QTECH
МИР ДОСТУПНЕЕ

КОНФИГУРИРОВАНИЕ L3, ARP И ND

Коммутатор агрегации

СЕРИЯ QSW-8400

Оглавление

1 КОНФИГУРИРОВАНИЕ L3

Коммутатор QWS-8400 поддерживает только функцию пересылки пакетов для уровня L2, однако позволяет настроить управление портом для всех видов IP-протоколов управления на уровне L3.

1.1 Интерфейс уровня L3

1.1.1 Начальные сведения об интерфейсах 3-го уровня

В коммутаторах может быть создан интерфейс 3-го уровня. Он является не физическим интерфейсом, а виртуальным. Интерфейс 3-го уровня строится на интерфейсе VLAN. Интерфейс уровня 3 может содержать один или более интерфейсов уровня 2, принадлежащих одному и тому же VLAN, либо не содержать интерфейсов уровня 2. По крайней мере, один из интерфейсов уровня 2, содержащихся в интерфейсе уровня 3, должен быть включен (находиться в состоянии UP) — тогда будет включен и интерфейс уровня 3. В противном случае интерфейс уровня 3 будет выключен (будет находиться в состоянии DOWN). Все интерфейсы 3-го уровня коммутатора по умолчанию имеют один и тот же MAC адрес, этот адрес выбирается из зарезервированных MAC адресов при создании интерфейса 3-го уровня. Интерфейс 3-го уровня является основой для работы протоколов 3-го уровня. Коммутатор может использовать IP адреса, установленные на интерфейсах 3-го уровня, для коммуникации с другими устройствами через IP протокол. Коммутатор может пересылать IP пакеты между разными интерфейсами 3-го уровня. Loopback интерфейс принадлежит к интерфейсам 3-го уровня.

1.1.2 Настройка интерфейса 3-го уровня

1. Создание интерфейса 3-го уровня.

Команда	Описание
Режим глобального конфигурирования	
interface vlan *<vlan-id>* **no interface vlan** *<vlan-id>*	Создание VLAN интерфейса (VLAN интерфейс это интерфейс 3-го уровня); команда «no» удаляет VLAN интерфейс, созданный на коммутаторе.
interface loopback *<loopback-id>* **no interface loopback** *<loopback-id>*	Создание Loopback интерфейса и вход в режим настройки порта loopback; команда «no» удаляет Loopback интерфейс, созданный на коммутаторе.

2. Настройка описания VLAN интерфейса.

Команда	Описание
Режим конфигурирования VLAN интерфейса	
description *<text>* **no description**	Настройка описания VLAN интерфейса. Команда «no» уберет описание VLAN интерфейса.

3. Включение/выключение VLAN интерфейса.

Команда	Описание
Режим конфигурирования VLAN интерфейса	
shutdown **no shutdown**	Включает или выключает VLAN интерфейса.

1.2 Настройка протокола IP

1.2.1 Введение в IPv4, IPv6

IPv4 это текущая версия глобального универсального Интернет-протокола. Практика доказала, что IPv4 является простым, гибким, открытым, мощным, а так же легким в реализации протоколом. Он обладает хорошей совместимостью с различными протоколами верхнего и нижнего уровней. Хотя IPv4 почти не менялся с момента его появления в 80-х годах, он продолжает распространяться по всему миру вместе с распространением Интернет. Однако по мере роста инфраструктуры Интернет и услуг, использующих Интернет-приложения, выявляются и некоторые недостатки протоколаIPv4, связанные с масштабом и сложностью сегодняшней Интернет.

IPv6 — это шестая версия Интернет-протокола, следующее его поколение. IPv6 разработан IETF и должен заменить используемый в настоящее время Интернет-протокол версии4 (IPv4). IPv6 был разработан специально для того, чтобы ликвидировать нехватку адресов IPv4, препятствующую дальнейшему развитию Интернет.

Наиболее важная проблема, которая решена вIPv6 — это добавление достаточного количества IP-адресов. Запас адресов IPv4 почти исчерпан, в то время как число пользователей Интернет растет в геометрической прогрессии. Объемы предоставляемых Интернет-услуг и число прикладных устройств продолжают расти опережающими темпами (домашние и малые офисные сети, IP-телефония, терминалы беспроводного информационного обслуживания, использующие Интернет и т. д.). В результате требуется все большее количество IP-адресов, предоставлять которые становится все более затруднительно. Работа по преодолению нехватки IPv4-адресов велась долгое время;

были предложены различные технологии, позволяющие продлить срок эксплуатации существующей IPv4-инфраструктуры, в том числе трансляция сетевых адресов NAT (Network Address Translation), технология CIDR (Classless Inter-Domain Routing) и т. д.

Хотя сочетание CIDR, NAT и частных адресов временно смягчило проблемы нехватки IPv4 адресов, NAT технология разрушила модель «из конца в конец» (end-to-end), которая являлась первоначальной целью замысла IP, сделав необходимым для промежуточных маршрутизаторов поддержание статуса каждого соединения, что значительно увеличивает задержки в сети и снижает производительность сети. Кроме того, трансляция сетевых адресов пакетов данных препятствует проверке безопасности соединений «из конца в конец», заголовок аутентификации IPSec – явный пример.

Поэтому, чтобы комплексно решить все виды проблем, существующих в IPv4, следующее поколение интернет-протокола IPv6, разработанное IETF, стало единственным возможным решением в настоящее время.

Прежде всего, 128-битная схема адресации протокола IPv6 гарантированно обеспечивает достаточное число глобально уникальных IP-адресов для узлов глобальной IP-сети— и по времени, и в пространстве. Кроме увеличения адресного пространства протокол IPv6 улучшает многие другие важные аспекты IPv4.

Иерархическая схема адресации облегчает объединение маршрутов, эффективно снижает количество записей таблицы маршрутизации и улучшает эффективность маршрутизации и обработки пакетов данных.

