Устранение неполадок протокола магистральных каналов VLAN (VTP)

Содержание

Введение

В этом документе представлена информация по устранению неполадок протокола VTP (VLAN Trunk Protocol).

Предварительные условия

Требования

Для данного документа нет особых требований.

Используемые компоненты

Этот документ не ограничен специфическими версиями оборудования и программного обеспечения.

Условные обозначения

Более подробные сведения о применяемых в документе обозначениях см. в статье Условные обозначения, используемые в технической документации Cisco.

Общие сведения о VTP

Дополнительную информацию по VTP см. в Общие сведения о протоколе VTP.

Настройка VTP

Для получения дополнительной информации по настройке VTP см. Настройка магистральных каналов VLAN (VTP).

Предупреждения о неполадках, связанных с протоколом VTP, и их устранение

В данном разделе описаны некоторые стандартные способы устранения неисправностей VTP.

В выходных данных команды show run не отображается подробная информация о VLAN

Изменения конфигурации, вносимые в CatOS, записываются в энергонезависимое ПЗУ сразу после внесения этих изменений. В противоположность этому, ПО Cisco IOS® не сохраняет изменения конфигурации в энергонезависимом ПЗУ до тех пор, пока не будет введена команда **copy running-config startup-config**. Системам клиентов и серверов VTP необходимо немедленное сохранение обновлений с серверов VTP в энергонезависимое ПЗУ без вмешательства пользователя. Требования к обновлению VTP удовлетворяются в случае, когда CatOS работает в режиме, заданном по умолчанию, однако, для модели обновления Cisco IOS требуется альтернативный режим работы обновления.

В качестве способа немедленного сохранения обновлений для клиентов и серверов VTP в ПО Cisco IOS встроена база данных VLAN. В некоторых версиях ПО эта база данных VLAN хранится в энергонезависимом ПЗУ в виде отдельного файла с именем vlan.dat. Увидеть информацию VTP/VLAN, касающуюся VTP-клиента или VTP-сервера и хранящуюся в файле vlan.dat, можно при помощи команды **show vtp status**.

При вводе команды **copy running-config startup-config** коммутаторы, работающие в режимах сервера/клиента VTP, не сохраняют в файле загрузочной конфигурации в энергонезависимом ПЗУ полную конфигурацию VTP/VLAN. Они сохраняют конфигурацию в файл vlan.dat. Это не относится к системам, работающим в прозрачном режиме VTP. При вводе команды **copy running-config startup-config** системы, работающие в прозрачном режиме VTP, сохраняют в файл загрузочной конфигурации в энергонезависимом ПЗУ полную конфигурацию VTP/VLAN. Например, при удалении файла vlan.dat после настройки VTP в режиме сервера или режиме клиента и последующей перезагрузке коммутатора, он установит для конфигурации VTP настройки по умолчанию. Однако при настройке VTP в прозрачном режиме, файл vlan.dat удаляется и коммутатор будет перезагружен. При этом будет сохранена конфигурация VTP.

Это пример конфигурации VTP, устанавливаемой по умолчанию.

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CISCO
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xD3 0x78 0x41 0xC8 0x35 0x56 0x89 0x97
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Когда коммутатор находится в режиме сервера или прозрачном режиме VTP можно настроить VLAN из стандартного диапазона (от 2 до 1000). Однако в коммутаторах, работающих в прозрачном режиме VTP, можно настроить только VLAN с поддержкой расширенного диапазона (от 1024 до 4094).

- Для отображения всех настроек VLAN, идентификатора VLAN, имени и другой информации, которая хранится в двоичном файле, необходимо ввести команду **show vlan**.
- Информацию о VTP, режим, домен и другую информацию можно отобразить при помощи команды **show vtp status**.
- Когда коммутатор находится в режиме сервера/клиента VTP, в выходных данных команды **show running-config** информация о VLAN и информация о VTP не отображается. Это стандартное поведение коммутатора.

```
Router#show run | include vlan
vlan internal allocation policy ascending
```

```
Router#show run | include vtp
```

- Когда коммутатор находится в прозрачном режиме VTP, в выходных данных команды **show running-config** отображается информация о VLAN и информация о VTP, поскольку эта информация также хранится в текстовом файле конфигурации.

```
Router#show run | include vlan
vlan internal allocation policy ascending
vlan 1
tb-vlan1 1002
tb-vlan2 1003
vlan 20-21,50-51
vlan 1002
tb-vlan1 1
tb-vlan2 1003
vlan 1003
tb-vlan1 1
tb-vlan2 1002
vlan 1004
vlan 1005
Router#show run | include vtp
vtp domain cisco
vtp mode transparent
```

Примечание. Сети VLAN расширенного диапазона не поддерживаются 3500XL. 2900XL и 3500XL могут использовать только VLAN в диапазоне от 1 до 1001. Они не поддерживают сети VLAN расширенного диапазона. При обновлении программного обеспечения коммутатора не будет реализована поддержка настройки сетей VLAN расширенного диапазона.

Коммутаторы Catalyst не обмениваются информацией VTP

VTP позволяет коммутаторам обмениваться информацией о VLAN с другими участниками одного и того же домена VTP. VTP позволяет организовать у всех коммутаторов согласующееся представление о коммутируемой сети. Существует несколько причин, по которым обмен информацией о VLAN может не осуществляться.

Если коммутаторы, работающие с VTP, не могут обмениваться информацией о VLAN, проверьте следующее:

- Информация VTP проходит только через магистральный порт. Проверьте, чтобы все порты, соединяющие коммутаторы, настроены в качестве магистральных, в действительности являются магистральными.

  Убедитесь, что каналы EtherChannel созданы между двумя коммутаторами; только каналы EtherChannel уровня 2 передают информацию о VLAN.
- Убедитесь в том, что VLAN активны на всех устройствах.
- В домене VTP по крайней мере один из коммутаторов должен быть сервером VTP. Чтобы все изменения VLAN были переданы клиентам VTP, такие изменения должны вноситься на этом коммутаторе.
- Доменные имена VTP чувствительны к регистру, они должны совпадать. CISCO и cisco - это два различных имени доменов.
- Проверьте, чтобы между сервером и клиентом не было установлено паролей. Если установлены какие-либо пароли, проверьте,

чтобы они совпадали с обеих сторон.

