Оглавление

Лекция по бд № 1 от 9 сентября 2009 г.

В последнее время информационные системы стали меняться, потому что большую популярность приобрели сетевые различных взаимодействия программных систем (в отличие от моносистем, работающих только на 1 компьютере). Современные программы работают в тех или иных сетях (интернет, корпоративные сети – большие и маленькие). Идея состоит в том, чтобы разделить функции системы между различными компьютерами (к примеру, один хранит данные, а другой считает).

В моносистемах было 3 уровня модели данных: концептуальная, логическая и физическая. Существует 3 базовых модели данных: реляционная, сетевая и иерархическая (но также существуют и промежуточные варианты). Из этих 3 моделей самой распространённой является реляционная, так как в основе реляционной модели лежит реляционная алгебра, а значит можно делать различные операции, имея под собой мощную математическую базу. Реляционная модель полностью детерминированная, это значит, что в ней нет тупиковых ситуаций, как, например, в иерархической (можно потерять связи при удалении записи). Сейчас реляционная модель притерпевает изменения к объектости. Это означает, что в поле таблицы находится некий объект. Как следствие, появляется проблема: необходимо добавить поле, которое служит описанием того, что этот объект из себя представляет (или даже какие-то программы для его обработки). В этих условиях полезно распределить функции.

В распределенной системе необходима взаимосвязь и синхронизация , поэтому необходим некотрый коммуникационный узел.

Проблемы распределённых систем:

- Сеть имеет конечную пропускную способность (даже если само оборудование очень хорошее, оно может быть соединено чем-то, что имеет низкую пропускную способность)
- Взаимодействие информационных потоков
- Проблемы аппаратного характера (выход узлов из строя)

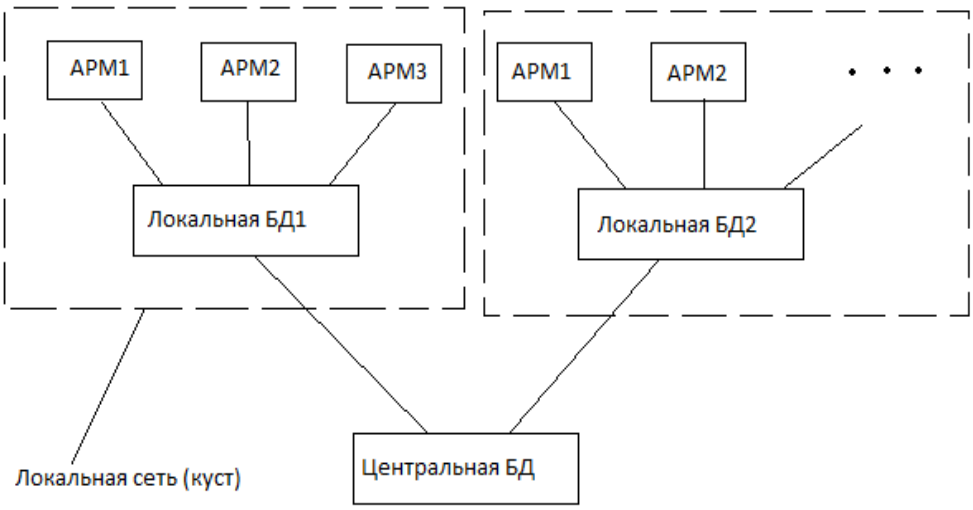
Таким образом, самая сложная задача состоит даже не в сохранении целостности данных, а в поддержке их актуального состояния. Системы управления базами данных делятся на профессиональные (которые умеют работать с сетью) и для домашнего использования (которые не обязаны уметь работать с сетью).

Архитектура и принципы распределенного подхода.

1) Базовая модель распределенной системы является реляционной.

2) Распределённые системы не поддерживают независимость данных от способа их хранения и обработки (из-за того, что канал передачи информации не считается надёжным).

АРМ – автоматизированное рабочее место (кассы, пк и т.д.)



В распределенных системах существует проблема репликации данных (Пример: если эта система представляет собой систему для продажи жд билетов, то в случае разрыва связи Локальной БД1 и Локальной БД2, один и тот же билет могут купить 2 разных человека).

Репликация

Репликация – размещение нескольких копий одних и тех же данных (реплик), к которым осуществляется доступ со стороны одного или более процессов.

Цели репликации:

- Повышение надёжности системы
- Повышение производительности системы

Полная репликация – все данные Центральной БД хранятся на всех АРМах. (Для большой дб эта операция сложная, поэтому делают кустовую репликацию).

Набор требований к распределённой бд:

1) Она должна обладать локальными и глобальными средствами доступа к данным
2) Единообразная логика всех систем на армах куста
3) Малое время реакции системы на запрос пользователей
4) Достоверно высокая степень надёжности, которая исключает разрушение данных при выходе из строя отдельных компонентов системы
5) Достаточная степень открытости, позволяющая наращивать число армов в локальной бд
6) Должна существовать система восстановления данных после сбоев и аварий
7) Высокая степень защищенности
8) Высокая эффективность за счёт использования эффективности алгоритмов использования сетевых ресурсов
9) Механизм репликации и обновления множественных копий

При составлении технических заданий к распределённой бд необходимо учитывать след. Элементы:

I.

1) Требования к количеству данных (в распределенных системах они измеряются терабайтами)
2) Типы запросов (есть класс типовых запросов)
3) Кластеризация типовых запросов по критериям
4) Количество аппаратных ресурсов
5) Величины затрат (на прокладку коммуникаций и т.д.)

Лекция по бд № 2 от 9 сентября 2009 г.

Основные проблемы на этапе проектирования распределенных систем:

- Проблема репликации
- Проблема транзакций

Принципы построения распределенных систем:

1) Минимизация интенсивности обмена данными (в рамках куста существует некий трафик, межкустовой трафик – трафик в степени N)
2) Оптимальное размещение приложений (какая часть бд должна быть на армах? Вообще необходимо уменьшить число программ, передаваемых по сети из соображений безопасности)
3) Декомпозиция данных (распределение данных между узлами)
4) Периодическое выполнение действий, обеспечивающих целостность данных (арбитраж: проверка поступления информации и её целостности по специальным правилам, пользовательский арбитраж – есть внутренние и внешние процедуры)

При построении распределённой системы необходимо написание технического задания.

Требования к тех. заданию:

1) надо учитывать количество узлов в сети
2) Учитывать кластеризацию самих узлов(из отдельных компьютеров формируется сеть, которая подчиняется единым принципам маршрутизации , есть сервер, есть клиент), моделировать предполагаемый сетевой трафик, локальную сеть надо правильно коммутировать в глобальную сеть
3) Декомпозиция элементов данных и программ обработки между разными узлами
4) Разработка механизмов приведения армов к непротиворечивому состоянию

Типы распределенных архитектур (по возможности репликации данных)

1. Недублирующее разбиение (использует большой объем часто меняющихся данных).
2. Системы с частичной репликацией (используют небольшой объём часто меняющихся данных). Так работают всякие новостные системы.
3. Полное дублирование данных (небольшой объём редко меняющейся информации). Полученная информация тут же дублируется на куе узлов.

