Best Practices for Catalyst 6500/6000 Series and Catalyst 4500/4000 Series Switches Running Cisco IOS Software

Содержание

Введение

Данный документ содержит рекомендации по работе с коммутаторами серий Catalyst 6500/6000 и 4500/4000, использующими программное обеспечение Cisco IOS® на управляющем модуле Supervisor Engine.

Коммутаторы серий Catalyst 6500/6000 и Catalyst 4500/4000 поддерживают одну из следующих двух операционных систем, под управлением которых работает модуль Supervisor Engine:

- ОС Catalyst OS (CatOS)
- ПО Cisco IOS)

Одновременно с CatOS существует возможность использовать программное обеспечение Cisco IOS на следующих дочерних платах или модулях маршрутизации:

- На плате многоуровневой коммутации (MSFC) коммутатора Catalyst 6500/6000
- На модуле 4232 уровня 3 (L3) коммутатора Catalyst 4500/4000

В таком режиме для настройки существуют две командные строки:

- Командная строка CatOS для коммутации
- Командная строка ПО Cisco IOS для маршрутизации

CatOS является системным программным обеспечением, работающим на модуле Supervisor Engine. Для использования программного обеспечения Cisco IOS, работающего на модуле маршрутизации, требуется системное программное обеспечение CatOS.

При работе с программным обеспечением Cisco IOS для настройки существует только одна командная строка. В таком режиме функции, выполняемые CatOS, интегрированы в ПО Cisco IOS. Результатом интеграции стало существование всего одной командной строки для настройки и коммутации, и маршрутизации. В этом случае программное обеспечение Cisco IOS является системным программным обеспечением и заменяет CatOS.

И система CatOS, и программное обеспечение Cisco IOS используются в важных сетях. CatOS с установленным ПО Cisco IOS для дочерних плат и модулей маршрутизации поддерживается следующими сериями коммутаторов:

- Для Catalyst 6500/6000
- Catalyst 5500/5000
- Catalyst 4500/4000

Следующие серии коммутаторов поддерживают системное программное обеспечение Cisco IOS:

- Для Catalyst 6500/6000
- Catalyst 4500/4000

Для получения информации по CatOS обратитесь к разделу Рекомендации по настройке и управлению коммутаторами серий Catalyst 4500/4000, 5500/5000 и 6500/6000, работающими под управлением CatOS, так как данный документ рассказывает о системном программном обеспечении Cisco IOS.

Системное программное обеспечение Cisco IOS дает пользователю следующие преимущества:

- Единый пользовательский интерфейс
- Унифицированная платформа сетевого управления
- Улучшенные функции QoS
- Поддержка распределенной коммутации

Данный документ структурирован по модулям. Каждый раздел может быть прочитан независимо от другого, а изменения в настройках могут осуществляться поэтапно. При подготовке документа предполагалось, что читатель имеет общее представление о пользовательском интерфейсе программного обеспечения Cisco IOS. В документе не содержится сведений об общей структуре кампусной сети.

Перед началом работы

Общие сведения

Решения, предложенные в данном документе, были разработаны инженерами Cisco, имеющими многолетний опыт в данной области. Они работают со сложными сетями, обслуживают множество крупнейших клиентов. Поэтому в документе делается упор на реальные конфигурации, которые позволяют сетям работать успешно. Данный документ предлагает следующие решения:

- Решения, статистически имеющие самое широкое распространение, а следовательно обеспечивающие наименьший риск
- Простые решения – обеспечивающие некоторую гибкость при достижении определенных результатов
- Решения, которыми легко управлять и которые сможет настроить группа обеспечения работы сети
- Решения, обеспечивающие высокий уровень доступности и стабильности

Ссылки

На сайте Cisco.com есть множество ссылок на сайты, содержащие информацию о линии продуктов Catalyst 6500/6000 и Catalyst 4500/4000. Ссылки, приведенные в этом разделе, содержат углубленную информацию по темам, обсуждаемым в данном документе.

См. Поддержку технологии коммутации LAN для получения дополнительной информации о любой из тем тот этот документ покрытия. Страница поддержки содержит документацию по продуктам, справочные документы по настройке и устранению неполадок.

В данном документе имеются ссылки на общедоступные интерактивные материалы, в которых также можно найти дополнительную информацию. Следующие ссылки также представляют собой хорошие справочные и образовательные материалы:

- Основные элементы Cisco ISP
- Сравнение операционных систем Cisco Catalyst и Cisco IOS для коммутаторов серии Cisco Catalyst 6500
- Коммутация Cisco LAN (серия повышения квалификации сертифицированного специалиста по межсетевому оборудованию Cisco \(CCIE \))
- Построение Cisco многоуровневые коммутируемые сети
- Производительность и защита от ошибок и неисправностей

- БЕЗОПАСНЫЙ: Рекомендации по обеспечению безопасности корпоративной сети
- Руководство по обслуживанию Cisco: Настройка коммутатора Catalyst

Основная конфигурация

В данном разделе рассматриваются функции, применяемые при использовании большинства сетей Catalyst.

Протоколы плоскости управления Catalyst

Этот раздел знакомит с протоколами, действующими между коммутаторами при нормальной работе. Общее представление об этих протоколах будет полезным при изучении каждого раздела.

Трафик модуля Supervisor Engine

Большинство возможностей, включенных в сети Catalyst, требуют взаимодействия двух или более коммутаторов. Поэтому необходимо установить управляемый обмен сообщениями keepalive, параметрами настройки и изменениями управления. Все протоколы — и протоколы Cisco, такие как протокол обнаружения Cisco (CDP), и протоколы, основанные на стандартах, такие как IEEE 802.1d (протокол связующего дерева (STP)) — при реализации на серии Catalyst имеют определенные общие элементы.

При обычной пересылке фреймов фреймы данных пользователя возникают в конечных системах. Адрес источника (SA) и адрес назначения (DA) фреймов данных сохраняются во всех коммутируемых доменах уровня 2 (L2). Таблицы поиска ассоциативной памяти (CAM) каждого модуля управления коммутатора Supervisor Engine заполняются при процессе изучения SA. Эти таблицы показывают, какой выходной порт переслал полученный фрейм. Если назначение неизвестно или фрейм предназначен широковещательным или многоадресным адресам, процесс изучения адресов будет незаконченным. В таком случае фрейм будет разослан на все порты данной сети VLAN. Коммутатор должен также распознать, какие фреймы должны быть коммутированы через систему, а какие – направлены на CPU коммутатора. ЦП коммутатора также называют процессором сетевого управления (NMP).

Для создания плоскости управления Catalyst используются специальные записи в таблице CAM. Такие записи называются системными. Плоскость управления получает и направляет трафик на процессор NMP на порте внутреннего коммутатора. Таким образом с помощью протоколов с известными MAC-адресами назначения трафик управляющей плоскости может быть отделен от трафика данных.

У Cisco есть зарезервированный диапазон MAC-адресов и адресов протоколов для Ethernet. Он приведен в таблице ниже. В данном документе каждый из зарезервированных адресов описывается подробно, но для удобства данные были сведены в таблицу:

Функция	Тип протокола SNAP1 HDLC2	MAC-адрес получателя групповой адресации
PAgP3	0x0104	01-00-0c-cc-cc-cc
PVST+, RPVST+4	0x010b	01-00-0c-cc-cc-cd

Мост VLAN	0x010c	01-00-0c-cd-cd-ce
UDLD5	0x0111	01-00-0c-cc-cc-cc
CDP	0x2000	01-00-0c-cc-cc-cc
DTP6	0x2004	01-00-0c-cc-cc-cc
STP Uplink Fast	0x200a	01-00-0c-cd-cd-cd
Протокол связующего дерева IEEE 802.1d	N/A—DSAP7 42 SSAP8 42	01-80-c2-00-00-00
ISL9	Н/Д	01-00-0c-00-00-00
VTP10	0x2003	01-00-0c-cc-cc-cc
IEEE Pause, 802.3x	N/A—DSAP 81 SSAP 80	01-80-C2-00-00-00> 0F

1 SNAP = протокол доступа к подсети.

2 HDLC = высокоуровневый протокол управления каналом передачи данных.

3 PAgP = протокол агрегирования портов.

4 PVST+ = сеть со связующими деревьями VLAN, RPVST+ = Быстрая сеть PVST+.

5 UDLD = обнаружение однонаправленного канала.

6 DTP = протокол динамического группирования магистралей.

7 DSAP = точка доступа к службе назначения.

8 SSAP = точка доступа к службе источника.

9 ISL = межкоммутаторный канал.

10 VTP = магистральный протокол VLAN.

Большинство протоколов управления Cisco используют инкапсуляцию IEEE 802.3 SNAP, включающую управление логическим каналом (LLC) 0xAAAA03 и организационный уникальный идентификатор (OUI) 0x00000C. Все это можно увидеть в записях анализатора LAN.

Данные протоколы подразумевают подключение точка-точка. Следует учесть, что обдуманное использование адресов назначения многоадресной рассылки позволяет двум коммутаторам Catalyst явно обмениваться информацией через коммутаторы других производителей (не Cisco). Устройства, которые не распознают и не перехватывают фреймы, просто обеспечивают их лавинное распространение. Однако соединения типа точка – многие точки, выполненное с использованием компонентов различных изготовителей, могут продемонстрировать несогласованное поведение. В общем случае необходимо избегать соединений типа точка – многие точки, в которых задействуются компонентов различных изготовителей. Работа этих протоколов прерывается на маршрутизаторах уровня 3, они работают только в пределах домена коммутатора. Специализированная микросхема (ASIC) обработки и планирования входящего трафика назначает этим протоколам приоритет перед пользовательскими данными.

Теперь обратим внимание на SA. Протоколы коммутаторов используют MAC-адреса, полученные из банка доступных адресов. Банк доступных адресов расположен в памяти EPROM на шасси. **Выполните команду show module для отображения диапазона адресов, доступных каждому модулю для генерации трафика, например STP BPDU или фреймов ISL.** Вот примерный результат, который дает выполнение команды:

```
>show module … Mod MAC-Address(es) Hw Fw Sw --- ---------------------------------------- ------ --
-------- ---------------- 1 00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2 6.1(3) 6.1(1d) 00-01-c9-
da-0c-1c to 00-01-c9-da-0c-1 00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff !--- These are the MACs for
sourcing traffic.
```

VLAN 1

VLAN 1 имеет особое значение в сетях Catalyst.

При транкинге Catalyst Supervisor Engine всегда использует VLAN, установленную по умолчанию – VLAN 1 – для сопровождения метками протоколов управления. Среди таких протоколов можно назвать CDP, VTP и PAgP. Все порты коммутатора, содержащие внешний интерфейс sc0, по умолчанию настроены на то, чтобы быть членами VLAN 1. Все магистрали по умолчанию поддерживают VLAN 1.

Следующие определения необходимы для объяснения некоторых распространенных терминов, связанных с сетями Catalyst:

- Управляющая VLAN – это VLAN, в которой находится sc0 для коммутаторов CatOS и низкопроизводительных коммутаторов. Эту VLAN можно сменить. Об этом необходимо помнить при работе с коммутаторами CatOS и Cisco IOS.
- Собственная VLAN – это VLAN, к которой возвращается порт, когда он не работает в транковом режиме. Также собственная VLAN – это немеченая VLAN в магистрали IEEE 802.1Q.

Вот несколько хороших причин, чтобы настроить сеть и изменить поведение портов в сети VLAN 1:

- Если диаметр VLAN 1, как и в случае с любой другой VLAN, становится достаточно большим, чтобы угрожать стабильности, в частности с позиции STP, его нужно сократить. Дополнительную информацию см. в разделе Интерфейс управления коммутаторами и собственная VLAN.
- Необходимо держать данные плоскости управления VLAN 1 отдельно от данных пользователя, так как это позволит упростить устранение неполадок и увеличить число доступных циклов ЦП. При разработке многоуровневых кампусных сетей без STP следует избегать петель уровня 2 во VLAN 1. Для этого необходимо вручную удалять магистральные порты из VLAN 1.

В заключение, следует помнить данную информацию о магистральных каналах:

- Обновления CDP, VTP, и PAgP всегда перенаправляются на магистраль с меткой VLAN 1. Это правило не нарушается, даже если VLAN 1 была удалена с магистралей и не являлась стандартной VLAN. Сброс пользовательских данных во VLAN 1 не влияет на трафик плоскости управления, который по-прежнему отсылается при помощи VLAN 1.
- В магистрали ISL пакеты DTP посылаются на VLAN1. Это правило не нарушается, даже если VLAN 1 была удалена из магистрали и больше не является собственной VLAN. В магистральном канале 802.1Q пакеты DTP передаются по собственной VLAN. Это

правило не нарушается, даже если VLAN была удалена из магистрали.
- Если VLAN 1 не была удалена из магистрали, BPDU 802.1Q IEEE в PVST+ пересылаются немечеными по общему связующему дереву VLAN 1 для обеспечения взаимной совместимости с коммутаторами других производителей. Это происходит независимо от конфигурации стандартной VLAN. Для всех других VLAN BPDU Cisco PVST+ отпарвляются с метками. Дополнительные сведения см. в разделе Протокол связующего дерева.
- BPDU множественных связующих деревьев (MST) 802.1s всегда посылаются на VLAN 1 и по ISL и по 802.1Q магистралям. Это правило не нарушается, даже если VLAN 1 была удалена из магистралей.
- Не следует удалять или отключать VLAN 1 от магистралей между мостами MST и мостами PVST+. В случае отключения VLAN 1 мост MST должен стать корневым, для того чтобы все VLAN избежали размещения в мосту MST их граничных портов в состоянии несогласованности корня. Дополнительные сведения см. в разделе Общие сведения о протоколе множественных связующих деревьев (802.1s).

Стандартные функции

В данном разделе документа рассматриваются основные коммутационные функции, являющиеся общими для любой среды. Эти функции следует настраивать на всех коммутирующих устройствах Catalyst, использующих программное обеспечение Cisco IOS, в клиентской сети.

Транкинговый протокол VLAN

Цель

Домен VTP, который также называют управляющим доменом VLAN, соединен с одним или несколькими соединенными между собой коммутаторами посредствам магистрали, использующей то же имя домена VTP. VTP дает пользователю возможность осуществлять изменения настроек VLAN централизованно на одном или нескольких коммутаторах. VTP автоматически передает изменения всем остальным коммутаторам домена VTP (сети). Можно настроить коммутатор таким образом, что он будет частью только одного домена VTP. Перед созданием VLAN необходимо определить режим VTP, который будет использоваться в сети.

Технологическое описание

VTP представляет собой протокол обмена сообщениями уровня 2. VTP управляет созданием, удалением и переименованием сетей VLAN во всей сети для обеспечения согласованности настроек VLAN. VTP минимизирует ошибки и несогласованности настроек, которые могут привести ко многим проблемам. Например дублированию имен VLAN, неправильным спецификациям типа VLAN и нарушениям безопасности.

По умолчанию коммутатор находится в режиме VTP-сервера и состоянии домена без управления. Эти настройки изменяются, когда коммутатор получает объявление через общедоменный магистральный канал или когда настраивается управляющий домен.

Протокол VTP обеспечивает связь между коммутаторами, используя известный MAC-адрес

назначения многоадресной рассылки Ethernet (01-00-0c-cc-cc-cc) и тип протокола SNAP HDLC 0x2003. Как и другие внутренние протоколы, VTP использует инкапсуляцию IEEE 802.3 SNAP, включающую LLC 0xAAAA03 и OUI 0x00000C. Все это можно увидеть в записях анализатора LAN. VTP не работает через немагистральные порты. Поэтому сообщения не могут быть посланы до тех пор, пока DTP не приведет магистраль в рабочее состояние. Другими словами, VTP является полезной нагрузкой ISL или 802.1Q.

Существуют следующие типы сообщений:

- Сводные оповещения каждые 300 секунд
- Объявления поднабора и объявления запроса при наличии изменений
- Присоединения в случаях, когда включено отсечение VTP

Номер версии конфигурации VTP увеличивается на единицу при каждом изменении на сервере, и эта таблица распространяется по всему домену.

`VLAN , VLAN, inactive`. Схожим образом, если коммутатор в режиме клиента не может при загрузке принять таблицу VTP VLAN (либо с VTP-сервера, либо от другого VTP-клиента), все порты во VLAN, отличных от VLAN 1, включенной по умолчанию, будут отключены.

Большинство коммутаторов Catalyst могут быть настроены на работу в любом из следующих VTP-режимов:

- Сервер. В режиме VTP-сервера можно выполнять следующие действия:Создайте виртуальные LAN (VLAN)Модифицировать сети VLANУдалять сети VLANОпределять другие параметры настройки всего домена VTP, такие как версия VTP и отсечение VTPСерверы VTP сообщают свои настройки VLAN другим коммутаторам того же домена VTP. Серверы VTP также синхронизируют свои настройки VLAN с другими коммутаторами с помощью сообщений, получаемых по магистральным каналам. Режим VTP-сервера является режимом по умолчанию.
- Клиент. VTP-клиенты работают точно так же, как VTP-серверы. Но в режиме VTP-клиента нельзя ни создавать, ни изменять, ни удалять сети VLAN. Более того, клиент не помнит VLAN после перезагрузки, так как информация о VLAN не записывается в NVRAM.
- Прозрачный режим. Коммутаторы, работающие в прозрачном режиме VTP, не участвуют в VTP. В этом режиме коммутаторы не сообщают настроек своей VLAN и не синхронизируют настройки своей VLAN на основании полученных сообщений. Но в VTP 2 коммутаторы, работающие в прозрачном режиме, пересылают сообщения VTP, полученные коммутаторами за пределами их магистральных интерфейсов.

Функция	Сервер	Клиент	Прозрачный	Off 1
Исходные сообщения VTP	Да	Да	Нет	—
Обнаружение сообщений VTP	Да	Да	Нет	—
Создайте виртуальные LAN (VLAN)	Да	Нет	Да (только локальное значение)	—
Помните о	Да	Нет	Да (только	—

виртуальных локальных сетях (VLAN)			локальное значение)	

1 Программное обеспечение Cisco IOS не предусматривает отключение VTP при помощи использования режима off.

Эта таблица содержит общие сведения о начальной конфигурации:

Функция	**Значение по умолчанию**
Vtp domain имя	NULL
Режим VTP	Сервер
Версия VTP	Версия 1 включена
Процедура отсечения каналов в протоколе VTP	Отключенный

При прозрачном режиме VTP обновления VTP просто игнорируются. Известный MAC-адрес многоадресной рассылки VTP удаляется из системы CAM, которая обычно используется для сбора контрольных фреймов и направления их в модуль Supervisor Engine. Так как протокол использует адреса многоадресной рассылки, коммутатор в прозрачном режиме или коммутатор другого производителя просто разошлют фрейм другим коммутаторам Cisco в домене.

Версия 2 VTP (VTPv2) имеет возможности, описанные в списке ниже. Но не имеет возможности взаимодействовать с версией 1 VTP (VTPv1):

- Поддержка Token Ring
- Поддержка нераспознанной информации VTP – коммутаторы пересылают величины, которые они не могут проанализировать.
- Прозрачный режим, зависимый от версии – в прозрачном режиме не проверяется имя домена. Это делает возможной поддержку более чем одного домена через домен в прозрачном режиме.
- Распространение номера версии – если на всех коммутаторах возможен VTPv2, то все коммутаторы могут быть настроены по примеру одного коммутатора.

См. Понимание Транкингового протокола VLAN (VTP) для получения дополнительной информации.

Работа VTP в программном обеспечении Cisco IOS

Изменения конфигурации, вносимые в CatOS, записываются в энергонезависимое ПЗУ сразу после внесения этих изменений. **Программное обеспечение Cisco IOS, наоборот, не сохраняет в NVRAM изменения настроек, если не была выполнена команда copy run start.** Системам клиентов и серверов VTP необходимо немедленное сохранение обновлений с серверов VTP в энергонезависимое ПЗУ без вмешательства пользователя. Требования обновления VTP выполняются при стандартной работе CatOS, но модель обновления в программном обеспечении Cisco IOS требует альтернативной операции обновления.

В виде такой альтернативы в программном обеспечении Cisco IOS для Catalyst 6500 была

представлена база данных VLAN, которая явилась методом немедленного сохранения обновлений для VTP-клиентов и серверов. В некоторых версиях ПО эта база данных VLAN хранится в энергонезависимом ПЗУ в виде отдельного файла с именем vlan.dat. Для того чтобы определить, необходима ли резервная копия базы данных VLAN, необходимо проверить версию программного обеспечения. **Увидеть информацию VTP/VLAN, касающуюся VTP-клиента или VTP-сервера и хранящуюся в файле vlan.dat, можно при помощи команды show vtp status.**

В этих системах при выполнении команды copy run start в файле загрузочной конфигурации NVRAM сохраняются не все настройки VTP/VLAN. Это не относится к системам, работающим в прозрачном режиме VTP. **Такие системы сохраняют все настройки VTP/VLAN в файле загрузочной конфигурации в NVRAM при выполнении команды copy run start.**

В ПО Cisco IOS, выпущенном до Cisco IOS 12.1(11b)E с помощью баз данных VLAN можно только настраивать VTP и VLAN. Режим базы данных VLAN существует отдельно от режима глобальной конфигурации. Причиной для такого требования по конфигурации является то, что при настройке устройства в режиме VTP-сервера или VTP-клиента его VTP-соседи могут динамически обновлять базу данных VLAN с помощью VTP-сообщений. Эти обновления не должны автоматически учитываться в настройке. Поэтому база данных VLAN и информация VTP хранится не в главной конфигурации, а в NVRAM, в файле vlan.dat.

Данный пример показывает, как создать Ethernet VLAN в режиме базы данных VLAN:

```
Switch#vlan database Switch(vlan)#vlan 3 VLAN 3 added: Name: VLAN0003 Switch(vlan)#exit APPLY completed. Exiting....
```

В ПО Cisco IOS 12.1(11b)E и более поздних версий VTP и VLAN можно настраивать при помощи режима базы данных VLAN или режима глобальной конфигурации. В режиме VTP-сервер и в прозрачном режиме настройка VLAN обновляет файл vlan.dat в NVRAM. Однако в конфигурации эти команды не сохраняются. Следовательно, они не влияют на текущую конфигурацию.

Дополнительные сведения см. в разделе Настройка VLAN в режиме глобальной конфигурации документа Настройка VLAN.

Данный пример демонстрирует, как создать Ethernet VLAN в режиме глобальной конфигурации и как проверить ее настройки:

```
Switch#configure terminal Switch(config#vtp mode transparent Setting device to VTP TRANSPARENT mode. Switch(config#vlan 3 Switch(config-vlan)#end Switch# OR Switch#vlan database Switch(vlan#vtp server Switch device to VTP SERVER mode. Switch(vlan#vlan 3 Switch(vlan#exit APPLY completed. Exiting.... Switch#
```

Примечание: Конфигурация VLAN сохранена в файле vlan.dat, который хранится в энергонезависимой памяти. Для того чтобы обеспечить создание полной резервной копии конфигурации, необходимо включить файл vlan.dat в резервную копию вместе с конфигурацией. Затем, если весь коммутатор или модуль Supervisor Engine требуют замены, для полного восстановления конфигурации системный администратор должен загрузить оба эти файла:

- Файл vlan.dat
- Файл конфигурации

VTP и расширенные VLAN

Функция расширенного системного идентификатора используется для поддержки расширенного диапазона идентификации VLAN. Когда функция расширенного системного идентификатора включена, она отключает пул MAC-адресов, используемый для связующего дерева VLAN, и оставляет только один MAC-адрес, идентифицирующий коммутатор. ПО Catalyst IOS 12.1(11b)EX и 12.1(13)E предлагает поддержку функции расширенного системного идентификатора для Catalyst 6000/6500 для приведения VLAN 4096 в соответствие со стандартом IEEE 802.1Q. Эта функция представлена в программном обеспечении Cisco IOS 12.1(12c)EW для коммутаторов Catalyst 4000/4500. Такие сети VLAN разбиты на несколько диапазонов, каждый из которых может быть использован по-разному. Некоторые из этих VLAN при использовании VTP передаются другим коммутаторам сети. VLAN расширенного диапазона не передаются, поэтому они должны настраиваться на каждом сетевом устройстве вручную. Функция расширенного системного идентификатора аналогична функции сокращения MAC-адреса в ОС Catalyst.

В следующей таблице описаны диапазоны VLAN:

VLAN	Диапазон	Использование	Пересылается VTP?
0, 4095	Зарезервированный	Только для системного использования. Использовать или увидеть эти VLAN нельзя.	—
1	Обычный	По умолчанию Cisco. Эти VLAN можно использовать, но нельзя удалять.	Да
2–1001	Обычный	Для VLAN Ethernet. Эти VLAN можно создавать, использовать и удалять.	Да
1002–1005	Обычный	По умолчанию Cisco для FDDI и Token Ring. Удалять VLAN 1002–1005 нельзя.	Да
1006–4094	Зарезервированный	Только для VLAN Ethernet.	Нет

Протоколы коммутатора используют MAC-адреса, взятые из банка доступных адресов, хранящихся в памяти EPROM на шасси как части идентификаторов моста для VLAN, работающих на базе PVST+ и RPVST+. Коммутаторы Catalyst 6000/6500 и Catalyst 4000/4500 поддерживают 1024 или 64 MAC-адреса в зависимости от типа шасси.

Для коммутаторов Catalyst с 1024 MAC-адресами функция расширенного системного идентификатора по умолчанию не включена. MAC-адреса размещены последовательно: первый MAC-адрес диапазона назначен VLAN 1, второй – VLAN 2 и так далее. Это позволяет коммутаторам поддерживать 1024 VLAN, а каждая VLAN использует уникальный

идентификатор моста.

Тип корпуса	Адрес шасси
WS-C4003-S1, WS-C4006-S2	1024
WS-C4503, WS-C4506	641
WS-C6509-E,WS-C6509, WS-C6509-NEB, WS-C6506-E, WS-C6506, WS-C6009, WS-C6006, OSR-7609-AC, OSR-7609-DC	1024
WS-C6513, WS-C6509-NEB-A, WS-C6504-E, WS-C6503-E, WS-C6503, CISCO7603, CISCO7606, CISCO7609, CISCO7613	641

1 Для шасси с 64 MAC-адресами по умолчанию включена функция расширенного системного идентификатора и отключить ее невозможно.

Дополнительные сведения см. в разделе Общие сведения об идентификаторе моста документа Настройка STP и IEEE 802.1s MST.

Для коммутаторов Catalyst с 1024 MAC-адресами включение функции расширенного системного идентификатора позволяет поддерживать 4096 VLAN, работающих под PVST+, или возможность иметь 16 экземпляров MISTP с уникальными идентификаторами без увеличения количества MAC-адресов, необходимых коммутатору. Функция расширенного системного идентификатора уменьшает количество MAC-адресов, необходимых STP, с одного на каждую VLAN или экземпляр MISTP до одного на коммутатор.

На этом рисунке изображен идентификатор моста при отключенной функции расширенного системного идентификатора. Идентификатор моста состоит из 2 байтов, задающих приоритет моста, и 6 байтов MAC-адреса.

Расширенный системный идентификатор модифицирует идентификатор моста протокола связующего дерева BPDU. Исходное 2-байтное поле приоритета разбивается на 2 поля: 4 бита под поле приоритета и 12 битов под расширение идентификатора системы, что позволяет нумеровать Vlan от 0 до 4095.

Чтобы использовать VLAN расширенного диапазона на коммутаторах Catalyst, функция расширенного идентификатора должна быть включена на всех коммутаторах в пределах одного STP домена. Это необходимо для того, чтобы сохранять согласованность корневых расчетов STP для всех коммутаторов. При включенной функции расширенного системного идентификатора приоритет корневого моста умножается на 4096 и к нему прибавляется идентификатор VLAN. Коммутаторы без расширенного системного идентификатора могут неосторожно объявить корневыми, так как они имеют лучшую детализацию в выборе идентификатора своего моста.

Так как рекомендуется сохранять согласованную конфигурацию расширенного системного идентификатора в пределах STP домена, практика задавать расширенный системный идентификатор на всех устройствах сети при внедрении в STP домен нового шасси с 64 MAC-адресами не применяется. Но важно понимать, что когда две системы имеют одинаковый приоритет связующего дерева, то высший приоритет будет иметь система без

расширенного системного идентификатора. Для настройки функции расширенного системного идентификатора используйте следующую команду:

spanning-tree extend system-id

Внутренние VLAN располагаются в возрастающем порядке, начиная с VLAN 1006. Рекомендуется назначать пользовательские VLAN как можно ближе к VLAN 4094, для того чтобы избежать конфликтов между пользовательскими и внутренними VLAN. **Выполните на коммутаторе команду show vlan internal usage, чтобы отобразить все назначенные внутренние VLAN.**

```
Switch#show vlan internal usage VLAN Usage ---- -------------------- 1006 online diag vlan0 1007
online diag vlan1 1008 online diag vlan2 1009 online diag vlan3 1010 online diag vlan4 1011
online diag vlan5 1012 PM vlan process (trunk tagging) 1013 Port-channel100 1014 Control Plane
Protection 1015 L3 multicast partial shortcuts for VPN 0 1016 vrf_0_vlan0 1017 Egress internal
vlan 1018 Multicast VPN 0 QOS vlan 1019 IPv6 Multicast Egress multicast 1020 GigabitEthernet5/1
1021 ATM7/0/0 1022 ATM7/0/0.1 1023 FastEthernet3/1 1024 FastEthernet3/2 ------deleted------
```

В собственном IOS vlan internal allocation policy descending может быть настроено таким образом, что внутренние VLAN будут располагаться в убывающем порядке. CLI-эквивалент программного обеспечения CatOS официально не поддерживается.

vlan internal allocation policy descending

[Рекомендации Cisco по настройке]

VLAN могут быть созданы, когда Catalyst 6500/6000 находится в режиме сервера VTP даже без имени VTP-домена. Прежде чем настраивать VLAN на коммутаторах Catalyst 6500/6000, использующих системное программное обеспечение Cisco IOS, необходимо настроить имя VTP-домена. Настройка в таком порядке обеспечит согласование с другими использующими CatOS коммутаторами Catalyst.

/ VIP VTP . Некоторые клиенты предпочитают простоту управления режимов VTP-клиента и VTP-сервера, несмотря на некоторые рассуждения, изложенные в данном разделе. Мы рекомендуем установить в каждом домене по два коммутатора в режиме сервера (обычно это коммутаторы уровня распределения) для резервирования. Остальные коммутаторы домена необходимо установить в режим клиента. При реализации режима клиент/сервер с использованием VTPv2 необходимо помнить, что в одном VTP-домене всегда принимается старший номер версии. Если коммутатор, работающий в режиме VTP-клиента или сервера, вводится в VTP-домен и номер его версии превышает номера существующих VTP-серверов, то база данных VLAN в пределах VTP-домена будет переписана. Если такое изменение в настройке было совершено по неосторожности и VLAN были удалены, замена может вызвать выход сети из строя. Для того чтобы быть уверенными в том, что клиентские или серверные коммутаторы имеют номер версии конфигурации ниже, чем у сервера, необходимо изменить имя VTP-домена клиента со стандартного на любое другое, а затем снова вернуть стандартное. Такое действие сбрасывает значение версии конфигурации на клиенте в 0.

У возможностей VTP по простому внесению изменений в сети есть "за" и "против".
VTP :

- Такая практика обеспечивает хороший контроль изменений, так как требование модифицировать VLAN на коммутаторе или магистрали должно быть рассмотрено на каждом коммутаторе отдельно.

- Прозрачный режим VTP ограничивает риск ошибки администратора, такой как, например, случайное удаление VLAN. Подобные ошибки могут повлиять на целый домен.
- VLAN могут быть отсечены от магистралей, связанных с коммутаторами, которые не имеют портов в данной VLAN. Это приведет к тому, что лавинная рассылка фреймов станет более эффективной с точки зрения полосы пропускания. Отсечение вручную также имеет уменьшенный диаметр связующего дерева. Дополнительные сведения см. в разделе Протокол динамического группирования магистралей. Настройка VLAN по одному коммутатору также поддерживает такую практику.
- Можно безо всякого риска установить новый коммутатор в сети с более поздней версией VTP и изменить тем самым конфигурацию VLAN всего домена.
- Прозрачный режим VTP программного обеспечения Cisco IOS поддерживается Campus Manager 3.2, являющимся частью CiscoWorks2000. Существовавшее ранее требование иметь хотя бы один сервер в VTP-домене теперь снято.

Команды VTP	**Комментарии**
vtp domain имя	CDP проверяет имя, чтобы предупредить плохую проводку между доменами. Имена доменов учитывают регистры.
vtp mode {server | client | transparent}	VTP работает в одном из трех режимов.
vlan номер_vlan	Эта команда создает VLAN с предусмотренным идентификатором.
switchport trunk allowed диапазон_vlan	Это интерфейсная команда, позволяющая магистралям передавать VLAN там, где это необходимо. По умолчанию это все VLAN.
switchport trunk pruning диапазон_vlan	Это интерфейсная команда, ограничивающая диаметр STP с помощью отсечения вручную, как, например, на магистралях от уровня распределения до уровня доступа, где VLAN не существует. По умолчанию все VLAN являются пригодными для отсечения.

Дополнительные варианты

В средах token ring, для которых крайне рекомендуется использование режимов client/server, использование VTPv2 является обязательным.

В разделе Рекомендации Cisco по настройке данного документа рассказывается о преимуществах отсечения VLAN для уменьшения ненужной лавинной рассылки фреймов.

Команда vtp pruning автоматически отсекает VLAN и прекращает неэффективную лавинную рассылку фреймов там, где они не нужны.

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

В IEEE была создана архитектура, основанная на стандартах, для достижения результатов, похожих на результаты протокола VTP. Являясь частью общего протокола регистрации атрибутов (GARP) 802.1Q, общий протокол регистрации VLAN (GVRP) предоставляет возможности управления сетями VLAN, состоящими из устройств разных производителей. GVRP в данном документе не рассматривается.

Примечание: Программное обеспечение Cisco IOS не имеет VTP режим выключено возможностью, и это только поддерживает VTPv2 и VTPv2 с отсечением.

Автосогласование Fast Ethernet

Цель

Автосогласование – это дополнительная функция стандарта IEEE 802.3u Fast Ethernet (FE). Автосогласование позволяет устройствам автоматически обмениваться информацией о скорости и дуплексных возможностях по каналу. Автосогласование работает на уровне 1 (L1). Данная функция предназначена для портов, расположенных в областях, в которых к сети подключены временные пользователи и устройства. В качестве примера можно назвать коммутаторы и концентраторы уровня доступа.

