Доклад

Настройка сетевых сервисов на сетевом оборудовании. DHCP. Безопасность DHCP (option 82).

Демидова Екатерина Алексеевна

Содержание

Список иллюстраций

1 Цель работы

Рассмотреть принципы работы DHCP, его настройку на сетевом оборудовании и обеспечение безопасности.

2 Задачи

- Рассмотреть принцип работы DHCP
- Рассмотреть способы обеспечения безопаснти DHCP
- Привести практический пример настройки DHCP

3 Теоретические сведения

3.1 Понятие протокола DHCP

Для нормальной работы сети каждому сетевому интерфейсу компьютера и маршрутизатора должен быть назначен IP-адрес[1]. Процедура присвоения адресов происходит в ходе конфигурирования компьютеров и маршрутизаторов. При конфигурировании назначается не только IP-адрес, но маска подсети, IP-адрес машрутизатора по умолчанию, IP-адреса DNS-сервера, доменное имя и другие параметры стека TCP-IP. Поэтому вручную эта процедура представляет собой для администратора утомительную процедуру.

Протокол динамической конфигурации хоста (Dynamic Host Configuration Protocol, DHCP)[2] – автоматизирует процесс конфигурирования сетевых интерфейсов, обеспечивая отсутствие дублирования адресов за счет централизованного управления их распределением.

3.2 Режимы DHCP

Протокол DHCP работает в соответствии с моделью клиент-сервер. Во время старта си стемы компьютер, являющийся DHCP-клиентом, посылает в сеть широковещательный запрос на получение IP-адреса. DHCP-сервер откликается и посылает сообщение-ответ, содержащее IP-адрес и некоторые другие конфигурационные параметры.

При этом сервер DHCP может работать в разных режимах, включая:

- ручное назначение статических адресов;
- автоматическое назначение статических адресов;
- автоматическое распределение динамических адресов.

Во всех режимах работы администратор при конфигурировании DHCP-сервера сообщает ему один или несколько диапазонов IP-адресов, причем все эти адреса относятся к одной сети, то есть имеют одно и то же значение в поле номера сети.

В ручном режиме администратор, помимо пула доступных адресов, снабжает DHCP- сервер информацией о жестком соответствии IP-адресов физическим адресам или другим идентификаторам клиентских узлов. DHCP-сервер, пользуясь этой информацией, всегда выдаст определенному DHCP-клиенту один и тот же назначенный ему администратором IP-адрес (а также набор других конфигурационных параметров).

В режиме автоматического назначения статических адресов DHCP-сервер самостоятельно без вмешательства администратора произвольным образом выбирает клиенту IP-адрес из пула наличных IP-адресов. Адрес дается клиенту из пула в постоянное пользование, то есть между идентифицирующей информацией клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первого назначения DHCP-сервером IP-адреса клиенту. При всех последующих запросах сервер возвращает клиенту тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, называемое сроком аренды. Когда компьютер, являющийся DHCP- клиентом, удаляется из подсети, назначенный ему IP-адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес. Ни пользователь, ни сетевой администратор не вмешиваются в этот процесс. Это дает возможность впоследствии повторно использовать этот IP-адрес для назначения другому компьютеру.

3.3 Принцип работы DHCP

Получение адреса проходит в четыре шага. Этот процесс называют DORA по первым буквам каждого шага: Discovery, Offer, Request, Acknowledgement(рис. [3.1]):

