Министерство образования Республики Беларусь
Учреждение образования «Витебский государственный университет имени П.М. Машерова»
Кафедра прикладного и системного программирования

В.В. Новый

КОМПЬЮТЕРНЫЕ СЕТИ

Курс лекций

Витебск
ВГУ имени П.М. Машерова
2023

УДК 004.7(075.8)
ББК 32.971.35я73
Н76

Печатается по решению научно-методического совета учреждения образования «Витебский государственный университет имени П.М. Машерова». Протокол № 1 от 30.10.2023.

Автор: старший преподаватель кафедры прикладного и системного программирования ВГУ имени П.М. Машерова, магистр педагогики **В.В. Новый**

Р е ц е н з е н т :
доцент кафедры информационных технологий и управления бизнесом
ВГУ имени П.М. Машерова,
кандидат биологических наук, доцент *А.А. Чиркина*

Новый, В.В.

Н76 Компьютерные сети : курс лекций / В.В. Новый. – Витебск : ВГУ имени П.М. Машерова, 2023. – 83 с.

ISBN 978-985-30-0081-8.

В данном курсе лекций приведены материалы для систематизации знаний в рамках дисциплины «Компьютерные сети», читаемой студентам специальности «Информационные системы и технологии (в здравоохранении)». Содержание предлагаемого учебного издания соответствует тематике указанной дисциплины и может быть использовано в ходе подготовки к лабораторным занятиям, контрольным работам и экзамену.

Предназначается для студентов специальности «Информационные системы и технологии (в здравоохранении)».

УДК 004.7(075.8)
ББК 32.971.35я73

ISBN 978-985-30-0081-8

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Компьютерные сети и сетевые технологии прочно вошли практически во все сферы современной жизни и особую важную роль играют в информационных технологиях. Данное учебное издание предлагает материалы конспекта лекций, читаемых для студентов специальности «Информационные системы и технологии (в здравоохранении)» в рамках дисциплины государственного компонента учебного плана специальности «Компьютерные сети».

Материал охватывает все темы курса и построен в соответствии с нисходящим подходом к изучению дисциплины: изложение начинается с общей терминологии и освоения верхних уровней стека протоколов и продолжает рассмотрение тем в соответствии с моделью OSI и движением к нижнему, физическому уровню.

Курс лекций позволяет повторить необходимый для успешного выполнения лабораторных и контрольных работ материал дисциплины «Компьютерные сети», в частности вопросы, связанные с IP-адресацией, маршрутизацией в сетях, основными службами сети Интернет. Рекомендуемые материалы могут служить отправной точкой для подготовки к сдаче экзамена по дисциплине или углубленного изучения отдельных вопросов.

Приведенная информация соответствует темам рабочей программы дисциплины «Компьютерные сети» специальности «Информационные системы и технологии (в здравоохранении)».

Лекция № 1. Введение

Основные понятия дисциплины

Сеть (**Network**) – взаимодействующая совокупность **объектов** (**узлов**, **nodes**).

Компьютерная сеть или *сеть передачи данных* (**Computer Network**) – это совокупность связанных между собой компьютеров, телекоммуникационного оборудования и программного обеспечения, обеспечивающая информационный обмен между компьютерами в сети.

Узел компьютерной сети – **хост** или **конечная система**.

Конечные системы соединяются между собой при помощи **линий связи** и **коммутаторов пакетов**.

Пакеты – отдельные порции информации, передаваемые по сети.

Состав компьютерной сети.

- Компьютеры, соответствующие назначению компьютерной сети;
- Коммуникационное оборудование;
- Сетевые операционные системы (NOS – Network Operation System);
- Сетевые приложения.

Телекоммуникации – (греч. **tele** – вдаль, далеко и лат. **communicatio** – общение) – это передача и прием любой информации (звука, изображения, данных, текста) на расстояние по различным электромагнитным системам.

Телекоммуникационная сеть – это система технических средств, посредством которой осуществляются телекоммуникации.

Телекоммуникационную сеть условно принято разделять на коммуникационную сеть и информационную сеть (см. рис. 1.1).

Коммуникационная сеть – предназначена для передачи данных.

Информационная сеть – предназначена для обработки, хранения и передачи данных и создается подключением к коммуникационной сети абонентских систем.

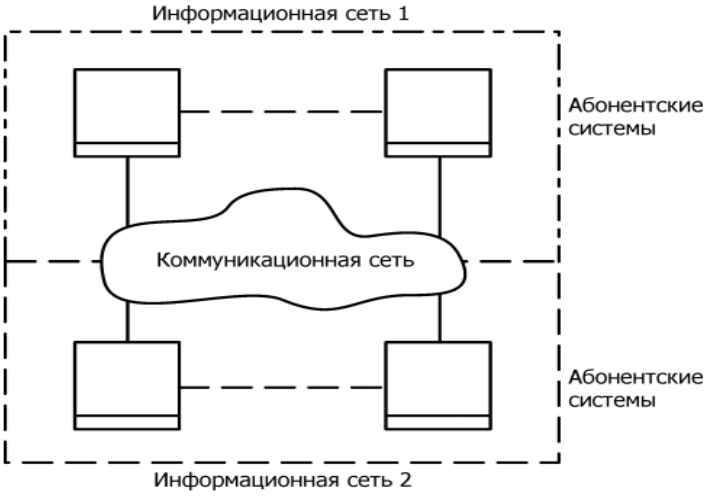

Рисунок 1.1 – Структура телекоммуникационной сети

К телекоммуникационным сетям относятся:

- Компьютерные сети (передача данных);
- Телефонные сети (передача голосовой информации);
- Радиосети (передача голосовой информации – широковещательные услуги);
- Телеграфные сети (передача текстовых сообщений);
- Телевизионные сети и т.д.

Телекоммуникационные сети

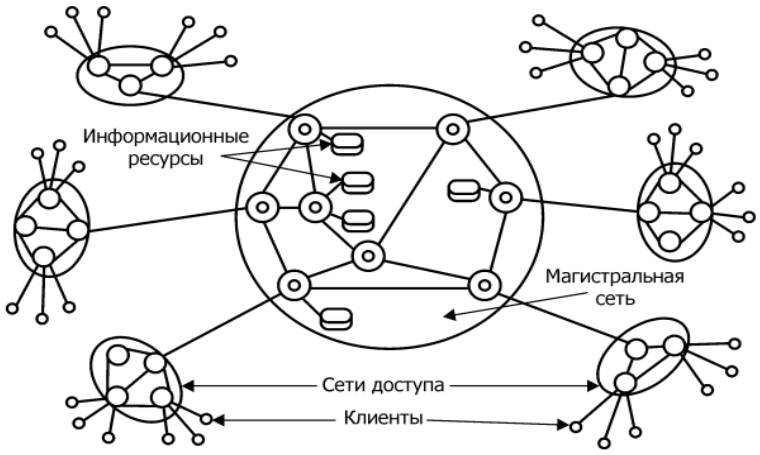

Рисунок 1.2 – Состав телекоммуникационной сети

Состав телекоммуникационных сетей (см. рис. 1.2):

- **сети доступа** (access network);
- **магистральная сеть** или **магистраль** (core network или backbone);
- **информационные центры** или центры управления сервисами (data centers или service control point).

Сеть доступа – нижний уровень ТС, к которому подключаются «конечные узлы» – оборудование пользователей.

Магистральная сеть – объединяет СД и выполняет транзит трафика по высокоскоростным каналам.

Информационные центры – собственные информационные ресурсы сети на основе которых выполняется обслуживание пользователей.

Классификации сетей

- По территориальному признаку
- По масштабу производственного объединения
- По технологии передачи
- По принципу организации обмена данными между абонентами
- По типу среды передачи данных
- По принципу организации иерархии компьютеров и т.д.

Классификация сетей по территориальному признаку:

- **Локальные сети** (ЛС, LAN – Local Area Network);

- **Глобальные сети** (ГС, WAN – Wide Area Network);
- **Региональные** (городские) **сети** (MAN, Metropolitan Area Network).

Локальная сеть – сеть ЭВМ, включающая в себя узлы, расположенные в пределах одного помещения, здания или небольшой территории, позволяющая обмениваться данными и совместно использовать различные устройства.

Примеры: компьютерная сеть в отдельной лаборатории университета, локальная сеть главного корпуса университета, а также сеть, расположенная в главном корпусе университета и корпусе худграфа.

Глобальные сети – сети, объединяющие территориально рассредоточенные компьютеры, возможно находящиеся в различных городах и странах.

Примеры: глобальная сеть Интернет, сеть Fido и др.

Региональные (городские) **сети** – сети, предназначенные для обслуживания территории района, крупного города или региона.

Пример: городские сети определенного провайдера интернет-услуг, например, МТС.

Классификация по масштабу производственного подразделения:

- **Сети отделов** (рабочих групп);
- **Сети кампусов** (от англ campus – университет, территория университета) а также домовые сети, объединяющие несколько домов;
- **Корпоративные сети** (сети масштаба предприятия – enterprise wide networks).

Классификация по технологии передачи данных:

Вещание (или один – ко многим) использует broadcast или, по-другому, основана на разделяемых каналах передачи данных (shared channel);

Соединение точка – точка (point-to-point) – передача данных ведется между двумя абонентами.

Классификация по принципу организации обмена данными между абонентами:

Сети на основе коммутации:

- Каналов;
- Пакетов;
- *Сообщений (промежуточный вариант)*.

Коммутация – технология выбора направления и организации передачи данных в сетях, имеющих несколько альтернативных маршрутов, по которым может производиться обмен информацией между двумя узлами.

При этом передаваемые по сети информационные потоки называются сетевым **трафиком** (от англ. traffic – движение).

Классификация по типу среды передачи данных:

– Проводные (wired) (коаксиальный кабель, витая пара, оптоволоконные линии);
– Беспроводные (wireless) (радиочастоты, инфракрасный диапазон).

Классификация по принципу организации иерархии компьютеров:

– Одноранговые (Peer-to-Peer Network);
– Клиент-серверные (с выделенным сервером, Dedicated Server Network).

Сервер (от англ. *server* – служащий, служитель) – компьютер или программа, предоставляющая услуги другим компьютерам или программам, обычно называемым **клиентами**.

Клиент – это компьютер или программа, запрашивающая некоторые услуги.

Распределенная программа – это программа, состоящая из нескольких взаимодействующих частей, причем каждая часть может выполняться и, как правило, выполняется на отдельном компьютере.

Основное назначение компьютерных сетей

– Обеспечение доступа к разделяемым ресурсам;
– Межперсональная коммуникация.

Разделяемый (сетевой) **ресурс** (**network share**) – это устройство или информация, к которой возможен удалённый доступ с другого компьютера (обычно в ЛС или интранет), как к локальному ресурсу.

Услуги доступа к ресурсам:

– Удаленный доступ (Remote Login);
– Передача файлов (File Transfer);
– Удаленный вызов процедур (RPC – Remote procedure call);
– Совместное использование устройств.

Услуги межперсональной коммуникации:

– Электронная почта (e-mail) 1:1
– Списки рассылки (news group) 1:n
– Телеконференции n:n
– Системы электронных бюллетеней (BBS – Bulletin Board System)
– Видеоконференции и т.д.

История сетей

60-е – DARPA ведет проект по объединению двух удаленных мейнфреймов, первые глобальные связи компьютеров, эксперименты с пакетными сетями, начало передачи голоса по телефонным сетям в цифровой форме.

1969 год – ARPA (Advanced Research Project Agency) мин.обороны США инициировала работы по объединению в единую сеть суперкомпьютеров оборонных и научно-исследовательских центров – сеть ARPANET (см. рис. 1.3–1.4).

Рисунок 1.3 – Начало развития ARPANET

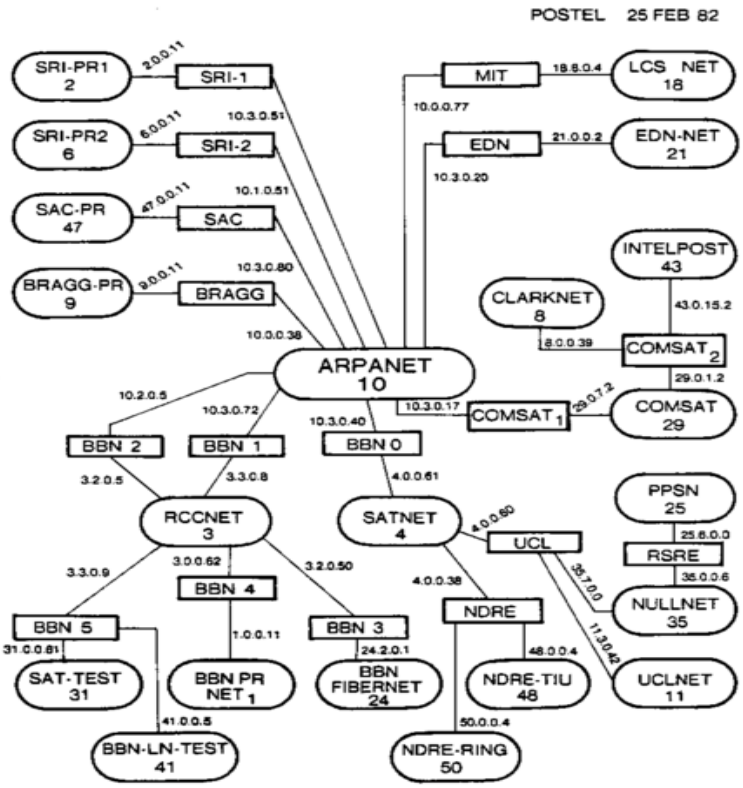

Рисунок 1.4 – Сеть ARPANETв 1982 году

Начало 70-х – появление первых нестандартных локальных сетей.

1971 г. – инженер BBN Рей Томлинсон написал первую программу для работы с электронной почтой.

1973 г. – Роберт Меткалф (Xerox) предложил идею и название сетевой технологии – Ethernet (см. рис. 1.5).

1974 год – Винтон Серф и Роберт Кан разработали протокол управления передачей TCP.

1978/79 – разработка эталонной модели OSI.

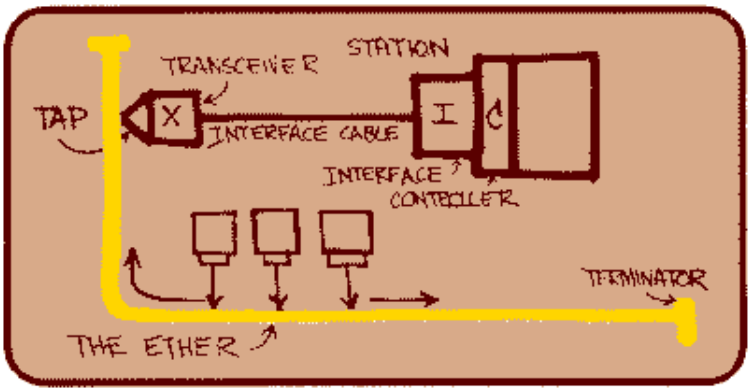

Рисунок 1.5 – Один из набросков сети Ethernet Роберта Меткалфа

Начало 1980-х – создание стека протоколов TCP/IP, рассчитанного на независимость компьютера и сети. Развертывание его на всех узлах ARPANET-сетей и создание сети Интернет в современном виде.

2 ноября 1988 года – червь Морриса (т.н. великий червь) поразил около 6000 узлов ARPANET и практически вывел из строя сеть. Как один из результатов была организована CERT (computer emergency response team).

Середина 80-х – разработка стандартных технологии локальных сетей (1980 – Ethernet, 1985 – Token Ring, 1985 – FDDI).

Конец 1980-х – начало 1990-х – замена ARPANET на NSFNet – сеть национального научного фонда NSF (National Science Foundation).

1991–1992 год – изобретение в CERN Тимом Бернерс-Ли с коллегами технологии World Wide Web.

1994 – создание протокола PPP

1995 – замена сети NFSNet более современной коммерческой опорной сетью и появление поставщиков услуг Интернета (ISP, Internet Service Providers). Переход к современному статусу сети Интернет.

Лекция № 2. Сетевые модели и протоколы

Протокол и стек протоколов (см. рис. 2.1)

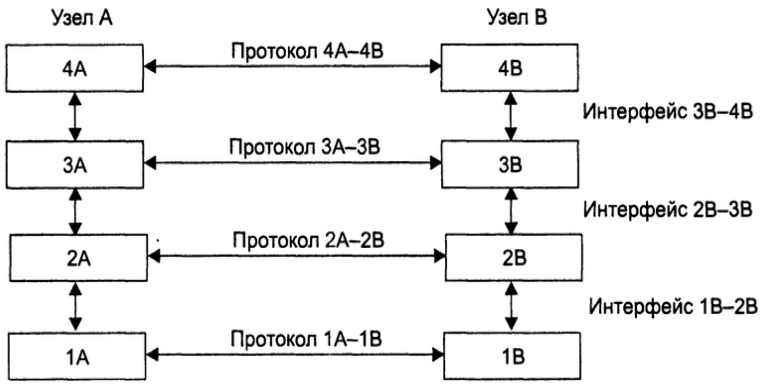

Рисунок 2.1 – Понятие стека протоколов

Коммуникационный протокол – формализованный набор правил взаимодействия узлов сети;

Стек протоколов – иерархически организованный набор протоколов, достаточный для взаимодействия узлов в сети.

Эталонная модель OSI (Open System Interconnection)

Разработана в начале 80-х ISO как международный стандарт архитектуры компьютерной сети.

Определяет уровни взаимодействия в сетях с коммутацией пакетов, стандартные названия уровней и функции, которые должен выполнять каждый уровень.

Уровни OSI (см. рис. 2.2)

1. Прикладной <==== Верхний
2. Представления данных
3. Сеансовый
4. Транспортный
5. Сетевой
6. Канальный
7. Физический <==== Нижний

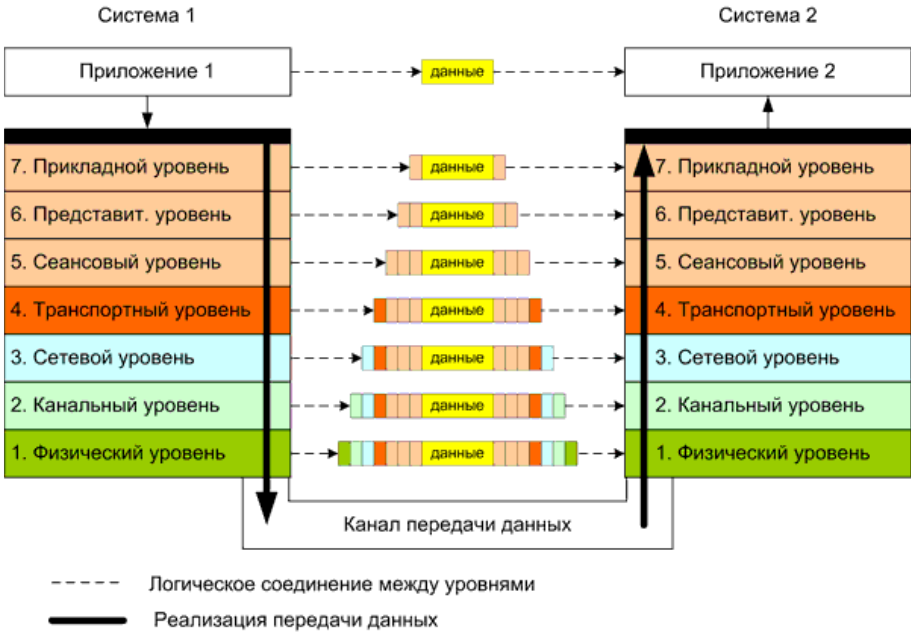

Рисунок 2.2 – Модель OSI

Физический уровень (physical layer)

Функция: передача потока битов по физическим каналам связи (например, витая пара).

Реализуется на всех устройствах, подключенных к сети.

Пример протокола: спецификация 100Base-T4 стандарта Ethernet

Канальный уровень (data link layer)

Первый из уровней, который работает в режиме коммутации пакетов.

PDU (Protocol Data Unit) носит название кадр (frame).

Функции:

для LAN: обеспечить доставку кадра между любыми узлами сети;

для WAN: обеспечить доставку кадра между двумя соседними узлами, соединенными индивидуальной линией связи. (PPP, HDLC).

Поддержание интерфейсов с физическим и сетевым уровнями.

Задачи:

- Обнаружение и коррекция ошибок;
- Проверка доступности среды передачи данных (иногда выделяют в отдельный подуровень – управления доступом к среде (Media Access Control, MAC)

Реализуется компьютерами (адаптер+драйвер), мостами, коммутаторами и маршрутизаторами.

Сетевой уровень (network layer)

Служит для образования составной сети или межсетевого взаимодействия (internetworking)

Реализуется группой протоколов и маршрутизаторами.

Функции:

- Физическое объединение сетей;
- PDU сетевого уровня – пакет

Задачи:

- Связь между транспортным и канальным уровнями;
- определение маршрута;

Пример протоколов: IP, IPX, RIP, BGP

Транспортный уровень (transport layer)

Обеспечивает верхним уровням стека передачу данных с нужной степенью надежности.

OSI определяет 5 классов транспортного сервиса: от 0 (низший) до 4 (высший).

Все протоколы с транспортного уровня и выше реализуются ПО сетевых узлов.

PDU (Protocol Data Unit, единица данных протокола) – сегмент или дейтаграмма (датаграмма).

Задачи:

- Реализация транспортного соединения;
- Мультиплексирование/демультиплексирование нескольких транспортных соединений в одном сетевом;
- Управление потоком.

Пример: TCP, UDP

Сеансовый уровень (session layer)

Обеспечивает управление взаимодействием сторон и предоставляет средства синхронизации сеанса.

Пример: SSH

Уровень представления данных (presentation layer)

Обеспечивает представление передаваемой информации не меняя ее содержания.

Задачи:

- Отображение данных (из локальной формы в сетевую);
- Шифрование/дешифрование данных (пример – SSL – Secure Socket Layer);
- Сжатие данных.

Прикладной уровень (application layer)

Набор протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, а также организуют совместную работу.

PDU – сообщение (message).

Примеры: FTP, SMB, NCP.

Модель DoD (или модель межсетевых связей)

Четырехуровневая модель сетевого взаимодействия, разработанная Министерством обороны США (Department of Defense).

Практической реализацией этой модели является стек протоколов TCP/IP, поэтому она также называется моделью TCP/IP.

Уровни модели:

1. Уровень приложений (объединяет функциональность прикладного уровня, уровня представления данных и сеансового из модели OSI);
2. Транспортный уровень (примерно соответствует транспортному уровню модели OSI).
3. Межсетевой (Internet) (соответствует сетевому уровню OSI).
4. Уровень доступа к сети (объединяет функциональность канального и физического уровней OSI).

Стандартные стеки коммуникационных протоколов:

- OSI
- TCP/IP
- IPX/SPX
- NetBIOS/SMB
- DECnet
- SNA

Лекция № 3. Прикладной уровень

Набор протоколов с помощью которых пользователи сети получают доступ к разделяемым ресурсам, а также организуют совместную работу.

Архитектура прикладных протоколов Internet

Принципы построения протокола:

- «клиент-сервер»;

Примеры: веб-сервер и браузер, сервер TELNET и TELNET-клиент.

