ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«Иркутский государственный университет путей сообщения»
Сибирский колледж транспорта и строительства

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ПРАКТИЧЕСКИМ РАБОТАМ

ОП. 13 Технологии физического уровня передачи данных

общепрофессиональные дисциплины, профессиональный цикл
по специальности
09.02.06 Сетевое и системное администрирование
базовая подготовка среднего профессионального образования

Иркутск 2022

РАССМОТРЕНО:
Цикловой методической
комиссией специальности 09.02.06
Сетевое и системное
администрирование
«08» июня 2022 г.
Председатель: _____/Саквенко Т.В.

СОГЛАСОВАНО:
Заместитель директора по УВР
_____/А.П.Ресельс
«09» июня 2022 г.

Разработчик: Фитисова Н.Н., преподаватель высшей категории Сибирского колледжа транспорта и строительства ФГБОУ ВО «Иркутский государственный университет путей сообщения».

Практическая работа № 1
Исследование амплитудной и импульсной модуляции

Цели: Ознакомиться с видами модуляции сигналов

Модуляция — это процесс преобразования одного или нескольких информационных параметров несущего сигнала в соответствии с мгновенными значениями информационного сигнала.

В результате модуляции сигналы переносятся в область более высоких частот.

Использование модуляции позволяет:

- согласовать параметры сигнала с параметрами линии;
- повысить помехоустойчивость сигналов;
- увеличить дальность передачи сигналов;
- организовать многоканальные системы передачи (МСП с ЧРК).

Модуляция осуществляется в устройствах *модуляторах.* Условное графическое обозначение модулятора имеет вид:

М

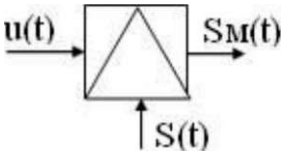


Рисунок 1 - Условное графическое обозначение модулятора

При модуляции на вход модулятора подаются сигналы:

u(t) — модулирующий, данный сигнал является информационным и низкочастотным (его частоту обозначают W или F);

S(t) — модулируемый (несущий), данный сигнал является неинформационным и высокочастотным (его частота обозначается w0 или f0);

Sм(t) — модулированный сигнал, данный сигнал является информационным и высокочастотным.

В качестве несущего сигнала может использоваться:

- гармоническое колебание, при этом модуляция называется *аналоговой* или *непрерывной',*
- периодическая последовательность импульсов, при этом модуляция называется *импульсной*;
- постоянный ток, при этом модуляция называется *шумоподобной.*

Так как в процессе модуляции изменяются информационные параметры несущего колебания, то название вида модуляции зависит от изменяемого параметра этого колебания.

1. Виды аналоговой модуляции:

амплитудная модуляция (АМ), происходит изменение амплитуды несущего колебания;

частотная модуляция (ЧМ), происходит изменение частоты несущего колебания;

фазовая модуляция (ФМ), происходит изменение фазы несущего колебания.

2. Виды импульсной модуляции:

- амплитудно-импульсная модуляция (АИМ), происходит изменение амплитуды импульсов несущего сигнала;
- частотно-импульсная модуляция (ЧИМ), происходит изменение частоты следования импульсов несущего сигнала;
- Фазо-импульсная модуляция (ФИМ), происходит изменение фазы импульсов несущего сигнала;
- Широтно-импульсная модуляция (ШИМ), происходит изменение длительности импульсов несущего сигнала.

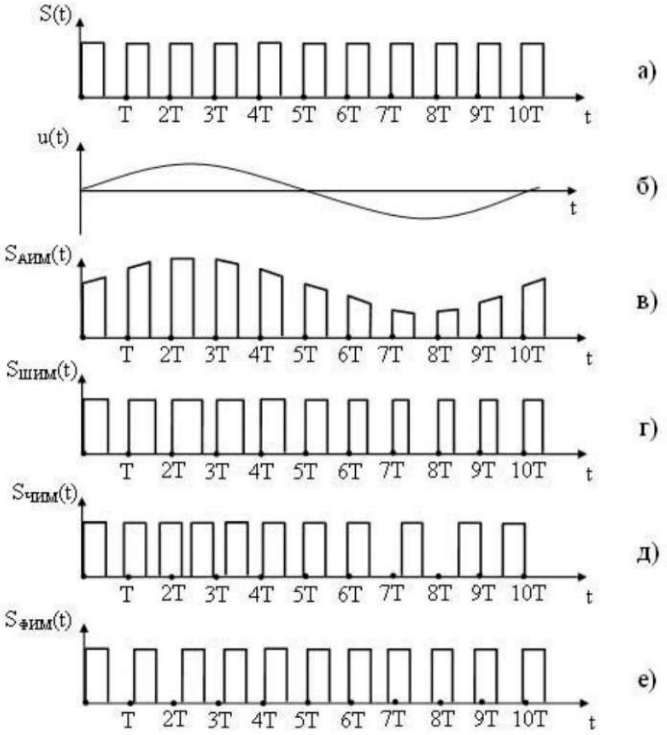
Импульсная модуляция

Импульсная модуляция — это модуляция, при которой в качестве несущего сигнала используется периодическая последовательность импульсов, а в качестве модулирующего может использоваться аналоговый или дискретный сигнал.

Поскольку периодическая последовательность характеризуется четырьмя информационными параметрами (амплитудой, частотой, фазой и длительностью импульса), то различают четыре основных вида импульсной модуляции:

- амплитудно-импульсная модуляция (АИМ); происходит изменение амплитуды импульсов несущего сигнала;
- частотно-импульсная модуляция (ЧИМ), происходит изменение частоты следования импульсов несущего сигнала;
- фазо-импульсная модуляция (ФИМ), происходит изменение фазы импульсов несущего сигнала;
- широтно-импульсная модуляция (ШИМ), происходит изменение длительности импульсов несущего сигнала.

Временные диаграммы импульсно-модулированных сигналов представлены на рисунке 2.



Амплитудная модуляция — процесс изменения амплитуды несущего сигнала в соответствии с мгновенными значениями модулирующего сигнала

Рисунок 3.

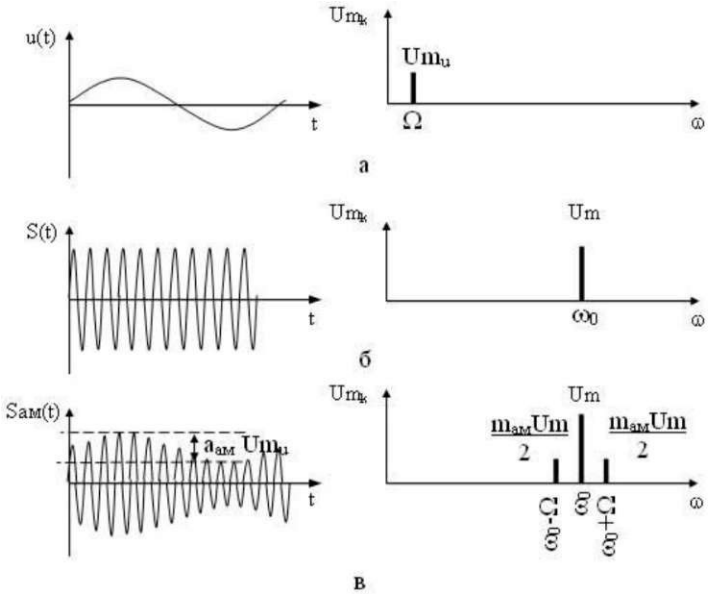


Рисунок 3 - Временные и спектральные диаграммы модулирующего (а), несущего
(б) и ампдтудно-модулированного (в) сигналов

Вопросы для контроля.

1. Дайте определение модуляции?
2. Какие сигналы могут использоваться как несущие?
3. Опишите амплитудную и импульсную модуляцию

Практическая работа № 2
Расчет пропускной способности проводных линий связи.

Цель: Научиться рассчитывать пропускную способность проводных линий связи.

Обмен информацией производится по каналам передачи информации.

Каналы передачи информации могут использовать различные физические принципы. Так, при непосредственном общении людей информация передаётся с помощью звуковых волн, а при разговоре по телефону — с помощью электрических сигналов, которые распространяются по линиям связи.

Канал связи — технические средства, позволяющие осуществлять передачу данных на расстоянии.

Компьютеры могут обмениваться информацией с использованием каналов связи различной физической природы: кабельных, оптоволоконных, радиоканалов и др.

Скорость передачи информации (скорость информационного потока) — количество информации, передаваемое за единицу времени.

Общая схема передачи информации включает в себя отправителя информации, канал передачи информации и получателя информации.

Основной характеристикой каналов передачи информации является их *пропускная способность.*

Пропускная способность канала — максимальная скорость передачи информации по каналу связи в единицу времени.

Пропускная способность канала равна количеству информации, которое может передаваться по нему в единицу времени.

