

Практическое занятие 1

Сети как основное средство информационного обмена

Цель: Изучение базовых технологий построения локальных сетей; получение навыков конфигурирования локальной компьютерной сети в зависимости от возлагаемых на нее функций. Применение метода анализа иерархий для выбора оптимального решения.

Знать: Виды базовых технологий построения локальных сетей

Уметь: Применять методы анализа иерархий для выбора оптимального решения..

Формируемые компетенции:

Код	Формулировка:
ОК-5	быть готовым работать с информацией в различных формах, использовать для ее получения, обработки, передачи, хранения и защиты современные компьютерные технологии
ОПК-7	способностью учитывать современные тенденции развития теории автоматического управления, электронного оборудования, измерительной и вычислительной техники, информационных технологий в профессиональной деятельности
ПК-12	способностью разрабатывать инструкции по эксплуатации используемого технического оборудования и программного обеспечения для обслуживающего персонала
ПК-13	способностью разрабатывать информационное обеспечение систем автоматизации и управления на основе современных технологий программирования
ПК-15	способностью использовать в разработках программно-технических комплексов современные технологии передачи данных и алгоритмы их обработки

Актуальность: аналитического исследование в конфигурировании локальной компьютерной сети в зависимости от возлагаемых на нее функций и применение метода анализа иерархий для выбора оптимального решения.

Теоретическая часть:

Локальные компьютерные сети, базовые понятия

Компьютерная сеть – это совокупность компьютеров, устройств печати, сетевых устройств и компьютерных программ, связанных между собой кабелями или радиоволнами. Большинство первых сетей передавали данные по медному проводу, а сегодня они могут обеспечивать обмен данными, речевыми и видеосигналами, используя провода, оптоволоконную среду, радио и УКВ-волны. Компьютерные сети развиваются со скоростью света, если сравнивать их с другими коммуникационными технологиями, такими как радио, телевидение и телефония.

Компьютерные сети, обычно классифицируемые по их радиусу действия и сложности, делятся на три группы: локальные сети, региональные сети и глобальные сети (рис. 1.). На одном конце этой классификации находятся *локальные сети* (local area network, LAN), состоящие из связанных между собой компьютеров, принтеров и другого компьютерного оборудования, причем, все эти устройства совместно используют аппаратные и программные ресурсы, расположенные на небольшом удалении друг от друга. Радиус действия (область обслуживания) локальной сети может представлять небольшой офис, этаж здания или все здание целиком.

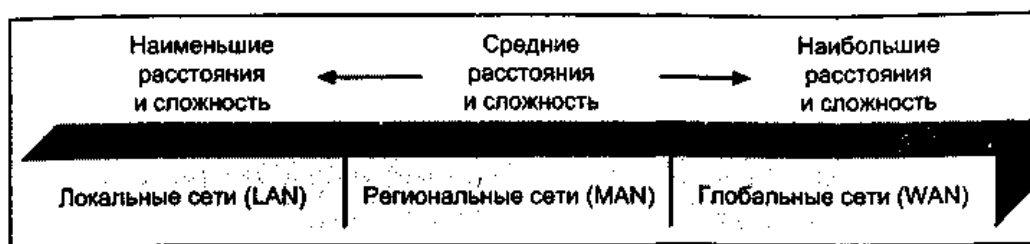


Рисунок 1. – Сравнение локальных, региональных и глобальных сетей

Региональная, или городская сеть (metropolitan area network, MAN) имеет большую область обслуживания, чем локальная сеть, и обычно в ней для обеспечения передачи данных на средние расстояния используется более сложное сетевое оборудование. Региональная сеть объединяет несколько локальных сетей, находящихся в большом городе или некотором регионе, и обычно простирается на расстояния не более 40-50 километров. Отдельные локальные сети, образующие региональную сеть, могут принадлежать как одной организации, так и нескольким различным организациям. Высокоскоростные каналы между локальными сетями в составе региональной сети обычно выполняются с использованием оптоволоконных соединений.

Глобальная сеть (wide area network, WAN) представляет собой наивысший уровень в классификации сетей, поскольку она является крупномасштабной системой сетей, образующих единое целое со сложной структурой. Глобальная сеть образуется из нескольких локальных (или региональных) сетей, охватывающих расстояния свыше 40-50 километров. В состав крупных глобальных сетей могут входить множество локальных и региональных сетей, находящихся на разных континентах.

Примером простейшей глобальной сети может служить модемное подключение к поставщику сетевых услуг по обычным телефонным линиям. Более сложная глобальная сеть – спутниковый мост между локальными сетями, расположенными в разных странах. Самой известной всемирной глобальной сетью является *Интернет*, состоящий из тысяч локальных и региональных сетей, связанных между собой с помощью разнообразных технологий глобальных коммуникаций.

Помимо рассмотренной классификации сетей, существует еще один тип – *корпоративная сеть*. Подобные сети объединяют различных пользователей в пределах одной или нескольких организаций и предоставляют им множество ресурсов. Несмотря на то, что большую локальную сеть можно рассматривать как корпоративную, все же корпоративная сеть обычно состоит из нескольких локальных сетей, образующих региональную или глобальную сеть.

Одной из главных характеристик корпоративной сети является наличие разных ресурсов, позволяющих пользователям решать офисные, исследовательские и образовательные задачи.

Определение типа сети

Иногда различия между локальными, региональными и глобальными сетями (или границы между рабочей группой или корпоративной сетью) являются размытыми, бывает трудно определить, где заканчивается одна сеть и начинается другая. Однако тип сети чаще всего можно определить по результатам анализа следующих четырех сетевых характеристик:

- коммуникационная среда;
- протокол;
- топология;
- тип использования сети (частная или общедоступная).

Понимание границ между сетями может быть чрезвычайно важно при разработке мер безопасности, поскольку, например, для защиты сети от вторжения или вирусов вы можете поместить сетевые устройства в некоторые или во все точки пересечения этих границ.

Причины, обусловившие появление локальных и глобальных сетей

История и развитие сетевых технологий отражают запросы общества, которое нуждается в быстрых средствах связи, используемых в деловой сфере, образовании, для развлечений и взаимного общения. Несмотря на появление все новых и новых, более совершенных коммуникаций, основные требования к ним остаются одними и теми же необходимо иметь простые и быстрые средства взаимодействия со многими людьми, находящимися в разных точках.

История локальных и глобальных сетей

1965. Томас Меррил (Thomas Merrill) и Лоуренс Роберте (Lawrence Roberts) создают первую глобальную сеть между Массачусетским технологическим институтом и компанией System Development Corporation (SDC). Тед Нельсон (Ted Nelson) *впервые использует термин "гипертекст"*.

1966. Исследователи впервые используют волоконную оптику для передачи телефонных сигналов. Дональд Дэйвис (Donald Davies) применяет термины "пакеты" и "коммутация пакетов" при описании метода использования нескольких цепей (маршрутов) для передачи пакетов.

1967. На конференции исследователей ARPA Уэс Кларк (Wes Clark) предлагает идею использования специализированных аппаратных средств для выполнения сетевых функций. Позднее эти устройства были названы "интеллектуальными процессорами сообщений" (Interface Message Processors, IMP). В этом же году Лоуренс Роберте публикует первый проектный документ по ARPANET — "Multiple Computer Networks and Intercomputer Communications" ("Межкомпьютерные сети и коммуникации").

1968. Национальная исследовательская лаборатория Великобритании (National Research Laboratory, NRL) испытывает первую глобальную сеть, использующую коммутацию пакетов.

1971. Сеть ARPANET охватывает 15 вычислительных систем и в общей сложности 23 хост-компьютера в следующих организациях: UCLA, SRI, Университет штата Юта, UCSB, MIT, BBN, RAND Corporation, System Development Corporation, Lincoln Lab, Стэнфорд, Гарвард, Университет штата Иллинойс, центр NASA в Эймсе (Ames), Case Western Reserve University и Central Michigan University. Дневной сетевой трафик достигает 700 000 пакетов. Кроме того, RFC 172 определяет спецификацию протокола передачи файлов File Transfer Protocol (FTP).

1972. Рей Томлинсон (Ray Tomlinson) из BBN создает электронную почту, которая вскоре становится самой популярной программой в сети ARPANET. Также, Ион Постел (Jon Postel) в RFC 318 предлагает сетевую *эмуляцию терминала* (terminal emulation) при помощи прикладного протокола Telnet. Позднее в этом же году Боб Канн (Bob Kahn) демонстрирует сетевое взаимодействие 40 компьютеров по сети ARPANET на Международной конференции по компьютерным коммуникациям, а для создания стандартов ARPANET и сетей образуется Inter-Networking Group (INWG).

1973. Английский University College of London и норвежская организация Royal Radar Establishment реализуют первое международное подключение к ARPANET. К этому моменту ARPANET передает более трех миллионов пакетов в день. Позднее Меткалф и Дейвид Боггс (David Boggs) создали первую сетевую операционную систему с использованием протокола Ethernet, имеющую скорость передачи около трех миллионов бит в секунду.

1976. Создается новый протокол для общедоступных сетей с коммутацией пакетов, названный X.25; к концу 1970-х годов этот протокол получает широкое распространение в открытых сетях Tymnet и Telenet.

1977. Компания Tymshare развертывает общедоступную сеть Tymnet. Позже в этом же году к сети ARPANET подключается первый шлюз беспроводной связи. Эта система передает пакеты с помощью радиоволн, используя технологию, называемую "пакетной радиосвязью" и применяемую до настоящего времени.

1978. Винтон Серф, Стив Крокер и Дэнни Коэн (Danny Cohen) начинают разрабатывать протокол Internet Protocol (IP). Он предлагается как средство

маршрутизации, отдельное от TCP. В последующие годы протоколы TCP и IP становятся жизненно важными компонентами коммуникаций Интернета. В этом же году в Массачусетском технологическом институте демонстрируется первый гипермедиа-видеодиск.

1979. Организуется Internet Configuration Control Board (ICCB) (Совет по управлению структурой Интернета), работа которого направлена на проблемы сетевых шлюзов. Том Траскот (Tom Truscott), Стив Белловин (Steve Bellovin) и Джим Эллис (Jim Ellis) создают сеть USENET, связывающую Университет Дюка (Duke University) и Университет штата Северная Каролина. Также в конце 1970-х годов интегральные микросхемы (integrated circuits, IC) применяются во всех типах электронных устройств. Создаются сложные кристаллы, использующие интеграцию высокого (large scale integration, LSI) и сверхвысокого (very large scale integration, VLSI) уровней (БИС и СБИС). БИС и СБИС прокладывают путь более быстрым и дешевым цифровым устройствам, таким как компьютеры и компьютерные терминалы, после чего открывается дверь для появления персональных компьютеров.

1981. Аира Фукс (Ira Fucks) и Грейдон Фриман (Greydon Freeman) создают академическую сеть Because It's Time NETwork² (BITNET), соединившую Городской Университет Нью-Йорка и Йельский Университет.

²Это название можно перевести как "Потому что время работать в сети!"

1982. Протоколы TCP и IP принимаются как основной набор протоколов для ARPANET. На Национальной компьютерной конференции в июне Дрю Мэйжер (Drew Major), Кэрил Пауэл и Дейл Нейбор представляют первую локальную сеть персональных компьютеров, используя при этом программное обеспечение, явившееся основой для сетевой операционной системы Novell NetWare.

1983. ARPANET становится по-настоящему общедоступной сетью. В сети ARPANET протокол NCP заменяется на TCP/IP, а система Berkeley UNIX начинает поддерживать TCP/IP. Количество хостов, подключенных к ARPANET, достигает 500.

1984. К Интернету подключено свыше 1000 хостов, и в романе Уильяма Гибсона (William Gibson) "Neuromancer" появляется термин "киберпространство".

1986. Число хостов Интернета превышает 5000. Национальный научный фонд США (National Science Foundation) выделяет средства на создание пяти университетских суперкомпьютерных центров, расположенных в разных частях США. Эти центры соединяются каналами 56 Кбит/с в рамках новой сети NSFNET. Суперкомпьютеры и NSFNET открывают возможность выполнения широкомасштабных исследовательских проектов для множества колледжей и университетов США, уже подключенных к сетям, таким как BITNET и Интернет.

1987. Интернет соединяет свыше 10 000 хост-компьютеров. Компания Apple Computer выпускает на рынок первую систему для создания гипермедиа, что означает начало эры авторских средств для настольных компьютеров и продуктов мультимедиа. Создан протокол Simple Gateway Monitoring Protocol (SGMP) (Простой протокол управления шлюзом), впоследствии интегрированный со стеком TCP/IP и названный Simple Network Management Protocol (SNMP) (Простой протокол сетевого управления).

Число хостов Интернета превышает 60 000, и сеть NSFNET работает со скоростью 1,544 Мбит/с, что увеличивает трафик в этой сети до 75 миллионов пакетов в день. В этом же году Европа и Северная Америка соединяются первым трансатлантическим оптоволоконным кабелем, способным одновременно передавать 40 000 телефонных звонков. Internet Worm, первый вирус, созданный Робертом Моррисом младшим (Robert Morris Jr.) специально для Интернета, поражает около 10 процентов интернет-хостов.

1989. Еще 40 000 хостов подключается к Интернету, что в конечном результате дает цифру 100 000. Тим Бернерз Ли (Tim Berners-Lee) распространяет среди интернет-сообщества первый проект "всемирной паутины" – сети World Wide Web. К концу 1980-х годов локальные сети распространены повсеместно, обеспечивая передачу данных как в отдельных помещениях, так и в целых зданиях. Пользователи компьютеров осознают тот факт, что они могут в любой точке обращаться к любым ресурсам – компьютерам,

принтерам и глобальным сетям, таким как Интернет, и что они получили в свое распоряжение феноменальные технологические и программные технологии. Новое сетевое оборудование во все возрастающей степени способно расширить область обслуживания локальных сетей и увеличить скорость передачи данных. Хосты Интернета и сетей перемещаются с мэйнфреймов на небольшие рабочие станции и персональные компьютеры, поскольку распространяются сетевые операционные системы UNIX и NetWare.

1990. Сеть ARPANET, вытесненная Интернетом, официально прекращает существование.

1990 год знаменует начало десятилетия разработки технологий быстрых локальных и глобальных сетевых коммуникаций. Одиннадцать стран становятся новыми членами сети NSFNET.

1991. Количество хостов Интернета превышает 600 000, при этом каждый месяц включаются в работу тысячи новых хостов. Сеть NSFNET становится доступной для коммерческого использования – кардинальный шаг, изменивший характер ее применения. Теперь NSFNET работает со скоростью 44,736 Мбит/с, обеспечивая передачу 10 миллиардов пакетов за месяц. На индивидуальных хостах Интернета можно размещать службы Gopher и World Wide Web, что инициирует гонку за лидерство той или иной технологии.

1993. Количество интернет-хостов переваливает за 2 миллиона. Выпускается веб-браузер Mosaic.

1994. Имеется свыше 3 миллионов хостов Интернета. Скорость передачи по сети NSFNET достигает 155 Мбит/с, что позволяет за месяц передавать свыше 10 триллионов (10^{12}) пакетов. Начинает работу первый кибербанк "First Virtual", а также компания Mosaic Communications Corporation, предшественница фирмы Netscape Communications.

1995. Количество хостов Интернета равно 4 миллионам, а наибольший Интернет-трафик приходится на долю обращений к веб-ресурсам. Национальный и международный сетевой трафик в основном создается различными поставщиками услуг, называемыми провайдерами Интернета (Internet service provider, ISP); совокупность провайдеров, пользователей и хостов рассматривается как "Интернет".

1996. В Интернете 9 миллионов хостов, телекоммуникационная компания MCI достигает скорости передачи, равной 622 Мбит/с.

Закон о телекоммуникациях (Telecommunications Act) от 1996 года поддерживает развитие новых интерактивных коммуникационных функций, включая сетевые операции по телевизионным кабелям и кабелям связи.

1998. Трафик в Интернете удваивается каждые 100 дней, значительно расширяется использование Интернета в бизнесе. Свыше 10 миллионов человек в США и Канаде вовлечены в Интернет-бизнес, покупая авиабилеты, книги, аппаратуру и домашнюю технику, компьютеры и автомобили. Также в 1998 году поставщики сетевого оборудования начали широко предлагать 1-гигабитные коммуникационные устройства.

1999. Академическая и исследовательская сеть Internet2 начинает охватывать университетские сети в Европе и США. В Интернете создан первый полноценный банк, базирующийся в штате Индиана и предлагающий весь спектр услуг. Для ускорения сетевого взаимодействия фрагменты интернет-магистралей США начинают передачу данных со скоростью 2,5 Гбит/с. *Магистраль* (backbone) состоит из высокопроизводительных коммуникационных каналов, объединяющих сети в одном здании, в пределах кампуса или на больших расстояниях.

2000. Для магистральных каналов сети Internet2 используется новая версия протокола IP – IPv6. Европейские страны определяют основу для реализации новой межгосударственной гигабитной сети, названной Geant. Кроме того, многие новые сети позволяют просматривать по Интернету видеоклипы, а множество радиостанций вещает через Интернет.

2001. Поставщики предлагают 10-гигабитные сетевые коммуникационные устройства. Кроме этого, дается толчок развитию беспроводной телекоммуникации. Некоторые компании (например, Microsoft) реализуют в своих кампусах широкополосные беспроводные сети. Высшие школы (университеты) в США получают доступ к исследовательской и академической сети Internet2.

Интеграция локальных и глобальных сетей

С 1960-х и до начала 1980-х годов процедура передачи цифровых данных подразумевала непосредственное подключение неинтеллектуальных (без своего центрального процессора) терминалов к мэйнфреймам и мини-ЭВМ с использованием протокола *Systems Network Architecture (SNA)* компании IBM. Устаревший метод непосредственного подключения к мэйнфреймам почти повсеместно заменен сетями, которые позволяют соединяться с любыми устройствами, в число которых входят следующие:

- серверы;
- мэйнфреймы и мини-ЭВМ;
- равноправные компьютеры, например, рабочие станции, работающие под управлением операционных систем Windows XP/2000/7 или UNIX;
- дисковые устройства централизованного хранения данных;
- массивы приводов CD-ROM;
- принтеры;
- факсимильные аппараты.

Компьютерные сети также позволяют реализовать *клиент-серверные вычисления*, при которых вычислительные мощности распределяются между серверами и клиентскими рабочими станциями.

Дальнейшим развитием клиент-серверных систем является архитектура .NET, разработанная компанией Microsoft. Она взаимодействует с Интернетом и предназначена для такой интеграции данных и пользовательских функций, чтобы их выполнение могло осуществляться в любой точке и на многих типах устройств, включая карманные компьютеры и сотовые телефоны. Кроме того, архитектура .NET позволяет объединять различные языки программирования и использовать их для построения крупномасштабных приложений.

Построение локальных, региональных, глобальных и корпоративных сетей возможно благодаря использованию сетевых устройств, позволяющих расширять область охвата сети, связывать сети воедино, преобразовывать протоколы, а также направлять фреймы и пакеты в нужные сети, т. е. выполнять все операции по *межсетевому обмену* (internetworking). Несмотря на наличие большого количества типов сетевых устройств, имеются четыре группы устройств, играющих основную роль при объединении сетей:

- мосты;
- маршрутизаторы;
- шлюзы;
- коммутаторы.

Мосты (bridge) — это сетевые устройства, которые позволяют удлинить локальную сеть или объединить несколько локальных сетей, соединяя таким образом многочисленные рабочие станции, серверы и другие сетевые устройства, которые иначе не смогли бы взаимодействовать. Как показано на рис. 1.7, мосты могут соединять две или несколько локальных сетей, использующих один и тот же протокол.

Маршрутизаторы (router) — это устройства межсетевого обмена, работающие на более высоком уровне сетевого взаимодействия по сравнению с мостами. Как показано на рис. 1.8, они позволяют локальным и глобальным сетям направлять (маршрутизировать) данные в указанные места назначения.

Маршрутизаторы регулярно взаимодействуют друг с другом и динамически изменяют информацию о сетевых маршрутах по мере того, как меняется топология сети или условия передачи информации. Маршрутизатор может быть специализированным

устройством или компьютером с программным обеспечением, выполняющим функции маршрутизации.

Шлюз (gateway) представляет собой сетевое устройство, обеспечивающее взаимодействие между различными устройствами, системами или протоколами, и которое может работать на любом уровне сетевого обмена в зависимости от заданных ему функций. Чаще всего шлюзы используются для преобразования протоколов. Подобное преобразование может потребоваться при передаче данных из одной локальной сети в другую или из локальной сети в глобальную.

Подобно маршрутизаторам шлюзы могут быть автономными устройствами или службами операционной системы..

Первоначально **коммутаторы (switch)** предназначались для выполнения функций мостов (2-й уровень модели OSI), обеспечивающих более высокую производительность, чем обычные мосты. Это достигалось за счет того, что коммутаторы могут передавать данные непосредственно в заданный сетевой порт или сегмент. В настоящее время коммутаторы некоторых производителей имеют возможности, близкие к возможностям маршрутизаторов (3-й уровень модели OSI), поскольку они анализируют адреса протокола IP и на основе этого анализа посылают сетевые пакеты по указанному маршруту.

Основные термины

Ethernet. Коммуникационная технология, использующая для передачи данных по сети метод доступа CSMA/CD.

Системная сетевая архитектура (Systems Network Architecture (SNA)) -. Многоуровневый коммуникационный протокол, используемый компанией IBmf для передачи данных между мэйнфреймами и периферийными устройствами такими как терминалы и принтеры.

Виртуальная частная сеть (Virtual private network (VPN)) - Частная сеть, работающая как туннель внутри сети большого масштаба (например, внутри Интернета или корпоративной сети) и, таким образом, доступная только для определенных клиентских компьютеров.

Глобальная сеть (Wide area network (WAN)). Совокупность сетей, охватывающих большие площади (на расстояниях свыше нескольких десятков километров друг от друга) и зачастую находящихся в различных странах и на разных континентах.

Интернет (Internet). Всемирная сеть взаимосвязанных локальных и региональных сетей, работающих по протоколу TCP/IP; позволяет людям обмениваться сообщениями электронной почты и получать доступ к самой различной информации.

Клиент-серверные вычисления (Client/server computing). Архитектура компьютерных аппаратных и программных средств, в которой различные модули приложения могут выполняться на отдельных компьютерах или разными компонентами одного компьютера. Обычно клиентские компоненты приложений обеспечивают пользовательский ввод/вывод, а серверные программы выполняют поиск в базах данных, управляют выводом на печать и т. д.

Коммутатор (Switch). Устройство для связи сетевых сегментов, пересылающее и фильтрующее фреймы между ними. Изначально коммутаторы работали, в первую очередь, на Уровне 2 модели OSI и для пересылок использовали физические адреса, или адреса устройств; однако современные коммутаторы могут также функционировать на Уровне 3 модели OSI и более высоких уровнях.

Компьютерная сеть (Computer network). Совокупность компьютеров, устройств печати, сетевых устройств и программных средств, между которыми осуществляется передача информации по кабелям или при помощи радио и УКВ-волн.

Корпоративная сеть, сеть предприятия (Enterprise network). Объединение локальных, региональных или глобальных сетей, позволяющее пользователям компьютеров использовать многочисленные вычислительные и сетевые ресурсы для выполнения различных задач.

Локальная сеть (Local area network (LAN)). Совокупность взаимосвязанных компьютеров, устройств печати и другого сетевого оборудования, в которой аппаратные и программные средства используются совместно. Область обслуживания обычно ограничена пределами отдельного офиса, этажа или здания.

Магистраль (Backbone). Скоростная коммуникационная среда, соединяющая сети на одном или разных этажах здания или на удаленных расстояниях.

Маршрутизатор (Router). Сетевое устройство, соединяющее сети с одним или разными методами доступа и передающими средами (например, сети Ethernet и сеть с маркерным кольцом). Маршрутизатор пересылает пакеты и фреймы в соответствующие сети, для чего используется определенный метод принятия решений, основанный на данных таблицы маршрутизации, способах обнаружения наиболее эффективных маршрутов, а также параметрах, предварительно заданных сетевым администратором.

Межсетевой обмен, объединение сетей (Internetworking). Процесс соединения сетей как одного типа, так и сетей различных типов для обеспечения взаимного обмена информацией.

Мост (Bridge). Сетевое передающее устройство, соединяющее различные локальные сети или сегменты одной локальной сети, которые используют один и тот же метод доступа. Примером могут служить две локальные сети Ethernet, соединенные между собой. Мосты функционируют на Канальном уровне.

Пакет (Packet). Модуль данных, упакованных в виде, пригодном для передачи по сети, и содержащих управляющую и иную информацию. Соответствует Сетевому уровню модели OSI (Уровню 3).

