



# Сетевой инженер VLAN и маршрутизация между VLAN

otus.ru

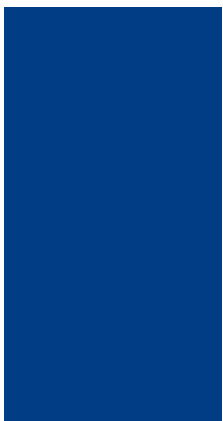
• REC Проверить, идет ли запись

**Меня хорошо видно  
&& слышно?**



Тема вебинара

# VLAN и маршрутизация между VLAN



**Николай Колесов**

**Эксперт ТАС**

**Релевантный опыт**

19 лет в сетевых технологиях

Вендоры, операторы связи, энтерпрайз

# Правила вебинара



Активно  
участвуем



Отвечаем на  
вопросы



Задаем вопросы в чате или голосом  
во время секций Q&A

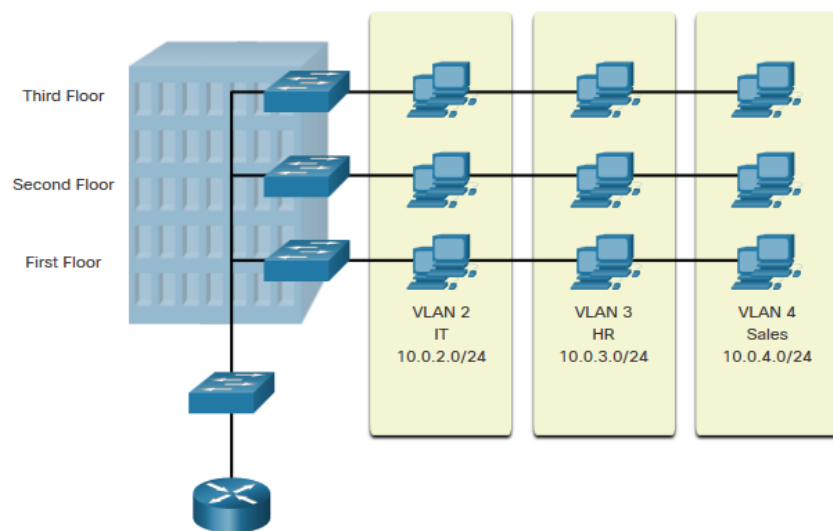


Вопросы вижу в чате,  
отвечу во время секций Q&A

# Для чего нужен VLAN



## Определение сети VLAN

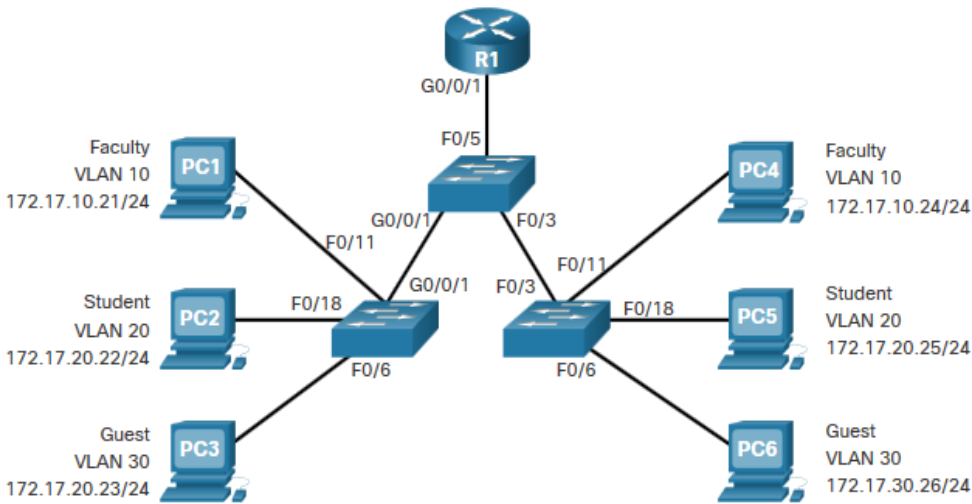


VLAN делят сеть на отдельные широковещательные домены, как следствие:

- Разделяют различные группы устройств, подключенные к одним и тем же коммутаторам
- Способствуют более удобному и безопасному управлению:
  - Широковещательные, многоадресные и одноадресные передачи изолированы в отдельной VLAN
  - Каждая VLAN может иметь свой уникальный диапазон IP-адресации
  - Меньший размер широковещательных доменов
  - Свой набор правил безопасности

# Обзор сетей VLAN

## Преимущества сетей VLAN



Преимущества	Описание
Меньший размер широковещательных доменов	Разделение локальной сети уменьшает количество широковещательных доменов
Повышенный уровень безопасности	Только пользователи одной и той же сети VLAN могут общаться напрямую между собой по L2
Повышение эффективности ИТ-инфраструктуры	VLAN могут группировать устройства с аналогичными требованиями, например, преподаватели и студенты
Снижение затрат	Один коммутатор может поддерживать несколько VLAN
Повышение производительности	Малые широковещательные домены уменьшают трафик, улучшая пропускную способность
Упрощенное и более безопасное управление	Подобным группам понадобятся аналогичные приложения и другие сетевые ресурсы