Объем переданной информации V вычисляется по формуле:

$V=q\text{-}t$

где q — пропускная способность канала (в битах в секунду или подобных единицах), а t— время передачи.

Обычно пропускная способность измеряется в битах в секунду (бит/с) и кратных единицах Кбит/с и Мбит/с.

Однако иногда в качестве единицы используется байт в секунду (байт/с) и кратные ему единицы Кбайт/с и Мбайт/с.

Соотношения между единицами пропускной способности канала передачи информации такие же, как между единицами измерения количества информации:

л

1байт/с = 2 бит/с = 8 бит/с;

1 Кбит/с = 2^{10} бит/с = 1024 бит/с;

1 Мбит/с = 2^{10} Кбит/с = 1024 Кбит/с;

1 Гбит/с = 2^{10} Мбит/с = 1024 Мбит/с.

Задание 1:

Сколько секунд потребуется модему, передающему сообщения со скоростью 28800бит/с, чтобы передать 100 страниц текста в 30 строк по 60 символов каждая, при условии, что каждый символ кодируется 1 байтом?

Задание 2:

Устройство *A* передает информацию устройству *C* через устройство *B* в рамках следующих правил:

1. Информация передается пакетами по 200 байт.

2. Устройство *B* может одновременно принимать информацию от устройства *A* и передавать ранее полученную информацию устройству *C.*

3. Устройство *B* может передавать очередной пакет устройству *C* только после того, как полностью получит этот пакет от устройства *A.*

4. Устройство *B* обладает неограниченным по объему буфером, в котором может хранить полученные от устройства *A,* но еще не переданные устройству *C* пакеты.

Пропускная способность канала между *A* и *B* - 100 байт в секунду.

Пропускная способность канала между *B* и *C* - 50 байт в секунду.

Было отправлено три пакета информации. Через сколько секунд *C* закончит прием всей информации от А?

Вопросы для контроля.

1) Дайте определение пропускной способности канала?

2) Дайте определение скорости передачи информации?

Практическая работа № 3
Монтаж кабеля «витая пара»

Цель: Научиться проводить кроссировку кабеля «витая пара» и сетевой розетки

Оборудование и программное обеспечение:

1) Кабель «витая пара».
2) Обжимное устройство.
3) Сетевая розетка.
4) Коннекторы RJ-45.

Опрессовка прямого провода по стандарту Т568В

При монтаже локальных сетей сегодня наиболее распространена неэкранированная витая пара 5й категории (CAT-5E) . Рисунок 1.

Оборудование и программное обеспечение:

5) Кабель «витая пара».
6) Обжимное устройство.
7) Сетевая розетка.
8) Коннекторы RJ-45.

Опрессовка прямого провода по стандарту Т568В

При монтаже локальных сетей сегодня наиболее распространена неэкранированная витая пара 5й категории (CAT-5E) . Рисунок 1.

Рисунок 1 – Кабель категории 5Е.

Обжим такого кабеля для соединения ПК (PC)-ХАБ (HUB) по стандарту Т568В изображен на РисункеОбжим такого кабеля для соединения ПК (PC)-ХАБ (HUB) по стандарту Т568В изображен на Рисунке2

Рисунок 2 - Прямой обжим для соединения ПК-ХАБ (Одинаковый цвет проводников с обеих сторон кабеля)

Примечание

Обжим (опрессовка) по варианту Т568А - стандарт, имеющий хождение в США и Канаде, а в России, в основном, применяется стандарт Т568В.

Для обжима (опрессовки) витой пары вам потребуются пара коннекторов Ю-45и специальные клещи (кримпер) - Рисунок 3, 4

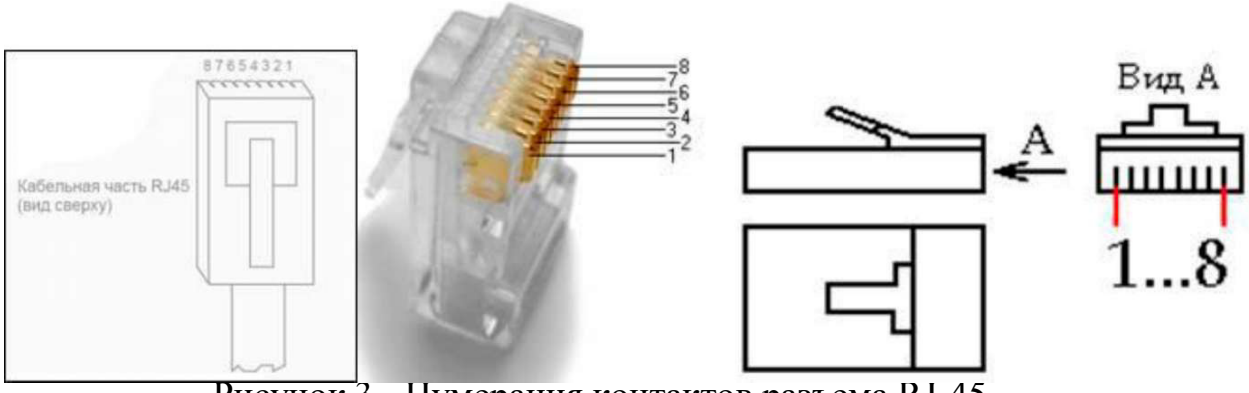


Рисунок 3 - Нумерация контактов разъема RJ-45

Рисунок 4 - Кримпер

Последовательность действий при обжиме:

- Аккуратно обрежьте конец кабеля резаком, встроенным в обжимной инструмент.
- Снимите с кабеля изоляцию ножом, встроенным в обжимной инструмент.
- Разведите и расплетите проводки, выровняйте их в один ряд. Обкусите проводки так, чтобы их осталось чуть больше сантиметра (см. примечание).
- Вставьте проводники в коннектор RJ-45. Убедитесь, все ли провода полностью вошли в разъем и уперлись в его переднюю стенку.
- Вставьте коннектор в устройство для обжима коннектора.
- Надавите на клещи так, чтобы контакты коннектора зажали проводники внутри него.

Примечание

На Рисунке 5 показан неправильный обжим витой пары. На примере слева оставлены слишком длинные жилы, из-за чего расстояние от коннектора до оплетки остается незащищенным. Также кабель теряет прочность. На втором примере жилы срезаны слишком коротко, оплетка входит в коннектор и длина концов проводников не позволяет создать их полноценный контакт с коннектором.

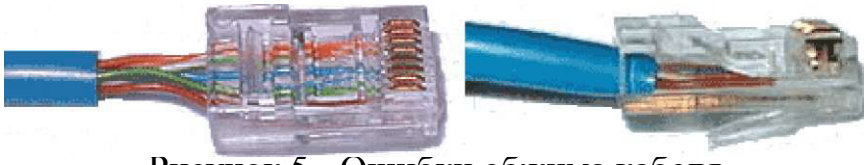


Рисунок 5 - Ошибки обжима кабеля

Контроль результата

Для проверки правильности обжима соедините кабелем сетевую карту и HUB (коммутатор, свич) и убедитесь в правильной работе такого кабеля. Другой вариант - использовать специальный тестер со светодиодной индикацией.

Все контакты в розетках категории 5 пронумерованы, поэтому никаких проблем с разводкой кабеля возникнуть не должно.

В продаже представлено множество тестеров для проверки витых пар RJ-45 разного уровня сложности и ценового диапазона. Однако, принцип работы их аналогичен. Так, например, кабельный тестер FA-7012B состоит из 2

функциональных блоков - передатчика и приемника, которые подключаются к концам кабельной линии через разъемы RJ-45 или RJ-12. Он позволяет обнаружить оборванные пары, закороченные пары, перепутанные провода в одной паре, перепутанные пары и перепутанные провода между разными парами. Также прибор позволяет проверить целостность экрана кабеля. Блок-передатчик последовательно опрашивает состояние каждого провода в кабеле, а блок- приёмник возвращает ответ по неиспользуемой в конкретный момент паре. Последовательное загорание светодиодов сигнализирует о правильном соединении. Устройство питается от 1 батареи типа "Крона" 9 В.

Обжим розетки категории 5 под разъем RJ45.

Стандартная схема подключения ПК к локальной или глобальной сети приведена на Рисунке .

Ситуация 1. Розетка с одним гнездом на 8 проводов

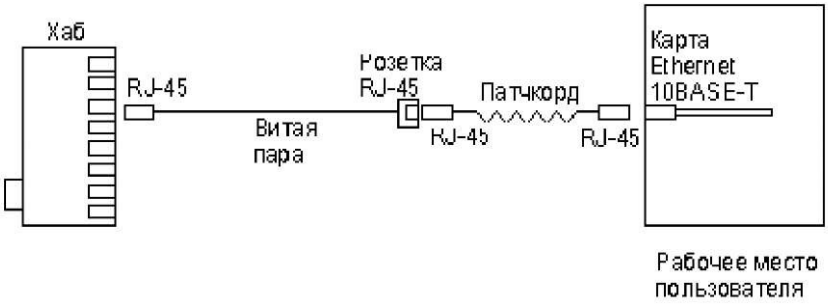


Рисунок 7 - Обычная схема подключения домашнего или офисного ПК к сети Так же, как и сам кабель, витая пара, сетевые розетки различаются по категориям. В идеале, для профессионального монтажа вам понадобятся: розетка RJ-45 категории 5е для настенного монтажа, устройство для зачистки и обрезки витой пары, устройство для заделки витой пары, 4-парный кабель UTP, категория 5е и маркеры для нанесения обозначений на кабель Рисунок 8.

