Компьютерные сети

Преподаватель:

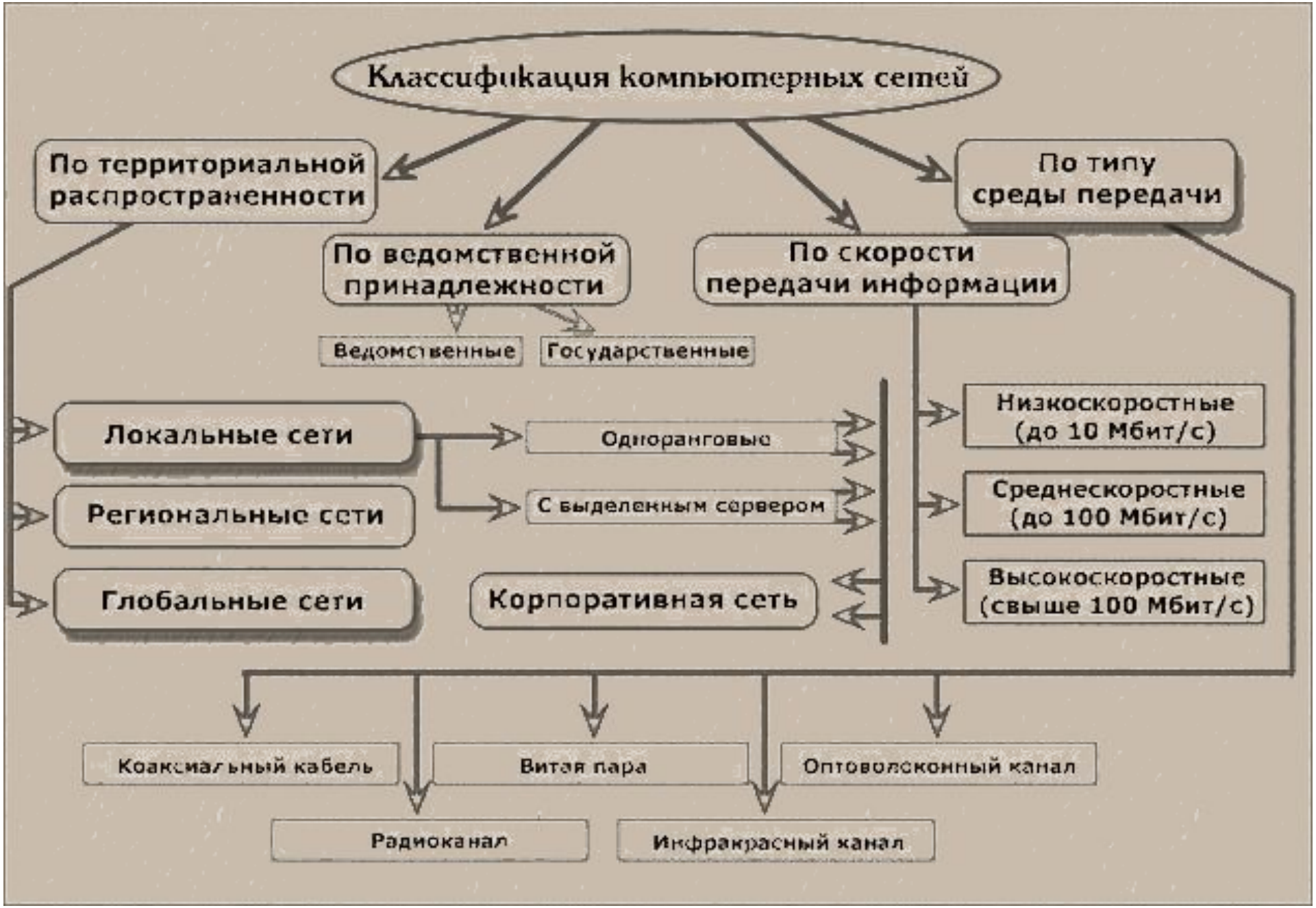
Абрамов Сергей Андреевич

Компьютерная сеть (вычислительная сеть, сеть передачи данных) — система связи компьютеров и/или компьютерного оборудования (серверы, маршрутизаторы и другое оборудование).

Распределённая вычислительная система – компьютерная сеть, имеющая *несколько центров обработки данных*

Мультипроцессорные компьютеры имеют несколько процессоров, каждый из которых может независимо от остальных выполнять свою программу.

Многомашинный вычислительный комплекс (МВК) – это вычислительный комплекс, включающий в себя несколько компьютеров, а также программные и аппаратные средства связи компьютеров, которые обеспечивают работу всех компьютеров комплекса как единого целого.


Классификация компьютерных сетей
По территориальной распространенности
По ведомственной принадлежности
По скорости передачи информации
По типу среды передачи
Ведомственные
Государственные
Локальные сети
Региональные сети
Глобальные сети
Одноранговые
С выделенным сервером
Корпоративная сеть
Низкоскоростные (до 10 Мбит/с)
Среднескоростные (до 100 Мбит/с)
Высокоскоростные (свыше 100 Мбит/с)
Коаксиальный кабель
Витая пара
Оптоволоконный канал
Радиоканал
Инфракрасный канал

К **локальным сетям** (англ. Local Area Networks, LAN) относят сети компьютеров, сосредоточенные на небольшой территории (обычно в радиусе не более 1-2 км). В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации.

Городские сети (англ. Metropolitan Area Networks, MAN) являются менее распространенным типом сетей. Они предназначены для обслуживания территории крупного города – мегаполиса.

Глобальные сети – (англ. Wide Area Networks, WAN) объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах, то есть радиус таких сетей может составлять тысячи километров.

Корпоративные сети (англ. Enterprise-Wide Networks) объединяют большое количество компьютеров на всех территориях компании. Они могут быть сложно связаны и покрывать город, регион или даже континент.

Мейнфрейм - (от англ. mainframe) — большой универсальный высокопроизводительный отказоустойчивый сервер со значительными ресурсами ввода-вывода, большим объёмом оперативной и внешней памяти, предназначенный для использования в критически важных системах.

Обеспечение качества работы сети:

1) Гарантия некоторой числовой величины;
2) Негарантированная доставка

Гарантия некоторой числовой величины:

Frame Relay (FR-сеть) – гарантирует скорость E3=34,368 Мбит/с.

Asynchronous Transfer Mode (ATM) – гарантирует определённый уровень пропускной способности.

Негарантированная доставка:

Best Effort (BE) – технология передачи данных, которая не гарантирует ни доставку данных, ни предоставления определённого качества обслуживания (QoS).

Основные характеристики современных компьютерных сетей

- производительность
- надёжность
- совместимость
- управляемость
- прозрачность
- расширяемость
- масштабируемость

Производительность сети

- **Время реакции –** время между возникновением запроса к какому-либо сетевому сервису и получением ответа на него.
- **Пропускная способность –** отражает объем данных, переданных сетью в единицу времени.
- **Задержка передачи –** интервал времени, между моментом поступления пакета на вход какого-либо сетевого устройства и моментом его появления на выходе этого устройства.

Надёжность сети

- **Коэффициент готовности** – вероятность того, что оборудование в данный момент времени находится в работоспособном состоянии.
- **Безопасность** – способность сети защитить данные от несанкционированного доступа.
- **Отказоустойчивость** – способность сети работать в условиях отказа некоторых её элементов.

- **Совместимость сети –** способность сети включать в себя разнообразное программное и аппаратное обеспечение и поддерживать работу с ними.
- **Управляемость сети –** возможность централизованно контролировать состояние основных элементов сети, выявлять и разрешать проблемы, возникающие при работе сети, выполнять анализ производительности и планировать развитие сети.

- **Прозрачность сети –** свойство сети скрывать от пользователя детали своего внутреннего устройства, тем самым упрощая его работу в сети.
- **Расширяемость сети –** возможность добавления отдельных элементов сети, наращивания длины сегментов сети и замены существующей аппаратуры более мощной.
- **Масштабируемость сети –** возможность увеличения количества узлов и протяженности связей в очень широких пределах.

Преимущества компьютерных сетей

- Распределение вычислительной нагрузки;
- Повышение отказоустойчивости сети в целом;
- Разделение дорогостоящих ресурсов;
- Совершенствование коммуникаций;
- Улучшение доступа к информации;
- Быстрое и качественное принятие решений;
- Свобода в территориальном размещении компьютеров.

Распределение вычислительной нагрузки

- Способность выполнять **параллельные вычисления**
- Лучшее соотношение **производительность-стоимость**

Повышенная отказоустойчивость

- **Избыточность сети –** наличие в сети резервных маршрутов для прохождения трафика из точки А в точку Б.

Распределение ресурсов

- **Распределение дорогостоящих ресурсов –** возможность совместного использования данных и устройств, а также гибкого распределения работ по всей системе.

Совершенствование коммуникаций

- **Совершенствование коммуникаций –** улучшение процесса обмена информацией и взаимодействия между сотрудниками предприятия, а также его клиентами и поставщиками.

Улучшенный доступ к информации

- Оперативный доступ к обширной корпоративной информации достигается с помощью технологии **Intranet.**
- **Intranet** – это «частный» Интернет, ограниченный виртуальным пространством отдельно взятой организации.

Топология физических связей

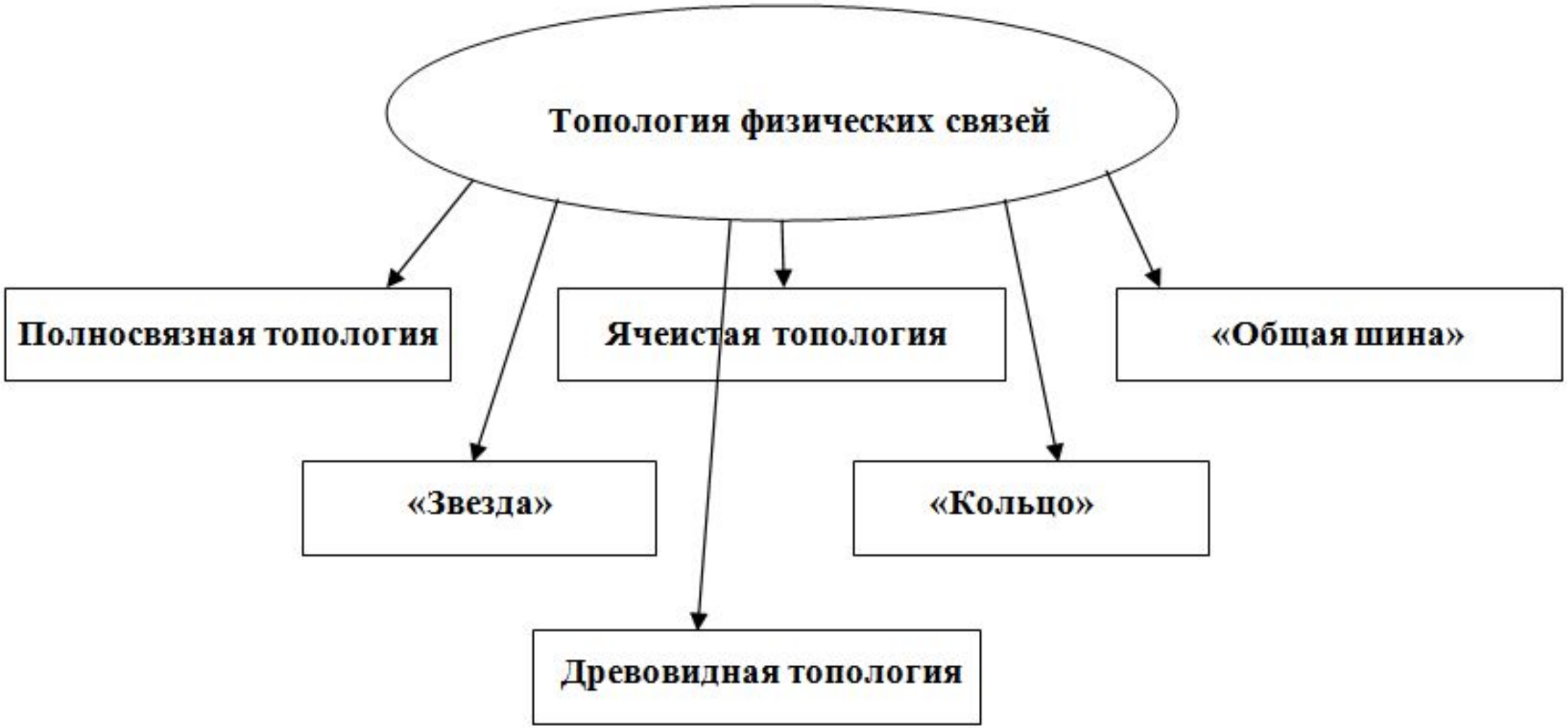
- **Топология физических связей -** способ организации физических связей.
- В компьютерной сети – это конфигурация графа, вершинам которого соответствуют компьютеры сети, а рёбрам – физические связи между ними (линии связи).

Компьютеры, подключенные к сети, называют ***станциями*** или ***узлами сети***.

Связи в компьютерной сети

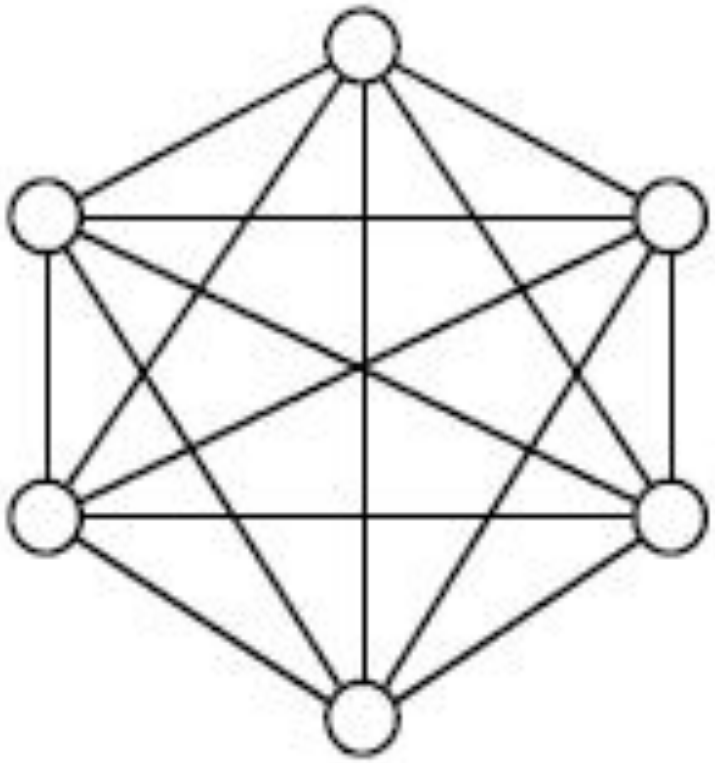
- **Логические связи –** маршрут передачи данных по сети (коммутаторы/маршрутизаторы и т.п.);

- **Физические связи –** способ передачи данных по сети (проводная/беспроводная связь).


Топология физических связей
Полносвязная топология
Ячеистая топология
«Общая шина»
«Звезда»
«Кольцо»
Древовидная топология

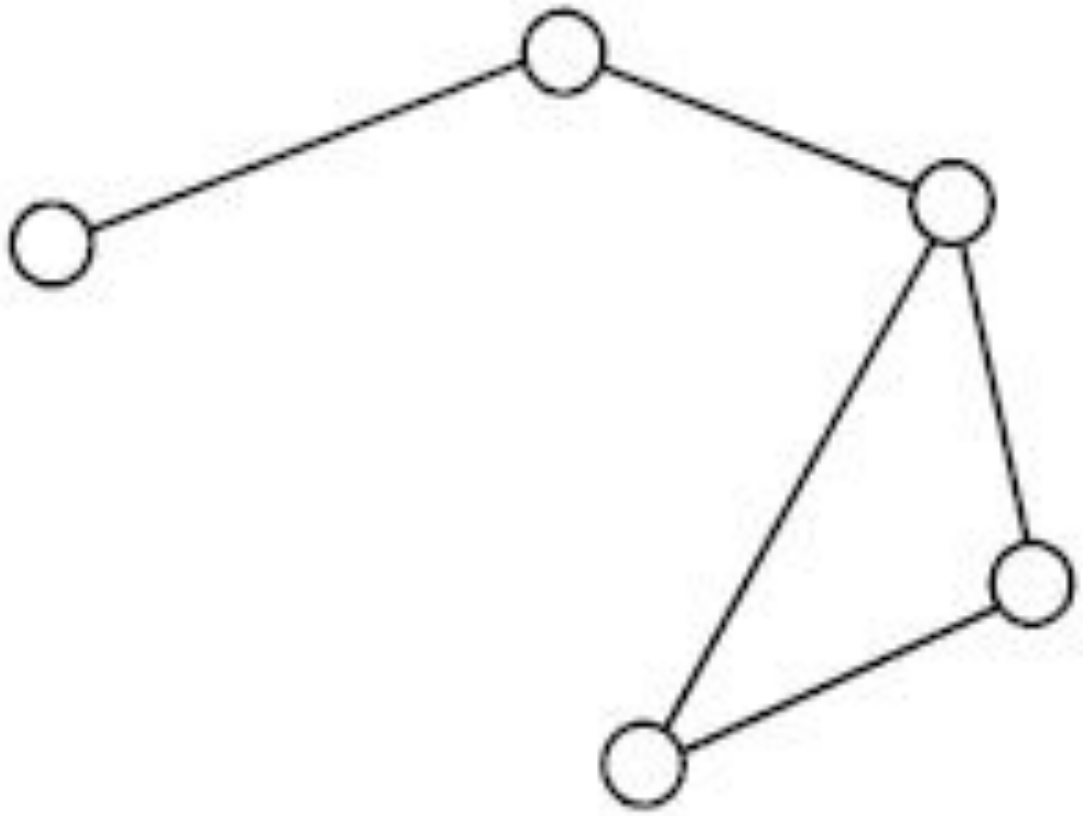
Полносвязная топология

- Иначе называют «Каждый с каждым». Очень **громоздкий** и **неэффективный** вариант. Под каждый компьютер необходимо много портов и кабелей. Применяется очень редко.



