ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ
(ВОЛГОГРАДСКИЙ ФИЛИАЛ)

УТВЕРЖДАЮ
Директор Волгоградского
филиала МГГЭУ
_____Рябишин А.П.
«_04_» _июня_ 2019 г.

МЕТОДИЧЕСКОЕ ПОСОБИЕ

по учебной дисциплине

Компьютерные сети

по специальности
09.02.05 Прикладная информатика (по отраслям)
квалификация – техник-программист

Волгоград, 2019 г.

Методическое пособие по учебной дисциплине «Компьютерные сети» разработано на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 09.02.05 Прикладная информатика (по отраслям).

Организация-разработчик: Волгоградский филиал федерального государственного бюджетного образовательного учреждения инклюзивного высшего образования «Московский государственный гуманитарно-экономический университет»

Разработчик:

Вахранев Андрей Борисович, преподаватель высшей квалификационной категории, Волгоградский филиал МГГЭУ

Рецензенты: _____

_____

_____

_____

Рассмотрено на заседании предметной цикловой комиссии

_____

Протокол № 10 от « 16 » мая 2019 г.

Председатель ПЦК _____ / Ермакова О.В /

Заключение методического совета № 8 от « 28 » мая 2019 г.

Комитет образования, науки и молодежной политики Волгоградской области
Государственное автономное учреждение дополнительного профессионального образования
«Волгоградская государственная академия последипломного образования»
(ГАУ ДПО «ВГАПО»)

400012, г. Волгоград, ул. Новодвинская, 19А
Тел. 8442-606-613, 606-614, 606-609
E-mail: vgapkro@mail.ru (приемная)
E-mail: timnpo@yandex.ru (кафедра ТиМНПО)

ПОРЯДК. №88

ВЫПИСКА
из протокола №1 от «16» сентября 2019 года заседания Экспертного научно-методического совета профессионального образования Волгоградской области

Обсуждали: Предложение УМО по УГС 09.00.00. об использовании в *учебном процессе профессиональных образовательных организаций* ***методического пособия по учебной дисциплине Компьютерные сети*** *разработчика* ***Вахранева А.Б.,*** *Московского государственного гуманитарно-экономического университета (Волгоградский филиал).*

Постановили: ***Методическое пособие по учебной дисциплине Компьютерные сети*** *разработчика* ***Вахранева А.Б.,*** *Московского государственного гуманитарно-экономического университета (Волгоградский филиал),* ***соответствует*** *установленным в системе СПО ВО требованиям в части комплексного учебно-методического обеспечения и* ***рекомендуется*** *в качестве учебного издания* ***по специальности 09.02.05 Прикладная информатика (по отраслям)*** *для использования в учебном процессе профессиональных образовательных организаций, реализующих программы среднего профессионального образования.*

Председатель ЭНМС _____ **/С.В. Куликова, д.п.н., профессор, ректор ГАУ ДПО «ВГАПО»/**

Оглавление

Введение

Данное методическое пособие разработано преподавателем А.Б. Вахраневым для студентов 2 курса на базе среднего (полного общего) образования и 3 курса на базе основного общего образования ФГБОУИ ВО МГГЭУ (Волгоградский филиал) специальности 09.02.05 «Прикладная информатика (по отраслям)» по дисциплине «Компьютерные сети» на основе ФГОС СПО (Приказ Министерства образования и науки РФ от 13 августа 2014 г. N 1001 "Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.05 Прикладная информатика (по отраслям)"), РУП СПО и рабочей программы по данной дисциплине.

По дисциплине «Компьютерные сети», на основе рекомендаций работодателей, выделены следующие дидактические единицы:

В результате освоения дисциплины обучающийся должен уметь:

– проектировать вычислительные сети;

– настраивать сетевое оборудование;

– выбирать сетевое оборудование для различных целей;

– обнаруживать и устранять ошибки при передаче данных;

– организовывать межсетевое взаимодействие.

В результате освоения дисциплины обучающийся должен знать:

– установку и настройку параметров компьютерной сети;

– способы проверки правильности передачи данных;

– способы обнаружения и устранения ошибок при передаче данных;

– взаимодействие с прикладными протоколами;

– организацию сетевого взаимодействия;

– техническое сетевое оборудование;

– основных производителей сетевого оборудования;

– понятия маршрутизатора, сетевого шлюза, брэндмауэра и т.п.

В тематическом плане предусмотрено 2 раздела: «Основы сетей передачи данных» и «Сетевое оборудование».

Раздел 1 «Основы сетей передачи данных» состоит из двух тем:

1. Знакомство с сетями передачи данных
2. Изучение стандартов, моделей и протоколов компьютерных сетей

Раздел 2 «Сетевое оборудование» так же состоит из двух тем:

1. Изучение сетевого оборудования
2. Проектирование, монтаж и настройка компьютерных сетей

В данном методическом пособии содержатся теоретические сведения по темам разделов, вопросы для контроля знаний, описания и практические задания, а также список актуальной литературы и Интернет-ресурсов.

I. Основы сетей передачи данных

Для успешного изучения дисциплины, с целью становления высококвалифицированным специалистом в области компьютерных сетей, обучающемуся необходимо серьезное понимание таких смежных дисциплин, как «Основы теории информации», «Операционные системы и среды» и «Архитектура электронно-вычислительных машин и вычислительные системы». Работодателям Волгограда и области нужны специалисты, способные собрать рабочие станции, установить и настроить операционные системы, разработать и провести монтаж локальных компьютерных систем, настроить сетевое взаимодействие и адресацию, поднять сетевые серверы и т.п. Речь идет о том, что простых умений использования Интернет-приложений явно не достаточно для того, чтобы считаться компетентным в данной сфере.

I.1. Знакомство с сетями передачи данных

Для того, чтобы составить верное представление о компьютерных сетях в целом, необходимо познакомиться с историей эволюции сетей передачи данных, с основными задачами построения сетей, с необходимой терминологией (без знания которой невозможно и частичное освоение дисциплины), и с технологиями, лежащими в основе компьютерных сетей.

I.1.1. Эволюция вычислительных сетей

История появления и развития компьютерных сетей происходила под влиянием различных факторов, как то: развитие кибернетики[1] и науки об информации, электроники и схемотехники, алгоритмизации, радио и телефонных сетей, и т.п. Все подобные науки основаны на современных естественных философских науках – физике и математике. И любые

[1] **Кибернетика** (от греч. kybernetike — «искусство управления», от греч. kybernao — «правлю рулём, управляю», от греч. Κυβερνήτης — «кормчий») — наука об общих закономерностях процессов управления и передачи информации в машинах, живых организмах и обществе.

Информационные Технологии[1] (Information Technologies, IT), в том числе и Компьютерные сети, основаны на физике и математике.

Исторически сложилась ситуация, что терминология в сфере IT не сразу понятна, или же термин, описывающий какой-либо объект или явление, трактуется по-разному либо понимается не верно. Так, например, такие термины, как «Компьютерная сеть», «Вычислительная сеть» и «Сеть передачи информации», являются, по сути, одним и тем же. Но, тем не менее, это различные термины, с различными определениями. Компьютерная сеть – это система компьютеров и автоматических цифровых устройств, объединенных линиями связи. Вычислительная сеть – это система из вычислительных элементов, работающая над решением определенного круга проблем. А сеть передачи данных – это система линий связи с принимающими и посылающими данные элементами. Не говоря уже, что бытовые выражения явно не вносят четкости и адекватности в науку, а частенько, из-за наложения терминологии, затрудняют понимание. Например, многие не-специалисты часто называют системный блок компьютера процессором, кто-то не отличает хранение данных в локальной системе от ресурса на сервере. Подобная некомпетентность может самым серьезным образом сказаться на качестве изучения компьютерных сетей. Поэтому наука о компьютерных сетях является системной, а не линейной, состоящей из многих отдельных объектов. Любая компьютерная сеть – система[2], в которой каждый элемент очень важен, а не просто куча отдельных объектов. Так, для успешного администрирования компьютерных сетей не достаточно уметь нажимать кнопки и быть просто оператором ЭВМ. Необходимо знать весь комплекс IT, в том числе и операционные системы, и информационные системы, и архитектуру вычислительных систем, и теорию безопасности.

---

[1] **Информационные технологии** — широкий класс дисциплин и областей деятельности, относящихся к технологиям управления и обработки данных, в том числе, с применением вычислительной техники.

[2] **Систе́ма** (от греч. σύστημα, «составленный») — множество взаимосвязанных объектов и ресурсов, организованных процессом системогенеза в единое целое и, возможно, противопоставляемое среде.

Считается, что по мере развития телекоммуникаций[1] и вычислительной техники, эти две ранее отдельные сферы наук пересеклись, и в месте пересечения возник корень науки о вычислительных сетях (Рис.1). И теперь эти науки слились в одну общую и развиваются взаимосвязано.

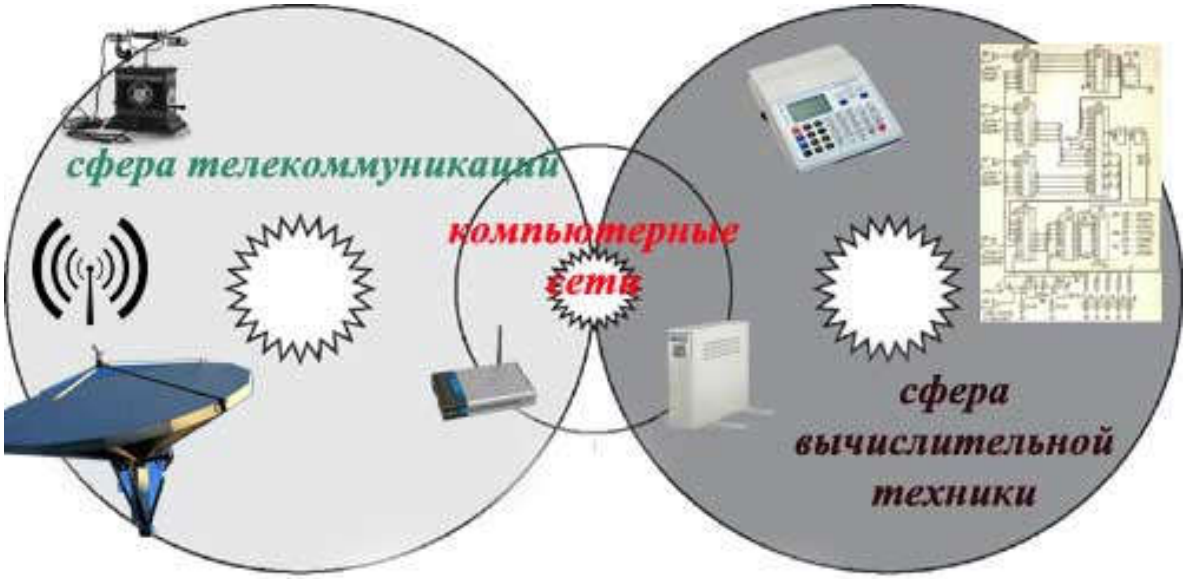


Рис.1. Сфера развития компьютерных сетей

Одной из ранних (конец XVIII века) технологий систем связи был оптический телеграф. Впоследствии он был вытеснен электрическим телеграфом, а затем и телефоном. Системы цифровой связи развиваются с 1960-х годов.

В 1623г Вильгельм Шикард придумал «Считающие часы» — первый механический калькулятор, умевший выполнять четыре арифметических действия. Примерно в 1820 году Charles Xavier Thomas создал первый удачный, серийно выпускаемый механический калькулятор — Арифмометр Томаса, который мог складывать, вычитать, умножать и делить.

[1] **Телекоммуникации** - связь в технике — передача информации (сигналов) на расстояние.

С появлением и развитием ЭВМ, со временем, появились терминальные[1] технологии, то есть стало возможным работать с ЭВМ, находящейся в вычислительном центре, непосредственно на своем рабочем месте. Терминалы не обладали свей вычислительной мощностью, но, работая за терминалом, складывалось впечатление единоличного использования ЭВМ. Такие многотерминальные системы явились прообразом компьютерных сетей.

Сейчас, классифицируя компьютерные сети, их делят на два вида: локальные сети и глобальные сети.

Локальная сеть (ЛВС, *локальная вычислительная сеть*; англ. *Local Area Network, LAN*) — компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт). Также существуют локальные сети, узлы которых разнесены географически на расстояния более 12 500 км (космические станции и орбитальные центры). Несмотря на такие расстояния, подобные сети всё равно относят к локальным.

Глобальная сеть (Global Area Network, GAN) – сеть передачи данных, покрывающая глобальные территории и часто соединяющая локальные сети.

Несмотря на кажущуюся нелогичность, первыми появились глобальные сети, а не локальные. Еще до того, как реализовали связь типа компьютер-компьютер, терминалы, посредством глобальных сетей, уже соединяли с мейнфреймом[2]. Глобальные компьютерные сети разворачивались очень часто на базе других глобальных сетей – телефонных. При таких обстоятельствах и появились модемы – устройства модуляции[3] и демодуляции.

Со временем, при появлении новейших сетевых технологий, компьютерные сети развернулись на всю нашу планету и проникли

---

[1] **Термина́л** (англ. *terminal*) — оконечная часть некоей системы, которая обеспечивает связь системы с внешней средой.

[2] **Мейнфрейм** - большая универсальная ЭВМ — высокопроизводительный компьютер со значительным объёмом оперативной и внешней памяти, предназначенный для организации централизованных хранилищ данных большой ёмкости и выполнения интенсивных вычислительных работ.

[3] **Модуля́ция** [лат. modulatio мерность, размерность] — процесс изменения одного или нескольких параметров высокочастотного модулируемого колебания по закону информационного низкочастотного сообщения (сигнала).

практически во все сферы человеческой деятельности. Уже невозможно представить серьезное предприятие без своей локальной или корпоративной сети, ведение бизнеса без использования Internet[1], полеты самолетов без систем автонавигации и связи, без мобильных телефонов т.д. Компьютерные сети настолько сильно вошли в жизнь современной цивилизации, что страшно представить что будет, если, вдруг, это все перестанет работать или выйдет из-под контроля.

[1] **Интерне́т** (англ. *Internet*, от *Inter*connected *Net*works — объединённые сети) — глобальная телекоммуникационная сеть информационных и вычислительных ресурсов.

Вопросы для самоконтроля

1. Под влиянием каких факторов родились компьютерные сети?
2. Что такое компьютерная сеть?
3. Что такое вычислительная сеть?
4. Что такое сеть передачи данных?
5. На стыке каких сфер наук возник корень сферы компьютерных сетей?
6. Что такое терминал?
7. Что такое локальная сеть?
8. Что такое глобальная сеть?
9. Какие сети появились ральше? LAN или GAN?
10. Что такое мейнфрейм?
11. Что такое модем?
12. Что такое Интернет?

I.1.2. Основные задачи построения сетей

Все, с чем сталкивается любая наука – решение определенного круга задач. Так и компьютерные сети – если бы они не были нужны, они вряд ли бы когда-либо появились. Задачи, решаемые сегодня компьютерными сетями, не поддаются простому перечислению. Как уже было замечено в предыдущей главе, компьютерные сети плотно окутали всю планету и прочно вошли во все сферы человеческой деятельности. Но основные задачи перечислить все-же можно.

Во-первых, компьютерные сети – это вычислительные сети. То есть, задача компьютерной сети – увеличение мощности всей системы, посредством увеличения числа вычисляющих элементов. Несколько компьютеров могут справиться с задачей быстрее, чем один.

Во-вторых, компьютерные сети – сети передачи данных. То есть, задача компьютерных сетей – обмениваться данными, хранить данные, обрабатывать данные.

Для каждой сферы бизнеса существуют свои задачи построения сетей. Бизнес, с точки зрения IT, принято делить на малый, средний и крупный в зависимости от количества рабочих станций сети, а не в зависимости от денежного оборота, как в экономике. Так малый бизнес – от 10 до 100 компьютеров, средний – от 100 до 200, еще больше – крупный. Это примерные приблизительные цифры, которые используются для удобства описания задач, ПО, техники и т.п. Но меньше 10ти компьютеров – это вообще не бизнес, это – частная сеть (Personal Area Network, PAN). Это стоит запомнить хотя бы для того, что бы правильно выбирать серверные технологии.

Для малого бизнеса характерны свои задачи построения компьютерных сетей. Как правило, это автоматизация документооборота. Для этого достаточно десятка компьютеров и выделенный сервер[1] для обработки и хранения данных. И, конечно же, документы необходимо выводить на печать.

Рассмотрим подробнее задачу печати.

Пусть имеется рабочая станция, с подключенным принтером, и необходимо вывести на печать документ из прикладной программы (Рис.2). Прикладная программа работает в операционной системе рабочей станции. У ОС есть уровень ядра и уровень драйверов. Драйвер[1] управляет контроллером передающего интерфейса. Передающий интерфейс генерирует управляющие сигналы.

У принтера тоже есть информационный интерфейс и контроллер, управляющий печатью.

---

[1] **Сервер** - логический или физический узел сети, обслуживающий запросы к одному адресу и/или доменному имени (смежным доменным именам), состоящий из одного или системы аппаратных серверов, на котором выполняются один или система серверных программ.

