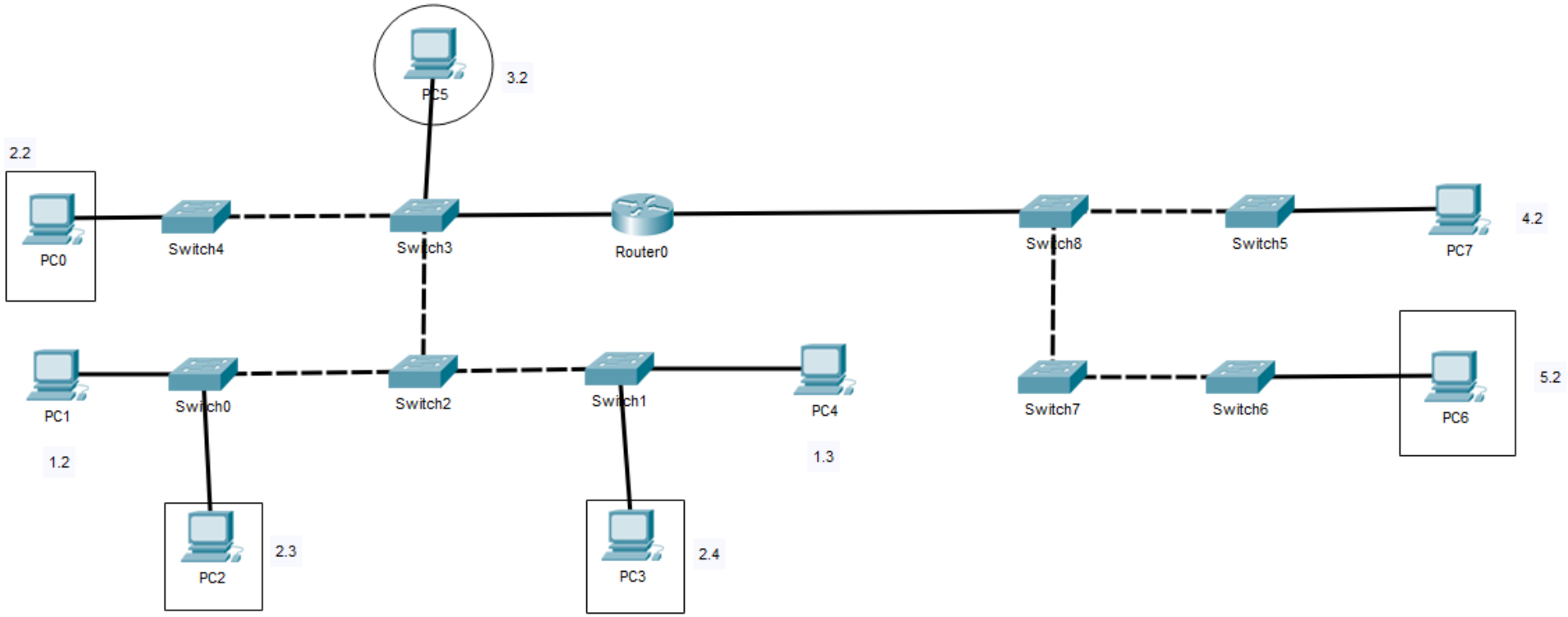
Оглавление

Топология


PC5
3.2
2.2
PC0
Switch4
Switch3
Router0
Switch8
Switch5
PC7
4.2
PC1
Switch0
Switch2
Switch1
PC4
Switch7
Switch6
PC6
5.2
1.2
1.3
PC2
2.3
PC3
2.4

Цели:

Повторить:

1) Понятие VLAN +
2) Понятие trunk, структура кадра 802.1Q +
3) Создание VLANs, конфигурирование access ports +
4) Роль протокола VTP +
5) Конфигурирование trunk +

Для приведенной топологии настроить:

1) 5 VLAN: 3 слева от роутера и 2 справа.
2) При помощи настройки trunk allowed запретить компьютерам во VLAN 1 взаимодействовать с роутером и другими VLAN, как следствие.

Ход работы (повторение):

1. VLAN

Виртуальная локальная сеть (VLAN).

Default/native vlan 1. (не тэгируется).

IEEE 802.1Q – в кадре eth после da и sa появляется поле tag.

