



**Лабораторные работы для курса
«Основы сетевых технологий.
Учебный курс D-Link»**

Москва, 2013

Версия 1.1

Оглавление

Рекомендации по организации лабораторных работ.....	3
Лабораторная работа №1. Основные понятия сетевых технологий.....	4
Лабораторная работа №2. Разработка топологии сети небольшого предприятия.....	8
Лабораторная работа №3. Изучение элементов кабельной системы.....	11
3.1. Изучение волоконно-оптического кабеля.....	14
3.2. Обжим UTP-кабеля разъемами RJ-45.....	16
3.3. Расчет кабельной сети.....	19
Лабораторная работа №4. Построение одноранговой сети.....	20
4.1. Создание подключения типа «компьютер-компьютер».....	22
4.2. Создание одноранговой сети с использованием коммутатора.....	28
Лабораторная работа №5. Адресация канального уровня. MAC-адреса.....	38
Лабораторная работа №6. Создание коммутируемой сети.....	49
6.1 Управление коммутатором через Web-интерфейс и изучение таблицы коммутации.....	50
6.2 Логическая сегментация сети с помощью технологии VLAN на основе портов (Port-Based VLAN).....	55
Лабораторная работа №7. Создание беспроводной сети.....	60
7.1 Создание беспроводной сети в режиме Ad-Hoc.....	61
7.1.1 Создание беспроводной сети в режиме Ad-Hoc при помощи службы «Беспроводная настройка» ОС Windows XP.....	64
7.1.2 Создание беспроводной сети в режиме Ad-Hoc для рабочих станций с ОС Windows Vista/7.....	71
7.1.3 Создание беспроводной сети в режиме Ad-Hoc при помощи утилиты D-Link Connection Manager.....	78
7.2 Создание беспроводной сети в режиме инфраструктуры.....	81
Лабораторная работа №8. IP-адресация.....	87
8.1 Определение адреса сети, широковещательного адреса и количества узлов по заданному IP-адресу и маске подсети.....	89
8.2 Формирование подсетей с использованием масок переменной длины (VLSM).....	93
8.3 Формирование подсетей IPv6.....	95
Лабораторная работа №9. Установка и настройка протокола IPv6 на рабочей станции и точке доступа D-Link.....	97
9.1 Установка и настройка протокола IPv6 на рабочей станции.....	98
9.2 Подключение к точке доступа через Web-интерфейс с помощью IPv6-адреса.....	102
Лабораторная работа №10. Изучение принципа работы протокола ARP.....	107
Лабораторная работа №11. Организация межсетевого взаимодействия с помощью маршрутизатора DIR-615.....	111
11.1 Организация межсетевого взаимодействия.....	112
11.2 Обеспечение доступа из внешней сети к FTP-серверу, который находится во внутренней сети.....	119
Лабораторная работа №12. Динамическое распределение IP-адресов по протоколу DHCP.....	123
Лабораторная работа №13. Итоговая работа.....	126

Рекомендации по организации лабораторных работ

Для выполнения настоящих лабораторных работ рекомендуется следующий комплект оборудования, из расчёта на учебную группу, состоящую из 10 человек:

Коммутатор DES-1100-16	5 шт.
Точка доступа DAP-2310	5 шт.
Маршрутизатор DIR-615	5 шт.
Беспроводной адаптер DWA-160	10 шт.
Рабочая станция	15 шт.
Кабель Ethernet (“прямой”)	20 шт.
Кабель Ethernet (“перекрестный”)	10 шт.

Дополнительное оборудование:

Обжимной инструмент (кримпер)	5 шт.
Сетевой тестер	5 шт.
Волоконно-оптический кабель	1 шт.
Разъем SC-FC (или SC-ST)	1 шт.
Разъем RJ-45	20 шт.

Каждая лабораторная работа содержит схему установки с указанием количества рабочих мест, на которое она рассчитана. 1 рабочее место = 2 человека.

Команды в лабораторных работах приведены для устройств со следующими версиями программного обеспечения:

- Коммутатор DES-1100-16 – ПО версии 1.00.09 или выше;
- Точка доступа DAP-2310 – ПО версии 1.15 или выше;
- Маршрутизатор DIR-615 – ПО версии 1.0.22 или выше.

Для проведения лабораторных работ потребуется ПО:

- FTP-сервер *Golden FTP Server v5.00* (<http://www.goldenftpserver.com/download.html>);
- Анализатор трафика *Wireshark* (<http://www.wireshark.org>).

Лабораторная работа №1. Основные понятия сетевых технологий

Цель: закрепить материал по базовым понятиям сетевых технологий, изученным в Главе 1 и Главе 2.

ЗАДАНИЕ

Ответьте на вопросы, приведенные ниже. Выберите один правильный ответ или дайте развернутый ответ там, где это необходимо.

1. Дайте определение компьютерной сети.

2. К какому классу относится сеть, объединяющая компьютеры разных городов, регионов, государств?

- локальная сеть;
- глобальная сеть;
- городская сеть.

3. Что такое беспроводная сеть?

- сеть, в которой передача информации осуществляется при помощи электромагнитных волн в определенном частотном диапазоне;
- сеть, в которой для передачи данных используется телефонный провод, коаксиальный кабель или витая пара.

4. Какой тип взаимодействия между компьютерами показан на рисунке 1.1.

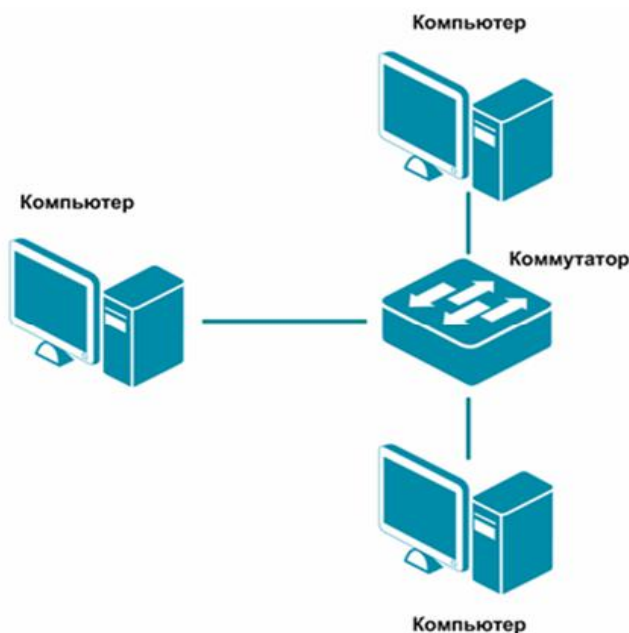


Рисунок 1.1 Взаимодействие между компьютерами

- сеть типа «клиент-сервер»;
- одноранговая сеть;
- беспроводная сеть.

5. Как называется установленное в компьютер устройство, которое позволяет ему подключаться к сети и взаимодействовать с другими устройствами?

- сетевой адаптер;
- маршрутизатор;
- коммутатор.

6. Что такое проводная сеть?

- сеть, в которой передача информации осуществляется при помощи электромагнитных волн в определенном частотном диапазоне;
- сеть, в которой для передачи данных используется телефонный провод, коаксиальный кабель или витая пара.

7. Как называлась первая глобальная сеть, созданная в 1969 году Министерством обороны США?

- Internet;
- Arpanet;
- Intranet.

8. Перечислите все уровни модели OSI?

9. Каким из перечисленных ниже терминов называют блок данных канального уровня?

- сегмент;
- пакет;
- кадр.

10. Какой из перечисленных ниже терминов не является названием уровня в модели OSI?

- уровень приложений;
- уровень Интернет;
- сеансовый уровень.

11. Перечислите основные достоинства и недостатки сетей типа «клиент-сервер».

12. Какой из уровней модели OSI отвечает за выбор наилучшего маршрута до сети назначения.

- уровень приложений;
- канальный уровень;
- сетевой уровень.

13. Соотнесите перечисленные термины с уровнями модели OSI, к которым они относятся.

- | | |
|-----------------|----------------------------|
| а) кадр; | Транспортный уровень _____ |
| б) IP-адрес; | |
| в) MAC-адрес; | Сетевой уровень _____ |
| г) пакет; | |
| д) номер порта; | Канальный уровень _____ |
| е) сегмент; | |
| ж) биты. | |

14. Перечислите все уровни модели TCP/IP.

15. Как называется процесс, при котором к данным добавляется заголовок определенного уровня перед отправкой в сеть?

- декапсуляция;
- мультиплексирование;
- инкапсуляция.

16. Какие из перечисленных ниже протоколов относятся к транспортному уровню модели OSI? (Выберите 2 ответа).

- IP;
- Ethernet;
- TCP;
- UDP.

17. Какой из уровней модели OSI отвечает за логическую адресацию и маршрутизацию?

- уровень приложений;
- канальный уровень;
- сетевой уровень.

18. Соотнесите перечисленные протоколы с уровнями модели OSI, к которым они относятся.

- | | |
|--------------|----------------------------|
| а) TCP; | Транспортный уровень _____ |
| б) IP; | |
| в) Ethernet; | Сетевой уровень _____ |
| г) HTTP; | |
| д) UDP; | Уровень приложений _____ |
| е) FTP; | |
| ж) Telnet. | Физический уровень _____ |

19. Каким из перечисленных ниже терминов называют блок данных сетевого уровня?

- сегмент;
- пакет;
- кадр.

20. Какой из перечисленных ниже терминов не является названием уровня в модели TCP/IP?

- уровень приложений;
- уровень Интернет;
- сеансовый уровень.

21. Каким из перечисленных ниже терминов называют блок данных транспортного уровня?

- сегмент;
- пакет;
- кадр.

22. Какой из уровней модели OSI задает стандарты для кабельной системы?

- уровень приложений;
- сеансовый уровень;
- физический уровень.

23. Какой из уровней модели OSI описывает стандарты форматов данных и шифрование трафика?

- уровень представлений;
- сеансовый уровень;
- физический уровень;
- канальный уровень.

24. Когда протокол TCP передающего узла маркирует сегмент порядковым номером равным 1, а принимающий узел отправляет в ответ подтверждение приема с порядковым номером 1, такой процесс будет примером:

- инкапсуляции данных;
- взаимодействие двух систем на одинаковом уровне;
- взаимодействие двух смежных уровней;
- ни один из указанных ответов не верен.

25. Какие из перечисленных ниже протоколов относятся к уровню приложений модели OSI? (Выберите 2 ответа).

- IP;
- Ethernet;
- TCP;
- HTTP;
- DNS.

Лабораторная работа №2. Разработка топологии сети небольшого предприятия

При создании сети передачи данных, когда соединяются все компьютеры сети и другие сетевые устройства, формируется **сетевая топология компьютерной сети**.

Сетевая топология — это способ описания конфигурации сети, схема расположения и соединения сетевых устройств. Существуют три базовые топологии, на основе которых строится большинство сетей:

- «Шина» (*Bus*) — все узлы соединяются между собой одним кабелем;
- «Кольцо» (*Ring*) — каждый компьютер соединяется с двумя другими так, чтобы от одного он получал информацию, а другому передавал ее. Последний компьютер подключается к первому;
- «Звезда» (*Star*) — каждый из узлов подключается к центральному соединительному устройству (коммутатору, концентратору).

Комбинированные топологии:

- «Дерево» (*Tree*) — объединение нескольких «звезд»;
- *Полносвязная топология* — каждый компьютер и другие устройства соединены друг с другом напрямую;
- *Топология неполной связности* — получается из полносвязной путем удаления некоторых возможных связей. Каждый узел сети соединяется с несколькими другими узлами сети.

При построении любой компьютерной сети используется **коммуникационное** или **сетевое оборудование**. Основной его задачей является объединение компьютеров в сеть, подключение компьютерных сетей разных топологий и технологий друг к другу, увеличение расстояния передачи сигнала. Устройства, применяемые для построения компьютерной сети следующие:

Медиаконвертер (Mediaconverter) — это устройство физического уровня модели OSI, преобразующее среду распространения сигнала из одного типа в другой;

Повторитель (Repeater) — это устройство физического уровня модели OSI, используемое для соединения сегментов среды передачи данных с целью увеличения общей длины сети;

Концентратор (Concentrator) или *Хаб (Hub)* — это повторитель, который имеет несколько портов и соединяет несколько физических сегментов сети;

Мост (Bridge) — это устройство канального уровня модели OSI, которое соединяет между собой два сегмента локальной сети;

Коммутатор (Switch) — это устройство канального уровня модели OSI, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети;

Маршрутизатор (Router) — это устройство сетевого уровня модели OSI, пересылающее пакеты данных между различными сегментами сети (подсетями);

Шлюз (Gateway) — любое устройство, соединяющее разные сетевые архитектуры.

Цель: разработать топологию сети небольшого предприятия.

ЗАДАНИЕ 1

На рисунке 2.1 показан план 1-го этажа центрального офиса. В каждом кабинете по 6 рабочих станций. Требуется объединить в локальную сеть все сетевые устройства, находящиеся на 1-ом этаже, так, чтобы они могли обмениваться информацией друг с другом с меньшей вероятностью возникновения коллизий.

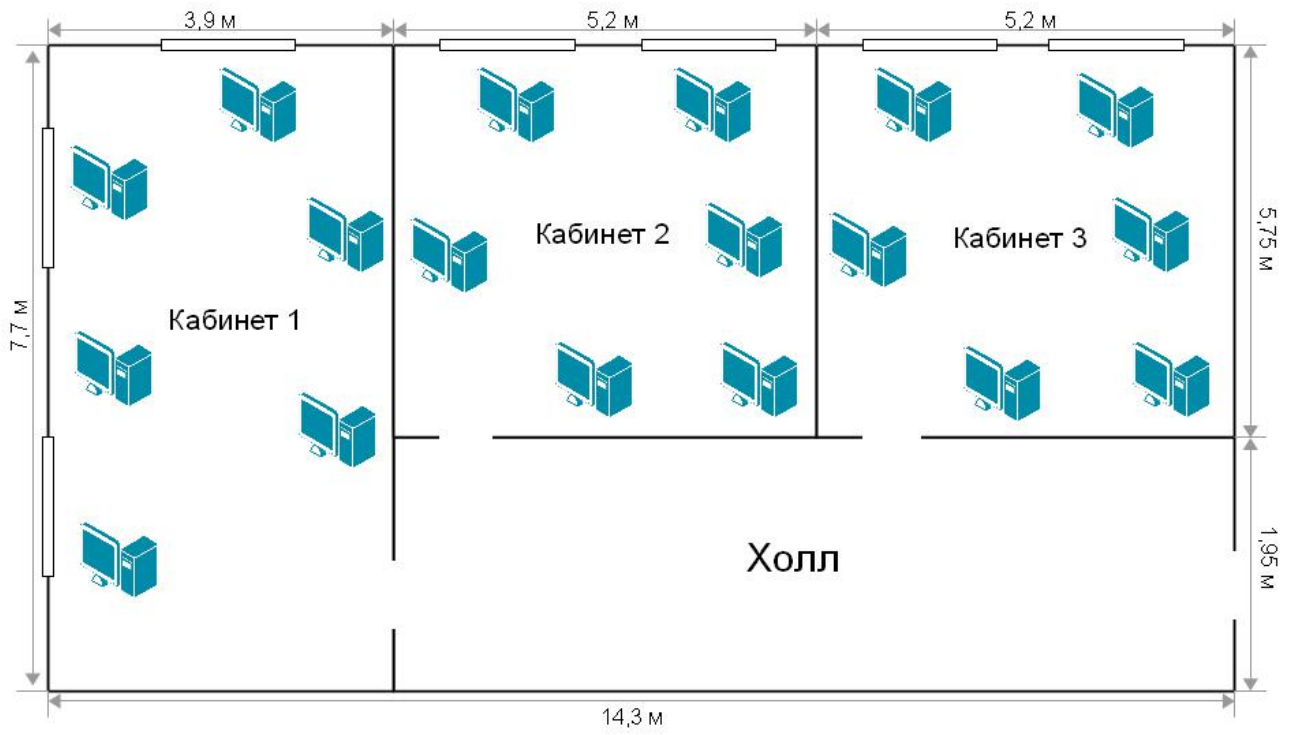


Рисунок 2.1 План 1-го этажа центрального офиса

Зарисуйте получившуюся топологию сети.

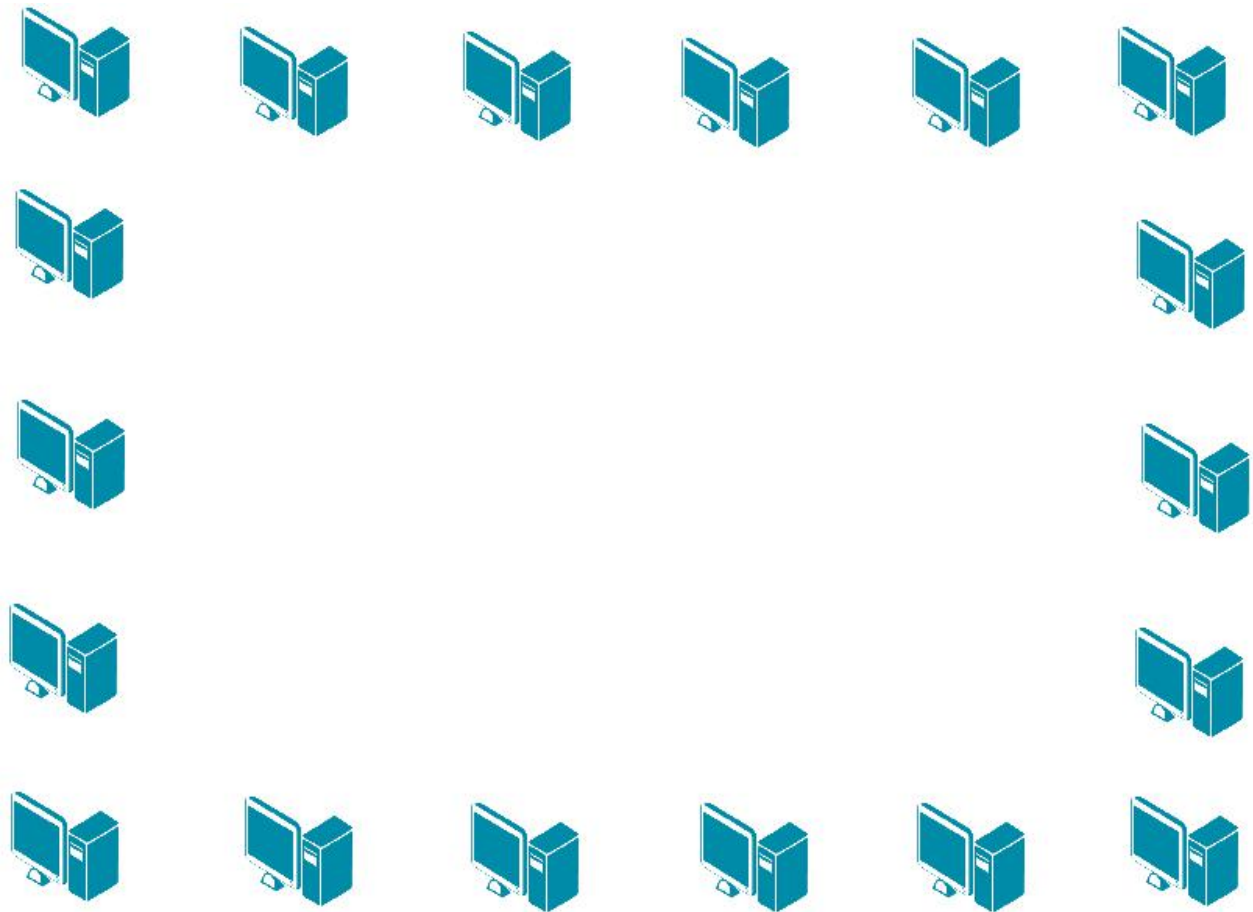


Рисунок 2.2 Топология сети центрального офиса

Какое сетевое оборудование необходимо использовать, чтобы избежать возникновения коллизий при передаче данных между компьютерами? _____

Какое минимальное количество портов должно быть у сетевого оборудования? _____

Обоснуйте выбор топологии сети. В чем преимущества данной топологии по сравнению с топологией «Общая шина»? _____

ЗАДАНИЕ 2

Предположим, что компания расширилась и теперь занимает такое же помещение в соседнем здании на расстоянии 500 метров (рис. 2.3). Требуется объединить сеть центрального офиса и сеть подразделения так, чтобы сотрудники центрального офиса могли обмениваться данными с сотрудниками подразделения.

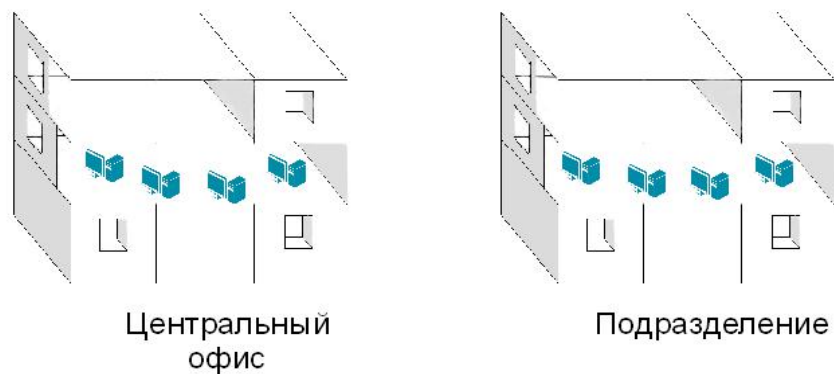


Рисунок 2.3

Зарисуйте получившуюся топологию сети.

Лабораторная работа №3. Изучение элементов кабельной системы

Кабельная система — это система, элементами которой является *пассивное* сетевое оборудование, включающее в себя кабели, разъемы для кабелей, патч-панели, монтажные шкафы и телекоммуникационные стойки.

Кабель состоит из проводников, заключенных в несколько слоев изоляции и бывает трех типов:

- коаксиальный кабель;
- кабель на основе витой пары;
- волоконно-оптический (оптоволоконный) кабель.

Коаксиальный кабель — электрический кабель, состоящий из расположенных соосно центрального проводника и экрана. Центральная часть кабеля представляет собой монолитный или скрученный медный провод, заключенный в изолирующую пластиковую оболочку. Эту изоляцию окружает второй проводник в виде трубки (может быть из фольги), который служит экраном от электромагнитных помех. Снаружи он покрыт жесткой пластиковой трубкой, формирующей оболочку кабеля. В настоящее время коаксиальный кабель не используется для построения локальных сетей.

Кабель на основе витой пары (twisted pair) — вид кабеля, представляющий собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой. Попарное скручивание проводов позволяет уменьшить воздействие перекрестных помех, так как электромагнитные волны, излучаемые каждым проводником, взаимно гасятся.

Различают два типа кабеля на основе витой пары:

- кабель на основе неэкранированной витой пары (unshielded twisted pair, UTP);
- кабель на основе экранированной витой пары (shielded twisted pair, STP).

Кабель на основе неэкранированной витой пары (UTP) состоит из четырех скрученных между собой пар проводов.

Кабели на основе экранированной витой пары (STP) имеют дополнительную защиту из алюминиевой фольги, которая позволяет уменьшить воздействие внешних электромагнитных полей.

Кабели на основе экранированной и неэкранированной витой пары подключаются к компьютерам и сетевым устройствам при помощи **разъема 8P8C** (ошибочное, но общепринятое название RJ-45).

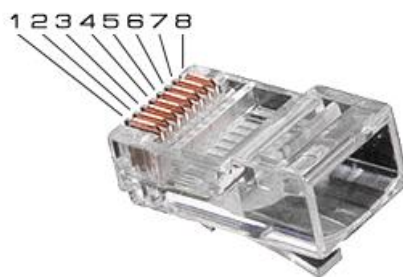


Рисунок 3.1 Разъем 8P8C (RJ-45)

Последовательность распределения проводников в разъеме определяется стандартами EIA/TIA-568A и EIA/TIA-568B (рис.3.2).

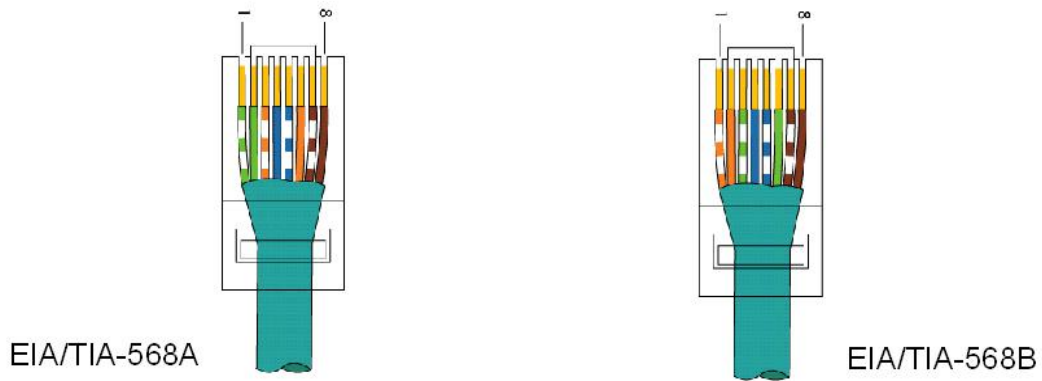
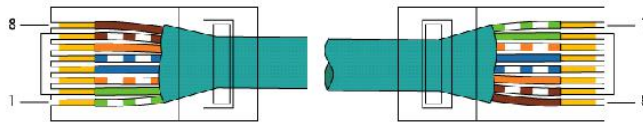


Рисунок 3.2 Распределение проводников в разъеме по стандартам EIA/TIA-568A и EIA/TIA-568B

В зависимости от схемы распределения проводников в разъемах с двух сторон кабеля, кабели делятся на:

- **Прямые кабели (straight through cable)** – витая пара с обеих сторон обжата одинаково, без перекрещивания пар внутри кабеля.

Прямой кабель по стандарту EIA/TIA-568A



Прямой кабель по стандарту EIA/TIA-568B

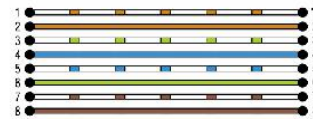
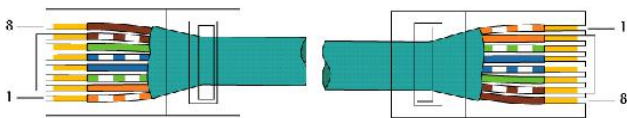


Рисунок 3.3 Прямой кабель

- **Перекрестные кабели (crossover cable)** – инвертированная разводка с перекрещиванием пар внутри кабеля.

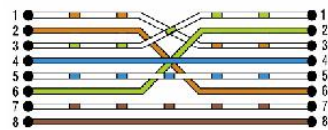
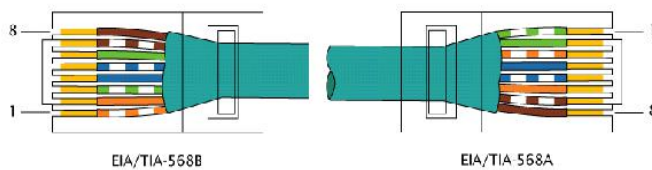


Рисунок 3.4 Перекрестный кабель

Для обжима кабеля разъемами RJ-45 используется специальный инструмент, который называется **кримпер** (рис. 3.5).



Рисунок 3.5 Инструмент для обжима кабеля разъемами RJ-45 (кримпер)

Оборудование (на 1 рабочее место):

Кабель Ethernet (UTP)	0,2 м.
Волоконно-оптический кабель	0,2 м.
Разъем RJ-45	2 шт.
Обжимной инструмент (кримпер)	1 шт.
Разъем типа SC-FC (или SC-ST)	1 шт.
Сетевой тестер	1 шт.

Цель:

- 1) Изучить волоконно-оптический кабель;
- 2) Научиться обжимать кабель UTP разъемами RJ-45;
- 3) Получить навыки в расчете кабельной сети.

3.1. Изучение волоконно-оптического кабеля

ЗАДАНИЕ

Так как заделка волоконно-оптического кабеля производится методом сварки и требует специальной подготовки, в данной работе производится только визуальное изучение образца волоконно-оптического кабеля и разъемов.

Волоконно-оптический (оптоволоконный) кабель состоит из светопроводящего стеклянного сердечника, окруженного стеклянной оболочкой с меньшим коэффициентом преломления.

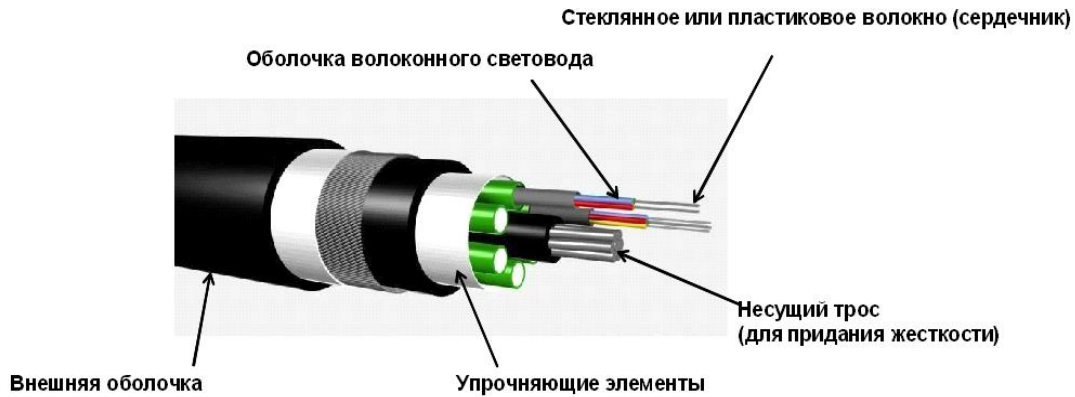


Рисунок 3.6 Волоконно-оптический кабель

В зависимости от распределения показателя преломления и от величины диаметра сердечника различают:

- одномодовый волоконно-оптический кабель;
- многомодовый волоконно-оптический кабель.

В **одномодовом кабеле (Single Mode Fiber, SMF)** оптический сигнал, распространяющийся по сердцевине, представлен одной модой. В одномодовом кабеле используется центральный сердечник очень малого диаметра, соизмеримого с длиной волны света — 5-10 мкм. В качестве источников излучения света в одномодовом кабеле применяются полупроводниковые лазеры с длиной волны 1300 нм, 1550 нм. Максимальная длина кабеля — 100 км, поэтому он используется, как правило, для протяженных линий связи, городских и региональных сетей. Пропускная способность одномодового оптического кабеля превышает 10 Гбит/с.

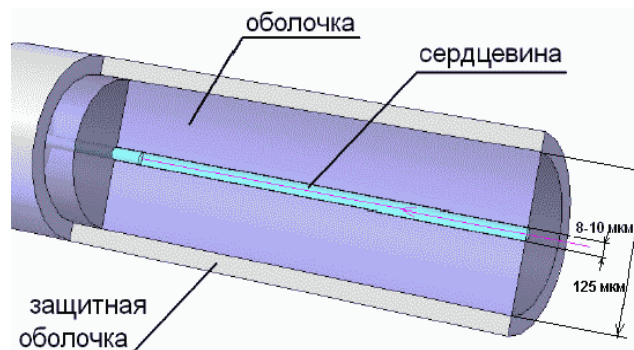


Рисунок 3.7 Одномодовый оптический кабель в разрезе

В **многомодовом кабеле (Multi Mode Fiber, MMF)** оптический сигнал, распространяющийся по сердцевине, представлен множеством мод. В многомодовых кабелях используются внутренние сердечники с диаметрами 62,5/125 мкм и 50/125 мкм, где 62,5 мкм или 50 мкм — это диаметр центрального проводника, а 125 мкм — диаметр внешнего проводника. В качестве источников излучения света в многомодовом кабеле применяются светодиоды с длиной волны 850 нм. Максимальная длина кабеля — 2 км. Используется в

локальных и домашних сетях небольшой протяженности.

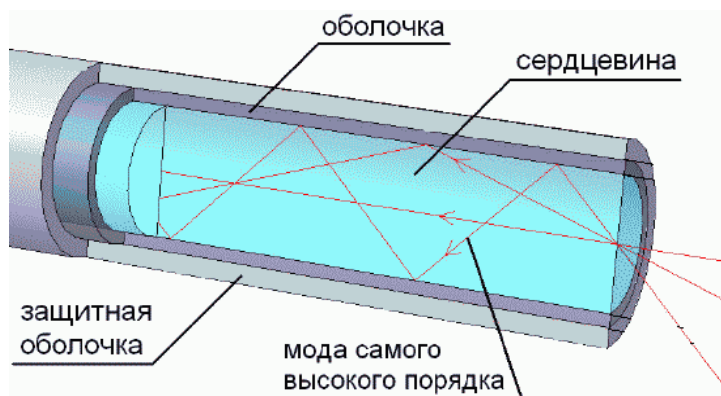


Рисунок 3.8 Многомодовый оптический кабель в разрезе

Волоконно-оптические кабели присоединяются к оборудованию разъемами: MT-RJ, ST, FC, SC, LC.

Разъем типа MT-RJ представляет собой миниатюрный дуплексный разъем.



Рисунок 3.9 Разъем типа MT-RJ

Разъем типа ST использует быстро сочленяемое байонетное соединение, которое требует поворота разъема на четверть оборота для осуществления соединения/разъединения.



Рисунок 3.10 Разъем типа ST

Разъемы типа FC ориентированы на работу с одномодовым кабелем.



Рисунок 3.11 Разъем типа FC

Разъемы типа SC широко используются как для одномодового, так и для многомодового волокна. Относится к классу разъемов общего пользования. В разьеме используется механизм сочленения «push-pull». Может объединяться в модуль, состоящий из нескольких разъемов. В этом случае модуль может использоваться для дуплексного соединения, одно волокно которого используется для передачи в прямом, а другое в обратном направлениях.



Рисунок 3.15 Распределение проводников в разъеме по стандартам EIA/TIA-568A и EIA/TIA-568B

Шаг 4. Плотно прижимая проводники, обрежьте неровные края, оставляя примерно 1 см.

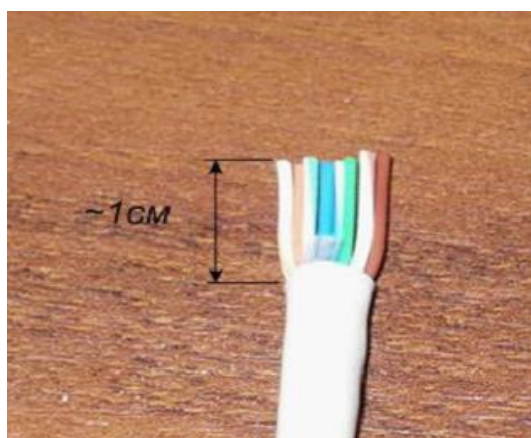


Рисунок 3.16 Выравнивание проводников

Шаг 5. Возьмите разъем RJ-45 и поверните его контактами вверх. Аккуратно вставьте проводники в разъем так, чтобы они попали в соответствующие дорожки и цветовое расположение не перепуталось. Следите за тем, чтобы все проводники доходили до конца разъема и внешняя изоляция кабеля выходила за фиксирующую защелку.

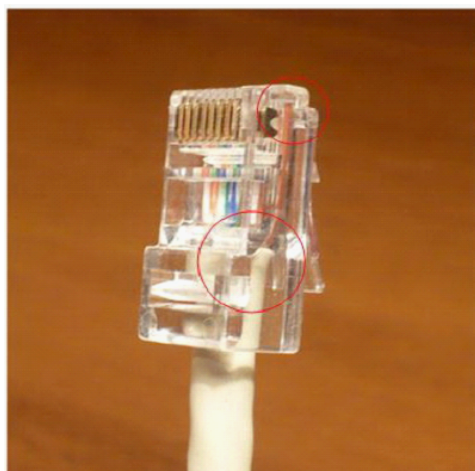


Рисунок 3.17 Места, на которые необходимо обратить внимание при обжиме кабеля

Внимание: часто на этом шаге проводники смещаются, особенно если используется некачественный кабель. В этом случае извлеките кабель из разъема и повторите шаг 5.

Шаг 6. Убедившись в правильном расположении проводников, вставьте разъем в обжимной инструмент (кримпер), как показано на рисунке 3.18, и аккуратно зажмите.

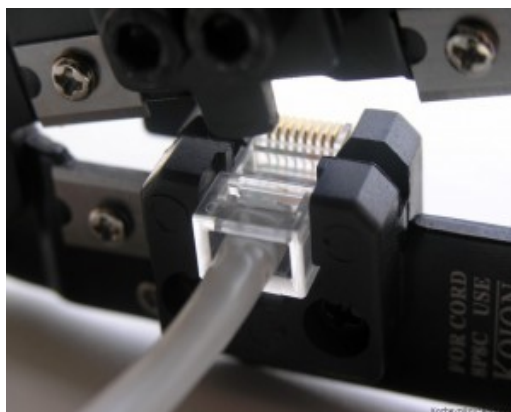


Рисунок 3.18 Обжим разъема RJ-45 кримпером

Шаг 7. Извлеките обжатый разъем из кримпера и еще раз проверьте расположение проводников. Правильно обжатый кабель показан на рисунке 3.19.

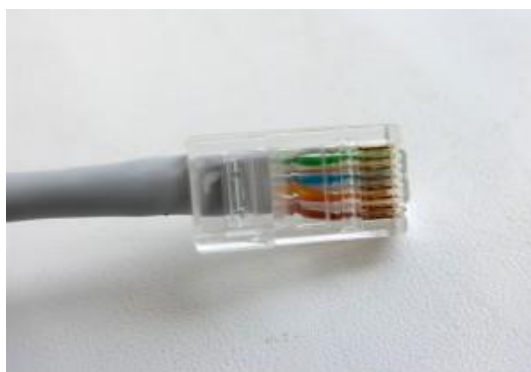


Рисунок 3.19 Правильно обжатый кабель

При неправильном обжиге внешняя изоляция кабеля не закреплена фиксирующей защелкой разъема и проводники могут смещаться. Пример неправильно обжатого кабеля показан на рисунке 3.20.

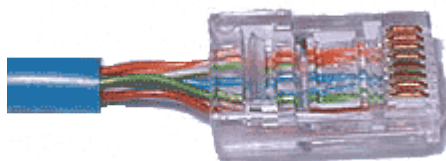


Рисунок 3.20 Неправильно обжатый кабель

Шаг 8. Повторите шаги 1-7 для обжима другого конца кабеля. Используйте ту же схему, что и для первого конца кабеля. Такой тип обжима называется *прямой обжим*.

Прямой тип кабеля используется в тех случаях, когда устройства на противоположных концах используют разные номера проводников для приема и передачи информации. Например, прямым кабелем соединяются компьютер-коммутатор.

Для подключения друг к другу устройств, использующих одинаковые номера проводников для приема и передачи информации, в самом кабеле необходимо поменять местами пары проводников. Такой кабель называется **перекрестным кабелем**. Таким типом кабеля соединяют, например, компьютер-компьютер.

Шаг 9. Подключите кабель к сетевому тестеру обоими концами.



Рисунок 3.21 Сетевой тестер

Сетевой тестер состоит из двух независимых частей, на каждой из которых расположены 8 индикаторов и по одному разъему RJ-45. Если кабель обжат правильно, то все индикаторы должны загораться последовательно, если кабель обжат неправильно, то индикатор не загорится.

3.3. Расчет кабельной сети

ЗАДАНИЕ

Для топологии сети из лабораторной работы №2 (задание 1) выберите тип кабельной системы и рассчитайте длину кабеля. На рисунке 3.22 обозначьте расположение коммутатора и соедините с ним каждый компьютер при помощи кабеля.

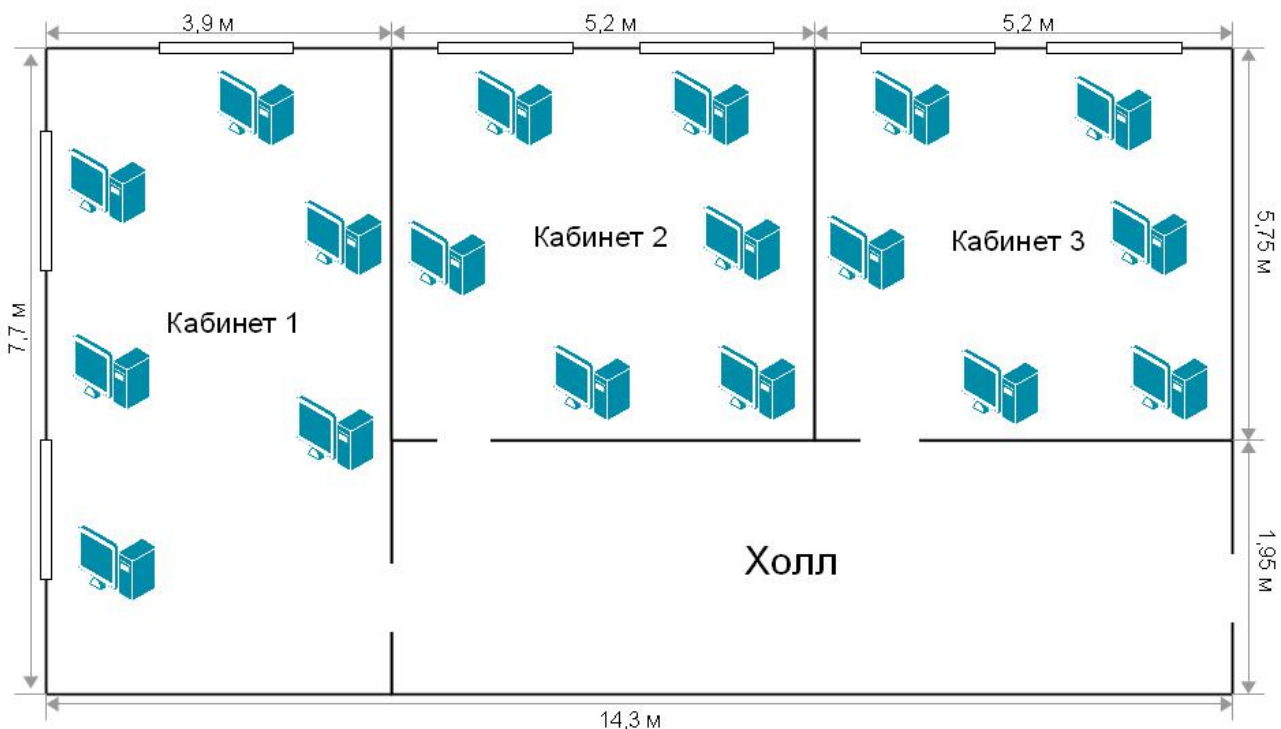


Рисунок 3.22 Схема 1-го этажа центрального офиса

Тип кабеля _____

Сколько кабеля (в метрах) понадобится для объединения компьютеров центрального офиса в сеть, если все компьютеры стоят у стен и коммутатор размещен в кабинете 3? (В межкомнатных перегородках запрещается просверливать отверстия) _____

Лабораторная работа №4. Построение одноранговой сети

По типу взаимодействия между компьютерами и с точки зрения распределения ролей между ними различают *одноранговые* и *клиент-серверные* сети.

В *одноранговой сети (peer-to-peer)* все компьютеры равны. Каждый из них может выступать как в роли сервера, предоставлять файлы и аппаратные ресурсы (принтеры, жесткие диски и т.д.) другим компьютерам, так и в роли клиента, пользующегося ресурсами других компьютеров. Число компьютеров в одноранговых сетях обычно не превышает 10, поэтому их другое название – *рабочая группа*. Примерами рабочих групп являются домашние сети или сети небольших офисов.

Сети типа «*клиент-сервер*» (*client-server*), как правило, создаются в учреждениях или крупных предприятиях. В таких сетях выделяются один или несколько компьютеров, называемых *серверами*, задача которых состоит в быстрой и эффективной обработке большого числа запросов других компьютеров – *клиентов*. Сети клиент-сервер являются наилучшим вариантом для объединения в сеть более десяти компьютеров. Они более дорогие, чем одноранговые сети, но для больших компаний или в случаях, когда необходимо хранить большой объем информации, это самый лучший выбор.

Как компьютеры, объединенные в сеть, взаимодействуют друг с другом? Чтобы это стало возможным, для начала необходимо объединить участников сети. Для этой цели применяется сетевая кабель, который одним концом подключается в *сетевой адаптер* – специальную печатную плату, установленную в компьютер и позволяющую подключить его к сети, а другим концом в какое-нибудь устройство связи (концентратор, маршрутизатор, коммутатор и т.д.). В большинстве современных компьютеров сетевой адаптер является встроенным.



Рисунок 4.1 Сетевой адаптер DGE-560T

При соединении двух компьютеров используется *перекрестный кабель*, если сетевой адаптер не поддерживает функцию автоматического определения полярности витой пары *Auto MDI/MDIX*.

Существует два типа Ethernet-портов: *MDI* и *MDIX*.

Как правило, *MDI порт* — это порт абонентского устройства (сетевая карта ПК), в котором 1 и 2 контакты используются для передачи сигнала, 3 и 6 контакты для приема сигнала. *Порт MDIX* — это порт коммутатора или концентратора, в котором 1 и 2 контакты используются для приема сигнала, 3 и 6 контакты для передачи сигнала. Поэтому для соединения портов MDI-MDIX (компьютер-коммутатор) применяют «прямой» кабель UTP, а для соединения портов MDIX-MDIX и MDI-MDI – «перекрестный».

Если интерфейс поддерживает функцию *Auto MDI/MDIX*, то устройство само определяет, какой тип кабеля подключен к порту. Эта функция перенастраивает коммутирующие микросхемы под установленный кабель, поэтому тип используемого кабеля значение не имеет.

Однако соединить компьютеры друг с другом недостаточно. Нужно их еще научить «разговаривать». Для этого требуются *сетевые операционные системы*, поддерживающие один и тот же набор *протоколов*, с помощью которых компьютеры общаются по сети. Для сетевых протоколов используется многоуровневая модель OSI (Open System Interconnection –

взаимодействие открытых систем). Протоколы необходимы для организации и поддержания связи, для безошибочной передачи данных, а также для того, чтобы определить, как отправляется информация и как ее получить.

Утилиты диагностики соединения

Существует ряд утилит и программ, позволяющих выполнять диагностику и поиск неисправностей в сетях.

Команда **ipconfig** — позволяет просмотреть конфигурацию сетевого адаптера компьютера. При вызове утилиты ipconfig без параметров, выводится только IP-адрес, маска подсети и шлюз по умолчанию.

Пример: **ipconfig**

При вызове команды ipconfig с параметром /all, выводится полная конфигурация TCP/IP для всех сетевых адаптеров.

Пример: **ipconfig /all**

Для проверки соединения между узлами сети и вывода результата на экран можно воспользоваться утилитой **ping**. Команда ping сообщает, ответил ли опрошенный узел и сколько времени прошло до получения ответа.

Пример: **ping <IP-адрес или доменное имя>**

Проверить MAC-адреса сетевых интерфейсов компьютера можно при помощи команды getmac.

Пример: **getmac**

Оборудование (на 1 рабочее место):

Рабочая станция	2 шт.
Коммутатор DES-1100-16	1 шт.
Кабель Ethernet («перекрестный»)	1 шт.
Кабель Ethernet («прямой»)	2 шт.

Цель: изучить принципы построения одноранговых сетей.

4.1. Создание подключения типа «компьютер-компьютер»

Шаг 1. Подключите один конец «перекрестного» Ethernet-кабеля к сетевому адаптеру ПК1, а другой конец кабеля — к сетевому адаптеру ПК2 (рис. 4.2). Проверьте наличие физического соединения между компьютерами по индикации светодиодов на сетевых адаптерах ПК1 и ПК2.

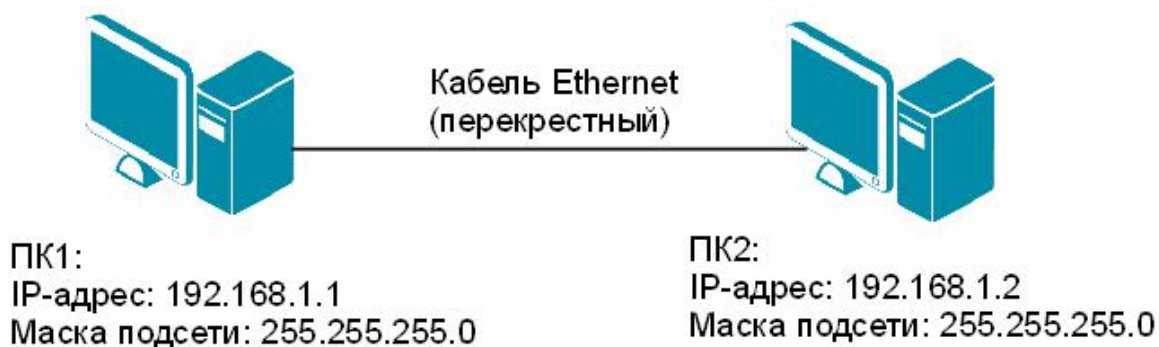


Рисунок 4.2 Схема подключения типа «компьютер-компьютер»

Шаг 2. Настройте статический IP-адрес на рабочей станции ПК1 и ПК2.

Настройка IP-адреса на рабочей станции с ОС Windows XP (рис. 4.3):

1. Откройте *Сетевые подключения*;

Пуск → Панель управления → Сетевые подключения

- Щелкните правой кнопкой мыши на *Подключение по локальной сети* и выберите *Свойства*;
- В диалоговом окне выберите *Протокол Интернета (TCP/IP)* и нажмите *Свойства*;
- Выберите *Использовать следующий IP-адрес*;
- В поле *IP-адрес* введите: 192.168.1.1 (для ПК1) или 192.168.1.2 (для ПК2);
- В поле *Маска подсети* введите: 255.255.255.0;
- Нажмите кнопку *Ок*.

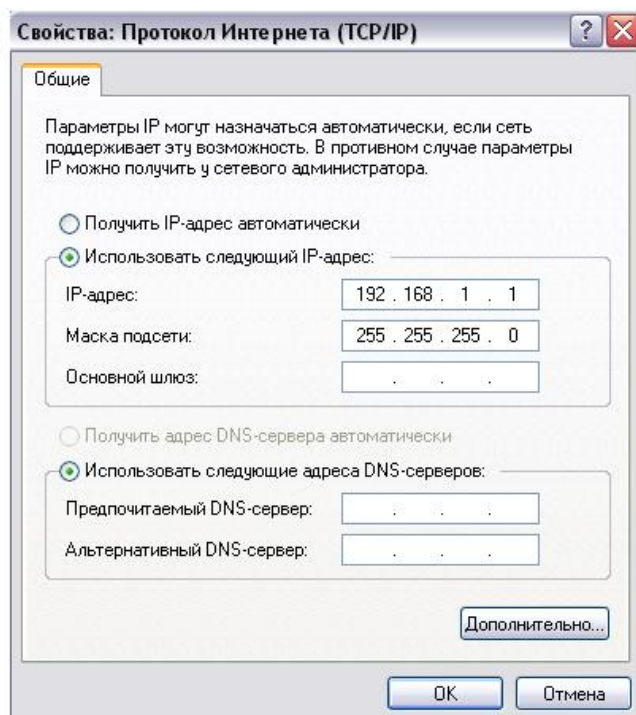
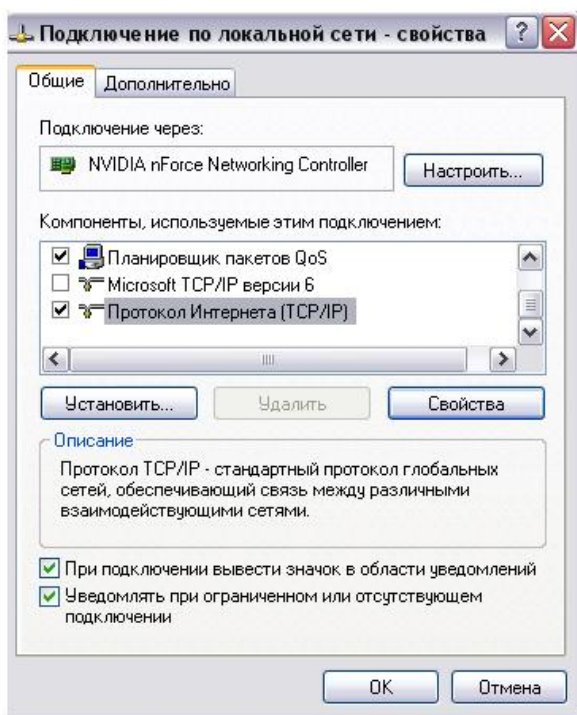
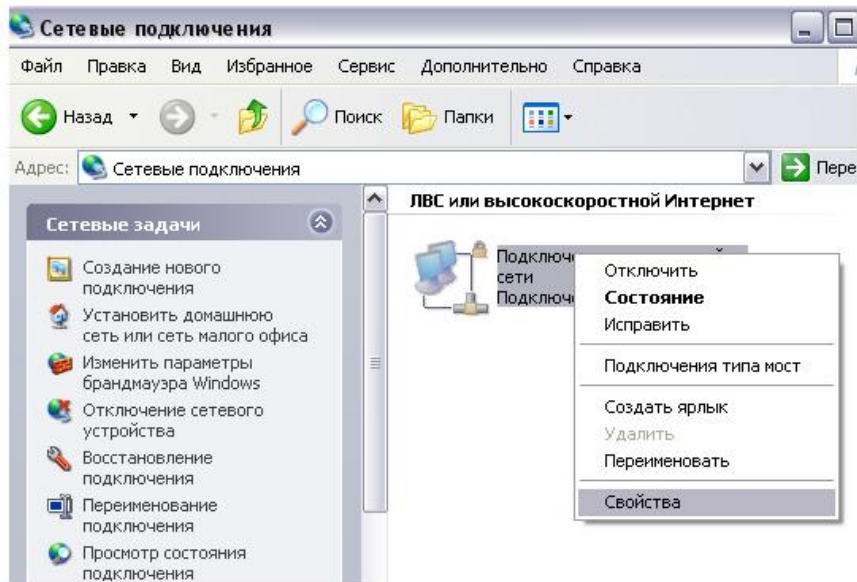


Рисунок 4.3 Настройка статического IP-адреса для ОС Windows XP

Настройка IP-адреса на рабочей станции с ОС Windows 7/Vista:

1. Откройте *Центр управления сетями и общим доступом* (рис. 4.4);

Пуск → Панель управления → Центр управления сетями и общим доступом

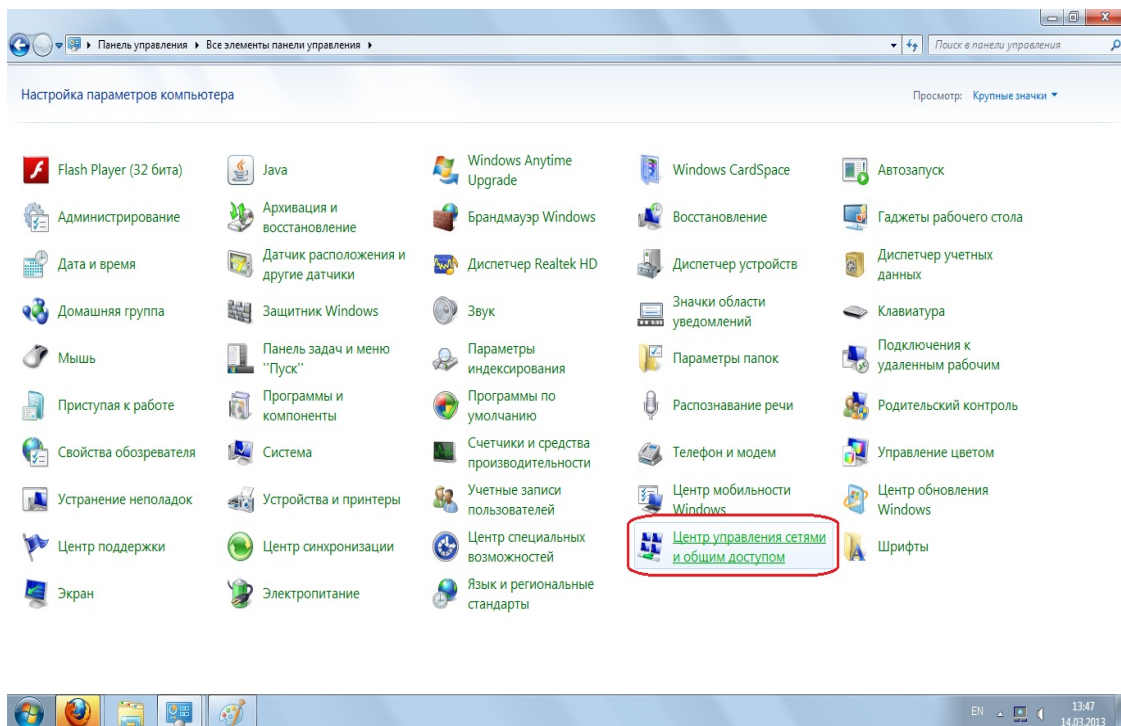


Рисунок 4.4 Окно *Панель управления*

Примечание: если панель управления имеет вид «по категориям» (в верхнем правом углу окна в списке *Просмотр* выбран пункт *Категория*), выберите строку *Просмотр состояния сети и задач* под пунктом *Сеть и Интернет*.

