров, физически объединенных в единую сеть. На компьютере, выполняющего роль VPN-сервера должно быть две сетевые карты и установленная Windows Server 2008 R2, на двух других – Windows XP/7. На рис. 5 показана структура рабочей схемы сети.

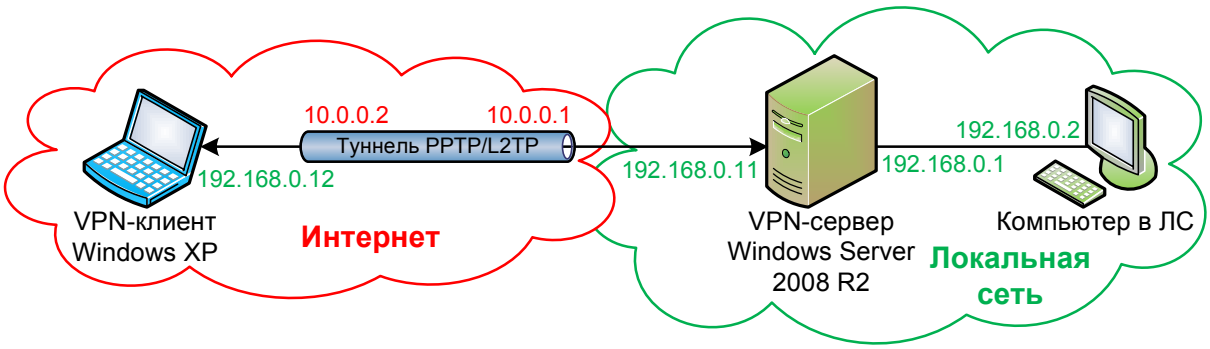

Рис. 5. Структура рабочей схемы сети

Этап 1 – Настройка VPN-сервера с ОС Windows Server 2008 R2:

а) Настройка сетевого интерфейса с сетью 10.0.0.0:

1) Пуск ⇨ Панель управления ⇨ Сеть и Интернет ⇨ Центр управления сетями и общим доступом ⇨ Изменение параметров адаптера (или Win+R ⇨ ncpa.cpl ⇨ Enter);

2) правой кнопкой мыши на «Подключение по локальной сети» ⇨ Свойства ⇨ Протокол Интернета версии 4 ⇨ Свойства;

3) установить следующие параметры:

- выбрать опцию «Использовать следующий IP-адрес»,
- IP-адрес: 10.0.0.1,
- Маска подсети: 255.0.0.0,
- Предпочитаемый DNS-сервер: 127.0.0.1;

4) ОК ⇨ Закрыть;

5) включить «Подключение по локальной сети» двойным кликом.

б) Настройка сетевого интерфейса с сетью 192.168.0.0:

1) Пуск ⇨ Панель управления ⇨ Сеть и Интернет ⇨ Центр управления сетями и общим доступом ⇨ Изменение параметров адаптера;

2) правой кнопкой мыши на «Подключение по локальной сети 2» ⇨ Свойства ⇨ Протокол Интернета версии 4 ⇨ Свойства;

3) установить следующие параметры:

- выбрать опцию Использовать следующий IP-адрес,
- IP-адрес: 192.168.0.1,
- Маска подсети: 255.255.255.0,
- Предпочитаемый DNS-сервер: 127.0.0.1;

4) ОК ⇨ Закрыть;

5) включить «Подключение по локальной сети 2» двойным кликом.

в) Установка роли «Службы политики сети и доступа»:

1) Пуск ⇨ Администрирование ⇨ Диспетчер сервера;

2) в дереве консоли кликнуть правой кнопкой мыши на Роли ⇨ Добавить роли;

3) установить флажки напротив «Службы политики сети и доступа» ⇨ Далее ⇨ Далее;

4) установить флажок «Службы маршрутизации и удаленного доступа» ⇨ Далее ⇨ Установить ⇨ Закрыть.

г) Настройка службы «Маршрутизация и удаленный доступ»:

1) Пуск ⇨ Администрирование ⇨ Маршрутизация и удаленный доступ;

2) кликнуть правой кнопкой мыши на имени сервера WINSRV-2008-R2 (если его нет, то добавить через контекстное меню) ⇨ Настроить и включить маршрутизацию и удаленный доступ;

3) в открывшемся Мастере нажать Далее ⇨ выбрать опцию «Особая конфигурация» ⇨ Далее;

4) установить флажок «Доступ к виртуальной частной сети (VPN)» ⇨ Далее ⇨ Готово;

5) запустить службу – значок рядом с именем сервера должен принять вид зеленой стрелки направленной вверх (рис. 6).

