Содержание

Введение

Чтобы начать понимать понятия Коммутации Token Ring, очень важно, чтобы вы поняли прозрачный режим моста, мостовое соединение исходного маршрута и Связующее дерево. Catalyst 3900 и Catalyst 5000 используют новые концепции, как описано в приложении K IEEE 802.5. Эти понятия являются составляющий компонентами для Вртуальных локальных сетей Token Ring. Этот документ объясняет другие понятия мостового соединения и как они работают:

- Транкинг протокола ISL
- Связующее дерево
- Протокол магистральных каналов VLAN (VTP)
- Протокол DRiP (Duplicate Ring Protocol) (DRIP)

Этот документ также объясняет некоторые проблемы, которые происходят, когда вы выполняете Протокол HSRP по Вртуальным локальным сетям Token Ring и их обходные пути.

Примечание: Для определения Акронимов Token Ring, которые используются в этом документе, обратитесь к Акронимам Коммутации Token Ring.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

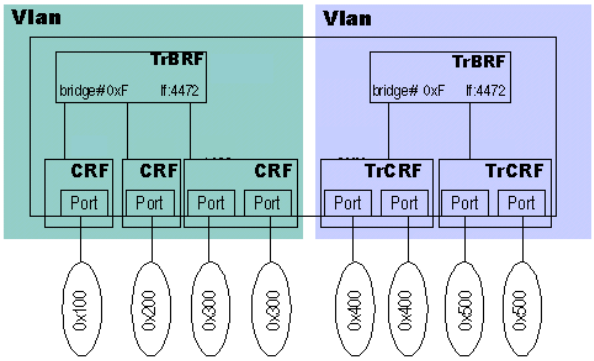
Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

TrBRF и TrCRF

Передающая функция моста Token Ring (TrBRF) и Передающая функция концентратора Token Ring (TrCRF) является составляющий компонентами архитектуры Catalyst 3900 и функциональности Catalyst 5000. TrBRF является просто функцией моста коммутатора, и TrCRF является функцией концентратора коммутатора. Важно понять, что мостовое соединение происходит на обоих из этих уровней, потому что в Token Ring будут обсуждены три различных типа мостового соединения.

Функциональные возможности TrBRF коммутации средств управления за коммутатором трафика мостовой передачи с маршрутизацией от источника, как мостовое соединение с маршрутизацией от источника (SRB) и прозрачное соединение маршрут-источник (SRT). TrCRF покрывает функциональность маршрутизации от источника (SRS) и прозрачного соединения с помощью моста (TB). Например, возможно иметь Коммутатор Catalyst 3900, который только имеет один TrBRF и один TrCRF, и все порты коммутатора находятся в том же TrCRF. Это заставляет коммутатор только быть в состоянии сделать SRS и ТБ. При определении десяти других TrCRFs под тем же родительским TrBRF то трафик от портов, которые связаны с тем же TrCRF, был бы передан через функциональность TrCRF SRS или ТБ. Трафик, переходящий к другому TrCRFs в коммутаторе, использовал бы функциональные возможности TrBRF коммутатора и был бы или соединенным исходным маршрутом или исходным маршрутом, прозрачно соединенным. Другие механизмы переключения будут обсуждены позже в этом документе.

Эта схема относится TrBRF и TrCRF к физическому слову:



Вы видите, что каждый TrCRF связан с одним определенным вызовом. TrCRF может поставить под угрозу множественные порты, и эти порты поставили бы под угрозу тот же номер кольца. TrBRF подключает TrCRFs вместе.

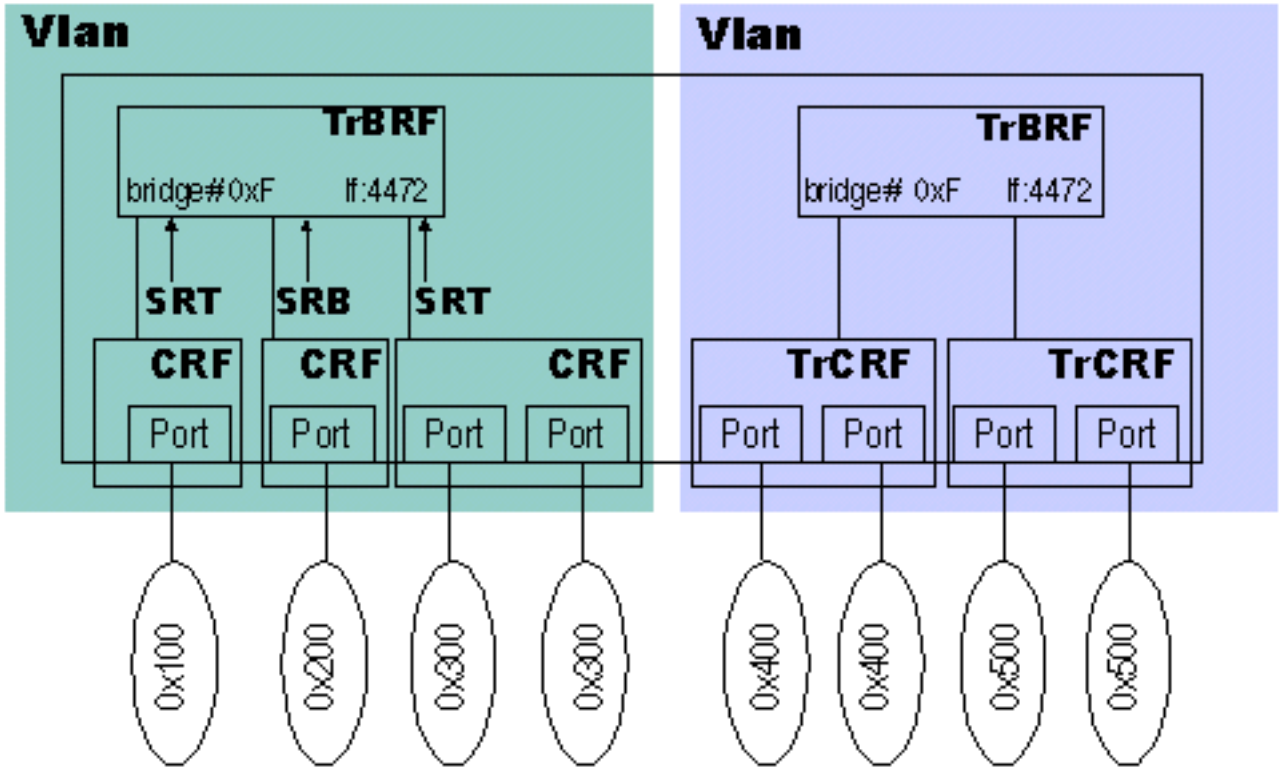
TrCRF и TrBRF сам по себе являются другой VLAN. Так, в Token Ring можно соединить между VLAN. Мостовое соединение между Вртуальными локальными сетями Token Ring придерживается двух правил:

- Мостовое соединение между двумя VLAN TrBRF может только быть выполнено внешним устройством, как маршрутизатор или Модульный коммутатор с функциями маршрутизатора (RSM).
- Мостовое соединение между VLAN TrCRF может только быть выполнено с VLAN TrCRF, которые являются потомками той же родительской VLAN TrBRF.

Это очень важно для учета для Вртуальных локальных сетей Token Ring, потому что это ломает парадигму Ethernet. Для суммирования что было бы похоже, Виртуальная локальная сеть Ethernet является суммой одного TrBRF и его дочернего TrCRF. Поскольку можно соединить между определенными VLAN в Token Ring, необходимо понять, как происходит это мостовое соединение.

Примечание: Чтобы упростить понимать Вртуальные локальные сети Token Ring относительно Виртуальных локальных сетей Ethernet, помните, что комбинация TrCRF и TrBRF делает VLAN сам по себе.

В этой схеме вы видите, что TrCRF решает режим моста между TrCRF и TrBRF.



Отдельные TrCRFs настроили, какое мостовое соединение они будут делать к TrBRF. Это важно, потому что у вас могут быть VLAN TrCRF, которые сделают мостовое соединение исходного маршрута к другому TrCRFs, но не сделают нефреймов с внутренней маршрутизацией. В предыдущей схеме один TrCRF настроен для режима SRB, и два находятся в режиме SRT. Это означает, что трафик SRB может течь между всеми тремя TrCRFs, но SRT может только течь между двумя, которые находятся в режиме SRT. Это

позволяет вам гранулировано устанавливать, как трафик должен течь между TrCRFs. Если бы режим моста был установлен в TrBRF, то он влиял бы на все потомки TrCRF той VLAN.

Режимы коммутации

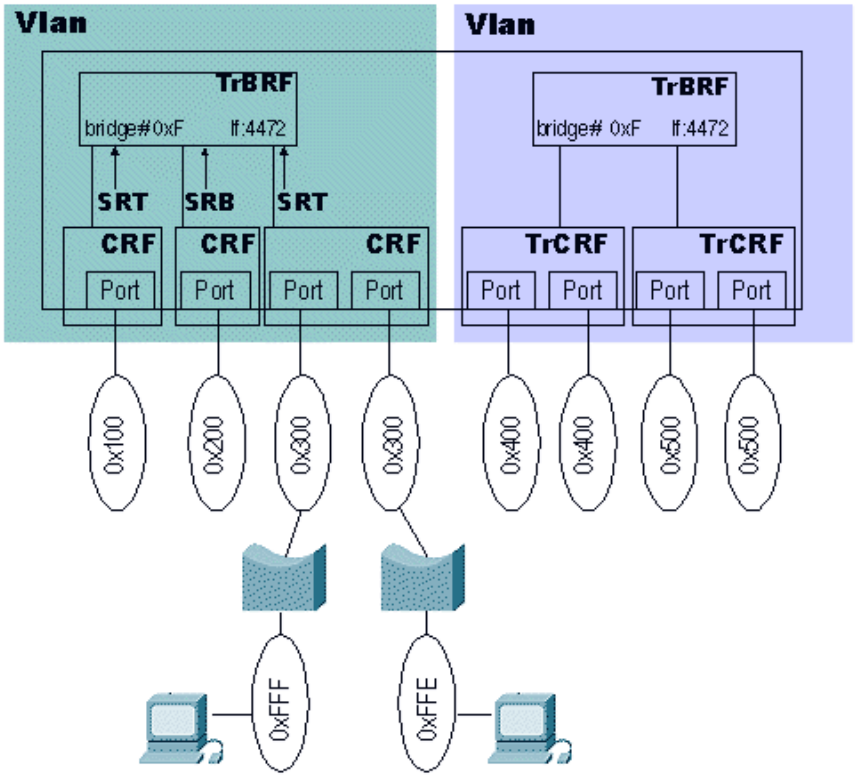
Из коробки Catalyst 3900 настроен с одним TrBRF и одним TrCRF. Все порты назначены на TrCRF VLAN 1003 по умолчанию. То же применяется к Token Ring Blade Catalyst 5000. Это важно, потому что это дает бесспорную коробку??? plug and Play??? функциональность. Из коробки эти коммутаторы могут сделать передачу на основе маршрутизации от источника и прозрачного режима моста. Следующие разделы предоставляют подробную информацию об этих технологиях.

Прозрачное соединение

Прозрачный режим моста является самым основным из всех механизмов переключения и основывается на адресе MACa - адреса назначения (DMAC) кадров в сети. Это - механизм переадресации Сетей Ethernet. Любое время коммутатор принимает кадр, он делает запись адреса MAC источника (SMAC) адрес кадра как тот, который принадлежит тому порту и, впредь, передает трафик, который предназначен к тому MAC к тому порту. Если в процессе обучения коммутатор не будет знать о MAC-адресе, то это лавинно разошлет тот пакет ко всем портам в состоянии пересылки.