По сравнению с IPv4, конструкция заголовка IPv6 более совершенна. Заголовок содержит меньше полей данных, из него изъята контрольная сумма, что увеличивает скорость обработки основного заголовка IPv6. В заголовке IPv6 поле фрагмента может быть показано как дополнительное расширенное поле, поэтому больше не будет необходимости в фрагментации пакетных данных в процессе их передачи в маршрутизаторе. Кроме того, эффективность работы маршрутизатора повышается за счет механизма обнаружения маршрута MTU (Path MTU Discovery Mechanism) работающего с источником пакетных данных.

Поддерживается автоматическая настройка адреса и Plug-And-Play. Большое количество хостов могут легко найти сетевые маршрутизаторы используя функцию автоматической конфигурации IPv6, автоматически получая глобально уникальные IPv6 адреса, что делает устройства, использующие протокол IPv6, устройствами Plug-And-Play. Функция автоматической настройки адреса, так же делает процесс смены адресов в существующей сети проще и удобнее, администраторам сети проще переходить от одного провайдера к другому.

Поддержка IPSec. IPSec обязателен в IPv6, в отличие от IPv4. IPv6 обеспечивает расширенный заголовок безопасности, который обеспечивает сервисы безопасности «из конца в конец», такие как контроль доступа, конфиденциальность и целостность данных, следовательно, делает проще реализацию механизмов шифрования, проверки и виртуальных частных сетей (VPN).

Улучшена поддержка мобильных IP-устройств и мобильных вычислительных устройств. Мобильный IP-протокол, определенный стандартом IETF, обеспечивает работу мобильных устройств в движении без разрыва существующего соединения. Эта сетевая функция приобретает сейчас все большую важность. В отличие от IPv4, мобильность IPv6 обеспечивается встроенным автоматическим конфигурированием для получения адреса передачи (Care-Of-Address). Поэтому при использовании IPv6 не требуется Другого Агента. Более того, при таком связывании включается Корреспондентский узел, связывающийся с Мобильным узлом напрямую. Это позволяет избежать удорожания системы из-за треугольного маршрута, требующегося при IPv4.

Удалось избежать и трансляции сетевых адресов. Целью введения NAT было использование механизма совместного и повторного использования одного и того же адресного пространства в различных сегментах сети. Этот механизм временно смягчает проблему нехватки IPv4-адресов, однако добавляются ограничения, накладываемые процессом трансляции адресов на сетевые устройства и приложения. Так как адресное пространство IPv6 значительно больше, то в трансляции адресов больше нет необходимости. В результате, проблемы с NAT и со стоимостью ее развертывания решаются естественным способом.

IPv6 сохранил и расширил поддержку существующих протоколов маршрутизации внутреннего шлюза (Internal Gateway Protocols – IGP) и протоколов внешнего шлюза (Exterior Gateway Protocols – EGP). Например, протоколы маршрутизации IPv6, такие как RIPng, OSPFv3, IS-ISv6, MBGP4+ и т.д.

Расширена поддержка Multicast и увеличено количество Multicast адресов. Работая с broadcast функциями IPv4, такими как Router Discovery and Router Query, IPv6 multicast полностью заменил IPv4 broadcast в плане функций. Multicast не только экономит пропускную способность сети, но и повышает эффективность сети в целом.

1.2.2 Настройка IP протокола

Интерфейс 3-го уровня может быть настроен как IPv4 интерфейс, либо как IPv6 интерфейс.

1.2.2.1 Настройка адреса IPv4

1. Настройка IPv4 адрес интерфейса 3-го уровня.

Команда	Описание
Режим конфигурирования VLAN интерфейса	
ip address *<ip-address> <mask>* **[secondary]** **no ip address [**<ip-address> <mask>**]**	Настройка IP адреса VLAN интерфейса; команда **no ip address [**<ip-address> <mask>**]** отменяет IP адрес VLAN интерфейса.

2. Настройка шлюза по умолчанию.

Команда	Описание
Режим глобального конфигурирования	
ip default-gateway <A.B.C.D> **no ip default-gateway <A.B.C.D>**	Настройка IP-адреса шлюза по умолчанию; **no default-gateway** отменяет настройки.

1.2.2.2 Настройка адреса IPv6

Последовательность настройки адреса IPv6:

Базовая настройка IPv6

1. Настройка адреса IPv6 интерфейса;
2. Настройка шлюза по умолчанию.

Настройка IPv6 Neighbor Discovery

1. Настройка количества сообщений DAD neighbor solicitation;
2. Настройка интервала отправки сообщений neighbor solicitation;
3. Настройка статических записей IPv6 соседей (neighbor);
4. Удаление всех записей в таблице соседей IPv6.

Настройка адреса IPv6 интерфейса

Команда	Описание
Режим конфигурирования интерфейса	
ipv6 address <ipv6-address/prefix-length> **[eui-64]** **no ipv6 address** <ipv6-address/prefix-length>	Настройка IPv6 адреса, включая объединяемые глобальные unicast адреса, site-local адреса и link-local адреса. Команда **no ipv6 address** <ipv6-address/prefix-length> отменяет IPv6 адрес.

Настройка шлюза по умолчанию

Команда	Описание
Режим глобального конфигурирования	
ipv6 default-gateway <X:X::X:X>	Настройка IP-адреса IPv6 шлюза по умолчанию; **no default-gateway**

no ipv6 default-gateway <X:X::X:X>	отменяет настройки.

Настройка количества сообщений DAD neighbor solicitation

Команда	Описание
Режим конфигурирования интерфейса	
ipv6 nd dad attempts <value> **no ipv6 nd dad attempts**	Установка количества сообщений, отправляемых последовательно при обнаружении интерфейсом дубликата адреса. Команда no восстанавливает значение по умолчанию (1).

Настройка интервала отправки сообщений neighbor solicitation

Команда	Описание
Режим конфигурирования интерфейса	
ipv6 nd ns-interval *<seconds>* **no ipv6 nd ns-interval**	Установка интервала отправки запросов соседям. Команда no восстанавливает значение по умолчанию (1 секунда).

Настройка статических записей IPv6 соседей (neighbor)

Команда	Описание
Режим конфигурирования интерфейса	
ipv6 neighbor <ipv6-address> <hardware-address> **interface** <interface-type interface-name>	Установка статической записи в таблице соседей, включая IPv6 адрес соседа, MAC адрес и порт второго уровня.
no ipv6 neighbor *<ipv6-address>*	Удаление записи в таблице соседей.