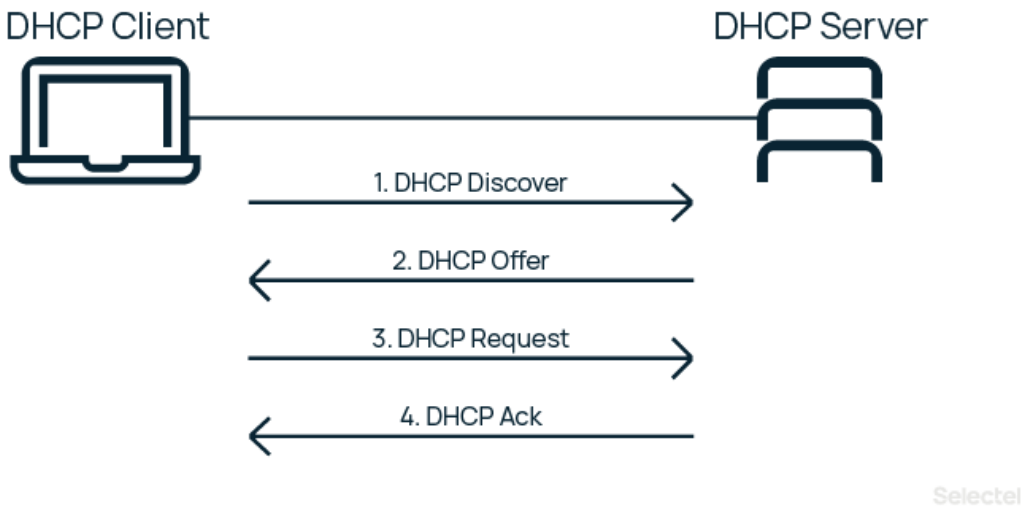

Рис. 3.1: Принцип работы DHCP

Каждая сеть должна иметь DHCP-сервер, отвечающий за настройки. Также могут существовать DHCP-агенты, которые играют роль посредников между клиентами и серверами. Таким образом один DHCP-сервер может обслуживать клиентов нескольких разных сетей.

Рассмотрим этот алгоритм[3]:

- Для отыскания своего IP-адреса компьютер широковещательным способом распространяет специальный пакет DHCPDISCOVER. Он должен прибыть на DHCP-сервер. Сервер всегда слушает 67 порт, ожидает широковещательное сообщение от клиента, а после его получения отправляет ответное предложение — DHCPOFFER. Клиент принимает сообщение на 68 порту.

- Когда сервер получает пакет, он выделяет свободный IP-адрес и отправляет его обратно с помощью пакета DHCPOFFER (который также может ретранслироваться). Чтобы это было возможным, даже если у хоста нет IP-адреса, сервер определяет хост по его Ethernet-адресу (который содержится в пакете DHCPDISCOVER).

IP выделяются из области (SCOPE) доступных адресов, которая задается администратором.

Если имеются адреса, которые не должны быть назначены DHCP-сервером, область можно ограничить, указав только разрешенные адреса. Например, администратор может задать диапазон используемых IP-адресов от 192.0.0.10 до 192.0.0.254.

Бывает и так, что не все доступные адреса должны быть назначены клиентам. Например, администратор может исключить (exclude) диапазон 192.0.0.100 - 192.0.0.200 из используемой области. Такое ограничение называется исключением.

- Клиент получает DHCPOFFER, а затем отправляет на сервер сообщение DHCPREQUEST. Этим сообщением он принимает предлагаемый адрес и уведомляет DHCP-сервер об этом. Широковещательное сообщение почти полностью дублирует DHCPDISCOVER, но содержит в себе уникальный IP, выделенный сервером. Таким образом, клиент сообщает всем доступным DHCP-серверам «да, я беру этот адрес», а сервера помечают IP как занятый.

- Сервер получает от клиента DHCPREQUEST и окончательно подтверждает передачу IP-адреса клиенту сообщением DHCPACK. Это широковещательное или прямое сообщение утверждает не только владельца IP, но и срок, в течение которого клиент может использовать этот адрес.

3.4 Безопасность DHCP

DHCP Starvation

Эта атака основана на проведении рассылок огромного количества сообщений DHCPDISCOVER с целью истощить адресное пространство на сервере DHCP. Сервер DHCP будет реагировать на каждый запрос и выдавать IP-адрес. После переполнения допустимого адресного пространства сервер DHCP больше не сможет обслуживать новых клиентов в своей сети, выдавая им IP-адреса.