- На всех коммутаторах в домене VTP должна использоваться одинаковая версия VTP. VTP V1 и VTP V2 несовместимы на коммутаторах в одном домене VTP. Не включайте VTP V2, если не все коммутаторы в домене VTP поддерживают V2.

  Примечание. По умолчанию в коммутаторах, поддерживающих протокол VTP V2, он отключен. При включении VTP V2 в одном коммутаторе, V2 включается во всех коммутаторах домена VTP, поддерживающих V2. Версию можно настраивать только на коммутаторах, работающих в режиме сервера или прозрачном режиме VTP.

- Если коммутаторы, работающие в прозрачном режиме, находятся в другом домене VTP, то они отбрасывают объявления VTP. Коммутатор, работающий в прозрачном режиме VTP и использующий VTP V2, передает все сообщения VTP вне зависимости от указанного домена VTP. Однако коммутатор с VTP V1 передает только сообщения VTP с доменом VTP, совпадающим с доменом, настроенным на локальном коммутаторе.

- VLAN из расширенного диапазона не передаются. Поэтому VLAN из расширенного диапазона необходимо настраивать вручную на всех сетевых устройствах.

  Примечание. В будущем ПО Cisco IOS коммутаторов Catalyst 6500 будет поддерживать VTP версии 3. Данная версия может передавать VLAN из расширенного диапазона. К настоящему моменту VTP версии 3 поддерживается только в CatOS. Дополнительную информацию по VTP версии 3 см. в разделе *Принципы работы протокола VTP версии 3* документа Настройка протокола VTP.

- Значения идентификаторов сопоставления безопасности (SAID) должны совпадать. SAID – это настраиваемый пользователем 4-байтный идентификатор VLAN. SAID идентифицирует трафик, принадлежащий определенной VLAN. SAID также определяет, в какую VLAN какой пакет коммутируется. Значение SAID равно 100 000 плюс номер VLAN. Ниже приведены два примера:

  - Значение SAID для VLAN 8 равно 100008.
  - Значение SAID для VLAN 4050 равно 104050.

- Обновления с сервера VTP не применяются на клиенте, если он содержит большее значение версии VTP. Если клиент содержит большее значение версии VTP, чем посылаемое сервером VTP, он не допускает передачу этих обновлений на клиенты, подключенные в каскаде после него.

Коммутаторы Catalyst автоматически переключаются из режима клиента VTP в прозрачный режим VTP

Некоторые коммутаторы Catalyst уровня 2 и уровня 3 с фиксированной конфигурацией автоматически переключаются из режима клиента VTP в прозрачный режим VTP, выдавая следующее сообщение об ошибке:

```
%SW_VLAN-6-VTP_MODE_CHANGE: VLAN manager changing device mode from
CLIENT to TRANSPARENT.
```

Любая из следующих двух причин может привести к автоматическому переключению режима VTP в этих коммутаторах:

- **Протокол связующего дерева (STP) обслуживает больше локальных сетей, чем может поддерживать коммутатор.**

  Коммутаторы Catalyst уровня 2 и уровня 3 с фиксированной конфигурацией поддерживают различное максимальное количество экземпляров STP с использованием протокола per-VLAN spanning tree+ (PVST+). Например, Catalyst 2940 в режиме PVST+ поддерживает четыре экземпляра STP, тогда как Catalyst 3750 в режиме PVST+ поддерживает 128 экземпляров STP. Если в VTP определено больше максимального количества виртуальных сетей, остальные VLAN работают без поддержки STP.

  Если количество используемых экземпляров STP превышает максимальное количество, можно отключить протокол STP в одной из виртуальных сетей и включить его в той сети, в которой вам нужно. Для отключения STP в определенной VLAN введите команду глобальной настройки **no spanning-tree vlan *vlan-id***. После этого для включения STP в определенной VLAN введите команду глобальной настройки **spanning-tree vlan *vlan-id***.

  Примечание. Коммутаторы, на которых STP не работает, продолжают пересылать получаемые ими сообщения протокола моста (BPDU). При этом другие коммутаторы в виртуальной сети, в которой работает экземпляр STP, могут разрывать петли. Поэтому для разрыва всех петель в сети протокол STP должен работать на достаточном количестве коммутаторов. Например, как минимум на одном коммутаторе в каждой петле VLAN должен работать протокол STP. Нет необходимости в запуске STP на всех коммутаторах виртуальной сети. Однако при запуске STP на минимальном количестве коммутаторов любое изменение в сети может привести к образованию петли и распространению широковещательного шторма.

Обходные пути:

- Уменьшите количество настроенных VLAN до количества, поддерживаемого коммутаторами.
- Чтобы преобразовать несколько VLAN в один экземпляр STP, настройте на коммутаторе протокол множественного STP (MSTP), соответствующий стандарту IEEE 802.1s.
- Используйте коммутаторы и/или образы (усовершенствованные образы [EI]), поддерживающие большее количество VLAN.

- **Коммутатор получает от соединенного с ним коммутатора больше VLAN, чем способен поддерживать.**

  Если коммутатор получает сообщение базы данных конфигурации VLAN, в котором содержится количество VLAN, превышающее заданное значение, при этом также может быть выполнено автоматическое переключение режима VTP. Обычно это имеет место в коммутаторах Catalyst уровня 2 и уровня 3 с фиксированной конфигурацией, когда они подключены к домену VTP, в котором количество виртуальных сетей превышает локально поддерживаемое количество сетей.

  Обходные пути:

  - Для ограничения количества VLAN, передаваемых коммутатору-клиенту, настройте список разрешенных VLAN на магистральном порту подключенного коммутатора.
  - Включите отсечение каналов на коммутаторе, работающем в качестве сервера VTP.
  - Используйте коммутаторы и/или образы (EI), поддерживающие большее количество VLAN.

