	Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный колледж»
	Учебно-методический отдел
	Учебно-методические материалы
	Методические указания

**Методические указания по выполнению практических работ
 обучающихся по учебной дисциплине
 Компьютерные сети**

Специальность 09.02.07 Информационные системы и программирование

Челябинск, 2019

	Должность	Фамилия/Подпись	Дата
Разработал	Преподаватель	Чераева О.А.	
Проверил	Зам. директора по учебно-методической работе	Манапова О.Н.	
Согласовал	Зам. директора по учебной работе	Калиновская Т.С.	
Версия: 01	Без подписи документ действителен 3 суток после распечатки. Дата и время распечатки:	Экземпляр № _____	с. 1 из 78

	ГБПОУ «ЮУГК»
	Учебно-методический отдел
	Учебно-методические материалы
	Методические указания

ББК 74.57

Чераева О.А. Методические указания по выполнению практических работ обучающихся по учебной дисциплине Компьютерные сети: методические указания для студентов. - Издательский центр ЮУГК, 2019. – 78 с.

Рассмотрено и одобрено на заседании ПЦК *Информационных технологий*
 Протокол от 19 февраля 2018 г. №6
 Председатель ПЦК _____ Н.А. Назарова

Рекомендовано к изданию методическим советом ГБПОУ «ЮУГК»
 Протокол от _____ 2018 г. №

Данные методические рекомендации способствуют эффективному выполнению практических работ обучающимися. Содержат требования к знаниям, умениям, общие компетенции, на формирование которых направлено выполнение самостоятельных работ; перечень видов и описание практических работ; формы контроля и критерии оценки выполнения практических работ.

Версия: 01	<i>Без подписи документ действителен 3 суток после распечатки. Дата и время распечатки: _____</i>	Экземпляр № 01	с. 2 из 78
------------	---	----------------	------------

Содержание

Пояснительная записка.....	4
Практическая работа № 1	8
Практическая работа № 2	12
Практическая работа № 3	16
Практическая работа № 4	18
Практическая работа № 5	21
Практическая работа № 6	26
Практическая работа № 7	28
Практическая работа № 8	31
Практическая работа № 9	36
Практическая работа № 10	40
Практическая работа № 11 (часть 1)	43
Практическая работа № 11 (часть 2)	47
Практическая работа № 12	50
Практическая работа № 13	58
Практическая работа № 14	60
Практическая работа № 15	63
ПРИЛОЖЕНИЕ 1	76
ПРИЛОЖЕНИЕ 2	77

Пояснительная записка

Методические указания по выполнению практических работ студентов по дисциплине Компьютерные сети предназначены для студентов по специальности 09.02.07 Информационные системы и программирование.

Цель методических указаний: оказание помощи студентам в выполнении практической работы по дисциплине Компьютерные сети.

Настоящие методические указания содержат работы, которые позволят студентам овладеть фундаментальными знаниями, профессиональными умениями и навыками деятельности по специальности, опытом творческой и исследовательской деятельности и направлены на формирование следующих компетенций:

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

ПК 4.4 Обеспечивать защиту программного обеспечения компьютерных систем программными средствами

ПК 5.3 Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием

ПК 6.1 Разрабатывать техническое задание на сопровождение информационной системы

ПК 6.5 Осуществлять техническое сопровождение, обновление и восстановление данных ИС в соответствии с техническим заданием

ПК 7.1 Выявлять технические проблемы, возникающие в процессе эксплуатации баз данных и серверов

ПК 7.2 Осуществлять администрирование отдельных компонент серверов

ПК 7.3 Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов

ПК 9.4 Осуществлять техническое сопровождение и восстановление веб-приложений в соответствии с техническим заданием

ПК 9.6 Размещать веб приложения в сети в соответствии с техническим заданием

ПК 9.10 Реализовывать мероприятия по продвижению веб-приложений в сети Интернет

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

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

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

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

ОК 9. Использовать информационные технологии в профессиональной деятельности

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках

В результате освоения учебной дисциплины Компьютерные сети обучающийся должен уметь:

- Организовывать 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.

В результате освоения учебной дисциплины Компьютерные сети обучающийся должен знать:

- Основные понятия компьютерных сетей: типы, топологии, методы доступа к среде передачи.
- Аппаратные компоненты компьютерных сетей.
- Принципы пакетной передачи данных.
- Понятие сетевой модели.
- Сетевую модель OSI и другие сетевые модели.
- Протоколы: основные понятия, принципы взаимодействия, различия и особенности распространенных протоколов, установка протоколов в операционных системах.
- Адресацию в сетях, организацию межсетевого воздействия

Описание каждой практической работы содержит: тему, цели работы, задания, формы контроля, требования к выполнению и оформлению заданий. Для получения дополнительной, более подробной информации по изучаемым вопросам, приведено учебно-методическое и информационное обеспечение.

Перечень практических работ представлен в таблице 1.

Таблица 1

№ и название темы	Кол-во часов	Вид практической работы	Форма контроля
Тема 1. Общие сведения о компьютерной сети	8		
1. Построение схемы компьютерной сети	2	Аудиторная	Представление выполненных работ
2. Использование топологий локальных и глобальных сетей, различия в принципе (алгоритме) работы	2	Аудиторная	Представление выполненных работ
3. Применение принципов работы сетевых технологий	2	Аудиторная	Представление выполненных работ
4. Построение одноранговой сети	2	Аудиторная	Представление выполненных работ

Тема 2. Аппаратные компоненты компьютерных сетей	4		
5. Применение видов кабельной продукции.	4	Аудиторная	Представление выполненных работ
Тема 3. Передача данных по сети	18		
6. Применение методов доступа к среде передачи данных (методы доступа к каналам связи).	2	Аудиторная	Представление выполненных работ
7. Использование асинхронной и синхронной передачи данных	4	Аудиторная	Представление выполненных работ
8. Настройка протоколов TCP/IP в операционных системах	4	Аудиторная	Представление выполненных работ
9. Работа с диагностическими утилитами протокола TCP/IP	4	Аудиторная	Представление выполненных работ
10. Решение проблем с TCP/IP	2	Аудиторная	Представление выполненных работ
11. Преобразование форматов IP-адресов. Расчет IP-адреса и маски подсети	2	Аудиторная	Представление выполненных работ
Тема 4. Сетевые архитектуры	10		
12. Монтаж кабельных сред технологий Ethernet	4	Аудиторная	Представление выполненных работ
13. Настройка удаленного доступа к компьютеру	4	Аудиторная	Представление выполненных работ
14. Использование принципов работы технологий ГС на основе выделенных линий	2	Аудиторная	Представление выполненных работ
15. Использование принципов работы технологий ГС на основе коммутации каналов и пакетов	2	Аудиторная	Представление выполненных работ
Итого	44		

Практическая работа № 1

Тема Построение схемы компьютерной сети

Цели: Изучить виды топологий компьютерных сетей. Построить схему компьютерной сети

Теоретические сведения

Под топологией компьютерной сети обычно понимается физическое расположение компьютеров сети один относительно одного и способ соединения их линиями связи. Важно отметить, что понятие топологии относится, в первую очередь, к локальным сетям, в которых структуру связей можно легко проследить.

Топология определяет требования к оборудованию, тип используемого кабеля, возможные и наиболее удобные методы управления обменом, надежность работы, возможности расширения сети.

Существует три основные топологии сети:

1. Топология типа **шина**, представляет собой общий кабель, к которому подсоединены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала. (рисунок 1);

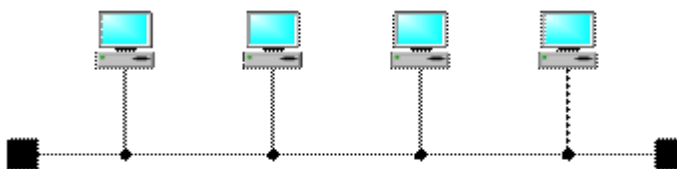


Рисунок 1 – Сетевая топология «шина»

Достоинства

- небольшое время установки сети;
- дешевизна (требуется меньше кабеля и сетевых устройств);
- простота настройки;
- выход из строя рабочей станции не отражается на работе сети.

Недостатки

- любые неполадки в сети, как обрыв кабеля, выход из строя терминатора полностью уничтожают работу всей сети;

- сложная локализация неисправностей;
- с добавлением новых рабочих станций падает производительность сети.

2. **Звезда** — базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу (обычно сетевой концентратор), образуя физический сегмент сети.

Никакие конфликты в сети с топологией звезда в принципе невозможны, потому что управление полностью централизовано. (рисунок 2)

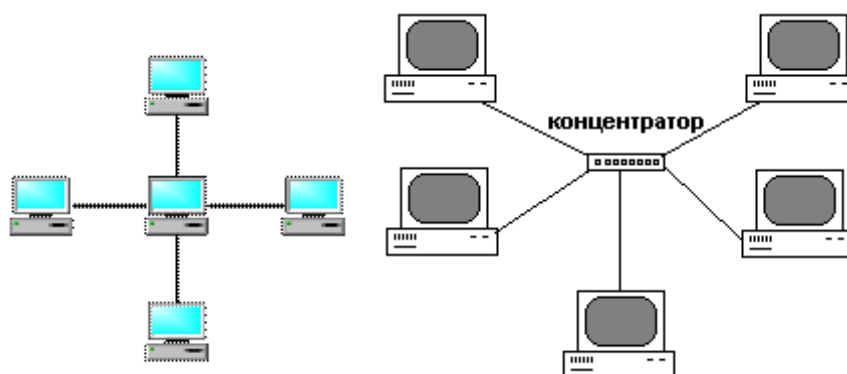


Рисунок 2 – Сетевая топология «звезда»

Достоинства

- выход из строя одной рабочей станции не отражается на работе всей сети в целом;
- хорошая масштабируемость сети;
- лёгкий поиск неисправностей и обрывов в сети;
- высокая производительность сети;
- гибкие возможности администрирования.

Недостатки

- выход из строя центрального концентратора обернётся неработоспособностью сети (или сегмента сети) в целом;
- для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;
- конечное число рабочих станций в сети (или сегменте сети) ограничено количеством портов в центральном концентраторе.

3. **Кольцо** — это топология, в которой каждый компьютер соединен линиями связи только с двумя другими: от одного он только получает информацию, а другому только передает. На каждой линии связи, как и в случае звезды, работает только один передатчик и один приемник.

Это позволяет отказаться от применения внешних терминаторов (рисунок 3).

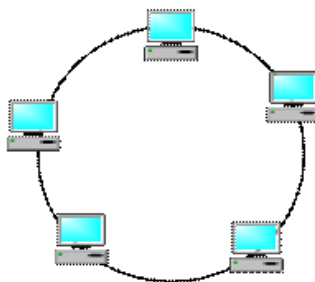


Рисунок 3 – Сетевая топология «кольцо»

Достоинства

- простота установки;
- практически полное отсутствие дополнительного оборудования;
- возможность устойчивой работы без существенного падения скорости передачи данных при интенсивной загрузке сети, поскольку использование маркера исключает возможность возникновения коллизий.

