Как уже было описано выше, DHCP обеспечивает раздачу IP-адресов устройствам. Он довольно часто используется в современных сетях. DHCP — протокол прикладного уровня модели TCP/IP. В целом, IP-адреса можно задавать вручную, но на сегодняшний день локальные сети имеют довольно большое количество хостов, что затрудняет ручную настройку. Процесс взаимодействия основан на передаче сообщений. Устройство, в котором настроено автоматическое получение IP-адреса, отправляет широковещательное сообщение DHCPDISCOVER. В сообщении указывается исходный IP-адрес 0.0.0.0, и адрес доставки 255.255.255.255. DHCP-сервер принимает запрос, и резервирует адрес. Здесь необходимо пояснить, что DHCP-сервер представляет собой маршрутизатор или коммутатор.

Далее сервер отправляет клиенту сообщение DHCPOFFER. В свою очередь клиент формирует широковещательный запрос DHCPREQUEST, в котором указан IP-адрес сервера, который выдал предложение. Это означает что клиент принял отправленные настройки. Теперь сервер отправляет сообщение DHCPACK, это своего рода подтверждение от сервера начала авторизации клиента и принятие параметров конфигурации. После того как клиент получил необходимые параметры, процесс можно считать завершенным. Это было четыре основных вида сообщений.

Также необходимо рассмотреть два следующих вида. Первый, это DHCPNACK, оно отправляется клиенту для того, чтобы уведомить его об отказе аренды IP-адреса. Второй, DHCPRELEASE, используется клиентом для информирования о том, что он больше не будет использовать IP-адрес. После получения данного запроса, сервер возвращает адрес в список свободных адресов.

# 5.2 Атаки DHCP STARVATION и Rogue DHCP

Одной из популярных атак на DHCP-серверы является DHCP STARVATION. Ее суть заключается в атаке сервера отправкой ложных пакетов типа DHCPDISCOVER со случайными MAC-адресами. Так как DHCP-сервер ведет определенную таблицу с информацией о выданных клиентам IP-адресам и соответствующим MAC-адресам, он будет резервировать новые адреса и записывать к себе в таблицу. В результате через некоторое время произойдет переполнение стека, и сервер не сможет выдавать IP-адреса.

Приведем пример. Допустим есть определенная сеть с адресом 192.168.1.0, в ней DHCP-сервер зарезервировал адреса в диапазоне 192.168.1.2–254. Если будет запущена атака DHCP STARVATION, со временем все эти адреса из диапазона попадут в таблицу DHCP и не смогут быть выданы. Это будет продолжаться пока ведется атака. Такая атака может привести к отказу в обслуживании DHCP-сервера.

Второй тип атак называется Rogue DHCP и заключается в развертывании поддельного DHCP-сервера. Это необходимо для того, чтобы начать выдавать клиентам ложные сетевые параметры. ель этой атаки — заставить клиентов использовать ложную службу доменных имен (DNS), а также использовать узел или устройство злоумышленника в качестве шлюза по умолчанию. Как правило, перед проведением этой атаки, злоумышленник организовывает отказ в обслуживании легитимного сервера, что, собственно, и было описано выше.

# 5.3 Настройка доверенных и недоверенных портов

Теперь рассмотрим способы защиты от рассмотренных атак. Для того чтобы не допустить появление поддельного DHCP-сервера, необходимо использовать концепцию доверенных и недоверенных портов (DHCP Snooping). DHCP Snooping - это функция безопасности коммутатора, обеспечивающая получение DHCP клиентом IP-адреса только от легитимного DHCP сервера. Доверенный порт разрешает пересылать сообщения DHCP от сервера [4]. В таком случае поддельный сервер не сможет довести до клиента ложные параметры, так как клиент будет находиться за ненадежным портом.

Под доверенными портами понимают порты, которые напрямую подключены к серверу или «направлены» в его сторону [5]. Соответственно все остальные порты будут считаться недоверенными.