DHCP Spoofing

Эта атака основана на подмене настоящего DHCP-сервера сервером хакера. Когда поддельный DHCP-сервер выдает IP-адреса хостам в сети, он передает и информация о том, что его IP-адрес является шлюзом по умолчанию.

DHCP Snooping – это функция безопасности коммутатора, обеспечивающая получение DHCP клиентом IP-адреса только от легитимного DHCP сервера.

При настройке DHCP Snooping порт, к которому подключен легитимный DHCP сервер, назначаются в качестве доверенного (trusted). Обычно это транзитные uplink порты коммутатора. Все прочие порты считаются недоверенными (обычно это клиентские Ethernet порты коммутатора).

При получении DHCP запросов от клиентского оборудования коммутатор отправляет их только в сторону доверенного порта. При этом коммутатор блокирует DHCP ответы от “нелегальных” DHCP серверов, подключенных к недоверенным портам, препятствуя тем самым получению сетевых настроек от недоверенного DHCP сервера.

Еще одна очень полезная функция DHCP Snooping – ограничение на отправку DHCP-сообщений. Это ограничение допускает отправку через порт коммутатора определенного количества DHCP-трафика в секунду.

3.4.1 Опция 82

Опция 82 протокола DHCP используется для того, чтобы проинформировать DHCP-сервер о том, от какого DHCP-ретранслятора и через какой его порт был получен запрос. Коммутатор с функцией DHCP-snooping добавляет опцию в DHCP-запросы от клиента и передает их серверу. DHCP-сервер, в свою очередь, предоставляет IP-адрес и другую конфигурационную информацию в соответствии с преднастроенными политиками на основании информации, полученной в заголовке опции 82. Коммутатор снимет заголовок опции с принятого от DHCP-сервера сообщения и передаст сообщение клиенту в соответствии с информацией о физическом интерфейсе, указанной в опции. Применение опции 82 прозрачно для клиента(рис. [3.2]).

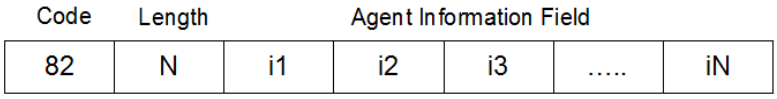

Рис. 3.2: Формат опции Relay Agent Information

4 Практический пример

Создадим сеть для демонстрации настройки dhcp.

Расположим в сети один маршрутизатор, к нему подключим сервер и коммутатор, а к коммутатору еще один сервер и два компьютера(рис. [4.1]).

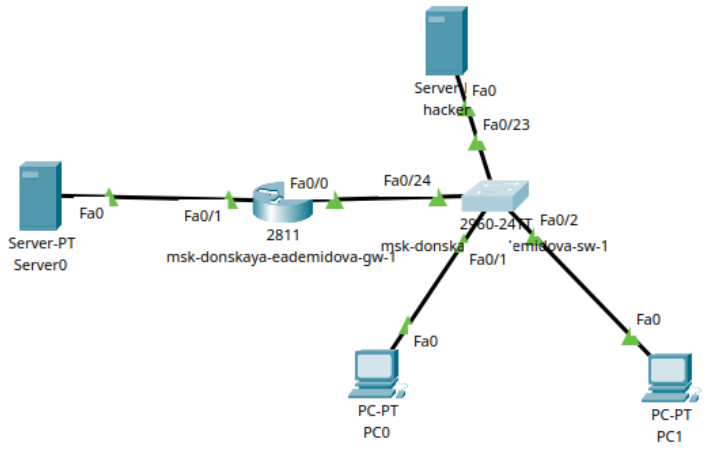

Рис. 4.1: Схема сети

Маршрутизатор сделаем dhcp-сервером и зададим два пула для сетей 10.128.0.0 и 10.128.1.1(рис. [4.2]).

