

М 1159

**МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН**

**ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ**

Факультет “Компьютерный инжиниринг”

Кафедра “Компьютерные системы”

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

**для выполнения лабораторных работ по предмету
«ВВЕДЕНИЕ В КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ»**

ТАШКЕНТ 2020

УДК 004.7

Авторы: доцент К.Т. Абдурашидова, ассистент Ким Е.В.

«Введение в компьютерные системы и сети»/ ТУИТ, 56 с. Ташкент, 2020г.

В методических указаниях описаны лабораторные работы, которые дают необходимые умения и практические навыки для основы моделирования компьютерных систем и сетей, а также получение практических навыков в адресации и статической маршрутизации в IPV4-сетях, в организации беспроводных сетей, в исследовании структуры пакетов протокола уровня приложений.

Адресовано студентам, обучающимся по направлению «Искусственный интеллект», а также специалистам, которые изучают программируемые мобильные системы.

Рецензенты:

А.И. Назаров - к.т.н., доцент кафедры «Компьютерные системы».

А.А. Ганиев - к.т.н., доцент, заведующий кафедры «Криптология».

© Ташкентский университет информационных технологий имени Мухаммада ал-Хоразми, 2020.

ВВЕДЕНИЕ

Методические указания предназначены для основы моделирования компьютерных систем и сетей, а также получение практических навыков в адресации и статической маршрутизации в IPv4-сетях, в организации беспроводных сетей, в исследовании структуры пакетов протокола уровня приложений.

В Методических рекомендациях четко определен алгоритм действия обучающихся при подготовке их к занятиям по вышеуказанной дисциплине, что систематизирует и упорядочивает самостоятельную работу студентов.

Цель методических указаний дать необходимые умения и практические навыки для построения работоспособных моделей сети. Каждая тема работы включает в себя теоретическую часть и вопросы, которые надо изучить.

В данном методическом указании приводятся лабораторные занятия, основные этапы взаимодействия между несколькими пользователями, создание сложных макетов сетей, возможность проверять на работоспособность топологию сети. В каждой лабораторной работе четко определен алгоритм действия обучающихся при подготовке их к занятиям по вышеуказанной дисциплине, что систематизирует и упорядочивает самостоятельную работу студентов.

Методическое указание ориентированы на студентов, изучающих программирование аппаратной части мобильных устройств и программируемые мобильные системы. Разработанные методические указания могут служить хорошим пособием для проведения лабораторных занятий, а также для самостоятельной работы студентов.

Лабораторная работа № 1. Основы моделирования компьютерных систем и сетей.

Цель работы: Изучить основные топологии сетей и стандарты линий связи, выявить достоинства и недостатки линий связи локальных сетей.

Теоретический материал:

Компьютерная сеть – совокупность программных и аппаратных средств и среды передачи, служащая для обмена информацией между участниками.

Локальная сеть – система для непосредственного соединения многих компьютеров. При этом подразумевается, что информация передается от компьютера к компьютеру без каких-либо посредников и по единой среде передачи. Однако говорить о единой среде передачи в современной локальной сети не приходится. Например, в пределах одной сети могут использоваться как электрические кабели различных типов (витая пара, коаксиальный кабель), так и оптоволоконные кабели. Определение передачи «без посредников» также не корректно, ведь в современных локальных сетях используются репитеры, трансиверы, концентраторы, коммутаторы, маршрутизаторы, мосты, которые порой производят довольно сложную обработку передаваемой информации. Не совсем понятно, можно ли считать их посредниками или нет, можно ли считать подобную сеть локальной.

Из этого можно сделать вывод, что компьютеры, связанные локальной сетью, объединяются в один виртуальный компьютер, ресурсы которого могут быть доступны всем пользователям, причем этот доступ не менее удобен, чем к ресурсам, входящим непосредственно в каждый отдельный компьютер. Сформулировать отличительные признаки локальной сети можно следующим образом:

1. Высокая скорость передачи информации, большая пропускная способность сети. Приемлемая скорость сейчас – не менее 10 Мбит/с.
2. Низкий уровень ошибок передачи (или, что-то же самое, высококачественные каналы связи). Допустимая вероятность ошибок передачи данных должна быть порядка 10^{-8} – 10^{-12} .
3. Эффективный, быстродействующий механизм управления обменом по сети.
4. Заранее четко ограниченное количество компьютеров, подключаемых к сети.

При таком определении понятно, что глобальные сети отличаются от локальных прежде всего тем, что они рассчитаны на неограниченное число абонентов. Кроме того, они используют (или могут использовать) не слишком качественные каналы связи и сравнительно низкую скорость передачи. А

механизм управления обменом в них не может быть гарантированно быстрым. В глобальных сетях гораздо важнее не качество связи, а сам факт ее существования.

Однако сети имеют и довольно существенные недостатки, о которых всегда следует помнить:

1. Сеть требует дополнительных, иногда значительных материальных затрат на покупку сетевого оборудования, программного обеспечения, на прокладку соединительных кабелей и обучение персонала.
2. Сеть требует приема на работу специалиста (администратора сети), который будет заниматься контролем работы сети, ее модернизацией, управлением доступом к ресурсам, устранением возможных неисправностей, защитой информации и резервным копированием. Для больших сетей может понадобиться целая бригада администраторов.
3. Сеть ограничивает возможности перемещения компьютеров, подключенных к ней, так как при этом может понадобиться перекладка соединительных кабелей.
4. Сети представляют собой прекрасную среду для распространения компьютерных вирусов, поэтому вопросам защиты от них придется уделять гораздо больше внимания, чем в случае автономного использования компьютеров. Ведь достаточно инфицировать один и все компьютеры сети будут поражены.
5. Сеть резко повышает опасность несанкционированного доступа к информации с целью ее кражи или уничтожения, Информационная защита требует проведения целого комплекса технических и организационных мероприятий.

Здесь же следует упомянуть о таких важнейших понятиях теории сетей, как абонент, сервер, клиент.

Абонент (узел, хост, станция) – это устройство, подключенное к сети и активно участвующее в информационном обмене. Чаще всего абонентом (узлом) сети является компьютер, но абонентом также может быть, например, сетевой принтер или другое периферийное устройство, имеющее возможность напрямую подключаться к сети. Далее вместо термина «абонент» для простоты будет использоваться термин «компьютер».

Сервером называется абонент (узел) сети, который предоставляет свои ресурсы другим абонентам, но сам не использует их ресурсы. Таким образом, он обслуживает сеть. Серверов в сети может быть несколько, и совсем не обязательно, что сервер – самый мощный компьютер. Выделенный (dedicated) сервер – это сервер, занимающийся только сетевыми задачами. Невыделенный

сервер может помимо обслуживания сети выполнять и другие задачи. Специфический тип сервера – это сетевой принтер.

Клиентом называется абонент сети, который только использует сетевые ресурсы, но сам свои ресурсы в сеть не отдает, то есть сеть его обслуживает, а он ей только пользуется. Компьютер–клиент также часто называют рабочей станцией. В принципе каждый компьютер может быть одновременно как клиентом, так и сервером.

Под сервером и клиентом часто понимают также не сами компьютеры, а работающие на них программные приложения. В этом случае то приложение, которое только отдает ресурс в сеть, является сервером, а то приложение, которое только пользуется сетевыми ресурсами – клиентом.

2 Топология локальных сетей

Под топологией (компоновкой, конфигурацией, структурой) компьютерной сети обычно понимается физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи.

Существует три, базовые топологии сети:

Шина (bus) – все компьютеры параллельно подключаются к одной линии связи. Информация от каждого компьютера одновременно передается всем остальным компьютерам.

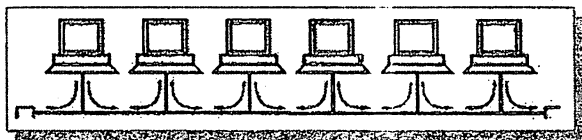


Рис. 1.1 – Сетевая топология шина

Звезда (star) – к одному центральному компьютеру присоединяются остальные периферийные компьютеры, причем каждый из них использует отдельную линию связи. Информация от периферийного компьютера передается только центральному компьютеру, от центрального – одному или нескольким периферийным.

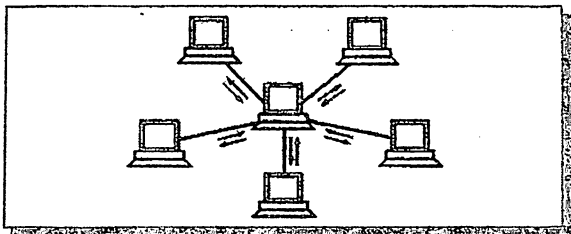


Рис. 1.2 – Сетевая топология звезда

Кольцо (ring) – компьютеры последовательно объединены в кольцо. Передача информации в кольце всегда производится только в одном направлении. Каждый из компьютеров передает информацию только одному компьютеру, следующему в цепочке за ним, а получает информацию только от предыдущего в цепочке компьютера.

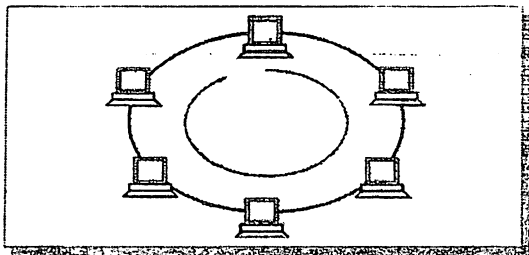


Рис. 1.3 – Сетевая топология кольцо

На практике нередко используют и другие топологии локальных сетей, однако большинство сетей ориентировано именно на три базовые топологии.