Технологическое описание

При автосогласовании используется модифицированная версия проверки целостности канала, применяемая в устройствах 10BASE-T для согласования скорости и обмена другими параметрами автосогласования. Тест на целостность стандартного канала 10BaseT называется обычным импульсом канала (NLP). Измененная версия проверки целостности канала для автоматического согласования 10/100 Мбит/с называется импульсом быстрого канала (FLP). Устройства 10BASE-T ожидают группу импульсов, отправляемую каждые 16 (+/- 8) миллисекунд для прохождения проверки целостности канала. FLP для автосогласования со скоростью 10/100 Мбит/с посылает такие группы импульсов каждые 16 (+/-8) миллисекунд и дополнительные импульсы каждые 62,5 (+/-7) микросекунд. Импульсы в последовательности блоков образуют кодовые слова, используемые при обмене данными о совместимости между партнерами во время соединения.

В 10BASE-T импульс соединения посылается, как только включается станция. Это единичный импульс, отправляемый каждые 16 миллисекунд. Устройства 10BASE-T посылают импульс соединения каждые 16 миллисекунд, даже когда канал находится в состоянии бездействия. Такой импульс соединения также называют пульсацией, или NLP.

Устройство 100BASE-T посылает FLP. Этот импульс посылается в виде группы импульсов, а не в виде единичного импульса. Группа импульсов завершается в пределах 2 миллисекунд и снова повторяется каждые 16 миллисекунд. После инициализации устройство передает партнеру по связи 16-битное FLP-сообщение для согласования скорости, дуплексного режима и контроля потока. Такое 16-битное сообщение посылается повторно до тех пор, пока его получение не будет подтверждено партнером по связи.

Примечание: Согласно спецификации IEEE 802.3u, вы не можете вручную настроить одного партнера по соединению связи для полного дуплекса на 100 Мбит/с и все еще автосогласования к полному дуплексу с другим партнером по соединению связи. Попытка настроить одного участника связи на 100 Мбит/с в режиме полный дуплекс, а второго – на автосогласование, приведет к несоответствию дуплексных режимов. Несоответствие дуплексных режимов является результатом того, что один партнер по связи автосогласуется и не видит параметров автосогласования, поступающих от другого партнера по связи. В таком случае первый партнер по связи перейдет в полудуплексный режим.

Все коммутирующие модули Catalyst 6500 Ethernet поддерживают 10/100 Мбит/с и дуплексный или полудуплексный режимы. **Выполните команду show interface capabilities для того, чтобы убедится в том, что данная функциональность существует и на других коммутаторах.**

Одна из основных причин, по которым возникают проблемы с производительностью каналов Ethernet 10/100 Мбит/с, заключается в том, что один порт канала функционирует в полудуплексном, а второй – в дуплексном режиме. Это иногда случается, если один или оба порта на линии связи сброшены, а процесс автосогласования не приводит к одинаковой конфигурации обоих партнеров по связи. То же самое происходит, когда конфигурацию изменяют на одном конце канала, не сделав это на другом конце. Можно избежать звонков в службу поддержки, связанных с производительностью, выполнив следующие действия:

- Создать политику, требующую настройки необходимого поведения для портов всех непередающих устройств
- Применять эту политику вместе с адекватными мерами по контролю изменений

Типичным симптомом возникновения проблем с производительностью является увеличение показаний счетчиков последовательности проверки кадров (FCS), циклического избыточного контроля (CRC), выравнивания или пакетов с недопустимо малой длиной.

При полудуплексном режиме в наличии есть одна принимающая и одна передающая витые пары. Витые пары не могут использоваться одновременно. Устройство не может передавать данные в тот момент, когда существует пакет на стороне получения.

При дуплексном режиме в наличии те же одна принимающая и одна передающая витые пары. Однако тут они могут использоваться одновременно, потому что функции контроля несущей и обнаружения коллизий отключены. Устройство может одновременно передавать и получать данные.

Следовательно, соединение устройств, работающих в разных дуплексных режимах возможно, но на стороне с полудуплексным режимом будет возникать большое количество коллизий, что приведет к снижению производительности. Коллизии будут возникать, потому что устройство, настроенное на полный дуплексный режим, может принимать и отправлять данные одновременно.

Документы, приведенные в данном списке, в подробностях описывают автосогласование. В них поясняется работа автосогласования и предлагаются различные параметры его настройки:

- Устранение неполадок и настройка автоматического согласования соединений Ethernet 10/100/1000 Мбит/с в полудуплексном и дуплексном режимах
- Устранение неполадок коммутаторов Cisco Catalyst, связанных с проблемами

совместимости сетевых плат

Общее заблуждение об автосогласовании состоит в том, что считается возможным вручную настроить одного участника соединения на работу в полнодуплексном режиме на скорости 100 Мбит/с и обеспечить автосогласование дуплексного режима с другим участником. Фактически попытка выполнить это выльется в несогласованность дуплексных параметров. Эта несогласованность станет результатом автосогласования, выполненного одним из партнеров по каналу, когда тот, не увидев параметров автосогласования от другого партнера, по умолчанию устанавливает полудуплексный режим.

Большинство модулей Catalyst Ethernet поддерживают 10/100 Мбит/с и дуплексный/полудуплексный режим. *Вы можете проверить поддержку при помощи команды show interface mod/port capabilities.*

FEFI

Индикация ошибок на удаленной стороне (FEFI) защищает интерфейсы 100BaseFX (оптоволокно) и Gigabit, в то время как автоматическое согласование защищает 100BaseTX (медь) от сбоев физического уровня/передачи сигналов.

Ошибка дальнего конца – это ошибка канала, которую одна станция может обнаружить, а другая – нет. Примером может быть отключенный провод передачи. В этом примере отправляющая станция продолжает получать достоверные данные и определять, что канал исправен, с помощью монитора целостности канала. Однако отправляющая станция не может определить, что другая станция передаваемых данных не получает. 100BASE-FX, , IDLE, . FEFI-IDLE. FEFI-IDLE (ErrDisable). Дополнительную информацию о защите от ошибок см. в разделе Обнаружение однонаправленного канала данного документа.

Следующие модули/аппаратное обеспечение поддерживают FEFI:

- Catalyst 6500/6000 и 4500/4000:Все модули 100BASE-FX и модули GE

Рекомендации Cisco по инфраструктуре портов

Выбор действия – настроить автосогласование на скорости 10/100 Мбит/с или аппаратно запрограммировать скорость и дуплексную организацию – зависит от партнера по каналу или от конечного устройства, подключенного к коммутатору Catalyst. Автоматическое согласование между оконечными устройствами и коммутаторами Catalyst обычно функционирует надлежащим образом, и коммутаторы Catalyst соответствуют спецификации IEEE 802.3u. Тем не менее, если коммутаторы сетевой интерфейсной платы или другого производителя не точно соответствуют техническим требованиям IEEE 802.3u, то могут возникнуть проблемы. К тому же, расширенные функции, предлагаемые другим производителем и не описанные в спецификации IEEE 802.3u для автоматического согласования 10/100 Мбит/с, могут вызвать несовместимость аппаратного обеспечения и другие проблемы. Под расширенными функциями подразумеваются, например, автоматическая полярность и целостность кабельного соединения. В данном документе рассматривается следующий пример:

- Оповещение при эксплуатации: Проблемы производительности с подключением плат NIC Intel Pro/1000T к CAT4K/6K

В некоторых ситуациях может потребоваться настроить узел, скорость порта и дуплексный

режим. Выполните следующие основные шаги по поиску и устранению неисправностей:

- Убедитесь, что автоматическое согласование настроено на обеих сторонах канала или аппаратно запрограммировано на обеих сторонах.
- Проверьте примечания к выпуску ПО на предмет стандартных предупреждений.
- Проверьте версию используемых драйвера NIC или операционной системы. Часто требуется самый последний драйвер или набор исправлений.

Как правило, сначала необходимо использовать автосогласование для любого типа партнеров по каналу. Существуют очевидные преимущества настройки автосогласования на передающих устройствах, таких как переносные ПК. Автосогласование также хорошо работает с другими устройствами, например:

- С фиксированными устройствами, такими как серверы и стационарные рабочие станции
- Между коммутатором и коммутатором
- Между коммутатором и маршрутизатором

Но по ряду причин, упомянутых в данном документе, могут возникнуть проблемы согласования. Способы поиска и устранения неисправностей в таких случаях см. в разделе Устранение неполадок и настройка автоматического согласования Ethernet 10/100/1000 Мбит/с в полудуплексном и дуплексном режимах.

Необходимо отключать автосогласования для:

- Портов, поддерживающих устройства сетевой инфраструктуры, такие как коммутаторы и маршрутизаторы
- Других фиксированных конечных систем, таких как серверы и принтеры

Для таких портов настройки скорости и дуплексного режима всегда должны быть аппаратно запрограммированы.

Вручную настройте для этих 10/100 Мбит/с каналов, обычно использующих полнодуплексный режим и 100 Мбит/с, режим скорости и дуплексный режим:

- Коммутатор - коммутатор
- Коммутатор сервер
- Коммутатор маршрутизатор

Если для скорости порта установлено значение auto на порте Ethernet со скоростью 10/100 Мбит/с, скорость и параметры дуплексной передачи согласуются автоматически. Для того чтобы перевести порт в режим auto, необходимо выполнить интерфейсную команду:

```
Switch(config)#interface fastethernet slot/port Switch(config-if)#speed auto !--- This is the default.
```

Выполните следующие интерфейсные команды, для того чтобы настроить дуплексный режим и скорость:

```
Switch(config)#interface fastethernet slot/port Switch(config-if)#speed {10 | 100 | auto}
Switch(config-if)#duplex {full | half}
```

Рекомендации по портам доступа Cisco

Конечные пользователи, мобильные сотрудники и транзитные узлы нуждаются в автосогласовании для минимизации управления этими узлами. Можно организовать автосогласование с коммутаторами Catalyst. Часто требуются последние драйверы NIC.

Для того чтобы активизировать автосогласование скорости для порта, выполните следующие глобальные команды:

```
Switch(config)#interface fastethernet slot/port Switch(config-if)#speed auto
```

Примечание: При установке скорости порта в автоматическое включение 10/100-Mbps Порт Ethernet обе скорости и дуплексных режима автосогласованы. Изменить режим дуплексной передачи портов с автосогласованием нельзя.

Если коммутаторы NIC или другого производителя не точно соответствуют техническим требованиям IEEE 802.3u, то могут возникнуть проблемы. К тому же, расширенные функции, предлагаемые другим производителем и не описанные в спецификации IEEE 802.3u для автоматического согласования 10/100 Мбит/с, могут вызвать несовместимость аппаратного обеспечения и другие проблемы. Под расширенными функциями подразумеваются, например, автоматическая полярность и целостность кабельного соединения.

Дополнительные варианты

Когда между коммутаторами отключено автосогласование, индикация некоторых ошибок уровня 1 может быть нарушена. Для усиления обнаружения ошибок необходимо использовать протоколы уровня 2, например агрессивное UDLD.

Автосогласование даже во включенном состоянии не может выявить следующие проблемы:

- Порт завис и не получает или не передает данные
- Один конец канала находится в рабочем состоянии, а другой – в нерабочем
- Волоконные кабели соединены неверно

Автосогласование не выявляет подобные проблемы, потому что они не являются проблемами физического уровня. Эти проблемы могут привести к появлению STP-петель или «черных дыр» трафика.

Если UDLD настроено на обоих концах канала, оно способно выявить все подобные случаи и отключить в результате ошибки оба порта канала. Таким образом, UDLD предотвращает появление STP-петель или «черных дыр» трафика.

Автосогласование Gigabit Ethernet

Цель

Процедура автосогласования Gigabit Ethernet (GE) является более развернутой, чем процедура, используемая для 10/100 Мбит/с Ethernet (IEEE 802.3z). На GE-портах автосогласование используется для обмена:

- Параметрами управления потоком
- Информацией об удаленных ошибках
- Дуплексной информацией**Примечание:** Порты GE серий Catalyst только поддерживают полностью дуплексный режим.

IEEE 802.3z был заменен спецификацией IEEE 802.3:2000. См. Локальные и Общегородские сети + Проекты (LAN/MAN 802 с) Подписка на стандарты для получения дополнительной информации.

Технологическое описание

В отличие от автосогласования на 10/100 Мбит/с FE, автосогласование GE не включает согласования скорости порта. **Также для отключения автосогласования нельзя использовать команду set port speed.** Согласование для портов GE включено по умолчанию, а у портов по обеим сторонам соединения GE должны быть одинаковые настройки. Канал не будет работать, если порты на разных его концах будут настроены по-разному, так как при этом параметры обмена будут отличаться.

Например, пусть существуют два устройства: A и B. Для каждого из них автосогласование может быть включено или отключено. Ниже приведена таблица их возможных настроек и соответствующих этим настройкам состояний канала:

Negotiation	B включено	B отключен
Включен A	`up`	`A down, B up`
A недоступен	`A up, B down`	`up`

В GE синхронизация и автосогласование (если они включены) выполняются при включении соединения посредством использования специальной последовательности из зарезервированных для соединения кодовых слов.

Примечание: Существует словарь допустимых слов, но не все возможные слова действуют в GE.

Существование соединения GE можно охарактеризовать следующим образом:

Потеря синхронизации означает, что MAC обнаруживает отключение соединения. Потеря синхронизации применяется вне зависимости от состояния автосогласования. Потеря синхронизации происходит в определенных условиях при возникновении неисправностей, таких как получение трех недопустимых слов подряд. `10 , link_down.` После потери синхронизации для восстановления синхронизации необходимо возникновение трех последовательных действительных состояний бездействия. Другие неблагоприятные события, как, например, потеря сигнала приема (Rx), приводит к отключению соединения.

Автоматическое согласование составляет часть процесса установления соединения. Когда соединение установлено, процесс автоматического согласования прекращается. Однако коммутатор продолжает отслеживать состояние соединения. Если в порту автосогласование отключено, фаза autoneg не будет существовать.

Спецификация GE медь (1000BASE-T) поддерживает автосогласование через функцию Next Page Exchange. Next Page Exchange делает возможным автосогласование 10/100/1000 Мбит/с по скорости для медных портов.

Примечание: Однако спецификация матрицы GE только делает условия для согласования дуплекса, управления потоками и удаленного обнаружения ошибок. Порты оптоволоконного GE не выполняют согласование скорости портов. Дополнительные сведения по автосогласованию см. в разделах 28 и 37 спецификации IEEE 802.3-2002 .

Задержка повторного запуска синхронизации представляет собой программную функцию, которая управляет общим временем автоматического согласования. Если за это время синхронизация не проходит успешно, в случае зависания микропрограмма перезапускает автосогласование. **При включенном автосогласовании только команда sync-restart-delay**

является эффективной.

Рекомендации Cisco по инфраструктуре портов

Конфигурация автосогласования в среде GE является более критичным фактором, нежели в среде 10/100 Мбит/с. Автосогласование рекомендуется отключать только в следующих ситуациях:

- Порты коммутатора подключены к устройствам, не поддерживающим согласование
- Из-за проблем взаимной совместимости возникают проблемы соединения

Согласование Gigabit должно быть включено на всех каналах коммутатор–коммутатор и в общем на всех устройствах GE. Автосогласование является режимом по умолчанию на интерфейсах Gigabit. Однако все таки стоит выполнить следующую команду для того, чтобы убедиться, что автосогласование включено:

```
switch(config)#interface type slot/port switch(config-If)#no speed !--- This command sets the port to autonegotiate Gigabit parameters.
```

Существует одно известное исключение: когда осуществляется подключение к маршрутизирующему коммутатору Gigabit (GSR), использующему программное обеспечение Cisco IOS, версия которого была выпущена раньше, чем выпуск ПО Cisco IOS 12.0(10)S, так как именно к этому выпуску были добавлены контроль потока и автосогласование. В таком случае эти две функции необходимо отключить. Если они не будут отключены, порты коммутатора будут сообщать о том, что они не подключены, а GSR будет сообщать об ошибках. Ниже приведен пример последовательности интерфейсных команд:

```
flowcontrol receive off flowcontrol send off speed nonegotiate
```

Рекомендации по портам доступа Cisco

С тех пор как FLP производится разными производителями, соединения коммутатор–сервер должны проверяться индивидуально. Клиенты Cisco обнаружили некоторые проблемы с согласованием Gigabit на серверах Sun, HP и IBM. Необходимо, чтобы все устройства использовали автосогласование Gigabit, если иное не предусмотрено специальными указаниями производителя NIC.

Дополнительные варианты

Контроль потока является дополнительной частью спецификации 802.3x. Контроль потока, если он используется, должен согласовываться. Устройства могут иметь или не иметь возможность отправлять и отвечать на фрейм PAUSE (хорошо известный MAC 01-80-C2-00-00-00 0F). И они могут не соглашаться на запрос контроля потока данных от соседа на дальнем конце линии связи. Порт с буфером ввода, который начинает заполняться, посылает фрейм PAUSE своему партнеру по каналу. Партнер по каналу прекращает передачу и задерживает все дополнительные фреймы в буферах вывода партнера по каналу. Эта функция не решает никаких установившихся проблем избыточной подписки. Но эта функция эффективно увеличивает с помощью пакетов объем буфера ввода за счет части буфера вывода партнера.

Функция PAUSE разработана для предотвращения ненужного отброса устройствами фреймов (коммутаторами, маршрутизаторами или конечными станциями) по причине

переполнения буфера, которое вызвано кратковременной перегрузкой трафиком. Устройство, подвергающееся перегрузке трафиком, предотвращает переполнение внутреннего буфера, посылая фрейм PAUSE. Фрейм PAUSE содержит параметр, указывающий партнеру в режиме полнодуплексной передачи, сколько времени он должен подождать, прежде чем отправлять следующие фреймы данных. Партнер, получивший фрейм PAUSE, перестает отправлять данные в течение указанного периода времени. Когда это время истекает, станция начинает снова посылать фреймы данных, начиная с того места, на котором она приостановила пересылку.

Станция, передавшая фрейм PAUSE, может передать другой фрейм PAUSE, содержащий нулевой параметр времени. Такое действие отменит остаток периода паузы. Таким образом, вновь полученный фрейм PAUSE переопределит любую операцию PAUSE, выполняющуюся в этот момент. Также станция, отправившая фрейм PAUSE, может увеличить период действия PAUSE. Для этого она должна отправить новый фрейм PAUSE, содержащий ненулевой параметр времени, до того как истечет время действия предыдущего фрейма PAUSE.

Такая операция PAUSE не является контролем потока на основании скорости. Эта операция представляет собой простой механизм остановки и возобновления, который позволяет устройству, получающему трафик и посылающему фрейм PAUSE, уменьшить наполнение своего буфера.

Наилучшими объектами использования данной функции являются порты доступа и конечные узлы, для которых выходной буфер узла потенциально является настолько же большим, насколько велика виртуальная память. Использование связи между коммутаторами ограниченные преимущества.

Выполните следующие интерфейсные команды для того, чтобы проверить эту функцию на портах коммутатора:

```
flowcontrol {receive | send} {off | on | desired} >show port flowcontrol Port Send FlowControl
Receive FlowControl RxPause TxPause admin oper admin oper ----- -------- -------- -------- -----
--- ------- ------- 6/1 off off on on 0 0 6/2 off off on on 0 0 6/3 off off on on 0 0
```

Примечание: `PAUSE` `Catalyst.` Некоторые модули (например, WS-X5410 и WS-X4306) никогда не посылают фреймы паузы даже если по причине согласования они должны это сделать, потому что эти модули являются неблокируемыми.

Динамический транкинговый протокол (Dynamic Trunking Protocol)

Цель

Для расширения VLAN между устройствами магистрали временно идентифицируют и маркируют (локальный канал) исходные фреймы Ethernet. Благодаря этому действию, фреймы смогут быть мультиплексированы через один канал. При этом также обеспечивается использование отдельных доменов широковещательной рассылки и доменов безопасности VLAN в коммутаторах. Таблицы CAM позволяют фрейму сопоставить VLAN внутри коммутатора.

Технологическое описание

DTP – это второе поколение динамического ISL (DISL). DISL поддерживал только ISL. DTP

поддерживает и ISL и 802.1Q. Этот факт дает уверенность в том, что коммутаторы на обоих концах магистрали согласуют различные параметры фреймов магистрали. Такие параметры включают:

- Настроенный тип инкапсуляции
- Native VLAN
- Аппаратные возможности

Оддержка DTP также помогает защитить от лавинной рассылки меченых фреймов немагистральными портами, которые представляют собой серьезную потенциальную угрозу безопасности. DTP защищает от подобной лавинной рассылки благодаря обеспечению согласованного состояния портов и соседних узлов.

Режим транкинга

DTP представляет собой протокол уровня 2, согласующий параметры конфигурации между портом коммутатора и его соседями. DTP использует другой хорошо известный MAC-адрес многоадресной рассылки 01-00-0c-cc-cc-cc и тип протокола SNAP 0x2004. В данной таблице описаны функцию каждого из возможных режимов согласования DTP:

Режим	Функция	DTP-фреймы переданы?	Конечное состояние (локальный порт)
Dynamic Auto (эквивалентный режиму Auto в CatOS)	Порт становится готов к преобразованию канала в магистраль. , "on" "desirable".	Да, периодически	Trunking
Trunk (эквивалентный режиму ON в CatOS)	, . Порт становится магистральным портом, даже если соседний порт не согласен на это изменение.	Да, периодически	,
Nonegotiate	trunking, DTP-. Для того чтобы установить магистральный канал, необходимо вручную настроить соседний порт как магистральный. Этот метод удобно использовать в устройствах, которые не поддерживают DTP.	Нет	,
Dynamic desirable	Заставляет порт активно	Да,	trunki

(CatOS сопоставимой командой является desirable),	пытаться преобразовать канал в магистральный канал. , "on", "desirable" "auto".	периодически	ng, on, auto desirable.
Access	non-trunking, , , . Порт становится немагистральным портом, даже если соседний порт не согласен на это изменение.	, , on.	Non-trunking

Примечание: ISL и тип инкапсуляции 802.1Q могут быть установлены или выполнены согласование.

При стандартной настройке DTP допускает следующие характеристики канала:

- Соединения точка–точка и устройства Cisco поддерживают порты магистрали 802.1Q, которые бывают только двухточечными.
- Во время DTP согласования порты не будут участвовать в протоколе STP. Порт будет добавлен к STP только после того, как станет портом одного из следующих трех типов:ДоступISL802.1QPAgP – это следующий процесс, который должен пройти порт, прежде чем он начнет участвовать в STP. PAgP используется для автосогласования EtherChannel.
- На магистральном порту всегда присутствует VLAN 1. Если порт является магистральным портом в режиме ISL , DTP-пакеты посылаются в VLAN 1. Если порт является немагистральным портом в режиме ISL, DTP пакеты посылаются в собственную VLAN (правило работает для магистральных или немагистральных портов 802.1Q).
- DTP-пакеты переносят доменное имя VTP, параметры конфигурации магистрали и статус администратора. Доменное имя VTP должно быть соответствующим для того, чтобы привести согласующуюся магистраль в рабочее состояние. Эти пакеты отправляются каждую секунду во время согласования и каждые 30 секунд после согласования. auto desirable DTP- 5 , .

Внимание. : Необходимо понять, что , nonegotiate и явно задают, в котором состоянии заканчивается порт. Неправильная настройка может привести к опасному или несовместимому состоянию, когда одна сторона выполняет транкинг, а другая – нет.

Дополнительные сведения по ISL см. в документе Настройка магистральных каналов ISL в коммутаторах семейства Catalyst 5500/5000 и 6500/6000. Дополнительные сведения по 802.1Q см. в документе Создание магистральных каналов между коммутаторами Catalyst серий 4500/4000, 5500/5000 и 6500/6000 с использованием инкапсуляции 802.1Q с системным ПО Cisco CatOS.

Тип инкапсуляции

Практический обзор связей между коммутаторами (ISL)

ISL – это собственный транкинговый протокол Cisco (схема маркировки VLAN). ISL использовался много лет. 802.1Q, напротив, гораздо новее, но 802.1Q представляет стандарт IEEE.

ISL полностью инкапсулирует исходный фрейм по двухуровневой схеме маркировки. Таким образом, ISL – это эффективный туннельный протокол и, что является его дополнительным преимуществом, он переносит фреймы не Ethernet. В стандартный кадр Ethernet ISL добавляет 26-битовый заголовок и 4-битовую последовательность проверки кадров (FCS). Большие фреймы Ethernet ожидаются и обрабатываются портами, настроенными как магистрали. ISL поддерживает 1024 сети VLAN.

Формат фрейма – ISL-метка затенена

Дополнительные сведения см. в разделе Формат фрейма соединения между коммутатором и IEEE 802.1Q.

Технологическое описание 802.1Q

Хотя стандарт IEEE 802.1Q принадлежит только Ethernet, этот стандарт включает гораздо больше, чем типы инкапсуляции. 802.1Q включает среди других общих протоколов регистрации атрибутов (GARP) улучшения связующего дерева и маркировку 802.1p QoS. См. Стандарты IEEE Онлайн для получения дополнительной информации

Формат фрейма 802.1Q защищает исходные Ethernet SA и DA. Однако теперь коммутаторы должны ожидать получения фреймов baby-giant, даже на портах доступа, узлы которых могут использовать маркировку, чтобы обозначить приоритет пользователя 802.1p для QoS сигнализации. Метка состоит из 4 байт. Фреймы 802.1Q Ethernet v2 состоят из 1522 байт, что является достижением рабочей группы IEEE 802.3ac. 802.1Q также поддерживает пространство нумерации для 4096 VLAN.

Все передаваемые и получаемые фреймы данных маркированы 802.1Q, кроме тех, которые находятся в собственной VLAN. Для этого случая существует скрытая метка, основывающаяся на настройке входного порта коммутатора. В собственной VLAN фреймы всегда передаются немечеными и получают их тоже обычно немечеными. Однако такие фреймы тоже могут быть получены меченными.

Дополнительные сведения см. в следующих документах:

- Возможность взаимодействия VLAN
- Группирование магистралей между Catalyst 4500/4000, 5500/5000, и 6500/6000 Series Switches с использованием инкапсуляции 802.1Q с системным ПО Cisco CatOS

Формат фрейма 802.1Q/802.1p

Рекомендации Cisco по настройке

Первичной целью разработок Cisco является добиваться устойчивости сети там, где эта устойчивость возможна. Все новейшие продукты Catalyst поддерживают 802.1Q, а некоторые, такие как ранее созданные модули серий Catalyst 4500/4000 и Catalyst 6500, поддерживают только 802.1Q. Поэтому все новые разработки должны следовать стандарту IEEE 802.1Q, а более старые сети должны постепенно уходить от ISL.

Для того чтобы включить на определенном порту транкинг 802.1Q, выполните следующие интерфейсные команды:

```
Switch(config)#interface type slot#/port# Switch(config-if)#switchport !--- Configure the interface as a Layer 2 port. Switch(config-if)#switchport trunk encapsulation dot1q
```

Стандарт IEEE позволяет обеспечить совместимость с устройствами других производителей. Взаимодействие с продукцией других производителей является преимуществом в любой среде Cisco, поскольку появляются новые NIC и устройства, работающие с новым хостом 802.1p. Хотя и ISL и 802.1Q разработки являются надежными, стандарт IEEE в конечном счете является более распространенным и имеет большее количество поддерживаемых сторонних устройств, например, этот стандарт поддерживает сетевые анализаторы. Также, хотя это и является незначительным отличием, стандарт 802.1Q имеет более низкую степень инкапсуляции, чем ISL.

Наконец, скрытая маркировка в собственных VLAN обеспечивает безопасность. Передача фреймов из одной VLAN, VLAN X, в другую VLAN, VLAN Y, без маршрутизатора возможна. Передача может осуществляться без маршрутизатора, если исходный порт (VLAN X) находится в той же VLAN, что и собственная VLAN магистрали 802.1Q на том же коммутаторе. Альтернативный прием – использовать модель VLAN вместо собственной VLAN магистрали.

Для того чтобы установить на определенном порту VLAN как собственную (по умолчанию) для транкинга 802.1Q, выполните следующий интерфейсные команды:

```
Switch(config)#interface type slot#/port# Switch(config-If)#switchport trunk native vlan 999
```

Так как все новейшее аппаратное обеспечение поддерживает 802.1Q, необходимо, чтобы все новые разработки следовали стандарту IEEE 802.1Q, а ранее спроектированные сети постепенно отказывались от ISL. До сих пор многие модули Catalyst 4500/4000 не поддерживают ISL. Тем не менее, 802.1Q представляет собой единственную функцию для транкинга Ethernet. **См. выходные данные команды show interface capabilities или команды show port capabilities для CatOS.** Так как поддержка транкинга требует соответствующего аппаратного обеспечения, модуль, не поддерживающий 802.1Q, никогда не сможет поддерживать 802.1Q. Модернизация программного обеспечения не приводит к появлению поддержки 802.1Q. Самое новое оборудование для коммутаторов Catalyst 6500/6000 и Catalyst 4500/4000 поддерживает и ISL, и 802.1Q.

Если VLAN 1 удалена из магистрали, как описано в разделе Интерфейс управления коммутаторами и собственная VLAN, хотя никакие данные пользователя не передаются и не получаются, NMP продолжает передавать протоколы управления в VLAN 1. Примерами протоколов управления являются CDP и VTP.

Также, как обсуждалось в разделе VLAN 1, пакеты CDP, VTP и PAgP всегда отсылаются на VLAN 1 при транкинге. Если изменилась собственная VLAN коммутатора, то при использовании инкапсуляции dot1Q эти контрольные фреймы будут маркированы VLAN 1. Если включен транкинг dot1q на маршрутизатор и собственная VLAN коммутатора изменилась, необходим подинтерфейс в VLAN 1, чтобы принимать меченные фреймы CDP и обеспечивать видимость соседей CDP на маршрутизаторе.

Примечание: Существует потенциальная угроза безопасности с dot1q, который вызывает неявная маркировка собственного VLAN. Передача фреймов из одной VLAN в другую без маршрутизатора может быть возможной. См. часто задаваемые вопросы Обнаружения несанкционированного доступа для получения дальнейшей информации. Обойти это можно при помощи идентификатора VLAN для собственной виртуальной локальной сети магистрального канала, которая не используется для доступа конечных пользователей. Для достижения этого большинство клиентов Cisco просто оставляют VLAN 1 собственной VLAN магистрали и назначают портами доступа к VLAN порты, не принадлежащие VLAN 1.

Cisco dynamic desirable . Этот режим является режимом по умолчанию. ,
, up . on, , . , desirable , trunk.

Если тип инкапсуляции согласуется между коммутаторами при помощи DTP, а ISL по умолчанию выбирается победителем, если оба конца канала поддерживают его, то для того, чтобы указать dot1q1, необходимо выполнить следующую интерфейсную команду:

switchport trunk encapsulation *dot1q*
1 Некоторые модули, такие как WS-X6548-GE-TX и WS-X6148-GE-TX, не поддерживают транкинг ISL. *Эти модули не примут команду switchport trunk encapsulation dot1q.*

Примечание: Выполните команду **switchport mode access** для отключения транков на порту. Это отключение помогает избежать затрат времени на согласование, когда порты хоста активизируются.

Switch(config-if)#**switchport host**

Дополнительные варианты

dynamic desirable (dynamic auto) . Некоторые коммутаторы, такие как Catalyst 2900XL, маршрутизаторы Cisco IOS и устройства других производителей, в настоящее время не поддерживают магистральное согласование при помощи DTP. nonegotiate, . Этот режим может помочь стандартизировать все настройки в кампусе до общих.

Cisco nonegotiate Cisco IOS. **На протяжении моста некоторые фреймы DTP, полученные от порта, настроенного командой switchport mode trunk, могут возвращаться в порт магистрали.** После получения DTP-фрема порт коммутатора пытается выполнить повторное ненужное согласование. , down, – up. nonegotiate, DTP.

switch(config)#**interface type** *slot#/port#* switch(config-if)#**switchport mode dynamic desirable** *!--- Configure the interface as trunking in desirable !--- mode for switch-to-switch links with multiple VLANs. !--- And...* switch(config-if)#**switchport mode trunk** *!--- Force the interface into trunk mode without negotiation of the trunk connection. !--- Or...* switch(config-if)#**switchport nonegotiate** *!--- Set trunking mode to not send DTP negotiation packets !--- for trunks to routers.* switch(config-if)#**switchport access vlan** *vlan_number !--- Configure a fallback VLAN for the interface.* switch(config-if)#**switchport trunk native vlan 999** *!--- Set the native VLAN.* switch(config-if)#**switchport trunk allowed vlan** *vlan_number_or_range !--- Configure the VLANs that are allowed on the trunk.*

Протокол связующего дерева

Цель

Связующее дерево поддерживает среду уровня 2, исключающую зацикливание, в резервных коммутаторах и мостах сети. Без использования STP фреймы зацикливаются или размножаются неопределенным образом. Это вызывало бы критическую перегрузку сети, так как все устройства широковещательного домена прерывались бы интенсивным трафиком.

STP является ранним протоколом, разработанным для низкоскоростных программных спецификаций мостовых соединений (IEEE 802.1D). Однако STP может быть усложнен для применения его в крупных коммутируемых сетях, имеющих:

- Большое количество VLAN
- Большое количество коммутаторов в домене

- Обслуживание у нескольких поставщиков
- Новейшие разработки IEEE

Cisco IOS System Software занимается разработкой нового STP. Новые стандарты IEEE, включающие протоколы 02.1w Rapid STP и 802.1s Multiple Spanning Tree, обеспечивают быструю сходимость, распределение нагрузки и масштабирование плоскости управления. К тому же, улучшенные функции STP, такие как RootGuard, фильтрация BPDU, защита BPDU Portfast и Loopguard, обеспечат дополнительную защиту от возникновения петель на уровне 2.

Технологическое описание PVST+ Operational Overview

В выборах корневого моста VLAN побеждает коммутатор с наименьшим корневым идентификатором моста (BID). BID — это приоритет моста, объединенный с MAC-адресом коммутатора.

Изначально BPDU, содержащие BID каждого коммутатора и путь к нему, посылаются из всех портов. Это активизирует определение корневого моста и наименьшей нагрузки пути к корню. Дополнительные параметры настройки, передаваемые при помощи BPDU с корневого порта, переопределяют параметры, настроенные локально, благодаря чему вся сеть использует согласованные таймеры. Для каждого BPDU, полученного коммутатором с корневого порта, создается, обрабатывается центральным NMP и высылается новый BPDU с информацией корневого порта.

Для обеспечения схождения топологии выполняются следующие действия:

1. Для всего домена связующего дерева выбирается один корневой мост.
2. На каждом некорневом мосту выбирается один корневой порт (лицевой мост корневого узла).
3. Указанный порт выбран для пересылки BPDU в каждом сегменте.
4. Неуказанные порты блокируются.

