САНКТ-ПЕТЕРБУРГСКОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «КОЛЛЕДЖ «КРАСНОСЕЛЬСКИЙ»

РАССМОТРЕНО И ПРИНЯТО
на заседании Педагогического Совета
СПб ГБПОУ «Колледж «Красносельский»

Протокол № 6 от _07.06._ 2024 г.

УТВЕРЖДАЮ
Директор СПб ГБПОУ
«Колледж «Красносельский»
_____ Г.И. Софина
«_____» _____ 2024 г.
Приказ № 101-осн. от 07.06. 2024 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

по дисциплине

ОП.11 Компьютерные сети

для обучающихся по специальности

09.02.07 Информационные системы и программирование
(Программист)

СОГЛАСОВАНО:

_____

_____

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00EC2D20EFC3421C789C8AAB01A59A5674
Владелец: Софина Галина Ивановна
Действителен: с 14.05.2024 до 07.08.2025

Санкт-Петербург
2024 г.

РАССМОТРЕНО И ОДОБРЕНО
На заседании МК СПб ГБПОУ «Колледж «Красносельский»
Протокол № _____ от _____ 2024 г.
Председатель МК _____ Н.В. Медведева

Организация-разработчик: СПб ГБПОУ «Колледж «Красносельский»

Разработчик: Борисов Н.М., мастер производственного обучения.

Методические указания к практическим занятиям являются частью основной профессиональной образовательной программы СПО по специальности 09.02.07 Информационные системы и программирование (программист).
Укрупненная группа специальностей 09.00.00 Информатика и вычислительная техника.
Дисциплина «ОП.11 Компьютерные сети».

Содержание

Пояснительная записка

Методические указания по выполнению практических работ обучающимися составлены в соответствии с рабочей программой учебной дисциплины «Компьютерные сети» для специальности 09.02.07 «Информационные системы и программирование».

Цель проведения работ – отработка необходимых навыков работы компьютерными сетями для решения конкретных задач.

Порядок выполнения работы

- записать название работы, ее цель в тетрадь;
- выполнить основные задания в соответствии с ходом работы;
- выполнить самостоятельные задания.

Рекомендации по оформлению практической работы

- при выполнении практической работы в прикладных программах использовать оформление в соответствие с заданием
- работы проводятся согласно календарно-тематическому планированию, в соответствии с учебной программой.

Пропущенные практические работы выполняются студентом самостоятельно и сдаются в отведенные на изучение дисциплины сроки.

При изучении теоретического материала требуется выполнение описанных операций на ПК.

Критерии оценки работ

- наличие оформленной цели выполняемой работы, выполнение более половины основных заданий (удовлетворительно);
- наличие оформленной цели выполняемой работы, выполнение всех основных и более половины дополнительных заданий (хорошо);
- наличие оформленной цели выполняемой работы, выполнение всех основных и дополнительных заданий (отлично).

Освоение содержания учебной дисциплины «Информационные технологии» обеспечивает достижение обучающимися следующих результатов:

- оОрганизовывать и конфигурировать компьютерные сети;
- Строить и анализировать модели компьютерных сетей;
- Эффективно использовать аппаратные и программные компоненты компьютерных сетей при решении различных задач;
- Выполнять схемы и чертежи по специальности с использованием прикладных программных средств;
- Работать с протоколами разных уровней (на примере конкретного стека протоколов: TCP/IP, IPX/SPX);
- Устанавливать и настраивать параметры протоколов;
- Обнаруживать и устранять ошибки при передаче данных;

При реализации содержания учебной дисциплины «Информационные технологии» обязательная нагрузка обучающихся — 64 часа, включая практические занятия. Итоговая форм контроля – экзамен. Обучающиеся не выполнившие все практические задания до экзамена не допускаются.

Перечень практических работ

№	Наименование практических работ	Кол-во часов
1	Построение схемы компьютерной сети	2
2	Монтаж кабельных сред технологий Ethernet	2
3	Построение одноранговой сети	2
4	Настройка протоколов TCP/IP в операционных системах	2
5	Работа с диагностическими утилитами протокола TCP/IP	2
6	Решение проблем с TCP/IP	2
7	Преобразование форматов IP-адресов. Расчет IP-адреса и маски подсети	3
8	Настройка удаленного доступа к компьютеру	3
ВСЕГО		18

Практическая работа № 1 Построение схемы компьютерной сети

Цель работы: построение схемы компьютерной сети с помощью MS Visio 2016.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

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.

ПРАКТИЧЕСКАЯ ЧАСТЬ

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 (**ме-ню **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 (рис.1).

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

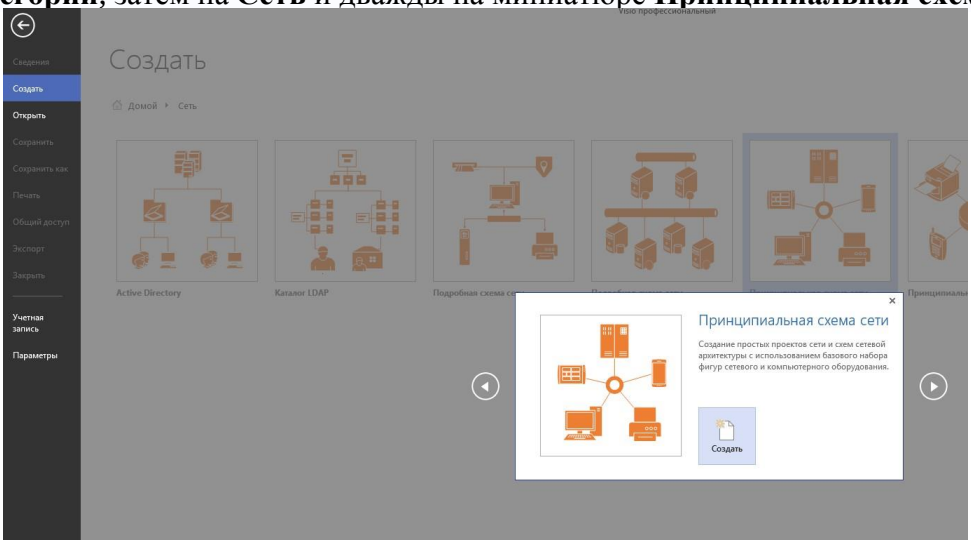


Рисунок 1

– 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.

