Если вы помните, то ранее мы с вами уже обсуждали настройку VLAN на коммутаторах фирмы Cicso. Для этого, первым делом, мы создавали на каждом коммутаторе требуемые нам VLANы. Делалось это с помощью довольно простых команд (в данном случае создаем только один vlan с номером 7 и именем god\_lan):

**Switch(config)#vlan 7**

**Switch(config-vlan)#name god\_lan**

Конечно, когда необходимо ввести эти команды на одном – двух коммутаторах, то никаких проблем это не составляет. Но что если нам необходимо добавить не одну виртуальную сеть, а скажем с десяток, и это требуется сделать не на одном коммутаторе, а скажем на 10 или нет даже на 100, что тогда? Вводить сотни строк кода каждый раз когда нам необходимо изменить присутствующие на коммутаторах [VLAN](http://www.netza.ru/2012/10/vlan.html)? К счастью нет, избавиться от такой нудной и кропотливой работы нам поможет протокол VTP.

Протокол VTP отвечает за распространение сведений о VLAN существующих на одних коммутаторах,  между  остальными коммутаторами определенной группы (такую группу коммутаторов обычно называют VTP доменом) и сильно упрощает процесс реконфигурации виртуальных локальных сетей на коммутаторах фирмы [Cisco](http://www.netza.ru/2012/10/cisco.html).

Все коммутаторы, на которых функционирует протокол VTP, могут работать в одном из трех режимов: сервер, клиент, прозрачный режим. Коммутаторы, работающие в режиме сервера, позволяют вносить изменения в конфигурацию VLAN на текущем коммутаторе, а так же способны распространять данную конфигурацию между другими  коммутаторами VTP домена, передавая данные о внесенных изменениях через магистральные порты. Коммутаторы, работающие в режиме клиента, способны принимать данные об изменениях в составе виртуальных локальных сетей отправленные коммутаторами, работающими в режиме VTP серверов, и способны на основание этих данных перестраивать свои списки существующих VLAN. Коммутаторы работающие в прозрачном режиме пропускают через свои магистральные порты данные об изменение в конфигурации VLAN, но не применяют их по отношению к своей конфигурации VLAN.

Давайте рассмотрим процесс конфигурации протокола VTP на конкретном примере. Пусть у нас есть сеть следующего вида:

|  |
| --- |
| [Тестовая сеть](http://3.bp.blogspot.com/-dKWzLeJkaT4/UZesOCguUhI/AAAAAAAABFY/E7J14AZJPuI/s1600/1_vtp.png) |
| Тестовая сеть |

Устройства имеют следующую конфигурацию:

Коммутатор Switch0:

**Switch(config)#interface range fastEthernet 0/1-2**

**Switch(config-if-range)#switchport mode trunk**

Коммутатор Switch1:

**Switch(config)#interface fastEthernet 0/1**

**Switch(config-if)#switchport mode trunk**

Коммутатор Switch2:

**Switch(config)#interface fastEthernet 0/1**

**Switch(config-if)#switchport mode trunk**

Как легко понять с помощью данной конфигурации мы связываем коммутаторы 1 и 2 с коммутатором 0 с помощью магистральных (транковых) портов. Если схема настроена верна то при выполнение команды show interfaces trunk на коммутаторе Switch0, то мы должны увидеть следующую картину:

**Port        Mode         Encapsulation  Status        Native vlan**

**Fa0/1       on           802.1q         trunking      1**

**Fa0/2       on           802.1q         trunking      1**

Теперь допустим нам необходимо добавить на все эти три коммутатора какой то новый VLAN, пусть это будет все тот же VLAN 7 - god\_lan. Конечно это можно сделать обычным способом с помощью команды vlan в режиме конфигурации, но не торопитесь так делать, ведь мы все таки разбираем протокол VTP, и по этому для решения данной задачи мы будем использовать именно его возможности.

Как мы говорили выше все коммутаторы в протоколе VTP играют определенные роли: сервер, клиент и т.д. Поэтому нам необходимо определиться с тем какие роли будут выполнять коммутаторы нашей сети. Сначала выберем коммутатор играющий роль сервер. Обычно в качестве такого коммутатора выбирают устройство приблизительно равноудаленное от всех остальных устройств VTP домена, для того чтобы сократить хоть и небольшую, но нагрузку, возникающую в сети при распространении обновлений протокола VTP между коммутаторам (обновления рассылаются при изменение конфигурации VLAN сетей на сервере, а так же каждые 300 секунд).Так же необходимо отметить что в сети может быть несколько VTP серверов.