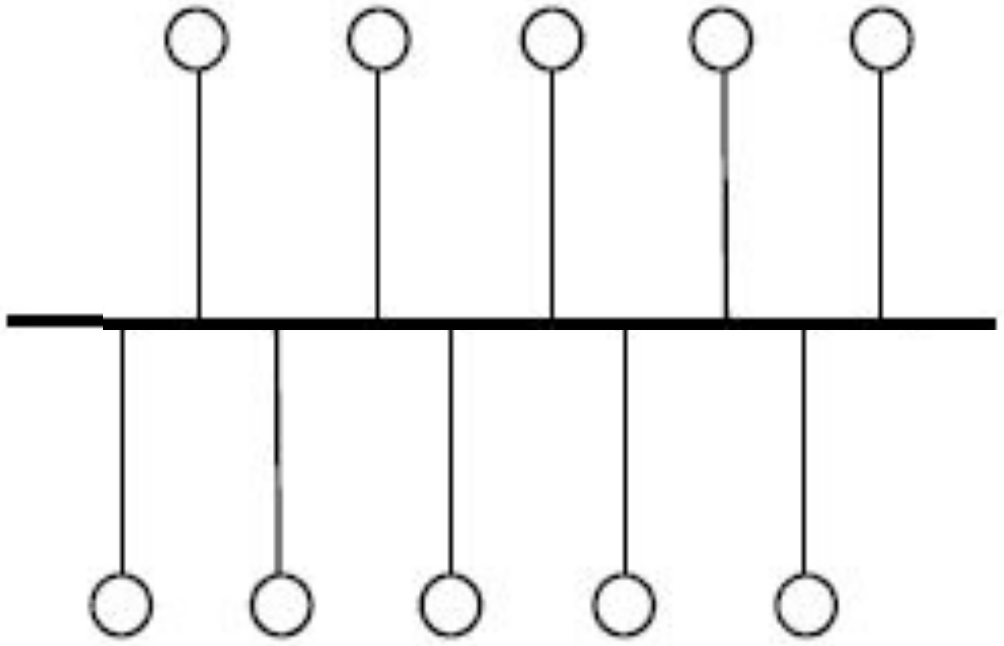
Ячеистая топология

- Связываются только те компьютеры, между которыми происходит интенсивный обмен данными



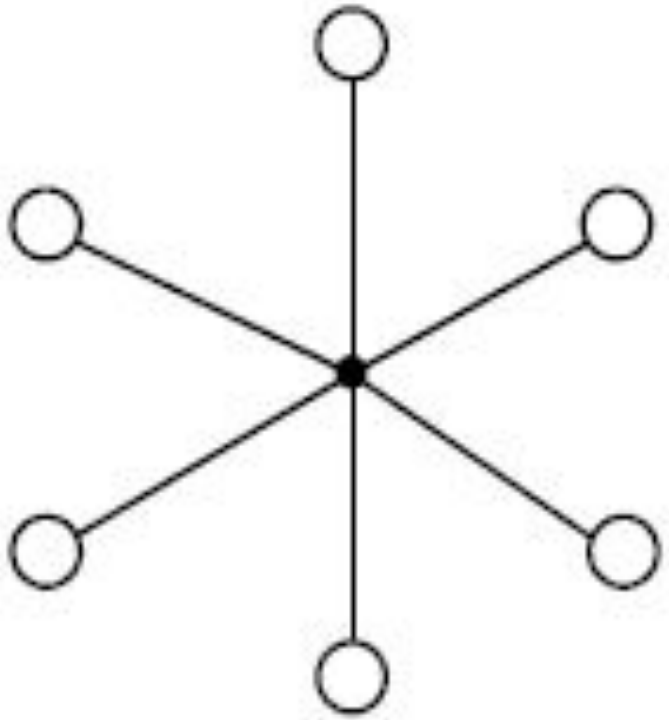
Топология «общая шина»

- Также называют «Bus» или «автобус». Все компьютеры сети подключаются к единому каналу передачи данных.



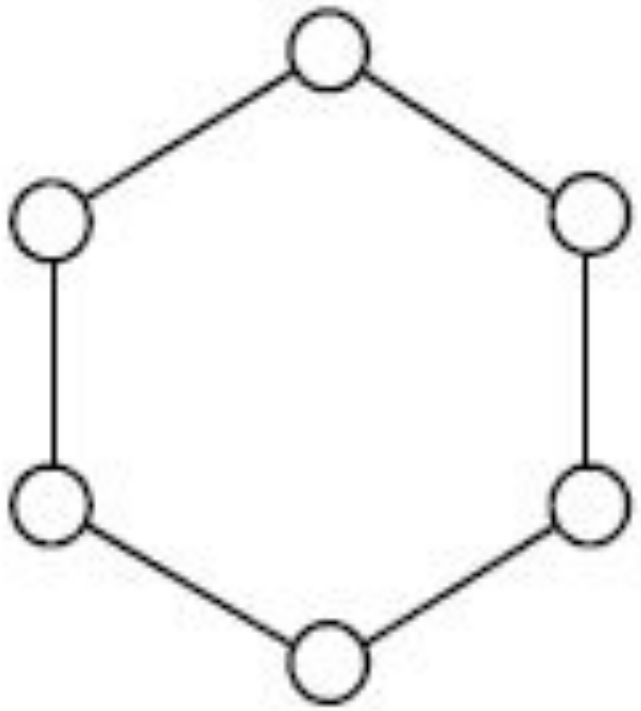
Топология «звезда»

- Каждый компьютер подключается к общему устройству – концентратору (Hub) или коммутатору (Switch) при помощи отдельного кабеля.



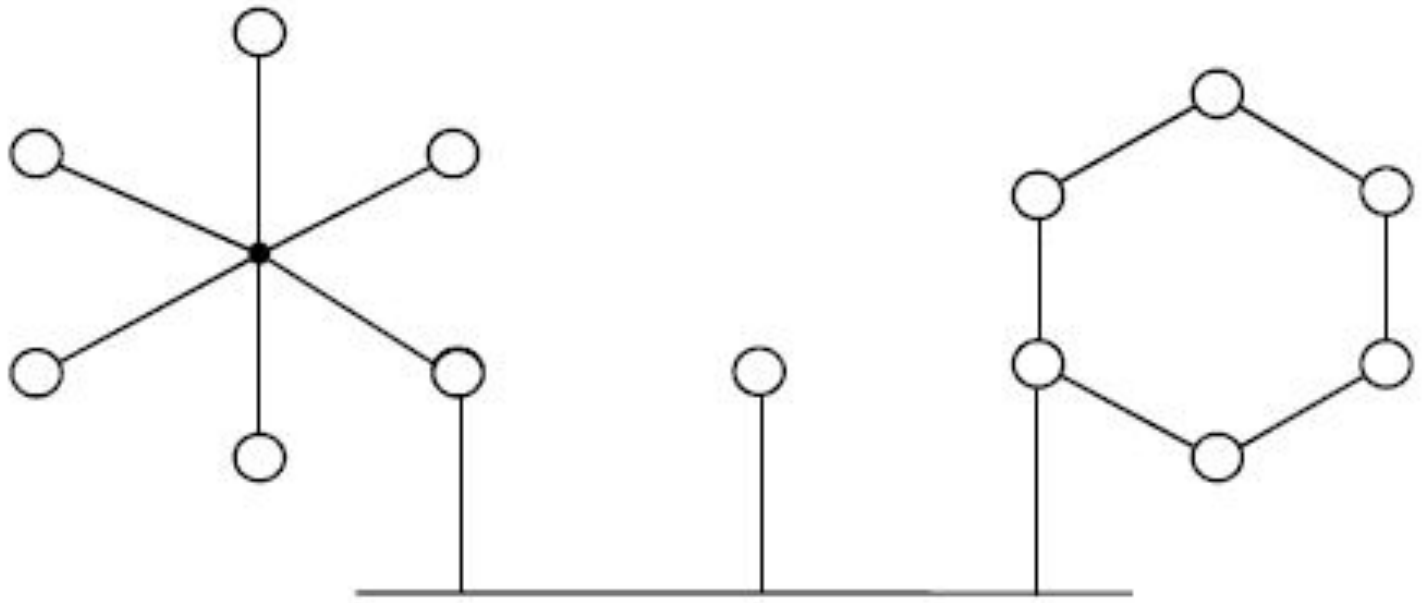
Топология «кольцо»

- Данные передаются по кольцу от одного компьютера к другому, обычно в одном направлении. Если компьютер распознаёт данные как «свои», то он копирует их себе во внутренний буфер.



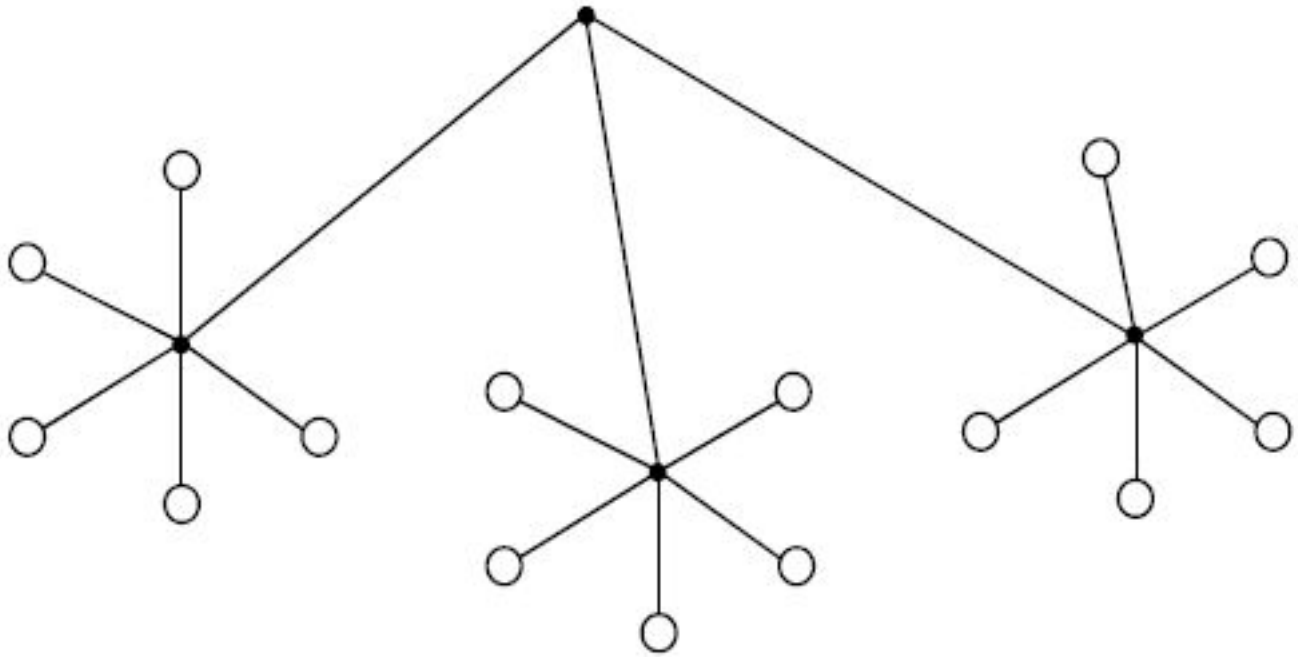
Составные топологии

- Все перечисленные топологии в чистом виде встречаются довольно редко. Поэтому зачастую используют составную (смешанную) топологию.



Древовидная топология

- Среди составных топологий наиболее актуальна **древовидная топология**, которая на данный момент является наиболее распространенной топологией для локальных сетей предприятий.



Линии связи

- **Линия (канал) связи** состоит в общем случае из физической среды, по которой передаются электрические информационные сигналы, аппаратуры передачи данных и промежуточной аппаратуры.
- **Кабель -** набор проводов, изоляционных и защитных оболочек и соединительных разъемов.

Линии связи

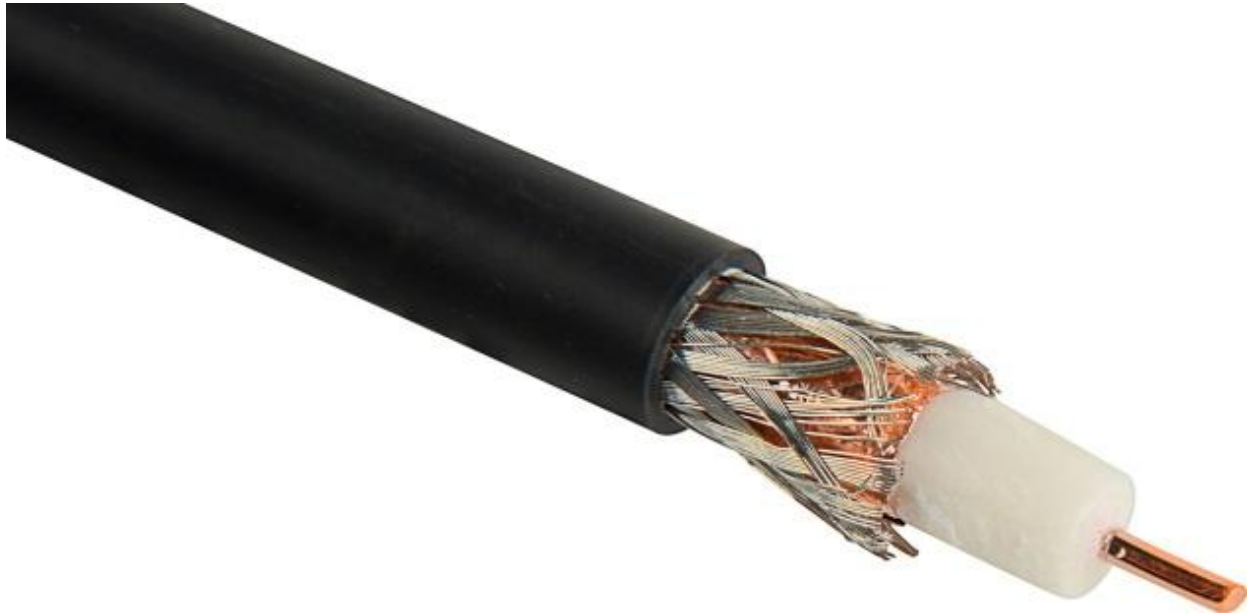
- проводные (воздушные);
- кабельные:
- медные:
- коаксиальные (Coaxial);
- «витая пара» (Twisted Pair, TP);
- волоконно-оптические (Fiber);
- радиоканалы:
- наземная радиосвязь;
- спутниковая радиосвязь.

Проводные (воздушные) линии связи

- Представляют собой провода без каких-либо изолирующих или экранирующих оплёток, проложенные между столбами и висящие в воздухе.

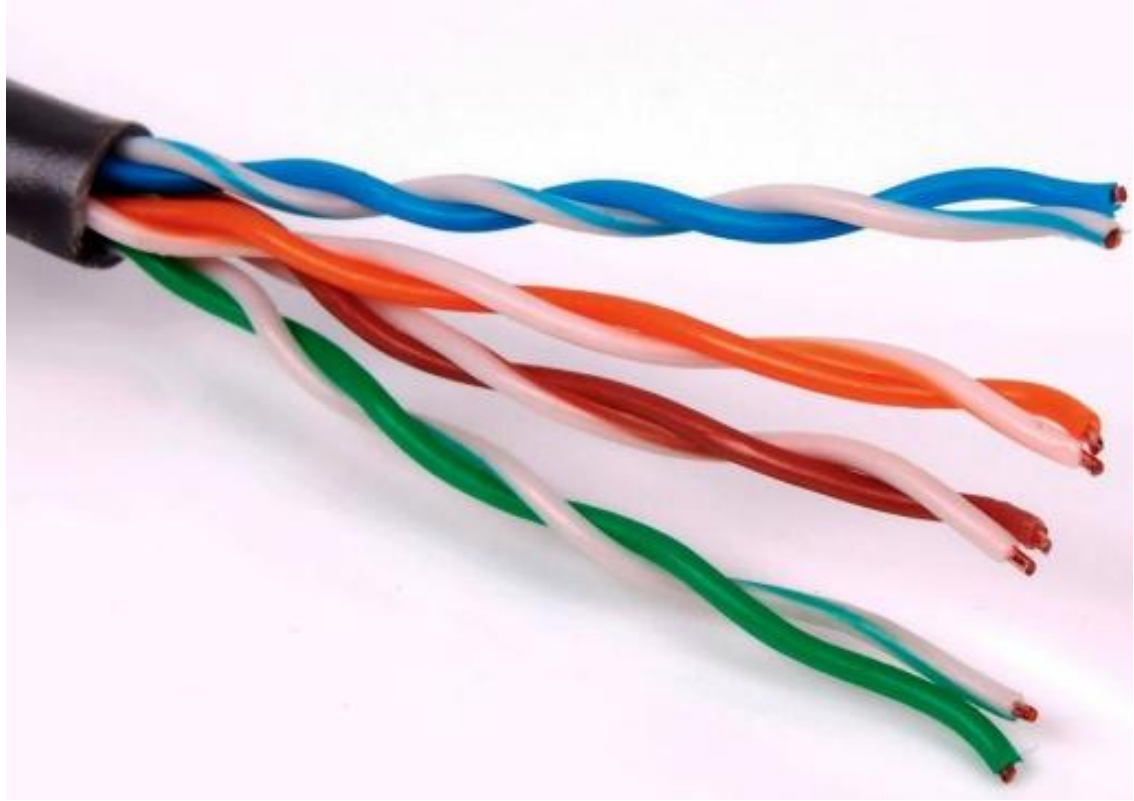
Коаксиальные кабели

- **Коаксиальный кабель** – имеет симметричную конструкцию и состоит из внутренней медной жилы и оплётки, которая отделена от жилы слоем изоляции. Центральная медная жила и оплётка играют роль парных проводников.



