Реализация виртуальных локальных сетей

Глава 9

В рамках этой темы…

Работа сетей передачи данных IP

Передача данных между двумя хостами по сети.

Технологии коммутации сетей LAN

Базовые концепции коммутации и работа коммутаторов Cisco.

- Широковещательные домены.
- Таблица CAM.

Создание логических сегментов сети VLAN и необходимость маршрутизации между ними.

Принцип сегментации сети и базовые концепции управления трафиком.

Настройка и проверка сети VLAN.

Настройка и проверка магистрального соединения на коммутаторах Cisco.

- Протокол DTP.

Поиск и устранение неисправностей

Поиск неисправностей и решение проблем сетей VLAN.

- Идентификация настроенных сетей VLAN.
- Исправление принадлежности порта.
- Настройка IP-адреса.

Поиск неисправностей и решение проблем магистрального соединения на коммутаторах Cisco.

- Исправление состояния магистрального канала.
- Исправление конфигурации инкапсуляции.
- Исправление разрешенных VLAN.

Концепция VLAN

- Локальная сеть (LAN) объединяет все устройства в том же **широковещательном домене**.

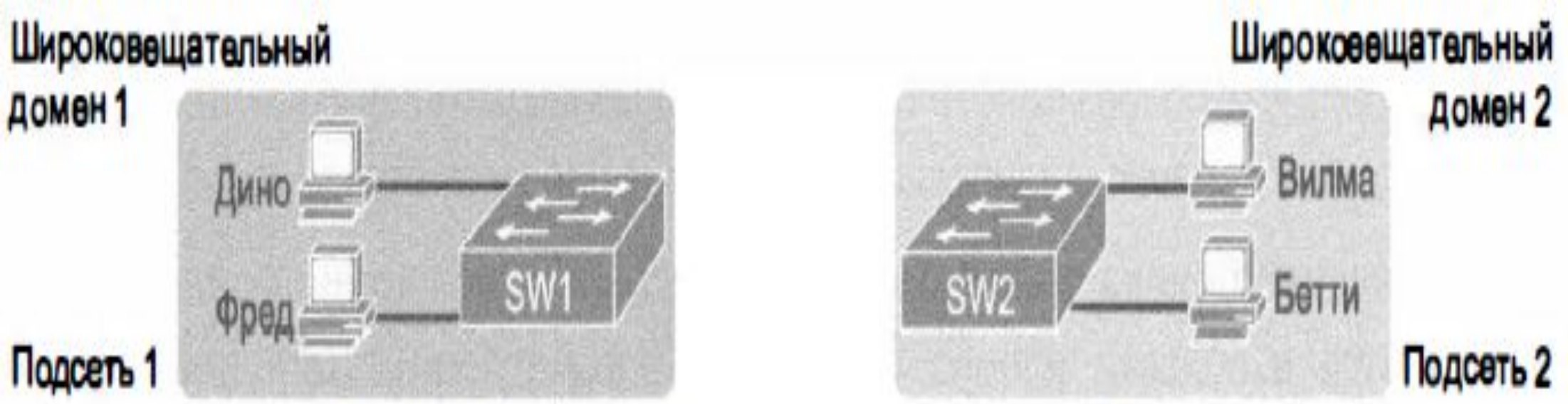

Рис. 9.1. Создание двух широковещательных доменов с двумя физическими коммутаторами и без сетей VLAN

Концепция VLAN

- **Коммутатор VLAN** может настроить часть интерфейсов на один широковещательный домен, а часть на другой , создав в результате два широковещательных домена (2 виртуальные локальные сети (virtual LAN - VLAN)).

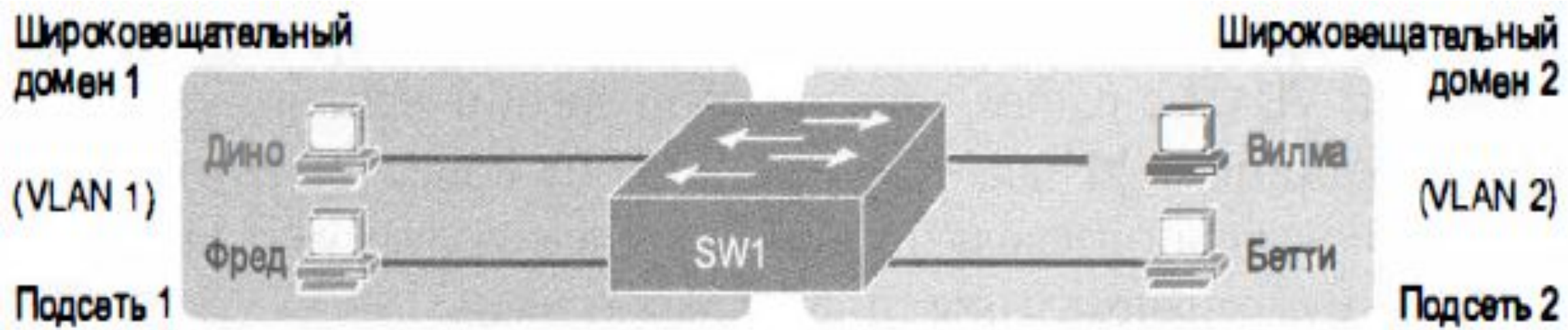

Рис. 9.2. Создание двух широковещательных доменов с использованием одного коммутатора и сети VLAN

Причины применения VLAN

1. **Сокращение дополнительных затрат процессоров** всех устройств за счет сокращения количества устройств, получающих каждый широковещательный фрейм.
2. **Улучшение защиты** за счет сокращения количества хостов, получающих копии фреймов при их лавинной рассылке коммутатором (широковещание, групповая передача и одноадресатные фреймы с неизвестным получателем).
3. **Улучшение защиты хостов**, пересылающих важные данные, за счет их помещения в отдельную сеть VLAN.
4. **Возможность более гибкого объединения** пользователей в группы (например, по отделам) вместо физического разделения по местоположению.
5. **Упрощение поиска проблемы** в сети, поскольку большинство проблем локализуется в области набора устройств, формирующих широковещательный домен.
6. **Сокращение дополнительных** затрат на работу протокола распределенного связующего дерева (STP) за счет ограничения VLAN одним коммутатором доступа.

Магистральное соединение VLAN

- Когда сети VLAN используются в сетях с несколькими соединенными между собой коммутаторами, на каналах связи между ними применяется магистральное соединение **VLAN (VLAN trunking).**

- Магистральное соединение VLAN подразумевает использование коммутаторами процесса **назначения тегов VLAN (VLAN tagging)**:

  ✔ передающий коммутатор добавляет к фрейму дополнительный заголовок перед его передачей по магистральному каналу, включающий **поле идентификатора VLAN (VLAN ID)**, позволяющего передающему и получающему коммутаторам ассоциировать фрейм с конкретной сетью VLAN.

