QTECH
МИР ДОСТУПНЕЕ

КОНФИГУРАЦИЯ DHCP

Коммутатор агрегации

СЕРИЯ QSW-8400

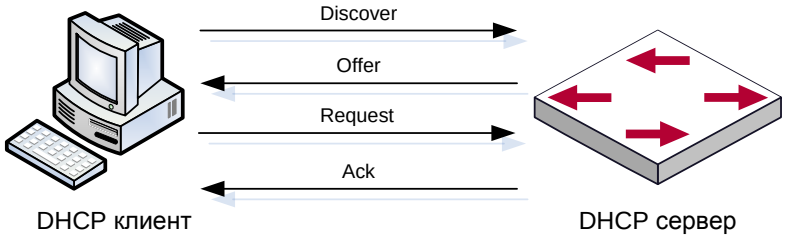
Оглавление

1 КОНФИГУРИРОВАНИЕ DHCP

1.1 Введение в DHCP

DHCP [RFC2131] сокращенно от Dynamic Host Configuration Protocol (протокол динамической настройки хостов). Это протокол, который динамически назначает IP адрес из пула адресов, так же устанавливает другие сетевые параметры, такие как шлюз по умолчанию, DNS сервер и расположение в сети файла образа. DHCP это расширенная версия BOOTP. Это основная технология, которая не только может обеспечить загрузочной информацией бездисковые рабочие станции, но так же может освободить администраторов от ручного ведения IP адресного пространства и упростить пользователям процесс настройки. Еще одно преимущество DHCP в том, что он может снизить требования к количеству IP адресов, когда пользователь покидает сеть, его IP может быть назначен другому.

DHCP является протоколом типа «клиент-сервер», DHCP клиент запрашивает у DHCP сервера сетевой адрес и параметры конфигурации, сервер предоставляет клиенту сетевой адрес и параметры конфигурации. Если клиент и сервер находятся в разных подсетях, необходимо использовать DHCP ретранслятор (relay) для передачи DHCP пакетов между клиентом и сервером. Реализация DHCP представлена ниже:



1. DHCP клиент рассылает в локальную подсеть широковещательные пакты DHCPDISCOVER.
2. DHCP сервер при получении пакета DHCPDISCOVER отправляет DHCP клиенту пакет DHCPOFFER вместе с IP адресами и другими сетевыми параметрами.
3. DHCP шлет широковещательный пакет DHCPREQUEST с информацией о DHCP сервере, который он выбрал из DHCPOFFER пакетов.
4. Выбранный клиентом DHCP сервер отправляет пакет DHCPACK и клиент получает IP адрес и другие параметры.

Эти четыре шага производят процесс динамической настройки хоста.

Однако, если DHCP сервер и DHCP клиент находятся в разных подсетях, сервер не получит широковещательные DHCP пакеты, отправленные клиентом и не ответит ему. В этом случае необходим DHCP ретранслятор (relay) для передачи таких DHCP пакетов между клиентом и сервером.

Коммутатор может работать и как DHCP сервер, и как DHCP ретранслятор. DHCP поддерживает не только динамическое назначение IP адресов, но так же ручную

привязку адреса (например, указать определенный IP адрес для определенного MAC адреса или определенного ID устройства). Различия между динамическим и статическим назначением адресов:

- Динамически получаемый адрес может быть каждый раз разным; привязанный вручную адрес всегда будет одинаковый.
- Время аренды IP адреса, полученного динамически, одинаково для всего адресного пула, и оно ограничено. Время аренды IP адреса, привязанного вручную, теоретически бесконечно.
- Динамически выделяемые адреса не могут быть привязаны вручную.
- Пул динамических адресов может наследовать параметры конфигурации сети пула динамических адресов, относящегося к сегменту.

1.2 Конфигурация DHCP сервера

1. Включить/выключить сервис DHCP.

Команда	Описание
Общий режим	
service dhcp **no service dhcp**	Включить/выключить сервис DHCP.

2. Создать/удалить адресный пул DHCP.

Команда	Описание
Общий режим	
ip dhcp pool <*name*> **no ip dhcp pool <*name*>**	Настроить адресный пул DHCP. Команда no отменяет пул адресов DHCP.

3. Настроить параметры адресного пула DHCP.

Команда	Описание
Режим адресного пула DHCP	
network-address <*network-number*> [mask | prefix-length] **no network-address**	Настройка области адресов, которые могут быть выделены адресному пулу. Команда no отменяет выделение

	адресного пула.
default-router [<address1>[<address2>[…<address8>]]] **no default-router**	Настройка шлюза по умолчанию для DHCP клиентов. Команда no отменяет шлюз по умолчанию.
dns-server [<address1>[<address2>[…<address8>]]] **no dns-server**	Настройка DNS сервера для DHCP клиентов. Команда no отменяет настройку DNS сервера.
domain-name *<domain>* **no domain-name**	Настройка доменного имени для DHCP клиентов. Команда no отменяет доменное имя.
netbios-name-server [<address1>[<address2>[…<address8>]]] **no netbios-name-server**	Настройка адреса WINS сервера. Команда no отменяет настройку.
netbios-node-type {b-node|h-node|m-node|p-node|*<type-number>*} **no netbios-node-type**	Настройка типа узла для DHCP клиентов. Команда no отменяет тип узла.
bootfile <filename> **no bootfile**	Настройка загрузочного файла для DHCP клиентов. Команда no отменяет загрузочный файл.
next-server [<address1>[<address2>[…<address8>]]] **no next-server [<address1>[<address2>[…<address8>]]]**	Настройка адреса сервера, размещающего загрузочный файл. Команда no отменяет удаляет адрес сервера.
option *<code>* {ascii *<string>* | hex *<hex>* | ipaddress *<ipaddress>*} **no option *<code>***	Настройка сетевого параметра, определенного кодом опции. Команда no удаляет сетевой параметр.
lease { days [hours][minutes] | infinite } **no lease**	Настройка времени аренды адресов пула. Команда no удаляет настройку времени аренды.
Общий режим	
ip dhcp excluded-address *<low-address>* [*<high-address>*] **no ip dhcp excluded-address *<low-address>* [*<high-address>*]**	Исключение из адресного пула адресов, которые не предназначены для динамического выделения.

4. Настроить параметры ручного адресного пула DHCP.

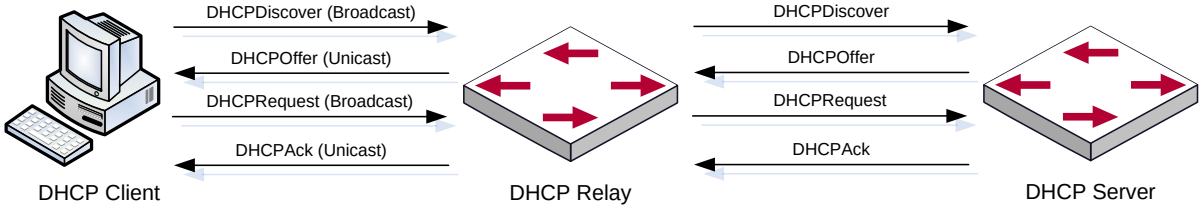
Команда	Описание
Режим адресного пула DHCP	
hardware-address *<hardware-address>* [{Ethernet | IEEE802|*<type-number>*}] **no hardware-address**	Задать/удалить аппаратный адрес, при ручном назначении адреса.
host <address> [<mask> | <prefix-length>] **no host**	Задать/удалить IP адрес, который будет назначен заданному клиенту.
client-identifier <unique-identifier> **no client-identifier**	Задать/удалить уникальный ID пользователя.