Протокол (Protocol). Установленный регламент, определяющий способ форматирования сетевых данных в пакете или фрейме, механизм их передачи и методы интерпретации данных, полученных на принимающем узле.

Региональная сеть (Metropolitan area network (MAN)). Сеть, связывающая несколько локальных сетей в пределах большого города или значительной городской территории.

Сеть общего пользования (Public network). Сеть, предлагающая свои услуги всем членам некоторого сообщества (например, сетевые службы, предоставляемые телекоммуникационной компанией или компанией кабельного телевидения).

Топология (Topology). Физическая конфигурация кабеля и логические маршруты, по которым следуют сетевые пакеты, передаваемые по этому кабелю.

Транслирующий мост (Translation bridge). Мост между сетями, использующими различные транспортные протоколы, который может направлять трафик по этим протоколам в соответствующие сети.

Трансляция (Translation). Способ преобразования одного транспортного протокола в другой.

Фрейм (Frame). Этот термин иногда используется как эквивалент понятия "пакет" и обозначает блок данных, передаваемый по сети и содержащий управляющую и адресную информацию, соответствующую Канальному уровню модели OSI (Уровню 2).

Хост, (Host). Компьютер (мэйнфрейм, мини-ЭВМ, сервер или рабочая станция), имеющий операционную систему, позволяющую другим компьютерам одновременно обращаться к нему для получения доступа к файлам, данным и службам. Программы и обработка информации могут выполняться непосредственно на хосте или могут быть загружены для выполнения на клиентский компьютер, обращающийся к хосту. В другом значении "хост" – это любой компьютер, подключенный к сети.

Частная сеть (Private network). Сеть, принадлежащая некоторой организации и управляемая силами этой организации (например, университетская сеть, которую поддерживает один из колледжей).

Шлюз (Gateway). Сетевое устройство, обеспечивающее обмен информацией между сетевыми системами разного типа (например, между сложными протоколами или различными почтовыми системами).

Эмуляция терминала (Terminal emulation). Использование программных решений для того, чтобы компьютер (например, персональный) функционировал как терминал.

Вопросы:

1. Локальные компьютерные сети, базовые понятия
2. Определение типа сети
3. Причины, обусловившие появление локальных и глобальных сетей
4. История локальных и глобальных сетей
5. Какие аспекты из перечисленных вы рассматривали бы при проектировании корпоративной сети?
6. Какой из перечисленных типов сети охватывает наибольшие расстояния?
7. Какое устройство вы, скорее всего, использовали бы в качестве "дешевого" канала для передачи обычных данных и "дорогого" – для передачи мультимедиа?
8. Что было разработано раньше — TCP или IP, и что означают эти аббревиатуры?
9. Что дало основной импульс развитию Интернета в 1998 году?
10. Что такое "запрос на комментарии" (Request for Comment, RFC)?
11. Фрейм содержит информацию о получателе передаваемых цифровых данных, но не об их источнике. Верно это или нет?

Список литературы

Основная литература:

1. Новиков Ю.В. Основы локальных сетей [Электронный ресурс]/ Новиков Ю.В., Кондратенко С.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 405 с.— Режим доступа: <http://www.iprbookshop.ru/22425>.— ЭБС «IPRbooks», по паролю

Дополнительная литература

1. Построение коммутируемых компьютерных сетей / Е.В. Смирнова, И.В. Баскаков, А.В. Пролетарский, Р.А. Федотов. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 429 с. : схем., ил. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=429834>
2. Синицын Ю.И. Волоконно-оптические линии связи в компьютерных сетях и телекоммуникациях [Электронный ресурс]: методические указания к практическим и лабораторным занятиям/ Синицын Ю.И.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014.— 142 с.— Режим доступа: <http://www.iprbookshop.ru/50050>.— ЭБС «IPRbooks», по паролю

Интернет-ресурсы:

1. <http://www.intuit.ru> – сайт дистанционного образования в области информационных технологий
2. <http://www.iqlib.ru> - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия;
3. <http://www.biblioclub.ru> - электронная библиотечная система «Университетская библиотека – online»: специализируется на учебных материалах для ВУЗов по научно-гуманитарной тематике, а так же содержит материалы по точным и естественным наукам.
4. <http://window.edu.ru> – образовательные ресурсы ведущих вузов.
5. <http://algolist.manual.ru> - сайт, посвященный алгоритмам и методам.
6. <http://www.intuit.ru/> - Образовательный портал. Текстовые и видеолекции.
7. [www. http://bic.pfnctu.ru](http://bic.pfnctu.ru) Электронная библиотека СКФУ

Практическое занятие 2

Анализ пропускной способности каналов множественного доступа

Цель: Изучение основ способности каналов множественного доступа

Знать: Основные особенности способности каналов множественного доступа

Уметь: Применять знания в анализе пропускной способности каналов множественного доступа

Формируемые компетенции:

Код	Формулировка:
ОК-5	быть готовым работать с информацией в различных формах, использовать для ее получения, обработки, передачи, хранения и защиты современные компьютерные технологии
ОПК-7	способностью учитывать современные тенденции развития теории автоматического управления, электронного оборудования, измерительной и вычислительной техники, информационных технологий в профессиональной деятельности
ПК-12	способностью разрабатывать инструкции по эксплуатации используемого технического оборудования и программного обеспечения для обслуживающего персонала
ПК-13	способностью разрабатывать информационное обеспечение систем автоматизации и управления на основе современных технологий программирования
ПК-15	способностью использовать в разработках программно-технических комплексов современные технологии передачи данных и алгоритмы их обработки

Актуальность: аналитическое исследование в изучении особенностей сети Ethernet

Теоретическая часть: Анализ пропускной способности каналов множественного доступа

Методы обмена данными в локальных сетях

Для управления обменом (управления доступом к сети, арбитражу сети) используются различные методы, особенности которых в значительной степени зависят от топологии сети.

Метод доступа – это способ определения того, какая из рабочих станций сможет следующей использовать ЛВС. То, как сеть управляет доступом к каналу связи (кабелю), существенно влияет на ее характеристики.

1.Метод опроса

Обмен данными в ЛВС с топологией звезда с активным центром (центральным сервером). При данной топологии все станции могут решить передавать информацию серверу одновременно. Центральный сервер может производить обмен только с одной рабочей станцией. Поэтому в любой момент надо выделить только одну станцию, ведущую передачу.

Центральный сервер посылает запросы по очереди всем станциям. Каждая рабочая станция, которая хочет передавать данные (первая из опрошенных), посылает ответ или же сразу начинает передачу. После окончания сеанса передачи центральный сервер продолжает опрос по кругу. Станции, в данном случае, имеют следующие приоритеты: максимальный приоритет у той из них, которая ближе расположена к последней станции, закончившей обмен.

Обмен данными в сети с топологией шина. В этой топологии, возможно, такое же централизованное управление, как и в “звезде”. Один из узлов (центральный) посылает всем остальным запросы, выясняя, кто хочет передавать, и затем разрешает передачу тому из них, кто после окончания передачи сообщает об этом.

2. Множественный доступ с передачей полномочия (Token Passing Multiple Access – TPMA) или метод передачи полномочий (передача маркера).

Маркер (token), или полномочие - уникальная комбинация битов, позволяющая начать передачу данных, это служебный пакет определенного формата, в который клиенты могут помещать свои информационные пакеты, он может быть свободным или занятым.

Последовательность передачи маркера по сети от одной рабочей станции к другой задается сервером. Данный метод доступа для сетей с шинной и звездной топологией обеспечивается протоколом ArcNet.

Метод с передачей маркера – это метод доступа к среде, в котором от рабочей станции к рабочей станции передается маркер, дающий разрешение на передачу сообщения. При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит это сообщение по сети. Каждая станция между передающей станцией и принимающей видит это сообщение, но только станция – адресат принимает его. При этом она создает новый маркер.

Алгоритм передачи следующий:

1. Узел, желающий передать, ждет свободный маркер, получив который помечает его как занятый (изменяет соответствующие биты), добавляет к нему свой пакет и результат отправляет дальше в кольцо.

2. Каждый узел, получивший такой маркер, принимает его, проверяет, ему ли адресован пакет.

3. Если пакет адресован этому узлу, то узел устанавливает в маркере специально выделенный бит подтверждения и отправляет измененный маркер с пакетом дальше.

4. Передававший узел получает обратно свою посылку, прошедшую через все кольцо, освобождает маркер (помечает его как свободный) и снова посылает маркер в сеть. При этом передававший узел знает, была ли получена его посылка или нет.

Для нормального функционирования данной сети необходимо, чтобы один из компьютеров или специальное устройство следило за тем, чтобы маркер не потерялся, а в случае пропажи маркера данный компьютер должен создать его и запустить в сеть.

Алгоритм множественного доступа с передачей полномочия, или маркера, приведен на рис. 3.5.

Каждый узел принимает пакет от предыдущего, восстанавливает уровни сигналов до номинального уровня и передает дальше. Передаваемый пакет может содержать данные или являться маркером. Когда рабочей станции необходимо передать пакет, ее адаптер дожидается поступления маркера, а затем преобразует его в пакет, содержащий данные, отформатированные по протоколу соответствующего уровня, и передает результат далее по ЛВС.

Пакет распространяется по ЛВС от адаптера к адаптеру, пока не найдет своего адресата, который установит в нем определенные биты для подтверждения того, что данные достигли адресата, и ретранслирует его вновь в ЛВС. После чего пакет возвращается в узел, из которого был отправлен. Здесь после проверки безошибочной передачи пакета, узел освобождает ЛВС, выпуская новый маркер.

Таким образом, в ЛВС с передачей маркера невозможны коллизии (конфликты). Метод с передачей маркера в основном используется в кольцевой топологии.

Данный метод характеризуется следующими достоинствами:

- гарантирует определенное время доставки блоков данных в сети;
- дает возможность предоставления различных приоритетов передачи данных.

Вместе с тем он имеет существенные недостатки:

- в сети возможны потеря маркера, а также появление нескольких маркеров, при этом сеть прекращает работу;
- включение новой рабочей станции и отключение связаны с изменением адресов всей системы.

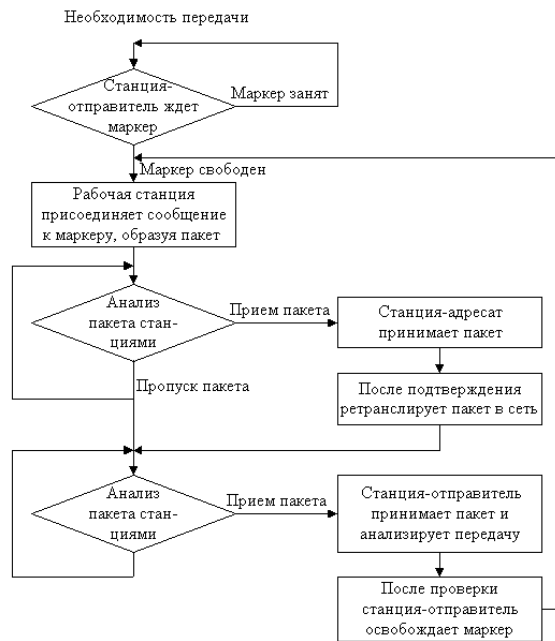


Рис. 3.5. Алгоритм TRMA

3. Метод множественного доступа с контролем несущей и обнаружением коллизий (столкновений) (CSMA/CD).

Метод множественного доступа с контролем (прослушиванием) несущей и обнаружением (разрешением) коллизий (CSMA/CD) устанавливает следующий порядок: если рабочая станция хочет воспользоваться сетью для передачи данных, она сначала должна проверить состояние канала, то есть начинать передачу станция может, если канал свободен. В процессе передачи станция продолжает прослушивание сети для обнаружения возможных конфликтов. Если возникает конфликт из-за того, что два узла попытаются занять канал, то обнаружившая конфликт интерфейсная плата, выдает в сеть специальный сигнал, и обе станции одновременно прекращают передачу. Принимающая станция отбрасывает частично принятое сообщение, а все рабочие станции, желающие передать сообщение, в течение некоторого, случайно выбранного промежутка времени выжидают, прежде чем начать сообщение.

Алгоритм множественного доступа с прослушиванием несущей и разрешением коллизий приведен на рис. 3.6. Суть алгоритма в следующем:

1. Узел, желающий передавать информацию, следит за состоянием сети, и как только она освободится, то начинает передачу.

2. Узел передает данные и одновременно контролирует состояние сети (контролем несущей и обнаружением коллизий). Если столкновений не обнаружилось, передача доводится до конца.

3. Если столкновение обнаружено, то узел усиливает его (передает еще некоторое время) для гарантии обнаружения всеми передающими узлами, а затем прекращает передачу. Также поступают и другие передававшие узлы.

4. После прекращения неудачной попытки узел выдерживает случайно выбираемый промежуток времени $t_{\text{зад}}$, а затем повторяет свою попытку передать, при этом контролируя столкновения. При повторном столкновении $t_{\text{зад}}$ увеличивается. В конечном счете, один из узлов опережает другие узлы и успешно передает данные. Метод CSMA/CD часто называют методом состязаний. Этот метод для сетей с шиной топологией реализуется протоколом Ethernet.

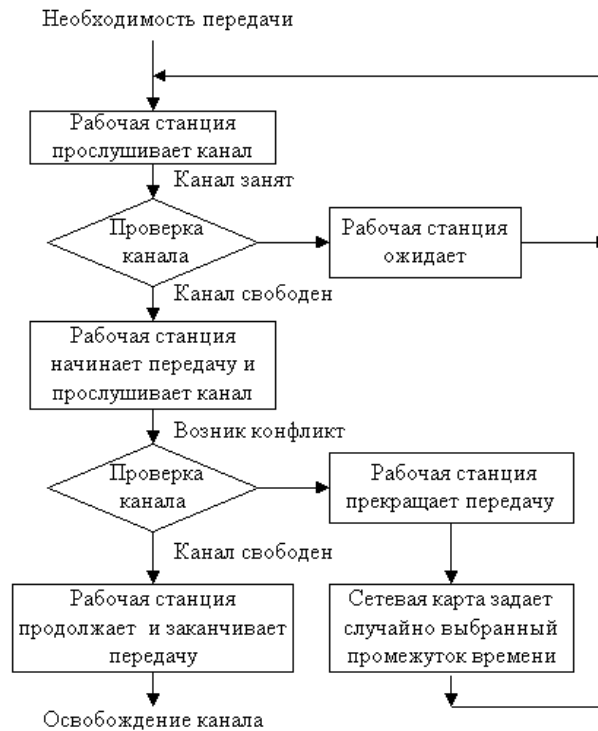


Рис. 3.6. Алгоритм CSMA/CD

4. Множественный доступ с разделением во времени (Time Division Multiple Access – TDMA).

Множественный доступ с разделением во времени основан на распределении времени работы канала между системами (рис. 3.7).

Доступ TDMA основан на использовании специального устройства, называемого тактовым генератором. Этот генератор делит время канала на повторяющиеся циклы. Каждый из циклов начинается сигналом Разграничителем. Цикл включает n пронумерованных временных интервалов, называемых ячейками. Интервалы предоставляются для загрузки в них блоков данных.

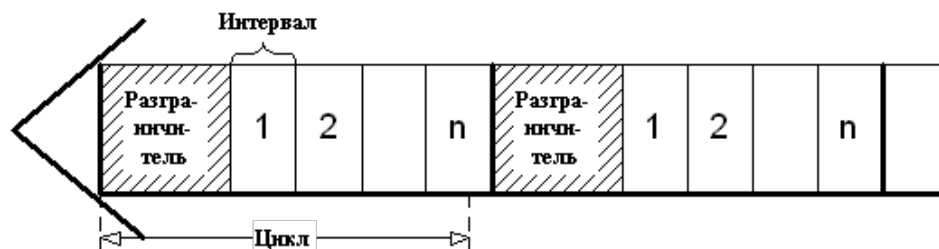


Рис. 3.7. Структура множественного доступа с разделением во времени

Данный способ позволяет организовать передачу данных с коммутацией пакетов и с коммутацией каналов.

Первый (простейший) вариант использования интервалов заключается в том, что их число (n) делается равным количеству абонентских систем, подключенных к рассматриваемому каналу. Тогда во время цикла каждой системе предоставляется один интервал, в течение которого она может передавать данные. При использовании рассмотренного метода доступа часто оказывается, что в одном и том же цикле одним системам нечего передавать, а другим не хватает выделенного времени. В результате неэффективное использование пропускной способности канала.

Второй, более сложный, но высокоэкономичный вариант заключается в том, что система получает интервал только тогда, когда у нее возникает необходимость в передаче

данных, например при асинхронном способе передачи. Для передачи данных система может в каждом цикле получать интервал с одним и тем же номером. В этом случае передаваемые системой блоки данных появляются через одинаковые промежутки времени и приходят с одним и тем же временем запаздывания. Это режим передачи данных с имитацией коммутации каналов. Способ особенно удобен при передаче речи.

5. Множественный доступ с разделением частоты (Frequency Division Multiple Access – FDMA) или множественный доступ с разделением длины волны (Wavelength Division Multiple Access – WDMA).

Доступ FDMA основан на разделении полосы пропускания канала на группу полос частот (рис. 3.8), образующих логические каналы.

Широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. Размеры узких полос могут быть различными.

При использовании FDMA, именуемого также множественным доступом с разделением волны WDMA, широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. В каждой узкой полосе создается логический канал. Размеры узких полос могут быть различными. Передаваемые по логическим каналам сигналы накладываются на разные несущие и поэтому в частотной области не должны пересекаться. Вместе с этим, иногда, несмотря на наличие защитных полос, спектральные составляющие сигнала могут выходить за границы логического канала и вызывать шум в соседнем логическом канале.

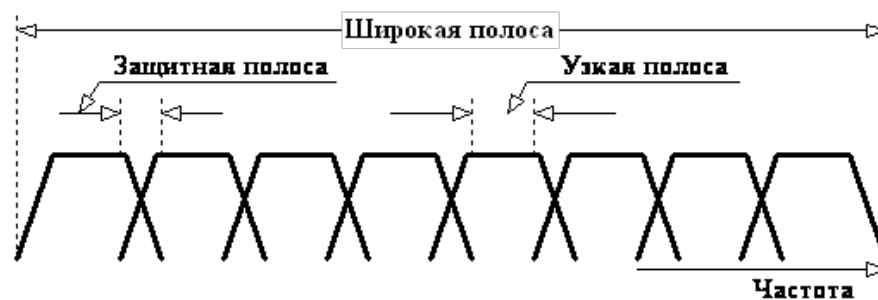


Рис. 3.8. Схема выделения логических каналов

В оптических каналах разделение частоты осуществляется направлением в каждый из них лучей света с различными частотами. Благодаря этому пропускная способность физического канала увеличивается в несколько раз. При осуществлении этого мультиплексирования в один световод излучает свет большое число лазеров (на различных частотах). Через световод излучение каждого из них проходит независимо от другого. На приемном конце разделение частот сигналов, прошедших физический канал, осуществляется путем фильтрации выходных сигналов.

Метод доступа FDMA относительно прост, но для его реализации необходимы передатчики и приемники, работающие на различных частотах.

Вопросы:

1. Методы обмена данными в локальных сетях
 2. Метод опроса
 3. Множественный доступ с передачей полномочия (Token Passing Multiple Access – TPMA) или метод передачи полномочий (передача маркера).
 4. Метод множественного доступа с контролем несущей и обнаружением коллизий (столкновений) (CSMA/CD).
 5. Множественный доступ с разделением во времени (Time Division Multiple Access – TDMA).
 6. Множественный доступ с разделением частоты (Frequency Division Multiple Access – FDMA) или множественный доступ с разделением длины волны
- Список литературы

Основная литература:

1. Новиков Ю.В. Основы локальных сетей [Электронный ресурс]/ Новиков Ю.В., Кондратенко С.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 405 с.— Режим доступа: <http://www.iprbookshop.ru/22425>.— ЭБС «IPRbooks», по паролю

Дополнительная литература

1. Построение коммутируемых компьютерных сетей / Е.В. Смирнова, И.В. Баскаков, А.В. Пролетарский, Р.А. Федотов. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 429 с. : схем., ил. ; То же [Электронный ресурс]. - URL: [//biblioclub.ru/index.php?page=book&id=429834](http://biblioclub.ru/index.php?page=book&id=429834)

2. Сеницын Ю.И. Волоконно-оптические линии связи в компьютерных сетях и телекоммуникациях [Электронный ресурс]: методические указания к практическим и лабораторным занятиям/ Сеницын Ю.И.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014.— 142 с.— Режим доступа: <http://www.iprbookshop.ru/50050>.— ЭБС «IPRbooks», по паролю

Интернет-ресурсы:

1.<http://www.intuit.ru> — сайт дистанционного образования в области информационных технологий

2.<http://www.iqlib.ru> - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия;

3.<http://www.biblioclub.ru> - электронная библиотечная система «Университетская библиотека – online»: специализируется на учебных материалах для ВУЗов по научно-гуманитарной тематике, а так же содержит материалы по точным и естественным наукам.

4.<http://window.edu.ru> – образовательные ресурсы ведущих вузов.

5.<http://algolist.manual.ru> - сайт, посвященный алгоритмам и методам.

6.<http://www.intuit.ru/> - Образовательный портал. Текстовые и видеолекции.

7.[www. http://bic.pfnctu.ru](http://bic.pfnctu.ru) Электронная библиотека СКФУ

Практическое занятие 3

Эталонная модель взаимодействия открытых систем (Модель OSI)

Цель: Изучение Топология и способ построения компьютерной сети

Знать: Основные способы построения компьютерных сетей

Уметь: Применять методы топологии и способы построения компьютерных сетей.

Формируемые компетенции:

Код	Формулировка:
ОК-5	быть готовым работать с информацией в различных формах, использовать для ее получения, обработки, передачи, хранения и защиты современные компьютерные технологии
ОПК-7	способностью учитывать современные тенденции развития теории автоматического управления, электронного оборудования, измерительной и вычислительной техники, информационных технологий в профессиональной деятельности
ПК-12	способностью разрабатывать инструкции по эксплуатации используемого технического оборудования и программного обеспечения для обслуживающего персонала
ПК-13	способностью разрабатывать информационное обеспечение систем автоматизации и управления на основе современных технологий программирования
ПК-15	способностью использовать в разработках программно-технических комплексов современные технологии передачи данных и алгоритмы их обработки

Актуальность: аналитического исследование в топологических способах построения компьютерных сетей

Теоретическая часть:

Взаимодействие локальных и глобальных сетей

Эталонная модель взаимодействия открытых систем OSI

Без соответствующих стандартов сетевые коммуникации представляли бы собой неупорядоченный набор частных протоколов и устройств, созданных различными производителями с использованием разных концепций и моделей.

К счастью, объединение локальных и глобальных сетей с первых шагов выполнялось в соответствии с некоторой идеологией, называемой *эталонной моделью взаимодействия открытых систем* (Open Systems Interconnection, OSI). Модель OSI является детищем двух регламентирующих организаций: *Международной организации по стандартизации* (International Organization for Standardization, ISO) и *Национального института стандартизации США* (American National Standards Institute, ANSI).

Модель OSI, разработанная в 1974 году, регламентирует взаимодействие локальных и глобальных сетей и представляет собой попытку стандартизации сетевых программных и аппаратных средств.

На протяжении многих лет модель OSI способствовала развитию сетевых коммуникаций, позволяющих решать следующие вопросы:

- обеспечение передачи информации между различными типами локальных и глобальных сетей;
- стандартизация сетевого оборудования, что позволяет устройствам одного производителя взаимодействовать с устройствами других производителей;
- обеспечение возможности взаимодействия старого сетевого оборудования с новыми устройствами; при этом устраняется необходимость замены оборудования при установке новых устройств;
- разработка программного и аппаратного обеспечения, использующего общие

интерфейсы для передачи данных как внутри сети, так и между различными сетями;

Появление модели OSI предшествовало созданию большинства современных сетевых устройств, однако она явилась основой для разработки идей межсетевого обмена и постоянно развивается, впитывая в себя новые сетевые технологии.

Нормативы OSI описывают следующие моменты:

- как сетевые устройства общаются друг с другом и как взаимодействуют устройства, использующие разные протоколы;
- каким образом сетевое устройство узнает, когда можно и когда нельзя передавать данные;
- способы организации и физического соединения сетевых устройств;
- методы обеспечения правильности передачи данных по сети;
- способы поддержания непрерывного потока данных в сетевых устройствах;
- способы представления данных в виде электрических сигналов при передаче по сетевой среде.

Как показано на рис. 1, модель OSI состоит из семи отдельных уровней, расположенных один поверх другого:

- Физический;
- Канальный;
- Сетевой;
- Транспортный;
- Сеансовый;
- Представительский;
- Прикладной.