– Перетащим маркер изменения размера с правого края фигуры **Ethernet** вправо так, чтобы ее ширина стала 100 мм.

– Не снимая выделение с фигуры **Ethernet**, введем *Филиал 1* в качестве подписи для сегмента сети, затем щелкнем на любой точке фона страницы.

– Перетащим фигуру **Сервер** на страницу и поместим ее над фигурой Ethernet ближе к левому краю последней.

– 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 (рис.2).

Рисунок 2

– 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.

− Перетащим на страницу две фигуры **ПК** и одну фигуру **Ноутбук** из набора **Компьютеры и мониторы** и сбросим их под фигурой **Ethernet**.

− Перетащим желтый управляющий маркер к каждой из фигур **ПК (рис.3.)**.

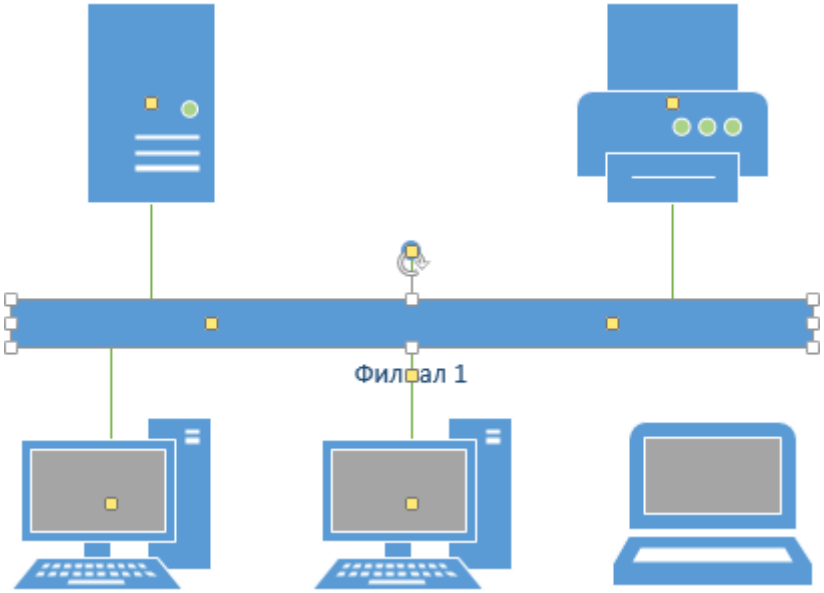


Рисунок 3

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.

− 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 4.

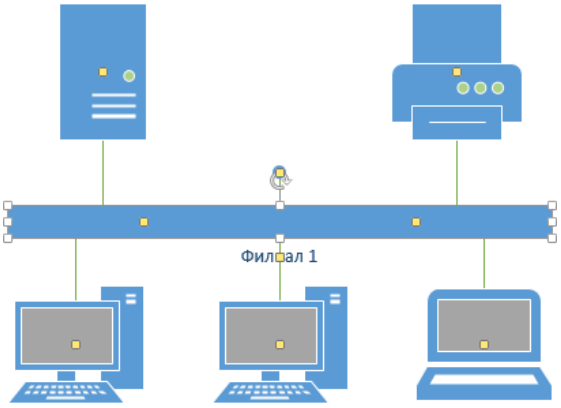


Рисунок 4

– Перетащим другую фигуру **Ethernet** в верхний правый угол страницы, оставив достаточно места для того, чтобы над ней можно было разместить другие фигуры.

– Перетащим левый маркер изменения размера влево, чтобы сделать сег- мент **Ethernet** шире. Продолжим перетаскивать, пока не появится двунаправленная стрел-ка, показывая, что новый сегмент сети имеет такую же длину, как и уже существующий на странице (рис 5).

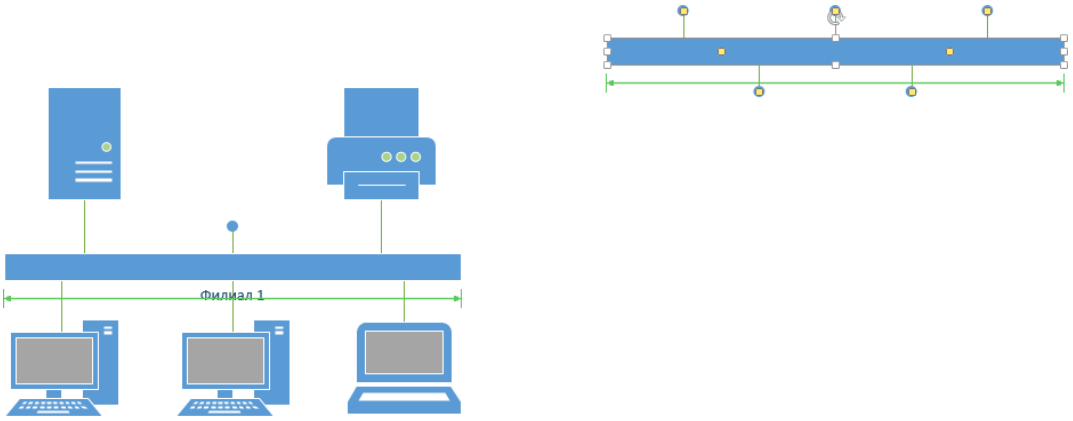


Рисунок 5

– Не снимая выделения с фигуры **Ethernet**, введем **Филиал 2** и щелкнем на пу-стом месте страницы.