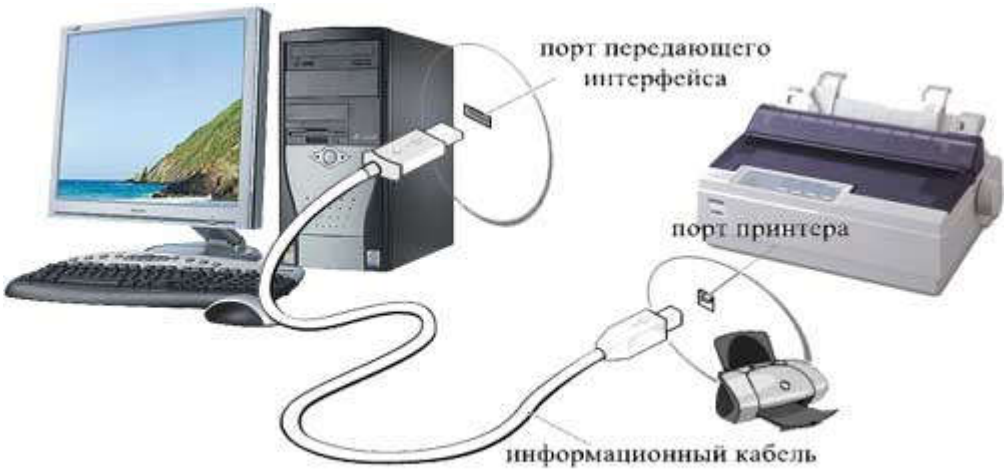


Рис.2. Соединение компьютер-принтер

Таким образом, прикладная программа передает данные для печати ядру ОС, ядро ОС, посредством драйвера, генерирует управляющий сигнал на интерфейсе, к которому подключен принтер, через порт интерфейса сигналы попадают на порт принтера, и контроллер принтера производит необходимые действия над механикой принтера для вывода на печать.

Рассмотрим теперь другой случай – когда один компьютер локальной сети посылает на печать документ, используя принтер, подключенный к другому компьютеру этой сети (Рис.3).

Рис.3. Соединение компьютер-компьютер-принтер

Приложение 1го компьютера передает данные ядру своей ОС, ядро ОС, посредством драйвера, управляет контроллером сетевого интерфейса, с интерфейса через порт данные попадают на порт сетевого интерфейса второго компьютера, потом через драйвер сетевого интерфейса в ядро ОС второго

[1] **Дра́йвер** (англ. *driver*) - компьютерная программа низкого уровня, с помощью которой другая программа (обычно операционная система) получает доступ к аппаратному обеспечению некоторого устройства.

компьютера, потом опять через драйвер принтера, как описано в предыдущем примере, происходит вывод на печать.

Итак, еще раз восстановим цепочку целиком.

Прикладное ПО 1го компьютера – ядро ОС 1го компьютера – драйвер сетевого интерфейса 1го компьютера – контроллер сетевого интерфейса 1го компьютера - порт сетевого интерфейса 1го компьютера – линия передачи данных – порт сетевого интерфейса 2го компьютера – контроллер сетевого интерфейса 2го компьютера – драйвер сетевого интерфейса 2го компьютера – ядро ОС 2го компьютера – драйвер интерфейса печати – контроллер интерфейса печати – порт интерфейса печати – информационный кабель – порт принтера – контроллер принтера.

Поэтому, чтобы реализовать печать документов в сети на один принтер, надо не только настроить сеть, но и настроить соответствующие драйверы и права доступа в операционных системах компьютеров сети.

Но для продвижения данных в более масштабных сетях, со сложной структурой и различными устройствами, необходимо решать и более сложные задачи, такие как коммутация, мультиплексирование, маршрутизация и т.п. Об этом далее.

Вопросы для самоконтроля

1. Назовите основные задачи построения сетей
2. Расскажите про масштабы бизнеса с точки зрения IT
3. Что характерно для малого бизнеса с точки зрения IT?
4. Прокомментируйте задачу вывода документа на печать
5. Прокомментируйте задачу сетевой печати
6. Выполните задачу на построение цепи передачи данных (по заданию преподавателя)
7. Что нужно для администрирования двух компьютеров и одного принтера?

I.1.3. Коммутация и мультиплексирование

Сложность графа физического построения практически любой серьезной сети, предполагает связь компьютеров (или других элементов сети). И чем сложнее структура сети, тем сложнее задача коммутации[1], то есть логической связи компьютеров (абонентов).

Пусть имеется абстрактная сеть произвольной структуры (Рис.4). На рисунке узлы 8 и 7 непосредственно друг-с-другом не связаны, а значит, вынуждены пользоваться транзитным узлом – 6. К тому же, у транзитного узла 6 имеются три порта – a, b и c. Соответственно данные с узла 8, чтобы поступить на узел 7, должны попасть на узел 6 через порт a, и потом поступить через порт b на узел 7. Соответственно, чтобы коммутировать узлы 1 и 5 можно пройти двумя путями.

Первый: 1 – 2a – 2c – 3a – 3c – 9a – 9b – 4c – 4b – 5

Второй: 1 – 2a – 2c – 3a – 3b – 4a – 4b – 5

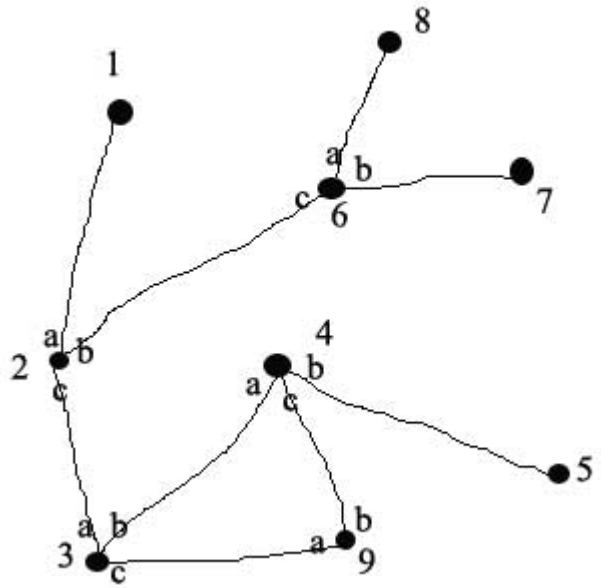


Рис.4. Сеть произвольной структуры

[1] **Коммутация** - процесс соединения абонентов коммуникационной сети через транзитные узлы

Как наглядно можно увидеть, второй путь короче первого, так как на узле 3 данные, после поступления с порта a, ушли не на порт c, а на порт b, избегая лишнего пребывания на узле 9.

На практике задачу коммутации решают коммутаторы – устройства коммутации. А тот путь, которые проделывают данные с узла отправления до узла доставки – маршрутом.

Вся задача коммутации может быть представлена в виде пяти отдельных задач:

1. Определение информационных потоков, для которых необходимо установить маршрут
2. Определение конкретного маршрута для потока
3. Сообщение выбранного маршрута транзитным узлам
4. Продвижение потока и локальная коммутация на каждом транзитном узле
5. Мультиплексирование и демультиплексирование потоков

I.1.4. Информационные потоки

Информационным потоком (data flow, data stream) называют последовательность данных, объединенных набором общих признаков, который выделяет эти данные из общего сетевого трафика[1].

Данные передаются порциями различного объема. Поэтому и информационный поток состоит из таких порций. Общими признаками таких порций, для определения потока при коммутации, могут служить пара узел-приемник и узел-отправитель, а так же определенный маршрут. Но этого не всегда оказывается достаточно. Если на оконечных узлах работают различные сетевые приложения, им понадобятся разные потоки. И тогда выбор каждого пути должен осуществляться с учетом характеристик передаваемых данных.

---

[1] **Тра́фик** (от англ. *traffic* — «движение, транспорт, торговля») - объём информации, передаваемой по сети

Признаки потока могут иметь локальные и глобальные значения. Глобальные значения служат для определения потока в пределах всей сети, а локальные – в пределах, например, одного транзитного узла.

Существует особый тип признака потока – это метка потока[1]. Определить потоки – это значит задать для них набор отличительных признаков, на основании которых коммутаторы смогут направлять потоки по предназначенным для них маршрутам.

I.1.5. Маршрут потока

Определение маршрута для потока, то есть пути, по которому пройдут все порции данных от отправителя к приемнику, сложная задача. В ней придется решить задачи нахождения оптимального пути, через все транзитные узлы и сетевые интерфейсы.

В качестве критериев выбора оптимального маршрута, могут выступать:

- номинальная пропускная способность (у разных линий передачи данных пропускная способность может быть различна);
- загруженность каналов связи;
- задержки в каналах связи;
- количество транзитных узлов и сетевых интерфейсов;
- надежность каналов и транзитных узлов.

Вообще, маршрут потока можно сравнить с маршрутом такси. Водитель решает подобные задачи – выбирает кратчайший путь, с хорошей дорогой, объезжая пробки на дорогах. Так и маршрутизация в сетях – каждая порция данных должна быть снабжена служебной информацией об узле-отправителе, об узле-приемнике, и, часто динамически меняющейся информацией о транзитных узлах.

---

[1] **Метка потока** — уникальное число, одинаковое для однородного потока данных

I.1.6. Мультиплексирование и демультиплексирование

Чтобы выполнить переброску порции данных на коммутаторе по выбранному маршруту, коммутатор должен «знать», к какому потоку принадлежат данные и на какой порт их передать (Рис.5).

Рис.5. Коммутатор (swith)

А так как в сетях одновременно существует множество потоков, возникли проблемы мультиплексирования и демультиплексирования.

Мультиплексирование[1] – процесс образования из нескольких потоков одного общего потока.

Демультиплексирование – процесс образования из одного общего (агрегированного) потока нескольких отдельных потоков. То есть процесс, обратный мультиплексированию.

Пусть имеется сеть следующего вида (Рис.6): Компьютеры ПК1 и ПК2 подключены к коммутатору К1, коммутатор К1 подключен к коммутатору К2, к коммутатору К2 подключены компьютеры ПК3 и ПК4.

[1] **Мультиплекси́рование** (англ. *multiplexing, muxing*) — уплотнение канала, т. е. передача нескольких потоков (каналов) данных с меньшей скоростью (пропускной способностью) по одному каналу, при помощи устройства под названием мультиплексор.

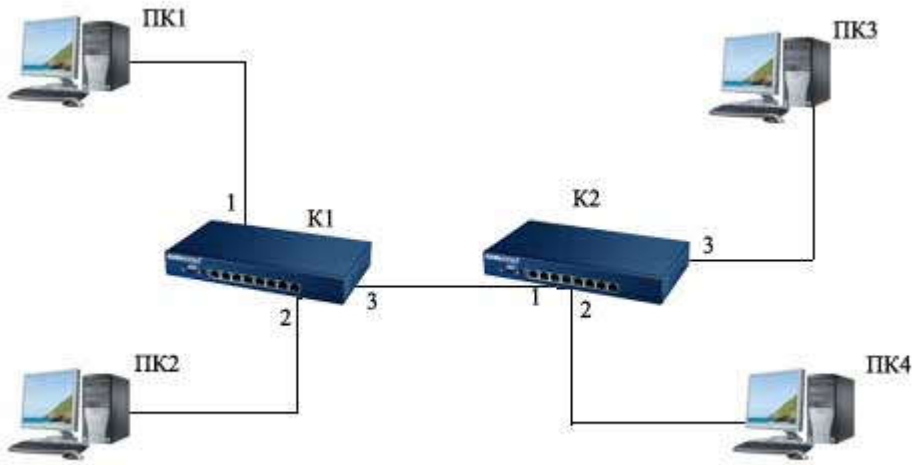


Рис.6. Задача мультиплексирования

Пусть имеется два потока: ПК1-ПК4 и ПК2-ПК3. Маршрут первого потока будет: ПК1-К1-К2-ПК4; маршрут второго потока: ПК2-К1-К2-ПК3. Как можно видеть, у обоих маршрутов есть общая часть К1-К2. Рассмотрим маршруты с учетом портов:

Первый: ПК1 – К1(1) – К1(3) – К2(1) – К2(2) – ПК4

Второй: ПК2 – К1(2) – К1(3) – К2(1) – К2(3) – ПК3

Как можно видеть, общим отрезком двух маршрутов будет соединение третьего порта коммутатора К1 и первого порта коммутатора К2. Именно на этом участке и будет передаваться мультиплексированный информационный поток, который, затем, на коммутаторе К2 будет демультиплексирован на два потока.

I.1.7. Подходы к выполнению коммутации

В различных случаях для связи абонентов (или компьютеров в сети) используются различные подходы к выполнению коммутации. Понятно, что такие подходы будут различны между коммутацией мобильных телефонов или коммутацией компьютеров в игровом клубе. Рассмотрим два основополагающих подхода:

- коммутация каналов (circuit switching);
- коммутация пакетов (packet switching).

Как видно из названий, при коммутации каналов, при установке соединения между конечными узлами, создается канал связи на весь сеанс связи. Такой коммутацией удобно пользоваться, например, для абонентов стационарных телефонов.

Достоинства коммутации каналов:

1. Постоянная и известная скорость передачи данных по установленному между конечными узлами каналу.

2. Низкий и постоянный уровень задержки передачи данных через сеть.

Недостатки коммутации каналов:

1. Отказ сети в обслуживании запроса на установление соединения, например, из-за того, что абонент занят.

2. Нерациональное использование пропускной способности физических каналов. Та часть пропускной способности, которая отводится составному каналу после установления соединения, предоставляется ему на все время, т.е. до тех пор, пока соединение не будет разорвано.

3. Обязательная задержка перед передачей данных из-за фазы установления соединения.

Коммутация пакетов была разработана специально для эффективного компьютерного трафика. При коммутации пакетов все передаваемые сообщения делятся на специальные порции – пакеты данных. Каждый пакет состоит не только из информации сообщения. В нем есть так же служебная информация, по которой данные маршрутизируются и собираются в сообщения. Пакеты транспортируются по сети как независимые информационные блоки. Коммутаторы передают такие пакеты друг другу, пока они не достигнут узла-получателя.

Достоинства коммутации пакетов:

1. Высокая общая пропускная способность сети при передаче пульсирующего трафика.

2. Возможность динамически перераспределять пропускную способность физических каналов связи между абонентами в соответствии с реальными потребностями их трафика.

Недостатки коммутации пакетов

1. Неопределенность скорости передачи данных между абонентами сети, обусловленная тем, что задержки в очередях буферов коммутаторов сети зависят от общей загрузки сети.

2. Переменная величина задержки пакетов данных, которая может быть достаточно продолжительной в моменты мгновенных перегрузок сети.

3. Возможные потери данных из-за переполнения буферов.

На основе подхода коммутации пакетов была разработана технология коммутации сообщений. Под коммутацией сообщений понимается передача единого блока данных между транзитными компьютерами сети с временной буферизацией этого блока на диске каждого компьютера. Сообщение в отличие от пакета имеет произвольную длину, которая определяется не технологическими соображениями, а содержанием информации, составляющей сообщение.

Вопросы для самоконтроля

1. Что такое коммутация?
2. Как можно представить задачу коммутации?
3. Что такое информационный поток?
4. Какие значения могут иметь признаки потока и для чего они?
5. Что значит определить поток?
6. Что такое трафик?
7. Как определить маршрут для потока?
8. Что такое мультиплексирование и демультиплексирование?
9. Расскажите достоинства и недостатки основополагающих принципов коммутации
10. Что такое коммутация сообщений?

I.2. Изучение стандартов, моделей и протоколов компьютерных сетей

Если вдруг обучающийся освоил основную терминологию и получил верное представление об основах компьютерных сетей, можно перейти к изучению их построения и соответствующих правил.

I.2.1. Структуризация сетей, топологии и сетевые модели

В малых сетях на сегодняшний день чаще всего используется структура, когда компьютеры сети подключены к концентратору или коммутатору. Такие устройства могут быть свои в каждом помещении, и все они могут подключаться к корневому (центральному) коммутатору. Такая ситуация сложилась со временем, и такая структура совсем не обязательна.

Мы уже рассматривали случаи связи компьютер-принтер и компьютер-компьютер-принтер. Но как только компьютеров или любых других узлов становится больше двух, возникают различные варианты их соединения. Можно подключать их последовательно один за другим, можно подключать их, используя центральное устройство и т.п. Структура, образованная линиями

связи, называется топологией[1]. Топология может быть физической, и описывать, соответственно, структуру физических линий связи; может быть логической – описывать прохождение сигнала в рамках физической топологии; информационной – описывать направление передачи информации; и управления обменом – описывать принцип передачи права на управление сетью.

Существует множество способов соединения сетевых устройств, из них можно выделить пять базовых топологий: шина, кольцо, звезда, ячеистая топология и решётка. Остальные способы являются комбинациями базовых. В общем случае такие топологии называются смешанными или гибридными, но некоторые из них имеют собственные названия, например «Дерево». И еще в различной литературе по компьютерным сетям упоминают полносвязанную топологию (когда каждый узел сети соединен с каждым другим) и неполносвязанную.

Рассмотрим основные базовые топологии. Топология «шина».

На рисунке 7 представлена топология «шина» или «общая шина». Такая топология характерна тем, что имеется один общий физический канал передачи данных, к которому подключены все компьютеры сети.

Рис.7. Топология «шина»

На концах шины при такой топологии должны быть специальные устройства, называемые терминаторами, как правило, служащие для установления нужных режимов волны в кабеле.

---

[1] **Сетевая тополо́гия** (от греч. τόπος, - место) — способ описания конфигурации сети, схема расположения и соединения сетевых устройств.

Можно заметить, что если при такой топологии повредится физическая линия связи или хотя бы один из терминаторов, вся сеть перестанет функционировать.

Топология «кольцо»

На рисунке 8 представлена топология «кольцо». Такая топология характерна тем, что все узлы такой сети подключены последовательно в кольцо.

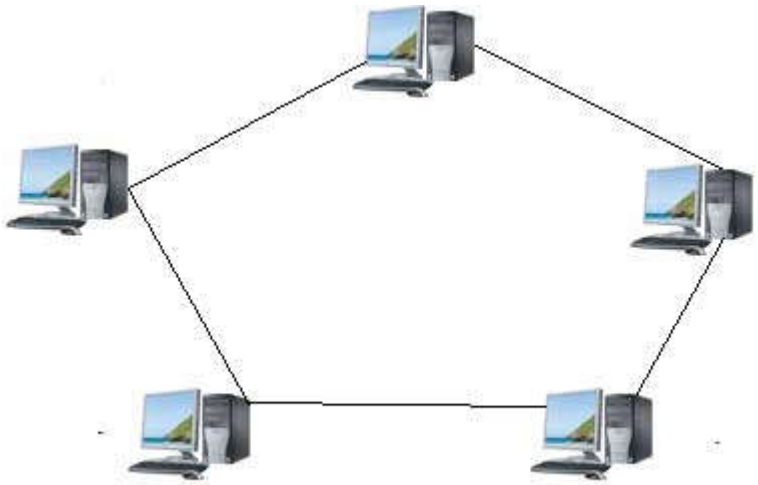


Рис.8. Топология «кольцо»

Многие литературные источники называют топологию «кольцо» вариацией топологии «шина», при которой оконечные устройства соединены.

