РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

ДОКЛАД

на тему Протокол VTP. Различия версий протокола VTP.
дисциплина: Администрирование локальных сетей

Студент: Логинов Сергей Андреевич

Группа: НФИбд-01-18

МОСКВА
2021 г.

Содержание

Введение

Протокол VTP – протокол, служащий для обмена информацией о VLAN, имеющихся на выбранном транковом порту. Разработан и используется компанией Cisco.

История протокола VTP

Протокол VTP был создан для решения возможных проблем в среде коммутации виртуальных сетей VLAN. Например, рассмотрим домен, в котором имеются несколько связанных друг с другом коммутаторов, которые поддерживают несколько VLAN-сетей. Для создания и поддержания соединений внутри VLAN-сетей каждая из них должна быть настроена вручную на каждом коммутаторе. По мере роста сети и количества коммутаторов в ней ручная конфигурация нового коммутатора становится все более проблематичной. Всего одна ошибка может привести к проблемам:
Перекрестное соединение VLAN-сетей
Противоречивость конфигурации в смешанной среде передачи(например в среде, включающей Ethernet)
В протоколе VTP согласованность конфигураций VLAN-сетей поддерживается в общем административном домене. Кроме того, протокол VTP уменьшает сложность управления и мониторинга VLAN-сетей.

Зачем нужен VTP и как он работает

Основной функцией протокола VTP является решение вопроса синхронизации информации о VLAN между коммутаторами в сети. Протокол упрощает операции с VLAN’ами в сети, позволяя добавлять или изменять информацию на VTP-сервере и отправлять ее VTP-клиентам. В таком случае ручная настройка VLAN на коммутаторах не требуется, количество ошибок сокращается.
Используя протокол VTP, коммутаторы делятся на два основных вида:
VTP Server – коммутаторы, на которых можно производить изменения базы VLAN’ов.
VTP Client – коммутаторы, которые работают только в режиме получения анонсов от других VTP устройств. Не имеют возможности изменять информацию.
Также существуют устройства, которые пользуются своей локальной базой VLAN’ов, являющиеся простыми ретрансляторами и не выполняющими функцию обработки кадра.

В целом, работа VTP заключается в передаче базы данных VLAN между устройствами. Это происходит в случаях изменения базы данных на сервере и по прошествии определенного времени. Сначала на сервере обновляется база данных, далее всем транковым портам рассылается анонс, все коммутаторы, работающие в VTP, применяют его к себе(кроме Transperent) и отправляют дальше.

Хранение информации о VLAN’ах и настройках

В разных ролях VTP это реализовано различными способами:

- Коммутатор с ролью VTP Server будет хранить настройки в файле vlan.dat на указанном устройстве хранения (один из flash’ей устройства)

- Коммутатор с ролью VTP Transparent или VTP Off будет хранить настройки в конфигурации (это config.text, или, говоря проще, NVRAM)
- Коммутатор с ролью VTP Client будет хранить настройки в оперативной памяти (их не будет видно в конфигурации или на flash)

VTP Pruning

Задача этой функции проста – каждый коммутатор будет “считать” фактически используемые VLAN’ы, и в случае, когда по VTP приходит неиспользуемый VLAN, уведомлять соседа, что этот трафик не имеет смысла присылать. Под этот механизм будут подпадать только первые 1000 VLAN’ов, исключая самый первый (т.е. pruning работает только для VLAN’ов с номерами от 2 до 1001). Более того, под pruning будет подпадать только уникастовый и неизвестный мультикастовый трафик, поэтому, к примеру, BPDU протоколов семейства STP фильтроваться не будут. Т.е. допустим, у нас есть два коммутатора – A и B. Коммутатор A имеет роль VTP Server, а B – VTP Client. Между ними – транковый канал, 802.1Q. На коммутаторе B включен vtp pruning. Допустим, на коммутаторе A в базу VLAN добавлены VLAN 10 и VLAN 20. Соответственно, коммутатор A уведомит по протоколу VTP своего соседа – B – о новой ревизии базы VLAN’ов. Сосед B добавит эти VLAN’ы в базу и теперь, когда подключенный к коммутатору A клиент, например, передаст броадкаст в VLAN’е 10, этот броадкаст дойдёт и до коммутатора B. Невзирая на то, что у коммутатора B может вообще не быть ни одного порта и интерфейса в VLAN 10, а также не быть других транков (т.е. трафик 10го VLAN’а коммутатору B совсем не нужен). В данном случае механизм pruning сможет сэкономить полосу пропускания канала между коммутаторами A и B просто не отправляя трафик неиспользуемого VLAN’а коммутатору B.

