Федеральное государственное бюджетное образовательное учреждение высшего образования

Сибирский государственный университет телекоммуникаций и информатики

Расчетно-графическая работа

По дисциплине “Сети ЭВМ и Телекоммуникации”

Выполнил:

Студент группы ИП-217

Ковалев Даниил Артемович

Новосибирск, 2024

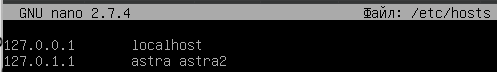
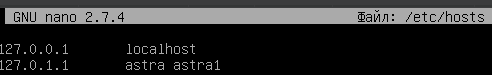
1. Собрали конфигурацию сети.
2. Задаем уникальные имена виртуальным машинам:

Астралинуксы:





Добавляем созданное имя по пути в /etc/hosts, чтобы при заходи в рута оно не выдавало ошибок:



Микротики:



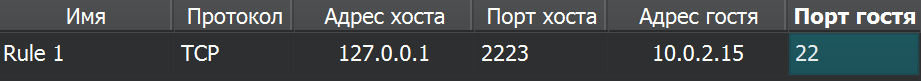
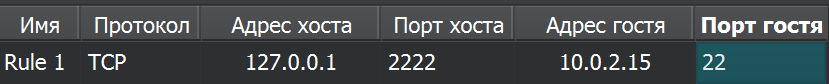




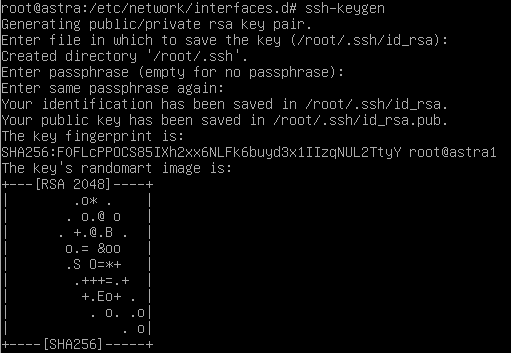


Настраиваем проброс портов для машин (настраивается в NAT):

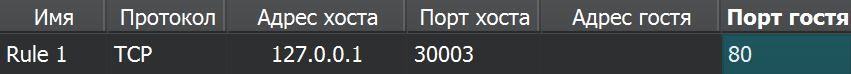
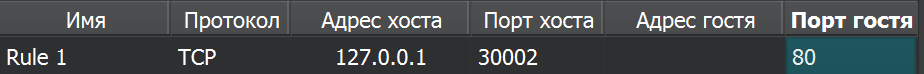
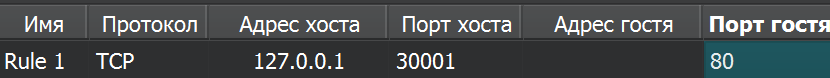
Астралинуксы (Для подключения по ssh, 22 порт гостя):



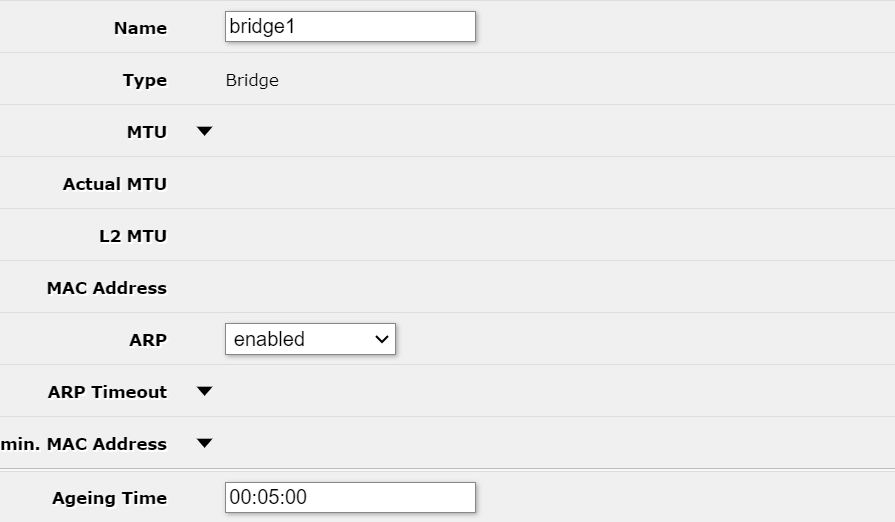
Генерируем ssh-ключи:



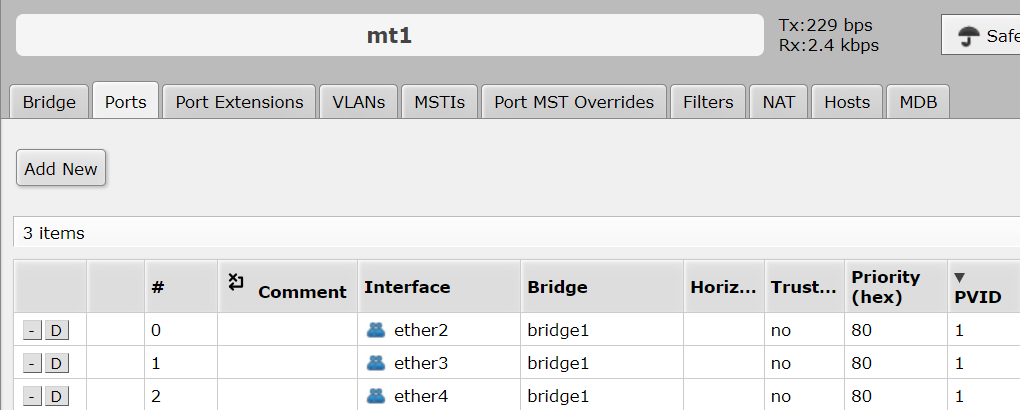
Микротики (Для доступа к веб-интерфейсу):

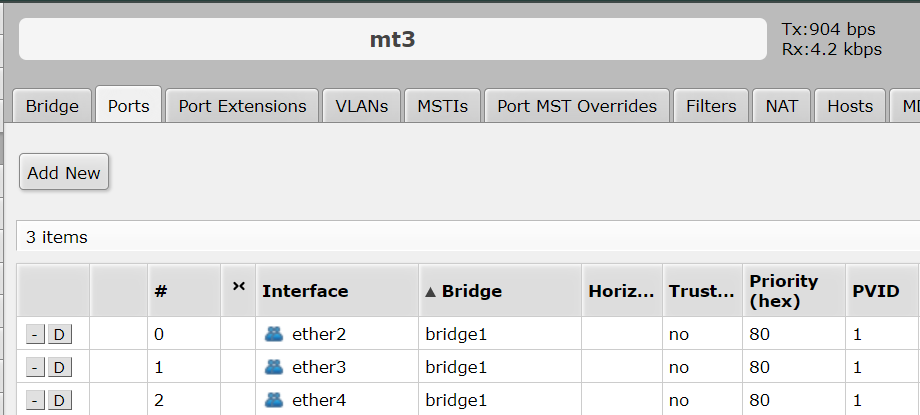
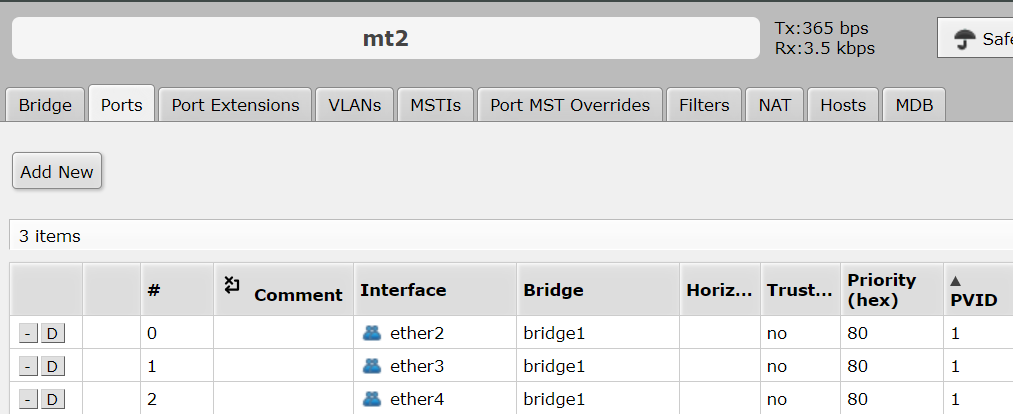


