

# 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. МАС-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-Нос при помощи службы	
«Беспроводная настройка» ОС Windows XP	64
7.1.2 Создание беспроводной сети в режиме Ad-Нос для рабочих станций с	- 1
OC Windows Vista//	71
7.1.3 Создание оеспроводной сети в режиме Ad-Нос при помощи утилиты	70
D-Link Connection Manager.	/8
/.2 Создание оеспроводной сети в режиме инфраструктуры	81
Лаоораторная раоота №8. IP-адресация	ð /
8.1 Определение адреса сети, широковещательного адреса и количества узлов по	00
заданному IF-адресу и маске подсети.	09
8.2 Формирование подсетей с использованием масок переменной длины (VLSM)	95
8.5 Формирование подсетей и изстройка протокода IPv6 на рабоной стании	95
лаобраторная работа №2. эстановка и настроика протокола 11 vo на рабочен станци топка поступа D-L ink	ии и 07
9 1 Установка и настройка протокода IPv6 на рабоней станции	98
9.2 Полключение к точке доступа через Web-интерфейс с помощью IPv6-адреса	102
Лабораторная работа №10 Изучение принципа работы протокода ARP	107
Лабораторная работа №11. Организация межсетевого взаимолействия с помошью	•••107
маршрутизатора DIR-615	111
11 1 Организация межсетевого взаимолействия	112
11.2 Обеспечение доступа из внешней сети к FTP-серверу, который нахолится 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-cepbep Golden FTP Server v5.00 (http://www.goldenftpserver.com/download.html);
- Анализатор трафика Wireshark (<u>http://www.wireshark.org</u>).

## 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) МАС-адрес;	Сетевой уровень
г) пакет;	
д) номер порта;	Канальный уровень
е) сегмент;	
ж) биты.	

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.

a) TCP;	Транспортный уровень
б) IP;	
в) Ethernet;	Сетевой уровень
г) HTTP;	
д) UDP;	Уровень приложений
e) 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 ТСР 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;
- и 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;

*Mocm (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 8Р8С (RJ-45)

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





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



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.

### <u>Цель:</u>

- 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 волокно-оптический кабель;
- многомодовый волокно-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 МТ-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 разъеме 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 3.12 Разъем типа SC

*Разъем типа LC* имеет размер примерно в два раза меньше, чем разъемы SC, FC, ST, что позволяет реализовать большую плотность при установке на коммутационной панели.



Рисунок 3.13 Разъем типа LC

### 3.2. Обжим UTP-кабеля разъемами RJ-45

### ЗАДАНИЕ

Обожмите UTP-кабель с обеих сторон по стандарту EIA/TIA-568A или EIA/TIA-568B (прямой кабель) и проверьте его работоспособность при помощи сетевого тестера.

Шаг 1. Аккуратно снимите с одного конца кабеля 3-4 см внешней изоляции. После этого вы увидите восемь разноцветных проводов, скрученных попарно (рис.3.14).



Рисунок 3.14 Кабель UTP без внешней изоляции

Шаг 2. Раскрутите каждый проводник до начала внешней изоляции. Все проводники должны быть ровными и прямыми.

Шаг 3. Расположите восемь цветных проводников плотно друг к другу в соответствии со стандартом EIA/TIA-568A или EIA/TIA-568B (рис.3.15).



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 обжиме 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 сетевой кабель, который одним концом подключается в *сетевой аdanmep* – 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 определение 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.

#### <u>Пример:</u> 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.

#### <u>Пример:</u> ping <IP-адрес или доменное имя>

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

<u>Пример:</u> 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 ІР-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

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 ІР-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.

Фаил Правка Вил Избранное Сервис Л	ополнительно. Справка	
Саназад - Сана Поралко серона д		
Адрес:	🗸 🕞 Пере	
лв	С или высокоскоростной Интернет	
Сетевые задачи 🙁		
Создание нового	сети Отключить	
👰 Установить домашнюю	Подключ Состояние	
сеть или сеть малого офиса		
брандмауэра Windows		
Отключение сетевого устройства	Удалить	
Восстановление	Переименовать	
Подолозания	Свойства	
Подключения		
подключения		
одключение по локальной сети «свойства	conclusi ripotokon mitephera (ren m )	1
	0.6 mm	
щие Дополнительно	Общие	
щие Дополнительно одключение через:	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парам	етры
щие Дополнительно одключение через: IIII NVIDIA nForce Networking Controller Настроить	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парам IP можно получить у сетевого администратора.	етры
щие Дополнительно одключение через: NVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением:	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парам IP можно получить у сетевого администратора.	етры
щие Дополнительно одключение через: IIII NVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением: IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парам IP можно получить у сетевого администратора. Получить IP-адрес автоматически О Использовать следующий IP-адрес:	етры
щие Дополнительно одключение через: WVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением: Планировщик пакетов QoS Microsoft TCP/IP версии 6	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парами IP можно получить у сетевого администратора. Получить IP-адрес автоматически О Получить IP-адрес автоматически Использовать следующий IP-адрес: IP-адрес: 192.168.1.1	етры
щие Дополнительно одключение через: МVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением: Планировщик пакетов QoS Т Мicrosoft TCP/IP версии 6 Потокол Интернета (TCP/IP)	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парами IP можно получить у сетевого администратора. Получить IP-адрес автоматически О Получить IP-адрес автоматически О Использовать следующий IP-адрес: IP-адрес: IP-адрес: 192.168.1.1 Маска подсети: 255.255.0	етры
щие Дополнительно одключение через: МVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением: Планировщик пакетов QoS Г Мicrosoft TCP/IP версии 6 Г Протокол Интернета (TCP/IP) С	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парам IP можно получить у сетевого администратора. Получить IP-адрес автоматически О Использовать следующий IP-адрес: IP-адрес: IP-адрес: IP-адрес: 0сновной шлюз: 	етры ] ]
щие Дополнительно одключение через: МVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением: Планировщик пакетов QoS Г Мicrosoft TCP/IP версии 6 Потокол Интернета (TCP/IP) Установить Удалить Свойства	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парами IP можно получить у сетевого администратора. Получить IP-адрес автоматически VIспользовать следующий IP-адрес: IP-адр	етры
щие Дополнительно одключение через: ■ NVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением: Планировщик пакетов QoS Планировщик пакетов QoS Планировщик пакетов QoS Потокол Интернета (TCP/IP) Установить Удалить Свойства Описание	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парам IP можно получить у сетевого администратора. Получить IP-адрес автоматически VICпользовать следующий IP-адрес: IP-адрес: IP-адрес: IP-адрес: IP-адрес: ISS 255 255 0 Основной шлюз: Получить адрес DNS-сервера автоматически	етры
щие Дополнительно одключение через: ■ NVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением: Планировщик пакетов QoS Місгоsoft TCP/IP версии 6 Протокол Интернета (TCP/IP) Цалить Свойства Описание Протокол TCP/IP - стандартный протокол глобальных сетей, обеспечивающий связь между различными	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парами IP можно получить у сетевого администратора. Получить IP-адрес автоматически VICпользовать следующий IP-адрес: IP-адр	етры
щие Дополнительно одключение через: № NVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением: № Планировщик пакетов QoS № Мicrosoft TCP/IP версии 6 № Потокол Интернета (TCP/IP) № Установить Удалить Свойства Описание Протокол TCP/IP - стандартный протокол глобальных сетей, обеспечивающий связь между различными взаимодействующими сетями.	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парам IP можно получить у сетевого администратора. О Получить IP-адрес автоматически О Использовать следующий IP-адрес: IP-а	етры
щие Дополнительно одключение через: ■ NVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением: Планировщик пакетов QoS Планировщик пакетов QoS Протокол Интернета (TCP/IP) Свойства Описание Протокол TCP/IP - стандартный протокол глобальных сетей, обеспечивающий связь между различными взаимодействующими сетями.	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парам IP можно получить у сетевого администратора. Получить IP-адрес автоматически VICпользовать следующий IP-адрес: IP-адре	етры ] ] ]
щие Дополнительно одключение через: NVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением: Ланировщик пакетов QoS Microsoft TCP/IP версии 6 Microsoft TCP/IP естандартный протокол глобальных сетей, обеспечивающий связь между различными взаимодействующими сетями. При подключении вывести значок в области уведомлений Уведомлять при ограниченном или отсутствующем подключении	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парам IP можно получить у сетевого администратора. Получить IP-адрес автоматически	етры
цие Дополнительно одключение через: № NVIDIA nForce Networking Controller Настроить омпоненты, используемые этим подключением: № Планировщик пакетов QoS № Мicrosoft TCP/IP версии 6 № Протокол Интернета (TCP/IP) № Протокол Интернета (TCP/IP) № Ш Установить Удалить Свойства Описание Протокол TCP/IP - стандартный протокол глобальных сетей, обеспечивающий связь между различными взаимодействующими сетями. При подключении вывести значок в области уведомлений Уведомлять при ограниченном или отсутствующем подключении	Общие Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае парами IP можно получить у сетевого администратора. Получить IP-адрес автоматически <ul> <li>Получить IP-адрес автоматически</li> <li>Использовать следующий IP-адрес:</li> <li>IP-адрес:</li> <li>192.168.1.1</li> <li>Маска подсети:</li> <li>255.255.255.0</li> <li>Основной шлюз:</li> <li>.</li> </ul> <li>Получить адрес DNS-сервера автоматически <ul> <li>Использовать следующие адреса DNS-серверов:</li> <li>Предпочитаемый DNS-сервер:</li> <li>.</li> </ul> </li>	стры

Рисунок 4.3 Настройка статического IP-адреса для OC 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

ройка параметров компью	гера							Просмотр: Крупные значки 🔻
Flash Player (32 бита)		Java	<b>N</b>	Windows Anytime Upgrade	In	Windows CardSpace		Автозапуск
Администрирование	2	Архивация и восстановление	1	Брандмауэр Windows	R	Восстановление		Гаджеты рабочего стола
Дата и время		Датчик расположения и другие датчики	han	Диспетчер Realtek HD	-	Диспетчер устройств	0	Диспетчер учетных данных
Домашняя группа	調	Защитник Windows	0	Звук	0 0 0.01	Значки области уведомлений	۹	Клавиатура
Мышь		Панель задач и меню "Пуск"	R	Параметры индексирования		Параметры папок	-	Подключения к удаленным рабочим
Приступая к работе		Программы и компоненты	۲	Программы по умолчанию	Ŷ	Распознавание речи		Родительский контроль
Свойства обозревателя	N	Система	No	Счетчики и средства производительности	٩	Телефон и модем	1	Управление цветом
Устранение неполадок	-	Устройства и принтеры	8	Учетные записи пользователей	5	Центр мобильности Windows	æ	Центр обновления Windows
Иентр поддержки	۲	Центр синхронизации	٢	Центр специальных возможностей	4	Центр управления сетями и общим доступом	A	Шрифты
Экран	۶	Электропитание	P	Язык и региональные стандарты				

Рисунок 4.4 Окно Панель управления

<u>Примечание:</u> 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);

Танель управления - домашняя страница	Просмотр основных сведений о сети и н	настройка подключений
Изменение параметров	🦓 —— 🐺 —	<b>Ж</b> Просмотр полной карты
	EDU1-NOTE Неопознанная сеть (этот компьютер)	Интернет
параметры общего доступа	Просмотр активных сетей	Подключение или отключение
		Тип доступа: Без доступа к Интернету
	Неопознанная сеть Общественная сеть	Подключения: 📱 Подключение по локальной сети
	Изменение сетевых параметров	
	🚛 Настройка нового подключения или сети	
	Настройка беспроводного, широкополос или же настройка маршрутизатора или то	сного, модемного, прямого или VPN-подключения очки доступа.
	📸 Подключиться к сети	
	Подключение или повторное подключен сетевому соединению или подключение	ие к беспроводному, проводному, модемному к VPN.
	🚜 Выбор домашней группы и параметров о	общего доступа
	Доступ к файлам и принтерам, располож изменение параметров общего доступа.	сенным на других сетевых компьютерах, или
	Устранение неполадок	
	Диагностика и исправление сетевых проб	блем или получение сведений об исправлении.

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 ІР-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.

	Диа	ностика подключе	ния	**	1. St	- •		0
Беспроводное сетевое	одключ еть 13	чение по локальної	й сети					
Вг.	•	Отключить Состояние Диагностика Настройка моста Создать ярлык Удалить						
	8 8	Переименовать Свойства						
лючение через:	\$	Общие Параметры IP мог	ут назна	чаться авт	гоматическ	ки, еслі	и сеть	
слючение через: Broadcom NetLink (TM) Gigabit Ethemet Настроить		Овщие Параметры IP мог поддерживает эт IP можно получит Получить IP	гут назна гу возмож гь у сетен -адрес ав	чаться ав кность. В п вого админ	гоматическ ротивном ( истратора ски	ки, еслі случае а.	и сеть параме	тры
спючение через: Broadcom NetLink (TM) Gigabit Ethemet Настроить зченные компоненты используются этим подключением: Клиент для сетей Microsoft	5	Параметры IP мог поддерживает эт IP можно получит Получить IP	гут назна гу возмож гь у сете -адрес ав гь следун	ичаться ав кность. В п вого админ втоматичес ощий IP-ад	гоматическ ротивном ( истратора жи црес:	ки, еслі случае а.	и сеть параме	тры
спючение через: Broadcom NetLink (TM) Gigabit Ethemet Настроить еченные компоненты используются этим подключением: Клиент для сетей Microsoft Планировщик пакетов QoS Служба доступа к Файлам и принтерам сетей Micro Построиться (использование) Служба доступа к Файлам и принтерам сетей Micro	÷.	Овщие Параметры IP мог поддерживает эт IP можно получит Получить IP О Использоват IP-адрес: Маска подсети	гут назна гу возмож љ у сетен -адрес ан гъ следун 1:	нчаться ав: кность. В п вого админ зтоматиче ощий IP-ад	гоматическ ротивном с истратора ски црес: 192 . 168 255 . 25	ки, если случае а. 8 . 1 5 . 255	и сеть параме , 1 , 0	тры
слючение через: Broadcom NetLink (TM) Gigabit Ethemet Настроить еченные компоненты используются этим подключением: Клиент для сетей Microsoft Планировщик пакетов QoS Служба доступа к Файлам и принтерам сетей Micro Протокол Интернета версии 6 (TCP/IPv6) Протокол Интернета версии 4 (TCP/IPv4)		Овщие Параметры IP мог поддерживает эт IP можно получит Получить IP Оспользоват IP-адрес: Маска подсети Основной шлю	гут назна гу возмож - у сете - адрес ав гъ следун 1: 1:	ичаться ав кность. В п вого админ зтоматичею ощий IP-ад	гоматическ ротивном ( истратора ски црес: 192 . 164 255 . 255	ки, если случае а. 8 . 1 5 . 255	и сеть параме , 1 , 0 ,	тры
слючение через: Broadcom NetLink (TM) Gigabit Ethemet Настроить еченные компоненты используются этим подключением: Чилент для сетей Microsoft Планировщик пакетов QoS Служба доступа к файлам и принтерам сетей Micro Протокол Интернета версии 6 (TCP/IPv6) Протокол Интернета версии 4 (TCP/IPv4) Драйвер в/в тополога канального уровня Ответчик обнаружения топологии канального уровня		Овщие Параметры IP мог поддерживает эт IP можно получит © Получить IP @ Использоват IP-адрес: Маска подсети Основной шлю © Получить ад @ Использоват	тут назна гу возмож гь у сетен -адрес ан гь следун н: 13: црес DNS- гь следун	чаться ав кность. В п вого админ этоматичек ощий IP-ад -сервера аг ощие адре	гоматическ ротивном ( истратора жи црес: 192 . 160 255 . 251	ки, если случае а. 8 . 1 5 . 255 ски оверов:	и сеть параме , 1 , 0	тры
спючение через: Вroadcom NetLink (TM) Gigabit Ethemet Настроить вченные компоненты используются этим подключением: ченные компоненты использии использи использии использии использии использии использии использи		Овщие Параметры IP мог поддерживает эт IP можно получит © Получить IP © Использоват IP-адрес: Маска подсети Основной шлю © Получить ад © Использоват Предпочитаем Альтернативне	тут назна гу возмож ть у сетен -адрес ав ть следун и: ирес DNS-с ый DNS-с ый DNS-с	чаться ав кность. В п вого админ этоматичес ощий IP-ад ощий IP-ад ощие адре ервер: ервер:	гоматическ ротивном ( истратора жи црес: 192.16( 255.25)	ки, если случае а. 8 . 1 5 . 255 ски рверов:	и сеть параме . 1 . 0	тры

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

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



Рисунок 4.7 Проверка конфигурации сетевого адаптера

<u>Чтобы открыть командную строку в Windows XP, выполните следующие действия:</u> 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 OC Windows XP

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

Пуск → Все программы→ Стандартные → Командная строка

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

- 1. Нажмите меню Пуск и в строке поиска введите ста;
- 2. Нажмите на клавиатуре Enter.



