

Лекция 1

Ограничения топологии сети, построенной на коммутаторах
Структура коммутатора ЛВС
Логика работы коммутатора
Полнодуплексный протокол ЛВС

Лекция 2

Управление потоком данных при полном дуплексе
Управление потоком данных при полудуплексном режиме работы
Техническая реализация коммутаторов

Лекция 3

Техническая реализация КМ
Комбинированные коммутаторы
Характеристика, влияющая на производительность КМ
Скорость фильтрации с продвижением кадра
Пропускная способность КМ
Задержка передачи данных
Размер адресной таблицы

Лекция 4

Объем буфера порта
Дополнительные функции коммутаторов

Лекция 5

Способы организации VLAN
Варианты применения коммутатора в ЛВС
Стянутая в точку магистраль (collapsed backbone)
Распределенная магистраль

Лекция 6

Сетевой уровень
Маршрутизаторы
Принципы объединения сетей на основе протоколов сетевого уровня
Ограничение сетей на коммутаторах
Межсетевое взаимодействие

Лекция 7

Принципы маршрутизации

Лекция 8

Таблица маршрутизации
Протоколы маршрутизации
Функции маршрутизатора
Реализация сетевого взаимодействия средствами TCP/IP

Лекция 9

Основной уровень (транспортный)
Прикладной уровень
Уровень сетевых интерфейсов
Соответствие уровней стека TCP/IP 7миуровневой модели ISO\OSI
Типы адресов стека TCP/IP

Лекция 10

IP-адрес
Классы IP-адресов
Специальные IP-адреса

Лекция 11

[Маска в IP-адресации](#)
[Порядок распределения IP-адресов](#)
[Технология NAT](#)
[Двойная трансляция](#)

[Лекция 12](#)

[Автоматизация процесса назначения IP-адресов](#)
[Отображение IP-адреса на локальные адреса](#)
[Отображение доменных имен](#)
[Система доменных имен](#)
[Схема разрешения IP-адресов](#)

[Лекция 13](#)

[Интернет-протокол IP](#)
[Структура IP пакета](#)

[Лекция 14](#)

[Таблица маршрутизации в IP сетях](#)
[Источники записи таблиц маршрутизации](#)
[Алгоритм по продвижению пакетов в сети](#)

[Лекция 15](#)

[Маршрутизация с использованием масок](#)
[Работа в сети](#)
[Использование масок переменной длины](#)

[Лекция 16](#)

[Использование масок переменной длины](#)
[Некоторые особенности масок переменной длины](#)
[Технология бесклассовой междоменной маршрутизации](#)

[Лекция 17](#)

[Технология CIDR](#)
[Фрагментация пакетов](#)

[Лекция 18](#)

[Протокол надежной доставки сообщений TCP](#)
[Порты](#)
[Сегменты и потоки](#)
[Соединение](#)

[Лекция 19](#)

[Скользящее окно в TCP](#)
[Внутренние и внешние протоколы маршрутизации в Internet](#)

[Лекция 20](#)

[Дистанционно-векторный протокол RIP](#)
[Этапы работы RIP](#)
[Адаптация RIP-маршрутизатора к изменениям состояния сети](#)
[Протокол OSPF](#)

[Лекция 21](#)

[Классификация МШ по областям применения](#)
[Основные технические характеристики МШ](#)
[Корпоративные модульные концентраторы](#)

[Лекция 22](#)

[Стирание грани между МШ и КМ](#)
[КМ 3 уровня с классической маршрутизацией](#)
[Маршрутизация потоков](#)

[Лекция 23](#)

[Глобальные сети](#)

[Присвоение номера AC](#)

[Типы AC](#)

[Обобщенная структура и функции ГС](#)

[Транспортные функции ГС](#)

[Структура ГС](#)

[Лекция 24](#)

[Интерфейс DTE-DCE](#)

[Типы глобальных сетей](#)

[Магистральные сети и сети доступа](#)

[Лекция 25](#)

[ГС на основе выделенных линий](#)

[Аналоговые выделенные линии](#)

[Модемы для выделенных каналов](#)

[Цифровые выделенные линии](#)

[Технология PDH \(плэзиохронная\)](#)

[Лекция 26](#)

[Иерархия цифровых скоростей](#)

[Физический уровень технологии PDH](#)

[Недостатки технологии PDH](#)

[Лекция 27](#)

[Технология синхронной цифровой иерархии SONET/SDH](#)

[Кадры данных технологии SONET](#)

[Структура сети SONET/SDH](#)

[Устройства DSU/CSU для подключения выделенными каналами](#)

[Протоколы канального уровня для выделенных линий](#)

[Лекция 28](#)

[Отказоустойчивость сети SONET/S](#)

[Automatic Protection Switching \(APS\)](#)

[Использование двойных колец для отказоустойчивости SONET/SDH:](#)

[Применение цифровых первичных сетей](#)

[SLIP-Serial Line IP](#)

[Лекция 29](#)

[Протокол PPP](#)

[Лекция 30](#)

[Глобальные связи на основе связей с коммутацией каналов.](#)

[Организация аналогов. телеф. сетей.](#)

[Модемы для работы на аналог. коммутир. линиях.](#)

[Сети ISDN](#)

[Пользоват. интерф. ISDN сети.](#)

[BRI:](#)

[PRI:](#)

[Подключение пользов. оборуд. к сети ISDN](#)

[Лекция 31](#)

[Использование служб ISDN в корпоративной сети.](#)

[Коммутация пакетов](#)

[Режим PVC](#)

[Лекция 32](#)

[Семинар 1](#)

[Средства оптической передачи](#)

[Семинар 2](#)

[Существует дисперсия трёх видов](#)

[Мощность сигнала, потери, усиление](#)

[Окна прозрачности](#)

[Семинар 3](#)

[Солитоновая технология](#)

[Источники и приёмники излучения](#)

[Светодиоды](#)

[Лазеры](#)

[Детекторы излучения](#)

[Оптический интерфейс](#)

[Передачик](#)

[Приёмник](#)

[Семинар 4](#)

[Семинар 5](#)

[Топология соединений. Разветвители и мультиплексоры](#)

[Оптические разветвители](#)

[Основные техн. параметры WDM фильтров \(устройств\)](#)

[Семинар 6](#)

[Оптические изоляторы](#)

[Вращение плоскости поляризации света](#)

[Принцип действия оптического изолятора](#)

[Технические параметры оптических изоляторов](#)

[Оптические аттенюаторы](#)

[Семинар 7](#)

[Оптические переключатели](#)

[Оптические коммутаторы](#)

[Разветвитель-коммутатор 2x2](#)

[Оптические коммутатор nxn.](#)

[Волновые конвертеры](#)

[Семинар 8](#)

[Параметры кабеля](#)

[Оптические соединители](#)

[Разъемные соединения \(коннекторы\)](#)

[Аксессуары и инструменты](#)

[Приборы для монтажа](#)

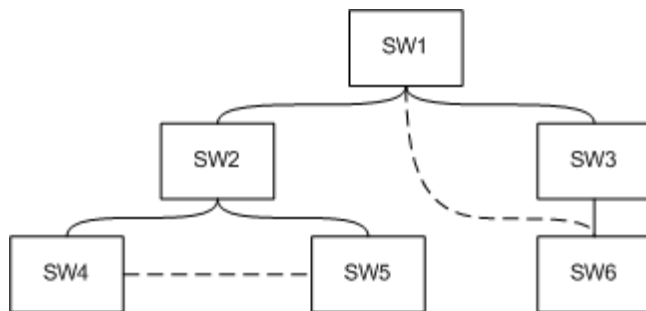
[Введение полностью оптической сети](#)

[Где используются?](#)

Лекция 1

Ограничения топологии сети, построенной на коммутаторах

1. слабая защита от широковещательного шторма;
2. невозможность поддержки петлеобразных топологий сети - необходимо строить только древовидную структуру.



Ветки дерева не должны сходиться

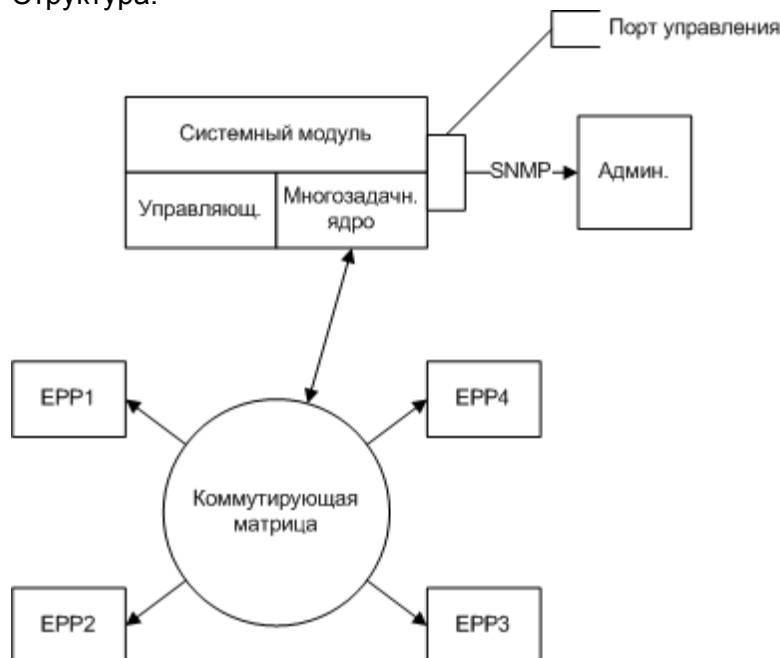
Запасные провода прокладываются заранее.

Алгоритм покрывающего дерева (STA Spoming Tree Alogorithm) - работает автоматически, т.е. автоматически поддерживает древовидную структуру сети и восстанавливает её если нужно.

Структура коммутатора ЛВС

Впервые предложено фирмой Kalpana в 1990г.

Структура:



Системный модуль координирует работу коммутатора - ведёт единую адресную таблицу и обеспечивает управление коммутатором по протоколу SNMP (Simple Network Management Protocol).

Логика работы коммутатора

1. При поступлении кадра на порт, ЕРР буферизует несколько первых байт кадра для определения адреса кадра;
2. Получив адрес назначения, системный модуль получает решения о передаче кадра на какой-то порт по таблице (Table), не дожидаясь прихода других байт кадра;
3. По MAC-назначению и таблице в формате Table принимается решение о либо

передаче на порт, либо применении спецоперации (Flood Discond);

4. Выработав управляющую команду для коммутир. матрицы, КМ проверяет готовность порта к приёму данных. Если порт не занят, то производится передача транзитом. Если порт занят, то КМ буферизует все остальные байты кадра и после освобождения порта передаёт их на выход.

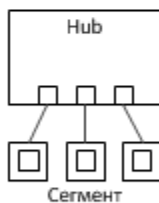
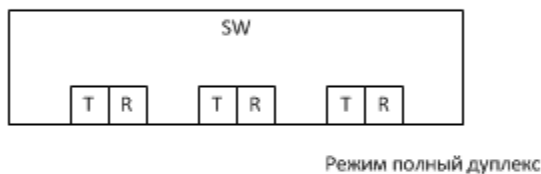
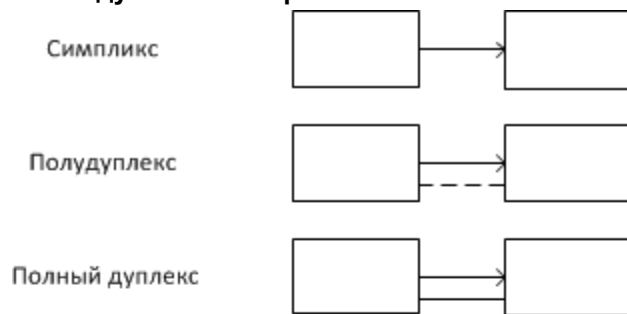
Описанный режим работы КМ называется “Коммутатор на лету” (задержка на выходе ≤ 40 мкс).

Также есть и коммутатор с полной буферизацией.

Современные коммутаторы совмещают режим “на лету” и “с полной буферизацией”.

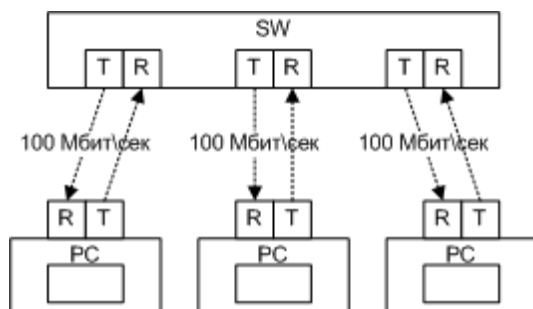
Исходно они работают “на лету”, но в процессе работы определяют, если он превышает процент загруженности, то переходит в режим “с полной буферизацией” (если в КМ нет дополнительных функций).

Полнодуплексный протокол ЛВС



Достоинства - одновременная передача туда и обратно

Лекция 2



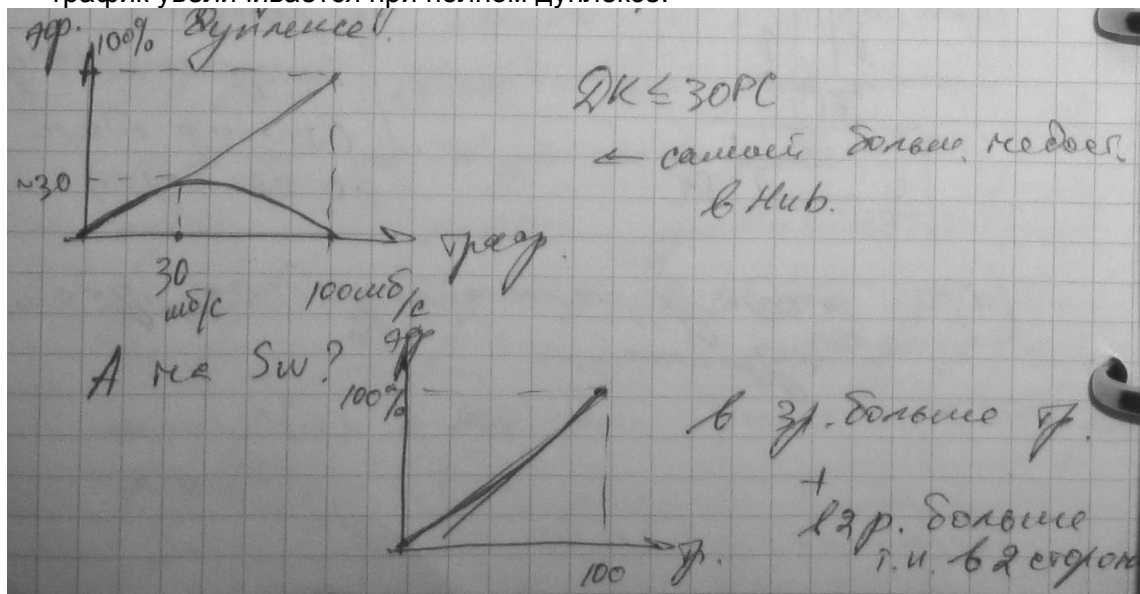
Полный дуплекс - одновременная передача в 2 стороны.

СА не умеет работать в этом режиме, так как он привык работать с Hub'ами и в режиме контроля коллизий. Чтобы заставить его работать при полном дуплексе, надо отключить контроль коллизий.

Hub - вкл. режим коллизий

Switch - выкл. режим коллизий

В современных СА есть автомат. определ. к чему подключен PC (Hub или Switch) и он автоматически включает или выключает режим коллизий для режима полного дуплекса => трафик увеличивается при полном дуплексе.



В 3 раза больше тр. + в 2 раза больше, т.к. полный дуплекс => эффективность на Switch увеличивается в 6 раз.

Подключенный к портам коммутатора не сегмент, а отдельный PC - называется микросегментацией.

В случае использования полного дуплекса необходимо отключать режим фиксации коллизий, иначе полный дуплекс будет воспринят как коллизия.

При использовании СА с Hub необходимо фиксировать коллизию - полудуплекс.

Многие СА сейчас поддерживают оба режима работы - отраб. работу полудуплекса при подключ. к Hub и логику полного дуплекса при подключ. к Switch.

Методы доступа (кольцо, случайный FDDI) в полном дуплексе не нужны. Этот метод сближает все технологии.

Недостатки - разные форматы кадра (разные поля) у разных технологий и поэтому объединять технологии нельзя.

Полудупл. протокол сближает различные сетевые технологии (Eth, TR,...) т.к. их определ. метод доступа к среде. При полном дуплексе метода нет - выход в сеть любой. Различия

остались только в различных форматах кадра.

Управление потоком данных при полном дуплексе

В Switch портов: от 4 до 100 и более. К ним подключаются PC, и каждый PC выходит в сеть когда хочет (когда есть кадр для передачи). Поток данных неограничен ничем. Это накладывает некоторые проблемы.

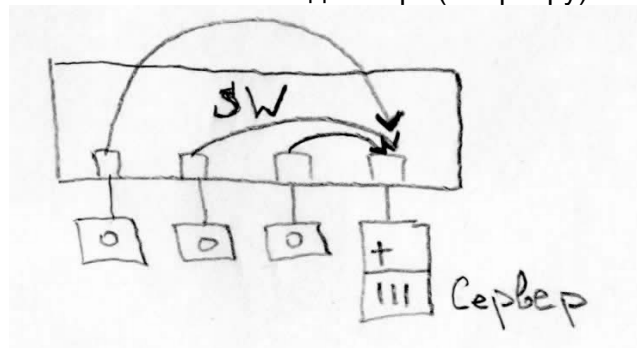
Пример: к одной PC (сервер) обращается куча других PC, она не успевает обрабатывать => заполняется буферная память (производительность PC должна быть выше средней загрузки канала). Но кадр не должен быть потерян => надо притормаживать трафик, а то даже буферная память не спасёт.

Выход из ситуации: загруженная PC сообщает остальным PC - прекратить поставку кадров. А сам освобождает буфер (~ до 10%).

RNR - приёмник не готов.

RR - приёмник готов.

В полнодуплексном режиме поток кадров регулируется самим методом доступа. При переходе на полный дуплекс узлу разрешается посылать кадр всегда => Switch может сталкиваться с перегрузками - нужны средства притормаживания трафика. Причина - ограниченная пропускная способность порта. Особенно ярко проявляется, когда трафик всех PC стекается в один порт (к серверу).



Метод управления потоком X.25, протокол LAP-B. Спец. кадры управления потоком:

- RNR - Receiver Not Ready
- RR - Receiver Ready (стандарт 802.3z)

Когда в буфере порта память заполняется почти до верху, порт вырабатывает спец команду RNR, по которой все остальные порты прекращают передачу, а буфер постепенно освобождается. И при достижении почти дна буфера (~ 10%) вырабатывает спец. команду RR, которая открывает вновь порт, т.е. доступ к PC.

Линейное регулирование - грубое. Необходимо плавное регулирование, а линейное - слишком грубое.

Управление потоком данных при полудуплексном режиме работы

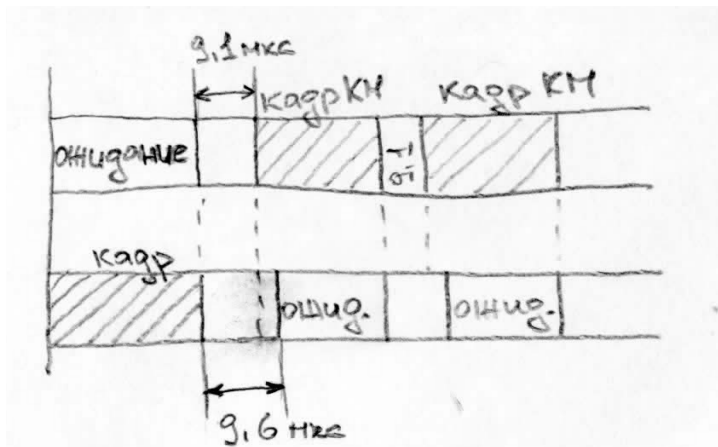
Воздействие на поток данных производится с помощью использования механизма доступа к сети. Эти приёмы основаны на том, что порты CA строго отрабатывают методы доступа а Switch нет.

Применяются два способа управления потоком данных:

1. обратное давление (backpressure). Заключается в создании искусственной коллизии в сегменте, в кот. очень интенсивно посылается кадр. Для этого KM(SW) использует Jam. последовательность (чтобы включить задержку передачи на

конкретный порт др. РС);

2. метод агрессивного захвата. Основан на агрессивном поведении порта КМ:
 - а. либо после окончания передачи кадра;
 - б. либо после коллизии (Jam).



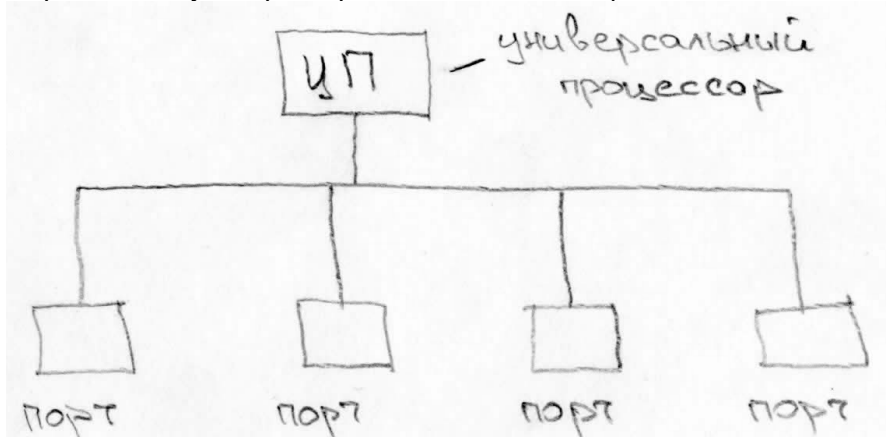
Кадр КМ посыл. раньше, чем за 9,6мкс и РС не может выйти в сеть. Т.е. КМ занимает среду раньше, чем положено.

С помощью этих способов можно довольно плавно регулировать трафик путём увеличения агрессивности КМ по мере необходимости.

Практически во всех КМ(SW), кроме простых используется один из этих алгоритмов.

Техническая реализация коммутаторов

Первые коммутаторы строились на одном ЦП.



Недостатки: основной недостаток - низкая скорость => стали использовать специализированные процессоры, которые можно использовать на каждом порту (форма Kalpana).

ASIC - Application Specific Integrated Circuit

Таким образом современные КМ - многопроцессорные устройства.

В настоящее время используется одна из трех схем построения КМ:

1. коммутационная матрица;
2. разделённая многовходовая память;
3. КМ на общей шине.

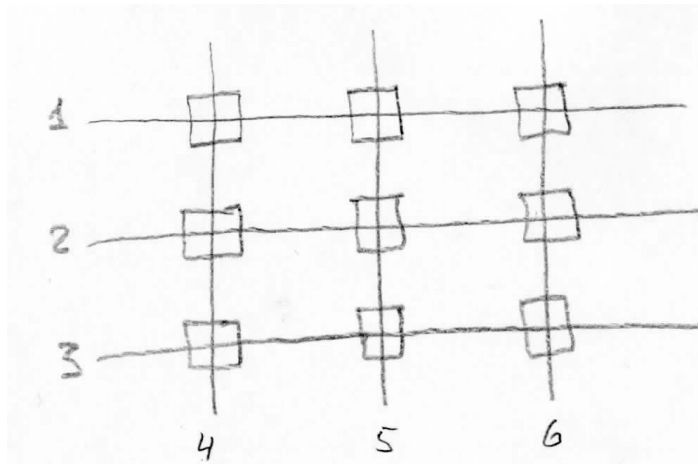
Лекция 3

Техническая реализация КМ

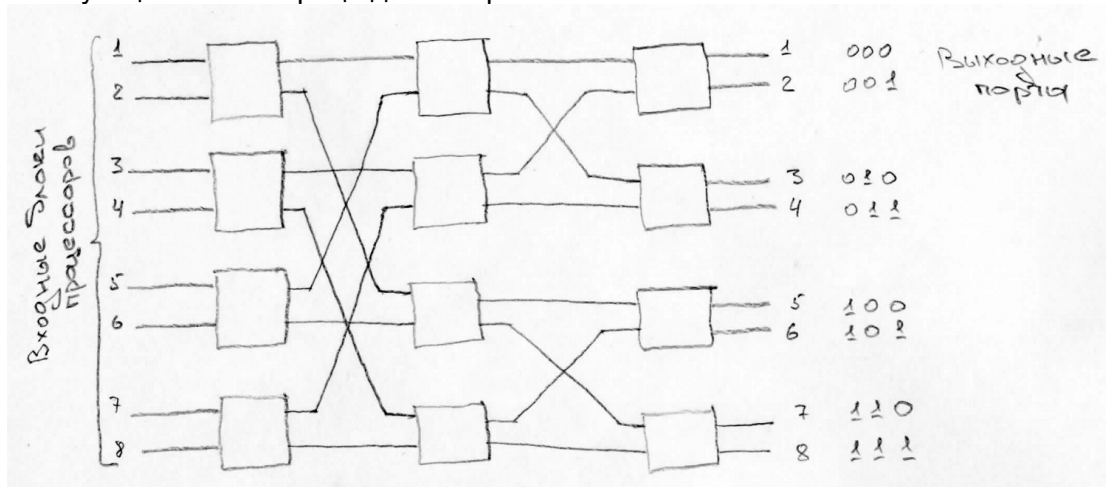
Способы построения:

1. на основе коммутационной матрицы

Коммутационная матрица - основной и наиболее быстрый способ коммутации портов. Но основной минус - ограничение по количеству портов, так как сложность схемы пропорциональна квадрату числа портов



Коммутационная матрица для 8 портов



Адрес назначения - тэг.

Коммут. вх. память на любой выходной порт.

Приходит пакет с адресом назначения (6 байт тэг) на КМ.

Адрес назначения становится в соответствие выходному порту (тэг - 3 разряда).

Эти 3 разряда с помощью таблицы Table управляют КМ.

- а. Входные блоки процессоров порта на основе таблицы адресов определяют по MAC адресам назначения № выходного порта. Эту информацию они добавляют к исходному кадру в виде спецярлыка - тэга (tag). В данном случае - это 3-х разрядный номер выходного порта.
- б. Матрица состоит из 3х уровней двоичных переключений, каждый из них соединяет свой вход и одним из 2х выходных в зависимости от значения бита тэга. Переключатели первого уровня - управляется 1ым битом тэга и

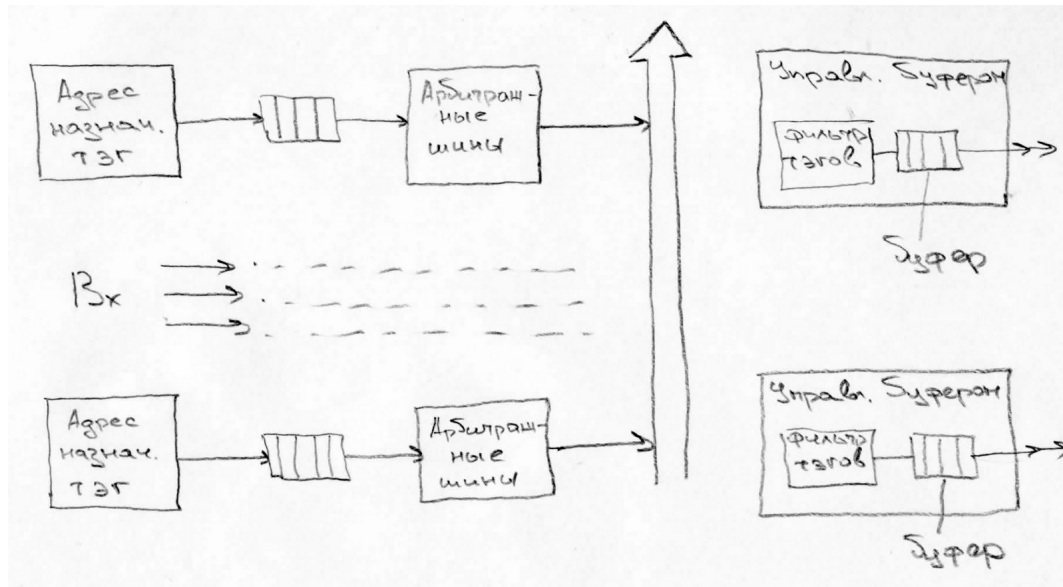
т.д.

Недостатки - отсутствует буферизация данных

Достоинства - высокая скорость коммутации

2. Коммутаторы с общей шиной

Процессоры портов связаны высокоскоростной шиной в режиме разделения времени. Производительность шины должна быть по крайней мере $\geq$ производительности всех портов коммутатора. Кадр передается по шине по несколько байт. Чтобы обеспечить псевдо параллельный режим.

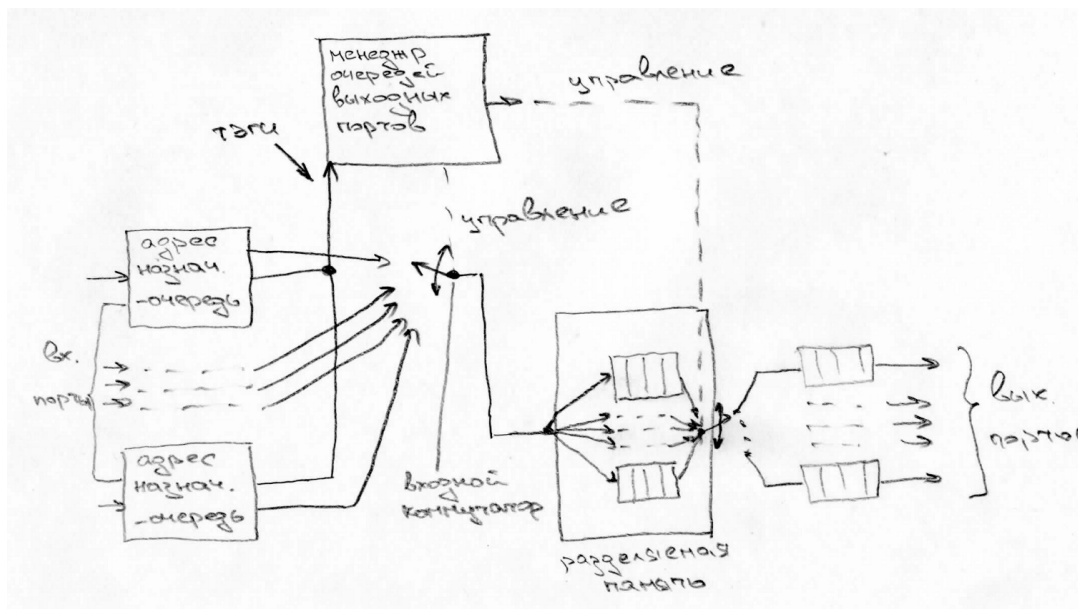


Кадры поступают на вход. Каждый разбивается на кусочки и параллельно поступает на шину первый кусочек из первого кадра, первый кусочек из второго кадра и т.д. С помощью фильтра...

Входные блоки процессора помещают в выделенные ячейки тэга, а которых указан № порта назначения; каждый выходной блок процессора имеет фильтр тэгов - выбирает тэги только для этого блока.

Недостатки - псевдо параллельная передача всех кадров по кусочкам - ничего по времени не выигрывается. идёт разбиение кадра и надо добавлять тэг к каждому кусочку, а не к каждому кадру в целом.

3. Коммутаторы с разделяемой памятью



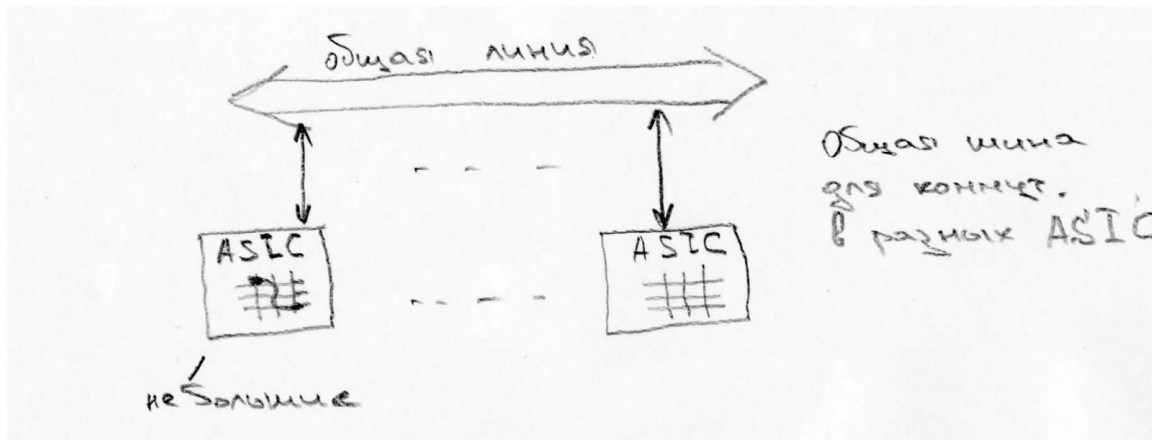
Входные порты связаны с переключаемым входом разделяемой памяти.
 Выходные порты связаны с переключаемым выходом этой памяти.
 Переключением входов и выходов управляет менеджер очередей.
 Принцип работы:

- a. входные блоки передают менеджеру запросы на запись данных в очередь того порта, который соответствует адресу назначения (тэг)
- b. менеджер по очереди переключает вход памяти к каждому входному блоку
- c. менеджер производит поочередное переключение выходов памяти к выходным блокам процессора

Достоинство - обширная буферизация

Комбинированные коммутаторы

У каждого типа КМ - свои плюсы и минусы. Поэтому часто комбинируются КМ с коммутационной матрицей и общей шиной.



Такой КМ состоит из модулей с фиксированным количеством портов (до 12), которые выполнены на ASIC. Если коммутируемые порты принадлежат одному модулю, то коммутация через ASIC. А если разным модулям, то процессоры связываются через общую шину. Скорость шины должна быть ~30-40 Гбит/с

Характеристика, влияющая на производительность КМ

Основные показатели, характеризующие производительность КМ:

1. скорость фильтрации кадра;
2. скорость продвижения кадра;
3. пропускная способность;
4. задержка передачи кадра.

Характеристики наиболее влияющие на производительность:

1. тип коммутации (на лету, с полной буферизацией);
2. размер буфера кадра;
3. производительность внутренней шины;
4. производительность процессора;
5. размер внутренней адресной таблицы.

Скорость фильтрации с продвижением кадра

Основные показатели.

Фильтрация выполняет следующие действия:

1. приём кадра в буфер;
2. просмотр адресной таблицы (для определения № выходного порта);
3. уничтожение кадра.

Порт назначения, порты источника - в одном логическом сегменте (порте).

Обычная скорость фильтрации - неблокирующая (не задерживающая передачу).

Скорость продвижения:

1. приём кадров в буфер;
2. просмотр адресной таблицы;
3. передача кадров (в найденный выходной порт).

Эта скорость исчисляется в [кадр/с]

Пропускная способность КМ

Это количество пользовательских данных в Мбит/с через все его порты. Максимальная производительность реализуется на кадрах максимальной длины.

Задержка передачи данных

Это время с момента прихода одного кадра на вход до его появления на выходном порту.

Это время включает следующие моменты:

- время на буферизацию;
- время на обработку кадра:
 - просмотр адресной таблицы;
 - принятие решения о фильтрации или продвижении;
 - получение доступа у выходному порту

Величина задержки зависит от типа КМ. На лету - 5-40мкс. С полной буферизацией - 50-200мкс.

КМ “на лету” дополнительных функций не имеют

Размер адресной таблицы

Это максимальное количество MAC-адресов, с которыми одновременно может оперировать КМ. Каждый порт хранит только те наборы адресов, с которыми он работал в последнее время.

Это значительно зависит от области применения КМ:

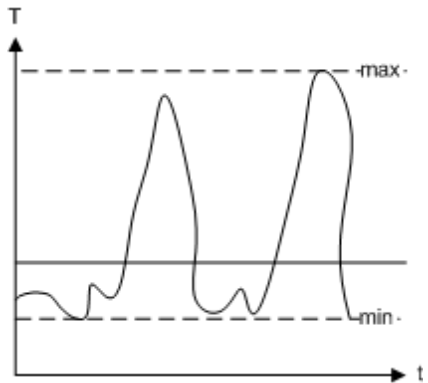
1. КМ рабочих групп (несколько адресов на входе);
2. КМ отделов (несколько сот адресов на входе);
3. КМ магистральной сети (несколько тысяч адресов на входе; 4000-8000 адресов на входе).

Частичное облегчение даёт такой приём, когда один из портов конфигурируется как магистральный, на который отправляются все кадры с неопознанным адресом. Этот порт подключен к вышестоящему КМ, который имеет более мощную адресную таблицу.

Лекция 4

Объем буфера порта

Буфер используется для временного хранения кадров когда выходной порт занят, а так же сглаживания кратковременных пульсаций трафика.



Размер буфера кадров обычно составляет десятки-сотни Кб/порт в зависимости от типа. В ответственных (магистральных) коммутаторах до нескольких Мб/порт.

Дополнительные функции коммутаторов

Коммутатор - сложное многопроцессорное вычислительное устройство, поэтому может выполнять кроме основных функций коммутатора многие дополнительные функции. Однако, не каждый коммутатор имеет эти дополнительные функции.

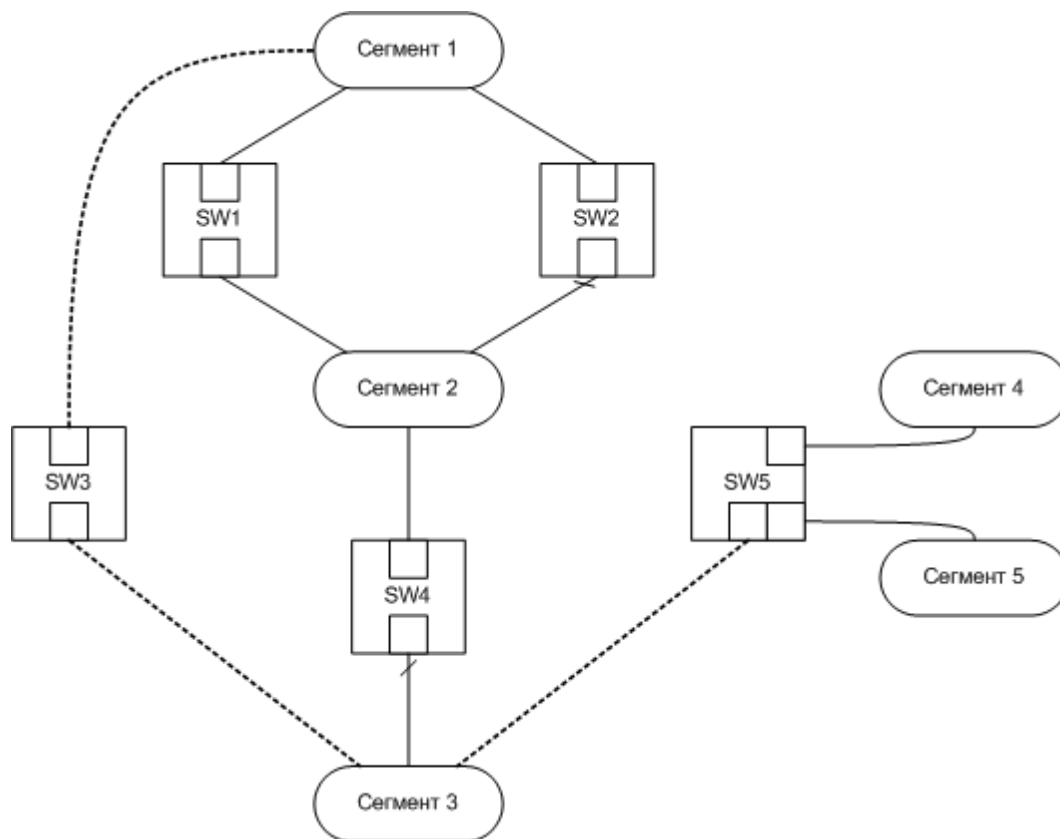
Функции:

Поддержка алгоритма STA (Spanning Tree Algorithm)

Позволяет автоматически определять древовидную конфигурацию связей обнаруживая петли и отключая их (стандарт IEEE 802.1D). Коммутаторы находят покрывающее дерево автоматически с помощью обмена служебными пакетами и строят топологию сети.

STL определяет конфигурацию сети за 3 этапа:

1. В сети определяется корневой коммутатор, от которого строится дерево. Выбор может осуществляться автоматически или вручную. Если выбор автоматический, то по минимальному MAC-адресу порта управления.
2. Для каждого коммутатора определяется его корневой порт (root port), который имеет по сети кратчайшее расстояние до корневого коммутатора.
3. Для каждого сегмента сети выбирается назначенный порт, который имеет кратчайшее расстояние до корня. После определения корневого и назначенного портов остальные порты коммутатора блокируются.