Настройка имени домена VTP

host(config)#vtp domain *имя_домена*
Стереть имя домена штатно нельзя, только сменить.

Настройка пароля VTP

host(config)#vtp password *пароль*
Пароль можно сбросить на пустой, если ввести команду no vtp password. Важно помнить, что пароль VTP хранится небезопасно (у VTP Server – в файле vlan.dat, у VTP Transparent – в NVRAM), поэтому используя VTP, необходимо задавать такой пароль, который более нигде не дублируется, т.к. получить пароль VTP – относительно несложно. Всё, от чего защищает этот пароль – это, например, случайное добавление в сеть неправильно настроенного коммутатора и последующие проблемы. Пароль VTP не защищает передаваемую между коммутаторами информацию.

Настройка версии VTP

host(config)#vtp version *версия*

Выбор версии 1,2 или 3.

Настройка VTP pruning

Включение выполняется командой:
host(config)#vtp pruning
выключение:
host(config)#no vtp pruning

Настройка режима VTP

host(config)#vtp mode *режим*
Где режим – это server, client, transparent или off. Режим off получится поставить только на устройствах, поддерживающих VTPv3; на коммутаторах, которые поддерживают только VTPv1 и VTPv2 отключить протокол нельзя.

Устранение неисправностей

Проверка каналов:

- Проверьте физическую доступность интерфейсов
- Проверьте корректность режима дуплекса и скорости
- Проверьте, что корректно согласовался транк

Проверка настройки VTP:

- Участвующие коммутаторы должны быть непосредственно подключены друг к другу
- Должен быть хотя бы один VTP Server
- Версии VTP, а также имя домена и пароль должны быть идентичны у всех устройств

Проблема добавления нового коммутатора

Новый коммутатор при добавлении делает следующее – он слушает трафик VTP и при получении первого же advertisement берёт из него настройки (имя домена и пароль). Также известно, что стандартная настройка коммутатора – это режим VTP Server (т.е. когда Вы достаёте коммутатор из коробки, Вы сразу можете на нём создавать VLAN'ы, в случае VTP Client это было бы невозможно).

Соответственно, возможна неприятная ситуация. Состоит она в том, что можно взять коммутатор, заранее его сконфигурировать, внеся больше изменений, чем есть сейчас в инфраструктурном VTP, задать правильные параметры домена и под-

ключить к сети. Тогда коммутатор своей базой затрёт существующую. Почему так произойдёт и как это может быть? Рассмотрим подробнее.

Вы покупаете новый коммутатор и вводите его в эксплуатацию. Отдельно от других, которые работают в VTP. Начинаете с ним работать. Работаете интенсивно – добавляете на него vlan'ы, удаляете их, переименовываете. Каждое действие плюсует единицу к revision number. Но через некоторое время возникает необходимость подключения коммутатора к другой сети. У данного коммутатора ревизия(число) выше, чем у местного VTP Server. Имя домена и пароль совпадают. Как только транк поднимается, новый коммутатор выстреливает advertisement, который начинают слушать все остальные коммутаторы и ретранслировать дальше. Это штатный функционал – Вы не можете ограничить получение VTP-данных только от одного, "правильного" сервера. Соответственно, эта волна накрывает все коммутаторы в режиме Client и тот, который в Server. Это тоже штатное поведение – VTP Server, получив VTP-данные с большим номером ревизии, чем у себя, перезаписывает свою базу. Имеется большая проблема – вместо Вашей базы VLAN'ов у Вас на всех коммутаторах та, которая была в прошлом месте эксплуатации коммутатора.

Чтобы избежать этого, можно поступить по-разному. Например, не делать у этого коммутатора имя домена и пароль, как в основной VTP-сети. Но можно и проще – ведь чтобы этого всего не произошло, надо просто сбросить номер ревизии. Для этого достаточно переименовать домен у коммутатора в какое-нибудь временное название и после вернуть назад. Ревизия сбросится. После не забудьте включить режим VTP Client.

