



# Компьютерные сети

Лекция 13. Протоколы DTP и VTP

# Динамический протокол транкинга

## Общие сведения о DTP

Протокол динамического транкинга (DTP) — это собственный протокол Cisco.

Характеристики DTP являются следующими:

- Включен по умолчанию на коммутаторах Catalyst 2960 и 2950
- Динамический автоматический используется по умолчанию для коммутаторов 2960 и 2950
- Может быть отключен с помощью команды **nonegotiate**
- Может быть снова включен, установив интерфейс на **dynamic-auto**
- Установка коммутатора на статический магистраль или статический доступ позволит избежать проблем согласования с **switchport mode trunk** или **switchport mode access**.

```
S1(config-if)# switchport mode trunk
S1(config-if)# switchport nonegotiate

S1(config-if)# switchport mode dynamic auto
```

# Динамический протокол транкинга

## Режимы интерфейса для согласования

Команда **switchport mode** имеет дополнительные параметры.

Используйте команду конфигурации интерфейса **switchport nonegotiate**, чтобы остановить согласование DTP.

Параметр	Описание
<b>access</b>	Режим постоянного доступа и согласовывает преобразование соседнего канала в канал доступа
<b>dynamic auto</b>	Будет становиться интерфейсом магистрали, если соседний интерфейс установлен в транк или режим desirable
<b>dynamic desirable</b>	Активно стремится стать магистралью путем переговоров с другими auto или desirable интерфейсами
<b>транк</b>	режим постоянного транкинга и согласовывает преобразование соседнего канала

# Динамический протокол транкинга (DTP)

## Результаты настройки DTP

Варианты конфигурации DTP являются следующими:

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

## Dynamic Trunking Protocol (DTP)

# Проверка режима DTP

Конфигурация DTP по умолчанию зависит от версии и платформы Cisco IOS.

- Используйте команду **show dtp interface** для определения текущего режима DTP.
- В соответствии с рекомендациями рекомендуется установить для интерфейсов режим доступа или транк и отключить DTP.

```
S1# show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE
Neighbor address 1: C80084AEF101
Neighbor address 2: 000000000000
Hello timer expiration (sec/state): 11/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state: S2:ACCESS
# times multi & trunk 0
Enabled: yes
In STP: no
```