Каждый уровень выполняет определенные коммуникационные задачи и с помощью соответствующих протоколов взаимодействует с соседними уровнями иерархии. Передача информации между двумя сетевыми устройствами осуществляется с использованием этой иерархии уровней (стека) в каждом из устройств. Например, если рабочая станция обменивается данными с сервером, передача информации начинается в рабочей станции на Прикладном уровне. Затем формируется определенная информация на более нижних уровнях до тех пор, пока данные не достигнут Физического уровня и не будут по сети переданы серверу. Сервер принимает данные на Физическом уровне своего стека и передает их для интерпретации более высоким уровням, пока данные не достигнут Прикладного уровня. Каждый уровень называется либо по имени, либо по положению в стеке (1-й уровень, 2-й уровень и т. д.). Например, нижний уровень стека называется Физическим уровнем или Уровнем 1.

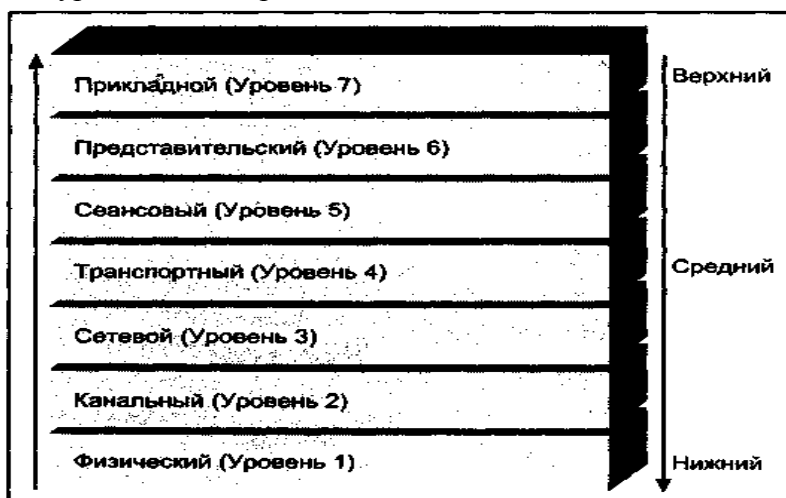


Рисунок 1– Уровни модели OSI

Нижние уровни стека выполняют функции, относящиеся к передаче физического сигнала (например, они создают фреймы и передают сигналы, содержащие пакеты данных). Средние уровни координируют сетевые коммуникации между узлами (например, обеспечивают бесперебойное и безошибочное осуществление сеанса связи). Верхние

уровни выполняют задачи, непосредственно влияющие на прикладные программы и представление данных, включая форматирование и шифрование информации, а также управление передачей файлов. В совокупности набор уровней называется *стеком*.

Физический уровень (1)

Самый нижний из уровней модели OSI называется *Физическим уровнем* (physical layer). Этот уровень описывает:

- все физические среды передачи данных (кабель, оптоволокно, волны радио и других диапазонов);
- сетевые разъемы;
- топологию сети;
- методы передачи и кодирования сигнала;
- устройства передачи данных;
- сетевые интерфейсы;
- методы распознавания ошибок при передаче сигналов.

Устройства, используемые на Физическом уровне, отвечают за генерирование, передачу и распознавание электрических сигналов, предназначенных для передачи и приема данных. Сетевые сигналы могут быть представлены в аналоговом или цифровом виде. Аналоговые сигналы используются в глобальных сетях, где для передачи данных применяются аналоговые модемы. Например, с помощью такого модема пользователь может подключиться к Интернету через поставщика услуг Интернета (интернет-провайдера). Аналоговый сигнал изображен на рис. 2.

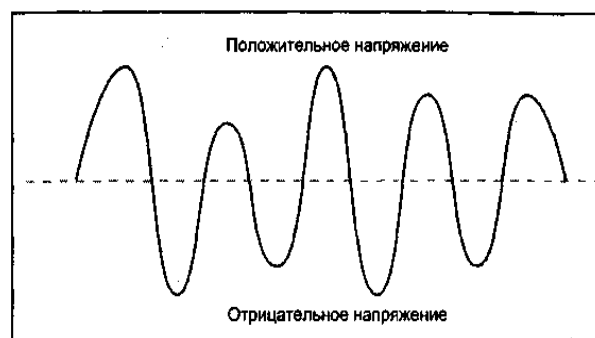


Рисунок 2 – Аналоговый сигнал

В *цифровом* сигнале для представления единиц и нулей используются фиксированные уровни напряжения. Такие сигналы чаще всего используются в локальных и скоростных глобальных сетях. Например, наличие напряжения +5 вольт может трактоваться как единица, а нулевое напряжение – как ноль (что проиллюстрировано на рис. 3). Другой путь для представления единиц и нулей – использование некоторого положительного напряжения (скажем, +5 вольт) для передачи единиц и отрицательного напряжения (например, -5 вольт) для передачи нулей. В оптоволоконных каналах двоичные единицы и нули обозначаются наличием или отсутствием света. Все названные варианты показаны на рис. 3.

Кодируемый сигнал преобразуется в двоичный формат (система счисления с основанием 2), имеющий определенное значение для компьютера или сетевого устройства. В сетях чаще всего используется метод, называемый *манчестерским кодированием* (Manchester encoding), при котором двоичная единица представлена переходом от низкого уровня сигнала к высокому, а двоичный ноль соответствует переходу сигнала от высокого к низкому.

Физический уровень управляет скоростью передачи данных, анализом потока ошибок и уровнями напряжения, используемыми для передачи сигнала. На его работу влияют физические проблемы в сети, например, разрывы передающего кабеля или электромагнитные наводки. Наводки могут создаваться близко расположенными

электромоторами, линиями высокого напряжения, осветительными и другими электрическими приборами.

Электромагнитное излучение и радиопомехи - вот два источника ошибок физического уровня.

Понимание концепций Физического уровня особенно важно при работе с сетями, поскольку ошибки именно на этом уровне зачастую мешают правильной работе сети.

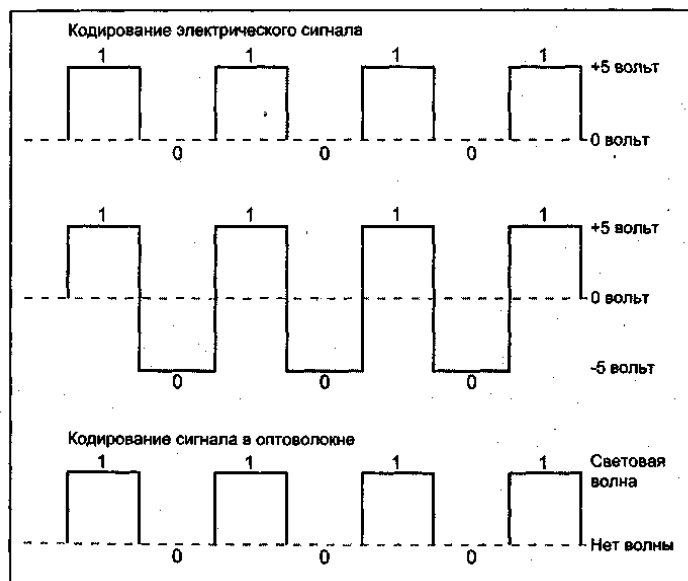


Рисунок 3 – Примеры цифровых сигналов

Канальный уровень (2)

Задача *Канального уровня* (data link layer) в локальной сети – компоновать передаваемые биты данных в виде фреймов, или кадры (frame). Каждый фрейм определенным образом форматирован – так, чтобы для надежной передачи данных от узла к узлу информационные пакеты были упорядочены. Этот уровень кодирует данные в виде фреймов, после чего отформатированные фреймы поступают на Физический уровень, где передающий узел может отправить их в коммуникационную среду (например, в кабель). Принимающий узел получает фрейм от Физического уровня, декодирует электрический сигнал, представляющий разряды данных, преобразует отдельные разряды во фрейм и проверяет наличие ошибок во фрейме.

Канальный уровень представляет информационные разряды в виде «фрейма» канального уровня, который содержит поля с адресной и управляющей информацией. Таким образом, фрейм содержит:

- признак начала фрейма (start of frame, SOF);
- адрес устройства или передающего узла, отправляющего фрейм (адрес источника);
- адрес устройства или принимающего узла, получающего переданный фрейм (адрес назначения);
- административную или управляющую информацию (для контроля коммуникационного процесса);
- данные;
- информацию для обнаружения ошибок (контрольные данные);
- трейлер (концевик) или признак конца фрейма (end of frame, EOF).

На Канальном уровне выполняется проверка входящих сигналов, а также обнаруживаются повторно, неправильно или частично переданные данные во входящем потоке. При обнаружении ошибок уровень запрашивает у передающего узла повторную передачу данных – фрейм за фреймом. Для обнаружения ошибок на Канальном уровне используется *контроль циклическим избыточным кодом* (cyclic redundancy check, CRC).

Канальный уровень обеспечивает очередность фреймов – т. е. они должны передаваться в том же порядке, в котором и принимаются.

Канальный уровень содержит два важных подуровня: более высокий - *управление логическим соединением* (logical link control, LLC) и более низкий - *протокол управления доступом к передающей среде* (media access control, MAC). Подуровень LLC обеспечивает надежность коммуникаций путем установки канала передачи данных между двумя узлами и поддержки устойчивости этого канала. Подуровень MAC распознает *физический адрес* (или *адрес устройства*) иногда называемый *MAC-адресом*, содержащийся в каждом фрейме (уникальный адрес, "защитый" в микросхему сетевого интерфейса. Этот адрес представлен некоторым шестнадцатеричным числом (например, 0004AC8428DE).)

Сетевой уровень (3)

Третьим уровнем стека является *Сетевой уровень* (network layer). Этот уровень управляет прохождением пакетов по сети. Все сети содержат физические маршруты передачи информации (кабельные тракты) и логические маршруты (программные тракты). Сетевой уровень анализирует адресную информацию протокола передачи пакетов и посылает их по наиболее подходящему маршруту – физическому или логическому, обеспечивая максимальную эффективность сети. Также этот уровень обеспечивает пересылку пакетов между сетями через маршрутизаторы.

Контролируя прохождение пакетов, Сетевой уровень выступает в роли "управляющего трафиком": он маршрутизирует (направляет) пакеты по наиболее эффективному из нескольких возможных трактов передачи данных. Для определения наилучшего маршрута Сетевой уровень постоянно собирает информацию (метрики) о расположении различных сетей и узлов, этот процесс называется *обнаружением маршрута* (discovery).

Примечание

Сетевой уровень может направлять данные по разным маршрутам, создавая виртуальные каналы (circuit). *Виртуальные каналы* (virtual circuit) представляют собой логические коммуникационные линии для передачи и приема данных. Виртуальные каналы, представленные только на сетевом уровне, образуются между сетевыми узлами, обменивающимися информацией..

Транспортный уровень (4)

Транспортный уровень (transport layer) – подобно Канальному и Сетевому уровням – выполняет функции, обеспечивающие надежную пересылку данных от передающего узла к принимающему. Например, Транспортный уровень гарантирует, что данные передаются и принимаются в одном и том же порядке. Кроме этого, по завершении пересылки принимающий узел может послать подтверждение (иногда называемое квитанцией).

Когда в сети используются виртуальные каналы, Транспортный уровень отслеживает уникальные идентификаторы, назначенные каждому каналу. Эти значения называются портами, идентификаторами соединения или сокетами; они назначаются Сеансовым уровнем. Также Транспортный уровень обеспечивает проверку пакетов. При этом на самом верхнем уровне контроля гарантируется безошибочная передача пакетов от узла к узлу в заданный промежуток времени.

Еще одной функцией Транспортного уровня является деление посылаемых сообщений на более мелкие фрагменты в тех случаях, когда в сетях используются разные протоколы с отличающимися размерами пакетов. Данные, разбитые на мелкие блоки Транспортным уровнем передающей сети, собираются в правильном порядке Транспортным уровнем принимающей стороны и интерпретируются Сетевым уровнем.

Именно Транспортный уровень обеспечивает получение каждого пакета или фрейма без потерь. Задача Транспортного уровня - обеспечить такую скорость передачи информации, чтобы не было ее потерь. Транспортный уровень также может регулировать размер "окон" данных, передаваемых между сигналами подтверждения приема, в результате чего объем переданных данных за единицу времени может увеличиться.

Сеансовый уровень (5)

Сеансовый уровень (session layer) отвечает за установление и поддержку коммуникационного канала между двумя узлами, он обеспечивает очередность работы узлов: например, определяет, какой из узлов первым начинает передачу данных. Помимо этого, Сеансовый уровень определяет продолжительность работы узла на передачу, а также способ восстановления информации после ошибок передачи. Если сеанс связи был ошибочно прерван на более низком уровне, Сеансовый уровень пытается восстановить передачу данных.

Подобно тому, как почтовый индекс связан с некоторым географическим районом, Сеансовый уровень ассоциирует с каждым узлом уникальный адрес. По окончании сеанса связи этот уровень отключает узлы.

Примером связи на Сеансовом уровне может быть подключение рабочей станции к некоторому серверу Интернета. Станция и сервер имеют уникальные адреса протокола Интернета (IP) (например, 122.72.15.122 и 145.19.20.22). Сеансовый уровень использует эти адреса для установки соединения между узлами. После того как подключение осуществлено, и рабочая станция зарегистрировалась на сервере, на данном уровне устанавливается сеанс передачи данных.

Представительский уровень (6)

Представительский уровень (presentation layer) управляет форматированием данных, поскольку прикладные программы нередко используют различные способы представления информации. Он гарантирует, что числа и символьные строки передаются именно в том формате, который понятен Представительскому уровню принимающего узла.

Также Представительский уровень отвечает за шифрование данных. *Шифрование* (encryption) – это такой процесс засекречивания информации, который не позволяет неавторизованным пользователям прочесть данные в случае их перехвата.

Еще одной функцией Представительского уровня является сжатие данных

После их форматирования между символьными строками и числами может оставаться свободное место. При сжатии информации эти промежутки удаляются, в результате чего требуется значительно меньше времени на передачу более компактных данных. После пересылки Представительский уровень принимающего узла выполняет декомпрессию данных.

Прикладной уровень (7)

Прикладной уровень (application layer). Этот уровень непосредственно управляет доступом к приложениям к сетевым службам. Примером таких служб являются передача файлов, управление файлами, удаленный доступ к файлам и принтерам, управление сообщениями электронной почты и эмуляция терминалов. Именно этот уровень программисты используют для связи рабочих станций с сетевыми службами (например, для предоставления некоторой программе услуг электронной почты или доступа к базе данных через сеть).

На Прикладном уровне работает *редиректор* (redirector) систем Microsoft Windows. Редиректор – это служба, позволяющая видеть компьютер в сети и обращаться к нему. Если в сети Microsoft разрешается общий доступ к некоторой папке, то при помощи редиректора другие компьютеры могут видеть эту папку и использовать ее.

Многие широко используемые компьютерные программы реализованы благодаря наличию Прикладного уровня. Всякий раз, когда вы запускаете веб-браузер (например, Microsoft Internet Explorer или Netscape Communicator) или же посылаете сообщение по электронной почте, вы работаете с Прикладным уровнем.

В табл. 1 представлены функции каждого из семи уровней модели OSI. На рисунке 4 показана передача информации с использованием эталонной модели OSI.

Взаимодействие между стеками протоколов

Для того чтобы два компьютера могли взаимодействовать между собой в локальной или глобальной сети, они оба должны использовать одну и ту же модель коммуникаций (например, модель OSI). Эта модель определяет стандарты взаимодействия как внутри

локальной сети, так и при передаче данных между локальными сетями, между локальной и глобальными сетями, а также между глобальными сетями

Таблица 1. – Функции уровней эталонной модели OSI

Уровень	Функции
Физический (Уровень 1)	Реализует физическую среду передачи сигнала (например, кабельную систему) Преобразует данные в передаваемый сигнал, соответствующий физической среде Посылает сигнал по физической среде Распознает физическую структуру сети Обнаруживает ошибки передачи Определяет уровни напряжения, используемые для передачи цифровых сигналов и синхронизации передаваемых пакетов Определяет тип сигнала - цифровой или аналоговый
Канальный (Уровень 2)	Образует фреймы данных соответствующего формата с учетом типа сети Генерирует контрольные суммы Обнаруживает ошибки, проверяя контрольные суммы Повторно посылает данные при наличии ошибок Инициализирует канал связи и обеспечивает его бесперебойную работу, что гарантирует физическую надежность коммуникаций между узлами Анализирует адреса устройств Подтверждает прием фреймов
Сетевой (Уровень 3)	Определяет сетевой маршрут для передачи пакетов Позволяет уменьшить вероятность перегруженности сети Реализует виртуальные каналы (маршруты) Маршрутизирует пакеты в другие сети, при необходимости переупорядочивая передаваемые пакеты Выполняет преобразования между протоколами
Транспортный (Уровень 4)	Обеспечивает надежность передачи пакетов между узлами Обеспечивает правильный порядок передачи и приема пакетов данных Подтверждает прием пакета Отслеживает ошибки передачи пакетов и повторно посылает плохие пакеты Разбивает большие фрагменты данных и собирает их на приемном узле в сетях, использующих разные протоколы
Сеансовый (Уровень 5)	Инициализирует канал связи Проверяет состояние установленного канала связи В каждый момент времени определяет очередность работы узлов, (например, какой узел первым начинает передачу данных) Разрывает канал по окончании сеанса связи Преобразует адреса узлов
Представительский (Уровень 6)	Преобразует данные в формат, понятный для принимающего узла (например, перекодирует символы EBCDIC в ASCII) Выполняет шифрование данных Выполняет сжатие данных
Прикладной (Уровень 7)	Обеспечивает совместный доступ к удаленным дискам Обеспечивает совместный доступ к удаленным принтерам Обрабатывает сообщения электронной почты Обеспечивает работу служб передачи файлов Обеспечивает работу служб управления файлами Обеспечивает работу служб эмуляции терминалов

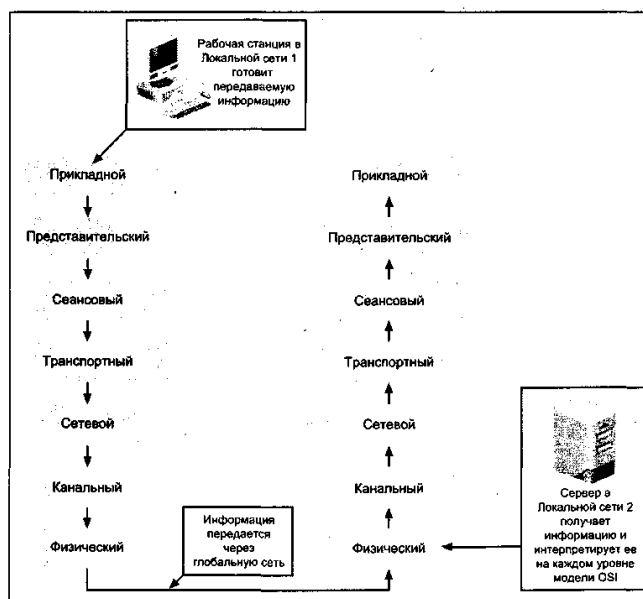


Рисунок 4 – Передача информации с использованием эталонной модели OSI

Между уровнями информация передается при помощи команд, называемых *примитивами* (primitive) (рис. 5). Передаваемая информация называется *протокольной единицей обмена* или *модулем данных протокола* (protocol data unit, PDU). Когда данные поступают от одного уровня к другому (более высокому или более низкому), к модулю PDU добавляется новая управляющая информация. После того как на некотором уровне сформирован модуль PDU, он пересылается аналогичному уровню взаимодействующего узла с помощью одноранговых протоколов (рис. 6). Вместе с тем, когда модуль PDU готов к передаче следующему уровню, предыдущий уровень добавляет к этому модулю команды пересылки.

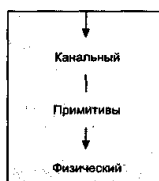


Рисунок 5 – Взаимодействие между уровнями с применением примитивов

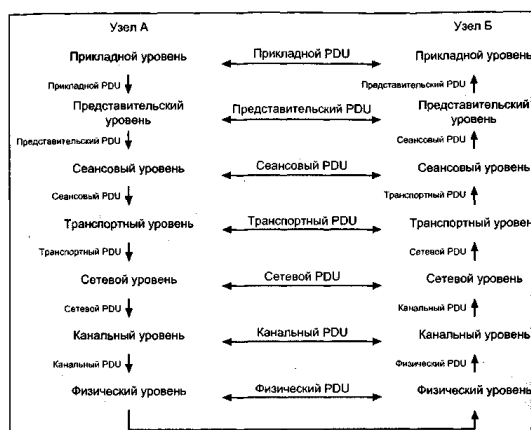


Рисунок 6 – Пример передачи информации

Взаимодействие между уровнями с использованием модулей PDU

После того как модуль PDU принимается следующим уровнем, управляющая информация и команды пересылки отбрасываются. Полученный называется *модулем данных службы* (service data unit, SDU). В процессе пересылки модуля SDU от одного уровня к следующему каждый уровень добавляет к модулю свою управляющую информацию.

На каждом уровне OSI для получения модуля PDU к нужному модулю SDU добавляются управляющая информация и команды пересылки. Если, например, модуль PDU формируется на некотором уровне компьютера А, то затем он пересылается этому же уровню компьютера Б. Если же на компьютере А проходит взаимодействие между уровнями стека, то модуль PDU передается следующему уровню стека, расположенному ниже. Управляющая информация и команды пересылки удаляются из модуля PDU, остается только модуль SDU, после чего добавляется новая управляющая информация.

Таблица 2. Сетевые аппаратные и программные средства, связанные с различными уровнями модели OSI

Уровень OSI	Сетевые аппаратные и программные средства
Прикладной	Прикладные программные интерфейсы, браузеры Интернета, программы передачи сообщений и электронной почты, программы удаленного доступа к компьютерам и шлюзы
Представительский	Программы преобразования и шифрования данных, программы форматирования графики (например, для преобразования в GIF- и JPG-файлы), а также шлюзы
Сеансовый	Программные драйверы сетевого оборудования, программное обеспечение для поиска имен компьютеров, средства для полу- и полнодуплексного режима работы, средства удаленного вызова процедур (RPC) для запуска программ на удаленном компьютере, а также шлюзы
Транспортный	Программные драйверы сетевого оборудования, программы и средства управления потоком данных, а также шлюзы
Сетевой	Шлюзы, маршрутизаторы, протоколы маршрутизации, мосты с исходными маршрутами и коммутаторы Уровня 3
Канальный	Сетевые адаптеры, интеллектуальные концентраторы и мосты, коммутаторы Уровня 2 и шлюзы
Физический	Кабельная система, кабельные разъемы, мультиплексоры, трансмиттеры и ресиверы, пассивные и активные концентраторы, репитеры и шлюзы

Успешно функционирующие локальные сети следуют рекомендациям, установленным моделью OSI.

Две основных характеристики локальной сети – *тип (топология)* сети и *методы передачи* данных – являются обязательными критериями, подтверждающими, что сети соответствуют стандартам.

Выводы

Данное занятие знакомит с идеологией объединения локальных и глобальных сетей, для чего подробно рассматривается эталонная модель взаимодействия открытых систем – OSI (Open Systems Interconnection). Без этой модели, устанавливающей разработанные более 20 лет назад стандарты для локальных и глобальных сетей, современные сетевые коммуникации были бы в состоянии хаоса и возможностей межсетевого общения было бы гораздо меньше.

Взаимодействие локальных и глобальных сетей является быстроразвивающейся областью техники, что объясняется жесткой конкуренцией между компаниями, работающими в трех следующих секторах промышленности: телекоммуникации, кабельное телевидение и

спутниковые средства связи. Быстрый рост этих отраслей увеличил возможности совместного использования информации, доступной через сети и Интернет. Например, пользователь, живущий в небольшом городе, может подключаться к Интернету по телефонной линии, с помощью спутниковой "тарелки" или входа кабельного телевидения. Много дополнительных возможностей появляется при соединении локальных сетей, находящихся в разных странах или частях света.

Телекоммуникационные компании могут обеспечить связь локальных сетей через глобальную сеть, используя для этого междугородные высокоскоростные телефонные линии. Глобальные сети строятся на основе радио, радиорелейных (СВЧ) и спутниковых каналов. Жесткая конкуренция между поставщиками услуг глобальных сетей приводит к быстрому появлению новых возможностей передачи данных.

Вопросы:

1. Объяснить эталонную модель OSI, устанавливающую стандарты взаимодействия локальных и глобальных сетей;
2. Объяснить процесс передачи информации между стеками OSI для компьютеров, объединенных в сеть;
3. Применять модель OSI в реальных сетевых конфигурациях;
4. Описать типы сетей с точки зрения топологии локальных сетей;
5. Описать основные методы передачи данных в локальных сетях, включая Ethernet, Token Ring и FDDI;
6. Понимать основные топологии глобальных сетевых коммуникаций и методы передачи данных, включая каналы телекоммуникации и кабельного телевидения, спутниковые технологии.

