



# Глава 1. Введение в коммутируемые сети



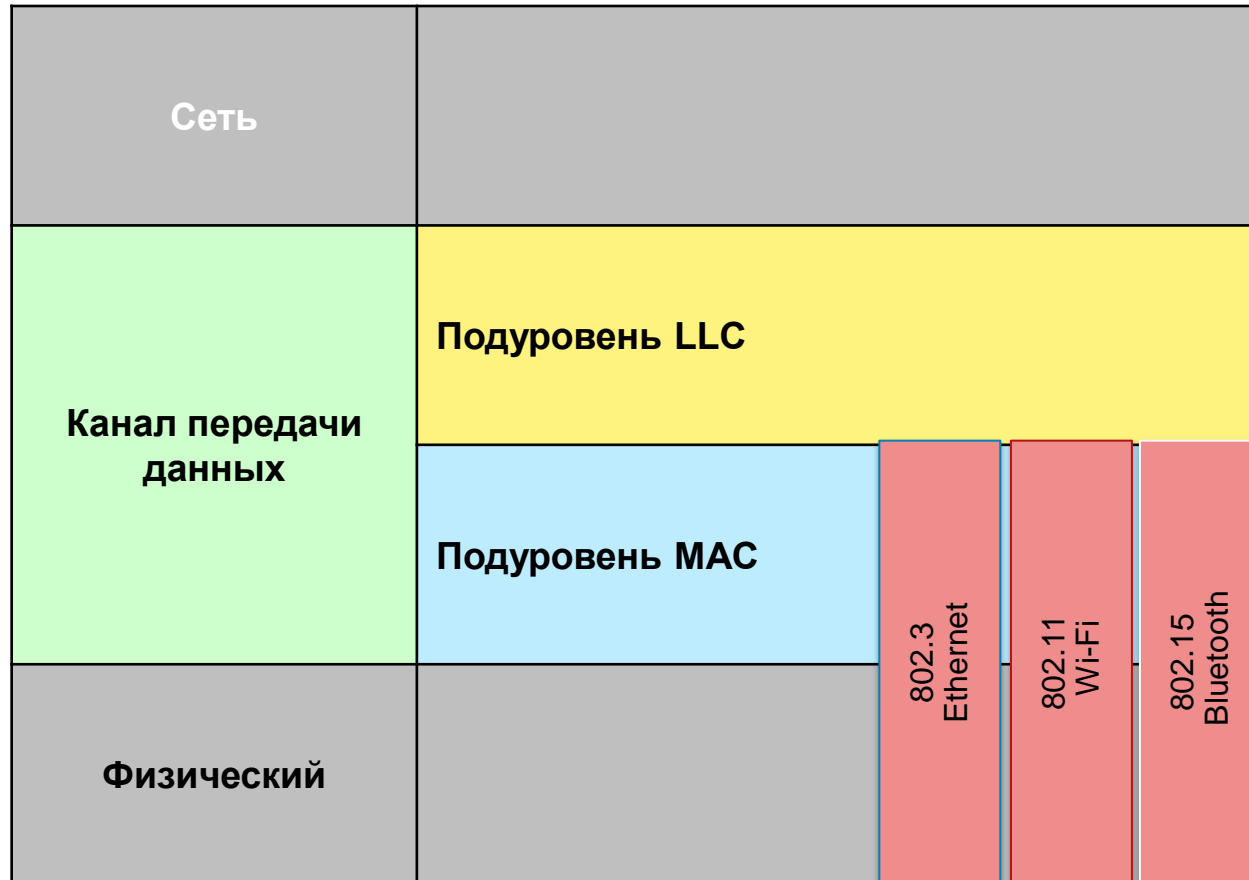
## Канальный уровень и технология VLAN

Cisco | Networking Academy®  
Mind Wide Open™



## Назначение канального уровня

# Подуровни канального уровня

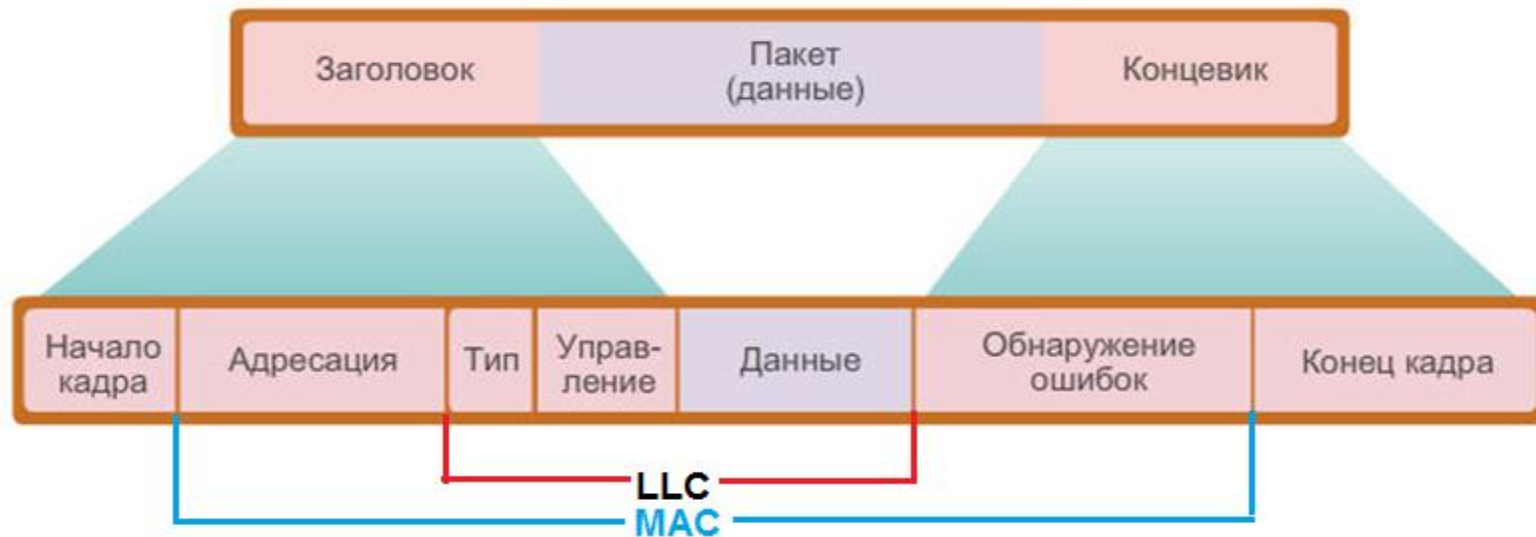


Состоит из двух подуровней:

- управления логическим каналом (**Logical Link Control**, LLC);
- управления доступом к среде (**Media Access Control**, MAC).



# Обобщенный формат кадра канального уровня

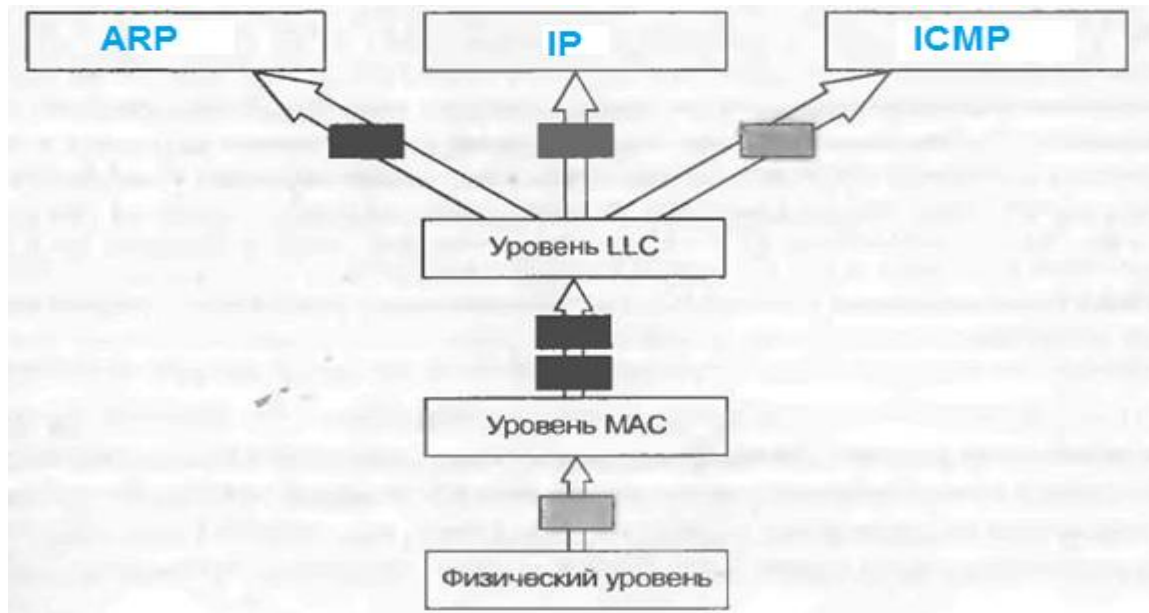


- **LLC** - управления логическим каналом (**Logical Link Control**):
  - **Тип** протокола сетевого уровня, данные которого находятся в пакете
  - **Управление** приоритетом кадра и потоком кадров
  - **Исправление** ошибок передачи
- **MAC** - управления доступом к среде (**Media Access Control**) добавляет:
  - Поле с аппаратными **MAC-адресами**
  - Поле для обнаружение **ошибок передачи**.

Каждая сетевая технология имеет свой формат кадра канального уровня



# Уровень LLC



## ■ Уровень LLC:

- **Распределение данных кадров** по различным протоколам верхнего уровня (IP, ICMP, ARP );
- **Обеспечение требуемой надежности** (*исправление ошибок*)
- **и управление потоком** (предотвращение «затопления» медленного получателя быстрым отправителем);
- Реализуется **программно**, драйвером сетевой карты



# Подуровень МАС

- Основные функции :
  - **определение доступности** общей разделяемой физической среды передачи и разрешение коллизий;
  - **адресация узлов** сети с помощью аппаратных адресов МАС – адресов (*чтобы знать кому передавать в общей среде*) ;
  - **конечная упаковка/распаковка кадра**
- **Обнаружение ошибок.**
- Реализуется аппаратно, сетевой картой



# Обнаружение и исправление ошибок

- Обнаружение ошибок
  - Контрольная сумма
- Исправление ошибок
  - Избыточные коды коррекции ошибок
  - Позволяют исправлять ошибки
- Повторная отправка кадра
  - Требуется наличия подтверждения о приеме кадра
  - Если обнаружена ошибка или кадр «потерялся» - подтверждения нет и кадр передается повторно



# Технологии канального уровня в локальных сетях

- Современные:
  - Ethernet
  - WI-FI
  - PPP
  
- Устаревшие:
  - Token Ring
  - ATM
  - FDDI
  - 100VG-AnyLan



# Кадр протокола «точка-точка»

## Протокол PPP (протокол «точка-точка»)

Распространённый протокол канального уровня для глобальных сетей

Кадр						
Имя поля	Флаг	Адрес	Управление	Протокол	Данные	Контрольная последовательность кадра (FCS)
Размер	1 байт	1 байт	1 байт	2 байта	переменная	2 или 4 байта

**Флаг** — один байт, который указывает начало и конец кадра. Поле флага состоит из двоичной последовательности 01111110.

**Адрес** — один байт, который содержит стандартный адрес широковещательной рассылки PPP. PPP не назначает отдельные адреса станции.

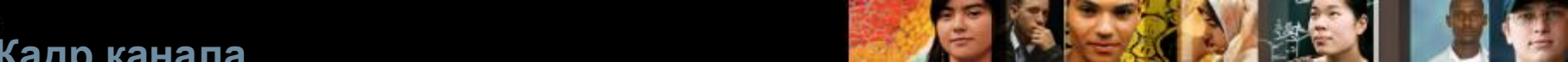
**Управление** — один байт, содержащий двоичную последовательность 00000011, которая требует передачи пользовательских данных в непоследовательном кадре.

**Протокол** — два байта, которые идентифицируют протокол, инкапсулированный в поле данных кадра. Последние значения поля протокола определены в последнем документе установленных номеров (RFC).

**Данные** — ноль или несколько байт, содержащие дейтаграмму по протоколу, указанному в поле протокола.

**Контрольная последовательность кадра (FCS)** — как правило, 16 битов (2 байта). Согласно прежнему соглашению внедрения PPP могут использовать 32-битную версию (4 байта) контрольной последовательности кадра для эффективного обнаружения ошибок.





# Кадр Ethernet

## Протокол Ethernet

Распространённый протокол канального уровня для локальной сети

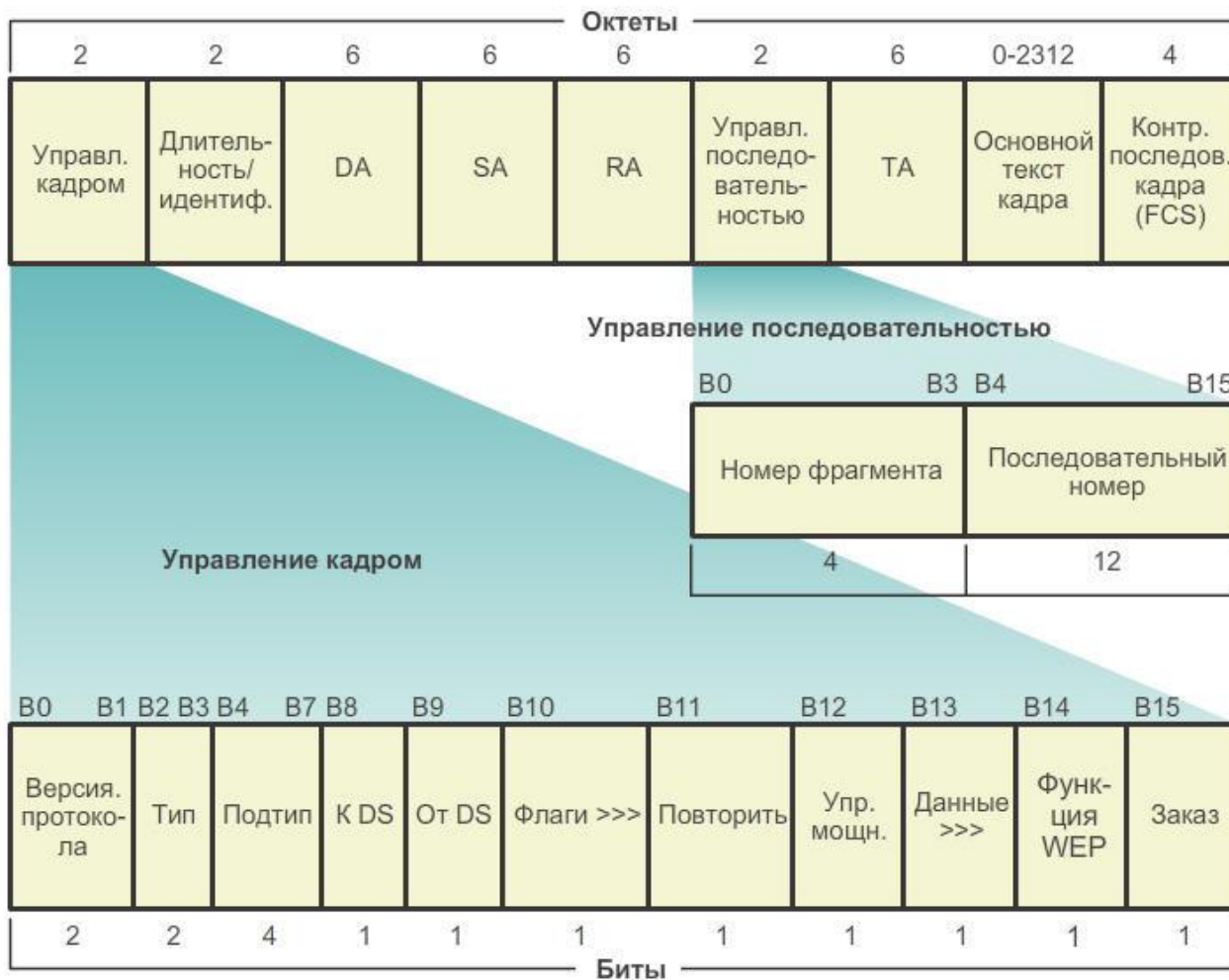
Кадр						
Имя поля	Преамбула	Назначение	Источник	Тип	Данные	Контроль- ная последова- тельность кадра
Размер	8 байт	6 байт	6 байт	2 байта	от 46 до 1500 байт	4 байта

- Преамбула** — используется для синхронизации; также содержит разделитель, отмечающий конец информации о временных параметрах
- Адрес назначения** — 48-битный MAC-адрес узла назначения
- Адрес источника** — 48-битный MAC-адрес узла источника
- Тип** — значение, указывающее, какой протокол верхнего уровня получит данные после завершения процесса Ethernet
- Данные или полезная нагрузка** — протокольный блок данных, как правило, пакет IPv4, который предназначен для передачи по среде.
- Контрольная последовательность кадра (FCS)** — значение, используемое для поиска повреждённых кадров



# Кадр беспроводной сети 802.11

Протокол беспроводной локальной сети 802.11





# MAC-адреса

- Служат для идентификации сетевых интерфейсов узлов сети
  - Ethernet
  - Wi-Fi
  
- Регламентированы стандартом IEEE 802
  - Длина 6 байт (48 бит)
  
- Форма записи – шесть шестнадцатеричных чисел:
  - 1C-75-08-D2-49-45
  - 1C: 75: 08: D2: 49: 45



# Типы MAC-адресов

- Индивидуальный (unicast):
  - 30-9C-23-15-E8-8C
  
- Групповой (multicast)- первый бит старшего байта равен 1:
  - Для IPv4 : 01-00-5E-XX-XX-XX (XX последние 23 бита группового IPv4-адреса)
  - Для IPv6 : 33-33-XX-XX-XX-XX (XX последние 32 бита группового IPv6-адреса) **FF02::2 =33-33-00-00-00-02;FF02::1:FF5C:B300= 33-33-FF-5C-B3-00**
  
