QTECH
МИР ДОСТУПНЕЕ

КОНФИГУРАЦИЯ ПОРТОВ

Коммутатор агрегации

СЕРИЯ QSW-8400

Оглавление

1 КОНФИГУРИРОВАНИЕ ПОРТОВ

1.1 Введение в функцию изоляции портов

Изоляция портов — это независимая порто-ориентированная функция, работающая между портами, которая изолирует потоки различных портов друг от друга. С помощью этой функции пользователь может изолировать порты в пределах VLAN для сохранения ресурсов VLAN и усиления секретности сети. После того, как эта функция будет сконфигурирована, порты в группе изолированных портов будут изолированы друг от друга, в то время как порты из различных групп изоляции или неизолированных могут пересылать данные друг другу совершенно нормально. На коммутаторе может быть сконфигурировано не более 16 групп изоляции портов.

1.2 Список команд для конфигурации изоляции портов

1. Создать группу изолированных портов.

Команда	Описание
Режим глобального конфигурирования	
isolate-port group <*WORD*> **no isolate-port group <*WORD*>**	Создает группу изолированных портов. С оператором NO эта команда удаляет группу изолированных портов.

2. Добавить Ethernet порты в группу.

Команда	Описание
Режим глобального конфигурирования	
isolate-port group <*WORD*> switchport interface [ethernet | port-channel] <*IFNAME*> **no isolate-port group <*WORD*> switchport interface [ethernet | port-channel] <*IFNAME*>**	Добавляет один порт или группу портов в группу изолированных портов, которые будут изолированы от других портов в группе. Оператор NO удаляет один порт или группу портов из группы изолированных портов.

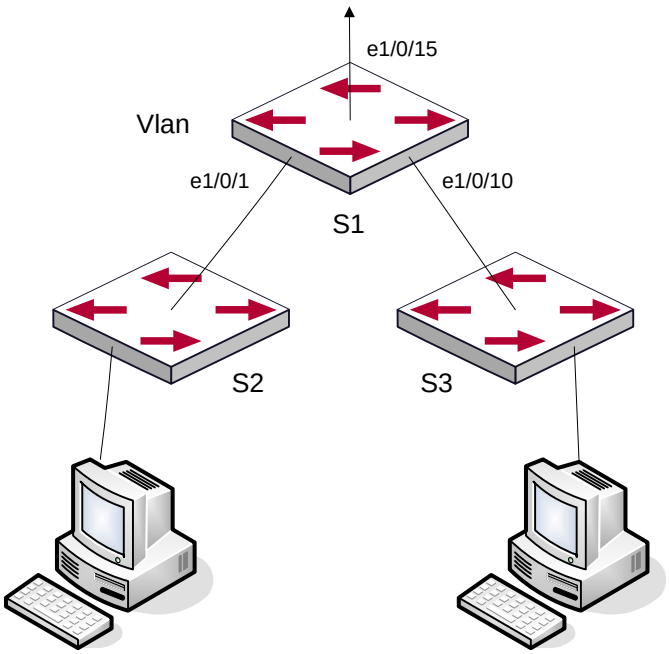
3. Определить потоки, которые будут изолироваться.

Команда	Описание
Режим глобального конфигурирования	
isolate-port apply [<l2|l3|all>]	Применяет конфигурацию изоляции портов для изоляции потоков второго или третьего уровня или обоих уровней сразу.

4. Отобразить конфигурацию группы изоляции портов.

Команда	Описание
Режим администратора, Режим глобального конфигурирования	
show isolate-port group [*<WORD>*]	Показывает конфигурацию групп изолированных портов, включая все сконфигурированные группы изолированных портов и Ethernet порты в каждой группе.

1.3 Типовые примеры функции изоляции портов



Топология и конфигурация коммутаторов показана на рисунке выше. Порты e1/0/1, e1/0/10 и e1/0/15 принадлежат к VLAN 100. Требование заключается в том, чтобы после включения функции изоляции портов на коммутаторе switch1 порты e1/0/1 и e1/0/10 на этом коммутаторе не могли связываться друг с другом и оба могли связываться с портом e1/0/15, смотрящим в сеть. То есть, связи между любыми парами низлежащих портов нет, и в то же время связь между любым низлежащим портом и вышестоящим работает. Вышестоящий порт может работать с любым портом нормально.

Конфигурация коммутатора S1:

```
Switch(config)#isolate-port group test
Switch(config)#isolate-port group test switchport interface ethernet 1/0/1;1/0/10
```

2 КОНФИГУРАЦИЯ ФУНКЦИИ РАСПОЗНАВАНИЯ ПЕТЛИ НА ПОРТУ

2.1 Введение в функцию распознавания петли

С развитием сетевых устройств все больше и больше пользователей подключаются к сети через Ethernet-коммутаторы. В промышленных сетях пользователи получают доступ через коммутаторы 2-го уровня, что предъявляет строгие требования к взаимодействию между устройствами как внешней, так и внутренней сети. Когда требуется взаимодействие на 2-м уровне, сообщение должно отправляться точно в соответствии с MAC адресом для корректной работы между пользователями. Устройства второго уровня запоминают MAC адреса, изучая входящие MAC адреса источников пакетов, и при поступлении пакета с неизвестным адресом источника они записывают его MAC адрес в таблицу, закрепляя его за портом, откуда пришел этот пакет. Таким образом, следующий пакет с данным MAC адресом в качестве порта назначения будет отправлен сразу на этот порт. То есть адрес сразу фиксируется на порту для отправки всех пакетов.