Необходимо выделить некоторые важнейшие факторы, влияющие на физическую работоспособность сети и непосредственно связанные с понятием топология:

1. Исправность компьютеров (абонентов), подключенных к сети. В некоторых случаях поломка абонента может заблокировать работу всей сети. Иногда неисправность абонента не влияет на работу сети в целом, не мешает остальным абонентам обмениваться информацией.
2. Исправность сетевого оборудования, то есть технических средств, непосредственно подключенных к сети (адаптеры, трансиверы, разъемы и т.д.). Выход из строя сетевого оборудования одного из абонентов может сказаться на всей сети, но может нарушить обмен только с одним абонентом.
3. Целостность кабеля сети. При обрыве кабеля сети (например, из-за механических воздействий) может нарушиться обмен информацией во всей

сети или в одной из ее частей. Для электрических кабелей столь же критично короткое замыкание в кабеле.

4. Ограничение длины кабеля, связанное с затуханием распространяющегося по нему сигнала. Как известно, в любой среде при распространении сигнал ослабляется (затухает). И чем большее расстояние проходит сигнал, тем больше он затухает (рис. 1.4). Необходимо следить, чтобы длина кабеля сети не была больше предельной длины $L_{пр}$, при превышении которой затухание становится уже неприемлемым (принимающий абонент не распознает ослабевший сигнал).

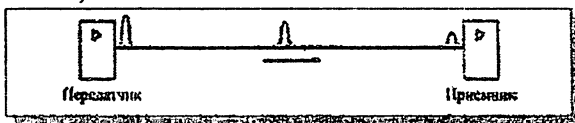


Рис. 1.4 – Затухание сигнала при распространении по сети

3 Типы линий связи локальных сетей

Средой передачи информации называются те линии связи (или каналы связи), по которым производится обмен информацией между компьютерами. В подавляющем большинстве компьютерных сетей (особенно локальных) используются проводные или кабельные каналы связи, хотя существуют и беспроводные сети, которые сейчас находят все более широкое применение, особенно в портативных компьютерах.

Каждый тип кабеля имеет свои преимущества и недостатки, так что при выборе надо учитывать, как особенности решаемой задачи, так и особенности конкретной сети, в том числе и используемую топологию.

Можно выделить следующие основные параметры кабелей, принципиально важные для использования в локальных сетях:

1. Полоса пропускания кабеля (частотный диапазон сигналов, пропускаемых кабелем, - это интервал от минимальной до максимальной пропускаемой частоты, измеряется в Гц и его производных) и затухание сигнала в кабеле. Два этих параметра тесно связаны между собой, так как с ростом частоты сигнала растет затухание сигнала. Надо выбирать кабель, который на заданной частоте сигнала имеет приемлемое затухание. Или же надо выбирать частоту сигнала, на которой затухание еще приемлемо. Затухание измеряется в децибелах и пропорционально длине кабеля.

2. Помехозащищенность кабеля и обеспечиваемая им секретность передачи информации. Эти два взаимосвязанных параметра показывают, как кабель взаимодействует с окружающей средой, то есть, как он реагирует на внешние

помехи, и насколько просто прослушать информацию, передаваемую по кабелю.

3. Скорость распространения сигнала по кабелю или обратный параметр – задержка сигнала на метр длины кабеля. Этот параметр имеет принципиальное значение при выборе длины сети. Типичные величины скорости распространения сигнала – от 0,6 до 0,8 от скорости распространения света в вакууме. Соответственно типичные величины задержек – от 4 до 5 нс/м.

4. Для электрических кабелей очень важна величина волнового сопротивления кабеля. Волновое сопротивление важно учитывать при согласовании кабеля для предотвращения отражения сигнала от концов кабеля. Волновое сопротивление зависит от формы и взаиморасположения проводников, от технологии изготовления и материала диэлектрика кабеля. Типичные значения волнового сопротивления – от 50 до 150 Ом.

3.1 Кабели на основе витых пар

Витые пары проводов используются в дешевых и сегодня, пожалуй, самых популярных кабелях. Кабель на основе витых пар представляет собой несколько пар скрученных попарно изолированных медных проводов в единой диэлектрической (пластиковой) оболочке. Он довольно гибкий и удобный для прокладки. Скручивание проводов позволяет свести к минимуму индуктивные наводки кабелей друг на друга и снизить влияние переходных процессов.

Обычно в кабель входит две или четыре витые пары.

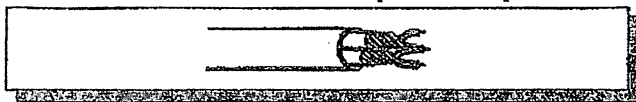


Рис. 1.5 – Кабель с витыми парами

Неэкранированные витые пары характеризуются слабой защищенностью от внешних электромагнитных помех, а также от подслушивания, которое может осуществляться с целью, например, промышленного шпионажа. Причем действие помех и величина излучения вовне увеличивается с ростом длины кабеля. Для устранения этих недостатков применяется экранирование кабелей.

В случае экранированной витой пары каждая из витых пар помещается в металлическую оплетку–экран для уменьшения излучений кабеля, защиты от внешних электромагнитных помех и снижения взаимного влияния пар проводов друг на друга. Для того чтобы экран защищал от помех, он должен быть обязательно заземлен. Естественно, экранированная витая пара заметно

дороже, чем неэкранированная. Ее использование требует специальных экранированных разъемов. Поэтому встречается она значительно реже, чем неэкранированная витая пара.

Чаще всего витые пары используются для передачи данных в одном направлении (точка-точка), то есть в топологиях типа звезда или кольцо. Топология шина обычно ориентируется на коаксиальный кабель. Поэтому внешние терминаторы, согласующие неподключенные концы кабеля, для витых пар практически никогда не применяются.

3.2 Коаксиальные кабели

Коаксиальный кабель представляет собой электрический кабель, состоящий из центрального медного провода и металлической оплетки (экрана), разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку (рис. 1.6).

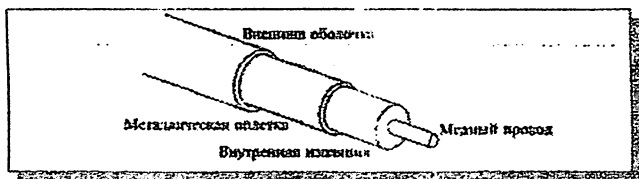


Рис. 1.6 – Коаксиальный кабель

Коаксиальный кабель до недавнего времени был очень популярен, что связано с его высокой помехозащищенностью (благодаря металлической оплетке), более широкими, чем в случае витой пары, полосами пропускания (свыше 1ГГц), а также большими допустимыми расстояниями передачи (до километра). К нему труднее механически подключиться для несанкционированного прослушивания сети, он дает также заметно меньше электромагнитных излучений вовне. Однако монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а стоимость его выше (он дороже примерно в 1,5 – 3 раза). Сложнее и установка разъемов на концах кабеля.

Основное применение коаксиальный кабель находит в сетях с топологией типа шина. При этом на концах кабеля обязательно должны устанавливаться терминаторы для предотвращения внутренних отражений сигнала, причем один (и только один!) из терминаторов должен быть заземлен. Реже коаксиальные кабели применяются в сетях с топологией звезда. В этом случае проблема согласования существенно упрощается, так как внешних терминаторов на свободных концах не требуется.

Существует два основных типа коаксиального кабеля:

1. тонкий (thin) кабель, имеющий диаметр около 0,5 см, более гибкий;
2. толстый (thick) кабель, диаметром около 1 см, значительно более жесткий. Он представляет собой классический вариант коаксиального кабеля, который уже почти полностью вытеснен современным тонким кабелем.

Тонкий кабель используется для передачи на меньшие расстояния, чем толстый, поскольку сигнал в нем затухает сильнее. Зато с тонким кабелем гораздо удобнее работать: его можно оперативно проложить к каждому компьютеру, а толстый требует жесткой фиксации на стене помещения. Подключение к тонкому кабелю (с помощью разъемов BNC байонетного типа) проще и не требует дополнительного оборудования. А для подключения к толстому кабелю надо использовать специальные довольно дорогие устройства, прокалывающие его оболочки и устанавливающие контакт как с центральной жилой, так и с экраном. Толстый кабель примерно вдвое дороже, чем тонкий, поэтому тонкий кабель применяется гораздо чаще.

В настоящее время считается, что коаксиальный кабель устарел, в большинстве случаев его вполне может заменить витая пара или оптоволоконный кабель. И новые стандарты на кабельные системы уже не включают его в перечень типов кабелей.

3.3 Оптоволоконные кабели

Оптоволоконный (он же волоконно-оптический) кабель – это принципиально иной тип кабеля по сравнению с рассмотренными двумя типами электрического или медного кабеля. Информация по нему передается не электрическим сигналом, а световым. Главный его элемент – это прозрачное стекловолокно, по которому свет проходит на огромные расстояния (до десятков километров) с незначительным ослаблением.

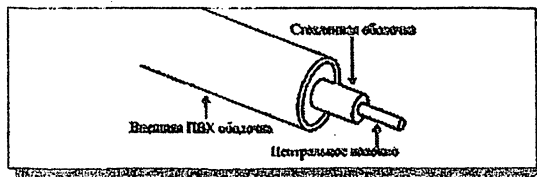


Рис. 1.7 – Структура оптоволоконного кабеля

Структура оптоволоконного кабеля очень проста и похожа на структуру коаксиального электрического кабеля. Только вместо центрального медного провода здесь используется тонкое (диаметром около 1 – 10 мкм) стекловолокно, а вместо внутренней изоляции – стеклянная или пластиковая

оболочка, не позволяющая свету выходить за пределы стекловолокна. В данном случае речь идет о режиме так называемого полного внутреннего отражения света от границы двух веществ с разными коэффициентами преломления (у стеклянной оболочки коэффициент преломления значительно ниже, чем у центрального волокна). Металлическая оплетка кабеля обычно отсутствует, так как экранирование от внешних электромагнитных помех здесь не требуется. Однако иногда ее все-таки применяют для механической защиты от окружающей среды (такой кабель иногда называют броневым, он может объединять под одной оболочкой несколько оптоволоконных кабелей).