Список литературы

Основная литература:

1. Новиков Ю.В. Основы локальных сетей [Электронный ресурс]/ Новиков Ю.В., Кондратенко С.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 405 с.— Режим доступа: <http://www.iprbookshop.ru/22425>.— ЭБС «IPRbooks», по паролю

Дополнительная литература

1. Построение коммутируемых компьютерных сетей / Е.В. Смирнова, И.В. Баскаков, А.В. Пролетарский, Р.А. Федотов. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 429 с. : схем., ил. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=429834>
2. Сеницын Ю.И. Волоконно-оптические линии связи в компьютерных сетях и телекоммуникациях [Электронный ресурс]: методические указания к практическим и лабораторным занятиям/ Сеницын Ю.И.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014.— 142 с.— Режим доступа: <http://www.iprbookshop.ru/50050>.— ЭБС «IPRbooks», по паролю

Интернет-ресурсы:

1. <http://www.intuit.ru> — сайт дистанционного образования в области информационных технологий
2. <http://www.iqlib.ru> - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия;
3. <http://www.biblioclub.ru> - электронная библиотечная система «Университетская библиотека – online»: специализируется на учебных материалах для ВУЗов по научно-гуманитарной тематике, а так же содержит материалы по точным и естественным наукам.
4. <http://window.edu.ru> – образовательные ресурсы ведущих вузов.
5. <http://algotlist.manual.ru> - сайт, посвященный алгоритмам и методам.
6. <http://www.intuit.ru/> - Образовательный портал. Текстовые и видеолекции.
7. [www. http://bic.pfnctu.ru](http://bic.pfnctu.ru) Электронная библиотека СКФУ

Практическое занятие 4

Структурированная кабельная система (СКС)

Цель: Изучение, порядок проектирования и создание структурированной кабельной системы (СКС)

Знать: Основные особенности и порядок проектирования Структурированной кабельной системы

Уметь: Применять полученные знания о Структурированной кабельной системе (СКС)

Код	Формулировка:
ОК-5	быть готовым работать с информацией в различных формах, использовать для ее получения, обработки, передачи, хранения и защиты современные компьютерные технологии
ОПК-7	способностью учитывать современные тенденции развития теории автоматического управления, электронного оборудования, измерительной и вычислительной техники, информационных технологий в профессиональной деятельности
ПК-12	способностью разрабатывать инструкции по эксплуатации используемого технического оборудования и программного обеспечения для обслуживающего персонала
ПК-13	способностью разрабатывать информационное обеспечение систем автоматизации и управления на основе современных технологий программирования
ПК-15	способностью использовать в разработках программно-технических комплексов современные технологии передачи данных и алгоритмы их обработки

Актуальность: аналитическое исследование в изучении структурированной кабельной системы. Порядок проектирования и создания ЛВС

Теоретическая часть

Перед проектированием ЛВС необходимо определить цели создания сети, особенности ее организационного и технического использования:

1. Какие проблемы предполагается решать при использовании ЛВС?
2. Какие задачи планируется решать в будущем?
3. Кто будет выполнять техническую поддержку и обслуживание ЛВС?
4. Нужен ли доступ из ЛВС к глобальной сети?
5. Какие требования предъявляются к секретности и безопасности информации?

При построении сети конфигурация сети определяется требованиями, предъявляемыми к ней, а также финансовыми возможностями компании и базируется на существующих технологиях и на принятых во всем мире стандартах построения ЛВС.

Структурированной кабельной системой (СКС) называется кабельная система:

- имеющая стандартизированную структуру и топологию;
- использующая стандартизированные элементы (кабели, разъемы, коммутационные устройства и т.п.);
- обеспечивающая стандартизированные параметры (скорость передачи данных, затухание и т.п.);
- управляемая (администрируемая) стандартизованным образом.

Структурированная кабельная система (СКС) – это набор коммутационных элементов (кабели, разъемов, коннекторов и т.п.), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

Термин «стандартизированный» не означает здесь «одинаковый», а определяет лишь, что все различные **СКС** строятся по одинаковым принципам и правилам и в

соответствии с национальными и международными стандартами в области информационных технологий.

Преимущества структурированных кабельных систем:

- Универсальность: одна кабельная система обслуживает все необходимые в здании системы: телефонную, ЛВС, пожарную, охранную и др.

- Высокая адаптивная способность к изменениям внешних условий («гибкость»): действительно, без изменений в пространстве, без перекладки кабелей СКС легко приспосабливается:

- 1. К изменениям организационной структуры предприятия (организация новых и ликвидация старых подразделений);

- 2. К передислокации сотрудников и подразделений (например, обладая СКС, переместил за субботу и воскресенье в новое помещение 590 сотрудников, которые в понедельник продолжили работу без проблем);

- 3. К смене типов оборудования и, следовательно, к смене поставщиков (заметим, что оборудование обновляется в компьютерной области примерно за три года), а независимость от конкретных поставщиков всегда полезна.

- Небольшая численность и моноспециализированность обслуживающего СКС персонала (не нужны отдельные специалисты по проводке для пожарных, охранных, телефонных и других систем – нужен лишь администратор СКС);

- Высокая экономичность по критерию «затраты-эффективность».

Исходя из требований, в каждом отдельном случае выбирается топология сети, кабельная структура, протоколы и методы передачи данных, способы организации взаимодействия устройств, сетевая операционная система.

Эффективность функционирования ЛВС определяется параметрами, выбранными при конфигурировании сети:

- типом (одноранговая или с выделенным сервером);
- топологией;
- типом доступа к среде передачи данных;
- максимальной пропускной способностью сети;
- максимальным количеством рабочих станций;
- типом компьютеров в сети (однородные или неоднородные сети);
- максимальной допустимой протяженностью сети;
- максимальным допустимым удалением рабочих станций друг от друга;
- качеством и возможностями сетевой операционной системы;
- объемом и технологией использования информационного обеспечения (баз данных);
- средствами и методами защиты информации в сети;
- средствами и методами обеспечения отказоустойчивости ЛВС.

Принципы проектирования. Стадии проектирования

Перед выполнением работ по монтажу ЛВС проводятся мероприятия по разработке и проектированию локальных сетей. К этому процессу могут привлекаться различные специалисты, которые должны учесть все конструктивные особенности здания и отдельных помещений, где планируется прокладка ЛВС. В результате получают технический проект, составленный в соответствии с нормами и правилами, принятыми в РФ. Он включает схему монтажа локальной сети, описание ее основных характеристик, с указанием регламентирующих их нормативных документов.

Порядок проектирования локальных сетей

Типовое проектирование ЛВС может выполняться в несколько этапов и предусматривает определение следующих характеристик:

- основных и второстепенных задач, возлагаемых на сеть;
- функциональных возможностей сети;

- пропускной способности различных участков и характера передаваемой информации;
- вида монтируемой сети;
- возможности прокладки кабелей внутри помещений и обеспечения их безопасной эксплуатации;
- структуры ЛВС, ее иерархии и основных частей по отделам, рабочим местам;
- возможности дальнейшего расширения сети;
- необходимости подключения к уже существующим локальным сетям предприятия и к глобальной сети Интернет;
- возможности использования средств защиты информации.

Все работы, которые предусматривает проектирование компьютерных сетей, выполняются в строгом соответствии с предварительным планом, разработанным на основе ТЗ (технического задания). Одним из приоритетных условий является простота обслуживания, монтажа, а при необходимости и демонтажа локальной сети предприятия.

Исходные данные

Важность этого этапа связана как с необходимостью упорядочивания требований к создаваемой ЛС и ее отдельным составляющим для обеспечения возможности принятия в будущем взвешенных конкретных решений, так и с ее обоснованием.

При создании новой сети для какого-нибудь предприятия желательно учитывать следующие факторы:

1. Требуемый размер сети (в настоящее время, в ближайшем будущем и по прогнозу на перспективу).
2. Структура, иерархия и основные части сети (по подразделениям предприятия, а также по комнатам, этажам и зданиям предприятия).
3. Основные направления и интенсивность информационных потоков в сети (в настоящее время, в ближайшем будущем и в дальней перспективе). Характер передаваемой по сети информации (данные, оцифрованная речь, изображения), который непосредственно сказывается на требуемой скорости передачи (до нескольких сотен Мбит/с, для телевизионных изображений высокой четкости).
4. Технические характеристики оборудования (компьютеров, адаптеров, кабелей, *репитеров*, концентраторов, коммутаторов) и его стоимость.
5. Возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля.
6. Обслуживание сети и контроль ее *безотказности* и безопасности.
7. Требования к программным средствам по допустимому размеру сети, скорости, гибкости, разграничению прав доступа, стоимости, по возможностям контроля обмена информацией и т.д.
8. Необходимость подключения к глобальным или к другим локальным сетям.

Вполне возможно, что после изучения всех факторов выяснится, что можно обойтись без сети, избежав тем самым довольно больших затрат на аппаратуру и *программное обеспечение*, установку, эксплуатацию, поддержку и ремонт сети, зарплату обслуживающему персоналу, и т.д.

Сеть по сравнению с автономными компьютерами порождает множество дополнительных проблем: от простейших механических (компьютеры, подключенные к сети, труднее перемещать с места на место) до сложных информационных (необходимость контролировать совместно используемые ресурсы, предотвращать заражение сети вирусами). К тому же пользователи сети уже не так независимы, как пользователи автономных компьютеров, им надо придерживаться определенных правил, подчиняться установленным требованиям, которым их необходимо научить.

Наконец, *сеть* остро ставит вопрос о безопасности информации, защиты от несанкционированного доступа, ведь с любого компьютера сети можно считать данные с общих сетевых дисков. Защитить один *компьютер* или даже несколько одиночных гораздо проще, чем целую *сеть*. Поэтому приступать к установке сети целесообразно

только тогда, когда без сети работа становится невозможной, непроизводительной, когда отсутствие межкомпьютерной связи сдерживает развитие дела.

В начале проектирования сети необходимо провести полную "инвентаризацию" имеющихся компьютеров и их программного обеспечения, а также периферийных устройств (принтеров, сканеров и т.д.). Это позволит при организации сети исключить ненужное дублирование (оборудование и *программное обеспечение* теперь могут быть разделяемыми ресурсами), а также поставить задачи модернизации как аппаратных, так и программных средств. Для корректного определения характеристик компьютеров целесообразно использовать специальные диагностические программы или встроенные программы ОС (например, в ОС *Windows Millennium* это *программа* "Сведения о системе" из раздела служебных программ и *программа* "Система" из панели управления). Следует выбирать такие варианты программ, которые обеспечивают получение правильных данных ("старые" диагностические программы могут неверно указать тип процессора и версию ОС), а также *сохранение данных* в файле (это особенно ценно при большом числе компьютеров). Кроме того, следует уделить внимание наличию встроенной сетевой карты или сетевого контроллера на системной плате, а также типу поддерживаемых ими сетевых стандартов (как правило, поддерживается *сеть Ethernet* на витой паре, но принципиально знать ее разновидность – 10/100/1000 Мбит/с). Не все характеристики компьютеров, которые важны при их объединении в *сеть*, могут быть определены описанными выше способами. Из сопроводительной документации к компьютеру или после вскрытия системного блока можно и нужно определить число и тип свободных слотов (разъемов) расширения, а также максимальную *мощность* блока питания. Это необходимо для оценки возможности установки в *компьютер* новых плат.

Выбор оборудования

При выборе сетевого оборудования надо учитывать множество факторов, в частности:

- уровень стандартизации оборудования и его совместимость с наиболее распространенными программными средствами;
- скорость передачи информации и возможность ее дальнейшего увеличения;
- возможные топологии сети и их комбинации (шина, пассивная звезда, пассивное дерево);
- *метод управления обменом* в сети (*CSMA/CD*, полный дуплекс или *маркерный метод*);
- разрешенные типы кабеля сети, максимальную его длину, защищенность от помех;
- стоимость и технические характеристики конкретных аппаратных средств (сетевых адаптеров, *трансиверов*, *репитеров*, концентраторов, коммутаторов).

Всем этим часто пренебрегают, а напрасно: заменить *программное обеспечение* сравнительно просто, а вот замена аппаратуры, особенно прокладка кабеля, обходится порой очень дорого, а иногда бывает просто невозможна. В первую *очередь* следует проанализировать применимость для рассматриваемого случая сети *Ethernet*, как наиболее популярной, недорогой и допускающей развитие (*Fast Ethernet* и *Gigabit Ethernet*).

Еще одна важная задача – это выбор компьютеров. Если для рабочих станций или невыделенных серверов обычно используют те компьютеры, которые уже имеются на предприятии, то *выделенный сервер* желательно приобретать специально для сети. Лучше, если это будет быстродействующий специализированный *компьютер-сервер*, спроектированный с учетом специфических нужд сети (такие серверы выпускаются всеми крупнейшими производителями компьютеров).

Для любой сети крайне критична ситуация перебоев в системе электропитания. Несмотря на то, что многие сетевые *программные средства* применяют специальные меры против этого, как и против других отказов аппаратуры (например, дублирование дисков), проблема очень серьезная. Иногда отключение питания может полностью и надолго вывести *сеть* из строя.

В идеале защищенными от отключения питания должны быть все серверы сети (желательно и рабочие станции). Проще всего этого добиться, если *сервер* в сети всего один. Источник бесперебойного питания при сбое питания переходит на питание подключенного компьютера от аккумулятора и подает специальный сигнал компьютеру, который за короткое время завершает все текущие *операции* и сохраняет данные на диске. При выборе источника бесперебойного питания надо, прежде всего, обращать внимание на максимальную *мощность*, которую он обеспечивает, и на время поддержания им номинального уровня напряжения (это время составляет от нескольких минут до нескольких часов). *Стоимость* устройства довольно высока (до нескольких тысяч долларов). Поэтому целесообразно один источник бесперебойного питания применять для двух-трех серверов.

Наиболее *устойчивы к отказам* питания портативные компьютеры (ноутбуки). Встроенный аккумулятор и низкое потребление энергии обеспечивают их нормальную работу без внешнего питания в течение одного-двух часов и даже более. Если еще учесть низкий уровень излучений и высокое качество изображения мониторов этих компьютеров, то стоит всерьез рассмотреть возможность использования ноутбуков в качестве рабочих станций, а вероятно, и не слишком мощного, невыделенного сервера. Тем более что многие ноутбуки имеют встроенные сетевые адаптеры довольно неплохого качества. Особенно удобно применение ноутбуков в *одноранговых сетях* с множеством серверов. Применение внешних источников бесперебойного питания в подобных случаях становится чересчур дорогим удовольствием.

Многослойная модель сети

Весь комплекс программно-аппаратных средств сети может быть описан многослойной моделью, состоящей из слоев:

- компьютеры или компьютерные платформы;
- коммуникационное оборудование;
- операционные системы;
- сетевые приложения.

Компьютеры

В основе любой сети лежит аппаратный слой стандартизированных компьютерных платформ. В настоящее время широко используются компьютерные платформы различных классов - от персональных компьютеров до мэйнфреймов и суперЭВМ. Компьютеры подключаются к сети с помощью сетевой карты.

Коммуникационное оборудование

Ко второму слою относится коммуникационное оборудование, которое играет не менее важную роль, чем компьютеры.

Коммуникационное оборудование сетей можно разделить на три группы:

- сетевые адаптеры (карты);
- сетевые кабели;
- промежуточное коммуникационное оборудование (трансиверы, повторители, концентраторы, коммутаторы, мосты, маршрутизаторы и шлюзы).

Операционные системы

Третьим слоем, образующим программную платформу сети, являются операционные системы. В зависимости от того, какие концепции управления локальными и распределенными ресурсами положены в основу сетевой ОС, зависит эффективность работу всей сети.

Сетевые приложения

Четвертый слой - это сетевые приложения. К сетевым приложениям относятся такие приложения как сетевые базы данных, почтовые приложения, системы автоматизации коллективной работы и т.д.

Техническое обеспечение вычислительных систем

Рассмотрим более подробно аппаратные средства сетей - компьютеры. Архитектура компьютера включает в себя как структуру, отражающую аппаратный состав

ПК, так и программно – математическое обеспечение. Все компьютеры сетей можно разделить на два класса: серверы и рабочие станции.

Сервер (server)- это многопользовательский компьютер, выделенный для обработки запросов от всех рабочих станций. Это мощный компьютер или мэйнфрейм, предоставляющий рабочим станциям доступ к системным ресурсам и распределяющий эти ресурсы. Сервер имеет сетевую операционную систему, под управлением, которой происходит совместная работа всей сети.

Основными требованиями, которые предъявляются к серверам, являются высокая производительность и надежность их работы. Серверы в больших сетях стали специализированными и, как правило, используются для управления сетевыми базами данных, организации электронной почты, управления многопользовательскими терминалами (принтерами, сканерами, плоттерами) и т.д.

Существует несколько типов серверов:

- 1.Файл-серверы. Управляют доступом пользователей к файлам и программам.
- 2.Принт-серверы. Управляют работой системных принтеров.
- 3.Серверы приложений. Серверы приложений - это работающий в сети мощный компьютер, имеющий прикладную программу, с которой могут работать клиенты. Приложения по запросам пользователей выполняются непосредственно на сервере, а на рабочую станцию передаются лишь результаты запроса.
- 4.Почтовые серверы. Данный сервер используется для организации электронной корреспонденции с электронными почтовыми ящиками.
- 5.Прокси-сервер. Это эффективное средство подключения локальных сетей к сети Интернет. Прокси-сервер - компьютер, постоянно подключенный к сети Интернет, через который происходит общение пользователей локальной сети с сетью Интернетом.

Мониторинг и анализ локальных сетей

Контроль – это необходимый первый этап, который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и собственно управления полезно для небольших и средних сетей, для которых установка интегрированной системы управления экономически нецелесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети, а их отключение или реконфигурацию он может выполнять в этом случае вручную.

Процесс контроля работы сети обычно делят на два этапа – мониторинг и анализ.

На этапе мониторинга выполняется более простая процедура – процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т. п.

Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Все многообразие средств, применяемых для анализа и диагностики вычислительных сетей, можно разделить на несколько крупных классов.

Агенты систем управления, поддерживающие функции одной из стандартных MIB и поставляющие информацию по протоколу SNMP или CMIP. Для получения данных от агентов обычно требуется наличие системы управления, собирающей данные от агентов в автоматическом режиме.

Встроенные системы диагностики и управления (Embedded systems). Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления. Примером средств этого класса может служить модуль управления многосегментным повторителем Ethernet, реализующий функции автосегментации портов при обнаружении неисправностей, приписывания портов внутренним сегментам повторителя и некоторые другие. Как правило, встроенные модули управления «по совместительству» выполняют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления.

Анализаторы протоколов (Protocol analyzers). Представляют собой программные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями мониторинга и анализа трафика в сетях. Хороший анализатор протоколов может захватывать и декодировать пакеты большого количества протоколов, применяемых в сетях, — обычно несколько десятков. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, то есть показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.

Экспертные системы. Этот вид систем аккумулирует знания технических специалистов о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая система помощи. Более сложные экспертные системы представляют собой, так называемые базы знаний, обладающие элементами искусственного интеллекта. Примерами таких систем являются экспертные системы, встроенные в систему управления Spectrum компании Cabletron и анализатора протоколов Sniffer компании Network General. Работа экспертных систем состоит в анализе большого числа событий для выдачи пользователю краткого диагноза о причине неисправности сети.

Оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

1. Сетевые мониторы (называемые также сетевыми анализаторами) предназначены для тестирования кабелей различных категорий. Сетевые мониторы собирают также данные о статистических показателях трафика — средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т. п. Эти устройства являются наиболее интеллектуальными устройствами из всех четырех групп устройств данного класса, так как работают не только на физическом, но и на канальном, а иногда и на сетевом уровнях.

Анализаторы протоколов чаще всего представляют собой специальное программное обеспечение для персональных компьютеров и ноутбуков, которое переводит сетевой адаптер компьютера в режим «беспорядочного» захвата всех кадров. Анализатор протоколов выполняет декодирование захваченных кадров для вложенных пакетов протоколов всех уровней, включая прикладной.

2. Устройства для сертификации кабельных систем выполняют сертификацию в соответствии с требованиями одного из международных стандартов на кабельные системы.

Сетевые анализаторы представляют собой прецизионные приборы для сертификации кабельных систем по международным стандартам. Кроме того, эти устройства могут выполнять некоторые функции анализаторов протоколов.

3. Кабельные сканеры используются для диагностики медных кабельных систем.

Кабельные сканеры являются портативными приборами, которые могут измерить электрические параметры кабелей, а также обнаружить место повреждения кабеля. Кабельные тестеры представляют собой наиболее простые портативные приборы, способные обнаружить неисправность кабеля.

4. Тестеры предназначены для проверки кабелей на отсутствие физического разрыва. Многофункциональные портативные устройства анализа и диагностики. В связи с развитием технологии больших интегральных схем появилась возможность производства портативных приборов, которые совмещали бы функции нескольких устройств: кабельных сканеров, сетевых мониторов и анализаторов протоколов.

Многофункциональные портативные приборы сочетают в себе функции кабельных сканеров и анализаторов протоколов. Они снабжены многострочными дисплеями, контекстно-чувствительной системой помощи, встроенным микропроцессором с программным обеспечением и позволяют выполнять комплексную проверку сегментов сети на всех уровнях, от физического (что не умеют делать анализаторы протоколов), до прикладного. Отличаются от анализаторов протоколов поддержкой только базового набора протоколов локальных сетей.

Анализатор протоколов представляет собой либо специализированное устройство, либо персональный компьютер, обычно переносной, класса Notebook, оснащенный специальной сетевой картой и соответствующим программным обеспечением. Применяемые сетевая карта и программное обеспечение должны соответствовать технологии сети (Ethernet, Token Ring, FDDI, Fast Ethernet). Анализатор подключается к сети точно так же, как и обычный узел. Отличие состоит в том, что анализатор может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция — только адресованные ей. Для этого сетевой адаптер анализатора протоколов переводится в режим «беспорядочного» захвата — promiscuousmode.

Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и программного обеспечения, декодирующего протокол канального уровня, с которым работает сетевой адаптер, а также наиболее распространенные протоколы верхних уровней, например IP, TCP, ftp, telnet, HTTP, IPX, NCP, NetBEUI, DECnet и т. п. В состав некоторых анализаторов может входить также экспертная система, которая позволяет выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправности сети.

Вопросы

1. Что такое структурированная кабельная система
2. Преимущества структурированных кабельных систем
3. Порядок проектирования локальных сетей
4. Коммуникационное оборудование
5. Назначение Порядка проектирования и создания ЛВС.
6. Классификация и порядок проектирования и создания ЛВС
7. Мониторинг и анализ локальных сетей
8. Техническое обеспечение вычислительных систем

Список литературы

Основная литература:

1. Новиков Ю.В. Основы локальных сетей [Электронный ресурс]/ Новиков Ю.В., Кондратенко С.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 405 с.— Режим доступа: <http://www.iprbookshop.ru/22425>.— ЭБС «IPRbooks», по паролю

Дополнительная литература

1. Построение коммутируемых компьютерных сетей / Е.В. Смирнова, И.В. Баскаков, А.В. Пролетарский, Р.А. Федотов. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 429 с. : схем., ил. ; То же [Электронный

ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=429834>

2. Синицын Ю.И. Волоконно-оптические линии связи в компьютерных сетях и телекоммуникациях [Электронный ресурс]: методические указания к практическим и лабораторным занятиям/ Синицын Ю.И.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014.— 142 с.— Режим доступа: <http://www.iprbookshop.ru/50050>.— ЭБС «IPRbooks», по паролю

Интернет-ресурсы:

1.<http://www.intuit.ru> – сайт дистанционного образования в области информационных технологий

2.<http://www.iqlib.ru> - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия;

3.<http://www.biblioclub.ru> - электронная библиотечная система «Университетская библиотека – online»: специализируется на учебных материалах для ВУЗов по научно-гуманитарной тематике, а так же содержит материалы по точным и естественным наукам.

4.<http://window.edu.ru> – образовательные ресурсы ведущих вузов.

5.<http://algotlist.manual.ru> - сайт, посвященный алгоритмам и методам.

6.<http://www.intuit.ru/> - Образовательный портал. Текстовые и видеолекции.

7.[www. http://bic.pfnrcfu.ru](http://bic.pfnrcfu.ru) Электронная библиотека СКФУ

Практическое занятие 5

Сетевое оборудование.

