# [Введение](http://blog.netskills.ru/2014/03/3.html)

Пусть имеется следующая сеть.

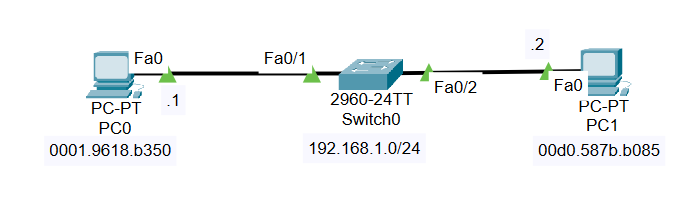


Рис. 1.

В данной сети присутствуют коммутатор 2960 и два пользовательских хоста. Каждый из хостов имеет индивидуальный мас-адрес. Предположим, что сеть была обесточена и мы начинаем работу. При передаче какого-либо кадра с компьютера РС0 (например при выполнении команды ping 192.168.1.2 к компьютеру РС1) на уровне L3 источник (РС0) формирует ip-пакет, содержащий ip-адрес источника (1) и ip-адрес приемника (2):

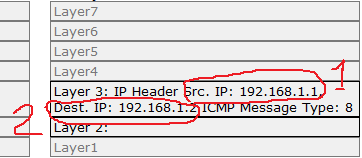


Рис. 2.

Но уровень L2, на котором работает коммутатор, не понимает ip-адреса, он поддерживает только мас-адресацию. Поэтому протокол ARP прежде всего проверяет содержимое своей arp-таблицы, которая в данный момент ничего не содержит. И прежде, чем передавать пакет с полезной информацией протокол ARP создает служебный кадр на канальном уровне L2 с запросом «Кто обладает ip-адресом 192.168.1.2 (1) сообщите свой мас-адрес» ко всем хостам, находящимся в данном сегменте, об этом говорит мас-адрес узла назначения (2).

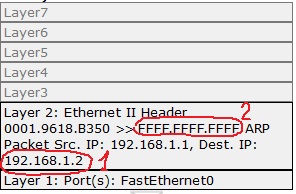


Рис. 3.

После получения ответа, в котором указано от кого (1) и кому (2):

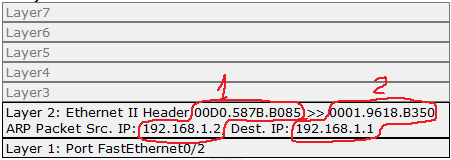


Рис. 4.

Протокол ARP заносит связку «ip-адрес - мас-адрес» в свою arp-таблицу и отправляет кадр с адресами источника (2) и приемника (1) с инкапсулированным внутри кадра ip-пакетом, в котором указаны ip-адреса источника (4) и приемника (5).

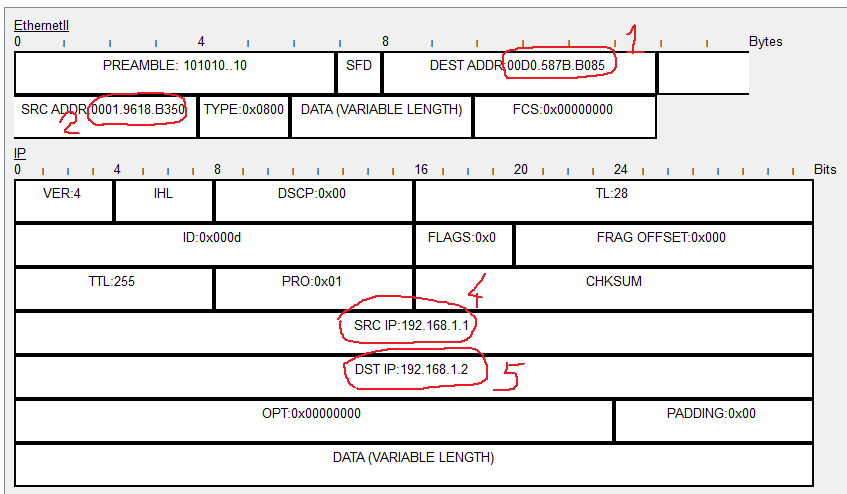


Рис. 5.