Как только будет включен DHCP Snooping, все порты по умолчанию станут недоверенными. Доверенный порт же указывается явно [6]. При этом использование доверенных портов никак не влияет отправку DHCP-запросов, они так же приходят и на легальный, и на поддельный серверы, однако ответы серверов будут проходить лишь через доверенные порты.

**5.4** **Настройка ограничения на отправку DHCP-сообщений и проверки MAC-адресов**

Довольно важной функцией DHCP Snooping является ограничение на отправку сообщений DHCP (Rate Limit). Данная функция ограничивает количество сообщений, проходящих через порт коммутатора в секунду. Компания Cisco рекомендует ставить значение не более 100 пакетов в секунду. Ограничение на отправку сообщений полезно тем, что не дает нарушителю выполнить атаку отказ в обслуживании или же быстро опустошить список зарезервированных адресов.

При включении DHCP Snooping автоматически включается функция ––––проверки MAC-адреса по умолчанию (Verify MAC-Address). Дело в том, что в заголовке запроса DHCP в поле CHADDR передается MAC-адрес устройства. Также его можно увидеть в заголовке пакета Ethernet. Если все функционирует нормально, эти значения в полях совпадают. При включении этой функции, коммутатор начинает проверять эти два значения, если они не совпадают, процесс прерывается.

Вычислительный процесс проверки MAC-адресов ресурсоемкий, и может нагружать центральный процессор маршрутизатора [3]. В случае нормального функционирования нагрузка не возникает. Однако, если злоумышленник запустит программу, которая будет генерировать огромное количество DHCP запросов, производительность сильно упадет, так как каждый пакет будет проверяться на соответствие MAC-адресов. Для того, чтоб таких ситуаций не возникало, данную функцию используют в комбинации с ограничением количества сообщений.

# 5.5 Конфигурация Port Security

Еще одной немаловажной функцией защиты коммутатора можно выделить Port Security. Она не входит в состав технологии DHCP Snooping. Port Security позволяет выбрать MAC-адреса хостов, которые могут передавать данные через порт [4]. Функция используется для предотвращения:

* подмены MAC-адреса сетевого устройства или подключения к сети;
* атак, направленных на переполнение таблицы коммутации.

В случае включения данной функции порт не передает пакеты, если MAC-адрес отправителя не указан как разрешенный. Кроме того, можно указывать не конкретные MAC-адреса, разрешенные на порту коммутатора, а ограничить количество MAC-адресов, которым разрешено передавать трафик через порт.

Нарушением безопасности для Port Security считаются ситуации:

* максимальное количество безопасных MAC-адресов было добавлено в таблицу адресов и хост, чей MAC-адрес не записан в таблице адресов пытается получить доступ через интерфейс;
* адрес, выученный или настроенный как безопасный на одном интерфейсе, появился на другом безопасном интерфейсе в том же VLAN'е.

На интерфейсе может быть выбран один из следующих режимов реагирования на нарушение:

none — случай при котором количество безопасных MAC-адресов достигает максимального значения, указанного на порту, пакеты с неизвестным MAC-адресом отправителя отклоняются до тех пор, пока не будет удалено достаточное количество безопасных MAC-адресов, чтобы их количество было меньше максимального значения, или увеличено максимальное количество разрешенных адресов. Оповещения о нарушении безопасности нет.

send-alarm — Режим, при котором количество безопасных MAC-адресов достигает максимального ограничения, указанного на порту, пакеты с неизвестным MAC-адресом отправителя отклоняются до тех пор, пока не будет удалено достаточное количество безопасных MAC-адресов, чтобы их количество было меньше максимального значения, или увеличено максимальное количество разрешенных адресов. Данный режим при нарушении безопасности посылает уведомление через протокол SNMP и добавляет запись в системный лог.

send-disable — в случае нарушения безопасности интерфейс переключается в заблокированное состояние и выключается немедленно. Здесь так же отправляются SNMP trap и формируется запись в системный лог. Когда порт в заблокированном состоянии — вывести его из этого состояния можно, введя команду *port-security <port-id> clear-intrusion-flag*, и затем вручную включить интерфейс, введя в режиме настройки интерфейса *enable*.