5. Включить ведение журнала для конфликтов адресов.

Команда	Описание
Общий режим	
ip dhcp conflict logging **no ip dhcp conflict logging**	Включить/выключить ведение журнала для DHCP адресов, чтобы обнаружить конфликты адресов.
Режим администратора	
clear ip dhcp conflict *<address>* / all >	Удалить единичную запись конфликта или удалить все записи.

1.3 Конфигурация DHCP ретранслятора

Когда DHCP клиент и сервер находятся в разных сегментах, для передачи DHCP пакетов необходим DHCP ретранслятор. Использование DHCP ретранслятора делает необязательным настройку DHCP сервера для каждого сегмента, один DHCP сервер может обслуживать несколько сегментов, что эффективнее не только с точки зрения затрат, но и с точки зрения управления.



Как показано на рисунке, DHCP клиент и DHCP сервер находятся в разных подсетях. DHCP клиент выполняет те же четыре шага DHCP, как обычно, только к процессу добавлен DHCP ретранслятор.

Клиент шлет широковещательный пакет DHCPDISCOVER, DHCP ретранслятор вставляет свой собственный IP адрес в поле «relay agent» в пакете DHCPDISCOVER и пересылает пакет указанному DHCP серверу (для описания формата DHCP кадра обратитесь к RFC2131).

При получении пакета DHCPDISCOVER, пересылаемого через DHCP ретранслятор, DHCP сервер шлет клиенту пакет DHCPOFFER через DHCP ретранслятор.

DHCP клиент выбирает сервер и шлет широковещательный пакет DHCPREQUEST, DHCP ретранслятор таким же образом пересылает его серверу.

При получении пакета DHCPDISCOVER, пересылаемого через DHCP ретранслятор, DHCP сервер шлет клиенту пакет DHCPACK через DHCP ретранслятор.

1. Включить DHCP ретранслятор.

Команда	Описание
Общий режим	
service dhcp **no service dhcp**	DHCP сервер и DHCP ретранслятор включаются при включении сервиса DHCP.

2. Настроить DHCP ретранслятор для пересылки широковещательных DHCP пакетов.

Команда	Описание
Общий режим	
ip forward-protocol udp bootps **no ip forward-protocol udp bootps**	Порт UDP 67 используется для пересылки широковещательных пакетов DHCP.
Режим конфигурации интерфейса	
ip helper-address ***<ipaddress>*** **no ip helper-address** ***<ipaddress>***	Установить адрес DHCP сервера. Команда **no ip helper-address <ipaddress>** отменяет настройку.

1.4 Примеры конфигурации DHCP

Сценарий 1

Чтобы упростить настройку, компания использует коммутатор в качестве DHCP сервера. Адрес в VLAN-е управления - 10.16.1.2/16. Локальная сеть разделена на две сети – A и B, в

соответствии с расположением офисов. Настройки сети для расположений A и B показаны ниже.

Пул A(сеть 10.16.1.0)		**Пул B(сеть 10.16.2.0)**	
Устройство	IP address	**Устройство**	IP address
Шлюз по умолчанию	10.16.1.200 10.16.1.201	**Шлюз по умолчанию**	10.16.1.200 10.16.1.201
DNS сервер	10.16.1.202	**DNS сервер**	10.16.1.202
WINS сервер	10.16.1.209	**WWW сервер**	10.16.1.209
Тип узла WINS	H-узел		
Время аренды	3 дня	**Время аренды**	1 день

В расположении A машине с MAC адресом 00-03-22-23-dc-ab назначен фиксированный IP адрес 10.16.1.210 и имя хоста “management”.

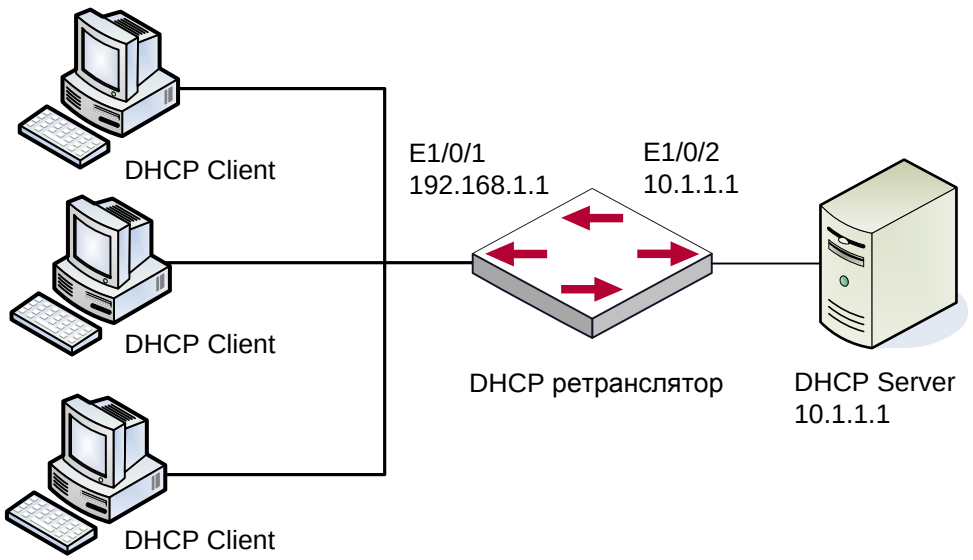
```
Switch(config)#service dhcp
Switch(config)#interface vlan 1
Switch(Config-Vlan-1)#ip address 10.16.1.2 255.255.0.0
Switch(Config-Vlan-1)#exit
Switch(config)#ip dhcp pool A
Switch(dhcp-A-config)#network 10.16.1.0 24
Switch(dhcp-A-config)#lease 3
Switch(dhcp-A-config)#default-route 10.16.1.200 10.16.1.201
Switch(dhcp-A-config)#dns-server 10.16.1.202
Switch(dhcp-A-config)#netbios-name-server 10.16.1.209
Switch(dhcp-A-config)#netbios-node-type H-node
Switch(dhcp-A-config)#exit
Switch(config)#ip dhcp excluded-address 10.16.1.200 10.16.1.201
Switch(config)#ip dhcp pool B
Switch(dhcp-B-config)#network 10.16.2.0 24
Switch(dhcp-B-config)#lease 1
Switch(dhcp-B-config)#default-route 10.16.2.200 10.16.2.201
Switch(dhcp-B-config)#dns-server 10.16.2.202
Switch(dhcp-B-config)#option 72 ip 10.16.2.209
Switch(dhcp-config)#exit
Switch(config)#ip dhcp excluded-address 10.16.2.200 10.16.2.201
Switch(config)#ip dhcp pool A1
Switch(dhcp-A1-config)#host 10.16.1.210
Switch(dhcp-A1-config)#hardware-address 00-03-22-23-dc-ab
```

```
Switch(dhcp-A1-config)#exit
```

Руководство по использованию: Когда DHCP/BOOTP клиент подключается к VLAN1 порту коммутатора, клиент может получить адрес только из сети 10.16.1.0/24 вместо 10.16.2.0/24. Это потому, что широковещательный пакет от клиента будет запрашивать IP адрес в том же сегменте VLAN интерфейса, а IP адрес VLAN интерфейса - 10.16.1.2/24, поэтому адрес, назначаемый клиенту, будет принадлежать сети 10.16.1.0/24.