VLAN без магистрального соединения

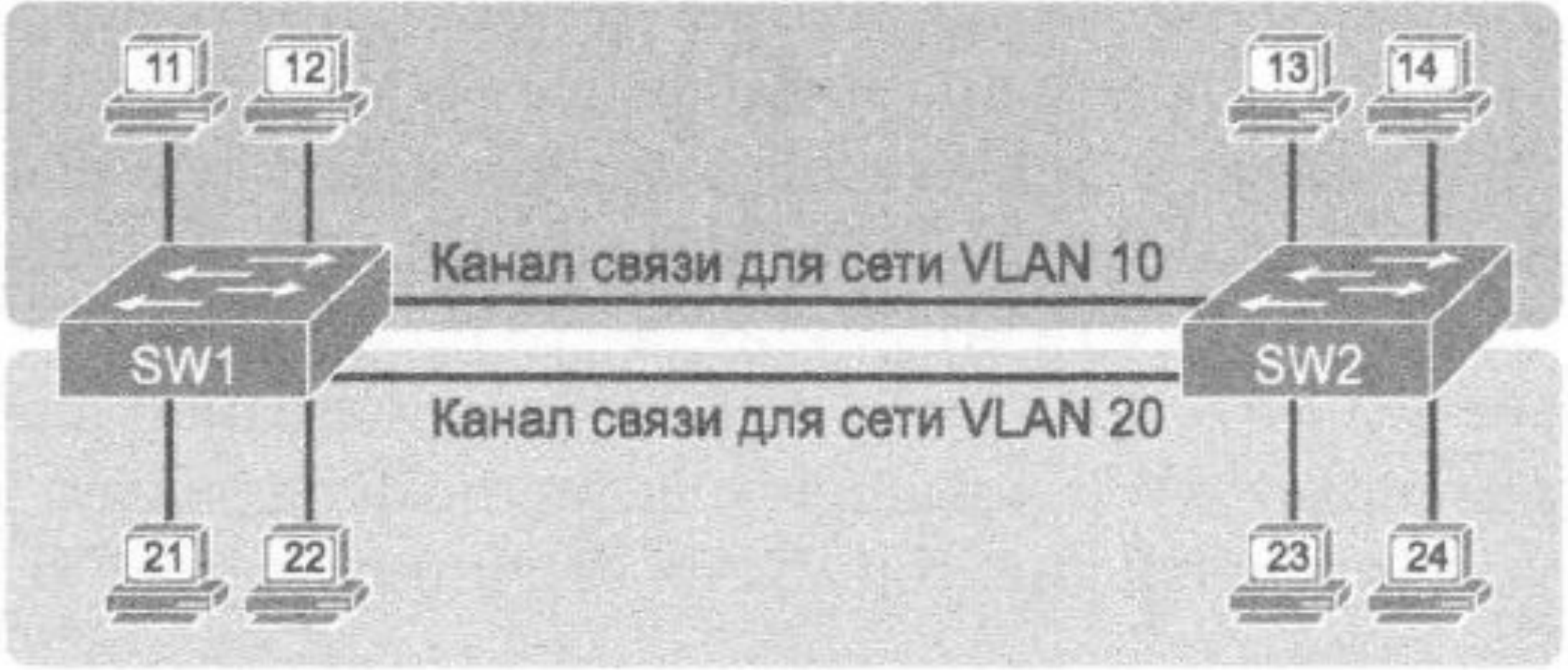

Рис. 9.3. Сети VLAN при наличии нескольких коммутаторов, но без магистрального соединения

Концепция тегов

- **Магистральное соединение VLAN** создает между коммутаторами один канал связи, способный поддерживать столько сетей VLAN, сколько необходимо.