Блокирование трафика между доменами VTP

Иногда возникает необходимость подключения к коммутаторам, принадлежащим к различным доменам VTP. Например, есть два коммутатора Switch1 и Switch2. Switch1 относится к домену VTP cisco1, а Switch2 относится к домену VTP cisco2. При настройке магистрали между этими двумя коммутаторами при помощи протокола согласования динамической магистрали (DTP) согласование магистрали не выполняется и магистраль между коммутаторами не формируется, поскольку протокол DTP передает в пакете DTP имя домена VTP. По этой причине обмена трафиком между коммутаторами не происходит.

```
Switch1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
VTP Operating Mode              : Server
VTP Domain Name                 : cisco1
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled

Switch2#show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 42
VTP Operating Mode              : Server
VTP Domain Name                 : cisco2
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled


Switch1#show interface fastethernet 1/0/23 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa1/0/23    auto         802.1q         not-trunking  1

Port      Vlans allowed on trunk
Fa1/0/23    1

Port        Vlans allowed and active in management domain
Fa1/0/23    1

Port        Vlans in spanning tree forwarding state and not pruned
Fa1/0/23    1
```

Также можно увидеть следующее сообщение об ошибке.

Примечание. Некоторые коммутаторы не отображают это сообщение об ошибке.

```
4w2d: %DTP-SP-5-DOMAINMISMATCH: Unable to perform trunk negotiation on port Fa3/
3 because of VTP domain mismatch.
```

Решение данного вопроса заключается в ручной настройке магистрали вместо ее настройки с использованием DTP. Настройте магистральные порты между коммутаторами при помощи команды **switchport mode trunk**.

```
Switch1(config)#interface fastethernet 1/0/23
switch1(config-if)#switchport mode trunk

Switch2(config)#interface fastethernet 3/3
switch2(config-if)#switchport mode trunk


switch1#show interface fastethernet 1/0/23 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa1/0/23    on           802.1q         trunking      1

Port      Vlans allowed on trunk
Fa1/0/23    1-4094

Port        Vlans allowed and active in management domain
Fa1/0/23    1-5

Port        Vlans in spanning tree forwarding state and not pruned
Fa1/0/23    1-5
```

Изменения коммутатора CarOS в прозрачном режиме VTP, VTP-4-UNSUPPORTEDCFGRCVD:

Недавно в CatOS была встроена защитная функция, работа которой приводит к тому, что коммутатор с CatOS переключается в прозрачный режим VTP для предотвращения возможной перезагрузки коммутатора в результате превышения времени ожидания контрольного таймера. Это изменение описано в следующих идентификаторах ошибок Cisco:

- CSCdt80707 (только для зарегистрированных клиентов)
- CSCdv77448 (только для зарегистрированных клиентов)

Как определить наличие этой ошибки в коммутаторе?

Превышение времени ожидания контрольного таймера может происходить при выполнении следующих двух условий:

- Token Ring VLAN (1003) преобразуется в VLAN 1.
- В VLAN 1 вносятся изменения.

Чтобы просмотреть преобразование Token Ring в VLAN, введите в Catalyst команду **show vlan**. Ниже приведен пример выходных данных команды **show vlan**:

```
VLAN Type  SAID       MTU   Parent RingNo BrdgNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ ------ ---- -------- ------ ------
1    enet  100001     1500  -      -      -      -    -        1003
```

Как CatOS Release 6.3(3) защищает коммутатор от превышения времени ожидания контрольного таймера?

Наличие защитной функции позволяет предотвратить превышение времени ожидания в данной версии CatOS. Коммутатор Catalyst переключается из режима сервера/клиента VTP в прозрачный режим VTP.

Как определить, что коммутатор переключился в прозрачный режим VTP для защиты от превышения времени ожидания контрольного таймера?

Коммутатор перешел в прозрачный режим протокола VTP, если уровень регистрации для VTP повысился до 4.

```
Console> (enable) set logging level vtp 4 default
```

Когда происходит переключение, выводится следующее сообщение:

```
VTP-4-UNSUPPORTEDCFGRCVD:Rcvd VTP advert with unsupported vlan config on
trunk mod/port- VTP mode changed to transparent
```

Какие отрицательные последствия влечет переключение коммутатора в прозрачный режим VTP?

- Если отсечение включено, каналы связи ухудшаются.
- Если магистрали отключаются и в этой виртуальной сети нет других портов, то интерфейс VLAN в установленной плате многоуровневой коммутации (MSFC) также отключается.

Если это имеет место, а данный коммутатор находится в центре сети, в таком случае производительность сети может понизиться.

Что является источником неподдерживаемой конфигурации VTP?

Любой коммутатор из приведенного списка, работающий под управлением ПО Cisco IOS, может привести к созданию неподдерживаемой конфигурации VTP:

- Catalyst 2900/3500XL
- Catalyst 6500 с ПО Cisco IOS
- Catalyst 4000 с ПО Cisco IOS

Эти продукты по умолчанию преобразуют 1003 VLAN в VLAN 1.

В чем состоит решение?