При такой топологии есть вероятность, что при повреждении какого-либо узла или физической линии связи, сеть может остаться функционирующей. Но при больших повреждениях вся сеть выйдет из строя.

Топология «звезда»

На рисунке 9 представлена топология «звезда». Такая топология характерна тем, что все узлы такой сети подключены к одному центральному устройству.

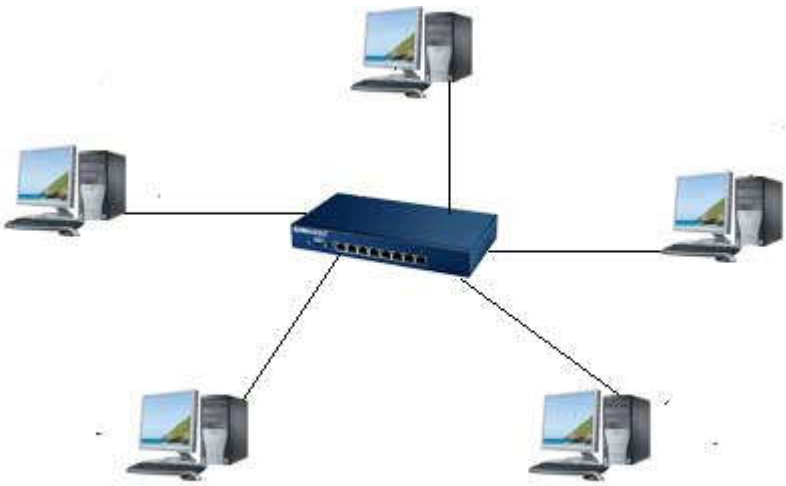


Рис.9. Топология «звезда»

Именно такую основу и используют сегодня для построения сетей. Такие сети обладают повышенной отказоустойчивостью, т.к. при выходе из строя любого узла или физической линии связи, из строя выйдет лишь один соответствующий сегмент. Вся остальная сеть будет продолжать функционировать, как ни в чем не бывало. Лишь вывод из строя центрального устройства может повредить сети.

Другие топологии, по сути, являются смешенными звездой и шиной.

I.2.2. Сетевые модели

Распространение компьютерных технологий привело к распространению компьютерных сетей. Локальные сети стали появляться в каждом учреждении и организации. Каждая такая локальная сеть подобна островку в океане, не имеющему связи с другими подомными островами. Решить проблему передачи информации между локальными сетями помогли глобальные сети.

В течение развития IT и компьютерных сетей весь мир убедился в эффективности использования таких технологий и экономии средств, повышении производительности труда. Новые технологии почти сразу же внедрялись, что привело к появлению совершенно различных аппаратных и программных средств. Это привело к тому, что многие сети оказались несовместимы и стало сложно организовать не то что совместную работу, а

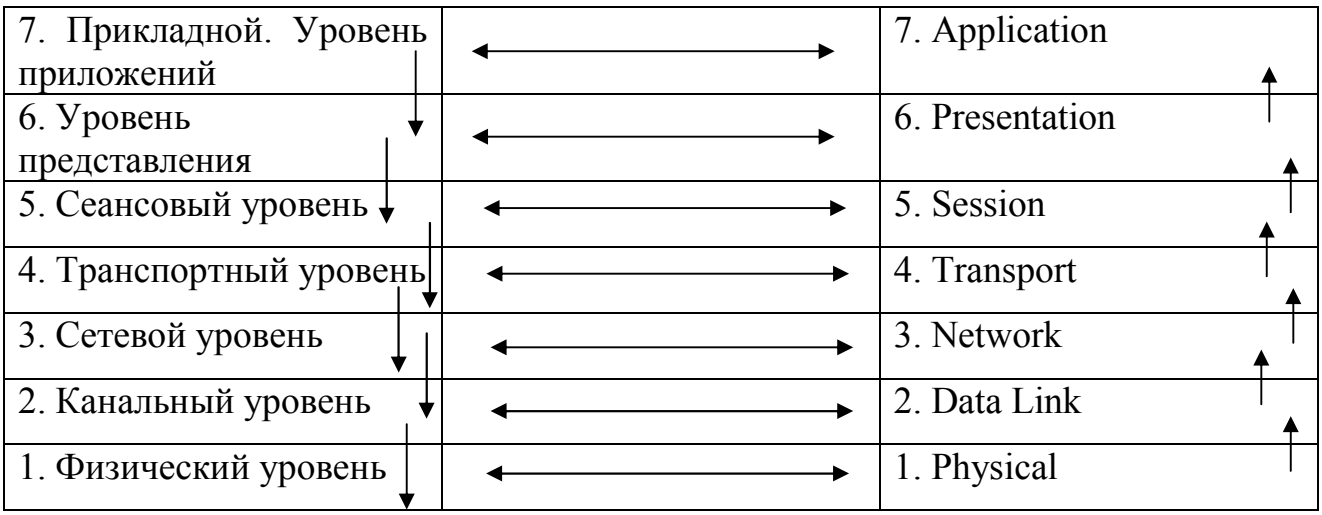
даже простой обмен информацией между компьютерами, использующими различные сетевые спецификации.

Для решения проблемы совместимости разрабатывались различные модели сетевого взаимодействия, но эталонной стала модель, разработанная международной организацией по стандартизации (ISO). В 1984 ISO выпустила в свет эталонную модель взаимодействия открытых систем OSI (Open System Interconnection). Эта модель стала основой архитектуры открытого сетевого взаимодействия. Это значит, что теперь производители сетевых технологий могут разрабатывать технологии, совместимые со всеми сетевыми технологиями, разработанными на основе OSI. Теперь поставщики сетевых технологий, желая показать пользователю, что все будет работать и будет совместимо с другими технологиями, ссылаются на их совместимость с моделью OSI.

Эталонная модель OSI – это описательная модель, то есть она описывает сетевое взаимодействие и ее стандарты гарантируют высокую совместимость и способность к взаимодействию различных типов сетевых технологий. Кроме того она иллюстрирует процесс передачи информации по сетям. Модель оси описывает весь путь информации через информационную среду. По мере продвижения информации от уровня пользователя (например, когда люди общаются посредством какой-либо сетевой программы) информация превращается в вид логических единиц и нулей и, в конце концов, в электрические или радио или оптические сигналы. Эталонная модель OSI делит всю задачу продвижения информации на семь менее крупных, а значит более легко решаемых задач. Каждая задача относительно автономна и возможны отдельные решения для каждой такой задачи. Такое разделение на уровни называется иерархическим представлением. Уровни модели OSI можно представить в виде таблицы:

Таблица 1. Модель OSI

Уровень (рус)	Взаимодействие	Уровень (en)



Три нижних уровня (физический, канальный и сетевой) управляют физической доставкой сообщений сети и вместе называются уровнями среды передачи данных (media layers). Четыре верхних уровня (прикладной, представлений, сеансовый и транспортный) обеспечивают точную доставку данных и называются уровнями хост-машины (host-layers).

Модель OSI не является схемой реализации, поэтому в некоторых источниках есть информация, что модель OSI не может быть реализована. Это не совсем так. Модель только определяет функции каждого уровня.

Уровни модели OSI

Рассмотрим уровни модели OSI сверху вниз.

Уровень 7. Прикладной

Уровень приложений. На этом уровне работают программы. Он не предоставляет никаких услуг другим уровням и служит только прикладным процессам, лежащим вне модели OSI. То есть, если, например, пользователь общается через какой-либо Internet-пейджер, эту программу обслуживает седьмой уровень модели OSI. Он идентифицирует и устанавливает доступность предполагаемых партнеров для связи, синхронизирует совместно работающие приложения, устанавливает договоренность о процессах восстановления после ошибок и контроля целостности данных; так же определяет достаток ресурсов для установления связи.

Уровень 6. Представлений

Этот уровень отвечает за то, чтобы информация, поступающая из какого-либо приложения была читаема и понятна для уровня приложений (7) любой другой системы. При необходимости можно использовать преобразования форматов данных.

Уровень 5. Сеансовый

Этот уровень управляет сеансами – устанавливает, завершает, контролирует сеансы взаимодействия приложений. Так же предоставляет средства для синхронизации участвующих в диалоге сторон, обеспечивает класс услуг и средства формирования отчетов об особых ситуациях на сеансовом уровне(5), а так же на уровне приложений(7) и представлений(6).

Уровень 4. Транспортный

Делит и повторно собирает данные в один поток. На этом уровне часто происходят процессы мультиплексирования и демультиплексирования. Этот уровень решает задачи о транспортировки данных, избавляя от этого другие хост-уровни.

Уровень 3. Сетевой

Это комплексный уровень, обеспечивающий соединение и выбор маршрута между двумя оконечными системами. На этом уровне часто реализовывается маршрутизация.

Уровень 2. Канальный

Обеспечивает надежный транзит данных через физический канал связи. Решает вопросы физической адресации, топологии сети, уведомления об ошибках, задержках, управления потоками данных.

Уровень 1. Физический

Определяет электротехнические, механические, процедурные и функциональные характеристики физического канала между оконечными узлами. Это кабельные системы, радиоволны, передающая среда. Спецификации физического уровня определяют такие характеристики, как уровни напряжения, скорость физической передачи данных, максимальные расстояния сегментов, физические разъемы и т.п.

I.2.3. Сетевая модель DARPA

Модель DARPA (сокращение от Defense Advanced Research Projects Agency - организация, в которой в свое время разрабатывались сетевые проекты, в том числе протокол TCP/IP, и которая стояла у истоков сети Интернет) – она же модель Министерства обороны США (модель DoD, Department of Defense, проект DARPA работал по заказу этого ведомства), является моделью TCP/IP и была разработана еще до разработки модели OSI.

Модель состоит из четырех уровней:

1. прикладной уровень;

2. транспортный уровень;

3. уровень межсетевого взаимодействия;

4. уровень сетевого интерфейса

Между моделью DARPA и моделью OSI можно выявить приблизительное соответствие уровней:

Уровни DARPA	**Уровни OSI**
1. Прикладной	7. Прикладной
	6. Представления
	5. Сеансовый
2. Транспортный	4. Транспортный
3. Уровень межсетевого взаимодействия	3. Сетевой
4. Уровень сетевого интерфейса	2. Канальный
	1. Физический

Формальные правила, определяющие последовательность и формат сообщений на одном уровне, называются протоколами. Иерархически организованная совокупность протоколов называется стеком коммуникационных протоколов.

На прикладном уровне модели DARPA функционируют такие сетевые протоколы, как WWW, FTP, TFTP, SNMP, Telnet, SMTP DNS, DHCP, WINS.

На транспортном - TCP, UDP.

На уровне межсетевого взаимодействия - ARP, IP, ICMP, RIP, OSPF.

Уровень сетевого интерфейса в модели DARPA не регламентируется спецификациями стека TCP/IP (Ethernet, Token Ring, FDDI, ATM, X.25, Frame Relay, SLIP, PPP).

Вопросы для самоконтроля:

1. Что такое топология сети?
2. Какие топологии бывают?
3. Что такое топология «шина»?
4. Что такое топология «звезда»?
5. Какие топологии можно назвать полносвязанными?
6. Какие топологии можно назвать неполносвязанными?
7. К чему привело быстрое внедрение новых технологий?
8. Если Вам предложат перевести свой бизнес на более быстродействующую, более дешевую новую технологию со своими специфическими сетевыми спецификациями, Вы согласитесь?
9. В каком году была разработана эталонная сетевая модель?
10. На сколько задач поделено сетевое взаимодействие по OSI?
11. Что такое иерархическое представление?
12. Как называются вместе три нижних уровня OSI?
13. Как называются вместе четыре верхних уровня OSI?
14. Опишите уровни модели OSI
15. Опишите задачу отправки и приема сообщения через Internet посредством ICQ, используя уровни модели OSI
16. Расскажите про модель DARPA

I.2.4. Стандартизация сетей и сетевые протоколы

Как следует из названия модели OSI (Open System Interconnection), она описывает взаимодействие **открытых систем**. Под открытой системой следует понимать систему, построенную в соответствии с открытыми принципами и

спецификациями[1]. Под открытыми спецификациями понимаются опубликованные, общедоступные спецификации, соответствующие стандартам и принятые в результате достижения согласия после всестороннего обсуждения всеми заинтересованными сторонами. Использование открытых спецификаций позволяет разработчикам сетевых технологий производить совместимое оборудование, создавать программное или аппаратное обеспечение, которое будет работать в общей открытой системе.

Поэтому для реальных систем полная открытость является недостижимым идеалом. Фактически, даже в системах, называемых открытыми, реально открыта лишь часть системы. Обусловлено это, в том числе, и с точки зрения безопасности. Поэтому у открытых систем реально открыта лишь часть, отвечающая за общение с уровнями модели OSI.

Но если две системы построены в соответствии с принципами открытости, это дает явные преимущества:

– возможность построения сети из аппаратных и программных средств различных производителей, придерживающихся одного и того же стандарта;

– возможность безболезненной замены одних компонентов сети другими, что позволяет сети развиваться с минимальными затратами;

– возможность легкого сопряжения одной сети с другой;

– простота освоения и обслуживания сети.

Для поддержания открытых систем стали разрабатывать сетевые стандарты. Разрабатывать технологии, опираясь на стандарты, гораздо легче, чем с нуля пытаться разработать технологию, отвечающую принципам открытых систем.

---

[1] **Специфика́ция** — (от англ. *Specification*) инженерный термин, обозначающий набор требований и параметров, которым удовлетворяет некоторая сущность.

В итоге открытость стандартов и спецификаций важна не только для сетевых протоколов[1], но и для всевозможных устройств, программ, и других программно-аппаратных частей систем.

Стоит отметить, что не стоит бояться слова протокол. Протокол в IT – это общая договоренность, по которой будет разрабатываться и реализовываться технология. Существует множество сетевых протоколов. Рассмотрим основные на сегодняшний день сетевые протоколы.

I.2.5. Основные сетевые протоколы

Основная база современных компьютерных сетей строится на стеке протоколов TCP/IP, но во многих сетях продолжают функционировать и другие протоколы, например, NetBEUI, IPX/SPX, и т.п.

Протокол NetBEUI (NetBIOS Extended User Interface) произошел от сетевого программного интерфейса NetBIOS (Network Basic Input/Output System), который был сетевым расширением стандартных функций базовой системы ввода/вывода (BIOS) IBM PC для сетевой программы PC Network фирмы IBM.

Протокол NetBEUI разрабатывался как эффективный протокол, потребляющий немного ресурсов, для использования в сетях, насчитывающих не более 200 рабочих станций. Этот протокол содержит много полезных сетевых функций, которые можно отнести к сетевому, транспортному и сеансовому уровням модели OSI, однако с его помощью невозможна маршрутизация пакетов. Это ограничивает применение протокола NetBEUI локальными сетями, не разделенными на подсети, и делает невозможным его использование в составных сетях. Некоторые ограничения NetBEUI снимаются реализацией этого протокола NBF (NetBEUI Frame), которая была включена в операционную систему Microsoft Windows NT.

---

[1] **Протоко́л** (от др.греч. protos — «первый» и kolla — «клей») — первый лист, приклеенный к свитку. На нем фиксировались титульная информация (например, дата написания, имя писца) и краткое основное содержание свитка (изображение).

Современные ОС Windows данный протокол уже практически не используется, в системах Windows XP/2003/Vista/7 отсутствует даже возможность добавления данного протокола в Свойствах сетевого подключения системы (хотя, если необходима совместимость с какими-либо приложениями, унаследованными от старых систем и работающих только по протоколу NetBEUI, в дистрибутивах систем Windows XP/2003/Vista/7 имеются установочные файлы для добавления данного протокола).

Стек протоколов IPX/SPX является оригинальным стеком протоколов фирмы Novell, разработанным для сетевой операционной системы NetWare еще в начале 80-х годов. Протоколы сетевого и сеансового уровня Internetwork Packet Exchange (IPX) и Sequenced Packet Exchange (SPX), которые дали название стеку, являются прямой адаптацией протоколов XNS фирмы Xerox, распространенных в гораздо меньшей степени, чем стек IPX/SPX. Популярность стека IPX/SPX непосредственно связана с операционной системой Novell NetWare, но, начиная с версии 5.0 фирма Novell в качестве основного протокола своей серверной операционной системы стала использовать протокол TCP/IP, и с тех пор практическое применение IPX/SPX стало неуклонно снижаться.

Служба DHCP (Dynamic Host Configuration Protocol) — одна из служб поддержки протокола TCP/IP, разработанная для упрощения администрирования IP-сети за счет использования специально настроенного сервера для централизованного управления IP-адресами и другими параметрами протокола TCP/IP, необходимыми сетевым узлам.

Наиболее известные протоколы, используемые в сети Интернет:

– HTTP (Hyper Text Transfer Protocol) – это протокол передачи гипертекста. Протокол HTTP используется при пересылке Web-страниц с одного компьютера на другой.

– FTP (File Transfer Protocol)- это протокол передачи файлов со специального файлового сервера на компьютер пользователя. FTP дает возможность абоненту обмениваться двоичными и текстовыми файлами с

любым компьютером сети. Установив связь с удаленным компьютером, пользователь может скопировать файл с удаленного компьютера на свой или скопировать файл со своего компьютера на удаленный.

– POP (Post Office Protocol) – это стандартный протокол почтового соединения. Серверы POP обрабатывают входящую почту, а протокол POP предназначен для обработки запросов на получение почты от клиентских почтовых программ.