Маршрутизация от источника

Маршрутизация от источника является механизмом переадресации, который необходим, когда существует только один TrCRF, назначенный на порты, и коммутатор получает пакеты с Полями сведений о маршрутизации (RIF) в них. Поскольку коммутатор не будет модифицировать RIF кадра (потому что это не передаст его к TrBRF), сеть должна быть в состоянии принять решения о передаче, с RIF, без модификаций. Рассмотрите эту схему сети, которая показывает SRS:



Трафик, идущий от вызова 0xFFF для вызова на 0xFFE, должен пройти коммутатор. Этот трафик был бы трафиком маршрутизации от источника. Это - последовательность запуска связи между этими двумя клиентами:

1. Одна станция передает пакет анализатора к вызову, на котором она находится. Предположите, что клиент на вызове 0xFFF передает пакет; это выглядит примерно так (в шестнадцатеричном):**Примечание:** Те сведения о пакете только показывают DMAC, SMAC и информацию RIF.
2. Как только пакет достигает маршрутизации от источника и передает кадр к проводу, пакет похож на это:`C670` является контрольным полем маршрутизации, и `FFF1 3000` является вызовом 0xFFF, мост 0x1, вызов 0x300. Для получения дополнительной информации о декодировании RIF обратитесь к Мостовому соединению исходного маршрута Настройки.
3. Теперь, пакет поражает коммутатор. Поскольку коммутатор видит, что пакет прибывает из далеко вызов, это изучает дескриптор маршрута. В этом случае коммутатор теперь знает, что вызов 0xFFF через мост 0x1 расположен на порту 3.
4. Поскольку пакет является пакетом анализатора, коммутатор передает кадр ко всем портам под тем же TrCRF. Если проводник должен перейти к портам в другом TrCRFs, он отправит кадр TrBRF, который сделает его функциональность моста. Если будут порты в том же TrCRF, то он передаст кадр, исходящий без модификации.
5. Станция в вызове 0xFFE должна получить проводник и ответить на него. Предположите, что клиент отвечает directed frame. Этот directed frame похож на это:`08E0` является контрольным полем маршрутизации, и `FFF1 3001 FFE0` является вызовом 0xFFF, мост 0x1, вызов 0x300, мост 0x1, вызов 0xFFE.
6. Наконец, коммутатор узнает, что вызов 0xFFE расположен на порту 4 и поддерживает дескриптор маршрута.

Впредь, коммутатор знает о тех вызовах. При рассмотрении таблиц необходимо видеть, что коммутатор учился о номере моста и номере кольца. Любые другие вызовы после вызова 0xFFF и вызова 0xFFE не необходимы, потому что они должны пройти или через вызов 0xFFF или звонить на 0xFFE для достижения коммутатора.

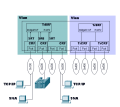
SRS являются основной передачей основанных на RIF пакетов без функциональных возможностей SRB, как имеет место с TrCRF.

Примечание: Для просмотра таблицы сведений о маршрутизации в Catalyst 3900 обратитесь к Просмотру Таблицы дескриптора маршрутов для Каждой VLAN в Управлении Catalyst 3900. Для Catalyst 5000, проблема **команда show rif**.

Мостовое соединение исходного маршрута и Source Route Transparent

Вся функциональность мостового соединения исходного маршрута расположена в логике TrBRF. TrCRF является тем, который переходит к команде режим моста к TrBRF. Так, если TrCRF настроен для режима SRB к TrBRF тогда, когда TrCRF получает NSR (нес маршрутизацией источника) структурируют, коммутатор не передаст его логике TrBRF.

Это может использоваться, если вы не хотите, чтобы определенные типы трафика поразили или оставили определенный вызов. Данный пример представлен на рисунке:



Если бы у клиентов TCP/IP не было способности передать пакеты с RIF, то коммутатор не поместил бы те кадры в тот же вызов с мейнфреймом (0x200). Однако SNA структурирует к хосту (которые обычно имеют RIF), достиг бы мейнфрейма. Это очень устаревший способ для фильтрования кадры в коммутируемой сети.

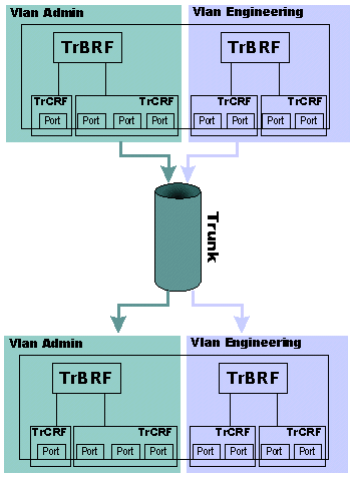
Это - последовательность, которой коммутатор придерживается для передачи фрейма с мостовыми соединениями исходного маршрута через TrBRF:

1. Станция SNA на вызове 0x300 (порт 4) передает проводник для достижения мейнфрейма.
2. Когда пакет анализатора поражает коммутатор, это вперед проводник, без модификации, в том же TrCRF; тогда это передает копию к TrBRF для передачи остатку TrCRFs. В этом случае, потому что пакет имеет RIF, он проходит путь SRB. Коммутатор также должен изучить маршрут.
3. Коммутатор переходит, изучают SMAC кадра, потому что пакет показывает как происходящий на местном кольце, с которым связан коммутатор. Это вызвано тем, что, в сочетании TrCRF множественных портов, RIF показывает вызов абонента, но коммутатор должен знать который порт в TrCRF. Поэтому коммутатор изучает SMAC кадров, которые входят на уровне TrCRF.
4. Пакет выходит в весь остаток TrCRFs, модифицируемого с их соответствующими комбинациями номеров мостового кольца.
5. Как только хост отвечает кадром SRB, коммутатор изучает SMAC хоста к тому TrCRF и передает его к порту исходящих соединений. Трафик тогда течет назад и вперед между двумя.