2. В меню, расположенном в левой части окна, выберите пункт *Изменение параметров адаптера* (рис. 4.5);

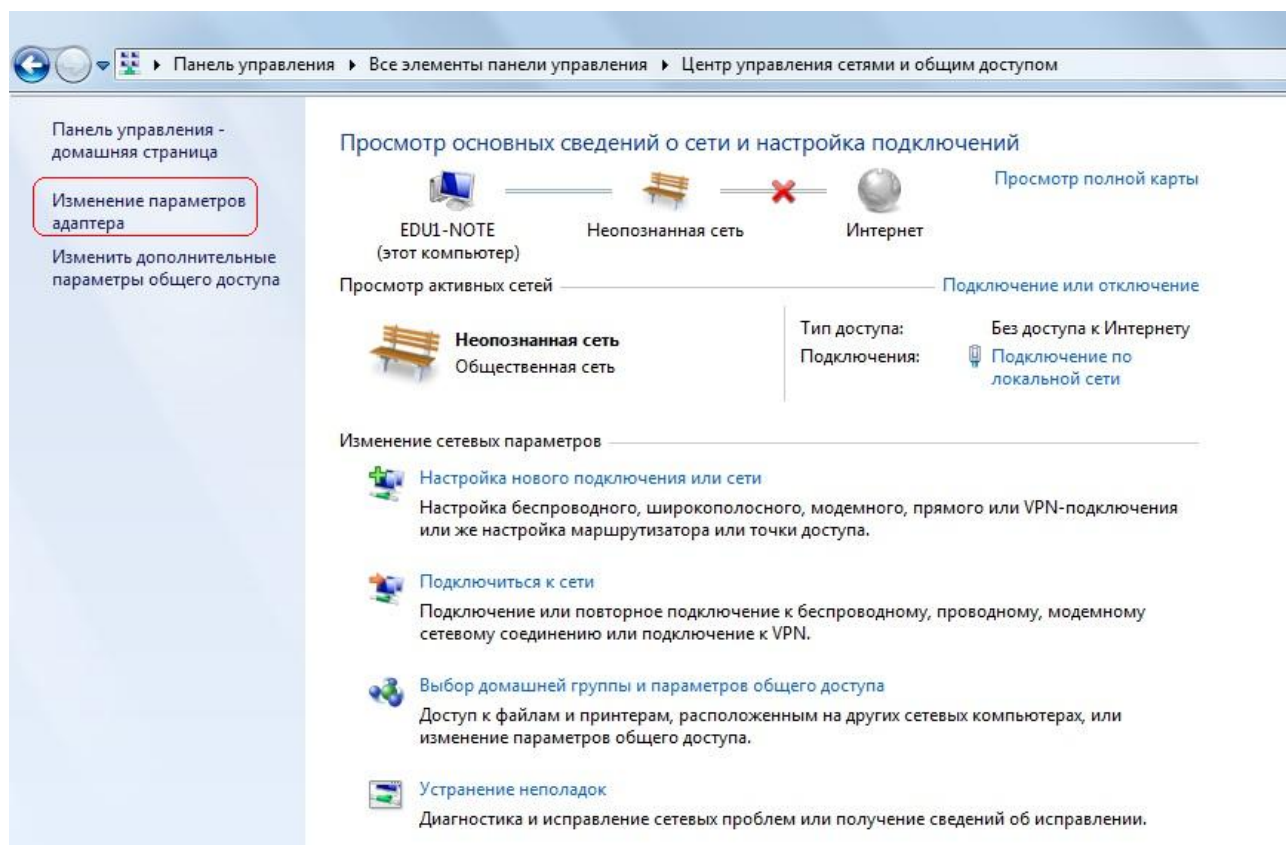


Рисунок 4.5 Окно *Центр управления сетями и общим доступом*

3. Щелкните правой кнопкой мыши на *Подключение по локальной сети* и выберите *Свойства*;
4. На вкладке *Сеть* выделите строку *Протокол Интернета версии 4 (TCP/IP)* и нажмите кнопку *Свойства*;
5. Выберите *Использовать следующий IP-адрес*;
6. В поле *IP-адрес* введите: 192.168.1.1(для ПК1) или 192.168.1.2 (для ПК2);
7. В поле *Маска подсети* введите: 255.255.255.0;
8. Нажмите кнопку *Ок*.

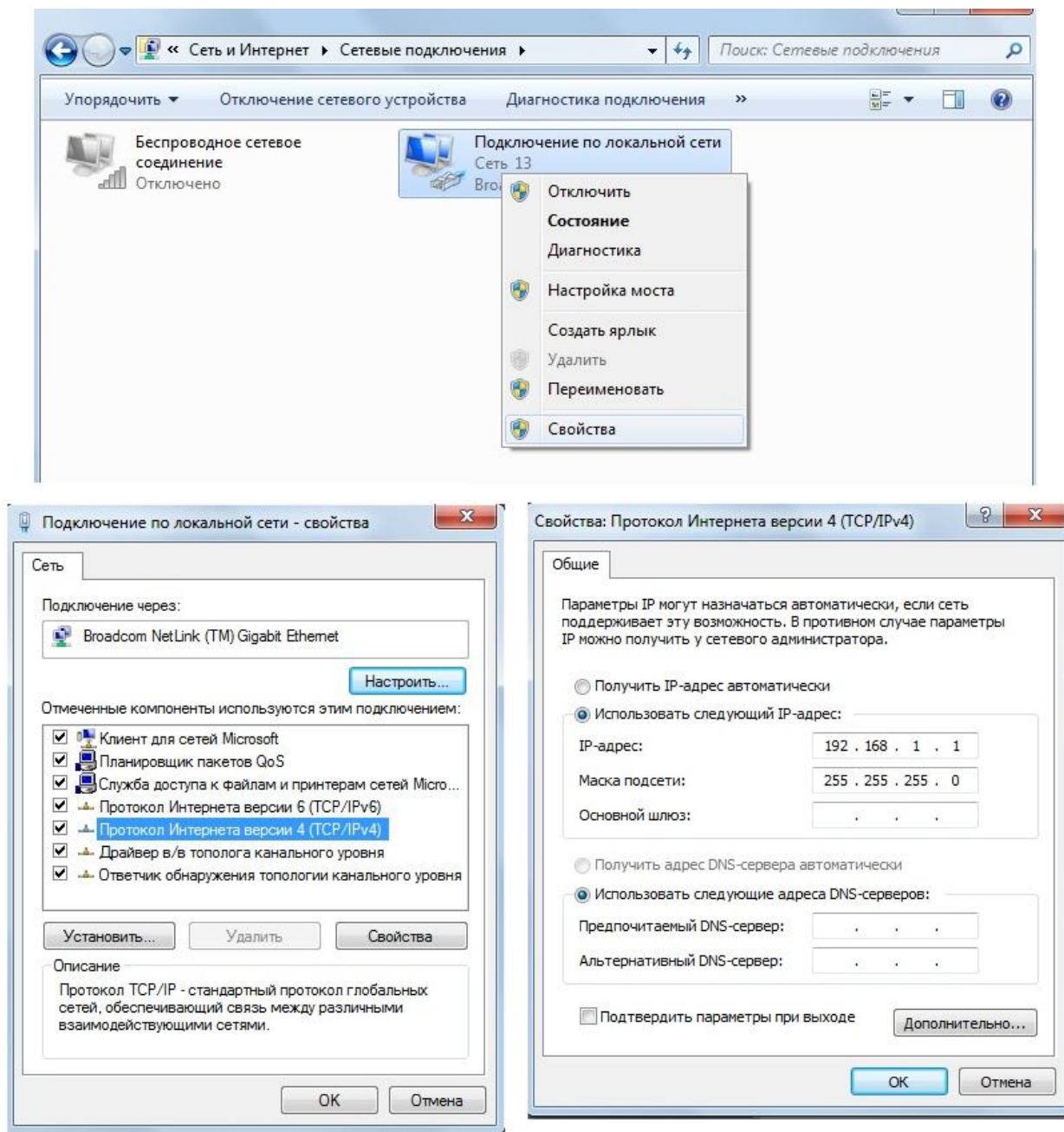


Рисунок 4.6 Настройка статического IP-адреса для ОС Windows 7/ Vista

Шаг 3. Проверьте конфигурацию сетевого адаптера ПК1. В командной строке введите: ipconfig

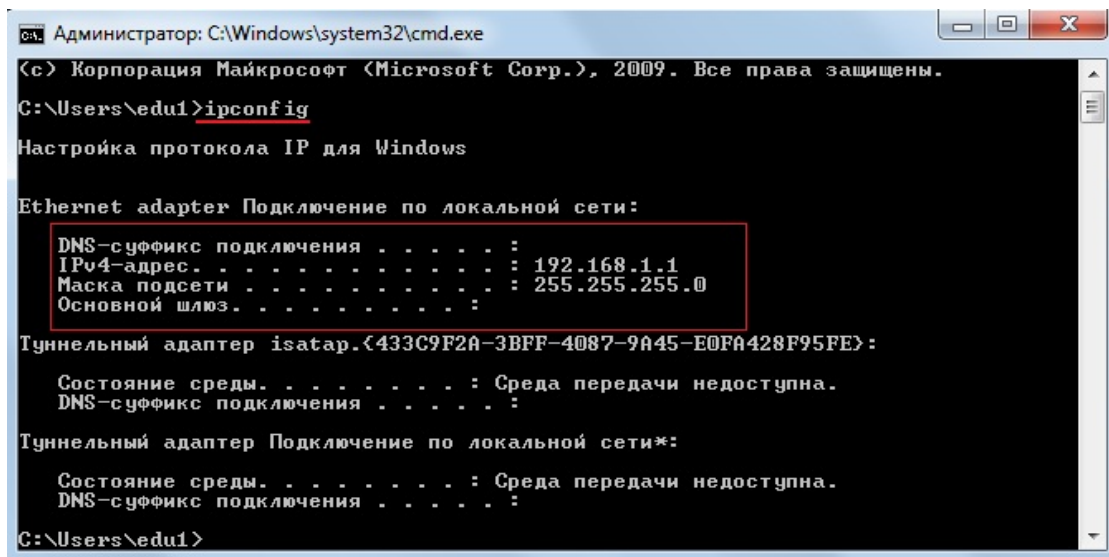


Рисунок 4.7 Проверка конфигурации сетевого адаптера

Чтобы открыть командную строку в Windows XP, выполните следующие действия:

1. Откройте окно *Запуск программы*;

Пуск → *Выполнить*

или

одновременно нажмите клавиши Windows+R

2. В появившемся окне введите *cmd* и нажмите *Ок*.

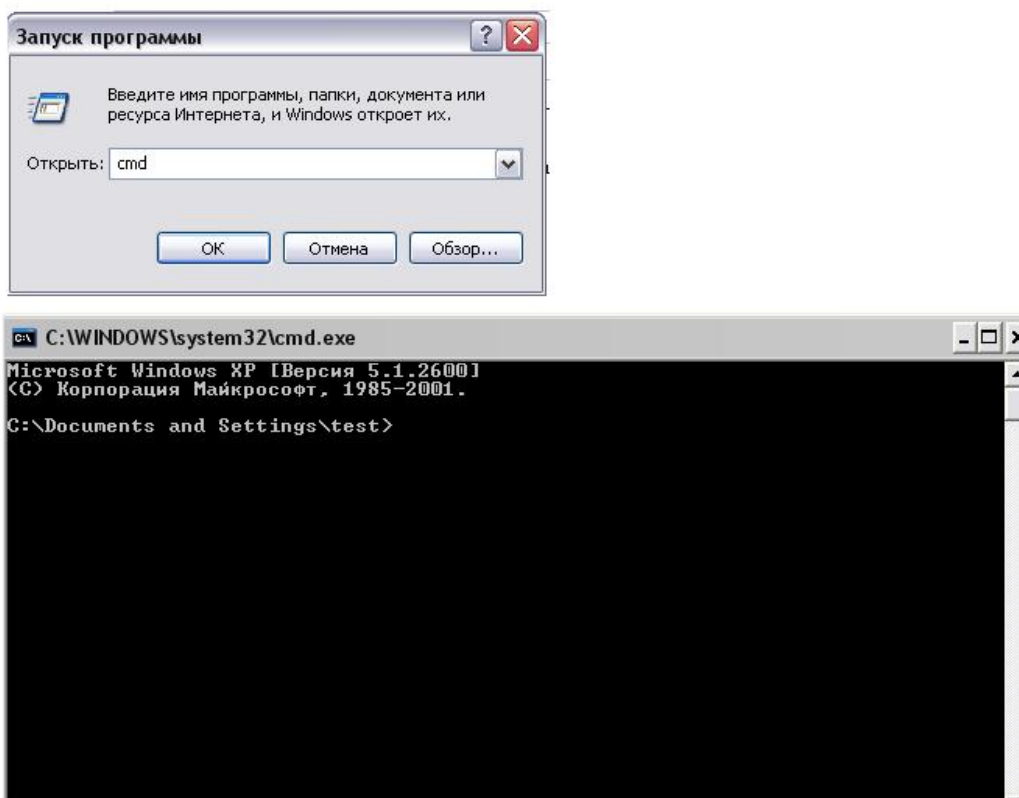


Рисунок 4.8 Запуск командной строки через cmd.exe для ОС Windows XP

Кроме того, открыть командную строку можно с помощью элементов меню *Пуск*:

Пуск → *Все программы* → *Стандартные* → *Командная строка*

Чтобы открыть командную строку в Windows 7/Vista, выполните следующие действия (рис. 4.9):

1. Нажмите меню *Пуск* и в строке поиска введите *cmd*;
2. Нажмите на клавиатуре *Enter*.

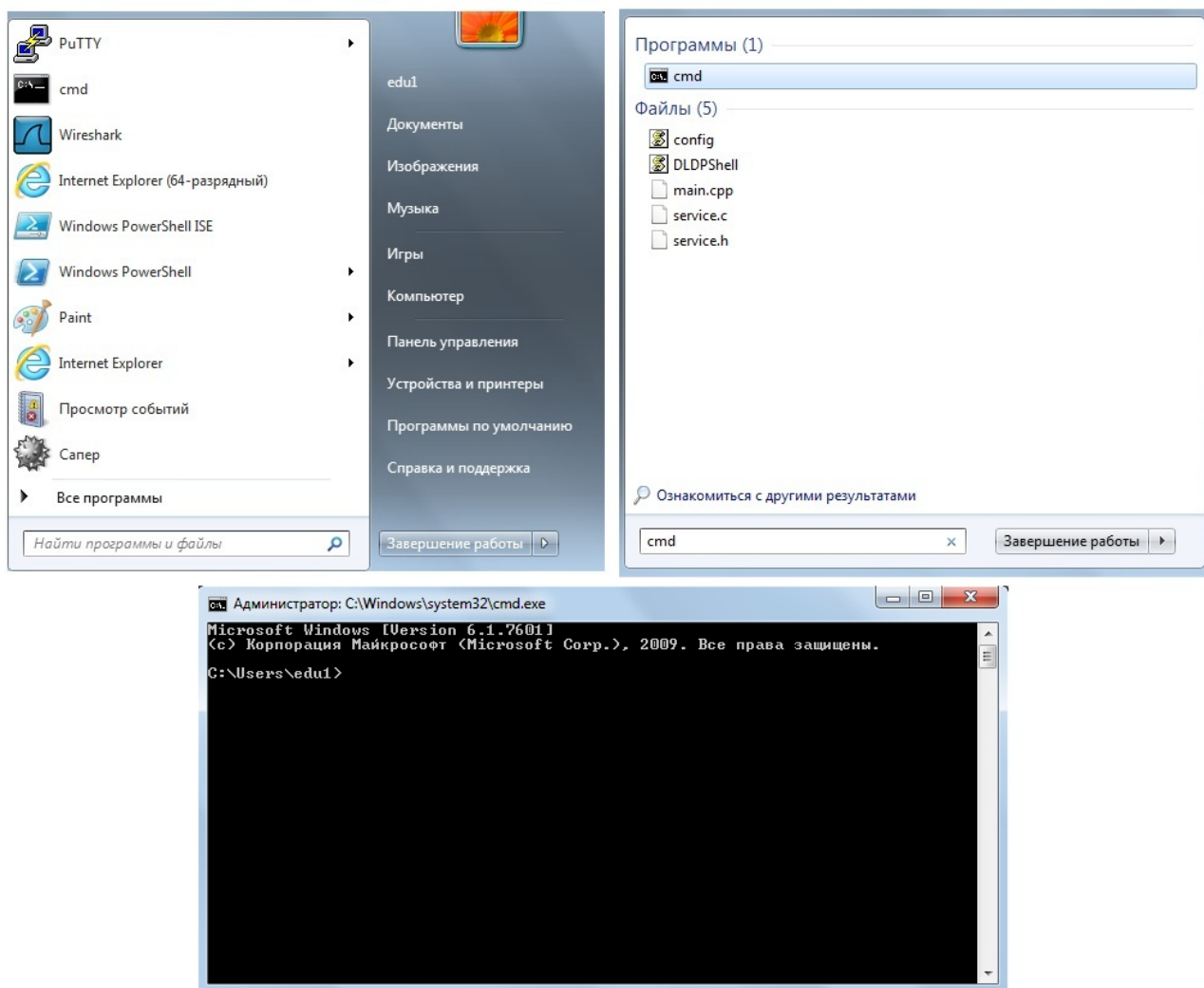


Рисунок 4.9 Запуск командной строки через cmd.exe для ОС Windows 7/ Vista

Шаг 4. Проверьте конфигурацию сетевого адаптера ПК2. В командной строке введите: `ipconfig`

Шаг 5. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1 введите: `ping 192.168.1.2`

Ответил ПК2? _____

В командной строке ПК2 введите: `ping 192.168.1.1`

Ответил ПК1? _____

Шаг 6. Подключите один конец «прямого» Ethernet-кабеля к сетевому адаптеру ПК1, а другой конец кабеля — к сетевому адаптеру ПК2 (рис. 4.2). Проверьте наличие физического соединения между компьютерами по индикации светодиодов на сетевых адаптерах ПК1 и ПК2.

Шаг 7. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1 введите: `ping 192.168.1.2`

Ответил ПК2? _____

В командной строке ПК2 введите: `ping 192.168.1.1`

Ответил ПК1? _____

Объясните наличие/отсутствие связи между ПК1 и ПК2 _____

4.2. Создание одноранговой сети с использованием коммутатора

Шаг 1. Подключите ПК1 и ПК2 к коммутатору DES-1100-16 «прямым» Ethernet-кабелем, как показано на рисунке 4.10. Проверьте наличие физического соединения между ПК1 и коммутатором по индикации светодиодов (порт коммутатора, к которому подключена рабочая станция, должен загореться зеленым). Аналогично проверьте наличие физического соединения между ПК2 и коммутатором.

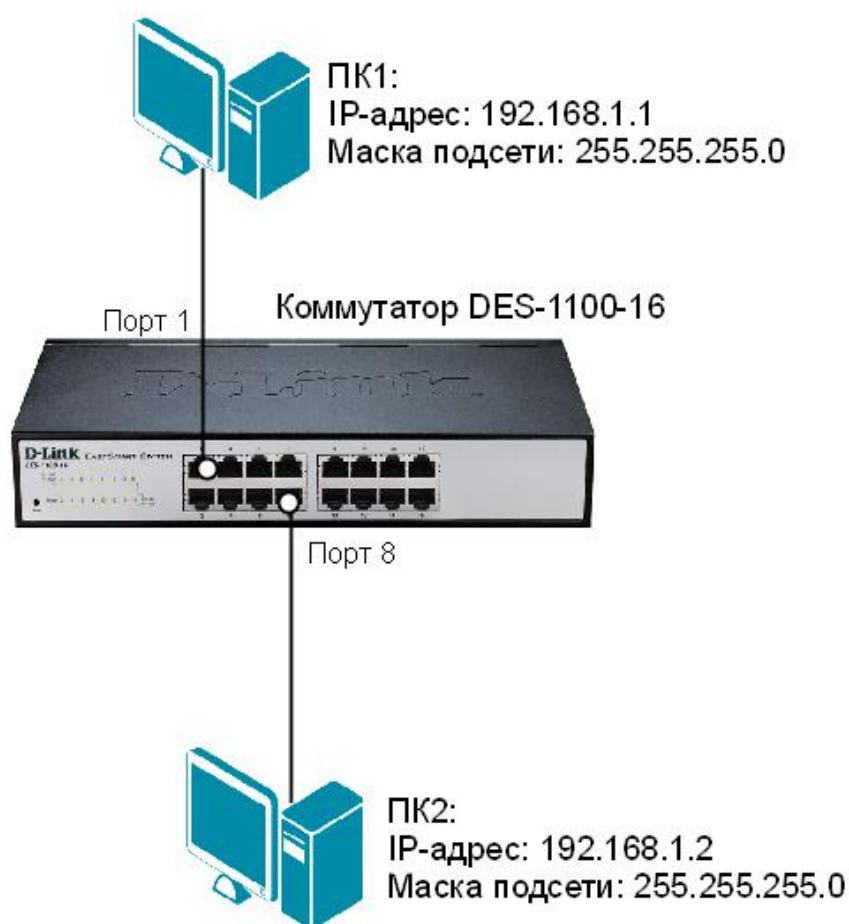


Рисунок 4.10 Схема подключения рабочих станций к коммутатору

Внимание: если индикатор не горит, возможно, что не включено питание одного из устройств или возникли проблемы с сетевым адаптером подключенного устройства, или имеются неполадки с кабелем.

Шаг 2. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1 введите: `ping 192.168.1.2`

Ответил ПК2? _____

В командной строке ПК2 введите: ping 192.168.1.1
Ответил ПК1? _____

Шаг 3. Создайте на рабочих станциях ПК1 и ПК2 папки для общего доступа по сети.

Чтобы открыть общий доступ к папке в Windows XP, выполните следующие действия:

1. Создайте папку, которая будет применяться для обмена информацией по сети;
2. Вызовите контекстное меню созданной папки и выберите пункт *Общий доступ и безопасность*;

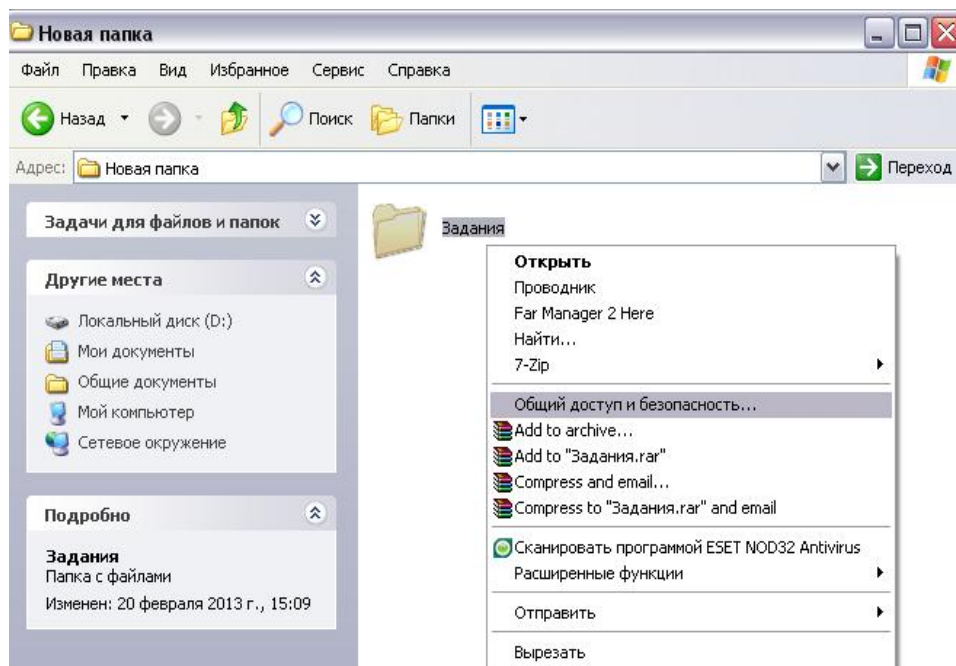


Рисунок 4.11 Настройка общего доступа

3. Во вкладке *Доступ* → *Сетевой общий доступ и безопасность* выберите *Открыть общий доступ к этой папке* и *Разрешить изменение файлов по сети*;

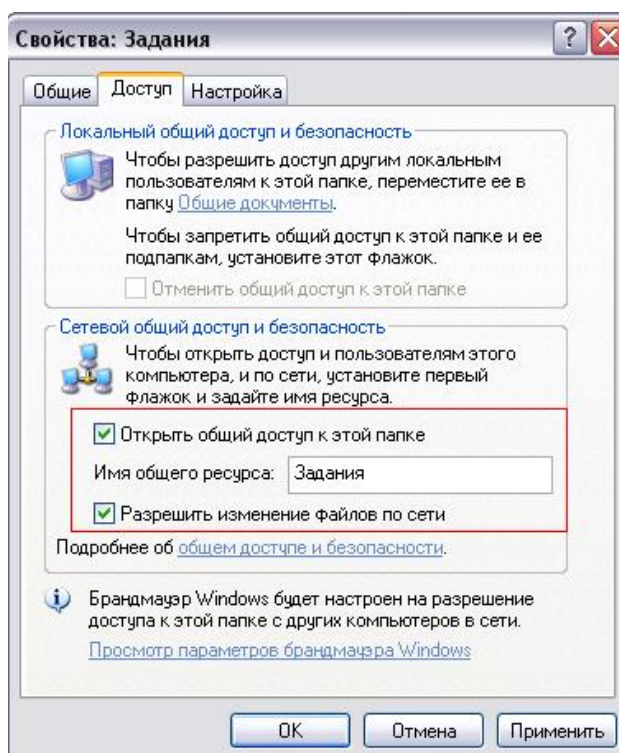


Рисунок 4.12

4. Нажмите кнопку *Применить*;
5. В данной сетевой папке создайте какой-либо документ.

Чтобы открыть общий доступ к папке в Windows 7/Vista, выполните следующие действия:

1. Включите общий сетевой доступ:

*Пуск → Панель управления → Центр управления сетями и общим доступом →
Изменить дополнительные параметры общего доступа*

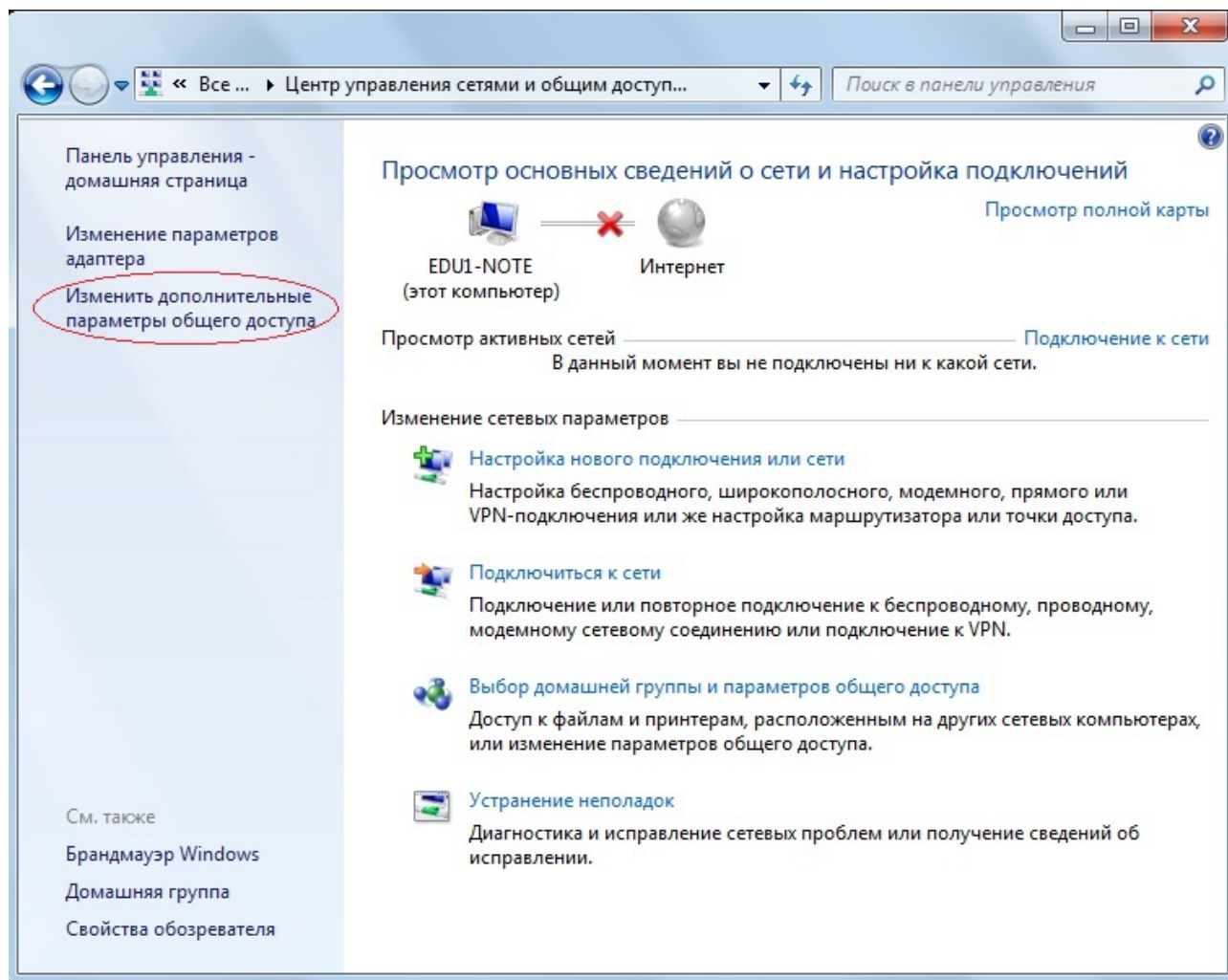


Рисунок 4.13 Изменение дополнительных параметров общего доступа

2. Включите опции *Сетевое обнаружение* и *Доступ к общим папкам*;

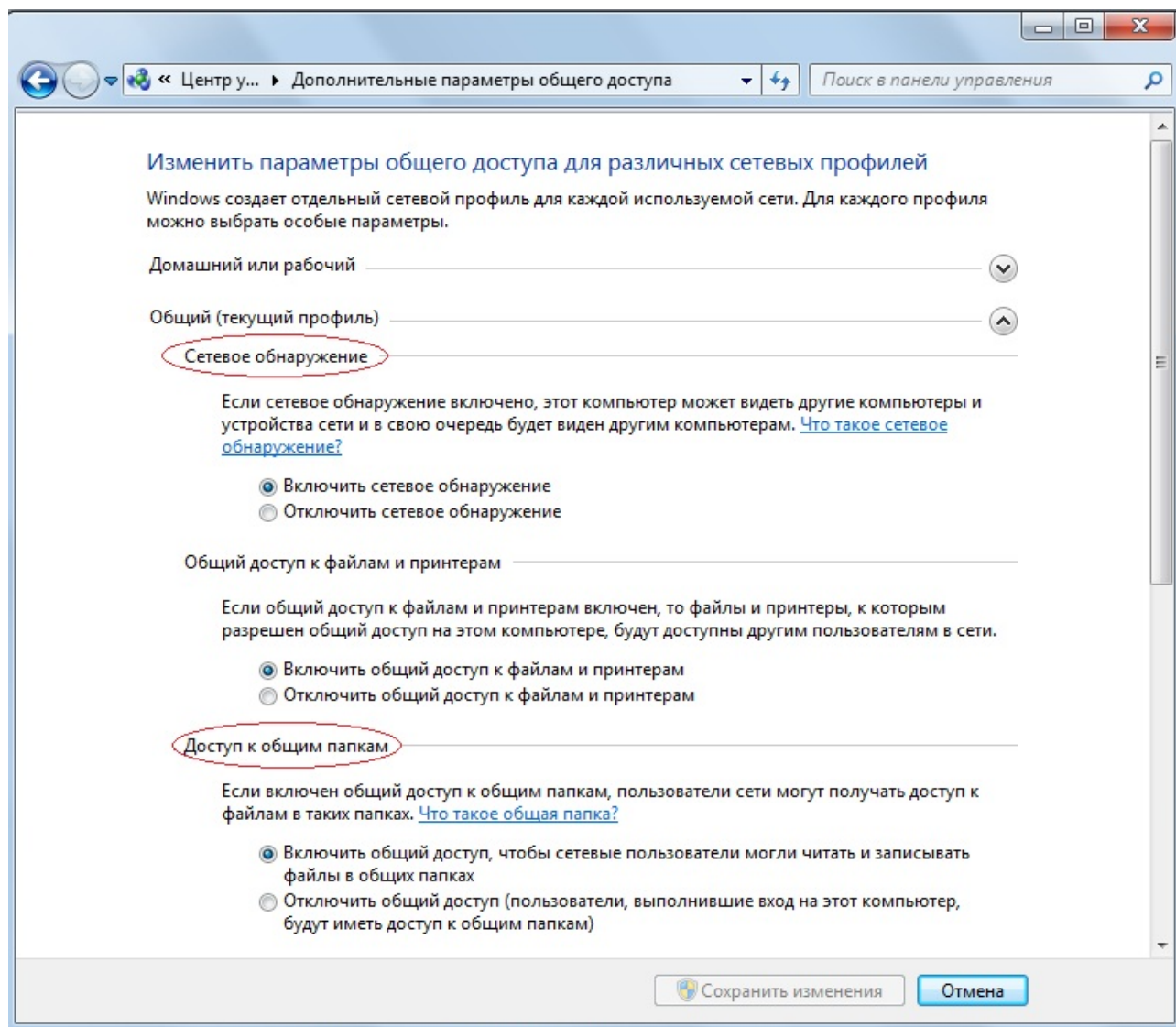


Рисунок 4.14 Включение опций

3. Отключите опцию *Общий доступ с парольной защитой*;

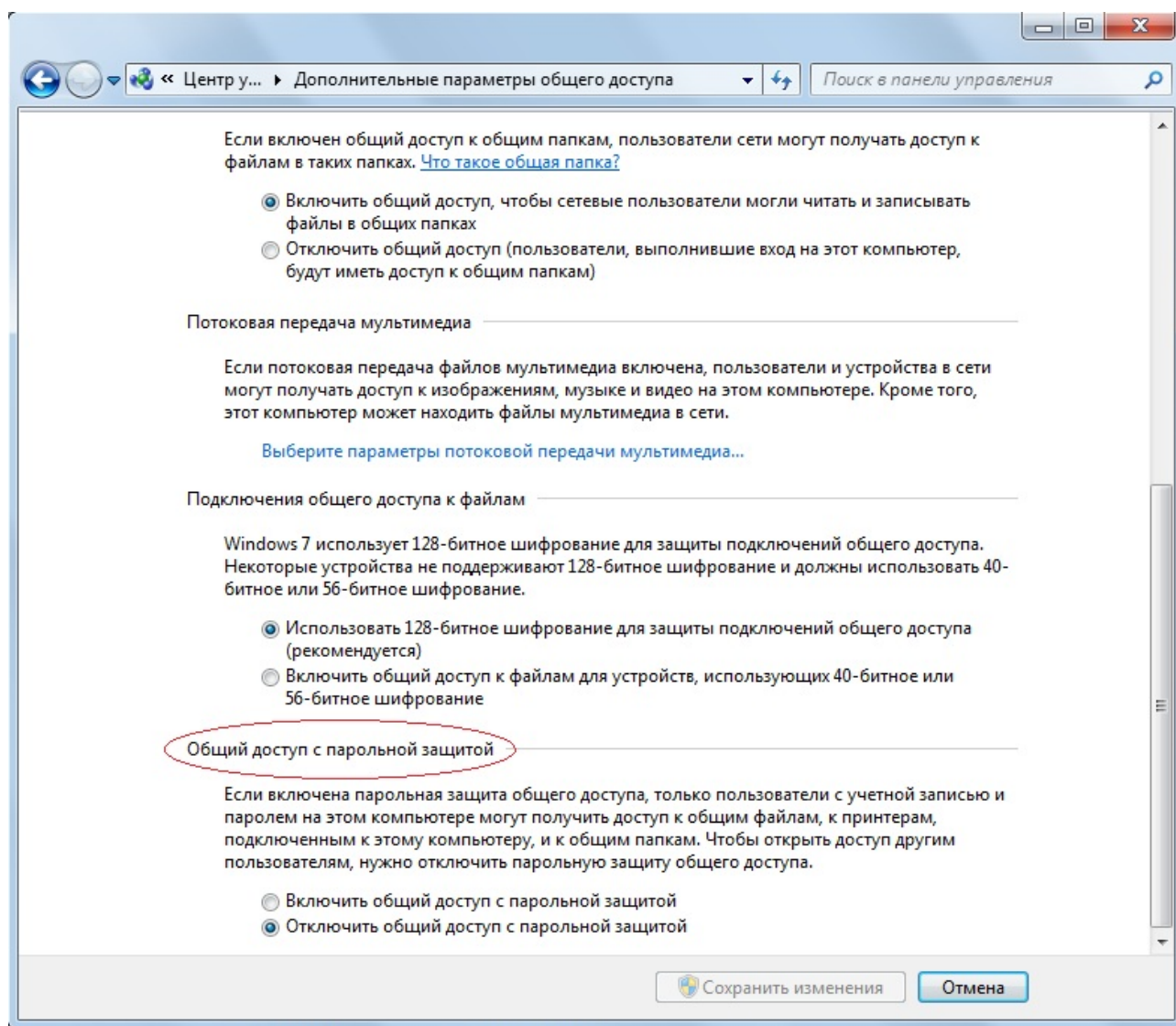


Рисунок 4.15 Отключение опций

4. Нажмите *Сохранить изменения*;

5. Создайте папку, которая будет применяться для обмена информацией по сети;

6. Вызовите контекстное меню созданной папки и выберите *Свойства*;

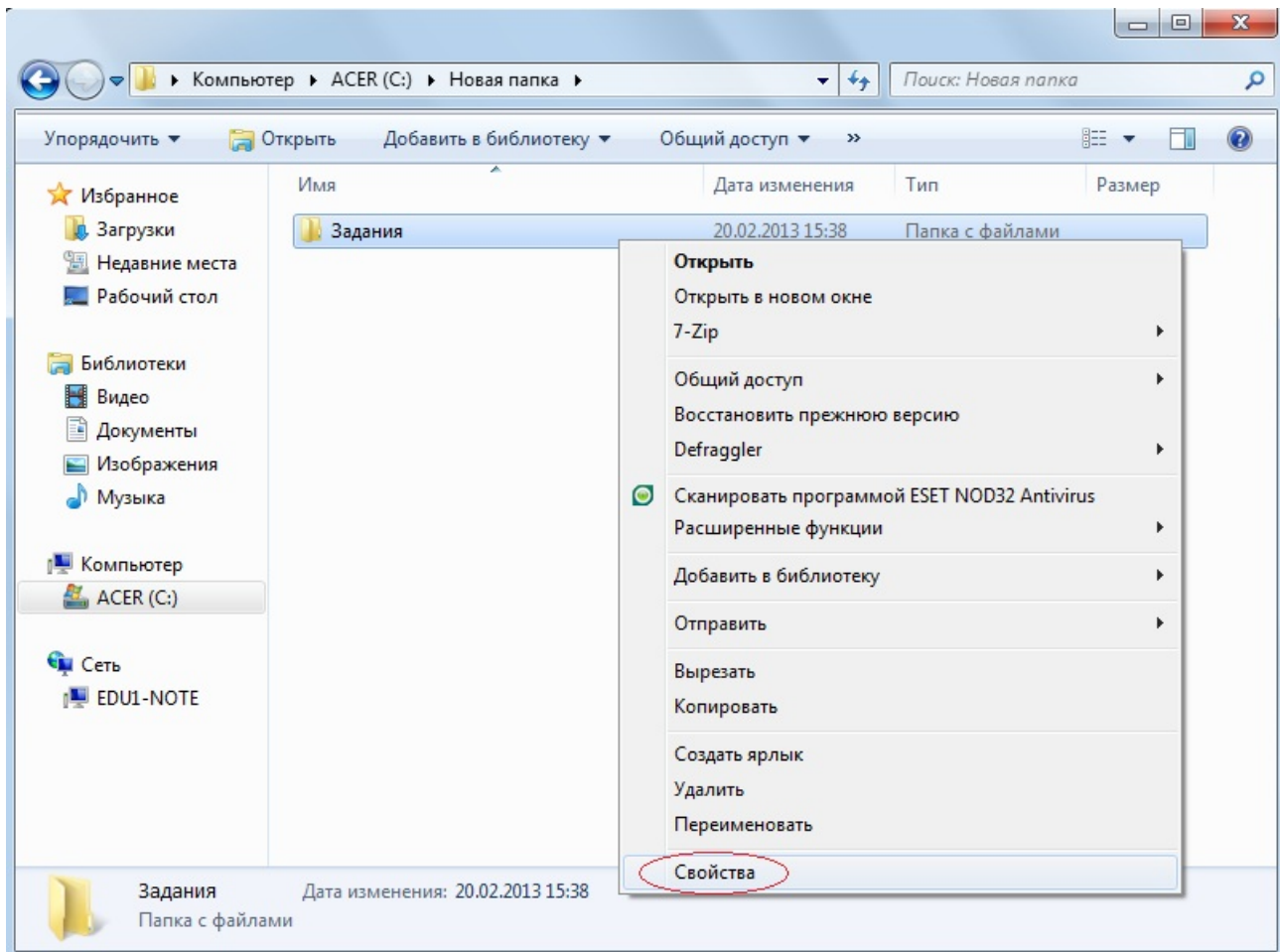


Рисунок 4.16

7. На вкладке *Доступ* нажмите на кнопку *Расширенная настройка*;

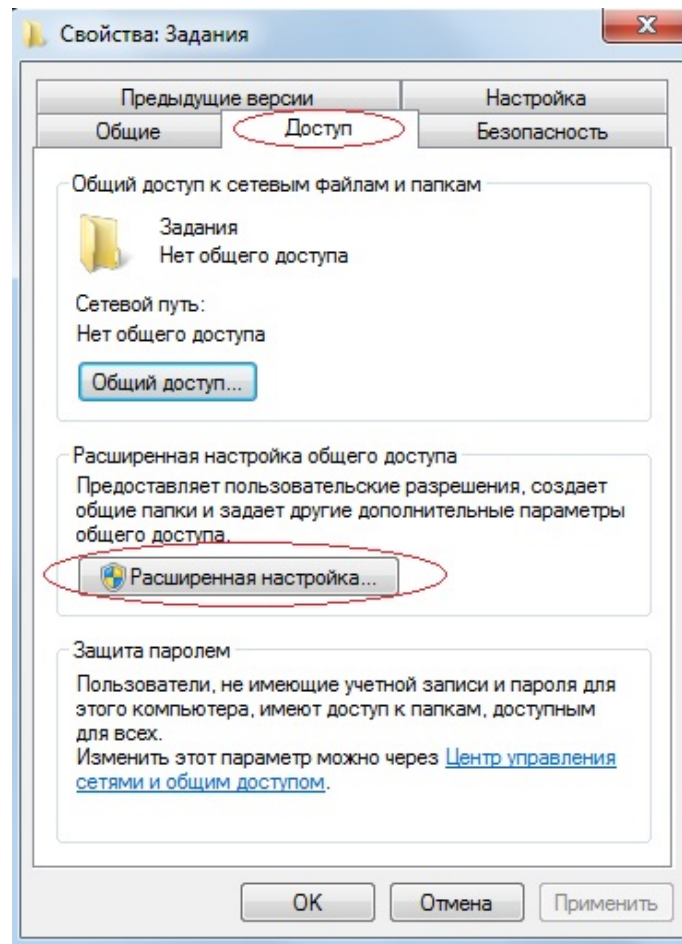


Рисунок 4.17

8. Установите галочку *Открыть общий доступ к этой папке* и нажмите на кнопку *Разрешения*;

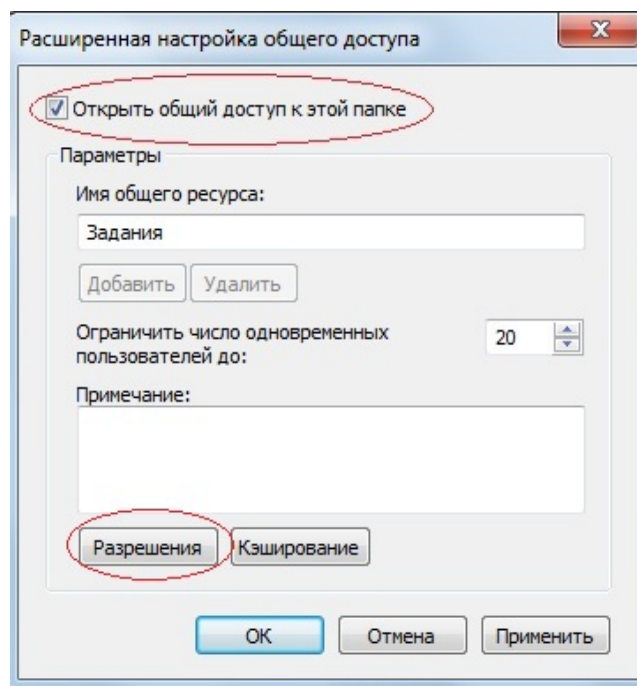


Рисунок 4.18

9. Установите галочку *Полный доступ* → *Разрешить*;

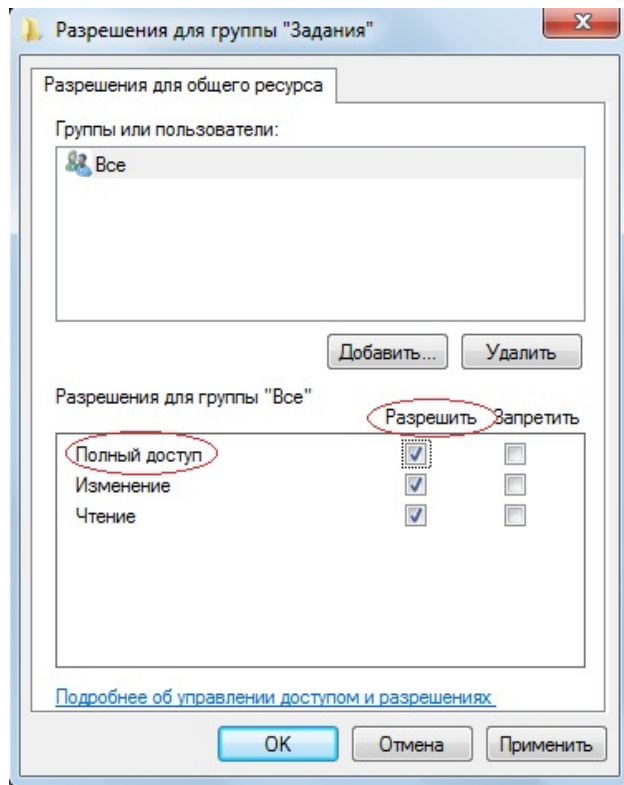


Рисунок 4.19

10. Нажмите кнопку *Ок*, чтобы вернуться во вкладку *Доступ*;

11. Во вкладке *Доступ* нажмите на кнопку *Общий доступ*.