Решение для коммутаторов на основе CatOS позволяет коммутаторам правильно обрабатывать преобразованные данные. Решение для коммутаторов, работающих под управлением программного обеспечения Cisco IOS, заключается в том, чтобы удалить это преобразование по умолчанию и сделать так, чтобы они работали аналогично коммутаторам под управлением CatOS. В настоящий момент доступны следующие объединенные версии с исправлениями:

Коммутатор Catalyst	Исправленные версии
	5.5(14) и более поздние версии

Коммутаторы CatOS	6.3(6) и более поздние версии 7.2(2) и более поздние версии
Catalyst 4000 (Supervisor Engine III)	Не затронуты
Catalyst 6500 (Supervisor Engine ПО Cisco IOS)	Программное обеспечение Cisco IOS Release 12.1(8a)EX и более новые версии
Catalyst 2900 и 3500XL	Программное обеспечение Cisco IOS 12.0(5)WC3 и более новые версии

Если невозможно выполнить обновление с использованием исправленных образов, в коммутаторах, работающих под управлением ПО Cisco IOS, можно исправить конфигурацию. Если коммутатор является сервером VTP, выполните следующие действия:

```
goss#vlan data

goss(vlan)#no vlan 1 tb-vlan1 tb-vlan2

Resetting translation bridge VLAN 1 to default
Resetting translation bridge VLAN 2 to default

goss(vlan)#no vlan 1003 tb-vlan1 tb-vlan2

Resetting translation bridge VLAN 1 to default
Resetting translation bridge VLAN 2 to default

goss(vlan)#apply

APPLY completed.

goss(vlan)#exit

APPLY completed.
Exiting....
```

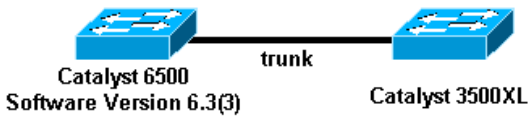
Преобразование сети 1002 VLAN может выполняться, однако при добавлении в конфигурацию следующих настроек ее можно удалить:

```
goss(vlan)#no vlan 1002 tb-vlan1 tb-vlan2

Resetting translation bridge VLAN 1 to default
Resetting translation bridge VLAN 2 to default
```

При каких условиях коммутатор обязательно перейдет в прозрачный режим VTP?

Существует некоторая путаница относительно того, когда происходит переключение в прозрачный режим VTP. Следующие сценарии описывают условия, при которых может произойти переключение:



- **Пример 1**

Исходные условия:

- Catalyst 6500 и Catalyst 3500XL являются серверами VTP с одинаковыми номерами версий конфигурации VTP;
- Оба сервера имеют одинаковое имя домена VTP и пароль VTP (если пароль был задан).
- В Catalyst 3500XL выполняется преобразование Token Ring в VLAN;
- Серверы запускаются, будучи отключенными друг от друга.

Если их соединить, Catalyst 6500 переходит в прозрачный режим VTP. Конечно, это также происходит, если номер версии конфигурации протокола VTP у Cisco 3500XL выше, чем номер версии конфигурации Catalyst 6500. Кроме того, если при физическом подключении происходит переключение в прозрачный режим VTP, то следует предположить, что это произойдет также при первой загрузке уже подключенного коммутатора Catalyst 6500.

- **Пример 2**

  Исходные условия:

  - Catalyst 6500 является сервером VTP.
  - Catalyst 3500XL является клиентом VTP;
  - У Catalyst 3500XL номер версии конфигурации VTP больше номера версии конфигурации Catalyst 6500;
  - Оба коммутатора используют одинаковые домен и пароль VTP (если таковой пароль установлен).
  - В Catalyst 3500XL выполняется преобразование Token Ring в VLAN;
  - Серверы запускаются, будучи отключенными друг от друга.

  Если их соединить, Catalyst 6500 переходит в прозрачный режим VTP. В случае такого сценария, если номер версии конфигурации Catalyst 3500XL меньше номера версии конфигурации Catalyst 6500, Catalyst 6500 не переключается в прозрачный режим VTP. Если номер версии конфигурации Catalyst 3500XL совпадает с номером версии конфигурации Catalyst 6500, последний не переключается в прозрачный режим VTP. Однако преобразование в Catalyst 3500XL продолжает выполняться.

Какой способ устранения проблем после обнаружения преобразования в сети является самым быстрым?

Даже после исправления информации для преобразования Token Ring в VLAN в одном коммутаторе, поскольку коммутатор работал неправильно, информация могла распространиться по сети. Чтобы определить, произошло ли это, можно воспользоваться командой **show vlan**. При этом самым быстрым способом устранения неисправностей является следующее:

1. Переключите подключенный к сети коммутатор, работающий под управлением ПО Cisco IOS, например, Catalyst XL, в режим сервера VTP.
2. Удалите преобразуемые виртуальные сети.
3. После применения изменений в коммутаторе подключите его к сети.

   Изменения должны распространиться на остальные серверы и клиенты VTP.

   Для проверки прекращения преобразования в сети воспользуйтесь командой **show vlan**. Теперь затронутый коммутатор с CatOS 6.3(3) можно снова сделать сервером VTP.

   Примечание. Коммутаторы Catalyst XL поддерживает меньше виртуальных сетей, чем Catalyst 6500s. Перед подключением коммутаторов Catalyst XL проверьте, чтобы в них были все виртуальные сети, которые есть в Catalyst 6500. Например, не стоит подключать Catalyst 3548 XL, в котором настроено 254 VLAN, и больший номер версии конфигурации VTP к Catalyst 6500, в котором настроено 500 VLAN.

Как добавленный коммутатор может привести к проблемам в сети

Примечание. См. раздел *Флэш-анимация: VTP* в разделе Общие сведения о протоколе VLAN (VTP) для получения демонстрационного флэш-ролика с решением данной проблемы.

Эта проблема возникает в случае, когда при наличии большого коммутируемого домена, целиком входящего в домен VTP, требуется добавить в сеть один коммутатор.

Этот коммутатор раньше использовался в лаборатории, и было введено правильное имя домена VTP. Он был настроен как клиент VTP и подключен к остальной части сети. Затем для остальной сети организовывается канал ISL. Всего через несколько секунд нарушается работа всей сети. Почему это происходит?

Номер версии конфигурации на добавленном коммутаторе был больше, чем номер версии конфигурации домена VTP. Поэтому при добавлении коммутатора, в котором практически не было настроенных виртуальных сетей, произошло удаление всех виртуальных сетей домена VTP.

Это происходит, если коммутатор является либо клиентом VTP, либо сервером VTP. Клиент VTP может удалять информацию о VLAN на сервере VTP. Можно сказать, что это происходит, когда многие из портов сети переходят в неактивное состояние, но по-прежнему остаются назначенными несуществующей VLAN.