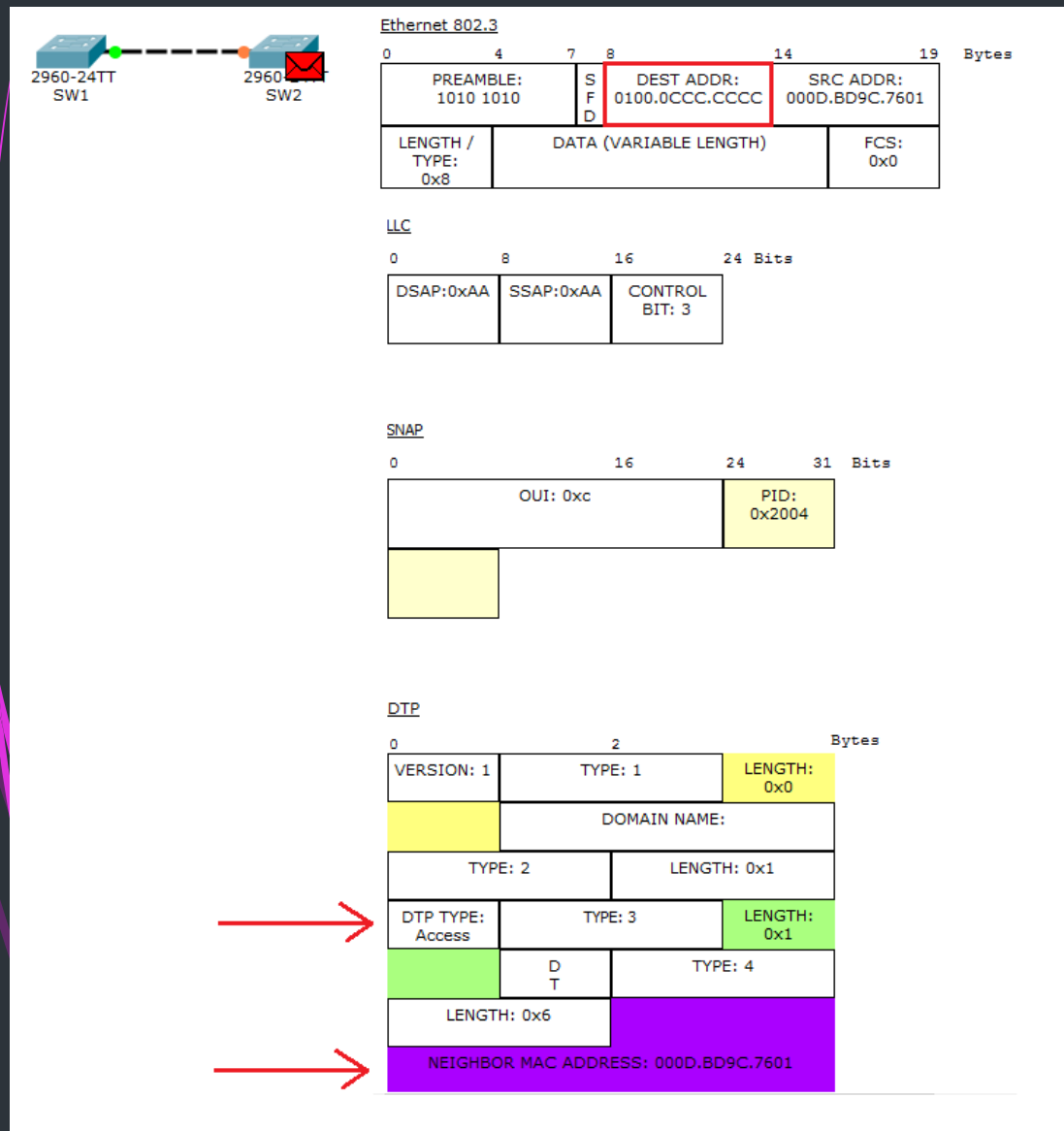


Проверим командой **show interfaces switchport**.

```
SW1#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

**Administrative Mode** - эта строка показывает, в каком из 4-режимов работает данный порт на коммутаторе. Убеждаемся, что на обоих коммутаторах порты в режиме «Dynamic auto». А строка **Operational Mode** показывает, в каком режиме работы они согласовали работу. Мы пока их не соединяли, поэтому они в состоянии «down».

Соединяем коммутаторы кабелем и, при поднятии линков, один из коммутаторов генерирует DTP-сообщение.



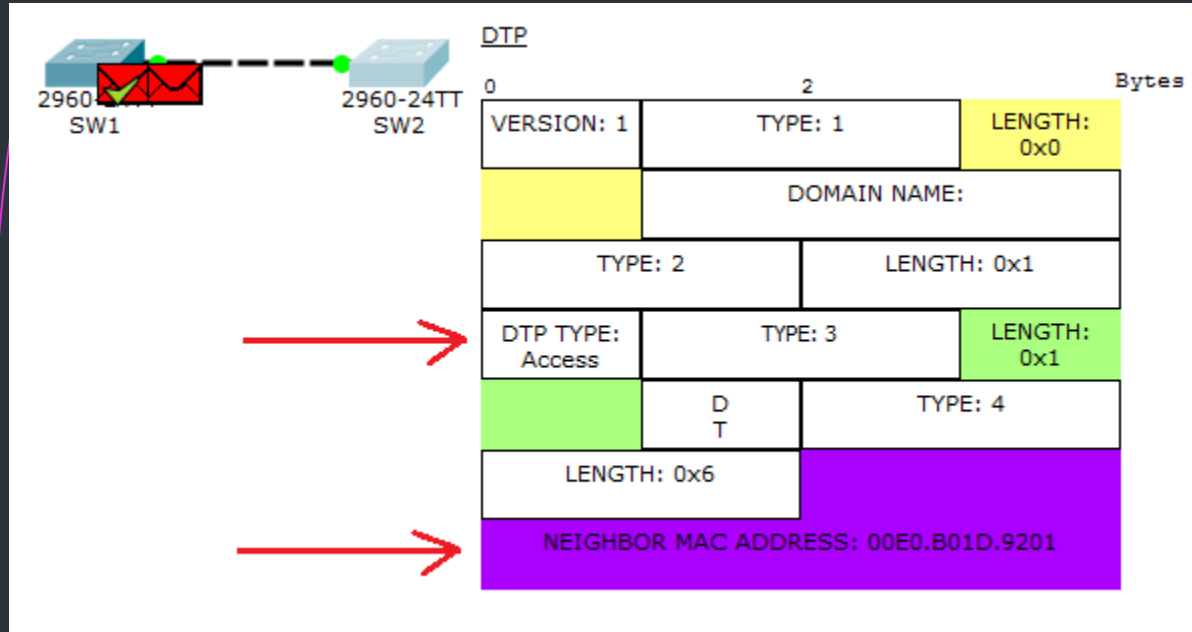
Видим, что это DTP инкапсулированный в Ethernet-кадр. Отправляет он его на мультикастовый адрес «0100.0ccc.cccc», который относится к протоколам DTP, VTP, CDP.