Рисунок 4.9 Запуск командной строки через cmd.exe для OC 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 соединение между ПК2 и коммутатором.



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

<u>Чтобы открыть общий доступ к nanke в Windows XP, выполните следующие действия:</u>

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;

6 ULT IDCTUD Lagrange average	1
пощие достэн Пастроика	
Локальный общий доступ	и безопасность
Чтобы разрешить л пользователям к з папку <u>Общие доку</u> г	доступ другим локальным лой папке, переместите ее в <u>менты</u> .
Чтобы запретить с подпапкам, устано	общий доступ к этой папке и ее вите этот флажок.
Отменить общи	й доступ к этой папке
Открыть общий доо	ступ к этой папке
Имя общего ресурса:	Задания
	ние файлов по сети
🗹 Разрешить измене	Conception of the second s
Разрешить измене Подробнее об <u>общем дости</u>	пе и безопасности.

Рисунок 4.12

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

<u>Чтобы открыть общий доступ к папке в Windows 7/Vista, выполните следующие действия:</u> 1. Включите общий сетевой доступ:

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

🚱 🗢 🖳 « Все 🕨 Центр у	правления сетями и общим доступ 👻 🍫 Поиск в панели управления 🔎
Панель управления - домашняя страница Изменение параметров адаптера Изменить дополнительные параметры общего доступа	Просмотр основных сведений о сети и настройка подключений Просмотр полной карты EDU1-NOTE (этот компьютер) Просмотр активных сетей В данный момент вы не подключены ни к какой сети.
	Изменение сетевых параметров Настройка нового подключения или сети Настройка беспроводного, широкополосного, модемного, прямого или VPN-подключения или же настройка маршрутизатора или точки доступа. Подключение или повторное подключение к беспроводному, проводному, модемному сетевому соединению или подключение к VPN. Выбор домашней группы и параметров общего доступа Доступ к файлам и принтерам, расположенным на других сетевых компьютерах, или изменение параметров общего доступа.
См. также Брандмауэр Windows Домашняя группа Свойства обозревателя	Устранение неполадок Диагностика и исправление сетевых проблем или получение сведений об исправлении.

Рисунок 4.13 Изменение дополнительных параметров общего доступа

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

🚱 🔍 🔻 Щентр у 🕨 Дополнительные параметры общего доступа 💿 👻 🥠 Поиск в панели управл	ения 🔎
Изменить параметры общего доступа для различных сетевых профилей	
Windows создает отдельный сетевой профиль для каждой используемой сети. Для каждого профиля можно выбрать особые параметры.	
Домашний или рабочий 🦳 😪	)
Общий (текущий профиль)	)
Сетевое обнаружение	
Если сетевое обнаружение включено, этот компьютер может видеть другие компьютеры и устройства сети и в свою очередь будет виден другим компьютерам. <u>Что такое сетевое</u> <u>обнаружение?</u>	
Включить сетевое обнаружение	
Отключить сетевое обнаружение	
Общий доступ к файлам и принтерам	
Если общий доступ к файлам и принтерам включен, то файлы и принтеры, к которым разрешен общий доступ на этом компьютере, будут доступны другим пользователям в сети.	
Включить общий доступ к файлам и принтерам	
Отключить общий доступ к файлам и принтерам	
Доступ к общим папкам	
Если включен общий доступ к общим папкам, пользователи сети могут получать доступ к файлам в таких папках. <u>Что такое общая папка?</u>	
Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках	
Отключить общий доступ (пользователи, выполнившие вход на этот компьютер, будут иметь доступ к общим папкам)	
	+
Сохранить изменения     Отмена	

Рисунок 4.14 Включение опций

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

🚱 🔍 💌 💐 « Центр у ) Дополнительные параметры общего доступа 🔹 😽 Поиск в панели управлен	ия 🔎
Если включен общий доступ к общим папкам, пользователи сети могут получать доступ к файлам в таких папках. <u>Что такое общая папка?</u>	*
Включить общий доступ, чтобы сетевые пользователи могли читать и записывать файлы в общих папках	
Отключить общий доступ (пользователи, выполнившие вход на этот компьютер, будут иметь доступ к общим папкам)	
Потоковая передача мультимедиа	
Если потоковая передача файлов мультимедиа включена, пользователи и устройства в сети могут получать доступ к изображениям, музыке и видео на этом компьютере. Кроме того, этот компьютер может находить файлы мультимедиа в сети.	
Выберите параметры потоковой передачи мультимедиа	
Подключения общего доступа к файлам	
Windows 7 использует 128-битное шифрование для защиты подключений общего доступа. Некоторые устройства не поддерживают 128-битное шифрование и должны использовать 40- битное или 56-битное шифрование.	
<ul> <li>Использовать 128-битное шифрование для защиты подключений общего доступа (рекомендуется)</li> </ul>	
Включить общий доступ к файлам для устройств, использующих 40-битное или 56-битное шифрование	E
Общий доступ с парольной защитой	
Если включена парольная защита общего доступа, только пользователи с учетной записью и паролем на этом компьютере могут получить доступ к общим файлам, к принтерам, подключенным к этому компьютеру, и к общим папкам. Чтобы открыть доступ другим пользователям, нужно отключить парольную защиту общего доступа.	
<ul> <li>Включить общий доступ с парольной защитой</li> <li>Отключить общий доступ с парольной защитой</li> </ul>	
Сохранить изменения Отмена	•

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;

🔾 🗢 📕 🕨 Компьк	тер 🕨 ACER (С:) 🕨 Новая папка 🕨		🔻 🔩 Поиск: Новая папка		Q
Упорядочить 🔻 🗦	Открыть Добавить в библиотеку	•	Общий доступ 🔻 🚿	•	?
🔆 Избранное	Имя		Дата изменения Тип	Размер	
〕 Загрузки	길 Задания		20.02.2013 15:38 Папка с файлами		
🗓 Недавние места 💻 Рабочий стол			Открыть Открыть в новом окне 7-Zip		
Библиотеки Видео Документы Изображения			Общий доступ Восстановить прежнюю версию Defraggler	•	
🚽 Музыка		۲	Сканировать программой ESET NOD32 Antiviru Расширенные функции	JS	
🖳 Компьютер			Добавить в библиотеку	- F	
🚢 ACER (C:)		8	Отправить	+	
Фт Сеть 1∰ EDU1-NOTE			Вырезать Копировать		
			Создать ярлык Удалить Переименовать		
Залания	Лата изменения: 20.02.2013 15:38		Свойства		

Рисунок 4.16

7. На вкладке Доступ нажмите на кнопку Расширенная настройка;

Общие         Доступ         Безопасность           Общий доступ к сетевым файлам и папкам         Задания         Задания           Мет общего доступа         Задания         Нет общего доступа           Сетевой путь:         Нет общего доступа         Общий доступ           Расширенная настройка общего доступа         Предоставляет пользовательские разрешения, создает общие папки и задает другие дополнительные параметры общего доступа.           Расширенная настройка         Защита паролем           Пользователы, не имеющие учетной записи и пароля для этого компьютера, имеют доступ к папкам, доступным для всех.           Изменить этот параметр можно через Центр управления сетями и общим доступом.	Предыдущ	ие версии	Настройка
Общий доступ к сетевым файлам и папкам Задания Нет общего доступа Сетевой путь: Нет общего доступа Общий доступ Расширенная настройка общего доступа Предоставляет пользовательские разрешения, создает общие папки и задает другие дополнительные параметры общего доступа. Расширенная настройка Расширенная настройка Защита паролем Пользователи, не имеющие учетной записи и пароля для этого компьютера, имеют доступ к папкам, доступным для всех. Изменить этот параметр можно через Центр управления сетями и общим доступом.	Общие	Доступ	Безопасность
Расширенная настройка общего доступа Предоставляет пользовательские разрешения, создает общие папки и задает другие дополнительные параметры общего доступа. Расширенная настройка Защита паролем Пользователи, не имеющие учетной записи и пароля для этого компьютера, имеют доступ к папкам, доступным для всех. Изменить этот параметр можно через <u>Центр управления</u> <u>сетями и общим доступом</u> .	Общий доступ к Задан Нет об Сетевой путь: Нет общего дою	: сетевым файлам и г ия и́щего доступа ступа	апкам
Защита паролем Пользователи, не имеющие учетной записи и пароля для этого компьютера, имеют доступ к папкам, доступным для всех. Изменить этот параметр можно через <u>Центр управления</u> <u>сетями и общим доступом</u> .	Общий достуг Расширенная н	1 астройка общего дос	тупа
Пользователи, не имеющие учетной записи и пароля для этого компьютера, имеют доступ к папкам, доступным для всех. Изменить этот параметр можно через <u>Центр управления</u> <u>сетями и общим доступом</u> .	Общий достуг Расширенная н Предоставляет общие папки и общего доступа Прасширен	п астройка общего дос пользовательские р задает другие дополн а. нная настройка	тупа азрешения, создает нительные параметры
	Общий доступ Расширенная н Предоставляет общие папки и общего доступа Фрасширен Защита пароле	п астройка общего дос пользовательские р задает другие дополн а. иная настройка	тупа азрешения, создает нительные параметры

Рисунок 4.17

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

араметры	
имя оощего ресурса: Задания	
Добавить Удалить	
Ограничить число одновременных	20 🌲
пользователеи до: Примечание:	
Разрешения Кэширование	

Рисунок 4.18

9. Установите галочку Полный доступ → Разрешить;

Разрешения для общего ресурса	3	
Группы или пользователи.		
e pce		
	Побарить	Vasaut
		7 10 10 10
	дооавить	у далить
Разрешения для группы "Все"	Разреши	ть Запретить
Разрешения для группы "Все"	Разреши	ъ Вапретить
Разрешения для группы "Все" Полный доступ Изменение	Paspeuur	вапретить
Разрешения для группы "Все" Полный доступ Изменение Чтение	Paspeuur V V	ъ Запретить
Разрешения для группы "Все" Полный доступ Изменение Чтение	Paspeuur V V	љ Вапретить
Разрешения для группы "Все" Полный доступ Изменение Чтение		ъ Вапретить
Разрешения для группы "Все" Полный доступ Изменение Чтение	Paspeuur V V	ъ Вапретить
Разрешения для группы "Все" Полный доступ Изменение Чтение	Paspeuur V V	ъ Вапретить
Разрешения для группы "Все" Полный доступ Изменение Чтение	Paspeuur V V	ъ Вапретить
Разрешения для группы "Все" Полный доступ Изменение Чтение Подробнее об управлении дост	Разреши Г Г Г Г Г Г Г Г Г Г Г Г Г	ъ Вапретить

Рисунок 4.19

- Нажмите кнопку Ок, чтобы вернуться во вкладку Доступ;
   Во вкладке Доступ нажмите на кнопку Общий доступ.

Предыдущие версии		Настройка
Общие	Доступ	Безопасность
Общий доступ к Задани Есть о Сетевой путь: \\Edu1note\заи Общий достуг Расширенная на	сетевым файлам и па ия бщий доступ дания	пкам
Предоставляет общие папки и	астроика оощего досту пользовательские ра: задает другие дополни	/па зрешения, создает (тельные параметры
Предоставляет общие папки и общего доступа Расширен	астроика оощего досту пользовательские ра: задает другие дополни а. ная настройка	па зрешения, создает ітельные параметры
Предоставляет общие папки и общего доступа Расширен Защита паролег	астроика оощего досту пользовательские раз задает другие дополни а. иная настройка	па зрешения, создает тельные параметры

Рисунок 4.20

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

Выберите пользо	вателей, которым следует	открыть доступ	
Введите имя и нажмит	е кнопку "Добавить" либо исполь	зуйте стрелку для поиска определенного	
edu1		Добавить	
Гость		азрешений	
Все	ORATEDO	апись 🔻	
	obare/M	оладелец	
			×
-			
6	列 🛃 Общий доступ к файлам		
	Выберите пользовател	ей, которым следует открыть доступ	
Проблемы при от	bioopine nonboobaron	си, которыш следует открыть доступ	
	Введите имя и нажмите кнопк	у "Добавить" либо используйте стрелку для поиска определе	нного
	пользователя.		
	Bce	- Добавить	
	Имя	Уровень разрешений	
	🙎 edul	Чтение и запись 💌	
	(2 A	Владелец	
	Администраторы		
	м Администраторы		×
	а Администраторы	0.5	×
	ма Администраторы	🕞 🖪 Общий доступ к файлам	
	ад Администраторы	🕞 🖪 Общий доступ к файлам	
	ад Администраторы	Общий доступ к файлам Выберите пользователей, которым следует	
	Проблемы при открытии о(	Общий доступ к файлам Выберите пользователей, которым следует	т открыть доступ
	Проблемы при открытии о!	Общий доступ к файлам Выберите пользователей, которым следует Веедите имя и нажмите кнопку "Добавить" либо исполи	т открыть доступ ьзуйте стрелку для поиска определенного
	Проблемы при открытии о	Общий доступ к файлам Выберите пользователей, которым следует Введите имя и нажмите кнопку "Добавить" либо исполи пользователя.	т открыть доступ взуйте стрелку для поиска определенного
	Проблемы при открытии о	Общий доступ к файлам Выберите пользователей, которым следует Введите имя и нажмите кнопку "Добавить" либо исполи пользователя.	Т ОТКРЫТЬ ДОСТУП Базуйте стрелку для поиска определенного
	Проблемы при открытии о!	Общий доступ к файлам Выберите пользователей, которым следует Введите имя и нажмите кнопку "Добавить" либо исполя пользователя.	<ul> <li>Т ОТКРЫТЬ ДОСТУП</li> <li>ьзуйте стрелку для поиска определенного</li> <li>Добавить</li> </ul>
	Проблемы при открытии о!	Общий доступ к файлам Выберите пользователей, которым следует Введите имя и нажмите кнопку "Добавить" либо исполь пользователя. Имя	<ul> <li>Т ОТКРЫТЬ ДОСТУП</li> <li>ьзуйте стрелку для поиска определенного</li> <li>Добавить</li> <li>Уровень разрешений</li> </ul>
	Проблемы при открытии о!	<ul> <li>Общий доступ к файлам</li> <li>Выберите пользователей, которым следует</li> <li>Введите имя и нажмите кнопку "Добавить" либо исполи пользователя.</li> <li>Имя</li> <li>edul</li> </ul>	Т ОТКРЫТЬ ДОСТУП ьзуйте стрелку для поиска определенного ↓ Добавить Уровень разрешений Чтение и запись ↓
	Проблемы при открытии о(	<ul> <li>Общий доступ к файлам</li> <li>Выберите пользователей, которым следует</li> <li>Введите имя и нажмите кнопку "Добавить" либо испольпользователя.</li> <li>Имя</li> <li>д edul</li> <li>Алминистраторы</li> </ul>	х т открыть доступ ьзуйте стрелку для поиска определенного ↓ Добавить Уровень разрешений Чтение и запись ↓ Влалелен
	Проблемы при открытии о(	<ul> <li>Общий доступ к файлам</li> <li>Выберите пользователей, которым следует</li> <li>Введите имя и нажмите кнопку "Добавить" либо испольпользователя.</li> <li>Имя</li> <li>edul</li> <li>Администраторы</li> <li>Все</li> </ul>	х т открыть доступ ьзуйте стрелку для поиска определенного √ Добавить Уровень разрешений Чтение и запись ▼ Владелец Чтение и запись ▼

Рисунок 4.21
#### 13. Нажмите Общий доступ;

Выберите пользователей, которы	м следует открыть доступ
Введите имя и нажмите кнопку "Добавить" .	либо используйте стрелку для поиска определенног
пользователя.	
	- Добавить
Имя	Уровень разрешений
🙎 edu1	Чтение и запись 🔻
🚨 Администраторы	Владелец
Sce	Чтение и запись 🔻

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. МАСадреса

*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 (МАС-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,	Адреса	Информация о	Данные	Контрольная	Поле,
определяющее	отправителя и	протоколе		сумма	определяющее
начало кадра	получателя	сетевого уровня			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-adpeca*.