- Широковещательный
  - FF-FF-FF-FF-FF-FF



# ТЕХНОЛОГИЯ Ethernet



# Разновидности Ethernet

Название	Скорость	Кабель	Стандарт
Ethernet	10 Мб/с	«Толстый», «тонкий» коаксиал, витая пара, оптика	802.3
Fast Ethernet	100 Мб/с	Витая пара, оптика	802.3u
Gigabit Ethernet	1 Гб/с	Витая пара, оптика	802.3z, 802.3ab
5G Ethernet	2,5 Гб/с 5 Гб/с	Витая пара	802.3bz
10G Ethernet	10 Гб/с	Витая пара, оптика	802.3ae, 802.3an
100G Ethernet	40 Гб/с 100 Гб/с	Оптика	802.3ba



# Форматы кадров Ethernet

**Кадр 802.3/LLC**

6	6	2	1	1	1(2)	46-1497 (1496)	4
DA	SA	L	DSAP	SSAP	Control	Data	FCS
Заголовок LLC							

**Кадр Raw 802.3/Novell 802.3**

6	6	2	46-1500	4
DA	SA	L	Data	FCS

**Кадр Ethernet DIX (II)**

6	6	2	46-1500	4
DA	SA	T	Data	FCS

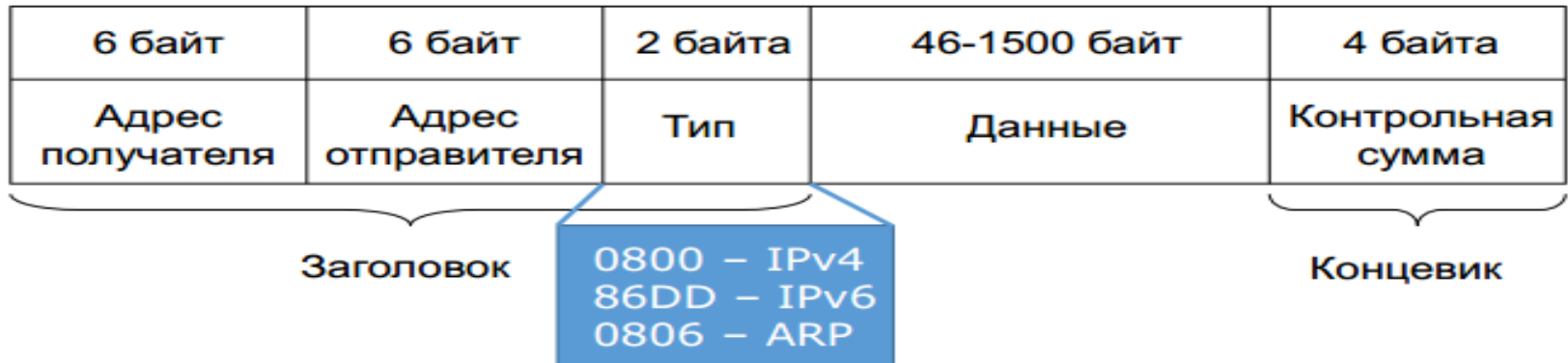
**Кадр Ethernet SNAP**

6	6	2	1	1	1	3	2	46-1492	4
DA	SA	L	DSAP	SSAP	Control	OUI	T	Data	FCS
			AA	AA	03	000000			
Заголовок LLC						Заголовок SNAP			

- Реально используется кадр Ethernet II (DIX)



# Ethernet II (DIX)



- Максимальная длина поля данных 1500 байт
  - Выбрана разработчиками Ethernet
  - Ограничение на размер памяти для буфера
  - Существует расширение JumboFrame (до 9000 байт)
- Минимальная длина 46 байт (512 для 1Гб/сек)
  - Ограничение технологии Ethernet
  - Меньше нельзя, коллизии не обнаружатся.





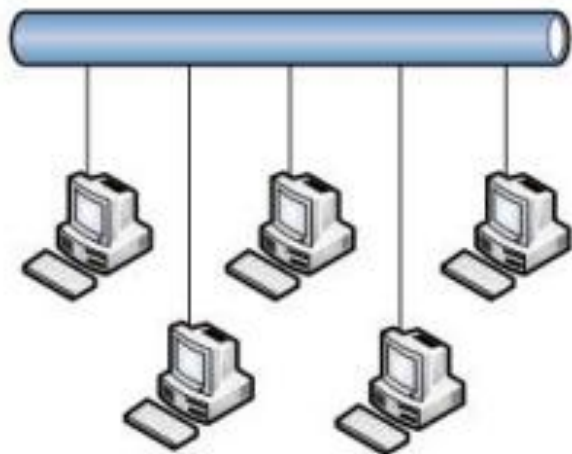
# Ethernet

- Классический Ethernet (1973г)
  - Разделяемая среда и коллизии
  - Метод CSMA/CD
  - Плохая масштабируемость и безопасность
  - Концентраторы (HUB) работает на физическом уровне
  
- Коммутируемый Ethernet (1995 Fast Ethernet)
  - Нет разделяемой среды, нет коллизий
  - Мосты и коммутаторы – работают на канальном уровне

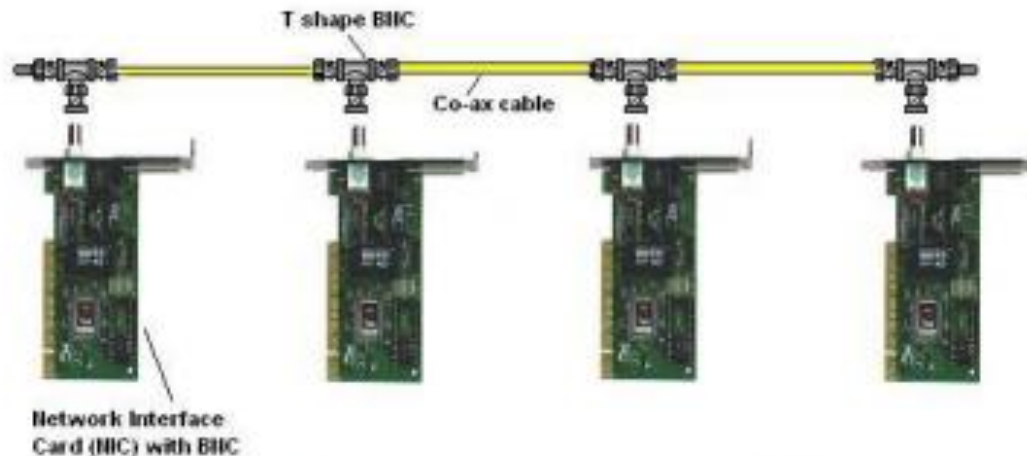


# Классический Ethernet

# Классический Ethernet – коаксиальный кабель

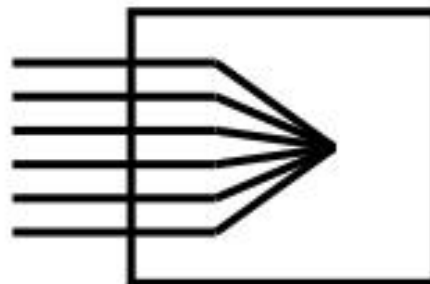


Общая шина



# Классический Ethernet – витая пара

- Это HUB==Концентратор – устройства физического уровня



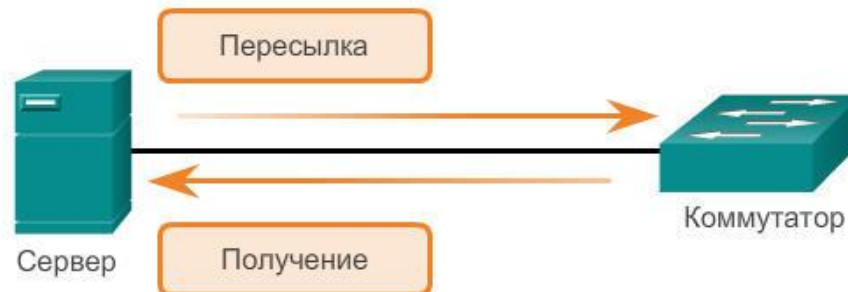
Коллизии – основная проблема общей шины

# Дуплекс и полудуплекс

- **Полудуплексная передача:** оба устройства могут передавать и получать данные в среде, но не одновременно.



- **Полнодуплексная передача:** оба устройства могут одновременно передавать и получать данные в среде.



# Топология «точка-точка»



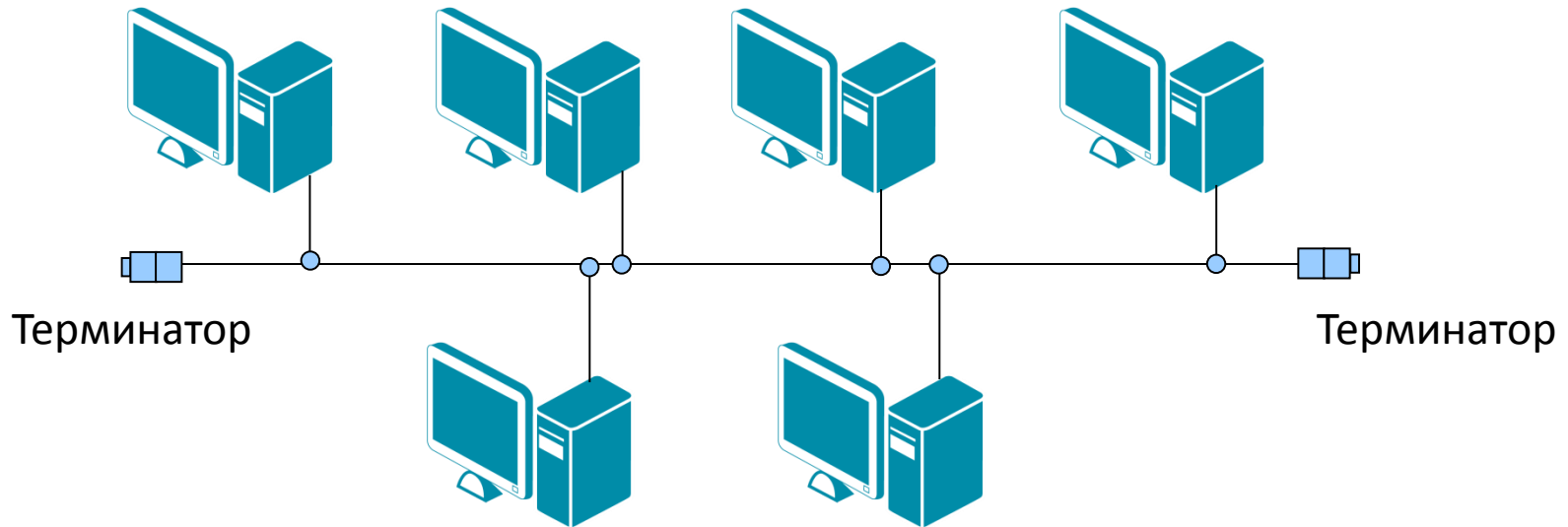
- **Постоянное соединение** между **двумя** конечными устройствами.

# Топология «точка-точка»



- Конечные узлы могут быть физически подключены с помощью нескольких промежуточных устройств (например модемов).
- Чаще используется для организации глобальных сетей

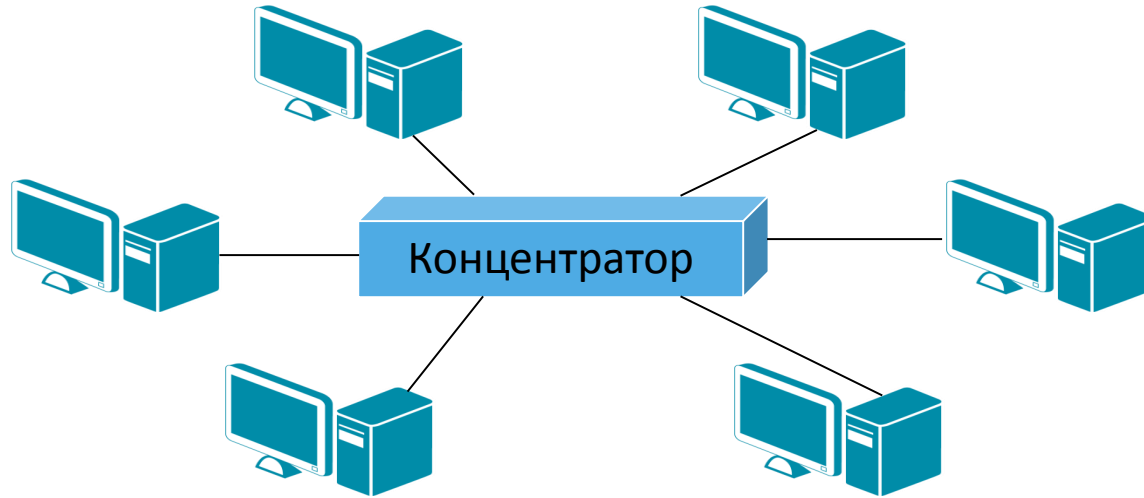
# Общая шина



Все компьютеры анализируют адрес получателя , но данные **принимает только один** компьютер, адрес которого соответствует адресу получателя.



# Звезда



- Общую шину «сжали» в одно центральное устройство.
- В качестве центрального узла может выступать компьютер или чаще специальное устройство – концентратор, коммутатор, маршрутизатор.
- Наиболее распространённая физическая топология сети

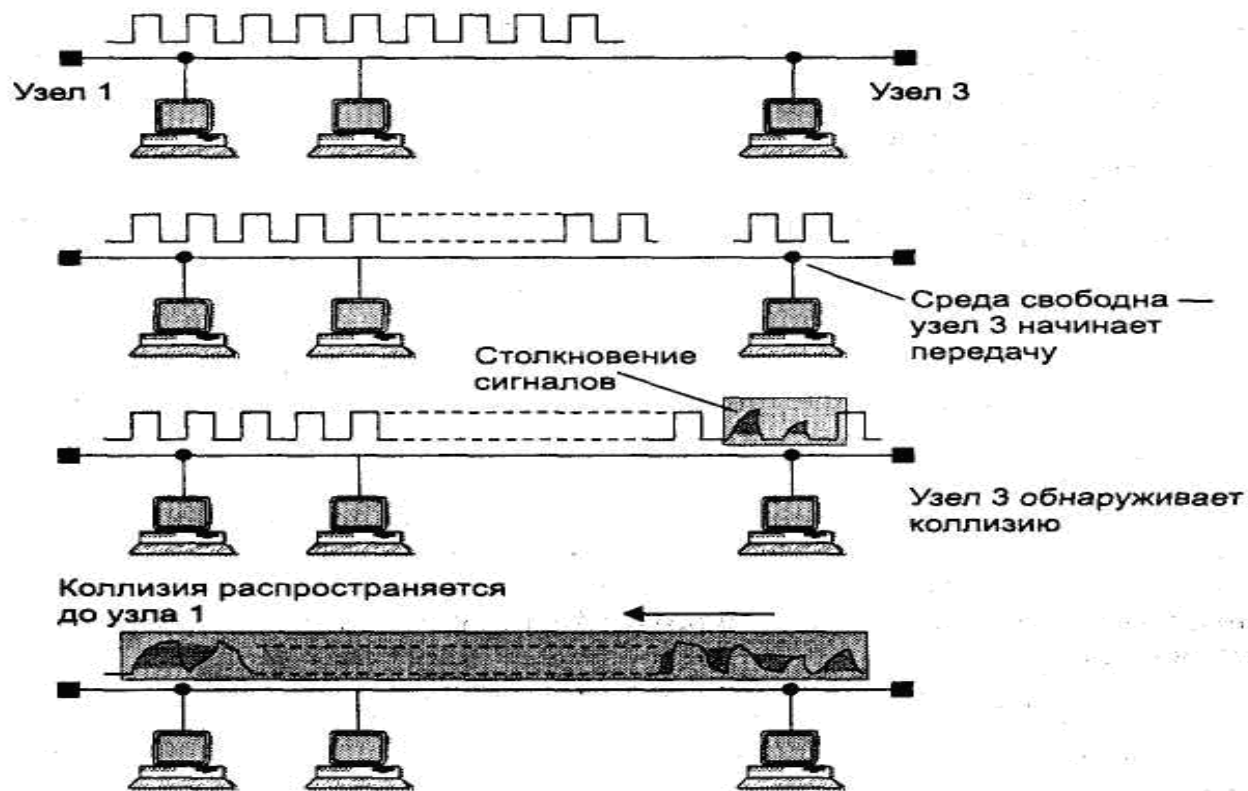
# Кольцо



Пакеты передаются по кольцу в одном направлении и проходят через каждый компьютер.