## VLAN по умолчанию

- VLAN 1 является VLAN по умолчанию
- Невозможно удалить или переименовать
- Сеть управления по умолчанию
- Native VLAN на транках по умолчанию

```
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



# Обзор сетей VLAN

## Типы VLAN

### **VLAN для данных**

- Передает пользовательский трафик
- VLAN 1 является VLAN для данных по умолчанию, так как для этой VLAN назначены все интерфейсы.

### **Native VLAN с нетегированным трафиком**

- Используется только для транков
- Все кадры помечены на магистральном канале 802.1Q, за исключением тех, которые находятся в собственной VLAN.

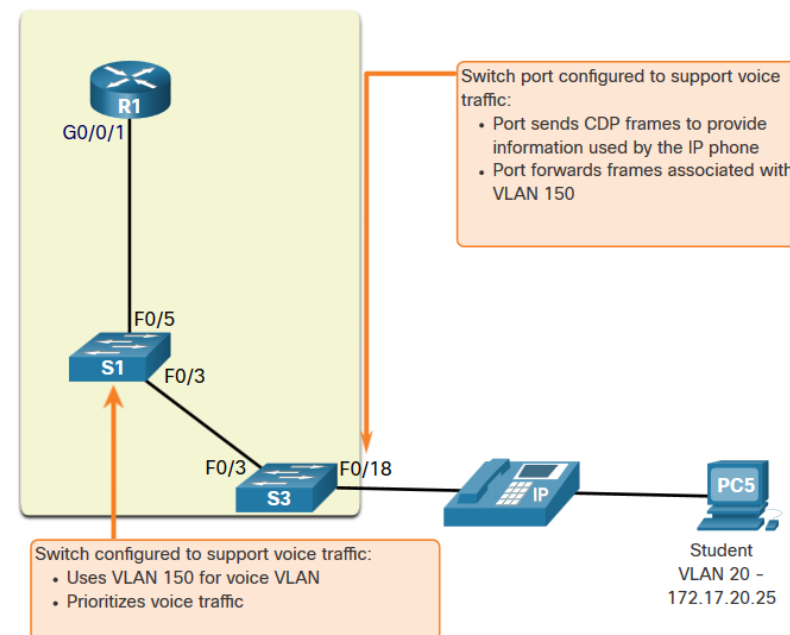
### **Сеть VLAN управления (Management VLAN)**

- Это используется для SSH/Telnet VTY трафика и не должно переноситься с трафиком конечного пользователя.

## Типы сетей VLAN

### Голосовой VLAN

- Отдельный VLAN, т.к. для голосового трафика может потребоваться:
  - Гарантированная пропускная способность
  - Высокий приоритет QoS
  - Задержка менее 150 мс от источника к месту назначения
- Вся сеть должна быть спроектирована для поддержки голосовой связи (политик QoS).



# Вопросы?



Ставим “+”,  
если вопросы есть



Ставим “-”,  
если вопросов нет

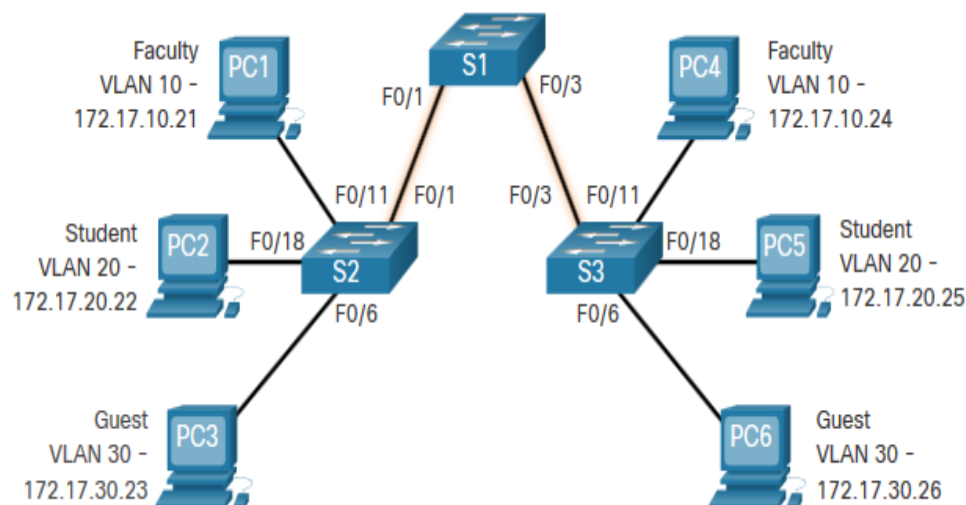
# **VLAN в среде с несколькими коммутаторами**

# Сети VLAN в среде с несколькими коммутаторами

## Магистраль сетей VLAN (trunks)

Функции trunk:

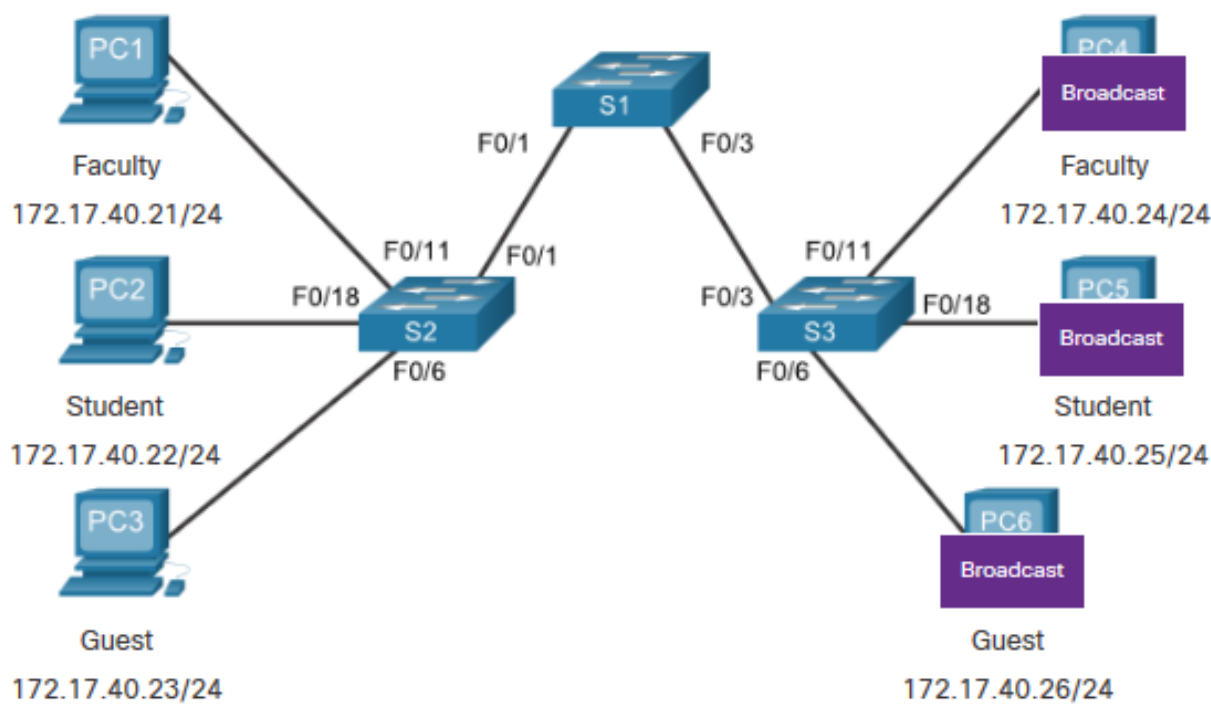
- Разрешить несколько VLAN на одном порту
- Расширение VLAN на несколько коммутаторов
- По умолчанию разрешены все VLAN
- 802.1Q (vs ISL)



# Виртуальные локальные сети в среде с несколькими коммутаторами

## Сети без VLAN

Без VLAN все устройства, подключенные к коммутаторам, будут получать весь одноадресный (**u**nknown **u**nicast), многоадресный (**m**ulticast) и широковещательный (**b**roadcast) (**BUM**) трафик.

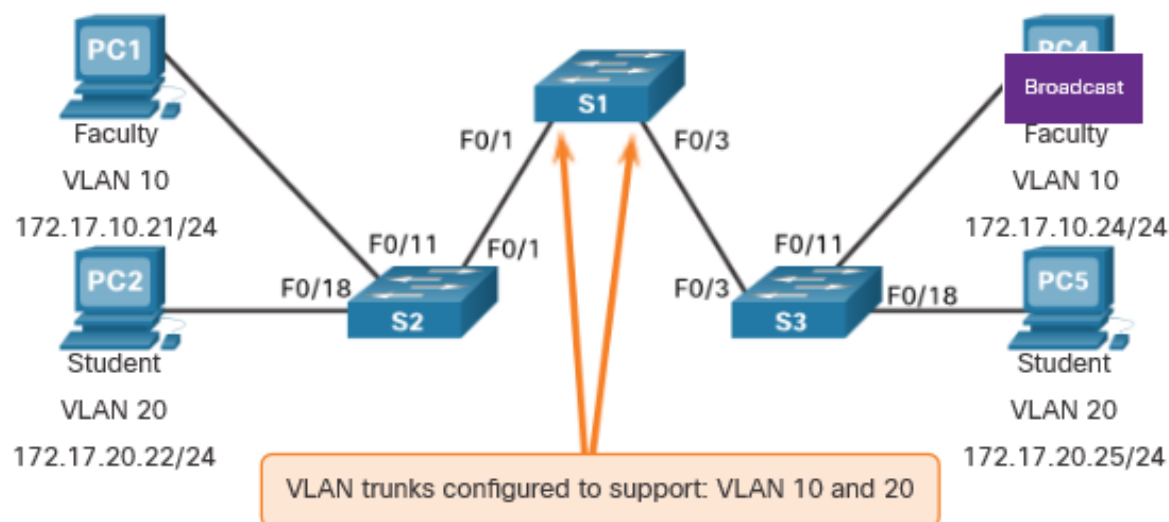


PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame out all available ports.

## Сети без VLAN

В VLAN одноадресный (unicast), многоадресный (multicast) и широковещательный (broadcast) трафик ограничен VLAN.

Устройства в разных VLAN не могут обмениваться данными, для этого необходимо устройство уровня 3 (маршрутизатор).

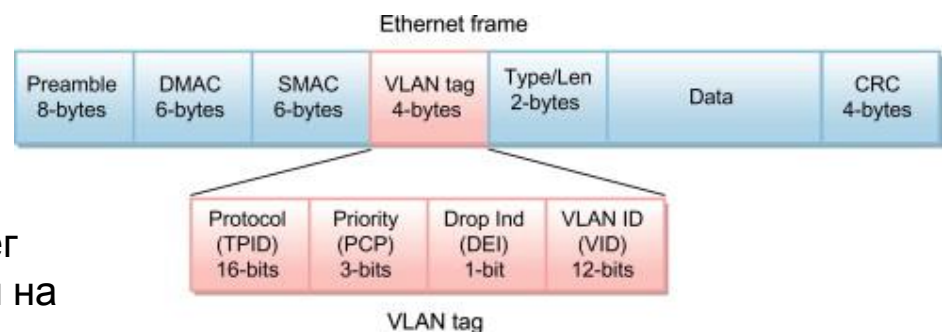


PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.

# Сети VLAN в среде с несколькими коммутаторами

## Тегирование кадров Ethernet для идентификации сети VLAN

- Заголовок IEEE 802.1Q составляет 4 байта
- При создании тега 802.1Q необходимо пересчитать FCS (CRC)
- При отправке на конечные устройства этот тег должен быть удален и FCS снова пересчитан на исходное значение



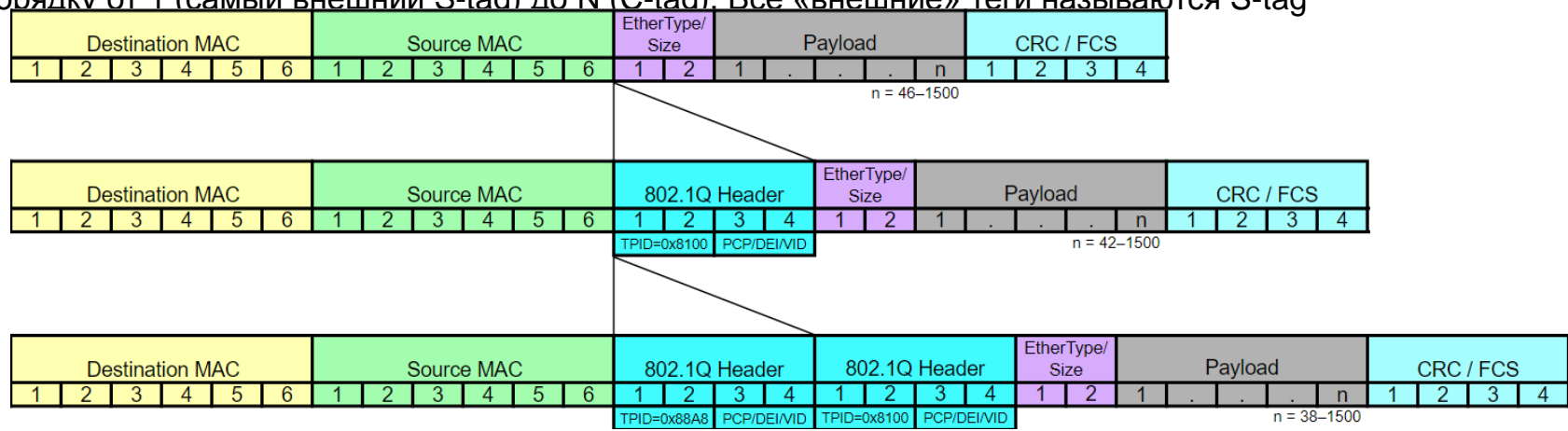
Поле тегов VLAN 802.1Q		Функция
Tag protocol identifier (TPID)		<ul style="list-style-type: none"><li>16 бит</li><li>0x8100</li></ul>