Дополнительные сведения см. в следующих документах:

- Настройка STP и IEEE 802.1s MST
- Общие сведения о протоколе Rapid STP (802.1w)

Основные стандартные таймеры	**Name**	**Функция**
2 сек	hello	Контролирует отправку BPDU.
15 сек.	задержка передачи (Fwd delay)	, listening learning .
20 сек.	max age	Контролирует, как долго коммутатор будет поддерживать текущую

		топологию перед поиском альтернативного пути. По истечении времени максимального устаревания (maxage), BPDU считается устаревшим, поэтому коммутатор ищет новый корневой порт среди блокированных портов. Если доступных заблокированных портов нет, коммутатор объявляет корнем на указанных портах себя.

Cisco рекомендует не изменять таймеры, так как это может отрицательно сказаться на стабильности. Большинство развернутых сетей не настроены. Простые STP-таймеры, доступные из командной строки (такие как интервал-hello, maxage и т.д.), сами состоят из сложного набора других допустимых и внутренних таймеров. Поэтому настроить таймеры и учесть все ответвления сложно. Более того, можно повредить защиту UDLD. Дополнительные сведения см. в разделе Обнаружение однонаправленного канала.

Примечания по таймерам STP:

Значения таймеров STP по умолчанию основываются на расчете, учитывающем сетевой диаметр семи коммутаторов (семь коммутаторов переходят из корня на границы сети) и время, необходимое BPDU для перемещения из корневого моста на периферийные коммутаторы сети, находящиеся на расстоянии семи переходов. Это допущение рассчитывает значения таймера, допустимое для большинства сетей. Но можно изменить значения таймеров на более оптимальные, для того чтобы ускорить схождение при помощи изменения топологии сети.

Можно настроить для определенной VLAN корневой мост с диаметром сети, а значения таймера будут рассчитаны в соответствии с этими настройкам. При необходимости внести изменения Cisco рекомендует настраивать на корневом мосту только параметры диаметра и времени приветствия для данной VLAN.

```
spanning-tree vlan vlan-id [root {primary | secondary}] [diameter diameter-value [hello hello-time]] !--- This command needs to be on one line.
```

Этот макрос формирует корневой коммутатор для определенной VLAN, рассчитывает новые значения таймера на основании определенных диаметра и времени приветствия и передает информацию в конфигурационных BPDU всем коммутаторам в топологии.

Раздел Новые состояния и роли портов описывает 802.1D STP и противопоставляет 802.1D STP протоколу Rapid STP (RSTP). Дополнительную информацию об RSTP см. в разделе Общие сведения о протоколе быстрого связующего дерева (802.1w).

Новые состояния и роли портов

802.1D определен в четырех различных состояниях порта:

- Прослушивание
- Обучение
- Блокирование
- Передача

Дополнительные сведения см. в таблице в разделе Состояния портов. Состояние порта может быть смешанным (при блокировании или пересылке трафика), как и роль, которую он играет в активной топологии (корневой порт, выделенный порт и т.д.). Например, с операционной точки зрения между портом в состоянии прослушивания и портом в состоянии блокады нет никакой разницы. Оба они отбрасывают фреймы и не изучают MAC-адреса. Разница заключается в ролях, которые связующее дерево назначает этим портам. Можно предположить, что порт в состоянии прослушивания, является либо назначенным портом, либо корневым и собирается перейти в состояние пересылки. К сожалению, как только порт войдет в состояние пересылки, из состояния порта нельзя будет понять, является ли порт корневым или назначенным. Это показывает несостоятельность этой терминологии состояний. Чтобы устранить эту проблему, RSTP разделяет термины роли и состояния порта.

Состояния порта

Состояния порта в STP 802.1D

Состояния потров	Средства	Время до следующего состояния. Значение по умолчанию
Disabled	Административно выключен.	
Blocking	Получает BPDU и останавливает данные пользователя.	Отслеживает принятие BPDU. Ждет 20 секунд до истечения времени maxage или немедленно изменяет состояние, если регистрируется сбой прямого/локального соединения.
Listening	Отправляет или получает BPDU, чтобы проверить, возвращаются ли они, и заблокироваться в случае необходимости.	Ждет 15 секунд Fwddelay.
Learning	Строит топологию/таблицу CAM.	Ждет 15 секунд Fwddelay.
Forwarding	Посылает/получает данные.	

Общее изменение основной топологии составляет:

- 20 + 2 (15) = 50 сек, если ожидание maxage истекло
- 30 сек на сбой прямого соединения

В RSTP остается только три состояния порта, соответствующих трем возможным рабочим

состояниям. Состояния 802.1d disabled (отключен), blocking (блокировка) и listening (прослушивание) были объединены в одно состояние 802.1w discarding (отбрасывание).

Состояние порта STP (802.1D)	Состояние порта RSTP (802.1w)	Порт включен в активную топологию?	Порт обнаруживает MAC-адреса?
Отключенный	Отмена	Нет	Нет
Блокирование	Отмена	Нет	Нет
Прослушивание	Отмена	Да	Нет
Обучение	Обучение	Да	Да
Передача	Передача	Да	Да

Роли портов

Роль теперь представляет собой переменную, назначаемую данному порту. Роли корневого порта и назначенного порт остались, а роль блокирующего порта теперь разделена на роли резервного и альтернативного порта. Алгоритм связующего дерева (STA) определяет роль порта на основании BPDU. Чтобы было проще, необходимо запомнить о BPDU следующее: всегда можно сравнить любые два BPDU и решить, является ли один из них полезнее, чем другой. Роль определяется на основании переменной, хранящейся в BPDU, и иногда на основании порта, получившего BPDU. Оставшаяся часть данного раздела поясняет практическое применение ролей порта.

Роль корневого порта

Порт, получающий оптимальный блок BPDU по мостовому соединению, называется корневым. Этот порт является ближайшим к корневому мосту с позиции стоимости пути. STA выбирает один корневой мост во всей сети с мостовыми подключениями (на каждую VLAN). Корневой мост посылает BPDU, являющиеся более полезными, чем те, которые могут послать другие мосты. Корневой мост – это единственный мост в сети, у которого нет корневого порта. Все другие мосты получают BPDU хотя бы на один порт.

Роль назначенного порта

Порт является назначенным, если он может послать оптимальный BPDU на сегмент, к которому подключен порт. Мосты 802.1D соединяют разные сегменты (сегменты Ethernet, например) для создания домена с мостовыми соединением. В определенном сегменте может быть только один путь к корневому мосту. Если есть два пути – в сети возникла мостовая петля. Все мосты, связанные с данным сегментом, прослушивают BPDU друг друга и соглашаются на то, чтобы мост, отправивший оптимальный BPDU, стал назначенным мостом для этого сегмента. Соответствующий порт данного моста назначен.

Роли резервного порта и альтернативного порта

Эти две роли порта соответствуют блокаде по стандарту 802.1D. Блокированный порт – это порт, который не является назначенным или корневым портом. Блокированный порт получает более полезные BPDU, чем те, которые он посылает в свой сегмент. Помните, что

для удержания блокировки порту необходимо принимать пакеты BPDU. Эти две роли портов введены в RSTP со следующей целью.

Альтернативный порт – это порт, заблокированный получением более полезных BPDU от другого моста. Это показано на схеме:

Резервный порт – это порт, заблокированный получением более полезных BPDU от того же моста, в котором находится порт. Это показано на схеме:

Это разграничение было сделано уже в рамках стандарта 802.1D. Это является важным в работе функции UplinkFast Cisco. Дело в том, что альтернативный порт предоставляет альтернативный путь к корневому мосту. Таким образом, этот порт может заменить корневой порт в случае его сбоя. Естественно, резервный порт обеспечивает резервное подключение к тому же сегменту и не может гарантировать резервирование подключения к корневому мосту. Поэтому резервный порт был исключен из группы восходящих каналов.

В результате RSTP рассчитывает конечную топологию для связующего дерева с помощью критериев, аналогичных 802.1D. В способе использования различных приоритетов мостов и портов нет никаких изменений. Блокировка имени используется для отбрасывания состояния во внедрении Cisco. CatOS версии 7.1 или более новых версий все еще отображают состояния прослушивания и обучения, предоставляющих даже больше сведений о порте, чем необходимо по стандарту IEEE. Новая функциональность состоит в том, что теперь существует разница между ролью, которую порту отвел протокол, и его текущим состоянием. Например, порт может быть назначенным и заблокированным одновременно, и теперь такая ситуация является допустимой. Поскольку такая ситуация длится очень недолго, это просто значит, что порт до следующей отправки данных находится в переходном состоянии.

Взаимодействия STP с VLAN

Есть три различных способа поддержания соответствия VLAN и связующего дерева:

- Одно связующее дерево для всех VLAN или протокол общего связующего дерева (CST), как IEEE 802.1D
- Связующее дерево для каждой VLAN или совместное связующее дерево, как Cisco PVST
- Связующее дерево для совокупности VLAN или множественные связующие деревья (MST), как IEEE 802.1s

С точки зрения конфигурации, эти три типа режимов связующего дерева – по тому, как они взаимодействуют с VLAN – могут быть настроены на работу в одном из следующих трех режимов:

- **pvst – связующее дерево для каждой VLAN.** На самом деле этот режим реализует PVST+, но в программном обеспечении Cisco IOS он указывается как просто PVST.
- **rapid-pvst – продукт развития стандарта 802.1D демонстрирует улучшение показателей времени конвергенции и поддержку основанных на стандарте (802.1w) свойств, таких как UplinkFast и BackboneFast.**
- **mst – представляет собой стандарт 802.1s связующего дерева для совокупности VLAN или MST.** Он также поддерживает быстрый компонент 802.1w в пределах стандарта.

Одно связующее дерево для всех VLAN предусматривает только одну активную топологию и, как результат, отсутствие распределения нагрузки. Блокированный STP порт блокирует

все VLAN и не переносит данных.

Связующее дерево для каждой VLAN или PVST+ позволяет распределять нагрузку, но требует большей загрузки CPU при обработке BPDU, так как количество VLAN возрастает.

Новый стандарт 802.1s (MST) позволяет определить до 16 активных экземпляров STP/топологий, а также позволяет выполнить сопоставление всех VLAN для этих экземпляров. В типичной кампусной среде должны быть определены только два экземпляра. Эта методика позволяет масштабировать STP на многие тысячи виртуальных локальных сетей при включенном распределении нагрузки.

Поддержка Rapid-PVST и предстандарта MST обеспечивается в программном обеспечении Cisco IOS 12.1(11b)EX и 12.1(13)E для Catalyst 6500. Catalyst 4500 с программным обеспечением Cisco IOS 12.1(12c)EW и более поздними версиями поддерживают предстандарт MST. Поддержка Rapid PVST была добавлена в программном обеспечении Cisco IOS 12.1(19)EW для платформы Catalyst 4500. Стандартный совместимый MST поддерживается программным обеспечением Cisco IOS 12.2(18)SXF для Catalyst 6500 и программным обеспечением Cisco IOS 12.2(25)SG для серии коммутаторов Catalyst 4500.

Дополнительную информацию см. в документах Общие сведения о протоколе быстрого связующего дерева (802.1w) и Общие сведения о протоколе множественных связующих деревьев (802.1s).

Логические порты связующего дерева

Заметки к выпуску Catalyst 4500 и 6500 содержат руководство по множеству логических портов, рекомендованных в связующем дереве каждого коммутатора. Сумма всех логических портов равна количеству магистралей в коммутаторе умноженному на количество активных VLAN в магистралях, плюс количество немагистральных интерфейсов коммутатора. Программное обеспечение Cisco IOS генерирует сообщение системного журнала, если максимальное количество логических интерфейсов превысит предел. Рекомендуется не выходить за пределы рекомендованного руководства.

Следующая таблица сравнивает количество логических портов, поддерживаемых разными режимами STP и типами сигнализации:

Супервизор	PVST +	RPVST +	MST
Catalyst 6500 Supervisor 1	6,0001 общих 1,200 на модуль коммутации	6,000 общих 1,200 на модуль коммутации	25,000 общих 3,0002 на модуль коммутации
Catalyst 6500 Supervisor 2	13,0001 общих 1,8002 на модуль коммутации	10,000 общих 1,8002 на модуль коммутации	50,000 общих 6,0002 на модуль коммутации
Catalyst 6500 Supervisor 720	13,000 общих 1,8002 на модуль коммутации	10,000 общих 1,8002 на модуль коммутации	50,0003 общих 6,0002 на модуль коммутации
Catalyst	1,500 общих	1,500 общих	25,000

4500 Supervisor II plus	количеств	количеств	общих количеств
Catalyst 4500 Supervisor II plus-10GE	1,500 общих количеств	1,500 общих количеств	25,000 общих количеств
Catalyst 4500 Supervisor IV	всего 3000	всего 3000	50,000 общих количеств
Catalyst 4500 Supervisor V	всего 3000	всего 3000	50,000 общих количеств
Catalyst 4500 Supervisor V 10GE	всего 3000	всего 3000	80 000 всего

1 Максимальное количество логических портов, поддерживаемых PVST+ более ранней версии, чем ПО Cisco IOS выпуска 12.1(13)E, равняется 4 500.

2 Коммутирующие модули 10 Мбит/с, 10/100 Мбит/с и 100 Мбит/с поддерживают максимум 1 200 логических интерфейсов на модуль.

3 Максимальное общее количество логических портов, поддерживаемых MST, который предшествовал ПО Cisco IOS выпуска 12.2(17b)SXA, равняется 30 000.

Рекомендация

Трудно дать какие-либо рекомендации касательно режима связующего дерева без такой информации, как аппаратное обеспечение, программное обеспечение, количество устройств и количество VLAN. В общем, если количество логических портов не превышает рекомендованного руководством, то для развертывания сети рекомендуется режим Rapid PVST. Режим Rapid PVST обеспечивает быструю конвергенцию сети без дополнительных настроек, таких как Backbone Fast и Uplink Fast. Для того чтобы перевести связующее дерево в режим Rapid-PVST, выполните следующую команду:

```
spanning-tree mode rapid-pvst
```

Дополнительные варианты

В сети, состоящей из устаревшего оборудования и использующей старое программное обеспечение, рекомендуется режим PVST+. Для того чтобы перевести связующее дерево в режим PVST+, выполните следующую команду:

```
spanning-tree mode pvst ----This is default and it shows in the configuration.
```

Режим MST рекомендуется для разработки сетей VLAN с большим количеством VLAN. Для такой сети сумма логических портов может превышать рекомендованную для PVST и Rapid-PVST. Для того чтобы перевести связующее дерево в режим MST, выполните следующую

команду:

```
spanning-tree mode mst
```

BPDU форматы

Для поддержки стандарта IEEE 802.1Q Cisco расширил протокол PVST, существующий для обеспечения работы протокола PVST+. В PVST+ добавлена поддержка каналов в зоне одного связующего дерева IEEE 802.1Q. PVST+ совместим с существующими протоколами одного связующего дерева IEEE 802.1Q и Cisco PVST. Кроме того, в PVST+ добавлены механизмы проверки отсутствия среди коммутаторов несогласованности конфигураций транкинга портов и идентификаторов VLAN. Совместимость PVST+ с PVST настраивается автоматически (plug-and-play), не требуя новых команд интерфейса командной строки (CLI) или настройки.

Ниже приведены несколько основных моментов операционной теории протокола PVST+:

- PVST+ взаимодействует с единственным связующим деревом 802.1Q. PVST+ взаимодействует с 802.1Q-совместимыми коммутаторами, использующими общий STP, при помощи транкинга 802.1Q. Общее связующее дерево находится в VLAN 1, собственной VLAN, по умолчанию. Один BPDU общего связующего дерева передается или получается MAC-адресом (01-80-c2-00-00-00, тип протокола 0x010c) группы мостов стандарта IEEE через каналы 802.1Q. Общее связующее дерево может укореняться в зоне PVST или единственного связующего дерева.
- PVST+ передает BPDU PVST по тунелям через зону VLAN 802.1Q в виде многоадресных данных. Для каждой VLAN в магистрали передается или получается BPDU с MAC адресом (01-00-0c-cc-cd) совместного STP (SSTP) Cisco. Для VLAN, равных идентификатору VLAN порта (PVID), BPDU являются немечеными. Для всех остальных VLAN BPDU меченые.
- PVST+ обратно совместимы с существующими коммутаторами Cisco, использующими PVST через транкинг ISL. ISL-инкапсулированные BPDU передаются или получаются по магистралям ISL, которые являются теми же предыдущими Cisco PVST.
- PVST+ осуществляет проверку на несогласованность порта и VLAN. Во избежание возникновения петель переадресации PVST+ блокирует порты, принимающие несогласованные BPDU. PVST+ также уведомляет пользователей при помощи сообщений системного журнала о любых несогласованностях.

Примечание: В сетях ISL все BPDU передаются с использованием MAC-адреса IEEE.

Рекомендации Cisco по настройке

Во всех коммутаторах Catalyst протокол STP включен по умолчанию. Даже при выборе структуры, не включающей петли уровня 2, с отключенным STP для активного поддержания блокированного порта необходимо оставить эту функцию включенной по следующим причинам:

- При возникновении петли STP предотвращает проблемы, которые могут усугубляться многоадресными или широковещательными данными. Часто причинами возникновения петли становятся неправильная установка патча, неисправный кабель и другие.
- STP защищает от неисправностей EtherChannel.

- Конфигурация большинства сетей включает STP, что и обусловило их широкое распространение. Широкое распространение обычно означает более стабильный код.
- STP защищает от неправильного поведения сетевых интерфейсных плат с двойным подключением (или мостовых соединений, включенных на серверах).
- Многие протоколы тесно связаны по коду с STP. Примеры таких устройств:PAgPОтслеживание Internet Group Message Protocol (IGMP)ТранкингЕсли вы работаете без STP, вы можете получить нежелательные результаты.
- Инженеры Cisco при обнаружении сбоя сети, как правило, предполагают, что основной причиной стало именно неиспользование STP.

Для того чтобы включить связующее дерево на всех VLAN, выполните следующие глобальные команды:

```
Switch(config)#spanning-tree vlan vlan_id !--- Specify the VLAN that you want to modify.
Switch(config)#default spanning-tree vlan vlan_id !--- Set spanning-tree parameters to default values.
```

Не изменяйте таймеры, которые могут отрицательно повлиять на стабильность. Большинство развернутых сетей не настроены. Простые STP-таймеры, доступные из командной строки, такие как интервал-hello и maxage, сами состоят из сложного набора других допустимых и внутренних таймеров. Поэтому при попытке настроить таймеры и учесть все ответвления можно столкнуться с трудностями. Более того, можно повредить защиту UDLD.

Лучше всего не использовать управляющую VLAN для абонентского трафика. Это не касается коммутатора Cisco IOS Catalyst 6500/6000. Однако необходимо соблюдать эти рекомендации для меньших конечных коммутаторов Cisco IOS и коммутаторов CatOS, которые могут использовать раздельный интерфейс управления и должны интегрироваться с коммутаторами Cisco IOS. Особенно в случае более старых процессоров коммутаторов Catalyst необходимо держать VLAN управления отдельно от пользовательских данных для того, чтобы избежать проблем с STP. Одна конечная станция с некорректным поведением потенциально может настолько загрузить процессор Supervisor Engine широковещательными пакетами, что процессор пропустит один или более BPDU. Однако более новые коммутаторы с более мощными ЦПУ и дросселирующими регуляторами избавляют от таких опасностей. См. раздел данного документа Интерфейс управления коммутаторами и собственная VLAN для получения дополнительной информации.

Избегайте чрезмерной избыточности. Это может привести к возникновению большого количества заблокированных портов и отрицательно сказаться на долгосрочной стабильности. Не рекомендуется использовать общий диаметр SPT более семи переходов. Необходимо стараться проектировать именно многоуровневую модель Cisco, там, где такое строение возможно. Функции такой модели:

- Меньшие коммутируемые домены
- Треугольники STP
- Детерминистические блокированные порты

См. Гигабитный Проект сети уровня кампуса для подробных данных.

Необходимо проверить и узнать, где располагается корень и заблокированные порты. Затем нужно задокументировать их на схеме топологии сети. Для поиска и устранения неисправностей очень важно знать топологию связующего дерева. Поиск неисправностей STP должен начинаться с блокированных портов. Поиск причины, по которой порты из блокированных стали пересылающими, часто является ключевой частью анализа причин неисправностей. Выберите уровни распределения или магистральные уровни местом

расположения корня/вторичного корня, так как именно эти уровни считаются самыми стабильными участками сети. Проверьте, оптимально ли покрытие уровня 3 и протокола маршрутизатора горячего резервирования (HSRP) путями пересылки данных уровня 2.

Следующая команда является макросом, настраивающим приоритет моста. Корень устанавливает приоритет намного ниже, чем стандартный (32,768), а вторичный корень устанавливает приоритет, который обоснованно ниже стандартного:

```
Switch(config)#interface type slot/port Switch(config)#spanning-tree vlan vlan_id root primary
!--- Configure a switch as root for a particular VLAN.
```

Примечание: Этот макрос заставляет корневой приоритет быть также:

- 8192 по умолчанию
- Текущий приоритет корня минус 1, если известен другой корневой мост
- Приоритет текущего корня, если его MAC адрес ниже, чем текущий корень

Отключите ненужные VLAN от магистральных портов, это называется двунаправленной задачей. При этом сокращается диаметр STP и издержки обработки NMP в тех отрезках сети, где определенные VLAN не требуются. Автоматическое отсечение VTP не удаляет STP из магистрального канала. Также можно удалить из магистралей стандартную VLAN.

Для получения дополнительных сведений см. документ Ошибки протокола связующего дерева и соответствующие рекомендации по разработке.

Дополнительные варианты

У Cisco есть другой протокол, называемый мост VLAN, который использует в своей работе хорошо известный MAC адрес назначения 01-00-0c-cd-cd-ce и тип протокола 0x010c.

Этот протокол наиболее полезен при существовании необходимости обеспечения мостового соединения немаршрутизированных или устаревших протоколов между VLAN без вмешательства экземпляров связующего дерева IEEE, использующих эти VLAN. Если интерфейсы VLAN для немостового трафика блокируются для трафика уровня 2, наложенный трафик уровня 3 будет также случайно отсечен, что станет сторонним нежелательным эффектом. Блокада уровня 2 легко может случиться, если интерфейсы VLAN для немостового трафика принимают участие в том же STP, что и IP VLAN. Мост VLAN является отдельным экземпляром STP для мостовых протоколов. Этот протокол обеспечивает отдельную топологию, которой можно управлять, не оказывая влияния на IP-трафик.

Рекомендуется использовать протокол моста VLAN, если необходимо мостовое соединение между VLAN на маршрутизаторах Cisco, таких как, например, MSFC.

Функция STP PortFast

PortFast можно использовать для обхода нормальной работы связующего дерева на портах доступа. PortFast повышает скорость соединения между конечными станциями и службами, к которым конечные станции должны подключиться после инициализации канала.

```
Microsoft, DHCP,       forwarding   ,      up,       IP-.  ,      (IPX)/   (SPX),
forwarding   ,      up,         (GNS).
```

Дополнительные сведения см. в разделе Использование PortFast и других команд для

устранения задержек соединения во время запуска рабочей станции.

Технологическое описание PortFast

PortFast STP, listening, learning forwarding. blocking forwarding, up. , STP . Этот процесс может занять время (2 x ForwardDelay), которое по умолчанию составляет 30 секунд.

Portfast STP (TCN) , learning forwarding. Появление TCN является нормальным. Но лавина TCN, обрушивающаяся на корневой мост, может излишне увеличить время конвергентности. Лавина TCN часто возникает по утрам, когда люди включают свои ПК.

Рекомендации Cisco по настройке портов доступа

STP PortFast on . STP PortFast off - , .

Выполните макро команду switchport host в режиме настройки интерфейса, для того чтобы настроить порт доступа согласно рекомендациям. Такая конфигурация также значительно поможет автосогласованию и повысит производительность соединения:

```
switch(config)#interface type slot#/port# switch(config-if)#switchport host switchport mode will be set to access spanning-tree portfast will be enabled channel group will be disabled !--- This macro command modifies these functions.
```

Примечание: PortFast не означает, что связующее дерево не выполнено вообще на портах. Пакеты BPDU все еще отправляются, принимаются и обрабатываются. Наличие связующего дерева значительно для полной исправности LAN. Без определения и блокирования петель петля может быстро случайно остановить работу целой LAN.

Также необходимо отключить транкинг и выделение каналов для всех узловых портов. Все порты доступа включены по умолчанию для транков и передачи по каналам, а соседних коммутаторов по проекту не должно быть на портах хоста. Если эти протоколы будут оставлены для согласования, последующая задержка активации порта может привести к нежелательным последствиям. Начальные пакеты из рабочих станций, например DHCP- и IPX-запросы, не пересылаются.

Лучше в режиме глобальной настройки настроить запуск PortFast по умолчанию при помощи следующей команды:

```
Switch(config)#spanning-tree portfast enable
```

Затем на любом порту доступа, имеющем концентратор или коммутатор в одной VLAN, необходимо отключить функциональность PortFast для каждого интерфейса при помощи команды interface:

```
Switch(config)#interface type slot_num/port_num Switch(config-if)#spanning-tree portfast disable
```

Дополнительные варианты

Защита BPDU PortFast предоставляет метод защиты от петель. BPDU errDisable BPDU.

В обычных условиях порт доступа, на котором настроен PortFast, никогда не получит пакетов BPDU. Входящий BPDU означает неправильную настройку. Лучшим выходом в таком случае будет отключить этот порт доступа.

Cisco IOS , BPDU-ROOT-GUARD , UplinkFast. *Всегда используйте эту команду.* Эта команда работает для каждого коммутатора, а не для каждого порта.

, BPDU-ROOT-GUARD:

```
Switch(config)#spanning-tree portfast bpduguard default
```

Прерывание протокола управления простой сетью (SNMP) или сообщение системного журнала уведомляют администратора сети об отключении порта. errDisabled ( ) . Дополнительные сведения см. в разделе Обнаружение однонаправленного канала данного документа.

Более подробную информацию см. в разделе Новая функция протокола связующего дерева – защита BPDU PortFast.

Примечание: PortFast для магистральных портов был представлен в программном обеспечении Cisco IOS версии 12.1(11b)E. PortFast для магистральных портов разработан для увеличения времен согласования для сетей Уровня 3. При использовании этой функциональности необходимо убедиться в том, что на основе интерфейса отключены защита BPDU и фильтрация BPDU.

UplinkFast

Цель

Функция UplinkFast обеспечивает быструю сходимость STP после сбоя прямого соединения на уровне сетевого доступа. UplinkFast работает без модификации STP. Целью этой функциональности является ускорение сходимости в специфических условиях до менее чем трех секунд, в отличие от обычных 30 секунд задержки. См. раздел Общие понятия и настройка функции Cisco UplinkFast.

Технологическое описание

Cisco forwarding. listening learning.

Группа восходящих каналов – это набор портов для каждой VLAN, которые можно рассматривать как корневой и резервный корневой порт. При нормальных условиях корневые порты гарантируют соединение точки доступа с корнем. Если первичное корневое соединение по каким-либо причинам прерывается, резервный корневой канал немедленно активизируется без обычного ожидания в течение 30 секунд задержки сходимости.

UplinkFast STP (listening learning), . Этот механизм должен обновлять сведения коммутаторов в домене о том, что локальные конечные станции доступны по альтернативному пути. Таким образом, коммутатор уровня доступа, использующий UplinkFast, также генерирует фреймы для каждого MAC адреса в своей таблице CAM до хорошо известного MAC-адреса многоадресной рассылки (01-00-0c-cd-cd-cd HDLC протокол 0x200a). Этот процесс обновляет новой топологией таблицу CAM каждого коммутатора в домене.

Рекомендации Cisco

Cisco рекомендует подключать UplinkFast для коммутаторов доступа с блокированными портами, если используется связующее дерево 802.1D. Не следует использовать UplinkFast

на коммутаторах без знания предполагаемой топологии резервного корневого канала – обычно в многоуровневой схеме Cisco это коммутаторы распределения и основные коммутаторы. В общем случае, не нужно включать UplinkFast на коммутаторах, имеющих более двух выходов из сети. Если коммутатор находится в среде сложного доступа и есть более чем один блокированный канал и один пересылающий, необходимо избегать использования этой функциональности или проконсультироваться с инженером UplinkFast.

Для запуска UplinkFast выполните следующую глобальную команду:

```
Switch(config)#spanning-tree uplinkfast
```

В программном обеспечении Cisco IOS эта команда не увеличивает автоматически все значения приоритетов моста. Скорее эта команда изменяет приоритет моста только тех VLAN, приоритеты которых не были изменены на какое-либо другое значение вручную. **К тому же, в отличие от CatOS, при восстановлении коммутатора, имеющего включенный UplinkFast, никакая из форм этой команды (no spanning-tree uplinkfast) не возвратит все измененные значения к стандартным.** *Поэтому при использовании этой команды необходимо проверить текущий статус приоритетов моста до и после, чтобы убедится в том, что желаемый результат был достигнут.*

Примечание: Когда опция фильтрации протоколов активирована, вам нужно **все ключевое слово all protocols** для команды UplinkFast. Поскольку при включенной фильтрации протокола CAM записывает тип протокола, а также данные MAC и VLAN, для каждого протокола на каждом MAC адресе должен быть создан фрейм UplinkFast. **Ключ rate означает скорость с которой топология UplinkFast обновляет фреймы, измеряемая в числе пакетов в секунду.** Рекомендуется оставить значение по умолчанию. Необходимо настраивать UplinkFast с RSTP, потому что RSTP изначально содержит этот механизм и автоматически включает его.

BackboneFast

Цель

BackboneFast обеспечивает быструю сходимость от сбоев непрямых каналов. BackboneFast уменьшает время сходимости со стандартных 50 секунд до 30 секунд (обычно) и таким образом добавляет функциональность STP. Эта функциоанльность также применима только при использовании 802.1D. Не нужно настраивать эту функцию при использовании Rapid PVST или MST (включающих быстрый компонент).

Технологическое описание

BackboneFast инициируется, когда корневой или заблокированный порты коммутатора получают от назначенного моста подчиненные BPDU. Порт обычно получает подчиненные BPDU, когда нисходящий коммутатор теряет соединение с корнем и начинает посылать BPDU для выбора нового корня. Подчиненный BPDU определяет коммутатор и как корневой мост, и как назначенный мост.

По обычным правилам связующего дерева получающий коммутатор игнорирует подчиненный BPDU в течение настроенного времени maxage. По умолчанию maxage составляет 20 секунд. Но при включенной BackboneFast коммутатор расценивает подчиненный BPDU как сигнал о возможной смене топологии. Для того чтобы определить имеет ли он альтернативный путь к корневому мосту, коммутатор использует BPDU запроса связи с корнем (RLQ). Добавление RLQ протокола позволяет коммутатору проверить,

доступен ли еще корень. RLQ forwarding , BPDU, .

Ниже приведены несколько основных моментов работы протокола:

- Коммутатор передает пакет RLQ только на корневой порт (это означает, что пакет следует к корню).
- Коммутатор, получивший RLQ, может ответить, если он является корневым или знает, что он потерял соединение с корнем. Если коммутатору такие данные не известны, он должен переслать запрос со своего корневого порта.
- Если коммутатор потерял подключение к корню, он должен дать отрицательный ответ на этот запрос.
- Ответ должен быть послан только с того порта, на который поступил запрос.
- Корневой коммутатор всегда должен положительно отвечать на этот запрос.
- Если ответ получен некорневым портом, он должен быть отброшен.

Эта операция может уменьшать время сходимости STP на величину до 20 секунд, так как нет необходимости ждать, пока истечет время maxage. Дополнительную информацию см. в разделе Общие сведения и настройка Backbone Fast на коммутаторах Catalyst.

Рекомендации Cisco

Можно включать BackboneFast на всех коммутаторах, использующих STP, только если весь домен связующего дерева поддерживает эту функциональность. Добавление этой функциональности не вызовет сбоев в рабочей сети.

Для запуска BackboneFast выполните следующую глобальную команду:

```
Switch(config)#spanning-tree backbonefast
```

Примечание: Необходимо настроить эту команду глобального уровня на всех коммутаторах в домене. Эта команда добавляет функциональность к STP, что должны понять все коммутаторы.

Дополнительные варианты

Функция Backbone Fast не поддерживается коммутаторами Catalyst 2900XL и 3500XL. В общем случае, необходимо подключить BackboneFast, если домен коммутатора содержит эти коммутаторы наряду с коммутаторами Catalyst 4500/4000, 5500/5000 и 6500/6000. При использовании Backbone Fast в средах строгой топологии с коммутаторами XL можно включать эту функцию там, где коммутатор XL является последним коммутатором на линии и подключен в двух местах только к ядру. Не следует использовать эту функцию, если коммутаторы XL подключены последовательно.

Не нужно настраивать BackboneFast с RSTP или 802.1w, потому что RSTP изначально содержит этот механизм и автоматически включает его.

Защита от петель связующего дерева

Loop guard – это разработка Cisco для оптимизации STP. Эта функциональность защищает сети уровня 2 от петель, возникающих при неисправной работе сетевого интерфейса, занятости ЦПУ или по каким-либо другим причинам, препятствующим нормальной пересылке BPDU. Петля STP возникает, когда блокирующий порт в топологии с резервированием ошибочно переходит в состояние передачи. Обычно это происходит,

потому что один из портов физически избыточной топологии (не обязательно блокирующий порт) перестает получать BPDU STP.

Защита от петель полезна только в коммутируемых сетях, в которых коммутаторы соединены двухточечными каналами, как в случае самых современных кампусных сетей и сетей центра данных. Идея состоит в том, что в двухточечном канале назначенный мост не может исчезнуть, не отправив подчиненного BPDU или не приведя к отказу канала. Функциональность защиты от петель STP была впервые представлена в ПО Cisco IOS выпуска 12.1(13)E программного обеспечения Cisco IOS для Catalyst 6500 и ПО Cisco IOS выпуска 12.1(9)EA1 для коммутаторов Catalyst 4500.

Дополнительные сведения см. в разделе Усовершенствование протокола связующего дерева с помощью функций Loop Guard (защита от петель) и BPDU Skew Detection (обнаружение искажения BPDU).

Технологическое описание

Защита от петель проверяет, получает ли BPDU корневой порт или альтернативный/резервный корневой порт. Если порт не получает BPDU, защита от петель переводит порт в неустойчивое состояние (блокада) до тех пор, пока он снова не начнет получать BPDU. Порт в несовместимом состоянии не передает BPDU. Если такой порт получает BPDU снова, порт (и соединение) снова считается действующим. Условие неустойчивой петли удаляется из порта и STP определяет состояние порта. Таким образом, восстановление происходит автоматически.

Loop guard изолирует неисправность и позволяет связующему дереву сходиться в стабильную топологию без нарушенного канала или моста. Loop guard предотвращает образование петель STP со скоростью используемой версии STP. Не существует зависимости от самого STP (802.1D или 802.1w) или от того настроены ли таймеры STP. По этим причинам Cisco рекомендует применять защиту от петель в топологиях, зависящих от STP, в сочетании с UDLD и при использовании программного обеспечения, поддерживающего эту функциональность.