Недостатки

- выход из строя одной рабочей станции, и другие неполадки (обрыв кабеля), отражаются на работоспособности всей сети;
- сложность конфигурирования и настройки;
- сложность поиска неисправностей.

На практике нередко используют и комбинации базовой топологии, но большинство сетей ориентированные именно на этих три.

Методические указания

1. Создать схему соединения компьютерной сети согласно варианта из таблицы 2

Таблица 2

Варианты заданий

№	Сервер	ПК	Топология	
			Сервер	ПК
1	4	6	Общая шина	Кольцо
2	3	7	Звезда	Звезда
3	4	5	Звезда	Полносвязная
4	6	5	Звезда	Общая шина
5	3	7	Кольцо	Звезда
6	6	3	Звезда	Кольцо
7	4	11	Общая шина	Кольцо
8	5	4	Кольцо	Полносвязная
9	6	5	Звезда	Звезда
10	7	4	Общая шина	Полносвязная
11	5	6	Звезда	Кольцо
12	8	4	Звезда	Полносвязная
13	3	7	Общая шина	Общая шина
14	6	6	Общая шина	Кольцо
15	5	5	Полносвязная	Звезда
16	4	7	Полносвязная	Общая шина
17	5	6	Полносвязная	Кольцо
18	7	3	Общая шина	Звезда
19	8	4	Кольцо	Кольцо
20	5	6	Полносвязная	Полносвязная
21	8	5	Общая шина	Звезда
22	6	4	Кольцо	Полносвязная
23	5	5	Звезда	Полносвязная
24	4	6	Звезда	Звезда
25	5	6	Общая шина	Кольцо

2. Описать принцип работы построенной топологии.

Контрольные вопросы

1. Что такое топология сети?
2. Перечислите все топологии.
3. Достоинства и недостатки топологий?
4. Пример применения топологии в сетях?

Практическая работа № 2

Тема Использование топологий локальных сетей

Цель: применить на практике знания о назначении, принципах построения и функционирования локальных компьютерных сетей.

Краткие теоретические сведения

Локальная компьютерная (вычислительная) сеть (ЛВС) – это комплекс программного обеспечения и устройств, объединяющих абонентов, находящихся на незначительной дистанции друг от друга. Как правило, такие системы используются в границах одного предприятия или здания.

Главная задача ЛВС – это реализация совместного доступа всех пользователей к данным, устройствам и программам.

Типы локальных сетей

Выбор топологии следует производить, основываясь на имеющемся типе ЛВС. Сеть может быть представлена двумя моделями: одноранговой и иерархической.

1. *Одноранговая сеть*

Этот тип ЛВС подразумевает равноправие каждой рабочей станции, распределяя данные между ними.

Доступ к информации, хранящейся на узле, может быть разрешен либо запрещен его пользователем. Как правило, в таких случаях топология локальных компьютерных сетей «шина» будет наиболее подходящей.

Одноранговая сеть подразумевает доступность ресурсов рабочей станции остальным пользователям. Одноранговая ЛВС представлена на рисунке 4.



Рисунок 4 – Одноранговая локальная сеть

Достоинства:

- легкость реализации, монтажа и обслуживания;
- небольшие финансовые затраты;
- исключает надобность в покупке дорогого сервера.

Недостатки:

- быстродействие сети уменьшается пропорционально увеличению количества подсоединенных рабочих узлов;
- отсутствует единая система безопасности;
- доступность информации: при выключении компьютера данные, находящиеся в нем, станут недоступными для остальных;
- нет единой информационной базы.

2. Иерархическая модель

Наиболее часто используемые топологии локальных сетей основаны именно на этом типе ЛВС. Его еще называют «клиент-сервер».

Суть данной модели состоит в том, что при наличии некоторого количества абонентов имеется один главный элемент – сервер.

Этот управляющий компьютер хранит все данные и занимается их обработкой (рисунок 5)

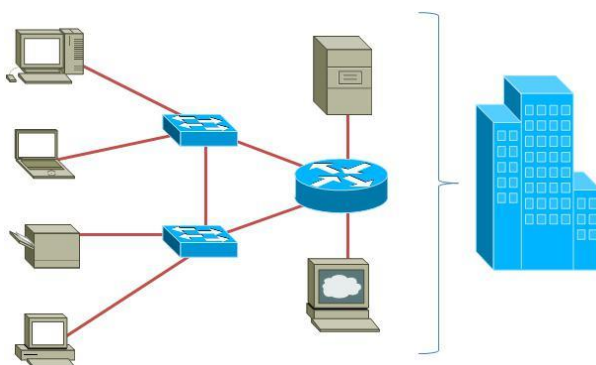


Рисунок 5 – Иерархическая ЛВС

Достоинства:

- отличное быстродействие сети;
- единая надежная система безопасности;
- одна, общая для всех, информационная база;
- облегченное управление всей сетью и ее элементами.

Недостатки:

– необходимость наличия специальной кадровой единицы – администратора, который занимается мониторингом и обслуживанием сервера;

– большие финансовые затраты на покупку главного компьютера.

Наиболее часто используемая конфигурация (топология) локальной компьютерной сети в иерархической модели – это «звезда».

Выбор топологии (компоновка сетевого оборудования и рабочих станций) является исключительно важным моментом при организации локальной сети. Выбранный вид связи должен обеспечивать максимально эффективную и безопасную работу ЛВС.

Методические указания

1. Описать одноранговую локальную сеть с топологией «линейная шина».
2. Описать одноранговую локальную сеть с топологией «звезда».
3. Описать локальную сеть на основе сервера.
4. Проанализировать описание данных ЛВС и сделать выводы.
5. Заполните таблицу 3

Таблица 3

Одноранговая ЛВС на основе топологии «Шина»

Характеристика/ ЛВС	Локальная вычислительная сеть на основе:		
	Топологии «Шина»	Топологии «Звезда»	Сервера
Схема локальной сети			
Недостатки			
Преимущества			
Количество компьютеров в сети			
Оборудование, необходимое для создания сети и его стоимость			
Общая стоимость создания локальной сети			
Выводы:			

Контрольные вопросы

1. Что называется, локальной сетью компьютеров?
2. Каковы причины создания локальных сетей? Для чего они создаются?
3. Какие схемы соединения компьютеров в локальную сеть существуют?
4. Какие сети называются одноранговыми? Что такое сервер локальной сети?
5. Какие кабели используются для соединения компьютеров в локальную сеть? Охарактеризуйте условия применения таких соединений.
6. Какие виды электронного оборудования используются для создания локальных сетей?
7. Какое программное обеспечение требуется для создания и работы в локальной сети?
8. Охарактеризуйте основные операционные системы, используемые для создания локальных сетей.
9. Что называется, администрированием локальной сети?
10. Каким образом происходит идентификация пользователя локальной сети? Для чего она нужна?
11. Что называется, рабочей группой?
12. Какие сетевые приложения называют клиент-серверными?

Практическая работа № 3

Тема Применение принципов работы сетевых технологий

Цель: научиться применять принципы работы сетевых технологий

Теоретические сведения

В локальных сетях, как правило, используется разделяемая среда передачи данных (моноканал) и основная роль отводится протоколами физического и канального уровней, так как эти уровни в наибольшей степени отражают специфику локальных сетей.

Сетевая технология – это согласованный набор стандартных протоколов и реализующих их программно-аппаратных средств, достаточный для построения локальной вычислительной сети. Сетевые технологии называют базовыми технологиями или сетевыми архитектурами локальных сетей.

В современных локальных вычислительных сетях широкое распространение получили такие технологии или сетевые архитектуры, как: Ethernet, Token-Ring, ArcNet, FDDI.

Методические указания

1. По таблице 4 выбрать вариант работы

Таблица 4

Варианты заданий

№	Задание
1	Информационная система для факультета университета.
2	Информационная система для филиала банка.
3	Информационная система для небольшого торгового предприятия.
4	Информационная система для поликлиники.
5	Информационная система для больницы.
6	Информационная система железнодорожной станции.
7	Информационная система для школы.
8	Информационная система для библиотеки.
9	Информационная система юридической фирмы

2. Определить базовую топологию сети (сегментов)
3. Определить применяемую сетевую технологию
4. Определить каналы связи и методы организации управления локальной сетью

Контрольные вопросы

1. Понятие информационно-вычислительной сети. Виды ЛВС.
2. Основные этапы проектирования ЛВС.
3. Принципы проектирования ЛВС.
4. Понятие и виды топологий.
5. Что такое одноранговая сеть?
6. Основные критерии оценки локальных вычислительных сетей.

Практическая работа № 4

Тема «Построение одноранговой сети»

Цель: научиться создавать локальную одноранговую вычислительную сеть

Теоретические сведения

Одноранговая сеть – это сеть равноправных компьютеров, каждый из которых имеет уникальное имя (имя компьютера) и обычно пароль для входа в него во время загрузки ОС. Имя и пароль входа назначаются владельцем компьютера средствами ОС. Каждый компьютер такой сети может одновременно являться и сервером, и клиентом сети, хотя вполне допустимо назначение одного компьютера только сервером, а другого только клиентом.

Достоинством одноранговых сетей является их высокая гибкость: в зависимости от конкретной задачи сеть может использоваться очень активно, либо совсем не использоваться. Из-за большой самостоятельности компьютеров в таких сетях редко бывает ситуация перегрузки (к тому же количество компьютеров обычно невелико).

В одноранговых сетях допускается определение различных прав пользователей по доступу к сетевым ресурсам, но система разграничения прав не слишком развита. Если каждый ресурс защищен своим паролем, то пользователю приходится запоминать большое число паролей.

К недостаткам одноранговых сетей относятся также слабая система контроля и протоколирования работы сети, трудности с резервным копированием распределенной информации. К тому же выход из строя любого компьютера-сервера приводит к потере части общей информации, то есть все такие компьютеры должны быть по возможности высоконадежными.

Эффективная скорость передачи информации по одноранговой сети часто оказывается недостаточной, поскольку трудно обеспечить быстроедействие процессоров, большой объем оперативной памяти и высокие скорости обмена с жестким диском для всех компьютеров сети. К тому же компьютеры сети работают не только на сеть, но и решают другие задачи.

Считается, что одноранговая сеть наиболее эффективна в небольших сетях (около 10 компьютеров). При значительном количестве компьютеров сетевые операции сильно замедляют работу компьютеров и создадут множество других проблем.

Самая распространенная в настоящий момент одноранговая сеть – это сеть на основе Windows XP (или более ранних версий ОС Windows).

Методические указания

5. Установите одинаковое имя рабочей группы для всех компьютеров, которые должны быть подключены к локальной сети.

Откройте свойства «Моего компьютера», один из быстрых способов сделать это — нажать клавиши Win + R на клавиатуре и ввести команду *sysdm.cpl*.

