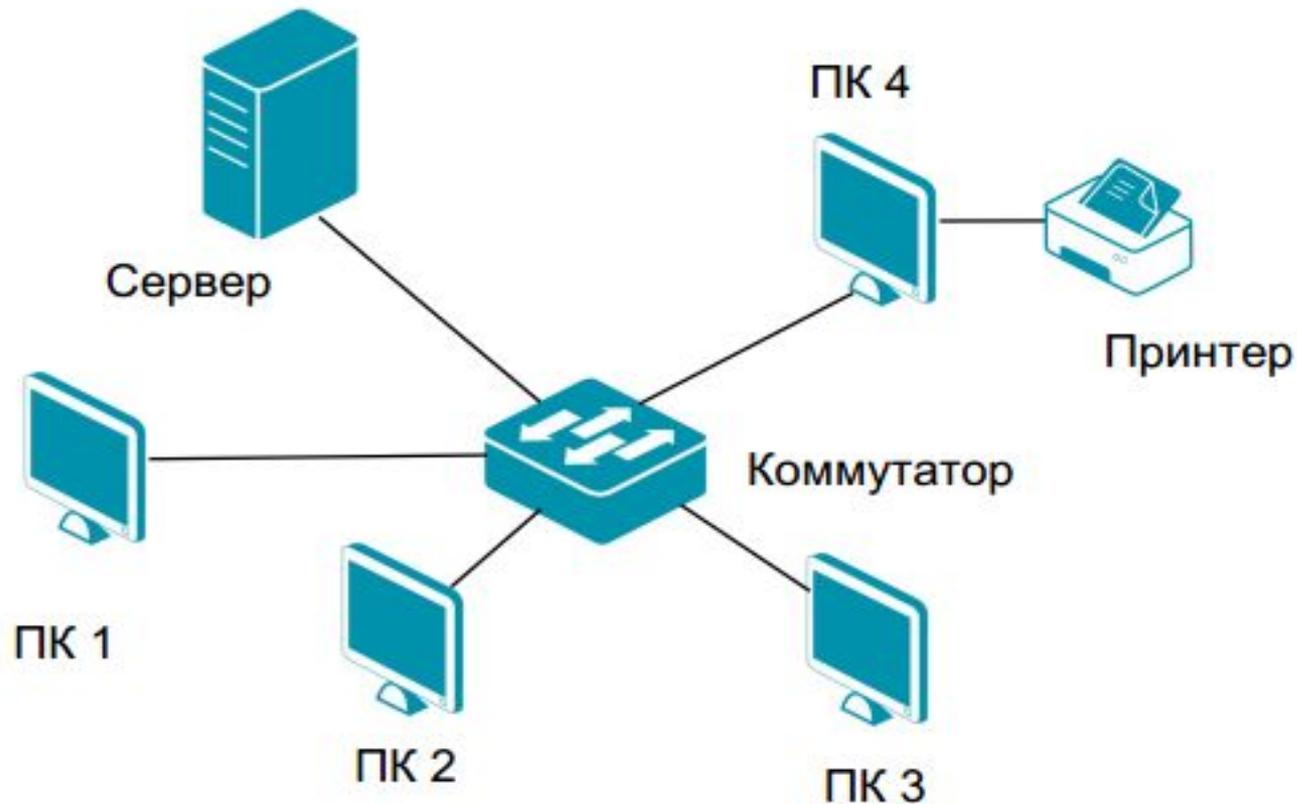


Основы сетевых технологий на базе оборудования D-Link

Компьютерная сеть

Компьютерная сеть — группа устройств, объединенных между собой каким-либо способом с целью совместного доступа к ресурсам и обмена информацией.



Компьютерная сеть

Основные определения:

- Узел, абонент, хост - устройство, непосредственно подключенное к сети.
- Сервер – специально выделенный высокопроизводительный компьютер, оснащенный соответствующим программным обеспечением, централизованно управляющий работой сети и/или предоставляющий другим компьютерам свои ресурсы (файлы данных, накопители, процессорное время и т. д.)
- Клиентский компьютер (рабочая станция) – компьютер пользователя сети, получающий доступ к ресурсам сервера (серверов).
- Среда передачи (канал связи, линия связи) - физическая среда распространения сигналов от источника к приемнику.
- Пропускная способность - максимально возможная скорость передачи данных по линии связи.
- Сегмент сети - логически или физически обособленная часть сети.
- Сегментация сети - разделения сети на сегменты с целью уменьшения в них количества узлов, увеличения пропускной способности в расчете на один узел и повышения безопасности.

Компьютерная сеть

Компьютерные сети можно классифицировать по разным признакам:

- По территориальному признаку
- По типу среды передачи
- По скорости передачи информации
- По типу функционального взаимодействия
- По типу сетевой топологии
- По функциональному назначению
- По сетевым операционным системам

Компьютерная сеть

По территориальному признаку:

- **Локальная сеть** (Local Area Network, **LAN**) – группа компьютеров, связанных друг с другом и расположенных на небольшой территории. В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации.

Пример: домашние сети, офисные сети, кампусные сети.

- **Глобальная сеть** (Wide Area Network, **WAN**) – сеть, объединяющая компьютеры разных городов, регионов, государств.

Пример: Интернет, сети между странами/городами.

- **Городская сеть** или сеть мегаполиса (Metropolitan Area Network, **MAN**) – сеть, связывающая множество локальных сетей на территории одного города. Сочетает в себе признаки как локальной, так и глобальной сети. Для нее характерна большая плотность подключения конечных абонентов, высокоскоростные линии связи и большая протяженность линий связи.

Пример: опорная сеть провайдера, сеть кабельного телевидения.

Компьютерная сеть

Пример объединения сетей



Компьютерная сеть

Виртуальная частная сеть (Virtual Private Network, VPN)– несколько локальных сетей предприятия, объединенных через Интернет.



Компьютерная сеть

По типу среды передачи:

Проводные: телефонный провод, коаксиальный кабель, витая пара, волоконно-оптический кабель

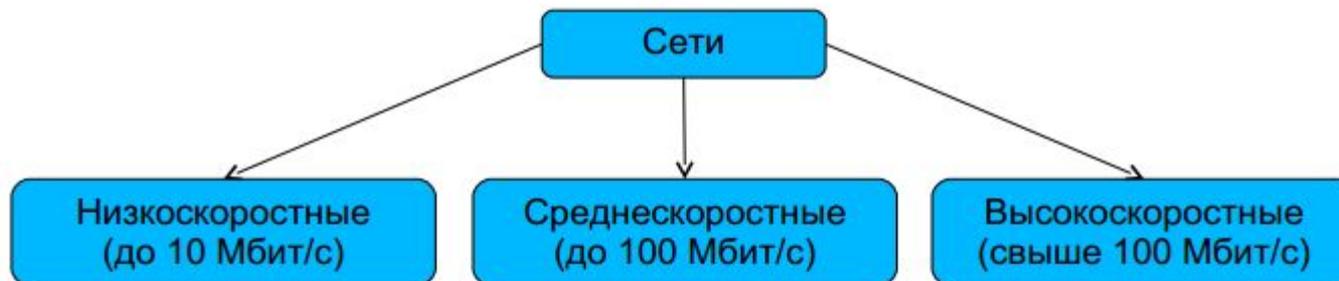


Беспроводные: передача информации по радиоволнам в определенном частотном диапазоне



Компьютерная сеть

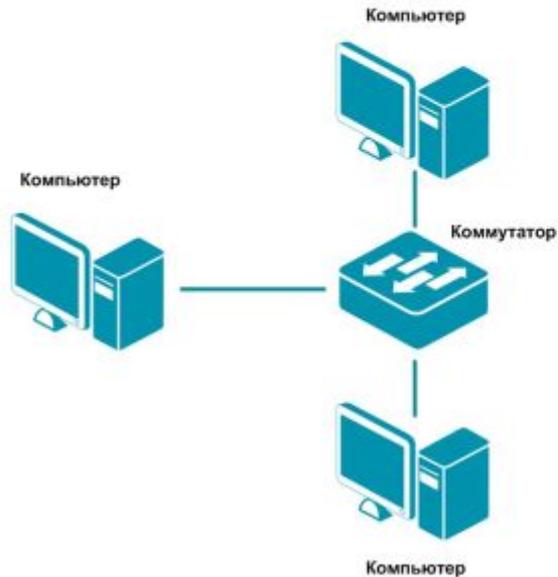
Классификация сетей по скорости передачи информации



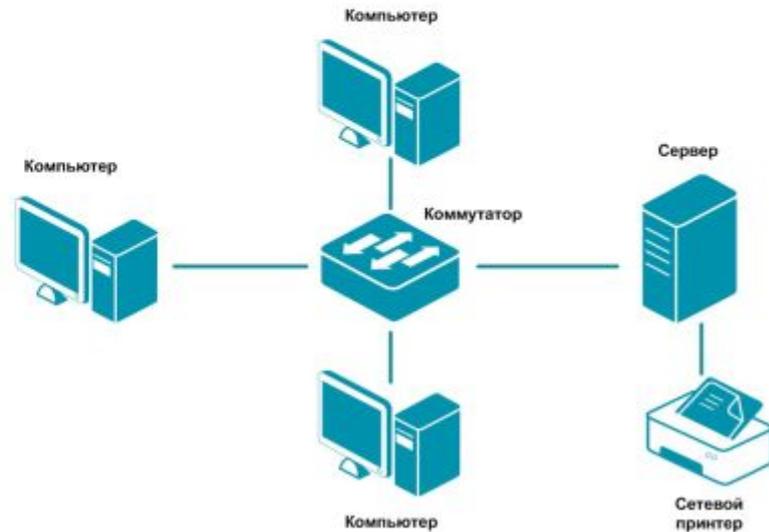
Компьютерная сеть

По типу взаимодействия:

Одноранговые сети: все компьютеры равноправны.



Сети типа «клиент-сервер»: выделяются один или несколько компьютеров, называемых серверами.



Компьютерная сеть

Топология сети - способ описания конфигурации сети, схема расположения и соединения сетевых устройств.

Различают:

- ❑ **Физическую топологию** - описывает реальное расположение и связи между узлами сети;
- ❑ **Логическую топологию** - описывает способы взаимодействия узлов и характер распространения сигналов по сети рамках физической топологии.

Компьютерная сеть

Физические топологии

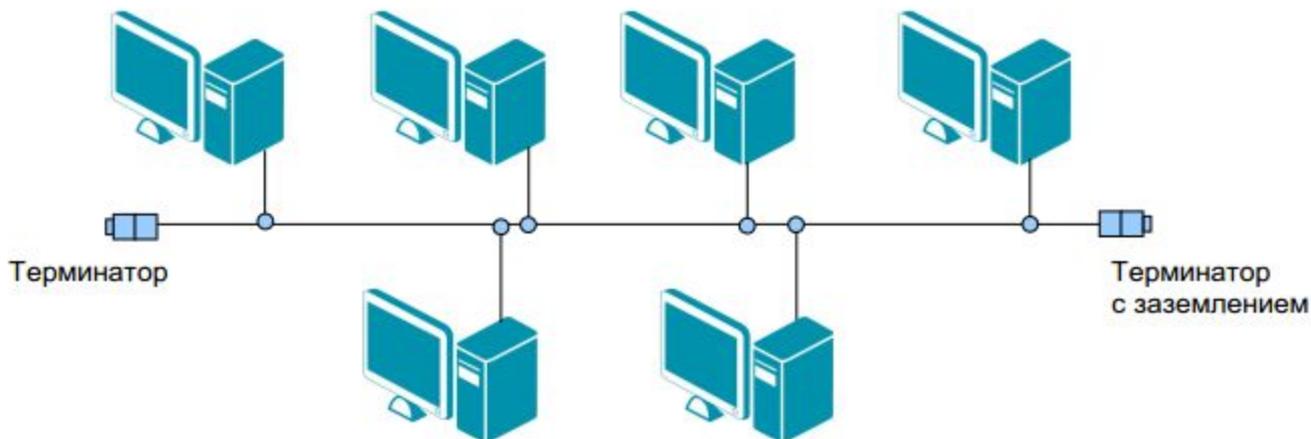
Существует три базовые топологии, на основе которых строится большинство сетей:

- «Шина» (Bus);
- «Кольцо» (Ring);
- «Звезда» (Star).

Компьютерная сеть

Топология «Шина»

Все узлы соединяются между собой одним кабелем.



+: простота реализации и дешевизна.

- : сложность расширения;

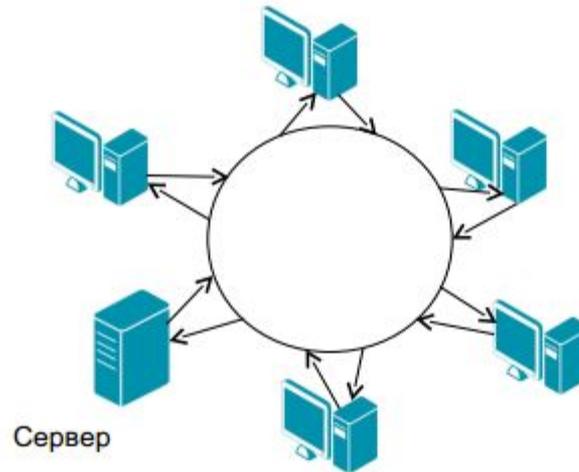
в каждый момент времени может передавать только один компьютер;

невысокая надежность.

Компьютерная сеть

Топология «Кольцо»

- Каждый из компьютеров соединяется с двумя другими так, чтобы от одного он получал информацию, а второму передавал ее.
- Последний компьютер подключается к первому.

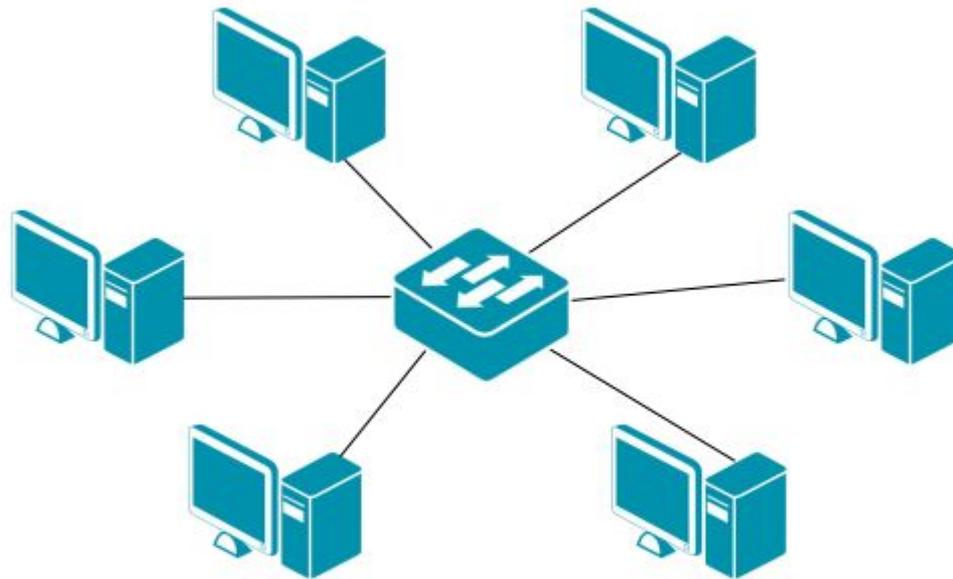


- +: каждый компьютер выступает в роли повторителя сигнала; отсутствие столкновений.
- : сигнал в кольце должен пройти последовательно через все компьютеры; невысокая надежность.

