

# Полное руководство по настройке VLAN

Создание VLAN-ов, как и все другие конфигурации на сетевом оборудовании, достигается путем ввода соответствующих команд. В этой статье рассматриваются настройка разных типов VLAN на коммутаторах Cisco.



## ПОЛНОЕ РУКОВОДСТВО ПО НАСТРОЙКЕ VLAN

CISCO

MERION NETWORKS

### Диапазоны VLAN на коммутаторах Catalyst

В зависимости от модели, коммутаторы Cisco поддерживает разное число VLAN. Числа поддерживаемых VLAN обычно вполне достаточно для задач большинства компаний. Например, коммутаторы Cisco Catalyst 2960 и 3650 поддерживают больше 4000 виртуальных сетей. Нормальный диапазон VLAN начинается от 1 до 1005, а расширенный – от 1006 до 4094. На выводе внизу можно увидеть VLAN по умолчанию на коммутаторе Cisco Catalyst 2960 с Cisco IOS 15 версии.

```
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

### Нормальный диапазон VLAN

Ниже перечислены основные характеристики нормального диапазона:

- Они используются в малых, средних и больших сетях;
- Нумерация начинается от 1 до 1005;
- Идентификаторы с 1002 до 1005 зарезервированы для устаревших сетей (Token Ring, FDDI);
- Идентификаторы с 1002 до 1005 созданы автоматически и не могут быть удалены;
- Созданные VLAN хранятся в памяти коммутатора в файле базы данных VLAN, именуемого vlan.dat;
- VTP, если настроен, помогает распространять все VLAN между коммутаторами.

### Расширенный диапазон

Ниже перечислены основные характеристики расширенного VLAN:

- Используется провайдерами и очень большими компаниями;
- Нумерация начинается с 1006 по 4094;
- По умолчанию, они хранятся в running-config;
- Имеют меньшую функциональность, чем нормальные VLAN;
- Для настройки расширенного VLAN VTP должен работать в режиме transparent.

*Примечание: Ограничение количества доступных VLAN продиктовано особенностями заголовка 802.1Q. Полю VLAN ID заголовка 802.1Q IEEE выделено всего 12 бит, поэтому 4096 -- верхняя граница доступных VLAN на коммутаторах Catalyst. А если нужно больше, то можно обратиться к такой технологии как VXLAN.*

## Команды для создания VLAN

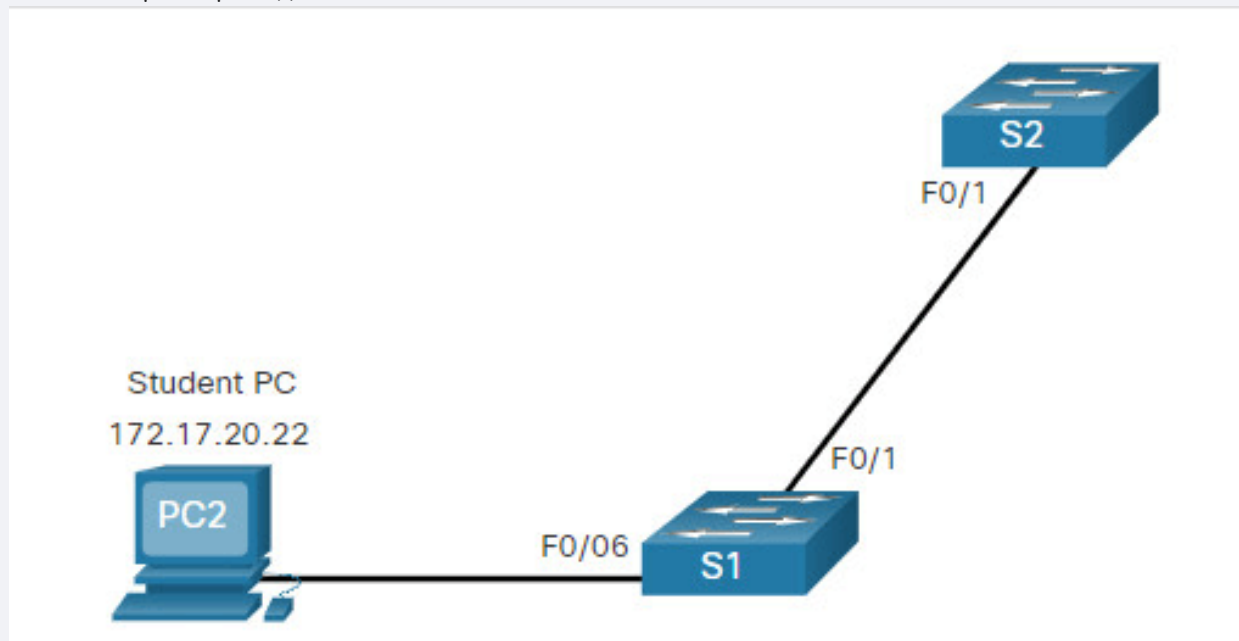
Когда создается VLAN нормального диапазона, как уже было отмечено, эти настройки хранятся в файле `vlan.dat`, то есть не нужно вводить команды `copy running-config startup-config` или `write memory`. Тем не менее, чтобы не потерять изменения сделанные наряду с созданием VLAN, рекомендуется сохранять текущую конфигурацию.