Цель: Изучение Сетевого оборудования

Знать: Основные особенности Сетевого оборудования

Уметь: Сетевое оборудование

Формируемые компетенции:

Код	Формулировка:
ОК-5	быть готовым работать с информацией в различных формах, использовать для ее получения, обработки, передачи, хранения и защиты современные компьютерные технологии
ОПК-7	способностью учитывать современные тенденции развития теории автоматического управления, электронного оборудования, измерительной и вычислительной техники, информационных технологий в профессиональной деятельности
ПК-12	способностью разрабатывать инструкции по эксплуатации используемого технического оборудования и программного обеспечения для обслуживающего персонала
ПК-13	способностью разрабатывать информационное обеспечение систем автоматизации и управления на основе современных технологий программирования
ПК-15	способностью использовать в разработках программно-технических комплексов современные технологии передачи данных и алгоритмы их обработки

Актуальность: Основные особенности Сетевого оборудования

Теоретическая часть:

Сетевое оборудование — устройства, необходимые для работы компьютерной сети, например: маршрутизатор, коммутатор, концентратор, патч-панель и др. Можно выделить активное и пассивное сетевое оборудование.

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

Пассивное сетевое оборудование – оборудование, не наделенное «интеллектуальными» особенностями. Например - кабельная система: кабель (коаксиальный и витая пара (UTP/STP)), вилка/розетка (RG58, RJ45, RJ11, GG45), повторитель (репитер), патч-панель, концентратор (хаб), балун (balun) для коаксиальных кабелей (RG-58) и т.д. Также, к пассивному оборудованию можно отнести монтажные шкафы и стойки, телекоммуникационные шкафы.

Основными компонентами сети являются рабочие станции, серверы, передающие среды (кабели) и сетевое оборудование.

Рабочие станции – компьютеры сети, на которых пользователями сети реализуются прикладные задачи.

Серверы сети – аппаратно-программные системы, выполняющие функции управления распределением сетевых ресурсов общего доступа. Сервером может быть это любой подключенный к сети компьютер, на котором находятся ресурсы, используемые другими устройствами локальной сети. В качестве аппаратной части сервера используется достаточно мощные компьютеры.

1.Сетевые адаптеры

Сетевые адаптеры (**сетевые карты**) – это сетевое оборудование, обеспечивающее функционирование сети на физическом и канальном уровнях. Сетевой адаптер относится к периферийному устройству компьютера, непосредственно взаимодействующему со средой передачи данных, которое прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Это устройство решает задачи

надежного обмена двоичными данными, представленными соответствующими электромагнитными сигналами, по внешним линиям связи. Как и любой контроллер компьютера, сетевой адаптер работает под управлением драйвера операционной системы, и распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации.

Компьютер, будь то сервер или рабочая станция, подключается к сети с помощью внутренней платы – сетевого адаптера. Сетевой адаптер вставляется в свободное гнездо материнской платы компьютера. Карты сетевых адаптеров устанавливаются на каждой рабочей станции и на файловом сервере. Рабочая станция отправляет запрос к файловому серверу и получает ответ через сетевой адаптер, когда файловый сервер готов. На сетевых картах выставляются адреса компьютеров в сети, без которых невозможна передача. Когда информация циркулирует по сети, любой сетевой компьютер отбирает из нее лишь ту, что предназначена именно для него. Определяется она в соответствии с адресом компьютера.

2.Маршрутизатор (роутер) –сетевое устройство, пересылающее пакеты данных между различными сегментами сети и принимающее решения на основании информации о топологии сети и определенных правил, заданных администратором.

Маршрутизатор (router) – ретрансляционная система, соединяющая две коммуникационные сети либо их части. Каждый маршрутизатор реализует протоколы физического (1A, 1B), канального (2A, 2B) и сетевого (3A, 3B) уровней, как показано на рисунке 1. Специальные сетевые процессы соединяют части коммутатора в единое целое. Физический, канальный и сетевой протоколы в разных сетях различны.

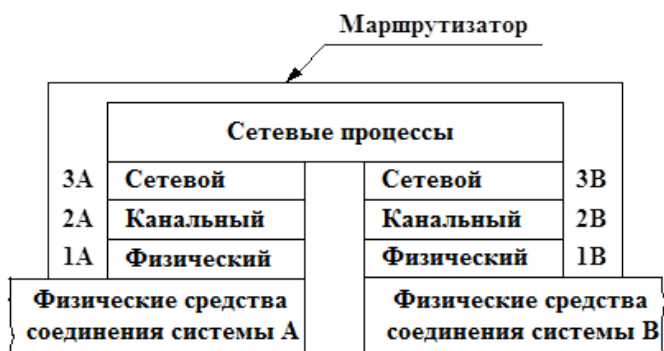


Рисунок 1 – Структура маршрутизатора

Поэтому соединение пар коммуникационных сетей осуществляется через маршрутизаторы, которые осуществляют необходимое преобразование указанных протоколов. Сетевые процессоры выполняют взаимодействие соединяемых сетей. Маршрутизатор работает с несколькими каналами, направляя в какой-нибудь из них очередной блок данных.

Маршрутизаторы обмениваются информацией об изменениях структуры сетей, трафике и их состоянии. Благодаря этому выбирается оптимальный маршрут следования блока данных в разных сетях от абонентской системы-отправителя к системе-получателю.

Различие между маршрутизаторами и мостами

Маршрутизаторы превосходят мосты своей способностью фильтровать и направлять пакеты данных на сети. Так как маршрутизаторы работают на сетевом уровне, они могут соединять сети, использующие разную сетевую архитектуру, методы доступа к каналам связи и протоколы.

Маршрутизаторы не обладают такой способностью к анализу сообщений как мосты, но зато могут принимать решение о выборе оптимального пути для данных между двумя сетевыми сегментами.

Мосты принимают решение по поводу адресации каждого из поступивших пакетов данных, переправлять его через мост или нет в зависимости от адреса назначения. Маршрутизаторы же выбирают из таблицы маршрутов наилучший для данного пакета.

В поле зрения маршрутизаторов находятся только пакеты, адресованные к ним предыдущими маршрутизаторами, в то время как мосты должны обрабатывать все пакеты сообщений в сегменте сети, к которому они подключены.

Мостовой маршрутизатор (англ. Brouter) — это гибрид моста и маршрутизатора, который сначала пытается выполнить маршрутизацию, где это только возможно, а затем, в случае неудачи, переходит в режим моста.

3.Шлюз –адрес маршрутизатора, на который отправляется трафик, для которого невозможно определить маршрут исходя из таблиц маршрутизации. **Шлюз** (англ. GateWay) – ретрансляционная система, обеспечивающая взаимодействие информационных сетей.

Шлюз является наиболее сложной ретрансляционной системой, обеспечивающей взаимодействие сетей с различными наборами протоколов всех семи уровней. В свою очередь, наборы протоколов могут опираться на различные типы физических средств соединения. На рисунке 2 показана структура шлюза.



Рисунок 2 – Структура шлюза

В тех случаях, когда соединяются информационные сети, то в них часть уровней может иметь одни и те же протоколы. Тогда сети соединяются не при помощи шлюза, а на основе более простых ретрансляционных систем, именуемых маршрутизаторами и мостами. Шлюзы оперируют на верхних уровнях модели OSI (сеансовом, представительском и прикладном) и представляют наиболее развитый метод подсоединения сетевых сегментов и компьютерных сетей. Необходимость в сетевых шлюзах возникает при объединении двух систем, имеющих различную архитектуру.

В качестве шлюза обычно используется выделенный компьютер, на котором запущено программное обеспечение шлюза и производятся преобразования, позволяющие взаимодействовать нескольким системам в сети. Другой функцией шлюзов является преобразование протоколов. Шлюзы сложны в установке и настройке и работают медленнее, чем маршрутизаторы.

4. Повторители и Концентраторы (хаб) –сетевое устройство, предназначенное для объединения нескольких устройств ethernet в общий сегмент сети. Основная функция **повторителя** (репитеры), как это следует из его названия, – повторение сигналов, поступающих на его порт. Повторитель улучшает электрические характеристики сигналов и их синхронность, и за счет этого появляется возможность увеличить общую длину кабеля между самыми удаленными в сети узлами (рисунок 3).

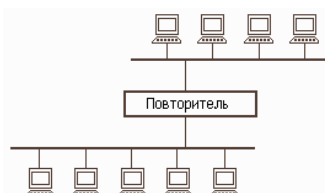


Рисунок 3 - Повторители

Многопортовый повторитель часто называют **концентратором** или **Hub** (хабом от англ. hub — центр деятельности), что отражает тот факт, что данное устройство реализует не только функцию повторения сигналов, но и концентрирует в одном центральном устройстве функции объединения компьютеров в сеть. Практически во всех современных сетевых стандартах концентратор является необходимым элементом сети, соединяющим отдельные компьютеры в сеть. **Концентратор** или **хаб** – сетевое устройство, действующее на физическом уровне сетевой модели OSI. Отрезки кабеля, соединяющие два компьютера или какие-либо два других сетевых устройства, называются **физическими сегментами**, поэтому концентраторы и повторители, которые используются для добавления новых физических сегментов, являются средством физической структуризации сети.

Концентратор – устройство, у которого суммарная пропускная способность входных каналов выше пропускной способности выходного канала. Так как потоки входных данных в концентраторе больше выходного потока, то главной его задачей является концентрация данных. При этом возможны ситуации, когда число блоков данных, поступающее на входы концентратора, превышает его возможности. Тогда концентратор ликвидирует часть этих блоков.

Ядром концентратора является процессор. Концентратор является активным оборудованием. Он служит центром звездообразной конфигурации сети и обеспечивает подключение сетевых устройств. В концентраторе для каждого узла (ПК, принтеры, телефоны и пр.) должен быть предусмотрен отдельный порт. Нарастиваемые концентраторы представляют собой отдельные модули, которые объединяются при помощи быстродействующей системы связи. Такие концентраторы предоставляют удобный способ поэтапного расширения возможностей и мощности ЛВС. Это устройство осуществляет электрическую развязку отрезков кабеля до каждого узла, поэтому короткое замыкание на одном из отрезков не выведет из строя всю ЛВС. Концентраторы образуют из отдельных физических отрезков кабеля общую среду передачи данных – **логический сегмент**. Логический сегмент также называют доменом коллизий, поскольку при попытке одновременной передаче данных любых двух компьютеров этого сегмента, хотя бы и принадлежащих разным физическим сегментам, возникает блокировка передающей среды. **Следует особо подчеркнуть**, что, какую бы сложную структуру ни образовывали концентраторы, например, путем иерархического соединения (рисунок 4), все компьютеры, подключенные к ним, образуют единый логический сегмент, в котором любая пара взаимодействующих компьютеров полностью блокирует возможность обмена данными для других компьютеров.

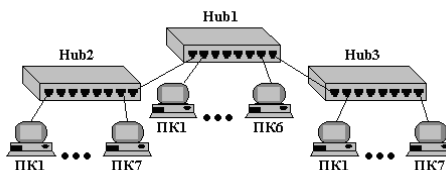


Рисунок 4 – Логический сегмент, построенный с использованием концентраторов.

При выборе места для установки концентратора необходимо учитывать:

1. местоположение;
2. расстояния;
3. питание.

Выбор места установки концентратора является наиболее важным этапом планирования небольшой сети. Хаб разумно расположить вблизи геометрического центра сети (на одинаковом расстоянии от всех компьютеров). Такое расположение позволит минимизировать расход кабеля. Длина кабеля от концентратора до любого из подключаемых к сети компьютеров или периферийных устройств не должна превышать 100м.

Концентраторы всегда работают в режиме полудуплекса (Полудуплексный обмен – передача возможна в двух направлениях, но только не одновременно, а поочередно).

Преимущества концентратора

Использование концентраторов имеет преимущества. Во-первых, в сети используется топология звезда, при которой соединения с компьютерами образуют лучи, а хаб является центром звезды. Такая топология упрощает установку и управление сети. Любые перемещения компьютеров или добавление в сеть новых узлов при такой топологии несложно выполнить. Кроме того, эта топология значительно надежнее, поскольку при любом повреждении кабельной системы, сеть сохраняет работоспособность (перестает работать лишь поврежденный луч). Светодиодные индикаторы хаба позволяют контролировать состояние сети и легко обнаруживать неполадки.

5. Мосты и коммутаторы

Коммутатор (свич) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети.

Мост (англ. Bridge) – ретрансляционная система, соединяющая каналы передачи данных. В соответствии с базовой эталонной моделью взаимодействия открытых систем, мост описывается протоколами физического и канального уровней, над которыми располагаются канальные процессы. Мост опирается на пару связываемых им физических средств соединения, которые в этой модели представляют физические каналы. Мост преобразует физический (1A, 1B) и канальный (2A, 2B) уровни различных типов (рисунок 5). Канальный процесс объединяет разнотипные каналы передачи данных в один общий. Мост, а также его быстродействующий аналог – **коммутатор** (*switching hub* от англ. – переключатель), делят общую среду передачи данных на логические сегменты. Логический сегмент образуется путем объединения нескольких физических сегментов (отрезков кабеля) с помощью одного или нескольких концентраторов.



Рисунок 5 – Структура моста

Каждый логический сегмент подключается к отдельному порту моста/коммутатора. При поступлении кадра на какой-либо из портов мост/коммутатор повторяет этот кадр, но не на всех портах, как это делает концентратор, а только на том порту, к которому подключен сегмент, содержащий компьютер – адресат.

Различие между мостом и коммутатором

Разница между мостом и коммутатором состоит в том, что мост в каждый момент времени может осуществлять передачу кадров только между одной парой портов, а коммутатор одновременно поддерживает потоки данных между всеми своими портами. Другими словами, мост передает кадры последовательно, а коммутатор параллельно. Мосты используются только для связи локальных сетей с глобальными, то есть как средства удаленного доступа, поскольку в этом случае необходимость в параллельной передаче между несколькими парами портов просто не возникает.

Когда появились первые устройства, позволяющие разъединять сеть на несколько доменов коллизий (по сути фрагменты ЛВС, построенные на Hub), они были двухпортовыми и получили название мостов. По мере развития данного типа оборудования, устройства стали многопортовыми и получили название коммутаторов. Некоторое время оба понятия существовали одновременно, а позднее вместо термина «мост» стали применять «коммутатор». Мы будем использовать термин «коммутатор» для

обозначения этих обеих разновидностей устройств, поскольку все сказанное в равной степени относится и к мостам и к коммутаторам. В последнее время локальные мосты полностью вытеснены коммутаторами.

Коммутатор

Коммутатор – устройство, осуществляющее выбор одного из возможных вариантов направления передачи данных. В коммуникационной сети коммутатор является ретрансляционной системой (система, предназначенная для передачи данных или преобразования протоколов), обладающей свойством прозрачности (то есть, коммутация осуществляется без какой-либо обработки данных). Коммутатор не имеет буферов и не может накапливать данные. Поэтому, при использовании коммутатора скорости передачи сигналов в соединяемых каналах передачи данных, должны быть одинаковыми.

На рисунке 6 показана структура коммутатора. Канальные процессы, реализуемые коммутатором, выполняются специальными интегральными схемами. В отличие от других видов ретрансляционных систем, здесь, как правило, не используется программное обеспечение.



Рисунок 6 – Структура коммутатора

Вопросы

1. Что такое сетевое оборудование
2. Сетевые адаптеры
3. Классификация сетевого оборудования
4. Маршрутизатор (роутер)
5. Различие между маршрутизаторами и мостами
6. Повторители и Концентраторы
7. Мосты и коммутаторы
8. Различие между мостом и коммутатором

Список литературы

Основная литература:

1. Новиков Ю.В. Основы локальных сетей [Электронный ресурс]/ Новиков Ю.В., Кондратенко С.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 405 с.— Режим доступа: <http://www.iprbookshop.ru/22425>.— ЭБС «IPRbooks», по паролю

Дополнительная литература

1. Построение коммутируемых компьютерных сетей / Е.В. Смирнова, И.В. Баскаков, А.В. Пролетарский, Р.А. Федотов. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 429 с. : схем., ил. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=429834>
2. Сеницын Ю.И. Волоконно-оптические линии связи в компьютерных сетях и телекоммуникациях [Электронный ресурс]: методические указания к практическим и лабораторным занятиям/ Сеницын Ю.И.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014.— 142 с.— Режим доступа: <http://www.iprbookshop.ru/50050>.— ЭБС «IPRbooks», по паролю

Интернет-ресурсы:

1. <http://www.intuit.ru> – сайт дистанционного образования в области информационных технологий
2. <http://www.iqlib.ru> - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия;

- 3.<http://www.biblioclub.ru> - электронная библиотечная система «Университетская библиотека – online»: специализируется на учебных материалах для ВУЗов по научно-гуманитарной тематике, а так же содержит материалы по точным и естественным наукам.
- 4.<http://window.edu.ru> – образовательные ресурсы ведущих вузов.
- 5.<http://algolist.manual.ru> - сайт, посвященный алгоритмам и методам.
- 6.<http://www.intuit.ru/> - Образовательный портал. Текстовые и видеолекции.
- 7.[www. http://bic.pfnctu.ru](http://bic.pfnctu.ru) Электронная библиотека СКФУ

Практическое занятие 6

Особенности сетевых технологий Ethernet

Цель: Изучение основ сети Ethernet

Знать: Основные особенности сети Ethernet

Уметь: Применять знания в сети Ethernet

Формируемые компетенции:

Код	Формулировка:
ОК-5	быть готовым работать с информацией в различных формах, использовать для ее получения, обработки, передачи, хранения и защиты современные компьютерные технологии
ОПК-7	способностью учитывать современные тенденции развития теории автоматического управления, электронного оборудования, измерительной и вычислительной техники, информационных технологий в профессиональной деятельности
ПК-12	способностью разрабатывать инструкции по эксплуатации используемого технического оборудования и программного обеспечения для обслуживающего персонала
ПК-13	способностью разрабатывать информационное обеспечение систем автоматизации и управления на основе современных технологий программирования
ПК-15	способностью использовать в разработках программно-технических комплексов современные технологии передачи данных и алгоритмы их обработки

Актуальность: аналитическое исследование в изучении особенностей сети Ethernet

Теоретическая часть: Технология Ethernet

Ethernet – это наиболее распространённая технология организации локальных сетей. Стандарты Ethernet описывают реализацию двух первых уровней модели OSI – проводные соединения и электрические сигналы (физический уровень), а так же форматы блоков данных и протоколы управления доступом к сети (канальный уровень).

Название Ethernet произошло от двух английских слов – ether (эфир) и net (сеть). Ethernet использует концепцию общего эфира. Каждый ПК посылает данные в этот эфир и указывает, кому они адресованы. Данные могут дойти до всех ПК сети, но обрабатывает их только тот ПК, которому они предназначены. Остальные ПК чужие данные игнорируют. Такая работа аналогична эфиру радиостанций. Все радиостанции транслируют свои передачи в общее электромагнитное поле – радиоэфир. Ваш радиоприёмник получает электромагнитные сигналы всех станций. Но слушаете вы не всё сразу, а ту станцию, которая вам нужна.

В рамках стандарта Ethernet принято различать несколько типов построения распределенной вычислительной системы, исходя из ее топологической структуры. Фактически можно сказать, что топология локальной сети — это конфигурация кабельных соединений между компьютерами, выполненных по некоему единому принципу. Какая-либо конкретная топология сети выбирается, во-первых, исходя из используемого оборудования, которое, как правило, поддерживает некий строго определенный вариант организации сетевых подключений; во-вторых, на основе имеющихся требований к мобильности, масштабируемости и вычислительной мощности всей системы в целом. В ряде ситуаций возможна организация нескольких подсетей, построенных с использованием различных топологий и связанных впоследствии в единую сеть. В частности, применительно к стандарту Ethernet возможна организация локальных сетей с топологией «общая шина» или «звезда».

Топология «общая шина»

Технология построения локальной сети на основе топологии «общая шина» подразумевает последовательное соединение компьютеров в цепочку наподобие «гирлянды» с использованием специальных Т-образных разъемов (Т-коннекторов), подключаемых к соответствующему порту сетевого адаптера каждого из узлов сети. В качестве физической линии передачи данных применяется коаксиальный кабель с пропускной способностью 10 Мбит/с. Оконечности «цепочки», то есть ответвления Т-образных разъемов, к которым не подводится кабель для подсоединения к соседним компьютерам, ограничиваются специальными металлическими колпачками, создающими в сети необходимое сопротивление нагрузки, — они называются заглушками или терминаторами (рис. 1).

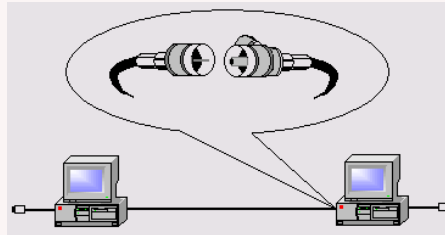


Рис. 1. – Конфигурация локальной сети с топологией «общая шина»

Некогда весьма популярные локальные сети с топологией «общая шина» в настоящее время все больше и больше утрачивают свои позиции. Причина снижения их популярности вполне очевидна. Несмотря на видимую простоту прокладки и монтажа, и относительную мобильность с точки зрения изменения конфигурации всей системы (ведь для того, чтобы переставить сетевой компьютер с места на место, достаточно лишь открутить и закрутить соответствующий разъем), такие сети имеют множество очевидных **недостатков**. И самый существенный из них — крайне низкая надежность. Достаточно произойти потере контакта в одном из терминаторов или многочисленных Т-коннекторов, что на практике случается достаточно часто, и целый сегмент локальной сети выходит из строя. В такой ситуации все сетевые компьютеры продолжают работать вполне стабильно, но неожиданно перестают «видеть» друг друга, вследствие чего системному администратору приходится последовательно проходить всю сеть, проверяя наличие контакта в разъемах, что занимает порой очень много времени. Именно поэтому топология «общая шина» идеально подходит для создания малой домашней сети «точка—точка», то есть для объединения двух компьютеров, но в случае более сложной и разветвленной сетевой структуры следует поразмыслить о возможности использования иной конфигурации.

Топология «звезда»

Альтернативой топологии «общая шина» в сетях Ethernet является звездообразная конфигурация локальной сети (рис. 2).

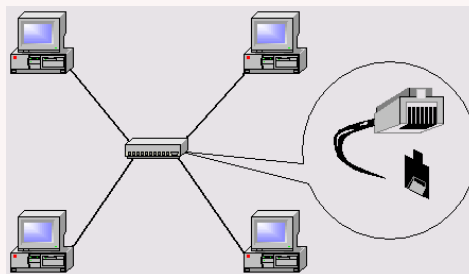


Рис. 2. Конфигурация локальной сети с топологией «звезда»

В этом случае компьютеры соединяются между собой не последовательно, а параллельно, то есть каждый из узлов сети подключается собственным отрезком провода к соответствующему порту некоего устройства, называемого концентратором, или хабом (от англ. hub — центр). В качестве линии передачи данных

используется специальный неэкранированный кабель «витая пара», который обеспечивает соединение со скоростью до 10 Мбит/с.

Преимущества топологии «звезда» по сравнению с «общей шиной» заключаются в более высокой надежности и отказоустойчивости локальной сети, в ней значительно реже возникают «заторы», да и конечное оборудование работает по «витой паре» на порядок быстрее. При этом в случае выхода из строя одного из узлов сети вся остальная система продолжает работать стабильно: полный отказ такой локальной сети происходит только при поломке концентратора. Безусловно, организация сетевой системы на основе топологии «звезда» требует значительно больших финансовых затрат, но они целиком и полностью оправдываются, когда речь заходит о необходимости обеспечить надежную связь между работающими в сети компьютерами.

Классы сетей Ethernet

Классы сети стандарта Ethernet различаются, прежде всего, пропускной способностью линий, типом используемого кабеля, топологией и некоторыми иными характеристиками. Каждый из классов сетей Ethernet имеет собственное обозначение, отражающее его технические характеристики, такое обозначение имеет вид XBase/BroadY, где X — пропускная способность сети, обозначение Base или Broad говорит о методе передачи сигнала — основополосный (baseband) или широкополосный (broadband), и, наконец, число Y отображает максимальную длину сегмента сети в сотнях метров, либо обозначает тип используемого в такой системе кабеля, который и накладывает ограничения на максимально возможное расстояние между двумя узлами сети, исходя из собственных технических характеристик. Например, сеть класса 10Base2 имеет пропускную способность 10 Мбит/с, использует метод передачи данных baseband и допускает максимальную длину сегмента в 200 м.