Если DHCP/BOOTP клиент хочет получить адрес в сети 10.16.2.0/24, шлюз, пересылающий широковещательные пакеты клиента, должен принадлежать сети 10.16.2.0/24. Чтобы клиент получил адрес из пула 10.16.2.0/24, должна быть обеспечена связность между клиентским шлюзом и коммутатором.

Сценарий 2



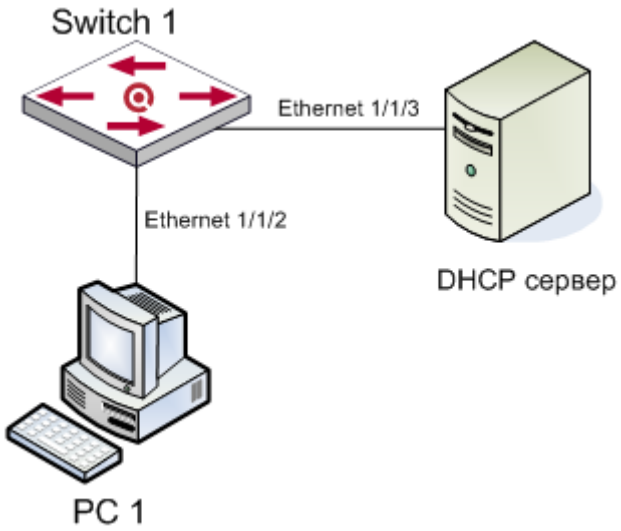
Как показано на рисунке, маршрутизирующий коммутатор настроен в качестве DHCP ретранслятора. Адрес DHCP сервера - 10.1.1.10. Шаги конфигурации следующие:

```
Switch(config)#service dhcp
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#vlan 2
Switch(Config-Vlan-2)#exit
Switch(config)#interface Ethernet 1/0/2
Switch(Config-Erthernet1/0/2)#switchport access vlan 2
Switch(Config-Erthernet1/0/2)#exit
Switch(config)#interface vlan 2
```

```
Switch(Config-if-Vlan2)#ip address 10.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(config)#ip forward-protocol udp bootps
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip help-address 10.1.1.10
Switch(Config-if-Vlan1)#exit
```

Заметка: Рекомендуется использовать комбинацию команд **ip forward-protocol udp <port>** и **ip helper-address <ipaddress>**. Команда **ip help-address** может быть настроена только на портах 3-го уровня и не может быть настроена на портах 2-го уровня.

Сценарий 3



Как показано на рисунке, PC1 является DHCP клиентом, получающим IP-адрес по DHCP. Коммутатор 1 является устройством доступа уровня 2 с поддержкой DHCP Relay и опции 82, Ethernet1/1/2 это порт доступа, принадлежащий VLAN3. Также Ethernet1/1/3 является транковым портом, соединённым с DHCP сервером с IP-адресом 192.168.40.199. Коммутатор 1 создаёт VLAN1 и VLAN2, назначает VLAN1 IP-адрес 192.168.40.50, и DHCP Relay присваивается IP-адрес 192.168.40.199, а также VLAN3 настраивается как подсеть VLAN1. Шаги конфигурации следующие:

```
switch(config)#vlan 1
switch(config)#vlan 3
switch(config)#interface ethernet 1/1/2
Switch(Config-If-Ethernet1/1/2)#switchport access vlan 3
switch(config)#interface ethernet 1/1/3
Switch(Config-If-Ethernet1/1/2)#switchport mode trunk
switch(config)#service dhcp
switch(config)#ip forward-protocol udp bootps
```

```
switch(config)#ip dhcp relay information option
switch(config)#ip dhcp relay share-vlan 1 sub-vlan 3
switch(config-if-vlan1)#ip address 192.168.40.50 255.255.255.0
switch(config-if-vlan1)#ip helper-address 192.168.40.199
```

1.5 Поиск неисправностей DHCP

Если DHCP клиенты не получают IP адреса и другие параметры сети, после проверки кабелей и клиентского оборудования, следует выполнить следующее:

1. Проверьте, запущен ли DHCP сервер, запустите его, если он не запущен. Если DHCP клиенты и серверы находятся не в одной физической сети, проверьте, имеет ли маршрутизатор, отвечающий за пересылку DHCP пакетов, функцию DHCP ретранслятора. Если на промежуточном маршрутизаторе нет функции DHCP ретранслятора, рекомендуется заменить этот роутер или обновить его ПО.
2. В таком случае, DHCP сервер должен быть проверен на предмет наличия адресного пула в том же сегменте, что и VLAN коммутатора, если такой пул не существует, его необходимо добавить.
3. Адресный пул может быть либо динамическим, либо статическим. Например, если в пуле присутствуют команды “network-address” и “host”, только одна из них вступит в силу. Кроме того, в ручной привязке только одна привязка IP-MAC может быть настроена в каждом пуле. Если необходимо несколько привязок, нужно создать отдельный адресный пул для каждой из них. Новая конфигурация в старом пуле перезапишет старую.

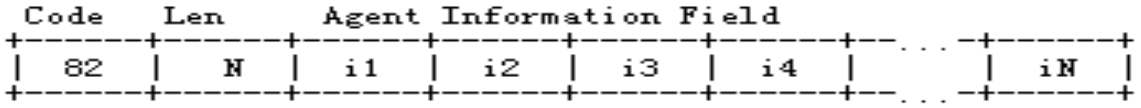
2 КОНФИГУРАЦИЯ ОПЦИИ 82 DHCP

2.1 Введение в опцию 82 DHCP

Опция 82 DHCP это опция информации ретранслирующего агента (Relay Agent). Опция 82 DHCP направлена на укрепление безопасности серверов DHCP и улучшения политики конфигурации IP адресов. Ретранслирующий агент добавляет опцию 82 (включающую физический порт доступа клиента, идентификатор устройства доступа и другую информацию) в DHCP запрос, полученный от клиента, затем пересылает его DHCP серверу. Когда DHCP сервер, который поддерживает функцию опции 82, получает сообщение, он выделяет клиенту IP адрес и другие параметры в соответствии с преднастроенными политиками и информацией в опции 82. В то же время DHCP сервер может идентифицировать все возможные атаки DHCP сообщениями в соответствии с информацией в опции 82 и защитить от них. DHCP ретранслирующий агент снимет опцию 82 с ответного сообщения и передаст его определенному порту устройства доступа, в соответствии с информацией о физическом порте в опции. Применение опции 82 DHCP прозрачно для клиента.

