

# Сеть и сетевые протоколы: L2-сеть

Ильмир Сахипов  
Руководитель центра управления сетью АО “Уфанет”



# Ильмир Сахипов

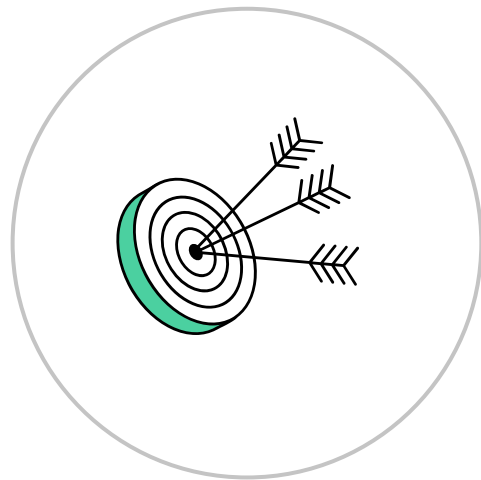
О спикере:

- Руководитель центра управления сетью АО “Уфанет”
- Более 10 лет опыта в области телекоммуникаций
- Эксперт в решении сложных клиентских и сетевых инцидентов на мультивендорной мультисервисной операторской сети



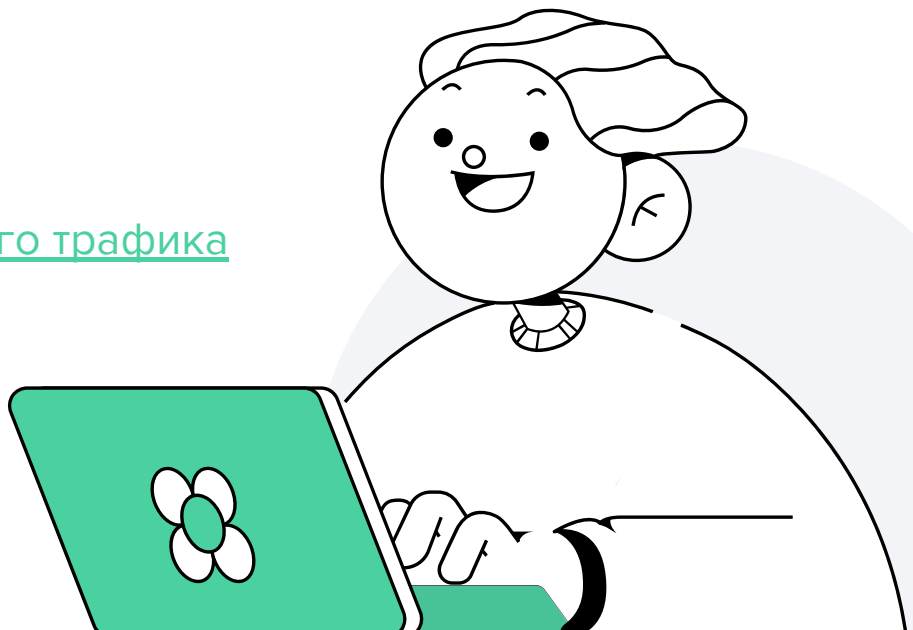
# Цели занятия

- Разобраться в основах работы канального уровня модели OSI
- Изучить различные среды, используемые для передачи данных
- Понять принципы работы протокола Ethernet
- Изучить протокол ARP
- Научиться работать с ARP-таблицами и проверять коннективити с помощью утилиты arping
- Ознакомиться с проблематикой служебного трафика и методами ее решения через протоколы SRP и VLAN
- Научиться настраивать VLAN в Linux

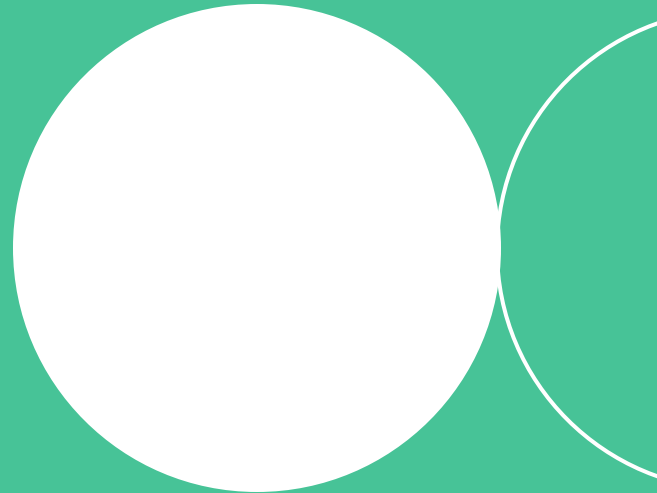


# План занятия

- 1 Канальный уровень L2 в модели OSI
- 2 Виды сред передачи данных
- 3 Домен коллизий и широковещательный домен
- 4 Протокол Ethernet IEEE 802.3
- 5 Address Resolution Protocol (ARP)
- 6 Решение проблем широковещательного трафика  
STP & VLAN
- 7 Домашнее задание

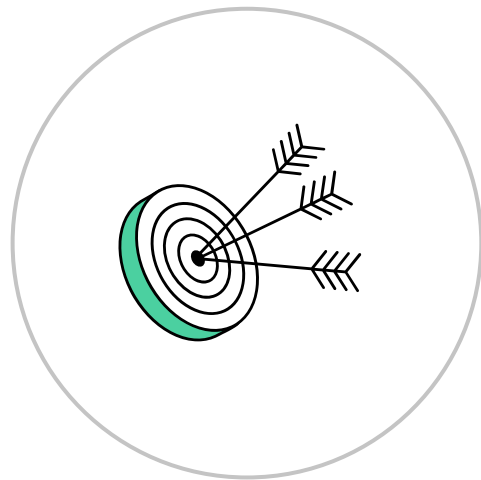


# Канальный уровень L2 в модели OSI



# Цели темы

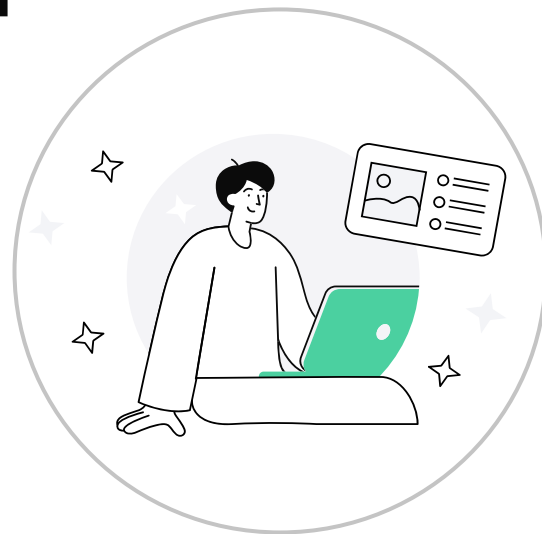
- Обзорно изучить канальный уровень L2 в модели OSI: назначение, решаемые проблемы, используемое оборудование
- Познакомиться с понятием сегмента сети
- Разобраться с разными типами передачи трафика, их особенностями и применением в бизнесе.





## Канальный уровень (Data Link layer)

**определяет способы передачи данных между устройствами, находящимися в одном сегменте сети**



# Уровни модели OSI

**Прикладной уровень**

Application layer

**Уровень представления**

Presentation layer

**Сеансовый уровень**

Session layer

**Транспортный уровень**

Transport layer

**Сетевой уровень**

Network layer

**Канальный уровень**

Data link layer

**Физический уровень**

Physical layer

определяет способы передачи данных  
между устройствами, находящимися в  
одном сегменте сети



# Канальный уровень: решаемые проблемы

- Обнаружение ошибок физического уровня
- Одновременная передача данных разным устройствам
- Аппаратная адресация

# Канальный уровень: единица данных

**Frame (кадр)**

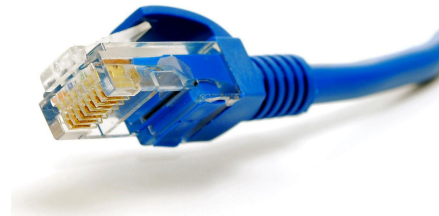
# Канальный уровень: примеры оборудования и протокола



Коммутатор



Сетевая карта



Ethernet



## Сегмент сети

**логически или физически обособленная часть сети**



# Целью разделения сети на сегменты является

1

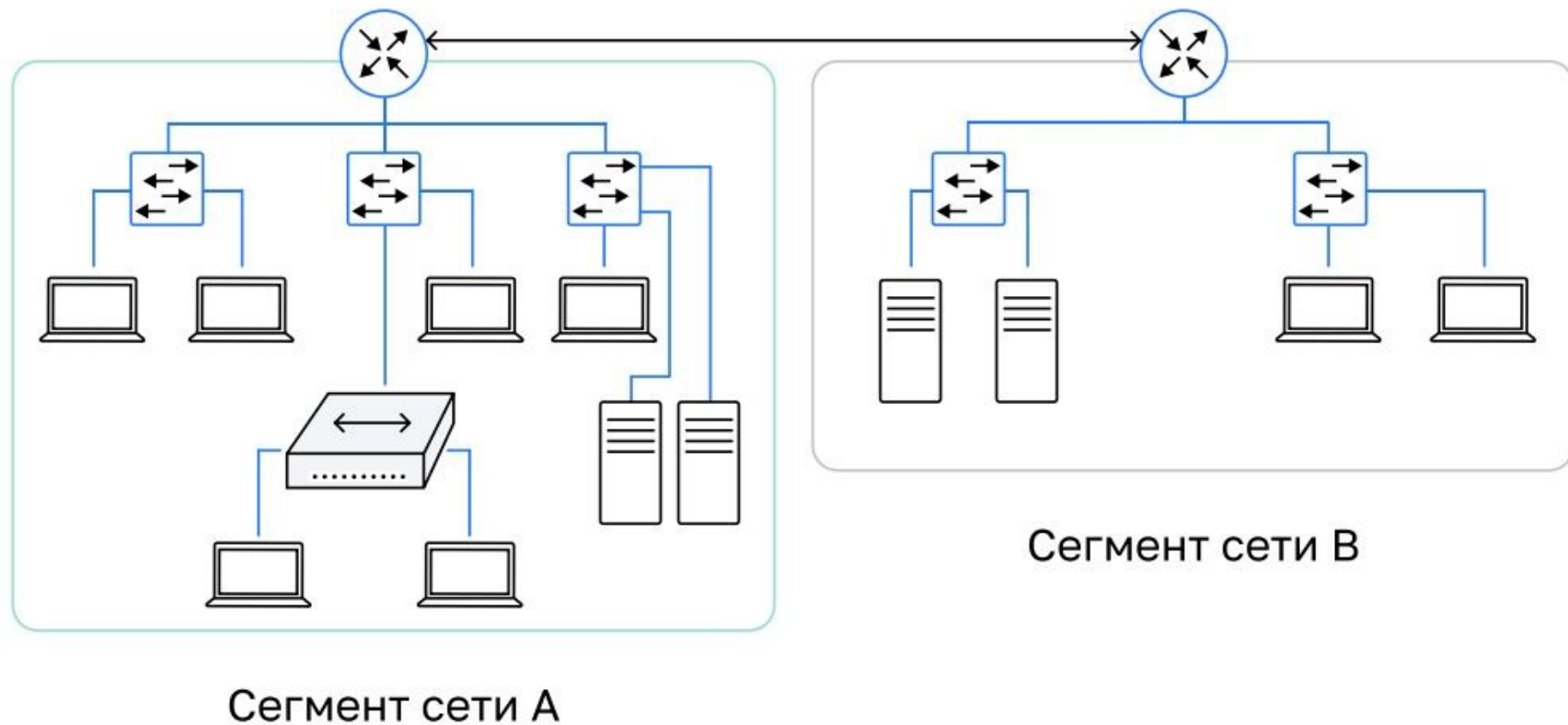
Оптимизация  
сетевого трафика

и/или

2

Повышение  
безопасности сети

# Пример сети из двух сегментов



# Типы передачи трафика

1

## Broadcast трафик

от одного хоста  
ко всем хостам в сети

2

## Unicast трафик

от одного хоста  
к другому хосту

3

## Multicast трафик

от одного хоста к  
некоторой ограниченной  
группе хостов

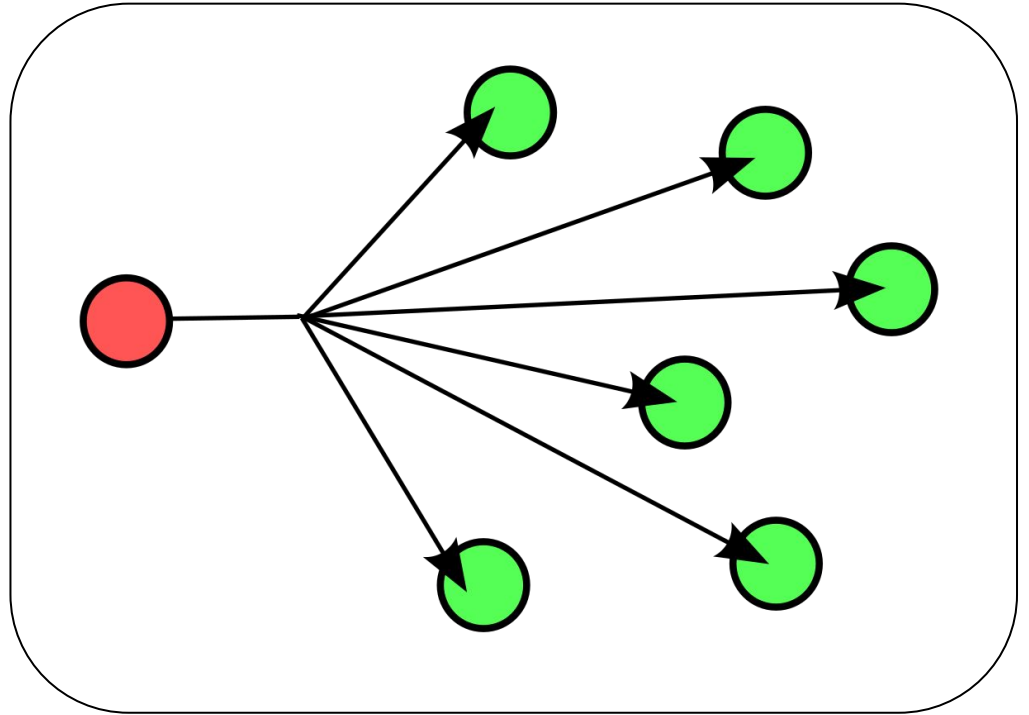
# Типы передачи трафика: аналогия из жизни





# Схема работы Broadcast трафика

- Для отправки используется широковещательный адрес
- Передается только в одном сегменте сети



