МЕТОДИЧЕСКИЕ УКАЗАНИЯ
для реализации программы дисциплины
ОП.11 КОМПЬЮТЕРНЫЕ СЕТИ

для специальности

09.02.07 Информационные системы и программирование

Базовая подготовка

2024

СОДЕРЖАНИЕ

Введение

Практические работы направлены на экспериментальное подтверждение и проверку существенных теоретических положений (законов, зависимостей и закономерностей) необходимых при освоении учебной дисциплины. В процессе практического занятия обучающиеся выполняют одну практическую работу под руководством преподавателя в соответствии с изучаемым содержанием учебного материала.

Содержанием практических работ является выполнение различных практических приемов, в том числе профессиональных, работа с компьютером, программами.

Состав заданий для практического занятия спланирован с расчетом, чтобы за отведенное время они могли быть выполнены качественно большинством обучающихся.

Выполнению практических работ предшествует проверка знаний студентов – их теоретической готовности к выполнению задания.

Формы организации работы обучающихся на практических работах, как правило, фронтальная или индивидуальная. При фронтальной форме организации работ все обучающиеся выполняют одновременно одну и ту же работу. При индивидуальной форме организации занятий каждый обучающийся выполняет индивидуальное задание.

Выполнение практических работ по дисциплине ОП.11 Компьютерные сети и средства их реализации направлено на формирование общих компетенций:

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности

ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста

ОК 9. Использовать информационные технологии в профессиональной деятельности

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке

Выполнение лабораторных работ по дисциплине ОП.11 Компьютерные сети направлено на формирование профессиональных компетенций:

ПК 4.1 Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем

ПК 4.4 Обеспечивать защиту программного обеспечения компьютерных систем программными средствами

Практическая работа № 1
Построение схемы компьютерной сети

Цель работы: построение схемы компьютерной сети с помощью MS Visio 2016.
Оборудование: ПК, ПО MS Visio 2016.
Время выполнения: 90 минут.

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Программный продукт Visio

Программный продукт Visio является разработкой компании VisioCorporation, которая была куплена в 2000-м году компанией Microsoft, а программа получила название MicrosoftVisio.

- VisioStandard – служит для создания бизнес-диаграмм, в том числе блок-схем, структурных схем, графиков работ, и др.
- VisioProfessional – средство моделирования и документирования бизнес-процессов, проектирования и построения схем сетей, планов помещений, схематических чертежей, предназначенных для IT-специалистов, инженеров, технических руководителей и разработчиков

программного обеспечения.

Расширенные средства создания схем сетей выделены в дополнительный продукт – MicrosoftVisioEnterpriseNetworkTools, который предоставляет возможности автоматического создания схем сетей, документирование структур каталогов ActiveDirectory, и др.

Область применения

Программный продукт MicrosoftVisio (в дальнейшем - MS Visio) в последнее время активно завоевывает рынок, выступая в качестве эталона деловой графики.

Для рисования на компьютере существуют десятки различных приложений. Это и простейшие графические редакторы типа Paint, и профессиональные системы типа CorelDraw. Visio не заменяет существующих, особенно сильно развитых систем. Но в этой ситуации появляется много примеров, когда инженер, использующий скажем AutoCAD, начинает дополнительно применять MS Visio. Кроме того, существуют области, для которых нет специализированных продуктов кроме MS Visio, например, рисование химических структурных диаграмм.

Для IT-специалистов и разработчиков программного обеспечения особый интерес представляют такие функции пакета MS Visio:

- построение планов зданий и инженерных коммуникаций;
- разработка схем компьютерных сетей;
- разработка диаграмм баз данных;
- проектирование карт web-сайтов.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1.

Запустить *MicrosoftVisio* из группы программ *Microsoft Office.*

Запустить и ознакомиться с разделами справочной системы для работы с *MicrosoftVisio.* Открыть интересующий Вас раздел справки и изучить его.

Просмотреть образцы шаблонов схем, доступных для использования. Изучить интерфейс программы.

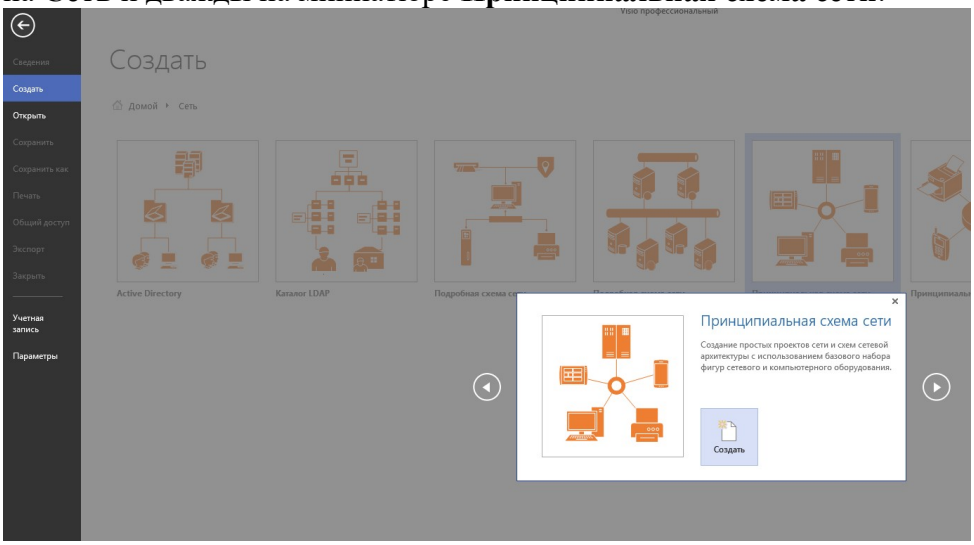
Добавить панели инструментов **Формат текста** и **Формат фигуры (**меню **Вид → Панели инструментов**).

Для добавления необходимой фигуры следует выбрать меню Файл → Фигуры → группа фигур (дополнительные фигуры).

Задание 2.

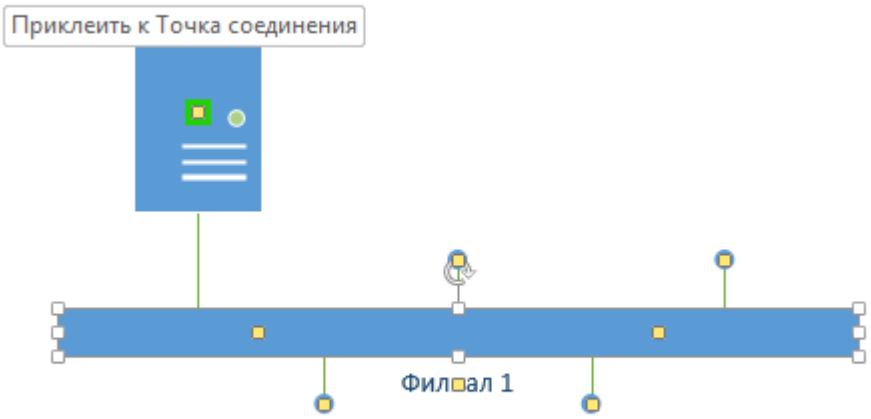
Программы Visio 2016 включают шаблон схемы сети, который называется Принципиальная схема сети. На основе этого шаблона можно построить схему простой корпоративной сети, что мы и продемонстрируем на примере.

1. Для этого щелкнем на вкладке **Файл** и выберем вкладку **Создать**. Щелкнем на **Категории**, затем на **Сеть** и дважды на миниатюре **Принципиальная схема сети**.

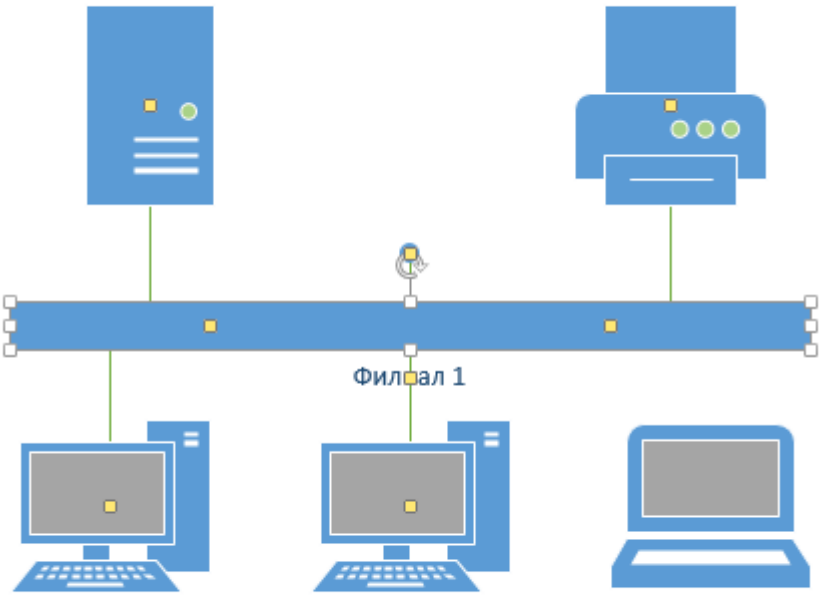


2. Перетащим фигурку **Ethernet** из набора элементов **Сеть и периферийные устройства** на страницу документа и сбросим ее по вертикали по центру чуть правее левого поля страницы.

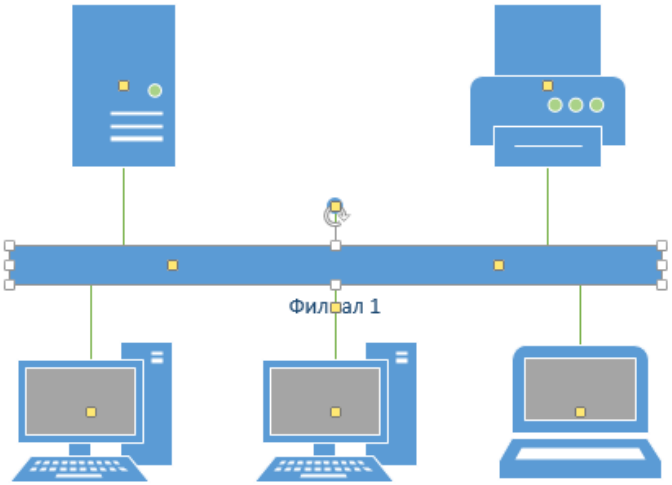
3. Перетащим маркер изменения размера с правого края фигуры **Ethernet** вправо так, чтобы ее ширина стала 100 мм.
4. Не снимая выделение с фигуры **Ethernet**, введем *Филиал 1* в качестве подписи для сегмента сети, затем щелкнем на любой точке фона страницы.
5. Перетащим фигуру **Сервер** на страницу и поместим ее над фигурой Ethernet ближе к левому краю последней.
6. Щелкнем один раз на фигуре **Ethernet**, чтобы выделить ее, а затем перетащим любой и желтых управляющих маркеров в центр сервера, пока вокруг управляющего маркера не появится зеленый квадрат.



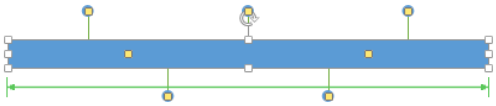
7. Перетащим фигуру **Принтер** над фигурой **Ethernet** ближе к ее правому краю, а затем соединим принтер с сетью, перетащив и приклеив желтый управляющий маркер к принтеру.
8. Перетащим на страницу две фигуры **ПК** и одну фигуру **Ноутбук** из набора **Компьютеры и мониторы** и сбросим их под фигурой **Ethernet**.
9. Перетащим желтый управляющий маркер к каждой из фигур **ПК**.

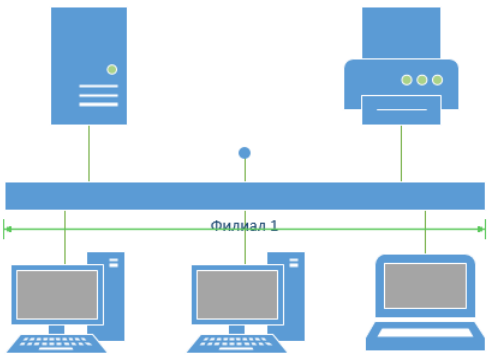


Сейчас только один управляющий маркер остается под фигурой **Ethernet**, но его назначение – перемещение блока текста. А, следовательно, его нельзя использовать для привязки ноутбука к сети.
10. Перетащим управляющий маркер из середины фигуры **Ethernet** и приклеим его к ноутбуку. Теперь ноутбук подключен к сегменту **Ethernet**, но все еще доступны дополнительные управляющие маркеры, как показано на рисунке.



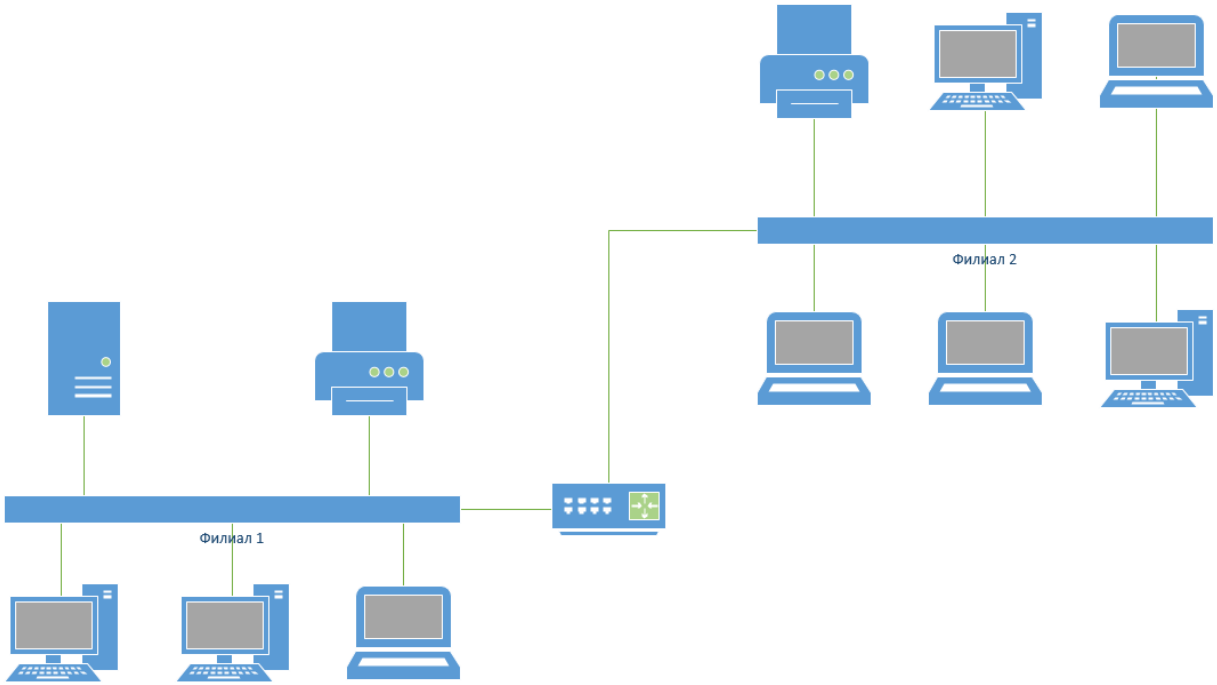
11. Перетащим другую фигуру **Ethernet** в верхний правый угол страницы, оставив достаточно места для того, чтобы над ней можно было разместить другие фигуры.
12. Перетащим левый маркер изменения размера влево, чтобы сделать сегмент **Ethernet** шире. Продолжим перетаскивать, пока не появится двунаправленная стрелка, показывая, что новый сегмент сети имеет такую же длину, как и уже существующий на странице.





13. Не снимая выделения с фигуры **Ethernet**, введем **Филиал 2** и щелкнем на пустом месте страницы.
14. Перетащим фигуру **Принтер**, две фигуры **ПК** и три фигуры **Ноутбук** и соединим их с новым сегментом сети.
15. Перетащим фигуру **Маршрутизатор** из набора элементов **Сеть и периферийные устройства** и разместим ее по центру страницы.

16. Перетащим оставшийся неиспользованный управляющий маркер из фигуры сети **Филиал 1** и приклеим его к маршрутизатору.
17. Перетащим управляющий маркер из сети **Филиал 2** и приклеим его к маршрутизатору.
Соединительная линия изгибается, когда мы перетаскиваем управляющий маркер к маршрутизатору – она ведет себя как динамическая соединительная, а не как простая линия. Получившаяся схема сети представлена на следующем рисунке.



Предоставьте результат работы преподавателю.

