**Филиал федерального государственного бюджетного образовательного учреждение высшего образования «Университет «Дубна» -**

**Лыткаринский промышленно-гуманитарный колледж**

УТВЕРЖДАЮ

Зам. директора филиала

по учебно-методической работе

\_\_\_\_\_\_\_\_\_\_\_\_ Аникеева О.Б.

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2024 г.

**Фонд оценочных средств**

по профессиональному модулю

**ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих**

*Выполнение работ по профессии 06.026 Системный администратор информационно-коммуникационных систем*

Специальности

**09.02.06 Сетевое и системное администрирование**

Квалификация выпускника - **системный администратор**

Форма обучения - очная

Лыткарино, 2024

Составители (разработчики) фонда оценочных средств:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

*подпись*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

*подпись*

Фонд оценочных средств рассмотрен на заседании цикловой методической (предметной) комиссии технологических дисциплин.

Протокол заседания № \_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_ 2024г.

Председатель цикловой методической (предметной) комиссии Силяева Н.П. \_\_\_\_\_\_\_\_\_\_\_\_

*подпись*

Представитель работодателя

М.А. Непомнящий,

директор по программному обеспечению,

ООО Фирма «Рассвет Гагаринское Отделение» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(подпись) М.П.*

«\_\_\_» \_\_\_\_\_\_\_\_ 2024г.

**I.Паспорт оценочных средств**

Комплект оценочных средств предназначен для проверки результатов освоения профессионального модуля ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих основной профессиональной образовательной программы по специальности 09.02.06 Сетевое и системное администрирование.

|  |  |  |
| --- | --- | --- |
| Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля | Критерии оценки | Методы оценки |
| ПК 4.1. Выполнение работ по выявлению и устранению типичных инцидентов информационно-коммуникационных систем | Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.  Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.  Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию. | Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием  Защита отчетов по практическим и лабораторным работам |
| ПК 4. 2. Выполнение работ по управлению стандартными изменениями в технических и программных средствах информационно-коммуникационных систем по инструкции | Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.  Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.  Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию. | Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием  Защита отчетов по практическим и лабораторным работам |
| ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различными контекстам | Подбор вариантов решения конкретной профессиональной задачи или проблемы | Оценка полноты перечня подобранных вариантов |
| ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности | Демонстрация навыков использования информационных порталов в сети Интернет, включая официальные информационно-правовые порталы | Оценка полноты перечня подобранных вариантов |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях | Демонстрация интереса к выбранной специальности, к инновационным технологиям в области профессиональной деятельности | Участие в мероприятиях (олимпиады, конкурсы профессионального мастерства, стажировки и др.), проводимых как образовательным заведением, так и ведущими предприятиями отрасли |
| ОК 04. Эффективно взаимодействовать и работать в коллективе и команде | Демонстрировать навыки межличностного общения с соблюдением общепринятых правил со сверстниками в образовательной группе, с преподавателями во время обучения, с руководителями производственной практики | Экспертное наблюдение поведенческих навыков в ходе обучения |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста | Демонстрация навыков грамотной устной и письменной речи | Экспертное наблюдение навыков устного и письменного общения в ходе обучения |
| ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения | Формирование чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению;  взаимного уважения, бережного отношения к культурному наследию и традициям многонационального народа Российской Федерации;  нетерпимости к коррупционным проявлениям | Участие в мероприятиях патриотической направленности, в проведении военно-спортивных игр; участие в программах антикоррупционной направленности |
| ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях | Формирование бережного отношения к природе и окружающей среде | Экспертное наблюдение демонстрации навыков соблюдения правил экологической безопасности в ведении профессиональной деятельности; формирование навыков эффективных действий в чрезвычайных ситуациях |
| ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности | Формирование бережного отношения к здоровью | Участие в спортивных мероприятиях, проводимых образовательным учреждением; ведение здорового образа жизни |
| ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках | Демонстрация умения составлять тексты документов, относящихся к профессиональной деятельности, на государственном и иностранном языках | Экспертная оценка соблюдения правил составления документов |

**II. КОМПЛЕКТ МАТЕРИАЛОВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ**

Практические занятия – 80 ч

**Практическое занятие №1 (4 ч).**

Создание карты сети добавление сетевых устройств (для облегчения поиска используется сканирование сети), рисование линий-связей между устройствами, рисование областей для объединения устройств в группы. Использование линий, областей.

**Цель:** закрепление изученного материала по организации межсетевого взаимодействия

**Задание.** Построить сеть с использованием маршрутизаторов, коммутаторов и оконечного оборудования с обеспечение шлюза.

Ниже на рис.1 приведена спроектированная сеть, которая включает в себя следующее оборудование:

Маршрутизаторы; Коммутаторы; ПК; IP-телефоны; Сервер.

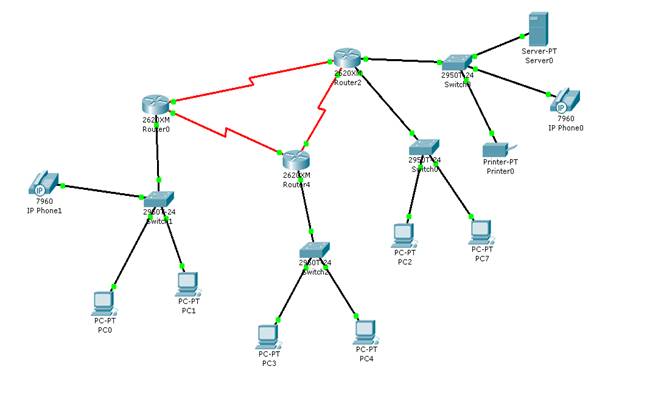
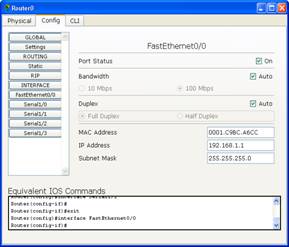
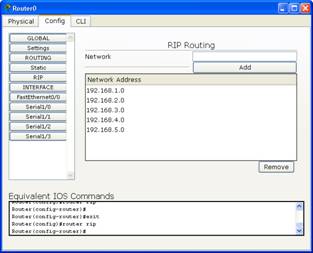


Рис. 1. Результат построения сети

Маршрутизаторы соединяются между собой при помощи DCE – кабеля. В данной сети маршрутизаторы используют RIP – протокол для осуществления передачи данных между различными подсетями(рис. 2).



|  |  |
| --- | --- |
| Рис. 2. Список подсетей | Рис. 3. Назначение IP-адреса маршрутизатору |

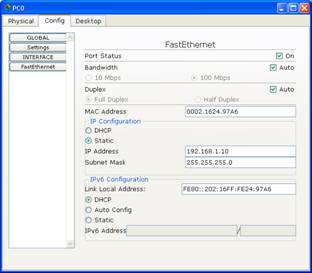
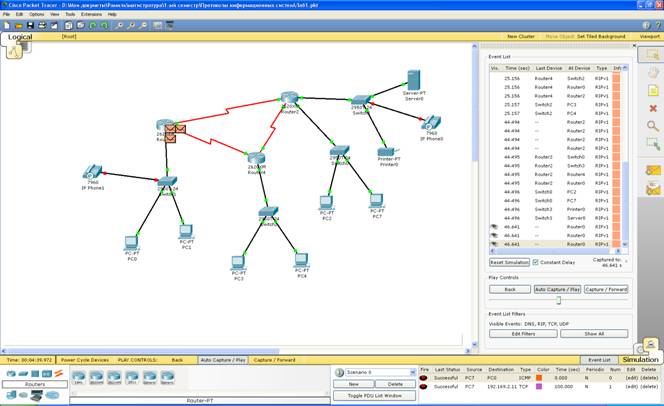


Рис.4. Назначение IP-адреса ПК



При этом, IP-адреса назначаются статически для маршрутизаторов и оконечного оборудования (рис. 3, 4).

**Задание:**

1.  Построить аналогичную сеть. Сеть должна быть работоспособной на 100%;

2.  В отчет необходимо включить таблицу следующего характера:

|  |  |  |  |
| --- | --- | --- | --- |
| № п. п. | Наименование оборудования | IP – адрес | MAC - адрес |
|  |  |  |  |
|  |  |  |  |

3.  Отправить пакеты по маршрутам представленным в таблице через команду ping, результат записать в таблицу.

|  |  |  |  |
| --- | --- | --- | --- |
| № п. п. | Маршрут отправки | Команда | Полученный результат |
| 1 | **S1 => PC-PT PC4** |  |  |
| 2 | **S3 => PC-PT PC2** |  |  |
| 3 | **S1 => PC-PT PC4=> PC-PT PC1** |  |  |
| 4 | **S1 => S3** |  |  |
| 5 | **S3 => PC-PT PC3** |  |  |
| 6 | **S2 => 7960 IP Phone0** |  |  |

4.  Полученный отчет показать преподавателю.

**Контрольные вопросы**

* + - 1. Опишите параметры, используемые при настройке статического адреса TCP/IP.

1. Какие преимущества дает применение стека протоколов TCP/IP .
2. Дайте определение понятию стек протоколов TCP/IP.

**Практическое занятие №2 (2 ч)**

Транспортная аналогия для сетей с коммутацией пакетов и каналов

Количественное сравнение задержек

Ethernet — пример стандартной технологии с коммутацией пакетов

**Цель работы.** Получить навыки выбора оборудования, кабельной системы для построения инфраструктуры локальной вычислительной сети уровня предприятия по технологии Ethernet с использованием пакета NetCracker.

**Теоретическая справка.**

Физический уровень Fast Ethernet имеет состоит из трех подуровней:

* подуровень согласования (reconciliation sublayer);
* независимый от среды интерфейс (Media Independent Interface, MII); устройство физического уровня (Physical layer device, PHY).

Устройство физического уровня (PHY) обеспечивает кодирование данных, поступающих от MAC-подуровня, для передачи их в среду определенного типа, синхронизацию передаваемых данных, а также прием и декодирование данных в узле-приемнике. Интерфейс MII поддерживает независимый от используемой физической среды способ обмена данными между MAC-подуровнем и подуровнем PHY. Подуровень согласования предназначен для согласования работы подуровня MAC с интерфейсом MII.

В таблице 1 приведены основные характеристики сетей Fast Ethernet.