Удаление всех записей в таблице соседей IPv6

Команда	Описание

Режим администратора	
clear ipv6 neighbors	Очистка всех статических записей в таблице соседей.

1.2.3 Поиск неисправностей IPv6

Настройка времени жизни маршрутизатора не должна быть меньше интервала объявления маршрутизатора. Если подключенный PC не получил IPv6 адрес, необходимо проверить RA анонсирование на коммутаторе (выключено по умолчанию).

1.3 ARP

1.3.1 Введение в ARP

ARARP (Address Resolution Protocol - протокол определения адреса) в основном используется для определения Ethernet MAC адреса по IP адресу. Коммутатор поддерживает обе конфигурации – динамический ARP и статический ARP. Кроме того, коммутатор поддерживает настройку прокси-ARP для некоторых приложений. Например, когда на порт поступает ARP запрос на IP адрес в том же IP сегменте порта, но в другой физической сети, если на порту включена функция proxy ARP, порт будет отвечать на ARP запрос своим MAC адресом и пересылать принятые пакеты. Включение proxy ARP позволит физически разделенным машинам одного IP сегмента игнорировать физическое разделение и общаться через proxy ARP интерфейс как будто в одной физической сети.

1.3.2 Список задач конфигурации ARP

1. Настроить статический ARP.

Команда	Описание
Режим VLAN интерфейса	
arp <*ip_address*> <*mac_address*> {interface [ethernet] <portName>} **no arp <ip_address>**	Настраивает статическую запись ARP; команда no удаляет запись ARP указанного IP адреса.

2. Очистить динамический ARP.

Команда	Описание
Режим администратора	

clear arp-cache	Очистить динамические записи ARP, выученные коммутатором.

3. Сбросить статистику ARP сообщений.

Команда	Описание
Режим администратора	
clear arp traffic	Сбросить статистику ARP сообщений.

1.3.3 Поиск неисправностей ARP

Если не проходит ping от коммутатора к устройствам, подключенным напрямую, можно использовать следующие действия для поиска и устранения возможной причины:

- Проверьте, есть ли соответствующая ARP запись на коммутаторе.
- Если ARP записи нет, включите отладку ARP и посмотрите условия приема/отправки ARP пакетов.
- Самая распространенная причина проблемы – дефектный кабель.

2 НАСТРОЙКА ФУНКЦИИ ПРЕДОТВРАЩЕНИЯ ARP СКАНИРОВАНИЯ

2.1 Введение в функцию предотвращения ARP сканирования

ARP сканирование это обычный способ сетевой атаки. Для того, чтобы обнаружить все активные хосты в сегменте сети, источник атаки будет рассылать большое количество ARP сообщений, что будет занимать большую часть пропускной способности сети. Можно даже сделать атаку большим количеством трафика используя поддельные ARP сообщения, что приведет к коллапсу сети из-за исчерпания пропускной способности. Обычно ARP сканирование это просто предпосылка к другой, более опасной атаке, такой, как автоматическое заражение вирусом или последующее сканирование портов, сканирование уязвимостей, нацеленное на хищение информации, атака искаженными сообщениями, DOS атака и т.д.

Поскольку ARP сканирование угрожает безопасности и стабильности сети, очень важно его предотвратить. Коммутатор обеспечивает полное решение для предотвращения ARP сканирования: если в сегменте найден хост или порт с признаками ARP сканирования, коммутатор отрежет источник атаки для обеспечения безопасности сети.

Есть два метода предотвращения ARP сканирования: на основе порта и на основе IP. Метод на основе порта считает количество ARP сообщений, полученных с порта за определенный период, если число превышает заданный порог, порт будет выключен. Метод на основе IP считает количество ARP сообщений, полученных от IP адреса в сегменте за определенный период, если число превышает заданный порог, любой трафик от этого IP будет заблокирован до тех пор, пока порт, связанный с IP адресом, не будет погашен. Эти два метода могут быть включены одновременно. После того, как порт или IP адрес были заблокированы, пользователь может восстановить их статус, используя функцию автоматического восстановления.

Чтобы повысить эффективность, пользователи могут настроить доверенные порты и IP адреса, ARP сообщения от которых не будут проверяться коммутатором. Таким образом, нагрузка на коммутатор может быть значительно снижена.

2.2 Последовательность задач конфигурации предотвращения ARP сканирования

1. Включить функцию предотвращения ARP сканирования.

Команда	Описание
Общий режим конфигурации	
anti-arpscan enable **no anti-arpscan enable**	Включение/выключение функции предотвращения ARP сканирования.

2. Настроить пороговое значение для метода, основанного на портах и метода, основанного на IP.

Команда	Описание
Общий режим конфигурации	
anti-arpscan port-based threshold <threshold-value> **no anti-arpscan port-based threshold**	Установка порогового значения для метода, основанного на портах.
anti-arpscan ip-based threshold *<threshold-value>* **no anti-arpscan ip-based threshold**	Установка порогового значения для метода, основанного на IP.

3. Настроить доверенные порты.

Команда	Описание
Режим конфигурации порта	
anti-arpscan trust <port | supertrust-port> **no anti-arpscan trust <port | supertrust-port>**	Установка атрибутов доверия портов.

4. Настроить доверенные IP.

Команда	Описание
Общий режим конфигурации	
anti-arpscan trust ip *<ip-address>* [*<netmask>*] **no anti-arpscan trust ip *<ip-address>* [*<netmask>*]**	Установка атрибутов доверия IP.