Контрольные вопросы:
1. Назначение и возможности *Microsoft Office Visio*.
2. Какие способы настройки окна и панели инструментов программы *MsVisio* вы знаете?
3. Какие группы фигур программы *MsVisio* используются для создания схем и других графических изображений?
4. Какие инструменты для работы с текстом доступны в программе *MsVisio*?

Практическая работа №2
Логическое планирование локальной сети

Цель работы: Изучить структуру сети.
Оборудование: ПК, интернет.
Время выполнения: 90 минут.

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Под логической структурой сети понимается ее организация на 3-м и выше уровнях модели OSI, т.е. сетевые протоколы, адресация, взаимодействие рабочих станций с серверами. В качестве основного сетевого протокола в вычислительной сети предприятия используется протокол IP. Адреса на сетевом уровне для рабочих станций задаются динамически по протоколу DHCP. Логическая топология представляет собой логическую структуру сети. Такая схема определяет, как элементы сети взаимодействуют между собой, как передается информация в сети, и какой путь она при этом преодолевает

В топологии «логическое кольцо» - неразрывное кольцо, с помощью которого передается информация между ПК, в топологии сети обеспечивается соединением всех узлов каналами связи.

Благодаря этому, вся информация движется по кругу в одном направлении. На рис.3.2 представлена логическая топология предприятия.

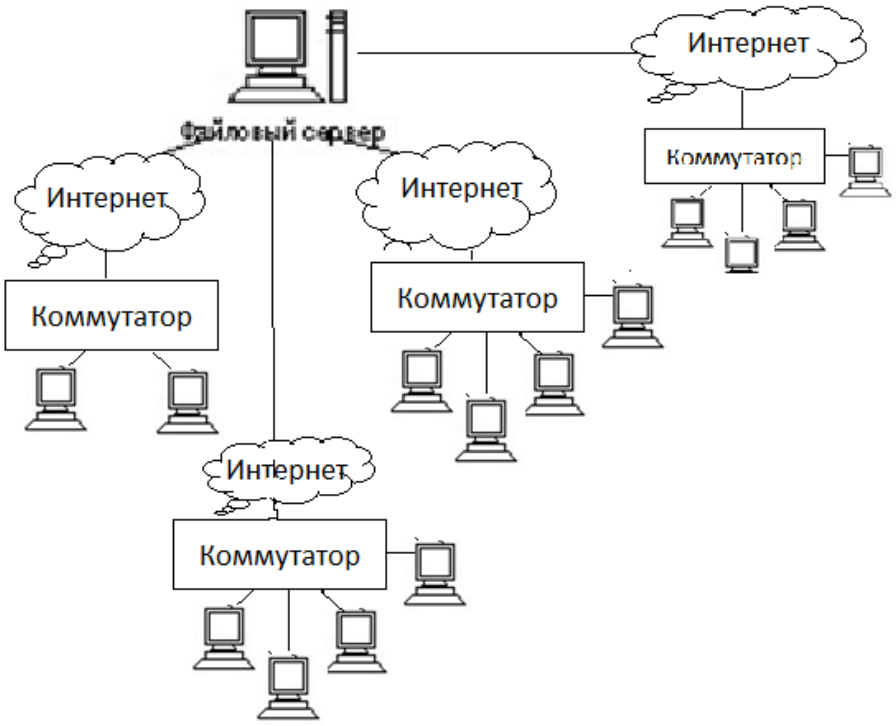


Рис.1- логическая топология предприятия

Планирование физической структуры сети

При проектировании локально-вычислительной сети одним из основных моментов является учет факторов, влияющих на выбор кабельной системы. Перечислим некоторые основные факторы:

• требуемая пропускная способность, скорость передачи в сети

• размер сети, то есть сколько будет в сети рабочих станций;

• требуемый набор служб (передача данных, речи, мультимедиа и т.д.), который необходимо организовать;

• требования к уровню шумов и помехозащищенности;

• общая стоимость проекта, включающая покупку оборудования, монтаж и последующую эксплуатацию.

Можно выделить несколько основных кабельных средств передачи данных в ЛВС:

• витая пара;

• коаксиальный кабель;

• оптоволокно.

Было принято решение использовать экранированную витую пару, так как она соответствует всем основным, предъявляемым к кабельной системе:

• гибкость;

• скорость передачи данных достаточная для ООО «Промагро»

• простота монтажа и обслуживания;

• безопасность передачи данных;

• недорогая себестоимость.

Технико-экономическое обоснование

Выбор сетевой операционной системы

При проектирование сети в трёхэтажном здание, где находится управление ООО «Промагро» была выбрана сетевая операционная система Windows Server Standard R2 2012.

Выбранная операционная система Windows Server Standard R2 2012 обладает следующими качествами:

• позволяет работать с высокими нагрузками;

• обеспечивает резервное восстановление и бесперебойное функционирование всех служб;

• обладает высокой надежностью, легкой доступностью и масштабируемостью;

• предоставляет средства для упрощения управления и администрирования;

• предоставляет расширенную платформу приложений для быстрого создания решений для

обеспечения связей между сотрудниками, партнерами, системами и клиентами путем предоставления встроенного веб-сервера и сервера потоков мультимедиа, обеспечивающих быстрое, простое и надежное создание динамических веб-узлов интрасети Internet

• возможность получения сотрудниками доступа к информации не зависимо от инфраструктуры, сетей, устройств и приложений с которыми они работают;

• обеспечивает непрерывный и безопасный доступ к ресурсам компании и корпоративной сети, упростив при этом процесс идентификации пользователей и управление учетными данными на локальных и облачных ресурсах;

• имеется возможность удаленного доступа к серверу.

Выбор сетевого аппаратного обеспечения

Наиболее дешевый вариант сервера базируется на ПК общего назначения с достаточно большим объемом оперативной памяти.

Кроме сервера, необходимо использовать 13 ПК (по количеству рабочих мест). Для оптимального сочетания стоимости (ремонтопригодности) и качества работы (привлечения клиентов) предлагается использовать следующую конфигурацию каждого ПК.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1.

1. Описать одноранговую локальную сеть с топологией линейная шина.
2. Произвести расчёт стоимости подключения к локальной сети. Расчёт производить согласно ценам на соответствующие товары в магазине (использовать ресурс интернет) и с учётом схемы расположения компьютеров в офисе.
3. Проанализируйте описание локальной сети и сделайте выводы.

Схема локальной сети		
Недостатки		
Преимущества		
Количество компьютеров в сети		
Оборудование, необходимое для создания сети и его стоимость	оборудование	стоимость
Общая стоимость создания локальной сети		
Выводы:		

Задание 2.

1. Описать одноранговую локальную сеть с топологией звезда.
2. Произвести расчёт стоимости подключения к локальной сети. Расчёт производить согласно ценам на соответствующие товары в магазине (использовать ресурс интернет) и с учётом схемы расположения компьютеров в офисе.
3. Проанализируйте описание локальной сети и сделайте выводы.

Схема локальной сети		
Недостатки		
Преимущества		
Количество компьютеров в сети		
Оборудование, необходимое для создания сети и его стоимость	оборудование	стоимость
Общая стоимость создания локальной сети		
Выводы:		

Задание 3.

1. Описать локальную сеть на основе сервера.
2. Произвести расчёт стоимости подключения к локальной сети. Расчёт производить согласно ценам на соответствующие товары в магазине (использовать ресурс интернет) и с учётом схемы расположения компьютеров в офисе.
3. Проанализируйте описание локальной сети и сделайте выводы.

Схема локальной сети		
Недостатки		
Преимущества		
Количество компьютеров в сети		
Оборудование, необходимое для создания сети и его стоимость	оборудование	стоимость
Общая стоимость создания локальной сети		
Выводы:		

Задание 4.

1. Описать беспроводную локальную сеть для портативных компьютеров (ноутбуков).
2. Произвести расчёт стоимости подключения к локальной сети. Расчёт производить согласно ценам на соответствующие товары в магазине (использовать ресурс интернет) и с учётом схемы расположения компьютеров в офисе.
3. Проанализируйте описание локальной сети и сделайте выводы.

Схема локальной сети		
Недостатки		
Преимущества		
Количество компьютеров в сети		
Оборудование, необходимое для создания сети и его стоимость	оборудование	стоимость
Общая стоимость создания локальной сети		
Выводы:		

Контрольные вопросы:

1. Какие топологии сетей вы знаете?
2. Чем отличается локальная сеть от глобальной?
3. Может ли быть компьютер одновременно клиентом и сервером?
4. По вашему мнению какая из топологий сети наиболее подходит образовательному учреждению? почему?

Практическая работа №3
Построение одноранговой сети

Цель работы: освоение умений по построению одноранговой локальной вычислительной сети.

Оборудование: рабочая станция, коммутатор DES-1100-16, витая пара, комплект для обжима кабеля, сетевой тестер**,** разъемы RG – 45 - 4 шт.

Время выполнения: 90 минут.

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Одноранговая сеть представляет собой сеть равноправных компьютеров – рабочих станций, каждая из которых имеет уникальное имя и адрес. Все рабочие станции объединяются в рабочую группу. В одноранговой сети нет единого центра управления – каждая рабочая станция сети может отвечать на запросы других компьютеров, выступая в роли сервера, и направлять свои запросы в сеть, играя роль клиента.

Одноранговые сети являются наиболее простым для монтажа и настройки, а также дешевым типом сетей. Для построения одноранговой сети требуется всего лишь несколько компьютеров с установленными клиентскими ОС, и снабженных сетевыми картами. Все параметры безопасности определяются исключительно настройками каждого из компьютеров.

К основным достоинствам одноранговых сетей можно отнести:

- простоту работы в них;
- низкую стоимость, поскольку все компьютеры являются рабочими станциями;
- относительную простоту администрирования.
- Недостатки одноранговой архитектуры таковы:
- эффективность работы зависит от количества компьютеров в сети;
- защита информации и безопасность зависит от настроек каждого компьютера.

Серьезной проблемой одноранговой сетевой архитектуры является ситуация, когда компьютеры отключаются от сети. В этих случаях из сети исчезают все общесетевые сервисы, которые они предоставляли (например, общая папка на диске отключенного компьютера, или общий принтер, подключенный к нему).

Администрировать такую сеть достаточно просто лишь при небольшом количестве компьютеров. Если же число рабочих станций, допустим, превышает 25-30 – то это будет вызывать определенные сложности.

Построить одноранговую сеть просто. Ее особенность заключается в том, что все входящие в ее состав компьютеры работают сами, то есть ими никто не управляет.

Одноранговая сеть выглядит как некоторое количество компьютеров, объединенных в рабочую группу с помощью одного из существующих вариантов связи. Отсутствие управляющего компьютера – сервера – делает ее построение дешевым и эффективным.

Любой компьютер в такой сети можно называть сервером, поскольку он сам определяет набор правил, которых должны придерживаться другие пользователи, если хотят использовать его ресурсы. За компьютером такой сети следит пользователь (или пользователи), который работает на нем. В этом заключается главный недостаток одноранговой сети: ее пользователи должны не просто уметь работать на компьютере, но и иметь представление об администрировании. В большинстве случаев им приходится самостоятельно справляться с возникающими внештатными ситуациями и защищать свои компьютеры от неприятностей, начиная с вирусов и заканчивая программными и аппаратными неполадками.

Одноранговая сеть позволяет использовать общие ресурсы, файлы, принтеры, модемы и т. п. Из-за отсутствия управляющего компьютера каждый пользователь разделяемого ресурса должен самостоятельно устанавливать правила его использования.

Для работы с одноранговыми сетями подходит любая существующая операционная система. К примеру, ее поддержка реализована в операционной системе Windows начиная с версии Windows 95, поэтому дополнительного программного обеспечения для работы в локальной сети не требуется. Однако если вы хотите обезопасить себя от программных проблем, лучше использовать операционную систему высокого класса, к примеру Windows XP.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

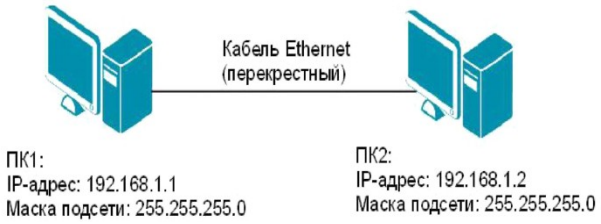
1. Выполните практические задания 1, 2 и 3, делая промежуточные записи в карте - отчете.
2. Результаты выполнения каждого практического задания продемонстрируйте преподавателю.
3. После контроля выполнения последнего практического задания, восстановите исходные сетевые параметры на своем рабочем компьютере и проверьте работоспособность локальной и глобальной сети.
4. Приведите рабочее место в порядок.

Задание 1.

Обожмите 2 отрезка UTP – кабеля с обеих сторон по стандарту EIA/TIA-568A (прямой кабель).

Методические рекомендации: Вставляя проводники в разъем, следите за тем, чтобы они доходили до конца разъема, а внешняя изоляция кабеля выходила за фиксирующую защелку. Для проверки правильности обжима используйте сетевой тестер.

Практическое задание № 2. Создайте подключение типа «компьютер-компьютер».



Методические рекомендации: Проверьте наличие физического соединения между компьютерами по индикации светодиодов на сетевых адаптерах ПК1 и ПК2. Перед тем как изменить параметры IP – адресации, запишите в тетрадь все сетевые параметры, установленные на вашем компьютере (IP – адрес, маску подсети, основной шлюз) для последующего их восстановления. Осуществите настройку сетевых параметров и проверьте наличие соединения между ПК 1 и ПК 2.

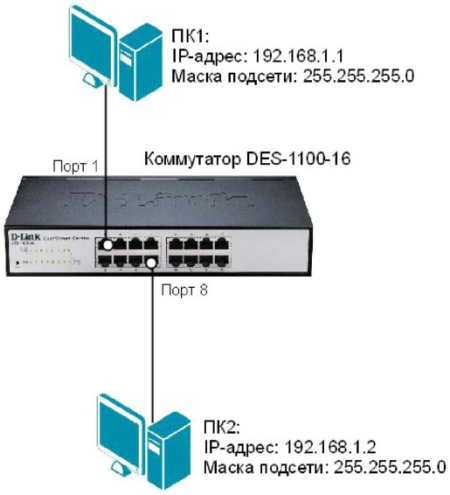


Рисунок 1 - Схема подключения типа «компьютер-компьютер»

Задание 2.

Создайте одноранговую сеть с использованием коммутатора. Получите доступ к текстовому файлу, расположенному на соседнем компьютере.

Методические рекомендации: Осуществите подключение элементов сети по схеме. Проверьте наличие физического соединения между ПК1, ПК 2 и коммутатором по индикации светодиодов.

Осуществите настройку сетевых параметров и проверьте наличие соединения между ПК 1 и ПК 2.

Для обеспечения доступа к вашему файлу с соседнего компьютера настройте для текущей папки общий доступ.

Инструкции по выполнению практических заданий:

Создание подключения типа «компьютер-компьютер».

Шаг 1. Подключите ПК1 и ПК2 в соответствии со схемой прямым Ethernet -ткабелем (рис. 1).

Шаг 2. Настройте статический IP-адрес на рабочих станциях ПК1 и ПК2.

1. Откройте *Сетевые подключения* (Пуск - Панель управления - Сетевые подключения);
2. В контекстном меню пункта *Подключение по локальной сети* выберите *Свойства*;
3. В диалоговом окне выберите *Протокол Интернета (TCP/IP)* и нажмите *Свойства*;
4. Выберите *Использовать следующий IP-адрес (см. рис. 2)*;
5. Задайте новые IP – адрес и маску подсети для ПК1 (или ПК 2) (см. рис. 1).