Компьютерная сеть

Топология «Звезда»

Каждый из компьютеров подключается к центральному соединительному устройству.



Преимущества:

- Легкость обслуживания и устранения неисправностей;
- Защищенность.

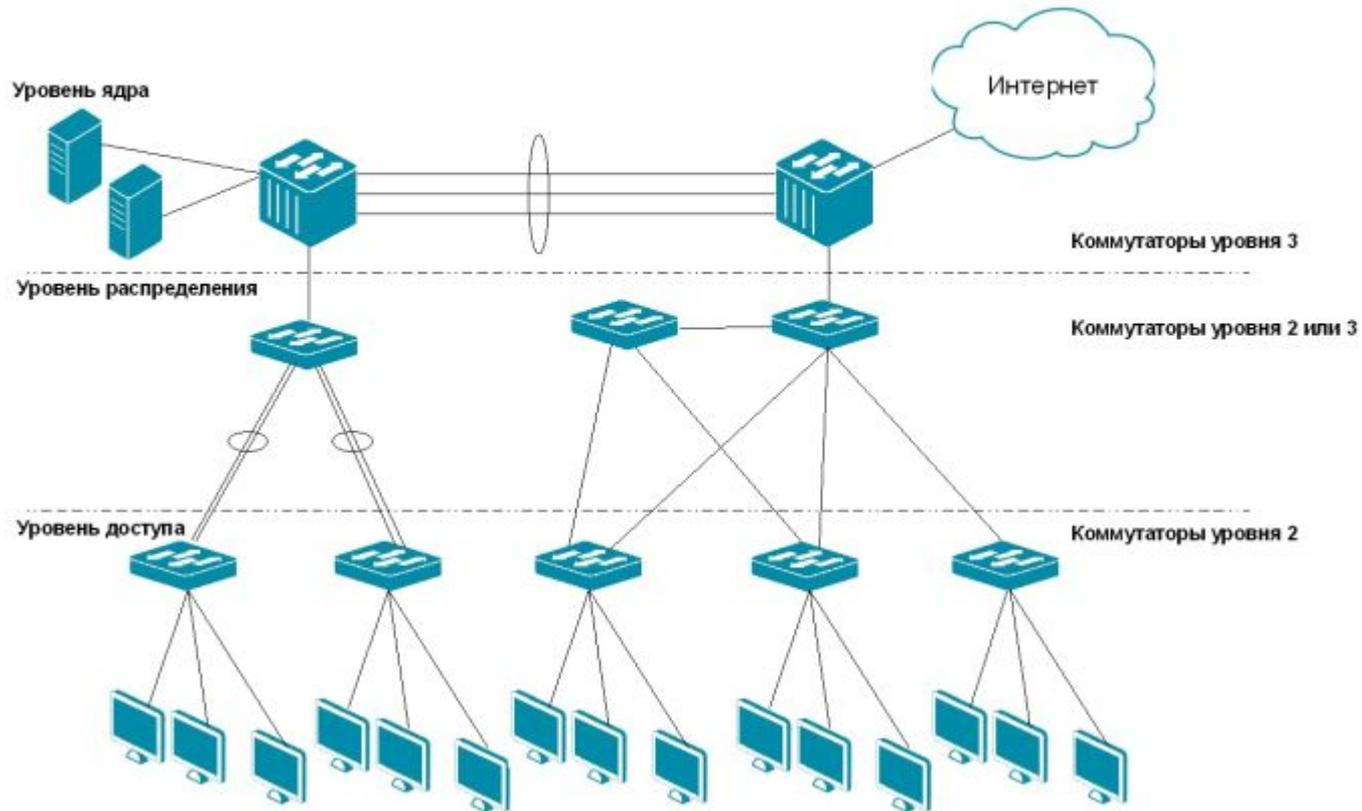
Недостатки:

- Единая точка отказа

Компьютерная сеть

Топология «Дерево» (Tree)

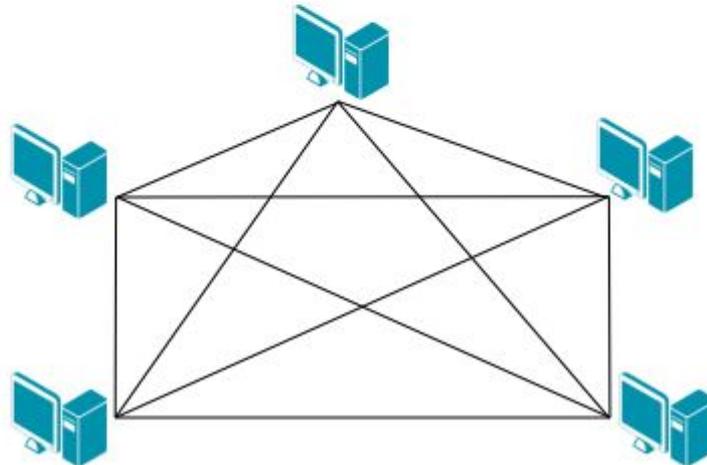
- Объединение нескольких «звезд».
- Наиболее распространенная топология при построении локальных сетей.



Компьютерная сеть

Полносвязная топология

- Каждый компьютер и другие устройства соединены друг с другом напрямую
- Высокая надежность – имеется несколько маршрутов передачи информации.
- Используется там, где требуется обеспечение максимальной отказоустойчивости сети: при объединении нескольких сегментов сети крупного предприятия или при подключении к Интернет.
- Существенно увеличивается расход кабеля, усложняется сетевое оборудование и его настройка.



Компьютерная сеть

Выбор топологии сети

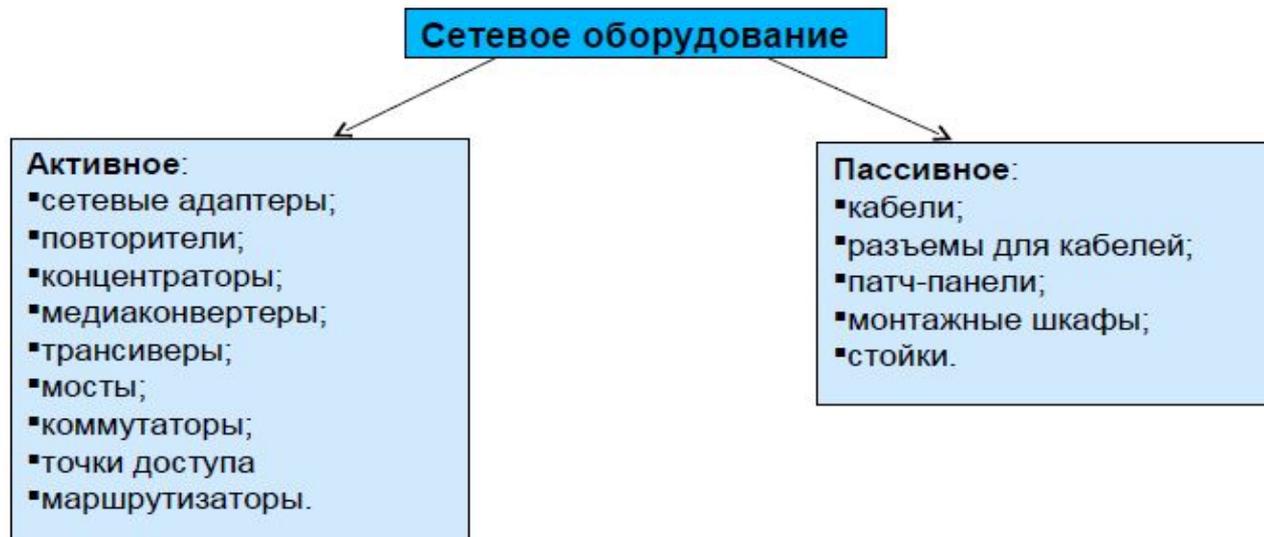
- Устойчивость к неисправностям узлов, подключенных к сети и обрывам кабеля.
- Обеспечение возможности для дальнейшего расширения сети и перехода к новым высокоскоростным технологиям.
- Низкая стоимость создания и сопровождения сети.
- Удобное управление потоками сетевых данных.

Также следует учитывать:

- ✓ Имеющуюся кабельную систему и оборудование.
- ✓ Физическое размещение устройств.
- ✓ Размеры планируемой сети.
- ✓ Объем и тип информации для совместного использования.

Компьютерная сеть

- При построении любой компьютерной сети используется **коммуникационное** или **сетевое** оборудование.
- Основной его задачей является объединение компьютеров в сеть, сегментов (подсетей) одной сети, подключение компьютерных сетей разных топологий и технологий друг к другу, увеличение расстояния передачи сигнала.
- **Активное оборудование** – это электронные и электронно-оптические устройства, обрабатывающие, формирующие, преобразующие и коммутирующие электрические и/или оптические сигналы, передавая и получая эти сигналы с использованием дополнительных источников энергии.
- **Пассивное оборудование** представляет собой сетевое оборудование, не потребляющее электричества и не вносящее изменений в сигнал на информационном уровне. Все это оборудование является частью структурированных кабельных систем.



Компьютерная сеть

Сетевой адаптер

Для подключения компьютера к сети используется **сетевой адаптер (Network Interface Card, NIC)**. Он позволяет компьютеру подключаться к сети и взаимодействовать с другими устройствами.

Сетевой адаптер выполняет функции физического и канального уровней модели OSI. Он хранит уникальный физический адрес (MAC-адрес), который позволяет уникально идентифицировать каждый узел в данном сегменте сети.



Сетевой адаптер



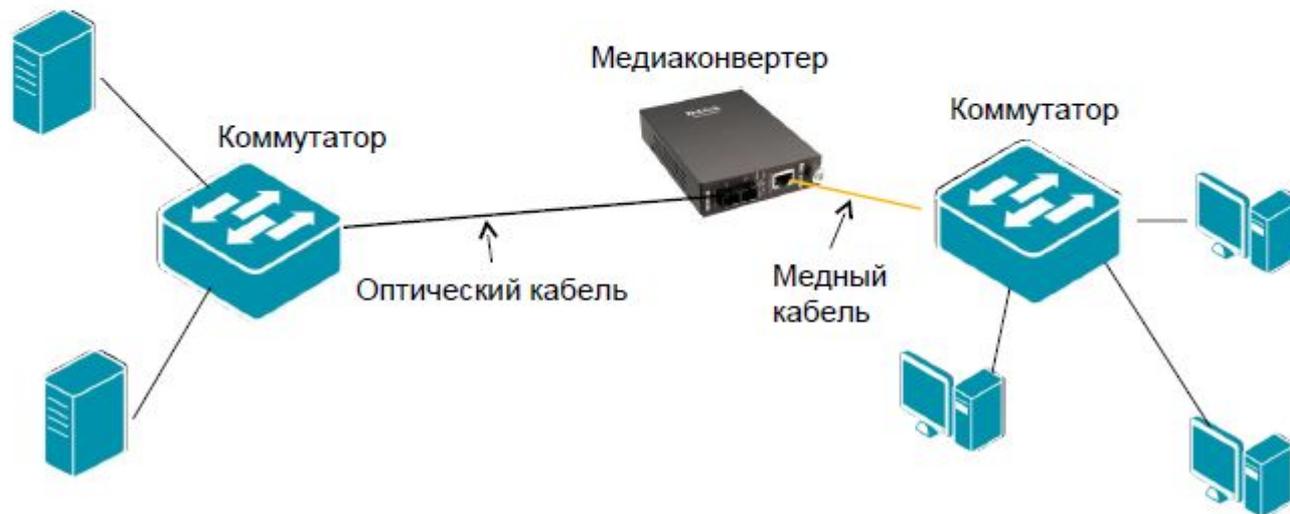
Точка доступа



Компьютерная сеть

Медиаконвертер

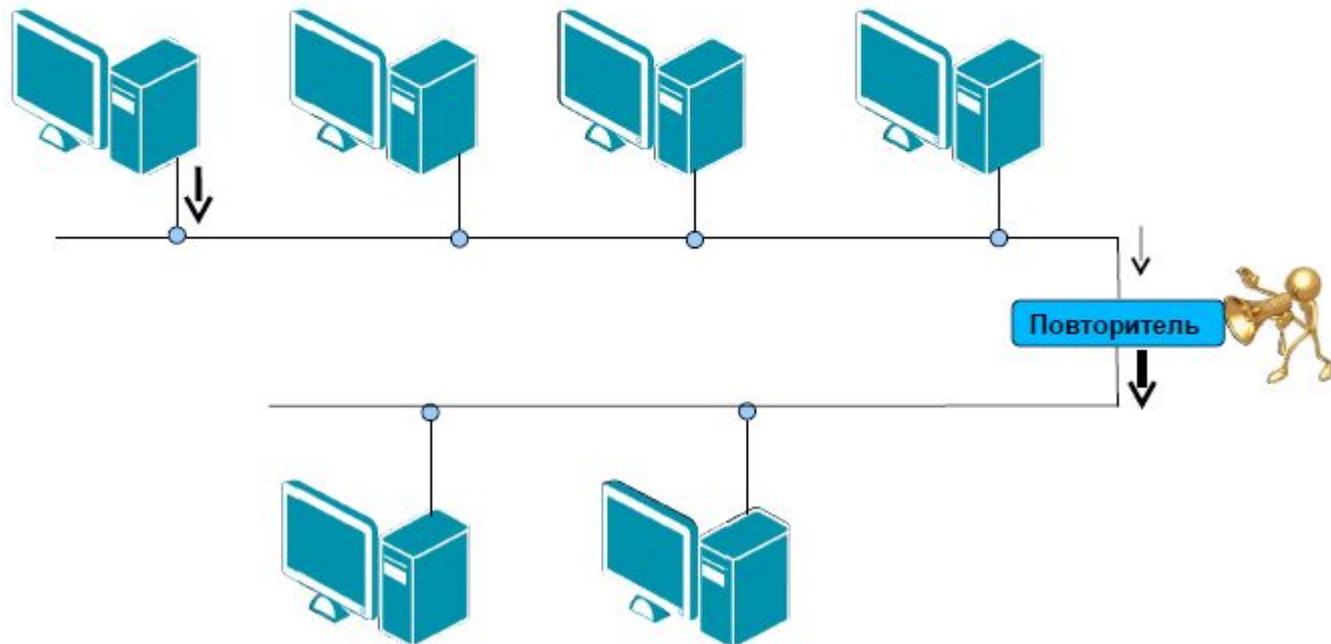
Медиаконвертер (Mediaconverter) — это устройство физического уровня модели OSI, преобразующее среду распространения сигнала из одного типа в другой.