Tag control information (TCI)	Priority code point (PCP)	<ul style="list-style-type: none"><li>3 бита</li><li>Class of Service (CoS), IEEE 802.1p</li></ul>
	Drop eligible indicator (DEI)	<ul style="list-style-type: none"><li>1 бит</li><li>Указывает на то, может ли фрейм быть сброшен в случае перегрузки</li><li>Ранее назывался Canonical Format Indicator (CFI) и использовался для совместимости с Token Ring</li></ul>
	VLAN identifier (VID)	<ul style="list-style-type: none"><li>12 бит =&gt; до 4096 VLAN</li><li>0 и 4095 зарезервированы</li><li>0 может использоваться как priority tag (фрейм считается нетегированным, а тег нужен для переноса информации CoS)</li></ul>



# Сети VLAN в среде с несколькими коммутаторами

## Многократное тегирование кадров (Q-in-Q)

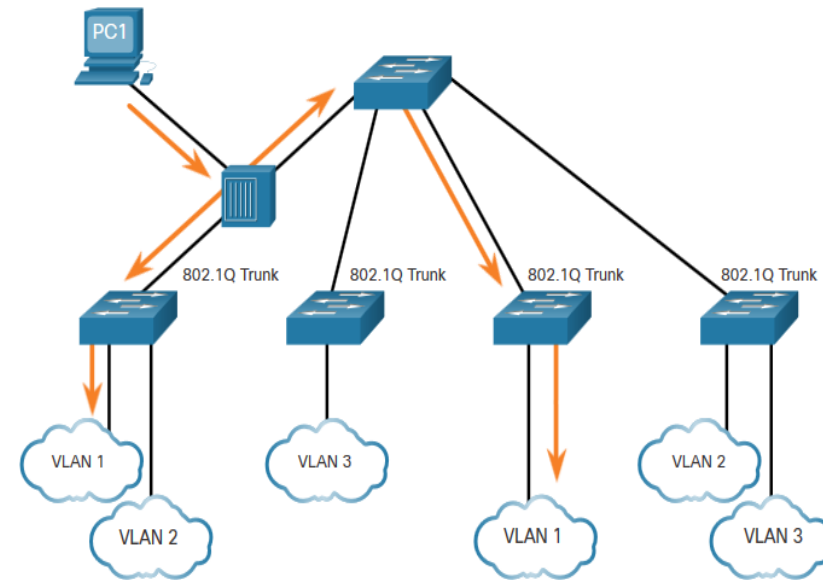
- Может понадобиться передавать теги между сегментами сети, где они не созданы или пересекаются (например, в сети сервис провайдера)
- Тегированный фрейм можно инкапсулировать в новый тег
- «Внешний» (outer) тег – Service tag или S-tag
- «Внутренний» (inner) тег – Customer tag или C-tag
- S-tag TPID = 0x88a8
- FCS пересчитывается каждый раз при изменении стека тегов
- IEEE 802.1ad
- Стандарт не запрещает использовать более одного S-tag. В этом случае, теги нумеруются по порядку от 1 (самый внешний S-tag) до N (C-tag). Все «внешние» теги называются S-tag



# Сети VLAN в среде с несколькими коммутаторами

## Native VLAN

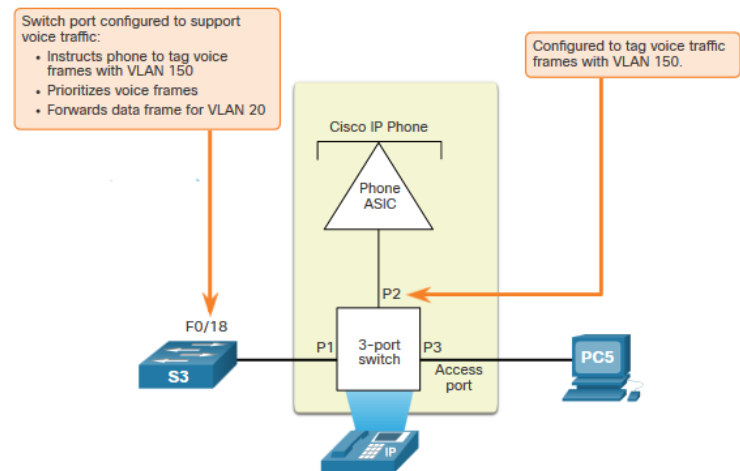
- Использование native VLAN было разработано для совместимости с устаревшим оборудованием, например, концентраторами/hub (см. пример)
- По умолчанию VLAN 1 является нативным VLAN.
- Оба конца транка должны быть сконфигурированы с одним и тем же нативным VLAN \*
- Каждый транк настраивается отдельно, поэтому на отдельных транках можно иметь разные нативные VLAN.



# Сети VLAN в среде с несколькими коммутаторами

## Голосовой VLAN

- VoIP телефон представляет собой трехпортовый коммутатор:
- Коммутатор будет использовать CDP для информирования телефона о голосовом VLAN.
  - Телефон помечает свой собственный трафик (Voice) и может установить стоимость обслуживания (CoS). CoS является QoS для уровня 2.
  - Телефон может помечать или не помечать кадры с ПК.



Трафик	Функция маркировки
Голосовой VLAN	в голосовой VLAN, тегированной значением приоритета класса обслуживания (CoS) уровня 2;
VLAN доступа	также может быть помечен значением приоритета CoS уровня 2
VLAN доступа	VLAN нетегирован (без значения приоритета CoS уровня 2).

# Сети VLAN в среде с несколькими коммутаторами

## Голосовой VLAN - пример

Команда **show interfaces fa0/18 switchport** показывает информацию о VLAN, назначенных интерфейсу, включая голосовой

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
```