Клиентская и серверная стороны взаимодействуют обмениваясь сообщениями.

– Peer-to-peer.

Участники взаимодействия равноправны.

На прикладном уровне конечная точка коммуникации задается с помощью **сокета** (интерфейс между прикладным и транспортным уровнями).

1. Имя хоста:
   – Символьное имя;
   – IP-адрес.
2. Идентификация процесса производится с помощью уникального для каждого процесса хоста номера порта.

(HTTP – 80, SMTP – 25, …)

Соответствующие номера портов заданы в RFC-1700, RFC-3232, и на www.iana.org.

По принципу передачи данных:

– Текстовые протоколы;
– Бинарные протоколы.

Как правило, прикладной протокол определяет следующие элементы:

– Типы используемых сообщений (запросы и ответы);
– Синтаксис каждого из типов сообщений;
– Семантику полей (смысл содержащейся в них информации);
– Правила, описывающие события, которые вызывают генерацию сообщений.

Система доменных имен

– Небольшие сети – плоские имена (NW1_1, MAIL2)
– Крупные сети – доменная система имен (en.wikipedia.org, msdn.microsoft.com).

<простое_имя_хоста>.<имя_домена_N>.<имя_домена_N-1>…..<имя_домена_верхнего_уровня>

Домен имен – множество хостов, объединенное в логическую группу.

Каждый домен разделяется на поддомены, которые в свою очередь могут состоять из других доменов => все множество доменов можно представить в виде иерархической древовидной системы.

Различают:

– Краткое доменное имя;
– Относительное доменное имя;
– Полное доменное имя (FQDN – Fully Qualified Domain Name)

Домены верхнего уровня разделяются на 2 основных группы:

– Родовые (com, edu, org, …);
– Домены государств (by, ru, uk, us, …).

Помимо этого, в последнее время вошли в практику т.н. sponsored-домены – домены верхнего уровня, зарегистрированные на определенную компанию или организацию на платной основе для последующей продажи (аренды) доменных имен.

Корневой домен управляется IANA.

Разрешение доменных имен основано на специальной службе – DNS (Domain Name System).

DNS – централизованная служба, основанная на распределенной базе записей ресурсов.

У каждого домена в базе может быть ассоциированный с ним набор записей ресурсов. В большинстве случаев, запись ресурса – ASCII строка из таких полей:

DomainName Class Type Value

DomainName – имя домена, к которому относится запись;

Class – тип сети (для Internet – IN);

Type – тип записи (A – IP-адрес хоста, NS – информация о сервере имен верхнего уровня, CNAME – псевдоним, MX – запись почтового сервера и др.);

Value – значение, которое зависит от типа записи.

Все пространство имен DNS поделено на непересекающиеся зоны.

Каждая зона содержит часть общего дерева имен и обслуживается отдельным основным сервером имен.

За разрешение символьного имени в операционной системе отвечает отдельный компонент – т.н. резольвер DNS (resolver).

Основные схемы разрешения DNS-имен:

- Рекурсивная (косвенная);
- Нерекурсивная (итеративная);
- Гибридная (объединение первых двух).

Рекурсивная схема

DNS-клиент запрашивает локальный DNS-сервер (сервер поддомена клиента);

Альтернатива:

DNS-сервер знает ответ (имя из его зоны или оно сохранено в кэше) – сервер посылает ответ клиенту.

Сервер не знает ответ – сервер выполняет итеративные запросы к корневому серверу и получив ответ возвращает его клиенту.

Итеративная схема

DNS-клиент обращается к корневому серверу с указанием полного доменного имени.

DNS-сервер отвечает клиенту указав адрес следующего DNS-сервера, обслуживающего домен верхнего уровня, из старшей части запроса.

DNS-клиент делает запрос к следующему серверу, пока не будет найден DNS-сервер в котором хранится соответствие запрошенного имени IP-адресу. Этот сервер дает окончательный ответ клиенту.

Обратная зона

Для решения обратной задачи – поиска DNS-имени по IP-адресу используется обратная зона – система таблиц, которая хранит соответствие между IP-адресами и DNS-именами хостов сети.

Используется специальная зона in-addr.arpa (ip6.arpa)

Пример: для адреса 192.31.106.10 заводится запись 10.106.31.192.in-addr.arpa.

Для ускорения поиска IP-адресов DNS-сервера применяется кэширование проходящих через них ответов.

Для оперативной реакции на изменения имена кэшируются на относительно короткое время.

Порядок разрешения имени в Windows:

- Проверка имени локального узла;
- Кэш DNS (запросы+файл hosts);
- Запрос DNS-серверу;
- Если имя не плоское – **Ошибка !!!**,
- иначе – NetBIOS имя в кэше;
- Запрос WINS-серверу;
- Широковещательный запрос в подсеть (x3);
- Файл lmhosts.
- Ошибка!!!

Файл hosts расположен в ОС Windows по пути /Windows/system32/drivers/etc/hosts и в ОС GNU/Linux /etc/hosts.

Протокол передачи файлов FTP

File Transfer Protocol – услуги передачи файлов между удаленными компьютерами.

Поддерживает идентификацию по уникальной учетной записи (unique user account) или через анонимную учетную запись (anonymous account).

Использует два TCP соединения: управляющее и передачи данных.

Управляющее соединение инициируется интерпретаторами протоколов PI (Protocol Interface) на 21 порт TCP. Активно в течение всего сеанса (см. рис. 3.1).

Используется для обмена командами и ответами на базе протокола NVT.

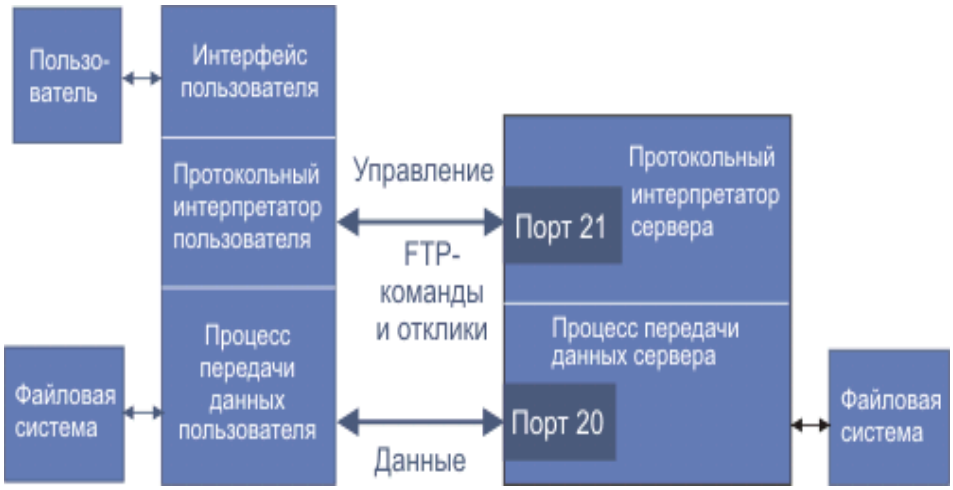

Рисунок 3.1 – Обмен данными в протоколе FTP

Для каждой операции по передаче файла – отдельное соединение передачи данных. Подробное описание в RFC 959. Пример взаимодействия клиента с сервером FTP

Протокол TFTP

TFTP (Trivial FTP) – упрощенная версия FTP.

Не имеет системы безопасности и идентификации.

Базируется на протоколе UDP (69 порт).

Данные передаются блоками по 512 байт.

Используется для загрузки ОС в бездисковые рабочие станции и конфигурационных файлов в маршрутизатор.

Электронная почта (E-mail)

В основе лежит модель обмена электронными сообщениями X.400.

Модель включает следующие компоненты (см. рис. 3.2):

UA (User Agent) или MUA (Mail User Agent) – агент пользователя (почтовый клиент);

MTA (MessageTransfer Agent) – агент передачи сообщений;

MDA (Message Delivery Agent) – агент доставки сообщений

MS (Message Store) – банк сообщений.

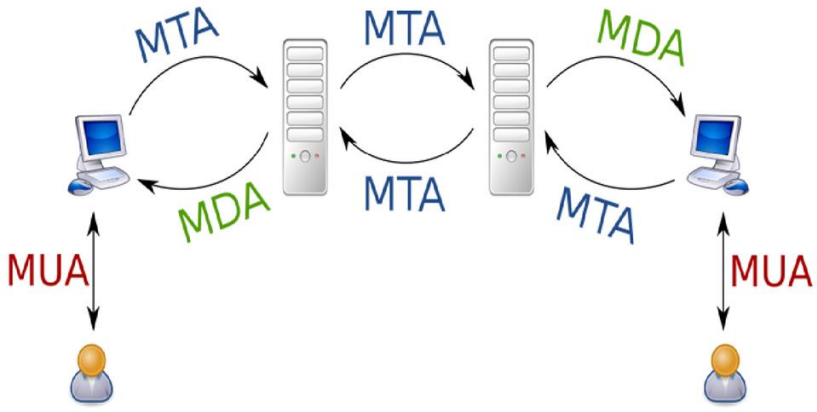

Рисунок 3.2 – Архитектура электронной почты

Функции MTA:

- Прием сообщений для доставки (mail submission);
- Маршрутизация сообщений;
- Формирование сообщения о невозможности доставки;
- Создание копии сообщения и доставка их по разным адресам.

Основные протоколы:

Отправка:

SMTP (Simple Mail Transfer Protocol) RFC 2821 (ESMTP – Extended SMTP RFC 5321)

Доставка:

POP3 (Post Office Protocol v.3) RFC 1939

IMAP4 (Internet Mail Access Protocol) RFC 2060.

WEB-доступ по протоколам HTTP/HTTPS

Сообщение = тело + заголовок, которые помещаются в «конверт» (envelope) в кодировке ASCII. Структура заголовков определяется в RFC 5322 (RFC 822).

Для передачи сообщений в других кодировках используется **Многоцелевое расширение почты Интернета** (Multipurpose Internet Mail Extensions, MIME) RFC 2045 и 2046.

Наиболее важные заголовки RFC 5322:

- From:
- To:
- Sender:
- Return-Path:
- Cc: (Carbon Copy – «под копирку»)
- Received:

Наиболее важные заголовки MIME:

- Content-Type:
- Content-Transfer-Encoding:

POP3. Использует 110 порт.

Состоит из 3 фаз:

- Авторизация
- Транзакция
- Обновление

Поддерживается только полнотекстовая авторизация.

IMAP4 (порт 143 TCP)

Поддерживает:

- организацию иерархии папок на почтовом сервере;
- поиск писем, отвечающих заданному условию;
- позволяет получать отдельные компоненты сообщений: заголовки, части составных MIME-сообщений;
- поддерживает различные схемы авторизации.

Протокол HTTP

HTTP (HyperText Transfer Protocol) – ядро технологии WWW (World Wide Web, web).

WWW – основа доступа к связанным между собой документам – страницам.

Каждая страница может содержать гиперссылки, на другие станицы. Поэтому такое множество страниц называется гипертекстом.

Агент пользователя – браузер.

Протокол реализован в виде набора команд, передаваемых посредством строк текста в формате ASCII.

Взаимодействие по протоколу состоит из транзакции HTTP, включающих следующие части:

1. К: Установление соединения (connection request);
2. К: Запрос (request);
3. С: Ответ (response);
4. С: Завершение соединения;

Шаги 1–4 повторяются для каждого из объектов.

С 1998 года переход на HTTP 1.1:

- конвейеризация запросов (отправка в рамках долговременного соединения нескольких запросов без ожидания ответов на предыдущие);
- постоянные соединения.

В настоящее время принят стандарт HTTP/2 (ранее HTTP 2.0) основанный на SPDY.

Для идентификации ресурсов используется URI (Universal Resource Identifier) – универсальный идентификатор ресурса. URI включает имя ресурса, его местоположение и используемый протокол.

На практике часто используется частный случай URI – URL (Universal Resource Locator):

<схема_доступа>://<имя_сервера>:<порт>/<имя_ресурса>?<параметры>

Протокол поддерживает 2 типа сообщений: запрос и ответ (подробнее см. лаб. работы в СДО).

Дополнительную информация RFC 1945 (HTTP 1.0), 2616 (HTTP 1.1), 7540 (HTTP/2).

Структура HTTP-запроса:

Начальная строка (Start Line) – содержит запрашиваемую команду или индикатор статуса ответа

[Заголовки (Headers)]

Пустая строка (Empty Line) – окончание раздела заголовков

[Тело сообщения (Message body)]

Начальная строка:

RequestType RequestURI HTTPVersion

HTTP 1.1 определяет 7 типов сообщений-запросов:

GET – запрос на информацию, определенную значением переменной RequestURI;

HEAD – ответ должен содержать только начальную строку и заголовки. Тело не включается.

POST – требует, чтобы информация, включенная в тело сообщения была принята системой назначения в качестве дополнения к ресурсу;

OPTIONS – запрос на получение информации об опциях обмена;

PUT – требует, чтобы информация, включенная в тело сообщения была сохранена в месте, заданном RequestURI;

DELETE – запрос на уничтожение системой назначения ресурса, заданного RequestURI;

TRACE – требует, чтобы система назначения выполнила на прикладном уровне обратную петли и возвратила сообщение отправителю;

CONNECT – зарезервирован для использования прокси-серверами.

HTTPVersion указывает версию протокола HTTP, поддерживаемую системой, создавшей запрос.

- HTTP/0.9
- HTTP/1.0
- HTTP/1.1

Простейший запрос:

GET / HTTP/1.1

Заголовки HTTP

Текстовые строки в формате:

FieldName: FieldValue

- FieldName – идентифицирует тип информации в заголовке
- FieldValue – содержит саму информацию

Включают информацию о системе и характере запроса.

Сервер может использовать, а может и игнорировать информацию из заголовков.

Управление сетями. SNMP-модель

NMS (система управления сетью):

- Управление конфигурацией сети и именованием элементов сети (NE);
- Обработка ошибок;
- Анализ производительности и надежности;
- Управление безопасностью;
- Учет работы сети.

Основная схема:

- Менеджер (запрашивает данные объекта);
- Агент (наполняет MIB данными объекта);
- Управляемый объект (NE).

MIB (Management Information Base) – модель управляемого объекта – база данных управляющей информации.

SNMP (Simple Network Management Protocol).

UDP 161, UDP 162.

Менеджер может запросить информацию (GET-request, GET-next-request) или обновить конфигурацию (SET-request).

Агент отвечает (GET-response) или может предоставить информацию сам (TRAP).

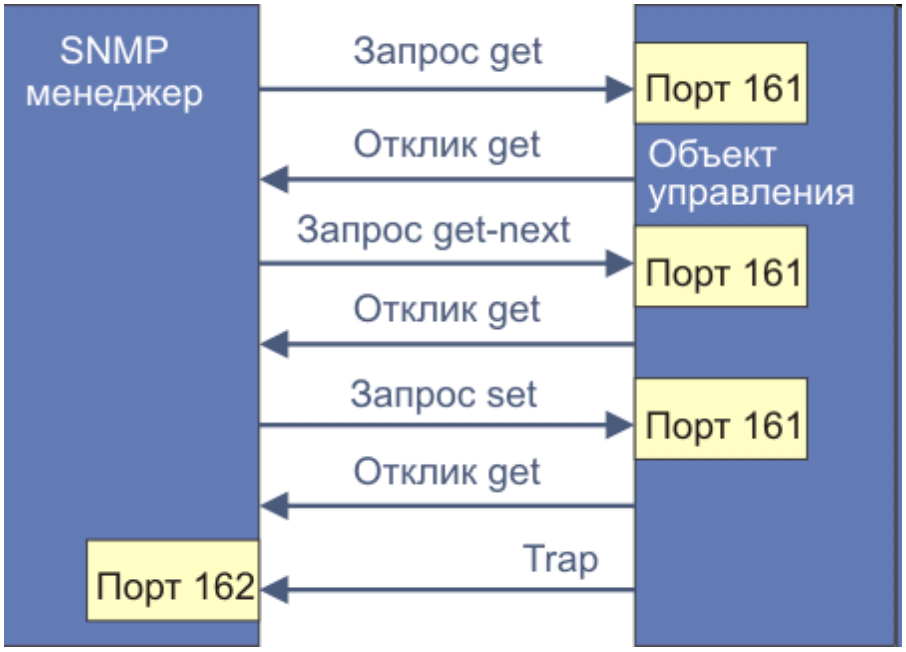

Рисунок 3.3 – Сообщения протокола SNMP

Структура управляющей информации MIB описывается с помощью ASN.1 (abstract syntax notation 1).

Каждый описываемый объект имеет уникальный идентификатор объекта (OID). Например: 1.3.6.1.4.1.171.30.2.1.0

iso.org.dod.internet.private.enterprises.171.11.30.2.1.adslmode

0=link down, 1=T1-413, 2=G-lite, 3=G-DMT

Лекция № 4. Транспортный уровень

Транспортный уровень (transport layer) Обеспечивает приложениям или верхним уровням передачу данных с нужной степенью надежности.

Выбор сервиса:

– степенью надежности верхних уровней;

– качеством линий связи.

PDU – сегмент или дейтаграмма (датаграмма)

Пример: TCP, SPX, DCCP, SCTP

Два основных протокола транспортного уровня:

- TCP (Transmission Control Protocol) – протокол управления передачей (RFC 793);
- UDP (User Datagram Protocol) – протокол пользовательских дейтаграмм (RFC 768).

Ошибки передачи:

- искажение;
- потеря;
- дублирование пакетов;
- нарушение порядка.

Протокол UDP

Дейтаграммный режим работы;
Получение и защита от дублирования не гарантированы;
Возможна широковещательная рассылка.
Структура UDP-дейтаграммы представлена ниже (рис. 4.1).

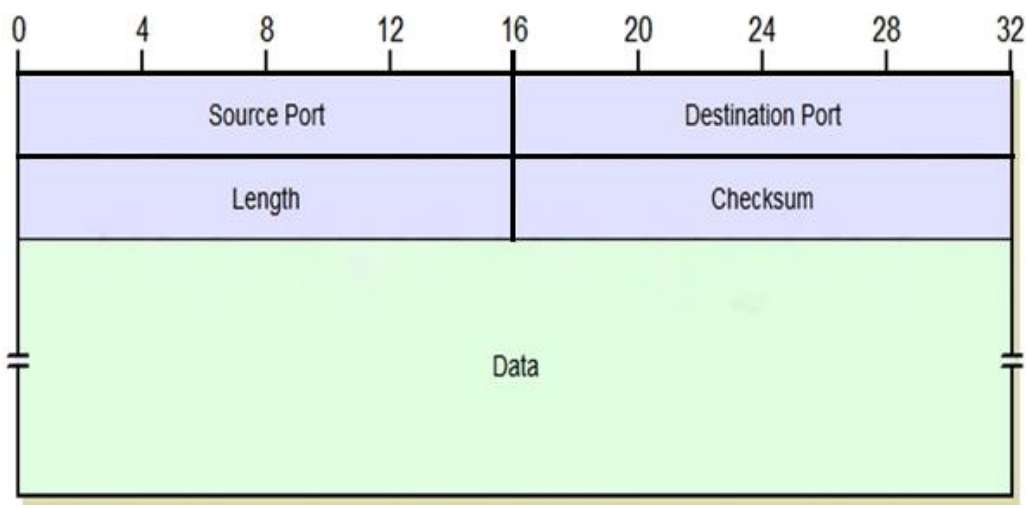

Рисунок 4.1 – UDP-дейтаграмма

Length – длина пакета в байтах (заголовок + данные); min=8;
Source Port* – порт отправителя;
Destination Port – порт получателя;
Checksum* – контрольная сумма;
Data – поле данных [0 – 65507 байт]
* – не обязательны (0);

Контрольная сумма – 16 битное дополнение до 1 суммы дополнений UDP заголовка, данных и псевдозаголовка (содержит данные из заголовка в протоколе IP). В случае необходимости дейтаграмма дополняется в конце нулевыми байтами, чтобы их общее число было четным.

Если расчетная контрольная сумма равна нулю, она передается как поле, целиком состоящее из единиц. Вычисление контрольной суммы не обязательно (в этом случае поле = 0).

Для получения адресной информации для сокета используется т.н. псевдозаголовок (см. рис. 4.2) – фрагмент заголовка IP-дейтаграммы с сетевого уровня:

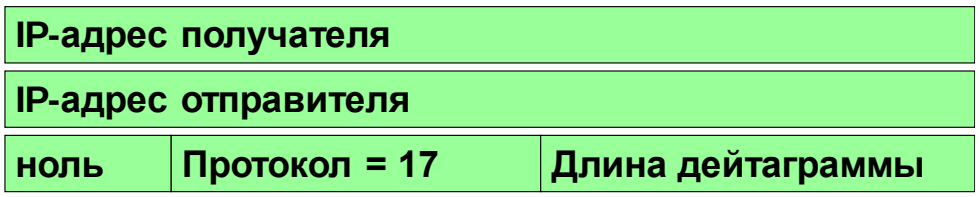

Рисунок 4.2 – Формат псевдозаголовка

Длина псеводзаголовка 12 байт (4+4+1+1+2)

Протокол: UDP=17; TCP=6

Один из плюсов UDP – возможность широковещательной и групповой рассылки.

- сохраняет границы сообщений прикладного протокола;
- никогда не объединяет и не делит сообщения (обычно – 8192 и менее).

Прикладной процесс в сети однозначно определяет пара (IP-адрес, номер порта UDP), называемая UDP-сокетом.

Протокол TCP

TCP обеспечивает надежную передачу данных: гарантирует, что вся переданная информация будет получена в правильном порядке и без искажений.

Для обращения к службе TCP должно быть установлено соединение – задан блок управления соединением на каждой из сторон:

- Адреса сокетов;
- Последовательные номера передаваемых байтов;
- Размер окна;
- Максимальный размер сегмента.

Аналогично UDP, прикладной процесс в сети однозначно определяет пара (IP-адрес, номер порта TCP), называемая TCP-сокетом, а логическое соединение – пара сокетов.

Один сокет одновременно может участвовать в нескольких соединениях.

Соединения – дуплексные, двухточечные (point-to-point).

Широковещательная и групповая рассылка протоколом TCP не поддерживается.