– SMTP (Simple Mail Transfer Protocol) – протокол, который задает набор правил для передачи почты. Сервер SMTP возвращает либо подтверждение о приеме, либо сообщение об ошибке, либо запрашивает дополнительную информацию.

– UUCP (Unix to Unix Copy Protocol) – это ныне устаревший, но все еще применяемый протокол передачи данных, в том числе для электронной почты. Этот протокол предполагает использование пакетного способа передачи информации, при котором сначала устанавливается соединение клиент-сервер и передается пакет данных, а затем автономно происходит его обработка, просмотр или подготовка писем.

– TELNET – это протокол удаленного доступа. TELNET дает возможность абоненту работать на любой ЭВМ сети Интернет, как на своей собственной, то есть запускать программы, менять режим работы и т. д. На практике возможности лимитируются тем уровнем доступа, который задан администратором удаленной машины.

– DTN – протокол дальней космической связи, предназначенный для обеспечения сверхдальней космической связи.

I.2.6. Сетевая адресация

Сетевой адрес — уникальный числовой идентификатор устройства, работающего в компьютерной сети.

В локальных сетях, не имеющих сложной иерархии, все партнёры доступны друг другу и достаточно сетевого адреса в виде одного числа.

В сетях, связанных в глобальную сеть Internet, возникает проблема идентификации неопределённого и постоянно растущего числа участников. При этом используются два вида адресов:

– MAC-адрес, состоящий из двух частей, первая определяет производителя оборудования, а вторая уникальный номер, присваиваемый производителем оборудованию, обеспечивает уникальный адрес любого устройства в сети.

– IP-адрес, состоит из двух частей, первая – адрес подсети, вторая – адрес устройства в пределах подсети.

Альтернативой адресу являются идентификаторы устройств в форме символических имён, удобных для запоминания. Например, в пределах локальной сети — это сетевое имя компьютера, в глобальной сети — доменное имя. Специальные сетевые протоколы (DNS, WINS и т.п.) обеспечивают автоматическое определение соответствия между именами и адресами.

Упрощенная схема сети Internet

Интернет – это глобальная сеть, которая:

– логически связана единым адресным пространством;

– может поддерживать соединения с коммутацией пакетов на основе семейства специализированных протоколов;

– предоставляет услуги высокого уровня.

Что это значит? Во-первых, связанность единым адресным пространством можно сравнить с обычной почтой. Чтобы написать обычное письмо, его кладут в конверт, на котором пишут адрес получателя и адрес отправителя, состоящие из индекса, города (иногда и страны), улицы, номера дома, квартиры.

Примерно по такому же типу реализовано адресное пространство Интернет. И реализовано оно с помощью протокола IP1. IP реализован согласно стандарта RFC 791 в сентябре 1981г. Используется для негарантированной

доставки данных, разделяемых на так называемые пакеты от одного узла сети к другому.

Это означает, что на уровне этого протокола (третий уровень сетевой модели OSI) не даётся гарантий надёжной доставки пакета до адресата. В частности, пакеты могут прийти не в том порядке, в котором были отправлены, продублироваться (когда приходят две копии одного пакета; в реальности это бывает крайне редко), оказаться повреждёнными (обычно повреждённые пакеты уничтожаются) или не прибыть вовсе. Гарантии безошибочной доставки пакетов дают протоколы более высокого (транспортного) уровня сетевой модели OSI — например, TCP[2] — которые IP используют в качестве транспорта.

В современной сети Интернет используется IP четвёртой версии, также известный как IPv4. В протоколе IP этой версии каждому узлу сети ставится в соответствие IP-адрес длиной 4 октета (иногда говорят «байта», подразумевая распространённый восьмибитовый минимальный адресуемый фрагмент памяти ЭВМ; название «октет» идёт с тех времён, когда байты на разных компьютерах содержали разное число битов). При этом компьютеры в подсетях объединяются общими начальными битами адреса. Количество этих бит, общее для данной подсети, называется маской подсети (ранее использовалось деление пространства адресов по классам — A, B, C; класс сети определялся диапазоном значений старшего октета и определял число адресуемых узлов в данной сети, сейчас используется бесклассовая адресация).

В настоящее время вводится в эксплуатацию шестая версия протокола — IPv6, которая позволяет адресовать значительно большее количество узлов, чем IPv4. Эта версия отличается повышенной разрядностью адреса, встроенной возможностью шифрования и некоторыми другими особенностями. Переход с IPv4 на IPv6 связан с трудоёмкой работой

[1] **IP** (англ. Internet Protocol — межсетевой протокол) — маршрутизируемый сетевой протокол, основа стека протоколов TCP/IP.

[2] **Transmission Control Protocol (TCP)** (протокол управления передачей) — один из основных сетевых протоколов Интернет, предназначенный для управления передачей данных в сетях и подсетях TCP/IP.

операторов связи и производителей программного обеспечения и не может быть выполнен одномоментно.

На начало 2007г в Интернете присутствовало около 760 сетей, работающих по протоколу IPv6. Для сравнения, на то же время в адресном пространстве IPv4 присутствовало более 203 тысяч сетей, но в IPv6 сети гораздо более крупные, нежели в IPv4.

Таким образом, стек протоколов[1] TCP/IP является на сегодняшний день одним из основных стеков.

I.2.7. IP-адресация и маски подсетей

Каждый компьютер в сети на основе стека протоколов TCP/IP, имеет уникальный числовой адрес, называемый IP-адресом, который позволяет адресовать пакеты данных определенному получателю.

IP-адрес состоит из четырех так называемых октетов, отделенных точками. Октет – двоичное число из восьми цифр, равное десятичным цифрам от 0 до 255. Чтобы сделать IP-адреса более простыми в чтении и написании, они часто выражаются как четыре десятичных числа, отделенных точкой (Рис.10). Этот формат называется «точечно-десятичным представлением».

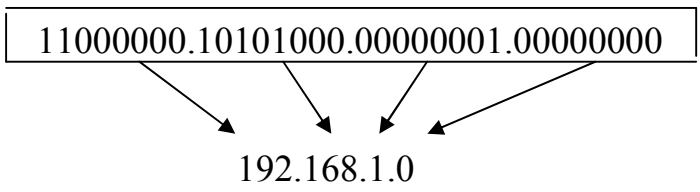


Рис.10. Адрес IP в его десятичном и двоично-точечном представлении

В локальной сети, основанной на TCP/IP, IP-адрес должен быть присвоен каждому узлу (компьютеру или устройству) в сети. IP-адрес должен быть уникален для каждого узла.

[1] **Стек протоколов** — набор взаимодействующих сетевых протоколов.

Устройство, которое служит маршрутизатором, содержит два или более сетевых адаптера, и может принадлежать двум или более сетям. В этом случае каждому адаптеру должен быть назначен уникальный IP-адрес для каждой сети.

Адрес состоит из двух логических частей – номера сети (network number) и номера узла в сети (host number).

Все узлы в одной сети используют одинаковый сетевой номер, но уникальный номер узла. Например, IP-адрес 192.168.0.10 может говорить (при определенных условиях, рассмотренных далее), что в сети 192.168.0 узел имеет адрес 10.

I.2.8. Классы IP-адресов

Расчет отделения сетевой части адреса узла от номера самого узла в сети – процесс не столь однозначный, и было несколько способов. Классовый способ, при котором определенные наборы 0 и 1 классифицировались отдельно, и способ битовой маски. Рассмотрим подробнее.

Чтобы обеспечивать гибкость, требуемую для поддержки сети разного размера, IP-адреса бывают трех классов: A, B и C (Рис.11). Каждый класс устанавливает границу между сетевой частью и узловой частью IP-адреса различными способами. Это позволяет приспособить их для сетей различного размера.

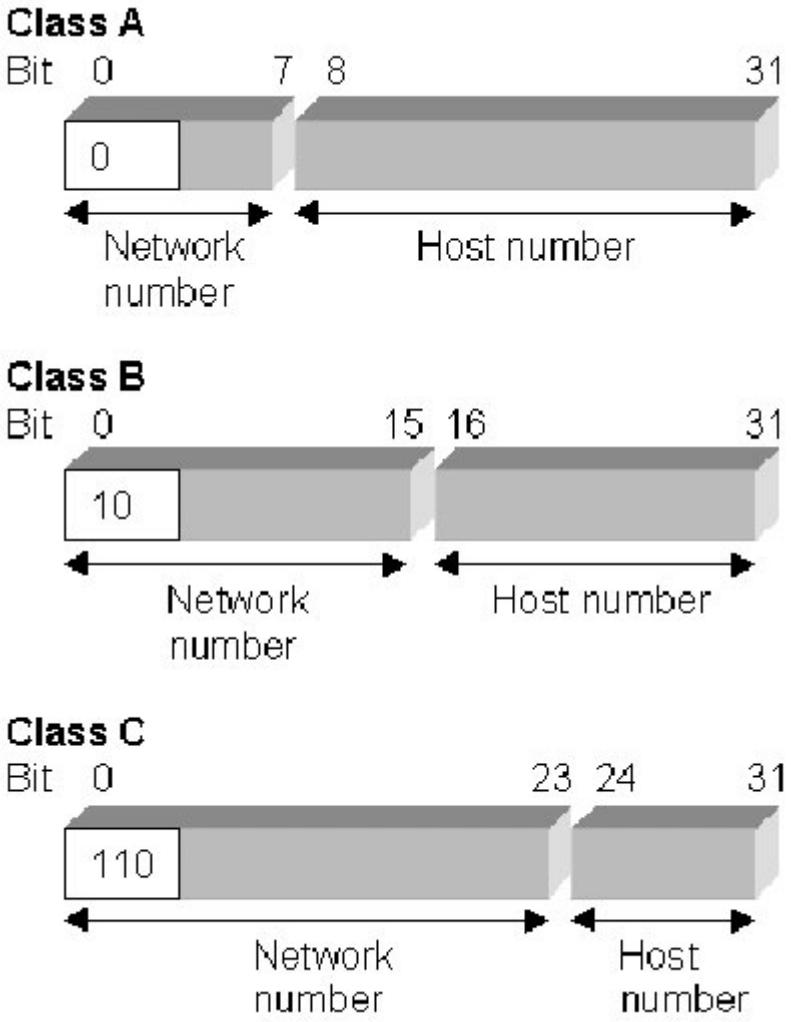


Рис.11. Классы IP-адресов

– Если адрес сети начинается с 0, то есть относится к классу А, и номер сети занимает 1 байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126. (0 не используется, а 127 зарезервирован для специальных целей). В сетях класса А количество узлов не должно превышать 224 (Рис.12).

– Если первые два бита адреса равны 10, то есть относятся к классу В, сеть является средних размеров с числом узлов 28 – 216. В сетях класса В под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта (Рис.12).

– Если адрес начинается с последовательности 110, то это сеть класса С с числом узлов не больше 28. Под адрес сети отводится 24 бита, а под адрес узла – 8битов (Рис.12).

– Кроме основных классов IP-адресов выделяются еще 2 дополнительных:

– Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес – multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес (Рис.12).

– Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений (Рис.12).

В таблице приведены диапазоны номеров сетей, соответствующих каждому классу сетей.

Класс	Наименьший адрес	Наибольший адрес
A	1.0.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0.	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Рис.12. Классы A-E

I.2.9. Глобальные и локальные сетевые IP-адреса

Есть два типа IP-адресов – те, которые являются глобально маршрутизированными (включенными в таблицы маршрутизации в Internrt), и те, которые были зарезервированы для локальных сетей. Система маршрутизируемых IP-адресов была представлена для предотвращения будущей нехватки IP-адресов из-за быстрого роста Internet. Поскольку локальные адреса не находятся в системе маршрутизации Internet, те же самые числа могут использоваться одновременно многими организациями.

Три вида IP-адресов, которые были сохранены для локальных сетей:

10.0.0.0 – 10.255.255.255 (24bit block/Class A)

172.16.0.0 – 172.31.255.255 (20bit block/Class B)

192.168.0.0 – 192.168.255.255 (16bit block/Class C)

Локальные компьютеры не могут связываться непосредственно с Internet. Для получения доступа необходимо наличие «посредника», который выступает в роли шлюза Internet. Он должен иметь глобальный

маршрутизированный IP-адрес, который используется при связи с Internet, и локальный сетевой IP-адрес, который используется для связи с локальными компьютерами. Такие организации называются провайдерами. Когда локальная сеть подключается к сети Интернет, она вся для Интернет имеет свой уникальный IP-адрес.

I.2.10. Подсети

Деление сети на несколько подсетей (subnet) служит для достижения ряда целей: уменьшение сетевого трафика путем уменьшения числа пересылок, защиты локальных сетей. Подсети созданы с использованием, так называемой, маски подсети (subnet mask) для разделения отдельного класса на меньшие части. Подсети могут снова быть разделены на подсети. Подсеть создана с заимствованием битов от части IP-адреса, который обычно определяет узел (host number). Номер сети и номер подсети определяют расширенный сетевой префикс (extended network prefix)(Рис.13).

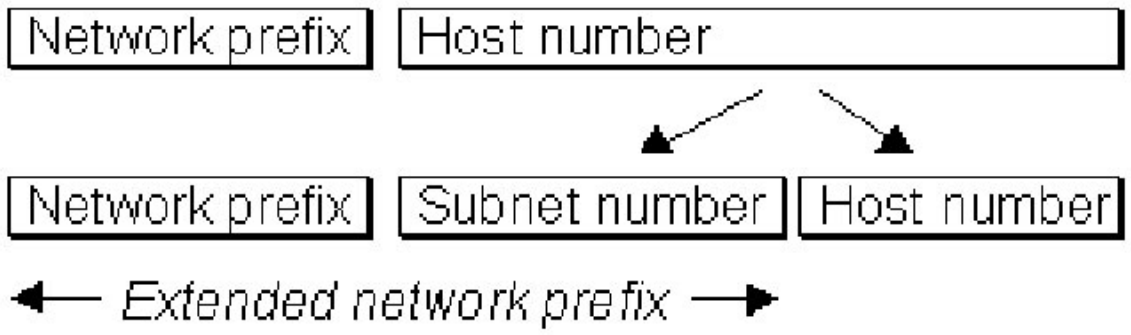


Рис.13. Деление на подсети

I.2.11. Маска подсети

Маска подсети состоит из 32 (8*4) битов и используется как ключ для декодирования, чтобы определить, как IP-адрес должен быть разделен на расширенный сетевой префикс и номер узла. Она используется маршрутизаторами и сетевыми устройствами, чтобы определить, куда должны направляться пакеты данных.

Подобно IP-адресам, маски состоят из четырех чисел по 8 бит, отделенных точками. Они обычно написаны в соответствующем десятичном представлении.

Типичные маски подсети, используемые для адресов класса A, B и C следующие:

Class A subnet mask:

Decimal	*Binary*
255.0.0.0	11111111.00000000.00000000.00000000

Class B subnet mask:

Decimal	*Binary*
255.255.0.0	11111111.11111111.00000000.00000000

Class C subnet mask:

Decimal	*Binary*
255.255.255.0	11111111.11111111.11111111.00000000

Все нули в маске определяют, что эта часть в соответствующем IP-адресе – является номером узла, в то время как единицы указывают, что соответствующие биты в IP-адресе составляют сетевую часть.

I.2.12. Вычисление адреса сети с использованием маски подсети

Номер сети - IP-адреса, который используется всеми компьютерами. Номер сети, или расширенный сетевой префикс IP-адреса, вычисляется с использованием подсетевой маски для того, чтобы отделить его от части IP-адреса, определяющей узел.

Пример:

Выбираем IP-адрес 192.168.1.1 и подсетевую маску 255.255.255.0. Вышеупомянутый IP-адрес и подсетевая маска, написанная в их двойном представлении выглядят следующим образом:

192.168.1.1	11000000.10101000.00000001.00000001	
		Network portion → till here
255.255.255.0	11111111.11111111.11111111.00000000	

Каждый бит в IP-адресе сравнивается с соответствующим битом в маске подсети: «1» в маске подсети указывает, что соответствующий бит в IP-адресе принадлежит сетевой части, в то время как «0» в маске иллюстрирует, что соответствующий бит в IP-адресе принадлежит части хоста.

Таким образом, в вышеупомянутом примере ведущая часть – это все биты в первых трех октетах, которые в десятичных числах записаны как 192.168.1.0.

I.2.13. Вычисление широковещательного адреса

Широковещательный адрес – адрес, в котором все биты в части установлены в 1. Он используется, когда необходимо послать данные на все компьютеры в сети.

В нашем примере последние 8 битов определяли компьютеры в сети. Широковещательный адрес для сети 192.168.1.0 с маской подсети 255.255.255.0 будет выглядеть следующим образом: 11000000.10101000.00000001.11111111 (ведущий набор битов к 1) или в десятичном виде: 192.168.1.255

Для удобства, префиксные представления длины (Classless Inter-Domain Routing представление, CIDR) часто используется вместо записи маски подсети. Это означает, что IP-адрес более чем 192.168.1.1 с маской 255.255.255.0 может быть также записан как 192.168.1.1/24, где «/24» указывает сетевую префиксную длину, которая является равной числу непрерывных битов единиц маски.

I.2.14. Вычисление маски подсети

Разбивая сеть, во-первых, необходимо определить:

– количество подсетей;

– количество адресов для каждой сети (необходимо всегда добавлять несколько дополнительных адресов с учетом возможного роста сети).

После определения этих параметров, следующий шаг – вычисление соответствующей маски, которая будет поддерживать сетевую структуру.

Пример: Выделить из сети 192.168.1.0/24 подсеть с рабочими станциями, серверами и другими устройствами – в сумме больше 80 единиц. Чтобы позволить некоторое расширение, необходимо установить число требуемых компьютеров – 90. Теперь можно начать вычисление маски.

Вычисление лучше производить с числами в двоичной форме. Также необходимо определить, какое адресное пространство остается свободным.