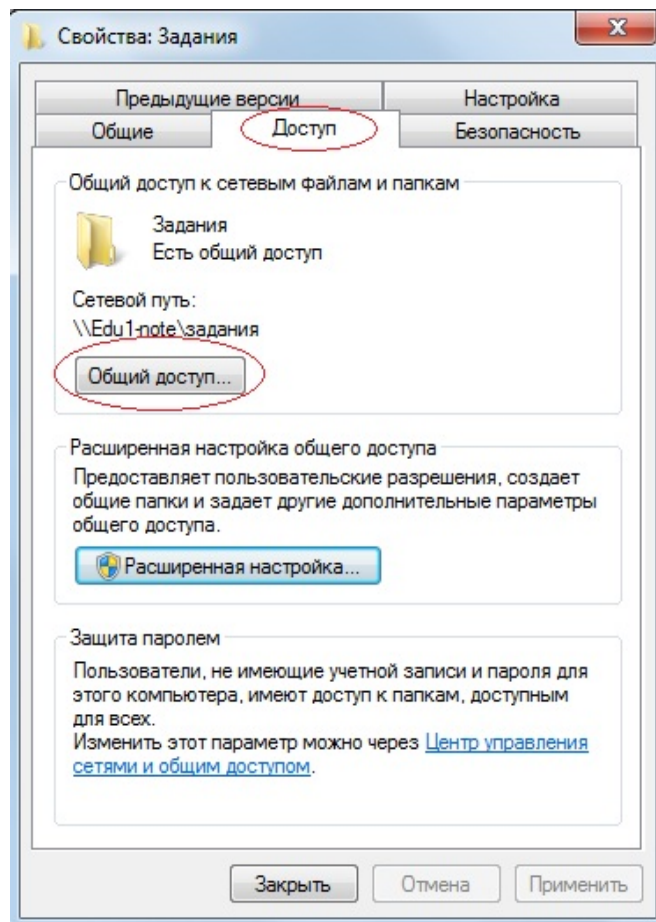


Рисунок 4.20

12. Из выпадающего меню выберите пользователей *Все* → *Добавить* → *Чтение и запись* (если предполагаются изменения в данной папке по сети другими пользователями);

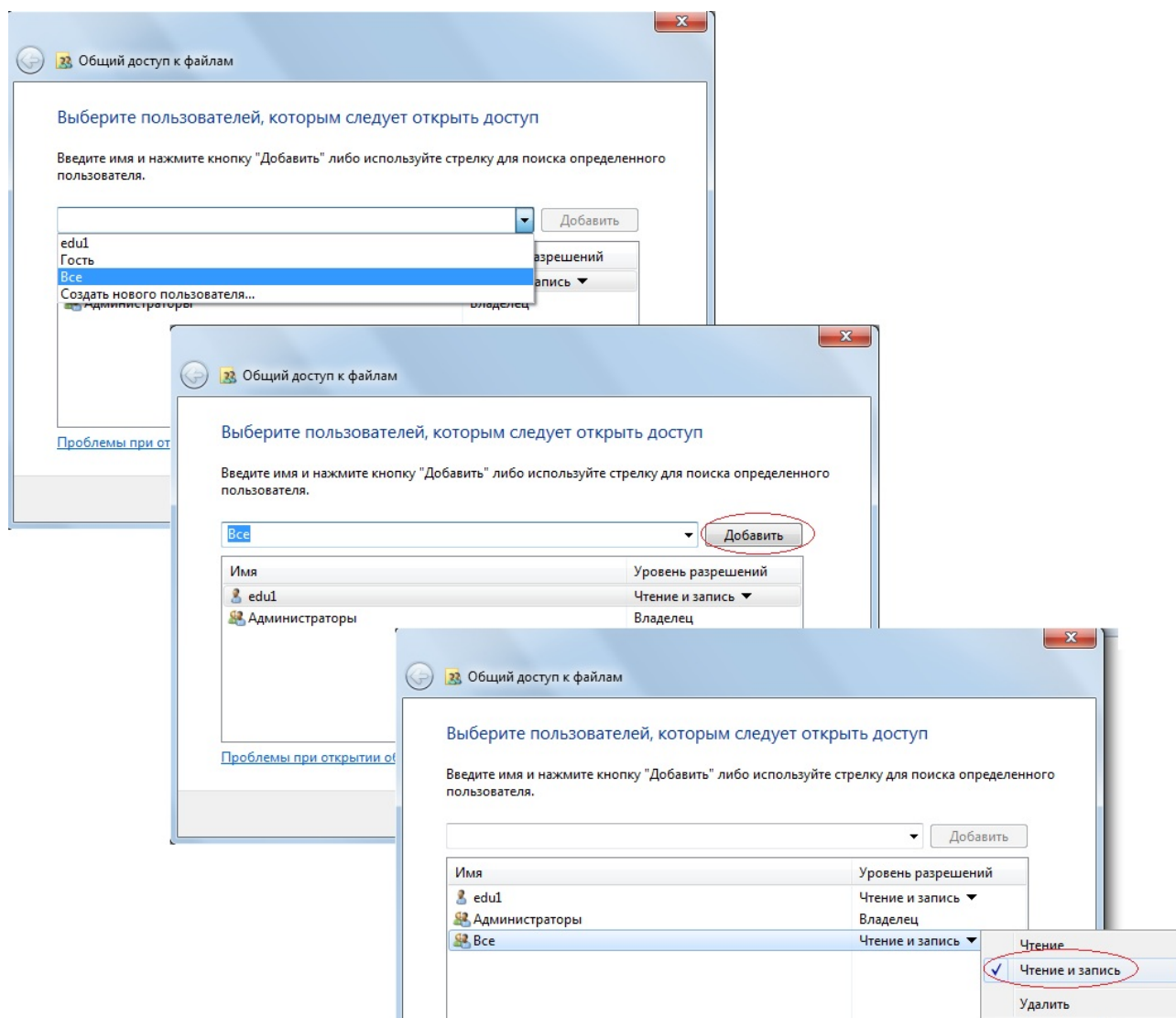


Рисунок 4.21

13. Нажмите *Общий доступ*;

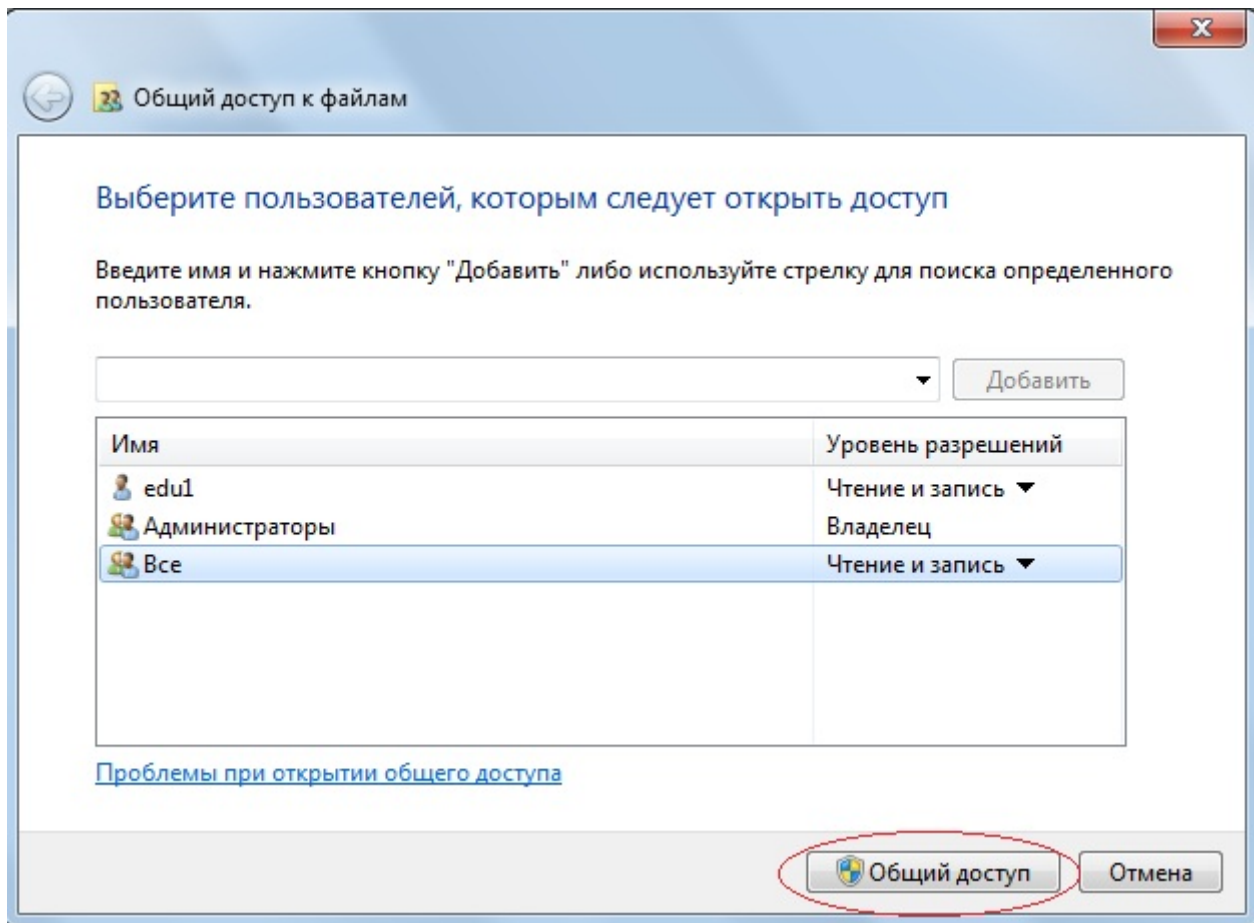


Рисунок 4.22

14. В данной сетевой папке создайте какой-либо документ.

Шаг 4. На рабочей станции ПК1 проверьте доступ к документам на рабочей станции ПК2, внесите изменения и сохраните.

1. Нажмите меню *Пуск* → *Мой компьютер*;
2. В адресной строке введите `\\192.168.1.2` и нажмите *Enter*

Шаг 5. На рабочей станции ПК2 проверьте доступ к документам на рабочей станции ПК1, внесите изменения и сохраните.

Лабораторная работа №5. Адресация канального уровня. MAC-адреса

Канальный уровень модели OSI обеспечивает передачу данных, полученных от вышележащего сетевого уровня, через физический уровень между непосредственно подключенными устройствами.

Функции канального уровня:

- управление доступом к среде передачи;
- физическая адресация (MAC-адреса);
- формирование кадров.

На канальном уровне данные рассматриваются как последовательный поток битов. Перед передачей по физическим каналам этот поток разделяется на небольшие части, каждая из которых снабжается заголовком, содержащим некоторую служебную информацию, т. е. формируется **кадр (frame)**.

В заголовке кадра присутствуют информационные поля, показанные в таблице 1.

Таблица 1

Поле, определяющее начало кадра	Адреса отправителя и получателя	Информация о протоколе сетевого уровня	Данные	Контрольная сумма	Поле, определяющее конец кадра
---------------------------------	---------------------------------	--	--------	-------------------	--------------------------------

Для обеспечения адресации узлов в сети в заголовке кадров должны присутствовать адрес отправителя и адрес получателя. Большинство протоколов канального уровня для идентификации устройств используют **MAC-адреса**.

MAC-адрес (Media Access Control) – это уникальный идентификатор, присваиваемый каждому сетевому устройству во время изготовления. Он позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу.

Обычно MAC-адрес состоит из 48 бит (6 октетов) и записывается в виде шестнадцатеричных цифр, разделенных тире или двоеточиями, например 20:6A:8A:72:A5:82. Структура MAC-адреса показана на рис. 5.1.

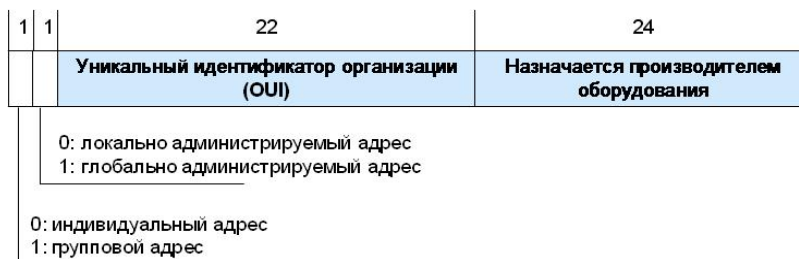


Рисунок 5.1 Структура MAC-адреса

Первый (младший) бит старшего байта определяет, является адрес индивидуальным или групповым:

- **Индивидуальный** — адрес, ассоциированный с определенным сетевым устройством;
- **Групповой** — адрес, ассоциированный с несколькими или всеми узлами данной сети.

Второй (младший) бит старшего байта определяет, является адрес глобально или локально администрируемым:

- **Глобально администрируемый адрес** глобально уникален и обычно «зашит» в аппаратуру;
- **Локально администрируемый адрес** выбирается произвольно и может содержать информацию об OUI.

В данной лабораторной работе для анализа трафика, передаваемого между рабочими станциями, будет использоваться программа **Wireshark**.

Wireshark – бесплатная программа, которая является анализатором трафика

Шаг 6. Запустите на рабочей станции ПК1 анализатор протоколов Wireshark. Интерфейс программы представлен на рис. 5.3.

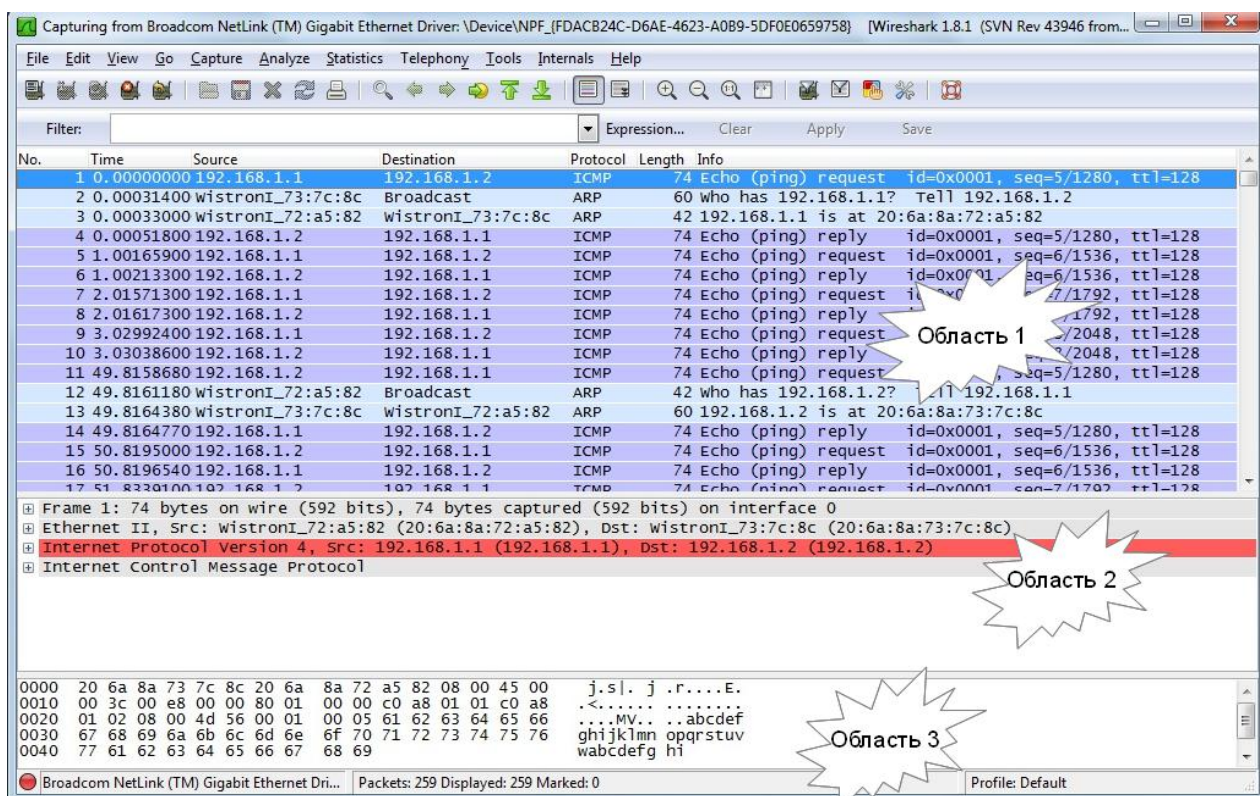


Рисунок 5.3 Интерфейс программы Wireshark

Окно Wireshark включает в себя 3 области просмотра с различными уровнями детализации. Область 1 содержит список всех захваченных кадров, организованный в виде таблицы с заголовками. Если выделить строку, то более подробная информация о кадре и ее расшифровка будут отображены в области 2. Область 3 содержит код кадра в шестнадцатеричном или текстовом представлении.

Чтобы начать перехват трафика, нужно выбрать правильный сетевой интерфейс, с которого будет выполняться перехват. Для этого выберите пункт главного меню *Capture* → *Interfaces* или нажмите кнопку на верхней панели инструментов *List the available capture interfaces* (рис. 5.4).

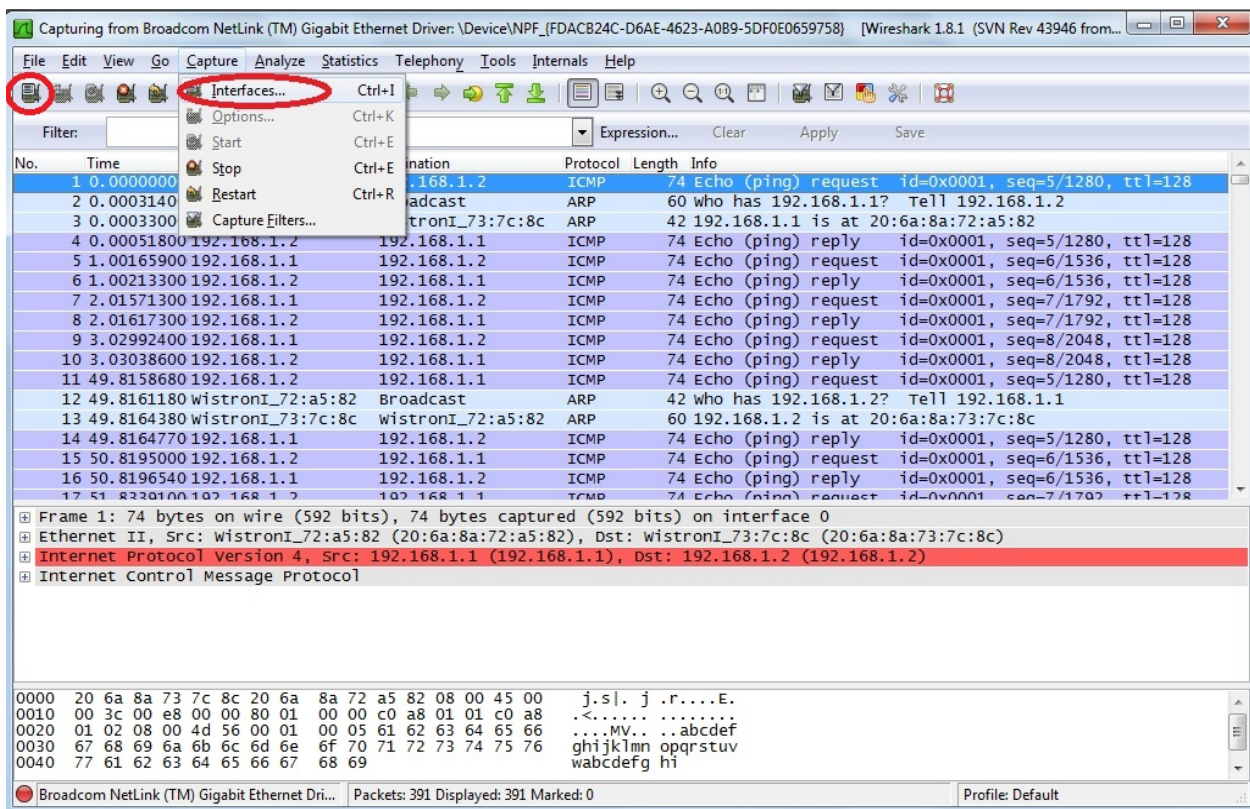


Рисунок 5.4 Выбор сетевого интерфейса для перехвата трафика

После этого на экране появится окно со списком сетевых интерфейсов, доступных системе (рис. 5.5).

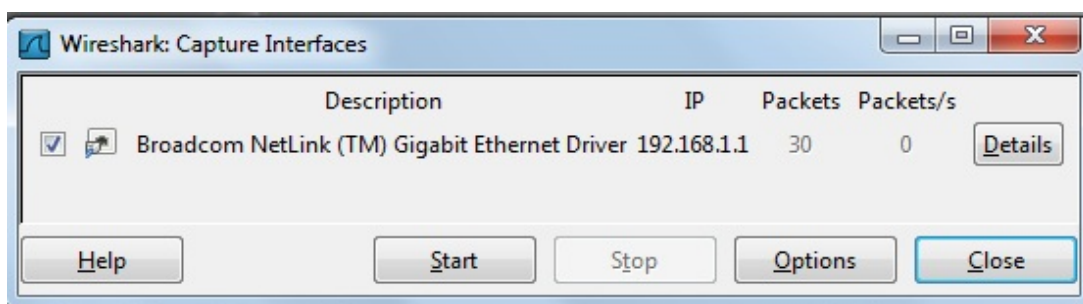


Рисунок 5.5 Сетевой интерфейс, доступный системе

Выберите сетевой интерфейс и нажмите кнопку *Start*.

Шаг 7. Запустите на рабочей станции ПК2 анализатор протоколов Wireshark.

ЗАДАНИЕ

Захватите и проанализируйте пакеты с помощью анализатора протоколов Wireshark.

Шаг 8. Выполните тестирование соединения между ПК1 и ПК2, и наоборот командой `ping`.

В командной строке ПК1 введите: `ping 192.168.1.2`

В командной строке ПК2 введите: `ping 192.168.1.1`

Наблюдаете ли вы трафик, передаваемый между ПК1 и ПК2 в окне Wireshark? _____

Шаг 9. Утилита ping работает по протоколу ICMP. Чтобы в окне Wireshark отображались только пакеты протокола ICMP, установите фильтр *Filter* → *ICMP* и нажмите *Apply* (рис. 5.6).

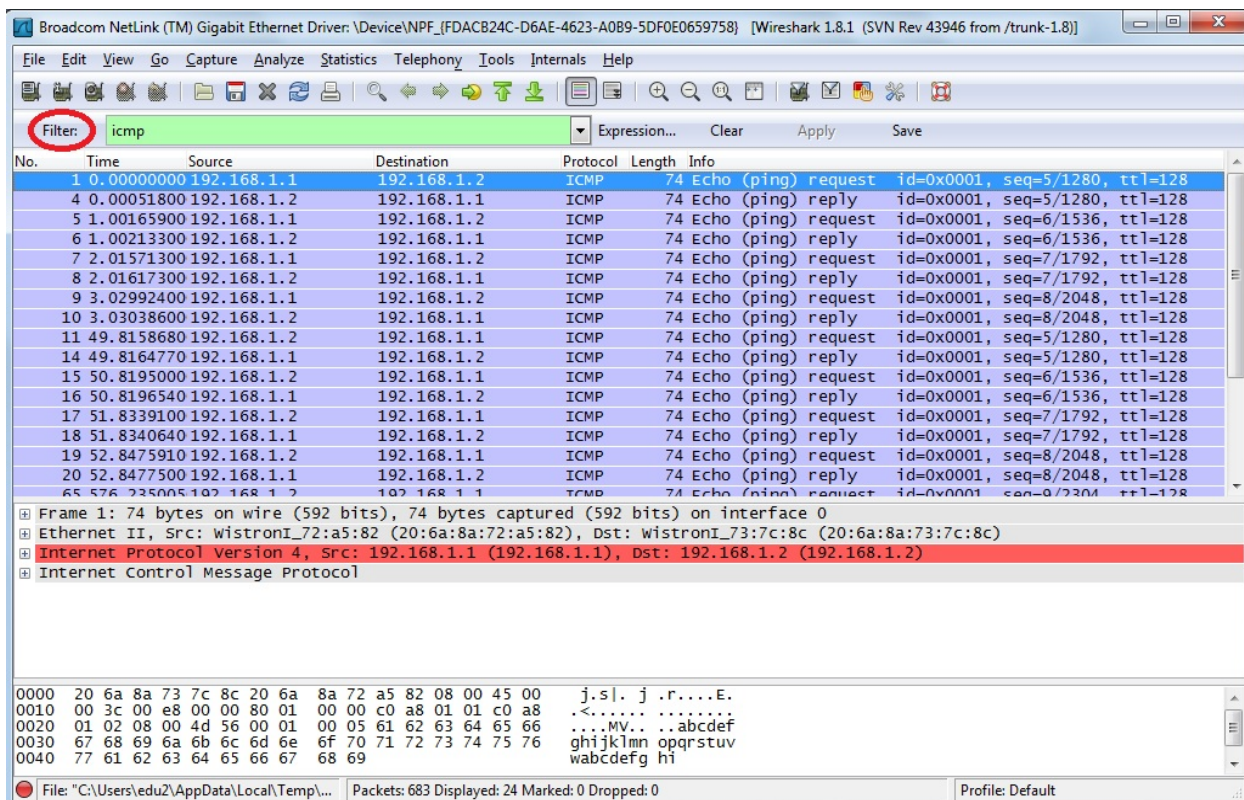


Рисунок 5.6 Установка фильтра

Шаг 10. Остановите захват трафика. Для этого нажмите кнопку на верхней панели инструментов *Stop the running live capture* (рис. 5.7).

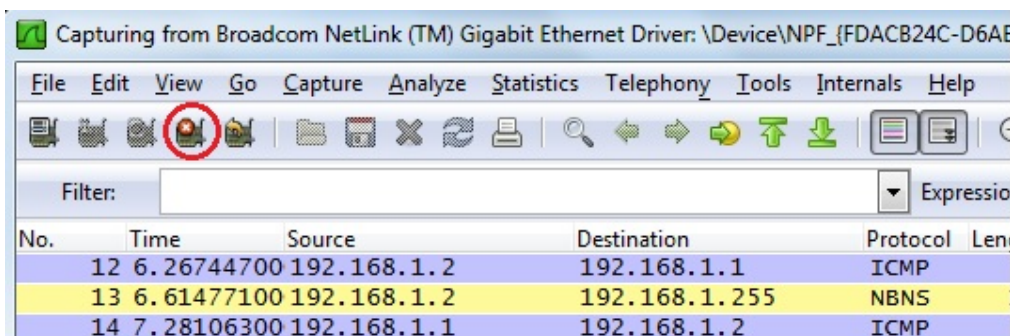


Рисунок 5.7 Остановка захвата трафика

Шаг 11. Проанализируйте захваченный трафик. Выберите один пакет ICMP из области 1, в области 2 появится подробная информация о кадре и ее расшифровка.

Шаг 12. В области 2 разверните информацию для кадра *Ethernet II* (рис. 5.8).

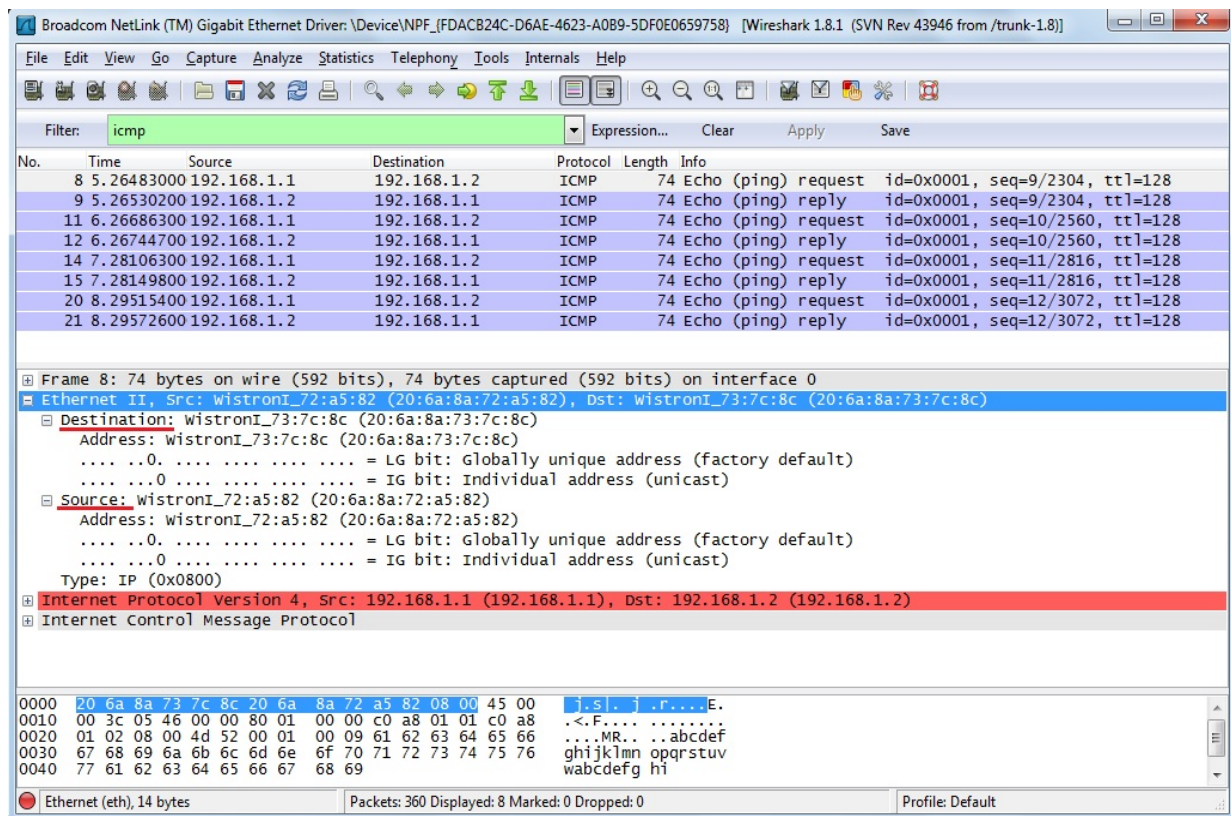


Рисунок 5.8 Детализация кадра Ethernet II

Чему равен MAC-адрес отправителя пакета? _____

Чему равен MAC-адрес получателя пакета? _____

Шаг 13. Измените MAC-адрес на рабочей станции ПК1 и ПК2.

Новый MAC-адрес ПК1 — 08-00-27-3F-B6-0B

Новый MAC-адрес ПК2 — 09-00-27-3F-B6-0C

Чтобы изменить MAC-адрес в Windows XP, выполните следующие действия:

1. Откройте *Сетевые подключения*;

Пуск → Панель управления → Сетевые подключения

2. Щелкните правой кнопкой мыши на *Подключение по локальной сети* и выберите *Свойства*;

3. В свойствах подключения нажмите на кнопку *Настроить*. Откроется окно настроек сетевой карты (рис. 5.9);

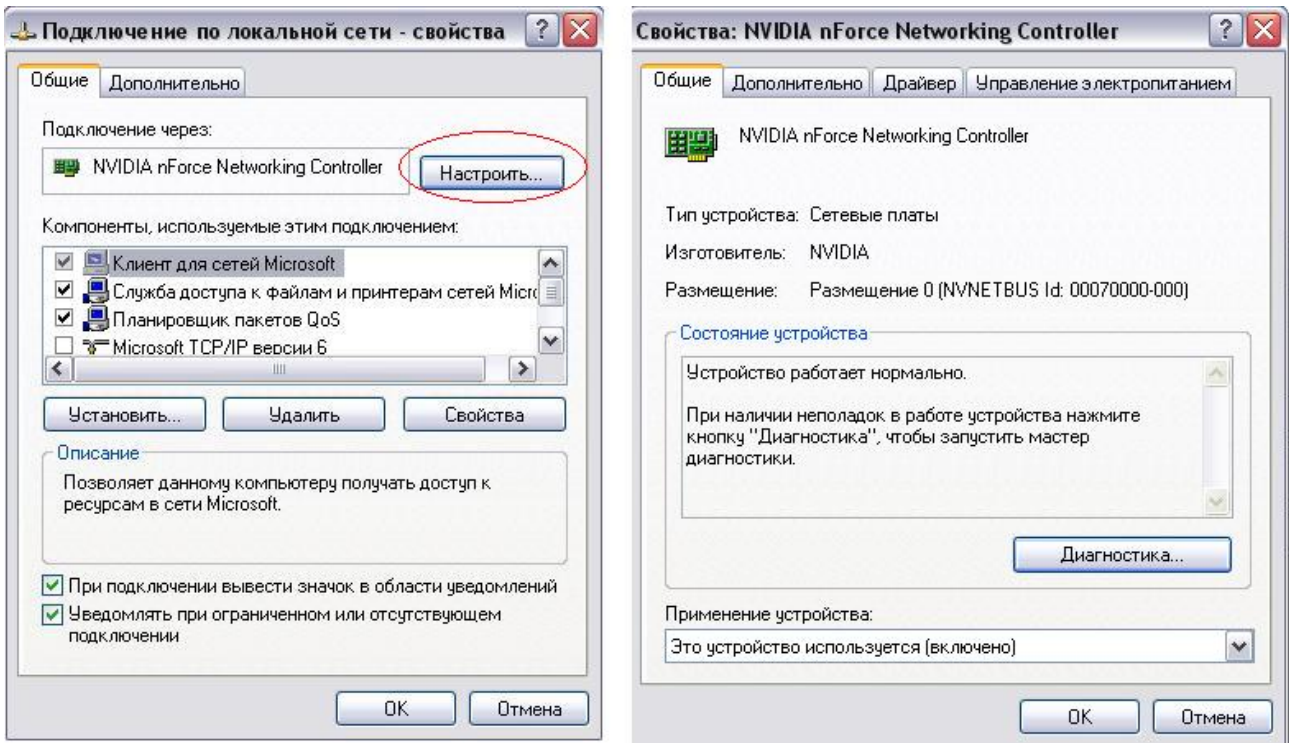


Рисунок 5.9 Настройка сетевой карты

4. Откройте вкладку *Дополнительно* и выберите один из пунктов: *Сетевой адрес* или *Network Address*;

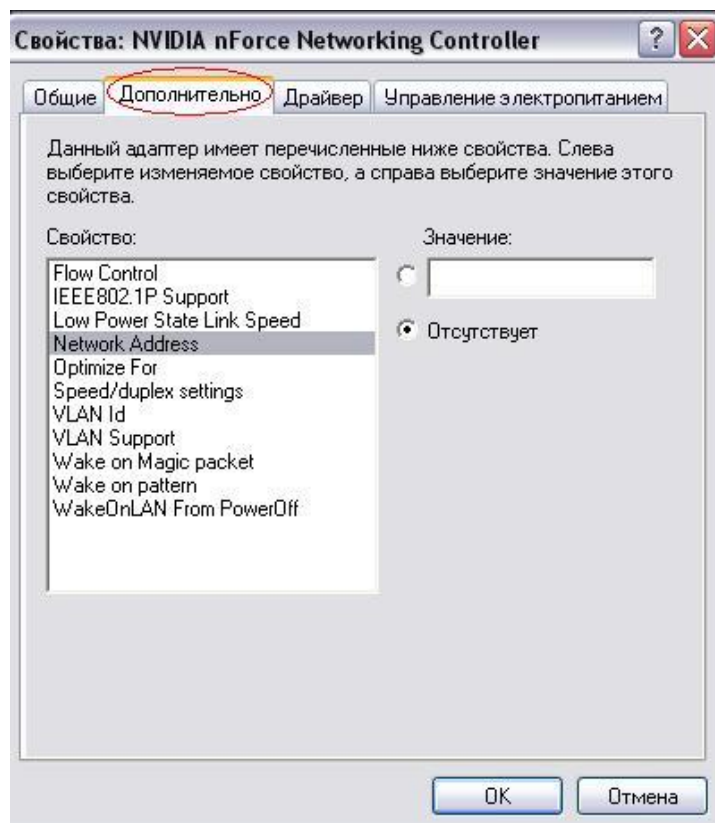


Рисунок 5.10

5. В правой части окна установите галочку напротив строки *Значение* и впишите 12 символов нового значения MAC-адреса (без пробелов);

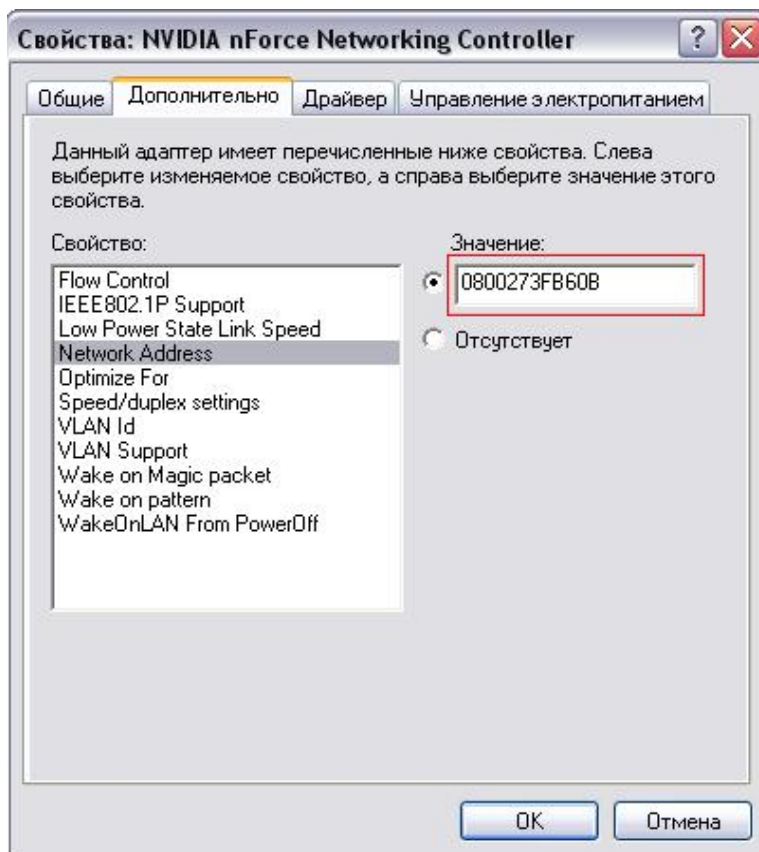


Рисунок 5.11 Настройка нового MAC-адреса

6. Нажмите кнопку *Ок*;
7. Перезагрузите ПК.

Чтобы изменить MAC-адрес в Windows 7/Vista, выполните следующие действия:

1. Откройте *Изменение параметров адаптера*;

Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера

2. Щелкните правой кнопкой мыши на *Подключение по локальной сети* и выберите *Свойства* (рис. 5.12);

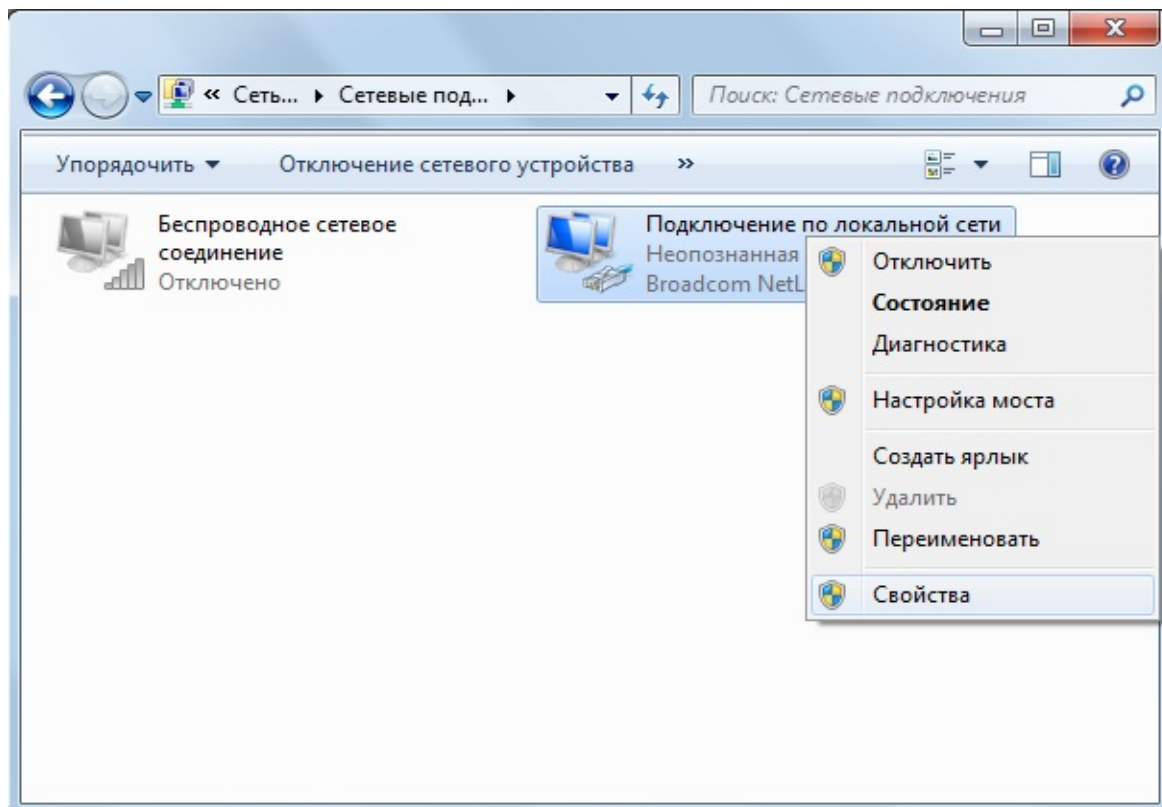


Рисунок 5.12

3. В свойствах подключения нажмите на кнопку *Настроить*. Откроется окно настроек сетевой карты;

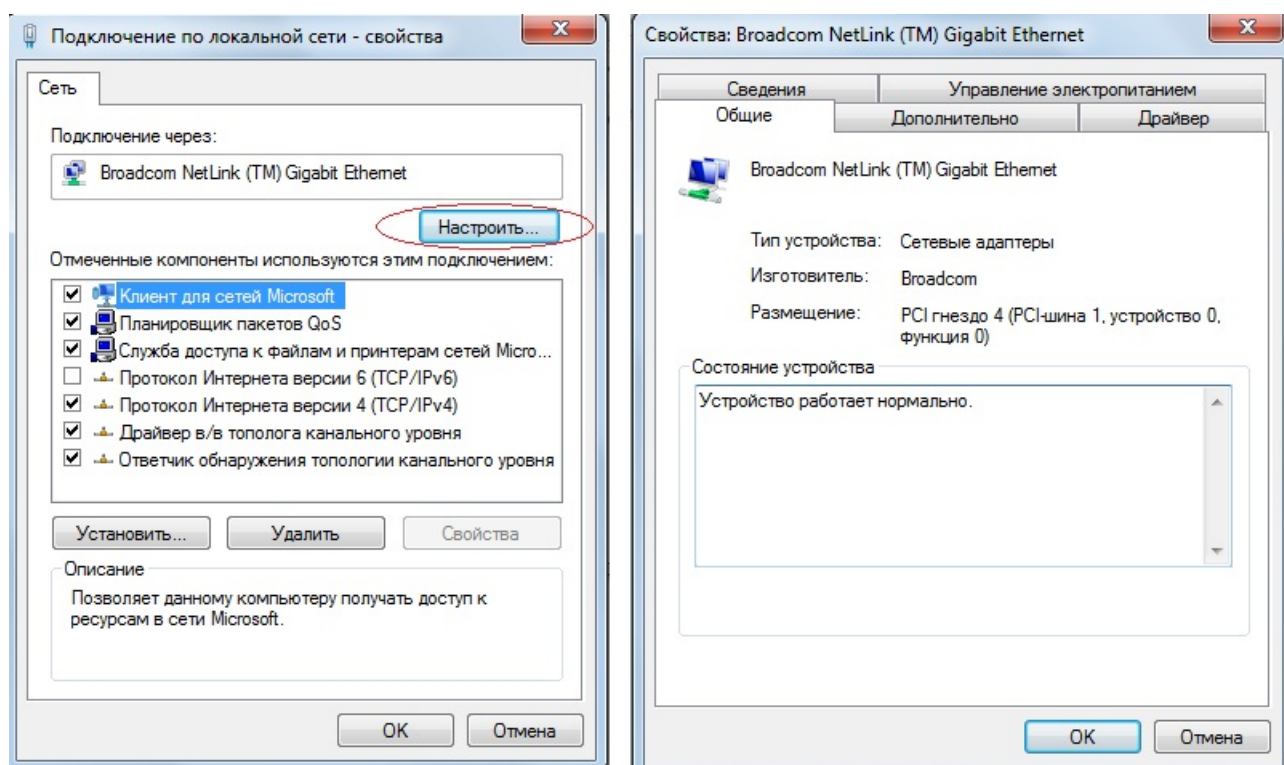


Рисунок 5.13

4. Откройте вкладку *Дополнительно* и выберите один из пунктов: *Сетевой адрес*, *Network Address*, *Локально администрируемый адрес* или *Locally Administered Address*;

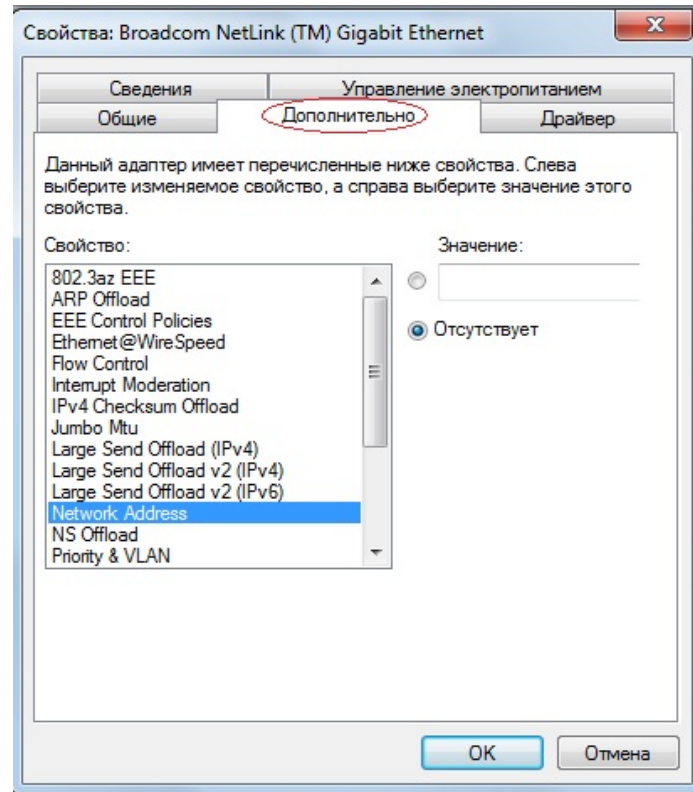


Рисунок 5.14

5. В правой части окна установите галочку напротив строки *Значение* и впишите 12 символов нового значения MAC-адреса (без пробелов);

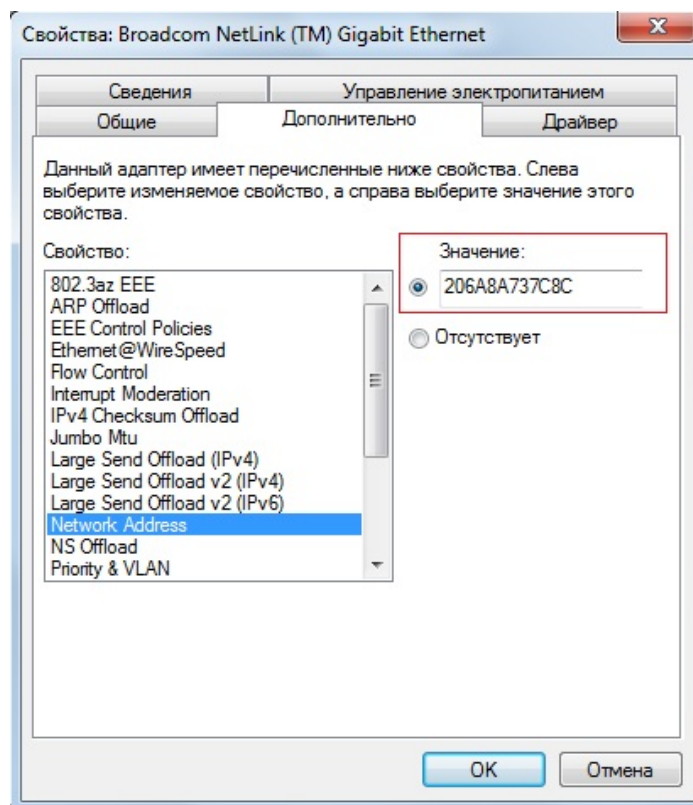


Рисунок 5.15

- 6. Нажмите кнопку *Ок*;
- 7. Перезагрузите ПК.

Шаг 14. Проверьте, изменился ли MAC-адрес ПК1. В командной строке введите: `getmac`

Шаг 15. Проверьте, изменился ли MAC-адрес ПК2. В командной строке введите: `getmac`

Шаг 16. Повторите шаг 7 — шаг 12.

Чему теперь равен MAC-адрес отправителя пакета? _____

Чему теперь равен MAC-адрес получателя пакета? _____

Шаг 17. Верните первоначальный MAC-адрес на рабочей станции ПК1 и ПК2.

Лабораторная работа №6. Создание коммутируемой сети

Коммутатор (switch) — основное активное сетевое оборудование современных локальных сетей. В отличие от концентратора, коммутатор работает на канальном уровне модели OSI и передает кадры не на все порты, а непосредственно получателю, анализируя MAC-адрес источника/назначения.

Передача кадров коммутатором осуществляется на основе *таблицы коммутации*. Каждая запись в таблице коммутации состоит из номера порта и MAC-адреса. Как создаются записи в таблице коммутации? Например, если на порт 1 коммутатора поступает кадр от рабочей станции ПК1, то в таблице создается запись, ассоциирующая MAC-адрес рабочей станции ПК1 с номером входного порта. Таблица коммутации может строиться коммутатором автоматически, на основе динамического изучения MAC-адресов источников поступающих на порты кадров, или создаваться вручную администратором сети.

Для группировки сетевых пользователей в виртуальные рабочие группы используется *виртуальная локальная сеть (Virtual LAN, VLAN)*. Виртуальной локальной сетью называется логическая группа узлов сети, трафик которой, в том числе и широкоэвещательный, на канальном уровне полностью изолирован от других узлов сети.

В коммутаторах могут быть реализованы следующие типы VLAN:

- на основе портов (Port-based VLAN);
- на основе стандарта IEEE 802.1Q;
- на основе MAC-адресов;
- на основе стандарта IEEE 802.1ad (Q-in-Q VLAN);
- на основе портов и протоколов IEEE 802.1v.

В данной лабораторной работе будет показана настройка VLAN на основе портов.

Основные характеристики VLAN на основе портов:

- применяются в пределах одного коммутатора;
- простота настройки;
- каждый порт может входить только в одну VLAN.

Оборудование (на 1 рабочее место):

Рабочая станция	2 шт.
Коммутатор DES-1100-16	1 шт.
Кабель Ethernet	2 шт.

Цель: изучить таблицу коммутации, Web-интерфейс коммутатора D-Link и понять технологию VLAN.

6.1 Управление коммутатором через Web-интерфейс и изучение таблицы коммутации

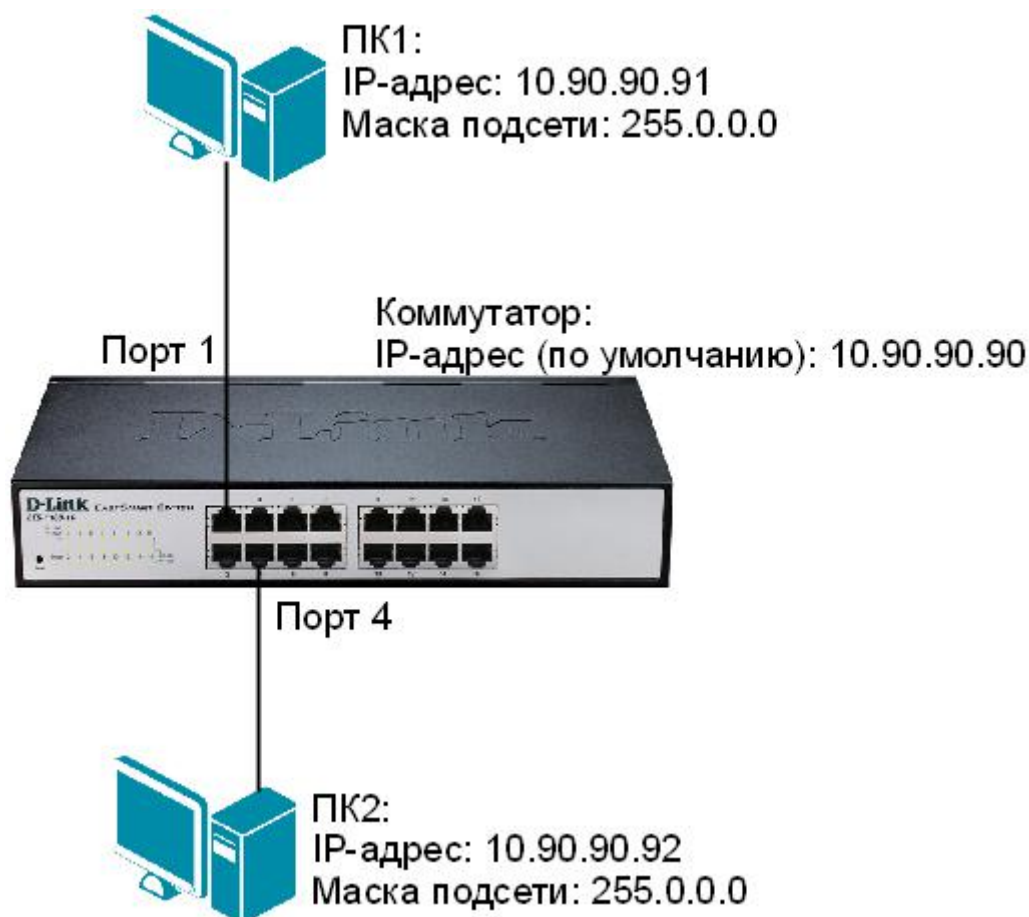


Рисунок 6.1 Схема сети

Шаг 1. Подключите ПК1 и ПК2 к коммутатору, как показано на рис. 6.1.

Шаг 2. Настройте на рабочей станции ПК1 и ПК2 статический IP-адрес в соответствии со схемой.

Шаг 3. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1 введите: `ping 10.90.90.92`

В командной строке ПК2 введите: `ping 10.90.90.91`

Шаг 4. Зайдите на Web-интерфейс коммутатора.

Чтобы зайти на Web-интерфейс коммутатора, выполните следующие действия:

1. На рабочей станции ПК1 запустите Web-браузер (Internet Explorer, Mozilla Firefox), в адресной строке которого укажите IP-адрес интерфейса управления коммутатора по умолчанию:

`http://10.90.90.90`

Внимание: IP-адрес управления коммутатора по умолчанию обычно указывается в руководстве пользователя. Для коммутатора D-Link DES-1100-16 IP-адрес управления по умолчанию — 10.90.90.90

2. В появившемся окне аутентификации, в поле *Password* введите *admin* и нажмите кнопку *Ок* (рис. 6.2).

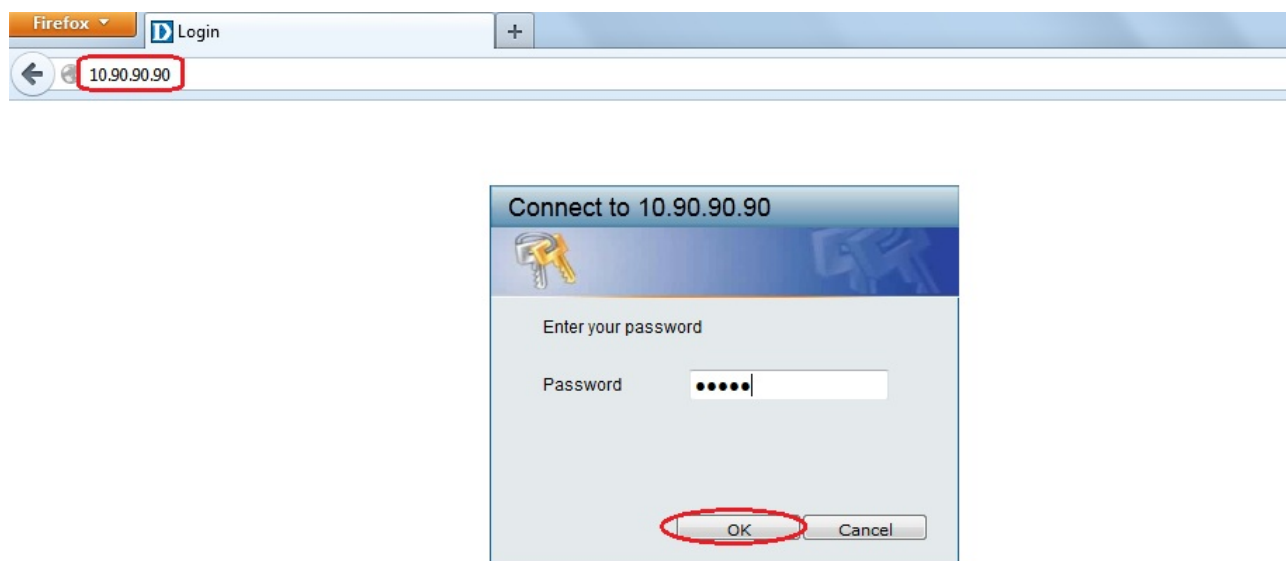


Рисунок 6.2 Окно аутентификации

3. После нажатия кнопки *Ок* появится окно Web-интерфейса управления коммутатора (рис. 6.3).

Внимание: Если на рабочей станции произведены настройки прокси-сервера, то их нужно отключить.

Для Mozilla Firefox: меню *Инструменты* → *Настройки* → *Дополнительные*. Далее вкладка *Сеть* → *Настройка параметров соединения Firefox с Интернетом* → *Настроить* → *Без прокси*.

Для Internet Explorer: меню *Сервис* → *Свойство обозревателя*. Далее вкладка *Подключения* → *Настройка сети* → *Автоматическое определение параметров*.