6. Откроется как раз нужная нам вкладка, в которой можно увидеть, к какой рабочей группе принадлежит компьютер. Для того, чтобы изменить имя рабочей группы, нажмите «Изменить» и задайте новое имя (не используйте кириллицу). Имя рабочей группы на всех компьютерах должно совпадать.

7. Зайдите в Центр управления сетями и общим доступом Windows (его можно найти в панели управления, либо с помощью правого клика по значку подключения в области уведомлений).

8. Для всех профилей сети включите сетевое обнаружение, автоматическую настройку, общий доступ к файлам и принтерам.

9. Перейдите к пункту «Дополнительные параметры общего доступа», перейдите к разделу «Все сети» и в последнем пункте «Общий доступ с парольной защитой» выберите «Отключить общий доступ с парольной защитой» и сохраните изменения.

Предоставление доступа к файлам и папкам на компьютере

10. Для того, чтобы предоставить общий доступ к папке Windows в локальной сети, кликните правой кнопкой мыши по этой папке и выберите

пункт «Свойства» и перейдите к вкладке «Доступ», на ней нажмите кнопку «Расширенная настройка».

11. Установите отметку «Открыть общий доступ к этой папке», после чего нажмите «Разрешения».

12. Отметьте те разрешения, которые необходимы для этой папки. Если требуется возможность только чтения, можете оставить значения по умолчанию. Примените сделанные настройки.

13. После этого, в свойствах папки откройте вкладку «Безопасность» и нажмите кнопку «Изменить», а в следующем окне — «Добавить».

14. Укажите имя пользователя (группы) «Все» (без кавычек), добавьте его, после чего, установите те же разрешения, что устанавливали в предыдущий раз. Сохраните сделанные изменения.

15. Перезагрузите компьютер

16. Зайдите в «Проводник», откройте пункт «Сеть» и посмотрите созданную папку

Контрольные вопросы

1. Для чего нужна локальная сеть между компьютерами?
2. Для чего нужна команда «`sysdm.cpl`»?
3. Как предоставить доступ к файлам и папкам на компьютере?

Практическая работа № 5

Тема Применение видов кабельной продукции

Цели:

1. изучить различные каналы передачи данных в сетях;
2. построить схему соединения при помощи соответствующей кабельной продукции.

Теоретические сведения

Выбор проводника изначально всегда обусловлен топологией ЛВС, и самыми распространенными являются коаксиальные провода и витая пара.

Для подключения локальной сети Ethernet провода бывают двух видов:

Коаксиальный — представляющий собой одножильный провод с экраном, отделенные друг от друга изоляционным материалом или воздушной прослойкой.

«Витая пара» — состоит из восьми жил, переплетенных между собой попарно. Каждая жила маркируется отдельным цветом для упрощения монтажа. Цвета закреплены и описаны спецификацией и все производители продукции придерживаются этих правил.

Оптоволоконный или волоконно-оптический — имеет очень сложную конструкцию и довольно дорогой для монтажа. Сигнал в нем передается в виде световых импульсов через специальные световоды.

Коаксиальный кабель.

Этот тип провода является наиболее старым из проводников (рисунок 6).

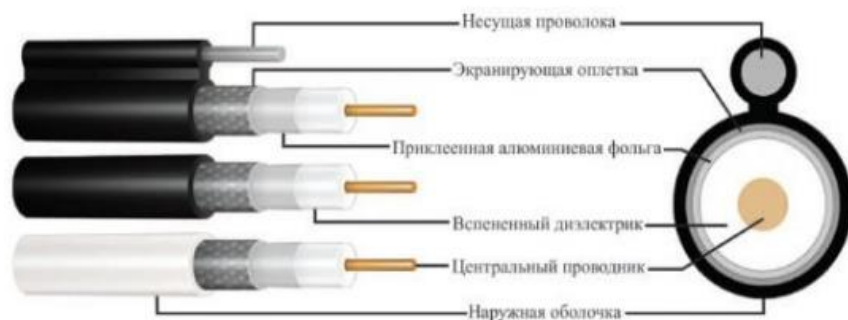


Рисунок 6 – Состав коаксиального кабеля

Этот шнур имеет одну несущую медную или алюминиевую жилу, которая покрыта толстым слоем изоляционного материала. Далее идет экран, выполненный в виде ленты, опоясывающей центральную жилу из алюминия или меди. Верхним внешним слоем идет оболочка, защищающая жилы от повреждений, изготавливаемая из полиэтилена или поливинилхлорида.

Благодаря хорошей изоляции сигнал в проводнике практически не гасится, т.е. пакеты не теряются, и не нужны дополнительные алгоритмы проверки, переданной или принятой информации.

Единственным недостатком является довольно высокая стоимость производства и низкая скорость, поэтому впоследствии он был вытеснен «витой парой».

«Витая пара»

Кабель для локальной сети «витая пара» получил свое название из-за того, что он состоит из восьми жил, попарно переплетенных между собой (рисунок 7)

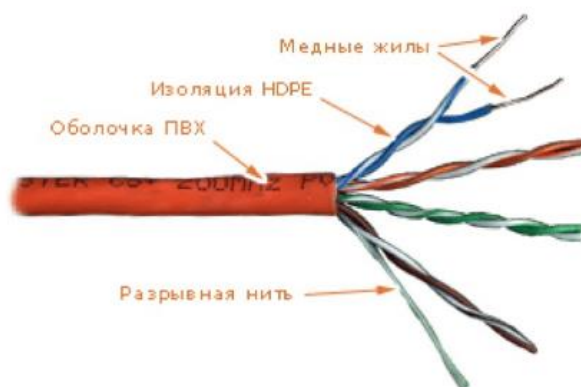


Рисунок 7 – Состав кабеля «Витая пара»

Каждая жила имеет изоляцию строго закрепленного в спецификации цвета. В качестве внешнего изолирующего материала, защищающего сигнал от электромагнитных помех, используется поливинилхлорид или полиэтилен.

Существует несколько разновидностей такого кабеля:

UTP (Unshilded Twisted Pair) — не экранированная модификация, наиболее часто используемая для прокладки домашних или офисных сетей, когда не оказываются сильные помехи на передаваемый сигнал.

FTP (Foiled Twisted Pair) — кабель с дополнительным экраном из алюминиевой фольги под внешней изоляцией.

STP (Shilded Twisted Pair) — помимо общего экрана имеет дополнительный, для каждой пары по отдельности. Витая пара имеет 7 категорий, и, чем больше номер категории, тем провод более защищен от электромагнитного излучения. Для сетей Ethernet применяется кабель 5-й категории (CAT5), который имеет полосу пропускания 100 МГц.

Рекомендуется при монтаже новых объектов использовать более совершенную модификацию CAT5e для более высокочастотных сигналов с полосой в 125 МГц.

Оптоволоконный кабель

Оптоволокно — наиболее прогрессивная технология для передачи сигнала на большие расстояния на огромной скорости (рисунок)

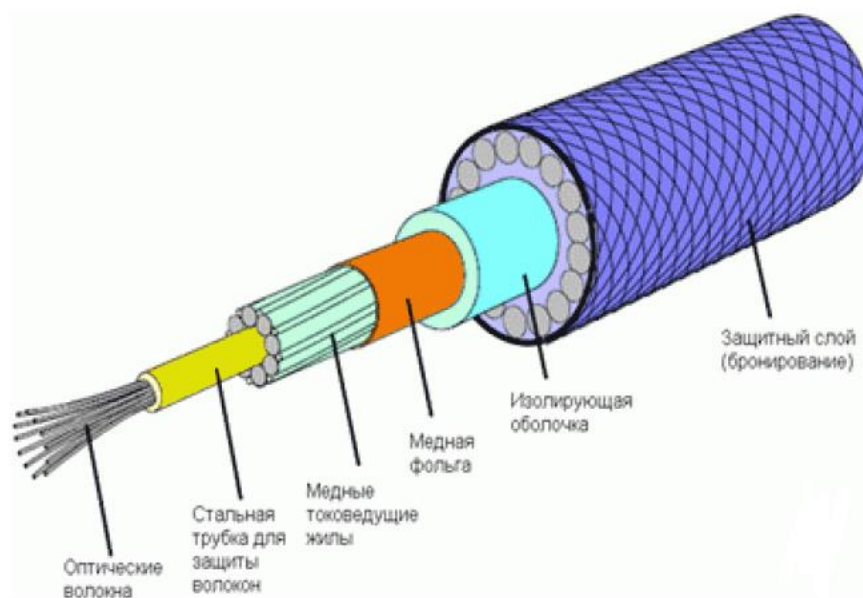


Рисунок 8 – Состав оптоволоконного кабеля

Отличием в передаче сигнала является то, что в качестве импульса используется не электричество, а свет. Свет передается по жилам из стекольного волокна отражаясь от внутренних стенок проводника. Можно

одновременно передавать несколько сигналов: они не будут пересекаться или гасить друг друга.

Скорость передачи информации по такому кабелю ограничена возможностями только самих сетевых карт или адаптеров. Кабель не подвержен помехам, и выполняется из негорючих материалов.

Стоимость такого кабеля относительно низкая, по сравнению с другими проводниками, но его монтаж может проводиться только квалифицированными сотрудниками с применением высокоточного и дорогого оборудования, поэтому в домашних условиях его использовать практически невозможно.

Методические указания

1. Создать схему соединения соответствующих кабелей к топологиям по вариантам (таблица 5)

Таблица 5

Варианты заданий

№	Сервер	ПК	Топология	Кабель
1	3	3	Звезда	Витая пара
2	3	5	Кольцо	Оптоволоконный
3	3	6	Звезда	Оптоволоконный
4	3	3	Общая шина	Коаксиальный
5	4	6	Полносвязная	Витая пара
6	4	7	Общая шина	Коаксиальный
7	5	3	Звезда	Витая пара
8	6	9	Кольцо	Оптоволоконный
9	2	9	Кольцо	Витая пара
10	3	6	Ячеистая	Коаксиальный
11	5	5	Общая шина	Коаксиальный
12	4	9	Звезда	Витая пара
13	3	8	Звезда	Оптоволоконный
14	6	7	Кольцо	Оптоволоконный
15	5	8	Звезда	Оптоволоконный
16	6	9	Общая шина	Коаксиальный

17	4	5	Полносвязная	Витая пара
18	4	6	Общая шина	Коаксиальный
19	7	7	Звезда	Витая пара
20	5	7	Кольцо	Оптоволоконный
21	2	8	Полносвязная	Оптоволоконный
22	6	6	Общая шина	Коаксиальный
23	4	5	Полносвязная	Витая пара
24	4	7	Общая шина	Коаксиальный
25	5	8	Звезда	Витая пара

2. Описать принцип работы, построенной сети

Контрольные вопросы

1. Перечислите достоинства и недостатки коаксиального кабеля?
2. Перечислите достоинства и недостатки витой пары?
3. Перечислите достоинства и недостатки оптоволоконного кабеля?