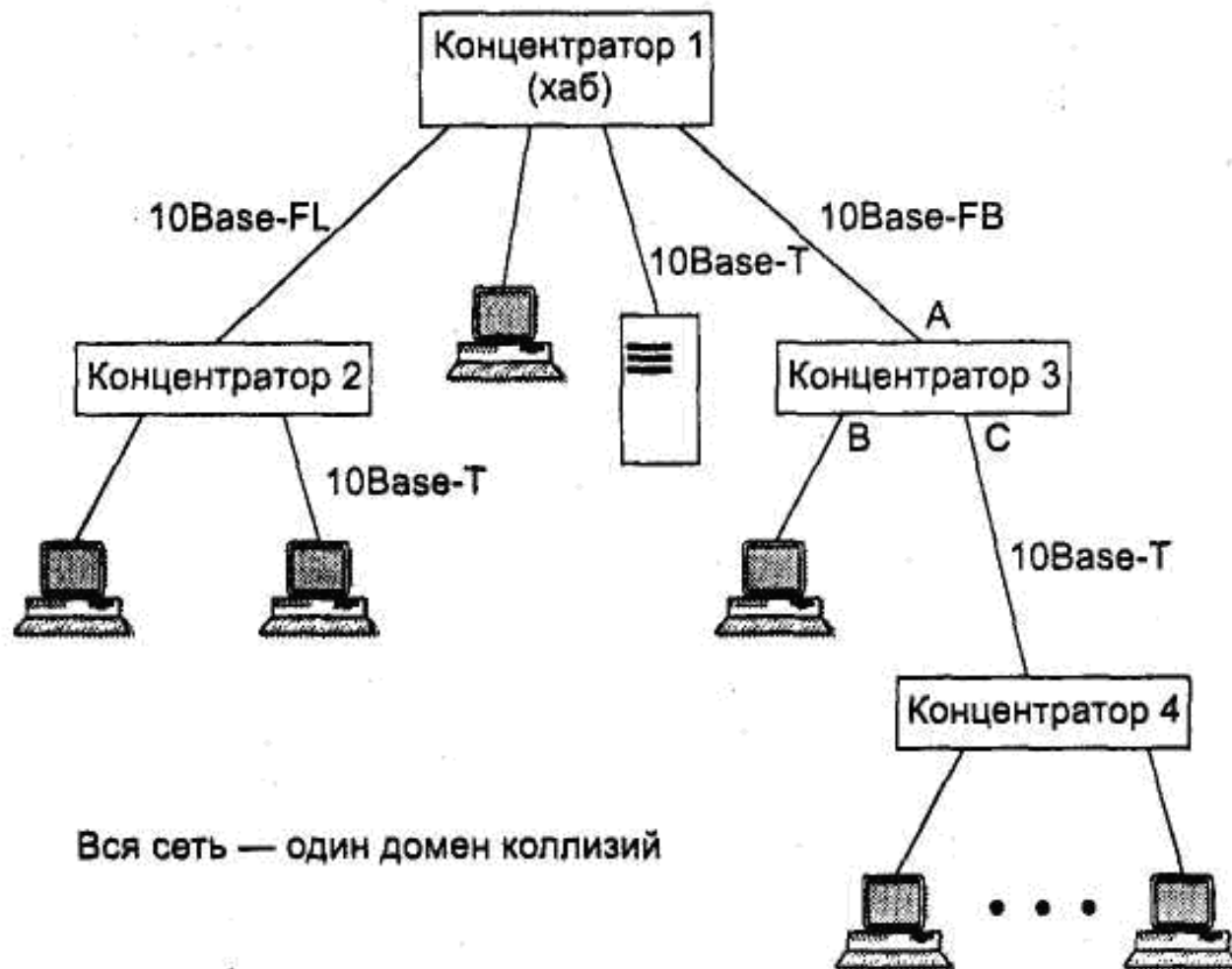
# Коллизии



- **Коллизия** – **одновременная передача** информации несколькими узлами.
- Узлы постоянно «прослушивают» среду передачи на предмет наличия коллизий.



# Домен коллизий



Часть сети, узлы которой распознают коллизию, называют  
**доменом коллизий**



# Методы доступа к разделяемой среде

## ■ Случайные

- Топология общая шина, звезда
- Сети Ethernet и WI-FI

## ■ Управляемые (детерминированные)

- Сети с топологией «Кольцо»
- Синхронизация с помощью маркерного пакета



# Методы случайного доступа

## ■ Сети Ethernet

- **CSMA/CD** – *Carrier Sense Multiple Access with Collision Detection*
- Множественный доступ с контролем несущей и **обнаружение** коллизий.

## ■ Сети WI-FI

- **CSMA/CA** – *Carrier Sense Multiple Access With Collision Avoidance*
- Множественный доступ с контролем несущей и **предотвращением** коллизий



# Коммутируемый Ethernet



# Коммутируемый Ethernet

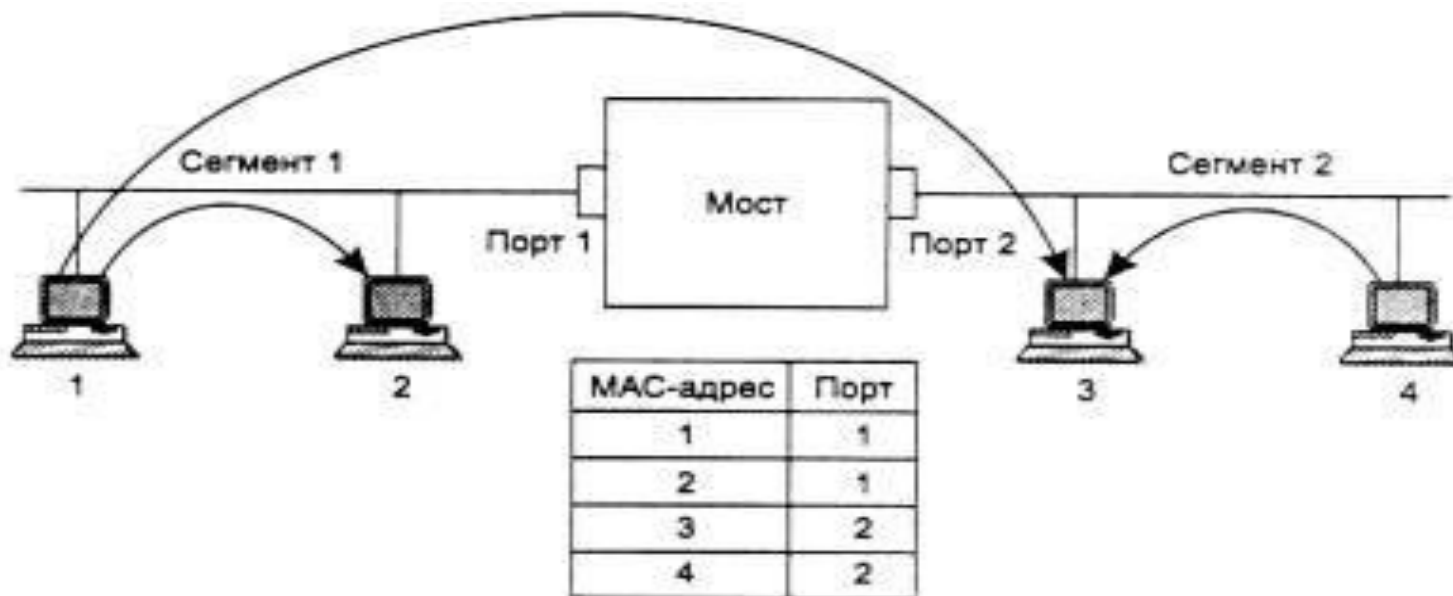
- Коммутируемый Ethernet (1995 Fast Ethernet)
  - Коллизий может не быть
  - Мосты и коммутаторы – работают на канальном уровне





# Мост

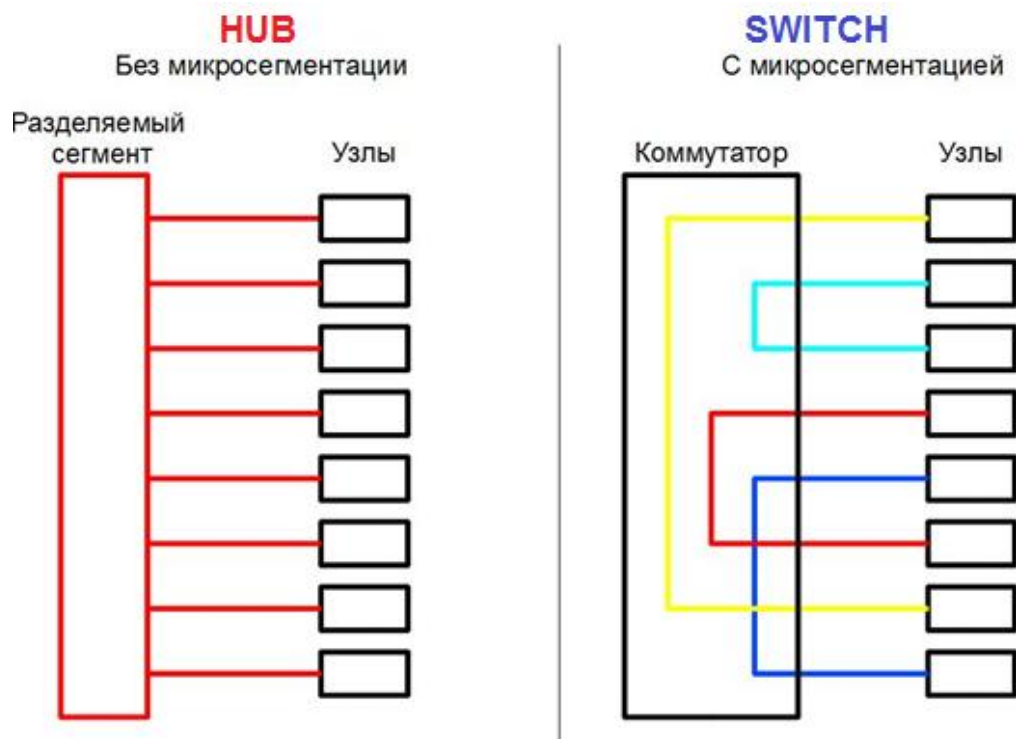
- Мост **не передает кадры** предназначенные для одного сегмента сети в другие сегменты.
- Мост для своей работы строит **таблицу коммутации**
- **Прозрачный мост**
  - не заметен для сетевых устройств (*у портов нет своего MAC-адреса* )
  - не требует настройки
- В качестве мостов выступали отдельные компьютеры





# Коммутатора

- Коммутатор - **набор мостов**
- На основе анализа MAC-адресов одновременно устанавливает несколько соединений между разными парами портов (*микросегментация*).



- Полудуплекс
  - Каждый порт коммутатора - **отдельный домен коллизий**
- Дуплекс - **коллизии отсутствуют**



# Архитектура коммутаторов



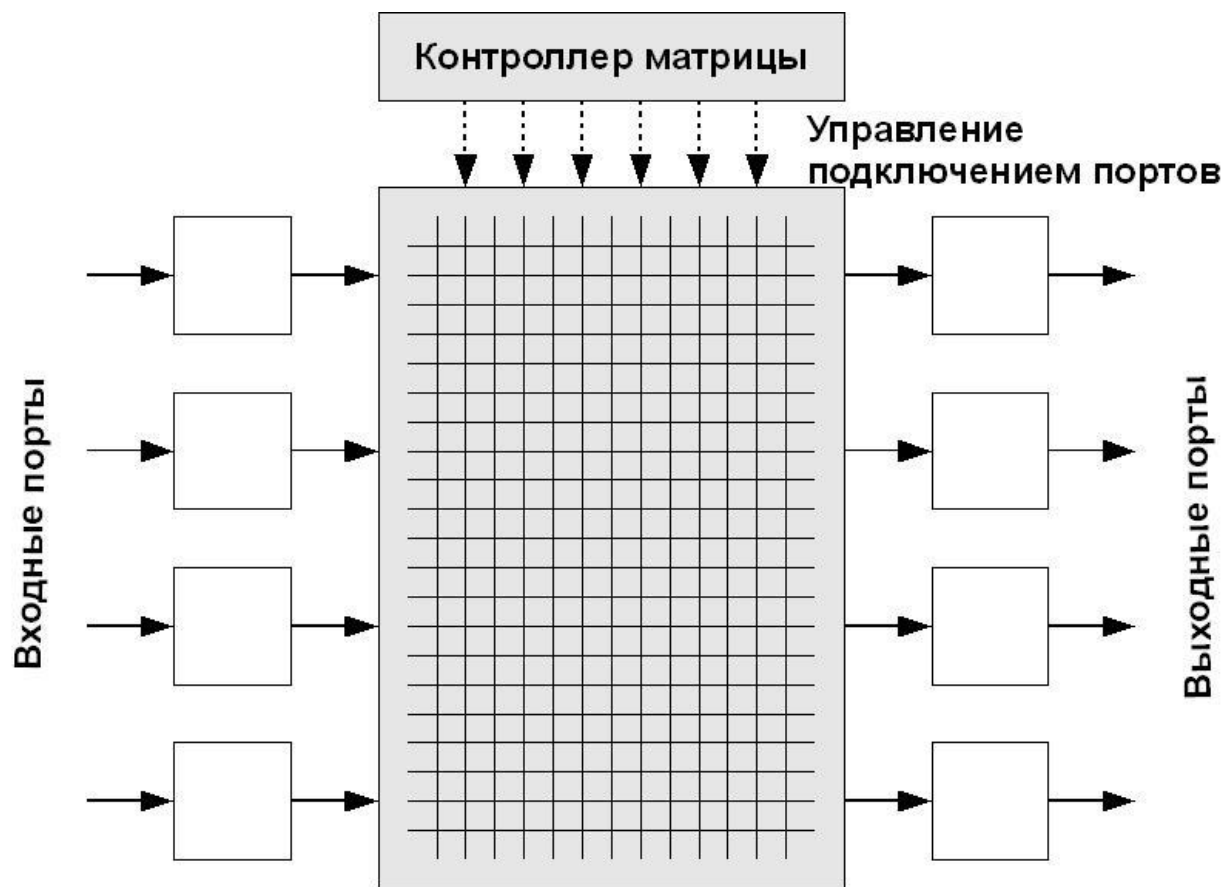
- Пакеты на каждом порту коммутатора обрабатываются специализированными цифровыми процессорами **ASIC** (*Application Specific Integrated Circuit*).



# Коммутационная матрица

## Switch fabric

- Все порты соединены друг с другом по технологии точка – точка через коммутационную матрицу





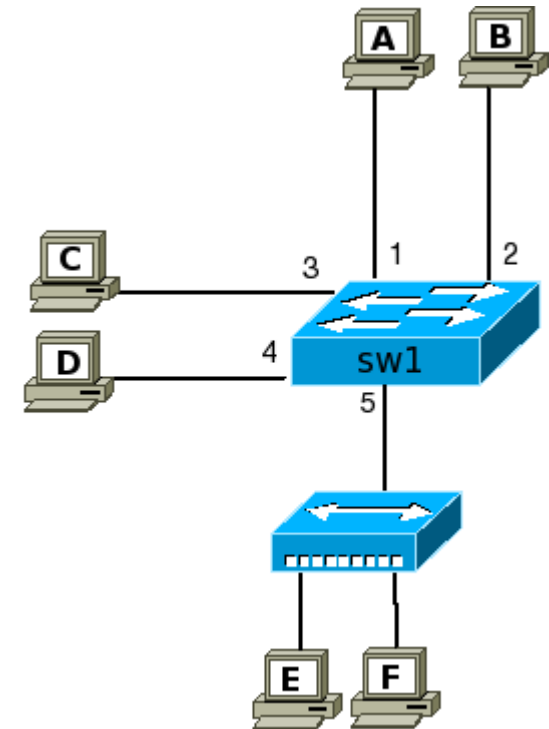
# Работа коммутатора

- Коммутатор использует три базовых механизма:
- **Forwarding** (*пересылка*)
  - передача кадра с одного порта на другой порт в соответствии с записью в таблице коммутации.
- **Flooding** (*лавинная рассылка*) - кадр, полученный на один из портов, передается на все остальные порты кроме того на который был получен :
  - при получении широковещательного кадра ARP протокола, для заполнения arp таблицы.
  - при получении кадра с неизвестным MAC-адресом узла назначения для которого нет записи в таблице коммутации. Это позволяет доставить кадр этому узлу.
- **Filtering** (*фильтрация*)



# Фильтрация

Порт коммутатора	MAC-адрес хоста
1	A
2	B
3	C
4	D
5	E
5	F



**Filtering**— если MAC-адрес получателя и отправителя доступны через один и тот же порт, то коммутатор не пересылает кадр дальше.