Когда защита от петель блокирует неустойчивый порт, в системный журнал записывается следующее сообщение:

```
%SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010
```

После того как портом, находящимся в неустойчивом состоянии цикла STP, был получен BPDU, порт переходит в другое состояние STP. В соответствии с полученным BPDU, это означает, что восстановление является автоматическим и никакое вмешательство не требуется. После восстановления регистрируется следующее сообщение:

```
%SPANTREE-SP-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet2/1 on
VLAN0010
```

Взаимодействие с другими функциями STP

Защита корня дерева STP

Root guard заставляет порт всегда быть назначенным портом. Защита от петель является эффективной только для корневых или альтернативных портов, что означает, что их функции являются взаимоисключающими. Поэтому защита от петель и корневая защита не могут быть включены на порте в одно и то же время.

UplinkFast

Функция Loop guard совместима с UplinkFast. Если защита от петель переводит корневой порт в блокирующее состояние, UplinkFast переводит в передающее состояние новый корневой порт. *Также UplinkFast не выбирает корневым портом порт в неустойчивом состоянии цикла.*

BackboneFast

Функция Loop guard совместима с BackboneFast. BackboneFast запускается получением подчиненного BPDU, пришедшего с назначенного моста. Так как BPDU получаются из этого канала, защита от петель не активизируется, поэтому BackboneFast и защита от петель являются совместимыми.

PortFast

Portfast переводит порт в назначенное состояние пересылки сразу после установления соединения. Так как активизированный PortFast порт не является корневым/альтернативным, защита от петель и PortFast взаимно исключают друг друга.

PAgP

Loop guard использует порты, известные для STP. Поэтому loop guard может использовать преимущества абстрагирования логических портов, обеспечиваемые PAgP. Но для того чтобы сформировать канал, все физические порты, сформированные в канал, должны иметь совместимые настройки. PAgP вынуждает все физические порты принять унифицированные настройки защиты от петель для того, чтобы сформировать канал. Эти предупреждения необходимо помнить при настройке защиты от петель на EtherChannel:

- STP всегда выбирает первый рабочий порт в канале, для того чтобы посылать BPDU. Если эта линия связи становится однонаправленной, защита от петель блокирует канал, даже если другие линии связи в канале функционируют должным образом.
- Если совокупность портов, уже заблокированных защитой от петель, сгруппировалась для формирования канала, STP теряет всю информацию о состоянии этих портов, а порт нового канала возможно может достичь передающего состояния с назначенной ролью.
- Если канал заблокирован защитой от петель и канал прерывает эту блокаду, STP теряет всю информацию о состоянии. Индивидуальный физический порт может достичь передающего состояния с назначенной ролью, даже если одна или более линий связи, формирующих канал, являются однонаправленными.

В двух последних случаях возможность возникновения петли будет существовать, пока UDLD не зафиксирует сбой. Но защита от петель определить его не может.

Сравнение защиты от петель и функции UDLD

Защита от петель и функциональность UDLD частично пересекаются между собой – отчасти из-за того, что обе предотвращают сбои протокола STP, вызванные однонаправленными линиями связи. Разница между этими двумя функциями заключается в различном подходе к проблеме и разных функциональных возможностях. Существуют специфические однонаправленные сбои, которые не способно зафиксировать UDLD, например, сбои, вызванные ЦПУ, не посылающим BPDU. К тому же использование агрессивных таймеров

STP и режима RSTP может привести к возникновению петель еще до того, как UDLD сможет зафиксировать сбой.

Защита от петель не действует на совместных линиях связи или в ситуациях, когда канал с момента соединения был однонаправленным. В случае, когда канал был однонаправленным с момента соединения, порт никогда не получает BPDU и становится назначенным. Это может быть нормальным поведением системы, поэтому этот частный случай защита от петель не покрывает. UDLD не предоставляет защиту против такого сценария.

Включение и UDLD, и защиты от петель обеспечивает наивысший уровень защиты. Дополнительные сведения см. в следующих разделах:

- *В разделе Противопоставление защиты от петель и обнаружения однонаправленных линий связи документа совершенствование протокола связующего дерева с помощью функций Loop Guard (защита от петель) и BPDU Skew Detection (обнаружение искажения BPDU)*
- В разделе UDLD данного документа

Рекомендации Cisco

Cisco рекомендует включать loop guard глобально в сетях коммутаторов с физическими петлями. Можно включить защиту от петель глобально на всех портах. Эффективность обеспечивается включением функции для всех соединений типа "точка-точка". Соединение "точка-точка" определяется по состоянию дуплексной передачи соединения. Если настроен полнодуплексный режим, соединение считается соединением "точка-точка".

```
Switch(config)#spanning-tree loopguard default
```

Дополнительные варианты

Для коммутаторов, не поддерживающих глобальную настройку защиты от петель, рекомендуется подключать функциональность на всех индивидуальных портах, включая порты канала. Хотя при включении защиты от петель на назначенном порту не возникнет никаких преимуществ, не стоит рассматривать это включение как проблему. Кроме того, действительная повторная сходимость связующего дерева может сделать назначенный порт корневым портом, что делает функцию полезной на этом порте.

```
Switch(config)#interface type slot#/port# Switch(config-if)#spanning-tree guard loop
```

Сети, в топологиях которых петли отсутствуют, все-таки получают преимущества от использования функции loop guard при случайном образовании петель. Но включение защиты от петель в такой топологии может привести к проблемам изоляции сети. При построении топологии, свободной от петель, и при желании избежать проблем с изоляцией сети можно отключать защиту от петель глобально или индивидуально. Не следует отключать защиту от петель на совместных линиях связи.

```
Switch(config)#no spanning-tree loopguard default !--- This is the global configuration.
```

или

```
Switch(config)#interface type slot#/port# Switch(config-if)#no spanning-tree guard loop !---
This is the interface configuration.
```

Корневая защита для протокола связующего дерева

Функция защиты корня обеспечивает возможность задать расположение корневого моста в

сети. Функция защиты корня обеспечивает, чтобы порт, для которого включена эта функция, был назначенным портом. Обычно все порты корневого моста являются назначенными, если два или более портов корневого моста не соединены вместе. Если мост получает вышестоящий BPDU STP на порт, на котором включена защита, мост переводит этот порт в несовместимое с корневым состояние STP. Состояние несогласованности корня аналогично состоянию прослушивания. Трафик через порт в таком состоянии не пересылается. Таким образом, защита корня задает расположение корневого моста. Корневая защита доступна уже в самых ранних версиях программного обеспечения Cisco IOS – начиная с версии 12.1E.

Технологическое описание

Root guard является механизмом, встроенным в STP. У корневой защиты нет собственного таймера и она зависит только от приема BPDU. Когда для порта включена корневая защита, у порта нет возможности стать корневым. Если прием BPDU вызывает сходимость связующего дерева, которая попытается сделать назначенный порт корневым, этот порт будет переведен в состояние несогласованности корня. Это продемонстрировано следующим сообщением системного журнала:

```
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/1 on VLAN0010
```

После того как порт прекращает передавать вышестоящие BPDU, порт разблокируется снова. Благодаря STP порт переходит из состояния прослушивания в состояние обучения и в конечном итоге в состояние пересылки. Сообщение системного журнала показывает этот переход:

```
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/1
on VLAN0010
```

Восстановление происходит автоматически; участия администратора не требуется.

Так как корневая защита вынуждает порт быть назначенным, а защита от петель эффективна, только если порт является корневым или альтернативным, эти функциональные возможности являются взаимоисключающими. Поэтому защита от петель и корневая защита не могут быть включены для порта одновременно.

Дополнительные сведения см. в разделе Новая функция корневой защиты для протокола связующего дерева.

Рекомендации Cisco

Cisco рекомендует включать функцию root guard на портах, подключенных к сетевым устройствам, управление которыми не осуществляется. Для настройки корневой защиты используйте следующие команды в режиме настройки интерфейса:

```
Switch(config)#interface type slot#/port# Switch(config-if)#spanning-tree guard root
```

EtherChannel

Цель

EtherChannel охватывает алгоритм распределения фреймов, который эффективно мультиплексирует фреймы в компоненте 10/100 Мбит/с или каналах Gigabit. Алгоритм распределения фреймов позволяет инверсное мультиплексирование множества каналов в одну логическую линию связи. Хотя каждая реализация каждой следующей платформы

отличается от предыдущей, необходимо понимать следующие общие требования:

- В платформе должен быть алгоритм статистического мультиплексирования фреймов по множеству каналов. Для коммутаторов Catalyst это связано с аппаратным обеспечением. Рассмотрим примеры:Catalyst 5500/5000s – наличие или отсутствие в модуле Ethernet Bundling Chip (EBC)Catalyst 6500/6000s – алгоритм, способный дополнительно читать фрейм и мультиплексировать по IP-адресу
- Есть возможность создания логического канала, поэтому, в зависимости от того, находится EtherChannel на уровне 2 или уровне 3, может выполняться единичный экземпляр STP или использоваться единичная одноранговая маршрутизация.
- Существует протокол управления, проверяющий согласованность параметров на обоих концах линии связи и помогающий управлять восстановлением пакетирования при сбое или добавлении линии связи. Таким протоколом может быть PAgP или протокол управления агрегацией каналов(LACP).

Технологическое описание

EtherChannel охватывает алгоритм распределения фреймов, который эффективно мультиплексирует фреймы в компоненте 10/100 Мбит/с или каналах Gigabit. Различия в алгоритмах на той или иной платформе проистекают из способности каждого типа оборудования извлекать сведения заголовка кадра для принятия решения о распределении.

Алгоритм распределения нагрузки – это общая функция для обоих протоколов управления каналами. В PAgP и LACP используется алгоритм распределения кадров, поскольку стандарт IEEE не обязывает использовать какой-либо определенный алгоритм распределения. Но любой алгоритм распределения дает уверенность в том, что, когда фреймы получены, алгоритм не приведет к беспорядочности фреймов, являющихся частью любого данного сообщения, или задваиванию фреймов.

Следующая таблица описывает алгоритм распределения фреймов для каждой из перечисленных платформ:

Платформа	Алгоритм распределения нагрузки канала
Catalyst 3750 Series	Алгоритм распределения нагрузки Catalyst 3750, функционирующих на базе программного обеспечения Cisco IOS, использует MAC-адреса или IP-адреса, источник сообщений или назначение сообщений, или и то и другое.
Серия Catalyst 4500	Алгоритм распределения нагрузки Catalyst 4500, функционирующих на базе программного обеспечения Cisco IOS, использует MAC-адреса, IP-адреса или номера портов уровня 4 (L4), источник сообщений или назначение сообщений, или и то и другое.
Catalyst серии	Существует два алгоритма хеширования, которые могут быть использованы, какой из них будет использован, зависит от аппаратного обеспечения Supervisor Engine.

6500/6000	Хеш – это многочлен семнадцатой степени, используемый оборудованием. В любом случае хеш берет MAC-адрес, IP-адрес или номер порта IP TCP/UDP и применяет алгоритм для генерации 3-битовой величины. Этот процесс происходит отедельно от SA и DA. После для результатов используется опреация XOR для генерации другой 3-битовой величины. Эта величина определяет, какой порт в канале используется для пересылки пакета. Каналы в Catalyst 6500/6000 могут формироваться между портами любого модуля и работать для восьми портов.

Следующая таблица демонстрирует методы распределения, поддерживаемые различными моделями Catalyst 6500/6000 Supervisor Engine. В таблице также показано поведение по умолчанию:

Аппаратные средства	Описание	Методы распределения
WS-F6020A (Механизм уровня 2) WS-F6K-PFC (Механизм уровня 3)	Более поздний Supervisor Engine IA Supervisor Engine I и Supervisor Engine IA / Policy Feature Card 1 (PFC1)	MAC уровня 2: SA; DA; SA и IP уровня 3 DA: SA; DA; SA и DA (по умолчанию)
WS-F6K-PFC 2	Supervisor Engine II/PFC2	MAC уровня 2: SA; DA; SA и IP Уровня 3 DA: SA; DA; SA и DA (по умолчанию) сеанс Уровня 4: S-порт; D-порт; S- и D-порт
WS-F6K-PFC3A WS-F6K-PFC3B WS-F6K-PFC3BXL	Supervisor Engine 720/PFC3A Supervisor Engine 720/Supervisor Engine 32/PFC3B Supervisor Engine 720/PFC3BXL	MAC уровня 2: SA; DA; SA и IP Уровня 3 DA: SA; DA; SA и DA (по умолчанию) сеанс Уровня 4: S-порт; D-порт; S- и D-порт

Примечание: С распределением Уровня 4 первый фрагментированный пакет использует распределение Уровня 4. Все последующие пакеты используют распределение уровня 3.

Примечание: См. эти документы для обнаружения большего количества подробных данных о Поддержке EtherChannel на других платформах и как настроить и устранить неполадки EtherChannel:

- Балансировка загрузки EtherChannel и избыточность на коммутаторах Catalyst

- Настройка уровня 2 и уровня 3 EtherChannel (руководство по настройке программного обеспечения Cisco IOS Catalyst 6500 Series, 12.2SX)
- Настройка уровня 2 и уровня 3 EtherChannel (руководство по настройке программного обеспечения Cisco IOS Catalyst 6500 Series, 12.1E)
- Настройка EtherChannel (руководство по настройке программного обеспечения Cisco IOS Catalyst 4500 Series, 12.2(31)SG)
- Настройка EtherChannel (руководство по настройке программного обеспечения коммутатора Catalyst 3750, 12.2(25)SEE)
- Настройка EtherChannel между коммутаторами Catalyst 4500/4000, 5500/5000 и 6500/6000, работающими на базе системного программного обеспечения CatOS

Рекомендации Cisco

Коммутаторы серий Catalyst 3750, Catalyst 4500 и Catalyst 6500/6000 осуществляют балансировку нагрузки путем хеширования IP адресов источника и назначения по умолчанию. Данная рекомендация сделана с учетом предположения, что IP является доминирующим протоколом. Для настройки распределения нагрузки введите следующую команду:

```
port-channel load-balance src-dst-ip !--- This is the default.
```

Дополнительные варианты

В зависимости от потока трафика, если большинство трафика приходится на обмен данными между одними и теми же IP адресами источника и назначения, можно использовать распределение уровня 4 для того, чтобы улучшить балансировку нагрузки. Необходимо понимать, что, когда настроено распределение уровня 4, хеширование включает только исходные порты и порты назначения. IP-адреса уровня 3 в алгоритме хеширования не объединяются. Для настройки распределения нагрузки введите следующую команду:

```
port-channel load-balance src-dst-port
```

Примечание: Распределение уровня 4 не конфигурируемо на коммутаторах серии Catalyst 3750.

Выполните команду show etherchannel load-balance для проверки политики распределения кадров.

В зависимости от платформ оборудования, можно использовать команды CLI, чтобы определить, какой интерфейс EtherChannel пересылает специфический поток трафика, на основании политики распределения фреймов.

Для коммутаторов Catalyst 6500 выполните команду remote login switch для того, чтобы удаленно войти в систему консоли процессора коммутатора (SP). *Затем выполните команду test etherchannel load-balance interface номер порта-канала {ip | l4port | mac} [source_ip_add | source_mac_add | source_l4_port] [dest_ip_add | dest_mac_add | dest_l4_port].*

Для коммутаторов Catalyst 3750 выполните команду test etherchannel load-balance interface номер порта-канала {ip | mac} [source_ip_add | source_mac_add] [dest_ip_add | dest_mac_add].

Для Catalyst 4500 эквивалентной команды пока не существует.

Руководство по настройке EtherChannel и ограничения

Перед агрегированием совместимых портов в один логический порт EtherChannel проверяет свойства всех физических портов. Рекомендации и ограничения для настройки различаются для различных коммутирующих платформ. Следуйте этим инструкциям и ограничениям для того, чтобы избежать проблем пакетирования. Например, если включен QoS, каналы EtherChannel не формируются при пакетировании коммутирующих модулей серий Catalyst 6500/6000 с различными возможностями QoS. **Для коммутаторов Catalyst 6500, работающих на базе программного обеспечения Cisco IOS, можно отключить проверку атрибутов QoS порта при пакетировании EtherChannel интерфейсной командой no mls qos channel-consistency.** *Команда show interface capability mod/port отображает возможности QoS порта и определяет, совместимы ли порты.*

Обратитесь к следующим инструкциям для различных платформ для того, чтобы избежать проблем конфигурации:

- Настройка уровня 2 и уровня 3 EtherChannel (руководство по настройке программного обеспечения Cisco IOS Catalyst 6500 Series, 12.2SX)
- Настройка уровня 2 и уровня 3 EtherChannel (руководство по настройке программного обеспечения Cisco IOS Catalyst 6500 Series, 12.1E)
- Настройка EtherChannel (руководство по настройке программного обеспечения Cisco IOS Catalyst 4500 Series, 12.2(31)SG)
- Настройка EtherChannel (руководство по настройке программного обеспечения коммутатора Catalyst 3750, 12.2(25)SEE)

Максимальное количество поддерживаемых каналов EtherChannels также зависит от аппаратной платформы и релиза программного обеспечения. Коммутаторы Catalyst 6500, работающие на базе программного обеспечения Cisco IOS релиза 12.2(18)SXE и более поздних версий поддерживают максимум 128 интерфейсов портов-каналов. Релизы программного обеспечения более ранние, чем Cisco IOS 12.2(18)SXE, поддерживают максимум 64 интерфейса портов-каналов. Количество реконфигурируемых групп может быть от 1 до 256 независимо от релиза программного обеспечения. Коммутаторы серии Catalyst 4500 поддерживают максимум 64 канала EtherChannels. Для коммутаторов Catalyst 3750 рекомендуется не настраивать более 48 каналов EtherChannel на стек коммутатора.

Расчет стоимости порта связующего дерева

Необходимо понять расчет стоимости порта связующего дерева для каналов EtherChannel. Рассчитать стоимость порта связующего дерева для каналов EtherChannel можно коротким или длинным методом. По умолчанию стоимость порта рассчитывается в коротком режиме.

Эта таблица иллюстрирует стоимость порта связующего дерева для EtherChannel Уровня 2 на основе пропускной способности:

Bandwidth	Старое значение STP	Новое длинное значение STP
10 Мбит/с	100	2,000,000
100 Мбит/с	19	200,000
1 Гбит/с	4	20,000
N X 1 Гбит/с	3	6660
10 Гбит/с	2	2,000

100 Гбит/с	Н/Д	200
1 ТБ/сек	Н/Д	20
10 ТБ/сек	Н/Д	2

Примечание: В CatOS стоимость порта связующего дерева для EtherChannel остается то же после сбоя участвующего соединения канала порта. В программном обеспечении Cisco IOS стоимость порта для EtherChannel обновляется немедленно для отображения нового значения доступной ширины полосы пропускания. *Если необходимо избегать ненужных изменений топологии связующего дерева, можно настроить стоимость порта связующего дерева статически при помощи команды стоимости spanning-tree cost стоимость.*

Протокол агрегации портов (PAgP)

Цель

Протокол PAgP представляет собой протокол управления, обеспечивающий проверку согласованности параметров на обоих концах канала. PAgP также помогает каналу с адаптацией при сбое или добавлении канала. Ниже приведены характеристики PAgP:

- Для PAgP требуется, чтобы все порты в канале принадлежали одной VLAN или были настроены в качестве портов магистрали. Поскольку динамические VLAN могут вызывать изменение порта в другой VLAN, динамические VLAN не принимают участия в EtherChannel.
- Когда пучок уже существует, а конфигурация порта изменяется, изменяются все порты в пучке, для того чтобы соответствовать этой конфигурации. `VLAN trunking.`
- PAgP не группирует порты, работающие на различных скоростях, или дуплексные порты. Если скорость или дуплексный режим изменяются, когда каналы объединены в группу, PAgP изменит скорости портов и дуплексный режим для всех портов в группе.

Технологическое описание

Порт PAgP контролирует каждый индивидуальный физический (или логический) порт, который должен быть сгруппирован. Тот же самый MAC-адрес многоадресной группы, который используется для пакетов CDP, используется и для рассылки пакетов PAgP. Этот MAC-адрес – 01-00-0c-cc-cc-cc. Но значение протокола – 0x0104. Ниже приведено краткое описание работы протокола:

- Если физический порт работает, пакеты PAgP передаются каждую секунду во время обнаружения и каждые 30 секунд в устойчивом режиме.
- При получении пакетов данных и отсутствии пакетов PAgP считается, что порт подключен к устройству без поддержки PAgP.
- Протокол ищет пакеты PAgP, которые подтвердили бы, что физический порт имеет двустороннее соединение с другим устройством, поддерживающим PAgP.
- Как только группа физических портов получает два таких пакета, протокол пытается сформировать агрегированный порт.
- `PAgP , PAgP - "".`

Нормальная обработка

Следующие понятия помогут продемонстрировать поведение протокола:

- Agport – логический порт, состоящий из всех физических портов одной группы и

идентифицируемый собственным ifIndex SNMP. Agport не содержит неработающих портов.

- Канал – группа, удовлетворяющая критерию формирования. Канал может содержать неработающие порты и надмножество agport. Протоколы, включающие STP и VTP, но исключающие CDP и DTP, работают поверх PAgP в портах agport. Для этих протоколов передача и прием пакетов невозможны до тех пор, пока протокол PAgP не подключит порты agport к одному или нескольким физическим портам.
- – agport , group-capability. , group-capability, .
- – UpData UpPAgP agport. Когда порт переходит из какого-либо из этих состояний в другое, он отсоединяется от agport.

Эта таблица содержит дополнительную информацию об этих состояниях:

Состояние	Значение
UpData	Не было получено ни одного пакета PAgP. Отправка пакетов PAgP выполнена. Физический порт – это единственный порт, подключенный к agport. Выполнена двусторонняя передача отличных от PAgP пакетов между физическим портом и портом agport.
BiDir	Ровно один пакет PAgP был получен, что свидетельствует о существовании двунаправленного соединения ровно с одним соседом. Физический порт не подключен ни к какому агрегируемому порту. Пакеты PAgP переданы и могут быть получены.
UpPAgP	Этот физический порт, возможно в сопоставлении с другими физическими портами, подключен к агрегируемому порту. Пакеты PAgP отправляются и принимаются в физическом порту. Выполнена двусторонняя передача отличных от PAgP пакетов между физическим портом и портом agport.

Оба конца обоих соединений должны быть согласны на группирование. Группирование определено как наибольшая группа портов в agport, разрешенная обоими концами соединения.

UpPAgP, agport, , group-capability BiDir UpPAgP. (, BiDir, UpPAgP.). При отсутствии agport, параметры составляющего физического порта которого совместимы с новым физическим портом, порту назначается agport с подходящими параметрами, который не имеет связанных физических портов.

Задержка PAgP может возникнуть на последнем соседе, известном физическому порту. Порт, превысивший время ожидания, удаляется из agport. В то же время удаляются все физические порты на одном порту agport, на таймерах которых также превышено время ожидания. Это позволяет отключить целиком весь агрегируемый порт, на другом конце которого потеряна связь, вместо последовательного отключения одного физического порта за другим.

Поведение при сбое

Если на линии связи в существующем канале произошел сбой, agport обновляется, а трафик направляется по линиям связи, оставшимся в рабочем состоянии. Примеры таких сбоев следующие:

- Порт не подключен
- Преобразователь интерфейса Gigabit (GBIC) удален
- Оптоволоконный кабель сломан

Примечание: При сбое ссылки в канале с питанием прочь или удалением модуля поведение может быть другим. По определению каналу необходимо два физических порта. Если один порт пропадает из системы в двухпортовом канале, логический agport разрывается, а исходный физический порт повторно инициализируется на основе связующего дерева. Трафик может отклоняться до тех пор, пока STP не позволит порту снова стать доступным для данных.

Эта разница в двух режимах сбоя важна при планировании эксплуатации сети. При интерактивном удалении или добавлении модуля необходимо принимать в расчет возможные изменения топологии STP. Необходимо управлять каждым физическим портом в канале при помощи системы управления сетями (NMS), так как agport может оставаться нетронутым из-за сбоя.

Для того чтобы смягчить нежелательные изменения топологии на Catalyst 6500/6000, необходимо следовать одной из следующих рекомендаций:

- Если для формирования канала используется один канал на модуль, необходимо использовать три или более модулей (всего три).
- Если канал соединяет два модуля, на каждом модуле должно использоваться два порта (всего четыре).
- Если между двумя платами необходим двухпортовый канал, нужно использовать только порты Supervisor Engine.

Параметры настройки

Каналы EtherChannel LACP можно настраивать для работы в разных режимах, как показано в таблице:

Режим	Настраиваемые параметры
	PAgP не работает. Порт продолжает передачу по каналу вне зависимости от того, как настроен соседний порт. `on`, .
`Auto`	Агрегирование выполняется под управлением PAgP. Порт переведен в состояние пассивного согласования. `PAgP` , `PAgP`, , `desirable`.
`Desirable`	Агрегирование выполняется под управлением PAgP. Порт переводится в состояние активного согласования, в котором порт начинает согласование с другими портами, посылая пакеты PAgP. .

Non-silent Это - по умолчанию на FE волокна Catalyst 5500/5000 и портах GE.	. Если интерфейсом не были получены никакие пакеты данных, этот интерфейс не будет подключен к agport и не может использоваться для данных. Эта проверка двунаправленности была предложена для определенного оборудования Catalyst 5500/5000, так как некоторые сбои линий связи происходили из-за поломок канала извне. non-silent . По умолчанию в оборудовании Catalyst серий 4500/4000 и 6500/6000 присутствует более гибкое объединение и улучшенная проверка двунаправленности.
Silent Это - по умолчанию на всем Catalyst 6500/6000 и 4500/4000 портах, а также 5500/5000 медных портах.	. Если интерфейсом не были получены никакие пакеты данных, после 15 секунд ожидания интерфейс будет один подключен к agport. Таким образом, этот интерфейс может быть использован для передачи данных. , , PAgP.

silent/non-silent , , . Когда порт не может передавать данные по причине сбоя физического интерфейса или разрыва оптоволокна или кабеля, соседний порт все еще может оставаться в рабочем состоянии. Партнер продолжает передавать данные. Но данные буду утеряны, потому что обратный трафик не может быть получен. По причине однонаправленности линии связи также могут формироваться петли связующего дерева.

На некоторых оптоволоконных портах есть возможность перевода порта в нерабочее состояние при потере им входящего сигнала (FEFI). Это действие приводит к тому, что порт-партнер становится нерабочим, и в результате порты на обоих концах линии связи отключаются.

, (BPDU), non-silent, , . Время, необходимое PAgP на определение однонаправленности линии, составляет около 3,5 * 30 сек = 105 сек. Тридцать секунд – это время между прохождением двух успешных сообщений PAgP. UDLD является более быстрым детектором однонаправленных каналов.

, , silent. silent , . , , , silent . Примерами таких портов являются новейшие платформы, использующие FEFI и UDLD уровня 1.

Для того чтобы выключить на интерфейсе выделение каналов, необходимо выполнить команду no channel-group number:

```
Switch(config)#interface type slot#/port# Switch(config-if)#no channel-group 1
```

Проверка

PAgP , . , STP errDisable, , . Функциональная возможность защиты от неправильной настройки EtherChannel включена по умолчанию.

Режим канала коммутатора A	Режим канала коммутатора B	Состояние канала коммутатора A	Режим создания логических каналов в коммутаторе B
Включено	Включено	Канал (не PAgP)	Канал (не PAgP)
Включено	Не настроен	Нет канала (errdisable)	Нет канала
Включено	Auto	Нет канала (errdisable)	Нет канала
Включено	Desirable	Нет канала (errdisable)	Нет канала
Не настроен	Включено	Нет канала	Нет канала (errdisable)
Не настроен	Не настроен	Нет канала	Нет канала
Не настроен	Auto	Нет канала	Нет канала
Не настроен	Desirable	Нет канала	Нет канала
Auto	Включено	Нет канала	Нет канала (errdisable)
Auto	Не настроен	Нет канала	Нет канала
Auto	Auto	Нет канала	Нет канала
Auto	Desirable	Канал PAgP	Канал PAgP
Desirable	Включено	Нет канала	Нет канала
Desirable	Не настроен	Нет канала	Нет канала
Desirable	Auto	Канал PAgP	Канал PAgP
Desirable	Desirable	Канал PAgP	Канал PAgP

Рекомендации Cisco по настройке каналов L2

PAgP desirable-desirable EtherChannel. Рассмотрим в качестве дополнительной информации следующие выходные данные:

```
Switch(config)#interface type slot#/port# Switch(config-if)#no ip address !--- This ensures that there is no IP !--- address that is assigned to the LAN port. Switch(config-if)#channel-group number mode desirable !--- Specify the channel number and the PAgP mode.
```

Удостоверьтесь, что настройки выглядят следующим образом:

```
Switch#show run interface port-channel number Switch#show running-config interface type slot#/port# Switch#show interfaces type slot#/port# etherchannel Switch#show etherchannel number port-channel
```

Предотвращение ошибок настройки EtherChannel

Существует возможность неправильной настройки EtherChannel, в результате чего возникнет петля связующего дерева. Такая неправильная настройка может привести к перегрузке процесса коммутации. **Для предотвращения подобной проблемы системное программное обеспечение Cisco IOS включает функциональную возможность spanning-tree etherchannel guard misconfig.**

Выполните следующую конфигурационную команду на всех коммутаторах Catalyst, использующих программное обеспечение Cisco IOS в качестве системного программного обеспечения:

```
Switch(config)#spanning-tree etherchannel guard misconfig
```

Дополнительные варианты

При соединении каналом двух устройств, не поддерживающих PAgP, но поддерживающих LACP, рекомендуется включить LACP, настроив его как LACP active на устройствах обоих концов. Дополнительные сведения см. в разделе Протокол управления агрегацией каналов (LACP) данного документа.

, PAgP LACP, on. Это требование применимо к следующим устройствам, приведенным для примера:

- Серверы
- Локальный управляющий узел
- Коммутаторы контента
- Маршрутизаторы
- Коммутаторы с ПО более ранних версий
- Коммутаторы Catalyst 2900XL/3500XL
- Catalyst 8540s

Введите следующие команды:

```
Switch(config)#interface type slot#/port# Switch(config-if)#channel-group number mode on
```

Протокол управления агрегацией каналов (LACP)

LACP представляет собой протокол, который позволяет портам со схожими характеристиками формировать логические каналы при помощи динамического согласования со смежными коммутаторами. PAgP – это принадлежащий Cisco протокол, который может работать только на коммутаторах Cisco и коммутаторах производства других лицензированных производителей. Однако LACP, определенный в IEEE 802.3ad, позволяет коммутаторам Cisco управлять организацией каналов Ethernet с устройствами, соответствующими спецификации 802.3ad.

LACP поддерживается следующими платформами и версиями:

- Catalyst серии 6500/6000 с программным обеспечением Cisco IOS 12.1(11b)EX и более

поздних версий
- Серия Catalyst 4500 с программным обеспечением Cisco IOS 12.1(13)EW и более поздних версий
- Серия Catalyst 3750 с программным обеспечением Cisco IOS 12.1(14)EA1 и более поздних версий

С функциональной точки зрения между LACP и PAgP очень небольшая разница. Оба протокола поддерживают не более восьми портов в каждом канале, а перед формированием группы проверяются одинаковые свойства портов. Среди этих свойств портов:

- Скорость
- Дуплекс
- Собственная VLAN и тип транкинга

LACP и PAgP значительно различаются в следующем:

- Протокол LACP может работать только на полнодуплексных портах и не поддерживает полудуплексных портов.
- Протокол LACP поддерживает порты горячего резервирования. LACP всегда пытается настроить максимальное количество совместимых портов в канале, допустимое оборудованием (восемь портов). Если LACP не может агрегировать все совместимые порты (например, если удаленная система имеет более строгие аппаратные ограничения), все порты, которые нельзя активно включить в канал, переводятся в состояние горячего резервирования и используются только при сбое одного из используемых портов.

Примечание: Для Коммутаторов серии Catalyst 4500 максимальное число портов, для которых можно назначить тот же административный ключ, равняется восьми. Для коммутаторов Catalyst 6500 и 3750, работающих на базе программного обеспечения Cisco IOS, LACP пытается настроить максимальное количество совместимых портов в канале EtherChannel, которое допускает оборудование (восемь портов). Дополнительно восемь портов можно настроить в качестве горячего резерва.

Технологическое описание

LACP контролирует все индивидуальные физические (или логические) порты, которые должны быть включены в группу. **Пакеты LACP передаются с использованием группового MAC-адреса многоадресной рассылки, 01-80-c2-00-00-02.** Тип/рабочее значение равно 0x8809 с подтипом 0x01. Ниже приведено краткое описание работы протокола:

- Протокол полагается на объявление возможностей агрегирования и информации о состоянии устройств самими устройствами. Пакеты пересылаются периодически на каждый "агрегируемый" физический канал.
- Если физический порт работает, пакеты LACP передаются каждую секунду во время обнаружения и каждые 30 секунд в устойчивом режиме.
- Партнеры по агрегируемому соединению отслеживают информацию, которая передается по протоколу, и принимают решение о том какое действие или действия предпринять.
- Совместимые порты, количество которых может быть не более допустимого оборудованием (восемь портов), настраиваются в канал.
- Агрегирования поддерживаются посредством постоянного своевременного обмена

обновленной информацией о состоянии между партнерами по соединению. При изменении конфигурации (из-за сбоя соединения, например), время ожидания партнеров по протоколу истекает, и они предпринимают действия в соответствии с новым состоянием системы.
- Кроме периодической передачи блоков данных LACP (LACPDU), при наличии изменений в информации о состоянии, протокол передает партнерам LACPDU, обусловленные определенными событиями. Партнеры по протоколу предпринимают действия в соответствии с новым состоянием системы.

Параметры LACP

Для того чтобы LACP мог определить, что совокупность линий связи подключена к одной системе и что эти линии связи совместимы с точки зрения агрегирования, необходима возможность определения следующих параметров:

- Глобально уникальный идентификатор для каждой системы, участвующей в агрегировании линий связи.Каждой системе, работающей с LACP, должен быть назначен приоритет, который либо выбирается автоматически (приоритет по умолчанию – 32768), либо назначается администратором. Приоритет системы главным образом используется в сочетании с MAC-адресом системы для формирования идентификатора системы.
- Способ идентифицировать набор возможностей, связанных с каждым портом и с каждым агрегатором, как понятные для данной системы.Каждому порту в системе должен быть назначен приоритет, который либо выбирается автоматически (приоритет по умолчанию – 128), либо назначается администратором. Приоритет используется в сочетании с номером порта для формирования идентификатора порта.
- Возможность идентифицировать группу агрегирования каналов связи и связанный с ней агрегатор.Возможность агрегирования порта с другими портами определяется простым 16-битовым целочисленным параметром, строго большим нуля, который называется ключом. Каждый ключ определяется на основании различных факторов, таких как:Физические характеристики порта, включающие скорость передачи данных, дуплексный режим и соединение типа «точка-точка» или общая среда обмена даннымиОграничения настройки, наложенные администратором сетиДва ключа, связанных с каждым из портов:Административный ключРабочий ключАдминистративный ключ позволяет администрации манипулировать значениями ключей, следовательно, пользователь может выбирать этот ключ. Рабочий ключ используется системой для формирования объединений. Пользователь не может напрямую выбирать или изменять данный ключ. Порты в системе, для которых используется одно и то же значение рабочего ключа, называются участниками одной ключевой группы.