*MAC-adpec (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 МАС-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 МАС-адреса показана на рис. 5.1.



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

(снифером), то есть программой для анализа пакетов сети Ethernet и некоторых других сетей. Характеризуется тем, что имеет графический интерфейс пользователя и много возможностей по сортировке и фильтрации информации. *Wireshark* позволяет просматривать весь трафик сети в режиме реального времени. С помощью нее можно определить причину странного поведения какого-либо оборудования и источник, вызвавший это поведение.

*Wireshark* «знает» структуру разнообразных протоколов и поэтому позволяет разбирать сетевой пакет, отображая значение каждого поля протокола любого уровня.

- Основные возможности Wireshark следующие:
- захват пакетов из сети в режиме реального времени;
- отображение пакета с очень подробной информацией о протоколе;
- открытие и сохранение записанных данных;
- фильтрация пакетов по многим критериям;
- поиск пакетов по многим критериям;
- выделение разными цветами пакетов на основании фильтров.

### Оборудование (на 1 рабочее место):

Рабочая станция	2 шт.
Кабель Ethernet	1 шт.
ПО — анализатор трафика Wireshark	

**Цель:** анализ сетевого трафика при помощи программы Wireshark, исследование структуры кадра.



Шаг 1. Подключите один конец Ethernet-кабеля к сетевому адаптеру ПК1, а другой конец кабеля — к сетевому адаптеру ПК2 (рис. 5.2).

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

Шаг 3. Проверьте МАС-адрес сетевого адаптера ПК1. В командной строке введите: getmac

Запишите МАС-адрес (физический адрес) ПК1\_\_\_\_\_

Шаг 4. Проверьте МАС-адрес сетевого адаптера ПК2. В командной строке введите: getmac

Запишите МАС-адрес (физический адрес) ПК2

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

File       Edit       Yiew       Go       Capture       Analyze       Statistics       Telephony       Jools       Internals       Help         Image: Image
Image: Solution
Filter:       Expression       Clear       Apply       Save         No.       Time       Source       Destination       Protocol       Length       Info       Implementation       Protocol       Length       Implementation       Implementation       Protocol       Length       Implementation       Protocol       Length       Implementation       Implementation       Implementation       Protocol       Length       Implementation       Protocol       Length       Implementation       Implementation       Implementation       Implementation       Implementation       Implementation       Implementation
No.         Time         Source         Destination         Protocol Length Info         A           1         0.00000000 192.168.1.1         192.168.1.2         TCMP         7.4 Echo         (ping)         request         id=0x0001, seq=5/1280, ttl=128         Id=0x0001, seq=5/1280, ttl=128           2         0.00033000 wistronI_72:a5:82         wistronI_73:7c:8c         ARP         60 who has 192.168.1.1         Tell 192.168.1.2         Tell 192.168.1.1         Tell 192.168.1.2         1d=0x0001, seq=5/1280, ttl=128           4         0.00033000 wistronI_72:a5:82         wistronI_73:7c:8c         ARP         42 192.168.1.1         is a 20:6a:8a:72:a5:82           4         0.0003192.168.1.2         192.168.1.1         ICMP         74 Echo (ping) reply         id=0x0001, seq=5/1280, ttl=128           5         1.00165900 192.168.1.1         192.168.1.1         ICMP         74 Echo (ping) reply         id=0x0011, seq=6/1536, ttl=128           6         1.00213300 192.168.1.2         192.168.1.1         ICMP         74 Echo (ping) reply         id=0x0011, seq=6/1536, ttl=128           7         2.01671300 192.168.1.2         192.168.1.1         ICMP         74 Echo (ping) reply         id=0x0011, seq=6/1536, ttl=128           9         3.02992400 192.168.1.2         192.168.1.1         ICMP         74 Echo (ping) reply         id=0x0
1 0.0000000 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) request id=0x0001, seq=5/1280, tt]=128         2 0.00031400 wistronT_73:7C:8c       Broadcast       ARP       60 who has 192.168.1.1?       Tell 192.168.1.2         3 0.00033000 wistronT_72:35:82       WistronT_73:7C:8c       ARP       60 who has 192.168.1.1?       Tell 192.168.1.2         4 0.00051800 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request id=0x0001, seq=5/1280, tt]=128         5 1.00165900 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) request id=0x0001, seq=5/1280, tt]=128         6 1.00213300 192.168.1.1       192.168.1.1       ICMP       74 Echo (ping) request id=0x0001, seq=6/1536, tt]=128         8 2.01617300 192.168.1.1       192.168.1.1       ICMP       74 Echo (ping) request id=0x0001, seq=6/1536, tt]=128         9 3.02992400 192.168.1.1       192.168.1.1       ICMP       74 Echo (ping) request id=0x001, seq=5/1280, tt]=128         10 3.03038600 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request id=0x001, seq=5/1280, tt]=128         11 49.8158680 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request id=0x001, seq=5/1280, tt]=128         12 49.8161180 wistronT_72:3582       Broadcast       ARP       42 who has 192.168.1.2?       192.168.1.1         13 49.8164380 wistronT_73:7C:8c       wistronT_72:35:82
2 0.00031400 WistronI_73:7C:8c Broadcast ARP 60 Who has 192.168.1.1? Tell 192.168.1.2 3 0.00033000 WistronI_72:a5:82 WistronI_73:7C:8c ARP 42 192.168.1.1 is at 20:6a:8a:72:a5:82 4 0.00051800 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 5 1.00165900 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=128 6 1.00213300 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reply id=0x001, seq=6/1536, ttl=128 8 2.01617300 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0701 eq=6/1536, ttl=128 9 3.02992400 192.168.1.1 192.168.1.1 ICMP 74 Echo (ping) reply 77/2, ttl=128 10 3.03038600 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) request 7/2048, ttl=128 10 3.03038600 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) request 7/2048, ttl=128 12 49.8161180 WistronI_72:a5:82 Broadcast ARP 42 Who has 192.168.1.2? APP 42 Hox 0001, seq=5/1280, ttl=128 13 49.8164380 wistronI_72:a5:82 Broadcast ARP 42 Who has 192.168.1.2? APP 42 Hox 0001, seq=5/1280, ttl=128 14 49.816470 192.168.1.1 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 14 9.8164380 wistronI_72:a5:82 Broadcast ARP 42 Who has 192.168.1.2? APP 42 Hox 0001, seq=5/1280, ttl=128 15 50.8195000 192.168.1.1 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 15 50.8195000 192.168.1.1 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 15 50.8195000 192.168.1.1 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 16 50.819540 192.168.1.1 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 17 51 8330100102 168.1.1 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 17 51 8330100102 168.1.1 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 17 51 833010102 168.1.1 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 18 Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
3 0.00033000 WistronI_72:a5:82 WistronT_73:7C:8c ARP 42 192.168.1.1 is at 20:6a:8a:72:a5:82 4 0.00051800 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 5 1.00165900 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=128 6 1.00213300 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=128 7 2.01571300 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=128 8 2.01617300 192.168.1.1 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 9 3.02992400 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 10 3.03038600 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) request //2048, ttl=128 11 49.8158680 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) request //2048, ttl=128 12 49.8161180 wistronI_72:a5:82 Broadcast ARP 42 who has 192.168.1.2? ICMP 74 Echo (ping) request //2048, ttl=128 13 49.8164380 wistronI_73:7c:8c WistronI_72:a5:82 ARP 60 192.168.1.2 is at 20:6a:8a:73:7c:8c 14 49.8164770 192.168.1.1 192.168.1.1 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 15 50.8195000 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 15 50.8195000 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 15 50.8195000 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 16 50.8196540 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 17 51 833010102 168.1.2 192.168.1.1 ICMP 74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=128 17 51 833010102 168 1 2 192.168.1.1 ICMP 74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=128 17 51 833010102 168 1 1 TCMP 74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=128 18 Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
4 0.00051800 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 5 1.00165900 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 6 1.00213300 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) request id=0x001 seq=6/1536, ttl=128 7 2.01571300 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reply id=0x071 sq=6/1536, ttl=128 8 2.01617300 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) request id=0x071 sq=6/1536, ttl=128 9 3.02992400 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) request 792, ttl=128 10 3.03038600 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reply 74 Echo (ping) request 7/2048, ttl=128 11 49.8158680 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) request 7/2048, ttl=128 12 49.8161180 wistronI_72:a5:82 Broadcast ARP 42 Who has 192.168.1.2? 11 192.168.1.1 13 49.8164380 wistronI_73:7c:8c wistronI_72:a5:82 ARP 60 192.168.1.2 is at 20:6a:8a:73:7c:8c 14 49.8164770 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 15 50.8195000 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 15 50.8195000 192.168.1.1 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 15 50.8195000 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 16 50.8196540 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 17 51 833010102 168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=5/1586, ttl=128 17 51 833010102 168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=5/1586, ttl=128 17 51 833010102 168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 833010102 168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 833010102 168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 833010102 168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 833010102 168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=7/1
51.00165900 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) request       id=0x0001, seq=6/1536, ttl=128         61.00213300 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request       id=0x001, seq=6/1536, ttl=128         72.01571300 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) request       id=0x001, seq=6/1536, ttl=128         82.01617300 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) request       id=0x001, seq=6/1536, ttl=128         93.02992400 192.168.1.1       192.168.1.1       ICMP       74 Echo (ping) request       id=0x011, seq=6/1536, ttl=128         103.0303660192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request       id=0x011, seq=6/1536, ttl=128         1149.8158680 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request       id=0x014, seq=6/1526, ttl=128         1249.8161180 wistronI_72:a5:82       Broadcast       ARP       42 who has 192.168.1.2?       id=0x0001, seq=5/1280, ttl=128         13 49.8164380 wistronI_73:7C:8c       wistronI_72:a5:82       Broadcast       ARP       42 who has 192.168.1.2?       id=0x0001, seq=5/1280, ttl=128         15 50.8195000 192.168.1.1       192.168.1.1       ICMP       74 Echo (ping) request       id=0x0001, seq=5/1280, ttl=128         15 50.8195000 192.168.1.1       192.168.1.1       ICMP       <
6 1.00213300 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) reply       id=0x00 1       eq=6/1536, ttl=128         7 2.01571300 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) request       id=0x00 1       eq=6/1536, ttl=128         8 2.01617300 192.168.1.1       192.168.1.1       ICMP       74 Echo (ping) request       id=0x00 1       eq=6/1536, ttl=128         9 3.02992400 192.168.1.1       192.168.1.1       ICMP       74 Echo (ping) request       1792, ttl=128         10 3.03038600 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request       06nactb 1       2048, ttl=128         11 49.8158680 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request             12 49.8161180 wistronI_72:a5:82       Broadcast       ARP       42 who has 192.168.1.2
7 2.01571300 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) request       1       2/1792, ttl=128         8 2.01617300 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) requy       1792, ttl=128         9 3.02992400 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) requy       06nactb 1       /2048, ttl=128         10 3.03038600 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) requy       2048, ttl=128         11 49.8158680 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request       /2048, ttl=128         12 49.8161180 wistronI_72:a5:82       Broadcast       ARP       42 who has 192.168.1.2?       11 192.168.1.1         13 49.8164380 wistronI_73:7C:8c       WistronI_72:a5:82       ARP       60 192.168.1.2 is at 20:6a:8a:73:7c:8c         14 49.8164770 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) requy       id=0x0001, seq=5/1280, ttl=128         15 50.8195000 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) requy       id=0x0001, seq=6/1536, ttl=128         16 50.8196540 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) requy       id=0x0001, seq=6/1536, ttl=128         16 50.8196540 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) requy       id=0x0001, seq=6/1536, ttl=128         1
8 2.01617300 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) reply       1792, ttl=128         9 3.02992400 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) request       OGnactb 1       2048, ttl=128         10 3.03038600 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request       72, ttl=128         11 49.8158680 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request       72048, ttl=128         12 49.8161180 wistronI_72:a5:82       Broadcast       ARP       42 who has 192.168.1.2?       11 192.168.1.1         13 49.8164380 wistronI_73:7C:8c       wistronI_72:a5:82       Broadcast       ARP       42 who has 192.168.1.2?       11 192.168.1.1         13 49.8164380 wistronI_73:7C:8c       wistronI_72:a5:82       ARP       60 192.168.1.2 is at 20:6a:8a:73:7C:8c       11 192.168.1.1         15 50.8195000 192.168.1.1       192.168.1.1       ICMP       74 Echo (ping) request       id=0x0001, seq=5/1280, ttl=128         16 50.819540 192.168.1.1       192.168.1.1       ICMP       74 Echo (ping) request       id=0x0001, seq=6/1536, ttl=128         17 51 833010102 168.1.1       192.168.1.1       ICMP       74 Echo (ping) request       id=0x0001, seq=6/1536, ttl=128         17 51 833010102 168.1.1       192.168.1.1       ICMP       74 Echo (ping) request       id=0x0001, s
9 3.02992400 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) request Область 1 /2048, ttl=128 10 3.03038600 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reqly /2048, ttl=128 11 49.8158680 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) reqly /2048, ttl=128 12 49.8161180 wistronI_72:a5:82 Broadcast ARP 42 who has 192.168.1.2? /1192.168.1.1 13 49.8164380 wistronI_73:7c:8c wistronI_72:a5:82 ARP 60 192.168.1.2 is at 20:6a:8a:73:7c:8c 14 49.8164770 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) reqly id=0x0001, seq=5/1280, ttl=128 15 50.8196540 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 16 50.8196540 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 8330100 192.168.1.2 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 8330100 192.168.1.2 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 8330100 192.168.1.2 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 8330100 192.168.1.2 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 8330100 192.168.1.2 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 8330100 192.168.1.2 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 8330100 192.168.1.2 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 17 51 8330100 192.168.1.2 192.168.1.2 ICMP 74 Echo (ping) request id=0x0001, seq=7/1792 ttl=128
10 3.03038600 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) reply       3/2048, ttl=128         11 49.8158680 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request       3/2048, ttl=128         12 49.8161180 wistronI_72:a5:82       Broadcast       ARP       42 who has 192.168.1.2?       11 192.168.1.1         13 49.8164380 wistronI_73:7c:8c       wistronI_72:a5:82       ARP       60 192.168.1.2?       11 192.168.1.1         14 49.8164770 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) reply       id=0x0001, seq=5/1280, ttl=128         15 50.8195000 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, ttl=128         16 50.8196540 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, ttl=128         16 50.8196540 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, ttl=128         17 51 833010102 168 1.2       192.168.1.1       ICMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, ttl=128         17 51 833010102 168 1.2       192.168.1.1       ICMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, ttl=128         17 51 833010102 168 1.2       192.168.1.2       ICMP       74 Echo (ping) reply       id=0x0001, seq=7/1702       1128
11 49.8158680 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request       , sq=5/1280, tt]=128         12 49.8164180 wistronI_72:a5:82       Broadcast       ARP       42 who has 192.168.1.2?       (1192.168.1.1         13 49.8164380 wistronI_72:a5:82       WistronI_72:a5:82       ARP       60 192.168.1.2?       (1192.168.1.1         13 49.8164380 wistronI_72:a5:82       WistronI_72:a5:82       ARP       60 192.168.1.2?       (1192.168.1.1         13 49.8164380 wistronI_73:7C:8c       WistronI_72:a5:82       ARP       60 192.168.1.2?       (1192.168.1.2)         14 49.8164770 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) reply       id=0x0001, seq=5/1280, tt]=128         15 50.8195000 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, tt]=128         16 50.8196540 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, tt]=128         17 51 833010102 168 1 2       192.168.1.1       ICMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, tt]=128         17 51 833010102 168 1 2       192.168.1.1       TCMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, tt]=128         18 Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0       1128       1128
12 49.8161180 wistronI_72:a5:82       Broadcast       ARP       42 who has 192.168.1.2?       A1192.168.1.1         13 49.8164380 wistronI_73:7c:8c       wistronI_72:a5:82       ARP       60 192.168.1.2 is at 20:6a:8a:73:7c:8c         14 49.8164770 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) reply       id=0x0001, seq=5/1280, tt]=128         15 50.8195000 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, tt]=128         16 50.8196540 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, tt]=128         17 51 8330100 102 168 1 2       102 168 1 1       TCMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, tt]=128         18 Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0       102 168 1 1       102 168 1 1
13 49.8164380 wistronI_73:7c:8c       wistronI_72:a5:82       ARP       60 192.168.1.2 is at 20:6a:8a:73:7c:8c         14 49.8164770 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) reply       id=0x0001, seq=5/1280, tt]=128         15 50.8195000 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request       id=0x0001, seq=5/1280, tt]=128         16 50.8196540 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) reply       id=0x0001, seq=6/1536, tt]=128         17 51 8330100 102 168 1 2       102 168 1 1       TCMP       74 Echo (ping) repuest       id=0x0001, seq=6/1536, tt]=128         18 Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0       102 168 1 2       102 168 1 1
14 49.8164770 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0001, seq=5/1280, tt]=128 15 50.8195000 192.168.1.2 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, tt]=128 16 50.8196540 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) reply id=0x0001, seq=6/1536, tt]=128 17 51 833010102 168 1 2 192.168.1 1 TCMP 74 Echo (ping) reply id=0x0001, seq=6/1536, tt]=128 B Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
15       50.8195000 192.168.1.2       192.168.1.1       ICMP       74 Echo (ping) request       id=0x0001, seq=6/1536, ttl=128         16       50.819500 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) request       id=0x0001, seq=6/1536, ttl=128         16       50.8196540 192.168.1.1       192.168.1.2       ICMP       74 Echo (ping) request       id=0x0001, seq=6/1536, ttl=128         17       51       8330100 192.168.1.2       102.168.1.1       TCMP       74 Echo (ping) request       id=0x0001, seq=6/1536, ttl=128         17       51       8330100 192.168.1.2       102.168.1.1       TCMP       74 Echo (ping) request       id=0x0001, seq=7/1702 ttl=128         18       Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0       74       102.168.1.2       102.168.1.2
16 50.8196504 192.168.1.1 192.168.1.2 ICMP 74 Echo (ping) reguest id=0x0001, seq=6/1536, tt1=128 17 51 8330100 192 168 1 2 192 168 1 1 TCMP 74 Echo (ping) reguest id=0x0001, seq=6/1536, tt1=128 19 Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
17 51 8330100 102 168 1 2       102 168 1 1       TCMP       74 Echo (ping) Tepty       Id-0x0001, Seq=0/1330, Ct1=128         18 Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0       1       1       1
B Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
The Frame 1. 74 bytes on whe (352 bits), 74 bytes captured (352 bits) on internate o
$\Box$ Ethennet TT Cnet Wistner 70, E, 90 (00, E, 9, 70, E, 9) Dett Wistner 70, 7, 9, 9, (00, E, 9, 7), 7, 9, 9) $\land$
H Ethernet 11, SrC: Wistroni_/2:a532 (20:0a/8a/2/a3/82), DS: Wistroni_/3:/C:6C (20:0a/8a/2/3:/C:6C)
B Internet Protocol Version 4, Src: 192.108.1.1 (192.108.1.1), DSC: 192.108.1.2 (192.108.1.2)
B Internet Control Message Protocol
1
0000 20 6a 8a 73 7c 8c 20 6a 8a 72 a5 82 08 00 45 00 j.s .j.rE.
0020 01 02 08 00 4d 56 00 01 00 05 61 62 63 64 65 66NVabcdet
0000 07 61 62 63 64 65 65 77 68 69
wabelerg m
Broadcom NetLink (TM) Gigabit Ethernet Drive Packets: 259 Displayed: 259 Marked: 0