Практическая работа № 6

Тема Применение методов доступа к среде передачи данных (методы доступа к каналам связи)

Цель закрепить методы доступа к каналам связи

Теоретические сведения

Наиболее известны и распространены три конкретные реализации методов доступа: Ethernet, Arcnet и Token Ring.

Ethernet

Для метода доступа Ethernet используется топология «общая шина», поэтому все сообщения, посылаемые каждым отдельным компьютером, принимаются всеми остальными компьютерами в сети, подключенными к «общей шине». Однако в целенаправленном, предназначенном для конкретной станции сообщении обязательно указан адрес станции назначения и адрес отправителя, поэтому принимает его только станция назначения, а остальные не обращают на него внимания.

Перед началом передачи станция определяет, свободен ли канал связи, и, если свободен - начинает передачу. Однако возможна одновременная передача сообщений двумя и более станциями. В этом случае станции на короткое время задерживают передачу, а затем возобновляют. Практически быстродействие сети уменьшается только при одновременной работе 80 - 100 станций.

Arcnet

Метод доступа Arcnet принадлежит фирме Datapoint Corp. и тоже широко распространен: оборудование Arcnet заметно дешевле, чем оборудование Ethernet или Token Ring. Arcnet применяется в локальных сетях с топологией «звезда». Один из компьютеров создает сообщение специального вида (так называемый маркер), которое передается от одного компьютера к другому последовательно. При передаче обычного информационного сообщения от одной станции к другой очередная станция дожидается маркера и дополняет его этим сообщением, а также адресами

отправителя и назначения. Когда отправленный пакет достигает станции назначения, информационное сообщение отделяется от маркера и передается станции.

Token Ring. Этот метод доступа разработан фирмой IBM и предполагает топологию сети «кольцо». Метод Token Ring во многом напоминает предыдущий метод Arcnet: он использует сообщение-маркер, передаваемое от одной станции к другой; однако здесь есть возможность разным рабочим станциям назначать различные приоритеты.

Методические указания

1. Определить согласно варианту в таблице 6 максимальное время доступа абонента к сети и также время доступа при заданном числе передающих абонентов.

Таблица 6

Варианты заданий

№ варианта	Число абонентов в сети	Число передающих абонентов
1.	10	5
2.	12	6
3.	15	8
4.	11	9
5.	17	13
6.	18	9
7.	14	10
8.	16	12
9.	19	13
10.	14	6
11.	17	9
12.	12	10
13.	11	9
14.	20	17
15.	18	8
16.	23	14
17.	14	8

Контрольные вопросы

1. Характеристики сети Token ring.
2. Структура пакета сети Token ring.
3. Метод управления обменом и правила обмена в сети Token ring.

Практическая работа № 7

Тема Использование асинхронной и синхронной передачи данных

Цель: закрепить знания о использовании асинхронной и синхронной передачи данных

Теоретические сведения

Передача данных – вид электросвязи, обеспечивающий обмен сообщениями между прикладными процессами пользователей, удалённых ЭВМ с целью обработки вычислит. средствами.

Сеть передачи данных – организационно-техническая структура, состоящая из узлов коммутации и каналов связи, соединяющих узлы связи между собой и с оконечным оборудованием, предназначенная для передачи данных между удалёнными точками.

Канал передачи – комплекс технических средств и среды распространения, обеспечивающий передачу сигналов электросвязи в определённой полосе частот и с определённой скоростью передачи между сетевыми станциями и узлам, а также между ними и оконечным устройством.

Синхронная и асинхронная передача данных

При обмене данными по каналам связи используются три метода передачи данных:

1. симплексная (однонаправленная) — TV, радио;
2. полудуплексная передача — (приём и передача данных осуществляются поочерёдно);
3. дуплексная (двунаправленная) – каждая станция одновременно передаёт и принимает данные.

Для передачи данных в информационных системах наиболее часто применяется последовательная (полудуплексная) передача. Она разделяется на два метода:

Асинхронная передача

При асинхронной передаче каждый символ передаётся отдельной посылкой. Стартовые биты предупреждают о начале передачи. Затем

передаётся символ. Для определения достоверности передачи используется бит чётности (бит чётности равен 1, если количество единиц в символе нечётно, и равен 0 в противном случае). Последний бит сигнализирует об окончании передачи (рисунок 9)



Рисунок 9 – Ассинхронная передача

Преимущества:

- 1) несложная отработанная система;
- 2) недорогое интерфейсное оборудование.

Недостатки:

- 1) третья часть пропускной способности теряется на передачу служебных битов;
- 2) невысокая скорость передачи данных по сравнению с синхронной;
- 3) при множественной ошибке с помощью бита чётности невозможно определить достоверность полученной информации.

Асинхронная передача используется в системах, где обмен данными происходит время от времени, и не требуется высокая скорость передачи данных.

б) Синхронная передача.

При использовании синхронного метода данные передаются блоками. Для синхронизации работы приёмника и передатчика в начале блока передаются биты синхронизации.

Затем передаются данные, код обнаружения ошибки и символ окончания передачи. Код обнаружения ошибки вычисляется по содержимому поля данных и позволяет однозначно определить достоверность принятой информации.



Рисунок 10 – Синхронная передача

Преимущества:

- 1) высокая эффективность передачи данных;
- 2) высокая скорость передачи данных;
- 3) надёжный встроенный механизм обнаружения ошибок.

Недостатки:

- 1) Интерфейсное оборудование более сложное и дорогое.

Методические указания

1. Описать цепи и назначение сигналов интерфейса RS-232.
2. Составить краткую сравнительную характеристику протоколов обмена данными X-modem и Z-modem.
3. Составить блок-схемы следующих алгоритмов:
 - алгоритм организации соединения и ведения диалога с удаленным абонентом;
 - алгоритм организации соединения и передачи файлов;
 - алгоритм организации соединения и приема файлов.

Контрольные вопросы

1. Протоколы X-modem и Z-modem.
2. Цепи и назначение сигналов интерфейса RS-232.
3. Методы управления потоком в модеме и режимы обмена данными между модемом и компьютером.

Практическая работа № 8

Тема Настройка протокола TCP/IP в операционных системах

Цель: обобщение и систематизация знаний по вопросам настройки протокола TCP/IP

Теоретические сведения

TCP/IP — это аббревиатура термина Transmission Control Protocol / Internet Protocol (Протокол управления передачей / Протокол Интернета).

Протокол — это заранее согласованный стандарт, который позволяет двум компьютерам обмениваться данными. Фактически TCP/IP не один протокол, а несколько. Именно поэтому его называют набором, или комплектом, протоколов, среди которых TCP и IP — два основных.

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

- обеспечивает межсетевое взаимодействие компьютеров с разной аппаратной архитектурой и ОС;
- является основным протоколом, используемым в Интернете;
- необходим для функционирования Active Directory («активный каталог», хранит данные и настройки среды в централизованной базе данных).

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

Реализация протокола TCP/IP в ОС Windows дает следующие преимущества:

1. стандартный корпоративный сетевой протокол, который представляет собой наиболее завершённый и популярный сетевой протокол. Все современные ОС поддерживают TCP/IP, а почти все большие сети передают основную часть своего трафика с помощью протокола TCP/IP;
2. метод получения доступа к Интернету;

3. технология для соединения разнородных систем. Он предоставляет многие стандартные средства взаимодействия для доступа и передачи данных между разнородными системами, включая протокол передачи файлов FTP и протокол эмуляции терминала Telnet;

4. устойчивая масштабируемая межплатформенная среда для приложений клиент-сервер.

Протокол TCP/IP в среде Windows содержит:

1. базовые протоколы — TCP, IP, UDP, ARP, ICMP;

2. прикладные программные интерфейсы — Windows Sockets для сетевого программирования, RPC для взаимодействия между компьютерами, NetBIOS для использования логических имен и сессий в сети, сетевую версию DDE для разделения информации, встроенной в документы, по сети;

3. сервисы прикладного уровня — Finger, FTP, RCP, REXEC, RSH, Telnet, TFTP. Эти сервисы позволяют пользователям Windows Server использовать ресурсы компьютеров с ОС, разработанными отличными от Microsoft компаниями, например, UNIX;

4. диагностические средства TCP/IP — ARP, HOSTNAME, IPCONFIG, NBTSTAT, NETSTAT, PING, ROUTE. Эти утилиты используются для обнаружения и устранения сетевых проблем при работе со стеком TCP/IP.

Сервисы прикладного уровня стека TCP/IP реализованы в Windows в виде утилит, которые работают в режиме командной строки (кроме утилиты telnet). Некоторые вспомогательные утилиты реализуют протоколы или некоторые функции протоколов нижних уровней, таких как ICMP или ARP. Имеются также утилиты, не реализующие коммуникационные протоколы, а отображающие информацию о конфигурации стека TCP/IP или сессии TCP/IP.

Можно выделить некоторые утилиты TCP/IP:

– PING — проверяет конфигурацию и тестирует соединения;

– FTP — обеспечивает двунаправленную передачу файлов между компьютерами Windows NT и хостами TCP/IP с использованием протокола UDP;

– TELNET — обеспечивает эмуляцию терминала;

– IPCONFIG — отображает текущую конфигурацию стека TCP/IP.

Методические указания

1. Проверьте работоспособность стека протоколов TCP/IP

a) Запустите виртуальную машину VM-1 и загрузите ОС Windows.

b) Запустите консоль (*Пуск/Программы/Стандартные/Командная строка*).

c) В командной строке введите `ipconfig /all / more`.

2. Используя приведенную ниже информацию, создайте в своей папке текстовый документ со следующими данными:

a) имя компьютера;

b) основной DNS-суффикс;

c) описание DNS-суффикса для подключения;

d) физический адрес;

e) DHCP включен;

f) автоконфигурация включена;

g) IP-адрес автоконфигурации;

h) маска подсети;

i) шлюз по умолчанию.

3. Убедитесь в работоспособности стека *TCP/IP*, отправив эхо-запросы на IP-адреса. Для этого воспользуйтесь командой `ping`:

a) отправьте эхо-запросы на локальный адрес компьютера (loopback) `ping 127.0.0.1` (на экране должны появиться сообщения о полученном ответе от узла 127.0.0.1);

b) отправьте эхо-запрос по другому IP-адресу, например 172.21.5.1.

4. Настройте стек протоколов TCP/IP для использования статического IP-адреса.

a) Откройте окно Сетевые подключения (*Пуск/Панель управления/Сетевые подключения*).

b) Вызовите свойства подключения по локальной сети. Для этого можно воспользоваться контекстным меню.

c) В появившемся диалоговом окне на вкладке Общие откройте свойства Протокол Интернета TCP/IP.

d) Щелкните переключатель *Использовать следующий IP-адрес* и введите в соответствующие поля данные: IP_адрес; Маску подсети; Основной шлюз; Предпочитаемый DNS.

e) Примените параметры кнопкой *OK*.

f) Закройте окно свойств подключения кнопкой *OK* (если потребуется, то согласитесь на перезагрузку компьютера).

g) Проверьте работоспособность стека протоколов *TCP/IP*.

