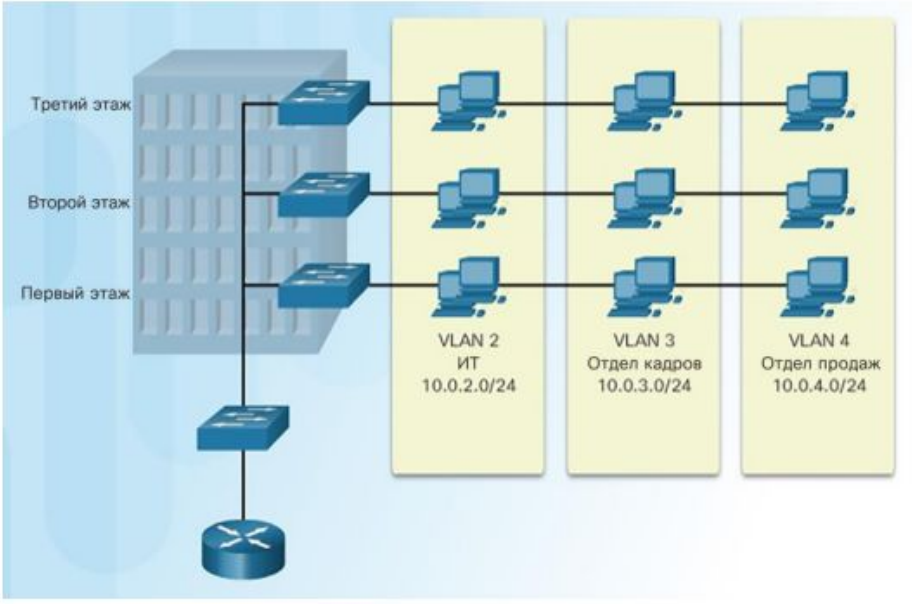
Масштабирование сетей VLAN

Фомочкина Алиса 91ИТ

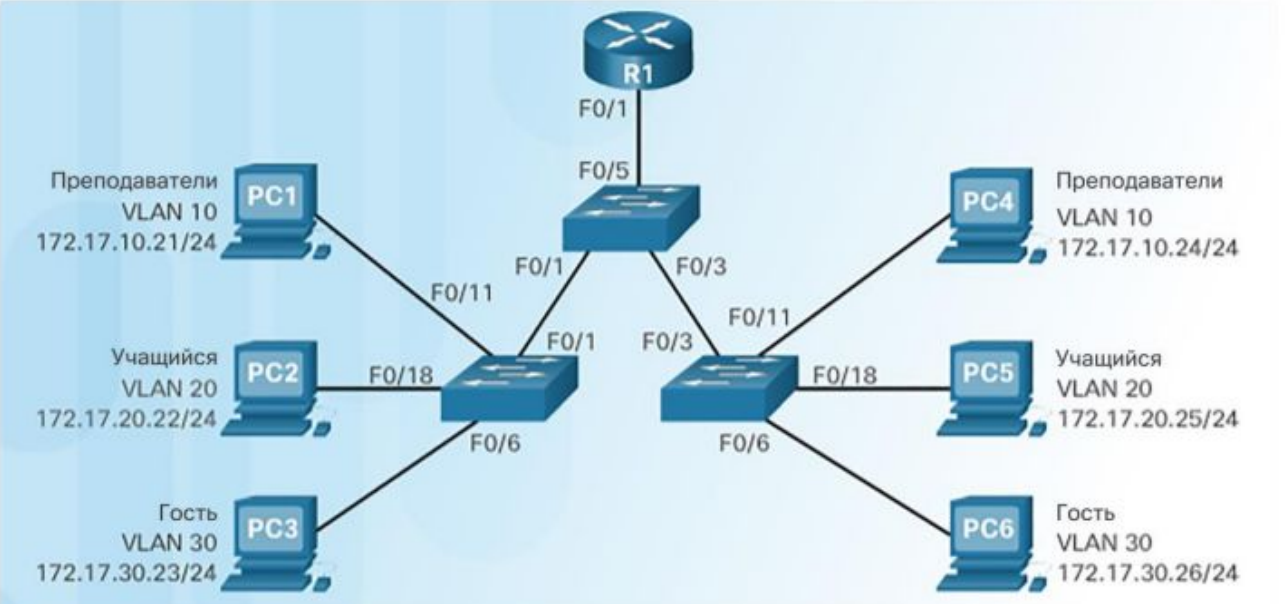
Определение сети VLAN

- Сети VLAN могут сегментировать устройства локальной сети без учета физического расположения пользователя или устройства.
  - На рисунке все ИТ-пользователи на первом, втором и третьем этажах находятся в одном сегменте локальной сети. То же самое относится к пользователям из отдела кадров и отдела продаж.
- Сеть VLAN — это логический раздел сети 2-го уровня.
  - Можно создать несколько разделов, и несколько сетей VLAN могут работать одновременно.
  - Разделение сети 2-го уровня выполняется внутри устройства 2-го уровня, обычно с помощью коммутатора.
  - Каждая сеть VLAN — это домен широковещательной рассылки, который может охватывать несколько физических сегментов локальной сети.
  - Имеющиеся в одной сети VLAN узлы не знают о существовании этой сети VLAN.



- Сети VLAN изолированы друг от друга и могут обмениваться пакетами только через маршрутизатор.