Таким образом, после обмена полезной информацией у компьютера РС0 будет следующая arp-таблица:

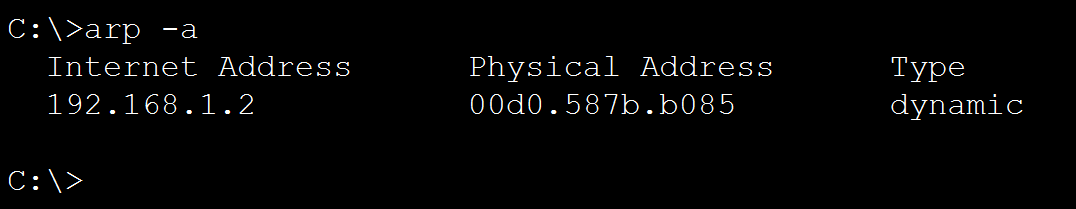


Рис. 6.

Здесь мы видим связку «ip-адрес (Internet Address) - мас-адрес (Physical Address)» узла-партнера по обмену информацией и тот факт, что она создана динамически.

Протокол ARP устроен таким образом, что в качестве ответа в виде связки ip-адрес - мас-адрес он будет принимать любую пару ip-адрес - мас-адрес. В этом и кроется суть атаки на ARP: можно подменять ip-адрес любым другим мас-адресом. Предположим, что в сети появился злоумышленник Laptop0.

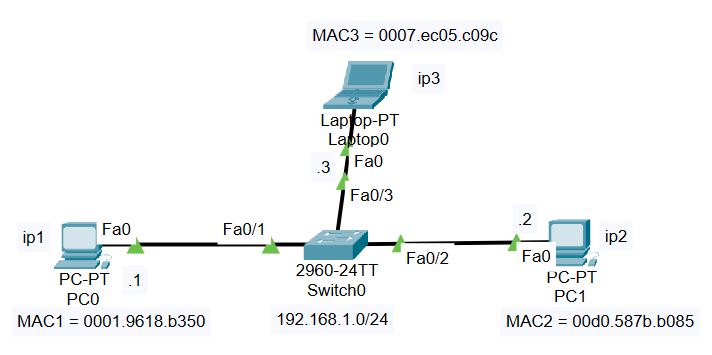


Рис. 7.

После обмена в сети хотя бы одним пакетом с Laptop0 у пользователя РС0 будет такая arp-таблица, в которой присутствует ip-адрес и мас-адрес злоумышленника:

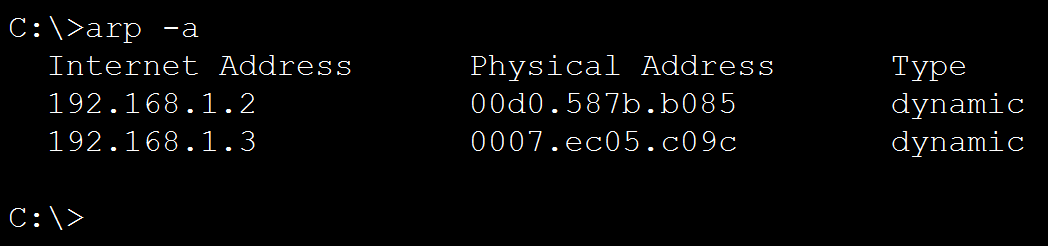


Рис. 8.

А на РС1 arp-таблица следующая:

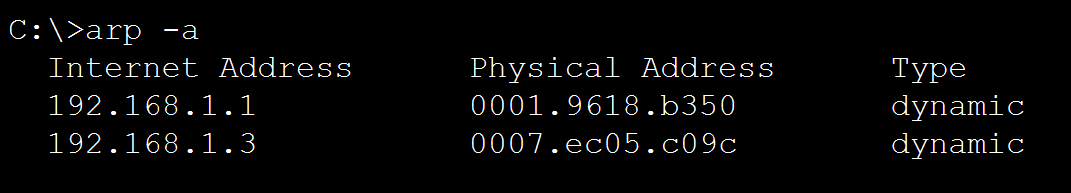


Рис. 9.

В arp-таблице не может быть такого случая, когда одинаковые ip-адреса соответствуют разным мас-адресам, но может быть, когда разным ip-адресам соответствуют одинаковые мас-адреса.

Для проведения атаки злоумышленнику достаточно подменить в arp-таблице жертвы, которая будет передавать информацию таким образом, чтобы ip-адрес его партнера соответствовал мас-адресу злоумышленника. То есть изменить arp-таблицу на рис. 8 следующим образом:

192.168.1.2 0007.ec05.c09c dynamic

А в arp-таблице партнера жертвы (рис. 9) сделать аналогичные изменения:

192.168.1.1 0007.ec05.c09c dynamic

В таком случае при отправке данных с РС0 на РС1 кадры с инкапсулированными в них пакетами информации будут попадать вместо РС1 на Laptop0 (рис. 10а), потому, что коммутатор получив с интерфейса f0/1 кадр со следующими мас-адресами: 0007.ec05.c09c (адрес назначения) и 0001.9618.b350 (адрес источника) отправит его на интерфейс f0/3 (см. рис. 10).