Реальные распределенные системы обычно колеблются между этими 3 крайностями.

Синхронизация доступа к данным.

1. Необходимо управлять данными быстро
2. Необходима система, обеспечивающая целостность операций синхронизации
3. … *(тут Дэн непонятно написал)* спецификации. Тут важно построить критерий вероятности того, что информация будет нормально передаваться.

Для распределенных систем большое значение имеет словарь данных :

1. Позиция … *(тут тоже непонятно)*
2. Спецификация (настроечные переменные)
3. Необходимый информационный поток, который нужен данному арму
4. Режим доступа к данным:
    - Чтение, запись, добавление - низкоуровневый режим
    - Удаление, изменение – высокоур. режим
5. Полномочия пользователя данного узла

Лекции 3, 4. (первый абзац с intuit.ru)

Транзакции

Транзакция – логическая единица работы в базе данных, а так же единица восстановления информации при сбое СУБД. При фиксации изменений в базе данных гарантируется сохранение либо всех изменений, либо ни одного. Более того, выполняются все правила и проверки, обеспечивающие целостность данных.

Транзакции базы данных обладают свойствами, сокращенно называемыми ACID (Atomicity, Consistency, Isolation, Durability).

- Неделимость (Atomicity). Транзакция либо выполняется полностью, либо не выполняется.
- Согласованность (Consistency). Транзакция переводит базу данных из одного согласованного состояния в другое.
- Изолированность (Isolation). Результаты транзакции становятся доступны для других транзакций только после ее фиксации.
- Продолжительность (Durability). После фиксации транзакции изменения становятся постоянными.

Модели непротиворечивости.

1) *Строгая непротиворечивость.*

   Появляются данные -- они сразу копируются на все узлы. Но в такой модели время между чтением элемента X и его записью растёт экспоненциально в зависимости от числа узлов сети. Мы не можем прочитать X, пока мы его не скопировали на все узлы.

2) *Линеаризованная модель непротиворечивости.*

   Чтение и запись элемента X здесь происходит в некоторой последовательности.

   $T_{op1}(X) < T_{op2}(X)$, где op1(X) и op2(X) – операции чтения или записи элемента данных X. Тогда операция op1(X) предшествует операции op2(X). Механизм реализации – синхронизация времени (Но нельзя делать синхронизация во время сеанса репликации).

3) *Последовательная непротиворечивость.*

   Чтение и запись элемента X производятся в некоторой последовательности, определяемой программой (Например, запишем несколько блоков элемента X, сообщим об этом остальным узлам, они тоже запишут).

4) *Причинная непротиворечивость.*

   Операция записи имеет причинно-следственную связь с операцией чтения. Здесь перед какой-либо операцией сообщается всем узлам о том, что сейчас произойдёт эта операция (посылается пакет), в результате, узлы уже готовы к ней.
   Недостаток: необходима служба, которая будет ловить пакеты, она должны всё время быть в оперативной памяти (пример: процесс прослушивания сети у Oracle).

5) *Fifo модель.*

   Отличается от причинной непротиворечивости тем, что есть специальный стек, куда помещаются эти пакеты.

6) *Модель слабой непротиворечивости.*

   Это модель, в которой есть некоторая синхронизирующая переменная, с которой ассоциируется реплика.

Назовём эту переменную S. Над S может выполняться только операция синхронизации (По умолчанию S = 0. Проходит изменение значения X на некотором узле —> (S = 1) —> вызывается алгоритм копирования X на другие узлы. Когда S = 0, переменная X реплицирована на всех узлах).

3 основные свойства модели слабой непротиворечивости:

- Доступ к S должен выполняться на условиях последовательной непротиворечивости (S = S1 S2 S3 …)
- С S не может быть произведена ни одна операция до полного завершения предшествующей операции чтения или записи.
- С элементом данных X не может быть выполнена ни одна операция до полного завершения репликации.

Недостатки это модели:

- Недоступность X до окончания репликации
- Распространение неправильных данных в случае ошибки по всей сети.
- Если происходит разрыв связи хотя бы с 1 узлом, то S = 1 до тех пор, пока связь с узлом не наладится.

7) *Свободная непротиворечивость.*

Синхронизация делится на 2 этапа: захват и освобождение. Захват(S) импортирует изменения из всех копий в локальную копию. В данном случае S – это список. Изменить X можно сразу же после предшествующего изменения, тогда создастся ещё один список (список ещё называется карантином, потому что там все данные на время блокируются).

Освобождение(S) – распространение всех изменений из локальной копии на ассоциированные узлы. Из всех вариантов значения X надо найти те, которые могут быть достоверными. Надо выбрать одно из них. Тут есть несколько способов, но ни один из них не гарантирует достоверности X: спросить администратора БД, расставить приоритет узлов и выбрать X с главного узла, признать достоверным последнее значение X.

http://jonni3.narod.ru/I_Progr/gl4/gl4.html#9

Лекция 5

Протоколы непротиворечивости

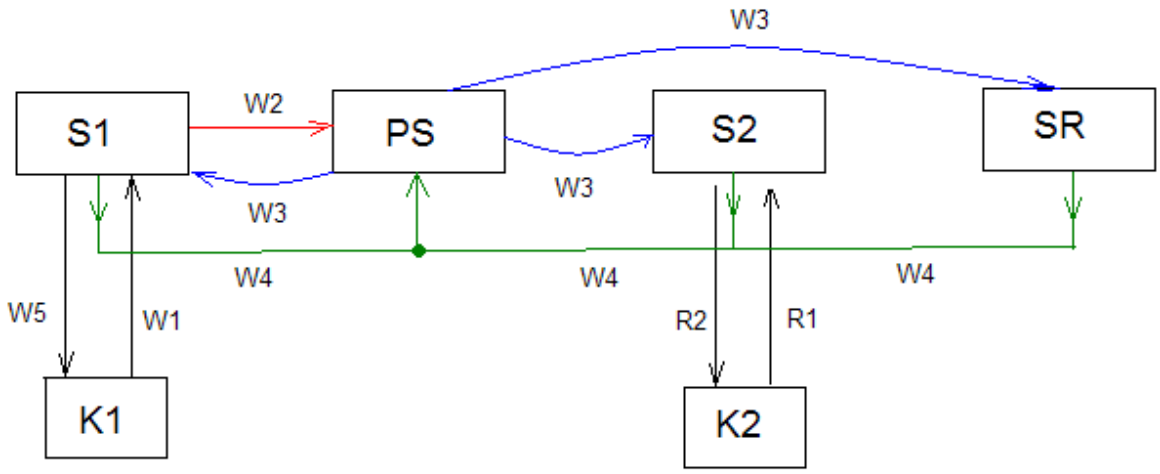
На базе первичной копии.

Первичная копия – достоверные данные. Менять информация на первичной копии можно только после завершения изменения данных на других узлах.