Компьютерная сеть

Повторитель

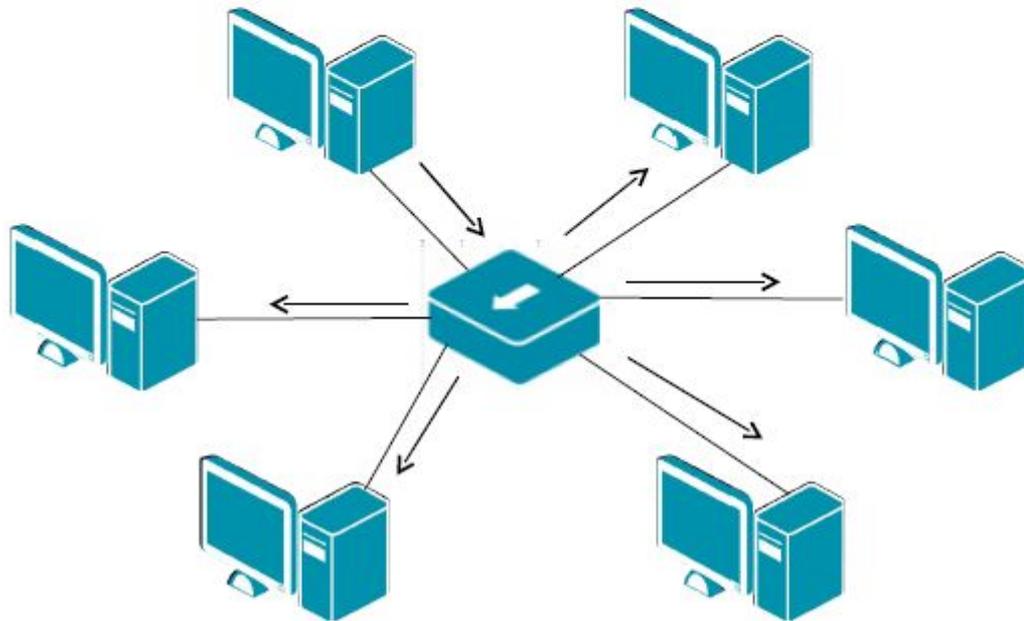
- Простейшим из сетевых устройств является **повторитель (repeater)** – это устройство физического уровня модели OSI, используемое для соединения сегментов среды передачи данных с целью увеличения общей длины сети.
- Повторитель принимает сигналы из одного сегмента сети, усиливает их, восстанавливает синхронизацию и передает в другой сегмент сети.



Компьютерная сеть

Концентратор

- Повторитель, который имеет несколько портов и соединяет несколько физических сегментов сети, называется **концентратором (concentrator)** или **хабом (hub)**.
- Концентратор устройство физического уровня. Он принимает, усиливает и ретранслирует сигнал пришедший с одного из своих портов, на другие свои порты.
- Концентратор всегда изменяет физическую топологию сети, но при этом оставляет без изменения ее логическую топологию.

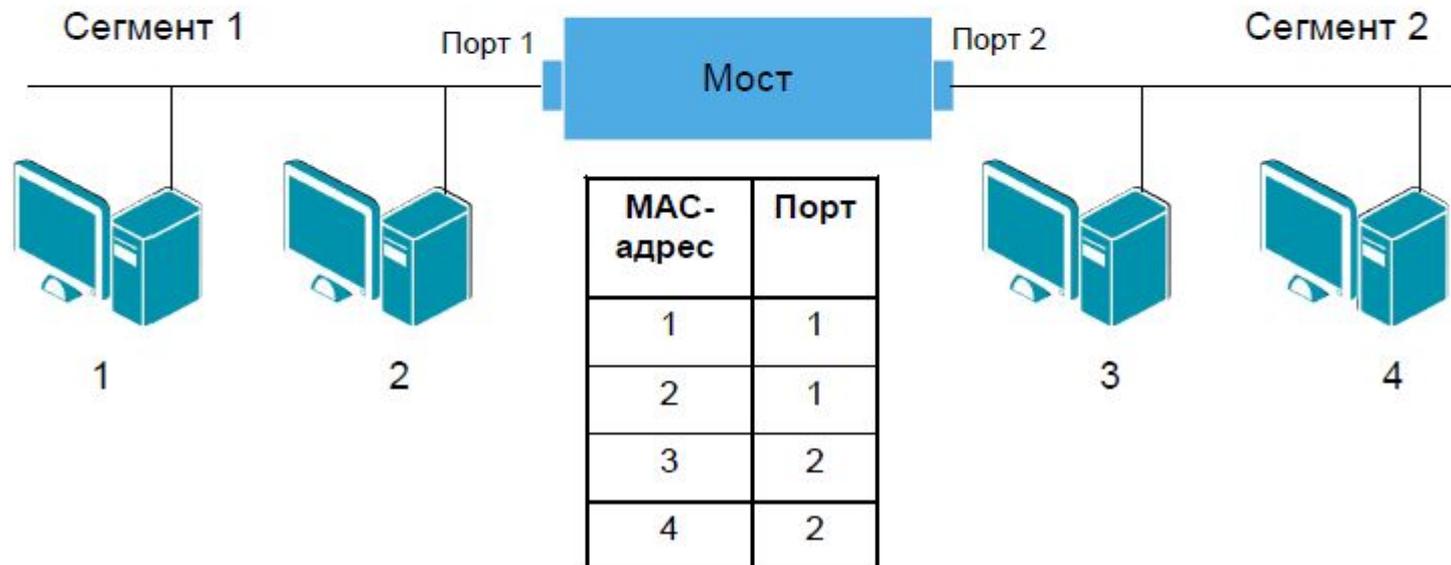


Компьютерная сеть

Мост

Мост (bridge) – это устройство канального уровня модели OSI, которое соединяет между собой два сегмента локальной сети.

- Мост передает информацию из одного сегмента в другой только в том случае, если такая передача действительно необходима, то есть если MAC-адрес компьютера назначения принадлежит другому сегменту.
- Мост изолирует трафик одного сегмента от трафика другого, повышая общую производительность передачи данных в сети.

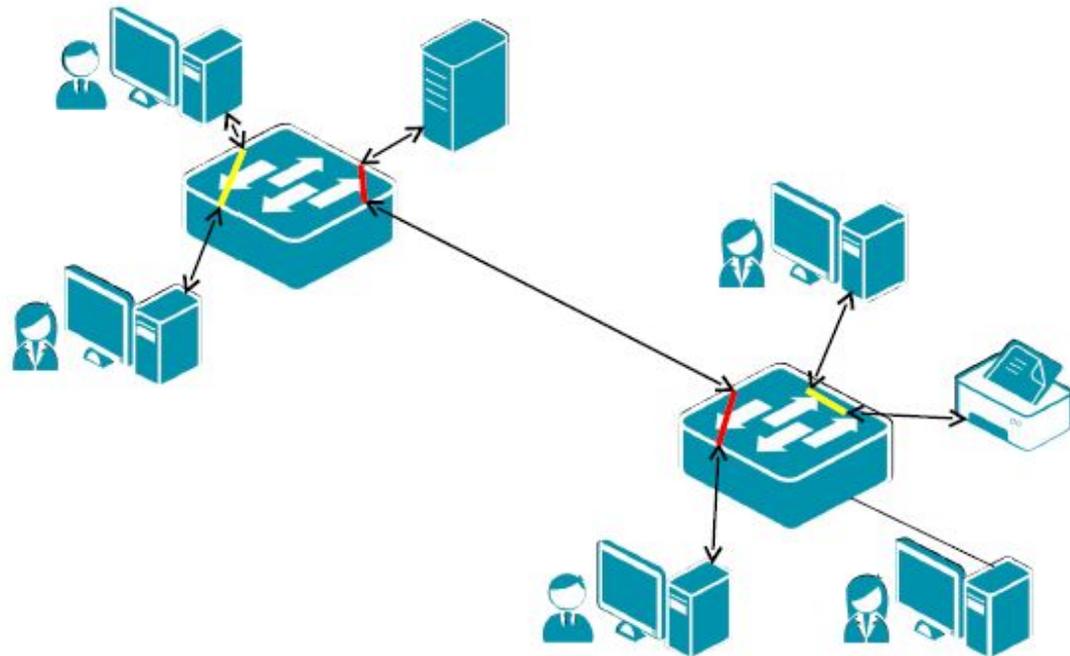
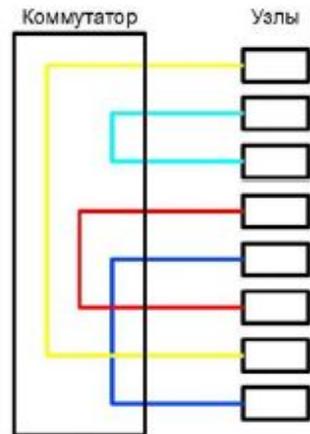


Компьютерная сеть

Коммутатор

Коммутатор (switch) – это устройство канального уровня модели OSI, которое предназначено для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети.

- Коммутатор – многопортовый мост.
- Строит таблицу коммутации, устанавливающую связь между портами и MAC-адресами, подключенных к ним устройств.
- Одновременно устанавливает несколько соединений между разными парами портов (микросегментация).

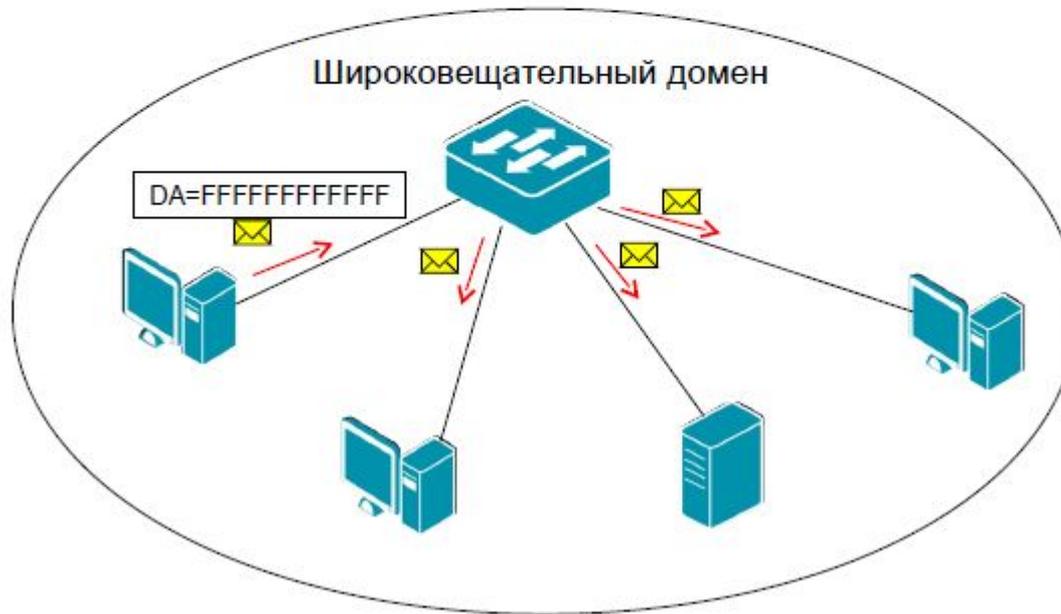


Компьютерная сеть

Коммутатор

Коммутатор передает кадры через все порты:

- Если в таблице коммутации отсутствует запись соответствия MAC-адреса устройства и порта коммутатора;
- если MAC-адрес назначения широковещательный, т.е. кадр предназначен всем узлам сети. В этом случае говорят, что коммутатор образует широковещательный домен (*broadcast domain*)

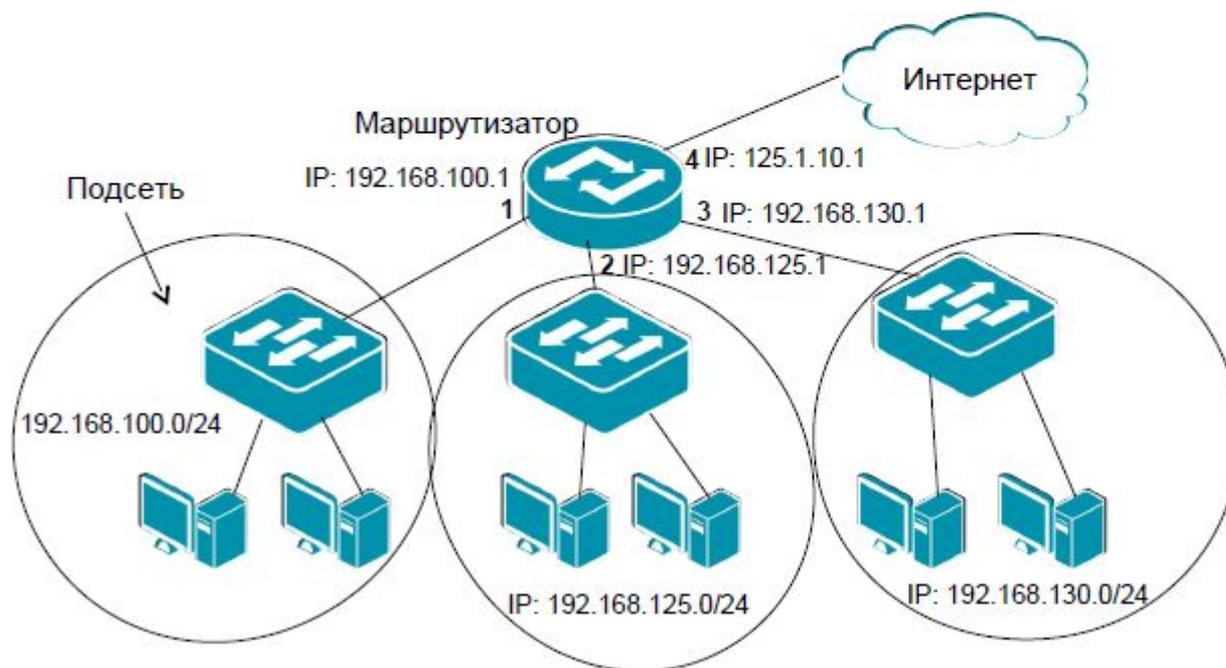


Компьютерная сеть

Маршрутизатор

Маршрутизатор (router) – это устройство сетевого уровня модели OSI, пересылающее пакеты данных между различными сегментами сети (подсетями) и принимающее решения на основании информации о топологии сети и определённых правил, заданных администратором.