# Broadcast трафик: аналогия из жизни

Поиск человека в Торговом центре по громкой связи



# Broadcast трафик: аналогия из жизни

Узнать, кто последний в очереди





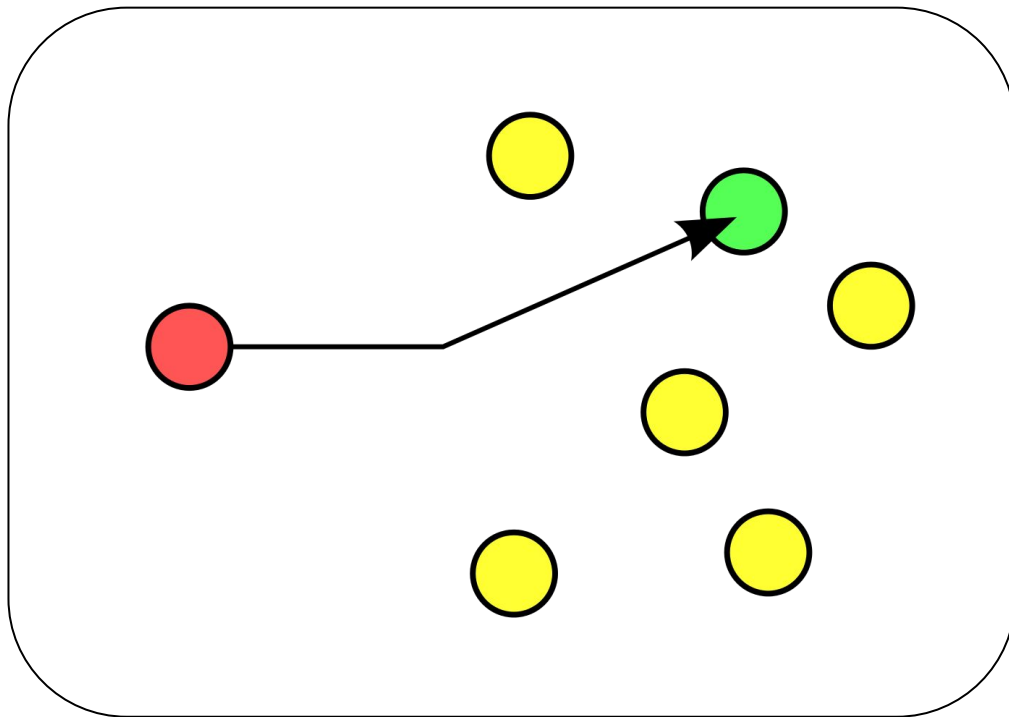
**Broadcast трафик**  
используют для  
служебного трафика

# Использование Broadcast трафика

- Определения нужного адреса
- Получения настроек
- Поиска сервера DHCP

# Схема работы Unicast трафика


- Для отправки используется конкретный адрес другого устройства
- Передается как в одном, так и в разных сегментах сети



# Unicast трафик: аналогия из жизни

Звонок по мобильному  
телефону



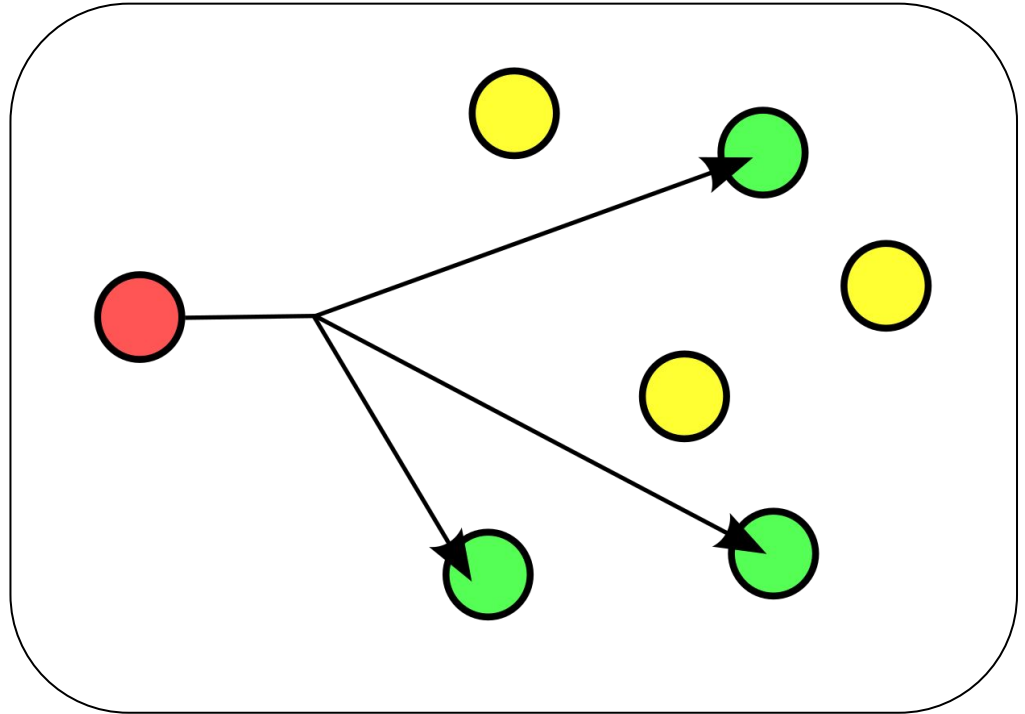


**Unicast трафик**  
**используют**  
**для обмена данными по**  
**клиент-серверной модели**



# Схема работы Multicast трафика

- Для отправки используется адрес из специального диапазона, к которому привязана группа получателей
- Передается как в одном, так и в разных сегментах сети



# Multicast трафик: аналогия из жизни

Доступ к вебинару только  
для тех, у кого есть ссылка





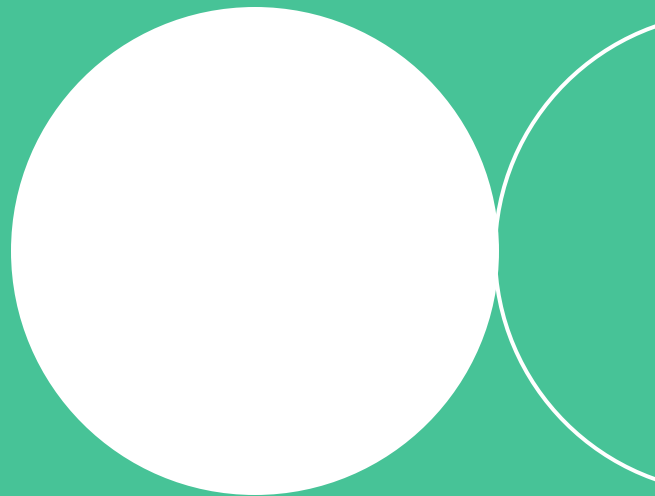
**Multicast трафик**  
используют  
для рассылки сообщений  
ограниченной группе

# Итоги

- ① Канальный уровень - это второй уровень в модели OSI, который отвечает за обмен данными между устройствами в одном сегменте сети
- ② Сегмент сети - это логически или физически обособленный участок сети
- ③ Существует 3 типа трафика: broadcast, unicast и multicast:
  - для служебного трафика используется broadcast
  - для взаимодействия между 2 узлами используется unicast
  - для рассылки сообщений ограниченной группе используется multicast

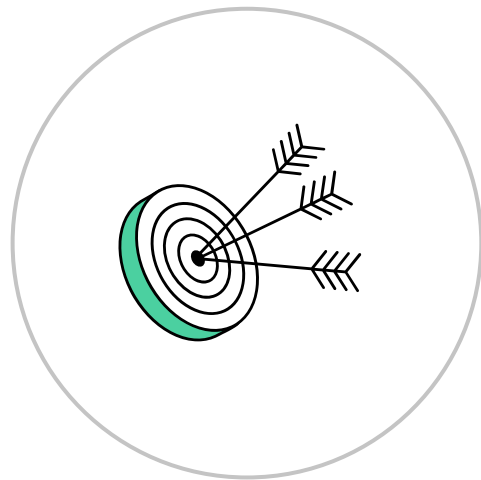


# Виды сред передачи данных

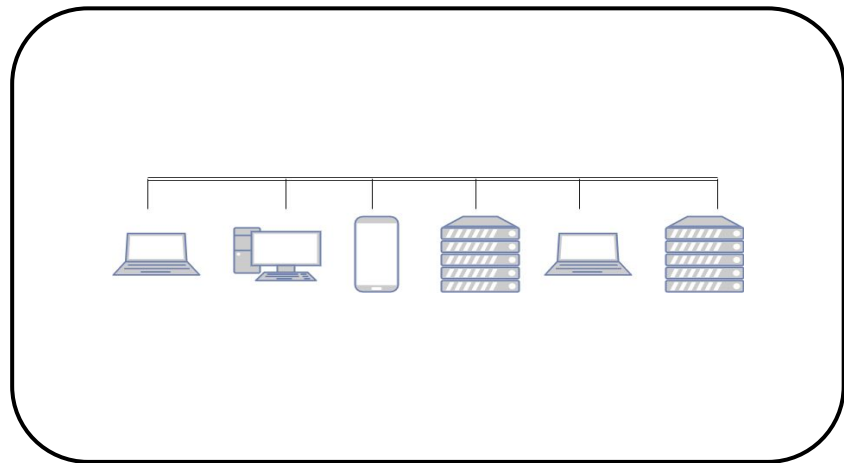


# Цели темы

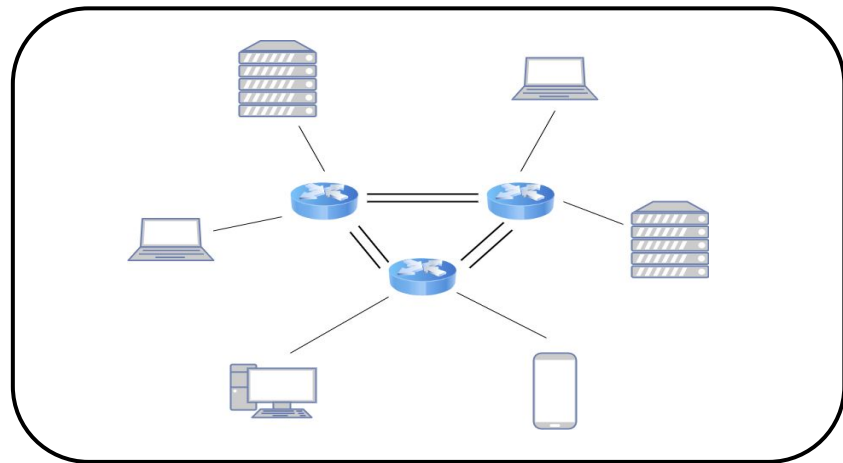
- Узнать о различных типах сред, используемых для передачи информации
- Познакомится с их ключевыми особенностями, достоинствами и недостатками
- Рассмотреть практические возможности применения различных сред



# Виды сред



**Общая среда**  
разделяемая среда



**Switched**  
коммутируемая среда



## Общая среда

**метод реализации сетей, когда все устройства имеют доступ к среде передачи данных, используя ее одновременно для приема и передачи**