Решение

Быстро перенастройте все VLAN на одном из VTP-серверов.

Что следует запомнить

Всегда проверяйте, чтобы номера версий конфигураций всех коммутаторов, добавляемых в домен VTP, были меньше номеров версий конфигураций коммутаторов, уже имеющихся в домене VTP.

При наличии выходных данных после выполнения в устройстве Cisco команды **show-tech support** для отображения потенциальных проблем и исправлений можно использовать Интерпретатор выходных данных (только для зарегистрированных клиентов).

Пример

Чтобы ознакомиться с примером данной проблемы, проделайте следующие действия:

1. Введите следующие команды, чтобы узнать, что у сервера clic имеется 7 виртуальных сетей (1, 2, 3 и сети, настроенные по умолчанию), clic является сервером VTP в домене с именем test, а порт 2/3 принадлежит VLAN 3:

```
clic (enable) show vlan

1993 May 25 05:09:50 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1 lan
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
1    default                          active    65      2/2,2/4-50
2    VLAN0002                         active    70
3    VLAN0003                         active    71      2/3
1002 fddi-default                     active    66
1003 token-ring-default               active    69
1004 fddinet-default                  active    67
1005 trnet-default                    active    68      68

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
7          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000

clic (enable) show port 2/3

Port  Name               Status     Vlan       Level  Duplex Speed Type
```

```
----- ------------------ ---------- ---------- ------ ------ ----- ------------
2/3                     connected 3          normal   10  half 10/100BaseTX
```

2. Подключите bing (тестовый коммутатор, на котором были созданы VLAN 4, 5 и 6).

   Примечание. На этом коммутаторе используется версия конфигурации с номером 3.

```
bing (enable) show vlan

VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
1    default                          active    4       2/1-48
                                                       3/1-6
4    VLAN0004                         active    63
5    VLAN0005                         active    64
6    VLAN0006                         active    65
1002 fddi-default                     active    5
1003 token-ring-default               active    8
1004 fddinet-default                  active    6
1005 trnet-default                    active    7
```

3. Добавьте коммутатор bing в тот же домен VTP (test).

```
bing (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
8          1023             3               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
10.200.8.38     disabled disabled 2-1000
```

4. Чтобы встроить bing в сеть, настройте между двумя коммутаторами магистраль.

   Bing удалил виртуальные сети clic, и теперь у clic настроены VLAN 4, 5 и 6. Однако в нем нет VLAN 2 и 3, а порт 2/3, неактивен.

```
clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
8          1023             3               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
10.200.8.38     disabled disabled 2-1000
clic (enable)

clic (enable) show vlan

VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- ------------------------
1    default                          active    65      2/2,2/4-50
4    VLAN0004                         active    72
5    VLAN0005                         active    73
6    VLAN0006                         active    74
1002 fddi-default                     active    66
1003 token-ring-default               active    69
1004 fddinet-default                  active    67
1005 trnet-default                    active    68      68

clic (enable) show port 2/3

Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
2/3                     inactive   3          normal   auto  auto 10/100BaseTX
```

Недавно добавленный коммутатор не получает сети VLAN с сервера VTP

Убедитесь, что номер версии конфигурации недавно добавленного коммутатора меньше текущего номера домена. Для получения дополнительной информации см. разделы Как добавленный коммутатор может привести к проблемам в сети и Сброс номера версии конфигурации.

Новый коммутатор не может в данный момент получить список сконфигурированных VLAN с VTP-сервера. Чтобы устранить данную ситуацию выполните следующие модификации с базой данных VLAN.

- Создайте сеть VLAN.
- Удалите сеть VLAN.
- Измените свойства текущей сети VLAN.

Внесите изменения в базу данных VLAN на любом VTP-сервере в одном и том же домене.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 50

Switch(config-vlan)#name 50thVLAN

Switch(config-vlan)#end
Switch#
```

После завершения внесения изменений новый добавленный коммутатор получит информацию о сети VLAN от VTP-сервера.

Сброс номера версии конфигурации

Номер версии конфигурации можно сбросить любым из двух способов, описанных в данном разделе.

Сброс номера версии конфигурации с использованием имени домена

Чтобы номер версии конфигурации при изменении имени домена был сброшен, выполните следующие действия.

1. Чтобы убедиться в том, что конфигурация пуста, введите следующую команду.

```
clic (enable) show vtp domain

Domain Name                      Domain Index VTP Version Local Mode  Password
-------------------------------- ------------ ----------- ----------- ----------
                                 1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
5          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

2. Настройте имя домена (в данном примере это **test**) и создайте две сети VLAN.

Номер версии конфигурации увеличивается до 2:

```
clic (enable) set vtp domain test

VTP domain test modified

clic (enable) set vlan 2

Vlan 2 configuration successful

clic (enable) set vlan 3

Vlan 3 configuration successful

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
7          1023             2               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

3. Измените имя домена с test на cisco.

   Номер версии конфигурации снова равен 0, а все VLAN по-прежнему присутствуют:

```
clic (enable) set vtp domain cisco

VTP domain cisco modified

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
cisco                          1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
7          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
```

4. Измените имя домена VTP с cisco снова на test.

   Номер версии конфигурации равен 0. При этом нет опасности удалить что-либо, а все ранее настроенные VLAN сохраняются:

```
clic (enable) set vtp domain test

VTP domain test modified

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
7          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

Сброс версии конфигурации при помощи режима VTP

Чтобы сбросить номер версии конфигурации при изменении режима VTP, выполните следующие действия:

1. Чтобы убедиться в том, что конфигурация пуста, введите следующую команду.

```
clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
                               1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
5          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

2. Настройте имя домена (в данном примере это **test**) и создайте две сети VLAN.

   Номер версии конфигурации увеличивается до 2:

```
clic (enable) set vtp domain test

VTP domain test modified

clic (enable) set vlan 2

Vlan 2 configuration successful

clic (enable) set vlan 3

Vlan 3 configuration successful

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
7          1023             2               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

3. Измените режим сервера VTP на прозрачный режим VTP.