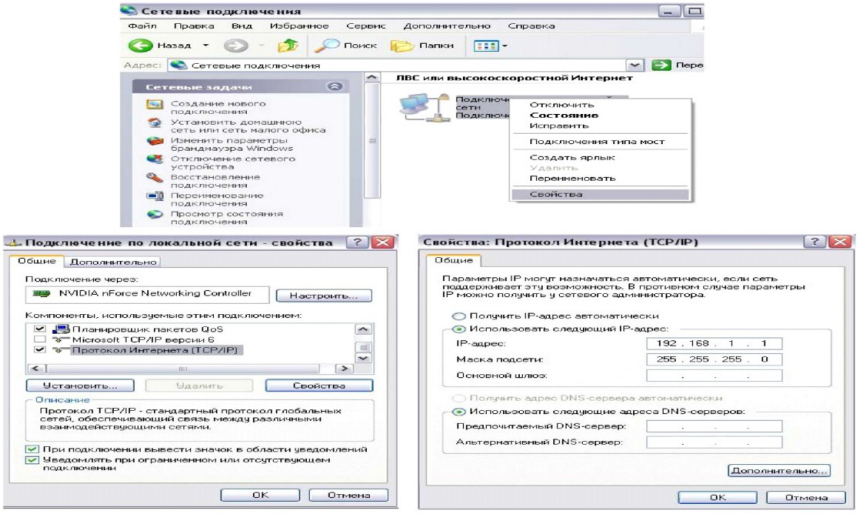
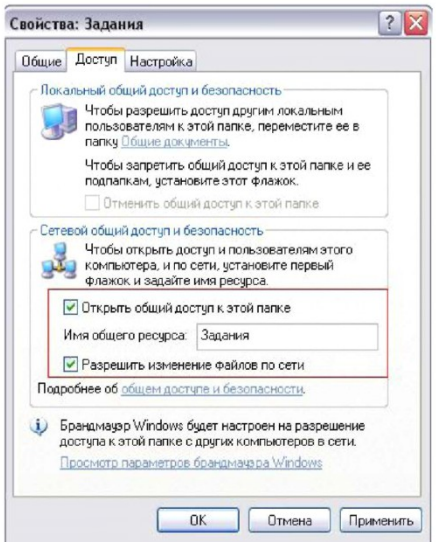


Рисунок 3 - Настройка статического IP-адреса для ОС Windows XP

Шаг 3. Проверьте конфигурацию сетевого адаптера ПК1 (или ПК 2) с помощью команды *ipconfig*.

Шаг 4. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2 с помощью команды ping .



Задание 3.

Создание одноранговой сети с использованием коммутатора. Получение доступа к текстовому файлу, расположенному на соседнем компьютере.

Шаг 1. Подключите ПК1 и ПК2 к коммутатору DES-1100-16 «прямым» Ethernet-кабелем в соответствии со схемой (см. рис. 2).

Шаг 2. Проверьте доступность соединения между рабочими станциями ПК1 и ПК2 с помощью команды ping.

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

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

3. Во вкладке *Доступ - Сетевой общий доступ и безопасность* выберите *Открыть общий доступ к этой папке* и *Разрешить изменение файлов по сети;* Рисунок 4 - Настройка общего доступа

4. Нажмите кнопку *Применить;*

5. В данной сетевой папке создайте пустой текстовый документ.

Шаг 4. На рабочей станции ПК1 (ПК 2) проверьте доступ к документам на рабочей станции ПК2, внесите изменения и сохраните.

1. В адресной строке папки *Мой компьютер* введите \ \192.168.1.2 (\ \192.168.1.1) и нажмите *Enter;*

2. Найдите созданную папку соседнего компьютера с открытым общим доступом;

3. Внесите в представленный текстовый файл свои личные данные и сохраните его.

Контрольные вопросы:

1. Одноранговой называется сеть, которая…
2. Для построения одноранговой сети могут использоваться следующие топологии:
3. Правильность обжима кабеля Ethernet определяется…
4. Чтобы установить новый IP- адрес для компьютера необходимо…
5. Чтобы получить информацию о конфигурации сетевого адаптера необходимо использовать сетевую утилиту …
6. Как проверить наличие соединения между ПК1 и ПК2 необходимо?
7. Папка, для которой настроен общий доступ, отличается от обычной папки тем, что …
8. Чтобы получить доступ к открытым ресурсам другого компьютера необходимо …

Практическая работа №4
Создание общих сетевых ресурсов

Цель работы: научиться настраивать общие папки, для организации общего доступа к файлам и папкам для компьютеров, которые расположены в одной локальной группе или в одном домене.

Оборудование: ПК, MS Windows

Время выполнения: 90 минут.

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

При работе с домашней локальной сетью или с компьютерами интрасети организации вам придется настраивать общие папки, так как, вероятнее всего, что ваши пользователи захотят разрешать сотрудникам просматривать, изменять и создавать файлы и папки для компьютеров, которые расположены в одной локальной группе или в одном домене. В настройке общего доступа к файлам и папкам нет ничего сложного, но в связи с тем, что для открытия общего доступа нужны права администратора, не всем пользователям вашей сети будет предоставлена такая возможность. Но после того как вы настроите на пользовательских компьютерах параметры общего доступа, пользователи смогут самостоятельно предоставлять доступ к своим папкам и файлам.

Какие же задачи можно выполнить при помощи общего доступа? Для того чтобы ваши пользователи могли просматривать содержимое локальной сети и иметь доступ к компьютерам и устройствам вы можете включить сетевое обнаружение. Если к каждому компьютеру вашей сети не подключен локальный принтер, вам придется открывать общий доступ к принтерам, для того чтобы пользователи могли распечатывать свою документацию. Вы можете предоставлять общий доступ к ресурсам компьютера, как для всех пользователей, так и для тех пользователей, учетные данные которых имеются на компьютере, предоставляющем общий доступ к файлам и папкам. Вы можете разрешить пользователям обмениваться музыкой, видеофайлами и картинками, разрешив общий доступ к потоковому мультимедиа и прочее.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1. Поиск других ПК в сети

Поиск компьютеров и рабочих групп в сети возможен с помощью поисковой системы Windows XP. Зайдите в "Сетевое окружение" и нажмите на клавишу F3, затем заполните поле "Введите имя искомого компьютера или его IP адрес". Мы будем искать, например, второй ПК в рабочей группе 110 (рис.1).

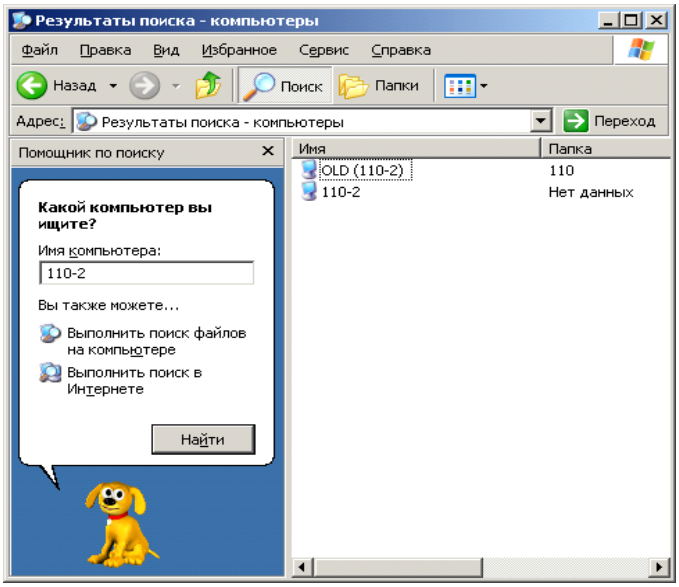


Рис. 1. Поиск компьютера 110-2 в сети

Настройка_11 общего доступа к сетевым ресурсам

В этом примере мы сделаем общей папку Мои документы.

Простой общий доступ к файлам

Правой кнопкой мыши щелкните на папке Мои документы и выполните команду Свойства-Доступ. На вкладке Доступ установите флажки как на рис.2.

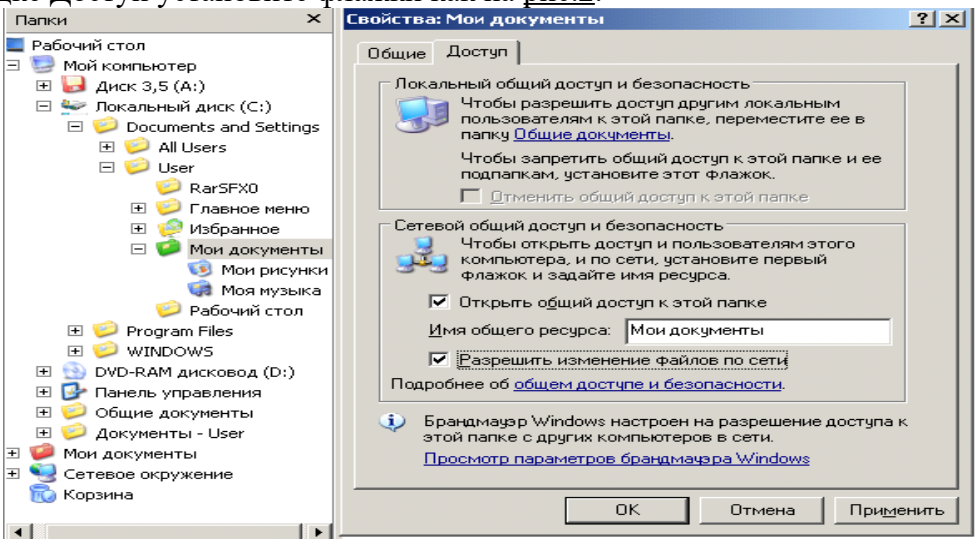


Рис. 2. В окне Мои документы активна вкладка Доступ

После закрытия данного окна с новыми настройками на значке папки Мои документы появиться рука, что означает, что этот ресурс сети – общий.

Расширенный общий доступ к файлам

Обычно достаточно режима "Простой общий доступ к файлам", однако, если требуется более серьёзное разграничение прав пользователей, то необходимо включить "Расширенный общий доступ", для этого, в любом окне нужно выбрать: Сервис-Свойства папки-Вид, и убрать галочку с параметра "Использовать простой общий доступ к файлам" (рис.3).

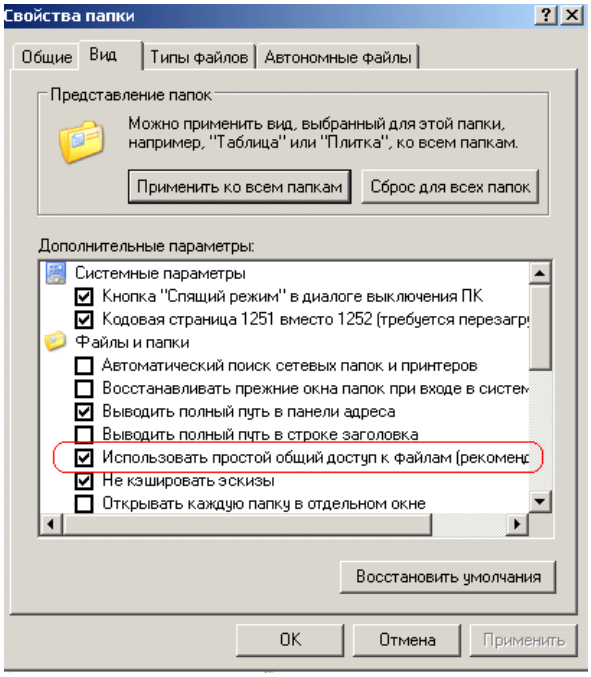


Рис.3. Задаем Расширенный общий доступ

Снова для папки Мои документы выполняем команду Свойства – Доступ (рис.4).

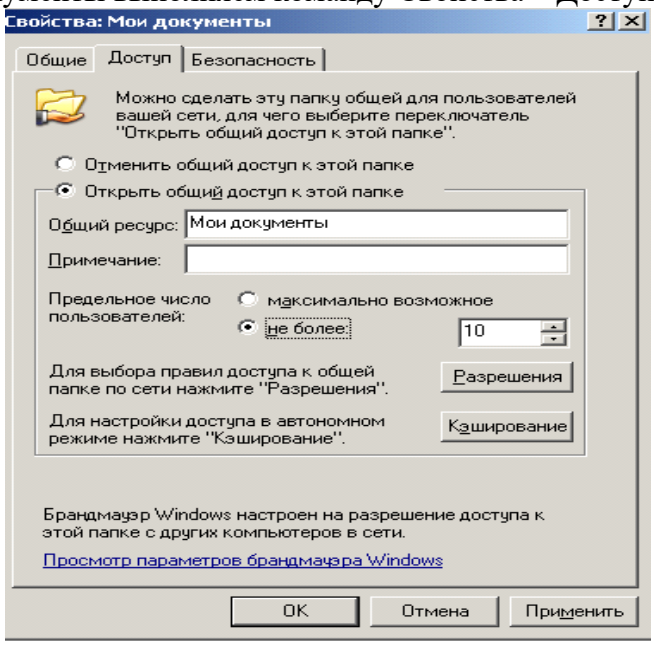


Рис.4. Активна вкладка Доступ

Теперь мы видим новый элемент - кнопку "Разрешения", которая задает пользователей, которым будет доступна данная папка (рис.5).

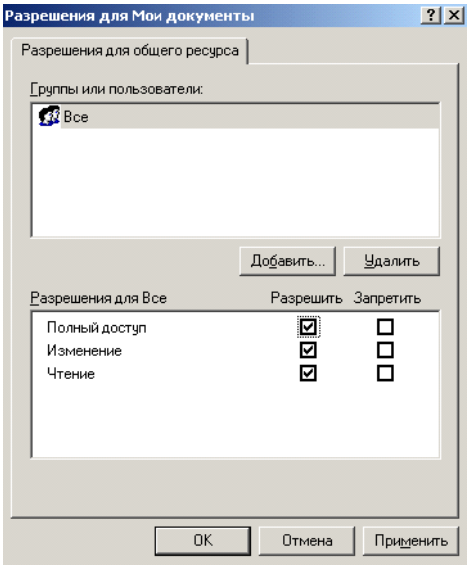


Рис5. Разрешено всем все

Возможные проблемы с общим доступом к ресурсам сети

Если создать сетевой доступ к ресурсам не получается, то постарайтесь исправить ситуацию, придерживаясь следующих рекомендаций:

- Проверьте правильность сетевых настроек антивируса и брандмауэра.
- Не используйте в именах компьютера русские буквы, это может привести к программным ошибкам.

Измените необходимые разрешения прав пользователя на вкладке Безопасность (рис.6):

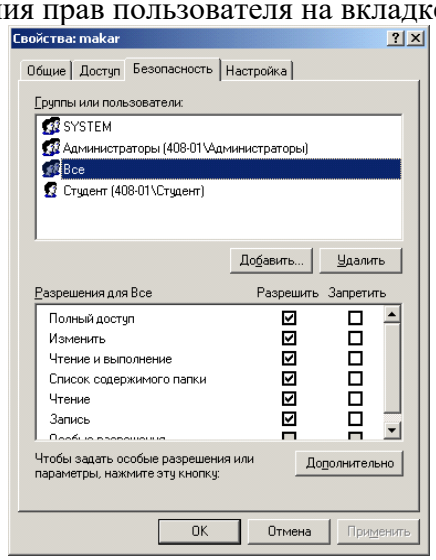


Рис.6. Всем пользователям даны все права

Вместо задания конкретного IP вручную можно установить переключатель на автоматическое определение IP (рис.7).

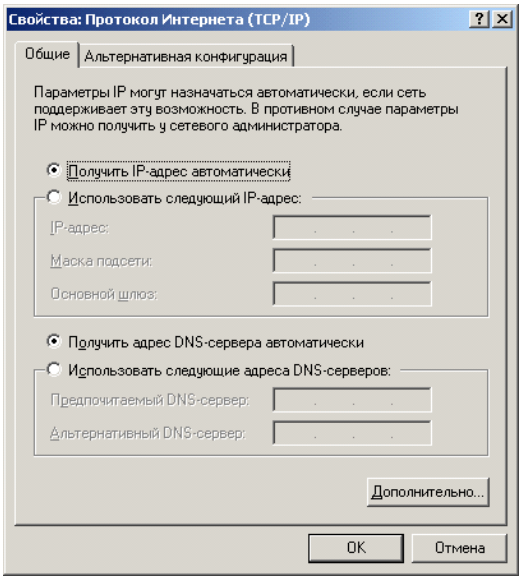


Рис.7. Переключатель получения IP автоматически

Время и дата на часах всех ПК должны быть одинаковы.

Создаем сетевой диск Z, общий для всех ПК

Каждый раз искать общую папку в Сетевом окружении не очень удобно. Имеет смысл подключить ее к вашему компьютеру в качестве сетевого диска. Он будет отображаться в списке дисков окна Мой компьютер, и вы сможете быстро работать с его содержимым. Чтобы подключить общую папку с другого компьютера как сетевой диск выполните команду Пуск - Мой компьютер - Сетевое окружение, затем выберите компьютер локальной сети и находящуюся на нем общую папку, которую вы хотите подключить на свой ПК в качестве сетевого диска. Щелкните по папке правой кнопкой мыши и выберите Подключить сетевой диск (рис.8).

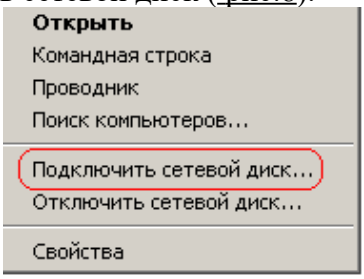


Рис.8. Контекстное меню подключения сетевого диска

В появившемся окошке выберите букву, под которой сетевой диск будет отображаться в списке дисков вашего компьютера. Также отметьте галочкой пункт "Восстанавливать при входе в систему", чтобы при включении компьютера и загрузке Windows автоматически отображала сетевой диск в списке дисков вашего ПК (рис.9).