Рисунок 8 - Набор для монтажа розетки (слева инструмент для снятия изоляц сверху - для обрезки концов проводников)

Для работы потребуется отвертка с плоским тонким жалом, по толщине, не превышающей диаметр медного проводника витой пары - Рисунок 9. Также заталкивать провода в щели розетки можно ножом с тонким лезвием, например, канцелярским ножом, у которого лезвие выдвигается.

Рисунок 9 - Нумерация контактов в розетке с одним гнездом по стандарту Т568В (для стандарта Т568А

Подготавливается для разделки кабель, снимается на длину не более 3 см его внешняя оболочка. Расплетаются пары на длину не более 13-15 мм. Далее, по схеме цветов, проводники по очереди заводятся в гребенку, заправляются боковой плоскостью лезвия отвертки и затем торцом лезвия заталкиваются до упора. В особых случаях (при необходимости) в одно гнездо можно вставить два кабеля витой пары, смонтированных на одну вилку Рисунок 10.

Рисунок 10 - Особый вариант обжима кабеля

Скорость информации при таком монтаже будет не 100, а 10 Мбит/сек.

Ситуация 2. Розетка на 2 гнезда по 8 проводов

Для надежной фиксации проводников в контактах розетки существует специальный инструмент, позволяющий поместить провод на максимальную глубину, хотя, можно обойтись обыкновенным пинцетом и отверткой. Провода перед вбиванием в клеммы зачищать не надо - щели оснащены специальной режущей кромкой, которая сама прекрасно снимает с них изоляцию. Заведите кабель на модуль розетки. Подготавливается для разделки кабель, снимается на длину не более 3 см его внешняя оболочка. Расплетаются пары на длину не более 13-15 мм. Закрепите кабель стяжкой на печатной плате розетки. Обрежьте конец стяжки с помощью кусачек или ножниц. На самой розетке всегда есть схема, какой цвет кабеля, в какой контакт должен приходить. На печатной плате наклеена табличка, на которой прорисованы в цветах варианты Т568В и Т568А разделки проводников витой пары в гребенки - Рисунок 11.

Рисунок 11 - Цветовая маркировка проводов розетки стандарта Т568В это: 1 бело-ор, 2 ор, 3 бело-зел, 4 син, 5 бело-син 6 зел 7 бело кор, 8 кор

После выбора места установки розетки нужно ее закрепить на стене с помощью двух шурупов или приклеить двусторонним скотчем (обычно прилагаются в комплекте с розеткой). Для крепления шурупами нужно снять крышку и печатную плату, чтобы добраться до крепежных отверстий в основании розетки. Чтобы снять крышку, нужно двумя пальцами сдавить ее с боков в месте, близком к основанию и потянуть на себя. Защелки выйдут из зацепления, и крышка легко отойдет в сторону. Далее снимается печатная плата отведением в стороны четырех защелок по углам.

Вопросы для контроля.

1) Охарактеризуйте кабель «Витая пара».

2) Опишите шаги для обжима кабеля «витая пара» и кроссирования сетевой розетки.

Практическая работа № 4
Топология компьютерных сетей

Цель: Изучить виды топологий компьютерных сетей.

Теоретические основы.

Под топологией(компоновкой, конфигурацией, структурой) 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. В глобальных сетях структура связей обычно спрятана от пользователей не слишком важная, потому что каждый сеанс связи может выполняться по своему собственному пути. 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. Топологиятипаши́на, представляет собой общий кабель (называемый шина или магистраль), к которому подсоединены всерабочие станции. На концах кабеля находятсятерминаторы, для предотвращения отражения сигнала. (рис. 1);

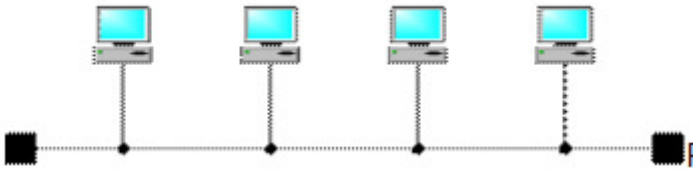


Рис. 1. Сетевая топология «шина»

Отправляемое рабочей станцией сообщение распространяется на все компьютерысети. Каждая машина проверяет — кому адресовано сообщение и если ей, то обрабатывает его. Для того, чтобы исключить одновременную посылку данных, применяется либо «несущий» сигнал, либо один из компьютеров является главным и «даёт слово» остальным станциям.

Шина самой своей структурой допускает идентичность сетевого оборудованиякомпьютеров, а также равноправие всех абонентов. При таком соединении компьютеры могут передавать только по очереди, потому что линия связи единственная. В противном случае переданная информация будет искажаться в результате наложения (конфликту, коллизии). Таким образом, в шине реализуется режим полудуплексного (half duplex) обмена (в обоих направлениях, но по очереди, а не одновременно).

В топологии «шина» отсутствует центральный абонент, через которого передается вся информация, которая увеличивает ее надежность (ведь при отказе любого центра перестает функционировать вся управляемая этим центром система). Добавление новых абонентов в шину достаточно простое и обычно возможно даже во время работы сети. В большинстве случаев при использовании шины нужно минимальное количество соединительного кабеля по сравнению с другой топологией. Правда, нужно учесть, что к каждому компьютеру (кроме двух крайних) подходит два кабеля, что не всегда удобно.

Шине не страшны отказы отдельных компьютеров, потому что все другие компьютеры сети могут нормально продолжать обмен. Может показаться, что шине не страшен и обрыв кабеля, поскольку в этом случае остаются две полностью работоспособных шины. Однако из-за особенности распространения электрических сигналов по длинным линиям связи необходимо предусматривать включение на концах шины специальных устройств – терминаторов.

Без включения терминаторов сигнал отражается от конца линии и искажается так, что связь по сети становится невозможной. Так что при разрыве или повреждении кабеля нарушается согласование линии связи, и прекращается обмен даже между теми компьютерами, которые остались соединенными между собой. Короткое замыкание в любой точке кабеля шины выводит из строя всю сеть. Любой отказ сетевого оборудования в шине очень трудно локализовать, потому что все адаптеры включены параллельно, и понять, который из них вышел из строя, не так-то просто.

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.

Сегмент компьютерной сети, использующей коаксиальный кабель в качестве носителя и подключенных к этому кабелю рабочих станций. В этом случае шиной будет являться отрезок коаксиального кабеля, к которому подключены компьютеры. Пример сеть Ethernet.

2. Звезда́— базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу (обычно сетевой концентратор), образуя физический сегмент сети. Подобный сегмент сети может функционировать как отдельно, так и в составе сложной сетевой топологии(как правило "дерево"). Весь обмен информацией идет исключительно через центральный компьютер, на который таким способом ложится очень большая нагрузка, потому ничем другим, кроме сети, оно заниматься не может. Как правило, именно центральный компьютер является самым мощным, и именно на него возлагаются все функции по управлению обменом. Никакие конфликты в сети с топологией звезда в принципе невозможные, потому что управление полностью централизовано. (рис. 2);

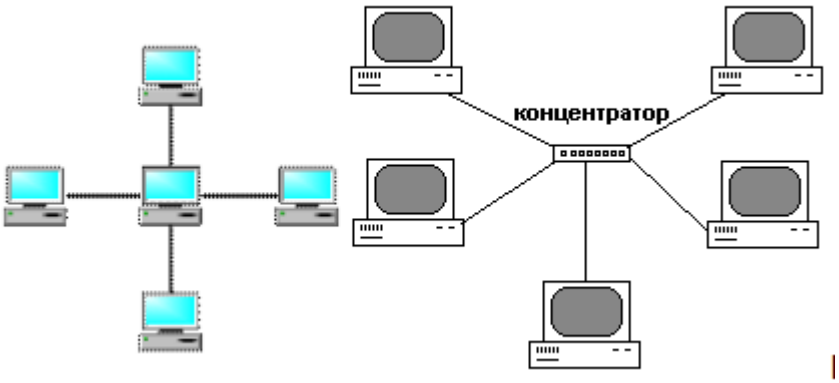


Рис. 2. Сетевая топология «звезда»

Активная звезда - В центре сети содержится компьютер, который выступает в роли сервера.