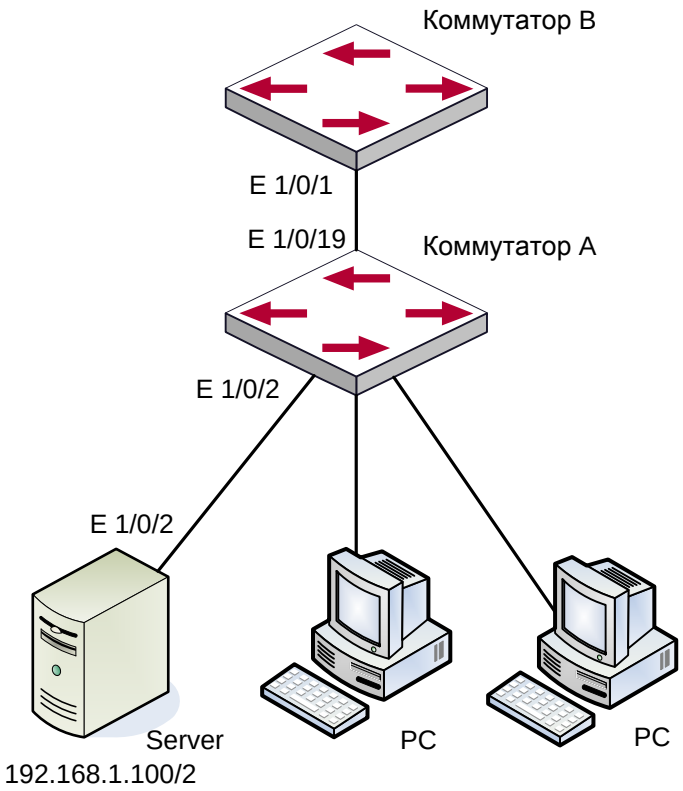
5. Настроить время автоматического восстановления.

Команда	Описание
Общий режим конфигурации	
anti-arpscan recovery enable **no anti-arpscan recovery enable**	Включение/выключение функции автоматического восстановления.
anti-arpscan recovery time *<seconds>* **no anti-arpscan recovery time**	Установка времени автоматического восстановления.

6. Посмотреть информацию, относящуюся к ARP сканированию, а также отладочную информацию.

Команда	Описание
Общий режим конфигурации	
anti-arpscan log enable **no anti-arpscan log enable**	Включение/выключение функции журнала предотвращения ARP сканирования.
anti-arpscan trap enable **no anti-arpscan trap enable**	Включение/выключение функции SNMP Trap предотвращения ARP сканирования.
show anti-arpscan [trust <ip | port | supertrust-port> | prohibited <ip | port>]	Отображение состояния работы и конфигурации предотвращения ARP сканирования.
Режим администратора	
debug anti-arpscan *<port | ip>* **no debug anti-arpscan *<port | ip>***	Включение/выключение отладки предотвращения ARP сканирования.

2.3 Типовые примеры предотвращения ARP сканирования



В сети, топология которой показана выше, порт E1/0/1 коммутатора B подключен к порту E1/0/19 коммутатора A, порт E1/0/2 коммутатора A подключен к файловому серверу (IP адрес 192.168.1.100/24), все остальные порты коммутатора A подключены к обычным PC. Следующая конфигурация может эффективно предотвратить ARP сканирование, не влияя на нормальную работу системы.

Последовательность настройки коммутатора A:

```
SwitchA(config)#anti-arpscan enable
SwitchA(config)#anti-arpscan recovery time 3600
SwitchA(config)#anti-arpscan trust ip 192.168.1.100 255.255.255.0
SwitchA(config)#interface ethernet1/0/2
SwitchA (Config-If-Ethernet1/0/2)#anti-arpscan trust port
SwitchA (Config-If-Ethernet1/0/2)#exit
SwitchA(config)#interface ethernet1/0/19
SwitchA (Config-If-Ethernet1/0/19)#anti-arpscan trust supertrust-port
Switch A(Config-If-Ethernet1/0/19)#exit
```

Последовательность настройки коммутатора B:

```
Switch B(config)# anti-arpscan enable
SwitchB(config)#interface ethernet1/0/1
SwitchB (Config-If-Ethernet 1/0/1)#anti-arpscan trust port
```

```
SwitchB (Config-If-Ethernet 1/0/1)exit
```

2.4 Поиск неисправностей предотвращения ARP сканирования

Предотвращение ARP сканирования по умолчанию выключено. После включения предотвращения ARP сканирования пользователь может включить отладку (“debug anti-arpscan”) для просмотра отладочной информации.

3 КОНФИГУРАЦИЯ ЗАЩИТЫ ОТ ПОДМЕНЫ ARP/ND

3.1 Обзор

3.1.1 ARP (Address Resolution Protocol)

В общем, протокол ARP (RFC-826), в основном, отвечает за соотношение IP адреса соответствующему 48-битному физическому адресу, то есть MAC адресу, например, IP адрес 192.168.0.1, MAC адрес сетевой карты 00-1F-CE-FD-1D-2B.

Весь процесс соотношения состоит в том, что хост отправляет широковещательный (broadcast) пакет данных, включающий в себя информацию об IP адресе хоста назначения (ARP запрос), затем хост назначения отправляет исходному хосту пакет данных, включающий в себя информацию об IP адресе и MAC адресе. Таким образом, два хоста могут обмениваться информацией по MAC адресу.

3.1.2 Подмена ARP

С точки зрения протокола ARP, чтобы уменьшить ARP трафик в сети, если хост получит ARP ответ, который он не запрашивал, он так же добавит запись в свой ARP кэш, что делает возможным подмену ARP (ARP spoofing). Если хакер хочет прослушать обмен данными между двумя хостами в одной сети (даже если они подключены через коммутаторы), он отправляет пакет ARP ответа двум хостам по отдельности, это приводит к тому, что каждый из хостов считает MAC адрес хакера адресом другого хоста. Таким образом, вместо прямого обмена, хосты обмениваются трафиком через хост хакера. Хакеры не только получают необходимую им информацию. Им для успешной передачи необходимо всего лишь изменить некоторую информацию в пакете. В этом случае на компьютере хакера не нужно настраивать смешанный режим сетевой карты, т.к. пакеты данных поступают на компьютер хакера на физическом уровне, компьютер работает как ретранслятор.

3.1.3 Как предотвратить подмену ARP/ND

Есть много видов атак, основанных на протоколе ARP,. Большинство атак основаны на подмене ARP, так что очень важно предотвратить подмену ARP.