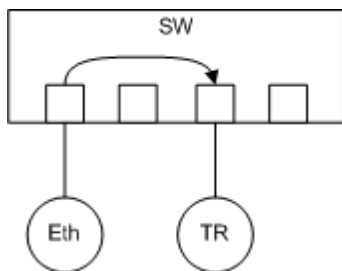


На рисунке отображена конфигурация сети с петлями и работающим STL, который заблокировал часть связей между коммутаторами (зачеркнутые линии). Топология сети на коммутаторах с резервными связями.

Процесс стабилизации сети:

1. Для автоматического определения начальной конфигурации, все коммутаторы после включения обмениваются служебными пакетами: BPDU - Bridge Protocol Data Unit.
2. Коммутаторам присваиваются идентификаторы из 8 байт: 6 байт - MAC и 2 байта - число от администратора (старшие байты - можно не выставлять, тогда они будут нулями).
3. Отрабатывают 3 этапа STL.
4. После окончания работы алгоритма STA все порты кроме корневых переводятся в заблокированное состояние.
5. Процедура передачи пакетов BPDU периодически повторяется.

Трансляция протоколов канального уровня



Трансляция – подготовка кадра для новой технологии сети (вставка полей и пересчет CRC).

Например: есть кадры Ethernet с MTU 1500 байт и есть кадры TR с размером поля данных 4000 байт. При передаче из Eth в TR всё нормально, из TR в Eth – не входит в размер, поэтому надо разбить кадр на фрагменты со своими заголовками, пронумеровать их и отправить. Но коммутатор не может этого сделать – это большой недостаток. Нужно договариваться о размере кадра заранее.

Фильтрация трафика

Многие коммутаторы позволяют администратору создавать дополнительные условия фильтрации кадров. Кроме основных (по адресной таблице), создавать пользовательские фильтры.

Самый простой фильтр – на основе MAC-адреса. Например: запретить некоторым PC по их MAC-адресам доступ к серверу. Бывают более тонкие условия, которые задаются с помощью булевых выражений .AND., .OR., .NOT.

Приоритетная обработка трафика

Коммутатор позволяет реализовать приоритезацию трафика. Это является следствием буферизации трафика. Возможно назначение приоритетов портам коммутатора через порт администратора. «+»: быстрая установка приоритетов. «-»: на порте с наивысшим приоритетом может быть PC, не нуждающийся в наивысшем приоритете.

Коммутатор ведет для каждого порта не одну, а несколько очередей, причем каждая очередь имеет свой приоритет. Обычно коммутатор конфигурируется так, что на один низкоприоритетный пакет передается 10 высокоприоритетных. Приоритезация важна при передаче мультимедийного трафика, где задержки критичны.

Способы установки приоритета трафика

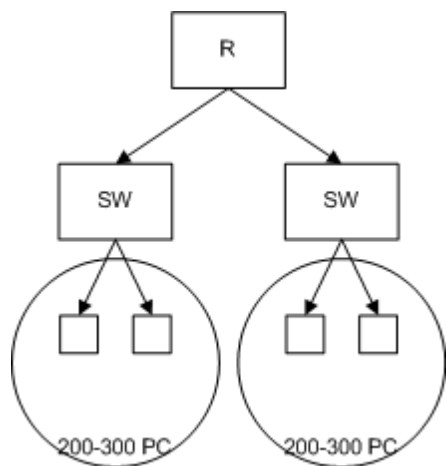
1. Приоритезация порта (приоритет имеют порты и, соответственно, все PC к ним относящиеся) – простой, но не гибкий способ (например, приоритет нужен одному PC, а получают его всех, находящиеся на заданном порте). Или же приоритезация CA – сложно реализуема, т.к. нужно менять все старые CA.

Главный изъян – не работает при каскадировании КМ, т.к. при передаче кадра теряется приоритет.

2. Приоритезация кадра (в кадр встраивается специальное поле приоритета) - очень трудоемко, зато дает возможность управления доставкой конкретного кадра. Размер поля приоритета 2 байта, но используются из них всего 3 бита.

Идеально метод не реализован (т.е. PC не выставляет приоритет своим кадрам), поэтому используется комбинация первого и второго методов: приоритет кадра выставляется на основании порта, на который он пришел, и тегируется (добавляются биты приоритета), после чего кадр отправляется выше по каскаду. Все остальные коммутаторы выше в дереве коммутации смотрят уже на поле приоритета.

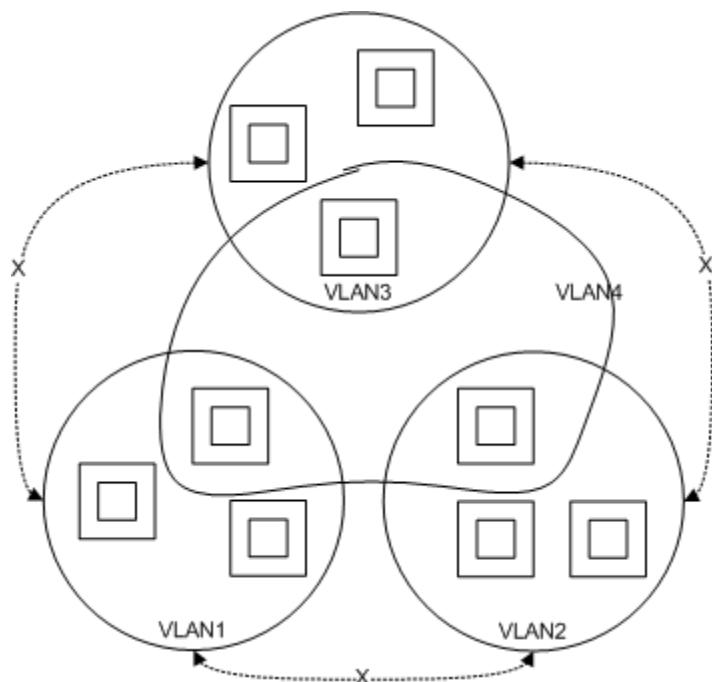
Виртуальные локальные сети (VLAN)



Количество PC для коммутатора ограничено. На одном коммутаторе можно выделить несколько сетей, разделённых логически, но не физически.

На логическом уровне взаимодействие различных коммутаторов не возможно. Порядок подключения в одну виртуальную сеть портов абсолютно не важен. Виртуальные сети - очень гибкий подход.

Виртуальной сетью называется группа узлов сети, трафик которой (в том числе широковещательный) полностью изолирован от других узлов сети на канальном уровне. Т.е. передача кадров между разными VLAN-ами невозможна без маршрутизации.



В виртуальных сетях кадры передаются по технологии коммутации, а между виртуальными сетями - только через маршрутизатор (иначе это не отдельные локальные сети).

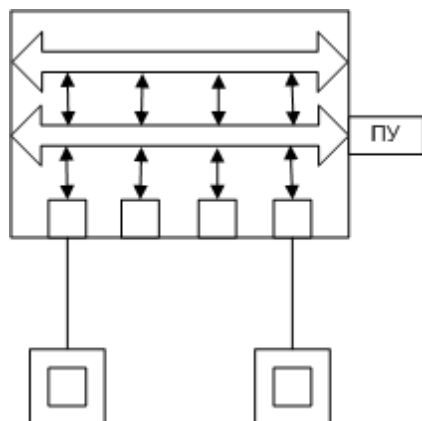
Говорят, что VLAN образуют домены широковещательного трафика – 200-300 PC.

Назначение технологии VLAN в облегчении процесса создания изолированных сетей.

Лекция 5

Сегодня считается, что любая крупная сеть должна включать в себя маршрутизаторы, иначе потоки ошибочных широковещательных кадров будут периодически затоплять сеть через прозрачные для них коммутаторы. Нужно разделить большие сети на несколько доменов широковещательного трафика.

Технология VLAN дает гибкую основу для построения крупной сети, объединенной маршрутизаторами. Коммутаторы позволяют создать полностью изолированные сегменты программным путем без физической коммутации.

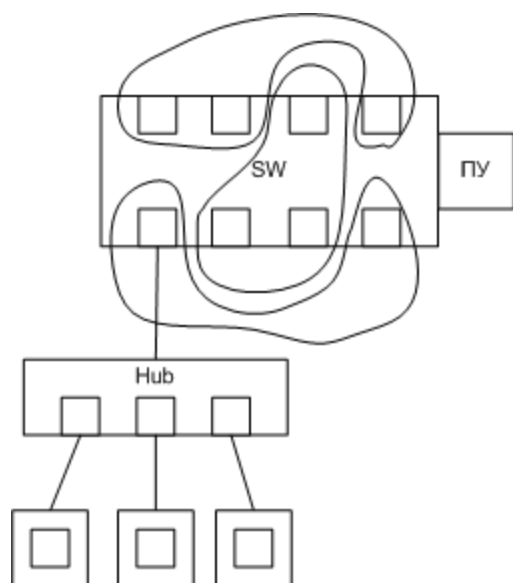


Для связи VLAN привлекается сетевой уровень, причем он может быть реализован на отдельном маршрутизаторе, но может работать и в составе ПО коммутатора, который становится комбинированным устройством - коммутатором третьего уровня (уровень модели ISO/OSI). Технология VLAN стандартизована в 1998 году: IEEE 802.1Q, которая описывает базовые правила построения VLAN.

Способы организации VLAN

1. С помощью группирования портов - есть проблемы с каскадированием (т.к. не используется тегирование кадров). Программным путем через ПУ группы портов распределяют в разные VLAN. Способ простой и популярный.

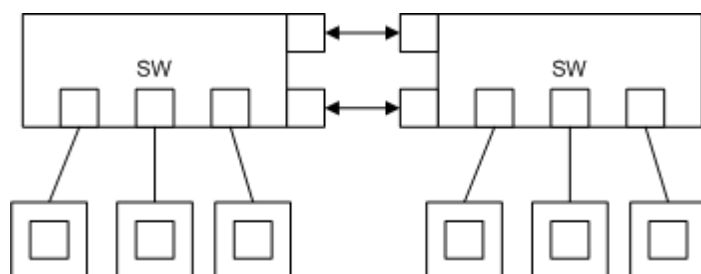
«-»: в VLAN включается не только порт, но и подключенный к нему сегмент из нескольких PC (до 30) – все они попадают в VLAN, а иногда это не нужно. Если используется режим микросегментирования (один PC – один порт SW), то проблема отпадает



2. С помощью группирования MAC-адресов. Требуется большого количества ручной работы и поэтому используется ограниченно.

«-»: много ручной работы

«-»:



При каскадном соединении коммутаторов, на каждый VLAN нужно выделить по два порта, а это затратно (делается для того, чтобы VLAN не пересекались).

3. С помощью тегирования кадров - в каждый кадр вставляется дополнительное поле о номере VLAN (тег) перед полем данных. При каскадировании коммутаторов любой коммутатор выше по уровню может посмотреть в это дополнительное поле в кадре и определить куда его можно передавать. Для хранения тега по стандарту 802.1Q используется то же двухбайтовое поле, которое используется в 802.1P. Получается что максимальный номер VLAN'a = 4096.

Тег используется при передаче только до того момента, как кадру будет предан узлу назначения. Перед передачей тег удаляется из кадра. Делается это для того, чтобы CA PC назначения не считало ошибкой поле, которое не описано в стандарте на Ethernet-кадры.

802.1Q используют в совокупности с группировкой портов, т.е. тег организует коммутатор.

4. С использованием специальных полей, характерных для кадров определенного типа, для маркировки принадлежности кадра к сети VLAN.

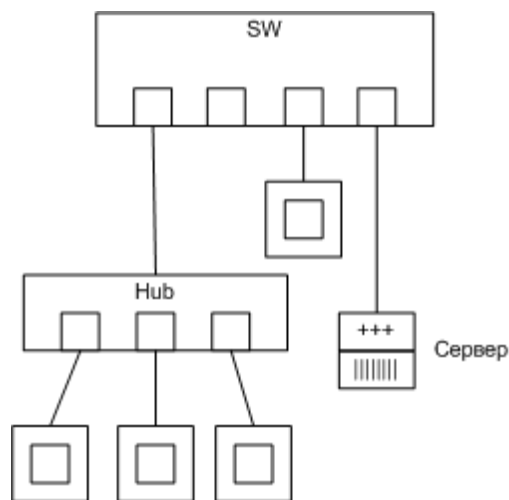
Этот способ предусматривает использование коммутатора на сетевом уровне (т.е. на уровне использования IP-адресов). При этом коммутатор должен поддерживать как сетевой, так и канальный уровень.

Скорее всего, этот способ позволяет распределить IP-адреса по всей сети даже при каскадном соединении.

Используется редко.

Варианты применения коммутатора в ЛВС

Существует устойчивая тенденция замены хабов на коммутаторы.



Есть проблема: если у всех портов одинаковая производительность и в сети есть сервер, к которому обращаются все порты, то сервер не справляется. Решение: если использовать технология FE 100 Мбит/сек, то в SW производительность все портов 100 Мбит/сек, а одного в 10 раз больше (1 Гбит/сек) для сервера).

Все структуры сети на коммутаторе сводятся к двум базовым структурам:

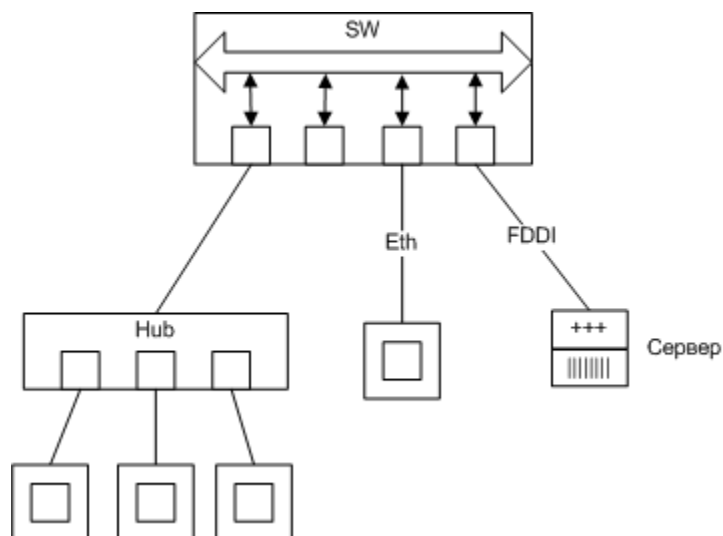
1. Стянутая в точку магистраль

2. Распределенная магистраль

На сочетании этих двух структур организуются все остальные.

Стянутая в точку магистраль (collapsed backbone)

Объединение узлов сегмента сети организуется на внутренней магистрали коммутатора.

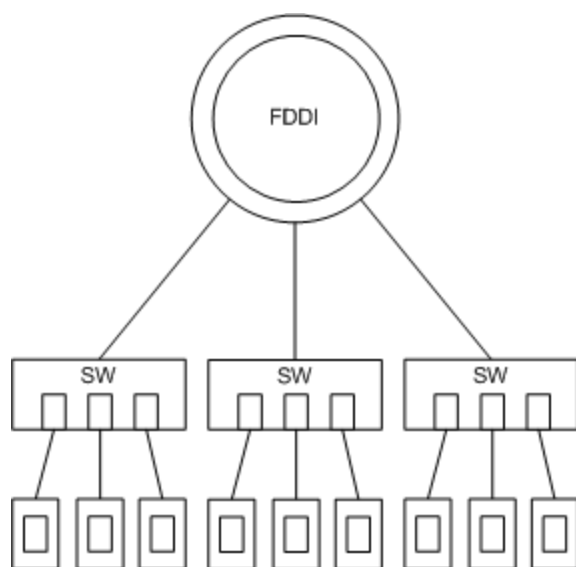


«+»: Высокая производительность магистрали.

«+»: Протокольная независимость магистрали - по ней можно передавать данные разных протоколов. Включение новой технологии в сеть требует только наличия интерфейса для ее подключения.

Распределенная магистраль

Используется в сетях больших зданий, кампусов. Строится на основе протяженной кабельной системы.



Трафик PC и отделов на каждом этаже транслируется на FDDI (не требуется фрагментация).

Лекция 6

Сетевой уровень

Маршрутизаторы

С помощью маршрутизаторов можно объединить несколько сотен сетей (локальных) в автономную систему (у них есть свой адрес).

Сетевой уровень – средство построения больших сетей

Принципы объединения сетей на основе протоколов сетевого уровня

В семиуровневой модели ISO\OSI сетевой уровень решает следующие задачи:

1. *Передача пакетов между конечными узлами в составной сети.*
2. *Выбор маршрута передачи* - наилучшего по критерию. Для критериев отводятся три бита DRT: 100 – D, 010 – R, 001 – T.

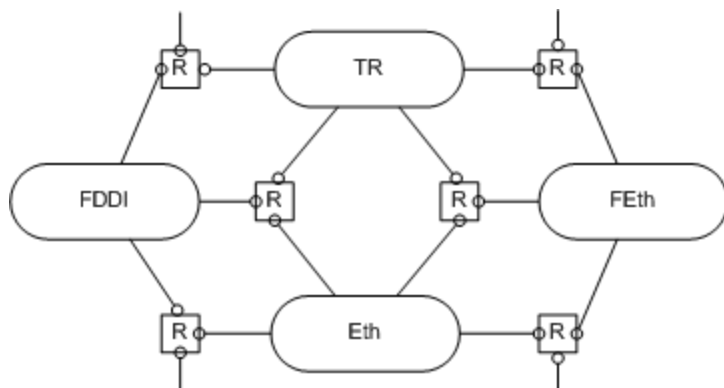
Критерии:

D (Delay) - минимальная задержка пакета (т.е., к примеру, через ЛВС с FETH) – UDP (нет проверки на ошибки). Этот критерий используется для мультимедиа.

R (Reliability) - максимальная надежность передачи (минимум искажений - минимум вероятности порчи кадра) для важных данных – TCP.

T (Traffic) - минимальная загруженность линии.

3. *Согласование разных протоколов канального уровня, использующихся в отдельных подсетях составной сети.*



IP-адрес используется на сетевом уровне – 4 байта. Основное отличие от MAC-адреса – структура. № сети|№ узла.

Порты R тоже входят в состав ЛВС, так же имеют IP и MAC. Порты R – члены сети, к которой они подключены.

R работают на IP-адресах, ЛВС работают на MAC-адресах.

4. Фрагментация кадра

У TR MTU (max transmission unit) – 0...4000 байт, у Eth – 1500 байт.

При передаче из Eth в TR всё нормально, из TR в Eth – 4000 не входит в формат 1500, поэтому надо разбить кадр TR на фрагменты 1500 со своими заголовками, пронумеровать их и отправить. Этим занимается маршрутизатор.

Сетевые протоколы реализуются программным путем на маршрутизаторах, называемых шлюзами.

Главная цель маршрутизатора – передвижения кадра по маршруту.

Нужно «нащупывание» сети и составление таблицы. По ней строятся маршруты по таблице маршрутизации.

Ограничение сетей на коммутаторах

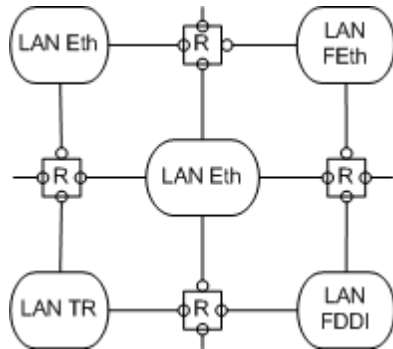
1. В топологии сети на коммутаторах должны отсутствовать петли. Пакет может доставлять только по единственному пути. Это очень плохо, т.к. нет альтернативных маршрутов.
2. Сегменты такой сети подвержены широковещательным штормам. Поэтому она ограничена в размерах – 200-300 PC.
3. Фильтрация пакетов (на втором уровне) плохая. Должна быть на более высоком уровне.
4. Негибкая одноуровневая система MAC-адресации (не структурированная, как IP-адрес).
5. Возможности трансляции протоколов ограничены тем, что они не поддерживают фрагментацию.

Таким образом, построение крупной сети требует привлечения более высокого – сетевого

– уровня.

Межсетевое взаимодействие

Сеть, рассматриваемая, как совокупность нескольких локальных сетей, называется составной сетью (интерсетью). Входящие в состав интерсети называются подсетями (subnet). Они соединяются маршрутизаторами. В составную сеть могут входить подсети разных технологий: Eth, FEth, TR, FDDI, AnyLAN.



Лекция 7

IP-адрес содержит 4 байта, никак не связанные с MAC-адресом (6 байт). MAC-адреса в подсетях называются локальными адресами. IP-адреса используются для связи отдельных подсетей и работают на маршрутизаторах.

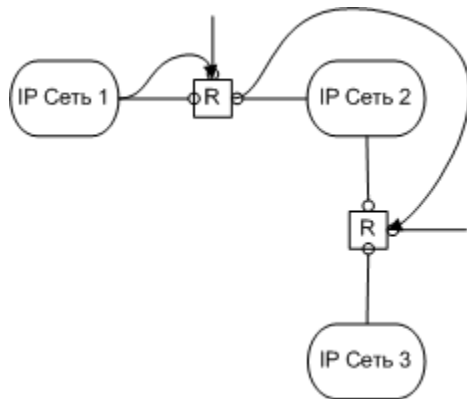


Таблица маршрутизации строится специальным протоколом.

II - канальный | III - сеансовый

|MAC-источн.|MAC-назнач.|IP-источн.|IP-назнач.| - кадр

1. Посмотреть в кадре IP назначения,
2. Посмотреть в таблице маршрутизации, какой хоп нужно сделать.
3. Для передачи данных в локальной сети используются MAC-адрес, но в таблице маршрутизации хранится только IP. Чтобы узнать MAC-адрес, маршрутизатор выполняет специальный ARP-запрос.

ARP – Address Resolution Protocol. Таблица маршрутизации работает на сетевом уровне.

ARP-запросы широковещательны.

4. Заполняет MAC-адрес и готовится кадр.

IP	MAC
...	...
...	...

Один маршрутизатор ранил не все хопы всей глобальной сети, т.к. в этом случае он будет работать очень медленно – хранится только ближайшее окружение.

Проблема: кадр может ходить кругами. Для этого в IP-адресации есть поле TTL (Time To Live) - максимальное количество хопов, которое может пройти кадр до станции назначения, время жизни кадра. При переходе кадра число хопов в кадре уменьшается на единицу.

Но в IPv6, где IP-адрес шестнадцатибайтный, вернулись к идее с вхождением MAC-адреса.

IP-адрес назначения – путеводитель, не изменяется.

IP-адрес источника – переписывается каждый раз.

MAC-заголовок – постоянно переписывается.

Кроме номера подсети, заголовок сетевого уровня содержит:

1. Номер фрагмента пакета – для сборки пакета (фрагментация происходит на сетевом уровне).
2. Время жизни пакета – для уничтожения заблудившихся пакетов.
3. Критерий выбора маршрута – D, R, T.

Когда несколько подсетей организуют совместную транспортную службу, такой режим называется межсетевым взаимодействием.

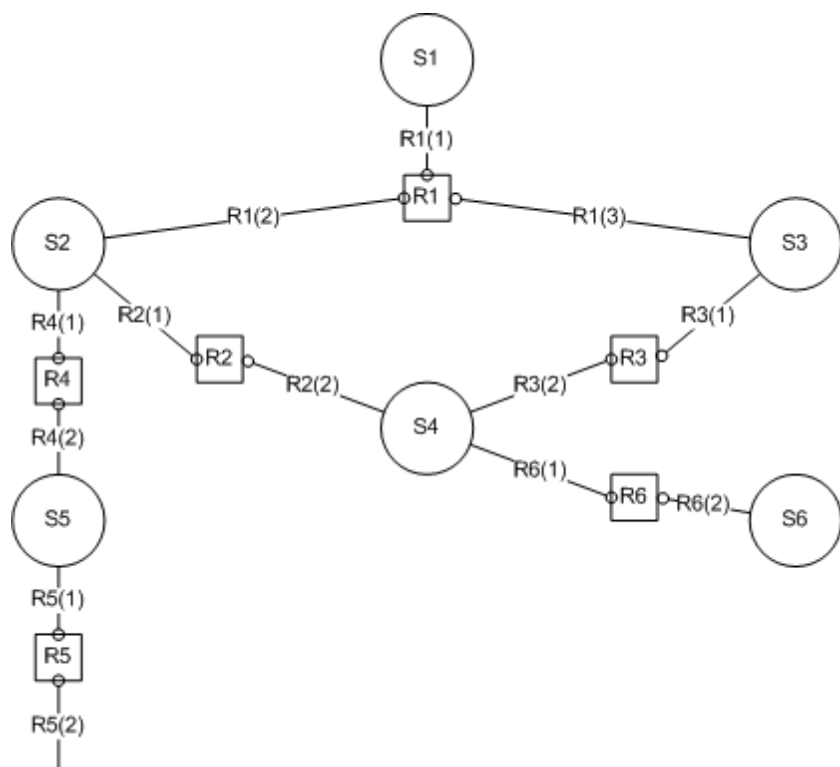
Принципы маршрутизации

Каждый порт маршрутизатора выступает как отдельный узел сети, в которую он включен, т.к. он имеет свой собственный IP и MAC. В простейшем случае - один порт на одну подсеть.

Помимо адресов в сетях, к которым он подключен, маршрутизатор также имеет собственные IP и MAC для управления (например под SNMP).

В сетях на маршрутизаторах всегда имеется несколько альтернативных маршрутов для доставки пакетов.

Маршрут - это последовательность маршрутизаторов, которую должен пройти пакет для доставки.



Таблицу адресов имеет каждый маршрутизатор (R). Возьмём в качестве примера таблицу маршрутизации R4 (с рисунка)

№ сети назн.	IP-адрес след. МШ	IP-адрес вых. порта	Расст. до сети назн.
S1	R1(2)	R4(1)	1
S2	R4(1)	R4(1)	0
S3	R1(1)	R4(1)	1
S4	R2(1)	R4(1)	1
S5	R4(2)	R4(2)	0
S6	R2(1)	R4(2)	2
default			

В «№ сети назначения» указываются ближайшие сети (не все).

Может существовать несколько маршрутов из-за критериев или даже по одному критерию несколько маршрутов.

Строку «default» заносит администратор сети.

Если нет назначения, то направляется в «default». Когда на маршрутизатор поступает новый пакет, из него выделяется IP-адрес сети назначения, который последовательно сравнивается с № сетей в таблице маршрутизации и в случае, если в какой-то строке произошло совпадение, то выполняется хоп по этой строке.

На практике число строк в таблице ограничивают – указывают только ближайшие сети и на тупиковых маршрутах, остальные направления указываются строкой «default», которая

вносится администратором.

Лекция 8

Таблица маршрутизации

2 этапа маршрутизации:

1. Подготовка таблицы маршрутизации
2. Маршрутизация пакетов на основании таблицы.

Узлы-отправители также содержат информацию, куда направлять пакет вне сети (в другую сеть). Она содержится в виде IP-адреса шлюза по умолчанию.

Протоколы маршрутизации

Таблица маршрутизации в основной своей части производится автоматически. Маршрутизаторы обмениваются информацией о топологии сети. Этот обмен выполняется с использованием специализированных протоколов:.

RIP - Routing Internet Protocol

OSPF - Open Shortest Path First

IS-IS - Intermediate System to Intermediate System

BGP – Board Gateway Protocol

Пакет продвигается другими сетевыми протоколами:

IP – Internet Protocol

IPX – Internetwork Packet Exchange фирмы Novell.

При обмене маршрутной информацией пакеты содержат информацию о подключенных к маршрутизатору сетях и соединяющих их линиях (оптика, медь). В результате сбора этой информации маршрутизатор создает у себя карту сети, на основании которой впоследствии строится таблица маршрутизации.

При определении маршрута существует 2 способа:

1. Указывается только следующий (ближайший) маршрутизатор, и окончательный маршрут складывается в результате работы всех маршрутизаторов по этому маршруту. Такие маршрутизаторы называются одношаговые (используются наиболее часто).
2. Маршрутизация от источника (многошаговая) - Source Routing. Узел-источник задает в передаваемом пакете полный маршрут через все промежуточные маршрутизаторы - не нужно строить таблиц, весь маршрут прописан в передаваемом пакете. «-»: очень большая нагрузка на узел-отправитель.

Одношаговые алгоритмы по способу формирования таблицы маршрутизации делятся на:

1. Алгоритм статической (фиксированной) маршрутизации – администратор с помощью утилите route записывает таблицу маршрутизации. Возможен только в простых сетях

2. Алгоритм простой маршрутизации - таблица маршрутизатора либо вовсе не используется, либо строится без протоколов маршрутизации.

Типы простой маршрутизации:

- 1) Случайная – пакет отправляется в первом попавшемся направлении (но не назад). Иногда можно (1% таких маршрутизаторов в сети. Если больше – сеть не работает)
- 2) Лавинная - пакет ширококестельно рассылается по всем портам кроме исходного. Какой-то порт сработает и отправит пакет в нужном направлении
- 3) Маршрутизация по предыдущему опыту - таблица маршрутизации строится по принципу коммутатора: самообучением.

3. Динамическая (адаптивная) маршрутизация - построение и обновление таблиц с помощью протоколов маршрутизации (RIP и т.д.). В этом случае записи в таблице маршрутизации имеют время жизни (TTL).

В последнее время в сети организуются т.н. серверы маршрутов. Они собирают маршрутную информацию и по запросам маршрутизаторов отсылают ее им.

Адаптивная маршрутизация делится на 2 группы:

1. Дистанционно-векторный алгоритм (Distance Vector Algorithm - DVA) - каждый маршрутизатор периодически ширококестельно отсылает по сети вектор, компоненты которого - расстояния от данного маршрутизатора до всех известных ему сетей в хопх. Так работает протокол RIP. «-»: каждый раз при обновлении RIP пересматривает всю сеть.
2. Алгоритм состояния связей (Link State Algorithm - LSA) - ширококестельные рассылки только при изменениях состояний связей или появлении новых. Маршрутизаторы периодически обмениваются через сеть короткими пакетами «Hello». Если у того, кто получил такой пакет, с момента последнего привет ничего не изменилось, он отвечает «Hello», если были изменения, то он отправляет только эти изменения.

Функции маршрутизатора

Основная задача – продвижение пакетов по выданному адресом назначения и таблице маршруту.

В соответствии с 7миуровневой моделью, функции маршрутизатора разделяются на три группы (уровня):

1. *Уровень интерфейса* - как и любое другое сетевое устройство, маршрутизатор должен иметь физический сетевой интерфейс: уровни сигнала, тип кодирования, метод доступа к разделяемому КС. Маршрутизатор должен иметь набор портов, соответствующих подключаемым к нему сетям. Каждый порт должен реализовать набор функций физического и канального уровней и должен иметь собственный аппаратный и сетевой адреса (MAC и IP). Перечень физической информации – его важнейшая функция.

2. *Уровень сетевого протокола* - извлекает свой (сетевой) заголовок из принятого кадра и выполняет следующие действия:

- 1) Проверяет CRC – если не верно, пакет отбрасывается. Отправителю отсылается сообщение о том, что пакет уничтожен (SNMP);
- 2) Проверяет TTL – если истекло, пакет отбрасывается. Отправителю отсылается сообщение о том, что пакет уничтожен (SNMP);
- 3) На сетевом уровне опционально может быть организована фильтрация трафика – маршрутизатор может анализировать пакет. Пример – запретить все пакеты, кроме пакетов данной сети. Маршрутизатор может анализировать пакеты транспортного уровня, фильтровать пакеты служб и т.д.
- 4) Если на вход пакеты поступают слишком быстро, то образуется очередь. Она может обслуживаться по следующим алгоритмам:

– FIFO (First In First Out).

– Random Early Detection (RED) – случайное раннее обнаружение. обслуживание по правилу FIFO, но по достижении некоторого значения новые пакеты отбрасываются.

– Приоритетный разбор пакетов - различные варианты приоритетов.

Основная задача - определение маршрута осуществляется по номеру сети назначения. Если в таблице строка с № данной сети отсутствует, используется «default».

5) Заполняются заголовка канального уровня (MAC-адрес) перед передачей. Выполняется каждый раз при выполнении нового хопа. Заголовок каждый раз переписывается. Для определения MAC-адреса следующего маршрутизатора используется протокол ARP. Запрос ARP выполняется однократно, а результат заносится в кэш-таблицу.

3. Уровень протоколов маршрутизации.

Сетевые протоколы используют таблицу маршрутизации, но построением её не занимаются – этим занимаются другие протоколы (RIP и т.д.).

Реализация сетевого взаимодействия средствами TCP/IP

На практике работает четырёхуровневая модель.

Стек TCP/IP самый популярный, для работы с сетью. В нем определены четыре уровня:

1. Прикладной;
2. Транспортный;
3. Межсетевого взаимодействия;
4. Сетевых интерфейсов.

-Уровень межсетевого взаимодействия-

Реализует передачу пакетов дэйтagramмным способом.

Основной протокол - IP. Не гарантирует доставку пакетов. К этому уровню так же относятся протоколы маршрутизации RIP, IS-IS, протокол межсетевых управляющий

сообщений - ICMP (Internet Command Message Protocol) - для обмена информацией об ошибках между маршрутизатором и узлом источника: невозможность доставки пакета, превышение TTL, изменение маршрута пересылки, аномальное увеличение размера пакета.

Лекция 9

Основной уровень (транспортный)

Отвечает за надежную доставку сообщений. Уровень межсетевого взаимодействия не устанавливает соединений и не дает гарантии, что все пакеты будут доставлены целыми и вообще будут доставлены. Эту задачу обеспечивает основной уровень – транспортный.

На этом уровне работают протоколы:

TCP (Transmission Control Protocol) – обеспечивает надежную доставку сообщений между прикладными процессами (портами). Позволяет без ошибок передать поток байт от источника. Действия TCP:

1. TCP делит сообщения на сегменты. Сегменты обрастают заголовками и становятся кадрами.
2. Передаёт на сетевой уровень для транспортировки.
3. После доставки сегментов средствами уровня межсетевого взаимодействия, TCP на приемном конце снова собирает их в общее сообщение и передает на верхний уровень.

UDP – User Datagram Protocol.

UDP (User Datagram Protocol) - выполняет те же действия, но не обеспечивает надежность - не делает запрос на контроль доставки служебными кадрами. Передаются сообщения, не терпящие задержек.

Прикладной уровень

Объединяет все службы для пользовательских приложений. За долгие годы существования в TCP/IP накопилось достаточное количество приложений (портов). Протоколы прикладного уровня. Занимаются каждым приложением и не интересуются способом доставки. Telnet, FTP, DNS, SNMP, HTTP.

Уровень сетевых интерфейсов

Сеть с TCP/IP должна иметь средства включения в себя любой сети с любой технологией передачи.

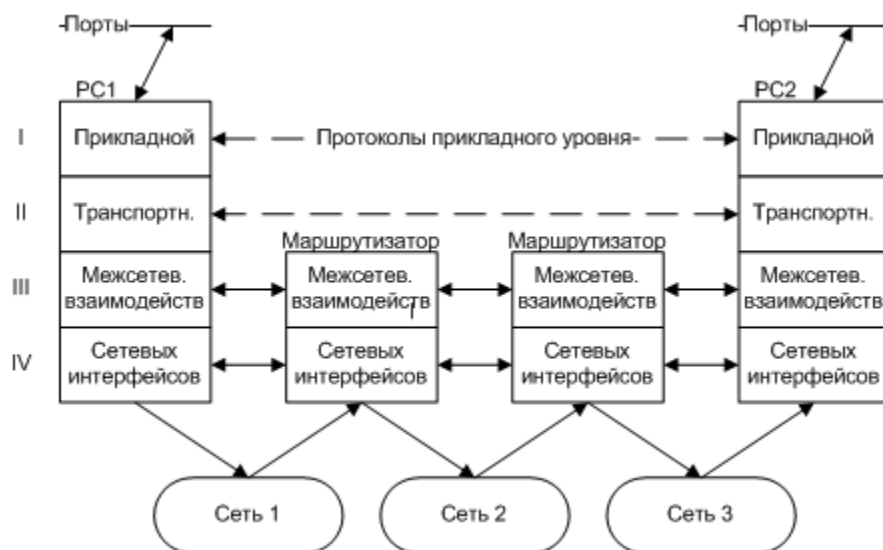
Уровень сетевых интерфейсов должен поддерживать все популярные стандарты физических и канальных уровней. Ethernet, FE, TR, FDDI, ArcNET, GE, 100VG-AmgLAN, SLIP (протокол глобальных сетей\межсетевых соединений – для соединения отдалённых автономных сетей), PPP (точка-точка), технологии глобальных сетей FrameRelay, X.25, ISDN, ATM.

Соответствие уровней стека TCP/IP 7миуровневой модели ISO\OSI

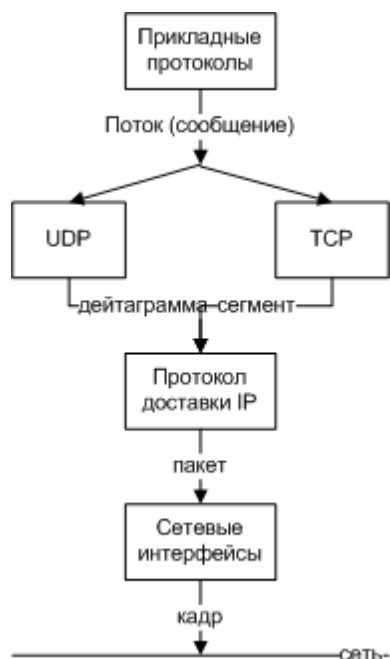
ISO/OSI	Протоколы	TCP/IP
7,6	SNMP, FTP, Telnet, TFTP, Gopher	I
5,4	TCP, UDP	II
3	IP, ICMP, RIP, OSPF, IS-IS, ARP	III
2,1	Ethernet, TR, FE, GE, X.25, FDDI...	IV

I, II, III, IV – логичные и понятные уровни. I, II – сетезависимые, III, IV – сетезависимые (при смене технологии сети меняются протоколы).

У Маршрутизатора только уровни межсетевого взаимодействия и сетевых интерфейсов.



Каждый уровень TCP/IP оперирует с определённой единицей данных. Поэтому существует устоявшаяся терминология.



Типы адресов стека TCP/IP

1. Локальные (аппаратные), MAC-адреса – 6 байт;
2. Сетевые, IP-адреса. IPv4- 4 байта, IPv6 – 16 байт;

[MAC-источн.|MAC-назнач.|IP-источн.|IP-назнач.] - кадр IPv4

3. Символьные доменные имена – это не адреса, а обозначения. Попытка представить IP-адрес в формате, понятно человеку.

Лекция 10

IP-адрес

В оконечный узел может входить несколько сетей, следовательно содержит несколько сетевых карт. Отдельное сетевое соединение характеризует IP-адрес.

Символы доменного адреса строятся по иерархическому принципу и составляющие разделяются точкой по принципу *имя узла.имя группы.имя большой группы*

По географическому принципу: .ru, .uk, .us

По деловому принципу: .com, .edu, .gov, .org, .net

Существует соответствие между IP-адресом и доменным именем. DNS (Domain Name System) – система доменных имен.

В IPv6 адрес записывается в виде тетрад.

Принципы разделения сетей на адрес сети и адрес хоста:

1. Классовый – раздача адресов (граница в строго по байтам).
2. На основе маски – структуризация (граница может быть различной).

Классы IP-адресов

1. Класс А: 01. . . – Номеру сети соответствует первый байт IP-адреса. 128 сетей, в каждой сети 16 106 хостов. Группы очень крупные – для самых крупных провайдеров.

байты:	1...	№ сети		№ узла	
	1	2	3	4	

2. Класс В: 10. . . – Номеру сети соответствуют 2 байта. Сетей 16 103, в каждой сети 65534 хоста.

байты:	10...	№ сети		№ узла	
	1	2	3	4	

3. Класс С: 110. . . – Номеру сети соответствуют 3 байта. Сетей 2 106, в каждой сети 254 хоста. Много мелких групп.

	110...		№ сети		№ узла
байты:	1	2	3	4	

4. Класс D: 1110. . . – Весь адрес является адресом группы Multicast. Пользователи подписываются на этот адрес для получения рассылки.

	1110...	адрес группы	Multi	cast
байты:	1	2	3	4

5. Класс E: 11110. . . – зарезервирован. Но в силу вступает IPv6, где IP-адресов гораздо больше (не 4 байта, а 16), поэтому зарезервированные адреса класса E уже не понадобятся.

	11110...		зар	езерви	ван
байты:	1	2	3	4	

Целая группа адресов выбыла из применения. Групп 228 ~256*106.

Специальные IP-адреса

1. Адрес 0.0.0.0 – адрес узла, сгенерировавшего пакет. Используется только в кадрах протокола ICMP(Internet Control Message Protocol). Если в адресе назначения пакета стоит 0.0.0.0, то адрес отправляется назад по маршруту (к отправителю).

2. Поле «№ сети» 000...0 + нормальный № узла – узел назначения находится в той же сети, что и отправитель.