Пассивная звезда -В центре сети с данной топологией содержится не компьютер, а концентратор, или хаб(hub), что выполняет ту же функцию, что и репитер. Он возобновляет сигналы, которые поступают, и пересылает их в другие линии связи

Достоинства

- выход из строя одной рабочей станции не отражается на работе всей сети в целом;
- хорошая масштабируемостьсети;
- лёгкий поиск неисправностей и обрывов в сети;
- высокая производительность сети (при условии правильного проектирования);
- 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.

Одна из наиболее распространённых топологий, поскольку проста в обслуживании. В основном используется в сетях, где носителем выступает кабель витая пара. UTP категория 3 или 5. Пример сеть Fast Ethernet.

3. Кольцó — 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.» (рис. 3).

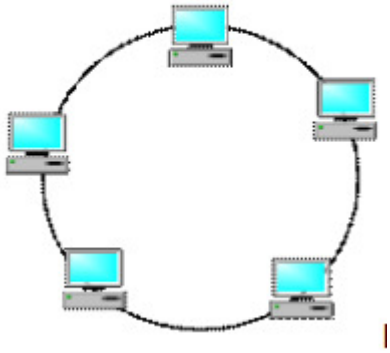


Рис. 3. Сетевая топология «кольцо»

Важна особенность кольца заключается в том, что каждый компьютер ретранслирует (возобновляет) сигнал, то есть выступает в роли репитера, потому затухание сигнала во всем кольце не имеет никакого значения, важно только затухание между соседними компьютерами кольца. Четко выделенного центра в этом случае нет, все компьютеры могут быть одинаковыми. Однако достаточно часто в кольце выделяется специальный абонент, который управляет обменом или контролирует обмен. Понятно, что наличие такого управляющего абонента снижает надежность сети, потому что выход его из строя сразу же парализует весь обмен.

Компьютеры в кольце не являются полностью равноправными (в отличие, например, от шинной топологии). Одни из них обязательно получают информацию от компьютера, который ведет передачу в этот момент, раньше, а другие – позже. Именно на этой особенности топологии и строятся методы управления обменом по сети, специально рассчитанные на «кольцо». В этих методах право на следующую передачу (или, как еще говорят, на захвата сети) переходит последовательно к следующему по кругу компьютеру.

Подключение новых абонентов в «кольцо» обычно совсем безболезненно, хотя и требует обязательной остановки работы всей сети на время подключения. Как и в случае топологии «шина», максимальное количество абонентов в кильке может быть достаточно большая (до тысячи и больше). Кольцевая топология обычно является самой стойкой к перегрузкам, она обеспечивает уверенную работу с самими большими потоками переданной по сети информации, потому что в ней, как правило, нет конфликтов (в отличие от шины), а также отсутствует центральный абонент (в отличие от звезды).

В кольце, в отличие от других топологий (звезда, шина), не используется конкурентный метод посылки данных, компьютеров сети получает данные от стоящего предыдущим в списке адресатов и перенаправляет их далее, если они адресованы не ему. Список адресатов генерируется компьютером, являющимся генератором маркера. Сетевой модуль генерирует маркерный сигнал (обычно порядка 2-10 байт во избежание затухания) и передает его следующей системе (иногда по возрастанию MAC-адреса). Следующая система, приняв сигнал, не анализирует его, а просто передает дальше. Это так называемый нулевой цикл.

Для устранения недостатков используется топология двойное кольцо. Двойное кольцо– эта сеть построенная на двухоптоволоконных кольцах, соединяющих компьютеры с двумя сетевыми картами кольцевой топологией. Для повышения отказоустойчивости, сеть строится на оптоволоконных кольцах образующих основной и резервный путь для передачи данных. Первое кольцо используется для передачи данных, а второе не используется. При выходе из строя 1-го кольца оно объединяется со 2-м и сеть продолжает функционировать. Данные при этом по первому кольцу передаются в одном направлении, а по второму в обратном.

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.

Наиболее широкое применение получила в оптоволоконных сетях. Используется в стандартах FDDI, Token ring.

Полносвязная топология соответствует сети, в которой каждый компьютер сети связан со всеми остальными. Несмотря на логическую простоту, этот вариант оказывается громоздким и неэффективным. Действительно, каждый компьютер в сети должен иметь большое количество коммуникационных портов, достаточное для связи с каждым из остальных компьютеров сети. Для каждой пары компьютеров должна быть выделена отдельная электрическая линия связи. Полносвязные топологии применяются редко. Чаще этот вид топологии используется в многомашинных комплексах или глобальных сетях при небольшом количестве компьютеров или маршрутизаторов (рис. 4)

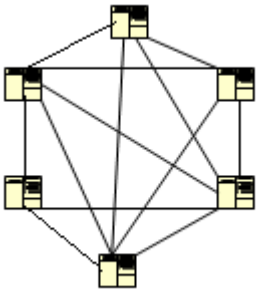


Рис 4.

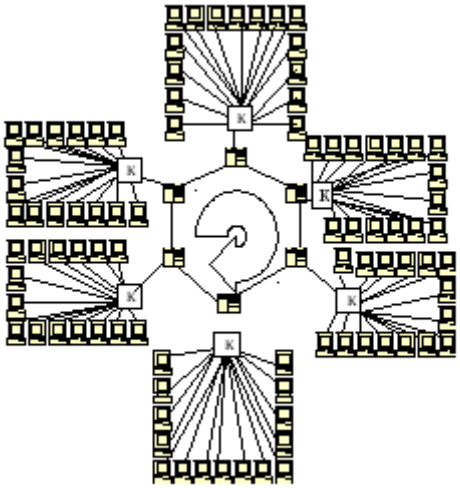
На практике нередко используют и комбинации базовой топологии, но большинство сетей ориентированные именно на этих три. Рассмотрим теперь коротко особенности перечисленной сетевой топологии.

Практическая часть

Задание

1. Создать схему соединения компьютерной сети согласно своему заданию.
2. Описать построенную топологию.
3. Ответить на вопросы
4. Вывод.

Пример Сервер 6 кольцо, ПК 15 звезда.



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
26	8	5	Звезда	Полносвязная
27	5	7	Общая шина	Кольцо
28	8	4	Общая шина	Полносвязная
29	5	7	Полносвязная	Кольцо

30	3	8	Кольцо	Общая шина

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

Практическая работа № 5
Коммутация, маршрутизация

Цель: Изучить маршрутизацию и коммутацию.

Коммутация является необходимым элементом связи узлов между собой, что позволяет сократить количество необходимых линий связи и повысить загрузку каналов связи. Практически невозможно предоставить каждой паре узлов выделенную линию связи, потому в сетях всегда применяется тот или другой **способ коммутации абонентов,** которая использует существующие линии связи для передачи данных разных узлов.

Способы коммутации сетей, называются сети, в которых связь между узлами устанавливается только по запросу. Абоненты соединяются с коммутаторами выделенными (индивидуальными) линиями связи. Линии связи, которые соединяют коммутаторы, используются абонентами совместно.

Коммутация может осуществляться в двух режимах: динамически и статически. В первом случае коммутация выполняется на время сеанса связи (обычно от секунд до часов) по инициативе одного из узлов, а по окончании сеанса связь разрывается. Во втором случае коммутация выполняется обслуживающим персоналом сети на значительно больше длительный период времени (несколько месяцев или лет) и не может быть изменена по инициативе пользователей. Такие каналы называются **выделенными** (*dedicated)* или **арендованными** *(leased).*

Две группы способов коммутации: коммутация каналов ***(circuitswitching)*** **и** коммутация с промежуточным хранением ***(store-and-forward).*** **Вторая группа состоит из двух способов:** коммутации сообщений ***(messageswitching)*** **и** коммутации пакетов **(*packetswitching).***

При **коммутации каналов** между узлами, которым необходимо установить связь друг с другом, обеспечивается организация непрерывного составленного канала, который состоит из последовательно соединенных отдельных каналов между узлами. Отдельные каналы соединяются между собой коммутирующим оборудованием (коммутаторами). Перед передачей данных необходимо выполнить процедуру установления соединения, в процессе которой создается составленный канал.

Под **коммутацией сообщений** понимается передача единого блока данных между узлами сети из временный буферизациею этого блока каждым из транзитных узлов. Сообщениям может быть текстовый файл, файл с графическим изображением, электронное письмо - сообщение имеет произвольный размер, обусловленный исключительно его содержанием, а не теми или другими технологическими рассуждениями.

При **коммутации пакетов** все переданы пользователем данные разбиваются передаточным узлом на небольшие (до нескольких килобайт) части - **пакеты** (packet). Каждый пакет оснащается заглавием, в котором указывается, как минимум, адрес узла- получателя и номер пакета. Передача пакетов по сети происходит независимо один от одного. Коммутаторы такой сети имеют внутреннюю буферную память для временного хранения пакетов, что позволяет сглаживать пульсации трафша на линиях связи между коммутаторами. Пакеты иногда называют **дейтаграмами** *(datagram),* а режим индивидуальной коммутации пакетов - **дейтаграмним** режимом.