– Перетащим фигуру **Принтер**, две фигуры **ПК** и три фигуры **Ноутбук** и соеди-ним их с новым сегментом сети.

– Перетащим фигуру **Маршрутизатор** из набора элементов **Сеть и периферий-ные устройства** и разместим ее по центру страницы.

– Перетащим оставшийся неиспользованный управляющий маркер из фигуры сети **Филиал 1** и приклеим его к маршрутизатору.

– 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 6.

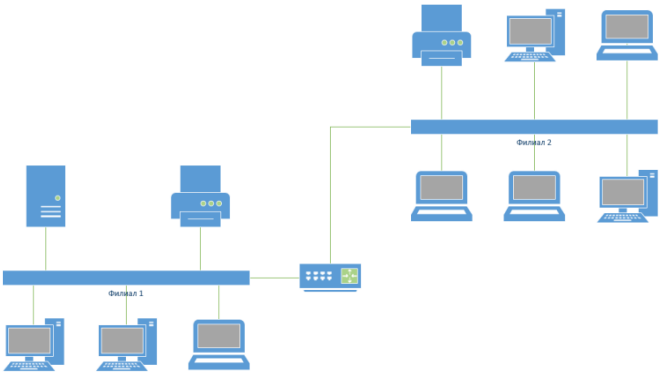


Рисунок 6

Практическая работа №2 Монтаж кабельных сред технологий Ethernet

Цель работы: создать и протестировать прямой и перекрестный кабели UTP (неэкранированная витая пара) для сети Ethernet.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

На сегодняшний день подавляющая часть компьютерных сетей использует для соединения провода и кабели. Существуют различные типы кабелей, но на практике в большинстве сетей применяются только три основные группы:

1. Коаксиальный кабель (coaxial cable).
2. Витая пара (twisted pair).
   − неэкранированная;
   − экранированная.
3. Оптоволоконный кабель (fiber cable).

Назначение и структура коаксиального кабеля. Коаксиальный кабель предназначен для передачи высокочастотных сигналов в различной электронной аппаратуре, особенно в радио- и ТВ-передатчиках, компьютерах, трансмиттерах.

Рисунок 7

Конструкция коаксиального кабеля состоит из медной жилы или стальной жилы плакированной медью, изоляции, ее окружающей, экрана в виде герметичного слоя фольги и металлической оплетки, внешней оболочки (см. рис. 7). При наличии сильных электромагнитных помех в месте прокладки сети можно воспользоваться кабелем с трехкратной (фольга + оплетка + фольга) или четырехкратной (фольга + оплетка + фольга + оплетка) экранизацией. Экран защищает передаваемые по кабелю данные, поглощая внешние электромагнитные сигналы - помехи или шумы. Таким образом, экран не позволяет помехам исказить данные. Трехкратный экран рекомендуется использовать в условиях сильного электромагнитного шума, например в городских индустриальных районах. Четырехкратный экран разработан для использования в местах с чрезвычайно высоким уровнем электромагнитного шума, например, вблизи от электрических машин, магистралей, в метро или поблизости от организаций оборудованных мощными радиопередатчиками.

Электрические сигналы, кодирующие данные, передаются по жиле. Жила - это один провод (сплошная) или пучок проводов. Сплошная жила изготавливается, из меди или стали плакированной медью. Жила окружена изоляционным слоем, который отделяет ее от металлической оплетки. Оплетка играет роль заземления и защищает жилу от электрических шумов и перекрестных помех (электрические наводки, вызванные сигналами в соседних проводах). Проводящая жила и металлическая оплетка не должны соприкасаться, иначе произойдет короткое замыкание, помехи проникнут в жилу, и данные разрушатся. Снаружи кабель покрыт непроводящим слоем - из резины, тефлона или пластика.

Коаксиальный кабель более помехоустойчив, затухание сигнала в нем меньше чем в витой паре. Ввиду того, что плетеная защитная оболочка поглощает внешние электромагнитные сигналы, не позволяя им влиять на передаваемые по жиле данные, то коаксиальный кабель можно использовать при передаче на большие расстояния и в тех случаях, когда высокоскоростная передача данных осуществляется на несложном оборудовании.

Существует два типа коаксиальных кабелей:

− **Тонкий коаксиальный кабель -** гибкий кабель диаметром около 0,5 см, прост в применении и годится практически для любого типа сети, способен передавать сигнал на расстояние до 185 м без его заметного искажения, вызванного затуханием. Основная отличительная особенность — медная жила. Она может быть сплошной или состоять из нескольких переплетенных проводов.

− **Толстый коаксиальный кабель -** относительно жесткий кабель с диаметром около 1 см. Иногда его называют «стандартный Ethernet», поскольку он был первым ти- пом кабеля, применяемым в Ethernet — популярной сетевой архитектуре. Медная жила толстого коаксиального кабеля больше в сечении, чем тонкого, поэтому он передает сиг- налы на расстояние до 500 м. Толстый коаксиальный кабель иногда используют в качестве основного кабеля, который соединяет несколько небольших сетей, построенных на тон- ком коаксиальном кабеле.