Протокол на базе первичной копии с удалённой записью.

S_i – сервера, PS – первичный сервер, SR – сервер резерва (обеспечивает хранение дополнительной информации с целью восстановления данных после сбоя, здесь хранятся, в частности, удалённые данные), К1 и К2 – клиенты.

Допущение: все операции и сигналы распространяются мгновенно.



- W1 – запрос на запись;
- W2 – пересылка запроса на PS;
- W3 – сигнал на обновление резервных копий. Он активирует серверы S2 и SR. Активация происходит, пока не начнётся таймаут. Если оп каким-либо причинам не удаётся активировать S2 и SR, то операция записи не пройдёт.
- W4 – подтверждение готовности выполнения обновления элемента X. Блокирует элемент X.

- W5 – сигнал того, что обновление успешно проходит, запись X на S1.
- R1 – запрос на чтение элемента X:
- R2 – чтение элемента X.

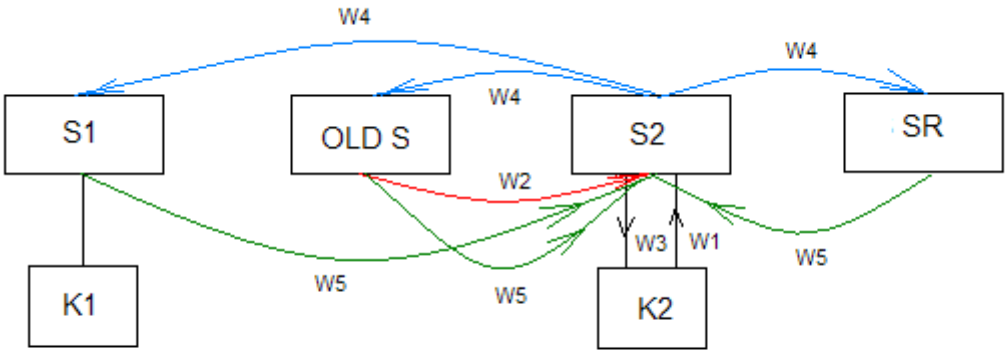
Достоинства: повышение надёжности системы и увеличение производительности на стадии записи (за счёт отсутствия откатов).

Недостатки:

- Отсутствие реального механизма контроля связи сети. Здесь работает только таймаут (таймаут может быть разным в зависимости от физического соединения узлов. Например, в оптоволоконных сетях данные передаются быстрее, поэтому таймаут меньше).
- Между W3, W4, W5 нет механизма контроля данных, особенно на сервере PS, который подвержен хакерским атакам.
- K2 может длительное время находиться в состоянии ожидания чтения элемента X.

Протокол на базе первичной копии с локальной записью.

OLD S – старый сервер (содержит устаревшие данные). Теперь Si – первичные сервера.



- K2 подаёт сигнал W1 на S2 (сигнал на запись).
- W2 – перемещение элемента X на новый первичный сервер S2 с OLD S.
- W3 – подтверждение записи на S2.
- W4 – сигнал на обновление резервных копий.
- W5 – подтверждение обновления.

Достоинства: локальный сервер кочует в сети — повышена безопасность. Локальные серверы могут быть виртуальными.

Недостатки:

- Если один из серверов не ответит на W4 (S2 уже обновился, а какие-либо другие серверы не обновились), то происходит откат репликации.
- Копирование элемента X с OLD S на S2 может занять время и место на сервере S2 — канал между S2 и OLD S должен быть быстрым и устойчивым к хакерскому вмешательству.

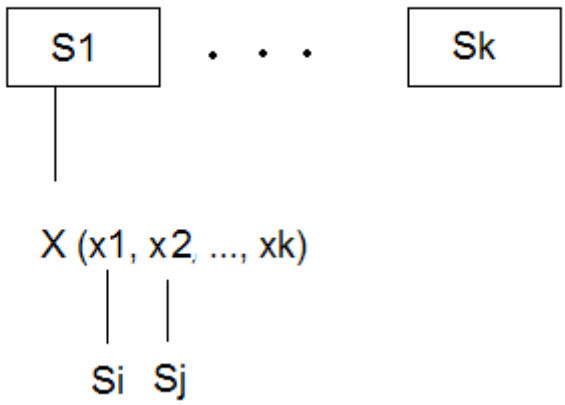
Отложенная репликация – такая репликация, которая может производиться не сразу на каком-либо сервере, если ему не очень нужны реплицированные данные.

Первая модель характерна для банков. Вторая – для мобильных операторов.

Лекция 6

Протоколы непротиворечивости на базе реплицирующих записей

Основная идея: с операцией репликации ассоциируется несколько реплик.



Способы:

1) Хабовский. Передача избыточной информации.
   Недостаток: избыточность. **Достоинство:** простота.

2) Фильтрация Si: собрать в пул реплик только те реплики, которые принадлежат одинаковым серверам и направить в сеть.

   - **Достоинства:** разгружается сеть, используются только те серверы, которые необходимы для репликации.
   - **Недостатки:** загружается сервер Si дополнительной работой. Они должны знать, на какие узлы что загружать.

3) Программно-аппаратная фильтрация серверов. Заставить программу выполнять алгоритм фильтрации серверов, а не сами сервера.

Протокол Кворума.

Кворум – обобщённый сетевой ресурс. N – число реплик на некотором узле, Nr – число реплик, которые отданы в кворум чтения, Nw – число реплик, которые отданы в кворум записи. Если (Nr + Nw) > N, то при опросе Nr серверов хотя бы 1 содержит последнюю версию обновляемых данных. Если Nw > N/2, не существует одних и тех же данных, имеющих одинаковую версию.

Выводы:

1) Модели репликации данных являются фундаментальной основой распределенных информационных систем.

2) Протоколы репликации реализуют те или иные гипотетические модели о отображают их на алгоритмы.

3) Компоненты репликации и алгоритмы репликации участвуют в программно-аппаратном кворуме распределенной информационной системы.

Физическая модель распределенной информационной системы.

Сетевой узел – любой электронный элемент, имеющий свой собственный адрес. Адрес обеспечивает идентификацию в сети.

Сегмент – некоторая сетевая последовательность узлов и их соединений, выполненная на одинаковом уровне соединения (с одинаковым типом соединения).

- кабель (кабель, оптоволокно).
- некабельное соединение (радиосоединение). Например, IRDA – инфракрасное соединение.
- бескабельное соединение (w-less).

Беспроводные сети.

1) ИК-диапозон (IRDA). Расстояние 10-15 м.
   - **Достоинства:** простота, дешевизна.
   - **Недостатки:** малое расстояние, не умеет преодолевать преграды (прямая видимость). – принтер, пульты и т.д.
2) Bluetooth.
   - **Достоинства**: расширяется частотный диапазон —>более мощный сигнал, умеет преодолевать препятствия, быстрота.
   - **Недостаток**: энергозависимость.
3) IEEE 802.11 – WiFi.