   Номер версии конфигурации снова равен 0, а все VLAN по-прежнему присутствуют:

```
clic (enable) set vtp mode transparent

VTP domain test modified

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           transparent -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
7          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
```

```
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
```

4. Измените прозрачный режим VTP на режим сервера или клиента VTP.

   Номер версии конфигурации равен 0. При этом нет опасности удалить что-либо, а все ранее настроенные VLAN сохраняются:

```
clic (enable) set vtp mode server

VTP domain test modified

clic (enable) show vtp domain

Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
test                           1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- -------------
7          1023             0               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
0.0.0.0         disabled disabled 2-1000
clic (enable)
```

После отключения и включения питания все порты неактивны

Порты коммутатора переходят в неактивное состояние, когда они являются участниками VLAN, не существующими в базе данных VLAN. Обычно переход всех портов в неактивное состояние происходит после выключения и включения питания. Обычно это наблюдается в случаях, когда коммутатор настроен в качестве клиента VTP с каскадным магистральным портом, включенным в сеть VLAN, отличную от VLAN 1. Поскольку коммутатор находится в режиме клиента VTP, при сбросе настроек коммутатора происходит потеря базы данных VLAN, в результате чего каскадный порт и все остальные порты, которые не принадлежали к VLAN 1, переходят в неактивное состояние.

Чтобы устранить данную проблему, выполните следующие действия.

1. Временно измените режим сервера VTP на прозрачный режим VTP.

```
switch (enable) set vtp mode transparent

VTP domain austinlab modified
switch (enable)
```

2. Добавьте в базу данных VLAN виртуальную сеть, которой назначен каскадный порт.

   Примечание. В данном примере предполагается, что каскадный порт назначен виртуальной сети VLAN 3.

```
switch (enable) set vlan 3

VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 3 configuration successful
switch (enable)
```

3. После того, как каскадный порт начнет пересылку, измените режим VTP обратно на режим клиента.

```
switch (enable) set vtp mode client

VTP domain austinlab modified
```

После выполнения этих действий VTP должен заново заполнить базу данных VLAN с сервера VTP. Повторное заполнение приводит к тому, что все порты, которые принадлежали сетям VLAN, объявленным сервером VTP, переходят в активное состояние.

Отключение магистрали вызывает проблемы VTP

Помните: пакеты VTP передаются в сети VLAN 1, но исключительно по магистралям (ISL, dot1q или по имитируемой LAN [LANE])

Если внести изменения в VLAN в то время, когда магистраль или подключение LANE между двумя сегментами сети неактивны, можно потерять конфигурацию VLAN. Когда магистральное соединение восстанавливается, две стороны сети повторно синхронизируются. Поэтому коммутатор с максимальным номером версии конфигурации стирает конфигурацию VLAN коммутатора с меньшим номером версии конфигурации.

VTP и STP (логический порт связующего дерева)

При наличии большого домена VTP домен STP также будет большим. VLAN1 должна охватывать весь домен VTP полностью. Таким образом, один уникальный STP используется для VLAN во всем домене.

Когда используется VTP и создается новая VLAN, последняя распространяется по всему домену VTP. На всех коммутаторах в домене VTP будет создана VLAN. Во всех коммутаторах Cisco используется PVST, а это означает то, что в коммутаторах для каждой VLAN работает отдельный экземпляр STP. Это приводит к увеличению загрузки ЦП коммутатора. Необходимо помнить о максимальном количестве логических портов (для STP), поддерживаемых коммутатором, чтобы знать количество STP, которое может работать на каждом из коммутаторов. Количество логических портов примерно равно количеству портов, на которых работает STP.

Примечание. На магистральном порту для каждой активной VLAN магистрали работает по одному экземпляру STP.

При помощи следующей формулы можно быстро оценить это количество для коммутатора:

```
(Number of active VLANs x Number of trunks) + Number of access ports
```

Это количество (максимальное количество логических портов для STP) зависит от коммутатора и указано в примечаниях к версии любого продукта. Например, на Catalyst 5000 с Supervisor Engine 2 может быть не более 1500 экземпляров STP. Всякий раз при создании новой VLAN при помощи VTP виртуальная сеть по умолчанию распространяется на все коммутаторы и в результате является активной на всех портах. Во избежание превышения количества логических портов может потребоваться отсечение ненужных сетей VLAN от магистрали.

Примечание. Отсечение ненужных VLAN от магистрали можно выполнить одним из двух способов.

- **Ручное отсечение ненужных VLAN от магистрали**. Это лучший способ, который не требует использования протокола связующего дерева. Наоборот, данный способ позволяет работать отсекаемым VLAN в магистралях. Подробное описание отсечения вручную содержится в разделе Процедура отсечения каналов в протоколе VTP.
- **Процедура отсечения каналов в протоколе VTP** - если необходимо уменьшить количество экземпляров STP, применение данного способа не рекомендуется. VLAN, отсеченные в магистрали при помощи VTP продолжают принадлежать связующему дереву. Поэтому при отсечении VLAN при помощи VTP количество экземпляров портов связующего дерева не уменьшается.

Процедура отсечения каналов в протоколе VTP

Отсечение каналов в протоколе VTP расширяет доступную полосу пропускания. Отсечение каналов в VTP ограничивает доступ лавинного трафика в магистрали, которые должны использоваться трафиком для доступа к соответствующим устройствам сети. По умолчанию отсечение каналов в протоколе VTP отключено. Включение отсечения каналов в протоколе VTP на сервере VTP позволяет выполнять отсечение во всем управляемом домене. Команда **set vtp pruning enable** автоматически отсекает VLAN и прекращает неэффективную передачу кадров туда, где они не нужны. По умолчанию отсечению подвергаются виртуальные сети с 1 по 1000. Отсечение каналов в протоколе VTP не влияет на трафик, идущий из виртуальных сетей, не подвергающихся отсечению. VLAN 1

никогда не подвергается отсечению; трафик из VLAN 1 отсекаться не может.