Преимущества сетей VLAN



- Повышенный уровень безопасности
- Снижение затрат
- Повышение производительности
- Меньше Широковещательные домены
- Эффективное использование ИТ-инфраструктуры
- Эффективность управления
- Упрощенная форма управления проектами и приложениями

Типы сетей VLAN

- Распространенные типы сетей VLAN:
  - **VLAN по умолчанию** — также называется VLAN 1. По умолчанию все порты коммутатора назначаются сети VLAN 1.
  - **VLAN данных** — виртуальные локальные сети данных обычно создаются для отдельных групп пользователей или устройств. Они передают пользовательский трафик.
  - **VLAN с нетегированным трафиком** — сеть VLAN, которая передает весь нетегированный трафик. Это трафик, который не исходит из порта сети VLAN (например, трафик BPDU STP, которым обмениваются коммутаторы с поддержкой STP). Сетью VLAN с нетегированным трафиком по умолчанию является сеть VLAN 1.
  - **VLAN управления** — сеть VLAN, которая создается для передачи трафика управления сетью, включая SSH, SNMP, системный журнал и др. По умолчанию для управления сетью используется сеть VLAN 1.

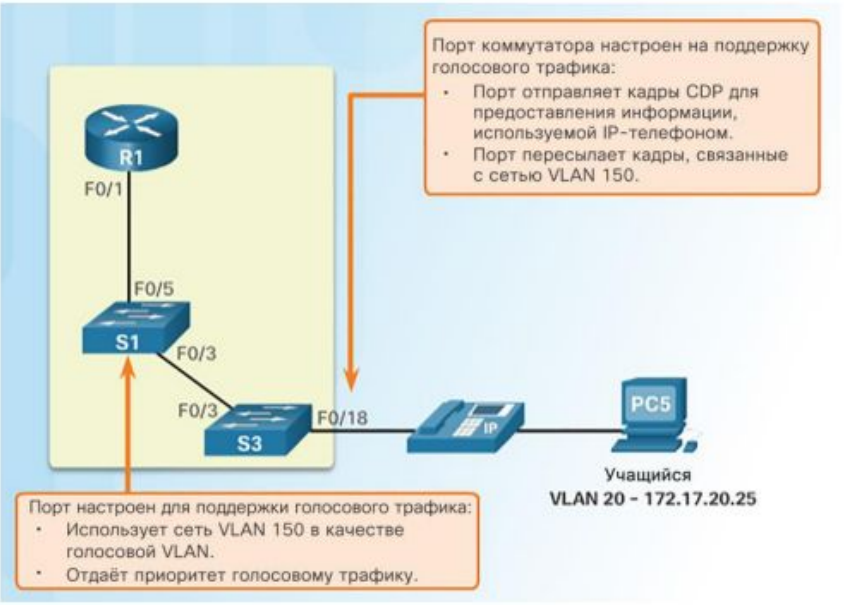
Назначение сети VLAN по умолчанию

```
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
```

Изначально все порты коммутатора относятся к сети VLAN 1.

Голосовые сети VLAN

- Для обслуживания чувствительного к задержкам трафика голосовых данных коммутаторы Cisco поддерживают голосовую VLAN со следующими требованиями.
  - Гарантированная пропускная способность
  - Задержка менее 150 мс во всей сети для обеспечения качественной передачи голоса
  - Приоритет передачи перед другими типами сетевого трафика
  - Возможность маршрутизации в обход перегруженных участков

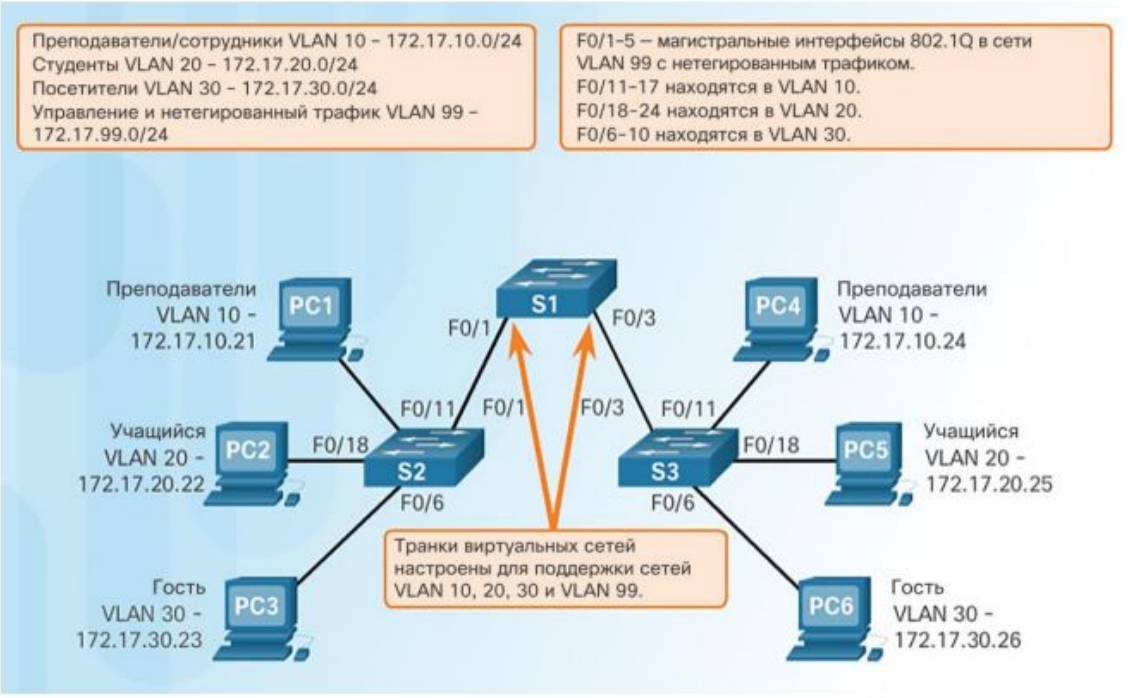


- Функции голосовой сети VLAN позволяют портам доступа передавать трафик голосовых данных пользователей и IP-связи.
  - На рисунке интерфейс F0/18 коммутатора S3 настроен для тегирования трафика с компьютера студента в сети VLAN 20 и трафика голосовых данных в сети VLAN 150.