   Мощность сигнала зависит от расстояния.

   Если мощность сигнала плохая, то зарядка быстро садится.

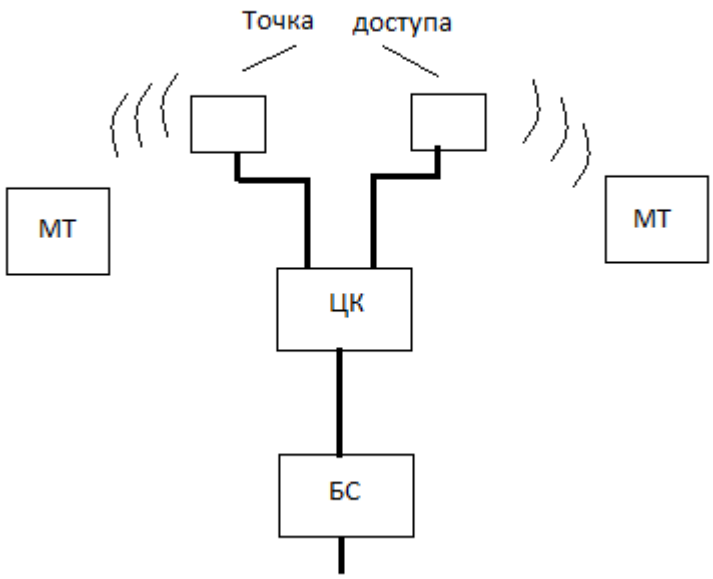
Архитектура беспроводной компьютерной сети.

Централизованная.

- Базовая станция (БС) – набор специальных серверов, с помощью которых происходит передача данных + компьютерная поддержка.
- ЦК – центральный коммутатор.

Такая архитектура используется в сотовых телефонах, в удалённых системах (мониторинг нефтяных вышек, например)

БС, ЦК и точки доступа связаны кабельными сегментами, а вот МТ (мобильные терминалы) связываются с точками доступа беспроводной связью.



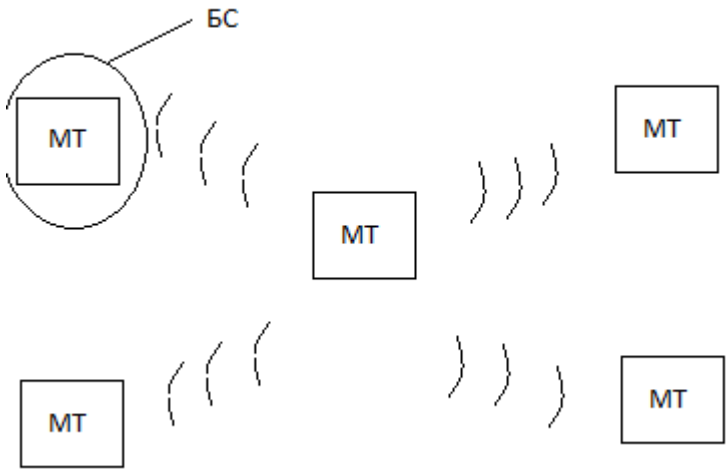
Достоинства:

- Высокая эффективность
- Высокая дальность сигнала

Недостатки:

- Все устройства привязаны к ЦК, т.е. при сбое ЦК МТ тоже отключаются.

Децентрализованная архитектура.



В пределах сети существует дискретное количество диапазонов. 1 МТ выделается в качестве БС, остальные автоматически настраиваются на частоту БС.

Достоинства:

- Защита системы от несанкционированного доступа
- Широкое применение

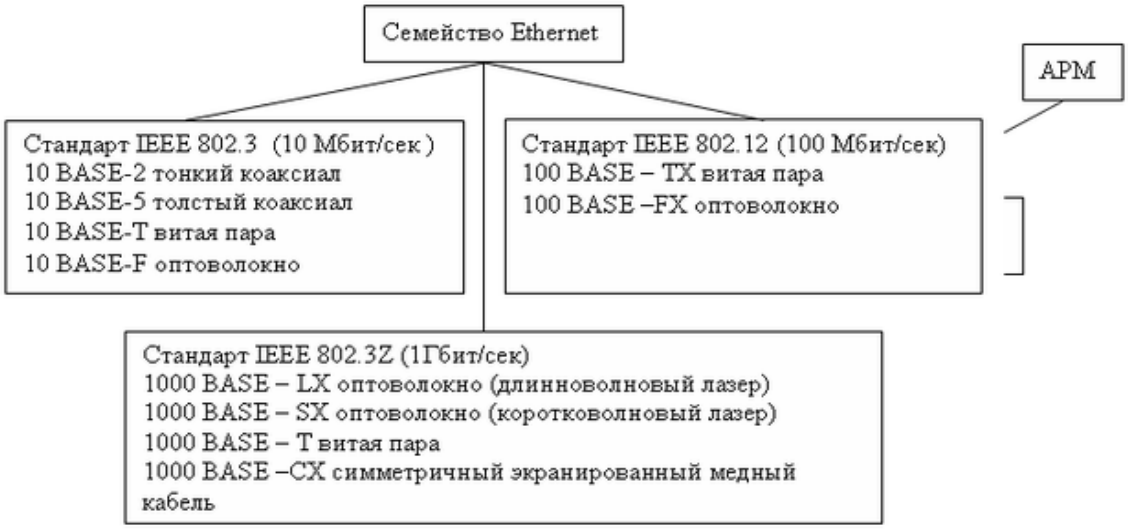
Недостатки:

- С увеличением числа энергоносителей увеличивается время работы. Также увеличивается количество коллизий, если вещание в широком диапазоне.
- Ограниченная дальность.

Локальные вычислительные сети стандарта рабочей группы

В настоящее время в области телекоммуникационных технологий высокопроизводительные компьютерные сети - наиболее динамично развивающееся звено. Сейчас, практически в любом офисе, организации компьютеры объединены в локальные сети, многие – имеют выходы в глобальную мировую сеть по интернетовскому протоколу или другим LAN протоколам.

В данном курсе мы ограничимся рассмотрением наиболее популярной и распространенной сети стандарта Ethernet и ей подобных в контексте проектирования и реализации систем распределённых БД. На рисунке приведены подсемейства Ethernet с разной скоростью передачи данных и *НЕКОТОРЫЕ* стандарты кабельных соединений.



Важное свойство сетей семейства Ethernet декларирует сходство в правилах построения сетевых топологий.