Оптоволоконный кабель обладает исключительными характеристиками по помехозащищенности и секретности передаваемой информации. Никакие внешние электромагнитные помехи в принципе не способны исказить световой сигнал, а сам сигнал не порождает внешних электромагнитных излучений. Подключиться к этому типу кабеля для несанкционированного прослушивания сети практически невозможно, так как при этом нарушается целостность кабеля. Стоимость оптоволоконного кабеля постоянно снижается и сейчас примерно равна стоимости тонкого коаксиального кабеля.

Однако оптоволоконный кабель имеет и некоторые недостатки:

1. Самый главный из них – высокая сложность монтажа (при установке разъемов необходима микронная точность, от точности скола стекловолокна и степени его полировки сильно зависит затухание в разьеме).
2. Использование оптоволоконного кабеля требует специальных оптических приемников и передатчиков, преобразующих световые сигналы в электрические и обратно, что порой существенно увеличивает стоимость сети в целом.
3. Оптоволоконные кабели допускают разветвление сигналов (для этого производятся специальные пассивные разветвители (couplers) на 2–8 каналов), но, как правило, их используют для передачи данных только в одном направлении между одним передатчиком и одним приемником.
4. Оптоволоконный кабель менее прочен и гибок, чем электрический.
5. Чувствителен оптоволоконный кабель и к ионизирующим излучениям, из-за которых снижается прозрачность стекловолокна, то есть увеличивается затухание сигнала.
6. Применяют оптоволоконный кабель только в сетях с топологией звезда и кольцо. Никаких проблем согласования и заземления в данном случае не существует. Кабель обеспечивает идеальную гальваническую развязку

компьютеров сети. В будущем этот тип кабеля, вероятно, вытеснит электрические кабели или, во всяком случае, сильно потеснит их. Запасы меди на планете истощаются, а сырьё для производства стекла более чем достаточно.

Существуют два различных типа оптоволоконного кабеля:

1. многомодовый или мультимодовый кабель, более дешёвый, но менее качественный;
2. одномодовый кабель, более дорогой, но имеет лучшие характеристики по сравнению с первым.

Суть различия между этими двумя типами сводится к разным режимам прохождения световых лучей в кабеле.

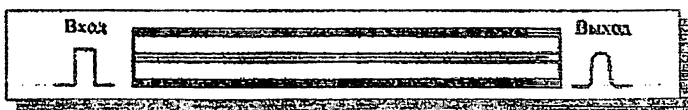


Рис. 1.8 – Распространение света в одномодовом кабеле

В одномодовом кабеле практически все лучи проходят один и тот же путь, в результате чего они достигают приемника одновременно, и форма сигнала почти не искажается. Одномодовый кабель имеет диаметр центрального волокна около 1,3 мкм и передает свет только с такой же длиной волны (1,3 мкм). Дисперсия и потери сигнала при этом очень незначительны, что позволяет передавать сигналы на значительно большее расстояние, чем в случае применения многомодового кабеля. Для одномодового кабеля применяются лазерные приемопередатчики, использующие свет исключительно с требуемой длиной волны. Затухание сигнала в одномодовом кабеле составляет около 5 дБ/км и может быть даже снижено до 1 дБ/км.

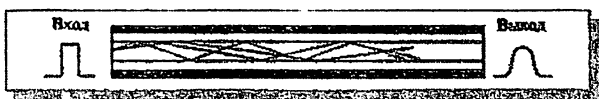


Рис. 1.9 – Распространение света в многомодовом кабеле

В многомодовом кабеле траектории световых лучей имеют заметный разброс, в результате чего форма сигнала на приемном конце кабеля искажается. Центральное волокно имеет диаметр 62,5 мкм, а диаметр внешней оболочки 125 мкм (это иногда обозначается как 62,5/125). Для передачи используется обычный (не лазерный) светодиод, что снижает стоимость и увеличивает срок службы приемопередатчиков по сравнению с одномодовым

кабелем. Длина волны света в многомодовом кабеле равна 0,85 мкм, при этом наблюдается разброс длин волн около 30 – 50 нм. Допустимая длина кабеля составляет 2 – 5 км. Многомодовый кабель – это основной тип оптоволоконного кабеля в настоящее время, так как он дешевле и доступнее. Затухание в многомодовом кабеле больше, чем в одномодовом и составляет 5 – 20 дБ/км.

Типичная величина задержки для наиболее распространенных кабелей составляет около 4–5 нс/м, что близко к величине задержки в электрических кабелях.

3.4 Бескабельные каналы связи

Кроме кабельных каналов в компьютерных сетях иногда используются также бескабельные каналы. Их главное преимущество состоит в том, что не требуется никакой прокладки проводов (не надо делать отверстий в стенах, закреплять кабель в трубах и желобах, прокладывать его под фальшполами, над подвесными потолками или в вентиляционных шахтах, искать и устранять повреждения). К тому же компьютеры сети можно легко перемещать в пределах комнаты или здания, так как они ни к чему не привязаны.

Радиоканал использует передачу информации по радиоволнам, поэтому теоретически он может обеспечить связь на многие десятки, сотни и даже тысячи километров. Скорость передачи достигает десятков мегабит в секунду (здесь многое зависит от выбранной длины волны и способа кодирования).

Особенность радиоканала состоит в том, что сигнал свободно излучается в эфир, он не замкнут в кабель, поэтому возникают проблемы совместимости с другими источниками радиоволн (радио- и телевещательными станциями, радарам, радиолюбительскими и профессиональными передатчиками и т.д.). В радиоканале используется передача в узком диапазоне частот и модуляция информационным сигналом сигнала несущей частоты.

Главным недостатком радиоканала является его плохая защита от прослушивания, так как радиоволны распространяются неконтролируемо. Другой большой недостаток радиоканала – слабая помехозащищенность.

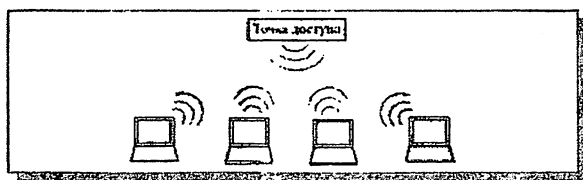


Рис. 1.10 – Объединение компьютеров

Радиоканал широко применяется в глобальных сетях как для наземной, так и для спутниковой связи. В этом применении у радиоканала нет конкурентов, так как радиоволны могут дойти до любой точки земного шара.

Инфракрасный канал также не требует соединительных проводов, так как использует для связи инфракрасное излучение (подобно пульту дистанционного управления домашнего телевизора). Главное его преимущество по сравнению с радиоканалом – нечувствительность к электромагнитным помехам, что позволяет применять его, например, в производственных условиях, где всегда много помех от силового оборудования. Правда, в данном случае требуется довольно высокая мощность передачи, чтобы не влияли никакие другие источники теплового (инфракрасного) излучения. Плохо работает инфракрасная связь и в условиях сильной запыленности воздуха.

Скорости передачи информации по инфракрасному каналу обычно не превышают 5–10 Мбит/с, но при использовании инфракрасных лазеров может быть достигнута скорость более 100 Мбит/с. Секретность передаваемой информации, как и в случае радиоканала, не достигается, также, требуются сравнительно дорогие приемники и передатчики.

4 Аппаратура локальных сетей

Аппаратура локальных сетей обеспечивает реальную связь между абонентами. Выбор аппаратуры имеет важнейшее значение на этапе проектирования сети, так как стоимость аппаратуры составляет наиболее существенную часть от стоимости сети в целом, а замена аппаратуры связана не только с дополнительными расходами, но зачастую и с трудоемкими работами.

К аппаратуре локальных сетей относятся:

1. кабели для передачи информации;
2. разъемы для присоединения кабелей;
3. согласующие терминаторы;
4. сетевые адаптеры;
5. репитеры;
6. трансиверы;
7. концентраторы.

О первых трех компонентах сетевой аппаратуры уже говорилось в предыдущих разделах. А сейчас следует остановиться на функциях остальных компонентов.

4.1 Сетевые адаптеры

Сетевые адаптеры (они же контроллеры, карты, платы, интерфейсы, NIC – Network Interface Card) – это основная часть аппаратуры локальной сети. Назначение сетевого адаптера – сопряжение компьютера (или другого абонента) с сетью, то есть обеспечение обмена информацией между компьютером и каналом связи в соответствии с принятыми правилами обмена. Именно они реализуют функции двух нижних уровней модели OSI. Плата сетевого адаптера обычно имеет также один или несколько внешних разъемов для подключения к ней кабеля сети.

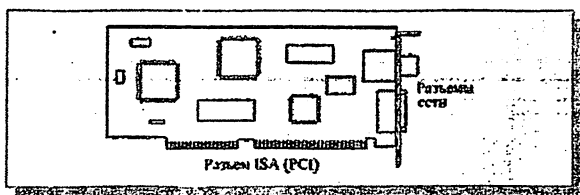


Рис. 1.11 – Плата сетевого адаптера

К основным сетевым функциям адаптеров относятся:

1. гальваническая развязка компьютера и кабеля локальной сети (для этого обычно используется передача сигналов через импульсные трансформаторы);
2. преобразование логических сигналов в сетевые (электрические или световые) и обратно;
3. кодирование и декодирование сетевых сигналов, то есть прямое и обратное преобразование сетевых кодов передачи информации (например, манчестерский код);
4. опознание принимаемых пакетов (выбор из всех приходящих пакетов тех, которые адресованы данному абоненту или всем абонентам сети одновременно);
5. преобразование параллельного кода в последовательный при передаче и обратное преобразование при приеме;
6. буферирование передаваемой и принимаемой информации в буферной памяти адаптера;

7. организация доступа к сети в соответствии с принятым методом управления обменом;

8. подсчет контрольной суммы пакетов при передаче и приеме.