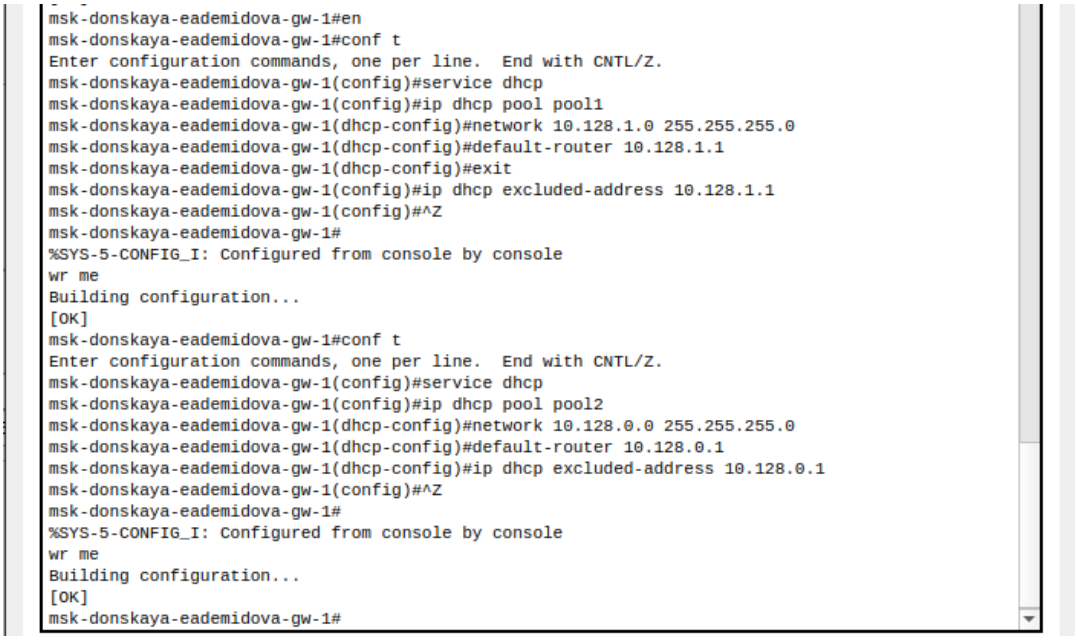

Рис. 4.2: Настройка dhcp-сервера

Можно увидеть, что автоматически выдаются адреса из разных пулов для сервера и ПК(рис. [4.3], [4.4]).