Таблица 1 - Основные характеристики сетей Fast Ethernet

|  |  |  |  |
| --- | --- | --- | --- |
| Спецификация физического уровня | 100BASE-TX | 100BASE-FX | 100BASE-T4 |
| Скорость передачи данных, Мб/с | 100 | 100 | 100 |
| Передача данных | Узкополосная | Узкополосная | Узкополосная |
| Тип среды передачи | UTP cat. 5 | ВОК | UTP cat. 3, 4, 5 |
| Топология | Звезда | Звезда | Звезда |
| Максимальная длина сегмента, м | 100 | 412 (полудуплекс)  2000 (дуплекс) | 100 |
| Максимальное количество абонентов в сегменте | 1024 | 1024 | 1024 |
| Максимальный диаметр сети, м | 205 | 272 | 200 |

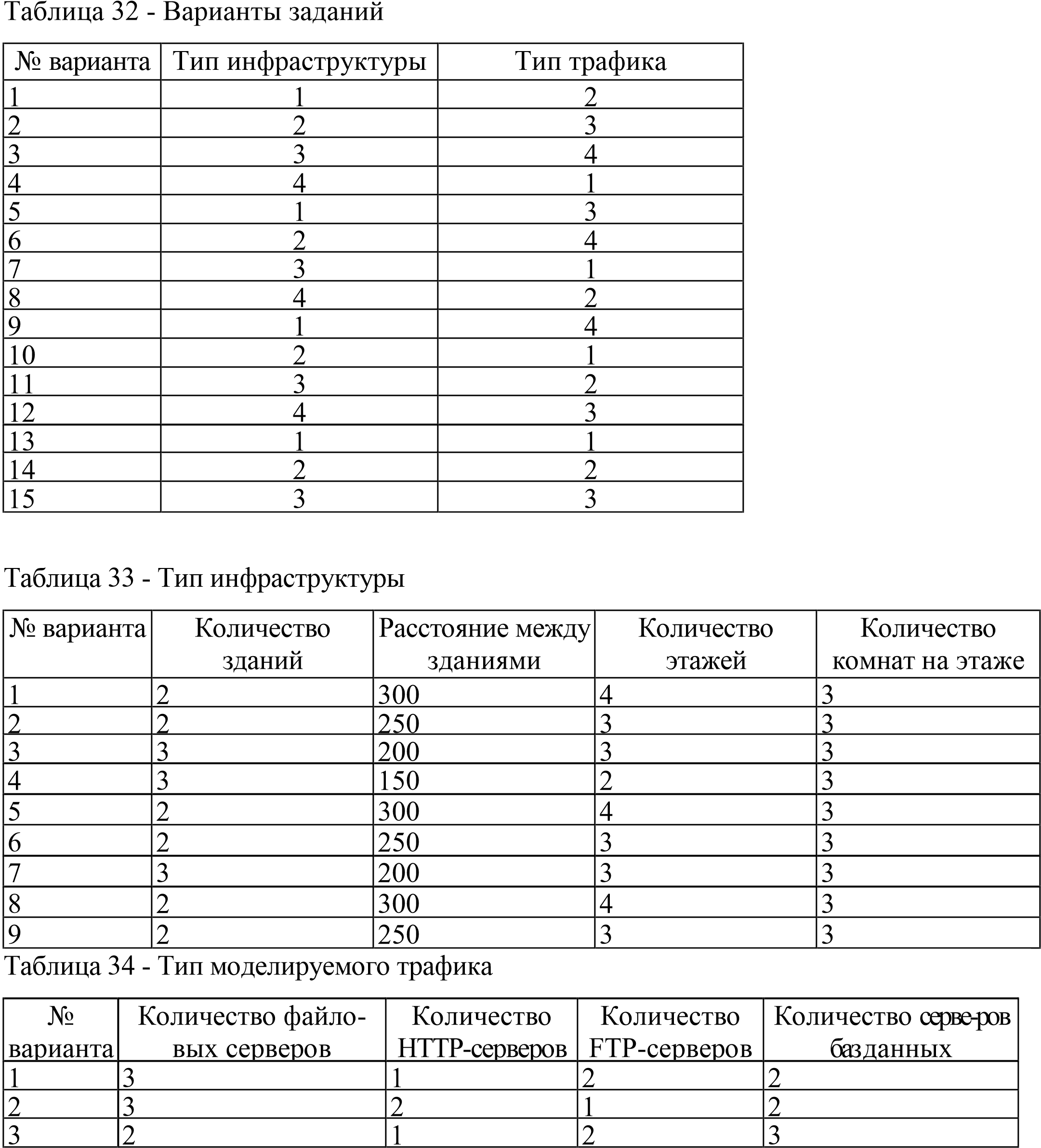
Технология Fast Ethernet рассчитана на подключение конечных узлов – компьютеров с соответствующими сетевыми адаптерами – к многопортовым концентраторам (повторителям) или коммутаторам.

**Задание на выполнение работы**

1. Используя пакет NetCracker, изучить состав и функциональные характеристики типового оборудования локальных сетей на основе технологии

Ethernet.

1. В соответствии с вариантом задания построить сеть предприятия с использованием технологий Ethernet и Fast Ethernet, исходя из расчета минимизации стоимости проектируемой сети.
2. Для полученной модели сети задать необходимые типы потоков данных между рабочими станциями и серверами и произвести имитационное моделирование работы сети.
3. Проанализировать среднюю загрузку сетевого оборудования и среды передачи данных и время ответа для потока данных. Указать участки сети, уязвимые к перегрузкам, и определить средства повышения надежности функционирования сети.



**Практическое занятие №3 (2 ч)**

Стандартные стеки коммуникационных протоколов

Соответствие популярных стеков протоколов модели OSI

IETF, RFC

**Цель:** закрепление изученного материала по организации межсетевого взаимодействия

**Задание.** Построить сеть с использованием маршрутизаторов, коммутаторов и конечного оборудования с обеспечение шлюза.

**Практическое занятие №4 (4 ч)**

Обжим витой пары, Стандарты 568А, 568Б

Оборудование, инструменты для монтажа локальной сети. Тестирование

Монтаж розеток RJ45 (одиночных, двойных), демонтаж RJ45 (одиночных, двойных). Тестирование

**Цели:** обобщить и систематизировать знания по теме «Монтаж кабельных сред технологий Ethernet».

**Теоретический материал**

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 1.** Конструкция коаксиального кабеля

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. 1). 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:**

**1. 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.

**2. Толстый коаксиальный кабель -** относительно жесткий кабель с диаметром около 1 см. Иногда его называют «стандартный Ethernet», поскольку он был первым типом кабеля, применяемым в Ethernet — популярной сетевой архитектуре. Медная жила толстого коаксиального кабеля больше в сечении, чем тонкого, поэтому он передает сигналы на расстояние до 500 м. Толстый коаксиальный кабель иногда используют в качестве основного кабеля, который соединяет несколько небольших сетей, построенных на тонком 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 2), BNC T коннектор (рисунок 3) и BNC баррел коннектор.



Рисунок 2. BNC коннектор



Рисунок 3. BNC T коннектор

**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.

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 5e** 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.

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

**Кросс-разводка**– применяется для соединения ПК друг с другом.

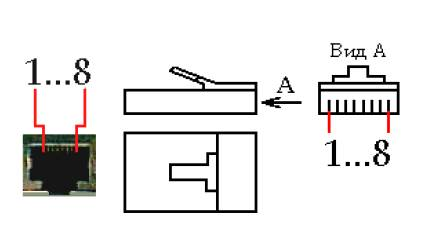


Рисунок 4. Порт MDI/MDI-X и разъем RJ-45

Таблица 1. Прямая разводка кабеля

|  |  |
| --- | --- |
| № контакта коннектора | Цвет проводника |
| 1. | Бело-зеленый |
| 2. | Зеленый |
| 3. | Бело-оранжевый |
| 4. | Синий |
| 5. | Бело-синий |
| 6. | Оранжевый |
| 7. | Бело-коричневый |
| 8. | Коричневый |

Таблица 2. Кросс-разводка кабеля

|  |  |  |
| --- | --- | --- |
| № контакта коннектора | Первый конец | Второй конец |
| 1. | Бело-зеленый | Бело-оранжевый |
| 2. | Бело-синий | Оранжевый |
| 3. | Бело-оранжевый | Бело-зеленый |
| 4. | Синий | Синий |
| 5. | Бело-синий | Бело-синий |
| 6. | Оранжевый | Бело-синий |
| 7. | Бело-коричневый | Бело-коричневый |
| 8. | Коричневый | Коричневый |

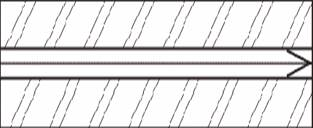
После подключения коннекторов кабель следует проверить с помощью специального тестера, который определит, правильно ли проводники витых пар подсоединены к контактам коннекторов, а также целостность самого кабеля.

**Назначение и функции оптоволокна.** 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 5. Структура оптоволоконного кабеля: 1 – сердцевина с показателем преломления n1; 2 – отражающая оболочка с показателем преломления n2, n1>n2; 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 называются модами, а волокно, поддерживающее несколько мод - многомодовым. По одномодовому волокну распространяется только один луч.



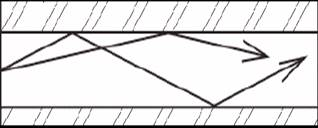
Рисунок 6. Одномодовое оптоволокно

Рисунок 7. Многомодовое оптоволокно

**Задания к работе**

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

**Контрольные вопросы:**

1. Коаксиальный кабель: назначение и структура.

2. Неэкранированная витая пара: назначение и структура.

3. Экранированная витая пара: назначение и структура.

4. Оптоволоконный кабель: назначение и структура.

**Практическое занятие №5 (2 ч)**

Кодирование

Характеристики физических каналов

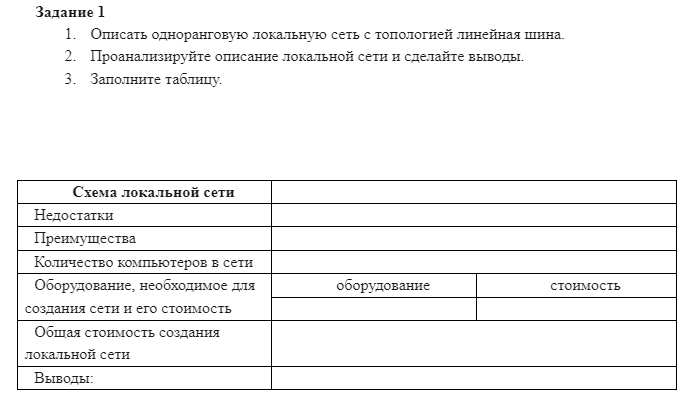
Проблемы связи нескольких компьютеров

Топология физических связей

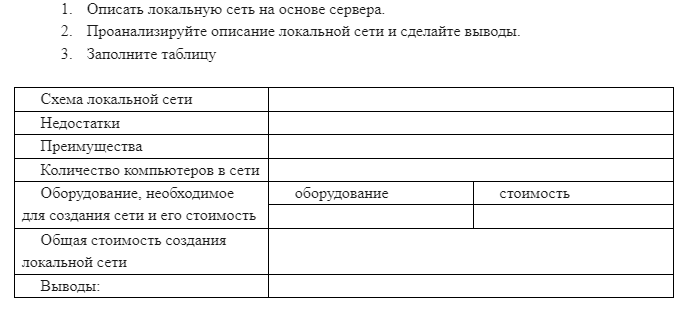
Адресация узлов сети

Коммутация

**Цель работы:** применить на практике знания о назначении, принципах работы и функционирования локальных компьютерных сетей



**Задание 2**



**Практическое занятие №6 (4 ч)**

Подключение беспроводной сетевой карты. Подключение и настройка Wi-Fi роутера

**Задания:**

1. Ответить на тестовые вопросы:

1.1. Стандарты WiFi, обеспечивающие передачу данных со скоростью 54 Мбит/с

* 802.11a
* 802.11g
* 802.11e
* 802.11n

1.2.При работе в каком режиме в сети WiFi требуется точка доступа?