3. Адрес назначения 255.255.255.255 – пакет отправляется всем узлам локальной сети (широковещательный пакет). Limited broadcast – ограниченная широковещательная рассылка.

4. Нормальный «№ сети» + «№ узла» 111...1 – широковещательный пакет в удаленную сеть.

5. 127.x.x.x – loopback адрес сети. Предназначены для тестирования программ и процессов в пределах одной машины. Когда PC посылает пакет на адрес 127.0.0.1 (например), то образуется «петля» – данные не передаются по сети, а возвращаются на верхний уровень.

6. Адрес класса D 224.x.x.x – широковещательная рассылка. В протоколе IP нет понятия абсолютного широковещания (как в локальных сетях). Широковещание распространяется только на свою сеть или на ту, адрес которой указан в кадре.

Такой пакет должен быть разослан всем подписчикам. Один PC обрабатывается маршрутизатором особым образом (т.е. кадры отправляются только подписчикам). Связь «1»-«много». PC, желающие передать кадры, организуют рассылку с помощью протокола IGMP (Internet Group Management Protocol), сообщаящего сети о создании новой группы. Маршрутизатор распространяет эту информацию в сетях (широковещательно). PC, желающие получать эту рассылку заявляют о подписке.

Лекция 11

Маска в IP-адресации

Маска это число. Кол-во единиц в левой части определяет границу номера сети. Номер сети получается путем умножения (логического «И») IP-адреса и маски.

IP-адрес:

129.64.134.5

10000001.01000000.10000110.00000101

Маска

11111111. 11111111. 11000000.00000000

111...1 – определяет границу сети

Таким образом «№ сети» = 129.64.128.0, «№ узла»=0.0.6.5

Порядок распределения IP-адресов

Номера сетей назначаются либо централизованно, если сеть является частью Internet, либо произвольно, если сеть работает автономно. Номера узлов и в том и в другом случае администратор волен назначать по своему усмотрению, не выходя, разумеется, из разрешенного для этого класса сети диапазона.

Координирующую роль в централизованном распределении IP-адресов до некоторого времени играла организация InterNIC, однако с ростом сети задача распределения адресов стала слишком сложной, и InterNIC делегировала часть своих функций другим организациям и крупным поставщикам услуг Internet.

Уже сравнительно давно наблюдается дефицит IP-адресов. Очень трудно получить адрес класса В и практически невозможно стать обладателем адреса класса А. При этом надо отметить, что дефицит обусловлен не только ростом сетей, но и тем, что имеющееся множество IP-адресов используется нерационально. Очень часто владельцы сети класса С расходуют лишь небольшую часть из имеющихся у них 254 адресов.

Если же некоторая IP-сеть создана для работы в «автономном режиме», без связи с Internet, тогда администратор этой сети волен назначить ей произвольно выбранный номер. Но и в этой ситуации для того, чтобы избежать каких-либо коллизий, в стандартах Internet определено несколько диапазонов адресов, рекомендуемых для локального использования. Эти адреса не обрабатываются маршрутизаторами Internet ни при каких условиях. Адреса, зарезервированные для локальных целей, выбраны из разных классов:

в классе А - это сеть 10.0.0.0,

в классе В - это диапазон из 16 номеров сетей 172.16.0.0-172.31.0.0,

в классе С - это диапазон из 255 сетей - 192.168.0.0-192.168.255.0.

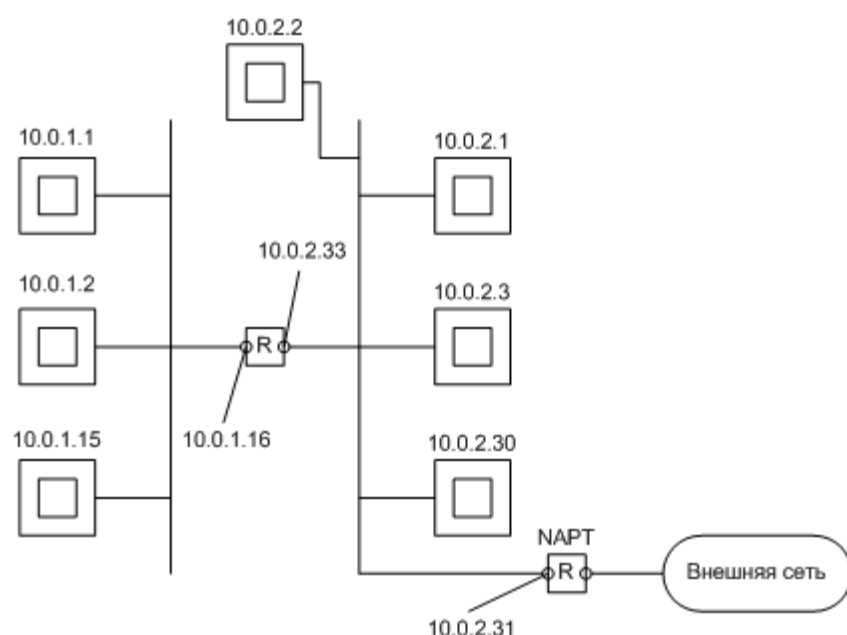
Для смягчения проблемы дефицита адресов разработчики стека TCP/IP предлагают разные подходы.

1. Переход на новую версию IPv6, в которой резко расширяется адресное пространство за счет использования 16-байтных адресов. Однако и текущая версия IPv4 поддерживает некоторые технологии, направленные на более экономное расходование IP-адресов.

2. Технология масок и ее развитие - технология бесклассовой междоменной маршрутизации (Classless Inter-Domain Routing, CIDR). Технология CIDR отказывается от традиционной концепции деления адресов протокола IP на классы, что позволяет получать в пользование столько адресов, сколько реально необходимо. Благодаря CIDR поставщик услуг получает возможность «нарезать» блоки из выделенного ему адресного пространства в точном соответствии с требованиями каждого клиента, при этом у него остается пространство для маневра на случай его будущего роста.

3. Трансляция адресов (Network Address Translator, NAT). Узлам внутренней сети адреса назначаются произвольно (естественно, в соответствии с общими правилами, определенными в стандарте), так, как будто эта сеть работает автономно. Внутренняя сеть соединяется с Internet через некоторое промежуточное устройство (маршрутизатор, межсетевой экран). Это промежуточное устройство получает в свое распоряжение некоторое количество внешних «нормальных» IP-адресов, согласованных с поставщиком услуг или другой организацией, распределяющей IP-адреса. Промежуточное устройство способно преобразовывать внутренние адреса во внешние, используя для этого некие таблицы соответствия. Для внешних пользователей все многочисленные узлы внутренней сети выступают под несколькими внешними IP-адресами. При получении внешнего запроса это устройство анализирует его содержимое и при необходимости пересылает его во внутреннюю сеть, заменяя IP-адрес на внутренний адрес этого узла. Процедура трансляции адресов определена в RFC 1631.

Технология NAT



Внешняя сеть		Внутренняя сеть	
IP	Порт	IP	Порт
10.0.1.1	1220	121.32.28.5	3451
10.0.1.3	1232	121.32.28.6	3452
10.0.1.15	1220	121.32.28.7	3453
10.0.1.16	1245	121.32.28.8	3460

Всего 65536 портов, следовательно, на один IP-адрес можно сделать 65536 соответствий (подсетей). PC из внутренней сети не всегда во внешней сети.

Двойная трансляция

Когда в качестве внутреннего адреса используют белый адрес, то может быть 2 случая:

1. Белые адреса назначены произвольно без рекомендации;
2. Сменили провайдера, но его белые адреса желаем оставить у себя.

Тогда при выходе во внешнюю сеть – двойная трансляция:

PC запрашивает DNS-сервер, который в ответе сообщает серый адрес из рекомендованного диапазона. Теперь с этим адресом кадр поступает на NAPT. На нём подмена на внешний белый адрес.

Лекция 12

Автоматизация процесса назначения IP-адресов

Протокол Dynamic Host Configuration Protocol (DHCP) автоматизирует процесс назначения IP-адресов и поддерживает способ автоматического динамического распределения адресов, а также более простые способы ручного и автоматического статического назначения адресов. Протокол DHCP работает в соответствии с моделью клиент-сервер:

- 1) Компьютер, являющийся DHCP-клиентом, посылает в сеть широковещательный запрос на получение IP-адреса.
- 2) DHCP-сервер откликается и посылает сообщение-ответ, содержащее IP-адрес. Предполагается, что DHCP-клиент и DHCP-сервер находятся в одной IP-сети.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, называемое временем аренды (lease duration), что дает возможность впоследствии повторно использовать этот IP-адрес для назначения другому компьютеру. Динамическое разделение адресов позволяет строить IP-сеть, количество узлов в которой превышает количество имеющихся в распоряжении администратора IP-адресов.

В ручной процедуре назначения статических адресов активное участие принимает администратор, который предоставляет DHCP - серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. DHCP-сервер, пользуясь этой информацией, всегда выдает определенному клиенту назначенный администратором адрес.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес из пула наличных IP-адресов без вмешательства оператора. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Адрес дается клиенту из пула в постоянное пользование, то есть с неограниченным сроком аренды. Между идентификатором клиента и его IP-адресом существует постоянное соответствие, установленное в момент первого назначения DHCP-сервером IP-адреса клиенту.

DHCP-сервер может назначить клиенту не только IP-адрес клиента, но и другие параметры стека TCP/IP, необходимые для его эффективной работы:

- маску,
- IP-адрес маршрутизатора по умолчанию,
- IP-адрес сервера DNS,
- доменное имя компьютера.

Отображение IP-адреса на локальные адреса

При выполнении последовательного хопа, необходимо знать MAC-адрес следующего маршрутизатора. Из таблицы маршрутизации известен его IP-адрес, поэтому маршрутизатор широковещательно (т.к. нет адреса назначения) запрашивает у промежуточной сети MAC-адрес, указав в запросе его IP-адрес.

Для определения локального адреса по IP-адресу используется протокол разрешения адреса (Address Resolution Protocol, ARP). Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети:

1. Протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети. Получает MAC-адрес автоматически.
2. Протокол глобальной сети (X.25, frame relay), как правило не поддерживающий широковещательный доступ. Администратор вручную устанавливает соответствие MAC-адреса и IP-адреса.



Существует также протокол, решающий обратную задачу - нахождение IP-адреса по известному локальному адресу. Он называется реверсивным ARP (Reverse Address Resolution Protocol, RARP) и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

Работа протокола ARP начинается с просмотра так называемой ARP-таблицы. Каждая строка таблицы устанавливает соответствие между IP-адресом и MAC - адресом. Для каждой сети, подключенной к сетевому адаптеру компьютера или к порту маршрутизатора, строится отдельная ARP-таблица.

IP-адрес	MAC - адрес	Тип записи
194.85.135.75	008048EB7E60	Динамический
194.85.135.70	08005A21A722	Динамический
194.85.60.21	008048EB7567	Статический

Поле «Тип записи» может содержать одно из двух значений - «динамический» или «статический». Статические записи создаются вручную с помощью утилиты `arp` и не имеют срока устаревания, точнее, они существуют до тех пор, пока компьютер или маршрутизатор не будут выключены. Динамические же записи создаются модулем протокола ARP, использующим широковещательные возможности локальных сетевых технологий. Динамические записи должны периодически обновляться. Если запись не обновлялась в течение определенного времени (порядка нескольких минут), то она исключается из таблицы. Таким образом, в ARP - таблице содержатся записи не обо всех узлах сети, а только о тех, которые активно участвуют в сетевых операциях. Поскольку такой способ хранения информации называют кэшированием, ARP-таблицы иногда называют ARP-кэш.

В последнее время наметилась тенденция автоматизации работы протокола ARP и в глобальных сетях. Для этой цели среди всех маршрутизаторов, подключенных к какой-либо глобальной сети, выделяется специальный маршрутизатор, который ведет ARP-таблицу для всех остальных узлов и маршрутизаторов этой сети. При таком централизованном подходе для всех узлов и маршрутизаторов вручную нужно задать только IP-адрес и локальный адрес выделенного маршрутизатора. Затем каждый узел и маршрутизатор регистрирует свои адреса в выделенном маршрутизаторе, а при необходимости установления соответствия между IP-адресом и локальным адресом узел обращается к выделенному маршрутизатору с запросом и автоматически получает ответ без участия администратора. Работающий таким образом маршрутизатор называют ARP-сервером.

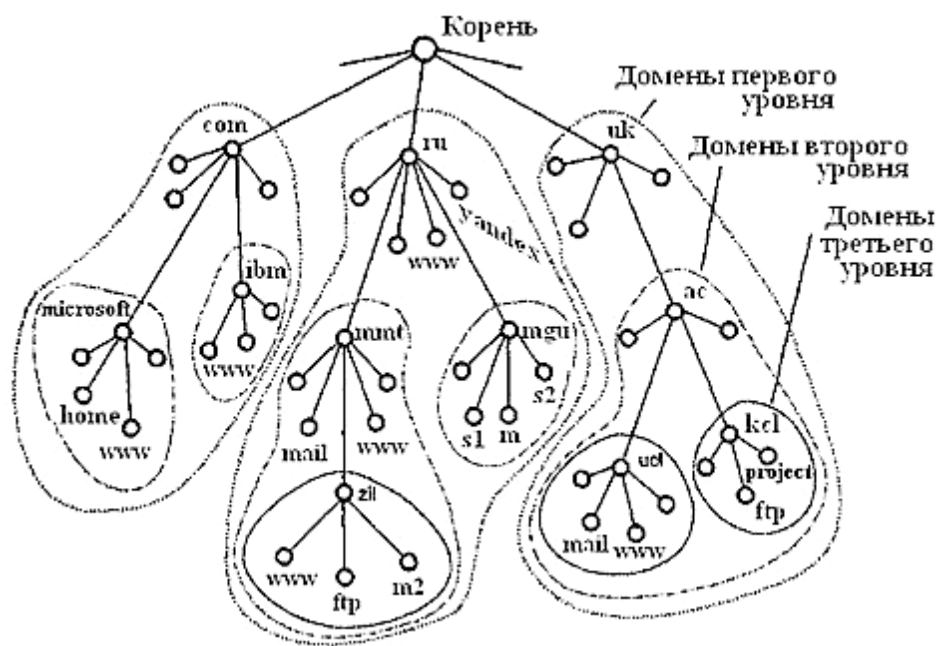
Итак, после того как модуль IP обратился к модулю ARP с запросом на разрешение адреса, происходит поиск в ARP-таблице указанного в запросе IP-адреса. Если таковой адрес в ARP-таблице отсутствует, то исходящий IP-пакет, для которого нужно было определить локальный адрес, ставится в очередь. Далее протокол ARP формирует свой запрос (ARP-запрос), вкладывает его в кадр протокола канального уровня и рассылает запрос широковещательно.

Отображение доменных имен

Для идентификации компьютеров аппаратное и программное обеспечение в сетях TCP/IP полагается на IP-адреса, поэтому для доступа к сетевому ресурсу в параметрах программы вполне достаточно указать IP-адрес, чтобы программа правильно поняла, к какому хосту ей нужно обратиться. Например, команда ftp://192.45.66.17 будет устанавливать сеанс связи с нужным ftp-сервером, а команда http://203.23.106.33 откроет начальную страницу на корпоративном Web-сервере. Однако пользователи обычно предпочитают работать с символьными именами компьютеров. Следовательно, в сетях TCP/IP должны существовать символьные имена хостов и механизм для установления соответствия между символьными именами и IP-адресами.

Иерархия доменных имен аналогична иерархии имен файлов, принятой во многих популярных файловых системах. Дерево имен начинается с корня, обозначаемого здесь точкой (.). Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т. д. Составные части доменного имени отделяются друг от друга точкой.

В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру, допускающую использование в имени произвольного количества составных частей.



В Internet корневой домен управляется центром InterNIC. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций - следующие обозначения:

com - коммерческие организации (например, microsoft.com);

edu - образовательные (например, mit.edu);

gov - правительственные организации (например, nsf.gov);

org - некоммерческие организации (например, fidonet.org);

net - организации, поддерживающие сети (например, nsf.net).

Каждый домен администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Чтобы получить доменное имя, необходимо зарегистрироваться в какой-либо организации, которой InterNIC делегировал свои полномочия по распределению имен доменов. В России такой организацией является РосНИИРОС, которая отвечает за делегирование имен поддоменов в домене ru.

Система доменных имен

Соответствие между доменными именами и IP-адресами может устанавливаться как средствами локального хоста, так и средствами централизованной службы – системы доменных имен (Domain Name System, DNS). DNS - это централизованная служба, основанная на распределенной базе отображений «доменное имя - IP-адрес». Служба DNS использует в своей работе протокол типа «клиент-сервер». В нем определены DNS-серверы и DNS-клиенты. DNS-серверы поддерживают распределенную базу отображений, а DNS-клиенты обращаются к серверам с запросами о разрешении доменного имени в IP-адрес.

Служба DNS использует текстовые файлы почти такого формата, как и файл hosts, и эти файлы администратор также подготавливает вручную. Однако служба DNS опирается на иерархию доменов, и каждый сервер службы DNS хранит только часть имен сети. При росте количества узлов в сети проблема масштабирования решается созданием новых доменов и поддоменов имен и добавлением в службу DNS новых серверов.

Каждый DNS-сервер кроме таблицы отображений имен содержит ссылки на DNS-серверы своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов. Для обслуживания корневого домена выделено несколько дублирующих друг друга DNS-серверов, IP-адреса которых являются широко известными (их можно узнать, например, в InterNIC).

Схема разрешения IP-адресов

Для ускорения поиска IP-адресов DNS-серверы широко применяют процедуру кэширования проходящих через них ответов. Чтобы служба DNS могла оперативно отрабатывать изменения, происходящие в сети, ответы кэшируются на определенное время - обычно от нескольких часов до нескольких дней.

Существуют две основные схемы разрешения DNS-имен.

1. Итеративная процедура. Работу по поиску IP-адреса координирует DNS-клиент (загружает клиента достаточно сложной работой, то она применяется редко). Клиент сам итеративно выполняет последовательность запросов к разным серверам имен:

1) DNS-клиент обращается к корневому DNS-серверу с указанием полного доменного имени;

2) DNS-сервер отвечает, указывая адрес следующего DNS-сервера, обслуживающего домен верхнего уровня, заданный в старшей части запрошенного имени;

3) DNS-клиент делает запрос следующего DNS-сервера, который отсылает его к DNS-серверу нужного поддомена, и т. д., пока не будет найден DNS-сервер, в котором хранится соответствие запрошенного имени IP-адресу. Этот сервер дает окончательный ответ клиенту.

2. Рекурсивная процедура . В этой схеме клиент перепоручает работу своему серверу. Практически все DNS-клиенты используют рекурсивную процедуру:

1) DNS-клиент запрашивает локальный DNS-сервер, то есть тот сервер, который обслуживает поддомен, к которому принадлежит имя клиента;

2.1) Если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту; это может соответствовать случаю, когда запрошенное имя входит в тот же поддомен, что и имя клиента, а также может соответствовать случаю, когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше;

2.2) Если же локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и т. д. точно так же, как это делал клиент в первом варианте; получив ответ, он передает его клиенту, который все это время просто ждал его от своего локального DNS-сервера.

Лекция 13

Интернет-протокол IP

Основу транспортных средств стека протоколов TCP/IP составляет протокол межсетевого взаимодействия (Internet Protocol, IP). Он обеспечивает передачу дейтаграмм от отправителя к получателям через объединенную систему компьютерных сетей. Протокол IP относится к протоколам без установления соединений. Перед IP не ставится задача надежной доставки сообщений от отправителя к получателю. Протокол IP обрабатывает каждый IP-пакет как независимую единицу, не имеющую связи ни с какими другими IP-пакетами. Все вопросы обеспечения надежности доставки данных по составной сети в стеке TCP/IP решает протокол TCP, работающий непосредственно над протоколом IP. Именно TCP организует повторную передачу пакетов, когда в этом возникает необходимость.

Важной особенностью протокола IP, отличающей его от других сетевых протоколов (например, от сетевого протокола IPX), является его способность выполнять динамическую фрагментацию пакетов при передаче их между сетями с различными, максимально допустимыми значениями поля данных кадров MTU. Свойство фрагментации во многом способствовало тому, что протокол IP смог занять доминирующие позиции в сложных составных сетях.

Структура IP пакета

IP-пакет состоит из заголовка и поля данных. Заголовок, как правило, имеющий длину 20 байт, имеет следующую структуру:

0	8	16	32
№ версии (4 бита)	Длина заголовка (4 бита)	Тип сервиса (8 бит)	Общая длина (16 бит)
		PR D T R	
Идентификатор пакета (16 бит)			Флаги (3 бита)
			Смещение фрагмента (13 бит)
Время жизни (8 бит)		Протокол верхнего уровня (8 бит)	Контрольная сумма (16 бит)
IP-адрес источника (32 бита)			
IP-адрес назначения (32 бита)			
Опции и выравнивание			

Поле Номер версии (Version), занимающее 4 бит, указывает версию протокола IP. Сейчас повсеместно используется версия 4 (IPv4), и готовится переход на версию 6 (IPv6).

Поле Длина заголовка (IHL) IP-пакета занимает 4 бит и указывает значение длины заголовка, измеренное в 32-битовых словах. Обычно заголовок имеет длину в 20 байт (пять 32-битовых слов), но при увеличении объема служебной информации эта длина может быть увеличена за счет использования дополнительных байт в поле Опции (IP Options). Наибольший заголовок занимает 60 октетов.

Поле Тип сервиса (Type of Service) занимает один байт и задает приоритетность пакета и вид критерия выбора маршрута. Первые три бита этого поля образуют подполе приоритета пакета (Precedence), Приоритет может иметь значения от самого низкого - 0 (нормальный пакет) до самого высокого - 7 (пакет управляющей информации). Маршрутизаторы и компьютеры могут принимать во внимание приоритет пакета и обрабатывать более важные пакеты в первую очередь. Поле Тип сервиса содержит также три бита, определяющие критерий выбора маршрута. Реально выбор осуществляется между тремя альтернативами:

- бит D (delay) говорит о том, что маршрут должен выбираться для минимизации задержки доставки данного пакета,
- бит T - для максимизации пропускной способности,
- бит R - для максимизации надежности доставки. Во многих сетях улучшение одного из этих параметров связано с ухудшением другого, кроме того, обработка каждого из них требует дополнительных вычислительных затрат. Поэтому редко, когда имеет смысл устанавливать одновременно хотя бы два из этих трех критериев выбора маршрута. Зарезервированные биты имеют нулевое значение.

Поле Общая длина (Total Length) занимает 2 байта и означает общую длину пакета с учетом заголовка и поля данных. Максимальная длина пакета ограничена разрядностью поля, определяющего эту величину, и составляет 65 535 байт, однако в большинстве хост-компьютеров и сетей столь большие пакеты не используются.

Поле Идентификатор пакета (Identification) занимает 2 байта и используется для распознавания пакетов, образовавшихся путем фрагментации исходного пакета. Все фрагменты должны иметь одинаковое значение этого поля.

Поле Флаги (Flags) занимает 3 бита и содержит признаки, связанные с фрагментацией.

Установленный бит DF (Do not Fragment) запрещает маршрутизатору фрагментировать данный пакет, а установленный бит MF (More Fragments) говорит о том, что данный пакет является промежуточным (не последним) фрагментом. Оставшийся бит зарезервирован.

Поле Смещение фрагмента (Fragment Offset) занимает 13 бит и задает смещение в байтах поля данных этого пакета от начала общего поля данных исходного пакета, подвергнутого фрагментации. Используется при сборке/разборке фрагментов пакетов при передачах их между сетями с различными величинами MTU. Смещение должно быть кратно 8 байт.

Поле Время жизни (Time to Live) занимает один байт и означает предельный срок, в течение которого пакет может перемещаться по сети. Время жизни данного пакета измеряется в секундах и задается источником передачи. На маршрутизаторах и в других узлах сети по истечении каждой секунды из текущего времени жизни вычитается единица; единица вычитается и в том случае, когда время задержки меньше секунды. Поскольку современные маршрутизаторы редко обрабатывают пакет дольше, чем за одну секунду, то время жизни можно считать равным максимальному числу узлов, которые разрешено пройти данному пакету до того, как он достигнет места назначения. Если параметр времени жизни станет нулевым до того, как пакет достигнет получателя, этот пакет будет уничтожен. Время жизни можно рассматривать как часовой механизм самоуничтожения. Значение этого поля изменяется при обработке заголовка IP-пакета.

Идентификатор Протокол верхнего уровня (Protocol) занимает один байт и указывает, какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета (например, это могут быть сегменты протокола TCP, дейтаграммы UDP, пакеты ICMP или OSPF). Значения идентификаторов для различных протоколов приводятся в документе RFC «Assigned Numbers».

Контрольная сумма (Header Checksum) занимает 2 байта и рассчитывается только по заголовку. Поскольку некоторые поля заголовка меняют свое значение в процессе передачи пакета по сети (например, время жизни), контрольная сумма проверяется и повторно рассчитывается при каждой обработке IP-заголовка. Контрольная сумма - 16 бит - подсчитывается как дополнение к сумме всех 16-битовых слов заголовка. При вычислении контрольной суммы значение самого поля «контрольная сумма» устанавливается в нуль. Если контрольная сумма неверна, то пакет будет отброшен, как только ошибка будет обнаружена.

Поля IP-адрес источника (Source IP Address) и IP-адрес назначения (Destination IP Address) имеют одинаковую длину - 32 бита - и одинаковую структуру.

Поле Опции (IP Options) является необязательным и используется обычно только при отладке сети. Механизм опций предоставляет функции управления, которые необходимы или просто полезны при определенных ситуациях, однако он не нужен при обычных коммуникациях. Это поле состоит из нескольких подполей, каждое из которых может быть одного из восьми predetermined типов. В этих подполях можно указывать точный маршрут прохождения маршрутизаторов, регистрировать проходимые пакетом маршрутизаторы, помещать данные системы безопасности, а также временные отметки. Так как число подполей может быть произвольным, то в конце поля Опции должно быть добавлено несколько байт для выравнивания заголовка пакета по 32-битной границе.

Поле Выравнивание (Padding) используется для того, чтобы убедиться в том, что IP-заголовок заканчивается на 32-битной границе. Выравнивание осуществляется нулями.

Лекция 14

Таблица маршрутизации в IP сетях

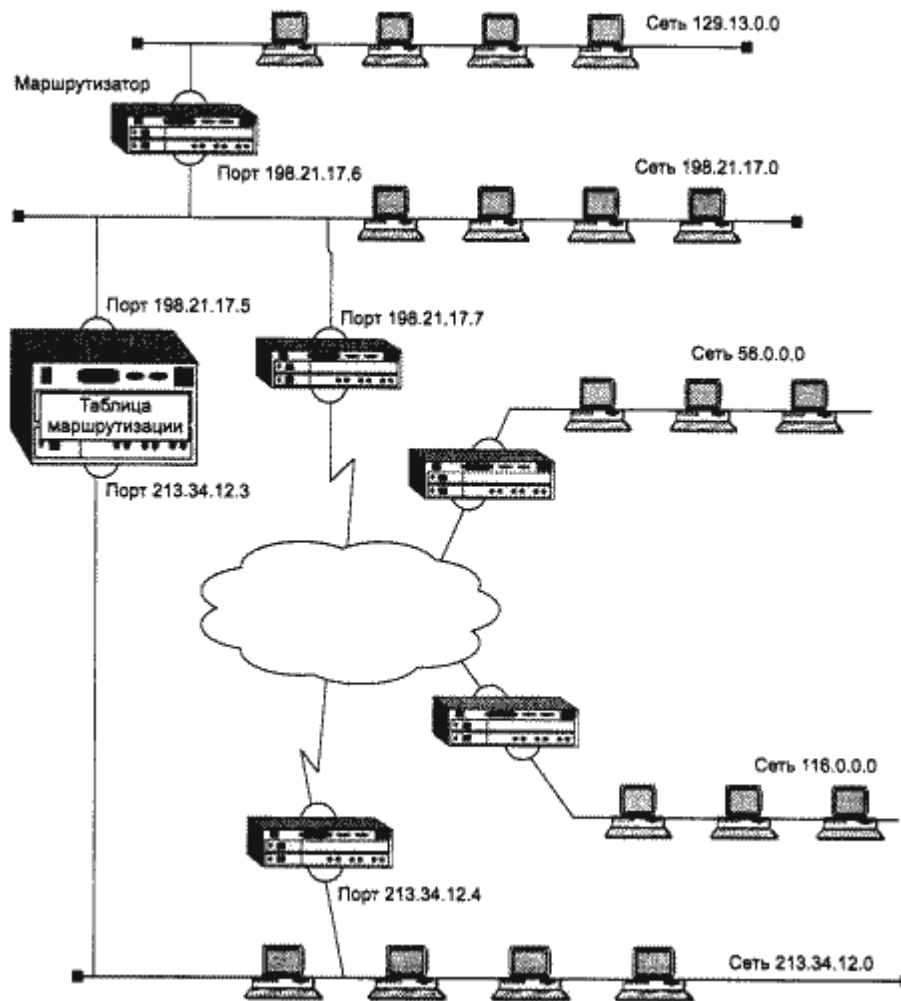


Таблица маршрутизации:

Network Address	Netmask	Gateway Address	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0	1
0.0.0.0	0.0.0.0	198.21.17.7	198.21.17.5	1
56.0.0.0	255.0.0.0	213.34.12.4	213.34.12.3	15
116.0.0.0	255.0.0.0	213.34.12.4	213.34.12.3	13
129.13.0.0	255.255.0.0	198.21.17.6	198.21.17.5	2
198.21.17.0	255.255.255.0	198.21.17.5	198.21.17.5	1
198.21.17.5	255.255.255.255	127.0.0.1	127.0.0.1	1
198.21.17.255	255.255.255.255	198.21.17.5	198.21.17.5	1
213.34.12.0	255.255.255.0	213.34.12.3	213.34.12.3	1
213.34.12.3	255.255.255.255	127.0.0.1	127.0.0.1	1
213.34.12.255	255.255.255.255	213.34.12.3	213.34.12.3	1
224.0.0.0	224.0.0.0	198.21.17.6	198.21.17.6	1
224.0.0.0	224.0.0.0	213.34.12.3	213.34.12.3	1
255.255.255.255	255.255.255.255	198.21.17.6	198.21.17.6	1

Источники записи таблиц маршрутизации

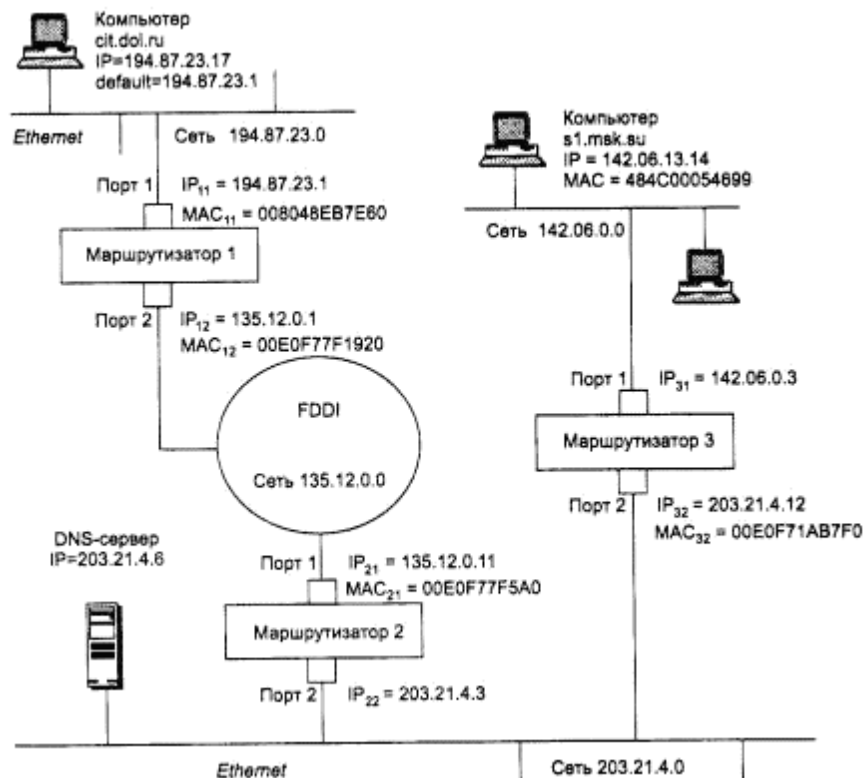
1. Программное обеспечение стека TCP/IP - при инициализации маршрутизатору оно автоматически заносит в таблицу несколько записей. Создаётся минимальная таблица:

- 1) Записи о непосредственно подключенных к маршрутизатору сетях;
- 2) ПО автоматически заносит в таблицу особые адреса (loopback, 224)

2. Администратор сети заносит в таблицу записи с помощью утилиты route. Это всегда статические записи без срока жизни. Может быть записан специфический адрес или маршрут. Тогда вместо номера сети - полный адрес узла. Для этого узла маршрут определяется специфически.

3. Протоколы маршрутизации (RIP, OSPF) - динамические записи.

Алгоритм по продвижению пакетов в сети



1. Итак, пусть пользователь компьютера cit.dol.ru, находящегося в сети Ethernet и имеющего IP-адрес 194.87.23.17 (адрес класса C), обращается по протоколу FTP к компьютеру sl.msk.su, принадлежащему другой сети Ethernet и имеющему IP-адрес 142.06.13.14 (адрес класса B): > ftp sl.msk.su

Модуль FTP упаковывает свое сообщение в сегмент транспортного протокола TCP, который в свою очередь помещает свой сегмент в пакет протокола IP. В заголовке IP-пакета должен быть указан IP-адрес узла назначения. Так как пользователь компьютера cit.dol.ru использует символьное имя компьютера sl.msk.su, то стек TCP/IP должен определить IP-адрес узла назначения самостоятельно.

При конфигурировании стека TCP/IP в компьютере cit.dol.ru был задан его собственный IP-адрес, IP-адрес маршрутизатора по умолчанию и IP-адрес DNS-сервера. Модуль IP может сделать запрос к серверу DNS, но обычно сначала просматривается локальная таблица соответствия символьных имен и IP-адресов. Такая таблица хранится чаще всего в виде текстового файла простой структуры - каждая его строка содержит запись об одном символьном имени и его IP-адресе. В ОС Unix такой файл традиционно носит имя hosts и находится в каталоге /etc.

2. Будем считать, что компьютер dt.dol.ru имеет файл hosts, а в нем есть строка 142.06.13.14 sl.msk.su.

Таким образом, разрешение имени выполняется локально, и протокол IP может теперь формировать IP-пакеты с адресом назначения 142.06.13.14 для взаимодействия с компьютером sl.msk.su.

3. Модуль IP компьютера cit.dol.ru проверяет, нужно ли маршрутизировать пакеты с адресом 142.06.13.14. Так как адрес сети назначения (142.06.0.0) не совпадает с адресом (194.87.23.0) сети, которой принадлежит компьютер-отправитель, то маршрутизация необходима.

4. Компьютер cit.dol.ru начинает формировать кадр Ethernet для отправки IP-пакета маршрутизатору по умолчанию, IP-адрес которого известен - 194.87.23.1, но неизвестен MAC - адрес, необходимый для перемещения кадра в локальной сети. Для определения MAC - адреса маршрутизатора протокол IP обращается к протоколу ARP, который просматривает ARP-таблицу. Если в последнее время компьютер cit.dol.ru выполнял какие-либо межсетевые обмены, то скорее всего искомая запись, содержащая соответствие между IP- и MAC - адресами маршрутизатора по умолчанию уже находится в кэш-таблице протокола ARP. Пусть в данном случае нужная запись была найдена именно в кэш-таблице: 194.87.23.1 008048EB7E60

Обозначим найденный MAC - адрес 008048EB7E60 в соответствии с номером маршрутизатора и его порта через MAC11.

5. В результате компьютер cit.dol.ru отправляет по локальной сети пакет, упакованный в кадр Ethernet, имеющий следующие поля:

MAC ₁₁ 008048EB7E60		IP назначения 142.06.13.14	
Заголовок кадра Ethernet		Заголовок пакета IP	Поле данных пакета IP

6. Кадр принимается портом 1 маршрутизатора 1 в соответствии с протоколом Ethernet, так как MAC - узел этого порта распознает свой адрес MAC11. Протокол Ethernet извлекает из этого кадра IP-пакет и передает его программному обеспечению маршрутизатора, реализующему протокол IP. Протокол IP извлекает из пакета адрес назначения 142.06.13.14 и просматривает записи своей таблицы маршрутизации. Пусть маршрутизатор 1 имеет в своей таблице маршрутизации запись 142.06.0.0 135.12.0.11 2, которая говорит о том, что пакеты для сети 142.06. 0.0 нужно передавать маршрутизатору 135.12.0.11, находящемуся в сети, подключенной к порту 2 маршрутизатора 1.

7. Маршрутизатор 1 просматривает параметры порта 2 и находит, что к нему подключена сеть FDDI. Так как сеть FDDI имеет значение MTU большее, чем сеть Ethernet, то фрагментация IP-пакета не требуется. Поэтому маршрутизатор 1 формирует кадр формата FDDI. На этом этапе модуль IP должен определить MAC - адрес следующего маршрутизатора по известному IP-адресу 135.12.0.11. Для этого он обращается к протоколу ARP. Допустим, что нужной записи в кэш-таблице не оказалось, тогда в сеть FDDI отправляется широковещательный ARP-запрос, содержащий наряду с прочей следующей информацией.

MAC широковещат. FFF...F	MAC отправителя 00E0F77F1920		Искомый MAC 000...0	Заданный IP 135.12.0.11
Заголовок кадра FDDI			ARP-запрос	

Порт 1 маршрутизатора 2 распознает свой IP-адрес и посылает ARP-ответ по адресу

запросившего узла:

MAC назначения 00E0F77F1920	MAC отправителя 00E0F77F51A0		Найденный MAC 00E0F77F51A0	Заданный IP 135.12.0.11
--------------------------------	---------------------------------	--	-------------------------------	----------------------------

Заголовок кадра FDDI

ARP-ответ

Теперь, зная MAC - адрес следующего маршрутизатора 00E0F77F51A0, маршрутизатор 1 отправляет кадр FDDI по направлению к маршрутизатору 2. Заметим, что в поле IP-адреса назначения никаких изменений не произошло.

MAC ₁₂ 00E0F77F51A0		IP назначения 142.06.13.14	
--------------------------------	--	-------------------------------	--

Заголовок кадра FDDI

Заголовок
пакета IP

Поле данных пакета IP

8. Аналогично действует модуль IP на маршрутизаторе 2. Получив кадр FDDI, он отбрасывает его заголовок, а из заголовка IP извлекает IP-адрес сети назначения и просматривает свою таблицу маршрутизации. Там он может найти запись о конкретной сети назначения:

142.06.0.0 203.21.4.12 2

или при отсутствии такой записи будет использована запись о маршрутизаторе по умолчанию:

default 203.21.4.12 2.

Определив IP-адрес следующего маршрутизатора 203.21.4.12, модуль IP формирует кадр Ethernet для передачи пакета маршрутизатору 3 по сети Ethernet. С помощью протокола ARP он находит MAC - адрес этого маршрутизатора и помещает его в заголовок кадра. IP-адрес узла назначения, естественно, остается неизменным.

MAC ₃₂ 00E0F71AB7F0		IP назначения 142.06.13.14	
--------------------------------	--	-------------------------------	--

Заголовок кадра Ethernet

Заголовок
пакета IP

Поле данных пакета IP

9. Наконец, после того как пакет поступил в маршрутизатор сети назначения - маршрутизатор 3, - появляется возможность передачи этого пакета компьютеру назначения. Маршрутизатор 3 определяет, что пакет нужно передать в сеть 142.06.0.0, которая непосредственно подключена к его первому порту. Поэтому он посылает ARP-запрос по сети Ethernet с IP-адресом компьютера sl.msk.su. ARP-ответ содержит MAC - адрес конечного узла, который модуль IP передает канальному протоколу для формирования кадра Ethernet:

MAC конечного узла 484C00054699		IP назначения 142.06.13.14	Сегмент TCP
------------------------------------	--	-------------------------------	-------------

Заголовок кадра Ethernet

Заголовок
пакета IP

Поле данных пакета IP

10. Сетевой адаптер компьютера sl.msk.ru захватывает кадр Ethernet, обнаруживает совпадение MAC - адреса, содержащегося в заголовке, со своим собственным адресом и направляет его модулю IP. После анализа полей IP-заголовка из пакета извлекаются данные, которые в свою очередь содержат сообщение выше лежащего протокола. Поскольку в данном примере рассматривается обмен данными по протоколу FTP, который использует в качестве транспортного протокола TCP, то в поле данных IP-пакета находится TCP - сегмент. Определив из TCP-заголовка номер порта, модуль IP переправляет сегмент в соответствующую очередь, из которой данный сегмент попадет программному модулю FTP-сервера.