5. Настройте TCP/IP для автоматического получения IP-адреса.

a) Откройте окно Сетевые подключения.

b) Вызовите свойства Подключения по локальной сети.

c) Откройте свойства Протокол Интернета TCP/IP.

d) Установите переключатель *Получить IP-адрес автоматически*.

e) Закройте диалоговое окно Свойства: Протокол Интернета TCP/IP кнопкой *OK*.

f) Примените параметры кнопкой *OK*.

g) Проверьте настройку стека протоколов *TCP/IP*.

6. Получите другой адрес для своего компьютера. Для этого:

– запустите консоль (командную строку);

– введите команду для сброса назначенных адресов - `ipconfig /release`;

– введите команду для получения нового адреса `ipconfig / renew`;

7. Проверьте работоспособность стека протоколов *TCP/IP*.

Контрольные вопросы

1. Опишите параметры, используемые при настройке статического адреса TCP/IP.
2. Какие преимущества дает применение стека протоколов TCP/IP.
3. Дайте определение понятию стек протоколов TCP/IP.

Практическая работа № 9

Тема: Работа с диагностическими утилитами протокола TCP/IP.

Цель: научиться работать с диагностическими утилитами протокола TCP/IP

Теоретические сведения

Целью диагностических утилит является устранения неисправностей в настройке TCP/IP и восстановление нормальной работы сети. Для поиска неисправностей можно использовать специальные диагностические утилиты, предназначенные для проверки конфигурации стека TCP/IP и тестирования сетевого соединения.

Список некоторых утилит приведен в таблице 7

Таблица 7

Диагностические утилиты TCP/IP

Утилита	Применение
arp	Выводит для просмотра и изменения таблиц 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.

Методические указания

1. Получение справочной информации по командам

Выведите на экран справочную информацию по всем рассмотренным утилитах (смотри таблицу 8). Для этого в командной строке введите имя утилиты без параметров и дополните /?.

Сохраните справочную информацию в отдельном файле.

Изучите ключи, используемые при запуске утилит.

2. Получение имени хоста

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

3. Изучение утилиты ipconfig

Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Заполните таблицу 8:

Таблица 8

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

4. Тестирование связи с помощью утилиты ping.

а) Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.

б) Проверьте функционирование основного шлюза, послав 5 эхо-пакетов длиной 64 байта.

с) Проверьте возможность установления соединения с удаленным хостом.

d) Проверить с помощью ping, можете ли вы обратиться к компьютерам в своей локальной сети. Сравнить результаты выполнения программы ping с указанием адреса компьютера, который отключен, и несуществующего адреса. Отличаются ли эти результаты?

e) Проверить возможность установления соединения с различными удаленными хостами, используя DNS-имена. Определите IP-адреса этих узлов. Отметить время отклика (время кругового обращения пакета). Попробовать увеличить время отклика. Как влияет размер пакета на время кругового обращения?

5. Определение пути IP-пакета.

– Воспользоваться командой tracer для определения числа участков маршрута от вашего компьютера к различным хостам (локальному хосту, шлюзу по умолчанию, удаленному хосту). Отметьте, через какие промежуточные узлы проходят эхо-пакеты.

– Сравнить значения времени кругового обращения, полученные при выполнении программы ping, с числом участков маршрута, полученным при выполнении программы tracer, для ряда адресов назначения. Существует ли зависимость между продолжительностью задержки и числом участков маршрута?

6. Просмотр ARP-кэша

a) С помощью утилиты arp просмотрите ARP-таблицу локального компьютера.

b) Внести в кэш локального компьютера любую статическую запись.

7. Просмотр локальной таблицы маршрутизации.

c) С помощью утилиты netstat вывести перечень сетевых соединений и прослушиваемых портов локального узла.

d) Получить статистическую информацию для протоколов UDP, TCP, ICMP, IP.

е) Вывести на экран локальную таблицу маршрутизации. Изучить ее содержимое.

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

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

Контрольные вопросы

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. Каково назначение протокола ARP?

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

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

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

8. Какой тип записи запрашивает у DNS-сервера простейшая форма nslookup?

Практическая работа № 10

Тема: Решение проблем с TCP/IP

Цель: научиться решать проблемы с протоколом TCP/IP

Краткие теоретические сведения

Даже в самом простом случае сети с двумя узлами, существует много аппаратуры и параметров программного обеспечения, взаимосвязь между которыми может значительно влиять на эффективность работы сети.

Обычно, подход к такой сложной проблеме должен начинаться с декомпозиции общей проблемы на более мелкие части и так далее, до нахождения первоисточников проблемы и затем уж выполняется систематический и логический план удаления возможных причин, пока не будет достигнуто её решение.

Ограничивают производительность TCP/IP обычно следующие факторы:

- недостаточное относительное быстродействие аппаратных средств;
- количество циклов CPU, необходимых для выполнения данной части кода;
- размер пакетов, передаваемых данных;
- производительность, с которой данные кэшируются в клиентской памяти, промежуточном звене и системах сервера;
- качество кода пользователей, который обращается к подсистеме локальной вычислительной сети.

Таким образом, нужно понимать, как каждый из этих факторов способствует недостаточной сетевой эффективности.

Методические указания

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.

1. 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).

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

a) Использует ли машина статичную или динамичную конфигурацию?

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

c) Получает ли машина адрес DNS сервера автоматически?

d) Если адрес DNS сервера вводится вручную, то какой адрес используется?

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

f) Проверьте тип адаптера.

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

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

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

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

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

Контрольные вопросы

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

Практическая работа № 11 (часть 1)

Тема Преобразование форматов IP-адресов

Цель: обобщение и систематизация знаний по теме «Адресация в сетях»

Краткие теоретические сведения

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например, 128.10.2.30 - традиционная десятичная форма представления адреса, а 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая - к номеру узла, определяется значениями первых бит адреса. Значения этих бит являются также признаками того, к какому *классу* относится тот или иной IP-адрес.

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов.

- Если весь IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет; этот режим используется только в некоторых сообщениях ICMP.

- Если в поле номера сети стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет.

- Если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется *ограниченным широковещательным сообщением (limited broadcast)*.

- Если в поле номера узла назначения стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети. Например, пакет с адресом 192.190.21.255 доставляется всем узлам сети

192.190.21.0. Такая рассылка называется *широковещательным сообщением (broadcast)*.

При адресации необходимо учитывать те ограничения, которые вносятся особым назначением некоторых IP-адресов.

Особый смысл имеет IP-адрес, первый октет которого равен 127. Он используется для тестирования программ и взаимодействия процессов в пределах одной машины. Когда программа посылает данные по IP-адресу 127.0.0.1, то образуется как бы «петля».

Данные не передаются по сети, а возвращаются модулям верхнего уровня как только что принятые. Поэтому в IP-сети запрещается присваивать машинам IP-адреса, начинающиеся со 127. Этот адрес имеет название *loopback*. Можно отнести адрес 127.0.0.0 ко внутренней сети модуля маршрутизации узла, а адрес 127.0.0.1 - к адресу этого модуля на внутренней сети.

На самом деле любой адрес сети 127.0.0.0 служит для обозначения своего модуля маршрутизации, а не только 127.0.0.1, например 127.0.0.3.

Особые адреса

В протоколе IP нет понятия широковещательности в том смысле, в котором оно используется в протоколах канального уровня локальных сетей, когда данные должны быть доставлены абсолютно всем узлам.

Как ограниченный широковещательный IP-адрес, так и широковещательный IP-адрес имеют пределы распространения в интерсети - они ограничены либо сетью, к которой принадлежит узел-источник пакета, либо сетью, номер которой указан в адресе назначения.

Поэтому деление сети с помощью маршрутизаторов на части локализует широковещательный шторм пределами одной из составляющих общую сеть частей просто потому, что нет способа адресовать пакет одновременно всем узлам всех сетей составной сети.

Методические указания

1. Переведите следующие двоичные числа в десятичные.

Двоичное значение

- | | |
|---------------|--|
| 1. 1111011 | 5. 10101100.00101000.00000000.00000000 |
| 2. 1001001101 | 6. 01011110.01110111.10011111.00000000 |
| 3. 101101111 | 7. 10010001 0110000 10000000 00011001 |
| 4. 1011110001 | 8. 01111111 00000000 00000000 00000001 |

2. Переведите следующие десятичные числа в двоичные.

Десятичное значение

- | | |
|--------|--------------------|
| 1. 250 | 5. 874 |
| 2. 19 | 6. 109.128.255.254 |
| 3. 348 | 7. 131.107.2.89 |
| 4. 93 | 8. 129.46.78.0 |

3. Укажите классы следующих IP-адресов.

Адрес

- | | |
|------------------|-----------------|
| 1. 126.102.128.0 | 5. 168.224.0.1 |
| 2. 1.191.248.0 | 6. 201.76.98.5 |
| 3. 185.74.41.184 | 7. 186.112.0.10 |
| 4. 96.247.128.0 | 8. 28.0.0.0 |

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

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

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?

Практическая работа № 11 (часть 2)

Тема «Расчет IP-адреса и маски подсети»

Цель: научиться производить расчёт IP-адреса и маски подсети

Краткие теоретические сведения

Маска подсети — битовая маска для определения по IP-адресу адреса подсети и адреса узла (хоста, компьютера, устройства) этой подсети. В отличие от IP-адреса маска подсети не является частью IP-пакета.

Благодаря маске можно узнать, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу самого узла в этой сети.

Маски подсети являются основой метода бесклассовой маршрутизации (англ. *CIDR*). При этом подходе маску подсети записывают вместе с IP-адресом в формате «*IP-адрес/количество единичных бит в маске*». Число после знака дроби (т. н. *длина префикса сети*) означает количество единичных разрядов (бит) в маске подсети.

Методические указания

1. Выполните логическую операцию «И» с перечисленными ниже IP-адресами и маской подсети и определите, принадлежит ли IP-адрес получателя к локальной или удаленной сети.

IP-адрес отправителя	10011001 1010101000100101 10100011
Маска подсети	11111111 111111110000000000000000
Результат	
IP-адрес получателя	11011001 10101010 10101100 11101001
Маска подсети	11111111 111111110000000000000000
Результат	
1. Получен ли одинаковый результат?	

2. Принадлежит IP-адрес получателя к локальной или удаленной сети? Для заданных IP-адресов классов А, В и С и предложенных масок определить:

- a) класс адреса;
- b) максимально возможное количество подсетей;
- c) диапазон изменения адресов подсетей;
- d) максимальное число узлов в подсетях.