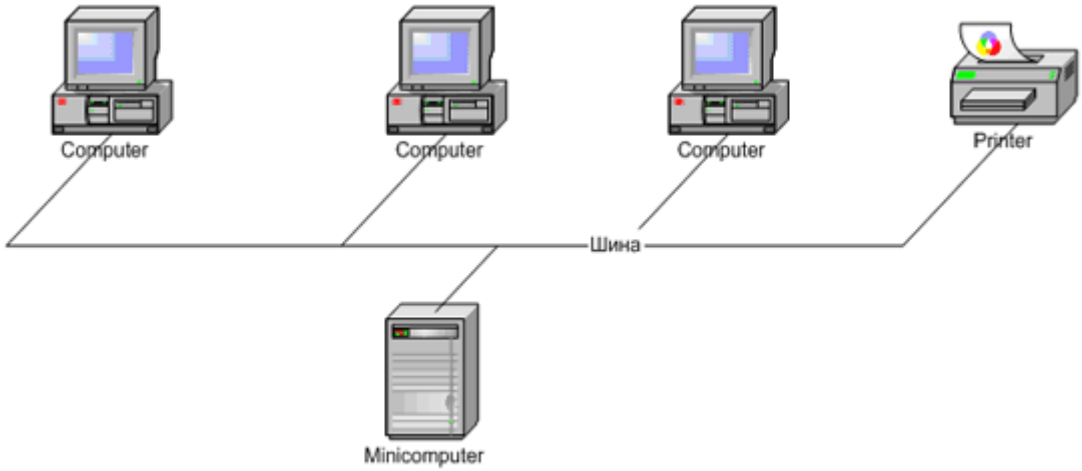
Основные понятия сетевой терминологии

1. Устройство, являющееся источником/приемником сетевого трафика называется **узлом**. Узел всегда имеет сетевой адрес. Примеры узлов: компьютер, принтер, маршрутизатор, HUB.

2. **Кабелем** называется несколько проводников, объединённых общей защитной оболочкой. Проводниками могут быть как медные или стальные провода, так и стекловолокна.

3. Участок сети, выполненный из кабеля одного типа, называется **кабельным сегментом**.

4. Подсоединение узлов по длине коаксиального сегмента называется **шинной топологией**.



5. Подсоединение узлов к центральному концентратору (многопортовому повторителю) посредством витой пары или оптоволоконного кабеля точечного сегмента называется **звездообразной топологией**.

6. **Концентратор** (HUB) – устройство, повторяющее все сигналы (в том числе и коллизионные) по всем портам.

- простое решение
- нет анализа поступающих пакетов
- нет фильтрации

7. **Маршрутизатор** – устройство, позволяющее определять и назначать маршрут следования сигналов.

8. **Мост** – устройство, позволяющее фильтровать сигналы сети и пропускать определённые пакеты.
Есть 2 режима работы: *режим обучения & режим фильтрации*

9. **Локальная вычислительная сеть** (ЛВС) - это набор соединённых кабельным сегментом устройств, которые получают одни и те же пакеты данных (трафик) в виде стандартных сигналов.

Итак, в сети все устройства посылают пакеты и «слушают» друг друга.

10. Появление на некотором узле пакетов от разных адресатов в один и тот же момент времени называется **коллизией**. Попавшие в неё узлы через случайно выбранный промежуток времени повторяют попытку послать пакет. Отсутствие коллизий указывает узлу на успешное прохождение пакета.Несложно определить максимальный период кругового обращения пакета – это время прохождения коллизионного пакета между двумя наиболее удаленными узлами сети (туда и обратно). Тогда коллизионной областью называется зона оповещения (о коллизии) всех узлов сети в течение максимального периода кругового обращения.

Стандарт IEEE 802.x определяет ЛВС как коллизионную область.

Проектирование сетей рабочей группы (инженерный подход)

Обычно начинается с выбора кабельных систем. Рассмотрим некоторые, наиболее используемые в практической области, виды кабелей.

Тонкий коаксильный кабель (диаметр до 5 мм)

Выполняется с оболочкой из:

- поливинилхлорида (PVC-кабель)
- тефлона (FEP-кабель)

Пропускная способность: 10 Мбит/сек.

Подключение узлов в шинной топологии через Т-образные BNC-соединители

Минимальная длина сегмента: 0.5 м

Максимальная длина сегмента: 185 м

Максимальное число подключений узлов к одному кабельному сегменту: 30

Особенности:

- требует концевых 50-омных заглушек
- не требует заземления.

Толстый коаксиальный кабель (диаметр до 10 мм)

Выполняется с оболочкой из:

- поливинилхлорида (PVC-кабель)
- тефлона (FEP-кабель).

Пропускная способность: 10 Мбит/сек.

Соединительные элементы: разъём N-series (с возможным переходником на AUI порт)

Минимальная длина сегмента: 2.5 м.

Максимальная длина сегмента: 500 м.

Максимальное число подключений узлов к одному кабельному сегменту: 100

Особенности:

- требует установки концевых заглушек
- требует заземления в одной точке

Кабель с витыми парами

Выполняется в виде:

- 4-х парного кабеля
- кабельного жгута из 25 и более пар

Бывает экранированный (STP,FTP) и неэкранированный (UTP).

Делится на следующие категории по полосе пропускания:

- 3-категория(level 3) 15МГц STP, FTP, UTP
- 4-категория(level 4) 20МГц STP, FTP, UTP
- 5-категория(level 5) 100 МГц STP, FTP, UTP
- 5е-категория (улучшенная leve1 5) 100 МГц STP, FTP, UTP
- 6-категория (класс E) 200 МГц STP, FTP, UTP
- 7-категория (класс F) 600 МГц S-STP

Пропускная способность:

- 10 Мбит/с - все категории
- 100 Мбит/с - 5,5е,6,7 категории
- 1000 Мбит/с - 5е,6,7 категории

Соединительные элементы: розетки и вилки

- 8 контактные RJ-45 - 3,4,5,5е,6 категории
- гибридные RJ-45 – 7 категории
- 50 контактный разъём Telco

Максимальная длинна сегмента:

- без усиления сигнала до 150 м;
- с усилителем сигнала- до 225 м (level 5 и выше)

Тестирование витой пары

1. Схема соединений
2. Длина сегмента
3. Погонное затухание (ослабление сигнала с удалением от источника)
4. Переходное (наведённое) затухание на ближнем/дальнем конце (влияние сигнала одной пары на другую)
5. Сигнал-шум

Факторы увеличения пропускной способности

- Чистота металла (меди)
- Медная проволока увеличенного диаметра (снижает погонное затухание)
- Применение специальных разделителей между парами

Оптоволоконный кабель

Обычно состоит из двух пучков оптоволокна, но может быть и один световод. Соотношения диаметров сердцевины световедущей жилы/окружающего слоя 50/125 микрон, 62/5.125 микрон для многомодового кабеля и 8/125 - для одномодового.

Многомодовое и одномодовое оптоволокно отличается емкостью и способом прохождения сигнала.

Так для многомодового оптоволокна по независимым световым путям (модам) может передаваться сигналы с различными длинами волн или фазами. Диаметр светопроводящей жилы (50 или 62.5 микрона) выбирается из соображений минимальной дисперсии отраженного от поверхности серцевины луча. Пропускная способность многомодового оптоволокна может изменяться в пределах от 2.5 до 10 Гбит/сек.