Сеть с коммутацией пакетов замедляет процесс взаимодействия каждой конкретной пары узлов, поскольку их пакеты могут ожидать в коммутаторах, пока передадутся другие пакеты. Однако общая эффективность (объем переданных данных в единицу времени) при коммутации пакетов будет выше, чем при коммутации каналов. Это связано с тем, что траффик каждого отдельного абонента носит пульсирующий характер, а пульсации разных абонентов, в соответствии с законом больших чисел, распределяются во времени, увеличивая равномерность нагрузки на сеть.

Маршрутизатором, или **шлюзом,** называется узел сети с несколькими IP- интерфейсами (содержащими свой MAC-адрес и IP-адрес), подключенными к разным IP- сетям, осуществляющий на основе решения задачи маршрутизации перенаправление дейтаграмм из одной сети в другую для доставки от отправителя к получателю.

Маршрутизаторы представляют собой либо специализированные вычислительные машины, либо компьютеры с несколькими IP-интерфейсами, работа которых управляется специальным программным обеспечением.

Маршрутизация служит для приема пакета от одного устройства и передачи его по сети другому устройству через другие сети. Если в сети нет маршрутизаторов, то не поддерживается маршрутизация. Маршрутизаторы направляют (перенаправляют) трафик во все сети, составляющие объединенную сеть.

Для маршрутизации пакета маршрутизатор должен владеть следующей информацией:

- Адрес назначения
- Соседний маршрутизатор, от которого он может узнать об удаленных сетях
- Доступные пути ко всем удаленным сетям
- Наилучший путь к каждой удаленной сети
- Методы обслуживания и проверки информации о маршрутизации

Маршрутизатор узнает об удаленных сетях от соседних маршрутизаторов или от

сетевого администратора. Затем маршрутизатор строит таблицу маршрутизации, которая описывает, как найти удаленные сети.

Если сеть подключена непосредственно к маршрутизатору, он уже знает, как направить пакет в эту сеть. Если же сеть не подключена напрямую, маршрутизатор должен узнать (изучить) пути доступа к удаленной сети с помощью статической маршрутизации (ввод администратором вручную местоположения всех сетей в таблицу маршрутизации) или с помощью динамической маршрутизации.

Динамическая маршрутизация — это процесс протокола маршрутизации, определяющий взаимодействие устройства с соседними маршрутизаторами. Маршрутизатор будет обновлять сведения о каждой изученной им сети. Если в сети произойдет изменение, протокол динамической маршрутизации автоматически информирует об изменении все маршрутизаторы. Если же используется статическая маршрутизация, обновить таблицы маршрутизации на всех устройствах придется системному администратору.

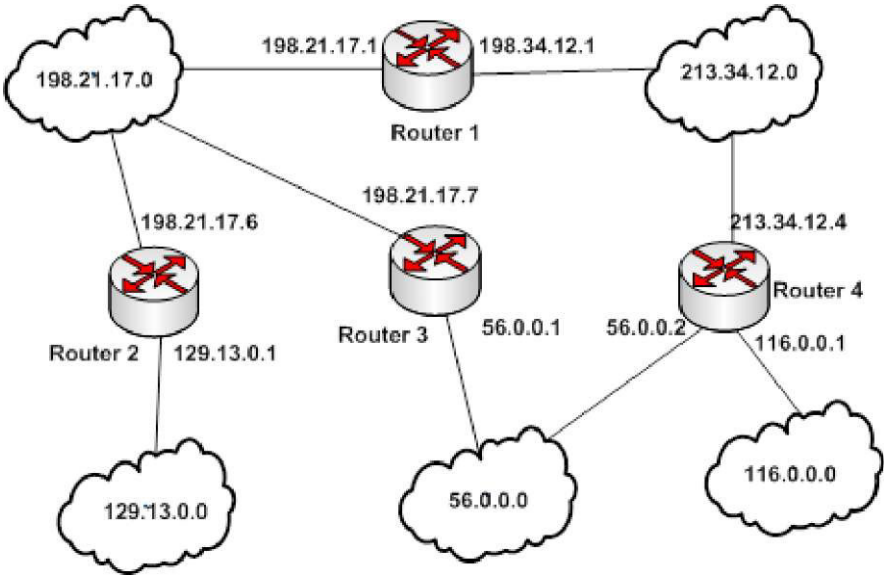
Таблицы маршрутизации

В стеке TCP/IP маршрутизаторы и конечные узлы принимают решения о том, кому передавать пакет для его успешной доставки узлу назначения, на основании так называемых таблиц маршрутизации (routing tables).

Таблица представляет собой типичный пример таблицы маршрутов, использующей IP-адреса сетей, для сети, представленной на рисунке.

Таблица маршрутизации для Router 2.

Сетевой адрес	Маска сети	Адрес шлюза	интерфейс	Метрика
129.13.0.0	255.255.0.0	-	129.13.0.1	подключен
19821.17.0	255.25 5.255.0	■	193.21.17.6	подключен
213.34,12.0	255,255-255 0	198.21.17.1	198.21.17.6	1
56.0.0.0	255.0.0.0	198.21.17.7	193.21.17.6	1
116.0-0-0	255-00 0	196.21,17.7	198.21.17.6	2
116.0.0.0	255.0.0.0	198.21.17.1	198.21.17.6	2
0.0.0.0	0.0.0.0	193.21.17.7	193.21.17.6	-



В таблице представлена таблица маршрутизации многомаршрутная, так как содержится два маршрута до сети 116.0.0.0. В случае построения

одномаршрутной таблицы маршрутизации, необходимо указывать только один путь до сети 116.0.0.0 по наименьшему значению метрики.

Как нетрудно видеть, в таблице определено несколько маршрутов с разными параметрами. Читать каждую такую запись в таблице маршрутизации нужно следующим образом:

Чтобы доставить пакет в сеть с адресом из поля Сетевой адрес и маской из поля Маска сети, нужно с интерфейса с IP-адресом из поля Интерфейс послать пакет по IP- адресу из поля Адрес шлюза, а «стоимость» такой доставки будет равна числу из поля Метрика.

В этой таблице в столбце "Адрес сети назначения" указываются адреса всех сетей, которым данный маршрутизатор может передавать пакеты. В стеке TCP/IP принят так называемый одношаговый подход к оптимизации маршрута продвижения пакета (next- hop routing) - каждый маршрутизатор и конечный узел принимает участие в выборе только одного шага передачи пакета. Поэтому в каждой строке таблицы маршрутизации указывается не весь маршрут в виде последовательности IP-адресов маршрутизаторов, через которые должен пройти пакет, а только один IP-адрес - адрес следующего маршрутизатора, которому нужно передать пакет. Вместе с пакетом следующему маршрутизатору передается ответственность за выбор следующего шага маршрутизации. Одношаговый подход к маршрутизации означает распределенное решение задачи выбора маршрута. Это снимает ограничение на максимальное количество транзитных маршрутизаторов на пути пакета.

Для отправки пакета следующему маршрутизатору требуется знание его локального адреса, но в стеке TCP/IP в таблицах маршрутизации принято использование только IP-адресов для сохранения их универсального формата, не зависящего от типа сетей, входящих в интерсеть. Для нахождения локального адреса по известному IP- адресу необходимо воспользоваться протоколом ARP.

Вопросы для контроля.

1) Чем маршрутизация отличается от коммутации?

2) Выведите и вставьте в отчет таблицу маршрутизации на вашем ПК.

3)В каких случаях в сети необходимо использовать маршрутизатор?

Практическая работа № 6
Изучение настроек Ethernet и способов анализа трафика на сетевых интерфейсах в ОС Windows

Цель: Ознакомиться с настройками сетевой платы и встроенными инструментальными средствами ОС MS Windows анализа трафика на сетевых интерфейсах.

2. Теоретические сведения

Правильная настройка сетевой платы позволяет не только обеспечить соединение с сеть, но улучшить производительность сетевого подключения и получить необходимое качество сервиса предоставляемой локальной сетью.

Для просмотра состояния взаимодействия компьютера с локальной сетью различные разработчики операционных систем представляют средства диагностик.

Средства диагностики могут быть графическими или использовать командную строку (так называемый CLI — Command lininterface). Диагностика с помощью CLI позволяет создавать скрипты или программы для включения их в приложения занимающиеся мониторингом или анализом сети в целом.

