**DHCP snooping**

DHCP snooping — функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP. Например, атаки с подменой DHCP-сервера в сети или атаки DHCP starvation, которая заставляет DHCP-сервер выдать все существующие на сервере адреса злоумышленнику.

DHCP snooping регулирует только сообщения DHCP и не может повлиять напрямую на трафик пользователей или другие протоколы. Некоторые функции коммутаторов, не имеющие непосредственного отношения к DHCP, могут выполнять проверки на основании таблицы привязок DHCP snooping (DHCP snooping binding database). В их числе:

* Dynamic ARP Protection (Inspection) — проверка ARP-пакетов, направленная на борьбу с ARP-spoofing,
* IP Source Guard — выполняет проверку IP-адреса отправителя в IP-пакетах, предназначенная для борьбы с IP-spoofingом.

DHCP snooping позволяет:

* защитить клиентов в сети от получения адреса от неавторизованного DHCP-сервера,
* регулировать какие сообщения протокола DHCP отбрасывать, какие перенаправлять и на какие порты.

Для правильной работы DHCP snooping, необходимо указать какие порты коммутатора будут доверенными (trusted), а какие — нет (untrusted, в дальнейшем — ненадёжными):

* Ненадёжные (Untrusted) — порты, к которым подключены клиенты. DHCP-ответы, приходящие с этих портов отбрасываются коммутатором. Для ненадёжных портов выполняется ряд проверок сообщений DHCP и создаётся база данных привязки DHCP (DHCP snooping binding database).
* Доверенные (Trusted) — порты коммутатора, к которым подключен другой коммутатор или DHCP-сервер. DHCP-пакеты полученные с доверенных портов не отбрасываются.

**Принципы работы DHCP snooping**

По умолчанию коммутатор отбрасывает DHCP-пакет, который пришел на ненадёжный порт, если:

* Приходит одно из сообщений, которые отправляет DHCP-сервер (DHCPOFFER, DHCPACK, DHCPNAK или DHCPLEASEQUERY);
* Приходит сообщение DHCPRELEASE или DHCPDECLINE, в котором содержится MAC-адрес из базы данных привязки DHCP, но информация об интерфейсе в таблице не совпадает с интерфейсом, на котором был получен пакет;
* В пришедшем DHCP-пакете не совпадают MAC-адрес указанный в DHCP-запросе и MAC-адрес отправителя;
* Приходит DHCP-пакет, в котором есть опция 82.

**Использование опции 82**

По умолчанию коммутатор на котором включен DHCP snooping, вставляет опцию 82 в DHCP-запросы. Коммутатор может изменять или вставлять опцию 82, даже если клиент и сервер находятся в одной подсети.

При вставке опции 82, коммутатор фактически вставляет два значения:

* Remote ID (MAC-адрес или IP-адрес коммутатора). Это значение можно настраивать;
* Circuit ID (порт с которого пришел запрос). Это значение не настраивается.

По умолчанию коммутатор, использующий DHCP snooping, обнаруживает и отбрасывает любой DHCP-запрос, содержащий опцию 82, который он получил через ненадёжный порт.

Этот режим стоит оставить, если коммутатор соединен с конечными клиентами. Получение запроса с опцией 82 от клиента будет говорит об атаке, которую коммутатор должен предотвратить.

Но если функция DHCP snooping включена на нескольких коммутаторах, которые соединены последовательно, то такое поведение по умолчанию, приведет к тому, что клиенты не смогут получить адрес по DHCP (если сервер находится через несколько коммутаторов).