Сравнение двух типов коаксиальных кабелей. Как правило, чем толще кабель, тем сложнее его прокладывать. Тонкий коаксиальный кабель гибок, прост в установке и относительно недорог. Толстый коаксиальный кабель трудно гнуть, следовательно, его сложнее монтировать, это очень существенный недостаток, особенно в тех случаях, когда необходимо проложить кабель по трубам или желобам.

Выбор того или иного типа коаксиальных кабелей зависит от места, где этот кабель будет прокладываться. Существуют поливинилхлоридные и пленумные классы коаксиальных кабелей.

Поливинилхлорид – это пластик, который применяется в качестве изолятора или внешней оболочки у большинства коаксиальных кабелей. Его прокладывают на открытых участках помещений. Однако при горении он выделяет ядовитые газы.

Пленумные коаксиальные кабели – прокладываются в вентиляционных шахтах, между подвесными потолками и перекрытиями пола.

Монтирование кабельной системы .Для подключения к толстому коаксиальному кабелю применяют специальное устройство – трансивер. Он снабжен специальным коннектором пронзающим ответвителем, который проникает через слой изоляции и вступает в контакт с проводящей жилой.

Для подключения тонкого коаксиального кабеля используются BNC-коннекторы. BNC коннектор (рисунок 8), BNC T коннектор (рисунок 9) и BNC баррел коннектор.

Рисунок 8

Рисунок 9

Назначение и структура витой пары. Самая простая витая пара – это два перевитых изолированных медных провода. Согласно стандарту различают два вида витых пар:

− **UTP - кабель на основе неэкранированной медной пары;**

− **STP - кабель на основе экранированной медной пары.**

Неэкранированная витая пара (UTP, unshielded twisted pair) - это кабель, в котором изолированная пара проводников скручена с небольшим числом витков на единицу длины. Скручивание проводников уменьшает электрические помехи извне при распространении сигналов по кабелю (рис.10).

Кабель на основе неэкранированной медной пары различают по его пропускной способности, выделяя тем самым несколько категорий:

Категория 3: Кабель этой категории имеет частоту передачи сигналов до 16 МГц и предназначен для использования в сетях скоростью до 10 Мбит/с.

Категория 4: Кабель 4-й категории передает данные с частотой до 20 МГц, используется в сетях Token Ring (скорость передачи до 16 Мбит/с)

Категория 5:, Кабель этой категории предназначен для передачи сигнала с частотой 100 МГц при на скорости 100М\бит 4 витые пары.

Категория 5е Кабель этой категории предназначен для передачи сигнала с частотой 100 МГц при на скорости 1000М\бит для сетей 1000BaseT, Gigabit Ethernet.

Категория 6: Кабель этой категории является одной из наиболее совершенных сред передачи данных среди вышеперечисленных категорий. Его частота передачи сигнала доходит до 250 МГц, что почти в два раза больше пропускной способности категории 5е. Улучшена помехозащищенность.

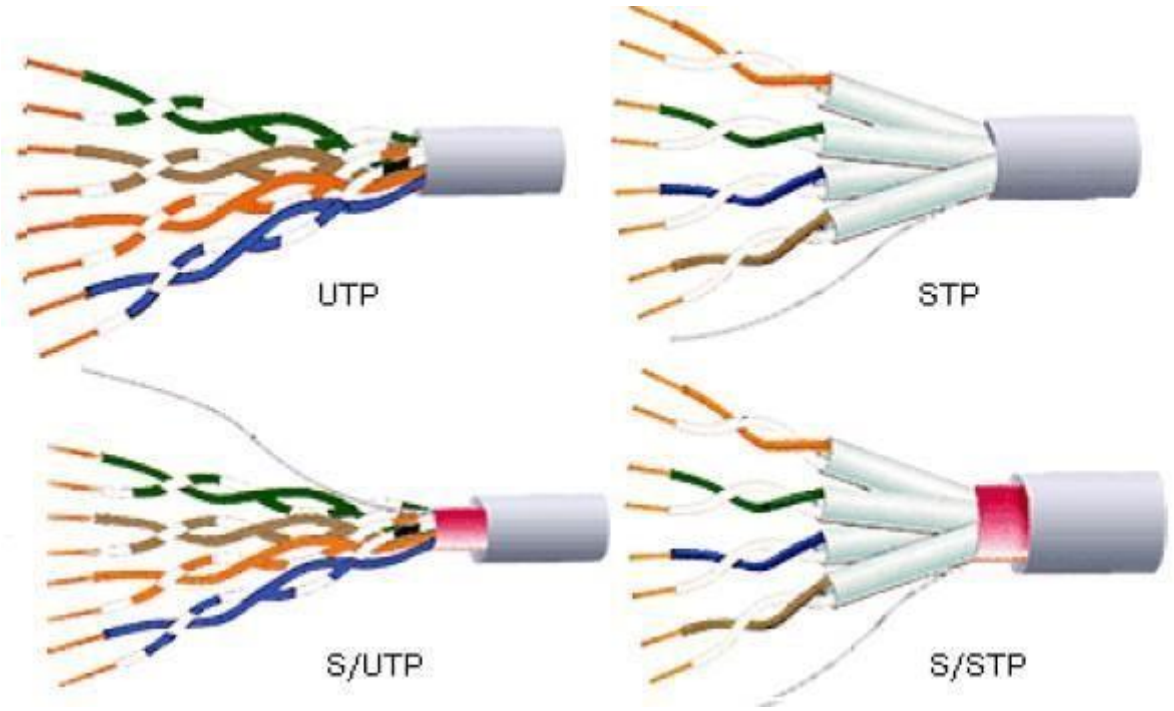


Рисунок 10

Монтаж кабельной системы на основе витой пары. ***Прямая разводка*** – применяется, когда кабель соединяет ПК с концентратором или концентратор с концентратором (таб. 1)

Кросс-разводка – применяется для соединения ПК друг с другом (таб. 2).