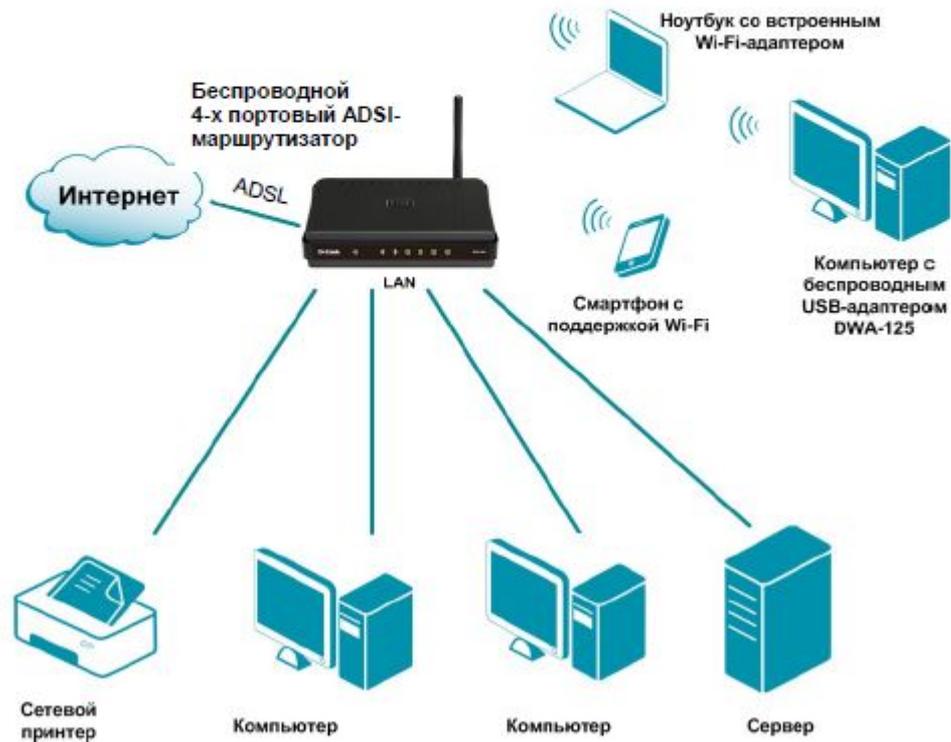
Маршрутизаторы часто применяются для связи локальных сетей разных типов и для подключения локальных сетей к глобальным.



Компьютерная сеть

Шлюз

- Под шлюзом понимается любое устройство, соединяющие разные сетевые архитектуры.
- Шлюз должен не только иметь разные физические порты, но и понимать «разные» протоколы.
- Примером шлюза может служить беспроводной ADSL-маршрутизатор.



Эталонная модель OSI

Эталонная модель взаимодействия открытых систем (Open System Interconnection, OSI) описывает способ передачи информации по сети от приложения на одном компьютере к приложению на другом компьютере.

- ❑ Модель OSI является концептуальной моделью, она разбивает процесс передачи данных по сети на семь уровней.
- ❑ Каждому уровню соответствуют строго определенные операции, оборудование и протоколы.
- ❑ Эта модель считается основной архитектурной моделью передачи данных между компьютерами.

Эталонная модель OSI

Уровни модели OSI

- Важной концепцией модели OSI является деление на сетевые уровни.
- Каждый уровень выполняет специальную задачу или наборы задач и взаимодействует с уровнем лежащим выше и ниже его.
- Каждый уровень имеет имя и номер от 1 до 7, номер уровня определяет его позицию в модели, а также показывает насколько «близко» этот уровень расположен к реальному оборудованию, используемому для построения сети.
- Нижние уровни (с 1 по 3) модели OSI управляют физической доставкой сообщений по сети. Эти уровни реализуются в виде аппаратных средств и программного обеспечения.
- Верхние уровни (с 4 по 7) модели OSI обеспечивают точную доставку данных между компьютерами в сети. Верхние уровни модели OSI работают с приложениями и обычно реализуются только на программном уровне.

Уровни хост-машины (host layers)	Уровень приложений	7
	Уровень представлений	6
	Сеансовый уровень	5
	Транспортный уровень	4
Уровни среды передачи данных (media layers)	Сетевой уровень	3
	Канальный уровень	2
	Физический уровень	1

Эталонная модель OSI

Основные концепции модели OSI

- Каждый уровень (кроме уровня 7) предоставляет сервисы уровню выше его.
- Каждый уровень (кроме уровня 1) использует сервисы, предоставляемые уровнем ниже его.
- Другими словами, каждый уровень «N» предоставляет сервисы уровню «N+1» и использует сервисы уровня «N-1».



Эталонная модель OSI

Взаимодействие между уровнями

- ❑ Обмен данными становится возможным благодаря коммуникационным протоколам.
Протокол - формальный набор правил и соглашений, регламентирующий обмен информацией между компьютерами по сети. Он реализует функции одного или нескольких уровней OSI.
- ❑ Протоколы, принадлежащие определенному уровню эталонной модели OSI взаимодействуют с аналогичными протоколами одноименных уровней на других устройствах только посредством передачи сообщений через нижележащие уровни своего стека протоколов.

Стек протоколов - совокупность протоколов разных уровней.

Правила и процедуры, которые отвечают за взаимодействие между соседними уровнями внутри одного устройства, называются **интерфейсами**.

Эталонная модель OSI

7	Уровень приложений	→ Обеспечивает интерфейс взаимодействия программ, работающих на компьютерах в сети. С помощью этих программ пользователь получает доступ к сетевым услугам.
6	Уровень представлений	→ Определяет форматы передаваемой информации. Задачей данного уровня является перекодировка, сжатие и распаковка данных, их шифрование и дешифрование.
5	Сеансовый уровень	→ Позволяет сетевым приложениям устанавливать, поддерживать и завершать соединение, называемое сетевым сеансом. Обеспечивает синхронизацию. Отвечает за восстановление аварийно прерванных сеансов связи.
4	Транспортный уровень	→ Сегментирует и повторно собирает данные в один поток. Обеспечивает надежную доставку информации между узлами сети.
3	Сетевой уровень	→ Обеспечивает соединение и выбор маршрута между двумя конечными системами, которые могут находиться в сетях, расположенных в разных концах земного шар, обеспечивает единую систему адресации.
2	Канальный уровень	→ Обеспечивает надежную передачу данных через физический канал связи. Решает вопросы физической адресации, доступа к среде передачи, сообщений об ошибках, порядка доставки кадров и управления потоком данных.
1	Физический уровень	→ Выполняет передачу неструктурированного потока бит по физической среде. Отвечает за топологию, поддержание связи и описывает электрические, оптические, механические и функциональный интерфейсы со средой передачи: напряжения, частоты, длины волн, разъемы, число и функциональность контактов, схемы кодирования сигналов.

Эталонная модель OSI

Взаимодействие между уровнями



Эталонная модель OSI

	Уровень	Тип обрабатываемых данных	Функции	Протоколы
7	Уровень приложений	Пользовательские данные	Предоставление сервисов для сетевых приложений	DNS; NFS; BOOTP; DHCP; SNMP; RMON; FTP; TFTP; SMTP; POP3; IMAP; NNTP; HTTP; Telnet
6	Уровень представлений	Закодированные пользовательские данные	Общий формат представления данных, кодирование и шифрование	SSL; Shells and Redirectors; MIME
5	Сеансовый уровень	Сессии	Установление сессий между приложениями	NetBIOS, Sockets, Named Pipes, RPC
4	Транспортный уровень	Дэйтаграммы/ сегменты	Адресация процессов, сегментация повторная сборка данных, управление потоком, надежная доставка	TCP и UDP; SPX; NetBEUI/NBF
3	Сетевой уровень	Дэйтаграммы/ пакеты	Передача сообщений между удаленными устройствами, выбор наилучшего маршрута, логическая адресация	IP; IPv6; IP NAT; IPsec; Mobile IP; ICMP; IPX; DLC; PLP; протоколы маршрутизации, например RIP и BGP
2	Канальный уровень	Кадры	Доступ к среде передачи и физическая адресация	IEEE 802.2 LLC, семейство Ethernet Token Ring; FDDI; IEEE 802.11 (WLAN, Wi-Fi); HomePNA; HomeRF; ATM; SLIP и PPP
1	Физический уровень	Биты	Передача электрических и оптических сигналов между устройствами	Физический уровень большинства технологий канального уровня

Коммутация каналов

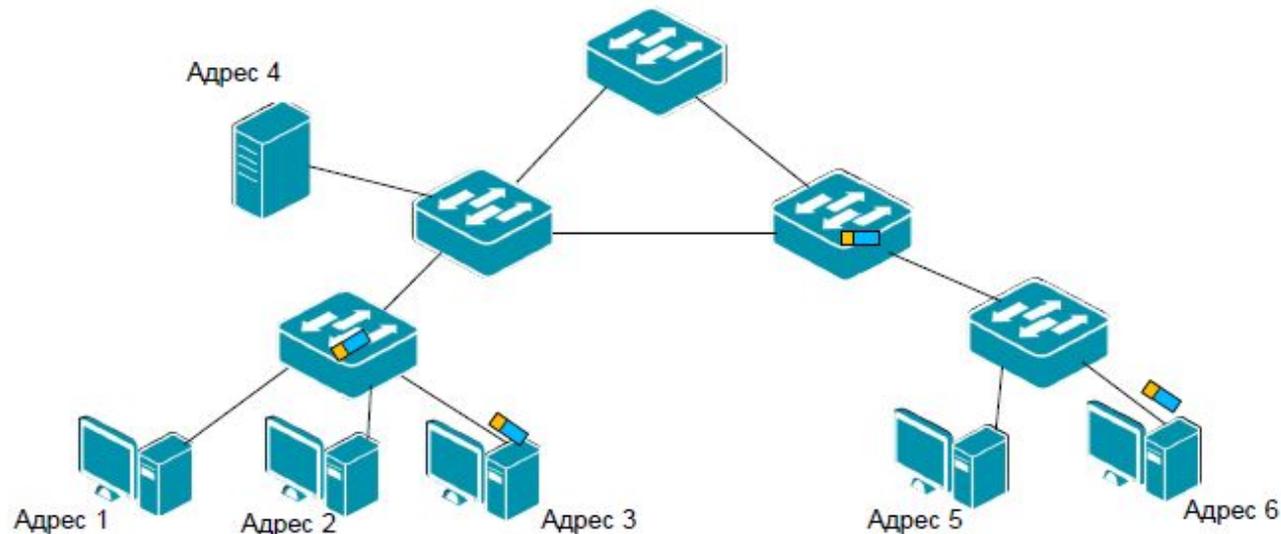
- **Коммутация** — процесс соединения абонентов коммуникационной сети через транзитные узлы.
- Одной из центральных проблем организации передачи данных по физическим каналам является проблема параллельного использования одного и того же канала несколькими парами абонентов.
- Методы, лежащие в основе ее решения получили название **методов коммутации**, которые обеспечивают разделение имеющихся физических каналов между несколькими сеансами связи и между абонентами сети.

В настоящее время существует 4 метода коммутации. Рассмотрим следующие из них:

- коммутация каналов
- коммутация пакетов

Коммутация каналов

- Метод **коммутации пакетов** основан на разбиении передаваемых по сети данных на небольшие части, называемые **пакетами**.
- Каждый пакет обычно состоит из двух частей – **заголовка**, содержащего служебные данные, необходимые для управления доставкой пакета (адресную информацию, порядковый номер пакета), и **данных**, подлежащих передаче.
- Пакеты передаются по сети как независимые информационные блоки.
- Порядок обмена пакетами, а также конкретный состав заголовка пакетов определяется сетевым протоколом.
- Такой метод является очень удобным для параллельного использования физического канала несколькими парами узлов: канал является занятым только во время прохождения пакета. Временные промежутки между передачей пакетов одними узлами могут быть использованы другими для отправки собственных пакетов.



Структура кадра данных

- Состав заголовка кадра зависит от многих факторов, определяемых набором функций, которые выполняет протокол.
- Можно выделить ряд информационных полей, которые обычно присутствуют в заголовке кадра:

Поле, определяющее начало кадра	Адрес отправителя и получателя	Информация о протоколе сетевого уровня	Данные (Data)	Контрольная сумма	Поле, определяющее конец кадра
---------------------------------	--------------------------------	--	---------------	-------------------	--------------------------------

1. Специальные поля, предназначенные для определения границ кадров. Поскольку в физической среде могут постоянно проходить какие-либо сигналы, то приемник должен уметь разбираться в том, когда начинается передача кадра и когда она заканчивается.

2. Поле, предназначенное для определения протокола сетевого уровня, которому необходимо передать данные. Так как на одном компьютере могут функционировать программные модули различных протоколов сетевого уровня, то протоколы канального уровня должны уметь распределять данные по этим протоколам.

3. Контрольная сумма (или специальный код) содержимого кадра, которая позволяет принимающей стороне определить наличие ошибок в принятых данных.

Понятие MTU

- Для большинства протоколов канального уровня существует ограничение на максимально допустимый объем данных, передаваемых в одном кадре, вызванное различными техническими условиями.
- Характеристика, используемая для определения максимального размера блока данных (в байтах), который может быть передан на канальном уровне называется **MTU** (Maximum Transfer Unit, **максимальная единица передачи данных**).
- Значение MTU может быть определено стандартом (например, для Ethernet), либо выбираться в момент установки соединения (обычно в случае подключений «точка-точка»).

Протоколы локальных сетей

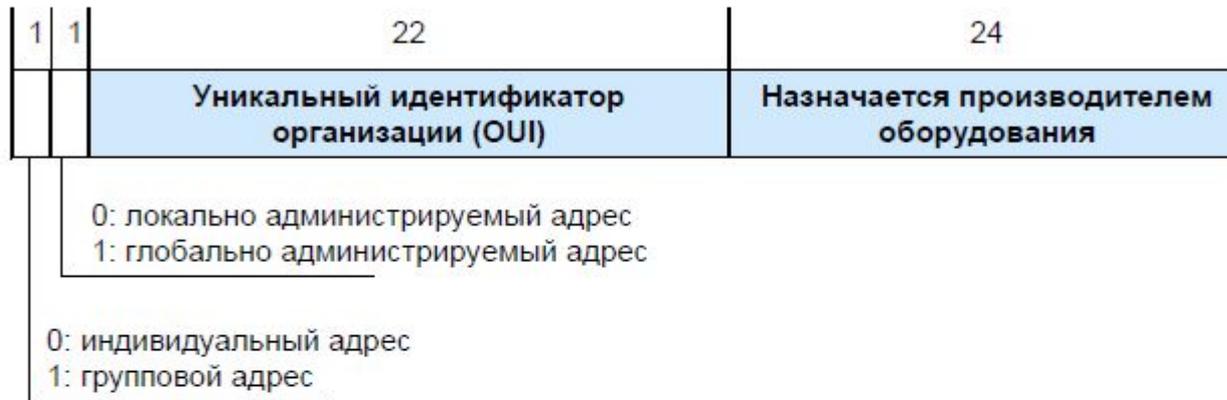
Адресация

- Для обеспечения адресации узлов в сети в заголовке кадров должны присутствовать адрес отправителя и адрес получателя.
- Большинство протоколов канального уровня для идентификации устройств используют MAC-адрес.
- **MAC-адрес** (*Media Access Control*) — это уникальный идентификатор, присваиваемый каждому сетевому устройству во время изготовления.
- MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу.