Компьютеры самостоятельно не маркируют трафик. Этим занимается коммутатор, пришедший кадр он маркирует согласно правилу switchport access vlan такой-то.

Если кадр идёт с сабинтерфейса роутера, где настроена соответствующая инкапсуляция vlan – кадр уже промаркирован. В нем есть поля TCI и TPID.

С портов доступа (access ports) к конечным устройствам кадры выходят без меток (коммутатор снимает метку перед передачей).

Магистральное соединение – trunk (метки не снимаются).

2. Trunk (c.180)

VLANs также используются для ускорения работы STP.

Можно создавать сети без trunk'ов, только с access-портами, как на рисунке. Тогда для передачи кадров одной VLAN между коммутаторами потребуется отдельное физическое подключение (по одному интерфейсу каждого коммутатора).

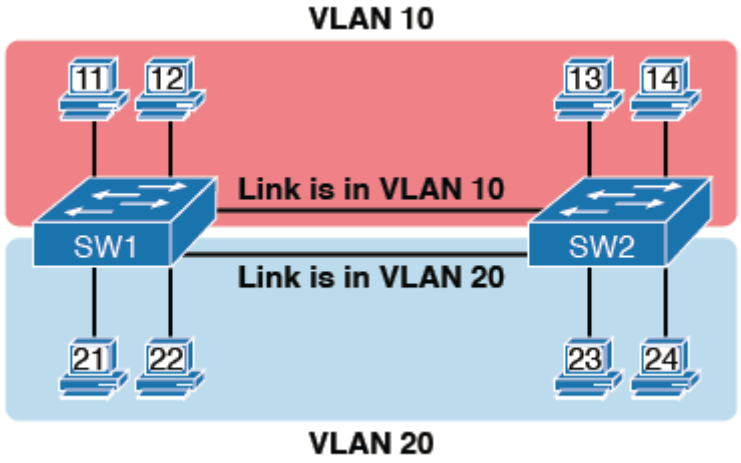
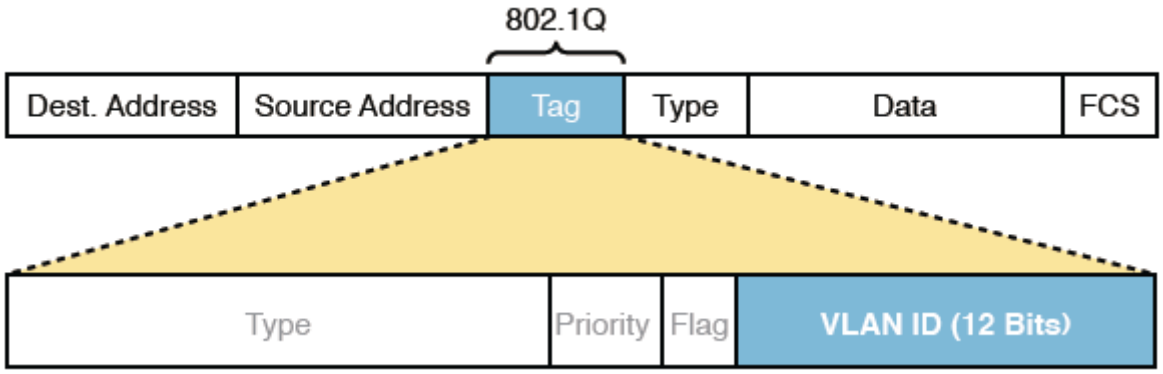
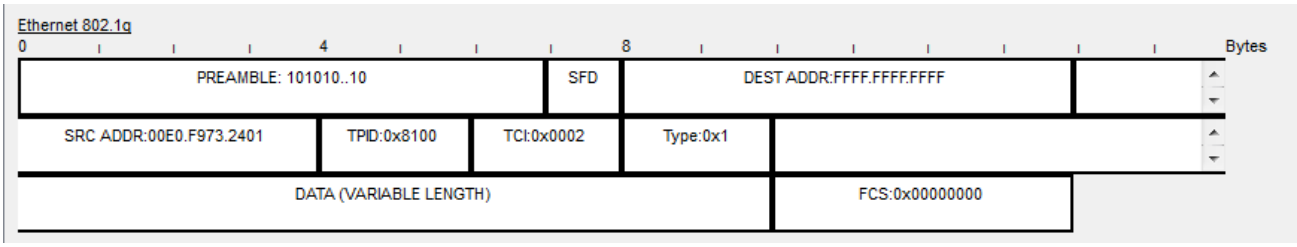


Схема работает, но плохо масштабируется (для 20 VLAN потребуется 20 портов с каждой стороны).