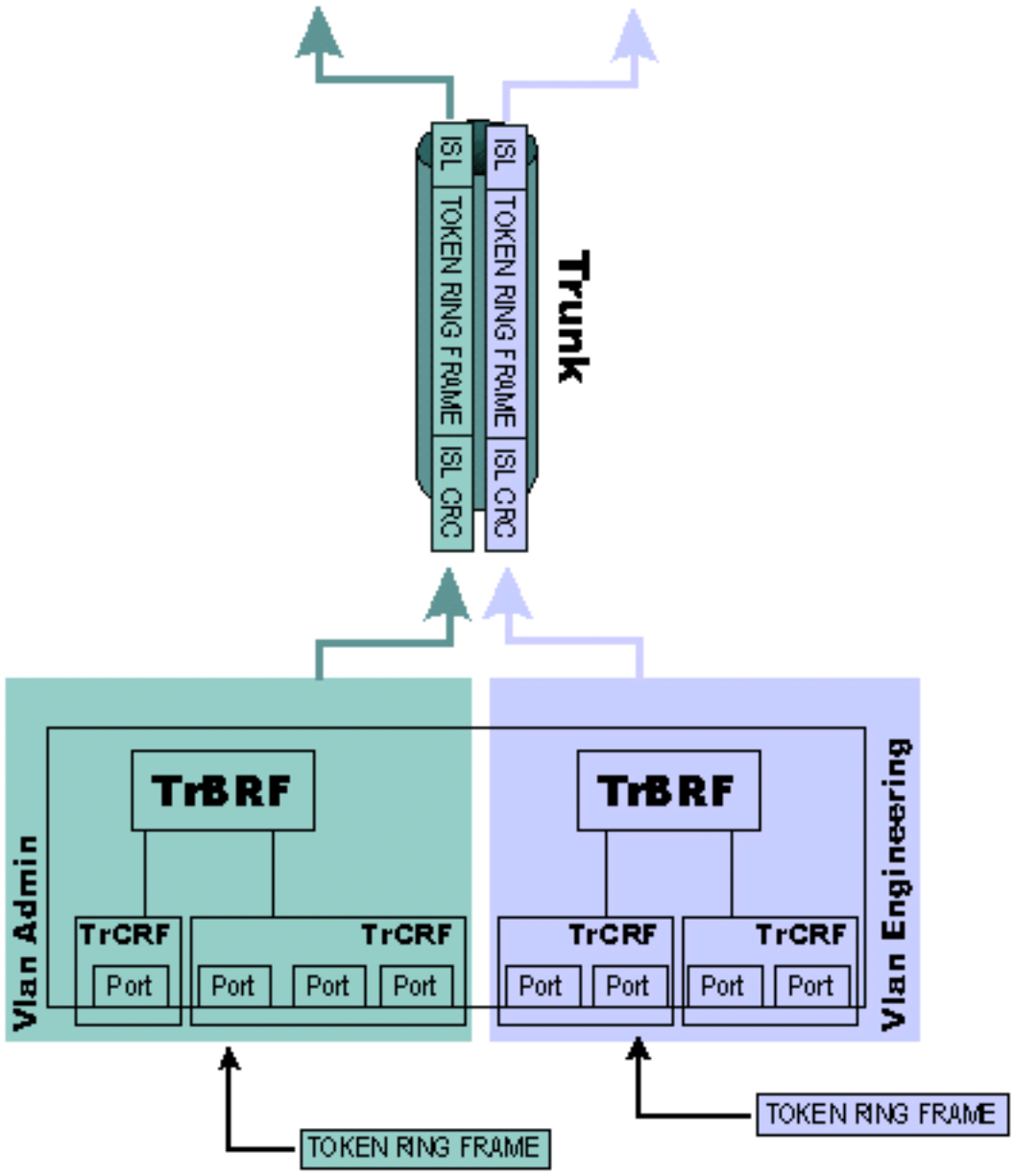
Примечание: Для проверки таблицы MAC-адресов на Catalyst 3900 обратитесь к Просмотру Главной таблицы адресов в Управлении Catalyst 3900. Для Catalyst 5000 выполните **команду show cam**.

Связь между коммутаторами

Связь между коммутаторами очень простой протокол. В основном кадры, которые идут через магистральный канал ISL, инкапсулируются в кадре ISL, который говорит другую сторону, которой VLAN принадлежат кадры. Из-за этого сведения о виртуальной локальной сети (VLAN) должны быть разделены или вручную или автоматически между коммутаторами. Протокол, известный как Протокол магистральных каналов VLAN (VTP), может обработать эту задачу. Для Вртуальных локальных сетей Token Ring необходимо выполнить VTP V2 в сети. Рассмотрим следующую диаграмму:



В этом случае одиночный магистральный канал ISL был создан для переноса, отдельно, технических VLAN и VLAN admin. Ни один из трафика в любой VLAN не смешивается после того, как это пройдет транк. Эта схема показывает способ, которым достигнуто это разделение:



Каждый кадр от тех VLAN, который должен пойти через транк, инкапсулируется в кадре ISL, и его VLAN включена в кадр. Это позволяет принимающему коммутатору правильно направлять кадр к своей определенной VLAN. Token Ring ISL (TRISL) кадр имеет еще несколько полей, чем обычный кадр ISL. Эта схема показывает план кадра TRISL:

40 DA	4 TYPE	4 USER	48 SA	16 LEN	24 AAAA03

24 HSA	15 DESTVLAN	1 BPDU	16 INDX	15 SRCVLAN	1 EXP

16 DESTRD	16 SRCRD	1 t	1 F	6 Extra	8 to 196600 (1 to 24575 bytes) ENCAP FRAME

ENCAP FRAME (Continued)	8 to 196600 (1 to 24575 bytes) ENCAP FRAME	32 Syn CRC	32 ISL CRC

Примечание: Даже при том, что TRISL работает на основе Интерфейсов Fast Ethernet, пакеты содержат Кольцевой кадр стандартного маркера и сведения о виртуальной локальной сети (VLAN), привязанные к тому кадру, до некоторой степени. Вртуальные локальные сети Token Ring разрешают до 18k размеров фрейма, как делает ISL. Это *не* достигнуто через фрагментацию кадра. Весь кадр инкапсулируется в кадре ISL в целой части и передается через ссылку. Существует общее несовпадение, что ISL является Ethernet и что ее максимальный размер фрейма составляет 1500 байтов.

На Catalyst 5000 протокол, известный, поскольку, Протокол DTP стал доступным в выпуске 4. x . DTP – это стратегическая замена динамического ISL (DISL), так как в него введена поддержка согласования транкинга 802.1q. DISL??? s функция должен выполнить согласование, для ISL только, должна ли ссылка между двумя устройствами быть магистральной. DTP в состоянии выполнить согласование об инкапсуляции типа транкинга, которая будет использоваться между магистралями VLAN IEEE 802.1Q и ISL. Это полезная возможность, поскольку некоторые устройства Cisco поддерживают только ISL или 802.1Q, тогда как другие поддерживают оба протокола.