Одномодовое оптоволокно передает сигнал только с одной длиной волны или фазой. Малый диаметр световода (8 микрон) обеспечивает меньшую отраженную дисперсию, что в свою очередь увеличивает длину сегмента до 2 км. Пропускная способность одномодового оптоволокна > 10 Гбит/сек (30-60 Гбит/сек). Электронно оптические компоненты одномодового оптоволокна дороже многомодового.

Топология сети - звезда или кольцо.

Оптоволоконный жгут может содержать произвольное число световодов (обычно кратное 6). Стандарт не оговаривает их количество, поэтому проектировщик должен сам определить сколько ему необходимо многомодовых и одномодовых пар.

Кабель, в котором часть световодов — одномодовая (~25%), а другая — многомодовая (~75%), назывется ***гибридным***.

При выборе оптоволоконного кабеля необходимо учитывать:

1. Длину (нельзя ошибаться в меньшую сторону, так как оптоволоконный кабель дорого, не надежно и трудоемко соединять)
2. Диаметр световодов (обычно 62.5 микрона для многомодового и 8 микрон для одномодового)
3. Оптическое окно - длину волны лазерного оборудования (850, 1300, 1310, 1550 нм)
4. Затухание (аналог сопротивления для медного кабеля)
5. Пропускную способность принимающего/передающего оборудования
6. Качество оптоволокна (стандартное, высококачественное, премиумное)

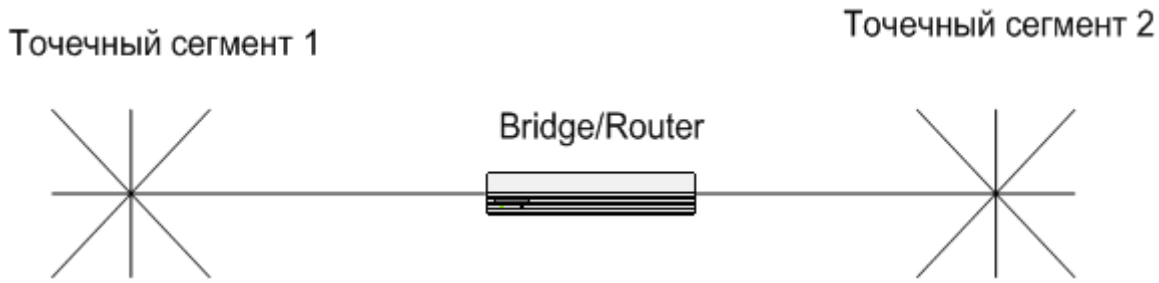
Соединительные штекеры:

1. ST (штыковидные);
2. SC (двухсторонние защелкивающиеся)
3. SMA.

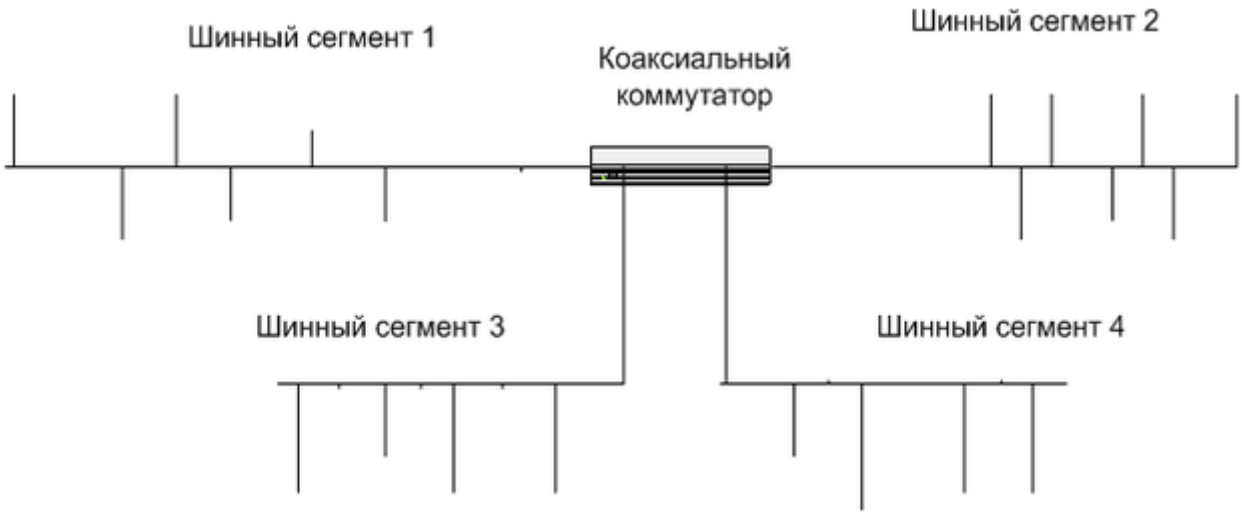
Расширение сети

Под **расширением сети** понимается увеличение числа рабочих мест.

Расширение при топологии «звезда» производится через специальный порт маршрутизаторов:



Соединение шинных сегментов:



Возможна также смешанная топология. При этом коммутационное оборудование должно поддерживать режим dual speed.

Средства управления ЛВС

Управление сетью разделяется на:

- управление устройствами
- управление трафиком

Средства:

- Агенты SNMP (Simple Network Multiply Protocol)
- Агенты среды анализа трафика
- Внутриполостное наблюдение
- Внеполосное наблюдение
- Распределенное наблюдение

Программно-аппаратная поддержка:

- Терминальная консоль (прямое подключение, режим VT100, управление через консольные порты)
- Консоль управления цепочкой (ПЭВМ, ОС, специальное программное обеспечение, соединение с концентратором 0-модемным или коаксиальным кабелем)
- Консоль сетевого трафика (ПЭВМ, ОС, развитое программное обеспечение, соединение с концентратором через стандартный порт RJ45)

Оценочный коэффициент насыщенности коллизионной области сети

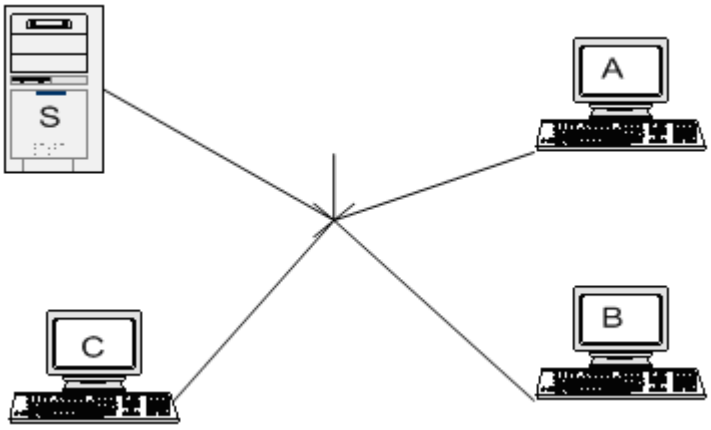
*LAN = 100% * (число бит) / ((число секунд) * (скорость)*10^6)*