Первый шаг – определение самого низкого числа битов, требуемых, чтобы идентифицировать 90 компьютеров. Так как IP-адреса компьютеров могут быть созданы только по двоичным границам, число компьютеров должно быть вычислено по степеням двойки – $2(2^1)$, $4(2^2)$, $8(2^3)$, $16(2^4)$ и так далее. Другими словами, необходимо сначала определить, какая наименьшая степень, при возведении в которую числа 2, результат будет равен или больше 90. 26 – 64, 27 – 128. Значит нуждаемся в 7 битах, чтобы определить 90 компьютеров. То есть ведущая часть IP-адреса будет содержаться в последних 7 битах. IP-адрес в целом состоит из 32 битов. Сетевая часть, таким образом, должна состоять из 32-7=25 битов. Т.к. каждая «1» в маске указывает, что соответствующий бит в IP-адресе принадлежит сетевой части, и каждый «0» указывает, что соответствующий бит в IP-адресе принадлежит ведущей части, то соответствующая маска должна состоять из ряда 25ти единиц, сопровождаемых 7ю нулями. В десятичном представлении такая маска будет 255.255.255.128 (Рис.14).

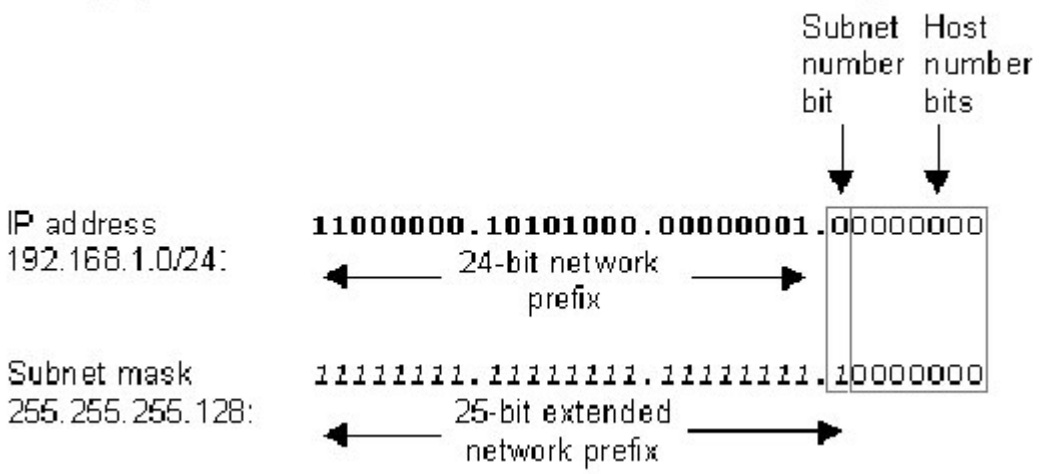


Рис.14. Вычисление маски подсети

Число подсетей, которые могут быть созданы, используя эту маску, рассчитано следующим образом: первый сетевой префикс был (192.168.1.0/24) в 24 бита длинной, и расширенный сетевой префикс (сетевой префикс +

подсетевой префикс), замаскированный маской длиной 25 бит. Один бит доступен, чтобы определять подсети. Другими словами, можно создать $2(2^1)$ подсети, использующих эту маску.

В таблице 2 приведен список масок подсетей.

Таблица 2. Список масок подсетей

Number of IP addresses	Subnet mask	Class
1	255.255.255.255	Class C subnet
2 (2^1)	255.255.255.254	
4 (2^2)	255.255.255.252	
8 (2^3)	255.255.255.248	
16 (2^4)	255.255.255.240	
32 (2^5)	255.255.255.224	
64 (2^6)	255.255.255.192	
128 (2^7)	255.255.255.128	
256 (2^8)	255.255.255.0	
512 (2×2^8)	255.255.254.0	Class B subnet
1024 (4×2^8)	255.255.252.0	
2048 (8×2^8)	255.255.248.0	
4096 (16×2^8)	255.255.240.0	
8192 (32×2^8)	255.255.224.0	
16384 (64×2^8)	255.255.192.0	
32768 (128×2^8)	255.255.128.0	
65536 (2^{16})	255.255.0.0	
131072($2^1\times2^{16}$)	255.254.0.0	Class A subnet
$2^2\times2^{16}$	255.252.0.0	
$2^3\times2^{16}$	255.248.0.0	
$2^4\times2^{16}$	255.240.0.0	
$2^5\times2^{16}$	255.224.0.0	
$2^6\times2^{16}$	255.192.0.0	
$2^7\times2^{16}$	255.128.0.0	
$2^8\times2^{16}$	255.0.0.0	

Вопросы для самоконтроля

1. Что означает открытая система?
2. Что такое спецификация?
3. Что такое открытые спецификации?
4. Какие преимущества дают принципы открытости?
5. Что такое сетевой протокол?
6. Какие сетевые протоколы Вы знаете?
7. Что значит единое адресное пространство?
8. Что такое IP?
9. Что такое TCP?
10. На каких версиях IP функционирует современная сеть Интернет?
11. Что означает фраза «Интернет может поддерживать соединения с коммутацией пакетов на основе семейства специализированных протоколов»?
12. Что означает фраза «Интернет предоставляет услуги высокого уровня»?
13. Что такое маска подсети?
14. Что такое точечно-десятичное представление?
15. Какие IP-адреса являются глобально маршрутизированными?
16. Какие существуют классы IP-адресов?
17. Что такое подсеть?
18. Каким образом вычисляется широковещательный адрес?
19. Что такое CIDR представление?

Практические задания

1. **Укажите классы следующих IP-адресов.**

Адрес	Класс
131.107.2.89	
3.3.57.1	
200.200.5.2	
191.107.2.10	
224.0.0.0	

2. **В сетях каких классах IP-адресов:**

менее 100 узлов	
более 1000 узлов	
менее 10000 узлов	
менее 100000 узлов	
более 1000000 узлов	

3. **Какие из адресов относятся к глобальным, а какие к локальным?**

192.169.1.3	
172.30.1.1	
10.0.0.1	
9.8.7.6	
220.254.254.1	

4. **Что из перечисленного является маской подсети для адреса 195.16.55.30/28?**

255.255.255.0
255.255.0.255
255.255.255.240
255.255.255.28
255.0.0.0

5. **Что из перечисленного является адресом сети для хоста 195.16.55.30/28?**

195.16.55.16
195.16.55.0
195.16.55.255
195.16.55.30
255.255.255.0

6. **Что из перечисленного является широковещательным адресом для сети 192.16.55.32 с маской 255.255.255.224?**

195.16.55.32
195.16.55.63
195.16.55.64
195.16.55.255
195.16.55.224

7. Выделить из сети 172.16.1.0/24 подсеть с рабочими станциями, серверами и другими устройствами, в сумме более чем N единиц. Чтобы позволить некоторое расширение – число требуемых компьютеров будет N+13.

Вариант 1	N=10
Вариант 2	N=35
Вариант 3	N=49
Вариант 4	N=114
Вариант 5	N=225

II. Сетевое оборудование

С одной стороны, для того, чтобы просто втыкать штекер провода в сетевой порт и даже обжать сетевой кабель, много знаний и не требуется – достаточно неоднократно проделать соответствующие однотипные действия для наработки опыта. С другой стороны – при любой проблеме или внештатной ситуации такой рабочий не будет знать, что делать, так как не понимает принципов функционирования и технологических аспектов технологий. Для верной работы с сетевым оборудованием все же необходимо изучить основы сетевых технологий и принципы сетевой адресации. Поэтому тем, кто не освоил предыдущие части, настоятельно рекомендуется разобраться с соответствующим материалом.

II.1. Изучение сетевого оборудования

Под сетевым оборудованием понимается комплекс технологий и устройств, предназначенных для функционирования компьютерных сетей.

К примеру, свободная Интернет-энциклопедия Википедия содержит следующее определение:

Def: Сетевое оборудование — устройства, необходимые для работы компьютерной сети, например: маршрутизатор, коммутатор, концентратор, патч-панель и др.

Таким образом, для успешной профессиональной деятельности обучающемуся необходимо разбираться в классификации сетевого оборудования, а так же постоянно следить за новшествами и актуальными решениями производителей.

II.1.1. Производители сетевого оборудования

Производить сетевое оборудование в современном мире – не простая задача. Уже говорилось о необходимости стандартизации сетей и о том, что сетевое оборудование одного производителя должно быть совместимым с сетевым оборудованием других производителей. К тому же необходимо, чтобы новое сетевое оборудование было быстрее, надежнее, может даже дешевле, чем

предыдущие варианты. Производители сетевого оборудования, соответственно, для достижения высоких целей производства, должны постоянно развивать технологии, предоставляя на рынок сетевых технологий все более и более лучшие решения. В такой ситуации специалисту-профессионалу по компьютерным сетям необходимо знать вендоров[1], необходимо разбираться в брендах[2].

В мире сетевых технологий, как и во всем мире IT, есть популярные бренды, наиболее качественные вендоры, и, так называемые no-name, то есть устройства (devices), у которых либо вообще нет подписи от фирмы-производителя, либо такая фирма не входит даже в десятку лучших и не известна специалисту.

Для специалистов-профессионалов в области компьютерных сетей на первом месте располагается бренд Cisco Systems. Компания основана учеными из Стэндфордского университета и является мировым лидером в области сетевых технологий. О них подробнее далее.

Сразу за Cisco Systems идет компания ZyXEL - Основными направлениями деятельности компании являются ADSL, Ethernet, VoIP, Wi-Fi и другие технологии. Штаб-квартира — в городе Синьчжу (Тайвань). Основана в 1989, в 1992 открыла представительство в России.

Название ZyXEL произносится «за́йксель»; в России распространены также чтения «зиксел», «зиксель», «зюксель», «зуксел», «зюхель», «зухель» и т. п. Как отмечают представители компании, им без разницы, как пользователи читают название – главное, что бренд известный и пользуется популярностью.

Прославилась своими dialup-модемами, широко использовавшимися в России. В настоящее время наибольшей популярностью пользуется DSL-оборудование компании, в частности ADSL-модемы и интернет-центры.

---

[1] **Вендор** — это компания-поставщик бренд-продуктов, сервисов и услуг, под чьей торговой маркой выпускается продукция

[2] **Бренд** (англ. *brand*, [brænd] — марка) — термин в маркетинге, символическое воплощение комплекса информации, связанного с определённым продуктом или услугой

Отличительной особенностью профессиональной техники ZyXEL является собственная масштабируемая сетевая операционная система ZyNOS (ZyXEL Network Operating System), которая с успехом сегодня применяется и в домашней Интернет-технике компании. Первая версия ZyNOS была выпущена в 1998 году, как конкурент успешной операционной системе Cisco IOS (Cisco Internetwork Operating System).

Cisco Systems и ZyXEL являются лучшими брендами в мире сетевых технологий. За ними идут 3Com, D-Link и другие. В Российских реалиях наибольшей популярностью обладает бренд D-Link, и, хотя эта компания и отстает в предложениях от ZyXEL и Cisco Systems, для Российских потребителей они зачастую выступают как наилучшее соотношение цены и качества.

Компании-лидеры в области сетевых технологий производят обучение специалистов, и каждый профессионал в области сетевых технологий может проходить курсы повышения квалификации. Так же, часто проводятся семинары-тренинги от вендоров во всех крупных городах[1] России. По окончанию подобных курсов выдаются дипломы и сертификаты.

Компания Cisco Systems – мировой лидер в области сетевых технологий и Интернет, меняющих способы человеческого общения, связи, сотрудничества. Сегодня сети стали важнейшим элементом бизнеса, образования, государственного управления и домашних коммуникаций. IP-решения Cisco можно с полным правом назвать фундаментальной основой этих сетей. Cisco Systems занимает прочное положение на IT-рынке – доля рынка, приходящаяся на маршрутизаторы Cisco, составляет 80%, а система CRS-I занесена в книгу рекордов Гиннеса как самый мощный в мире маршрутизатор.

Компания Cisco Systems была основана в 1984 году группой ученых-компьютерщиков из Стэндфордского университета. С самого начала инженеры

[1] В Волгограде чаще всего обучающие семинары проводятся в Академии АйТи, но, бывает, семинары проводятся и в различных арендуемых залах

Cisco Systems стали лидерами по разработке сетевых технологий, основанных на интернет-протоколе IP. Сегодня без малого 50 000 сотрудников компании, рассредоточенных по всему миру, продолжают традиции новаторства и разрабатывают лучшие в отрасли продукты и решения в базовых для Cisco областях (коммутация и маршрутизация), а также в сфере современных технологий, к которым относятся IP-коммутации, сетевая безопасность, беспроводные сети LAN, сети хранения (SAN), домашние сети, видеосистемы, прикладные сетевые услуги и пр.

Cisco Systems стала инициатором многих перемен в сфере технологий, и сегодня она продолжает эту традицию. Сейчас, когда отрасль высоких технологий вновь переживает период больших перемен, Cisco сохраняет лидерство в самых разных сегментах, таких как маршрутизация, коммутация, унифицированные коммуникации, беспроводная связь и безопасность, а так же системы хранения и обработки данных. Услуги и решения Cisco Systems используются для создания компьютерных сетей, позволяющих частным лицам, компаниям и даже целым странам повысить производительность труда, улучшить качество предоставляемых услуг, укрепить конкурентоспособность. Сознавая, что новаторство во многом определяет успех бизнеса, руководство Cisco Systems ежегодно расходует более $3 млрд на научно-исследовательскую деятельность (в том числе $300 млн – на исследования и разработки в области информационной безопасности), т.е. тратит на эти цели самую большую в IT-индустрии долю доходов.

Ресурсы Cisco Systems – это самый широкий в отрасли портфель аппаратных и программных средств, которые используются для строительства информационных сетей и предоставления доступа к ним, плюс операционная система Cisco IOS, предназначенная для поддержки сетевых услуг и приложений, опыт проектирования и развертывания сетей, а также система технической поддержки и профессиональных услуг по обслуживанию и оптимизации своей работы.

Всемирная штаб-квартира Cisco Systems находится в Сан-Хосе (США, Калифорния). Компанию возглавляет Джон Чемберс (John Chambers), председатель и главный исполнительный директор Cisco Systems.

К декабрю 2006г. численность сотрудников Cisco превысила 47 тысяч человек.

После того, как в 1990 г. Cisco стала акционерным обществом открытого типа, ее ежегодные доходы выросли с $69 млн до $28,5 млрд в 2006 финансовом году.

Бренд Cisco – один из самых дорогостоящих в мире (стоит $17,5 млрд)

В СНГ Cisco Systems работает с 1995 года. К настоящему времени офисы Cisco открыты в Алма-Ате, Киеве, Москве, Санкт-Петербурге, Ташкенте.

Корпорация ZyXEL Communications является ведущим разработчиком сетевых решений на базе интернет-технологий. К приоритетным направлениям бизнеса компания относит решения для широкополосного доступа, решения для универсальных конвергентных сетей (NGN) и сетевой безопасности, а также оборудование для цифрового дома.

В компании работает более трех тысяч сотрудников. Созданием новой продукции, поставляющейся в 150 стран мира, занимаются три центра НИОКР. Колоссальный опыт, накопленный за 20 лет развития компании, и установившиеся партнерские отношения с крупнейшими производителями чипсетов позволяют ZyXEL быстро адаптироваться к требованиям любых проектов, предлагать высококонкурентную продукцию и решения и выстраивать длительные и плодотворные отношения с клиентами.

В нашей стране ZyXEL работает с 1992 года. Полная адаптация продукции к российским условиям и активное развитие партнерской сети, объединяющей сегодня более 230 системных интеграторов и реселлеров, дали возможность ZyXEL быстро занять лидирующие позиции на рынке телекоммуникационного оборудования. Сегодня в России и СНГ более миллиона линий работают на DSL-коммутаторах ZyXEL. Ethernet-коммутаторы

ZyXEL эксплуатируются в сетях доступа и агрегации трафика крупных операторов России и СНГ. IP NGN-коммутаторы ZyXEL сертифицированы для использования с рядом программных платформ NGN/IMS, используемых российскими операторами связи.

В России, Украине, Казахстане и Беларуси действуют шесть авторизованных учебных центров по подготовке сертифицированных инженеров. Среди клиентов ZyXEL можно назвать Комстар, Таттелеком, Башинформсвязь, Центральный телеграф, Эффортел, Мостелеком и ряд национальных операторов стран СНГ.

Опора на собственные разработки, предоставляющая полный контроль над функциональностью продукции, в противовес копированию чужих решений.

Развитие масштабируемой сетевой операционной системы собственной разработки ZyNOS™, обеспечивающей быструю интеграцию новых технологий в продукцию и реализацию единого унифицированного интерфейса настройки, диагностики и управления.

Создание решений на базе общепринятых технологий и стандартов – IP, DSL, Ethernet, SIP, Wi-Fi, WiMAX.

Применение в продукции наборов микросхем собственной разработки с целью получения качественного превосходства и снижения издержек (телефонные и ADSL-модемы, Gigabit Ethernet и беспроводные локальные сети).

Тесное взаимодействие с операторами связи, в том числе изготовление специализированных устройств, рассчитанных под их специфические нужды и требования.

D-Link, основанная в 1986 году в Парке Шинчу (Тайвань), является всемирно известным разработчиком и производителем сетевого и телекоммуникационного оборудования и предлагает широкий набор решений для домашних пользователей, корпоративного сегмента и провайдеров интернет-услуг.

127 региональных офисов компании D-Link осуществляют продажу и поддержку оборудования на территории более чем 100 стран мира. В компании работает более 2000 сотрудников. Начиная с 2005 года годовой оборот компании превышает $1 миллиард долларов.

Согласно исследованиям, проведенным аналитической компанией Synergy Research Group, D-Link занимает первое место в мире по объему продаж оборудования в потребительском секторе рынка сетевого оборудования.