Таким образом, при наличии двух систем и совокупности портов с одним административным ключом, каждая из систем попытается объединить порты, начиная с порта и системы с наивысшими приоритетами. Такое поведение возможно, потому что каждой системе известны следующий приоритеты:

- Ее собственный приоритет, назначенный пользователем или программным обеспечением
- Приоритет партнера, взятый из пакетов LACP

Поведение при сбое

Поведение LACP при сбое аналогично поведению при сбое PAgP. Если в линии связи существующего канала произошел сбой (например, если отключен порт, удален GBIC или нарушено оптоволокно), агрегированный порт обновляется и в течение одной секунды трафик перераспределяется между оставшимися соединениями. Трафик, не требующий перераспределения после сбоя (трафик, который продолжает идти через ту же линию связи), не испытывает никаких потерь. Восстановление нарушенной линии связи приводит к новому обновлению агрегированного порта и трафик перераспределяется снова.

Параметры настройки

Каналы EtherChannel LACP можно настраивать для работы в разных режимах, как показано в таблице:

Режим	Настраиваемые параметры
Включено	Агрегирование линий связи производится принудительно без согласования LACP. Коммутатор не пересылает пакеты LACP и не обрабатывает входящие пакеты LACP. Если соседний порт находится в режиме on, то формируется канал.
Off (или) Not Configured	Порт не участвует в формировании логического канала вне зависимости от того, как настроен соседний порт.
Passive (режим по умолчанию)	**Это аналогично автоматическому режиму в PAgP.** Коммутатор не инициирует создание логического канала, но понимает входящие пакеты LACP. Соседний узел (в состоянии active) инициирует согласование (передачей пакета LACP), который коммутатор получает и на который отвечает, в конце концов формируя агрегированный канал с соседним узлом.
Активный	**Аналогичен режиму desirable в PAgP.** Для формирования агрегированной линии связи коммутатор инициирует согласование. Объединение линий связи формируется, если другая сторона работает в режимах LACP active или passive.

Кроме того, после установления каналов EtherChannels LACP протокол LACP использует таймер (Slow_Periodic_Time) с 30-секундным интервалом. Количество секунд до аннулирования полученной информации LACPDU при использовании длинных задержек (3 умножить на Slow_Periodic_Time) составляет 90. UDLD рекомендован как более быстрое средство обнаружения однонаправленных линий связи. Таймеры LACP нельзя регулировать, а поэтому нельзя настраивать коммутаторы на использование быстрого протокола передачи блоков данных PDU (каждую секунду) в целях поддержания канала после его формирования.

Проверка

Таблица в этом разделе содержит краткое изложение всех возможных сценариев режима создания каналов LACP между двумя напрямую соединенными коммутаторами (Коммутатор A и Коммутатор B). Некоторые из этих комбинаций могут привести к тому, что защита EtherChannel переведет порты со стороны, создавшей канал, в состояние errdisable. Функциональная возможность защиты от неправильной настройки EtherChannel включена по умолчанию.

Режим канала коммутатора A	Режим канала коммутатора B	Состояние канала коммутатора A	Режим создания логических каналов в коммутаторе B
Включено	Включено	Канал (не LACP)	Канал (не LACP)
Включено	Выключен	Нет канала (errdisable)	Нет канала
Включено	Пассивный	Нет канала (errdisable)	Нет канала
Включено	Активный	Нет канала (errdisable)	Нет канала
Выключен	Выключен	Нет канала	Нет канала
Выключен	Пассивный	Нет канала	Нет канала
Выключен	Активный	Нет канала	Нет канала
Пассивный	Пассивный	Нет канала	Нет канала
Пассивный	Активный	Канал LACP	Канал LACP
Активный	Активный	Канал LACP	Канал LACP

Рекомендации Cisco

Cisco рекомендует включать PAgP в соединенных логическими каналами коммутаторах Cisco. При соединении каналом двух устройств, не поддерживающих PAgP, но поддерживающих LACP, рекомендуется включить LACP, настроив его как LACP active на устройствах обоих концов.

По умолчанию все порты коммутаторов Catalyst 4500/4000 и Catalyst 6500/6000, работающих под управлением CatOS, используют PAgP как протокол канала. Для настройки использования на портах LACP необходимо установить протокол канала в модулях в значение LACP. В коммутаторах, работающих под управлением CatOS, LACP и PAgP не могут одновременно работать в одном модуле. Это ограничение не применяется к коммутаторам, работающим под управлением программного обеспечения Cisco IOS. Коммутаторы, работающие под управлением программного обеспечения Cisco IOS, могут поддерживать работу PAgP and LACP в одном модуле. Выполните следующие команды для того, чтобы установить режим канала LACP в состояние active и назначить номер административного ключа:

`Switch(config)#`**`interface range`** *`type slot#/port#`* `Switch(config-if)#`**`channel-group`** *`admin_key`* **`mode active`**

Команда show etherchannel summary отображает сводные данные по группе каналов, включающие следующую информацию:

- Номера групп
- Номера каналов порта
- Состояние портов
- Порты, входящие в состав канала

Команда show etherchannel port-channel отображает подробную информацию о канале порт для всех групп каналов. Выходные данные включают следующую информацию:

- Состояние канала
- Используемый протокол
- Период времени с объединения портов

Для того чтобы отобразить подробную информацию об определенной группе каналов с отдельно показанными данными каждого порта, необходимо использовать команду show etherchannel channel_number detail. Выходные данные этой команды включают подробную информацию о партнере и канале порта. Для получения дополнительной информации, см. Настройка LACP (802.3ad) между Catalyst 6500/6000 и Catalyst 4500/4000.

Дополнительные варианты

`,  PAgP or LACP,  on.` Это требование применимо к следующим устройствам:

- Серверы
- Локальный управляющий узел
- Коммутаторы контента
- Маршрутизаторы
- Коммутаторы с ПО более поздних версий
- Коммутаторы Catalyst 2900XL/3500XL
- Catalyst 8540s

Введите следующие команды:

`Switch(config)#`**`interface range`** *`type slot#/port#`* `Switch(config-if)#`**`channel-group`** *`admin_key`* **`mode on`**

Обнаружение однонаправленного канала

Цель

UDLD – это принадлежащий Cisco упрощенный протокол, разработанный для обнаружения однонаправленных соединений между устройствами. Существуют и другие способы обнаружения двунаправленного состояния среды передачи, такие как FEFI. Но есть определенные случаи, для которых механизмов обнаружения уровня 1 недостаточно. К таким случаям могут привести:

- Непредсказуемая работа STP
- Неправильная или избыточная лавинная маршрутизация пакетов
- Исчезновение трафика

Функция UDLD отслеживает следующие условия сбоя в оптоволоконных и медных

интерфейсах Ethernet:

- errdisable.
- – , /, errDisabled. В системном журнале генерируются соответствующие сообщения.
- Кроме того, в агрессивном режиме UDLD проверяет, чтобы линия связи, ранее считавшаяся двунаправленной, не потеряла способности к подключению вследствие того, что линия стала непригодной для использования из-за перегрузки. UDLD в агрессивном режиме непрерывно проверяет способность линии связи к подключению. Основная задача агрессивного режима UDLD заключается в предотвращении исчезновения трафика в условиях некоторых неисправностей, которые не могут быть обнаружены при работе UDLD в нормальном режиме.

Дополнительные сведения см. в документе Общие сведения и настройка протокола обнаружения однонаправленных соединений (UDLD).

Связующее дерево имеет устойчивый режим однонаправленного потока BPDU и может подвергаться сбоям, перечисленным в этом разделе. BPDU, STP blocking forwarding. Однако будет все еще существовать петля, потому что порт не утратил способности получать данные.

Технологическое описание

UDLD – это протокол уровня 2, работающий над уровнем LLC (MAC-адрес назначения 01-00-0c-cc-cc-cc, тип протокола SNAP HDLC 0x0111). При работе UDLD в комбинации с механизмами FEFI и автоматического согласования уровня 1 можно проверять физическую (уровня 1) и логическую (уровня 2) целостность соединения.

UDLD обеспечивает функциональные возможности и защиту, которые не могут обеспечить FEFI и автосогласование. Это следующие функциональные возможности:

- Обнаружение и хранение информации о соседях
- Отключение любого неправильно подключенного порта
- Обнаружение неисправностей логических интерфейсов/портов или ошибок в линиях связи типа, отличного от «точка-точка»**Примечание:** Когда ссылки не являются точка-точка, они пересекают медиаконвертеры или концентраторы.

UDLD применяет два основных механизма.

1. UDLD изучает информацию о соседних узлах и хранит свежую информацию в локальном кэше.
2. При обнаружении нового соседнего узла или когда соседний узел запрашивает повторную синхронизацию кэша, UDLD передает группу сообщений UDLD probe/echo (hello).

UDLD постоянно посылает сообщения probe/echo на все порты. При получении на порт соответствующего сообщения UDLD начинается фаза обнаружения и процесс проверки. Порт будет включен, если будут соблюдены все необходимые условия. Для соблюдения условий порт должен быть двунаправленным и правильно подключенным. , errDisabled, :

```
UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link.
   Port disabled
UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link.
```

```
   Failed to disable port
UDLD-3-DISABLE: Unidirectional link detected on port disabled.
UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port.
UDLD-3-SENDFAIL: Transmit failure on port.
UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars]
   was detected.
```

Полный список системных сообщений по механизмам, среди которых также события UDLD, см. в документе Сообщения UDLD (системные сообщения Cisco IOS, часть 2 из 2).

После того как соединение установлено и классифицировано как двунаправленное, UDLD продолжает рассылать сообщения probe/echo через установленные по умолчанию интервалы времени, равные 15 секундам.

Следующая таблица содержит информацию о состоянии портов:

Состояние порта	Комментарий
Неопределенный	Выполняется определение/соседний элемент UDLD был отключен.
Не применимо	UDLD отключен.
Отключение	Обнаружена однонаправленная линия связи и порт отключен.
Bidirectional	Обнаружен двунаправленный канал.

Поддержание кэша соседнего узла

UDLD периодически отправляет пакеты hello probe/echo на каждый активный интерфейс, чтобы обеспечивать целостность кэша UDLD соседнего узла. Всякий раз, когда принимается сообщение hello, оно кэшируется и хранится в памяти в течение максимального периода, определенного как время промежуточного хранения. Когда время ожидания истекает, соответствующая запись кэша устаревает. Если новое приветственное сообщение получено в течение этого времени занятости, происходит замена старой записи на новую и сброс соответствующего таймера времени существования.

При отключении интерфейса, поддерживаемого UDLD, или перезагрузке устройства все имеющиеся записи кэша об интерфейсах, затронутых изменением конфигурации, удаляются. Такое удаление поддерживает целостность кэша UDLD. UDLD передает как минимум одно сообщение, информирующее соседние узлы о необходимости удалить соответствующие записи кэша.

Механизм обнаружения эхо-ответов

Механизм эха формирует основу для алгоритма обнаружения. Когда устройство UDLD узнает о новом соседнем узле или получает запрос на повторную синхронизацию от несинхронизированного соседнего узла, оно запускает или перезапускает окно обнаружения на своей стороне подключения и отправляет в ответ пакет эхо-сообщений. Поскольку такое поведение должно быть одинаковым для всех соседних узлов, отправитель эхо-запроса ожидает получить эхо-ответ. Если достигнут конец окна обнаружения и при этом не было получено ни одного корректного ответного сообщения, линия связи считается однонаправленной. На этом этапе может быть инициирован процесс переподключения или выключения порта. Иначе устройство может осуществить проверку на редкие аномальные условия такие, как:

- Оптоволокно обратной передачи (Tx) и Rx разъем принадлежат одному и тому же порту
- Неправильные подключения в случае совместной среды внутреннего подключения (например, концентратор или подобное устройство)

Время сходимости

Для предотвращения образования петель STP, в программном обеспечении Cisco IOS 12.1 и более поздних версий интервал передачи сообщений UDLD, установленный по умолчанию, уменьшен с 60 секунд до 15 секунд. Этот интервал был изменен для того, чтобы отключать однонаправленную линию связи до того, как ранее заблокированный порт связующего дерева 802.1D сможет перейти в состояние forwarding. Значение интервала между сообщениями определяет скорость, с которой соседний узел отсылает проверочные сообщения UDLD после фазы включения соединения или определения. Интервал между сообщениями не обязательно должен совпадать на обоих концах соединения, хотя по возможности рекомендуется поддерживать согласованную конфигурацию. Когда соседние узлы UDLD установлены, соседу посылается значение интервала между сообщениями и вычисляется время задержки для этого соседнего узла следующим образом:

```
3 * (message interval)
```

Связь с соседним узлом прерывается после истечения времени ожидания вследствие пропуска трех последовательных сообщений hello (или probe). Так как интервалы между сообщениями различаются с обеих сторон, это значение времени ожидания также различается и одна сторона определяет сбой быстрее.

Приблизительное время, необходимое UDLD для обнаружения однонаправленного сбоя ранее стабильной линии связи, составляет:

```
2.5 * (message interval) + 4 seconds
```

Это приблизительно 41 секунда при интервале между сообщениями, установленному по умолчанию, в 15 секунд. Это значительно меньше 50 секунд, которые обычно требуются для схождения STP. Если у ЦП NMP есть несколько свободных циклов и при тщательном отслеживании уровня загрузки (рекомендуем) можно уменьшить интервал между сообщениями до минимального значения, составляющего 7 секунд. Такой интервал между сообщениями помогает значительно ускорить обнаружение по значительным факторам.

Примечание: Минимум составляет 1 секунду в программном обеспечении Cisco IOS версии 12.2(25)SEC.

Таким образом, UDLD имеет предполагаемую зависимость от таймеров связующего дерева по умолчанию. При настройке более быстрой сходимости STP по сравнению с UDLD следует рассмотреть возможность использования альтернативного механизма, как, например, функции loop guard STP. Возможность использования альтернативного механизма следует рассмотреть также в случаях использования RSTP (802.1w), поскольку сходимость RSTP исчисляется миллисекундами и зависит от топологии. В таких случаях необходимо использовать loop guard в сочетании с UDLD, чтобы обеспечить максимальную защиту. Loop guard предотвращает образование петель STP со скоростью используемой версии STP. А UDLD обнаруживает однонаправленные линии связи в отдельных линиях EtherChannel или в случаях, когда в нарушенном направлении не передаются BPDU.

Примечание: UDLD независим от STP По этой причине Cisco рекомендует в топологиях, основанных на STP, использовать UDLD в сочетании с функцией loop guard.

Внимание. : Остерегайтесь более ранних релизов UDLD в коммутаторах 2900XL/3500XL, которые используют неизменяемый, 60-секундный стандартный интервал сообщений. Эти версии подвержены образованию петель связующего дерева.

Агрессивный режим UDLD

Агрессивный UDLD был создан специально для тех нескольких случаев, в которых требуется непрерывная проверка двунаправленности подключения. По существу, функция агрессивного режима обеспечивает улучшенную защиту от опасных условий образования однонаправленных линий связи в следующих ситуациях:

- Когда потеря PDU UDLD является симметричной и на обоих концах происходит превышение времени ожидания. В этом случае ни один из портов не переходит в состояние errdisabled.
- На одной стороне линии связи порт зависает (осуществляет и передачу (Tx) и прием (Rx)).
- Один конец канала остается в рабочем состоянии, в то время как другой отключается.
- Автосогласование или другой механизм обнаружения сбоев уровня 1 отключены.
- Желательно не особо полагаться на механизмы FEFI уровня 1.
- Необходима максимальная защита от сбоев однонаправленных линий связи в каналах FE/GE типа «точка-точка». В частности, там, где недопустимы сбои между двумя соседними узлами, проверочные сообщения агрессивного режима UDLD можно рассматривать как пульсацию, наличие которой гарантирует работоспособность соединения.

Наиболее распространенным случаем использования агрессивного режима UDLD является проверка подключения участника группы, когда автосогласование или другой механизм обнаружения сбоев на уровне 1 отключены или бесполезны. Это в особенности полезно для соединений EtherChannel, поскольку PAgP и LACP, даже когда они включены, в устойчивом состоянии не используют очень маленькие значения таймеров сообщений hello. В этом случае агрессивный режим UDLD обладает дополнительным преимуществом предупреждения образования петель связующего дерева.

Важно понимать, что в обычном режиме UDLD выполняет проверку на условия однонаправленной линии связи, даже после того, как линия перейдет в двунаправленное состояние. Цель UDLD заключается в обнаружении проблем уровня 2, приводящих к образованию петель STP, а эти проблемы обычно связаны с однонаправленностью (поскольку в устойчивом состоянии BPDU передаются только в одном направлении). Поэтому использование обычного UDLD в сочетании с автосогласованием и loop guard (для сетей, полагающихся на STP) практически всегда является достаточным. При включенном агрессивном режиме UDLD после устаревания всех соседних узлов порта в фазе объявления или в фазе обнаружения, агрессивный режим UDLD перезапускает последовательность установления соединений, пытаясь выполнить ресинхронизацию с любыми потенциально рассинхронизированными соседними узлами. Если после быстрой последовательности сообщений (восемь неудачных попыток) соединение все еще считается неопределенным, порт переводится в состояние errdisable.

Примечание: В некоторых коммутаторах отсутствует поддержка интенсивного режима UDLD. В настоящее время интервал между сообщениями в Catalyst 2900XL и Catalyst 3500XL установлен неизменным и равен 60 секундам. Этот значение не считается достаточно коротким для защиты от потенциального возникновения петель STP (с использованием параметров STP по умолчанию).

Автоматическое восстановление линий связи UDLD

По умолчанию восстановление из состояния errdisable на глобальном уровне отключено. После его глобального включения, если порт переходит в состояние errdisable, то через заданный промежуток времени происходит автоматическое включение порта. По умолчанию это время составляет 300 секунд. Значение этого таймера является глобальным и поддерживается для всех портов в коммутаторе. В зависимости от релиза программного обеспечения можно вручную предотвратить повторное включение порта, отключив время ожидания состояния errdisable для этого порта при помощи механизма UDLD восстановления после истечения времени ожидания состояния errdisable:

```
Switch(config)#errdisable recovery cause udld
```

Следует рассмотреть возможность использования времени ожидания состояния errdisable при использовании интенсивного режима UDLD при отсутствии возможностей управления сетью через выделенное подключение, в частности на уровне доступа или в любом устройстве, которое становится изолированным от сети в случае возникновения состояния errdisable.

Дополнительные сведения о том, как настроить время ожидания портов в состоянии errdisable, см. в разделе Восстановление из состояния errdisable (справочник Catalyst 6500 Series Cisco IOS, 12.1 E).

Восстановления после состояния errdisable может быть особенно важным для UDLD на уровне доступа, когда коммутаторы доступа распределены по кампусной среде и обслуживание каждого коммутатора вручную для восстановления обоих восходящих каналов занимает значительное время.

Cisco не рекомендует подключать функциональную возможность восстановления после состояния errdisable в ядре сети, так как в ядро обычно есть множество точек входа и автоматическое восстановление может привести к повторяющимся проблемам. Поэтому в случае, если UDLD отключит порт в ядре, его нужно будет подключить вручную.

UDLD в маршрутизируемых линиях связи

В данном разделе маршрутизируемое соединение – это соединение одного из двух типов:

- Соединение типа «точка-точка» между двумя узлами маршрутизатора (настроенное с 30-битовой маской подсети)
- VLAN с множеством портов, но поддерживающая только маршрутизируемые соединения, как например разделенная топология ядра уровня 2

Все протоколы внутренней маршрутизации шлюзов (IGRP) обладают уникальными характеристиками в отношении того, как они обрабатывают соседние связи и сходимость маршрутов. Этот раздел рассматривает характеристики, являющиеся значимыми для обсуждаемой темы при сравнении двух и более распространенных протоколов маршрутизации, используемых сегодня: протокол открытия кратчайшего пути (OSPF) и усовершенствованный IGRP (EIGRP).

Примечание: Сбой Уровня 1 или Уровня 2 на любой протрассированной сети "точка-точка" приводит к почти мгновенное освобождение соединения Уровня 3. Поскольку единственный порт коммутатора в этой VLAN при ошибке уровня 1/уровня 2 переходит в неподключенное состояние, функция автоматического определения состояния интерфейса синхронизирует состояния порта уровня 2 и уровня 3 приблизительно за две секунды и переводит

интерфейс VLAN уровня 3 в состояние up/down (при выключенном протоколе линии связи).

При установленных по умолчанию значениях таймера OSPF передает сообщения hello каждые 10 секунд, время ожидания ответа составляет 40 секунд (4 * hello). Эти таймеры согласуются для сетей OSPF с соединениями типа "точка-точка" и широковещательных сетей. Поскольку для формирования смежности для OSPF требуется двунаправленное соединение, время восстановления после сбоя в худшем случае составляет 40 секунд. Это выполняется даже в случае, когда сбой уровня 1/уровня 2 в соединении типа «точка-точка» не является полным, оставляя неясную ситуацию, с которой должен работать протокол уровня 3. Поскольку определение времени в UDLD очень похоже на определение времени таймера бездействия OSPF (около 40 секунд), преимущества конфигурации обычного режима UDLD в линиях связи типа "точка-точка" уровня 3 OSPF являются ограниченными.

В большинстве случаев EIGRP сходится быстрее OSPF. Однако необходимо помнить, что двунаправленное соединение не является необходимым условием для того, чтобы соседние узлы обменивались информацией о маршрутах. В очень ограниченных случаях неполного сбоя протокол EIGRP уязвим в плане исчезновения трафика, которое длится до тех пор, пока другое событие не создаст маршруты посредством приведения соседнего узла в состояние active. Обычный режим UDLD может смягчить эту обстановку, потому что он обнаруживает ошибку однонаправленной линии связи и отключает порт в результате этой ошибки.

Для маршрутизируемых соединений уровня 3, использующих любой протокол маршрутизации, обычный режим UDLD еще и обеспечивает защиту от неполадок, присутствующих при начальном включении соединения, таких как неправильное подключение или неисправное оборудование. Кроме того, агрессивный режим UDLD обеспечивает в маршрутизируемых подключениях уровня 3 следующие преимущества:

- Предотвращает ненужное исчезновение трафика (при минимальных значениях таймеров, требуемых в некоторых случаях)
- Переводит нестабильную линию связи в состояние errdisable
- Обеспечивает защиту от петель, возникающих вследствие настроек EtherChannel уровня 3

Поведение UDLD при настройках по умолчанию

По умолчанию служба UDLD отключена на глобальном уровне и включена на оптоволоконных портах. Поскольку UDLD – это инфраструктурный протокол, необходимый только между коммутаторами, по умолчанию на медных портах, используемых только для доступа хостов, UDLD отключен. Необходимо заметить, что UDLD должен быть включен глобально и на уровне интерфейса до того как соседние узлы смогут достичь статуса двунаправленных. Значение интервала между сообщениями по умолчанию равно 15 секундам. Но в некоторых случаях значение интервала между сообщениями по умолчанию может быть показано равным семи секундам. Обратитесь к дефекту номер CSCea70679 (только для зарегистрированных пользователей) для получения дополнительной информации. Значение интервала между сообщениями по умолчанию настраивается между семью и 90 секундами, а агрессивный режим UDLD должен быть отключен. В программном обеспечении Cisco IOS релиза 12.2(25)SEC минимальное значение таймера уменьшено до одной секунды.

Рекомендации Cisco по настройке

В преобладающем большинстве случаев Cisco рекомендует включать обычный режим

UDLD на всех линиях связи FE/GE типа «точка-точка» между коммутаторами Cisco, и устанавливать интервал между сообщениями UDLD в значение 15 секунд при использовании стандартных таймеров связующего дерева 802.1D. Кроме того, в целях обеспечения избыточности и сходимости (что означает, что существует один или более портов в топологии, находящиеся в состоянии STP blocking) в сетях, полагающихся на STP, следует использовать UDLD в сочетании с подходящими функциональными возможностями и протоколами. Такими функциональными возможностями могут быть FEFI, автосогласование, loop guard и так далее. Обычно при включенном автосогласовании нет необходимости использовать агрессивный режим, поскольку автосогласование компенсирует обнаружение сбоев на уровне 1.

Для того чтобы включить UDLD выполните одну из двух следующих команд:

Примечание: Синтаксис изменился через различные платформы/версию.

- **udld enable** *!--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default.* **udld port** или
- **udld enable** *!--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled by individual port command.*

Порты, отключенные при возникновении симптомов однонаправленной линии связи, необходимо включать вручную. Используйте один из следующих методов:

udld reset *!--- Globally reset all interfaces that UDLD shut down.* **no udld port udld port [aggressive]** *!--- Per interface, reset and reenable interfaces that UDLD shut down.*

Команды глобальной конфигурации errdisable recovery cause udld и errdisable recovery interval interval могут использоваться для автоматического восстановления из состояния UDLD отключения в результате ошибки.

Cisco рекомендует использовать механизм восстановления из состояния errdisable только в портах доступа сети и со значениями таймеров восстановления 20 минут или более, если физический доступ к коммутатору проблематичен. Лучше всего оставить время на стабилизацию сети и осуществление поиска и устранения неисправностей до того, как порт вернется в строй и вызовет нестабильность сети.

Cisco рекомендует не использовать механизм восстановления в ядре сети, так как это может приводить к нестабильности, связанной с событиями сходимости, всякий раз, когда неисправная линия связи подключается вновь. Избыточное строение ядра сети обеспечивает резервный путь вместо неисправной линии связи и позволяет потратить некоторое время на исследование причин сбоя UDLD.

Используйте UDLD без STP Loop Guard

Для линий связи типа «точка-точка» уровня 3 или линий связи уровня 2 со свободной от петель топологией STP (нет заблокированных портов) Cisco рекомендует включать на линиях связи FE/GE типа «точка-точка» между коммутаторами Cisco агрессивный UDLD. В этом случае значение интервала между сообщениями составляет семь секунд, а STP 802.1D использует стандартные таймеры.

UDLD на каналах EtherChannel

Вне зависимости от того развернута или нет loop guard STP для любых конфигураций

EtherChannel рекомендуется агрессивный режим UDLD в сочетании с режимом канала desirable. В конфигурации EtherChannel сбой в линии связи канала, переносящего BPDU связующего дерева и управляющий трафик PAgP, может повлечь за собой немедленное образование петли между партнерами по каналу, если линии связи канала были разгруппированы. Агрессивный режим UDLD отключает порт, в котором произошел сбой. PAgP (режим канала auto/desirable) после этого может согласовать новую управляющую линию связи и эффективно удалить из канала линию связи, в которой произошел сбой.

UDLD со связующим деревом 802.1w

Для того чтобы предотвратить образование петель, при использовании новейших версий связующего дерева необходимо включать нормальный режим UDLD и loop guard STP с RSTP как 802.1w. *UDLD может обеспечить защиту от однонаправленных линий связи в течение фазы установления соединения, а loop guard STP может предотвратить образование петель STP после событий, приведших к тому, что линии связи стали однонаправленными после того, как UDLD установил, что эти линии двунаправленные.* Так как невозможно настроить UDLD таким образом, чтобы значения таймеров были меньше, чем значения стандартных таймеров 802.1w, loop guard STP необходима для того, чтобы полностью предотвратить образование петель в избыточных топологиях.

Дополнительные сведения см. в документе Общие сведения и настройка протокола обнаружения однонаправленных соединений (UDLD).

Тестирование и мониторинг UDLD

UDLD трудно проверить без откровенно неисправного/однонаправленного компонента, такого как дефектный GBIC, в лабораторных условиях. Этот протокол был разработан для выявления сценариев отказа, которые встречаются реже, чем те, которые обычно используют в тестовых условиях. , , , errdisable, 1. down, UDLD. undetermined UDLD errdisable UDLD.

Дополнительный способ проверки имитирует потерю PDU соседнего узла для UDLD. Метод состоит в том, чтобы использовать фильтры уровня MAC для блокирования аппаратных адресов UDLD/CDP и разрешения прохождения остальных адресов. Некоторые коммутаторы не посылают фреймов UDLD, когда порт настроен как порт назначения анализатора коммутируемых портов (SPAN), который имитирует не отвечающий соседний узел UDLD.

Для мониторинга UDLD используйте следующие команды:

show udld gigabitethernet1/1 Interface Gi1/1 --- Port enable administrative configuration setting: Enabled Port enable operational state: Enabled Current bidirectional state: Bidirectional Current operational state: Advertisement - Single neighbor detected Message interval: 7 Time out interval: 5

Также в режиме enable коммутаторов, использующих программное обеспечение Cisco IOS 12.2(18)SXD или более поздних версий, можно использовать скрытую команду show udld neighbor для проверки содержимого кэша UDLD (так как это делает CDP). Часто для проверки наличия нарушений, связанных с конкретными протоколами, полезным бывает сравнение кэша UDLD и кэша CDP. Если поражен также и CDP, то это обычно означает, что поражены все BPDU/PDU. Поэтому необходимо также проверять STP. Например, проверьте наличие недавних изменений корневых узлов или изменений положения корневых/назначенных портов.

С помощью переменных Cisco UDLD SNMP MIB можно контролировать состояние UDLD и корректность конфигурации.

Многоуровневая коммутация

Обзор

В системном программном обеспечении Cisco IOS многоуровневая коммутация (MLS) поддерживается сериями Catalyst 6500/6000, причем поддерживается только внутренняя коммутация. Это означает, что маршрутизатор должен быть установлен внутри коммутатора. Новейшие модули Catalyst 6500/6000 Supervisor Engines поддерживают MLS CEF, в которой таблица маршрутизации загружена в каждую плату. Это требует дополнительного оборудования, включая наличие платы распределенной переадресации (DFC). DFC не поддерживается программным обеспечением CatOS, несмотря на наличие предпочтений использования программного обеспечения Cisco IOS для платы маршрутизатора. DFC поддерживается только системным программным обеспечением Cisco IOS.

Кэш MLS, используемый для включения статистики NetFlow на коммутаторах Catalyst, является кэшем на основе потоков, который используется для включения коммутации уровня 3 платами Supervisor Engine I и традиционными коммутаторами Catalyst. MLS включен по умолчанию на модуле Supervisor Engine 1 (или Supervisor Engine 1A) с MSFC или MSFC2. Для стандартной функциональности MLS не требуется дополнительной настройки MLS. Можно настроить кэш MLS на работу в одном из следующих трех режимов:

- destination
- пара источник/получатель
- source-destination port

Для определения режима MLS коммутатора используется маска потока. Эти данные впоследствии используются для подключения потоков уровня 3 в коммутаторах Catalyst, снабженных Supervisor Engine IA. Модули Supervisor Engine II не используют кэш MLS для коммутации пакетов, потому что эта плата является оборудованием, подключаемым CEF – технологией, которая масштабируется намного лучше. Кэш MLS поддерживается на плате Supervisor Engine II только для включения статистического экспорта NetFlow . Поэтому в случае необходимости Supervisor Engine II может включаться для полного потока без негативных последствий для коммутатора.

!--- конфигурацию

Время устаревания MLS применимо для всех записей кэша MLS. Значение времени устаревания применяется непосредственно к устареванию режима назначения. Необходимо разделить время устаревания MLS на два для того, чтобы разделить время действия режима source-to-destination. При делении времени устаревания MLS на восемь получится время действия полного потока. Значение по умолчанию времени устаревания MLS составляет 256 секунд.

Можно настроить время устаревания в диапазоне от 32 до 4092 секунд с шагом в 8 секунд. Любое значение времени устаревания, которое не делится на восемь секунд нацело, будет округлено до ближайшего произведения 8 секунд. Например, величина 65 будет округлена до 64, а величина 127 – до 128.

Другие события могут вызвать удаление записей MLS. Это могут быть следующие события:

- Изменения маршрутизации
- Изменение состояния линии связиНапример, линия связи PFC отключена.

Для того, чтобы размер кэша MLS не превышал 32 000 записей, после выполнения команды mls aging подключите следующие параметры:

```
Normal: configures the wait before aging out and deleting shortcut entries in
the L3 table.

Fast aging: configures an efficient process to age out entries created for flows that
only switch a few packets and then are never used again. The fast aging parameter uses
the time keyword value to check if at least the threshold keyword value of packets has
been switched for each flow. If a flow has not switched the threshold number of packets
during the time interval, then the entry in the L3 table is aged out.

Long: configures entries for deletion that have been up for the specified value even if
the L3 entry is in use. Long aging is used to prevent counter wraparound, which could
cause inaccurate statistics.
```

!--- конфигурацию

Типичная удаленная запись кэша – это запись потока с или на сервер доменных имен (DNS) или сервер TFTP, которые после создания этой записи возможно никогда не будут больше использованы. Обнаружение и устранение таких записей сохраняет пространство в кэше MLS для трафика других данных.

Для включения времени быстрого устаревания необходимо установить начальное значение равное 128 секундам. Если размер кэша MLS продолжает расти после 32 000 записей, необходимо уменьшать это значение до тех пор, пока размер кэша не будет оставаться в пределах 32 000. Если размер кэша продолжает увеличиваться после 32 000 записей, нужно уменьшить обычное время устаревания MLS.

Рекомендации Cisco по настройке MLS

Если не требуется экспорт NetFlow, MLS можно оставить равной значению по умолчанию и только destination. Если необходим NetFlow, MLS должен быть включен только в режиме полного потока на системах Supervisor Engine II.

Для подключения потока назначения MLS выполните следующую команду:

```
Switch(config)#mls flow ip destination
```

Кадры большого размера

Максимальный размер передаваемого блока данных

Максимальный размер передаваемого блока данных (MTU) – это самая большая дейтаграмма или размер пакета в байтах, которые может получить или отправить интерфейс без фрагментации пакета.

Согласно стандарту IEEE 802.3 максимальный размер фрейма Ethernet составляет:

- **1518 байт для обычных кадров (1500 байт плюс 18 дополнительных байтов заголовка**

Ethernet и концевика CRC)
- 1522 байт для инкапсулированных кадров 802.1Q (1518 плюс 4 байта маркировки)

Кадры Baby giant: Функциональная возможность Baby Giants позволяет коммутатору пропустить/переслать пакеты немного большие, чем IEEE Ethernet MTU, не заявляя, что у кадров превышены размеры, и не отклоняя их.