В данной работе необходимы следующие понятия:

- **Скрипт (script)** — небольшая программа для выполнения средствами операционной системы и для расширения ее возможностей
- **Loopback** (обратная, возвратная петля) Тип диагностического интерфейса, при котором сигнал возвращается передающему устройству, пройдя по коммуникационному каналу в обоих направлениях.
- **GUI** — (Graphical User Interface) графический пользовательский интерфейс
- **CLI** — (Command Line Interface) Интерфейс командной строки, в котором инструкции компьютеру даются только путём ввода с клавиатуры текстовых строк (команд). Также известен под названием консоль.
- **MMC** (Microsoft Management Console) -средство для создания, сохранения и открытия средств администрирования (называемых консолями MMC), которые управляют оборудованием, программными и сетевыми компонентами операционной системы Windows.

3. Порядок выполнения работы

Для выполнения лабораторной работы достаточно одного компьютера без подключения к какой-либо сети.

3.1. Описание свойств сетевой платы.

Выполнить в следующей последовательности доступ к настройкам сетевой платы:

Пуск — панель управления — подключение к локальной сети (сетевые подключения) – вызов контекстного меню- свойства- настроить.

Сохранить в отчет все свойства сетевой интерфейса виде таблицы 1:
<Название сетевой платы>

Свойство	Установленное значение	Возможные значение
Скорость и дуплекс	Автосогласование	От 10Мбит/с дуплекс…до 100Мбит/с полудуплекс
Wake Up Capabilities Magic packet	None,	Wake Up Frame, Both,

3.2. Изучить возможность консоли управления ММС по встроенной справке (Консоль — действия – справка). Кратко отразить полученные сведения в отчете.

3.3. Настройка консоли ОС MS Windows для анализа трафика сетевого интерфейса.

Панель управления – Администрирование – Производительность — контекстное меню – добавить счетчики — объект — сетевой интерфейс — добавить счетчики: «отправлено байт/сек», «получено байт/сек». В свойствах графика указать диапазон вертикальной шкалы =5. Вывести заголовок над динамическим графиком- «Сетевой трафик».

3.4. В окне командного процессора выполнить команду:
ping -l 10000 127.0.0.1 -t (Выход – ctrl+c)

В течении ~1 минуты снять статистику, проанализировать, сделать вывод. В отчет вставить формат отклика.

3.5. В окне командного процессора выполнить команду:
ping -l 65500 127.0.0.1 -t
В течении ~1 минуты снять статистику, проанализировать сделать вывод. В отчет вставить формат отклика.

Данные процедуры позволяют рассмотреть скорее качественное состояние статистики интерфейса, чем количественное.

Это связано с тем, что ping отправляет 1 пакет/сек, а статистика собирается за секунду. Т.о статистика отображает среднюю за секунду величину, а не текущую.

3.6. Определение размера ICMP-пакетов.

Подобрать значение длины пакетов, чтобы не было сообщений ошибках пакетов. Для этого в текстовом редакторе создать командный файл proba.bat следующего содержания:

```
@echo off
for /L %%i in (1000#,100#,100000#) do (
for /F «usebackq delims=< tokens=2» %%a IN (
`ping -l %%i 127.0.0.1 -n 1`) DO @echo Размербуфера
отправки=%%i……Время отклика=%%a)
```

В отчете дать объяснения остановки команды ping и при какой величине.

Подобрать значение длины пакетов, чтобы не было сообщений ошибках при фрагментации пакетов.

В текстовом редакторе создать командный файл proba_2.bat следующего содержания:

```
@echo off
for /L %%i in (1000#,1#,10000#) do (
for /F «skip=2 usebackq delims=< tokens=2» %%a IN (
`ping -f -l %%i 127.0.0.1 -n 1`) DO @echo Размербуфера
отправки=%%i……Время отклика=%%a)
```

В отчете дать объяснения остановки команды ping и при какой величине.

3.7. Просмотр статистики Ethernet интерфейса и протоколов IP стека.

Работа и оформление отчета в виде таблицы 2 :

Описание действий	Команды
Просмотреть MAC-адреса Ethernet	getmac
С помощью утилит собрать статистику Ethernet интерфейса и протоколов стека IP	netstat
Ознакомление с командами	netstat –s –p ICMP l
	netstat –s –p UDP l
	netstat –s –p TCP l

В отчете описать имеющуюся статистику.

Практическая работа № 7
Модель OSI. Канальный уровень

Цель: Изучить действие сетевых анализаторов

В качестве примера исследования некоторого протокола с использованием сниффера рассмотрим протокол ARP.

Протокол ARP

ARP (англ. Address Resolution Protocol — протокол разрешения адресов) — сетевой протокол, предназначенный для преобразования IP-адресов (адресов сетевого уровня) в MAC-адреса (адреса канального уровня) в сетях TCP/IP. Он определён в RFC 826.

Данный протокол очень распространенный и чрезвычайно важный. Каждый узел сети имеет как минимум два адреса, физический адрес и логический адрес. В сети Ethernet для идентификации источника и получателя информации используются оба адреса. Информация, пересылаемая от одного компьютера другому по сети, содержит в себе физический адрес отправителя, IP-адрес отправителя, физический адрес получателя и IP-адрес получателя. ARP-протокол обеспечивает связь между этими двумя адресами. Существует четыре типа ARP-сообщений: ARP-запрос (ARP request), ARP-ответ (ARP reply), RARP-запрос (RARP-request) и RARP-ответ (RARP-reply). Локальный хост при помощи ARP-запроса запрашивает физический адрес хоста-получателя. Ответ (физический адрес хоста-получателя) приходит в виде ARP-ответа. Хост-получатель, вместе с ответом, шлет также RARP-запрос, адресованный отправителю, для того, чтобы проверить его IP адрес. После проверки IP адреса отправителя, начинается передача пакетов данных.

Перед тем, как создать подключение к какому-либо устройству в сети, IP-протокол проверяет свой ARP-кеш, чтобы выяснить, не зарегистрирована ли в нём уже нужная для подключения информация о хосте-получателе. Если такой записи в ARP-кеше нет, то выполняется широковещательный ARP-запрос. Этот запрос для устройств в сети имеет следующий смысл: «Кто-нибудь знает физический адрес устройства, обладающего следующим IP-адресом?» Когда получатель примет этот пакет, то должен будет ответить: «Да, это мой IP-адрес.

Мой физический адрес следующий: ...» После этого отправитель обновит свой ARP-кеш, и будет способен передать информацию получателю.

RARP (англ. Reverse Address Resolution Protocol - обратный протокол преобразования адресов) - выполняет обратное отображение адресов, то есть преобразует аппаратный адрес в IP-адрес.

Протокол применяется во время загрузки узла (например компьютера), когда он посылает групповое сообщение-запрос со своим физическим адресом. Сервер принимает это сообщение и просматривает свои таблицы (либо перенаправляет запрос куда-либо ещё) в поисках соответствующего физическому IP-адреса. После обнаружения найденный адрес отсылается обратно на запросивший его узел. Другие станции также могут «слышать» этот диалог и локально сохранить эту информацию в своих ARP- таблицах.

RARP позволяет разделять IP-адреса между не часто используемыми хост-узлами. После использования каким либо узлом IP-адреса он может быть освобождён и выдан другому узлу. RARP является дополнением к ARP, и описан в RFC 903.

Для просмотра ARP-кеша можно использовать одноименную утилиту arp с параметром «-a». Например: D:\>arp -a

Interface: 192.168.1.2 --- 0x10003 Internet Address Physical Address Type 192.168.1.1 00-15-e9-b6-67-4f dynamic 192.168.1.6 00-01-4e-00-21-11 dynamic Из данного результата команды arp видно, что в кеше на данный момент находится 2 записи и видны соответственно ip-адреса машин и MAC-адреса их сетевых адаптеров.

Записи в ARP-кеше могут быть статическими и динамическими. Пример, данный выше, описывает динамическую запись кеша. Хост-отправитель автоматически послал запрос получателю, не уведомляя при этом пользователя. Записи в ARP-кеш можно добавлять вручную, создавая статические (static) записи кеша. Это можно сделать при помощи команды:

arp -s <IP адрес> <MAC адрес>

Также можно удалять записи из ARP-кеша. Это осуществляется путем следующего вызова:

arp -d <IP адрес>

После того, как IP-адрес прошёл процедуру разрешения адреса, он остается в кеше в течение 2-х минут. Если в течение этих двух минут произошла повторная передача данных по этому адресу, то время хранения записи в кеше продлевается ещё на 2 минуты. Эта процедура может повторяться до тех пор, пока запись в кеше просуществует до 10 минут. После этого запись будет удалена из кеша и будет отправлен повторный ARP-запрос.

ARP изначально был разработан не только для IP протокола, но в настоящее время в основном используется для сопоставления IP- и MAC-адресов.

Посмотрим же на практике как работает протокол ARP/RARP. Для этого воспользуемся сниффером для захвата сетевого трафика.