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*  $\rightarrow$  *Interfaces* или нажмите кнопку на верхней панели инструментов *List the available capture interfaces* (рис. 5.4).

Capturing from Broadcom NetLink (TM) Gigabit Ethernet Driver:	: \Device\NPF_{FDACB24C-D6AE-4623-A0B9-5DF0E0659758} [Wireshark 1.8.1 (SVN Rev 43946 from 📼 📼 🗪
<u>File Edit View Go Capture Analyze Statistics Telephon</u>	ny <u>T</u> ools <u>I</u> nternals <u>H</u> elp
E al a a Interfaces Ctrl+I a 🏟	
Filter: Options Ctrl+K	Expression Clear Apply Save
No. Time Stop Ctrl+E ination	Protocol Length Info
1 0.000000 Restart Ctrl+R .168.	1.2 ICMP 74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128
2 0.0003140 Kestan Cuirk adcas	st ARP 60 who has 192.168.1.1? Tell 192.168.1.2
3 0.0003300 M Capture Filters tronI	L_73:7c:8c ARP 42 192.168.1.1 1s at 20:6a:8a:72:a5:82
4 0.00051800 192.168.1.2 192.168.	1.1 ICMP /4 Echo (ping) reply id=0x0001, seq=5/1280, ttl=128
5 1.00165900 192.168.1.1 192.168.	1.2 ICMP /4 Echo (ping) request 1d=0x0001, seq=6/1536, tt=128
6 1.00213300 192.168.1.2 192.168.	1.1 ICMP /4 Echo (ping) reply id=0x0001, seq=6/1536, ttl=128
/ 2.015/1300 192.168.1.1 192.168.	1.2 ICMP /4 Echo (ping) request id=0x0001, seq=//1/92, ttl=128
8 2.0161/300 192.168.1.2 192.168.	1.1 ICMP /4 Echo (ping) reply id=0x0001, seq=//1/92, ttl=128
9 3.02992400 192.168.1.1 192.168.	1.2 ICMP /4 Echo (ping) request 1d=0x0001, seq=8/2048, tt=128
10 3.03038600 192.168.1.2 192.168.	1.1 ICMP /4 Echo (ping) reply 1d=0x0001, seq=8/2048, ttl=128
11 49.8158680 192.168.1.2 192.168.	1.1 ICMP /4 ECno (ping) request id=0x0001, seq=5/1280, tt1=128
12 49.8161180 WistronI_/2:a5:82 Broadcas	ST ARP 42 Who has 192.168.1.2? Tell 192.168.1.1
13 49.8164380 WistronI_/3:/c:8c WistronI	L_/2:a5:82 ARP 60 192.168.1.2 is at 20:6a:8a:/3:/C:8C
14 49.8164770192.168.1.1 192.168.	1.2 ICMP 74 Echo (ping) reply 1d=0x0001, seq=5/1280, ttl=128
15 50.8195000 192.168.1.2 192.168.	1.1 ICMP 74 Echo (ping) request id=0x0001, seq=6/1536, ttl=128
16 50.8196540 192.168.1.1 192.168.	1.2 ICMP 74 Echo (ping) reply id=0x0001, seq=6/1536, ttl=128
17 51 8330100 102 168 1 2 102 168	1 1 TCMD 74 Echo (nino) request id=0v0001 seg=7/1702 ttl=128
Frame 1: 74 bytes on wire (592 bits), 74 by	ytes captured (592 bits) on interface 0
	:8a:/2:a5:82), Dst: WistronI_/3:/c:8c (20:6a:8a:/3:/c:8c)
Internet Protocol Version 4, Src: 192.168.1	1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)
Internet Control Message Protocol	
0000 20 6a 8a 73 7c 8c 20 6a 8a 72 a5 82 08	3 00 45 00 j.s . j .rE.
0010 00 3c 00 e8 00 00 80 01 00 00 c0 a8 01	01 c0 a8 .<
0020 01 02 08 00 40 56 00 01 00 05 61 62 63	24 65 66MVADCGET
0040 77 61 62 63 64 65 66 67 68 69	wabcdefa hi
Broadcom Netlink (TM) Gigabit Ethernet Dri     Dacketer 201 Disc	snlaved: 301 Marked: 0
Broadconn Netenik (Twi) orgabit Ethemet Dit Packets: 351 Dis	Profile Default

Рисунок 5.4 Выбор сетевого интерфейса для перехвата трафика

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

Wireshark: Capture I	nterfaces				x
	Description	IP	Packets	Packets/s	
🔽 😥 Broadcom No	etLink (TM) Gigabit Etherne	t Driver 192.168.1.1	30	0	<u>)</u> etails
Help	Start	S <u>t</u> op	<u>Option</u>	s <u>C</u> le	ose

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*  $\rightarrow$  *ICMP* и нажмите *Apply* (рис. 5.6).

<b>I</b>	Broadco	m Net	Link (TN	/I) Giga	bit Eth	ernet D	Driver	: \Devi	ce\NPF	FDA	CB24C	C-D6AE	-4623-	A0B9-5	DFOEO	659758	{Wires	hark	1.8.1 (SV	N Rev	43946 fro	om /t	trunk-1.	8)]		×	
Eile	<u>E</u> dit	View	Go	Captu	re <u>A</u> r	alyze	Stat	istics	Teleph	iony	Tool	s <u>I</u> nte	ernals	<u>H</u> elp													
	<b>i</b>					8	8	0	(i)	¢	) T	₫ 🕹			€ 0			2	¥ 🖪	*	Ø						
(	Filter:	icm	р										•	Expressi	on	Clea	r	App	ply	Save							
No.	Т	lime		Sourc	e			De	stinatio	on			Proto	col Le	ngth	Info											*
	1 (	0.000	00000	)192.	168.	1.1			92.16	8.1.			ICM		74	Echo	(ping)		equest	id=	=0x0001		eq=5/	1280,	tt]=12	3	
	4 (	0.000	51800	) 192.	168.	1.2		1	92.16	8.1.	1		ICM	Р	74	Echo	(ping)	) r	eply	id=	0x0001	, s	eq=5/	1280,	tt]=12	3	
	5 1	1.001	65900	) 192.	168.	1.1		1	92.16	8.1.	2		ICM	Р	74	Echo	(ping)	) r	equest	id=	0x0001	, s	eq=6/	1536,	tt]=12	3	
	6 1	1.002	13300	) 192.	168.	1.2		1	92.16	8.1.	1		ICM	Р	74	Echo	(ping)	) r	eply	id=	0x0001	, s	eq=6/	1536,	tt]=12	3	
	7 2	2.015	71300	) 192.	168.	1.1		1	92.16	8.1.	2		ICM	Р	74	Echo	(ping)	) r	equest	id=	0x0001	, s	eq=7/	1792,	tt]=12	3	
	8 2	2.016	17300	) 192.	168.	1.2		1	92.16	8.1.	1		ICM	Р	74	Echo	(ping)	) r	eply	id=	0x0001	, s	eq=7/	1792,	tt]=12	3	Ξ
	9 3	3.029	92400	) 192.	168.	1.1		1	92.16	8.1.	2		ICM	Р	74	Echo	(ping)	) r	equest	id=	0x0001	, s	eq=8/	2048,	tt]=12	3	
	10 3	3.030	38600	) 192.	168.	1.2		1	92.16	8.1.	1		ICM	Р	74	Echo	(ping)	) r	eply	id=	0x0001	, s	eq=8/	2048,	tt]=12	3	
	11 4	49.81	58680	) 192.	168.	1.2		1	92.16	8.1.	1		ICM	Р	74	Echo	(ping)	) r	equest	id=	0x0001	, s	eq=5/	1280,	tt]=12	3	
	14 4	49.81	.64770	) 192.	168.	1.1		1	92.16	8.1.	2		ICM	Р	74	Echo	(ping)	) r	eply	id=	0x0001	, s	eq=5/	1280,	tt]=12	3	
	15	50.81	95000	) 192.	168.	1.2		1	92.16	8.1.	1		ICM	Р	74	Echo	(ping)	) r	equest	id=	0x0001	, s	eq=6/	1536,	tt]=12	3	-
	16	50.81	96540	) 192.	168.	1.1		1	92.16	8.1.	2		ICM	Р	74	Echo	(ping)	) r	eply	id=	0x0001	, s	eq=6/	1536,	tt]=12	3	
	17 !	51.83	39100	) 192.	168.	1.2		1	92.16	8.1.	1		ICM	Р	74	Echo	(ping)	) r	equest	id=	0x0001	, s	eq=7/	1792,	tt]=12	3	
	18	51.83	40640	) 192.	168.	1.1		1	92.16	8.1.	2		ICM	Р	74	Echo	(ping)	) r	eply	id=	0x0001	, s	eq=7/	1792,	tt]=12	3	
	19	52.84	75910	) 192.	168.	1.2		1	92.16	8.1.	1		ICM	Р	74	Echo	(ping)	) r	equest	id=	0x0001	, s	eq=8/	2048,	tt]=12	3	
	20	52.84	77500	) 192.	168.	1.1		1	92.16	8.1.	2		ICM	Р	74	Echo	(ping)	) r	eply	id=	0x0001	, s	eq=8/	2048,	tt]=12	3	
	65	576 7	25005	107	168	17		1	07 16	R 1	1		TCM	D	7/	Echo	(nina)	) r	trainna	id-	-0×0001	c	on_0/	2201	++1-17	2	-
÷F	Frame	e 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0																									
÷E	Etherr	hernet II, Src: WistronI_72:a5:82 (20:6a:8a:72:a5:82), Dst: WistronI_73:7c:8c (20:6a:8a:73:7c:8c)																									
• I	Interr	net P	rotoc	01 V	ersic	on 4,	Sno	:: 19	2.168	.1.1	. (19	92.16	8.1.	1), Ds	it: 1	.92.16	58.1.2	(1	92.168.	1.2)							
± 1	Interr	net C	ontro	1 Me	ssage	Prot	toco	51																			
000	0 20	) 6a	8a 73	7c 8	3c 20	6a	8a	72 a'	5 82	08 0	0 45	00	j.	s . j	.r.	E.		-				-					-
001	0 00	) 3c	00 e8	00 (	00 80	01	00	00 cf	) a8	01 0	1 c0	a8	.<.														
002	0 01	02	08 00	4d 5	56 00	01	00	05 61	62	63 64	4 65	66	abi	.MV	a	bcdef											Ε
003	0 77	61	62 63	64 6	55 66	67	68	69	12	13 /1	4 / 3	10	wał	cdefa	hi	rscuv											
																											-
	File: "C:	\Users	edu2\A	ppDat	a\Loca	\\Temp	N	Packe	ts: 683	Displa	yed: 2	4 Mark	ed: 0 D	ropped	0						Prof	file: [	Default				

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).