Класс 10Base5 (Thick Ethernet)

Класс 10Base5, который также иногда называют «толстым Ethernet», — это один из наиболее старых стандартов локальных сетей. Сегодня уже очень трудно отыскать в продаже оборудование этого типа, тем более трудно найти действующую сеть, работающую с данным типом устройств. Сети стандарта 10Base5 использовали топологию «общая шина» и создавались на основе коаксиального кабеля. Максимальная длина коаксиального кабеля, протянутого между трансивером и сетевым адаптером компьютера (трансиверного кабеля) в таких сетях может достигать 25 м, максимальная длина одного сегмента сети (отрезка сети между двумя терминаторами) — 500 м, а минимальное расстояние между точками подключения — 2,5 м. Всего в одном сегменте сети 10Base5 может работать не более 100 компьютеров, при этом количество совместно работающих сегментов сети не должно превышать пяти.

Класс 10Base2

Локальные сети, относящиеся к классу 10Base2, который также иногда называют Thin Ethernet, являются прямыми «наследницами» сетей 10Base5.

Как и в предыдущем случае, для соединения компьютеров используется тонкий экранированный коаксиальный кабель. Такая сеть имеет стандартную конфигурацию «общая шина».

Максимальная длина одного сегмента сети 10Base2 может достигать 185 м, при этом минимальное расстояние между точками подключения составляет 0,5 м. Наибольшее число компьютеров, подключаемых к одному сегменту такой сети, не должно превышать 30, максимально допустимое количество сегментов сети составляет 5. Пропускная способность данной сети, как это следует из обозначения ее класса, составляет 10 Мбит/с.

Класс 10BaseT (Ethernet на «витой паре»)

Одним из наиболее распространенных сегодня классов локальных сетей Ethernet являются сети 10BaseT. Как и стандарт 10Base2, такие сети обеспечивают передачу данных со скоростью 10 Мбит/с, однако используют в своей архитектуре топологию «звезда» и строятся с применением специального кабеля, называемого twisted pair, или «витая пара». Фактически витая пара представляет собой восьмижильный провод, в котором для обмена информации по сети используется лишь две пары проводников: одна

— для приема сигнала, и одна — для передачи. В качестве центрального звена в звездообразной структуре локальной сети 10BaseT применяется специальное устройство, называемое хабом, или концентратором. Для построения распределенной вычислительной системы, состоящей из нескольких сетевых сегментов, возможно подключение нескольких хабов в виде каскада, либо присоединение через хаб к сети 10BaseT локальной сети другого класса (рис. 3.), однако следует учитывать то обстоятельство, что общее число точек подключения в такой системе не должно превышать 1024.

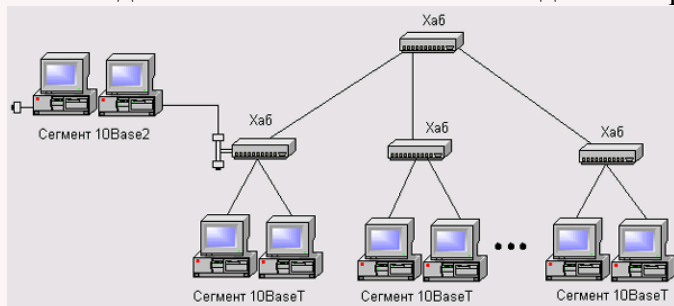


Рис. 3.— Пример реализации многосегментной локальной сети Ethernet

Класс 10BaseF (Fiber Optic)

К классу 10BaseF (другое название — Fiber Optic) принято относить распределенные вычислительные сети, сегменты которых соединены посредством магистрального оптоволоконного кабеля, длина которого может достигать 2 км. Очевидно, что в силу высокой стоимости такие сети используются в основном в корпоративном секторе рынка и по карману они достаточно крупным предприятиям, располагающим необходимыми средствами для организации подобной системы. Сеть 10BaseF имеет звездообразную топологию, которая, однако, несколько отличается от архитектуры, принятой для сетей 10BaseT.

Компьютеры каждого сегмента такой сети подключаются к хабу, который, в свою очередь, соединяется с внешним трансивером сети 10BaseF посредством специального коммуникационного шнура. Задача трансивера состоит в том, чтобы, получив из своего сегмента сети электрический сигнал, трансформировать его в оптический и передать в оптоволоконный кабель. Приемником оптического сигнала является аналогичное устройство, которое превращает его в последовательность электрических импульсов, направляемых в удаленный сегмент сети.

Преимущества оптических линий связи:

1. Прежде всего диэлектрическое волокно, используемое в оптоволоконных кабелях в качестве волноводов, обладает уникальными физическими свойствами, благодаря которым затухание сигнала в такой линии крайне мало: позволяет передавать информацию на расстояния до 100 км без использования дополнительных усилителей и ретрансляторов.

2. Кроме того, скорость передачи данных по такой магистрали может составлять 1012 бит в секунду. Если принять во внимание тот факт, что несколько световых волн может одновременно распространяться в световоде в различных направлениях, то эту скорость можно значительно увеличить, организовав между конечными точками оптоволоконного кабеля двунаправленный обмен данными. Другой способ удвоить пропускную способность оптической линии связи заключается в одновременной передаче по оптоволокну нескольких волн с различной поляризацией. Фактически можно сказать, что на сегодняшний день максимально возможная скорость передачи информации по оптическим линиям пока еще не достигнута, поскольку достаточно жесткие ограничения на «быстродействие» подобных сетей накладывает конечное оборудование.

3. Оптическая линия в силу естественных физических законов абсолютно не подвержена воздействию электромагнитных помех, а также обладает существенно большим ресурсом долговечности, чем линия, изготовленная из стандартного металлического проводника.

Fast Ethernet.

Класс локальных сетей **100BaseT**, называемый также, Fast Ethernet, появился относительно недавно. Фактически Fast Ethernet позволяет передавать данные со скоростью до 100 Мбит/с. Так же как и сети 10BaseT, локальные сети Fast Ethernet имеют звездообразную топологию и могут быть собраны с использованием кабеля различных типов, наиболее часто применяемым из которых является витая пара.

Предполагается, что в не столь отдаленном будущем эта технология вытеснит большинство действующих на сегодняшний день «устаревших» стандартов, поскольку в процессе разработки данной спецификации одной из основных задач являлось сохранение совместимости новой разновидности локальных сетей с различными типами кабеля, используемого в сетях старого образца, создано несколько модификаций стандарта Fast Ethernet.

Технология **100BaseTX** подразумевает использование стандартной витой пары пятой категории, в которой задействовано только четыре проводника из восьми: два — для приема данных, и два — для передачи. Таким образом, обеспечивается двунаправленный обмен информацией.

В сетях **100BaseT4** используется витая пара, однако в ней задействованы все восемь жил проводника. Технология 100BaseT4 подразумевает разделение всех по сети данных на три независимых логических канала (прием, передача, прием-передача), при этом пропорционально уменьшается частота сигнала, это позволяет прокладывать такие сети с использованием менее качественного и, следовательно, более дешевого кабеля. Последний стандарт в семействе Fast Ethernet носит наименование **100BaseFX**. Предназначен он для работы с оптоволоконными линиями связи. Максимальная длина одного сегмента в сетях 100BaseT (кроме подкласса 100BaseFX) не превышает 100 м, в качестве конечного оборудования используются сетевые адаптеры и концентраторы, поддерживающие этот стандарт. Принцип их работы состоит в том, что в локальных сетях этих двух классов используются одинаковые линии с одним и тем же типом разъемов.

Несмотря на все преимущества спецификации 100BaseT, такие сети по сравнению с более старыми реализациями Ethernet не лишены и ряда недостатков.

Прежде всего в моменты пиковой нагрузки, то есть в случае возникновения ситуации, при которой к ресурсам сети одновременно обращается более 50% всех узлов, на линии образуется хорошо знакомый пользователям 10BaseT «затор» — другими словами, сеть начинает заметно «тормозить». И во-вторых, если в распределенной вычислительной системе применяется комбинированная технология (одна часть сети работает со стандартом 10BaseT, другая — со стандартом 100BaseT), высокая скорость соединения будет возможна только на участке, поддерживающем пропускную способность в 100 Мбит/с. Поэтому даже если ваш компьютер оснащен сетевым адаптером 100BaseT, при обращении к удаленному узлу, оборудованному сетевой картой 10BaseT, скорость соединения не превысит 10 Мбит/с.

Gigabit Ethernet (Класс1000BaseT)

Чем быстрее растут вычислительные мощности современных персональных компьютеров, тем больше становится среднестатистический объем обрабатываемых с их помощью файлов. Соответственно возникает потребность в пропорциональном увеличении пропускной способности линий связи. В итоге это заметно ускорило процесс эволюции сетевых технологий: не успел окончательно прижиться стандарт 100BaseT, как ему на смену подоспел новый класс локальных сетей, позволяющих передавать информацию со скоростью до гигабита в секунду. Эти сети получили обозначение 1000BaseT и альтернативное название Gigabit Ethernet.

Технология Gigabit Ethernet имеет много общего с Fast Ethernet и Ethernet:

- Скорость передачи данных в сетях, построенных по этому стандарту — 1000 Мбит/с или 1 Гбит/с.
- Поддерживаются кабели, используемые в Fast Ethernet: волоконно – оптический, витая пара, двойной коаксиальный.

– Сохраняются две версии протокола доступа к среде: в дуплексном и полудуплексном режимах.

Для сохранения приведенных свойств Ethernet на физическом уровне и уровне доступа к среде были внесены следующие изменения:

1. Минимальный размер кадра был увеличен в 8 раз, то есть с 64 байтов до 512 байт. Для увеличения размера кадра используются биты расширения, это позволяет увеличить размер сети в 8 раз и сохранить размер сети в полудуплексном режиме 200м.

2. Маленькие кадры могут передаваться подряд без обязательного межкадрового интервала. Такой режим передачи называется монопольным пакетным режимом, общая длина передаваемых в пакетном режиме кадров может достигать до 8192 байтов.

3. Для обеспечения скорости передачи данных в 1 Гбит/с по витой паре был специально разработан код RAM5, который использует пять уровней при кодирования сигналов, и кроме того, передача осуществляется одновременно по четырем витым парам как в дуплексном так и в полудуплексном режимах. Таким образом, оба передатчика работают навстречу друг другу. В этом случае требуется специальный процессор для определения принимаемого сигнала путем вычитания из результирующего сигнала собственного сигнала. Если, в результате вычитания обнаруживается встречный поток, то в полудуплексном режиме это считается конфликтом, а в полудуплексном режиме – нормальной работой.

Технология Gigabit Ethernet поддерживает **следующие среды передачи:**

– 1000 BAS – LX– одномодовый оптический кабель с максимальной длиной сегмента 5км, применяется лазер с длиной волны 1300нм.

– 1000 BAS – SX– одномодовый оптический кабель с максимальной длиной сегмента 220м, используется лазер с длиной волны 850нм.

– 1000 BAS – T– кабель с четырьмя витыми парами пятой категории, максимальная длина сегмента 100м.

– 1000 BAS – CX – двойной коаксиальный кабель с одновременной передачей по паре проводов. Режим работы только дуплексный, длина сегмента 25м.

– 1000 BAS – LH – одномодовое оптическое волокно с длиной сегмента 50км при длине волны лазера 1310нм и 100км при длине волны лазера 1550нм.

10G Ethernet

Скорость передачи данных в сетях, построенных по этому стандарту — 10 000 Мбит/с.

Технология построения сети 10G Ethernet принципиально отличается от других Ethernet-технологий. Сети 10G Ethernet — это сети с **коммутацией пакетов**.

Если в сетях с разделяемыми средами пакет, переданный одной станцией, поступает на все другие станции, то в коммутируемых сетях пакет следует от передающей станции к станции назначения по маршруту, который уточняется по мере продвижения пакета от одного маршрутизатора к другому.

Сеть с разделяемыми средами, построенная только на хабах и коммутаторах, должна иметь строго иерархическую структуру: на схеме соединений не должно быть циклов.

Достоинства стандарта Ethernet:

– наилучшее соотношение цена/скорость/возможности в сравнении со всеми другими технологиями;

– возможность использовать внутренние ресурсы сетей на огромной скорости без ограничений и дополнительной оплаты;

– никаких первоначальных вложений на оборудование в квартире;

– независимость ни от наличия городского телефона/телевизионного кабеля, ни от их тех.состояния;

– существует множество дополнительных устройств для простого подключения на одну линию нескольких компьютеров и/или других устройств (игровые приставки, IP-

камеры видеонаблюдения и пр.), так как это основная и самая распространённая сетевая технология сегодня и в обозримом будущем;

- возможность получить высокоскоростные тарифы, достаточные для самых продвинутых пользователей;

- возможность быстро, без проблем и дополнительных расходов на оборудование сменить провайдера.

Недостатки:

- необходимость ввода в квартиру дополнительного кабеля.

Ethernet — это не один, а целое семейство стандартов, имеющих разные пользовательские характеристики.

Если за основу сравнения этих стандартов взять скорость передачи данных и максимально возможное расстояние между двумя узлами (диаметр сети), то получим такую сравнительную таблицу 1.

Сначала рассмотрим принцип построения локальных сетей на основе исторически первого варианта Ethernet (10 Мбит/с), который появился в конце 70 –х годов как стандарт трёх компаний — Digital, Intel, Xerox. Эта технология, как и технологии Fast Ethernet, Gigabit Ethernet основана на понятии разделяемой среды: каждый узел получает всё, что передаётся по сети; передачу выполняет только один узел, остальные ждут паузы для начала собственной передачи.

Таблица 1 - Типы технологии Ethernet

Тип стандарта Ethernet	Скорость передачи данных	Максимальный диаметр сети
Ethernet	10 Мбит/с	2 500 м
Fast Ethernet	100 Мбит/с	200 м
Gigabit Ethernet	1000 Мбит/с	200 м
10G Ethernet	10 Гбит/с	40 км

В основе технологии 10G Ethernet положен другой принцип: информация не “разбрасывается” по всей сети, а целенаправленно “проталкивается” от узла к узлу по направлению к пункту назначения. За продвижение данных в такой сети отвечают маршрутизаторы. Они определяют соседний узел, в который нужно передвинуть информационный пакет для приближения его к пункту назначения. Такие сети называются сетями с коммутацией пакетов.

Сеть Ethernet сейчас наиболее популярна в мире (более 90% рынка), предположительно таковой она и останется в ближайшие годы. Этому в немалой степени способствовало то, что с самого начала характеристики, параметры, протоколы сети были открыты, в результате чего огромное число производителей во всем мире стали выпускать аппаратуру Ethernet, полностью совместимую между собой.

На рисунке 4 показана схема сети Ethernet на коаксиальном кабеле. Сегмент кабеля на концах оборудован терминаторами («заглушками») для поглощения распространяемого сигнала (на рисунке терминаторы нарисованы чёрными квадратиками). Кабель при помощи Т-образного разъёма соединяет между собой сетевые адаптеры компьютеров.



Рисунок 4 – Схема сети Ethernet

Принцип работы Ethernet.

Любой участник может послать в сеть сообщение, но только тогда, когда в ней «тихо» – нет другой передачи.

Например, узел 2 слушает сеть, и стартуется передачу, начиная её адресами отправителя и получателя («компьютер 2 передаёт сообщение для компьютера 4»).

Передача распространяется по кабелю в обе стороны (поглощаясь терминаторами на концах), и все участники слышат её (в том числе и сам отправитель).

Все, кроме компьютера 4, игнорируют передаваемые данные, обнаружив чужой адрес получателя, а компьютер 4 принимает данные полностью.

Понятно, что при таком способе передачи нельзя допустить длительного захвата сети одним узлом. Если компьютер 2 задумает переслать компьютеру 4 большой файл, все остальные сетевые участники не скоро получат возможность начать передачу.

В силу этой причины сообщения передаются разделёнными на пакеты (в технологии Ethernet они называются кадрами). Длина пакета лежит в диапазоне от 64 до 1518 байтов.

Передав один пакет, узел на некоторое время прерывает работу, и если в сети «тихо», отправляет следующий пакет. Но паузой может воспользоваться другой узел и начать свой сеанс передачи. Таким образом, все узлы разделяют одну среду (кабель), имея равные возможности для посылки в сеть информационных пакетов.

Вопросы:

1. Технология Ethernet
2. Топология «общая шина», «звезда»
3. Классы сетей Ethernet
4. Класс 10BaseT (Ethernet на «витой паре»)
5. Класс 10BaseF (Fiber Optic)
6. Gigabit Ethernet (Класс 1000BaseT)
7. Принцип работы Ethernet.

Список литературы

Основная литература:

1. Новиков Ю.В. Основы локальных сетей [Электронный ресурс]/ Новиков Ю.В., Кондратенко С.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 405 с.— Режим доступа: <http://www.iprbookshop.ru/22425>.— ЭБС «IPRbooks», по паролю

Дополнительная литература

1. Построение коммутируемых компьютерных сетей / Е.В. Смирнова, И.В. Баскаков, А.В. Пролетарский, Р.А. Федотов. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 429 с. : схем., ил. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=429834>

2. Сеницын Ю.И. Волоконно-оптические линии связи в компьютерных сетях и телекоммуникациях [Электронный ресурс]: методические указания к практическим и лабораторным занятиям/ Сеницын Ю.И.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014.— 142 с.— Режим доступа: <http://www.iprbookshop.ru/50050>.— ЭБС «IPRbooks», по паролю

Интернет-ресурсы:

1. <http://www.intuit.ru> – сайт дистанционного образования в области информационных технологий

2. <http://www.iqlib.ru> - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия;

3. <http://www.biblioclub.ru> - электронная библиотечная система «Университетская библиотека – online»: специализируется на учебных материалах для ВУЗов по научно-гуманитарной тематике, а так же содержит материалы по точным и естественным наукам.

4. <http://window.edu.ru> – образовательные ресурсы ведущих вузов.
5. <http://algotlist.manual.ru> - сайт, посвященный алгоритмам и методам.
6. <http://www.intuit.ru/> - Образовательный портал. Текстовые и видеолекции.
7. [www. http://bic.pfnctu.ru](http://bic.pfnctu.ru) Электронная библиотека СКФУ

Практическое занятие 7

Сетевые технологии локальных сетей: Token Ring, FDDI, Arcnet

Цель: Изучение сетевых операционных систем

Знать: Основные особенности сетевых операционных систем

Уметь: Применять полученные знания в Сетевых операционных системах

Формируемые компетенции:

Код	Формулировка:
ОК-5	быть готовым работать с информацией в различных формах, использовать для ее получения, обработки, передачи, хранения и защиты современные компьютерные технологии
ОПК-7	способностью учитывать современные тенденции развития теории автоматического управления, электронного оборудования, измерительной и вычислительной техники, информационных технологий в профессиональной деятельности
ПК-12	способностью разрабатывать инструкции по эксплуатации используемого технического оборудования и программного обеспечения для обслуживающего персонала
ПК-13	способностью разрабатывать информационное обеспечение систем автоматизации и управления на основе современных технологий программирования
ПК-15	способностью использовать в разработках программно-технических комплексов современные технологии передачи данных и алгоритмы их обработки

Теоретическая часть

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

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

Сетевая технология или архитектура определяет топологию и метод доступа к среде передачи данных, кабельную систему или среду передачи данных, формат сетевых кадров тип кодирования сигналов, скорость передачи в локальной сети. В современных локальных вычислительных сетях широкое распространение получили такие технологии или сетевые архитектуры, как: Ethernet, Token-Ring, ArcNet, FDDI.

Сетевые технологии локальных сетей IEEE802.5/Token-Ring

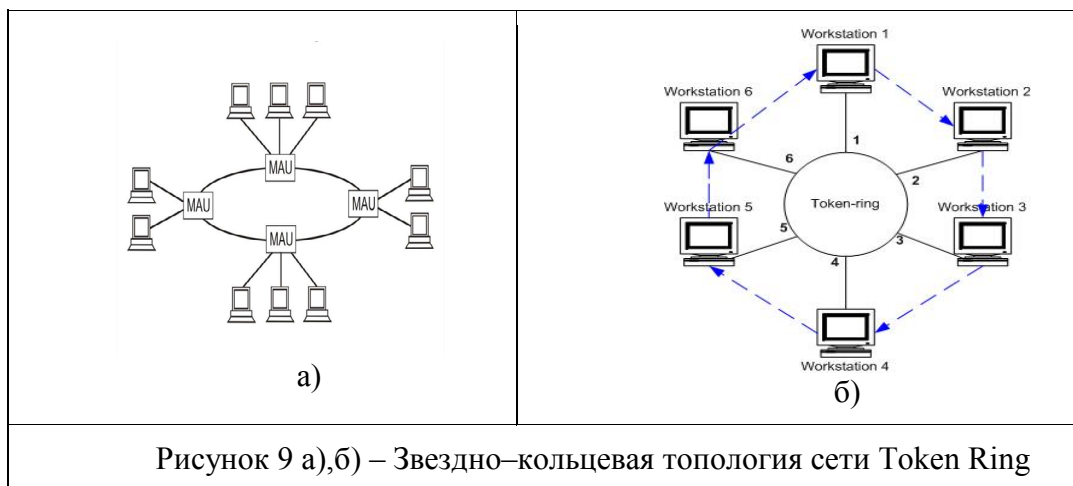
Token Ring разработан фирмой IBM. В качестве передающей среды применяется неэкранированная или экранированная витая пара (UTP или STP) или оптоволокно. Скорость передачи данных 4 Мбит/с или 16Мбит/с. В качестве метода управления доступом станций к передающей среде используется метод – маркерное кольцо (Token Ring). Ограничения на размер сети – длина кольца не более 4км.

Эта топология основана на топологии "физическое кольцо с подключением типа звезда" (рис.9б). В данной топологии все рабочие станции подключаются к центральному концентратору (Token Ring) как в топологии физическая звезда. Центральный концентратор - это интеллектуальное устройство, которое обеспечивает последовательное соединение выхода одной станции со входом другой станции.

Другими словами с помощью концентратора каждая станция соединяется только с двумя другими станциями (предыдущей и последующей станциями). Таким образом, рабочие станции связаны петлей кабеля, по которой пакеты данных передаются от одной станции к другой и каждая станция ретранслирует эти посланные пакеты. В каждой

рабочей станции имеется для этого приемо-передающее устройство, которое позволяет управлять прохождением данных в сети. Физически такая сеть построена по типу топологии “звезда”.

Концентратор создаёт первичное (основное) и резервное кольца. Если в основном кольце произойдёт обрыв, то его можно обойти, воспользовавшись резервным кольцом, так как используется четырёхжильный кабель. Отказ станции или обрыв линии связи рабочей станции не влечет за собой отказ сети как в топологии кольцо, потому что концентратор отключит неисправную станцию и замкнет кольцо передачи данных.



В архитектуре Token Ring маркер передаётся от узла к узлу по логическому кольцу, созданному центральным концентратором. Такая маркерная передача осуществляется в фиксированном направлении (направление движения маркера и пакетов данных представлено на рисунке стрелками синего цвета). Станция, обладающая маркером, может отправить данные другой станции.

Для передачи данных рабочие станции должны сначала дожидаться прихода свободного маркера. В маркере содержится адрес станции, пославшей этот маркер, а также адрес той станции, которой он предназначается. После этого отправитель передает маркер следующей в сети станции для того, чтобы и та могла отправить свои данные.

Один из узлов сети (обычно для этого используется файл-сервер) создаёт маркер, который отправляется в кольцо сети. Такой узел выступает в качестве активного монитора, который следит за тем, чтобы маркер не был утерян или разрушен.

Преимущества сетей топологии Token Ring:

- топология обеспечивает равный доступ ко всем рабочим станциям;
- высокая надежность, так как сеть устойчива к неисправностям отдельных станций и к разрывам соединения отдельных станций.

Недостатки сетей топологии Token Ring: большой расход кабеля и соответственно дорогостоящая разводка линий связи.

(Хост (от англ. *Host* —«хозяин, принимающий гостей») — любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам. В более частном случае под хостом могут понимать любой компьютер, сервер, подключённый к локальной или глобальной сети.)

Сетевые технологии локальных сетей IEEE802.4/ArcNet

Технология Arcnet – простая, недорогая, надежная и достаточно гибкая архитектура локальной сети, на ее долю выпадало до 30%рынка, и все-таки на сеть Arcnet до сих пор нет стандарта (разработана корпорацией Datapoint в 1977 году). При подключении устройств в Arcnet применяют топологии шина и звезда. На рисунке 11 показана топология сети Arcnet.

В сети Arcnet используется маркерный метод доступа (метод передачи права), но он несколько отличается от аналогичного в сети Token-Ring. Последовательность действий абонентов при данном методе:

1. Абонент, желающий передавать, ждет прихода маркера.
2. Получив маркер, он посылает запрос на передачу абоненту – приемнику информации (спрашивает, готов ли приемник принять его пакет).
3. Приемник, получив запрос, посылает ответ (подтверждает свою готовность).
4. Получив подтверждение готовности, абонент-передатчик посылает свой пакет.
5. Получив пакет, приемник посылает подтверждение приема пакета.
6. Передатчик, получив подтверждение приема пакета, заканчивает свой сеанс связи. После этого маркер передается следующему абоненту по порядку убывания сетевых адресов.