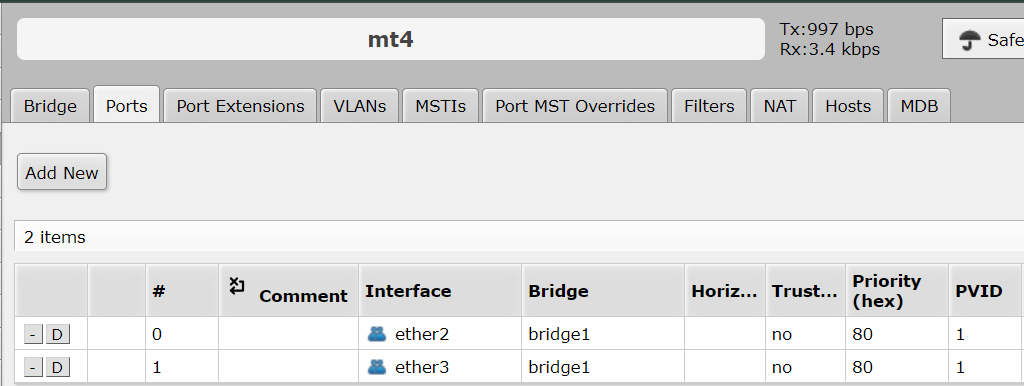
1. Объединяем все рабочие порты коммутаторов в сетевые мосты (сетевое устройство второго уровня модели OSI, предназначенное для объединения сегментов (подсети) компьютерной сети в единую сеть) на микротиках:

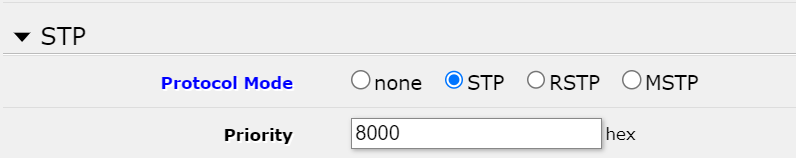


Добавляем интерфейсы в порты моста:

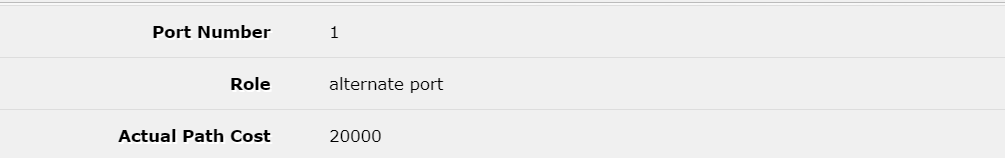




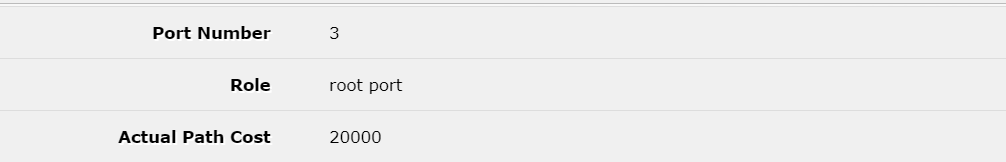
 Настраиваем работу STP протокола (сетевой протокол, предназначенный для предотвращения образования петель в сети):



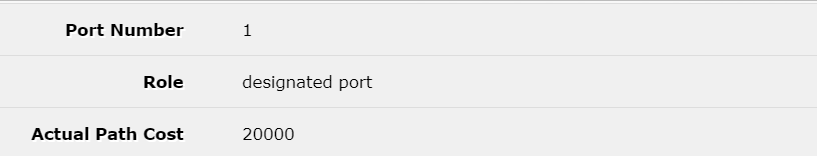
Состояние портов:



Alternate port — это порт, который имеет альтернативный путь к корневому коммутатору (root bridge) по сравнению с текущим выбранным путем (через designated port). Этот порт находится в состоянии блокировки (blocking) и не участвует в передаче данных, но он готов к использованию в случае, если основной путь станет недоступным.



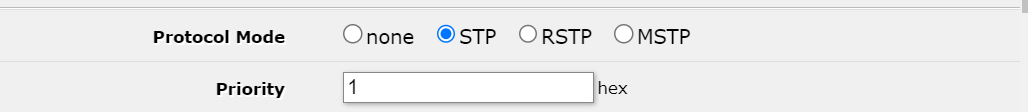
Root port — это порт коммутатора, который имеет наиболее оптимальный путь к корневому коммутатору (root bridge). Этот порт находится в активном состоянии (forwarding) и участвует в передаче данных между коммутатором, на котором он находится, и остальной частью сети.