Витая пара

- **Витая пара –** скрученная пара проводов. Существует UTP - неэкранированная и STP экранированная витые пары. Гораздо дешевле коаксиального кабеля.



Волоконно-оптический кабель (ОВ)

- **Волоконно-оптический кабель (ОВ)** – состоит из тонких волокон, по которым распространяются световые сигналы.

Радиоканалы

- **Радиоканалы наземной и спутниковой связи** образуются с помощью передатчика и приемника радиоволн: Wi-Fi, WiMAX, 3G, 4G (LTE), Bluetooth, АОЛС.

Взаимные влияния

Взаимные влияния (ВВ) – появление помех в цепи связи в результате перехода сигнала из соседней цепи.

Цепь, из которой переходит сигнал, называется **влияющей цепью.**

Цепь, в которой появляется помеха – **подверженная влиянию.**

Взаимные влияния

Помеха – нежелательный сигнал.

Причина ВВ – асимметрия расстояний между проводниками взаимовлияющих цепей.

- **Условия ВВ:**

- **1)** Наличие внешнего ЭМП.
- **2)** Близость ВВ цепей (находятся в одном кабеле).

Классификация ВВ

- **1)** По способу проникновения в линию связи: **электрическое влияние** (разность потенциалов) и **магнитное влияние** (разность ЭДС).
- **2)** В зависимости от места проявления помехи: **на ближнем конце** и **на дальнем конце.**
- **Ближний конец –** влияющий передатчик и подверженный приёмник находятся на 1 конце линии связи. **Дальний конец –** на разных концах линии связи.

Классификация ВВ

- **3)** В зависимости от времени воздействия: **систематические влияния** и **случайные влияния.**
- **4)** В соответствии с путями перехода помехи: **непосредственные влияния** и **косвенные влияния.** К косвенным влияниям относится:
- **Влияние через третью цепь.**
- **Влияние через ЭМП отраженного сигнала.**

Защита от ВВ

- **Со стороны производителя:**
- Скрутка жил в элементарные группы.
- Чем меньше шаг скрутки, тем меньше влияние помехи (меньше асимметрия кабеля).
- Скрутка приводит к выравниванию расстояний между проводниками ВВ цепей.

Методы доступа к среде передачи данных

- **Метод доступа -** способ определения того, какая из рабочих станций сможет следующей использовать линию связи.
- **Коллизия –** наложение двух и более кадров от станций, пытающихся передать кадры в один и тот же момент времени.
- **Jam-сигнал –** сигнал, который останавливает передачу на всех передатчиках (заглушка).

Принцип работы CSMA/CD

- **CSMA/CD –** *множественный доступ с прослушиванием несущей и разрешением коллизий.*
- **1)** Передатчик прослушивает канал связи и начинает передачу, если канал свободен;
- **2)** В процессе передачи, передатчик продолжает прослушивание канала;
- **3)** В случае коллизии, передатчик останавливает передачу и посылает **jam-сигнал**;

Принцип работы CSMA/CD

- **4)** Приёмник отбрасывает уже частично принятое сообщение, а все передатчики в течение некоторого, случайно выбранного промежутка времени выжидают, прежде чем начать передачу сообщения.

Обнаружение коллизий

- Коллизии могут быть обнаружены сравнением передаваемой и получаемой информации. Если она различается, то другая передача накладывается на текущую (возникла коллизия) и передача прерывается немедленно. Посылается **jam signal**, что вызывает задержку передачи всех передатчиков на произвольный интервал времени, снижая вероятность коллизии во время повторной попытки.

Принцип работы CSMA/CA

- **CSMA/CA** – *метод множественного доступа с прослушиванием несущей частоты и избеганием коллизий.*
- **1)** Станция, которая собирается начать передачу, посылает **jam-сигнал**;
- **2)** После продолжительного ожидания всех станций, которые могут послать **jam-сигнал**, станция начинает передачу фрейма;

Принцип работы CSMA/CA

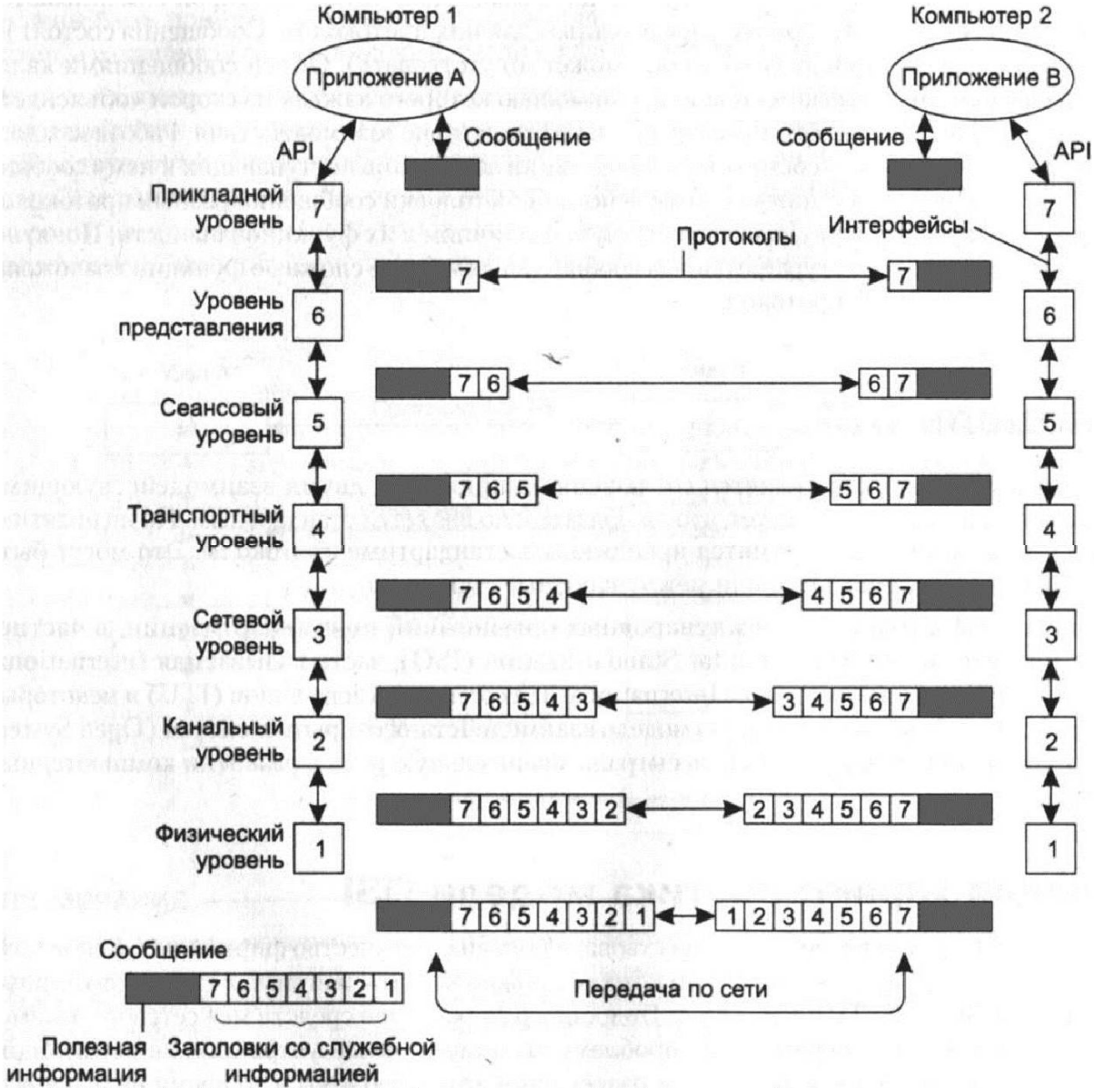
- **3)** Если во время передачи станция обнаруживает **jam-сигнал** от другой станции, она останавливает передачу на отрезок времени случайной длины и затем повторяет попытку.
- **CSMA/CA** отличается от **CSMA/CD** тем, что коллизиям подвержены не пакеты данных, а только **jam-сигналы**.
-

Принцип работы ТРМА (Token Ring)

- **ТРМА (Token Ring) –** *множественный доступ с передачей полномочия или метод с передачей маркера*.
- Это метод доступа к среде, в котором от рабочей станции к рабочей станции передается маркер, дающий разрешение на передачу сообщения.
-

Сетевая модель OSI

- **Модель OSI (Open System Interconnection)** – разработка 80-х годов ряда международных организаций ISO и ITU-T, под названием *модель взаимодействия открытых систем*.


Компьютер 1
Компьютер 2
Приложение А
Приложение В
API
Сообщение
Сообщение
API
Прикладной уровень
Уровень представления
Сеансовый уровень
Транспортный уровень
Сетевой уровень
Канальный уровень
Физический уровень
Протоколы
Интерфейсы
7
6
5
4
3
2
1
7
7
7 6
6 7
7 6 5
5 6 7
7 6 5 4
4 5 6 7
7 6 5 4 3
3 4 5 6 7
7 6 5 4 3 2
2 3 4 5 6 7
7 6 5 4 3 2 1
1 2 3 4 5 6 7
Сообщение
7 6 5 4 3 2 1
Передача по сети
Полезная информация
Заголовки со служебной информацией

- **Физический уровень** имеет дело с передачей данных по физическим каналам связи, таким, например, как коаксиальный кабель, витая пара или оптоволоконный кабель.

- **Канальный уровень** обеспечивает прозрачность соединения для сетевого уровня. Для этого он предлагает ему следующие услуги:
- установление логического соединения между взаимодействующими устройствами;
- согласование скоростей передатчика и приемника;
- обеспечение надежности передачи, обнаружение и коррекция ошибок.

- **Сетевой уровень** служит для образования единой транспортной системы, объединяющей несколько сетей, называемой составной сетью (интернетом).
- Одной из важнейших задач сетевого уровня является определение маршрута (маршрутизация).

Транспортный уровень обеспечивает приложениям или верхним уровням стека – прикладному и сеансовому – передачу данных с той степенью надежности, которая им требуется.

TCP, UDP стека TCP/IP.

- **Сеансовый уровень** обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации.
- Используется редко. Чаще всего объединен с прикладным уровнем.

Уровень представления обеспечивает представление передаваемой по сети информации, не меняя при этом ее содержания.

- **Прикладной уровень** — это просто набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры и т.п.

Популярные стеки протоколов

Модель OSI	IBM/Microsoft	TCP/IP	Novell
Прикладной	SMB	Telnet, FTP, SMTP, HTTP	NCP, SAP
Представления			
Сеансовый	NetBIOS	TCP	
Транспортный			SPX
Сетевой		IP, RIP, OSPF	IPX, RIP, **PEP**
Канальный	802.3 (Ethernet), 802.5 (Token Ring), FDDI, ATM, PPP		
Физический	Коаксиальный кабель, экранированная и неэкранированная витая пара, оптоволокно, радиодиапазоны		

- **Стек протоколов TCP/IP** - согласованный набор сетевых протоколов, обеспечивающий взаимодействие узлов в разновидных сетях.

Задачи TCP/IP:

- Согласование использования адресов различного типа;
- Обеспечение уникальности адресов;
- Конфигурирование сетевых интерфейсов и сетевых приложений

Уровни модели OSI		Протоколы группы TCP/IP	Уровни стека TCP/IP	
7	Прикладной	Telnet, FTP, SMTP, HTTP, POP3, IMAP, SMB	Прикладной	I
6	Представления			
5	Сеансовый	TCP, UDP	Транспортный	II
4	Транспортный			
3	Сетевой	IP, ICMP, RIP, ARP	Межсетевого взаимодействия	III
2	Канальный	Ethernet, Token Ring, PPP, FDDI и т.д.	Сетевых интерфейсов	IV
1	Физический			

TCP (Transmission Control Protocol) – предназначен для управления передачей данных в сетях и подсетях.

IP (Internet Protocol) – маршрутизируемый протокол сетевого уровня стека TCP/IP.

UDP (User Datagram Protocol) – использует простую модель передачи без обеспечения надёжности, упорядочивания или целостности данных.

HTTP (HyperText Transfer Protocol) – протокол прикладного уровня передачи данных (вида гипертекстовых документов).

SMTP (Simple Mail Transfer Protocol) – широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

POP (Post Office Protocol) – стандартный Интернет-протокол прикладного уровня, используемый клиентами электронной почты для извлечения электронного сообщения с удалённого сервера.

IMAP (Internet Message Access Protocol) – протокол прикладного уровня для доступа к электронной почты.

Получает доступ к хранилищу корреспонденции на сервере так, как будто эта корреспонденция расположена на компьютере получателя.

FTP (File Transfer Protocol) – стандартный протокол, предназначенный для передачи файлов по TCP-сетям.

SMB (Server Message Block) - сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия.

ARP (Address Resolution Protocol) - протокол сетевого уровня, предназначенный для определения MAC-адреса по известному IP-адресу.

IPX/SPX (Novell)

<table>
<tr><td>Уровни OSI</td><td rowspan="5">SAP

(Service Advertisement Protocol)</td><td rowspan="5">NCP

(NetWare Core Protocol)</td><td rowspan="4"></td></tr>
<tr><td>Прикладной</td></tr>
<tr><td>Представитель

Ный</td></tr>
<tr><td>Сеансовый</td></tr>
<tr><td>Транспортный</td><td>SPX</td></tr>
<tr><td>Сетевой</td><td colspan="3">IPX , RIP , NLSP</td></tr>
<tr><td>Канальный</td><td colspan="3" rowspan="2">Ethernet , FDDI , TokenRing

Fast Ethernet , ATM , 100VG-AnyLAN</td></tr>
<tr><td>Физический</td></tr>
</table>

IPX/SPX - протоколы сетевого и сеансового уровней, работающих на основе ОС Novell NetWare.

Применяется в основном в небольших локальных сетях, состоящих из ПК со скромными ресурсами.

IPX - протокол межсетевого обмена пакетами.

IPX выполняет функции адресации, маршрутизации и переадресации в процессе передачи пакетов сообщений.

IPX не гарантирует доставку и не корректирует ошибки.

SPX - протокол последовательного обмена пакетами, обеспечивает надёжность передачи данных.

PEP - протокол обмена пакетами. Используется исключительно для доставки команд протокола NCP.

NCP - основной протокол верхнего уровня.

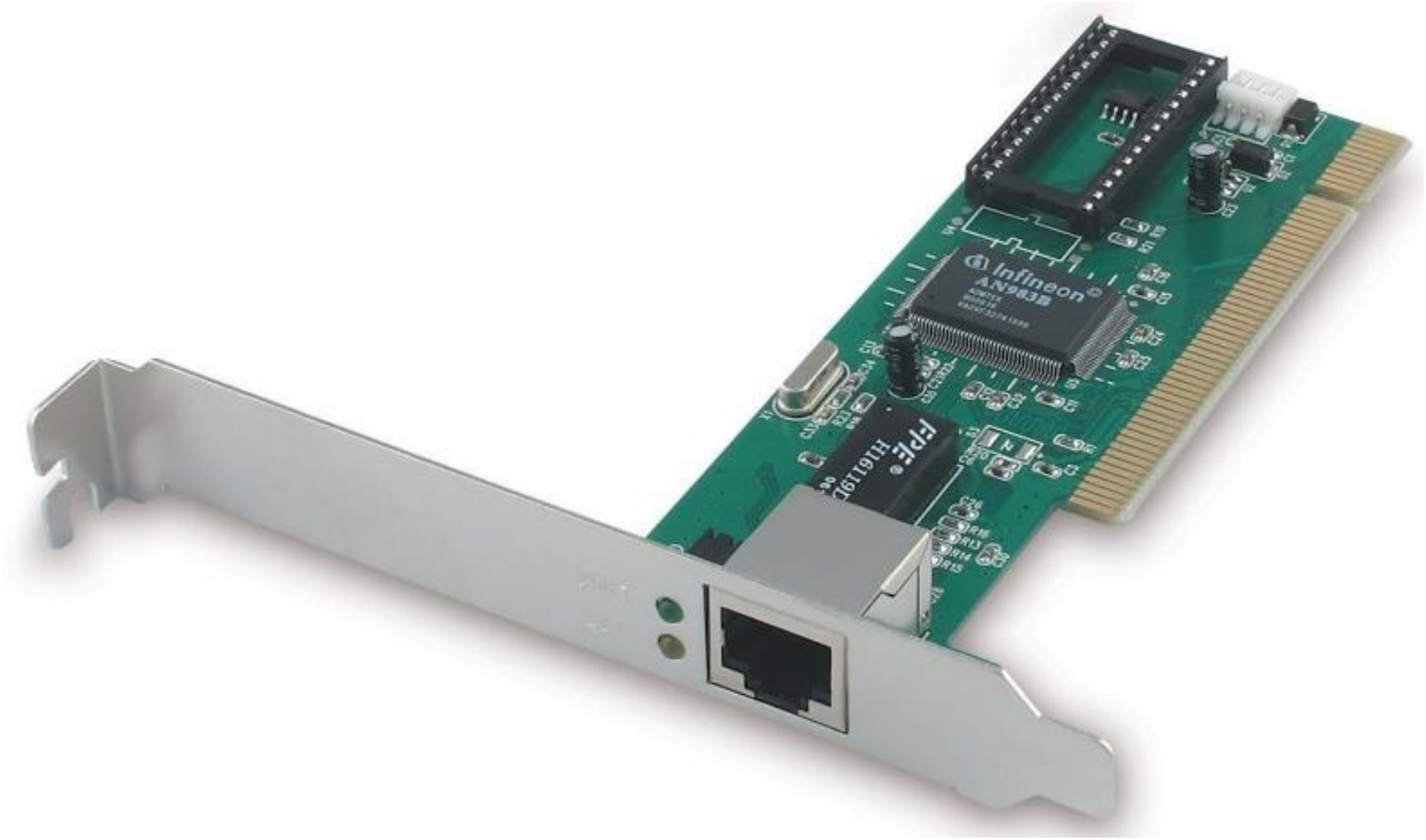
Он обеспечивает работу основных служб сетевой ОС и объединяет функции всех уровней от транспортного до прикладного модели OSI.