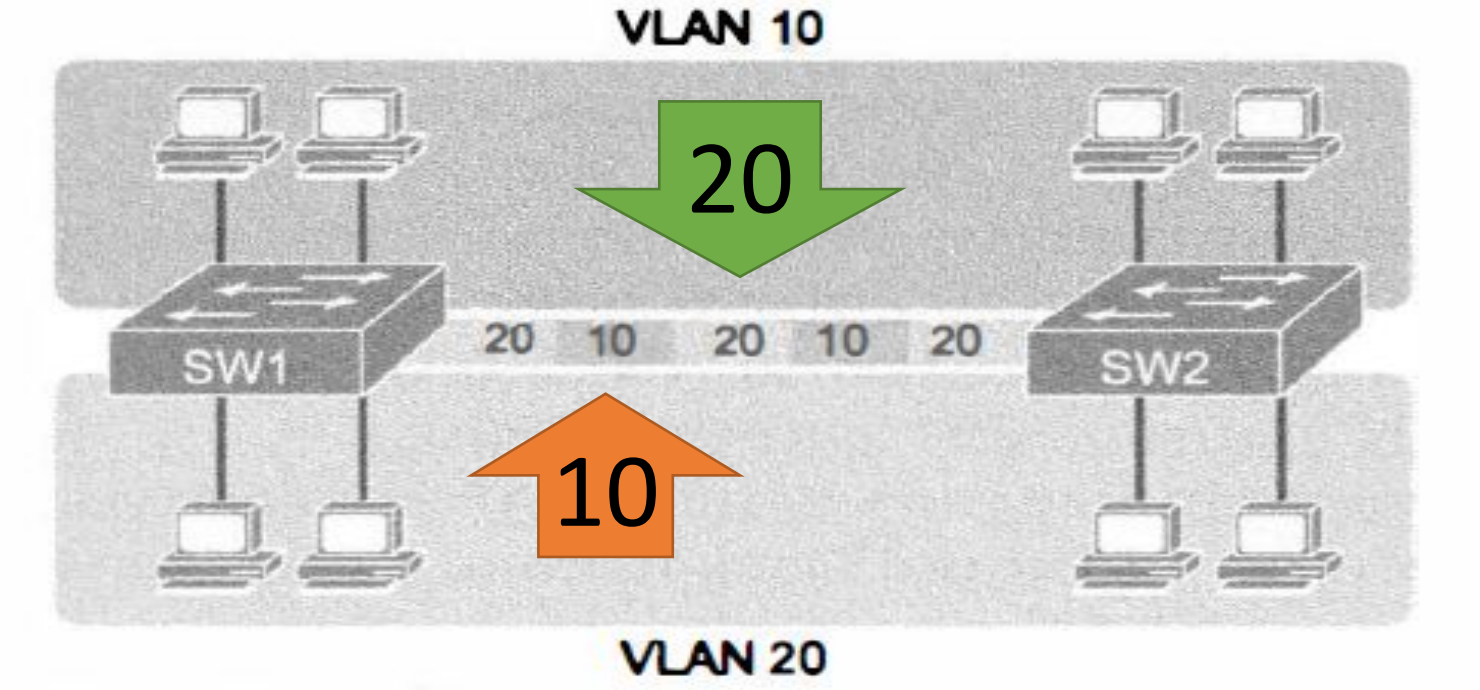

Рис. 9.4. Сети VLAN с несколькими коммутаторами и магистральным соединением

Пересылка фреймов

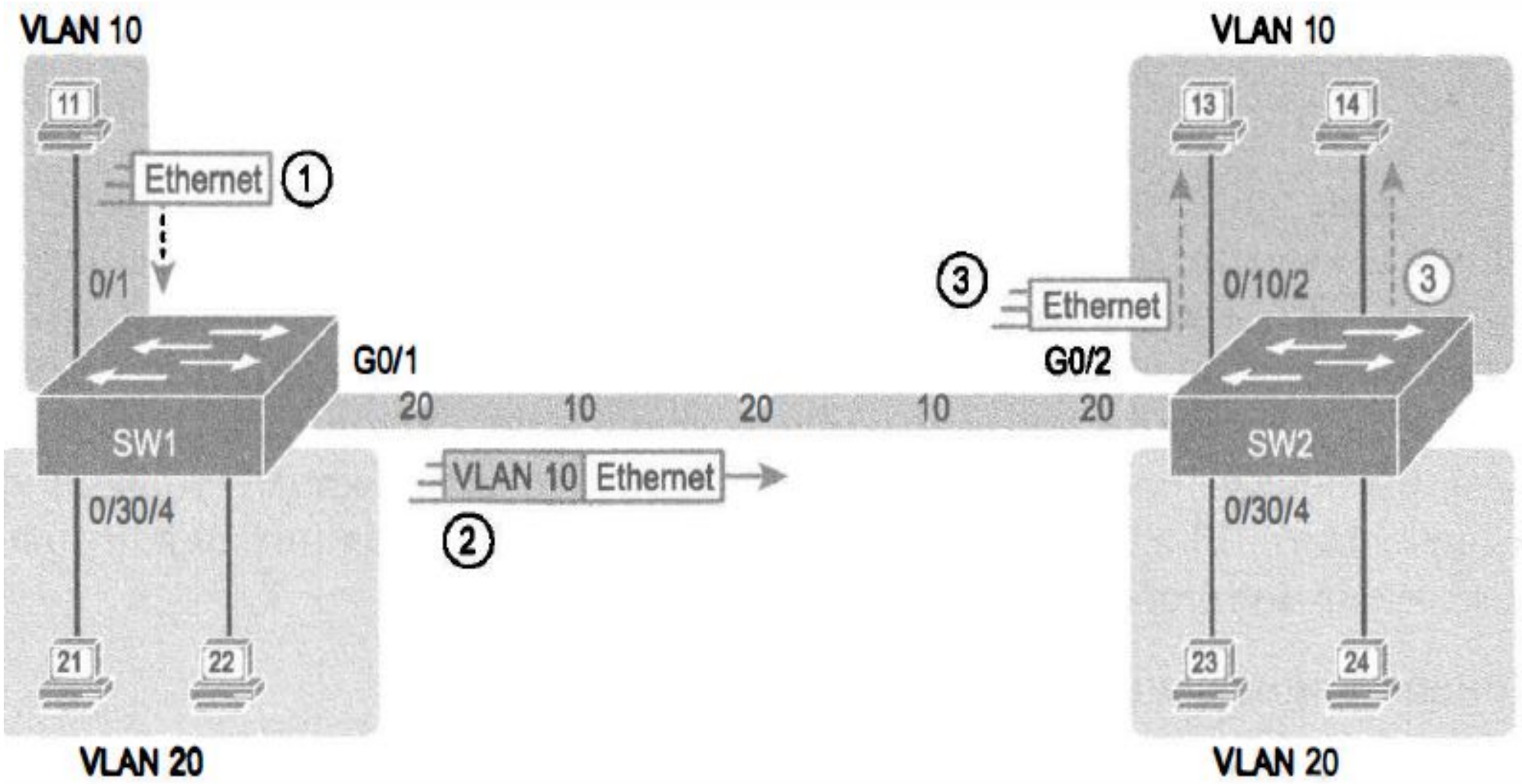

Рис. 9.5. Магистральное соединение VLAN между двумя коммутаторами

Протокол магистралей VLAN 802.1Q

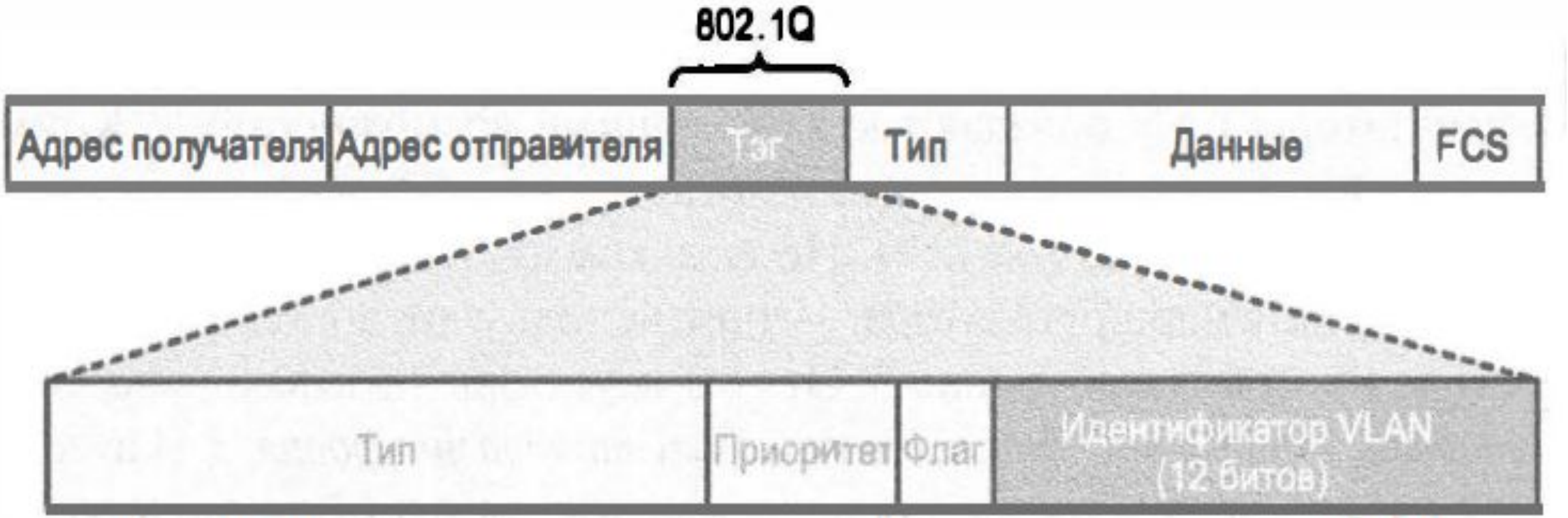

Рис. 9.6. Заголовок магистрального соединения по стандарту 802.1Q

Протокол магистралей VLAN 802.1Q

- Протокол 802.1Q использует дополнительное 4-байтовое поле - **заголовок 802.1Q** в заголовке Ethernet первоначального фрейма

- 12-битовое поле способно идентифицировать **максимум 2^12 (4096) сетей VLAN**, хотя на практике доступно **максимум 4094 значения**. (0 и 4095 - зарезервированы).