№	Адрес	Маска
1.	135.209.23.246	11111111.11111111.11111111.11000000
2.	200.131.197.27	11111111.11111111.11111111.11111000
3.	214.147.120.38	11111111.11111111.11111111.11110000
4.	176.72.82.62	11111111.11111111.11111111.10000000
5.	82.67.174.114	11111111.11000000.00000000.00000000

3. По заданным классу (А, В или С), количеству подсетей N и максимальному количеству компьютеров M1...MN в каждой подсети определить маску для разбиения на подсети. Сделать вывод о возможности такого разбиения. Если разбиение невозможно, то сформулируйте рекомендации по изменению каких-либо исходных данных для обеспечения возможности разбиения.

1.	Класс	А							
	N	3							
	M1...MN	1568		55996				1555847	
2.	Класс	В							
	N	4							
	M1...MN	1024	2048	4069				1024	
3.	Класс	С							
	N	8							
	M1...MN	12	10	5	8	15	16	13	12

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?

Практическая работа № 12

Тема Монтаж кабельных сред технологий Ethernet

Цель: научиться производить монтаж кабельных сред технологии Ethernet

Теоретические сведения

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.

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 (рисунок 11)



Рисунок 11 – Конструкция коаксиального кабеля

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 12), BNC T коннектор (рисунок 13) и BNC баррел коннектор.



Рисунок 12 – BNC коннектор



Рисунок 13 – 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 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.

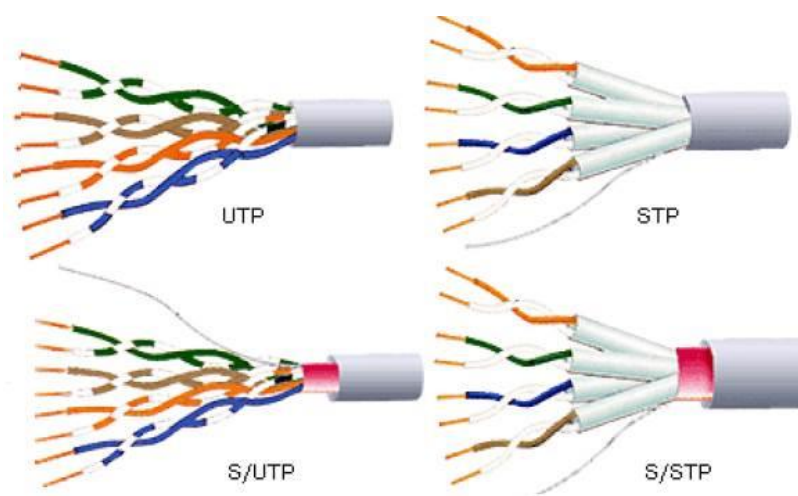


Рисунок 14 – Витая пара

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 персональных компьютеров друг с другом.

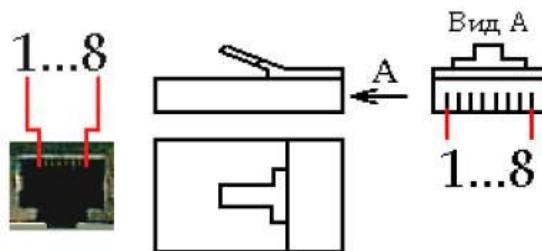


Рисунок 15 – Порт MDI/MDI-X и разъем RJ-45

Таблица 9

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 10

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 оптоволоконна

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 16 – Структура оптоволоконного кабеля: 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 оптоволоконном, может достигать 100 километров.

Стоит оптический кабель чрезвычайно дорого, и для работы с ним требуется специальные сетевые карты, коммутаторы и т.д. Без специального оборудования оптоволоконно 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.

Методические указания

1. Надрезать внешнюю оболочку кабеля специальным инструментом и снять на длину 2-3 см.
2. Расплести проводники и упорядочить их согласно выбранной схемы
3. Выровнять и распрямить концы проводников, а после - обрезать, оставив от оболочки кабеля примерно 12,5 мм.
4. Зажимая оболочку кабеля одной рукой, другой аккуратно оденете на кабель коннектор, держа его защелкой вниз и следя, чтобы проводники зашли в коннектор до упора и не перепутались, а оболочка кабеля вошла в корпус. Осталось только аккуратно вставить оконцованный кабель в специальные обжимные клещи (кримпер), несколько раз плавно их нажать.
5. Убедитесь, что проводники и оболочка кабеля не сдвинулись, а ножи равномерно и без загиба вонзились в проводники. Зажимаются не только проводники, но и сама оболочка кабеля потому следите, чтобы она достаточно заходила в корпус.
6. Если кабель очень тонкий (встречаются двухпарные кабеля диаметром 2-3 мм) - для надежного обжима оболочки можно намотать немножко изолянты или надеть подходящий кембрик (кусочек оболочки толстой витой пары)

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.

Практическая работа № 13

Тема Настройка удаленного доступа к компьютеру

Цель: научиться производить настройку удаленного доступа к компьютеру

Теоретические сведения

С помощью функции подключения к удаленному рабочему столу можно подключиться с одного компьютера под управлением Windows к другому. Для этого оба компьютера должны быть подключены к одной сети или к Интернету. Например, с домашнего компьютера можно работать с программами, файлами и сетевыми ресурсами рабочего компьютера точно так же, как в офисе.

Для подключения к удаленному компьютеру пользователю необходимы: включенный компьютер с сетевым подключением, включенный удаленный рабочий стол, сетевой доступ к удаленному компьютеру (например, через Интернет) и разрешение на подключение. Для получения разрешения на подключение необходимо быть в списке пользователей.

Перед подключением рекомендуется определить имя целевого компьютера и убедиться, что в его брандмауэре разрешены подключения к удаленному рабочему.

Чтобы получить возможность подключаться к удаленному компьютеру, необходимо добавить пароль к учетной записи (если в текущей учетной записи пользователя не требуется пароль для входа).

Методические указания

Настройка удаленного рабочего стола

1. Для настройки удаленного доступа необходимо открыть свойства системы. Находим ярлык «Этот компьютер» и нажимаем на него правой кнопкой мышки.
2. В появившемся окне нажимаем «Свойства». Далее, откроется меню, в котором следует выбрать «Настройка удаленного доступа». Здесь нас интересует вкладка «Удаленный доступ», в которой мы можем разрешить или запретить подключение

3. Выбираем один из вариантов соединения.

4. Выбираем пункт «Разрешить удаленные подключения к этому компьютеру». Убираем галочку с пункта «Проверка подлинности на уровне сети». Нажимаем «Ок».

5. На этом настройка завершена. Стоит также отметить, что удаленный доступ не будет возможен только для участников одной группы. То есть все компьютеры должны быть подключены к одной сети и иметь одинаковое название рабочей группы.

Подключение к удаленному компьютеру

6. Теперь необходимо запустить службу, которая выполняет подключение к компьютерам. Открыть сервис можно при помощи нажатия комбинации клавиш Win+R. В появившемся окне пишем команду mstsc и нажимаем «Enter».

7. В появившемся окне требуется ввести IP-адрес компьютера, к которому нужно получить доступ, и нажимаем «Подключиться».

8. Запустится окно. В нем необходимо ввести имя и ключ учетной записи устройства, с которым нужно соединиться.

9. Далее, может появиться окно, сообщающее вам, что не удалось проверить сертификат удаленного компьютера. Нажимаем «Да».

10. После этого, если все данные введены правильно, вы попадете на рабочий стол удаленного компьютера.

Контрольные вопросы

1. Для чего необходимо удаленное подключение компьютера?
2. Как подключиться к другому компьютеру по локальной сети?
3. Что такое сертификат удаленного компьютера?

Практическая работа № 14

Тема Использование принципов работы технологий глобальных сетей на основе выделенных линий

Цель: обобщение и систематизация знаний по теме технологии глобальных сетей

Теоретические сведения

Выделенный канал — это канал с фиксированной полосой пропускания или фиксированной пропускной способностью, постоянно соединяющий двух абонентов. Абонентами могут быть как отдельные устройства (компьютеры или терминалы), так и целые сети.

Выделенные каналы обычно арендуются у компаний — операторов территориальных сетей, хотя крупные корпорации могут прокладывать свои собственные выделенные каналы.

Выделенные каналы делятся на аналоговые и цифровые в зависимости оттого, какого типа коммутационная аппаратура применена для постоянной коммутации абонентов — FDM или TDM.

На аналоговых выделенных линиях для аппаратуры передачи данных физический и канальный протоколы жестко не определены. Отсутствие физического протокола приводит к тому, что пропускная способность аналоговых каналов зависит от пропускной способности модемов, которые использует пользователь канала.

Модем собственно и устанавливает нужный ему протокол физического уровня для канала. На цифровых выделенных линиях протокол физического уровня зафиксирован — он задан стандартом G.703.

На канальном уровне аналоговых и цифровых выделенных каналов обычно используется один из протоколов семейства HDLC или же более поздний протокол PPP, построенный на основе HDLC для связи многопротокольных сетей.

Методические указания

1. Заполните таблицу 11

Таблица 11

Протоколы модемной связи

Название стандарта	Стандарт определяет	Основные технические характеристики
V.22		
V.22bis		
V.32		
V.32bis		
V.34		
V.42		
V.42bis		
V.90		
V.92.		
V.100.		
V.120.		
V.150.1		

2. Составьте схему подключения модема. При составлении схемы принять следующие исходные данные. Имеются два ПК. Первый ПК укомплектован внешним модемом, второй – внутренним модемом. На обоих ПК предусмотреть использование телефонов. Телефонная сеть двухпроводная.

3. Поясните назначение световых индикаторов на лицевой панели внешнего модема.

4. Составьте перечень команд, обеспечивающих следующую инициализацию модема:

- разрешить эхо-вывод команд, передаваемых модему;
- разрешить ответ модема на AT-команды в символьном виде;

- выводить сообщения модема об установлении связи в полном виде;
- номер набирается модемом после паузы при наличии гудка на линии;
- состояние «занято» определяется;
- сигнал DCD устанавливается только тогда, когда модем обнаруживает несущую частоту от удаленного модема;
- режим автоответа выключен;
- при тональном наборе длительность передачи одной цифры номера должна быть 55 миллисекунд.

5. Составьте схему и опишите локальный аналоговый тест с самотестированием

Контрольные вопросы

1. Назначение модемов?
2. Взаимодействие модемов с оконечным оборудованием и каналом связи?
3. Описать световые индикаторы на лицевой панели внешнего модема и их назначение?

Практическая работа № 15

Тема Использование принципов работы технологий глобальных сетей на основе коммутации каналов и пакетов

Цель: закрепить использование технологий глобальных сетей на основе коммутации каналов и пакетов

Теоретические сведения

Любые сети передачи данных поддерживают некоторый способ коммутации своих абонентов между собой. Этими абонентами могут быть удаленные компьютеры, локальные сети, факс-аппараты или просто собеседники, общающиеся с помощью телефонных аппаратов.