Способы и средства увеличения пропускной способности ЛВС

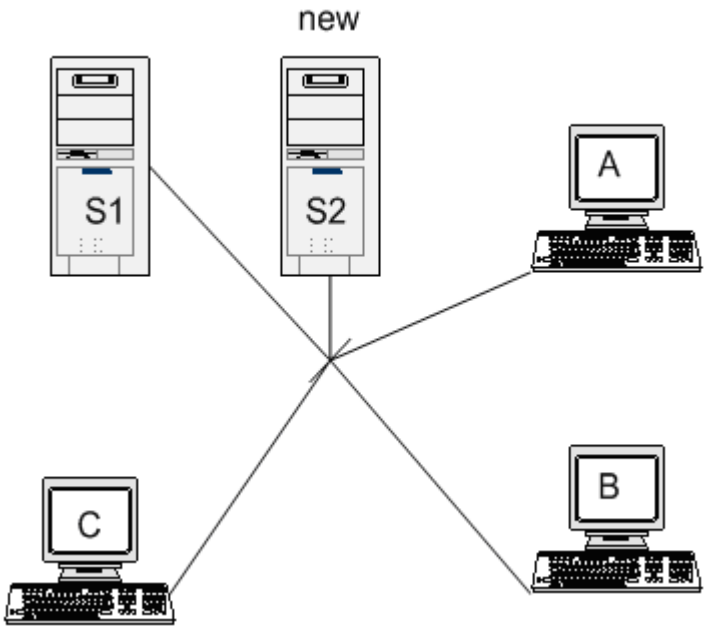
Увеличение пропускной способности ЛВС может осуществляться:

- пассивно – за счет замены оборудования и увеличения скорости сетевого обмена с 10 до 100 или 1000 мбит/сек
- активно – за счет деления коллизионной области с помощью маршрутизаторов, мостов и коммутаторов в соответствии со схемами трафика, обеспечивая этим наилучшее использование ширины полосы пропускания сигналов.

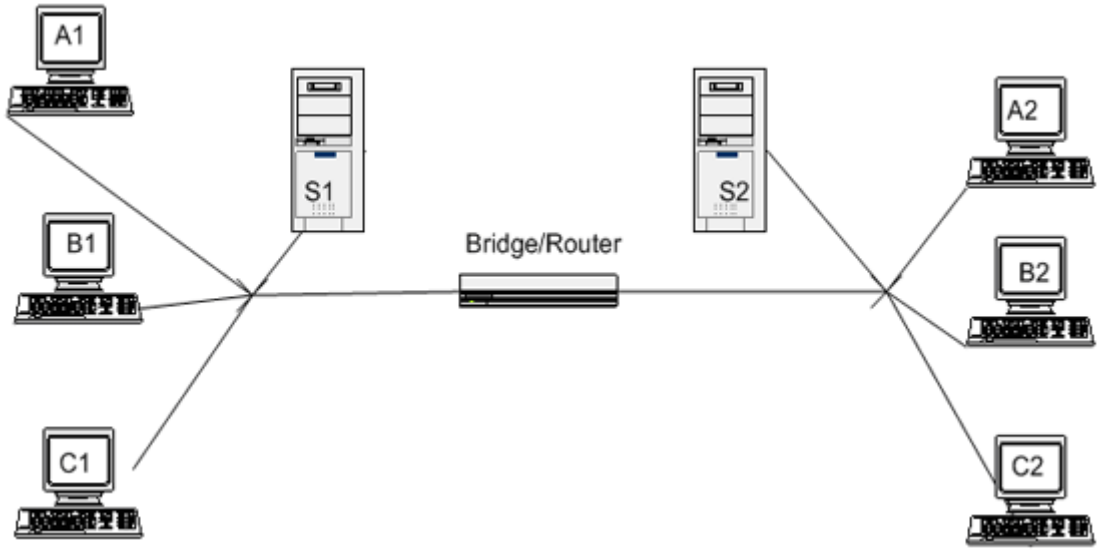
Рассмотрим точечный сегмент Ethernet.



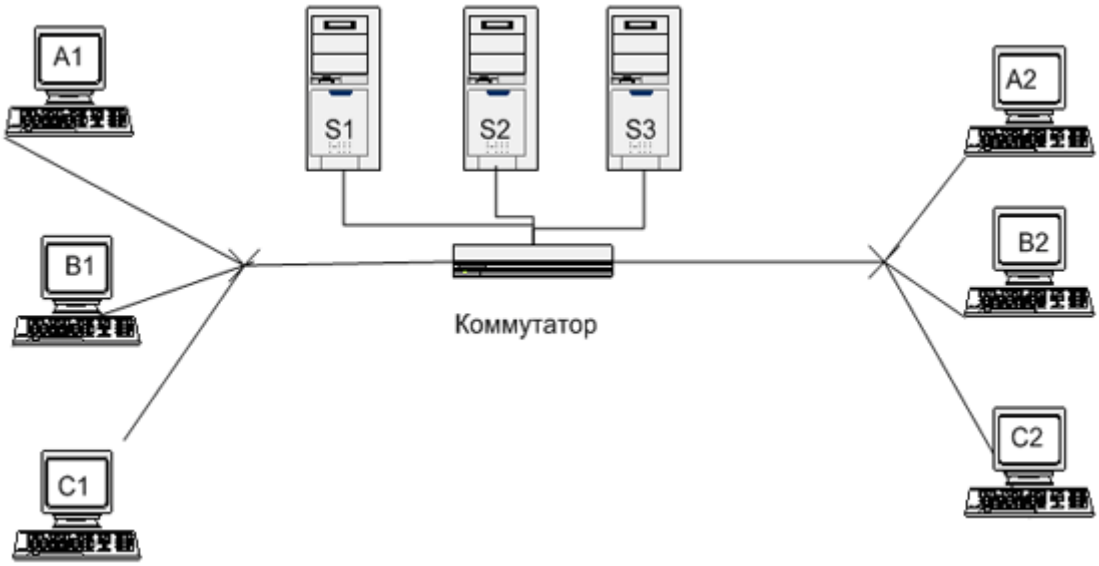
Сеть работает медленно при слабом насыщении коллизионной области (LAN << 40%)
Критическое место – *сервер*, требуется разделить его функции и часть портировать на новое оборудование.