C C	apturi	ing fro	om Broa	dcom N	VetLir	nk (TN	M) Gi	gabit	Ether	net D	river:	\Dev	ice\N	PF_{FDA	CB24C-	D6AE
<u>F</u> ile	<u>E</u> dit	<u>V</u> ie	w <u>G</u> o	<u>C</u> apt	ure	<u>A</u> nal	yze	<u>S</u> tati	stics	Tele	phon	<u>y 1</u>	ools	Interna	ls <u>H</u> e	lp
		<b>e</b> (	R) (A			*	2		Q				T	₽ [[		]  6
F	ilter:														▼ Exp	ressio
No.		Time		Sour	ce				D	estina	tion			Pi	rotocol	Len
	12	6.20	574470	00 192	.16	8.1.	2		1	92.1	168.	1.1		I	CMP	
	13	6.61	L4771(	00 192	.16	8.1.	2		1	92.1	168.	1.2	55	N	BNS	
	14	7.28	810630	00 1 92	.16	8.1.	1		1	92.1	168.	1.2		I	CMP	
			Р	исуно	ж 5.	7 0	стан	ювк	а зах	вата	а тра	афи	ка			

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).

Broadcom NetLink (TM) Gigabit Ethernet Drive	r: \Device\NPF_{FDACB24C-D6AE-462	23-A0B9-5DF0E0659758}	[Wireshark 1.8.1 (SVN R	Rev 43946 from /trunk-1.8)]	
<u>File Edit View Go Capture Analyze Sta</u>	tistics Telephony <u>T</u> ools <u>I</u> nternal	s <u>H</u> elp			
	°, * * • • 7 ½		🖭   🖉 🕅 🍢		
Filter: icmp		Expression Clear	Apply Sa	ave	
No. Time Source	Destination Pro	otocol Length Info			
8 5.26483000 192.168.1.1	192.168.1.2 IC	MP 74 Echo	(ping) request i	d=0x0001, seq=9/2304,	tt]=128
9 5.26530200 192.168.1.2	192.168.1.1 IC	MP 74 Echo	(ping) reply i	d=0x0001, seq=9/2304,	tt]=128
11 6.26686300 192.168.1.1	192.168.1.2 IC	MP 74 Echo	(ping) request i	d=0x0001, seq=10/2560,	tt]=128
12 6.26744700 192.168.1.2	192.168.1.1 IC	MP 74 Echo	(ping) reply i	d=0x0001, seq=10/2560,	tt]=128
14 7.28106300 192.168.1.1	192.168.1.2 IC	MP 74 Echo	(ping) request i	d=0x0001, seq=11/2816,	ttl=128
15 7.28149800 192.168.1.2	192.168.1.1 IC	MP 74 Echo	(ping) reply i	d=0x0001, seq=11/2816,	ttl=128
20 8.29515400 192.168.1.1	192.168.1.2 IC	MP 74 Echo	(ping) request i	d=0x0001, seq=12/3072,	ttl=128
21 8.29572600 192.168.1.2	192.168.1.1 IC	MP 74 Echo	(ping) reply i	d=0x0001, seq=12/30/2,	tt1=128
Ename R: 74 butter on wine (502	hits) 74 but os contuned	(502 hits) on int	torface 0		
E Ethernet TT Src: Wistront 72:a	5:82 (20:63:83:72:35:82)	Dst: WistronT 7	3:7c:8c (20:6a:8a	.73.76.86)	
Destination: Wistront 73:7c:8	c (20:6a:8a:73:7c:8c)	Dot. whothom_/.	5.70.00 (20.00.00		
Address: WistronT 73:7c:8c	(20:6a:8a:73:7c:8c)				
	= LG bit: Globally uni	que address (fact	torv default)		
	= IG bit: Individual a	ddress (unicast)	,		
□ Source: WistronI_72:a5:82 (20)	:6a:8a:72:a5:82)				
Address: WistronI_72:a5:82	(20:6a:8a:72:a5:82)				
0	= LG bit: Globally uni	que address (fact	tory default)		
0	= IG bit: Individual a	ddress (unicast)	-		
Type: IP (0x0800)					
Internet Protocol Version 4, Sr	c: 192.168.1.1 (192.168.1	1), Dst: 192.168	8.1.2 (192.168.1.	2)	
🗄 Internet Control Message Protoc	0]				
0000 20 6a 8a 73 7c 8c 20 6a 8a	72 a5 82 08 00 45 00	j.s . j .rE.			~
	00 C0 a8 01 01 C0 a8	<.F abcdef			-
0030 67 68 69 6a 6b 6c 6d 6e 6f	70 71 72 73 74 75 76 a	hijklmn opgrstuv			=
0040 77 61 62 63 64 65 66 67 68	69 w	abcdefg hi			-
Ethernet (eth) 14 hytes	Packets: 360 Displayed: 8 Marked: 0	Dropped: 0		Profile: Default	
- conciner (con), in oyies	r dekees 500 bisplayed o Marked o	broppearo		rione berdar	

Рисунок 5.8 Детализация кадра Ethernet II

Чему равен МАС-адрес отправителя пакета?

Чему равен МАС-адрес получателя пакета?

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

Новый МАС-адрес ПК1 — 08-00-27-3F-B6-0В Новый МАС-адрес ПК2 — 09-00-27-3F-B6-0С

<u>Чтобы изменить MAC-адрес в Windows XP, выполните следующие действия:</u> 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);

бщие Дополнительно	Общие Дополнительно Драйвер Управление электропитанием
Подключение через:	NVIDIA nForce Networking Controller
Компоненты, используемые этим подключением:	Тип устройства: Сетевые платы
<ul> <li>✓ Клиент для сетей Microsoft</li> <li>✓ Служба доступа к файлам и принтерам сетей Microsoft</li> <li>✓ Планировщик пакетов QoS</li> <li>Э⊂ Microsoft TCP/IP версии 6</li> </ul>	Изготовитель: NVIDIA Размещение: Размещение 0 (NVNETBUS Id: 00070000-000) Состояние устройства
Установить Удалить Свойства Описание Позволяет данному компьютеру получать доступ к ресурсам в сети Microsoft.	Устройство работает нормально. При наличии неполадок в работе устройства нажмите кнопку "Диагностика", чтобы запустить мастер диагностики.
При подключении вывести значок в области уведомлений	Диагностика
Уведомлять при ограниченном или отсутствующем подключении	Применение устройства: Это устройство используется (включено)

Рисунок 5.9 Настройка сетевой карты

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

laнный адаптер имеет перечисленные ниже свойства. Слев ыберите изменяемое свойство, а справа выберите значени войства. войство: Поw Control EEE802.1P Support Low Power State Link Speed Network Address Dptimize For Speed/duplex settings /LAN Support Wake on Magic packet	а ие этог
Wake on pattern WakeOnLAN From PowerOff	

Рисунок 5.10

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

lанныі ыбери	й адаптер имеет г гге изменяемое сі	еречислені войство, а і	ные ниже свойства. Слева справа выберите значение этого
Eorieri Flow C IEEE8 Low Po Networ Optimiz Speed, VLAN I VLAN S VLAN S Wake Wake	sa. Bo: J2.1P Support J2.1P Support Swer State Link Spe k Address te For /duplex settings d Support on Magic packet on pattern DnLAN From Power	eed Off	Значение: • 0800273FB60B • Отсутствует

Рисунок 5.11 Настройка нового МАС-адреса

6. Нажмите кнопку Ок;

7. Перезагрузите ПК.

<u>Чтобы изменить MAC-адрес в Windows 7/Vista, выполните следующие действия:</u> 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);

СЭ С ♥ 🔮 « Сеть ) Сетевые под ) ▼ У Поиск: Со	етевые подключения 👂
Упорядочить 🔻 Отключение сетевого устройства 🛛 »	u= 0
Беспроводное сетевое соединение Отключено Отключено	по локальной сети

Рисунок 5.12

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

	Сведения	Управление эле	стропитанием
ючение через:	Общие	Дополнительно	Драйвер
Broadcom NetLink (TM) Gigabit Ethemet	Broadcom Ne	etLink (TM) Gigabit Ethernet	
Настроить	Тип устройс Изготовите	тва: Сетевые адаптеры	
Клиент для сетей Microsoft Планировщик пакетов QoS	Размещени	е: PCI гнездо 4 (PCI-шина функция 0)	1, устройство 0,
Служба доступа к файлам и принтерам сетей Micro	Состояние устройс	тва	
<ul> <li>Протокол Интернета версии 4 (TCP/IPv4)</li> <li>Драйвер в/в тополога канального уровня</li> <li>Ответчик обнаружения топологии канального уровня</li> </ul>	Устройство работ	ает нормально.	
новить Удалить Свойства			-
ние оляет данному компьютеру получать доступ к исам в сети Microsoft.			

Рисунок 5.13

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

Сведения	Управление электропитанием		
Общие	Дополнитель	но	Драйвер
Цанный адаптер имее выберите изменяемое войства.	т перечисленные н свойство, а справ	иже с а выб	звойства. Слева берите значение этого
войство:		3	Значение:
802.3a2 EEE ARP Offload EEE Control Policies Ethemet@WireSpeed Flow Control Interrupt Moderation IPv4 Checksum Offload Jumbo Mtu Large Send Offload (IP Large Send Offload v2 Large Send Offload v2 NS Offload Priority & VLAN	(IPv4) (IPv6)	•	)тсутствует
			ОК Отмена

Рисунок 5.14

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

Сведения	Управ.	Управление электропитанием	
Общие нный адаптер име берите изменяемо ойства.	Дополнителы ет перечисленные н е свойство, а справ	но иже сво а выбер	Драйвер йства. Слева ите значение этого
ойство:		Зна	чение:
)2.3az EEE RP Offload	•	، 20	6A8A737C8C
vow Control terrupt Moderation v4 Checksum Offloa umbo Mtu arge Send Offload (If arge Send Offload v2 arge Send Offload v2 etwork Address S Offload	id 2v4) 2 (IPv4) 2 (IPv6) ▼		

Рисунок 5.15

6. Нажмите кнопку Ок;

7. Перезагрузите ПК.

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

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

### Шаг 16. Повторите шаг 7 — шаг 12.

Чему теперь равен МАС-адрес отправителя пакета? \_\_\_\_\_ Чему теперь равен МАС-адрес получателя пакета? \_\_\_\_\_

Шаг 17. Верните первоначальный МАС-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 широковещательный, на канальном уровне полностью изолирован он 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 МАС-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)	:
I V	~ · · · · · · · · · · · · · · · · · · ·	1 /	_

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



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.

<u>Чтобы зайти на Web-интерфейс коммутатора, выполните следующие действия:</u>

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).

Firefox 🔻 D Login	+	
€ € 10.90.90.90		



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.

<u>Для Mozilla Firefox:</u> меню Инструменты  $\rightarrow$  Настройки  $\rightarrow$  Дополнительные. Далее вкладка Сеть  $\rightarrow$  Настройка параметров соединения Firefox с Интернетом  $\rightarrow$  Настроить  $\rightarrow$  Без прокси.

<u>Для Internet Explorer</u>: меню Сервис  $\rightarrow$  Свойство обозревателя. Далее вкладка Подключения  $\rightarrow$  Настройка сети  $\rightarrow$  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  $\rightarrow$  MAC Address Table  $\rightarrow$  Dynamic Forwarding Table (рис. 6.4).

D-Link Building Networks for People					🍳 admin - 10.90.90.91
💾 Save 🚽 🐔 Tools 🗸					🙋 Logou
DES-1100-16 B- System	Dynamic Fo	rwarding Tab	le Settings		
CL2 Features	Port All	•		Se	Find Ect All Clean all
Static MAC	ID 1	Port 4	MAC Address 20-6A-8A-72-A5-82 20-6A-8A-73-7C-8C	Type Dynamic Dynamic	Add
	2		20-04-04-13-10-00	Dynamic	
			Page 01	Pre Page Ne	xt Page Apply

Рисунок 6.4 Таблица коммутации. Динамически изученные МАС-адреса

Сколько записей наблюдаете?

Какой тип (Туре) у каждой записи в таблице коммутации?



Шаг 7. Посмотрите содержимое таблицы коммутации. Что изменилось?

Шаг 8. Создайте статическую запись в таблице коммутации для ПК2 на порте 5. Для этого выберите Security  $\rightarrow MAC \ Address \ Table \rightarrow Static \ MAC$  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 MACадрес ПК2 и нажмите кнопку *Apply* (рис. 6.6).

D-Link	
Building Networks for People	admin - 10.90.90.91
💾 Save 🚽 🌋 Tools 🗸	🔀 Logout
■ DES-1100-16 ■ System ■ L2 Features ■ VLAN	Static MAC Settings
Dos	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
E- MAC Address Table	
Static MAC	Static MAC Address Lists ( Maximum Entries 128 )
	ID Port MAC Address
	Add MAC Port 5  MAC Address 20-6a-8a-72-a5-82 Cancel Apply

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  $\rightarrow MAC \ Address \ Table \rightarrow Static \ MAC$ . В правой части окна нажмите кнопку Delete напротив записи для ПК2 (рис. 6.7).

ding Networks for People		🥊 admin - 10.90.90.91
Save 👻 🌠 Tools 🗸		💆 Logo
DES-1100-16	Static MAC Settings	
L2 Features VLAN	Disable Auto Learning Excluding Uplink Port O On Off	
QoS Security ⊡- ∭MAC Address Table	01 02 03 04 05 06 07 08 09 10 11 12 Uplink Port V V V V V V V V V V V	13 14 15 16 V V V
Static MAC Dynamic Forwarding Table	Static MAC Address Lists ( Maximum Entries :128 )	Apply Delete all
	ID Port MAC Address	
	1 5 20-6A-8A-72-A5-82	te
		Add MAC

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*  $\rightarrow$  *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.



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  $VLAN \rightarrow Port$ -Based VLAN (рис. 6.10).