Есть два протокола для реализации trunk (изменяющих обычный Ethernet, добавляя туда метки). Старый протокол от Cisco - ISL (Inter-Switch Link) и более новый 802.1Q, которым пользуется большинство производителей, включая Cisco. Диапазон VLAN в обоих -–1-4094, для меток используется 12 бит с двумя зарезервированными значениями (0 и 4095). Этот диапазон дробится на два: обычный 1-1005 и расширенный 1006-4094, только некоторые коммутаторы могут использовать последний.



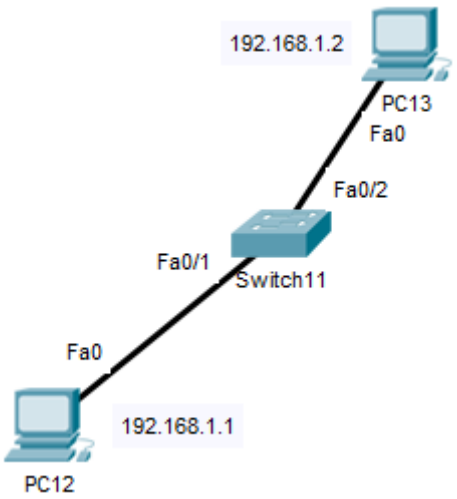


По умолчанию vlan 1 – native vlan. У native vlan есть важная особенность – с его помощью можно передавать пакеты коммутаторы, не поддерживающему 802.1q. Метка 802.1q просто не добавляется к пакетам vlan 1.

В итоге trunk – это одно общее подключение (обычно между коммутаторами, либо между коммутатором и маршрутизатором), по которому передаются тэгированные пакеты разных VLAN.

3. Примеры конфигурирования (с. 185)

Первый пример.



Создание VLAN и конфигурирование портов доступа (access ports). Последовательность действий следующая:

1) В режиме глобальной конфигурации создать VLAN.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name new_vlan
Switch(config-vlan)#exit
```

2) На каждом порте доступа настроить, для какого VLAN будет выставляться/сниматься метка. Также можно настроить режим работы порта – switchport mode access – чтобы данный порт не передавал подключенному устройству пакеты других VLAN с меткой. (Важно: похоже, возможность прописать снятие метки для определенного vlan, при возможности работы порта в режиме trunk, необходимо для администрирования коммутаторов в рамках конкретного VLAN, т.е. коммутатор для определенного VLAN может выступать конечным устройством, для которого нужно снять метку?)

```
Switch(config)#int fa 0/1
Switch(config-if)#switchport access vlan 2
Switch(config-if)#int fa0/2
Switch(config-if)#switchport access vlan 2
```

С interface-range:

```
Switch(config)#int range fa0/3-15
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#end
```

Вывести информацию о принадлежности интерфейсов к VLANs.

```
Switch#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
2    new_vlan                         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
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#!
```

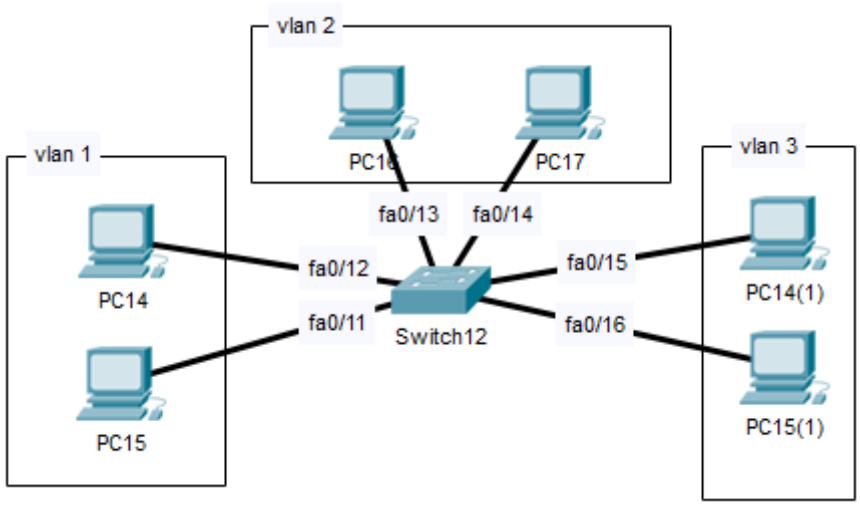
Вывести информацию о конкретном VLAN, его названии и номерах его интерфейсов.