Итого: заголовки сетевого уровня (IP-адреса) не меняются на протяжении всего маршрута. Заголовок транспортного уровня (MAC-адреса) меняются на каждом хопе.

Лекция 15

Маршрутизация с использованием масок

К появлению данного вида маршрутизации привела необходимость структуризации (разбиения) сетей. При получении группы IP-адресов определенного класса возникает необходимость распределения этих адресов между клиентами. Для региональных провайдеров такими клиентами являются локальные провайдеры. Им нужно выдавать определенные диапазоны адресов, но использование для этого целых классов сетей не обеспечивает достаточной точности распределения.

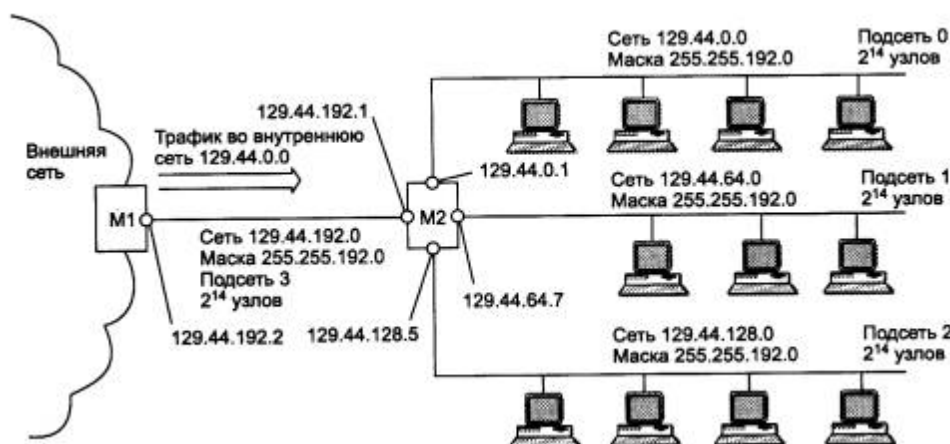
Например, региональный провайдер получил себе сеть класса А. В нее входит много адресов. Услугами этого провайдера пользуются несколько локальных провайдеров. Для каждого из них вся сеть класса А слишком большая, но они хотят находиться в своем личном адресном пространстве, которым кроме них гарантировано никто не сможет воспользоваться. Если использовать для разделения на сети только классы адресов, то региональный провайдер просто не сможет разделить свою единственную сеть на части. Для того, чтобы разделить ее на части и придумали маски сетей.

Маска сети указывает на то, какая часть сетевого адреса относится к номеру сети, а какая к номеру узла в сети. Маски позволяют вписать в одну сеть несколько подсетей.

Например: региональный провайдер получил себе сеть 129.44.0.0 (Класс В) Ему необходимо разделить адреса из этой сети на несколько сетей, по 255 узлов в каждой. Для этого, выдавая клиентам сети, он снабжает их информацией о масках сетей, закрепляя таким образом за ними небольшие части своей большой сети (подсети). В итоге получается, что каждый клиент получает свой кусочек, платит только за него и использует только его. Экономия средств и IP-адресов.

Сеть (10)	129.	44.	0.	0
Сеть (2)	10000001	00101100	00000000	00000000
Маска (класс В)	11111111	11111111	00000000	00000000
Маска (клиентам)	11111111	11111111	11111111	00000000

Для того, чтобы такое разделение был возможен, нужно чтобы маршрутизатор, занимающийся распределением пакетов между сетями, понимал маскирование. Снаружи (из глобальной сети Net) сеть 129.44.0.0 выглядит как единый кусок. Разделение на несколько подсетей происходит только внутри этой сети, и получается, что внутренняя структура сети скрыта от внешнего наблюдателя.



Для того, чтобы использовать маски сетей, пришлось изменить логику работы IP (конкретно маршрутизацию):

1. В каждой записи таблицы маршрутизатора появляется новое поле - маска сети.
2. При просмотре каждой записи в таблице маска накладывается на IP-адрес назначения из принятого пакета.
3. Полученное в результате число - номер сети назначения - сравнивается с номером сети в таблице маршрутизатора
4. Если номера совпадают, то пакет перенаправляется в соответствии с данной записью.
5. Если таких совпадений несколько, то выбирается маршрут, в котором фигурирует самая длинная маска (больше всего 1)
6. Маршрут по умолчанию теперь задается маской 0.0.0.0, которая является самой короткой. Таким образом любой адрес, на который будет наложена маска маршрута по умолчанию, совпадет с адресом сети 0.0.0.0 (адрес маршрута по умолчанию).

Работа в сети

1. Все маршрутизаторы внешней сети, встретив пакеты 129.44.x.x интерпретируют их как класс В, и направляют по маршрутам, ведущим к R1.
2. Маршрутизатор направляет весь входной трафик на R2 (тут можно было обойтись

и без такого перенаправления а просто использовать R1, который понимает маски, и подключить сети .64.0 и .128.0 непосредственно к R1).

3. Маршрутизатор R2 смотрит на адрес назначения, смотрит на свою таблицу маршрутизации и перенаправляет пакет с использованием масок.

Все маршрутизаторы внешней сети, встретив пакеты с адресами, начинающимися с 129.44, интерпретируют их как адреса класса В и направляют по маршрутам, ведущим к маршрутизатору M1. Маршрутизатор M1 в свою очередь направляет весь входной трафик сети 129.44.0.0 на маршрутизатор M2, а именно на его порт 129.44.192.1.

Маршрутизатор M2 обрабатывает все поступившие на него пакеты в соответствии с таблицей маршрутизации:

Номер сети	Маска	Адрес следующего маршрутизатора	Адрес порта	Расстояние
129.44.0.0	255.255.192.0	129.44.0.1	129.44.192.2	Подключена
129.44.64.0	255.255.192.0	129.44.64.7	129.44.64.7	Подключена
129.44.128.0	255.255.192.0	129.44.128.5	129.44.128.5	Подключена
129.44.192.0	255.255.192.0	129.44.192.1	129.44.192.1	Подключена
0.0.0.0	0.0.0.0	129.44.192.2	129.44.192.1	—

Использование масок переменной длины

Предположим, что у нас есть сеть, поделенная на подсети. Все подсети одинаковой длины. Поле номера сети - 18 бит, поле номера узла - 14 бит. Для каких-то клиентов это нормально, для каких-то - слишком много. Более эффективно распределять адреса разным клиентам разными порциями. Администратор может более рационально распределять адресное пространство с помощью масок переменной длины.

Лекция 16

Использование масок переменной длины

1 байт	2 байт	3 байт	4 байт	
№ сети		№ подсети	Поле адресов	
класс В			узлов	
129.	44.			
1000 0001	0010 0100	0000 0000	0000 0000	
1000 0001	0010 0100	0111 1111	1111 1111	
1000 0001	0010 0100	1000 0000	0000 0000	
1000 0001	0010 0100	1011 1111	1111 1111	
1000 0001	0010 0100	1100 0000	0000 0000	
1000 0001	0010 0100	1100 0000	0000 0111	
1000 0001	0010 0100	1100 0000	0000 1000	
1000 0001	0010 0100	1101 1111	1111 1111	
1000 0001	0010 0100	1110 0000	0000 0000	

1000 0001 | 0010 0100 | 1111 1111 | 1111 1111 |

2 большие группы
128.44

```

      /           \
    0/...         1/...
      /  \         /  \
    0/0...0 0/1...1 10/  \
                  /    \
                10/0...0 10/1...1
  
```

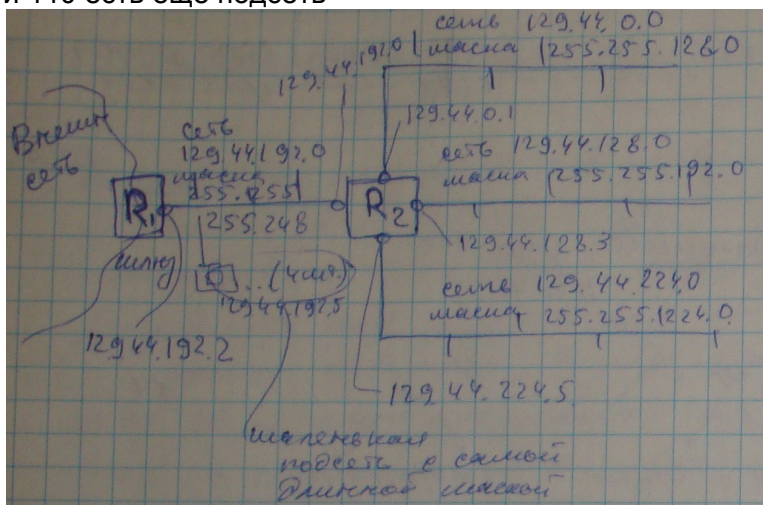
11/

Если адреса совпадают с маской 1100 0000 0000 0000, то хоп выполняется по самой длинной маске. Таблица маршрутизации всегда просматривается до конца, поскольку могут быть еще совпадения.

В этом примере 4 подсети разного размера. Подсеть с данной маской вырезана из другой подсети (110) специально для связи R1 и R2. В ней 6 IP-адресов, из которых 2 на вх. МШ, остальные 4 свободны.

Внутренняя структура сети скрыта от внешней сети. Для внешней сети она представляет собой просто сеть класса B.

4 подсети + в сети 110 есть еще подсеть



Некоторые особенности масок переменной длины

Это наличие перекрытий, то есть выделение нескольких строк в таблице маршрутизации. Адрес сети в пришедшем пакете выделяется с помощью наложения масок в разных строках. Может совпасть с адресом сразу нескольких записей в таблице. МШ работает по следующему правилу: в случае совпадения выбран будет наиболее специфичный маршрут, то есть строка с наиболее длинной маской.

Таблица МШ R2:

№ сети	Маска	Адрес след. МШ	Адрес вых. порта	Расст.	
129.44.0.0	255.255.128.0	129.44.0.1	129.44.0.1	подключ.	
129.44.128.0	255.255.192.0	129.44.128.3	129.44.128.3	—/—	
129.44.192.0	255.255.248.0	129.44.192.1	129.44.192.1	—/—	

129.44.224.0	255.255.224.0	129.44.224.5	129.44.224.5		—//—	
0.0.0.0	0.0.0.0	129.44.192.2	129.44.192.2		—//—	

Пример: Пусть из внешней сети поступает пакет по адресу 129.44.192.1. МШ R1 имеет следующую таблицу маршрутизации:

№ сети	Маска	Адрес след. МШ	Адрес вых. порта	
129.44.0.0	255.255.0.0	129.44.192.1	129.44.192.2	
129.44.192.0	255.255.248.0	129.44.192.	129.44.192.2	

В таблице первая строка отправляет все пакеты на R2 (129.44.0.0). Однако среди этих пакетов есть поступившие по адресу 129.44.192.x (например, 129.44.192.5), сопровождаемые маской 255.255.248.0. После наложения масок совпадут 2 строки, и из них будет выбрана строка с более длинной маской (вторая). То есть пакеты будут отправлены на PC минуя R2.

В IP сетях с использованием масок протокол маршрутизации передается адрес сети, если во всех сетях одинаковая маска - это приемлемо, но если используется переменная маска, необходимо вместе с IP-адресом передавать также маску. Для этого предназначены протоколы OSPF, RIPv2.

Технология бесклассовой междоменной маршрутизации

Предположим, что провайдер предоставил нам адреса 129.44.x.x + мы купили адреса 129.45.x.x, 129.46.x.x и 129.47.x.x.

1000 0001. 0010 1100.....
 1000 0001. 0010 1101.....
 1000 0001. 0010 1110.....
 1000 0001. 0010 1111.....

Все комбинации, начинающиеся с 1000 0001. 0010 11 принадлежат нам, поэтому можно сдвинуть маску на два разряда влево. В этом и состоит бесклассовая междоменная маршрутизация (Classless Inter-Domain Routing, CIDR). Если у нас есть лишь часть адресов, маску сдвигать нельзя.

МШ будет работать по префиксу, который определяется маской.

В последнее время резко увеличилось число узлов Internet, в результате чего сети перегружены. Технология CIDR позволяет улучшить обстановку. Она была предложена в 1993 году RFC 1517-1520

Суть технологии: каждому провайдеру назначается некоторый непрерывный диапазон IP адресов. Все адреса провайдера имеют общую старшую часть - префикс. Тогда маршрутизация может производиться по префиксу, а не по полному адресу сети.

Лекция 17

При использовании технологии CIDR каждому провайдеру назначается некоторый непрерывный диапазон IP адресов. Все адреса провайдера имеют общую старшую часть - префикс. Тогда маршрутизация может производиться по префиксу, а не по полному адресу сети. За счёт этого уменьшается размер таблицы маршрутизации,

следовательно, ускоряется работа маршрутизаторов. Деление IP адреса на № сети и № узла производится не на основе класса, а на основе масок переменной длины. Все адреса имеют общую часть (префикс) в k разрядах, остальные n разрядов используются для наполнения переменной части адреса.

Если клиент просит выделить некоторый объем адресов в имеющемся пуле 2^n адресов, то вырезается некоторая непрерывная область S1;S2;S3 или S4 нужного размера.

Технология CIDR

префикс 00... 10 р. ... 8 р.	- S1
префикс 00... 9 р. ... 9 р.	- S2
префикс 00... 8 р. ... 10 р.	- S3
префикс 00...7 р.... 11 р.	- S4

(k=14, n=18)

Для S1,S2,S3,S4 одинаковый префикс: 255.252.0.0

S1:

подсеть 193.20.0.0

маска 255.255.255.0

256 узлов (с учётом особых адресов)

S2:

подсеть 193.21.0.0

маска 255.255.254.0

512 узлов

S3:

1024 узла

S4:

2048 узлов

Технология CIDR решает 2 основные задачи:

1)более экономное распределение адресного пространства за счёт отказа от классов и точного деления адресного пространства.

2)уменьшение числа записей в таблице маршрутизации за счёт использования префиксов и объединения групп IP-адресов.

Технология CIDR поддерживает протоколы: IPv4; OSPF; IPv6; BGP4.

Фрагментация пакетов

Различают фрагменты:

1)в узле-отправителе, восп. трансп. уровень протокол TCP

2)динамическая фрагментация - в случае, если при выполнении хопа MTU (макс. перед. ед.) в транзит. сети < MTU пакета. Эту фрагментацию производит протокол IP на промежуточном МШ.

В большинстве сетей MTU (max. transfer unit) значительно отличается:

Ethernet: MTU=1500 байт

FDDI (TR): MTU=4096 байт

x.25: MTU=128 байт

Имеется бит, который помечает пакет как не фрагментируемый ни при каких условиях.

Если на маршруте возникает необходимость фрагментации, такой пакет не может быть

доставлен и удаляется. Отчёт посылается источнику сообщением ICMP.

При фрагментации модуль IP отправляет пакет, установив в поле № пакета уникальный номер, присутствующий в каждом фрагменте для операции сборки фрагментов именно этого пакета. Если пришел последний фрагмент и все остальные приняты, то можно приступить к сборке.

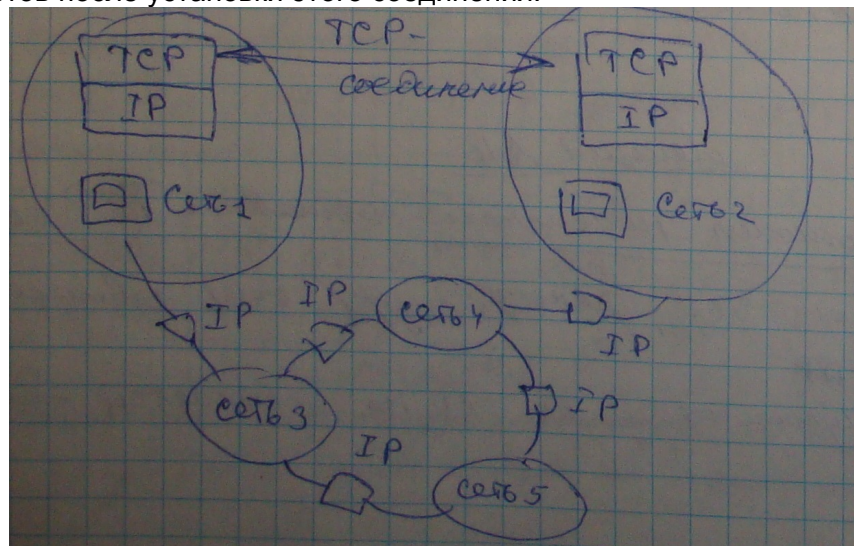
В каждом фрагменте значения полей отличаются от исходного пакета, значит, для каждого фрагмента должна быть подсчитана новая контрольная сумма. Сборка фрагментов пакетов на PC получателя на сетевом уровне происходит с помощью модуля IP.

Лекция 18

Протокол надежной доставки сообщений TCP

TCP - протокол четвертого, транспортного уровня. Не используется для мультимедиа-передачи - слишком медленный (для этих целей используется другой протокол транспортного уровня - UDP. Это дейтаграммный протокол, не гарантирующий надежную доставку).

TCP используется для решения задачи надежной доставки. TCP - transmission control protocol. Работает над протоколом IP и использует IP для транспортировки своих кадров. TCP основан на установлении логического соединения между взаимодействующими процессами (портами). При этом TCP помещает свои блоки в IP пакеты для передачи. На рисунке - процессы на двух конечных узлах. С помощью TCP через составную сеть устанавливается предварительное надежное соединение. Протокол IP используется для доставки пакетов после установки этого соединения.



ICMP-сообщения используются для обмена МШ с источником (при невозможности передачи или в случае потери сообщения)

Порты

Порты хар-ся приложениями.

Задача сетевого уровня (IP) - передача между узлами сети. А задача транспортного уровня (TCP) - передача между любыми прикладными процессами на узлах сети (между портами). Каждая PC может одновременно взаимодействовать с несколькими портами, то

есть иметь несколько входов-адресов назначения для пакетов. Пакеты на транспортном уровне организованы ОС в виде очередей с точками входа. В терминологии TCP это порты. Таким образом, адресом назначения для TCP является № порта. {№сети, № узла, № порта} - однозначно определяют прикладной процесс в сети. Этот набор параметров называется сокетом.

Сокет=№порта+№сети+№узла=IP-адрес+№порта

№ порта - 2 байта (плоский адрес, не структурированный, как MAC). Таким образом, существует 65 536 портов.

Назначение № портов:

1) Централизованно - для популярных служб (1000 зарезервировано под специальные приложения)

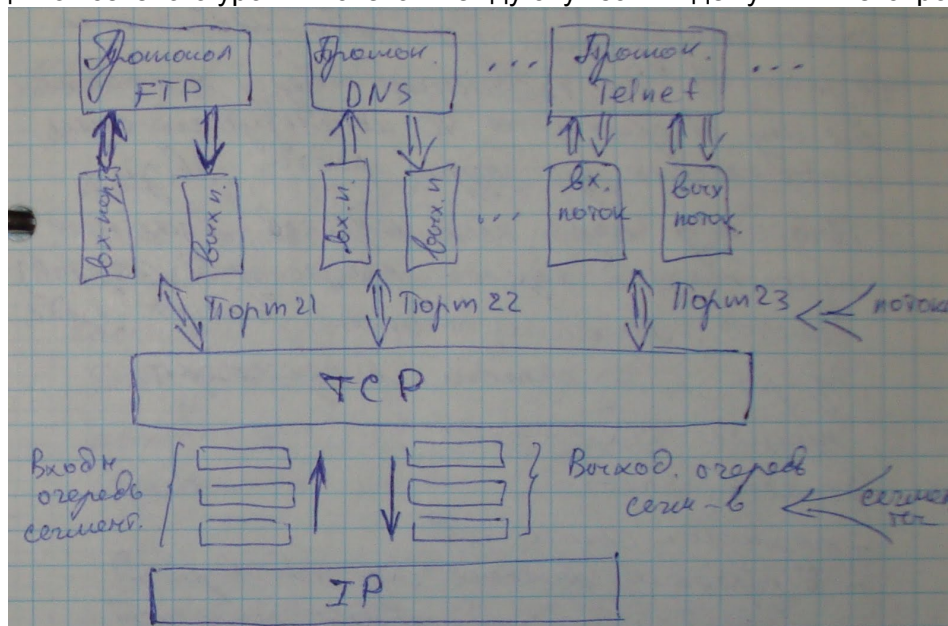
21 - FTP

23 - Telnet

Это назначение осуществляет специальная организация Internet Assigned Numbers Authority - IANA. Стандартные № публикуются в стандартах Internet (RFC 1700) - можно посмотреть весь список назначенных стандартных адресов. (RFC - Request For Comment)

2) Локально - для остальных служб. Сам пользователь на своей PC назначает своим приложениям конкретные номера.

TCP ведёт для каждого порта 2 очереди: входную и выходную. Процедура обслуживания TCP запроса от нескольких прикладных служб (портов) называется мультиплексированием. Обратная операция - распределение протоколом TCP поступающих от сетевого уровня пакетов между службами - демultipлексирование.



Сегменты и потоки

Единицей данных TCP является сегмент. Информация TCP с верхних уровней - поток байт (сообщение) - буферизируется в TCP для передачи на сетевой уровень.

Из буфера вырезается сегмент. Размер сегмента не должен превышать максимальный размер поля данных IP пакета.

Соединение

Для надежной передачи TCP организует логическое соединение между приложениями процессами. Так как соединение осуществляется через ненадежную систему IP протокола, то используется специальная многошаговая процедура подтверждения связи. Идентифицируется пара полных адресов процессов (портов) - сокетов. Помимо этого сюда включаются параметры, определенные в процессе переговоров двух сторон. Согласовывается:

- размеры сегментов
- объем передачи данных без подтверждения (какой объем можно передать, после которого будет подтверждение. Лучше осуществлять подтверждение для группы байтов).
- размер окна
- начальный и текущий номера передаваемых байтов

Соединение TCP позволяет вести передачу в обе стороны, то есть полный дуплекс.

Лекция 19

Скольльзящее окно в TCP

Квитирование - традиционный метод защиты от ошибок.

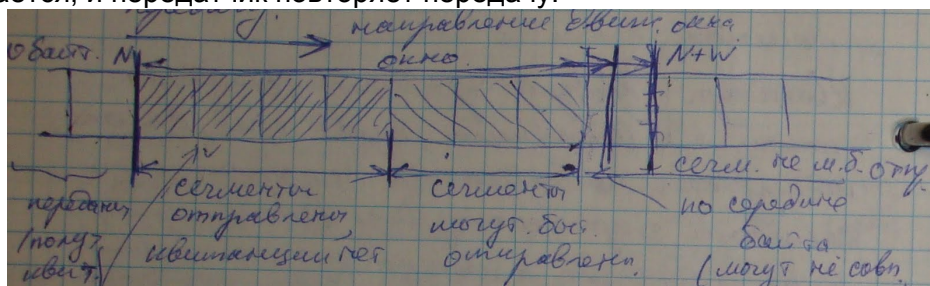
Квитирование - проверка правильности, отправление положительной квитанции, передача следующего байта. Но побайтная передача неэффективна. Частный случай - скользящее окно. Посылаются байт за байтом, а только потом положительная квитанция. Осуществляется передача по окнам. Хотя единица данных - сегмент, окно определено на множестве нумерованных байтов потока (или сообщения).

Получающий модуль TCP (приемник) отправляет окно посылающему - задает количество байт, после получения положительной квитанции на следующее окно. Окно - количество байтов, передаваемых за раз.

передачик |<-----окно----->| приемник
|-----байты----->|
|<-----квитанция----->|

Окно может равняться и 0, если приемник не успевает обрабатывать поток. Система скользящего окна является гибкой.

Квитанция посылается приемником только в случае правильного приема. В случае ошибки - не посылается, и передатчик повторяет передачу.



Последняя квитанция - на байт с № N. Если пришла квитанция на байт N+1 - сдвигаем окно.

Когда TCP передает сегмент, он помещает его в очередь повторной передачи и запускает таймер. Если нет квитанции к моменту истечения таймера, происходит повторная

передача. Если квитанция приходит, соответствующий сегмент изымается из очереди и окно сдвигается. При выборе времени таймера учитывается скорость передачи по маршруту, длина маршрута, надежность линии связи. Варьируя величину окна, приемник может влиять на величину входного потока. При переполнении буфера приемника TCP отправляет квитанцию, в которую помещает меньший размер окна (вплоть до 0). Но даже после этого передатчик может послать сегменты с пометкой "срочно" в заголовке TCP. Приемник должен принять такой сегмент, даже если для этого придется вытеснить из буфера данные.

Как после обрыва передачи её возобновить? Ведь нет сегмента - нет квитанции - нет размера окна (то есть он по-прежнему равен 0). Решение: после приема квитанции с нулевым размером окна передатчик делает контрольные попытки обмена - кадры с нулевым полем данных (пустые кадры). Если приемник готов, то в ответ он посылает квитанцию с ненулевым размером окна.

Внутренние и внешние протоколы маршрутизации в Internet

Большинство протоколов маршрутизации происходят от Internet. Рассмотрим сначала структуру Internet. Это сеть, объединяющая большое количество автономных сетей.

Выделяют:

- 1) магистральную сеть (Core backbone network)
- 2) автономные системы Autonomous System - AS (сети, подсоединенные к магистралям)

Предел сетей на МШ - десятки и сотни тысяч РС (объединение локальных сетей - это и есть автономная система).

Internet сеть - совокупность автономных систем.

Автономные сети имеют ограничения на размер из-за протокола маршрутизации (таблица маршрутизации). Для больших сетей обновление данных (посредством работы протокола RIP) будет затруднительной.

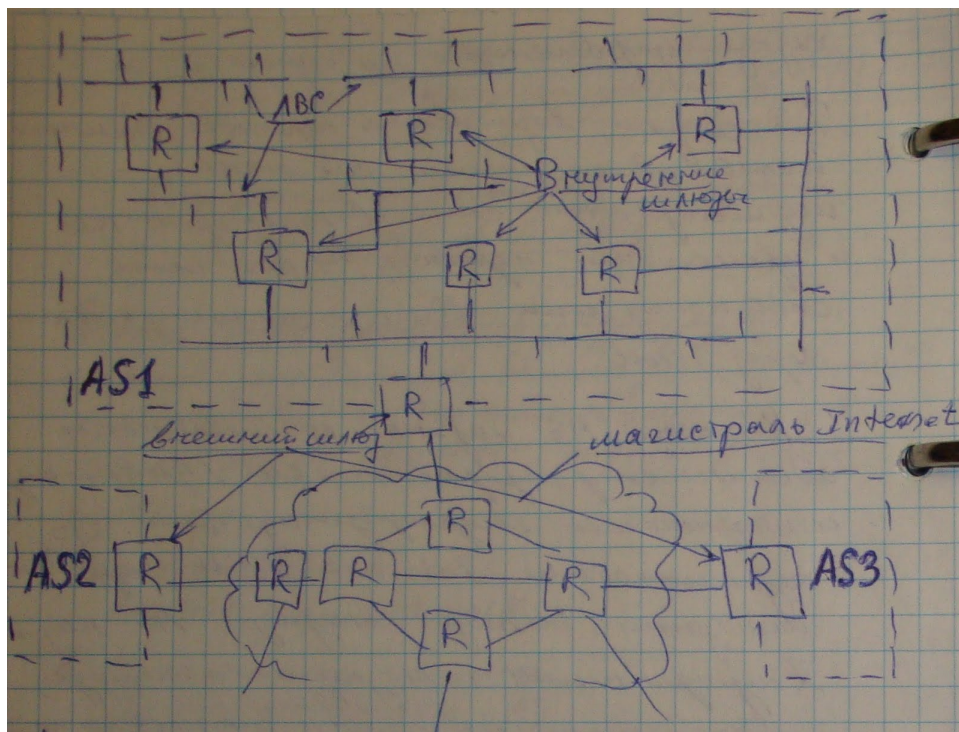
Обязательно должна быть возможность передачи данных между автономными системами - магистральная сеть. С помощью неё и происходит передача. У неё есть свой номер сети. Связь с магистралью осуществляется через МШ.

Каждая АС характеризуется собственным администр. управлением (провайдер) и протоколом маршрутизации. По терминологии Internet МШ называют шлюзами. Шлюзы внутри АС называют внутренними шлюзами, а соединяющие АС и магистраль - внешними. Все АС имеют свой уникальный 16-ти разрядный номер, который выделяется организацией InterNIC.

Протоколы МШ:

- 1) Протоколы внутренних шлюзов (RIP, IP)
- 2) Протоколы внешних шлюзов

Пример: фрагмент Internet с единственной магистралью.



Для этой структуры (Internet с единственной магистралью) протоколом обмена между АС является EGP - exterior gateway protocol. В начале 90-ых была единственная магистраль с этим протоколом. Но с развитием интернета, сеть стала более сложной с произвольными связями между АС. Протокол EGP был заменен на BGP (Boarder gateway protocol). BGP распознает петли. Оба протокола используются во внешних шлюзах и организуются провайдерами.

Лекция 20

Дистанционно-векторный протокол RIP

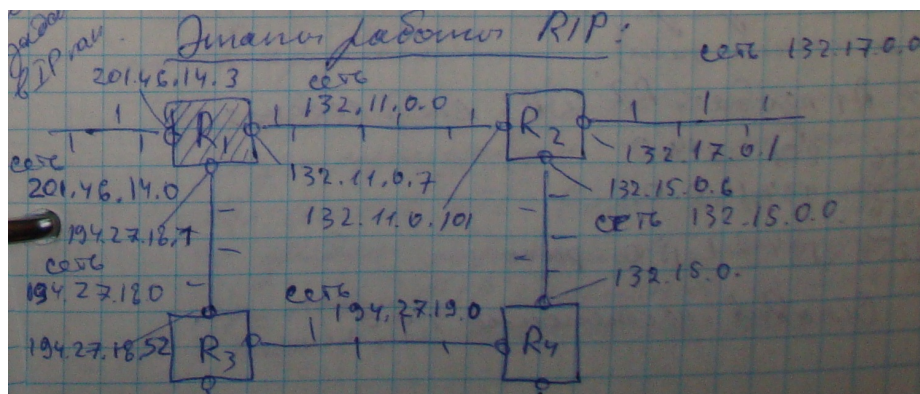
Дистанционно-векторного типа. Используется две версии для сетей IP:

1. RIPv.1 - не поддерживает масок
2. RIPv.2 - передает информацию о масках сетей

В кач-ве расстояния использует следующие метрики:

- Хопы
- Пропускная способность
- Задержки
- Надежность

Этапы работы RIP



Этап 1 - создание минимальной таблицы маршрутизации - только непосредственно подключаемые сети.

№ сети	Адрес след. порта	Адрес вых. МШ	Расстояние
201.46.14.0	201.46.14.3	201.46.14.3	1
132.11.0.0	132.11.0.7	132.11.0.7	1
194.27.18.0	194.27.18.1	194.27.18.1	1

Этап 2 - рассылка минимальных таблиц соседям с помощью служебных RIP-сообщений по протоколу UDP. Сообщения включают два параметра: адрес и расстояние от неё до передающего МШ.

Таким образом R1 передаёт R2 и R3 следующее сообщение:

сеть 201.46.14.0

сеть 132.11.0.0

сеть 194.27.18.0

Этап 3 - получение RIP-сообщения от соседей. Каждый МШ наращивает каждое полученное поле метрики на 1 и запоминает, через какой порт и от какого МШ получена информация. Совпадающие записи с худшими расстояниями отбрасываются.

Этап 4 - рассылка новой (не минимальной) таблицы соединений - данные о всех известных ему сетях.

Этап 5 - получение RIP-сообщений от соседей (повторяет этап 3).

В результате в сети устанавливается конкретный режим маршрутизации - любая сеть будет доступна из любой сети.

Адаптация RIP-маршрутизатора к изменениям состояния сети

К новым маршрутам МШ приспосабливаются просто. Они передают свою информацию через соседей. К потере маршрута - сложнее. Используется 2 варианта уведомлений об отказавших маршрутах:

1. Истечение времени жизни в таблице маршрутизации - каждая запись в таблице имеет TTL. Если за это время не придёт подтверждение маршрута, при новых RIP-рассылках запись помечается как недействительная - в RIP IP рассылки каждые 30 секунд. TTL задается $30 \text{ с} \cdot 6 = 180 \text{ с}$. Через 180 с маршрут помечается как недействительный. Такая ситуация возникает, если МШ, к которому была подключена данная сеть, неработоспособен.

2. Указание специального расстояния для сети, которая стала недоступна. Используется если МШ работоспособен, но подключенная к нему сеть отказала. Тогда он указывает расстояние до сети 16 хопов (бесконечность).

Область применения протокола RIP ограничена сетями диаметром не больше 16 хопов. При использовании сетей большего размера сеть разбивается на несколько сетей с диаметром <16.

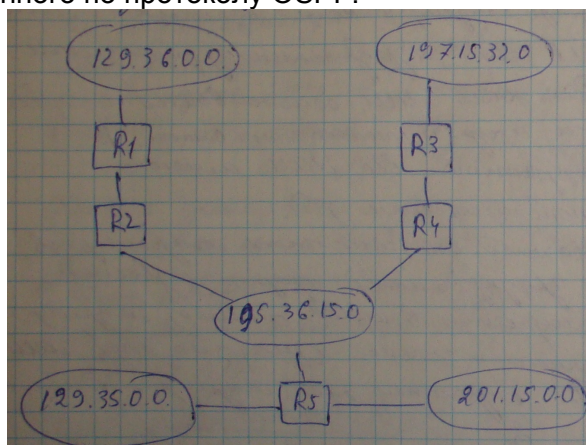
Протокол OSPF

OSPF - Open Shortest Path First. Появился в 1991 году. Ориентирован на большие (>16 хопов) сети. Выбирает лучший кратчайший маршрут. OSPF предполагает построение большой сети. Этот протокол осуществляет логическое разбиение большой сети на области.

Построение таблицы МШ можно разделить на два крупных этапа:

1. Каждый МШ строит граф связей в котором вершины - МШ и IP-сети. Ребра - интерфейсы МШ. Для этого МШ обменивается с соседями информацией о топологии сети. В рез-те все МШ имеют топологические базы данных.
2. Нахождение оптимальных маршрутов по графу до каждой известной ему сети. Но в каждом оптимальном маршруте запоминается только первый шаг до следующего МШ. То есть строится одношаговая таблица маршрутизации. Определение оптимального маршрута - сложная задача. При этом используется итеративный алгоритм Дейкстры. После построения таблицы МШ необходимо отслеживать изменения в сети, но при этом OSPF не обменивается полной информацией (как RIP).

Пример графа, построенного по протоколу OSPF:



Протокол OSPF распространяет сообщения двух типов - МШ-МШ и МШ-сеть.

Вместе с IP-адресом сети передаётся её маска.

Каждая связь характеризуется метрикой (расстоянием). OSPF применяет стандартные значения метрики, в которой отражается производительность промежуточных сетей:

-Ethernet: 10 единиц (100 нс)

-FEth: 1 единица (10 нс)

-канал T1: 65 единиц

OSPF разрешает хранить в таблице маршрутизации несколько маршрутов одной сети.

Недостаток OSPF - большая вычислительная сложность - растет с увеличением размера сети. Для этого OSPF использует отдельные области сети. В каждой - свой граф связи.

Между областями - связь через пограничные шлюзы.

Лекция 21

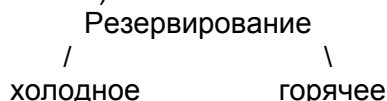
Классификация МШ по областям применения

МШ -мощное вычислительное устройство со скоростью внутренней шины 600-2000 мбит/с. Это ОС реального времени.

МШ поддерживает обычно один или несколько протоколов сетевого уровня: IP, IPX, DecNET.

По области применения МШ делятся на следующие классы:

1)магистральные (backbone routers): для построения централизованной сети корпорации. Она может состоять из большого числа ЛВС в разных зданиях с различными технологиями. Это наиболее мощное устройство - несколько млн пакетов/с. Обладает несколькими интерфейсами. Часто МШ строится по модульному принципу с соответствующим количеством модулей (слотов) - до 14. В этом типе МШ предусмотрена высокая надежность (резервирование).



При холодном резервировании работает только основной канал, при горячем - основной и резервный работают параллельно.

Примеры магистральных МШ:

-BCN (Backbone Concentrator Node)

-Cisco 7500, Cisco 12000

2)МШ региональных отделений

Соединяет региональные отделения между собой и с центральной сетью. В каждом отделении своя ЛВС, то есть, упрощенный вариант магистральной ЛВС. Максимальное количество слотов: 4-5. Менее скоростные интерфейсы.

Примеры:

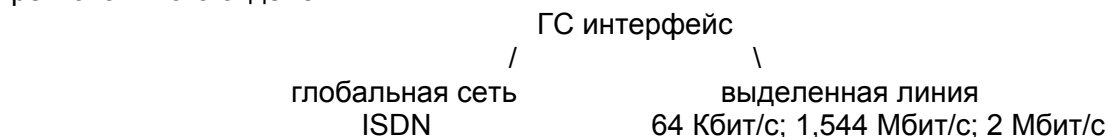
-BIN, ASN фирмы Nortel Networks

-Cisco 3600; Cisco 2500

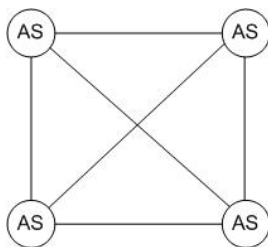
Это самый обширный класс устройств

3)МШ удаленных офисов

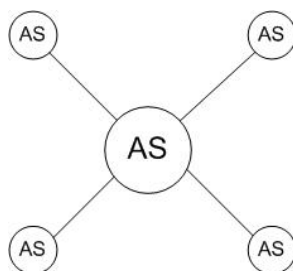
Соединяют единственную ЛВС офиса с центральной сетью или с сетью регионального отделения.



Технология "точка-точка"



Количество связей равно $n(n-1)/2$, т.е. оно растёт пропорционально квадрату числа АС. Поэтому при большом количестве АС используется другая технология - ГС:



Примеры:

-Cisco 1600

-Office Connect фирмы 3COM

4)МШ ЛВС (коммутаторы 3-его уровня)

Используются для разделения крупных ЛВС на подсети. Часто используются в составе VLAN. Имеют высокоскоростные порты (не менее 100 Мбит/с)

Представляет собой КМ-МШ (на аппаратном уровне - свитч, на программном - роутер)

+: работает на порядок выше, чем МШ

Примеры:

-Core Builder 3500 (3COM)

-Cisco 3560

Основные технические характеристики МШ

Соответствуют основному назначению МШ.

1)Перечень поддерживаемых сетевых протоколов.

Магистральные МШ должны поддерживать большое количество протоколов, чтобы обеспечивать трафик всех существующих на предприятии сетевых технологий.

Если центральная сеть образует отдельную АС, то необходимо поддерживать в ней протоколы маршрутизации BGP (EGP). Программное обеспечение строится по модульному принципу. Т.е. имеется возможность добавлять необходимые модули. Обычно поддерживаются сетевые протоколы IP, IPX, DecNet и др. Протоколы маршрутизации: IPRIP, IPXRIP, OSPF, EGP, BGP.

2)Перечень поддерживаемых интерфейсов локальных и глобальных сетей (ЛВС и ГВС)

Для ЛВС: интерфейсы физического и канального уровней сетей: Eth, FEth, TR, FDDI, AnyLAN, ATM.

Для ГВС: это интерфейсы физического уровня для связи с аппаратурой передачи данных.

Поддерживаемые интерфейсы: RS-232C, RS449/422 V.35 (до 6 Мбит/с), ASSI (52 Мбит/с), T1/E1, T3/E3, BRI, PRI (сети ISDN)

Поддержка глобальных технологий: X.25

3)Общая производительность МШ

Зависит от производительности используемых процессоров и производительности интерфейсов.

-От нескольких десятков тысяч пакетов/с

-От нескольких миллионов пакетов/с

а)Производительность магистральных МШ: несколько млн пакетов/с

б)МШ удаленных офисов: до 30 тысяч пакетов/с

в)МШ региональных отделений: до 1 млн пакетов/с

Наиболее производительные МШ - коммутаторы 3-его уровня, т.к. большинство функций в них исполнено аппаратно.