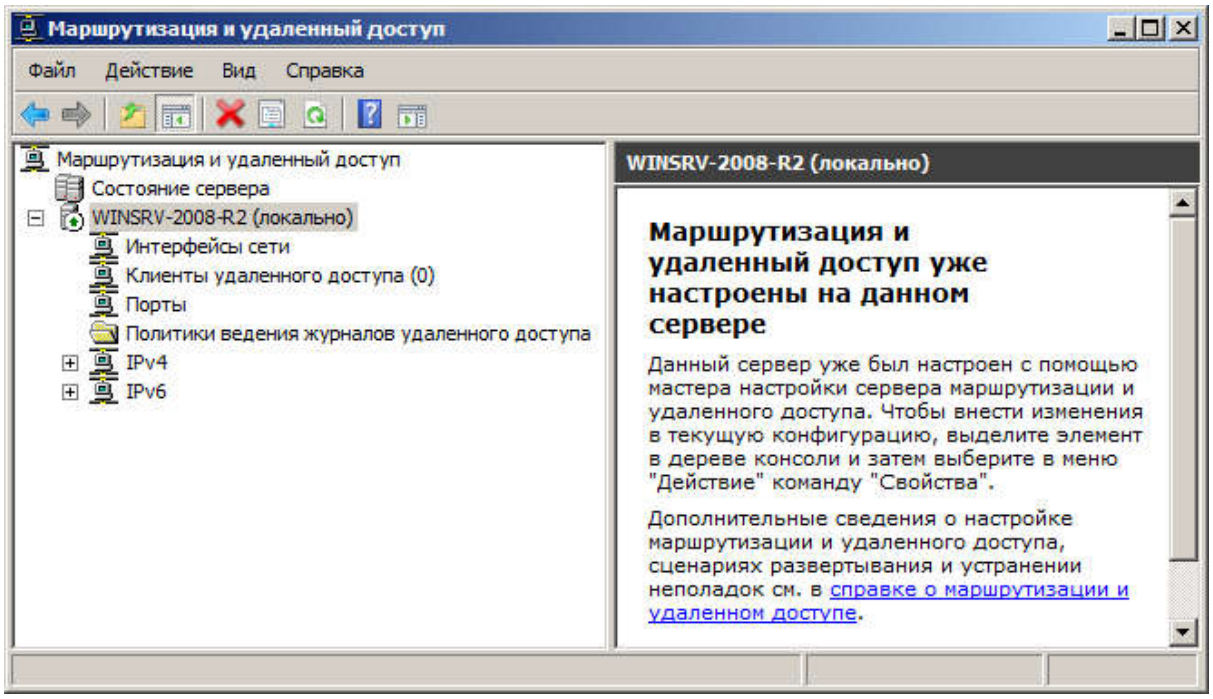

Рис. 6. Служба маршрутизации и удаленного доступа

д) Настройки безопасности и назначение IP-адресов для удаленных VPN-клиентов:

1) кликнуть правой кнопкой мыши на «Маршрутизация и удаленный доступ» ⇨ Свойства;

2) перейти во вкладку Безопасность ⇨ Методы проверки подлинности;

3) установить флажок напротив «Шифрованная проверка (Microsoft, версия 2, MS-CHAP v2)» (рис. 7) ⇨ OK;

4) установить флаг «Разрешать пользовательские IPSec-политики»;

5) ввести предварительный ключ: Pre-Shared Key;

6) перейти во вкладку IPv4;
7) выбрать опцию статический пул адресов ⇨ Добавить;