А теперь как пойдет кадр в обратном направлении:

Ответное сообщение компьютер РС1 будет формировать в виде пакета с адресом назначения 192.168.1.1 и адресом отправителя 192.168.1.2, который инкапсулируется в кадр с адресом назначения из arp-таблицы, а именно 0007.ec05.c09c и адресом отправителя 00d0.587b.b085 (рис. 10с).

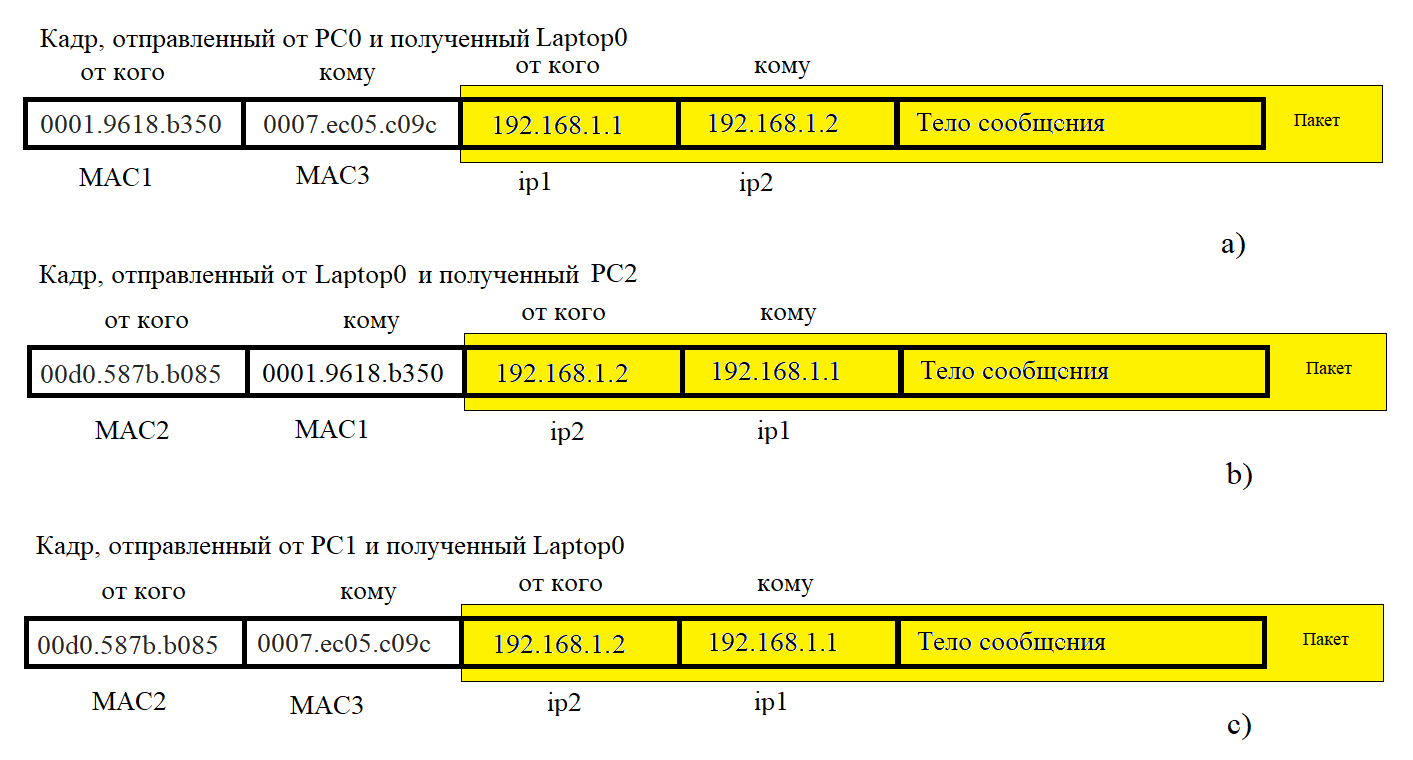


Рис. 10.