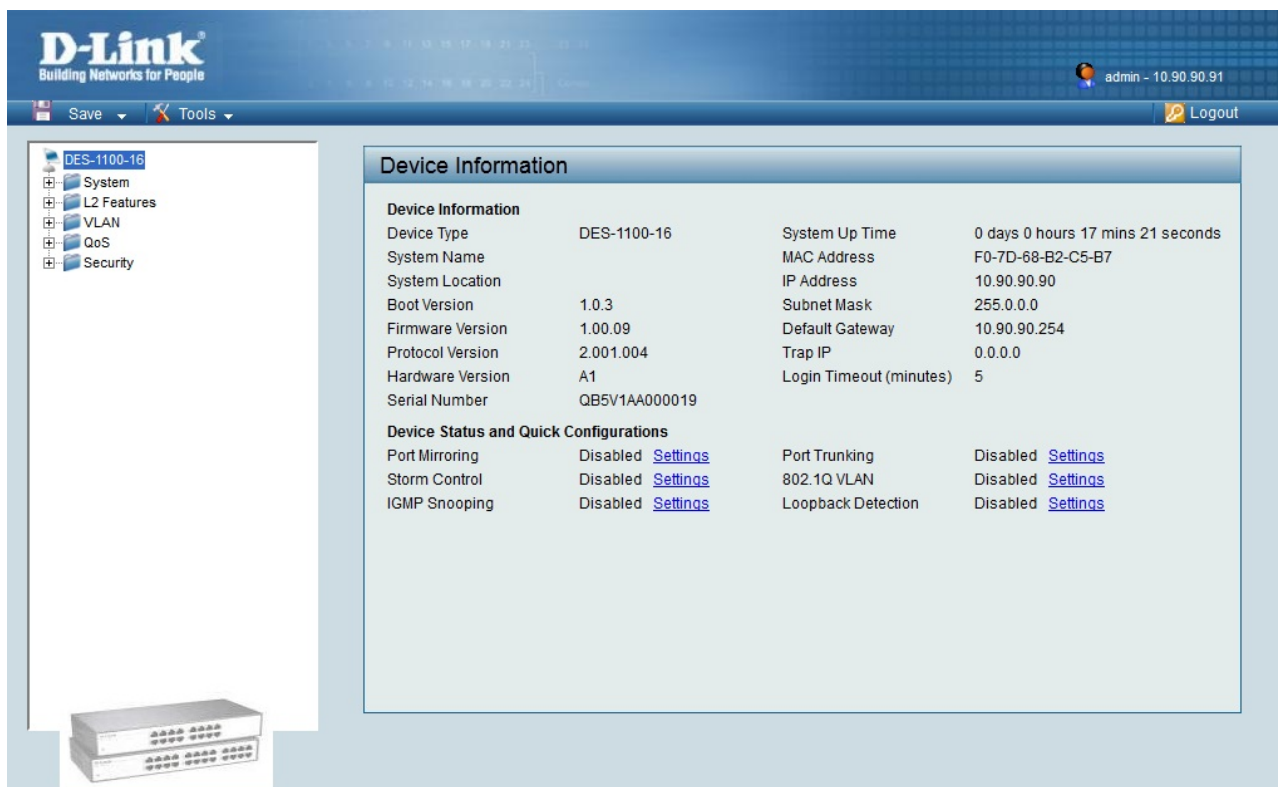


Рисунок 6.3 Web-интерфейс управления коммутатора DES-1100-16

В левой части Web-интерфейса расположены папки, объединяющие семейство функций, предназначенных для выполнения той или иной задачи. Например, в папке *System* находятся функции, предназначенные для базовой конфигурации коммутатора, включая настройку IP-адреса управления, конфигурации портов и т. д. Если щелкнуть кнопкой мыши по одной из папок и выбрать необходимую функцию, то в правой части Web-интерфейса появится окно для ввода и/или выбора данных.

Шаг 5. Посмотрите содержимое таблицы коммутации. В левой части окна выберите *Security* → *MAC Address Table* → *Dynamic Forwarding Table* (рис. 6.4).

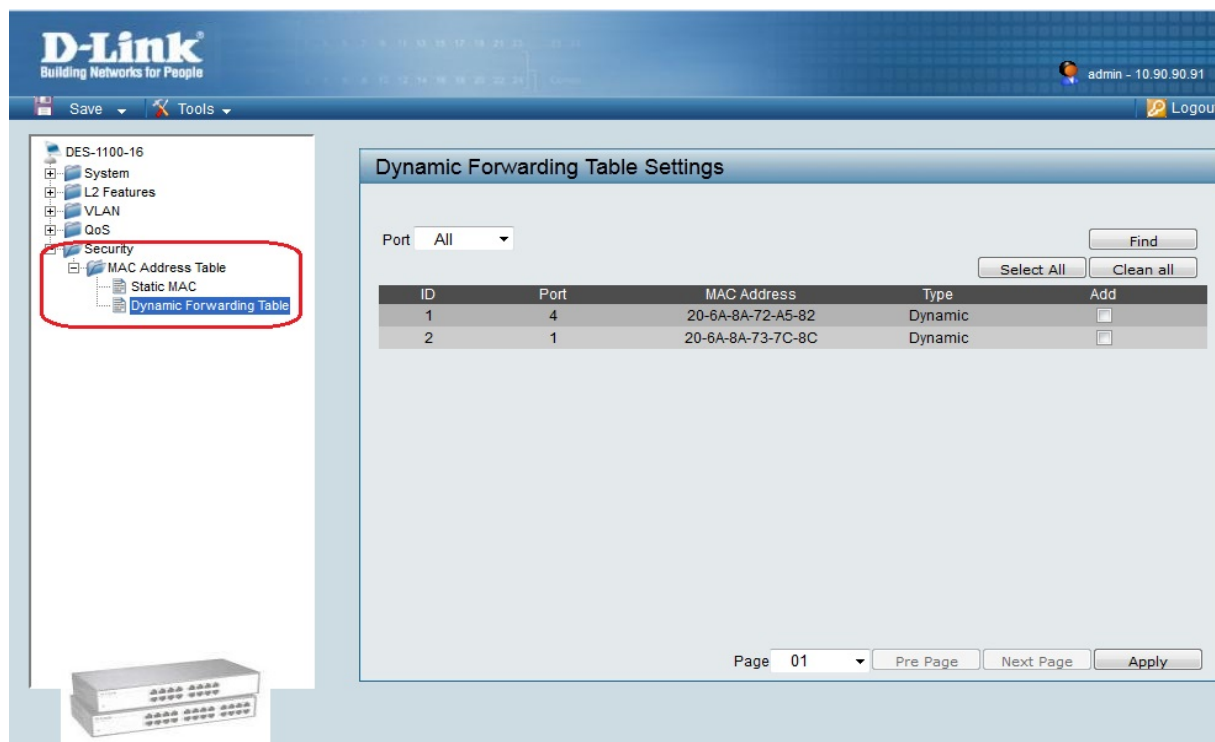


Рисунок 6.4 Таблица коммутации. Динамически изученные MAC-адреса

Сколько записей наблюдаете? _____

Какой тип (Type) у каждой записи в таблице коммутации? _____

Шаг 6. Отключите рабочую станцию ПК2 от 4 порта и подключите к 5 порту.

Шаг 7. Посмотрите содержимое таблицы коммутации. Что изменилось? _____

Шаг 8. Создайте статическую запись в таблице коммутации для ПК2 на порту 5. Для этого выберите *Security* → *MAC Address Table* → *Static MAC* и нажмите на кнопку *Add MAC* (рис. 6.5).

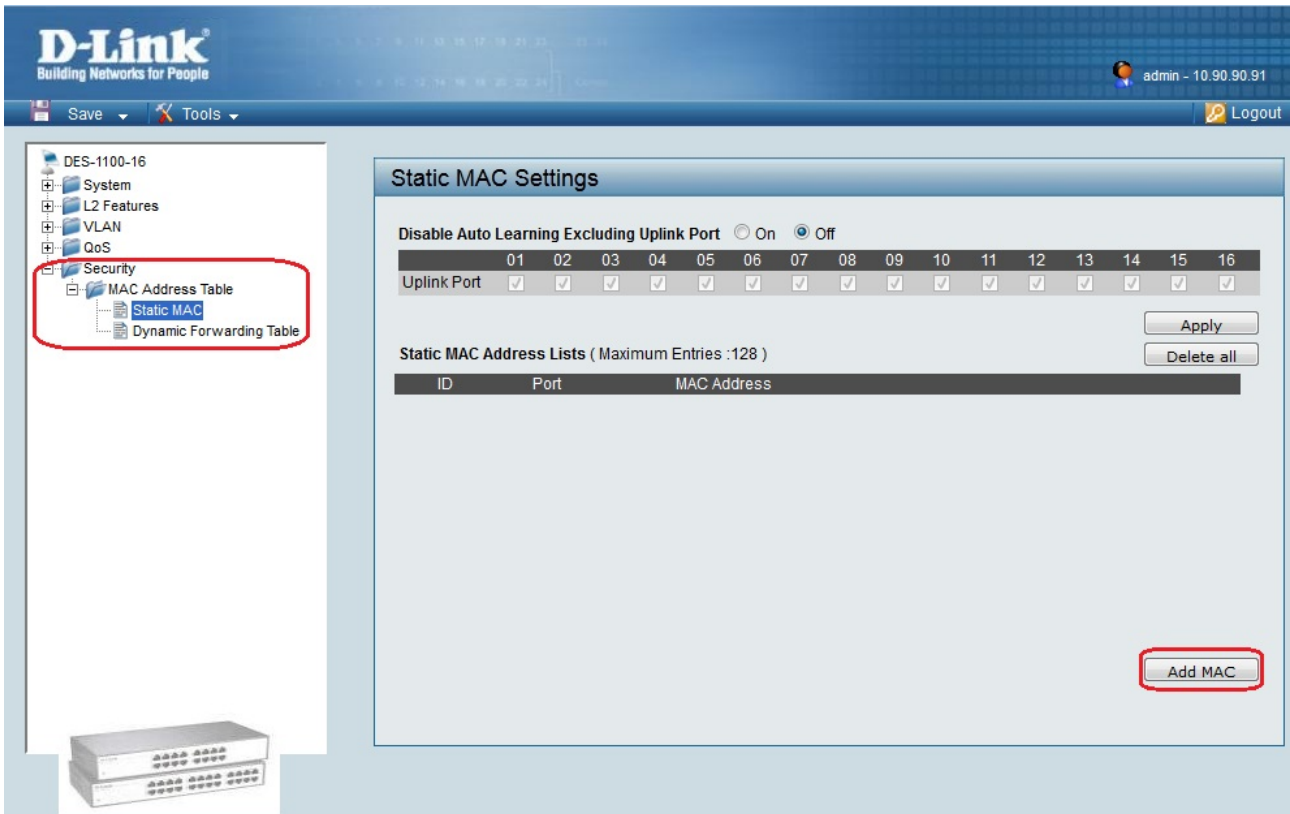


Рисунок 6.5 Создание статической записи

Шаг 9. Из выпадающего меню *Port* выберите 5, в поле *MAC Address* введите реальный MAC-адрес ПК2 и нажмите кнопку *Apply* (рис. 6.6).

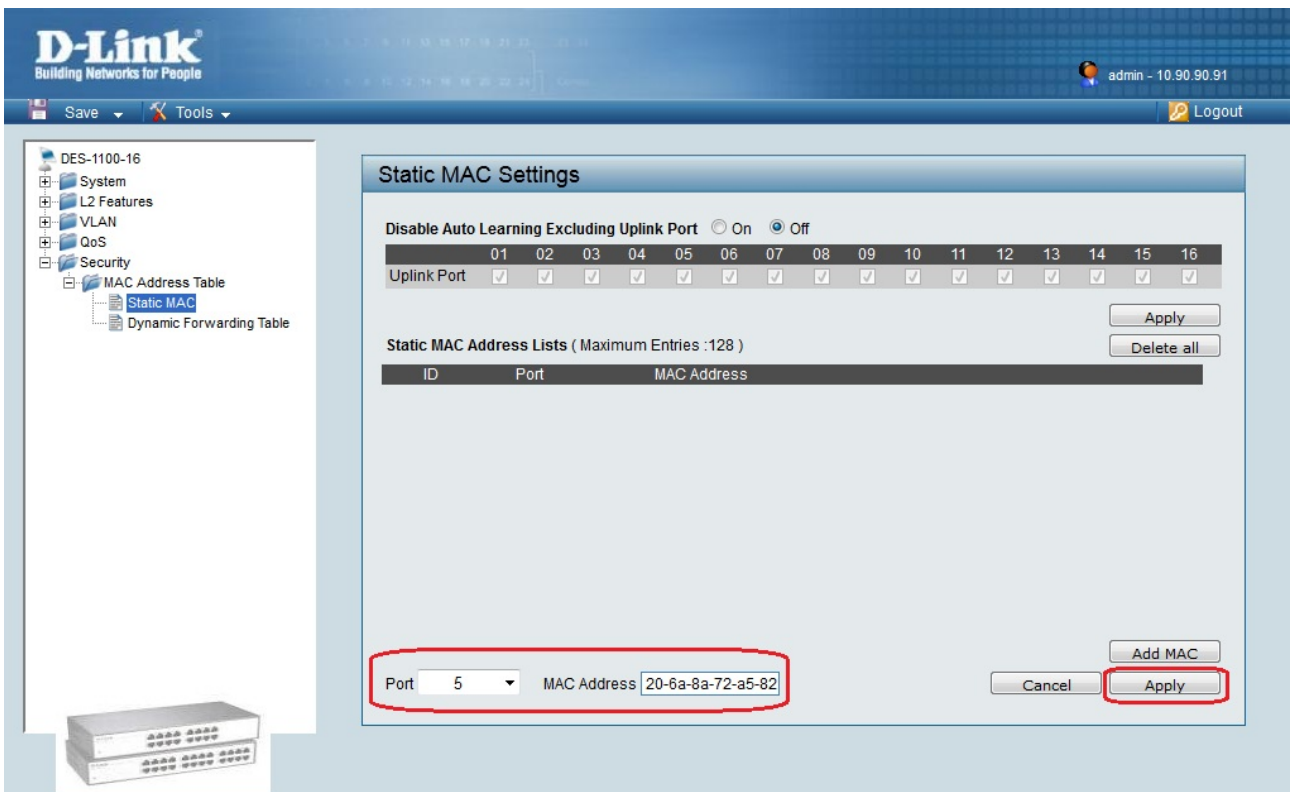


Рисунок 6.6 Создание статической записи

Шаг 10. Отключите рабочую станцию ПК2 от 5 порта и подключите к 4 порту.

Шаг 11. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1 введите: `ping 10.90.90.92`

В командной строке ПК2 введите: `ping 10.90.90.91`

Объясните, почему нет связи между ПК1 и ПК2 _____

Шаг 12. Удалите статическую запись из таблицы коммутации. В левой части окна выберите *Security* → *MAC Address Table* → *Static MAC*. В правой части окна нажмите кнопку *Delete* напротив записи для ПК2 (рис. 6.7).

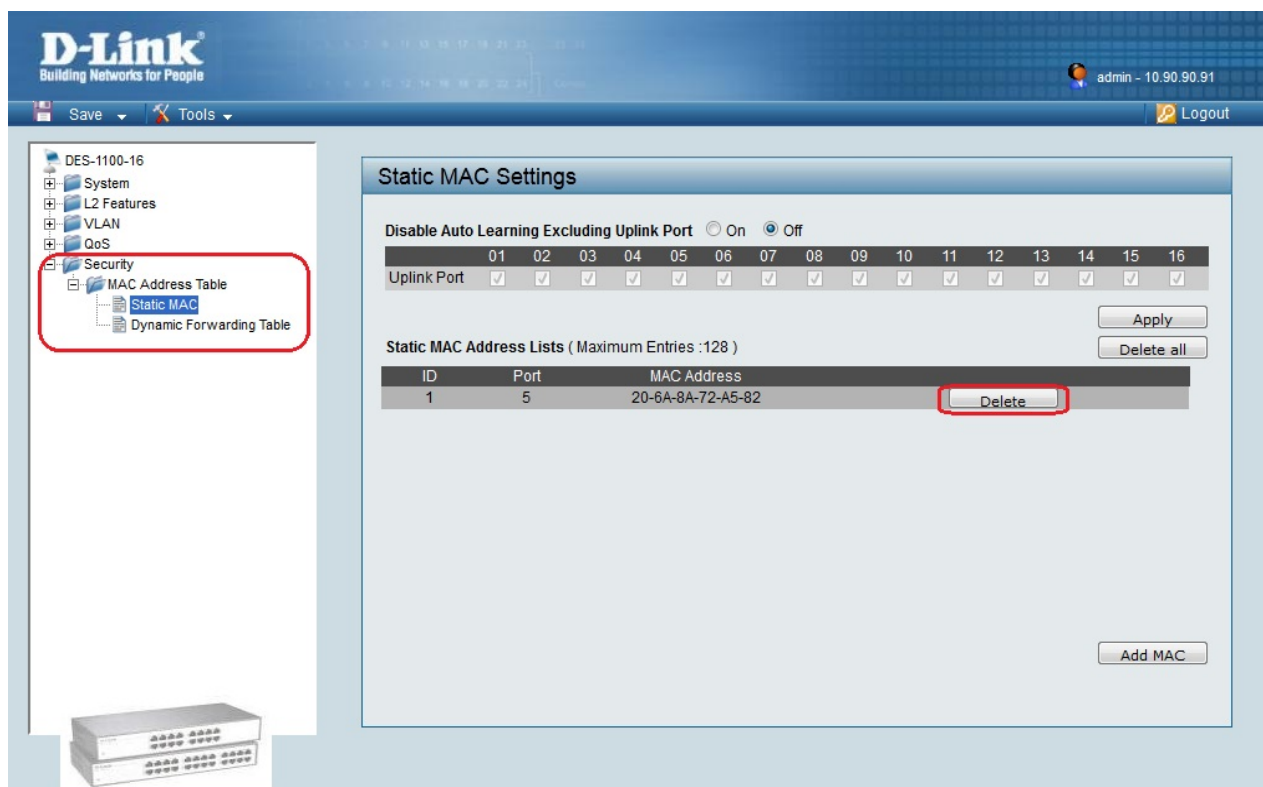


Рисунок 6.7 Удаление статической записи из таблицы коммутации

Шаг 13. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1 введите: `ping 10.90.90.92`

В командной строке ПК2 введите: `ping 10.90.90.91`

Шаг 14. Сбросьте настройки коммутатора к заводским настройкам по умолчанию. Выберите *Tools* → *Reset System* и нажмите кнопку *Apply* (рис. 6.8).

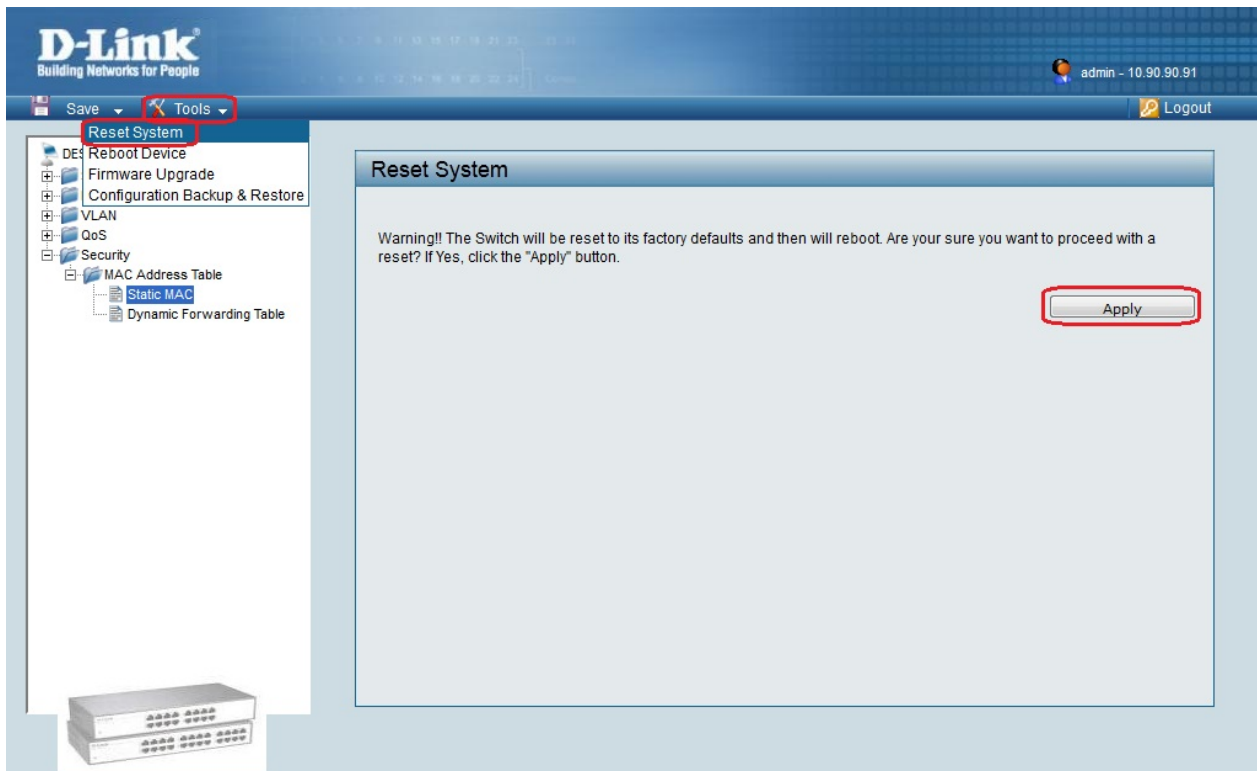


Рисунок 6.8 Сброс настроек коммутатора к заводским настройкам по умолчанию

6.2 Логическая сегментация сети с помощью технологии VLAN на основе портов (Port-Based VLAN)

Шаг 1. Подключите ПК1 и ПК2 к коммутатору, как показано на рис. 6.9.

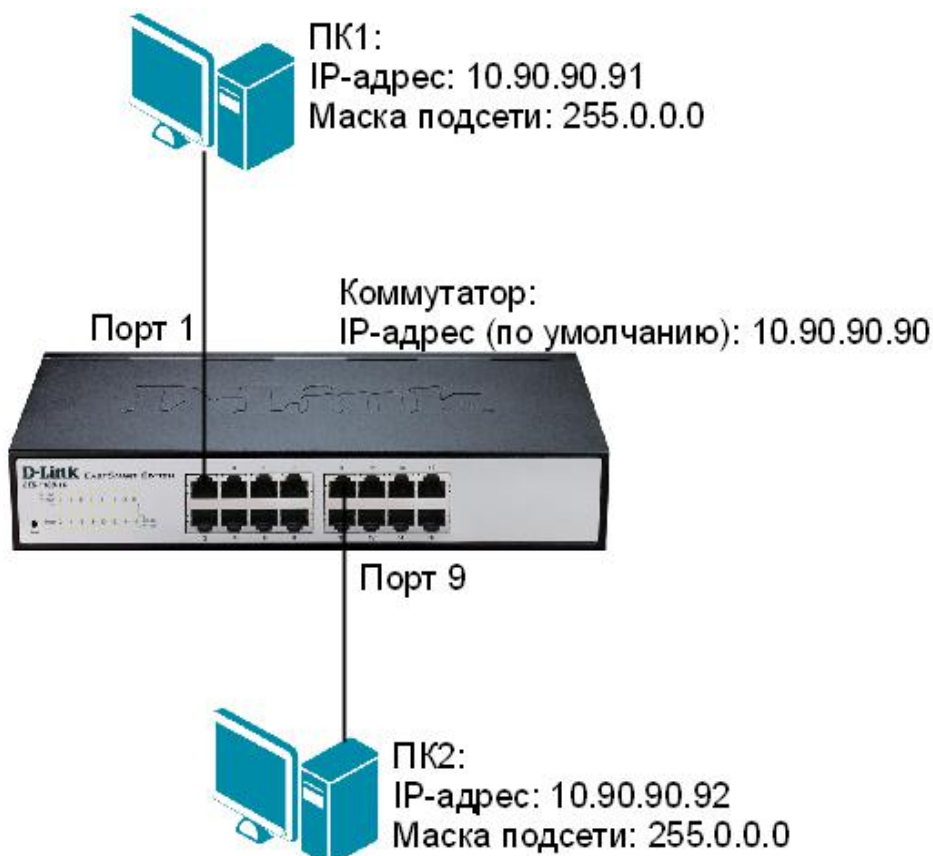


Рисунок 6.9 Схема сети

Шаг 2. Настройте на рабочей станции ПК1 и ПК2 статический IP-адрес в соответствии со схемой сети (рис.6.9).

Шаг 3. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1 введите: `ping 10.90.90.92`

В командной строке ПК2 введите: `ping 10.90.90.91`

Шаг 4. Зайдите на Web-интерфейс коммутатора.

Шаг 5. Создайте VLAN на основе портов на коммутаторе DES-1100-16. Для этого выберите *VLAN* → *Port-Based VLAN* (рис. 6.10).

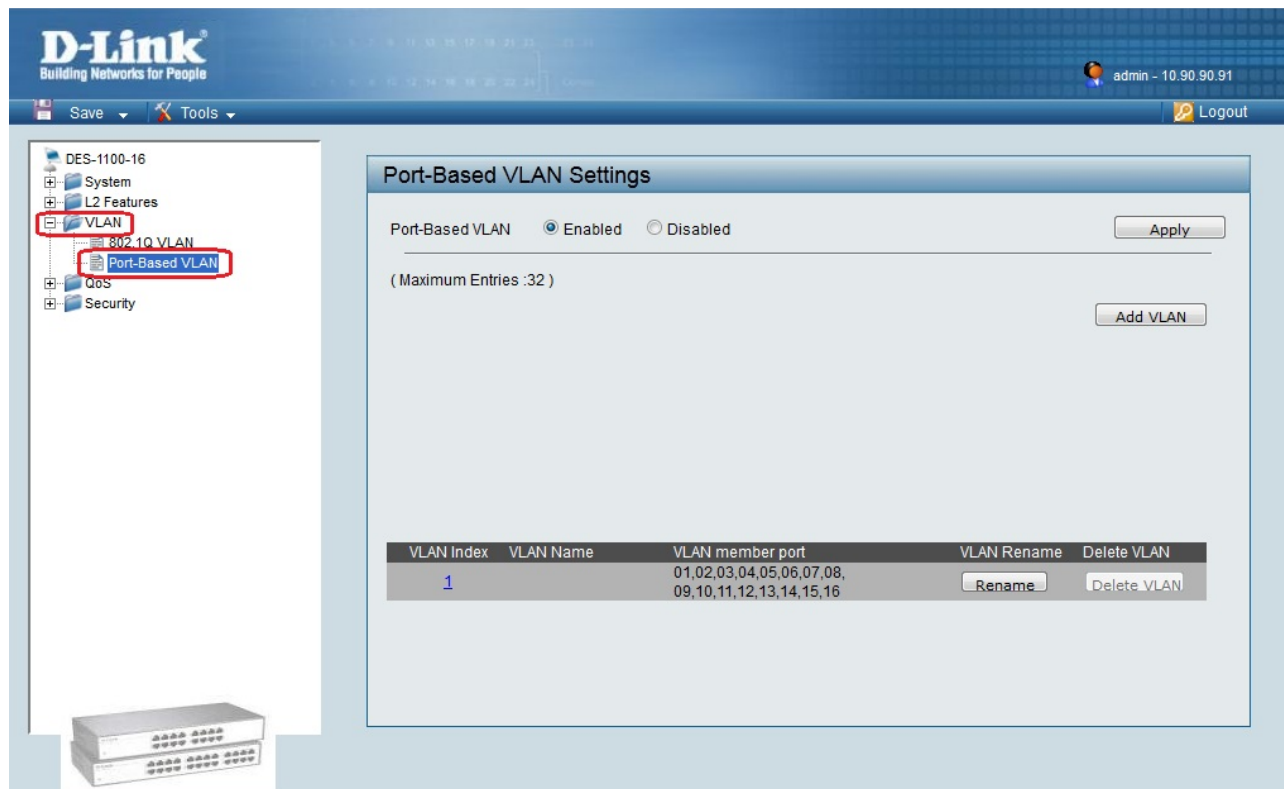


Рисунок 6.10

В открывшемся окне установите галочку *Port-Based VLAN* → *Enable* и нажмите кнопку *Apply* (рис. 6.11).

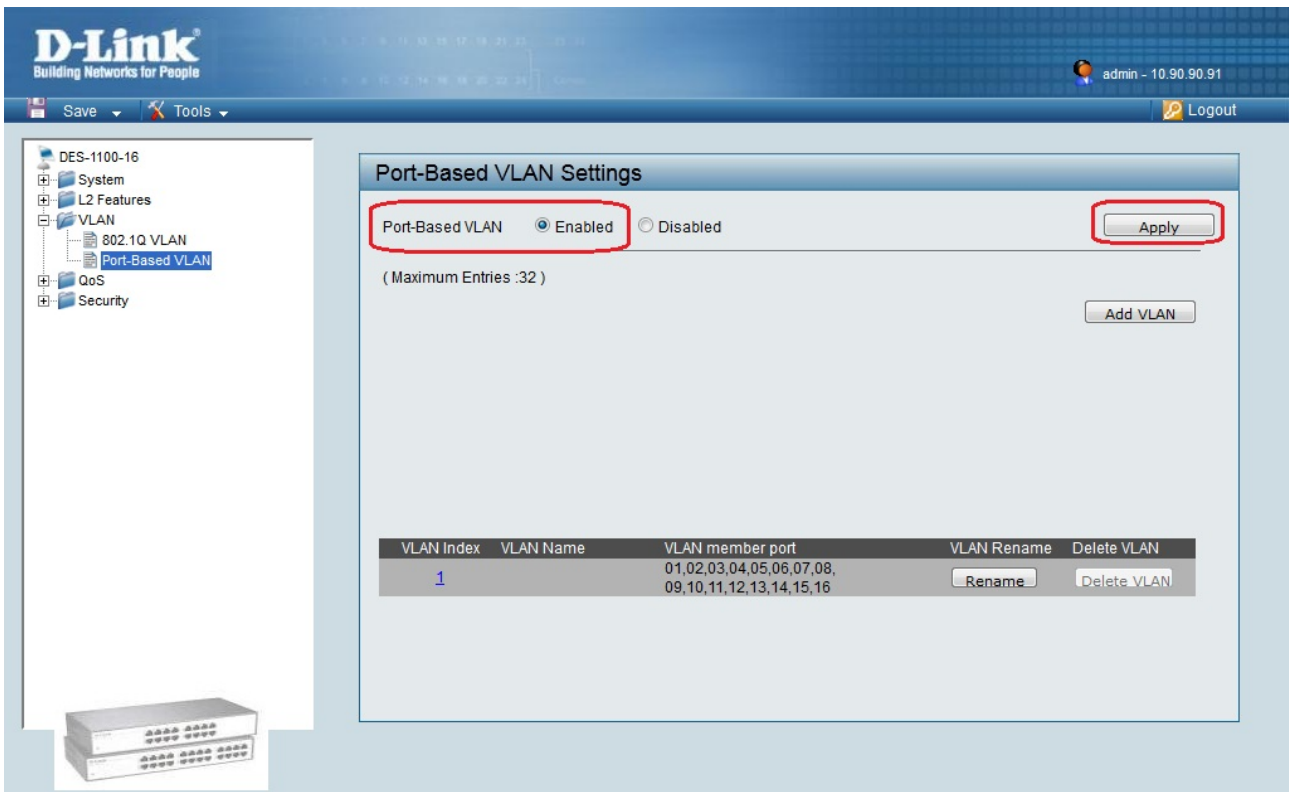


Рисунок 6.11

Примечание: по умолчанию все порты коммутатора входят в одну VLAN с идентификатором $VLAN\ Index = 1$.

Шаг 6. Удалите порты 9-16 из VLAN по умолчанию ($VLAN\ Index = 1$). Нажмите на *VLAN Index 1* (рис. 6.12). В открывшемся окне снимите галочки с номеров портов 9-16 и нажмите кнопку *Apply* (рис. 6.13).

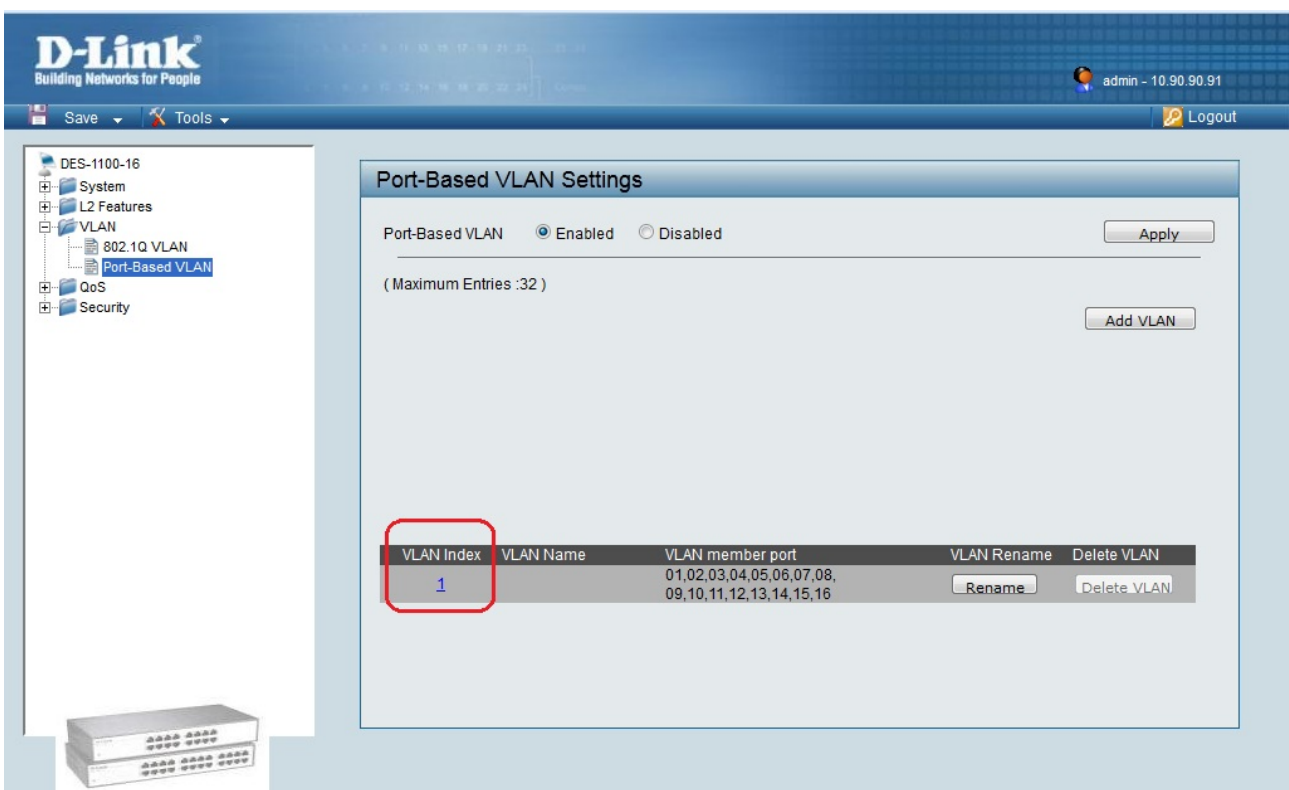


Рисунок 6.12

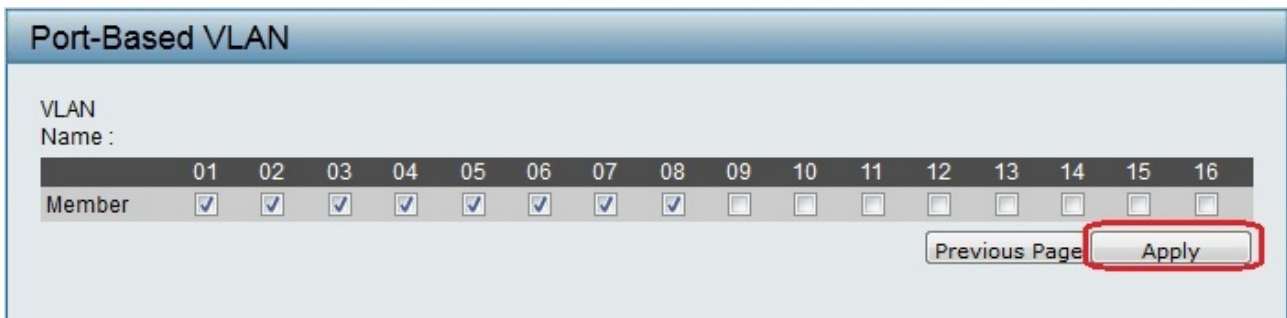


Рисунок 6.13

Шаг 7. Создайте VLAN с именем v2 и добавьте порты 9-16. Для этого нажмите на кнопку *Add VLAN* (рис. 6.14). В поле *VLAN Name* введите v2 и установите галочки 9-16, нажмите кнопку *Apply* (рис. 6.15).

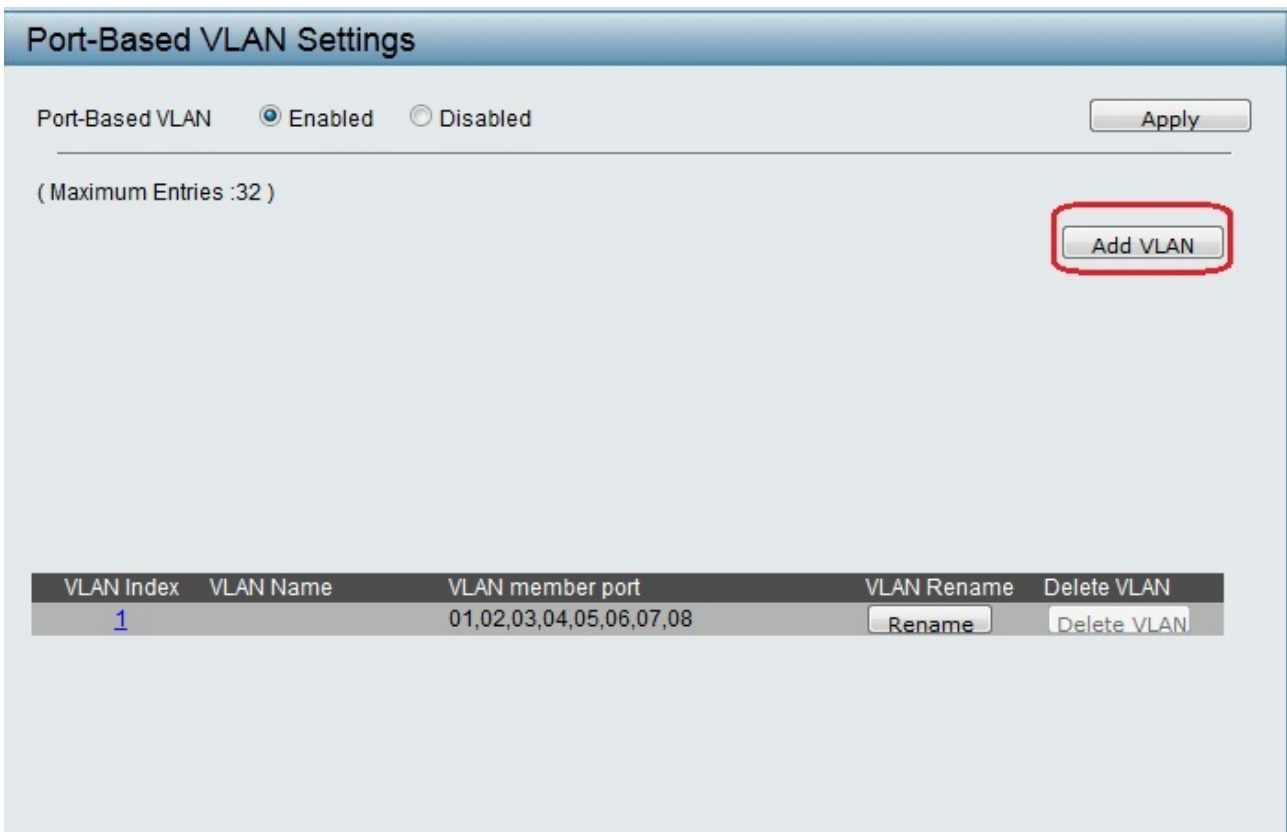


Рисунок 6.14

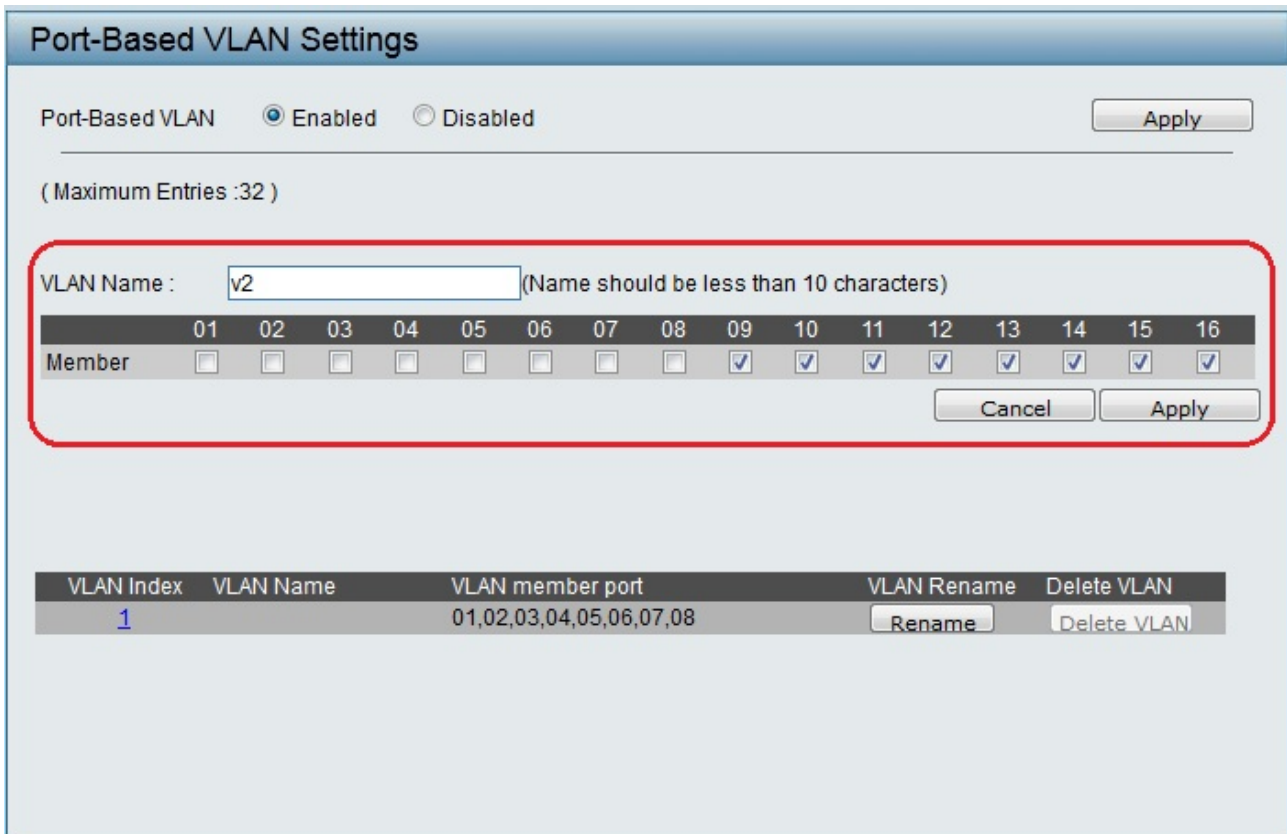


Рисунок 6.15

Шаг 8. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1 введите: `ping 10.90.90.92`

В командной строке ПК2 введите: `ping 10.90.90.91`

Объясните наличие/отсутствие связи между ПК1 и ПК2 _____

Шаг 9. Подключите рабочую станцию ПК1 к порту 10.

Шаг 10. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2.

В командной строке ПК1 введите: `ping 10.90.90.92`

В командной строке ПК2 введите: `ping 10.90.90.91`

Объясните наличие/отсутствие связи между ПК1 и ПК2 _____

Лабораторная работа №7. Создание беспроводной сети

Беспроводная локальная сеть (Wireless Local Area Network, WLAN) — это сетевая инфраструктура, в которой прием и передача данных осуществляется с помощью радиосигналов.

Беспроводные сети имеют ряд преимуществ перед обычными кабельными сетями:

- сеть можно быстро развернуть, что удобно при проведении презентаций или в условиях работы вне офиса;
- пользователи мобильных устройств, при подключении к локальным беспроводным сетям, могут легко перемещаться в рамках действующих зон сети;

Беспроводная сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Существуют два базовых режима функционирования беспроводной сети:

- Режим Ad-Нос;
- Режим инфраструктуры.

Режим Ad-Нос аналогичен одноранговой сети, когда клиенты устанавливают связь непосредственно друг с другом по типу соединения «точка-точка».

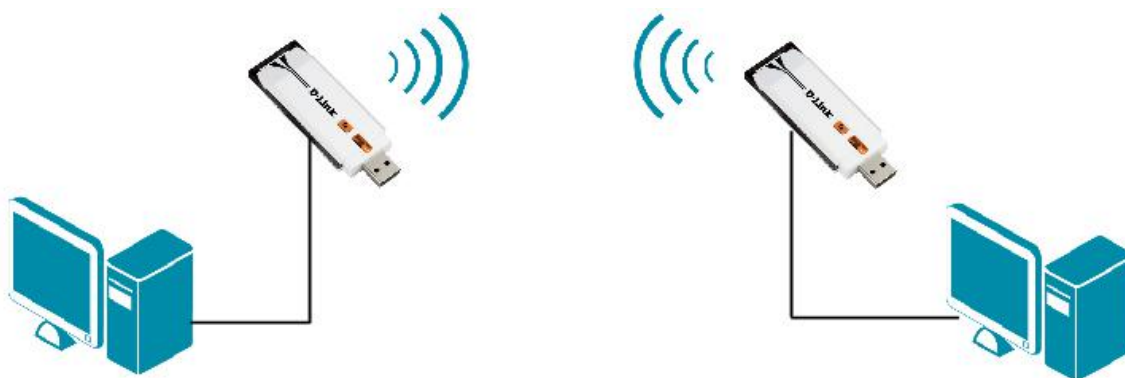
В *режиме инфраструктуры* компьютеры взаимодействуют друг с другом не напрямую, а через точку доступа, которая выполняет в беспроводной сети роль своеобразного коммутатора.

Оборудование (на 1 рабочее место):

Рабочая станция	3 шт.
Беспроводной адаптер DWA-160	2 шт.
Точка доступа DAP-2310	1 шт.
Кабель Ethernet	1 шт.

Цель работы: создать беспроводную сеть в режиме Ad-Нос и инфраструктурном режиме, изучить Web-интерфейс точки доступа DAP-2310.

7.1 Создание беспроводной сети в режиме Ad-Hoc



ПК1:
IP-адрес: 192.168.1.1
Маска подсети: 255.255.255.0

ПК2:
IP-адрес: 192.168.1.2
Маска подсети: 255.255.255.0

Рисунок 7.1 Схема подключения оборудования в режиме Ad-Hoc

Шаг 1. На рабочей станции ПК1 и ПК2 установите драйвер для беспроводного адаптера DWA-160 и утилиту D-Link Connection Manager (установочный CD-диск входит в комплект оборудования). Следуйте инструкциям мастера установки (рис. 7.2 — 7.7).



Рисунок 7.2

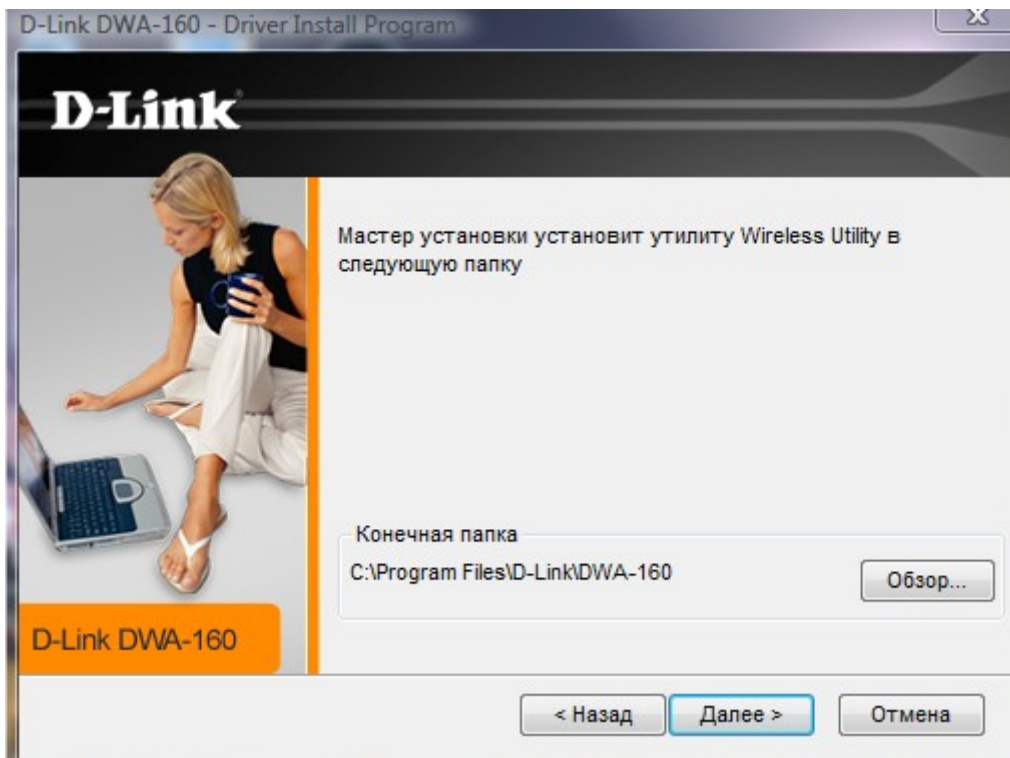


Рисунок 7.3

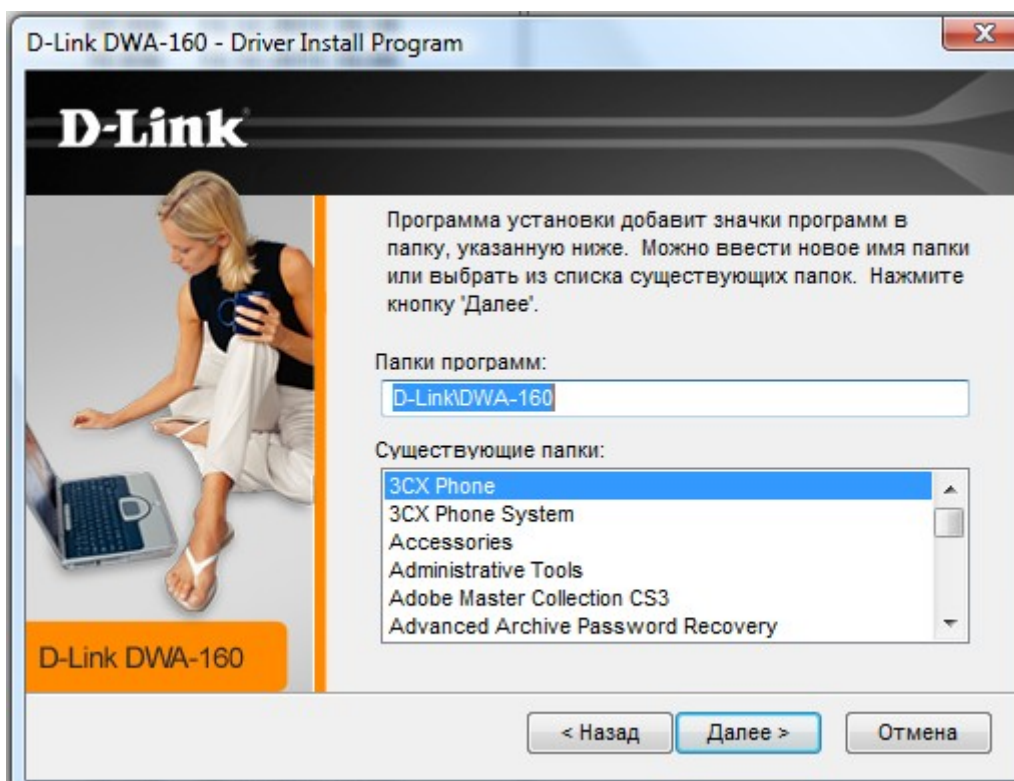


Рисунок 7.4

Подключите адаптер DWA-160 к рабочей станции через USB-порт и нажмите *Далее*.