# Сеть с общей средой



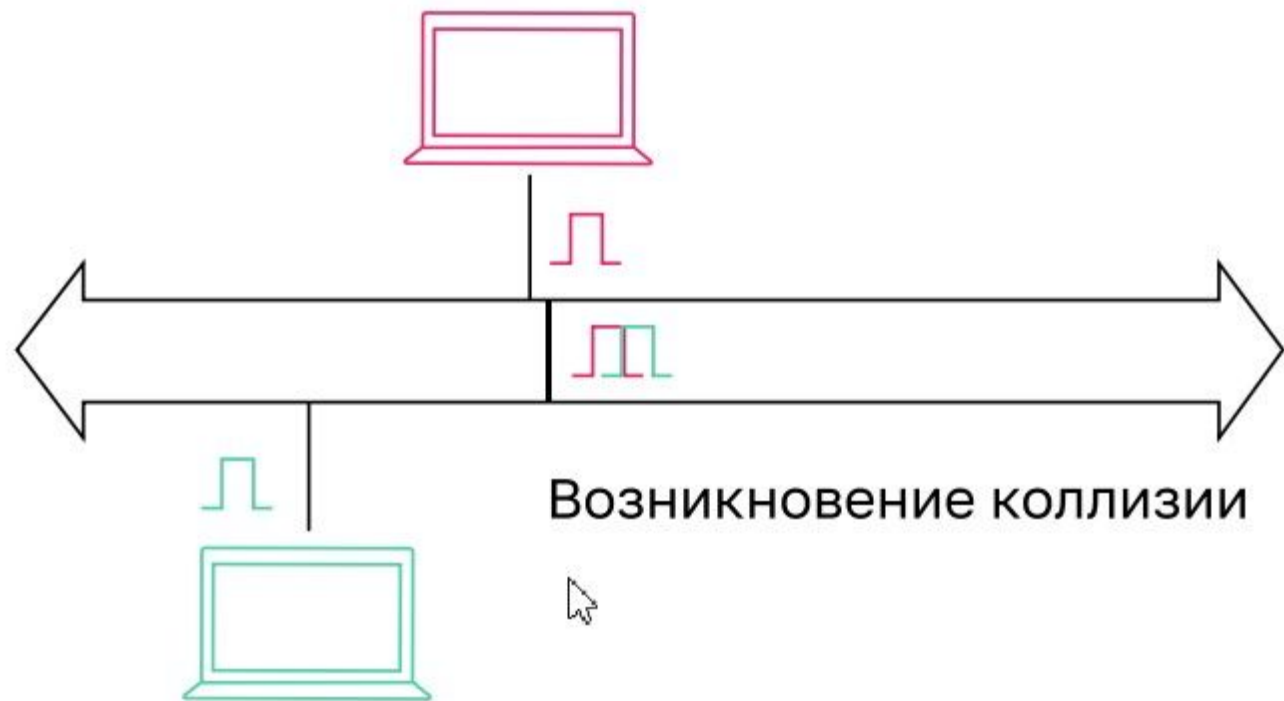


## Коллизии

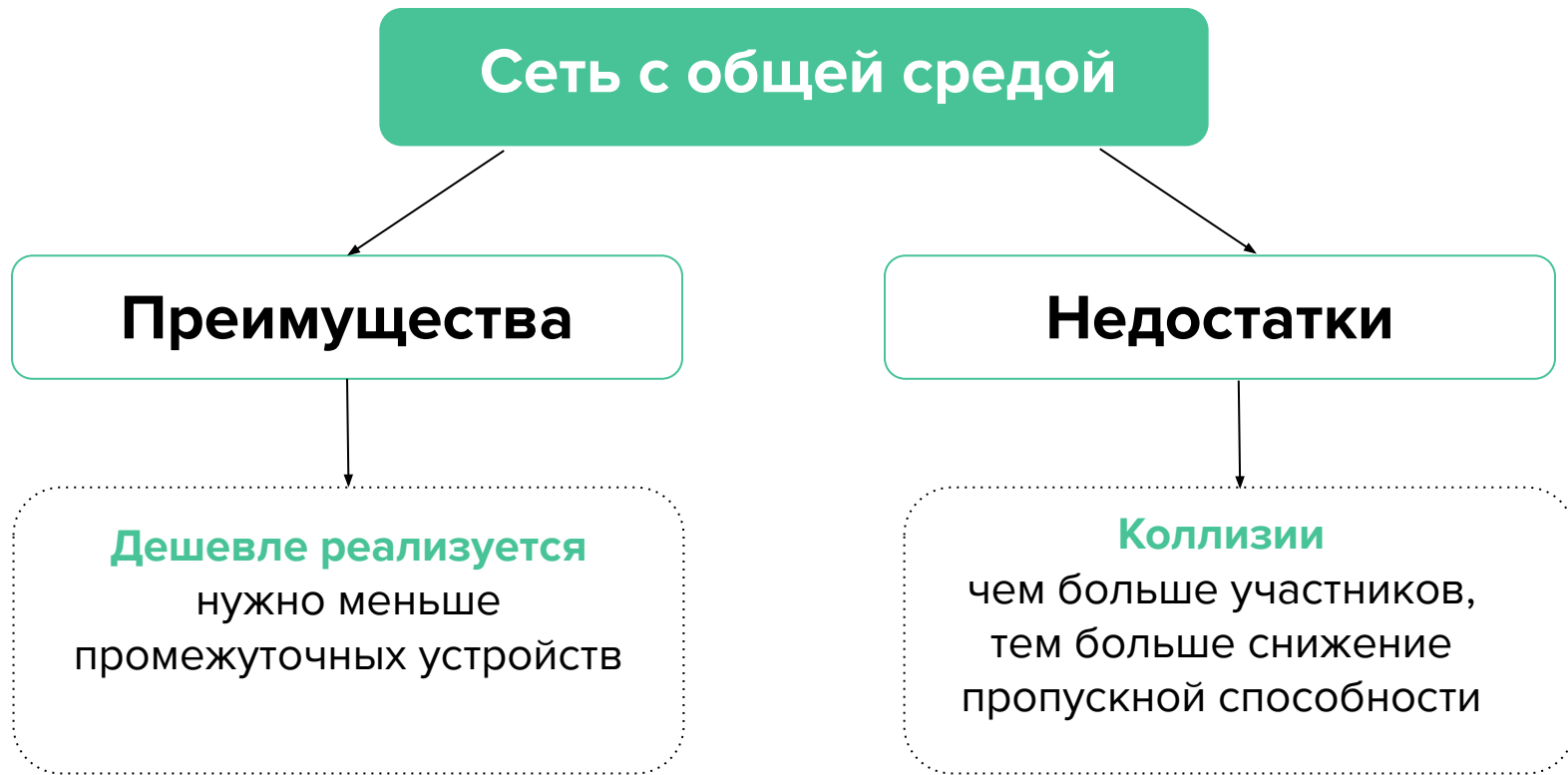
**наложение двух и более кадров от станций, пытающихся передать кадр в один и тот же момент времени в сети с общей средой передачи данных**



# Возникновение коллизии в сети с общей средой

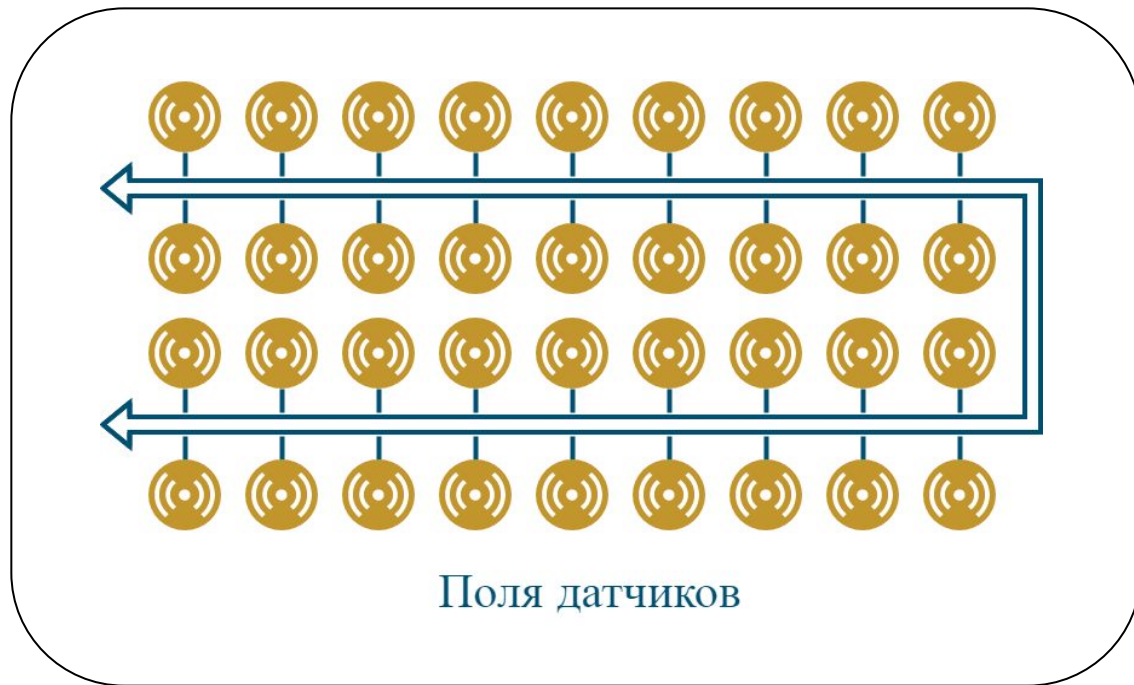


# Плюсы и минусы сети с общей средой



# Примеры использования

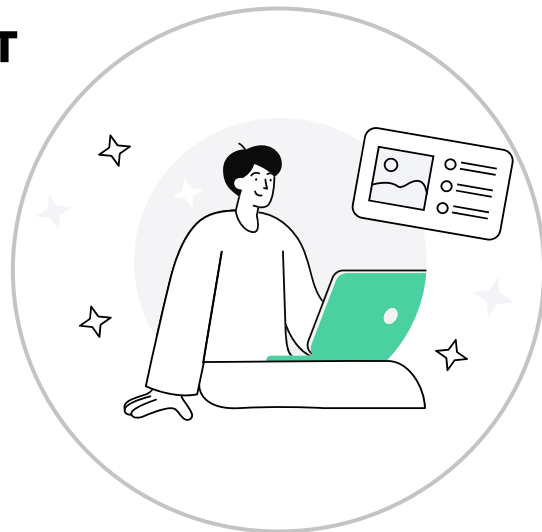
- построение сетей датчиков на производстве
- сигнализация



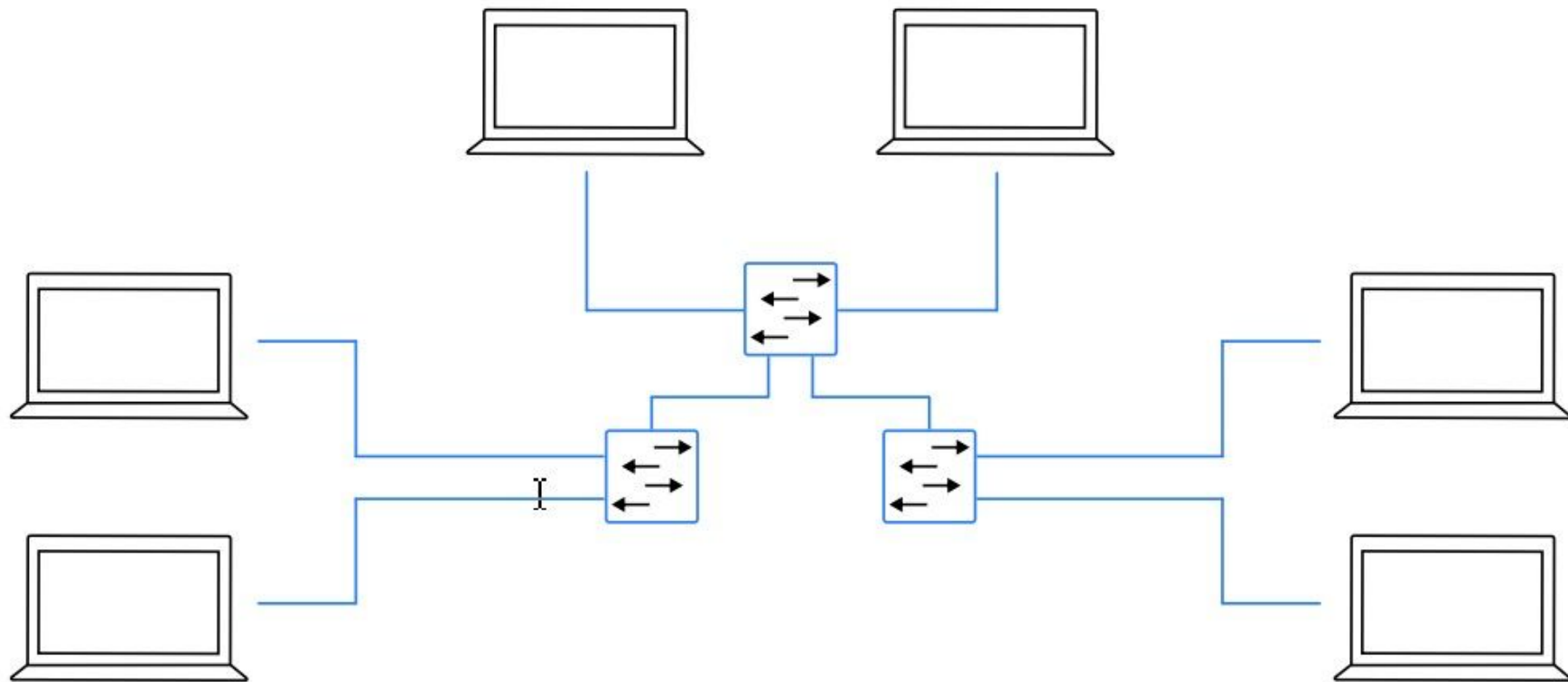


## Коммутируемый доступ

**метод построения сетей на основе выделения каналов приема-передачи от конечных устройств к коммутаторам, которые обеспечивают маршрутизацию данных на основе адреса получателя**



# Сеть с коммутируемым доступом



# Стандарты связи

1

Полудуплексный  
режим

2

Дуплексный  
режим





## Полудуплексный режим

**один и тот же канал может использоваться  
или для передачи или для приема, но  
не одновременно**



# Сеть с коммутируемым доступом

Полудуплексный режим



“

## Дуплексный режим

приём и передача могут осуществляться  
одновременно за счет физического  
разделения соответствующих каналов



# Сеть с коммутируемым доступом

Дуплексный режим



# Плюсы и минусы сети с коммутируемым доступом

## Сеть с коммутируемым доступом

```
graph TD; A[Сеть с коммутируемым доступом] --> B[Преимущества]; A --> C[Недостатки]; B --> D[Нет коллизий<br/>выше производительность<br/>при большом количестве<br/>участников]; C --> E[Выше цена реализации<br/>больше промежуточных<br/>устройств];
```

### Преимущества

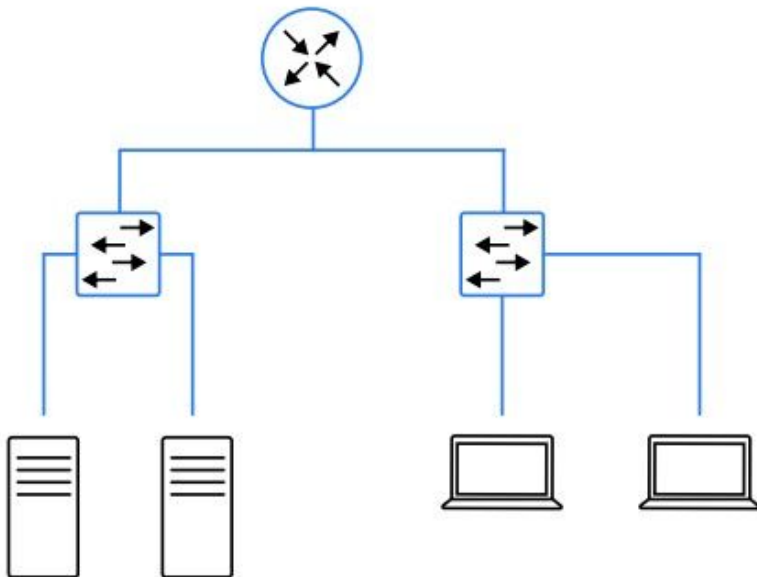
**Нет коллизий**  
выше производительность  
при большом количестве  
участников

### Недостатки

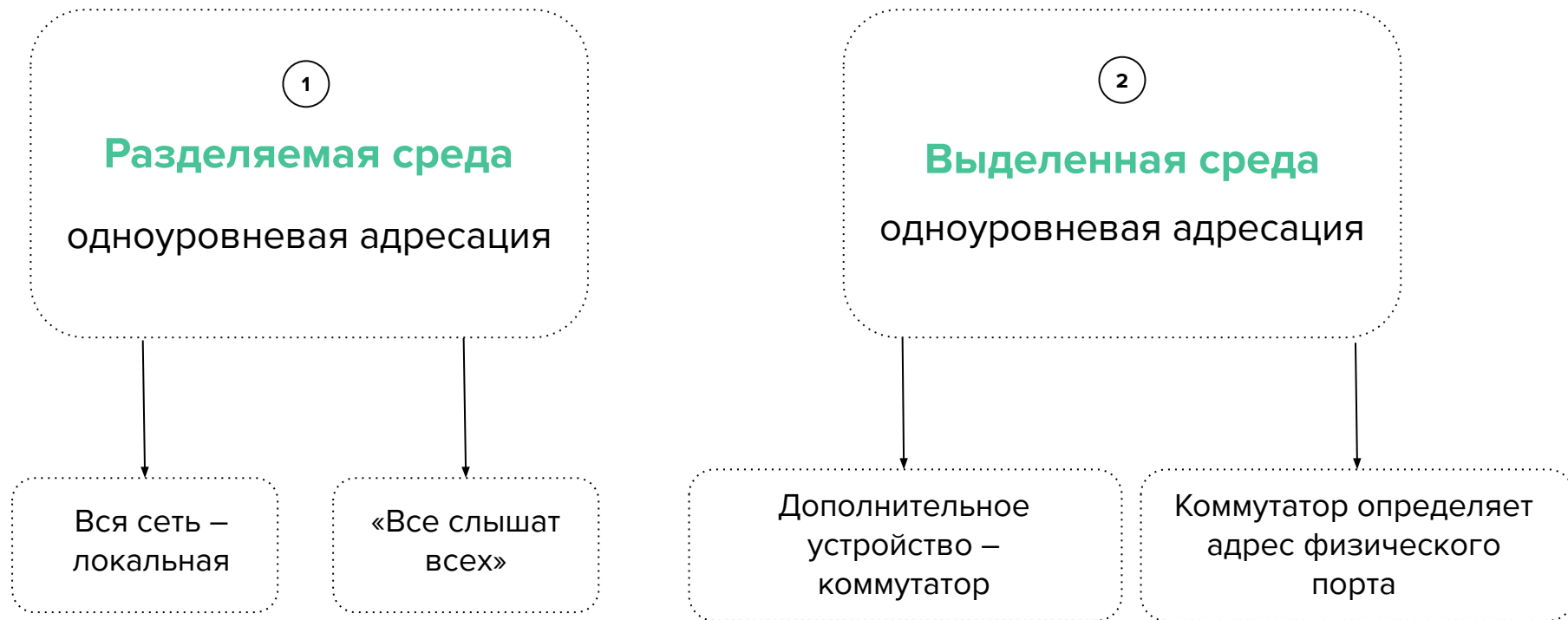
**Выше цена реализации**  
больше промежуточных  
устройств