Таким образом злоумышленник может принимать кадры по своему мас-адресу, но для этого необходимо на своей операционной системе указать, чтобы она перенаправляла полученные кадры в сеть нужному адресату, т.е. создать ipforwarding. Легче всего это сделать на Linux операционных системах. Понятно, что информация, побывавшая у злоумышленника может быть прочитана, искажена или заменена на другую. Однако если посмотреть внимательнее, то можно заметить несоответствие: на машину злоумышленника в поле кому приходит кадр с мас-адресом МАС3 (принадлежащим ему) и с ip-адресом ip2 (принадлежащим не ему). Поскольку включена функция ipforwarding, то машина злоумышленника перепакует этот пакет в новый кадр и сделает его правильным, поскольку у него в arp-таблице правильные связки между МАС и ip адресами (рис. 10b).

Для выполнения работы используем EVE-NG. Создаем коммутатор на базе Cisco IOL (1) уровня L2 (2) – это будет коммутатор второго уровня, меняем наименование (3) и иконку (4).

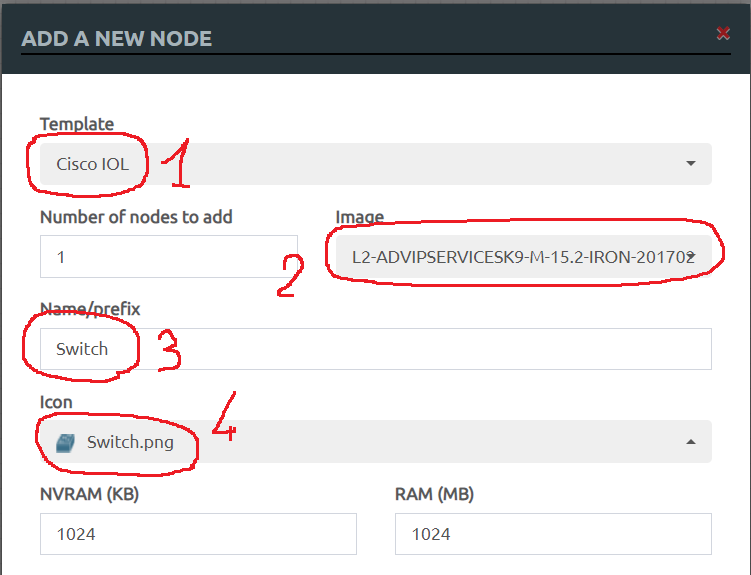


Рис. 11.

Используя образ Linux (1) создаем две легкие Linux-машины (2), изменяем количество нод (3) и имя (4), выбираем QEMU Nic (5)

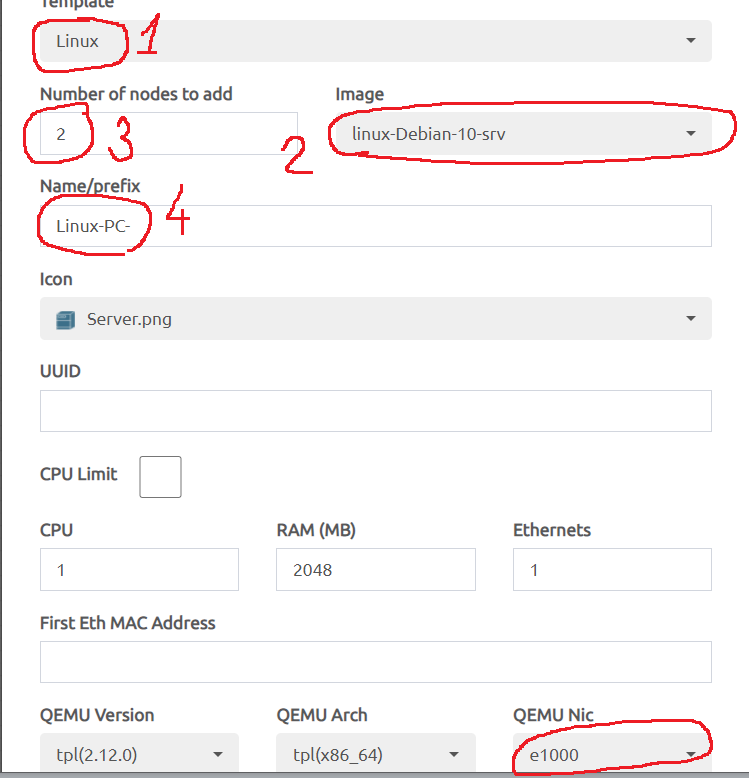


Рис. 12.