Рассмотрим пример работы протокола ARP при обращении к машине с адресом 192.168.1.5, выполнив запрос с машины с адресом 192.168.1.2. Для успешного эксперимента предварительно очистим arp-кеш командой arp -d 192.168.1.5

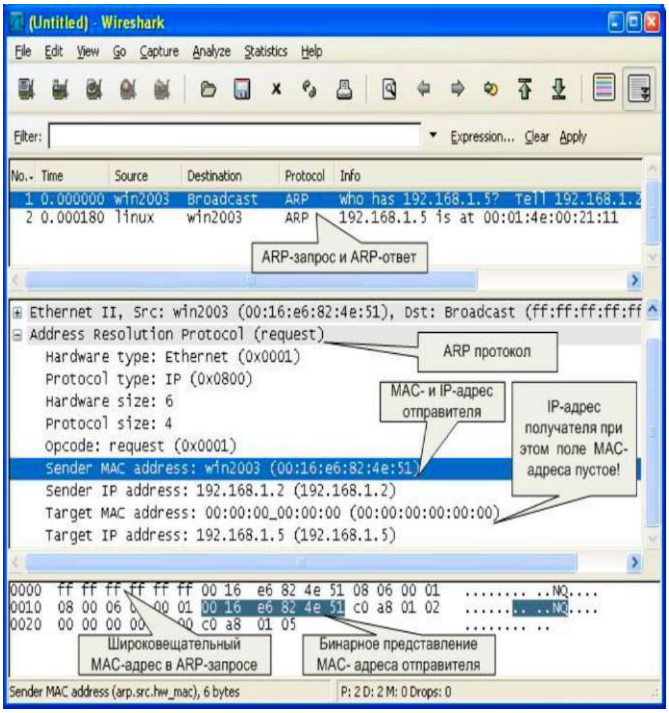
Для фильтрации ARP/RARP трафика воспользуемся фильтром захвата. В нашем случае это будет простой фильтр arp or rarp

Далее запустим захват трафика командой «Start» и выполним обращение к заданной машине, например, «пропинговав» ее: D:\>ping 192.168.1.5 Pinging 192.168.1.5 with 32 bytes of data: Reply from 192.168.1.5: bytes=32 time<1ms TTL=64 Reply from 192.168.1.5: bytes=32 time<1ms TTL=64 Reply from 192.168.1.5: bytes=32 time<1ms TTL=64 Reply from 192.168.1.5: bytes=32 time<1ms TTL=64 Ping statistics for 192.168.1.5:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms Так как на момент начала работы утилиты ping в arp-кеше не было информации о MAC-адресе соответствующего узла, то первоначально система должна выполнить определение это самого MAC-адреса, сгенерировав ARP-запрос и отослав его в сеть широковещательным пакетом. После чего она будет ожидать ответа от заданного узла.

Посмотрим же, что мы получим на практике. После остановки сниффера мы должны увидеть результат схожий с тем, что отображен на рис. 8. В нашем случае мы видим 2 захваченных пакета: ARP-запрос и ARP-ответ.



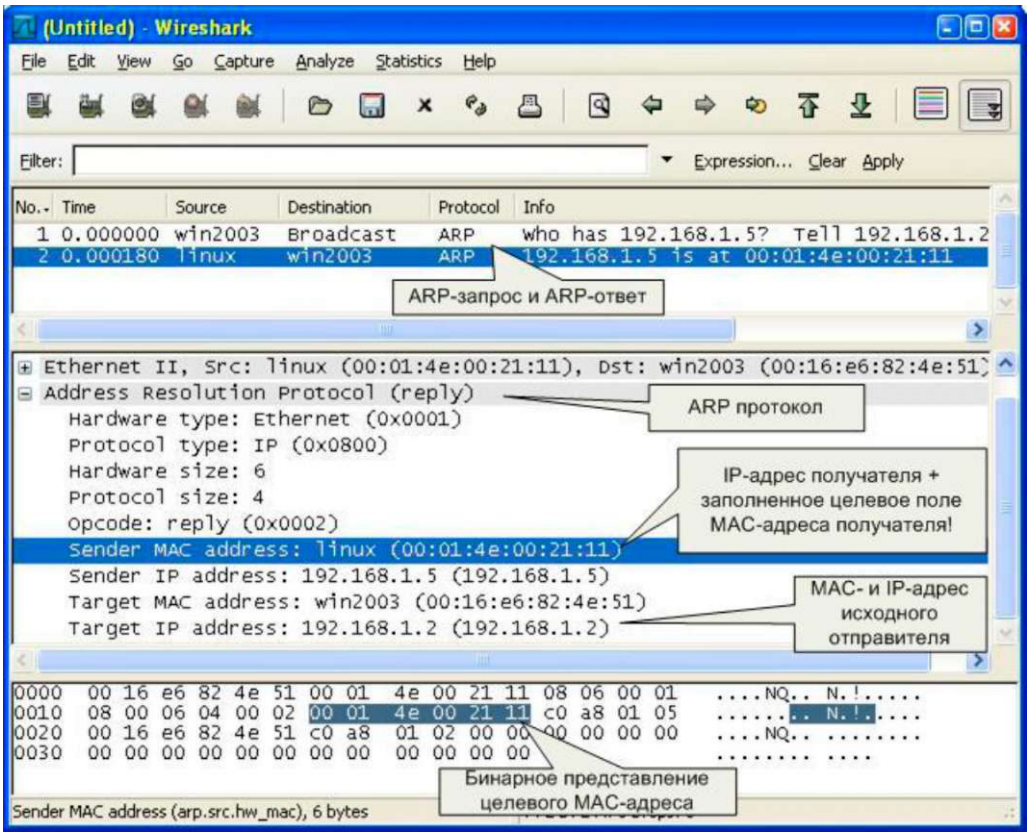
Проанализируем полученные пакеты. Сначала рассмотрим ARP-запрос (пакет №1). Выделив пакет курсором, мы получаем его раскладку по протоколам (Ethernet+ARP) в среднем окне. Wireshark очень наглядно «раскладывает» заголовок протокола по полям.

Мы можем видеть, что в пакете указаны MAC- и IP-адреса отправителя («Sender MAC address» и «Sender IP address» соответственно). Это параметры машины, с которой выполняется запрос. В данном случае запрос направлен на получения («Opcode: request» - запрос) MAC-адреса машины, у которой IP-адрес («Protocol type: IP») 192.168.1.5 («Target IP address»). При этом поле «Target MAC address» обнулено. Так как получатель ARP-запроса на момент запроса не известен, Ethernet-пакет отправляется всем машинам в данном локальном сегменте, о чем сигнализирует MAC адрес Ethernet-пакета «ff:ff:ff:ff:ff:ff».

Примечание. Обратите внимание, что пакет представляет собой бинарную последовательность и сниффер выполняет большую работу по преобразованию полей из бинарного представления в удобочитаемый вариант.

Все работающие машины в сети получают пакет с ARP-запросом, анализируют его, а ответ отсылает только та машина, чей IP-адрес соответствует IP-адресу в запросе. Таким образом, второй полученный пакет является ARP-ответом (см. рис. 9). Это следует из параметра поля «Opcode: reply». Обратите внимание, что данный пакет был отправлен

именно той машиной, чей MAC-адрес нас и интересовал («Sender IP address: 192.168.1.5»). При этом поле «Sender MAC address» заполнено значением «00:01:4E:00:21:11».



Примечание. Обратите внимание на поле «Info» в списке захваченных пакетов. Сниффер и тут упрощает анализ сетевого трафика, подсказывая назначение пакетов.

Теперь мы можем повторно просмотреть ARP-кеш и сверить данные в нем с данными, которые мы узнали из анализа пакетов ARP-запрос/ответа: D:\>arp -a

Interface: 192.168.1.2 --- 0x10003 Internet Address Physical Address Type 192.168.1.5 00-01-4e-00-21-11 dynamic

Задание.

1. Изучить интерфейс программы Wireshark (\\corp .mgkit.ru\dfs\work\wireshark).

2. Выполнить анализ ARP-протокола по примеру из методических указаний.

Вопросы для контроля.

1. Каковы основные цели мониторинга сетевого трафика?
2. Чем отличается мониторинг трафика от фильтрации?
3. Каково назначении класса программ-снифферов?
4. Какие основные функции выполняют снифферы?

Практическая работа № 8
Настройка технических устройств беспроводных сетей передачи данных.

Цель: Научиться настраивать wi-fi роутер

Оборудование и программное обеспечение:

1) Персональный компьютер.
2) Патч-корд.
3) Роутер.

1. Подключить Wi-Fi роутер к одному из компьютеров сети.
2. Настроить протокол (TCP/IP) на компьютере
3. Настроить Wi-Fi роутер через WEB-интерфейс

Порядок выполнения работы: Настройте протокол интернета (TCP/IP)

-Пуск ^ "Настройка" ^ "Панель управления" ^ "Сетевые подключения" ^ Подключение по локальной сети ^-"Свойства" ^-Протокол Интернета (TCP/IP) ^ Свойства.