* режим инфраструктуры (Infrastructuremode)
* режим эпизодической сети (AdHocmode)
* режим прямого обмена (DirectConnect)
* режим точка-точка (Point-to-Point)

1.3.На частоте 2,4 ГГц работает беспроводное оборудование, поддерживающее стандарт(ы)

* 802.11a
* 802.11g
* 802.11e
* 802.11n

1.4.Стандарт Bluetooth используется для построения…

* персональных сетей (PAN)
* локальных сетей (LAN)
* глобальных сетей (WAN)
* региональных сетей (MAN)

1.5.Инфракрасное излучение подвержено помехам со стороны…

* дождя
* солнечных бликов
* окон
* радиоволн

1. Подготовить ответы на контрольные вопросы по теме:

2.1. Какие беспроводные способы передачи данных существуют?

2.2. Опишите область применения группы стандартов 802.11.

2.3. Для чего используются беспроводные маршрутизаторы?

2.4. Опишите стандарты безопасности, применяемые для построения беспроводных сетей?

2.5. Как увеличить зону охвата беспроводной сети, построенной на базе стандартов 802.11a/g/n?

**Практическое занятие №7 (6 ч)**

Создание локальной сети с использованием сетевого оборудования. Подключение по различным топологиям

**Цель:**обобщение и систематизация знаний по теме «Удаленный доступ к компьютеру»

**Задания к работе**

* 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. 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.

11. 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**

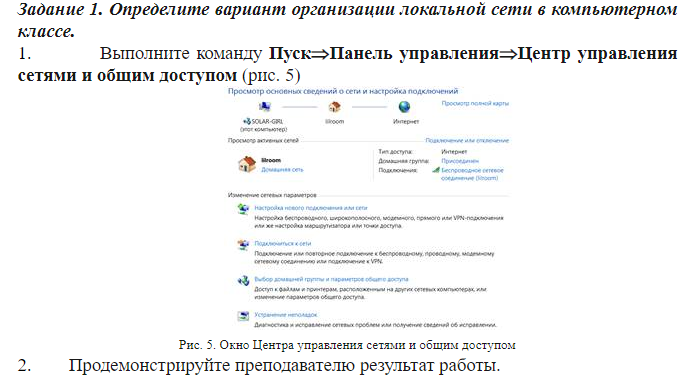
1. Поясните, что может означать, если время TTL закончилось до получения ответа.
2. Как подтвердить наличие сетевого соединения?
3. Что показывает команда IPCONFIG /ALL?
4. Что означает наличие IP адрес со значением 0.0.0.0.?
5. С помощью какой команды можно проверить то, что конфигурация IP адреса работает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

**Практическое занятие №8 (2 ч)**

Виртуальные локальные сети

**Цель работы**: ознакомиться с вариантами организации локальных компьютерных сетей.

**Ход выполнения работы:**



**Практическое занятие №9 (2 ч)**

Структура стека протоколов TCP/IP

Типы адресов стека TCP/IP

Формат IP-адреса

Порядок назначения IP-адресов

Система DNS

Протокол DHCP

**Цель работы**: изучить принципы работы протоколов TCP/IP и научиться их настраивать для работы в сети Интернет.

**Теоретическая справка**

Хотя Windows поддерживает большое количество сетевых протоколов, TCP/IP используется чаще всего по целому ряду причин:

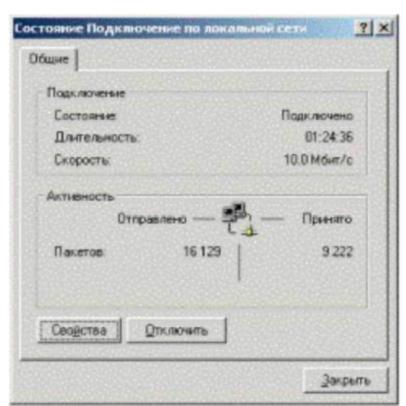
* обеспечивает межсетевое взаимодействие компьютеров с разной аппаратной архитектурой и операционными системами;
* является основным протоколом, используемым в сети Интернет;  
  необходим для функционирования Active Directory.

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.

В Windows параметры протокола TCP/IP являются частью параметров настройки сетевого адаптера, поэтому все изменения, связанные с этим протоколом, осуществляются через Панель управления.

Для настройки сетевых адаптеров и протоколов дважды щелкните значок ***Сеть и удаленный доступ к сети*** в ***Панели управления.***

В появившемся окне представлены различные соединения вашего компьютера с внешним миром. После успешной установки сетевого адаптера (во время установки или позже) в окне должен присутствовать как минимум один значок с именем *Подключение по локальной сети.*

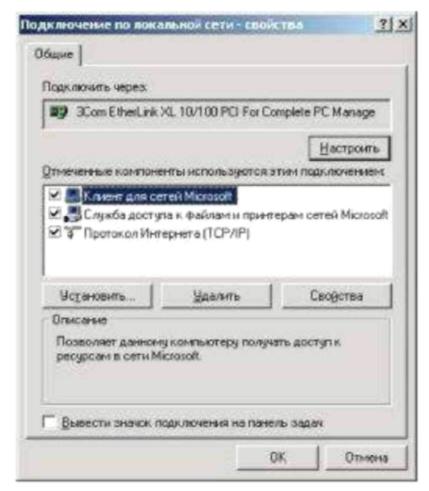


Двойной щелчок значка выводит окно с информацией о состоянии соединения. Можно узнать длительность соединения, его скорость, количество отправленных и принятых пакетов данных.

Кнопка ***Отключить*** позволяет выключить сетевой адаптер, прекратив тем самым обмен данными через него. Аналогичная команда доступна в контекстном меню, вызываемом щелчком правой кнопкой мыши значка соответствующего соединения. Отключенные соединения отображаются в виде "серых" значков.

Кнопка *Свойства* вызывает окно настройки свойств соединения, в том числе и параметров используемых протоколов. Аналогичная команда доступна в контекстном меню, вызываемом щелчком правой кнопкой мыши значка соответствующего соединения.

В этом окне можно получить информацию о сетевом адаптере, через который осуществляется соединение. Щелкнув кнопку *Настроить,* вы откроете окно свойств сетевого адаптера и сможете их изменить.



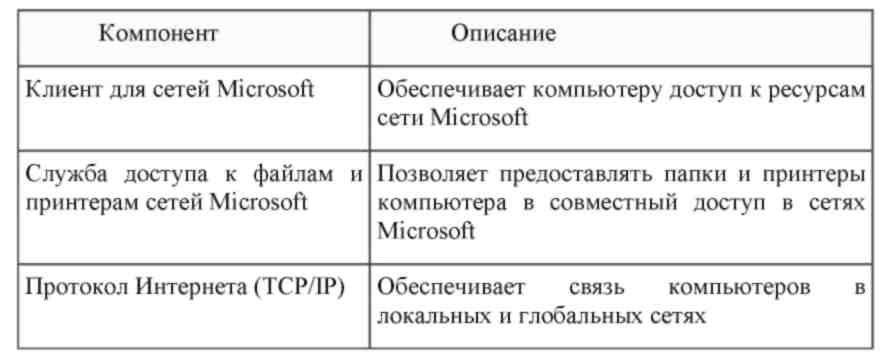
Установив флажок *Вывести значок подключения на панель задач,* вы включите отображение значка, представляющего соединение, на панели задач Windows. Это позволит наблюдать за активностью соединения и быстро осуществлять его настройку, не используя *Панель управления.*

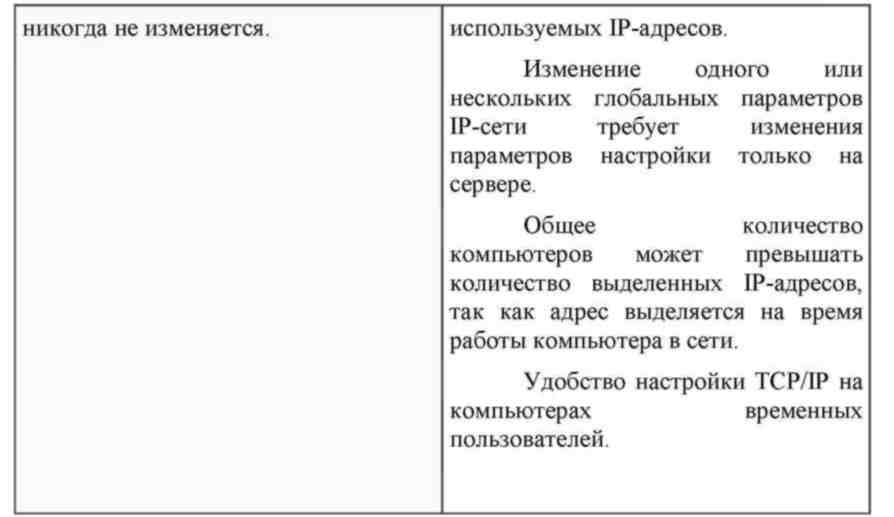
В центральной части окна в списке представлены все клиенты, службы и протоколы, связанные соединением Для нормального функционирования домена или рабочей группы Windows необходимо наличие следующих компонентов

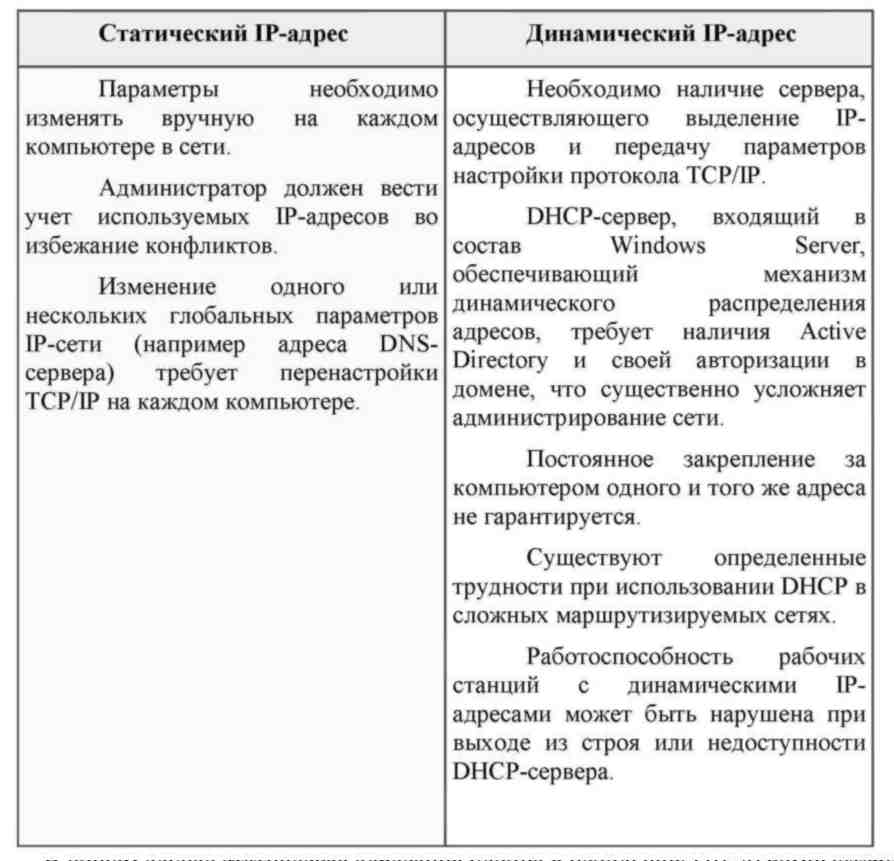
**Настройка основных параметров TCP/IP**