Это пять других состояний, для которых можно настроить DTP:

- Auto??? В Автоматическом режиме порт прислушивается к кадрам DTP от соседнего коммутатора. Если бы соседний коммутатор указывает, что хотел бы быть транком??? или это - транк??? тогда Автоматический режим создает транк с соседним коммутатором. Когда соседний порт установлен в На или Выбираемый режим, это происходит.
- Desirable??? Выбираемый режим указывает к соседнему коммутатору, что это, может быть магистральный канал ISL и что это хотело бы, чтобы соседний коммутатор также был магистральным каналом ISL. Порт становится магистральным, если соседний порт работает в режиме "on", "desirable" или "auto".
- Включено??? На режиме автоматически включает Транкинг ISL на его порту, независимо от состояния его соседнего коммутатора. Он остается магистралью ISL до получения ISL-пакета, явно отключающего ISL-магистраль.
- Nonegotiate??? Несогласованный режим автоматически включает Транкинг ISL на своем порту??? независимо от состояния его соседнего коммутатора??? но не позволяет порту генерировать кадры DTP.
- Выключен??? В Режим выключено, ISL не позволен на этом порту независимо от режима DTP, который настроен на другом коммутаторе.

Семейство Catalyst 5000 коммутаторов, как правило, используется для обеспечения магистрали ISL. Коммутатор Catalyst 3900 может тогда быть связан с этой магистралью через двойной модуль расширения ISL на 100 Мбит/с. Коммутатор Catalyst 3900 Token Ring не поддерживает никакой другой режим, чем ISL, таким образом, это всегда соединяется магистралью. Кроме того, модули ISL Catalyst 3900 только поддерживают соединения на 100 Мбит/с и по умолчанию к полному дуплексу.

Будьте очень осторожны при соединении Catalyst 3900 и Коммутатора Catalyst 5000 через ссылку ISL. Основная проблема - то, что Catalyst 3900 не поддерживает согласование среды Fast Ethernet. Поэтому, если Catalyst 5000 настроен для Автоматического режима, то это принимает значение по умолчанию к полудуплексу на 100 Мбит/с. Это вызывает проблемы как порт, идущий от транка до нетранкового и потери пакета.

Если вы хотите подключить порт ISL Catalyst 3900 к порту ISL Catalyst 5000, необходимо вручную настроить порт ISL на Catalyst 5000:

1. Выполните **команду set port speed** для установки в 100 Мбит/с:**`set port speed`** `mod/port` **`{4 | 10 | 16 | 100 | auto}`**
2. Выполните **команду set port duplex** для установки в полный дуплекс:**`set port duplex`** `mod/port` **`{full | half}`**

Если вы хотите вызвать порт коммутатора к режиму магистрали, выполнить **команду set trunk** (на одной линии):

`set trunk` *`mod/port`* **`{on | off | desirable | auto | nonegotiate}`** **`[`***`vlans`***`]`** **`[`***`trunk_type`***`]`**

В предыдущей команде *vlans* является значением от 1 до 1005 (например, **2-10** или **1005**), и *trunk_type* установлен в **isl**, **dot1q**, **dot10**, **переулок**, или **выполнить согласование**.

Как только магистральные порты активны на коммутаторах, можно выполнить **команду show trunk**, чтобы видеть, что эти переданные по транку порты активны.

```
Pteradactyl-Sup> (enable) show trunkPort      Mode         Encapsulation  Status        Native
vlan--------  -----------  -------------  ------------  ----------- 5/1      on           isl
trunking      110/1      on           isl            trunking      1Port      Vlans allowed on
trunk--------  ------------------------------------------------------------------- 5/1      1-
100510/1      1-1005Port      Vlans allowed and active in management domain--------  -----------
------------------------------------------------------ 5/110/1      1Port      Vlans in
spanning tree forwarding state and not pruned--------  ---------------------------------------
------------------------- 5/110/1      1
```

Важная команда для использования для наблюдения магистральных каналов ISL является **командой show cdp neighbors detail**. Эта команда также помогает вам понимать топологию сети.

```
Pteradactyl-Sup> (enable) show cdp neighbors detailPort (Our Port): 10/1Device-ID:
000577:02C700Device Addresses:Holdtime: 164 secCapabilities: SR_BRIDGE SWITCHVersion:  Cisco
Catalyst 3900 HW Rev 002; SW Rev 4.1(1)  (c) Copyright Cisco Systems, Inc., 1995-1999  - All
rights reserved.  8 Megabytes System Memory  2 Megabytes Network memoryPlatform: CAT3900Port-ID
(Port on Neighbors's Device): 1/21VTP Management Domain: unknownNative VLAN: unknownDuplex:
unknown
```

От тех выходных данных можно ясно видеть, что Catalyst 3900 связан с портом 10/1. При осмотре порта 10/1 в выходных данных предыдущей **команды show trunk** можно сказать, что это - магистральный порт.

Связующее дерево

Связующее дерево в Средах Token Ring может стать очень сложным, потому что можно одновременно выполнить в общей сложности три других Протокола связующего дерева. Например, типичная среда выполняет Связующее дерево IBM на уровне TrBRF и выполняет IEEE (802.1d) или Cisco на уровне TrCRF. Поэтому Связующее дерево немного более сложно для устранения проблем.

Эта таблица говорит вам, что происходит на основе различных типов возможных конфигураций:

Режим моста TrCRF	TrCRF	TrBRF
SRB	Выполняет протокол IEEE (связующее дерево).	Выполняет как маршрутизация от источника.