# Вопросы?



Ставим “+”,  
если вопросы есть



Ставим “-”,  
если вопросов нет

# Конфигурация VLAN

# Диапазоны VLAN на коммутаторах Catalyst

Коммутаторы Catalyst 2960 и 3560 способны поддерживать более 4000 сетей VLAN.

```
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
```

VLAN нижнего диапазона 1-1005	VLAN расширенного диапазона 1006-4096
Используется в малых и средних предприятиях	Используется поставщиками услуг
1002 — 1005 зарезервированы для старых VLAN	в файле текущей конфигурации Running-Config
1, 1002 — 1005 создаются автоматически и не могут быть удалены	Требуется конфигурация VTP
Хранится в файле vlan.dat во флэш-памяти	
VTP может синхронизировать между коммутаторами	

# VLAN конфигурация

## Команды создания VLAN

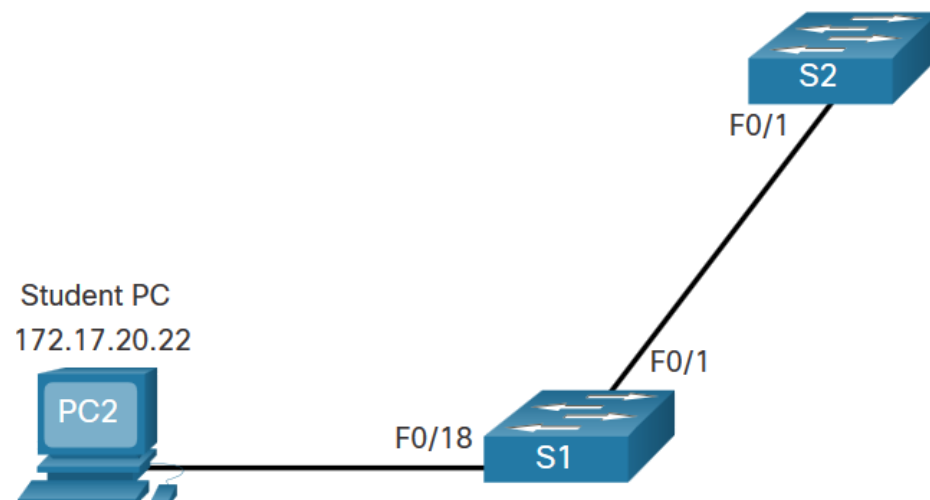
Создание VLAN в режиме глобальной конфигурации.

Задача	Команда IOS
Войдите в режим глобальной настройки.	Switch# <b>configure terminal</b>
Создайте сеть VLAN с допустимым номером идентификатора.	Switch(config)# <b>vlan</b> <i>vlan-id</i>
Укажите уникальное имя для идентификации сети VLAN.	Switch(config-vlan)# <b>name</b> <i>vlan-name</i>
Вернитесь в привилегированный режим.	Switch (config-vlan) # <b>end</b>
Войдите в режим глобальной настройки.	Switch# <b>configure terminal</b>



## Команды создания VLAN - пример

- Если студенческий ПК будет находиться в VLAN 20, сначала создадим VLAN, а затем назовем ее (от 1 до 32 символов ASCII )
- Если его не назвать, Cisco IOS присваивает ему имя `vlan` по умолчанию и четырехзначный номер VLAN. Например, `vlan0020` для VLAN 20.



Командная строка	Команда
S1#	Configure terminal
S1(config)#	vlan 20
S1 (config-vlan) #	name student
S1 (config-vlan) #	end

## Команды назначения портов VLAN

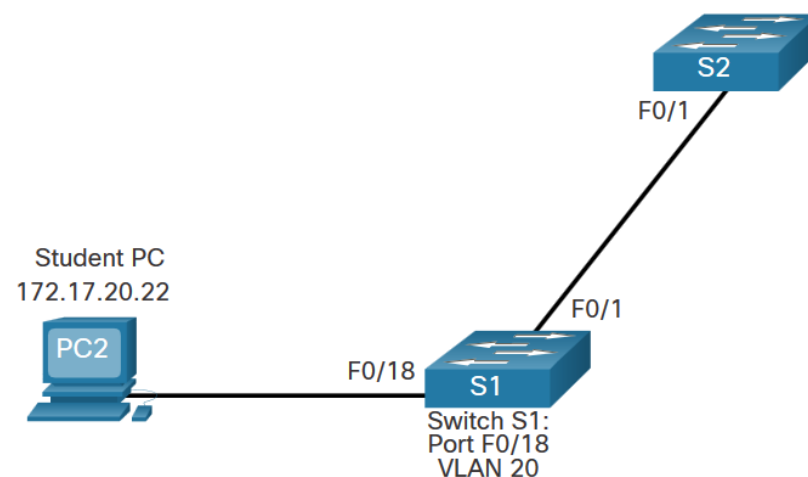
Задача	Команда
Режим глобальной конфигурации.	Switch# <b>configure terminal</b>
Режим конфигурации интерфейса.	Switch(config)# <b>interface</b> <i>interface-id</i>
Перевод порт в режим доступа.	Switch(config-if)# <b>switchport mode access</b>
Назначение VLAN.	Switch(config-if)# <b>switchport access vlan</b> <i>vlan-id</i>
Возврат в привилегированный режим.	Switch(config-if)# <b>end</b>



## Команды назначения портов VLAN - пример

Мы можем назначить VLAN интерфейсу.

- После назначения устройству VLAN ему потребуется информация об IP-адресе для этой VLAN
- Здесь Студенческий ПК получает 172.17.20.22

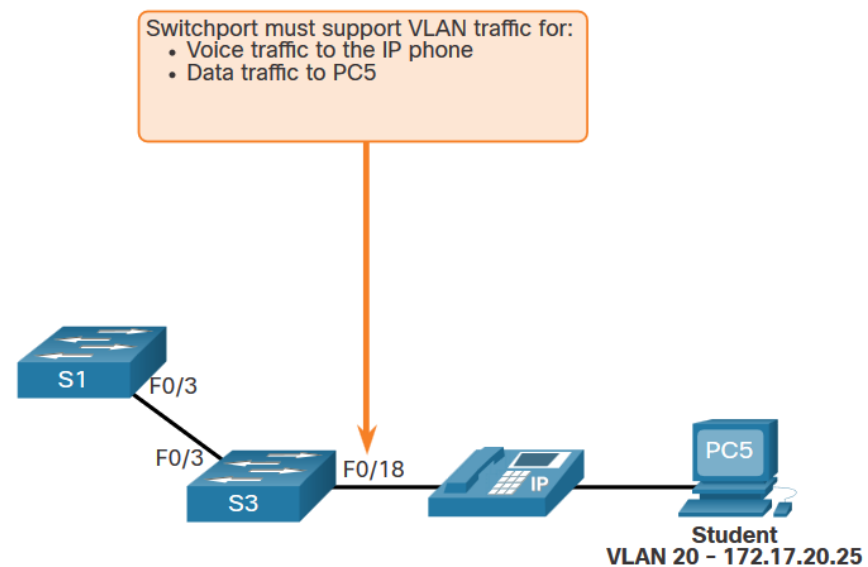


Командная строка	Команда
S1#	Настройте терминал
S1(config)#	Interface fa0/18
S1(config-if)#	switchport mode access
S1(config-if)#	switchport access vlan 20
S1(config-if)#	end

# Данные конфигурации VLAN и голосовые VLAN

Порту доступа (access) можно назначить только один VLAN.