Jumbo-кадр: Определение размера фрейма зависит от производителя, поскольку размер фрейма не является частью стандарта IEEE. Фреймы Jumbo – это фреймы, размер которых превышает размер стандартного фрейма Ethernet (равный 1518 байт, включая заголовок уровня 2 и последовательность проверки фреймов [FCS]).

После включения поддержки кадров большого размера на отдельном порту размер MTU по умолчанию составляет 9216 байт.

Когда следует ожидать пакетов, больших, чем 1518 байт

Для передачи трафика по коммутируемым сетям следует обращать внимание на то, чтобы MTU передаваемого трафика не превышал поддерживаемый на платформах коммутаторов. Есть много причин, по которым размер MTU определенных фреймов может быть обрезан:

- **Требования определенных производителей оборудования – приложения и некоторые платы NIC могут задавать размер MTU, превышающий стандартные 1500 байт.** Это изменение произошло потому, что ряд исследований доказал, что увеличение размера фрейма Ethernet может привести к увеличению средней пропускной способности.
- **Создание магистралей (транкинг) для увеличения стандартного размера кадра Ethernet с целью передачи данных об идентификаторе VLAN между коммутаторами или другими сетевыми устройствами используется функция создания магистралей.** Сегодня двумя самыми распространенными формами транкинга являются:Протокол инкапсуляции ISL, разработанный и принадлежащий Cisco802.1Q
- **Многопротокольная коммутация на основе признаков (MPLS) – после включения MPLS на интерфейсе она может увеличить размер фрейма пакета в зависимости от количества меток в стеке меток для меченного MPLS пакета.** Общий размер меток составляет 4 байта. Общий размер стека меток составляет:`n * 4 bytes`Если сформирован стек меток, кадры могут превышать MTU.
- **Туннелирование 802.1Q – в туннельных пакетах 802.1Q содержится две метки 802.1Q, только одну из которых видит оборудование в каждый момент времени.** В результате внутренняя метка добавляет к значению MTU 4 байта (размер полезной информации).
- **Универсальный транспортный интерфейс (UTI) / протокол туннелирования уровня 2 версии 3 (TPv3 уровня 2) – UTI / TPv3 уровня 2 инкапсулирует данные уровня 2, которые необходимо пересылать по IP сети.** UTI / TPv3 уровня 2 может увеличить исходный размер фрейма на величину до 50 байт. Новый кадр включает новый заголовок IP (20-байт), заголовок TPv3 уровня 2 (12-байт) и новый заголовок уровня 2. Полезная информация TPv3 уровня 2 состоит из полного фрейма уровня 2, в состав которого входит заголовок уровня 2.

Цель

Скоростная (1 Гбит/с и 10 Гбит/с) аппаратная коммутация сделала фреймы jumbo конкретным решением проблем условно оптимальной пропускной способности. Хотя не

существует официальных стандартов размера фреймов jumbo, часто встречающейся на практике величиной является 9216 байт (9 KB).

Анализ сетевой эффективности

Можно рассчитать сетевую эффективность прохождения пакета, разделив объем его полезной нагрузки на сумму величины потерь и объема полезной нагрузки.

Даже если увеличение сетевой эффективности при использовании фреймов jumbo будет умеренным и колебаться в пределах от 94.9 процентов (1500 байт) до 99.1 процентов (9216 байт), потери обработки (использование ЦП) сетевых устройств и конечных узлов будет уменьшаться пропорционально размеру пакета. Вот почему для высокопроизводительных сетевых технологий LAN и WAN предпочитают использовать максимально большие размеры фреймов.

Увеличение производительности возможно только тогда, когда осуществляется пересылка длинных данных. Примеры приложений следующие:

- Серверное соединение с встречно-параллельным подключением (например, транзакции сетевой файловой системы [NFS])
- Серверная кластеризация
- Высокоскоростное резервное копирование данных
- Высокоскоростное соединение суперкомпьютеров
- Передача данных графических приложений

Анализ производительности сети

Пропускная способность TCP в глобальных сетях (WAN) (Интернет) была подвергнута тщательному изучению. Данное уравнение объясняет как зависит верхняя граница пропускной способности TCP от следующих факторов:

- Максимальный размер сегмента (MSS), равный разнице между длиной MTU и длиной заголовков TCP/IP
- Период кругового обращения (RTT)
- Потери пакетов

В соответствии с данной формулой максимальная достижимая пропускная способность TCP прямо пропорциональна MSS. Это означает, что при постоянных значениях RTT и потерь пакетов, при двукратном увеличении размера пакета, пропускную способность TCP можно удвоить. Аналогично, при использовании кадров большого размера вместо кадров размером 1518 байт шестикратное увеличение размера может позволить добиться шестикратного увеличения пропускной способности TCP Ethernet-подключения.

Технологическое описание

В спецификации стандарта IEEE 802.3 определен максимальный размер кадра Ethernet, который составляет 1518. Инкапсулированные 802.1Q фреймы длиной от 1519 до 1522 байт были добавлены в спецификацию 802.3 на последнем этапе подготовки в приложении IEEE Std 802.3ac-1998. **В литературе такие фреймы иногда упоминаются как baby giants.**

В общем случае пакеты классифицируются как гигантские фреймы, когда их длина для конкретного соединения Ethernet превышает определенную максимальную длину фреймов Ethernet. Гигантские пакеты также известны как кадры большого размера.

Наибольшим источником неразберихи в применении фреймов jumbo является их настройка: разные интерфейсы поддерживают разные максимальные размеры пакетов, а иногда даже ведут себя в отношении больших пакетов немного по-разному.

Catalyst серии 6500

Данная таблица является попыткой объединить размеры MTU, поддерживаемые в настоящее время разными платами платформы Catalyst 6500:

Линейная карта	Размер MTU
По умолчанию	9216 байт
WS-X6248-RJ-45, WS-X6248A-RJ-45, WS-X6248-TEL, WS-X6248A-TEL, WS-X6348-RJ-45, WS-X6348-RJ45V, WS-X6348-RJ-21 и WX-X6348-RJ21V	8092 байт (ограничен чипом PHY)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V), WS-X6148-45AF и WS-X6148-21AF	9100 байтов (в 100 Мбит/с) 9216 байтов (в 10 Мбит/с)
WS-X6516-GE-TX	8092 байта (в 100 Мбит/с) 9216 байтов (в 10 или 1000 Мбит/с)
WS-X6148(V)-GE-TX, WS-X6148-GE-45AF, WS-X6548(V)-GE-TX и WS-X6548-GE-45AF	1500 байтов
OSM ATM (OC12c)	9180 байтов
OSM CHOC3, CHOC12, CHOC48 и CT3	9216 байтов (OCx и DS3) 7673 байта (T1/E1)
Flex WAN	7673 байта (T1/DS0 CT3) 9216 байтов (OC3c POS) 7673 байта (T1)
WS-X6148-GE-TX и WS-X6548-GE-TX	Не поддерживается

Дополнительные сведения см. в разделе Настройка коммутации Ethernet, Fast Ethernet, Gigabit Ethernet и 10-гигабитного Ethernet.

Поддержка Jumbo уровня 2 и уровня 3 в программном обеспечении Cisco IOS Catalyst 6500/6000

Существует поддержка jumbo уровня 2 и уровня 3 при помощи PFC/MSFC1, PFC/MSFC2 и PFC2/MSFC2 на всех портах GE, настроенных как физические интерфейсы уровня 2 и уровня 3. Поддержка существует вне зависимости от того, принадлежат эти порты

магистрали или каналу. Эта функциональная возможность доступна в программном обеспечении Cisco IOS релиза 12.1.1E и более поздних.

- Размеры MTU всех физических портов, на которых включена поддержка jumbo, связаны. Изменение одного из них повлечет за собой изменение всех. Они всегда поддерживают тот же размер MTU фрейма jumbo, который был при включении.
- Во время настройки необходимо либо включить поддержку jumbo на всех портах одной VLAN, либо не включать ее ни на одном порту этой VLAN.
- Размер MTU коммутируемого виртуального интерфейса (SVI) (интерфейс VLAN) устанавливается отдельно от физических портов MTU. Изменение MTU физических портов не изменит размера MTU SVI. Также изменение MTU SVI не изменит MTU физических портов.
- Поддержка фреймов jumbo уровня 2 и уровня 3 на интерфейсах FE впервые появилась в программном обеспечении Cisco IOS релиза 12.1(8a) EX01. **Команда mtu 1500 отключает jumbo на FE, а команда mtu 9216 – включает.** Обратитесь к дефекту номер CSCdv90450(только для зарегистрированных клиентов).
- Фреймы jumbo уровня 3 в интерфейсах VLAN поддерживаются только:PFC/MSFC2 (программное обеспечение Cisco IOS 12.1(7a)E и более поздних версий)PFC2/MSFC2 (программное обеспечение Cisco IOS 12.1(8a)E4 и более поздних версий)
- Не рекомендуется использовать фреймы jumbo с PFC/MSFC1 для интерфейсов VLAN, так как MSFC1 может не справиться с фрагментацией.
- Для пакетов в пределах одной и той же VLAN (jumbo уровня 2) фрагментация не поддерживается.
- Пакеты, нуждающиеся в фрагментации в VLAN/подсетях (jumbo уровня 3), посылаются для фрагментации программному обеспечению.

Общие сведения о поддержке фреймов jumbo в ПО Cisco IOS Catalyst 6500/6000

Фрейм jumbo – это фрейм, размер которого превышает размер фрейма Ethernet, установленный по умолчанию. Для того чтобы включить поддержку фреймов jumbo, необходимо настроить для порта или интерфейса VLAN размер MTU больший, нежели по умолчанию, и при помощи программного обеспечения Cisco IOS релиза 12.1(13)E и более поздних настроить общий размер MTU портов LAN.

Проверка размеров трафика, проходящего через мост, и маршрутизируемого трафика в программном обеспечении Cisco IOS

Линейная карта	Вход	Выход
Порты 10-, 10/100-, 100 Мбит/с	Проверка размера MTU выполнена. Поддержка фреймов jumbo сравнивает размер входящего трафика с общим размером MTU портов LAN на входных портах Ethernet 10-, 10/100- и 100 Мбит/с и портах LAN 10-GE, для которых настроен размер MTU, отличный	Проверка размера MTU не выполнена. Порты, для которых настроен размер MTU, отличный от значения по умолчанию, передают фреймы,

	от значения по умолчанию. Порт отбрасывает трафик с превышенными размерами.	содержащие пакеты любого размера больше 64 байт. Порты LAN Ethernet 10-, 10/100- и 100 Мбит/с с нестандартным размером MTU не проверяют исходящие фреймы на предмет превышения допустимых размеров.
Порты GE	Проверка размера MTU не выполнена. Порты, для которых настроен размер MTU, отличный от значения по умолчанию, принимает фреймы, содержащие пакеты любого размера больше 64 байт, и не проверяет входящие фреймы на предмет превышения допустимых размеров.	Проверка размера MTU выполнена. Поддержка фреймов jumbo сравнивает размер исходящего трафика с общим размером MTU выходных портов LAN на выходных портах GE и портах LAN 10-GE, для которых настроен размер MTU, отличный от значения по умолчанию. Порт отбрасывает трафик с превышенными размерами.
Портв 10-GE	Проверка размера MTU выполнена. Порт отбрасывает трафик с превышенными размерами.	Проверка размера MTU выполнена. Порт отбрасывает трафик с превышенными размерами.

SVI	Проверка размера MTU не выполнена. SVI не проверяет размер фрейма на стороне входа.	Проверка размера MTU выполнена. Размер MTU проверяется на стороне выхода SVI.
	PFC	
Весь маршрутизируемый трафик	Для трафика, подлежащего маршрутизации, поддержка фреймов jumbo на PFC сравнивает размеры трафика с настроенными размерами MTU и обеспечивает коммутацию уровня 3 между интерфейсами, которые настроены таким образом, что размеры MTU достаточно велики, чтобы вмещать трафик. Между интерфейсами, для которых не настроены достаточно большие размеры MTU: • Если бит с командой «не фрагментировать» (DF) не установлен, PFC посылает трафик MSFC для фрагментации и маршрутизации программным обеспечением. • Если бит DF установлен, PFC отбрасывает трафик.	

Рекомендации Cisco

При правильном применении фреймы jumbo могут обеспечить потенциальное шестикратное увеличения пропускной способности TCP соединения Ethernet со сниженными потерями фрагментации (плюс сниженные потери ЦП на конечных устройствах).

Необходимо убедиться в том, что внутри нет устройства, неспособного работать с определнным размером MTU. Если такое устройство фрагментирует и перешлет пакеты, весь процесс сойдет на ноль. Это может привести к дополнительным потерям на этом устройстве на фрагментацию и пересборку пакетов.

В таких случаях отыскание MTU IP пути поможет отправителю найти общую минимальную длину пакета, приемлемую для трафика, передаваемого по всему пути. В качестве альтернативы можно настроить в устройствах, которые могут работать с фреймами jumbo, размер MTU, который является наименьшим из поддерживаемых в сети.

Необходимо тщательно проверить каждое устройство, чтобы убедиться в том, что оно поддерживает размер MTU. См. таблицу поддержки размеров MTU в данном разделе.

Поддержка фреймов jumbo может быть включена на следующих типах интерфейсов:

- Канальный интерфейс порта
- SVI

- Физический интерфейс (уровня 2/уровня 3)

Можно включить поддержку фреймов jumbo на портах каналах или физических интерфейсах, участвующих в портах каналах. Очень важно убедиться, что MTU на всех физических интерфейсах одинаковый. Иначе работа интерфейса может быть приостановлена. Необходимо изменить MTU интерфейса порта канала, так как это изменит MTU всех участников порта.

Примечание: Если MTU участвующего порта не может быть изменен на новое значение, потому что участвующий порт является блокирующим портом, канал порта приостановлен.

Перед тем как настроить поддержку фреймов jumbo на SVI, необходимо обязательно убедиться в том, что все физические интерфейсы VLAN настроены под фреймы jumbo. MTU пакета на стороне входа SVI не проверяется. Тем не менее, он проверяются на стороне выхода SVI. Если пакет MTU больше, чем исходящий MTU SVI, то он будет фрагментирован программным обеспечением (если не установлен бит DF), что приведет к потерям производительности. Фрагментация программным обеспечением происходит только для коммутации уровня 3. Фрагментация программным обеспечением происходит, когда пакет пересылается на порт уровня 3 или на SVI с меньшим MTU.

MTU SVI должен всегда быть меньше, чем наименьшее значение MTU среди всех портов коммутаторов в VLAN.

Серия Catalyst 4500

Фреймы jumbo поддерживаются, главным образом, на неблокирующих портах линейной платы Catalyst 4500. Неблокирующие порты GE напрямую соединены с коммутирующей матрицей Supervisor Engine и поддерживают фреймы jumbo:

- Supervisor EnginesWS-X4515, WS-X4516 – два порта GBIC восходящей линии связи на Supervisor Engine IV или VWS-X4516-10GE – две линии связи 10-GE и четыре подключаемые восходящие линии связи малого форм-фактора (SFP) 1-GEWS-X4013+ – две восходящие линии связи 1-GEWS-X4013+10GE – две линии связи 10-GE и четыре SFP восходящие линии связи 1-GEWS-X4013+TS – 20 портов 1-GE
- Линейные картыWS-X4306-GB – модуль GE 1000BASE-X (GBIC) с шестью портамиWS-X4506-GB-T – шесть портов 10/100/1000 Мбит/с и шесть портов SFPWS-X4302-GB – модуль GE 1000BASE-X (GBIC) с двумя портамиПервые два порта GBIC на 18-портовом сервере коммутирующего модуля GE (WS-X4418-GB) и GBIC порты модуля WS-X4232-GB-RJ
- Коммутаторы с фиксированной конфигурациейWS-C4948 – все 48 портов 1-GEWS-C4948-10GE – все 48 портов 1-GE и два порта 10-GE

Эти неблокирующие порты GE можно использовать для поддержки фреймов jumbo размером 9 Кбайт или подавления широковещательной рассылки (только Supervisor Engine IV). Все остальные линейные платы поддерживают фреймы baby giant. Baby giants могут использоваться для мостового соединения MPLS или транзитной пересылки Q in Q с максимальной полезной нагрузкой в 1552 байта.

Примечание: Размер фрейма увеличивается с метками ISL/802.1Q.

Baby giants и фреймы jumbo понятны для других функциональностей Cisco IOS, использующих Supervisor Engines IV и V.

Функциональные возможности обеспечения безопасности ПО Cisco IOS

Основные функции безопасности

Было время, когда безопасность кампусного построения упускалась из виду. Но в сейчас обеспечению безопасности отводится значительная часть любой корпоративной сети. Обычно у клиента уже существует политика безопасности, которая поможет определить, какие инструменты и технологии Cisco ему подходят.

Основная защита паролем

Большинство устройств программного обеспечения Cisco IOS настроены на работу с использованием двух уровней паролей. Первый уровень предназначен для Telnet доступа к устройству, также известному как vty доступ. После получения vty-доступа необходимо получить доступ к режиму активации или привилегированному режиму exec.

Режим активации коммутатора должен быть защищен

Пароль активации позволяет пользователю получить полный доступ к устройству. Пароль активации должен даваться только доверенным лицам.

```
Switch(config)#enable secret password
```

Необходимо убедиться в том, что пароль подчиняется следующим правилам:

- Пароль должен содержать от одного до 25 заглавных и строчных буквенно-цифровых символов.
- Первым символом пароля не может быть цифра.
- Можно использовать пробел как первый символ, но он будет игнорироваться. Пробелы в середине и конце пароля распознаются.
- Проверка пароля чувствительна к регистрам. Например, пароль Secret отличается от пароля secret.

Примечание: Команда enable secret использует одностороннюю криптографическую функцию хеширования алгоритма представления сообщения в краткой форме 5 (MD5). **Этот зашифрованный пароль можно увидеть при выполнении команды show running-config. Другим способом задания пароля активации является команда enable password. Но алгоритм шифрования, используемый командой enable password, слаб и может быть легко отменен для получения пароля. Поэтому не следует использовать команду enable password. Используйте разблокированную шифрованную команду для более высокой безопасности.** Дополнительные сведения см. в разделе Данные шифрования пароля Cisco IOS.

Безопасный Telnet/VTY доступ к коммутатору

По умолчанию программное обеспечение Cisco IOS поддерживает пять активных сеансов Telnet. Эти сеансы упоминаются как vty от 0 до 4. Для доступа можно подключить эти линии. Но для того чтобы сделать возможной авторизацию, необходимо также установить пароли для этих линий.

```
Switch(config)#line vty 0 4 Switch(config-line)#login Switch(config-line)#password password
```

Команда login настраивает эти линии для Telnet доступа. Команда password задает пароль. Необходимо убедиться в том, что пароль подчиняется следующим правилам:

- Первый символ не должен быть цифрой.
- Строка может содержать только буквенно-цифровые символы, до 80 символов. Эти символы могут включать пробелы.
- Нельзя использовать формат пароля число-пробел-символ. Пробел после числа приводит к возникновению проблем. Например, hello 21 – допустимый пароль, а 21 hello – недопустимый.
- Проверка пароля чувствительна к регистрам. Например, пароль Secret отличается от пароля secret.

Примечание: С этой конфигурацией с командной строки VTY коммутатор хранит пароль в открытом тексте. **Если кто-либо выполнит команду show running-config, этот пароль станет видимым. Чтобы этого избежать, необходимо использовать команду service password-encryption.** Это команда свободно шифрует пароль. **Эта команда шифрует только пароль vty-линии и пароль активации, настроенный командой enable password. Пароль активации, настроенный командой enable secret, использует усиленное шифрование. Рекомендуемым методом является настройка при помощи команды enable secret.**

Примечание: Для имения большей гибкости в управлении системой безопасности быть уверенными, что все Cisco IOS Doftware Device внедряют модель безопасности аутентификации, авторизации и учета (AAA). В модели AAA может использоваться локальная база данных, RADIUS и TACACS+. Дополнительные сведения см. в разделе Настройка аутентификации TACACS+.

Службы безопасности AAA

Технологическое описание AAA

Контроль доступа проверяет, у кого есть доступ к коммутатору и какие службы может этот пользователь использовать. Службы безопасности сети AAA обеспечивают первичную возможность установить контроль доступа на коммутаторе.

Этот раздел подробно описывает различные аспекты AAA:

- Аутентификация – этот процесс проверяет заявленную личность конечного потребителя или устройства. Во-первых, определено несколько различных методов, которые могут использоваться для аутентификации. Эти методы определяют тип аутентификации, которая должна быть выполнена (например, TACACS+ or RADIUS). Последовательность, в которой эти методы аутентификации будут пробоваться, также определена. Эти методы затем применяются к соответствующим интерфейсам, которые активируют аутентификацию.
- Авторизация – этот процесс предоставляет права доступа пользователю, группе пользователей или процессу. AAA-процесс способен выполнять авторизацию один раз или для каждой задачи. Процесс определяет атрибуты (на AAA-сервере) на выполнение которых у пользователя есть доступ. Как только пользователь попытается запустить какую-либо службу, коммутатор запросит у AAA-сервера разрешение авторизовать данного пользователя. Если AAA-сервер одобрит, пользователь будет авторизован. Если AAA-сервер не одобрит – пользователь не получит разрешения на запуск этой

службы. Процесс можно использовать для того, чтобы задать, что некоторые пользователи могут выполнять только некоторые команды.
- Учет – этот процесс позволяет отслеживать службы, к которым пользователи получают доступ, а также потребляемый пользователями объем сетевых ресурсов. Когда учет включен, коммутатор отчитывается о деятельности пользователя AAA-серверу в форме учетных записей. Примеры деятельности пользователя, которая подлежит отчетности, включают время сеанса, время начала и остановки. Затем можно осуществить анализ этой деятельности для управленческих или бухгалтерских целей.

Хотя AAA является первичным и рекомендованным методом для контроля доступа, программное обеспечение Cisco IOS обеспечивает дополнительные функциональные возможности для простого контроля доступа, который выходит за рамки AAA. Это следующие дополнительные функциональные возможности:

- Аутентификация имени локального пользователя
- Аутентификация пароля линии
- Включение аутентификации пароля

Однако эти функции не обеспечивают той же степени контроля доступа, который возможен при использовании AAA.

Для того, чтобы лучше понять AAA, обратитесь к следующим документам:

- Аутентификация, авторизация и учет (AAA)
- Настройка основных средств аутентификации, авторизации и учета на сервере доступа
- Сравнение TACACS+ и RADIUS

Эти документы касаются не только коммутаторов. Но концепция AAA, описанная в этих документах, применима к коммутаторам.

TACACS +

Цель

По умолчанию пароли непривилегированного и привилегированного режима глобальны. Эти пароли применимы для каждого пользователя, который обращается к коммутатору или маршрутизатору с порта консоли или при помощи сеанса Telnet через сеть. Реализация этих паролей в сетевых устройствах является трудоемкой и нецентрализованной. Также могут возникнуть трудности с ограничением доступа при помощи списков контроля доступа (ACL), которые при ошибках в настройках могут стать бесполезными. Для того чтобы избежать таких проблем, необходимо применить централизованный подход при настройке на центральном сервере имен пользователей, паролей и управления доступом. Этим сервером может быть сервер управления доступом Cisco Secure (ACS) или сервер производства третьей стороны. Устройства настроены таким образом, чтобы использовать эти централизованные базы данных для функций AAA. В данном случае устройства – это коммутаторы под управлением программного обеспечения Cisco IOS. Протоколы, используемые между устройствами и центральным сервером, могут быть следующими:

- TACACS +
- RADIUS
- Kerberos

TACACS+ является распространенным решением в сетях Cisco и в данном разделе упор

делается на него. TACACS+ обеспечивает следующие функциональные возможности:

- Аутентификация – процесс, который идентифицирует и проверяет пользователей. Для того чтобы аутентифицировать пользователя, могут быть использованы различные методы. Но наиболее распространенный метод включает сочетание имени пользователя и пароля.
- Авторизация – когда пользователь пытается выполнить команду, коммутатор может осуществить проверку при помощи сервера TACACS+, чтобы определить есть ли у пользователя разрешения на использование определенной команды.
- Учет – этот процесс записывает, что пользователь делает или сделал на устройстве.

Для ознакомления со сравнением TACACS+ и RADIUS см. документ Сравнение TACACS+ и RADIUS.

Технологическое описание

Протокол TACACS+ пересылает имена пользователей и пароли на централизованный сервер. Информация пересылается по сети зашифрованной при помощи одностороннего перераспределения MD5. См. RFC 1321 для получения дополнительной информации. TACACS+ использует в качестве транспортного протокола TCP порт 49, который по сравнению с UDP предлагает следующие преимущества:

Примечание: RADIUS использует UDP.

- Этот транспортный протокол ориентирован на соединение
- Отдельное подтверждение, что запрос был получен (подтверждение TCP [ACK]), вне зависимости от того, как был загружен внутренний механизм аутентификации
- Немедленная индикация сбоя сервера (пакеты reset [RST])

Во время сеанса при необходимости дополнительной проверки авторизации коммутатор осуществляет такую проверку при помощи TACACS+, для того чтобы определить есть ли у пользователя разрешения на использование определенной команды. Это обеспечивает лучший контроль над командами, которые могут быть выполнены на коммутаторе, и обеспечивает разрыв связи с механизмом аутентификации. При помощи учета выполнения команд можно выполнять аудит команд, выполненных определенным пользователем при его подключении к определенному сетевому устройству.

Следующая схема показывает процесс аутентификации:

Когда пользователь проходит аутентификацию при простом ASCII входе на сетевое устройство при помощи TACACS+, обычно происходит следующий процесс:

- Когда соединение установлено, коммутатор связывается с демоном TACACS+ для получения приглашения на ввод имени пользователя. Коммутатор отображает приглашение на ввод имени пользователя. Пользователь вводит свое учетное имя пользователя, и коммутатор обращается к демону TACACS+ для получения приглашения на ввод пароля. Коммутатор отображает приглашение на ввод пароля для пользователя, пользователь вводит пароль, который также отправляется демону TACACS+.
- Через некоторое время сетевое устройство получает один из следующих ответов от демона TACACS+:ACCEPT – , . Если сетевое устройство настроено так, что требуется авторизация, авторизация начнется в это время.REJECT . Пользователю

может быть отказано в доступе или предложено повторить последовательность входа. Результат зависит от демона TACACS+.ERROR . Ошибка может быть связана с демоном или сетевым подключением между демоном и коммутатором. ERROR, .CONTINUE .

- Прежде чем перейти к авторизации TACACS+, пользователи сначала должны успешно пройти аутентификацию TACACS+.
- Если требуется авторизация TACACS+, демону TACACS+ отправляется запрос. TACACS+ ACCEPT REJECT. ACCEPT, , EXEC NETWORK . Эти атрибуты определяют команды, доступ к которым разрешен пользователю.

Основные этапы настройки AAA

Настройка AAA относительно проста при условии общего понимания процесса. Для того чтобы настроить безопасность на маршрутизаторе Cisco или сервере доступа с использованием AAA, необходимо выполнить следующие шаги:

1. **Для включения AAA выполните команду глобальной конфигурации aaa new-model.**`Switch(config)#aaa new-model` **Совет:** Сохраните свою конфигурацию перед настройкой команд AAA. Повторное сохранение должно произойти только после того, как настройка AAA будет выполнена полностью и вы убедитесь в том, что новые настройки работают корректно. Затем необходимо перезапустить коммутатор для того, чтобы провести восстановление из непредусмотренных блокировок (до сохранения конфигурации), если это необходимо.
2. При использовании отдельного сервера безопасности необходимо настроить параметры протокола безопасности на RADIUS, TACACS+ или Kerberos.
3. **Используйте команду aaa authentication для того, чтобы определить списки методов аутентификации.**
4. **Используйте команду login authentication для того, чтобы применить списки методов к определенному интерфейсу или линии.**
5. **Выполните дополнительную команду aaa authorization для того, чтобы настроить авторизацию.**
6. **Выполните дополнительную команду aaa accounting для того, чтобы настроить учет.**
7. Настройте внешний сервер AAA для обработки запросов аутентификации и авторизации от коммутатора.**Примечание:** См. вашу документацию AAA-сервера для получения дополнительной информации.

Настройка аутентификации TACACS+

Для того чтобы настроить аутентификацию TACACS+, выполните следующие действия:

1. **Выполните команду aaa new-model в режиме глобальной конфигурации для включения на коммутаторе AAA.**
2. Определите сервер TACACS+ и связанный с ним ключ.Этот ключ используется для шифрования трафика между сервером TACACS+ и коммутатором. **В команде tacacs-server host 1.1.1.1 key mysecretkey сервер TACACS+ находится по IP адресу 1.1.1.1, а ключ шифрования – mysecretkey.** Чтобы убедится в том, что коммутатор может достичь сервера TACACS+, инициируйте утилиту протокола управляющих сообщений Internet (ICMP) с коммутатора.

3. Составьте список методов.Список методов определяет последовательность механизмов аутентификации, которые будут применяться для различных служб. Различными службами могут быть, например:EnableLogin (для доступа vty/Telnet)**Примечание:** Посмотрите раздел Базовых функций безопасности этого документа для получения информации о доступе vty/Telnet.Консоль**Этот пример рассматривает только login.** Необходимо применить список методов к интерфейсу/линии:`Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line Switch(config)#line vty 0 4 Switch(config-line)#login authentication METHOD-LIST-LOGIN Switch(config-line)#password hard_to_guess` **При данной конфигурации команда aaa authentication login использует вымышленное имя списка METHOD-LIST-LOGIN и метод tacacs+ перед использованием линии метода.** Пользователи проходят аутентификацию на сервере Radius в качестве первого метода. Если сервер TACACS+ не отвечает или присылает сообщение ERROR, пароль, настроенный в этой линии, используется для второго метода. Но если сервер TACACS+ отказывает пользователю в доступе и присылает сообщение REJECT, AAA рассматривает транзакцию как успешную и не использует второй метод.**Примечание:** Конфигурация не завершена, пока вы не применяете список (METHOD-LIST-LOGIN) к линии VTY. **Выполните команду login authentication METHOD-LIST-LOGIN в режиме настройки линии, как показано в примере.Примечание:** Пример создает черный ход для того, когда TACACS + сервер недоступен. Администраторы безопасности могут принять или, возможно, не принять наличие в сети такой лазейки. Необходимо убедиться в том, что решение о необходимости оставить лазейку не противоречит политике безопасности компании.

Настройка аутентификации RADIUS

Настройка для RADIUS почти идентична настройке для TACACS+. Нужно просто заменить в настройках слово TACACS на RADIUS. Ниже приведен пример настройки RADIUS для доступа на порт COM:

```
Switch(config)#aaa new-model Switch(config)#radius-server host 1.1.1.1 key mysecretkey
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group radius line Switch(config)#line
con 0 Switch(config-line)#login authentication METHOD-LIST-LOGIN Switch(config-line)#password
hard_to_guess
```

Баннер регистрации

Создайте для устройств соответствующие сообщения, перечисляющие действия, предпринимаемые в случае несанкционированного доступа. Не разглашайте имя сайта или информацию о сети неавторизованным пользователям. Эти сообщения обеспечивают право обращения в суд при компрометации устройства и задержании нарушителя. Для создания таких сообщений используйте следующую команду:

```
Switch(config)#banner motd ^C *** Unauthorized Access Prohibited *** ^C
```

Защита на физическом уровне

Необходимо убедиться в том, что для физического доступа к устройствам необходима должная авторизация. Оборудование должно храниться в контролируемом (запертом) пространстве. Для того чтобы быть уверенными в том, что сеть будет оставаться в рабочем состоянии и не будет подвергаться злонамеренному вмешательству окружающих факторов, у всего оборудования должны быть:

- Соответствующий источник беспербойного питания (UPS) с подключением резервных источников, где это возможно
- Температурный контроль (кондиционирование воздуха)

Помните, что если какое-либо лицо со злым умыслом осуществит физический несанкционированный доступ, последующее нанесение ущерба путем восстановления паролей или иными методами более чем вероятно.

Настройка управления

Сетевые графики

Цель

Понятные сетевые графики имеют большое значение для обеспечения работы сети. Они приобретают особую важность при поиске и устранении неполадок и являются единственным и самым важным средством передачи информации поставщикам и партнерам в период выхода из строя. Не следует недооценивать подготовку, готовность и доступность, которые обеспечивают схемы сетей.

Рекомендация

Необходимыми являются следующие три типа схем:

- **Общая схема – даже для самых больших сетей большую роль играет схема, на которой отображены физические или логические сквозные соединения.** Часто предприятия, на которых реализована иерархическая структура, описывают каждый уровень отдельно. При планировании и устранении неисправностей значение имеет хорошее представление о соединении доменов между собой.
- **Схема физических соединений – на этой схеме отображаются все коммутаторы, маршрутизаторы и разводка кабелей.** Необходимо убедиться в том, что на схему нанесен каждый из следующих аспектов:Кол-во магистралейСсылкиСкоростиГруппы каналовНомера портовСлотыТипы шассиПрограммное обеспечениеVTP-доменыКорневой мостПриоритет резервного корневого мостаMAC-адресБлокированные порты каждой VLANДля большей ясности нужно нанести внутренние устройства, такие как маршрутизатор Catalyst 6500/6000 MSFC как маршрутизатор в каскаде, подключенный при помощи магистрали.
- **Логическая схема – эта схема содержит только функциональные возможности уровня 3, то есть изображает маршрутизаторы в виде объектов, а VLAN в виде сегментов Ethernet.** Необходимо убедиться в том, что на схему нанесены следующие аспекты:IP-адресаПодсетиВторичная адресацияHSRP в активном и дежурном режимахУровни основного распределения доступаСведения о маршрутизации

Интерфейс управления коммутаторами и собственная VLAN

Цель

В данном разделе описана значимость и потенциальные проблемы использования VLAN 1,

настроенной по умолчанию. Также раздел содержит потенциальные проблемы направления управляющего трафика к коммутатору по той же VLAN, по которой передается пользовательский трафик, в коммутаторах серий 6500/6000.

Процессоры Supervisor Engines и MSFCs для серий Catalyst 6500/6000 используют VLAN 1 для большого количества протоколов контроля и управления. Примеры таких устройств:

- Протоколы контроля коммутатора:STP BPDUsПротокол VTPDTPCDP
- Протоколы управления:SNMPTelnetSecure Shell Protocol (SSH)Системный журнал

Когда VLAN используется подобным образом, она называется собственной VLAN. Конфигурация коммутатора по умолчанию устанавливает VLAN 1 как собственную VLAN, заданную по умолчанию, на магистральных портах Catalyst. Можно оставить VLAN 1 как собственную VLAN. Но необходимо помнить, что каждый коммутатор в сети, работающий на базе системного программного обеспечения Cisco IOS, по умолчанию устанавливает все интерфейсы, настроенные как порты коммутатора уровня 2, портами доступа в VLAN 1. Вероятнее всего, какой-то коммутатор в сети использует VLAN 1 как VLAN для трафика пользователя.