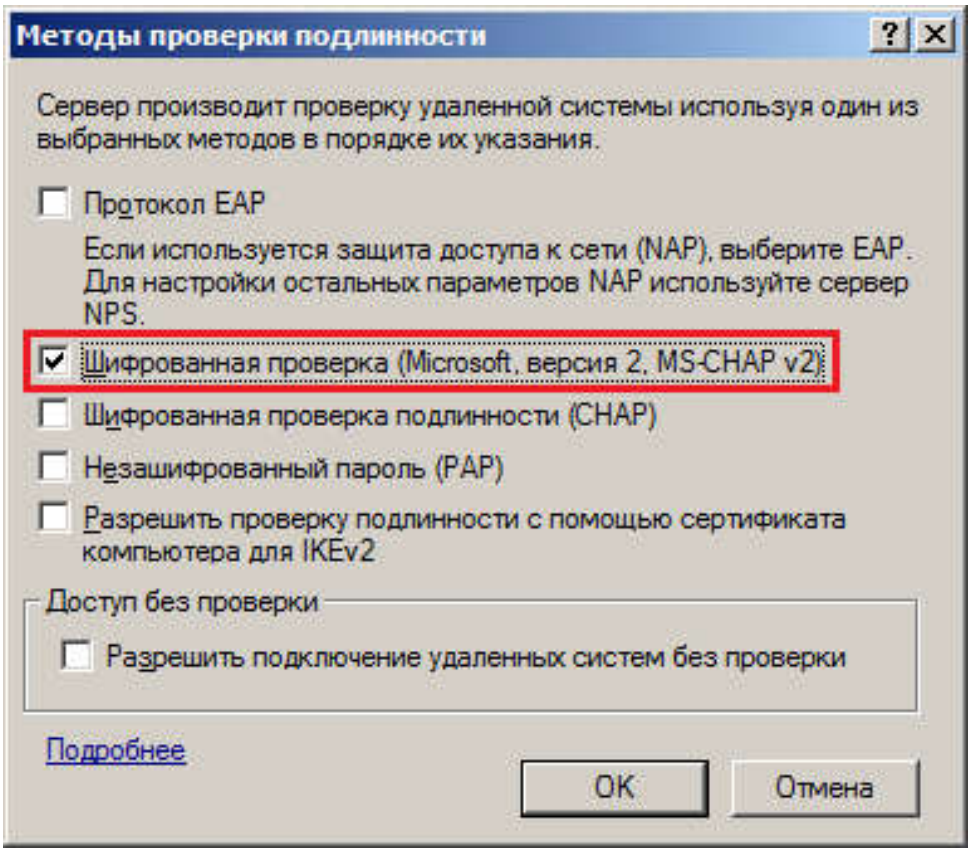

Рис. 7. Методы проверки подлинности

8) ввести значения:
- Начальный IP-адрес: 192.168.0.11,
- Конечный IP-адрес: 192.168.0.12,

⇨ ОК;

9) выбрать адаптер «Подключение по локальной сети», через который подключаются VPN-клиенты (если включен только один адаптер, то данный список не отображается);

10) перейти во вкладку PPP ⇨ снять флажок «Многоканальные подключения»;

11) перейти во вкладку «Ведение журнала» ⇨ выбрать опцию «вести журнал всех событий»;

12) закрыть окно свойств нажав ОК.

е) Создание и настройка виртуальных портов для приема VPN-подключений:

1) в ветви «Маршрутизация и удаленный доступ» кликнуть правой кнопкой мыши на Порты ⇨ Свойства;

2) в новом окне выделить WAN Miniport (L2TP) ⇨ Настроить;

3) оставить только флажок «Подключения удаленного доступа (только входящие)» (рис. 8);

4) задать «Максимальное число портов» равное 1 ⇨ OK ⇨ Да;

5) вернувшись в окно Свойства, аналогично настроить порты PPTP;

6) отключить порты «WAN Miniport (IKEv2)» и «WAN Miniport (SSTP)» сняв флажки всех подключений в их настройках;

7) закрыть окно Свойства нажав OK.