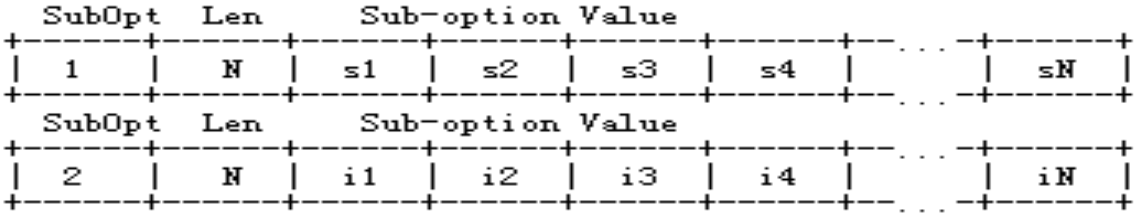
2.1.1 Структура сообщения опции 82 DHCP

Сообщение DHCP может иметь несколько сегментов опций, опция 82 один из них. Она должна быть после других опций, но до опции 255. Вот ее формат:



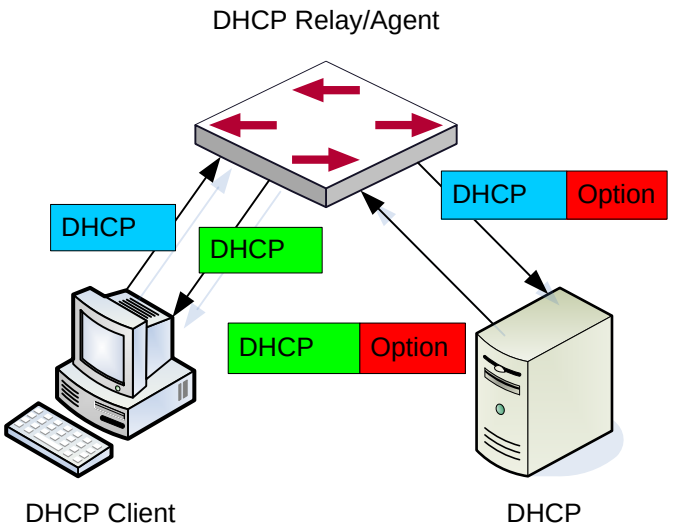
- Code: представляет порядковый номер опции информации ретранслирующего агента, опция 82 так называется потому, что RFC3046 определяет ее как 82.
- Len: количество байт в поле информации агента, не включая два байта в сегменте Code и сегменте Len.

Опция 82 может иметь несколько суб-опций, требуется как минимум одна суб-опция. RFC3046 определяет следующие две суб-опции, формат которых показан ниже:



- SubOpt: порядковый номер суб-опции, порядковый номер суб-опции Circuit-ID – 1, порядковый номер суб-опции Remote ID – 2.
- Len: количество байт в суб-опции, не включая два байта в сегменте SubOpt и сегменте Len.

2.1.2 Механизм работы опции 82



Если DHCP ретранслирующий агент поддерживает опцию 82, DHCP клиент должен пройти следующие четыре шага, чтобы получить IP адрес от DHCP сервера: discover, offer, select и acknowledge. Протокол DHCP следует приведенной ниже процедуре:

1. DHCP клиент при инициализации посылает широковещательное сообщение запроса. Это сообщение не имеет опции 82.
2. DHCP ретранслирующий агент добавит опцию 82 к сообщению запроса, которое он получит, затем перешлет это сообщение DHCP серверу. По умолчанию суб-опция 1 опции 82 (Circuit ID) это информация об интерфейсе, к которому подключен DHCP клиент (VLAN и физической порт), но пользователь может настроить Circuit ID по своему усмотрению. Суб-опция 2 опции 82 (Remote ID) это MAC адрес устройства DHCP ретранслятора.
3. После получения DHCP запроса DHCP сервер выделит клиенту IP адрес и другую информацию, в соответствии с преднастроенными политиками и информацией в опции 82. Затем он направит DHCP ретранслирующему агенту ответное сообщение с DHCP конфигурацией и опцией 82.
4. DHCP ретранслирующий агент очистит ответное сообщение от опции 82 и направит его клиенту.

2.2 Список задач конфигурации опции 82 DHCP

1. Включить опцию 82 DHCP ретранслирующего агента.

Команда	Описание
Общий режим	

ip dhcp relay information option **no ip dhcp relay information option**	Включает функции опции 82 на ретранслирующем агенте коммутатора. Команда no выключает функцию.

2. Настроить атрибуты интерфейса опции 82 DHCP.

Команда	Описание
Режим конфигурации интерфейса	
ip dhcp relay information policy {drop | keep | replace} **no ip dhcp relay information policy**	Устанавливает политики ретрансляции сообщения, которое уже содержит опцию 82. Режим drop означает, что сообщение, содержадее опцию 82, будет отброшено без какой либо обработки. Режим keep означает, что система оставит оригинальную опцию 82 и передаст сообщение серверу. Режим replace означает, что система заменит существующую опцию 82 своей и передаст сообщение серверу. Команда no установит политику в режим по умолчанию – **replace**.
Ip dhcp relay information option subscriber-id {standard | *<circuit-id>*} **no ip dhcp relay information option subscriber-id**	Устанавливает формат суб-опции 1 опции 82 (*Circuit* ID), **standard** означает стандартные названия VLAN и физического порта, например «Vlan2+Ethernet1/0/12», <**circuit-id**> это сожержание circuit-id, заданного пользователем (строка не более 64 символов). Команда no установит стандартный формат.
Общий режим	
ip dhcp relay information option remote-id {standard | *<remote-id>*} **no ip dhcp relay information option remote-id**	Устанавливает формат суб-опции 1 опции 82 (Remote ID). Команда no установит стандартный формат.

3. Включить опцию 82 DHCP сервера.

Команда	Описание
Общий режим	
ip dhcp server relay information enable **no ip dhcp server relay information enable**	Позволяет DHCP серверу коммутатора идентифицировать опцию 82. Команда no отключает эту функцию.

4. Настроить формат по умолчанию опции 82 DHCP ретранслирующего агента.

Команда	Описание
Общий режим	
ip dhcp relay information option subscriber-id format {hex | acsii | vs-hp}	Устанавливает формат subscriber-id опции 82 ретранслирующего агента.
ip dhcp relay information option remote-id format {default | vs-hp}	Устанавливает формат remote-id опции 82 ретранслирующего агента.

5. Настроить разделитель.

Команда	Описание
Общий режим	
ip dhcp relay information option delimiter [colon | dot | slash | space] **no ip dhcp relay information option delimiter**	Настраивает разделитель каждого параметра субопций в опции 82 в глобальном режиме. Команда no восстанавливает разделитель по умолчанию – **slash**.

6. Настроить метод создания опции 82.