Механизм подмены ARP проникает в сеть, в первую очередь, путем подделки легального IP адреса, затем посылая много поддельных ARP пакетов коммутаторам, после чего коммутаторы заменяют правильные связки IP-MAC соответствующими связками из атакующих пакетов. Таким образом, коммутатор ошибочно отправляет пакеты атакующему хосту, и это действует на всей сети.

Основным методом предотвращения атак и подмены ARP на коммутаторах является отключение на коммутаторе функции автоматического обновления. Обманщик не сможет изменить правильные связки IP-MAC на коммутаторе, тем самым предотвращается неправильная пересылка пакетов. В то же время это не прерывает функцию автоматического обучения ARP. Таким образом, это значительно предотвращает подмену ARP.

ND это протокол обнаружения соседей в IPv6, аналогичный протоколу ARP по принципу действия, поэтому для предотвращения подмены ND мы делаем то же самое, что и для ARP.

3.2 Конфигурация предотвращения подмены ARP, ND

1. Отключить функцию автоматического обновления ARP, ND.

Команда	Описание
Общий режим и Режим порта	
ip arp-security updateprotect **no ip arp-security updateprotect** **ipv6 nd-security updateprotect** **no ipv6 nd-security updateprotect**	Отключить/включить функцию автоматического обновления ARP, ND.

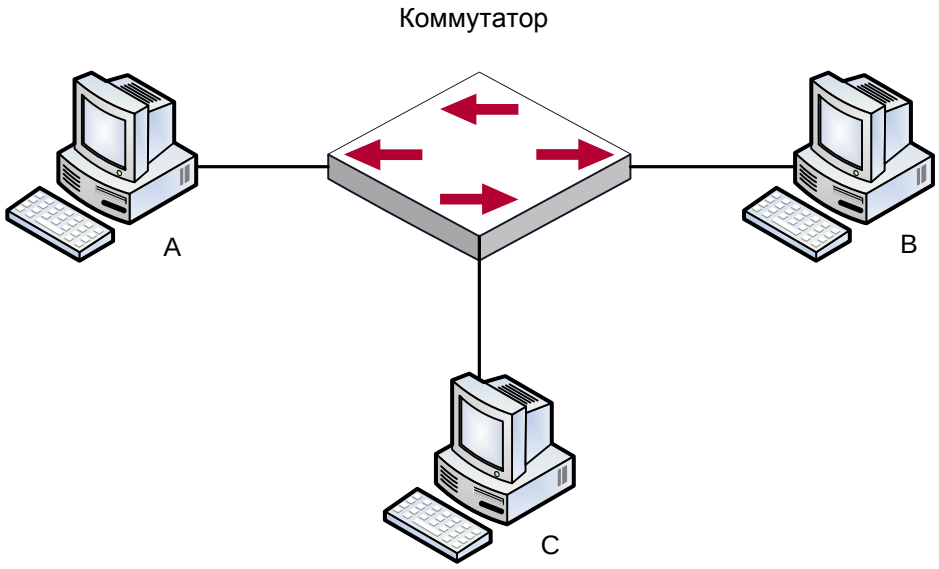
2. Отключить функцию автоматического обучения ARP, ND.

Команда	Описание
Общий режим и Режим интерфейса	
ip arp-security learnprotect **no ip arp-security learnprotect** **ipv6 nd-security learnprotect** **no ipv6 nd-security learnprotect**	Отключить/включить функцию автоматического обучения ARP, ND.

3. Поменять динамические ARP, ND на статические.

Команда	Описание
Общий режим и Режим порта	
ip arp-security convert **ipv6 nd-security convert**	Поменять динамические ARP, ND на статические.

3.3 Пример предотвращения подмены ARP, ND



Описание оборудования

Оборудование	Конфигурация	Кол-во
switch	IP:192.168.2.4; IP:192.168.1.4; mac: 00-00-00-00-00-04	1
A	IP:192.168.2.1; mac: 00-00-00-00-00-01	1
B	IP:192.168.1.2; mac: 00-00-00-00-00-02	1
C	IP:192.168.2.3; mac: 00-00-00-00-00-03	несколько

На диаграмме показана нормальная связь между B и C. Хост A хочет, чтобы коммутатор направлял ему пакеты, отправленные хостом B. В первую очередь A отправляет пакет ARP ответа на коммутатор в формате: 192.168.2.3, 00-00-00-00-00-01, сопоставляя его MAC адрес с IP адресом хоста C, коммутатор обновляет ARP список и начинает отправлять пакеты для 192.168.2.3 на MAC адрес 00-00-00-00-00-01 address (адрес хоста A).

В дальнейшем хост A пересылает принятые пакеты хосту C, меняя адрес источника и адрес назначения. Так как ARP список своевременно обновляется, еще одной задачей для хоста A является непрерывная отправка ARP ответов и обновление ARP списка коммутатора.

Поэтому очень важно защитить ARP список, настроить запрещение ARP обучения в стабильной среде и затем изменить все динамические ARP записи на статические. Выученные ARP не будут обновляться и будут защищены.

```
Switch#config
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)#arp 192.168.2.1 00-00-00-00-00-01 interface eth 1/0/2
```

```
Switch(Config-If-Vlan1)#interface vlan 2
Switch(Config-If-Vlan2)#arp  192.168.1.2  00-00-00-00-00-02  interface  eth
1/0/2
Switch(Config-If-Vlan2#interface vlan 3
Switch(Config-If-Vlan3)#arp  192.168.2.3  00-00-00-00-00-03  interface  eth
1/0/2
Switch(Config-If-Vlan3)#exit
Switch(Config)#ip arp-security learnprotect
Switch(Config)#
Switch(config)#ip arp-security convert
```

Если окружающая среда меняется, это позволяет запретить ARP обновления, как только ARP будет изучено, оно не может быть обновлено новым ARP ответом, данные будут защищены от прослушивания.