- Коммутаторы Cisco **разделяют** диапазон идентификаторов VLAN (1 -4094) на два диапазона: **нормальный** (1-1005) и **расширенный** (1005 - 4094).

- Правила использования коммутаторами расширенного диапазона идентификаторов VLAN зависят от конфигурации **протокола создания магистралей VLAN (VLAN Trunking Protocol - VTP).**

Собственная сеть VLAN

- Для каждого магистрального канала стандарт 802.1Q определяет также один специальный идентификатор VLAN, обозначающий **собственную сеть VLAN (native VLAN):**

1. протокол 802.1Q не добавляет заголовок 802.1Q к фреймам в собственной сети VLAN.

2. когда коммутатор с другой стороны магистрального канала получает фрейм без заголовка 802.1Q, он понимает, что фрейм принадлежит собственной сети VLAN.

3. оба коммутатора должны "договориться", какую сеть VLAN считать собственной.

Коммутаторы уровней

- Коммутаторы LAN, передающие данные на основании логики уровня 2, называют **коммутаторами уровня 2 (Layer 2 switch).**

- Есть коммутаторы, способные выполнять некоторые функции маршрутизатора, - они используют дополнительную логику, определенную протоколами уровня 3. Эти коммутаторы называют **многоуровневыми коммутаторами (multilayer switch), или коммутаторами уровня 3 (Layer 3 switch).**

Маршрутизация между VLAN

- Все устройства сети VLAN находятся **в одной подсети,** а устройства в разных сетях VLAN принадлежат **разным подсетям**.

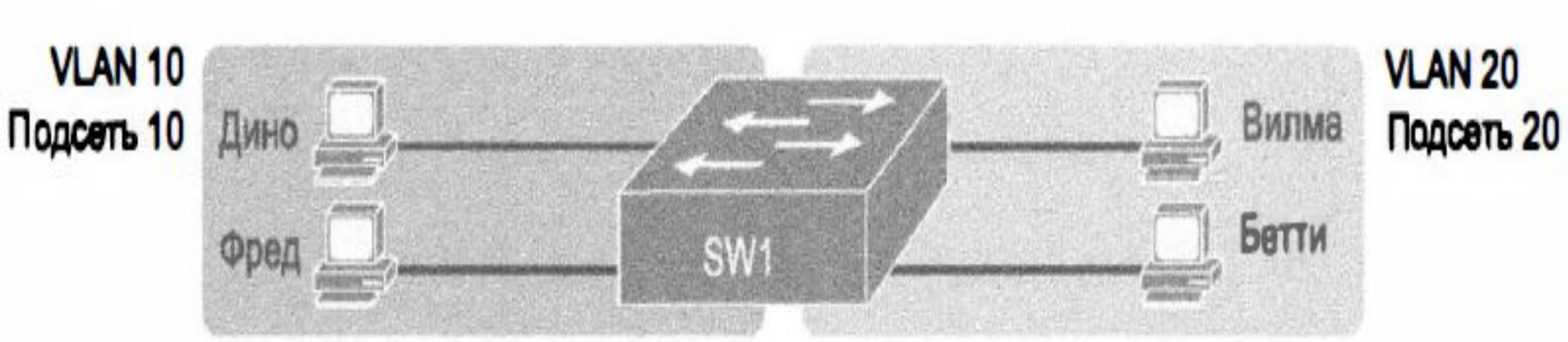

Рис. 9.7. Маршрутизация на коммутаторах между двумя физически отделенными сетями VLAN

Маршрутизация между VLAN

- **Логика уровня 2** не позволяет коммутатору уровня 2 перенаправлять фреймы Ethernet уровня 2 (L2PDU) между сетями VLAN. Однако **маршрутизаторы** могут перенаправить пакеты уровня 3 (L3PDU) между подсетями.

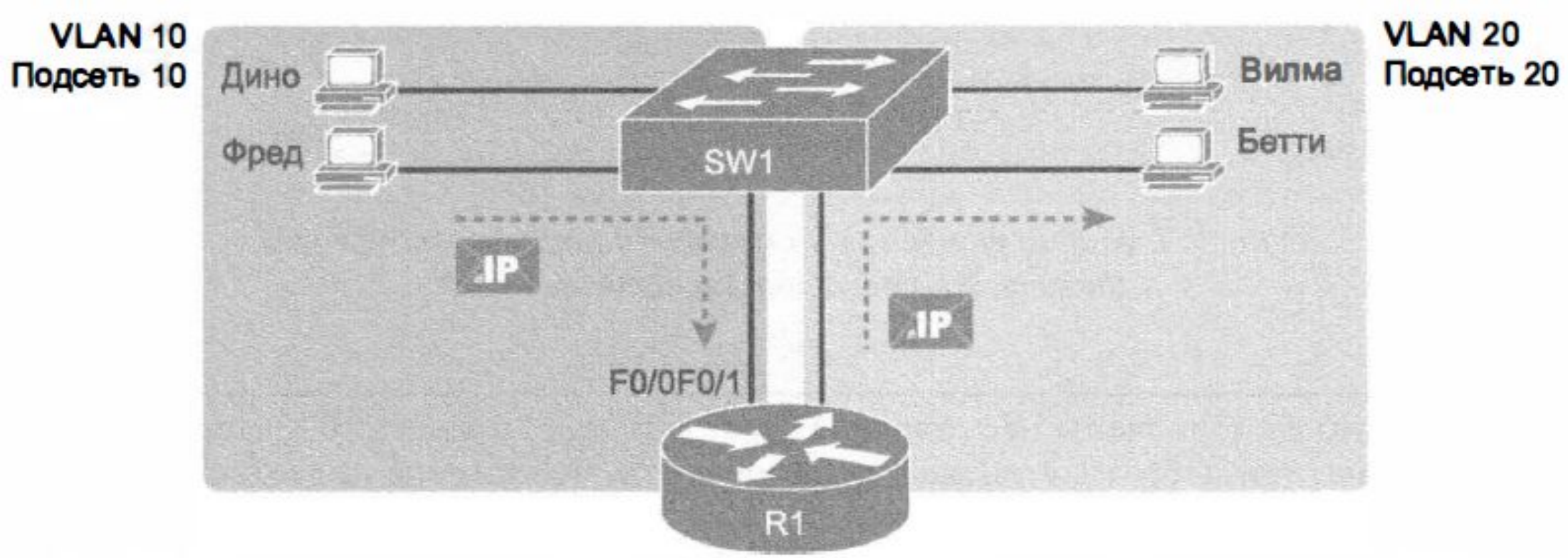

Рис. 9.8. Маршрутизация между двумя сетями VLAN на двух физических интерфейсах

Маршрутизация между VLAN

- Теперь маршрутизатор R1 использует **магистральное соединение VLAN** вместо отдельного канала связи для каждой сети VLAN .