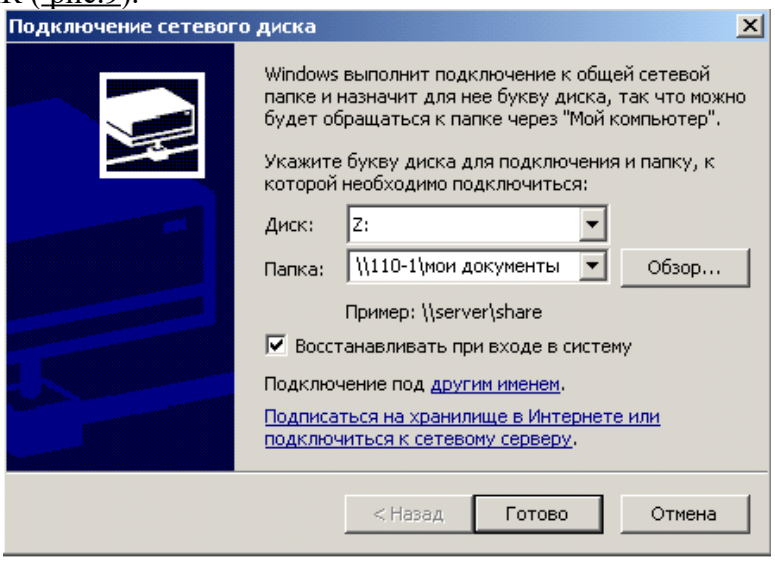


Рис.9. Назначаем диску букву Z

Теперь можете просто зайти в Мой компьютер, и вы увидите сетевой диск (рис.10).

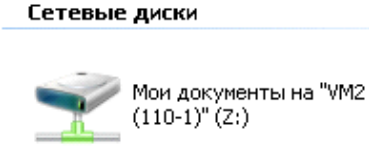


Рис.10. В качестве сетевого диска будем использовать общую папку Мои документы, размещенную на ПК 110-1

Контрольные вопросы

1. Каким образом можно получить доступ к окну «Дополнительные параметры общего доступа»?
2. Опишите функции «Сетевого обнаружения».
3. Какие особенности функционала сетевого обнаружения существуют в доменном окружении?
4. В каком случае доступ к файлам и папкам можно организовать по умолчанию?
5. Приведите примеры различных видов доступа для различных пользователей.
6. Что представляют собой дополнительные настройки для папок открытого доступа?
7. Опишите ситуацию подключения к общим папкам пользователей компьютеров сети.
8. Для чего и каким образом настраивается потоковая передача мультимедиа?
9. Опишите алгоритмы шифрования для подключений, которые предоставляет операционная система Windows 7.
10. В каких ситуациях целесообразно назначать доступ с парольной защитой, и какие особенности настройки при этом возникают?
11. Каким образом настраивается доступ к файлам и папкам для домашней группы?

Практическая работа №5
Организация сетевого шлюза (Настройка программного маршрутизатора)

Цель работы: Усвоить навыки настройки маршрутизатора.
Оборудование: ПК
Время выполнения: 90 минут.

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

С распространением широкополосного доступа в Интернет все большую популярность среди домашних пользователей приобретают беспроводные маршрутизаторы, позволяющие организовать в квартире разделяемый на несколько компьютеров доступ в Интернет. Кроме того, учитывая возможности маршрутизаторов по организации беспроводных каналов связи, их использование избавляет от необходимости прокладывать сетевые кабели по всей квартире. Сегодня предлагается множество разнообразных моделей беспроводных маршрутизаторов для домашнего применения. Но как сделать правильный выбор? Какой маршрутизатор предпочесть и, главное, как его правильно настроить? В настоящей статье мы рассмотрим основные возможности современных маршрутизаторов и дадим пошаговую инструкцию по их настройке.

Современный домашний компьютер уже немыслим без подключения к Интернету. Аналоговые модемы безвозвратно ушли в прошлое, и на смену им появились технологии высокоскоростного доступа в Интернет, а тарифы за организацию безлимитного доступа стали сравнимы с ежемесячной платой за телефон. Поэтому вполне естественно, что вслед за покупкой домашнего компьютера пользователи задумываются об организации выхода в Интернет.

При подключении к Интернету одного домашнего компьютера проблем не возникает. Это, конечно, нетривиальная задача для начинающих пользователей, поскольку требуется создать новое сетевое соединение и произвести необходимые для него настройки, но если повезет, то все это выполнят инженеры, которые будут подключать компьютер к Интернету.

Однако со временем у вас может появиться второй компьютер, ноутбук или КПК с беспроводным адаптером. Конечно же, вы захотите подключить к Интернету и все эти устройства. Для этого вам

уже придется использовать маршрутизатор, который будет выполнять функцию шлюза между вашей локальной сетью в квартире и внешней сетью Интернет.

Естественно, возникает вопрос о выборе маршрутизатора и о его функциональных возможностях.

Сразу отметим, что все современные маршрутизаторы, ориентированные на домашних пользователей, объединяют в себе множество сетевых устройств и маршрутизатор — лишь одно из них, хотя и главное. Именно поэтому некоторые производители, стремясь подчеркнуть ориентацию своих устройств на домашних пользователей, а также их многофункциональность, из маркетинговых соображений называют их домашними интернет-центрами. Правда, это лишь вносит путаницу в классификацию такого рода устройств, общепризнанное же их название — широкополосные беспроводные маршрутизаторы.

До недавнего времени маршрутизаторы для домашних пользователей не имели интегрированной точки беспроводного доступа. Сейчас эти устройства уже морально устарели и ориентироваться на них не стоит.

Функциональные возможности беспроводных маршрутизаторов

Итак, современный широкополосный беспроводной маршрутизатор представляет собой многофункциональное устройство, в котором объединены:

- маршрутизатор;
- коммутатор сети Fast Ethernet (10/100 Мбит/с);
- точка беспроводного доступа;
- брандмауэр;
- NAT-устройство.

Основная задача, возлагаемая на беспроводные маршрутизаторы, — это объединение всех компьютеров домашней сети в единую локальную сеть с возможностью обмена данными между ними и организация высокоскоростного, безопасного подключения к Интернету всех домашних компьютеров

В настоящее время наиболее популярными способами являются подключение к Интернету по телефонной линии с использованием ADSL-модема и по выделенной линии Ethernet. Исходя из этого, все беспроводные маршрутизаторы можно условно разделить на два типа:

- для подключения по выделенной Ethernet-линии;
- для подключения по телефонной линии.

В последнем случае в маршрутизатор встроен еще и ADSL-модем.

Согласно статистике, у провайдеров все более популярным становится способ подключения по выделенной Ethernet-линии. При этом предназначенные для этого маршрутизаторы могут использоваться и для подключения к Интернету по телефонной линии, но для этого придется дополнительно приобрести ADSL-модем.

Итак, маршрутизаторы — это сетевые устройства, устанавливаемые на границе внутренней локальной домашней сети и Интернета, а следовательно, выполняющие роль сетевого шлюза. С конструктивной точки зрения маршрутизаторы должны иметь как минимум два порта, к одному из которых подключается локальная сеть (этот порт называется внутренним LAN-портом), а ко второму — внешняя сеть, то есть Интернет (данный порт называется внешним WAN-портом). В домашних маршрутизаторах предусмотрены один WAN-порт и четыре внутренних LAN-порта, которые объединяются в коммутатор. И WAN-, и LAN-порты имеют интерфейс 10/100Base-TX, и к ним можно подключать сетевой Ethernet-кабель.

Интегрированная в маршрутизатор точка беспроводного доступа позволяет организовать беспроводной сегмент сети, который для маршрутизатора относится к внутренней сети. В этом смысле компьютеры, подключаемые к маршрутизатору беспроводным способом, ничем не отличаются от тех, что подключены к LAN-порту.

Задача интегрированного в маршрутизатор брандмауэра сводится к обеспечению безопасности внутренней сети. Для этого брандмауэры должны уметь маскировать защищаемую сеть, блокировать известные типы хакерских атак и утечку информации из внутренней сети, контролировать приложения, получающие доступ во внешнюю сеть.

Для того чтобы реализовать указанные функции, брандмауэры анализируют весь трафик между внешней и внутренней сетями на предмет его соответствия тем или иным установленным критериям или правилам, определяющим условия прохождения трафика из одной сети в другую. Если трафик отвечает заданным критериям, то брандмауэр пропускает его через себя. В противном случае, то есть

если установленные критерии не соблюдены, трафик блокируется. Брандмауэры фильтруют как входящий, так и исходящий трафик, а также позволяют управлять доступом к определенным сетевым ресурсам или приложениям.

По своему назначению брандмауэры напоминают контрольно-пропускной пункт охраняемого объекта, где производится проверка документов всех входящих на территорию объекта и всех покидающих ее. Если пропуск в порядке — доступ на территорию разрешен. Аналогично действуют и брандмауэры, только в роли людей, проходящих через КПП, выступают сетевые пакеты, а пропуском является соответствие заголовков этих пакетов заданному набору правил.

Все современные маршрутизаторы со встроенными брандмауэрами являются NAT-устройствами, то есть поддерживают протокол трансляции сетевых адресов NAT (Network Address Translation). Данный протокол не является составной частью брандмауэра, но способствует повышению безопасности сети. Основная его задача — решение проблемы дефицита IP-адресов, которая становится все более актуальной по мере роста числа компьютеров.

Протокол NAT определяет, каким образом происходит преобразование сетевых адресов. NAT-устройство преобразует IP-адреса, зарезервированные для частного использования в локальных сетях, в открытые IP-адреса. К частным адресам относятся следующие IP-диапазоны: 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255. Частные IP-адреса нельзя использовать в Глобальной сети, поэтому они могут свободно применяться только для внутренних целей.

Помимо перечисленных функциональных возможностей некоторые модели беспроводных маршрутизаторов имеют ряд дополнительных. К примеру, они могут быть оборудованы портами USB 2.0, к которым можно подключать внешние устройства с возможностью организации разделяемого сетевого доступа к ним. Так, при подключении к маршурутизатору принтеров по интерфейсу USB 2.0 мы получаем еще и принт-сервер, а при подключении внешнего жесткого диска — сетевое устройство хранения данных типа NAS (Network Attached Storage). Кроме того, в последнем случае используемое в маршрутизаторах ПО позволяет организовать даже FTP-сервер.

Существуют модели маршрутизаторов, которые имеют не только USB-порты, но и встроенный жесткий диск, а потому могут применяться для сетевого хранения данных, в качестве FTP-серверов для доступа как извне, так и из внутренней сети и даже выполнять функции мультимедийных центров.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 3: Настройте базовые параметры для маршрутизатора R1.

- Отключите поиск DNS.
- Назначьте имя устройства.
- Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTY и активируйте вход.
- Настройте адресацию на интерфейсах G0/0 и G0/1 и включите оба интерфейса.

Шаг 4: Настройте базовые параметры на коммутаторах S1 и S2.

- Отключите поиск DNS.
- Назначьте имя устройства.
- Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTY и активируйте вход.

Шаг 5: Настройте базовые параметры на компьютерах PC-A и PC-B.

На компьютерах PC-A и PC-B настройте IP-адреса и адрес шлюза по умолчанию в соответствии с таблицей адресации.

Задание 2.

Настройте коммутаторы для работы с сетями VLAN и создания транковых каналов

Шаг 1: Настройте сети VLAN на коммутаторе S1.

- Создайте сеть VLAN 10 на коммутаторе S1. Назначьте **Student** в качестве имени сети VLAN.
- Создайте виртуальную локальную сеть VLAN 20. Назначьте **Faculty-Admin** в качестве имени для этой сети VLAN.
- Настройте F0/1 в качестве транкового порта.
- Назначьте порты F0/5 и F0/6 сети VLAN 10 и настройте оба порта в качестве портов доступа.
- Назначьте IP-адрес сети VLAN 10 и активируйте его. Сверьтесь с таблицей адресации.
- Настройте шлюз по умолчанию в соответствии с таблицей адресации.

Шаг 2: Настройте сети VLAN на коммутаторе S2.

- Создайте сеть VLAN 10 на коммутаторе S2. Назначьте **Student** в качестве имени сети VLAN.
- Создайте виртуальную локальную сеть VLAN 20. Назначьте **Faculty-Admin** в качестве имени для этой сети VLAN.
- Настройте F0/1 в качестве транкового порта.
- Назначьте порты F0/11 и F0/18 сети VLAN 20 и настройте оба порта в качестве портов доступа.
- Назначьте IP-адрес сети VLAN 10 и активируйте его. Сверьтесь с таблицей адресации.
- Настройте шлюз по умолчанию в соответствии с таблицей адресации.

Задание 3.

Проверка транковой связи, сетей VLAN, маршрутизации и подключения

Шаг 1: Проверьте таблицу маршрутизации маршрутизатора R1.

- На маршрутизаторе R1 выполните команду **show ip route**. Какие маршруты указаны в маршрутизаторе R1?
- На коммутаторах S1 и S2 выполните команду **show interface trunk**. Настроен ли порт F0/1 на обоих коммутаторах на транковую связь?
- На коммутаторах S1 и S2 выполните команду **show vlan brief**. Убедитесь, что сети VLAN 10 и 20 активны и что соответствующие порты в коммутаторах находятся в соответствующих VLAN. Почему порт F0/1 не указан в какой-либо из активных VLAN?
- От компьютера PC-A в сети VLAN 10 отправьте эхо-запрос на компьютер PC-B в сети VLAN 20.

Если маршрутизация VLAN работает правильно, эхо-запросы между сетями 192.168.10.0 и 192.168.20.0 должны быть успешными.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

- Проверьте наличие подключения между всеми устройствами. Эхо-запросы должны быть успешными между всеми устройствами. Если эхо-запросы не удались, исправьте неполадки.

Контрольные вопросы:

1. В чём заключается преимущество использования устаревшего метода маршрутизации между VLAN?
2. На кого ориентированы современные маршрутизаторы ?

Практическая работа №6
Настройка протоколов TCP/IP в операционных системах

Цель: обобщение и систематизация знаний по теме «Межсетевое взаимодействие»

Оборудование: ПК, MS Windows, виртуальная машина VM-1, IP-адрес, маска подсети, основной шлюз, предпочитаемый DNS;

Время выполнения: 90 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Стек протоколов TCP/IP является основным набором протоколов сети Интернет. В настоящее время стек протоколов поддерживается всеми без исключения операционными системами общего

назначения и является наиболее широко распространенным стеком, используемым как в глобальных, так и локальных сетях любого масштаба. Стек TCP/IP соответствует пятиуровневой сетевой модели и включает в себя большое число протоколов. Основу коммуникационной составляющей данного стека (транспортной подсистемы) составляют протокол сетевого уровня IP – Internet Protocol (Межсетевой протокол), а также протокол транспортного уровня TCP – Transmit Control Protocol (Протокол управления передачей). Функции данных протоколов поддерживаются специальными модулями операционных систем, входящими в состав их ядра. Это определяет необходимость выполнение работ по настройке данных протоколов при конфигурировании операционной системы для работы в IP– сетях.

Замечание: Настройки требует только протокол IP. Однако в документации на ОС семейства Windows практически повсеместно употребляется оборот "протокол TCP/IP", что является неточным, так как аббревиатуру TCP/IP часто используют либо для обозначения всего стека протоколов Интернет, либо для обозначения пары протоколов TCP и IP, работающих на транспортном и сетевом уровнях семиуровневой модели OSI . Протокол TCP в процессе работы ОС в IP– сетях обычно никаких настроек не требует, хотя такая возможность имеется.

Установка протокола TCP/IP

Установка TCP/IP в ОС Windows XP достаточно проста и понятна. Имеется несколько способов выполнения данной процедуры. В различных ОС семейства Windows число этих вариантов различно. Рассмотрим основной способ установки, поддерживаемый всеми без исключения типами ОС семейства Windows, – установку с помощью панелиь **Управления (Control Panel).** Необходимо вызвать панель управления **(Пуск/Настройка/Панель управления),** а затем дважды щелкнуть значок **Network ("Сеть" или "Сетевые подключения").** В появившемся окне "**Сетевые подключения**" найти настраиваемый сетевой интерфейс, в контекстном меню интерфейса выбрать пункт "**Свойства**". Откроется окно свойств сетевого подключения. Если для сетевого интерфейса отсутствует протокол TCP/IP, то необходимо выбрать кнопку "**Установить**" (кнопка "**Добавить**" в более ранних версиях ОС Windows) и затем найти нужный протокол и подтвердить сделанный выбор. Протокол будет установлен в операционную систему, которая будет осуществлять поддержку. После включение модулей, реализующих функции протоколов TCP/IP в состав операционной системы семейства ОС Windows, необходимо выполнить настройку протоколов.