SAP – протокол оповещения о сервисах. Используется при широковещательных сообщениях. SAP передает информацию о запрашиваемых сетевых устройствах и ресурсах.

RIP – протокол маршрутной информации. Маршрутизирует IPX-пакеты в другие удаленные подсети.

Коммуникационное оборудование сетей

Сетевые адаптеры



Сетевые адаптеры (сетевые карты) – NIC (Network Interface Controller) – устройство, используемое для обеспечения сетевых подключений.

Функции NIC: Передаёт сигналы на физическом уровне и доставляет пакеты данных на сетевом уровне. Выступает в качестве посредника между компьютером/сервером и сетью передачи данных.

Классификация NIC

1. **На основе сетевых подключений:** проводные и беспроводные.
2. **На основе интерфейсов:**
   a) **ISA (Industry Standard Architecture) -** разработана в 1981 году, скорость 9 Мбит/с. Не используется.
   b) **PCI (Peripheral Component Interconnect)** – разработана в 1990 году. Бывает 32-битная и 64-битная (133 Мбит/с и 266 Мбит/с соответственно). Тоже не используется.

Классификация NIC

2. **На основе интерфейсов:**

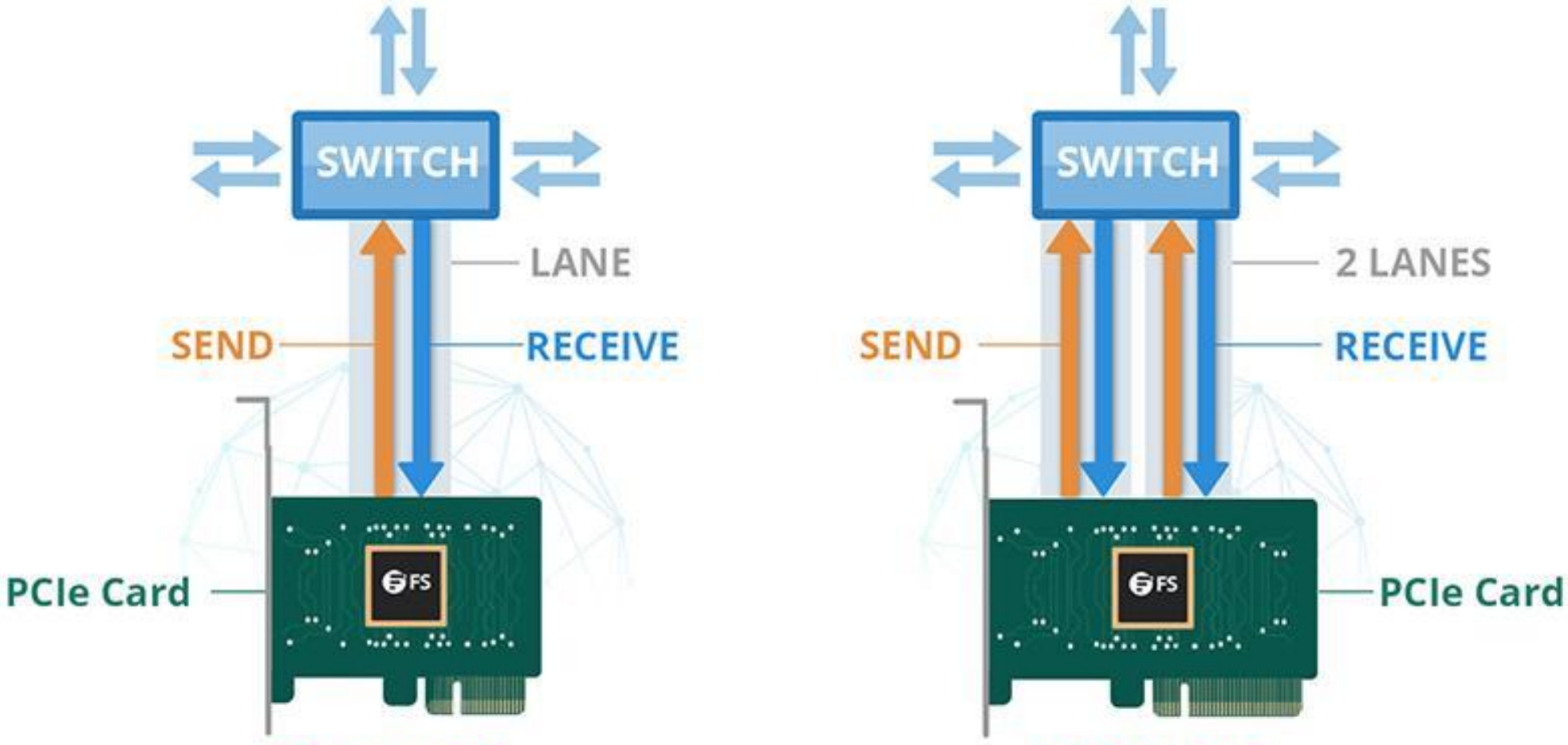
c) **PCI-X (Peripheral Component Interconnect eXtended)** – усовершенствованный вид PCI. 64-битный, скорость до 1064 Мбит/с.

d) **PCIe (Peripheral Component Interconnect Express)** – новейший стандарт. Устанавливается на материнских платах компьютеров и серверов. Существует 5 версий PCIe.

Версии PCIe

Версия PCIe	Код линии	x1	x2	x4	x8	x16
1.0	8b/10b	250MB/s	0.50GB/s	1.0GB/s	2.0GB/s	4.0GB/s
2.0	8b/10b	500MB/s	1.0GB/s	2.0GB/s	4.0GB/s	8.0GB/s
3.0	128b/130b	984.6MB/s	1.97GB/s	3.94GB/s	7.88GB/s	15.8GB/s
4.0	128b/130b	1969MB/s	3.94GB/s	7.88GB/s	15.75GB/s	31.5GB/s
5.0	128b/130b	3938MB/s	6.15GB/s	12.3GB/s	24.6GB/s	63.02GB/s

PCI EXPRESS
LINKS AND LANES



X1 LINK

X2 LINK

Классификация NIC

2. **На основе интерфейсов:**

e) **USB (Universal Serial Bus)** – внешний адаптер. Имеет 3 версии с разной скоростью. Простое подключение и высокая совместимость со многими устройствами.

Классификация NIC

3. **На основе типа портов:**

RJ-45 (Ethernet),

AUI (коаксиальный кабель),

BNC (тонкий коаксиальный кабель)

оптический порт для модуля (10G/25G модуль).

Классификация NIC

4. **На основе скорости передачи:**

10 Мбит/с,

100 Мбит/с,

10/100 Мбит/с,

1000 Мбит/с,

10 Гбит/с, 25 Гбит/с

Классификация NIC

5. На основе области применения:

- **В компьютерах:** большинство компьютеров имеют встроенную сетевую плату, как правило 10/100 Мбит/с или 1 Гбит/с.

- **В серверах:** отличается более высокой скоростью передачи данных, например 10G, 25G, 40G или 100G. Серверные NIC имеют низкую загрузку CPU, потому что у них есть специальный сетевой контроллер, который может выполнять многие задачи CPU.

Концентраторы

Концентратор

Концентратор (Hub) – один из видов сетевых устройств, предназначенных для организации компьютерной сети.

Концентратор принимает входящее сообщение на каком-либо порту и передаёт его на все остальные порты.

Сетевой мост

Сетевой мост

Сетевой мост (Network Bridge) – сетевое устройство, предназначенное для объединения сегментов сети передачи данных в единую сеть.

Маршрутизатор

Маршрутизатор

Маршрутизатор (Router) – сетевое устройство, которое пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации.

Маршрутизатор может связывать разнородные сети различных архитектур.

Коммутатор

Коммутатор

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

Шлюз

AddPac
AP2370D
AP-CPU
RESET
RUN/PWR
CONSOLE
LAN1
LAN0
PHONE
HS
AP-N1-FXS8
CPU
(E1 SLOT)

Шлюз

Шлюз (Gateway) – сетевой шлюз конвертирует протоколы одного типа физической среды в протоколы другой физической среды (сети).

Домашнее задание

Изучить принцип работы концентратора, коммутатора и маршрутизатора.

Расписать основные отличия.

Протоколы динамической маршрутизации

OSPF (Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути *алгоритм Дейкстры*.

OSPF

Distance-Vector – роутер узнает информацию о маршрутах посредством других роутеров, подключенных в один сегмент сети.

OSPF

Link-State – каждый роутер знает лучшие маршруты во все удалённые сети, а также имеет в памяти полную карту сети со всеми существующими связями.

Это достигается за счет построения специальной базы ***LSDB (Link-State Data Base)***

Принцип работы OSPF

1. После включения маршрутизаторов протокол ищет непосредственно подключенных соседей и устанавливает с ними «дружеские» отношения.

Принцип работы OSPF

2. Затем они обмениваются друг с другом информацией о подключенных и доступных им сетях. (Строят карту сети)

Принцип работы OSPF

3. На основе полученной информации запускается алгоритм **SPF (Shortest Path First «Выбор наилучшего пути»)**, который рассчитывает оптимальный маршрут к каждой сети.

Домашнее задание

Расписать типы сообщений, используемых в OSPF (Hello, DBD, LSR, LSU, LSAck).

EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) протокол маршрутизации, разработанный фирмой Cisco. EIGRP использует механизм DUAL (Diffusing Update Algorithm) для выбора наиболее короткого маршрута.

Преимущества EIGRP – высокий показатель масштабируемости и высокая скорость сходимости сети. Более простая реализация и меньше требований к вычислительным ресурсам.

Принцип работы EIGRP

1. Обнаружение соседних устройств;

2. Обнаружение маршрутов;

3. Выбор маршрутов;

4. Сопровождение маршрутов (DUAL).

Недостаток EIGRP

Работает только с сетевым оборудованием компании Cisco.

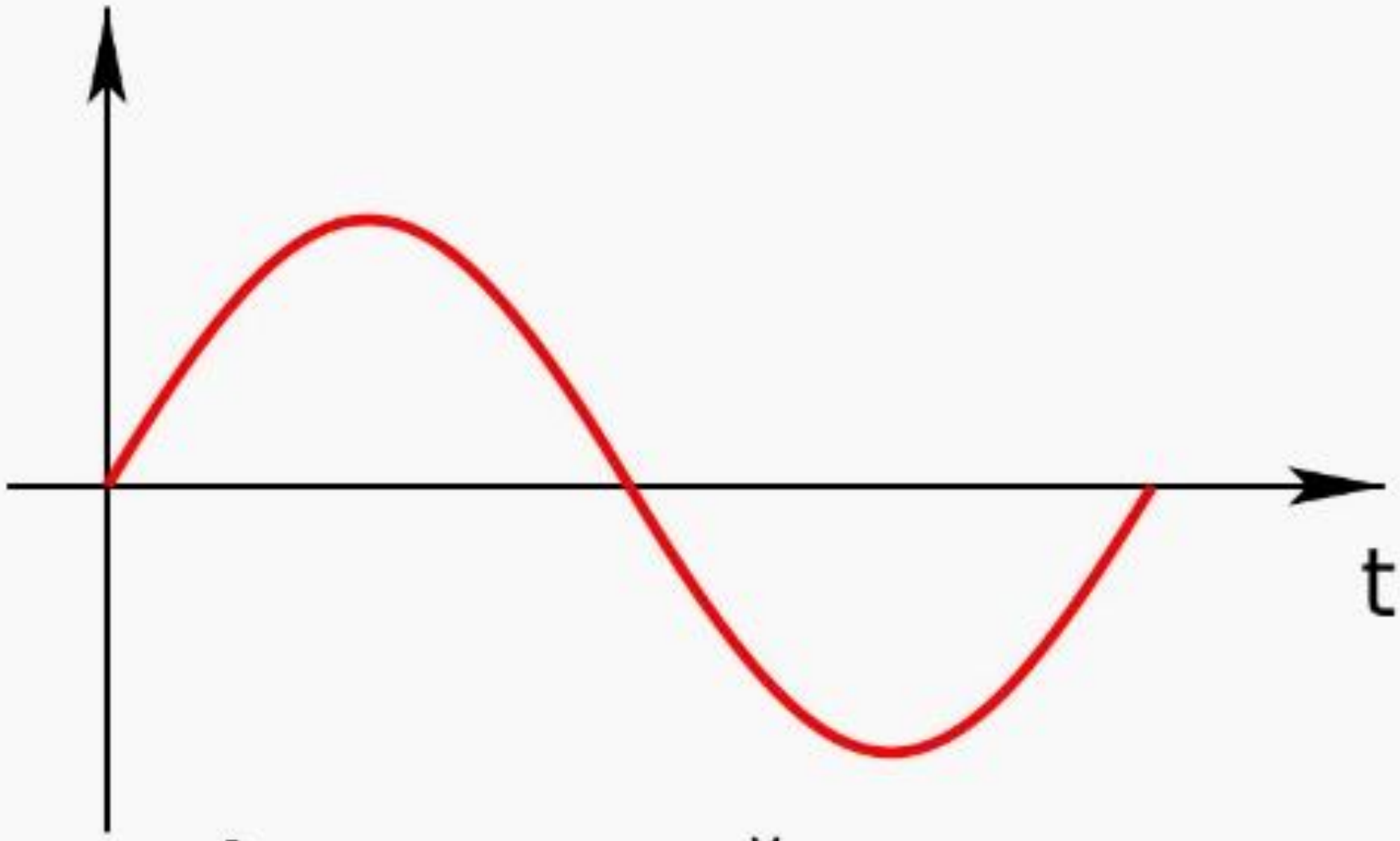
Основы передачи данных

Информация – совокупность сведений о каких-либо событиях, явлениях или предметах, предназначенных для передачи, приёма, обработки, преобразования или хранения.

Сигнал – некоторый физический процесс, параметры которого изменяются в соответствии с передаваемым сообщением (материальный носитель информации).