Когда пакет с MAC адресом источника, уже запомненным коммутатором, приходит через другой порт, запись в таблице MAC адресов изменяется таким образом, чтобы пакеты с данным MAC адресом направлялись через новый порт. В результате, если на участке между двумя адресатами существует какая-либо петля, все MAC адреса из сети второго уровня будут пересылаться на тот порт, где существует петля (обычно MAC адреса в этом случае с высокой частотой переключаются с одного порта на другой), что вызывает перегрузку и потерю работоспособности сети 2-го уровня. Вот почему необходимо проверять наличие петли на сетевых портах. Когда на порту определяется петля, обнаружившее ее устройство должно послать предупреждение в систему управления сетью, позволяя сетевому администратору обнаружить, локализовать и решить проблему в сети.

Поскольку система обнаружения петель может автоматически принимать решения о наличии петли в соединении и ее исчезновении, устройства с функциями контроля на портах (таких как изоляция портов и контроль за запоминанием MAC адресов) могут значительно снизить нагрузку с сетевого администратора, а также уменьшить время реакции на проблему, минимизируя воздействие петли на сеть.

2.2 Список команд для конфигурирования функции распознавания петли на порту

1. Конфигурирование временного интервала распознавания петли.

Команда	Описание
Режим глобального конфигурирования	

loopback-detection interval-time *<loopback> <no-loopback>* **no loopback-detection interval-time**	Конфигурирование временного интервала распознавания петли

2. Включение функции распознавания петли.

Команда	Описание
Режим конфигурирования порта	
loopback-detection specified-vlan <vlan-*list*> **no loopback-detection specified-vlan <vlan-*list*>**	Включение и выключение функции распознавания петли

3. Конфигурирование режима порта при распознавании петли.

Команда	Описание
Режим конфигурирования порта	
loopback-detection control {shutdown |block| learning} **no loopback-detection control**	Включение и выключение определенного режима порта при распознавании петли.

4. Вывод отладочной информации по распознаванию петли.

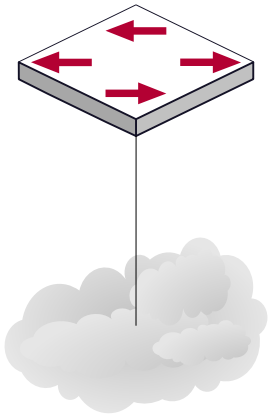
Команда	Описание
Режим администратора	
debug loopback-detection **no debug loopback-detection**	Вывод отладочной информации по распознаванию петли. С оператором NO данная команда прекращает вывод отладочной информации.

show loopback-detection [interface *<interface-list>*]	Показывает статус и результаты распознавания петли на всех портах, если других параметров не вводится; в противном случае показывается статус и результат распознавания петли для конкретных портов

5. Конфигурирование режима восстановления при распознавании петли.

Команда	Описание
Общий режим	
loopback-detection control-recovery timeout <0-3600>	Конфигурирование режима восстановления при распознавании петли (автоматическое восстановление или нет) или времени восстановления.

2.3 Примеры функции распознавания петли на порту



В приведенной ниже конфигурации, коммутатор определяет существование петли в топологии сети. После включения функции распознавания петли на порту, смотрящем во внешнюю сеть, коммутатор будет уведомлять подсоединенную сеть о существовании петли и контролировать порт коммутатора для обеспечения нормальной работы данной сети.

Последовательность конфигурации коммутатора:

```
Switch(config)#loopback-detection interval-time 35 15
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#loopback-detection special-vlan 1-3
Switch(Config-If-Ethernet1/0/1)#loopback-detection control block
```

Если выбран метод блокировки при определении петли, должен быть глобально включен протокол MSTP на всей сети, а также должны быть сконфигурированы соответствующие связи между протоколом связующего дерева и VLAN.

```
Switch(config)#spanning-tree
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1
Switch(Config-Mstp-Region)#instance 2 vlan 2
Switch(Config-Mstp-Region)#
```

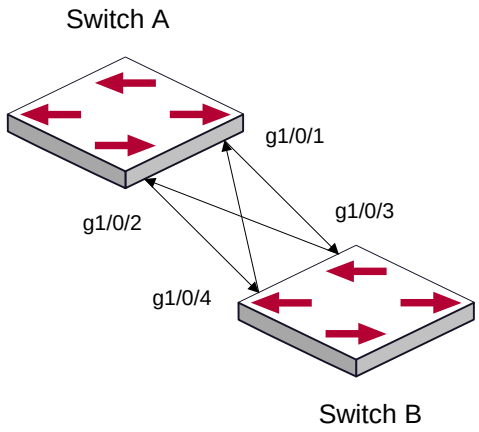
2.4 Решение проблем с функцией распознавания петли на порту

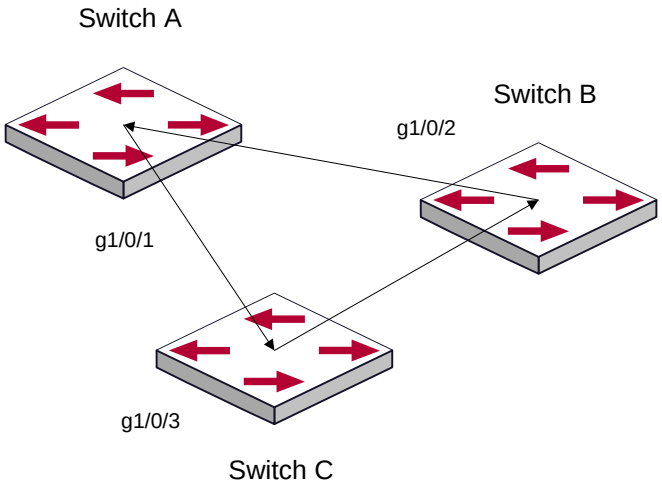
Функция распознавания петли на порту выключена по умолчанию и должна быть включена при необходимости.