Прямая разводка кабеля

Таблица 1

№ контакта	Цвет про-

коннектора	водника
1.	Бело-зеленый
2.	Зеленый
3.	Бело-оранжевый
4.	Синий
5.	Бело-синий
6.	Оранже-вый
7.	Бело-коричневый
8.	Коричне-вый

Кросс-разводка кабеля

Таблица 2

№ контакта коннектора	Первый конец	Второй конец
1.	Бело-зеленый	Бело-оранжевый
2.	Бело-синий	Оранже-вый
3.	Бело-оранжевый	Бело-зеленый
4.	Синий	Синий
5.	Бело-синий	Бело-синий
6.	Оранже-вый	Бело-синий
7.	Бело-коричневый	Бело-коричневый
8.	Коричне-вый	Коричне-вый

После подключения коннекторов кабель следует проверить с помощью специального тестера, который определит, правильно ли проводники витых пар подсоединены к контактам коннекторов, а также целостность самого кабеля.

Назначение и функции оптоволокна (рис 11). В оптоволоконном кабеле цифровые данные распространяются по оптическим волокнам в виде модулированных световых импульсов. Это относительно защищенный способ передачи, поскольку при нем не используются электрические сигналы. Следовательно, к оптоволоконному кабелю невозможно подключиться, не разрушая его, и перехватывать данные, от чего не застрахован любой кабель, проводящий электрические сигналы.

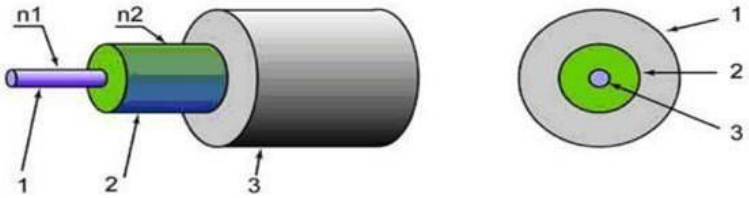


Рисунок 11

1 – сердцевина с показателем преломления n_1; 2 – отражающая оболочка с показателем преломления n_2, $n_1 > n_2$; 3 – защитное покрытие.

Кабель содержит несколько световодов, хорошо защищенных пластиковой изоляцией. Он обладает сверхвысокой скоростью передачи данных (до 2 Гбит), и абсолютно не подвержен помехам. Расстояние между системами, соединенными оптиковолокном, может достигать 100 километров. Казалось бы, идеальный проводник для сети найден, но стоит оптический кабель чрезвычайно дорого, и для работы с ним требуется специальные сетевые карты, коммутаторы и т.д. Без специального оборудования оптоволокно практически не подлежит ремонту. Данное соединение применяется для объединения крупных сетей, высокосортного доступа в Интернет (для провайдеров и крупных компаний), а также для передачи данных на большие расстояния. В домашних сетях, если требуется высокая скорость соединения, гораздо дешевле и удобнее воспользоваться гигабитной сетью на витой паре.

Лучи, входящие под разными углами в оптоволокно (рис. 12, 13) называются модами, а волокно, поддерживающее несколько мод - многомодовым. По одномодовому волокну распространяется только один луч.

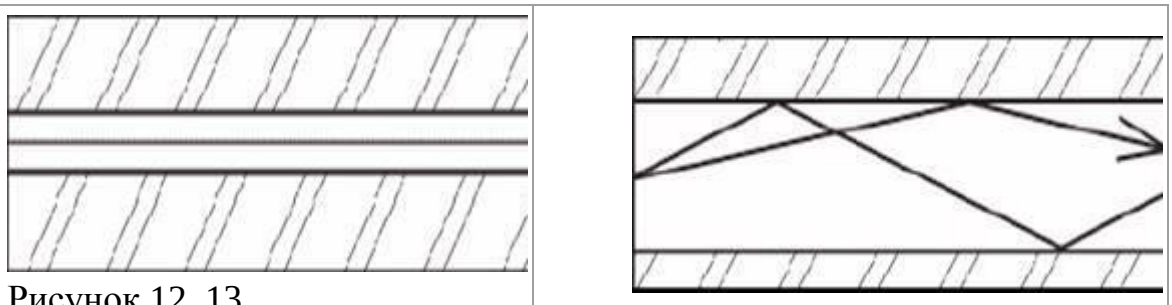


Рисунок 12, 13

ПРАКТИЧЕСКАЯ ЧАСТЬ

Осуществите обжим витой пары по типу прямой разводки и кросс-разводки, используя таблицы 1, 2.

Практическая работа № 3. Построение одноранговой сети

Цель работы: освоение умений по построению одноранговой локальной вычислительной сети

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

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.

ПРАКТИЧЕСКАЯ ЧАСТЬ

Задание 1.

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

− 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.

Задание 2.

Создайте подключение типа «компьютер-компьютер» (рис. 13)

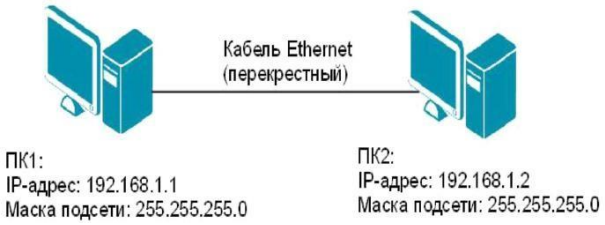


Рисунок 13

− 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.