Обращаем внимание на 2 поля в заголовке DTP.

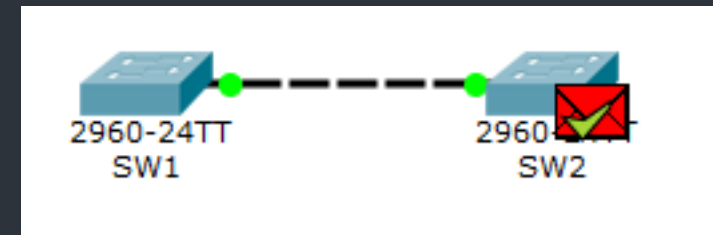
1) **DTP Type** — сюда отправляющий вставляет предложение. То есть в какой режим он хочет согласоваться. В нашем случае он предлагает согласовать «access».

2) **Neighbor MAC-address** — в это поле он записывает MAC-адрес своего порта.

Отправляет он и ждет реакции от соседа.



Доходит до SW1 сообщение и он генерирует ответный. Где также согласует режим «access», вставляет свой MAC-адрес и отправляет в путь до SW2.



Успешно доходит DTP. По идее они должны были согласоваться в режиме «access». Проверям. Как и предполагалось, согласовались они в режим «access».

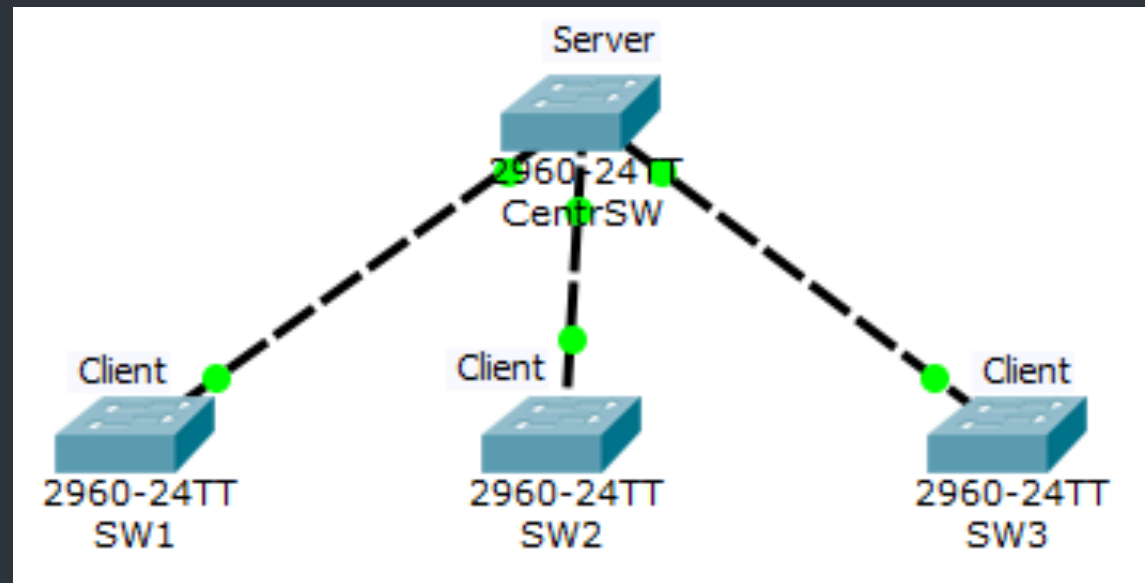
```
SW2#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```