Аналоговый (синусоидальный) сигнал описывается непрерывной функцией времени, т.е. имеет непрерывную линию с непрерывным множеством возможных значений

Основы передачи данных



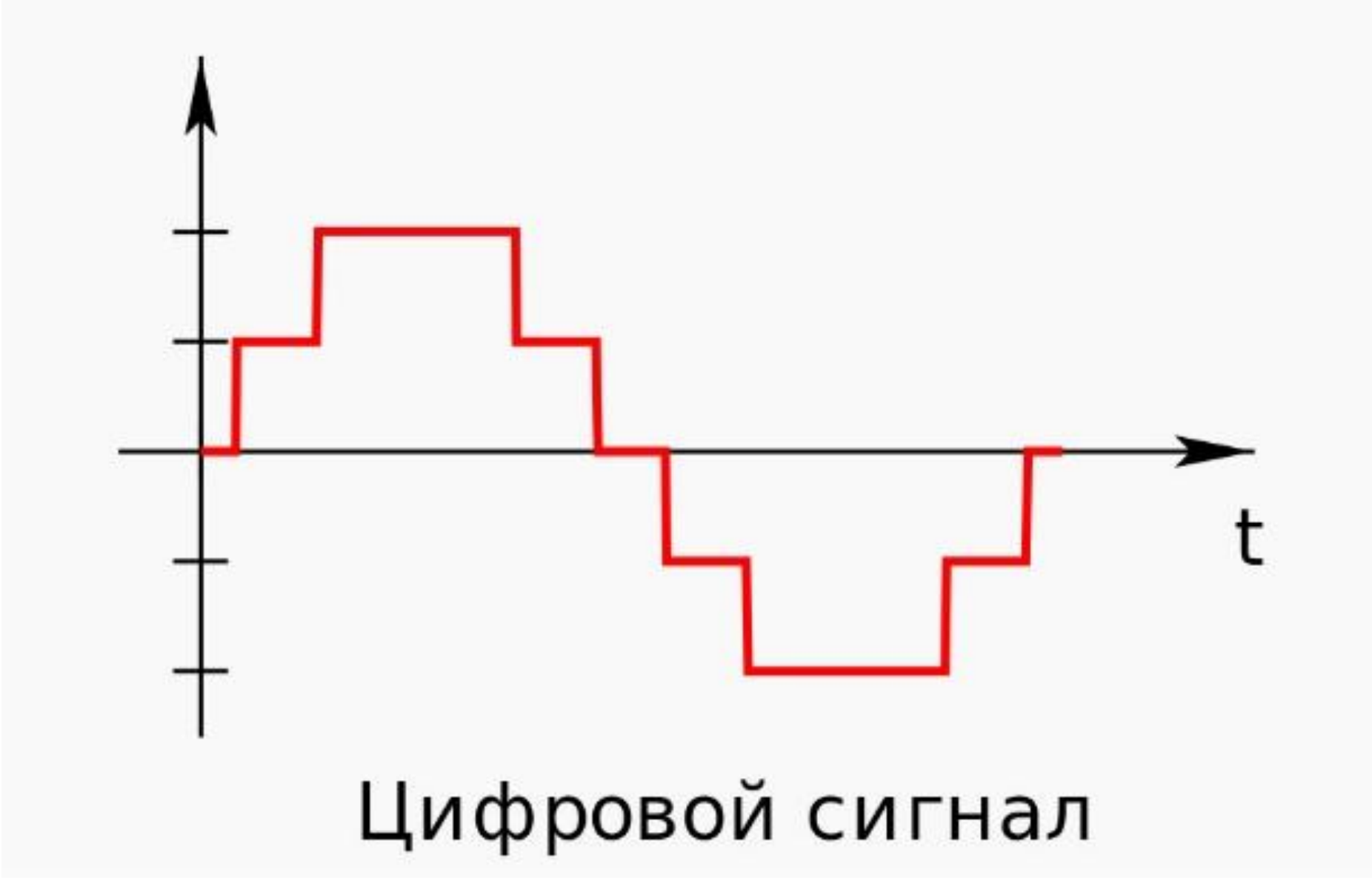
Аналоговый сигнал

Основы передачи данных

Цифровой сигнал — это сигнал, который можно представить как последовательность определенных цифровых значений. В любой момент времени он может принимать только одно определенное конечное значение

Аналоговый сигнал преобразуется в цифровой с помощью двух процессов - **дискретизация** и **квантование.**

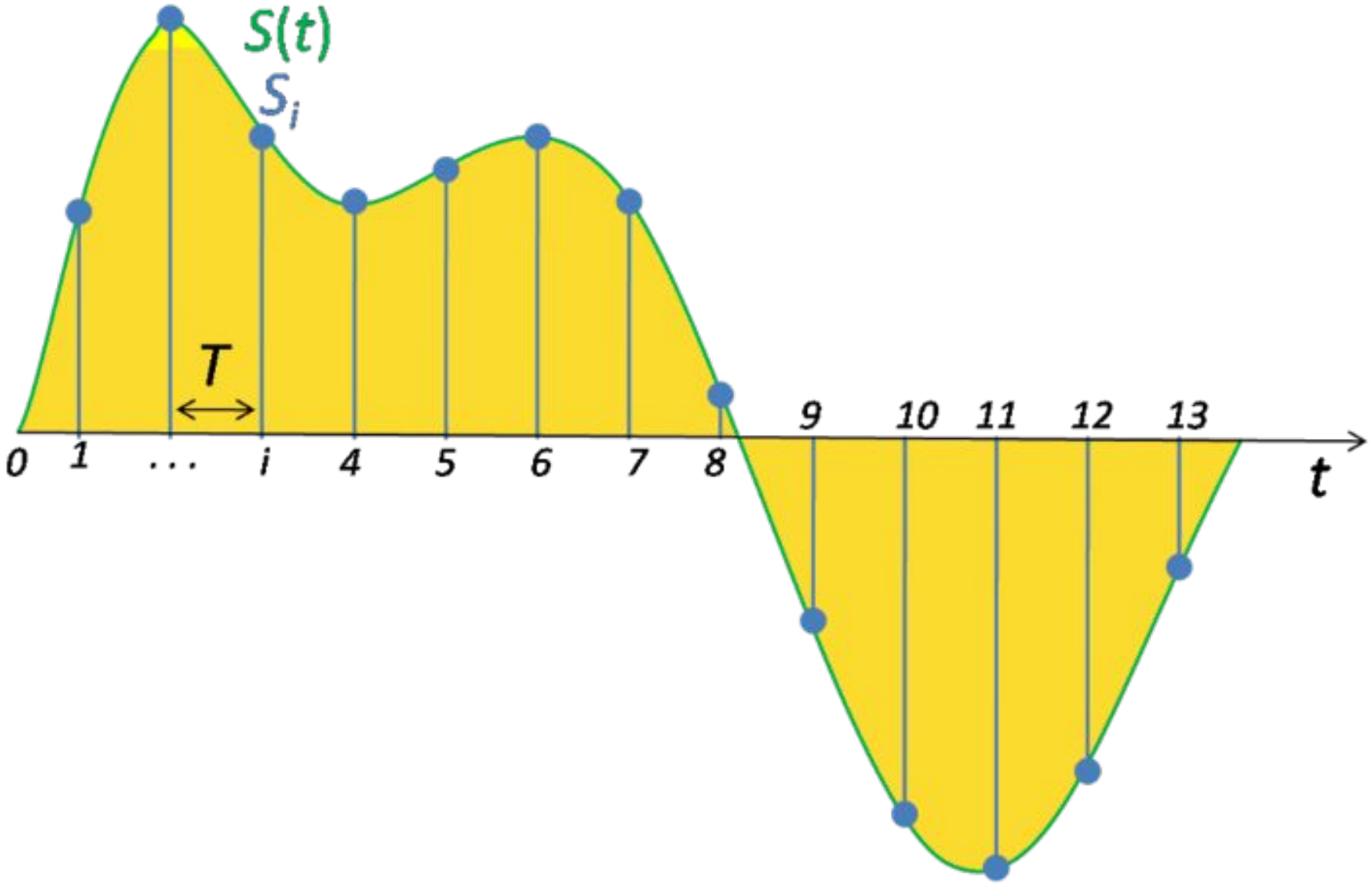
Основы передачи данных



Основы передачи данных

Дискретизацией называется процесс регистрации (измерения) значения сигнала через определенные промежутки (обычно равные) времени

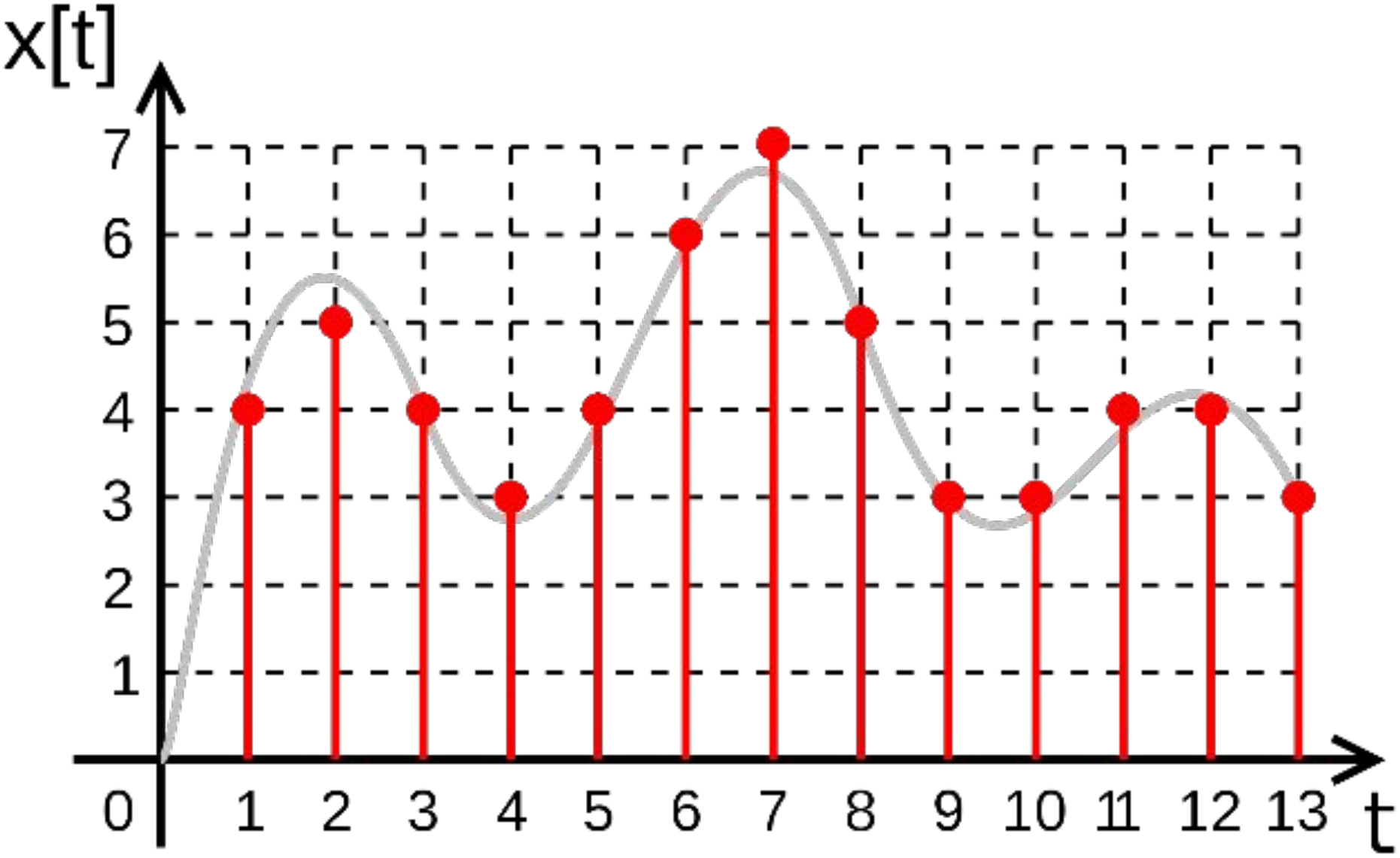
Основы передачи данных



Основы передачи данных

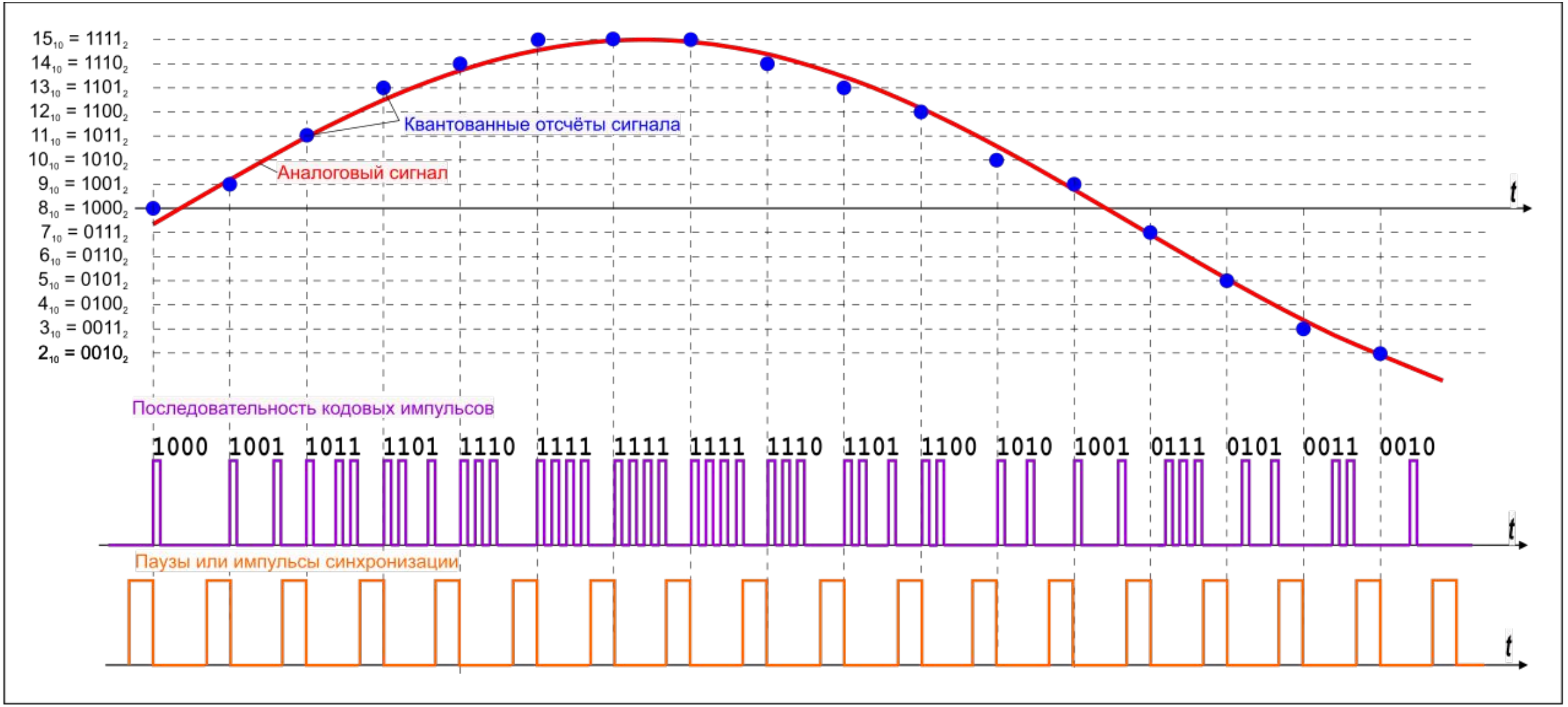
Квантование — это процесс разбиения диапазона амплитуды сигнала на определенное количество уровней и округление значений, измеренных во время дискретизации, до ближайшего уровня

Основы передачи данных



Основы передачи данных

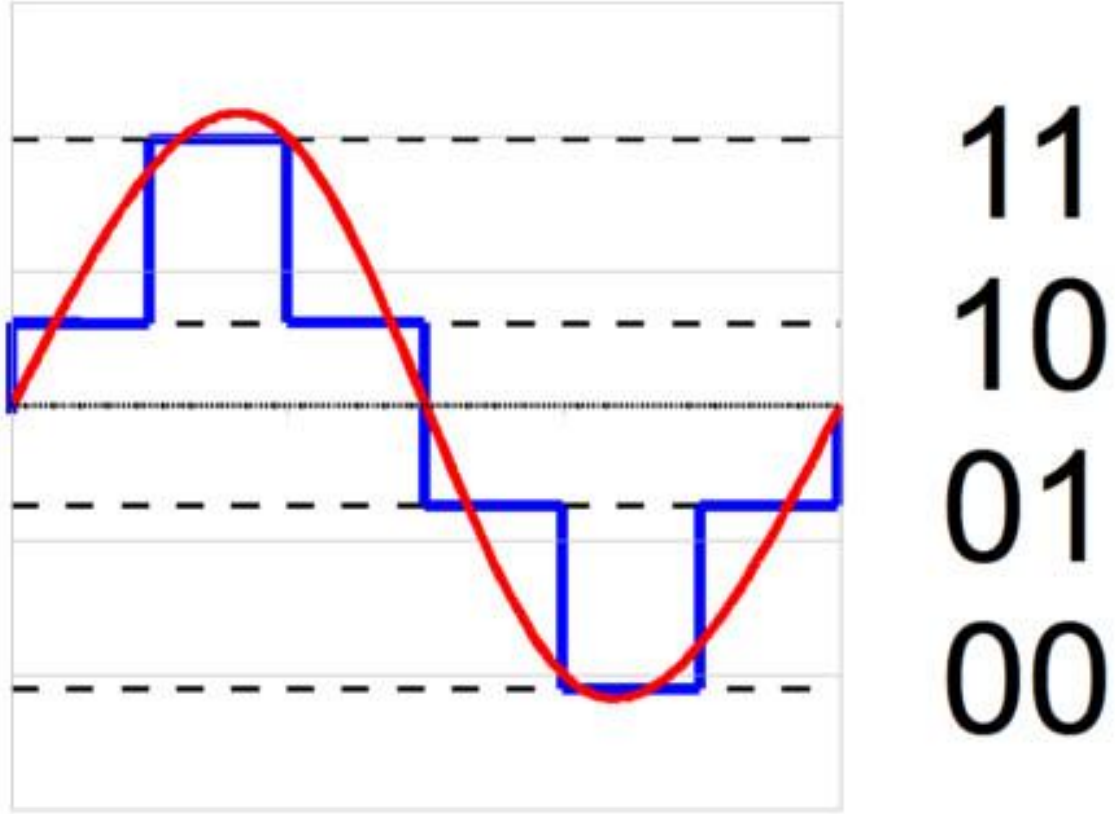
Основы передачи данных

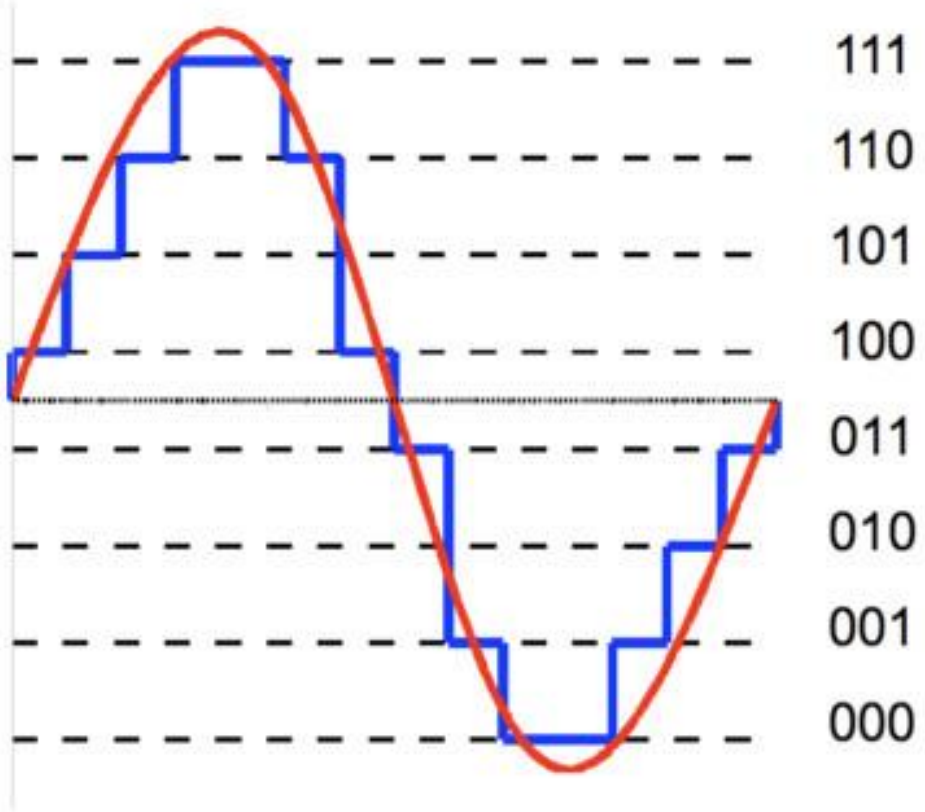


Основы передачи данных

Количество битов, которые присваиваются каждому уровню квантования называют **разрядностью** или **глубиной квантования**. Чем выше разрядность, тем больше уровней можно представить двоичным кодом