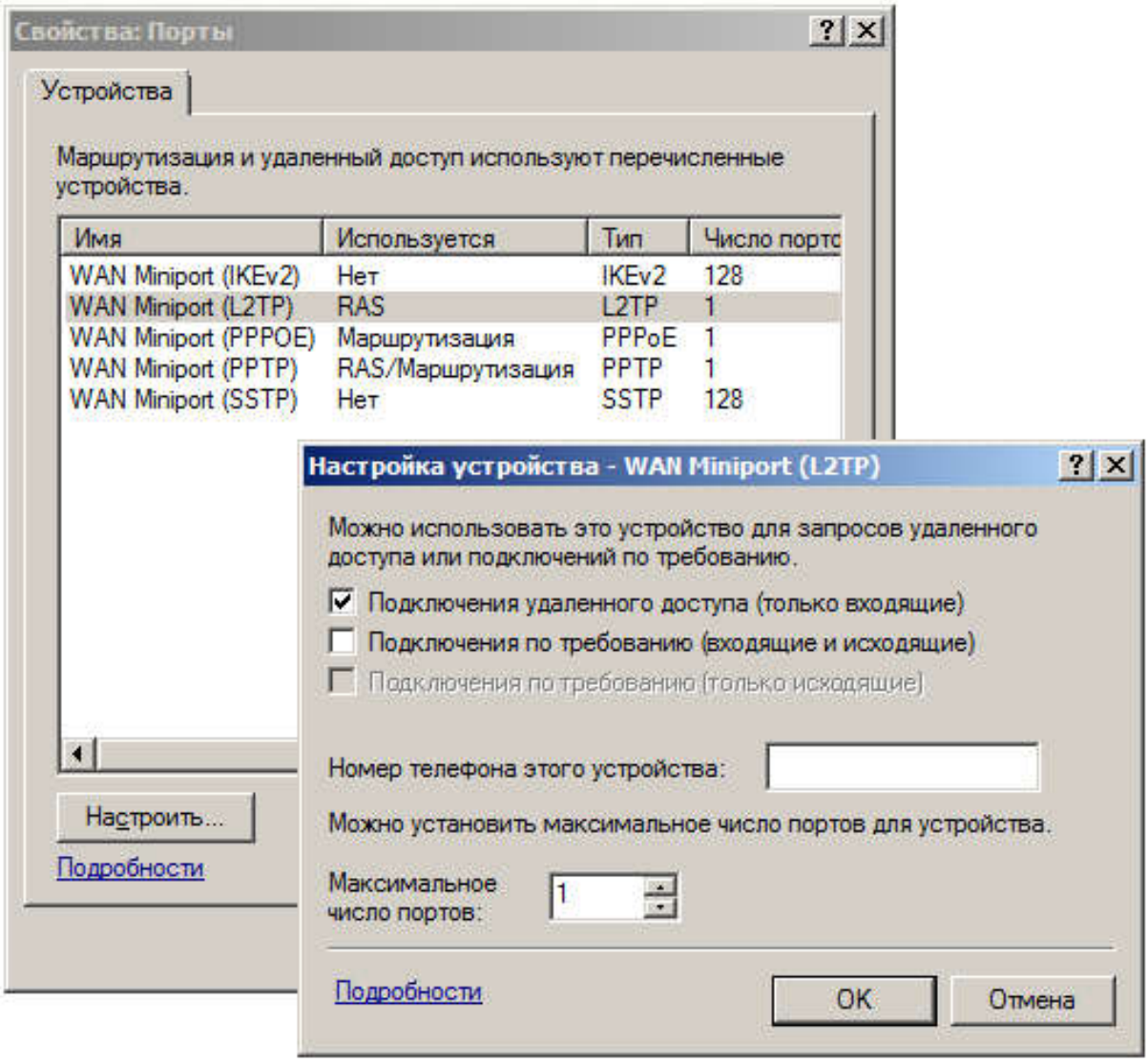

Рис. 8. Настройка VPN-портов

ж) Установка роли Active Directory и настройка сервера контроллером домена:

1) Пуск ⇨ Администрирование ⇨ Диспетчер сервера;

2) в Дереве консоли кликнуть правой кнопкой мыши на Роли ⇨ Добавить роли;

3) установить флажок «Доменные службы Active Directory»;

4) Далее ⇨ Далее ⇨ Установить ⇨ Закрыть.

5) нажать на клавиатуре сочетание Win+R ⇨ напечатать dcpromo.exe ⇨ Выполнить;

6) в «Мастере установки доменных служб Active Directory» нажать Далее;

7) Далее ⇨ Создать новый домен в новом лесу ⇨ Далее;

8) ввести доменное имя: testlab.net ⇨ Далее;

9) выбрать режим работы леса: Windows Server 2008 R2 ⇨ Далее;

10) оставить флажок «DNS-сервер» ⇨ Далее ⇨ Да ⇨ Далее;

11) ввести пароль: pa$$w0rd ⇨ Далее ⇨ Далее;

12) установить флажок «Перезагрузка по завершении», дождаться завершения настроек и перезагрузки компьютера.

Результат проведенных настроек представлен на рис. 9.