Протоколы локальных сетей

MAC-адрес

Стандарты IEEE определяют MAC-адрес длиной 48 бит (6 октетов):



- 1-й бит указывает является ли адрес индивидуальным или групповым:
 - **Индивидуальным** – адрес, ассоциированный с определенным сетевым устройством.
 - **Групповым** – адрес, ассоциированный с несколькими или всеми узлами данной сети.

Существует два вида групповых адресов:

- **Многоадресный** (multicast) – адрес ассоциированный с группой узлов сети.
- **Широковещательный** (broadcast) – адрес, ассоциированный со всеми узлами сети. Его значение – 0xFF-FF-FF-FF-FF-FF.
- 2-й бит указывает является ли MAC-адрес глобально или локально администрируемым:
 - **глобально администрируемый MAC-адрес** устройства **глобально уникален** и обычно «зашит» в аппаратуру.
 - **локально администрируемый MAC-адрес** выбирается произвольно и может не содержать информации об OUI.

Протоколы локальных сетей

Стек TCP/IP

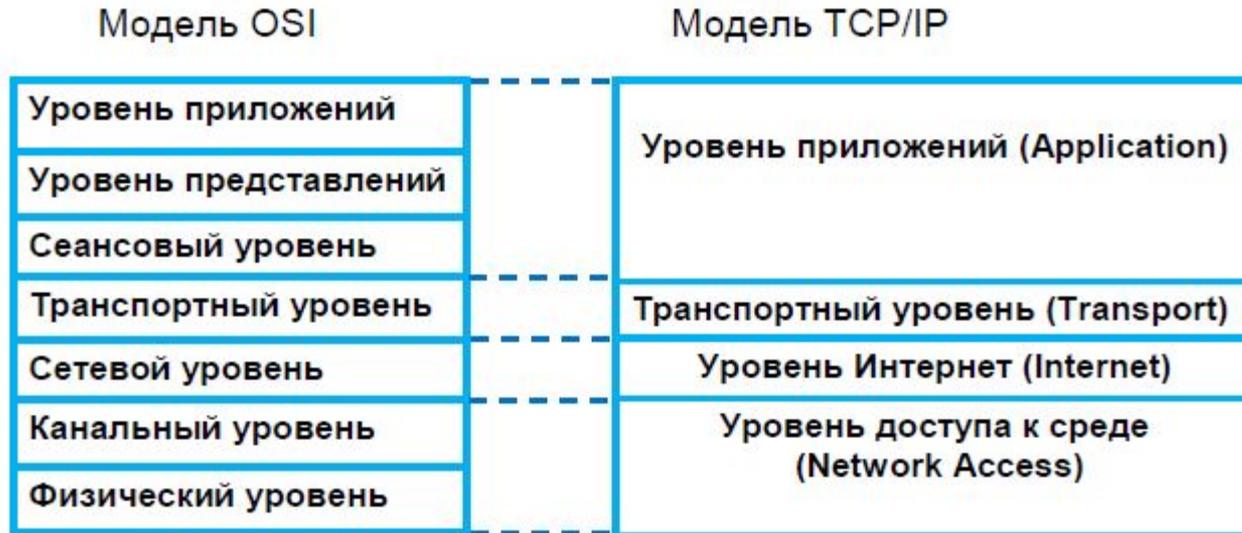
- Историческим и техническим стандартом для Интернет является модель и стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol).
- История развития стека TCP/IP началась с проекта ARPAnet – сети Агентства перспективных исследовательских проектов Министерства обороны США *Defense Advanced Research Projects Agency* (*DARPA* или *ARPA*).
- Изначально сеть ARPAnet задумывалась как высоконадежная сеть, объединяющая военные, научные и государственные учреждения.
- В 1973 г. началась разработка межсетевых протоколов для ARPAnet. Получившийся в результате стек протоколов TCP/IP оказался настолько удачным, что после прекращения финансирования проекта Министерством обороны он продолжал развиваться и стал основой Интернет.

Основные преимущества стека TCP/IP над другими стеками:

- Удобная система сетевой адресации.
- Возможность маршрутизации пакетов.
- Независимость от физической среды.
- Открытый стандарт, его документы публикуются в Интернет в виде документов RFC (Request for comments, «запрос комментариев»)

Протоколы локальных сетей

Модель TCP/IP



Протоколы локальных сетей

Технология Ethernet

□ Ethernet – наиболее широко используемая технология локальных сетей, которая определяет проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на MAC-подуровне канального уровня.

□ Первая экспериментальная сеть Ethernet, основанная на методе доступа CSMA/CD, была разработана компанией Xerox в 1970-х г.

□ В 1980 г. компании Digital Equipment Corporation, Intel и Xerox разработали и опубликовали спецификацию Ethernet 1.0 для передачи данных со скоростью 10 Мбит/с.

□ Первый стандарт IEEE 802.3 был основан на спецификации Ethernet 1.0. Проект стандарта был одобрен группой 802.3 в 1983 году и в 1985 опубликован как официальный стандарт.

□ В 1982 г. Digital Equipment Corporation, Intel Corporation и Xerox Corporation выпустили новую спецификацию Ethernet v.2. Эту версию стандарта называют Ethernet DIX или Ethernet II.

- В исходной версии Ethernet предусматривалось использование коаксиального кабеля (стандарты 10Base5 и 10Base2).
- В начале 1990-х годов появились спецификации на основе витой пары (10Base-T) и оптоволокна (10Base-FL).
- В 1995 г. был опубликован стандарт Fast Ethernet (IEEE 802.3u).
- В 1998 г. был опубликован стандарт Gigabit Ethernet (IEEE 802.3z и 802.3ab).
- В 2002 г. был опубликован стандарт 10 Gigabit Ethernet (IEEE 802.3ae).
- В 2010 г. был опубликован стандарт 40 и 100 Gigabit Ethernet (IEEE 802.3ba).

Протоколы локальных сетей

Форматы кадров Ethernet

Стандарт IEEE 802.3-2008 определяет следующую структура кадра, обязательную для всех MAC-реализаций:

7 байт	1 байт	6 байт	6 байт	4 байта (опционально)	2 байта	42 – 1500 байта		4 байта		
Preamble	SFP	Destination Address	Source Address	Tag 802.1Q	Length/Type	Data	PAD	FCS	Extension	
		64-1522 байта								

➤ На практике существует 4 формата кадров Ethernet:

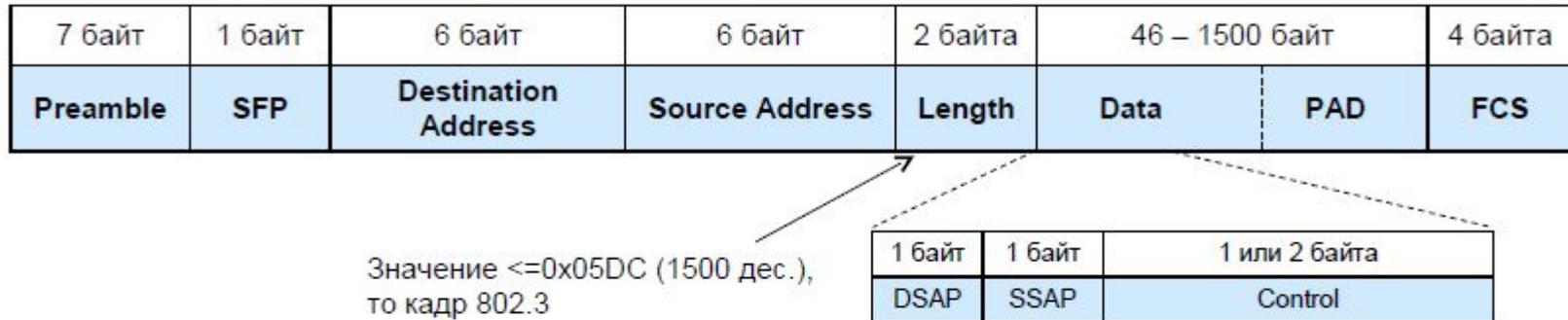
- Кадр Ethernet II (Ethernet v.2 или DIX Ethernet)
- Кадр IEEE 802.3 /LLC
- Кадр Ethernet SNAP
- Кадр Raw 802.3 (Novell 802.3)

➤ Разные типы кадра имеют различный формат и значение MTU (Maximum Transmission Unit), но могут сосуществовать в одной физической среде.

➤ Наибольшее распространение получил кадр Ethernet II .

Протоколы локальных сетей

Кадр IEEE 802.3/LLC



- **Preamble (преамбула)** – состоит из семи синхронизирующих байт 10101010.
- **Start-of-Frame-Delimiter (SFP, начальный ограничитель кадра)** – содержит значение 10101011. Эта комбинация указывает на то, что следующий байт начало заголовка кадра.
- **Destination Address (DA, адрес назначения)** – MAC-адрес получателя кадра.
- **Source Address (SA, адрес источника)** – MAC-адрес отправителя кадра.
- **Length (длина)** – если значение меньше или равно $0x05DC$ (1500 дес.), то поле указывает на длину поля данных в кадре.
- **Data (данные)** – поле данных переменной длины. Мин. длина поля 46 байт, макс. длина поля 1500 байт.
- **Pad (Padding, заполнение)** – состоит из такого количества байт заполнителей, которое обеспечивает минимальную длину поля данных в 46 байт. Это обеспечивает корректное распознавание коллизий. Если длина поля данных достаточна, поле заполнения в кадре отсутствует.
- **Frame Check Sequence (FCS, поле контрольной суммы)** – содержит контрольную сумму кадра. Служит для проверки не искажен ли кадр. Значение поля вычисляется на основе содержимого полей DA, SA, длина и поля данных с помощью 32-разрядного циклического избыточного кода (Cyclic Redundancy Code, CRC).

Протоколы локальных сетей

Кадр Ethernet II

7 байт	1 байт	6 байт	6 байт	2 байта	46 – 1500 байт		4 байта
Preamble	SFP	Destination Address	Source Address	Type	Data	PAD	FCS

Значение $\geq 0x0600$ (1536 дес.),
то кадр Ethernet II

IP v4 0x0800
IP v6 0x86DD
ARP 0x0806
802.1Q 0x8100

- Поле **Type (тип)** используется для указания типа протокола, вложившего пакет в поле данных кадра.

Протоколы локальных сетей

Жумбо-фреймы

- В компьютерных сетях **Жумбо-фреймы** (Jumbo-frame) – это кадры Ethernet размер поля данных которых может достигать 9000 байт.
- Жумбо-фреймы не являются частью стандарта IEEE 802.3.
- Использование Жумбо-фреймов позволяет передавать больше информации с меньшими усилиями, т.к. уменьшается нагрузка на ЦПУ и повышается пропускная способность линии связи, за счет уменьшения передачи количества кадров и сокращения служебной информации, добавляемой к кадрам.
- Жумбо-фреймы поддерживают многие модели коммутаторов и сетевых адаптеров Fast/Gigabit Ethernet.

Протоколы локальных сетей

Дуплексный и полудуплексный режимы работы

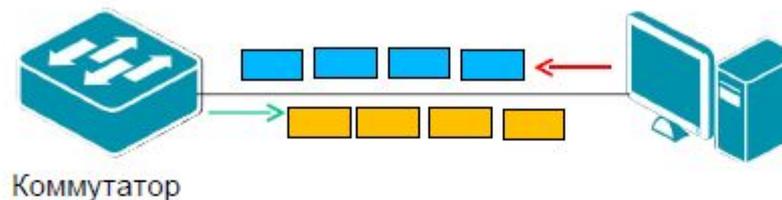
Стандарт IEEE 802.3 определяет два режима работы MAC-подуровня:

- *Полудуплексный (half-duplex)* – использует метод CSMA/CD для доступа узлов к разделяемой среде. Узел может только принимать или передавать данные в один момент времени, при условии получения доступа к среде передачи.
- *Полнодуплексный (full-duplex)* – полнодуплексный Ethernet позволяет паре узлов, имеющих соединение «точка-точка», одновременно принимать и передавать данные. Для этого каждый узел должен быть подключен к выделенному порту коммутатора.

Протоколы локальных сетей

Работа в полнодуплексном режиме

▪ Работа в полнодуплексном режиме обеспечивает возможность одновременного приема и передачи информации устройствами, подключенным по линии связи «точка – точка».



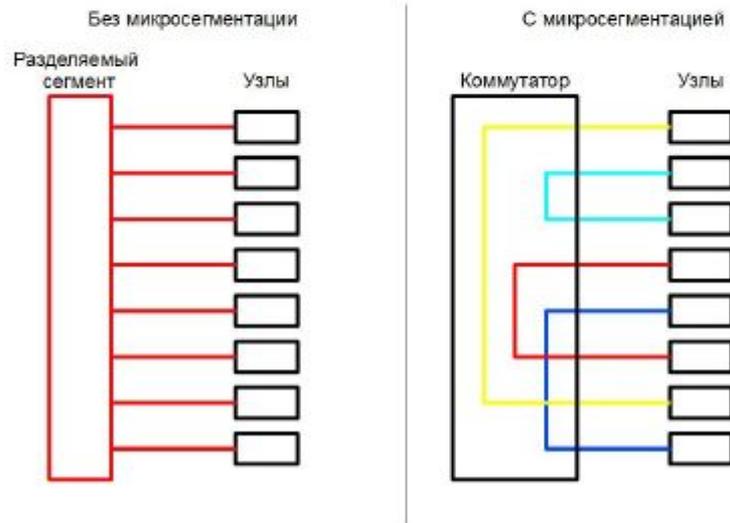
- Отсутствуют коллизии в среде передачи.
- Увеличивается время, доступное для передачи данных и удваивается полезная полоса пропускания канала, т.к. каждый канал обеспечивает полноскоростную одновременную двустороннюю передачу.
- Работа в полнодуплексном режиме возможна только при соединении сетевого адаптера с коммутатором или же при непосредственном соединении коммутаторов при условии, что оба взаимодействующих устройства его поддерживают.
- Интервал отправки между последовательными кадрами не должен быть меньше технологической паузы.
- В полнодуплексном режиме необходимо определить процедуры управления потоком кадров, так как без этого механизма возможны ситуации, когда буферы коммутатора переполняются и он начнет терять кадры, что нежелательно, так как восстановление информации будет осуществляться более медленными протоколами транспортного или прикладного уровней.
- Спецификации 10, 40 и 100 Gigabit Ethernet поддерживают только полнодуплексный режим работы.