# Протокол VTP

**VTP (англ. VLAN Trunking Protocol)** — проприетарный протокол компании Cisco, служащий для обмена информацией о VLAN-ах.

Представьте ситуацию, что у вас 40 коммутаторов и 70 VLAN-ов. По хорошему нужно вручную на каждом коммутаторе их создать и прописать на каких trunk портах разрешать передачу. Дело это муторное и долгое. Поэтому эту задачу может взять на себя VTP протокол. Вы создаете VLAN на одном коммутаторе, а все остальные синхронизируются с его базой.



Здесь присутствуют 4 коммутатора. Один из них является VTP-сервером, а 3 остальных клиентами. Те VLAN, которые будут созданы на сервере, автоматически синхронизируются на клиентах.  
Как работает VTP и что он умеет?

VTP может создавать, изменять и удалять VLAN. Каждое такое действие влечет к тому, что увеличивается номер ревизии (каждое действие увеличивает номер на +1). После он рассылает объявления, где указан номер ревизии. Клиенты, получившие это объявление, сравнивают свой номер ревизии с пришедшим. И если пришедший номер выше, они синхронизируют свою базу с ней. В противном случае объявление игнорируется.

# Роли протокола VTP

1. По-умолчанию все коммутаторы работают в роли сервера. Расскажу про них.

**VTP Server.** Умеет все. То есть создает, изменяет, удаляет VLAN. Если получает объявление, в которых ревизия старше его, то синхронизируется. Постоянно рассылает объявления и ретранслирует от соседей.

2. **VTP Client** — Эта роль уже ограничена. Создавать, изменять и удалять VLAN нельзя. Все VLAN получает и синхронизирует от сервера. Периодически сообщает соседям о своей базе VLAN-ов.

3. **VTP Transparent** — эта такая независимая роль. Может создавать, изменять и удалять VLAN только в своей базе. Никому ничего не навязывает и ни от кого не принимает. Если получает какое то объявление, передает дальше, но со своей базой не синхронизирует. Если в предыдущих ролях, при каждом изменении увеличивался номер ревизии, то в этом режиме номер ревизии всегда равен 0.

# Практика работы с VTP

Проверим, что центральный коммутатор в режиме Server.

Вводим команду **show vtp status**.

```
CentrSW#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode         : Server
VTP Domain Name            :
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MDS digest                 : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

Видим, что VTP Operating Mode: Server. Также можно заметить, что версия VTP 2-ая. К сожалению, в СРТ 3-ья версия не поддерживается. Версия ревизии нулевая.

Теперь настроим нижние коммутаторы.

```
SW1(config)#vtp mode client
```

```
Setting device to VTP CLIENT mode.
```

Видим сообщение, что устройство перешло в клиентский режим. Остальные настраиваются точно также.

Чтобы устройства смогли обмениваться объявлениями, они должны находиться в одном домене. Причем тут есть особенность. Если устройство (в режиме Server или Client) не состоит ни в одном домене, то при первом полученном объявлении, перейдет в объявленный домен. Если же клиент состоит в каком то домене, то принимать объявления от других доменов не будет. Откроем SW1 и убедимся, что он не состоит ни в одном домене.

```
SW1#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode         : Client
VTP Domain Name            : 
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Убеждаемся, что тут пусто.