D-Link предлагает законченные сетевые и коммуникационные решения для построения "цифрового дома", предприятий малого и среднего бизнеса, сетей масштаба рабочих групп и предприятий и провайдеров услуг Интернет. Кроме этого, компания производит полный спектр оборудования для создания проводных и беспроводных сетей, широкополосного доступа, IP-телефонии и мультимедиа-устройств.

D-Link обладает патентами и авторскими правами на ряд уникальных разработок, в числе которых компьютерные чипы ASIC, технологический дизайн, программное обеспечение и прочая интеллектуальная собственность. Принципы организации управления производством, используемые компанией, отмечены сертификатом системы менеджмента качества ISO 9001 и сертификатом системы экологического менеджмента ISO 14001.

Применение инновационных методик и высокие требования к качеству позволяют компании выпускать высокопроизводительные устройства, базирующиеся на современных стандартах. Идя навстречу требованиям потребителей, компания предлагает наилучшие цены на рынке систем связи в сочетании с высоким качеством устройств.

В 1999 году в Москве было открыто Представительство компании D-Link в России, СНГ и странах Балтии. За время своей работы Представительство добилось ощутимых результатов. Ежегодный прирост объема продаж компании составляет 70-80 процентов. Такие высокие

показатели обусловлены ценовой привлекательностью устройств, их функциональностью, качеством и надежностью.

Важнейшим результатом деятельности российского представительства явилось создание сети региональных офисов. В 2002 году был открыт первый региональный офис D-Link в Санкт-Петербурге. В настоящее время региональные офисы открыты в более чем 30 крупных городах России, СНГ и стран Балтии.

Региональные офисы компании D-Link отвечают за работу с местными каналами продаж и обеспечение маркетинговой и технической поддержки партнеров, включая предоставление образцов оборудования на тестирование, гарантийное обслуживание и ремонт. Региональные офисы регулярно проводят бесплатные технические семинары и тренинги как на своей территории, так и на территории партнеров компании или их заказчиков.

В настоящее время D-Link имеет развитую систему дистрибуции, ориентированную, в основном, на регионы. Дистрибуторские соглашения подписаны с крупнейшими российскими IT-компаниями. Кроме того, D-Link имеет официальных дистрибуторов в Украине, Белоруссии, Молдове, Казахстане, Литве, Латвии, Эстонии, Грузии, Армении, Киргизии, Узбекистане и Туркменистане.

Оборудование D-Link, представленное на российском рынке, имеет все необходимые сертификаты, включая сертификаты в области связи, Госстандарта России и Санитарно-эпидемиологической службы РФ.

Вопросы для самоконтроля

1. Что такое вендор?
2. Что такое бренд?
3. Что такое no-name?
4. Расскажите о Cisco Systems
5. Расскажите о ZyXEL
6. Расскажите о D-Link

II.1.2. Сетевое оборудование, классификация

Уже были рассмотрены случаи сетевого подключения «компьютер-компьютер»; различные сетевые топологии, сетевые стандарты и спецификации; устройства коммутации. Теперь рассмотрим то аппаратное и аппаратно-программное обеспечение, которое необходимо для построения компьютерных сетей.

Вообще, сетевое оборудование – достаточно широкое понятие и, к сожалению, люди часто путаются, когда пытаются в нем разобраться. Для начала, надо четко понимать, что такое сеть. Сетевое оборудование необходимо на каждом уровне функционирования компьютерных сетей, а значит, может относиться к любому уровню модели OSI, или сразу к нескольким.

Сетевое оборудование принято делить на активное и пассивное.

Под активным сетевым оборудованием подразумевается оборудование, за которым следует некоторая «интеллектуальная» особенность. То есть маршрутизатор, коммутатор (свитч) и т.д. являются активным сетевым оборудованием.

Под пассивным сетевым оборудованием подразумевается оборудование, не наделенное «интеллектуальными» особенностями. Например, кабель (коаксиальный и витая пара (UTP/STP)), вилка/розетка (RG58, RJ45, RJ11, GG45), повторитель (репитер), концентратор (хаб), балун (balun) для коаксиальных кабелей (RG-58) и т.д.

II.1.3. Пассивное сетевое оборудование

Итак, под пассивным сетевым оборудованием подразумевается оборудование, не наделенное «интеллектуальными» особенностями.

Разберем особенно актуальные примеры.

Сетевой концентратор или **хаб** (от англ. hub – центр) – устройство для объединения компьютеров в сеть Ethernet с применением кабельной инфраструктуры типа витая пара. В настоящее время вытеснены сетевыми коммутаторами.

Сетевые концентраторы также могли иметь разъемы для подключения к существующим сетям на базе толстого или тонкого коаксиального кабеля.

Концентратор работает на 1 (первом) – физическом уровне сетевой модели OSI, ретранслируя входящий сигнал с одного из портов в сигнал на все остальные (подключенные) порты, реализуя, таким образом, свойственную Ethernet топологию, с разделением пропускной способности сети между всеми устройствами и работой в режиме полудуплекса. Коллизии (т.е. попытка двух и более устройств начать передачу одновременно) обрабатываются аналогично сети Ethernet на других носителях – устройства самостоятельно прекращают передачу и возобновляют попытку через случайный промежуток времени, говоря современным языком, концентратор объединяет устройства в одном домене коллизий.

Сетевой концентратор также обеспечивает бесперебойную работу сети при отключении устройства от одного из портов или повреждении кабеля, в отличие, например, от сети на коаксиальном кабеле, которая в таком случае прекращает работу целиком.

Единственное преимущество концентратора – низкая стоимость, было актуально лишь в первые годы развития сетей Ethernet. По мере совершенствования и удешевления электронных микропроцессорных компонентов данное преимущество концентратора полностью сошло на нет, так как их стоимость вычислительной части коммутаторов и маршрутизаторов составляет лишь малую долю на фоне стоимости разъемов, разделительных трансформаторов, корпуса и блока питания, общих для концентратора и коммутатора.

Недостатки концентратора являются логическим продолжением недостатков топологии общая шина, а именно – снижение пропускной способности сети по мере увеличения числа узлов. Кроме того, поскольку на канальном уровне узлы не изолированы друг от друга все они будут работать со скоростью передачи данных самого худшего узла. Например, если в сети присутствуют узлы со скоростью 100 Мбит/с и всего один узел со скоростью 10

Мбит/с, то все узлы будут работать на скорости 10 Мбит/с, даже если узел 10 Мбит/с вообще не проявляет никакой информационной активности. Еще одним недостатком является вещание сетевого трафика во все порты, что снижает уровень сетевой безопасности и дает возможность подключения снифферов[1].

Коммутационная панель (**кросс-пане́ль, патч-пане́ль**) – одна из составных частей структурированной кабельной системы (СКС). Представляет собой панель со множеством соединительных разъёмов, расположенных на лицевой стороне панели. На тыльной стороне панели находятся контакты, предназначенные для фиксированного соединения с кабелями, и соединённые с разъёмами электрически.

Защищённый телекоммуникационный шкаф (антивандальный шкаф) (англ. Protective cabinet) – телекоммуникационный шкаф, для размещения и защиты телекоммуникационного оборудования (серверов, маршрутизаторов, коммутаторов, модемов, телефонных станций, элементов оптических кроссовых систем) в местах общего доступа – коридорах, чердаках, лестничных клетках подъездов, подвалах – где возможно хищение, повреждение или подмена оборудования посторонними лицами.

II.1.4. Активное сетевое оборудование

Итак, под этим названием подразумевается оборудование, за которым следует некоторая «интеллектуальная» особенность. Опять же стоит рассмотреть наиболее актуальные примеры.

Сетевой **коммутатор** (англ. **switch** – переключатель) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как

[1] **Анализатор трафика**, или **сниффер** (от англ. *to sniff — нюхать*) - сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов

многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы.

В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых не известен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Коммутатор хранит в памяти таблицу коммутации (хранящуюся в ассоциативной памяти), в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует кадры (фреймы) и, определив MAC-адрес хоста-отправителя, заносит его в таблицу на некоторое время. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес хоста-получателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того порта, с которого он был получен. Со временем коммутатор строит таблицу для всех активных MAC-адресов, в результате трафик локализуется. Стоит отметить малую латентность (задержку) и высокую скорость пересылки на каждом порту интерфейса.

Маршрутиза́тор (от англ. router) или **ро́утер** – специализированный сетевой компьютер, имеющий минимум два сетевых интерфейса и пересылающий пакеты данных между различными сегментами сети, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

Маршрутизаторы делятся на программные и аппаратные. Маршрутизатор работает на более высоком «сетевом» уровне 3 сетевой модели OSI, нежели коммутатор и сетевой мост, которые работают на 2 уровне и 1 уровне модели OSI соответственно.

Обычно маршрутизатор использует адрес получателя, указанный в пакетных данных, и определяет по таблице маршрутизации путь, по которому следует передать данные. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается.

Существуют и другие способы определения маршрута пересылки пакетов, когда, например, используется адрес отправителя, используемые протоколы верхних уровней и другая информация, содержащаяся в заголовках пакетов сетевого уровня. Нередко маршрутизаторы могут осуществлять трансляцию адресов отправителя и получателя, фильтрацию транзитного потока данных на основе определённых правил с целью ограничения доступа, шифрование/расшифрование передаваемых данных и т. д.

II.1.5. Лабораторные работы

II.1.5.1. Виртуальная лаборатория Packet Tracer

Цели и задачи:

иметь представление:

- об элементарных принципах проектирования компьютерных сетей;
- о профессиональной деятельности специалиста по компьютерным сетям;
- о принципах работы в Packet Tracer;

знать:

- основные элементы компьютерных сетей;
- принципы соединения элементов компьютерных сетей;
- принципы построения модели компьютерной сети в Packet Tracer;

уметь:

- создавать модели компьютерных сетей в Packet Tracer;

– сохранять и загружать созданные модели;

– моделировать отправку простого сетевого сообщения.

Оборудование и инструменты:

– современный ПК с программой Packet Tracer.

Теоретическое введение.

Медиатор Packet Tracer (букв. – система отслеживания пакетов) – программа для моделирования сети на основе оборудования CISCO, позволяет студентам имитировать поведение реальных сетей и выполнять действия, развивающие глубокое понимание сетевых технологий.

Инструмент обучения из курсов CCNA Academy (CCNA – Cisco Certified Network Associate (Сертифицированный Cisco сетевой специалист)). Позволяет генерировать соответствующие топологии сетей с оборудованием маршрутизации и коммутации и проверять, как проходят пакеты.

Качественный симулятор для выполнения лабораторных работ CCNA и проектирования сетей. Полезен вне зависимости от того, какой курс вы проходили. Большинство настроек интуитивно понятны.

Позволяет:

– симулировать локальную сеть с использованием маршрутизаторов, свичей, точек доступа и т.п;

– выбор различных конфигураций сетевого оборудования Cisco, много описаний модулей;

– симуляция командной строки;

– симуляция отладки;

– визуальная симуляция хождения пакетов в сети.

Вопросы для самоконтроля:

1. Что такое Packet Tracer?
2. Зачем нужен Packet Tracer?
3. Что такое CCNA Academy?
4. Что позволяет Packet Tracer?

Задания для самостоятельной работы:

1. Ознакомиться и описать принципы эксплуатации Packet Tracer, описать GUI. Снимки экрана приветствуются.

2. Составить модель соединения «компьютер-компьютер» и описать ее. Каким способом физической связи они соединяются?

3. Создайте простой пакет для пересылки с одного компьютера на другой.

4. Сохраните работу в установленном месте с пометкой comp-comp.

5. Создайте модель соединения «компьютер-хаб-компьютер» с 15-ю компьютерами.

6. Создайте простой пакет для пересылки с одного компьютера на любой другой.

7. Опишите и сохраните результат.

II.1.5.2. Получение сообщений и просмотр анимации в Simulation Mode

Цели и задачи:

иметь представление:

- о протоколе ICMP;
- о сетевых утилитах, использующих протокол ICMP;
- о формате ICMP-пакетов;
- о типах ICMP-пакетов;

знать:

- функции протокола ICMP;
- утилиты ping и tracerout (tracert);
- принципы работы в Simulation Mode;

уметь:

- отправлять пакеты ICMP в Simulation Mode;
- получать информацию о движении ICMP-пакетов;

– узнавать IP адрес по известному сетевому имени;
– посылать на заданный узел пакеты ICMP заданной величины;
– устанавливать параметры работы утилиты ping;
– считать транзитные узлы до заданного узла;
– отслеживать маршрут трафика.

Теоретическое введение

ICMP (англ. Internet Control Message Protocol — межсетевой протокол управляющих сообщений) — сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных. Также на ICMP возлагаются некоторые сервисные функции.

Протокол ICMP описан в RFC 792 (с дополнениями в RFC 950) и является стандартом Internet (входит в стандарт STD 5 вместе с IP). Хотя формально ICMP использует IP (ICMP пакеты инкапсулируются в IP пакеты), он является неотъемлемой частью IP и обязателен при реализации стека TCP/IP. Текущая версия ICMP для IPv4 называется ICMPv4. В IPv6 существует аналогичный протокол ICMPv6.

Протокол ICMP не делает протокол IP средством надёжной доставки сообщений. Для этих целей существует TCP.

ICMP сообщения (тип 12) генерируются при нахождении ошибок в заголовке IP пакета (за исключением самих ICMP пакетов, дабы не привести к бесконечно растущему потоку ICMP сообщений об ICMP сообщениях).

ICMP сообщения (тип 3) генерируются маршрутизатором при отсутствии маршрута к адресату.

Утилита ping, служащая для проверки возможности доставки IP пакетов использует ICMP сообщения с типом 8 (эхо-запрос) и 0 (эхо-ответ).

Утилита traceroute, отображающая путь следования IP пакетов, использует ICMP сообщения с типом 11.

ICMP сообщения с типом 5 используются маршрутизаторами для обновления записей в таблице маршрутизации отправителя.

ICMP сообщения с типом 4 используются получателем (или промежуточным маршрутизатором) для управления скоростью отправки сообщений отправителем.

Типы ICMP пакетов (неполный список)

– 0 — Эхо-ответ

– 3 — Адресат недоступен

код 0 — сеть недостижима;

код 2 — протокол недостижим;

код 3 — порт недостижим;

код 4 — необходима фрагментация, но установлен флаг ее запрета(DF);

код 5 — неверный маршрут от источника;

– 4 — Сдерживание источника (отключение источника при переполнении очереди)

– 5 — Перенаправление

код 0 — перенаправление пакетов в сеть;

Код 1 — перенаправление пакетов к хосту;

Код 2 — перенаправление для каждого типа обслуживания(TOS);

Код 3 — перенаправление пакета к хосту для каждого типа обслуживания;

– 8 — Эхо-запрос

– 9 — Объявление маршрутизатора

– 10 — Запрос маршрутизатора

– 11 — Превышение временно́го интервала (для дейтаграммы время жизни истекло)

тип 0 — время жизни пакета истекло при транспортировке

тип 1 — время жизни пакета истекло при дефрагментации

– 12 — Неверный параметр (проблема с параметрами дейтаграммы: ошибка в IP-заголовке или отсутствует необходимая опция)

– 13 — Запрос метки времени
– 14 — Ответ с меткой времени
– 15 — Информационный запрос
– 16 — Информационный ответ
– 17 — Запрос адресной маски
– 18 — Отклик на запрос адресной маски

ping — утилита для проверки соединений в сетях на основе TCP/IP.

Она отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа (RTT, от англ. Round Trip Time) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, то есть косвенно определять загруженность на каналах передачи данных и промежуточных устройствах.

Также пингом иногда ошибочно называют время, затраченное на передачу пакета информации в компьютерных сетях от клиента к серверу и обратно от сервера к клиенту. Это время называется лагом (англ. отставание; задержка, запаздывание) или собственно задержкой и измеряется в миллисекундах. Лаг связан со скоростью соединения и загруженностью каналов на всём протяжении от клиента к серверу.

Полное отсутствие ICMP-ответов может также означать, что удалённый узел (или какой-либо из промежуточных маршрутизаторов) блокирует ICMP Echo-Reply или игнорирует ICMP Echo-Request.

Программа ping является одним из основных диагностических средств в сетях TCP/IP и входит в поставку всех современных сетевых операционных систем. Функциональность ping также реализована в некоторых встроенных ОС маршрутизаторов, доступ к результатам выполнения ping для таких устройств по протоколу SNMP определяется RFC 2925 (Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations).

Так как для отправки ICMP-пакетов требуется создавать raw-сокеты, для выполнения программы ping в unix-системах необходимы права

суперпользователя. Чтобы обычные пользователи могли использовать ping в правах доступа файла /bin/ping устанавливают SUID-бит.

Traceroute — это служебная компьютерная программа, предназначенная для определения маршрутов следования данных в сетях TCP/IP. Traceroute основана на протоколе ICMP.

Программа traceroute выполняет отправку данных указанному узлу сети, при этом отображая сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к целевому узлу. В случае проблем при доставке данных до какого-либо узла программа позволяет определить, на каком именно участке сети возникли неполадки.

traceroute входит в поставку большинства современных сетевых операционных систем. В системах Microsoft Windows эта программа носит название tracert, а в системах GNU/Linux, Cisco IOS и Mac OS — traceroute.

Так, чтобы воспользоваться утилитами ping или tracert в ОС Windows можно вбить их с клавиатуры в Пуск - Выполнить, или выполнить команду cmd. Рекомендуется пользоваться именно cmd. В командной строке есть возможность просмотреть синтаксис утилиты и ее возможности путем использования ключа /? – например, ping /? или tracert /?

Чтобы узнать IP-адрес узла Internet (например, mail.ru), нужно ввести команду ping mail.ru. Чтобы узнать маршрут до узла, нужно ввести команду tracert mail.ru.

Вопросы для самоконтроля

1. Что такое ICMP?
2. Какими стандартами описан ICMP?
3. Для чего служит утилита ping?
4. Для чего служит утилита tracert?
5. Какие бывают типы ICMP-пакетов?
6. Как узнать IP-адрес узла Internet www.yandex.ru?
7. Как узнать маршрут до узла Internet www.yandex.ru?