Магистрали сетей VLAN

- Магистраль сетей VLAN — это двухточечный канал связи, который обслуживает более одной сети VLAN.
  - Обычно она устанавливается между коммутаторами для поддержки обмена данными между сетями VLAN.
  - Магистраль сетей VLAN или магистральные порты не привязаны к какой-либо сети VLAN.

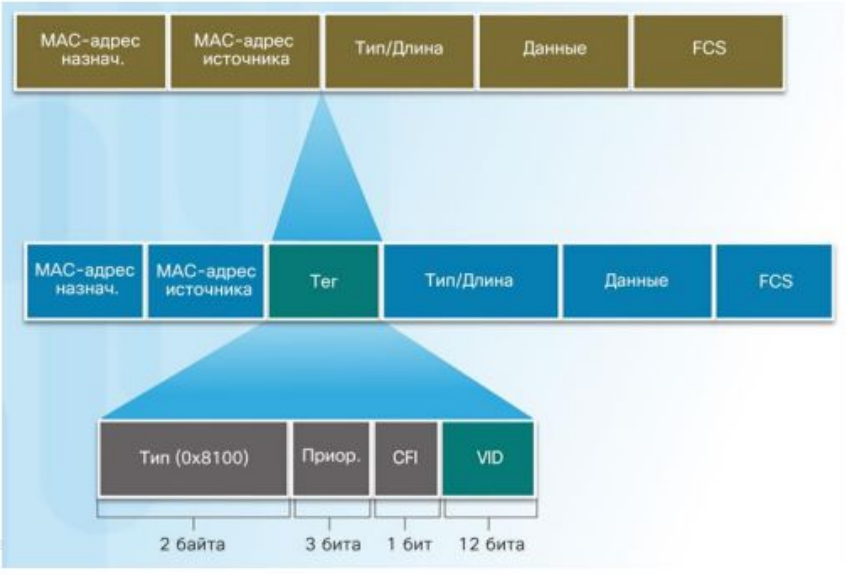
- Cisco IOS поддерживает IEEE 802.1q — популярный протокол магистральных каналов сетей VLAN.



Каналы между коммутаторами S1 и S2, а также между S1 и S3 настроены для передачи трафика, отправляемого по всей сети из VLAN 10, 20, 30 и 99.

Тегирование кадров Ethernet для идентификации сети VLAN

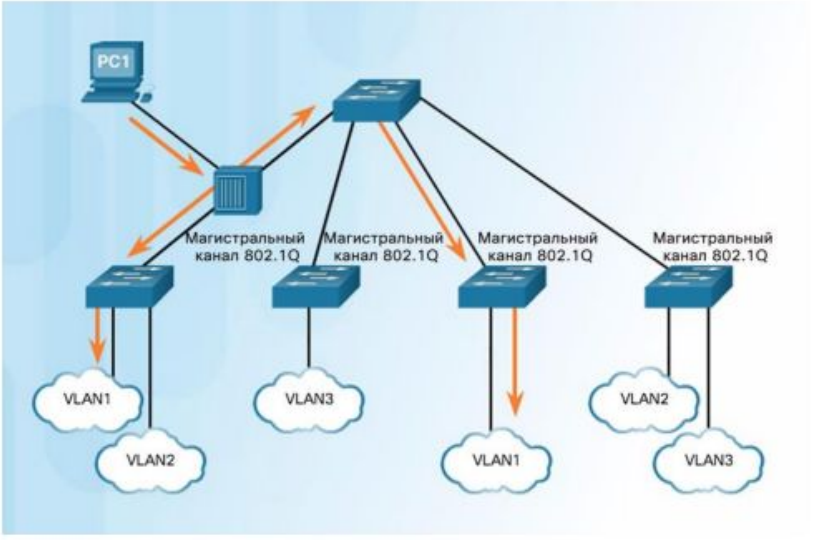
- Перед пересылкой через магистральный канал кадр должен быть снабжен тегом с информацией о сети VLAN, из которой он исходит.
  - Тегирование кадров — это процесс добавления в кадр заголовка с идентификацией сети VLAN.
  - Он используется для правильной передачи нескольких кадров сети VLAN по магистральному каналу.
- IEEE 802.1Q — один из самых распространенных протоколов VTP, определяющий структуру тегирующего заголовка, добавляемого в кадр.
  - Коммутаторы добавляют тегирующую информацию VLAN после поля исходного MAC-адреса.
  - В число имеющихся в теге VLAN протокола 802.1Q полей входит поле идентификатора сети VLAN (VID).
  - Магистральные каналы добавляют информацию тега перед отправкой кадра, а затем удаляют теги перед пересылкой кадров через немагистральные порты.



Сети VLAN в среде с несколькими коммутаторами

VLAN с нетегированным трафиком и тегирование по протоколу 802.1Q

- Управляющий трафик, отправляемый в сети VLAN с нетегированным трафиком, тегировать не следует.
- Кадры, полученные без тегов, остаются без тегов и при пересылке помещаются в сеть VLAN с нетегированным трафиком.
- Если с сетью VLAN с нетегированным трафиком не связаны никакие порты, а также нет других магистральных каналов, то кадр отбрасывается.
- При настройке порта коммутатора Cisco настраивайте устройства таким образом, чтобы они не отправляли тегированные кадры по сети VLAN с нетегированным трафиком.
- В коммутаторах Cisco сеть VLAN с нетегированным трафиком по умолчанию обозначена VLAN 1.



Общие сведения о протоколе VTP

- Протокол VTP помогает сетевому администратору управлять сетями VLAN на коммутаторе, который настраивается в режиме сервера VTP.
- Сервер VTP по магистральным каналам распространяет и синхронизирует данные о сетях VLAN на коммутаторах с поддержкой VTP во всей коммутируемой сети.