D-Link Building Networks for People		🍳 admin - 10.90.90.91
💾 Save 🗸 🌠 Tools 🗸		2 Logout
DES-1100-16	Port-Based VLAN Settings	
ELZ FEATURES	Port-Based VLAN	Apply
<ul> <li></li></ul>	(Maximum Entries :32)	Add VLAN
	VLAN Index         VLAN Name         VLAN member port           1         01,02,03,04,05,06,07,08, 09,10,11,12,13,14,15,16	VLAN Rename Delete VLAN Rename Delete VLAN

Рисунок 6.10

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

D-Link Building Networks for People		🍳 admin - 10.90.90.91
💾 Save 🚽 🐒 Tools 🗸		💋 Logout
DES-1100-16 E System L2 Features VLAN 802.10 VLAN Port-Based VLAN CoS Security	Port-Based VLAN Settings Port-Based VLAN  © Enabled  © Disabled (Maximum Entries :32)	Apply Add VLAN
	VLAN Index         VLAN Name         VLAN mem           1         01,02,03,0         09,10,11,13	nber port VLAN Rename Delete VLAN 4,05,06,07,08, 2,13,14,15,16 Rename Delete VLAN

Рисунок 6.11

<u>Примечание:</u> 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).

D-Link Building Networks for People		🤶 admin - 10.90.90,91
💾 Save 🗸 🌋 Tools 🗸		🙋 Logout
DES-1100-16	Port-Based VLAN Settings	
L2 Features     VLAN     So2.10 VLAN     Boot Record // AN	Port-Based VLAN	Apply
entebased victoria entername and the second	( Maximum Entries :32 )	Add VLAN
	VLAN Index         VLAN Name         VLAN member port           1         01,02,03,04,05,06,07,08,	VLAN Rename Delete VLAN
	09,10,11,12,13,14,15,16	
4444 4444 4444 4444 4444		

Рисунок 6.12

Port-Base	ed VL	AN															
VLAN Name :																	
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	
Member	1	<b>V</b>															
												Pre	vious (	Page	Ap	ply	]

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).

Port-Based VLAN Setting	S	
Port-Based VLAN	O Disabled	Apply
(Maximum Entries :32)		Add VLAN
VLAN Index VLAN Name <u>1</u>	VLAN member port 01,02,03,04,05,06,07,08	VLAN Rename Delete VLAN Rename Delete VLAN

Рисунок 6.14

Port-Based	VLA	N S	Settir	ngs												
Port-Based VL/ (Maximum Ent	AN ries :32	● Er 2 )	nabled	O	Disabl	ed									Ap	ply
VLAN Name :	v2					(Nam	ne shou	uld be l	ess th:	an 10 d	charact	ers)				
Member	01	02	03	04	05	06	07	08	09 V	10 <b>√</b>	11 <b>√</b>	12	13 Cance	14 V	15 ▼ 	16 V pply
																_
VLAN Index <u>1</u>	VLAI	N Nar	ne		VLAN 01,02	memt ,03,04,	ber port ,05,06,	t 07,08			VLA R	N Ren ename	ame	Delete	e VLAN te VLA	N

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-Hoc;
- Режим инфраструктуры.

*Режим Аd-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-Hoc 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



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-Hoc 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).

🎭 Службы						
Консоль Действие	Вид Справка					
← → 💽 🚰 🖸	) 🗟 😫 🖬 🕨 💷 🗉 🖦					
🍓 Службы (локальнь	🆏 Службы (локальные)					
	Беспроводная настройка	Имя 🖉	Описание	Состояние	Тип запуска	Вход от имени
	Запустить службу Описание: Предоставляет автоматическую настройку 802.11 адаптеров	QoS RSVP Remote Packet Capture Prot Skype Updater Telnet Windows Audio Windows Installer WLSVC Автоматическое обновление Автоматическое обновление	Обеспечи Allows to Enables th Позволяе Управлен Позволяе Загрузка Данная с	Работает Работает	Вручную Вручную Авто Вручную Авто Вручную Авто Авто Вручную	Локальная сис Локальная сис Локальная сис Локальная сис Локальная сис Локальная сис Локальная сис Локальная сис
×	Расшиленный / Станлалтный /	Агент защиты доступа к с Адаптер производительно Беспроводная настройка Брандмауэр Windows/Общ Веб-клиент Вторичный вход в систему	Позволяе Предоста Предоста Обеспечи Позволяе С	Работает Работает Работает	Вручную Вручную Авто Авто Авто Авто С	Локальная сис Локальная сис Локальная сис Локальная сис Локальная сис

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 ІР-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.

ощие Беспроводные сети Дополнительно	Оощие	
Подключение через: High-Power Wireless 150 USB adapt Настроить	Параметры IP могут назначаться а поддерживает эту возможность. В IP можно получить у сетевого адми	втоматически, если сеть противном случае параметры інистратора.
Компоненты, используемые этим подключением:	Получить IP-адрес автоматиче	ски
Vireless Lan NDIS Protocol I/O Control	Использовать следующий IP-а	идрес:
<ul> <li>✓ З<sup>™</sup> Місгозоft ТСР/ІР версии 6</li> <li>✓ З<sup>™</sup> Протокол Интернета (ТСР/ІР)</li> </ul>	ІР-адрес:	192.168.1.1
M	Маска подсети:	255 . 255 . 255 . 0
Истановить Ирадить Свойства	Основной шлюз:	R 6 6
Описание	🔘 Получить адрес DNS-сервера	автоматически
Протокол ТСР/ІР - стандартный протокол глобальных	🕟 Использовать следующие адр	еса DNS-серверов:
сетей, обеспечивающий связь между различными взаимодействующими сетями.	Предпочитаемый DNS-сервер:	
При подключении вывести значок в области уведомлений	Альтернативный DNS-сервер:	
Уведомлять при ограниченном или отсутствующем подключении		Дополнительно

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).

ощие	Беспроводн	ые сети	Допс	лнительн	-10		
🗸 Исг	юльзовать W	′indows д.	ля нас	тройки с	ети		
Дост	упные сети:	_					-
Чтоб	ы получить д в радинсе де	ополните йствия в	льные	сведени исле как	я о бе полк	еспровод лючиться	ной
откл	ючиться, щел	кните кн	опкун	иже.	пода	no wiebcy	
			1	Беспро	водны	ые сети	
cere	й из следуюш	(его спис	ка:		1	Reany	-
cere	й из следуюш	его спис	Ka:			Вверх Вниз	
До	й из следуюш бавить)	удалить	ка:	Свойств		Вверх Вниз	
До Подр	й из следуюш бавить) обнее <u>о настр</u>	удалити Удалити ройке бе	ка:	Свойств	] [] а	Вверх Вниз юлнитель	ьно

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);

Щие состроводные соги Дополнительно	Связи Проверка подлинност	и подключение	
🛾 Использовать Windows для настройки сети	Сетевое имя (SSID):		
Доступные сети: Чтобы получить дополнительные сведения о беспроводно сети в радиусе действия, в том числе как подключиться и отключиться, щелкните кнопку ниже.	Подключиться, даже ес Ключ беспроводной сети Данной сети требуется кли	ли сеть не ведет веш оч для следчющих опе	(ание ераций:
Беспроводные сети	Проверка подлинности:	Открытая	~
Предпочитаемые сети: Автоматически подключаться к первой из доступных сетей из следчюшего списка:	Шифрование данных:	WEP	~
Вверх	Ключ сети:		
Вниз	Подтверждение ключа:		
	Индекс ключа (расширенны	ай): [1	4.2
	Ключ предоставлен авто	оматически	
Подробнее о настроике респроводной сети. Дополнительно	Это прямое соединение к доступа не используются	омпьютер-компьютер	); точки

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.

Связи	Проверка подлинно	ости	Подключение	
Сетев	ое имя (SSID):	clas	sroom234	
□ I Клю Дан	Подключиться, даже ч беспроводной сети ной сети требчется	если ч ключ	сеть не ведет вещан для следчющих опера	ие
Про	верка подлинности:		Открытая	
Ши	фрование данных:		WEP	
Клю	ч сети:	•••	••	
Под	тверждение ключа:	•••	••	
Инд	екс ключа (расшире (люч предоставлен а	нный) автом	: 1	
Г до	о прямое соединени ступа не используют	е ком ся	пьютер-компьютер; т	рчки

Рисунок 7.12 Создание беспроводной сети с именем classroom243

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

<u>Чтобы посмотреть доступные беспроводные сети, выполните следующие действия:</u> 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).

Беспроводное сетевое	а подключение 🛛 🔯
Для подключения к сети " ключом WEP или WPA). Се несанкционированное под Введите ключ и нажмите и	classroom234" требуется ключ сети (также называется тевые ключи помогают предотвратить ключение к сети. кнопку "Подключить".
Ключ сети:	•••••
Подтверждение ключа:	•••••
	Подключить Отмена

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).

Использовать Windows для настройки	сети
Доступные сети:	
Чтобы получить дополнительные сведен сети в радиусе действия, в том числе ка отключиться, щелкните кнопку ниже.	ия о беспроводной к подключиться и
Беспр	оводные сети
Автоматически подключаться к первой и сетей из следующего списка:	на доступных
🔏 classroom234 (автоматически)	Вверх
	Вниз
Добавить Удалить Свойс	гва

Рисунок 7.17 Удаление беспроводной сети classroom234

### 7.1.2 Создание беспроводной сети в режиме Ad-Hoc для рабочих станций с OC 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);

Подк	лючение через:
2	Atheros AR5B97 Wireless Network Adapter
00	Настроить
Отме	ченные компоненты используются этим подключением:
•	🖳 Клиент для сетей Microsoft
	📮 Планировщик пакетов QoS
	📕 Служба доступа к файлам и принтерам сетей Micro
	Протокол Интернета версии 6 (TCP/IPv6)
<b>&gt;</b>	<ul> <li>Протокол Интернета версии 6 (TCP/IPv6)</li> <li>Протокол Интернета версии 4 (TCP/IPv4)</li> </ul>
Y Y Y	Протокол Интернета версии 6 (TCP/IPv6)     Протокол Интернета версии 4 (TCP/IPv4)     Драйвер в/в тополога канального уровня
Y Y Y	<ul> <li>Протокол Интернета версии 6 (TCP/IPv6)</li> <li>Протокол Интернета версии 4 (TCP/IPv4)</li> <li>Драйвер в/в тополога канального уровня</li> <li>Ответчик обнаружения топологии канального уровня</li> </ul>
<b>&gt; &gt; &gt;</b>	<ul> <li>Протокол Интернета версии 6 (TCP/IPv6)</li> <li>Протокол Интернета версии 4 (TCP/IPv4)</li> <li>Драйвер в/в тополога канального уровня</li> <li>Ответчик обнаружения топологии канального уровня</li> </ul>
2 2 2	<ul> <li>Протокол Интернета версии 6 (TCP/IPv6)</li> <li>Протокол Интернета версии 4 (TCP/IPv4)</li> <li>Драйвер в/в тополога канального уровня</li> <li>Ответчик обнаружения топологии канального уровня</li> </ul>
y y	<ul> <li>Протокол Интернета версии 6 (ТСР/ІРv6)</li> <li>Протокол Интернета версии 4 (ТСР/ІРv4)</li> <li>Драйвер в/в тополога канального уровня</li> <li>Ответчик обнаружения топологии канального уровня</li> <li>становить</li> </ul>
	<ul> <li>Протокол Интернета версии 6 (ТСР/ІРv6)</li> <li>Протокол Интернета версии 4 (ТСР/ІРv4)</li> <li>Драйвер в/в тополога канального уровня</li> <li>Ответчик обнаружения топологии канального уровня</li> <li>становить</li> <li>Удалить</li> <li>Свойства</li> </ul>
	<ul> <li>Протокол Интернета версии 6 (ТСР/ІРv6)</li> <li>Протокол Интернета версии 4 (ТСР/ІРv4)</li> <li>Драйвер в/в тополога канального уровня</li> <li>Ответчик обнаружения топологии канального уровня</li> <li>становить</li> <li>Удалить</li> <li>Свойства</li> <li>исание</li> <li>ютокол ТСР/ІР - стандартный протокол глобальных</li> </ul>
	<ul> <li>Протокол Интернета версии 6 (ТСР/ІРv6)</li> <li>Протокол Интернета версии 4 (ТСР/ІРv4)</li> <li>Драйвер в/в тополога канального уровня</li> <li>Ответчик обнаружения топологии канального уровня</li> <li>становить</li> <li>Удалить</li> <li>Свойства</li> <li>исание</li> <li>ютокол ТСР/ІР - стандартный протокол глобальных тей, обеспечивающий связь между различными</li> </ul>
	<ul> <li>Протокол Интернета версии 6 (ТСР/ІРv6)</li> <li>Протокол Интернета версии 4 (ТСР/ІРv4)</li> <li>Драйвер в/в тополога канального уровня</li> <li>Ответчик обнаружения топологии канального уровня</li> <li>Становить</li> <li>Удалить</li> <li>Свойства</li> <li>исание</li> <li>ютокол ТСР/ІР - стандартный протокол глобальных тей, обеспечивающий связь между различными аимодействующими сетями.</li> </ul>

Рисунок 7.19

- 4. Выберите Использовать следующий ІР-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.

араметры IP могут назначаться а ддерживает эту возможность. В можно получить у сетевого адми	втоматически, если сеть противном случае параметры нистратора.
Получить IP-адрес автоматиче Использовать сперионний IP-а	ески
• использовать следующий год IP-адрес:	192.168.1.1
Маска подсети:	255.255.255.0
Основной шлюз:	
<ul> <li>Получить адрес DNS-сервера</li> <li>Использовать следующие адр</li> <li>Предпочитаемый DNS-сервер:</li> </ul>	автоматически veca DNS-серверов:
Альтернативный DNS-сервер:	
🔲 Подтвердить параметры при	выходе Дополнительно

Рисунок 7.20
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

€ • Все элемен •	центр управления сетями и оощим доступом • • • • Плоиск в панели управления
Панель управления - домашняя страница	Просмотр основных сведений о сети и настройка подключений
Управление беспроводными сетями	Гросмотр полной карти EDU1-NOTE Интернет
Изменение параметров адаптера Изменить дополнительные параметры общего доступа	(этот компьютер) Просмотр активных сетей ———————————————————————————————————
См. также	Изменение сетевых параметров Настройка нового подключения или сети Настройка беспроводного, широкополосного, модемного, прямого или VPN-подключения или же настройка маршрутизатора или точки доступа.
Брандмауэр Windows Домашняя группа Свойства обозревателя	Подключиться к сети Подключение или повторное подключение к беспроводному, проводному, модемному срединению или подключение к VPN

Рисунок 7.21 Окно Центр управления сетями и общим доступом

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



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

<u>аш</u> Подк	лючение к беспроводной сети вручную	
Как до	бавить сеть?	
2	Создать профиль сети вручную При этом создается новый профиль сети или обнаруживается существующа сеть, и профиль сети сохраняется на компьютере. Необходимо знать имя сет (SSID) и ключ безопасности (если он есть).	я И
4	Создать сеть "компьютер-компьютер" При этом создается временная сеть для общего доступа к файлам или для подключения к Интернету	
		Отмена

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;

цайте имя этой сет	и и высерите парамет	DBI DESONACHOCTU
Лмя сети:	classroom234	
Гип безопасности:	WPA2-Personal	<ul> <li>Помочь выбрать</li> </ul>
(люч безопасности:	DlinkPassword	🔲 Скрыть символы
📝 Сохранить парам	іетры этой сети	

Рисунок 7.25 Создание беспроводной сети classroom234

10. Нажмите кнопку Закрыть (рис. 7.26).