Функционирование коммутаторов LAN

Коммутатор локальных сетей

Коммутатор – основное активное сетевое оборудование современных локальных сетей:

- Функционирует на канальном уровне модели OSI.
- Одновременно устанавливает несколько соединений между разными парами портов (микросегментация).
- Обеспечивает возможность работы в режиме полного дуплекса (full duplex).



Функционирование коммутаторов LAN

Функции коммутаторов

Современные коммутаторы, кроме основной своей функции – передачи кадров, могут выполнять множество дополнительных функций, например:

- фильтрация трафика;
- поддержка виртуальных локальных сетей (VLAN);
- определение и ограничение перегрузок в сети;
- определение петель;
- агрегирование физически соединений.

Функционирование коммутаторов LAN

Функционирование коммутаторов локальной сети

Коммутаторы локальных сетей обрабатывают кадры на основе алгоритма **прозрачного моста** (*transparent bridge*), который определен стандартом IEEE 802.1D.

Модель работы прозрачного моста, описанная в IEEE 802.1D определяет следующие процессы:

- продвижение кадров (Forwarding);
- изучение адресов (Learning);
- фильтрация кадров (Filtering).

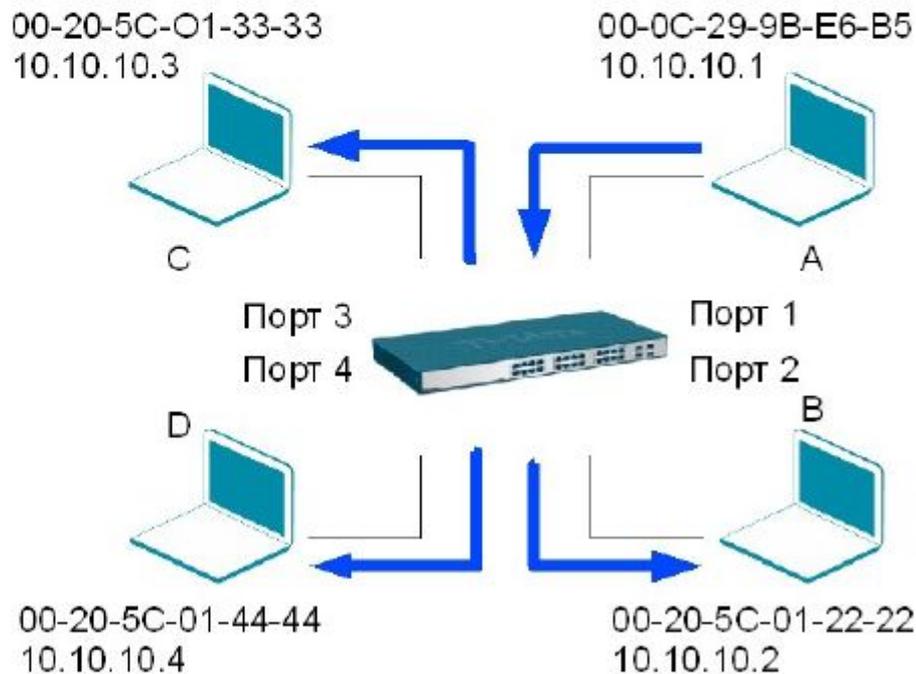
Процесс работы алгоритма прозрачного моста начинается с построения **таблицы коммутации** (*Forwarding DataBase, FDB*).

Функционирование коммутаторов LAN

Функционирование коммутаторов локальной сети

6 байт	6 байт	2 байта		4 байта
Адрес назначения	Адрес источника	Тип Ethernet	ARP	FCS
FF-FF-FF-FF-FF-FF	00-0C-29-9B-E6-B5	Ethernet		

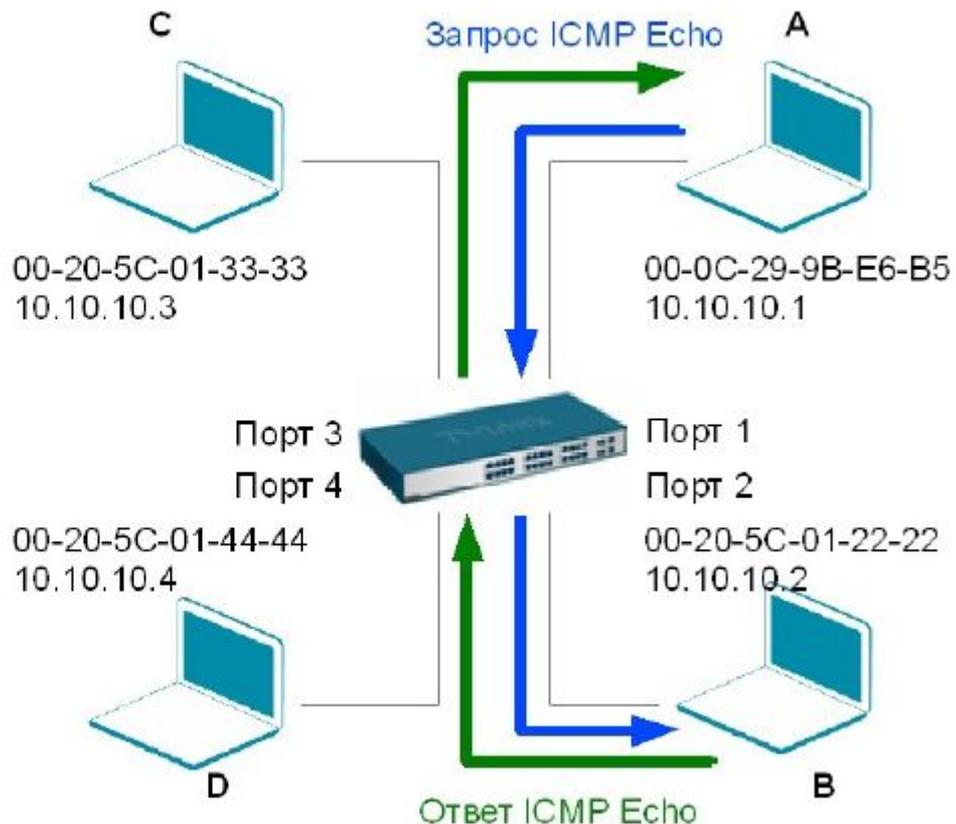
Таблица коммутации
Порт 1 00-0C-29-9B-E6-B5



Функционирование коммутаторов LAN

Функционирование коммутаторов локальной сети

Таблица коммутации	
Порт 1	00-0C-29-9B-E6-B5
Порт 2	00-20-5C-01-22-22



Как только в таблице коммутации появляется хотя бы одна запись, коммутатор начинает использовать ее для пересылки кадров.

Функционирование коммутаторов LAN

Методы коммутации

Первым шагом, который выполняет коммутатор, прежде чем принять решение о передаче кадра, является его получение и анализ содержимого. В коммутаторе может быть реализован один из трех режимов работы, определяющих его поведение при получении кадра:

- коммутация с промежуточным хранением (store-and-forward);
- коммутация без буферизации (cut-through);
- коммутация с исключением фрагментов (fragment-free).

Функционирование коммутаторов LAN

Методы коммутации



Функционирование коммутаторов LAN

Коммутаторы локальной сети можно классифицировать по возможности управления. Существует три категории коммутаторов:

❑ **Неуправляемые коммутаторы** работают по общим принципам коммутации и не поддерживают возможности настройки параметров и обновления программного обеспечения.

❑ **Управляемые коммутаторы** являются сложными устройствами, поддерживающими расширенный набор функций 2 и 3 уровня модели OSI. Управление коммутаторами может осуществляться посредством Web-интерфейса, командной строки (CLI), протокола SNMP, Telnet и т.д.

❑ **Настраиваемые коммутаторы** занимают промежуточную позицию между ними. Они предоставляют пользователям возможность настраивать определенные параметры сети с помощью интуитивно понятных утилит управления, Web-интерфейса, упрощенного интерфейса командной строки, протокола SNMP.

Функционирование коммутаторов LAN

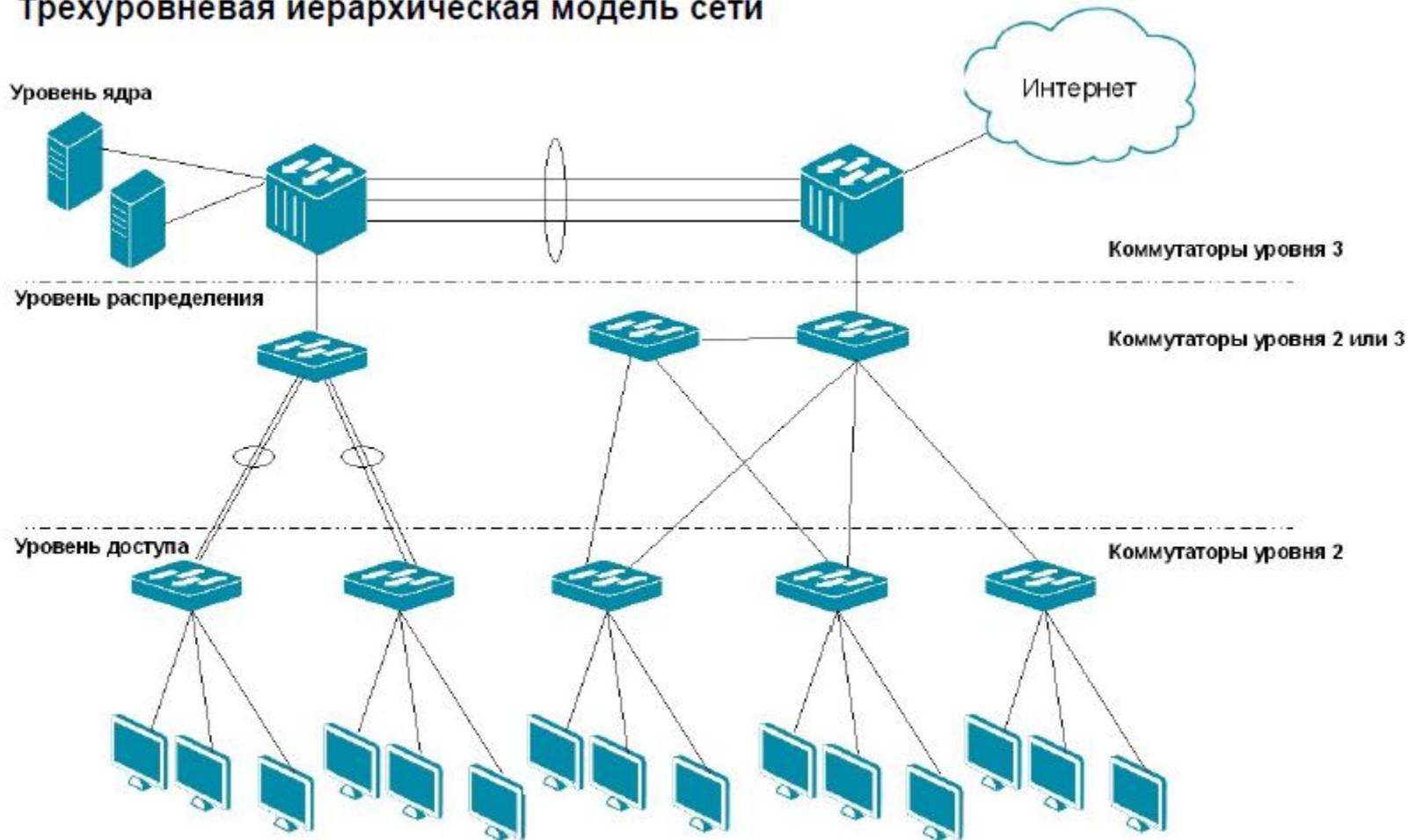
Коммутаторы локальных сетей можно классифицировать в соответствии с уровнями модели OSI, на которых они передают, фильтруют и коммутируют кадры.

Различают:

- **Коммутаторы уровня 2** (Layer 2 (L2) switch) анализируют входящие кадры, принимают решение об их дальнейшей передаче и передают их узлам назначения на основе MAC-адресов канального уровня модели OSI.
- **Коммутатор уровня 3** (Layer 3 (L3) switch) осуществляют коммутацию и фильтрацию на основе адресов канального (уровень 2) и сетевого (уровень 3) уровней модели OSI. Коммутаторы 3-го уровня выполняет коммутацию в пределах рабочей группы и маршрутизацию между различными подсетями или виртуальными локальными сетями (VLAN).

Функционирование коммутаторов LAN

Трёхуровневая иерархическая модель сети



Протокол IP



- **Протокол IP** (Internet Protocol) – основной протокол стека протоколов TCP/IP и сетевого уровня модели OSI, который обеспечивает доставку пакетов данных между любыми узлами составной сети.

Протокол IP выполняет следующие функции:

- Адресация узлов.
 - Инкапсуляция данных.
 - Фрагментация и последующая сборка пакетов.
 - Маршрутизация.
- Протокол IP не гарантирует надёжной доставки пакета до адресата, эта функция выполняется протоколами более высокого уровня. Поэтому его иногда называют *best-effort protocol*.

Протокол IP

Формат пакета (дейтаграммы) IPv4

Версия (4 бита)	Длина заголовка (4 бита)	Тип сервиса (8 бит)	Общая длина (16 бит)	
Идентификатор пакета (16 бит)			Флаги (3 бита)	Смещение фрагмента (13 бит)
Время жизни (8 бит)	Протокол (8 бит)		Контрольная сумма (16 бит)	
IP-адрес источника (32 бита)				
IP-адрес назначения (32 бита)				
Опции				Выравнивание
Данные				

- **Версия (Version)** — для IPv4 значение поля должно быть равно 4.
- **Длина заголовка (IHL, Internet Header Length)** IP-пакета в 32-битных словах. Указывает на начало блока данных (*payload*) в пакете. Обычно значение для этого поля равно 5.
- **Тип сервиса (Type of Service)** — задает приоритетность пакета.
- **Общая длина (Total Length)** - общая длина пакета с учетом заголовка и поля данных.
- **Идентификатор пакета (Identification)** — используется для распознавания пакетов, образовавшихся путем фрагментации исходного пакета. Все фрагменты должны иметь одинаковое значение этого поля.
- **Флаги (Flags)** — содержат признаки, связанные с фрагментацией.
- **Смещение фрагмента (Fragment Offset)** — значение, определяющее позицию фрагмента в потоке данных.
- **Время жизни (Time to Live)** — предельный срок, течения которого пакет может перемещаться по сети.
- **Протокол (Protocol)** — указывает, какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета.
- **Контрольная сумма (Header Checksum)** — рассчитывается только по заголовку и позволяет определить целостность пакета.
- **IP-адрес источника (Source IP Address)** и **IP-адрес назначения (Destination IP Address)** — указывают отправителя и получателя пакета.
- **Опции (IP options)** — необязательное поле, используется при отладке сети.
- **Выравнивание (Padding)** — дополнение IP-заголовка до 32-битной границы.