Компоненты VTP	Определение
Домен VTP	• Состоит из одного или нескольких соединенных между собой коммутаторов. • Все коммутаторы в домене обмениваются конфигурациями VLAN с помощью объявлений VTP. • Коммутаторы из разных доменов VTP сообщениями VTP не обмениваются. • Граница домена проходит по маршрутизатору или коммутатору уровня 3.
Объявления VTP	• Каждый коммутатор в домене VTP периодически отправляет глобальные объявления с конфигурацией из каждого порта транка на зарезервированный групповой адрес. • Соседние коммутаторы получают эти объявления и при необходимости обновляют свою конфигурацию VTP и сети VLAN.
Режимы VTP	Коммутатор можно настроить в одном из трех режимов VTP: серверном, клиентском или прозрачном.
Пароль VTP	Для коммутаторов в домене VTP также можно задать пароль.

Примечание. Обмен объявлениями VTP не будет выполняться, если магистраль между коммутаторами неактивна или неправильно настроена.

Основные понятия и принципы работы VTP

Режимы VTP

Вопрос о режиме VTP	Сервер VTP	Клиент VTP	Прозрачный режим VTP
В чем отличия?	• Управляет конфигурацией домена и сети VLAN. • Можно настроить несколько серверов VTP.	• Обновляет локальные конфигурации VTP. • Коммутаторы, настроенные в качестве клиентов VTP, не могут изменять конфигурации сети VLAN.	• Управляет локальными конфигурациями сетей VLAN. • Конфигурации сети VLAN не публикуются в сети VTP.
Реагирует ли на объявления VTP?	Участвует полностью	Участвует полностью	Только пересылает объявления VTP
Сохраняется ли глобальная конфигурация сетей VLAN при перезапуске?	Да, глобальные конфигурации сохраняются в NVRAM.	Нет, глобальные конфигурации сохраняются только в ОЗУ.	Нет, локальная конфигурация сети VLAN хранится только в энергонезависимом ПЗУ.
Обновляет ли другие коммутаторы с поддержкой VTP?	Да	Да	Нет

Объявления VTP

- Три типа объявлений VTP:
  - **Сводные объявления** — содержат имя домена VTP и номер версии конфигурации.
  - **Запрос объявления** — это ответ на сообщение сводного объявления, когда сводное объявление содержит более высокий номер версии конфигурации, чем текущее значение.
  - **Объявления подмножеств** — содержат сведения о сетях VLAN, в том числе обо всех изменениях.

Версии VTP

- Коммутаторы в одном домене VTP должны работать с одной версией протокола VTP.

Версия VTP	Определение
VTP версии 1	• Режим VTP по умолчанию на всех коммутаторах. • Поддерживает только сети VLAN в стандартном диапазоне.
VTP версии 2	• Поддерживает только сети VLAN в стандартном диапазоне. • Поддерживает традиционные сети Token Ring. • Поддерживает расширенные функции, включая нераспознанный TLV, прозрачный режим, зависящий от версии, а также проверки согласованности.

Конфигурация VTP по умолчанию

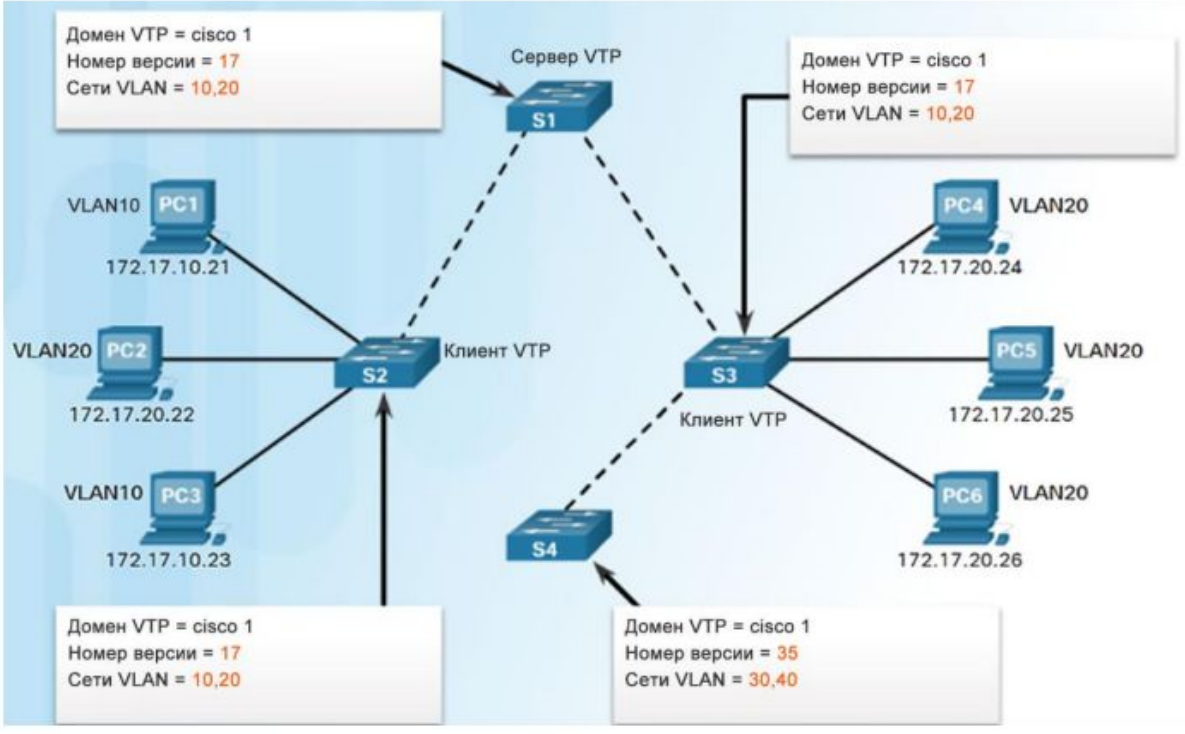
Проверка состояния VTP по умолчанию

```
S1# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : f078.167c.9900
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:11

Feature VLAN:
--------------
VTP Operating Mode                : Transparent
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 12
Configuration Revision            : 0
MD5 digest                        : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                                    0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC

S1#
```