Главным препятствием использования VLAN 1 является то, что, в общем случае, NMP Supervisor Engine не должен прерываться интенсивным многоадресным и широковещательным трафиком, который генерируют конечные станции. Многоадресные приложения в частности склонны посылать большое количество данных между серверами и клиентами. Supervisor Engine не нужно видеть эти данные. Если ресурсы или буферы Supervisor Engine полностью заняты, так как Supervisor Engine прослушивает ненужный ему трафик, Supervisor Engine может остановить работу до получения пактов управления, что может вызвать возникновение петли связующего дерева или сбой EtherChannel (в худшем случае).

Команды show interfaces interface_type slot/port counters и show ip traffic могут предоставить следующую информацию:

- Пропорция отношения широковещательного к однонаправленному трафику
- Пропорция отношения IP-трафика к не IP-трафику (это обычно нельзя увидеть во VLAN управления)

VLAN 1 помечает и обрабатывает основную часть трафика уровня управления. По умолчанию VLAN 1 включена во всех магистральных каналах. В более крупных кампусных сетях необходима осторожность с диаметром домена STP VLAN 1. Нестабильность в одной части сети может нанести вред VLAN 1 и повлиять на стабильность уровня управления и стабильность STP во всех остальных VLAN. Можно ограничить передачу данных пользователя по VLAN 1 и работу STP на интерфейсе. Для этого нужно просто не настраивать VLAN на магистральном интерфейсе.

Эта настройка не останавливает передачу контрольных пакетов от коммутатора к коммутатору по VLAN 1, как видно в сетевом анализаторе. Но данные не пересылаются и STP в данной линии связи не работает. Поэтому этот прием можно использовать, чтобы разбить VLAN 1 на меньшие сбойные домены.

Примечание: Вы не можете clear VLAN 1 от транков до Catalyst 2900XL/3500XLs.

Даже когда в общей сети предприняты меры по ограничению пользовательских VLAN относительно небольшими коммутируемыми доменами и соответственно узкими границами сбоев/уровня 3, некоторые клиенты пытаются подойти к управляющей VLAN по-другому.

Эти клиенты пытаются покрыть всю сеть одной управляющей подсетью. Нет ни технических оснований для того, чтобы центральное приложение NMS было смежным на уровне 2 с устройствами, которыми оно управляет, ни каких-либо обоснованных возражений в отношении безопасности. Рекомендуется ограничивать диаметр управляющих VLAN теми же маршрутизируемыми доменами, в которых находятся пользовательские VLAN. Для увеличения безопасности управления сетью рекомендуется использовать управление через выделенное подключение и/или поддержку SSH.

Дополнительные варианты

В связи с рекомендациями Cisco по некоторыми топологиями возникают определенные рассуждения по их строению. Например, в рекомендуемой и общераспространенной многоуровневой конфигурации Cisco стремятся не использовать активное связующее дерево. В этом случае структура призывает ограничить каждую подсеть IP/VLAN одним коммутатором уровня доступа (или кластером коммутаторов). При таком строении до уровня доступа не могут быть настроены магистрали.

Нужно ли создать отдельную VLAN управления и включить транкинг для проведения ее между уровнем 2 доступа и уровнем 3 распределения? Простого ответа на этот вопрос не существует. Рассмотрим следующие два варианта пересмотра строения с инженером Cisco:

- **Вариант 1 – соединить магистралью две или три уникальных VLAN уровня распределения с каждым коммутатором уровня доступа.** Такая конфигурация позволяет использовать VLAN для данных, голосовую VLAN и управляющую VLAN и при этом пользоваться преимуществами неактивного STP. Для того, чтобы удалить VLAN 1 из магистралей, необходим еще один шаг настройки. В данном решении есть также вопросы строения, которые следует рассмотреть для того, чтобы во время восстановления после сбоя избежать исчезновения маршрутизируемого трафика. Для магистралей (в будущем) следует использовать STP PortFast или синхронизацию VLAN autostate с пересылкой STP.
- **Вариант 2 – приемлем вариант одной VLAN для данных и управления.** Если необходимо держать интерфейс sc0 отдельно от данных пользователя, новейшее коммутационное оборудование позволяет этому более не представлять собой проблему, как это было ранее. Новейшее оборудование обеспечивает:Более мощный ЦП и регуляторы скорости уровня управленияСтроение с относительно небольшими широковещательными доменами, как рекомендуется для многоуровневой структурыДля принятия окончательного решения необходимо исследование широковещательного трафика для этой VLAN и обсуждение возможностей коммутирующего оборудования с инженером по обслуживанию оборудования Cisco. Если управляющая VLAN содержит всех пользователей в этом коммутаторе уровня доступа, необходимо использовать фильтры IP на входе для защиты коммутатора от пользователей, как это описано в разделе Функциональные возможности обеспечения безопасности ПО Cisco IOS.

Рекомендации по управляющему интерфейсу Cisco и собственной VLAN

Управляющий интерфейс

Системное программное обеспечение Cisco IOS дает возможность настраивать интерфейсы как интерфейсы уровня 3 или порты коммутатора уровня 2 в VLAN. **При использовании команды switchport в программном обеспечении Cisco IOS все порты**

коммутатора по умолчанию являются портами доступа в VLAN 1. Поэтому, если только вы не настроите иначе, во VLAN 1 могут также по умолчанию существовать данные пользователя.

Необходимо сделать управляющей VLAN, отличную от VLAN 1, и держать данные пользователя вне управляющей VLAN. Вместо этого необходимо настроить управляющим интерфейсом на каждом коммутаторе интерфейс loopback0.

Примечание: При использовании Протокола OSPF это также становится ID маршрутизатора OSPF.

Нужно убедиться в том, что интерфейс loopback имеет 32-битовую маску подсети, и настроить интерфейс loopback как интерфейс уровня 3 на этом коммутаторе. Ниже представлен пример:

```
Switch(config)#interface loopback 0 Switch(config-if)#ip address 10.x.x.x 255.255.255.255
Switch(config-if)#end Switch#
```

Native VLAN

Необходимо настроить собственную VLAN как явно фиктивную VLAN, которая никогда не включается на маршрутизаторе. В прошлом Cisco рекомендовал VLAN 999, но выбор этот был абсолютно случайным.

Для того чтобы установить на определенном порту VLAN как собственную (по умолчанию) для транкинга 802.1Q, выполните следующий интерфейсные команды:

```
Switch(config)#interface type slot/port Switch(config-if)#switchport trunk native vlan 999
```

Дополнительные рекомендации см. в разделе Динамический транкинговый протокол данного документа.

Внеполосное управление

Цель

Управление сетью можно сделать гораздо более доступным, сконструировав отдельную управляющую инфраструктуру вокруг рабочей сети. Такая настройка позволяет устройствам быть доступными отдаленно, несмотря на то, что происходит с трафиком или уровнем управления. Обычно используются два подхода:

- Управление через выделенное подключение при помощи выделенной LAN
- Управление через выделенное подключение при помощи терминальных серверов

Технологическое описание

Каждый маршрутизатор и коммутатор в сети может быть снабжен выделенным интерфейсом управления Ethernet в управляющей VLAN. Один порт Ethernet на каждом из устройств настроен в управляющей VLAN и подключен вне основной сети к отдельной коммутируемой управляющей сети.

Примечание: Коммутаторы Catalyst 4500/4000 имеют специальный интерфейс me1 на Supervisor Engine, который должен использоваться для управления при нестандартном

подключении только и не как порт коммутатора.

Кроме того, к серверу терминала можно подключиться, настроив маршрутизаторы Cisco 2600 или 3600 с кабелями последовательной связи RJ-45 для доступа к порту консоли каждого маршрутизатора и коммутатора в схеме. Использование сервера терминала также позволяет избежать настройки резервных сценариев, таких как модемы на вспомогательных портах для каждого устройства. Можно настроить модем на вспомогательном порту терминального сервера. Такая настройка обеспечит возможность соединения с другими устройствами при сбое в работе сети. Дополнительные сведения см. в документе Подключение модема к консольному порту коммутаторов Catalyst.

Рекомендация

При такой схеме кроме большого количества способов доступа к каждому коммутатору и маршрутизатору по полосе пропускания, возможны еще два способа доступа через выделенные подключения. Это обеспечивает крайне высокую доступность управления сетью. Преимущества следующие:

- Такая схема разделяет управляющий трафик и данные пользователя.
- Управляющий IP адрес для обеспечения безопасности находится в отдельных подсети, VLAN и коммутаторе.
- Существует высокая степень страховки доставки управляющих данных во время сбоев сети.
- В управляющей VLAN нет активного связующего дерева. Резервирование здесь не является критическим условием.

На данной схеме изображено управление через выделенное подключение:

Регистрация системы

Цель

Сообщения системного журнала являются специфическими для Cisco и могут предоставить более информативные и точные данные, чем стандартизованный SNMP. Например, управляющие платформы, такие как Cisco Resource Manager Essentials (RMEs) и Network Analysis Toolkit (NATkit), эффективно используют информацию системного журнала, для сбора сведений об изменении оборудования и настроек.

Рекомендации Cisco по настройке системного журнала

Рекомендации Cisco по настройке системного журнала. Системный журнал UNIX может захватывать и анализировать информацию/события на маршрутизаторе такие как:

- Состояние интерфейса
- Сигналы тревоги системы безопасности
- Условия среды
- Занятость ЦП
- Другие события

Программное обеспечение Cisco IOS может осуществлять протоколирование на сервере UNIX syslog. Формат Cisco UNIX syslog совместим с 4.3 Berkeley Standard Distribution (BSD)

UNIX. Используйте следующие настройки журнала для программного обеспечения Cisco IOS:

- **no logging console – по умолчанию все системные сообщения посылаются на системную консоль.** В программном обеспечении Cisco IOS протоколирование сообщений консоли является высокоприоритетной задачей. Эта функция первоначально была разработана для того, чтобы сообщения об ошибках отправлялись оператору системы до того, как произойдет сбой системы. Необходимо отключить протоколирование сообщений коносоли на всех устройствах для того, чтобы избежать ситуации, в которой маршрутизатор/коммутатор может зависнуть, пока устройство ожидает ответа с терминала. Но сообщения консоли могут быть полезными во время локализации неисправностей. В таких случаях протоколирование сообщений с коносоли можно включить. **Выполните команду logging console level для того, чтобы получить желаемый уровень протоколирования сообщений.** Уровни протоколирования варьируются от 0 до 7.
- **no logging monitor – эта команда отключает протоколирование для линий терминала. Может потребоваться экран протоколирования (при помощи команды logging monitor debugging или другой командной опции).** В этом случае необходимо включить экран протоколирования с определенным уровнем протоколирования, что является необходимым условием для иго деятельности. **См. пункт no logging console в данном списке для получения дополнительной информации об уровнях протоколирования.**
- **logging buffered 16384 – команда logging buffered должна быть добавлена в журнал системных сообщений во внутреннем буфере протоколирования.** Буфер протоколирования является кольцевым. Как только буфер протоколирования будет заполнен, новые записи начнут записываться поверх старых. Размер буфера протоколирования определен в байтах и может настраиваться пользователем. Размер системного буфера зависит от платформы. 16384 – это хорошее значение по умолчанию, обеспечивающее достаточное протоколирование в большинстве случаев.
- **logging trap notifications – эта команда задает отправку сообщений об уровне уведомления (5) на определенный сервер системного журнала.** Уровень протоколирования для всех устройств (консоль, монитор, буфер и ловушек) по умолчанию является настраиваемым (уровень 7). Если оставить уровень протоколирования ловушки в значении 7, будет возникать множество посторонних сообщений, имеющих слабое или не имеющих вовсе отношения к работоспособности сети. Уровень протоколирования ловушек по умолчанию лучше установить в значение 5.
- **logging facility local7 – эта команда устанавливает средство/уровень протоколирования для системного протоколирования UNIX.** Сервер системного журнала, получающий эти сообщения, необходимо настроить на те же средство/уровень.
- **logging host – эта команда задает IP-адрес сервера системного журнала UNIX.**
- **logging source-interface loopback 0 – эта команда задает IP SA для сообщений системного журнала по умолчанию.** Задайте аппаратно SA протоколирования для того, чтобы упростить идентификацию узла, отправившего сообщение.
- **service timestamps debug datetime localtime show-timezone msec – по умолчанию сообщения системного журнала не имеют штампа времени.** Можно использовать эту команду для активации установки штампа времени на сообщениях системного журнала и системных сообщениях отладки. Установка штампа времени обеспечивает определение времени протоколируемых событий и улучшает интерактивную отладку.

Эта информация особенно полезна, когда клиенты отправляют выходные данные отладки персоналу технической поддержки для оказания помощи. Для того, чтобы активировать установку штампов времени на системных сообщениях отладки, используйте эту команду в режиме глобальной настройки. Эта команда работает только когда отладка включена.

Примечание: Кроме того, enable logging для статуса соединения и статуса связки (bundle) на всех Гигабитных интерфейсах инфраструктуры.

Программное обеспечение Cisco IOS обеспечивает единственный механизм устанавливать средство и уровень протоколирования для всех системных сообщений, удаленных от сервера системного журнала. Установите уровень протоколирования ловушки в значение notification (уровень 5). Установив уровень протоколирования ловушки в значение notification, можно минимизировать количество информационных сообщений, пересылаемых на сервер системного журнала. Такие настройки могут значительно уменьшить количество трафика системного журнала в сети и нагрузку на ресурсы сервера системного журнала.

Добавьте следующие команды к каждому маршрутизатору и коммутатору, использующему программное обеспечение Cisco IOS, для того, чтобы включить сообщений системного журнала:

- Глобальные команды настройки системного журнала:
  `no logging console no logging monitor logging buffered 16384 logging trap notifications logging facility local7 logging host-ip logging source-interface loopback 0 service timestamps debug datetime localtime show-timezone msec service timestamps log datetime localtime show-timezone msec`
- Интерфейсные команды настройки системного журнала:
  `logging event link-status logging event bundle-status`

SNMP

Цель

Можно использовать SNMP для поиска статистики, счетчиков и таблиц, хранящихся в MIB сетевых устройств. NMS такой как HP OpenView может использовать эту информацию для:

- Генерирования предупреждений в режиме реального времени
- Оценки доступности
- Создания информации планирования производительности
- Помощи при проверках конфигурации и устранении неисправностей

Работа управляющего интерфейса SNMP

SNMP – это протокол уровня приложения, задающий формат сообщений для связи управляющих и агентов SNMP. SNMP обеспечивает стандартизованную структуру и общий язык для отслеживания и управления устройствами в сети.

Структурно SNMP состоит из следующих трех частей:

- Менеджер SNMP
- Агент SNMP
- MIB

Менеджер SNMP – это система, использующая SNMP для управления и отслеживания деятельности сетевых узлов. Наиболее распространенная управляющая система называется NMS. Термин NMS может быть применен и к специальному устройству, использующемуся для управления сетью, и к приложению, использующемуся на таком устройстве. Для использования с SNMP подходит множество приложений управления сетью. Диапазон этих приложений – от простых CLI приложений до богатых функциональными возможностями GUI, таких как линия продуктов CiscoWorks.

SNMP агент – это компонент программного обеспечения в пределах управляемого устройства, который хранит и отчитывается о данных этого устройства управляющим системам так, как это необходимо. Этот агент и MIB находятся на маршрутизирующем устройстве (маршрутизатор, сервер доступа или коммутатор). Для активации SNMP-агента на маршрутизирующем устройстве Cisco, необходимо определить взаимоотношения между менеджером и агентом.

MIB – это виртуальная область хранения информации управления сетью. MIB состоит из коллекций управляемых устройств. В пределах MIB существуют коллекции объектов, определенных в модулях MIB. Модули MIB записаны на языке модулей SNMP MIB, как STD 58, RFC 2578, RFC 2579, и RFC 2580 определяет.

Примечание: Отдельные модули MIB также упоминаются как MIB. Например, группа интерфейсов MIB (IF-MIB) – это модуль MIB в пределах MIB вашей системы.

SNMP-агент содержит переменные MIB, значения которых может запросить SNMP менеджер или которые могут быть изменены с помощью операций get или set. Менеджер может получить значение у агента или хранить значение в агенте. Агент собирает данные из MIB, который является хранилищем информации о параметрах устройства и данных сети. Агент также может отвечать на запросы менеджера на получение или установку данных.

Менеджер может отправлять запросы агенту, чтобы получить и задать значения MIB. Агент может ответить на эти запросы. Вне этого взаимодействия агент может посылать предоставляемые добровольно уведомления (trap-сообщения или информационные запросы) менеджеру для того, чтобы уведомить его о состоянии сети. NMS MIB get get next , set. Кроме того, сетевое устройство можно настроить на генерирование trap-сообщений для NMS для получения предупреждений в режиме реального времени. Для trap-сообщений используются IP UDP порты 161 и 162.

Технологическое описание уведомлений SNMP

Ключевая функциональная возможность SNMP – это способность генерировать уведомления от SNMP агента. Для того, чтобы эти уведомления были отправлены, не требуются запросы от SNMP менеджера. Предоставленные добровольно (асинхронные) уведомления могут генерироваться в виде trap-сообщений или информационных запросов. Trap-сообщения – это сообщения, предупреждающие SNMP менеджера об условиях в сети. Информационные запросы – это trap-сообщения, включающие запрос на подтверждение получения от SNMP менеджера. Уведомления могут сообщать о следующих значительных событиях:

- Неправильная аутентификация пользователя
- Перезапуски
- Закрытие соединения

- Потеря соединения с соседним маршрутизатором
- Другие события

Trap-сообщения являются менее надежными, чем информационные запросы, так как получатель не отправляет никакого подтверждения при получении trap-сообщения. Получатель не может определить, было ли получено trap-сообщение. SNMP-менеджер, получивший информационный запрос, подтверждает сообщение при помощи SNMP-ответа в виде блока данных протокола (PDU). Если менеджер не получит информационный запрос, он не пошлет ответ. Если отправитель не получит ответ, он может отправить информационный запрос еще раз. Информационные запросы достигают пункта назначения с большей вероятностью.

Но часто предпочитают все же trap-сообщения, потому что информационные сообщения потребляют больше ресурсов маршрутизатора и сети. Trap-сообщение отбрасывается сразу же после отправки. А информационный запрос может храниться в памяти до получения ответа или истечения времени ожидания запроса. Trap-сообщения передаются только один раз, в то время как передача информационных запросов может повторяться. Повторные попытки увеличивают трафик и косвенные затраты сети. Таким образом, trap-сообщения и информационные запросы представляют собой борьбу между надежностью и сохранностью ресурсов. Если SNMP-менеджер должен получать каждое уведомление, необходимо использовать информационные запросы. Но если важными являются трафик в сети или память маршрутизатора и нет необходимости получать каждое уведомление, лучше использовать trap-сообщения.

Следующие схемы изображают различия между trap-сообщениями и информационными запросами:

Данная схема показывает, как маршрутизатор агент успешно отправляет trap-сообщение SNMP менеджеру. Хотя менеджер получает trap-сообщение, он не отправляет агенту никаких подтверждений. Агент никак не может узнать, достигло ли trap-сообщения пункта назначения.

Данная схема показывает, как маршрутизатор агент успешно отправляет информационный запрос менеджеру. Когда менеджер получает информационный запрос, он отправляет агенту ответ. Таким образом агент узнает о том, что информационный запрос достиг пункта своего назначения. Примечательно, что в этом примере трафик вдвое больше. Но агент знает, что менеджер получил уведомление.

На этой схеме агент отправляет trap-сообщение менеджеру, но менеджер его не получает. Агент никак не может узнать, достигло ли trap-сообщения пункта назначения, поэтому не посылает trap-сообщение повторно. Менеджер так никогда и не получит это trap-сообщение.

На этой схеме агент отправляет информационный запрос менеджеру, но менеджер его не получает. Так как менеджер не получил информационный запрос, от него не будет никакого ответа. Через некоторое время агент снова посылает тот же информационный запрос. На этот раз менеджер получает его и отвечает. В этом примере использовано больше трафика. Но уведомление достигло SNMP менеджера.

Дополнительные сведения о MIB и RFC Cisco

MIB-модули обычно определяются RFC-документами. RFC документы утверждаются инженерной группой по развитию Internet (IETF), международным органом стандартизации. Отдельные представители или группы пишут RFC для рассмотрения Обществом Internet

(ISOC) и сообществом Internet в целом. См. интернет-Общественную домашнюю страницу для обучения о процессе стандартов и действиях IETF. См. домашнюю страницу IETF для чтения полного текста всех RFC, интернет-Проектов (ID) и STD та ссылка Документов Cisco.

Технология Cisco для SNMP использует:

- Определения MIB II переменных, которые описывает RFC 1213
- Определения trap-сообщений SNMP, которые описывает RFC 1215

Cisco предоставляет свои собственные расширения MIB вместе с каждой системой. Cisco производит MIB, которые выполняют все инструкции, предписанные соответствующим RFC, если иное не указано в документации. Файлы определений модулей MIB и список MIB, поддерживаемых каждой платформой Cisco, могут быть найдены на домашней странице Cisco MIB.

Версии SNMP

Программное обеспечение Cisco IOS поддерживает следующие версии SNMP:

- SNMPv1 — полный Интернет - стандарт, который определяет RFC 1157. RFC 1157 заменяет более ранние версии, которые были публикованы как RFC 1067 и RFC 1098. Безопасность основывается на строках сообщества.
- SNMPv2c – это управляющая структура на основе строк сообщества для SNMPv2. SNMPv2c (с представляет сообщество) является экспериментальный Протокол Интернета, который определяет RFC 1901, RFC 1905 и RFC 1906. SNMPv2c является обновлением работы протокола и типов данных, используемых в SNMPv2p (SNMPv2 Classic). SNMPv2c использует модель безопасности SNMPv1, основанную на строках сообщества.
- SNMPv3 — SNMPv3 является протоколом на основе стандартов взаимодействия, который определяют RFC 2273, RFC 2274 и RFC 2275. SNMPv3 обеспечивает безопасный доступ к устройствам всей сети при помощи сочетания аутентификации и шифрования пакетов.Функциональные возможности безопасности, предлагаемые SNMPv3, следующие:Целостность сообщений обеспечивает неизменность пакетов в пути.Аутентификация определяет происхождение сообщения из надежного источника.Шифрование шифрует содержимое пакета, предотвращая его простое прочтение посторонними лицами.

И SNMPv1, и SNMPv2c используют форму безопасности, основанную на сообществе. IP-адрес ACL и пароль определяют сообщество менеджеров, которые имеют доступ к агенту MIB.

Поддержка SNMPv2c включает механизм группового извлечения и более подробные отчеты об ошибках, направляемые на управляющие станции. Механизм группового извлечения поддерживает извлечение таблиц и больших количеств информации за минимальное число циклов приема-передачи. Поддержка улучшенной обработки ошибок SNMPv2c включает расширенные коды ошибок, определяющие различные типы условий ошибок. В SNMPv1 обо всех этих условиях сообщается одним кодом ошибки. Ошибка возвращает коды и тип ошибки.

SNMPv3 предусматривает и модели, и уровни безопасности. Модель безопасности – это стратегия аутентификации, установленная для пользователя и группы, в которой состоит этот пользователь. Уровень безопасности – это уровень безопасности, разрешенный в

пределах модели безопасности. Сочетание модели безопасности и уровня безопасности определяет, какой механизм безопасности будет использован при обработке SNMP пакета.

Общая настройка SNMP

Для того чтобы активировать управление SNMP, выполните на всех коммутаторах клиента следующие команды:

- Команда для ACL SNMP:`Switch(config)#`**`access-list 98 permit`** *`ip_address`* *`!--- This is the SNMP device ACL.`*
- Глобальные команды SNMP:
  `!--- These are sample SNMP community strings.` `Switch(config)#`**`snmp-server community RO-community ro 98 snmp-server community RW-community rw 98 snmp-server contact Glen Rahn (Home Number) snmp-server location`** *`text`*

Рекомендации по ловушкам SNMP

Протокол SNMP является основой всей системы управления сетью, он включается и используется во всех сетях.

Агент SNMP может обмениваться информацией со многими менеджерами. Поэтому можно настроить программное обеспечение на поддержку обмена информацией с одной управляющей станцией с помощью SNMPv1, а с другой управляющей станцией – с помощью SNMPv2. Большинство клиентов и NMS все еще используют SNMPv1 и SNMPv2c, потому что поддержка сетевых устройств SNMPv3 на платформах NMS слегка запаздывает.

Подключите прерывания SNMP для всех используемых функциональностей. Остальные функции можно отключить. **После активации прерывания, можно выполнить команду test snmp и установить соответствующую обработку ошибки для NMS.** Примерами такой обработки являются предупреждение на пейджер или всплывающее сообщение.

По умолчанию все прерывания отключены. Подключите все прерывания на основных коммутаторах, как показано в примере:

`Switch(config)#`**`snmp trap enable`** `Switch(config)#`**`snmp-server trap-source loopback0`**

Также подключите прерывания портов для ключевых портов, например соединений инфраструктуры маршрутизаторов, коммутаторов и основных серверов. Подключение для других портов, таких как узловые, не нужно. Выполните следующую команду для того, чтобы настроить порт и подключить уведомления включения/отключения канала:

`Switch(config-if)#`**`snmp trap link-status`**

Затем укажите устройства, получающие trap-сообщения и реагирующие на них соответствующим образом. Теперь можно настроить каждый пункт назначения trap-сообщения как получатель SNMPv1, SNMPv2 или SNMPv3. Для устройств SNMPv3 лучше настраивать отправку надежных информационных сообщений, а не trap-сообщений UDP. Вот конфигурация:

`Switch(config)#`**`snmp-server host`** *`ip_address`* **`[traps | informs] [version {1 | 2c | 3}]`** *`community-string !--- This command needs to be on one line. !--- These are sample host destinations for SNMP traps and informs.`* **`snmp-server host 172.16.1.27 version 2c public snmp-server host 172.16.1.111 version 1 public snmp-server host 172.16.1.111 informs version 3 public snmp-server host 172.16.1.33 public`**

Рекомендации по опросам SNMP

Убедитесь в том, что эти MIB являются ключевыми MIB, опрашиваемыми или отслеживаемыми в кампусных сетях:

Примечание: Эта рекомендация от консультационной группы по управлению сетями Cisco.

Протокол NTP (Network Time Protocol, протокол сетевого времени)

Цель

Протокол NTP, RFC 1305, синхронизирует хронометраж среди ряда распределенных временных серверов и клиентов. NTP позволяет сопоставлять события при создании системных журналов или возникновении других событий, происходящих в определенное время.

Технологическое описание

RFC 958 задокументировал NTP сначала. Но NTP развил через RFC 1119 (Версия 2 NTP). RFC 1305 теперь определяет NTP, который находится в его третьей версии.

NTP синхронизирует время компьютера клиента или сервера с другим сервером или рекомендованным источником времени, таким как радио, спутниковый приемник или модем. NTP обеспечивает точность времени клиента обычно в пределах миллисекунды в LAN и до нескольких десятков миллисекунд в WAN, относительно первичного синхронизированного сервера. Например, можно использовать NTP для согласования с всемирным координированным временем (UTC) через навигатор службы глобального позиционирования (GPS).

Типичные конфигурации NTP используют несколько резервных серверов и различные сетевые пути для достижения высокой точности и надежности. Некоторые конфигурации содержат криптографическую аутентификацию, чтобы предотвратить случайные или умышленные атаки на протокол.

NTP работает через UDP, который, в свою очередь, работает через IP. Все соединения NTP используют формат всемирного координированного времени (UTC), аналогичного гринвичскому времени.

В настоящий момент доступны NTP версии 3 (NTPv3) and NTP версии 4 (NTPv4). Самый последний выпуск этого программного обеспечения – это NTPv4, но официальным стандартом Internet все еще является NTPv3. К тому же, некоторые производители операционных систем изменяют использование этого протокола.

NTP Safeguards

Разработки NTP также стремятся избежать синхронизации с машиной, время на которой может быть не точным. NTP осуществляет это двумя способами:

- NTP не синхронизируется с машиной, которая сама не синхронизирована.
- NTP всегда сравнивает время, полученное от нескольких машин и не синхронизируется с машиной, на которой время значительно отличается от других, даже если у это машина с менее высоким статусом.

Ассоциации

Обмен информацией между машинами, осуществляемый NTP, который также называется сопоставлениями, обычно является настраиваемым статически. Каждой машине дается IP адрес всех машин, с которыми она должна осуществить сопоставления. Точное хронометрирование возможно при помощи обмена NTP сообщениями между парами машин и сопоставления их. В среде LAN можно настроить NTP на использование широковещательных IP сообщений. При помощи этой альтернативы можно настроить машину на отправку или получение широковещательных сообщений, но точность хронометрирования будет немного уменьшена, так как информационный поток является односторонним.

Если сеть изолирована от Интернета, разработка NTP Cisco позволяет настраивать машину таким образом, чтобы она действовала так, как будто синхронизируется с помощью NTP, когда на самом деле она использует для определения времени другие методы. Другие машины синхронизируются с этой машиной при помощи NTP.

Сопоставления NTP также могут быть:

- Одноранговое сопоставлениеЭто означает, что система может как синхронизироваться с другой системой, так и позволять другой системе синхронизироваться с собой.
- Серверное сопоставлениеЭто означает, что только эта система синхронизируется с другими системами. Другая система с этой не синхронизируется.

Если необходимо выполнить NTP-сопоставление с другой системой, используйте одну из следующих команд в режиме глобальной настройки:

Команда	Цель
ntp peer ip-address [normal-sync] [version number] [key key-id] [source interface] [prefer]	Формирует одноранговое сопоставление с другой системой
ntp server ip-address [version number] [key key-id] [source interface] [prefer]	Формирует серверное сопоставление с другой системой

Примечание: Только один конец ассоциации должен быть настроен. Другая система устанавливает режим сопоставления автоматически.

Доступ к общественным серверам времени

Подсеть NTP в настоящее время содержит более 50 общедоступных основных серверов, синхронизированных напрямую с всемирным скоординированным временем (UTC) с помощью радио, спутниковой связи или модема. Обычно клиентские рабочие станции и серверы со сравнительно небольшим числом клиентов не синхронизируются с основными серверами. Существует около 100 общедоступных вспомогательных серверов, синхронизированных с основными серверами. Эти серверы обеспечивает синхронизацию со 100 000 клиентов и серверов в Internet. Страница Public NTP Servers ведет текущие списки и часто обновляется.

Также существует также целый ряд частных основных и вспомогательных серверов, которые недоступны широким массам пользователей. См. Проект Протокола сетевого времени (Университет Делавэра) для списка общедоступных серверов NTP и информации о том, как использовать их. Нет гарантии, что эти общедоступные серверы NTP в Internet

будут доступны, или гарантии, что они будут выдавать правильное время. Поэтому рекомендуется рассмотреть другие возможности. Это может включать в себя, например, использование различных автономных устройств GPS, непосредственно подключенных к нескольким маршрутизаторам.

Другим возможным вариантом является использование различных маршрутизаторов, настроенных как Stratum 1 master. Но использование таких маршрутизаторов не рекомендуется.

Страта

NTP использует stratum для описания NTP переходов вне машины есть из надежных источников времени. Сервер времени stratum 1 имеет радио или атомные часы, подключенные напрямую. Сервер времени stratum 2 получает время от сервера времени stratum 1 и так далее. Машина, использующая NTP, автоматически выбирает в качестве источника времени машину с меньшим номером stratum, с которой, согласно настройкам, она должна обмениваться информацией при помощи NTP. Такая стратегия эффективно строит самоорганизующееся дерево абонентов NTP.

NTP избегает синхронизации с устройствами, на которых время, возможно, не является точным. *См. раздел NTP Safeguards документа Протокол сетевого времени для получения дополнительной информации.*

Одноранговое отношение серверов

- Сервер только отвечает на запросы клиентов, но не пытается получить какую-либо информацию о времени с источника времени клиента.
- Равноправный сервер отвечает на запросы клиентов и пытается использовать запросы клиентов в качестве потенциальных источников более правильного времени и для стабилизации частоты своих часов.
- Чтобы быть действительно равноправными, обе стороны подключения должны войти в равноправные отношения, в отличие от случая, когда один пользователь является равноправным, а второй является сервером. Рекомендуется выполнять обмен ключами равноправных узлов, чтобы только доверенные хосты могли взаимодействовать друг с другом на равноправной основе.
- В случае поступления запроса от клиента к серверу последний отвечает клиенту и забывает о том, что клиент когда-либо делал запрос.
- Когда клиент передает запрос равноправному узлу, сервер отвечает клиенту. Сервер сохраняет информацию о состоянии клиента, чтобы проследить, насколько успешно происходит хронометрирование и на каком stratum работает сервер.

NTP-сервер вполне способен обслуживать много тысяч клиентов одновременно. Но когда NTP сервер обслуживает более, чем несколько клиентов (до нескольких сотен), появляется недостаток памяти, сказывающийся на способности сервера хранить информацию о состоянии. Когда NTP-сервер обслуживает больше рекомендованного количества, процессом поглощаются больше ресурсов ЦП устройства и полосы пропускания.

Режимы коммуникации с NTP-сервером

Существует два отдельных режима коммуникации с сервером:

- Широковещательный режим

- Режим клиент/сервер

В широковещательном режиме клиенты слушают. В режиме клиент/сервер клиенты опрашивают сервер. Использовать широковещательную рассылку NTP из-за ее скорости можно только если в сети нет линий связи WAN. Для работы в линии связи WAN необходимо использовать режим клиент/сервер (путем последовательного опроса). Широковещательный режим разработан для LAN, в которой многим клиентам может понадобится опросить сервер. Без использования широковещательного режима такой опрос может привести к генерации большого количества пакетов в сети. Многоадресная рассылка NTP пока не доступна в NTPv3, но доступна в NTPv4.

По умолчанию программное обеспечение Cisco коммуницирует с помощью NTPv3. Но программное обеспечение обратно совместимо с более ранними версиями NTP.

Опрос

Протокол NTP разрешает клиенту посылать запрос на сервер в любое время.

```
NTP   Cisco NTP       NTP_MINPOLL (24^4= 16 ). NTP_MAXPOLL  2^14  (16 384   4 , 33 , 4 ).
```

Этот период времени – это самый длинный период времени перед тем, как NTP снова запросит ответ. `Cisco POLL.`

Счетчик опроса NTP запускается через 2^6 (64) сек или 1 мин, 4 сек. Время возводится в степень 2, так как два сервера синхронизируются друг с другом до 2^10. То есть, сообщения синхронизации будут отправляться с интервалами 64, 128, 256, 512 и 1024 секунд для каждого настроенного сервера или равноправного узла. Более длительное время между последовательными опросами применяется, когда текущие часы становятся более стабильными по причине синфазной петли. Синфазные петли накладываются на локальный часовой кристалл до 1024 секунд (17 мин).