Корпоративные модульные концентраторы

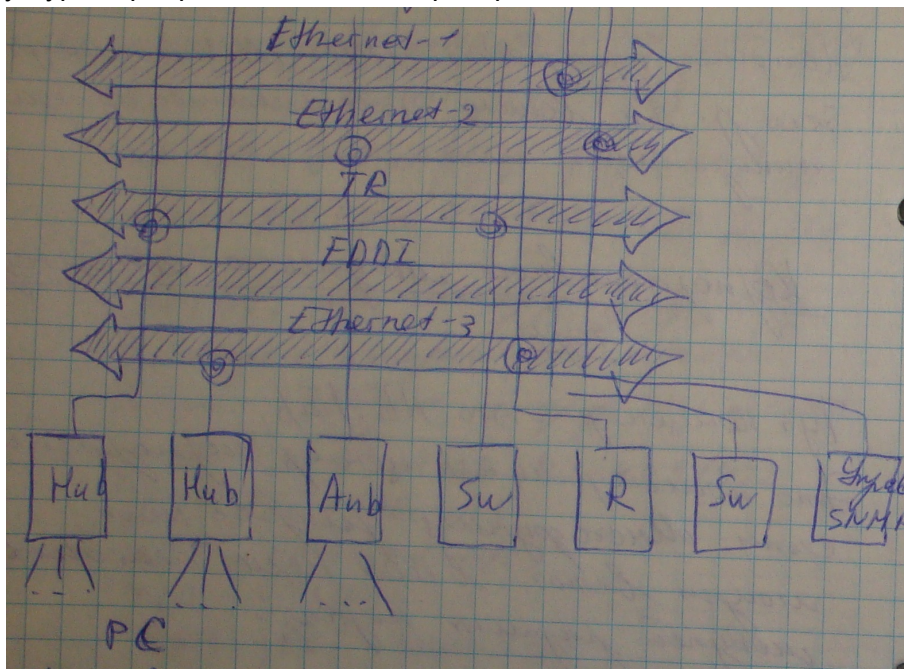
Концентратор здесь - НЕ хаб. Это коммуникационный центр корпоративной сети.

Многофункциональное устройство, которое может включать в себя несколько десятков модулей различного назначения:

- хабы различных технологий
- свитчи
- маршрутизаторы

Это позволяет централизованно объединить большое количество PC, что очень удобно в корпоративной сети. Модульный концентратор масштаба предприятия обладает набором шин высокой производительности и объединяет различные модули с высокой скоростью. Основная цель концентратора - получение настраиваемой конфигурации связи сети.

Пример: структура корпоративного концентратора:



Каждый из модулей имеет интерфейс для подключения к скоростным шинам. Конкретное подключение устанавливается через порт управления. Шины имеют скорость >10 МБит/с

Лекция 22

Трафик:

раньше 80/20, сейчас - 20/80 (слева - внутри МШ, справа - на выходе на внешнюю сеть)

Используются коммутаторы 3-его уровня.

Стирание грани между МШ и КМ

Классический КМ - это устройство, принимающее решение о продвижении пакетов на

основе MAC адресов (2 уровня). А МШ - на основе заголовков 3-его уровня (сетевого), то есть IP адресов. До 90-ых годов работало правило 80/20 - 80 на КМ и 20 на МШ. Это соответствовало производительности устройств. Но с конца 90-ых стало 20/80 и началось резкое противоречие между производительностью и трафиком. Дело осложняется тем, что в ГС резко увеличился трафик за счёт передачи мультимедийной информации. Встала задача - повысить производительность МШ. Для этого используются 2 решения:

- 1) Отказ от МШ
- 2) Увеличение производительности МШ

1) Отказ от МШ:

Применение МШ только там, где это остро необходимо - между ЛВС и ГВС (шлюз), для соединения сетей крупных размеров (200-300 РС).

Применение МШ в сети имеет преимущества:

- надёжная изоляция больших сетей от широковещательного шторма.
- возможность защиты на сетевом и транспортном уровне от несанкционированного доступа.

- сеть на КМ имеет ограниченные размеры (200-300)

Таким образом, в сети должны быть предусмотрены функции маршрутизации.

2) Наделение КМ функциями МШ (КМ третьего уровня):

Представляет собой КМ-МШ (на аппаратном уровне - свитч, на программном - роутер)

Скорость: до 5-8 млн пакетов/с

Преимущества:

- одна система буферизации
- функции МШ реализованы на аппаратном уровне.

Если IP адрес совпадает - используется КМ

Если IP адрес не совпадает - используется МШ

КМ 3 уровня с классической маршрутизацией

Это КМ с совмещением функций МШ двумя способами:

1) классический - МШ используется при каждой передаче пакета в другую сеть (когда IP адреса не совпадают). Иначе используется коммутация.

2) нестандартный - ускоренная МШ. Сообщения разбиваются на пакеты. Первый пакет проходит по 3 уровню, остальные - по 2 без проверки IP адреса (поскольку адресация у всех пакетов одного сообщения одна и та же). Быстрая передача. Однако, если она прервана, нужно начинать всё сначала.

КМ 3-его уровня часто применяется для VLAN.

Примеры КМ 3-его уровня с классической маршрутизацией:

LANplex 6000 (ЗСОМ)

CoreBuilder 2500 (ЗСОМ)

Маршрутизация потоков

Это второй тип КМ 3-его уровня. КМ ускоряет работу за счёт выявления устойчивых потоков и маршрутизации только первых пакетов для таких потоков.

Поток - последовательность пакетов с одинаковым IP адресом источника и получателя. Остальные пакеты (кроме первого) передаются на основе коммутации (быстро, за счёт запоминания пути прохождения первых пакетов). Защитные свойства МШ сохраняются,

т.к. первые пакеты проверяются на сетевом уровне.

Маршрут может быть помечен на канальном уровне (MAC адрес пути)

1) Определить долговременный поток (и пускать только его) - определяется по IP адресу.

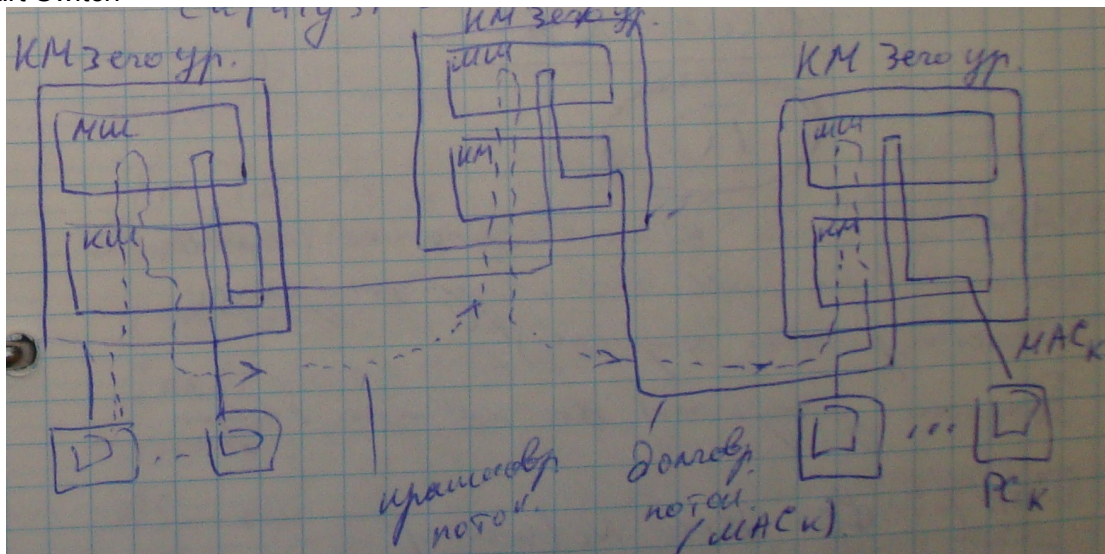
2) На основании какой информации первый МШ узнает MAC узла назначения? Протокол ARP не действует - т.к. есть несколько промежуточных сетей. Разные компании используют разные подходы. Используются специальные протоколы, по которым промежуточные МШ запрашивают друг у друга MAC адрес узла, пока последний МШ не выясняет его с помощью ARP.

3) Теперь каждый последующий пакет имеет метку - MAC адрес PC назначения и проходит по данному маршруту на втором уровне (быстро).

Примеры:

-Catalyst 5000 отCisco

-Smart Switch



Долговременные потоки обрабатываются быстро. После выявления долговременного потока и маршрутизации первый КМ выполняет нестандартную операцию - он помещает в кадр не MAC адрес следующего МШ, а MAC адрес узла назначения в качестве метки маршрута. Теперь кадр передается на уровне коммутации с использованием этой метки. Преимущество: скорость передачи на канальном уровне значительно выше, чем на сетевом.

Недостатки:

-имеется лишь один маршрут, и если он разорван, приходится все начинать заново (отсутствует резервирование)

-используется только один канал передачи, нет возможности распараллеливания.

Лекция 23

Глобальные сети

WAN (wide area network) - сети, включающие большое количество абонентов на больших территориях (область, регион, страна). Для них характерны большие затраты на каналы связи.

Глобальная сеть создается крупными телекоммуникационными компаниями, которые предоставляют платные услуги своим абонентам.

Оператор сети - компания, поддерживающая нормальную работу сети.

Поставщик услуг (провайдер) - компания, оказывающая платные услуги.

Владелец, оператор и поставщик могут объединяться в одной компании.

Иногда глобальная сеть создается крупной компанией. Такая глобальная сеть называется частной.

Глобальная сеть:

1)вычислительная

2)телеграфная

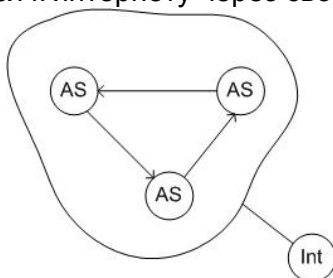
3)телефонная

Так как ГС дороги - тенденция использовать для данных любых типов ГС.

Главными составляющими ГС являются АС. АС - система IP сетей и маршрутизаторов, управляемых 1 или несколькими операторами, использующими единый протокол маршрутизации (например, RIP). Описаны в стандарте RFC 1930, RFC 1771.

Каждая АС имеет № - 2 байта.

Несколько АС могут подключаться к интернету через своего провайдера.



Хотя существует несколько АС, поддерживающихся данным провайдером, в Internet виден только данный провайдер, именно он должен иметь зарегистрированный публичный номер АС.

Присвоение номера АС

Номера АС выделяются организацией IANA (Internet Assigned Number Authority).

Выделение номеров региональным магистральям - RIR (Regional Internet Registry)

- выделение номеров отдельными блоками. Локальные RIR - присвоение номеров

АС отдельным организациям из блока адресов, полученных от IANA. Организации, желающие получить ASN (номер АС) должны пройти регистрацию в своем локальном RIR и получить одобрение.

Номера АС: $2^{16}=65\,536$

Номера АС распределены на 2 диапазона:

1)публичные номера АС - могут быть использованы в Internet (1-64 511)

2)приватные (частные) - не имеют выхода в Internet (64 512-65 534). Используются только локально внутри организации.

Номера 0 и 65 535 не используются.

Типы АС

3 категории в зависимости от их соединения и режима работы:

1)многоинтерфейсные - имеют соединение более, чем с одним интернет-провайдером.

2)ограниченные - единственное подключение к одной внешней АС.

3)транзитные - пропускают через себя трафик сетей, подключенных к ней.

Сеть А может использовать транзитную АС для связи с В:



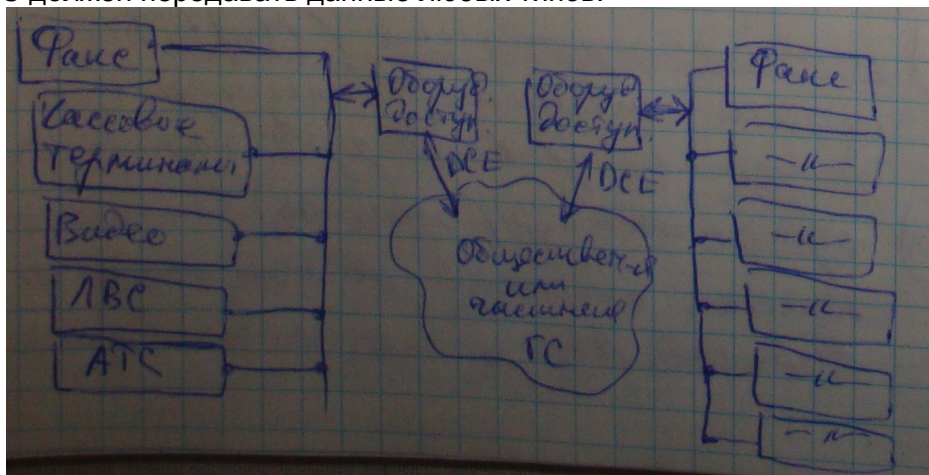
Провайдер всегда является транзитной АС. Это их основная работа - соединять различные сети.

Обобщенная структура и функции ГС

В основе работы АС и ГС один и тот же метод - коммутация пакетов. Но в ГС существенное отличие: маршрутизация основана на предварительном образовании виртуального канала.

Транспортные функции ГС

В идеале ГС должен передавать данные любых типов.



DTE - data terminal equipment

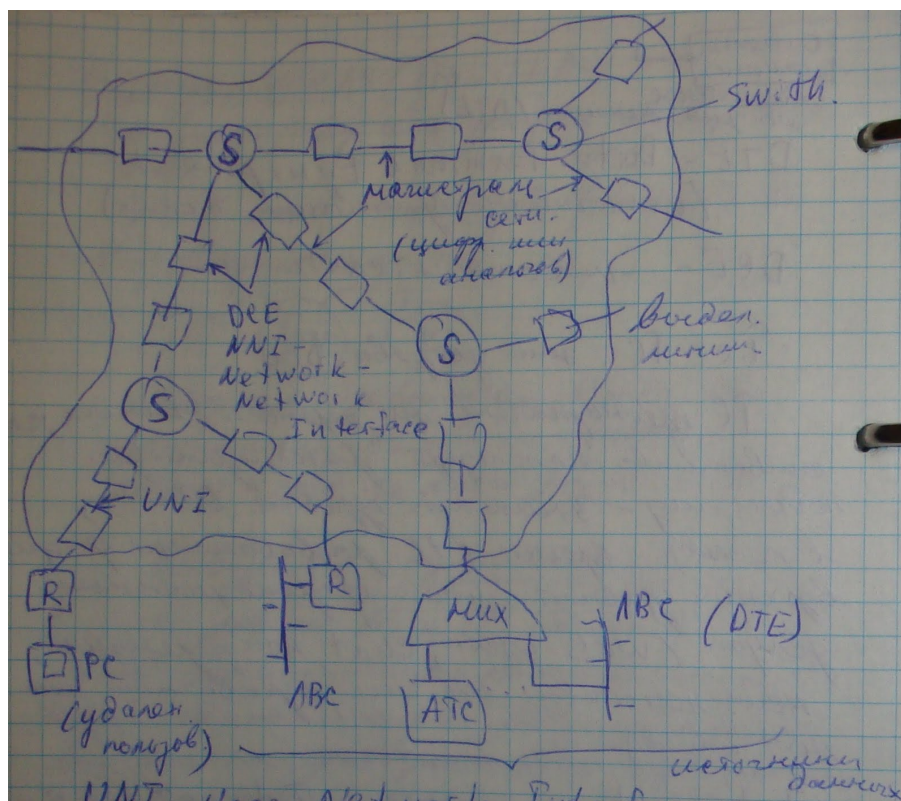
DCE - data communication equipment

ГС - устройство DCE.

ГС предназначена для переноса данных и использует транспортную подсистему - 3 нижних уровней. Однако, в последнее время в ГС развиваются функции верхних уровней - это информационные услуги (web-узлы, чат, конференции, новости, поисковые системы и т.д.)

Intranet - технологии Internet переносятся на корпоративную сеть. В результате ЛВС и ГС постепенно сближаются за счёт взаимопроникновения.

Структура ГС



UNI - User network interface

ГС построена на основе выделенных каналов связи, которые соединяют коммутаторы (на рисунке - S). Коммутаторы здесь - это центры коммутации пакетов. Коммутаторы S устанавливаются в тех географических пунктах, где требуется ответвление или слияние потоков данных, а также где возможно обслуживание.

Абоненты сети подключаются к S с помощью выделенных линий, но с меньшей пропускной способностью, чем на магистралях.

Устройство DCE обеспечивает необходимый протокол физического уровня для передачи в выделенную линию.

Есть 3 типа DCE:

- 1) Модемы - для работы с аналоговыми каналами
- 2) DSU/CSU - data(channel) service unit. Устройство обслуживания данных (канала)
- 3) Терминальные адаптеры - для работы по каналам ISDN

Лекция 24

В ГС строго описан и стандартизирован интерфейс пользователей UNI, так как пользователь должен иметь возможность подключаться к линии (цифровой, аналоговой). Протокол взаимодействия внутри сети - NNI. Он до конца не стандартизирован.

Интерфейс DTE-DCE

Интерфейс сопряжения пользователя с линией. Использует несколько стандартов физического уровня, в частности существуют две линии стандартов:

- 1) Стандарты серии V CCITT (Consultative Committee for International Telephone and Telegraph) - в настоящее время переименован в ITU - International Telecommunication

Unit

2)Стандарты EIA (Electronic Industry Association) серии RS - Recommended Standards: скорость 300 бит/с - несколько Мбит/с на расстоянии 15-20 м.

Наиболее частые интерфейсы:

1)RS-232C/V.24

первоначально 9600 бит/с на расстоянии <15 м. Для последней версии: 115 200 бит/с
2 режима работы: синхронный и асинхронный

2)RS 449/V.10/V.11

Высокоскоростной интерфейс. Имеет 2 спецификации сигнала:

а)V.10 - до 100 Мбит/с, $L \leq 10$ м

и до 10 Мбит/с, $L \leq 100$ м

б)V.11 - до 10 Мбит/с, $L \leq 10$ м

и до 1 Мбит/с, $L \leq 100$ м

2 режима работы: синхронный и асинхронный

3)V.35 интерфейс

Для синхронного подключения модемов со скоростью до 168 Кбит/с, $L \leq 15$ м

4)Интерфейс HSSI - High Speed Serial Interface

Для подключения DCE, работающего с высокоскоростными каналами: канал T3 (45 Мбит/с), SONET OC-1 (52 Мбит/с).

Только синхронный режим: 300 Кбит/с - 52 Мбит/с

Типы глобальных сетей

В предыдущем примере была показана сеть в режиме коммутации пакетов (S). Это оптимальный режим как по стоимости, так и по трафику. Куда более дешево, чем ТЛФ (телеф. каналы - коммутация каналов). Однако, сети с коммутацией каналов еще используются - это региональные сети.

Различные ГС строятся с использованием:

1)Выделенных каналов

2)Коммутации каналов(могут быть перекоммутированы на другие соединения)

3)Коммутации пакетов - наиболее благоприятный вариант.

1)Выделенные каналы.

Арендуемые каналы (leased) можно получить у телеф. компаний (ТЛФ, Ростелеком).

2 варианта использования выделенных линий:

а)Получение с помощью них территориальной сети определен. техн. (Frame relay, например). Линии используются для соединения территориально распределенных коммутац. пакетов (ЦКП)

б)Соединение линиями объединяемых ЛВС с использованием МШ или удаленных маршрутов.

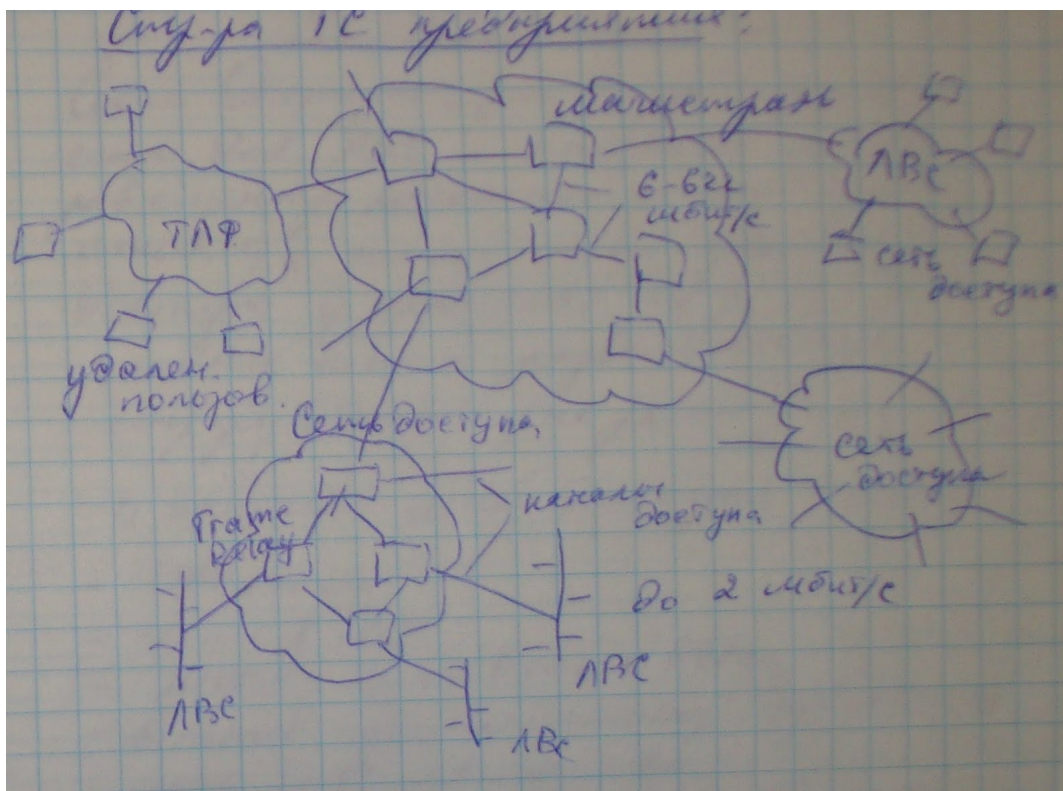
1)магистральные сети

2)сети доступа

Сети доступа объединяют удаленных региональных пользователей, а сами они объединяются магистральными сетями.

Магистральная сеть (Backbone Wide Area Network) служит для образования одноранговых связей между крупными ЛВС. Высокая пропускная способность, надежность. Скорость: 2-622 Мбит/с. Передает трафик IP,FR,ATM,X.25.

Для повышения надежности в магистральных сетях используется избыточная топология связи.



Лекция 25

Сети доступа - это территориальные сети для ЛВС и отдельных компьютеров с центральной локальной сетью предприятия. Поскольку точек удаленного доступа у предприятия может быть очень много, главное иметь разветвленную структуру доступа. В качестве сетей доступа используют:

-ТЛФ сети

-сети ISDN

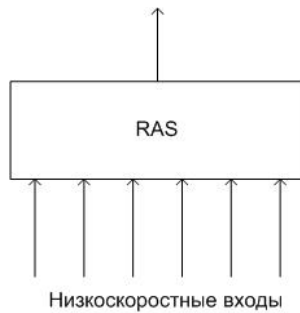
-иногда сети Frame Relay

-в последнее время используют публичную сеть Internet.

Недостаток публичных сетей - защита данных.

Программные и аппаратные средства, которые обеспечивают подключение удаленных пользователей к корпоративной сети, называются средствами удаленного доступа.

Для клиентов это модем с соответствующим ПО. Организацию массового удаленного доступа обеспечивает сервер удаленного доступа (Remote Access Server - RAS) - программно-аппаратный комплекс, соединяющий функции МШ и шлюза. RAS имеет много низкоскоростных входов и один выход:



ГС на основе выделенных линий

Абонентами такой сети могут быть как отдельные пользователи, так и ЛВС и даже АС. Арендуются выделенные линии у компании (например, у ТЛФ)

Делятся на:

-аналоговые - FDM

-цифровые - TDM

Применяется аппаратура уплотнения. На аналоговых линиях физического и канального уровня не стандартизованы.

В цифровых линиях используется стандарт 6.703 (канальный уровень PPP, HDLC)

Аналоговые выделенные линии

Предоставляют для пользователя двухпроводные или четырехпроводные окончания.

То есть используются 2 группы аналоговых выделенных линий:

-ненагруженные (полоса пропускания не ограничена средствами АТС)

-нагруженные

Ненагруженные используют только саму линию для передачи данных в кадрах не используют аппаратуру телефонных станций. Т.е. у ТЛФ берут только провод. f - до 1 МГц (высокая скорость по сравнению с нагруженной).

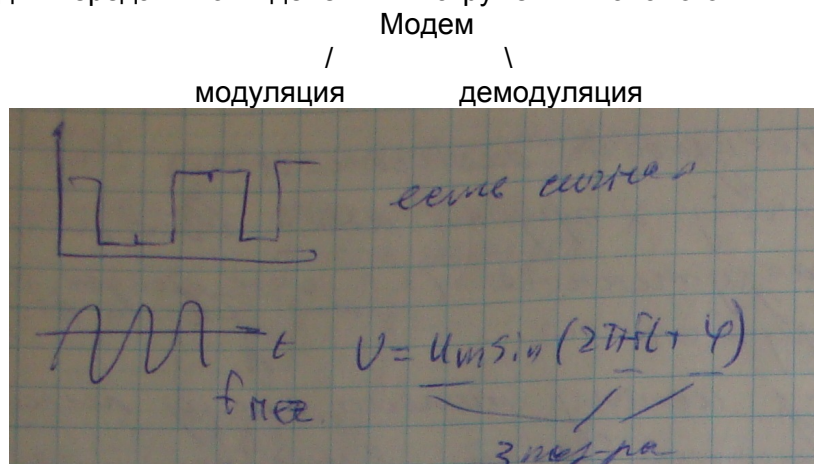
Нагруженная линия использует аппаратуру АТС. Нагруженные телеф. каналы:

-тональной частоты, полоса: 3,1 КГц

-широкополосный канал - состоит из 12 тональных. 48 КГц.

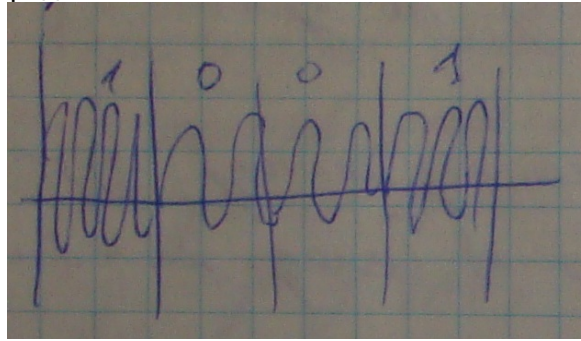
Модемы для выделенных каналов

Используются для передачи по выделенным нагруженным аналоговым линиям



Чаще всего используется частотная модуляция, т.е. аналоговый сигнал модулируется по

какому-то принципу и передается по линии.



Модемы используют следующие протоколы: CCITT серии V.

Эти протоколы делятся на 3 группы:

- 1)станд., определ. скорость передачи и метод кодирования
- 2)станд., определ. исправление ошибок
- 3)станд., определ. сжатие данных

Режимы работы:

- только асинхронный режим (передача по байтам: стартовый бит, информационный бит, четн. бит, стоповый бит)
- синхронный и асинхронный
- синхронный (более скоростной, передача идёт целыми блоками)

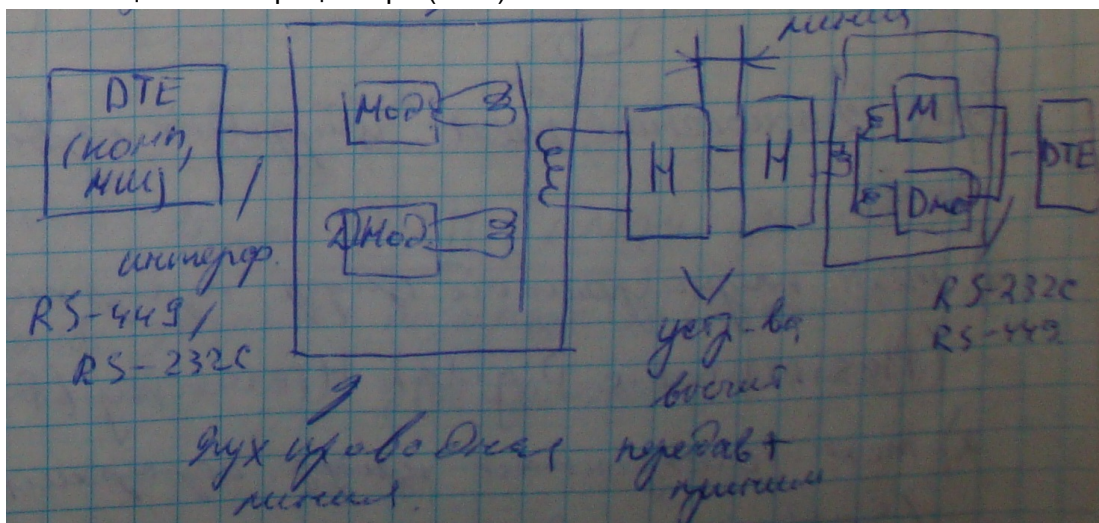
Только асинхронные модемы - низкоскоростные (до 1200 бит/с)

Синхронные и асинхронные: 4-х проводная линия, дуплекс.

Стандарты:

- v.26 2400 бит/с
- v.27 4800 бит/с
- v.29 9600 бит/с
- v.32 19200 бит/с

Дуплексный режим работы по двухпроводной линии осуществляется путем одновременной передачи в обоих направлениях и вычитанием передаваемого сигнала из смеси с помощью сигн. процессора (DSP)



Надо выделить принимаемый:

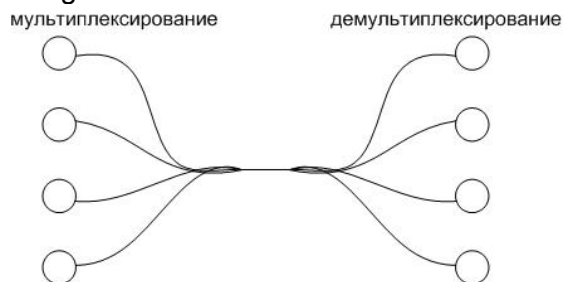
(передаваемый+принимаемый)-(передаваемый)=принимаемый

Для вычитания используется процессор DSP. Вычитание - весьма сложная задача.

Цифровые выделенные линии

Образуются с помощью постоянной коммутации в первичных сетях, построенных на базе коммутации аппаратуры, работающей на принципе разделения канала по техн.

TDM - time division multiplexing



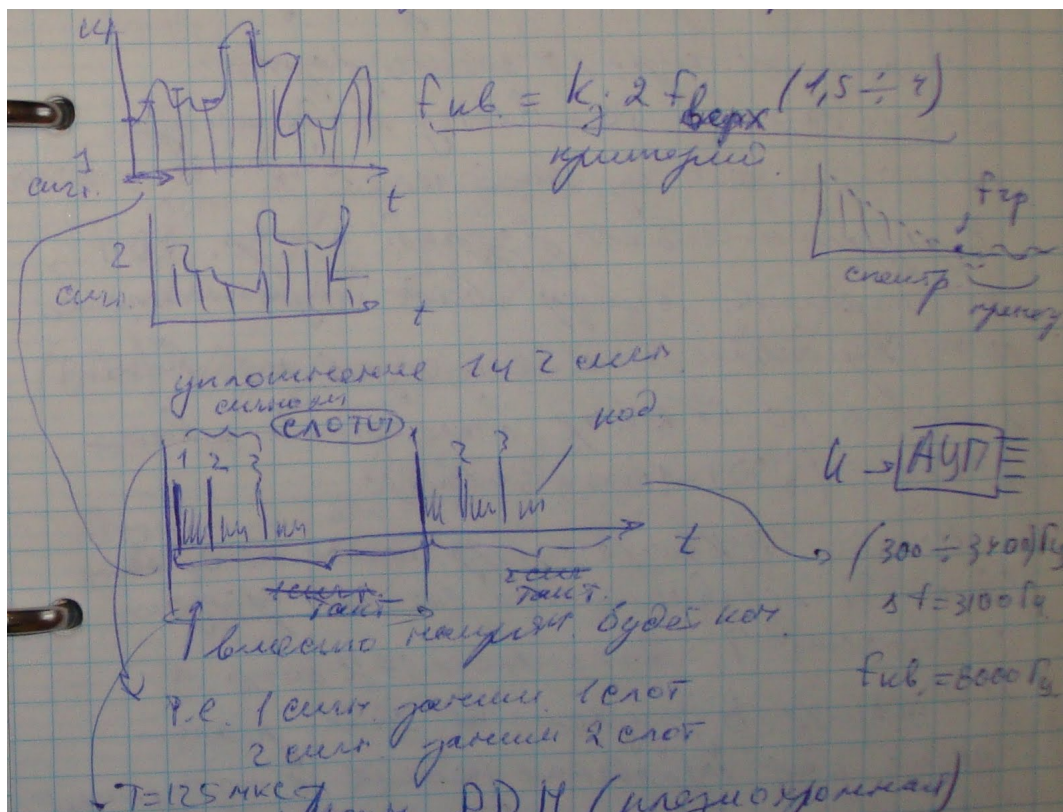
Существует 2 поколения техн. цифровых первичных сетей:

1) технология плезиохронной цифровой иерархии (Plesiochronous Digital Hierarchy - PDH)

2) технология синхронной цифровой иерархии (Synchronous Digital Hierarchy - SDH) или SONET - Synchronous Optical Network

Общий принцип:

Используется временное уплотнение. Аналоговый сигнал представляется в цифровом виде.



Технология PDH (плезиохронная)

Появилась значительно позднее FDM (частотного уплотнения). FDM имеет много недостатков.

Лекция 26

В конце 60-ых годов была разработана цифровая аппаратура мультиплексирования и коммутации. Мультиплексирование - объединения различных данных в одну выделенную линию. В результате была создана технология PDH, которая позволяет в цифровом виде мультиплексировать, передавать и коммутировать на выходе $T_1=24$ канала по 64 Кбит/с с частотой $f_{кв} = 8$ КГц.

Меньше 64 Кбит/с цифровой поток не бывает. Однако, T_1 - сравнительно слабая пропускная способность ($24 \text{ канала} \cdot 64 \text{ Кбит/с} = 1,544 \text{ Мбит/с}$). В результате была реализована идея образования канала с иерархией скоростей - 4 канала T_1 , объединенных в канал следующего уровня T_2 ($T_2=4 \cdot T_1=6,312 \text{ Мбит/с}$). $T_3=7 \cdot T_2=44,738 \text{ Мбит/с}$.

Аппаратура T_1 , T_2 , T_3 образует иерархическую сеть с магистральными каналами трёх скоростей.

С середины 70-ых годов эти каналы стали сдавать в аренду (для передачи мультимедиа).

Технология цифровой иерархии стандартизирована комитетом CCITT (или ITU)

Для обозначения иерархии скоростей: DSh - digital signal.

Иерархия цифровых скоростей

Америка:

Обозн. скорости	Кол-во элем. голосов. каналов	Кол-во каналов пред. уровня	Скорость (Мбит/с)
DS0	1	1	0,064
DS1	$T_1 \ 24$	24	1,544
DS2	$T_2 \ 96$	4	6,312
DS3	$T_3 \ 672$	7	44,736
DS4	$T_4 \ 4032$	6	274,176

Европа:

Кол-во элем. голосов. каналов	Кол-во каналов пред. уровня	Скорость (Мбит/с)
1	1	0,064
E1 30	30	2,048
E2 120	4	8,468
E3 480	4	34,368

E4 1920	4	139,264
---------	---	---------

Как физически реализовать сжатие 24 каналов в 1?

Ответ T1 заносится в память и считывается гораздо быстрее, но происходит задержка на 1 такт. Скорее всего надо использовать о/в, чтобы соблюсти полосу пропускания.

Преобразование канала T1 для данных использует 23 канала, а 24ый - для служебных целей (восстановления, синхронизации). Технология цифровой иерархии описана в стандарте G.700 - G.706

Любой клиент может арендовать любое количество каналов T1, T2, T3, T4, либо несколько элементарных каналов DS0. Тогда такой канал называется дробным (fractional) - из 24 можно арендовать один канал DS0.

Физический уровень технологии PDH

Используются кабели - витая пара, коаксиальный и о/в. 2 витые пары (2UTP) с разъема RJ-48 для дуплексного режима 1,544/2,048 Мбит/с.

Биполярное кодирование B8ZS.

Для восстановления сигнала на каждые 1800 м устанавливаются регенераторы.

Коаксиальные кабели поддерживают 1 канал T2/E2 и 4 канала T1.

Начиная с канала T3 - о/в.

Физический уровень описан стандартом G.703

Недостатки технологии PDH

-сложность операций мультиплексирования и демultipлексирования

-отсутствие развитых процедур контроля и управления сетью

-отсутствие процедур отказоустойчивости

-низкие по современным требованиям скорости иерархии - современная о/в линия позволяет значительно увеличить скорость.

Эти недостатки устранены в технологии SDH.

Лекция 27

Технология синхронной цифровой иерархии SONET/SDH

SONET/SDH - Synchronous Optical Network / Synchronous Digital Hierarchy

Цель - передавать трафик T1-T4 через ВОЛС, обеспечение иерархии скоростей, продолжающую PDH. При достижении скорости до нескольких Гбит/с, в стандарте G707-6709. Стандарты SDH и SONET стали совместимы и используют единую иерархию скоростей.

Иерархия скоростей SONET/SDH

SDH	SONET	Скорость, Мбит/с
-	STS-1; OC-1	51,840
STM-1	STS-3; OC-3	155,520
STM-3	STS-9; OC-9	466,560
STM-4	STS-12; OC-12	622,080

STM-6	STS-18; OC-18	933,120
STM-8	STS-24; OC-24	1244,0
STM-12	STS-56; OC-56	1866,0
STM-10	STS-48; OC-48	2488

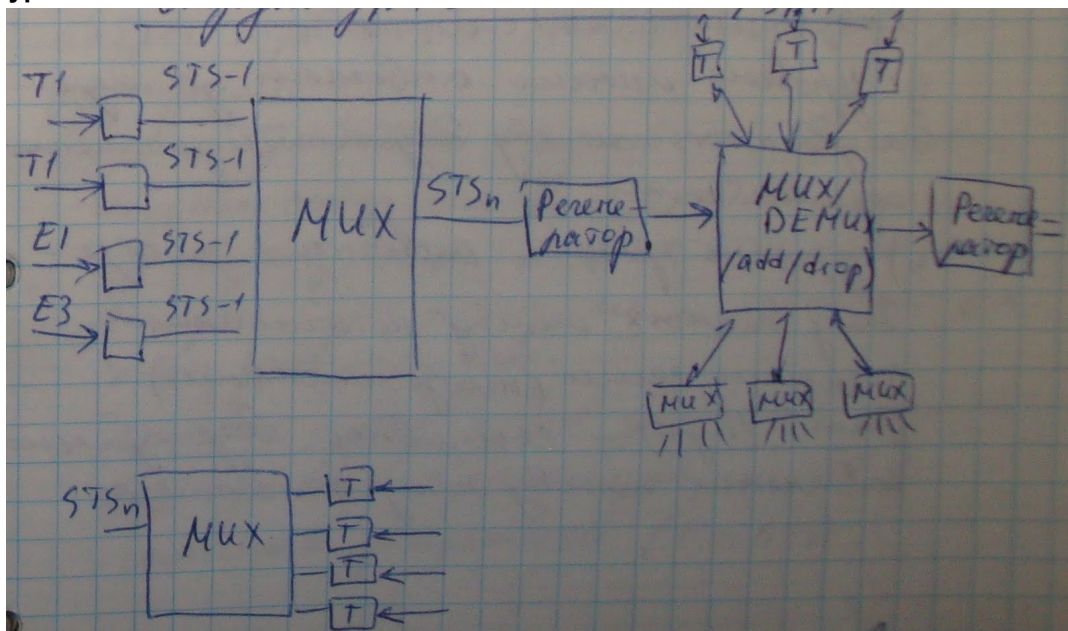
Скорости кратны STS-1. Кратны элементарной скорости 0,064 Кбит/с

Кадры данных технологии SONET

Форматы данных, начиная с STS-3, совпадают с STM-1. Кадры передают большое количество служебной информации для:

- 1) мультиплексирования/демультиплексирования потоков add/drop. Слоты выделяются динамически.
- 2) Обеспечение отказоустойчивости сети
- 3) Поддержка операций контроля и управления сетью

Структура сети SONET/SDH



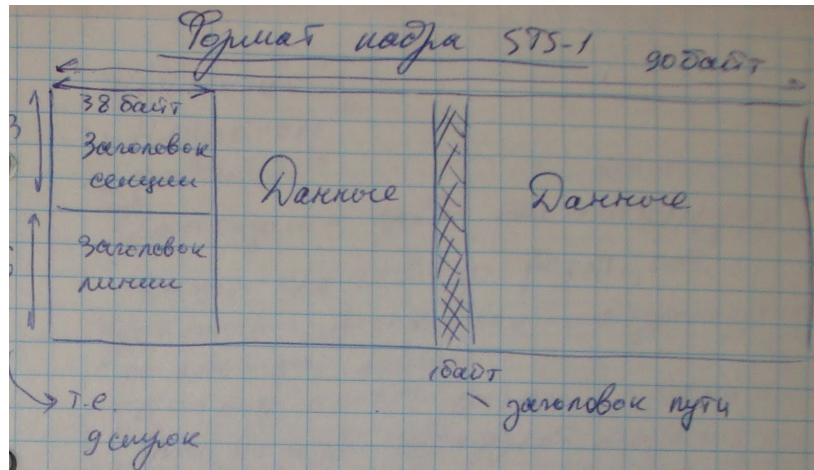
T - терминалы, принимающие пользовательские данные от канала PDH

Мультиплексоры принимают данные от терминала и преобразуют их в кадры более высоких иерархий STSn.