Все остальные аппаратные средства локальных сетей (кроме адаптеров) имеют вспомогательный характер, и без них часто можно обойтись. Это сетевые промежуточные устройства.

4.2 Трансиверы или приемопередатчики

Трансиверы или приемопередатчики (от английского TRANsmitter + reCEIVER) служат для передачи информации между адаптером и кабелем сети или между двумя сегментами (частями) сети. Трансиверы усиливают сигналы, преобразуют их уровни или преобразуют сигналы в другую форму (например, из электрической в световую и обратно). Трансиверами также часто называют встроенные в адаптер приемопередатчики.

4.3 Репитеры

Репитеры или повторители (repeater) выполняют более простую функцию, чем трансиверы. Они не преобразуют ни уровни сигналов, ни их физическую природу, а только восстанавливают ослабленные сигналы (их амплитуду и форму), приводя их к исходному виду. Цель такой ретрансляции сигналов состоит исключительно в увеличении длины сети (рис. 5.7).

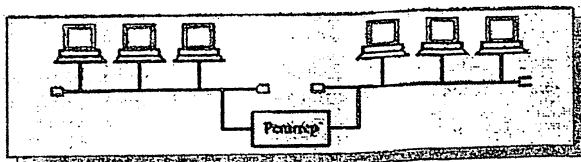


Рис. 1.12 – Соединение репитером двух сегментов сети

4.4 Концентраторы

Концентраторы (хабы, hub), как следует из их названия, служат для объединения в сеть нескольких сегментов. Концентраторы (или репитерные концентраторы) представляют собой несколько собранных в едином конструктиве репитеров, они выполняют те же функции, что и репитеры.

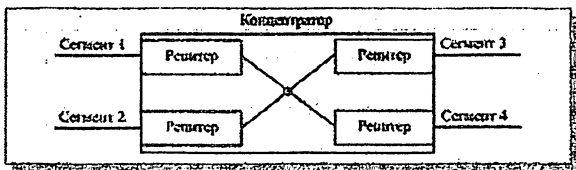


Рис. 1.13 – Схема концентратора

Преимущество подобных концентраторов по сравнению с отдельными репитерами в том, что все точки подключения собраны в одном месте, это упрощает реконфигурацию сети, контроль и поиск неисправностей. К тому же все репитеры в данном случае питаются от единого качественного источника питания.

4.5 Коммутаторы

Коммутаторы (свичи, коммутирующие концентраторы, switch), как и концентраторы, служат для соединения сегментов в сеть. Они также выполняют более сложные функции, производя сортировку поступающих на них пакетов.

Коммутаторы передают из одного сегмента сети в другой не все поступающие на них пакеты, а только те, которые адресованы компьютерам из другого сегмента. Пакеты, передаваемые между абонентами одного сегмента, через коммутатор не проходят. При этом сам пакет коммутатором не принимается, а только пересылается.

5 Стандарты линий связи

5.1 10-BASE-5

В качестве среды передачи используется толстый (желтый) коаксиальный кабель с волновым сопротивлением 50 Ом. Максимальная длина сегмента сети составляет 500 м, общая длина всех сегментов не более 2500 м. Общее число участников на один сегмент не более 100. Расстояние между участниками кратно 2.5 м.

Соединение участников с линией связи производится через трансиверы (устройства приема/передачи информации). Длина кабеля, соединяющего участника с трансивером не более 50 м.

Сегменты заканчиваются терминаторами, один из которых должен быть заземлен.

Скорость 10Мбит/с

Характеристики:

- низкая скорость
- + высокое качество

5.2 10–BASE–2

В качестве среды передачи используется тонкий коаксиальный кабель с волновым сопротивлением 50 Ом. Максимальная длина сегмента сети составляет 185 м, общая длина всех сегментов, соединенных через повторители не более 925 м. Общее число участников на один сегмент не более 30. Расстояние между соседними станциями не менее 0.5 м.

Сегменты заканчиваются терминаторами, один из которых должен быть заземлен. Ответвления от сегмента недопустимы.

Скорость 10Мбит/с

Характеристики:

- низкая скорость
- + низкая стоимость

5.3 10–BASE–T

В качестве среды передачи используется неэкранированная витая пара третьей категории (кабель состоит из 4-х пар проводов и сертифицирован на частоту до 10МГц).

Для приема/передачи используются две пары проводов. Максимальная длина кабеля между соседними участниками 100м, а общий размер сети не более 500м. Количество станций в сети не более 1024.

В качестве разъемов применяются 8–ми канальные разъемы типа RJ-45. Производится соединение типа «точка–точка», физическая топология сети – «звезда».

Скорость 10 Мбит/с.

Характеристики:

- низкая скорость
- + большой размер сети

5.4 100–BASE–T

Среда передачи – неэкранированная витая пара пятой категории (4 пары проводов, сертифицированных на частоту 100МГц).

Скорость передачи 100Мбит/с.

Характеристики:

+ хорошая скорость

+ наибольшая распространенность для витой пары

5.5 100–BASE–FL

Среда передачи – оптоволоконный кабель. Этот стандарт предназначен для соединения станций с концентратором. Для этого используются два оптоволоконных кабеля для приема и передачи.

Для многомодового кабеля длина сегмента до 2 км, для одномодового – при дуплексном режиме работы концентратора и станции больше 100 км, при стандартном оборудовании – до 10 км.

Скорость 100Мбит/с.

Характеристики:

+ хорошая скорость

– высокая стоимость

5.6 Группа стандартов GIGABIT

Используется несколько стандартов передачи данных со скоростями тысячи Мбит/с. Наиболее распространенные:

1000–BASE–F – Данные передаются по оптоволоконному кабелю

1000–BASE–T – Используется витая пара категории 5+. Данные передаются по двум парам (прием/передача) сигналами 4–х уровней на расстояние до 25м.

1000–BASE–T4 – Использует витую пару категории 5+. Для приема и передачи используется по две пары проводов длиной до 100м.

Характеристики:

+ высокая скорость

– высокая стоимость

6 Задания для выполнения

Построить схему сети университета и ее модель с указанием топологии сетей и стандартов линий связи. Основными критерием выбора должны быть: экономичность и достаточная пропускная способность. Сделать приблизительный расчет количества материалов и стоимости такой сети с учетом «сетевой» аппаратуры.

Исходные данные приведены в таблице.

№ корпуса	Количество классов	Количество ПК в классе
1	5	9
2	6	
3	7	
4	8	

Объяснить, чем Вы руководствовались при выборе тех или иных элементов сети и указать их преимущества.

Контрольные вопросы:

1. Какие топологии сетей вы знаете?
2. Чем отличается локальная сеть от глобальной?
3. Может ли быть компьютер одновременно клиентом и сервером?
4. Сколько проводов в витой паре?
5. Можно ли назвать соединение шина с соединенными концами – кольцом?
6. Чем отличается свитч (switch) от хаба (hub)?
7. Для чего нужен Терминатор?
8. Каково назначение сетевого адаптера?
9. Чем отличается витая пара в стандартах 100-BASE-T и 1000-BASE-T?
10. Чем обусловлена задержка в оптоволоконных и электрических кабелях?

Лабораторная работа №2. Исследование структуры пакетов протокола уровня приложений

Цель работы: изучение способов коммутации абонентов в КС и исследование пропускной способности сетей с различными режимами коммутации.

Теоретический материал:

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 оконечном 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

$$T_{к.к.} = (W/C), \text{ где } W - \text{ объем сообщения в битах,}$$

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

$$T_3 = (S/V), \text{ где } S - \text{ расстояние передачи в км,}$$

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 $t_{к.}$. 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 805 мс.

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.

Задания к работе:

1. Ответить на тестовые и контрольные вопросы
2. Определите, на сколько увеличится время передачи данных в сети с коммутацией пакетов по сравнению с сетью с коммутацией каналов, согласно исходных данных индивидуального варианта [индивидуальный вариант соответствует сумме двух последних цифр зачетной книжки] (скорость передачи сигнала примите равной 0,66 скорости света)

Содержание отчета:

1. Название, цель и задание к лабораторной работе.
2. Ответы на тестовые вопросы
3. Расчет времени передачи сообщения
4. Таблица аналитических выводов о свойствах способов коммутации

Индивидуальные варианты

В а р и а н т	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

1 0	700	2250	1	7	70	5	20	20
1 1	800	2500	1,1	8	80	1	2	20
1 2	900	2750	1,2	9	90	2	4	20
1 3	1000	3000	1,3	1	10	3	6	20
1 4	2000	3250	1,4	2	20	4	8	20
1 5	3000	3500	1,5	3	30	5	10	20
1 6	4000	3750	1,6	4	40	1	12	20
1 7	5000	4000	1,7	5	50	2	14	20
1 8	6000	4250	1,8	6	60	3	16	20
1 9	7000	4500	1,9	7	70	4	18	20
2 0	8000	4750	2	8	80	5	20	20
2 1	9000	5000	2,1	9	90	1	5	20
2 2	10000	5250	2,2	2	20	2	10	20
2 3	11000	5500	2,3	3	30	3	15	20
2 4	12000	5750	2,4	4	40	4	20	20
2 5	10000 0	6000	2,5	5	50	5	25	20

Контрольные вопросы.