Для работы злоумышленника создадим Linux-машину (1) на базе образа Linux-Kali (2), выбираем иконку (3), выделяем два процессора (4) 4Г памяти (5) и выбираем QEMU Nic (6).

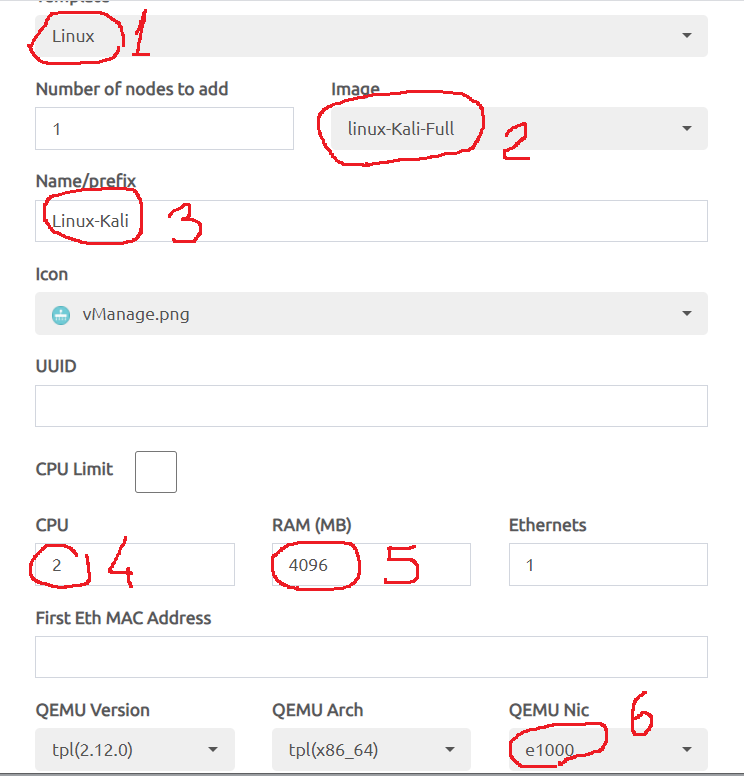


Рис. 13.

Соединяем созданные компоненты в схему, запускаем их и настраиваем Router так, чтобы он работал в режиме NAT и позволял выход в интернет.

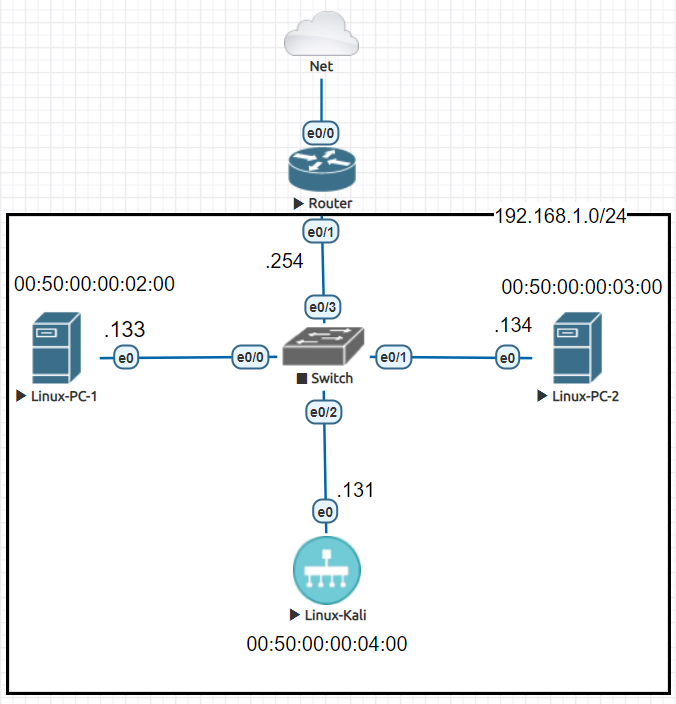


Рис. 14.

После старта системы вводим Login: root, Password: eve@123. Нажатие клавиш при вводе пароля не отображается. Проверим интерфейсы командой ip a (1).

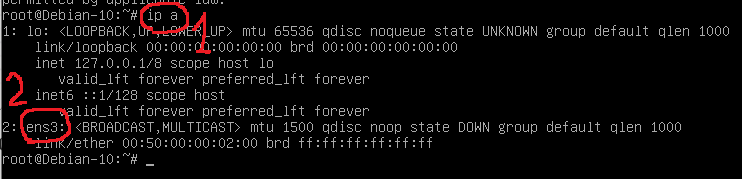


Рис. 15.