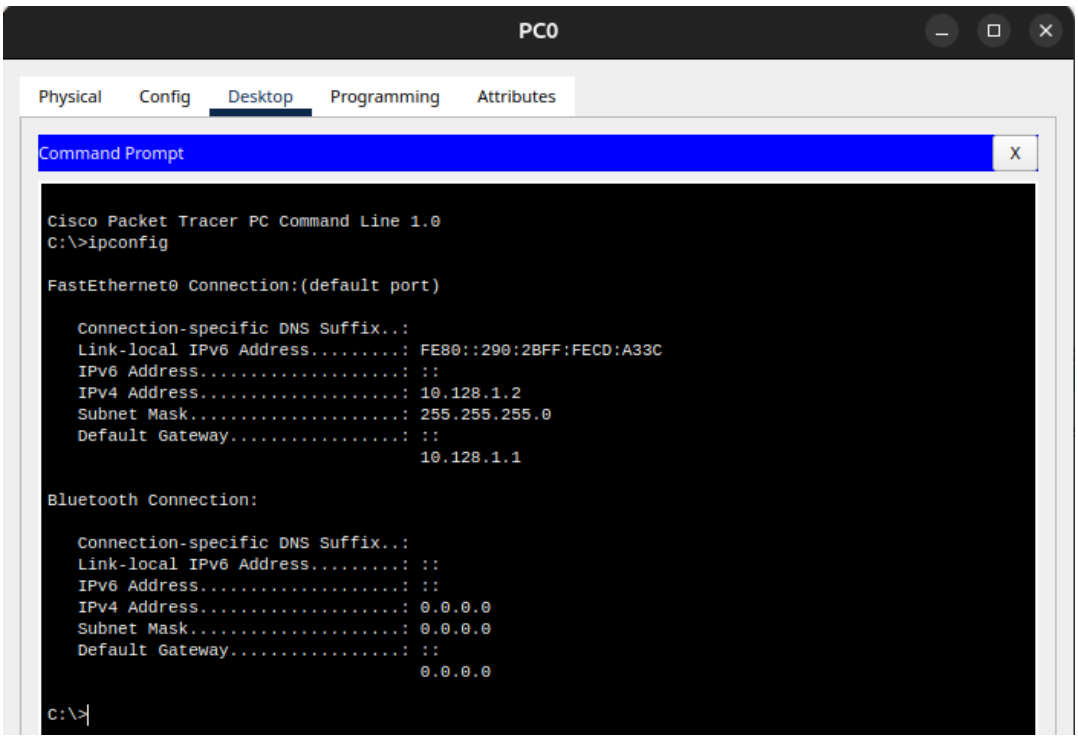

Рис. 4.3: Выдача адреса по dhcp в подсети 10.128.1.0

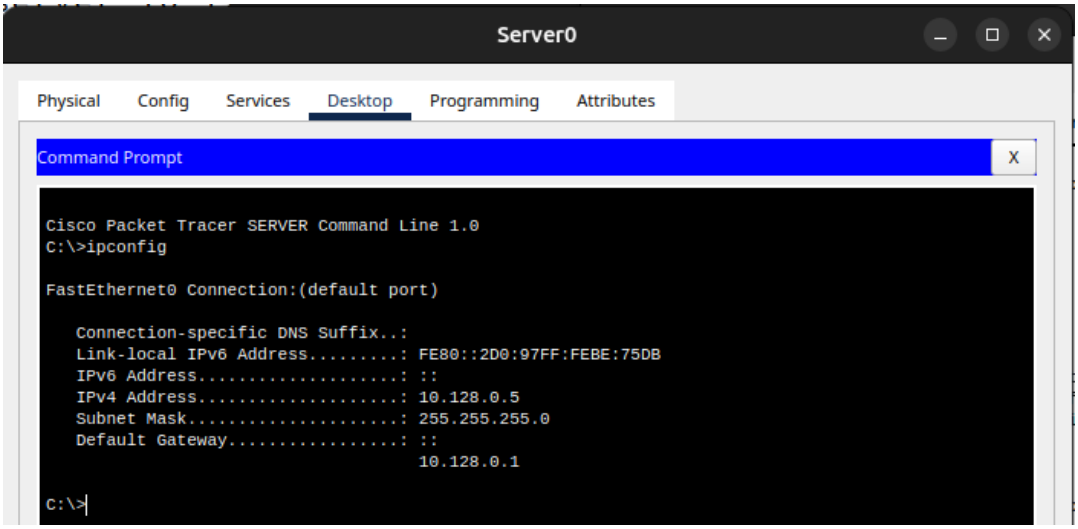

Рис. 4.4: Выдача адреса по dhcp в подсети 10.128.0.0

Теперь настроим поддельный dhcp-сервер с пулом адресов, начинающихся с 192.168.1.10(рис. [4.5]).