Однако можно назначить голосовой VLAN



# Данные конфигурации VLAN и голосовые VLAN

- Мы хотим создать и назвать VLAN для голоса и данных .
- Помимо назначения VLAN данных, мы также назначим голосовой VLAN и настроим доверие получаемым значениям QoS для голосового трафика к интерфейсу.
- Новый коммутатор автоматически создаст VLAN, если его еще не существует.

```
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# vlan 150
S1(config-vlan)# name VOICE
S1(config-vlan)# exit
S1(config)# interface fa0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# mls qos trust cos
S1(config-if)# switchport voice vlan 150
S1(config-if)# end
```

```
% Access VLAN does not exist. Creating vlan 30
```

# VLAN конфигурация

## Проверьте конфигурацию сети VLAN.

Использование команды **show vlan** Полный синтаксис:

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

```
S1# show vlan summary
Number of existing VLANs           : 7
Number of existing VTP VLANs      : 7
Number of existing extended VLANs : 0
```

```
S1# show interface vlan 20
Vlan20 is up, line protocol is up
  Hardware is EtherSVI, address is 001f.6ddb.3ec1 (bia 001f.6ddb.3ec1)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set

(Output omitted)
```

Задача	Вариант команды
Отображает имя, состояние и порты VLAN по одной VLAN на строку.	<b>brief</b>
Отображает информацию о VLAN по номеру идентификатора VLAN.	<b>id</b> <i>vlan-id</i>
Отображает информацию об имени одной сети VLAN. <i>Имя VLAN</i> — это код ASCII размером от 1 до 32 символов.	<b>name</b> <i>vlan-name</i>

# Конфигурация VLAN

## Изменение членства порта VLAN

Существует несколько способов изменить членство в VLAN:

- повторно использовать команду **switchport access vlan** *vlan-id*
- использовать команду **no switchport access vlan** для возвращения интерфейса обратно в VLAN 1

Используйте команды **show vlan brief** или **show interface fa0/18 switchport** для проверки правильности связи VLAN.

```
S1(config)# interface fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1#
S1# 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
20	student	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

# Конфигурация VLAN

## Удаление VLAN

S1(config)# **no vlan** *vlan-id*

Перед удалением сети VLAN необходимо сначала переназначить все ее порты другой сети VLAN

### Удаление всей VLAN database

- **delete flash:vlan.dat** или команды **delete vlan.dat** .
- Перезагрузить коммутатор

### Полный сброс коммутатора

- удалить начальную конфигурацию **write erase**
- удалите файл vlan.dat
- перезагрузить устройство



# Вопросы?



Ставим “+”,  
если вопросы есть



Ставим “-”,  
если вопросов нет

# VLAN trunk

## Команды конфигурации транка

Задача	Команда IOS
Режим глобальной конфигурации	Switch# <b>configure terminal</b>
Режим конфигурации интерфейса	Switch(config)# <b>interface</b> <i>interface-id</i>
Статическое назначение режима работы	Switch(config-if)# <b>switchport mode trunk</b>
Native VLAN, отличный от VLAN 1 по умолчанию	Switch(config-if)# <b>switchport trunk native vlan</b> <i>vlan-id</i>
Список VLAN, разрешенных на транке	Switch(config-if)# <b>switchport trunk allowed</b> <b>vlan</b> <i>vlan-list</i>
Завершение настройки и возврат в eхес режим	Switch(config-if)# <b>end</b>

# Команды конфигурации транка

Switch(config-if)# **switchport trunk allowed vlan** *vlan-list*

Команда **переписывает** список всех ранее настроенных VLAN на *vlan-list*

Например,

```
swi-00# sho run int e1/49
interface Ethernet1/49
  description Super important stuff
  switchport mode trunk
  switchport trunk allowed vlan 2-3,12,100,110-
112,151,300,302,400-
402,666,700,702,704,706,708,710,712,1106,1120,1124,1126,11
28,1130,1132,1134,1136,1138,1140,2300,2302,2306,2310,2316,
2318,2320,2324,2326,2328,2334,2336,2338,2342,2344,3200-
3203,3210-3214,3241-3242,3244
```

```
swi-00# conf t
swi-00(config)# int e1/49
swi-00(config-if)# switchport trunk allowed vlan 99
```

```
swi-00(config-if)# do sho run int e1/49
interface Ethernet1/49
  description Super important stuff
  switchport mode trunk
  switchport trunk allowed vlan 99
```

# Команды конфигурации транка

ВСЕГДА используйте **add** для добавления VLAN

```
swi-00(config)# int e1/49  
swi-00(config-if)# switchport trunk allowed vlan add 99
```

Некоторые платформы требуют, чтобы при первичной настройке порта первая команда была без add. Тогда можно использовать:

```
switchport trunk allowed vlan none
```

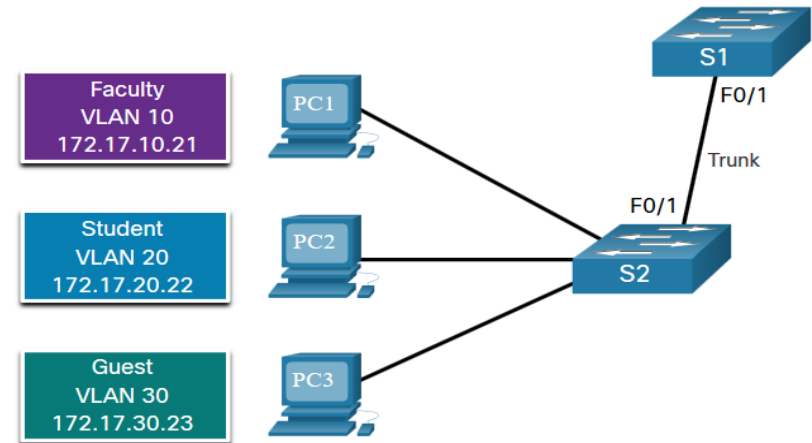
Для **удаления** VLAN с транка используется ключевое слово **remove**

```
swi-00(config-if)# switchport trunk allowed vlan remove 99
```

# Команды конфигурации транка - пример

К каждой VLAN относятся следующие подсети:

- VLAN 10 - Faculty/Staff - 172.17.10.0/24
- VLAN 20 - Students - 172.17.20.0/24
- VLAN 30 - Guests - 172.17.30.0/24
- VLAN 99 - Native - 172.17.99.0/24



Командная строка	Команда
S1(config)#	Interface fa0/18
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

Порт F0/1 на S1 настроен как магистральный порт.

# VLAN транки

## Проверка настроек

**sh int fa0/1 switchport :**

- Настройки режима работы порта
- Фактический режим работы порта
- Инкапсуляция dot1q = 802.1q
- Native VLAN - 99
- Все VLAN, созданные на коммутаторе, разрешены на этом транке

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# no switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

# VLAN транки

## Сброс в состояние по умолчанию

- Сброс параметров с помощью команды **no**.
  - Все VLAN, разрешенные для прохождения трафика
  - Native VLAN = VLAN 1
- Проверка настроек

```
sh int fa0/1 switchport
```

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

```
S1(config)# interface fa0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
```



# Вопросы?



Ставим “+”,  
если вопросы есть



Ставим “-”,  
если вопросов нет

# Dynamic Trunking Protocol (DTP)

# Динамический протокол транкинга

## Общие сведения о DTP

Протокол динамического транкинга (DTP) — это собственный протокол Cisco.

Характеристики DTP:

- Включен по умолчанию на коммутаторах Catalyst
- dynamic-auto используется по умолчанию для коммутаторов 2960 и 2950
- Может быть отключен с помощью команды nonegotiate
- Может быть снова включен, установив интерфейс на dynamic-auto
- Статически заданный режим работы trunk (`switchport mode trunk`) или access (`switchport mode access`) позволит избежать проблем согласования и **является рекомендованным**

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