1. Какие более частные задачи включает в себя обобщенная задача коммутации абонентов сети. Дайте краткое описание этих задач?

2. Какой способ коммутации более эффективен для сетей передачи данных: коммутация каналов или коммутация пакетов?

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

Лабораторная работа №3. Адресация и статическая маршрутизация в IPv4-сетях.


Цель работы: экспериментальное исследование сетевого конфигурирования в операционной системе Windows 7.

Теоретический материал:

Зачастую, настройка локальной сети в операционных системах Windows Vista, Windows 7, Windows Server 2008/2008 R2 начинается с такой области конфигурирования сетевых свойств, как компонент «Центр управления сетями и общим доступом». При помощи данного средства конфигурирования сетей можно выбирать сетевое размещение, просматривать карту сети, настраивать сетевое обнаружение, общий доступ к файлам и принтерам, а также настраивать и просматривать состояние ваших текущих сетевых подключений.

Открытие компонента «Центр управления сетями и общим доступом»

Для того чтобы воспользоваться функционалом средства конфигурирования сетей, нужно для начала его открыть. Чтобы открыть окно «Центр управления сетями и общим доступом», выполните одно из следующих действий:

- В области уведомлений нажмите правой кнопкой мыши на значке «Сеть» и из контекстного меню выберите команду «Центр управления сетями и общим доступом»;
- Нажмите на кнопку «Пуск» для открытия меню, выделите элемент «Сеть» и нажмите на нем правой кнопкой мыши. Из контекстного меню выберите команду «Свойства»;
- Нажмите на кнопку «Пуск» для открытия меню, откройте «Панель управления», из списка компонентов панели управления выберите категорию «Сеть и Интернет», а затем перейдите по ссылке «Центр управления сетями и общим доступом»;
- Нажмите на кнопку «Пуск» для открытия меню, в поле поиска введите Центр управления и в найденных результатах откройте приложение «Центр управления сетями и общим доступом»;
- Воспользуйтесь комбинацией клавиш +R для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть»

введите

%windir%\system32\control.exe

/name

Microsoft.NetworkAndSharingCenter и нажмите на кнопку «ОК».

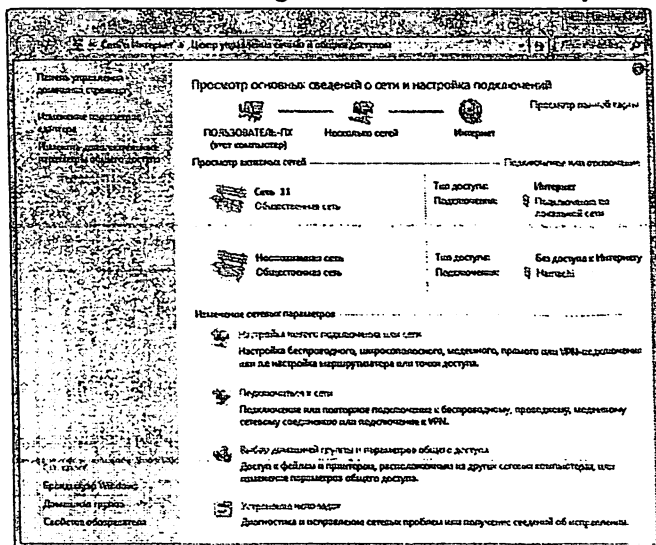


Рис. 3.1. «Центр управления сетями и общим доступом»

Понятие сетевого расположения

Перед началом работы с данным компонентом, следует разобраться с таким понятием как сетевое расположение. Этот параметр задается для компьютеров при первом подключении к сети и во время подключения автоматически настраивается брандмауэр и параметры безопасности для того типа сети, к которому производится подключение. В отличие от операционной системы Windows Vista, где для всех сетевых подключений используется самый строгий профиль брандмауэра для сетевого размещения, операционная система Windows 7 поддерживает несколько активных профилей, что позволяет наиболее безопасно использовать несколько сетевых адаптеров, подключенных к различным сетям. Существует четыре типа сетевого расположения (рис.3.2).

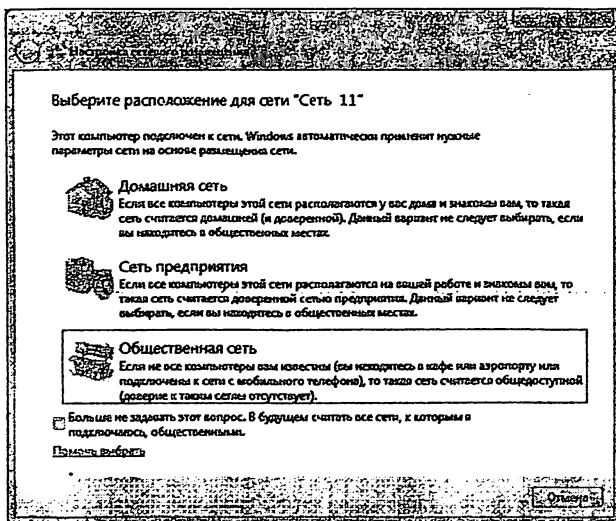


Рис. 3.2. Выбор сетевого расположения

Домашняя сеть. Данное сетевое расположение предназначено для использования компьютера в домашних условиях или в таких сетях, где пользователи очень хорошо знают друг друга. Такие компьютеры могут создавать и присоединяться к домашним группам. Для домашних сетей автоматически включается обнаружение сети.

Сеть предприятия. Такое сетевое расположение используется в сети малого офиса (SOHO). Для этого сетевого расположения также включено обнаружение сети, но вы не можете ни создавать, ни присоединять компьютер к домашней группе.

Общественная сеть. Это сетевое расположение предназначено для использования компьютера в таких общественных местах, как кафе или аэропорты. Это наиболее строгое размещение, у которого по умолчанию отключены возможности присоединения к домашней группе и сетевое обнаружение.

Доменная сеть. Если компьютер присоединён к домену Active Directory, то существующей сети будет автоматически назначен тип сетевого размещения «Домен». Доменный тип сетевого расположения аналогичен рабочей сети, за исключением того, что в домене конфигурация брандмауэра Windows, сетевого обнаружения, а также сетевой карты определяется групповой политикой.

Каким образом связаны компьютеры в сети, можно просматривать с помощью карты сети. Однако этот компонент доступен не для всех типов сетевого расположения.

Карта сети

Карта сети – это графическое представление расположения компьютеров и устройств, которое позволяет увидеть все устройства вашей локальной сети, а также схему их подключения друг к другу. В окне «Центр управления сетями и общим доступом» отображается только локальная часть сетевой карты, компоновка которой зависит от имеющихся сетевых подключений. Компьютер, на котором выполняется создание карты, отображается в левом верхнем углу. Другие компьютеры подсети отображаются слева. Такие устройства инфраструктуры, как коммутаторы, концентраторы и шлюзы в другие сети отображаются справа. Сетевое сопоставление работает в проводных и беспроводных сетях, однако, только в частных и доменных сетях. Просмотреть карту публичной сети невозможно. Протокол LLTD обеспечивает сопоставление только компьютеров в одной подсети, которая является обычной установкой в домашних или малых офисах.

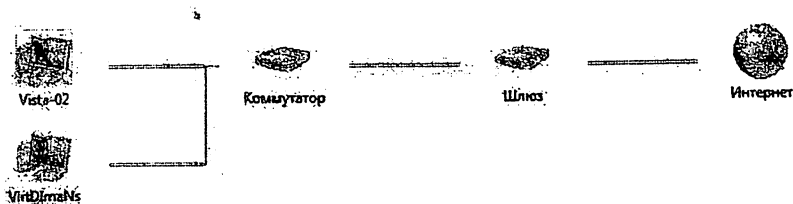


Рис. 3.3. Пример карты сети

Можно заметить, что некоторые компьютеры и устройства отображаются отдельно в нижней части окна «Карта сети» либо могут вообще отсутствовать. Например, если сервер печати беспроводной сети поддерживает технологию UPnP, а не LLTD, то он будет располагаться в нижней части окна «Карта сети». Подобная ситуация возникает, поскольку не все операционные системы и устройства предполагают поддержку протокола LLTD или вследствие возможной неправильной настройки устройств. Пример карты сети вы можете увидеть на рис.3.3.

За работу карты сети в операционных системах отвечают два компонента:

- Обнаружение топологии связи Link Layer (Link Layer Topology Discover Mapper – LLTD Mapper) – компонент, который запрашивает в сети устройства для включения их в карту;
- Отвечающее устройство LLTD (Link Layer Topology Discover Responder – LLTD Responder) – компонент, который отвечает за запросы компонента LLTD Mapper.

По умолчанию, карту сети можно просматривать только для расположений «Домашняя сеть» или «Сеть предприятия». При попытке просмотра сетевой карты для расположений «Доменная сеть» или «Общественная сеть» вы увидите сообщение о невозможности отображения карты.