	Bridge Protocol Data Units IBM Spanning Tree Protocol процессов (BPDU) от внешних мостов.	Выполняет Протоколы STP IBM к внешним мостам.
		Отбрасывает прозрачные BPDU IEEE Spanning-Tree Protocol TrCRF.
SRT	Выполняет протокол Cisco SPANNING-TREE.	Выполняет как мост Source Route Transparent.
	Адрес группы мостов замен поля адреса точки назначения с определяемым Cisco групповым адресом, так, чтобы внешние мосты не анализировали BPDU TrCRF.	Вперед прозрачный и трафик исходного маршрута.
	Генерируйте BPDU с установленным битом RIF в поле исходного адреса в исходящем фрейме и 2-байтовом добавленном RIF. Этот формат фрейма гарантирует, что TrCRF остается локальным для логического кольца и прозрачно не соединен, или источник маршрутизируется к другим LAN. Только TrCRFs, связанные через физические петли, получают BPDU.	Вперед трафик исходного маршрута ко всему другому TrCRFs в TrBRF, ли они быть в SRT или режиме SRB.
	BPDU Протокола IEEE (связующее дерево) процесса	

	от внешних мостов.	

Для получения дополнительной информации обратитесь к Протоколу связующего дерева во Вртуальных локальных сетях Token Ring и Связанных протоколах.

Протокол транкинга виртуальной локальной сети (VLAN)

Поскольку с ISL VLAN определяет, куда пакет должен пойти, важно, чтобы каждый коммутатор знал о VLAN в сети. Протокол VTP??? s цель в жизни должен распространиться сведения о виртуальной локальной сети (VLAN) через коммутаторы. VTP не работает в маршрутизаторах, потому что они должны завершить виртуальную локальную сеть (VLAN). Каждый коммутатор в сети должен выполнить VTP. В противном случае тогда коммутатор обычно только выполняет одну VLAN (обычно VLAN 1) и не выполнил бы ISL на той ссылке, потому что нет никакой потребности. VTP делает создание VLAN намного более легкой задачей, потому что вы могли настроить VLAN в одном коммутаторе, и они распространятся через сеть. Конечно, это идет с проблемами.

VTP не является надежной системой, как Протокол EIGRP или протокол маршрутизации Протокола OSPF. Это намного более просто и воздействует на очень важное понятие: пересмотры. В VTP существует три типа устройств VTP: клиенты, серверы и прозрачные устройства. Клиентские устройства VTP в основном просто принимают сведения о виртуальной локальной сети (VLAN) от устройств сервера и не могут модифицировать эту информацию. Серверы, однако, могут модифицировать информацию VTP на любом из серверов VTP. Поэтому VTP имеет систему проверки. Любой сервер VTP, который модифицирует или обновляет Базу данных VLAN, утверждает, что это - последний пересмотр. Поэтому экстремальное внимание должно использоваться, потому что коммутатор с самой высокой редакцией будет??? победа??? и его сведения о виртуальной локальной сети (VLAN) будут допустимым. Например, при изменении одного сервера VTP, чтобы сказать, что VLAN 100 TrBRF переходит, делают протокол IEEE (связующее дерево), это вызвало бы опустошение среди всех коммутаторов, потому что это могло заставить коммутаторы (как Catalyst 3900) помещать порты в режим блокировки, защищать себя против петель. Кроме того, будьте осторожны, когда вы вводите новые коммутаторы в сеть, потому что у них могли быть более поздние версии VTP. В прозрачном режиме пакеты VTP, полученные на одном транке, автоматически распространяются, без изменений, ко всем другим транкам на устройстве; но, они проигнорированы на самом устройстве.

Когда вы устанавливаете VTP с Коммутаторами Token Ring, необходимо выполнить VTP V2. Если вы переходите, имеют коммутаторы, которые выполняют и Ethernet и Вртуальные локальные сети Token Ring, то необходимо обновить VTP, даже для Виртуальных локальных сетей Ethernet. У вас *не может* быть двух других доменов VTP (например, вы не можете иметь один для Ethernet и один для Token Ring).

Для получения дополнительной информации обратитесь к Протоколу магистральных каналов VLAN во Вртуальных локальных сетях Token Ring и Связанных протоколах.

Процедура отсечения каналов в протоколе VTP

Одна проблема с транкингом VLAN состоит в том, что широковещательная информация от одной VLAN распространяется через все транки, потому что коммутаторы не знают, какие VLAN существуют в удаленном коммутаторе. Отсечение каналов VTP было создано поэтому. Это разрешает коммутаторам выполнять согласование, какие VLAN назначены на

порты в другом конце транка и, поэтому, для отсечения VLAN, которые не назначены удаленно. Отсечение отключено по умолчанию на коммутаторах Catalyst 3900 и Catalyst 5000.

Примечание: Отсечение каналов VTP поддерживается на Коммутаторе Catalyst 3900 в Выпуске 4.1 (1).

Каждое из сообщений отсечения каналов VTP содержит информацию о рассматриваемых VLAN и содержит немного, которое указывает, должна ли эта VLAN быть сокращена для этого транка (`1` указывает, что это не должно быть сокращено). С отсечением включенного, трафик виртуальной локальной сети (VLAN) обычно не передается через магистральную линию, пока магистральная линия не получает соответствующее сообщение присоединения с соответствующей VLAN??? s бит включен. Это очень важно, потому что это говорит вам, что при использовании отсечения каналов VTP необходимо удостовериться, что корректная информация и конфигурация существуют и что все коммутаторы выполняют отсечение; если коммутатор не передает сообщения присоединения к другому коммутатору через транк, это могло бы быть отключено для конкретной VLAN или VLAN. Когда отсечение согласования завершено, VLAN закончится или в сливе или в состоянии, к которому присоединяются, для того транка.

Одна очень важная функция отсечения каналов VTP позволяет вам настраивать VLAN для отсечения имеющий право или нет. Эта функция говорит коммутаторы, которые выполняют отсечение каналов VTP для не отсечения этой VLAN. При включении отсечения каналов VTP VLAN 2 до 1000 сокращают имеющие право VLAN по умолчанию. Так, при включении отсечения оно влияет на все VLAN по умолчанию. VLAN 1, TrCRF по умолчанию (1003), TrBRF по умолчанию (1005), и TrCRFs является всегда неподходящим на отсечение; поэтому, трафик от этих VLAN не может быть сокращен.

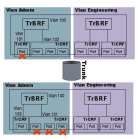
Для получения дополнительной информации обратитесь к Отсечению каналов VTP в Понимании Коммутации Token Ring.