# Пример использования

Офисная сеть



# Адресация в разных средах



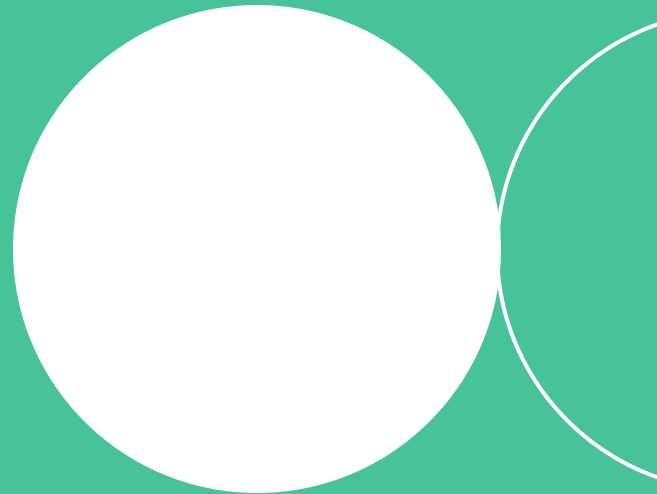
# Итоги

- 1 Существует два типа среды передачи данных:  
коммутируемая среда и среда с общим доступом
- 2 Среда с общим доступом позволяет без особых затрат развернуть сеть, но с увеличением количества абонентов возрастает количество коллизий и падает пропускная способность.
- 3 Коммутируемая среда более затратна для реализации, однако позволяет полностью использовать возможную пропускную способность сети



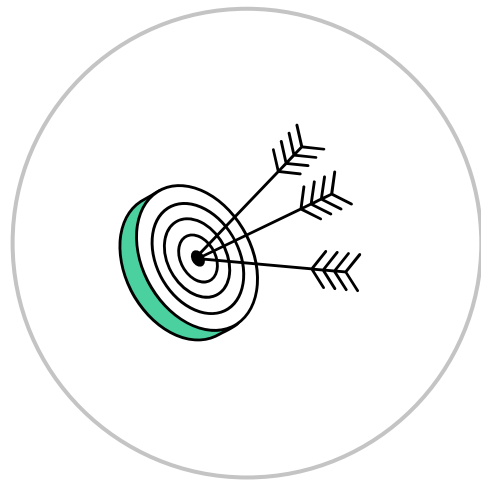


# Домен коллизий и широковещательный домен



# Цели темы

- Изучить понятия домен коллизий и широковещательный домен
- Узнать о причинах возникновения домена коллизий
- Понять, для чего используется широковещательный домен





## Домен коллизий

часть сети Ethernet, все узлы которой конкурируют за общую разделяемую среду передачи и, следовательно, каждый узел которой может создать коллизию с любым другим узлом этой части сети



# Домен коллизий

Чем больше узлов  
в сегменте



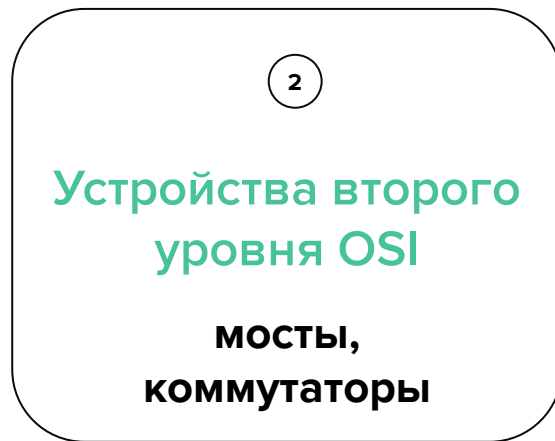
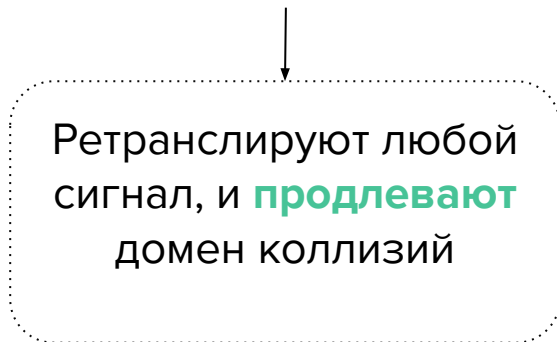
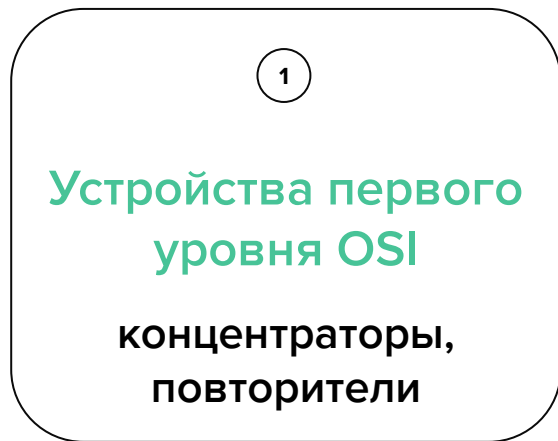
Тем выше вероятность  
коллизий

# Домен коллизий: аналогия из жизни

Телефонная  
конференция с  
большим  
количеством людей

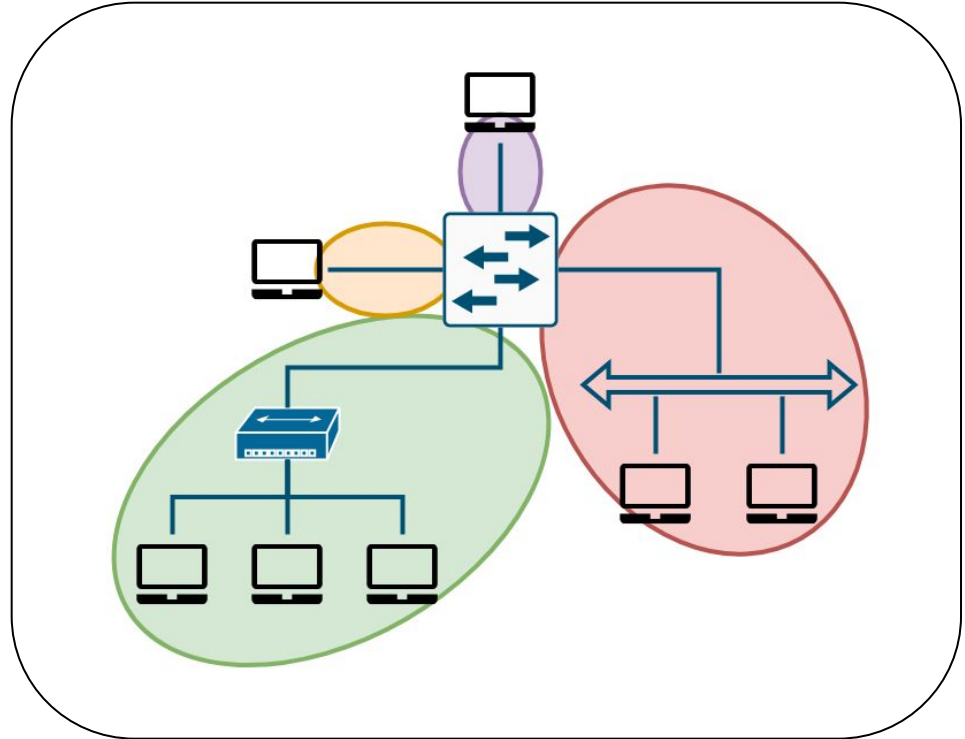


# Сетевые устройства и домен коллизий



# Схема четырех доменов коллизий

- Устройства канального уровня L2 и сетевого уровня L3 ограничивают домен коллизий
- Устройства физического уровня L1 продлевают домен коллизий





## Широковещательный домен

метод доставки сообщений, при котором сообщение получают сразу все участники обмена (связи)

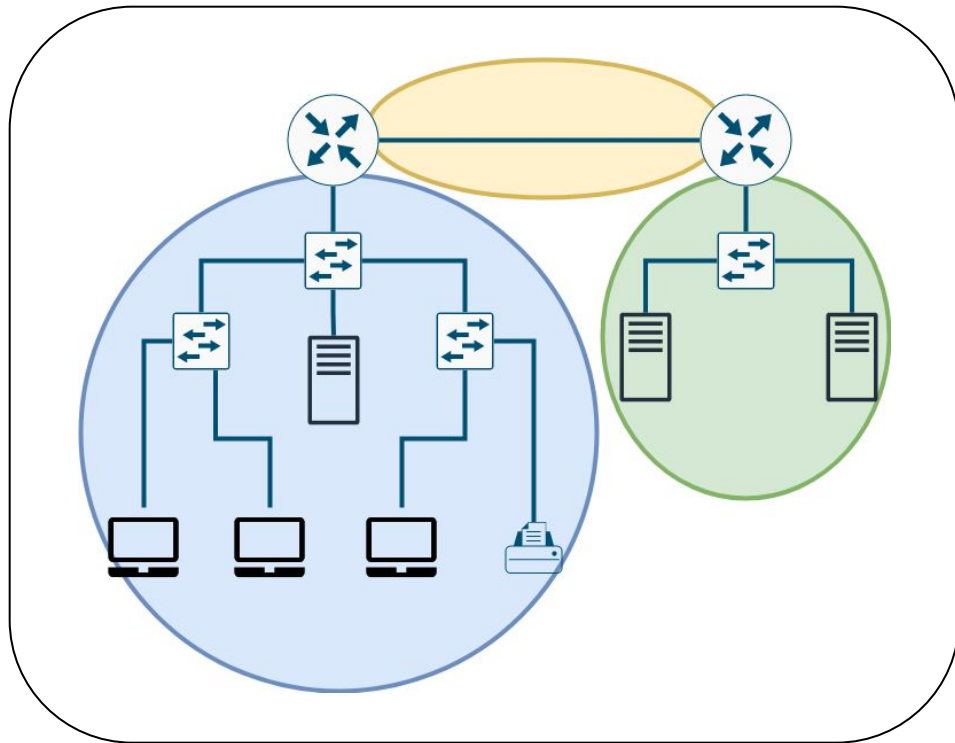




# Широковещательный домен ограничен сегментом сети

Ограничивающие устройства:

- Маршрутизаторы
- Коммутаторы с поддержкой виртуальных сетей

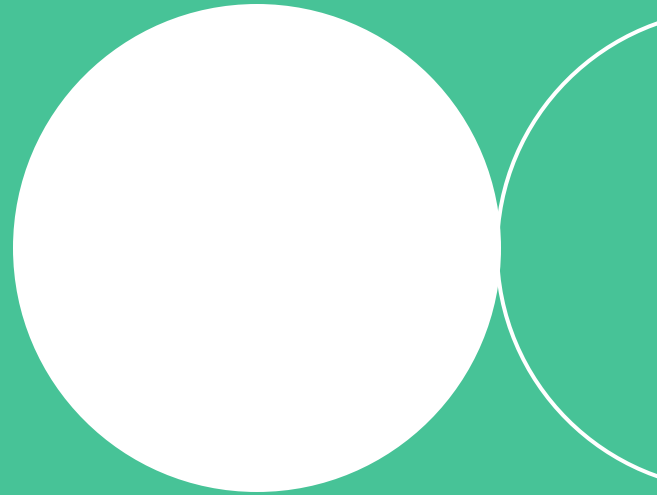


# Итоги

- 1 Домен коллизий - это участок сети, где возникают коллизии. Его нужно уменьшать насколько возможно с помощью устройств уровня L2/L3
- 2 Широковещательный домен ограничен сегментом сети, в нем все устройства имеют доступ друг к другу по аппаратному адресу
- 3 Все взаимодействие сети построено на основе широковещательного домена

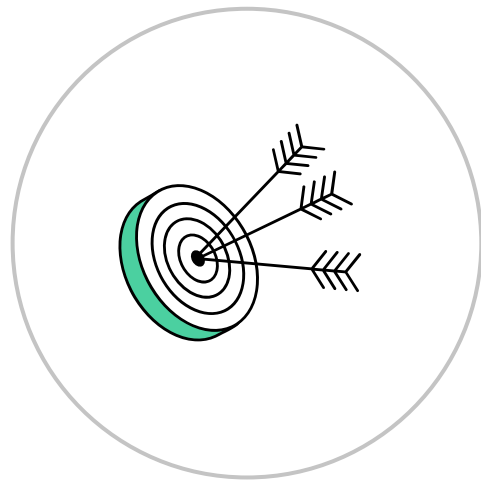


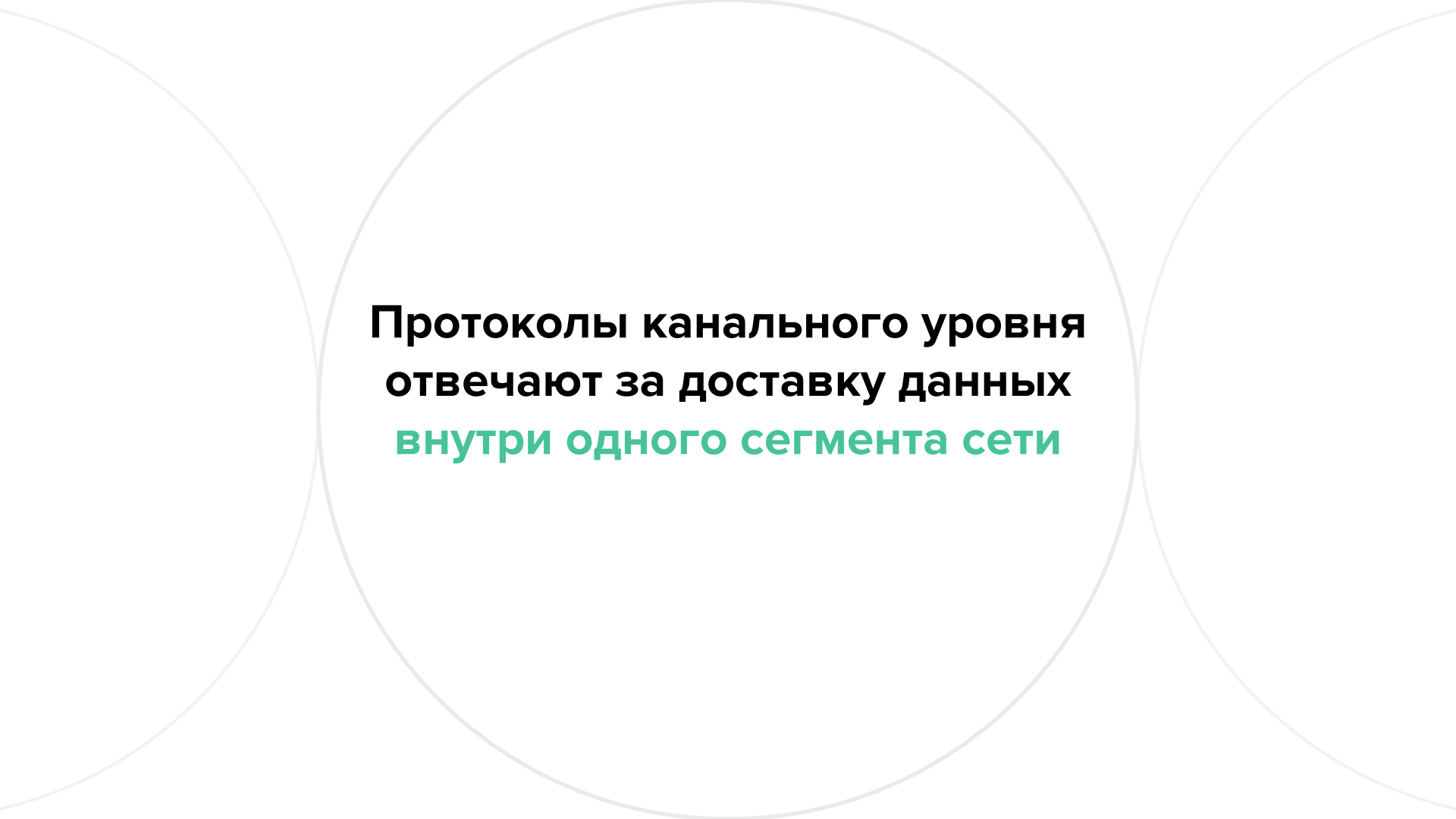
# Протокол Ethernet IEEE 802.3



# Цели темы

- Познакомиться с протоколом IEEE 802.3 Ethernet
- Узнать что такое MAC-адрес
- Разобраться с форматом кадра Ethernet
- Понять, что означает MTU