```
S1(config-if)# switchport mode dynamic auto
```

# Динамический протокол транкинга

## Режимы интерфейса для согласования

Команда **switchport mode** имеет дополнительные параметры.

Используйте команду конфигурации интерфейса **switchport nonegotiate**, чтобы остановить согласование DTP.

Параметр	Описание
<b>access</b>	Режим постоянного доступа и согласовывает преобразование соседнего порта в access при DTP
<b>dynamic auto</b>	Trunk, если соседний интерфейс установлен в транк или режим dynamic desirable
<b>dynamic desirable</b>	Активно стремится стать Trunk путем переговоров с другими auto или desirable интерфейсами
<b>trunk</b>	режим постоянного транкинга и согласовывает преобразование соседнего канала в trunk при DTP

# Динамический протокол транкинга (DTP)

## Результаты настройки DTP

Варианты конфигурации DTP являются следующими:

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Ограниченные возможности подключения
Access	Access	Access	Ограниченные возможности подключения	Access

# Dynamic Trunking Protocol (DTP)

## Проверка режима DTP

Конфигурация DTP по умолчанию зависит от версии и платформы Cisco IOS.

- Используйте команду **show dtp interface** для определения текущего режима DTP.
- Рекомендуется устанавливать для интерфейсов режим работы статически и отключать DTP

```
S1# show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE
Neighbor address 1: C80084AEF101
Neighbor address 2: 000000000000
Hello timer expiration (sec/state): 11/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state: S2:ACCESS
# times multi & trunk 0
Enabled: yes
In STP: no
```

# Вопросы?



Ставим “+”,  
если вопросы есть



Ставим “-”,  
если вопросов нет

# Маршрутизация между VLAN



# Процесс маршрутизации между сетями VLAN

## Что такое маршрутизация между сетями VLAN?

VLAN используются для сегментации коммутируемых сетей уровня 2 по разным причинам.

Хосты в одном VLAN не могут взаимодействовать с хостами в другом VLAN, если нет маршрутизатора или коммутатора уровня 3 для предоставления услуг маршрутизации.

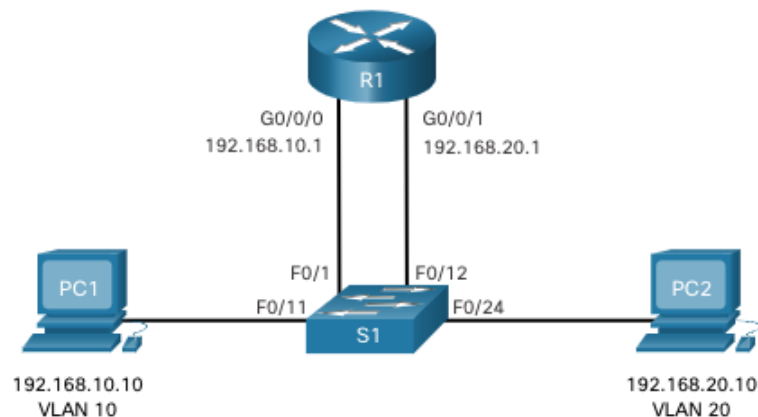
Маршрутизация между сетями VLAN — это процесс переадресации сетевого трафика из одной сети VLAN в другую с помощью маршрутизатора.

Существуют три варианта маршрутизации между VLAN.

- **«Старый метод» маршрутизации между VLAN** – маршрутизатор включается отдельным физическим портом в порт коммутатора в каждом VLAN. Плохо масштабируется
- **Router-on-a-Stick** - это приемлемое решение для сети малых и средних размеров.
- **Коммутатор уровня 3 с использованием коммутируемых виртуальных интерфейсов (SVI)** — это наиболее масштабируемое решение для средних и крупных организаций.

# Устаревший метод маршрутизации между сетями VLAN

- Первое решение маршрутизации между VLAN основывалось на использовании маршрутизатора с несколькими интерфейсами Ethernet. Каждый интерфейс маршрутизатора был подключен к порту коммутатора в разных VLAN. Интерфейсы маршрутизатора служат шлюзами по умолчанию для локальных узлов в подсети VLAN.
- Устаревший метод маршрутизации между VLAN, использующий физические интерфейсы, имеет большие ограничения. Он не является достаточно масштабируемым, поскольку маршрутизаторы имеют ограниченное количество физических интерфейсов. По мере возрастания количества VLAN в сети, требующих по одному физическому интерфейсу на каждую VLAN, количество свободных интерфейсов маршрутизатора быстро уменьшается.



# Процесс маршрутизации между сетями VLAN

## Маршрутизация между сетями VLAN с помощью метода Router-on-a-Stick

Для маршрутизации трафика между несколькими сетями VLAN в сети требуется только один физический интерфейс Ethernet.

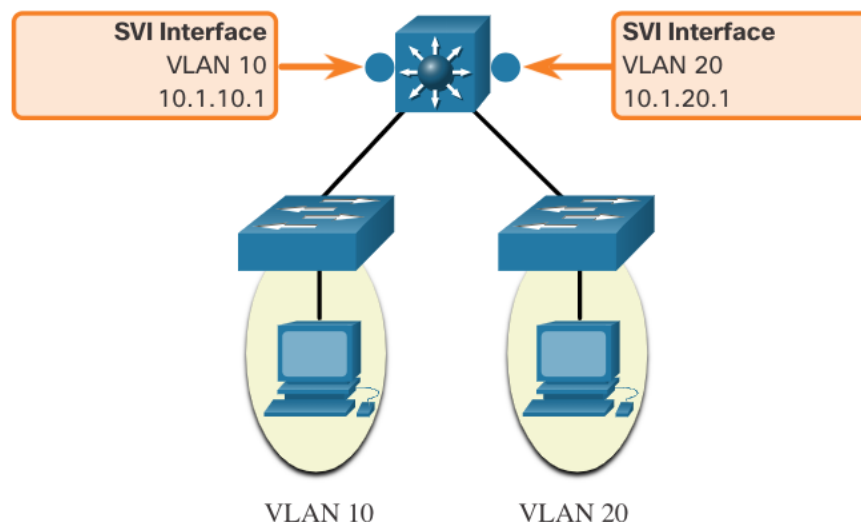
- Интерфейс Ethernet маршрутизатора настроен как транк 802.1Q и подключен к магистральному порту коммутатора уровня 2. В частности, интерфейс маршрутизатора настраивается с использованием подинтерфейсов (subinterfaces) для идентификации маршрутизируемых VLAN.
- Настроенные подинтерфейсы являются программными виртуальными интерфейсами. Каждый из них связан с одним физическим интерфейсом Ethernet. Каждому подинтерфейсу отдельно назначаются IP-адрес и длина префикса. Подынтерфейсы настроены для разных подсетей, которые соответствуют назначенным им VLAN.
- Когда трафик с тегом VLAN входит в интерфейс маршрутизатора, он перенаправляется на подинтерфейс VLAN. После принятия решения о маршрутизации на основе IP-адреса назначения маршрутизатор определяет интерфейс выхода для трафика.
- **Примечание.** Маршрутизация между VLAN с использованием метода router-on-a-stick может иметь проблемы с масштабируемостью

# Маршрутизация между VLAN на коммутаторе уровня

### 3

Современный способ выполнения маршрутизации между VLAN заключается в использовании коммутаторов уровня 3 и коммутируемых виртуальных интерфейсов (Switched Virtual Interface, SVI). Как показано на рисунке, SVI — это виртуальный интерфейс, настраиваемый в многоуровневом коммутаторе.

**Примечание.** Коммутатор уровня 3 также называется многоуровневым (multilayer) коммутатором, поскольку он работает на уровнях 2 и 3



# Маршрутизация между VLAN на коммутаторе уровня

## 3

Ниже приведены преимущества использования коммутаторов уровня 3 для маршрутизации между VLAN:

- Это более быстрая маршрутизация, чем конфигурация router-on-stick, поскольку и коммутация, и маршрутизация выполняются аппаратно
- Для маршрутизации не требуются внешние каналы от коммутатора к маршрутизатору
- Не ограничиваются одним портом, поскольку в качестве магистральных каналов между коммутаторами можно использовать **EtherChannels** уровня 2 для увеличения пропускной способности.
- Задержка меньше, поскольку для маршрутизации в другую сеть данным не нужно покидать коммутатор.
- Единственным недостатком является то, что коммутаторы уровня 3 дороже.

# Вопросы?



Ставим “+”,  
если вопросы есть



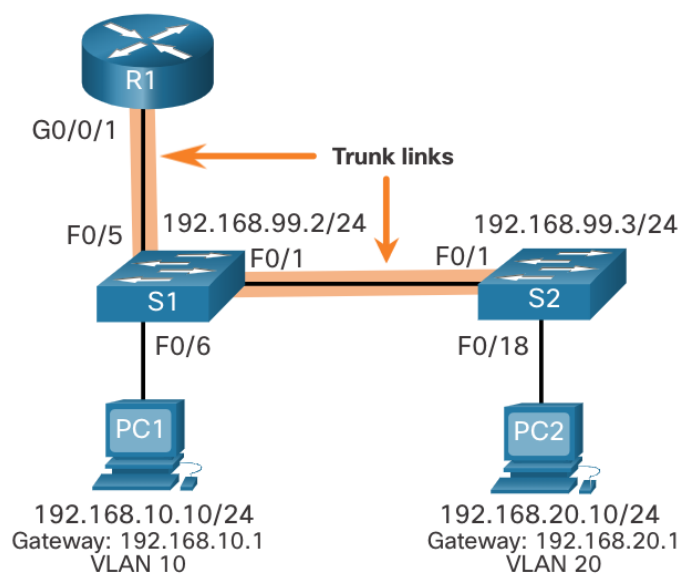
Ставим “-”,  
если вопросов нет

# Маршрутизация между VLAN с помощью Router-on-a-Stick

# Маршрутизация между сетями VLAN с помощью метода Router-on-a-Stick

## Маршрутизация между VLAN с помощью Router-on-a-Stick - Сценарий

- На рисунке интерфейс R1 GigabitEthernet 0/0/1 подключен к порту S1 FastEthernet 0/5. Порт S1 FastEthernet 0/1 подключен к порту S2 FastEthernet 0/1. Это транки, которые необходимы для пересылки трафика внутри VLAN и между ними.
- Для маршрутизации между VLAN интерфейс R1 GigabitEthernet 0/0/1 логически разделен на три подинтерфейса, как показано в таблице. В таблице также показаны три VLAN, которые будут настроены на коммутаторах.
- Предположим, что R1, S1 и S2 имеют начальные базовые конфигурации. В настоящее время PC1 и PC2 не могут обмениваться данными друг с другом, поскольку они находятся в разных сетях. Только S1 и S2 могут пинговать друг друга, но они недоступны PC1 или PC2, потому что они также находятся в разных сетях.
- Чтобы устройства могли выполнить эхо-запрос друг к другу, коммутаторы должны быть настроены для работы с VLAN и транками, а маршрутизатор должен быть настроен для маршрутизации между VLAN.



Подинтерфейс	VLAN	IP-адрес
G0/0/1.10	10	192.168.10.1/24
G0/0/1.20	20	192.168.20.1/24
G0/0/1.30	99	192.168.99.1/24



# Маршрутизация между сетями VLAN с помощью метода Router-on-a-Stick

## Настройка на R1 подинтерфейсов

Для использования метода Router-on-a-Stick требуется настроить подинтерфейсы для каждой маршрутизируемой сети VLAN. Подинтерфейс создается с помощью команды режима глобальной конфигурации