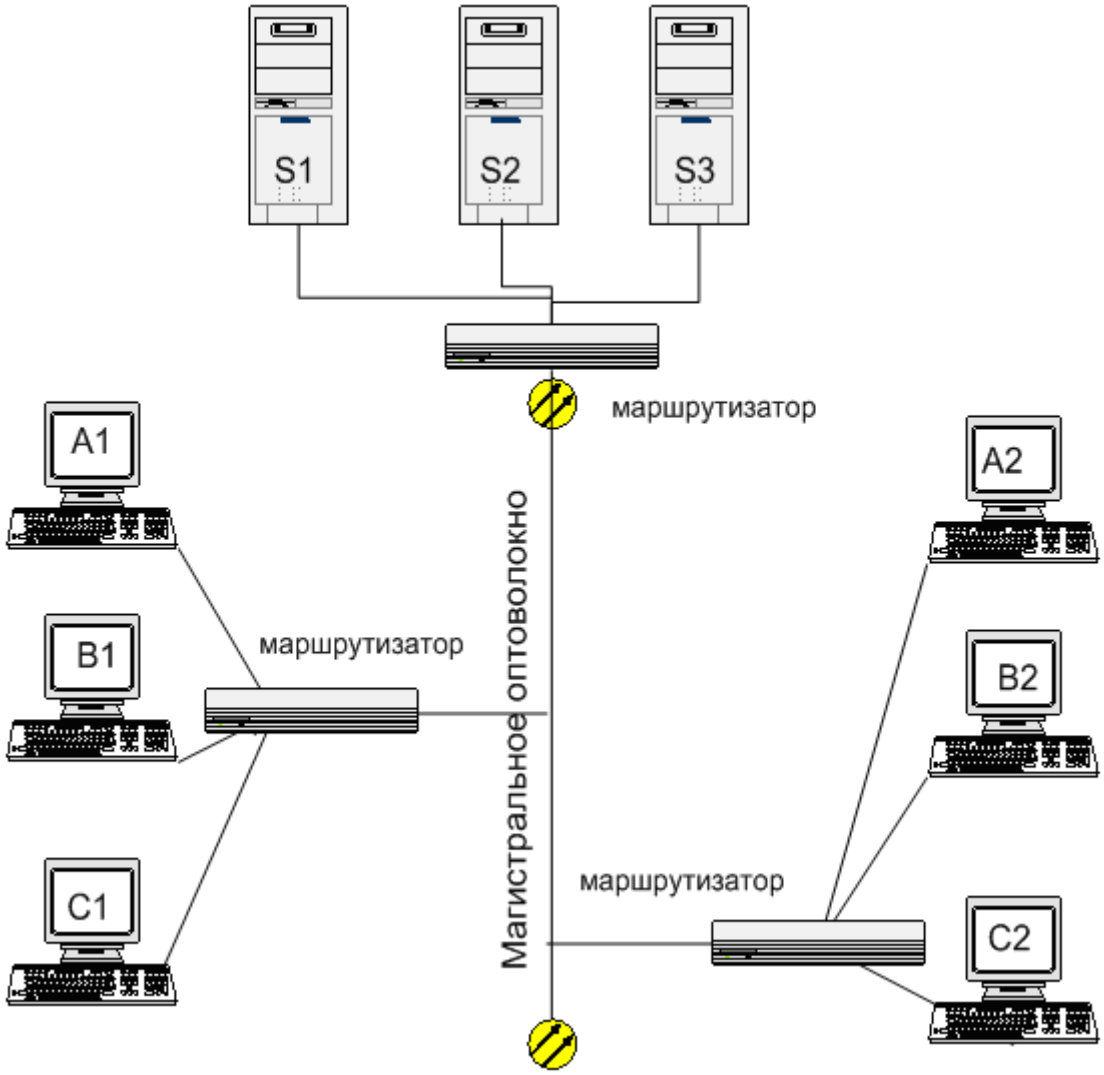
Сеть работает медленно при LAN ~ 40%, тогда можно *разделить сегмент на два подсегмента*, соединив их мостом или маршрутизатором. При этом в каждой коллизионной области имеется свой сервер.



Если всем клиентам сети при LAN >> 40% необходим online доступ к различными серверами, то при условии сбалансированного трафика, рекомендуемым *решением увеличения пропускной способности сети является установка коммутатора*.



Если имеется несколько коллизионных областей с высоким уровнем локального трафика и одновременно требующих разнообразного серверного обслуживания, то для увеличения пропускной способности сети *используются маршрутизаторы*.



Защита информации и повышение безопасности работы в ЛВС

Защита может быть:

- физической – закладывается при проектировании сети и включает меры, ограничивающие непосредственный доступ к сетевым устройствам (закрывающиеся монтажные шкафы, специальные короба, серверно-коммутационные зоны и т.п.)
- логической – на программно-аппаратном уровне коммутаторов, маршрутизаторов и мостов.

В любой сети передачи данных важно, прежде всего, ***ограничить физический доступ*** к сетевому оборудованию и линиям связи.

Защита сетевого оборудования осуществляется посредством решения следующих задач:

- выбор правильной конфигурации оборудования и политики контроля. Следует разработать план политики защиты сети в отношении сетевого оборудования и линий связи. Регулярно выполнять проверки состояния защиты, чтобы гарантировать требуемый уровень физической защиты.
- ограничение доступа к оборудованию и обеспечение надежности его электропитания и охлаждения.
- контроль прямого доступа ко всему сетевому оборудованию
- обеспечение защиты линий связи. Все коммуникационные линии и сетевые провода должны быть защищены от прослушивания.
- разработка плана восстановления системы в случае взлома

На уровне защиты административного интерфейса сетевых устройств применяются следующие меры:

- защита доступа к консоли
- использование шифрования паролей
- тщательная настройка параметров линий связи
- использование многоуровневой системы привилегий доступа
- использование информационных баннеров устройств

- управление доступом Telnet
- управление доступом SNMP (Simple Network Management Protocol – простой протокол сетевого управления)

Безопасность сети на ***программном уровне*** обеспечивается следующими мерами:

1. Доступ к сетевым ресурсам предоставляется только зарегистрированным пользователям
2. Ведение грамотной политики паролей для учетных записей:
   - задание минимальной длины пароля
   - задание срока действия пароля
   - блокировка учетной записи при некотором числе неудачных попыток ввода
3. Использование брандмауэров (аппаратные или программные средства ограничения и фильтрации трафика на стыке двух сетевых сегментов)
4. Использование фильтрования пакетов маршрутизаторами (фильтрование производится на основе заголовков протоколов)
5. Использование NAT (Network Addres Translation) – позволяет компьютерам сети не передавать свои IP-адреса, а пользоваться одним IP-адресом шлюзового компьютера для выхода в другой сегмент сети.
6. Использование прокси-серверов. Прокси-сервер действует на прикладном уровне модели OSI в отличие от NAT(сетевой уровень) и выполняет функцию ретрансляции данных, скрывая IP-адрес клиента.
7. Использование безопасных протоколов, шифрующих передаваемую информацию.
   - Ipsec(состоит из двух протоколов AH(Authentication Header) и ESP(Encapsulating Security Payload) выполняющих транспортную функцию и шифрование соответственно)
   - L2TP(Layer 2 Tunneling Protocol) создает туннели в виртуальных частных сетях и для шифрования использует средства Ipsec
   - SSL(Secure Sockets Layer) Состоит из двух частей-SSLHP и SSLRP первая отвечает за проверку подлинности вторая за шифрование.(система сертификатов)

- Kerberos используется службами каталога, чтобы предоставить пользователю единую точку входа в сеть т.е. пользователь получает доступ ко всем ресурсам сети (Active Directory) если доступ разрешен, система передачи билетов TGT, ST.