- Команда **Show vtp status** отображает статус VTP, в который входит следующая информация:
  - VTP Version capable и VTP Version running
  - доменное имя VTP
  - VTP Pruning Mode
  - VTP Traps Generation
  - Device ID
  - Configuration Last Modified
  - VTP Operating Mode
  - Maximum VLANs Supported Locally
  - Число существующих сетей VLAN.
  - Configuration Revision
  - MD5 Digest

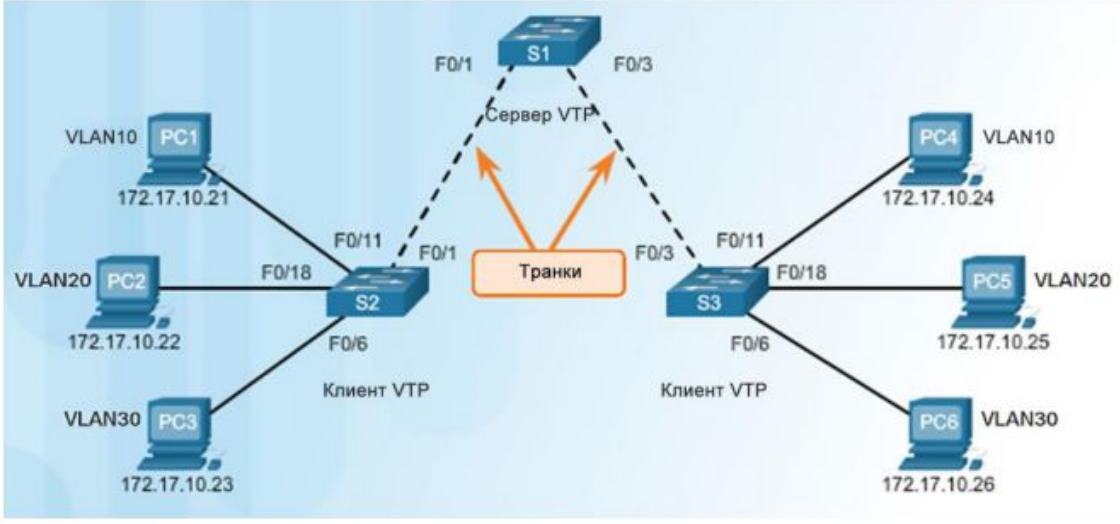
Предосторожность при использовании VTP

- Номер версии конфигурации VTP хранится в NVRAM.
- Чтобы сбросить номер версии конфигурации VTP на ноль:
  - изменить имя домена VTP коммутатора на несуществующее, а затем вернуть исходное имя домена;
  - изменить режим VTP коммутатора на прозрачный, а затем вернуть на исходный режим VTP.



Конфигурация VTP

Обзор конфигурации VTP



- Процедура настройки VTP:
  - **Шаг 1.** Настройка сервера VTP
  - **Шаг 2.** Настройка доменного имени и пароля VTP
  - **Шаг 3.** Настройка клиентов VTP
  - **Шаг 4.** Настройка сетей VLAN на сервере VTP
  - **Шаг 5.** Проверка получения клиентами VTP новых данных о VLAN

Настройка сервера VTP

```
S1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# vtp mode ?
  client           Set the device to client mode.
  off              Set the device to off mode.
  server           Set the device to server mode.
  transparent      Set the device to transparent mode.

S1(config)# vtp mode server
Setting device to VTP Server mode for VLANS.
S1(config)# end
S1#
```

```
S1# show vtp status
VTP Version capable                 : 1 to 3
VTP version running                 : 1
VTP Domain Name                     :
VTP Pruning Mode                    : Disabled
VTP Traps Generation                : Disabled
Device ID                           : f078.167c.9900
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:11
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                  : Server
Maximum VLANs supported locally     : 255
Number of existing VLANs            : 5
Configuration Revision              : 0
MD5 digest                          : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                                      0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC
S1#
```

- Используйте команду **vtp mode server** для настройки коммутатора в качестве сервера VTP.
  - Перед выполнением этой команды убедитесь, что на всех коммутаторах задана конфигурация по умолчанию, чтобы избежать проблем с версиями конфигураций.
- Для проверки используйте команду **show vtp status**.
  - Обратите внимание, что номер версии конфигурации по-прежнему равен 0, а число существующих сетей VLAN равно 5.
  - 5 сетей VLAN — это VLAN 1, существующая по умолчанию, и сети VLAN 1002–1005.

Настройка доменного имени и пароля VTP

- Задайте доменное имя с помощью команды **vtp domain** *доменное-имя*.
  - Чтобы клиент VTP мог принимать объявления VTP, у него должно быть такое же доменное имя, как у сервера VTP.
- Задайте пароль с помощью команды **vtp password** *пароль*.
  - Для проверки используйте команду **show vtp password**.

```
S1(config)# vtp domain ?
  WORD The ascii name for the VTP administrative domain.

S1(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
*Mar 1 02:55:42.768: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG:
VTP domain name changed to CCNA.
S1(config)#
```

```
S1(config)# vtp password cisco12345
Setting device VTP password to cisco12345
S1(config)# end
S1# show vtp password
VTP Password: cisco12345
S1#
```