```
interface interface_id subinterface_id
```

Синтаксис для подинтерфейсов следующий:

сначала указывается физический интерфейс, в данном случае g0/0, затем точка и номер подинтерфейса. Хотя это не требуется, обычно сопоставляют номер подинтерфейса с номером VLAN.

Затем каждый подинтерфейс настраивается с помощью следующих двух команд:

- **encapsulation dot1q *vlanid* [native]** - Эта команда настраивает подинтерфейс для ответа на инкапсулированный трафик 802.1Q из указанного идентификатора *vlan-id* . Параметр **native** ключевого слова добавляется только для установки собственной VLAN на что-то отличное от VLAN 1.
- **ip address *ip-address subnet-mask*** - Эта команда настраивает IPv4-адрес подинтерфейса. Этот адрес обычно служит шлюзом по умолчанию для идентифицированных VLAN.
- **no shutdown** для включения интерфейса. Если отключить физический интерфейс, то все подчиненные интерфейсы также отключаются.

# Маршрутизация между сетями VLAN с помощью метода Router-on-a-Stick

## Настройка на R1 подинтерфейсов

В конфигурации подинтерфейсы R1 G0/0/1 настроены для VLAN 10, 20 и 99.

```
R1(config)# interface G0/0/1.10
R1(config-subif)# Description Default Gateway for VLAN 10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip add 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.20
R1(config-subif)# Description Default Gateway for VLAN 20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip add 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.99
R1(config-subif)# Description Default Gateway for VLAN 99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# ip add 192.168.99.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1
R1(config-if)# Description Trunk link to S1
R1(config-if)# no shut
R1(config-if)# end
R1#
*Sep 15 19:08:47.015: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Sep 15 19:08:50.071: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Sep 15 19:08:51.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
R1#
```

# Маршрутизация между сетями VLAN с помощью метода Router-on-a-Stick

## Проверка подключения между PC1 и PC2

Конфигурация «маршрутизатора на палочке» завершается после настройки магистральной коммутатора и подинтерфейсов маршрутизатора. Конфигурацию можно проверить на хостах, маршрутизаторе и коммутаторе.

С узла проверьте подключение к узлу в другой VLAN с помощью команды **ping**. Лучше сначала проверить текущую конфигурацию IP хоста с помощью команды **ipconfig** для Windows.

Затем используйте команду **ping** для проверки соединения с PC2 и S1, как показано на рисунке. Выходные данные **ping** успешно подтверждают работу маршрутизации между VLAN.