# Методы коммутации

**IV**

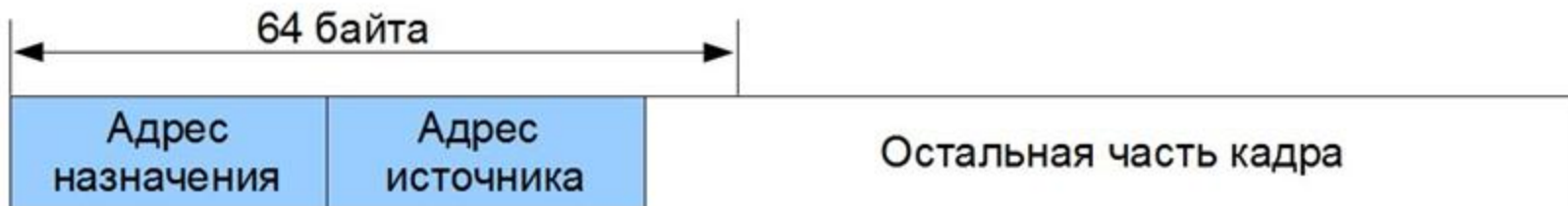
**Store-and-forward** С промежуточным хранением



**Cut-through** Без буферизации



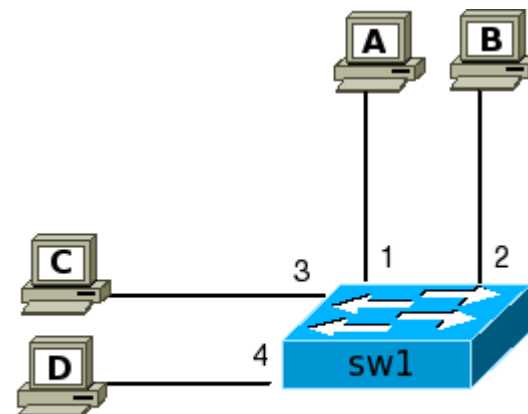
**Fragment-free** Исключение фрагментов





# Таблица коммутации

Порт коммутатора	MAC-адрес хоста
1	A
2	B
3	C
4	D



## Алгоритм обратного обучения

- Заполнение таблицы коммутации – коммутатор анализирует **MAC-адрес отправителя** и сопоставляет их с портом на который был получен кадр.
- Запись хранится в течение некоторого времени (обычно 5 минут)

`S#sh mac-address-table` – просмотр таблицы  
`S# clear mac-address-table` – очистка таблицы





# Коммутаторы и снижение перегрузки сети

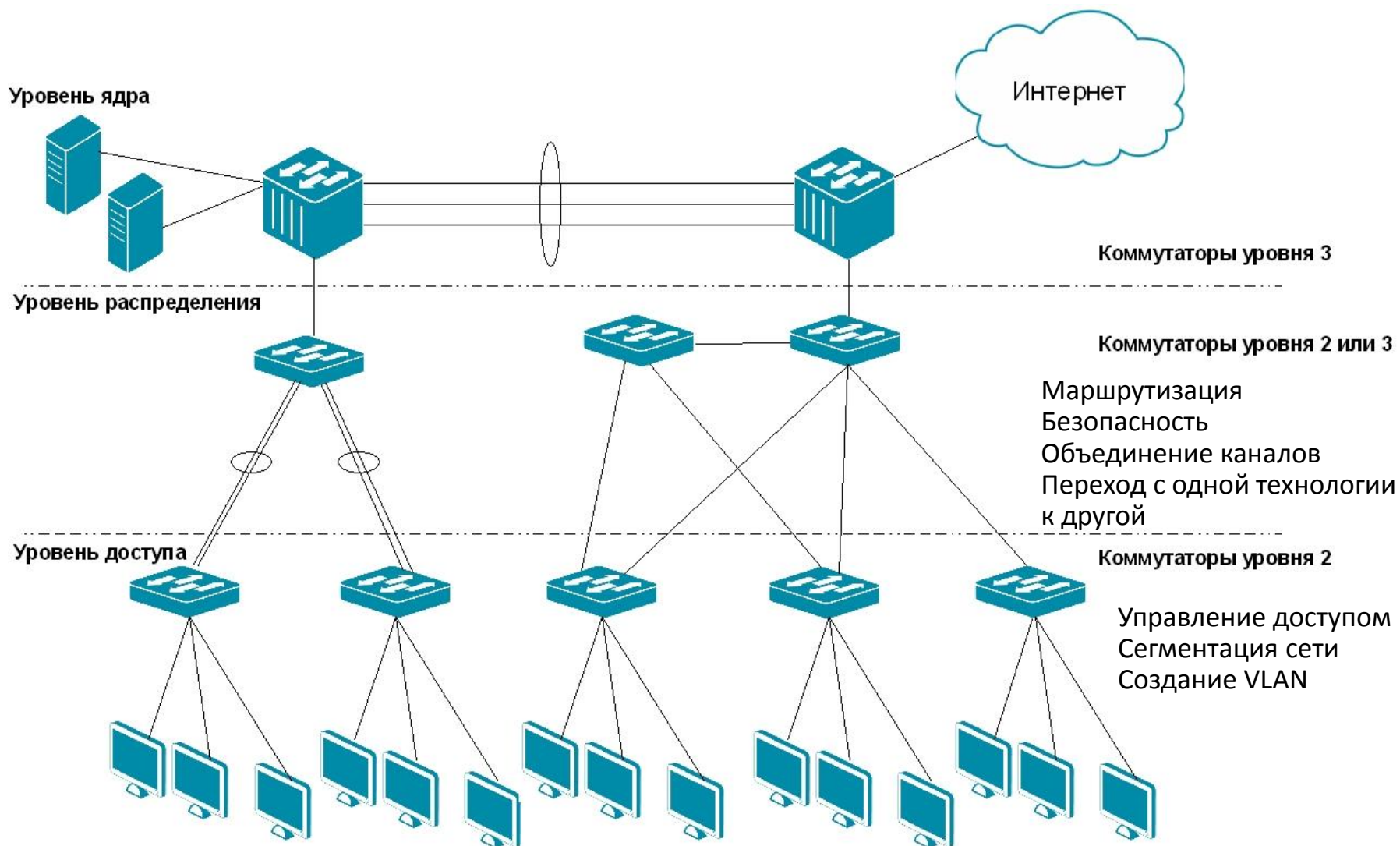
- Разделяют LAN на отдельные коллизийные домены;
- Полнодуплексная связь между устройствами;
- Высокая плотность портов;
- Буферизация больших кадров;
- Использование высокоскоростных портов;
- Быстрая внутренняя коммутация;
- Низкая стоимость портов.

## Классификация коммутаторов по уровням модели OSI

- **Коммутаторы уровня 2** коммутируют кадры на основе анализа MAC-адресов канального уровня модели OSI.
- **Коммутатор уровня 3** осуществляют коммутацию и фильтрацию на основе адресов канального (уровень 2) и сетевого (уровень 3) уровней модели OSI.



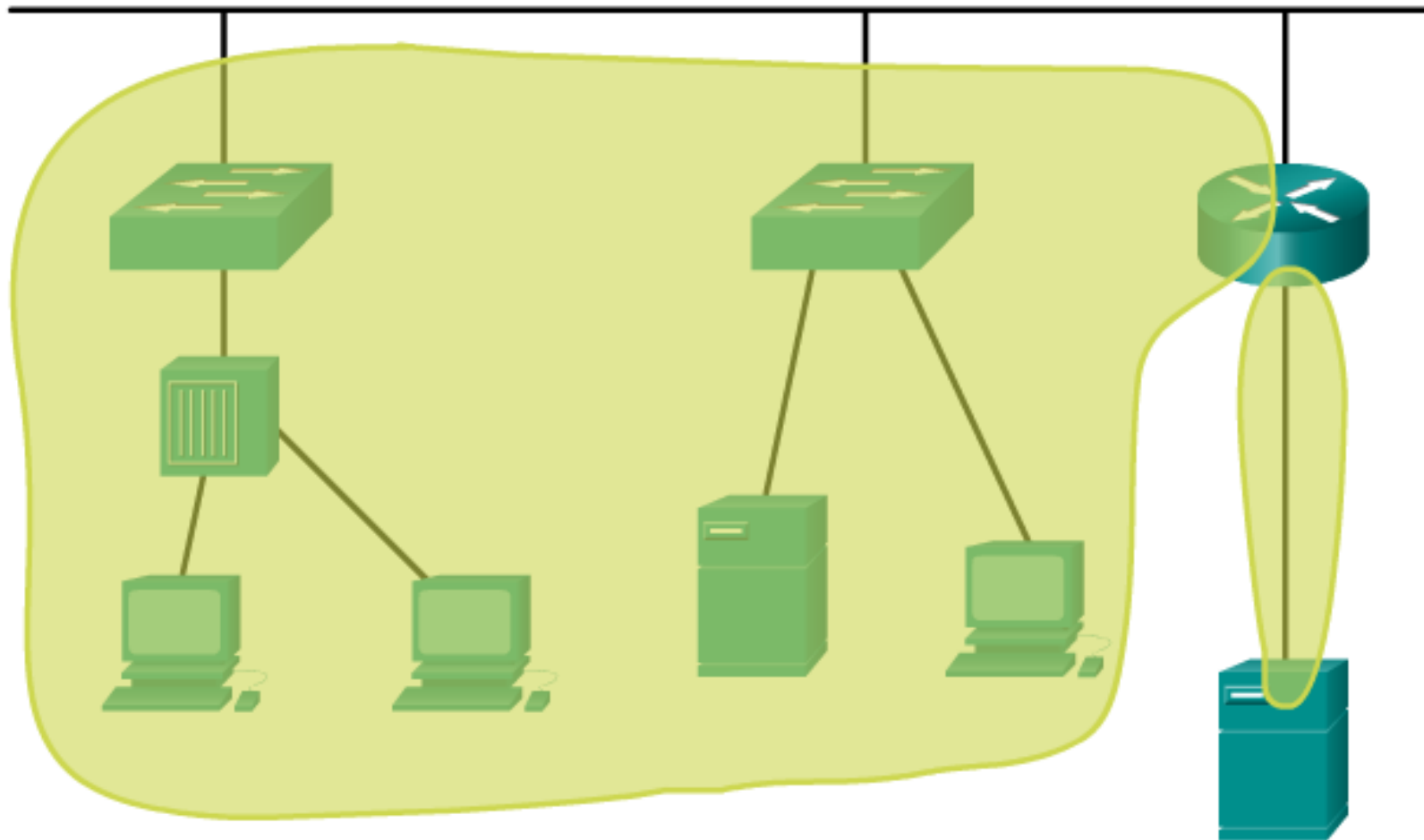
# Трехуровневая иерархическая модель сети





# Широковещательные домены

Обрисуйте контуры каждого широковещательного домена. (Подсказка. В некоторых случаях их может быть больше одного.)





# Коммутаторы и широковещательные домены

- Коммутаторы **пропускают широковещательные кадры** на все порты
- Коммутаторы **не ограничивают широковещательные домены**
- Все порты коммутатора **принадлежат одному широковещательному домену.**
- Если соединено несколько коммутаторов, они направляют широковещательные кадры **на все порты всех коммутаторов** (*кроме порта, принявшего такой кадр*)

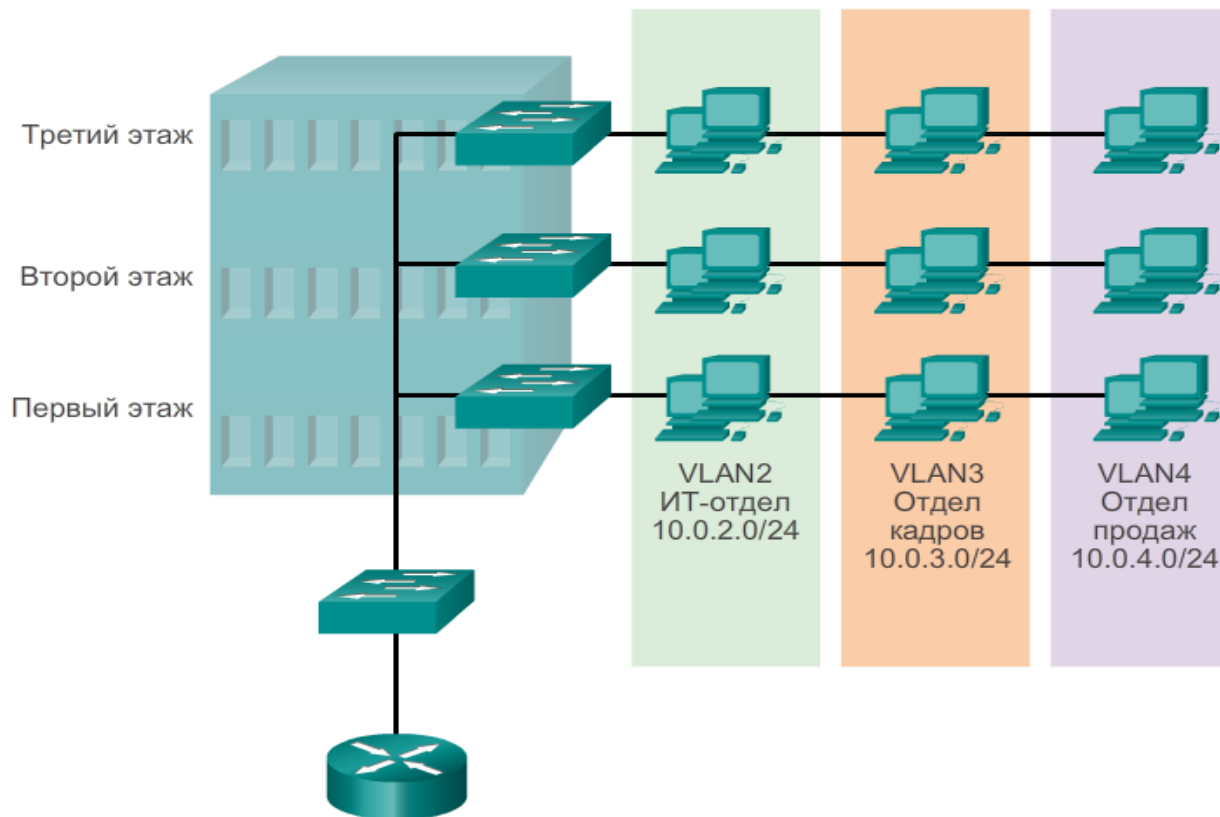


# Virtual Local Area Network

VLAN— группа узлов сети, трафик которой, в том числе и широковещательный, на канальном уровне полностью изолирован от других узлов сети.



# VLAN



## Изоляция сетей:

- Разные отделы в одной крупной компании
- Разные компании в одном бизнес-центре



# Преимущества сетей VLAN

- Безопасность
- Повышение производительности
- Гибкое разделение устройств на группы
- Улучшение администрирования (*проще применять политики безопасности*)
- Переход из одного VLAN в другой требует **устройство 3 уровня**, на котором, применяются политики, разрешающие или запрещающие доступ из одной VLAN в VLAN.





# Способы объединения узлов в VLAN

В коммутаторах могут быть реализованы следующие типы VLAN:

- на основе портов;
- на основе стандарта IEEE 802.1Q;
- на основе MAC-адресов;
- на основе стандарта IEEE 802.1ad (Q-in-Q VLAN);
- на основе портов и протоколов IEEE 802.1v;



# VLAN на основе портов

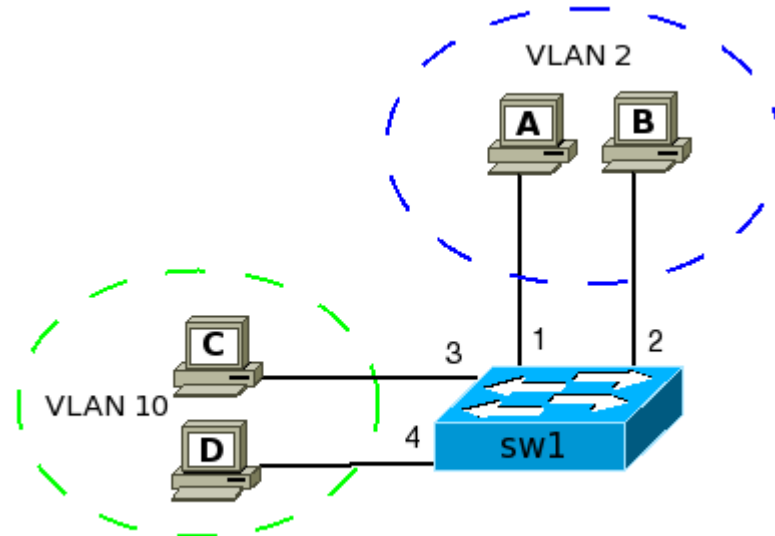
## Две VLAN-один коммутатор

Для VLAN 2:

Порт коммутатора	MAC-адрес хоста
1	A
2	B

Для VLAN 10:

Порт коммутатора	MAC-адрес хоста
3	C
4	D





## VLAN на основе портов

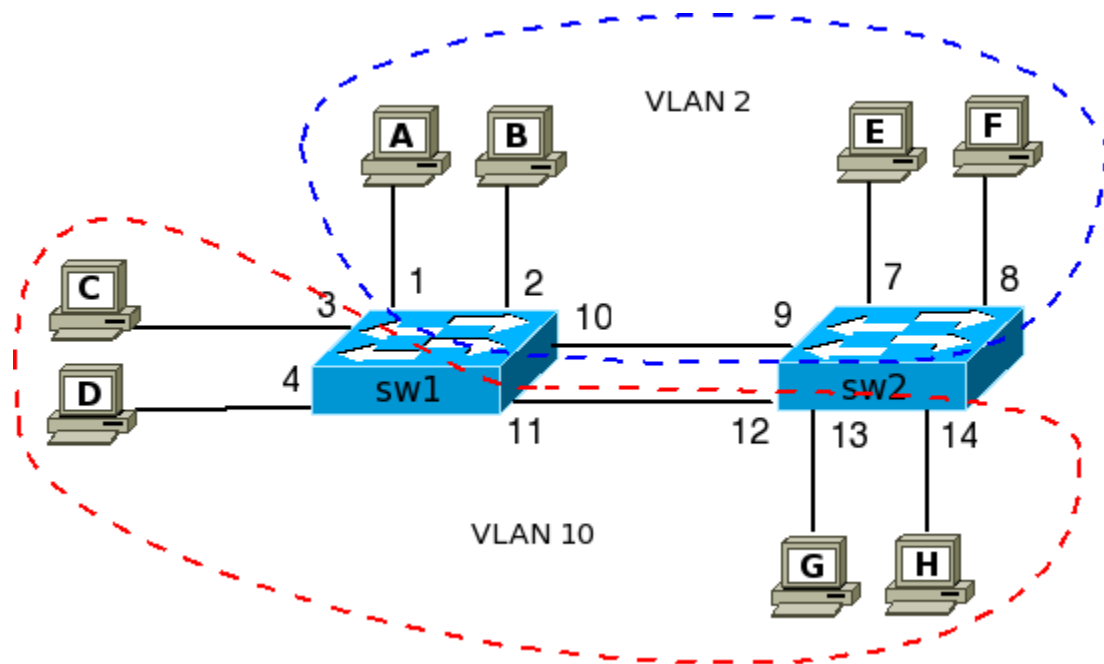
### Две VLAN- два коммутатора

Таблица коммутации sw 1 для VLAN 10:

Порт коммутатора	MAC-адрес хоста
3	C
4	D
11	G
11	H

Таблица коммутации sw2 для VLAN 10:

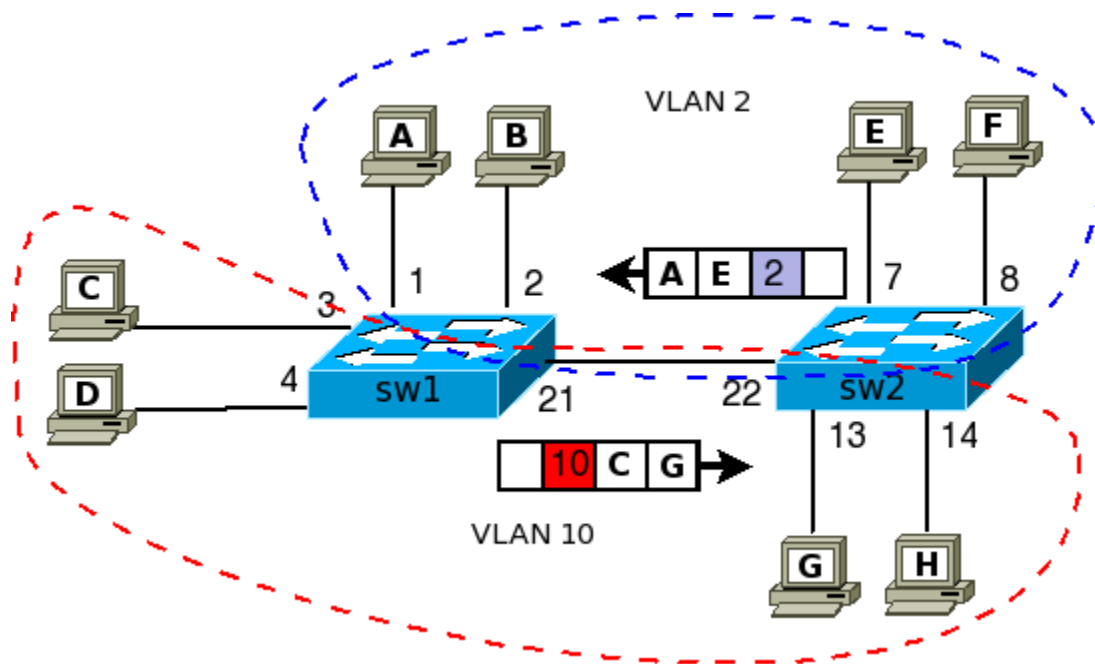
Порт коммутатора	MAC-адрес хоста
13	G
14	H
12	C
12	D



**Недостаток:** когда количество VLAN возрастает, то для каждой VLAN необходимо добавлять отдельную связь между коммутаторами .