Настройка сетей VLAN на сервере VTP

- Для создания сетей VLAN используется команда **vlan** *номер-vlan*.
- Для проверки сетей VLAN служит команда **show vlan brief**.
- Проверка статуса сервера выполняется с помощью команды **show vtp status**.
  - Каждый раз при добавлении сети VLAN регистр конфигурации увеличивается

```
S1(config)# vlan 10
S1(config-vlan)# name SALES
S1(config-vlan)# vlan 20
S1(config-vlan)# name MARKETING
S1(config-vlan)# vlan 30
S1(config-vlan)# name ACCOUNTING
S1(config-vlan)# end
S1#
```

```
S1# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------
1    default             active    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
10   SALES               active
20   MARKETING           active
30   ACCOUNTING          active
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
S1#
```

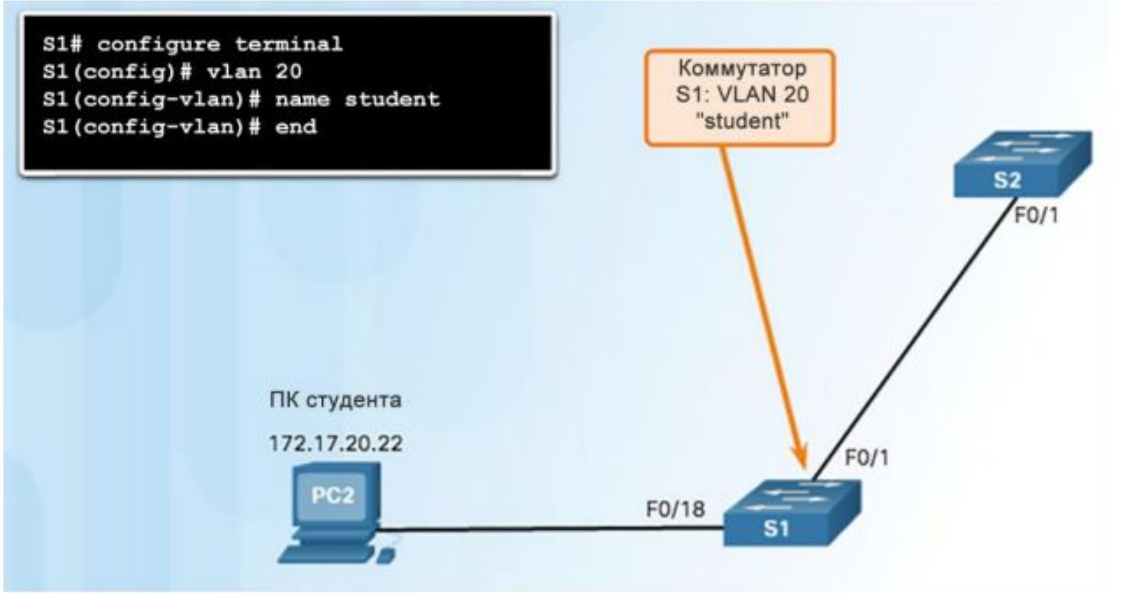
```
S1# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : f078.167c.9900
Configuration last modified by 0.0.0.0 at 3-1-93 02:02:45
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
Configuration Revision          : 6
MD5 digest                      : 0xFE 0x8D 0x2D 0x21 0x3A 0x30 0x99 0xC8
                                  0xDB 0x29 0xBD 0xE9 0x48 0x70 0xD6 0xB6

S1#
```

Назначение портов сетям VLAN

- Порт доступа может принадлежать только одной виртуальной сети VLAN.
  - Единственным исключением является подключение к порту IP-телефона. В этом случае с портом будут связаны две сети VLAN: одна для передачи голоса и одна для передачи данных.

Примечание. Для одновременной настройки нескольких интерфейсов используйте команду **interface range**.

Команды коммутатора Cisco под управлением ОС IOS	
Войдите в режим глобальной настройки.	`S1# configure terminal`
Войдите в режим интерфейсной конфигурации.	`S1 (config) # interface interface_id`
Переведите порт в режим доступа.	`S1 (config-if) # switchport mode access`
Назначьте порт сети VLAN.	`S1 (config-if) # switchport access vlan vlan_id`
Вернитесь в привилегированный исполнительский режим.	`S1 (config-if) # end`



Проблемы в работе протоколов VTP и DTP

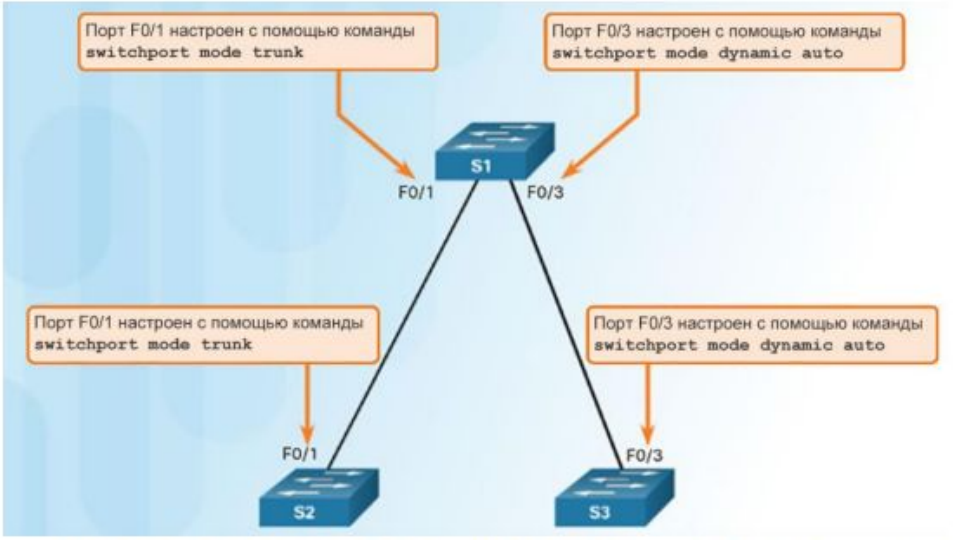
Поиск и устранение неполадок в работе протокола VTP