такой проект сети называют "маршрутизатор на палочке" (router-on-a-stick).

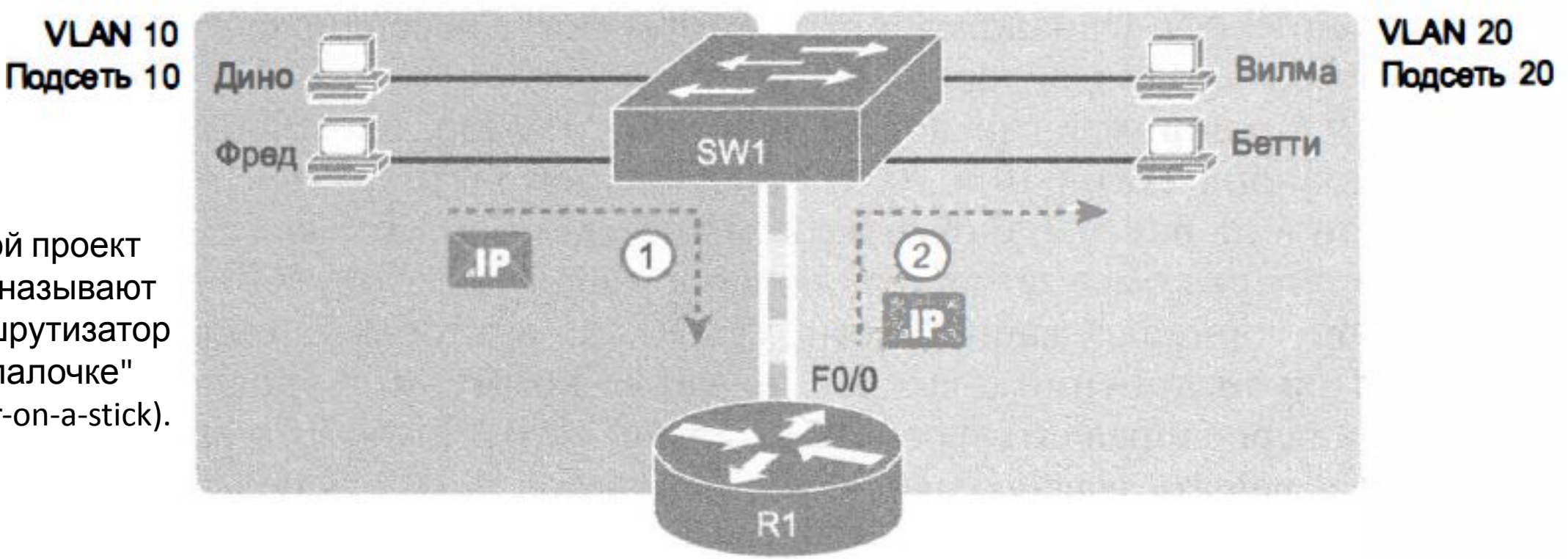

Рис. 9.9. Маршрутизация между двумя сетями VLAN с использованием магистрального канала на маршрутизаторе

Маршрутизация между VLAN (коммутаторы уровня 3)

- У маршрутизации пакетов с использованием физического маршрутизатора есть одна серьезная проблема: **производительность.**

- Для ее решения производители начали объединять аппаратные и программные средства коммутаторов уровня 2 с маршрутизаторами уровня 3, выпуская **коммутаторы уровня 3** (они же **многоуровневые**