3 КОНФИГУРАЦИЯ ФУНКЦИИ ULDP

3.1 Общая информация о ULDP

Однонаправленный линк — это распространенная проблема в сети, особенно для оптических соединений. Под однонаправленным соединением понимается ситуация, когда один порт соединения может принимать сообщения от другого порта, а тот не может получать их от первого. Если физический уровень соединения есть и работает нормально, проблема связи между устройствами не может быть обнаружена. Как показано на рисунке, проблема оптического соединения не может быть обнаружена посредством механизмов физического уровня, таких как автоматическое согласование параметров.





Такой вид проблем часто возникает в ситуации, когда или интерфейс или GBIC (Giga Bitrate interface Converter – конвертер интерфейса со скоростью 1Gb) имеют программные проблемы, в этом случае оборудование становится недоступным или работает неправильно. Однонаправленное соединение может вызывать целую серию

проблем, таких как зацикливание связующего дерева или широковещательным штормам.(broadcast black hole).

ULDP (Unidirectional Link Detection Protocol – протокол обнаружения однонаправленных соединений) может помочь обнаружить неисправность, которая возникает в ситуациях, перечисленных выше. В коммутаторе, подключенном через оптическую или медную Ethernet линию (такую как витая пара пятой категории), ULDP может следить за статусом физических соединений. В случае если обнаружено однонаправленное соединение, он посылает предупреждение пользователям и может выключить порт автоматически, или вручную, в зависимости от конфигурации пользователя.

Функция ULDP в коммутаторе распознает удаленные устройства и проверяет корректность соединений, используя интерактивную систему собственных сообщений. Когда ULDP включен на порту, механизм определения статуса порта запускается, что подразумевает посылку сообщений различного вида, которые посылаются различными подпрограммами этого механизма для проверки статуса соединений путем обмена информацией с удаленными устройствами. ULDP может динамически определять интервал, с которым удаленное устройство посылает свои уведомления и подстраивает в соответствии с ним свой локальный интервал. Кроме того, ULDP обеспечивает механизм рестарта, если порт был заблокирован ULDP, также соединение может быть проверено еще раз после рестарта. Временной интервал посылки уведомлений и рестарта порта в ULDP может конфигурироваться пользователями, таким образом, ULDP может быстрее реагировать на проблемы соединений в различном сетевом окружении. Показателем правильной работы ULDP является работа соединения в дуплексном режиме, это значит, что ULDP включен на обоих концах соединения и использует одинаковый метод авторизации и пароль.

3.2 Список команд для конфигурирования ULDP

1. Включение функции ULDP на коммутаторе.

Команда	Описание
Режим глобального конфигурирования	
uldp enable **uldp disable**	Включение или выключение функции ULDP на коммутаторе.

2. Включение функции ULDP на порту.

Команда	Описание
Режим конфигурирования порта	

uldp enable **uldp disable**	Включение или выключение функции ULDP на порт.

3. Конфигурация агрессивного режима на коммутаторе.

Команда	Описание
Режим глобального конфигурирования	
uldp aggressive-mode **no uldp aggressive-mode**	Устанавливает режим работы функции на коммутаторе.

4. Конфигурация агрессивного режима на порту.

Команда	Описание
Режим конфигурирования порта	
uldp aggressive-mode **no uldp aggressive-mode**	Устанавливает режим работы функции на порту.

5. Конфигурация метода выключения однонаправленного соединения.

Команда	Описание
Режим глобального конфигурирования	
uldp manual-shutdown **no uldp manual-shutdown**	Конфигурирует метод выключения однонаправленного соединения.

6. Конфигурация интервала уведомлений (Hello messages).

Команда	Описание
Режим глобального конфигурирования	
uldp hello-interval *<integer>*	Конфигурация интервала уведомлений (Hello messages), диапазон от 5 до 100

no uldp hello-interval	секунд. Значение по умолчанию - 10 сек.

7. Конфигурация интервала восстановления.

Команда	Описание
Режим глобального конфигурирования	
uldp recovery-time *<integer>* **no uldp recovery-time *<integer>***	Конфигурирует интервал восстановительного рестарта. Диапазон от 30 до 86400 секунд. Значение по умолчанию — 0 секунд.

8. Рестарт порта, выключенного функцией ULDP.

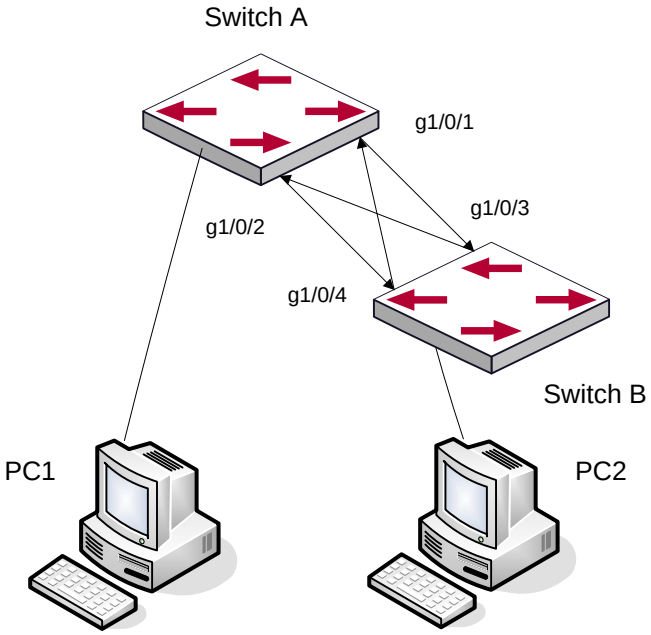
Команда	Описание
Режим глобального конфигурирования или режим конфигурирования порта	
uldp reset	Рестартует все порты в режиме глобального конфигурирования. Рестартует конкретный порт в режиме конфигурирования порта.