```
Switch#sh vlan id 2

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
2    new_vlan                            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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0
```

Второй пример.



В данном примере используется 6 портов коммутатора, каждый из которых является портом доступа (подключен к конечному устройству). Тэгированные пакеты одного VLAN не должны передаваться коммутатором в другие VLAN. Для этого необходимо использовать команду switchport mode access, упомянутую ранее. Данная команда отключает DTP протокол (Dynamic Trunking Protocol), который используется для установления trunk-соединения.

```
Switch>en
Switch#conf t
Switch(config)#int range fa0/11-12
Switch(config-if-range)#switchport access vlan 1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#int range fa0/13-14
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#int range fa0/15-16
Switch(config-if-range)#switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
```

```
Switch(config)#do sh 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
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    VLAN0002                         active    Fa0/13, Fa0/14
3    VLAN0003                         active    Fa0/15, Fa0/16
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Как итог использования switchport mode access – коммутатор точно не отправит ARP-пакет из, допустим, порта VLAN 1 в порт VLAN 3, на котором без этого внезапно могла оказаться настройка switchport mode trunk, и конечное устройство из VLAN 3 смогло бы перехватить этот пакет.

4. Роль VTP (с. 190)

VTP больше нет в CCNA (в 200/301), есть в CCNP.

Все примеры в Cert. guide используют коммутаторы с отключенным VTP (каким-либо способом, например через vtp mode transparent или vtp mode off).

VTP нужен, чтобы изменения конфигурации (создание новых VLAN или изменение параметров старых) на одном коммутаторе передавать на другие коммутаторы посредством широковещательной рассылки (но только между ними есть trunk-соединение). Инициировать рассылку может только vtp-server.

При помощи команды show vtp status можно узнать роль данного коммутатора в VTP. Если он является клиентом или сервером, то:

- Server может конфигурировать VLAN только внутри стандартного диапазона 1-1005

- Client не может конфигурировать VLAN

- И Server, и Client могут узнавать о новых VLAN от других коммутаторов и удалять имеющиеся у себя VLAN из-за их удаления на других коммутаторах

- sh run не покажет конфигурацию vlan, в данном случае нужно использовать другие команды sh

5. Конфигурирование trunk (с. 191)

switchport mode trunk – создать VLAN trunk, который переправляет пакеты любых VLAN. Помимо этой команды есть множество опций, например:

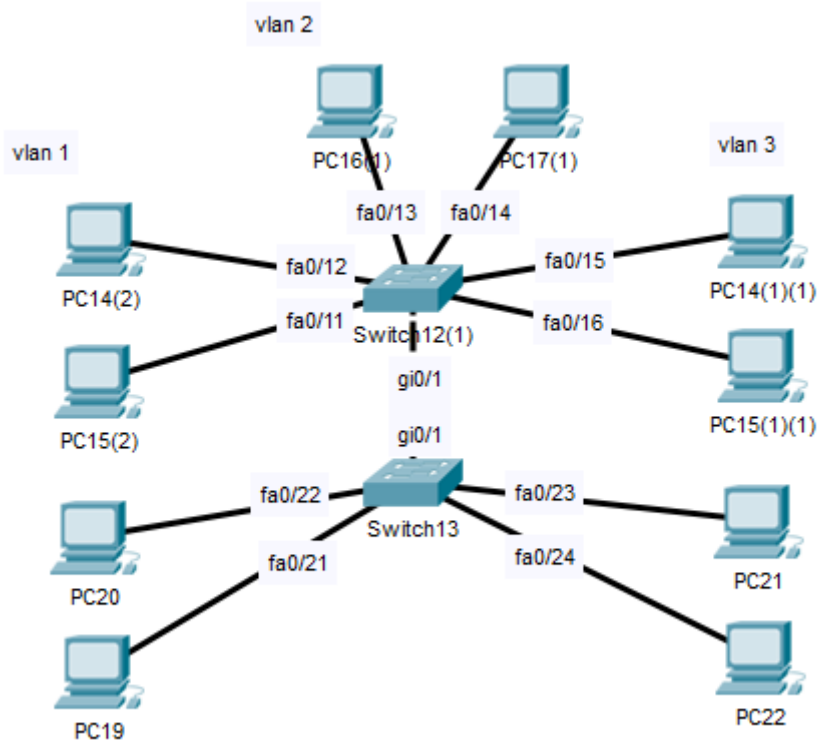
1) можно настроить тип trunking, это может быть IEEE 802.1Q, ISL, либо коммутаторы могут прийти к соглашению, какой именно тип использовать, при помощи DTP;
2) можно включить administrative mode, в котором есть возможность настроить на коммутаторе, всегда ли делать trunk, никогда ли, либо определять совместно с другим коммутатором, создавать trunk или нет.