TCP-соединение реализует неструктурированный байтовый поток, буферизируемый средствами TCP;

PDU – сегмент;

размер сегмента ограничивается размером поля данных IP-пакета;

границы между сегментами не сохраняются;

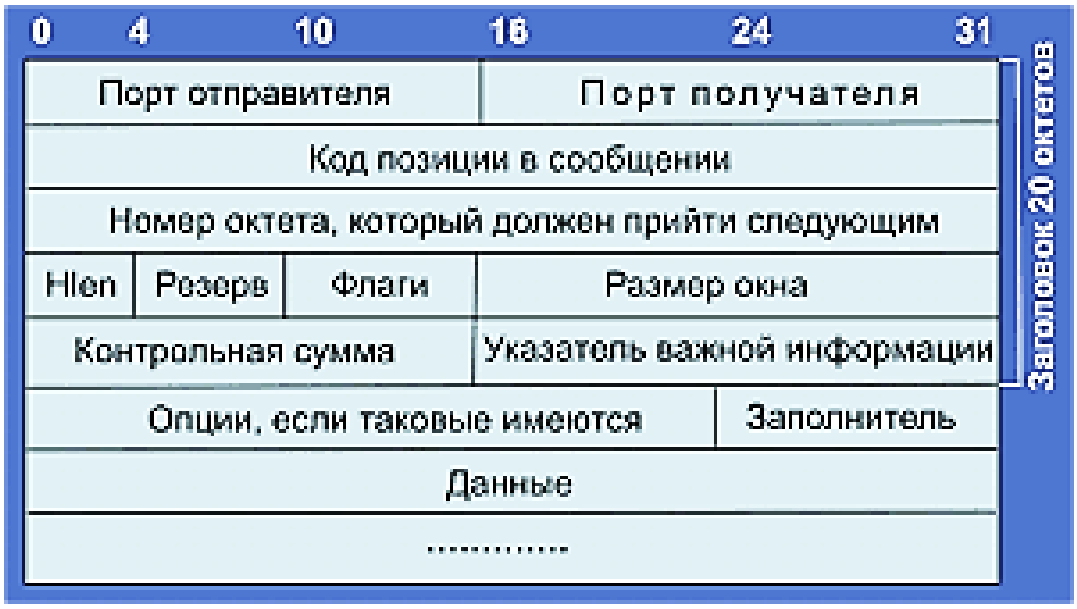

Рисунок 4.3 – Формат сегмента TCP

Структура сегмента (см. рис. 4.3):

порт отправителя (Source Port) (2 байта);

порт получателя (Destination Port) (2 байта);

код позиции в сообщении (Sequence Number или номер подтверждения) (4 байта);

номер октета, который должен прийти следующим (Acknowledgment Number) (4 байта);

Hlen – длина TCP заголовка в 32-битных словах (Data Offset) (4 бита);

Порядковый номер – служит для нумерации каждого байта в пределах блока данных. Начальный порядковый номер задается синхронизирующим генератором в TCP. Генератор увеличивает младший разряд слова каждые 4мс, что позволяет не повторять номера в течение ~4,6 часа.

Номер подтверждения – следующий ожидаемый байт (действует, если флаг ACK=1, иначе это не подтверждение)

Длина заголовка задает длину в 32-разрядных словах (нужно так как заголовок может иметь переменную длину – поле Параметры)

резерв (6 бит);

флаги (Control Bits) (6 бит);

размер окна передачи (Window) (2 байта);

контрольная сумма (Checksum) (2 байта);

указатель важной информации (Urgent Pointer) – используется только тогда, когда установлен флаг URG (см. ниже) (2 байта);

опции – дополнительные данные заголовка (макс. 3 байта);

заполнитель (Padding) – заполнитель переменной длины (для выравнивания на границу 32 бит);

данные.

Контрольная сумма содержит контрольную сумму заголовка, данных и псевдозаголовка. Алгоритм: суммирование всех 16-разрядных слов в дополнительном коде, а затем вычисление дополнения к сумме. В результате, когда получатель считает контрольную сумму (вместе с полем контрольной суммы) результат должен быть равен 0.

Флаги:

URG (Urgent) – срочное сообщение;

ACK (Acknowledgment) – квитанция на принятый сегмент;

PSH (Push) – запрос на отправку сообщения без ожидания заполнения буфера;

RST (Reset) – запрос на восстановление соединения;

SYN (Synchronize) – синхронизация счетчиков переданных данных;

FIN (Finish) – признак достижения передающей стороной последнего байта в потоке.

Структура псевдозаголовка совпадает с приведенной для протокола UDP за исключением номера протокола (TCP=6) и указанием длины TCP-сегмента вместо длины UDP-дейтаграммы.

Механизмы, обеспечивающие надежность протокола TCP:

- предварительное установление логического соединения;
- контроль доставки по контрольным суммам;
- циклическая нумерация пакетов;
- установление тайм-аутов доставки;
- квитирование;

Соединение в TCP устанавливается с помощью 3 этапного механизма, известного как «тройное рукопожатие» (TCP three-way/triple handshake) (см. рис. 4.4).

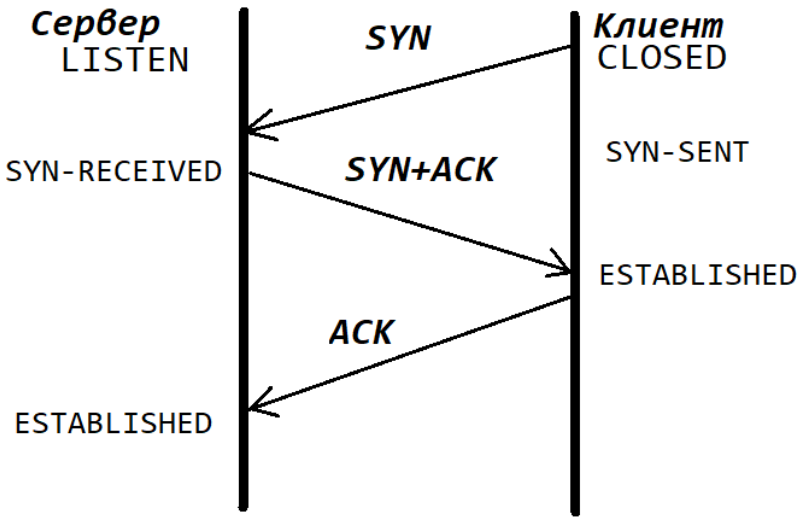

Рисунок 4.4 – «Тройное рукопожатие» TCP

Квитирование

Правильность передачи каждого сегмента подтверждается **квитанцией** от получателя.

При установлении соединения стороны договариваются о начальных номерах (у каждой – свой). Идентификатором каждого сегмента является номер его первого байта – последовательный номер.

По нему идентифицируется сегмент, обнаруживаются дубликаты или потеря данных.

Квитанция – ответное сообщение получателя с подтверждающим номером на единицу превышающим макс номер байта в полученном сегменте.

Квитанции могут подтверждать сразу несколько сегментов.

Используется частный случай квитирования – **алгоритм скользящего окна** (см. рис. 4.5).

Управление передачей осуществляет получатель, указывая Размер окна. Данное окно задает диапазон номеров очереди, который TCP в данный момент может принять.

Рисунок 4.5 – Алгоритм скользящего окна

Таким образом в потоке можно выделить: байты для которых сегменты отправлены и подтверждены, байты, сегменты которых отправлены, но не подтверждены, байты, которые могут быть отправлены (входят в окно) и байты которые не могут быть отправлены, пока окно не сдвинется. Механизм скользящего окна позволяет решить вопрос управления потоком данных.

Когда TCP отправляет сегмент, он помещает его в ***очередь повторной передачи*** и запускает **таймер**. Если подтверждение пришло до истечения времени таймера, сегмент удаляется из очереди, иначе пересылается повторно.

Таймеры в TCP:

- Таймер повторной передачи (retransmission timer);
- Таймер настойчивости (persistence timer) – применяется для предотвращения тупиковой ситуации с размером окна 0. По истечении посылает сегмент с запросом о размере окна;
- Таймер контроля соединения (keep-alive timer) – позволяет периодически проверять состояние и разрывать (5–45 с) соединение;

– Таймер задержки (quiet timer) – отсчитывает двойное время жизни пакетов, чтобы гарантировать, что после закрытия соединения будет отсутствие пакетов в сети для нового соединения;
– Таймер разъединения (idle timer) – ограничивает время ожидания ответа ~360 с.

Борьба с перегрузкой в TCP

– Алгоритм медленного старта (старт передачи с размером окна, равным длине максимального сегмента и удваивание размера окна, если период ожидания подтверждения не превышен);
– Использование порогового значения (по тайм-ауту пороговое значение уменьшается вдвое, а окно перегрузки – до одного сегмента).

Производительность TCP

1. Задержка подтверждений и обновлений размера окна, для того чтобы получить дополнительные данные и подтвердить их вместе.
2. Алгоритм Нагля (Nagle). Накопление данных в буфере, пока не будет подтвержден предыдущий сегмент.
3. «Синдром узкого окна» – буфер принимающей стороны полон и отправителю об этом известно – окно задается в 0. Читается 1 символ и посылается сообщение, что размер окна увеличился и можно послать 1 байт. Отправитель посылает 1 байт, буфер полон, получатель подтверждает прием и устанавливает размер окна 0. И т.д. Было предложено решение – не посылать уведомление о 1 байтовом окне, а подождать пока буфер освободится больше.
4. Масштаб окна. По умолчанию было 64K. Новые реализации позволяют расширить до 1Г.
5. Механизм отрицательного подтверждения, позволяющий использовать «выборочный повтор» вместо «возврата на n».

Сравнение TCP и UDP

1. UDP не использует соединения, следовательно, ему не нужно поддерживать информацию о состоянии соединения.
2. Небольшой размер заголовка UDP (8 против 20 байт).
3. Улучшенный механизм управления передачей данных приложением у UDP. (*Сообщение UDP отправляет сразу, а TCP может ожидать заполнения буфера => UDP более пригоден для приложения реального времени.*)
4. TCP гарантирует надежную передачу данных.
5. TCP содержит механизмы контроля потока данных.

Процедура приема данных протоколами TCP и UDP, поступающих от нескольких прикладных служб, называется м**ультиплексированием**.

Обратная процедура распределения поступающих от сетевого уровня пакетов между набором высокоуровневых служб называется **демультиплексированием** (см. рис. 4.6).

Пример: открыт браузер, закачка файла и несколько сеансов TELNET. Протокол транспортного уровня должен определить, какому процессу предназначается каждый сегмент данных.

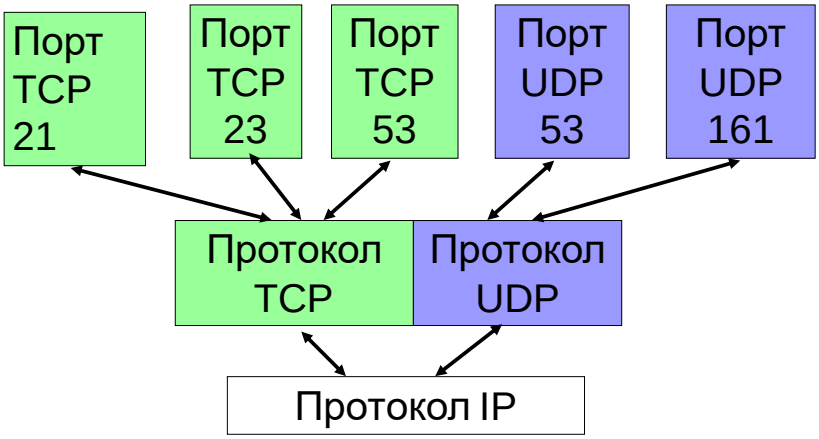

Рисунок 4.6 – Мультиплексирование и демультиплексирование транспортных потоков

TCP и UDP для каждого подключения прикладного процесса ведут 2 очереди:

- очередь поступающих пакетов из сети;
- очередь отправляемых в сеть.

В TCP/IP такие системные очереди называются **портами**, причем входная и выходная очередь рассматриваются как один порт.

Для идентификации портов им присваивают номера. В дальнейшем номера портов используются для адресации приложений.

Номер порта – 16 разрядное целое от 1 до 65535 (0 зарезервирован).

За популярными службами закреплены стандартные номера портов, называемые назначенными номерами или хорошо известными (well-known) – от 0 до 1023.

Управляются www.iana.org (RFC 1700, 3232)

На каждом компьютере ОС ведет список занятых и свободных портов.

Пространства номеров портов TCP и UDP в общем случае не зависимы.

В некоторых случаях, если приложение использует и TCP, и UDP, ему могут быть выделены совпадающие номера TCP- и UDP-портов.

Для точной идентификации процесса в сети используется комбинация из IP-адреса и номера порта, называемая сокет (socket).

API на базе сокетов – основа сетевого ПО TCP/IP и называется sockets.

Версия для Windows называется Windows Sockets или сокращенно WinSock.

Лекция № 5. Сетевой уровень

Основные функции:

- Обеспечение передачи пакетов от отправителя к получателю через составную (объединенную) систему КС
- Выполнение динамической фрагментации пакетов при передаче их между сетями с различными MTU.

Основной протокол сетевого уровня стека TCP/IP – протокол IP (Internet Protocol). Сегодня используются 2 версии этого протокола:

- IPv4 (RFC 791);
- IPv6 (RFC 2373, RFC 2460).

Адресация в IP-сетях

- Локальные адреса (они же аппаратные адреса, они же физические). MAC-адрес сетевого адаптера или маршрутизатора.
- IP-адреса (логические адреса).
- Символьные адреса или имена (DNS-имена или NetBIOS-имена).

Все 3 пространства адресов не зависимы: любой из адресов может быть изменен без влияния на остальные адреса.

Отображение IP-адреса на локальные решается с помощью протоколов разрешения адресов ARP и RARP.

Отображение доменных имен на IP-адреса решается с помощью службы DNS (Domain Name System) основанной на протоколе DNS или службы WINS (для NetBIOS имен).

IP-адрес имеет длину 4 байта и состоит из 2 частей: номера сети и номера узла (см. рис. 5.1).

Рисунок 5.1 – Структура IPv4-адреса

Для удобства каждый адрес делится на 4 октета: 11000000101010000000000100001010=

=11000000.10101000.00000001.00001010=192.168.1.10

IP-адреса структурированы – разбиты на классы. Класс IP адреса определяется значением первых бит адреса (см. рис. 5.2–5.3).

Рисунок 5.2 – Деление адресов IPv4 на классы

Класс	Наименьший адрес	Наибольший адрес	Максимальное число узлов в сети
A	1.0.0.0	126.0.0.0	~2^{24}
B	128.0.0.0	191.255.0.0	~2^{16}
C	192.0.0.0	223.255.255.0	~2^{8}
D	224.0.0.0	239.255.255.255	Multicast
E	240.0.0.0	247.255.255.255	зарезервирован

Рисунок 5.3 – Диапазоны IPv4 адресов, соответствующие классам

В протоколе IP существует ряд специальных адресов:

- адрес текущего узла (узла, который сгенерировал пакет);
- <номер_сети=0>.номер_узла – узел в этой сети (в той же, с которой отправлен пакет)
  (оба адреса могут выступать только как адреса источника!)
- 127.x.y.z – адреса зарезервированы для тестирования сетевого ПО под интерфейс обратной связи (loopback);
- 255.255.255.255 – ограниченная широковещательная рассылка (limited broadcast) (пакет с таким адресом должен рассылаться всем

узлам сети в которой находится источник; маршрутизаторы такой адрес не пропускают);

- <нормер_сети><все_нули> – адрес сети в целом;
- <номер_сети><все_единицы> – широковещательное сообщение (broadcast). Такой пакет рассылается всем узлам сети с заданным номером сети. Пакет с таким адресом может обрабатываться маршрутизаторами.

Multicast или групповой адрес – пакет должен быть доставлен сразу нескольким узлам сети, которые образуют группу с заданным в поле адреса номером.

Узел может входить в несколько групп. Некоторые группы назначаются как заранее заданные.

Примеры:

224.0.0.1 – «все системы в этой подсети»;

224.0.0.2 – «все маршрутизаторы в этой подсети»

У всех узлов одной сети должен быть один и тот же номер сети, но различные номера узлов. Это вызывает проблемы при структуризации сети или ее росте.

Существует 2 решения:

- Получение дополнительных номеров сетей;
- Разделение сетей на подсети с помощью маски.

Маска – это 32-битное число, двоичная запись которого содержит единицы в тех разрядах, которые должны интерпретироваться как номер сети.

Для стандартных классов сетей:

255.0.0.0 – маска сети класса A;

255.255.0.0 – маска сети класса B;

255.255.255.0 – маска сети класса C.

Пусть задана сеть 129.44.0.0 и маска 255.255.192.0

(10000001 00101100 00000000 00000000 AND
11111111 11111111 11000000 00000000)

Это означает, что мы можем использовать 4 подсети:

10000001 00101100 **00**000000 00000000
10000001 00101100 **01**000000 00000000
10000001 00101100 **10**000000 00000000
10000001 00101100 **11**000000 00000000

Теперь адрес 129.44.141.15 при наложении маски подсети

(10000001 00101100 10001101 00001111 AND
11111111 11111111 11000000 00000000
10000001 00101100 10000000 00000000)

будет трактоваться не как узел 141.15 в сети 129.44, а как узел 0.0.13.15 в подсети

129.44.128.0

Это часто обозначается в виде: 129.44.141.15/18, где /18 – означает, что 18 бит слева задают сетевую маску (префикс сети)

Подобный подход и маршрутизация на его основе со второй половины 90-х XX века вытеснила применение классовой маршрутизации.

Разбиение на подсети применимо для внутренней структуризации, в то же время для внешнего мира сеть выглядит единой.

При выборе адресов для сети руководствуются следующими правилами:

Если сеть работает **автономно**, то назначение адресов может быть произвольно. Однако в стандарте определены несколько диапазонов адресов для локального использования – ***приватные адреса*** (т.н. «серые» или «немаршрутизируемые» адреса). Такие адреса **не обрабатываются** маршрутизаторами в сети Интернет.

В классе A – сеть 10.0.0.0;

В классе B – 16 сетей 172.16.0.0 – 172.31.0.0;

В классе C – 255 сетей 192.168.0.0 – 192.168.255.0

Если сеть является частью глобальной сети Internet, то номера сетей назначаются **централизованно**.

С 1998 года регистрацию адресов возглавляет ICANN (Internet Corporation for Assigned Names and Numbers), управляющая 5 основными региональными отделами (Regional Internet Registry, RIR):

- ARIN, обслуживающий Северную Америку;
- APNIC, обслуживающий страны Юго-Восточной Азии;
- AfriNIC, обслуживающий страны Африки;
- LACNIC, обслуживающий страны Южной Америки и бассейна Карибского моря;
- **RIPE NCC** (Reseaux IP Europeens Network Coordination Centre) обслуживающий Европу, Центральную Азию, Ближний Восток. Региональные регистраторы выдают номера **локальным интернет-регистраторам** (Local Internet Registries, LIR), обычно являющимися крупными провайдерами.

Способы решения проблемы дефицита IP-адресов:

- Переход на новую версию IPv6 с 16-байтными адресами;
- Использование масок и технологии бесклассовой междоменной маршрутизации CIDR (Classless Inter-Domain Routing);
- Использование трансляции адресов NAT (Network Address Translation).

Classless Inter-Domain Routing (RFC1517-1520) использует деление IP-адреса на номер сети и номер узла не на основе нескольких старших битов, а на основе маски переменной длины, определяемой ISP. Необходимым условием является наличие у поставщика непрерывного диапазона адресов с одинаковым префиксом – несколькими цифрами в старших разрядах (см. рис 5.4).

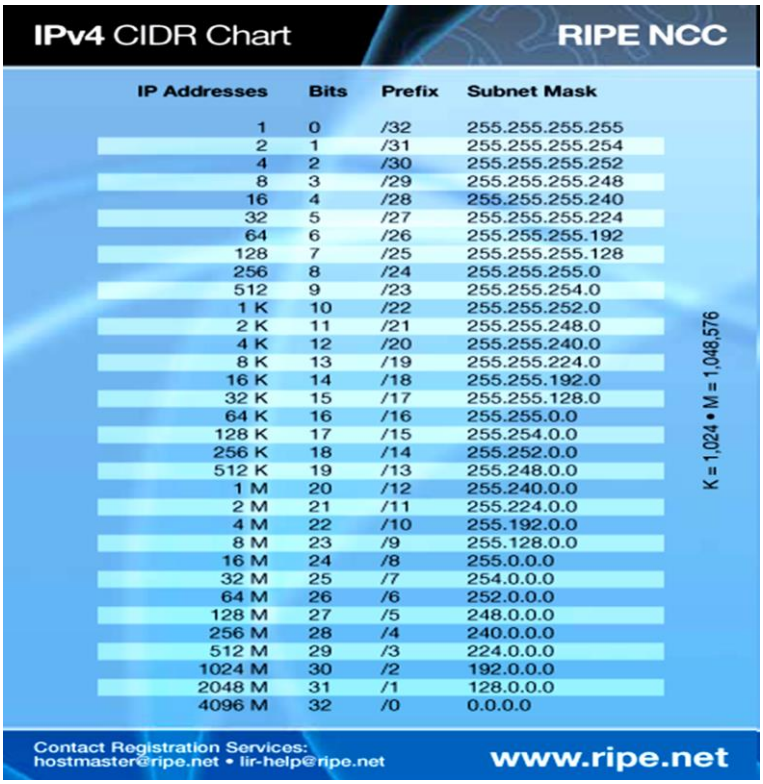

Рисунок 5.4 – Распределение IP-адресов для подсетей

IP (Internet Protocol)

IP относится к протоколам без установления соединения (дейтаграммным).

Каждый IP-пакет обрабатывается независимо от остальных (технология коммутации пакетов)

Размер IP-пакета кратен 32-битовым словам и состоит из заголовка и поля данных (см. рис. 5.5).

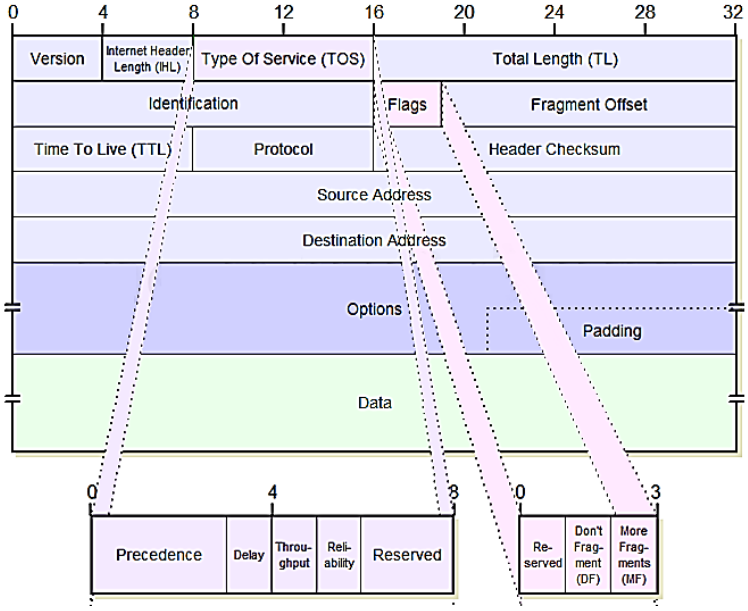

Рисунок 5.5 – Формат заголовка IPv4 пакета

- Номер версии (Version) – IPv4 или IPv6 (4 бит);
- Длина заголовка (Internet Header Length, IHL)(4 бит) – длина заголовка в 32-битных словах (м.б. до 60 байт);
- Тип сервиса (Type Of Service, TOS) 1 байт – задает приоритетность пакета и вид критерия выбора маршрута:
    - PR (Precedence) – подполе приоритета пакета (3 бита). От самого низкого 0 (нормальный пакет) до 7 (управляющая информация).
    - Критерий выбора маршрута (4 бита):
    - D (Delay) – минимизация задержки доставки;
    - T (Throughput) – максимизация пропускной способности;
    - R (Reliability) – максимизация надежности доставки.
    - C (Cost) – минимизация стоимости маршрута
- Зарезервированные биты (=0).
- Общая длина пакета (Total Length, TL, 2 байта) – общая длина с учетом заголовка и поля данных. Максимальное значение – 65535 байт, минимальное – 21 байт;
- Идентификатор пакета (Identification) – используется при фрагментации пакета для его идентификации (для каждого пакета все части должны иметь одно и то же значение);
- Флаги (Flags, 3 бита) – содержит признаки, связанные с фрагментацией:
    - Бит DF (Do not Fragment) – запрещает маршрутизатору фрагментировать пакет. Если такой пакет не м.б. доставлен без фрагментации – он уничтожается.
    - Бит MF (More Fragments) – данный пакет является промежуточным (не последним) фрагментом;
- Смещение фрагмента (Fragment Offset, 13 бит) – смещение поля данных этого пакета в пределах данных исходного пакета.
- Поле время жизни (TTL, Time To Live, 1 байт) – предельный срок в течение которого пакет может перемещаться по сети. Измеряется в секундах и задается источником передачи. На маршрутизаторах и промежуточных узлах сети по истечению каждой секунды вычитается 1. Если TTL станет равен 0 до достижения цели пакет будет уничтожен.
- Протокол (Protocol) – указывает, какому протоколу верхнего уровня принадлежит инкапсулированная информация;
- Контрольная сумма (Header Checksum, 2 байта) – рассчитывается только по заголовку как дополнение к сумме всех 16-битных слов заголовка. При вычислении значение самого поля Checksum устанавливается в нуль.
- IP-адрес источника (Source Address, 32 бита);
- IP-адрес назначения (Destination Address, 32 бита);

– Опции (Options) – необязательное и используется только при отладке сети;
– Padding – выравнивание заголовка по 32-битной границе;
– Поле данных (Data).