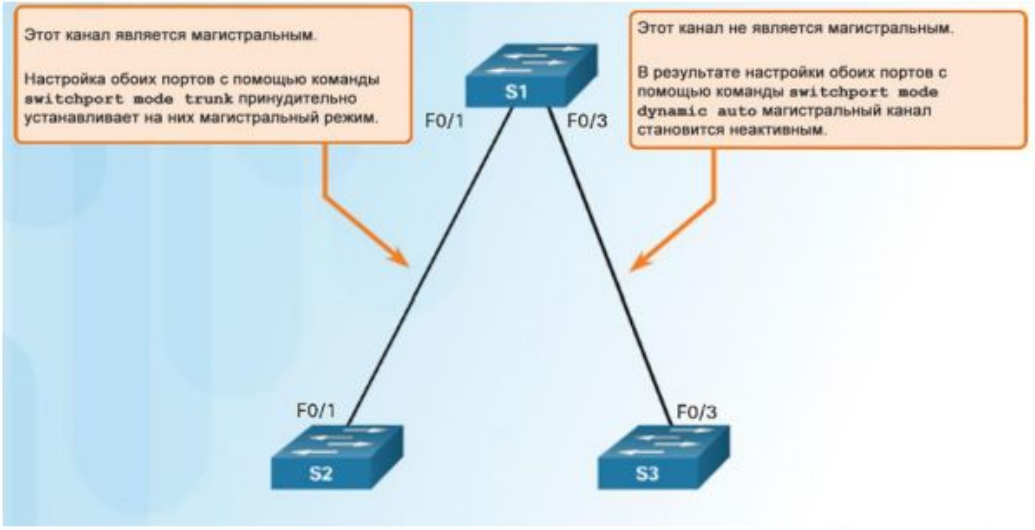
Распространенные проблемы с VTP

- Несовместимые версии VTP
- Проблемы с паролем VTP
- Неправильное имя домена VTP
- Все коммутаторы настроены в режиме клиента
- Неправильный номер версии конфигурации

Динамический протокол транкинга

Общие сведения о DTP





- Управление согласованием магистралей осуществляется по динамическому протоколу транкинга (Dynamic Trunking Protocol — DTP)
  - Протокол DTP — это собственный протокол компании Cisco,
  - который автоматически включен на коммутаторах Catalyst 2960 и Catalyst 3560.
- Для включения магистральной связи от коммутатора Cisco к устройству, которое не поддерживает DTP, используйте команды **switchport mode trunk** и **switchport nonegotiate**.

Динамический протокол транкинга

Режимы интерфейса для согласования

- Разные магистральные режимы:
  - **Switchport mode access** — интерфейс становится немагистральным.
  - **Switchport mode dynamic auto** — интерфейс становится магистральным, если соседний интерфейс переведен в магистральный или предпочтительный режим.
  - **Switchport mode dynamic desirable** — интерфейс становится магистральным, если соседний интерфейс переведен в магистральный, предпочтительный или динамический автоматический режим.
  - **Switchport mode trunk** — интерфейс становится магистральным, даже если соседний интерфейс не является таковым.
  - **Switchport nonegotiate** — не позволяет интерфейсу создавать кадры DTP.

	Dynamic Auto	Dynamic Desirable	Trunk	Доступ
Dynamic Auto	Доступ	Trunk	Trunk	Доступ
Dynamic Desirable	Trunk	Trunk	Trunk	Доступ
Trunk	Trunk	Trunk	Trunk	Ограниченные возможности подключения
Доступ	Доступ	Доступ	Ограниченные возможности подключения	Доступ

```
S1# show dtp interface f0/1
DTP information for FastEthernet0/1:
  TOS/TAS/TNS:                              TRUNK/ON/TRUNK
  TOT/TAT/TNT:                              802.1Q/802.1Q/802.1Q
  Neighbor address 1:                       0CD996D23F81
  Neighbor address 2:                       000000000000
  Hello timer expiration (sec/state):       12/RUNNING
  Access timer expiration (sec/state):      never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state):   never/STOPPED
  FSM state:                                S6:TRUNK
  # times multi & trunk                     0
  Enabled:                                  sim
  In STP:                                   no

<output omitted>
```

- При возможности настраивайте магистральные каналы статически.
- Для проверки протокола DTP служит команда **show dtp interface**.

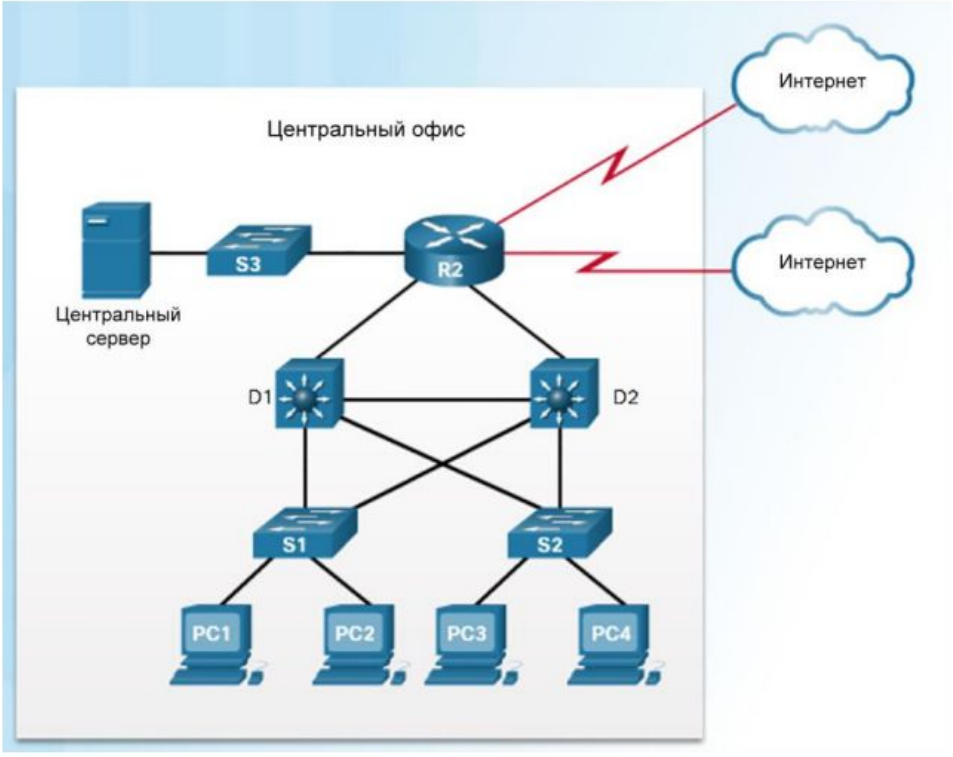
Поиск и устранение неполадок в работе DTP