В таблице ниже перечислены команды, которые нужно вводит для создания VLAN и присвоения им названия. Хорошей практикой считается давать VLAN понятные названия, чтобы облегчить поиск и устранение проблем в будущем.

Задача	IOS команда
Войти в режим глобальной конфигурации	Switch# configure terminal
Создать VLAN с валидным ID	Switch(config)# vlan vlan-id
Указать уникальное имя для идентификации VLAN	Switch(config-vlan)# name vlan-name
Вернуться в привилегированный режим EXEC	Switch(config-vlan)# end

## Пример создания VLAN

В топологии ниже, порт к которому подключен ПК Student, еще не добавлен ни в один VLAN, но у него есть IP 172.17.20.22, который принадлежит VLAN 20.



Пример ниже демонстрирует настройку VLAN 20 с названием student на коммутаторе S1.

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

Примечание: Кроме создание VLAN-ов по одному, так же есть возможность создания нескольких влан, вводя их идентификаторы через запятые или дефис. Например, команда `vlan 100,102,105-107` в режиме конфигурации создаст сразу 5 VLAN-ов с идентификаторами 100, 102, 105, 106, и 107

## Добавление портов в VLAN

После создания VLAN, следующий шаг – это добавление нужных портов в конкретный VLAN.

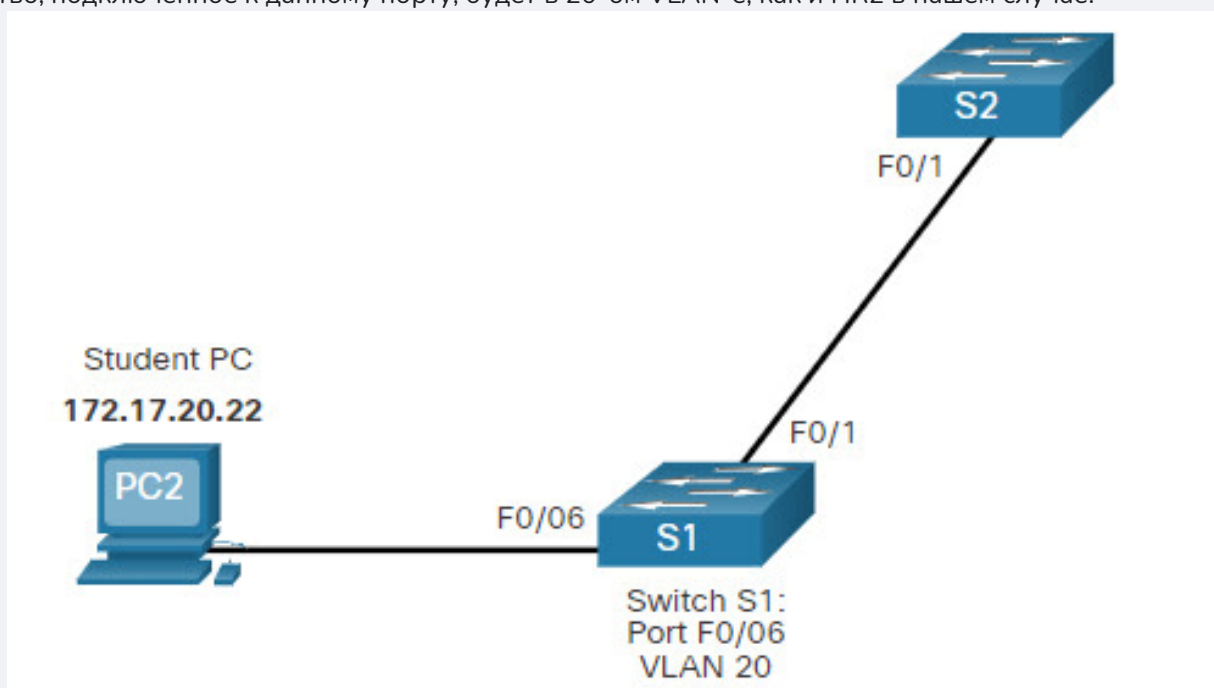
В таблице ниже приведены команды для перевода порта в режим **access** и добавления в конкретный VLAN. Команда `switchport mode access` опциональна, но в целях безопасности рекомендуется вводить ее, так как она принудительно переводит порт в режим **access**, что помогает защищаться от атак вроде VLAN Hopping.

Задача	IOS команда
Войти в режим глобальной конфигурации	Switch# configure terminal
Войти в режим конфигурации интерфейса	Switch(config)# interface interface-id
Установить порт в режим access	Switch(config-if)# switchport mode access
Присвоить порт VLAN'у.	Switch(config-if)# switchport access vlan vlan-id
Вернуться в привилегированный режим EXEC	Switch(config-if)# end

Примечание: Для одновременной конфигурации нескольких портов можно воспользоваться командой **interface range**.

#### Пример присвоения порту VLAN

В топологии ниже порт F0/6 коммутатора S1 настроен в режиме access и добавлен в VLAN 20. Теперь любое устройство, подключенное к данному порту, будет в 20-ом VLAN-е, как и ПК2 в нашем случае.



А ниже приведен пример команд для реализации вышеуказанной цели.