**Протоколы канального уровня  
отвечают за доставку данных  
внутри одного сегмента сети**

# Стандарт для сетей Ethernet





**Сегмент сети (согласно IEEE 802.3)**  
**электрически соединенные устройства,**  
**использующие общую среду**



# Способы соединения сегментов сети



Повторитель



Коммутатор



# Дословный перевод MAC

Media Access Control



```
graph LR; A[Media Access Control] --> B[контроль доступа к средствам массовой информации]
```


**контроль доступа к  
средствам массовой  
информации**



## MAC-адрес

**аппаратный номер оборудования (компьютера, сервера, порта коммутатора и прочее), который присваивается сетевой карте в момент его производства**





**В широковещательном домене  
сообщение фильтруется самим  
узлом по MAC-адресу**

# Формат кадра Ethernet

80 00 20 7A 3F 3E  
Destination MAC Address

80 00 20 20 3A AE  
Source MAC Address

08 00  
EtherType

**MAC Header**  
(14 bytes)

IP, ARP, etc.  
Payload

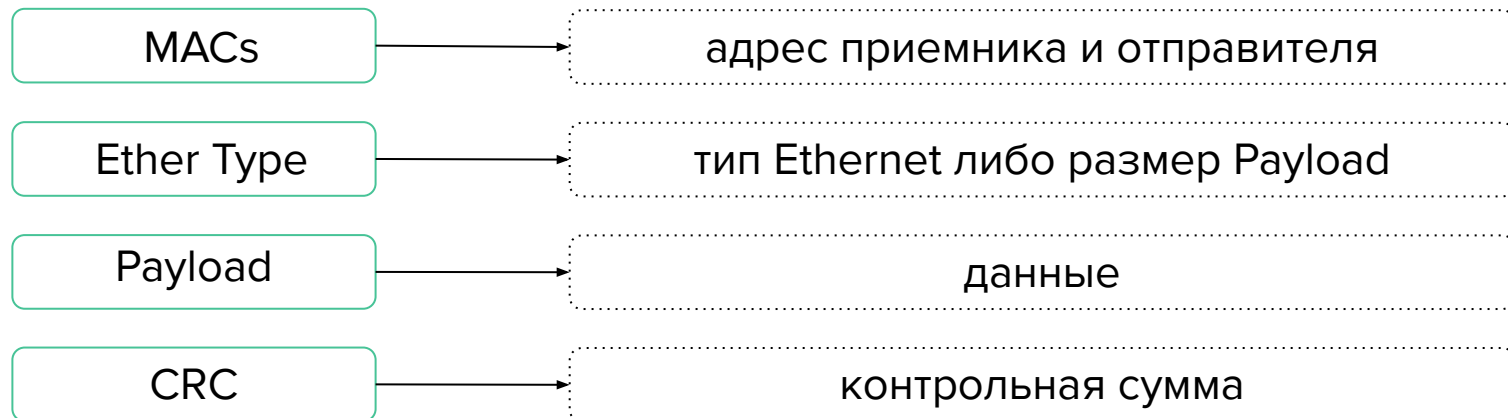
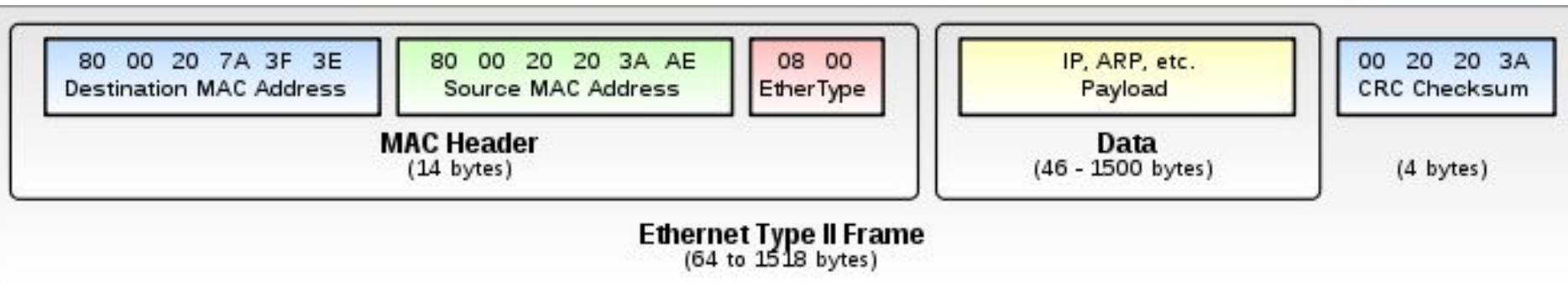
**Data**  
(46 - 1500 bytes)

00 20 20 3A  
CRC Checksum

(4 bytes)

**Ethernet Type II Frame**  
(64 to 1518 bytes)

# Формат кадра Ethernet



# Дословный перевод MTU

Maximum Transmission  
Unit

Максимальная  
единица передачи



## MTU

**максимальный размер полезного блока данных одного пакета (англ. *payload*), который может быть передан протоколом без фрагментации**



# Максимальный размер MTU

**L5**

Прикладные уровни

**L4**

Транспортный уровень

**L3**

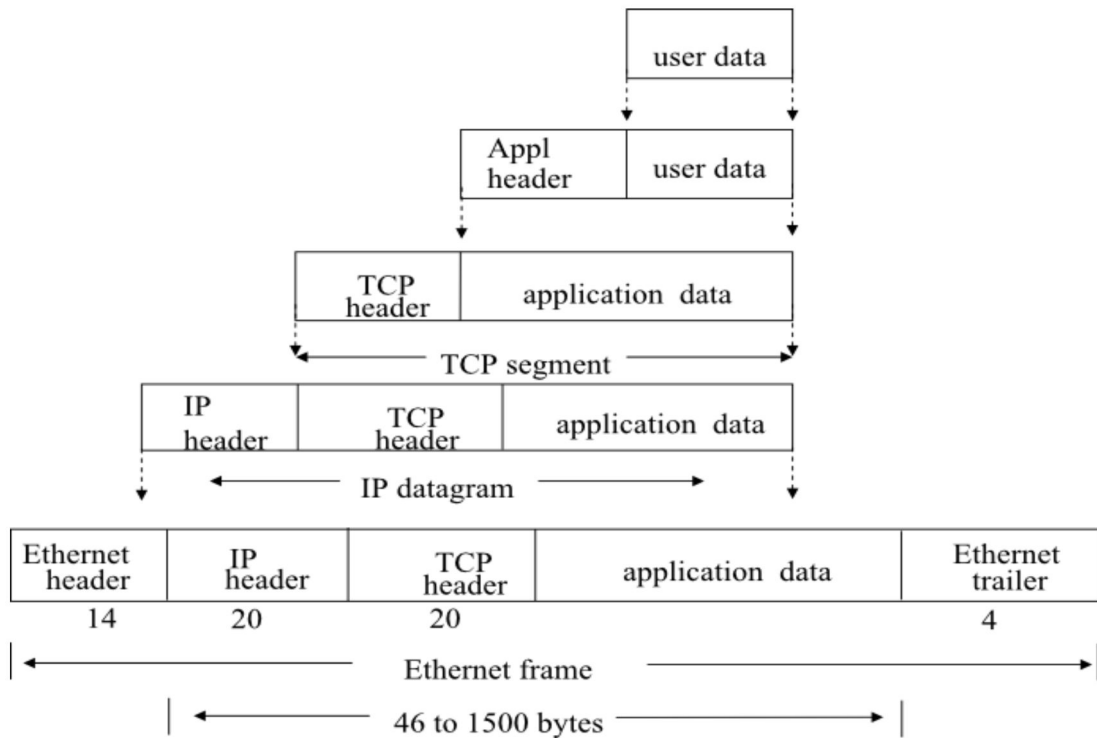
Сетевой уровень

**L2**

Канальный уровень

**L1**

Физический уровень



Источник

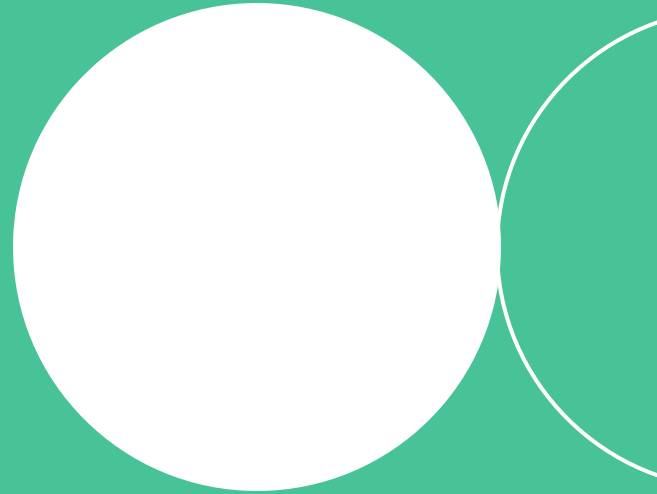


# Итоги

- 1 В рамках одного сегмента проводной сети для передачи используется протокол Ethernet
- 2 Сам протокол Ethernet для коммуникации устройств использует их MAC-адреса, обладает встроенным механизмом проверки корректности работы физического уровня L1
- 3 MTU - максимальный размер, который может быть передан протоколом без фрагментации, в большинстве сетей равен 1500 байт

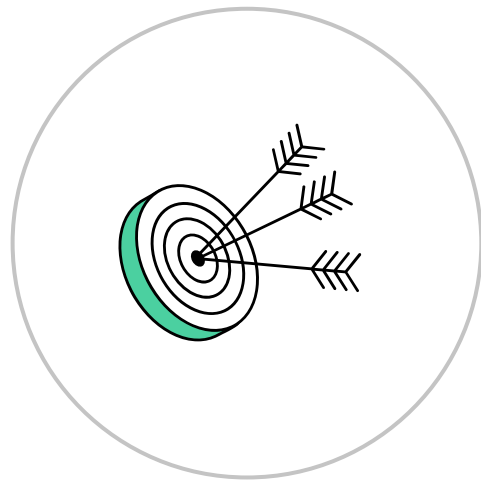


# Address Resolution Protocol



# Цели тем

- Разобраться, для чего используются широковещательные сообщения в сетях TCP/IP
- Понять взаимосвязь IP и MAC-адресов при работе протокола ARP
- Научиться работать с ARP таблицами в Linux
- Научиться проверять коннективити с помощью утилиты arping





**Что делать, если в  
коммутатор уже невозможно  
подключить новых  
участников сети, или  
они удалены по  
расстоянию?**

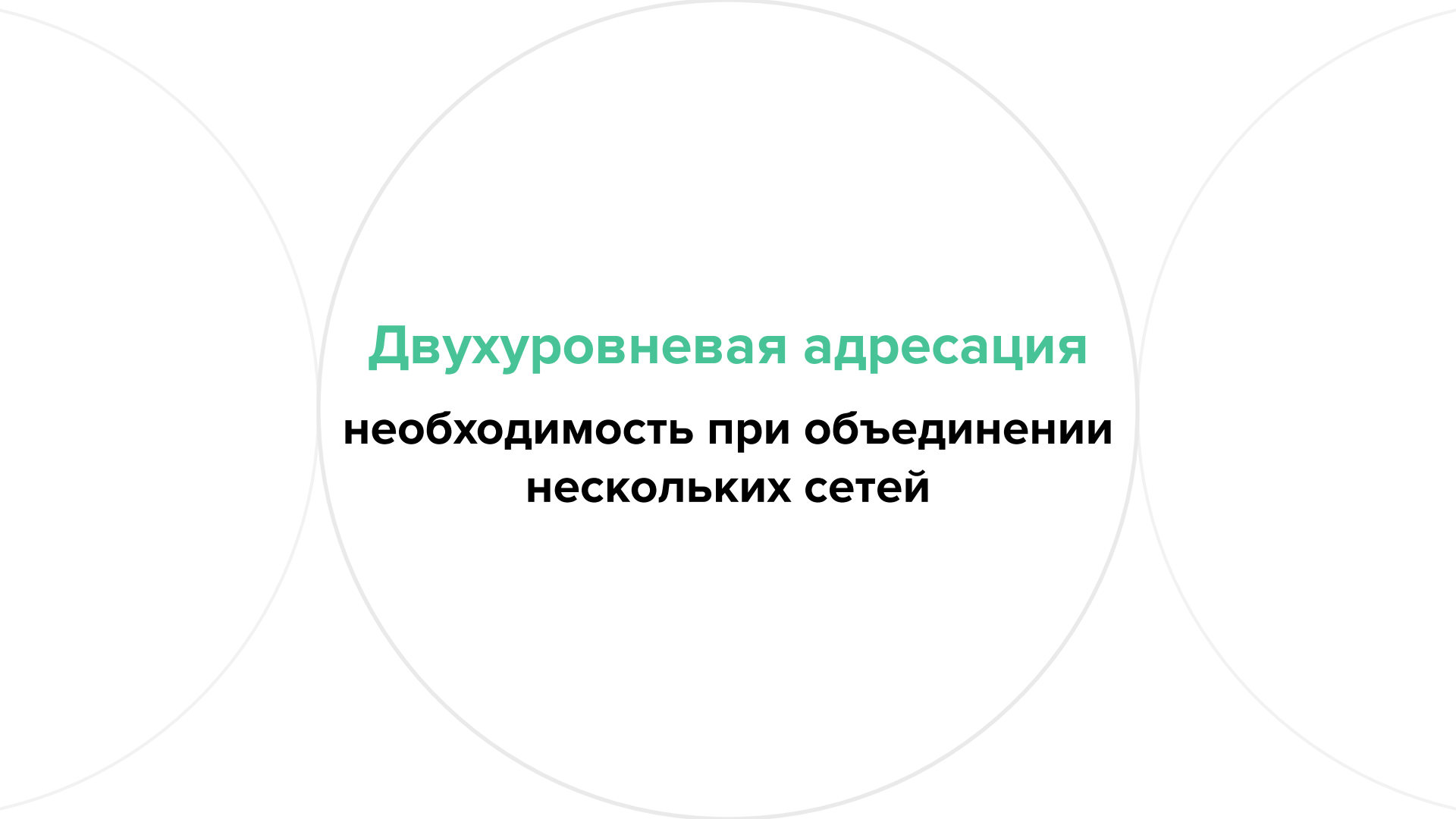
# Необходимые действия

1

Создать несколько  
локальных сетей

2

Объединить эти  
локальные сети



# **Двухуровневая адресация**

**необходимость при объединении  
нескольких сетей**



## Двухуровневая адресация

**необходима для глобальной адресации узлов интернет сети, при этом каждый узел имеет уникальный локальный адрес внутри своей сети и каждая сеть имеет свой идентификатор**