Параметры настройки протокола IP

Для настройки протокола IP необходимы следующие три параметра конфигурации: IP–адрес, маска подсети и шлюз по умолчанию.

IP– адрес

IP– адрес – это логический 32–битный адрес, используемый для идентификации TCP/IP– хоста. IP– адрес состоит из двух частей: идентификатора (ID) сети и ID хоста. ID сети (адрес сети) идентифицирует все хосты (самостоятельные машины, либо их сетевые интерфейсы, если машина имеет несколько сетевых адаптеров), которые находятся в одной физической сети. ID хоста (адрес хоста) идентифицирует конкретный хост в сети, а точнее конкретный сетевой интерфейс, имеющий свой собственный IP– адрес. Для выделения адреса сети из IP– адреса используется механизм сетевых масок, изначально предусмотренный стандартом адресации в IP сетях.

Каждый компьютер, имеющий в своем составе хотя бы один сетевой адаптер (сетевой интерфейс) и на котором установлен протокол TCP/IP, должен иметь уникальный IP– адрес. IP– адрес назначается сетевому интерфейсу, так как именно последний выполняет функции передачи и приема данных в/из сети. Одна машина может иметь несколько сетевых интерфейсов и, как результат, несколько IP– адресов. Одному сетевому интерфейсу может быть назначено несколько IP– адресов. В ОС Windows таких адресов на один интерфейс можно назначить не более 5, в других ОС эти ограничения могут быть иными. IP– адрес принято записывать в виде десятичных значений отдельных байтов слева на право, разделяя эти значения друг от друга с помощью точки. Примером IP– адреса является 131.107.2.200.

Сетевая маска (маска подсети)

Сетевая маска представляет собой 32–х битное число, содержащее непрерывную последовательность единиц в разрядах, соответствующих адресу сети. Все остальные разряды маски содержат нулевые значения.

В версии 4 стандарта протокола IP (IP v.4) предусмотрены фиксированные маски, соответствующие трем классам IP– сетей: классов A, B и C. У масок этих классов единицы

содержались в первом – класс A, первом и втором – класс B, первом, втором и третьем байтах – класс C. Соответственно длиной 8, 16 и 24 разряда. Пример корректной маски подсети класса C: 255.255.255.0. Маски для сетей класса A и B соответственно имеют вид – 255.0.0.0 и 255.255.0.0. Использование масок в соответствии с классами приводит к нерациональному расходованию адресов IP, что побудило комитет IETF (Internet Engeniring Task Force) принять стандарт, ко использовать маски подсетей переменной длины – технология VISM (Variable Length Subnet Mask). Эта технология позволила разбивать сети на множество подсетей, не придерживаясь при этом границ, задаваемых классами сетей. Если до введения технологии VLSM для сети в 500 машин требовалось выделение сети класса B, а это немного нимало, сеть на 64534 машины, то с введением VLSM появилась возможность для сети такого размера использовать всего лишь 2 сети класса C, общей емкостью 508 машин. Например, одна сеть класса B может быть разбита на 256 сетей класса C или на 512 подсетей размером по 128 адресов, или на более мелкие сети различной длины в любом сочетании. Ограничение только одно: маска подсети должна иметь непрерывную последовательность единиц в разрядах, соответствующих адресу подсети. С введением стандарта на маски переменной длины сетевые маски стали называть масками подсетей (subnet mask). Вычисление адреса сети выполняется с помощью операции конъюнкции (логическое "И") между IP–адресом и маской подсети.

Шлюз по умолчанию

Протокол IP обеспечивает доставку пакетов в пределах всей составной IP– сети. IP– сеть называется составной, так как предполагается, что отдельные IP– сети объединяются друг с другом с помощью средств сетевого уровня, которые реализуются специальным устройством, называемым шлюзом.

Чтобы обмениваться данными с хостом в другой сети, в таблице маршрутов IP– хоста должен быть указан маршрут к сети назначения. Если такой маршрут в таблице маршрутов хоста отсутствует, то для передачи данных в пункт назначения используется маршрут по умолчанию, который указывает на шлюз. Иными словами, шлюз используется для пересылки IP– пакетов, которые должны быть переданы в удаленные сети. Если шлюз не указан, возможности связи будут ограничены только пределами локальной сети.

Номера записей в таблице маршрутов отмечены полужирным шрифтом. Все записи, показанные в данной маршрутной таблице, создаются автоматически при задании сетевых параметров протокола IP в процессе его настройки.

==========

Активные маршруты:

Сетевой адрес Маска сети Адрес шлюза Интерфейс

1 0.0.0.0 0.0.0.0 192.168.126.254 192.168.126.1

2 127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1

3 192.168.126.0 255.255.255.0 192.168.126.1 192.168.126.1

4 192.168.126.1 255.255.255.255 127.0.0.1 127.0.0.1

5 192.168.126.255 255.255.255.255 192.168.126.1 192.168.126.1

6 255.255.255.255 255.255.255.255 192.168.126.1 192.168.126.1

Основной шлюз: 192.168.126.254

==========

Каждая запись таблицы маршрутов содержит 4 поля (могут быть и другие дополнительные поля):

• "Сетевой адрес" – это адрес пункта назначения;

• "Маска сети" – это сетевая маска, относящаяся к адресу, указанному в поле "сетевой адрес";

• "Адрес шлюза" – это сетевой адрес, по которому необходимо отправить пакет, для того чтобы он достиг адреса пункта назначения;

• "Интерфейс" – это адрес (или имя) сетевого интерфейса, через который доступен шлюз, указанный в поле "адрес шлюза".

Записи 1–3 и 5–6 являются адресами, имеющими специальное назначение, которые в терминологии протокола IP иногда называют "выделенными". Смысл этих записей следующий.

Запись 1 определяет маршрут по умолчанию, указывающий на адрес шлюза по умолчанию. В маршрутных таблицах этот маршрут всегда обозначается как 0.0.0.0 с маской 0.0.0.0.

Запись 2 содержит маршрут на интерфейс "программная петля", который всегда создается при установке протоколов TCP/IP. Он используется для обращения машины к себе самой, имеет адрес

127.0.0.1 и имя localhost.

Запись 3 – это маршрут к сети, в состав которой входит адрес сетевого интерфейса. Отправка пакетов по этому адресу не выполняется, он служит для адресации всей сети в маршрутных таблицах.

Запись 4 – это маршрут на сетевой интерфейс, с помощью которого хост подключается к сети, адрес которой указан в записи 3.

Записи 5 и 6 содержат адреса широковещательной рассылки. Пакеты, посланные по этим адресам, должны быть получены всеми хостами, входящими в сеть, адрес которой указан в записи 3.

При назначении адресов хостам надо помнить, что из всего множества адресов, определяемых маской подсети, два адреса имеют специальное назначение и не могут быть назначены сетевым интерфейсам машин, а именно – собственный адрес сети и широковещательный адрес сети. Все остальные адреса можно назначать сетевым интерфейсам машин.

Предположим, что машина m1 имеет данные, которые необходимо доставить машине c4. У нее есть 2 альтернативы: послать пакет непосредственно в локальную сеть, используя соответствующий протокол канального уровня (в нашем случае - это Ethernet), в случае, если машина получатель входит в ту же сеть, что и машина-отправитель. Либо, если машина получатель не принадлежит к той же сети, что и машина отправитель, то отослать данные шлюзу, соединяющему сеть с внешними сетями. Для того, чтобы определить принадлежность машины-получателя к сети машины-отправителя используется механизм сетевых масок. В нашем случае адрес получателя – 192.168.127.4, а маска подсети на сетевом интерфейсе – 255.255.255.0. В результате выполнения операции конъюнкции будет получен результат: 192.168.127.0 – это адрес сети назначения. Далее модуль, реализующий функции протокола IP на машине m1, выполнит просмотр маршрутной таблицы с целью поиска маршрута к сети назначения, и так как такого маршрута нет, то данные будут направлены шлюзу по адресу 192.168.126.254. В свою очередь, сеть назначения непосредственно подключена к одному из сетевых интерфейсов шлюза, поэтому в маршрутной таблице шлюза будет иметься запись о сети 192.168.127.0, что позволит ему доставить данные по адресу назначения.

Введение технологии VLSM потребовало создания технологии обработки масок переменной длины в маршрутных таблицах. Эта технология получила название бесклассовой междоменной маршрутизации (CIDR – Classless InterDomain Routing). В соответствии с этой технологией маршруты стали записывать в виде префиксов, которые представляют собой адрес сети с указанием через знак "/" числа разрядов маски, установленных в 1. Например, для классической сети класса C префикс будет иметь вид:

192.168.1.0/24, где 192.168.1.0 – адрес сети, а /24 соответствует маске 255.255.255.0.

При наличии в маршрутной таблице двух префиксов, относящихся к одной и той же сети, будет считаться префикс, маска которого имеет большее количество единиц. Это правило получило название "правила выбора более точного маршрута", так как маска с большим числом единиц указывает на сеть меньшего размера, а значит, более точно описывает разбиение адресного пространства на подсети. Еще одним результатом введения технологии CIDR явилось появление возможности объявлять объединенные маршруты, т.е. маршруты на смежные сети, объединенные с помощью "коротких" префиксов, имеющих небольшое количество единиц в соответствующих им масках подсетей. Введение технологий VLSM и CIDR, совместно с введением института локальных регистраторов (Local Registry), позволило значительно замедлить процесс исчерпания IP– адресов, а также значительно снизить размеры маршрутных таблиц магистральных маршрутизаторов Интернет

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

1. Изменение параметров настройки протокола IP.

1.1 Подключиться к виртуальной машине Windows XP. Перейти в окно конфигурирования сетевых подключений: открыть окно "Сетевые подключения": Пуск/Настройка/Сетевые подключения. Кликнуть правой клавишей мыши по значку "подключение по локальной сети" и выбрать пункт "Свойства".

1.2 В появившемся окне выберите сетевой адаптер, затем "Свойства", затем Протокол Интернета (TCP/IP) и его свойства.

1.3 Запишите значения сетевых параметров, установленных на Вашей машине:

− IP– адреса;
− Сетевой маски;
− Адреса шлюза по умолчанию;
− Адреса 1– го и 2– го серверов DNS (если они установлены).
Занесите значения этих параметров в отчет.
1.4 Удалите протокол NetBUI, если он установлен на Вашей машине.
1.5 Установите сетевые параметры протокола IP в соответствии с
таблицей 2. Таблица 2. Сетевые параметры протокола IP
IP– адрес** Сетевая маска Шлюз
192.168.20Y.G+XX 255.255.0.0 Использовать значение, которое было
установлено ранее, либо значение,
указанное преподавателем.
Где Y, G, XX – десятичные числа;
Y – год поступления (одна цифра 0-9).
G = номер группы. 00 – для группы УИР-1; 50 – для группы УИР-2; 100 – для группы УИР-3.
XX = – порядковый номер студента в группе.
Пример. Студент номер 21 (по журналу); группы УИР-2; год поступления 2003.
XX=21; G=50; Y=3.
Получим сетевой адрес машины: 192.168.203.71
Где 203 = 200+3
71 = 50+21.
1.6 Если в результате изменения параметров настройки протокола IP будет выдано сообщение о необходимости перезагрузки, ни в коем случае не делайте этого, просто откажитесь.
1.7 Открыть консоль системы (соответствующая процедура описана в приложении 2). В командной строке выполнить команду:
> ipconfig /all
Сохраните результат выполнения этой команды в отчете.
1.8 В командной строке консоли выполните команду:
> ping <адрес_шлюза>
Результаты занесите в файл отчета.
2. Оформление отчета по результатам выполнения практической
работы.

Контрольные вопросы:

1. Имеется сеть с IP = 192.168.55.0 и требуется разбить ее на ряд подсетей. Необходимо, чтобы в каждой подсети можно было использовать по 25 хостов. Какую маску необходимо применить в таком случае, чтобы обеспечить максимально возможное число таких подсетей?
A 255.255.255.192; B. 255.255.255.224; C. 255.255.255.240;
D 255.255.255.248.
2. У вас имеется маска 255.255.255.252. Какое значение имеет префикс?
A. /16; B. /24; C. /30, D. /32
3. Если имеется IP– адрес 172.16.10.5/25, то какой широковещательный адрес должен использовать этот хост?
A. 255.255.255.255; B. 172.16.10.127; C. 172.16.10.255;
D. 172.16.10.128.
4. Сколько машин позволяет иметь в подсети маска 255.255.255.252?
A. 16384; B. 2; C. 4094; D. 6.
5. Каков диапазон допустимых адресов машин для подсети 172.16.10.5/26?
A. с 172.16,10.1 по 172.16.10.30; B. с l72.16.10.1 по l72.16.10.31;
C. с 172.16.10.1 по 172.16.10.62; D. с 172.16.10.1 по 172.16.10.63.
6. Если вы хотите объединить в подсеть машины с адресами с 192.168.10.64 по 192.168.10.127, то какими будут адрес и маска подсети?
A. 192.168.10.64 255.255.255.192; B. 192.168.10.0 255.255.255.192;
C. 192.168.10.64 255.255.255.224; D. 192.168.10.0 255.255.255.224.

7. Назовите основное назначение и возможности технологии применения масок переменной длины (VLSM).

8. Назовите основное назначение и возможности технологии бесклассовой междоменной маршрутизации (CIDR).

9. Объясните основные функции, выполняемые шлюзом в коммуникационной схеме протокола IP.

10. Каким образом, машины, работающие в IP сети, определяют, когда пакет необходимо доставить шлюзу, а в каком случае доставка выполняется непосредственно с помощью протоколов канального уровня?

Практическая работа №7
Работа с диагностическими утилитами протокола TCP/IP

Цель: обобщение и систематизация знаний по теме «Межсетевое взаимодействие»
Оборудование: ПК, MS Windows, виртуальная машина VM-1, IP-адрес, маска подсети, основной шлюз, предпочитаемый DNS;
Время выполнения: 90 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Диагностические утилиты TCP/IP

В состав TCP/IP входят диагностические утилиты, предназначенные для проверки конфигурации стека и тестирования сетевого соединения.

Утилита:	**Применение:**
arp	Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP- адресу)
hostname	Выводит имя локального хоста. Используется без параметров.
ipconfig	Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System)
nbtstat	Выводит статистику и текущую информацию по NetBIOS, установленному поверх TCP/IP. Используется для проверки состояния текущих соединений NetBIOS.
netstat	Выводит статистику и текущую информацию по соединению TCP/IP.
nslookup	Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS.
ping	Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом.
route	Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP.
tracert	Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо- пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер.

Проверка правильности конфигурации TCP/IP

При устранении неисправностей и проблем в сети TCP/IP следует сначала проверить правильность конфигурации TCP/IP. Для этого используется утилита ipconfig.

Эта команда полезна на компьютерах, работающих с DHCP (Dynamic Host Configuration Protocol), так как дает пользователям возможность определить, какая конфигурация сети TCP/IP и какие величины были установлены с помощью DHCP.

Синтаксис:

ipconfig [/all | /renew[adapter] | /release]

Параметры:

all - выдает весь список параметров. Без этого ключа отображается только IP-адрес, маска и шлюз по умолчанию;

renew[adapter] - обновляет параметры конфигурации DHCP для указанного сетевого адаптера;

release[adapter] - освобождает выделенный DHCP IP-адрес;

adapter - имя сетевого адаптера;

displaydns - выводит информацию о содержимом локального КЭШа клиента DNS, используемого для разрешения доменных имен.

Таким образом, утилита ipconfig позволяет выяснить, инициализирована ли конфигурация и не дублируются ли IP- адреса:

- если конфигурация инициализирована, то появляется IP- адрес, маска, шлюз;
- если IP-адреса дублируются, то маска сети будет 0.0.0.0;
- если при использовании DHCP компьютер не смог получить IP-адрес, то он будет равен 0.0.0.0 .

Тестирование связи с использованием утилиты ping

Утилита ping (Packet Internet Grouper) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста. Использование ping лучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.

Команда ping проверяет соединение с удаленным хостом путем посылки к этому хосту эхо-пакетов ICMP и прослушивания эхо-ответов. Ping ожидает каждый посланный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно.

По умолчанию передается 4 эхо-пакета длиной 32 байта (периодическая последовательность символов алфавита в верхнем регистре). Ping позволяет изменить размер и количество пакетов, указать, следует ли записывать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д.. При получении ответа в поле time указывается, за какое время (в миллисекундах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд. Если вы получаете сообщение «Request time out» (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа –w.