# VLAN на основе стандарта 802.1Q



- Транковый порт
  - порт через который проходят кадры из разных VLAN.
- Транковый канал
  - это канал типа «точка-точка» между коммутатором и другими сетевыми устройствами.
  - Служит для передачи трафика нескольких VLAN через один канал.



# VLAN на основе стандарта IEEE 802.1Q

## Тег VLAN 802.1Q

К кадру Ethernet добавлены 4 байта, которые увеличивают его размер до 1522 байт.

Обычный (немаркированный) кадр

Адрес назначения (DA)	Адрес источника (SA)	Tun	Данные (Data)	Контрольная последовательность кадра (CRC)
-----------------------	----------------------	-----	---------------	--

Маркированный кадр 802.1p/802.1Q

Адрес назначения (DA)	Адрес источника (SA)	Тег (Tag)	Tun	Данные (Data)	Контрольная последовательность кадра (CRC)
-----------------------	----------------------	-----------	-----	---------------	--

Идентификатор кадра VLAN 0x8100	Приоритет (Priority)	Индикатор канонического формата (CFI)	Идентификатор VLAN (VID)
16 бит	3 бита	1 бит	12 бит

CFI передача кадра Token Ring в канале Ethernet

Тег:

- добавляется к кадру при входе в транковый канал
- удаляется при выходе из транкового канала



## Краткий обзор сетей VLAN

# Типы сетей VLAN

- VLAN передачи данных
- VLAN по умолчанию
  - В Cisco это VLAN1
- Native VLAN
  - в нее попадают все кадры без тега
  - обычно это VLAN1 по умолчанию
- VLAN управления
  - для удаленного доступа к функциям управления коммутатора.
  - виртуальному интерфейсу (SVI) данной VLAN назначается IP-адрес и маска подсети.
  - по умолчанию это VLAN1



# Краткий обзор сетей VLAN

## Типы сетей VLAN

### VLAN 1

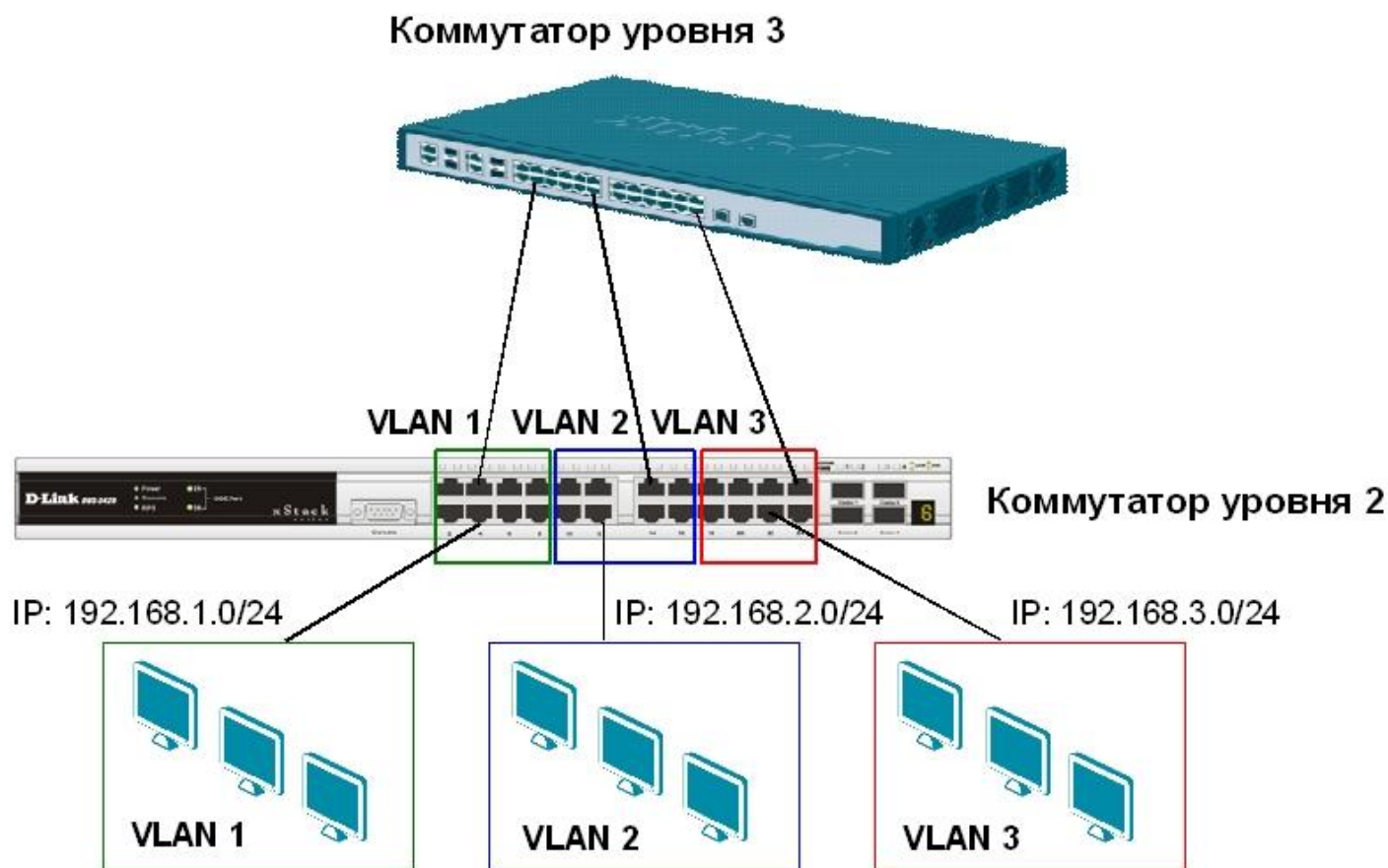
Switch# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- Все порты назначены сети VLAN 1 для пересылки данных по умолчанию.
- Сетью native VLAN по умолчанию является сеть VLAN 1.
- Сетью управления VLAN по умолчанию является сеть VLAN 1.
- VLAN 1 нельзя переименовывать или удалять.

# Объединение VLAN

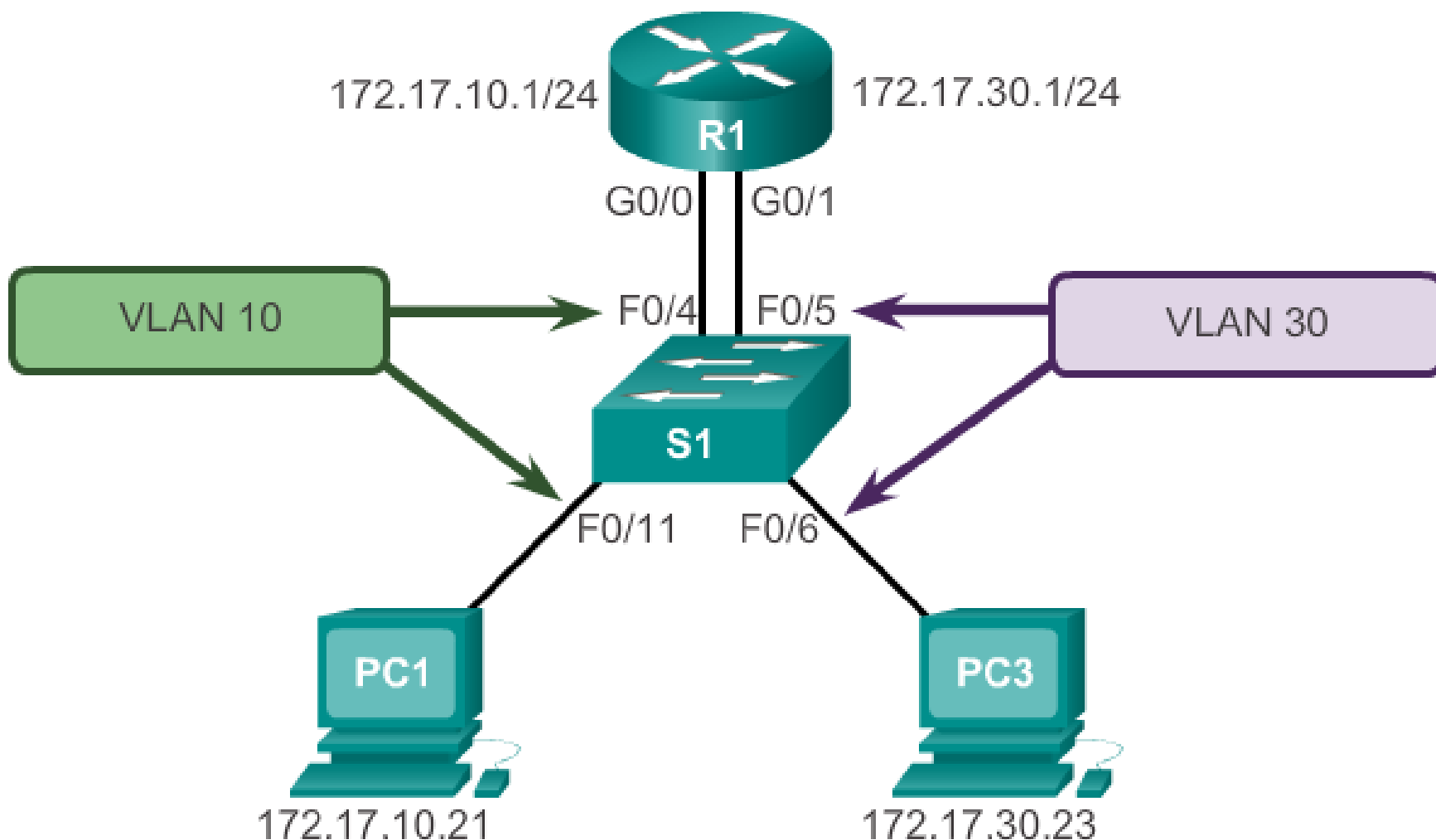
Для объединения виртуальных подсетей как внутри одного коммутатора, так и между двумя коммутаторами, нужно использовать сетевой уровень модели OSI.



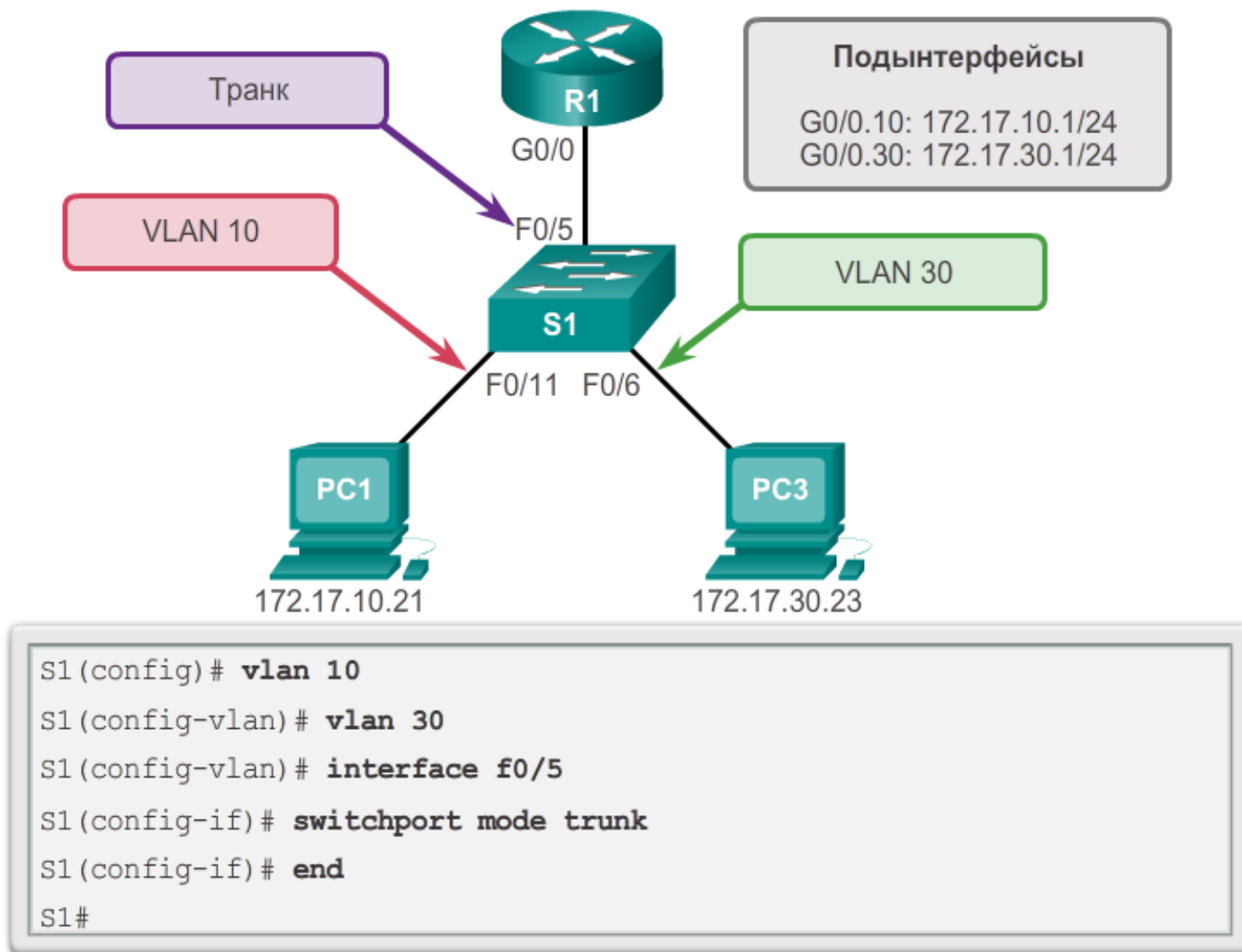




# Объединение VLAN



# Настройка конфигурации ROS (Router on a Stick) Объединение VLAN





# Назначение VLAN

## Создание VLAN

### Команды коммутатора Cisco под управлением ОС IOS

Войдите в режим глобальной конфигурации.

```
S1# configure terminal
```

Создайте сеть VLAN с допустимым номером идентификатора.

```
S1(config)# vlan    vlan-id
```

Укажите уникальное имя для идентификации сети VLAN.

```
S1(config-vlan)# name    vlan-name
```

Вернитесь в привилегированный режим.