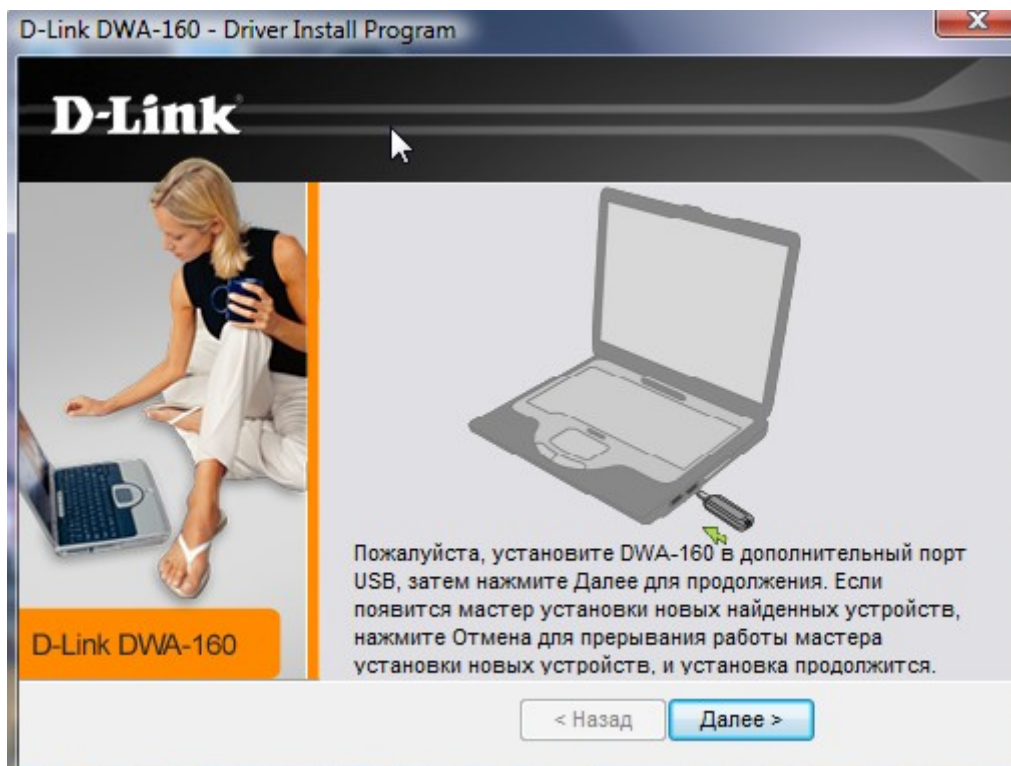


Рисунок 7.5

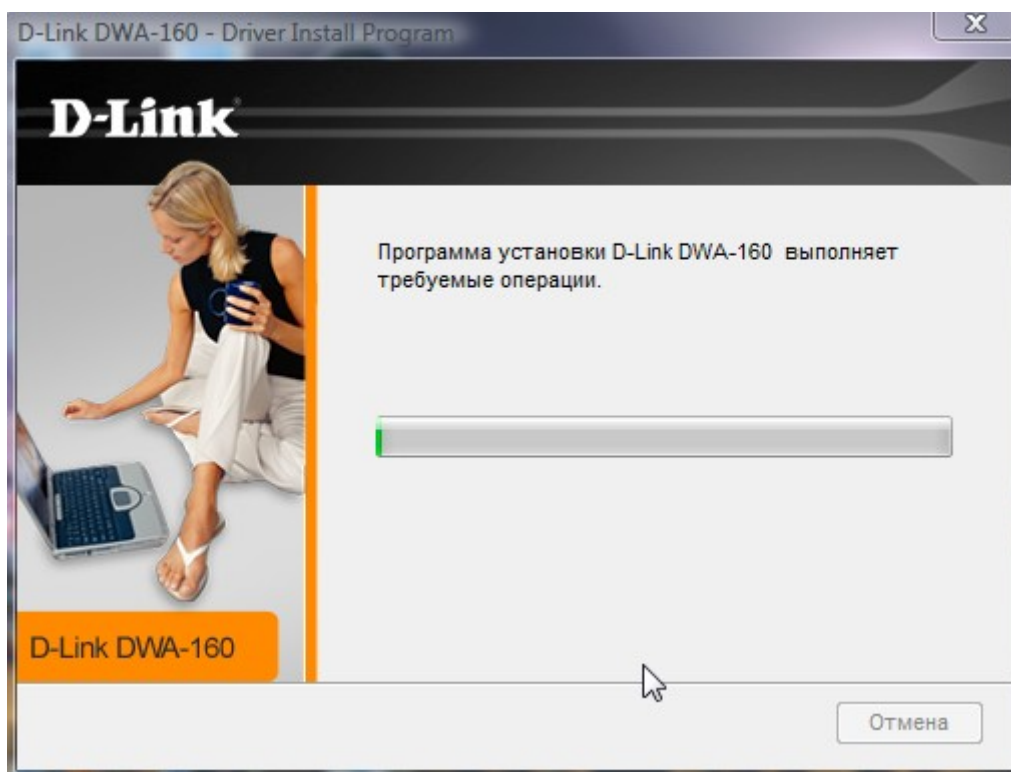


Рисунок 7.6

После установки нажмите кнопку *Выход*.

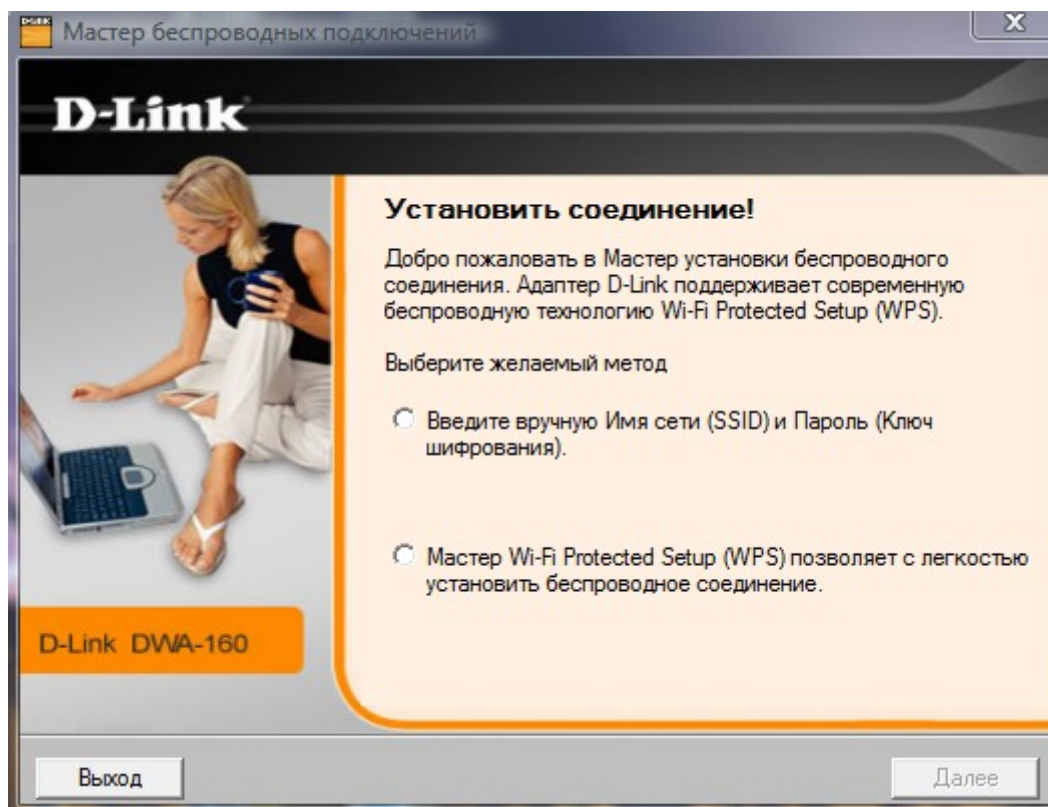


Рисунок 7.7

Настроить беспроводную сеть можно с помощью утилиты D-Link Connection Manager или через службу Windows.

7.1.1 Создание беспроводной сети в режиме Ad-Нос при помощи службы «Беспроводная настройка» ОС Windows XP

Шаг 1. Убедитесь, что служба «Беспроводная настройка» запущена и работает. Для этого выполните следующие действия:

1. Откройте окно *Службы*;

Пуск → Панель управления → Администрирование → Службы

2. Если служба «Беспроводная настройка» не запущена, выберите *Беспроводная настройка* и нажмите *Запустить службу* (рис. 7.8).

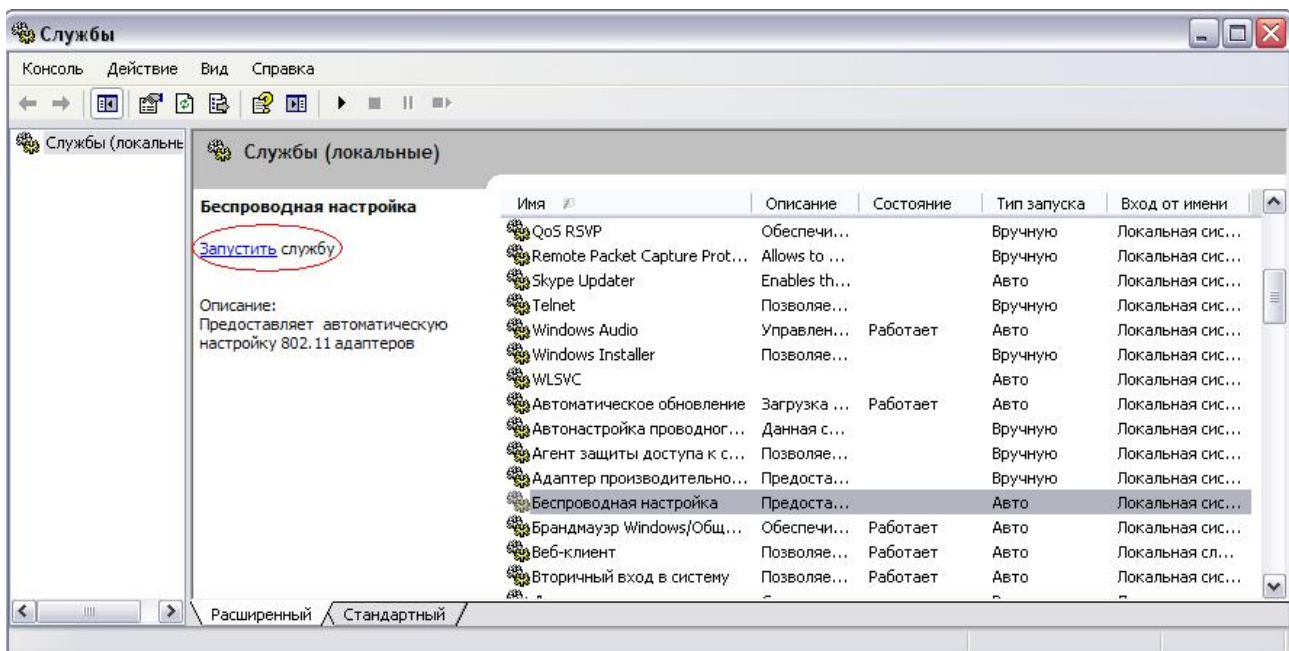


Рисунок 7.8 Запуск службы «Беспроводная настройка»

Шаг 2. Настройте статический IP-адрес на беспроводном интерфейсе ПК1 и ПК2.

1. Откройте *Сетевые подключения*;

Пуск → *Панель управления* → *Сетевые подключения*

2. Щелкните правой кнопкой мыши на *Беспроводное сетевое соединение* и выберите *Свойства*;

3. В диалоговом окне выберите *Протокол Интернета (TCP/IP)* и нажмите *Свойства*;

4. Выберите *Использовать следующий IP-адрес*;

5. В поле *IP-адрес* введите: 192.168.1.1(для ПК1) или 192.168.1.2 (для ПК2);

6. В поле *Маска подсети* введите: 255.255.255.0;

7. Нажмите кнопку *Ок*.

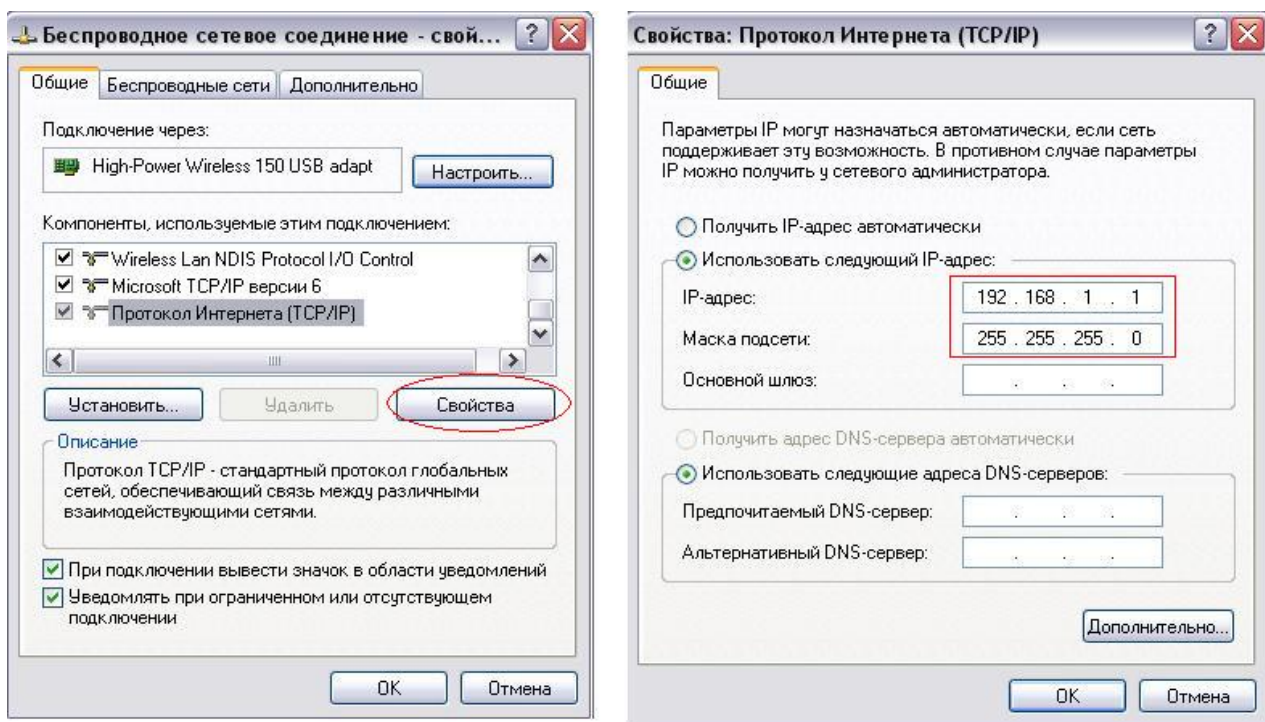


Рисунок 7.9 Настройка статического IP-адреса для беспроводного интерфейса

Шаг 3. На данном этапе выполнения лабораторной работы для настройки сети используйте только службу Windows. Для этого на рабочей станции ПК1 и ПК2 выполните следующие действия:

1. Откройте *Сетевые подключения*;

Пуск → Панель управления → Сетевые подключения

2. Щелкните правой кнопкой мыши на *Беспроводное сетевое соединение* и выберите *Свойства*;

3. Выберите вкладку *Беспроводные сети* и установите галочку *Использовать Windows для настройки сети* (рис. 7.10).

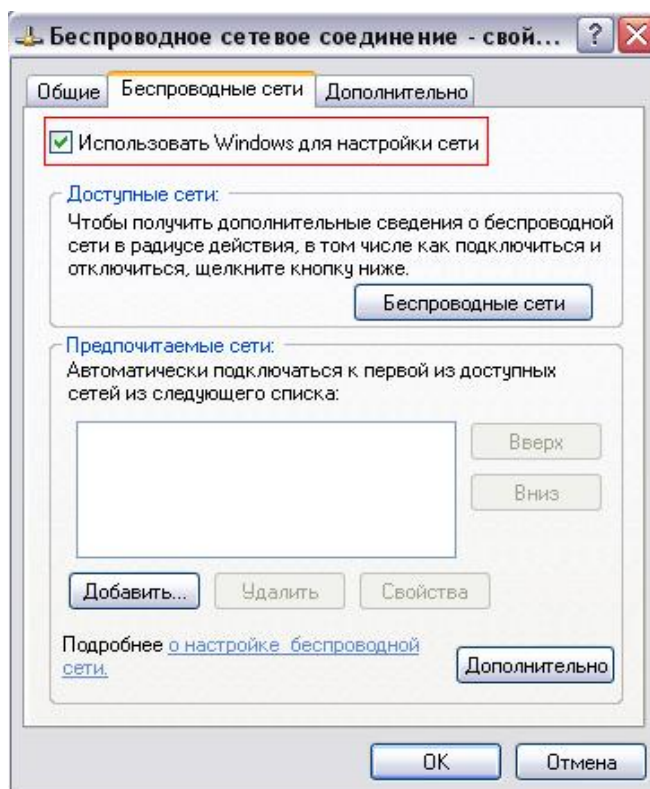


Рисунок 7.10

Шаг 4. На рабочей станции ПК1 создайте беспроводную сеть с именем *classroom243*.

Чтобы создать беспроводную сеть, выполните следующие действия:

1. Во вкладке *Беспроводные сети* нажмите на кнопку *Добавить*. Откроется окно *Свойства беспроводной сети* (рис. 7.11);

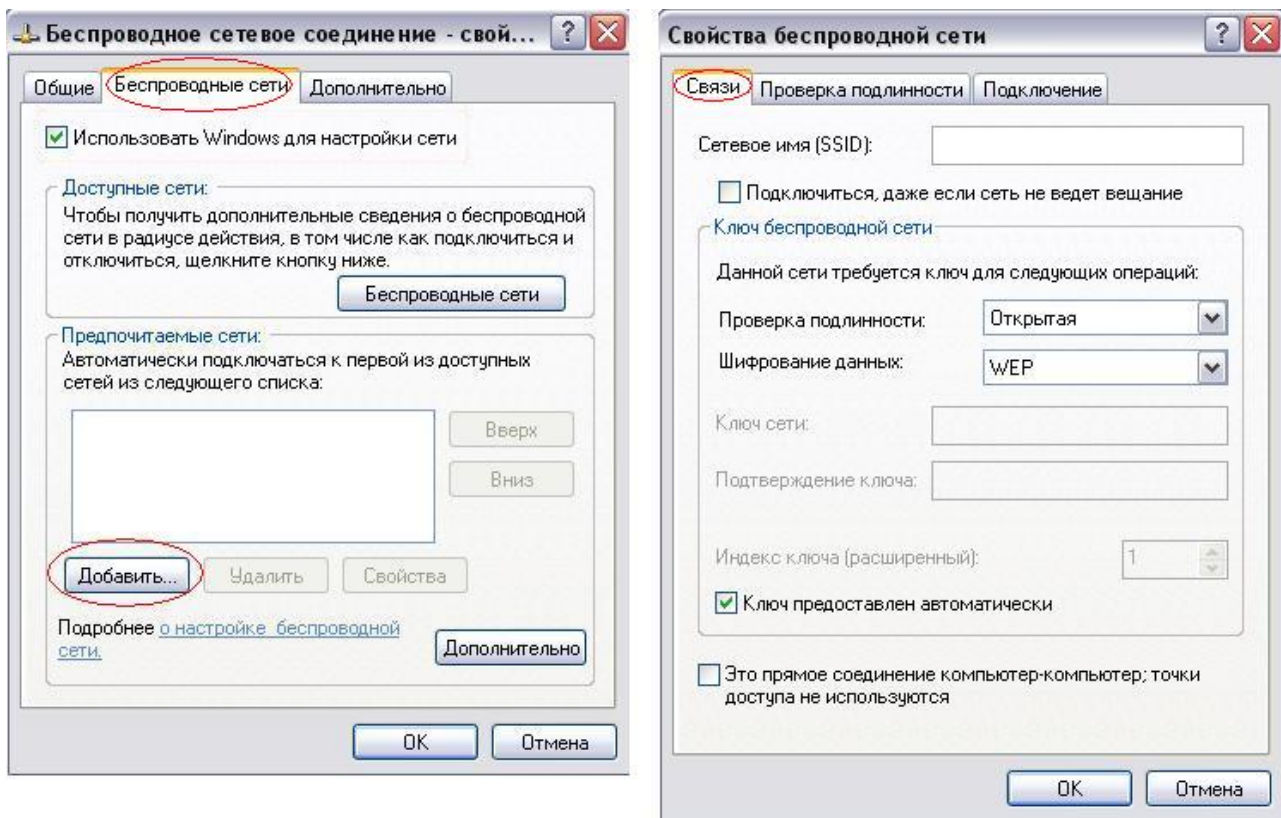


Рисунок 7.11

2. Во вкладке *Связи* заполните следующие поля (рис. 7.12):

2.1 Сетевое имя (SSID): *classroom243*;

2.2 Проверка подлинности: *Открытая*;

2.3 Шифрование данных: *WEP*;

2.4 Снимите галочку *Ключ предоставлен автоматически*;

2.5 Ключ сети: *DlinkPassword*;

2.6 Подтверждение ключа: *DlinkPassword*;

2.7 Установите галочку *Это прямое соединение компьютер-компьютер; точки доступа не используются*;

2.8 Нажмите кнопку *Ок*.

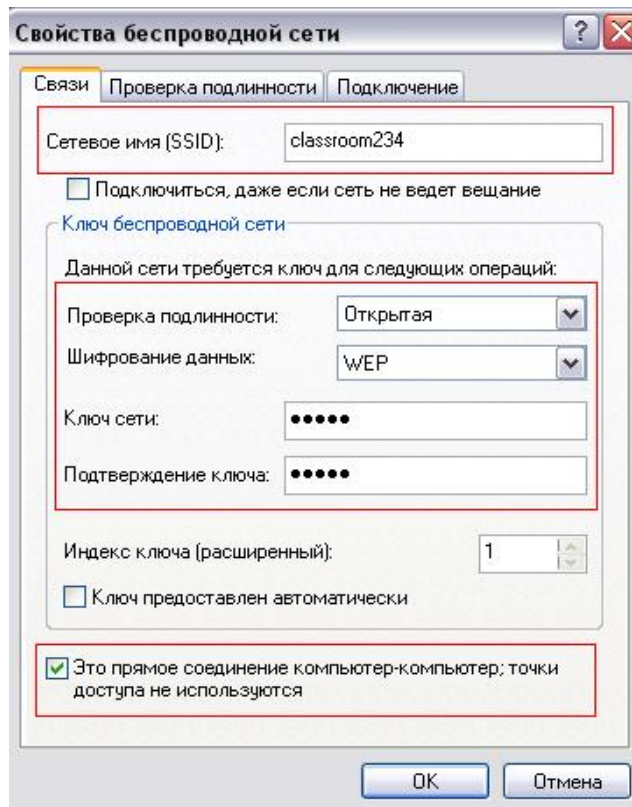


Рисунок 7.12 Создание беспроводной сети с именем *classroom234*

Шаг 5. Выполните поиск беспроводной сети на рабочей станции ПК2.

Чтобы посмотреть доступные беспроводные сети, выполните следующие действия:

1. Откройте *Сетевые подключения*;

Пуск → Панель управления → Сетевые подключения

2. Щелкните правой кнопкой мыши на *Беспроводное сетевое соединение* и выберите *Просмотр доступных беспроводных сетей* (рис. 7.13);

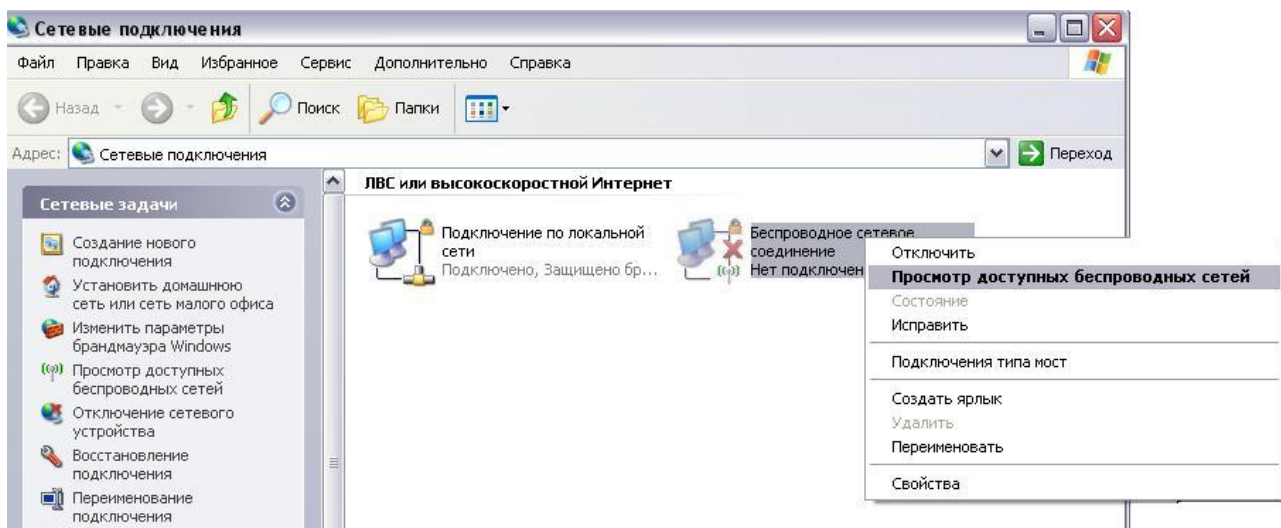


Рисунок 7.13 Окно *Сетевые подключения*

Шаг 6. В окне поиска найдите и выделите беспроводную сеть *classroom234*, которая была установлена на рабочей станции ПК1, и нажмите кнопку *Подключить*. Если созданная беспроводная сеть не отображается, нажмите *Обновить список сети* (рис. 7.14).

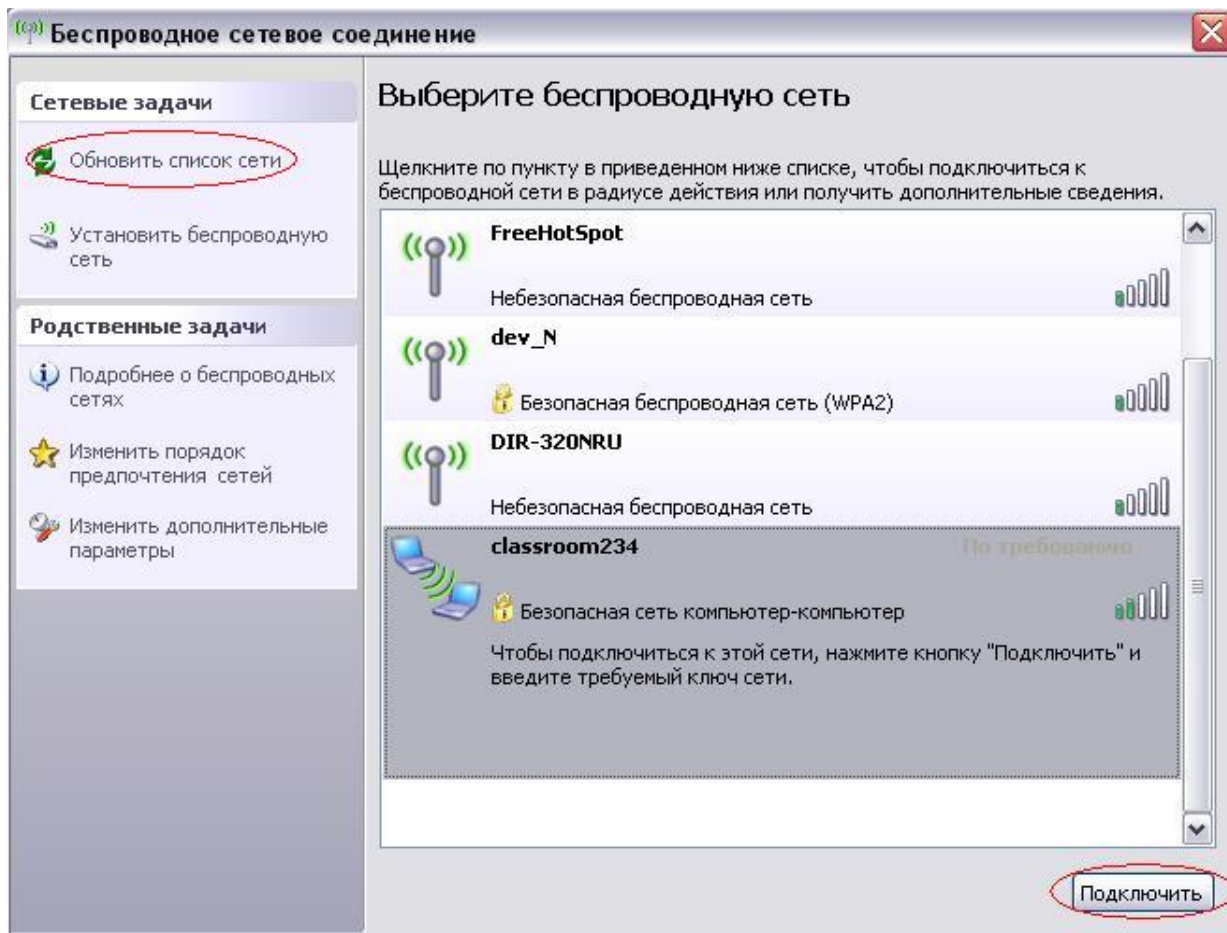


Рисунок 7.14 Подключение к беспроводной сети *classroom234*

Шаг 7. В появившемся окне введите *Ключ сети* и *Подтверждение ключа*, установленные при создании беспроводной сети *classroom234* на рабочей станции ПК1, и нажмите кнопку *Подключить* (рис. 7.15).

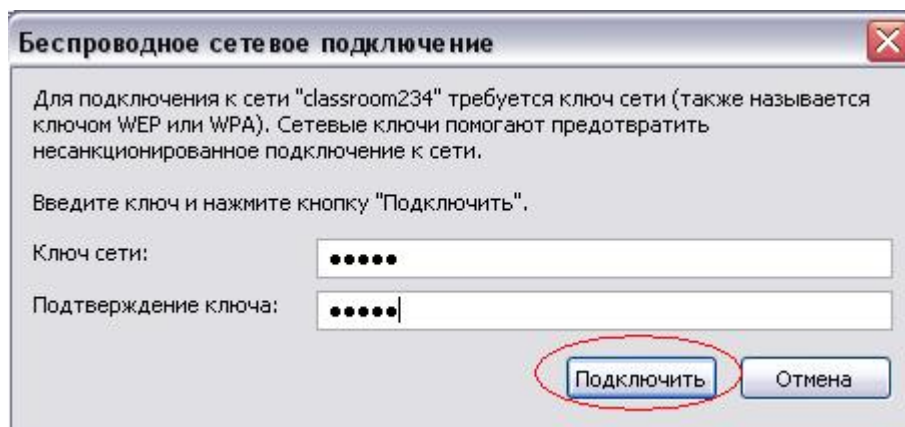


Рисунок 7.15 Ввод ключа сети

Шаг 8. Проверьте соединение между рабочими станциями ПК1 и ПК2 с помощью команды ping:

В командной строке ПК1 введите: `ping 192.168.1.2`

В командной строке ПК2 введите: `ping 192.168.1.1`

Шаг 9. Отключитесь от беспроводной сети *classroom234*. Для этого в окне поиска выделите беспроводную сеть *classroom234* и нажмите на кнопку *Разъединить* (рис.7.16).

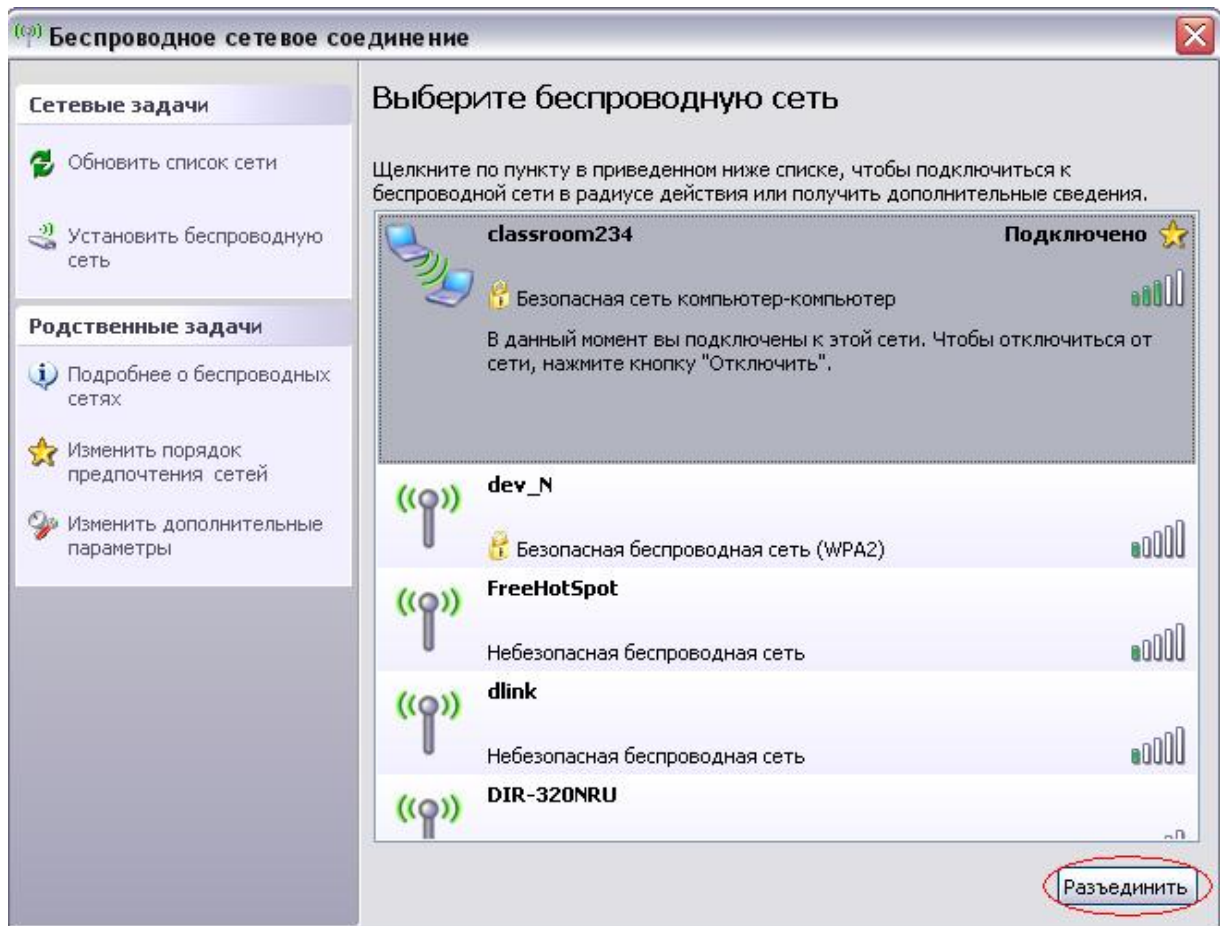


Рисунок 7.16 Отключение от беспроводной сети *classroom234*

Шаг 10. Удалите беспроводную сеть *classroom234*. Во вкладке *Беспроводные сети* выделите беспроводную сеть *classroom234* и нажмите на кнопки *Удалить* и *Ок* (рис. 7.17).

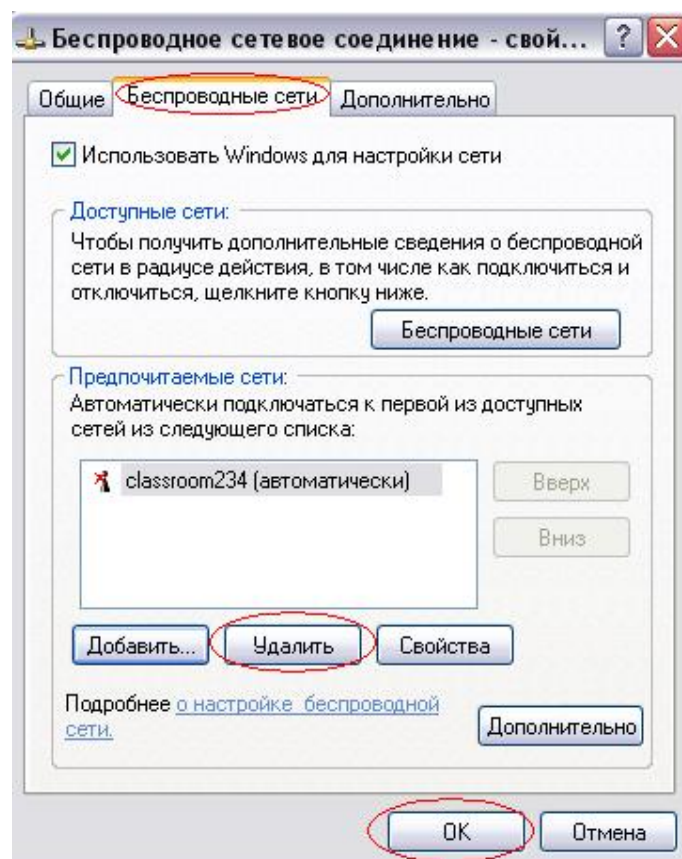


Рисунок 7.17 Удаление беспроводной сети *classroom234*

7.1.2 Создание беспроводной сети в режиме Ad-Hoc для рабочих станций с ОС Windows Vista/7

Шаг 1. Настройте статический IP-адрес на беспроводном интерфейсе ПК1 и ПК2.

1. Откройте *Изменение параметров адаптера*;

Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера

2. Щелкните правой кнопкой мыши по *Беспроводное сетевое соединение* и выберите *Свойства* (рис. 7.18);

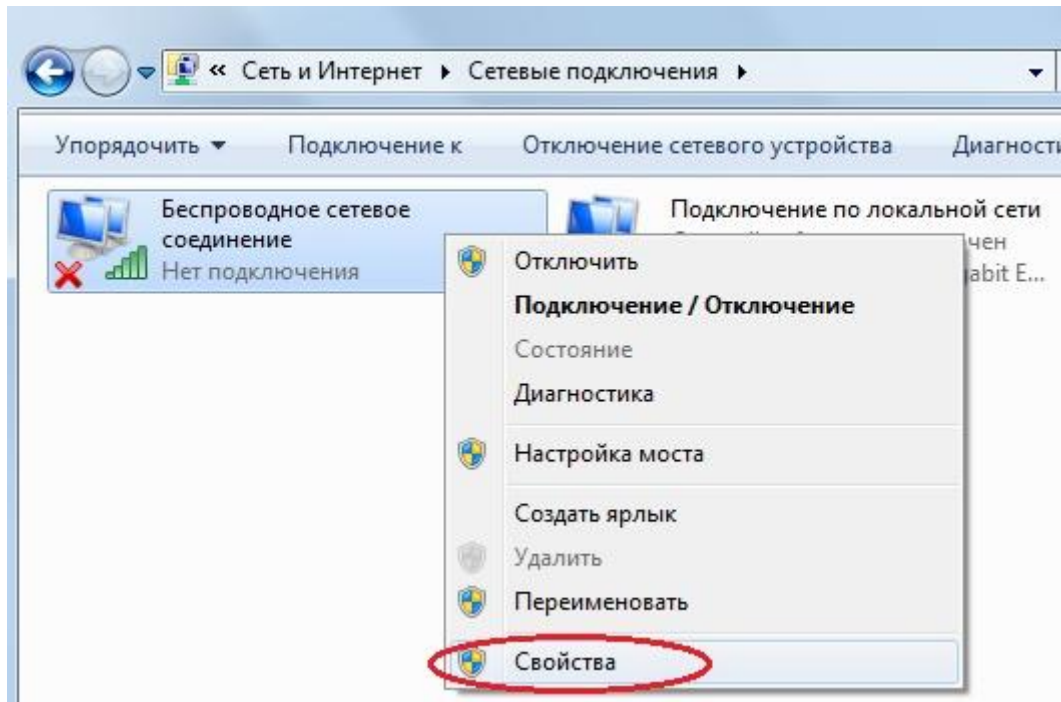


Рисунок 7.18 Окно *Изменение параметров адаптера*

3. В диалоговом окне выберите *Протокол Интернета 4 (TCP/IP)* и нажмите *Свойства* (рис. 7.19);

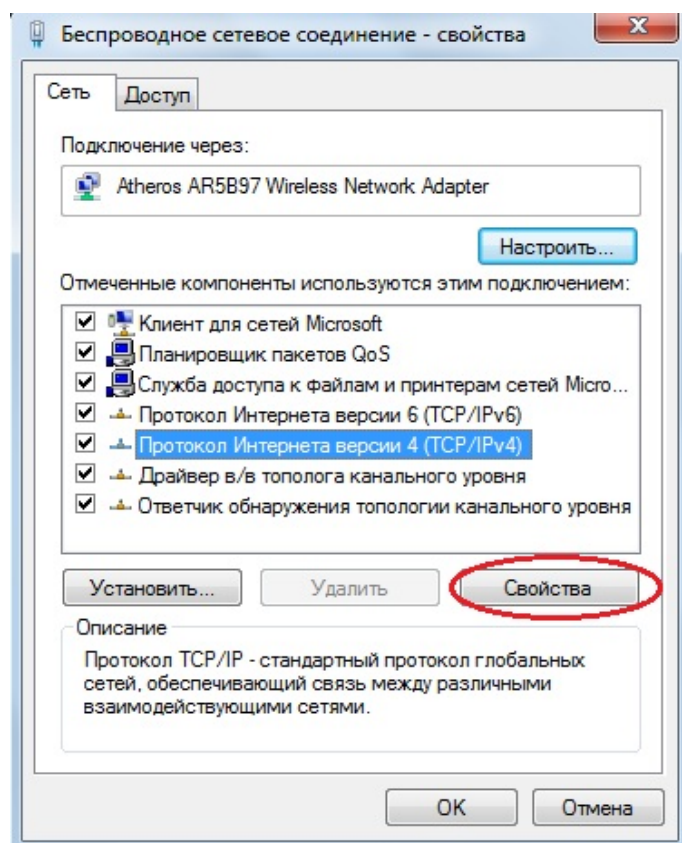


Рисунок 7.19

4. Выберите *Использовать следующий IP-адрес* (рис. 7.20);

5. В поле *IP-адрес* введите: 192.168.1.1(для ПК1) или 192.168.1.2 (для ПК2);

6. В поле *Маска подсети* введите: 255.255.255.0;

7. Нажмите кнопку *Ок*.

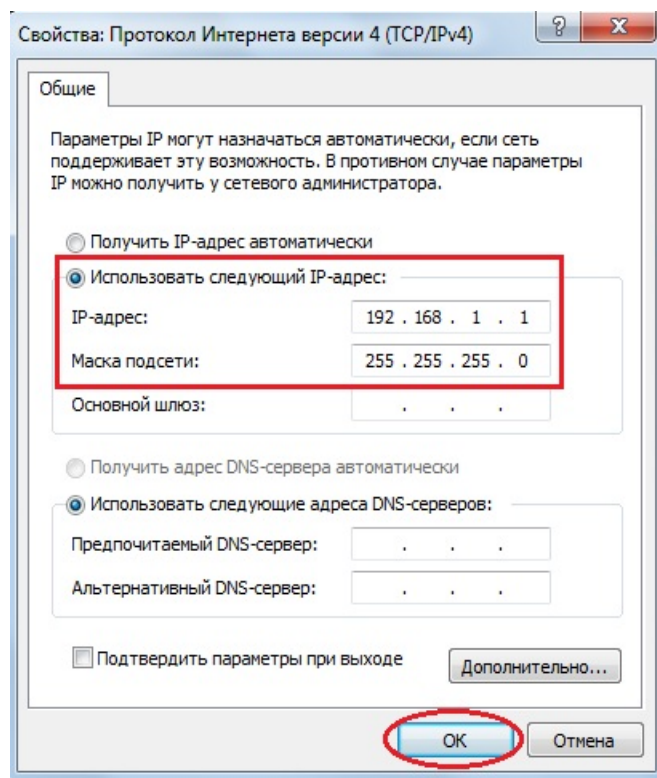


Рисунок 7.20

Шаг 2. На рабочей станции ПК1 создайте беспроводную сеть с именем *classroom243*.

Чтобы создать беспроводную сеть, выполните следующие действия:

1. Откройте *Управление беспроводными сетями* (рис. 7.21);

Пуск → *Панель управления* → *Центр управления сетями и общим доступом* → *Управление беспроводными сетями*

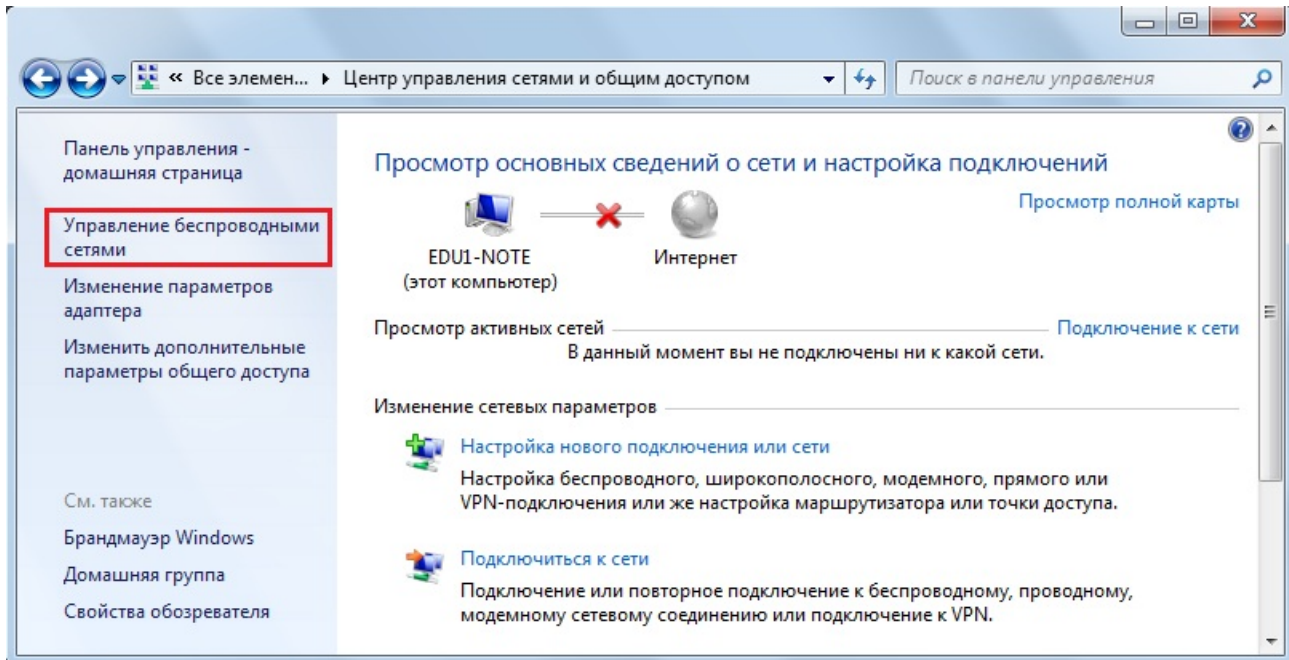


Рисунок 7.21 Окно *Центр управления сетями и общим доступом*

2. В открывшемся окне нажмите кнопку *Добавить* (рис. 7.22);

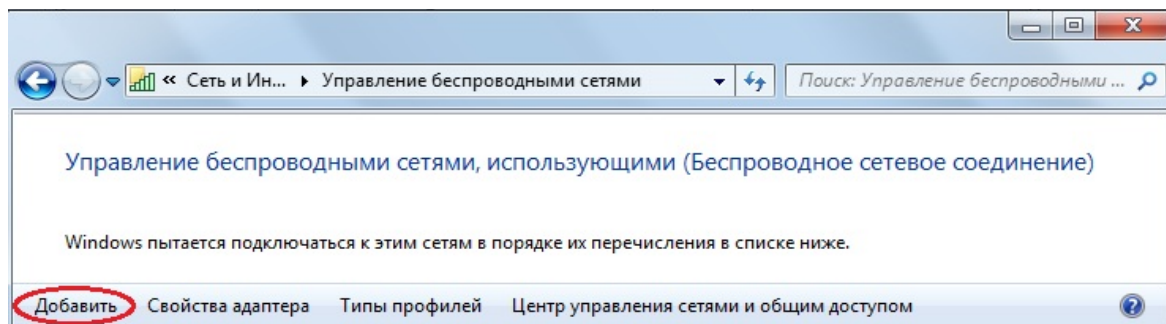


Рисунок 7.22 Окно *Управление беспроводными сетями*

3. Нажмите *Создать сеть «компьютер-компьютер»* (рис. 7.23);

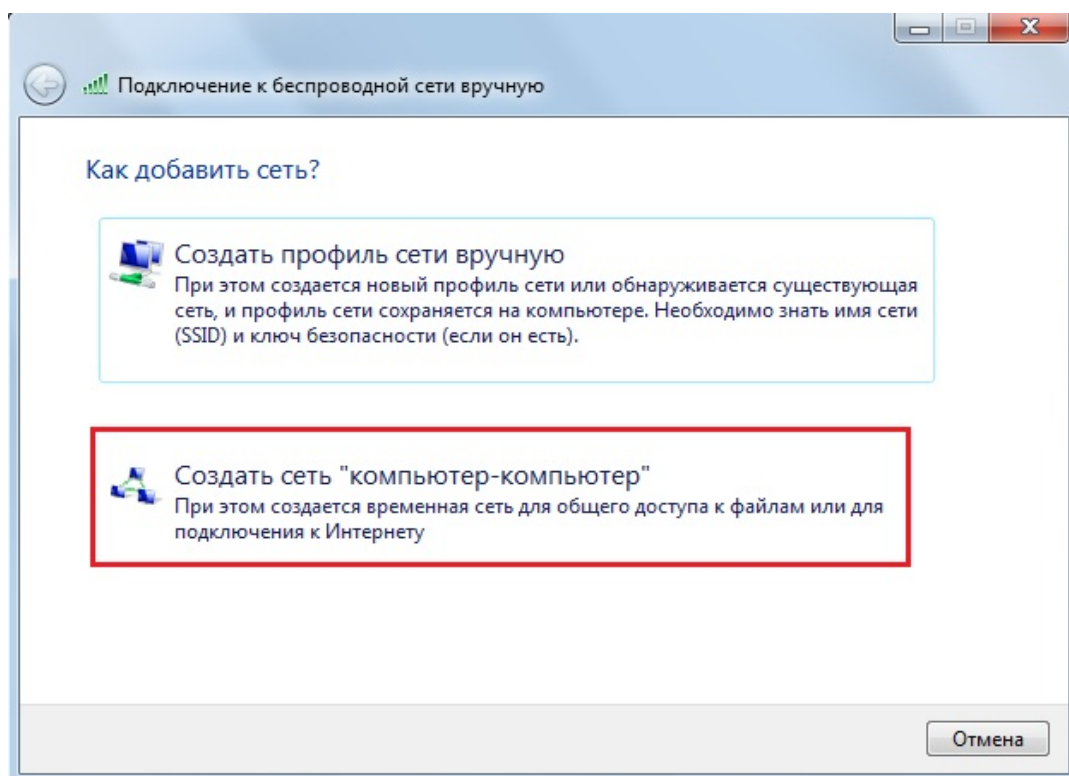


Рисунок 7.23

4. Нажмите кнопку *Далее* (рис. 7.24);

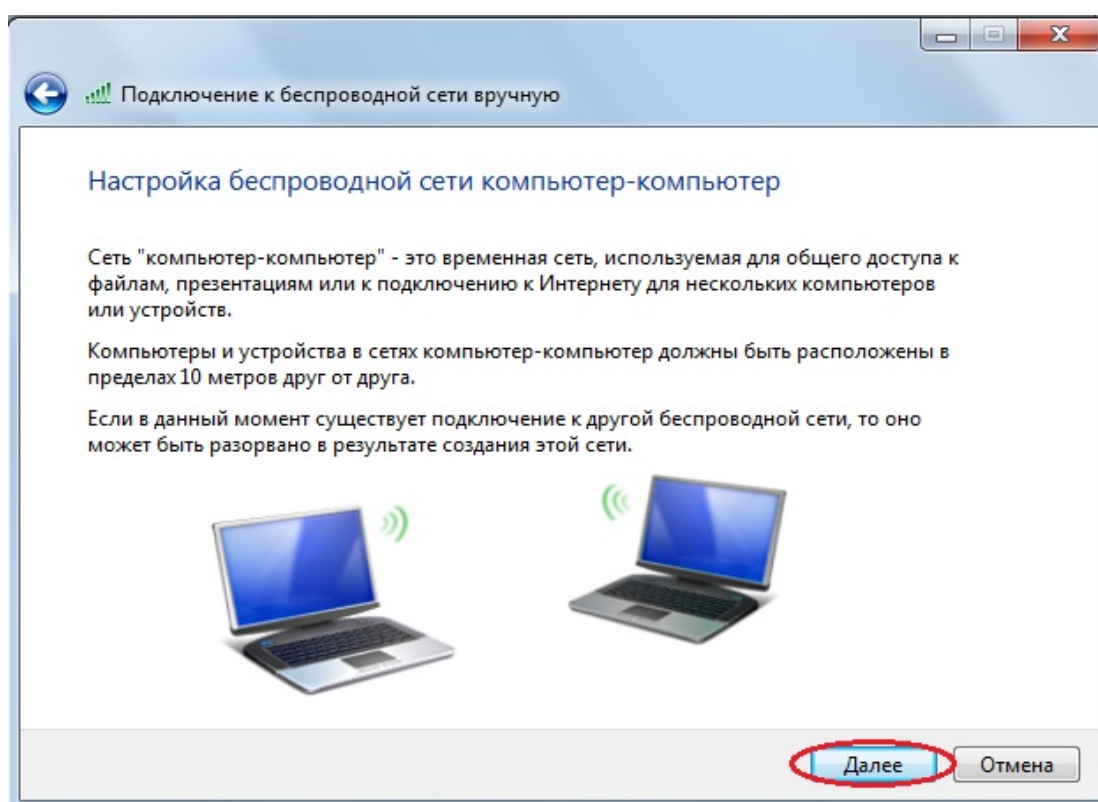


Рисунок 7.24

5. В поле *Имя сети* введите *classroom234* (рис. 7.25);

6. В поле *Тип безопасности*: WEP;

7. В поле *Ключ безопасности*: DlinkPassword;

8. Установите галочку *Сохранить параметры этой сети*;

9. Нажмите кнопку *Далее*;

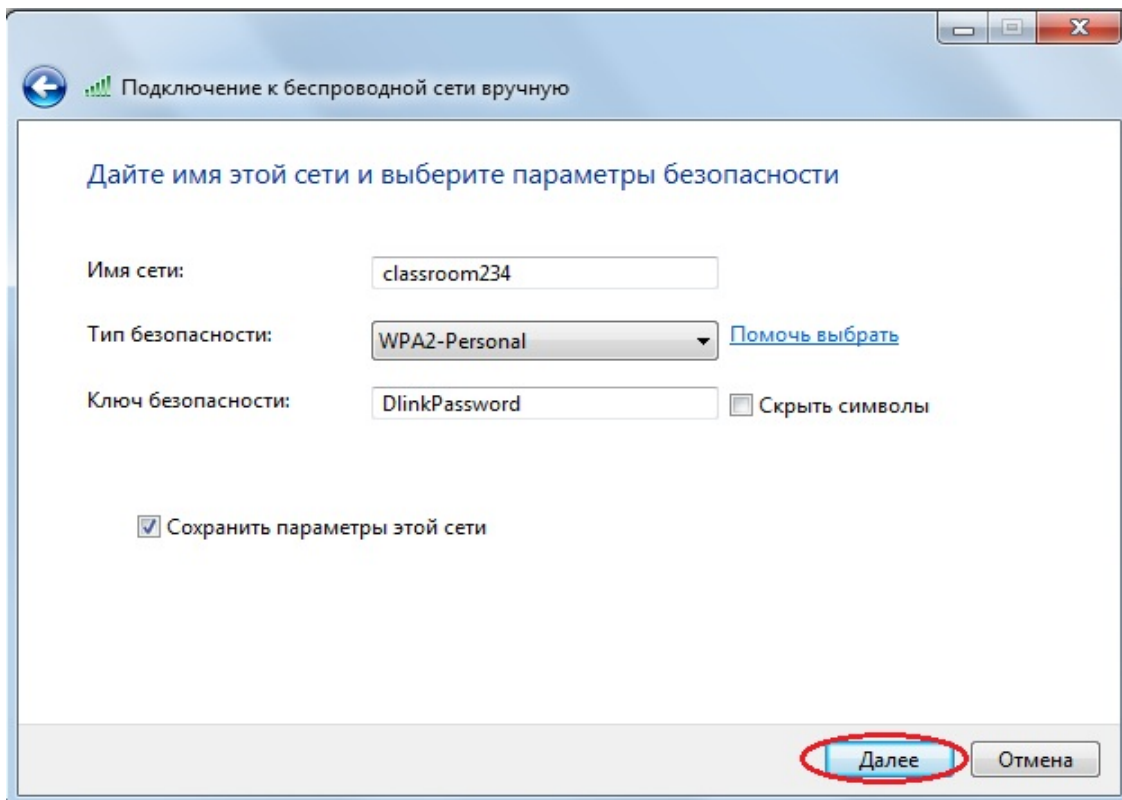


Рисунок 7.25 Создание беспроводной сети *classroom234*

10. Нажмите кнопку *Закреть* (рис. 7.26).