Примечание. В отличие от процедуры ручного отсечения VLAN, автоматическое отсечение не ограничивает диаметр связующего дерева.

Чтобы отсечение в протоколе VTP работало эффективно, все устройства в управляемом домене должны поддерживать отсечение в протоколе VTP. В устройствах, не поддерживающих отсечение в протоколе VTP, необходимо вручную настраивать виртуальные сети, у которых есть доступ к магистралям. При помощи команд **clear trunk *mod*/*port*** и **clear trunk *vlan_list*** можно вручную отсекать виртуальные сети от магистралей. Например, на каждом магистральном канале можно разрешить доступ центрального коммутатора только к действительно необходимым сетям VLAN. Это поможет снизить загрузку ЦП всех коммутаторов (центральных коммутаторов и коммутаторов доступа) и избежать использования STP для виртуальных сетей, охватывающих всю сеть. Такое отсечение сокращает количество проблем с STP в VLAN.

Ниже представлен пример:

- **Топология** - в топологии содержится два центральных коммутатора, соединенных друг с другом, у каждого из них по 80 магистральных подключений к 80 различным коммутаторам доступа. В данной конфигурации у каждого из центральных коммутаторов по 81 магистральному соединению и у каждого есть доступ к двум каскадным магистралям. Это предполагает, что у коммутаторов доступа кроме двух каскадных подключений есть два или три магистральных подключения к Catalyst 1900. Суммарно четыре-пять магистралей на ключ доступа.
- **Платформа** - функции центральных коммутаторов выполняют Catalyst 6500 с Supervisor Engine 1A и платами поддержки политик 1 (PFC1), работающие под управлением ПО Release 5.5(7). В соответствии с Примечаниями к версии 5.x программного обеспечения Catalyst 6000/6500, количество логических портов STP в данной платформе не может превышать 4000.
- **Коммутаторы доступа** - функции коммутаторов доступа выполняют:
    - Коммутаторы Catalyst 5000 с Supervisor Engine 2, поддерживающие не более 1500 логических портов STP.
    - Коммутаторы Catalyst 5000 с Supervisor Engine 1 и 20 Мб DRAM, поддерживающие не более 400 логических портов STP.
- **Количество VLAN** - следует помнить об использовании VTP. Виртуальная сеть, настроенная на сервере VTP, создается на всех коммутаторах сети. При наличии 100 VLAN центральный коммутатор должен обрабатывать около 100 VLAN x 81 магистраль = 8100 логических портов, что превышает предельное значение. Коммутатор доступа должен обрабатывать 100 VLAN x 5 магистралей = 500 логических портов. В данном случае количество логических портов для центральных коммутаторов Catalyst превышает поддерживаемое ими количество логических портов, так же как и в случае с коммутаторами доступа с Supervisor Engine 1.
- **Решение** - полагая, что в каждом из коммутаторов доступа действительно необходимы только четыре из пяти виртуальных сетей, можно отсечь все остальные виртуальные сети от магистрали центрального уровня. К примеру, если к магистрали 3/1, подключенной к коммутатору доступа, необходимо подключить сети VLAN 1, 10, 11 и 13, то конфигурация центрального коммутатора будет следующей:

```
Praha> (enable) set trunk 1/1 des

Port(s) 1/1 trunk mode set to desirable.

Praha> (enable) clear trunk 1/1 2-9,12,14-1005

Removing Vlan(s) 2-9,12,14-1005 from allowed list.
Port 1/1 allowed vlans modified to 1,10,11,13.

Praha> (enable) clear trunk 1/1 2-9,12,14-1005
```

Примечание. Даже если число допустимых логических портов не превышено, рекомендуется отсекать VLAN от магистрали. Причина заключается в том, что петля STP на одной VLAN распространяется только там, где разрешена VLAN, и не охватывает всю сеть. Широковещательные пакеты одной виртуальной сети не достигают коммутаторов, которым они не предназначены. До появления ПО Cisco IOS Release 5.4 очистить VLAN 1 от магистральных линий было нельзя. В более поздних версиях очистить VLAN 1 можно с помощью следующей команды:

```
Praha> (enable) clear trunk 1/1 1

Default vlan 1 cannot be cleared from module 1.
```

В разделе Пример с VLAN 1 описывается, как не допустить охватывания виртуальной сетью VLAN 1 всей сети.

Сети VLAN не отсечены

Если два коммутатора A и B подключены к однопортовому коммутатору A, который сконфигурирован в качестве магистрального и подключен к IP-телефону, VTP будет получать сообщения, проходящие от коммутатора A к коммутатору B. Поэтому коммутатор B не может отсечь неиспользуемые виртуальные сети VLAN.

Эту проблему можно устранить, если настроить подключенный к IP-телефону порт в качестве голосового порта доступа VLAN.

```
Switch#interface FastEthernet0/1
               switchport access vlan <vlan number>
               switchport voice vlan <vlan number>
```

Пример с VLAN 1

Процедура отсечения каналов в протоколе VTP не может быть применена к VLAN, которые должны охватывать всю сеть и все коммутаторы сети (чтобы была возможность передачи VTP и CDP (протокол обнаружения Cisco) трафика и другого управляющего трафика). Однако существует способ ограничить использование VLAN 1. Функция называется отключением VLAN 1 на магистральном канале. Функция доступна в коммутаторах Catalyst серий 4500/4000, 5500/5000 и 6500/6000, работающих под управлением ПО CatOS Release 5.4(x) и более новых его версий. Функция позволяет отсекать VLAN 1 от магистрального соединения так же, как и любую другую VLAN. Это отсечение не распространяется на трафик управляющих протоколов, свободно передаваемый в магистрали (DTP, PAgP, CDP, VTP и другие протоколы). Однако использование этой функции блокирует весь пользовательский трафик на данной магистрали. Данная функция позволяет не охватывать виртуальной сетью всю сеть. Протяженность петель STP ограничивается даже в VLAN 1. Сеть VLAN 1 можно отключить, так как другие сети VLAN будут настроены на удаление из магистрали:

```
Console> (enable) set trunk 2/1 desirable

Port(s)  2/1 trunk mode set to desirable.

Console> (enable) clear trunk 2/1 1

Removing Vlan(s) 1 from allowed list.
Port  2/1 allowed vlans modified to 2-1005.
```