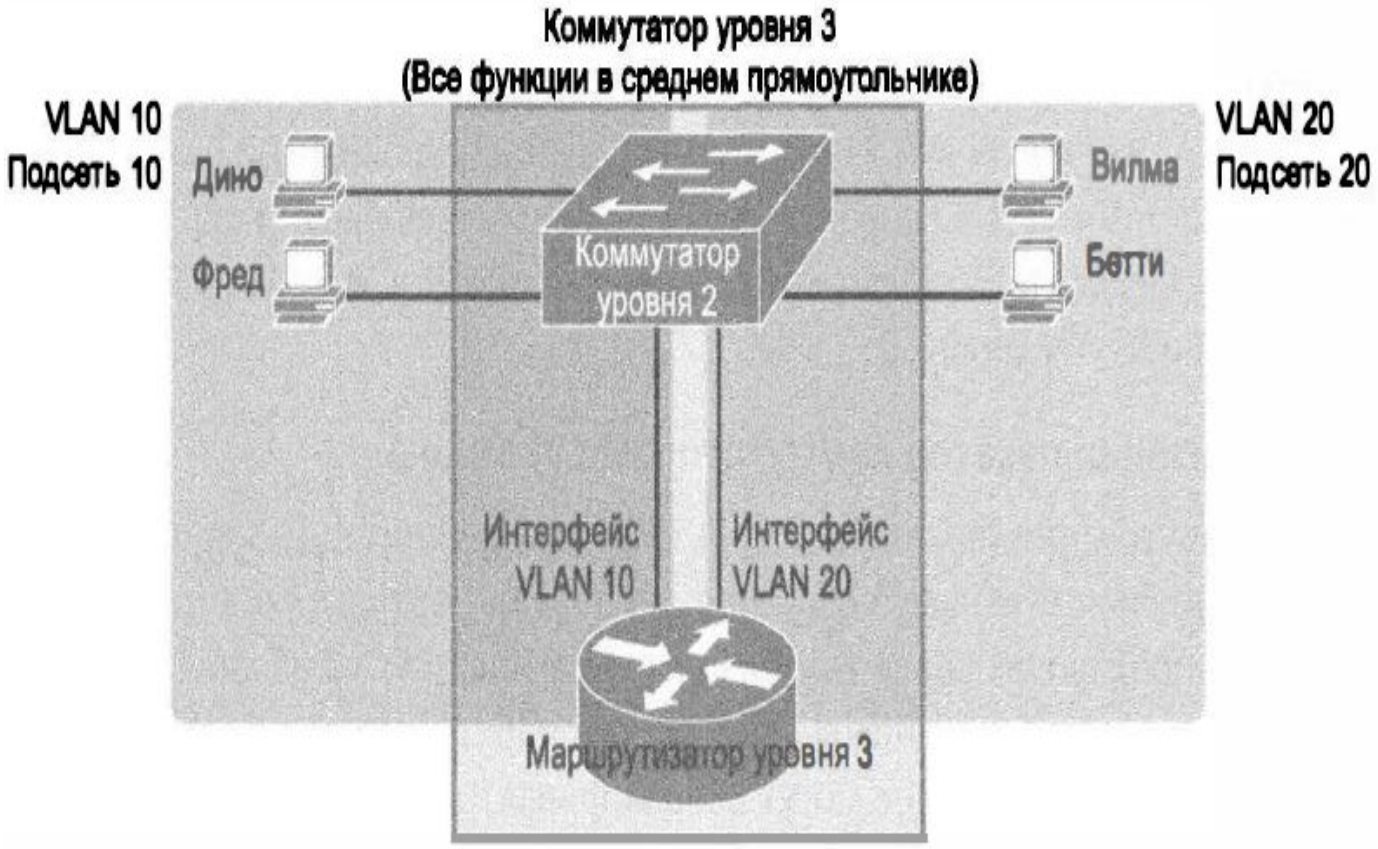

Рис. 9.10. Маршрутизация между сетями VLAN с использованием коммутатора уровня 3

Настройка VLAN

- Чтобы коммутатор Cisco начал **перенаправлять фреймы** в определенную сеть VLAN:

1. его нужно настроить, указав на существование еще **одной сети VLAN**.

2. у коммутатора должны быть **немагистральные интерфейсы** (интерфейсы доступа (access interface)), принадлежащие этой сети VLAN, и (или) **магистральные каналы**, поддерживающие эту VLAN.

Настройка VLAN

ЭТАП	ОПИСАНИЕ
1	В режиме настройки конфигурации введите глобальную команду конфигурации: **vlan идентификатор_ vlan** для создания сети VLAN и перейдите в режим настройки конфигурации сети VLAN.
	(Необязательно) Чтобы присвоить сети VLAN имя, введите подкоманду: **VLAN name имя** Если этого не сделать, именем VLAN будет VLANZZZZ, где zzzz десятичный идентификатор из четырех цифр.
2	Для каждого **интерфейса доступа** (интерфейса, принадлежащего не магистральному каналу, а отдельной сети VLAN) выполните следующие действия: 1. Используя команду **interface**, перейдите в режим конфигурации каждого настраиваемого интерфейса. 2. Используя подкоманду интерфейса **switchport access vlan идентификатор_ vlan**, укажите номер сети VLAN, связанной с данным интерфейсом. 3. (Необязательно) Чтобы отключить магистральное соединение на том же интерфейсе и запретить переговоры о создании магистрального канала, используйте подкоманду интерфейса **switchport mode access**.

Настройка VLAN

- Например, если порты коммутатора следует распределить по трем сетям VLAN (11, 12 и 13), нужно :

1. ввести три **команды vlan 11 , vlan 12 и vlan 13**.

2. затем для каждого интерфейса ввести **команду switchport access vlan 11** (или 12, или 13), чтобы присвоить соответствующий интерфейс надлежащей сети VLAN.

Полная настройка VLAN: пример 1

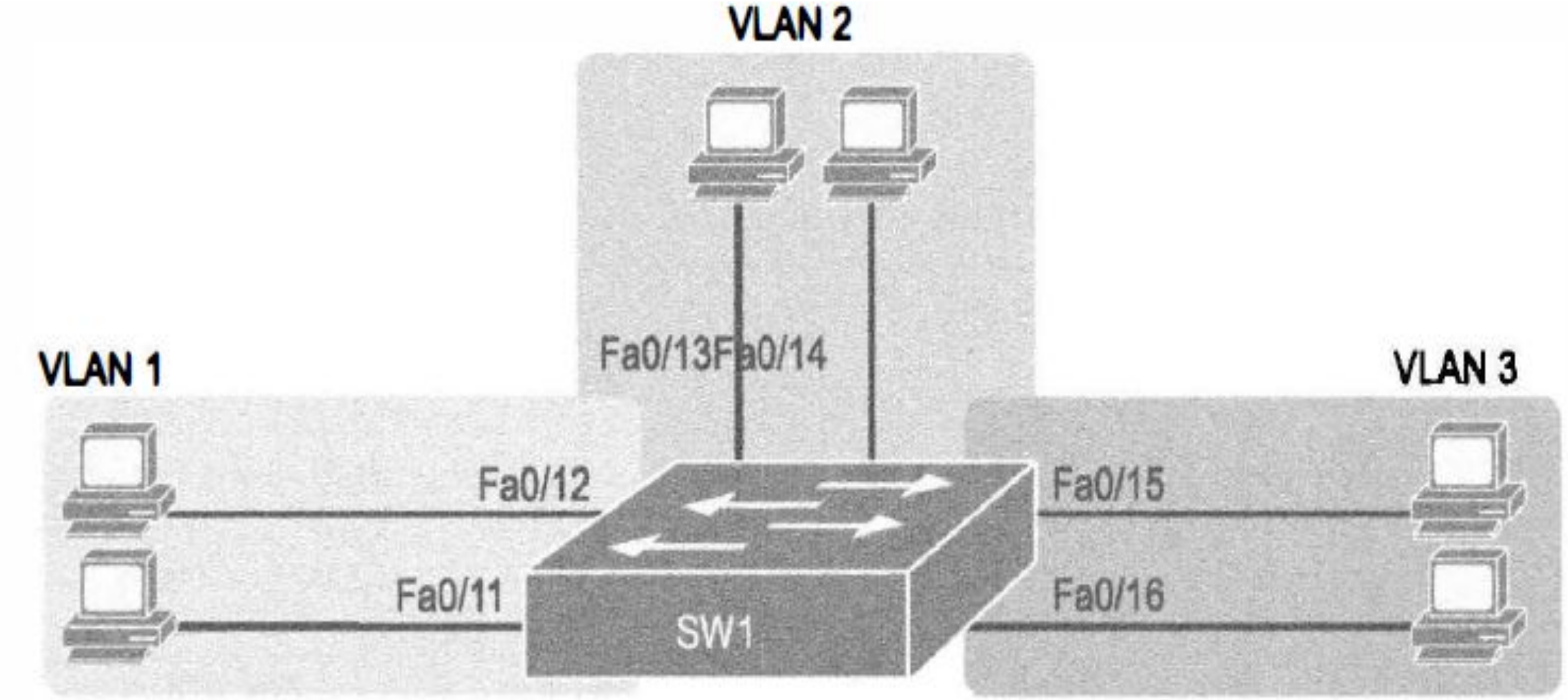

Рис. 9.11. Сеть с одним коммутатором и тремя сетями VLAN

Полная настройка VLAN: пример 1

```
SW1# 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
```