8. Что означает команда ping yandex.ru –t –l 333?

9. Что означает команда tracert –h 100 yandex.ru?

Задания для самостоятельной работы

1. Откройте свою сохраненную лабораторную работу №1 и, отражая все свои действия в лабораторном журнале, выполните следующие задания

2. В Realtime Mode пошлите простой PDU от одного компьютера другому

3. Удалите это сообщение из журнала и переключитесь в Simulation Mode

4. Уберите галочку All/None и верните галочку ICMP для просмотра ICMP пакетов

5. Снова передайте простой PDU от первого компьютера другому, при этом в поле Event List должно появиться соответствующее сообщение, а на первом компьютере изображение конверта

6. Нажмите кнопку Capture/Forward на панели Play Controls – опишите результат действия

7. Сохраните работу в установленном месте

8. На хост машине откройте командную оболочку

9. Изучите утилиту ping

10. Изучите утилиту tracert/traceroute

II.1.5.3. Просмотр пакетов в Simulation Mode

Цели и задачи:

иметь представление:

- о взаимодействии протоколов различных уровней модели OSI;
- о возможностях мониторинга деятельности пользователей сети по просмотру содержимого их трафика;
- о функциях сетевых сообщений;

знать:

– программы сетевого мониторинга;

– принципы мониторинга компьютерных сетей;

уметь:

– просматривать пакеты в Simulation Mode;

– производить мониторинг компьютерных сетей.

Теоретическое введение

Термином мониторинг сети называют работу системы, которая выполняет постоянное наблюдение за компьютерной сетью в поисках медленных или неисправных систем и которая при обнаружении сбоев сообщает о них сетевому администратору с помощью почты, пейджера или других средств оповещения. Эти задачи являются подмножеством задач управления сетью.

В то время как система обнаружения вторжений следит за появлением угроз извне, система мониторинга сети выполняет наблюдение за сетью в поисках проблем, вызванных перегруженными и/или отказавшими серверами, другими устройствами или сетевыми соединениями.

Например, для того, чтобы определить состояние веб-сервера, программа, выполняющая мониторинг, может периодически отправлять запрос HTTP на получение страницы; для почтовых серверов можно отправить тестовое сообщение по SMTP и получить по IMAP или POP3.

Неудавшиеся запросы (например, в том случае, когда соединение не может быть установлено, оно завершается по таймауту, или когда сообщение не было доставлено) обычно вызывают реакцию со стороны системы мониторинга. В качестве реакции может быть:

– отправлен сигнал тревоги системному администратору;

– автоматически активирована система защиты от сбоев, которая временно выведет проблемный сервер из эксплуатации, до тех пор, пока проблема не будет решена,

– и так далее.

Краткий список наиболее популярных программ сетевого мониторинга

- Программа ping
- Программа ipconfig
- Серверы SNMP
- Система управления и мониторинга AGNEKO SNMPc
- Hyperic HQ (Open Source)
- Zabbix (Open Source)
- NetXMS (Open Source)
- TclMon (Open Source)
- Big Brother
- Cacti (Open Source)
- Caligare Flow Inspector — Анализатор NetFlow
- MRTG (GNU)
- RRDtool (GNU)
- Intellipool Network Monitor
- Ipswitch WhatsUp
- ManageEngine OpManager
- Netmon - Appliance based network monitoring suite with email and pager alert system.
- Nagios (ранее *Netsaint*) (Open Source)
- OpenNMS (Open Source)
- Cricket
- PRTG
- Packet Analyzer: Network Traffic Monitoring, Analysis and Troubleshooting
- NetVizor
- NetDecision

- HP OpenView Network Node Manager (NNM)
- Cisco Works NMS
- ProLAN-Эксперт
- The Dude
- Total Network Monitor
- Monit (Open Source)
- Fluke Networks - Visual Performance Manager
- 10-Strike LANState

Рассмотрим подробнее ipcpnfog

ipconfig — утилита командной строки для управления сетевыми интерфейсами. В операционных системах Microsoft Windows ipconfig — это утилита командной строки для вывода деталей текущего соединения и управления клиентскими сервисами DHCP и DNS. Также есть подобные графические утилиты с названиями winipcfg и wntipcfg (последняя предшествовала ipconfig). Утилита ipconfig позволяет определять, какие значения конфигурации были получены с помощью DHCP, APIPA или другой службы IP-конфигурирования либо заданы администратором вручную.

Часто в операционных системах GNU/Linux и UNIX детали соединения отслеживаются несколькими утилитами, главной среди них является ifconfig. Тем не менее, ipconfig наряду с ifconfig присутствует в Mac OS X, там ipconfig команда сервиса как оболочка к агенту IPConfiguration и может использоваться для контроля BootP и DHCP клиента из CLI.

Просмотр пакетов в Simulation Mode

В Packet Tracer для просмотров пакетов необходимо перейти в Simulation Mode и на панели Simulation Panel сбросить при необходимости симуляцию кнопкой Reset Simulation (Рис. 15)

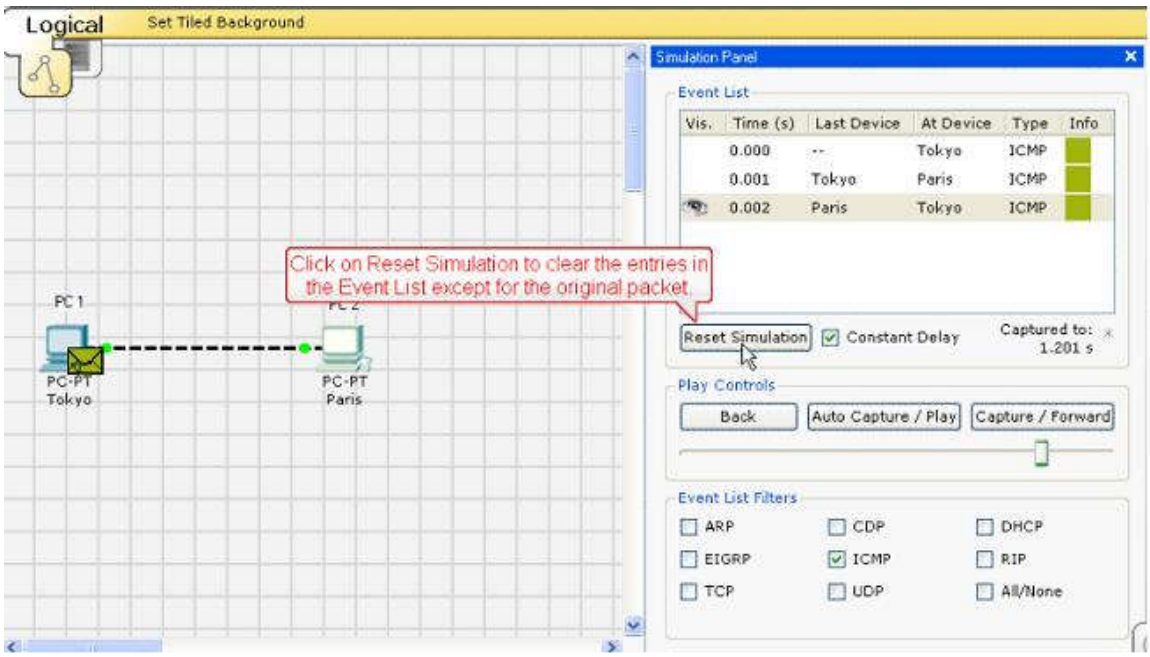


Рис. 15. Simulation Panel в Simulation Mode

Чтобы открыть окно информации PDU необходимо два раза щелкнуть на изображении пакета. Это окно содержит информацию об активности по уровням модели OSI. Просматриваемый пакет на панели Simulation Panel будет отражен строчкой с изображением глаза. Если двойным щелчком нажать на цветной квадрат в этой строчке (Info), то также должно открыться окно информации PDU. Если нажать кнопку Capture / Forward, то пакет полетит назад. При нажатии кнопки Auto Capture / Play должен появиться отчет о симуляции.

Вопросы для самоконтроля

1. Что такое мониторинг сети?

2. Какая может быть реакция системы мониторинга на те, или иные сбои?

3. Какие существуют программы сетевого мониторинга?

4. Что такое ipconfig?

5. Как просматривать пакеты в Simulation Mode?

Задание для самостоятельной работы

1. Загрузите сохраненную работу №2

2. Перейдите в Simulation Mode

3. Опишите Out Layers просматриваемого пакета

4. Опишите In Layers просматриваемого пакета

5. Опишите полную информацию о симуляции

6. Сохраните работу в условленном месте

7. В виртуальной Windows-машине запустите ipconfig и опишите функциональные возможности

8. Опишите результаты команды ipconfig /all

II.1.5.4. Таблицы ARP

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

ARP (протокол разрешения адресов) — очень распространённый и чрезвычайно важный протокол. Каждый узел сети имеет 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, шлёт 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. Ниже приведён пример ARP-запроса и ARP-ответа.

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 записи кеша. Это можно сделать при помощи команды:

```
arp -s <IP адрес> <MAC адрес>
```

После того, как IP-адрес прошёл процедуру разрешения адреса, он остаётся 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.

ARP также можно использовать для разрешения MAC-адресов для различных адресов протоколов 3-го уровня (Layer 3 protocols addresses). ARP был адаптирован также для разрешения других видов адресов 2-го уровня

(Layer 2 addresses); например, ATMARP используется для разрешения ATM NSAP адресов в Classical IP over ATM протоколе.

Таблица маршрутизации — электронная таблица (файл) или база данных, хранящаяся на маршрутизаторе или сетевом компьютере, описывающая соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора. Является простейшей формой правил маршрутизации.

Таблица маршутизации обычно содержит:

– адрес сети или узла назначения, либо указание, что маршрут является маршрутом по умолчанию;

– маску сети назначения (для IPv4-сетей маска /32 (255.255.255.255) позволяет указать единичный узел сети);

– шлюз, обозначающий адрес маршрутизатора в сети, на который необходимо отправить пакет, следующий до указанного адреса назначения;

– интерфейс (в зависимости от системы это может быть порядковый номер, GUID[1] или символьное имя устройства);

– метрику — числовой показатель, задающий предпочтительность маршрута. Чем меньше число, тем более предпочтителен маршрут (интуитивно представляется как расстояние).

В таблице может быть один, а в некоторых операционных системах и несколько шлюзов по умолчанию. Такой шлюз используется в сетях, для которых нет более конкретных маршрутов в таблице маршрутизации.

Стати́ческая маршрутиза́ция - вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора. Вся маршрутизация при этом происходит без участия каких-либо протоколов маршрутизации.

При задании статического маршрута указывается:

– Адрес сети (на которую маршрутизируется трафик), маска сети

[1] **GUID (Globally Unique Identifier)** — статистически уникальный 128-битный идентификатор.

– Адрес шлюза (узла), который отвечает за дальнейшую маршрутизацию (или подключен к маршрутизируемой сети напрямую)

– (опционально) метрика (иногда именуется также "ценой") маршрута. При наличии нескольких маршрутов на одну и ту же сеть некоторые маршрутизаторы выбирают маршрут с минимальной метрикой (однако, например, ядро Linux просто игнорирует параметр metric в таблице маршрутизации, и предназначается он только для протоколов маршрутизации, наподобии RIP[1]).

В некоторых маршрутизаторах возможно указывать интерфейс, на который следует направить трафик сети и указать дополнительные условия, согласно которым выбирается маршрут (например, SLA в маршрутизаторах cisco).

Основные достоинства статической маршрутизации:

– Лёгкость отладки и конфигурирования в малых сетях.

– Отсутствие дополнительных накладных расходов (из-за отсутствия протоколов маршрутизации)

– Мгновенная готовность (не требуется интервал для конфигурирования/подстройки)

– Низкая нагрузка на процессор маршрутизатора

– Предсказуемость в каждый момент времени

Недостатки:

– Очень плохое масштабирование (добавление N+1 сети потребует сделать 2*(N+1) записей о маршрутах, причём на большинстве маршрутизаторов таблица маршрутов будет различной, при N>3-4 процесс конфигурирования становится весьма трудоёмким).

---

[1] **Протокол RIP** (англ. *Routing Information Protocol*) — один из наиболее распространенных протоколов маршрутизации в небольших компьютерных сетях, который позволяет маршрутизаторам динамически обновлять маршрутную информацию (направление и дальность в хопах), получая ее от соседних маршрутизаторов.

– Низкая устойчивость к повреждениям линий связи (особенно, в ситуациях, когда обрыв происходит между устройствами второго уровня и порт маршрутизатора не получает статус down).

– Отсутствие динамического балансирования нагрузки

– Необходимость в ведении отдельной документации к маршрутам, проблема синхронизации документации и реальных маршрутов.

В реальных условиях статическая маршрутизация используется в условиях наличия шлюза по умолчанию (узла, обладающего связностью с остальными узлами) и 1-2 сетями. Помимо этого статическая маршрутизация используется для "выравнивания" работы маршрутизирующих протоколов в условиях наличия туннеля (для того, чтобы маршрутизация трафика, создаваемого туннелем, не производилась через сам туннель).

Вопросы для самоконтроля

1. Чем отличается хаб от свитча?
2. Как работает хаб?
3. Как работает свитч?
4. Что такое ARP?
5. Какие типы ARP-сообщений Вы знаете?
6. Какими могут быть записи в ARP-кеше?
7. Адресы каких уровней преобразуются протоколом ARP?
8. Что такое таблица маршрутизации?
9. Что обычно содержит таблица маршрутизации?
10. Что такое статическая маршрутизация?
11. Что указывается при задании статического маршрута?
12. Каковы основные достоинства и недостатки статической маршрутизации?
13. Используется ли статическая маршрутизация в реальных условиях?

Задание для самостоятельной работы:

1. Откройте свою сохраненную лабораторную работу №3

2. В правом меню выберите инструмент Inspect (увеличительное стекло)

3. Щелкните этим инструментом сперва на изображении одного, затем другого компьютера, чтобы открыть таблицу ARP

4. Подвиньте и раздвиньте окна таблиц так, чтобы было видно оба окна и они не закрывали карту с сетью

5. В режиме реального времени пошлите простой PDU от одного компьютера другому

6. Запишите полученные результаты таблиц в лабораторный журнал

7. Удалите лог пакета. Обратите внимание – таблица не очистилась

8. Нажмите на кнопку Reset Network и подтвердите сброс сети. Таблицы должны очиститься

9. Перейдите в Simulation Mode

10. Оставьте все галочки в Event List Filters

11. Снова пошлите простой PDU от одного компьютера другому

12. Нажмите Auto Capture/play

13. Запишите содержимое появившегося информационного окна

14. Нажмите Reset Simulatin. Как и в пункте 7, таблица не должна очиститься

15. Снова нажмите Auto Capture/play. На сей раз, когда есть запись таблицы ARP, информация должна пройти только о ICMP пакете

16. Запишите содержимое информационного окна

17. Снова нажмите на кнопку Reset Network. В поле Event List должен появиться новый ARP запрос

II.2. Проектирование, монтаж и настройка компьютерных сетей

Если в результате изучения предыдущего материала обучающийся действительно его освоил, можно изучить основы развертывания локальных сетей. При заказе или иной необходимости, прежде чем заказывать оборудование и приступать к монтажу, есть смысл разработать проект.

II.2.1. Проектирование компьютерных сетей

Этап проектирования компьютерной сети является очень важным этапом, при игнорировании которого можно достаточно сильно пострадать, в том числе финансово. При различных масштабах проектов потери так же будут различаться.

Проект сети – это чертеж. При создании проекта обязательно следует указать на нем все компьютеры и устройства, которые будут подключены к сети. При этом нужно стараться разместить их так, как они располагаются в реальной обстановке. При достаточном уровне абстрагирования, расчеты материалов и оборудования должны быть как можно более близкими к фактическим нуждам.

Выбрав необходимую конфигурацию сети, необходимо добавить в проект данные о прокладке кабельканала и кабельной системы. При этом нельзя забывать, что кабель должен быть защищен от случайного обрыва, то есть прокладывать его нужно подальше от рук и ног пользователей. Сделав это, можно получить длину всех кабельных сегментов.

В проекте также следует определить, где можно и/или нужно устанавливать активное сетевое оборудование. Сделать это необходимо независимо от того, будет создаваться одноранговая сеть или сеть с выделенным сервером. Если планируется подключать более 30 компьютеров, стоит задуматься об использовании монтажного шкафа, в котором можно будет установить не только необходимое сетевое оборудование, но и блоки бесперебойного питания.

Также в проекте стоит учесть потенциальный рост количества рабочих станций, тем самым обеспечив безболезненную расширяемость сети.

Проект следует разрабатывать в нескольких вариантах, каждый вариант в нескольких экземплярах. Обсуждение вариантов проекта с коллегами – так же важный этап проектирования. Свежий взгляд на проект может избавить от возможных проблем, которые разработчик мог не заметить.

После создания и анализа проекта можно приступать к выбору конкретных моделей сетевого оборудования: что именно имеется в наличии и по какой цене у разных поставщиков.

II.2.2. Структурированные кабельные системы

Структурированная кабельная система (СКС) – это универсальная кабельная система здания, группы зданий, предназначенная для использования достаточно длительный период времени без реструктуризации, СКС подразумевает замену собой всей кабельной системы и систем здания/зданий.

То, что СКС универсальная, означает, что она включает в себя:

– компьютерную сеть;

– телефонную сеть;

– охранную систему;

– сигнализацию;

– прочие.

Такая система независима от активного оборудования (оно подлежит заменам) и состоит в основном из следующего набора пассивного оборудования:

– кабель – этот компонент используется как среда передачи данных СКС, кабель можно различать экранированный и неэкранированный;

– розетки – этот компонент используют как точки входа в кабельную сеть;

– коммутационные панели – используются для администрирования кабельных систем в коммутационных центрах этажей и здания в целом;

– коммутационные шнуры – используются для подключения оборудования в кабельную сеть, организации структуры кабельной системы в центрах коммутации.