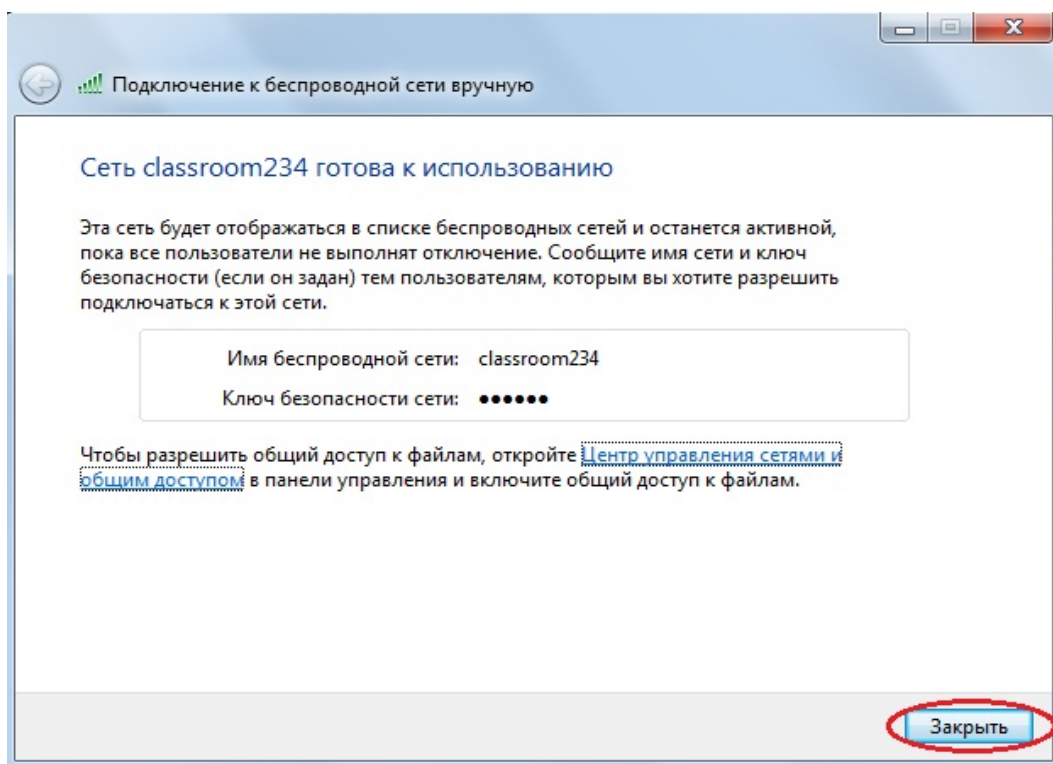


Рисунок 7.26

Шаг 3. Выполните поиск беспроводной сети на рабочей станции ПК2.

Чтобы посмотреть доступные беспроводные сети, выполните следующие действия:

1. Откройте *Изменение параметров адаптера*;

*Пуск → Панель управления → Центр управления сетями и общим доступом →
Изменение параметров адаптера*

2. Щелкните правой кнопкой мыши по *Беспроводное сетевое соединение* и выберите *Подключение/Отключение* (рис. 7.27);

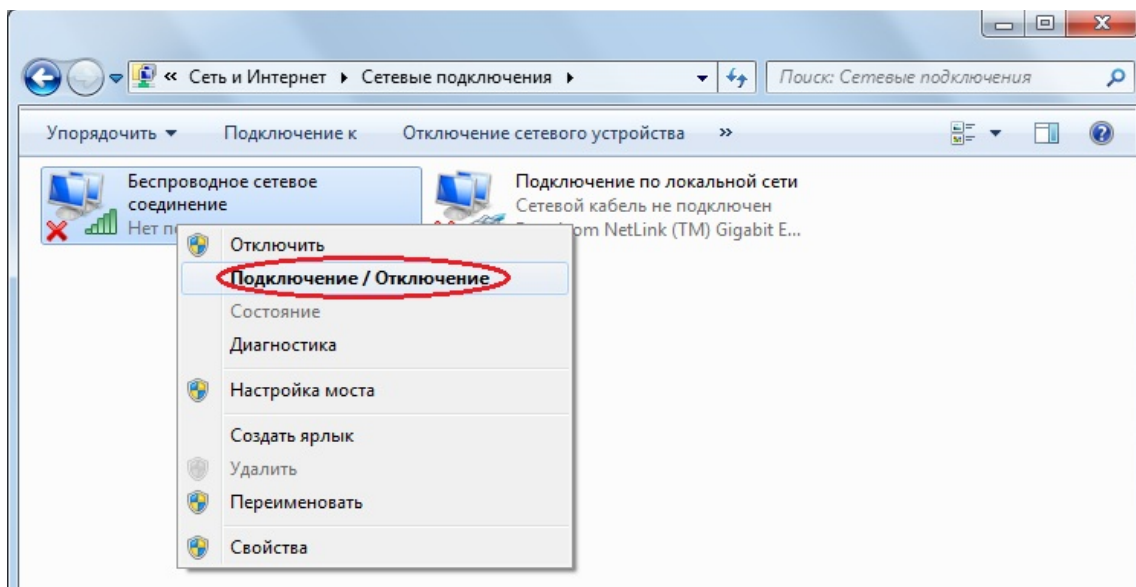



Рисунок 7.27

Шаг 4. В окне поиска найдите и выделите беспроводную сеть *classroom234*, которая была установлена на рабочей станции ПК1, и нажмите кнопку *Подключение*. Если созданная беспроводная сеть не отображается, нажмите кнопку  (рис. 7.28).

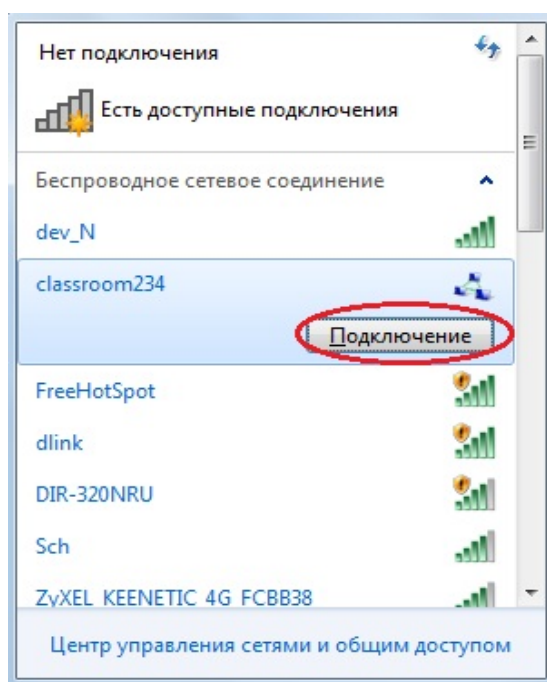


Рисунок 7.28 Подключение к беспроводной сети *classroom234*

Шаг 5. В появившемся окне аутентификации введите *Ключ безопасности*, установленный при создании беспроводной сети *classroom234* на рабочей станции ПК1, и нажмите кнопку *Ок* (рис. 7.29).

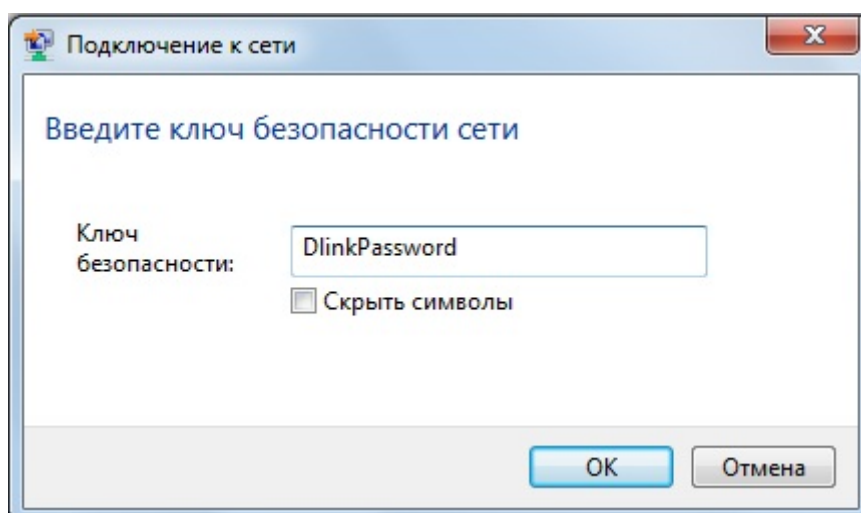


Рисунок 7.29

Шаг 6. Проверьте соединение между рабочими станциями ПК1 и ПК2 с помощью команды ping:

В командной строке ПК1 введите: `ping 192.168.1.2`

В командной строке ПК2 введите: `ping 192.168.1.1`

Шаг 7. Отключитесь от беспроводной сети *classroom234*. Для этого в окне поиска выделите беспроводную сеть *classroom234* и нажмите на кнопку *Отключение* (рис.7.30).

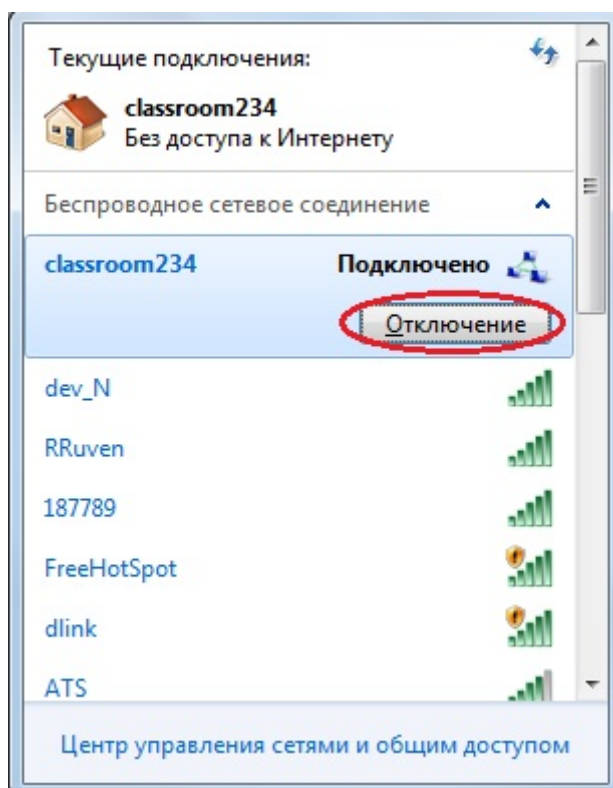


Рисунок 7.30 Отключение от беспроводной сети *classroom234*

Шаг 8. Удалите беспроводную сеть *classroom234*. Откройте *Управление беспроводными сетями*, выделите беспроводную сеть *classroom234* и нажмите на кнопку *Удалить* (рис. 7.31).

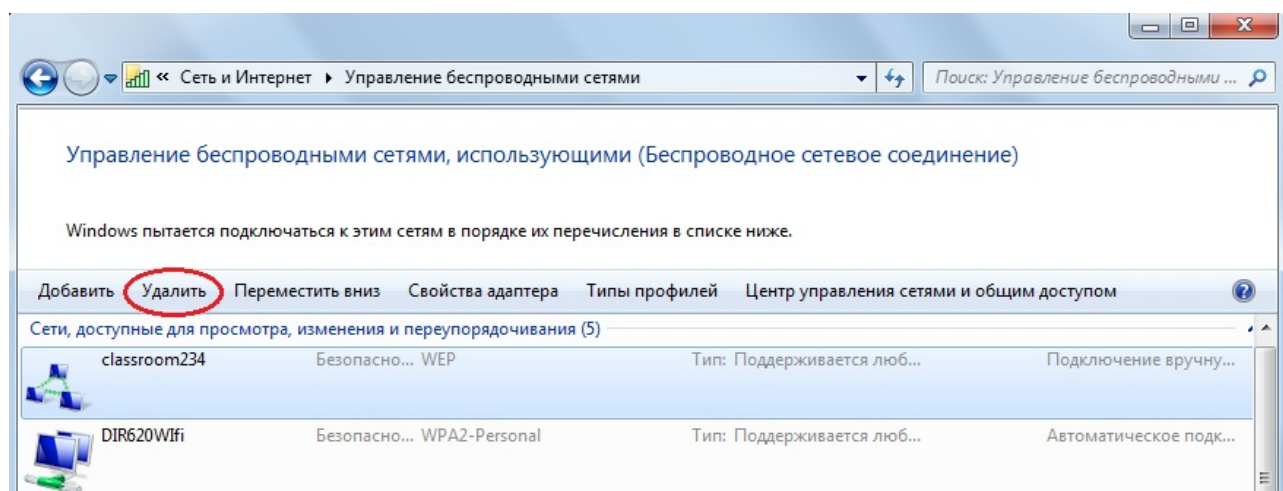


Рисунок 7.31 Удаление беспроводной сети *classroom234*

7.1.3 Создание беспроводной сети в режиме Ad-Нос при помощи утилиты D-Link Connection Manager

Внимание: для ОС Windows XP во вкладке *Беспроводные сети* снимите галочку *Использовать Windows для настройки сети*.

Шаг 1. На рабочей станции ПК1 откройте утилиту D-Link Connection Manager, щелкнув по ее иконке в панели задач Windows (рис. 7.32).

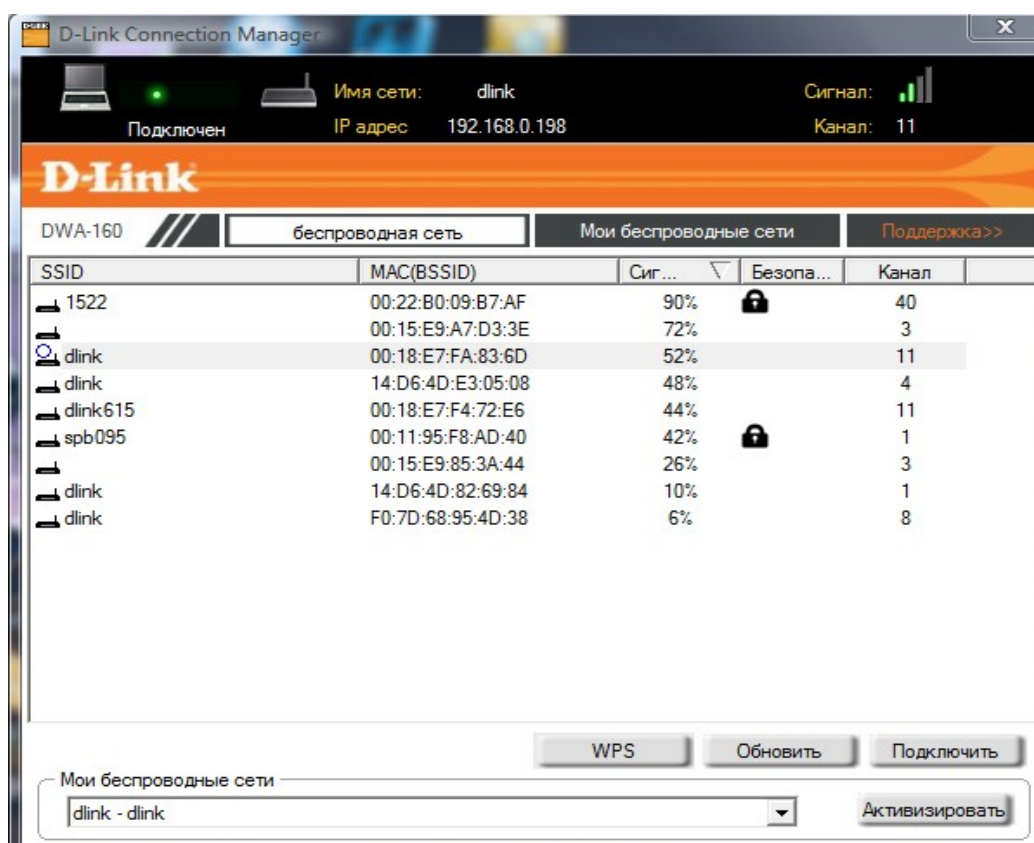


Рисунок 7.32 Интерфейс утилиты D-Link Connection Manager

Шаг 2. Перейдите во вкладку *Мои беспроводные сети* (рис. 7.33).

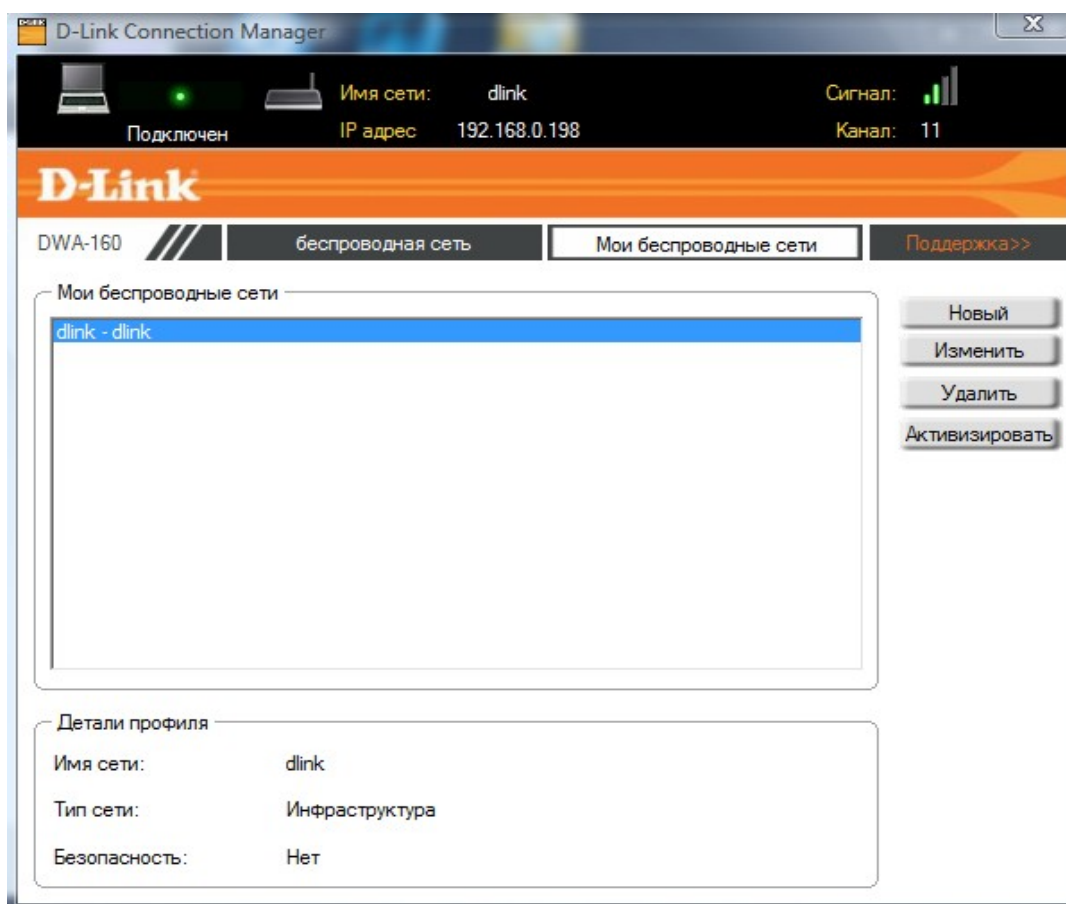


Рисунок 7.33

Шаг 3. Создайте новую беспроводную сеть в режиме Ad-Нос. Для этого нажмите на кнопку *Новый*.

Шаг 4. В открывшемся окне (рис. 7.34) укажите:

1. Имя профиля: *класс*;
2. SSID: *classroom243*;
3. Тип сети: *Ad-hoc*;
4. Установите параметры безопасности. Для этого установите галочку *Протокол WEP* и введите ключ *DlinkPassword*.

Примечание: чтобы в поле *Ключ* отображался пароль, установить галочку *Отобразить текст в поле пароля*.

5. Нажмите кнопку *Ок*;
6. Нажмите кнопку *Активизировать*.

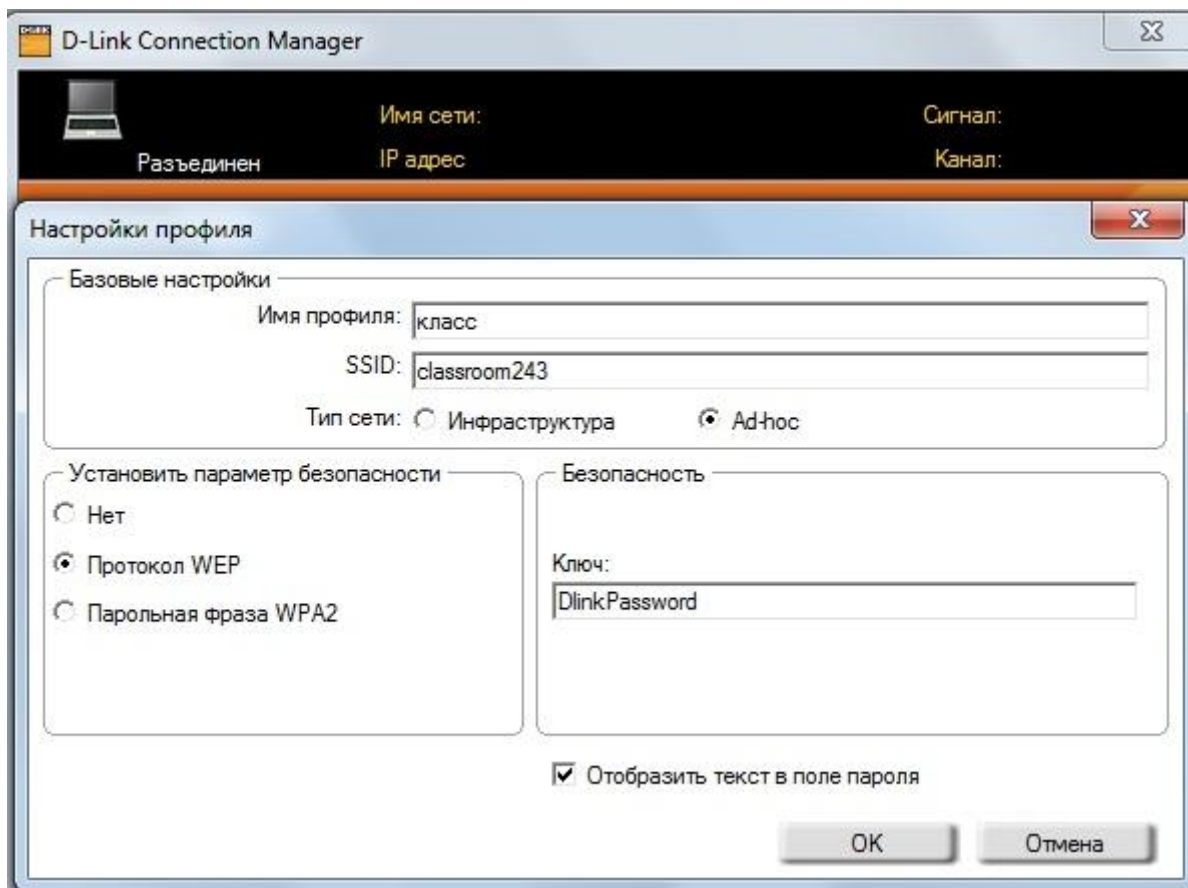


Рисунок 7.34 Создание беспроводной сети *classroom234*

Шаг 5. На рабочей станции ПК2 откройте утилиту D-Link Connection Manager и выберите беспроводную сеть *classroom234*, созданную на рабочей станции ПК1. Подключитесь к ней, нажав на кнопку *Подключить*, и введите пароль беспроводной сети.

Шаг 6. Проверьте соединение между рабочими станциями ПК1 и ПК2 с помощью команды ping:

В командной строке ПК1 введите: `ping 192.168.1.2`

В командной строке ПК2 введите: `ping 192.168.1.1`

7.2 Создание беспроводной сети в режиме инфраструктуры

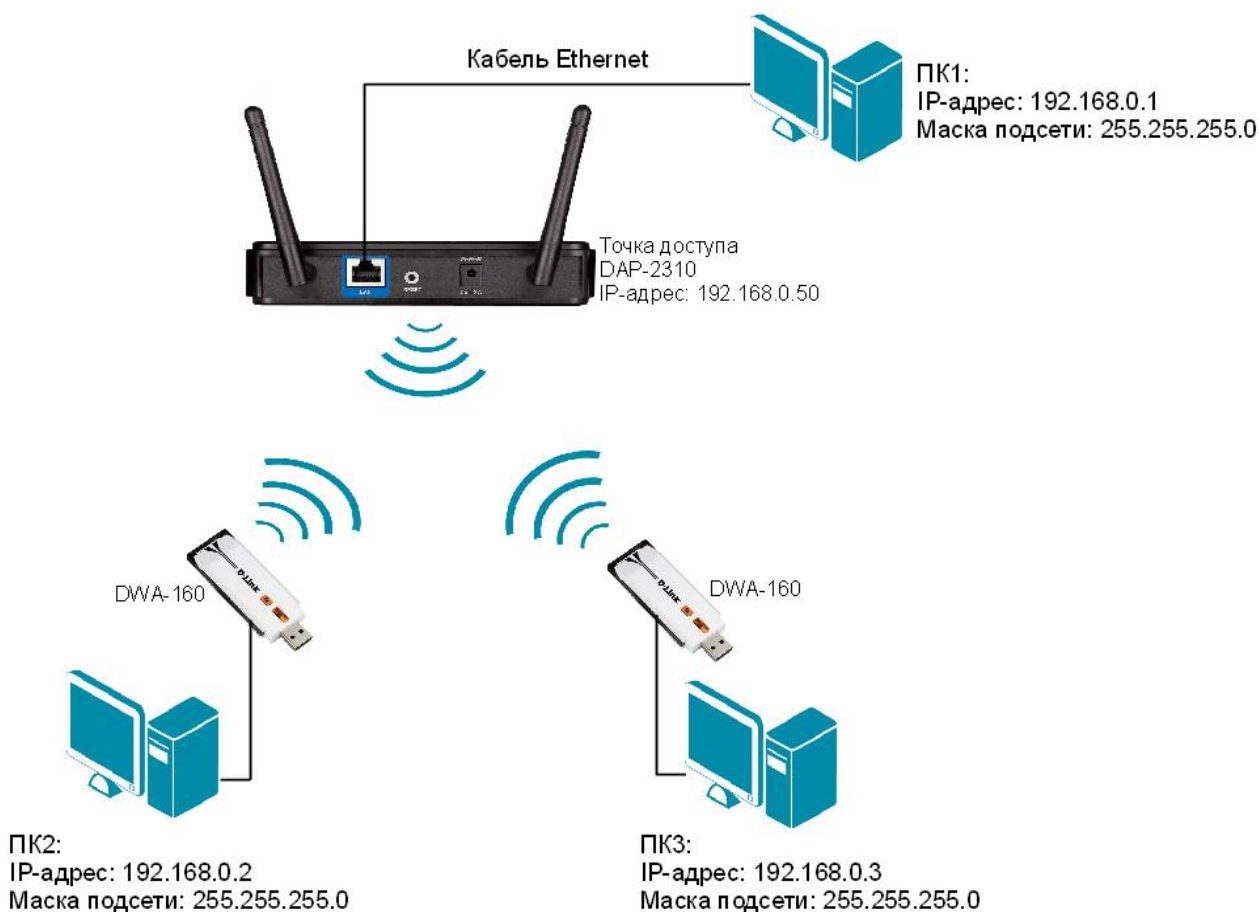


Рисунок 7.35 Схема подключения оборудования в инфраструктурном режиме

Шаг 1. Перед выполнением задания необходимо сбросить настройки точки доступа к заводским настройкам по умолчанию. Для этого подключите точку доступа к адаптеру питания и удерживайте в течение 10 секунд кнопку *Reset*, расположенную на задней панели устройства (рис. 7.36).



Рисунок 7.36 Расположение кнопки Reset на точке доступа DAP-2310

Шаг 2. Подключите один конец Ethernet-кабеля к LAN-порту точки доступа DAP-2310, а другой — к сетевому адаптеру рабочей станции ПК1, как показано на рисунке 7.35.

Шаг 3. Подключите беспроводной адаптер DWA-160 к USB-порту рабочей станции ПК2 и ПК3.

Шаг 4. Настройте статический IP-адрес на рабочей станции ПК1.

Шаг 5. Проверьте соединение между ПК1 и точкой доступа с помощью команды ping:

В командной строке ПК1 введите: ping 192.168.0.50

Внимание: IP-адрес управления точки доступа по умолчанию обычно указывается в руководстве пользователя. Для точки доступа D-Link DAP-2310 IP-адрес управления по умолчанию — 192.168.0.50

Шаг 6. Зайдите на Web-интерфейс точки доступа.

Чтобы зайти на Web-интерфейс точки доступа, выполните следующие действия:

1. На рабочей станции ПК1 запустите Web-браузер (Internet Explorer, Mozilla Firefox), в адресной строке которого укажите IP-адрес интерфейса управления точки доступа по умолчанию: http://192.168.0.50

2. В появившемся окне аутентификации (рис. 7.37), в поле *User Name* введите *admin*, поле *Password* оставьте пустым и нажмите кнопку *Login*.

Внимание: Если на рабочей станции произведены настройки прокси-сервера, то их нужно отключить.

Для Mozilla Firefox: меню *Инструменты* → *Настройки* → *Дополнительные*. Далее вкладка *Сеть* → *Настройка параметров соединения Firefox с Интернетом* → *Настроить* → *Без прокси*.

Для Internet Explorer: меню *Сервис* → *Свойство обозревателя*. Далее вкладка *Подключения* → *Настройка сети* → *Автоматическое определение параметров*.

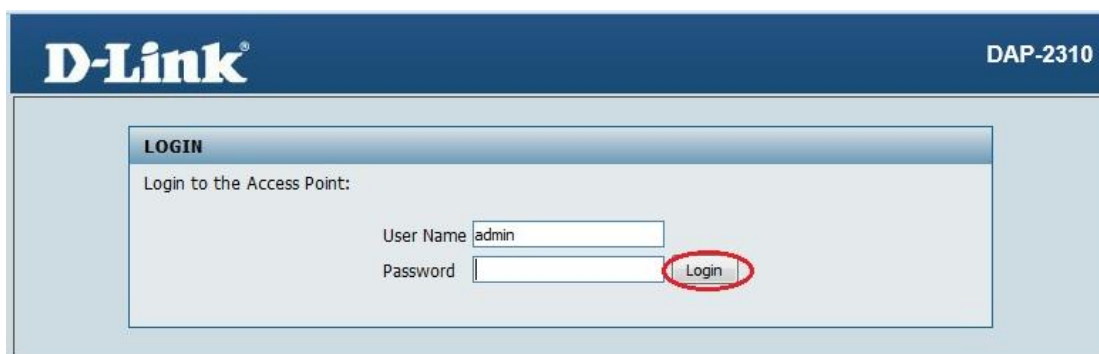


Рисунок 7.37 Окно аутентификации

После нажатия кнопки *Login* появится окно Web-интерфейса управления точки доступа (рис. 7.38).

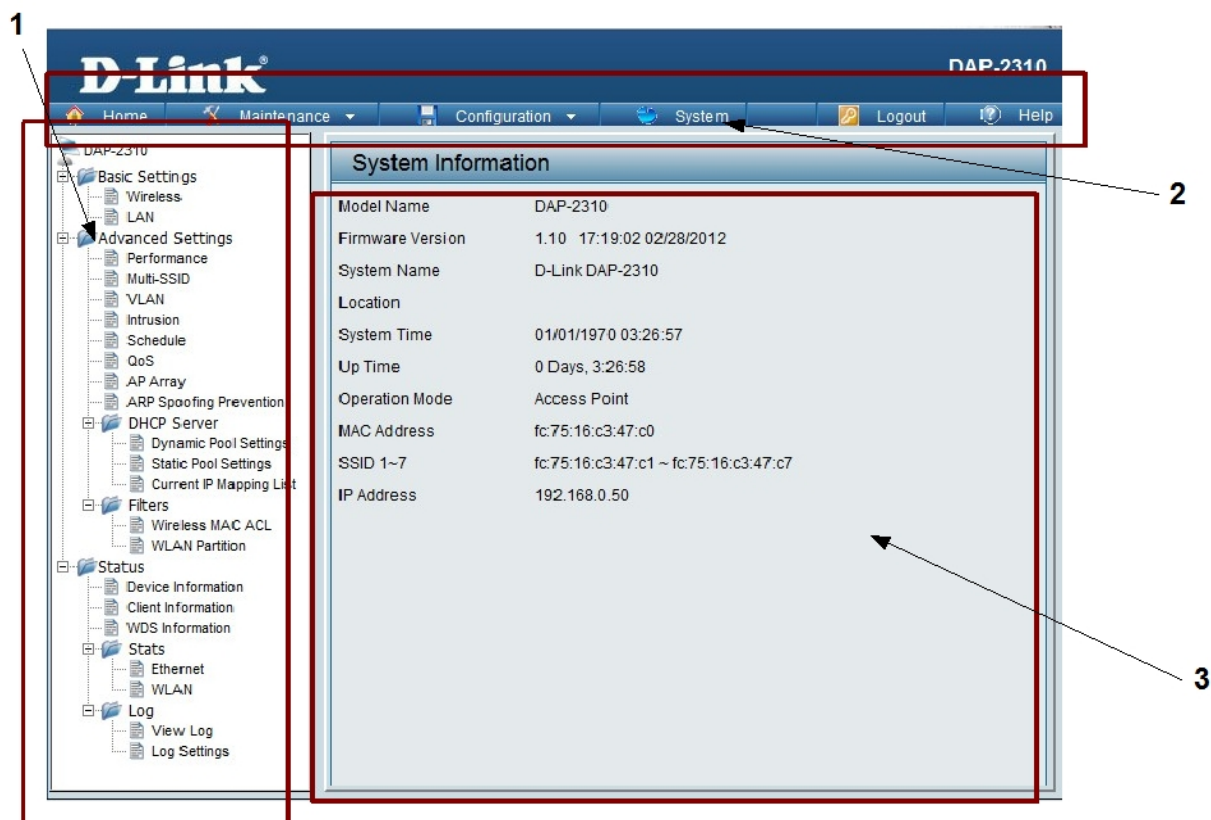


Рисунок 7.38 Web-интерфейс управления точки доступа

Условно Web-интерфейс точки доступа можно разделить на 3 области. Область 1 содержит список папок, объединяющих семейство настроек, предназначенных для выполнения той или иной задачи. В области 3 отображаются текущие настройки точки доступа и поля для их изменения (не для всех пунктов меню). В области 2 осуществляется доступ к настройкам *Administration Settings*, *Firmware and SSL Certification Upload*, *Configuration File* (пункт меню Maintenance), *Save and Activate*, *Discard Changes* (пункт меню Configuration), *System Settings* (пункт меню System).

Шаг 7. Измените IP-адрес управления точки доступа (рис. 7.39). В области 1 выберите папку *Basic Settings* → *LAN*. В области 3 введите:

Get IP From: Static IP (Manual)

IP Address: 192.168.0.51

Subnet Mask: 255.255.255.0

Поле *Default Gateway* оставьте пустым.

Нажмите кнопку *Save*.

Рисунок 7.39 Изменение IP-адреса управления точки доступа

Шаг 8. Сохраните и активируйте сделанные настройки точки доступа. Для этого в области 2 выберите *Configuration* → *Save and Activate* (рис. 7.40). Подождите 60 секунд, пока точка доступа перезагрузится, затем в адресной строке Web-браузера введите новый IP-адрес управления точки доступа:
`http://192.168.0.51`

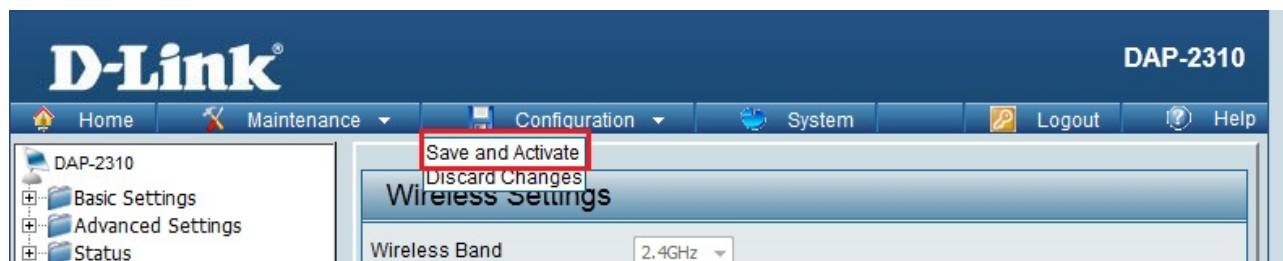


Рисунок 7.40 Сохранение настроек

Шаг 9. Настройте режим *Access Point*, чтобы рабочие станции могли взаимодействовать между собой через точку доступа. Для этого выполните следующие действия (рис. 7.41):

1. Выберите папку *Basic Settings* → *Wireless*;
2. В поле *Mode* выберите *Access Point*;
3. В поле *Network Name (SSID)* введите *class_test* (по умолчанию имя беспроводной сети *dlink*);
4. Отключите автоматический выбор канала. В поле *Auto Channel Selection* выберите *Disable*;
5. В поле *Channel* выберите *6*;
6. Настройте тип шифрования беспроводной сети. В поле *Authentication* выберите *WPA-Personal*;
7. В поле *PassPhrase* введите пароль *DlinkPassword*;
8. В поле *ConfirmPassPhrase* повторите пароль *DlinkPassword*;
9. Для сохранения настроек нажмите кнопку *Save*.

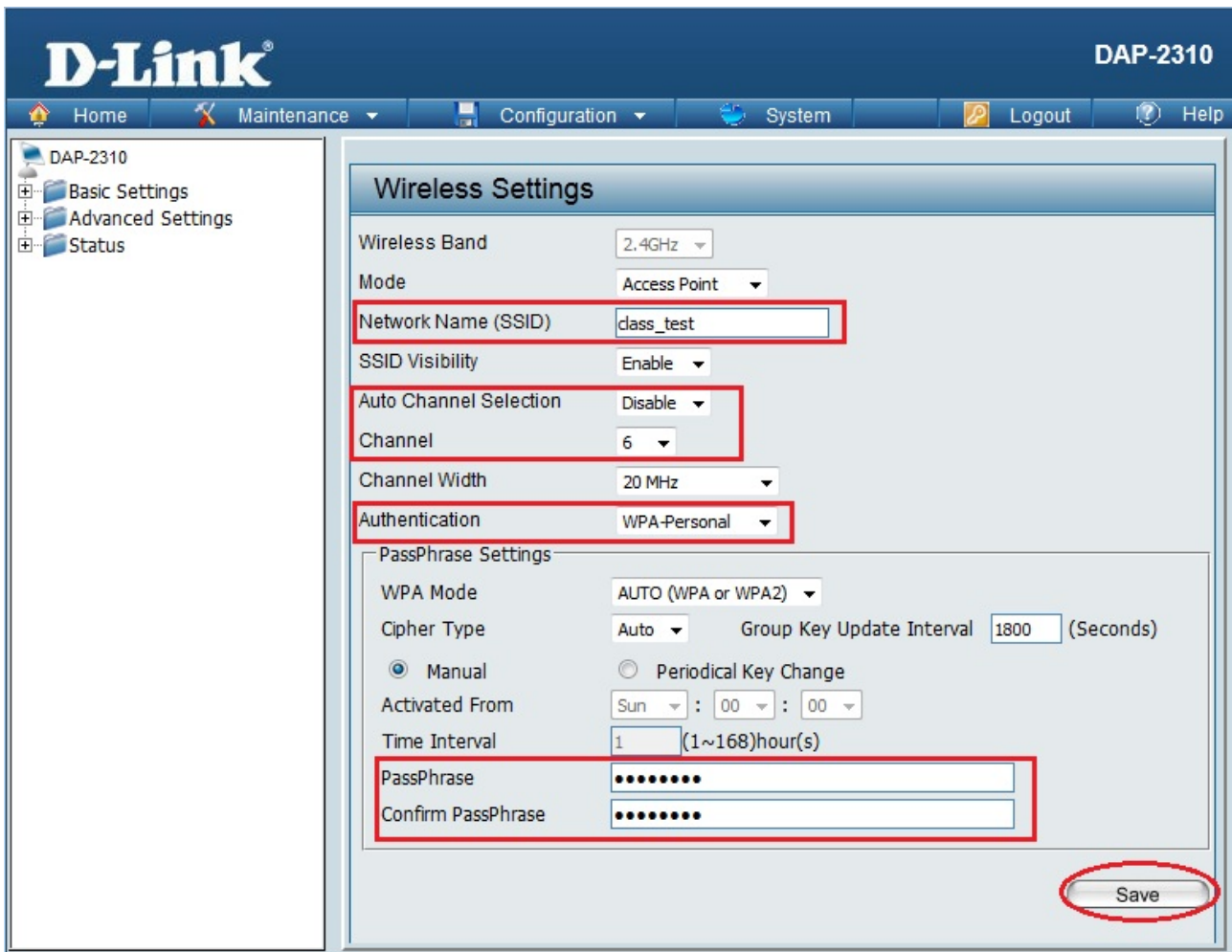


Рисунок 7.41 Настройка точки доступа в режиме *Access Point*

Шаг 10. Сохраните и активируйте сделанные настройки точки доступа. Для этого в области 2 выберите *Configuration* → *Save and Activate*. Дождитесь перезагрузки точки доступа.

Шаг 11. Настройте статический IP-адрес на беспроводном интерфейсе ПК2 и ПК3.

Настройка IP-адреса на рабочей станции с ОС Windows XP:

1. Откройте *Сетевые подключения*;

Пуск → *Панель управления* → *Сетевые подключения* → *Беспроводное сетевое соединение*

2. Щелкните правой кнопкой мыши на *Беспроводное сетевое соединение* и выберите *Свойства*;

3. В диалоговом окне выберите *Протокол Интернета (TCP/IP)* и нажмите *Свойства*;

4. Выберите *Использовать следующий IP-адрес*;

5. В поле *IP-адрес* введите: 192.168.0.2 (для ПК2) или 192.168.0.3 (для ПК3);

6. В поле *Маска подсети* введите: 255.255.255.0;

7. Нажмите кнопку *Ок*.

Настройка IP-адреса на рабочей станции с ОС Windows 7/Vista:

1. Откройте *Изменение параметров адаптера*;

Пуск → *Панель управления* → *Центр управления сетями и общим доступом* → *Изменение параметров адаптера*

2. Щелкните правой кнопкой мыши по *Беспроводное сетевое соединение* и выберите *Свойства*;
3. В диалоговом окне выберите *Протокол Интернета 4 (TCP/IP)* и нажмите *Свойства*;
4. Выберите *Использовать следующий IP-адрес*;
5. В поле *IP-адрес* введите: 192.168.0.1(для ПК2) или 192.168.0.3 (для ПК3);
6. В поле *Маска подсети* введите: 255.255.255.0;
7. Нажмите кнопку *Ок*.

Шаг 12. Запустите утилиту *D-Link Connection Manager* на рабочей станции ПК2 и ПК3. Если драйвер для DWA-160 и утилита не установлены, то проделайте шаги, которые описаны в пункте 7.1.

Шаг 13. Из списка доступных беспроводных сетей выберите сеть с именем (SSID) *class_test* и нажмите кнопку *Подключить*. Если в списке не отображается беспроводная сеть *class_test*, нажмите кнопку *Обновить*.

Шаг 14. Проверьте соединение между рабочими станциями ПК2 и ПК3 с помощью команды ping:

В командной строке ПК2 введите: ping 192.168.0.3

Ответил ПК3? _____

В командной строке ПК3 введите: ping 192.168.0.2

Ответил ПК2? _____

Шаг 15. Посмотрите информацию о клиентах, подключенных через точку доступа. На рабочей станции ПК1 зайдите на Web-интерфейс точки доступа, выберите папку *Status* → *Client Information* (рис. 7.42).

Client Information						
Client Information Station association (2.4GHz) : 2						
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	
Primary SSID	7C:E9:D3:28:10:B2	N	WPA2-PSK	94%	On	
Primary SSID	00:24:03:F9:B4:0F	G	WPA2-PSK	53%	On	

Рисунок 7.42 Информация о клиентах, подключенных к беспроводной сети *class_test* через точку доступа

Шаг 16. Посмотрите MAC-адрес рабочей станции ПК2. В командной строке введите: getmac

Запишите MAC-адрес ПК2 _____

Шаг 17. Посмотрите MAC-адрес рабочей станции ПК3. В командной строке введите: getmac

Запишите MAC-адрес ПК3 _____

классу С.

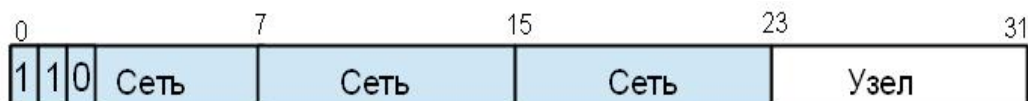


Рисунок 8.4 Формат IPv4-адреса класса С

Кроме IP-адреса сетевому узлу назначается маска подсети. *Маска подсети* – это 32-битное число, двоичная запись которого содержит единицы в тех разрядах, которые должны определяться как идентификатор сети. Поскольку идентификатор сети является частью IPv4-адреса, последовательность единиц в маске подсети должна быть также непрерывной.

Для сетей класса А, В и С определены фиксированные маски подсети, которые жестко определяют количество возможных IPv4-адресов и механизм маршрутизации (таблица 8.1).

Таблица 8.1 Маски подсети для стандартных классов сетей

Класс сети	Маска подсети	Количество бит под идентификатор сети
Класс А	255.0.0.0	8
Класс В	255.255.0.0	16
Класс С	255.255.255.0	24

При применении масок подсети сети можно разделять на меньшие по размеру подсети путем расширения сетевой части адреса и уменьшения узловой части. Технология разделения сети дает возможность создавать большее число сетей с меньшим количеством узлов в них, что позволяет эффективно использовать адресное пространство.

Для вычисления количества подсетей используется формула 2^s , где s – количество бит, занятых под идентификатор сети из части, отведенной под идентификатор узла. Количество узлов в каждой подсети вычисляется по формуле $2^n - 2$, где n – количество бит, оставшихся в части, идентифицирующей узел, а два адреса – *адрес сети* и *широковещательный адрес* – в каждой полученной подсети зарезервированы. Эти адреса не могут быть назначены конкретному узлу.

IPv4-адрес назначения, в узловой части которого присутствуют только единицы, называется *широковещательным*. Пакет с таким адресом получают и обрабатывают все узлы в текущей локальной сети. Если узловая часть IP-адреса содержит только нули, этот адрес является *адресом сети*.

В *бесклассовой модели IP-адресации* отсутствует привязка к классу сети и маске подсети по умолчанию. Бесклассовая адресация использует *маски подсети переменной длины (Variable Length Subnet Mask, VLSM)* и *технологии бесклассовой междоменной маршрутизации (Classless Inter Domain Routing, CIDR)*. Термин «маска переменной длины» означает, что сеть может быть разбита на подсети с различными масками подсети. Основная идея применения VLSM заключается в том, что можно разбить сеть на подсеть, потом подсеть разбить еще на подсети точно таким же образом, как была разбита первоначальная сеть. То есть сеть может быть разбита на подсети разных размеров, с разными масками. Маски подсети являются основой метода бесклассовой маршрутизации и записываются в виде нотации «IP-адрес/длина префикса». Число после «/» означает количество единичных разрядов в маске подсети. Например, сетевой адрес 192.168.1.8 с маской подсети 255.255.255.248 также может быть записан, как 192.168.1.8/29. Число 29 указывает, что в маске подсети 255.255.255.248 29 единичных бит.

Цель:

- научиться определять адрес сети и адрес узла по маске подсети;
- научиться определять количество узлов и диапазон адресов в заданной сети;
- научиться формировать подсети с использованием маски подсети.

8.1 Определение адреса сети, широковещательного адреса и количества узлов по заданному IP-адресу и маске подсети

ПРИМЕР

По IP-адресу узла **10.193.68.59** и маске подсети **255.255.248.0** определите:

Таблица 8.2

Адрес сети (десятичное представление)	
Адрес сети (двоичное представление)	
Широковещательный адрес (десятичное представление)	
Широковещательный адрес (двоичное представление)	
IP-адрес первого узла подсети (десятичное представление)	
IP-адрес последнего узла подсети (десятичное представление)	
Количество узлов в подсети (десятичное представление)	

Шаг 1. Переведите IP-адрес узла и маску подсети в двоичный вид (рис. 8.5).

	10	193	68	59
IP-адрес узла	00001010	11000001	01000100	00111011
Маска подсети	11111111	11111111	11111000	00000000
	255	255	248	0

Рисунок 8.5 Перевод IP-адреса и маски подсети из десятичного представления в двоичное

Шаг 2. Определите адрес сети. Для этого примените к IP-адресу и маске подсети операцию логическое «И» (&), показанную на рисунке 8.6. Результат запишите в таблицу.

Примечание: $1 \& 1 = 1$; $1 \& 0 = 0$; $0 \& 0 = 0$.

IP-адрес узла	00001010	11000001	01000100	00111011	10.193.68.59
					&
Маска подсети	11111111	11111111	11111000	00000000	255.255.248.0
Адрес сети	00001010	11000001	01000000	00000000	10.193.64.0

Рисунок 8.6 Определение адреса сети

Шаг 3. Определите широковещательный адрес подсети (рис. 8.7) и запишите результат в таблицу.

Маска подсети позволяет определить, какая часть адреса указывает на идентификатор подсети, а какая на идентификатор узла. *Широковещательный адрес* содержит единицы в тех разрядах, которые должны определяться как идентификатор узла.

IP-адрес узла	00001010	11000001	01000100	00111011	10.193.68.59
Маска подсети	11111111	11111111	11111000	00000000	255.255.248.0
Широковещательный адрес	00001010	11000001	01000111	11111111	10.193.71.255

Рисунок 8.7 Определение широковещательного адреса

Шаг 4. Определите IP-адрес первого узла подсети и запишите результат в таблицу. Этот IP-адрес всегда на единицу больше адреса сети (рис. 8.8).

Адрес сети	00001010	11000001	01000000	00000000	10.193.64.0
Маска подсети	11111111	11111111	11111000	00000000	255.255.248.0
Первый IP-адрес подсети	00001010	11000001	01000000	00000001	10.193.64.1

Рисунок 8.8 Определение первого IP-адреса подсети

Шаг 5. Определите IP-адрес последнего узла подсети. Этот IP-адрес всегда на единицу меньше широковещательного адреса подсети (рис. 8.9).

Адрес сети	00001010	11000001	01000000	00000000	10.193.64.0
Маска подсети	11111111	11111111	11111000	00000000	255.255.248.0
Широковещательный адрес	00001010	11000001	01000111	11111111	10.193.71.255
Последний IP-адрес подсети	00001010	11000001	01000111	11111110	10.193.71.254

Рисунок 8.9 Определение последнего IP-адреса подсети

Шаг 6. Определите количество узлов в подсети и запишите результат в таблицу. Количество узлов в подсети вычисляется по формуле $2^n - 2$, где n – количество бит, оставшихся в части, идентифицирующей узел, а два адреса – адрес сети и широковещательный адрес не могут быть назначены узлу (рис. 8.10).

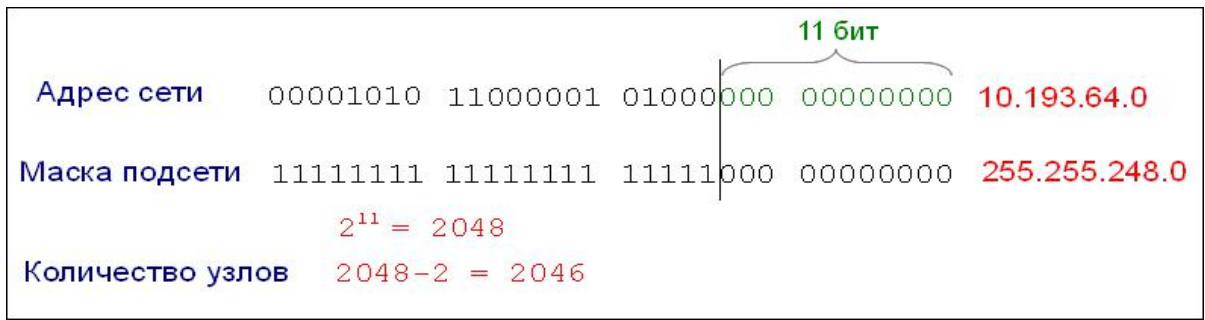


Рисунок 8.10 Определение количества узлов в подсети

ЗАДАНИЕ 1

По IP-адресу узла **172.30.1.33** и маске подсети **255.255.224.0** определите:

Таблица 8.3

Адрес сети (десятичное представление)	
Адрес сети (двоичное представление)	
Широковещательный адрес (десятичное представление)	
Широковещательный адрес (двоичное представление)	
IP-адрес первого узла подсети (десятичное представление)	
IP-адрес последнего узла подсети (десятичное представление)	
Количество узлов в подсети (десятичное представление)	

ЗАДАНИЕ 2

По IP-адресу узла **192.168.100.234** и маске подсети **255.255.192.0** определите:

Таблица 8.4

<i>Адрес сети</i> (десятичное представление)	
<i>Адрес сети</i> (двоичное представление)	
<i>Широковещательный адрес</i> (десятичное представление)	
<i>Широковещательный адрес</i> (двоичное представление)	
<i>IP-адрес первого узла подсети</i> (десятичное представление)	
<i>IP-адрес последнего узла подсети</i> (десятичное представление)	
<i>Количество узлов в подсети</i> (десятичное представление)	

ЗАДАНИЕ 3

По IP-адресу узла **172.17.99.171** и маске подсети **255.255.255.240** определите:

Таблица 8.5

<i>Адрес сети</i> (десятичное представление)	
<i>Адрес сети</i> (двоичное представление)	
<i>Широковещательный адрес</i> (десятичное представление)	
<i>Широковещательный адрес</i> (двоичное представление)	
<i>IP-адрес первого узла подсети</i> (десятичное представление)	
<i>IP-адрес последнего узла подсети</i> (десятичное представление)	
<i>Количество узлов в подсети</i> (десятичное представление)	

Организации требуется создать подсеть **172.16.0.0**, в которой должно быть **1000** узлов. Какую маску подсети необходимо использовать? _____

Организации требуется создать подсеть **192.168.12.0**, в которой должно быть **55** узлов. Какую маску подсети необходимо использовать? _____

8.2 Формирование подсетей с использованием масок переменной длины (VLSM)

ПРИМЕР

Организации выделена сеть класса C **192.168.1.0/24**. Требуется разделить данную сеть на 6 подсетей. В подсетях 1, 2, 3 и 4 должно быть 10 узлов, в 5-й подсети – 50 узлов, в 6-й подсети – 100 узлов.