**Как между собой связаны  
MAC и IP-адреса?**



# Дословный перевод ARP

Address Resolution  
Protocol



Протокол определения  
адреса

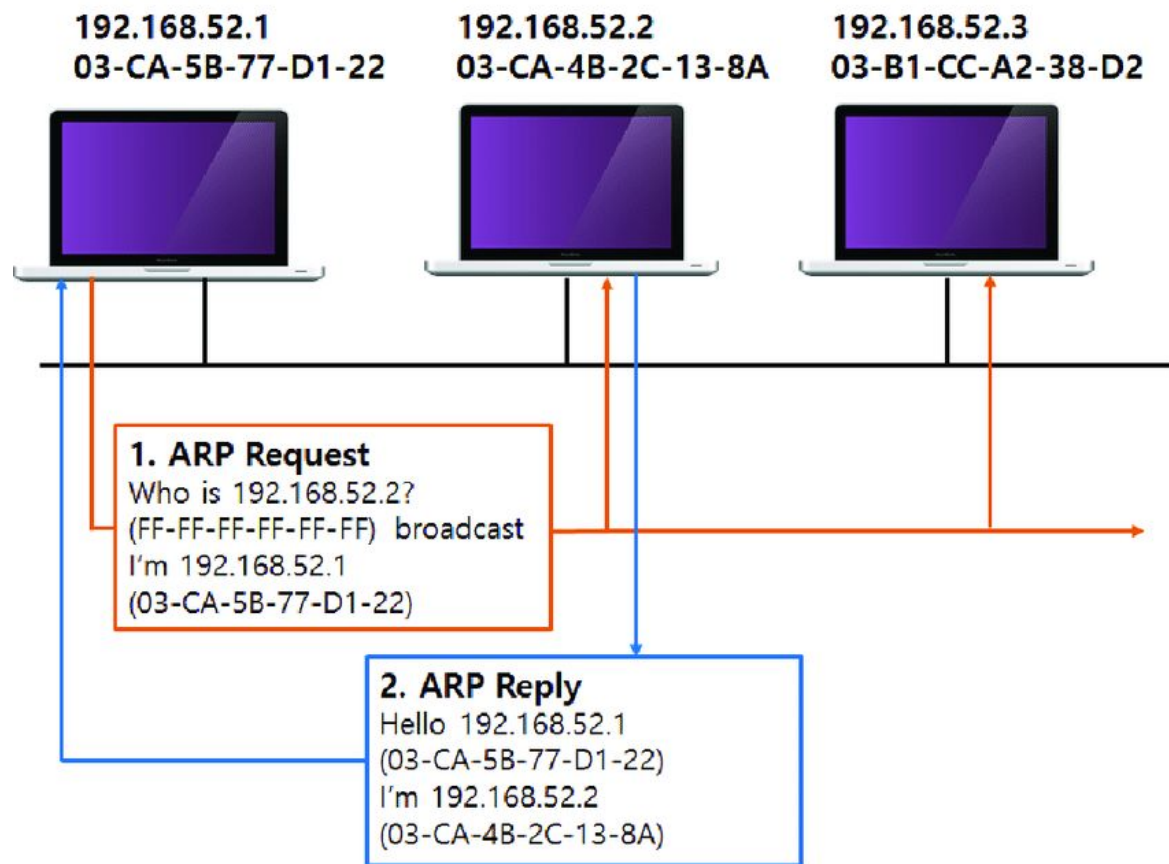


## ARP

**протокол в компьютерных сетях, предназначенный для определения IP-адреса по известному MAC-адресу узла и наоборот**



# ARP



# ARP таблица в Linux

```
# ip neigh show dev eth1

# ping -c 1 192.168.11.12
PING 192.168.11.12 (192.168.11.12) 56(84) bytes of data.
64 bytes from 192.168.11.12: icmp_seq=1 ttl=64 time=1.58 ms
--- 192.168.11.12 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.588/1.588/1.588/0.000 ms

# ip neigh show dev eth1
192.168.11.12 lladdr 08:00:27:23:22:97 REACHABLE
```

**REACHABLE**

Динамическая запись

# ARP таблица в Linux

## Добавление статической записи

```
# ip neigh add 192.168.11.100 lladdr 00:00:00:00:00:AA dev eth1  
  
# ip neigh show dev eth1  
192.168.11.100 lladdr 00:00:00:00:00:aa PERMANENT
```

**PERMANENT**

Статический характер записи

# ARP таблица в Linux

## Удаление записи

```
# ip neighb del 192.168.11.100 dev eth1
```

# ARP таблица в Linux: альтернативный способ

## Традиционная утилита ARP

```
# arp -s 192.168.11.100 00:00:00:00:00:AA
# arp -i eth1
Address HWtype HWaddress Flags Mask Iface
192.168.11.100 ether 00:00:00:00:00:aa CM eth1
# arp -d 192.168.11.100
```


# arping

## Опрос узлов на локальный сети L2

```
$ ping -c 1 10.0.2.3
PING 10.0.2.3 (10.0.2.3) 56(84) bytes of data.
..
--- 10.0.2.3 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

$ sudo arping -c 1 10.0.2.3
60 bytes from 52:54:00:12:35:03 (10.0.2.3): index=0 time=7.346 usec
--- 10.0.2.3 statistics ---
1 packets transmitted, 1 packets received, 0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.007/0.007/0.007/0.000 ms
```





**Если протокол ICMP –  
зафильтрован, мы можем  
использовать утилиту ARPING**



## Tcpdump

**утилита, позволяющая перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа**



# Опции tcpdump

1

## Опция - e

печатает заголовки  
канального уровня в каждой  
выведенной строке

2

## Опция - A

отображает на экране  
содержимое пакетов  
в формате ASCII

3

## Опция - v

при парсинге и выводе  
печатает чуть больше  
информации

4

## Опция - nn

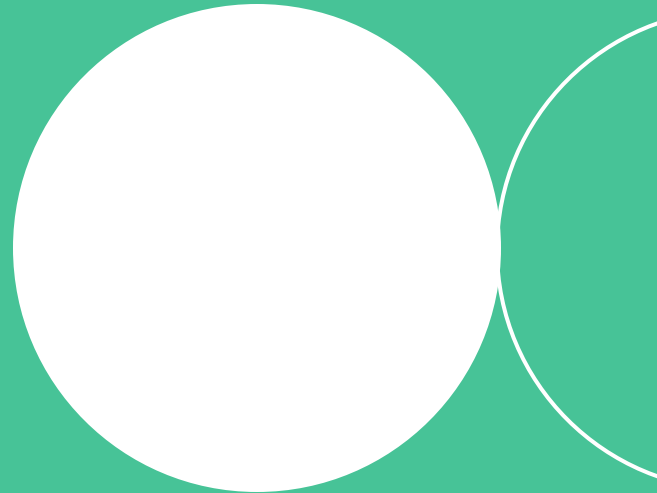
отображает порты и ip-адреса  
цифрами вместо имен  
(localhost, ssh, http и т.д.)

# Итоги

- 1 В рамках одного сегмента сети для нахождения MAC-адреса используются широковещательные запросы по протоколу ARP
- 2 Протокол ARP сопоставляет IP и MAC-адреса и составляет динамическую таблицу соответствия.
- 3 Редактирование таблицы возможно с помощью утилит `arp` и `ip`, при этом статические записи автоматически не удаляются
- 4 Связность устройств на канальном уровне L2 можно проверить с помощью утилиты `arping`. Универсальная утилита `tcpdump` может помочь в диагностике проблем на канальном уровне

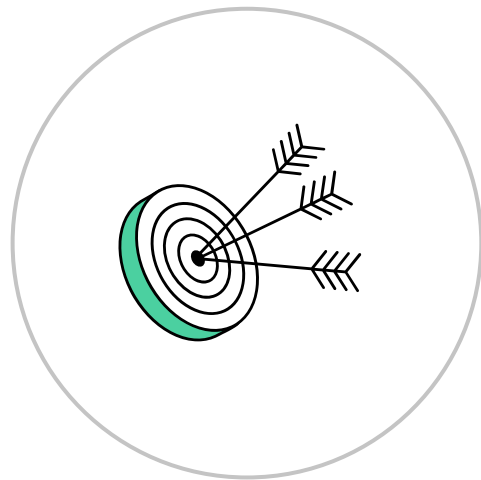


# Решение проблем широковещательного трафика: STP и VLAN



# Цели темы

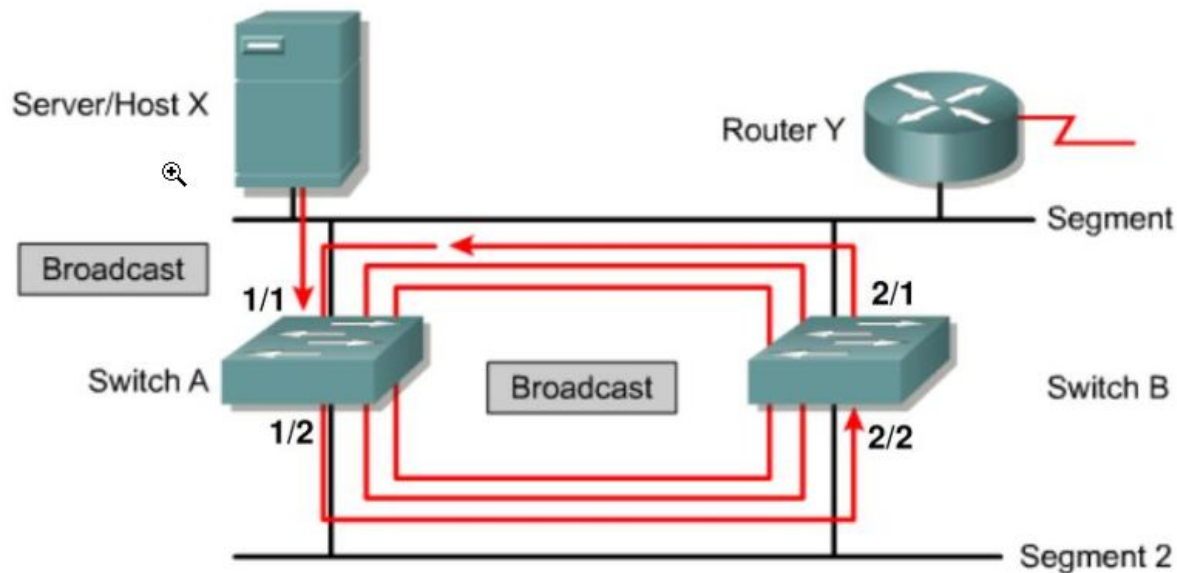
- Изучить проблемы, связанные с широковещательным трафиком и познакомиться с различными методами борьбы с ними
- Познакомиться с протоколом STP, понять основы его работы
- Разобраться с понятием VLAN и возможностями, которые предоставляет данная технология
- Научиться настраивать VLAN в Linux



# Broadcast шторм

Размножение широковещательных сообщений

Работа сети парализована



**Широковещательные пакеты  
должны составлять не более 10%  
от общего числа пакетов в сети**



# Дословный перевод STP

Spanning Tree Protocol



```
graph LR; A[Spanning Tree Protocol] --> B[Протокол остовного дерева]
```

The diagram consists of two rounded rectangular boxes connected by a horizontal arrow pointing from left to right. The left box has a solid black border and contains the text 'Spanning Tree Protocol' in a teal color. The right box has a dotted black border and contains the Russian text 'Протокол остовного дерева' in black. The arrow is a simple black line with a triangular head.