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если ping с IP- адресом выполнилась успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

Использование утилиты ping:

- Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде ping задается адрес петли обратной связи (loopback address):

ping 127.0.0.1

Если тест успешно пройден, то вы получите следующий ответ:

Reply from 127.0.0.1
Reply from 127.0.0.1
Reply from 127.0.0.1
Reply from 127.0.0.1

- Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, используется IP- адрес локального компьютера:

ping IP-адрес_локального_хоста

- Чтобы проверить, что шлюз по умолчанию функционирует и что можно установить соединение с любым локальным хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

ping IP-адрес_шлюза

- Для проверки возможности установления соединения через маршрутизатор в команде ping задается IP-адрес удаленного хоста:

ping IP-адрес_удаленного хоста

Синтаксис утилиты ping:

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list

Параметры:

-t - выполняет команду ping до прерывания. Control- Break - посмотреть статистику и продолжить. Control-C - прервать выполнение команды;

-a - позволяет определить доменное имя удаленного компьютера по его IP-адресу;

-n count - посылает количество пакетов ECHO, указанное параметром count;

-l length - посылает пакеты длиной length байт (максимальная длина 8192 байта);

-f - посылает пакет с установленным флагом «не фрагментировать». Этот пакет не будет фрагментироваться на маршрутизаторах по пути своего следования;

-i ttl - устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);

-v tos - устанавливает тип поля «сервис» в величину tos;

-r count - записывает путь выходящего пакета и возвращающегося пакета в поле записи пути. Count - от 1 до 9 хостов;

-s count - позволяет ограничить количество переходов из одной подсети в другую (хопов). Count задает максимально возможное количество хопов;

-j host-list - направляет пакеты с помощью списка хостов, определенного параметром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая маршрутизация). Максимальное количество хостов в списке, позволенное IP, равно 9;

-k host-list - направляет пакеты через список хостов, определенный в host-list. Последовательные хосты не могут быть разделены промежуточными маршрутизаторами (жесткая статическая маршрутизация). Максимальное количество хостов – 9;

-w timeout - указывает время ожидания (timeout) ответа от удаленного хоста в миллисекундах (по умолчанию – 1сек);

destination-list - указывает удаленный хост, к которому надо направить пакеты ping.

Пример использования утилиты ping: C:\Documents and Settings\user>ping www.ya.ru

Обмен пакетами с ya.ru [213.180.204.8] по 32 байт:

Ответ от 213.180.204.8: число байт=32 время=1887мс TTL=53
Ответ от 213.180.204.8: число байт=32 время=1475мс TTL=53
Ответ от 213.180.204.8: число байт=32 время=1094мс TTL=53
Ответ от 213.180.204.8: число байт=32 время=736мс TTL=53

Статистика Ping для 213.180.204.8:
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
Минимальное = 736мсек, Максимальное = 1887 мсек, Среднее = 1298 мсек

ние маршрута между сетевыми соединениями с помощью утилиты tracert

Tracert - это утилита трассировки маршрута. Она использует поле TTL (time-to-live, время жизни) пакета IP и сообщения об ошибках ICMP для определения маршрута от одного хоста до

другого.

Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим. С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа «Destination net unreachable», «Destination host unreachable», «Request time out», «Time Exeeded».

Утилита tracert работает следующим образом: посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP “Time Exeeded” (Время истекло). Маршрут определяется путем посылки первого эхо- пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Примечание: некоторые маршрутизаторы просто молча уничтожают пакеты с истекшим TTL и не будут видны утилите tracert.

Синтаксис:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] имя_целевого_хоста

Параметры:

-d - указывает, что не нужно распознавать адреса для имен хостов;

-h maximum_hops - указывает максимальное число хопов для того, чтобы искать цель;

-j host-list - указывает нежесткую статическую маршрутизацию в соответствии с host-list;

-w timeout - указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек.

Пример использования утилиты tracert: C:\Documents and Settings\user>tracert www.ya.ru

Трассировка маршрута к ya.ru [213.180.204.8]
с максимальным числом прыжков 30:

1 <1 мс <1 мс <1 мс mygateway1.ar7 [192.168.1.1]
2 16 ms 15 ms 23 ms 192.168.229.9
3 16 ms 16 ms 16 ms 192.168.224.46

4 * * * Превышен интервал ожидания для запроса.
5 * * * Превышен интервал ожидания для запроса.
6 24 ms 24 ms 25 ms 18.224.168.192.in-addr.arpa
[192.168.224.18]
7 23 ms 23 ms 23 ms 17.224.168.192.in-addr.arpa
[192.168.224.17]
8 2542 ms 2577 ms 2928 ms
18.13.22.172.in-addr.arpa [172.22.13.18]
9 2189 ms 1811 ms 2016 ms
225.126.18.84.in-addr.arpa [84.18.126.225]
10 2354 ms 2193 ms 1653 ms
87.226.230.253
11 1442 ms 1361 ms 1105 ms
87.226.133.38
12 56 ms 55 ms 68 ms 87.226.233.198
13 1715 ms 2206 ms 2579 ms www.ya.ru
[213.180.204.8]

Трассировка завершена

Утилита ARP

Основная задача протокола ARP – трансляция IP-адресов в соответствующие локальные адреса (MAC-адреса). Для этого ARP-протокол использует информацию из ARP-таблицы (ARP-кэша). Если необходимая запись в таблице не найдена, то протокол ARP отправляет широковещательный запрос ко всем компьютерам локальной подсети, пытаясь найти владельца данного IP-адреса. В кэше могут содержаться два типа записей: статические и динамические. Статические записи вводятся вручную и хранятся в кэше постоянно. Динамические записи помещаются в кэш в результате выполнения широковещательных запросов. Для них существует понятие времени жизни. Если в течение определенного времени (по умолчанию 2 мин.) запись не была востребована, то она удаляется из кэша.
Синтаксис:
адреса;

arp [-s inet_addr eth_addr] | [-d inet_addr] | [-a]
Параметры:
-s - занесение в кэш статических записей;
-d - удаление из кэша записи для определенного IP-

-a - просмотр содержимого кэша для всех сетевых

адаптеров локального компьютера; *inet_addr* - IP-адрес; *eth_addr* - MAC-адрес.

Пример использования утилиты ARP: C:\Documents and Settings\user>arp -a 169.254.15.2
Интерфейс: 169.254.15.1 --- 0x2
Адрес IP Физический адрес Тип 169.254.15.2 00-19-5b-82-fb-d0 динамический

Утилита netstat

Утилита netstat позволяет получить статическую информацию по некоторым из протоколов стека (TCP, UDP, IP, ICMP), а также выводит сведения о текущих сетевых соединениях. Особенно она полезна на брандмауэрах, с ее помощью можно обнаружить нарушения безопасности периметра сети.
Синтаксис:
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r]
Параметры:

-a - выводит перечень всех сетевых соединений и прослушивающихся портов локального компьютера;

-e - выводит статистику для Ethernet-интерфейсов (например, количество полученных и отправленных байт);

-n - выводит информацию по всем текущим соединениям (например, TCP) для всех сетевых интерфейсов локального компьютера. Для каждого соединения выводится информация об IP-адресах локального и удаленного интерфейсов вместе с номерами используемых портов;

-s - выводит статистическую информацию для протоколов UDP, TCP, ICMP, IP. Ключ «/more» позволяет

просмотреть информацию постранично;
-r - выводит содержимое таблицы маршрутизации.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

1. Получение справочной информации по командам

Выведите на экран справочную информацию по утилитам *ipconfig*, *ping*, *tracert*, *hostname*. Для этого в командной строке введите имя утилиты без параметров или с /?. Изучите ключи, используемые при запуске утилит.

2. Получение имеени хоста

Выведите на экран имя локального хоста с помощью команды *hostname*.

3. Изучение утилиты ipconfig

Проверьте конфигурацию TCP/IP с помощью утилиты *ipconfig*. Заполните таблицу:

Имя хоста	
IP-адрес	
Маска подсети	
Основной шлюз	
Используется ли DHCP (адрес DHCP-сервера)	
Описание адаптера	
Физический адрес сетевого адаптера	
Адрес DNS-сервера	
Адрес WINS-сервера	

4. Тестирование связи с помощью утилиты ping

- Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
- Проверьте, правильно ли добавлен в сеть локальный компьютер и не дублируется ли IP-адрес.
- Проверьте функционирование шлюза по умолчанию, послав 5 эхо-пакетов длиной 64 байта.
- Проверьте возможность установления соединения с удаленным хостом (например www.yandex.ru)

5. Определение пути IP-пакета

С помощью команды *tracert* проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Отметьте их:

192.168.0.1:
10.70.0.3:
10.70.1.1:
www.ineka.ru

6: Просмотр ARP-кэша

С помощью утилиты *arp* просмотрите ARP-таблицу локального компьютера.

7. Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

С помощью утилиты *netstat* выведите перечень сетевых соединений и статистическую информацию для протоколов UDP, TCP, ICMP, IP.

Контрольные вопросы:

- Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?
- Каким образом команда ping проверяет соединение с удаленным хостом?
- Что такое хост?
- Что такое петля обратной связи?
- Сколько промежуточных маршрутизаторов сможет пройти IP-пакет, если его время жизни равно 30?
- Как работает утилита tracert?
- Каково назначение протокола ARP?

Практическая работа №8
Решение проблем с TCP/IP

Цель: обобщение и систематизация знаний по теме «Межсетевое взаимодействие»
Оборудование: ПК, MS Windows
Время выполнения: 90 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

TCP/IP - это аббревиатура термина Transmission Control Protocol/Internet Protocol (Протокол управления передачей/Протокол Internet). В терминологии вычислительных сетей протокол - это заранее согласованный стандарт, который позволяет двум компьютерам обмениваться данными. Фактически TCP/IP не один протокол, а несколько. Именно поэтому вы часто слышите, как его называют набором, или комплектом протоколов, среди которых TCP и IP - два основных.

Программное обеспечение для TCP/IP, на вашем компьютере, представляет собой специфичную для данной платформы реализацию TCP, IP и других членов семейства TCP/IP. Обычно в нем также имеются такие высокоуровневые прикладные программы, как FTP (File Transfer Protocol, Протокол передачи файлов), которые дают возможность через командную строку управлять обменом файлами по Сети.

TCP/IP - зародился в результате исследований, профинансированных Управлением перспективных научно-исследовательских разработок (Advanced Research Project Agency, ARPA) правительства США в 1970-х годах. Этот протокол был разработан с тем, чтобы вычислительные сети исследовательских центров во всем мире могли быть объединены в форме виртуальной "сети сетей" (internetwork). Первоначальная Internet была создана в результате преобразования существующего конгломерата вычислительных сетей, носивших название ARPAnet, с помощью TCP/IP.

Причина, по которой TCP/IP столь важен сегодня, заключается в том, что он позволяет самостоятельным сетям подключаться к Internet или объединяться для создания частных интрасетей. Вычислительные сети, составляющие интрасеть, физически подключаются через устройства, называемые маршрутизаторами или IP-маршрутизаторами. Маршрутизатор - это компьютер, который передает пакеты данных из одной сети в другую. В интрасети, работающей на основе TCP/IP, информация передается в виде дискретных блоков, называемых IP-пакетами (IP packets) или IP-дейтаграммами (IP datagrams). Благодаря программному обеспечению TCP/IP все компьютеры, подключенные к вычислительной сети, становятся "близкими родственниками". По существу оно скрывает маршрутизаторы и базовую архитектуру сетей и делает так, что все это выглядит как одна большая сеть. Точно так же, как подключения к сети Ethernet распознаются по 48-разрядным идентификаторам Ethernet, подключения к интрасети идентифицируются 32-разрядными IP-адресами, которые мы выражаем в форме десятичных чисел, разделенных точками (например, 128.10.2.3). Взяв IP-адрес удаленного компьютера, компьютер в интрасети или в Internet может отправить данные на него, как будто они составляют часть одной и той же физической сети.

TCP/IP дает решение проблемы данными между двумя компьютерами, подключенными к одной и той же интрасети, но принадлежащими различным физическим сетям. Решение состоит из нескольких частей, причем каждый член семейства протоколов TCP/IP вносит свою лепту в общее дело. IP - самый фундаментальный протокол из комплекта TCP/IP - передает IP-дейтаграммы по интрасети и выполняет важную функцию, называемую маршрутизацией, по сути дела это выбор маршрута, по которому дейтаграмма будет следовать из пункта A в пункт B, и использование маршрутизаторов для "прыжков" между сетями.

TCP - это протокол более высокого уровня, который позволяет прикладным программам, запущенным на различных главных компьютерах сети, обмениваться потоками данных. TCP делит потоки данных на цепочки, которые называются TCP-сегментами, и передает их с помощью IP. В большинстве случаев каждый TCP-сегмент пересылается в одной IP-дейтаграмме. Однако при необходимости TCP будет расщеплять сегменты на несколько IP-дейтаграмм, вмещающихся в физические кадры данных, которые используют для передачи информации между компьютерами в сети. Поскольку IP не гарантирует, что дейтаграммы будут получены в той же самой

последовательности, в которой они были посланы, TCP осуществляет повторную "сборку" TCP-сегментов на другом конце маршрута, чтобы образовать непрерывный поток данных. FTP и telnet - это два примера популярных прикладных программ TCP/IP, которые опираются на использование TCP.

Другой важный член комплекта TCP/IP - User Datagram Protocol (UDP, протокол пользовательских дейтаграмм), который похож на TCP, но более примитивен. TCP - "надежный" протокол, потому что он обеспечивает проверку на наличие ошибок и обмен подтверждающими сообщениями чтобы данные достигали своего места назначения заведомо без искажений. UDP - "ненадежный" протокол, ибо не гарантирует, что дейтаграммы будут приходить в том порядке, в котором были посланы, и даже того, что они придут вообще. Если надежность - желательное условие, для его реализации потребуется программное обеспечение. Но UDP по-прежнему занимает свое место в мире TCP/IP, и испльзуется во многих программах. Прикладная программа SNMP (Simple Network Management Protocol, простой протокол управления сетями), реализуемый во многих воплощениях TCP/IP, - это один из примеров программ UDP.

Другие TCP/IP протоколы играют менее заметные, но в равной степени важные роли в работе сетей TCP/IP. Например, протокол определения адресов (Address Resolution Protocol, ARP) ппреобразует IP-адреса в физические сетевые адреса, такие, как идентификаторы Ethernet. Родственный протокол - протокол обратного преобразования адресов (Reverse Address Resolution Protocol, RARP) - выполняет обеспечивает обратное действие, преобразуя физические сетевые адреса в IP-адреса. Протокол управления сообщениями Internet (Internet Control Message Protocol, ICMP) представляет собой протокол сопровождения, который использует IP для обмена управляющей информацией и контроля над ошибками, относящимися к передаче пакетов IP. Например, если маршрутизатор не может передать IP-дейтаграмму, он использует ICMP, с тем чтобы информировать отправителя, что возникла проблема. Краткое описание некоторых других протоколов, которые "прячутся под зонтиком" TCP/IP, приведено во врезке.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

1. Открыть окно командной строки, ввести команду ping с IP адресом машины, при взаимодействии с которой возникают проблемы. Определить, использует ли проблемная машина конфигурацию статичного или динамичного IP адреса. Для этого откройте панель управления и выберите опцию Сетевые подключения. Теперь правой клавишей нажмите на подключении, которое собираетесь диагностировать, затем выберите опцию Свойства в появившемся меню быстрого доступа.
2. Перейдите по спискам элементов, используемых подключением, пока не дойдете до TCP/IP протокола (выбран на рисунке 3). Выберите этот протокол, нажмите на кнопке Свойства, чтобы открыть страницу свойств для Internet Protocol (TCP/IP).
3. Запишите IP конфигурацию машины. Особенно важно сделать заметки следующих элементов:
   1. Использует ли машина статичную или динамичную конфигурацию?
   2. Если используется статичная конфигурация, запишите значение IP адреса, маски подсети и основного шлюза?
   3. Получает ли машина адрес DNS сервера автоматически?
   4. Если адрес DNS сервера вводится вручную, то какой адрес используется?
4. Если на компьютере установлено несколько сетевых адаптеров, то в панели управления будут перечислены несколько сетевых подключений.
5. Проверьте тип адаптера.
6. Определите, принимает ли Windows такую конфигурацию. Для этого откройте окно командной строки и введите следующую команду: IPCONFIG /ALL.
7. Определите правильный сетевой адаптер. В этом случае определение нужного адаптера довольно простое, поскольку в списке есть всего лишь один адаптер.
8. Отправьте ping запрос на адрес локального узла. Существует два различных способа того, как это сделать. Одним способом является ввод команды: PING LOCALHOST.
9. Введите команду Nslookup, за которой должно идти полное доменное имя удаленного узла. Команда Nslookup должна суметь разрешить полное доменное имя в IP адрес.
10. Необходимо просканировать клиентскую машину на предмет вредоносного ПО. Если на машине

не обнаружено вредоносного ПО, сбросьте DNS кэш путем ввода следующей команды: IPCONFIG /FLUSHDNS.