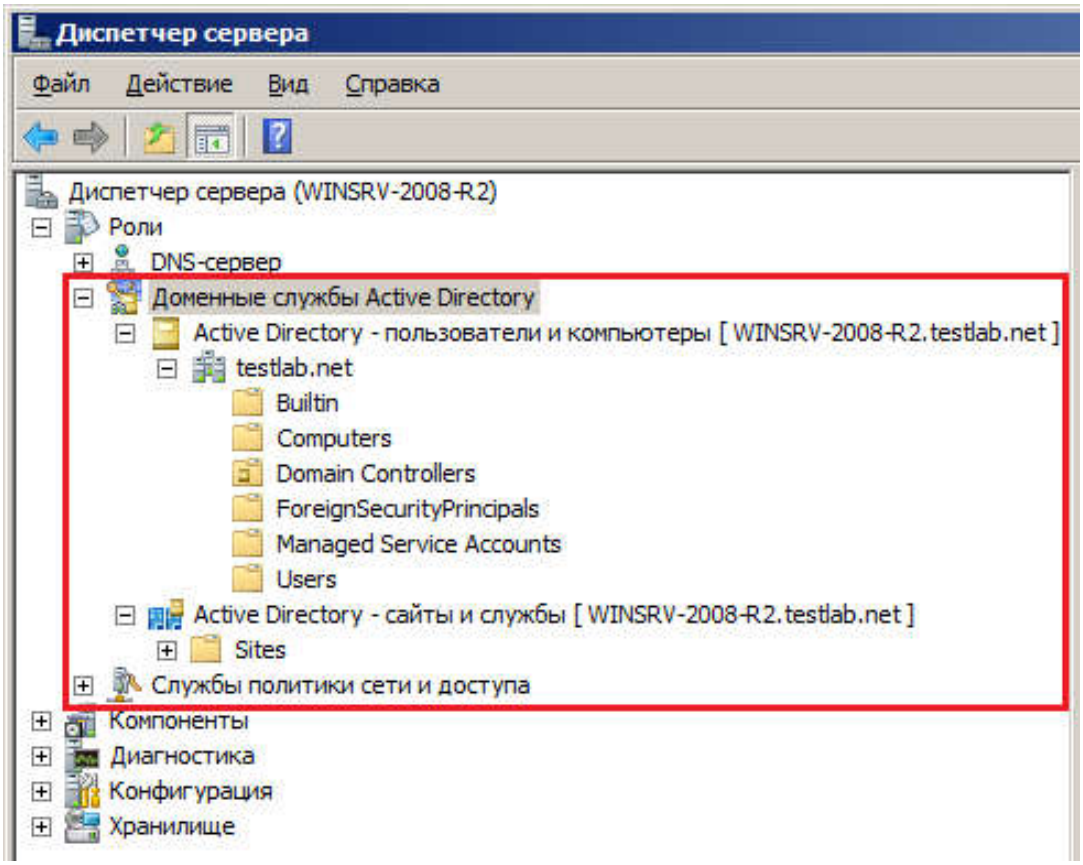

Рис. 9. Доменные службы Active Directory

и) Создание пользователей с правами на удаленное подключение к локальной сети 192.168.0.0:

1) Пуск ⇨ Администрирование ⇨ Active Directory – Пользователи и компьютеры;

2) раскрыть ветвь testlab.net ⇨ кликнуть правой кнопкой мыши на Users ⇨ Создать ⇨ Пользователь;

3) в окне «Новый объект – Пользователь» ввести:

- Имя: vpn-user,
- Имя входа пользователя: vpn-user ⇨Далее
- установить флажок «Срок действия пароля не ограничен» и ввести:
- Пароль: pa$$w0rd,
- Подтверждение: pa$$w0rd,
- Далее ⇨ Готово;

4) в основном окне «Active Directory – Пользователи и компьютеры» найти созданного vpn-user и кликнуть по нему правой кнопкой мыши ⇨ Свойства;

5) перейти во вкладку «Входящие звонки»;

6) установить опцию «Разрешить доступ» ⇨ OK;

7) закрыть окно «Active Directory – Пользователи и компьютеры».

Этап 2 – Настройка VPN-клиента с ОС Windows XP

а) Настройка сетевого интерфейса:

1) Пуск ⇨ Настройка ⇨ Панель управления ⇨ Сетевые подключения;

2) кликнуть правой кнопкой мыши на «Подключение по локальной сети» ⇨ Свойства;

3) выбрать «Протокол Интернета TCP/IP» ⇨ Свойства;

4) ввести следующие параметры:

IP-адрес: 10.0.0.2,

Маска подсети: 255.0.0.0,

OK ⇨ Закрыть;

включить «Подключение по локальной сети» двойным кликом.

б) Проверка соединения:

1) на клиентской машине нажать Win+R ⇨ cmd.exe ⇨ Enter;

2) ввести команду: ping 10.0.0.1 ⇨ Enter;

3) убедиться в успешности обмена пакетами с VPN-сервером при простом локальном соединении.

в) Создание PPTP-подключения:

1) открыть «Сетевые подключения»;

2) Файл ⇨ Новое подключение ⇨ Далее;
3) выбрать «Подключить к сети на рабочем месте» ⇨ Далее;
4) выбрать «Подключение к виртуальной частной сети» ⇨ Далее;
5) ввести имя подключения: PPTP ⇨ Далее;
6) ввести IP-адрес VPN-сервера: 10.0.0.1 ⇨ Далее ⇨ Готово;
7) в окне «Подключение: PPTP» ввести:
Пользователь: vpn-user,
Пароль: pa$$w0rd,
установить флажок «Сохранять имя пользователя и пароль»;
8) зайти в Свойства ⇨ открыть вкладку Безопасность;
9) выбрать опцию «Дополнительные (выборочные параметры)» ⇨ Параметры;
10) задать шифрование данных – обязательное;
11) установить флажок «Протокол проверки пароля Microsoft (MS CHAP v2)» ⇨ ОК;
12) перейти во вкладку Сеть ⇨ Тип VPN: PPTP VPN (рис. 10);