```

S1# configure terminal
S1(config)# interface fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
  
```

VLAN настраивается на порту коммутатора, а не на конечном устройстве. ПК2 присвоен IP адреси маска подсети, которая относится к VLAN 20, а последний указан на порту коммутатора. Если VLAN 20 настроить на другом коммутаторе, администратор сети должен настроить другой компьютер так, чтобы он был в одной подсети с ПК2 (172.17.20.0/24).

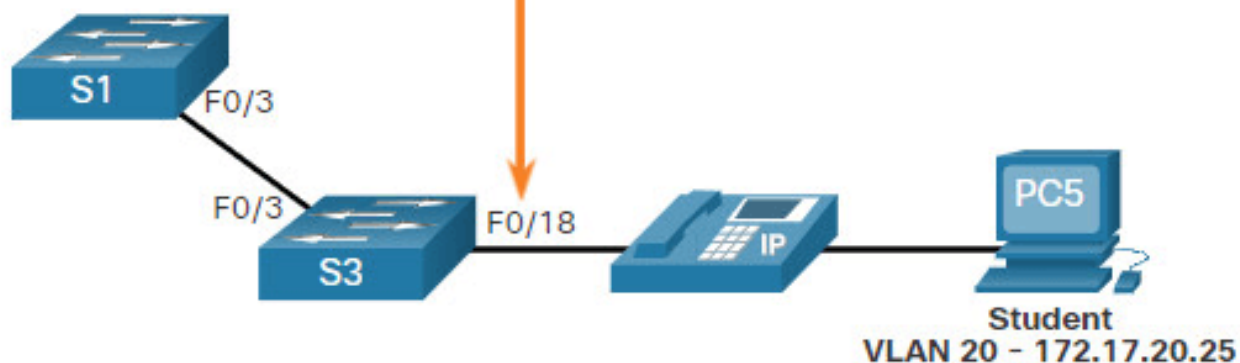
#### VLAN данных и голосовой VLAN

На порту коммутатора в режиме access можно настроить не более одного VLAN-а данных. Тем не менее, на том же порту можно настроить голосовой VLAN. Например, порт к которому подключены IP телефон и конечное устройство, может быть сразу в двух VLAN-ах, - голосовом и VLAN-е данных.

Например, в топологии ниже, ПК5 подключен к IP телефону, который в свою очередь подключен к порту F0/18 коммутатора S3. Для реализации данной идеи созданы VLAN данных и голосовой VLAN.

Switchport must support VLAN traffic for:

- Voice traffic to the IP phone
- Data traffic to PC5



Пример голосового VLAN и VLAN данных

Чтобы настроить на интерфейсе голосовой VLAN используется команда `switchport voice vlan [vlan-id]` в режиме конфигурации порта на коммутаторе.

В сетях, где поддерживается голосовой трафик, обычно настраиваются различные QoS. Голосовой трафик должен быть маркирован доверенным, как только попадет на интерфейс. Чтобы пометить голосовой трафик как доверенный, а так же указать какое поле пакета используется для классификации трафика, применяется команда `mls qos trust [cos | device cisco-phone | dscp | ip-precedence]` в режиме конфигурации интерфейса.

Конфигурация в примере ниже создаст два VLAN-а и присвоит порту F0/18 коммутатора S3 VLAN данных с идентификатором 20, а также голосовой VLAN 150 и включит QoS, на основе CoS.