Таким образом, в данном случае пакет передается только тогда, когда есть уверенность в готовности приемника принять его. Это существенно увеличивает надежность передачи.

Среди основных **достоинств** сети Arcnet можно назвать:

1. ограниченную величину времени доступа (по сравнению с Ethernet), 2. высокую надежность связи, 3. простоту диагностики, а также 4. сравнительно низкую стоимость адаптеров. К наиболее существенным **недостаткам** сети относятся низкая скорость передачи информации (2,5 Мбит/с), система адресации и формат пакета.

Но сейчас производство аппаратуры Arcnet практически прекращено. В качестве передающей среды используются коаксиальный кабель. Были предложены и варианты на оптоволоконном кабеле, но и они также не спасли Arcnet.

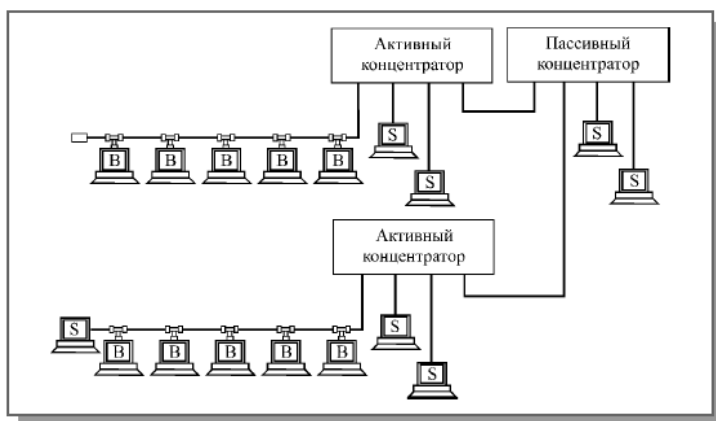


Рисунок 11 – Топология сети Arcnet

Сетевые технологии локальных сети FDDI (Fiber Distributed Data Interface)

Технология FDDI используется для организации высокоскоростных локальных сетей. Технология FDDI предназначена не для непосредственного соединения компьютеров, а для построения высокоскоростных магистральных каналов связи (backbone), объединяющих несколько сегментов локальной сети. Технология FDDI во многом основывается на технологии Token Ring, развивая и совершенствуя ее основные идеи. Разработчики технологии FDDI ставили перед собой в качестве наиболее приоритетных следующие цели:

- Повысить битовую скорость передачи данных по одному кольцу до 100 Мб/с, если второе кольцо резервное и 200 Мбит/с, если используется оба кольца.
- Количество абонентов в сети – 500;
- протяженность кольца – 100км.
- Повысить отказоустойчивость сети за счет стандартных процедур восстановления ее после отказов различного рода - повреждения кабеля, некорректной работы узла, концентратора, возникновения высокого уровня помех на линии и т.п.
- Максимально эффективно использовать потенциальную пропускную способность сети, как для асинхронного, так и для синхронного трафика.

Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Использование двух колец - это основной способ повышения отказоустойчивости в сети FDDI, и узлы, которые хотят им воспользоваться, должны быть подключены к обоим кольцам. В нормальном режиме работы сети данные проходят через все узлы и все участки кабеля первичного (Primary) кольца, поэтому этот режим назван режимом Thru - "сквозным" или "транзитным". Вторичное кольцо (Secondary) в этом режиме не используется.

Передающиеся сигналы движутся по кольцам в противоположных направлениях. Одно из колец называется первичным, а другое – вторичным (рисунок 14). При корректном функционировании сети первичное кольцо используется для передачи данных, а вторичное выступает в роли запасного.

В случае какого-либо вида отказа, когда часть первичного кольца не может передавать данные (например, обрыв кабеля или отказ узла), первичное кольцо объединяется со вторичным (рис.15), вновь образуя единое кольцо. Этот режим работы сети называется *Wrap*, то есть «свертывание» или «сворачивание» колец. Операция свертывания производится средствами концентраторов и/или сетевых адаптеров FDDI.

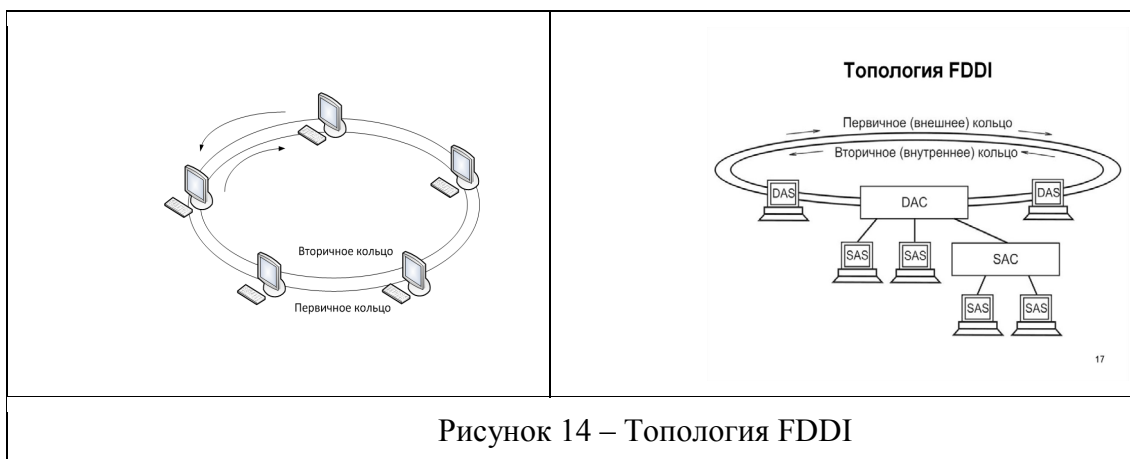


Рисунок 14 – Топология FDDI

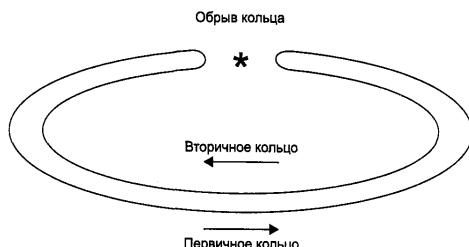


Рис.15 - Реконфигурация колец FDDI при отказе

Для упрощения этой процедуры данные по первичному кольцу всегда передаются в одном направлении (на диаграммах это направление изображается против часовой стрелки), а по вторичному – в обратном (изображается по часовой стрелке). Поэтому при образовании общего кольца из двух колец передатчики станций по-прежнему остаются подключенными к приемникам соседних станций, что позволяет правильно передавать и принимать информацию соседними станциями.

Особенности FDDI

1. В FDDI много внимания отводится различным процедурам, которые позволяют определить наличие отказа в сети, а затем произвести необходимую реконфигурацию. Сеть FDDI может полностью восстанавливать свою работоспособность в случае единичных отказов ее элементов. При множественных отказах сеть распадается на несколько не связанных сетей.

2. Кольца в сетях FDDI рассматриваются как общая разделяемая среда передачи данных, поэтому для нее определен специальный метод доступа. Этот метод очень близок

к методу доступа сетей Token Ring и также называется методом маркерного (или токенового) кольца — token ring. (рис. 16, а).

Отличия метода доступа заключаются в том, что время удержания маркера (маркер или токен, на рисунках черная точка; данные или кадры, на рисунках белые-полые кружочки) в сети FDDI не является постоянной величиной, как в сети Token Ring. Это время зависит от загрузки кольца — при небольшой загрузке оно увеличивается, а при больших перегрузках может уменьшаться до нуля.

Станция может начать передачу своих собственных кадров данных только в том случае, если она получила от предыдущей станции специальный кадр - токен доступа (рис. 16, б). После этого она может передавать свои кадры, если они у нее имеются, в течение времени, называемого временем удержания токена - Token Holding Time (ТНТ). После истечения времени ТНТ станция обязана завершить передачу своего очередного кадра и передать токен доступа следующей станции. Если же в момент принятия токена у станции нет кадров для передачи по сети, то она немедленно транслирует токен следующей станции. В сети FDDI у каждой станции есть предшествующий сосед (upstream neighbor) и последующий сосед (downstream neighbor), определяемые ее физическими связями и направлением передачи информации.

Каждая станция в сети постоянно принимает передаваемые ей предшествующим соседом кадры и анализирует их адрес назначения. Если адрес назначения не совпадает с ее собственным, то она транслирует кадр своему последующему соседу (рис. 16, в). Нужно отметить, что, если станция захватила токен и передает свои собственные кадры, то на протяжении этого периода времени она не транслирует приходящие кадры, а удаляет их из сети.

Если же адрес кадра совпадает с адресом станции, то она копирует кадр в свой внутренний буфер, проверяет его корректность (в основном, по контрольной сумме), передает его поле данных для последующей обработки протоколу, лежащего выше FDDI уровня (например, IP), а затем передает исходный кадр по сети последующей станции (рис. 16, г). В передаваемом в сеть кадре станция назначения отмечает три признака: распознавания адреса, копирования кадра и отсутствия или наличия в нем ошибок.

После этого кадр продолжает путешествовать по сети, транслируясь каждым узлом. Станция, являющаяся источником кадра для сети, ответственна за то, чтобы удалить кадр из сети, после того, как он, совершив полный оборот, вновь дойдет до нее (рис. 16, д). При этом исходная станция проверяет признаки кадра, дошел ли он до станции назначения и не был ли при этом поврежден. Процесс восстановления информационных кадров не входит в обязанности протокола FDDI, этим должны заниматься протоколы более высоких уровней.

3. Стандартом определены два режима передачи: синхронный и асинхронный.

В синхронном режиме станция при каждом поступлении маркера может передавать данные в течение определенного времени и независимо от появления маркера. Этот режим используется для приложений, чувствительных к временным задержкам. Время удержания маркера имеет заранее заданную фиксированную величину.

В асинхронном режиме длительность передачи информации связана с приходом маркера. Она не может продолжаться позднее определенного момента. Если до указанного момента маркер не появляется, то передача данных вообще не производится. Станции договариваются о величине максимально-допустимого времени оборота маркера по кадру во время инициализации кольца. На рисунке 17 показан синхронный и асинхронный режимы передачи.

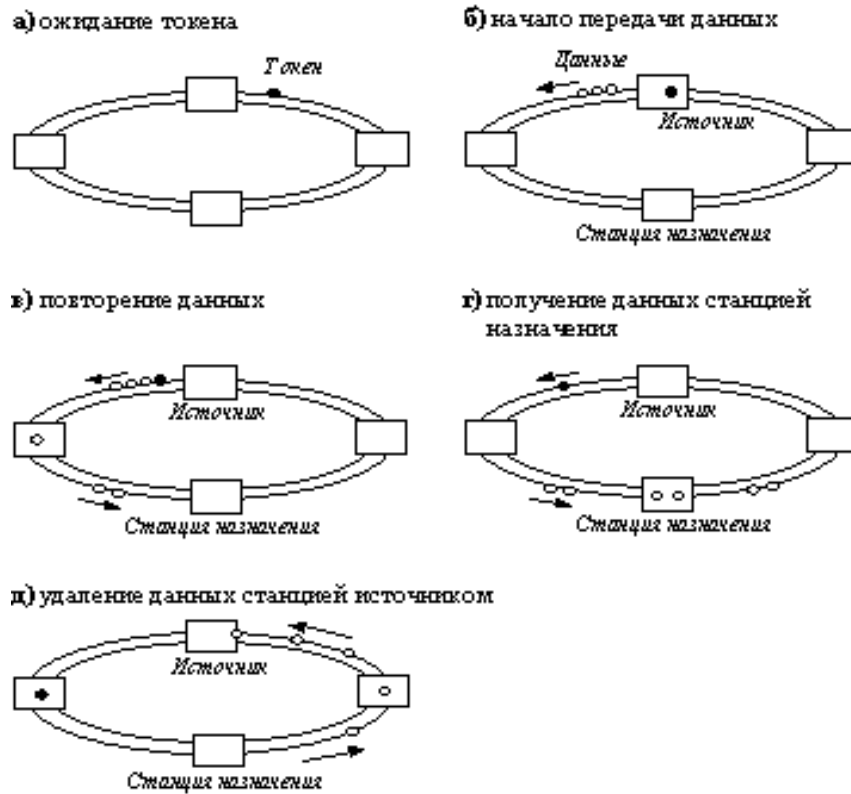


Рис. 16 – Обработка кадров станциями кольца FDDI

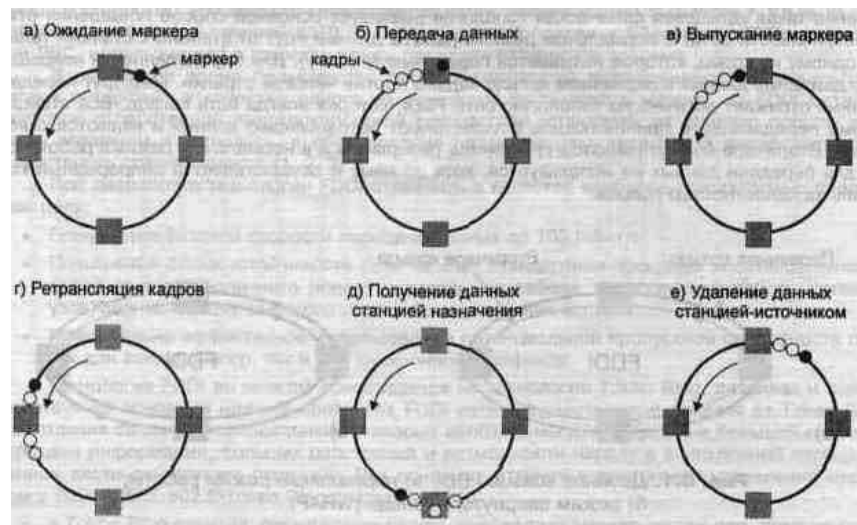
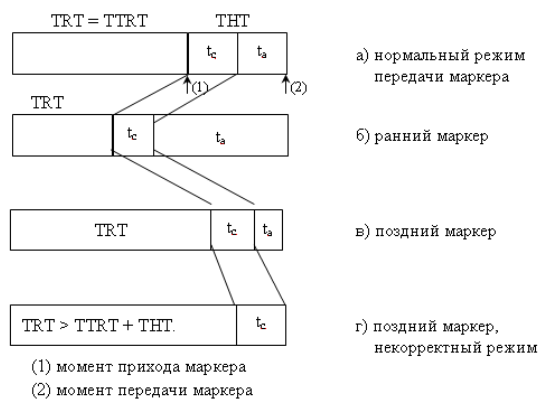


Рис. 16^I – Обработка кадров станциями кольца FDDI



t_c – время передачи синхронных данных (длина t_c всегда одинакова); t_a – время передачи асинхронных данных.

Рисунок 17 – Синхронный и асинхронный режимы передачи

Для управления доступом к сети используются временные параметры (рисунок 17):

1) Вре́мя возвра́щения маркера TRT (Token Rotation Time), то есть время, за которое маркер совершает полный оборот по кольцу;

2) TTRT (Target Token Rotation Time) – желательное время возвращения маркера, устанавливается при генерации сети;

3) TNT – время удержания маркера, время, в течение которого станция может передавать свои кадры. Также устанавливается при генерации сети.

4. Топология двойного физического кольца обеспечивает надежность передачи данных путем сохранения работоспособности сети в случае обрыва кабеля. В стандарт FDDI заложены функции управления сетью.

В дополнение к перечисленным преимуществам существует спецификация (CDDI - Copper Distributed Data Interface) на построение сети по технологии FDDI с использованием медной витой пары. Эта спецификация позволяет снизить стоимость развертывания сети за счет использования менее дорогого медного кабеля, вместо оптического.

Основным недостатком FDDI является цена построения сети. Сетевые карты и оптический кабель для FDDI обладают существенно большей стоимостью, чем для других технологий, обеспечивающих такую же скорость передачи данных. Специфика монтажа оптического кабеля требует дополнительной подготовки специалистов, выполняющих работу с кабелем. Несмотря на то, что сетевые карты CDDI дешевле FDDI, тем не менее, они являются более дорогими, чем сетевые карты 100Base-T.

В таблице 6 представлены сравнительные характеристики технологий FDDI, Token Ring и Ethernet.

Таблица 6 – Сравнительные характеристики технологий FDDI, Token Ring и Ethernet.

Характеристика	FDDI	Ethernet	Token Ring	ArcNet
Битовая скорость	100 Мб/с	10 Мб/с	16 Мб/с	2,5 Мбит/с
Топология	Двойное кольцо деревьев	Шина/звезда	Звезда/кольцо	шина, звезда
Среда передачи данных	Оптоволокно, неэкранированная витая пара	Толстый коаксиал, тонкий коаксиал, витая пара, оптоволокно	Экранированная и неэкранированная витая пара, оптоволокно	Коаксиальный кабель, витая пара, оптоволокно
Максимальная длина сети (без мостов)	200 км (100 км на кольцо)	2500 м	4000 м	6000 м
Максимальное расстояние между узлами	2 км (не больше 11 дБ потерь между узлами)	2500 м	100 м	600 м
Максимальное количество узлов	500 (1000 соединений) 0	1024	260 для экранированной витой пары, 72 для неэкранированной витой пары	255

Вопросы

1. Сетевые технологии локальных сетей IEEE802.5/Token-Ring
2. Сетевые технологии локальных сетей IEEE802.4/ArcNet
3. Сетевые технологии локальных сети FDDI (Fiber Distributed Data Interface)
4. Сетевые технологии локальных сети FDDI (Fiber Distributed Data Interface)
5. Особенности FDDI
6. Сравнительные характеристики технологий FDDI, Token Ring и Ethernet.

Список литературы

Основная литература:

1. Новиков Ю.В. Основы локальных сетей [Электронный ресурс]/ Новиков Ю.В., Кондратенко С.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 405 с.— Режим доступа: <http://www.iprbookshop.ru/22425>.— ЭБС «IPRbooks», по паролю

Дополнительная литература

1. Построение коммутируемых компьютерных сетей / Е.В. Смирнова, И.В. Баскаков, А.В. Пролетарский, Р.А. Федотов. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 429 с. : схем., ил. ; То же [Электронный ресурс]. - URL: [//biblioclub.ru/index.php?page=book&id=429834](http://biblioclub.ru/index.php?page=book&id=429834)
2. Сеницын Ю.И. Волоконно-оптические линии связи в компьютерных сетях и телекоммуникациях [Электронный ресурс]: методические указания к практическим и лабораторным занятиям/ Сеницын Ю.И.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014.— 142 с.— Режим доступа: <http://www.iprbookshop.ru/50050>.— ЭБС «IPRbooks», по паролю

Интернет-ресурсы:

1. <http://www.intuit.ru> — сайт дистанционного образования в области информационных технологий
2. <http://www.iqlib.ru> - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия;
3. <http://www.biblioclub.ru> - электронная библиотечная система «Университетская библиотека – online»: специализируется на учебных материалах для ВУЗов по научно-гуманитарной тематике, а так же содержит материалы по точным и естественным наукам.
4. <http://window.edu.ru> – образовательные ресурсы ведущих вузов.
5. <http://algolist.manual.ru> - сайт, посвященный алгоритмам и методам.
6. <http://www.intuit.ru/> - Образовательный портал. Текстовые и видеолекции.
7. <http://bic.pfnctu.ru> Электронная библиотека СКФУ

Практическое занятие 8

Виртуальные локальные сети (VLAN)

Цель: Понять технологию VLAN и ее настройку

Формируемые компетенции:

Код	Формулировка:
ОК-5	быть готовым работать с информацией в различных формах, использовать для ее получения, обработки, передачи, хранения и защиты современные компьютерные технологии
ОПК-7	способностью учитывать современные тенденции развития теории автоматического управления, электронного оборудования, измерительной и вычислительной техники, информационных технологий в профессиональной деятельности
ПК-12	способностью разрабатывать инструкции по эксплуатации используемого технического оборудования и программного обеспечения для обслуживающего персонала
ПК-13	способностью разрабатывать информационное обеспечение систем автоматизации и управления на основе современных технологий программирования
ПК-15	способностью использовать в разработках программно-технических комплексов современные технологии передачи данных и алгоритмы их обработки

Теоретическая часть

Поскольку коммутатор *Ethernet* является устройством канального уровня, то в соответствии с логикой работы он будет рассылать широковещательные кадры через все порты. Хотя трафик с конкретными адресами (соединения "точка — точка") изолирован парой портов, широковещательные кадры передаются во всю *сеть* (на каждый *порт*).

Широковещательные кадры — это кадры, передаваемые на все узлы сети. Они необходимы для работы многих сетевых протоколов, таких как *ARP*, *BOOTP* или *DHCP*. С их помощью *рабочая станция* оповещает другие компьютеры о своем появлении в сети. Так же рассылка широковещательных кадров может возникать из-за некорректно работающего сетевого адаптера. Широковещательные кадры могут привести к нерациональному использованию полосы пропускания, особенно в крупных сетях. Для того чтобы этого не происходило, важно ограничить область распространения широковещательного трафика (эта область называется *широковещательным доменом*) — организовать небольшие *широковещательные домены*, или **виртуальные локальные сети (Virtual LAN, VLAN)**.

Виртуальной локальной сетью называется логическая *группа* узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети. Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса — уникального, группового или широковещательного. В то же время, внутри виртуальной сети кадры передаются *по* технологии коммутации, то есть только на тот *порт*, который связан с адресом назначения кадра. Таким образом, с помощью виртуальных сетей решается проблема распространения широковещательных кадров и вызываемых ими последствий, которые могут развиваться в широковещательные штормы и существенно снизить *производительность* сети.

VLAN обладают следующими преимуществами:

- гибкость внедрения. *VLAN* являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы, несмотря на их физическое размещение в сети;

- *VLAN* обеспечивают возможность контроля широковещательных сообщений, что увеличивает полосу пропускания, доступную для пользователя;
- *VLAN* позволяют повысить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе, политику взаимодействия пользователей из разных виртуальных сетей.

Рассмотрим пример, показывающий эффективность использования логической сегментации сетей с помощью технологии *VLAN* при решении типовой задачи организации доступа в *Интернет* сотрудникам офиса. При этом трафик каждого отдела должен быть изолирован.

Предположим, что в офисе имеется несколько комнат, в каждой из которых располагается небольшое количество сотрудников. Каждая комната представляет собой отдельную рабочую группу.

При стандартном подходе к решению задачи с помощью физической сегментации трафика каждого отдела потребовалось бы в каждую комнату устанавливать отдельный *коммутатор*, который бы подключался к маршрутизатору, предоставляющему *доступ* в *Интернет*. При этом, *маршрутизатор* должен обладать достаточным количеством портов, обеспечивающим возможность подключения всех *физических сегментов* (комнат) сети. Данное решение плохо масштабируемо и является дорогостоящим, т.к. при увеличении количества отделов увеличивается количество необходимых коммутаторов, интерфейсов маршрутизатора и магистральных кабелей (рис.1).

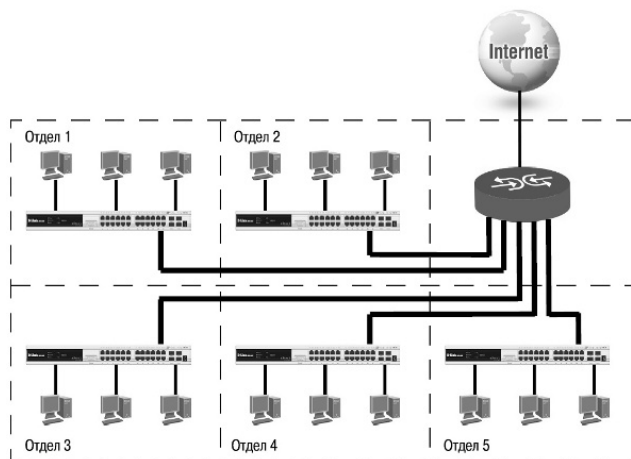


Рис. 1 – Физическая сегментация сети

При использовании *виртуальных локальных сетей* уже не требуется подключать пользователей одного отдела к отдельному коммутатору, что позволяет сократить количество используемых устройств и магистральных кабелей.

Коммутатор, программное обеспечение которого поддерживает функцию *виртуальных локальных сетей*, позволяет выполнять логическую сегментацию сети путем соответствующей программной настройки. Это дает возможность подключать пользователей, находящихся в разных сегментах, к одному коммутатору, а также сокращает количество необходимых физических интерфейсов на маршрутизаторе (рис.2).