Протокол Duplicate Ring

Протокол Duplicate Ring разработан для работы коммутаторов, которые выполняют Вртуальные локальные сети Token Ring. Его задание должно гарантировать правильную конфигурацию Вртуальных локальных сетей Token Ring и создать Explorer reduction. DRiP использует VTP для синхронизации его информации базы данных VLAN, но это не требуется для DRiP работать (База данных VLAN может быть установлена вручную). Одно неправильное представление состоит в том, что DRiP понимает номера кольца; это неверно. DRiP полагается на уникальность VLAN, настроенных в сети и той Конфигурации базы данных VLAN.

Одна из самых важных функций DRiP должна принудить распределение TrCRF. В мире Token Ring очень опасно распределить любую VLAN кроме 1003 из-за проблем связности. Поэтому, если TrCRF кроме VLAN 1003 распределен, все порты, к которым привязана та VLAN, отключены DRiP.

Данный пример иллюстрирует это понятие:



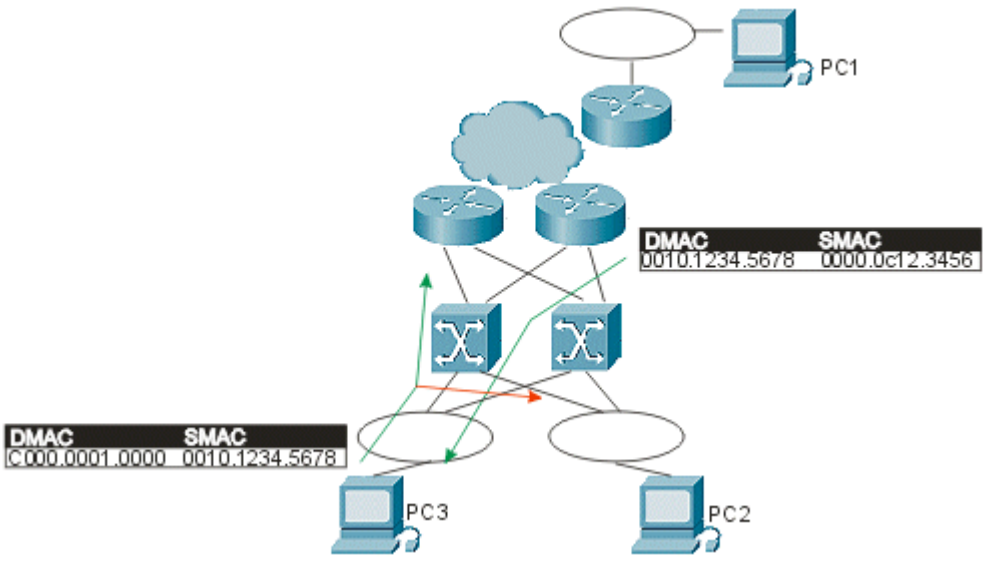
В том примере два других коммутатора имеют порт, который назначен на VLAN 101. Коммутатор, через DRiP, перемещает связующее дерево порта для отключения и останавливает перенаправление трафика. Это охраняет коммутатор против возможного условия зацикливания.

Если нет никакого изменения, DRiP объявляет статус TrCRF ко всем его магистральным портам каждые 30 секунд. Любое изменение, сделанное через CLI (Интерфейс командной строки) или SNMP, сразу передало бы обновление всех портов. Эти рекламные объявления являются кадрами ISL типа 0 и текут на виртуальной локальной сети (VLAN) по умолчанию 1. Поскольку DRiP только объявляет свои эффекты для VLAN, важно, чтобы корректные сведения о виртуальной локальной сети (VLAN) существовали в коммутаторах, которые связаны через ISL. Это сделано через VTP. Если VTP отключен, то эта функция должна быть поддержана вручную через все коммутаторы, которые совместно используют те же VLAN. Рекламные объявления DRiP только существуют на ссылках ISL. Они не существуют на ATM, Token Ring, Ethernet или FDDI. Нет никаких деревьев топологии, сохраненных в DRiP.

Для получения дополнительной информации обратитесь к Протоколу Duplicate Ring в Руководстве Вртуальных локальных сетей Token Ring и Связанных протоколов.

HSRP и вртуальные локальные сети Token Ring

Одной из самых больших проблем с HSRP является использование адреса групповой адресации в сети. Поскольку никто в сети фактически получения пакета с этим виртуальным MAC - адресом, коммутаторы никогда не изучают эти MAC-адреса. Поэтому они переполнение фреймами всюду по сети. Из-за этого использование **функции standby use-bia** HSRP потребовалось, чтобы передавать пакеты, который использовал фиксированный MAC - адрес интерфейса активного маршрутизатора HSRP. Основная проблема с этим сценарием - то, что, когда маршрутизаторы HSRP переключаются, они должны были бы передать Протокол разрешения широковещательного адреса (ARP; предварительный ARP запрос) ко всем станциям на проводе, так, чтобы станции изучили новый MAC-адрес шлюза. Даже при том, что этот процесс должен работать на основе спецификаций IP, были некоторые известные неполадки с ним. Из-за продолжительных запросов от поля был изменен HSRP так, чтобы вы могли иметь адрес групповой адресации и также быть в состоянии использовать HSRP без **standby use-bia**. Это изменение было внедрено в CSCdk55937 и освобождено в программном обеспечении Cisco IOS версии 11.3(7) и 12.0 (3) и позже.