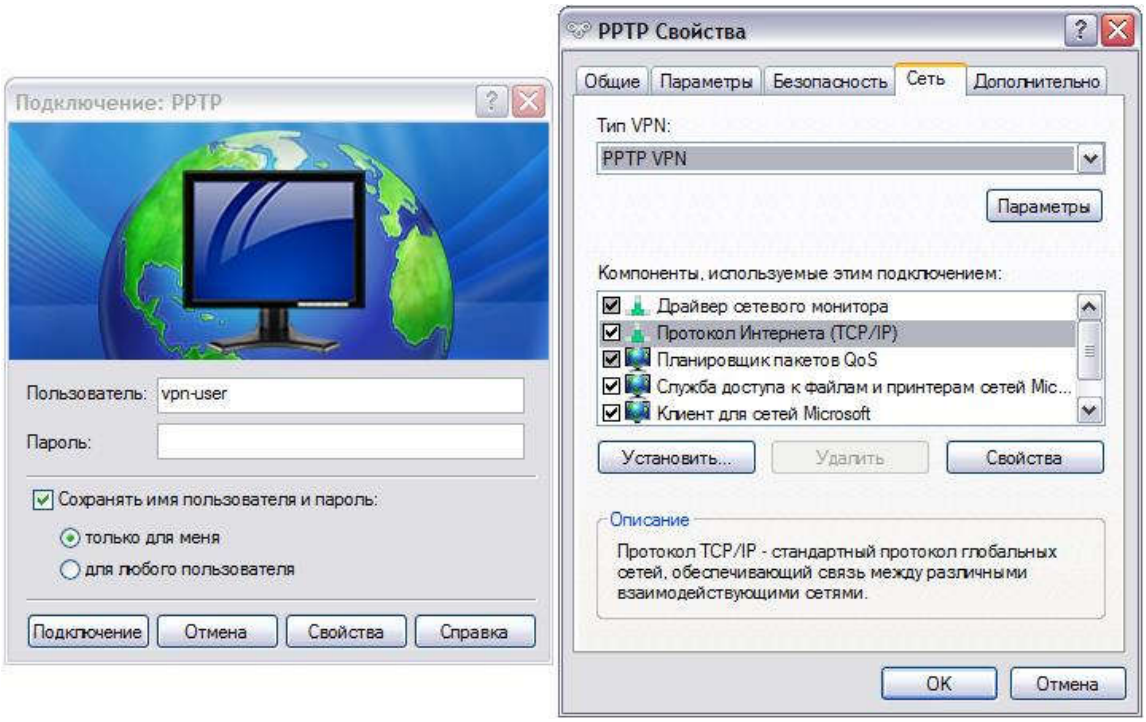

Рис. 10. PPTP-подключение на компьютере клиента

13) «Протокол Интернета TCP/IP» ⇨ Свойства ⇨ оставить включенной опцию «Получить IP-адрес автоматически»;
14) кнопка Дополнительно ⇨ снять флажок «Использоватьосновной шлюз в удаленной сети» (это нужно для того, чтобы на клиенте работало Интернет-соединение);

15) закрыть все окна: ОК ⇨ ОК ⇨ ОК.

г) Создание L2TP-подключения:

1) открыть «Сетевые подключения»;
2) Файл ⇨ Новое подключение ⇨ Далее;
3) выбрать «Подключить к сети на рабочем месте» ⇨ Далее;
4) выбрать «Подключение к виртуальной частной сети» ⇨ Далее;
5) ввести имя подключения: L2TP ⇨ Далее;
6) выбрать «Не набирать номер для предварительного подключения» ⇨ Далее;
7) ввести IP-адрес VPN-сервера: 10.0.0.1 ⇨ Далее ⇨ Готово;
8) в окне Подключение: L2TP ввести:

Пользователь: vpn-user,

Пароль: pa$$w0rd,

установить флажок «Сохранять имя пользователя и пароль»;

9) зайти в Свойства ⇨ открыть вкладку Безопасность;
10) выбрать опцию «Дополнительные (выборочные параметры)» ⇨ Параметры;
11) задать шифрование данных – обязательное;
12) установить флажок «Протокол проверки пароля Microsoft (MS CHAP v2)» ⇨ ОК;
13) нажать на кнопку «Параметры IPSec»;
14) установить флажок «Для проверки подлинности использовать предварительный ключ» ⇨ ввести: Pre-Shared Key ⇨ ОК (рис. 11);

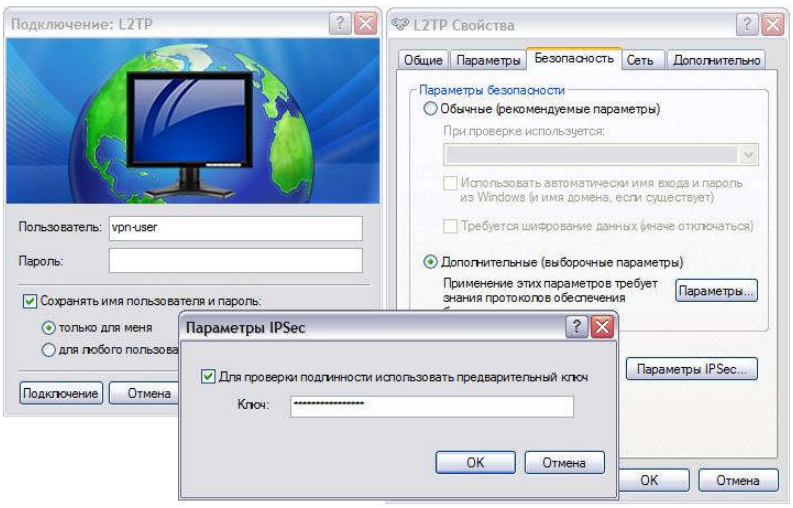

Рис. 11. L2TP-подключение на компьютере клиента

15) перейти во вкладку Сеть ⇨ Тип VPN: L2TP IPSec VPN;