СКС охватывает все пространство здания, соединяет все точки средств передачи данных, такие как компьютеры, телефоны, датчики пожарной и охранной сигнализации, системы видеонаблюдения и контроля доступа. Все

эти средства обеспечиваются индивидуальными точками входа в общую систему. Линии связи от каждой информационной розетки связывают точки входа с коммутационным центром этажа, образуя **горизонтальную кабельную подсистему**. Все этажные коммутационные узлы специальными магистралями объединяются в коммутационном центре здания. Это **вертикальная кабельная подсистема**. Сюда же подводятся внешние кабельные магистрали для подключения здания к глобальным информационным ресурсам. Такая топология позволяет надежно управлять всей системой здания, обеспечивает гибкость и простоту системы.

В каждом конкретном случае присутствуют три подсистемы СКС: вертикальная кабельная подсистема, горизонтальная кабельная подсистема и подсистема рабочих мест. Для крупных зданий, с большим количеством рабочих мест на этажах, все эти три подсистемы присутствуют в явном виде. Для небольших зданий с ограниченным количеством рабочих мест рекомендуется организовывать один узел коммутации СКС, куда сходится вся горизонтальная кабельная разводка. Т.е. вертикальная кабельная подсистема может отсутствовать, либо носить вырожденный характер, при котором вертикальная кабельная подсистема представляется совокупностью коммутационных шнуров, соединяющих порты коммутаторов с портами центрального коммутатора.

Требования при проектировании СКС:

– СКС должна быть спроектирована с избыточностью по количеству подключений;

– СКС должна быть выполнена в соответствии стандартам – международным, европейским, американским, таким как ANSI/EIA/TIA 568, ANSI/EIA/TIA 569;

– рабочее место должно иметь, как минимум, один разъем для подключения к ЛВС и один разъем для подключения к телефонной сети;

– максимальное расстояние горизонтальной проводки не должно превышать 90м;

– оборудование, использованное для построения СКС, должно соответствовать, как минимум, пятой категории;

– каждая линия связи кабельной системы от точки подключения оконечного оборудования до точки подключения к коммутационной панели должна пройти тестирование на принадлежность, как минимум, к пятой категории;

– СКС должна обеспечивать быструю перекоммутацию линий горизонтальной проводки и магистрали здания;

– прокладку кабелей в коридорах должна осуществляться за фальшпотолком, если таковой имеется, а при его отсутствии – в специализированных кабель-каналах (коробах) или в существующих закладных;

– в рабочих помещениях подвод кабеля к рабочим местам производится в кабельканалах.

II.2.3. Монтаж компьютерных сетей

При монтаже компьютерных сетей следует строго соблюдать требования и рекомендации, выполнение которых гарантирует функционирование всей сети. Основные правила, которые необходимо соблюдать при монтаже кабельной системы следующие:

– не допускать растяжения кабеля во время монтажных работ;

– не допускать изгиба кабеля под прямым углом, радиус изгиба кабеля должен быть не меньше 10 внешних диаметров кабеля;

– удалять оболочку кабеля следует лишь на столько, сколько требуется для монтажа;

– сохраняйте целостность скручивания пар как можно ближе к месту монтажа, что обеспечивает минимальное влияние сигналов различных пар друг на друга; раскрученные во время монтажа кабельные пары не следует скручивать снова, т.к. неправильное скручивание может отрицательно повлиять на рабочие характеристики;

– кабели локальной сети не должны располагаться рядом с силовыми проводами (220в), флуоресцентными лампами, силовыми трансформаторами и другими устройствами, мощные электромагнитные поля которых создают помехи и оказывают отрицательное воздействие на качество передачи сигнала.

В зависимости от категории смежных помещений, проходы сквозь стены выполняются открытыми или уплотненными. Для внутренних отапливаемых помещений проходы выполняются открытыми. Для этого в стенах рабочих помещений сверлятся отверстия, в которые устанавливаются закладные трубы.

В горизонтальных кабельных каналах устанавливаются розетки для каждого рабочего места. Розетки у большинства производителей устанавливаются простым защелкиванием.

В зависимости от типа несущей конструкции, могут применяться различные виды крепления коробов (шурупы, гвозди, силикон).

Короб следует крепить через каждый метр, на концах короба использовать по два крепления.

II.2.4. Настройка сети

Для того, чтобы один компьютер мог обращаться по сети к другому компьютеру (ресурсу), необходимо, чтобы было осуществлено физическое соединение на первом и втором уровнях OSI (link), а так же, чтобы компьютеры находились в одном адресном пространстве (настроить IP-адресацию, 3й уровень). Настройки стека протокола TCP/IP для разных ОС осуществляются по одним и тем же принципам. Для автоматических функций по обнаружению компьютеров/принтеров и т.п. так же нужно настроить имя сети/включения в домен и прочие, нужные в каждом конкретном случае.

К данному моменту обучающийся должен быть знаком с командами ping, tracert/traceroute, ipconfig/ifconfig. Посмотреть таблицу маршрутизации можно командой **route print**.

Команда **netstat** позволяет просмотреть список установленных соединений. В обычном режиме команда пытается преобразовывать все IP-адреса в доменные имена (при помощи службы DNS), что может работать

медленно. Если устраивает числовой вывод, можно вызвать команду **netstat -n**. Если также интересуют открытые порты на компьютере (что означает, что он готов принимать соединения по этим портам), то можно вызвать команду с ключом **-a**: например, **netstat -na**. Можно также вызвать команду **netstat -nb**, чтобы посмотреть, какие процессы установили соединения. Команда **netstat -r** эквивалентна команде **route print**.

Команда **netsh** позволяет изменить настройки сети через командную строку. Проверьте команду **netsh interface ip show address**.

Если название интерфейса «Ethernet», командой **netsh interface ip set address name="Ethernet" source=static addr=192.168.0.33 mask=255.255.255.0 gateway=192.168.0.1 gwmetric=30** можно задать настройки TCP/IP. Для динамического подключения: **netsh interface ip set address name="Ethernet" source=dhcp**.

II.2.5. Поиск и устранение неисправностей

Поиск и устранение неисправностей сетей, как правило, является работой первичного персонала поддержки сети – инженеров и техников. Общие проблемы включают проблемы с подключением пользователей и медленную скорость работы сетей.

Корни проблем локальных сетей часто кроются в одном из таких трех источников.

1. Физический уровень: медная проводка, оптоволокно или беспроводная связь. Возможные причины:

– поврежденные или загрязненные кабели или контакты;

– чрезмерное ослабление сигнала;

– недостаточная пропускная способность кабеля;

– помехи беспроводной связи.

2. Уровень сети: Ethernet и IP. Возможные причины:

– поврежденные сетевые устройства;

– неправильная или неоптимальная конфигурация устройства;

– проблемы аутентификации и сопоставления;

– недостаточная пропускная способность сети.

3. Коммутаторы и виртуальные локальные сети. Возможные причины:

– чрезмерная нагрузка;

– слишком большое количество ошибок;

– неправильно назначенное участие в виртуальной локальной сети;

– проблемы приоритета трафика (CoS/QoS).

Передовые методы успешного устранения неисправностей локальной сети включает следующие действия:

1. Определение точной сути проблемы: придется попросить человека, сообщившего о проблеме, объяснить, как выглядит нормальная работа, а затем показать, как выглядит проблема.

2. Воспроизведение проблемы при возможности: нужно спросить себя, понимаете ли сами симптомы, а затем при возможности нужно проверить самостоятельно, как выглядит сообщенная проблема.

3. Локализация и изоляция причины: нужно попытаться изолировать проблему на уровне одного устройства, подключения или программного приложения.

4. Разработка плана решения проблемы: необходимо исследовать и/или рассмотреть возможные пути решения проблемы. Нужно учитывать возможность того, что некоторые доступные решения проблемы могут вызвать другие проблемы.

5. Реализация плана: фактическим решением проблемы может оказаться замена оборудования, применение обновления/исправления программного обеспечения, переустановка приложения или компонента, или очистка файла, зараженного вредоносным кодом. Если проблема заключается в учетной записи пользователя, может потребоваться изменение параметров безопасности пользователя или сценариев входа в систему.

6. Проверка решения проблемы: После того, как было реализовано принятое решение, обязательно нужно убедиться, что проблема полностью решена, попросив пользователя проверить наличие проблемы еще раз.

7. Документация проблемы и решения: документация может использоваться в дальнейшем для помощи в устранении таких же или аналогичных проблем. Также можно использовать документацию для подготовки отчетов по общим проблемам сети для руководства и/или пользователей, или для обучения новых пользователей сети или участников команды поддержки сети.

8. Обеспечение взаимодействия с пользователем: такой подход побуждает пользователей сообщать о подобных ситуациях в будущем, что позволит улучшить производительность сети. Если пользователь сможет сделать что-то для исправления или избегания проблемы, обеспечение взаимодействия с ним может уменьшить количество проблем с сетью в будущем.

Предоставление персоналу передовой поддержки сети надлежащей подготовки, необходимых инструментов и надежных методов устранения неисправностей приводит к более быстрому решению проблем локальной сети, что экономит рабочее время сотрудников, позволяет быстрее обслуживать заявки на устранение неисправностей, сводя к минимуму время простоя, а также быстрее возвращая к работе пользователей сети.

II.2.6. Практические работы

II.2.6.1. Создание проекта компьютерной сети

Задание: с помощью рулетки провести замеры в обозначенном помещении. Составить проект компьютерной сети на указанное преподавателем количество рабочих станций и серверов. Указать линии передачи, обозначить информационные розетки.

II.2.6.2. Кабельканал, крепеж, стоимость проекта.

По разработанному проекту провести расчеты необходимого активного и пассивного оборудования, предложить стоимость проекта.

II.2.6.3. Витая пара

Витая пара используется для соединения компьютеров в сеть. Внутри внешней оплетки находятся пары проводов, скрученных вместе. Но, чтобы соединить компьютеры в сеть, кроме витой пары нужны еще коннекторы, которые ошибочно называют RJ-45 (настоящее название 8P8C) и специальный инструмент – кримпер (Рис. 16). Сперва провод надо зачистить – снять достаточно внешней оплетки. Для этого на кримпере чаще всего есть специальный нож. Витую пару нужно вложить в кримпер, сжать его ручки, повернуть инструмент и стащить отрезанную оплетку с проводов.

Рис. 16. Кримпер с ножом для зачистки внешней оплетки

Затем следует потянуть за сами провода витой пары, вытаскивая их из оплетки. Напоминаем, что для категории 5е понадобятся все четыре пары, а для категории 3 две пары. Иногда для крепости в кабеле под внешней оплеткой есть еще специальная нить – для того, чтобы она не мешала, ее можно придерживать пальцем. Итак, после очистки от внешней оплетки нужно разобрать провод по парам (Рис. 17), а затем раскрутить сами пары.

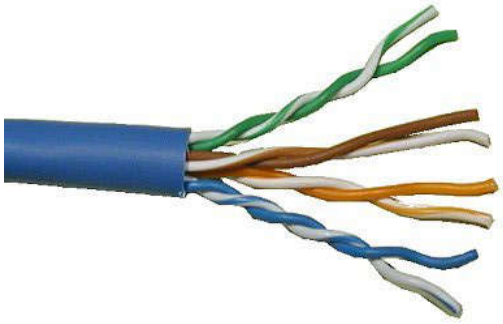


Рис. 17. Пары кабеля UTP cat5e

Стоит помнить, что если надо соединить компьютер с коммутатором, следует использовать следующую последовательность проводов по обеим сторонам кабеля:

1. бело-оранжевый
2. оранжевый
3. бело-зеленый
4. синий
5. бело-синий
6. зеленый
7. бело-коричневый
8. коричневый

При соединении компьютера с другим компьютером напрямую, используют на одном конце кабеля прямое обжатие, а на другой стороне оранжевая и зеленая пары меняются местами:

1. бело-зеленый
2. зеленый
3. бело-оранжевый
4. синий
5. бело-синий
6. оранжевый
7. бело-коричневый

8. коричневый

После того, как разложили кабель по парам, нужно взять коннектор, отрезать кримпером торчащие концы проводов, и вставить их в коннектор. Первый провод – это первый нож коннектора. Провода должны доходить до конца каналов коннектора, внешняя оплетка витой пары должна заходить под ключ коннектора. Осталось только зажать коннектор в кримпере, он должен нажать на ножи, которые проткнут оплетку каждого провода, так же ключ коннектора зажмет внешнюю оплетку кабеля.

При монтаже кабеля витой пары должен выдерживаться минимально допустимый радиус изгиба – сильный изгиб может привести к увеличению внешних наводок на сигнал или привести к разрушению оболочки кабеля.

При монтаже экранированной витой пары необходимо следить за целостностью экрана по всей длине кабеля. Растяжение или изгиб приводит к разрушению экрана, что влечёт уменьшение сопротивляемости наводкам. Дренажный провод должен быть соединен с экраном разъема.

После монтажа и обжима необходимо проверить кабель специальным тестером.

Кабельный тестер, **тестер витой пары** – устройство, обычно состоящее из двух частей, дающее возможность проверить состояние кабеля, и, возможно, измерить его характеристики (Рис. 18).

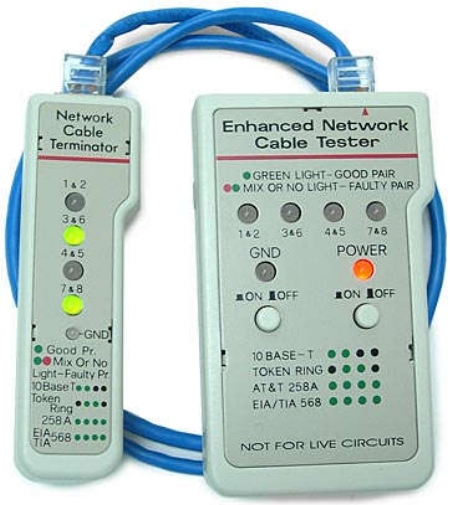


Рис. 18. Кабельный тестер

По сути, обычный кабельный тестер показывает только минимальное соответствие характеристик канала связи заложенным в него требованиям. Такие кабельные тестеры служат для повышения эффективности монтажа проводки и оперативного обнаружения неисправностей. Это простейшие тестеры со светодиодной индикацией. Они, например, не в состоянии измерить расстояние до неисправности или выявить такую ошибку как расщепленные пары («распарка» в жаргоне телефонистов). Основная задача тестеров данного типа – проверить правильность соединения проводников и определить наличие каких-либо механических повреждений – обрывы и/или замыкания.

Существуют еще тестеры:

– Тестеры с расширенными возможностями имеют встроенные генераторы тонального сигнала и могут выявлять расщеплённые пары.

– Типичный современный тестер с ЖК-дисплеем имеет возможность выявить все ошибки в схеме разводки (включая расщеплённые пары), определить длину кабеля, расстояние как до обрыва, так и до замыкания контактов и, кроме этого, определить тип розетки на стене (телефонная или сетевая).

Вопросы для самоконтроля:

1. Что такое витая пара?
2. Для чего служит витая пара?
3. В каких сетях используется витая пара?
4. С помощью чего кабель подключается к сетевым устройствам?
5. Какие категории кабеля существуют?
6. Опишите третью и пятую категории
7. Сколько схем обжима витой пары пятой категории существует и что это за схемы?
8. Как звучит очередность цветов проводов при прямой схеме обжима?
9. Какие пары меняются местами при схеме обжима кроссом?

10. Как называется инструмент для обжима?

11. Как нужно обжать витую пару, чтобы осуществить соединение «компьютер-компьютер»?

Задание для самостоятельной работы:

1. Изложите преподавателю процесс обжатия витой пары
2. При преподавателе обожмите витую пару прямой схемой и кроссом
3. Протестируйте полученный кабель

II.2.6.4. Концентраторы, коммутаторы

Произвести подключение рабочих станций к оборудованию.

II.2.6.5. Настройка сети

Продемонстрировать умение настройки стека TCP/IP в Desktop ОС Windows, Linux.

II.2.6.6. Консольные команды проверки сети

Продемонстрировать умение использования консольных команд проверки сети в ОС Windows, Linux.

II.2.6.7. Поиск и устранение неисправностей

Имеется проблемная сеть / участок сети. Необходимо найти и устранить проблему.

Рекомендуемая литература

1. Костров Б.В. Технологии физического уровня передачи данных ОИЦ «Академия», 2016

2. Баринов В.В., Баринов И.В., Пролетарский А.В. Компьютерные сети ОИЦ «Академия», 2018

3. Костров Б.В., Ручкин В.Н. Сети и системы передачи информации ОИЦ «Академия», 2016

4. Вахранев А.Б. Компьютерные сети. Ч.1: Основы сетей передачи данных [Электронный ресурс]: методическое пособие по дисциплине "Компьютерные сети" /А.Б.Вахранев. – Волгоград: МГГЭУ Волгоградский филиал, 2014. – Режим доступа: Электронная библиотека УМК Волгоградского филиала МГГЭУ

5. Вахранев А.Б. Компьютерные сети. Ч.2: Сетевое оборудование [Электронный ресурс]: методическое пособие по дисциплине "Компьютерные сети" /А.Б.Вахранев. – Волгоград: МГГЭУ Волгоградский филиал,2014. – Режим доступа: Электронная библиотека УМК Волгоградского филиала МГГЭУ

Дополнительные источники:

1. Исаченко О.В. Программное обеспечение компьютерных сетей [Текст]: учеб.пособие/О.В.Исаченко. – М.: Инфра-М, 2012

2. Максимов Н.В. Компьютерные сети [Текст]: учеб.пособие /Н.В.Максимов. –4-е изд., перер. и доп. – М.: Форум, 2011

Интернет-ресурсы:

1. Интернет-университет информационных технологий Интуит – intuit.ru

2. Свободная Интернет-энциклопедия Википедия – ru.wikipedia.org