Стек протоколов TCP/IP, входящий в состав Windows, поддерживает два режима настройки: с использованием статического или динамического IP-адреса. Каждый из этих режимов имеет свои преимущества и недостатки и должен использоваться в зависимости от конфигурации вашей локальной сети:

Преимущества:





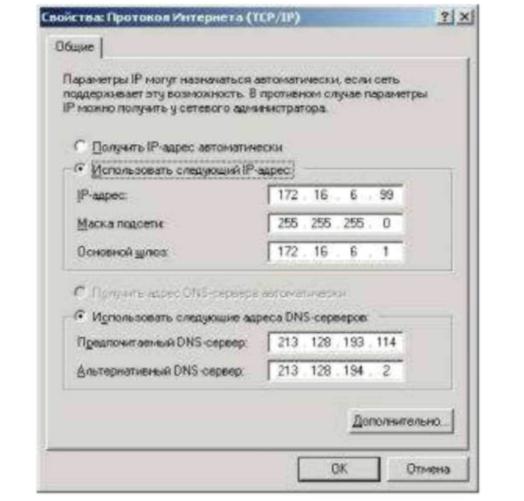


Недостатки:

В общем случае статическая адресация удобна в небольших (10-20 компьютеров) одноранговых сетях, состав которых редко изменяется. Если количество компьютеров в сети превышает 20, а компьютеры входят в домен Windows, гораздо проще и удобнее использовать динамическое выделение адресов.

**Использование статического IP-адреса**

По умолчанию Windows настраивает стек TCP/IP на использование динамически выделяемого IP-адреса. Чтобы использовать статический адрес, это необходимо указать в свойствах протокола TCP/IP. После этого вы должны задать следующие параметры.



***IP-адрес*** *-* 32-разрядный адрес, представленный в формате W.X.Y.Z. Адрес должен быть уникальным не только в пределах локальной, но и в пределах всего Интернета. Обычно используется один из IP-адресов, выделенный провайдером.

*Маска подсети -* 32-разрядное число, представленное в формате W.X.Y.Z, которое используется для разделение крупных сетей на несколько более мелких.

*Основной шлюз -* IP-адрес маршрутизатора, используемого для выхода в глобальные сети и взаимодействия с другими сетями.

***Предпочтительный и альтернативный*** *DNS-серверы -* IP-адреса основного и резервного DNS-серверов, которые будут использоваться стеком TCP/IP для разрешения символьных имен компьютеров в их IP-адреса.

Настроив параметры протокола, щелкните кнопку *ОК.* Для применения новых параметров TCP/IP щелкните кнопку *(Ж* в окне свойств соединения.

**Использование динамически выделяемого IP-адреса**

Для использование динамически выделяемого IP-адреса необходимо в настройках протокола TCP/IP указать автоматическое получение IP-адреса. Также рекомендуется указать автоматическое получение адресов DNS-серверов, хотя можно указать эту информацию вручную.

Для динамического выделения IP-адреса в локальной сети должен быть установлен и настроен DHCP-сервер.

При недоступности DHCP-сервера используется служба APIPA (автоматическая настройка частных LP-адресов), которая генерирует IP-адрес вида 169.254.Y.Z и маску подсети 255.255.0.0. Если выбранный адрес уже используется, служба генерирует следующий адрес.

**Отключение автоматической адресации**

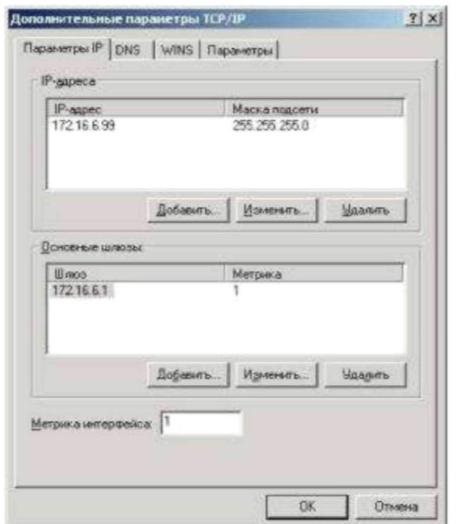
По умолчанию функция автоматической настройки частных IP-адресов включена, но можно ее отключить, добавив в системный реестр соответствующий параметр.



Чтобы изменения вступили в силу, необходимо перезагрузить компьютер.

**Настройка дополнительных параметров TCP/IP**

Стек протоколов TCP/IP в Windows достаточно сложен и позволяет настраивать  
множество дополнительных параметров. Доступ к ним можно получить, щелкнув  
кнопку *Дополнительно* в окне свойств протокола **TCP/IP.**



На вкладке ***Параметры IP*** можно связать с сетевым адаптером несколько LP-адресов и задать несколько основных шлюзов.

Стек TCP/IP Windows позволяет связать с любым сетевым адаптером несколько IP-адресов. Для каждого из адресов может быть задана своя маска подсети.

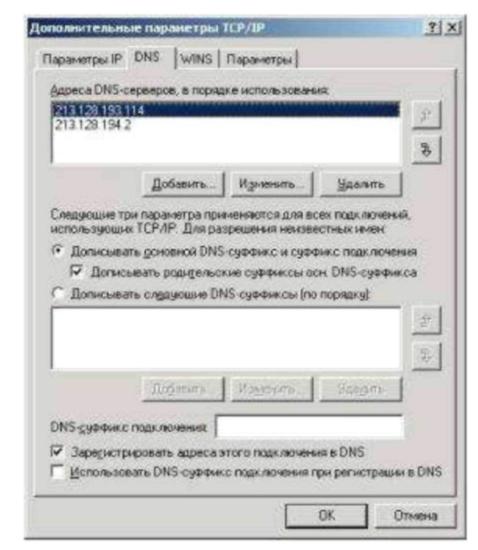
Несколько IP-адресов для одного сетевого адаптера принято использовать в следующих случаях:

- на web и ftp-серверах, обслуживающих большое количество сайтов, каждому из которых должен быть выделен отдельный ЕР-адрес;

- при подключении компьютера к локальной сети с несколькими наложенными IP-сетями; при постоянном перемещении компьютера из одной сети в другую.

Добавить адрес можно, щелкнув кнопку *Добавить.* Первый адрес из списка будет считаться основным и отображаться в окне основных свойств протокола TCP/IP. При использовании нескольких IP-адресов, особенно из разных сетей, необходимо указать несколько основных шлюзов, чтобы обеспечить возможность связи с компьютером извне по любому из связанных с ним адресов. Кроме того, для повышения надежности можно использовать несколько маршрутизаторов, соединяющих вашу сеть с другими. В этом случае имеет смысл указать в параметрах адреса нескольких основных шлюзов. Для каждого шлюза кроме его адреса задается метрика - целое число от 1 до 9999. Метрики служат для определения приоритета шлюзов. В любой момент времени используется первый доступный шлюз с минимальной метрикой. Таким  
образом, альтернативный шлюз с метрикой 2 будет использован только при  
недоступности основного с метрикой I.

Кроме того, можно задать метрику и самого интерфейса. Метрики интерфейсов служат для определения интерфейса, используемого для установления нового соединения. При использовании нескольких сетевых адаптеров метрики применяются для определения приоритета этих адаптеров.

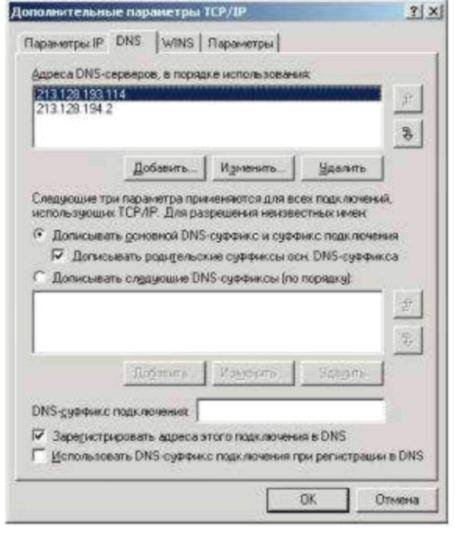


На вкладке *DNS* можно настроить все параметры, связанные со службой DNS. По аналогии с IP-адресами можно задать несколько (более двух) адресов DNS-серверов и определить порядок их использования. Метрики для определения порядка здесь не используются, т. к. при недоступности первого сервера будет использован второй, при недоступности второго - третий и т. д.

В работе DNS используются два параметра, отвечающие за разрешение неполных имен. Первый - основной суффикс DNS - задается на вкладке *Сетевая идентификация* свойств системы и обычно является полным DNS-именем домена, в который входит компьютер. При работе в рабочей группе этот суффикс может быть произвольным и задается при настройке Windows. Второй - DNS-суффикс подключения - задается на вкладке DNS свойств каждого подключения.

Если в параметрах настройки DNS указано *Дописывать основной DNS-суффикс и суффикс подключения,* то при разрешении неполных имен будет использованы соответствующие суффиксы. Например, при использовании основного суффикса [msk.net.fio.ru](http://msk.net.fio.ru/#_blank)и суффикса подключения [lab.msk.net.fio.ru](http://lab.msk.net.fio.ru/#_blank)при вводе команды **ping xyz** будет предпринята попытка разрешения имен [xyz.msk.net.fio.ru](http://xyz.msk.net.fio.ru/#_blank)и [xyz.lab.msk.net.fio.ru](http://xyz.lab.msk.net.fio.ru/#_blank)Кроме того, если включен параметр *Дописывать родительские суффиксы,* то при разрешении будут проверены еще и имена [xyz.net.fio.ru](http://xyz.net.fio.ru/#_blank), [xyz.fio.ru](http://xyz.fio.ru/#_blank) и [xyz.ru](http://xyz.ru/#_blank).

Если в параметрах настройки DNS указано *Дописывать следующие DNS-суффиксы,* то основной суффикс и суффикс подключения использованы не будут, а будет использован (последовательно) указанный список суффиксов. При разрешении неполных имен этот список будет использован аналогично приведенному примеру. Параметр *Зарегистрировать адреса* ***этого*** *подключения в DNS* использует основной DNS-суффикс для определения DNS-сервера, обеспечивающего функционирование соответствующей зоны, и автоматически регистрирует на нем запись А со своим именем и IP-адресом соединения. Если для соединения задано несколько IP-адресов или используется несколько соединений, то в DNS будут зарегистрированы несколько записей А с одним и тем же именем, но разными IP-адресами ■\*■. Параметр *Использовать DNS-суффикс подключения при регистрации в DNS* позволяет осуществить регистрацию соответствующей записи А на DNS-сервере по аналогии с предыдущим параметром.