Полная настройка VLAN: пример 1

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# vlan 2
SW1(config-vlan)# name Freds-vlan
SW1(config-vlan)# exit
SW1(config)# interface range fastethernet 0/13 - 14
SW1(config-if)# switchport access vlan 2
SW1(config-if)# end
```

Полная настройка VLAN: пример 1

```
SW1# show running-config
! Часть строк опущена для краткости
vlan 2
name Freds-vlan
!
! еще часть строк опущена для краткости
interface FastEthernet0/13
  switchport access vlan 2
  switchport mode access
!
interface FastEthernet0/14
  switchport access vlan 2
  switchport mode access
!
```

Полная настройка VLAN: пример 1

```
SW1# 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
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
2    Freds-vlan                       active    Fa0/13, Fa0/14
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Полная настройка VLAN: пример 1

```
SW1# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------

2    Freds-vlan                       active    Fa0/13, Fa0/14

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

2    enet  100010     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------

Disabled

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

Сокращенная настройка VLAN: пример 2

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface range Fastethernet 0/15 - 16
SW1(config-if-range)# switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
SW1(config-if-range)# ^Z
```

Сокращенная настройка VLAN: пример 2

```
SW1# 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
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
2    Freds-vlan                       active    Fa0/13, Fa0/14
3    VLAN0003                         active    Fa0/15, Fa0/16
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Протокол создания магистралей VLAN (VTP)

- **Протокол создания магистралей VLAN** (VLAN Trucking Protocol VTP) - это собственный протокол компании Cisco, выполняющийся на ее коммутаторах:
  - ✔ он анонсирует каждую сеть VLAN, настроенную на одном коммутаторе **командой vlan номер**, чтобы о ней узнали все остальные коммутаторы в территориальной локальной сети.

- Каждый коммутатор может работать в одном из **трех режимов VTP**: серверном, клиентском или прозрачном.

Протокол создания магистралей VLAN (VTP)

- Если коммутатор будет использовать **серверный или клиентский** режим VTP, то обнаружится следующее:
  1. серверные коммутаторы могут настраивать сети VLAN только в стандартном диапазоне (1-1005);
  2. клиентские коммутаторы не могут настраивать сети VLAN;
  3. команда show running-config не отображает команды vlan.

- Для включения прозрачного режима протокола VTP используется **глобальная команда vtp mode transparent,** а для его отключения - **глобальная команда vtp mode off**.

Настройка магистрального соединения

- Достаточно добавить одну подкоманду интерфейса для порта коммутатора на каждой стороне канала связи – **switchport mode trunk**, и будет получен магистральный канал VLAN, поддерживаемый всеми сетями VLAN , известными каждому коммутатору (**статическое соединение**).

- Конфигурация магистрали на коммутаторах Cisco имеет несколько вариантов для **динамических переговоров** о разных параметрах магистрали:

  - **тип магистрального соединения**: протокол ISL, протокол 802.1Q или переговоры о применяемом протоколе.
  - **административный режим**: всегда магистральный канал, никогда магистральный канал или переговоры.

Протокол DTP

- Коммутаторы Cisco, поддерживающие протоколы ISL и 802.1Q, способны вести переговоры об используемом типе при помощи **протокола динамического согласования магистральных каналов (Dynamic Trunk Protocol - DTP)**.

- Протокол DTP позволяет также согласовать административный режим локальных портов коммутаторов (**команда switchport mode**) и параметры:

access	Всегда быть портом доступа (а не магистрального канала)
trunk	Всегда быть портом магистрального канала
dynamic desirable	Передавать и отвечать на сообщения переговоров, чтобы динамически решить, использовать ли магистральное соединение
dynamic auto	Пассивно ожидать получения сообщений переговоров. При получении таковых вести переговоры об использовании магистрального соединения

Магистральные соединения: пример 3

переговоры DTP можно отключить с помощью **подкоманды интерфейса switch port nonegotiate**

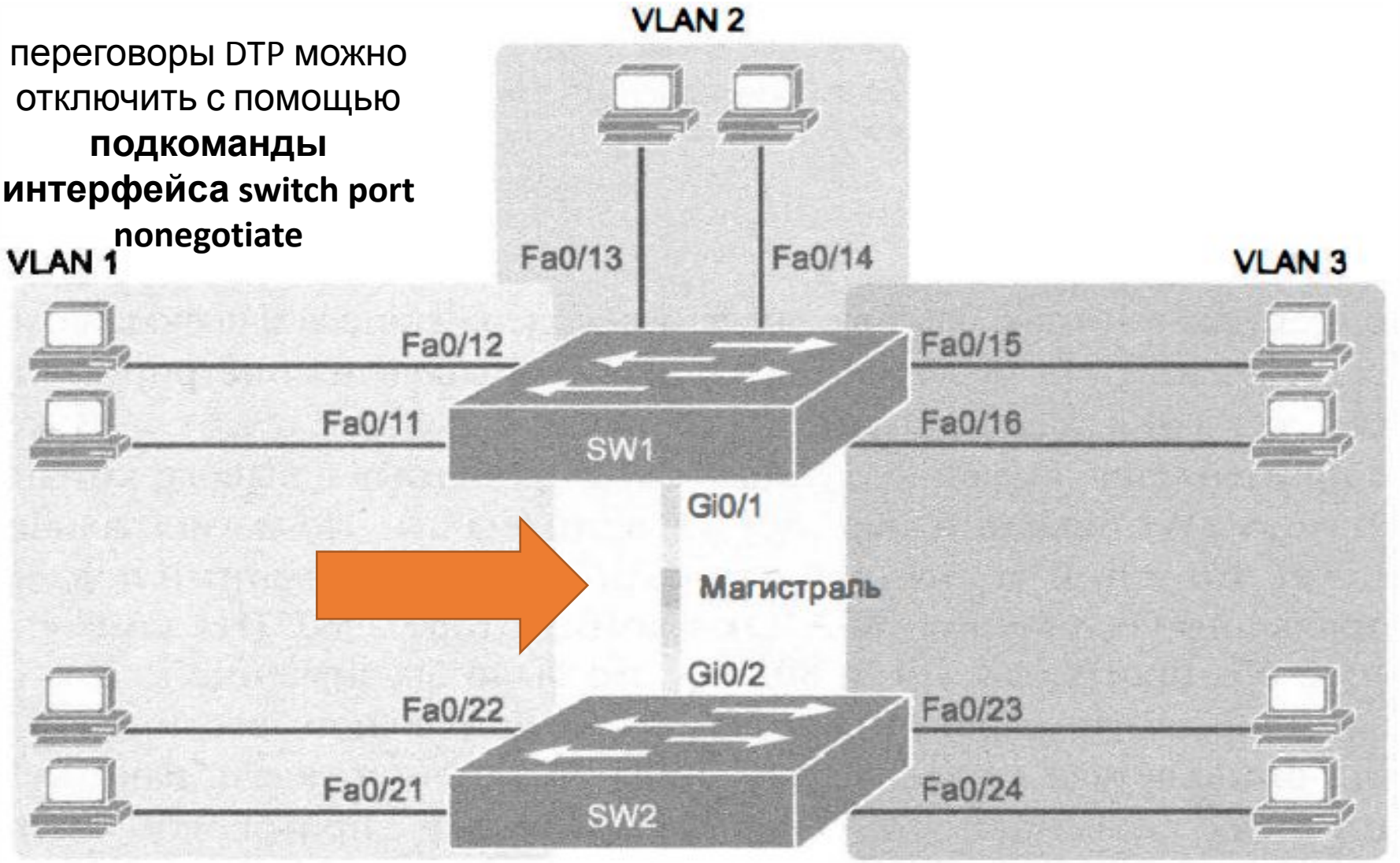

Рис. 9.12. Сеть с двумя коммутаторами и тремя сетями VLAN

Магистральные соединения: пример 3