Фрагментация IP-пакетов связана с тем, что их размер может превосходить параметр MTU (Maximum Transmission Unit) той технологии, через которую он проходит.

Ethernet MTU = 1500;
PPPoE MTU = 1492;
FDDI MTU = 4096;
X.25 MTU = 128.

В этом случае данные большого пакета **делятся на части** кратные 8 байтам, кроме последней и каждая помещается в новый пакет.

При поступлении первого фрагмента получатель запускает таймер, определяющий **максимально допустимое время ожидания** прихода остальных фрагментов.

Если **таймер истекает** до прихода всех фрагментов, **пакет отбрасывается**.

Во всех случаях ошибок при фрагментации отправителю пакета посылается **ICMP-сообщение об ошибке**.

Назначение IP-адресов

– Статически (администратором системы);
– Динамически (автоматически при загрузке ОС узла).

Для динамического назначения адресов используется протокол BOOTP (Bootstrap Protocol), и его усовершенствованная версия – DHCP (Dynamic Host Configuration Protocol) RFC 1541.

DHCP поддерживает 3 основных типа присвоения адресов:

1. «Ручное» статическое («псеводстатика»): список соответствия IP-адресов физическим задается администратором.
2. Автоматическое статическое: список соответствия задается при первом обращении.
3. Динамическое: сервер выдает IP-адрес клиенту на время – срок аренды (lease duration).

DHCP работает в модели «клиент-сервер»:

1. Клиент посылает широковещательное сообщение discover серверам DHCP.
2. Каждый из серверов отвечает сообщением offer с конфигурационной информацией и IP-адресом.
3. Клиент выбирает одно из предложений и посылает сообщение request выбранному серверу.
4. Выбранный сервер подтверждает сообщением acknowledgment выделение IP-адреса.
5. Клиент переходит к использованию адреса.

Удобная мнемоника для запоминания последовательности сообщений – DORA (по первым буквам сообщений).

Протоколы ARP и RARP

для отправки кадра с помощью технологии канального уровня необходимо **отобразить IP-адреса на локальные адреса**.

В стеке TCP/IP для определения локального адреса по IP-адресу используется **протокол разрешения адресов ARP** (Address Resolution Protocol). Протокол ARP зависит от технологии канального уровня.

Работа ARP основана на ведении ARP-таблицы (ARP-кэша) – соответствия между IP-адресом и MAC-адресом (см. рис. 5.6).

IP-адрес	MAC-адрес	Тип записи

Рисунок 5.6 – Структура кэша ARP

Поле «тип записи» может содержать:

- Статическая;
- Динамическая.

Структура заголовка ARP представлена на рис 5.7.

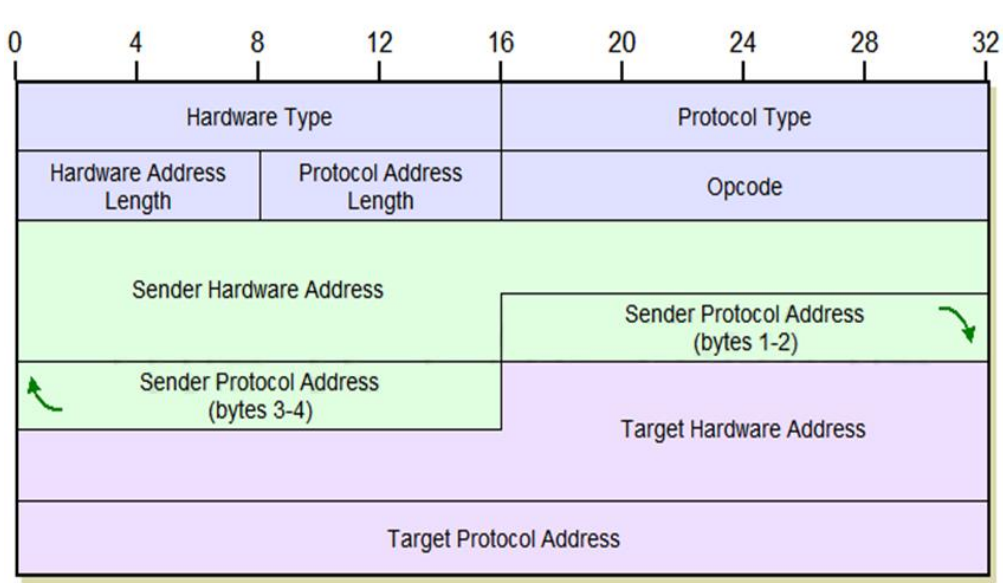

Рисунок 5.7 – Формат пакета ARP

- Тип сети (Hardware Type) – задается локальная технология (1 = Ethernet);
- Тип протокола (Protocol Type) – позволяет использовать ARP не только для IP(0x800);
- Длина локального адреса (Hardware Address Length);
- Длина сетевого адреса (Protocol Address Length);

- Операция (OpCode) (1 – ARP запрос, 2 – RARP);
- Локальный адрес отправителя (Sender Hardware Address);
- IP-адрес отправителя (Sender Protocol Address);
- Искомый локальный адрес (Target Hardware Address);
- Искомый IP-адрес (Target Protocol Address).

1. Источник проверят ARP-кэш на наличие искомого MAC-адреса для заданного IP-адреса.
2. Источник формирует ARP-запрос, указывая свои адреса и искомый IP-адрес.
3. Источник широковещательно рассылает кадр с запросом в сеть.
4. Все узлы (в том числе узел назначения) в сети получают кадр запроса и сравнивают запрошенный IP-адрес со своим.
5. Если IP-адрес совпал, то узел назначения генерирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес.
6. Узел назначения обновляет свой ARP-кэш, внося в него IP- и локальный адреса источника.
7. Узел назначения отсылает ARP-ответ источнику (не широковещательно).
8. Источник получает ответ.
9. Источник обновляет свой ARP-кэш.

Протокол RARP решает обратную задачу: по известному локальному адресу получить IP-адрес. (RFC 903).

Требует специального RARP-сервера, настроенного на прослушивание запросов.

RARP – это ARP. RFC 903 не описывает новый протокол, а новый метод использования ARP.

1. Источник генерирует запрос RARP: Opcode=3, SenderHardwareAddress=собственный локальный адрес = TargetHardwareAddress, поля SenderIPAddress и TargetIPAddress оставляются пустыми.
2. Источник рассылает широковещательно запрос по сети.
3. Узлы сети обрабатывают запрос. Все, кроме настроенных как RARP-сервер игнорируют его.
4. RARP-сервер генерирует ответное сообщение: Opcode=4, SenderHardwareAddress и SenderIPAddress устанавливает в свои, TargetHardwareAddress в адрес источника запроса, TargetIPAddress из таблицы в адрес, запрашиваемый источником.
5. RARP-сервер посылает ответное сообщение unicast'ом источнику.
6. Источник использует полученный адрес.

NAT

- Обход дефицита IP-адресов;
- Обеспечение безопасности частной сети.

Разновидности NAT:

- Базовая (Basic NAT, Basic Network Address Translation);
- Трансляция сетевых адресов и портов (NAPT, Network Address Port Translation или PAT, Port Address Translation)

Внутри сети адреса распределяются как для автономной системы.

Внутренняя сеть подключается к Internet через промежуточное устройство – сервер NAT, которое получает в свое распоряжение один или несколько внешних IP-адресов.

Все запросы во внешнюю сеть транслируются сервером NAT (см. рис. 5.8).

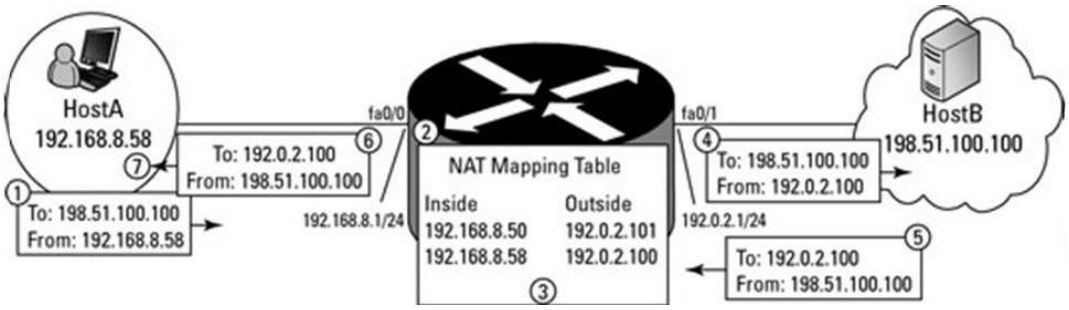

Рисунок 5.8 – Базовый NAT

PAT (NAPT, IP masquerading):

- NAPT позволяет всем узлам частной сети одновременно получить доступ во внешнюю сеть.
- Идея: привлечь дополнительную информацию для идентификации отправителя: IP-адрес узла и порт (см. рис. 5.9).

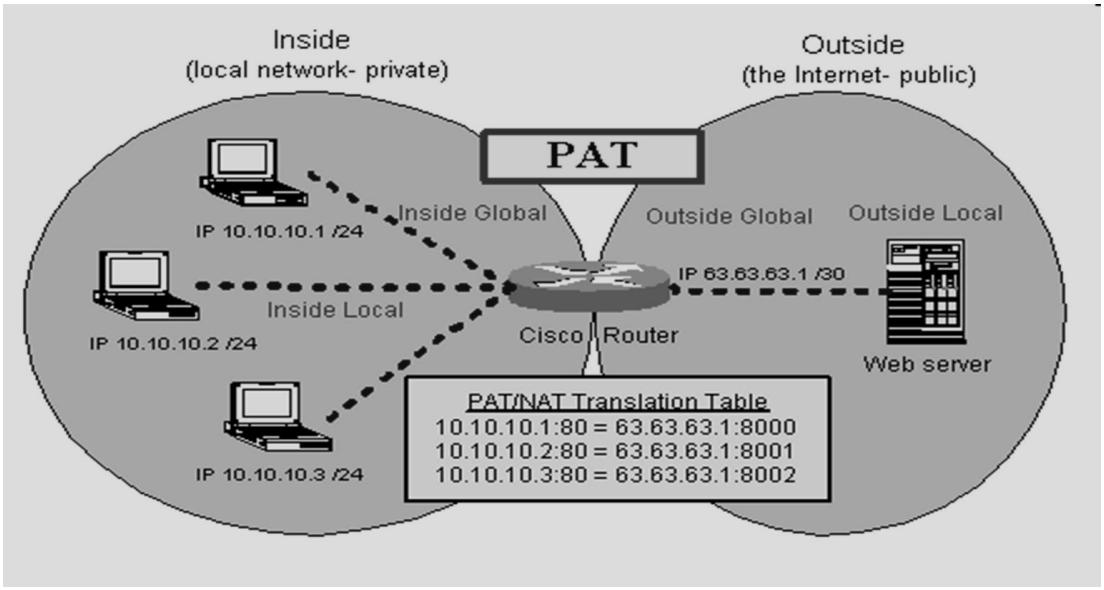

Рисунок 5.9 – NAPT (PAT)

Принципы модернизации протокола IP

- Создание масштабируемой схемы адресации;
- Сокращение объема работ выполняемых маршрутизаторами;
- Предоставление гарантии качества транспортных услуг;
- Обеспечение защиты данных, передаваемых по сети;
- Возможность дальнейшего развития протокола;
- Возможность сосуществования старой и новой версии.

В 1994 году был предложен Next Generation Internet Protocol, IPng, в настоящее время известный как IPv6.

Базовый набор протоколов был принят IETF в 1995 и пересмотрен в 1998 году (RFC 2460, RFC 2373).

Версия IPv6 использует адреса с разрядностью, увеличенной с 32 бит до 128 бит (16 байт).

Возможное число узлов: 340 282 366 920 938 463 463 374 607 431 762 211 456.

Вместо 2 уровней иерархии (номер сети и номер хоста) – 4 уровня: 3 для сетей и 1 для узлов.

3 типа адресов: unicast, multicast, anycast.

Проблема записи. Если следовать правилу IPv4, то мы получим 16 октетов:

128.91.45.157.220.40.0.0.0.0.252.87.212.200.31.25

Поэтому применяется подход аналогичный подходу к MAC-адресу:

805B:2D9D:DC28:0:0:FC57:D4C8:1FFF

При этом 0x0000 могут заменяться на 0 и длинная последовательность нулей может быть сокращена записью (::)

Например, FEDC:0A98:0:0:0:0:D4C8:0001 может быть записан как FEDC:0A98::D4C8:0001.

Общий формат глобального агрегированного уникального IP-адреса (см. рис. 5.10):

Рисунок 5.10 – Формат IPv6 адреса

Префикс формата (Format Prefix, FP) (для глобального агрегируемого уникального адреса = 001);

Поля агрегирования верхнего (Top-Level Aggregation, TLA), следующего (Next-Level Aggregation) и местного (Site-Level Aggregation) уровней – описывают 3 уровня идентификации сетей;

Идентификатор интерфейса – аналог номера узла. В общем случае просто совпадает с локальным адресом.

0:0:0:0:0:0:0:1 – loopback адрес (сокращенная запись ::1);

0:0:0:0:0:0:0:0 – неопределенный адрес, аналог 0.0.0.0 в IPv4.

Формат заголовка IPv6 (см. рис. 5.11):

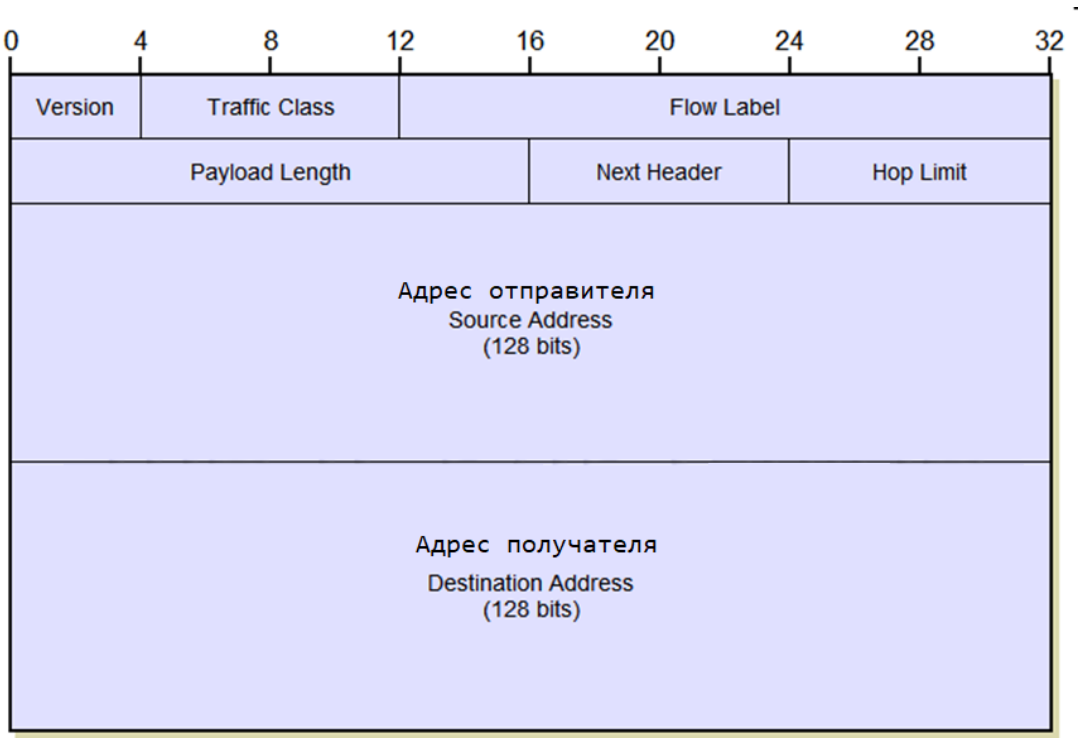

Рисунок 5.11 – Формат пакета IPv6

- Версия (Version) (значение = 6);
- Приоритет (Traffic Class);
- Метка потока (Flow Label);
- Длина полезной нагрузки (Payload Length);
- Следующий заголовок (Next Header);
- Максимальное число транзитных участков (Hope Limit) – аналог поля TTL в IPv4;
- IP-адрес отправителя (Source Address);
- IP-адрес получателя (Destination Address).

Для уменьшения объема служебной информации в IPv6 введено деление:

- Основной заголовок;
- Дополнительные заголовки.

Типы доп.заголовков:

- Маршрутизации;
- Фрагментации;

- Аутентификации;
- Системы безопасности;
- Специальные параметры;
- Параметры получателя.

Расширение дополнительными заголовками выполняется в виде односвязного списка по полю Next Header.

Дополнительные преимущества IPv6 по сравнению с IPv4:

- Возможность перенесения функции фрагментации с маршрутизаторов на конечные узлы;
- Агрегирование адресов, ведущее к уменьшению таблиц маршрутизации;
- Широкое использование маршрутизации от источника.

Маршрутизация

- **определение маршрута** (выбор последовательности транзитных узлов и их интерфейсов);
- **оповещение** сети о выбранном маршруте;
- **продвижение данных**.

Маршрутизация без таблиц:

- Лавинная маршрутизация;
- Маршрутизация, управляемая событиями (Event dependent routing);
- Маршрутизация от источника (source routing).

На основе таблиц:

- подготовка маршрутной таблицы (далее ТМ);
- переадресация дейтаграмм с помощью ТМ.

RRAS-ROUTER1 - IP Routing Table

Destination	Network mask	Gateway	Interface	Metric	Protocol
10.57.76.0	255.255.255.0	10.57.76.1	Local Area C...	1	Local
10.57.76.1	255.255.255.255	127.0.0.1	Loopback	1	Local
10.255.255.255	255.255.255.255	10.57.76.1	Local Area C...	1	Local
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.45.0	255.255.255.0	192.168.45.1	Local Area C...	1	Local
192.168.45.1	255.255.255.255	127.0.0.1	Loopback	1	Local
224.0.0.0	224.0.0.0	192.168.45.1	Local Area C...	1	Local
224.0.0.0	224.0.0.0	10.57.76.1	Local Area C...	1	Local
255.255.255.255	255.255.255.255	192.168.45.1	Local Area C...	1	Local
255.255.255.255	255.255.255.255	10.57.76.1	Local Area C...	1	Local

Рисунок 5.12 – Структура таблицы маршрутизации

Структура ТМ (см. рис. 5.12):

- Адрес назначения пакетов (Destination);
- Сетевой адрес следующего маршрутизатора (Next-Hop);
- Сетевой адрес выходного интерфейса (порт) (Interface);
- Метрика (Metric).

Адрес назначения:

- Адрес узла назначения;
- Адрес сети назначения;
  - Напрямую подключенные подсети;
  - Удаленные подсети;
- Маршрут по умолчанию (default route)

Источники записей ТМ:

- Программное обеспечение стека TCP/IP
- Администратор
- Протоколы маршрутизации

Просмотр таблицы маршрутизации с учетом масок:

1. Протокол IP извлекает из пакета IP-адрес цели;
2. Первая фаза поиска – поиск специфического маршрута: из каждой записи с маской 255.255.255.255 извлекается адрес назначения и сравнивается с адресом цели. Если есть совпадение – маршрут найден;
3. Вторая фаза поиска – если первая не дала результата – поиск неспецифического маршрута: для каждой записи ТМ:

- Маска накладывается на IP цели (M AND IPT);
- Полученное число сравнивается с адресом назначения;
- Если происходит совпадение, протокол отмечает эту строку;
- Если просмотрены все записи – переход к 4;

4. Выполняется одно из 4 действий:

- Если есть одно совпадение – пакет отправляется по этому маршруту;
- Если произошло несколько совпадений – помеченные строки сравниваются и пакет отправляется по маршруту с наибольшим количеством совпадений двоичных разрядов;
- Если совпадений нет, но есть маршрут(ы) по умолчанию – пакет отправляется по этому маршруту(ам);
- Если нет совпадений и нет маршрута по умолчанию – пакет отбрасывается.

Программное обеспечение операционной системы обычно формирует следующие маршруты на основе конфигурации сети (см. рис. 5.13):

- Маршрут по умолчанию;
- Loopback address (петля);
- Путь к напрямую подключенной подсети (directly attached subnet);
- Путь к узлу (host route);
- Широковещательный (broadcast) по текущей сети;
- Путь для группового (multicast) трафика;
- Ограниченный широковещательный адрес (Limited broadcast)

```
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 b0 d0 e9 41 43 ...... 3Com EtherLink PCI
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    157.60.136.1   157.60.136.41      20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
     157.60.136.0    255.255.252.0    157.60.136.41   157.60.136.41      20
    157.60.136.41  255.255.255.255        127.0.0.1       127.0.0.1      20
   157.60.255.255  255.255.255.255    157.60.136.41   157.60.136.41      20
        224.0.0.0        240.0.0.0    157.60.136.41   157.60.136.41       1
  255.255.255.255  255.255.255.255    157.60.136.41   157.60.136.41       1
Default Gateway:      157.60.136.1
===========================================================================
Persistent Routes:
  None
```

Рисунок 5.13 – Таблица маршрутизации ОС Windows

Маршрутизация на основе таблиц может быть разделена на следующие виды:

- **Статическая маршрутизация** – таблицы составляются и вводятся в память маршрутизатора вручную;
- **Адаптивная** (динамическая) **маршрутизация** – все изменения конфигурации сети отображаются в таблицах маршрутизации **протоколами маршрутизации**.