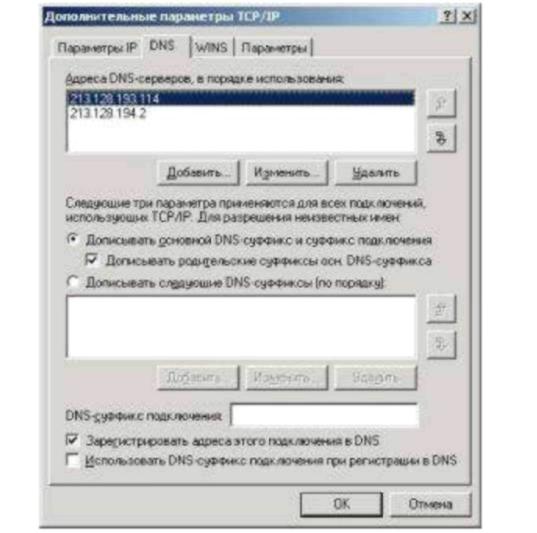


служба предназначена для разрешения имен NetBIOS в IP-адреса. При использовании домена и клиентов Windows использование этой службы не требуется - все ее функции выполняются службой DNS.

Для работы этой службы требуется WINS-сервер, адрес (адреса) которого добавляется в соответствующий список.

Помимо использования WINS-сервера Windows поддерживает устаревший способ разрешения имен NetBIOS- файл LMHOSTS. Можно включить использование этого файла и при необходимости импортировать уже существующий файл. Файл LMHOSTS можно редактировать самостоятельно в любом текстовом редакторе. Этот файл расположен в папке **%systemroot%\ system32\drivers\etc**

Кроме того, на этой вкладке осуществляется управление поддержкой NetBIOS поверх TCP/IP. Такая поддержка требуется для обеспечения совместной работы со старыми NetBIOS-клиентами (Windows 9х, NT). При использовании в локальной сети только Windows, NetBIOS поверх TCP/IP может быть отключен. При использовании динамически выделяемого IP-адреса можно задавать этот параметр через DHCP.



На вкладке ***Параметры*** можно настроить ряд необязательных параметров стека TCP/IP. Windows поддерживает настройку IP-безопасности (протокол IPSec) и фильтрации TCP/IP. Для настройки необходимо выбрать параметр из списка и щелкнуть кнопку *Свойства.*

**Порядок выполнения работы**

1. Изучить состав и назначение протоколов стека TCP/IP.
2. В системе Windows выполнить настройку стека протоколов TCP/IP для организации работы в сети Интернет. Для этого получить необходимые данные у преподавателя.
3. Создать группу в сети. Добавить в эту группу несколько компьютеров.
4. Поэкспериментировать с настройками Firewall, (пропускание/блокирование ping, HTTP и др.)

**Контрольные вопросы:**

1. Сколько протоколов образуют стек TCP/IP?
2. Какие уровни протоколов содержит стек TCP/IP?
3. что такое IP - адресация?
4. На каком уровне применяется IP - адресация?
5. Является ли IP - адресация абсолютной или относительной?
6. Поясните понятия статический и динамический IP - адрес.
7. Что такое шлюз?
8. Что такое маршрутизатор?
9. Для чего применяется маска подсети?
10. Какие службы, устройства, клиенты необходимы для работы в сетях
11. Какие три основных вида угроз безопасности при работе в сети Internet?
12. Рассказать о каждой угрозе при работе в сети Internet.
13. Виды программ-паразитов (и в чем их различие)
14. Адресация в сети Internet.
15. Основные сетевые протоколы (TCP, IP, UDP, POP, SMTP, DNS, WINS, 1CMP, HTTP, FTP). Рассказать о любом по выбору преподавателя.
16. Какие средства сетевой защиты существуют?

**Практическое занятие №10 (2 ч)**

Структуризация сети масками одинаковой длины

Просмотр таблиц маршрутизации с учетом масок

Использование масок переменной длины

Перекрытие адресных пространств

CIDR и маршрутизация

**Цель работы.** Научиться организовывать заданное число подсетей с учетом вырожденной сети, используя маску подсети постоянной длины.

Решить задачу в соответствии с вариантом, используя изложенную ниже методику.

1. В Основном меню курсором выбрать закладку **"Задание № 1"**. В появившейся таблице исходных данных выбрать строку с соответствующим номером варианта, дважды щелкнув мышью по строке таблицы. Например – вариант - 1, число подсетей - 3. Это значит, что необходимо будет организовать 3 подсети + 1 вырожденная (соединяющая маршрутизаторы **М1** и **М2**).
2. В появившейся форме ввод во всех окнах ввода десятичной записи заканчивается щелчком "мыши" в соответствующем окна двоичной записи и наоборот. Ввести в окне **"Номер внутренней сети"** любой номер сети из диапазона IP-адресов класса B, например - 128.0.0.0. Щелкнуть в окне двоичной записи номера сети - в данном окне отобразится двоичная запись номера сети. Для получения информации о классах IP - адресов щелкнуть правой кнопкой "мыши" на окне ввода, в появившемся меню выбрать **"Класс В"**. Появится диапазон номеров сетей данного класса (Internet - адрес) и диапазон адресов, не обрабатываемых Internet - маршрутизаторами (локальных), которые нельзя использовать при выполнении задания.
3. Ввести в окне **"Маска подсети"** десятичное значение стандартной маски класса В. Информацию о стандартных масках можно получить, щелкнув правой кнопкой мыши на окне десятичной записи **"Маска подсети"**.

Определить маску, необходимую для образования заданного количества подсетей (в нашем примере 4-х).

Для этого:

* определить количество старших разрядов в поле номера узла, подлежащих маскированию, исходя из заданного количества подсетей (в этих разрядах маски должны быть установлены «1»);
* расписать в отчете в двоичном исчислении последовательный перебор номеров подсетей, подлежащих образованию, учитывая, что номер не может содержать все «0» или все «1».

В данном примере - это сочетание 001 010 011 100 101 110.

В нашем примере - это 3 единицы в старших разрядах поля номера узла, и маска должна иметь все единицы в поле номера сети и 3 единицы в старших разрядах поля номера узла.

**Теоретическая справка.**

Варианты значения масок подсетей, применяемых в данной работе:

* 255.255.0.0 11111111.11111111.00000000.00000000;
* 255.255.128.0 11111111.11111111.10000000.00000000;
* 255.255.192.0 11111111.11111111.11000000.00000000;
* 255.255.224.0 11111111.11111111.11100000.00000000;
* 255.255.240.0 11111111.11111111.11110000.00000000;
* 255.255.248.0 11111111.11111111.11111000.00000000;
* 255.255.252.0 11111111.11111111.11111100.00000000;
* 255.255.254.0 11111111.11111111.11111110.00000000; - 255.255.255.0 11111111.11111111.11111111.00000000.

В окне ввода маски в двоичном изображении отделить в старшем октете слева определенное количество разрядов (в примере - 3 разряда) и установить в выделенных разрядах «1». Для этого:

* щелкнуть «мышью» в окне двоичного ввода маски;
* используя клавиши управления курсором и клавишу **«BackSpace»** удалить «0» в соответствующих разрядах;
* используя клавишу «1» цифровой клавиатуры установить в разрядах единицы.

Щелкнуть «мышью» в окне ввода десятичной записи маски.

В окне **«Маска подсети»** появится десятичная запись маски. В нашем примере это - 255.255.224.0.

Заполнение таблицы маршрутизации маршрутизатора **М2**.

1. Щелкнуть по кнопке **«Запись»**. В окне **«Номера подсетей»** будут отображены номера организуемых подсетей кроме номера подсети, соединяющей маршрутизаторы (в нашем примере это - 128.1.64.0).
2. Щелкнуть по кнопке **«Таблица маршрутизации»**. Раскроется таблица маршрутизации. Щелкая «мышью» на соответствующей записи в окне **«Номера подсетей»**, а затем в пустой ячейке таблицы маршрутизации и, таким образом, подключить подсети к портам маршрутизатора (IP - адреса портов маршрутизатора назначаются программой автоматически). По мере заполнения таблицы маршрутизации записи в окне **«Номера подсетей»** удаляются. При ошибочном вводе значений в таблицу маршрутизации дважды щелкнуть «мышью» в редактируемой строке таблицы - строка в таблице пропадет и переместится на последнюю строчку окна **«Номера подсетей»**. При записи значений в таблицу маршрутизации поверх уже существующей строки последняя также удаляется из таблицы и добавляется в окно **«Номера подсетей»**. Для восстановления содержимого окна **«Номера подсетей»** щелкнуть по кнопке «**Запись»**. Подключение подсетей заканчивается щелчком по кнопке **«Таблица маршрутизации»**. Для удобства вырожденная сеть, соединяющая маршрутизаторы **М1** и **М2** всегда подключена к 1-му порту **М2** и имеет номер X.X.64.0, где Х.Х.0.0 - номер сети (в нашем примере - 128.1.0.0). Порт 2 маршрутизатора **М1** имеет IPадрес Х.Х.64.2, порт 1 **М2** - Х.Х.64.1. Остальным портам **М2** автоматически будут присвоены IP-адреса Y.Y.Y.1, где Y.Y.Y.0 - номер подключаемой к порту подсети (**пример** - подсеть 128.1.32.0 подключается к порту 2, IP-адрес порта 2 - 128.1.32.1).

Пошаговая отработка алгоритма работы маршрутизатора **М2** при продвижении произвольного IP-пакета.

1. В окне «Внешний IP – адрес» записать любой IP - адрес или выбрать из предложенных в выпадающем списке.

**Примечание.** При вводе IP - адресов учесть, что в программе недопустимы следующие их значения:

* Х.Х.Х.255;
* Х.Х.Х.0;
* Х.Х.Х.1 - (адреса портов маршрутизатора М2, Х.Х.Х - номер подсети).

IP - адреса вырожденной сети:

* Х.Х.64.1;  Х.Х.64.2.

Запрещены адреса в диапазоне - 172.16.0.0 - 172.31.255.255 (локальные адреса, не обрабатываемые Internet - маршрутизаторами).

1. Мысленно наложить маску на IP - адрес, ориентируясь по записям в окнах двоичного представления адреса и маски. Замаскированные разряды 3-го октета покажут номер подсети.

В описываемом примере введем IP - адрес 128.1.192.2.

Маска подсети 11111111.11111111.11100000.00000000.

IP - адрес 10000000.00000001.11000000.00000010.

1. В выпадающем окне двоичной записи номеров подсетей выбрать строку с ранее определенным адресом подсети - 10000000.00000001.11000000.00000000.