9. Демонстрационная и отладочная информация функции ULDP.

Команда	Описание
Режим администратора	
show uldp [interface ethernet IFNAME]	Показывает информацию по ULDP. Для отображения общей ULDP информации параметров нет. При задании конкретного порта выводится общая информация и информация о соседях по данному порту.
debug uldp fsm interface ethernet *<IFname>* **no debug uldp fsm interface ethernet *<IFname>***	Включение или выключение вывода отладочной информации по определенному порту
debug uldp error	Включение или выключение отладочной информации об ошибках

no debug uldp error	
debug uldp event **no debug uldp event**	Включение или выключение отладочной информации о событиях
debug uldp packet {receive|send} **no debug uldp packet {receive|send}**	Включение или выключение вывода отладочной информации по типу сообщений
debug uldp {hello|probe|echo| unidir|all} [receive|send] interface ethernet <*IFname*> **no debug uldp {hello|probe|echo| unidir|all} [receive|send] interface ethernet <*IFname*>**	Включение или выключение вывода детальной информации об определенном типе сообщений, которые могут посылаться или приниматься на определенном порту.

3.3 Типовые примеры функции ULDP



В сетевой топологии на рисунке порты g1/0/1 и g1/0/2 на коммутаторе A, а так же порты g1/0/3 и g1/04 на коммутаторе B – оптические. И соединение имеет перекрестный тип. Физический уровень включен и работает нормально, но соединение на уровне данных неработоспособно. ULDP может определить и заблокировать такой тип ошибки на соединении. Конечным результатом будет то, что порты g1/0/1 и g1/0/2 на коммутаторе A, а так же порты g1/0/3 и g1/04 на коммутаторе B будут заблокированы функцией ULDP. Порты смогут работать (не будут заблокированы) только если соединение будет корректным.

Последовательность конфигурации коммутатора A:

```
SwitchA(config)#uldp enable
SwitchA(config)#interface ethernet 1/0/1
SwitchA (Config-If-Ethernet1/0/1)#uldp enable
SwitchA (Config-If-Ethernet1/0/1)#exit
SwitchA(config)#interface ethernet1/0/2
SwitchA(Config-If-Ethernet1/0/2)#uldp enable
```

Последовательность конфигурации коммутатора B:

```
SwitchB(config)#uldp enable
SwitchB(config)#interface ethernet1/0/3
SwitchB(Config-If-Ethernet1/0/3)#uldp enable
SwitchB(Config-If-Ethernet1/0/3)#exit
SwitchB(config)#interface ethernet1/0/4
SwitchB(Config-If-Ethernet1/0/4)#uldp enable
```

В результате порты g1/0/1 и g1/0/2 на коммутаторе A будут заблокированы функцией ULDP и на дисплее терминала PC1 появится следующая информация.

```
%Oct 29 11:09:50 2007 A unidirectional link is detected!  Port Ethernet1/0/1
need to be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/1 shut down!
%Oct 29 11:09:50 2007 A unidirectional link is detected!  Port Ethernet1/0/2
need to be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/2 shutted down!
```

Порты g1/0/3 и g1/0/4 на коммутаторе B будут заблокированы функцией ULDP и на дисплее терминала PC2 появится следующая информация.

```
%Oct 29 11:09:50 2007 A unidirectional link is detected!  Port Ethernet1/0/3
need to be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/3 shutted down!
%Oct 29 11:09:50 2007 A unidirectional link is detected!  Port Ethernet1/0/4
need to be shutted down!
%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/4 shutted down!
```

3.4 Устранение неполадок функции ULDP

Замечания по конфигурации:

- Для уверенности, что ULDP сможет определить, что один из оптических портов не подключен или порты некорректно соединены, порты должны работать в дуплексном режиме и иметь одинаковую скорость.
- Если механизм автоматического определения параметров оптических портов, один из которых включен некорректно, определит рабочий режим и скорость, ULDP не сможет отработать корректно, вне зависимости от того, включен он или нет. В данной ситуации порт помечается как выключенный.

- Для уверенности в том, что ответный порт корректно сконфигурирован, и однонаправленное соединение сможет быть корректно определено, необходимо, чтобы на обоих концах соединения ULDP был включен и использовался одинаковый метод авторизации и пароль. В нашем примере пароль с обеих сторон не установлен.
- Интервал отправки hello сообщений может быть изменен (это 10 секунд по умолчанию и колеблется от 5 до 100 секунд), так что ULDP могут быстрее реагировать на ошибки подключения линий в различных условиях работы сети. Но этот интервал должен быть меньше 1/3 от времени конвергенции STP. Если интервал слишком длинный, петля STP будет сформирована до того как ULDP обнаружит и отключит порт однонаправленного соединения. Если интервал слишком короткий, сетевая нагрузка на порт будет увеличена, что означает снижение пропускной способности.
- ULDP не обрабатывает события LACP. Он обрабатывает каждое соединение группы TRUNK (например, port-channal, TRUNK порты) независимо друг от друга.
- ULDP не работает с похожими протоколами других производителей. Это означает, что пользователи не могут использовать ULDP на одном конце и использовать другие подобные протоколы на другом конце соединения.
- ULDP функция отключена по умолчанию. После включения функции ULDP а режиме глобального конфигурирования можно включить вывод отладочных сообщений. Существует несколько команд отладки (DEBUG) для вывода отладочной информации. Например, информацию о событиях, состоянии, ошибках и сообщениях. Различные типы отладочных сообщений также могут быть выведены в соответствии с различными значениями параметров.
- Таймер восстановления по умолчанию выключен и может быть включен только в случае, когда пользователь задал время восстановления (30-86400 секунд).
- Команда рестарта и механизм перезагрузки порта воздействуют только на порт, который был выключен функцией ULDP. Порты, выключенные вручную, пользователями или другими функциями не могут быть рестартованы функцией ULDP.