$\bigcirc$	и Подключение к беспроводной сети вручную	
	Сеть classroom234 готова к использованию	
	Эта сеть будет отображаться в списке беспроводных сетей и останется активной, пока все пользователи не выполнят отключение. Сообщите имя сети и ключ безопасности (если он задан) тем пользователям, которым вы хотите разрешить подключаться к этой сети.	
	Имя беспроводной сети: classroom234 Ключ безопасности сети: ••••••	
	Чтобы разрешить общий доступ к файлам, откройте <u>Центр управления сетями и общим доступом</u> в панели управления и включите общий доступ к файлам.	
		Закрыть

Рисунок 7.26

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

<u>Чтобы посмотреть доступные беспроводные сети, выполните следующие действия:</u> 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 **4** (рис. 7.28).

47	-
	=
^	
lite.	
A	
ение	
30	
30	
31	
lie.	
	-
	тр 

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).

🕎 Подключение к се	ти
Введите ключ б	езопасности сети
Ключ безопасности:	DlinkPassword Скрыть символы
	ОК Отмена

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).

Текущие подключен Classroom234 Без доступа к	ния: ++++++++++++++++++++++++++++++++++++
Беспроводное сетево	ре соединение
classroom234	Подключено 🙏
	Отключение
dev_N	llee
RRuven	liter
187789	llee
FreeHotSpot	Sall
dlink	<b>Sal</b>
ATS	
Центр управления	сетями и общим доступом

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).

😋 🔵 🗢 📶 « Сеть и Ин	тернет 🕨 Управление беспроводными сетя	ми 🔫 🐓 Поиск:	Управление беспроводными 🔎		
Управление беспроводными сетями, использующими (Беспроводное сетевое соединение) Windows пытается подключаться к этим сетям в порядке их перечисления в списке ниже.					
Добавить Удалить Пе	реместить вниз Свойства адаптера Тип	ы профилей — Центр управления сетями и о	бщим доступом 🛛 🔞		
Сети, доступные для просм	отра, изменения и переупорядочивания (5)				
classroom234	Безопасно WEP	Тип: Поддерживается люб	Подключение вручну		
DIR620WIfi	Безопасно WPA2-Personal	Тип: Поддерживается люб	Автоматическое подк		

Рисунок 7.31 Удаление беспроводной сети classroom234

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

**Внимание:** для OC 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).

D-Link Connection N	1anager		×
Подключен	UMя сети: dlink IP адрес 192.168.0.198	Сигн 3 Кан	нал: <b>.)))</b> нал: 11
D-Link			
DWA-160	беспроводная сеть	Мои беспроводные сети	Поддержка>>
SSID	MAC(BSSID)	Сиг 🗸 Безопа	Канал
<b>1</b> 522	00:22:B0:09:B7:AF	90%	40
	00:15:E9:A7:D3:3E	72%	3
<b>u</b> dlink	00:18:E7:FA:83:6D	52%	11
- dlink	14:D6:4D:E3:05:08	48%	4
dink615	00:18:E7:F4:72:E6	44%	11
<b></b> spb095	00:11:95:F8:AD:40	42%	1
	00:15:E9:85:3A:44	26%	3
dink dink	14:D6:4D:82:69:84	10%	1
dlink	F0:7D:68:95:4D:38	6%	8
Мои беспроводные си dlink - dlink	ети	WPS Обновить	Подключить Активизировать

Рисунок 7.32 Интерфейс утилиты D-Link Connection Manager

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

D-Link Connection	Manager Имя сети: dlink IP адрес 192.168.	Си D.198 К	гнал: ,)) анал: 11
D-Link	беспроводная сеть	Мои беспроводные сети	Поддержка>>
Мои беспроводные с dlink - dlink	сети		Новый Изменить Удалить Активизировать
Детали профиля —			
Имя сети:	dlink		
Тип сети:	Инфраструктура		
Безопасность	Hat		

Рисунок 7.33

Шаг 3. Создайте новую беспроводную сеть в режиме Ad-Hoc. 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.

<u>Примечание:</u> чтобы в поле Ключ отображался пароль, установить галочку Отобразить текст в поле пароля.

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

D-Link Connection Manager		Σ
Разъелинен IP	ия сети: адрес	Сигнал: Канал:
астройки профиля		x
– Базовые настройки Имя профиля: SSID:	класс classroom243	
– Установить параметр безопасно С Нет • Протокол WEP С Парольная фраза WPA2	сти — Безопасность — Ключ: DlinkPassword	
	🔽 Отобразить те	жст в поле пароля
		ОК Отмена

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.

<u>Чтобы зайти на Web-интерфейс точки доступа, выполните следующие действия:</u>

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.

<u>Для Mozilla Firefox:</u> меню Инструменты  $\rightarrow$  Настройки  $\rightarrow$  Дополнительные. Далее вкладка Сеть  $\rightarrow$  Настройка параметров соединения Firefox с Интернетом  $\rightarrow$  Настроить  $\rightarrow$  Без прокси.

<u>Для Internet Explorer</u>: меню Сервис  $\rightarrow$  Свойство обозревателя. Далее вкладка Подключения  $\rightarrow$  Настройка сети  $\rightarrow$  Автоматическое определение параметров.

D-I	link		DAP-2310
	LOGIN		
	Login to the Access Point:	User Name admin Password Login	

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*  $\rightarrow$  *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.

LAN Settings		
Get IP From	Static IP (Manual) 🛛 🗸	
IP Address	192.168.0.51	
Subnet Mask	255.255.255.0	
Default Gateway		
		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*  $\rightarrow$  *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.

D-Link			DAP-2310
🔹 Home 🛛 🐒 Maintena	ance 🔻 📙 Configura	ition 👻 👙 System	💋 Logout 🛛 🕅 Help
Home     Maintena       DAP-2310     Basic Settings       ■ Advanced Settings     Status	Ance  Configura Wireless Settings Wireless Band Mode Network Name (SSID) SSID Visibility Auto Channel Selection Channel Channel Width Authentication PassPhrase Settings WPA Mode Cipher Type  Manual Activated From Time Interval PassPhrase Confirm PassPhrase	s   2.4GHz   Access Point   Class_test   Enable   Disable   6   20 MHz   6   20 MHz   WPA-Personal   AUTO (WPA or WPA2)   Auto   Group Key Update In   Periodical Key Change   Sun   1   (1~168)hour(s)	Logout (PHelp terval 1800 (Seconds)

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 OC Windows XP:

1. Откройте Сетевые подключения;

Пуск  $\rightarrow$  Панель управления  $\rightarrow$  Сетевые подключения  $\rightarrow$  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 ІР-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 ІР-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*  $\rightarrow$  *Client Information* (рис. 7.42).

Client Info	rmation				_
Client Informat	ion Station ass	ociation (2	2.4GHz): 2		
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode
Primary SSID	7C:E9:D3:28:10:E	32 N	WPA2-PSK	94%	On
Primary SSID	00:24:03:F9:B4:0	F 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 МАС-адрес ПК2

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

Запишите МАС-адрес ПК3\_\_\_\_\_

## Лабораторная работа №8. ІР-адресация

Для того чтобы устройство могло участвовать в сетевом взаимодействии с помощью протокола IP, ему должен быть присвоен уникальный IP-адрес (логический адрес), который позволяет однозначно идентифицировать интерфейс между устройством и сетью. Это требуется для обеспечения гарантии передачи пакета конкретному получателю. Отметим, что IP-адрес присваивается не конкретному устройству, а его интерфейсу. Любое устройство, которое передает данные, используя сетевой уровень, будет иметь как минимум один уникальный IP-адрес для сетевого интерфейса.

Адрес IPv4 представляет собой 32-разрядную (4 байта) двоичное поле. Для удобства восприятия и запоминания этот адрес разделяют на 4 части по 8 бит (октеты), каждый октет переводят в десятичное число и при записи октеты разделяют точками.

IPv4-адрес структурирован и состоит из двух логических частей: идентификатора сети (Net ID) – сетевая часть адреса и идентификатора узла (Host ID), который однозначно определяет устройство в сетевом сегменте. Такая структура IP-адреса представляет собой двухуровневую иерархическую модель и позволяет устройству при передаче данных в составную сеть указывать не только удаленную сеть, но и узел в этой сети.

Идентификатор сети определяет конкретную сеть или сегмент сети, в которой находится узел и используется для передачи данных на нужный сетевой интерфейс маршрутизатора или коммутатора 3-го уровня. После того как данные достигают нужной сети, они передаются уникальному узлу в соответствии с идентификатором узла. Все узлы, использующие один и тот же идентификатор сети, должны быть расположены в одной сети или подсети (логическом сегменте сети).



Рисунок 8.1 Структура IPv4-адреса

Адреса IPv4 делятся на 5 классов. К классам А, В, С относятся адреса, присваиваемые узлам. Класс D определяет адреса многоадресной рассылки. Класс E зарезервирован.

В адресах класса А под идентификатор сети отводится первый октет, остальные 3 байта используются для идентификатора узла, причем старший (левый) бит идентификатора сети всегда равен 0 (рис. 8.2).



Рисунок 8.2 Формат IPv4-адреса класса А

Сети класса В определяются значениями 10 в двух старших битах адреса. Первые 2 байта в адресе используются для идентификатора сети, а оставшиеся 2 байта – для идентификатора узла (рис. 8.3).

0	71	15 2	23 31
10 Сењ	Сеть	Узел	Узел

Рисунок 8.3 Формат IPv4-адреса класса В

В адресах класса С под идентификатор сети отводится первые три октета, в то время как под идентификатор узла только один последний октет (рис. 8.4). Три старших бита первого октета всегда равны 110, что позволяет определить, что адрес относится именно к

классу С.				
0	7	15	2	3 31
110 Cen	, c	еть	Сеть	Узел

#### Рисунок 8.4 Формат ІРv4-адреса класса С

Кроме IP-адреса сетевому узлу назначается маска подсети. *Маска подсети* – это 32битное число, двоичная запись которого содержит единицы в тех разрядах, которые должны определяться как идентификатор сети. Поскольку идентификатор сети является цельной 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).

100лици 0.1	тиолици 0.1 тиски поосети оля станоиртной клиссов сетси						
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					

Таблица 8.1 Маски подсети для стандартных классов сетей

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 получат и обработают 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 технологию 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 255.255.248 29 единичных бит.

<u>Цель:</u>

- 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)	
<i>IP-адрес первого узла подсети</i> (десятичное представление)	
<i>IP-адрес последнего узла подсети</i> (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.

<u>Примечание:</u> 1&1 = 1; 1&0 = 0; 0&0 = 0.

Рисунок 8.6 Определение адреса сети						
Адрес сети	00001010	11000001	01000000	00000000	10.193.64.0	
Маска подсети	11111111	11111111	11111000	00000000	255.255.248.0	
IP-адрес узла	00001010	11000001	01000100	00111011	10.193.68.59	

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 IPадрес всегда на единицу больше адреса сети (рис. 8.8).

	0.0.0		ID		
Первый IP-адрес подсети	00001010	11000001	01000 <mark>00</mark> 0	00000001	10.193.64.1
Маска подсети	11111111	11111111	11111000	00000000	255.255.248.0
Адрес сети	00001010	11000001	01000000	00000000	10.193.64.0

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 ІР-адреса подсети

Шаг 6. Определите количество узлов в подсети и запишите результат в таблицу. Количество узлов в подсети вычисляется по формуле 2<sup>n</sup>-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).

				11 бит	
Адрес сети	00001010	11000001	01000000	00000000	10.193.64.0
Маска подсети	11111111	11111111	11111000	00000000	255.255.248.0
	$2^{11} =$	2048			
Количество узл	ов 2048-	2 = 2046			

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

# ЗАДАНИЕ З

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



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:

0 /

Таолица 8.0		
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.

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 ІРv6

#### 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 895а473947. 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<sup>128</sup> 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 <u>https://www.ultratools.com/tools/rangeGenerator;</u>
- *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 отсутствии 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 станция1 шт.Кабель Ethernet1 шт.Точка доступа DAP-23101 шт.

## 9.1 Установка и настройка протокола IPv6 на рабочей станции

Шаг 1. Установите протокол IPv6 на рабочей станции.

<u>Чтобы установить протокол IPv6 на рабочей станции с OC Windows XP, выполните следующие действия (рис. 9.1):</u>

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.

одключение че	pes:		
👺 NVIDIA nF	orce Networking Control	ller Настро	ить
омпоненты, ис	пользуемые этим под	ключением:	
🗹 📙 Планир	овщик пакетов QoS		-
🗹 🔭 Wireless	Lan NDIS Protocol I/O	Control	0
⊻ 🐨 Microsof ∡ == ⊓	t TCP/IP версии 6		
⊻ 37—Протока С	л Интернета II СР/IPI		S
Установить	9далить	Свойст	ва
Описание			
ТСР/ІР верси	и 6. Версия нового пон	оления чего веримолейс	TEUS
разных сетей	токола, обеспечивающ	тего взаимодеис	TENC
] При подключ	ении вывести значок в	з области уведом	илений
9ведомлять	при ограниченном или	отсутствующем	

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

<u>Чтобы установить протокол IPv6 на рабочей станции с OC Windows 7/Vista, выполните следующие действия:</u>

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);

Сеть	
Поди	ключение через:
2	Broadcom NetLink (TM) Gigabit Ethemet
0	Настроить
	Служба доступа к файлам и принтерам сетей Місго Протокол Интернета версии 6 (TCP/IPv6)
2	<ul> <li>Протокол Интернета версии 4 (TCP/IPv4)</li> <li>Драйвер в/в тополога канального уровня</li> <li>Ответчик обнаружения топологии канального уровня</li> </ul>
	<ul> <li>Протокол Интернета версии 4 (TCP/IPv4)</li> <li>Драйвер в/в тополога канального уровня</li> <li>Ответчик обнаружения топологии канального уровня</li> </ul> Становить Удалить Свойства исание озволяет данному компьютеру получать доступ касурсам в сети Microsoft.

Рисунок 9.2

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

	устанавливаемого	о сетевого комп	юнента:
Клиент			
	<u>ں</u>		
Описание			
Протоколом передают и	і называется язы нформацию друг д	к, на котором к ругу.	омпьютерь

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.