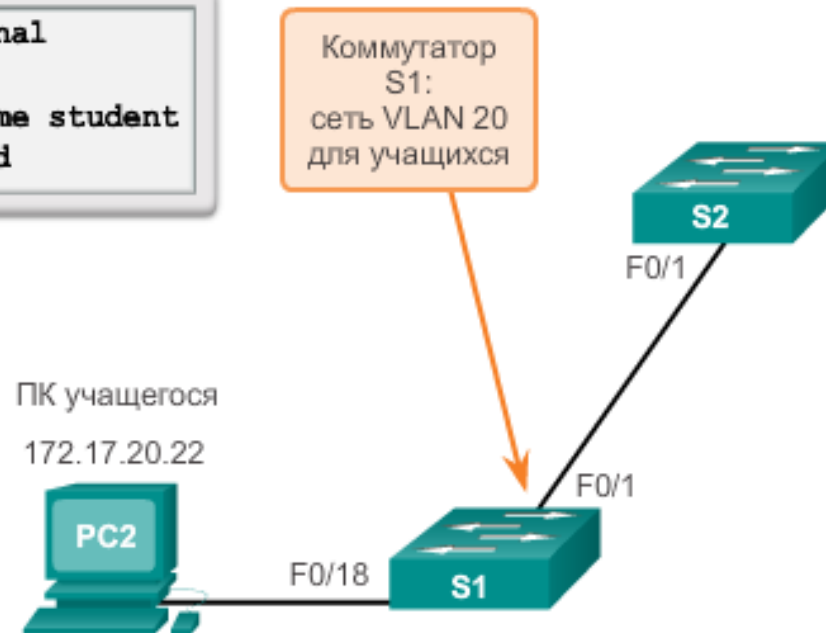
```
S1(config-vlan)# end
```



# Создание VLAN

## Пример конфигурации

```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```





# Назначение портов сетям VLAN

## Назначение портов сетям VLAN

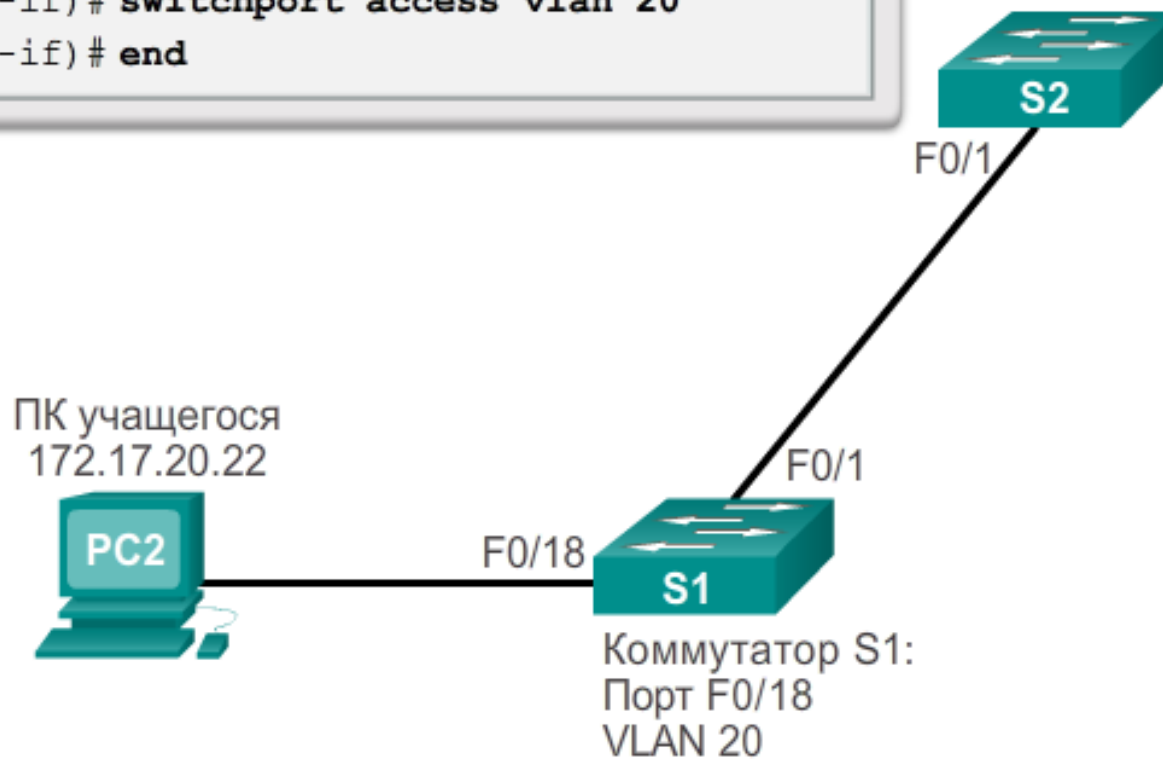
### Команды коммутатора Cisco под управлением ОС IOS

Войдите в режим глобальной конфигурации.	S1# <b>configure terminal</b>
Войдите в режим конфигурации интерфейса для SVI.	S1(config)# <b>interface</b> <i>interface_id</i>
Переведите порт в режим доступа.	S1(config-if)# <b>switchport mode access</b>
Назначьте порт сети VLAN.	S1(config-if)# <b>switchport access vlan</b> <i>vlan_id</i>
Вернитесь в привилегированный режим.	S1(config-if)# <b>end</b>

## Назначение VLAN

# Назначение портов сетям VLAN

```
s1# configure terminal  
s1(config)# interface F0/18  
s1(config-if)# switchport mode access  
s1(config-if)# switchport access vlan 20  
s1(config-if)# end
```





# Настройка транкового канала

## Настройка транкового канала

### Команды коммутатора Cisco под управлением ОС IOS

Войдите в режим глобальной конфигурации.

```
S1# configure terminal
```

Войдите в режим конфигурации интерфейса для SVI.

```
S1(config)# interface interface_id
```

Настройте канал в качестве транкового.

```
S1(config-if)# switchport mode trunk
```

Укажите сеть native VLAN для транков 802.1Q без меток.

```
S1(config-if)# switchport trunk native vlan  
vlan_id
```

Укажите список сетей VLAN, которым разрешён доступ в транковый канал.

```
S1(config-if)# switchport trunk allowed vlan  
vlan-list
```

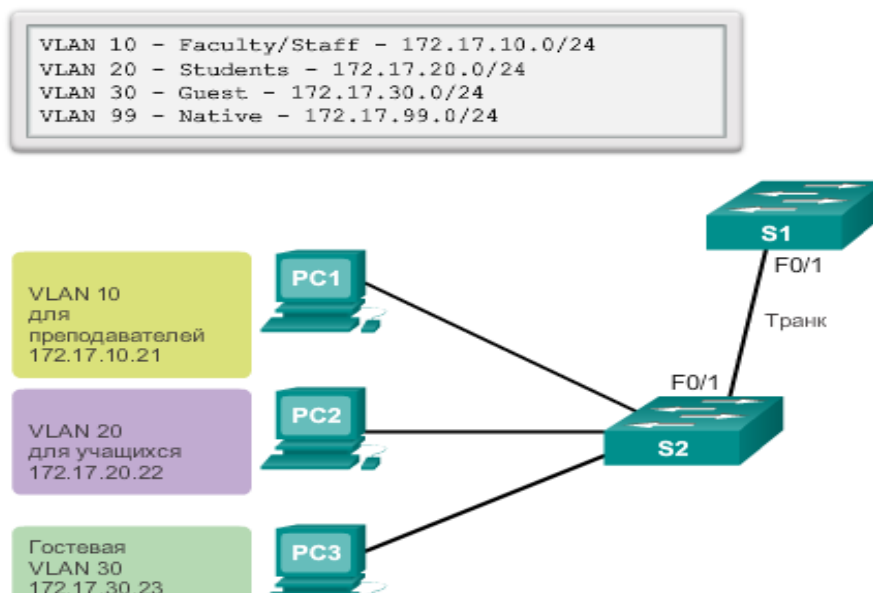
Вернитесь в привилегированный режим.

```
S1(config-if)# end
```



# Настройка транкового канала

## Пример топологии



## Пример конфигурации

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```





# Просмотр VLAN

## Синтаксис команд в интерфейсе командной строки Cisco IOS

**show vlan** [**brief** | **id** *vlan-id* | **name** *vlan-name* | **summary** ].

Отобразите одну строку для каждой сети VLAN с именем, состоянием и портами этой VLAN.

**brief**

Отобразите информацию об идентификационном номере одной сети VLAN.  
Диапазон для идентификатора *vlan* — от 1 до 4094.

**id** *vlan-id*

Отобразите информацию об имени одной сети VLAN. Имя VLAN — это код ASCII размером от 1 до 32 символов.

**name** *vlan-name*

Отобразите общую информацию о VLAN.

**summary**

Команда **show interfaces**

## Синтаксис команд в интерфейсе командной строки Cisco IOS

**show interfaces** [*interface-id* | **vlan** *vlan-id* ] | **switchport**

К допустимым интерфейсам относятся физические порты (включая тип, модуль и номер порта) и каналы портов. Диапазон каналов портов составляет от 1 до 6.

*interface-id*

Идентификация сети VLAN. Диапазон от 1 до 4094.

**vlan** *vlan-id*

Отобразите административное и рабочее состояние порта коммутации, включая настройки блокировки и защиты портов.

**switchport**



# Просмотр VLAN

```
S1# show vlan name student
```

VLAN Name	Status	Ports
20 student	active	Fa0/11, Fa0/18

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
20	enet	100020	1500	-	-	-	-	-	0	0

Remote SPAN VLAN

-----

Disabled

Primary	Secondary	Type	Ports
-----	-----	-----	-----

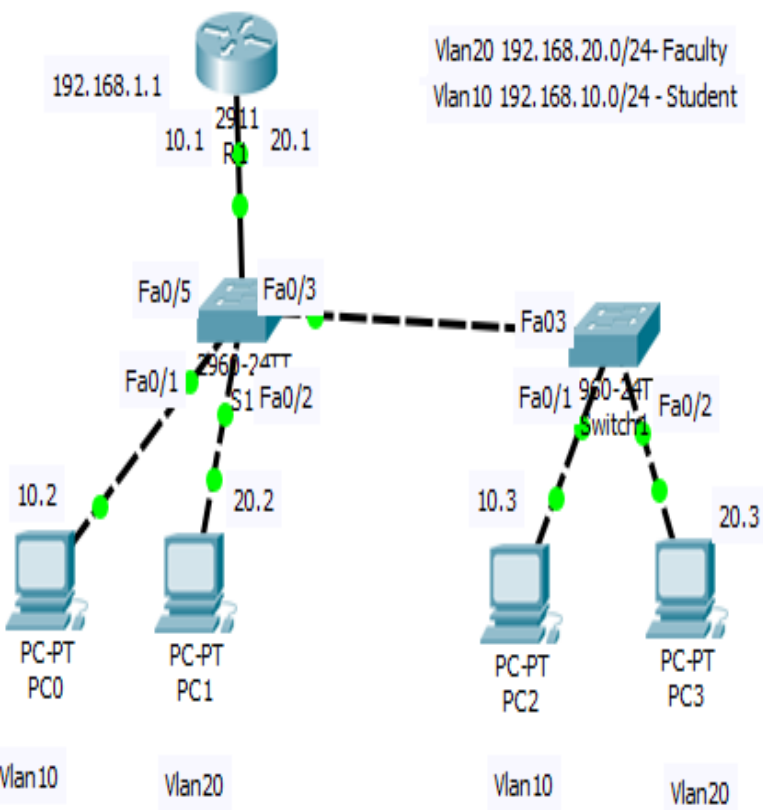
```
S1# show vlan summary
```

```
Number of existing VLANs      : 7
Number of existing VTP VLANs  : 7
Number of existing extended VLANs : 0
```

```
S1#
```



# Настройка VLAN



```
S1(config)# vlan 10
S1(config-vlan)# name Students
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# exit
S1(config)# interface f0/3
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
```

```
R1(config)# interface g0/1.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# interface g0/1.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface g0/1
R1(config-if)# no shutdown
```



# Настройка VLAN на S1

- S1(config)# vlan 10
- S1(config-vlan)# name Students
- S1(config-vlan)# vlan 20
- S1(config-vlan)# name Faculty
- S1(config-vlan)# exit
- S1(config)# interface f0/3
- S1(config-if)# switchport mode trunk
- S1(config-if)# interface f0/5
- S1(config-if)# switchport mode trunk
- S1(config-if)# interface f0/1
- S1(config-if)# switchport mode access
- S1(config-if)# switchport access vlan 10
- S1(config-if)# interface f0/2
- S1(config-if)# switchport mode access
- S1(config-if)# switchport access vlan 20



# Настройка подинтерфейсов роутера

- R1(config)# interface g0/1.10
- R1(config-subif)# encapsulation dot1Q 10
- R1(config-subif)# ip address 192.168.10.1 255.255.255.0
- R1(config-subif)# interface g0/1.20
- R1(config-subif)# encapsulation dot1Q 20
- R1(config-subif)# ip address 192.168.20.1 255.255.255.0
- R1(config-subif)# exit
- R1(config)# interface g0/1
- R1(config-if)# no shutdown



## Назначение VLAN

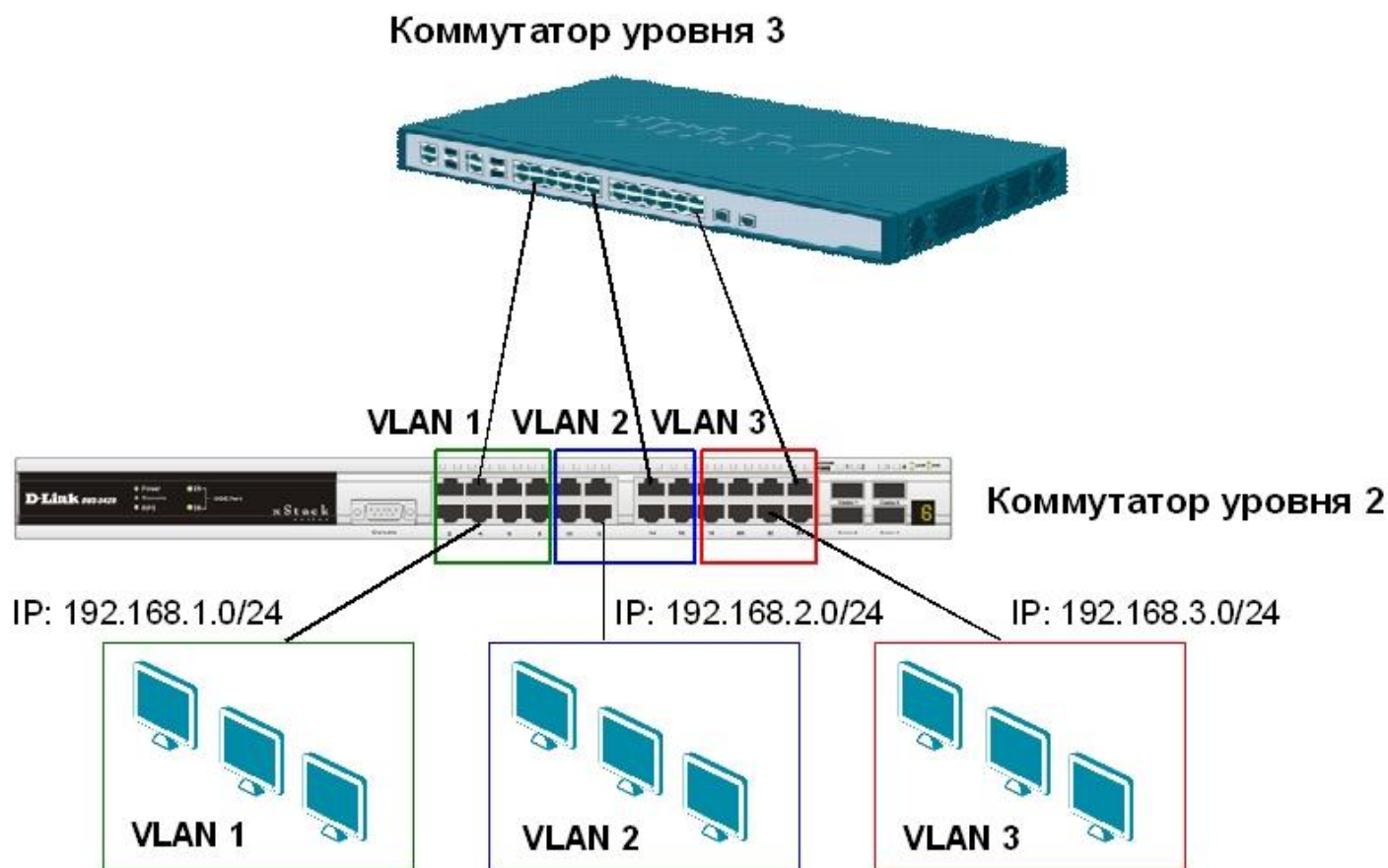
# Сброс настроек транкового канала до состояния по умолчанию

## Возвращение порта в режим доступа

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<выходные данные опущены>
```

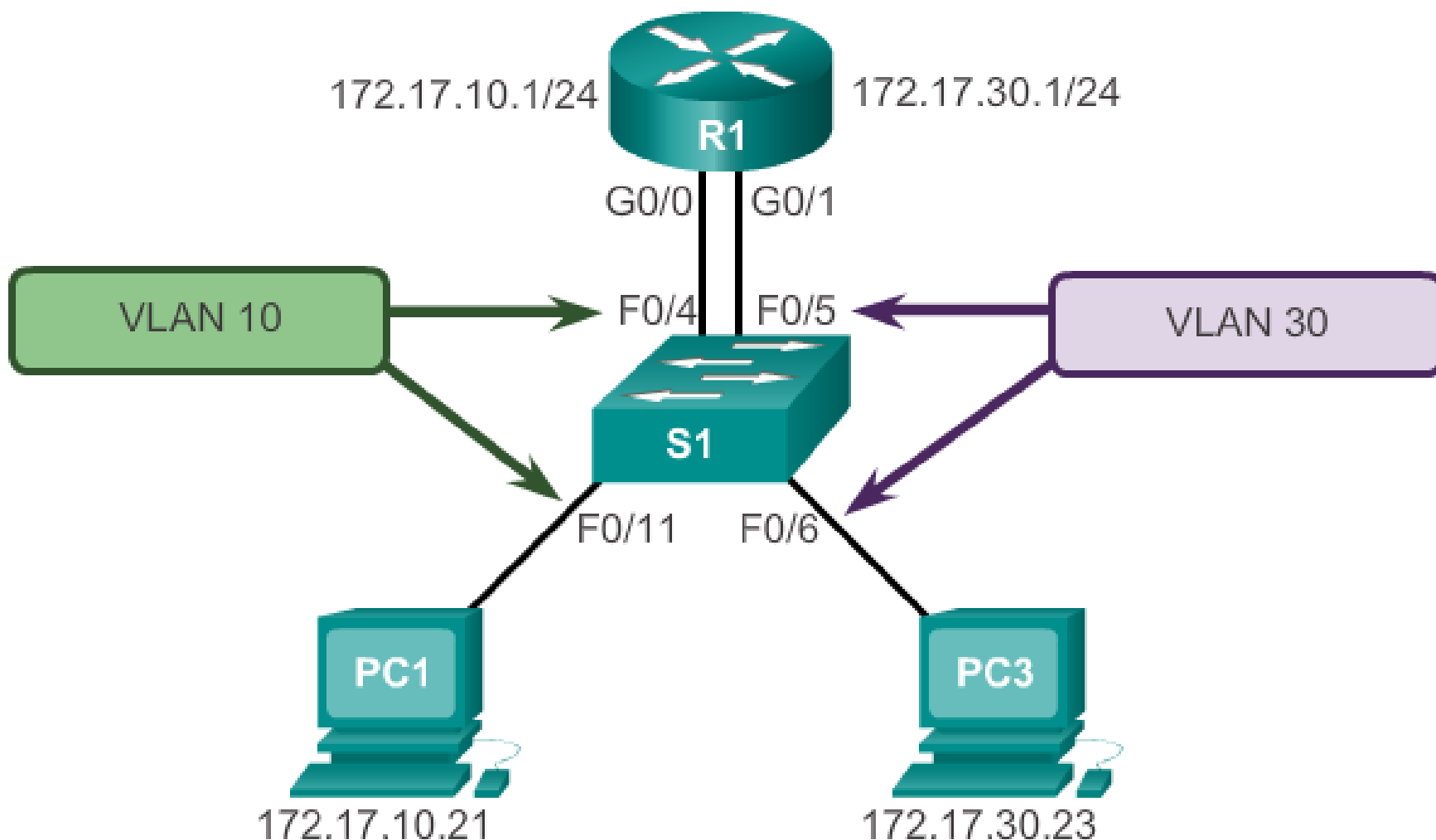
# Объединение VLAN

Для объединения виртуальных подсетей как внутри одного коммутатора, так и между двумя коммутаторами, нужно использовать сетевой уровень модели OSI.