В окне **«Номер подсети»** появится десятичная запись номера подсети:

128.1.192.0.

Определить, имеется ли данная подсеть во внутренней сети, сравнив с номерами подсетей на мнемосхеме. Если внешний IP-адрес адресует пакет в одну из образованных подсетей, то определенный номер подсети, сформировавшийся в окне **«Номер подсети»** будет совпадать с одним из адресов, подключенных к порту маршрутизатора **М2**. Щелкнуть по кнопке **«Test»** для удостоверения в правильности определения номера подсети.

1. Вычесть значения полей окна двоичного представления номера подсети из соответствующих значений окна двоичного представления IP-адреса - полученное значение будет номером узла, который необходимо записать в окне двоичного представления номера узла. Щелкнуть по кнопке **«Test»**.

**Пример 1:**

* IP - адрес 128.1.192.2;
* номер подсети 128.1.192.0;
* номер узла 0.2.

**Пример 2:**

* IP - адрес 128.1.197.2;  Номер подсети 128.1.192.0;
* Номер узла 5.2.

5. Определить широковещательный адрес подсети – «**BROADCAST»**.

Адрес позволяет обращаться ко всем узлам подсети и содержит '1' во всех разрядах номера узла (двоичное представление).

Для определения адреса необходимо:

* используя клавиши управления курсором, **«BackSpace»**, цифровую клавиатуру, записываем номер определенной подсети в окне двоичной записи широковещательного адреса - 10000000.00000001.1100000.00000000;
* используя клавиши управления курсором, **«BackSpace»**, цифровую клавиатуру, записываем единицы в немаскируемых разрядах поля номера узла, получаем - 10000000.00000001.11011111.11111111;
* после щелчка "мыши" вне окна ввода в окне **«BROADCAST»** появится запись широковещательного адреса подсети - 128.1.223.255.

Проверка результатов и имитация продвижения IP - пакета в сети.

1. Щелкнуть по кнопке **«Test»**. На элементах, составляющих изображение структурной схемы сети появятся кнопки-индикаторы в случае успешного продвижения пакета зеленого, иначе - красного цветов. Щелкнув по кнопке индикатору можно получить краткое сообщение о результате прохождения IP - пакета через данный элемент сети.
2. Если номер подсети в которую направляется IP-пакет определен правильно, то на схеме напротив соответствующего номера подсети появится сообщение **«CONNECT»**. Кроме того, о правильности выполнения этапов задания выдаются сообщение в информационном окне.

В случае правильного выполнения задания повторить подпункты разделов 5 и 6 не менее чем для 3 IP - адресов.

Ввести IP-адрес не принадлежащий ни одной из подсетей. Для этого в окне **«Внешний IP-адрес»** установить произвольный IP-адрес, отличный от адреса отображенного в окне **«Номер внутренней сети»** в нашем примере это может быть адрес 190.1.192.2. Убедиться, что он не подходит ни для одной из подсетей.

Возврат в основное меню производится щелчком «мыши» по кнопке **«Выход»**.

**Содержание отчета:**

1. Название и цель работы.
2. Определить маску, необходимую для образования заданного количества подсетей.
3. Заполнить таблицу маршрутизации маршрутизатора.
4. Представить пошаговую отработку алгоритма работы маршрутизатора при продвижении произвольного IP-пакета.
5. Провести проверку результатов продвижения IP - пакета в сети.
6. Эскизно представить пути продвижения IP - пакета в сети.
7. Представить в двоичном исчислении последовательный перебор номеров подсетей.
8. Обосновать принятые инженерные решения.
9. Выводы по выполненной работе.

**Практическое занятие №11 (4 ч)**

Утилита traceroute

Утилита ping

**Цель:**обобщить и систематизировать знания по теме «Работа с диагностическими утилитами протокола TCP/IP»

Ход работы.

**Задание 1. Получение справочной информации по командам.**

Выведите на экран справочную информацию по всем рассмотренным утилитам. Для этого в командной строке введите имя утилиты без параметров и дополните **/?**.

Сохраните справочную информацию в отдельном файле.

Изучите ключи, используемые при запуске утилит.

**Задание 2. Получение имени хоста.**

Выведите на экран имя локального хоста с помощью команды hostname. Сохраните результат в отдельном файле.

**Задание 3. Изучение утилиты traceroute.**

Проверьте конфигурацию TCP/IP с помощью утилиты traceroute. 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 |  |

**Задание 4. Тестирование связи с помощью утилиты ping.**

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверьте функционирование основного шлюза, послав 5 эхо-пакетов длиной 64 байта.
3. Проверьте возможность установления соединения с удаленным хостом.
4. С помощью команды ping проверьте адреса (взять из списка локальных ресурсов на сайте aspu.ru) и для каждого из них отметьте время отклика. Попробуйте изменить параметры команды ping таким образом, чтобы увеличилось время отклика. Определите IP-адреса узлов.

**Контрольные вопросы:**

1. Раскрыть термины: хост, шлюз, хоп, время жизни пакета, маршрут, маска сети, авторитетный/неавторитетный (компетентный) DNS-сервер, порт TCP, петля обратной связи, время отклика.

2. Какие утилиты можно использовать для проверки правильности конфигурирования TCP/IP?

3. Каким образом команда ping проверяет соединение с удаленным хостом?

4. Как утилита ping разрешает имена узлов в ip-адреса (и наоборот)?

5. Какие могут быть причины неудачного завершения ping и tracert? (превышен интервал ожидания для запроса, сеть недоступна, превышен срок жизни при передаче пакета).

6. Всегда ли можно узнать символьное имя узла по его ip-адресу?

**Практическое занятие №12 (2 ч)**

IP-пакет.

Схема IP-маршрутизации

Маршрутизация с использованием масок

Протокол ICMP

**Цель:** получить практические навыки по работе с пространством IP-адресов, масками и управления адресацией в IP сетях.

**Теоретические сведения**

1. Все пространство IP адресов делится на логические группы – IP-сети. Они нужны для организации иерархической адресации в составной IP-сети, например Интернете. Каждой локальной сети присваивается своя IP-сеть, маршрут до IP-узлов, находящихся в этой локальной сети строится на маршрутизаторах как маршрут до их IP-сети. И только после того, как пакет попал в конкретную IP-сеть, решается задача его доставки на отдельный узел.
2. В IP-адресе выделяются две части – адрес сети и адрес узла. Деление происходит с помощью маски – 4-x байтного числа, которое поставлено в соответствие IP-адресу. Макса содержит двоичные 1 в тех разрядах IP-адреса, которые определяют адрес сети и двоичные 0 в тех разрядах IP адреса, которые определяют адрес узла.
3. Адресом IP-сети считается IP-адрес из этой сети, в котором в поле адреса узла содержатся двоичные 0. Этот адрес обозначает сеть целиком в таблицах маршрутизации.

Есть еще служебный IP-адрес – адрес ограниченного широковещания – в поле адреса узла он содержит двоичные 1. Оба эти адреса не используются для адресации реальных узлов сети, однако входят в диапазон адресов IP-сети.

1. Рассмотрим пример: есть адрес 192.168.170.15 с маской 255.255.252.0. Определим адрес сети, адрес широковещания и допустимый для данной IP-сети диапазон адресов.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DEC IP | 192 | 168 | 170 | 15 |
| DEC MASK | 255 | 255 | 252 | 0 |
| BIN IP | 11000000 | 10101000 | 10101010 | 00001111 |
| BIN MASK | 11111111 | 11111111 | 11111100 | 00000000 |
| BIN IP сети  (скопируем сетевую часть IP и  заполним узловую часть 0) | 11000000 | 10101000 | 10101000 | 00000000 |
| DEC IP сети | 192 | 168 | 168 | 0 |
| BIN IP широковещания (скопируем сетевую часть IP и заполним узловую часть 1) | 11000000 | 10101000 | 10101011 | 11111111 |
| DEC IP широковещания | 192 | 168 | 171 | 255 |
| Начало диапазона IP-адресов для узлов (значение поля узла +1 к IP адресу сети) | 192 | 168 | 168 | 1 |
| Окончание диапазона IP-адресов для узлов (значение поля узла -1 от IP-адреса широковещания) | 192 | 168 | 171 | 254 |

5) если имеется сеть, составленная из нескольких локальных сетей, соединенных между собой маршрутизаторами, то нужно каждой из этих локальных сетей назначить отдельную IP-сеть. В случае, если вам для такой сети выдается большая IP-сеть в управление (например, такую сеть может назначить провайдер Интернет), то эту сеть необходимо разделить с помощью масок на части. (необходимо отметить, что подобная ситуация может иметь место, если вам необходимо назначить узлам вашей сети реальные IP адреса, для того чтобы ваши компьютеры были «видны» из Интернета каждый под своим адресом).

**Порядок выполнения работы:**

В работе даны 4 варианта задания (Табл. 1). Необходимо сделать все варианты. На приведенной схеме представлена составная локальная сеть. Отдельные локальные сети соединены маршрутизаторами. Для каждой локальной сети указано количество компьютеров. Провайдер, для вас выдал IP-cеть (данные о сети представлены в табл. 2). Ваша задача установить IP-адрес сети и допустимый диапазон адресов. Разделить вашу сеть на части, используя маски. Маску надо выбирать так, чтобы в отделяемой IP подсети было достаточно адресов. Помните, что и порт маршрутизатора, подключенный к локальной сети, имеет IP адрес! Некоторые маски представлены в табл.3.

Таблица 1

|  |  |
| --- | --- |
| Вариант | IP- адрес из сети |
| 1 | 192.169.168.70 |
| 2 | 172.21.25.202 |
| 3 | 83.14.53.9 |
| 4 | 190.23.23.23 |

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| маска | Сеть 1 | Сеть 2 | Сеть 3 |
| 255.255.248.0 | 500 комп. | 16 комп. | 19 комп. |
| 255.255.255.224 | 1 комп. | 4 комп. | 2 комп. |
| 255.255.255.128 | 10 комп. | 12 комп. | 8 комп. |
| 255.255.255.192 | 5 комп | 3 комп. | 3 комп. |

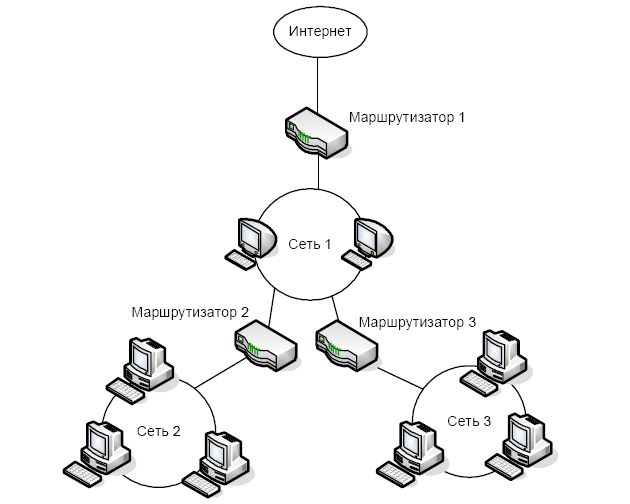


Рис 1.