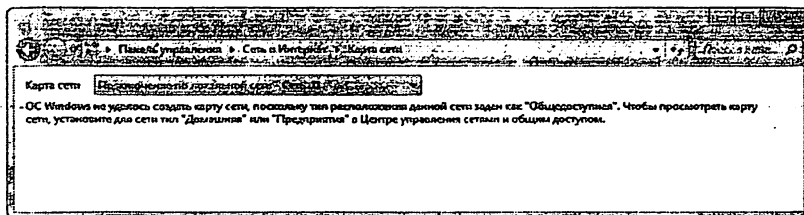


Рис. 3.4. Попытка просмотра карты сети

Для того чтобы включить сетевое сопоставление в доменной сети, вам нужно на контроллере домена выполнить следующие действия:

1. Откройте оснастку «Управление групповой политики»;
2. Выберите объект групповой политики (например, Default Domain Policy, область действия – весь домен), который будет распространяться на компьютер, расположенный в доменной сети, нажмите на нем правой кнопкой мыши и из контекстного меню выберите команду «Изменить»;
3. В оснастке «Редактор управления групповыми политиками» разверните узел Конфигурация компьютера/Политики/Административные шаблоны/Сеть/Обнаружение топологии связи (Link Layer) и выберите политику «Включает драйвер отображения ввода/вывода (LLTDIO)»;
4. В свойствах параметра политики установите переключатель на опцию «Включить» и установите флажок «Разрешить операцию для домена»;
5. Повторите аналогичные действия для параметра политики «Включить драйвер «Ответчика» (RSPNDR)»;

6. Обновите параметры политики на клиентской машине, используя команду `gpupdate /force /boot`;
7. Обновите карту сети.

Сетевые подключения

После установки драйвера для каждого сетевого адаптера, операционная система Windows пытается автоматически сконфигурировать сетевые подключения на локальном компьютере. Все доступные сетевые подключения отображаются в окне «Сетевые подключения». Сетевое подключение представляет собой набор данных, необходимых для подключения компьютера к Интернету, локальной сети или любому другому компьютеру.

Открыть окно «Сетевые подключения» вы можете любым из следующих способов:

- Откройте окно «Центр управления сетями и общим доступом» и перейдите по ссылке «Изменение параметров адаптера»;
- Нажмите на кнопку «Пуск» для открытия меню, в поле поиска введите «Просмотр сетевых и в найденных результатах откройте приложение «Просмотр сетевых подключений»;
- Воспользуйтесь комбинацией клавиш **Win+R** для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» введите `ncpa.cpl` или `control netconnection` и нажмите на кнопку «ОК».

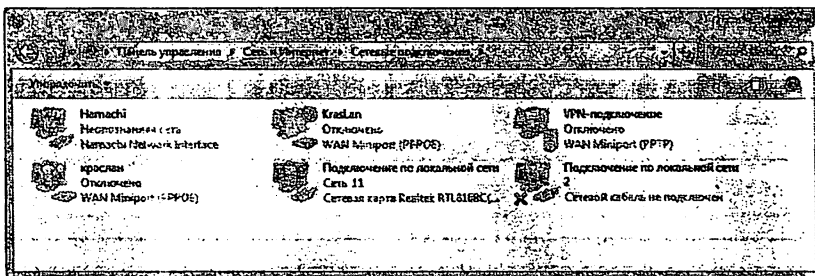


Рис. 3.5. Окно «Сетевые подключения»

При выборе любого сетевого подключения вы можете выполнить с ним следующие действия:

Переименование подключения. Операционная система по умолчанию назначает всем сетевым подключениям имена «Подключение по локальной

сети» или «Подключение к беспроводной сети» и номер подключения в том случае, если у вас существует более одного сетевого подключения. При желании, вы можете переименовать любое сетевое подключение одним из трех следующих способов:

- Нажмите на клавишу F2, введите новое имя сетевого подключения, после чего нажмите на клавишу Enter;
- Нажмите правой кнопкой мыши на переименовываемом сетевом подключении и из контекстного меню выберите команду «Переименовать». Введите новое имя сетевого подключения, после чего нажмите на клавишу Enter;
- Выберите сетевое подключение и нажмите на кнопку «Переименование подключения», которая расположена на панели инструментов. После чего введите новое имя сетевого подключения и нажмите на клавишу Enter.

Состояние сети. Используя данное окно, вы можете просмотреть любые данные о состоянии сетевого подключения и такие детали, как IP-адрес, MAC-адрес и прочее. Чтобы открыть диалоговое окно сведений о сетевом подключении, выполните следующие действия:

- Откройте диалоговое окно «Состояние» одним из следующих способов:
- Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «Состояние»;
- Выберите сетевое подключение и нажмите на кнопку «Просмотр состояния подключения», которая расположена на панели инструментов;
- Выберите сетевое подключение и нажмите на клавишу Enter.

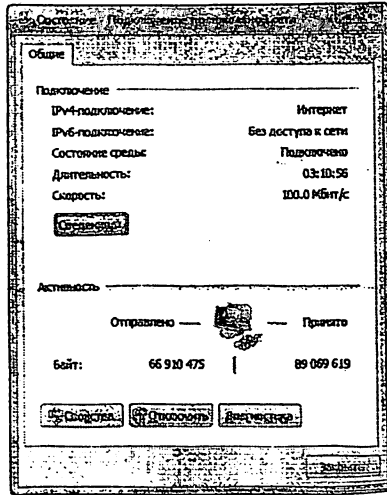


Рис. 3.6. Диалоговое окно состояния подключения по локальной сети

В окне «Состояние – подключение по локальной сети» нажмите на кнопку «Сведения». В диалоговом окне «Сведения о сетевом подключении», отображенном ниже, вы можете просмотреть подробные сведения о текущем сетевом подключении.

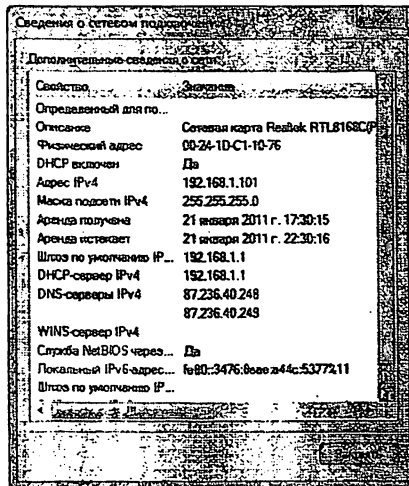


Рис. 3.7. Сведения о сетевом подключении

- **Диагностика подключения.** В случае обнаружения проблем в работе вашего сетевого подключения, окно «Сетевые подключения» предлагает средство диагностики «Устранение неполадок», которое содержит возможность решения при помощи анализа подключения. Для того чтобы воспользоваться данным средством выполните любое из следующих действий:
 - Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «Диагностика».
 - Выберите сетевое подключение и нажмите на кнопку «Диагностика подключения», которая расположена на панели инструментов.

В открывшемся диалоговом окне «Диагностика сетей Windows» для устранения неполадок следуйте действиям мастера.

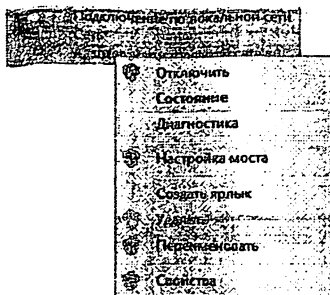


Рис. 3.8. Открытие мастера устранения неполадок подключения по локальной сети

- **Отключение сетевого устройства.** Иногда проблемы с сетевыми подключениями решаются посредством отключения сетевого адаптера компьютера от сети. Для того чтобы отключить сетевой адаптер выполните одно из следующих действий:
 - Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «Отключить»;
 - Выберите сетевое подключение и нажмите на кнопку «Отключение сетевого устройства», которая расположена на панели инструментов.

- **Настройка параметров подключения.** Как таковые, сетевые подключения не позволяют осуществлять коммуникации. Осуществление коммуникаций обеспечивают сетевые клиенты, службы и протоколы, которые привязаны к созданным сетевым подключениям (рис.3.9).

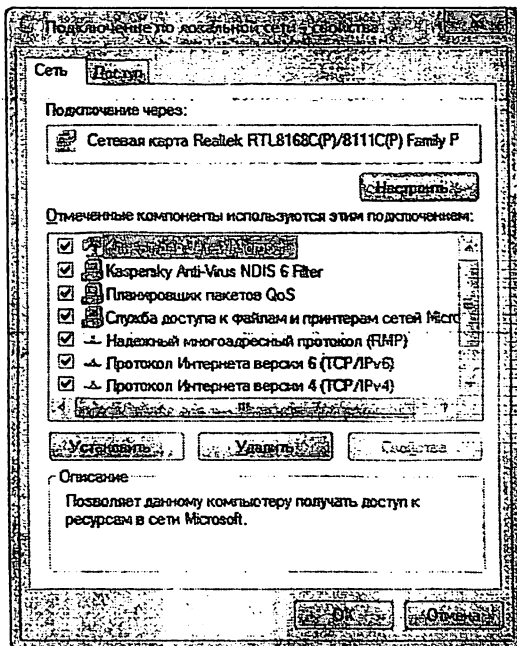


Рис. 3.9. Диалоговое окно свойств сетевого подключения

Для того чтобы изменить настройки вашего сетевого подключения, вы можете воспользоваться средствами настройки параметров подключения. Для изменения компонентов и настроек сетевого подключения, выполните следующие действия:

- Нажмите правой кнопкой мыши на сетевом подключении и из контекстного меню выберите команду «Свойства»;
- Выберите сетевое подключение и нажмите на кнопку «Настройка параметров подключения», которая расположена на панели инструментов;

- Выберите сетевое подключение и воспользуйтесь комбинацией клавиш Alt + Enter.

Установленные возле компонентов флажки указывают, что эти компоненты привязаны к подключению.

Таким образом, в рамках выполнения данной лабораторной работы были рассмотрены средства конфигурирования сетевых свойств операционных систем Windows – «Центр управления сетями и общим доступом». Рассмотрены понятия сетевого расположения, сетевых карт, при помощи которых отображается локальная часть сетевой карты, компоновка которой зависит от имеющихся сетевых подключений. Также вы ознакомились с окном сетевых подключений, которое позволяет конфигурировать сетевые подключения на локальном компьютере. В следующей лабораторной работе вы узнаете о том, как можно настроить клиенты, службы и протоколы сетевых подключений при помощи пользовательского графического интерфейса.