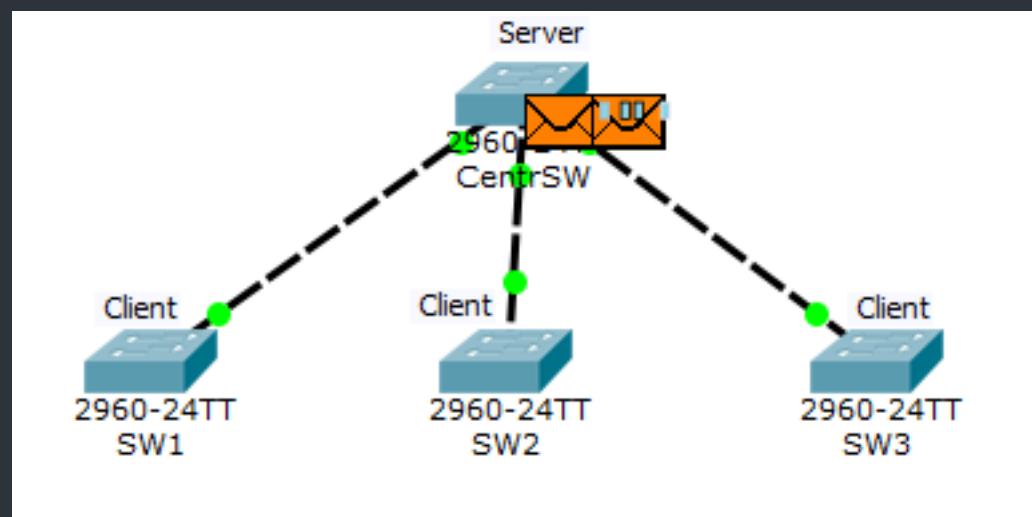
Теперь переходим центральному коммутатору и переведем его в домен.

```
CentrSW(config)#vtp domain cisadmin.ru
Changing VTP domain name from NULL to cisadmin.ru
```