# Объединение VLAN





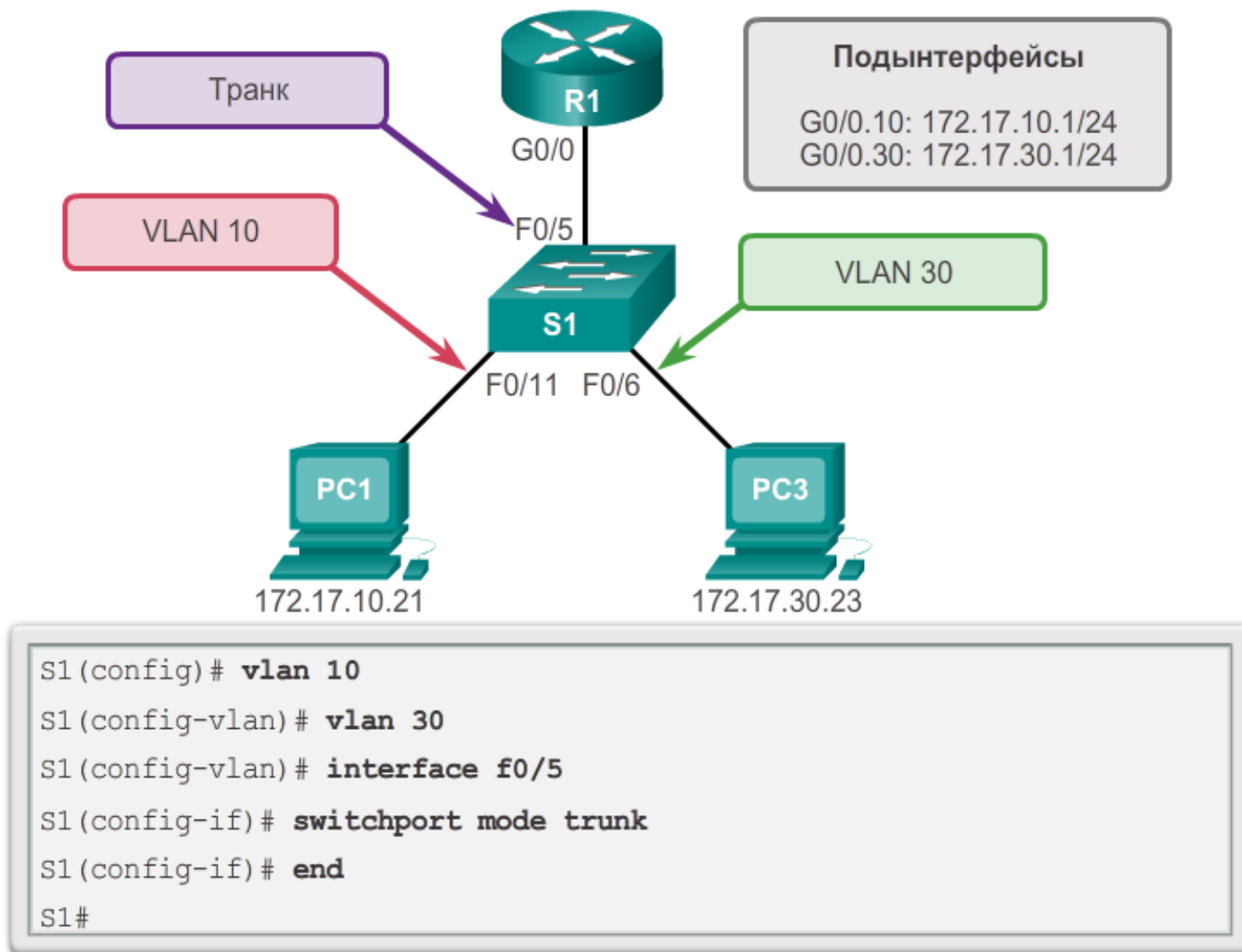


Настройка маршрутизации между VLAN по устаревшему методу

# Настройка интерфейса маршрутизатора

```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:12.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 01:42:13.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:54.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/1,
changed state to up
*Mar 20 01:42:55.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)# end
R1# copy running-config startup-config
```