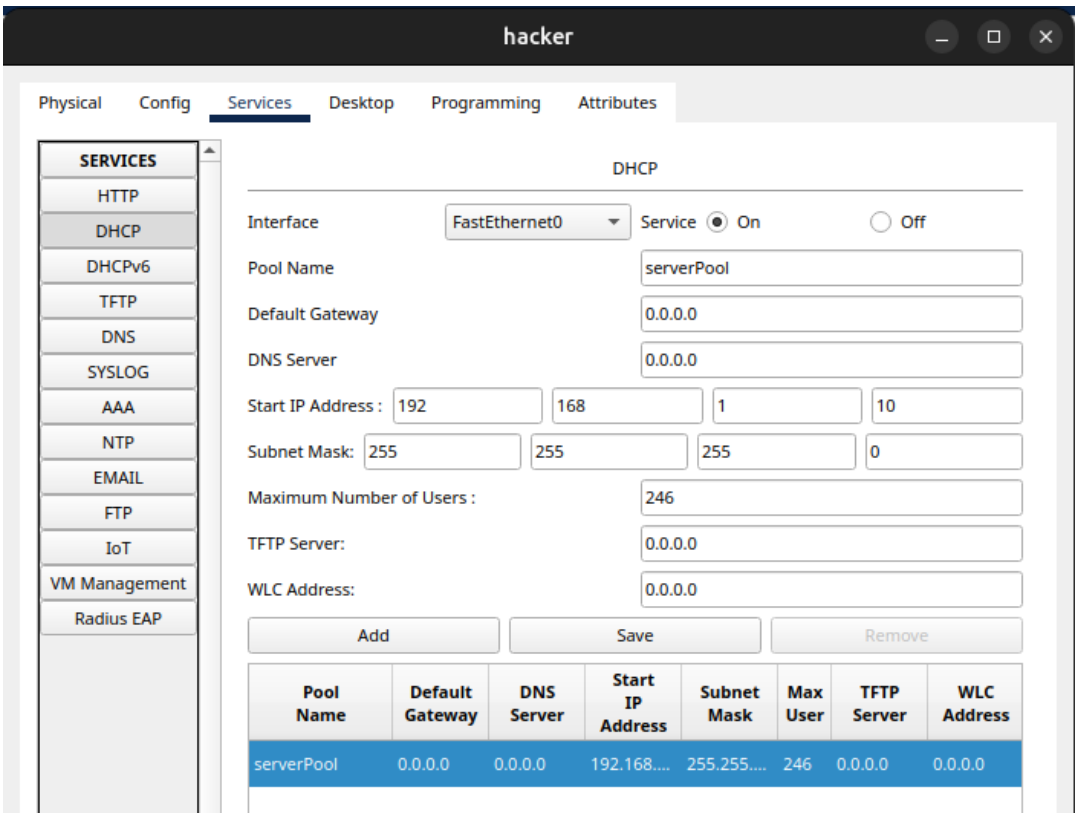

Рис. 4.5: Настройка поддельного dhcp-сервера

В результате адреса могут выдаваться в том числе и с этого сервера(рис. [4.6]).