Контрольные вопросы:

Какое назначение у компонента «Центр управления сетями и общим доступом»?

1. Продемонстрируйте, какие существуют способы открытия компонента «Центр управления сетями и общим доступом».
2. Охарактеризуйте типы сетевого расположения.
3. Что представляет собой карта сети, по сути, и по виду?
4. Какие протоколы отвечают за построение карты сети.
5. В каких ситуациях просмотр карты сети будет не возможен?
6. С каким аппаратным сетевым компонентом связываются свойства доступных сетевых подключений?
7. Какие существуют способы открытия окна «Сетевые подключения»?
8. Какие действия пользователь обычно может выполнить по отношению к любому сетевому подключению?
9. Охарактеризуйте свойства сведений о сетевом подключении для компьютера, на котором вы выполняете лабораторную работу. Объясните значения данных свойств.

Лабораторная работа №4. Организация беспроводных сетей.

Беспроводные системы и их виды.

Цель работы: приобрести навыки в настройке беспроводной сети; изучить состав аппаратного обеспечения для беспроводной связи.

Теоретический материал:

В современном мире все большее применение находят беспроводные сети Wi-Fi, позволяющие давать клиентам доступ к ресурсам сетей, например к Internet, с ноутбука или персонального компьютера, используя в качестве среды передачи данных радиоканал, что не требует наличия специальных проводных соединений клиентов с сетью, обеспечивая таким образом их мобильность.

Преимущества Wi-Fi

- Отсутствие проводов.

Передача данных в сети осуществляется по радиоканалу. Возможна установка в местах, где прокладка проводной сети по тем или иным причинам невозможна или нецелесообразна, например на выставках, залах для совещаний.

- Мобильность, как рабочих мест, так и самого офиса.

Так как беспроводная сеть не привязана к проводам, Вы можете свободно изменять местоположение Ваших компьютеров в зоне покрытия точки доступа, не беспокоясь о нарушениях связи. Сеть легко монтируется/демонтируется, при переезде в другое помещение Вы можете даже забрать свою сеть с собой.

Недостатки Wi-Fi

- Относительно высокая стоимость оборудования
- Небольшая дальность действия – 50-100 метров
- Велика опасность несанкционированного подключения к сети сторонних пользователей

В предлагаемой лабораторной работе мы освоим создание простейшей сети Wi-Fi на примере подключения ноутбуков к точке доступа Wi-Fi с использованием статической и динамической IP-адресации.

Схема сети имеет следующий вид (рис.4.1.):

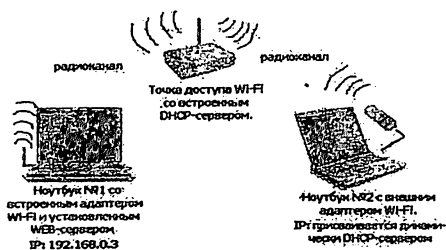


Схема сети

Рис.4.1. Схема сети

Задания:

1. Возьмите Wi-Fi-адаптер. Подключите адаптер к USB-порту ноутбука №2. (См. схему сети).
2. Включите ноутбуки. После загрузки операционной системы на ноутбуках, на обоих адаптерах должны загореться сигнальные лампочки, свидетельствующие о установке радиообмена между адаптерами и точкой доступа.

Сеть собрана, теперь ее необходимо настроить.

1-я часть работы. Настройка сети со статическим адресом компьютера клиента.

Настройка сети заключается в установке протоколов ноутбука клиента, которые необходимы для его работы, а также включение и настройка DHCP-сервера, который находится в точке.

Запомните. Протокол – это специальная программа, посредством которой компьютеры сети обмениваются между собой данными по специальным правилам. В нашей сети рабочим протоколом будет протокол TCP/IP. Чтобы компьютеры могли обмениваться между собой данными этот протокол должен быть установлен на всех компьютерах, которые находятся в сети. На ноутбуке сервере протокол TCP/IP уже установлен, нам осталось установить и настроить этот протокол на ноутбуке клиенте (см. схему сети). Помните, что все пункты настройки должны выполняться в той последовательности, в которой они указаны. Не нарушайте последовательность настройки.

На ноутбуке №2 выполните следующие действия:

Зайдите в «Панель управления», выберите в меню «Центр управления сетями и общим доступом» (рис.4.2.).

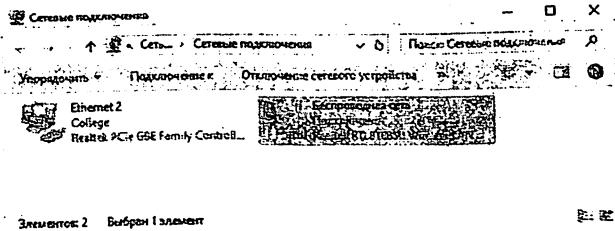


Рис.4.2. Центр управления сетями и общим доступом

Выберите в списке «Беспроводное сетевое соединение», щелкните по нему правой клавишей мыши и выберите пункт «Свойства»). Откроется окно свойств соединения (рис.4.3.)

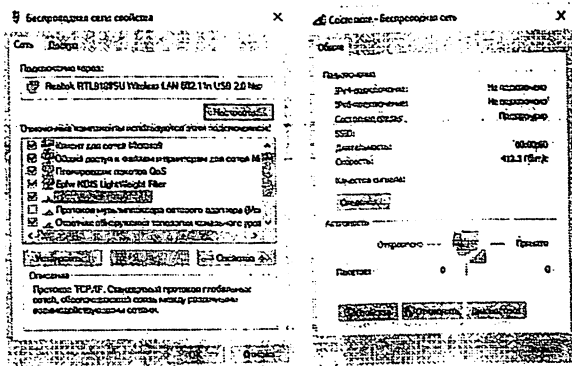


Рис.4.3. Окно свойств соединения

В появившемся окне выберите «Протокол Интернета (TCP/IP)», нажмите «Свойства». Откроется окно настроек протокола. Активируйте флажок «Использовать следующий IP-адрес». Введите в поля IP-адрес и Маска подсети адреса установок, которые изображены ниже.

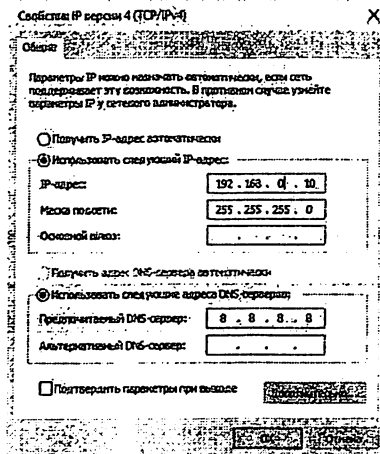


Рис.4.4. 255.255.255.0 – это IP-адрес компьютера в сети.

255.255.255.0 – маска подсети. Это специальный параметр, который вместе с адресом однозначно определяет сеть, в которой находится компьютер. После ввода настроек, нажмите «ОК», окно «Свойства: Протокол Интернета (TCP/IP)» закроется. В окне «Беспроводное сетевое соединение» нажмите «ОК».

Мы настроили ноутбук клиент для работы с беспроводной сетью. Для ноутбука прописан статический IP-адрес - это означает что мы присвоили ноутбуку выделенный, постоянный IP-адрес и прочие настройки, которые можно менять и назначать только вручную. Статический IP-адрес нам необходим для того, чтобы подключиться к точке доступа Wi-Fi и чтобы другие компьютеры в сети могли с ним связываться.

Для того чтобы начала функционировать сеть Wi-Fi необходимо настроить точку доступа.

Настройка точки доступа Wi-Fi и DHCP-сервер

Загрузите обозреватель Internet Explorer. Введите в его адресной строке адрес:

<http://192.168.0.50/> Это IP-адрес точки доступа Wi-Fi. По этому адресу расположена система ее конфигурации. Вход в систему конфигурации защищен логином и паролем и на экране появится окно для ввода этих данных.

Установите следующие параметры DHCP, либо измените существующие.

Щелкните по рисунку `hello_html_m673ab805.jpg` чтобы сохранить сделанные настройки. Точка доступа Wi-Fi уйдет на перезагрузку, которая занимает примерно полминуты.

Запомните. Выполненные выше настройки обеспечивают выполнение следующих функций:

- **Function Enable / Disable** – Включает (Enabled) или отключает (Disabled) DHCP-сервер.
- **IP Assigned From** – задает начальный IP-адрес, с которого начинается диапазон IP-адресов, выделяемых динамическим пользователям (пользователи, которые подключаются временно).
- **The Range of Pool** – задает конец диапазона IP-адресов, конечное значение последней цифры IP-адреса.
- Таким образом в нашем примере мы задали диапазон IP-адресов от 192.168.0.51 до 192.168.0.200 включительно.
- **SubMask** – маска подсети. Это специальный параметр, который вместе с адресом однозначно определяет сеть, в которой находится компьютер.
- **Lease Time** – время «жизни» выделенных пользователю сетевых настроек. При динамической адресации настройки пользователя существуют определенное время, после чего сбрасываются и программное обеспечение пользователя запрашивает новые настройки. Здесь задается время существования выделенных пользователю настроек (в секундах).
- **Status** – специальный параметр, он ставится в значение ON, если в сети используется совместно динамическая и статическая адресация. В нашем случае этот параметр установлен в ON, поскольку на ноутбуке клиента прописан статический, постоянный адрес.

Проверка работы беспроводной сети.

После того, как сеть настроена, нужно проверить ее работу и убедиться, что компьютеры могут обмениваться данными между собой. Необходимо знать, что в сети могут существовать самые разные службы и сервисы, каждый из которых выполняет свои задачи. В сети, которую мы настроили работают две службы: локальный WEB-сервер, предназначенный для размещения HTML-страниц в сети, и Сеть Microsoft, посредством которой производится обмен файлами и совместная работа с клиентами.