Задание 2.

− Создайте одноранговую сеть с использованием коммутатора (рис 14).

− Получите доступ к текстовому файлу, расположенному на соседнем компьютере.

− 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.

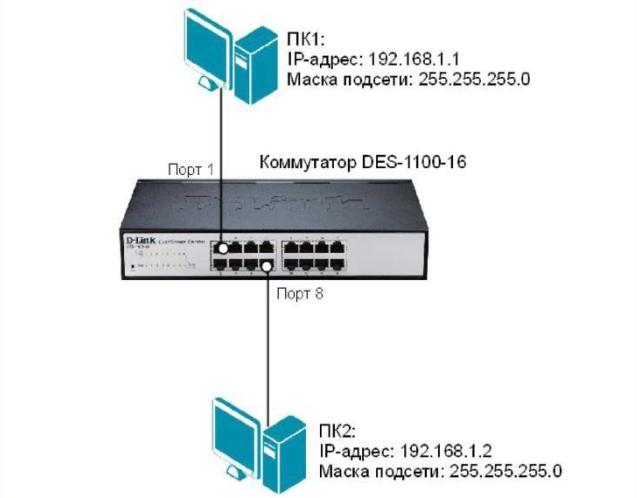


Рисунок 14

Дополнительные инструкции:

Создание подключения типа «компьютер-компьютер».

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

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

− Откройте Сетевые подключения (Пуск - Панель управления - Сетевые подключения);

− В контекстном меню пункта Подключение по локальной сети выберите Свойства;

− В диалоговом окне выберите Протокол Интернета (TCP/IP) и нажмите Свойства;

− Выберите Использовать следующий IP-адрес

− Задайте новые IP – адрес и маску подсети для ПК1 (или ПК 2)

− Проверьте конфигурацию сетевого адаптера ПК1 (или ПК 2) с помощью команды ipconfig.

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

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

− Подключите ПК1 и ПК2 к коммутатору DES-1100-16 «прямым» Ethernet- кабелем в соответствии со схемой

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

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

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

− Во вкладке Доступ - Сетевой общий доступ и безопасность выберите Открыть общий доступ к этой папке и Разрешить изменение файлов по сети4. Нажмите кнопку Применить;

− В данной сетевой папке создайте пустой текстовый документ.

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

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

− Найдите созданную папку соседнего компьютера с открытым общим доступом;

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

Практическая работа №4 Настройка протоколов TCP/IP в операционных системах

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

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

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.

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, работаю- щих на транспортном и сетевом уровнях семиуровневой модели OSI . Протокол TCP в процессе работы ОС в IP– сетях обычно никаких настроек не требует, хотя такая возмож- ность 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, поддерживае- мый всеми без исключения типами ОС семейства Windows, – установку с помощью пане- лиь **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 опреде-лить принадлежность машины-получателя к сети машины-отправителя используется ме- ханизм 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, реали- зующий функции протокола IP на машине m1, выполнит просмотр маршрутной таблицы сцелью поиска маршрута к сети назначения, и так как такого маршрута нет, то данные бу- дут 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, имею- щих 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

ПРАКТИЧЕСКАЯ ЧАСТЬ

Задание 1. Изменение параметров настройки протокола IP.

− 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".

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

− 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.

− Удалите протокол NetBUI, если он установлен на Вашей машине.

− Установите 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.

− Если в результате изменения параметров настройки протокола IP будет выдано сообщение о необходимости перезагрузки, ни в коем случае не делайте этого, просто откажитесь.

− Открыть консоль системы). В командной строке выполнить команду:

> ipconfig /all

− Сохраните результат выполнения этой команды в отчете.

− В командной строке консоли выполните команду:

> ping <адрес_шлюза>

− Результаты занесите в файл отчета.

− Оформление отчета по результатам выполнения практической работы.

Практическая работа №5 Работа с диагностическими утилитами протокола TCP/IP

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

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

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 послан- ный пакет и печатает количество переданных и принятых пакетов. Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостамиплохая, 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 па- кет и т.д.. При получении ответа в поле time указывается, за какое время (в миллисекун- дах) посланный пакет доходит до удаленного хоста и возвращается назад. Так как зна- чение 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 откли- ка, 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 Set-

tings\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

Изучение 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 экранпри этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жиз- ни. 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 ms68 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 протоколARP 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.

ПРАКТИЧЕСКАЯ ЧАСТЬ

Задание 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.

Получение имеени хоста

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

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	

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)

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

Просмотр ARP-кэша

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

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.

Практическая работа №6 Решение проблем с TCP/IP

Цель работы: изучение способов решения проблем с TCP/IP

ТЕОЕРЕТИЧЕСКАЯ ЧАСТЬ

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 ком- плекта 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 А в пункт В, 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.

ПРАКТИЧЕСКАЯ ЧАСТЬ

Задание 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.

− 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).

− Запишите IP конфигурацию машины. Особенно важно сделать заметки следующих элементов:

− Использует ли машина статичную или динамичную конфигурацию?

− Если используется статичная конфигурация, запишите значение IP адреса, маски подсети и основного шлюза?

− Получает ли машина адрес DNS сервера автоматически?

− Если адрес DNS сервера вводится вручную, то какой адрес используется?

− Если на компьютере установлено несколько сетевых адаптеров, то в панели управления будут перечислены несколько сетевых подключений.

− Проверьте тип адаптера.

− Определите, принимает ли Windows такую конфигурацию. Для этого откройте окно командной строки и введите следующую команду: IPCONFIG /ALL.

− Определите правильный сетевой адаптер. В этом случае определение нужного адаптера довольно простое, поскольку в списке есть всего лишь один адаптер.