**Протокол  
остовного дерева**

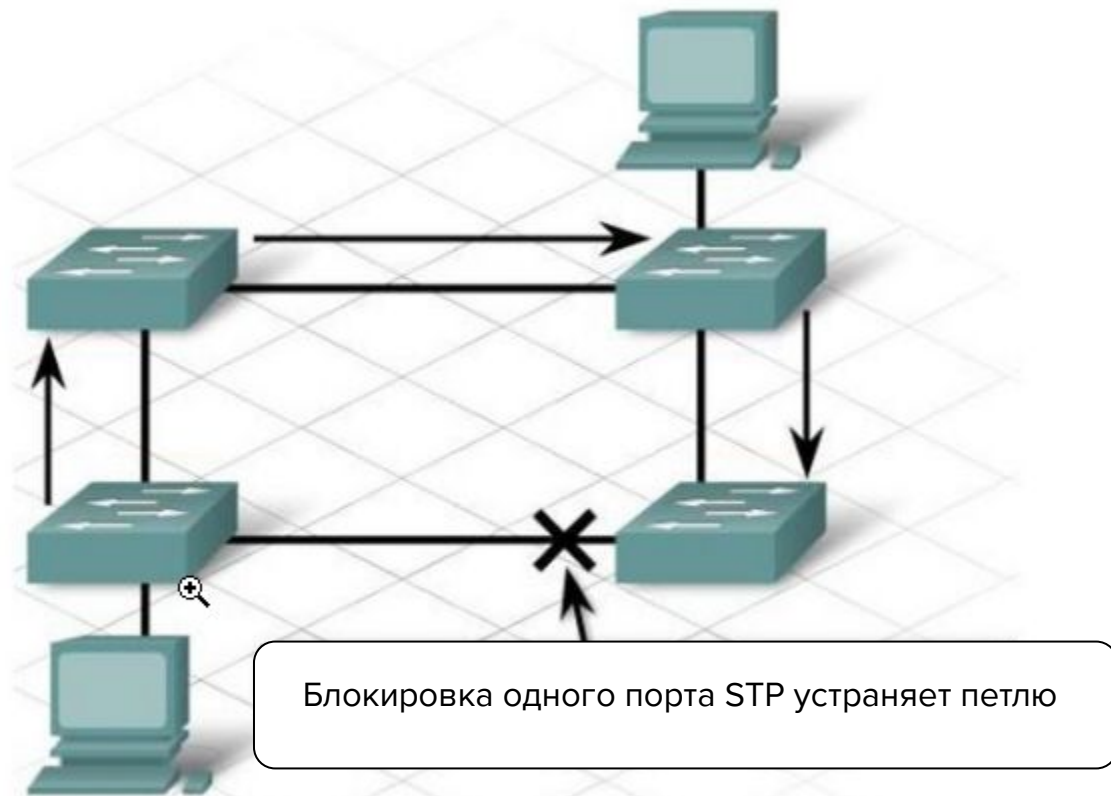


## STP

**канальный протокол, основной задачей которого является устранение петель в топологии произвольной сети Ethernet**



# Схема работы STP



# Дословный перевод LAN

Local Area Network

**Локальная  
вычислительная сеть**

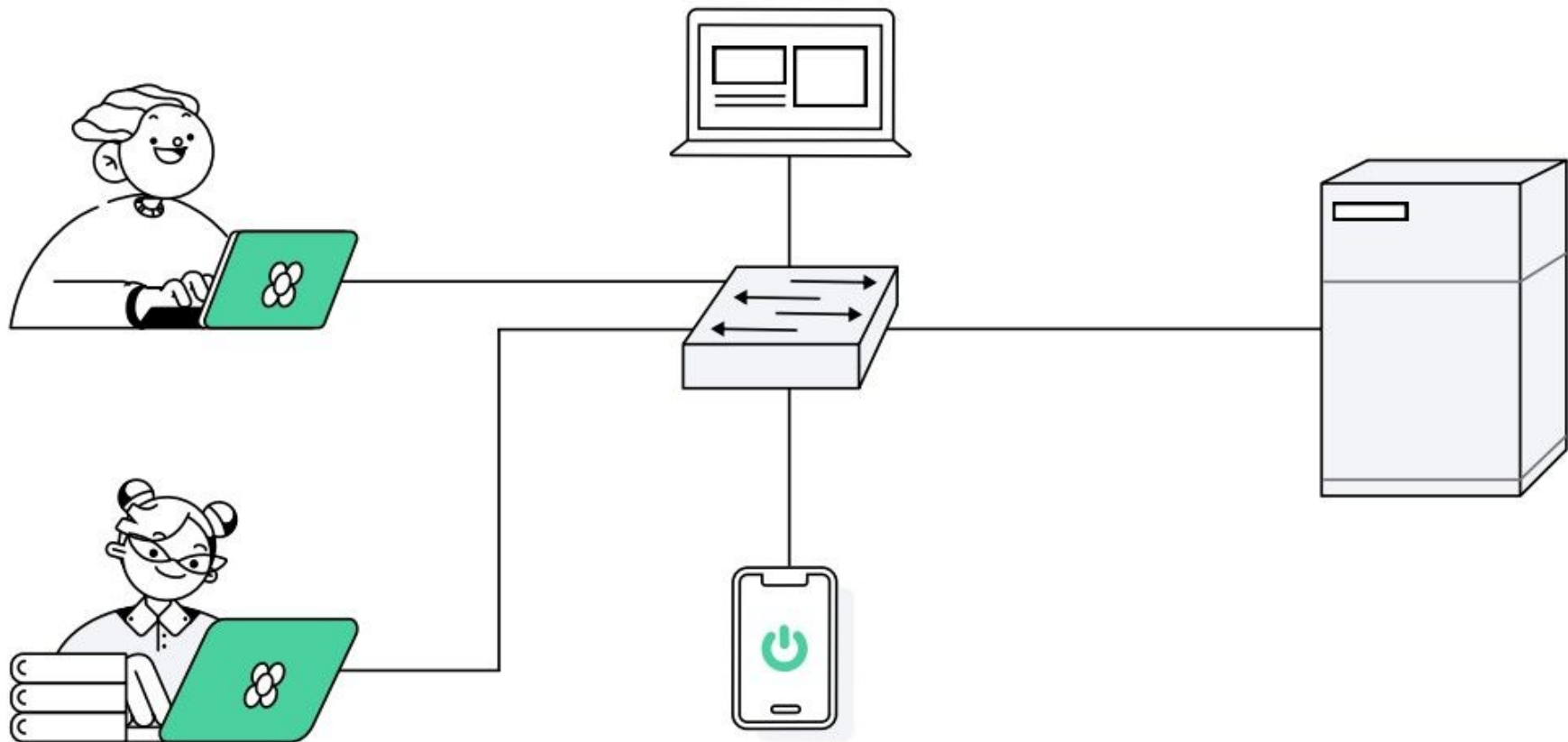


## LAN

**локальная компьютерная сеть, соединяющая компьютеры на небольшой территории, такой как офисные здания, университеты, здания**