```
SW1# show interfaces gigabit 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Магистральные соединения: пример 3

- **Команда show interfaces trunk** выводит информацию обо всех интерфейсах магистральных каналов, работающих в настоящий момент, т.е. она перечисляет интерфейсы, которые в настоящее время используют магистральное соединение VLAN.

```
SW1# show interfaces trunk

SW1#
```

- **Не перечисляя интерфейсы**, эта команда также подтверждает, что канал связи между коммутаторами не

Магистральные соединения: пример 3

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface gigabit 0/1
SW1(config-if)# switchport mode dynamic desirable
SW1(config-if)# ^Z
SW1#
01:43:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed
state to down
01:43:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed
state to up
SW1# show interfaces gigabit 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
```

Магистральные соединения: пример 3

```
SW1# show interfaces trunk

Port    Mode         Encapsulation   Status    Native vlan
Gi0/1   desirable    802.1q          trunking  1

Port    Vlans allowed on trunk
Gi0/1   1-4094

Port    Vlans allowed and active in management domain
Gi0/1   1-3

Port    Vlans in spanning tree forwarding state and not pruned
Gi0/1   1-3
```

Магистральные соединения: пример 3

```
SW1# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------

2    Freds-vlan                       active    Fa0/13, Fa0/14, G0/1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

2    enet  100010     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

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

Результаты переговоров DTP

Административный режим	access	dynamic auto	trunk	dynamic desirable
access	access	access	Не используется *	access
dynamic auto	access	access	trunk	trunk
trunk	Не используется *	trunk	trunk	trunk
dynamic desirable	access	trunk	trunk	trunk

Контроль сетей VLAN

- **Список разрешенных сетей VLAN (allowed VLAN list)** - это механизм, позволяющий административно отключать сети VLAN от магистрального канала.

- Стандартно коммутаторы включают в список разрешенных сетей VLAN каждой магистрали **все возможные сети VLAN** (от VLAN 1 до VLAN 4094).

- Однако впоследствии можно сократить количество сетей VLAN, которым разрешено использовать магистральный канал **подкомандой интерфейса**:

```
switchport trunk allowed vlan {add | all | except | remove} список_vlan
```

Причины невозможности передачи трафика по VLAN

1. Сеть VLAN **удалена из списка разрешенных сетей** VLAN для магистрального канала.

2. Сеть VLAN **отсутствует в конфигурации коммутатора** (как свидетельствует вывод команды **show vlan**).

3. Сеть VLAN существует, но **административно отключена** (командой **shutdown**).

4. Сеть VLAN **автоматически отсечена** протоколом VTP.

5. Экземпляр STP сети VLAN перевел магистральный интерфейс в **состояние блокировки**.

Команда show interfaces trunk

- Команда **show interfaces trunk** выводит список идентификаторов VLAN.

- Вывод указанной команды содержит продолжение в виде **трех списков сетей VLAN**, поддерживаемых магистральным каналом:

1. сети VLAN, разрешенные на магистральном канале (стандартно 1 - 4094).
2. сети VLAN настроенные и активные (не отключенные).
3. сети VLAN не отсеченные протоколом VTP и не блокированные протоколом STP.

Отключение VLAN: пример 4

```
SW1# show interfaces trunk

Port    Mode         Encapsulation   Status    Native vlan
Gi0/1   desirable    802.1q          trunking  1

Port    Vlans allowed on trunk
Gi0/1   1-4094

Port    Vlans allowed and active in management domain
Gi0/1   1-3

Port    Vlans in spanning tree forwarding state and not pruned
Gi0/1   1-3
```

Отключение VLAN: пример 4

Этап 1 Настройка сети VLAN 4
Этап 2 Отключение сети VLAN 2
Этап 3 Удаление сети VLAN 3 из списка разрешенных сетей VLAN магистрального канала

```
SW1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# vlan 4
SW1(config-vlan)# vlan 2
SW1(config-vlan)# shutdown
SW1(config-vlan)# interface gi0/1
SW1(config-if)# switchport trunk allowed vlan remove 3
SW1(config-if)# ^Z
```

Отключение VLAN: пример 4

```
! Три списка сетей VLAN в выводе следующей команды показывают разрешенные
! сети VLAN (1, 2 и 4-4094), разрешенные и активные сети VLAN (1 и 4) и
! разрешенные, активные, неотсеченные и перенаправляемые протоколом STP
! сети VLAN (1 и 4).

SW1# show interfaces trunk
Port    Mode         Encapsulation   Status    Native vlan
Gi0/1   desirable    802.1q          trunking  1

! Далее сеть VLAN 3 исключается, поскольку она была удалена из списка
! разрешенных сетей VLAN.
Port    Vlans allowed on trunk
Gi0/1   1-2,4-4094

! Сеть VLAN 2 исключается, поскольку она отключена. Сети VLAN 5-4094
! исключаются, поскольку на коммутаторе SW1 они не настроены.
Port    Vlans allowed and active in management domain
Gi0/1   1,4

Port    Vlans in spanning tree forwarding state and not pruned
Gi0/1   1,4
```

Ключевые темы

Описание
Создание двух широковещательных доменов с использованием одного коммутатора и сети VLAN
Причины применения сетей VLAN
Магистральное соединение VLAN между двумя коммутаторами
Заголовок магистрального соединения по стандарту 802.1Q
Маршругизация между двумя сетями VLAN с использованием магистрального канала на маршрутизаторе
Маршрутизация между сетями VLAN с использованием коммутатора уровня 3
Последовательность настройки конфигурации VLAN и назначения интерфейсов
Параметры команды switchport mode, определяющие административный режим магистрали
Ожидаемый рабочий режим магистрали на основании параметров административных режимов
Причины невозможности передачи трафика сети VLAN по магистральному каналу