Контрольные вопросы:

1. Поясните, что может означать, если время TTL закончилось до получения ответа.
2. Как подтвердить наличие сетевого соединения?
3. Что показывает команда IPCONFIG /ALL?
4. Что означает наличие IP адрес со значением 0.0.0.0.?
5. С помощью какой команды можно проверить то, что конфигурация IP адреса работает корректно, и что отсутствуют проблемы с стеком локального протокола TCP/IP?
6. Как производится опрос основного шлюза?
7. Как производится опрос DNS сервера?

Практическая работа №9
Преобразование форматов IP-адресов. Расчет IP-адреса и маски подсети

Цель работы: определение класса и расчет IP-адреса и маски подсети
Оборудование: ПК,
Время выполнения: 90 минут.

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

IP-адрес представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемых *октетами*.

Наиболее распространенной формой представления IP-адреса является запись в виде че- тырех чисел, представляющих значения каждого байта в *десятичной форме* и разделенных точками, например: 128.10.2.30

Этот же адрес может быть представлен в *двоичном формате*: 10000000 00001010 00000010 00011110.

А также в *шестнадцатеричном формате*: 80.0A.02.1D

Следует заметить, что максимальное значение октета равно 11111111 (двоичная система счисления), что соответствует в десятичной системе 255.

Поэтому IP-адреса, в которых хотя бы один октет превышает это число, являются недействительными. Пример: 172.16.123.1 – действительный адрес, 172.16.123.256 – несуществующий адрес, поскольку 256 выходит за пределы допустимого диапазона.

IP-адрес состоит из двух логических частей – ***номера подсети (ID подсети)*** и ***номера узла (ID хоста)*** в этой подсети. При передаче пакета из одной подсети в другую используется ID подсети. Когда пакет попал в подсеть назначения, ID хоста указывает на конкретный узел в рамках этой подсети.

Чтобы записать ID подсети, в поле номера узла в IP-адресе ставят нули. Чтобы записать ID хоста, в поле номера подсети ставят нули. Например, если в IP-адресе 172.16.123.1 первые два байта отводятся под номер подсети, остальные два байта – под номер узла, то номера записываются следующим образом:

ID подсети: 172.16.0.0.

ID хоста: 0.0.123.1.

По числу разрядов, отводимых для представления номера узла (или номера подсети), можно определить общее количество узлов (или подсетей) по простому правилу: если число разрядов для представления номера узла равно N, то общее количество узлов равно 2N – 2. Два узла вычитаются вследствие того, что адреса со всеми разрядами, равными нулям или единицам, являются особыми и используются в специальных целях.

Например, если под номер узла в некоторой подсети отводится два байта (16 бит), то общее количество узлов в такой подсети равно 216 – 2 = 65534 узла.

Для определения того, какая часть IP-адреса отвечает за ID подсети, а какая за ID хоста, применяются два способа:

- с помощью классов

- с помощью масок.

Общее правило: под ID подсети отводятся *первые* несколько бит IP-адреса, оставшиеся биты обозначают ID хоста.

Признаком, на основании которого IP-адрес относят к тому или иному классу, являются значения нескольких первых битов адреса.

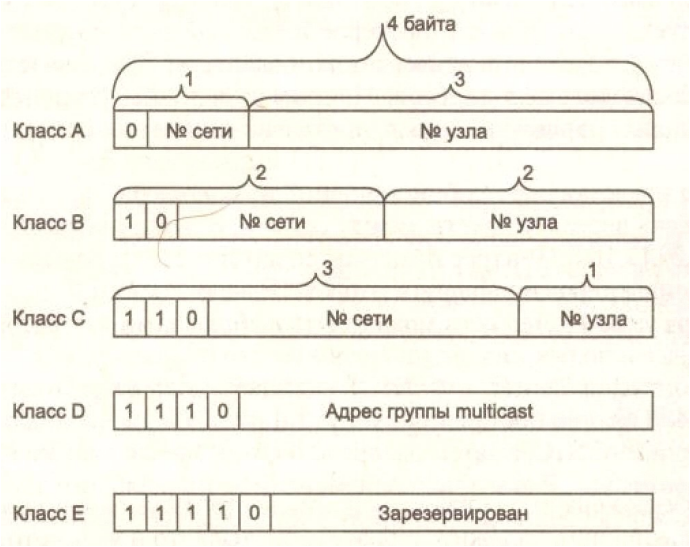


Таблица - Классы IP-адресов

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Количество сетей	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	126	$2^{24} - 2 = 16777214$
B	10	128.0.0.0	191.255.0.0	16384	$2^{16} - 2 = 65534$
C	110	192.0.1.0	223.255.255.0	2097152	$2^{8} - 2 = 254$
D	1110	224.0.0.0	239.255.255.255	Групповой адрес	
E	11110	240.0.0.0	247.255.255.255	Зарезервирован	

Адреса ***класса A*** предназначены для использования в больших сетях общего пользования.

Они допускают большое количество номеров узлов.

Адреса ***класса B*** используются в сетях среднего размера, например, сетях университетов и крупных компаний.

Адреса класса C используются в сетях с небольшим числом компьютеров.

Адреса класса D используются при обращениях к группам машин.

Адреса класса E зарезервированы на будущее.

Некоторые IP-адреса являются особыми, они не должны применяться для идентификации обычных сетей:

- Если все биты IP-адреса равны нулю, адрес обозначает узел- отправитель и используется в некоторых сообщениях ICMP.
- Если все биты ID сети равны 1, адрес называется *ограниченным широковещательным (limited broadcast)*, пакеты, направленные по такому адресу, рассылаются всем узлам той подсети, в которой находится отправитель пакета.
- Если все биты ID хоста равны 1, адрес называется *широковещательным (broadcast)*, пакеты, имеющие широковещательный адрес, доставляются всем узлам подсети назначения.
- Если все биты ID хоста равны 0, адрес считается идентификатором подсети (subnet ID).

Особый смысл имеет IP-адрес, первый октет которого равен 127. Этот адрес является *внутренним адресом стека протоколов* компьютера (или маршрутизатора). Он используется для тестирования программ, а также для организации работы клиентской и серверной частей приложения, установленных на одном компьютере. Обе программные части данного приложения спроектированы в расчете на то, что они будут обмениваться сообщениями по сети. В IP-сети запрещается присваивать сетевым интерфейсам IP-адреса, начинающиеся со значения 127. Когда

программа посылает данные по IP-адресу 127.x.x.x, то данные не передаются в сеть, а возвращаются модулям верхнего уровня того же компьютера, как только что принятые. Маршрут перемещения данных образует «петлю», поэтому этот адрес называется *адресом обратной петли* (loopback).

Форма *группового IP-адреса* - *multicast* - означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Групповой адрес не делится на номера сети и узла и обрабатывается маршрутизатором особым образом. Основное назначение групповых адресов распространение информации по схеме «один ко многим». Основное назначение multicast-адресов - распространение информации по схеме “один-ко-многим”. Хост, который хочет передавать одну и ту же информацию многим абонентам, с помощью специального протокола IGMP (Internet Group Manageme Protocol) сообщает о создании в сети новой мультивещательной группы с определенным адресом. Машрутизаторы, поддерживающие мультивещательность, распространяют информацию о создании новой группы в сетях, подключенных к портам этого маршрутизатора. Хосты, которые хотят присоединиться к вновь создаваемой мультивещательной группе, сообщают об этом своим локальным маршрутизаторам и те передают эту информацию хосту, инициатору создания новой группы. Групповая адресация предназначена для экономичного распространения в Internet или большой корпоративной сети аудио- или видеопрограмм, предназначенных сразу большой аудитории слушателей или зрителей.

Маска - число, которое служит для выделения частей IP-адреса, чтобы TCP/IP мог отличать номер сети от номера хоста. Используя маску подсети, TCP/IP-хосты могут связаться и определить, где находится хост назначения: в локальной или удаленной сети. Пример маски подсети: 255.255.255.0.

Биты IP-адреса, определяющие номер IP-сети, в маске подсети должны быть равны 1, а биты, определяющие номер узла, в маске подсети должны быть равны 0. Для стандартных классов сетей маски имеют следующие значения:

-класс A - 11111111. 00000000. 00000000. 00000000 (255.0.0.0);

-класс B - 11111111.11111111. 00000000. 00000000 (255.255.0.0);

-класс C-11111111.11111111.11111111. 00000000 (255.255.255.0).

Маски подсетей могут использоваться для маскирования тех частей адреса, которые согласно структуре класса, определяются как адреса сети. На практике разделение на подсети применяется в случае, когда конкретное сетевое адресное пространство разбивается дальше на отдельные подсети.

Подсети являются удобным средством структуризации сетей в рамках одной организации, когда все адресное пространство сети internet может быть разделено на непересекающиеся подпространства - "*подсети*", с каждой из которых можно работать как с обычной сетью TCP/IP. Таким образом единая IP-сеть организации может строиться как объединение подсетей. При этом организация должна получить один сетевой номер.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

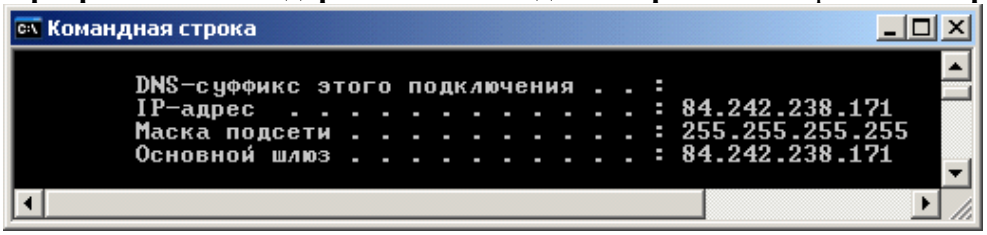
Задание 1. Изучить теоретические основы IP-адресации

- Сколько октетов в IP — адресе?
- Сколько битов в октете?
- Сколько бит в маске подсети?

Задание 2. Определить IP адрес вашего ПК

Узнайте собственный *IP адрес* компьютера и определите, к какому классу он относится.

Узнать свой собственный *IP адрес* вы можете, если запустите в ОС *Windows* XP на выполнение команду **Пуск – Программы – Стандартные – Командная Строка** и наберете в ней **ipconfig** .



Задание 3. Переведите следующие двоичные числа в десятичные, а десятичные в двоичные.

Двоичное значение	Десятичное значение		Десятичное значение	Двоичное значение
10101100.00101000.00000000.00000000			127.1.1.1	
01011110.01110111.10011111.00000000			109.128.255.254	
10010001.0110000.10000000.00011001			131.107.2.89	
01111111.00000000.00000000.00000001			129.46.78.0	

Задание 4. Определение частей IP- адресов.

Заполнить таблицу об идентификации различных классов IP-адресов.

IP- адреса хостов	Класс адреса	Адрес сети	Адреса хостов	Широковещательный (broadcast) адрес	Маска подсети по умолчанию
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.244					

Задание 5. Дан IP- адрес 142.226.0.15

- Чему равен двоичный эквивалент второго октета?
- Какому классу принадлежит этот адрес?
- Чему равен адрес сети, в которой находится хост с этим адресом?
- Является ли этот адрес хоста допустимым в классической схеме адресации?

Задание 6

Найти адрес сети, минимальный IP, максимальный IP и число хостов по IP-адресу и маске сети: IP-адрес: 192.168.215.89

Маска: 255.255.255.0

Задание 7

Найти маску сети, минимальный IP, максимальный IP по IP-адресу и адресу сети: IP-адрес: 124.165.101.45

Сеть: 124.128.0.0

Задание 8

Найти минимальный IP, максимальный IP по адресу сети и маске: Маска: 255.255.192.0

Сеть: 92.151.0.0

Задание 9. Определите, какие IP-адреса не могут быть назначены узлам. Объясните, почему такие IP-адреса не являются корректными.

1. 131.107.256.80
2. 222.222.255.222
3. 31.200.1.1
4. 126.1.0.0
5. 190.7.2.0
6. 127.1.1.1
7. 198.121.254.255
8. 255.255.255.255

Контрольные вопросы:

1. Какие октеты представляют идентификатор сети и узла в адресах классов A, B и C?
2. Какие значения не могут быть использованы в качестве идентификаторов сетей и почему?
3.Какие значения не могут быть использованы в качестве идентификаторов узлов? Почему?
4. Когда необходим уникальный идентификатор сети?
5. Каким компонентам сетевого окружения TCP/IP, кроме компьютеров, необходим идентификатор узла?

Практическая работа №10
Монтаж кабельных сред технологий Ethernet

Цель работы:Изучить основные этапы монтажа кабельных систем Ethernet.Отработать навыки монтажа сети на основе витой пары.

Оборудование: ПК, клещи обжимные, тестер кабеля, зачистной нож, UTP-кабель.

Время выполнения: 90 минут.

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

В качестве средств коммуникации наиболее часто используются витая пара, коаксиальный кабель и оптоволоконные линии. При выборе типа кабеля учитывают следующие показатели:

- Стоимость монтажа и обслуживания;
- Скорость передачи информации;
- Ограничения на величину расстояния передачи информации (без дополнительных усилителей–повторителей (репитеров));
- Безопасность передачи данных.

Главная проблема заключается в одновременном обеспечении этих показателей, например, наивысшая скорость передачи данных ограничена максимально возможным расстоянием передачи данных, при котором еще обеспечивается требуемый уровень защиты данных. Легкая наращиваемость и простота расширения кабельной системы влияют на ее стоимость и безопасность передачи данных.

Сетевые устройства

Сетевые карты отвечают за передачу информации между единицами сети. Любая сетевая карта состоит из разъема для сетевого проводника и микропроцессора, что кодирует/декодирует сетевые пакеты, а также вспомогательных программно-аппаратных комплексов и служб. Каждая карта имеет свой MAC-адрес – уникальный идентификатор устройства.

Коаксильный кабель

Коаксиальный кабель имеет среднюю цену, хорошо помехозащищен и применяется для связи на большие расстояния (несколько километров).

Рисунок 1 – Коаксиальный кабель

Скорость передачи информации от 1 до 10 Мбит/с, а в некоторых случаях может достигать 50 Мбит/с. Коаксиальный кабель используется для основной и широкополосной передачи информации.

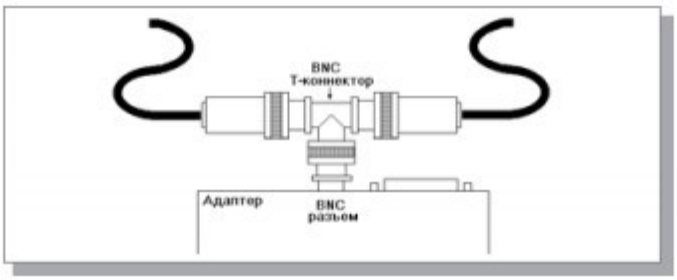


Рисунок 2 Присоединение адаптера к тонкому коаксиальному кабелю;

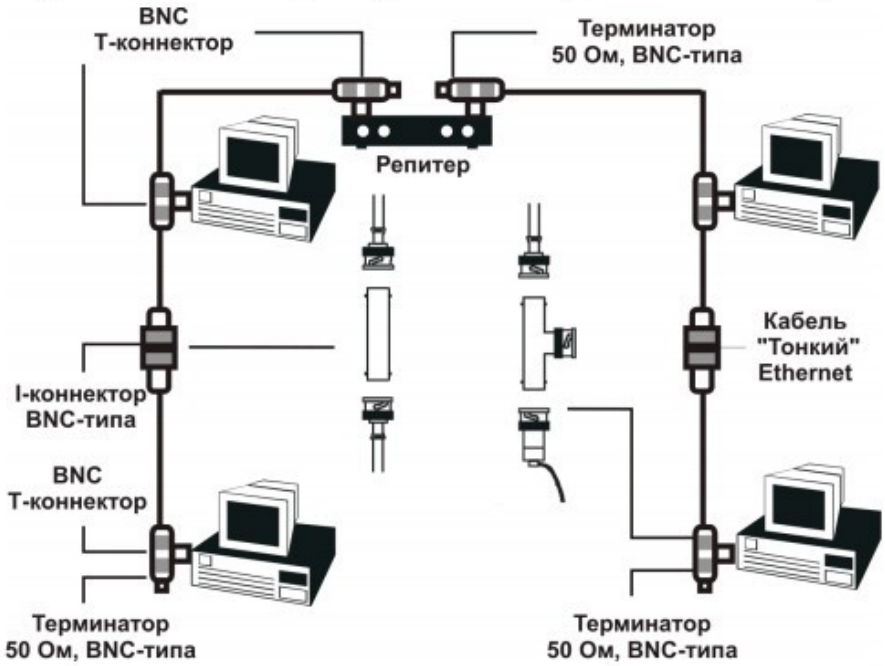


Рисунок 3 – Соединение компьютеров сети тонким коаксиальным кабелем

Минимальный набор оборудования для односегментной сети на тонком кабеле должен включать в себя следующие элементы:

- сетевые адаптеры (по числу объединяемых в сеть компьютеров);
- отрезки кабеля с BNC-разъемами на обоих концах, общая длина которых достаточна для объединения всех компьютеров;
- BNC Т-коннекторы (по числу сетевых адаптеров);
- один BNC терминатор без заземления;
- один BNC терминатор с заземлением.