Адресация сетевого уровня

- ✓ Для того, чтобы доставить данные через составную сеть, надо знать, где расположен адресат.
- ✓ Одной из основных функций протокола IP является адресация.

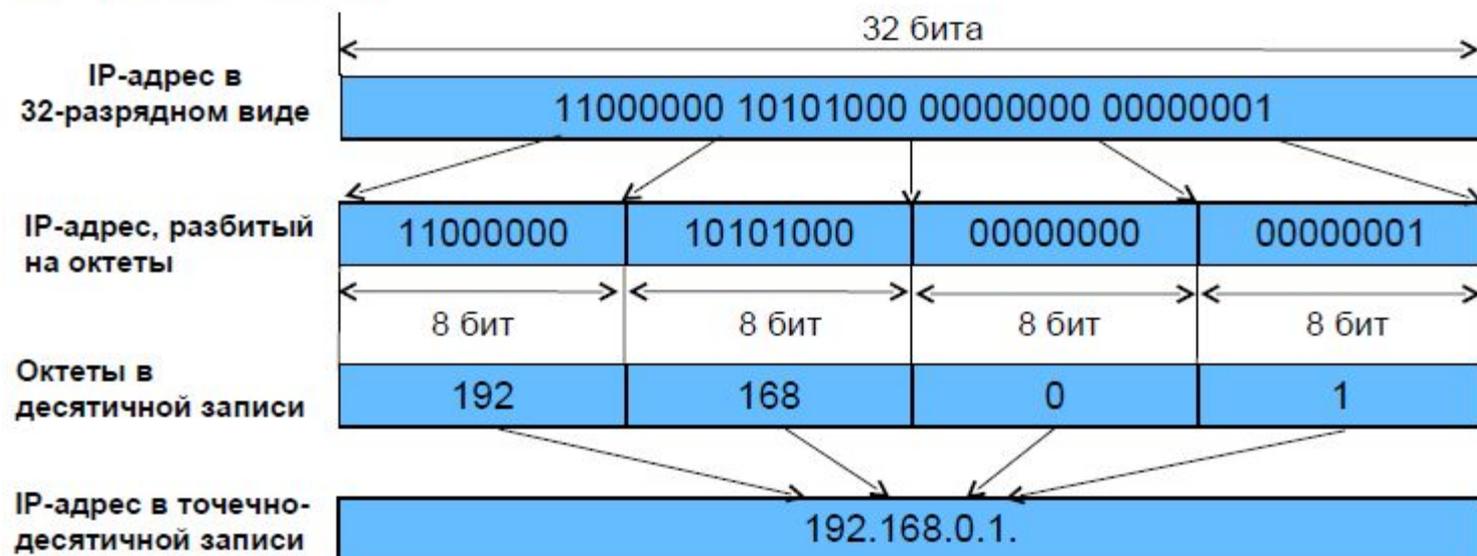
Функции IP-адреса:

- **Идентификация сетевых интерфейсов:** IP-адрес обеспечивает уникальную идентификацию интерфейса между устройством и сетью. Это требуется для гарантии, что пакет будет передан нужному получателю.
 - **Маршрутизация:** когда источник и получатель пакета находятся в разных сетях, пакет должен быть доставлен, используя промежуточные системы – этот процесс называется *маршрутизацией*. IP-адрес используется для маршрутизации пакетов.
- ✓ IP-адрес не идентифицирует непосредственно устройство.
 - ✓ Некоторые устройства, например, маршрутизаторы, могут иметь более одного сетевого подключения и соответственно несколько IP-адресов.

Адресация сетевого уровня

Представление адреса IPv4

■ IPv4-адрес имеет разрядность 32 бита и представляется в точечно-десятичной нотации для удобства запоминания.



Адресация сетевого уровня

Адрес IPv4

IP-адрес состоит из двух частей:

- Идентификатор сети - Network Identifier (Net ID) – используется для маршрутизации.
- Идентификатор узла - Host Identifier (Host ID) – используется для уникальной идентификации узла внутри сети.



Адресация сетевого уровня

Классовая IP-адресация

- Первой появилась «классовая модель» IP-адресации.
- Все пространство IP-адресов делится на 5 классов.
- Принадлежность к классу определяется по нескольким битам первого октета IP-адреса.



Адресация сетевого уровня

Классы IP-адресов

Согласно классовой модели IP-адресации, существует определенное количество сетей каждого класса (пул или пространство адресов), и в сети каждого класса может быть адресовано только определенное количество сетевых узлов.

Класс адреса	Диапазон адресов	Доступное количество сетей	Доступное количество узлов
Класс А	1.0.0.0-126.0.0.0	126	16 777 214
Класс В	128.0.0.0-191.255.0.0	16 384	65 532
Класс С	192.0.0.0-223.255.255.0	2 097 152	254
Класс D	224.0.0.0- 239.255.255.254	Multicast	-
Класс E	240.0.0.0-254.255.255.255	Зарезервировано	-

Адресация сетевого уровня

Публичные и частные IP-адреса

Публичные (public) IP-адреса – адреса, уникальные в масштабах планеты, используемые в Интернет.

Частный (private) IP-адрес – IP-адрес, принадлежащий к диапазонам адресов, зарезервированных для использования в локальных сетях и не используемых в сети Интернет.

Класс А От 10.0.0.0 до 10.255.255.255

Класс В От 172.16.0.0 до 172.31.255.255

Класс С От 192.168.0.0 до 192.168.255.255

Типы адресов и способы назначения

Private address

10.0.0.0 -10.255.255.255

172.16.0.0-172.31.255.255

192.168.0.0 -192.168.255.255

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: 1 . 1 . 1 . 100

Subnet mask: 255 . 0 . 0 . 0

default gateway: 1 . 1 . 1 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 1 . 1 . 1 . 200

Alternate DNS server:

Validate settings upon exit

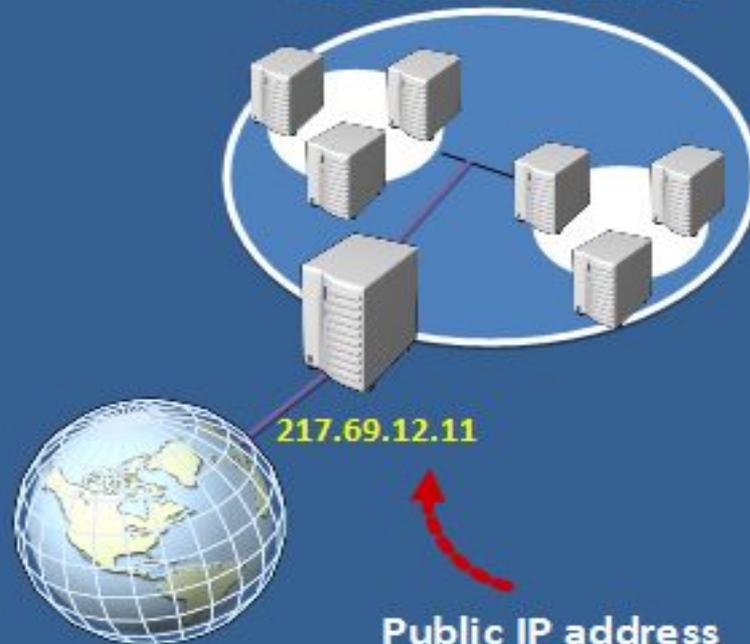
Advanced...

OK Cancel

Статика

Private range

10.10.0.1-10.10.0.20



Public IP address

Протоколы маршрутизации

Понятие маршрутизации

- *Маршрутизация* - процесс определения маршрута следования информации от отправителя к получателю в составной сети.
- Маршрутизация выполняется специальными устройствами – *маршрутизаторами*.
- Маршрутизаторы принимают решение о том куда передавать пакет на основе его сетевого адреса назначения, который сравнивается с информацией, хранимой в специальных *таблицах маршрутизации*.
- *Таблица маршрутизации* – электронная таблица (файл) или база данных, хранящаяся на маршрутизаторе или сетевом компьютере, описывающая соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора.



Протоколы маршрутизации

Таблица маршрутизации

- Каждая запись таблицы маршрутизации содержит следующую обязательную информацию:
 - **Адрес назначения** — адрес сети (в некоторых случаях узла) назначения;
 - **Маска сети** — маска, соответствующая адресу назначения (для сетей IPv4 маска /32 (255.255.255.255) позволяет указать единичный узел сети);
 - **Адрес шлюза** — IP-адрес интерфейса следующего транзитного маршрутизатора, находящегося на пути к получателю;
 - **Интерфейс** — идентификатор выходного интерфейса, через который пакет покидает устройство;
 - **Метрика** — числовой показатель, задающий предпочтительность маршрута. Чем меньше число, тем более предпочтителен маршрут (интуитивно представляется как расстояние).
 - **Тип протокола** - информация о протоколе маршрутизации, создавшем запись в таблице маршрутизации.

```
DGS-3620-28TC:admin#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway          Interface        Cost    Protocol
-----
10.0.0.0/8          0.0.0.0          System           1       Local
172.16.0.0/23       172.16.8.2       iptv-1           2       RIP
172.16.2.0/23       172.16.8.2       iptv-1           2       RIP
172.16.8.0/30       0.0.0.0          iptv-1           1       Local
172.16.8.4/30       0.0.0.0          iptv-2           1       Local
172.16.8.8/30       172.16.8.6       iptv-2           2       RIP
172.16.8.12/30      0.0.0.0          stream           1       Local

Total Entries: 7
```

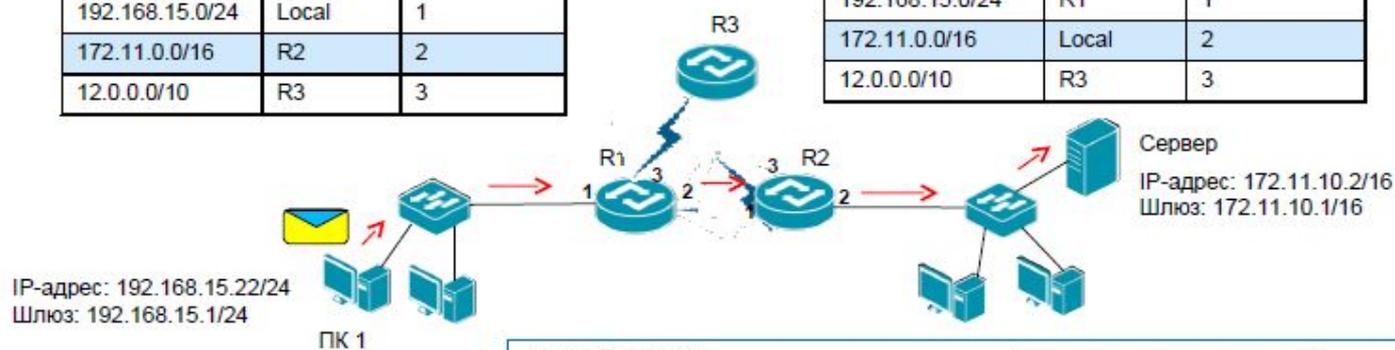
Протоколы маршрутизации

Процесс обработки пакета маршрутизатором

1. Маршрутизатор получает кадр на интерфейс.
2. Проверяет полученный кадр и если он не поврежден, извлекает из него пакет сетевого уровня.
3. Извлекает из заголовка сетевого уровня IP-адрес получателя.
4. Сравнивает IP-адрес назначения с записями в таблице маршрутизации.
5. Если соответствие найдено, данные передаются на нужный интерфейс, если нет – пакет отбрасывается и отправителю отправляется ICMP-сообщение «Destination Unreachable» (Получатель недоступен).
6. Модифицирует некоторые поля пакета, например TTL, изменяет контрольную сумму.
7. Формирует новый кадр, инкапсулируя в него пакет.
8. Пересылает кадр следующему на пути маршрутизатору.

IP-адрес/маска	Маршрут	Интерфейс
192.168.15.0/24	Local	1
172.11.0.0/16	R2	2
12.0.0.0/10	R3	3

IP-адрес/маска	Маршрут	Интерфейс
192.168.15.0/24	R1	1
172.11.0.0/16	Local	2
12.0.0.0/10	R3	3



Сетевой уровень	
192.168.15.22	171.11.10.2

Канальный уровень				
DA Сервер	SA R2.2	192.168.15.22	171.11.10.2	

Протоколы маршрутизации

Статическая маршрутизация

Статическую маршрутизацию полезно использовать в следующих случаях:

- Если к сети имеется небольшое число маршрутов;
- Если по соображениям безопасности необходимо скрыть определенную информацию о сетях с ограниченным доступом;
- Для создания маршрутов по умолчанию.
- *Маршрут по умолчанию* – это маршрут, который используется в том случае, если другой маршрут к пункту назначения неизвестен.



Протоколы маршрутизации



Динамическая маршрутизации

➤ Динамическая маршрутизация выполняет две важные функции:

- Обслуживание таблицы маршрутизации;
- Своевременный обмен данными о маршрутах между маршрутизаторами в форме обновлений.

➤ Для обмена информацией маршрутизаторы используют протоколы маршрутизации (*Routing protocols*).

➤ Протоколы маршрутизации определяют наборы правил, используемые маршрутизаторами при взаимодействии друг с другом.

□ Маршрутизаторы могут поддерживать сразу несколько протоколов маршрутизации и вести для них отдельные таблицы маршрутизации.