switchport trunk encapsulation (dot1q | isl | negotiate) – подкоманда интерфейса, определяющая используемый протокол (negotiate – если оба коммутатора поддерживают оба протокола, они используют ISL, иначе используют тот, который есть у обоих). В Cisco Packet Tracer у коммутатора 2960 данная команда отсутствует, но есть похожая роутерная команда:

encapsulation dot1q <vlan> - вводится на сабинтерфейсе и определяет протокол и метку vlan сабинтерфейса.

Административный режим (administrative mode) – позволяет коммутаторам взаимодействовать, чтобы динамически создавать trunk-соединения и выбирать протокол для этого соединения.

Рассмотрим топологию:



Преднастроены vlan 1 на всех компьютерах слева, vlan 2 – сверху, vlan 3 – справа.

На верхнем и нижних коммутаторах включен режим dynamic auto на интерфейсе gi0/1:

```
Switch(config)#int gi0/1
Switch(config-if)#switchport mode dynamic auto
```

```
Switch(config-if)#do sh int gi0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
```

Пакеты vlan 3 не проходят из верхней части в нижнюю, поскольку в dynamic auto режиме оба коммутатора ждут получения DTP от другого коммутатора. Пусть на одном из коммутаторов интерфейс перевели в режим dynamic desirable:

```
Switch(config)#int gi0/1
Switch(config-if)#switchport mode dynamic desirable
```

```
Switch(config-if)#do sh int gi0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
```

В этом случае arp и пинг из верхней части vlan 3 начинает проходить в нижнюю. Оба коммутатора настроили trunk по dot1q, поскольку 2960 поддерживает только dot1q.

```
Switch(config-if)#do sh int gi0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
```

```
Switch(config-if)#do sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,3

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,3
```

Стоит заметить, что если на одном коммутаторе настроен switchport mode trunk, а на другом – switchport mode dynamic auto, trunk-соединение будет создано через обмен DTP-пакетами. В целях безопасности рекомендуется отключать этот обмен командой switchport nonegotiate.

Также рекомендуется не использовать режим access с одной стороны, trunk с другой.

Далее приводится таблица, в которой столбцами и строками являются заданные на коммутаторах режимы, а в ячейках указан тип создаваемого соединения для этой комбинации.

Админ. режим	Access	Dyn. Auto	Trunk	Dyn. Desirable
access	access	access	Do not use	Access
Dyn. auto	access	access	trunk	Trunk
trunk	Do not use	trunk	trunk	Trunk
Dyn. desirable	access	trunk	trunk	trunk

Практика:

Компьютерам настроить IP-адреса, шлюзы. На коммутаторах настроить access-порты. Настроить trunk порты. Отключить vtp (vtp mode transparent). На роутере настроить subinterfaces. Нативному vlan (1) предоставить основной интерфейс, для остальных подинтерфейсы, на каждом подинтерфейсе включить encapsulation dot1q <vlan>. Обязательно настроить trunk между коммутатором и роутером.

Чтобы отрезать vlan 1 от внешнего мира между Switch2 и Switch3 настроить trunk-соединение таким образом, что switchport trunk allowed vlan 2-3.