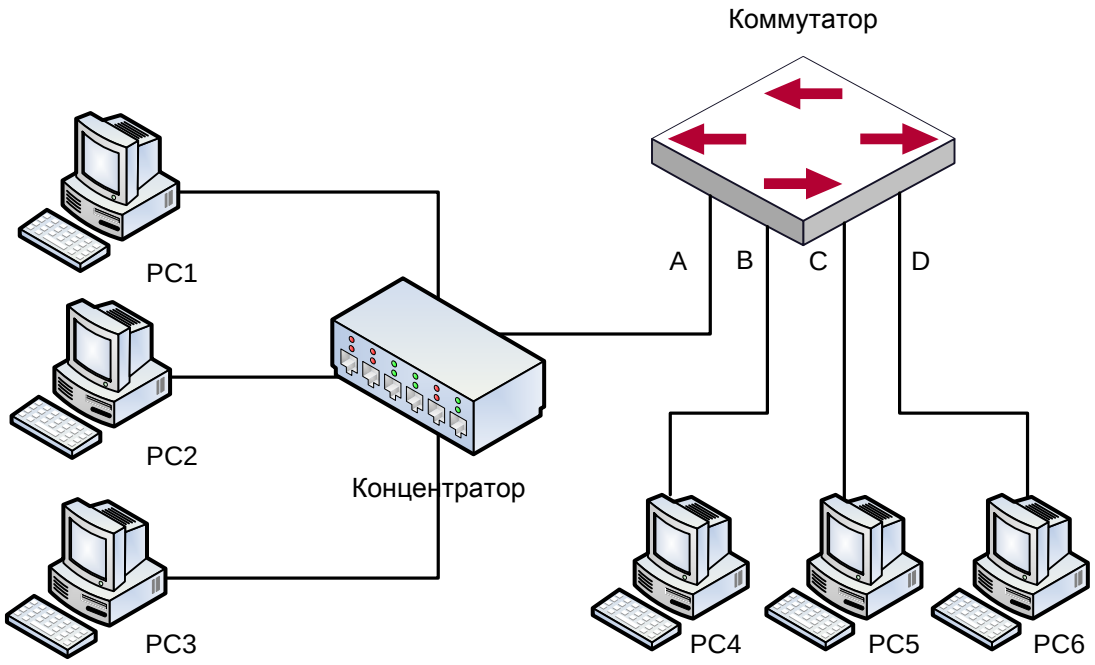
```
Switch#config
Switch(config)#ip arp-security updateprotect
```

4 НАСТРОЙКА ARP GUARD

4.1 Введение в ARP GUARD

Существует серьезная уязвимость в модели ARP протокола, которая заключается в том, что любое сетевое устройство может отправить ARP сообщение, чтобы объявить о связке IP и MAC адресов. Это делает возможным ARP мошенничество. Злоумышленники могут послать ARP запрос или ARP ответ, чтобы информировать о неверной связке между IP адресом и MAC адресом, которая приведет в проблемах связи. Есть две формы ARP мошенничества: 1. PC4 отправляет ARP сообщение, чтобы сообщить, что IP адрес PC2 привязан к MAC адресу PC4, это приведет к тому, что все IP пакеты, адресуемые PC2, будут отправлены к PC4, таким образом, PC4 сможет просматривать все пакеты, адресованные PC2; 2. PC4 отправляет ARP сообщение, чтобы сообщить, что IP адрес PC2 привязан к несуществующему MAC адресу, это приведет к тому, что PC2 не будет получать адресованные ему пакеты.

В частности, если злоумышленник, прибегая к ARP мошенничеству, выдает себя за шлюз, вся сеть выйдет из строя.



Мы используем фильтрующие элементы коммутатора для защиты ARP-записей важных сетевых устройств от подражания другими устройствами. Основной теорией этого является использование фильтрующих элементов коммутатора для проверки всех ARP сообщений, проходящих через порт. Если адрес источника ARP сообщения защищен, сообщения будут отброшены и не передадутся далее.

Функция ARP GUARD обычно используется для защиты шлюза от атак. Если все доступные компьютеры в сети будут защищены функцией ARP GUARD, для этого потребуется настроить на порту большое количество ARP GUARD адресов, что займет большую часть FFP записей в чипе, и, как результат, может отразиться на других приложениях. Так что это будет неправильно. Рекомендуется адоптировать свободные ресурсы согласно схемы доступа. Пожалуйста, обратитесь за подробностями к соответствующей документации.

4.2 Список задач конфигурации ARP GUARD

Настройка защищенных IP адресов

Команда	Описание
Режим конфигурации порта	
arp-guard ip <addr> **no arp-guard ip <addr>**	Настроить/удалить ARP GUARD адрес

5 КОНФИГУРАЦИЯ САМООБРАЩЕННОГО ARP (GRATUITOUS ARP)

5.1 Введение в самообращенный ARP

Самообращенный ARP это тип ARP запроса, отправляемый хостом и его IP адресом в качестве адреса назначения.

Базовый режим работы коммутаторов QTECH следующий: на интерфейсах 3-го уровня может быть настроен интервал рассылки самообращенных ARP запросов или это может быть настроено глобально на всех интерфейсах.

Назначение самообращенного ARP следующее:

- Чтобы уменьшить частоту ARP запросов хостов к коммутатору. Хосты в сети периодически посылают ARP запросы к шлюзу чтобы обновить MAC адрес шлюза. Если коммутатор рассылает самообращенные ARP запросы, хостам не нужно отправлять эти запросы. Это уменьшит частоту отправки хостами ARP запросов на шлюз.
- Самообращенный ARP это метод предотвращения ARP мошенничества. Рассылаемый коммутатором самообращенный ARP заставит хосты обновить свой ARP кэш.