Понятия:

- **Согласованные ТМ** – таблицы маршрутизации, обеспечивающие доставку пакета от исходной сети в сеть назначения.
- **Время конвергенции** – время, необходимое протоколу маршрутизации для согласования ТМ.

Протоколы маршрутизации:

- Распределенные (децентрализованные) – отсутствуют выделенные маршрутизаторы, работа распределяется между всеми;
- Централизованные – существует выделенный маршрутизатор – сервер маршрутов – который строит таблицы для всех остальных маршрутизаторов и распространяет их по сети.

Требования к алгоритмам маршрутизации:

- Обеспечивать рациональность маршрута;
- Быть достаточно простыми (вычислительно и по объему трафика);
- Обладать свойством сходимости.

Адаптивные протоколы обмена маршрутной информацией:

- Дистанционно-векторные алгоритмы (Distance Vector Algorithms, DVA);
- Алгоритмы состояния связей (Link State Algorithms, LSA).

DVA:

Каждый маршрутизатор периодически и широковещательно рассылает по сети **вектор дистанции**, содержащий расстояния от маршрутизатора до всех известных ему сетей (в некоторой метрике), и на основании такой информации изменяет свою ТМ.

Такие пакеты называют *объявлениями о расстояниях*.

Наиболее известный DVA – RIP.

LSA:

Обеспечивают каждый маршрутизатор полным графом связей сети. Все маршрутизаторы сети используют один и тот же граф.

Периодически тестируют состояние линии связи до ближайших соседей.

Типичные протоколы: OSI IS-IS, OSPF (TCP/IP), NLSP Novell.

В сети могут одновременно работать несколько протоколов маршрутизации.

По умолчанию каждый протокол маршрутизации распространяет только свою информацию.

Существует особый режим работы маршрутизатора – **перераспределение**.

Сети разделяются на отдельные области под единым административным управлением – **автономные системы** (Autonomous System, AS).

AS распознаются по глобально уникальным **номерам автономных систем** (Autonomous System Number, ASN)

Маршрутизаторы в пределах автономной области используют один и тот же протокол маршрутизации.

Автономные системы соединяются **внешними шлюзами** – маршрутизаторами, отвечающими за пересылку пакетов за пределы автономной системы (см. рис. 5.14).

Между внешними шлюзами используется стандартный протокол, называемый **внешним шлюзовым протоколом** (Exterior Gateway Protocol, EGP). BGPv4.

Протокол, используемый внутри автономной системы называется **протоколом внутренней маршрутизации** (Interior Gateway Protocol, IGP). RIP, OSPF, IS-IS.

Примеры протоколов маршрутизации

RIP (Routing Information Protocol – протокол маршрутной информации) – внутренний протокол маршрутизации дистанционно-векторного типа.

RIP v1 RFC1058

RIP v2 RFC2453 (передает информацию о масках сетей).

Поддерживает различные типы метрик: хопы (hop), значения пропускной способности, вносимые задержки, надежность сетей, а также их комбинации.

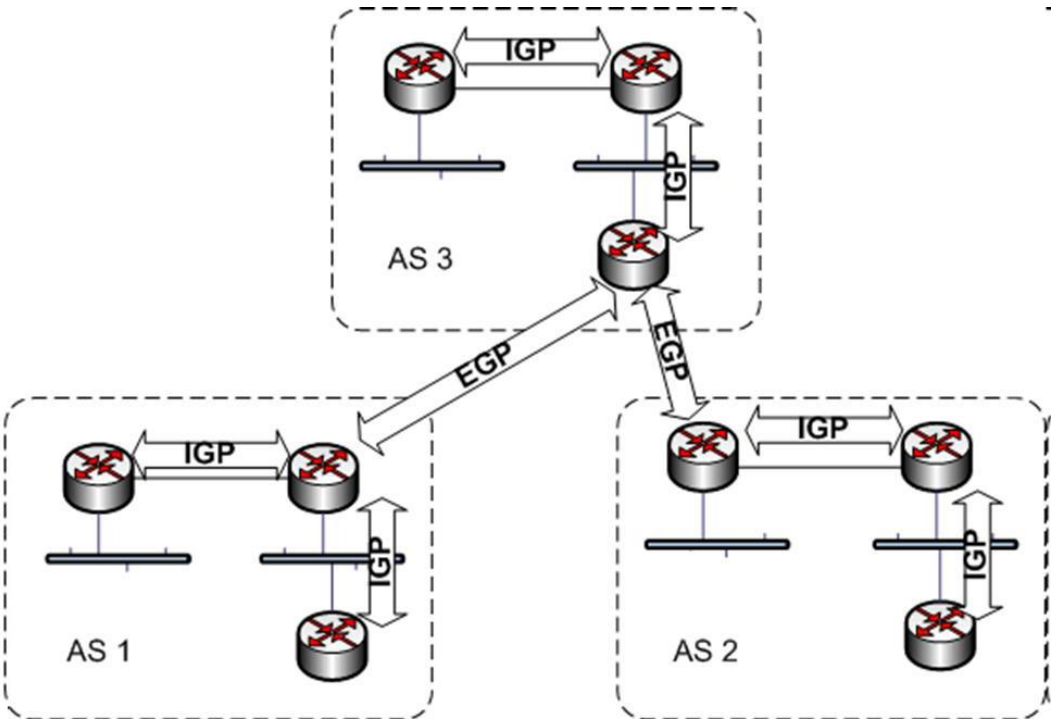

Рисунок 5.14 – Взаимодействие автономных систем

Главное требование: метрика должна быть аддитивной – метрика составного пути должна быть равна сумме метрик составляющих этого пути.

Этапы работы (процесс построения ТМ):

1. Создание минимальной ТМ (для непосредственно подсоединенных сетей);
2. Рассылка минимальной таблицы соседям (по протоколу UDP);
3. Получение RIP-сообщений от соседей и обработка полученной информации (увеличение метрики на 1 в полученных сообщениях и формирование ТМ).
4. Рассылка новой таблицы соседям;
5. Получение RIP-сообщений от соседей и обработка полученной информации (повторение этапа 3).

Адаптация к изменениям состояния сети:

Добавление новых маршрутов – маршрутизаторы приспосабливаются просто.

Изменения, связанные с потерей маршрута – гораздо сложнее. Для уведомления:

- Истечение времени жизни маршрута;
- Указание специального (бесконечного=16) расстояния до сети, ставшей недоступной.

Методы борьбы с ложными маршрутами в протоколе RIP:

- **Метод расщепления горизонта** – маршрутная информация о некоторой сети никогда не передается тому от кого она была получена;

- **Триггерные обновления** – информация об изменений маршрута передается сразу;
- **Замораживание изменений** – введение тайм-аута на прием информации о сети, которая только что стала недоступной.

OSPF (Open Shortest Path First – открытый протокол выбора кратчайшего пути первым) – протокол на базе алгоритма состояния связей. Предназначен для больших гетерогенных сетей.

Принят в 1991 году.

OSPF v2 RFC2328

Этапы построения ТМ:

1. Маршрутизатор строит граф связей сети в котором вершинами являются маршрутизаторы и IP-сети, а ребрами – интерфейсы маршрутизаторов. (Маршрутизаторы обмениваются объявлениями о состоянии связей сети. Эти объявления не модифицируются. В результате каждый маршрутизатор получает одинаковые сведения – базу данных о топологии сети.)
2. Нахождение оптимальных маршрутов с помощью полученного графа. В OSPF – итеративный алгоритм Дейкстры: каждый маршрутизатор считает себя центром сети и ищет путь до каждой известной сети. В каждом маршруте запоминается только один шаг – до следующего маршрутизатора.

Корректировка ТМ:

Для контроля связей и соседних маршрутизаторов каждые 10 сек. маршрутизаторы передают друг другу сообщение HELLO. Когда сообщения HELLO перестают поступать маршрутизатор делает вывод – состояние связи изменилось на неработоспособное и делает соответствующую отметку в своей БД, одновременно отсылает сообщение всем непосредственным соседям.

Если же состояние сети не меняется, то объявления о связях не генерируются.

Исключение: синхронизация всей БД каждые 30 минут.

OSPF строит отдельную ТМ для различных метрик (T, D, R) и использует их в зависимости от значения битов TOS.

Для сокращения вычислительной сложности OSPF используются области сети.

BGP (Border Gateway Protocol) – пограничный (внешний) шлюзовый протокол версии 4 – основной протокол обмена маршрутной информацией между автономными системами. Пришел на смену EGP.

В качестве адреса следующего маршрутизатора использует точку входа в соседнюю AS.

Маршрутизатор взаимодействует с другим только если администратор явно указал его как соседа.

Для установления сеанса используется протокол TCP на 179 порту и различные способы аутентификации.

Сообщения: OPEN, UPDATE, NOTIFICATION, KEEPALIVE.

Основной метод протокола – UPDATE – позволяет сообщить об изменении доступности сетей автономной системы (триггерное объявление) в формате:

BGP Route = AS_Path;NextHop;Network/Mask_length

Например:

AS 1021; 194.200.30.1; 202.100.5.0/24

Поддерживает две реализации:

- Exterior BGP (eBGP);
- Interior BGP (iBGP) – для обмена информацией между маршрутизаторами одной и той же автономной системы.

ICMP (Internet Control Message Protocol) протокол межсетевых управляющих сообщений – вспомогательный протокол, предназначенный для диагностики и мониторинга сети.

Определен в RFC 792.

Принцип доставки данных в IP – «по возможности».

Иногда доставка не возможна (истекает TTL пакета, в таблице маршрутизации отсутствует маршрут к адресу назначения, пакет не прошел проверку контрольной суммы, шлюз не имеет места в буфере для передачи пакета и т.д.).

ICMP – средство оповещения отправителя о проблемах с пакетами.

При обнаружении проблемы узел должен отправить диагностическое сообщение отправителю.

Обработка ICMP выполняется ядром ОС, протоколами транспортного или прикладного уровня, или игнорируется, но не протоколами IP или ICMP.

Заголовок пакета ICMP включает 3 поля:

- Тип (1 байт) – числовой ID типа сообщения;
- Код (1 байт) – числовой ID, уточняющий тип ошибки;
- Контрольная сумма (2 байта) – подсчитывается для всего ICMP-сообщения;

Типы сообщений ICMP можно разделить на:

- Сообщения об ошибках;
- Сообщения запрос-ответ (связаны в пары, например, эхо-запрос – эхо-ответ).

Пример типов сообщений второго вида приведен в табл. 5.1, а сообщений об ошибках – в табл. 5.2:

Значение в поле Тип	Тип сообщения
0	Эхо-ответ
8	Эхо-запрос
13	Запрос отметки времени
14	Ответ отметки времени
17	Запрос маски
18	Ответ маски

Таблица 5.1 – Типы сообщений «запрос-ответ»

Значение в поле Тип	Тип сообщения
3	Узел назначения недостижим
4	Подавление источника
5	Перенаправление маршрута
11	Истечение времени дейтаграммы
12	Проблема с параметрами пакета

Таблица 5.2 – Типы сообщений об ошибках

Поле кода используется для уточнения причины ошибки. Например, для типа 3 некоторые коды уточняющие его причины приведены в таблице 5.3:

Код	Причина
0	Сеть недостижима
1	Узел недостижим
2	Протокол недостижим
3	Порт недостижим
4	Ошибка фрагментации
…	…
9	Административный запрет

Таблица 5.3 – Коды, уточняющие ошибку типа 3

Протокол ICMP является основой для ряда сетевых утилит, таких как Ping (Packet Internetwork Groper), pathping, traceroute и др.

Лекция № 6. Глобальные сети

Глобальные сети (ГС, WAN) – это компьютерные сети, использующие средства связи дальнего действия для предоставления сетевых сервисов большому количеству конечных абонентов, расположенных на большой территории.

- Публичные или общественные (создаются крупными телекоммуникационными компаниями для оказания платных услуг абонентам);
- Частные (создаются крупными корпорациями для своих внутренних потребностей);
- Смешанный вариант (корпоративная сеть пользуется услугами или оборудованием общественной ГС, дополняя их собственными (аренда каналов связи)).

Выделяют:

- Владелец ГС;
- Оператор сети (network operator);
- Поставщик услуг (провайдер, service provider).

Оператор – компания, которая обеспечивает нормальную работу сети.

Поставщик услуг – компания, которая оказывает платные услуги абонентам сети.

Владелец, оператор сети и поставщик услуг могут объединяться в одну компанию, а могут представлять и разные компании.

Типичные абоненты ГС – распределенные локальные сети предприятии или отдельные компьютеры, которым нужно обмениваться данными между собой.

Структура ГС (см. рис. 6.1):

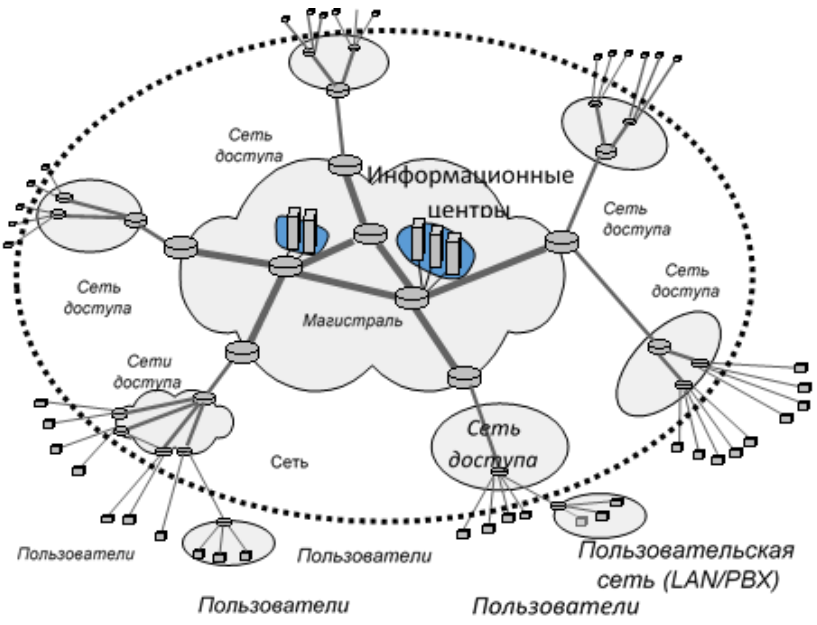

Рисунок 6.1 – Структура глобальных сетей

- Магистральные сети (backbone WAN);
  - Высокая пропускная способность;
  - Высокий коэффициент готовности (для обеспечения используется избыточная топология).
- Сети доступа (основная задача – концентрирование информационных потоков).
  - Разветвленная инфраструктура;
  - Экономическая оправданность подключения.

Удаленный доступ (remote access) – доступ конечных пользователей или сетей к ГС или LAN предприятия.

Организация удаленного доступа известна как «проблема последней мили» (см. рис. 6.2), где под последней милей понимается расстояние от точки присутствия (POP – Point Of Presence) оператора связи до помещения клиента.

- Коммутируемый аналоговый доступ (dial-up);
- Коммутируемый доступ через сеть ISDN (Integrated Services Data Network – цифровую сеть с интегрированными услугами);
- xDSL технологии;
- CATV;
- xPON-технологии;
- Беспроводной доступ.

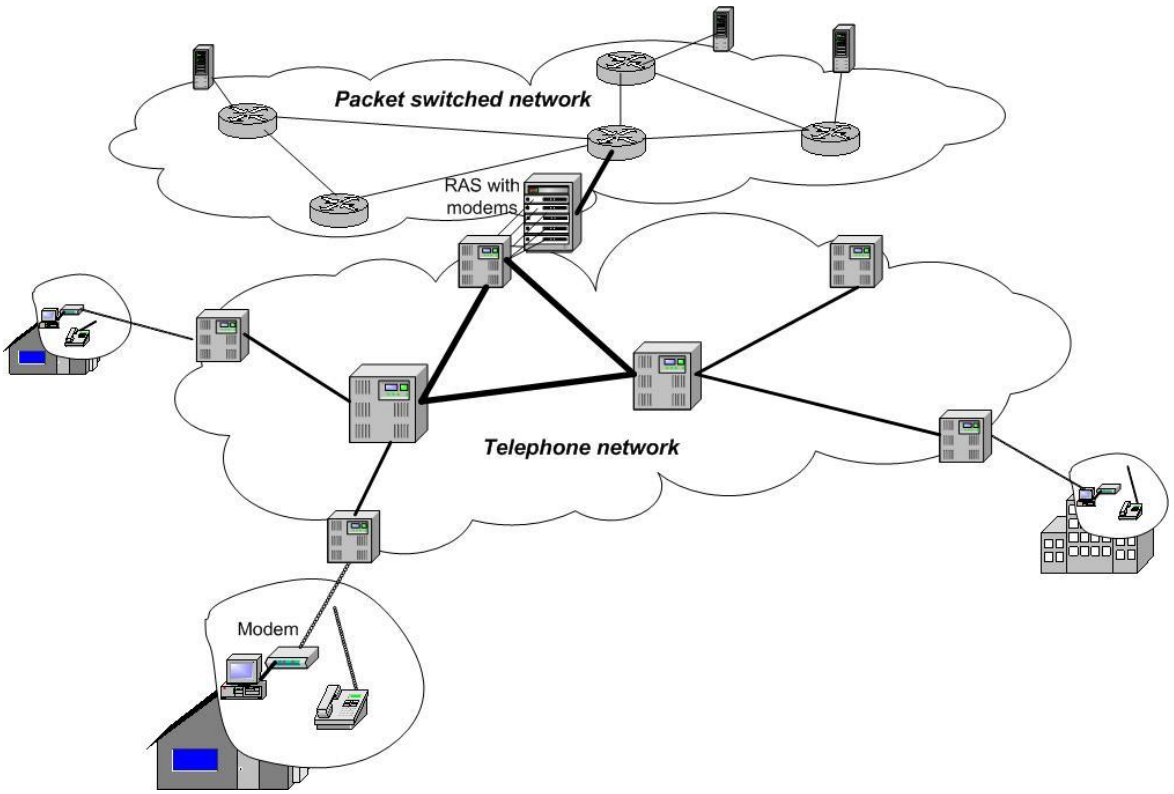

Рисунок 6.2 – Технологии «последней мили»

Протоколы и стандарты модемов определены в рекомендациях ITU-T серии V и делятся на 3 группы:

- Стандарты, определяющие скорость передачи данных и метод кодирования;
- Стандарты исправления ошибок;
- Стандарты сжатия данных.

Стандарты на метод и скорость передачи:

V.34 – дуплексная передача на скорости до 28.8 Кб/с (*первые модемы работали на скорости 300 бит/с*)

V.34+ – дуплексная передача на скорости до 33.6 Кб/с

V. 90 – передача на скорости до 33.6 Кб/с и прием – до 56 К

V.92 – возможность принятия 2 вызова во время соединения.

Стандарт V.34+ усовершенствовал метод кодирования.

Стандарты на метод исправления ошибок:

- V.42 – Протокол MNP (Microcom Networking Protocol) классов 2-4
- Протокол LAP-M (Link Access Protocol for Modems)
- Протокол ITU-T V.42 объединил два предыдущих.

Стандарты на компрессию данных

- протокол V.42bis

Технология ISDN.

Цели сетей ISDN:

- Обеспечить всемирную единообразную цифровую сеть, которая поддерживает широкий диапазон услуг (речь, данные, телевизионные сигналы, факсы и т.п. в цифровой форме)
- Обеспечить единый набор стандартов для цифровых передач в сетях – цифровые сети 56/64 Кб/с и T1/E1 в различных странах используют разные стандарты
- Обеспечить стандартный интерфейс пользователя
- Обеспечить независимость программного обеспечения от реализации цифровой сети

Семейство технологии xDSL (см. рис. 6.3):

- Асимметричного цифрового абонентского окончания (Asymmetric Digital Subscriber Line, ADSL);
- Симметричного цифрового абонентского окончания (Symmetric Digital Subscriber Line, SDSL);
- Цифрового абонентского окончания с адаптируемой скоростью передачи (Rate Adaptive DSL, RADSL);
- Сверхбыстрого цифрового абонентского окончания (Very high-speed DSL, VDSL).

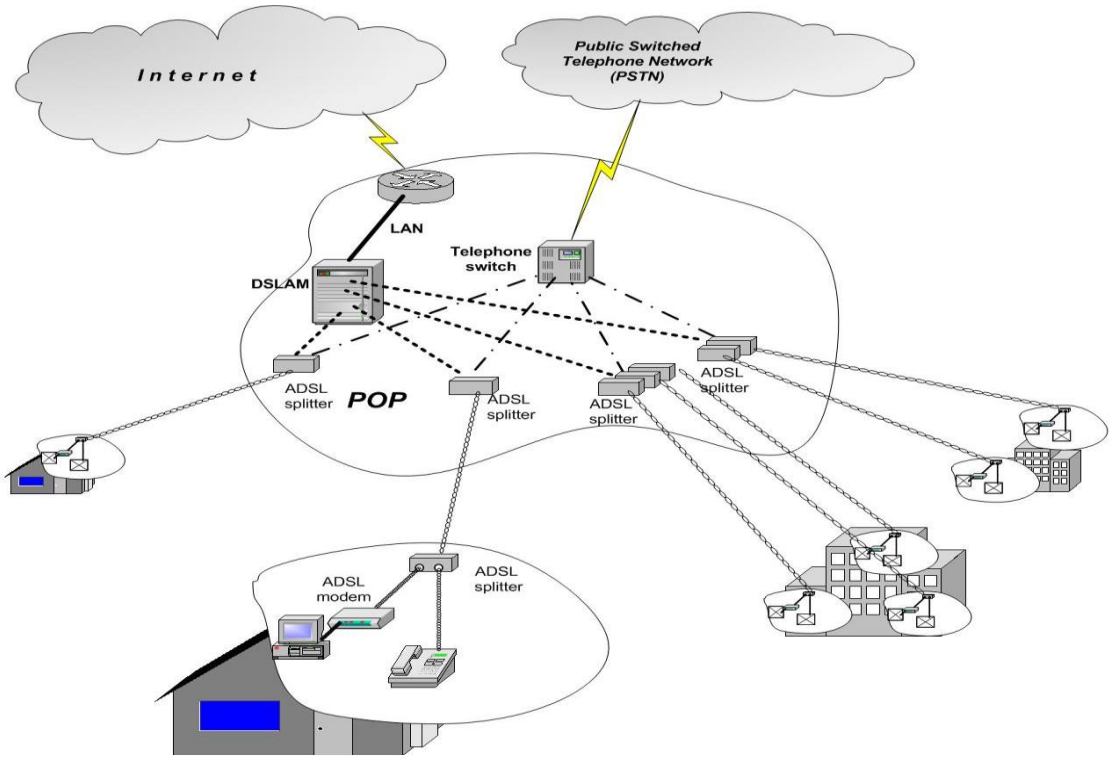

Рисунок 6.3 – Организация xDSL-доступа

Название ADSL обязано распределению полосы пропускания абонентского окончания между каналами ADSL: было замечено, что пользователь больше получает из сети (т.н. downstream), чем «отдает» в сеть (т.н. upstream) (см. рис. 6.4)

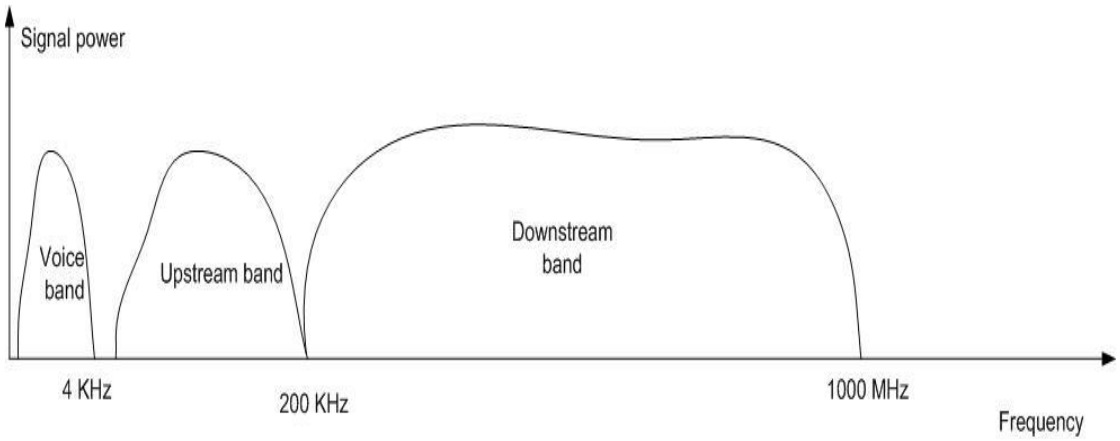

Рисунок 6.4 – Распределение частот ADSL

Доступ через сети CATV

Т.к. коаксиальный кабель обладает полосой пропускания в 700–800 МГц, то может справиться с одновременной передачей телефонного, компьютерного и телевизионного трафика.