Если сеть создается из нескольких сегментов с использованием репитеров и концентраторов, то надо учитывать, что некоторые концентраторы имеют встроенные 50-омные терминаторы (иногда – отключаемые), что упрощает проблемы согласования.

Cheapernet–кабель (RG-58, 10Base2)

Более дешевым, чем Ethernet–кабель является соединение Cheapernet-кабель (RG–58) или, как его часто называют, тонкий (англ. thin) Ethernet. Это также 50- омный коаксиальный кабель со скоростью передачи информации в 10 Мбит/с. При соединении сегментов Cheapernet–кабеля также требуются повторители. Вычислительные сети с Cheapernet–кабелем имеют небольшую стоимость и минимальные затраты при наращивании. Соединения сетевых плат производится с помощью широко используемых малогабаритных байонетных разъемов (СР–50). Дополнительное экранирование не требуется. Кабель присоединяется к ПК с помощью тройниковых соединителей (T–connectors). Расстояние между двумя рабочими станциями без повторителей может составлять максимум 300 м, а минимум – 0,5 м, общее расстояние для сети на Cheapernet–кабеля – около 1000 м. Приемопередатчик Cheapernet расположен на сетевой плате как для гальванической развязки между адаптерами, так и для усиления внешнего сигнала

Широкополосный коаксиальный кабель

Широкополосный коаксиальный кабель невосприимчив к помехам, легко наращивается, но цена его высокая. Скорость передачи информации равна 500 Мбит/с. При передачи информации в базисной полосе частот на расстояние более 1,5 км требуется усилитель, или так называемый

репитер (англ. repeater – повторитель). Поэтому суммарное расстояние при передаче информации увеличивается до 10 км. Для вычислительных сетей с топологией типа «шина» или «дерево» коаксиальный кабель должен иметь на конце согласующий резистор (терминатор).

Витая пара (10BaseT)

Наиболее дешевым кабельным соединением является, витое двухжильное проводное соединение, часто называемое «витой парой» (англ. twistedpair). Она 4 позволяет передавать информацию со скоростью до 10 Мбит/с, легко наращивается, однако является помехонезащищенной. Длина кабеля не может превышать 1000 м при скорости передачи 1 Мбит/с. Преимуществами являются низкая цена и беспроблемная установка.

Неэкранированная витая пара состоит из восьми проводов. Каждый провод изолирован отдельно; все восемь проводов собраны в четыре свитые пары. Завивка проводов предотвращает перекрестные помехи, наводимые соседними парами и внешними источниками. Все четыре пары помещены в общую оболочку.

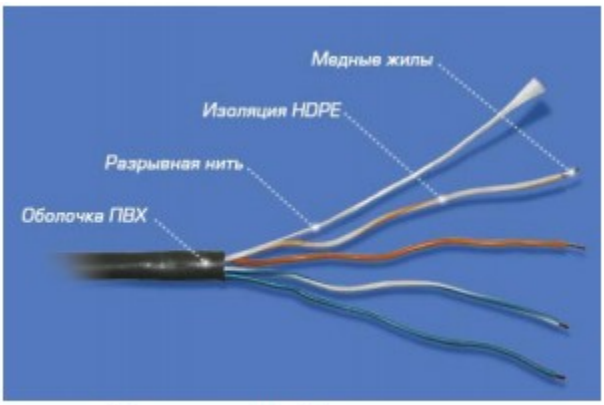


Рисунок 4 – Витая пара

С кабелями типа «витая пара» используются разъемы RJ45, те же, что и у стандартных телефонных кабелей, только с восемью контактами вместо четырех или шести.

Рисунок 5 – Разъем RJ45 под витую пару

Для повышения помехозащищенности информации часто используют экранированную витую пару, т.е. витую пару, помещенную в экранирующую оболочку, подобно экрану коаксиального кабеля. Это увеличивает стоимость витой пары и приближает ее цену к цене коаксиального кабеля.

В телефонных сетях витая пара используется уже не одно десятилетие, а вот к компьютерным сетям ее приспособили относительно недавно. Витая пара вытеснила коаксиальный кабель из мира ЛВС благодаря нескольким явным преимуществам. Во-первых, кабель «витая пара» состоит из восьми отдельных проводов, что делает его гибче коаксиального и, соответственно, облегчает его укладку. Во-вторых, к 5 прокладке кабелей для ЛВС можно смело привлекать тысячи готовых квалифицированных монтажников телефонных кабелей. В новых зданиях зачастую телефонный и сетевой кабели одновременно укладывает один и тот же подрядчик.

Минимальный набор оборудования для сети на витой паре включает в себя следующие элементы:

– сетевые адаптеры (по числу объединяемых в сеть компьютеров), имеющие UTP-разъемы RJ-45;

– отрезки кабеля с разъемами RJ-45 на обоих концах (по числу объединяемых компьютеров);

– один концентратор, имеющий столько UTP-портов с разъемами RJ-45, сколько необходимо объединить компьютеров.

Оптоволоконные линии (10BaseFL)

Наиболее дорогими являются оптопроводники, называемые также стекловолоконным кабелем.

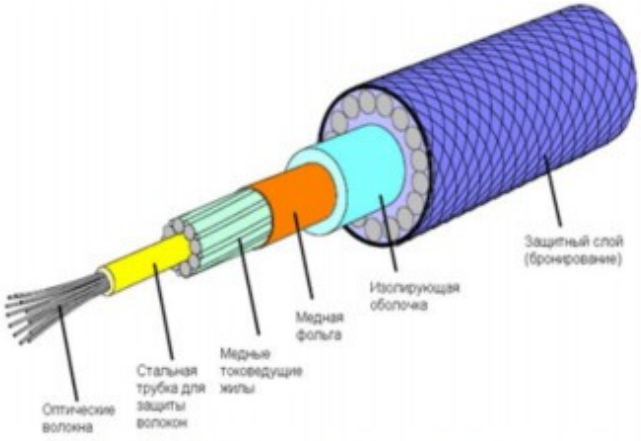


Рисунок 6 – Оптоволокно

Скорость распространения информации по ним достигает 100 Мбит/с, а на экспериментальных образцах оборудования – 200 Мбит/с. Допустимое удаление более 50 км. Внешнее воздействие помех практически отсутствует. На данный момент-это наиболее дорогостоящее соединение для ЛВС. Применяются там, где возникают электромагнитные поля помех или требуется передача информации на очень большие расстояния без использования повторителей. Они обладают противоподслушивающими свойствами, так как техника ответвлений в оптоволоконных кабелях очень сложна. Оптопроводники объединяются в JIBC с помощью звездообразного соединения.

Передача информации в данном случае идет по двум оптоволоконным кабелям, передающим сигналы в разные стороны (как и в 10BASE-T). Иногда используются двухпроводные оптоволоконные кабели, содержащие два кабеля в общей внешней оболочке, но чаще – два одиночных кабеля. Вопреки распространенному мнению, стоимость оптоволоконного кабеля не слишком высока 6 (она близка к стоимости тонкого коаксиального кабеля). Правда, в целом аппаратура в данном случае оказывается заметно дороже, так как требует использования дорогих оптоволоконных трансиверов.

Спецификация IEEE 802.3d FOIRL

Спецификация IEEE 802.3d FiberOpticInterRepeaterLink (FOIRL) была предложена в 1987 году. Она была предназначена для обеспечения информационного взаимодействия репитеров, которые находятся на значительном (до 1000 м) расстоянии друг от друга. Для подключения к волоконно-оптической линии использовались соединители типа SMA и ST.

В дальнейшем, однако данная технология не получила развития, поскольку появились новые сетевые технологии семейства 10Base-F, которые также использовали волоконно-оптический кабель для передачи данных и обеспечивали лучшие информационные и эксплуатационные характеристики.

Использование волоконно-оптического кабеля для передачи данных

Основными преимуществами передачи данных по волоконно-оптическим линиям связи являются:

- высокая скорость передачи данных - предел для промышленного ВОЛС 3ГГц, в то время, как для медного кабеля это значение составляет не более 500 МГц.
- нечувствительность к электромагнитным помехам
- отсутствие электромагнитного излучения при передаче данных
- обеспечение гальванической развязки между передатчиком и приемником данных

Волоконно-оптический кабель состоит из следующих компонентов: оптическое волокно, оптический экран, защитный экран.

Для обозначения типа волоконно-оптического кабеля используют выражение вида:

Диаметр волокна/Диаметр экрана, в микро метрах, например: 62.5/125

Наибольшее распространение для передачи данных в локальных сетях в настоящее время получил многомодовый волоконно-оптический кабель, однако, для обеспечения передачи данных со скоростью свыше 1ГГц на большие расстояния может быть использован только одномодовый волоконно-оптический кабель.

Для обеспечения синхронизма тактовых генераторов в отсутствие передаваемых и принимаемых кадров передатчик и приемник обмениваются синхронизирующими последовательностями 2.5 МГц.

Протокол 10 Base FB не является универсальным и не обеспечивает, в частности, информационное взаимодействие между репитером и рабочей станцией.

Спецификация 10 Base FP

Спецификация 10 Base FP (FiberPassive) определяет интерфейс физического уровня для обеспечения взаимодействия компонентов локальной сети с 7 использованием принципа пассивного оптического разветвителя. При использовании технологии 10 Base FP возможно построение пассивной объединяющей структуры, которая может обеспечить взаимодействие 33 рабочих станций, находящихся на удалении до 500 м.

Спецификация 10 Base FL

Спецификация 10 Base FL (FiberLink) определяет протокол передачи данных по двум волоконно-оптическим кабелям со скоростью 10 Мбит/сек на расстояние до 2000м. Протокол физического уровня 10 Base FL обеспечивает информационное взаимодействие в различных вариантах:

- Рабочая станция – рабочая станция
- Рабочая станция – репитер
- Репитер – репитер

В 10BASE-FL применяется мультимодовый кабель и свет с длиной волны 850 нанометров, однако имеется аппаратура и для использования одномодового кабеля (с предельной длиной до 5 км). Оптоволоконный трансивер называется FOMAU (FiberOptic MAU).Он выполняет все функции обычного трансивера (MAU), но, кроме того, преобразует электрический сигнал в оптический при передаче и обратно при приеме. FOMAU также формирует и контролирует сигнал целостности линии связи, передаваемый в паузах между пакетами. Целостность линии связи, как и в случае 10BASE-T, индицируется светодиодами "Link" и определяется по наличию между передаваемыми пакетами сигнала "Idle" частотой 1 МГц. Для присоединения трансивера к адаптеру применяется стандартный AUI-кабель, такой же, как и в случае 10BASE5,но длина его не должна превышать 25 метров. Имеются также сетевые адаптеры со встроенными трансиверами FOMAU, которые имеют только внешние оптоволоконные разъемы и не нуждаются в трансиверных кабелях.

Длина оптоволоконных кабелей, соединяющих трансивер и концентратор, может достигать 2 километров без применения каких бы то ни было ретрансляторов. Таким образом, возможно объединение в локальную сеть компьютеров, находящихся в разных зданиях, разнесенных территориально.

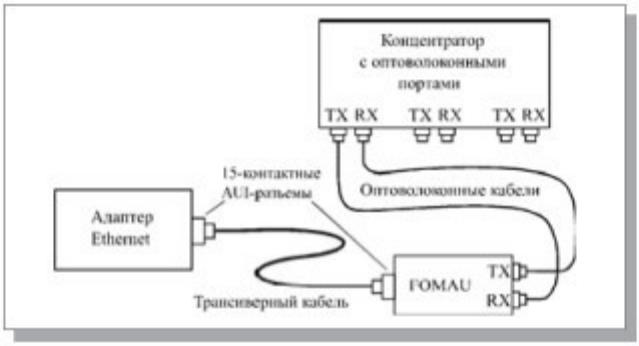


Рисунок 7 – Соединение адаптера и концентратора в 10BASE-FL

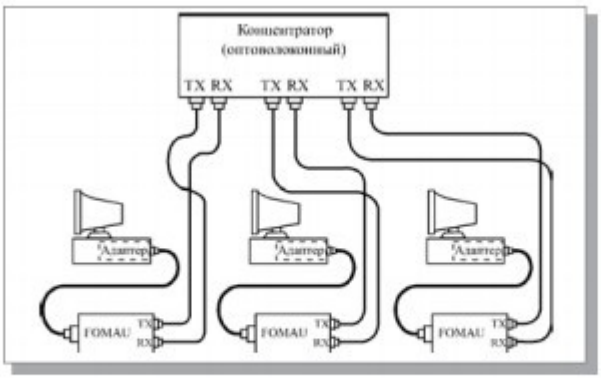


Рисунок 8 – Объединение компьютеров в сеть по стандарту 10BASE-FL

Последовательность действий при обжиме:

1. Аккуратно обрежьте конец кабеля, при этом лучше всего пользоваться резаком, встроенным в обжимной инструмент

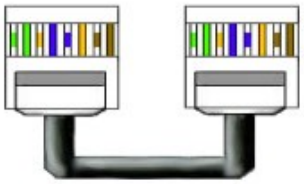
Обжимной инструмент RJ-45

Нож для зачистки изоляции витой пары.

2. Снимите с кабеля изоляцию. Можно использовать специальный нож для зачистки изоляции витой пары, его лезвие выступает ровно на толщину изоляции, так вы не повредите проводники. Впрочем, если нет специального ножа, можно воспользоваться обычным или взять ножницы, или использовать ножи обжимного инструмента.
3. Разведите и расплетите проводки, выровняйте их в один ряд, при этом соблюдая цветовую последовательность
4. Обкусите проводки так, чтобы их осталось чуть больше сантиметра
5. Вставляйте проводники в разъем RJ-45
6. Проверьте, правильно ли вы расположили проводки
7. Убедитесь все ли провода полностью вошли в разъем и уперлись в его переднюю стенку
8. Поместите коннектор с установленной парой в клещи, затем плавно, но сильно произведите обжим.

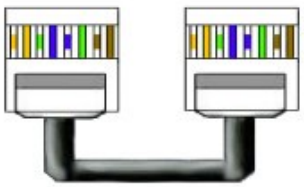
Цветовая последовательность проводников

Существует два распространенных стандарта по разводке цветов по парам: T568A компании Siemon и T568B компании AT&T. Оба этих стандарта абсолютно равнозначны.



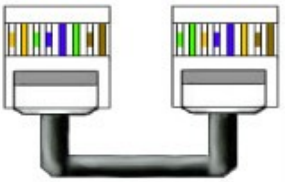
3.2.1 Сетевая карта <-> Коммутатор по стандарту: T568A

При такой раскладке информацию несут проводники: Бело-зелёный, Зелёный, Бело-оранжевый, Оранжевый.



3.2.2 Сетевая карта<->Коммутатор по стандарту: T568B

При такой раскладке информацию несут проводники: Бело-оранжевый, Оранжевый, Бело-зелёный, Зеленый.



3.2.3 Сетевая карта <-> Сетевая карта (Кроссовер кабель)

Обжатая таким образом, витая пара может вам понадобиться в 2 случаях:

1. Для соединения 2 компьютеров без коммутатора.
2. Для соединения 2 или более Hub/Switch

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:

Задание 1. Провести разделку кабеля витая пара.
Задание 2. Проверить работоспособность кабеля витая пара подключением ПЭВМ к сети.

Контрольные вопросы:

1. Виды кабелей.
2. Зачем в кабелях типа «Витая пара» отдельные проводники перекручивают между собой.
3. В чем разница UTPи STP.
4. Стандарты T568A и T568B.

Литература:

1. Основы локальных сетей: курс лекций / Ю.В. Новиков, С.В. Кондратенко. — Москва: Интуит НОУ, 2016. — 407 с. — ISBN 978-5-9556-0032-1.
Электронно-библиотечная система www.book.ru