Шаг 1. Разделите сеть 192.168.1.0/24 на две подсети (рис. 8.11). Для этого из 4-го октета займите 1 бит для идентификатора подсети. Таким образом, для идентификации узлов остается 7 бит. В итоге получится две подсети 192.168.1.0/25 и 192.168.1.128/25, в каждой из которых может быть по 126 узлов (не забывайте про два зарезервированных адреса, которые не могут быть назначены узлам — это адрес сети и широковещательный адрес).



Рисунок 8.11 Деление сети 192.168.1.0/24 на две подсети

Шаг 2. Разделите подсеть 192.168.1.128/25 еще на две подсети (рис. 8.12). Для этого займите 1 бит из оставшихся 7 бит, отведенных под идентификатор узла. Таким образом, получится две подсети 192.168.1.128/26 и 192.168.1.192/26, в каждой из которых допустимое количество узлов равно 62.



Рисунок 8.12 Деление сети 192.168.1.128/25 на две подсети

Шаг 3. Разделите подсеть 192.168.1.192/26 на четыре подсети (рис. 8.13). Для этого займите 2 бита из оставшихся 6 бит, отведенных под идентификатор узла. В результате получится четыре подсети с 14 узлами в каждой, это позволит адресовать требуемое количество узлов, необходимых для подсетей 1, 2, 3 и 4.

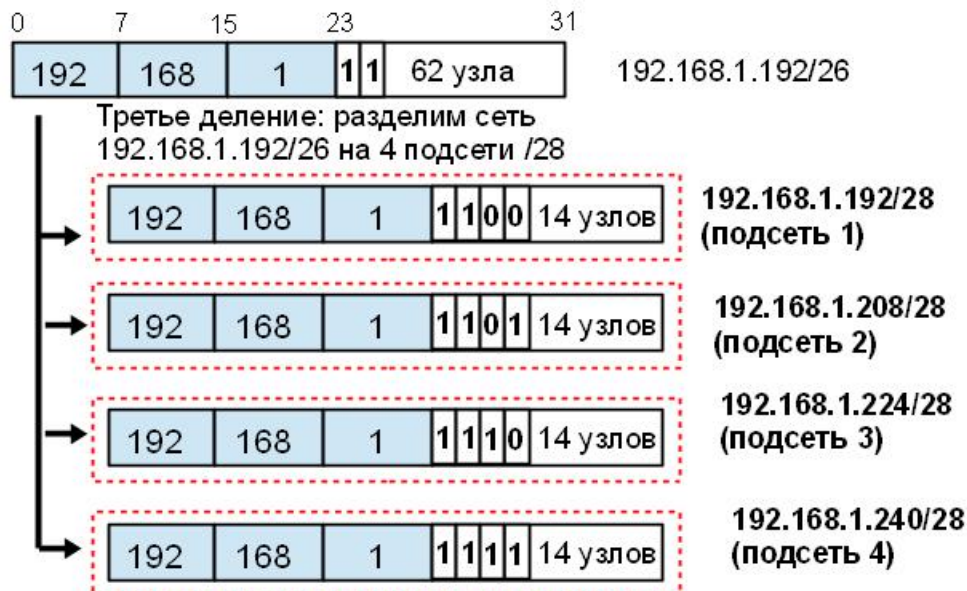


Рисунок 8.13 Деление сети 192.168.1.192/26 на четыре подсети

Результаты запишите в таблицу 8.6:

Таблица 8.6

Номер подсети	Адрес подсети/префикс	Количество узлов
1	192.168.1.192/28	14
2	192.168.1.208/28	14
3	192.168.1.224/28	14
4	192.168.1.240/28	14
5	192.168.1.128/26	62
6	192.168.1.0/25	126

ЗАДАНИЕ 1

Организации выделена сеть класса В **185.210.0.0/16**. Требуется разделить данную сеть на 256 подсетей. Определите количество узлов в каждой подсети. Укажите адрес Подсети 1 и Подсети 2. Результат запишите в таблицу 8.7.

Таблица 8.7

Номер подсети	Адрес подсети/префикс	Количество узлов
1		
256		

Сколько бит необходимо занять от идентификатора узла, чтобы организовать 256 подсетей?

Как определить максимальное число узлов в каждой подсети? _____

ЗАДАНИЕ 2

Организации выделена сеть класса С **212.100.54.0/24**. Требуется разделить данную сеть на 7 подсетей. В подсетях 1, 2, 3 и 4 должно быть 2 узла, в 5-й подсети – 10 узлов, в 6-й подсети – 26 узлов, в 7-ой подсети – 58 узлов. Результаты запишите в таблицу 8.8.

Таблица 8.8

Номер подсети	Адрес подсети/префикс	Количество узлов
1		
2		
3		
4		
5		
6		
7		

Можно сеть 212.100.254.124/30 разделить на 2 подсети? Ответ обоснуйте _____

Может маска подсети быть 255.254.128.0? Ответ обоснуйте _____

Можно назначить рабочей станции IP-адрес 160.54.255.255? Ответ обоснуйте _____

Какая маска подсети для IP-адресов класса А? _____

8.3 Формирование подсетей IPv6

ПРИМЕР

Организация использует в своей сети уникальные локальные адреса (Unique-Local Unicast). Требуется разделить сеть на 5 подсетей.

Шаг 1. Сформируйте 64-битный префикс сети. Уникальные локальные адреса начинаются с префикса FD00::/8.

Шаг 2. С помощью генератора локальных адресов IPv6 получите Global ID (40 бит), например 895a473947. Алгоритм для генерации уникального локального адреса можно найти в сети Интернет — <https://www.ultratools.com/tools/rangeGenerator>

Шаг 3. Назначьте 5 номеров подсети (Subnet ID) разрядностью 16 бит, при этом также можно воспользоваться генератором для получения номера подсети.

Результат запишите в таблицу 8.9:

Таблица 8.9

Номер подсети	Префикс сети	Диапазон адресов
710	fd89:5a47:3947:0710::/64	fd89:5a47:3947:710:0:0:0:0 – fd89:5a47:3947:710:ffff:ffff:ffff:ffff
711	fd89:5a47:3947:0711::/64	fd89:5a47:3947:711:0:0:0:0 – fd89:5a47:3947:711:ffff:ffff:ffff:ffff
712	fd89:5a47:3947:0712::/64	fd89:5a47:3947:712:0:0:0:0 – fd89:5a47:3947:712:ffff:ffff:ffff:ffff
713	fd89:5a47:3947:0713::/64	fd89:5a47:3947:713:0:0:0:0 – fd89:5a47:3947:713:ffff:ffff:ffff:ffff
714	fd89:5a47:3947:0714::/64	fd89:5a47:3947:714:0:0:0:0 – fd89:5a47:3947:714:ffff:ffff:ffff:ffff

ЗАДАНИЕ 1

Организация использует в своей сети уникальные локальные адреса (Unique-Local Unicast). Требуется разделить сеть на 7 подсетей. Результат запишите в таблицу 8.10.

Таблица 8.10

Номер подсети	Префикс сети	Диапазон адресов

Определите широковещательный адрес для подсети fd89:5a47:3947:0710::/64? _____

Лабораторная работа №9. Установка и настройка протокола IPv6 на рабочей станции и точке доступа D-Link

Протокол IPv6 — новая версия протокола IP, которая разработана в качестве преемника IPv4 и призвана решить проблему исчерпания адресного пространства. Основным отличием IPv6 от IPv4 является:

- большое адресное пространство (2^{128} адресов);
- улучшенные механизмы по автоматической настройке узлов;
- упрощение маршрутизации;
- улучшенные механизмы обеспечения качества обслуживания (QoS);
- упрощенный заголовок пакета.

Адрес IPv6 имеет длину 128 бит и состоит из двух логических частей - *префикса* и *идентификатора*. Отображается адрес как восемь групп по четыре шестнадцатеричные цифры, разделенные двоеточием. Например, ABCD:EF01:2345:6789:ABCD:EF01:2345:6789.

Префикс (64 бита) — это часть адреса, которая указывает количество фиксированных бит, отведенных под идентификатор сети/подсети (аналог адреса сети в IPv4).

Идентификатор (64 бита) — последние 64 бита адреса IPv6, используемые для идентификации интерфейса в сегменте сети (аналог адреса узла в IPv4), он должен быть уникальным внутри сети/подсети.

Идентификатор интерфейса может быть получен следующими способами:

- сформирован из 48-битного MAC-адреса путем конвертации в формат Modified EUI-64;
- сгенерирован автоматически случайным образом;
- настроен вручную;
- назначен с помощью протокола DHCP.

Существует три типа адресов IPv6:

- индивидуальный (unicast);
- групповой (multicast);
- альтернативный (anycast).

Индивидуальные адреса служат для идентификации одного интерфейса и разделяются на несколько видов:

- *Link-Local Unicast* - предназначены для коммуникаций в пределах одного сегмента сети или линии связи «точка-точка» и имеют значение только в пределах данной линии связи. Все адреса Link-Local начинаются с префикса FE80::/10;
- *Unique-Local Unicast* - предназначены для адресации внутри сети организации. Пакеты с адресами Unique-Local в качестве адреса источника или назначения не маршрутизируются через Интернет, они маршрутизируются только внутри сети организации (аналог частных адресов IPv4). Все адреса Unique-Local начинаются с префикса FC00::/7. Алгоритм для генерации уникального локального адреса можно найти в сети интернет <https://www.ultratools.com/tools/rangeGenerator>;
- *Global Unicast* — эти адреса выдаются локальными регистраторами и используются для идентификации узлов в глобальной сети (аналог глобальных адресов IPv4). В настоящее время назначаются адреса из диапазона 2000::/3.

В отличие от IPv4, где настройка параметров узла проводилась либо вручную, либо с помощью протокола DHCP, в IPv6 узел может практически самостоятельно сконфигурировать параметры своих интерфейсов. В IPv6 определены два механизма автоконфигурации:

- *Stateless autoconfiguration* - позволяет узлам генерировать свой собственный адрес на основе комбинации локально доступной информации и информации, объявляемой маршрутизаторами. Маршрутизаторы объявляют префиксы, идентифицирующие подсеть/и, а узлы генерируют идентификаторы интерфейсов. В отсутствие маршрутизатора узлы могут автоматически генерировать канальный IPv6-адрес (Link-Local Unicast);

- *Stateful autoconfiguration* - узлы получают адрес интерфейса и/или конфигурационную информацию и параметры от сервера с помощью протокола DHCPv6.

Stateless и stateful autoconfiguration дополняют друг друга. Они могут использоваться одновременно.

Ручная настройка для конфигурации интерфейсов узлов может использоваться:

- если в сети нет маршрутизаторов, которые рассылают объявления с информацией, требуемой для автоматической конфигурации.
- в случае обнаружения дублирования адресов при автоматической конфигурации узлов.

Цель: изучить настройку протокола IPv6 на рабочей станции и на точке доступа D-Link DAP-2310.

Оборудование (на 1 рабочее место):

Рабочая станция	1 шт.
Кабель Ethernet	1 шт.
Точка доступа DAP-2310	1 шт.

9.1 Установка и настройка протокола IPv6 на рабочей станции

Шаг 1. Установите протокол IPv6 на рабочей станции.

Чтобы установить протокол IPv6 на рабочей станции с ОС Windows XP, выполните следующие действия (рис. 9.1):

1. Откройте *Сетевые подключения*;

Пуск → Панель управления → Сетевые подключения

2. Щелкните правой кнопкой мыши *Подключение по локальной сети* и выберите *Свойства*;
3. Во вкладке *Общие* установите галочку *Microsoft TCP/IP версии 6*;
4. Нажмите кнопку *Ок*.

Примечание: Windows XP поддерживает протокол IPv6 в экспериментальном варианте.

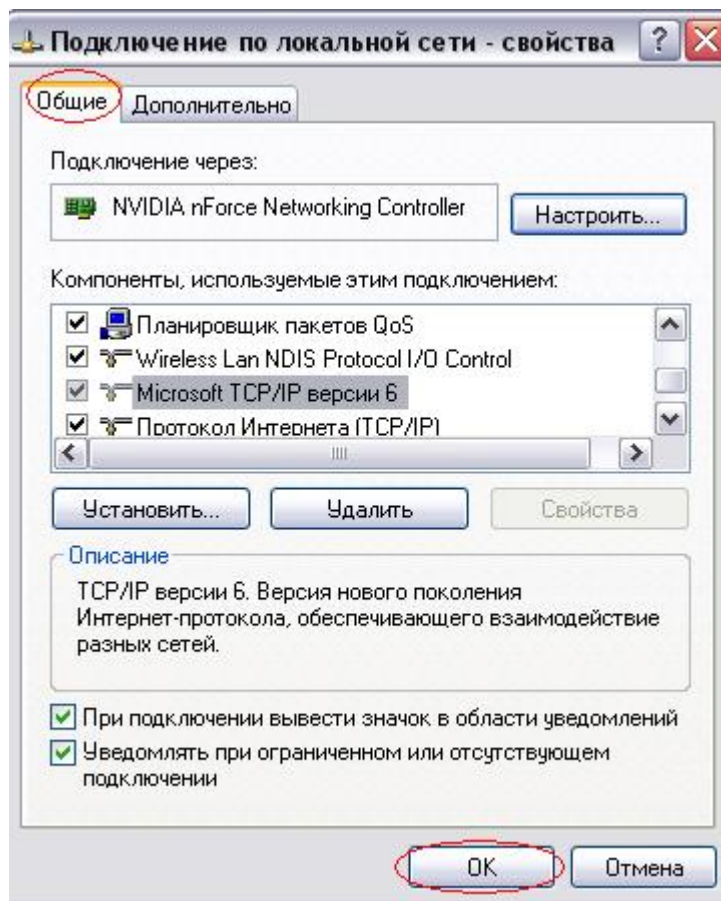


Рисунок 9.1 Установка протокола IPv6 на рабочей станции с ОС Windows XP

Чтобы установить протокол IPv6 на рабочей станции с ОС Windows 7/Vista, выполните следующие действия:

1. Откройте *Изменение параметров адаптера*;

Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера

2. Щелкните правой кнопкой мыши *Подключение по локальной сети* и выберите *Свойства*;

3. Нажмите кнопку *Установить* (рис. 9.2);

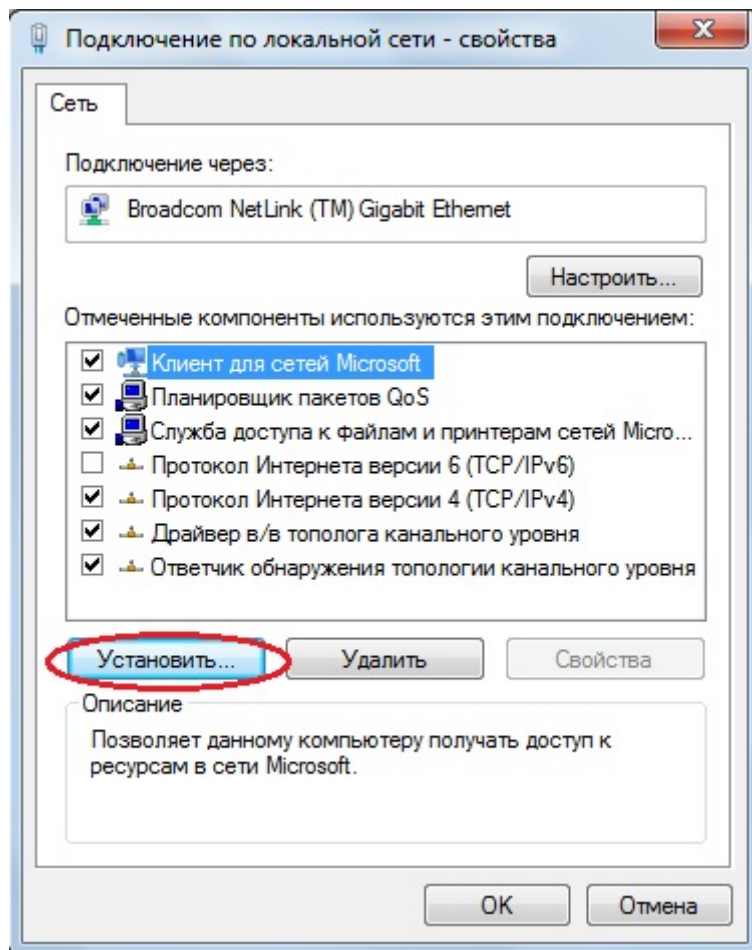


Рисунок 9.2

4. В диалоговом окне *Выбор сетевых компонентов* выберите строку *Протокол* и нажмите кнопку *Добавить* (рис. 9.3);

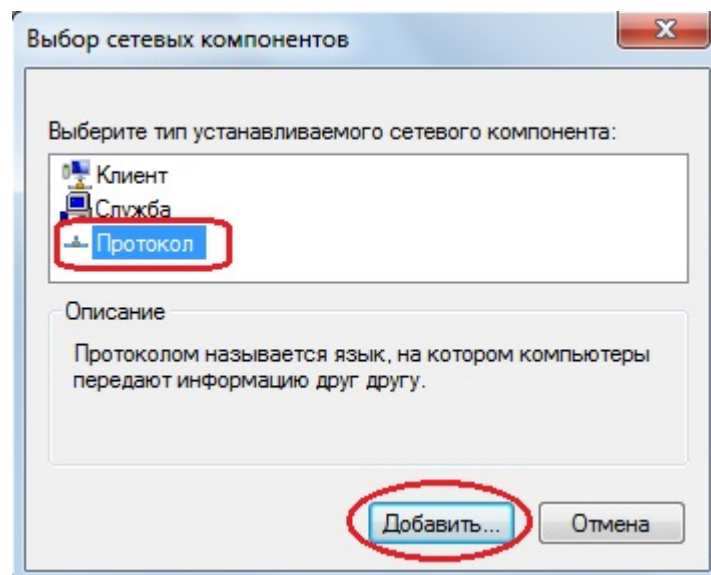


Рисунок 9.3

5. В диалоговом окне *Выбор сетевого протокола* выберите *Microsoft TCP/IP версия 6* и нажмите кнопку *Ок*.

Шаг 2. Проверьте конфигурацию сетевого адаптера. В командной строке введите `ipconfig`
Что вы наблюдаете? К какому типу адресов IPv6 относится наблюдаемый адрес? _____

Шаг 3. Настройте статический адрес IPv6 на рабочей станции.

Чтобы настроить статический адрес IPv6 на рабочей станции с ОС Windows 7/Vista, выполните следующие действия:

1. Откройте *Изменение параметров адаптера*;

Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера

2. Щелкните правой кнопкой мыши *Подключение по локальной сети* и выберите *Свойства*;

3. Во вкладке *Сеть* выберите *Протокол Интернета версии 6 (TCP/IPv6)* и нажмите кнопку *Свойства* (рис. 9.4);

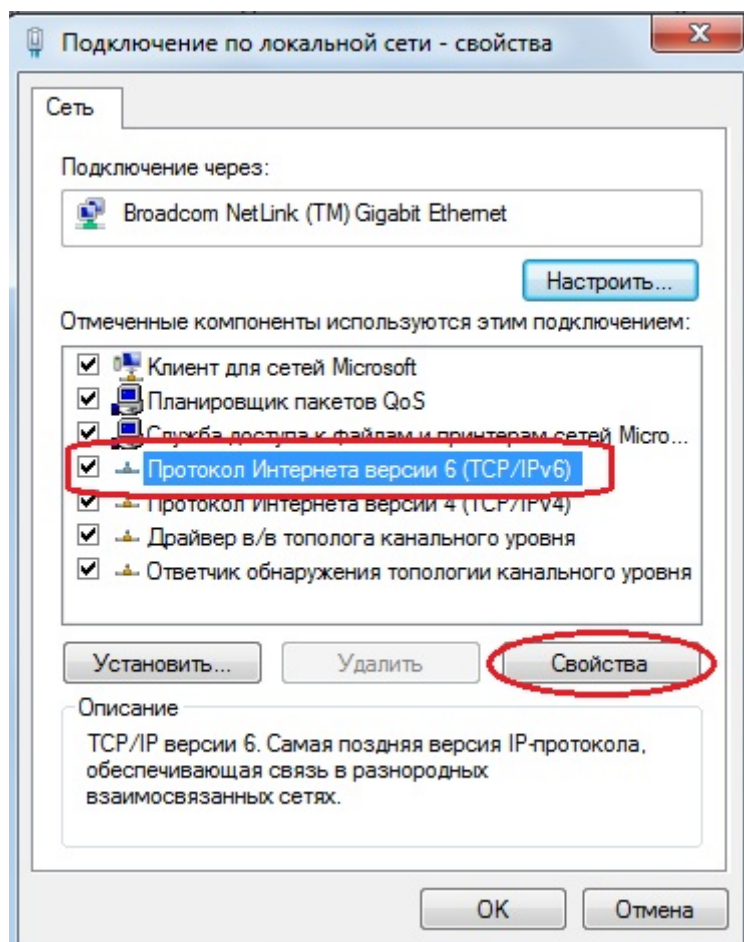


Рисунок 9.4

4. Выберите *Использовать следующий IPv6-адрес* (рис. 9.5);

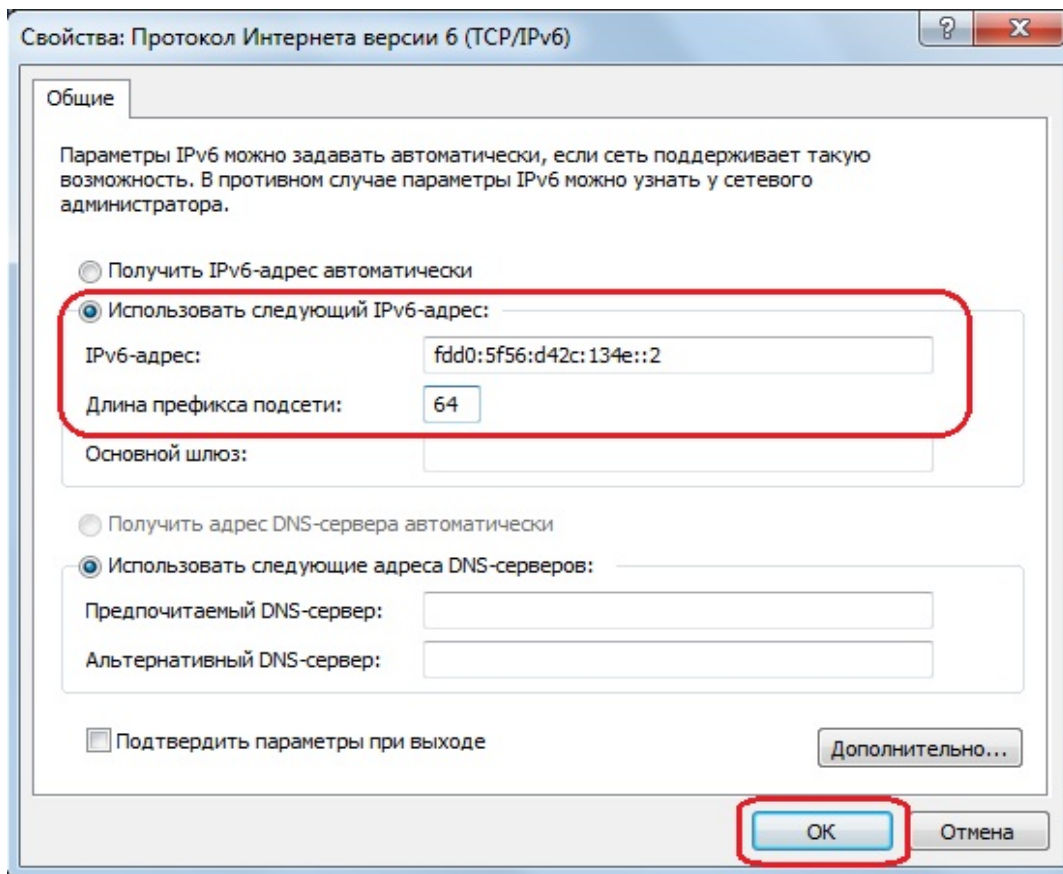


Рисунок 9.5 Настройка IPv6-адреса на рабочей станции

5. В поле *IPv6-адрес* введите: fdd0:5f56:d42c:134e::2;
6. В поле *Длина префикса подсети* введите: 64;
7. Нажмите кнопку *Ок*.

Шаг 4. Проверьте конфигурацию сетевого адаптера. В командной строке введите `ipconfig`

Что вы наблюдаете? К какому типу адресов IPv6 относятся наблюдаемые адреса? _____

9.2 Подключение к точке доступа через Web-интерфейс с помощью IPv6-адреса



Рисунок 9.6 Схема подключения

Шаг 1. Перед выполнением задания необходимо сбросить настройки точки доступа к заводским настройкам по умолчанию. Для этого подключите точку доступа к адаптеру питания и удерживайте в течение 10 секунд кнопку *Reset*, расположенную на задней панели

устройства.

Шаг 2. Подключите один конец Ethernet-кабеля к LAN-порту точки доступа DAP-2310, а другой — к сетевому адаптеру рабочей станции, как показано на рисунке 9.6.

Шаг 3. Настройте статический IP-адрес на рабочей станции.

Настройка IP-адреса на рабочей станции с ОС Windows XP:

1. Откройте *Сетевые подключения*;

Пуск → Панель управления → Сетевые подключения

2. Щелкните правой кнопкой мыши на *Подключение по локальной сети* и выберите *Свойства*;

3. В диалоговом окне выберите *Протокол Интернета (TCP/IP)* и нажмите *Свойства*;

4. Выберите *Использовать следующий IP-адрес*;

5. В поле *IP-адрес* введите: 192.168.0.1;

6. В поле *Маска подсети* введите: 255.255.255.0

7. Нажмите кнопку *Ок*.

Настройка IP-адреса на рабочей станции с ОС Windows 7/Vista:

1. Откройте *Изменение параметров адаптера*;

Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера

2. Щелкните правой кнопкой мыши на *Подключение по локальной сети* и выберите *Свойства*;

3. В диалоговом окне выберите *Протокол Интернета 4 (TCP/IP)* и нажмите *Свойства*;

4. Выберите *Использовать следующий IP-адрес*;

5. В поле *IP-адрес* введите: 192.168.0.1;

6. В поле *Маска подсети* введите: 255.255.255.0;

7. Нажмите кнопку *Ок*.

Шаг 4. Проверьте соединение между ПК1 и точкой доступа с помощью команды ping:

В командной строке ПК1 введите: ping 192.168.0.50

Шаг 5. Зайдите на Web-интерфейс точки доступа.

Чтобы зайти на Web-интерфейс точки доступа, выполните следующие действия:

1. На рабочей станции ПК1 запустите Web-браузер (Internet Explorer, Mozilla Firefox), в адресной строке которого укажите IP-адрес интерфейса управления точки доступа по умолчанию: http://192.168.0.50

2. В появившемся окне аутентификации в поле *User Name* введите *admin*, поле *Password* оставьте пустым и нажмите кнопку *Login*.

Шаг 6. Настройте Link-Local IPv6-адрес управления точки доступа. Выполните следующие действия (рис. 9.7):

1. Выберите папку *Basic Settings* → *IPv6*;

2. Установите галочку *Enable IPv6*;

3. В поле *Get IP From* выберите *Auto*;

4. Нажмите кнопку *Save*.

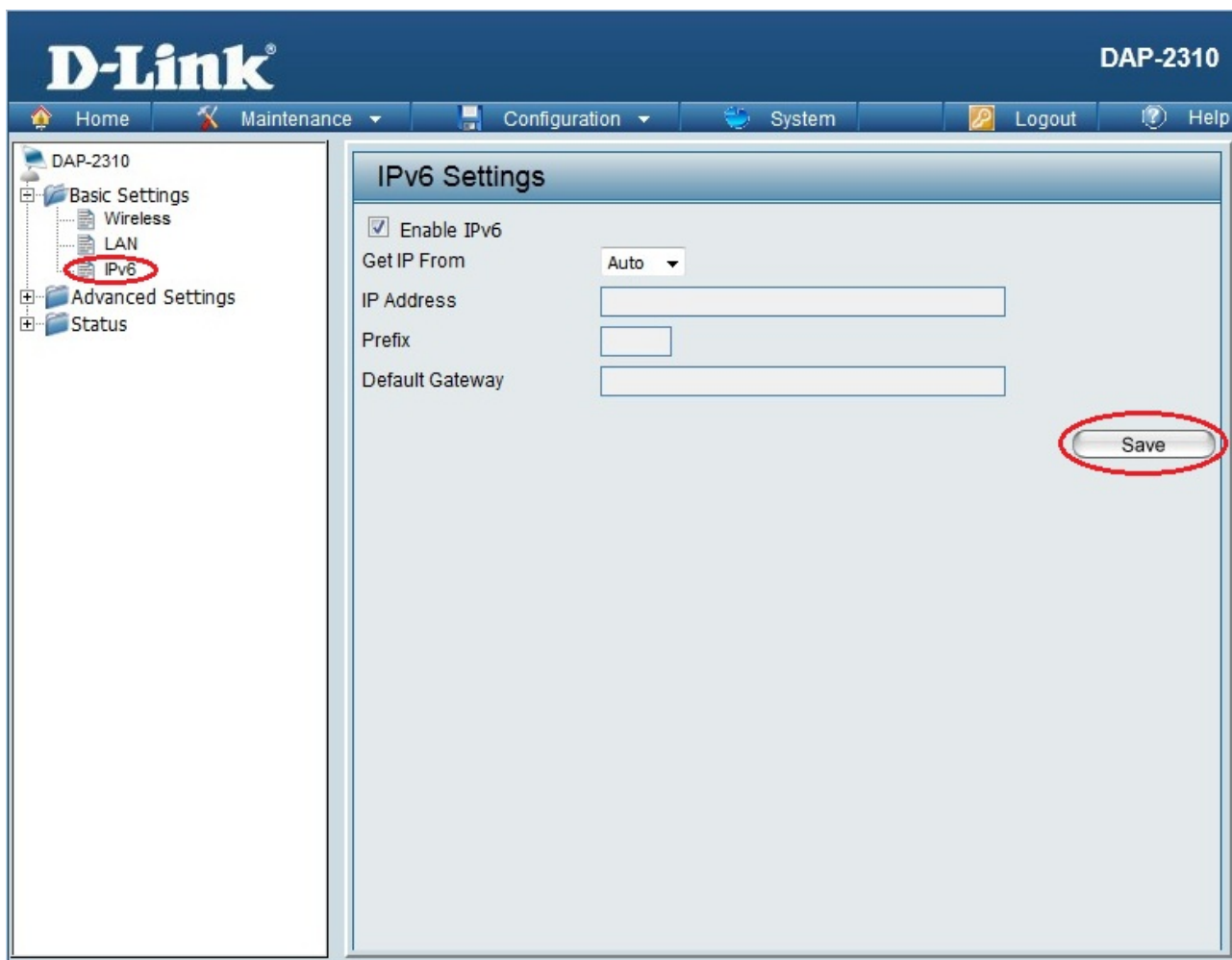


Рисунок 9.7 Настройка Link-Local IPv6-адреса управления точки доступа

Шаг 7. Сохраните и активируйте сделанные настройки. Выберите *Configuration* → *Save and Activate*. Подождите 60 секунд, пока точка доступа перезагрузится.

Шаг 8. После перезагрузки зайдите на Web-интерфейс точки доступа и нажмите *Home* (рис. 9.8).

Запишите Link-Local IPv6-адрес _____

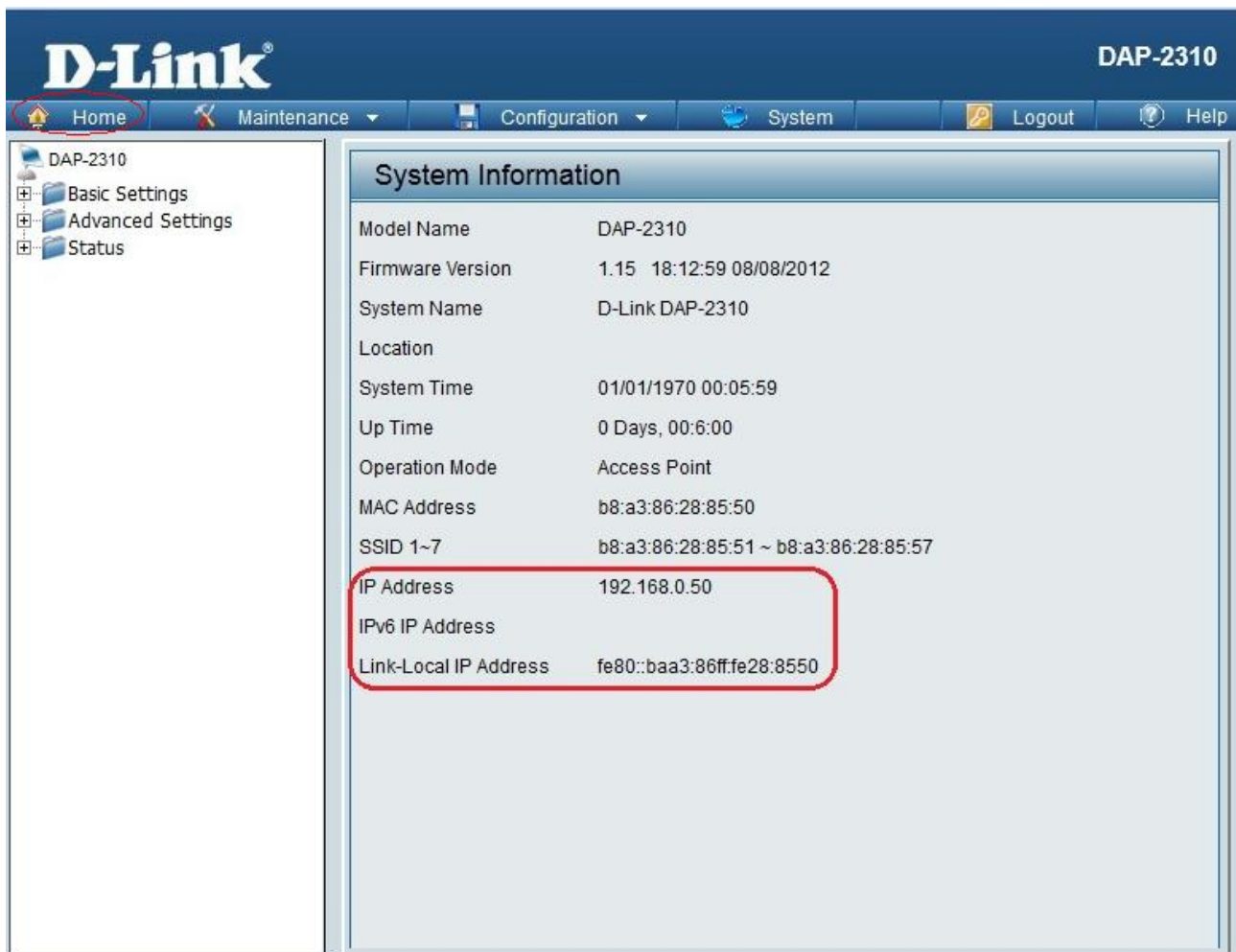


Рисунок 9.8

Шаг 9. Настройте на рабочей станции автоматическое получение IPv6-адреса.

1. Откройте *Изменение параметров адаптера*;

Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера

2. Щелкните правой кнопкой мыши *Подключение по локальной сети* и выберите *Свойства*;

3. Во вкладке *Сеть* выберите *Протокол Интернета версии 6 (TCP/IPv6)* и нажмите кнопку *Свойства*;

4. Выберите *Получить IPv6-адрес автоматически*;

5. Нажмите кнопку *Ок*.

Шаг 10. Укажите в адресной строке Web-браузера сконфигурированный Link-Local IPv6-адрес точки доступа (рис. 9.9).

`http://[ipv6address]`

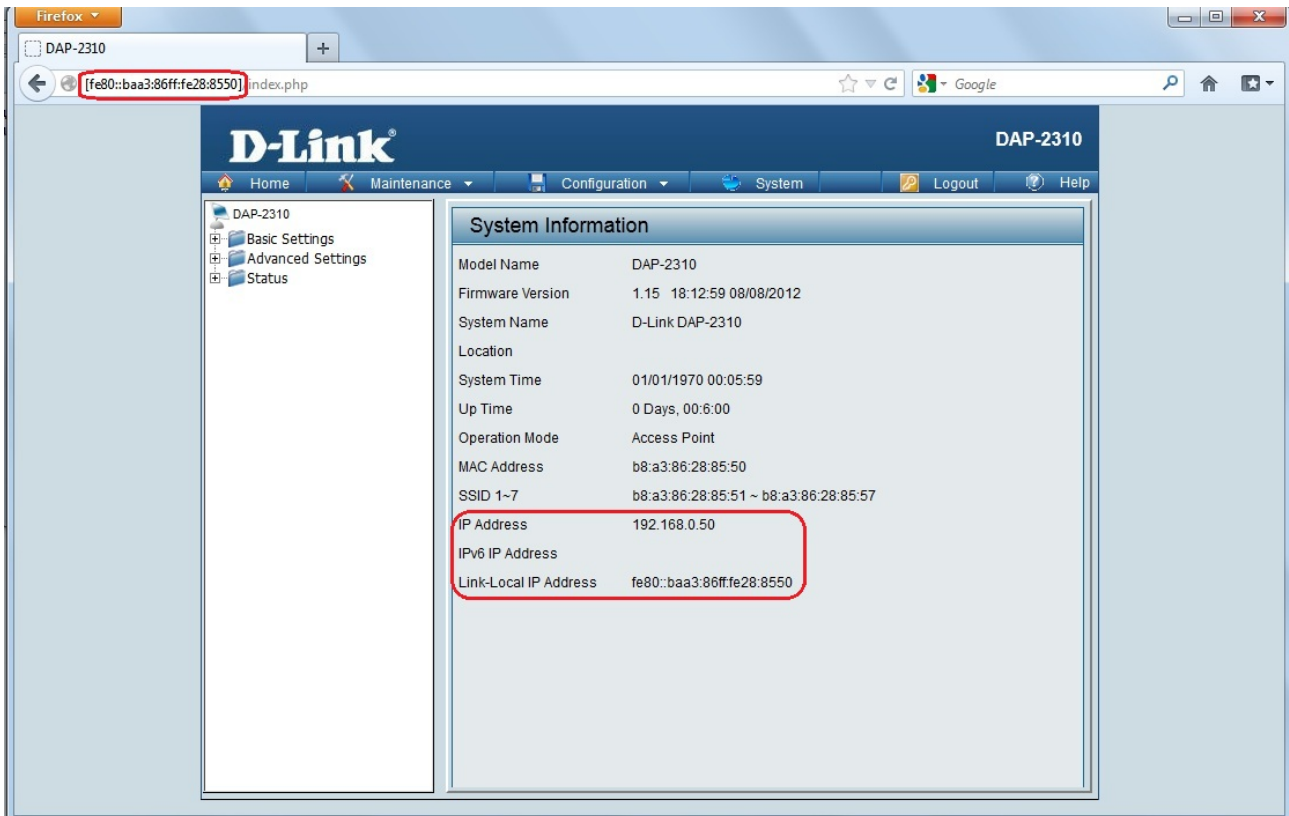


Рисунок 9.9

Внимание: вместо `[ipv6address]` введите автоматически сконфигурированный адрес Link-Local точки доступа.

Лабораторная работа №10. Изучение принципа работы протокола ARP

Протокол *ARP* (Address Resolution Protocol) используется для динамического разрешения адресов, то есть позволяет определить MAC-адрес канального уровня, используя известный IP-адрес сетевого уровня. В процессе разрешения адресов устройства обмениваются специальными сообщениями:

- *ARP-запрос* — устройство, которому требуется отправить IP-пакет, посылает широковещательный запрос всем устройствам локальной сети, чтобы определить кто является получателем пакета;
- *ARP-ответ* — устройство-получатель отправляет назад источнику одноадресное сообщение, сообщая в нем свой адрес канального уровня.

Каждый раз, когда устройство отправляет ARP-сообщение, оно использует полосу пропускания сети, а так же загружает ЦПУ сетевых устройств на его обработку. Решением данной проблемы является использование *кэширования (caching)*.

ARP-кэш представляет собой таблицу, связывающую между собой физические адреса и IP-адреса узлов. Каждое устройство в сети создает и обслуживает свою собственную таблицу ARP.

Существует два способа создания записей в ARP-таблице:

Статические записи создаются вручную администратором и постоянно хранятся в таблице. Обычно создаются с помощью утилиты *arp*.

Динамические записи создаются в процессе работы протокола ARP. Чтобы записи не использовали много системной памяти и были актуальными, они хранятся в таблице определенный период времени и затем удаляются. Стандартное время жизни динамической записи в ARP-таблице — 2 минуты.

Утилита *arp* позволяет просматривать и управлять ARP-таблицей устройства, в котором реализован стек TCP/IP.

Оборудование (на 1 рабочее место):

Рабочая станция	2 шт.
Кабель Ethernet	1 шт.
ПО — анализатор трафика <i>Wireshark</i>	

Цель: исследование принципа работы протокола ARP и управление записями в ARP-таблице, анализ сетевого трафика при помощи программы *Wireshark*.

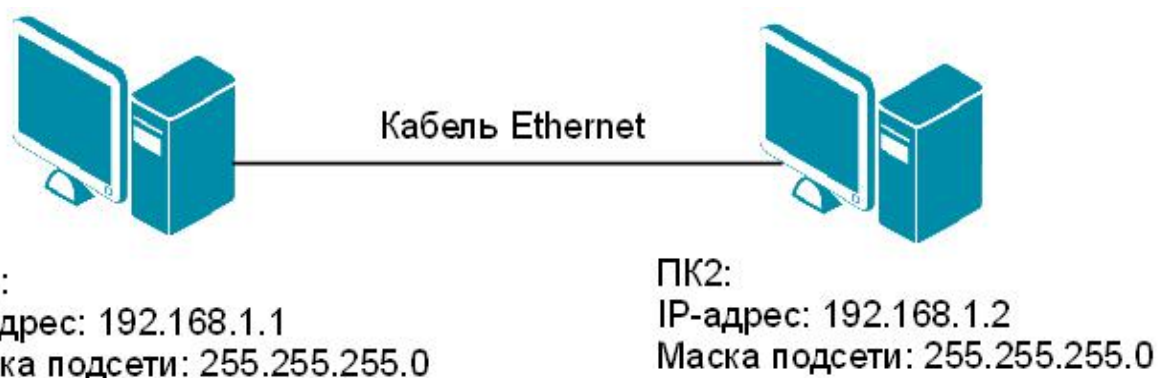


Рисунок 10.1 Схема подключения

Шаг 1. Подключите один конец Ethernet-кабеля к сетевому адаптеру ПК1, а другой конец кабеля — к сетевому адаптеру ПК2 (рис. 10.1).

Шаг 2. Настройте статический IP-адрес на рабочей станции ПК1 и ПК2 в соответствии с рисунком 10.1.

Шаг 3. На рабочей станции ПК1 откройте командную строку и введите команду `arp`.

Чтобы открыть командную строку в WindowsXP, выполните следующие действия:

1. Откройте окно *Запуск программы*;

Пуск → Выполнить
или
одновременно нажмите клавиши Windows+R

2. В появившемся окне введите `cmd` и нажмите *Ок*.

Кроме того, открыть командную строку можно с помощью элементов меню *Пуск*:

Пуск → Все программы → Стандартные → Командная строка

Чтобы открыть командную строку в Windows 7/Vista, выполните следующие действия:

1. Нажмите меню *Пуск* и в строке поиска введите `cmd`;

2. Нажмите *Ок*.

С помощью какой команды можно посмотреть все записи в ARP-таблице?

С помощью какой команды можно удалить все записи из ARP-таблицы?

Шаг 4. Пока рабочие станции ПК1 и ПК2 не обмениваются данными, ARP-таблица должна быть пуста. В командной строке ПК1 введите: `arp -a`

Что вы наблюдаете? Запишите _____

Шаг 5. Проверьте соединение между ПК1 и ПК2 с помощью команды `ping`:

В командной строке ПК1 введите: `ping 192.168.1.2`

В командной строке ПК2 введите: `ping 192.168.1.1`

Шаг 6. Посмотрите MAC-адрес рабочей станции ПК1. В командной строке введите: `getmac`

Запишите MAC-адрес ПК1 _____

Шаг 7. Посмотрите MAC-адрес рабочей станции ПК2. В командной строке введите: `getmac`

Запишите MAC-адрес ПК2 _____

Шаг 8. На рабочей станции ПК1 посмотрите все записи в ARP-таблице. В командной строке введите `arp -a`

Какой MAC-адрес у рабочей станции с IP-адресом 192.168.1.2? _____

Шаг 9. На рабочей станции ПК1 добавьте статическую запись в ARP-таблицу. В командной строке введите: `arp -s 192.168.1.3 00-aa-00-62-c6-09`

Шаг 10. Посмотрите все записи в ARP-таблице. В командной строке введите: `arp -a`

Какой тип у записи с IP-адресом 192.168.1.3? _____
Какой тип у записи с IP-адресом 192.168.1.2? _____

Шаг 11. На рабочей станции ПК1 удалите из ARP-таблицы запись с IP-адресом 192.168.1.3. В командной строке введите: `arp -d 192.168.1.3`

Шаг 12. На рабочей станции ПК1 посмотрите все записи в ARP-таблице. В командной строке введите: `arp -a`

Шаг 13. Запустите на рабочей станции ПК1 анализатор протоколов Wireshark (описание программы представлено в лабораторной работе №5). Выберите сетевой интерфейс, с которого будет выполняться перехват. Для этого выберите пункт главного меню *Capture* → *Interfaces* или нажмите кнопку на верхней панели инструментов *List the available capture interfaces*. После этого на экране появится окно со списком сетевых интерфейсов, доступных системе. Выберите сетевой интерфейс и нажмите кнопку *Start*.

Шаг 14. На рабочей станции ПК1 удалите все записи из ARP-таблицы. В командной строке введите: `arp -d`

Шаг 15. Выполните тестирование соединения между ПК1 и ПК2 с помощью команды `ping`.

В командной строке ПК1 введите: `ping 192.168.1.2`

В командной строке ПК2 введите: `ping 192.168.1.1`

Наблюдаете ли вы трафик, передаваемый между ПК1 и ПК2 в окне Wireshark? _____

Шаг 16. Остановите захват трафика. Для этого нажмите кнопку на верхней панели инструментов *Stop the running live capture* (рис. 10.2).

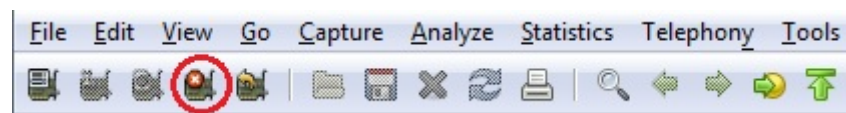


Рисунок 10.2 Остановка захвата трафика

Шаг 17. Чтобы в окне программы Wireshark отображались только пакеты протокола ARP, установите фильтр *Filter* → *ARP* и нажмите *Apply* (рис. 10.3).

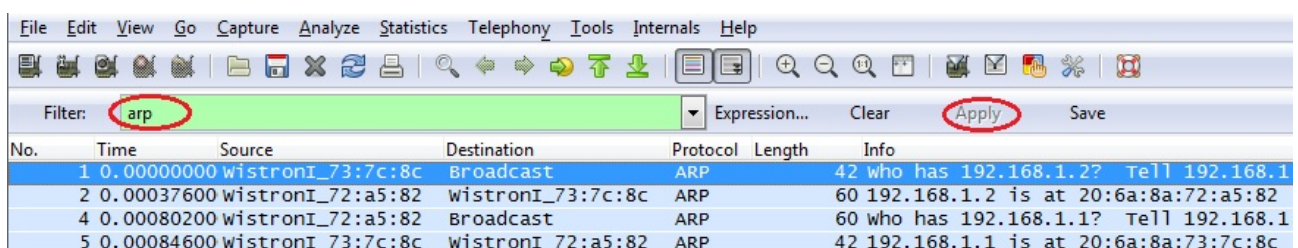


Рисунок 10.3 Установка фильтра

Шаг 18. Проанализируйте захваченный трафик.

Какое ARP-сообщение было отправлено первым? _____

Какое ARP-сообщение было отправлено вторым? _____

Выберите первый пакет ARP и разверните подробную информацию для кадра *Ethernet II*.

Чему равен MAC-адрес устройства-получателя сообщения? _____

Чему равен MAC-адрес устройства-источника сообщения? _____

Разверните подробную информацию для кадра *Address Resolution Protocol (request)*.

Если кадр для запроса ARP является широковещательным, почему *Target MAC address* равен 00:00:00:00:00:00? _____

Выберите второй пакет ARP и разверните подробную информацию для кадра *Ethernet II*.

Чему равен MAC-адрес устройства-получателя сообщения? _____

Чему равен MAC-адрес устройства-источника сообщения? _____

Лабораторная работа №11. Организация межсетевого взаимодействия с помощью маршрутизатора DIR-615

Маршрутизация является одним из важных процессов, который выполняется на сетевом уровне модели OSI. Она позволяет локальным сетям объединяться вместе. Маршрутизация выполняется специальными устройствами, *маршрутизаторами*, которые перенаправляют пакеты от одной сети в другую, даже в том случае, если заранее неизвестно, где находится пункт назначения.

Во внешней сети идентификация устройств происходит по уникальным IP-адресам, которые не должны повторяться в глобальной сети. Такие IP-адреса называются *публичными* адресами. Однако число публичных адресов ограничено, поэтому в каждом из классов IP-сетей определено так называемое *частное пространство IP-адресов*. Частные IP-адреса предназначены для использования в локальных компьютерных сетях и не маршрутизируются во внешнюю сеть. Для локальных сетей, не подключенных к Интернет, можно использовать любые возможные адреса, уникальные в пределах данной сети.

Публичные адреса находятся в пределах от 1.0.0.1 до 223.255.255.254, за исключением частных IPv4 адресов.

Адресное пространство частных IP-адресов состоит из 3 блоков:

- 10.0.0.0 – 10.255.255.255 (класс А);
- 172.16.0.0 – 172.31.255.255 (класс В);
- 192.168.0.0 – 192.168.255.255 (класс С).

Несмотря на то, что частные IP-адреса не могут передавать данные в Интернет, существует способ организации связи внутренней IP-сети, в которой используются такие адреса, с глобальной сетью. Это реализуется с помощью механизма *преобразования сетевых адресов (Network Address Translation, NAT)*, который позволяет подключать сети с частными IP-адресами к Интернет, преобразуя частные IP-адреса передаваемых пакетов в публичные IP-адреса, и наоборот.

Преобразование сетевых адресов выполняется маршрутизирующим устройством, которое изменяет IP-адрес источника на публичный адрес в тот момент, когда пакет покидает внутреннюю сеть, а затем изменяет IP-адрес получателя каждого пакета, который возвращается в локальную сеть на частный адрес. Механизм преобразования сетевых адресов позволяет группе узлов внутренней сети подключаться к Интернет, используя один публичный IP-адрес.

Если на маршрутизаторе выполняется преобразование сетевых адресов (NAT), то невозможно обратиться из внешней сети к рабочей станции, которая находится во внутренней сети. Решить эту проблему позволяет технология *Port Forwarding*, которая обеспечивает перенаправление данных из внешней сети во внутреннюю через определенные порты.

Цель: изучить Web-интерфейс маршрутизатора DIR-615, обеспечить доступ из внешней сети к FTP-серверу, который находится во внутренней сети.

Оборудование (на 1 рабочее место):

Рабочая станция с FTP-сервером	1 шт.
Рабочая станция	1 шт.
Кабель Ethernet	2 шт.
Маршрутизатор DIR-615	1 шт.
ПО — <i>Golden FTP Server</i>	

11.1 Организация межсетевого взаимодействия

Шаг 1. Сбросьте настройки маршрутизатора к заводским настройкам по умолчанию. Для этого подключите маршрутизатор к адаптеру питания и удерживайте в течение 10 секунд кнопку *Reset*, расположенную на задней панели устройства (рис. 11.1).



Рисунок 11.1 Расположение кнопки Reset на маршрутизаторе DIR-615

Шаг 2. Подключите рабочую станцию ПК1 к LAN-порту маршрутизатора DIR-615, а рабочую станцию ПК2 — к INTERNET-порту (WAN-порту), как показано на рисунке 11.2.