4 НАСТРОЙКА ФУНКЦИИ LLDP

4.1 Общие сведения о функции LLDP

Протокол исследования соединительного уровня (Link Layer Discovery Protocol – LLDP) - это новый протокол, описанный в спецификации 802.1ab. Он позволяет соседним устройствам посылать уведомления о своем статусе другим устройствам и на всех портах любого устройства сохранять информацию об этом. Если необходимо, порты так же могут посылать информацию об изменении статуса устройствам, непосредственно подключенным к ним. Эта информация будет сохранена в стандартных MIB SNMP. Система управления сетью может проверять состояние соединений второго уровня по информации из MIB. LLDP не конфигурирует или контролирует элементы сети или потоки, он только описывает конфигурацию второго уровня. В спецификации 802.1ab также описывается, как используется информация, предоставляемая LLDP для обнаружения конфликтов на втором уровне. Институт стандартизации (IEEE) в настоящее время использует существующую физическую топологию, интерфейсы и наборы MIB IETF.

Упрощенно, LLDP – протокол обнаружения соседних устройств. Он определяет стандартный метод, позволяющий Ethernet устройствам, таким, как коммутаторы, маршрутизаторы и точки доступа уведомлять о своем существовании другие узлы сети и сохранять информацию обо всех соседних устройствах. Как следствие, детальная информация о конфигурации устройства и о найденных соседях может объявляться посредством данного протокола.

В частности, LLDP определяет состав основного информационного объявления, передачу объявления и метод сохранения данной информации. Для объявления собственной информации устройство может посылать несколько частей информационного объявления в одном LAN пакете данных. Тип передачи определяется значением поля TLV (Type Length value – значение длины типа). Все устройства, поддерживающие LLDP, должны поддерживать оповещения об идентификаторе (ID) устройства и идентификаторе порта, но предполагается, что большинство устройств поддерживают оповещения об имени системы, ее описании и производительности системы. Оповещения с описанием системы и о производительности системы могут также содержать полезную информацию, необходимую для сбора информации о потоках в сети. Описание системы может включать такие данные как полное имя объявляемого устройства, тип устройства, версия его операционной системы и так далее.

Протокол LLDP позволяет упростить поиск проблем в корпоративной сети, расширить возможности инструментов управления сетью путем определения и хранения точной сетевой структуры.

Многие типы программ управления сетью используют функцию автоматического обнаружения (“Automated Discovery””) для отслеживания изменений и текущего состояния топологии, но большинство из них работает только на третьем уровне и в лучшем случае классифицирует устройства по их подсетям. Эти данные слишком примитивны, позволяют отслеживать только базовые события, такие как добавление или

удаление устройств вместо детальной информации о них и о том, как устройства взаимодействуют с сетью.

Информация, собранная на 2 уровне содержит сведения об устройствах, их портах и о том какие коммутаторы с какими соединены и т. п. Она так же может показывать маршруты между клиентами, коммутаторами, маршрутизаторами и сетевыми серверами. Такие данные очень важны для определения и исследования источника проблем на сети.

LLDP является полезным инструментом управления, предоставляющим точную информацию о зеркалировании сети, отображении потоков данных и поиске сетевых проблем.

4.2 Список команд для конфигурирования LLDP

1. Включение LLDP на устройстве.

Команда	Описание
Режим глобального конфигурирования	
lldp enable **lldp disable**	Общее включение/выключение

2. Включение функции LLDP на порту.

Команда	Описание
Режим конфигурирования порта	
lldp enable **lldp disable**	Включение/выключение функции LLDP на порту.

3. Конфигурация статуса LLDP на порту.

Команда	Описание
Режим конфигурирования порта	
lldp mode (send|receive|both|disable)	Конфигурация режима работы функции LLDP

4. Конфигурация интервала обновления сообщений LLDP.

Команда	Описание
Режим глобального конфигурирования	
lldp tx-interval *<integer>* **no lldp tx-interval**	Конфигурация интервала обновления сообщений LLDP как определенной величины или значения по умолчанию.

5. Конфигурация множителя времени поддержки сообщений LLDP.

Команда	Описание
Режим глобального конфигурирования	
lldp msgTxHold *<value>* **no lldp msgTxHold**	Конфигурация множителя времени поддержки сообщений LLDP как определенной величины или значения по умолчанию.

6. Конфигурация задержки отправки обновляющих сообщений.

Команда	Описание
Режим глобального конфигурирования	
lldp transmit delay *<seconds>* **no lldp transmit delay**	Конфигурация задержки отправки обновляющих сообщений как определенной величины или значения по умолчанию.

7. Конфигурация интервалов посылки TRAP пакетов.

Команда	Описание
Режим глобального конфигурирования	
lldp notification interval *<seconds>* **no lldp notification interval**	Конфигурация интервалов посылки TRAP пакетов как определенной величины или

	значения по умолчанию.

8. Включение функции TRAP на порту.