<u>Чтобы настроить статический адрес IPv6 на рабочей станции с OC Windows 7/Vista, выполните следующие действия:</u>

1. Откройте Изменение параметров адаптера;

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

 Щелкните правой кнопкой мыши Подключение по локальной сети и выберите Свойства;
 Во вкладке Сеть выберите Протокол Интернета версии 6 (TCP/IPv6) и нажмите кнопку Свойства (рис. 9.4);

Сеть Подключение через:		
Broadcom NetLink	k (TM) Gigabit Ethen	net
		Настроить
Отмеченные компонен	нты используются :	этим подключением:
🗹 🕎 Клиент для се	тей Microsoft	
🗹 📇 Планировщик	пакетов QoS	Miner
Протокол Инт	ернета версии 6 (1	CP/IPV6)
<ul> <li>Протокол Инт</li> <li>Протокол Инт</li> <li>Протокол Инт</li> <li>Лрайвер в/в т</li> </ul>	ернета версии 6 (1 ернета версии 4 (1 годолога канальног	
<ul> <li>Протокол Инт</li> <li>Протокол Инт</li> <li>Драйвер в/в т</li> <li>Ответчик обна</li> </ul>	ернета версии 6 () ернета версии 4 () гополога канальног аружения топологи	СРЛРУВ) СРЛРУВ) го уровня и канального уровня
<ul> <li>Протокол Инт</li> <li>Протокол Инт</li> <li>Драйвер в/в т</li> <li>Ответчик обна</li> </ul>	ернета версии 6 (1 ернета версии 4 (1 гополога канальног аружения топологи	СРЛРV6) СРЛРV4) го уровня и канального уровня
<ul> <li>Ш → Протокол Инт     <li>Щ → Протокол инт     <li>✓ → Драйвер в/в т     <li>✓ → Ответчик обна     </li> </li></li></li></ul>	ернета версии 6 (1 ернета версии 4 (1 гополога канально аружения топологи	СРЛРV6) СРЛРV4) го уровня и канального уровня
<ul> <li>✓ Протокол Инт</li> <li>✓ Протокол инт</li> <li>✓ Драйвер в/в т</li> <li>✓ Ответчик обна</li> </ul>	ернета версии 6 (1 ернета версии 4 (1 гополога канальног аружения топологи Удалить	СРЛРV6) СРЛРV4) го уровня и канального уровня Свойства
<ul> <li>✓ Шротокол Инт</li> <li>✓ Протокол Инт</li> <li>✓ Драйвер в/в т</li> <li>✓ Ответчик обна</li> <li>Установить</li> <li>Описание</li> </ul>	ернета версии 6 (1 ернета версии 4 (1 гополога канальног аружения топологи Удалить	СРЛРV6) СРЛРV4) го уровня и канального уровня Свойства
<ul> <li>Протокол Инт</li> <li>Протокол Инт</li> <li>Драйвер в/в т</li> <li>Ф ответчик обна</li> <li>Установить</li> <li>Описание</li> <li>ТСР/IР версии 6. Са</li> <li>обеспечивающая св</li> </ul>	ернета версии 6 (1 ернета версии 4 (1 гополога канальног аружения топологи Удалить Удалить	СР/1РV6) СР/1РV4) го уровня и канального уровня Свойства ия IP-протокола,
<ul> <li>Протокол Инт</li> <li>Протокол Инт</li> <li>Драйвер в/в т</li> <li>Драйвер в/в т</li> <li>Ответчик обна</li> <li>Установить</li> <li>Описание</li> <li>ТСР/IР версии 6. Са обеспечивающая св взаимосвязанных с</li> </ul>	ернета версии 6 (1 ернета версии 4 (1 гополога канальног аружения топологи Удалить Удалить амая поздняя верси яязь в разнородных сетях.	СР/1РV6) сР/1РV4) го уровня и канального уровня Свойства ия IP-протокола, к
<ul> <li>Протокол Инт</li> <li>Протокол Инт</li> <li>Драйвер в/в т</li> <li>Драйвер в/в т</li> <li>Ответчик обна</li> </ul> Установить Описание ТСР/IР версии 6. Са обеспечивающая св взаимосвязанных с	ернета версии 6 (1 ернета версии 4 (1 гополога канальног аружения топологи Удалить Удалить амая поздняя верси яязь в разнороднью гетях.	СРЛРV6) СРЛРV4) го уровня и канального уровня Свойства ия IP-протокола, к
<ul> <li>Протокол Инт</li> <li>Протокол Инт</li> <li>Драйвер в/в т</li> <li>Драйвер в/в т</li> <li>Ответчик обна</li> <li>Установить</li> <li>Описание</li> <li>ТСР/IР версии 6. Са обеспечивающая св взаимосвязанных с</li> </ul>	ернета версии 6 (1 ернета версии 4 (1 гополога канальног аружения топологи Удалить Удалить амая поздняя верси аязь в разнородных сетях.	СР/1РV6) сР/1РV4) го уровня и канального уровня Свойства ия IP-протокола, к

4. Выберите Использовать следующий ІРv6-адрес (рис. 9.5);

раметры IPv6 можно задавать . зможность. В противном случае	автоматически, если сеть поддерж параметры IPv6 можно узнать у с	кивает такую
министратора.	,,	
问 Получить IPv6-адрес автома	тически	
Оспользовать следующий ІР	v6-адрес:	
IPv6-адрес:	fdd0:5f56:d42c:134e::2	
Длина префикса подсети:	64	J
Основной шлюз:		
🔵 Получить адрес DNS-сервера	автоматически	
Оспользовать следующие ад	peca DNS-серверов:	
Предпочитаемый DNS-сервер:		
Альтернативный DNS-сервер:		
	и выходе	Дополнительно.

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 ІР-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 ІР-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  $\rightarrow$  Панель управления  $\rightarrow$  Центр управления сетями и общим доступом  $\rightarrow$  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 ІР-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.

<u>Чтобы зайти на Web-интерфейс точки доступа, выполните следующие действия:</u>

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*  $\rightarrow$  *IPv6*;

2. Установите галочку Enable IPv6;

3. В поле Get IP From выберите Auto;

#### 4. Нажмите кнопку Save.

D-Link <sup>®</sup>			DAP-2310
Home       Maintenal         DAP-2310       Basic Settings         Wireless       LAN         Py6       Advanced Settings         Image: Construction of the settings       Status	nce  Configu IPv6 Settings  Cet IP From IP Address Prefix Default Gateway	ration ▼ System	Logout () Help

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

Шаг 7. Сохраните и активируйте сделанные настройки. Выберите *Configuration*  $\rightarrow$  *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

<b>D-Link</b>				DAP-2310
🙆 Home 🔏 Mainten	ance 👻 🔚 Config	uration 🔻 👙 System	💋 Logout	🕐 Help
DAP-2310	System Inform	ation		
Advanced Settings	Model Name Firmware Version System Name Location System Time Up Time Operation Mode MAC Address SSID 1~7 IP Address IPv6 IP Address Link-Local IP Address	DAP-2310 1.15 18:12:59 08/08/2012 D-Link DAP-2310 01/01/1970 00:05:59 0 Days, 00:6:00 Access Point b8:a3:86:28:85:50 b8:a3:86:28:85:51 ~ b8:a3:86:28:85:57 192.168.0.50 fe80::baa3:86ff;fe28:8550		

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 ІРv6-адрес автоматически;

5. Нажмите кнопку Ок.

Шаг 10. Укажите в адресной строке Web-браузера сконфигурированный Link-Local IPv6адрес 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 агр.

<u>Чтобы открыть командную строку в WindowsXP, выполните следующие действия:</u> 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 командую строку можно с помощью элементов меню Пуск:

Пуск → Все программы→ Стандартные → Командная строка

<u>Чтобы открыть командную строку в Windows 7/Vista, выполните следующие действия:</u> 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 МАС-адрес рабочей станции ПК1. В командной строке введите: getmac

Запишите МАС-адрес ПК1\_\_\_\_\_

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

Запишите МАС-адрес ПК2

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

Какой МАС-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-аа-00-62-с6-09

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*  $\rightarrow$  *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*  $\rightarrow$  *ARP* и нажмите *Apply* (рис. 10.3).

<u>F</u> ile	Edit	View	<u>Go</u> <u>C</u> ap	ture A	nalyze	Statistics	Telepho	on <u>y T</u> oo	ls <u>I</u> nte	rnals <u>H</u> el	р							
		M 🕅		3 🗔 3	× 2		, 🧼 🝕	> 💫 र	F 🕹		]  €	Q 🔍 🖭		3 🐔	*	Ø		
F	Filter:	arp	>							- Expr	ession	. Clear	Apply	$\supset$	Save			
No.	Т	ime	Sou	irce		0	estinatio	n		Protocol	Length	Info						
	1 (	0.000	00000 Wi	stron	I_73:7	'c:8c I	Broadca	ast		ARP		42 Who	has 192	.168.1	L.2?	Tell	192.1	68.1
	2 (	0.000	37600 Wi	stron	I_72:a	a5:82 N	istror	I_73:7	c:8c	ARP		60 192.	168.1.2	is at	20:	6a:8a:	72:a5	:82
	4 (	0.000	80200 wi	stron	I_72:a	a5:82 B	roadca	ast		ARP		60 Who	has 192	.168.1	L.1?	Tell	192.1	68.1
	5 (	0.000	84600 Wi	stron	I_73:7	C:8c \	istror	11_72:a	5:82	ARP		42 192.	168.1.1	is at	20:	6a:8a:	73:7c	:8c
						D		u 10 3			<b>A</b> 14 B							

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 МАС-адрес устройства-получателя сообщения? _	
Чему равен МАС-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 МАС-адрес устройства-получателя сообщения? \_\_\_\_\_ Чему равен МАС-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.
$\Pi O - Golden FTP Server$	

#### 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.

<u>Чтобы зайти на Web-интерфейс маршрутизатора, выполните следующие действия:</u>

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.

<u>Для Mozilla Firefox:</u> меню Инструменты  $\rightarrow$  Настройки  $\rightarrow$  Дополнительные. Далее вкладка Сеть  $\rightarrow$  Настройка параметров соединения Firefox с Интернетом  $\rightarrow$  Настроить  $\rightarrow$  Без прокси.

<u>Для Internet Explorer</u>: меню Сервис  $\rightarrow$  Свойство обозревателя. Далее вкладка Подключения  $\rightarrow$  Настройка сети  $\rightarrow$  Автоматическое определение параметров.

Authorization	
Login	
admin	
Password	
	EnterClear

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).

Administrator password					
System password setting up					
Password					
•••••					
Confirmation					
•••••					
	Save Cancel				

Рисунок 11.4 Окно изменения пароля администратора, установленного по умолчанию

<u>Примечание:</u> 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*.

Соть	Информация об устрой	йстве	
Clidén'Conned	Модель: Версия прошивки: Время сборки:	DIR-615 1.0.22 Thu Apr 18 17:23:02 MSK 2013	
🥌 Wi-Fi	Производитель: Тех. поддержка:	D-Link Russia support@dlink.ru	
<u>Мастер настройки</u> <u>беспроводной сети</u>	Описание: Ревизия web:	Root filesystem image for DIR-615 791313940a37f62cefcd33a7039b232035ab063c	
Межсетевой экран	Сетевая информация		
Мастер настройки виртуального сервера	LAN IP: Статус подключения WAN: LAN MAC: SSID:	192.168.0.1 • Отключено;Кабель отключен ВС:F6:85:38:D5:F2 DIR-815	
IP телевидение <u>Мастер настройки IPTV</u>	000.		
		Быстрая настройка Расширенные настройки Поис	ĸ

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).

	System	-	Language	-
-			English	
			Русский	
			Українська	
			C• Türkçe	
			Français	
			العربية 🔜	
			فارسى 💶	

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*  $\rightarrow$  *LAN*;

Статус Сетевая статистика <u>DHCP</u> Таблица маршрутизации	»	Сеть WAN LAN	3	Wi-Fi Основные настройки Настройки безопасности МАС-фильтр
Дополнительно Уцан UPnP DDNS	»	Межсетевой экран <u>Р-Фильтры</u> <u>Вругальные серверы</u> » <u>DMZ</u>	0	Система Пароль администратора Конфигурация » Журнал событий

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*.

Сеть »	LAN	2 192.168.0.2	]		
Сетевая маск	a: <b>*</b>	255.255.255.0			
SIP:					
DHCP-c	ервер				
Режим:		Запретить▼			
Статиче	еский DHCP		•		
Известные IP/	/МАС-адреса:	Соверните IP/MAC	адрес		
	IP*	MAC*		Host	
Удалить	Добавить				
					Сохранить

Рисунок 11.9 Изменение ІР-адреса управления маршрутизатора

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



Рисунок 11.10 Сохранение ІР-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*  $\rightarrow$  *WAN*;

3. В открывшемся окне нажмите кнопку Добавить;

4. В поле Тип соединения выберите Статический ІР;

В поле *IP-адрес* введите 192.168.2.2;

В поле Сетевая маска введите 255.255.255.0;

В поле ІР-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.

ип соединения:	:≡ Статический IP	
Інтерфейс:		
1wg-*	etotio Internet 2	
азрешить:	∑ stauc_internet_z	
азрешить. Іаправление:	WAN	
Ethernet		
1TU: <b>*</b>	1500	
IAC:	BC:F6:85:3B:D5:F3	▼ 😅
IP	102 109 2 2	
адрес.	192.108.2.2	
етевая маска:	255.255.255.0	
-адрес шлюза:"	/ 192.168.2.2	
lepвичный DNS-cepвep:*	4.4.4.4	
торичныи DNS-сервер:	2 8.8.8.8	
Разное		
ключить RIP:		
ключить IGMP:		
IAT:		
сетевой экран:		
ing.		

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.

Настройка Go	Iden FTP Server v5.00	
Открытые ресурсы Соединения	⊽ Дата Имя Путь	
Настройки		
2 О программе	Добавить Изменить Удалить Информация	ОК Отмена

Рисунок 11.13

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

🗱 Добавить доступ на ресурс	×
	GOLDEN
	FTP
	SERVER
Путь	$\bigcirc$
Имя	
Разрешить полный доступ	ОК Отмена

Рисунок 11.14

🕅 Добавить д	оступ на ресурс	X
		Golden FTP Server
Путь	C:\Users\edu1\Desktop\soft	
Имя	soft	
🔲 Разрешить	полный доступ	ОК Отмена

Рисунок 11.15

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

Информация	
	GOLDEN
	SERVER
Для того чтобы получить доступ н Internet Explorer, команде Run в ме	< ресурсу по сети, введите в адресной строке ию Пуск или в любом FTP-клиенте следующую
ftp://	/192.168.10.3/soft
📝 Не отображать больше	Копировать в буфер 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).

<u>Примечание:</u> 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;

Статус Сетевая статистика <u>ОНСР</u> Таблица маршрутизации	»	Сеть WAN LAN	Ĩ.	Wi-Fi Вкл Основные настройки Настройки безопасности » МАС-фильтр
Дополнительно VLAN UPAP DDNS	»	Межсетевой экран <u>IP-фильтры</u> <u>Виртуальные серверы</u> » <u>DMZ</u>	0	Система <u>Пароль администратора</u> <u>Конфигурация</u> <u>Журнал событий</u>

Рисунок 11.17 Раздел Межсетевой экран

3. В открывшемся окне нажмите кнопку Добавить;

	Меж	ксетевой эк	ран » 🛛 🖪	Зиртуальные серверы			
	Имя	Интерфейс	Протокол	Внешний порт	Внутренний порт	Внутренний IP	Удаленный IP
<							
							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.

заонон.	Custom •			
1мя:*	<pre>// FTP_service</pre>			
1нтерфейс:	static_Internet_2			
Тротокол:	TCP TCP			
Знешний порт (начальный): <b>*</b>	21			
Знешний порт (конечный):	1			
Энутренний порт (начальный):*	21			
Знутренний порт (конечный):	1			
Знутренний IP:*	/ 192.168.0.3	•		
/даленный IP:	2 192.168.2.3			

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 IPадресов 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 назначается 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 *Cemb*  $\rightarrow$  *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 Сохр. и Перезагрузить.

Р-адрес:*	192.168.0.1		
Сетевая маска:*	255.255.255.0		
SIP:			
DHCP-сервер			
Режим:	Разрешить		
DNS Relay:			
Начальный IP:*	/ 192.168.0.10		
Конечный IP:*	/ 192.168.0.20		
Время аренды (мин).*	1440		
Статический DHC	P		
Известные IP/MAC-адреса:	🖉 <Выберите IP/MAC адресе		
	MAC*	Host	

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 ІР-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	
11/2	

IIKZ	
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 оборудование 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