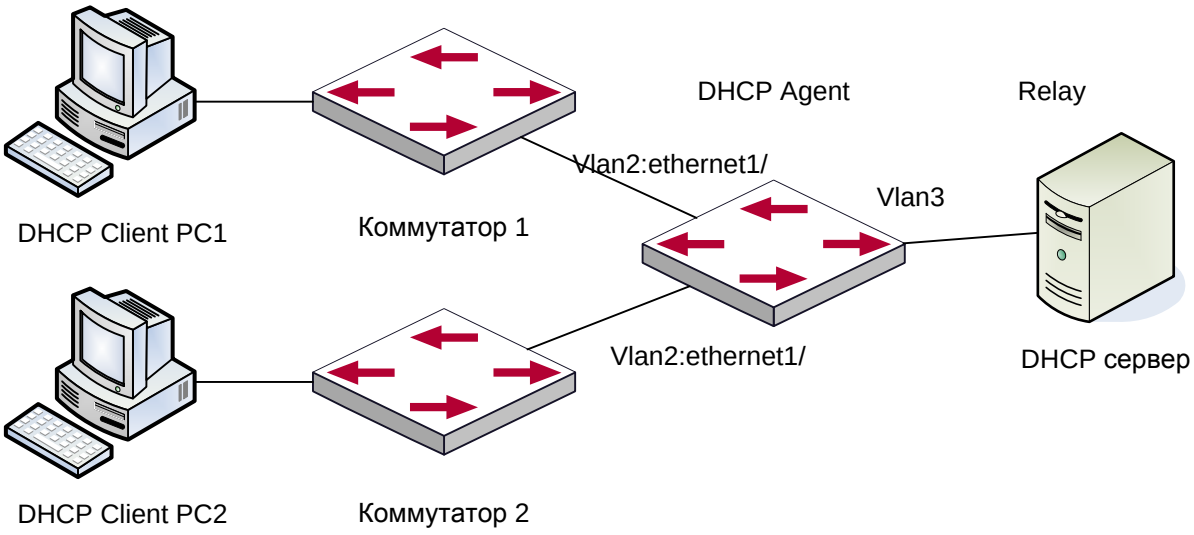
Команда	Описание
Общий режим	
ip dhcp relay information option self-defined	Устанавливает медот создания опции 82,

remote-id {hostname | mac | string WORD} **no ip dhcp relay information option self-defined remote-id**	пользователи могут самостоятельно определить параметры суб-опции remote-id.
ip dhcp relay information option self-defined remote-id format [ascii | hex]	Устанавливает пользовательский формат remote-id для опции 82.
ip dhcp relay information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac)| string WORD } **no ip dhcp relay information option self-defined subscriber-id**	Устанавливает метод создания опции 82, пользователи могут самостоятельно определить параметры суб-опции circuit -id.
ip dhcp relay information option self-defined subscriber-id format [ascii | hex]	Устанавливает пользовательский формат circuit -id для опции 82.

7. Проводить диагностику и поддержку опции 82 DHCP.

Команда	Описание
Режим администратора	
show ip dhcp relay information option	Отображает информацию о состоянии опции 82 в системе, включая все параметры настройки.
debug ip dhcp relay packet	Используется для отображения информации об обработке пакетов в DHCP ретранслирующем агенте, включая действия «добавить» и «очистить».

2.3 Примеры применения опции 82 DHCP



В данной схеме оба коммутатора второго уровня (1 и 2) подключены к коммутатору третьего уровня (3), который передает DHCP запросы от клиентов серверу. Если опция 82 выключена, DHCP сервер не сможет распознать, из какой подсети клиент, и все клиенты, подключенные к коммутаторам 1 и 2, будут получать адреса из общего адресного пула DHCP сервера. После включения опции 82, т.к. коммутатор 3 добавляет к запросу информацию о порте, сервер сможет распознать, в какой сети находится клиент (коммутатор 1 или коммутатор 2) и, таким образом, сможет выделять разное адресное пространство двум подсетям, чтобы упростить управление сетью.

Конфигурация коммутатора 3 (MAC адрес 00:1f:ce:02:33:01):

```
Switch3(Config)#service dhcp
Switch3(Config)#ip dhcp relay information option
Switch3(Config)#ip forward-protocol udp bootps
Switch3(Config)#interface vlan 3
Switch3(Config-if-vlan3)#ip address 192.168.10.222 255.255.255.0
Switch3(Config-if-vlan2)#ip address 192.168.102.2 255.255.255.0
Switch3(Config-if-vlan2)#ip helper 192.168.10.88
```

Linux ISC DHCP сервер поддерживает опцию 82, его конфигурационный файл /etc/dhcpd.conf:

```
ddns-update-style interim;
ignore client-updates;

class "Switch3Vlan2Class1" {
```

```
match if option agent.circuit-id = "Vlan2+Ethernet1/0/2" and option
agent.remote-id=00:1f:ce:02:33:01;
}

class "Switch3Vlan2Class2" {
match if option agent.circuit-id = "Vlan2+Ethernet1/0/3" and option
agent.remote-id=00:1f:ce:02:33:01;
}

subnet 192.168.102.0 netmask 255.255.255.0 {
option routers 192.168.102.2;
option subnet-mask 255.255.255.0;
option domain-name "example.com.cn";
option domain-name-servers 192.168.10.3;
authoritative;

pool {
range 192.168.102.21 192.168.102.50;
default-lease-time 86400; #24 Hours
max-lease-time 172800; #48 Hours
allow members of "Switch3Vlan2Class1";
}
pool {
range 192.168.102.51 192.168.102.80;
default-lease-time 43200; #12 Hours
max-lease-time 86400; #24 Hours
allow members of "Switch3Vlan2Class2";
}
}
```

Теперь DHCP сервер будет выделять адреса для узлов с коммутатора 2 из диапазона 192.168.102.21 ~ 192.168.102.50, а для коммутатора 1 из диапазона 192.168.102.51 ~ 192.168.102.80.

2.4 Поиск неисправностей опции 82 DHCP

- Опция 82 DHCP реализована как подфункция модуля DHCP ретранслятора. Прежде, чем ее использовать, необходимо убедиться, что DHCP ретранслирующий агент настроен правильно.
- Опция 82 требует взаимодействия DHCP ретранслятора и DHCP сервера. DHCP сервер должен установить политику выделения адресов основываясь на сетевой топологии DHCP ретранслятора, но, даже если ретранслятор работает нормально,

выделение адресов может не получиться. Если в сети больше одного ретранслятора, уделите внимание политике передачи DHCP запросов.

- При реализации функции опции 82 DHCP ретранслятора, подробная информация о процессе работы функции опции 82 DHCP ретранслятора может быть получена командой «debug ip dhcp relay packet». Эта информация может помочь в поиске неисправностей.
- При реализации функции опции 82 DHCP севера, подробная информация о процессе работы функции опции 82 DHCP сервера может быть получена командой «debug ip dhcp server packet». Эта информация может помочь в поиске неисправностей.

3 КОНФИГУРАЦИЯ DHCP SNOOPING

3.1 Введение в DHCP Snooping

DHCP Snooping означает, что коммутатор наблюдает за процессом присвоения IP адресов по протоколу DHCP. Это предотвращает появление нелегальных DHCP серверов и DHCP атаки путем настройки доверенных и недоверенных портов. DHCP сообщение с доверенных портов передается без проверки. При типичной конфигурации доверенные порты используются для подключения DHCP сервера или DHCP ретранслятора, а к недоверенным портам подключаются клиенты. С недоверенных портов коммутатор будет пересылать только DHCP запросы, но не ответы. Если с недоверенного порта получено сообщение DHCP ответа, коммутатор поднимет тревогу и предпримет определенные действия с портом, согласно настройкам, например выключение или создание «черной дыры».