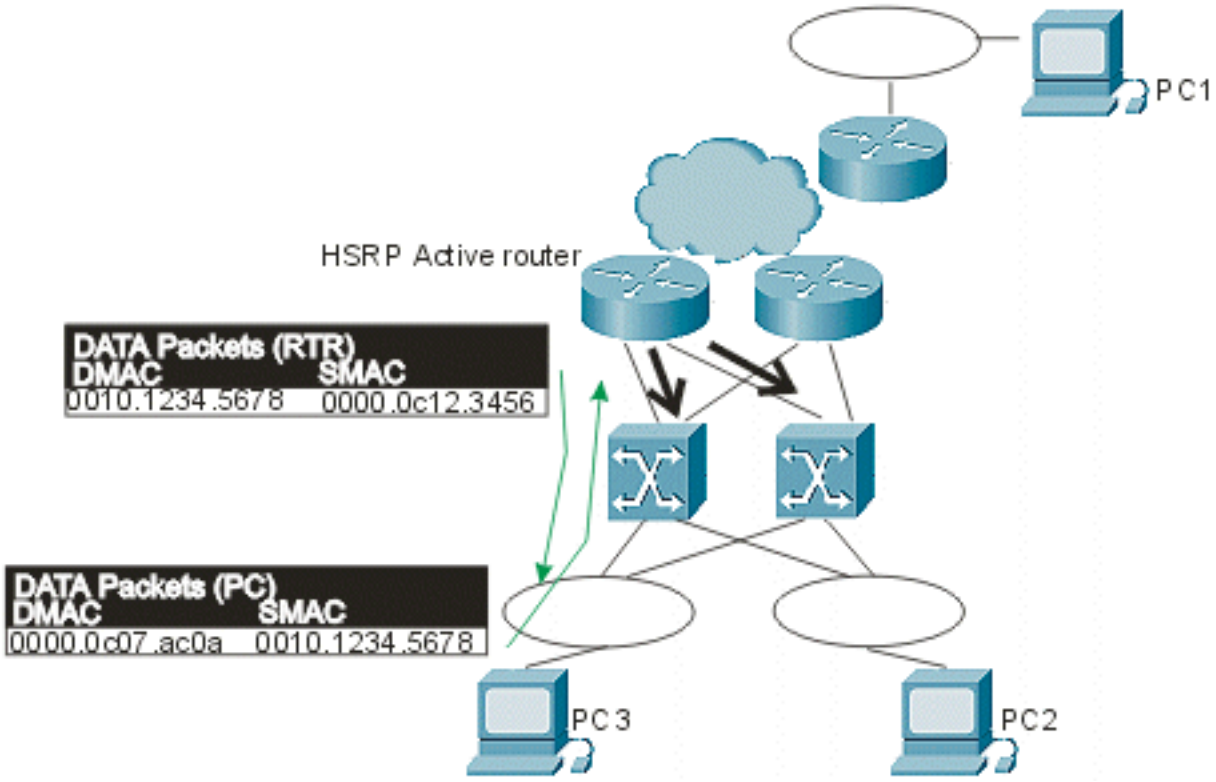


В предыдущей схеме связь происходит между PC1 и PC3. Проблема состоит в том, что IP - трафик от клиента к маршрутизатору по умолчанию в этом изображении использует адрес места назначения групповой адресации. Поскольку никто не может получить этот пакет от того адреса, коммутаторы никогда не изучают этот адрес и всегда лавинно рассылают пакеты. Традиционный DMAC, который зависит от групп, является C000.000X.0000, который никогда не может быть SMAC в Token Ring. Таким образом, все пакеты, предназначенные от PC3 до PC1 через шлюз по умолчанию, теперь замечены PC2. В сети с большим количеством мостов это может умножить очень быстро и вызвать то, что походило бы на широковещательные штормы, но что является фактически большим количеством многоадресного трафика.

Для преодоления этой проблемы необходимо использовать MAC-адрес, который может фактически использоваться в качестве SMAC маршрутизаторами в пакетах приветствия HSRP. Это позволяет коммутаторам изучать этот адрес и, поэтому, коммутировать пакеты соответственно. Чтобы сделать это, настройте новый виртуальный MAC - адрес в маршрутизаторах. Клиенты должны передать пакеты DMAC этого нового виртуального адреса. Это - пример выходных данных от **команды show standby**:

```
vdtl-rsm# show standbyVlan500 - Group 10Local state is Active, priority 100Hellotime 3 holdtime
10Next hello sent in 00:00:01.224Hot standby IP address is 1.1.1.100 configuredActive router is
localStandby router is unknown expiredStandby virtual mac address is 0000.0c07.ac0a
```

В тех выходных данных была создана резервная группа 10 (standby IP 1.1.1.100). MAC-адрес (`0000.0c07.ac0a`) является новым виртуальным MAC - адресом, и последний байт является группой (0xA = 10). Как только у вас есть эта новая конфигурация, у вас теперь была бы эта структура трафика, которая избегает лавинных распространений трафика:



Теперь, потому что маршрутизатор получает пакеты с DMAC Виртуального MAC - адреса HSRP, коммутаторы изучают этот MAC-адрес и только передают пакеты к активному маршрутизатору HSRP. Если сбои активного маршрутизатора HSRP и резерв пойдут активные, то новый активный маршрутизатор начнет передавать пакеты приветствия HSRP с тем же SMAC, который заставляет таблицы MAC-адресов коммутатора переключать свои полученные записи на новый порт коммутатора и транк.

Из-за многокольцевой, дополнительной операции должен вступить в силу, чтобы гарантировать, что RIF фактически изменяется во время перехода (даже при том, что это - тот же MAC-адрес). Многокольцевой возможность маршрутизатора привязать RIF к MAC-адресу, точно так же, как конечная станция. Маршрутизаторам нужно многокольцевой в средах, где мосты SRB существуют, так, чтобы пакеты могли пересечь их для достижения конечных станций.

В том же примере как прежде, вы видите дополнительные шаги, требуемые для клиента соединиться с новым активным маршрутизатором HSRP:

1. Активный маршрутизатор прекращает работать.
2. Как только резервный маршрутизатор обнаруживает потерю пакетов приветствия HSRP, он инициирует процесс для становления активным маршрутизатором HSRP.
3. Маршрутизатор отсылает предварительный ARP запрос от того же SMAC как прежде в обоих из MAC - уровней и в уровне ARP.
4. ПК теперь передает кадр, предназначенный к тому же MAC-адресу, но с новым RIF.
5. Как только маршрутизатор принимает этот кадр (предназначенный к MAC HSRP), это передает запрос ARP клиенту непосредственно, потому что это *не* имеет MAC-адреса того клиента в его таблице ARP.
6. Как только ответ на пакет ARP получен, маршрутизатор может передать пакеты клиенту - получателю.

Дополнительные сведения

- Понимание коммутации Token Ring
- Поддержка коммутаторов
- Поддержка технологии коммутации локальных сетей
- Cisco Systems – техническая поддержка и документация