Основы передачи данных





Основы передачи данных

- Данная формула позволяет вычислить количество уровней квантования:

Если N — количество уровней квантования,
n — разрядность, то

$$N=2^n$$

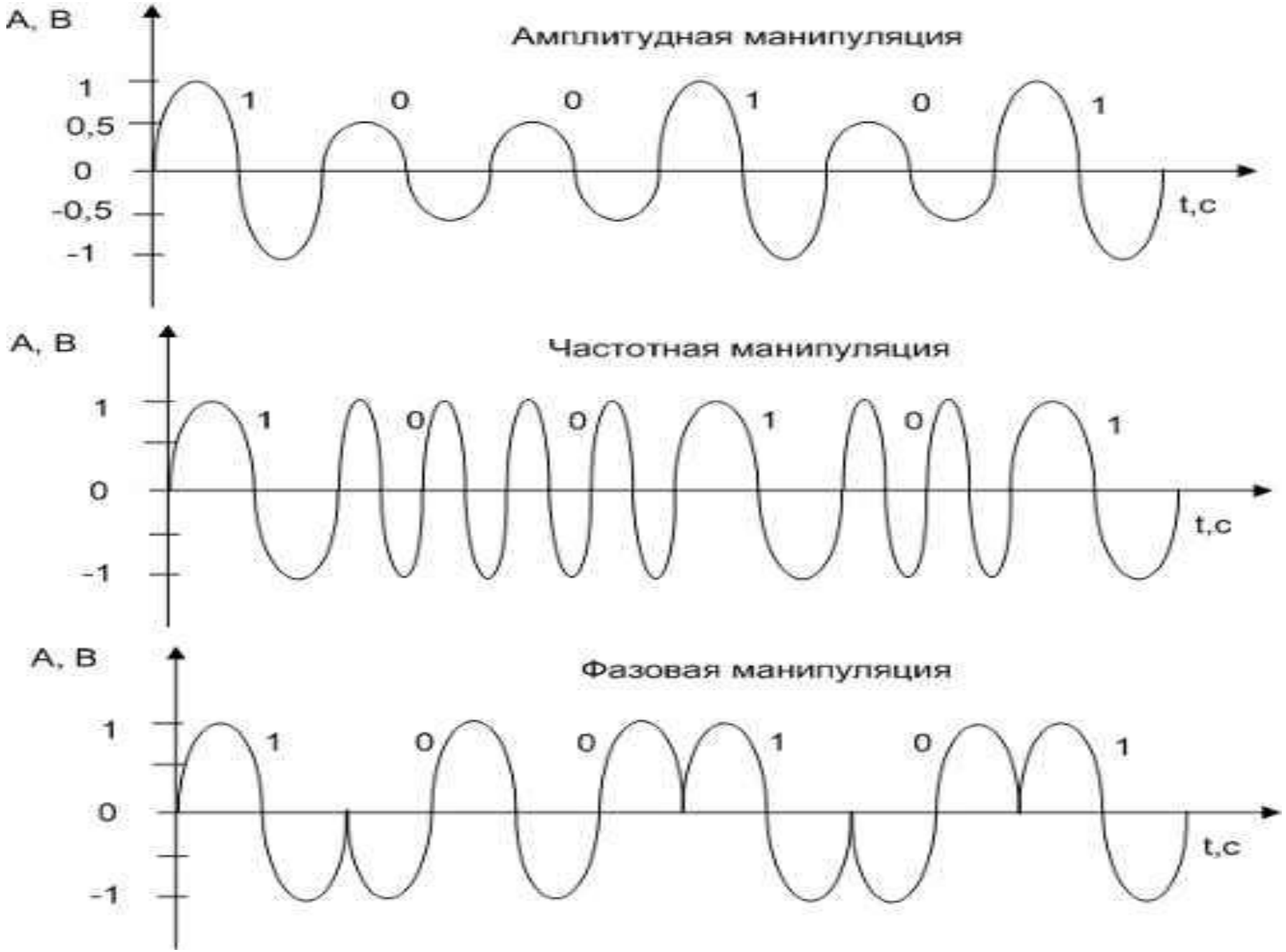
Основы передачи данных

Чтобы аналоговый сигнал можно было преобразовать обратно из цифрового сигнала, нужно следовать **теореме Котельникова** (теорема Найквиста — Шеннона).

Если аналоговый сигнал имеет ограниченной по ширине спектр, то он может быть восстановлен однозначно и без потерь по своим дискретным отсчетам, взятым с частотой, строго большей удвоенной верхней частоты.

Основы передачи данных

Модуляция – процесс передачи высокочастотного сигнала по закону низкочастотного сигнала


Амплитудная манипуляция
A, B
1
0,5
0
-0,5
-1
1
0
0
1
0
1
t,c
Частотная манипуляция
A, B
1
0
-1
1
0
0
1
0
1
t,c
Фазовая манипуляция
A, B
1
0
-1
1
0
0
1
0
1
t,c

Амплитудная модуляция

Имеет низкую помехозащищённость.

Применяется в основном для радиовещания, передачи изображения в телевизионном вещании, а также в гражданской авиации.

Частотная модуляция

Имеет высокую помехозащищенность.

Применяется для высококачественной передачи звукового сигнала (в радиовещании и телевизионном вещании).

Фазовая модуляция

Фазовая модуляция активно используется для формирования помехозащищенной связи в УКВ диапазоне.

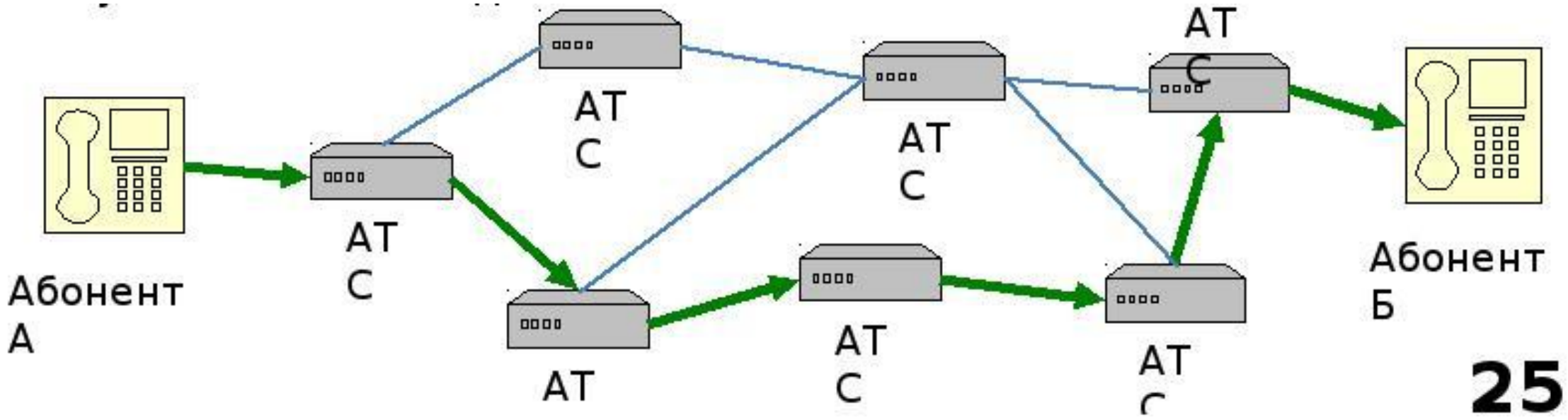
Основы передачи данных

Коммутация — процесс соединения абонентов коммуникационной сети через транзитные узлы.

Виды коммутации

Коммутация каналов (circuit switching) — способ коммутации, при котором обеспечивается временное соединение каналов на различных участках сети для образования прямого канала между любой парой абонентских пунктов этой сети.

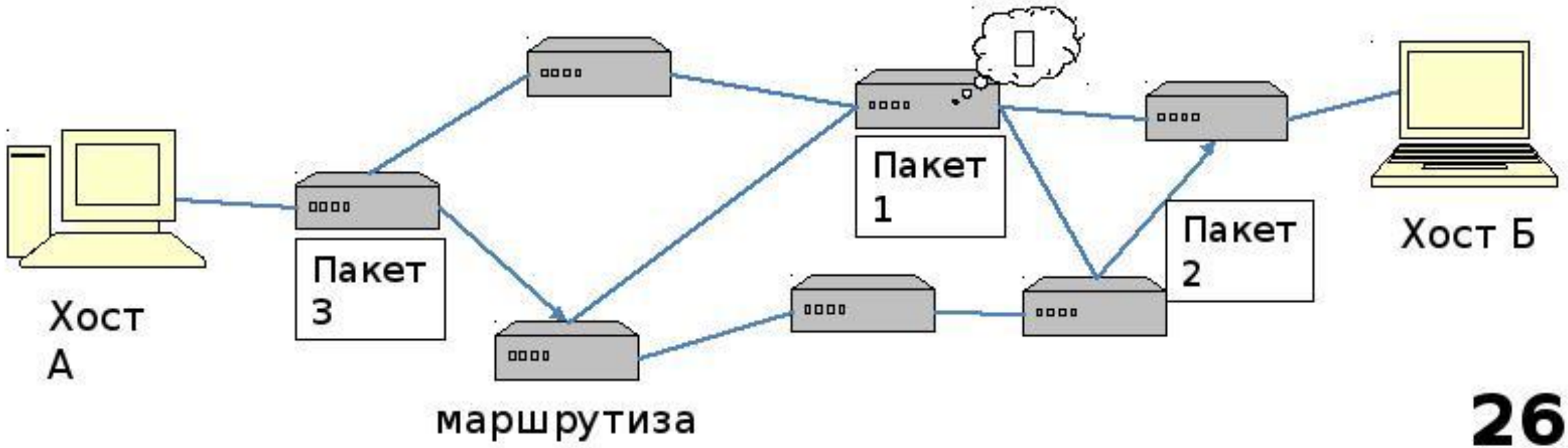
Коммутация каналов



Виды коммутации

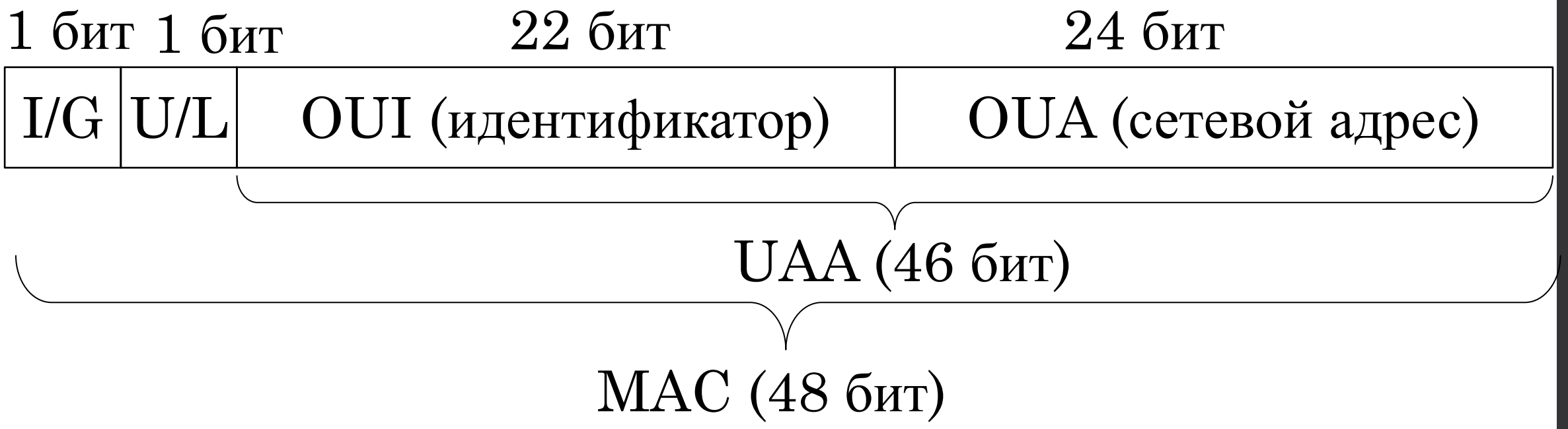
Коммутация пакетов (packet switch) – между абонентами не создается постоянное соединение. Данные передаются частями (пакетами), каждый из которых доставляется независимо от других.

Коммутация пакетов



MAC-адрес

Каждое сетевое устройство имеет индивидуальный уникальный **MAC-адрес (Media Access Control)**, назначаемый производителем («вшитый»).



MAC-адрес

OUI (Organizationally Unique Identifier) – уникальный идентификатор организации.

OUA (Organizationally Unique Address) – уникальный адрес сетевого адаптера.

UAA (Universally Administered Address) – универсальный администрируемый адрес.

MAC-адрес

I/G (Individual/Group) – указывает на тип адреса: если 0 – индивидуальный, 1 – групповой. Пакеты с групповым адресом получат все имеющие этот групповой адрес сетевые адаптеры.

U/L (Universal/Local) - Обычно он установлен 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого адаптера, а организацией, использующей данную сеть.

IP-адресация

Основная задача – обеспечить глобальную связь между всеми устройствами.

К IP-адресу предъявляются следующие требования:

- Уникальность адреса;
- Иерархичность;
- Удобство представления.

IPv4

IPv4 состоит из 4 байт. Максимальное число адресов $2^{32} \approx 4{,}3$ млрд.

На самом деле используется гораздо меньше из-за наличия зарезервированных диапазонов IP-адресов.

Способы представления IPv4

Двоичный:

10010001 11011101 01010101 10010100

Десятичный с точками:

145.221.85.148

Шестнадцатеричный:

0x91dd5594

Неправильные IPv4

1) 111.56.045.78

2) 221.34.7.8.20

3) 75.45.301.14

Классы IPv4

IP-адрес состоит из двух логических частей – номера подсети (NetID) и номера узла (HostID).

Определение того, какая часть адреса отводится под номер подсети, осуществляется двумя способами − с помощью **классов** и с помощью **масок**.

Классы IPv4

Всего существует пять классов, основными являются классы A, B и C.

Они отличаются друг от друга размерами и сложностью.

Классы определяют сколько бит в IP-адресе отводится под номер сети и сколько под номер узла.

Класс А

Класс А имеет адреса, которые начинаются в диапазоне от 1 до 127 для первого октета, а остальная часть адреса – это адрес узла.

Класс А допускает максимум 126 сетей, а в каждой из них **до 16 777 214 компьютеров**.

Как правило, это сети огромных компаний, которых в мире немного, объединяющих большое число сетевых устройств.

Класс B

Класс B для описания адреса сети использует первые два октета, а остальная часть – это адреса узлов.

Первый октет принимает значения от 128 до 191, что дает максимум 16 384 сети, в каждой из которых до **65 534** компьютеров.

Адреса класса B назначаются сетям большого и среднего размера.

Класс С

Класс С начинается из диапазона от 192 до 223 и используют три первых октета для описания адреса сети. Последний октет обозначает адрес узла.

Класс С допускает максимум 2 097 152 сети по 254 компьютера в каждой.

Адреса этого класса назначают малым сетям.

Класс D

Класс D представляет собой групповые адреса и назначается группам узлов.

Это используется некоторыми сетевыми службами для **многоадресной рассылки.**

Многоадресная рассылка (Multicast) – один отправитель, много получателей (например IPTV).

Класс E

Диапазон адресов **класса E** зарезервирован и в настоящее время не используется.