Мы видим, что присутствует один интерфейс ens3 и он не включен. Для включения интерфейса необходимо выполнить команду:



Рис. 16.

После чего откроется окно текстового редактора со следующим содержимым:

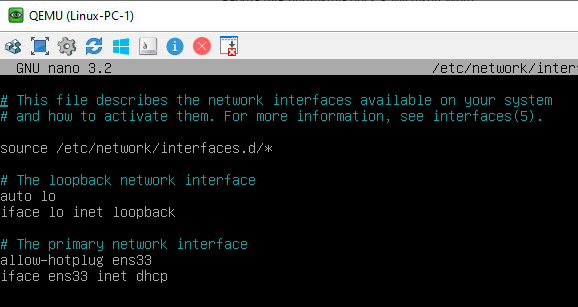


Рис. 17.

Текст нужно поменять так:

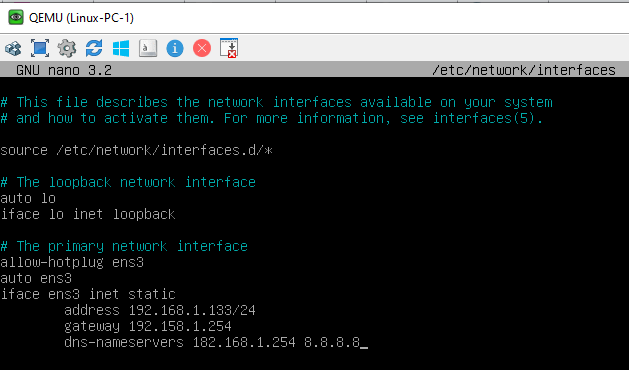


Рис. 18.

Для сохранения внесенных изменений нажать комбинацию клавиш CTRL+O, а затем ENTER. Для выхода из редактора - CTRL+X. Для того, чтобы изменения вступили в силу необходимо перезапустить службу следующим образом:



Рис. 19.

Теперь можно убедиться, что все работает.

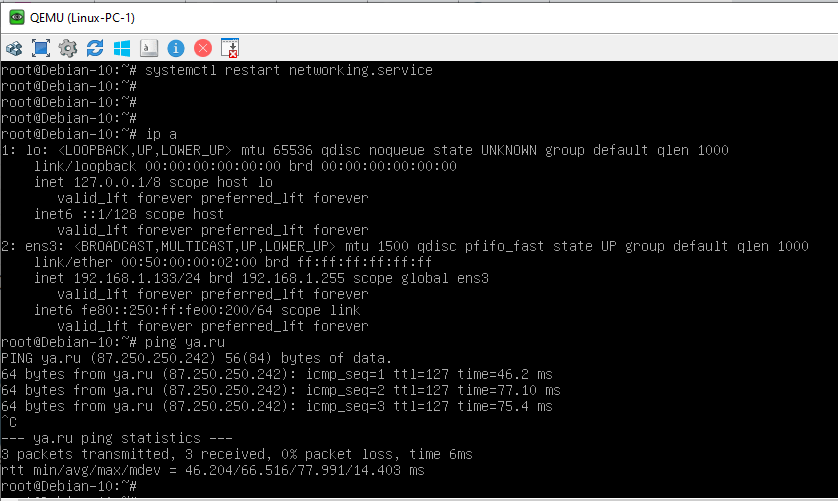


Рис. 20.

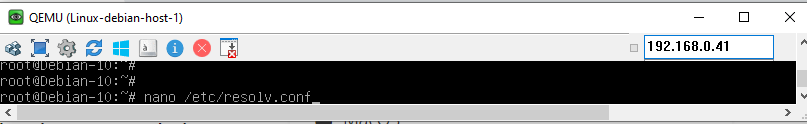


Рис. 21.

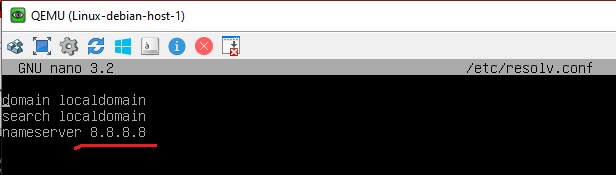


Рис. 22.

Точно так же настраиваем вторую машину Linux-PC.