```
S3(config)# vlan 20
S3(config-vlan)# name student
S3(config-vlan)# vlan 150
S3(config-vlan)# name VOICE
S3(config-vlan)# exit
S3(config)# interface fa0/18
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
S3(config-if)# end
```

Если на коммутаторе еще не создан нужный VLAN команда `switchport access vlan` принудительно создаст его. Например, VLAN 30 не выводится при вводе команды `switchport vlan brief`. Но если ввести команду `switchport access vlan 30` без предварительного создания под любым интерфейсом на терминале выведется соответствующее сообщение:

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

Проверка настроек VLAN

После настроек VLAN, правильность конфигурации можно проверить с помощью команды `show` с последующим ключевым словом.

Команда `show vlan` выводит список существующих VLAN. Данной команде можно задать разные параметры.

Полный синтаксис команды такой: `show vlan [brief | id vlan-id | name vlan-name | summary]`.

В таблице описываются параметры команды `show vlan`.

Задача	Опция команды
Отображение имени, статуса и портов VLAN по одной VLAN на строку	brief
Отображение информации об определенном номере VLAN ID. Для vlan-id диапазон от 1 до 4094	id vlan-id
Отображение информации об определенном имени VLAN. Vlan-name - это строка ASCII от 1 до 32 символов.	name vlan-name
Отображение сводной информации о VLAN	summary

Команда `show vlan summary` выводит количество настроенных VLAN на коммутаторе:

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

Есть и другие полезные команды вроде `show interfaces interface-id switchport` и `show interfaces vlan vlan-id`. Например, команда `show interfaces fa0/18 switchport` может использоваться для проверки правильно ли присвоен интерфейс F0/18 к голосовому VLAN и VLAN данных.

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
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: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 150
Administrative private-vlan host-association: none
(Output omitted)
```

## Переназначение VLAN на интерфейсе

Есть несколько вариантов переназначения интерфейсу VLAN-а.

Если неправильно сконфигурировали VLAN на интерфейсе, просто введите команду `switchport access vlan vlan-id` подставив нужный VLAN. Например, представим что порт F0/18 добавлен в VLAN по умолчанию VLAN 1. Чтобы поменять на VLAN 20, достаточно ввести `switchport access vlan 20`.

Чтобы вернуть обратно в VLAN по умолчанию в режиме конфигурации интерфейса введите команду `no switchport access vlan`.

На выводе ниже можно убедиться, что 18-ый порт коммутатора находится в VLAN по умолчанию.

```
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
Следует заметить, что 20-ый VLAN все еще активен, несмотря на то, что под ним нет
никакого интерфейса.
```

```
Чтобы убедиться, что на 18-ый порт в VLAN 1, можно воспользоваться командой show
interfaces f0/18 switchport:
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)
```

Удаление VLAN

Для удаления VLAN используется команда `no vlan vlan-id` в глобальном режиме конфигурации. Внимание: Прежде чем удалить VLAN убедитесь, что все интерфейсам с данным VLAN назначен другой. Чтобы удалить весь файл `vlan.dat` введите команду `delete flash:vlan.dat` в привилегированном режиме EXEC. После перезагрузки все настроенные на коммутаторе VLAN удалятся. *Примечание: Чтобы сбросить коммутаторы Catalyst до заводских настроек отсоедините все кабели кроме кабеля питания и консольного кабеля, от коммутатора. Затем введите `erase startup-config` после него `delete vlan.dat`. После перезагрузки коммутатор сбросится до первоначальных настроек.*