Команда	Описание
Режим конфигурирования порта	
lldp trap <enable|disable>	Включение/выключение функции TRAP на порту

9. Конфигурация дополнительных параметров информации для отправки на порту.

Команда	Описание
Режим конфигурирования порта	
lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap] **no lldp transmit optional tlv**	Конфигурация дополнительных параметров информации для отправки на порту как определенной величины или значения по умолчанию.

10. Конфигурация размера памяти, используемой для хранения таблиц на порту.

Команда	Описание
Режим конфигурирования порта	
lldp neighbors max-num *<value>* **no lldp neighbors max-num**	Конфигурация размера памяти, используемой для хранения таблиц на порту как определенной величины или значения по умолчанию.

11. Конфигурация действий при переполнении памяти для таблицы на порту.

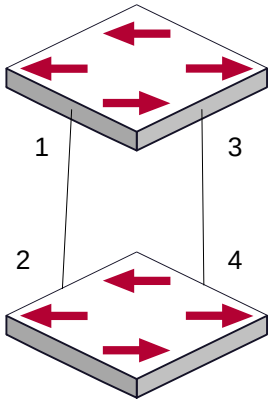
Команда	Описание
Режим конфигурирования порта	

lldp tooManyNeighbors {discard | delete}	Конфигурация действий при переполнении памяти для таблицы на порту

12. Отображение отладочной информации по функции LLDP.

Команда	Описание
Admin, Режим глобального конфигурирования	
show lldp	Отображение текущей конфигурации функции LLDP.
show lldp interface ethernet *<IFNAME>*	Отображение информации о конфигурации LLDP на конкретном порту
show lldp traffic	Отображение информации обо всех счетчиках.
show lldp neighbors interface ethernet *<IFNAME>*	Отображение информации о LLDP соседях на данном порту.
show debugging lldp	Отображение всех портов с включенной функцией отладки LLDP
Режим администратора	
debug lldp **no debug lldp**	Включение/выключение вывода отладочной иинформации LLDP.
debug lldp packets interface ethernet *<IFNAME>* **no debug lldp packets interface ethernet *<IFNAME>***	Включение/выключение вывода отладочной информации о отправке или приеме пакетов LLDP на порту или на коммутаторе.
Режим конфигурирования порта	
clear lldp remote-table	Очистка таблицы соседей на порту

4.3 Типовой пример функции LLDP



На схеме сетевой топологии, приведенной выше, порт 1,3 на коммутаторе B подключен к порту 2,4 коммутатора A. Порт 1 коммутатора B сконфигурирован в режиме приема пакетов. Опция TLV на порту 4 коммутатора A сконфигурирована как portDes и SysCap.

Коммутатор A. Последовательность команд конфигурации:

```
SwitchA(config)# lldp enable
SwitchA(config)#interface ethernet 1/0/4
SwitchA(Config-If-Ethernet1/0/4)# lldp transmit optional tlv portDesc sysCap
SwitchA(Config-If-Ethernet1/0/4)exit
```

Коммутатор B. Последовательность команд конфигурации:

```
SwitchB(config)#lldp enable
SwitchB(config)#interface ethernet1/0/1
SwitchB(Config-If-Ethernet1/0/1)# lldp mode receive
SwitchB(Config-If-Ethernet1/0/1)#exit
```

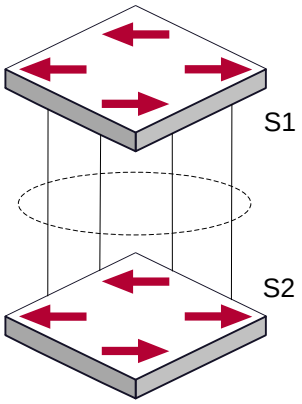
4.4 Устранение неисправностей функции LLDP

Функция LLDP по умолчанию выключена. После ее включения в режиме глобального конфигурирования, пользователи могут включить режим отладки “debug lldp” для проверки отладочной информации. Используя команду “show” функции LLDP можно вывести информацию о конфигурировании в глобальном режиме конфигурирования, либо в режиме настройки интерфейсов.

5 НАСТРОЙКА PORT CHANNEL

5.1 Общие сведения о Port channel

Для понимания термина порт-канала (Port channel) надо ввести понятие группы портов. Группа портов – это группа физических портов на конфигурационном уровне. Только физические порты в группе портов могут быть частью объединенного канала и стать членами Port channel. Логически группа портов является не портом, а набором портов. При определенных условиях физические порты в группе портов позволяют посредством объединения портов сформировать Port channel, который обладает всеми свойствами логического порта и таким образом становится независимым логическим портом. Агрегация портов — это абстрактное понятие, подразумевающее по собой объединение набора портов с одинаковыми свойствами в логический порт. Port channel — это набор физических портов, который логически используется как один физический порт. Он может использоваться пользователем как обычный порт. Он не может не только добавить пропускной способности на сеть, но и способен обеспечить резервирование соединений. Обычно объединение портов используется, когда коммутатор подключен к маршрутизатору, клиентской станции или другим коммутаторам.



Как показано выше, коммутатор S1 объединил порты в Port channel. Пропускная полоса Port channel равна сумме пропускных способностей четырех портов. Когда необходимо передать трафик с коммутатора S1 на S2, распределение трафика будет определяться на основе MAC адреса источника и младшего бита MAC адреса приемника. В результате вычислений определяется, какой порт будет передавать трафик. Если один порт в Port channel неисправен, трафик будет перераспределяться на другие порты посредством алгоритма распределения. Данный алгоритм поддерживается аппаратно.

Коммутатор предлагает два метода конфигурации объединения портов: ручное создание Port channel и динамическое посредством протокола контроля объединения соединений (Link Aggregation Control Protocol – LACP). Объединение возможно только для портов, работающих в режиме полного дуплекса.