```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
C:\Users\PC1> ping 192.168.99.2
Pinging 192.168.99.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.99.2: bytes=32 time=2ms TTL=254
Reply from 192.168.99.2: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.99.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC1>
```

# Маршрутизация между сетями VLAN с помощью метода Router-on-a-Stick

## Проверка маршрутизации между сетями VLAN с использованием метода Router-on-a-Stick

Помимо использования команды **ping** между устройствами, следующие команды **show** могут использоваться для проверки и устранения неполадок конфигурации маршрутизатора на палке.

- **show ip route**
- **show ip interface brief**
- **show interfaces**
- **show interfaces trunk**

# Вопросы?



Ставим “+”,  
если вопросы есть



Ставим “-”,  
если вопросов нет

# Маршрутизация между VLAN с помощью с помощью устройств коммутации уровня 3

# Маршрутизация между VLAN с использованием коммутаторов уровня 3

## Коммутаторы уровня 3

## Маршрутизация между VLAN

Возможности коммутатора уровня 3 по маршрутизации между VLAN:

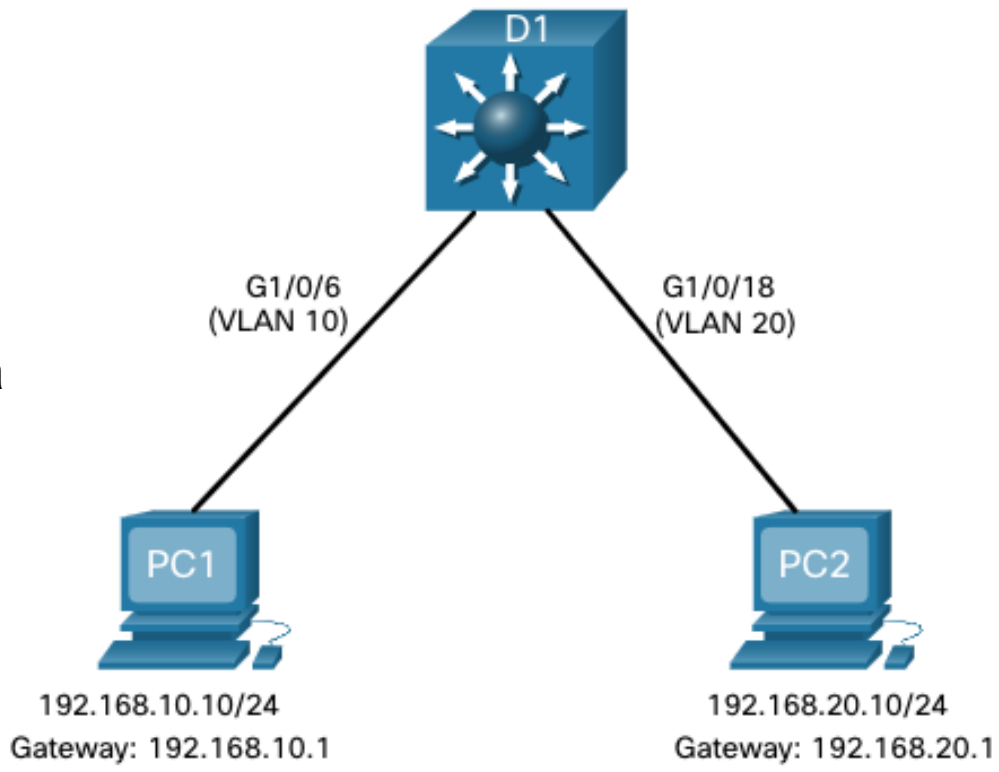
- с использованием нескольких коммутируемых виртуальных интерфейсов (SVI).
- с использованием интерфейса уровня 3 (т.е. маршрутизирующий порт) после конвертации из интерфейса уровня 2 (no switchport)

# Маршрутизация между VLAN с использованием коммутаторов уровня 3

## Сценарий использования коммутатора уровня 3

На рисунке коммутатор уровня 3 D1 подключен к двум узлам в разных VLAN. PC1 находится в VLAN 10, а PC2 — в VLAN 20.

Коммутатор уровня 3 будет предоставлять услуги маршрутизации между VLAN на обоих хостах.



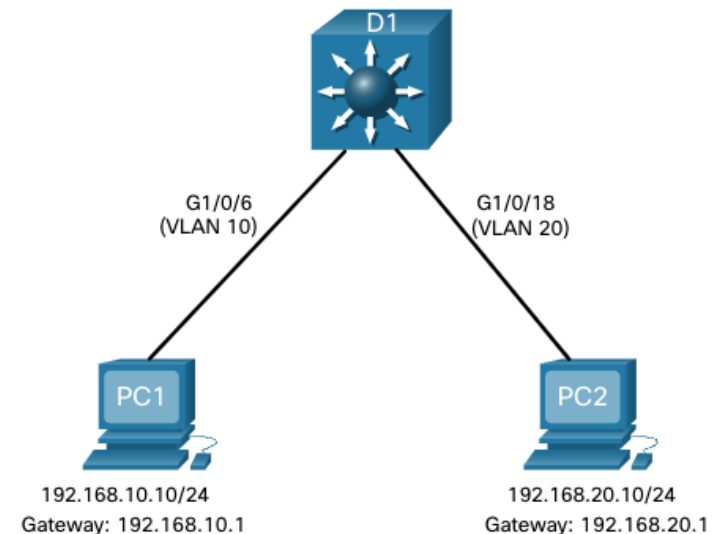


# Маршрутизация между VLAN с использованием коммутаторов уровня 3

## Настройка использования коммутатора уровня 3

Выполните следующие шаги для настройки S1 с VLAN и транкингом:

- **Шаг 1.** Создайте сети VLAN. В этом примере используются VLAN 10 и 20.
- **Шаг 2.** Создание интерфейсов VLAN SVI. Настроенный IP-адрес будет служить шлюзом по умолчанию для узлов в соответствующей VLAN.
- **Шаг 3.** Настройка портов доступа Назначьте соответствующий порт требуемой VLAN.
- **Шаг 4.** Активация IP-маршрутизации. Выполните команду глобальной конфигурации **ip routing**, чтобы разрешить обмен трафиком между VLAN 10 и 20. Эта команда должна быть настроена для включения маршрутизации между VLAN на коммутаторе уровня 3 для протокола IPv4. Маршрутизация между VLAN с помощью коммутатора уровня 3 проще в настройке, чем метод RoS.



# Маршрутизация между VLAN с использованием коммутаторов уровня 3

## Маршрутизация на коммутаторе уровня 3

Если VLAN должны быть доступны другим устройствам уровня 3, то они должны быть объявлены с помощью статической или динамической маршрутизации. Чтобы включить маршрутизацию на коммутаторе уровня 3, можно настроить маршрутизируемый порт.

Маршрутизированный порт создается на коммутаторе уровня 3 путем отключения функции порта коммутатора на порту уровня 2, подключенном к другому устройству уровня 3.

В частности, настройка команды **no switchport** для порта уровня 2 преобразует его в интерфейс уровня 3.

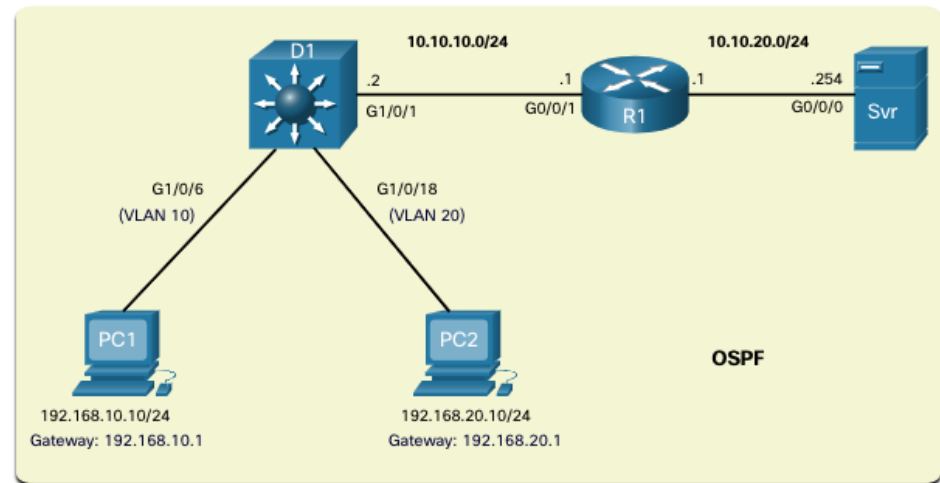
Затем интерфейс может быть настроен с конфигурацией IPv4 для подключения к маршрутизатору или другому коммутатору уровня 3.

# Маршрутизация между VLAN с использованием коммутаторов уровня 3

## Маршрутизация на коммутаторе уровня 3 - сценарий маршрутизации

На рисунке ранее настроенный коммутатор D1 уровня 3 теперь подключен к R1. R1 и D1 находятся в домене протокола маршрутизации OSPF.

Предположим, что маршрутизация между VLAN успешно реализована на D1. Интерфейс G0/0/1 R1 также был настроен и включен. Кроме того, R1 использует OSPF для объявления своих двух сетей: 10.10.10.0/24 и 10.20.0/24.



# Вопросы?



Ставим “+”,  
если вопросы есть



Ставим “-”,  
если вопросов нет

# Коммутация между VLAN

## Переназначение VLAN

Оборудование разных вендоров позволяет **переназначать** VLAN, таким образом делая возможным связь двух VLAN на уровне L2.

Например:

- Juniper – VLAN rewrite
- Cisco – VLAN remapping

Другой подход – «magic loop»: порт коммутатора, который настроен как access в VLAN **N**, подключается кабелем к другому порту этого же или другого коммутатора, который настроен как access в VLAN **M**.

Таким образом, фреймы в VLAN **N** попадают в VLAN **M** и наоборот.

Такие подходы применять **не рекомендуется**.

# Вопросы?



Ставим “+”,  
если вопросы есть



Ставим “-”,  
если вопросов нет

Заполните, пожалуйста,  
опрос о занятии

**Спасибо за внимание!**