Таблица 3

|  |  |  |
| --- | --- | --- |
| Маска | Количество двоичных 0 | Количество всех адресов в IP сети с такой маской |
| 255.255.255.252 | 00 | 4 |
| 255.255.255.248 | 000 | 8 |
| 255.255.255.240 | 0000 | 16 |
| 255.255.255.224 | 00000 | 32 |
| 255.255.255.192 | 000000 | 64 |
| 255.255.255.128 | 0000000 | 128 |
| 255.255.255.0 | 00000000 | 256 |
| 255.255.254.0 | 0.00000000 | 512 |

**В отчете заполняем таблицу:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Вариант:** | 1 |  |  |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 |
| IP-сети, маска |  |  |  |
| Количество IP адресов в IP-сети |  |  |  |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров. |  |  |  |
| **Вариант:** | 2 |  | |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 |
| IP-сети, маска |  |  |  |
| Количество IP адресов в IP-сети |  |  |  |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров. |  |  |  |
| **Вариант:** | 3 |  | |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 |
| IP-сети, маска |  |  |  |
| Количество IP адресов в IP-сети |  |  |  |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров. |  |  |  |
| **Вариант:** | 4 |  | |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 |
| IP-сети, маска |  |  |  |
| Количество IP адресов в IP-сети |  |  |  |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров. |  |  |  |

**Контрольные вопросы**

1. Может ли быть IP-адрес узла таким? Укажите неверные варианты IP-адрес. Ответ обоснуйте.

192.168.255.0

167.234.56.13  
224.0.5.3  
172.34.267.34  
230.0.0.7  
160.54.255.255

1. Может ли маска подсети быть такой? Укажите неверные варианты. Ответ обоснуйте.

255.254.128.0  
255.255.252.0  
240.0.0.0  
255.255.194.0  
255.255.128.0  
255.255.255.244  
255.255.255.255

1. Можно ли следующие подсети разделить на N подсетей. Если это возможно, то укажите варианты разбиения с максимально возможным количеством подсетей или узлов в каждой подсети. Ответ обоснуйте.

165.45.67.0, маска 255.255.255.224, N=3  
235.162.56.0, маска 255.255.255.224, N=6  
234.49.32.0, маска 255.255.255.192, N=3

**Практическое занятие №13 (5 ч)**

Передача с возвращением на N пакетов

Передача с выборочным повторением

Реализация метода скользящего окна в протоколе TCP

Сегменты и поток байтов

Система буферов при дуплексной передаче

Накопительный принцип квитирования

Параметры управления потоком в TCP

**Цель:** Познакомиться с принципами адресации в IP-сетях

**Задания к практической работе.**

**Задание 1.**

а) Проверьте правильность примера, приведенного выше.

б) Запишите двоичный IP-адрес 11111110101111110110001000000111 в стандартном формате.

**Задание 2.** Подсчитайте, сколько всего компьютеров может быть в Интернете. Расчет с необходимыми пояснениями запишите в отчет.

**Задание 3.** При помощи любой известной вам поисковой системы определите число документов Интернет, в которых цитируется описание протокола IP. Попробуйте найти собственно описание протокола.

Указание. Этот документ называется RFC-791 (Request For Comments-791).

**Задание 4.** Укажите классы следующих IP-адресов.

|  |  |
| --- | --- |
| Адрес | |
| 1. 126.102.128.0 2. 1.191.248.0 3. 185.74.41.184 4. 96.247.128.0 | 1. 168.224.0.1 2. 201.76.98.5 3. 186.112.0.10 4. 28.0.0.0 |

**Задание 5.** 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 | 1. 190.7.2.0 2. 127.1.1.1 3. 198.121.254.255 4. 255.255.255.255 |

**Задание 6.** Преобразуйте следующие доменные имена в IP-адреса: ***www.mail.ru***, ***www.google.com, www.bsu.edu.ru, ns.mmf.rsu.ru, ns.rsu.ru, krinc.rsu.ru, math.rsu.ru, www.rsu.ru, ftp.rsu.ru, uic.rsu.ru, rsu.ru. С***делайте выводы.

**Задание 7.** Даны имена веб-серверов:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Южная Америка** | www.uba.ar | www.castelobranko.br | www.univalle.edu.co | www.ucv.ve |
| **Австралия и Океания** | www.usyd.edu.au | www.usp.ac.fj | www.adelaide.edu.au | www.vu.edu.au |
| **Африка** | www.uz.ac.zw | www.unisa.ac.za | www.bau.edu.lb | www.aast.edu |
| **Азия** | www.mu.ac.in | www.ntu.edu.tw | www.sharjah.ac.ae | www.kimep.kz |
| **Европа** | www.us.es | www.sorbonne.fr | www.ox.ac.uk | www.unizh.ch |
| **Северная Америка** | www.stanford.edu | www.ufl.edu | www.nmt.edu | www.yale.edu |
| **Россия** | www.kubstu.ru | www.kbsu.ru | www.spbu.ru | www.festu.ru |

* Выберите по одному серверу из каждой строки таблицы. Следующие действия нужно выполнять для каждого выбранного сервера, результаты оформлять в виде таблицы.
* Определите IP-адрес.
* Выясните название владельца IP-адреса.
* Определите название и местонахождение организации, которой принадлежит веб-сервер.

**Контрольные вопросы:**

1. Какие октеты представляют идентификатор сети и узла в адресах классов А, В и С?
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?

**Практическое занятие №14 (5 ч)**

Протокол IP, Инкапсуляция, Протокол DHCP в WireShark, Протокол ARP, Протокол ICMP в WireShark, Протокол ICMP, утилита traceroute, Порты на транспортном уровне, Установка соединения в TCP, Протокол DNS в WireShark, Типы записей DNS в WireShark, DNS: итеративный и рекурсивный режим, HTTP в текстовом режиме, SMTP в текстовом режиме, POP3 в текстовом режиме, IMAP в текстовом режиме, FTP в WireShark, Протокол IPv6

Протокол NDP

**Цель работы**: изучить принципы работы протоколов и научиться их настраивать для работы в сети Интернет.

**Задание:**

Установить соединение в ТСР;

**Практическое занятие №15 (4 ч)**

Развёртывание контроллера домена – обычного и в варианте Server Core. Апгрейд с предыдущих версий. Развёртывание с носителя (Install From Media – IFM)

**Задание**

* Сформировать **собственное** рабочее пространство доменных имен узлов (не менее шести узлов) для проведения экспериментов с утилитами **ping, tracert, pathping**. Например, mstuca.ru (МГТУ ГА), [www.spb.ru](http://www.spb.ru/#_blank) (C-Петербург), [www.mail.ru](http://www.mail.ru/#_blank) (Москва), [www.romeguide.it](http://www.romeguide.it/#_blank) (Италия), [www.novol.pl](http://www.novol.pl/#_blank) (Польша), [www.newslink.org](http://www.newslink.org/#_blank) (США).
* С помощью команды **ping** проверить состояние связи с выбранными узлами. Число отправляемых запросов рекомендуется взять равным 20. Сделать экранные копии листингов, выводимых утилитой в каждом эксперименте (для формирования отчета по лабораторной работе).
* Результаты исследований представить в таблице:



* Построить диаграммы, графически представляющие статистические данные в последних трех столбцах таблицы .
* С помощью команды **tracert** произвести трассировку узлов из сформированного рабочего пространства доменных имен узлов. Результаты протоколировать в файл отчета по лабораторной работе.
* Представить графики времени прохождения шлюзов для каждого узла (для 3-х пакетов), указать наиболее узкие места в сети.
* Описать маршрут прохождения пакета **для двух** из ранее выбранных узлов (страна, город, сеть). Для этого можно использовать графические утилиты трассировки, например, **NeoTrace**, **VisualRoute** и т.п.
* Сравнить статистические данные, полученные в предыдущем эксперименте (для выбранной пары узлов) **с соответствующими** данными для выбранной пары узлов, выводимыми используемой графической утилитой.
* Оценить состояние маршрутов передачи пакетов в сети с помощью утилиты **pathping**.
* Определить перегруженные маршрутизаторы, перегруженные линии связи, процент потерь передаваемых пакетов на перегруженных участках сети. Сравнить результаты с **соответствующими** им в предыдущих экспериментах на основе работы утилит **ping** и **tracert**.

**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?

**Практическое занятие №16 (4 ч)**

Учетные записи компьютеров. Управление доступом и SPN (Service Principal Name). Работа secure channel.

Делегирование управления объектами Active Directory

**Практическое занятие №17 (6 ч)**

Использование Windows PowerShell для управления пользователями, группами, учётными записями компьютеров и OU.

Выполнение операций над группами объектов (bulk operations)

**Практическое занятие №18 (4 ч)**

Настройка IPv4. Ручное и автоматическое назначение адресов. Network Monitor и утилиты командной строки

**Практическое занятие №19 (4 ч)**

Управление БД DHCP. Резервное копирование и функция reconcile.

Безопасность и мониторинг DHCP. Защита от получения адреса неавторизованным для этого устройством. Защита от Rogue DHCP Servers

**Практическое занятие №20 (4 ч)**

Установка и управление сервером DNS.

Настройка root hints, ENDS0, форвардинга запросов, кэширования DNS

Типы зон DNS. Механизм динамических обновлений. Интеграция с Active Directory. DNSSEC.

**Практическое занятие №21 (2 ч)**

Динамическое расширение и уменьшение разделов NTFS.

Функционал Storage Spaces. Управление виртуальными дисками.

**Практическое занятие №22 (2 ч)**

Печать по сети. Enhanced Point and Print. Безопасность сетевой печати. Механизм Branch Office Direct Printing. Централизованное управление принтерами.

**Задания:**

1. Собрать конфигурацию 3 или 4 (по предложенным схемам):



2. Установить и настроить сетевые принтеры.

Задачи, которые необходимо решить при установке принтера, следующие:

1. Установить устройство(а) печати

2. Добавить локальный принтер на сервере печати

3. Определить необходимость и предоставить совместный доступ к принтеру

4. Если в сети используется служба Active Directory, опубликовать принтер

5. В Службе каталогов Active Directory включить функцию отслеживания местоположения принтеров

6. Если планируется использовать несколько однотипных устройств печати, настроить пулы принтеров

7. Определить группам пользователей соответствующие права доступа и администрирования принтеров

**Контрольные вопросы:**

1. Перечислите конфигурации клиентов, серверов и устройств печати.

2. Какие задачи решаются при установке принтера?

3. Как происходит установка и настройка сетевых принтеров?

4. Перечислите способы сетевой установки принтеров.

5. Что такое пул печати и пул принтеров? Как настроить пул принтеров?

6. Перечислите задачи администрирования принтеров.

7. Как определить права доступа к принтеру?

**Практическое занятие №23 (2 ч)**

Эшелонированная защита (Defense-In-Depth)

Настройка прав пользователей, UAC, аудита, механизма Restricted Groups и шаблонов безопасности в домене

Механизмы SRP (Software Restriction Policies) и AppLocker

Настройка Windows Firewall

**Задания:**

Укажите преимущества эшелонированной защиты от DDoS-атак. Какое количество эшелонов защиты является оптимальным?