Как понятно, именно из-за этой ситуации использование VTP в production-сети с высоким уровнем безопасности является нежелательным. Злоумышленник может провести достаточно простую атаку – ему хватит доступа к транковому порту и возможности отправить, допустим, vtp-уведомление о том, что пришла база с версией 10000 и одним vlan'ом, и всё – вся VTP-инфраструктура примет это как нормальное положение вещей и остальные vlan'ы пропадут. Поэтому в безопасных сетях все коммутаторы работают в VTP transparent, где такая ситуация невозможна в принципе.

Недостатки протокола VTP

Использование VTP обладает несколькими недостатками:
Необходимо находить баланс между простотой управления VTP, неотъемлемым риском образования большого домена STP, потенциальной нестабильностью STP и рисками, возникающими при использовании STP. Самый большой риск кроется в распространении петли STP на всю сеть.
При использовании VTP двум моментам необходимо уделить особое внимание:

Следует помнить о версиях конфигураций и сбрасывать их при добавлении в сеть нового коммутатора, чтобы не привести к сбою работы всей сети.
Следует тщательно избегать создания виртуальных сетей, распространяющихся на всю сеть.

Версии протокола VTP. Отличия v2 и v3.

У протокола существуют три версии. Пользователь может настраивать одну из них по своему усмотрению. По умолчанию используется версия 1.

Отличия v2 от v1:

- Основное различие заключается в том, что в VTP V2 содержится поддержка виртуальных локальных сетей Token Ring. При использовании виртуальных локальных сетей Token Ring необходимо включить VTP V2. В противном случае нет необходимости использовать VTP V2.
- Также есть отличие в «прозрачном» режиме. Если в первой версии коммутатор передает анонсы только для домена, к которому относится, то во второй версии анонсы передаются вне зависимости от принадлежности к какому-либо домену.

Отличия v3 от v2 и v1:

- Поддержка Private VLAN (раньше, если на коммутаторе используются PVLAN, то если и использовать VTP, то только режим VTP Transparent).
- Поддержка полного диапазона (всех 4094) VLAN'ов. Ранее, в силу наследства CatOS с 10ти битовыми рудиментами, техническое ограничение предполагало работу с VLAN в диапазоне номеров от 2 до 1001. Первый VLAN всегда есть и поэтому факт его наличия передавать на другие устройства Cisco не надо, VLANы с 1002 по 1005 зарезервированы для некрофункций, связанных с транзитом Token Ring / FDDI, а оставшийся до 1023 VLAN "хвостик" имеет свои специфичные применения. Остальные VLANы (с номерами от 1023) иметь на устройстве при VTPv1-v2 было можно, но вот VTP с ними не работал – а теперь может.
- Появилась настройка VTP на уровне отдельного порта коммутатора.
- Появилась возможность реального выключения VTP, а не просто перевода его в transparent mode.
- Усилена защита пароля VTP.
- Решена проблема с добавлением нового коммутатора – теперь испортить VTP-домен нельзя.
- Появились подвиды роли server – у VTP теперь есть просто server и primary server.

- Обмен данными между VTP-устройствами переработан и стал более эффективным (данные передаются компактнее и, следовательно, быстрее).
- VTPv3 стал модульным и поддерживает обмен не одной, а несколькими базами данных. На данный момент реализованы модули БД VLAN'ов и протокола MST (который 802.1s). Схема расширяема, и VTP теперь можно "научить" синхронизировать между несколькими устройствами нужные типы данных.

Заключение

В итоге можно сказать, что протокол VTP облегчает выполнение рутинных задач, таких как ручная настройка, сводя ошибки к минимуму. Но также у него есть свои недостатки. Понимая то, что необходимо сделать, можно принимать решение об использовании этого протокола.

Список литературы по теме

1. https://www.cisco.com/c/ru_ru/support/docs/lan-switching/vtp/10558-21.pdf
2. https://www.atraining.ru/protocol-vtp2/
3. https://www.atraining.ru/protocol-vtp3/
4. https://ru.wikipedia.org/wiki/VTP_(протокол)
5. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vtp.html#wp1020429