240.0.0.0 – 255.255.255.255

Эти адреса зарезервированы для будущих дополнений в схеме адресации IP.

IP-адресация в локальных сетях

В пределах одной локальной сети каждый компьютер должен обладать уникальным адресом.

Этот адрес должен входить в один из определённых диапазонов частных сетевых адресов:

10.0.0.0 - 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

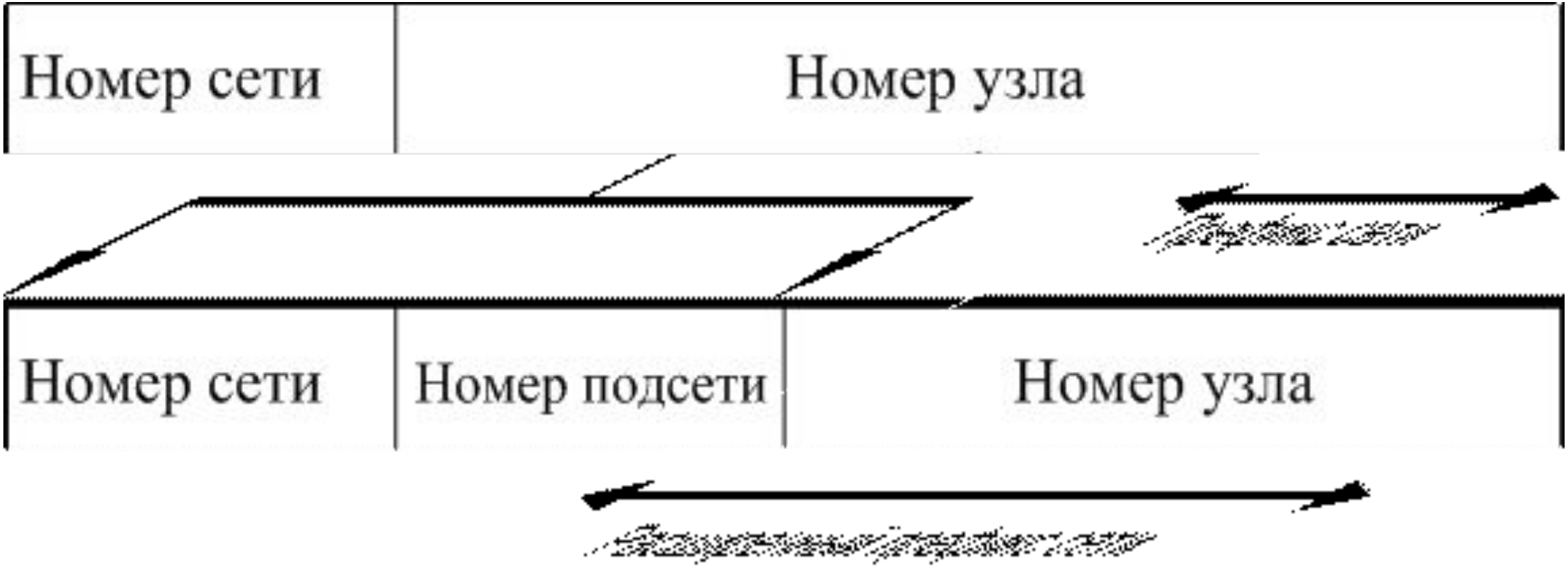
Маски подсети

Стандартная схема разбиения пула адресов на классы порождает ряд проблем, например:

- Резкий рост таблиц маршрутизации в Интернете;
- Нерациональной использование адресного пространства.

Для решения данных проблем был введён дополнительный уровень иерархии структуры IP-адреса: к номерам сети и хоста добавляется номер подсети

Маски подсети



Маски подсети

Расширенный сетевой префикс – поля номеров сети и подсети.

Для выделения расширенного сетевого префикса используется маска подсети (subnet mask).

Маска подсети – это 32-разрядное двоичное число (как IP-адрес), в разрядах расширенного префикса содержит «1», в остальных разрядах «0».

Бесклассовая адресация

CIDR (Classless Inter-Domain Routing) – метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации.

VLSM (Variable Length Subnet Mask) – переменная длина маски подсети (динамическая маска). Длина обычной маски могла принимать только 3 значения.

Бесклассовая адресация

IP: 201.164.80.35 **Маска**: 255.255.224.0

11001001 10100100 01010000 00100011

11111111 11111111 11100000 00000000

11001001 10100100 01000000 00000000

Полученный IP подсети: 201.164.64.0/19

Полученные IP хостов (8190 шт.):

201.164.64.1 – 201.164.95.254

IPv6

Состоит из 16 байт. Максимальное число адресов: $2^{128} = 3{,}4*10^{38}$.

Способы представления:

Шестнадцатеричная:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Сжатая форма:

1080::8:800:200C:417A

Смешанная форма:

::D:1:0.68.0.3

IPv6

Состоит из 16 байт. Максимальное число адресов: $2^{128} = 3{,}4*10^{38}$.

Способы представления:

Шестнадцатеричная:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Сжатая форма:

1080::8:800:200C:417A

Смешанная форма:

::D:1:0.68.0.3

Преимущества IPv6 над IPv4

- В сверхскоростных сетях возможна поддержка огромных пакетов (джамбограмм) – до 4 Гб.
- Появились метки потоков и классы трафика.
- Появилось многоадресное вещание.

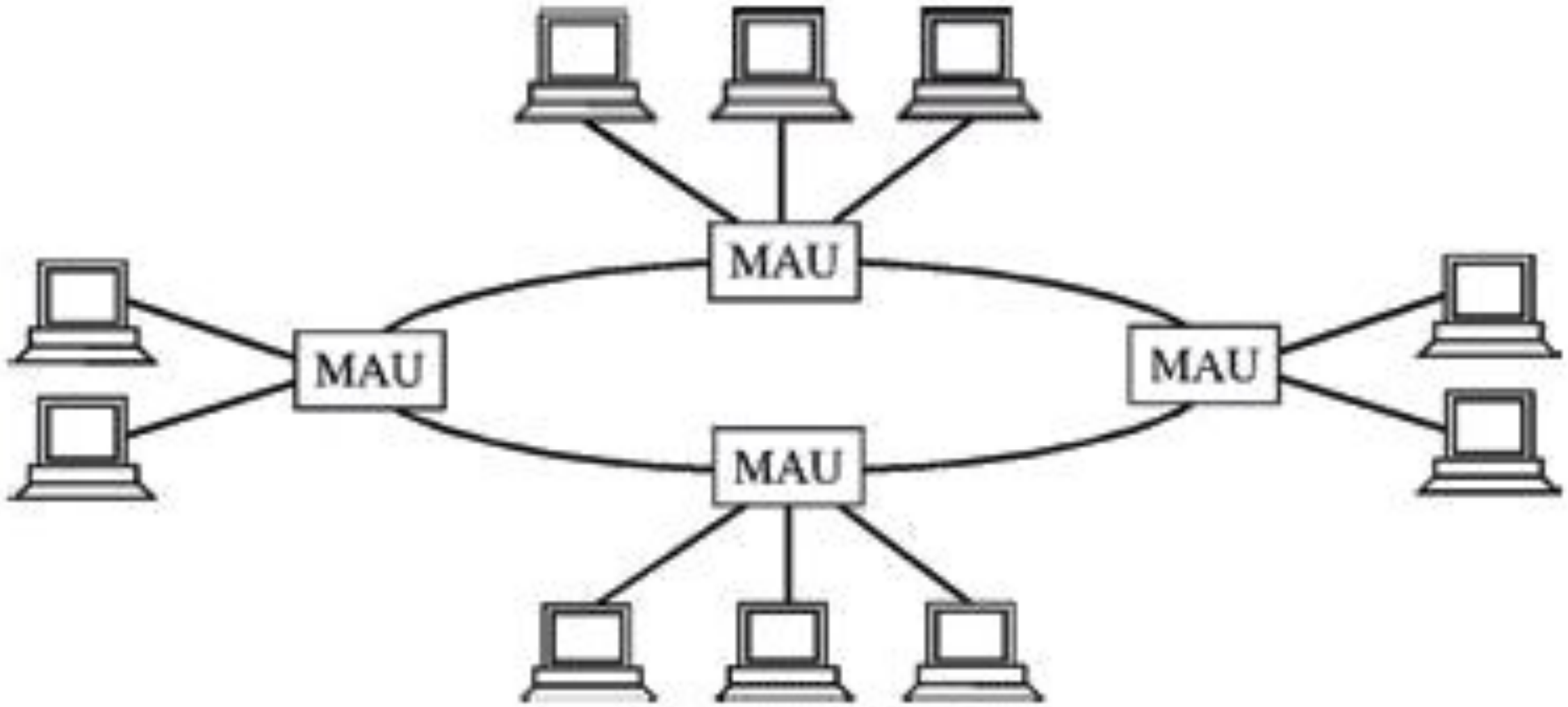
Сеть Token-Ring

- Стандарт IEEE 802.5. В настоящее время устарела.
- Основное преимущество – ограничение максимального времени передачи (детерминированный доступ).

Сеть Token-Ring

- топология – кольцо, звезда+кольцо;
- максимальное количество абонентов в сети – 96;
- максимальная длина кабеля, соединяющего все концентраторы – 120 м;
- скорость передачи данных – 4 Мбит/с и 16 Мбит/с

Сеть Token-Ring



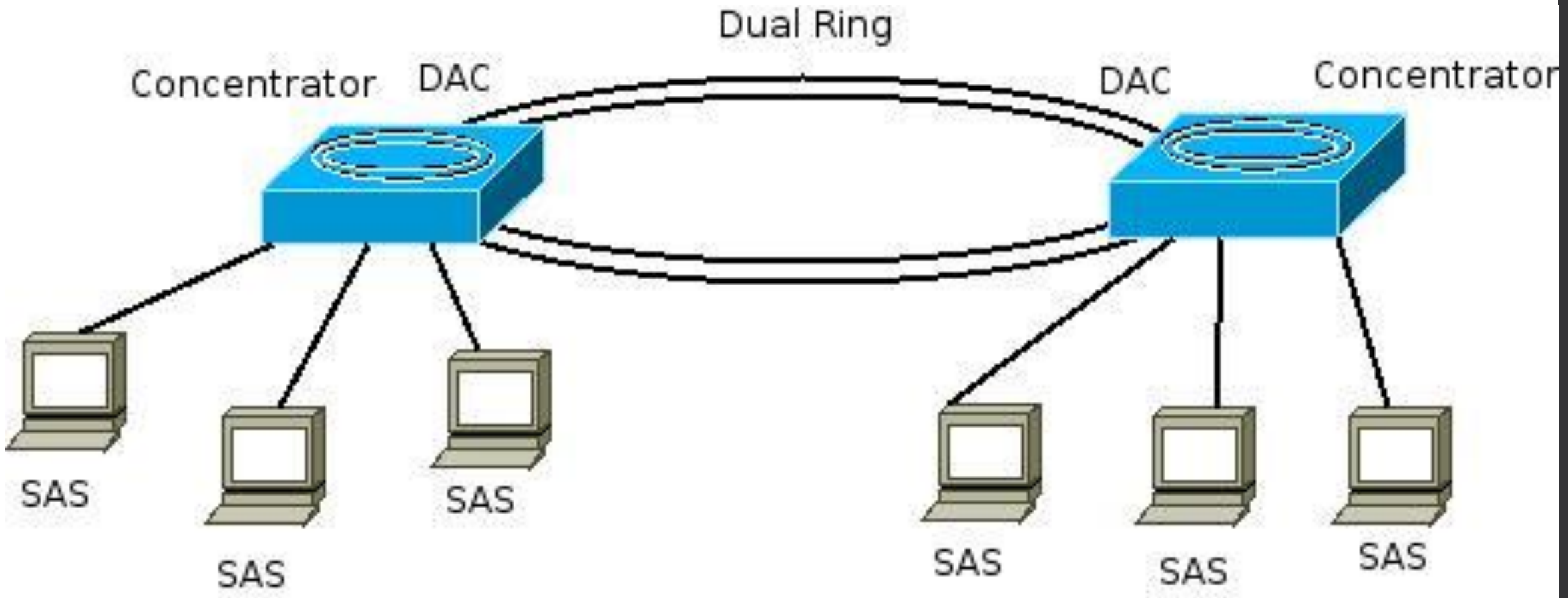
Сеть FDDI

- **Fiber Distributed Data Interface**. — стандарт передачи данных 1980-х годов для локальных сетей с расстояниями до 20 километров. Используются ВОЛП и предоставляется скорость до 100 Мбит/с. Стандарт основан на протоколе Token Ring.

Сеть FDDI

- Скорость передачи информации – 100 Мбит/с
- Топология – двойное кольцо, с возможностью включения концентраторов.
- Метод доступа – маркерный.
- Максимальное количество абонентов сети – 1000.
- Максимальная протяженность кольца сети – 20 километров.

Сеть FDDI


Dual Ring
Concentrator
DAC
DAC
Concentrator
SAS
SAS
SAS
SAS
SAS
SAS

Сеть FDDI

- **DAS** (Dual-Attachment Stations подключены к двум кольцам);
- **SAS** (Single-Attachment Stations подключены только к 1 кольцу)

- При повреждениях кабеля сеть реконфигурируется, при повреждении узлов может использоваться обходной коммутатор.

Сеть Ethernet

Стандарт IEEE 802.3. Сети Ethernet – самые распространенные кабельные сети.

- топология – шина, пассивная звезда или дерево;
- метод доступа – CSMA/CD;
- среда передачи:
  - коаксиальный кабель (толстый 10BASE5 и тонкий 10BASE2),
  - витая пара (10BASE-T);
- скорость передачи – 10 Мбит/с;
- максимальная длина сети – 5 км;
- максимальное количество абонентов – до 1024;
- длина сегмента сети – до 500 м;
- количество абонентов на одном сегменте – до 100.

10Base-5

AMP
228752-1
"30 VDC, 100 mA max. - Class 2 circuit"
"FOR USE ONLY WITH LISTED COAXIAL POWER-LIMITED CIRCUIT CABLES CLASSIFIED FOR FIRE AND SMOKE CHARACTERISTICS WHEN INSTALLED IN OTHER SPACE (SECTION 300-22 (c) OF THE NATIONAL ELECTRICAL CODE) USED FOR ENVIRONMENTAL AIR."
REMOVE SCREWS TO RELEASE CABLE TAP
ST-500 with LANVIEW™
PWR
SQE
XMT
RCV
CLN
cabletron

10Base-2

10Base-T

Сеть Ethernet

- **Основной недостаток** – случайный доступ не гарантирует минимальную задержку доставки сообщения.

Сеть Fast Ethernet

Стандарт IEEE 802.3u.

Основные отличия от Ethernet:

- топология – только пассивная звезда или дерево;
- скорость передачи – 100 Мбит/с;
- три основных типа сегментов, отличающихся типами среды передачи
- 100BASE-T4 – четыре витых пар (в России не используется).
- 100BASE-TX – две витые пары.
- 100BASE-FX – оптоволоконный кабель.

Сеть Gigabit Ethernet

Стандарт IEEE 802.3ab – используется витая пара категории 5e (4 шт.).

Скорость – 250 Мбит/с по одной паре.

Расстояние до 100 метров.

В основном применяется для связи между сетями Fast Ethernet или для доступа к высокопроизводительным серверам.

Уже существуют, а также активно используются сети 10G, 40G и 100G Ethernet.

Сеть 100VG-AnyLAN

Стандарт **IEEE 802.12** – основная альтернатива Fast Ethernet.