# Настройка конфигурации ROS (Router on a Stick) Объединение VLAN





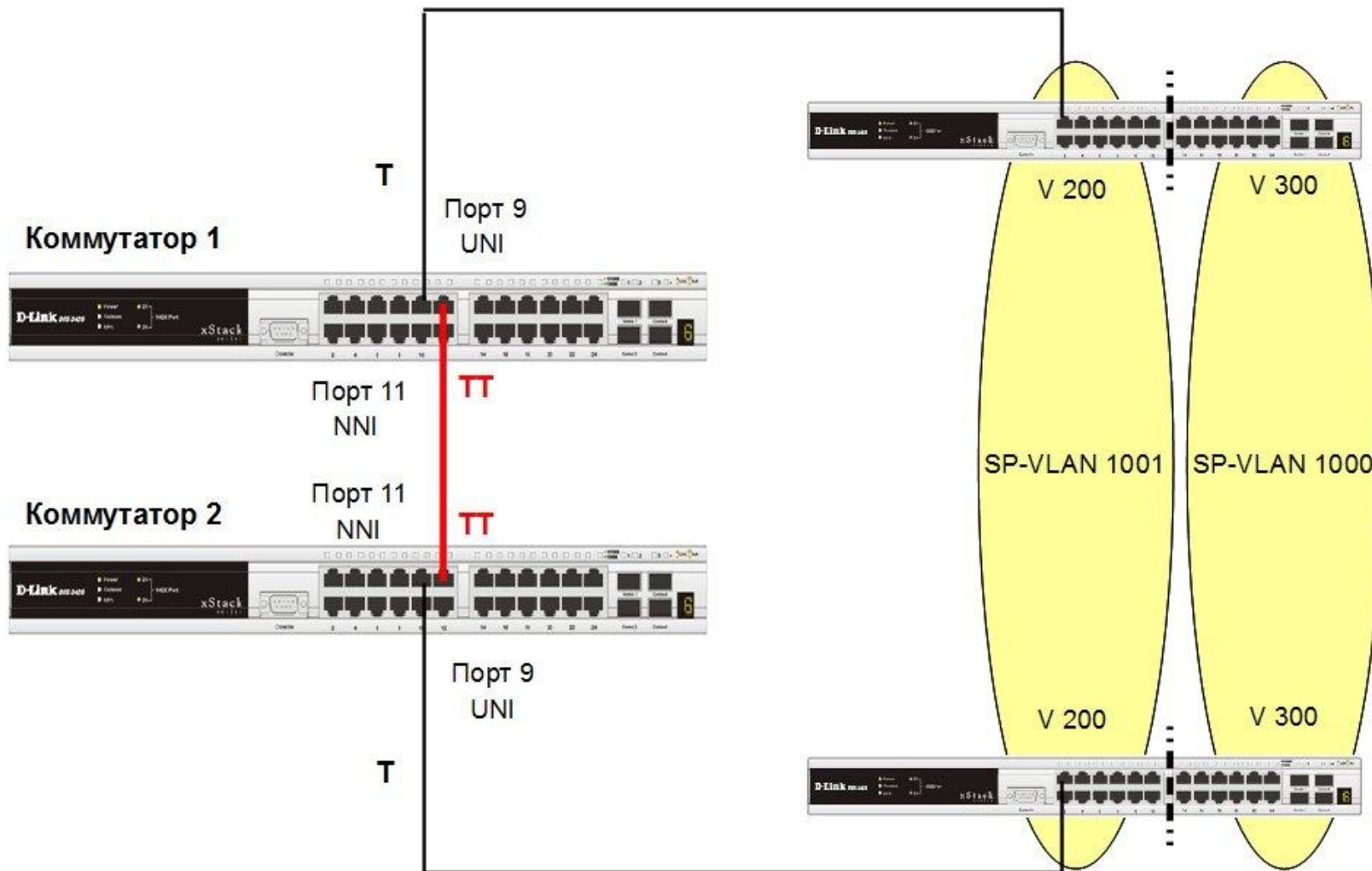
## Конфигурация ROS

# Настройка интерфейса маршрутизатора

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
```

# Q-in-Q VLAN

Два клиента, каждый включен в отдельную VLAN провайдера



## Базовая архитектура сети с функцией Port-based Q-in-Q



# Q-in-Q VLAN

## Пример настройки функции Port-based Q-in-Q

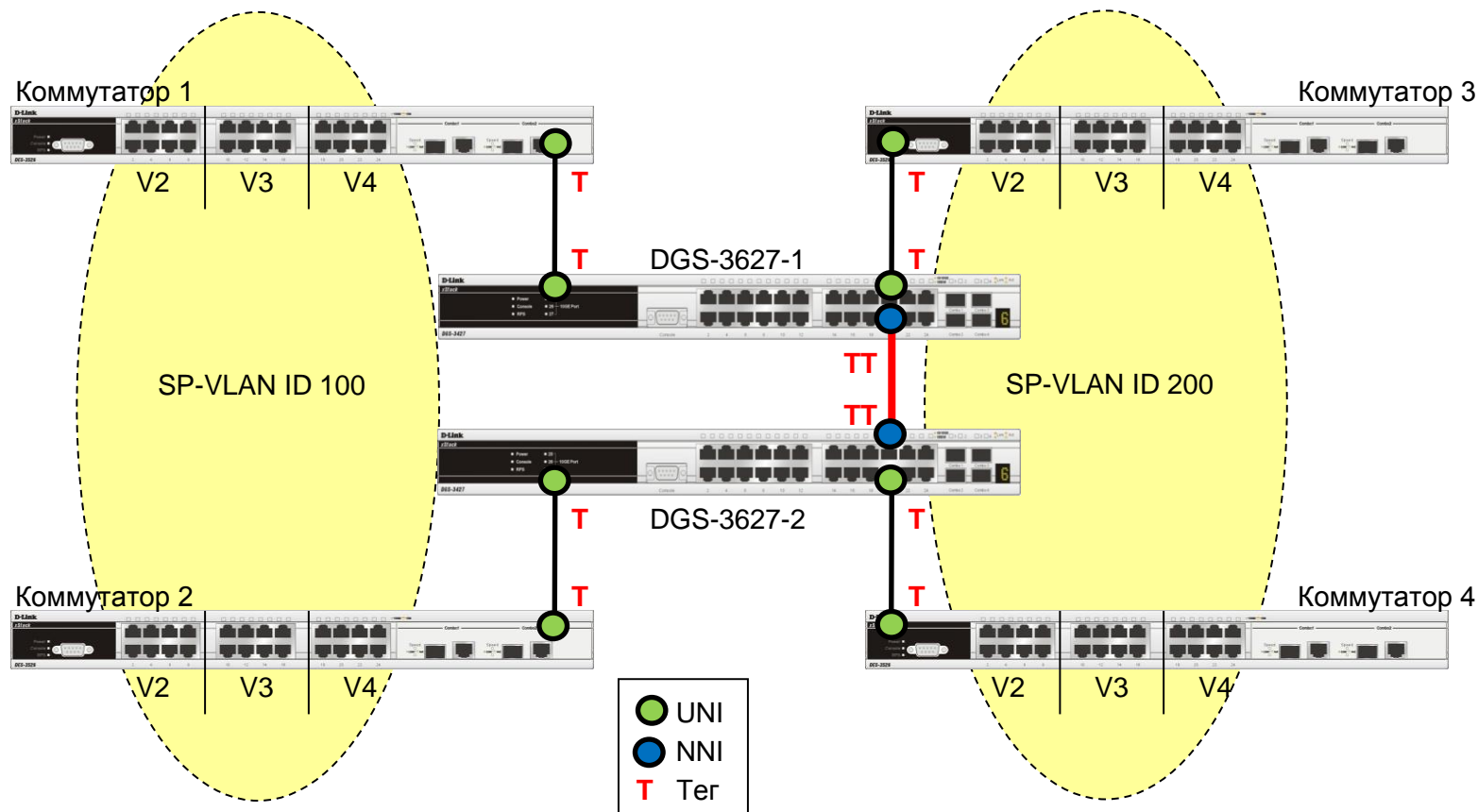


Схема подключения клиентских VLAN к сети провайдера услуг

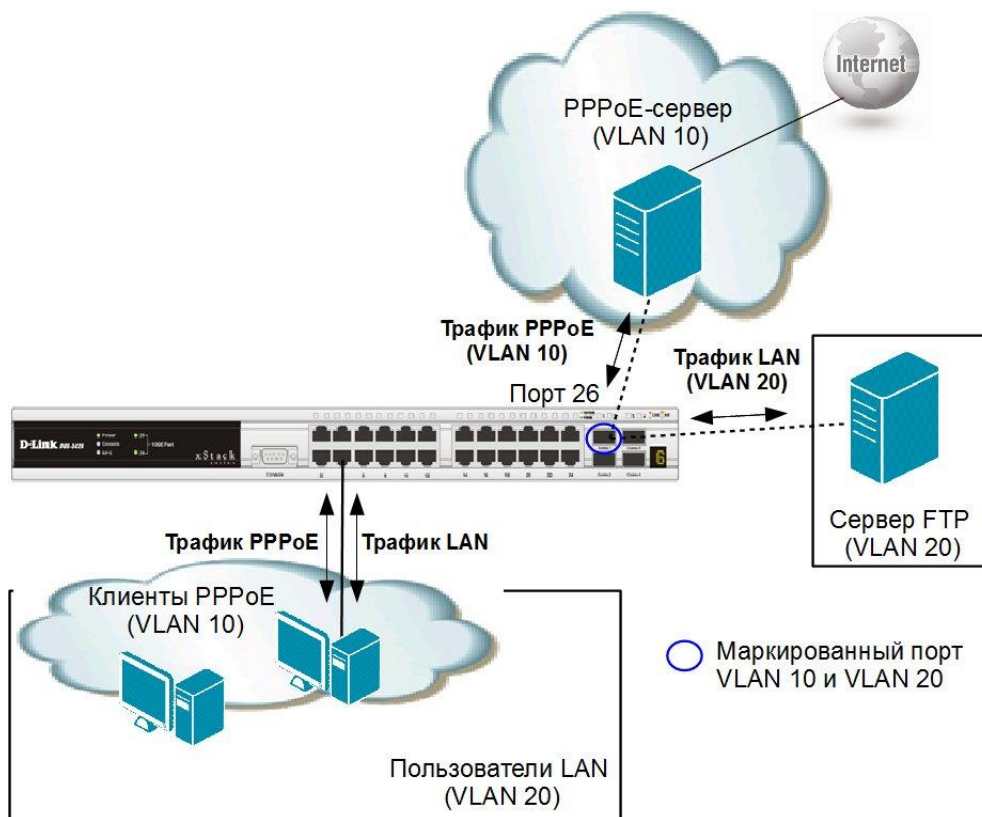
**Внимание:** функцию Q-in-Q VLAN необходимо настраивать только на устройствах сети провайдера услуг.



# VLAN на основе портов и протоколов – стандарт IEEE 802.1v

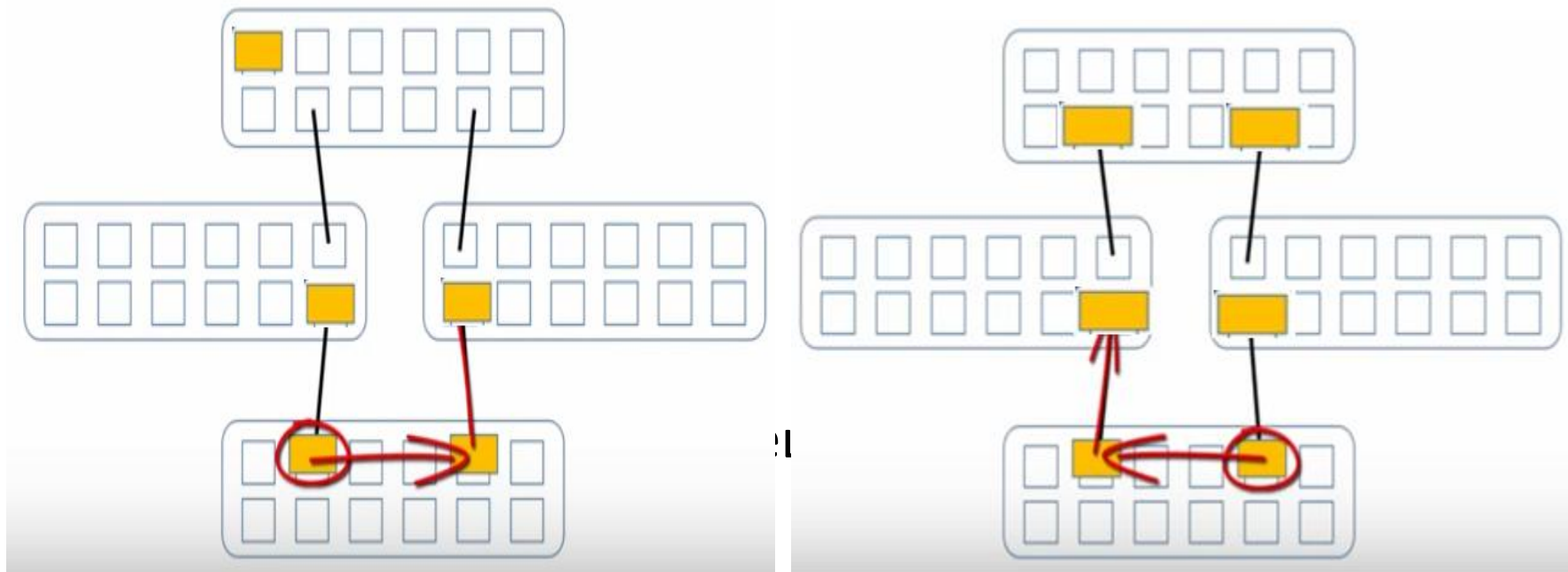
## Пример настройки IEEE 802.1v VLAN

Пользователи локальной сети находятся в выделенной VLAN (VLAN 20). Их подключение в Интернет осуществляется через PPPoE-сервер (VLAN 10). Для того чтобы трафик локальной сети был отделен от трафика PPPoE, на коммутаторе для протокола PPPoE создана VLAN 802.1v с идентификатором VID=10.





# Петли коммутаторов



- При получении кадра с неизвестным MAC-адресом коммутатор отправляет его на все порты
- Эту процедуру делают все коммутаторы. В результате кадры зацикливаются и размножаются. Резко возрастает трафик





# Протокол STP

## Протокол связующего (остовного) дерева (Spanning Tree Protocol, STP)

- Автоматическое отключение дублирующих соединений в Ethernet
- Связующее дерево – подграф без циклов, содержащий все вершины исходного графа

## Стандарт IEEE 802.1D

## Преимущества

- Надежность соединений между коммутаторами
- Защита от ошибок конфигурации



# Этапы работы STP

Выбор корневого коммутатора

Определение кратчайших путей до корневого коммутатора

Отключение всех остальных соединений



# Начало работы

Bridge Protocol Data Units (BPDU)

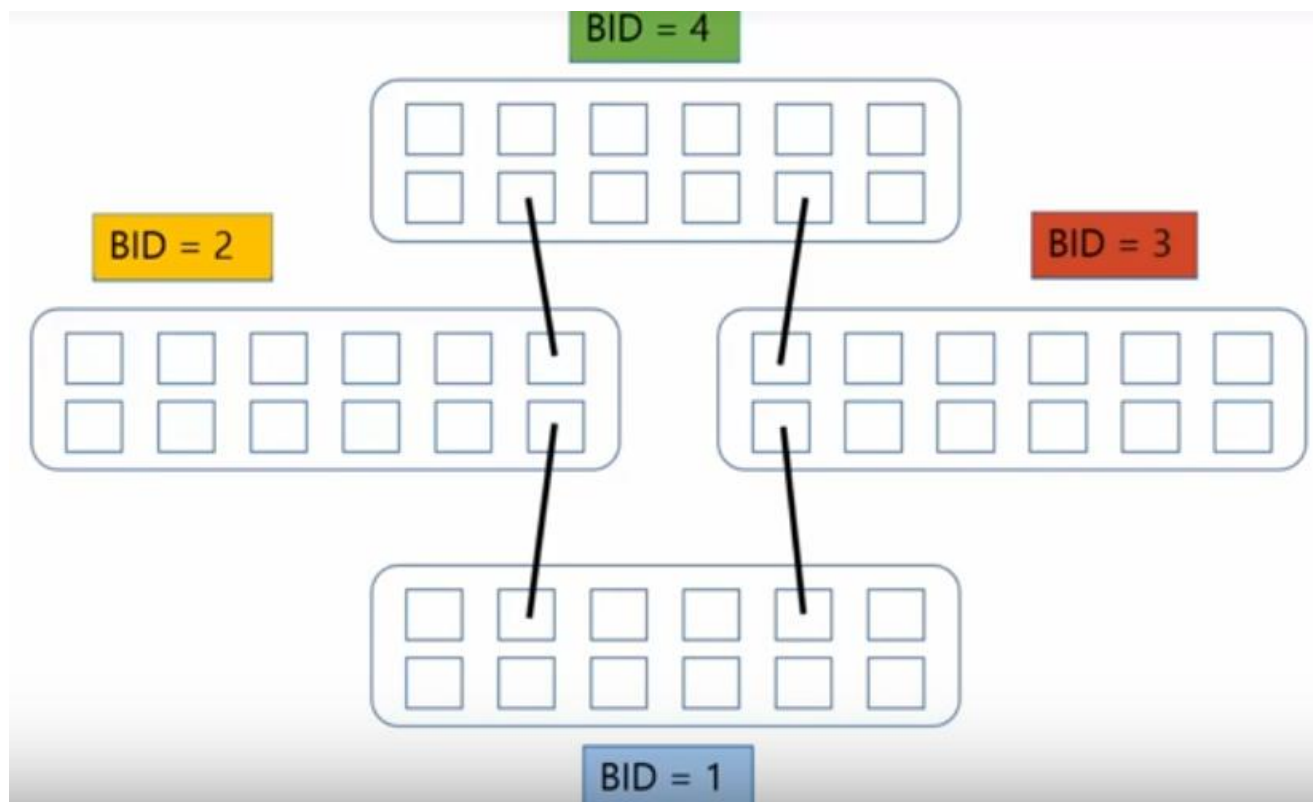
Отправляются каждые 2 секунды

Рассылаются на групповой адрес STP

- 01:80:C2:00:00:00



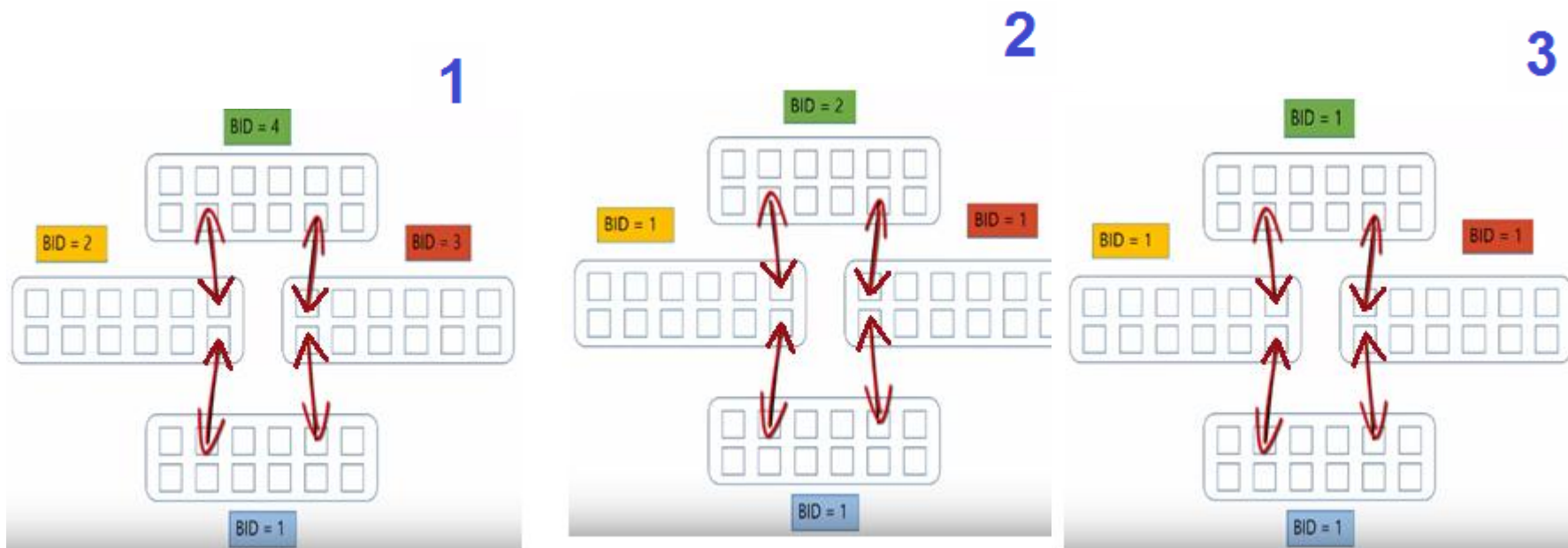
# Выбор корневого коммутатора



- Каждый коммутатор имеет свой идентификатор моста – BID
- BID может выбираться на основе MAC- адреса или назначаться администратором



# Выбор корневого коммутатора



1. Каждый коммутатор считает себя корневым и начинает рассылать BPDU-пакеты со своим идентификатором (BID) соседям.
2. Коммутаторы выбирают минимальный идентификатор и делают повторную рассылку, с другим минимальным BID
3. Через некоторое количество циклов все коммутаторы будут рассылать пакеты с минимальным BID
4. После этого момента BPDU-пакеты отправляет только корневой коммутатор (с минимальным ID)



# Расчет кратчайшего пути

- После выбора корневого коммутатора каждый из оставшихся коммутаторов рассчитывает кратчайшие пути до корневого
- Стоимость пути
  - Количество промежуточных маршрутизаторов
  - Скорость соединений
- Коммутаторы рассылают на все порты пакеты BPDU с минимальным расстоянием до корневого



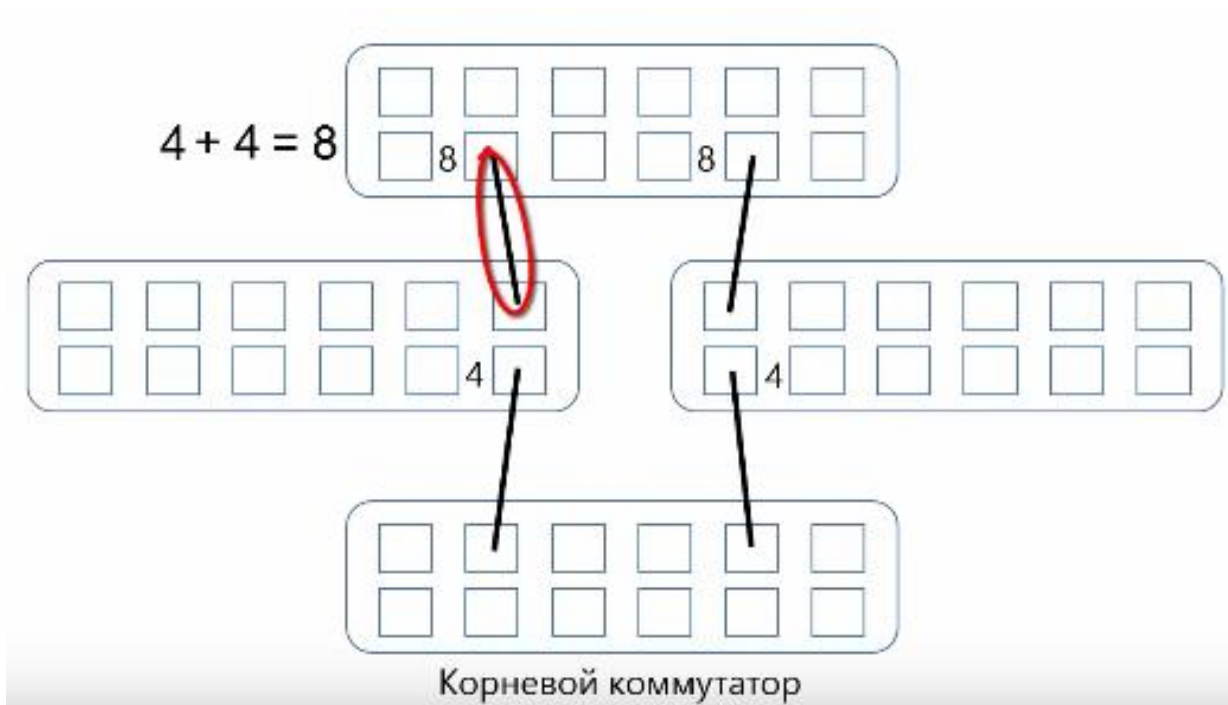
# Расчет кратчайшего пути

- Расчет стоимости пути приведен в стандарте IEEE 802.1d

Скорость соединения	Стоимость соединения в STP IEEE 802.1D
4 Mbit/s	250
10 Mbit/s	100
16 Mbit/s	62
100 Mbit/s	19
1 Gbit/s	4
2 Gbit/s	3
10 Gbit/s	2



# Расчет стоимости пути







# Отключение порта

- Выбирается путь с **наименьшей стоимостью**, остальные отключаются
- Если стоимость **одинакова**, отключается путь с **наибольшим номером порта**



- Номера портов считаются слева направо



## Состояние портов STP

**Listening** – порт обрабатывает BPDU, но не передает данные

**Learning** – порт не передает кадры, но изучает MAC-адреса в поступающих кадрах и формирует таблицу коммутации

**Forwarding** – порт принимает и передает кадры данных и BPDU

**Blocking** – порт заблокирован чтобы избежать кольцевого соединения

**Disabled** – порт выключен администратором



# Развитие STP

Переход от состояния Listening до Forwarding занимает 30 секунд

- Достаточно долго для современных крупных и часто меняющихся сетей

## RSTP (Rapid Spanning Tree Protocol)

- Улучшенная версия STP
- Срабатывает быстрее при подключении оборудования и изменении конфигурации сети
- Стандарт IEEE 802.1w

## STP и VLAN

- Multiple Spanning Tree Protocol (MSTP), 802.1s
- Отдельное связующее дерево для каждого VLAN



# Общая информация

- Одной из технологий повышения производительности сети является разделение крупных широковещательных доменов на более мелкие. Маршрутизаторы устроены таким образом, что блокируют широковещательный трафик на интерфейсе. При этом маршрутизаторы обычно имеют ограниченное количество интерфейсов LAN. Основная роль маршрутизатора заключается в передаче информации между сетями, а не в предоставлении оконечные устройства доступа к сети.
- Предоставление доступа в локальную сеть обычно обеспечивается коммутатором уровня доступа. Для уменьшения размера широковещательных доменов на коммутаторе 2-го уровня, как и на устройстве 3-го уровня, можно создать сеть VLAN. Сети VLAN обычно включаются в проекты сети, для того чтобы сеть облегчала процесс достижения целей организации.



## ■ Общая информация

Сети VLAN позволяют администратору производить сегментацию по функциям, проектным группам или областям применения, вне зависимости от физического расположения пользователя или устройства. Устройства в пределах сети VLAN работают таким образом, будто находятся в собственной независимой сети, даже если делят одну общую инфраструктуру с другими VLAN. Любой порт коммутатора может принадлежать сети VLAN. Одноадресные, широковещательные и многоадресные пакеты пересылаются и рассылаются только к конечным станциям в пределах той сети VLAN, которая является источником этих пакетов. Каждая сеть VLAN считается отдельной логической сетью, и пакеты, адресованные станциям, не принадлежащим данной сети VLAN, должны пересылаться через устройство, поддерживающее маршрутизацию.



## Общая информация

- **Безопасность:** группы, обладающие уязвимыми данными, отделены от остальной части сети, благодаря чему снижается вероятность утечки конфиденциальной информации. Как показано на рисунке, компьютеры преподавателей находятся в сети VLAN 10 и полностью отделены от трафика данных учащихся и гостей.
- **Снижение расходов:** благодаря экономии на дорогих обновлениях сетевой инфраструктуры и более эффективному использованию имеющейся полосы пропускания и восходящих каналов происходит снижение расходов.
- **Повышение производительности:** разделение однородных сетей 2-го уровня на несколько логических рабочих групп (широковещательных доменов) уменьшает количество лишнего сетевого трафика и повышает производительность.
- **Уменьшенные широковещательные домены:** разделение сети на сети VLAN уменьшает количество устройств в широковещательном домене. Сеть, показанная на рисунке, состоит из шести компьютеров и трёх широковещательных доменов: для преподавателей, для учащихся и гостевого домена.
- **Повышение производительности ИТ-отдела:** сети VLAN упрощают управление сетью, поскольку пользователи с аналогичными требованиями к сети используют одну и ту же сеть VLAN. При введении в эксплуатацию нового коммутатора на назначенных портах реализуются все правила и процедуры, уже применённые в этой конкретной VLAN. Также ИТ-специалистам легче определять функцию сети VLAN, назначая ей соответствующее имя. На данном рисунке для простой идентификации сеть VLAN 10 была названа «Для преподавателей», VLAN 20 — «Для учащихся» и VLAN 30 — «Гостевая».
- **Упрощённое управление проектами и приложениями:** сети VLAN объединяют пользователей и сетевые устройства для соответствия деловым или географическим требованиям сети. Управление проектом и работа на прикладном уровне упрощены благодаря использованию разделения функций. Пример такой прикладной задачи — платформа разработки приложений для электронного обучения преподавателей.