Нисходящий канал использует только станция CMTS. Восходящий канал задействуется в режиме множественного доступа. Станция CMTS играет роль арбитра.

Кабельный модем может иметь разъем для подключения телефона, которому выделяется 4МГц в нижнем диапазоне частот.

Для широковещательного распространения ТВ-программ используется диапазон частот от 50 до 550–868 МГц (по 6 или 8 МГц на канал).

CMTS (Cable Modem Termination Station) использует диапазон от 5 до 50 МГц (восходящий канал), а также более 550МГц (нисходящий).

Скорости:

- Восходящая – до 10 Мбит/с;
- Нисходящая – до 30–40 Мбит/с.

xPON (пассивные оптические сети) – оптоволоконная масштабируемая технология последней мили (до 2,5 Гбит, до 64 абонентов на одно волокно, на расстояние до 20 км).

Включает стандарты:

- GPON – Gigabit PON (ITU-T G.984);
- EPON (GEPON) – Ethernet PON (IEEE 802.3ah);
- 10GEPON – 10 Gigabit PON (IEEE 802.3av).

Основная идея архитектуры PON – организация по схеме «точка»-«мультиточка» = использование всего одного приёмопередающего модуля в OLT (англ. optical line terminal) для передачи информации множеству абонентских устройств ONT (optical network terminal в терминологии ITU-T), также называемых ONU (optical network unit в терминологии IEEE) и приема информации от них.

Число абонентских узлов, подключенных к одному приёмопередающему модулю OLT, может быть настолько большим, насколько позволяет бюджет мощности и максимальная скорость приёмопередающей аппаратуры. Для передачи потока информации от OLT к ONT – прямого (нисходящего) потока, как правило, используется длина волны 1490 нм. Наоборот, потоки данных от разных абонентских узлов в центральный узел, совместно образующие обратный (восходящий) поток, передаются на длине волны 1310 нм. Для передачи сигнала телевидения используется длина волны 1550 нм. В OLT и ONT встроены мультиплексоры WDM, разделяющие исходящие и входящие потоки.

Нисходящий трафик является широковещательным. Каждый абонентский узел читает только предназначенные ему данные: читая адресные поля, выделяет из этого общего потока предназначенную только ему часть информации. Фактически – распределённый демультиплексор.

Восходящий трафик передается на одной и той же длине волны от всех абонентов с технологией множественного доступа TDMA (Time Division Multiple Access). Чтобы исключить возможность пересечения сигналов от разных ONT, для каждого из них устанавливается свое индивидуальное расписание по передаче данных с учётом поправки на задержку, связанную с удалением данного ONT от OLT.

Лекция № 7. Канальный уровень модели OSI

Протоколы канального уровня выполняют управление каналами связи.

PDU канального уровня – **кадр** (**frame**).

Основные задачи канального уровня:

- **Формирование кадров** для передачи пакетов между физически связанными узлами КС;
- **Нахождение границ кадра** в потоке бит, передаваемом с физического уровня;
- **Обработка ошибок** передачи и управление потоком кадров.

Формирование кадров

По методу передачи протоколы канального уровня делятся на 2 группы:

- Синхронные;
- Асинхронные.

Асинхронные протоколы оперируют отдельными **символами**, а не кадрами.

Символ представляет собой байт данных, сопровождаемый специальными сигналами “Start” и “Stop”, предназначенными для синхронизации передатчика и приемника (см. рис. 7.1).

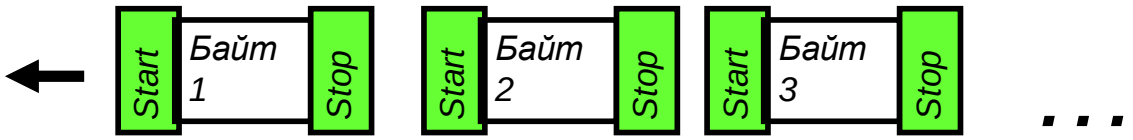

Рисунок 7.1 – Асинхронный протокол

Для передачи чаще всего используются стандартные наборы символов – ASCII, EBCDIC.

Асинхронные протоколы применяются для связи низкоскоростных устройств.

Пример: протокол XMODEM.

В **синхронных протоколах** обмен осуществляется кадрами. Все байты кадра передаются непрерывным синхронным потоком.

Для синхронизации приемника и передатчика используются байты синхронизации – известные коды, которые извещают приемник о приходе кадра.

При получении такого кода приемник должен перейти в режим байтовой синхронизации – правильно распознавать начало байта.

Для того чтобы избежать ошибок синхронизации битов при передаче длинного кадра на физическом уровне применяют самосинхронизирующиеся коды.

Общий формат кадра синхронного протокола включает в себя синхронизационную последовательность (преамбулу), служебную информацию, содержащую адреса отправителя и получателя данных, другую необходимую информацию, собственно данные и концевик (содержащий, как правило, контрольную сумму кадра) (см. рис. 7.2).

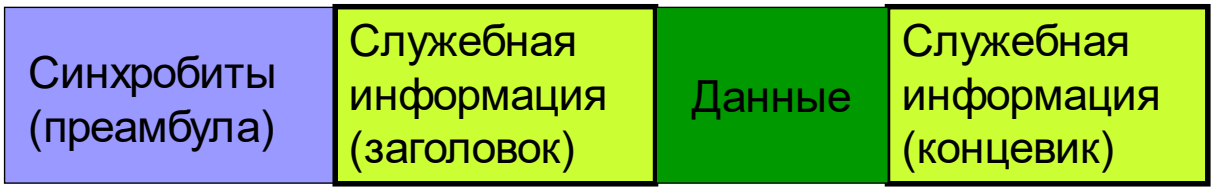

Рисунок 7.2 – Общий формат кадра синхронных протоколов

Приемник должен уметь определять начало и конец кадра, границы каждого поля кадра: адресную информацию (служебные поля), поля данных и контрольной суммы.

В большинстве протоколов канального уровня поле данных может быть переменной длины. Поэтому канальные протоколы определяют его максимальное возможное значение – **максимальную единицу передачи данных MTU (Maximum Transfer Unit)**.

По методу решения задачи синхронизации символов и кадров (определения границ полей кадра) в синхронных протоколах выделяют:

- Символьно-ориентированные протоколы;
- Бит-ориентированные протоколы.

Символьно-ориентированные протоколы

Используются для передачи блоков отображаемых символов.

В качестве синхробайтов используются два или более управляющих символов, называемых символами SYN (в ASCII – 0010110).

Граница начала кадра указывается специальным символом STX (Start of TeXt, ASCII = 0000010).

Окончание кадра указывается символом ETX (End of TeXt, ASCII=0000011).

Недостаток: возможность появления символов STX и ETX внутри кадра.

Кодопрозрачность протокола – способность протокола отличать граничные символы от символов данных кадра, совпадающих с граничными по кодам.

Решение проблемы:

использование **байт-стаффинга** (stuff – наполнитель) – процедуры экранирования символов STX и ETX символом **DLE** (Data Link Escape):

STX -> DLE STX

ETX ->DLE ETX

Ограничения символьно-ориентированных протоколов:

- Большая избыточность по сравнению с бит-ориентированными протоколами (за счет символов DLE);
- Зависимость от кодировок символов.

Бит-ориентированные синхронные протоколы

Границы кадра определяются в битовом потоке – длина кадра не обязана быть кратной 8 битам.

Выделяют 3 схемы строения бит-ориентированных протоколов по способу определения границ кадра:

1. Начало и конец кадра определяются одинаковой 8-битовой последовательностью – флагом (01111110) (см. рис. 7.3).

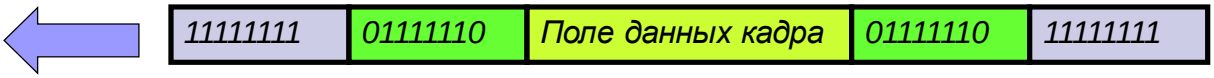

Рисунок 7.3 – Траницы кадра определяются последовательностью 01111110

Для синхронизации передатчика и приемника используется преамбула – последовательность байтов простоя «11111111».

Кодопрозрачность обеспечивается процедурой бит-стаффинга – вставкой бита 0 после каждых 5 «1» (последовательность 01111110 никогда не появится внутри кадра).

Бит-стаффинг имеет меньшую избыточность, чем байт-стаффинг.

2. Для определения начала кадра используется начальный флаг, для определения конца файла – поле длины кадра (при фиксированной длине заголовка – длина поля данных) (см. рис. 7.4).

Рисунок 7.4 – Траницы кадра определяются по фиксированному полю длины

Структура:

- 10101010 – преамбула;
- 10101011 – начальный флаг;
- Фиксированный заголовок;
- Длина поля данных в байтах;
- Поле данных кадра;
- Фиксированный концевик.

3. Для определения начала и конца кадра используются флаги, состоящие из **запрещенных** для данного кода символов (**code violation**).

Для манчестерского кодирования:

Манчестерский код: смена состояния в середине битового интервала – от –V к +V – «1», от +V к –V – «0», низкий уровень сигнала –V без смены

в середине интервала – «J», высокий уровень сигнала +V без смены в середине интервала – «K» (см. рис. 7.5).

J и K – запрещенные сигналы.

Начало кадра JK0JK000,

Конец кадра JK1JK100.

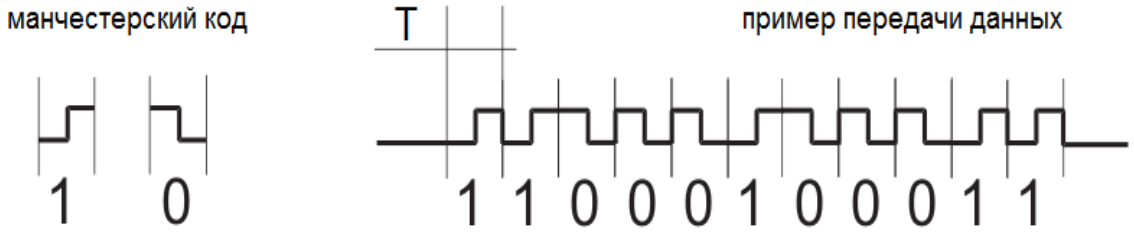

Рисунок 7.5 – Принцип формирования сигналов манчестерского кода

Плюс:

– Экономичность – нет ни бит-стаффинга, ни поля длины кадра.

Минус:

– Зависимость от метода кодирования на физическом уровне.

** Для обхода может быть использовано избыточное логическое кодирование и его запрещенные коды.

Протоколы с гибким форматом кадра

Существуют протоколы, использующие неопределенное количество полей переменной длины.

Способ представления данных в таких протоколах называется **TLV** (**Type Length Value**) (см. рис. 7.6).

Рисунок 7.6 – Способ представления данных TLV

Службы передачи кадров:

– Дейтаграммные службы (работающие без установления соединения – connectionless);
– Службы с предварительным установлением логического соединения (connection-oriented).

Фазы работы:

– Установление логического соединения (обмен служебными кадрами – установление соединения и согласование параметров);
– Передача данных (с отслеживанием корректности передачи);
– Разрыв логического соединения.

При передаче данных контролируется получение всех кадров и в правильном порядке.

Методы обнаружения и коррекции ошибок

Одной из задач канального уровня – обнаружение и коррекция ошибок.

Для этого к кадру добавляется контрольная сумма, которая называется также **контрольной последовательностью кадра** (Frame Check Sequence, FCS) или просто **контрольной суммой**

Коды, позволяющие обнаруживать ошибки называются **помехоустойчивыми**.

Коды, позволяющие исправлять ошибки – **корректирующими** или кодами с исправлением ошибок (ECC – Error Correcting Code).

Классы кодов:

1. Контроль по паритету.

Выполняется суммирование по модулю 2 всех бит контролируемого блока данных. Результат суммирования – бит паритета – пересылается вместе с информацией.

Позволяет контролировать одиночные ошибки. При применении к каждому байту обладает высокой избыточностью.

Существуют модификации: вертикальный и горизонтальный контроль по паритету: контролируемый блок рассматривается как матрица nxk бит; для каждой строки и столбца считается бит паритета.

Позволяет обнаруживать большую часть двойных ошибок.

2. Циклический избыточный контроль CRC (Cyclic Redundancy Check).

Основан на представлении битовых строк как полиномов с коэффициентами 0 и 1.

Например, 11001001 рассматривается как полином P(x) = x7+ x6 + x3 + x0.

На множестве полиномов определены операции сложения, вычитания по модулю 2 и деления (при этом вычитание эквивалентно операции XOR).

Для использования CRC отправитель и получатель определяют образующий полином – G(x) (стандартизирован), старший и младший биты которого = 1.

Пусть задан кадр M(x) из m бит. Алгоритм вычисления CRC:

- Строим $M_1(x) = 2^r M(x)$, где r – степень полинома G(x) (соответствует дополнению контролируемого кадра до длины r+m нулями).
- Вычисляем $R(x) = M_1(x) \bmod G(x)$
- Вычисляем $T(x) = M_1(x) + R(x)$ (добавляем остаток на освобожденные позиции)
- Получатель, приняв кадр, вычисляет $R_1(x) = T(x) \bmod G(x)$. При успешной передаче $R_1(x) == 0$, если $R_1(x)!=0$ – ошибка

На практике под поле CRC отводится 2 или 4 байта – соответственно применяют нотацию CRC-16 или CRC-32, чтобы указать степень соответствующих полиномов.

Алгоритм CRC обнаруживает как одиночные и двойные ошибки, так и ошибки в нечетном числе битов.

Плюсы:

- Низкая избыточность;
- Существование аппаратных схем вычисления

Минус:

- Высокая вычислительная сложность.

Одним из важнейших вопросов канального уровня является способ организации доступа к каналу передачи данных.

По методу доступа к каналу передачи данных сетевые технологии можно разделить:

- Коммутируемые – использующие соединение точка-точка (point-to-point);
- Использующие широковещание.

Основная проблема: распределение канала связи между многочисленными пользователями, претендующими на него.

Совместно используемый несколькими интерфейсами физический канал называют **разделяемым** (shared) или **разделяемой средой передачи данных**. Широковещательные каналы также называют **каналами с множественным доступом** или **каналами с произвольным доступом**.

Протоколы, определяющие порядок доступа к каналам с множественным доступом, относятся к подуровню MAC (Media Access Control – управление доступом к среде) канального уровня.

Методы распределения канала связи между абонентами можно разделить на:

- Статические;
- Динамические.

Статические методы распределения канала связи

- Частотное уплотнение (Frequency Division Multiplexing – FDM);
- Волновое мультиплексирование (Wave Division Multiplexing – WDM);
- Мультиплексная передача с временным уплотнением (Time Division Multiplexing).

FDM. Каждому соединению выделяется собственный диапазон частот в общей полосе пропускания линии связи.

Примеры: телефонные сети, сети кабельного телевидения.

WDM. Принцип действия совпадает с FDM, но используется при передаче оптического сигнала для разделения канала между волнами с разной длиной.

TDM. Канал выделяется каждому соединению на определенный период времени.

Существует два типа TDM:

- Синхронный режим TDM – каждое соединение периодически получает канал в свое распоряжение;
- Асинхронный режим TDM – канал выделяется пользователю только в случае необходимости передачи информации.

Недостатки статических методов распределения канала связи:

- Неэффективность при переменном количестве пользователей;
- Неэффективность при пульсирующем трафике.

По наличию управления методы распределения канала связи можно разделить на:

- Централизованные методы доступа к среде передачи данных;
- Децентрализованные.

По способу распределения канала:

- Методы случайного доступа – ALOHA, CSMA и др. децентрализованные методы;
- Методы детерминированного доступа (максимальное время ожидания доступа всегда известно)
    - Методы передача маркера (token passing);
    - Алгоритмы опроса (polling).

Условия:

- Станционная модель – сеть состоит из N независимых станции, каждая из которых формирует кадры для передачи. После формирования кадра станция блокируется до завершения передачи;
- Единый канал – единый канал связи доступен для всех;
- Коллизии – если два кадра передаются одновременно, они перекрываются во времени и сигнал искажается. Все станции могут обнаруживать коллизии. Искаженный кадр должен быть передан повторно. Других ошибок в сети нет.

Коллизия (collision) – явление наложения двух или более сигналов в разделяемой среде передачи данных.

По отношению ко времени начала передачи кадра:

- Непрерывное время – передача кадра может начаться в любое время, синхронизация отсутствует;
- Дискретное время – время разделено на такты. Передача кадра может начаться только в начале такта. В один такт может передаваться 0, 1 или более кадров (свободный канал, успешная передача кадра, коллизия соответственно).

По возможности определения передачи:

- Каналы с контролем несущей (carrier) – станции могут определить, свободна или занята линия связи до передачи данных
- Отсутствие контроля несущей – станции не могут определить свободна или занята линия, пока не используют ее. Только после передачи возможно определение ее успешности.

Система ALOHA

Разработана в 70-е годы XX века в Гавайском университете Норманом Абрамсоном с коллегами для широковещательной радиосвязи.

Идея: разрешить передачу, как только появятся данные. После этого прослушать канал и если кадр был разрушен, то выждать случайное время и пытаться переслать этот кадр повторно. Время ожидания должно быть **случайным**.

Эффективность протокола ALOHA в чистом виде ~18% использования канала. Существует дискретный вариант ALOHA, позволяющий увеличить эффективность до ~37%. Основная причина низкой эффективности – станции не учитывают поведение друг друга. В локальной сети можно организовать процесс таким образом, что станции будут учитывать поведение. Такие протоколы называются протоколами с контролем несущей.

Протоколы, учитывающие состояние линии связи, позволяют увеличить эффективность использования разделяемого канала.

Протоколы множественного доступа с контролем несущей (Carrier Sense Multiple Access, CSMA)

CSMA. Основная идея: когда у станции появляются данные для передачи, она проверяет канал – свободен он или занят. Если канал занят – станция ждет его освобождения. Если канал свободен – станция передает кадр. Если происходит коллизия – станция ждет в течение случайного интервала времени, прослушивает канал и пытается повторить передачу кадра.

Улучшением системы CSMA является **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) – множественный доступ с контролем несущей и обнаружением конфликтов.

Основная идея: как только станции, передающие данные, обнаруживают коллизию, они немедленно прекращают передачу.

CSMA/CD является основой MAC-уровня Ethernet, Apple EtherTalk, G-Net и др.

Множественный доступ с контролем несущей и предотвращением коллизии (Carrier Sense Multiple Access/Collision Avoidance) – **CSMA/CA**.

Идея: Узел, готовый послать кадр, прослушивает линию. При отсутствии несущей он посылает короткий сигнал запроса на передачу и определенное время ожидает ответа от адресата назначения. При отсутствии ответа передача откладывается, при получении – посылается кадр.

Пример: Apple LocalTalk.

Методы доступа с передачей маркера (иначе – методы передачи полномочий).

Используют специальный тип кадра – маркер.

Маркер (токен, token) – служебный кадр особого формата, определяющий доступ к разделяемой среде передачи данных.

Идея: маркер передается от узла к узлу, при этом только узел, владеющий маркером доступа, имеет право передачи данных.

Примеры: Token Ring, FDDI.

Лекция № 8. Базовые технологии локальных сетей. Беспроводные сети

Базовые технологии локальных сетей.

Специфику локальной сети отражают 2 нижних уровня OSI – физический и канальный. Другие уровни имеют общие черты для локальных и глобальных сетей.

Стандартизацию локальных сетей проводит комитет **802 института IEEE**.

Соответствующие стандарты нумеруются по схеме:

IEEE 802.X,

где X – номер подкомитета, занимающегося конкретным стандартом.

К основным стандартам относятся:

802.1 – межсетевой обмен;

802.2 – управление логическим каналом;

802.3 – локальные сети CSMA/CD (Ethernet);

802.4 – локальные сети с топологией «шина» и передачей маркера;

802.5 – локальные сети с топологией «кольцо» и передачей маркера;

802.6 – городские сети (MAN – Metropolitan Area Network);

802.7 – техническая группа по широкополосной связи;

802.8 – техническая группа по волоконной оптике;

802.9 – интегрированные сети для передачи голоса/данных;

802.10 – обеспечение сетевой безопасности;

802.11 – беспроводные сети;

802.12 – LAN с доступом по приоритету запроса, 100BaseVg-AnyLAN.

Канальный уровень в локальных сетях делится на два подуровня (уровня):

- Логической передачи данных LLC (Logical Link Control);
- Управления доступом к среде MAC (Media Access Control).

Уровень LLC отвечает за передачу данных между узлами с различной степенью надежности, реализует интерфейс с прилегающим сетевым уровнем, а также определяет использование логических интерфейсных точек SAP (Service Access Point).

Уровень MAC обеспечивает совместное использование разделяемой среды передачи данных в соответствии с протоколом доступа, который определяет специфику локальной сетевой технологии (Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, 100VG-AnyLAN и др.).

Протоколы каждого из уровней ***независимы***: любой протокол MAC-уровня может применяться с любым протоколом LLC-уровня.

Технология Ethernet (IEEE 802.3).

Прототипом Ethernet послужила радиосеть ALOHA Гавайского университета. В 1975 году фирма Xerox разработала на ее основе сеть Ethernet

Network со скоростью 2,94Мбит/с. Название технологии происходит от *luminiferous ether* – светоносного эфира – гипотетической среды, в которой распространяются электромагнитные волны.

В 1980 году DEC, Intel и Xerox совместно разработали стандарт Ethernet II для сети на основе коаксиального кабеля (т.н. Ethernet DIX).

На основе Ethernet II комитетом 802 был разработан стандарт IEEE 802.3.