# Схема LAN



# Дословный перевод VLAN

Virtual Local Area  
Network

Виртуальная локальная  
вычислительная сеть



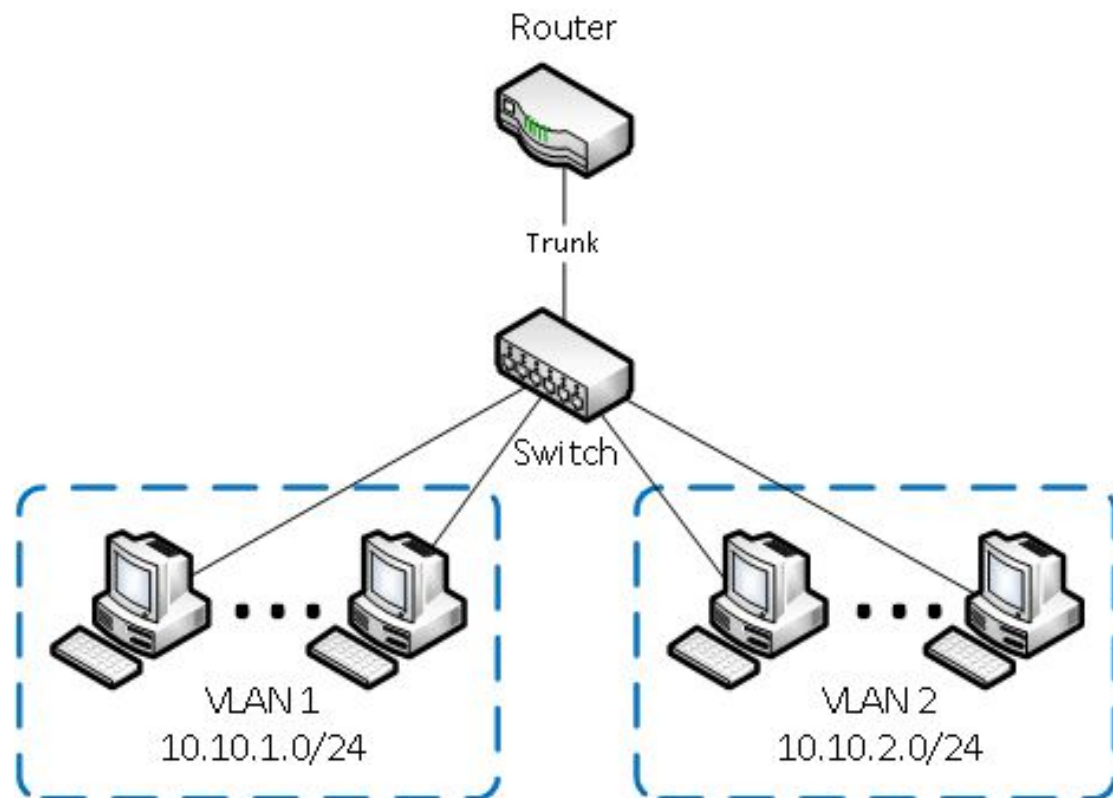
## VLAN

**логически обособленный сегмент локальной сети  
внутри одной физической сети**

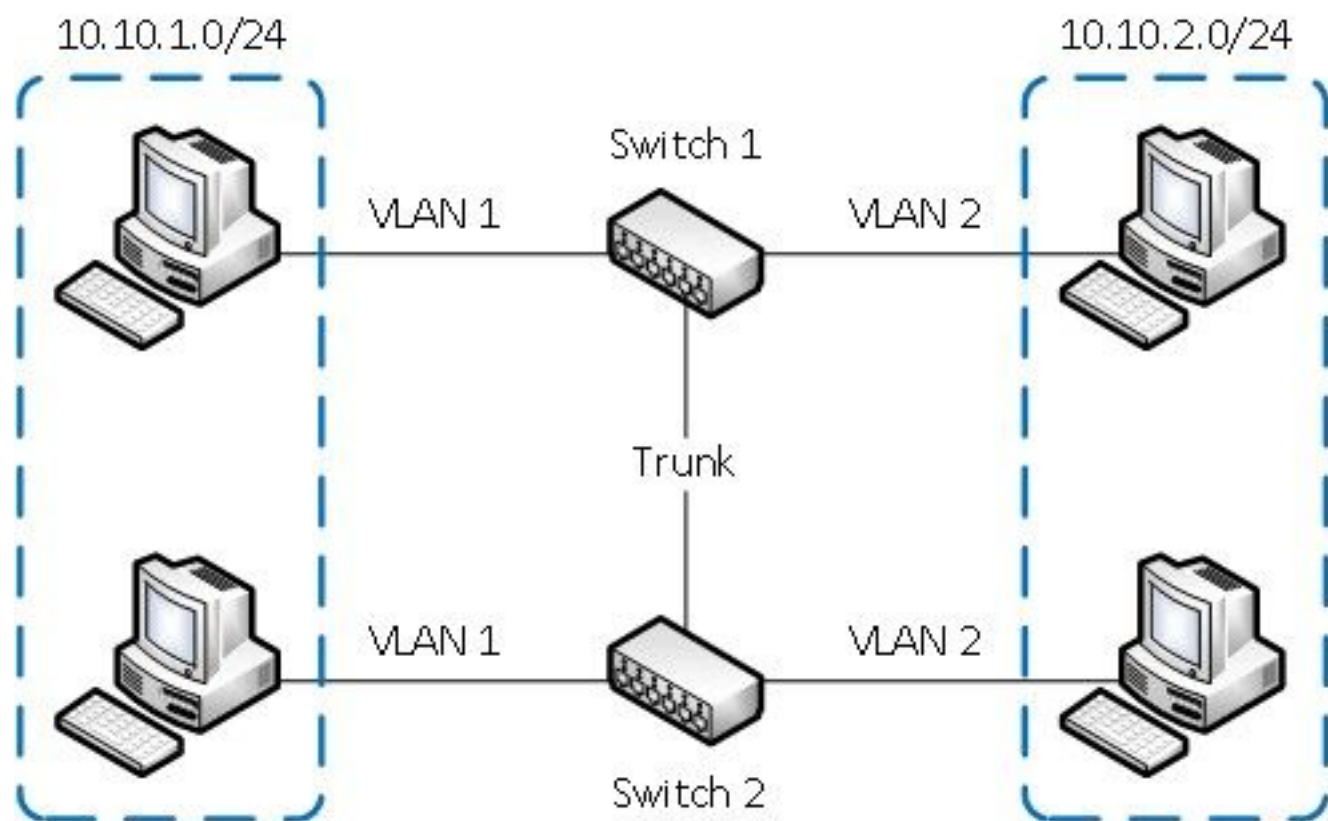




# Схема VLAN



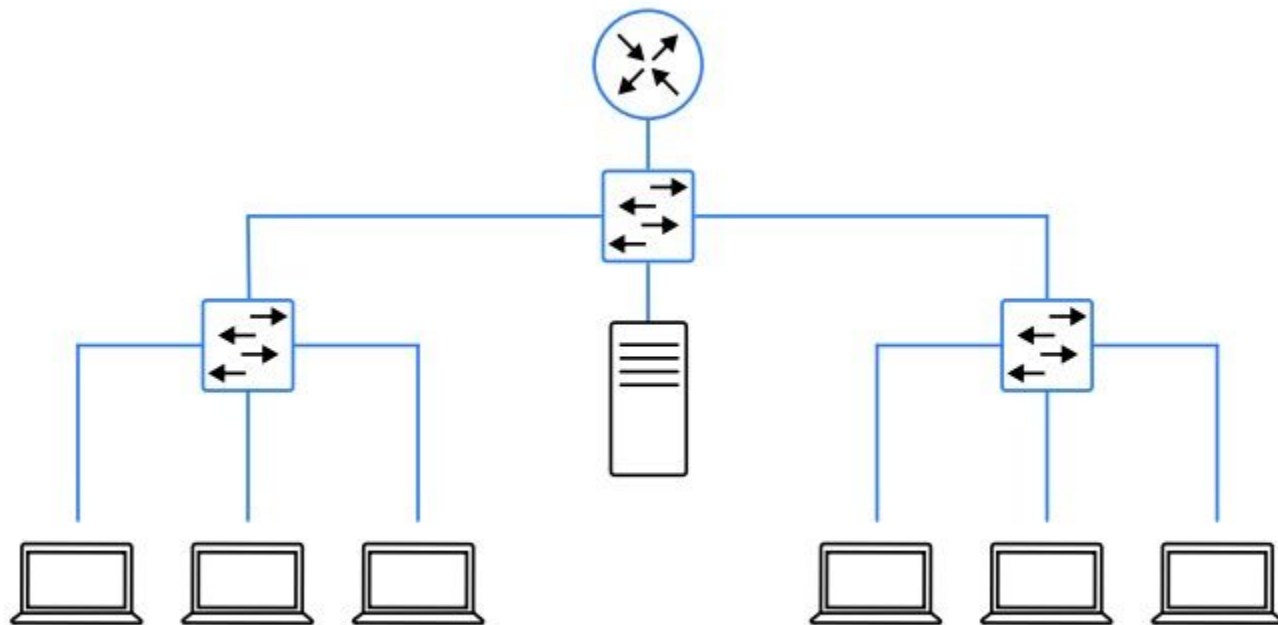
# Схема VLAN





**Как решить проблему  
роста сети?**

# Исходная сеть



# Варианты решения

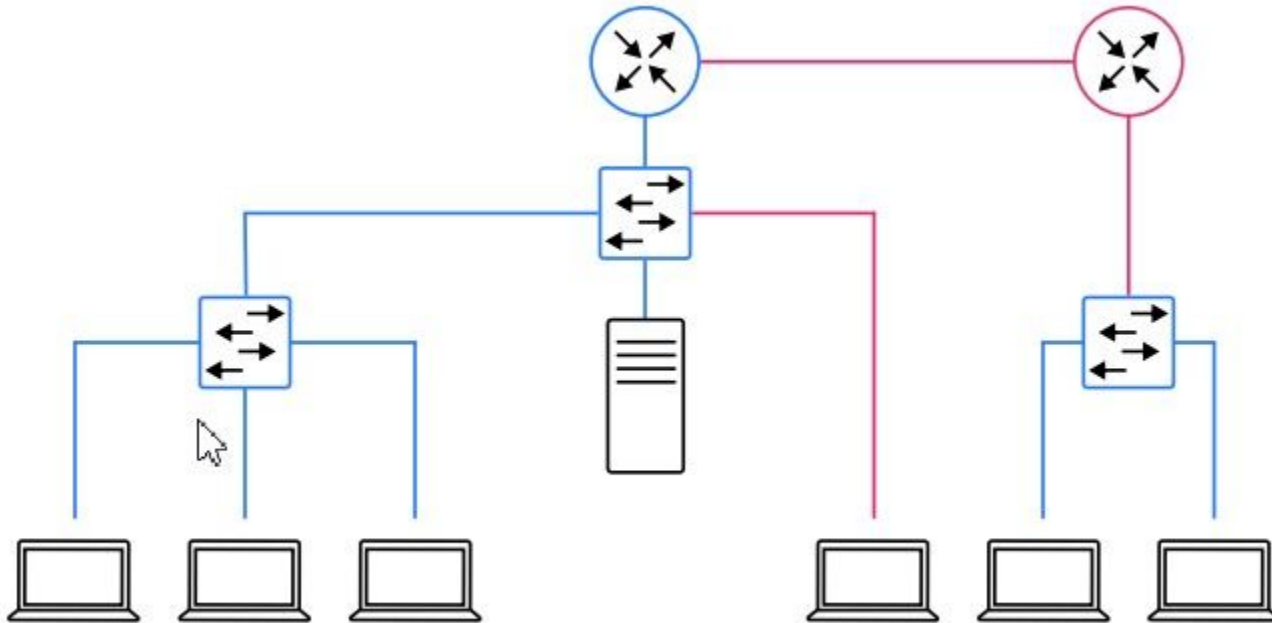
1

Физическое  
разделение сетей

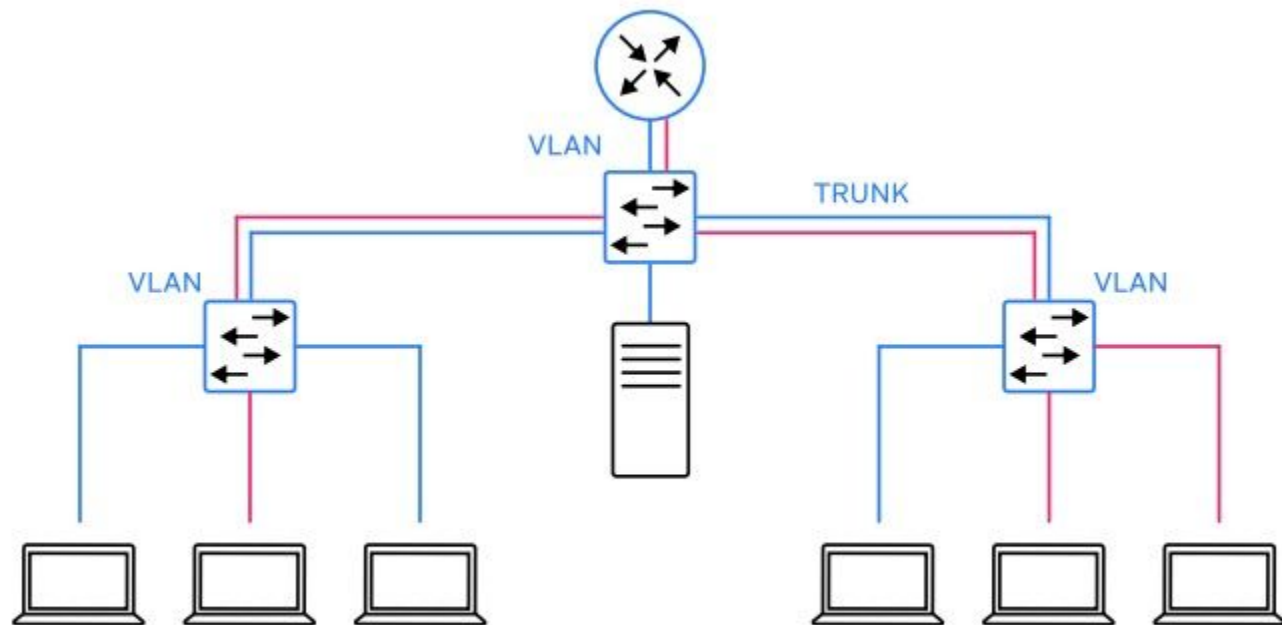
2

Логическое  
(виртуальное)  
обособление

# Решение # 1: физическое разделение сетей



## Решение # 2: виртуальное разделение сетей



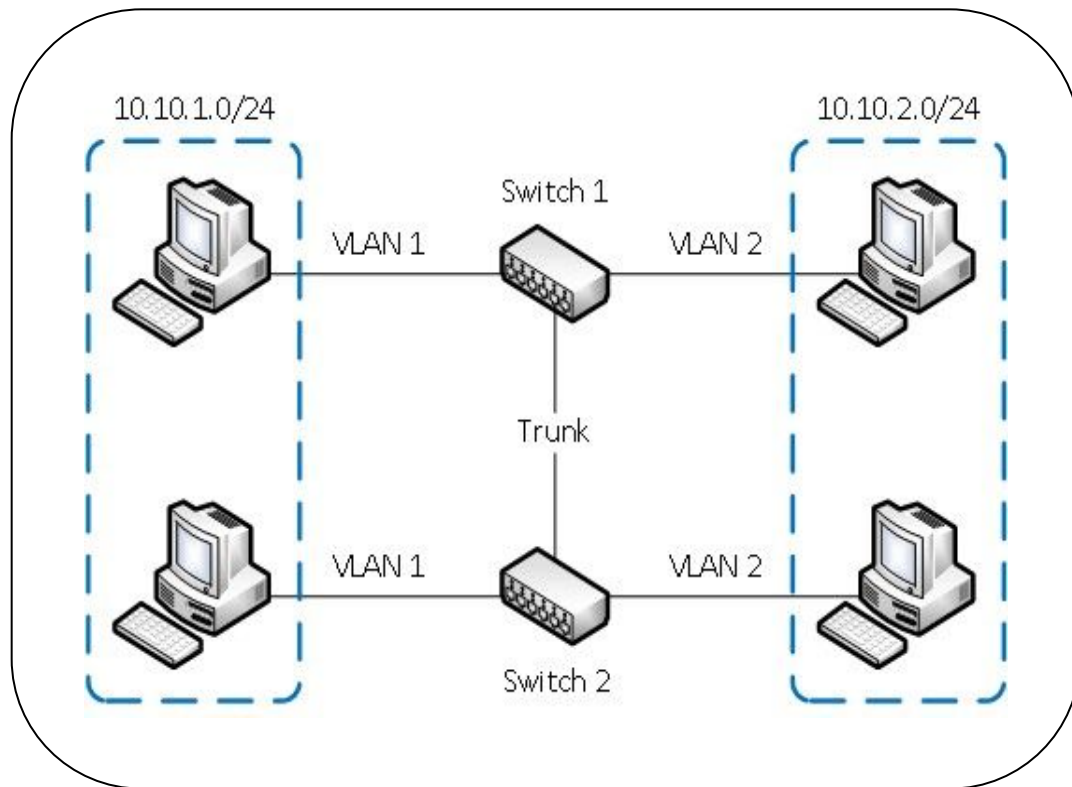
# VLAN

**технология, которая позволяет  
строить виртуальные сети с  
независимой от физических  
устройств топологией**



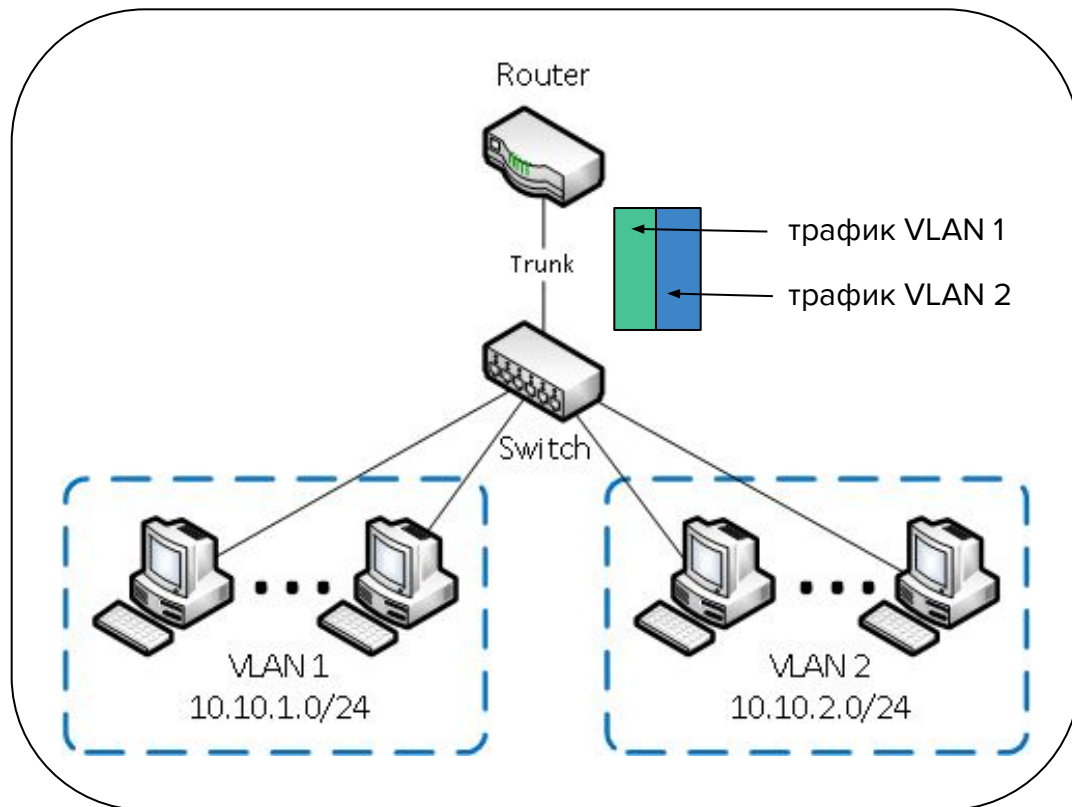
# Возможности VLAN

Объединить в единую сеть  
группы компьютеров,  
подключенных к разным  
коммутаторам



# Возможности VLAN

Разделить на разные сети компьютеры, подключенные к одному коммутатору



# Преимущества VLAN

- сокращение числа широковещательных запросов, которые снижают пропускную способность сети
- повышение безопасности каждой виртуальной сети
- создание новой виртуальной сети без прокладки кабеля и покупки коммутатора
- объединение в одну сеть компьютеров, подключенных к разным коммутаторам
- упрощение сетевого администрирования

# Пример VLAN с однократным запуском

```
lsmod | grep 8021q  
sudo modprobe 8021q # если появляется ошибка "Maybe you need to load the 8021q module"
```

```
# ip link add link eth0 name eth0.10 type vlan id 10  
# ip -d link show eth0.10
```

```
[root@localhost ~]# ip -d link show eth0.10  
4: eth0.10@eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group default qlen 1000  
    link/ether 52:02:a4:e3:26:b5 brd ff:ff:ff:ff:ff:ff promiscuity 0  
    vlan protocol 802.1Q id 10 <REORDER_HDR> addrngenmode eui64 numtxqueues 1 numrxqueues 1 gso_max_size 65536 gso_max_segs 65535  
[root@localhost ~]#
```

```
# ip addr add 192.168.1.200/24 brd 192.168.1.255 dev eth0.10  
# ip link set dev eth0.10 up  
  
# ip link set dev eth0.10 down  
# ip link delete eth0.10
```

# Пример VLAN с однократным запуском

- загружаем модуль ядра 8021q
- создаем новый виртуальный интерфейс с нужной меткой
- назначаем IP адрес
- поднимаем интерфейс
- после работы - удаляем его

# Пример VLAN с многократным запуском

```
# nano /etc/netplan/01-netcfg.yaml
network:
  version: 2
  ethernets:
    eth0:
      dhcp4: true
  vlans:
    vlan200:
      id: 200
      link: eth0
      dhcp4: no
      addresses: [192.168.200.2/24]
      gateway4: 192.168.200.1
      routes:
        - to: 192.168.100.1/24
          via: 192.168.200.3
          on-link: true
```

# Пример VLAN с многократным запуском

- включаем загрузку модуля ядра 8021q при старте системы
- создаем новую автоматическую конфигурацию виртуального интерфейса с нужной меткой:
  - для Debian через конфигурацию `/etc/network/interfaces`
  - для CentOS через создание конфигурации в `/etc/sysconfig/network-scripts/ifcfg-vlan**`
  - для Ubuntu(версии начиная с 17.10) через редактирование `/etc/netplan/*.yaml`

`ifcfg-vlan**` – необходимая метка

`*.yaml` – имя конфигурации

# Итоги

- 1 На ранних этапах развития сетей широковещательных трафик представлял угрозу возникновения broadcast-шторма. Для борьбы с этим используются различные вариации протокола STP
- 2 В современных сетях широковещательных трафик может серьезно снижать пропускную способность сетей при большом количестве устройств в сегменте сети
- 3 Уменьшение сегмента сети возможно с помощью физического изменения топологии и добавления новых





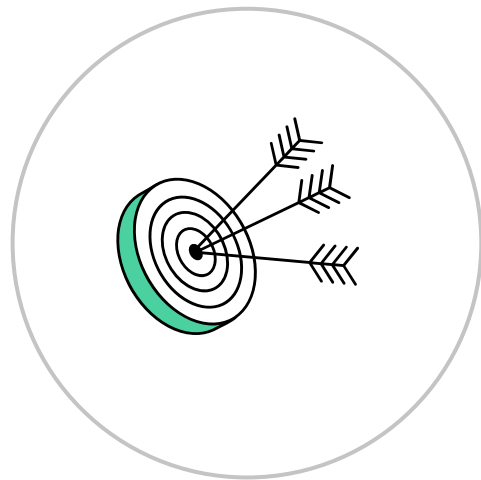
# Итоги

- 4 VLAN позволяет гибко настраивать сеть для достижения максимальных характеристик пропускной способности и безопасности
- 5 В Linux VLAN можно настроить вручную либо через автоматическую сетевую конфигурацию (в зависимости от дистрибутива)



# Общий итоги занятия

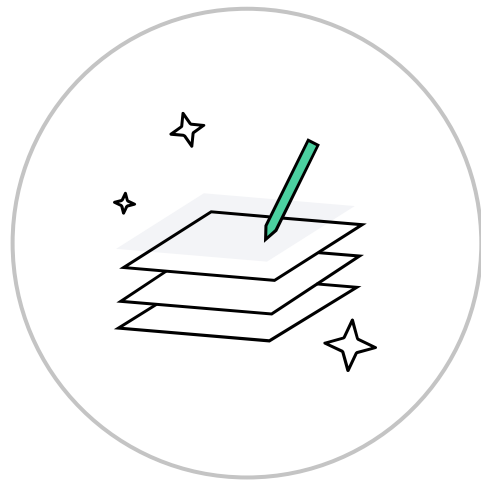
- Разобрались в основах работы канального уровня модели OSI
- Изучили различные среды, используемые для передачи данных
- Поняли принципы работы протокола Ethernet
- Изучили протокол ARP
- Научились работать с ARP-таблицами и проверять коннективити с помощью утилиты arping
- Познакомились с проблематикой служебного трафика и методами ее решения через протоколы SRP и VLAN
- Научились настраивать VLAN в Linux



# Домашнее задание

## Давайте посмотрим вашу практику после лекции

- 1 Практика состоит из обязательного теста и домашнего задания со звездочкой (необязательное)
- 2 В тесте 14 вопросов, на 10 нужно ответить верно. Есть 2 попытки
- 3 Вопросы по домашнему заданию со звездочкой задавайте в чате группы
- 4 Задачи можно сдавать по частям.  
Зачёт по домашней работе ставят после того, как приняты все задачи



# Задавайте вопросы. Оставляйте обратную связь по вебинару

Ильмир Сахипов  
Руководитель центра управления сетью АО “Уфанет”