Если включена привязка DHCP Snooping, коммутатор сохранит в соответствующей таблице связующую информацию о каждом DHCP клиенте с недоверенного порта (включая MAC адрес, IP адрес, аренду IP, номера VLAN и порта). Имея такую информацию DHCP Snooping можно комбинировать с другими модулями, такими, как dot1x и ARP, или самостоятельно реализовать контроль доступа пользователей.

Защита от поддельного DHCP сервера: если коммутатор перехватывает ответ DHCP сервера (включая DHCPOFFER, DHCPACK и DHCPNAK), он поднимет тревогу и предпримет определенные действия, согласно настройкам (выключение порта или создание «черной дыры»).

Защита от перегрузки DHCP: Чтобы избежать большого количества сообщений DHCP, атакующих процессор, пользователь может ограничить скорость получения DHCP пакетов на доверенных и недоверенных портах.

Запись связующих данных DHCP: DHCP Snooping при пересылке DHCP пакетов будет записывать связующие данные, выделенные DHCP сервером. Можно так же загрузить эти данные на сервер в целях восстановления утерянной информации. Связующие данные, в основном, используются для настройки динамических пользовательских портов dot1x. За подробной информацией о dot1x обратитесь, пожалуйста, к главе «Настройка dot1x».

Добавление связующего ARP: можно добавить статическую связку ARP в соответствии с динамическими данными, чтобы предотвратить ARP мошенничество.

Добавление доверенных пользователей: можно добавить записи в список доверенных пользователей в соответствии с параметрами связующих данных; эти пользователи получат доступ ко всем ресурсам без dot1x аутентификации.

Автоматическое восстановление: через некоторое время после выключения порта или создания «черной дыры», нужно автоматически убрать блокировку порта или MAC адреса и отправить при этом информацию на сервер через syslog.

Функция журнала: Когда коммутатор обнаруживает ненормальные пакеты, он должен отправить информацию на сервер журнала через syslog.

Шифрование приватных сообщений: связь между коммутатором и внутренней системой управления безопасностью сети TrustView происходит через приватные сообщения. Пользователи могут шифровать эти сообщения в версии 2.

Функция добавление опции 82: различные опции 82 добавляются в DHCP сообщение в соответствии со статусом аутентификации пользователя.

3.2 Последовательность задач конфигурации DHCP Snooping

1. Включить DHCP Snooping.

Команда	Описание
Глобальный режим	
ip dhcp snooping enable **no ip dhcp snooping enable**	Включить/выключить DHCP Snooping.

2. Включить функцию привязки DHCP Snooping.

Команда	Описание
Глобальный режим	
ip dhcp snooping binding enable **no ip dhcp snooping binding enable**	Включить/выключить функцию привязки DHCP Snooping.

3. Включить функцию привязки ARP DHCP Snooping.

Команда	Описание
Глобальный режим	
ip dhcp snooping binding arp **no ip dhcp snooping binding arp**	Включить/выключить функцию привязки ARP DHCP Snooping .

4. Включить функцию опции 82 DHCP Snooping.

Команда	Описание
Глобальный режим	
ip dhcp snooping information enable **no ip dhcp snooping information enable**	Включить/выключить функцию опции 82 DHCP Snooping.

5. Установить версию приватных пакетов.

Команда	Описание
Глобальный режим	
ip user private packet version two **no ip user private packet version two**	Настроить/удалить версию приватных пакетов.

6. Установить зашифрованный ключ DES для приватных пакетов.

Команда	Описание
Глобальный режим	
enable trustview key 0/7 <*password*> **no enable trustview key**	Настроить/удалить зашифрованный ключ DES для приватных пакетов.

7. Установить адрес DHCP сервера.

Команда	Описание
Глобальный режим	
ip user helper-address A.B.C.D [port <udpport>] source <ipAddr> (secondary|) **no ip user helper-address (secondary|)**	Настроить/удалить адрес DHCP сервера.

8. Настроить доверенные порты.

Команда	Описание
Режим порта	
ip dhcp snooping trust **no ip dhcp snooping trust**	Сделать порт доверенным. Команда no отменяет настройку.

9. Включить функцию привязки DHCP Snooping DOT1X.

Команда	Описание
Режим порта	
ip dhcp snooping binding dot1x **no ip dhcp snooping binding dot1x**	Включить/выключить функцию привязки DHCP Snooping DOT1X .

10. Включить функцию привязки DHCP Snooping USER.

Команда	Описание
Режим порта	
ip dhcp snooping binding user-control **no ip dhcp snooping binding user-control**	Включить/выключить функцию привязки DHCP Snooping USER .

11. Добавить записи в статический список.

Команда	Описание
Глобальный режим	
ip dhcp snooping binding user *<mac>* address *<ipAddr>* *<mask>* vlan *<vid>* interface (ethernet|) *<ifname>* **no ip dhcp snooping binding user *<mac>* interface (ethernet|) *<ifname>***	Добавить/удалить записи в статический список.

12. Установить действия защиты.

Команда	Описание
Режим порта	
ip dhcp snooping action {shutdown|blackhole} [recovery <*second*>] **no ip dhcp snooping action**	Установить/отменить автоматические защитные действия на портах.

13. Установить ограничение скорости передачи DHCP сообщений.

Команда	Описание
Глобальный режим	
ip dhcp snooping limit-rate <*pps*> **no ip dhcp snooping limit-rate**	Установить ограничение скорости передачи DHCP сообщений.

14. Включить отладку.

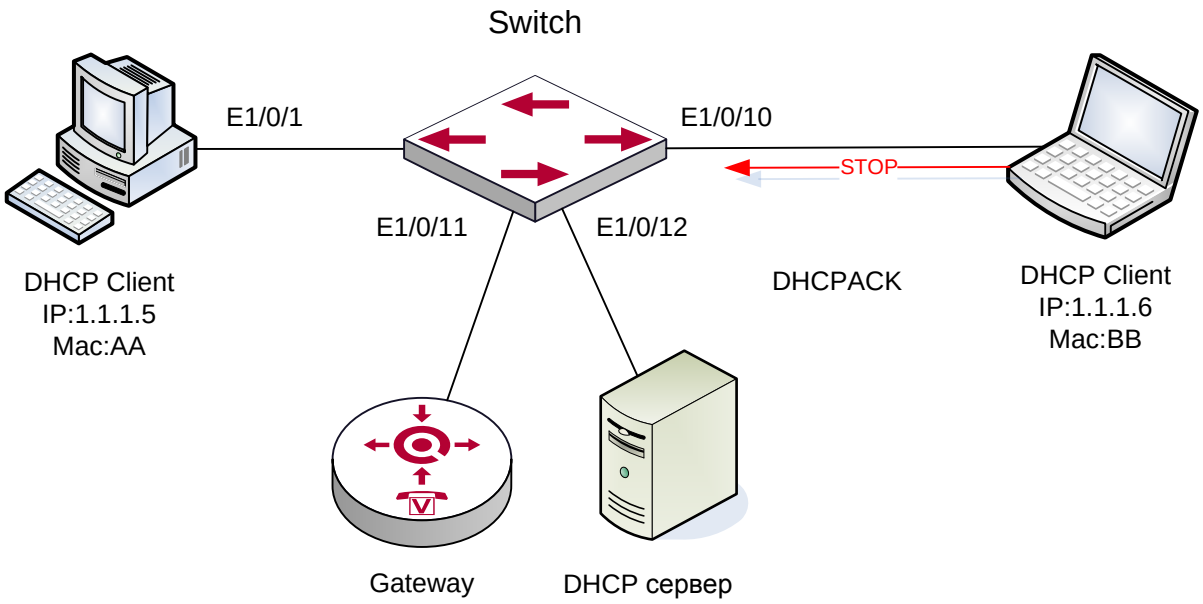
Команда	Описание
Режим администратора	
debug ip dhcp snooping packet **debug ip dhcp snooping event** **debug ip dhcp snooping update** **debug ip dhcp snooping binding**	Пожалуйста, обратитесь к соответствующей главе поиска неисправностей.