Главные особенности:

- сравнительно невысокая стоимость аппаратуры;
- централизованный метод управления;
- совместимость с Ethernet и Token-Ring;

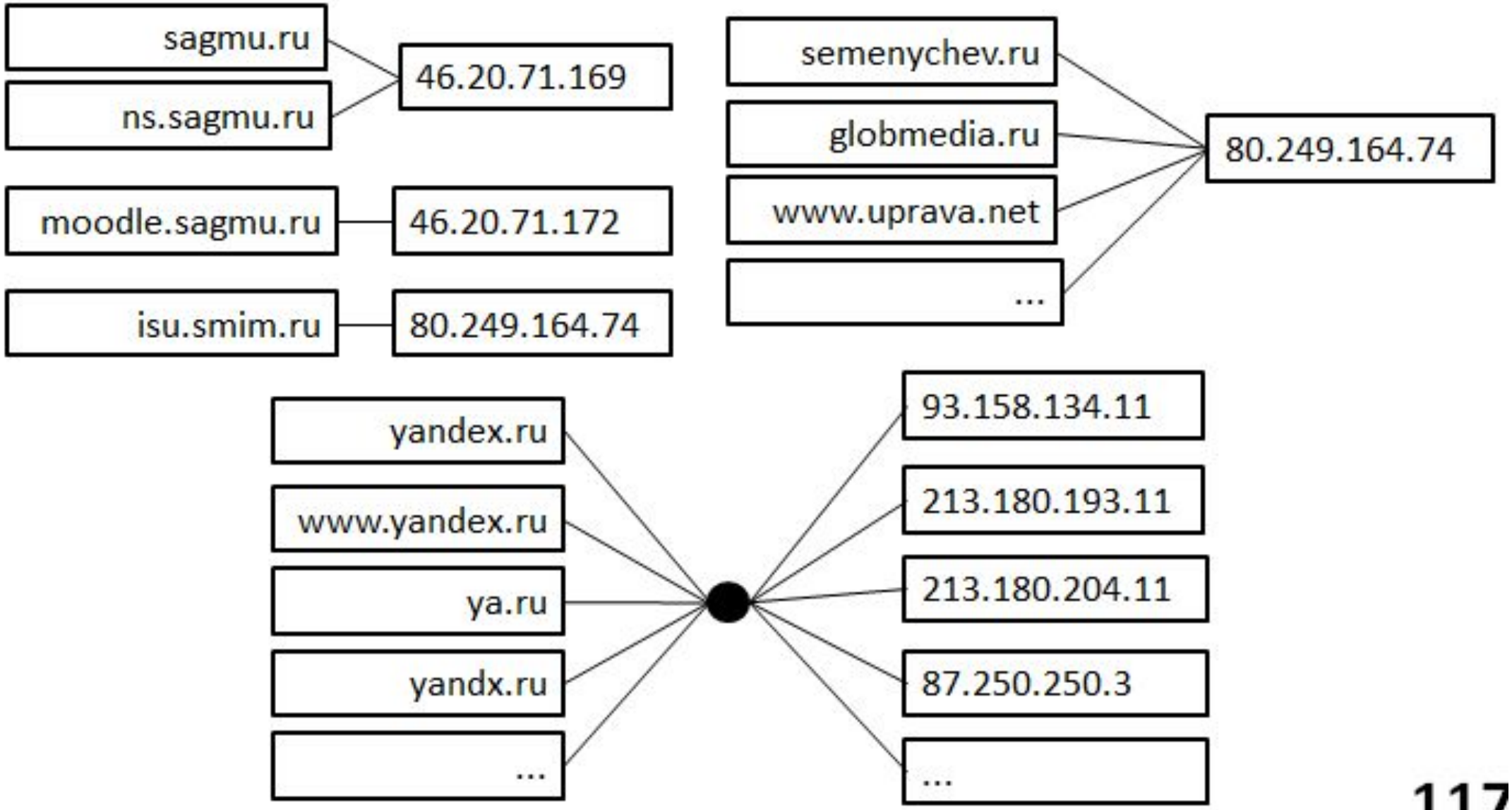
Система доменных имён

Система доменных имён

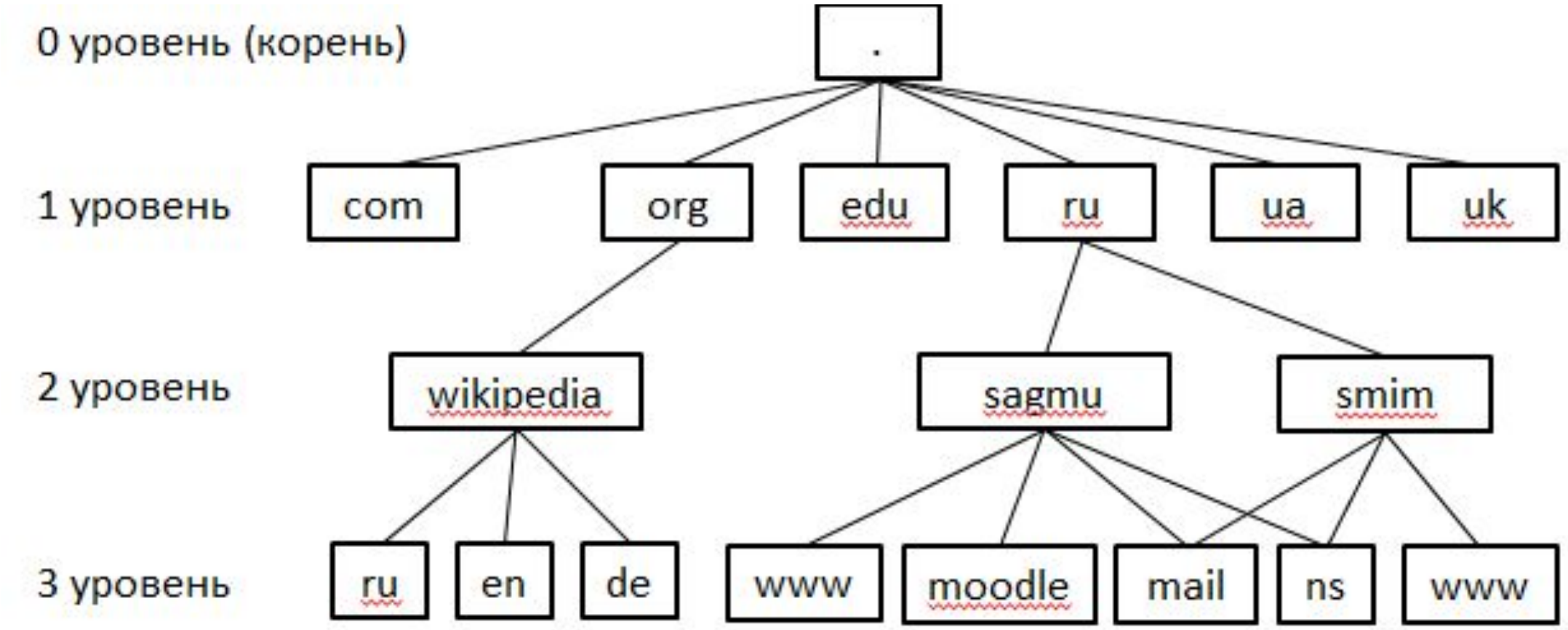
- **DNS (Domain Name System)** – система доменных имён. Используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и т.п.

- Одному доменному имени может соответствовать несколько IP-адресов, и наоборот.

Система доменных имён



Иерархия доменных имён



Система доменных имён

- **Домен** – ветвь иерархии со всеми подчиненными поддоменами.
- **Корневой домен** – домен самого верхнего уровня в любой системе доменных имён. Корневой домен Интернета (0 уровень) обслуживается корневыми серверами системы доменных имён, которые располагаются в различных странах мира.
- **Ресурсная запись** – единица хранения и передачи информации в DNS.

Система доменных имён

- **Зона** – часть дерева доменных имён (включая ресурсные записи), размещаемая как единое целое на одном или нескольких DNS-серверах.
- **DNS-сервер** – специализированное ПО для обслуживания DNS, а также компьютер, на котором это ПО выполняется.
- **DNS-клиент** – специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.

Система доменных имён

Полностью определенное доменное имя (FQDN, Fully Qualified Domain Name) – завершается нуль-меткой корня (пустой домен):

dom.sagmu.ru**.** www.google.com**.** myhost.org**.**

Частично определенное доменное имя:

domdom.sagmu sagmu.ru google.com

Домены верхнего уровня

Классификация		Метка	Описание
Родовые – определяют тип хоста по его роду деятельности, метка обычно состоит из трех букв.	Неспонсируемые	com	коммерческие организации
		net	центры поддержки сетей
		org	некоммерческие организации
		info	информационные сайты
	Спонсируемые	int	международные организации
		eco	связанные с экологией
		post	почтовые организации
	Ограниченного пользования	gov	правительственные учреждения
		edu	образовательные учреждения
Зарезервированные		example	для примеров в документации и тестирования
		test	
		invalid	
		localhost	=127.0.0.1
Национальные – определяют размещение хоста, метка обычно состоят из двух букв.		ru, рф	Россия
		su	СССР
		ua, укр	Украина
		kz	Казахстан
		de	Германия
		uk, gb	Великобритания

Правила записи доменных имён

В доменных именах разрешено использовать только 26 символов латинского алфавита (без различения заглавных и строчных букв), арабские цифры 0-9 и дефис.

Максимальный уровень доменного имени - 127. Максимальная длина метки каждого уровня – 63 символа.

Для использования национальных символов в DNS-именах они преобразуются в **Punycode** («пьюникод»).

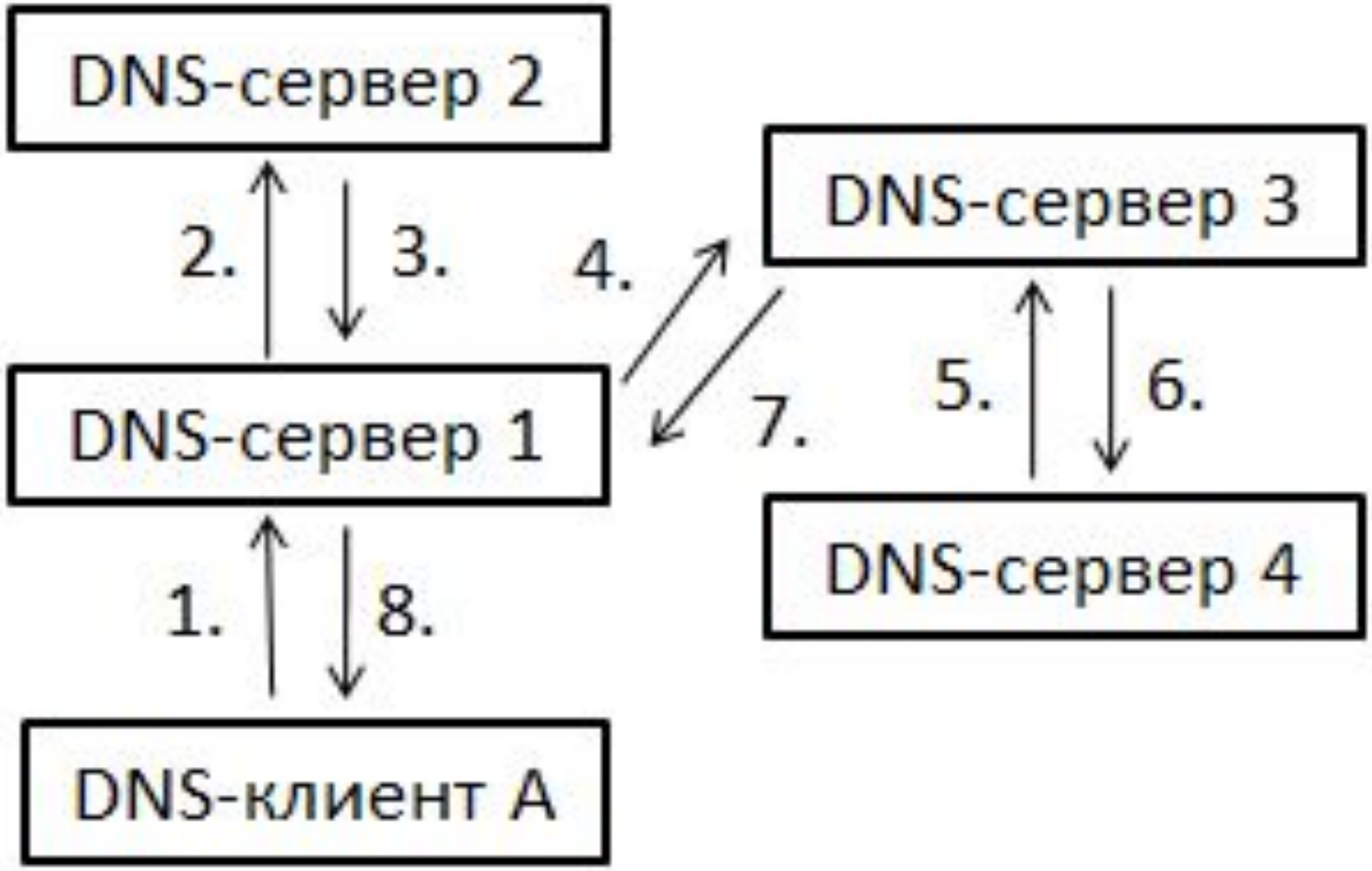
Punycode

Последовательность символов	Кодировка
abcdef	abcdef
abæcdöef	abcdef-qua4k
schön	schn-7qa
ยจฆฟคฏข	22cdfh1b8fsa
💩	74h
правда	80aafi6cg

DNS-сервер

Преобразование DNS-имен в IP-адреса и обратно осуществляется **DNS-серверами**. Соответствия хранятся в хост-файле. Каждый DNS-сервер отвечает за определенную зону доменных имен.

DNS-сервер


DNS-сервер 2
DNS-сервер 3
DNS-сервер 1
DNS-сервер 4
DNS-клиент А
1.
2.
3.
4.
5.
6.
7.
8.

DNS-сервер

Делегирование – процедура передачи сервером части своих полномочий серверу более низкого уровня.

Рекурсивный запрос – на него необходимо отвечать готовым ответом.

Итеративный запрос – на него необходимо ответить с информацией, куда обратиться.

Динамический DNS

IP-адреса хостов могут изменяться, в то время как их DNS-имена остаются постоянными.

Кэширование адресов – для ускорения поиска и снижения трафика DNS-сервера на некоторое время (TTL) сохраняют полученную от других серверов информацию в кэше.

Динамический DNS

Round Robin DNS (RR DNS) – метод распределения нагрузки между несколькими идентичными серверами.

Например, dsn.example.ru обслуживается четырьмя реальными серверами

20.1.1.1; **220.1.1.2**; **220.1.1.3**; **220.1.1.4**

Первый запросивший IP-адрес получит ответ 220.1.1.1, второй 220.1.1.2, третий 220.1.1.3, четвертый 220.1.1.4, пятый 220.1.1.1 и т.д. по кругу.

Динамическое назначение IP-адресов

DHCP (Dynamic Host Configuration Protocol) – протокол динамической настройки узла.

Позволяет узлам получить IP-адрес и другие настройки для работы в сети.

Для этого клиент обращается к DHCP-серверу. Протокол DHCP предоставляет три способа распределения IP-адресов:

Динамическое назначение IP-адресов

- **Ручное распределение**. Администратор сопоставляет аппаратному адресу каждого клиентского компьютера определённый IP-адрес.

Динамическое назначение IP-адресов

- **Автоматическое распределение**. При данном способе каждому компьютеру на постоянное использование выделяется случайный свободный IP-адрес из определённого администратором диапазона.

Динамическое назначение IP-адресов

- **Динамическое распределение**. Адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок (аренда адреса).

Пример получения адреса

- Предположим, клиент ещё не имеет собственного IP-адреса, но ему известен его предыдущий адрес - 192.168.1.100.

Пример получения адреса

1. Обнаружение (DHCPDISCOVER) – широковещательный запрос по всей сети с целью обнаружить доступные DHCP-серверы.

UDP Src=0.0.0.0 Dest=255.255.255.255			
OP	HTYPE	HLEN	HOPS
0x01	0x01	0x06	0x00
XID			
0x3903F326			
SECS		FLAGS	
0x0000		0x0000	
CIADDR			
0x00000000			
YIADDR			
0x00000000			
SIADDR			
0x00000000			
GIADDR			
0x00000000			
CHADDR			
0x0000001d6057ed80			
SNAME			
(пустое поле)			
FILE			
(пустое поле)			
OPTIONS			
Опция DHCP 53: обнаружение DHCP			
Опция DHCP 50: запрос адреса 192.168.1.100			

Пример получения адреса

2. Предложение (DHCPOFFER) – сервер определяет конфигурацию клиента, например, согласен с прежним адресом. Клиент может получить несколько предложений от разных серверов.

UDP Src=192.168.1.1 Dest=255.255.255.255			
OP	HTYPE	HLEN	HOPS
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SECS		FLAGS	
0x0000		0x0000	
CIADDR			
0x00000000			
YIADDR			
0xC0A80164			
SIADDR			
0xC0A80101			
GIADDR			
0x00000000			
CHADDR			
0x0000001d6057ed80			
SNAME			
(пустое поле)			
FILE			
(пустое поле)			
OPTIONS			
Опция DHCP 53: предложение DHCP			
Опция DHCP 1: маска подсети 255.255.255.0			
Опция DHCP 3: маршрутизатор 192.168.1.1			
Опция DHCP 51: срок аренды IP-адреса — 1 день			
Опция DHCP 54: DHCP-сервер 192.168.1.1			

Пример получения адреса

3. Запрос (DHCPREQUEST) – клиент выбирает одно из предложений и вновь отправляет сообщение, похожее на **DHCPDISCOVER,** но уже с указанием конкретного сервера.

UDP Src=0.0.0.0 Dest=255.255.255.255			
OP	HTYPE	HLEN	HOPS
0x01	0x01	0x06	0x00
XID			
0x3903F326			
SECS		FLAGS	
0x0000		0x0000	
CIADDR			
0x00000000			
YIADDR			
0x00000000			
SIADDR			
0x00000000			
GIADDR			
0x00000000			
CHADDR			
0x0000001d6057ed80			
SNAME			
(пустое поле)			
FILE			
(пустое поле)			
OPTIONS			
Опция DHCP 53: запрос DHCP			
Опция DHCP 50: запрос адреса 192.168.1.100			
Опция DHCP 54: DHCP-сервер 192.168.1.1			

Пример получения адреса

4. **Подтверждение (DHCPACK)** – сервер подтверждает запрос, клиент настраивает свой сетевой интерфейс.

UDP Src=192.168.1.1 Dest=255.255.255.255			
OP	HTYPE	HLEN	HOPS
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SECS		FLAGS	
0x0000		0x0000	
CIADDR			
0x00000000			
YIADDR			
0xC0A80164			
SIADDR			
0x00000000			
GIADDR			
0x00000000			
CHADDR			
0x0000001d6057ed80			
SNAME			
(пустое поле)			
FILE			
(пустое поле)			
OPTIONS			
Опция DHCP 53: подтверждение DHCP			
Опция DHCP 1: маска подсети 255.255.255.0			
Опция DHCP 3: маршрутизатор 192.168.1.1			
Опция DHCP 51: срок аренды IP-адреса — 1 день			
Опция DHCP 54: DHCP-сервер 192.168.1.1			