Для правильной работы Port channel необходимо соблюдать следующие условия:

- Все порты работают в режиме полного дуплекса;
- Все порты имеют одинаковую скорость;
- Все порты являются портами доступа и принадлежат одному VLAN, или все они являются транковыми портами или они все гибридные порты.
- Если все порты являются транковыми или гибридными, тогда сконфигурированные на них допустимые VLAN и основной VLAN должны быть у всех одинаковыми.

Если Port channel сконфигурирован на коммутаторе вручную иди динамически, система автоматически назначает порт с наименьшим номером мастер-портом Port channela. Если на коммутаторе активирован протокол spanning tree, протокол построения дерева воспринимает Port channel как логический порт и посылает BPDU пакеты через мастер-порт.

Объединение портов жестко связано с аппаратной частью коммутатора. Коммутатор позволяет агрегировать соединения между любыми двумя коммутаторами. Максимально возможно создать 128 групп по 8 портов к каждой.

После того, как порты агрегированы, их можно использовать, как обычный порт. Коммутатор имеет встроенный режим конфигурирования интерфейса агрегации, пользователь может создавать соответствующую конфигурацию в этом режиме точно также, как при конфигурировании VLAN или физического интерфейса.

5.2 Общие сведения о LACP

LACP – протокол, базирующийся на стандарте IEEE 802.3ad, и реализующий механизм динамического объединения каналов. Протокол LACP использует пакеты LACPDU (Link Aggregation Control Protocol Data Unit) для обмена информацией с ответными портами.

После того, как протокол LACP включен на порту, данный порт посылает пакеты LACPDU на ответный порт соединения, уведомляя о приоритете системы, MAC адресе системы, приоритете порта, идентификаторе порта и ключе операции. Когда ответный порт получает эту информацию, она сравнивается с информацией о других портах, которые могут быть объединены. Соответственно, обе стороны соединения могут достичь соглашения о включении или исключении порта из динамической объединенной группы.

Ключ операции создается протоколом в соответствии с комбинацией параметров конфигурации (скорость, дуплекс, базовая конфигурация, ключ управления) портов, которые будут объединяться.

После включения протокола динамического объединения портов (LACP), ключ управления по умолчанию равен 0. После статического объединения портов посредством LACP, ключ управления порта такой же, как ID объединенной группы.

При динамическом объединении портов все члены одной группы имеют одинаковый ключ операции. При статическом объединении только активные порты имеют одинаковый ключ операции.

5.2.1 Статическое объединение LACP

Статическое объединение выполняется путем конфигурирования пользователем и не требует протокола LACP. При конфигурировании статического LACP объединения, используется режим «on» для включения порта в группу агрегации.

5.2.2 Динамическое объединение LACP

1. Общие положения динамического объединения LACP.

Динамическое объединение — это объединение, создаваемое/удаляемое системой автоматически. Оно не позволяет пользователям самостоятельно добавлять или удалять порты из динамического объединения LACP. Порты, которые имеют одинаковые параметры скорости и дуплекса, подключенные к одним и тем же устройствам, имеющие одинаковую конфигурацию могут быть динамически объединены в группу. В случае, если только один порт может создавать динамическое объединение, это называется однопортовым объединением. При динамическом объединении LACP протокол на порту должен быть включен.

2. Режимы портов в динамической группе объединения

В динамической группе объединения порты имеют два статуса — выбранный (selected) или «в ожидании» (standby). Оба типа портов могут посылать и принимать пакеты протокола LACP, но порты в статусе «ожидания» не могут пересылать данные.

Поскольку существует ограничение на максимальное количество портов в группе агрегации, если текущий номер порта превышает предел в группе, тогда устройство на одном конце соединения договаривается с устройством на другом конце для определения статуса порта в соответствии с идентификатором порта.

Этапы согласования следующие:

- Сравнение идентификаторов (ID) устройств (приоритет системы и MAC адрес системы). Сначала сравниваются приоритеты систем. Если они одинаковые, тогда сравниваются MAC адреса устройств. Устройство с меньшим идентификатором имеет высший приоритет.
- Затем идет сравнение идентификаторов портов (приоритет порта и идентификатор порта). Для каждого порта на стороне устройства с наивысшим приоритетом системы сначала сравниваются приоритеты портов. Если приоритеты одинаковые, тогда сравниваются идентификаторы портов. Порт с наименьшим идентификатором порта становится выбранным (selected), а остальные становятся в режим «ожидание» (standby).
- В группе объединения порт с наименьшим идентификатором и статусом «выбранный» становится мастер-портом. Другие порты со статусом «выбранный» становятся членами группы.

5.3 Настройка Port channel

1. Создание группы портов.

Команда	Описание
Режим глобального конфигурирования	
port-group <port-group-number> **no port-group <port-group-number>**	Создание или удаление группы портов.

2. Добавление портов в определенную группу.

Команда	Описание
Режим конфигурирования порта	
port-group *<port-group-number>* mode {active | passive | on} **no port-group**	Добавляет порты в группу и устанавливает их режим.

3. Вход в режим конфигурирования port-channel.

Команда	Описание
Режим глобального конфигурирования	
interface port-channel *<port-channel-number>*	Вход в режим конфигурирования port-channel.

4. Задание метода балансировки для устройства.

Команда	Описание
Режим глобального конфигурирования	
load-balance {dst-src-mac | dst-src-ip | dst-src-mac-ip}	Задание метода балансировки для устройства, изменения начинают действовать на группе портов и ECMP функции сразу.