Устранение неисправностей, связанных с ошибками номера версии конфигурации VTP, которые обнаруживаются в выходных данных команды show vtp statistics

VTP разработан для управляющих сред, в которых изменения в базу данных VLAN домена вносятся одновременно только на одном коммутаторе. Предполагается, что новая версия распространяется в домене до создания следующей версии. Изменение базы данных одновременно на двух различных устройствах управляющего домена может привести к созданию двух различных баз данных с одинаковыми номерами версий. Эти базы данных, распространяясь, приводят к переписыванию существующей информации до тех пор, пока они не сойдутся на промежуточном коммутаторе Catalyst сети. Коммутатор не может принять ни одно из объявлений, поскольку номера версий пакетов совпадают, а значения MD5 различаются. Когда коммутатор обнаруживает подобную ситуацию, значение счетчика ошибок версий конфигурации `No of config revision errors` увеличивается.

Примечание. Ситуация, описанная в разделе, рассмотрена на примере выходных данных команды **show vtp statistics**.

Если обнаруживается, что на каком-либо коммутаторе информация о виртуальных сетях не обновляется, либо при обнаружении других аналогичных неисправностей, введите команду **show vtp statistics**. Определите, не увеличилось ли количество пакетов VTP, приводящих к возникновению ошибок номера версии конфигурации:

```
Console> (enable) show vtp statistics

VTP statistics:
summary advts received          4690
subset  advts received          7
```

```
request advts received          0
summary advts transmitted       4397
subset  advts transmitted       8
request advts transmitted       0
No of config revision errors    5
No of config digest errors      0
VTP pruning statistics:
Trunk     Join Transmitted  Join Received  Summary advts received from
                                          non-pruning-capable device
--------  ---------------  -------------  --------------------------
1/1       0                0              0
1/2       0                0              0
Console> (enable)
```

При обнаружении ошибки версии конфигурации эту проблему можно устранить, изменив базу данных VLAN таким образом, чтобы создать базу данных VTP с номером версии, превышающим номера остальных баз. Например, на коммутаторе, работающем в качестве основного сервера VTP, можно добавить в домен администрирования дополнительную VLAN, а затем удалить ее. Эта обновленная версия распространяется по всему домену, переписывая базу данных на всех устройствах. Когда все устройства домена объявляют одинаковую базу данных, ошибка более не возникает.

Устранение неисправностей, связанных с ошибками дайджеста конфигурации VTP, которые обнаруживаются в выходных данных команды show vtp statistics

В данном разделе описан способ устранения неисправностей, связанных с ошибками дайджеста конфигурации VTP, которые наблюдаются при введении команды **show vtp statistics**. Ниже представлен пример:

```
Console> (enable) show vtp statistics

VTP statistics:
summary advts received          3240
subset  advts received          4
request advts received          0
summary advts transmitted       3190
subset  advts transmitted       5
request advts transmitted       0
No of config revision errors    0
No of config digest errors      2
VTP pruning statistics:
Trunk     Join Transmitted  Join Received  Summary advts received from
                                           non-pruning-capable device
--------  ---------------  -------------  --------------------------
1/1       0                0              0
1/2       0                0              0
Console> (enable)
```

Главной задачей значения MD5 является проверка целостности полученных пакетов и обнаружение любых изменений или повреждений пакета во время передачи. Когда коммутатор обнаруживает новый номер версии, отличный от текущего сохраненного значения, он отправляет сообщение с запросом на сервер VTP и запрашивает сокращенные объявления VTP. Сокращенное оповещение содержит список сведений VLAN. Коммутатор вычисляет значение MD5 для сокращенных объявлений и сравнивает полученное значение со значением MD5, которое содержится в сводном объявлении VTP. В случае если эти значения различаются, значение счетчика ошибок дайджеста конфигурации `No of config digest errors` увеличивается.

Типичной причиной данных ошибок является несогласованность пароля VTP на всех серверах в доменах VTP. Устраните такие неполадки, как ошибки в конфигурации или повреждение данных.

Убедитесь в том, что во время исправления этой проблемы счетчик ошибок не находится в режиме статистики. Меню статистики обеспечивает подсчет ошибок с момента последнего сброса устройства или сброса статистики VTP.

Невозможность переключения коммутатора из режима сервера VTP или прозрачного режима VTP

Если коммутатор работает автономно (т.е. не подключен к сети) и при этом необходимо настроить режим клиента VTP, после перезагрузки коммутатор начинает работать либо в режиме сервера VTP, либо в прозрачном режиме VTP, в зависимости от режима VTP, в котором коммутатор находился до настройки в качестве клиента VTP. При отсутствии рядом сервера VTP коммутатор не допускает настройки в качестве клиента VTP.

Приветствия OSPF блокируются в домене VTP

Приветствия проткола OSPF могут быть заблокированы, и смежность может быть отброшена, если в коммутаторе в домене VTP клиентский режим или серверный режим изменен на прозрачный режим. Данная ситуация может произойти, если в домене разрешено отсечение каналов в протоколе VTP.

Для устранения этой проблемы используйте один из следующих вариантов:

- Запрограммируйте (на аппаратном уровне) соседей OSPF.
- Отключите отсечение по протоколу VTP в домене.
- Верните режим VTP коммутатора в серверный или клиентский режим.

Дополнительные сведения

- **Поддержка продуктов для LAN**
- **Техническая поддержка коммутационных решений для LAN**
- **Cisco Systems – техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/10/100276/tshoot-vlan.shtml