Используя механизмы SRP, создайте проект блокировки посторонних приложений на рабочих местах для стандартного рабочего места оператора клиентского call-центра.

Дано: Операционная система виртуальных рабочих мест – Windows. Все системы в одном домене AD.

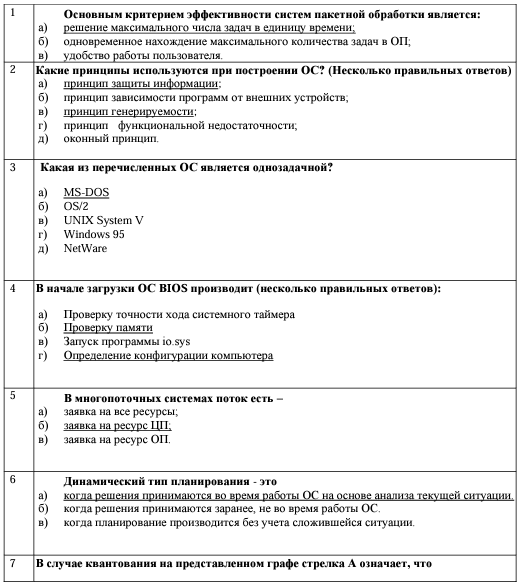
Исходный список «белых» приложений:

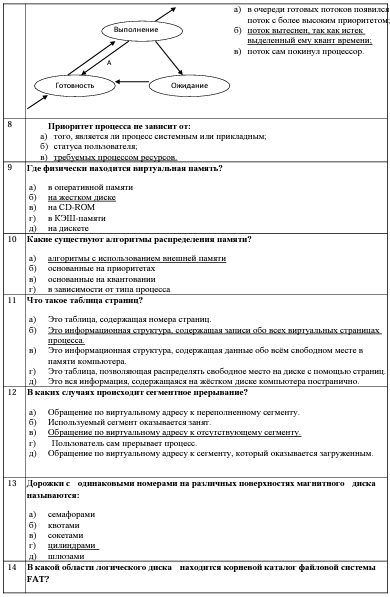
|  |  |
| --- | --- |
| **Приложение** | **Путь   и каталог запуска** |
| ***Пульт для работы с   чатом WorskpaceDesktopEdition*** | ***C:\Program Files\GCTI\Workspace Desktop Edition\InteractionWorkspace.exe*** |
| ***Статистика CCPulse*** | ***C:\GCTI\CCPulse+\CallCenter.exe*** |
| ***Управление системными   сообщениями в чате KnowledgeManager*** | ***C:\Program Files\GCTI\eServices 8.1.3\Knowledge   Manager\KnowledgeManager.BAT***    ***(Использует каталог C:\Program Files\Java\jre6)*** |
| ***WFM – Управление   расписаниями*** | ***C:\Program Files\NICE\_IEX\_WFM\totalview\ttv40.exe*** |
| ***HPSM*** | ***C:\Program Files\HP\Service Manager 7.11\Client\ServiceManager.exe*** |
| ***Citrix Access Gateway*** | ***C:\Program Files\Citrix\Secure Access Client\nsload.exe*** |
| ***Skype*** | ***C:\Program Files\Skype\Phone\Skype.exe*** |
| ***Lync 2010*** | ***C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Lync*** |
| ***Microsoft Office*** | ***C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Microsoft Office*** |
| ***Internet Explorer*** | ***C:\Program Files\Internet Explorer\iexplore.exe*** |
| ***Google Chrome*** | ***C:\Program Files\Google\Chrome\Application\chrome.exe*** |
| ***Mozilla Firefox*** | ***C:\Program Files\Mozilla Firefox\firefox.exe*** |

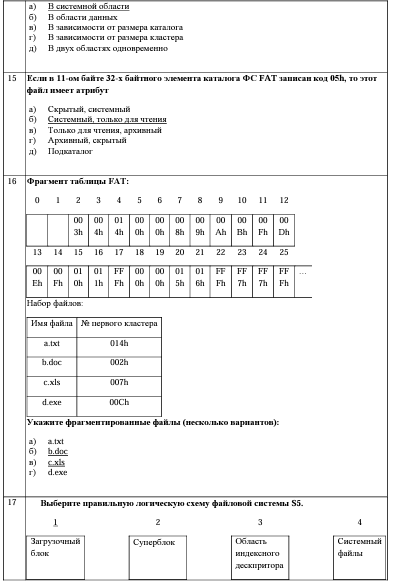
**III. КОМПЛЕКТ МАТЕРИАЛОВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

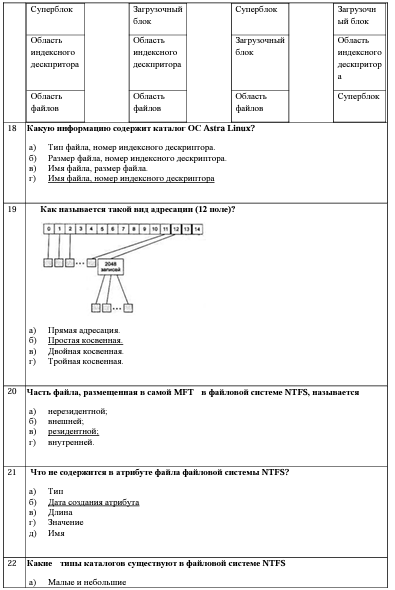
**Тест в формате Диагностической работы**

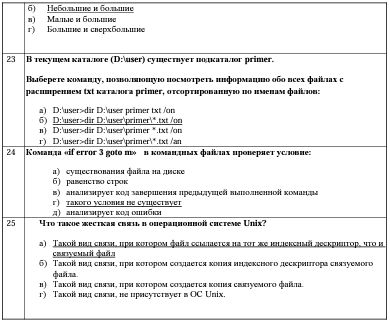
**(для дифференцированного зачета)**











**Вопросы к экзамену**

1. Классификация компьютерных сетей.
2. Модель взаимодействия открытых систем. Уровни модели OSI.
3. Методы защиты информации от ошибок. Классификация помехоустойчивых кодов
4. Помехоустойчивое кодирование. Кодирование с контролем четности
5. Помехоустойчивое кодирование. Код Хэмминга
6. Использование обратной связи. Основные термины.
7. Система с информационной обратной связью.
8. Система с решающей обратной связью.
9. Понятие коммутации. Коммутация каналов.
10. Понятие коммутации. Коммутация сообщений.
11. Понятие коммутации. Коммутация пакетов.
12. Способ передачи пакетов в сетях.
13. Протоколы. Стандартные стеки коммуникационных протоколов.
14. Стек протоколов TCP/IP.
15. Классы IP-адресов. Особые IP-адреса.
16. Стек протоколов IPX/SPX.
17. Семейство сетевых технологий Ethernet. Принцип работы Ethernet.
18. Принцип работы Ethernet. Взаимодействие на подуровнях LLC и MAC.
19. Характеристики физической среды передачи данных.
20. Коаксиальный кабель. Конструкция и характеристики.
21. Витая пара. Конструкция и характеристики.
22. Стандарты беспроводных сетей
23. Основные режимы работы беспроводных сетей
24. Область применения сетей Wi-Fi. Примеры использования.

Практические задания на экзамен

1. Беспроводные адаптеры. Подключение, настройка на примере Wi-Fi адаптера TP-LINK TL-WN821N (USB). Соединение компьютеров с помощью беспроводных адаптеров в режиме AD-HOC в соответствии с заданием. Организация общего доступа к сетевым ресурсам.
2. Беспроводные адаптеры. Подключение, настройка на примере Wi-Fi адаптера TP-LINK TL-WN722N (USB). Соединение компьютеров с помощью беспроводных адаптеров в режиме AD-HOC в соответствии с заданием. Организация общего доступа к сетевым ресурсам.
3. Беспроводные адаптеры. Подключение, настройка на примере Wi-Fi адаптера TP-LINK TL-WN881ND (PCI-E). Соединение компьютеров с помощью беспроводных адаптеров в режиме AD-HOC в соответствии с заданием. Организация общего доступа к сетевым ресурсам.
4. Беспроводные адаптеры. Подключение, настройка на примере Wi-Fi адаптера D-Link DWA-582 (PCI-E). Соединение компьютеров с помощью беспроводных адаптеров в режиме AD-HOC в соответствии с заданием. Организация общего доступа к сетевым ресурсам.
5. Беспроводные точки доступа. Подключение, настройка на примере точки доступа D-Link DAP-1360U в соответствии с заданием. Режим Access Point . Организация общего доступа к сетевым ресурсам.
6. Беспроводные точки доступа. Подключение, настройка на примере точки доступа D-Link DAP-3410 в соответствии с заданием. Режим Access Point. Организация общего доступа к сетевым ресурсам.
7. Беспроводные роутеры. Подключение, настройка на примере Wi-Fi роутера D-Link DIR-615S в соответствии с заданием. Режим Access Point. Организация общего доступа к сетевым ресурсам.
8. Беспроводные роутеры. Подключение, настройка на примере Wi-Fi роутера D-Link DIR-620S в соответствии с заданием. Режим Access Point. Организация общего доступа к сетевым ресурсам.
9. Беспроводные роутеры. Подключение, настройка на примере Wi-Fi роутера D-Link DIR-878 в соответствии с заданием. Режим Access Point. Организация общего доступа к сетевым ресурсам.
10. Беспроводные роутеры. Подключение, настройка на примере Wi-Fi роутера D-Link DIR-822 в соответствии с заданием. Режим Access Point. Организация общего доступа к сетевым ресурсам.
11. Беспроводные точки доступа. Подключение, настройка на примере точки доступа D-Link DAP-1360U в соответствии с заданием. Режим Infrastructure. Организация общего доступа к сетевым ресурсам.
12. Беспроводные точки доступа. Подключение, настройка на примере точки доступа D-Link DAP-3410 в соответствии с заданием. Режим Infrastructure. Организация общего доступа к сетевым ресурсам.
13. Беспроводные роутеры. Подключение, настройка на примере Wi-Fi роутера D-Link DIR-615S в соответствии с заданием. Режим Infrastructure. Организация общего доступа к сетевым ресурсам.
14. Беспроводные роутеры. Подключение, настройка на примере Wi-Fi роутера D-Link DIR-620S в соответствии с заданием. Режим Infrastructure. Организация общего доступа к сетевым ресурсам.
15. Беспроводные роутеры. Подключение, настройка на примере Wi-Fi роутера D-Link DIR-878 в соответствии с заданием. Режим Infrastructure. Организация общего доступа к сетевым ресурсам.
16. Беспроводные роутеры. Подключение, настройка на примере Wi-Fi роутера D-Link DIR-822 в соответствии с заданием. Режим Infrastructure. Организация общего доступа к сетевым ресурсам
17. Методика работы с кабелями типа «витая пара». Кроссирование. Соединение компьютеров с помощью сетевых адаптеров в соответствии с заданием. Организация общего доступа к сетевым ресурсам.