5. Задание приоритета системы в LACP протоколе.

Команда	Описание
Режим глобального конфигурирования	
lacp system-priority <*system-priority*> **no lacp system-priority**	Задание приоритета системы в LACP протоколе, команда no возвращает значение по умолчанию.

6. Задание приоритета для конкретного порта в LACP протоколе.

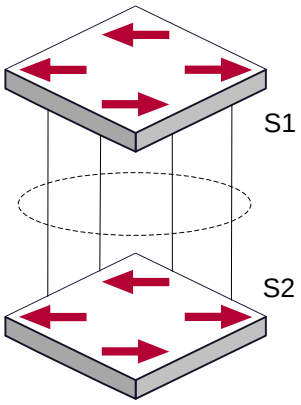
Команда	Описание
Режим конфигурирования порта	
lacp port-priority <*port-priority*> **no lacp port-priority**	Задание приоритета для конкретного порта в LACP протоколе. команда no возвращает значение по умолчанию.

7. Задание режима таймаута на порту в LACP протоколе.

Команда	Описание
Режим конфигурирования порта	
lacp timeout {short | long} **no lacp timeout**	Задание режима таймаута на порту в LACP протоколе. команда no возвращает значение по умолчанию.

5.4 Примеры использования Port channel

Вариант 1. Настройка Port channel для протокола LACP.



Имеется два коммутатора S1 и S2. Порты 1,2,3,4 на коммутаторе S1 - порты доступа и добавлены в группу1 в активном режиме. Порты 6,8,9,10 на коммутаторе S2 – тоже порты доступа и добавлены в группу 2 в пассивном режиме. Все порты соединены кабелями.

Этапы конфигурации показаны ниже:

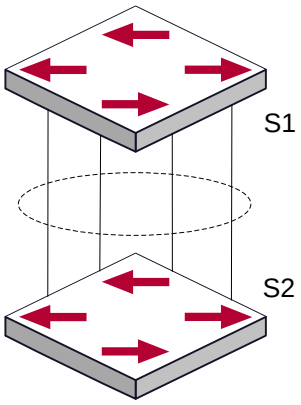
```
Switch1#config
Switch1(config)#interface ethernet 1/0/1-4
Switch1(Config-If-Port-Range)#port-group 1 mode active
Switch1(Config-If-Port-Range)#exit
Switch1(config)#interface port-channel 1
Switch1(Config-If-Port-Channel1)#

Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/0/6
Switch2(Config-If-Ethernet1/0/6)#port-group 2 mode passive
Switch2(Config-If-Ethernet1/0/6)#exit
Switch2(config)#interface ethernet 1/0/8-10
Switch2(Config-If-Port-Range)#port-group 2 mode passive
Switch2(Config-If-Port-Range)#exit
Switch2(config)#interface port-channel 2
Switch2(Config-If-Port-Channel2)#
```

Результат конфигурации:

Коммутатор сообщит, что агрегирование прошло успешно. Порты 1,2,3,4 коммутатора S1 входят в группу Port-Channel1, а порты 6,8,9,10 коммутатора S2 входят в группу Port-Channel2.

Вариант 2. Конфигурация Port channel в режиме ON.



Как показано на рисунке, порты 1,2,3,4 коммутатора S1 – порты доступа и будут добавлены в группу1 с режимом ON. Порты 6,8,9,10 коммутатора S2 – тоже порты доступа и будут добавлены в группу2 с режимом ON.

Этапы конфигурации показаны ниже:

```
Switch1#config
Switch1(config)#interface ethernet 1/0/1
Switch1(Config-If-Ethernet1/0/1)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/1)#exit
Switch1(config)#interface ethernet 1/0/2
Switch1(Config-If-Ethernet1/0/2)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/2)#exit
Switch1(config)#interface ethernet 1/0/3
Switch1(Config-If-Ethernet1/0/3)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/3)#exit
Switch1(config)#interface ethernet 1/0/4
Switch1(Config-If-Ethernet1/0/4)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/4)#exit

Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/0/6
Switch2(Config-If-Ethernet1/0/6)#port-group 2 mode on
Switch2(Config-If-Ethernet1/0/6)#exit
Switch2(config)#interface ethernet 1/0/8-10
Switch2(Config-If-Port-Range)#port-group 2 mode on
Switch2(Config-If-Port-Range)#exit
```

Результат конфигурации:

Порты 1,2,3,4 на коммутаторе S1 добавлены по порядку в группу портов 1 в режиме ON. Коммутатору на удаленном конце не требуется обмен пакетами LACP для завершения объединения. Агрегация завершается сразу, когда выполняется команда добавления

порта 2 в группу 1. Порты 1 и 2 объединяются в port channel 1. Когда порт 3 вступает в группу 1, port channel 1 из портов 1 и 2 разбирается и собирается заново с портом 3 опять в port channel 1. Когда порт 4 вступает в группу 1, port channel 1 из портов 1, 2 и 3 разбирается и собирается заново с портом 4 опять в port channel 1 (надо отметить, что каждый раз, когда новый порт вступает в группу объединения портов, группа разбирается и собирается заново). Теперь все 4 порта на обоих коммутаторах объединены в режиме “ON”.

5.5 Устранение неисправностей Port channel

Если во время конфигурации объединения портов возникли проблемы, в первую очередь проверьте следующее:

- Убедитесь, что все порты в группе имеют одинаковые настройки, например, они все в режиме полного дуплекса, имеют одинаковую скорость и настройки VLAN. Если обнаружены несоответствия, исправьте это.
- Некоторые команды не могут быть использованы на портах в port channel. Такие как arp, bandwigth, ip, ip-forward и т.д.