− Отправьте ping запрос на адрес локального узла. Существует два различных способа того, как это сделать. Одним способом является ввод команды: PING LOCALHOST.

− Введите команду Nslookup, за которой должно идти полное доменное имя удаленного узла. Команда Nslookup должна суметь разрешить полное доменное имя в IP адрес.

− Необходимо просканировать клиентскую машину на предмет вредоносного ПО. Если на машине не обнаружено вредоносного ПО, сбросьте DNS кэш путем ввода следующей команды: IPCONFIG /FLUSHDNS.

Практическая 7 Преобразование форматов IP-адресов. Расчет IP-адреса и маски подсети

Цель работы: определение класса и расчет IP-адреса и маски подсети

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

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, являют-

ся 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 (рис.15).

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	

Рисунок 15

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 *вну- тренним 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, указан- ным 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 мо- гут 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 стро- иться как объединение подсетей. При этом организация должна получить один сетевой номер.

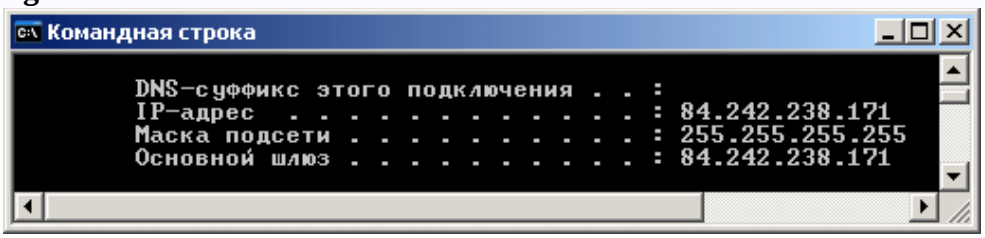
ПРАКТИЧЕСКАЯ ЧАСТЬ

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 WindowsXP 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.

- 131.107.256.80
- 222.222.255.222
- 31.200.1.1
- 126.1.0.0
- 190.7.2.0
- 127.1.1.1
- 198.121.254.255
- 255.255.255.255

Практическая работа №8 Настройка удаленного доступа к компьютеру

Цель работы: получение практических навыков по настройке удаленного доступа к компьютеру

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Удаленный рабочий стол соединяет два компьютера по сети или через Интернет. После подключения рабочий стол удаленного компьютера будет выглядеть так, словно вы сидите прямо перед ним, и вы сможете получить доступ ко всем его программам и фай- лам.

Эта функция предусмотрена во всех выпусках Windows 7, но подключиться можно только к компьютерам с Windows 7 Профессиональная, Максимальная или Корпоративная.

Удаленный доступ — функция, дающая пользователю возможность подключаться к компьютеру с помощью другого устройства через интернет практически отовсюду. Пользователь работает с файлами и программами точно так же, как если бы он находился возле этого компьютера. Особенно пригодится эта функция тем компаниям, где большинство сотрудников находится за пределами офиса, на частичном фрилансе, аутсорсинге или в командировках, но при этом они нуждаются в обновлении рабочей информации, просмотре корпоративной почты и пр. Им не нужно будет скачивать все необходимые для работы данные на внешний носитель или отправлять их по почте — достаточно связаться с офисным компьютером. Удаленный доступ используют системные администраторы для управления системой и устранения сбоев в ее работе, и руководители, желающие проконтролировать процесс выполнения задачи своими подчиненными. Применяется он и для

дистанционного обучения в образовательных учреждениях.

ПРАКТИЧЕСКАЯ ЧАСТЬ

− Выберите **Пуск > Панель управления > Система > Настройка удаленного доступа.**

− В разделе «Удаленный рабочий стол» выберите переключатель **Разрешать подключения только от компьютеров с удалённым рабочим столом с сетевой проверкой подлинности (безопаснее)**. Если появится сообщение о том, что на компьютере настроен переход в спящий режим, перейдите по ссылке **Электропитание**, измените значение на **Никогда** и нажмите кнопку «Сохранить изменения». Нажмите кнопку **ОК**, чтобы закрыть предупреждение. Нажмите кнопку **Применить** в окне «Свойства системы».

− В разделе «Удаленный рабочий стол» нажмите кнопку Выбрать пользователей. У какого пользователя уже есть удалённый доступ? Поскольку вы будете использовать эту учётную запись для получения удалённого доступа, нажмите кнопку Отмена, не добавляя пользователей.

− Выберите Пуск > Панель управления > Брандмауэр Windows > Изменить параметры. Убедитесь, что выбран переключатель **Включить (рекомендуется)**, и нажмите кнопку **ОК**. Закройте панель управления, окно «Брандмауэр Windows» и перейдите на Компьютер 1.

− Начните сеанс на Компьютере 1 под учётной записью администратора или участника группы администраторов. Имя пользователя узнайте у преподавателя. Выберите Пуск > Все программы > Стандартные > Подключение к удаленному рабочему столу. Откроется окно «Подключение к удаленному рабочему столу». Введите Computer2 (Компьютер 2) в поле «Компьютер» и нажмите кнопку Подключить. В поле «Имя пользователя» введите имя учётной записи, под которой вы начинали сеанс на Компьютере 2. Например: John_Computer2. В поле «Пароль» введите пароль для пользователя. Примечание. Учётная запись пользователя должна иметь пароль. ажмите кнопку ОК.

− На Компьютере 1 правой кнопкой мыши щёлкните рабочий стол Компьютера 2, выберите Создать > Папку и назовите папку Remote Permission (Разрешение удалённого доступа). Правой кнопкой мыши щёлкните папку Remote Permission (Разрешение удалённого доступа) и последовательно выберите Общий доступ > Дополнительный общий доступ > Общий доступ к папке, сохраните имя по умолчанию Remote Permission (Разрешение удалённого доступа) и нажмите кнопку «ОК».