В нашем случае в качестве VTP сервера удобно выбрать коммутатор Switch0 (Хотя если вам очень хочется можете выбрать любой другой). Для того чтобы сконфигурировать Switch0 в качестве VTP сервера выполним на нем следующие команды:

**Switch(config)#vtp domain TEST**

**Switch(config)#vtp password 123**

**Switch(config)#vtp version 2**

Грубо говоря обязательная из этих команд только первая. Остальные при желание можно опустить. Но обо всем по порядку. С помощью первой команды мы задаем имя нашему VTP домену, аккуратнее регистр имеет значение. По умолчанию каждый коммутатор сконфигурирован в качестве VTP сервера и пустым именем VTP домена. С помощью второй команды мы задаем пароль необходимый для того чтобы коммутатор мог вступить в VTP домен. С помощью третьей команды мы задаем используемую версию протокола VTP (по умолчанию и так используется версия 2, об отличие версий протокола VTP поговорим в следующих статьях ).

Далее сконфигурируем коммутаторы Switch1 и Switch2 в качестве клиентов VTP, для этого выполним на них команды:

**Switch(config)#vtp domain TEST**

**Switch(config)#vtp password 123**

**Switch(config)#vtp version 2**

**Switch(config)#vtp mode client**

Опять же здесь обязательные только первые две команды. Причем первая из них тоже может не понадобиться в том случае если вы подключаете к VTP домену коммутатор с пустым именем VTP домена, так как в этом случае он подхватит имя VTP домена автоматически от существующих в домене серверов. Последняя команда указывает коммутатору что ему необходимо функционировать в качестве клиента в VTP домене.

После введения данных команд базовую конфигурацию нашего VTP домена можно считать законченной. Настало время проверить его работу. Для этого мы выполним на коммутаторе Switch0 команды:

**Switch(config)#vlan 7**

**Switch(config-vlan)#name god\_lan**

А затем посмотрим вывод команды sho vlan brief на коммутаторе Switch1 или Switch0, если протокол VTP работает то мы должны увидеть следующую картину:

**VLAN Name                             Status    Ports**

**---- -------------------------------- --------- -------------------------------**

**1    default                          active    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, Gig1/1**

**Gig1/2**

**7    god\_lan                          active**

**1002 fddi-default                     active**

**1003 token-ring-default               active**

**1004 fddinet-default                  active**

**1005 trnet-default                    active**

Как можно увидеть из данного вывода команды, хотя мы и не выполняли команды добавления VLAN с номером 7 на коммутаторах Switch1 или Switch2, он все же присутствует на них и происходит это благодаря работе протокола VTP.

Теперь для интереса попробуем добавить новый VLAN на коммутаторе Switch1 выполнив команду:

**Switch(config)#vlan 8**

После ввода данной команды мы получим сообщение вида:

**VTP VLAN configuration not allowed when device is in CLIENT mode.**

Прямо говорящее нам о том, что мы не можем добавлять VLANы на коммутаторах функционирующих в качестве клиентов в VTP домене.

И так мы научились выполнять базовую конфигурацию протокола VTP, которая уже позволяет нам распространять обновления конфигурации VLAN на коммутаторах нашей сети. О других фишках протокола VTP мы поговорим в следующих статьях.

DTP (англ. *dynamic trunking protocol* — динамический протокол транкинга) — проприетарный сетевой протокол канального уровня, разработанный компанией Cisco для реализации транкинговой системы для связи в сети VLAN между двумя сетевыми коммутаторами и для реализации инкапсуляции.

Согласование характеристик магистральных каналов с использованием динамического протокола ISL (Dynamic ISL — DISL) или **динамического протокола формирования магистральных каналов (DTP)** позволяет двум соединенным между собой портам согласовать решение о том, должны ли они стать портами магистрального канала. Такое согласование применяется для того, чтобы администратору не приходилось настраивать конфигурацию с обеих сторон магистрального канала и достаточно было выполнить настройку только с одной стороны. Порт, находящийся на другом конце канала, может выполнить настройку требуемых параметров автоматически. Автор предпочитает настраивать все порты магистральных каналов вручную, поскольку автоматическое согласование обычно не позволяет сэкономить столь существенное время (но печально известно тем, что нарушения в его работе приводят к большим неприятностям).

Существуют следующие настройки режима порта коммутатора:

* Access — ставит Ethernet-порт в режим постоянного бестранкового состояния и преобразовывает канал связи в бестранковый. Ethernet-порт становится бестранковым, даже если соседний порт не согласен с изменением.
* Trunk — переводит порт Ethernet в постоянный режим транкинга и согласовывает с другими портами, чтобы преобразовать канал связи в одиночный канал связи; порт становится транк-портом даже если соседний порт не согласен с изменением.
* Dynamic Auto — делает порт Ethernet готовым преобразовать канал связи в одиночный канал связи; порт становится транк-портом, если соседний порт установит режим Trunk или Dynamic Desirable; этот режим используется по умолчанию для всех портов [Ethernet](https://ru.bmstu.wiki/AoE_(ATA_over_Ethernet)).
* Dynamic Desirable — порт активно пытается преобразовать канал связи в одиночный канал связи; порт становится транк-портом, если соседний Ethernet-порт установит режим Trunk, Dynamic Desirable или Dynamic Auto.
* Nonegotiate — отключает DTP, порт не будет отправлять DTP-кадры или использовать входящие DTP-кадры; чтобы установить одиночный канал связи между двумя коммутаторами, когда DTP отключен, транкинг на каждой из сторон настраивается вручную.