Настройка Trunk

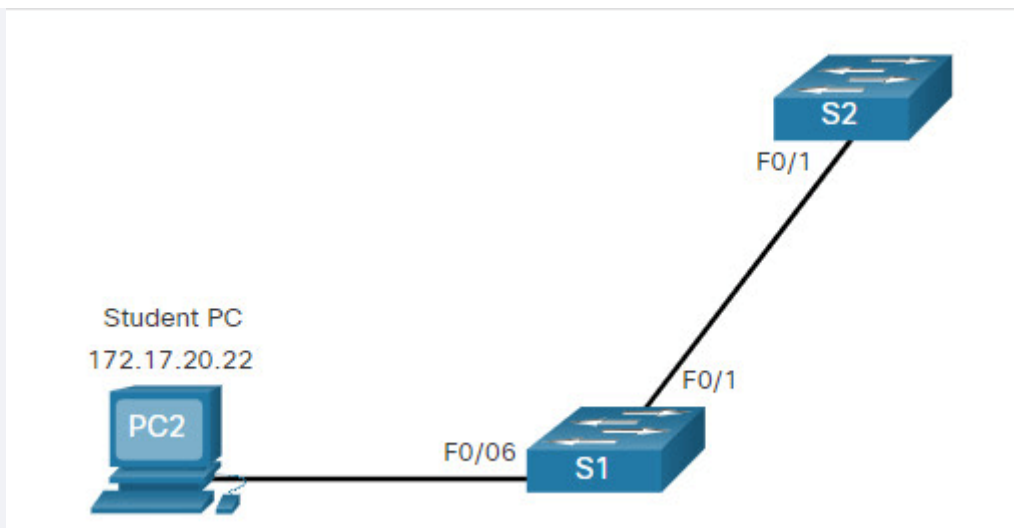
После создания и настройки VLAN, пора перейти к конфигурации **Trunk** портов. Trunk это связь на втором уровне OSI между коммутаторами, который пропускает все VLAN (если список разрешенных VLAN явно не указан). Для настройки интерфейса в режиме Trunk нужно воспользоваться команды, указанные ниже в таблице:

Задача	IOS команда
Войти в режим глобальной конфигурации	Switch# configure terminal
Войти в режим конфигурации интерфейса	Switch(config)# interface interface-id
Установите порт в режим постоянного транкинга	Switch(config-if)# switchport mode trunk
Устанавливает для native VLAN значение, отличное от VLAN 1	Switch(config-if)# switchport trunk native vlan vlan-id
Укажите список VLAN, разрешенных для транка	Switch(config-if)# switchport trunk allowed vlan vlan-list
Вернуться в привилегированный режим EXEC	Switch(config-if)# end

Пример настройки Trunk

В топологии ниже VLAN 10, 20 и 30 обслуживают компьютеры Faculty, Student и Guest. Порт F0/1 коммутатора S1 настроек в режиме Trunk и пропускает VLAN-ы 10, 20, 30. VLAN 99 настроен в качестве native (VLAN по умолчанию).





В данном примере показывается настройка порта в режиме trunk, смена VLAN по умолчанию и ограничение разрешенных VLAN.

```

S1(config) # interface fastEthernet 0/1
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
  
```

Примечание: В данном примере подразумевается, что используется коммутатор Cisco Catalyst 2960, в котором порты по умолчанию используют 802.1Q. На других коммутаторах может понадобится ручная настройка режима энкапсуляции на интерфейсе. Так же следует настроить VLAN по умолчанию на обоих концах, иначе коммутатор будет выдавать ошибки.

#### Проверка настройки Trunk

Вывод ниже демонстрирует настройки интерфейса Fa0/1 коммутатора S1. Данный вывод получен с помощью команды `show interfaces interface-ID 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: 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)
  
```

Подчеркнутые части показывают режим работы интерфейса и нативный VLAN.

#### Сброс trunk до настроек по умолчанию

Для сброса настроек транкового интерфейса используйте команды `no switchport trunk allowed vlan` и `no switchport trunk native vlan`. После сброса настроек данный порт будет пропускать все VLAN-ы и VLAN-ом по умолчанию будет VLAN 1.

```

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
```

Вывод команды `show interfaces f0/1 switchport` показывает, что порт сброшен до настроек по умолчанию:

```
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)
```

В вывод ниже показывает команды, которые используются для смены режима работы интерфейса с **trunk** на **access**.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces fa0/1 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
(output omitted)
```