15. Настроить атрибуты опции 82 DHCP Snooping.

Команда	Описание
Глобальный режим	

ip dhcp snooping information option subscriber-id format {hex | acsii | vs-hp}	Устанавливает формат subscriber-id опции 82 DHCP snooping.
ip dhcp snooping information option remote-id {standard | *<remote-id>*} **no ip dhcp snooping information option remote-id**	Устанавливает содержание суб-опции remote-id опции 82. Команда no возвращает стандартный формат.
ip dhcp snooping information option allow-untrusted **no ip dhcp snooping information option allow-untrusted**	Разрешает недоверенным портам принимать DHCP пакеты с опцией 82. Если не включено, все недоверенные порты будут отбрасывать DHCP пакеты с опцией 82.
ip dhcp snooping information option delimiter [colon | dot | slash | space] **no ip dhcp snooping information option delimiter**	Устанавливает разделитель для параметров суб-опций опции 82. Команда no устанавливает разделитель по умолчанию – slash.
ip dhcp snooping information option self-defined remote-id {hostname | mac | string WORD} **no ip dhcp snooping information option self-defined remote-id**	Задает метод создания опции 82, пользователи могут самостоятельно определить параметры суб-опции remote-id.
ip dhcp snooping information option self-defined remote-id format [ascii | hex]	Пользовательский формат remote-id для опции 82.
ip dhcp snooping information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac) | string WORD} **no ip dhcp snooping information option type self-defined subscriber-id**	Задает метод создания опции 82, пользователи могут самостоятельно определить параметры суб-опции circute-id.
ip dhcp snooping information option self-defined subscriber-id format [ascii | hex]	Пользовательский формат circuit-id для опции 82.
Режим порта	
ip dhcp snooping information option subscriber-id {standard | <*circuit-id*>} **no ip dhcp snooping information option subscriber-id**	Устанавливает содержание суб-опции circuit-id опции 82. Команда no возвращает стандартный формат.

3.3 Типовое применение DHCP Snooping



Как показано на рисунке, устройство Mac-AA – обычный пользователь, подключенный к недоверенному порту 1/0/1 коммутатора, получает IP настройки через DHCP, IP адрес клиента 1.1.1.5. DHCP сервер и шлюз подключены к доверенным портам коммутатора, 1/0/11 и 1/0/12 соответственно. Злоумышленник Mac-BB, подключенный к недоверенному порту 1/0/1 коммутатора, пытается подделать DHCP сервер (посылая пакеты DHCPACK). Функция DHCP Snooping на коммутаторе эффективно обнаружит и блокирует такой тип сетевой атаки.

Последовательность настройки:

```
switch#
switch#config
switch(config)#ip dhcp snooping enable
switch(config)#interface ethernet 1/0/11
switch(Config-If-Ethernet1/0/11)#ip dhcp snooping trust
switch(Config-If-Ethernet1/0/11)#exit
switch(config)#interface ethernet 1/0/12
switch(Config-If-Ethernet1/0/12)#ip dhcp snooping trust
switch(Config-If-Ethernet1/0/12)#exit
switch(config)#interface ethernet 1/0/1-10
switch(Config-Port-Range)#ip dhcp snooping action shutdown
switch(Config-Port-Range)#
```

3.4 Поиск неисправностей DHCP Snooping

3.4.1 Наблюдение и отладочная информация

Команда “debug ip dhcp snooping” может быть использована для получения отладочной информации.

3.4.2 Помощь в поиске неисправностей

Если возникает проблема с использованием функции DHCP Snooping, пожалуйста, проверьте следующее:

Включена ли функция DHCP Snooping глобально;

Если порт не реагирует на ложный DHCP пакет, проверьте, настроен ли этот порт как недоверенный.

4 КОНФИГУРАЦИЯ DHCPV6 SNOOPING

4.1 Введение DHCPv6 Snooping

Функция DHCPv6 Snooping отслеживает взаимодействие пакетов в потоке между клиентом и сервером DHCPv6 и создаёт таблицу привязок для применения политик безопасности, основанных на этой таблице.

Защита от поддельного DHCPv6 сервера: DHCPv6 Snooping устанавливает порт соединения с DHCPv6 сервером как доверенный порт, другие порты по умолчанию устанавливаются как недоверенные (ненадёжные). Это помогает избегать конфигурации DHCPv6 сервера в частном порядке в сети. DHCP Snooping не пересылает ответные пакеты на DHCPv6, которые были получены с ненадёжных портов, и в соответствии с MAC адресом источника полученных от DHCPv6 ответных пакетов применяются политики безопасности.

Защита от поддельного IPv6 адреса: DHCPv6 Snooping может посылать контрольный лист записей, основанный на привязках на порту. Порт отбрасывает IPv6 трафик по умолчанию, пропуская лишь переадресованные пакеты с устройства, IPv6 и MAC адрес которого определяются портом как параметры источника. Это позволяет эффективно предотвращать несанкционированный доступ при помощи поддельного IPv6 адреса.

Защита от атак с целью исчерпания лимита DHCPv6 адресов: DHCPv6 Snooping может ограничить число привязок на порт. Порт, число привязок на который превысило лимит, отбрасывает DHCPv6 пакеты, что предотвращает исчерпание лимита DHCPv6 адресов.

Защита от ND Cheat: IPv6 адрес, полученный по протоколу DHCPv6, может быть надёжным в сети IPv6, поэтому DHCPv6 Snooping преобразовывать записи о привязках в статические и эффективно предотвращать несанкционированные ND-атаки на шлюз. Функция привязки ND к DHCPv6 Snooping должна быть активирована на устройстве 3 уровня.

Ответ на удаление требований для порта: Через захват портов, через которые проходят пакеты DHCPv6, функция DHCPv6 Snooping оценивает порт, соединённый с DHCPv6 пользователем. После создания привязки DHCPv6 Snooping, если DHCPv6 Snooping получает CONFIRM/REQUEST пакеты и ответные пакеты от DHCPv6 клиентов других портов, необходимо использовать функцию DAD NS/NA для обнаружения привязки оригинальных портов, которые можно использовать. Если такие находятся (при этом получается ответ DAD NS/NA), то новые привязки не создаются на новых портах, в противном случае (ответ DAD NS/NA не получен) создаются новые привязки на новых портах и удаляются старые на оригинальных портах.