− Перейдите на вкладку Безопасность. Убедитесь, что в списке для Компьютера 2 есть имя пользователя с Компьютера 1. В противном случае создайте и добавьте имя пользователя. Последовательно нажмите кнопки ОК > Закрыть. Выберите Пуск > Отключить.

− Начните сеанс на Компьютере 2.

− Выберите Пуск > Панель управления > Система > Настройка удаленного доступа. Обратите внимание, что компонент «Удаленный помощник» активирован по умолчанию. Нажмите кнопку Дополнительно. Откроется окно «Параметры удаленного помощника». Убедитесь, что установлен флажок Разрешить удалённое управление этим компьютером, установите для приглашения значение 1 ч., установите флажок Создавать приглашения только для компьютеров с системой Windows Vista или новее и нажмите кнопку ОК. Когда откроется окно «Свойства системы», нажмите кнопку Применить.

− На Компьютере 2 выберите Пуск > Все программы > Обслуживание > Удаленный помощник Windows. Появится окно «Запросить или предложить помощь?». Выберите Пригласить того, кому вы доверяете, для оказания помощи. Появится окно «Каким образом пригласить кого-нибудь на помощь?». Какими способами можно связаться с помощником? Выберите Сохранить приглашение как файл. Появится окно «Сохранить приглашение как файл». Нажмите кнопку Обзор.

− Найдите общую папку "Remote Permission" (Разрешение удалённого доступа) и назовите файлInvitation to Computer1 (Приглашение на Компьютер 1). Ка кой тип расширения у файла? Нажмите кнопку Сохранить Когда появится окно «Сохранить приглашение как файл», введите пароль HelpMe и подтвердите пароль HelpMe. Нажмите кнопку Готово. Когда появится окно «Ожидание входящего подключения», нажмите кнопку Параметры. Какую клавишу нужно нажать для прекращения совместного управления? Какие функции отключены при среднем уровне использования пропускной способности? Нажмите кнопку ОК.

− На Компьютере 1 выберите Пуск > Сеть и дважды щёлкните Computer2 (Компьютер 2). Начните сеанс с учётной записью пользователя с Компьютера 1. Дважды щёлкните папку Remote Permission (Разрешение удалённого доступа) на Компьютере 2. Дважды щёлкните файл Invitation to Computer1 (Приглашение на Компьютер 1). Откроется окно «Удаленный помощник Windows». Введите пароль HelpMe. Нажмите кнопку ОК.

− На Компьютере 2 нажмите кнопку Да, чтобы разрешить доступ к компьютеру.Активируйте окно Удаленный помощник Windows – вам помогает John_Computer1, выбрав его. Выберите Разговор. В поле разговора введите Hi John_Computer1, my optical drive will not work (Здравствуйте, John_ Computer1, мой оптический диск не работает). Нажмите кнопку Отправить.

− На Компьютере 1 в главном меню удаленного помощника Windows нажмите кнопку Запросить управление.

На Компьютере 2 установите флажок **Позволить John_Computer1 отвечать на запросы службы контроля учётных записей.** Нажмите кнопку **Да.**

На Компьютере 1 выберите окно «Свойства системы» для Компьютера 2. **Примечание.** Если окно «Свойства системы» для Компьютера 2 закрыто, откройте его, прежде чем продолжить. Перейдите на вкладку **Оборудование** и выберите **Диспетчер устройств**. Правой кнопкой мыши щёлкните оптический диск, отмеченный **чёрной стрелкой вниз**. Выберите **Включить**. В главном меню удаленного помощника Windows нажмите кнопку **Прекратить общий доступ**. В главном меню удаленного помощника Windows нажмите кнопку **Отключить**. Нажмите кнопку **Да**. Закройте все открытые окна и выйдите из системы на Компьютере 1.

На Компьютере 2 нажмите кнопку **Да**. Щёлкните **Диспетчер устройств**, чтобы активировать его. Отмечен ли оптический диск чёрной стрелкой? Закройте окно диспетчера устройств и окно «Удаленный помощник Windows». Удалите папку «Разрешение удаленного доступа». Выберите окно «Свойства системы». Установите флажок **Не разрешать подключения к этому компьютеру** и нажмите кнопку «ОК».

Литература

Основные источники

1. Максимов, Н. В. Компьютерные сети: учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 464 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-454-0. - Текст: электронный. - URL: https://znanium.com/catalog/product/1189333 (дата обращения: 01.06.2021). – Режим доступа: по подписке.

Дополнительные источники

1. Кузин, А. В. Компьютерные сети: учебное пособие / А.В. Кузин, Д.А. Кузин. — 4-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2020. — 190 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-453-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/1088380 (дата обращения: 01.06.2021). – Режим доступа: по подписке.
2. Исаченко, О. В. Программное обеспечение компьютерных сетей: учебное пособие / О.В. Исаченко. — 2-е изд., испр. и доп. — Москва: ИНФРА-М, 2020. — 158 с. — (Среднее профессиональное образование). - ISBN 978-5-16-015447-3. - Текст: элек- тронный. - URL: https://znanium.com/catalog/product/1033087 (дата обращения: 01.06.2021). – Режим доступа: по подписке.

Интернет-источники

1. Электронная библиотечная система Znanium: сайт.- URL: https://znanium.com/ –Текст: электронный.
2. Электронная библиотечная система Юрайт: сайт. - URL: https://urait.ru/ -Текс: электронный.