Протоколы маршрутизации

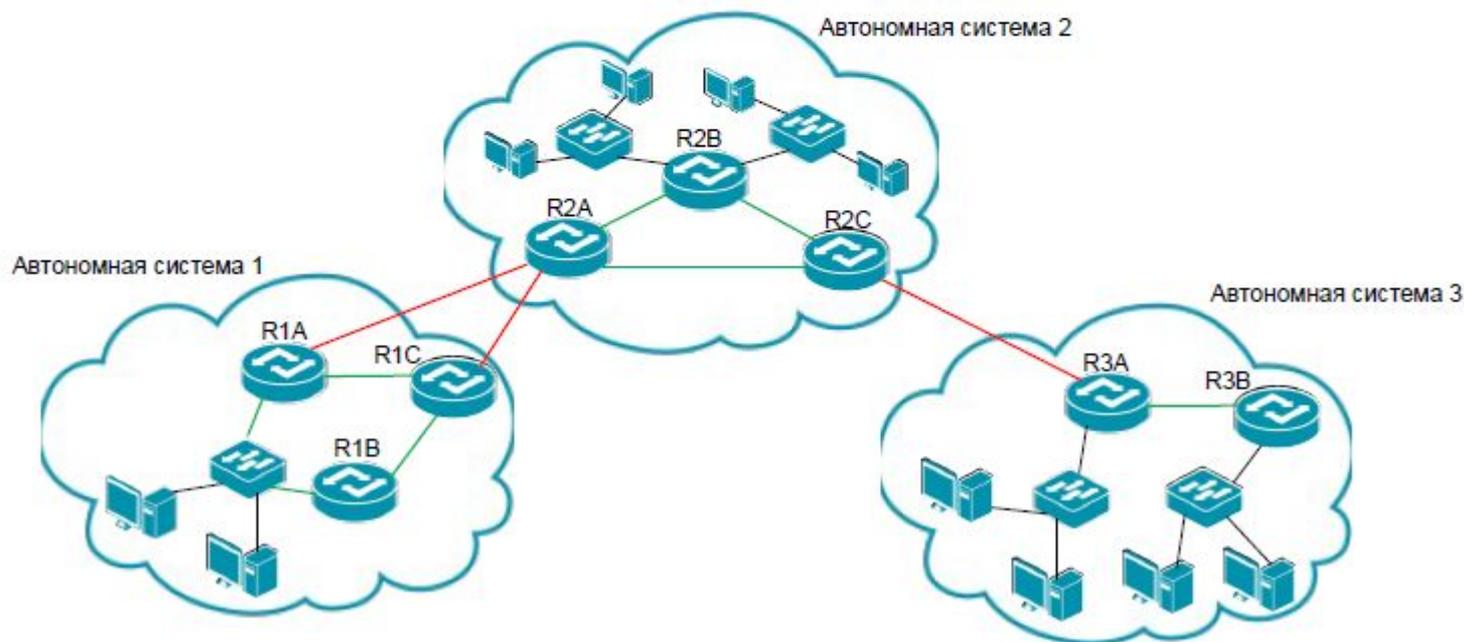
Протоколы маршрутизации

➤ Существует два типа протоколов маршрутизации :

▪ **Внутренние протоколы маршрутизации** (*Interior Routing Protocols*): используются для обмена маршрутной информацией внутри автономной системы.

▪ **Внешние протоколы маршрутизации** (*Exterior Routing Protocols*): используются для обмена маршрутной информацией между автономными системами.

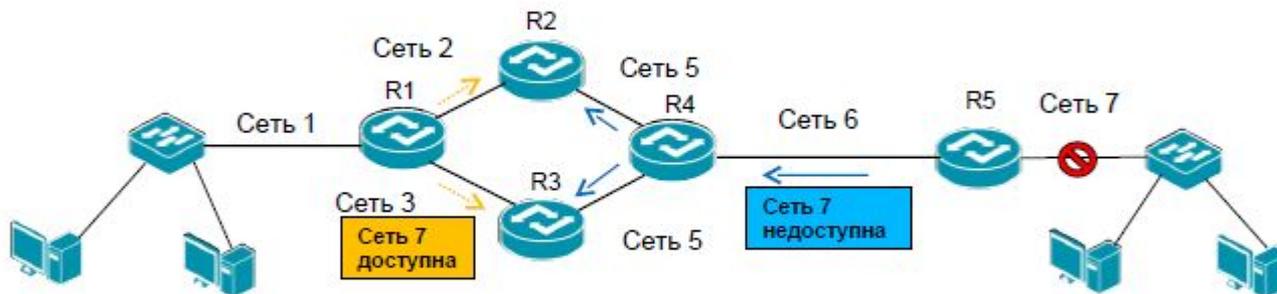
➤ **Автономная система** (*Autonomous system, AS*) представляет собой группу маршрутизаторов и IP-сетей, контролируемых одной организацией или находящихся под единым административным управлением, которые используют единую согласованную политику для внутренней маршрутизации.



Протоколы маршрутизации

Проблемы при работе дистанционно-векторного алгоритма маршрутизации: Стремление к бесконечности

- ❖ В результате медленной сходимости у маршрутизаторов появляется противоречивая информация о маршрутах, в результате чего появляются петли маршрутизации.
- ❖ Петли маршрутизации приводят к проблеме, которая называется «стремление к бесконечности».



Для решения этой проблемы используются следующие методы:

1. Ограничение максимального расстояния (числа переходов).
2. Метод расщепления горизонта (*Split horizon*).
3. Испорченный обратный маршрут (*Poisoned reverse*).
4. Триггерные обновления (*Triggered Update*).
5. Установка таймеров удержания (*Hold-down timer*).

Недостатки и ограничения протокола IPv4

- **Ограниченность адресного пространства**

Адрес IPv4 имеет длину 32 бита, что дает максимум 4294967296 адресов.

- **Слабая агрегацией адресов**, что приводит к катастрофическому росту таблиц маршрутизации в маршрутизаторах сетей

- **Отсутствие механизма автоматической конфигурации адресов**

В протоколе IPv4 не заложен механизм автоматического назначения адресов хостам сети . Эта операция обычно проводится сетевым администратором вручную ,либо полуавтоматически с использованием вспомогательных средств.

Недостатки и ограничения протокола IPv4

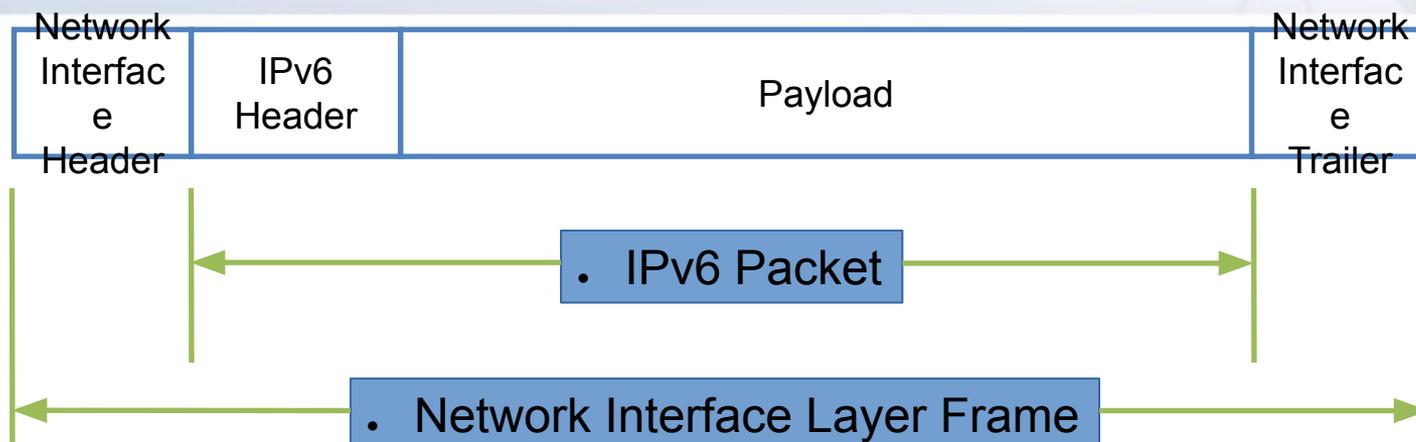
- **Проблемы, связанные с механизмом фрагментации**

Для передачи больших дейтаграмм протокол IPv4 фрагментирует их на несколько более мелких, при этом фрагментацию может осуществлять как отправитель, так и любой маршрутизатор на пути следования дейтаграммы. Возможность фрагментации дейтаграмм промежуточными маршрутизаторами в IPv4 ограничивает производительность этих маршрутизаторов

- **Проблема безопасности коммуникаций**

В протоколе IPv4 не предусмотрено каких-либо средств организации безопасности передачи данных.

IPv6



2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A/64

128-bit address space

2^{128} possible addresses

340,282,366,920,938,463,463,3

74,607,431,768,211, 456

addresses (3.4×10^{38})

IPv6



Отступ в октетах	Отступ в битах	0								1								2								3							
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Traffic Class				Flow Label																							
4	32	Payload Length																Next Header				Hop Limit											
8	64	Source Address																															
C	96																																
10	128																																
14	160																																
18	192	Destination Address																															
1C	224																																
20	256																																
24	288																																

IPv6

Описание полей:

Version: версия протокола; для IPv6 это значение равно 6 (значение в битах — 0110).

Traffic Class: приоритет пакета (8 бит). Это поле состоит из двух значений. Старшие 6 бит используются DSCP для классификации пакетов. Оставшиеся два бита используются ECN для контроля перегрузки.

Flow Label: метка потока.

Payload Length: в отличие от поля Total Length в протоколе IPv4 данное поле не включает фиксированный заголовок пакета (16 бит).

Next Header: задаёт тип расширенного заголовка (англ. IPv6 extension), который идёт следующим. В последнем расширенном заголовке поле Next Header задаёт тип транспортного протокола (TCP, UDP и т. д.)

Hop Limit: аналог поля time to live в IPv4 (8 бит).

Source Address и Destination Address: адрес отправителя и получателя соответственно; по 128 бит.

С целью повышения производительности и с расчётом на то, что современные технологии канального и транспортного уровней обеспечивают достаточный уровень обнаружения ошибок, заголовки не имеют контрольной суммы.

IPv6-адрес в двоичном виде:

```
00100000000000010000110110111000000000000000000010111100111011  
000000101010101010000000001111111111111110001010001001110001011010
```

Разделенные по 16-бит:

```
0010000000000001 0000110110111000 0000000000000000 0010111100111011 0000001010101010  
0000000011111111 1111111000101000 1001110001011010
```

Каждый 16-битный блок преобразуется в шестнадцатеричное и разделяется с помощью двоеточия:

```
2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A
```

Убираем ведущие нули в каждом блоке:

```
2001:DB8:0:2F3B:2AA:FF:FE28:9C5A
```

Примеры:

FE80:0:0:0:2AA:FF:FE9A:4CA2 становится

FE80::2AA:FF:FE9A:4CA2

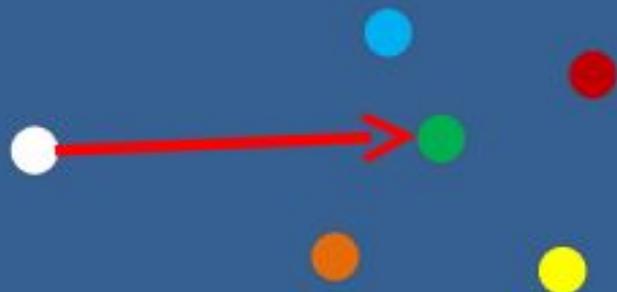
FF02:0:0:0:0:0:0:2 становится FF02::2

FF02:30:0:0:0:0:0:5 не FF02:3::5, но

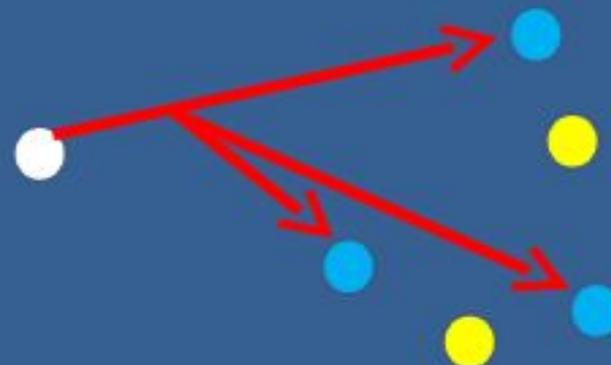
FF02:30::5

Типы адресов IPv6

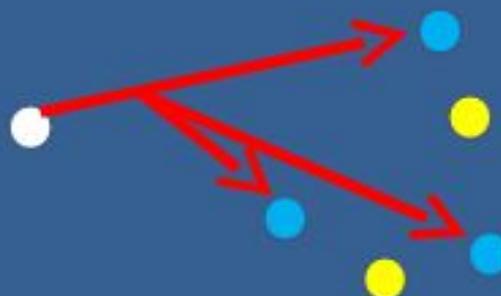
Unicast



Anycast



Multicast



Типы адресов IPv6

Unspecified address:

- 0:0:0:0:0:0:0:0 or ::
- Эквивалентен адресу IPv4 0.0.0.0

Loopback address:

- 0:0:0:0:0:0:0:0:1 or ::1
- Эквивалентен адресу IPv4 127.0.0.1
- Используется для тестирования локального стека IPv6

Типы адресов IPv6

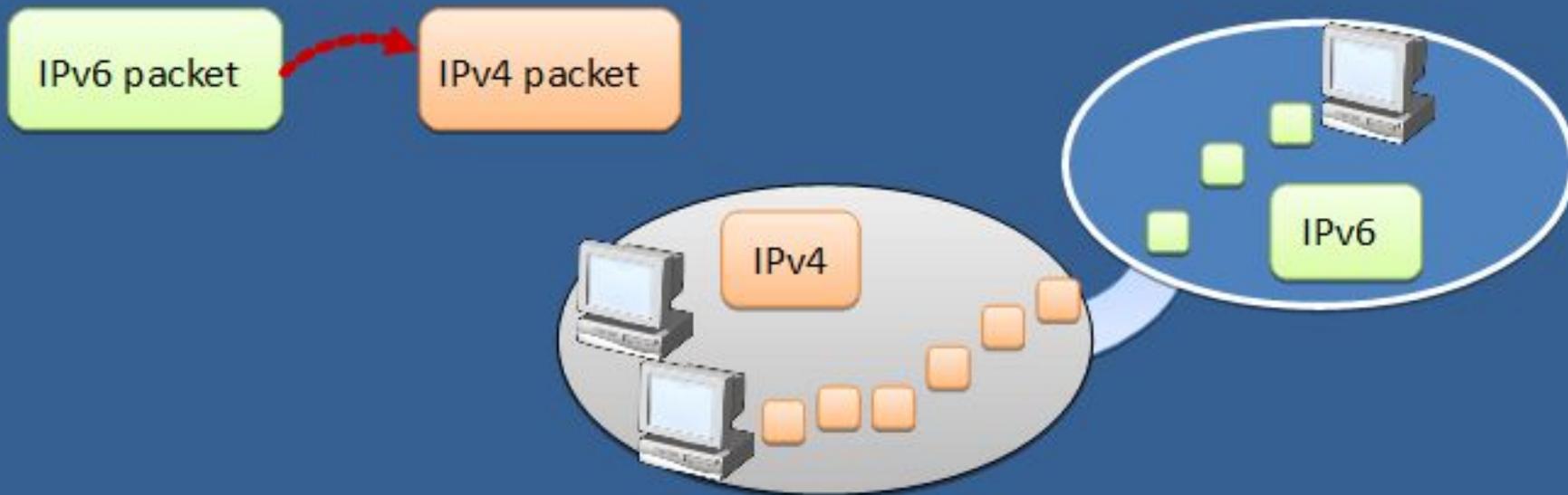
Unspecified address:

- 0:0:0:0:0:0:0:0:0 or ::
- Эквивалентен адресу IPv4 0.0.0.0

Loopback address:

- 0:0:0:0:0:0:0:0:1 or ::1
- Эквивалентен адресу IPv4 127.0.0.1
- Используется для тестирования локального стека IPv6

IPv6





Спасибо за внимание!