4.2 Конфигурация DHCPv6 Snooping

1. Включить/выключить функцию DHCPv6 Snooping.

Команда	Описание
Общий режим	
ipv6 dhcp snooping enable **no ipv6 dhcp snooping enable**	Включить/выключить функцию DHCPv6 Snooping.

2. Включить/выключить функцию привязок DHCPv6 Snooping.

Команда	Описание
Общий режим	
ipv6 dhcp snooping binding enable **no ipv6 dhcp snooping binding enable**	Включить/выключить функцию привязок DHCPv6 Snooping.

3. Включить/выключить функцию привязок ND.

Команда	Описание
Общий режим	
ipv6 dhcp snooping binding nd **no ipv6 dhcp snooping binding nd**	Включить/выключить функцию привязок ND.

4. Удалить информацию о динамических привязках для DHCPv6 Snooping.

Команда	Описание
Общий режим	
clear ipv6 dhcp snooping binding {<MAC> | <ipv6address> | interface {ethernet <IFNAME> | port-channel <IFNAME> | <IFNAME>} | all}	Удалить информацию о динамических привязках для DHCPv6 Snooping.

5. Установить ограничение на количество привязок на порту.

Команда	Описание
Режим конфигурации порта	
ipv6 dhcp snooping binding-limit <max-num> **no ipv6 dhcp snooping binding-limit**	Установить или удалить лимит количества динамических DHCPv6 Snooping привязок на порту

6. Настроить список статических привязок.

Команда	Описание
Общий режим	
ipv6 dhcp snooping binding user <MAC-address> address <ipv6-address> vlan <vid> interface [ethernet | port-channel] <ifname> **no ipv6 dhcp snooping binding user <MAC-address>**	Настроить или удалить текущий список статических привязок.

7. Установить надёжные порты.

Команда	Описание
Режим конфигурации порта	
ipv6 dhcp snooping trust **no ipv6 dhcp snooping trust**	Уставить или удалить DHCPv6 Snooping атрибут надёжного порта.

8. Установить функции защиты.

Команда	Описание
Режим конфигурации порта	
ipv6 dhcp snooping action {shutdown | blackhole} [recovery <second>] **no ipv6 dhcp snooping action**	Уставить или удалить автоматические защитные действия функции DHCPv6 Snooping для портов.

9. Установить максимальное количество Blackhole MAC.

Команда	Описание
Общий режим	
ipv6 dhcp snooping action {<max-num> | default}	Установить максимальное количество Blackhole MAC, которое может быть послано с каждого ненадёжного порта.

10. Активировать функцию контроля доступа пользователей.

Команда	Описание
Режим конфигурации порта	
ipv6 dhcp snooping binding user-control **no ipv6 dhcp snooping binding user-control**	Активировать или деактивировать функцию контроля доступа пользователей, связанную с DHCPv6 Snooping.

11. Включить режим отладки.

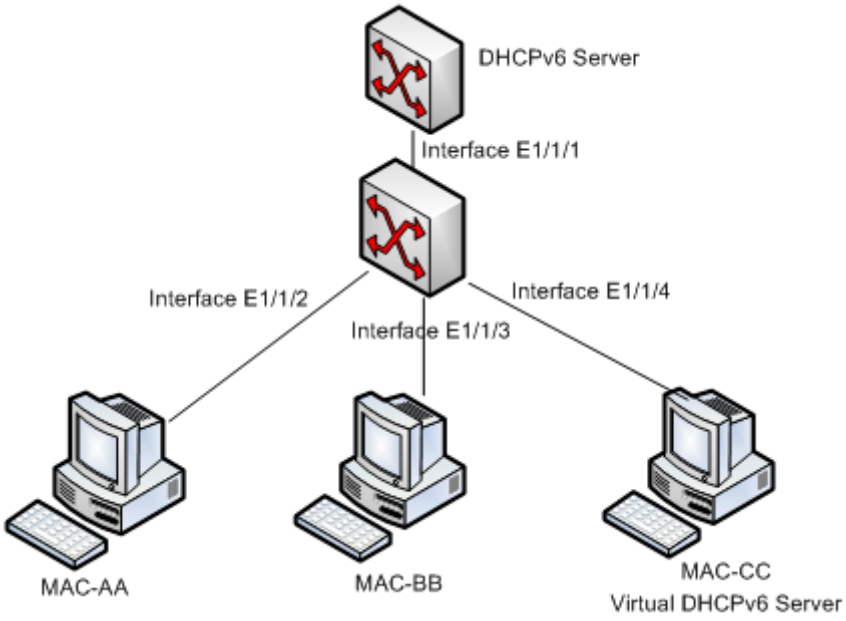
Команда	Описание
Режим администратора	
debug ipv6 dhcp snooping packet **debug ipv6 dhcp snooping event** **debug ipv6 dhcp snooping binding**	Включить режим отладки DHCPv6 Snooping.

12. Отобразить конфигурационный статус.

Команда	Описание
Режим администратора	
show ipv6 dhcp snooping interface [ethernet | port-channel] <ifname> **show ipv6 dhcp snooping binding {<MAC> | <ipv6address> | interface [ethernet | port-**	Отобразить конфигурационный статус DHCPv6 Snooping и информации о привязках.

channel] <ifname> | all}	

4.3 Примеры конфигурации DHCPv6 Snooping



Как показано на схеме выше, MAC-AA и MAC-BB устройства принадлежат к обычным пользователям, подключённым через ненадёжные порты коммутатора 1/1/2 и 1/1/3 и получающим IPv6 адрес 2010::3 and IP 2010::4 через DHCPv6 клиента. DHCPv6 сервер подключён к коммутатору через надёжный порт 1/1/1, далее осуществляется несанкционированный доступ с устройства MAC-CC, подключённого через ненадёжный порт 1/1/4. С данного устройства пытаются фальсифицировать DHCPv6 сервер. Активация и настройка функции DHCPv6 Snooping позволяет эффективно засечь и предотвратить такие действия.

Последовательность конфигурации:

```
switch#
switch#config
switch(config)#ipv6 dhcp snooping enable
switch(config)#ipv6 dhcp snooping binding enable
switch(config)#interface ethernet 1/1/1
switch(Config-Ethernet 1/1/1)#ipv6 dhcp snooping trust
switch(Config-Ethernet1/1/1)#exit
switch(config)#interface ethernet 1/1/4;1/2/1-4;1/3/1-2
switch(Config-Port-Range)#ipv6 dhcp snooping action shutdown
switch(Config-Port-Range)#
```

4.4 Поиск неисправностей DHCPv6 Snooping

Для включения режима отладки DHCPv6 Snooping используется команда **debug ipv6 dhcp snooping**.

При возникающих проблемах с работой функции DHCPv6 Snooping проверьте следующие пункты:

- Проверьте, активирована ли функция DHCPv6 Snooping в режиме глобального конфигурирования (общий режим).
- Если DHCP клиент не получает IP-адрес во время конфигурирования DHCPv6 Snooping, проверьте чтобы порт, соединённый с DHCPv6 сервером или ретранслятором, имел статус надёжного.
- Функция DHCPv6 Snooping взаимно исключает одновременную работу с функциями IPv6 ACL и QoS для IPv6 ACL.