Практически невозможно предоставить каждой паре взаимодействующих абонентов свою собственную некоммутируемую физическую линию связи, которой они могли бы монопольно «владеть» в течение длительного времени. Поэтому в любой сети всегда применяется какой-либо способ коммутации абонентов, который обеспечивает доступность имеющихся физических каналов одновременно для нескольких сеансов связи между абонентами сети.

В самом общем виде задача соединения конечных узлов через сеть транзитных узлов называется задачей коммутации. Она может быть представлена в виде нескольких взаимосвязанных задач.

- определение информационных потоков, для которых требуется прокладывать путь;
- определение маршрутов для потоков;
- продвижение потоков;
- мультиплексирование и демultipлексирование потоков.

Определение информационных потоков. Через один транзитный узел может происходить одновременно несколько сеансов передачи данных, принадлежащих разным абонентам. Транзитный узел должен уметь распознавать потоки данных, которые на него поступают, для того, чтобы

отрабатывать их передачу именно на тот свой интерфейс, который ведет к нужному узлу.

Информационным потоком называют непрерывную последовательность байтов (которые могут быть агрегированы в более крупные потоки данных – пакеты, кадры, ячейки), объединенных набором общих признаков, выделяющих его из общего сетевого трафика.

В качестве обязательного признака при коммутации выступает адрес назначения данных, поэтому весь поток входящих в транзитный узел данных должен разделяться как минимум на подпотоки, имеющие различные адреса назначения. Лучше, если в качестве признака используется пара адресов конечных узлов – адрес отправителя и получателя.

Определение маршрутов. Выбрать путь или маршрут передачи данных – значит определить последовательность транзитных узлов и их интерфейсов, через которые надо передавать данные, чтобы доставить их адресату.

Если путей несколько, то задача состоит в выборе из нескольких – оптимального пути. В качестве критериев оптимальности могут выступать пропускная способность, загруженность каналов, задержки, надежность каналов. Для этого конечные узлы и другие устройства сети оснащаются специальными программными средствами, которые организуют взаимный обмен служебными сообщениями, позволяющий каждому узлу составить свое представление и топологии сети. Затем на основании исследования и математических алгоритмов определяются рациональные маршруты.

Продвижение потоков. Когда задача определения маршрута решена, должно произойти соединение, или коммутация абонентов. Отправитель должен выставить данные на тот свой порт, из которого выходит найденный маршрут, а все транзитные узлы должны соответствующим образом выполнить «переброску» данных с одного своего порта на другой, то есть выполнить коммутацию.

Мультиплексирование и демультиплексирование. Прежде чем выполнить переброску данных с одного интерфейса на другой, коммутатор должен понять, к какому потоку они относятся. Эта задача должна решаться независимо от того, поступает ли на вход коммутатора только один поток в чистом виде, или смешанный поток, являющийся результатом агрегирования нескольких потоков.

В последнем случае к задаче распознавания добавляется задача демультиплексирования – разделение суммарного агрегированного потока на несколько составляющих потоков. Как правило, операцию коммутации сопровождает операция – мультиплексирование (*multipleing*), при которой из нескольких отдельных потоков образуется общий агрегированный поток, который можно передавать по одному физическому каналу связи.

На сегодняшний день существуют две принципиально различные схемы коммутации абонентов в сетях: коммутация каналов (*circuit switching*), коммутация пакетов (*packet switching*).

Коммутация каналов подразумевает образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между двумя узлами сети.

Отдельные каналы соединяются между собой специальной аппаратурой - коммутаторами, которые могут устанавливать связи между любыми конечными узлами сети.

В сети с коммутацией каналов перед передачей данных всегда необходимо выполнить процедуру установления соединения, в процессе которой и создается составной канал. Коммутаторы, а также соединяющие их каналы должны обеспечивать одновременную передачу данных нескольких абонентских каналов. Для этого они должны быть высокоскоростными и поддерживать какую-либо технику мультиплексирования абонентских каналов.

В настоящее время для мультиплексирования абонентских каналов используются две техники:

- техника частотного мультиплексирования (Frequency Division Multiplexing, FDM);

- техника мультиплексирования с разделением времени (Time Division Multiplexing, TDM).

В зависимости от направления возможной передачи данных способы передачи данных по линии связи делятся на следующие типы:

- симплексный - передача осуществляется по линии связи только в одном направлении;

- полудуплексный - передача ведется в обоих направлениях, но попеременно во времени;

- дуплексный - передача ведется одновременно в двух направлениях.

Сети с коммутацией каналов можно разделить на два класса:

- сети с динамической коммутацией;

- сети с постоянной коммутацией.

В сетях с динамической коммутацией:

- разрешается устанавливать соединение по инициативе пользователя сети;

- коммутация выполняется только на время сеанса связи, а затем (по инициативе одного из пользователей) разрывается;

- время соединения между парой пользователей составляет от нескольких секунд до нескольких часов и завершается после выполнения определенной работы - передачи файла, просмотра страницы текста или изображения и т.п.

Сеть, работающая в режиме постоянной коммутации:

- разрешает паре пользователей заказать соединение на длительный период времени;

- соединение устанавливается не пользователями, а персоналом, обслуживающим сеть;

период, на который устанавливается постоянная

- коммутация, составляет обычно несколько месяцев.

Свойства сетей с коммутацией каналов.

Если соединение в сети установлено, то абоненту выделяется фиксированная пропускная способность, которая остается неизменной в течение всего периода соединения с низким и постоянным уровнем задержки передачи данных через сеть.

Гарантированная пропускная способность сети после установления соединения является важным свойством, необходимым для таких приложений, как передача голоса, изображения или управления объектами в реальном масштабе времени.

Недостатком сетей с коммутацией каналов является обязательная задержка перед передачей данных, из-за фазы установления соединения, невозможность применения пользовательской аппаратуры, работающей с разной скоростью, нерациональное использование пропускной способности физических каналов, невозможность динамически изменять пропускную способность канала по требованию абонента сети. Это делает сети с коммутацией каналов неэффективными в условиях пульсирующего трафика.

Коммутация пакетов - это техника коммутации абонентов, которая была специально разработана для эффективной передачи компьютерного трафика. При коммутации пакетов все передаваемые пользователем сети сообщения предварительно разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами.

Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета узлу назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения.

Пакеты транспортируются в сети как независимые информационные блоки. Коммутаторы сети принимают пакеты от конечных узлов и на основании адресной информации передают их друг другу, а в конечном итоге - узлу назначения. Коммутаторы пакетной сети отличаются от коммутаторов

каналов тем, что они имеют внутреннюю буферную память для временного хранения пакетов, если выходной порт коммутатора в момент принятия пакета занят передачей другого пакета. В этом случае пакет находится некоторое время в очереди пакетов в буферной памяти выходного порта, а когда до него дойдет очередь, то он передается следующему коммутатору

В сетях коммутации пакетов различают два режима работы: режим виртуальных каналов (другое название - связь с установлением соединения) и дейтаграммный режим (связь без установления соединения).

При передаче пакетов по *виртуальному каналу* (*virtual circuit* или *virtual channel*) перед тем, как начать передачу данных между двумя конечными узлами, должен быть установлен виртуальный канал, который представляет собой единственный маршрут, соединяющий эти конечные узлы.

Виртуальный канал может быть динамическим или постоянным. Динамический виртуальный канал устанавливается при передаче в сеть специального пакета - запроса на установление соединения. Этот пакет проходит через коммутаторы и «прокладывает» виртуальный канал. Это означает, что коммутаторы запоминают маршрут для данного соединения и при поступлении последующих пакетов данного соединения отправляют их всегда по проложенному маршруту.

Постоянные виртуальные каналы создаются администраторами сети путем ручной настройки коммутаторов. При отказе коммутатора или канала на пути виртуального канала соединение разрывается, и виртуальный канал нужно прокладывать заново.

В *режиме виртуальных каналов* пакеты одного сообщения передаются в естественном порядке по устанавливаемому маршруту. При этом линии связи могут разделяться многими сообщениями, когда попеременно по каналу передаются пакеты разных сообщений.

Предусматривается контроль правильности передачи данных путем посылки от получателя к отправителю подтверждающего сообщения -

положительной квитанции. Этот контроль возможен как во всех промежуточных узлах маршрута, так и только в конечном узле.

В дейтаграммном режиме сообщение делится на дейтаграммы.

Дейтаграмма - часть информации, передаваемая независимо от других частей одного и того же сообщения в вычислительных сетях с коммутацией пакетов.

Дейтаграммы одного и того же сообщения могут передаваться в сети по разным маршрутам и поступать к адресату в произвольной последовательности, что может послужить причиной блокировок сети. На внутренних участках маршрута контроль правильности передачи не предусмотрен и надежность связи обеспечивается лишь контролем на конечном узле.

Дейтаграммный метод не требует предварительного установления соединения и поэтому работает без задержки перед передачей данных. Это особенно выгодно для передачи небольшого объема данных, когда время установления соединения может быть соизмеримым со временем передачи данных. Кроме того, дейтаграммный метод быстрее адаптируется к изменениям в сети.

Блокировкой сети в дейтаграммном режиме называется такая ситуация, когда в буферную память узла вычислительной сети поступило столько пакетов разных сообщений, что эта память оказывается полностью занятой. Следовательно, она не может принимать другие пакеты и не может освободиться от уже принятых, так как это возможно только после поступления всех дейтаграмм сообщения.

Свойства сетей с коммутацией пакетов.

Общая высокая пропускная способность сети при передаче пульсирующего трафика, возможность динамически перераспределять пропускную способность физических каналов связи между абонентами в соответствии с реальными потребностями их трафика.

Но процесс передачи данных для определенной пары абонентов в сети с коммутацией пакетов является более медленным, чем в сети с коммутацией каналов. Величина задержки пакетов данных может достигать значительных величин в моменты перегрузок сети, возможны потери данных из-за переполнения буферов.

Неопределенная пропускная способность сети с коммутацией пакетов - это плата за ее общую эффективность при некотором ущемлении интересов отдельных абонентов. На эффективность работы сети существенно влияют размеры пакетов, которые передает сеть.

Слишком большие размеры пакетов приближают сеть с коммутацией пакетов к сети с коммутацией каналов, поэтому эффективность сети при этом падает. Слишком маленькие пакеты заметно увеличивают долю служебной информации, так как каждый пакет несет с собой заголовок фиксированной длины, а количество пакетов, на которые разбиваются сообщения, будет резко расти при уменьшении размера пакета.

Существует некоторая золотая середина, которая обеспечивает максимальную эффективность работы сети, однако ее трудно определить точно, так как она зависит от многих факторов, некоторые из них к тому же постоянно меняются в процессе работы сети. На ненадежных каналах необходимо уменьшать размеры пакетов, так как это уменьшает объем повторно передаваемых данных при искажениях пакетов,

Пропускная способность сетей в режиме коммутации

Основная задача, для решения которой строится сеть - быстрая передача информации между компьютерами. Поэтому критерии, связанные с пропускной способностью сети или части сети, хорошо отражают качество выполнения сетью ее основной функции.