Сначала проверим работу WEB-сервера. WEB-сервер установлен на ноутбуке сервер. Для того, чтобы проверить работу WEB-сервера, запустите на ноутбуке №2 (компьютер Клиент) обозреватель Интернета Internet Explorer и в его адресной строке введите `http://192.168.0.3/wifi/`.

Если страница загрузится, действуйте в соответствии с указаниями, написанными на этой странице.

Если страница не загрузилась, значит сеть настроена неправильно. Тогда сделайте следующее:

Проверьте еще раз настройки протокола TCP/IP ноутбука клиента и убедитесь, что они введены правильно.

Если ошибка не исчезает, позвоните преподавателя.

Запомните. Статическая IP-адресация имеет следующие недостатки:

Для того, чтобы узнать все настройки сети, необходимо обратиться к администратору сети, который должен индивидуально выделить для каждого клиента свой уникальный IP-адрес. Это неудобно как для клиента, так и для администратора.

При подключении к какой-либо другой беспроводной сети, настройки компьютера клиента приходится снова изменять под новую сеть, узнавая их у администратора.

Если случайно ваши настройки совпадут с настройками другого клиента, вы не сможете подключиться к сети.

Всех указанных недостатков лишена динамическая IP-адресация.

2-я часть работы. Настройка сети с динамическим адресом компьютера клиента.

Динамическая IP-адресация осуществляется с помощью DHCP-сервера, который находится в точке доступа. Разберемся что это такое.

Запомните. DHCP-сервер использует DHCP протокол (англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Для этого компьютер, подключаемый к сети, обращается к серверу, DHCP, который на время проведения сеанса работы с сетью ему выдает динамический IP-адрес. Это позволяет избежать ручной настройки компьютеров сети, уменьшает количество ошибок и позволяет клиентам быстро подключаться к сети не тратя время на настройку протоколов связи вручную.

Настройка ноутбука на динамическую IP-адресацию.

Вернитесь к началу лабораторной работы, где вы осуществляли настройку сети ноутбука №2. (Раздел «Настройка сети»).

Повторите шаги 1-3, только на 3-м шаге, где вы вводили статический IP-адрес активируйте флажок «Получить IP-адрес автоматически». Это опция и включает динамическую IP-адресацию.

Нажмите «ОК», окно «Свойства: Протокол Интернета (TCP/IP)» закроется. В окне «Беспроводное сетевое соединение» (рис.2.) нажмите «ОК».

Динамическая IP-адресация на ноутбуке настроена!

Проверка динамической IP-адресации.

Используя процедуру «Безопасного извлечения устройства» отключите Wi-Fi адаптер от ноутбука клиента. Она выполняется так же, как и при отключении флеш-карт.

Удалите адаптер из разъема USB.

Подождите несколько секунд и снова вставьте адаптер в разъем USB. Произойдет автоматическое подключение ноутбука клиента к беспроводной сети Wi-Fi и ноутбуку будут динамически присвоены IP-адрес и прочие сетевые настройки.

Для того, чтобы убедиться в том, что сетевые настройки были динамически присвоены, сделайте следующее: Откройте «Пуск / Стандартные / Командная строка». Появится строка для ввода команд операционной системы. Введите в строке команду: ipconfig и нажмите Enter

Эта команда отображает на экран настройки протокола TCP/IP вашего компьютера.

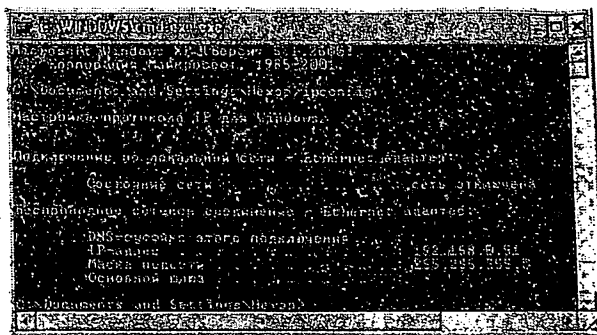


Рис.4.5. Команда ipconfig

Если указанный командой IP-адрес компьютера находится в диапазоне 192.168.0.51 – 192.168.0.200, значит динамическая IP-адресация работает нормально.

В случае, если указанный командой IP-адрес компьютера НЕ находится в диапазоне 192.168.0.51 – 192.168.0.200), необходимо:

Произвести настройку сети заново, установив статический IP-адрес, затем, подключившись к точке доступа Wi-Fi проверьте, включен - ли DHCP-сервер и правильно - ли выставлены его параметры.

Проверка работы беспроводной сети.

Сначала проверим работу WEB-сервера. WEB-сервер установлен на ноутбуке сервере. Для того, чтобы проверить работу WEB-сервера, запустите на ноутбуке клиенте обозреватель Интернета Internet Explorer и в его адресной строке введите <http://192.168.0.3/wifi/>. Если страница загрузится, действуйте в соответствии с указаниями, написанными на этой странице. Если страница не загрузилась, значит сеть настроена неправильно. Тогда сделайте следующее:

Проверьте еще раз настройки протокола TCP/IP ноутбука №2 и убедитесь, что они введены правильно. IP-адрес должен назначаться динамически, включите динамическую адресацию, если это не было сделано.

Контрольные вопросы:

1. Сети wi-fi – основные стандарты и принципы работы.
2. Методы доступа к среде в сетях Wi-Fi.
3. Слот и межкадровый интревал.
4. Режимы работы сетей Wi-Fi
5. Методы защиты сетей Wi-Fi.
6. Эталонная модель OSI/ISO.

ЗАКЛЮЧЕНИЕ

Методические указания предназначены для основы моделирования компьютерных систем и сетей, а также получение практических навыков в адресации и статической маршрутизации в IPv4-сетях, в организации беспроводных сетей, в исследовании структуры пакетов протокола уровня приложений.

Современный прогресс человечества связан в первую очередь с глобальной информатизацией всего мирового сообщества. Современные компьютерные сети являются системой, возможности и характеристики которой в целом существенно превышают соответствующие показатели простой суммы составляющих элементов сети персональных компьютеров при отсутствии взаимодействия между ними. Достоинства компьютерных сетей обусловили их широкое распространение в информационных системах кредитно-финансовой сферы, органов государственного управления и местного самоуправления, предприятий и организаций.

При всей этой общности мы использовали и конкретные инструкции, и свойства современных платформ, рассмотренные примеры могут быть практически сразу использованы в практике создания и проектирования для компьютерных сетей.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ:

Основная литература:

1. Стратегия действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017-2021 годах. 07.02.2017 г. УП 4947
2. Andrew S. Tanenbaum. Computer Networks, Fourth Edition. Publisher; Prentice Hall, 2014
3. Витаманюк А. Создание, обслуживание и администрирование сетей. СПб.: Питер. 2015 - 282 с.
4. Гук М. Энциклопедия. Аппаратные средства локальных сетей. СПб.: Питер. 2012 - 576 с.
5. Велихов А.В. и др. Компьютерные сети. Учебное пособие по администрированию локальных и объединенных сетей. 3-е изд. доп. и исп. – М.: Нов. Изд. Дом. 2015 г. – 304 с.

Дополнительная литература:

1. Мирзиёев Ш.М. Буюк келажгимизни мард ва олижаноб халкимиз билан бирга курамыз. Тошкент. «Узбекистон», НМИУ, 2017. – 488 б.
2. Мирзиёев Ш.М. Эркин ва фаворон, демократик Узбекистон давлатини биргаликда барпо этамыз. Тошкент. «Узбекистон», НМИУ, 2016. – 56 б.
3. Бройдо В.Л. Архитектура ЭВМ и систем. Учебник для вузов. – СПб. Питер.2018. – 720 с.
4. Цилькер Б.Я., Орлов С.А. «Вычислительные системы, сети и телекоммуникации» -- СПб. Питер.2015. – 384 с.

Веб-сайты:

1. www.intuit.ru
2. <http://www.kgtu.runnet.ru>
3. <http://www.piter.com>
4. <http://www.ciscopress.ru>

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	5
ЛАБОРАТОРНАЯ РАБОТА №1	
Основы моделирования компьютерных систем и сетей.....	4
ЛАБОРАТОРНАЯ РАБОТА №2	
Исследование структуры пакетов протокола уровня приложений.....	22
ЛАБОРАТОРНАЯ РАБОТА №3	
Адресация и статическая маршрутизация в IPV4-сетях.....	32
ЛАБОРАТОРНАЯ РАБОТА №4	
Организация беспроводных сетей.....	43
ЗАКЛЮЧЕНИЕ.....	51
СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ.....	52

Учебно-методическое пособие по предмету «Введение в компьютерные
системы и сети»
для бакалавров по направлению 5330500 – «Компьютерный инжиниринг»

Рассмотрено на заседании кафедры «Компьютерные системы»

от «__» _____ 2020 г. Протокол № _____

Рассмотрено на заседании факультета «Компьютерный инжиниринг»

от «__» _____ 2020 г. Протокол № _____

Рассмотрено и рекомендовано к изданию на заседании научно-
методического Совета ТУИТ

от «__» _____ 2020 г. Протокол № _____

Составители: К.Т. Абдурашидова,
Е.В. Ким

Рецензенты: М.Б. Зайнутдинова
М.М. Кодиров

Ответственный редактор: Ж.Х. Джуманов

Формат 60x84 1/16. Печ. лист 3,5.
Заказ № 90. Тираж 30.
Отпечатано в «Редакционно издательском»
отделе при ГУИТ.
Ташкент ул. Амир Темур, 108.