Общая формула спецификации классов сетей Ethernet 802.3 имеет вид:

xBase-y,

где x – битовая скорость технологии данного класса в Мбит/с (10, 100, 1000);

y – тип физической среды (F, T, TX и др.).

Base (band) – означает, что использована немодулированная передача в цифровой форме по каналу без частотного разделения.

В зависимости от x выделяют:

- X=10Мбит/с – базовые технологии Ethernet;
- X>=100Мбит/с – высокоскоростные технологии Ethernet (Fast Ethernet и выше).

В «классическом» Ethernet для доступа к среде передачи используется метод множественного доступа с прослушиванием несущей и обнаружением коллизии (CSMA/CD).

Основные этапы:

- Данные передаются в виде кадров, содержащих MAC-адреса узлов отправителя и получателя.
- Перед передачей узел должен убедиться, что среда передачи данных свободна. Это достигается прослушиванием несущей частоты (в базовом Ethernet – 5-10МГц);
- Если среда свободна – узел начинает передачу;
- Все узлы сети могут распознать передачу, синхронизируясь по преамбуле кадра. Узел, распознавший свой адрес буферизирует кадр в буфере сетевой карты. Окончание кадра определяется по исчезновению несущей. По этому сигналу приемник анализирует кадр, проверяет корректность и передает на следующий уровень;
- Если среда передачи данных занята, то узел ждет ее освобождения;
- После передачи кадра все узлы сети должны выдержать технологическую паузу – межкадровый интервал (IPG – Inter Packet Gap) длиной 9,6 мкс.

Домен коллизии – часть сети Ethernet, все узлы которой распознают коллизию, не зависимо от того, в какой части сети она возникла.

Схема обработки коллизии в Ethernet:

– Обнаружение коллизии (collision detection) выполняется детектором коллизии сетевого адаптера по результатам наблюдения за сигналами;
– Узел, обнаруживший коллизию, прерывает передачу кадра и посылает короткую цепочку бит (от 32 до 48), называемую jam (затор), после чего прекращает передачу. Цель посылки jam – заставить заметить коллизию остальные узлы домена коллизии;
– После прекращения передачи узел переходит в режим ожидания в течение случайного отрезка времени. Затем может снова предпринять попытку передачи данных.
– Если 16 попыток передачи завершились коллизией – кадр отбрасывается и NIC сообщает об ошибке.

Из механизма обнаружения коллизии следует Ограничение на размер домена коллизии: диаметр сети должен быть таким, чтобы время передачи кадра min длины было не меньше времени распространения сигнала коллизии до самого дальнего узла сети PDV (Path Delay Value).

10 Мбит/с – домен коллизии ограничен 2500 м.

1 Гбит/с – 200 м (25 м).

Для контроля целостности физического соединения между двумя непосредственно соединенными портами в стандарте 10Base-T введен так называемый тест целостности соединения (Link Integrity Test, LIT). Эта процедура заключается в том, что в те периоды, когда порт не посылает или получает кадры данных, он посылает своему соседу импульсы длительностью 100 нс через каждые 16 мс. Если порт принимает такие импульсы от своего соседа, то он считает соединение работоспособным и, как правило, индицирует это зеленым светом светодиода сетевого адаптера.

В Ethernet существует 4 основных типа кадров:
– Ethernet II (DIX – DEC, Intel, Xerox);
– Ethernet 802.3;
– Ethernet 802.2;
– Ethernet SNAP (SubNetwork Access Protocol).

Отличаются трактовкой полей заголовка и данных (см. рисунок 8.1).

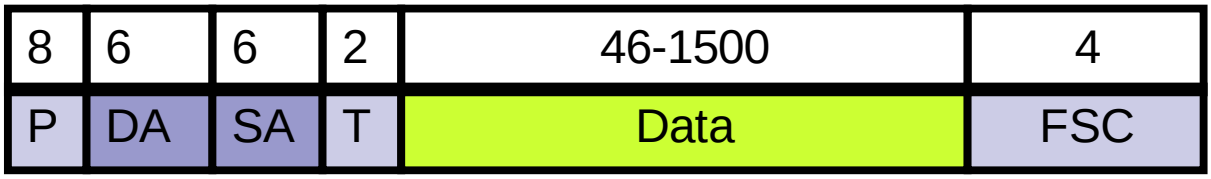

Рисунок 8.1 – Формат кадра Ethernet II

Формат кадра Ethernet II (один из наиболее распространенных):
P – Преамбула (Preamble) 7 байт «10101010»;

MAC-адреса узлов назначения DA(Destination Address) и отправителя SA(Source Address) по 6 байт;

T (Type) Тип протокола верхнего уровня;

FSC (Frame Check Sequence) Контрольная последовательность кадра;

Data – поле данных от 46 до 1500 байт (если размер меньше 46, то дополняется до 46);

MAC-адрес в Ethernet, Token Ring, FDDI состоит из 6 байт, которые принято записывать в шестнадцатеричном виде по шесть пар цифр:

12:B0:18:4E:CD:02

или

12-B0-18-4E-CD-02

Поле DA может содержать:

- Уникальный MAC-адрес (**unicast** address);
- Широковещательный адрес (**broadcast** address);
- Групповой адрес (**multicast** address).

Тип адреса определяется 1-м битом старшего байта адреса:

- 0 – уникальный адрес;
- 1 – групповой адрес;

Если все биты адреса равны «1»:

FF:FF:FF:FF:FF:FF – широковещательный адрес

2-м битом старшего байта адреса определяется способ назначения адреса:

0 – централизованно, комитетом IEEE;

1 – локально администратором сети;

IEEE раздаёт производителям оборудования организационно уникальные идентификаторы (OUI):

3-байтовые префиксы адресов;

00:00:0C – Cisco

00:20:AF – 3COM

3 младших байта задаются производителем.

В виду этого по MAC-адресу, как правило, можно определить производителя сетевого оборудования с этим адресом (или по крайней мере, производителя микросхемы, на которой собрано оборудование).

Базовые технологии Ethernet

10Base-5 («толстый» Ethernet) – сегмент до 500 м, максимальное количество станции – 100;

10Base-2 («тонкий» Ethernet) – сегмент до 185 м, максимальное количество узлов – 30;

10Base-T (802.3i UTP Cat3 или 5) – исп. 2 пары, топология – звезда с концентратором в центре, сегмент до 100 м, количество узлов <1024;

10Base-F (802.3j оптоволокно) – длина до 2100 м, количество узлов <1024.

Для кодирования сигнала в «толстом» и «тонком» Ethernet применялось Манчестерское кодирование или, по-другому, код Манчестер-II.

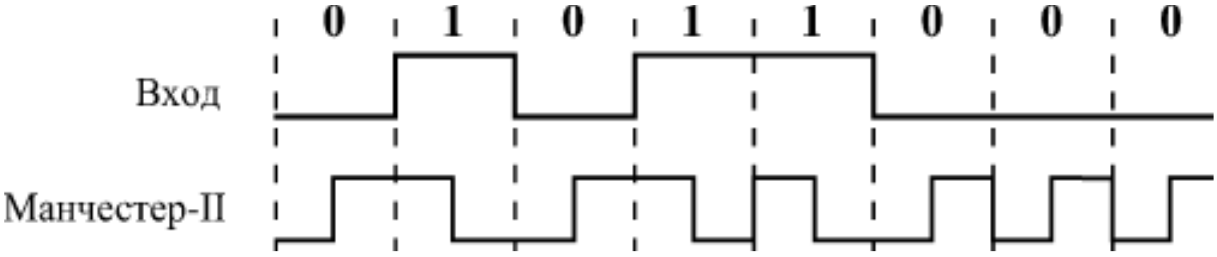

Рисунок 8.2 – Принцип манчестерского кодирования

Суть манчестерского кодирования иллюстрируется (см. рис. 8.2). Входной сигнал представляет собой последовательность бит равной длительности. В каждом такте передается один бит информации. Манчестерский код заменяет единичный информационный бит на отрицательный переход в центре битового интервала, а нулевой информационный бит – на положительный переход в центре битового интервала. Таким образом, в центре каждого битового интервала сигнала в манчестерском коде обязательно имеется фронт (положительный или отрицательный), который может быть использован приемником этого сигнала для синхронизации приема каждого информационного бита. Поэтому манчестерский код называется самосинхронизирующимся кодом.

Для подключения кабеля к сетевой карте компьютера использовались различные типы портов. Для кабеля на основе витой пары применяется разъем именуемый официально Modular 8-pin connector или 8p8c (8 position 8 contact, 8 position 8 conductor), также называемый RJ-45.

Проблема подключения заключается в том, что корректная разводка кабелей предполагает, что выход Tx (передачи сигнала) подключается ко входу Rx (приёма сигнала) и наоборот. Поэтому потребовались порты двух типов:

- MDI (Media Dependent Interface) – соответствует NIC;
- MDI-X (Media Dependent Interface Xover = Crossover – перевернутый) – для каскадирования.

При соединении портов MDI и MDI-X используется прямой кабель, а при соединении одноименных портов (например, двух компьютеров между собой) – перекрестный (кросс-кабель). Способы разводки проводников витой пары в разъемах описаны в стандартах T568A (прямой) и T568B (перекрестный).

Ethernet-сети на основе витой пары первоначально организовались на основе использования концентраторов (hub). Со второй половины 90-х годов начался процесс перехода на коммутируемый Ethernet и использование в качестве центрального устройства локальной сети коммутаторов Ethernet (switch), выполняющих роль, подобную коммутаторам сетевого уровня (маршрутизаторам) в глобальных сетях.

1995 г. Fast Ethernet (IEEE 802.3u)

- Скорость передачи данных = 100 Mbit/s;
- Метод доступа к среде передачи данных: CSMA/CD с сохранением формата кадров базовой технологии;
- Битовый интервал = 10 нс;
- Межкадровый интервал (IPG) = 0,96 мкс;
- Сохранены все временные параметры алгоритма доступа;
- Признак свободного состояния среды – передача по ней символа Idle.

Основные типы среды передачи данных:

- 100Base-TX (2 пары UTP Cat5 или STP Type1) – сегмент 100 м, < 1024 узлов;
- 100 Base-T4 (4 пары UTP Cat3 и выше) – сегмент 100 м, < 1024 узлов;
- 100 Base-FX (MMF) – сегмент 160 м, < 1024 узлов или сегмент 2000 м и 2 узла.

Коаксиальный кабель в число разрешенных сред передачи данных не попал.

Для кодирования передаваемых данных используются NRZI и MLT-3. Код NRZI (без возврата к нулю с инверсией единиц – Non-Return to Zero, Invert to one) предполагает, что уровень сигнала меняется на противоположный в начале единичного битового интервала и не меняется при передаче нулевого битового интервала. При последовательности единиц на границах битовых интервалов имеются переходы, при последовательности нулей – переходов нет. В этом смысле код NRZI лучше синхронизируется, чем NRZ (там нет переходов ни при последовательности нулей, ни при последовательности единиц).

Код MLT-3 (Multi-Level Transition-3) предполагает, что при передаче нулевого битового интервала уровень сигнала не меняется, а при передаче единицы – меняется на следующий уровень по такой цепочке: +U, 0, –U, 0, +U, 0, –U и т.д. Таким образом, максимальная частота смены уровней получается вчетверо меньше скорости передачи в битах (при последовательности сплошных единиц). Требуемая полоса пропускания оказывается меньше, чем при коде NRZ.

Еще одной особенностью Fast Ethernet является использование подуровня автопереговоров (AUTONEG), позволяющего согласовать режим работы (дуплексный или полудуплексный) и скорость (10 или 100 Мбит/с) между устройствами в сети. Это обеспечивает совместимость Fast Ethernet с 10Мбит/с Ethernet.

29 июня 1998 года принят стандарт IEEE 802.3z (использующий одномодовое, многомодовое оптоволокно и UTP cat.5 на короткие расстояния (до 25 метров)).

28 июня 1999 года был принят стандарт 802.3ab передачи по UTP на расстояние до 100 метров.

В рамках этих стандартов сохранено:

- форматы кадров Ethernet;
- Полудуплексная версия протокола с CSMA/CD (применяется редко) и дуплексная с коммутаторами;
- Поддержка всех основных видов кабельных систем.

Изменения в подуровне MAC:

- Минимальный размер кадра увеличен с 64 до 512 байт (допустимым диаметр сети = 200 м);
- Монопольный пакетный режим (Burst Mode) – разрешение передать несколько кадров длиной до 65536 бит (8192 байта) без передачи среды.

На физическом уровне используется логическое кодирование 8B/10B.

В качестве основных сред передачи данных:

- Оптоволокно (1000Base-SX, 1000Base-LX и др.) сегмент от 220м до 40 км;
- 1000Base-CX (твинаксиальный кабель (twinax)) – до 25 м;
- 1000Base-T – UTP категории 5e или 6 – до 100 м;

Для достижения длины сегмента в 100 метров по UTP были выполнены следующие инженерные решения:

- параллельная передача по 4 парам Cat5 (скорость 250Мбит/с для каждой);
- схема кодирования PAM-5 (это позволяет снизить частоту с 250МГц до 125МГц).

10 Gigabit Ethernet или 10 GbE (10 GigE) стандарт впервые опубликован в 2002 году IEEE как Std 802.3ae-2002. Он определяет версию Ethernet с номинальной частотой передачи данных 10Гбит/с, в 10 раз быстрее Gigabit Ethernet. Стандарт:

- Сохраняет подуровень MAC;
- Сохраняет формат кадров 802.3;
- Сохраняет диапазон допустимых размеров кадров.

Основные отличия:

- Только дуплексный режим (отказ от CSMA/CD);
- Ориентация на оптоволоконные КС
- (в июне 2006, после 4 лет разработки принят 10GBase-T – 802.3an – на STP с длиной сегмента до 100 м).

Наиболее высокоскоростными на данный момент являются стандарты: 40 Gigabit Ethernet (40 GbE) и 100 Gigabit Ethernet (100 GbE) принятые 17 июня 2010 года как P802.3ba.

К основным физическим средам этих стандартов относятся:

- 40GBase-CR4, 100GBase-CR10 – 10 м (медь)

– 40GBase-SR4, 100GBase-SR10 – 100 и 125 м (MMF)
– 40GBase-LR4, 100GBase-LR4 – 10 км (SMF)
– 100GBase-ER4 – 40 км (SMF)
– 40GBase-KR4 – 1 м на печатной плате

Характеристики:

– Только полнодуплексные операции;
– Сохранен формат кадра 802.3/Ethernet уровня MAC;
– Сохранены мин и макс размеры кадра;
– Частота битовых ошибок (BER – Bit Error Ratio) меньше или равна 10-12;
– 64 B/66 B логическое кодирование.

Кольцевые технологии Token Ring и FDDI

Token Ring (маркерное кольцо) – архитектура ЛС с логической кольцевой топологией и детерминированным методом доступа, основанным на передаче маркера.

Разработана IBM в 1984 и принята в 1985 в виде IEEE 802.5.

Существуют стандарты:

– 4 Мбит/с;
– 16 Мбит/с;
– 100 Мбит/с.

Логическая топология – однонаправленное кольцо (физически Token Ring сеть представляет собой звезду).

Возможно объединение двух колец с помощью активного оборудования.

Кабельная система – STP Type 1, UTP Type 3, Type 6, оптоволокно. STP Type1 позволяет использовать кольцо из 260 узлов при длине радиальных кабелей до 100 м; UTP – до 72 узлов при длине 45 м.

Максимальная длина кольца – 4000 м.

Физическое кодирование – манчестерский код.

3 формата кадра:

– Маркер;
– Кадр данных;
– Прерывающая последовательность (сигнализирует об отмене текущей передачи кадра или маркера).

Основное отличие: детерминированное время обслуживания – максимальное время ожидания передачи данных для каждой станции фиксировано и может быть рассчитано на основе количества станции и времени владения маркером THT (token holding time). Также поддерживается задание до 8 уровней приоритета для сетевого трафика.

FDDI (Fiber Distributed Data Interface) – оптоволоконная технология. FDDI разрабатывалась как следующее поколение LAN, но из-за большей стоимости и сложности в управлении она применяется в магистралях, а в LAN – не так широко.

Базовая скорость: 100 Мбит/с

Доступ к среде: детерминированный с передачей маркера

Логическая топология: двойное кольцо.

Max. число узлов: 500 – 1000 (2x – 1x).

Длина кольца: 100 км – 200 км (2x – 1x).

Одно из интересных решений в FDDI – механизм отказоустойчивости на основе 2 колец. Каждая станция должна быть подключена к обоим кольцам.

Доступно два режима работы:

Thru – «сквозной» или «транзитный» – используется только первичное (primary) кольцо.

Warp – «свертывание» или «сворачивание» колец (см. рис. 8.3).

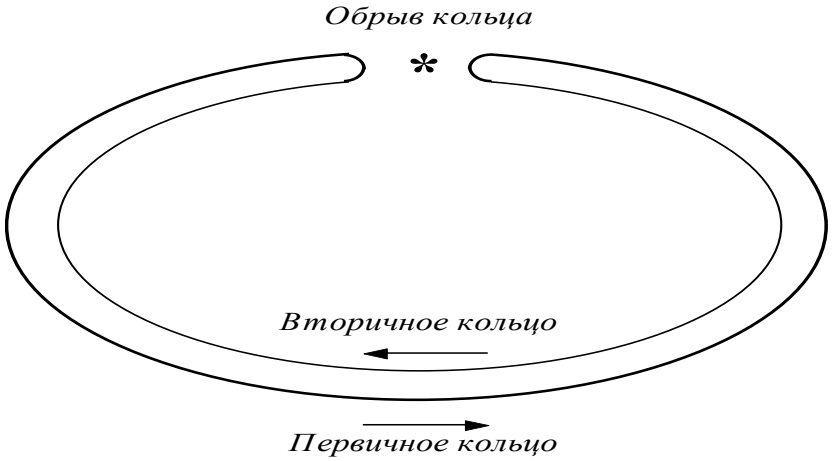

Рисунок 8.3 – Сворачивание колец (Warp) технологии FDDI

Отличия от Token Ring:

- Время обращения маркера не фиксировано заранее;
- Отсутствует приоритизация трафика;
- Адаптивное планирование трафика: синхронный и асинхронный.

Беспроводные локальные сети

Беспроводные сети (wireless networks) – сети, позволяющей организовать передачу данных без использования кабельных систем.

Существуют различные реализации, известные по маркетинговым именам: Wi-Fi, WiMAX, Bluetooth и др.

Беспроводная связь осуществляется в радиочастотном диапазоне 0,9–5 ГГц, инфракрасном и оптическом диапазонах.

Часто используется следующая классификация:

- Персональные беспроводные сети (WPAN – Wireless Personal Area Network) (Bluetooth для класса 2 – до 10 м);
- Беспроводные локальные сети (WLAN) (Wi-Fi = IEEE 802.11, внутри помещений – радиус действия до 100 м);

– Беспроводные городские сети (WMAN) (WiMAX = IEEE 802.16, радиус действия до 6–10 км).

Технология беспроводной связи известная как Wi-Fi соответствует стандарту IEEE 802.11.

Стандарт использует несколько спецификации: инфракрасный сигнал диапазона 850 нм, микроволновой частотный диапазон 2,4 ГГц и метод FHSS, тот же диапазон 2,4 ГГц и метод DSSS. С 802.11a также добавлен диапазон в 5 ГГц (см. таблицу 8.1).

На самом деле полосы частот: 2400–2483,5 МГц и 5180–5240 и 5745–5825 МГц с частотой шага в 5 МГц. Эти полосы отличаются по номеру радио-канала передачи (channel-number). В разных странах их количество может быть разным.

Стандарт	Частота, ГГц	Год	Пропускная спос.
802.11b	2,4	1999	11
802.11a	5	2001	54
802.11g	2,4	2003–05	54–108
802.11n	2,4	2006–09	150–450
802.11ac	5	2014	433–6770
802.11ad	60	2012	7000

Таблица 8.1 – Стандарты Wi-Fi

Для 802.11 определены 2 типа архитектуры: Ad Hoc и Infrastructure Mode:

– В режиме Ad Hoc (Independent Basic Service Set (IBSS) или Peer to Peer режим) узлы взаимодействуют непосредственно друг с другом;
– В режиме Infrastructure Mode узлы взаимодействуют друг с другом через точку доступа AP (Access Point) а не непосредственно.

В режиме Infrastructure Mode точка доступа передает идентификатор беспроводной сети SSID каждые 100 мс на скорости в 100 Кбит/с.

По SSID клиент может выяснить, есть ли возможность подключения к этой точке доступа.

Режим Infrastructure Mode поддерживает два режима взаимодействия с точками доступа:

– BSS (Basic Service Set) – все станции связываются между собой только через точку доступа (она же может быть мостом к внешней сети);
– ESS (Extended Service Set) – структура из сетей BSS, точки доступа взаимодействуют между собой и могут передавать данные между BSS.

Диапазон частот разделен на 11–13 (для разных стран) частично пересекающихся каналов. Не пересекающимися являются 1, 6 и 11 каналы (на самом деле можно выделить еще 4 пары попарно не пересекающихся каналов, например, 2 и 7). Центральная частота одного канала отстоит от центральной частоты другого на 5 МГц, а расстояние между не перекрывающимися каналами – 3 МГц.

Это ведет к наложению сигналов Wi-Fi-адаптеров при большой плотности точек доступа.

В Республике Беларусь использование Wi-Fi не требует обязательной регистрации, если оно не нарушает требования по мощности оборудования и частотному спектру.

Разрешены диапазоны частот:

От 2400 до 2483,5 МГц

От 2500 до 2700 МГц

От 3400 до 3800 МГц

От 5150 до 5875 МГц

Основные проблемы беспроводной передачи данных.

При доступе к среде передачи данных значение имеет интерференция сигналов на приемнике, а не на передатчике.

Существуют две проблемы, связанные с доступом к среде передачи данных:

– Проблема скрытой станции;
– Проблема засвеченной станции.

Проблема скрытой станции: узел A ведет передачу для узла B. Станция C находится вне радиуса узла A и тоже может начать передачу, вызвав искажение на B (см. рис. 8.4).

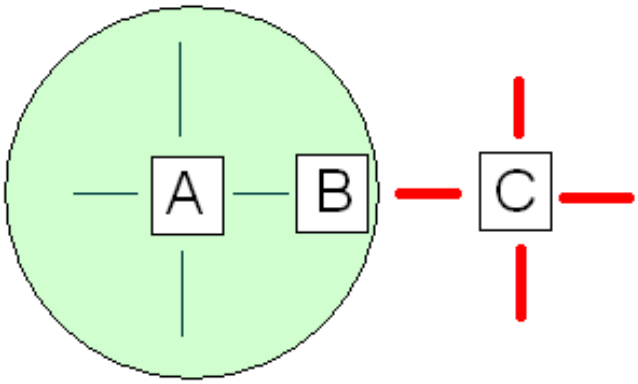

Рисунок 8.4 – Проблема скрытой станции

Проблема засвеченной станции: узел B ведет передачу. Станция C предполагает, что не может начать передачу для D, так как B уже ведет передачу (см. рис. 8.5).