-в свойствах подключения по локальной сети установите IP адрес 192.168.0.2 и маску подсети 255.255.255.0; основной шлюз 192.168.0.1; Рисунок 1.

Пуск ^ "Настройка" ^ "Панель управления" ^ "Сетевые подключения" ^ Подключение по локальной сети ^-"Свойства" ^Протокол Интернета (TCP/IP) ^ Свойства. Нажмите «ОК».

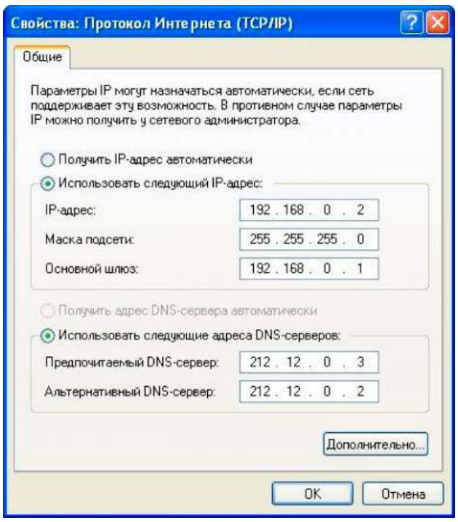


Рисунок 1 - Протокол Интернета (TCP/IP)

Настройка Статического IP адреса на роутере.

-Чтобы приступить к настройке нужно набрать в адресной строке вашего интернет браузера 192.168.0.1 и нажать клавишу "Enter".

В появившемся окне наберите имя пользователя admin и нажмите кнопку "Log In". Рисунок 2.

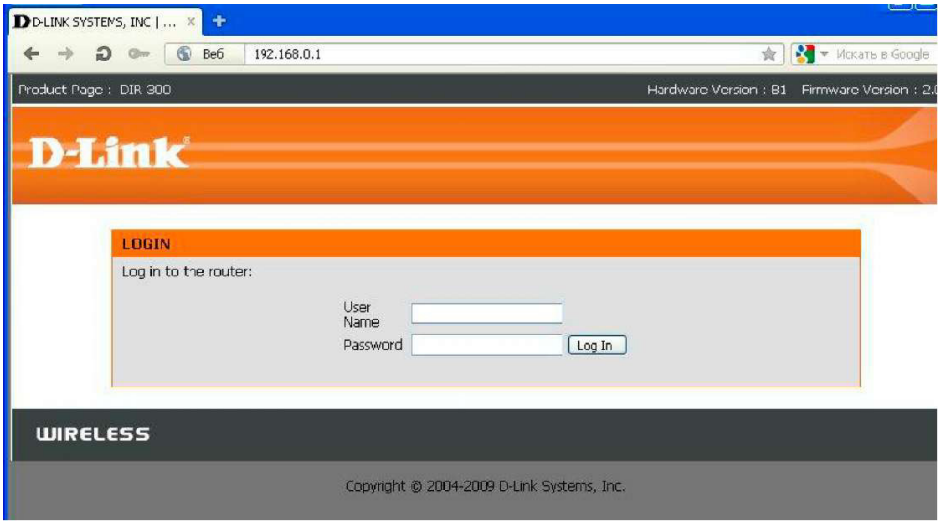


Рисунок 2 - Авторизация пользователя

Войдите в раздел «Manual Internet connection Setup» во вкладке «Internet setup». Для настройки интернета по статическому IP адресу необходимо в ниспадающем меню окна internet connection type выбрать пункт «Static IP».

В появившемся ниже окне в строке IP адрес, Subnet mask Gateway address введите данные 2222222 и нажмите «Save settings»

Настройка Wi-Fi сети в роутере

Войдите в раздел «Manual Wireless connection Setup» во вкладке «Wireless

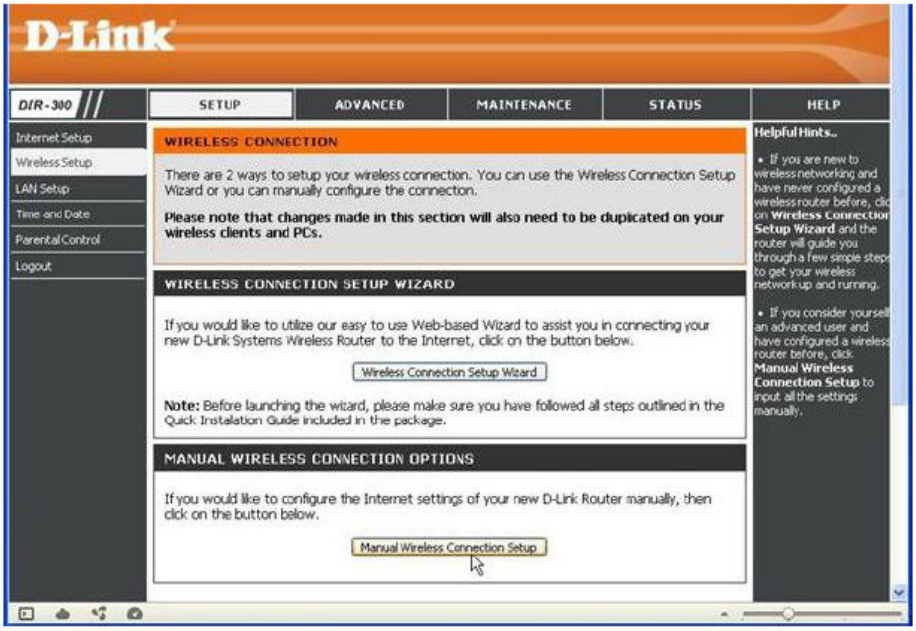


Рисунок 3 - Wireless setup

setup» Рисунок 3 для установки названия и пароля wi fi соединения.

Оставьте галку Enable Wireless для включения радиотракта. В поле SSID введите название беспроводной сети. (Примечание: В дальнейшем сеть будет отображаться под этим именем. Необходимо использовать только латинские буквы и/или цифры. В данном примере имя сети: «Skyline»).

- выбрать страну, для России это RUSSIAN FEDERATION. После внесения всех изменений нажать кнопку Save/Apply для сохранения параметров Рисунок 4.

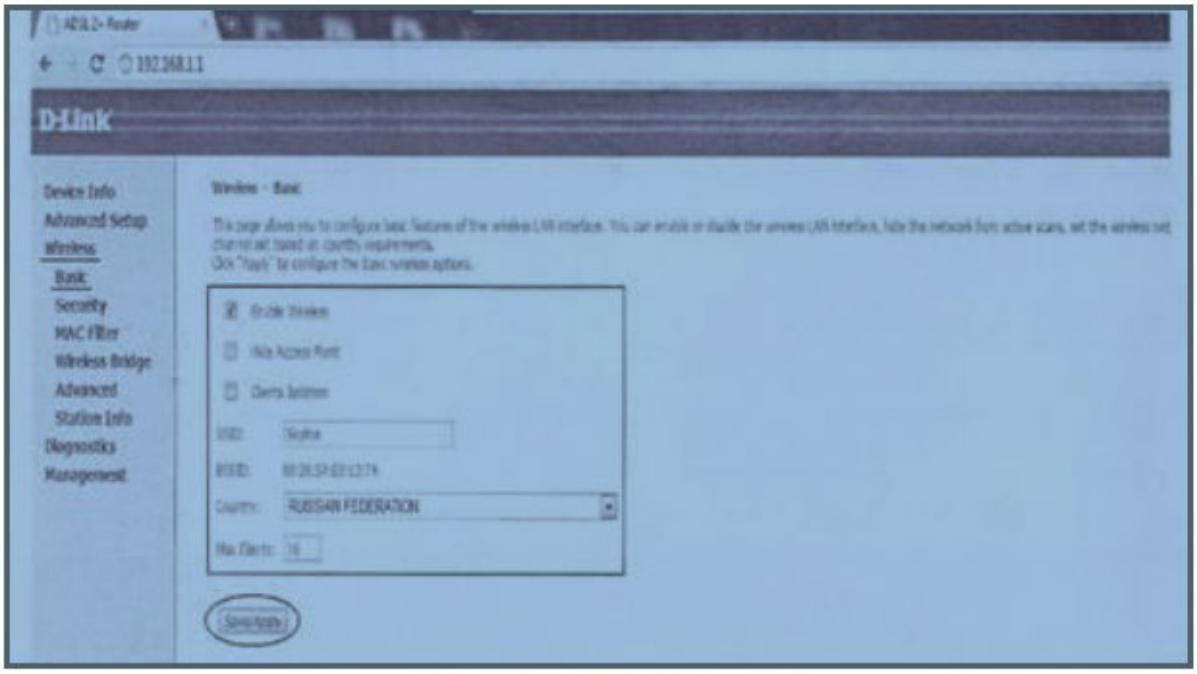


Рисунок 4 – Создание точки доступа

1) Что такое IP адрес?
2) Какие методы назначения ip адресов существуют?