Mux/demux/add/drop - принимают входные потоки или выделяют данные. Регенераторы - для восстановления мощности и формы сигналов.

SDH состоит из протоколов четырёх уровней:

- 1) физический - описывает кодирование бит с помощью модуляции света по коду NRZ
 - 2) уровень секций - каждый отдельный отрезок о/в. Заголовок секций: 11110110 00101000. Следующий байт - секция
 - 3) уровень линии отвечает за передачу данных между двумя мультиплексорами сети
 - 4) уровень тракта отвечает за передачу данных между конечными точками сети.
- Тракт (путь) - составное виртуальное соединение между пользователями.



Всего: $90 \times 9 = 810$ байт

Кадры технологии SONET/SDH принято представлять в виде матрицы из 9 строк и 90 столбцов. Кадры передаются последовательно - строка за строкой. Первые 3 байта - служебные. Заголовок секции содержит данные для контроля и реконфигурации уровня линии.

Заголовок пути - для указания места виртуальных контейнеров, слотов с помощью указателей.

Устройства DSU/CSU для подключения выделенными каналами

DSU - Data Service Unit; CSU - Channel Service Unit - устройство обслуживания данных/каналов

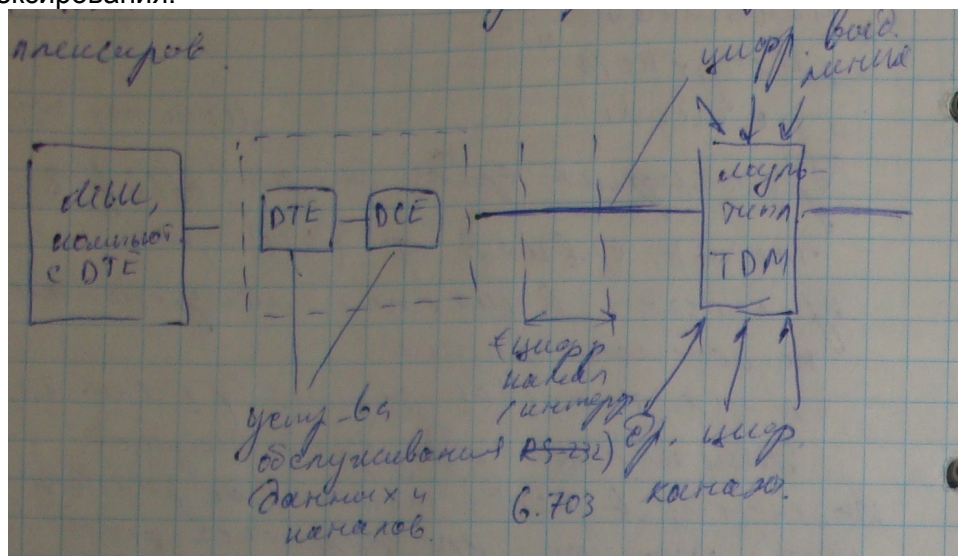
Связь PC или МШ с цифровой выделенной линией осуществляется с помощью пары устройств DSU/CSU.

DSU - преобразует сигнал от источника DTE по интерфейсу, например, RS-232C/RS-449

DSU выполняет синхронизацию и формирование кадров T1/E1

CSU - более узкие функции - создает оптимальные условия для передачи/создает особые характеристики в линии

DSU/CSU обычно исполняются в виде общего устройства и включают в себя устройства мультиплексирования.



Протоколы канального уровня для выделенных линий

Выделенные линии - для соединения ЛВС или отдельных РС. Бывают двух типов:

- 1) Аналоговая с определенной полосой пропускания (требуется модем - они задают соответствующий протокол физического и канального уровня)
- 2) цифровая выделенная линия. Если цифровая линия соединяет отдельные сети через МШ (технологии Eth, TR, FDDI), используются протоколы канального уровня для вышеуказанных технологий. Если соединяются сети по глобальным выделенным линиям, то протоколы локальных сетей не могут быть использованы, поэтому используются специальные протоколы. Например, протокол SLIP - протокол последовательной связи IP пакетов.

Лекция 28

Отказоустойчивость сети SONET/SDH

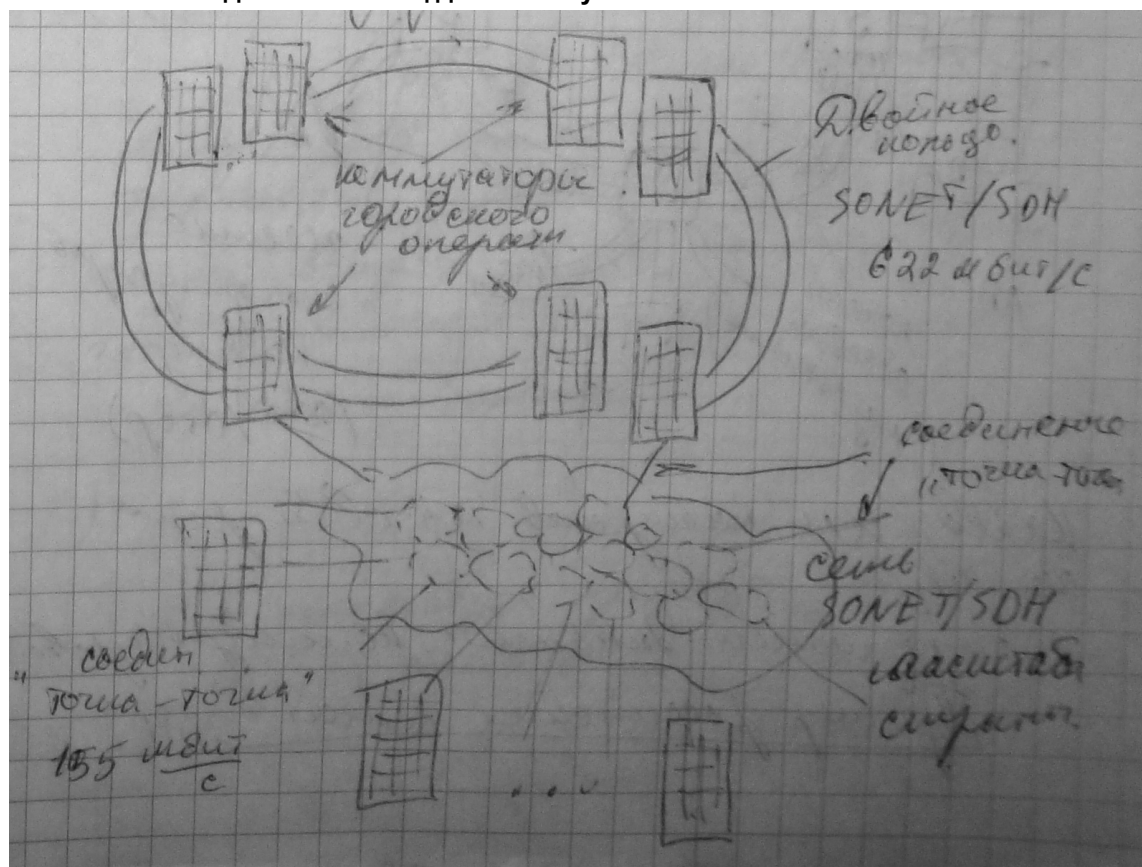
Встроена в протокол сети SONET/SDH – автоматич.защитное

Automatic Protection Switching (APS)

Сущ. 2 способа работы (по отказности):

1. защита по схеме 1-1: кажд.рабоч.волокно имеет защитное резервное волокно.
2. 1 - ∞. Для защиты n волокон используется только одно резервное.

Использование двойных колец для отказоустойчивости SONET/SDH:

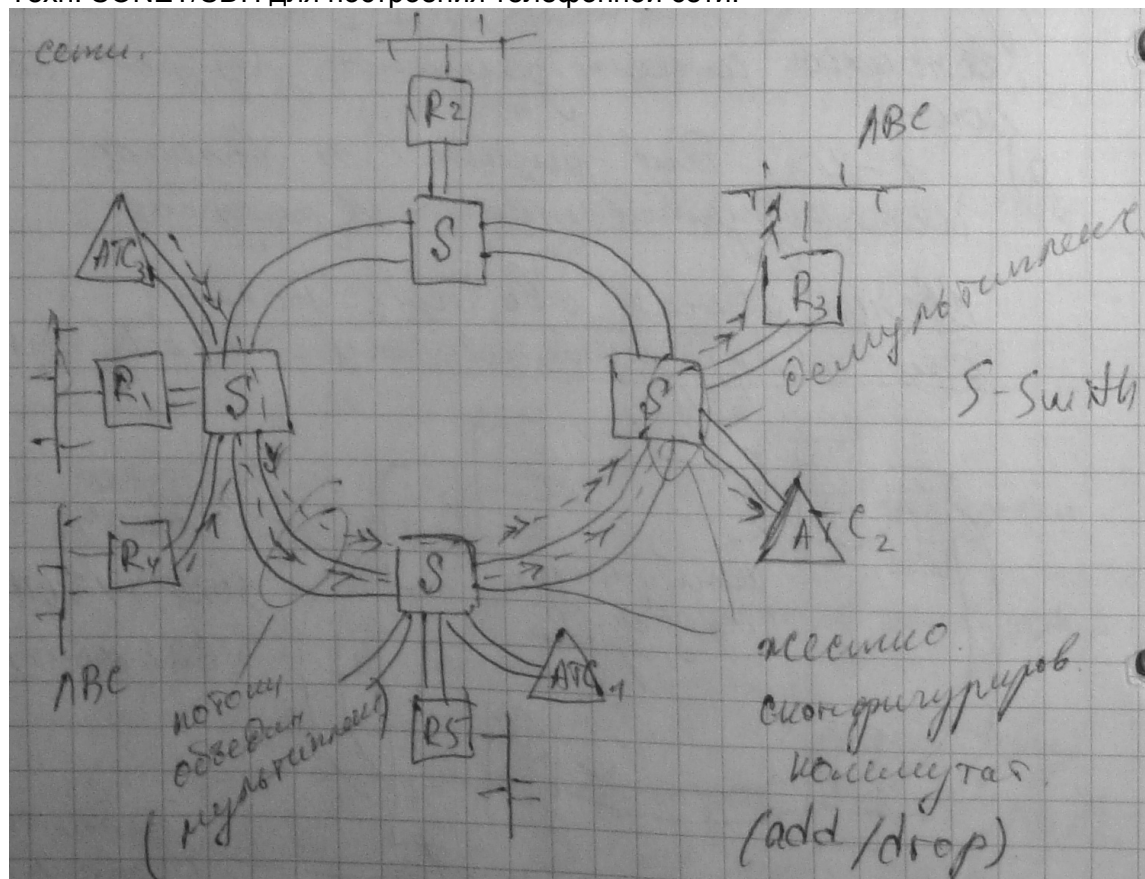


Применение цифровых первичных сетей

Техн. PDH и SDH используются для построения публичных и корпоративных сетей на базе выделенных цифровых каналов. Эти каналы соединяются МШ на границах ЛВС (шлюзы).

Телефонные АТС тоже могут использоваться

Техн. SONET/SDH для построения телефонной сети:



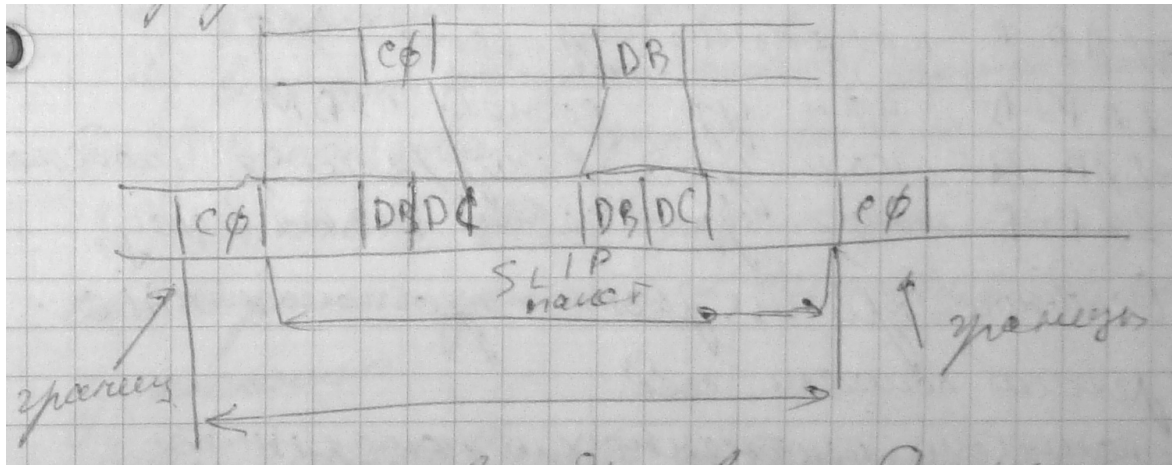
SLIP-Serial Line IP

Протокол SLIP поддерживает ОС ПО ПК.

Функции SLIP:

1. распознавание начала и конца пакета в потоке бит, передав. по выделенному каналу.

(-)1 Работает только с пакетами IP. Для обозначения границ пакета используется разделительный символ End (Cøh)



Т.е. если в кадре в поле данных встречается сф, то, чтобы не путать с границей, заменяем на DB, DC, а если встречается в поле данных DB DC, то заменяется DB. Из-за этого на 4 байта больше.

(-) 2: отсутствуют процедуры контр.и коррекц. ошибки.

SLIP – compressed SLIP
Поддерживается сжатие данных.

Протоколы семейства HDLC.

HDLC – High-Level Data Control (ISO).

высокоуровнев.соед.протокол.

Это семейство протоколов, которое используют:

- LAP-B – канальный уровень сетей X25
- LAP-D – кан.ур. сетей ISDN
- LAP-M – кан.ур. синхр\асинхр модемов
- LAP-F – канн.ур.сетей Frame Relay

Основные принципы работы протокола HDLC:

1. режим логического соединения
2. контроль искаженных и потерянных кадров
3. управление графиком по командам

RR/RNR (Reciever Not Ready)

В настоящее время протокол HDLC вытесняется протоколом «точка-точка» PPP (Point-to-Point Protocol), т.к. BER= 10⁻⁹ в наст. вр., то контроль искаж. и потер.кадров на.

Лекция 29

Протокол PPP

Принципы:

1. переговорное принятие параметров соединения.

В корпоративной сети могут отличаться:

- размеры буферов конечных систем
- ограничения на размеры пакетов
- списки поддерживаемых протоколов
- использование физич.линии.

В протоколе PPP существует набор стандартных установок, действующих по умолчанию.

1. При установлении соединения используется набор стандартных установок; по умолчанию – они используются в первую очередь. Если они устраивают, то принимаются окончательно. Если не устраивают, то принимается второй этап.

Протокол, по которому устанавливаются параметры соединения, называется: Link Control Protocol (LCP)

Протокол, устанавливающий, какие протоколы будут участвовать в соединении, называется Network Control Protocol (NCP).

Для аутентификации – Password Authentication Protocol (PAP) – передает пароль по линии связи с целью аутентификации.

Другой протокол для аутентификации – CHAP – Challenge Hand Shake Authentication Protocol – более безопасный (не передает ключ по линии).

2. Многопротокольная поддержка.

Лекция 30

Глобальные связи на основе связей с коммутацией каналов.

Телефонные сети разделяются на 2 вида:

- аналоговые
- цифровые (ТЛФ сети, в которых на абонент. оконч. инф. представляется в цифровом виде).

К цифровым сетям относятся:

- телеф. сети Switched 56 – коммутир.канал 56 кбит\с.
- цифр.сети ISDN – Integrated Service Digital Network (с интеграц.услуг). для передачи голоса, компют.данных.

Основной режим работы ISDN – коммут.каналов.

Организация аналогов.телеф.сетей.

Наиболее популярн.коммут.каналов:

PSTN – Public Switched Telephone Network.

9600 бит\с – пропускная способность

Использ.коммут.линии с модемами

max 56 кбит\с

Доступ по сети имеет наименование dial-up access. Его характеристики:

1. прямое соединение через телеф.коммут.(300/3400)Гц
2. импульсный набор – 10 Гц; тональный набор – 10 Гц, представлен 2 синусоид.сигналами.
3. недостаток заключ.в том, что хранение данных не предусмотрено.

В телеф. сетях использ.2 принц коммутации:

- аналог FDM
- цифр TDM

Модемы для работы на аналог.коммутир.линиях.

Для работы по коммут.каналу предусмотр.ряд стандартов:

- V.21 дуплексная асинхр.передача со скоростью 300 бит\с
- V.22 дуплекс.синхр\асинхр передача со скоростью 1,2 кбит\с
- V.22bis –“- 1,2 и 264 кбит\с
- V.32bis –“- до 4,8/9,6 кбит\с
- V.34+ –“- до 33,6 кбит\с

Использ.система команд для работы с модемами – ф. Hayes (протокол V.42)

Перед началом работы приустан.соед.модемы «договариваются» о параметрах соед.(подбор скорости передачи).

В модемах широко использ.сжатие данных с коэф. 1:4 и 1:8.

V.90 – до 56 кбит\с

Сети ISDN

Использ. полностью цифр.каналы.

В 1980г вышел стандарт G.705

Внедрение сетей – с конца 80х и по сей день. В нашей стране почти нет.

Архитектура ISDN содержит несколько служб:

1. некоммутир ср-ва(выделение цифр.канала)
2. коммутир. ТЛФ сеть общего назнач.
3. сеть передачи данных с коммутацией каналов
4. сеть передачи данных с коммут.пакетов
5. сеть передачи данных с трансляцией кадров (Frame Relay)
6. ср-ва контроля и упр работой сети

начальная базовая скорость 64 кбит\с (DS0) для передачи голоса.

Пользоват.интерф. ISDN сети.

Предусм.набор станд. услуг для пользов.(станд.интерфейсы).

Пользов.интерф.основ.на каналах 3 типов:

- канал типа B – скор.передачи 64 кбит\с
- канал типа D – скор.передачи 16 и 64 кбит\с(для организ.соед.сети)
- канал типа H – скор.передачи 384 кбит\с(H0), 1536 кбит\с (H11), 1920 кбит\с (H12)

Канал типа B – низкоскор.канал с разделением по времени (TDM).

Канал типа D - 2 ф-ции: передача адресной инф, на основе кот. производится коммут. при устан.соед; поддержание передачи данных при скор.64 кбит\с с коммут.каналов.
Канал типа Н – высокоскор.передача (факс, видео, звуки).

Пользов интер.представл.набором каналов опред.типа с опредл.скоростями.

2 типа польз.интер:

1. начальный Basic Rate Interface(BRI)
2. основной интерф. Primary Rate Interface (PRI)

BRI:

Интерф.BRI – предст.пользоват.

$BRI = 2B + D$ [2 канала типа В и один – типа D]

$\Sigma \text{скор} = 144 \text{ кбит\с}$

2-проводной кабель (уплотн.TDM).

Данные перед.кадрами по 48 бит.

описыв.в стандарте I 430.

PRI:

Для повышенной пропускной способности.

Поддерж схему:

$30B + D$ – Европа (2,048 мбит\с)

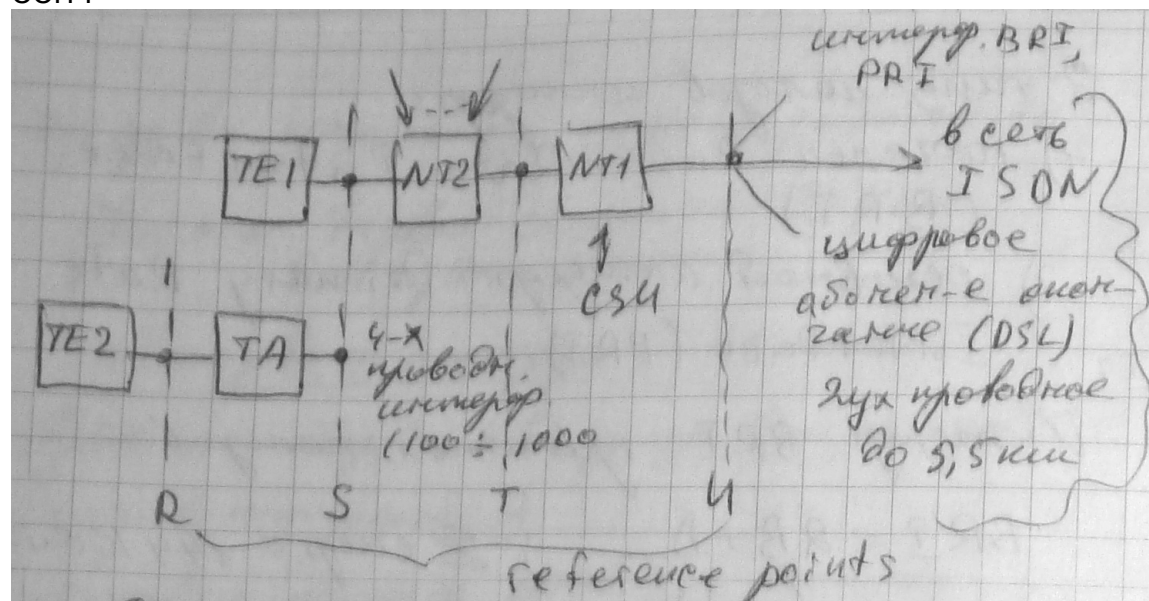
$23B + D$ – Америка, Япония (1,544 мбит\с)

Стандарт I 431

Кадры PRI – это кадры интерф. DS-1 (T1 или E1)

Подключение польз.оборуд.к сети ISDN

CCITT



Оборуд.делится на функц.группы и в завис.от групп, установл.неск.справочных точек

(R,S,T,U) соедин.разн.групп оборуд.

Устр-во функции группы NT1 – Network Termination 1 – образует цифр.абонент.окончание (DSL – Digital Subscriber Line)

Выполн.на кабеле.

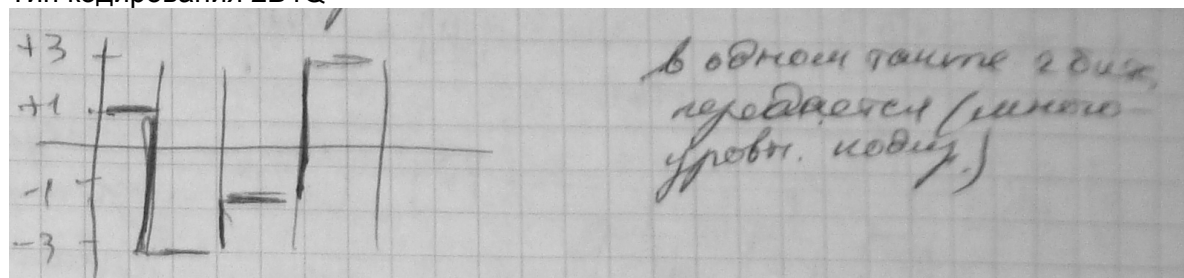
CSU – работ.на физ.ур. и обр.дуплексный канал.

Справочн. U – точка подкл.к сети

Размещ.в помещении пользоват.Часто встраивается в МШ-шлюз – соедин.с внешн.сетью.

Если польз.подкл.по интерф. BRI, то абон.оконч – 2-проводная линия.

Тип кодирования 2B1Q



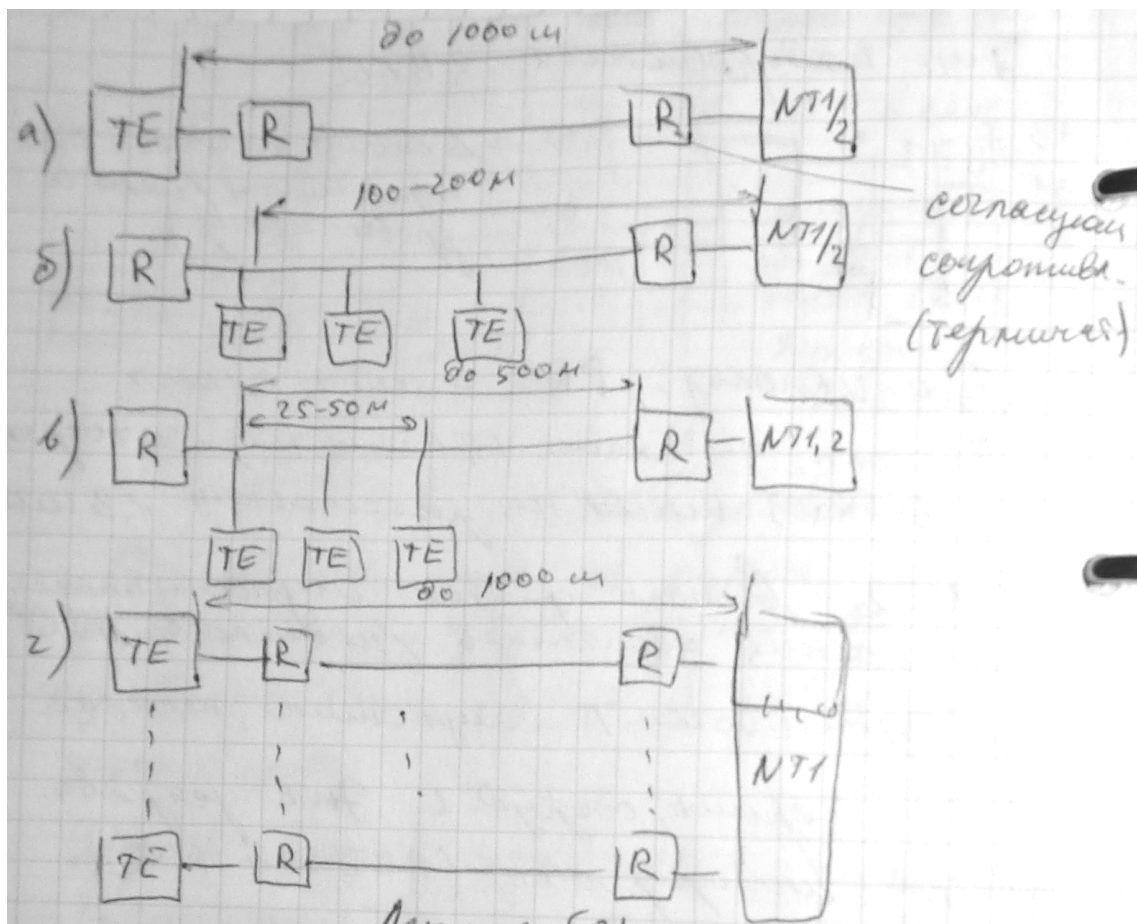
При использ.PRI – абон.оконч.выполн.по схеме (T1 или E1) – 4-проводная линия на расстоянии 1,8км.

NT2 – выполн.ф-цию мультиплексир.нескольких абонентов (комплекс. АТС)

Справочная точка T – мультипл.,неск.аб.

TE1 – термин.оборуд.1. Устройство поддержки интерф.польз. (BRI или PRI).

TE2 – оконеч.оборуд. 2.Не поддерж.интерф. (BRI и PRI), т.е. компьют. МШ. Для подкл.такого оборуд.в т.С использ.офисн.АТС, а подкл. до 8ми устройств к одной.



Лекция 31

Адресация в сетях ISDN

Техн. ISDN разраб. как основа всемир. телекомм. сети. Необх. емкая адресация и взаимосвязь с существ. ТЛФ сетями (привязка к сущ. стандартам в ТЛФ сетях).

Существ. стандарты:

ITU e.163 – адрес из 12 десятичных цифр.

новый ст. е.164 – адрес из 55 десят. цифр.

В сетях ISDN различ:

- № абонента (из этих 55 десят. знаков)
- адрес абонента

№ абонента – соотв. точке Т (выход АТС). Т.о. вся офис АТС адрес. номером абонента.

№ абонента = 15 дес. цифр

Делится на поля:

- код страны (1-3 знака)
- код города
- № абонента (т.Т – офис. АТС)

Т.о. адрес ISDN = № абон(вых. на конкр. АТС) + 40 дес. зн. (подадрес)

Подадрес использ. для адресации термин. устройств, подключ. к точке S (на слеше)

При вызове абонента из др.сети, не отн. к ISDN (пример x.25), используется 2 способа адресации:

1. адрес другой сети заменяется на адрес ISDN. Но для указания, что это адрес другого стандарта, ему предшествует поле префикса, в кот.указывается код этого станд.
Префикс по станд ISO – 498.
Сети ISDN способны обраб.этот адрес и устанавли.связь с др.сетью.(например x.25).
2. Указание в адр. ISDN 2 адресов: 1 – адрес ISDN погранич.устройства новой сети (пример x.25); 2 – адрес узла в новой сети (x.25)

При этом адреса раздел.спец.разделителем. Адреса использ.в 2 этапа:

- 1 этап. Сначала сеть ISDN соедин. коммут.канал с погран.устройством новой сети (x.25)
- 2 этап. используется 2 часть адреса: соедин.с абонентом внутри новой сети.

2 способ используется чаще (работает по своему стандарту, а во 2й части использ.новый адрес.)

Т.е. тащит всегда два адреса на всякий случай.

Использование служб ISDN в корпоративной сети.

Сети ISDN используются также, как ТЛФ сети с коммут.каналов, но более скоростные.

Интерф BRI – 128 кбит\с

Интерф PRI – 2,048 мбит\с

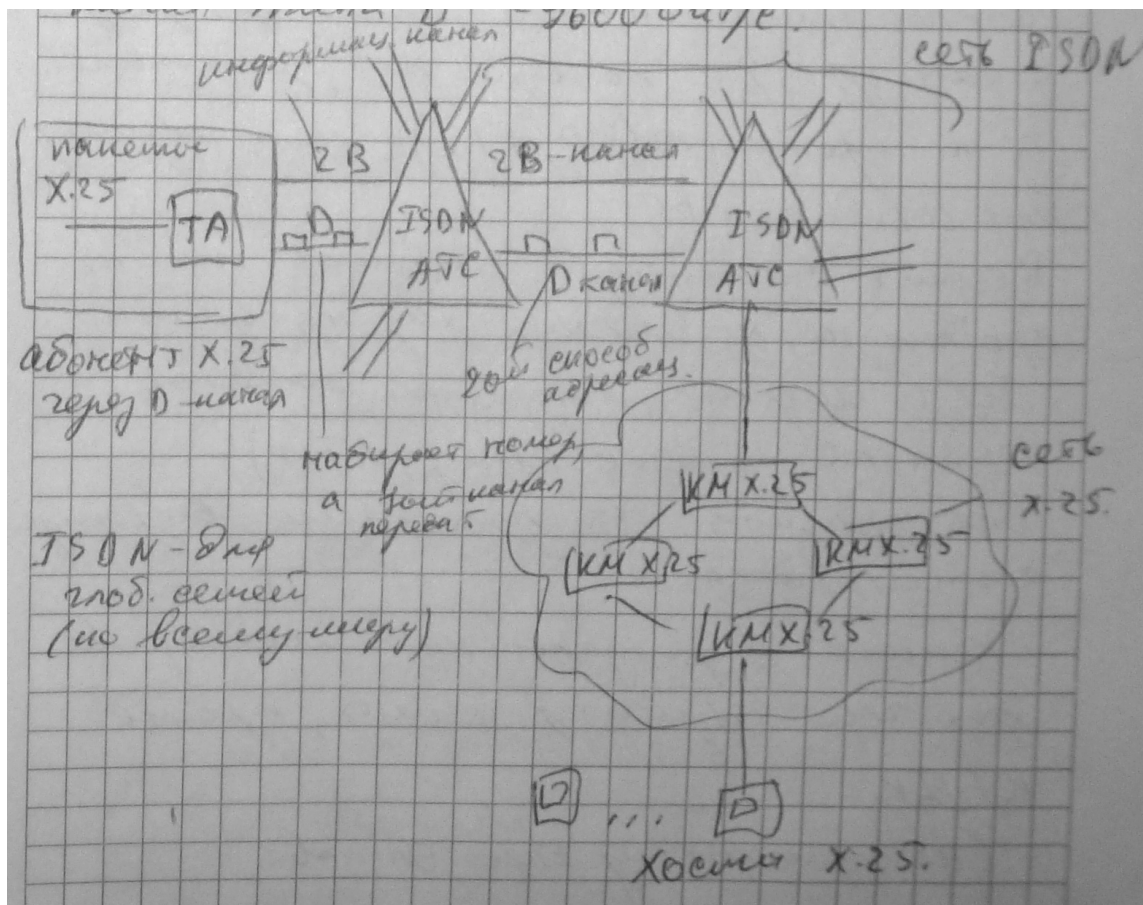
Качество передачи значительно выше, меньше искаж.сигнал.

Обычно инт. BRI – для подключ. отд. РС и неболь.ЛВС

Интерф PRI – для подключ. более крупных маршрутиз.сетей более крупного размера.

Чаще всего ISDN использ.как сеть доступа к менее геогр распротр.сетям (пример x.25).

Такая услуга называется доступ к сети x.25 через канал типа D – 9600 бит\с



Сети ISDN не являются средством для созд. магистр. сетей – отсутствие скоростных служб. Малые скорости канала. Использ. для подкл. мобильн. польз., домашних польз., небольших ЛВС, а также могут использ. как резервные каналы при нарушении основных.

Коммутация пакетов

Ранее использ. сети с коммут. каналов имели меньш. пробл. на физ. и канн. ур., т.к. поверх них работали те же протоколы (IP, IPx), которые исп. для объедин. ЛВС.

В сетях с коммут. пакетов таких проблем нет, но для них характерна оригинал. техн. маршрутизации пакетов (сети x.25, Frame Relay, ATM)

Она основана на понятии виртуальный канал.

Техника виртуальн. кан. исп. во всех глоб. территор. сетях, кроме TCP/IP.

Она состоит из эл-тов:

До передачи пакетов устан. вирт. соединение (проклад. путь).

2 типа вирт. соед:

- коммут. вирт. канал (Switched Virtual Circuit, SVC)

- постоянный вирт. канал (Permanent Virtual Circuit)

SVC. Коммут. нужен – подключился – коммут. настр. на передачу динамически по запросу абон.

PVC. Образуется заранее вручную администратором.

Маршрутизация пакетов по сети производится только 1 раз при созд.вирт.канала. А после созд.передача пакетов коммутаторами сети – на основании идентификации вирт.каналов – VCI (Virtual Channel Identify)

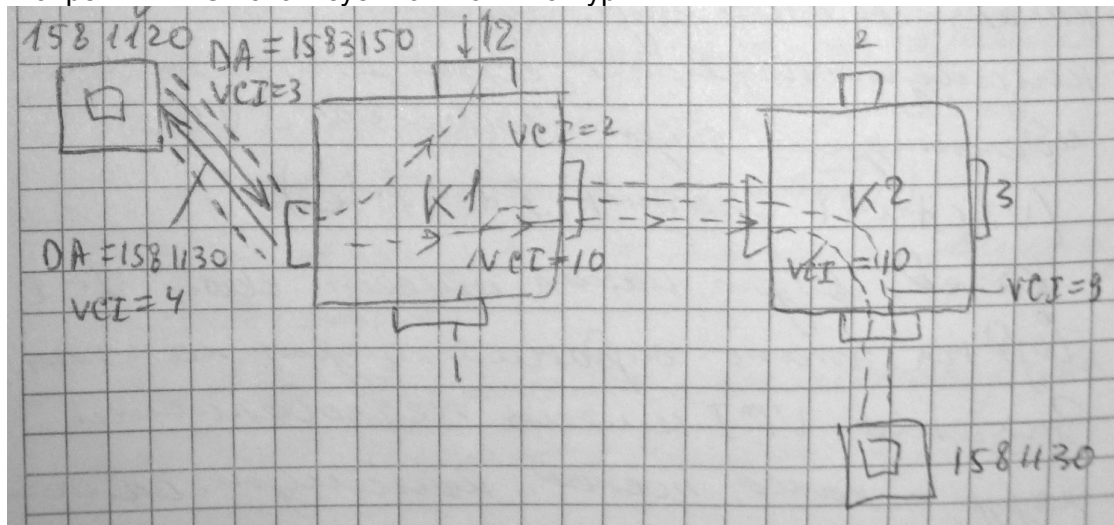
Кажд.вирт.канал имеет свой VCI.

Созд.на этапе создания вирт.канала. Значение VCI имеет неглобальный характер, а каждый послед.коммут.самостоят.нумерует свой VCI. Кроме этого, КМ настраив.таблицы коммутаций портов – на какой порт передать перешедш.пакет, если он имеет свой № VCI. После прокладки VCI, КМ больше не исп.табл.,а продвиг.пакетов – на основ. №. VCI больш.размерности.

Табл.коммут.портов имеет значит.меньше записей, чем табл.маршрут., т.к. хранят только действ.в этот момент соед. Работа сети ускоряется.

Режим PVC

Более эффект.по производ, т.к. работу по маршрутиз.пакетов уже заранее выполнил администратор. Не требуется call/request. Обмен пакетами в каждый момент времени. Т.о. режим PVC использует только 2й кан.ур.



Лекция 32

Пусть конечный узел с адресом 1581130 начинает установку соединения 1581130.

Одновременно с адресом назначения в пакете call-request указывается номер виртуального соединения VCI свободный в настоящее время при передаче на выходной порт. Связь между коммутаторами точка-точка, поэтому адрес следующего коммутатора не нужен. В этом случае протоколы маршрутизации не используются - обмен вручную. Строят таблицу маршрутизации. Каждый конечный узел и каждый км ведёт свои списки занятых и свободных VCI для всех своих портов. Изменение номера виртуального соединения при передаче для того, чтобы при продвижении пакетов в обратном направлении (дуплекс) можно было отличить пакеты данного виртуального соединения. После установки соединения пакеты уже не несут длинные адреса узлов, а используют короткий номер виртуального канала.

Техника виртуальных каналов. Свои преимущества и недостатки.

Преимущество - скорость. Недостатки - единственное соединение, Эффективны для долговременных потоков. В них мало служебной информации.

...

x.25

Особенности:

1. В структуре сети используются сборщики\разборщики пакетов (PAD - Packet Assembler\Disassembler). Для сборки нескольких входных низкоскоростных потоков.
2. Наличие трехуровневого стека.
3. Однородные стеки транспортных протоколов - невозможность объединения разнородных сетей.
4. Сети x.25 состоят из коммутаторов S, называемыми центрами коммутации пакетов. Обычно они расположены в различных географически удалённых районах и соединены друг с другом выделенными каналами. Терминалы подключаются через PAD по асинхронному интерфейсу RS-232C. Один хаб подключает 8, 16, 24 терминала.

...

Сеть x.25 состоит из коммутатора S, которые выполняют следующие функции:

- Сборка символов от терминала в пакеты;
- Разборка полей данных в пакетах и вывод на терминалах;
- Управление процедурой установки соединения по сети x.25.

Кадры Start, Stop, бит четности, продвижение...

Адрес присылается порту PAD, который подключается к коммутатору по дополнительному каналу. Взаимодействие терминалов с PAD производится по протоколу x.28.

На этапа установки соединения и передачи данных используются специальные команды передачи данных:

CTRL + P - PAD переходит в режим передачи данных.

IDN (International Data Numbers) имеет до 14 десятичных знаков. Первые 4 цифры - код идентификации сети (DNIC - Data Network Identification Code). 3 цифры - код страны, 1 - номер сети в стране. После 95го года 10 сетей стало не хватать. Коды 250 и 251. Остальные цифры - номер национального терминала (NTN - National Terminal Number). Идентифицирует конкретный источник\приемник данных. Префикс перед номером кодирует тип кода.

...

Frame Relay

Преимущества FR:

- высокая пропускная способность

Основная особенность - гарантированная поддержка средней скорости передачи по виртуальному каналу. Сеть FR стандартизована в сетях ISDN как служба.

В сети устанавливается два типа виртуальных каналов - постоянных PVC, коммутируемый - SVC. Соответственно, используются там, где по каналу передаётся трафик практически непрерывно. А в случае редкого трафика используется SVC.

Стек протокола FR

В отличие от x.25 использует два уровня - физический и канальный (после установления соединения).