Как правило, проще всего перевести порты с обеих концов канала либо в режим on, либо в режим off. Но если порт на одном из концов канала переведен в режим on или desirable, то порт, находящийся на другом конце, автоматически приступает к формированию магистрального канала, поскольку для всех портов, способных поддерживать магистральный канал (портов Ethernet со скоростью 100 Мбит/с или более высокой скоростью), по умолчанию предусмотрен режим auto[[1]](https://ru.bmstu.wiki/DTP_(Dynamic_Trunking_Protocol)" \l "cite_note-1)

**Подробнее о режимах и их включении**

Dynamic Trunking Protocol помогает автоматически создавать trunk между двумя устройствам Cisco. В случае, когда на двух портах включен DTP, и хотя бы один из них переведен в режим desirable, два коммутатора согласуют организацию trunk на этой линии связи. Не следует путать DTP и [VLAN (Virtual Local Area Network)](https://ru.bmstu.wiki/VLAN_(Virtual_Local_Area_Network)), хотя [VTP (VLAN Trunking Protocol)](https://ru.bmstu.wiki/VTP_(VLAN_Trunking_Protocol)) домен действительно играет значение для DTP.

Для начала рассмотрим пример как в ручную настроить порт в режим Trunk.

Switch(config)# interface gi0/20

Switch(config-if)# switchport mode trunk

Теперь рассмотрим как это происходит при помощи DTP. DTP имеет два динамических режима когда порт переходит в режим работы trunk.

1. Desirable – порт активно пытается сформировать trunk с удаленным портом другого коммутатора.

Switch(config)# interface gi0/21

Switch(config-if)# switchport mode dynamic desirable

2. Auto – порт в пассивном режиме ожидает когда удаленный коммутатор инициирует создание trunk-а.

Switch(config)# interface gi0/21

Switch(config-if)# switchport mode dynamic auto

Так же есть режим nonegotiate:

3. nonegotiate – порт находится в режиме trunk, но не отсылает DTP кадры и не ожидает их получить от другого коммутатора. Для того, чтобы trunk между коммутаторами заработал, на соседнем коммутаторе порт должен быть настроен в ручную в режиме trunk.

Switch(config)# interface gi0/21

Switch(config-if)# switchport nonegotiate

DTP кадры отсылаются через интерфейс каждые 30 секунд и по этому рекомендуется настраивать trunk в ручную.

Trunk между портами формируется при следующей настройке режима портов:

manual trunk <-> manual trunk manual trunk <-> dynamic desirable manual trunk <-> dynamic auto dynamic desirable <-> dynamic desirable dynamic desirable <-> dynamic auto

**Плюсы и минусы. Способы несанкционированного доступа**

DTP включен по умолчанию на всех современных коммутаторах [Cisco Systems, Inc.](https://ru.bmstu.wiki/Cisco_Systems,_Inc.). Возникает вопрос «зачем?». Действительно ли вы хотите, чтобы коммутаторы создавали trunk по собственной инициативе? Скорее всего нет, по нескольким причинам.

Использование DTP часто говорит о некачественном дизайне, т.к. trunk должны быть там, где запланировано и только там. Во-вторых, оставить порты в режиме DTP — значит создать брешь в безопасности. Все что будет необходимо злоумышленнику, это отправить корректный DTP кадр на access порт, преобразовав его тем самым в trunk. Тем самым злоумышленник получит доступ ко всем [VLAN (Virtual Local Area Network)](https://ru.bmstu.wiki/VLAN_(Virtual_Local_Area_Network)) на этом коммутаторе, которые разрешены на этом порту (по умолчанию все). К счастью, этих двух проблем можно избежать настроив статический режим порта «access» или «trunk» — что является по сути лучшим решением.

! '''Access port'''

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

! '''Trunk port'''

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk encapsulation dot1q

Однако, даже если порт настроен таким образом, DTP все равно активен в порте. Если вы попытаетесь настроить trunk между двумя коммутаторами в разных [VTP (VLAN Trunking Protocol)](https://ru.bmstu.wiki/VTP_(VLAN_Trunking_Protocol)) доменах, вы получите сообщение о ошибке:

*%DTP-5-DOMAINMISMATCH: Unable to perform trunk negotiation on port Fa0/1 because of* VTP domain mismatch.

Помните, что кадр DTP содержит имя [VTP (VLAN Trunking Protocol)](https://ru.bmstu.wiki/VTP_(VLAN_Trunking_Protocol)) домена. Коммутатор не сможет создать trunk на порту с включенным DTP с коммутатором у которого отличается имя домена DTP, даже в случае статической настройки Trunk.