5.2 Список задач конфигурации самообращенного ARP

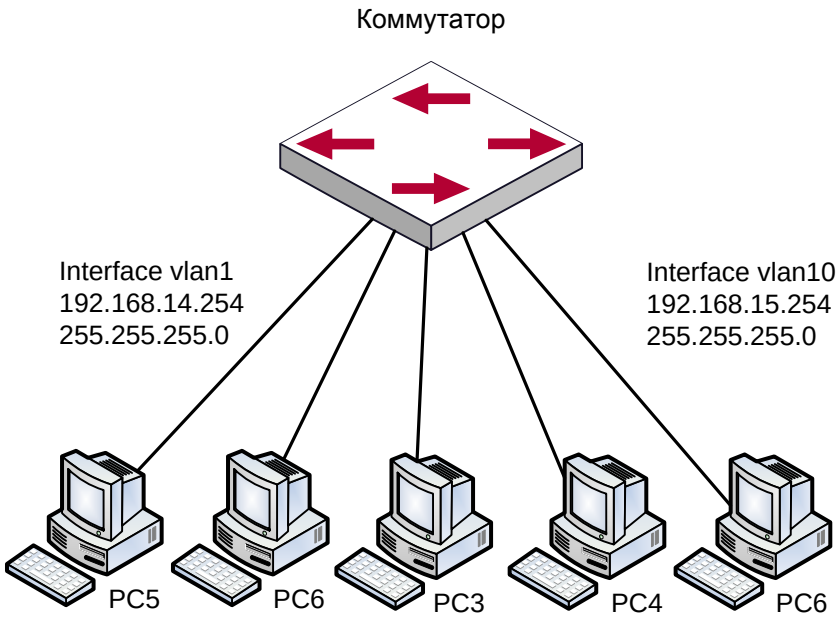
1. Включить самообращенный ARP и настроить интервал отправки ARP запросов.

Команда	Описание
Режим глобальной конфигурации и режим конфигурации интерфейса.	
ip gratuitous-arp <*5-1200*> **no ip gratuitous-arp**	Включить самообращенный ARP и настроить интервал отправки ARP запросов. Команда no отменяет самообращенный ARP.

2. Отобразить конфигурацию самообращенного ARP.

Команда	Описание
Режим администратора и режим конфигурации	
show ip gratuitous-arp [interface vlan <*1-4094*>]	Отобразить конфигурацию самообращенного ARP.

5.3 Пример конфигурации самообращенного ARP



Для топологии сети, показанной на рисунке, интерфейс коммутатора VLAN10 имеет IP адрес 192.168.15.254 и маску сети 255.255.255.0. Три компьютера – PC3, PC4, PC5 – подключены к этому интерфейсу. Интерфейс VLAN1 имеет IP адрес 192.168.14.254 и маску сети 255.255.255.0. Два компьютера – PC1 и PC2 - подключены к этому интерфейсу. Самообращенный ARP включается следующей конфигурацией:

Оба интерфейса используют самообращенный ARP.

```
Switch(config)#ip gratuitous-arp 300
Switch(config)#exit
```

Самообращенный ARP настроит только для одного интерфейса.

```
Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip gratuitous-arp 300
Switch(Config-if-Vlan10)#exit
Switch(config) #exit
```

5.4 Поиск неисправностей самообращенного ARP

Самообращенный ARP выключен по умолчанию. Когда самообращенный ARP включен, отладочную информацию можно получить, используя команду «debug ARP send».

Если самообращенный ARP включен глобально, он может быть выключен только глобально. Если самообращенный ARP включен на интерфейсе, он может быть выключен только на интерфейсе.

6 КОНФИГУРАЦИЯ ND SNOOPING

6.1 Введение в ND Snooping

Цель разработки модуля ND Snooping заключается в использовании механизма CPS (Control Packet Snooping), который используется для определения валидности доступа пакетов методом привязки IPv6-адреса источника к ключевой информации, в результате чего пропускаются промаркированные пакеты и немаркированные пакеты отбрасываются. Также механизм CPS управляет доступом по прямому подключению к узлам IPv6. Разработка требований к модулю ND Snooping относится к проекту IPv6 NDP и «Control Packet Snooping Based Binding draft-bi-savi-cps-00».

ND Snooping базируется на принципе «первый пришёл-первый обслужен» (проект «First-Come First-Serve Source-Address Validation Implementation draft-ietf-savi-fcfs-01»), что означает установку первых граничных узлов как легальных узлов, а также проверку узлов на валидность.

ND Snooping в основном применяется для устройств доступа, таких как коммутатор 2 уровня или беспроводной узел доступа. Устройство доступа создаёт таблицу информации привязок локальных узлов (к информации относятся IPv6 адрес, идентификатор порта и MAC адрес узлов) в соответствии с NDP пакетами, полученными с этих портов. Далее создаются правила FFP (Fast Filter Processor) в соответствии с информационной таблицей привязок, а также реализуется контроль доступа локальных узлов.

6.2 Основная конфигурация ND Snooping

1. Включение или отключение функции мониторинга ND Snooping.

Команда	Описание
Общий режим конфигурации	
ipv6 nd snooping enable **no ipv6 nd snooping enable**	Включение/выключение функции мониторинга ND Snooping.
Режим конфигурации порта	
ipv6 nd snooping user-control **no ipv6 nd snooping user-control**	Включение/выключение функции мониторинга ND Snooping на порту.

2. Настройка периода жизни ND Snooping.

Команда	Описание
Общий режим конфигурации	
[no] ipv6 nd snooping max-sac-lifetime <max-sac-lifetime>	Установка периода жизни в параметре **<max-sac-lifetime>** или 2 часа для SAC_BOUND
[no] ipv6 nd snooping max-dad-delay <max-dad-delay>	Установка периода жизни в параметре **<max-dad-delay>** или 1 секунда для SAC_START
[no] ipv6 nd snooping max-dad-prepare-delay <max-dad-prepare-delay>	Установка периода жизни в параметре **<max-dad-prepare-delay>** или полсекунды для SAC_QUERY

3. Функция привязки для ND Snooping.

Команда	Пояснение
Режим глобального конфигурирования	
ipv6 nd snooping policy {bind-eui64-address | bind-non-eui64-address} **no ipv6 nd snooping policy**	Настройка политики динамических привязок для адресов ND Snooping
ipv6 nd snooping static-binding <ipv6-address> hardware-address <hardware-address> interface <interface-name> **no ipv6 nd snooping static-binding <ipv6-address>**	Настройка статической привязки
ipv6 nd snooping mac-binding-limit <number> **no ipv6 nd snooping mac-binding-limit**	Установка максимального количества IPv6-адресов, которые могут быть привязаны к одному MAC-адресу

Режим конфигурации порта	
ipv6 nd snooping port-binding-limit <binding-number> **no ipv6 nd snooping port-binding-limit**	Установка количества динамических привязок для порта, номер привязки ограничивает только динамическую привязку количества портов
Режим администратора	
clear ipv6 nd snooping binding [<interface-name>]	Очистка всех статических привязок ND Snooping

4. Установка доверенного порта на коммутаторе.