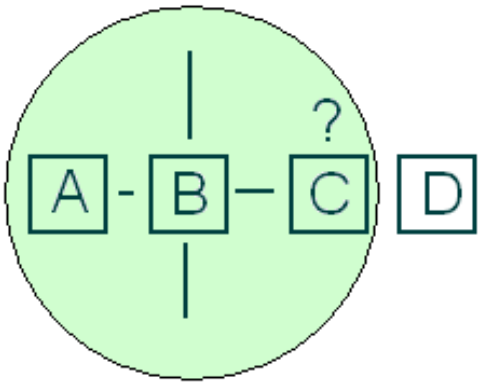

Рисунок 8.5 – Проблема засвеченной станции

Для решения этих проблем на MAC-уровне 802.11 предлагается 2 типа коллективного доступа к среде передачи данных:

- Функция распределенной координации DCF (Distributed Coordination Function) – базовая для 802.11;
- Функция централизованной координации PCF (Point Coordination Function).

DCF основана на CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) – методе коллективного доступа с избеганием коллизии (станция проверяет доступность среды по наличию несущей, затем выжидает и проводит отправку данных; сообщение получено если получено подтверждение от получателя, иначе считается, что произошла коллизия).

Для решения проблемы скрытых узлов может использоваться алгоритм RTS/CTS:

1. Отправитель посылает RTS (Ready To Send) получателю.
2. Получатель отвечает CTS (Clear To Send)
3. Отправитель отправляет кадр
4. Получатель подтверждает прием ACK.

PCF применяется только в сетях с точкой доступа. В этом случае один из узлов (точка доступа) является центром координации PC (Point Coordinator) и управляет доступом остальных узлов к среде передачи данных на основе определенного алгоритма опроса или приоритетов.

Лекция № 9. Технологии физического уровня

При объединении компьютеров между собой возникает проблема выбора топологии. Под **топологией КС** понимают способ организации физических связей в КС.

Формально: **топология** – конфигурация графа, вершинами которого являются узлы сети и коммуникационное оборудование (например, маршрутизаторы), а ребрами – физические или информационные связи между вершинами.

Следует отличать два термина:

- **Физическая топология** – описывает расположение физических линий связи между узлами сети;
- **Логическая топология** – описывает потоки данных, передаваемые в сети.

Эти два варианта могут не совпадать. В качестве примера можно рассмотреть сеть Token Ring (в которой используется логическая топология – кольцо и физическая топология – звезда).

Топология влияет на:

- Надежность сети и возможность балансирования нагрузки (наличие резервных связей повышает надежность сети и позволяет балансировать загрузку отдельных каналов);
- Расширяемость и масштабируемость сети (простота присоединения новых узлов делает сеть легко расширяемой);
- Стоимость сети (топология с минимальной суммарной длиной каналов как правило обойдется дешевле).

Полносвязная. Модель – полный граф. Соответствует сети, в которой каждый узел сети связан со всеми остальными (см. рис. 9.1).

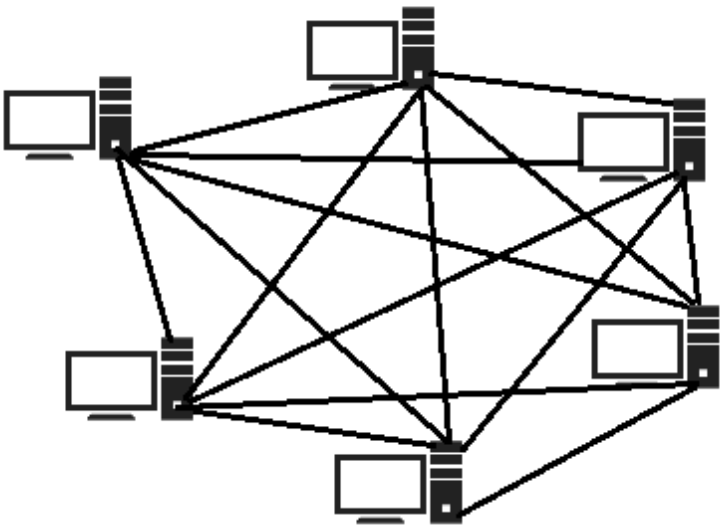

Рисунок 9.1 – Полносвязная топология

Характеризуется максимальной пропускной способностью, высокой сложностью реализации.

Применяется, как правило, для сети с небольшим числом узлов.

Ячеистая (mesh)

Модель – граф, в котором ребра связывают вершины, между которыми происходит интенсивный обмен данными (см. рис. 9.2).

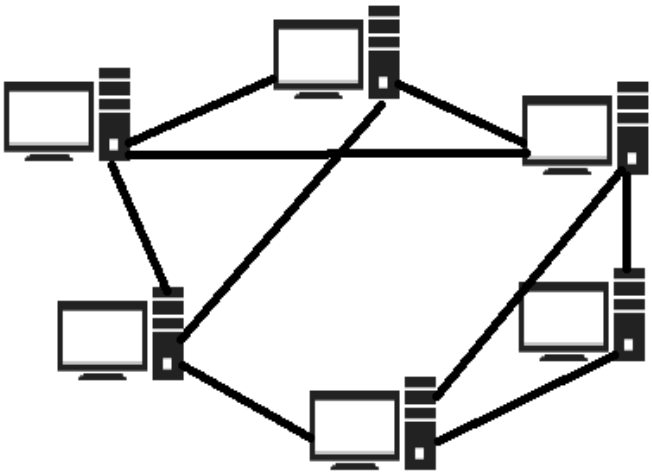

Рисунок 9.2 – Ячеистая топология

Для обмена между не соединенными прямыми связями узлами используются промежуточные узлы.

Общая шина (bus)

Компьютеры подключаются к одному каналу по схеме «монтажного ИЛИ» (см. рис. 9.3).

«Монтажное ИЛИ» соединение называют потому, что включить сигнал в канале могут как узел А, так и узел Б (хотя формально это схема И).

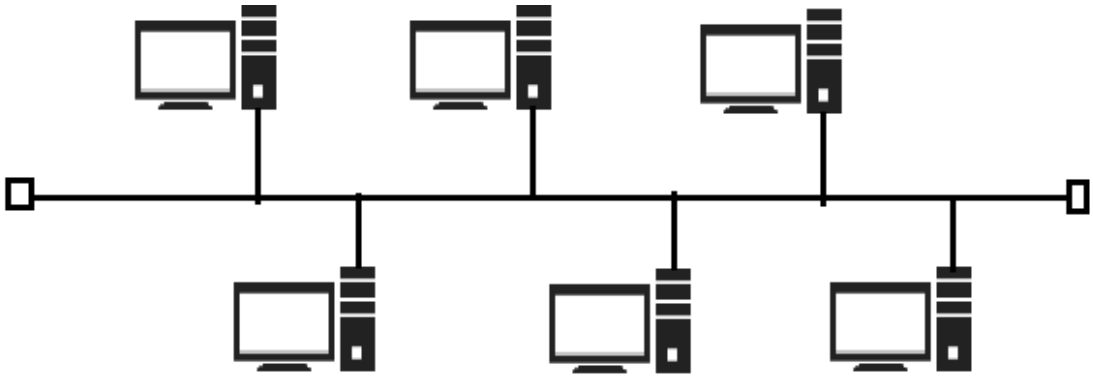

Рисунок 9.3 – Топология «общая шина»

Передаваемая информация может распространятся в обе стороны. Возможно широковещательное обращение ко всем узлам. Шина – разделяемая среда: в отдельный момент времени только один компьютер может передавать данные. Невысокая производительность.

Звезда (star)

В этой топологии каждый узел подключается отдельным каналом к коммуникационному устройству в центре сети, которое направляет информацию одному или всем остальным компьютерам сети (см. рис. 9.4).

Достаточная надежность. Довольно низкая масштабируемость (связанная с ограниченным количеством портов центрального устройства – коммутатора или концентратора (ранее)).

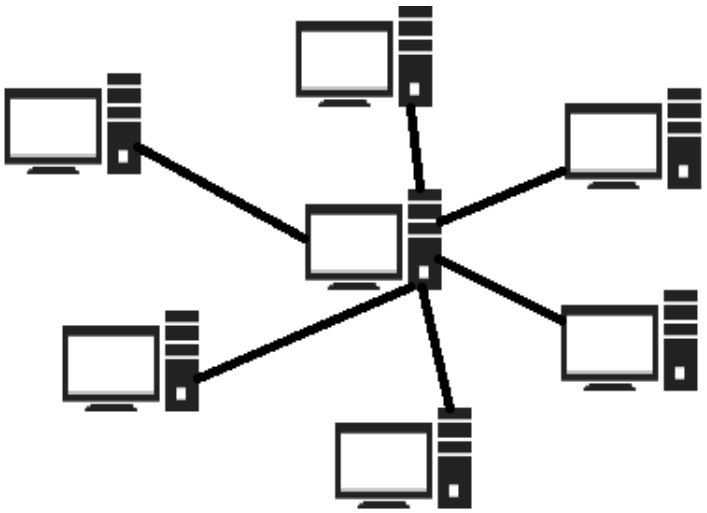

Рисунок 9.4 – Топология звезда

Иерархическая звезда или дерево (tree)

Недостаток расширяемости компенсируется каскадированием коммуникационных устройств: несколько таких устройств соединяются между собой связями типа звезда (см. рис. 9.5).

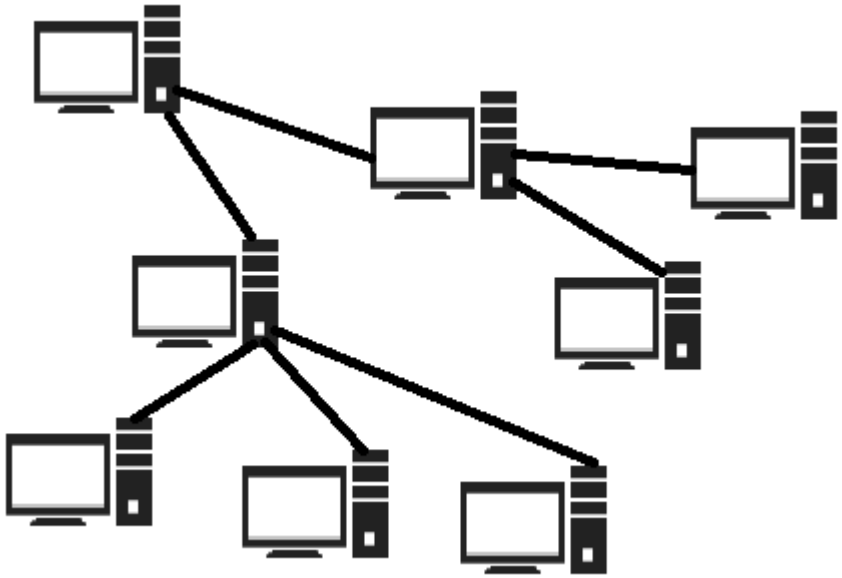

Рисунок 9.5 – Иерархическая звезда или дерево

Кольцо (ring)

Каждый узел выполняет роль ретранслятора: данные передаются по кольцу от одного узла другому (см. рис. 9.6).

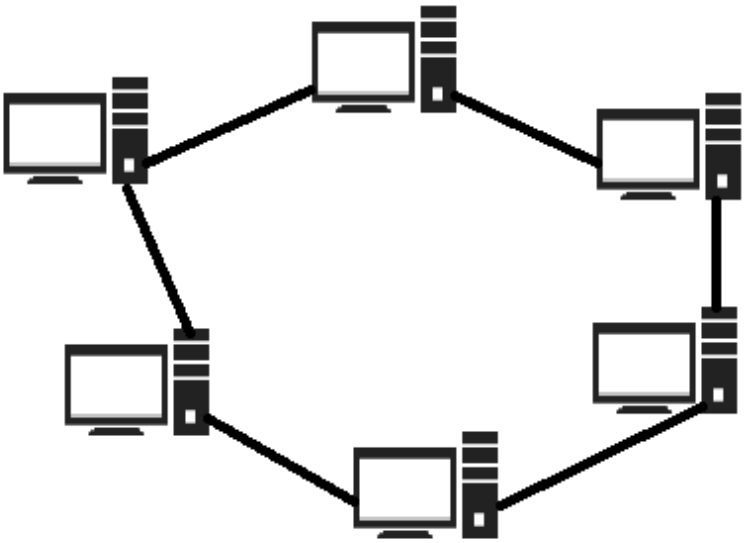

Рисунок 9.6 – Кольцевая топология

Топологии могут иметь 2 кольца, работающие в противоположных направлениях или использовать их для повышения надежности сети (см. технологию FDDI).

Смешанная топология (Hybrid).

Характерны для крупных сетей: отдельные подсети с типовыми топологиями, произвольно связанные между собой.

Проблема выбора топологии – организация совместного использования канала связи: разделяемые каналы или индивидуальные каналы. Сеть с разделяемой средой при большом количестве узлов имеет более низкую производительность, чем аналогичная сеть с индивидуальными каналами. Глобальная сеть обычно использует индивидуальные каналы. В последнее время в локальных сетях также прослеживается такая тенденция.

Физическая среда передачи данных

- Проводная (wired):
  - Проводные (воздушные) линии связи;
  - Кабельные линии связи;
  - Оптоволоконные линии связи.
- Беспроводная (wireless):
  - Земная атмосфера;
  - Космическое пространство.

Кабельные линии связи (медные кабельные системы) представлены следующими наиболее часто встречающимися вариантами:

Коаксиальный кабель (см. рис. 9.7):

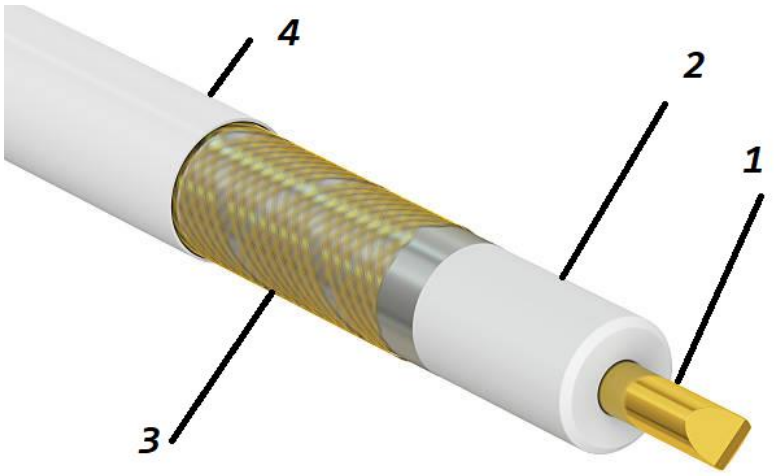

Рисунок 9.7 – Структура коаксиального кабеля

Коаксиальный кабель состоит из:

1) Внутренний (центральный) проводник;
2) Изоляция (диэлектрик);
3) Внешний проводник или экран (оплетка) – защищает от наводок и играет роль второго проводника;
4) Внешняя оболочка – служит для защиты от внешних воздействий.

Применялся в качестве среды передачи данных в ранних версиях Ethernet (т.н. «толстый» и «тонкий» Ethernet).

Витая пара (Twisted Pair cable, TP) (см. рис. 9.8):

Рисунок 9.8 – Витая пара

Применяемая в современных версиях Ethernet состоит из 8 попарно перевитых медных проводов с маркировкой цветовым ключом.

Кабель этого вида как правило подразделяется на:

- Экранированная витая пара, STP (Shielded TP);
- Неэкранированная витая пара, UTP (Unshielded TP).

Кроме этого, витая пара подразделяется на категории, определяющие частотный диапазон их применения (см. табл. 9.1).

CAT	Полоса частот, МГц
1	0,1–0,4
2	1–4
3	16
4	20
5	100
5e	100–125
6	200 (250)
6A	500
7	600

Таблица 9.1 – Категории витой пары

По принципу устройства, медные кабельные системы содержат по крайней мере 2 медных проводника.

Сигналы при этом может передаваться:

- в потенциальном представлении;
- в токовом представлении.

При потенциальном представлении информационный параметр – уровень напряжения сигнала между передатчиком и приемником.

Потенциальное представление:

- Асимметричное – один проводник назначается общим;
- Дифференциальное (симметричное) – оба проводника равноправны и сигнал снимается как разница между ними.

При токовом представлении – наличие или отсутствие тока в цепи или его направление.

Примеры:

Коаксиальный кабель (coaxial cable):

- RG-58 A/U (тонкий) – импеданс 50 Ом, D=5 мм, d=0,89 мм;
- RG-8 (толстый) – импеданс 50 Ом, D=12 мм, d=2,17 мм.

Недостаток (коаксиального кабеля): ограниченная пропускная способность (до 10 Мбит/с).

Волоконно-оптические кабельные системы

Сигнал передается несущей оптического диапазона волн по световоду.

Принцип работы основан на явлении полного внутреннего отражения луча на границах раздела двух сред с разными показателями преломления: если луч выходит из оптически более плотной среды в менее плотную, то при определенном значении угла падения луч начинает скользить по границе раздела сред без перехода в оптически более плотную.

Излучение внешнего источника возбуждает в световоде несколько типов волн, которые называются **модами**.

В зависимости от распределения показателя преломления и величины диаметра сердечника различают:

- **Многомодовые волокна** (MMF – Multi Mode Fiber);
- **Одномодовые волокна** (SMF – Single Mode Fiber) (см. рис. 9.9).

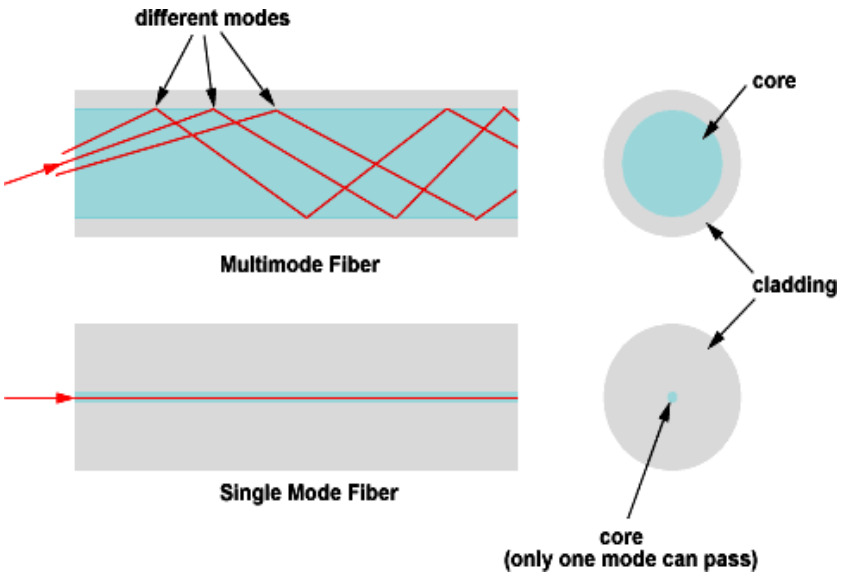

Рисунок 9.9 – Многомодовый и одномодовый оптоволоконный кабель

Оборудование в компьютерной сети

Сетевое оборудование (не только физического уровня) можно разделить на два вида:

- Активное сетевое оборудование – оборудование производящее цифровую обработку сигнала;
- Пассивное сетевое оборудование – не проводит цифровой обработки передаваемого через него сигнала.

К активному сетевому оборудованию относятся:

- Сетевые адаптеры;
- Коммутаторы;
- Маршрутизаторы;
- Модемы;

– Медиаконвертеры.

К пассивному сетевому оборудованию относятся:

– Кабельные системы;
– Повторители;
– Концентраторы;
– Коннекторы;
– Коммутационные панели.

Сетевой адаптер (Network Interface Card, NIC).

Вместе с драйвером реализует протокол доступа к среде, который уникален для сетевой технологии. Реализует функции физического и MAC-уровней.

Повторитель (repeater).

Повторитель используется для физического соединения различных сегментов кабеля сети с целью увеличения общей длины сети. Его назначение усиливать и повторять сигнал, полученный из одного сегмента в другой. Также может исправлять неравномерность интервалов между импульсами.

Концентратор или **хаб** (concentrator, hub).

Представляет собой повторитель, который имеет несколько портов и соединяет несколько сегментов. При получении сигнала на один из своих портов концентратор повторяет его в остальные порты. В данный момент концентраторы практически не выпускаются, так как им на смену пришли более функциональные устройства – сетевые коммутаторы (свитчи). Коммутаторы способны выделить каждое подключенное устройство в отдельный сегмент. Иногда коммутаторы ошибочно называют «концентраторами с интеллектом».

Медиаконвертер – оборудование, преобразующее среду распространения сигнала из одного типа в другой (чаще всего между оптическими и медными кабельными системами). На физическом уровне работают т.н. простые медиаконвертеры 1 уровня.

СПИСОК ЛИТЕРАТУРЫ

1. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл, А. Гребеньков; [пер. с англ. А. Гребенькова]. – 5-е изд. – Санкт-Петербург [и др.]: Питер, 2022. – 955 с.: ил.

2. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. 552800 «Информатика и вычислительная техника» и по спец. 220100 «Вычислительные машины, комплексы, системы и сети», 220200 «Автоматизированные системы обработки информации и управления» и 220400 «Программное обеспечение вычислительной техники и автоматизированных систем» / В. Олифер, Н. Олифер. – 5-е изд. – Санкт-Петербург [и др.]: Питер, 2017. – 992 с.: ил.

3. Фейт, С. TCP/IP. Архитектура, протоколы, реализация (включая IPv6 и IP Security) / С. Фейт. – М.: Издательство: Лори, 2014. – 424 с.

4. Куроуз, Д. Компьютерные сети: нисходящий подход / Д. Куроуз, К. Росс. – 6-е изд. – Москва: Изд-во «Эксмо», 2016. – 912 с.: ил.

5. Гук, М. Аппаратные средства локальных сетей / М. Гук. – СПб.: Издательство «Питер», 2002. – 576 с.: ил.

6. Телекоммуникационные технологии / Telecommunication technologies – телекоммуникационные технологии (v2.1) [Электронный ресурс] / Семенов Ю.А. (ГНЦ ИТЭФ). Оригинал: book.itep.ru. – Режим доступа: https://www.opennet.ru/docs/RUS/inet_book/. – Дата доступа: 20.11.2023.

7. The TCP/IP Guide / © 2003–2017 Charles M. Kozierok. All Rights Reserved [Electronic resource]. – Mode of access: http://tcpipguide.com/. – Date of access: 20.11.2023.

Учебное издание

НОВЫЙ Вадим Владимирович

КОМПЬЮТЕРНЫЕ СЕТИ

Курс лекций

Технический редактор *Г.В. Разбоева*

Компьютерный дизайн *Л.В. Рудницкая*

Подписано в печать 22.12.2023. Формат 60x84 $^{1}/_{16}$. Бумага офсетная.
Усл. печ. л. 4,82. Уч.-изд. л. 3,96. Тираж 50 экз. Заказ 159.

Издатель и полиграфическое исполнение – учреждение образования
«Витебский государственный университет имени П.М. Машерова».

Свидетельство о государственной регистрации в качестве издателя,
изготовителя, распространителя печатных изданий
№ 1/255 от 31.03.2014.

Отпечатано на ризографе учреждения образования
«Витебский государственный университет имени П.М. Машерова».
210038, г. Витебск, Московский проспект, 33.