Протоколы канального уровня LAP-F. Два режима работы - основной (core) и управляющий (control). При передаче кадров квитанции на каждый кадр не передаются (как это делается в x.25). В сети FR много заимствовано из стека протоколов ISDN. LAP-

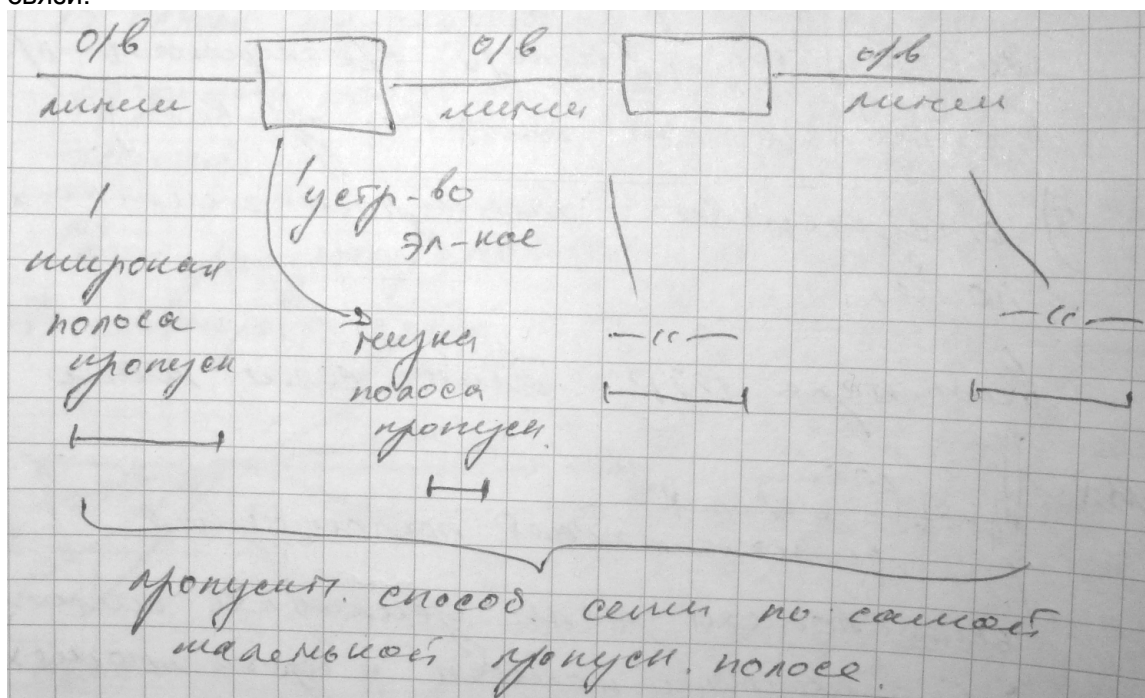
F core. При использовании коммутируемого канала предлагается использовать канал D и на нем работает протокол LAP-D. Data Link Connection Identifier (DLCI). Так как стек протоколов FR заканчивается на втором уровне, эта технология хорошо согласуется с инкапсуляцией пакетов сетевого уровня. Не контролируется на ошибки.

Семинар 1

AON - All Optical Network

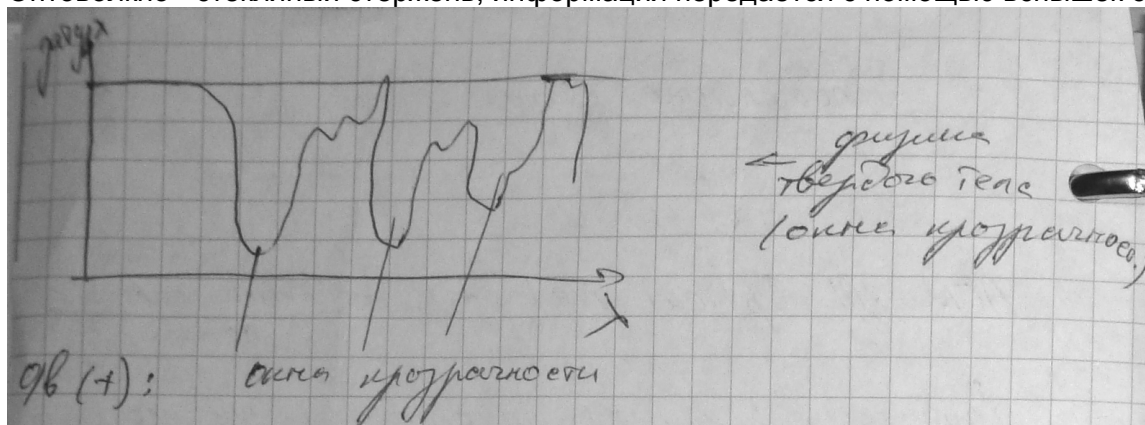
Оптическая линия и оптические сети - разные вещи.

Волоконно-оптическая линия связи (ВОЛС) – это вид системы передачи, при котором информация передается по оптическим диэлектрическим волноводам, известным под названием “оптическое волокно”. Волоконно-оптическая сеть – это информационная сеть, связующими элементами между узлами которой являются волоконно-оптические линии связи.



Средства оптической передачи

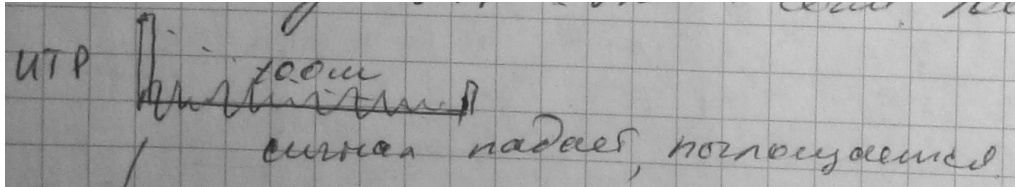
Оптоволкно - стеклянный стержень; информация передается с помощью вспышек света.



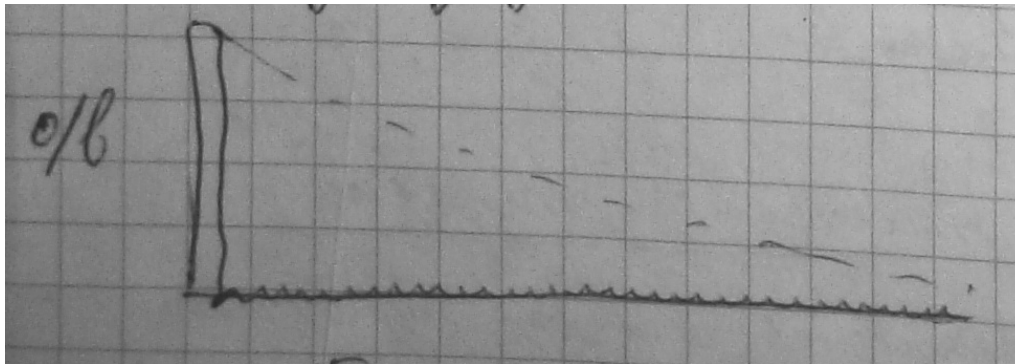
Преимущества:

1. Полоса пропускания
2. Несанкционированное вмешательство
3. Отсутствие помех

Витая пара UTP - длина сегмента - 100м.



Есть помехи. Если усиливать сигнал, будут усиливаться и помехи, и среди помех нельзя различить сигнал.



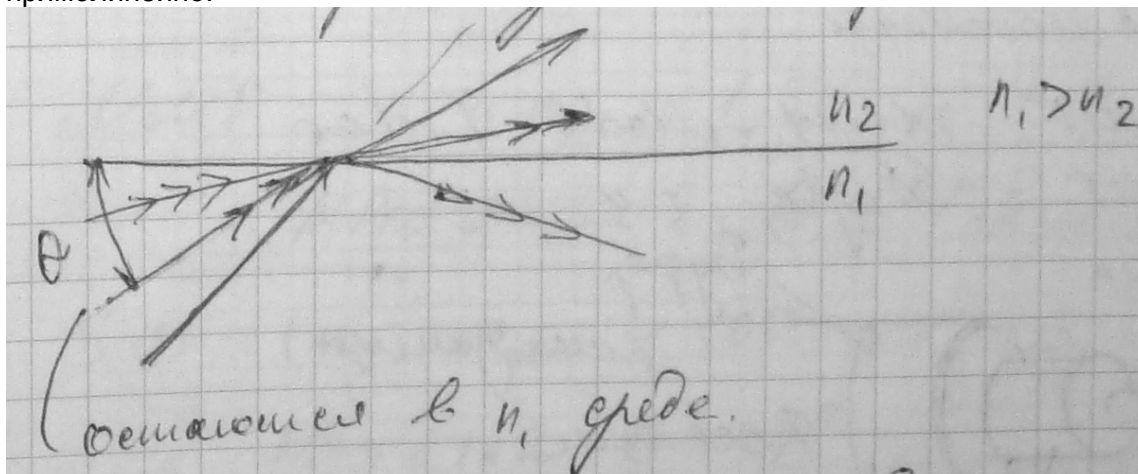
I тип оптоволоконна - 2000м. II тип оптоволоконна - 40-80км без промежуточного усилителя.

4. Долговечность

Недостатки - Неустойчивость к мощному ЭМ-воздействию (атомный взрыв)

Идея оптоволоконна появилась 60 лет назад

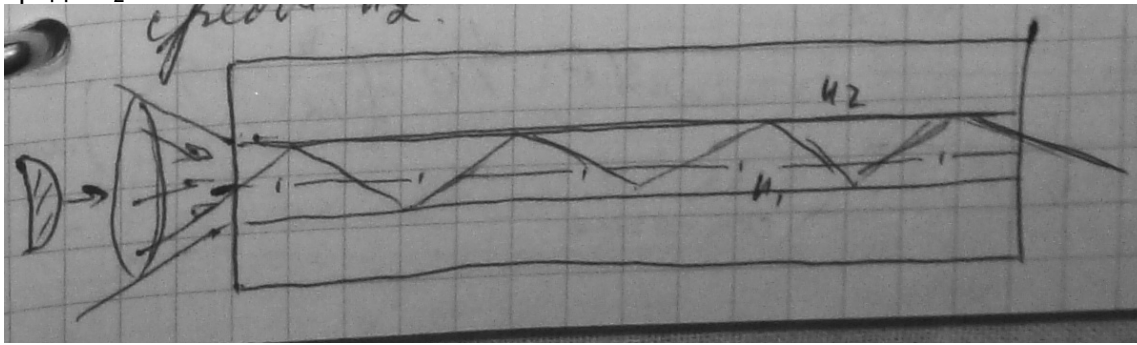
В основе использования оптоволоконна лежит эффект полного внутреннего отражения. Свет распространяется прямолинейно в однородной среде. В неоднородной - не прямолинейно.



Световод - это тонкий двухслойный стеклянный стержень.

Показатель преломления внутренней среды n_1 больше показателя преломления внешней

среды n_2 .

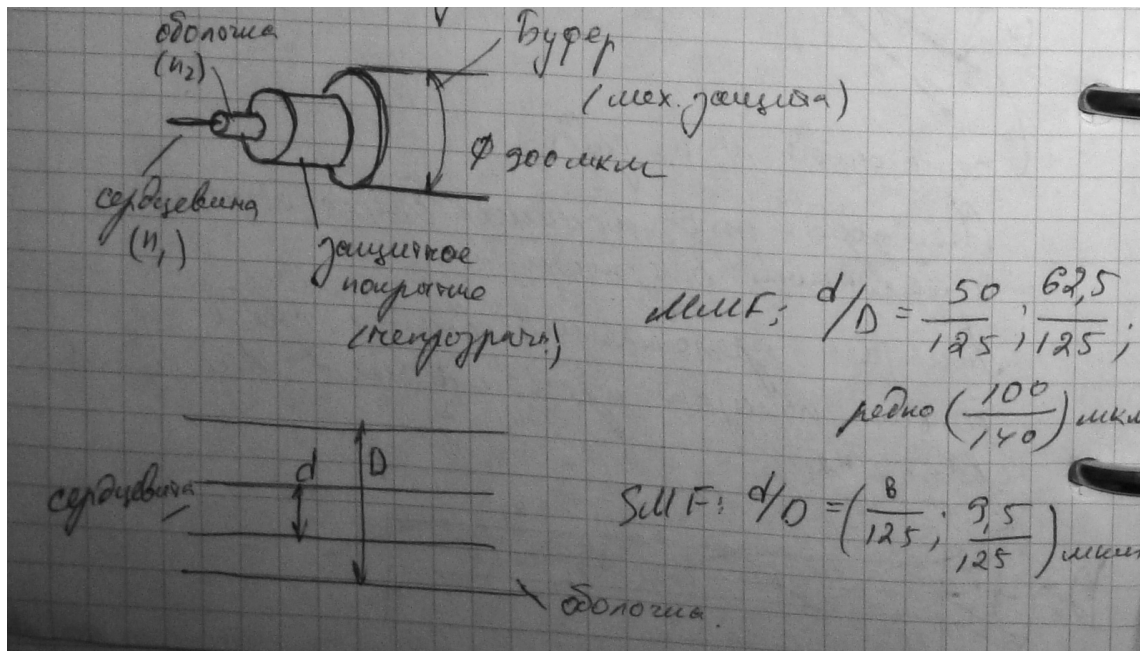


Световод можно слегка изгибать (главное, чтобы свет не ушёл в другой слой n_2). Световод, управляемый источник света и фотодетектор образуют канал оптической передачи информации. Используется свет с длиной волны в диапазоне 400-3000 нм (часть видимого спектра и ИК-диапазон).

$$f = \frac{c}{\lambda} \text{ используется} \quad f = (10^{13} - 10^{14}) [?] [?] [?]$$

В зависимости от траектории распространения света различают 2 вида оптоволокон:

- многомодовое MMF (Multi-Mode Fiber)
- одномодовое SMF (Single-Mode Fiber)



Оптоволокно с меньшим диаметром - более дорогое.

MMF - более дешёвое, подходит для локальных сетей.

SMF - дороже, подходит для глобальных сетей.

Чтобы луч распространялся вдоль сердечника, нужно, чтобы он вводился в световод под углом меньше критического $< \theta$. Синус этого угла называется числовой апертурой (NA).

$$NA = \sin \theta = \sqrt{n_1^2 - n_2^2}$$



MMF: n_c и $n_{об}$: 1,515 и 1,50

$NA = 0,2 \div 0,3$; $\Theta = (12 \div 18)$

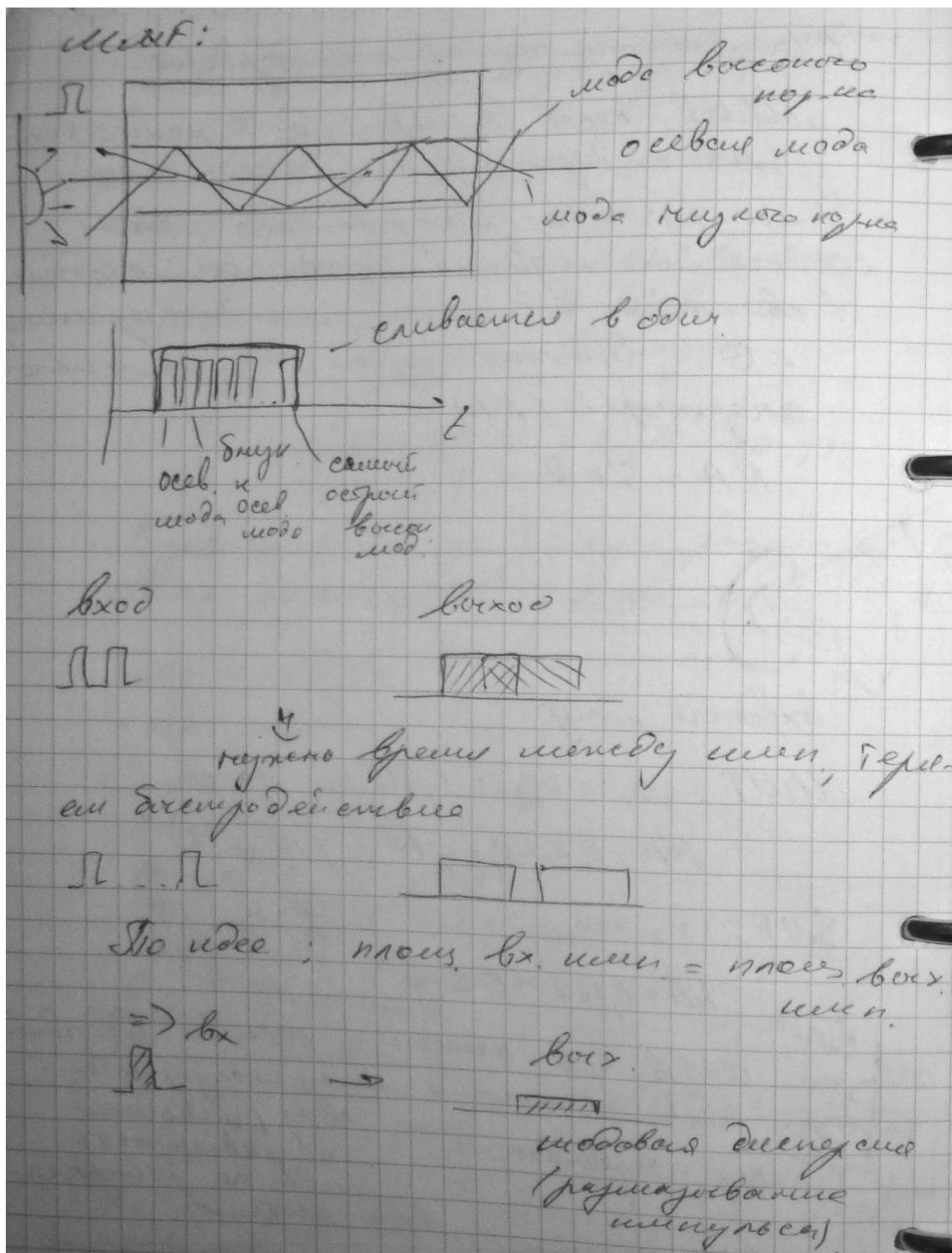
SMF: n_c и $n_{об}$: 1,505 и 1,50

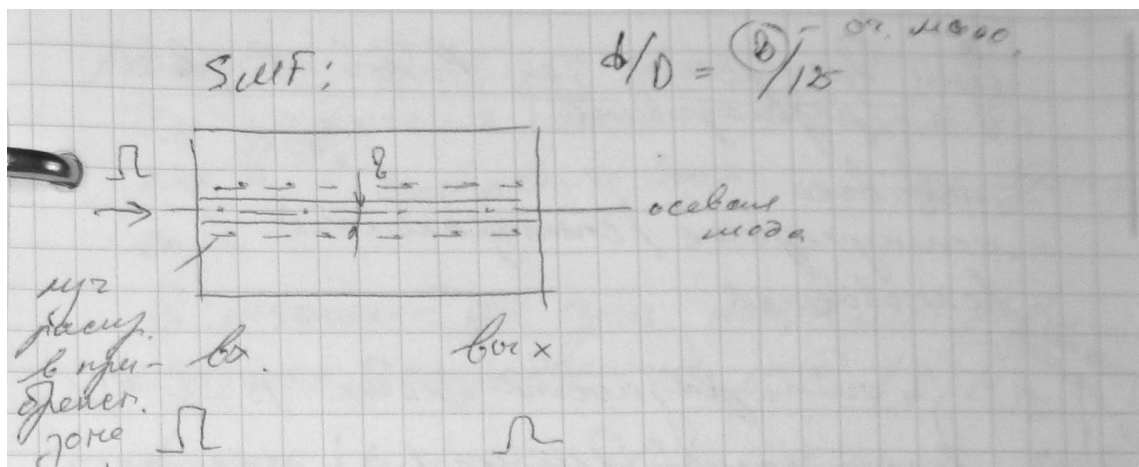
$NA = 0,122$; $\Theta \simeq 7^\circ$

В MMF в качестве источника света используется светодиод.

В SMF - полупроводниковый лазер (меньшая направленность, чтобы не растрчивать энергию).

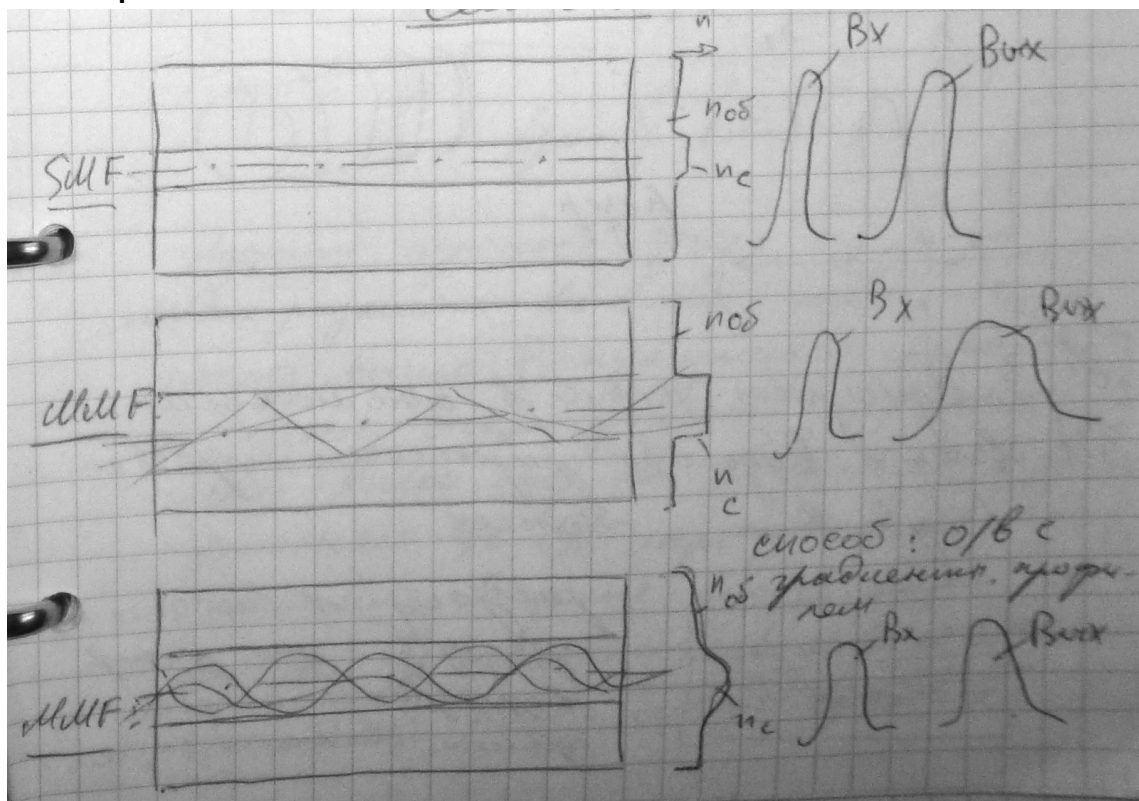
Чем больше апертура NA, тем легче ввести луч в оптоволокно.





Сигналы на вход и выходе почти одинаковые (нет дисперсии).
С меньшей скоростью идёт распространение - из-за них импульс на выходе слегка расплывается.

Семинар 2

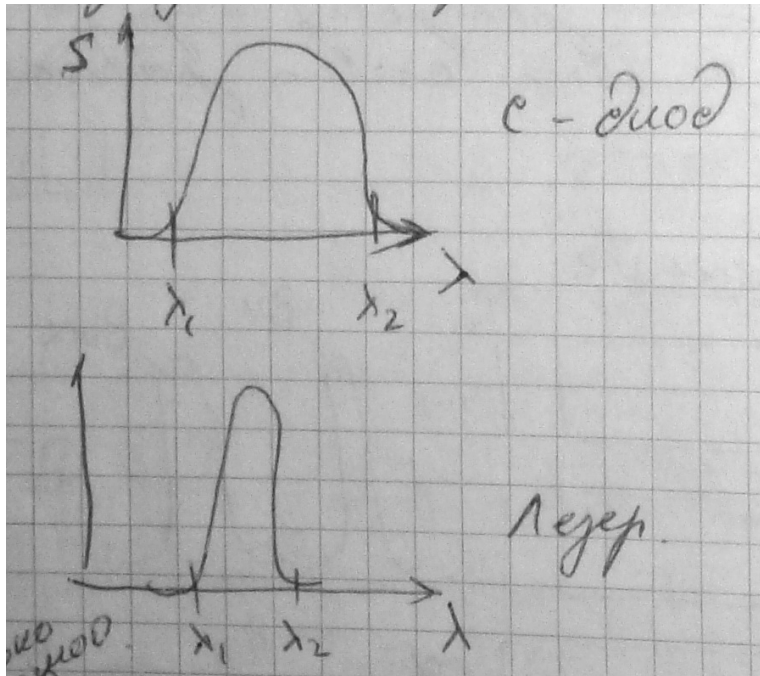


Существует дисперсия трёх видов

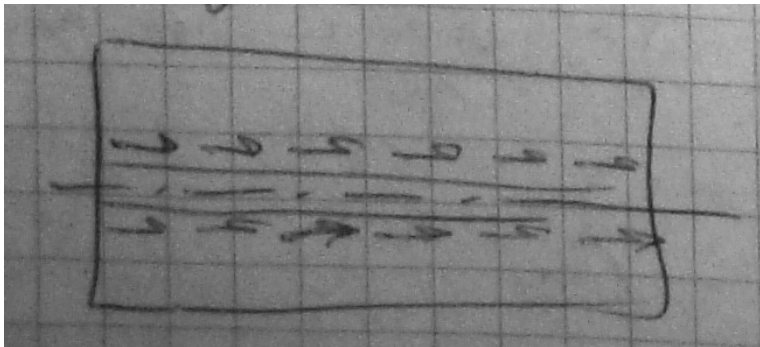
- модовая;
- молекулярная (спектральная);
- волноводная.

Модовая (только в многомодовых) - за счёт разности хода $15 \div 30$ [?/?/?/?]/[?/?/?/?]

Спектральная (только в многомодовых) - волны разной длины (λ) распространяются с разной скоростью, что обусловлено разной структурой (молекулярной).



Волноводная (только в одномодовых) - обусловлена разностью скоростей в сердцевине и оболочке.

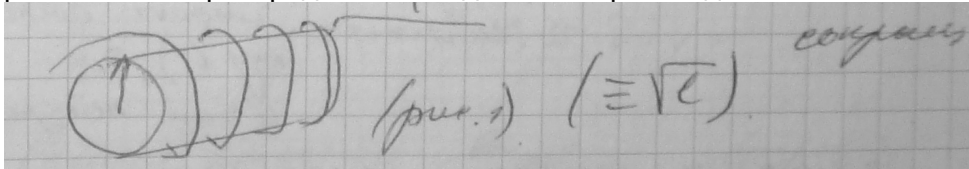


Распространение в оболочке чуть-чуть - это распространение в прибрежном слое происходит медленнее, чем вдоль оси.

Т.е. прозрачность волокна должна быть хороша как и в сердцевине, так и в прибрежном слое.

В многомодовом оптоволокне существует понятие равномерное распределение мод.

В MMF - широкая диаграмма направленности источника, т.е. при входе лучи очень насыщены, их много, они увеличивают своё количество за счёт неровностей и т.д. Но они постепенно поглощаются в течение прохождения по оптоволокну. И устанавливается равномерное распределение мод. Но это происходит на нескольких км ($\equiv l$).



Эффективность переноса энергии на разных модах различна. На высоких модах поглощение выше. В переполненном волокне в переносе энергии участвуют неэффективные моды высокого порядка. Светодиод обычно переполняет оптоволокно. По мере удаления от источника высокие моды уходят в оболочку за счёт изгибов и

). А после - ($\equiv \sqrt{l}$). Поэтому рационально добиться чтобы РРМ наступило раньше, для этого используется приём наматывания оптоволокну на цилиндр.

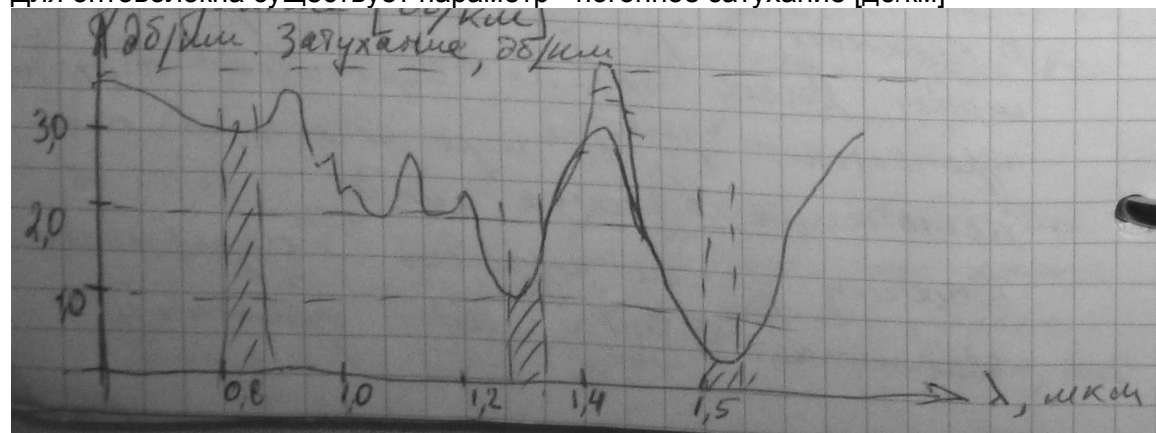
Мощность сигнала, потери, усиление

Мощность сигнала измеряется в дБ\мВт = $10\lg \frac{P_{\text{сигн}}}{P_{\text{сигн}} + P_{\text{ш}}}$.

Потери Loss = $-10\lg(P_{\text{вых}}/P_{\text{вх}}) = 10\lg(P_{\text{вх}}/P_{\text{вых}})$. Затухание вызвано рассеянием (уход "в молоко") и поглощением (непрозрачные примеси - тепловое рассеяние).

Погонное затухание дБ\км.

Для оптоволокна существует параметр - погонное затухание [дБ/км]



Окна прозрачности

Самая хорошая длина - $0,8\lambda$ - есть окно прозрачности + небольшое затухание.

0.8, 1.4 - MMF окна прозрачности

1.4, 1.5 - SMF окна прозрачности

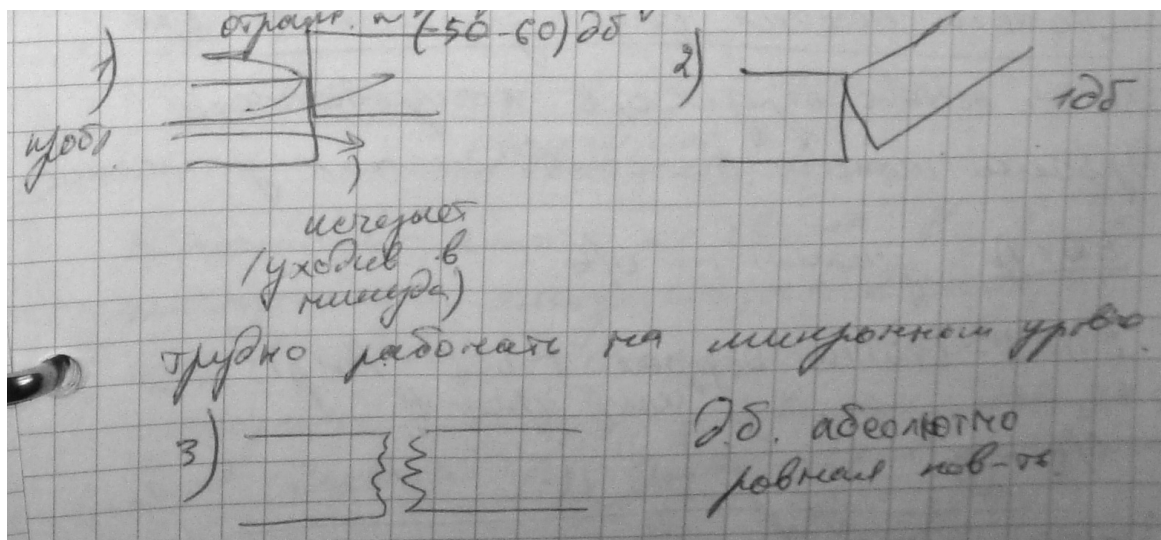
MMF: $\lambda = 850[?][?][?][?] [?][?] 1300[?][?][?][?]$

погон. затухание 2,7дб/км, 0,75дб/км

Узнать затухание: $\text{погон.затухание (в км размере)} \times \text{на количество км в оптоволокне} = \text{реальное затухание.}$

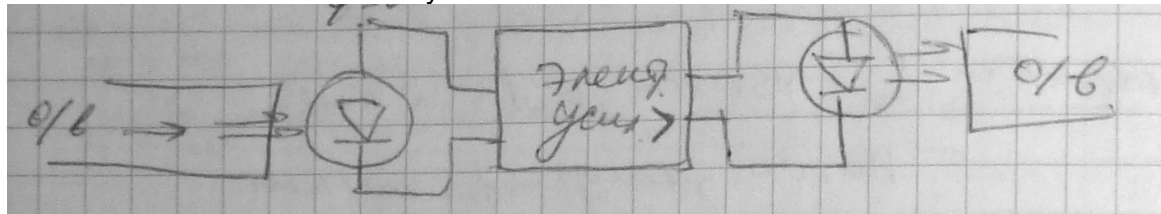
SMF: $\lambda = 1550$ [nm] - затухание 0,25дБ/км; $\lambda = 1300$ [nm] - 0,35дБ/км.

Самые сложные вопросы - вопросы стыковки разных участков оптоволокна.



Если отраженный сигнал попадает обратно на лазер и лазер прекращает генерацию сигналов.

Оптоволокно может выносить усилительные свойства



Старая схема усиление сводила все достоинства на нет: полоса пропускания, защита от ЭМ-волн, несанкционированное вмешательство.

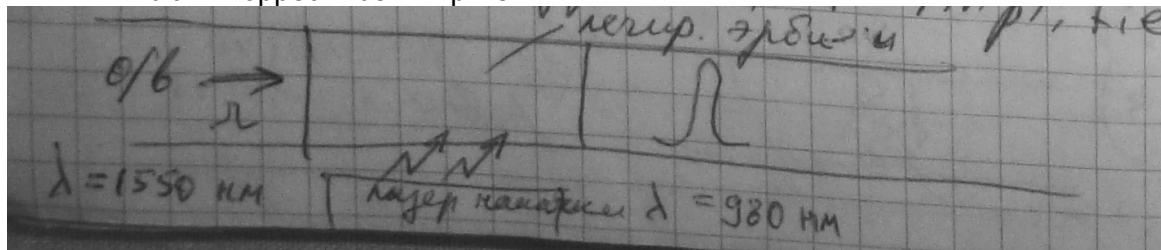
У оптоволокну широкая полоса пропускания, а у электрического усилителя маленькая полоса пропускания. + Электро-межанические помехи на оптоволокну не действуют, а на усилитель - действуют. И из оптоволокну откачать информацию нельзя, а из усилителя можно.

Потом появился специальный усилитель на оптоволокну.

Оптоволокну на основе отрезка оптоволокну легированного эрбием может выносить сигнал усиления.

EDFA - усилит. на о/в.

EDFA - Erbium-Dopped Fiber Amplifier.

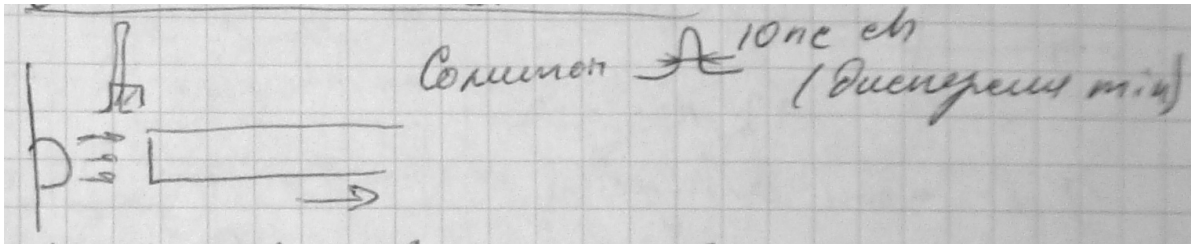


За счёт энергетического лазера мощность сигнала увеличивается

Усилитель - это когда есть источник доп. энергии (усилив. напряжение и ток).

Семинар 3

Солитоновая технология



рент-ть падает, но возрастает амплитуда сигнала.

Эта технология устроена так: очень узкий импульс, но с большой амплитудой. Есть ограничение по энергии. Т.е. оптоволокну может плавиться => энергию ограничивают по длительности и форме (не подвержена дисперсии). Неограниченное распр-ие для передачи.

Источники и приёмники излучения

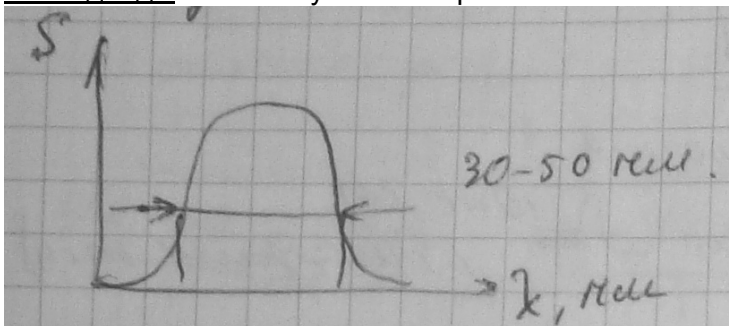
Источник - источник света. На входе электрические импульсы, на выходе соотв. электрич. импульсы. На выходе импульсы в электрич. сигналы. Это может быть диод. Главный недостаток - узкая полоса пропускания у оптоволокну.

На входе светодиода

На выходе не понял.

Светодиоды

Светодиоды - используют некогерентные источники энергии (30-59нм) - ширина спектра.



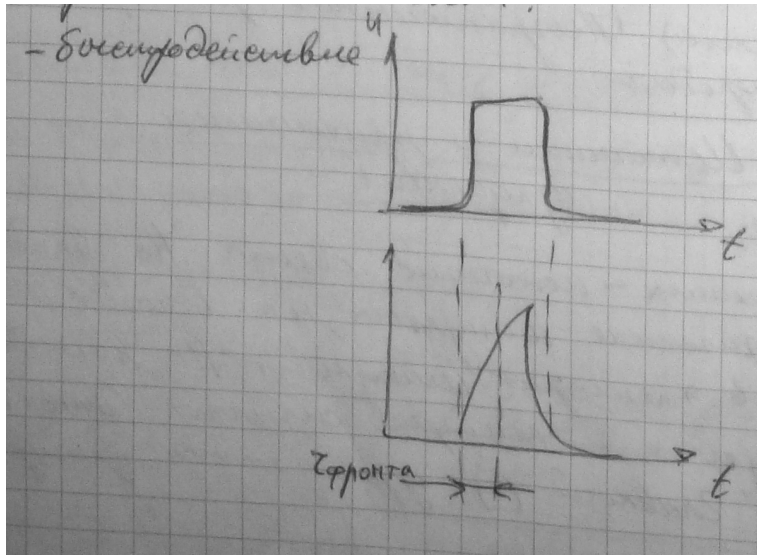
Существует волновая дисперсия.

Лазерные источники значительно дороже. Светодиод имеет широкую диаграмму направленности.

Достоинства светодиода: дешевле, особенно для $\lambda = 850$ нм (на $\lambda = 1300$ нм дороже).

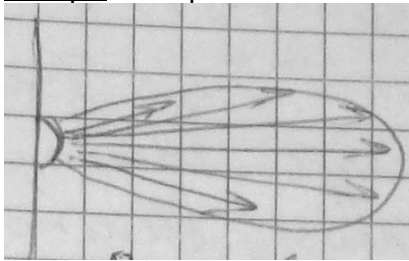
На $\lambda = 1550$ нм работают лазеры.

Характеристики источника света:



Лазеры

Лазеры - когерентные источники с узким спектром. (1-3нм - ширина спектра).



Волновая дисперсия отсутствует. Диаграмма направленности - узкая.

Лазеры используются в одномодовом волокне с $\lambda = 1300[?][?] 1550[?][?][?][?]$. Его быстрота действия значительно больше, чем у диода.

Недостатки:

- высокая стоимость
- малая долговечность, надёжность
- любые неоднородности вызывают отражение

Достоинства:

- быстродействие
- узкая полоса пропускания

Есть специальные оптические вентили, которые защищают лазер от отражённых сигналов.

Детекторы излучения

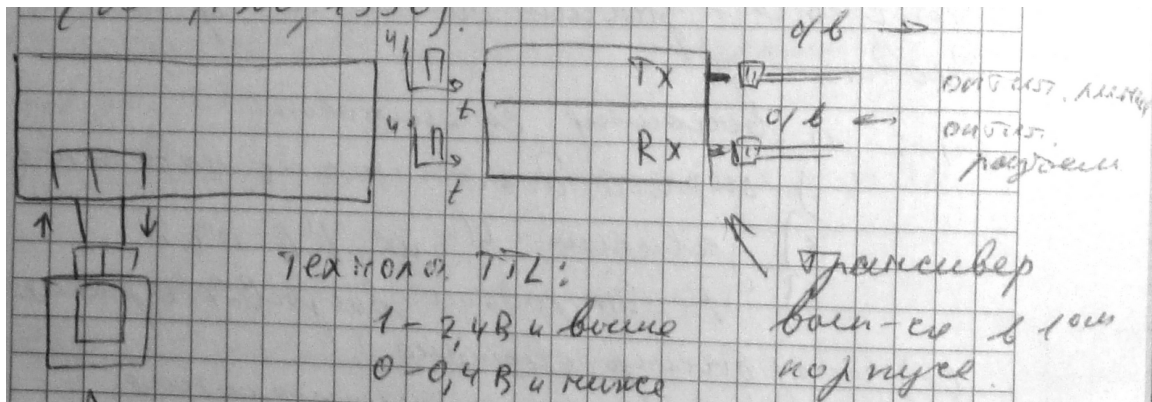
Детекторы излучения - фотодиоды, целый ряд из, которые различаются по быстродействию и чувствительности.