Пропускная способность характеризует максимально возможное количество данных переданных по линии связи в единицу времени. В качестве единицы измерения передаваемой информации обычно используются пакеты (или кадры, далее эти термины будут использоваться

как синонимы) или биты. Соответственно, пропускная способность измеряется в пакетах в секунду или же в битах в секунду.

Одним из отличий метода коммутации пакетов от метода коммутации каналов является неопределенность пропускной способности соединения между двумя абонентами.

В случае использования сети *коммутации каналов*, данные после задержки, связанной с установлением составного канала, начинают передаваться на максимальной для канала скорости. Время передачи сообщения в сетях с коммутацией каналов равно

$$T_{к.к.}=(W/C),$$

где W - объем сообщения в битах,

C - пропускная способность канала в битах в секунду.

Задержка передачи данных в сетях с коммутацией пакетов определяется (складывается из) временем передачи сообщения и задержкой распространения сигнала по линии связи.

Задержка распространения сигнала

$$T_3=(S/V)$$

где S - расстояние передачи в км,

V – скорость распространения электромагнитных волн в конкретной физической среде и колеблется от 0,6 до 0,9 скорости света в вакууме.

В сети с коммутацией пакетов нужно передать сообщение, которое разделено на пакеты, каждый из которых снабжен заголовком. При передаче этого разбитого на пакеты сообщения по сети с коммутацией пакетов возникают дополнительные задержки по сравнению с сетью с коммутацией каналов.

Во-первых, это задержки в источнике передачи, который, помимо передачи собственно сообщения, тратит дополнительное время на передачу заголовков $t_{п.з.}$, к тому же добавляются задержки $t_{инт.}$, вызванные интервалами между передачей каждого следующего пакета.

Во-вторых, дополнительное время тратится в каждом коммутаторе. Здесь задержки складываются из времени буферизации пакета $t_{б.п.}$ и времени коммутации t_k .

Время буферизации равно времени приема пакета. Время коммутации складывается из времени ожидания пакета в очереди и времени перемещения пакета в выходной порт.

Если время перемещения пакета фиксировано и, как правило, невелико (от нескольких микросекунд до нескольких десятков микросекунд), то время ожидания пакета в очереди колеблется в очень широких пределах и заранее неизвестно, так как зависит от текущей загрузки сети.

Проведем грубую оценку задержки при передаче данных в сетях с коммутацией пакетов по сравнению с сетями с коммутацией каналов на простейшем примере.

Пример. Пусть тестовое сообщение, которое нужно передать в сети с коммутацией канала имеет объем 200 Кбайт. Отправитель находится от получателя на расстоянии 5000 км. Пропускная способность линий связи составляет 2 Мбит/с.

В сети с коммутацией пакетов процедура установления соединения, если она используется, занимает примерно такое же время, как и в сетях с коммутацией каналов, поэтому будем сравнивать только время, затрачиваемое собственно на передачу данных.

Время передачи данных по сети с коммутацией каналов составит:
 $T_{к.к.} = (200 * 1024 * 8) / (2 * 1024 * 1024) = 780 \text{мс.}$

Задержка распространения сигнала в линии связи составит $T_3 = (5000 \text{км} / (0.66 * 300000 \text{км/с})) = 25 \text{мс.}$

Таким образом, общая задержка передачи данных (или общее время, затрачиваемое на передачу данных) в сети с коммутацией каналов составит 805мс.

При передаче сообщения по сети с коммутацией пакетов, обладающей такой же суммарной длиной и пропускной способностью каналов,

пролегающих от отправителя к получателю, время распространения сигнала и время передачи данных будут такими же - 810 мс. Однако из-за задержек в промежуточных узлах общее время передачи данных увеличится.

Пусть исходное сообщение разбивается на пакеты в 1 Кбайт, всего 200 пакетов. Будем считать, что путь от отправителя до получателя пролегает через 10 коммутаторов.

Вначале оценим задержку, которая возникает в исходном узле. Предположим, что доля служебной информации, размещенной в заголовках пакетов, по отношению к общему объему сообщения составляет 10%.

Следовательно, дополнительная задержка, связанная с передачей заголовков пакетов, составляет 10% от времени передачи целого сообщения, то есть 80 мс.

Если принять интервал между отправкой пакетов равным 1 мс, то дополнительные потери за счет интервалов составят 200 мс.

Таким образом, в исходном узле из-за пакетирования сообщения при передаче возникла дополнительная задержка в 280 мс. Каждый из 10 коммутаторов вносит задержку коммутации, которая может составлять от долей до тысяч миллисекунд.

В данном примере будем считать, что на коммутацию в среднем тратится 20 мс. Кроме того, при прохождении сообщений через коммутатор возникает задержка буферизации пакета. Эта задержка при величине пакета 1 Кбайт и пропускной способности линии 2 Мбит/с равна 4 мс. Общая задержка, вносимая 10 коммутаторами, составляет примерно 240 мс. В результате дополнительная задержка, созданная сетью с коммутацией пакетов, составила 520 мс.

Учитывая, что вся передача данных в сети с коммутацией каналов заняла 805 мс, эту дополнительную задержку можно считать существенной.

Методические указания

1. Определите, на сколько увеличится время передачи данных в сети с коммутацией пакетов по сравнению с сетью с коммутацией каналов, согласно исходных данных индивидуального варианта в таблице 12

Таблица 12

Список вариантов

Вариант	Общий объем передаваемых данных	Суммарная длина канала	Пропускная способность канала	Размер пакета без учета заголовка	Размер заголовка пакета	Межпакетный интервал передачи	Кол-во промежуточных коммутаторов	Время коммутации
	Кбайт	м	Мбит/с	Кбайт	Байт	мс	шт	мс
1	0,1	100	0,1	0,002	2	1	2	20
2	0,5	250	0,2	0,01	4	2	4	20
3	1	500	0,3	0,1	4	3	6	20
4	100	750	0,4	1	10	4	8	20
5	200	1000	0,5	2	20	5	10	20
6	300	1250	0,6	3	30	1	12	20
7	400	1500	0,7	4	40	2	14	20
8	500	1750	0,8	5	50	3	16	20
9	600	2000	0,9	6	60	4	18	20
10	700	2250	1	7	70	5	20	20
11	800	2500	1,1	8	80	1	2	20
12	900	2750	1,2	9	90	2	4	20
13	1000	3000	1,3	1	10	3	6	20
14	2000	3250	1,4	2	20	4	8	20
15	3000	3500	1,5	3	30	5	10	20
16	4000	3750	1,6	4	40	1	12	20
17	5000	4000	1,7	5	50	2	14	20
18	6000	4250	1,8	6	60	3	16	20
19	7000	4500	1,9	7	70	4	18	20
20	8000	4750	2	8	80	5	20	20
21	9000	5000	2,1	9	90	1	5	20
22	10000	5250	2,2	2	20	2	10	20
23	11000	5500	2,3	3	30	3	15	20
24	12000	5750	2,4	4	40	4	20	20
25	100000	6000	2,5	5	50	5	25	20

2. Заполните таблицу 13, отметив в каждой строке, для какого способа коммутации (каналов или пакетов) характерно указанное свойство.

Таблица 13

Свойства коммутации каналов и пакетов

<i>Свойство</i>	<i>Способ коммутации</i>
Гарантированная пропускная способность (полоса для взаимодействующих абонентов)	
Сеть может отказать абоненту в установлении соединения	
Трафик реального времени передается без задержек	
Ресурсы сети используются эффективно при передаче пульсирующего трафика	
Адрес используется только на этапе установления соединения	
Пропускная способность сети для абонентов неизвестна, задержка передачи носит случайный характер	
Сеть всегда готова принять данные от абонента	
Адрес передается с каждым сообщением	
Мультиплексирование на основе синхронного разделения времени	

Контрольные вопросы

1. Опишите принципы функционирования сетей с коммутацией каналов?
2. Опишите принципы функционирования сетей с коммутацией пакетов?
3. Как оценить время передачи данных в сетях с коммутацией каналов?
4. Как оценить время передачи данных в сетях с коммутацией пакетов?
5. Какие более частные задачи включает в себя обобщенная задача коммутации абонентов сети. Дайте краткое описание этих задач?
6. Какой способ коммутации более эффективен для сетей передачи данных: коммутация каналов или коммутация пакетов?

ПРИЛОЖЕНИЕ 1

Общие требования к выполнению и оформлению практических работ

Ход работы:

- изучить теоретический материал;
- выполнить задания;
- описать ход выполнения заданий;
- ответить на контрольные вопросы.

Выполнение практических работ должно быть оформлено в MS WORD.

Отчёт по практической работе должен содержать:

- номер практической работы;
- тему и цель практической работы;
- схемы и структуры;
- заполненные таблицы;
- задачи и их подробное решение;
- ответы на контрольные вопросы;
- выводы по работе.

ПРИЛОЖЕНИЕ 2

Критерии оценки работы студентов на практическом занятии

1. Критерии оценки выполнения практических заданий.

Оценка «отлично» ставится:

- если студент выполнил работу в полном объеме с соблюдением необходимой последовательности действий;
- в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления;
- правильно выполняет анализ ошибок.

Оценка «хорошо» ставится, если студент выполнил требования к оценке «5», но допущены 2-3 недочета.

Оценка «удовлетворительно» ставится,

- если студент выполнил работу не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы;
- в ходе проведения работы были допущены ошибки.

Оценка «неудовлетворительно» ставится, если студент выполнил работу не полностью или объем выполненной части работы не позволяет сделать правильных выводов;

2. Оценивание защиты контрольных вопросов.

Оценка «отлично» ставится в том случае, если студент

- правильно понимает сущность вопроса, дает точное определение и истолкование основных понятий;
- строит ответ по собственному плану, сопровождает ответ новыми примерами, умеет применить знания в новой ситуации;
- может установить связь между изучаемым и ранее изученным материалом из курса «Компьютерные сети», а также с материалом, усвоенным при изучении других дисциплин.

Оценка «хорошо» ставится, если

— ответ студента удовлетворяет основным требованиям к ответу на оценку 5, но дан без использования собственного плана, новых примеров, без применения знаний в новой ситуации, без использования связей с ранее изученным материалом и материалом, усвоенным при изучении других дисциплин;

— студент допустил одну ошибку или не более двух недочетов и может их исправить самостоятельно или с небольшой помощью преподавателя.

Оценка «удовлетворительно» ставится, если студент

— правильно понимает суть вопроса, но в ответе имеются отдельные пробелы в усвоении вопросов курса «Компьютерные сети», не препятствующие дальнейшему усвоению программного материала;

— допустил не более одной грубой ошибки и двух недочетов.

Оценка «неудовлетворительно» ставится, если студент

— не овладел основными знаниями и умениями в соответствии с требованиями программы и допустил больше ошибок и недочетов, чем необходимо для оценки 3.

— не может ответить ни на один из поставленных вопросов.