Распространенные проблемы с магистральными каналами

Компоненты DTP	Определение
Несовпадение режимов транкинга	• Например, один магистральный порт настроен на режим магистральных каналов, а другая сторона настроена в качестве порта доступа. Другой пример — обе стороны настроены в автоматическом режиме DTP. Возможны и другие несовпадения • При этой ошибке конфигурации магистраль перестает работать. • Чтобы устранить проблему, выключите интерфейс, исправьте настройки режимов DTP и включите интерфейс снова.
Разрешенные сети VLAN на транках	• Список разрешенных на магистрали сетей VLAN не был обновлен в соответствии с текущими требованиями VTP. • В этом случае по магистрали передается неизвестный трафик или передача трафика прекращается. • Настройте правильные сети VLAN, которые разрешены в магистрали.
Несовпадение native VLAN	• Когда сети native VLAN не совпадают, коммутаторы формируют информационные сообщения о проблеме. • Убедитесь, что на обеих сторонах магистрального канала используется одна и та же сеть VLAN с нетегированным трафиком.

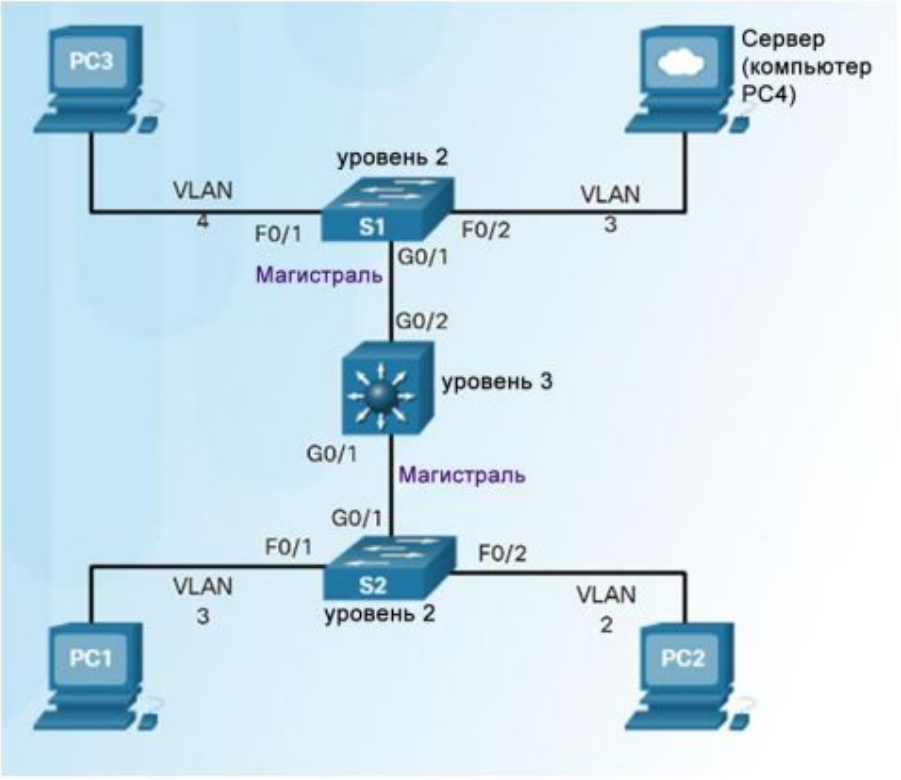
Принцип работы и настройка коммутации 3-го уровня

Введение в коммутацию 3-го уровня



- Многоуровневые коммутаторы обеспечивают высокую скорость обработки пакетов, используя аппаратную коммутацию.
- Многоуровневые коммутаторы Catalyst поддерживают следующие типы интерфейсов 3-го уровня:
  - **Маршрутизируемый порт** — интерфейс 3-го уровня
  - **Виртуальный интерфейс коммутатора (SVI)** — виртуальный интерфейс для маршрутизации между сетями VLAN
- Все коммутаторы Cisco Catalyst 3-го уровня поддерживают протоколы маршрутизации, но некоторые модели коммутаторов требуют ПО с расширенными возможностями для активации отдельных функций и протоколов маршрутизации.
- Коммутаторы серии Catalyst 2960 под управлением IOS 12.2(55) или более поздней версии поддерживают статическую маршрутизацию.

Неполадки в настройках коммутатора 3-го уровня



- Для поиска и устранения неполадок коммутации 3-го уровня проверьте следующее:
  - **Сети VLAN** — проверка правильности настройки.
  - **Интерфейсы SVI** — проверка правильности IP-адреса, маски подсети и номера сети VLAN.
  - **Маршрутизация** — проверка правильности настройки и включения статической или динамической маршрутизации.
  - **Хосты** — проверка правильности IP-адреса, маски подсети и шлюза по умолчанию.