Видим сообщение, что он перевелся в домен cisadmin.ru.  
Проверим статус.

```
CentrSW#sh
CentrSW#show vtp s
VTP Version           : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode    : Server
VTP Domain Name      : cisadmin.ru
VTP Pruning Mode     : Disabled
VTP V2 Mode          : Disabled
VTP Traps Generation : Disabled
MD5 digest           : 0xA4 0xF7 0xDE 0x24 0x07 0x3D 0x91 0xD2
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

И действительно. Имя домена изменилось. Обратите внимание, что номер ревизии пока что нулевой. Он изменится, как только мы создадим на нем VLAN. Но перед созданием надо перевести симулятор в режим *simulation*, чтобы посмотреть как он сгенерирует объявления.  
Создаем 20-ый VLAN и видим следующую картинку.



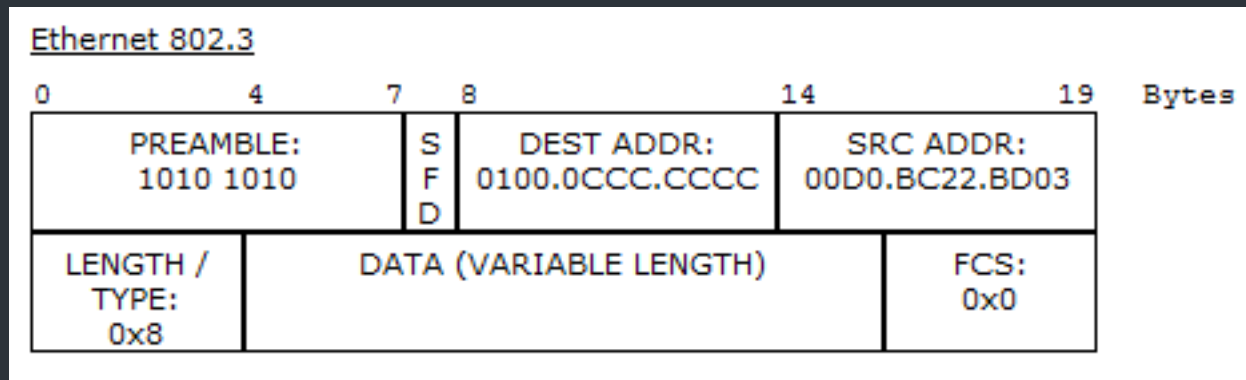
Как только создан VLAN и увеличился номер ревизии, сервер генерирует объявления. У него их два.

Сначала откроем тот, что левее. Это объявление называется «Summary Advertisement» или на русском «сводное объявление».

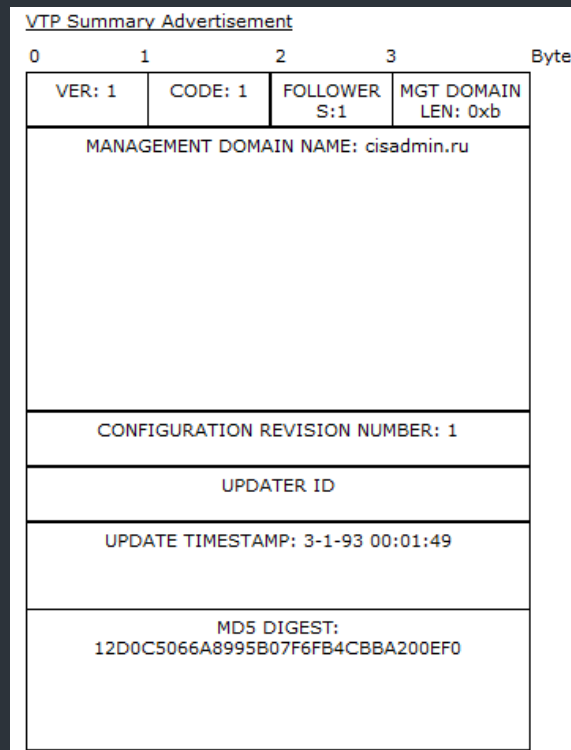
Это объявление генерируется коммутатором раз в 5 минут, где он рассказывает о имени домена и текущей ревизии.

Смотрим как выглядит.





В Ethernet-кадре обратите внимание на Destination MAC-адрес. Он такой же, как и выше, когда генерировался DTP. То есть, в нашем случае на него отреагируют только те, у кого запущен VTP. Теперь посмотрим на следующее поле.



- **Management Domain Name** — имя самого домена (в данном случае cisadmin.ru).
- **Updater Identity** — идентификатор того, кто обновляет. Здесь, как правило, записывается IP-адрес. Но так как адрес коммутатору не присваивали, то поле пустое
- **Update Timestamp** — время обновления. Время на коммутаторе не менялось, поэтому там стоит заводское.
- **MD5 Digest** — хеш MD5. Оно используется для проверки полномочий. То есть, если на VTP стоит пароль. Мы пароль не меняли, поэтому хэш по-умолчанию.

Теперь посмотрим на следующее генерируемое сообщение (то, что справа). Оно называется «Subset Advertisement» или «подробное объявление». Это такая подробная информация о каждом передаваемом VLAN

VTP Subset Advertisement				
0		2		Bytes
VER: 1	CODE: 2	SEQUENCE NUM:1	MGT DOMAIN LEN: 0xb	
MANAGEMENT DOMAIN NAME: cisadmin.ru				
CONFIGURATION REVISION NUMBER				

VTP VLAN Information				
0		2		Bytes
VLAN INFO LEN	STATUS: 0	VLAN TYPE: 1	VLAN NAME LEN: 0x7	
VLAN ID: 0x1		MTU SIZE: 0x13		
802.10 INDEX				
VLAN NAME: default				

VTP VLAN Information				
0		2		Bytes
VLAN INFO LEN	STATUS: 0	VLAN TYPE: 1	VLAN NAME LEN: 0x8	
VLAN ID: 0x14		MTU SIZE: 0x14		
802.10 INDEX				
VLAN NAME: VLAN0020				

Отдельный заголовок для каждого типа VLAN. Список настолько длинный, что не поместился в экран. Но они точно такие, за исключением названий.

Получают клиенты объявления. Видят, что номер ревизии выше, чем у них и синхронизируют базу. И отправляют сообщение серверу о том, что база VLAN-ов изменилась.