Команда	**Описание**
Режим глобальной конфигурации	
ipv6 nd snooping trust **no ipv6 nd snooping trust**	Установка доверенного (безопасного) порта

6.3 Примеры ND Snooping

Типичная схема показана ниже на рисунке.

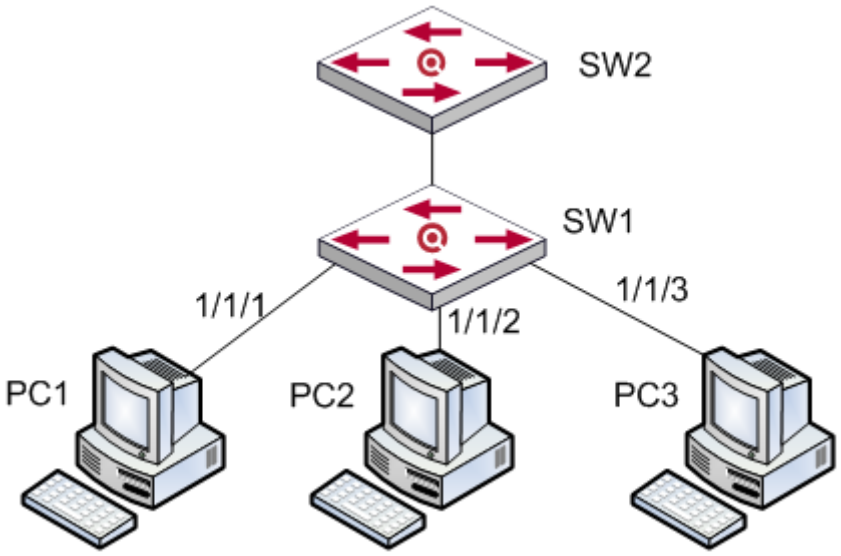


Схема конфигурации:

SW2 – это коммутатор третьего уровня, соединённый с коммутатором второго уровня SW1, функции IPv6 и RA активированы. На коммутаторе SW1 активированы функции ND Snooping и контроль ND Snooping на портах, которые соединены с тремя узловыми PC. PC1, PC2 и PC3 - три компьютера с поддержкой IPv6 и прямым соединением с коммутатором SW1, порты 1/1/1, 1/1/2, 1/1/3. PC1, PC2 и PC3 корректно получают RA пакеты от SW1. В соответствии с префиксом линка 2001::/64 RA пакетов три компьютера создают IPv6 адреса автоматически:

```
PC1: FE80::2AA:FF:FE9A:4CA2, 2001::2AA:FF:FE9A:4CA2, 2001::23:4A:1122:C411;
PC2: FE80::2BB:FF:FE9A:4CA2, 2001::2BB:FF:FE9A:4CA2, 2001::32:4B:2211:11C4;
PC3: FE80::2CC:FF:FE9A:4CA2, 2001::2CC:FF:FE9A:4CA2, 2001::22:4A:1133:C422;
```

В тоже время три PC посылают DAD (duplicate address detect) NS пакеты на локальный линк, модуль ND Snooping получает DAD NS пакеты и устанавливает соответствующую таблицу динамических привязок в соответствии с этими пакетами:

IPv6 адрес	MAC адрес	ID порта
FE80::2AA:FF:FE9A:4CA2	02-AA-00-9A-4C-A2	1/1/1
2001::2AA:FF:FE9A:4CA2	02-AA-00-9A-4C-A2	1/1/1
2001::23:4A:1122:C411	02-AA-00-9A-4C-A2	1/1/1
FE80:: BB:FF:FE9A:4CA2	02-BB-00-9A-4C-A2	1/1/2
2001::2BB:FF:FE9A:4CA2	02-BB-00-9A-4C-A2	1/1/2
2001::32:4B:2211:11C4	02-BB-00-9A-4C-A2	1/1/2
FE80:: CC:FF:FE9A:4CA2	02-CC-00-9A-4C-A2	1/1/3
2001::2CC:FF:FE9A:4CA2	02-CC-00-9A-4C-A2	1/1/3
2001::22:4A:1133:C422	02-CC-00-9A-4C-A2	1/1/3

Если три PC не получают соответствующие DAD ND пакеты в установленное время, порты 1/1/1, 1/1/2, 1/1/3 отправляют оборудованию FFP записи с привязками в соответствии с таблицей динамических привязок. После этого данные порты определяют адрес источника полученных пакетов, и при совпадении записей привязок IPv6 пакеты проходят дальше, иначе пакеты отбрасываются.

Конфигурационные шаги:

```
SW1:
SW1(config)# ipv6 nd snooping enable
SW1(config)# interface vlan 1
SW1(config-if-vlan1)# ipv6 address 2001::1/64
```

```
SW1(config)# interface ethernet 1/1/1; 1/1/2; 1/1/3
SW1(config-if-port-range)# ipv6 nd snooping user-control

SW2:
SW2(config)# interface vlan 1
SW2(config-if-vlan1)# ipv6 address 2001::2/64
SW2(config-if-vlan1)# no ipv6 nd suppress-ra
```

6.4 Поиск неисправностей ND Snooping

При возникновении проблем, связанных с функционированием ND Snooping, проверьте данные пункты:

- Проверьте, включена ли функция ND Snooping в глобальном режиме, и выполнена ли конфигурация контроля пользователей на порту.
- Используйте режим отладки ND Snooping для проверки корректности приёма и отправки связанных пакетов.
- После соединения коммутатора с PC и включения функции ND Snooping не создаются привязки кроме порта, соединённого с PC, который может быть выключен.