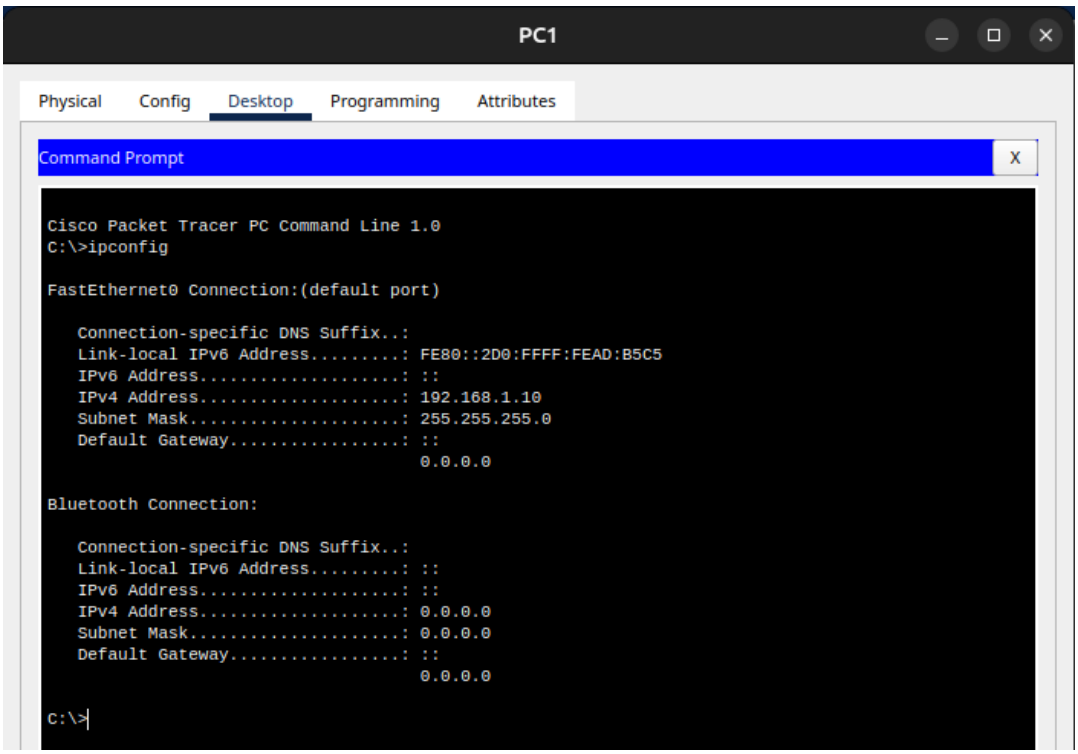

Рис. 4.6: Выдача адреса с поддельного dhcp-сервера

Для того чтобы адреса выдавались только с одного dhcp-сервера, нужно включить на коммутаторе dhcp-snooping и сделать порт, к которому подключен настоящий dhcp-сервер(в нашем случае f0.24) trusted-портом(остальные порты по умолчанию untrusted)(рис. [4.7]).

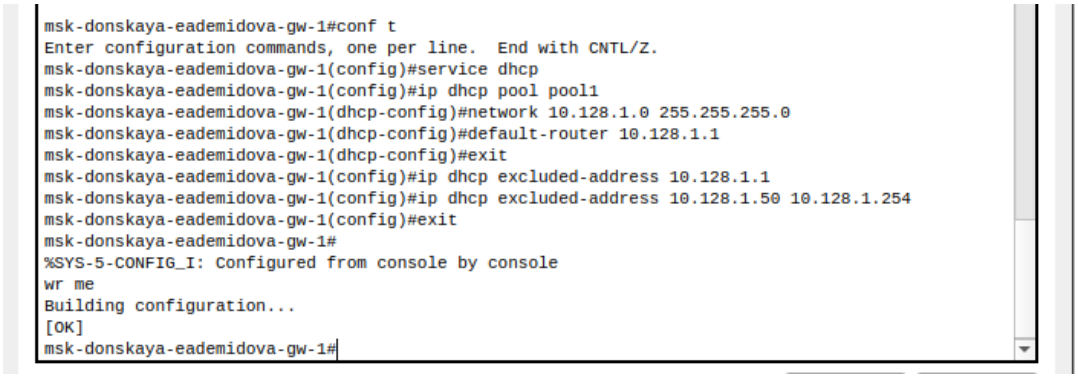

Рис. 4.7: Настройка dhcp-snooping

5 Выводы

Рассмотрены принципы работы DHCP, его настройку на сетевом оборудовании и обеспечение безопасности.

6 Список литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы – Учебник для вузов. 4-е изд. СПб.: Питер, 2010. 958 с.
2. ГОСТ Р 59802-2021. Национальный стандарт Российской Федерации. Телевидение вещательное цифровое. Расширенные технические требования к передаче транспортных потоков служб DVB по сетям с IP-протоколами. Часть 3. Процессы распределения адресов IP, реализации сетевых служб времени и обновления системного программного обеспечения домашнего оконечного оборудования. Основные параметры [Электронный ресурс]. Федеральное агенство по техническому регулированию и метрологии, 2022. URL: https://npalib.ru/2021/10/26/gost-r-59802-2021-id301215/.
3. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.