16) Протокол Интернета TCP/IP ⇨ Свойства ⇨ оставить включенной опцию «Получить IP-адрес автоматически»;

17) кнопка Дополнительно ⇨ снять флажок «Использовать основной шлюз в удаленной сети» (это нужно для того, чтобы на клиенте работало Интернет-соединение);

18) закрыть все окна: ОК ⇨ ОК ⇨ ОК.

Этап 3 – Настройка компьютера в локальной сети 192.168.0.0:

а) Настройка сетевого интерфейса:

1) Пуск ⇨ Настройка ⇨ Панель управления ⇨ Сетевые подключения;

2) кликнуть правой кнопкой мыши на «Подключение по локальной сети» ⇨ Свойства;

3) выбрать «Протокол Интернета TCP/IP» ⇨ Свойства;

4) ввести следующие параметры:

IP-адрес: 192.168.0.2,

Маска подсети: 255.255.255.0,

ОК ⇨ Закрыть;

5) включить «Подключение по локальной сети» двойным кликом.

б) Проверка соединения:

1) на компьютере в ЛС нажать Win+R ⇨ cmd.exe ⇨ Enter;

2) ввести команду: ping 192.168.0.1 ⇨ Enter;

3) убедиться в успешности обмена пакетами с сервером.

Этап 4. Тестирование виртуального защищенного соединения

Эксперимент 1 – Установка PPTP-соединения:

На машине VPN-клиента:

1) зайти в сетевые подключения (Win+R ⇨ ввести: ncpa.cpl ⇨ Enter);

2) двойной клик по значку PPTP ⇨ Подключение ⇨ дождаться установления соединения;

3) кликнуть правой кнопкой мыши по значку PPTP ⇨ Состояние;

4) изучить информацию во вкладках Общие и Сведения (обратить внимание на IP-адреса сервера и клиента) ⇨ Закрыть.

На машине VPN-сервера:

1) открыть Маршрутизация и удаленный доступ;

2) открыть ветвь Клиенты удаленного доступа;

3) в основном окне отобразится информация о клиенте удаленного доступа vpn-user ⇨ произвести двойной клик по этой записи;

4) изучить информацию о состоянии текущего подключения;

5) перейти в ветвь Порты ⇨ найти в списке открытый PPTP-порт и дважды кликнуть по нему;

6) изучить сведения о состоянии порта;

7) нажать кнопку Отключить ⇨ Закрыть.

Зафиксировать и проанализировать полученные сведения.

Эксперимент 2 – Установка L2TP-соединения:

Повторить действия *Эксперимента 1* с L2TP подключением на машинах VPN-клиента и VPN-сервера. Зафиксировать и проанализировать полученные результаты.

Эксперимент 3 – Просмотр журнала безопасности:

События, происходящие в системе, фиксируются в журнале безопасности Windows Server. Открыть журнал:

1) Пуск ⇨ Администрирование ⇨ Просмотр событий;

2) развернуть ветвь Журналы Windows ⇨ Безопасность;

3) просмотреть общие сведения последних по времени событий.

Эксперимент 4 – Анализ трафика PPTP-соединения:

Примечание. Для данного эксперимента на компьютере пользователя должна быть установлена утилита Microsoft Network Monitor 3.4, которую можно бесплатно скачать с официального сайта: http://www.microsoft.com/en-us/download/details.aspx?id=4865 (для 32- и 64-разрядных систем).

1) запустить программу MS Network Monitor 3.4 на машине VPN-клиента;

2) создать новый захват: File ⇨ New ⇨ Capture или Ctrl + N;

3) нажать на кнопку Capture Settings (F4) на панели инструментов;

4) в открывшемся окне параметров захвата установить флажок напротив имени «Подключение по локальной сети» для текущего сетевого адаптера (IPv4 = 10.0.0.2), остальные снять ⇨ Close;

5) запустить сканирование кнопкой Start (F5) на панели инструментов;

6) установить PPTP-соединение в сетевых подключениях (ncpa.cpl);

7) по завершении подключения нажать на Pause (F6); изучить какие протоколы использовались при установлении PPTP-соединения в окне Frame Summary;