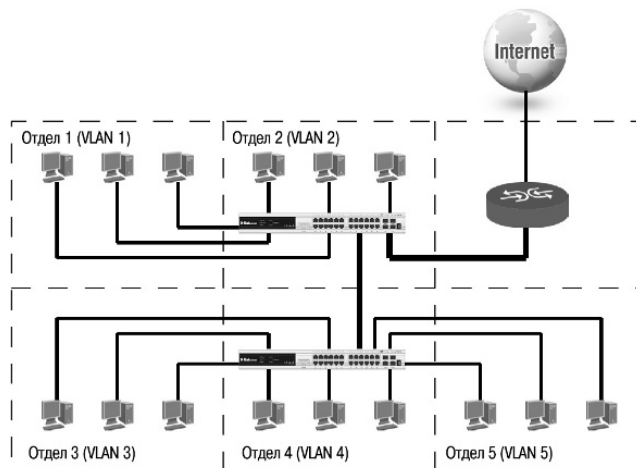


Рис. 2 – Логическая группировка сетевых пользователей в VLAN

Типы VLAN

В коммутаторах могут быть реализованы следующие типы *VLAN*:

- на основе портов;
- на основе стандарта *IEEE 802.1Q*;
- на основе стандарта *IEEE 802.1ad* (*Q-in-Q VLAN*);
- на основе портов и протоколов *IEEE 802.1v*;
- на основе MAC-адресов;
- асимметричные.

Также, для *сегментирования* сети на канальном уровне модели *OSI* в коммутаторах могут использоваться другие функции, например *функция Traffic Segmentation*.

VLAN на основе портов

При использовании *VLAN* на основе портов (*Port-based VLAN*) каждый *порт* назначается в определенную *VLAN*, независимо от того, какой *пользователь* или *компьютер* подключен к этому порту. Это означает, что все пользователи, подключенные к этому порту, будут членами одной *VLAN*. *Конфигурация* портов статическая и может быть изменена только вручную (рис.3).

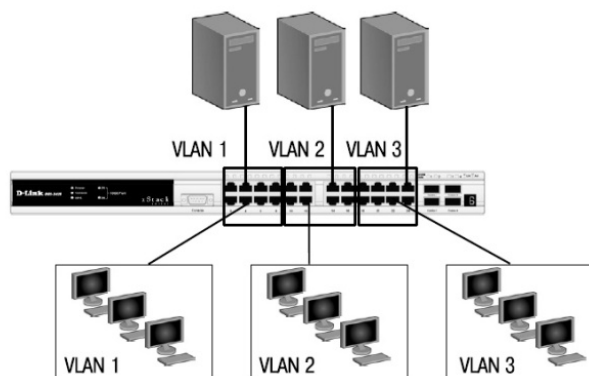


Рис. 3 – VLAN на основе портов

Основные характеристики *VLAN* на основе портов:

1. применяются в пределах одного коммутатора. Если необходимо организовать несколько рабочих групп в пределах небольшой сети на основе одного коммутатора, например, необходимо разнести технический отдел и отдел продаж, то решение *VLAN* на базе портов оптимально подходит для данной задачи;

2. простота настройки. Создание виртуальных сетей на основе группирования портов не требует от администратора большого объема ручной работы — достаточно всем портам, помещаемым в одну *VLAN*, присвоить одинаковый идентификатор *VLAN* (*VLAN ID*);

3. возможность изменения логической топологии сети без физического перемещения станций. Достаточно всего лишь изменить настройки порта с одной *VLAN* (например, *VLAN* технического отдела) на другую (*VLAN* отдела продаж), и рабочая станция сразу же получает возможность совместно использовать ресурсы с членами новой *VLAN*. Таким образом, *VLAN* обеспечивают гибкость при перемещениях, изменениях и наращивании сети;

4. каждый порт может входить только в одну *VLAN*. Для объединения виртуальных подсетей как внутри одного коммутатора, так и между двумя коммутаторами, нужно использовать сетевой уровень OSI-модели. Один из портов каждой *VLAN* подключается к интерфейсу маршрутизатора, который создает таблицу маршрутизации для пересылки кадров из одной подсети (*VLAN*) в другую (IP-адреса подсетей должны быть разными) (рис.4).

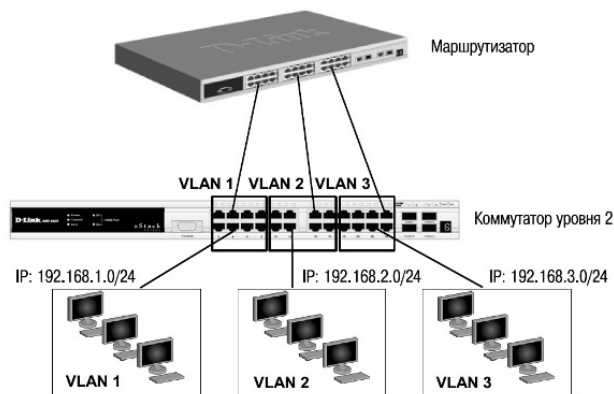


Рис. 4. – Объединение VLAN с помощью маршрутизирующего устройства

Недостатком такого решения является то, что один *порт* каждой *VLAN* необходимо подключать к маршрутизатору. Это приводит к *дополнительным расходам* на покупку кабелей и маршрутизаторов, а также порты коммутатора используются очень расточительно. Решить данную проблему можно двумя способами: использовать коммутаторы, которые на основе фирменного решения позволяют включать *порт* в несколько *VLAN*, или использовать коммутаторы уровня 3.

VLAN на основе стандарта IEEE 802.1Q

Построение *VLAN* на основе портов основано только на добавлении дополнительной информации к адресным таблицам коммутатора и не использует возможности *встраивания* информации о принадлежности к виртуальной сети в передаваемый кадр. *Виртуальные локальные сети*, построенные на основе стандарта *IEEE 802.1Q*, используют дополнительные поля кадра для хранения информации о принадлежности к *VLAN* при его перемещении по сети. С точки зрения удобства и гибкости настроек, *VLAN* стандарта *IEEE 802.1Q* является лучшим решением по сравнению с *VLAN* на основе портов. **Его основные преимущества:**

1. гибкость и удобство в настройке и изменении – можно создавать необходимые комбинации *VLAN* как в пределах одного коммутатора, так и во всей сети, построенной на коммутаторах с поддержкой стандарта *IEEE 802.1Q*. Способность добавления тегов позволяет информации о *VLAN* распространяться через множество 802.1Q-совместимых коммутаторов по одному физическому соединению (*магистральному каналу*, *Trunk Link*);

2. позволяет активизировать алгоритм связующего дерева (*Spanning Tree*) на всех портах и работать в обычном режиме. Протокол *Spanning Tree* оказывается весьма полезным для применения в крупных сетях, построенных на нескольких коммутаторах, и позволяет коммутаторам автоматически определять древовидную конфигурацию связей в сети при произвольном соединении портов между собой.

Для нормальной работы коммутатора требуется отсутствие *замкнутых маршрутов* в сети. Эти маршруты могут создаваться администратором специально для образования

резервных связей или же возникать случайным образом, что вполне возможно, если сеть имеет многочисленные связи, а кабельная система плохо структурирована или документирована. С помощью протокола *Spanning Tree* коммутаторы после построения схемы сети блокируют избыточные маршруты. Таким образом, автоматически предотвращается возникновение петель в сети;

3. способность *VLAN IEEE 802.1Q* добавлять и извлекать теги из заголовков кадров позволяет использовать в сети коммутаторы и сетевые устройства, которые не поддерживают стандарт *IEEE 802.1Q*;

4. устройства разных производителей, поддерживающие стандарт, могут работать вместе, независимо от какого-либо фирменного решения;

5. чтобы связать подсети на сетевом уровне, необходим маршрутизатор или коммутатор L3. Однако для более простых случаев, например, для организации доступа к серверу из различных *VLAN*, маршрутизатор не потребуется. Нужно включить порт коммутатора, к которому подключен сервер, во все подсети, а сетевой адаптер сервера должен поддерживать стандарт *IEEE 802.1Q* (рис.5).

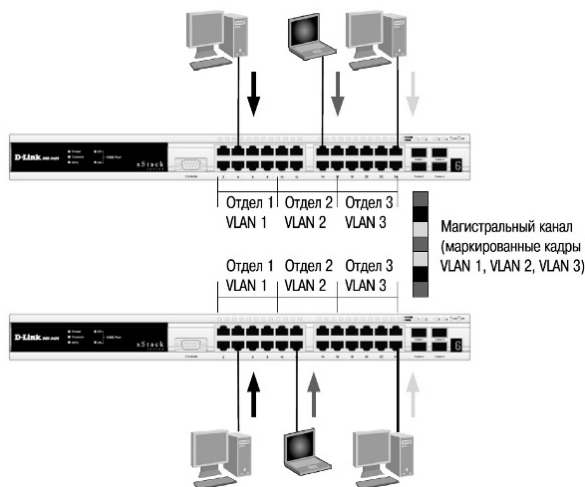


Рис. 5 – Передача кадров разных VLAN по магистральному каналу связи

Вот определения некоторых терминов, необходимых для понимания работы VLAN в сети:

– **Tagging (Маркировка пакета)** – процесс добавления информации о принадлежности к 802.1Q VLAN в заголовок кадра. Порты, на которых включена маркировка пакетов, могут добавлять в заголовки всех передаваемых пакетов номер VID, информацию о приоритете и пр. Если пакет приходит на порт уже маркированным, то данный пакет не изменяется и таким образом при пересылке сохраняется вся информация о VLAN. Маркировка пакетов в основном применяется для пересылки пакетов между устройствами, поддерживающими стандарт 802.1Q VLAN.

– **Untagging** – процесс извлечения информации 802.1Q VLAN из заголовка пакета. Порты, на которых включена данная функция, извлекают всю информацию, касающуюся VLAN из заголовков как входящих, так и исходящих пакетов, проходящих через данный порт. Если же пакет не содержит тэг VLAN'а, то порт не изменяет такой пакет. Данная функция коммутатора применяется при передаче пакетов от коммутаторов, поддерживающих стандарт 802.1Q на устройства, не поддерживающие этот стандарт.

Для согласования работы устройств, поддерживающих формат кадра 802.1 Q, с теми устройствами, которые не понимают этот формат, разработчики стандарта предложили делить весь трафик в сети на несколько типов.

– **Трафик входного порта (Ingress Port).** Каждый кадр, достигающий коммутируемой сети и идущий либо от маршрутизатора, либо от рабочей станции, имеет определенный порт-источник. На основании его номера коммутатор должен "принять решение" о приеме (или отбрасывании) кадра и передаче его в ту или иную VLAN.

Коммутатор проверяет пакет на наличие информации VLAN и на ее основании принимает решение о пересылке пакета.

Если пакет содержит информацию о VLAN, входной порт сначала определяет, является ли он сам членом данного VLAN. Если нет, то пакет отбрасывается. Если да, то определяется, является ли порт назначения членом данного VLAN. Если оба порта являются членами одного VLAN'а, то пакет пересылается.

Если пакет не содержит в заголовке информацию VLAN, т.е. является немаркированным пакетом (*untagged*), то входящий порт добавляет в заголовок пакета метку в соответствии со своим PVID (если он является маркированным портом (*tagged*)). Затем определяется, принадлежат ли входной порт и порт назначения одному VLAN (имеют одинаковые VID). Если нет, пакет отбрасывается. Если да, то пакет передается.

Если же входящий порт является немаркированным портом, то перед пересылкой проверяется только, являются ли входной порт и порт назначения членами одной VLAN.

Этот процесс называется *ingress filtering* (входной фильтрацией) и используется для сохранения пропускной способности внутри коммутатора.

– **Трафик выходного порта** (*Egress Port*). Чтобы попасть в межсетевой маршрутизатор или в оконечную рабочую станцию, кадр должен выйти за пределы коммутатора сети. Коммутатор "решает", какому порту (или портам) нужно передать пакет и есть ли необходимость удалять из него служебную информацию, предусмотренную стандартом 802.1Q. Дело в том, что традиционные рабочие станции не всегда воспринимают информацию о VLAN по стандарту 802.1Q, но сервер, обслуживающий несколько подсетей с помощью единственного интерфейса, должен ее активно использовать. Если выходной порт подключен к коммутатору, поддерживающему стандарт 802.1Q, то следует включить маркировку пакетов на данном порту, чтобы другой коммутатор мог получать информацию о VLAN и на ее основе принимать решения о передаче пакета. Если выходной порт подключен к устройству, не поддерживающему стандарт 802.1Q, то тэги должны извлекаться из заголовка пакета и теперь уже обычный пакет Ethernet может быть принят конечным устройством.

Любой порт коммутатора может быть настроен как *tagged* (маркированный) или как *untagged* (немаркированный). Функция *untagging*, позволяет работать с теми сетевыми устройствами виртуальной сети, которые не понимают тегов в заголовке кадра Ethernet. Функция *tagging* позволяет настраивать *VLAN* между несколькими коммутаторами, поддерживающими стандарт *IEEE 802.1Q* (рис.6).

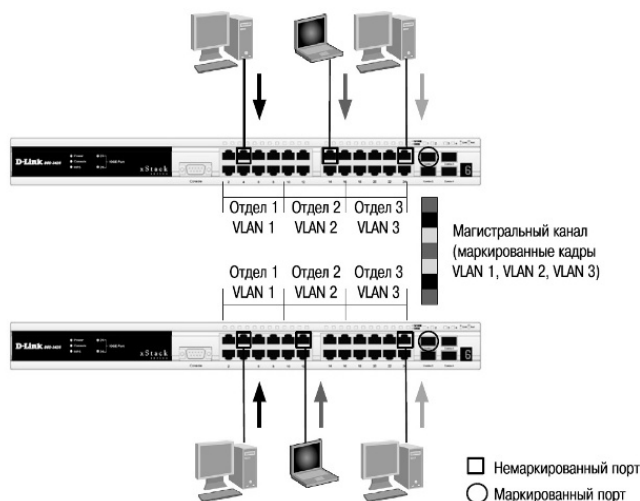


Рис. 6 – Маркированные и немаркированные порты VLAN

Тег VLAN IEEE 802.1Q

Стандарт *IEEE 802.1Q* определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о *VLAN* по сети. На рис. 7 изображен формат тега 802.1Q *VLAN*. К кадру Ethernet добавлены 32 бита (4 байта), которые увеличивают его

размер до 1522 байт. Первые 2 байта (поле Tag Protocol Identifier, TPID) с фиксированным значением 0x8100 определяют, что кадр содержит тег протокола 802.1Q. Остальные 2 байта содержат следующую информацию:

- Priority ("Приоритет") – 3 бита поля приоритета передачи кодируют до восьми уровней приоритета (от 0 до 7, где 7 – наивысший приоритет), которые используются в стандарте 802.1p;
- Canonical Format Indicator (CFI) – 1 бит индикатора канонического формата зарезервирован для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet;
- VID (VLAN ID) – 12-битный идентификатор VLAN определяет, какой VLAN принадлежит трафик. Поскольку под поле VID отведено 12 бит, то можно задать 4094 уникальных VLAN (VID 0 и VID 4095 зарезервированы).

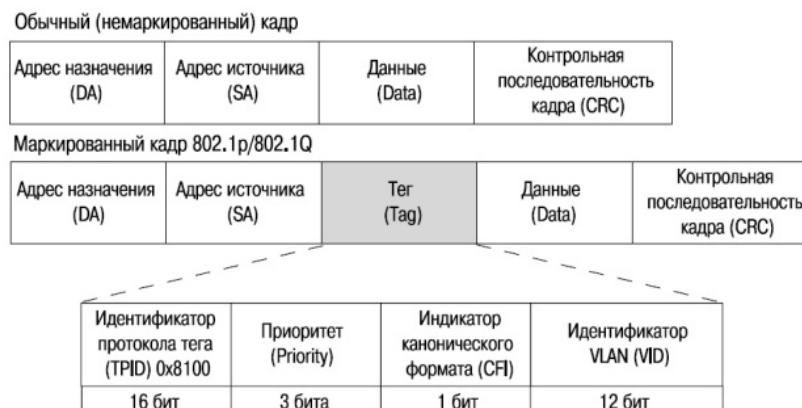


Рис. 7. – Маркированный кадр Ethernet

Port VLAN ID

Каждый физический порт коммутатора имеет параметр, называемый *идентификатор порта VLAN (PVID)*. Этот параметр используется для того, чтобы определить, в какую VLAN коммутатор направит входящий немаркированный кадр с подключенного к порту сегмента, когда кадр нужно передать на другой порт (внутри коммутатора в заголовки всех *немаркированных кадров* добавляется идентификатор VID, равный PVID порта, на который они были приняты). Этот механизм позволяет одновременно существовать в одной сети устройствам с поддержкой и без поддержки стандарта IEEE 802.1Q.

Коммутаторы, поддерживающие протокол IEEE 802.1Q, должны хранить таблицу, связывающую идентификаторы портов PVID с идентификаторами VID сети. При этом каждый порт такого коммутатора может иметь только один PVID и столько идентификаторов VID, сколько поддерживает данная модель коммутатора.

VLAN на основе портов и протоколов -стандарт IEEE 802.1v

Стандарт IEEE 802.1v является расширением стандарта IEEE 802.1Q. Он позволяет объединять узлы сети в *виртуальные локальные сети* на основе поддерживаемых ими протоколов. При определении членства в VLAN стандарт классифицирует немаркированные кадры по типу протокола и порту. Формат тега 802.1v аналогичен формату тега 802.1Q. В стандарте IEEE 802.1v определены следующие правила классификации входящих кадров (рис.8):

- при поступлении на порт *немаркированного* кадра, коммутатором осуществляется проверка заголовка канального уровня и типа протокола вышележащего уровня. Если тип протокола соответствует типу VLAN 802.1v на этом порте, то в заголовок кадра добавляется тег с идентификатором VID, равным идентификатору соответствующей

VLAN 802.1v. Если совпадения не найдены, то в заголовок кадра добавляется тег с идентификатором *VID*, равным идентификатору входного порта *PVID*;

- при поступлении на порт *маркированного* кадра значение тега *VLAN* в нем не изменяется.

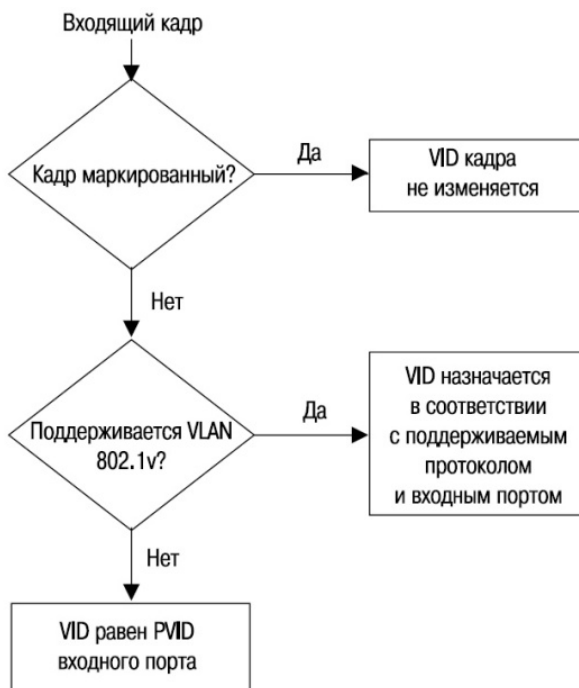


Рис. 8 – Правила классификации входящих кадров

Внутри коммутатора все кадры являются маркированными. Передача кадров осуществляется на основе таблицы *VLAN* путем сравнения значений идентификаторов *VID*. Если *порт* назначения является членом той же *VLAN*, что и *входной порт*, то он передает *кадр* в подключенный к нему сегмент сети. В противном случае *кадр* отбрасывается.

Для выходных портов действуют такие же правила, как для стандарта *IEEE 802.1Q*.

Механизм классификации 802.1v требует, чтобы на коммутаторе были настроены группы протоколов. Каждый протокол в группе определяется типом кадра и значением поля идентификации протокола в нем. *Порт* может быть ассоциирован с несколькими группами протоколов, что позволяет классифицировать поступающие немаркированные кадры *по* принадлежности к разным *VLAN* в зависимости от их содержимого. Одна и та же *группа* протоколов может быть ассоциирована с разными портами коммутатора, при этом на каждом входном порте ей должны быть присвоены уникальные идентификаторы *VLAN*.

Следующий способ, который используется для образования виртуальных сетей, основан на группировке **MAC-адресов**. При существовании в сети большого количества узлов этот способ требует большого количества ручных операций от администратора. Однако, он оказывается более гибким при построении виртуальных сетей на основе нескольких коммутаторов, чем способ группировки портов. Группирование **MAC-адресов** в сеть на каждом коммутаторе избавляет от необходимости их связи несколькими портами, однако, требует выполнения большого количества ручных операций по маркировке MAC-адресов в сеть на каждом коммутаторе сети.

Широковещательные домены на базе **MAC-адресов**, позволяют физически перемещать станцию, позволяя оставаться ей в одном и том же широковещательном домене без каких-либо изменений в настройках конфигурации.

Настройка виртуальной сети на основе MAC-адресов может отнять много времени - представьте себе, что вам потребуется связать с VLAN адреса 1000 устройств. Кроме того, MAC-адреса "наглухо защиты" в оборудование и может потребоваться много

времени на выяснение адресов устройств в большой, территориально распределенной сети.

Асимметричные VLAN

Для обеспечения возможности использования разделяемых ресурсов (серверов, Интернет-шлюзов и т.д.) пользователями из разных сетей *VLAN* в программном обеспечении коммутаторов **2-го уровня** D-Link реализована *поддержка* функции *Asymmetric VLAN* (асимметричные *VLAN*). Эта *функция* позволяет клиентам из разных *VLAN* взаимодействовать с разделяемыми устройствами (например, серверами), *не поддерживающими тегирование 802.1Q*, через один *физический канал* связи с коммутатором, не требуя использования внешнего маршрутизатора. Активизация функции *Asymmetric VLAN* на коммутаторе 2-го уровня позволяет сделать его *немаркированные* порты членами *нескольких виртуальных локальных сетей*. При этом рабочие станции остаются полностью изолированными друг от друга.

Например, асимметричные *VLAN* могут быть настроены так, чтобы обеспечить *доступ* к почтовому серверу всем почтовым клиентам. Клиенты смогут отправлять и получать данные через *порт* коммутатора, подключенный к почтовому серверу, но прием и передача данных через остальные порты будет для них запрещена.

При активизации асимметричных *VLAN* каждому порту коммутатора назначается уникальный PVID в соответствии с идентификатором *VLAN*, членом которой он является. При этом каждый *порт* может получать кадры от *VLAN* по умолчанию.

Основное различие между базовым стандартом 802.1Q *VLAN* (или симметричными *VLAN*) и асимметричными *VLAN* заключается в том, как выполняется *отображение* MAC-адресов. Симметричные *VLAN* используют отдельные адресные таблицы, и, таким образом, не происходит пересечения MAC-адресов между *виртуальными локальными сетями*. Асимметричные *VLAN* используют одну общую таблицу MAC-адресов.

Вопросы

1. Понятие виртуальной локальной сети
2. Типы VLAN. VLAN на основе портов.
3. VLAN на основе стандарта IEEE 802.1Q
4. Определения терминов, необходимых для понимания работы VLAN в сети

Список литературы

Основная литература:

1. Новиков Ю.В. Основы локальных сетей [Электронный ресурс]/ Новиков Ю.В., Кондратенко С.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 405 с.— Режим доступа: <http://www.iprbookshop.ru/22425>.— ЭБС «IPRbooks», по паролю

Дополнительная литература

1. Построение коммутируемых компьютерных сетей / Е.В. Смирнова, И.В. Баскаков, А.В. Пролетарский, Р.А. Федотов. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 429 с. : схем., ил. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=429834>
2. Сеницын Ю.И. Волоконно-оптические линии связи в компьютерных сетях и телекоммуникациях [Электронный ресурс]: методические указания к практическим и лабораторным занятиям/ Сеницын Ю.И.— Электрон. текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2014.— 142 с.— Режим доступа: <http://www.iprbookshop.ru/50050>.— ЭБС «IPRbooks», по паролю

Интернет-ресурсы:

1. <http://www.intuit.ru> — сайт дистанционного образования в области информационных технологий

- 2.<http://www.iqlib.ru> - интернет библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия;
- 3.<http://www.biblioclub.ru> - электронная библиотечная система «Университетская библиотека – online»: специализируется на учебных материалах для ВУЗов по научно-гуманитарной тематике, а так же содержит материалы по точным и естественным наукам.
- 4.<http://window.edu.ru> – образовательные ресурсы ведущих вузов.
- 5.<http://algotlist.manual.ru> - сайт, посвященный алгоритмам и методам.
- 6.<http://www.intuit.ru/> - Образовательный портал. Текстовые и видеолекции.
- 7.[www. http://bic.pfnrcfu.ru](http://bic.pfnrcfu.ru) Электронная библиотека СКФУ