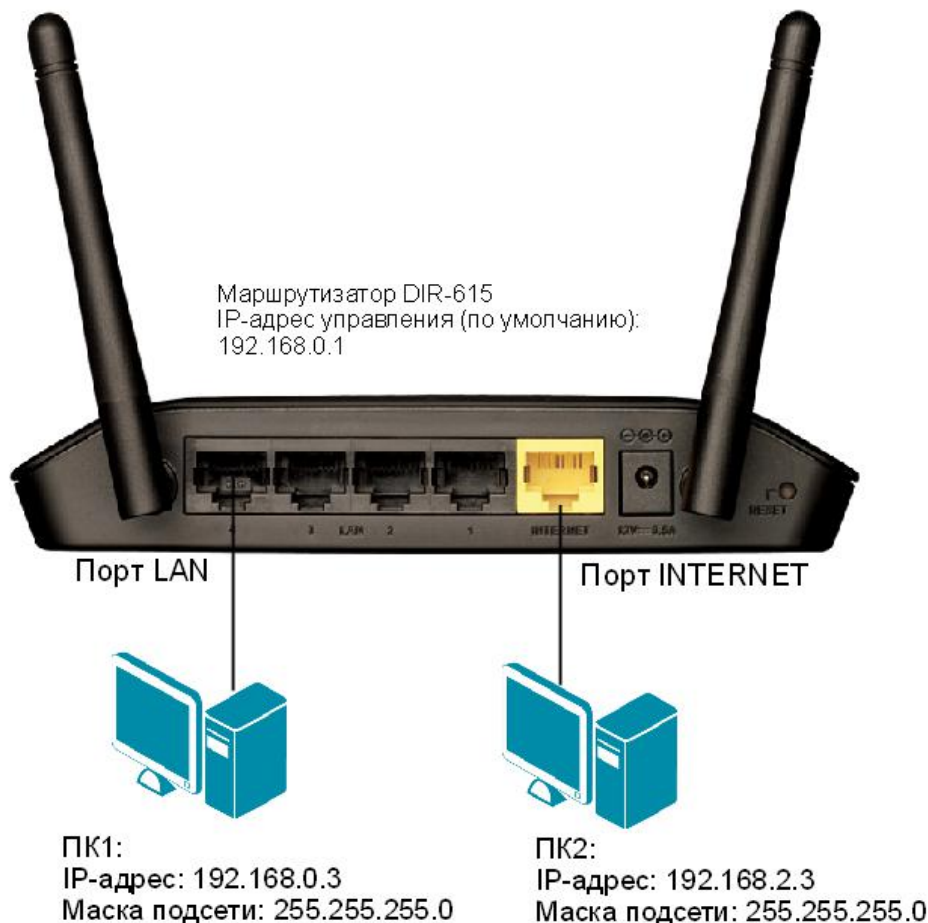


Рисунок 11.2 Схема подключения рабочих станции к маршрутизатору DIR-615

Шаг 3. Настройте статический IP-адрес на ПК1 и ПК2 в соответствии со схемой 11.2.

Шаг 4. Проверьте соединение между ПК1 и маршрутизатором с помощью команды ping:

В командной строке ПК1 введите: `ping 192.168.0.1`

Внимание: IP-адрес управления маршрутизатора по умолчанию обычно указывается в руководстве пользователя. Для маршрутизатора D-Link DIR-615 IP-адрес управления по умолчанию — 192.168.0.1

Шаг 5. Зайдите на Web-интерфейс маршрутизатора.

Чтобы зайти на Web-интерфейс маршрутизатора, выполните следующие действия:

1. На рабочей станции ПК1 запустите Web-браузер (Internet Explorer, Mozilla Firefox), в адресной строке которого укажите IP-адрес интерфейса управления маршрутизатора по умолчанию: `http://192.168.0.1`

2. В появившемся окне аутентификации (рис. 11.3), в поле *Login* и *Password* введите *admin* и нажмите кнопку *Enter*.

Внимание: Если на рабочей станции произведены настройки прокси-сервера, то их нужно отключить.

Для Mozilla Firefox: меню *Инструменты* → *Настройки* → *Дополнительные*. Далее вкладка *Сеть* → *Настройка параметров соединения Firefox с Интернетом* → *Настроить* → *Без прокси*.

Для Internet Explorer: меню *Сервис* → *Свойство обозревателя*. Далее вкладка *Подключения* → *Настройка сети* → *Автоматическое определение параметров*.

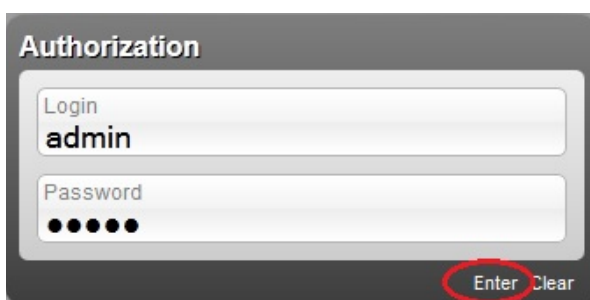


Рисунок 11.3 Окно аутентификации

Сразу после первого обращения к Web-интерфейсу управления маршрутизатора откроется окно для изменения пароля администратора, установленного по умолчанию.

В открывшемся окне в поле *Password* введите *11223344*, в поле *Confirmation* повторите пароль *11223344* и нажмите кнопку *Save* (рис. 11.4).

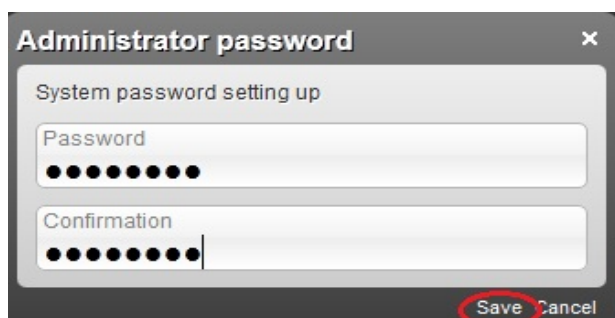


Рисунок 11.4 Окно изменения пароля администратора, установленного по умолчанию

Примечание: запомните или запишите новый пароль администратора. В случае утери нового пароля, доступ к настройкам маршрутизатора можно получить только после восстановления настроек по умолчанию при помощи кнопки *Reset*, расположенной на задней панели устройства.

В открывшемся окне аутентификации в поле *Login* введите *admin*, в поле *Password* введите новый пароль — *11223344*. Нажмите кнопку *Enter*.

После аутентификации откроется окно быстрых настроек маршрутизатора (рис. 11.5).

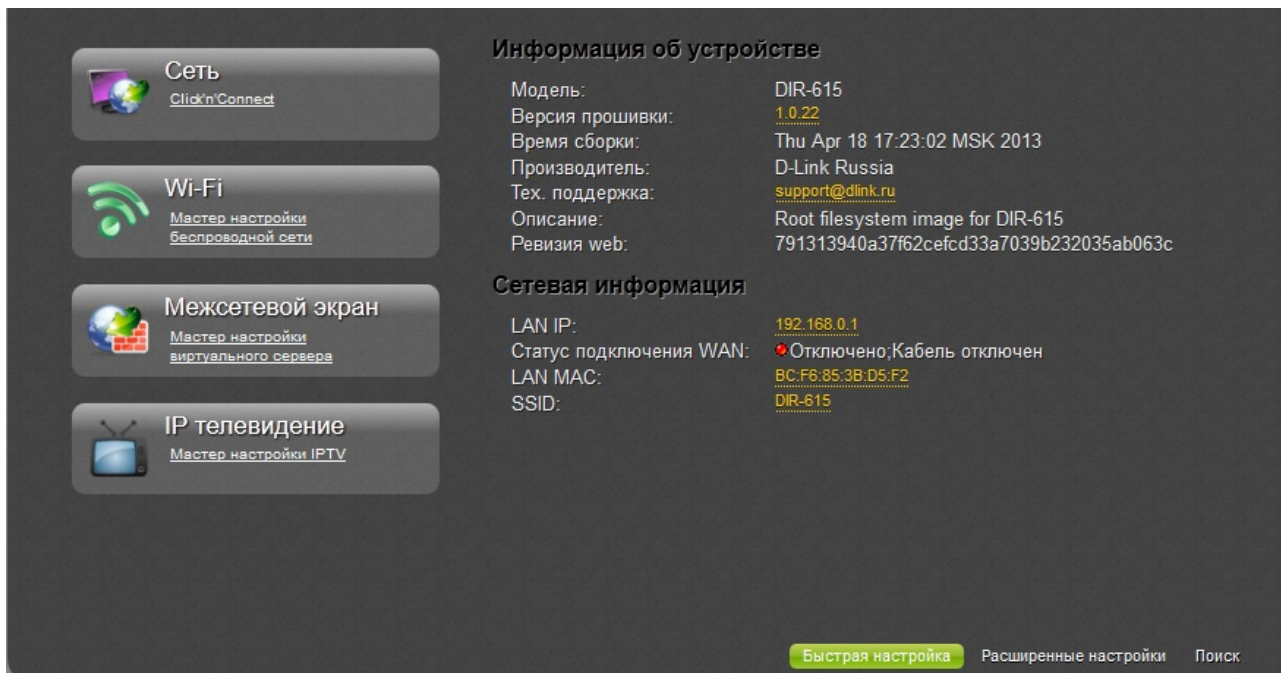


Рисунок 11.5 Web-интерфейс управления маршрутизатора

Web-интерфейс маршрутизатора доступен на нескольких языках. Наведите указатель мыши на надпись *Language*, расположенную в правом верхнем углу, и выберите значение *Русский*.

Нажмите значок *Сохранить*, чтобы сохранить текущий язык Web-интерфейса в качестве языка по умолчанию (рис. 11.6).

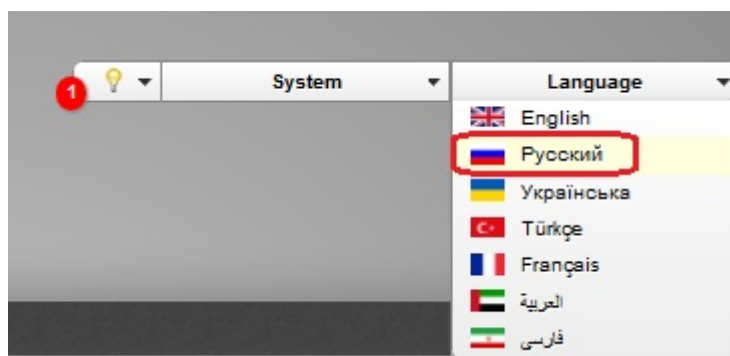


Рисунок 11.6 Изменение языка Web-интерфейса

Шаг 6. Измените IP-адрес управления маршрутизатора.

1. Нажмите ссылку *Расширенные настройки* в правом нижнем углу страницы;



Рисунок 11.7 Расширенные настройки маршрутизатора

2. Выберите раздел *Сеть* → *LAN*;

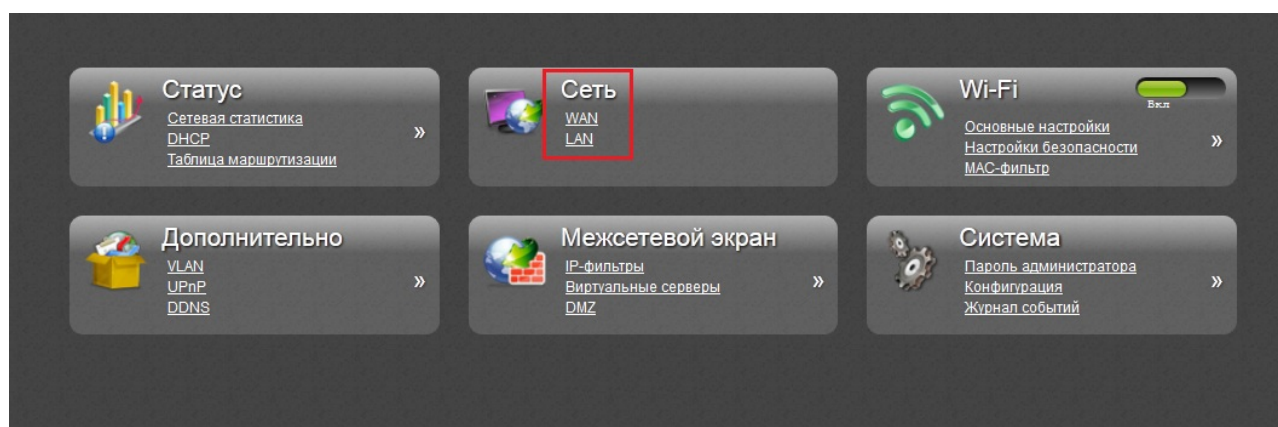


Рисунок 11.8 Раздел *Сеть*

3. В поле *IP-адрес* введите новый IP-адрес управления маршрутизатора — *192.168.0.2*. Значение поля *Сетевая маска* оставьте без изменений.

Отключите динамическое назначение адресов. Для этого в выпадающем меню *Режим* выберите *Запретить* и нажмите кнопку *Сохранить*.



Рисунок 11.9 Изменение IP-адреса управления маршрутизатора

4. Нажмите значок *Сохранить* и *Перезагрузить*, чтобы сохранить текущий IP-адрес управления маршрутизатора (рис. 11.10).

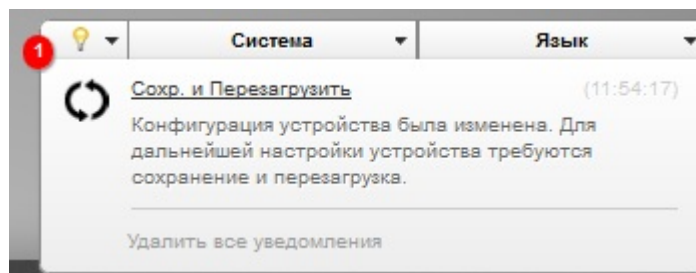


Рисунок 11.10 Сохранение IP-адреса управления маршрутизатора

Шаг 7. В адресной строке Web-браузера введите новый IP-адрес управления: `http://192.168.0.2`

Шаг 8. Настройте IP-адрес WAN-интерфейса маршрутизатора (рис. 11.11).

1. Нажмите ссылку *Расширенные настройки* в правом нижнем углу страницы;

2. Выберите раздел *Сеть* → *WAN*;

3. В открывшемся окне нажмите кнопку *Добавить*;

4. В поле *Тип соединения* выберите *Статический IP*;

В поле *IP-адрес* введите *192.168.2.2*;

В поле *Сетевая маска* введите *255.255.255.0*;

В поле *IP-адрес шлюза* введите *192.168.2.2*;

В поле *Первичный DNS-сервер* введите *4.4.4.4*;

В поле *Вторичный DNS-сервер* введите *8.8.8.8*;

Нажмите кнопку *Сохранить*.

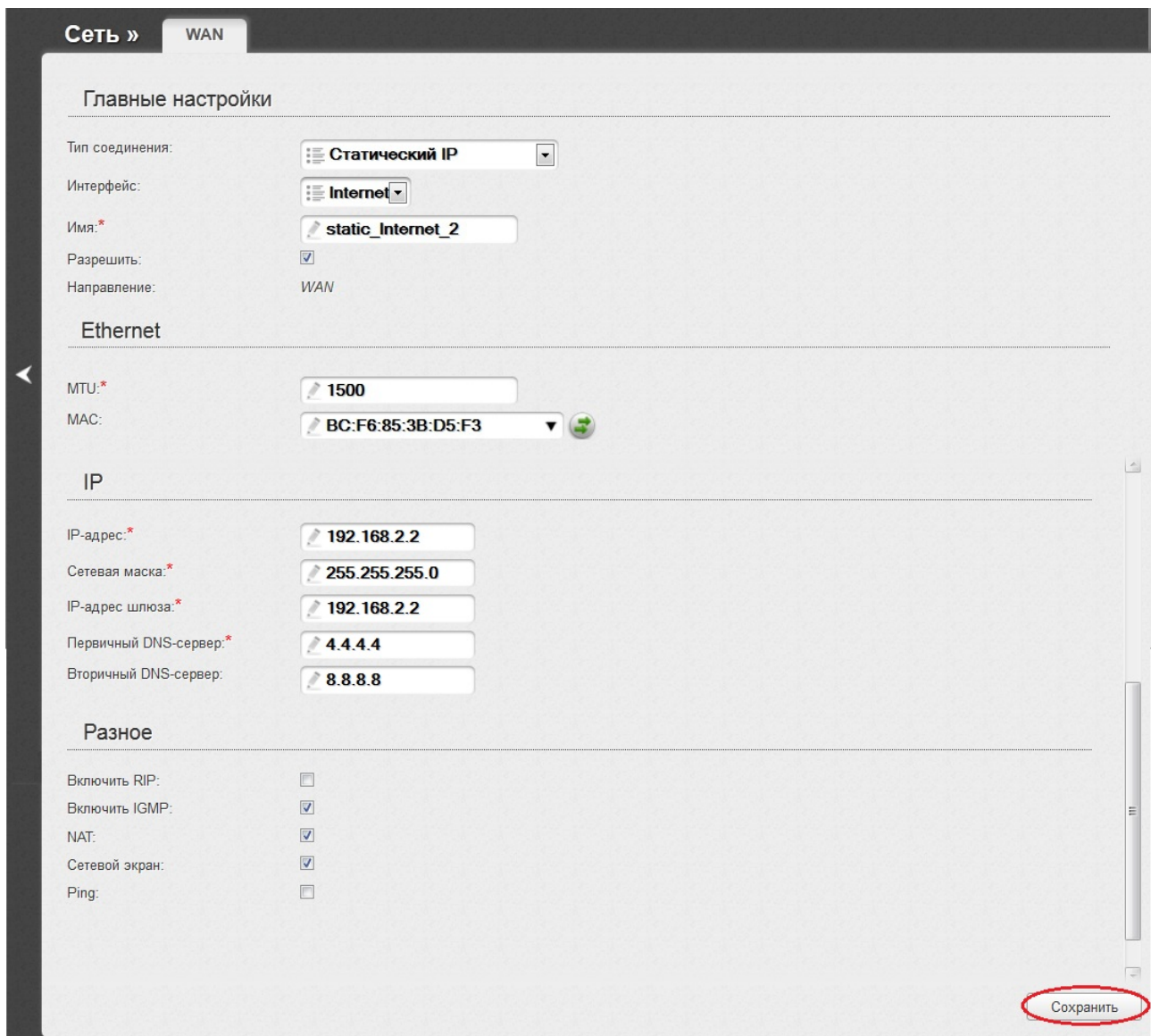


Рисунок 11.11 Настройка IP-адреса WAN-интерфейса маршрутизатора

Шаг 9. Проверьте соединение между рабочей станцией ПК1 и ПК2 с помощью команды ping:

В командной строке ПК1 введите: `ping 192.168.2.3`

В командной строке ПК2 введите: `ping 192.168.0.3`

Объясните наличие/отсутствие связи между рабочими станциями _____

Шаг 10. Настройте IP-адрес шлюза по умолчанию для ПК1 и ПК2. В качестве основного шлюза для ПК1 укажите IP-адрес LAN-интерфейса маршрутизатора, для ПК2 — IP-адрес WAN-интерфейса.

Настройка IP-адреса основного шлюза на рабочей станции с ОС Windows XP:

1. Откройте *Сетевые подключения*;

Пуск → Панель управления → Сетевые подключения

2. Щелкните правой кнопкой мыши на *Подключение по локальной сети* и выберите *Свойства*;

3. В диалоговом окне выберите *Протокол Интернета (TCP/IP)* и нажмите *Свойства*;

4. В поле *Основной шлюз* введите: для ПК1 — 192.168.0.2, для ПК2 — 192.168.2.2;
5. Нажмите кнопку *Ок*.

Настройка IP-адреса на рабочей станции с ОС Windows 7/Vista:

1. Откройте *Изменение параметров адаптера*;

Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера

2. Щелкните правой кнопкой мыши на *Подключение по локальной сети* и выберите *Свойства*;
3. В диалоговом окне выберите *Протокол Интернета 4 (TCP/IP)* и нажмите *Свойства*;
4. В поле *Основной шлюз* введите: для ПК1 — 192.168.0.2, для ПК2 — 192.168.2.2;
5. Нажмите кнопку *Ок*.

Шаг 11. Проверьте соединение между рабочей станцией ПК1 и ПК2 с помощью команды *ping*:

В командной строке ПК1 введите: `ping 192.168.2.3`

В командной строке ПК2 введите: `ping 192.168.0.3`

Объясните наличие/отсутствие связи между рабочими станциями _____

Почему по-прежнему отсутствует соединение между рабочей станцией ПК2 и ПК1?

11.2 Обеспечение доступа из внешней сети к FTP-серверу, который находится во внутренней сети

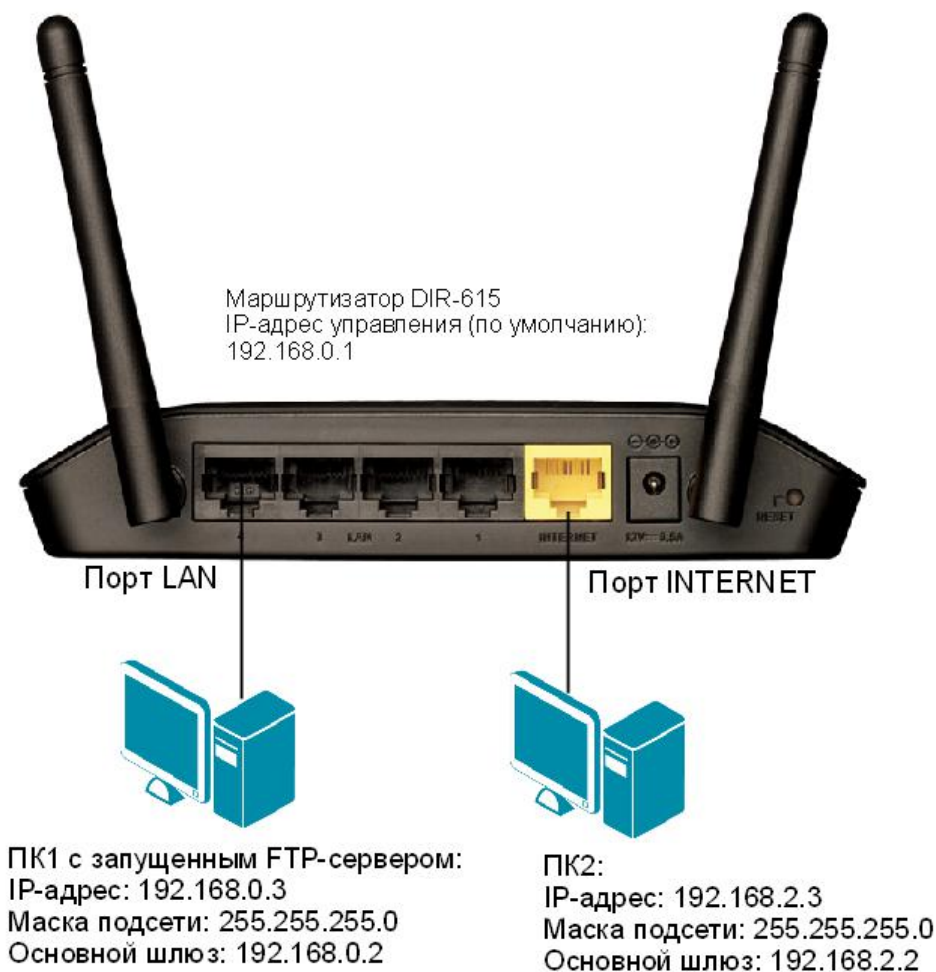


Рисунок 11.12 Схема подключения рабочих станции к маршрутизатору DIR-615

Шаг 1. Запустите на рабочей станции ПК1 программу *Golden FTP Server* и добавьте каталог, к которому требуется открыть общий доступ.

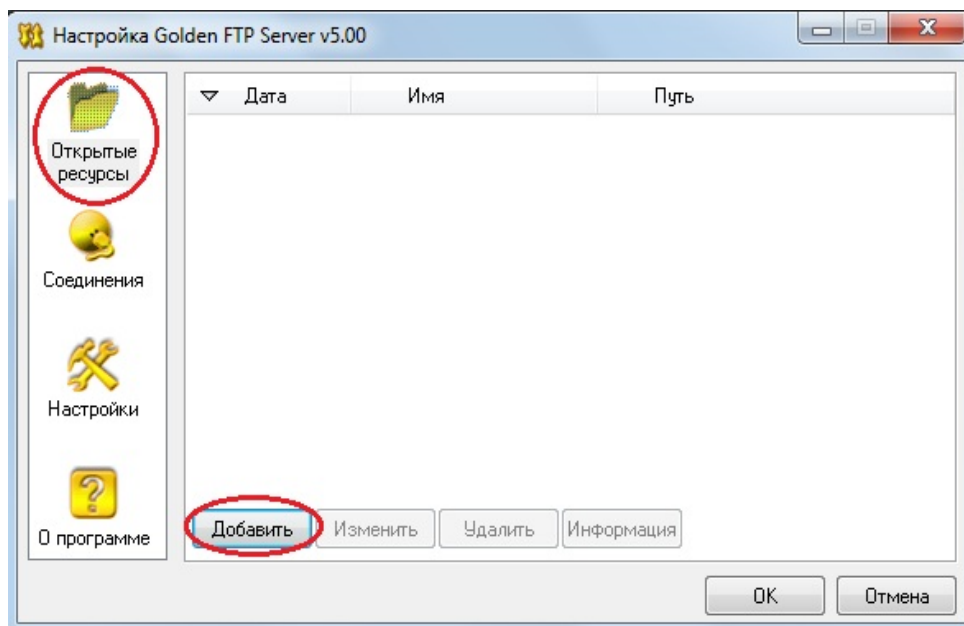


Рисунок 11.13

В открывшемся окне укажите путь к каталогу и его имя. Нажмите кнопку *Ок*.

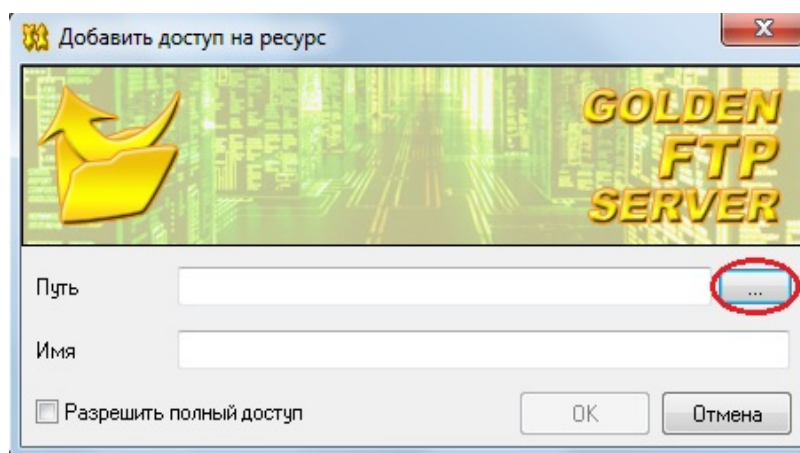


Рисунок 11.14

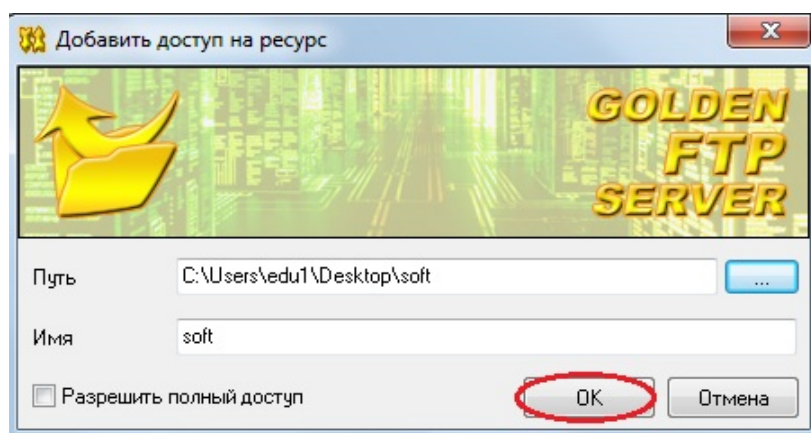


Рисунок 11.15

В открывшемся информационном окне установите галочку *Не отображать больше* и нажмите кнопку *Ок*.

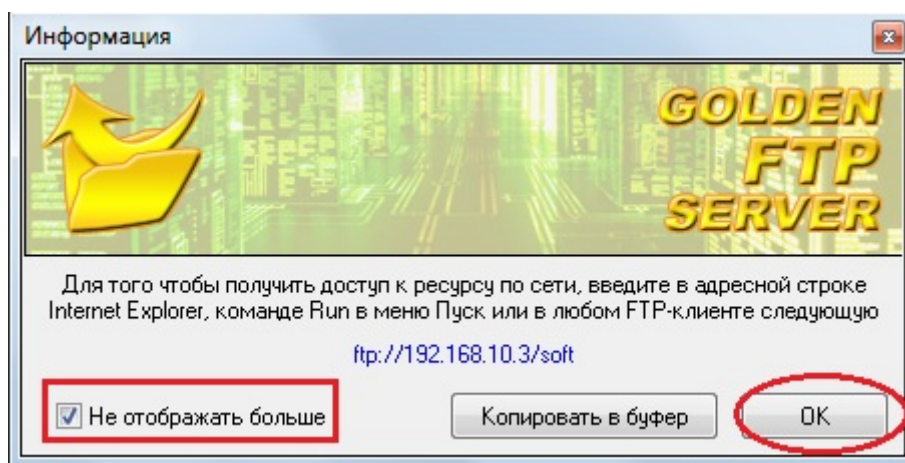


Рисунок 11.16

Шаг 2. Зайдите на Web-интерфейс маршрутизатора.

Шаг 3. Для того чтобы пользователи внешней сети могли получить доступ на FTP-сервер, который находится во внутренней сети за маршрутизатором, использующим NAT, используется функция *Port Forwarding* (проброс портов).

Примечание: в версии ПО 1.0.22 маршрутизатора DIR-615 функция проброса портов

называется «Виртуальные серверы».

1. Нажмите ссылку *Расширенные настройки* в правом нижнем углу страницы;
2. Выберите раздел *Межсетевой экран* → *Виртуальные серверы*;

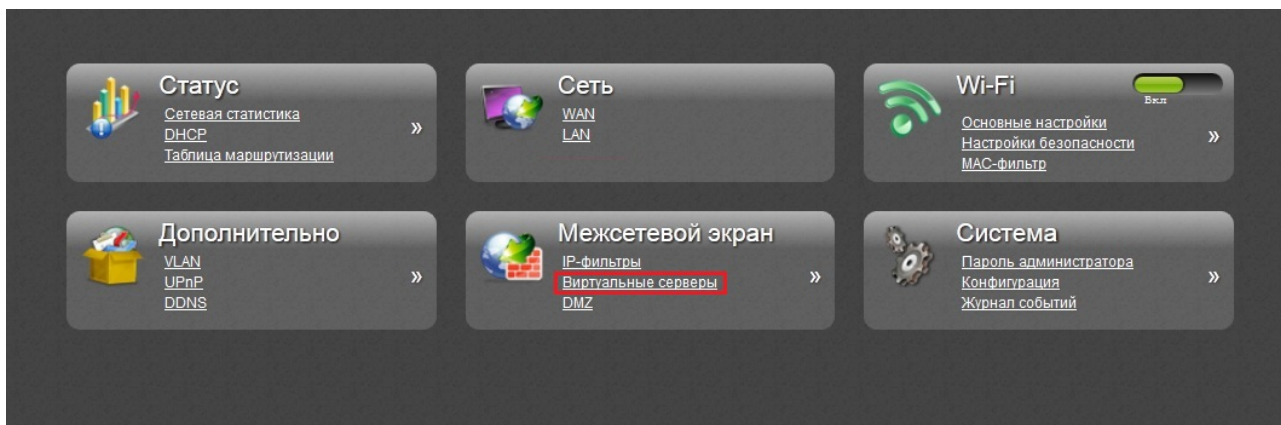


Рисунок 11.17 Раздел *Межсетевой экран*

3. В открывшемся окне нажмите кнопку *Добавить*;

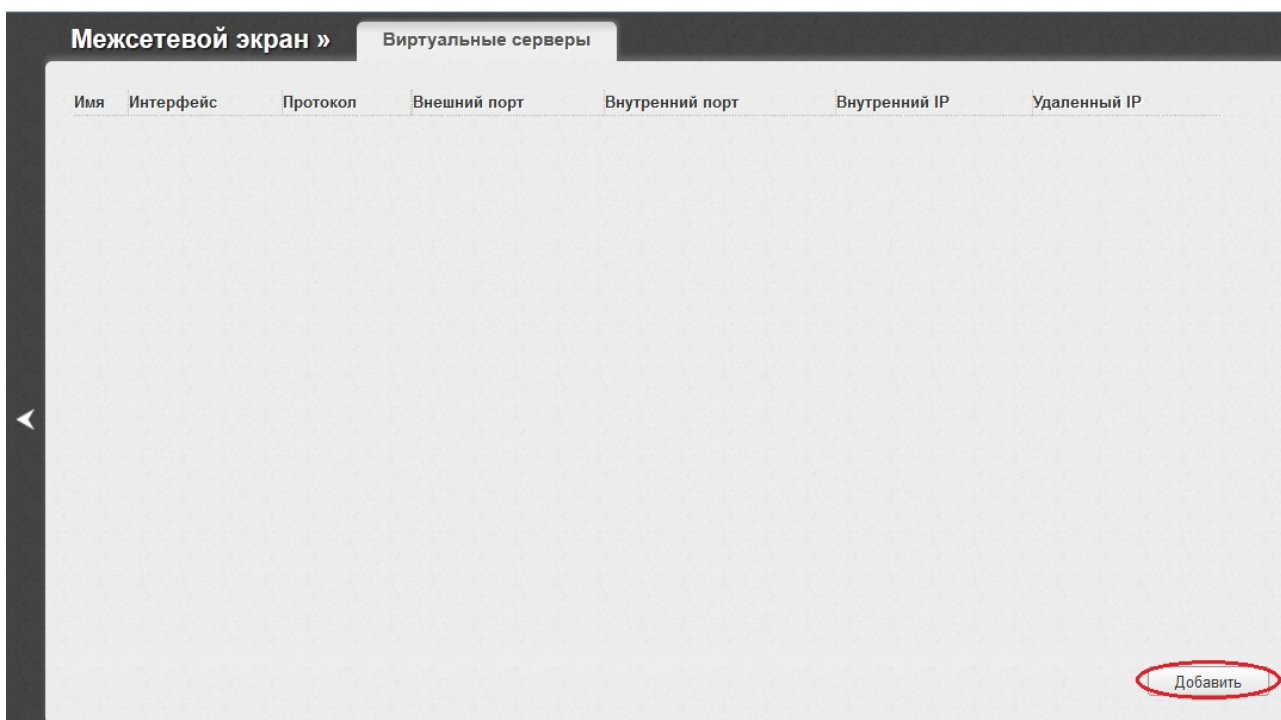


Рисунок 11.18

4. В открывшемся окне задайте следующие параметры:

В поле *Имя* введите *FTP_service*;

В поле *Интерфейс* выберите *static_Internet_2*;

В поле *Внешний порт (начальный)* укажите порт (по умолчанию), через который осуществляется прохождение FTP-трафика — *21*;

В поле *Внутренний порт (начальный)* укажите *21*;

В поле *Внутренний IP* выберите *192.168.0.3* (IP-адрес ПК1);

В поле *Удаленный IP* введите *192.168.2.3* (IP-адрес ПК2);

Нажмите кнопку *Сохранить*.

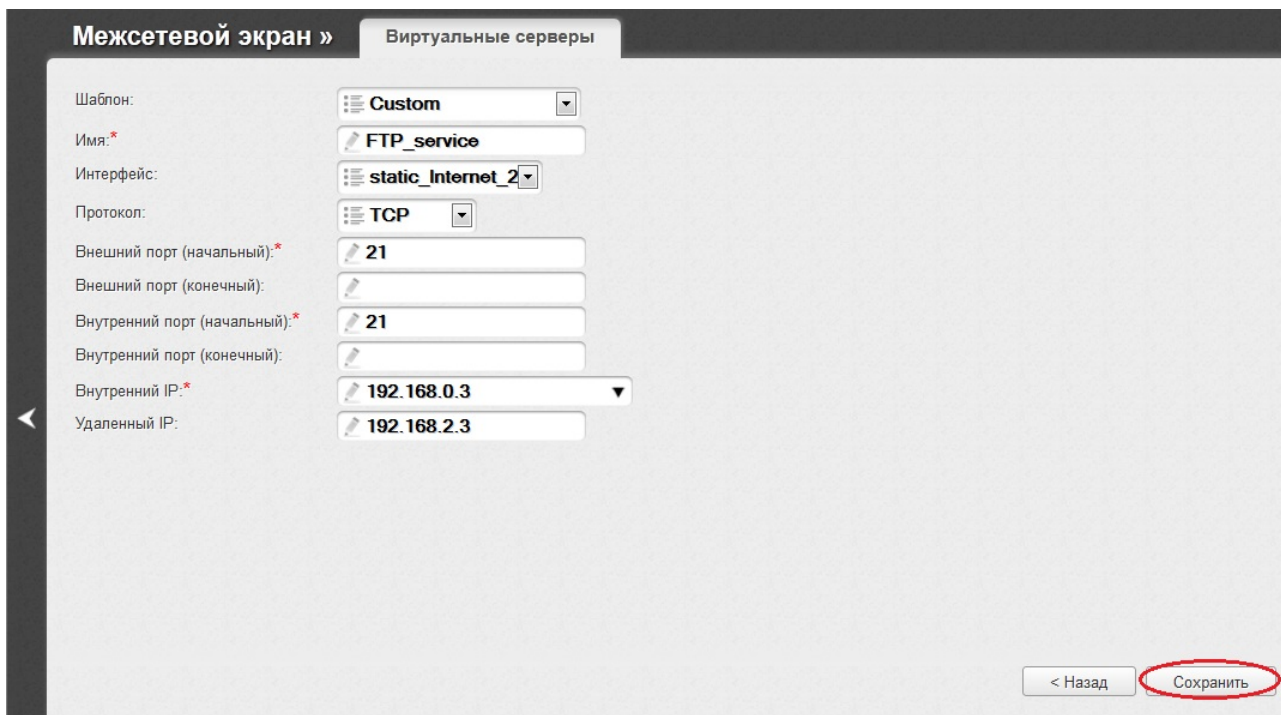


Рисунок 11.19 Создание правила для прохождения FTP-трафика

Шаг 4. Проверьте доступ на FTP-сервер на рабочей станции ПК2. Для этого откройте новую вкладку в Web-браузере и в адресной строке введите запрос:
`ftp://192.168.2.2`

Почему в качестве адреса FTP-сервера указывается IP-адрес шлюза по умолчанию рабочей станции ПК2? _____

Шаг 5. Сбросьте настройки маршрутизатора к заводским настройкам по умолчанию. Наведите указатель мыши на надпись *Система*, расположенную в правом верхнем углу, и выберите значение *Заводские настройки*. Подождите 95 секунд, пока маршрутизатор перезагрузится.

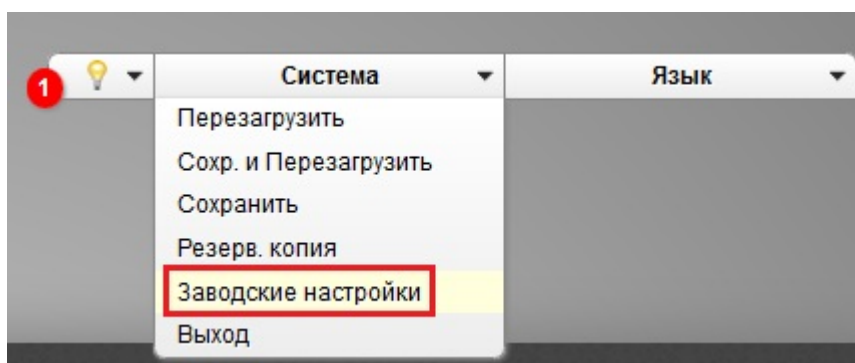


Рисунок 11.20 Сброс настроек маршрутизатора к заводским настройкам по умолчанию

Лабораторная работа №12. Динамическое распределение IP-адресов по протоколу DHCP

Для функционирования сети каждому сетевому интерфейсу компьютера и маршрутизатора должны быть назначены IP-адреса. IP-адрес может быть задан *статически* или присвоен сетевому интерфейсу *динамически*.

Статические адреса назначаются вручную администратором в процессе конфигурирования интерфейсов или автоматически. При автоматическом назначении статического адреса он становится неизменным и привязывается к определенному компьютеру (как правило, к его MAC-адресу).

Динамические адреса назначаются автоматически при подключении устройства к сети и используется в течение ограниченного промежутка времени, или до выключения компьютера. При новом назначении динамический IP-адрес клиента может быть изменен. Если все компьютеры сети не работают одновременно, то количество динамических адресов может быть меньше, чем количество компьютеров. Таким образом, можно экономнее использовать IP-адреса. Автоматическое конфигурирование IP-адреса и других сетевых параметров выполняется с помощью протокола *DHCP (Dynamic Host Configuration Protocol)*. Данный протокол основан на модели «клиент – сервер». В качестве DHCP-сервера может выступать устройство, поддерживающее функцию DHCP Server.

Цель: рассмотреть динамическое распределение IP-адресов по протоколу DHCP.

Оборудование (на 1 рабочее место):

Рабочая станция	2 шт.
Кабель Ethernet	2 шт.
Маршрутизатор DIR-615	1 шт.

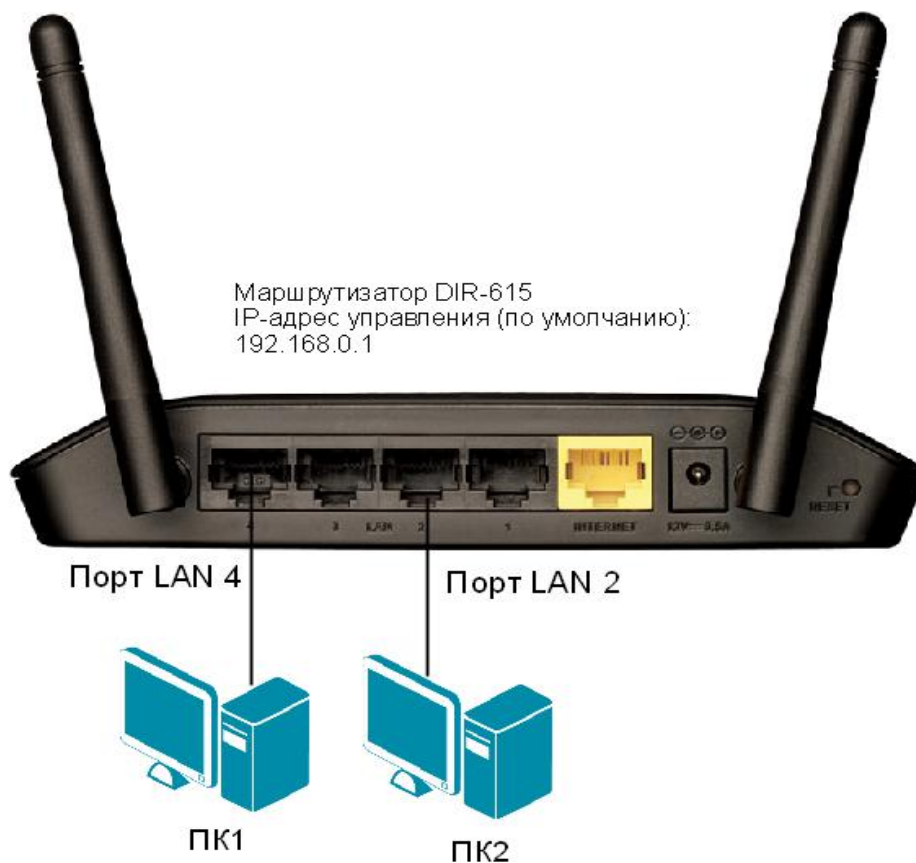


Рисунок 12.1 Схема подключения рабочих станции к маршрутизатору

Шаг 1. Подключите рабочие станции ПК1 и ПК2 к LAN-портам маршрутизатора DIR-615, как показано на рисунке 12.1.

Шаг 2. Настройте статический IP-адрес на рабочей станции ПК1.

IP-адрес — 192.168.0.3

Маска подсети — 255.255.255.0

Шаг 3. Зайдите на Web-интерфейс маршрутизатора.

Шаг 4. Настройте динамическое распределение IP-адресов рабочим станциям, находящимся во внутренней сети. IP-адрес, который может быть назначен рабочей станции, должен выбираться из диапазона адресов 192.168.0.10 — 192.168.0.20.

1. Нажмите ссылку *Расширенные настройки* в правом нижнем углу страницы;

2. Выберите раздел *Сеть* → *LAN*;

3. В выпадающем меню *Режим* выберите *Разрешить*, в поле *Начальный IP-адрес* введите 192.168.0.10, в поле *Конечный IP-адрес* введите 192.168.0.20, поле *Время аренды* оставьте без изменений. Нажмите кнопку *Сохранить*.

4. Нажмите значок *Сохранить* и *Перезагрузить*.

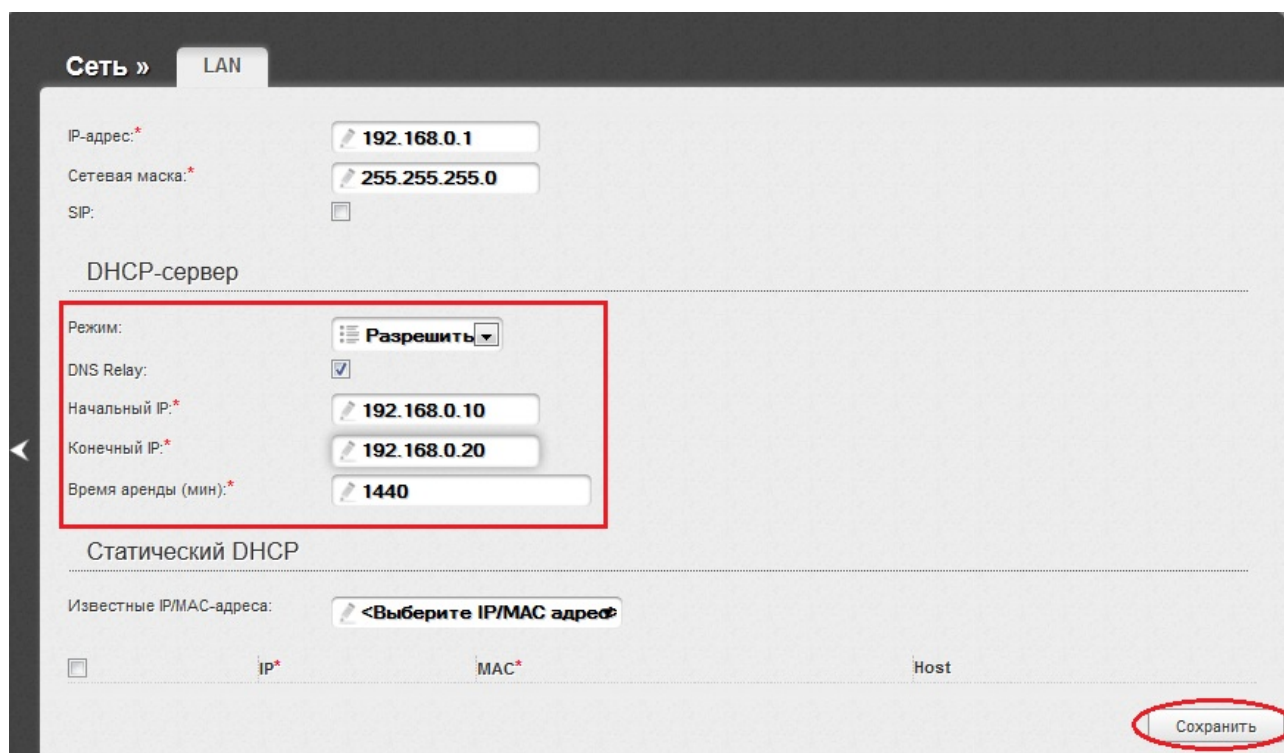


Рисунок 12.2 Настройка динамического распределения IP-адресов

Шаг 5. Настройте автоматическое получение IP-адреса на ПК1 и ПК2.

Настройка автоматического получения IP-адреса на рабочей станции с ОС Windows XP:

1. Откройте *Сетевые подключения*;

Пуск → *Панель управления* → *Сетевые подключения* → *Подключение по локальной сети*

2. Щелкните правой кнопкой мыши на *Подключение по локальной сети* и выберите *Свойства*;
3. В диалоговом окне выберите *Протокол Интернета (TCP/IP)* и нажмите *Свойства*;
4. Выберите *Получить IP-адрес автоматически*;
5. Нажмите кнопку *Ок*.

Настройка автоматического получения IP-адреса на рабочей станции с ОС Windows 7/Vista:

1. Откройте *Изменение параметров адаптера*;

Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера

2. Щелкните правой кнопкой мыши на *Подключение по локальной сети* и выберите *Свойства*;
3. В диалоговом окне выберите *Протокол Интернета 4 (TCP/IP)* и нажмите *Свойства*;
4. Выберите *Получить IP-адрес автоматически*;
5. Нажмите кнопку *Ок*.

Шаг 6. На рабочей станции ПК1 и ПК2 посмотрите полученный IP-адрес и другие сетевые параметры с помощью команды `ipconfig`.

ПК1:

IP-адрес _____

Маска подсети _____

Основной шлюз _____

ПК2:

IP-адрес _____

Маска подсети _____

Основной шлюз _____

Лабораторная работа №13. Итоговая работа

Данная лабораторная работа предполагает самостоятельную разработку топологии сети предприятия.

Цель: самостоятельно разработать топологию сети предприятия, определить тип физической среды передачи, тип и количество активного сетевого оборудования, необходимого для построения данной сети.

Входные данные:

1. Количество стационарных рабочих станций — 65;
2. Количество беспроводных клиентов — 10;
3. Количество кабинетов — 11;
4. Количество отделов — 3;
 - Отдел продаж* — кабинеты 1-4;
 - Маркетинговый отдел* — кабинеты 5, 7, 8;
 - Технический отдел* — кабинеты 9-11;
 - Серверная* — кабинет 6;
5. Количество FTP-серверов — 1.

Требования к телекоммуникационной сети:

1. Объединение проводных и беспроводных пользователей в локальную сеть;
2. Обеспечение всем пользователям выхода в сеть Интернет;
3. Изолирование трафика отдела продаж, отдела маркетинга и технического отдела друг от друга (логическая сегментация сети);
4. Обеспечение доступа на FTP-сервер удаленным пользователям (из внешней сети).

Выходные данные:

1. Нарисовать топологию сети и обосновать её выбор;
2. Указать тип физической среды передачи данных и обосновать её применение;
3. Рассчитать количество кабеля (в метрах);
4. Определить тип активного сетевого оборудования, требуемого для построения данной сети. Пояснить причины своего выбора;
5. Определить функции, необходимые для реализации логической сегментации сети и обеспечения доступа на FTP-сервер удаленным пользователям;
6. Рассчитать количество сетевого оборудования каждого типа, результаты записать в таблицу;
7. Разработать адресный план локальной сети предприятия (использовать адресацию IPv4);
8. Оценить стоимость активного сетевого оборудования (использовать файл рекомендованных цен <http://www.dlink.ru/up/news/Moscow/2013/RussiaPriceBook.xls>).

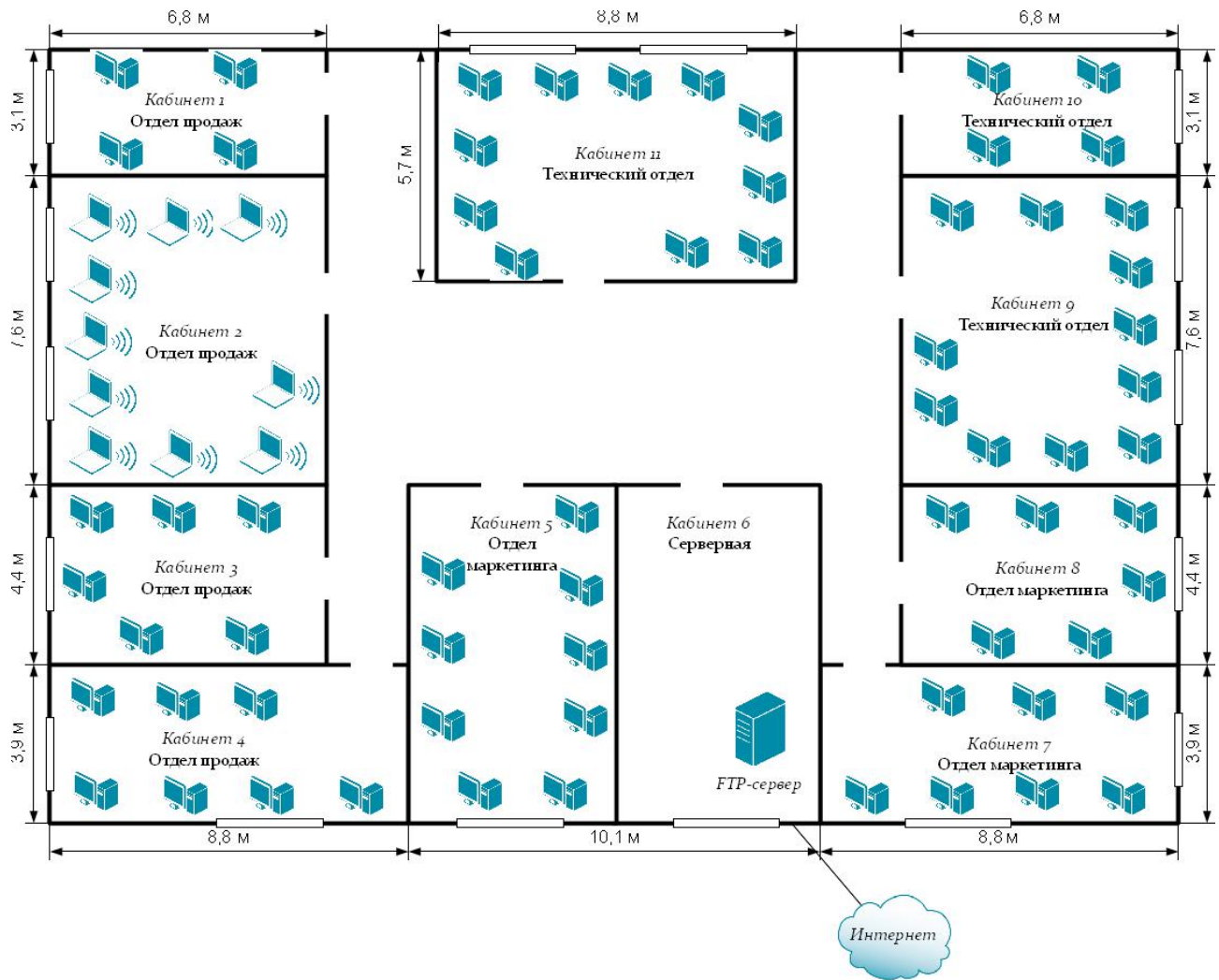


Рисунок 13.1 План предприятия