8) в окне Display Filter ввести PPTP и нажать Apply, в окне Frame Summary останется 7 PPTP-кадров; последовательно изучить PPTP-заголовки каждого кадра в окне Frame Details, обратить особое внимание на значение поля ControlMessageType;

9) в окне Display Filter ввести и применить новый фильтр – LCP; изучить заголовки протокола управления соединением (LCP), обратить внимание на порядок инкапсуляции данных;

10) создать новый фильтр для CHAP; изучить процесс проверки подлинности при «рукопожатии» между сервером и клиентом;

11) отключить фильтр кнопкой Remove;

12) перезапустить сканирование кнопками Stop (F7) и Start (F5);

13) с помощью утилиты cmd.exe запустить команду ping 192.168.0.11;

14) остановить сканирование Pause (F6); изучить трафик в окнах Frame Summary и Frame Details;

15) возобновить сканирование ⇨ разорвать соединение PPTP в Сетевых подключениях ⇨ остановить сканирование ⇨ создать PPTP-фильтр; последовательно изучить PPTP-заголовки каждого кадра в окне Frame Details, обратить особое внимание на значение поля ControlMessageType;

16) сбросить фильтр, программу Network Monitor оставить открытой.

Эксперимент 5 – Анализ трафика L2TP-соединения:

1) Запустить сканирование кнопкой Start (F5) на панели инструментов;

2) установить L2TP-соединение в сетевых подключениях (ncpa.cpl);

3) по завершении подключения нажать на Pause (F6); изучить какие протоколы использовались при установлении L2TP-соединения в окне Frame Summary. Изучить заголовки протоколов IKE и ESP в окне Frame Details;

4) перезапустить сканирование кнопками Stop (F7) и Start (F5);

5) с помощью утилиты cmd.exe запустить команду ping 192.168.0.11;

6) остановить сканирование Pause (F6); изучить исходящий и входящий трафик в окнах Frame Summary и Frame Details;

7) возобновить сканирование ⇨ разорвать соединение L2TP в Сетевых подключениях ⇨ остановить сканирование; просмотреть заголовки протоколов, участвующих при разрыве соединения (IKE и ESP);

8) закрыть программу Network Monitor.

Эксперимент 6 – Удаленный доступ к компьютеру локальной сети:

На компьютере в ЛС 192.168.0.0:

1) в рабочей директории создать папку test, в ней создать файл data.txt, заполнить его текстом (например всеми «1»);

2) нажать правой кнопкой мыши на папке test ⇨ Общий доступ и безопасность;

3) установить флажок Открыть общий доступ к папке ⇨ ОК.

На VPN-клиенте:

1) установить PPTP-соединение с сервером;

2) проверить доступность удаленного хоста в ЛС с VPN-клиента, для этого запустить cmd.exe ⇨ ввести и запустить команду: ping 192.168.0.2, убедиться в успешности обмена пакетами с хостом локальной сети;

3) открыть проводник: правой кнопкой на Пуск ⇨ Проводник;

4) в адресной строке ввести: \\192.168.0.2 ⇨ Enter;

5) в основном окне открыть папку test ⇨ скопировать data.txt;

6) запустить сканирование (F5) в Network Monitor;

7) вставить скопированный ранее файл в рабочую директорию на компьютере VPN-клиента;

8) остановить сканирование (F7) и просмотреть результаты. Изучить поле данных в окне Hex Details, убедиться, что они зашифрованы;

9) повторить передачу данный и сканирование трафика при L2TP-соединении, зафиксировать результат.

Этап 5. Восстановление начального состояния компьютеров

1. На компьютере ЛС 192.168.0.0:

- снять общий доступ к папке test и удалить ее;
- восстановить первоначальные настройки сетевого интерфейса.

2. На компьютере VPN-клиента:

- удалить виртуальные частные подключения PPTP и L2TP;
- восстановить первоначальные настройки сетевого интерфейса.

3. На компьютере VPN-сервера:

- восстановить первоначальные настройки сетевых интерфейсов на обеих сетевых адаптерах;
- отключить службу маршрутизации и удаленного доступа;
- удалить роли: Службы политики сети и доступа, Доменные службы Active Directory и DNS-сервер.

4. Закрыть все открытые окна.

5. Выйти из систем, завершив сеанс работы от имени администратора.

Требования к содержанию отчета

Отчет должен включать:
- номер, тема и цель работы;
- краткие теоретические сведения по работе;
- ход выполнения работы со скриншотами основных окон настроек;
- распечатки результатов экспериментов с комментариями к ним;
- выводы по работе.

Контрольные вопросы

1. Какой процесс доставки конфиденциальных данных по VPN-туннелю?
2. Архитектура протокола PPTP.
3. Архитектура протокола L2TP.
4. Опишите сходства и различия протоколов PPTP и L2TP. Достоинства и недостатки каждого из них.
5. Перечислите основные шаги настройки VPN-сервера.