Обычные с низким быстродействием не применяются.

Применяются:

- рпн-диоды (металло-полупроводники). В них время отклика = единицы нс.
- лавинные - диоды имеют ещё более быстродействие, максимальную чувствительность, но требуют питания больше, сильно зависят от температуры.

Фотодиоды имеют зависимость от длины волны. Их различают в зависимости от вида окна прозрачности (850, 1300, 1550).



На входе стандартные сигналы (ТТЛ технология), на выходе оптические сигналы.

Оптический интерфейс

Оптический интерфейс: разъём устанавливают на отрезке оптоволокна, приклеенному к кристаллу излучателя или детектора.

Передатчик

Передатчик - излучатель со схемой управления (эл. сигнала в свет).

Основные параметры передатчика:

- выходная мощность [дБ/мВт для опр. длины волны];
- длина волны;
- спектральная ширина;
- быстродействие;
- долговечность.

г-фронт - время, за которое мощность излучения упадёт на 3дБ (в 2 раза). Обычно это несколько часов.

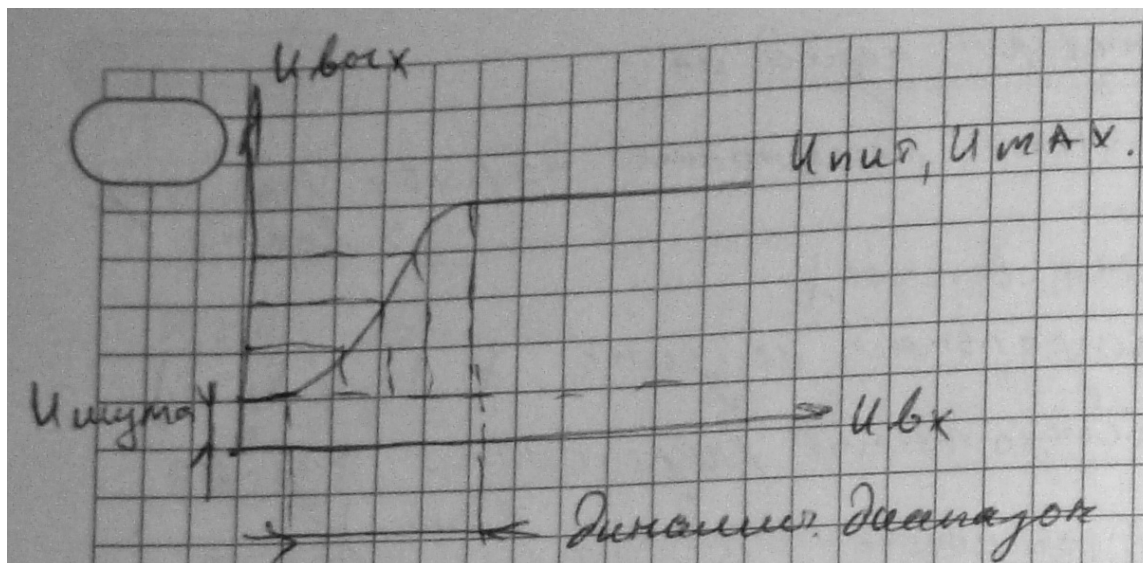
Приёмник

Приёмник - детектор с усилителем - формирователем (приводим к определённому стандартному виду, например в ТТЛШ).

Параметры:

- диапазон принимаемых волн;
- чувствительность - минимальная мощность сигнала различимой приёмником;
- динамический диапазон - отношение максимально возможного сигнала к минимальному;

Передаточная характеристика:



- быстродействие (полоса пропускания).

Полоса ВК определяется через время отклика (фронта).

$$B_{\text{ВК}} = 0,35 / t_r$$

Чувствительность определяется уровнем шумов фотодиода. Каждый прибор имеет некоторую степень неопределённости зашумлённости (в определённом диапазоне сигнал на фоне шумов не определится).

Семинар 4

Диаграмма потерь в линии



$$\text{Power budget РдБ} = 10 \lg(P_{\text{мВт}} / 1 \text{ мВт})$$

Расчет

Исходные данные:

Передатчик:

$$P_{\text{тр}} = -6 \text{ дБ/м}$$

$D_{\text{тр}} = 100 \text{ мкм}$ - диаметр сердечника

$NA_{\text{тр}} = 0,3$ - апертура $\sin(\text{teta})$ - угол разницы при стыковке $= >=$

Приемник:

Чувствительность $Pr_{sv} = -39$ дБ/мВт

$Dr_{sv} = 100$ мВ

$NA_{rsv} = 0,4$

Волокно1:

50/125 мкм

$Att = 3,5$ дБ/км

$L = 3$ км

$NA = 0,2$

Волокно2:

62,5/125 мкм

$Att = 3,5$ дБ/км

$L = 3$ км

$NA = 0,2$

1.

2.

3.

4. Потери в волокне 2:

$Loss = Att * L = 3,5 * 2 = 7$ дБ

5. Потери от волокна 2 до приемника:

Loss

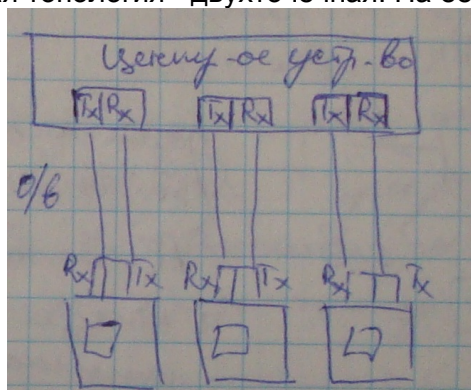
Приемник в насыщении и не чувствует сигнал.

...такие малы потери, что уровень сигнала на выходе не вписывается в динамический диапазон, применяют оптические аттенуаторы с фиксированным или переменным уровнем затухания. В них используется введение калиброванного воздушного зазора на 5, 10, 15, 20 дБ.

Семинар 5

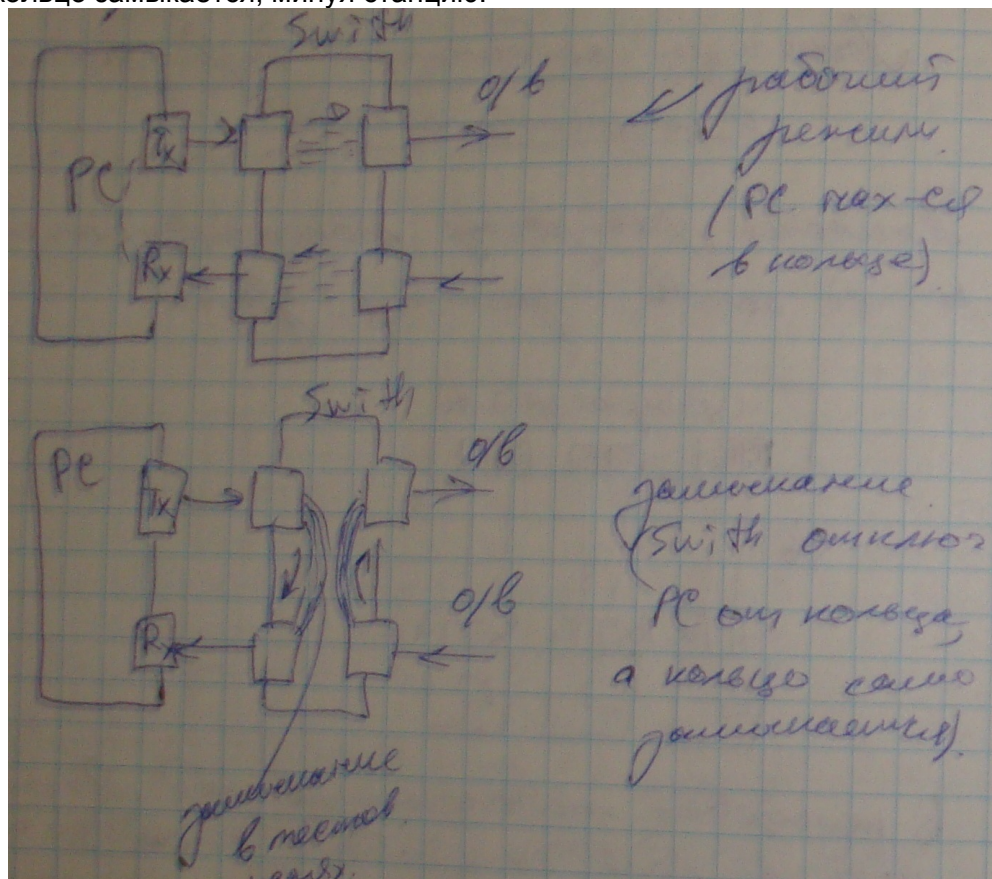
Топология соединений. Разветвители и мультиплексоры

Наиболее распространенная топология - двухточечная. На её основе строится звезда.

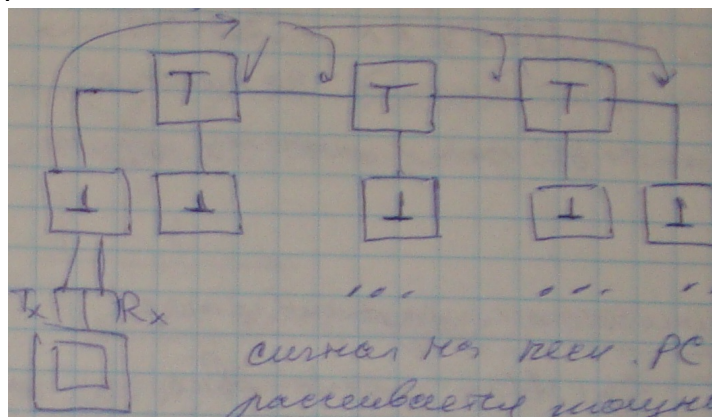


В кольцевой топологии выход одного устройства соединен со входом следующего и т.д. до замыкания кольца. При отключении одного из устройства нарушается целостность кольца. Для решения этой проблемы используются обходные (bypass) коммутаторы. Bypass switch - это пассивное управляющее устройство, имеет поворотное зеркало с электроприводом. При отсутствии управляющего напряжения зеркало поворачивается

так, что кольцо замыкается, минуя станцию.



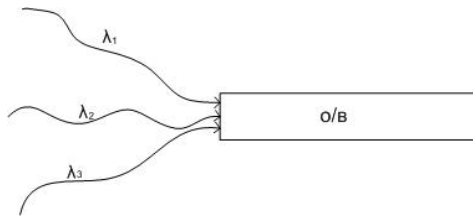
На о/в также возможна организация разделяемой среды на разветвлениях. Самое простое - сварка нескольких о/в линий в одной точке. Также с этой целью используются Т-разветвители (трёхпортовые). Их можно соединять в цепь, реализуя шинную топологию.



Сигнал на несколько PC - сильно рассеивается мощность. Поэтому нельзя подключать много PC. На Т-разветвителях построена технология 10Base FL. Разветвители вносят значительные потери, поэтому на много PC они не используются.

Для повышения эффективности использования о/в синий, по ним можно одновременно передавать сигналы с разными длинами волн. Для этого используется мультиплексирование с разделением по длине волн.

WDM - wavelength division multiplexing



Первые такие устройства объединяли 2 сигнала с длинами (850/1300) нм, затем - (1300/1550) нм. Сегодня достигнуто объединение 32 каналов, в лабораториях - до 80 каналов. Потенциально можно объединить до 300 каналов.

Оптические разветвители

Splitter - это один из элементов, применяемых в полностью оптических сетях. Это многополюсное устройство, в котором опт. мощ., подаваемая на часть входов, распределяется между остальными полюсами.

Различают разветвители:

- направленные
- двунаправленные

Двунаправленные - каждый полюс - на передачу и на прием, в том числе и одновременно.

А также:

- чувствительные к длине волны
- нечувствительные к длине волны

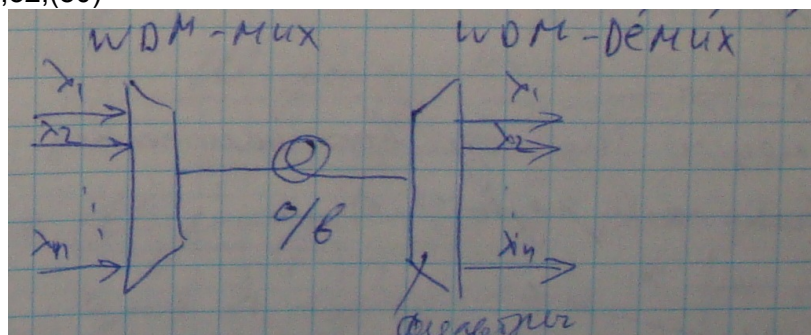
Основные категории оптических разветвителей:

- древовидные
- звездообразные
- ответвители

DWDM (Dense WDM - уплотненный). Использует каналы на разных длинах волн.

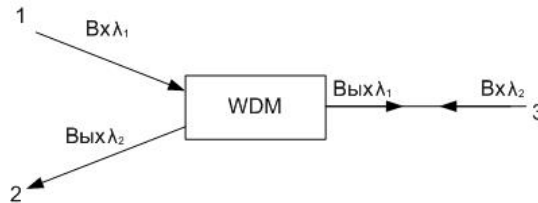
$\Delta\lambda \leq 1,6$ нм - нужно выделять входные длины волн, которые почти не различаются. Устройство очень дорогостоящее.

Для построения DWDM требуют пассивные узкополосные WDM фильтры, а также стабильные узкополосные лазеры. В настоящее время используют системы с числом каналов: 4;8;16;32;(80)



Основные техн. параметры WDM фильтров (устройств)

Обычно WDM устройства совмещают режимы mux-demux в одном устройстве.



В идеале первый сигнал поступает только на 3, но ответвление идёт и на 2. Для оценки этого паразитного явления вводится параметр “переходные помехи”. Он характеризует эффективность WDM устройства.

Переходные помехи:

-ближние (NEAR)

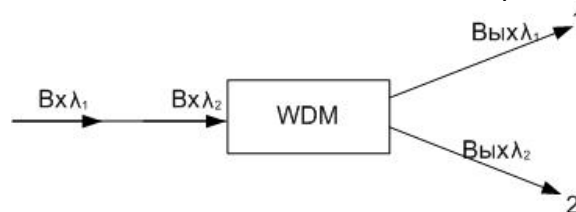
-дальние (FAR)

NEXT - Near End Cross Talk

Доля мощности на полюсе 2 при подаче сигнала на 1.

FAR

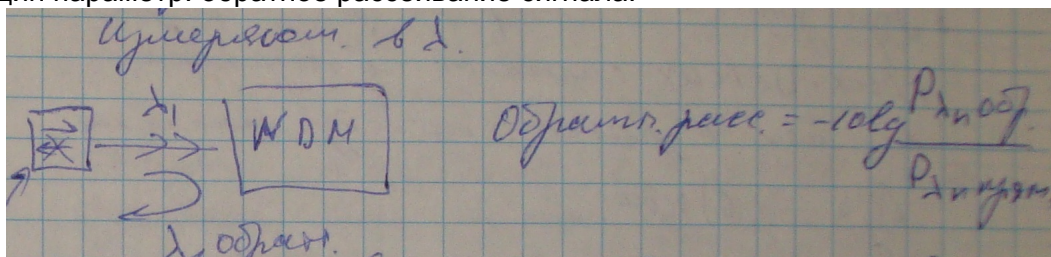
Мера изоляции между выходными полюсами по сигналам с разными длинами волн.



Это доля мощности сигнала 1 на полюсе 2.

WDM модуль в режиме mux-demux может иметь 1:n полюсов и описывается наборами из n матриц переходных коэффициентов (по одной матрице на каждую длину волны)

Еще один параметр: обратное рассеивание сигнала.



Влияет на обратную засветку лазера (лазер не терпит обратного света)

Используется специально устройство, которое пропускает прямой сигнал, но не пропускает обратный. У него свои параметры подавления.

Широкозонные и узкозонные WDM фильтры

1) широкозонные - используются для работы с сигналами с максимум двумя длинами волн. При расстоянии между каналами >70 нм. Это обычно каналы 1300; 1550; 1625. Пример: фирма Dicon

2) узкозонные - для режима mux-demux сигналов в многоканальных системах с расстояниями между каналами (0,8-1,6) нм. Основная область применения - о/в линии связи с использованием усилителя EOFA. Полностью оптические сети.

Поставщики таких услуг: Dicon, Nortel

Древовидные разветвители

Расщепляют входной сигнал на несколько выходных или наоборот. Обычно мощность входного сигнала разделяется в равных долях между выходными. Количество выходов: 2-32

Звездообразные разветвители

Обычно имеет конфигурацию $n \times n$. Оптический сигнал на одном из входов разветвляется на n выходов. Входы обозначаются буквами, выходы - цифрами.

Ответвители

Это обобщение древовидных разветвителей. Выходная мощность не обязательно разделяется в равных пропорциях между выходами. Используются конфигурации: (1x2), (1x3), (1x4), (1x5), (1x6), (1x8), (1x16), (1x32)

Обычно не менее 50% мощности передается в магистральный канал (первый)

Устройство волнового уплотнения (WDM)

Обычно выполняет функции мультиплексирования, демultipлексирования, фильтрации. Из множества входных волокон на разных λ сигнал подается в одно общее волокно. Или наоборот - из общего выделяются волокна разных λ .

Семинар 6

Оптические изоляторы

Оптический сигнал отражается от неоднородностей, мест стыка - часть энергии распространяется в обратном направлении. Часть энергии попадает в излучатель лазера, усиливается и ухудшает соотношение сигнал/помеха. Это приводит к росту шума источника излучения. С целью подавления отраженного сигнала используются оптические изоляторы - пропускают свет в прямом направлении почти без потерь, а в обратном - с большим затуханием. В современных сетях AON является одним из основных элементов и включается на выходе источника излучения, а так же на входе/выходе усилителей EDFA. В основе принципа действия изолятора вращение плоскости поляризации света.

Вращение плоскости поляризации света

В основе работы - эффект Фарадея - вращение плоскости поляризации света оптически неактивным веществом под действием продольного магнитного поля. Угол поворота плоскости поляризации $T = V \cdot B_z \cdot d$:

V - постоянная Верде - удельное магнитное вращение, зависящее от природы используемого вещества (а так же от t , λ),

B_z - продольная составляющая магнитного поля,

d - длина пути света в веществе (размер ячейки Фарадея).

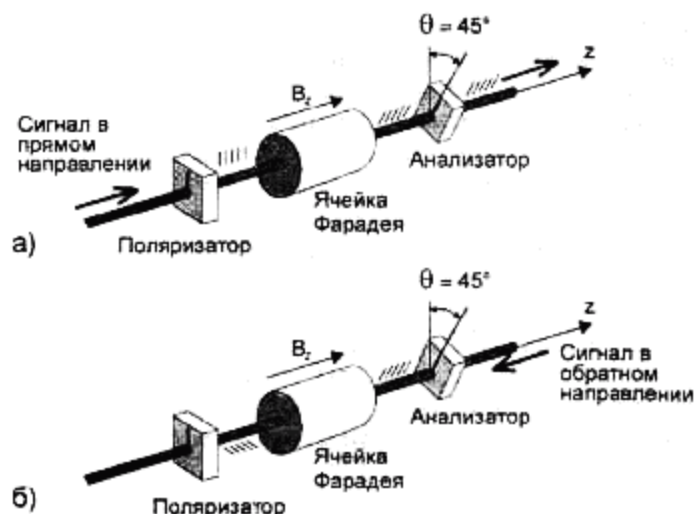
Направление вращения зависит только от природы вещества и направления магнитного поля. Зависимость угла вращения от λ называется вращательной дисперсией.

Принцип действия оптического изолятора

Оптический изолятор состоит из трёх элементов:

1. Входного поляризатора;
2. Ячейки Фарадея;
3. Выходного поляризатора - анализатора.

Параметры ячейки Фарадея выбираются так, чтобы ось поляризации света, проходящего через него, поворачивалась на угол 45° . Под таким же углом устанавливаются оси поляризаторов.



При распространении отраженного сигнала в обратном направлении он так же поляризуется в выходном поляризаторе и затем проходит ячейку Фарадея в обратном направлении (B_z). В рез-те поворачивается ещё на 45° влево. На выходе ячейки и на входе входного поляризатора направления поляризации составляют 90° . Т.е. ортогонально входному поляризатору. В результате входной поляризатор подавляет отражённый сигнал, т.е. не пропускает обратное излучение.

Технические параметры оптических изоляторов

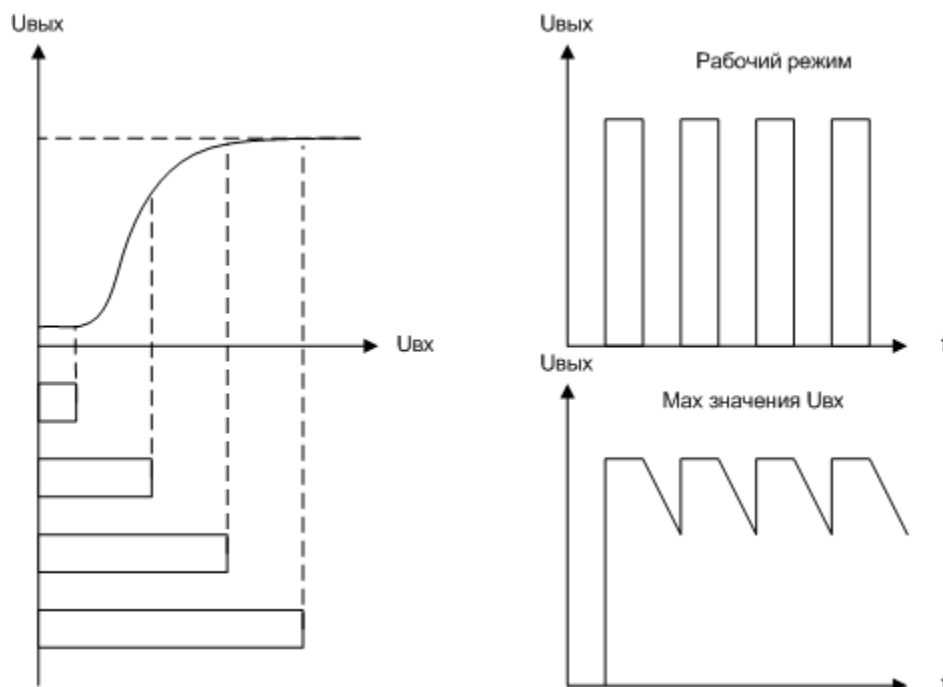
1. Потери в прямом направлении 1-2 дБ;
2. Подавление в обратном >30 дБ (в 1000 раз).

В диапазоне длин волн 1,3-1,55 мкм магнитооптическим материалом, используемом в ячейке Фарадея, является $\text{Y}_3\text{Fe}_3\text{O}_{12}$. Часто интегрируются в лазерный передающий модуль. Причём изолятор устанавливается в соответствии с большой осью эллипса лазера. Так же устанавливается на входе/выходе усилителя EDFA. При этом во всем диапазоне рабочих волн Л изолятор должен сохранять свои свойства.

Поставщики оптических изоляторов: DiCon, FiberPlex, FOCl, Shinokosha.

Оптические аттенюаторы

Применяются для уменьшения мощности оптического сигнала, т.к. большой уровень может привести к насыщению приёмника.



По принципу действия attenuаторы бывают переменные и фиксированные. Переменные attenuаторы допускают регулировку величины затухания в пределах 0-20 дБ для многомодовых и одномодовых волокон с точностью установки величины затухания 0,5 дБ. Регулировка достигается путем изменения величины воздушного зазора.

Фиксированные attenuаторы имеют установленное изготовителем значение затухания, величина которого может составлять 0, 5, 10, 15 или 20 дБ. Затухание может вноситься посредством воздушного зазора фиксированной величины, или посредством специального поглощающего фильтра, встроенного в attenuатор. В последнем случае значительно уменьшается обратное отражение, поскольку фильтр имеет близкий к волокну показатель преломления, что сильно уменьшает обратное френелевское рассеяние.

Семинар 7

Оптические переключатели

Оптические переключатели осуществляют механическую, то есть без оптоэлектронного преобразования, коммутацию одного или нескольких оптических сигналов, переходящих из одних волокон в другие.

Управление

Управление процессом переключения может быть ручное, например при помощи тумблера, или электрическое, при помощи электрического потенциала. Последний тип переключателей более распространен.

Область применения

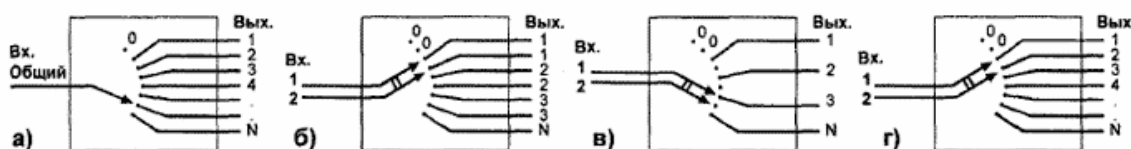
Основная область применения – в составе оборудования для тестирования и мониторинга ВОЛС, а также в составе системы, обеспечивающей повышенную надежность (как, например, оптический обходной переключатель в технологии FDDI).

Реализация.

Реализации отличаются функциональными возможностями: количеством входных и выходных волокон-полюсов и типом волокон (многомодовое или одномодовое), возможностью неблокирующей коммутации сигналов, а также техническими характеристиками, из которых наиболее важные: вносимые потери, обратное отражение, время срабатывания, влияние параметров окружающей среды, наработка на отказ. Разные инженерные технологии используются при коммутации, например, поворотные бипризмы, поворотные зеркала или подвижные волокна. Оптические переключатели являются изотропными устройствами – вносимые потери не зависят от направления распространения сигнала.

Различают несколько типов оптических переключателей:

- Переключатель $1 \times N$ – имеет один входной полюс, сигнал из которого перенаправляется в один из N выходных, рис. 3.19 а;
- Дуплексный переключатель $2 \times N$ – имеет два входных полюса, сигналы из которых могут перенаправляться в выходные полюсы с шагом 2, рис. 3.19 б;
- Блокирующий переключатель $2 \times N$ – имеет два входных полюса, но только один сигнал из двух входных можно передать в выходной полюс – оставшийся сигнал не выходит наружу, рис. 3.19 в;
- Неблокирующий переключатель $2 \times N$ – имеет два входных полюса, сигналы из которых могут перенаправляться в выходные полюсы с шагом 1.



В технологии FDDI используется 8-полюсный (4 входных и 4 выходных) оптический обходной переключатель OBS (optical bypass switch), причем он может находиться либо в основном состоянии с коммутацией полюсов: $vx1-vx1$, $vx2-vx2$, $vx3-vx3$, $vx4-vx4$; либо в байпасовом состоянии с коммутацией полюсов: $vx1-vx2$, $vx2-vx1$, $vx3-vx4$, $vx4-vx3$.

Оптические коммутаторы

Принципиально отличается от переключателей - время срабатывания - доли секунды.

Важный элемент ADN (полностью оптический сетей).

Основные параметры:

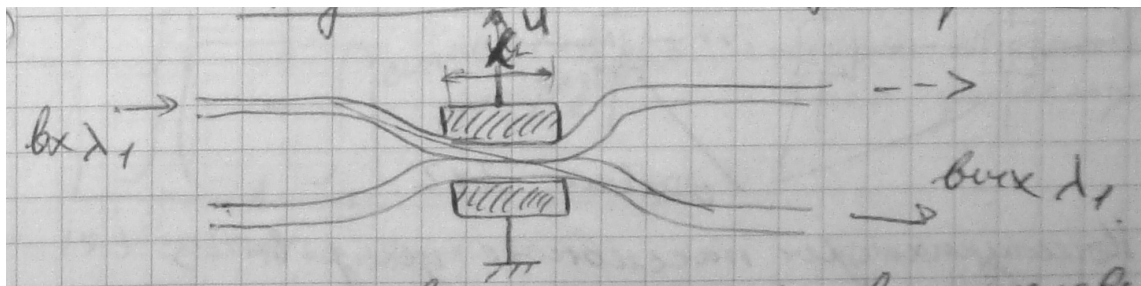
- перекрестные помехи
- вносимые помехи
- скорость переключения
- управляющее напряжение

Типы оптических коммутаторов:

- направленные ответвители
- мостовой балансный интерферометр
- коммутаторы на скрещивающихся волнах.

В основе работы оптических коммутаторов - эффект Поккельса: изменение показателя преломления материала пропорционально напряженности приложенного электрического поля. Эффект наблюдается только в кристаллах, не имеющих центра симметрии.

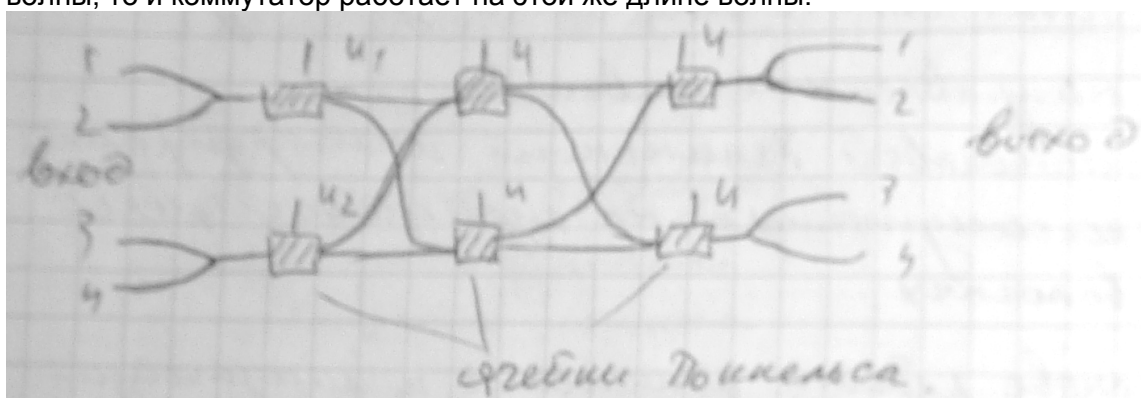
Разветвитель-коммутатор 2×2



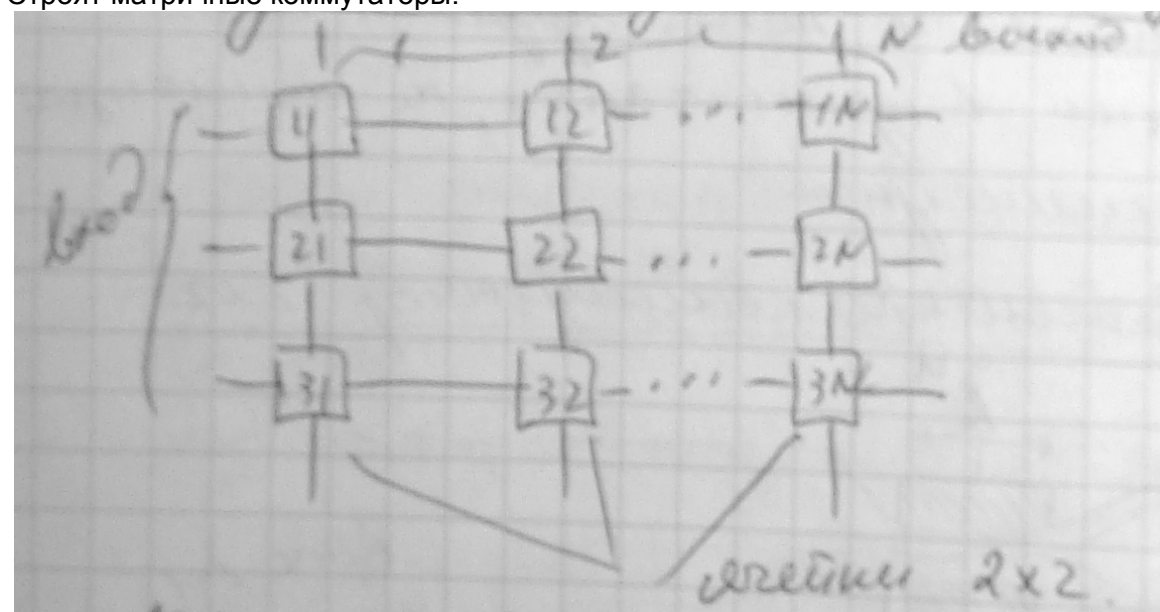
В отсутствии напряжения U связь между волокнами коммутатора 100% - оптический сигнал кроссируется (входит в окно, выходит из другого), а при подачи напряжения U связь изменяется до 0.

Оптические коммутатор пхп.

Строятся на основе коммутатора 2x2. Поскольку ячейка работает на конкретной длине волны, то и коммутатор работает на этой же длине волны.



Фирма D:son выпускает коммутатор 32x32 с 90 ячеек Поккельса.
Строят матричные коммутаторы.

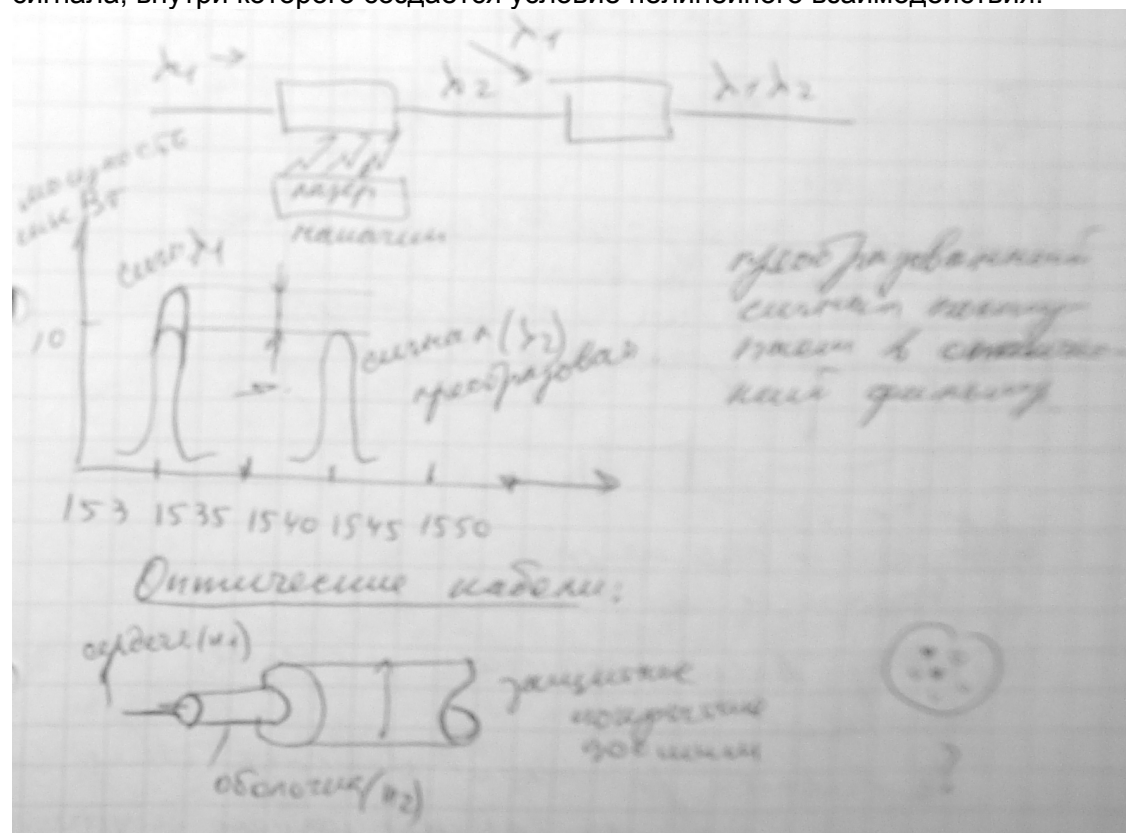


Коммутаторы - пассивные устройства.

Волновые конвертеры

Служат для преобразования сигнала одной длины волны в другую.

Принцип действия: на эффекте нелинейного взаимодействия оптического сигнала с сигналом от лазерной накачки. Метод основан на использовании электрического сигнала, внутри которого создается условие нелинейного взаимодействия.



По количеству волокон:

- симплексные
- дуплексные
- многожильные (4 сотни)

Буфер - первая ступень защиты.

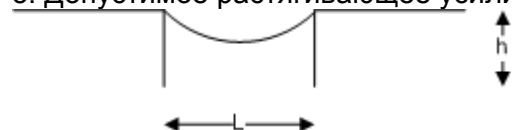
Бывает плотный.

Внешняя оболочка кабеля - полимерный материал для защиты.

Семинар 8

Параметры кабеля

1. Назначение;
2. Наличие электропроводных элементов;
3. Тип и количество волокон;
4. Диапазон рабочих температур;
5. Допустимое растягивающее усилие;



6. Внешний диаметр;
7. Погонный вес;

8. Материя внешней оболочки и характеристики горючести (в условиях радиации используется специальный кабель, т.к. обычный мутнеет).

Оптические соединители

Служат для постоянного и временного соединения волокон.

Основные параметры:

1. Вносимые потери;
2. Уровень обратного отражения (дБ/м).

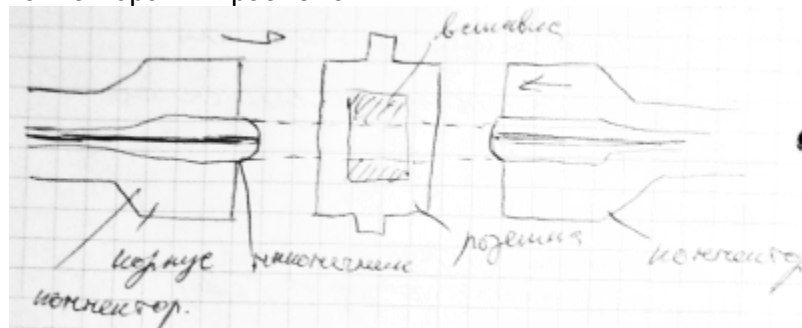
Неразъемные соединители

- Сварка (потери 0,05 дБ, обр.отр. 60 дБ). Специальные сварочные аппараты с автоматическим и ручным оппозicionированием.
- Сплайсы – механическое бессварочное соединение. Допускают многократное, многоразовое использование.



Разъемные соединения (коннекторы)

Используются для разъемных соединений двух волокон – концы волокон оборудованы коннекторами и разъемами.



По типу соединения волокон различают:

- одномодовые (керамические коммутаторы)
- многомодовые (более высокая точность соединения)

Аксессуары и инструменты

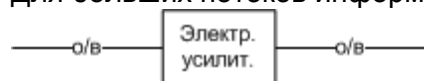
Специальные ножи, ножницы, шлифовальная аппаратура, сварочная аппаратура, стрипперы.

Приборы для монтажа

- Оптические тестеры (для контроля и измерения параметров оптического волокна). На экране видны неоднородности;
- Измерительные комплекты (более высокая точность, ТЛФ-связь);
- Индикаторы излучения (направления передачи и обнаружение сигнала).

Введение полностью оптической сети

Для больших потоков информации (> Гбит/с) на расстоянии нескольких сотен км.



Именно на электронном усилителе (SW, Hub, ...) теряются все «+» оптоволокон. «+»:

1. Поток;
2. Невозможность несанкционированного физического входа в сеть;
3. Низкие помехи.
4. Высокая пропускная способность

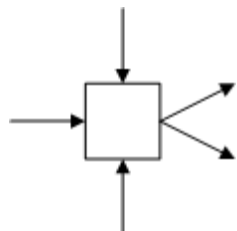
В полностью оптической сети не должно быть электронных усилителей.

DWDM (Density Wave Division Multiplexing – волновое уплотнение) – передача по оптоволокну на многих длинах волн.

Окна прозрачности – существует 3-е окно прозрачности (1530-1560 нм) EDFA. В этом диапазоне в настоящее время размещено до 40 каналов на различных длинах волн. При этом реализованные оптические передатчики TDM способны выводить сигнал в оптоволокну на частоту до 100 ГГц на подходящей длине волны, следовательно емкость одного оптоволокон – 4 Тбит\с.

Где используются?

Там, где используются их преимущества (большое расстояние, т.к. почти нет помех) – глобальные сети (для магистралей).



Оптический хаб, маршрутизатор, коммутатор. Статическая маршрутизация, все настройки вручную.

Лазер		Приемный оптоэлектронный модуль	
Оптическое волокно		Оптический усилитель EDFA	
Волновой конвертер		Оптический фильтр	
Оптический коммутатор		Аттенуатор	
Устройство волнового мультиплексирования (MUX), демультиплексирования (DEMUX)			
Оптический комбайнер, разветвитель			