Время варьируется между 64 и 1024 секундами как степень двойки (каждые 64, 128, 256, 512 или 1024 сек). Время определяется на основании синфазной петли, которая посылает и принимает пакеты. При наличии большого отклонения во времени опрос производится чаще. Если эталонные часы являются точными, а сетевое соединение постоянным, можно видеть, что время между опросами будет доходить до 1024 секунд.

Интервал опроса NTP изменяется, поскольку изменяется соединение между клиентом и сервером. Чем лучше соединение, тем дольше будет интервал опроса. В данном случае лучшее соединение означает, что NTP-клиент получил восемь ответов на восемь своих последних запросов. Затем интервал опроса был удвоен. Один пропущенный ответ приведет к сокращению интервала опроса вдвое. Интервал опроса может составлять от 64 секунд до максимальных 1024 секунд. В оптимальных условиях для увеличения интервала опроса с 64 секунд до 1024 секунд потребуется немногим более 2 часов.

Широковещательные сообщения

Многоадресные пакеты NTP никогда не пересылаются. **По команде ntp broadcast маршрутизатор начнет широковещательную рассылку пакетов NTP через интерфейс, в котором она настроена.**

Обычно команда ntp broadcast используется для начала широковещательной рассылки NTP в LAN с целью обслуживания клиентских конечных станций и серверов.

Синхронизация времени

Синхронизация клиента и сервера состоит из обмена различными пакетами. Каждый обмен представляет собой пару запрос/ответ. Когда клиент посылает запрос, он сохраняет свое локальное время в отправленном пакете. Когда сервер получает пакет, он заносит в пакет свою собственную оценку времени и пакет возвращается. Когда ответ будет получен, получатель еще раз запишет свое время получения для того, чтобы оценить, сколько времени пакет находился в пути.

Эта временная разница может быть использована для оценки времени, которое понадобилось на то, чтобы пакет проделал путь от сервера к отправителю запроса. Время в оба конца принимается во внимание при оценке текущего времени. Чем меньше время в оба конца, тем более точной будет оценка текущего времени.

Время не будет принято, пока не будут совершены несколько согласовательных обменов пакетами. Для того, чтобы оценить качество образцов, в многокаскадные фильтры помещаются некоторые значимые величины. Обычно NTP клиенту для синхронизации с сервером необходимо 5 минут. Интересен тот факт, что это также выполнятся для локальных эталонных часов, которые по определению не обладают задержкой.

К тому же, на конечную точность влияет качество сетевого соединения. Медленные и непредсказуемые сети с различными задержками плохо влияют на синхронизацию времени.

Для синхронизации NTP необходима временная разница менее 128 мсек. Обычная точность в Internet варьируется от 5 до 100 мсек и зависит от задержек сети.

Уровни трафика NTP

Ширина полосы пропускания, используемая NTP, минимальна. Интервал между сообщениями опроса, которыми обмениваются равноправные узлы, обычно задерживает движение до одного сообщения каждые 17 минут (1024 секунды). При правильном планировании синхронизацию времени можно производить в рамках сетей маршрутизаторов через соединения WAN. Клиенты NTP должны быть равноправными с локальным серверами NTP, а пути к центральным основным маршрутизаторам, являющимся серверами Stratum 2, должны не все лежать через WAN.

Средний NTP-клиент использует примерно 0,6 бит/с на каждом сервере.

Рекомендации Cisco по NTP

- Для достижения высокой точности и надежности Cisco рекомендует использовать несколько серверов времени и различные сетевые пути. Некоторые конфигурации содержат криптографическую аутентификацию, чтобы предотвратить случайные или умышленные атаки на протокол.
- Согласно RFC, NTP был разработан для получения возможности опрашивать несколько различных серверов времени и использовать сложный статистический анализ для выведения правильного времени, даже если нет уверенности в том, что все опрашиваемые серверы надежны. NTP оценивает ошибки всех часов. Поэтому NTP сервера возвращают время вместе с оценкой текущей погрешности. При использовании множества серверов времени NTP также хочет, чтобы эти сервера согласились на некоторое время.
- NTP в исполнении Cisco не поддерживает услугу stratum 1. Нельзя подключиться к радио или атомным часам. Cisco рекомендует получать услуги времени для сети с

общественных NTP серверов, доступных по IP Internet.

- Подключите на всех клиентских коммутаторах функцию отправки регулярных запросов времени дня на NTP сервер. Для достижения быстрой синхронизации можно настроить до 10 серверов/адресов равноправных узлов для каждого клиента.
- Для того чтобы уменьшить потери протокола, вторичные серверы распространяют время через NTP на оставшиеся узлы локальной сети. В интересах надежности можно оборудовать избранные узлы менее точными, но и менее дорогими, часами, которые будут использоваться как резервные в случае сбоя первичных и/или вторичных серверов или путей между ними.
- **ntp update-calendar – NTP обычно изменяет только системные часы.** Эта команда позволяет NTP обновлять информацию о дате/времени в календаре. Обновление происходит только если время NTP синхронизировано. В противном случае календарь сохраняет свое собственное время и остается нетронутым временем NTP или системными часами. Необходимо всегда пользоваться этим на высокопроизводительных маршрутизаторах.
- **clock calendar-valid – эта команда говорит о том, что информация календаря правильная и синхронизированная.** Используйте эту возможность на NTP master. Если это не настроено, высокопроизводительный маршрутизатор, имеющий свой собственный календарь, думает, что это время неавторитетно, даже если у него есть связь с NTP master.
- Любое stratum-число более 15 считается несинхронизированным. **Вот почему в выходных данных команды show ntp status на маршрутизаторах, для которых часы несинхронизированы, можно увидеть stratum 16.** Если master синхронизирован с NTP сервером общего доступа, необходимо убедится в том, что номер stratum в линии связи NTP master на единицу или двойку больше, чем наибольший номер stratum на сервере общего доступа.
- Многие клиенты настраивают NTP на платформах ПО Cisco IOS в серверном режиме и выполняют синхронизацию с несколькими надежными источниками в Интернете или радио часами. Однако, более простой альтернативой серверного режима при использовании большого количества коммутаторов является включение протокола NTP в широковещательном режиме в управляющей VLAN коммутируемого домена. Механизм позволяет Catalyst получать информацию о времени из одного сообщения широковещательной рассылки. Но точность синхронизации времени слегка снижается, поскольку поток информации является однонаправленным.
- Использование адресов обратной связи в качестве источника обновления позволяет повысить согласованность. Существуют два способа решения проблем, связанных с безопасностью:С использованием управления обновлениями сервера, рекомендуемыми CiscoПутем аутентификации

Команды глобальной настройки NTP

```
!--- For the client: clock timezone EST -5 ???? ntp source loopback 0 ????? ntp server ip_address key 1 ntp peer ip_address !--- This is for a peer association. ntp authenticate ntp authentication-key 1 md5 xxxx ntp trusted-key 1 !--- For the server: clock timezone EST -5 clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00 clock calendar-valid ntp source loopback0 ntp update-calendar !--- This is optional: interface vlan_id ntp broadcast !--- This sends NTP broadcast packets. ntp broadcast client !--- This receives NTP broadcast packets. ntp authenticate ntp authentication-key 1 md5 xxxxx ntp trusted-key 1 ntp access-group access-list !--- This provides further security, if needed.
```

Команда статуса NTP

show ntp status Clock is synchronized, stratum 8, reference is 127.127.7.1 nominal freq is 250.0000 Hz, actual freq is 249.9974 Hz, precision is 2**18 reference time is C6CF0C30.980CCA9D (01:34:00.593 IST Mon Sep 12 2005) clock offset is 0.0000 msec, root delay is 0.00 msec root dispersion is 0.02 msec, peer dispersion is 0.02 msec

Это адрес эталонных часов для маршрутизатора Cisco, когда маршрутизатор работает в качестве NTP master. *Если маршрутизатор не был синхронизирован с любым NTP сервером, маршрутизатор использует этот адрес как ID эталона. Для получения дополнительной информации о конфигурации и командах обратитесь к разделу Настройка NTP документа Основы управления системой.*

Протокол Cisco Discovery Protocol

Цель

CDP работает через уровень 2 (уровень линии связи данных) на всех маршрутизаторах, мостах, серверах доступа и коммутаторах Cisco. CDP позволяет приложениям управления сетью обнаруживать устройства Cisco, соседствующих с уже известными устройствами. В частности приложения управления сетью могут обнаруживать соседей, использующих прозрачные протоколы более низкого уровня. При помощи CDP устройства управления сетью могут изучать тип устройства и адрес агента SNMP соседних устройств. Эта функциональная возможность позволяет приложениям посылать запросы SNMP соседним устройствам.

Команды show, связанные с функциональностью CDP, позволяют разработчику сети определить следующую информацию:

- Номер модуля/порта других соседних устройств с включенным CDP
- Следующие адреса соседних устройств:MAC-адресIP-адресАдрес порта канала
- Версию программного обеспечения соседнего устройства
- Следующую информацию о соседнем устройстве:СкоростьДуплексДомен VTPНастройки собственной VLAN

Раздел Технологическое описание освещает некоторые преимущества CDP версии 2 (CDPv2) над CDP версии 1 (CDPv1).

Технологическое описание

CDP работает во всех LAN и WAN средах, поддерживающих SNAP.

Каждое устройство с настроенным CDP периодически посылает сообщения на адреса многоадресной рассылки. Каждое устройство сообщает как минимум один адрес, по которому это устройство может получать сообщения SNMP. Эти объявления могут также содержать информацию о времени существования или времени промежуточного хранения. Эта информация означает промежуток времени, в течение которого получающее устройство будет хранить информацию CDP прежде, чем ее отбросить.

CDP использует инкапсуляцию SNAP с типом кода 2000. В Ethernet, ATM и FDDI используется адрес назначения многоадресной рассылки 01-00-0c-cc-cc-cc. На устройствах Token Ring используется функциональный адрес c000.0800.0000. Фреймы CDP отправляются периодически каждую минуту.

CDP-сообщения содержат одно или более сообщений, которые помогают устройствам-получателям собирать и сохранять информацию обо всех соседних устройствах.

Эта таблица содержит параметры, поддерживаемые CDPv1:

Параметр	Введите	Описание
1	Идентификатор устройства	Имя узла устройства или серийный номер аппаратного обеспечения в кодировке ASCII
2	Адрес	Адрес уровня 3 интерфейса, отправляющего обновление
3	Идентификатор порта	Порт, на который отправляется обновление CDP
4	Возможности	Описывет функциональные возможности устройства следующим образом: • Маршрутизатор: 0x01 • Мост SR1: 0x04 • Коммутатор: 0x08 (обеспечивает коммутацию уровня 2 и/или уровня 3) • Хост: 0x10 • Условная фильтрация IGMP: 0x20 • Мост или коммутатор не пересылает пакеты отчетов IGMP на немаршрутизируемые порты.
5	Version	Строка символов, содержащая версию программного обеспечения **Примечание:** Выходные данные **команды Show version** показывают ту же информацию.
6	Платформа	Платформа оборудования, например WS-C5000, WS-C6009 и Cisco RSP2

1 SR = маршрутизация от источника.

2 RSP = Route Switch Processor (процессор маршрутизирующего коммутатора).

В CDPv2 были введены дополнительный тип, длина, значения (TLV). CDPv2 поддерживает любые TLV. Но данная таблица содержит параметры, которые могут быть чрезвычайно полезными в коммутируемых средах и в средах, использующих программное обеспечение Catalyst.

Когда в коммутаторе работает CDPv1, он отбрасывает фреймы CDPv2. Когда коммутатор,

работающий с CDPv2, получает на интерфейс фрейм CDPv1, он в дополнение к фреймам CDPv2 начинает передачу фреймов CDPv1 из этого интерфейса.

Параметр	Введите	Описание
9	Домен VTP	Домен VTP, если он настроен на устройстве
10	Native VLAN	В dot1q, фреймы для VLAN, в которой находится порт, если порт не является магистральным, остаются немечеными. Эта VLAN обычно называется собственной VLAN.
11	Дуплексная и полудуплексная связь	Эти TLV содержат дуплексные настройки отправляющего порта.
14	Идентификатор устройства VLAN	Позволяет трафику VoIP быть отделенным от другого трафика посредствам отдельного идентификатора VLAN (вспомогательная VLAN).
16	Потребляемая мощность	Максимальное количество электроэнергии, которое предположительно будет поглощаться подключенным устройством, в мВт.
17	MTU	MTU интерфейса, с помощью которого передается фрейм CDP.
18	Extended Trust	Обозначает, что порт находится в режиме Extended Trust.
19	COS для ненадежных портов	Величина класс обслуживания (CoS) должна использоваться для маркировки всех пакетов, полученных с ненадежных портов подключенного коммутирующего устройства.
20	SysName	Полное доменное имя устройства (0, если неизвестно).
25	Запрашиваемая мощность	Передается устройством, поглощающим мощность, для согласования подходящего уровня мощности.
26	Доступная мощность	Передается коммутатором. Позволяет устройству, поглощающему мощность, согласовывать и выбирать соответствующие настройки мощности.

CDPv2/Мощность через Ethernet

В некоторых коммутаторах, таких как Catalyst 6500/6000 и 4500/4000, есть возможность подачи мощности к устройствам, поглощающим электроэнергию, через неэкранированную витую пару. Информация, полученная через CDP (параметры 16, 25, 26) помогает при оптимизации управления питанием коммутатора.

CDPv2/Cisco IP-телефония

IP-телефоны Cisco обеспечивают способность к соединению устройствам Ethernet 10/100 Мбит/с, подключенным извне. Эта способность к соединению достигается при помощи интеграции внутреннего коммутатора уровня 2 с тремя портами в IP-телефон. Внутренние порты коммутатора упоминаются как:

- P0 (внутреннее телефонное IP устройство)
- P1 (внешний порт 10/100 Мбит/с)
- P2 (внешний порт 10/100 Мбит/с, подключенный к коммутатору)

Можно переправлять голосовой трафик в отдельную VLAN порта коммутатора, если настроить порты магистрали доступа dot1q. Эта дополнительная VLAN также известна как вспомогательная (CatOS) или голосовая (программное обеспечение Cisco IOS) VLAN. Следовательно, меченый dot1q трафик с IP-телефона может быть отправлен на вспомогательную/голосовую VLAN, а немеченый трафик может быть отправлен через внешний порт телефона 10/100 Мбит/с через VLAN доступа.

Коммутаторы Catalyst могут информировать IP-телефон о идентификаторе голосовой VLAN через CDP (параметр 14: TLV идентификатор устройства VLAN). В результате, метки IP-телефон метит все имеющие отношение к VoIP пакеты с соответствующим идентификатором VLAN и приоритетом 802.1p. Этот TLV CDP также используется для того, чтобы определить, подключен ли IP-телефон с использованием параметра идентификатора устройства.

Эта концепция может использоваться при разработке политики QoS. Взаимодействие коммутатора Catalyst с IP телефоном можно настроить тремя способами:

- Доверенное устройство IP-телефон CiscoУсловно доверять CoS только когда IP-телефон обнаруживается с помощью CDP. Когда IP-телефон определяется при помощи параметра 14 CDP, состояние надежности порта устанавливается в Trust COS. Если IP-телефон не обнаружен, порт становится ненадежным.
- Extended TrustКоммутатор может информировать IP-телефон с помощью CDP (параметр 18) о возможности доверять всем фреймам, полученным на внешний порт 10/100 Мбит/с устройства.
- Переписать COS для ненадежных портовКоммутатор может информировать IP-телефон с помощью CDP (параметр 19) о необходимости переписать значения 802.1p CoS, полученные на внешний порт 10/100 Мбит/с устройства.**Примечание:** По умолчанию весь трафик, который получен на IP-телефоне, внешнем 10/100-Mbps порты, Недоверяем.

Примечание: Это - пример конфигурации для того, как подключить IP-телефон не от компании Cisco с коммутатором.

Примечание: Пример,

```
Switch(config)#interface gigabitEthernet 2/1 Switch(config-if)#switchport mode trunk !--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-if)#switchport trunk native vlan 10 Switch(config-if)#switchport trunk allow vlan 10,30 Switch(config-if)#switchport voice vlan 30 Switch(config-if)#spanning-tree portfast trunk !--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

Рекомендации Cisco по настройке

Информация, которую предоставляет CDP, может быть чрезвычайно полезной при поске и устранении неисправностей, связанных со способностью к соединению уровня 2. Необходимо подключить CDP на всех устройствах, поддерживающих его работу. Введите следующие команды:

- Для того чтобы включить CDP глобально на коммутаторе:`Switch(config)#cdp run`
- Для того чтобы включить CDP для каждого порта по отдельности:`Switch(config)#interface type slot#/port# Switch(config-if)#cdp enable`

Контрольный список конфигурации

Глобальные команды

Выполните вход в систему, включите и установите режим глобальной настройки для начала процесса настройки коммутатора.

```
Switch>enable Switch# Switch#configure terminal Switch(Config)#
```

Характерные глобальные команды (общекорпоративные)

Данный раздел Глобальные команды перечисляет глобальные команды, применимые ко всем коммутаторам клиентской корпоративной сети.

Эта настройка содержит рекомендуемые глобальные команды, которые должны быть добавлены к начальной конфигурации. Необходимо изменить величины в выходных данных перед тем, как копировать и вставлять текст в CLI. Чтобы применить глобальную настройку, введите следующие команды:

```
vtp domain domain_name vtp mode transparent spanning-tree portfast bpduguard spanning-tree etherchannel guard misconfig cdp run no service pad service password-encryption enable secret password clock timezone EST –5 clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00 clock calendar-valid ip subnet-zero ip host tftpserver your_tftp_server ip domain-name domain_name ip name-server name_server_ip_address ip name-server name_server_ip_address ip classless no ip domain-lookup no ip http server no logging console no logging monitor logging buffered 16384 logging trap notifications logging facility local7 logging syslog_server_ip_address logging syslog_server_ip_address logging source-interface loopback0 service timestamps debug datetime localtime show-timezone msec service timestamps log datetime localtime show-timezone msec access-list 98 permit host_ip_address_of_primary_snmp_server access-list 98 permit host_ip_address_of_secondary_snmp_server snmp-server community public ro 98 snmp-server community laneng rw 98 snmp-server enable traps entity snmp-server host host_address traps public snmp-server host host_address traps public banner motd ^CCCCC This is a proprietary system, NOT for public or personal use. All work products, communications, files, data or information directly or indirectly created, input or accessed on this system are and shall become the sole property of the company. This system is actively monitored and accessed by the company. By logging onto this system, the user consents to such monitoring and access. USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES ^C line console 0 exec-timeout 0 0 password cisco login transport input none line vty 0 4 exec-timeout 0 0 password cisco login length 25 clock
```

calendar-valid ntp server *ntp_server_ip_address* **ntp server** *ntp_server_ip_address* **ntp update-calendar**

Глобальные команды, специфические для каждого шасси коммутатора

Глобальные команды в данном разделе являются специфическими для каждого шасси коммутатора, установленного в сети.

Переменные настройки, зависящие от шасси

Для того чтобы установить дату и время, выполните следующую команду:

Switch#**clock set** *hh:mm:ss day month year*

Для того чтобы задать имя узла устройства, выполните следующие команды:

Switch>**enable** Switch#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#**hostname Cat6500**

Для настройки интерфейса loopback для управления введите следующие команды:

CbrCat6500(config)#**interface loopback 0** Cat6500(config-if)#**description Cat6000 - Loopback address and Router ID** Cat6500(config-if)#**ip address** *ip_address subnet_mask* Cat6500(config-if)#**exit**

Для того чтобы показать версию программного обеспечения Cisco IOS Supervisor Engine, выполните следующие команды:

Cbrcat6500#**show version | include IOS** IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE ASE SOFTWARE (fc1) cat6500#

Для того чтобы показать версию загрузочного файла MSFC, выполните следующую команду:

Cat6500#**dir bootflash:** Directory of bootflash:/ 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a 15990784 bytes total (14111616 bytes free

Для того чтобы указать контактную информацию и расположение SNMP сервера, выполните следующие команды:

Cat6500(config)#**snmp-server contact** *contact_information* Cat6500(config)#**snmp-server location** *location_of_device*

Для копирования загрузочной конфигурации от Механизма существующего модуля управления до нового Supervisor Engine, мог быть, некоторые теряют конфигурации, например, конфигурации на интерфейсах существующего модуля управления. Cisco рекомендует скопировать конфигурацию к текстовому файлу и вставить ее в сегментах в консоль, чтобы видеть, существуют ли какие-либо проблемы конфигурации, которые происходят.

Команды интерфейса

Функциональные типы портов Cisco

Порты коммутатора в программном обеспечении Cisco IOS называются интерфейсами. В ПО Cisco IOS существуют два типа режимов интерфейса:

- Маршрутизируемый интерфейс уровня 3
- Маршрутизируемый интерфейс уровня 2

Функция интерфейса обращается к настройкам порта. Настройка порта может быть:

- Маршрутизируемый интерфейс
- Коммутируемый виртуальный интерфейс (SVI)
- Порт доступа
- Транк
- EtherChannel
- Комбинация всего перечисленного

Тип интерфейса обращается к типу порта. Тип порта может быть:

- FE
- GE
- Канал порта

Этот список коротко описывает функции интерфейсов ПО Cisco IOS:

- Маршрутизируемый физический интерфейс (по умолчанию) – каждый интерфейс коммутатора по умолчанию маршрутизируется интерфейсом уровня 3, похожим на любой маршрутизатор Cisco. Маршрутизируемый интерфейс должен попадать в одну IP-подсеть.
- Интерфейс порта коммутатора доступа – эта функция используется, чтобы поместить интерфейсы в одну и ту же VLAN. Порты должны преобразованы из маршрутизируемых интерфейсов в коммутируемые.
- SVI – SVI может соответствовать VLAN, содержащей порты коммутатора доступа для маршрутизации между сетями VLAN. Если необходим маршрутизатор или мост между портами коммутатора доступа на разных VLAN, необходимо настроить SVI таким образом, чтобы он соответствовал VLAN.
- Интерфейс магистрального порта коммутатора – эта функция используется для направления множественных VLAN к другому устройству. Порты должны преобразованы из маршрутизируемых интерфейсов в магистральный порт коммутатора.
- EtherChannel – EtherChannel используется для группирования индивидуальных портов в один логический порт для избыточности и баланса нагрузки.

Рекомендации Cisco по поводу функциональных типов портов

Информация этого раздела может быть использована как вспомогательная при определении параметров, применимых к интерфейсу.

Примечание: Некоторые специальные команды интерфейса включены, если это возможно.

Автосогласование

Не используйте автосогласование в следующих ситуациях:

- Для портов, поддерживающих устройства сетевой инфраструктуры, такие как коммутаторы и маршрутизаторы
- Для других непередающих конечных систем, таких как серверы и принтеры

Настройка скорости и дуплексного режима этих 10/100 Мбит/с линий связи должна

осуществляться вручную. Полнодуплексный режим при 100 Мбит/с обычно используется для:

- линий связи 100 Мбайт между двумя коммутаторами
- линий связи 100 Мбайт между коммутатором и сервером
- линий связи 100 Мбайт между коммутатором и маршрутизатором

Вы можете настроить эти параметры следующим образом:

```
Cat6500(config-if)#interface [type] mod#/port# Cat6500(config-if)#speed 100 Cat6500(config-if)#duplex full
```

Cisco рекомендует конечным пользователям настройки линии связи 10/100 Мбит/с. Мобильные сотрудники и передающие узлы нуждаются в автосогласовании, как показано в примере:

```
Cat6500(config-if)#interface [type] mod#/port# Cat6500(config-if)#speed auto
```

Gigabit. Однако, выполните следующие команды для того, чтобы убедиться, что автосогласование включено. Cisco рекомендует включать согласование Gigabit:

```
Cat6500(config-if)#interface gigabitethernet mod#/port# Cat6500(config-if)#no speed
```

Корень связующего дерева

При анализе структуры сети необходимо определить коммутатор, подходящий для того, чтобы быть корнем для каждой VLAN. Как правило, нужно выбрать мощный коммутатор в середине сети. Разместите корневой мост в центре сети и напрямую подключите к нему серверы и маршрутизаторы. Такая настройка позволяет уменьшить среднее расстояние от клиента до сервера или маршрутизатора. Обратитесь к документу Устранение неполадок протокола связующего дерева и решение соответствующих вопросов разработки для получения дополнительных сведений.

Для того чтобы вынудить коммутатор стать корневым для назначенной VLAN, выполните следующую команду:

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

Spanning-tree portfast

PortFast можно использовать для обхода нормальной работы связующего дерева на портах доступа для того, чтобы ускорить начальные задержки соединения, возникающие при соединении конечных станций к коммутатору. Дополнительные сведения о PortFast см. в разделе Использование PortFast и других команд для устранения задержек соединения во время запуска рабочей станции.

Установите PortFast STP в on на всех включенных портах доступа, подключенных к одному узлу. Ниже представлен пример:

```
Cat6500(config-if)#interface [type] mod#/port# Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION %Portfast has been configured on FastEthernet3/1 but will only have effect when the interface is in a non-trunking mode.
```

UDLD

Для отслеживания физической конфигурации кабелей включите UDLD только на

оптоволоконных портах инфраструктуры или медных Ethernet кабелях. Для включения UDLD введите следующую команду:

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#udld enable
```

Информация о настройке VLAN

Настройте VLAN при помощи следующих команд:

```
Cat6500(config)#vlan vlan_number Cat6500(config-vlan)#name vlan_name Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id Cat6500(config)#default spanning-tree vlan vlan_id
```

Повторите эти команды для каждой VLAN, а затем выйдите из системы. Введите следующую команду:

```
Cat6500(config)#exit
```

Выполните следующую команду, чтобы проверить все VLAN:

```
Cat6500#show vlan
```

Маршрутизируемые SVI

Для маршрутизации между сетями VLAN необходимо настроить SVI. Введите следующие команды:

```
Cat6500(config)#interface vlan vlan_id Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description Cat6500(config-if)#no shutdown
```

Повторите эти команды для каждой функции интерфейса, содержащей маршрутизируемый SVI, а затем выйдите из системы. Введите следующую команду:

```
Cat6500(config-if)#^Z
```

Маршрутизируемый единый физический интерфейс

Выполните следующие команды для того, чтобы настроить маршрутизируемый интерфейс уровня 3 по умолчанию:

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

Повторите эти команды для каждой функции интерфейса, содержащей маршрутизируемый физический интерфейс, а затем выйдите из системы. Введите следующую команду:

```
Cat6500(config-if)#^Z
```

Маршрутизируемый EtherChannel (L3)

Для того чтобы настроить EtherChannel на интерфейсах уровня 3, выполните в данном разделе следующие команды.

Настройте интерфейс логического порта канала следующим образом:

```
Cat6500(config)#interface port-channel port_channel_interface_# Cat6500(config-if)#description
port_channel_description Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

Выполните действия, описанные в данном разделе, для портов, формирующих конкретный канал. Примените оставшуюся информацию к порту каналу, как показано в примере:

```
Cat6500(config)#interface range [type] mod/port_range Cat6500(config-if)#channel-group 1-64 mode
[active | auto | desirable | on | passive] Cat6500(config-if)#no shutdown Cat6500(config-if)#^Z
```

Примечание: После настройки EtherChannel конфигурация, что вы применяетесь к интерфейсу порт-канал, влияет на EtherChannel. Конфигурация, примененная к портам LAN, влияет только на порт LAN, к которому была применена конфигурация.

EtherChannel (L2) с транкингом

Настройте Layer 2 EtherChannel для транкинга следующим образом:

```
Cat6500(config)#interface port-channel port_channel_interface_# Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type Cat6500(config-if)#switchport
trunk native vlan vlan_id Cat6500(config-if)#no shutdown Cat6500(config-if)#exit
```

Выполните действия, описанные в данном разделе, для портов, формирующих конкретный канал.

```
Cat6500(config)#interface range [type] mod/port_range Cat6500(config-if)#channel-group 1-64 mode
[active | auto | desirable | on | passive] Cat6500(config-if)#no shutdown Cat6500(config-
if)#exit
```

Примечание: После настройки EtherChannel конфигурация, что вы применяетесь к интерфейсу порт-канал, влияет на EtherChannel. Конфигурация, примененная к портам LAN, влияет только на порт LAN, к которому была применена конфигурация.

Проверьте создание всех каналов EtherChannel и магистралей. Ниже представлен пример:

```
Cat6500#show etherchannel summary Cat6500#show interface trunk
```

Порты доступа

Если функция интерфейса находится в порте доступа, настроенного как один интерфейс, выполните следующие команды:

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id Cat6500(config-if)#exit
```

Повторите эти команды для каждого интерфейса, который должен быть настроен как порт коммутатора уровня 2.

Если порт коммутатора должен быть подключен к конечным станциям, выполните следующую команду:

```
Cat6500(config-if)#spanning-tree portfast
```

Порты доступа (единый физический интерфейс)

Если функция интерфейса находится в порте магистрали, настроенного как один интерфейс, выполните следующие команды:

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#switchport Cat6500(config-
if)#switchport trunk encapsulation dot1q Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown Cat6500(config-if)#exit
```

Повторите эти команды для каждой функции интерфейса, который должен быть настроен как порт магистрали.

Информация о пароле

Выполните следующие команды для получения информации о пароле:

```
Cat6500(config)#service password-encryption Cat6500(config)#enable secret password
CbrCat6500(config)#line con 0 Cat6500(config-line)#password password CbrCat6500(config-
line)#line vty 0 4 Cat6500(config-line)#password password Cat6500(config-line)#^Z
```

Сохраните конфигурацию

Выполните следующую команду, чтобы сохранить конфигурацию:

```
Cat6500#copy running-config startup-config
```

Новые функциональные возможности программного обеспечения Cisco IOS релиза 12.1(13)E

Дополнительные сведения о поддержке IP-телефона см. в разделе Настройка поддержки IP-телефона Cisco.

Дополнительные сведения о сетевом распознавании приложений для портов LAN см. в разделе Сетевое распознавание приложений и распространенное сетевое распознавание приложений.

Примечания:

- NBAR для портов LAN поддерживается программным обеспечением на MSFC2.
- PFC2 обеспечивает поддержку оборудования для ввода ACL на портах LAN, на которых настроено NBAR.
- Когда PFC QoS включен, трафик через порты LAN, на которых настроено NBAR, проходит через входящую и исходящую очереди и порог падения.
- Когда PFC QoS включен, MSFC2 устанавливает исходящий класс обслуживания (CoS) равным исходящему IP приоритету.
- После того как трафик пройдет очередь входа, весь трафик будет обработан программным обеспечением на MSFC2 портов LAN, на которых настроено NBAR.
- Распределенное NBAR доступно на интерфейсах FlexWAN, использующих ПО Cisco IOS релиза 12.1(6)E и более поздних.

Улучшенная функция экспорта данных Netflow (NDE) включает:

- Интерфейс источника-назначения и маски потока интерфейса
- NDE версии 5 из PFC2
- Приведенный NetFlow
- Средство заполнения следующих дополнительных полей в записях NDE:IP-адрес следующего узла маршрутизатораВходящий интерфейс SNMP ifIndexИсходящий интерфейс SNMP ifIndexНомер автономной системы источника

Дополнительные сведения см. в разделе Настройка NDE.

Другие улучшенные функциональные возможности это:

- Настройка UDLD
- Настройка протокола VTP
- Настройка служб Web Cache при помощи WCCP

Следующие команды являются новыми:

- **standby delay minimum reload**
- **link debounce**
- **vlan internal allocation policy {ascending | descending}**
- **system jumbomtu**
- **clear catalyst6000 traffic-meter**

Следующие команды являются улучшенными:

- **show vlan internal usage – эта команда была улучшена, включив использование VLAN, которыми пользуются интерфейсы WAN.**
- **show vlan id – эта команда была улучшена поддержкой введения диапазона VLAN.**
- **show l2protocol-tunnel – эта команда была улучшена поддержкой введения идентификатора VLAN.**

Программное обеспечение Cisco IOS релиза 12.1(13)E поддерживает следующие программные функциональные возможности, которые ранее поддерживались в программном обеспечении Cisco IOS релиза 12.1 EX:

- Настройка каналов EtherChannels уровня 2, включающих интерфейсы на различных оборудованных DFC коммутирующих модуляхСм. раздел «Решенные общие предупреждения в релизе 12.1(13)E» в описании дефекта номер CSCdt27074 (только для зарегистрированных клиентов).
- Режим избыточности процессора маршрутизатора плюс (RPR+)См. раздел Настройка RPR или RPR+ избыточности Supervisor Engine.**Примечание:** В программном обеспечении Cisco IOS версии 12.1(13)E и позже, RPR и характеристики резервирования RPR+ заменяют резервирование повышенного уровня готовности системы (EHSA).
- 4096 VLAN уровня 2!--- см. в Настройка сетей VLAN.**Примечание:** Программное обеспечение Cisco IOS версии 12.1(13)E и более поздние версии поддерживают конфигурацию 4,096 интерфейсов виртуальной локальной сети (VLAN) Уровня 3. Настройте в общем не более 2 000 интерфейсов VLAN уровня 3 и порты уровня 3 на MSFC2 с Supervisor Engine II или Supervisor Engine I. Настройте в общем не более 1 000 интерфейсов VLAN уровня 3 и порты уровня 3 на MSFC.
- Туннелирование IEEE 802.1QСм. раздел Настройка туннелирования IEEE 802.1Q и туннельного протокола уровня 2.
- Туннельный протокол IEEE 802.1QСм. раздел Настройка туннелирования IEEE 802.1Q и туннельного протокола уровня 2.
- Множественные связующие деревья (MST) IEEE 802.1sСм. раздел Настройка STP и IEEE 802.1s MST.
- IEEE 802.1w быстрый STP (RSTP)См. раздел Настройка STP и IEEE 802.1s MST.
- IEEE 802.3ad LACPСм. раздел Настройка уровня 2 и уровня 3 EtherChannel.
- Фильтрация BPDU PortFastСм. раздел Настройка функций STP.
- Автоматическое создание интерфейсов VLAN уровня 3 для поддержки VLAN ACL (VACL)См. раздел Настройка параметров сетевой безопасности.
- Захватывающие порты VACL, способные быть любым портом Ethernet уровня 2 в любой VLANСм. раздел Настройка параметров сетевой безопасности.
- Настраиваемый размер MTU на индивидуальных физических портах уровня 3См. раздел Обзор конфигурации интерфейса.
- Настройка портов назначения SPAN как магистралей таким образом, чтобы весь трафик SPAN маркировалсяСм. раздел Настройка локального и удаленного SPAN.

Дополнительные сведения

- Инструменты и ресурсы – Cisco Systems
- Поддержка коммутаторов
- Поддержка технологии коммутации локальных сетей
- Cisco Systems – техническая поддержка и документация