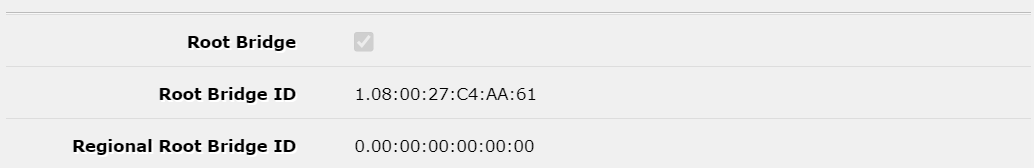


Designated port — это порт на коммутаторе, который обеспечивает наиболее оптимальный путь к корневому коммутатору (root bridge) для конкретного сегмента сети. Этот порт находится в активном состоянии (forwarding) и участвует в передаче данных между сегментом сети, к которому он подключен, и остальной частью сети.

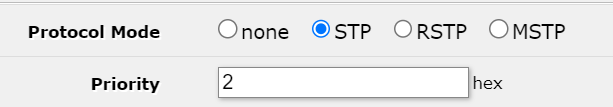
Изменяем настройки протокола STP так, чтобы корневым коммутатором был 2 Микротик, а 4 Микротик был резервным.

Для того, чтобы 2 Микротик стал корневым, то ему нужно снизить значение STP протокола сетевого моста:





Для того, чтобы 4 Микротик стал резервным, то значение STP протокола нужно сделать выше, чем, у 2 Микротика. Если 2 Микротик выйдет из строя, то 4 становится корневым коммутатором:

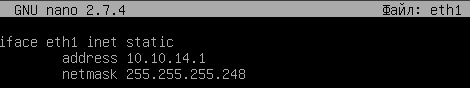


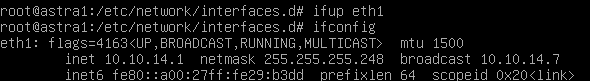
1. Диапазон IPv4 адресов – 10.10.14.0/24. Разделяем диапазон на максимальное количество подсетей так, чтобы каждая подсеть могла адресовать до 6 узлов (можем разделить на 32 подсети):

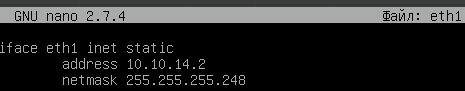


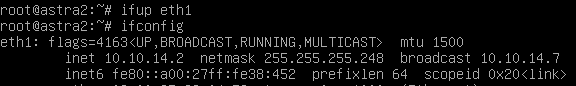
Выбираем один из диапазонов – 10.10.14.0/29 и назначаем адреса всем машинам:

Астры на интерфейс eth1:









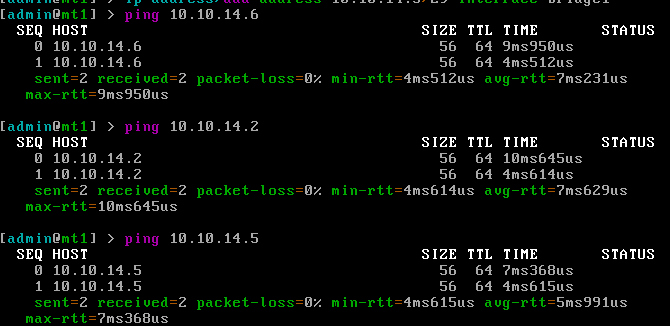
Микротикам назначем на сетевой мост:



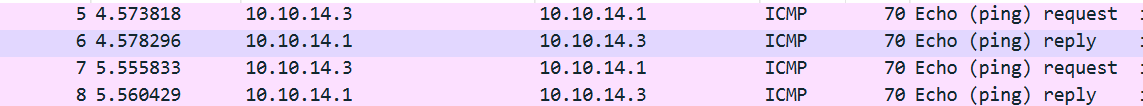




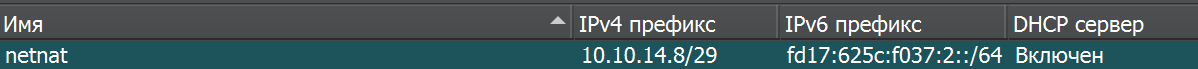
Так как все машины находятся в 1 подсети (в 1 диапазоне), то появилась связь между всеми ними:



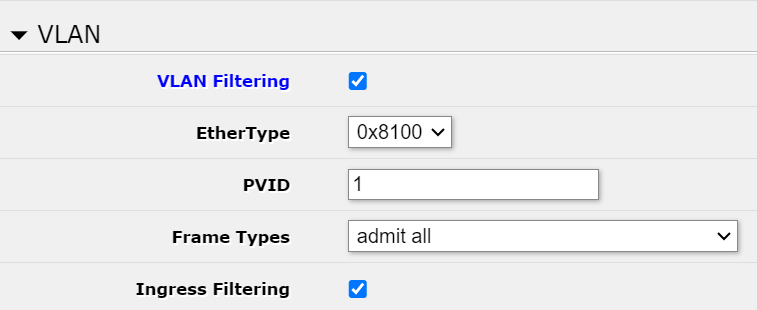
Смотрим в вайршарке, что есть связь:



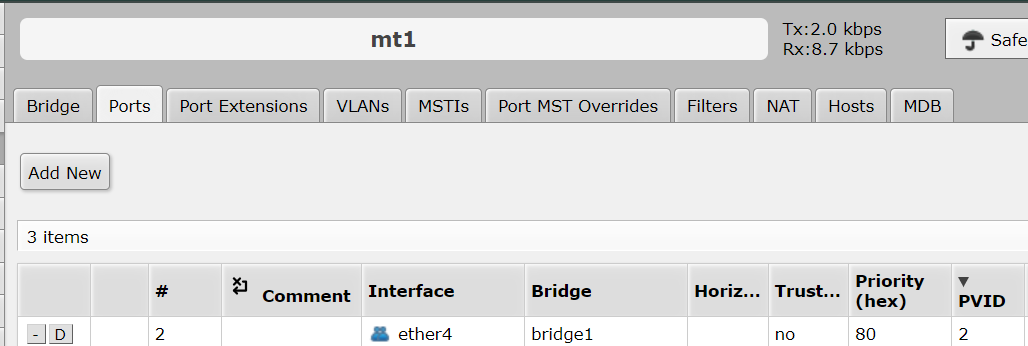
1. Настраиваем сеть NAT, чтобы функционировал DHCP, и она раздавала адреса из другого диапазона:

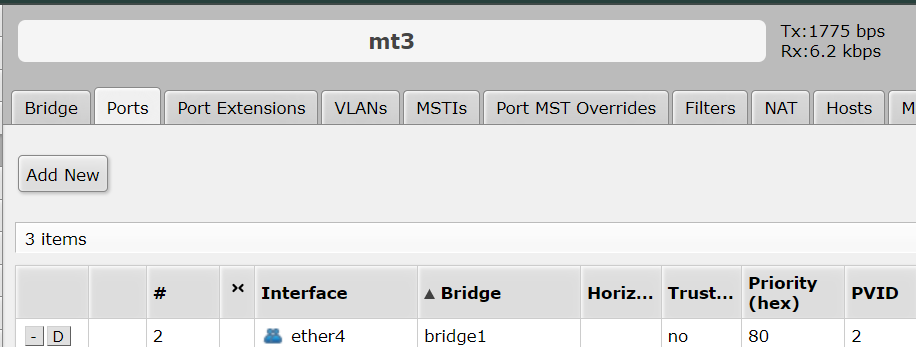


Включаем VLAN Filtering (позволяет управлять доступом к VLAN на коммутаторах и контролировать какие данные могут передаваться между различными VLAN) у сетевых мостов на 1- 3 микротике:

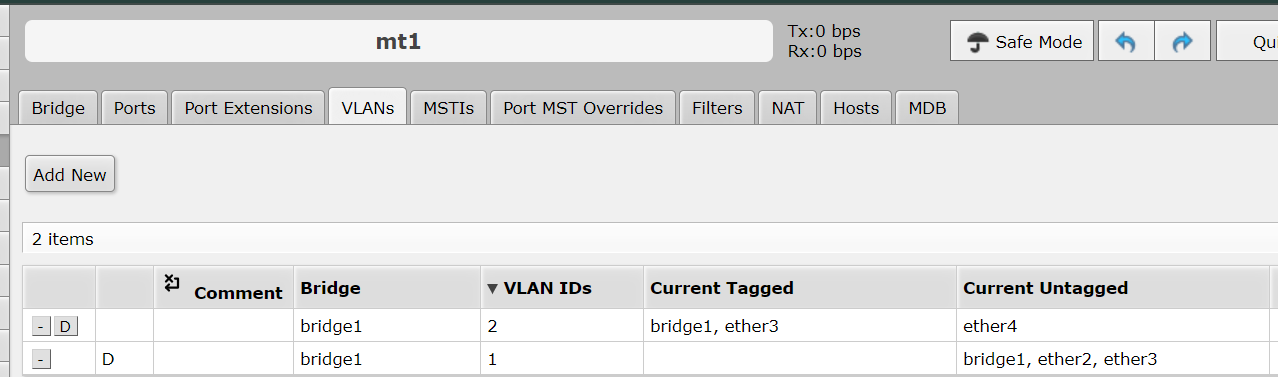


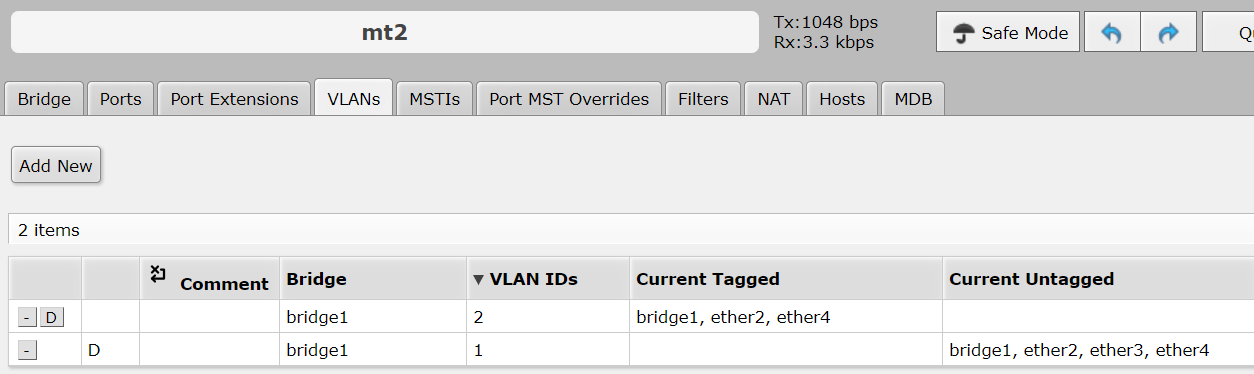
Настраиваем порту ether4, который идет до сети NAT у 1 и 3 Микротика VLAN 2, чтобы он функционировал только между VLAN 2:

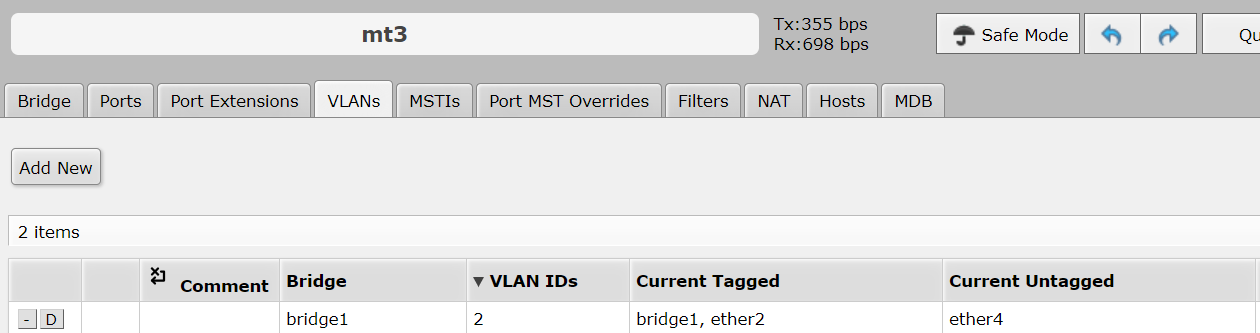




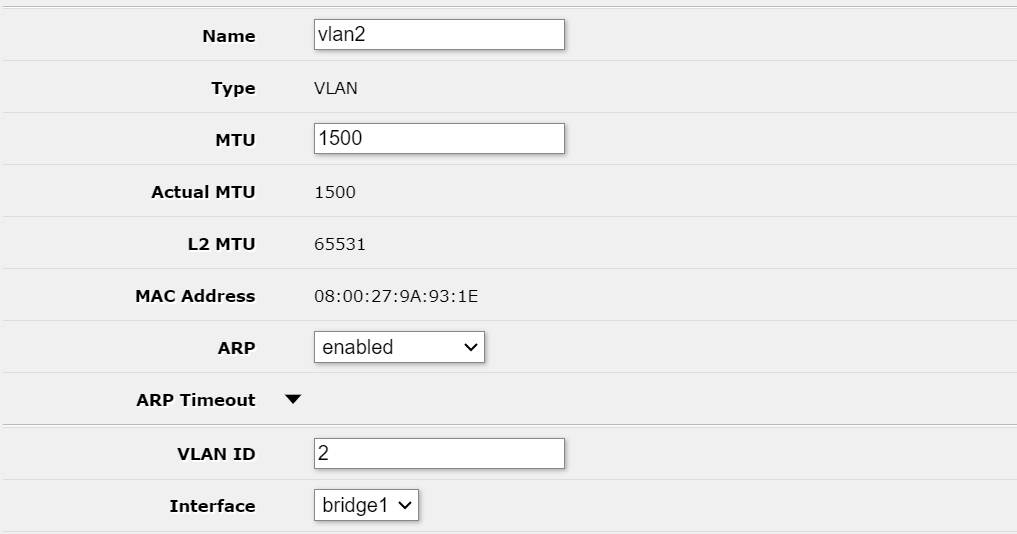
Создаем VLAN с номером 2, которая будет использоваться для доступа в сеть NAT, чтобы она работала только между 1 – 3 Микротиками (В тегированный трафик добавляем порты, соединяющие эти маршрутизаторы):



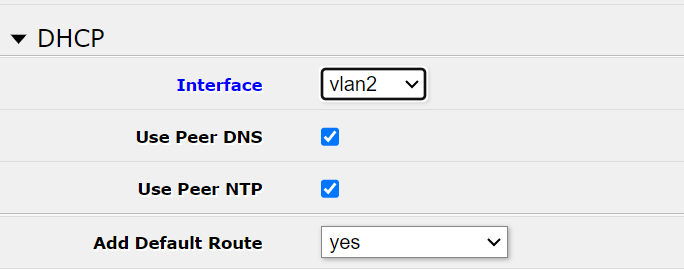




Создаем виртуальные интерфейсы для этих VLAN 2:

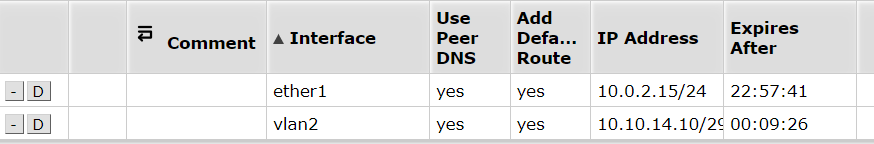


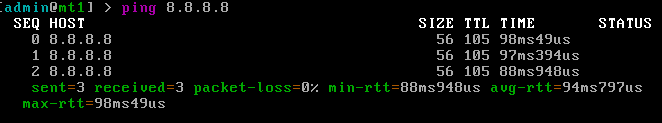
Настраиваем DHCP-клиента на созданный интерфейс vlan2, чтобы он получил адрес из сети NAT:



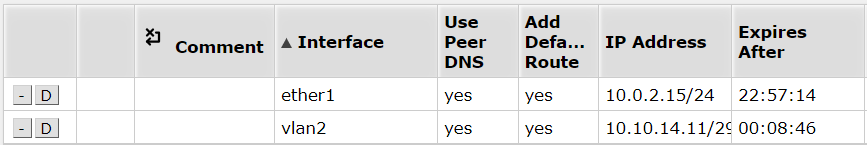
Каждый из микротиков получил собственный адрес из диапазона сети NAT и доступ в интернет:

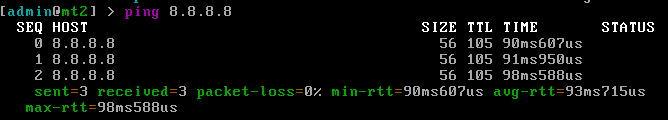
1 Микротик:



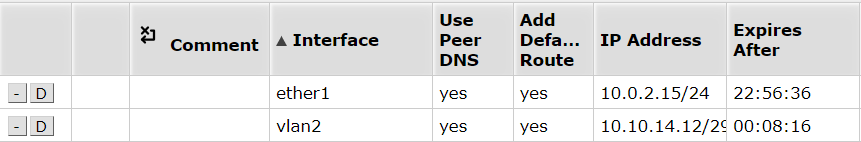


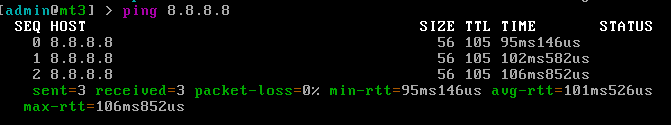
2 Микротик:





3 Микротик:





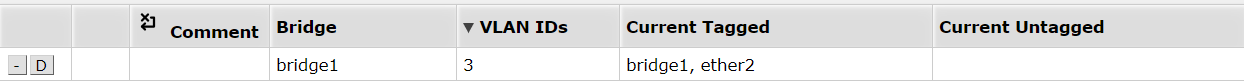
1. Назначаем адрес на vboxnet-4 (Ethernet Adapter 5) из доступного диапазона, для доступа к хост-машине:



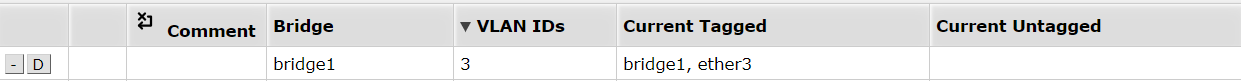
Создаем VLAN с номером 3, которая будет использоваться для доступа в сеть vboxnet-4:

В тегированный трафик ставим пути до 1 и 2 Астры, путь до хост-машины – нетегированный:

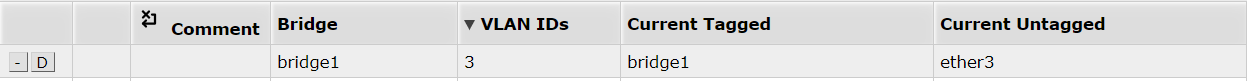
1 Микротик:

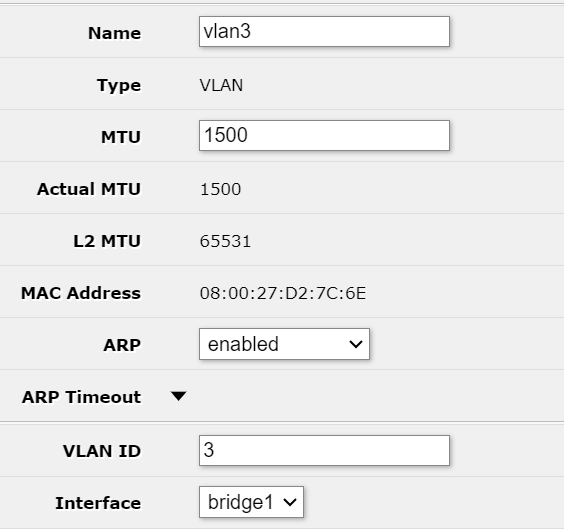


2 Микротик:



3 Микротик:



Создаем виртуальный интерфейс для VLAN 3: 

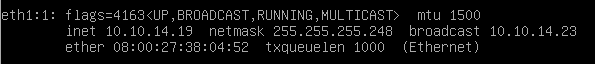
Назначаем адреса всем сетевым устройствам сети из этого же диапазона:

Астры:









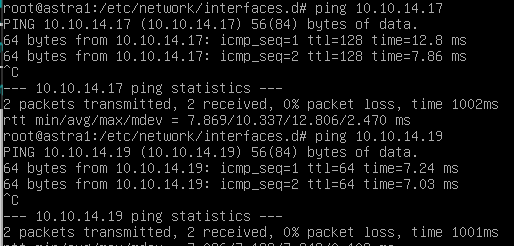
Микротикам добавляем адресна интерфейс VLAN 3:



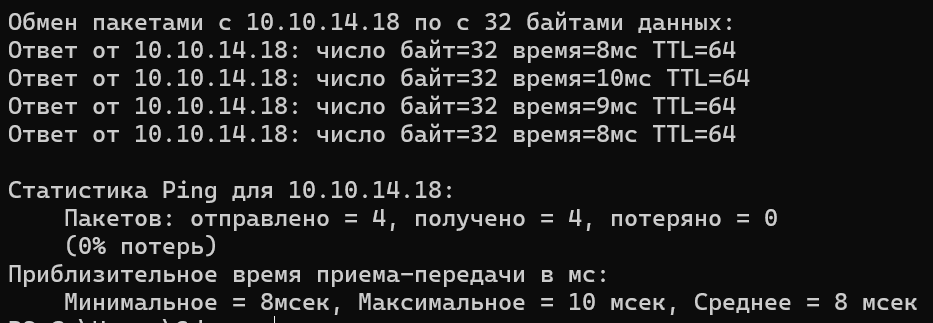




Появилась возможность пинговать с астралинуксов vboxnet-4, т.е хост-машину:

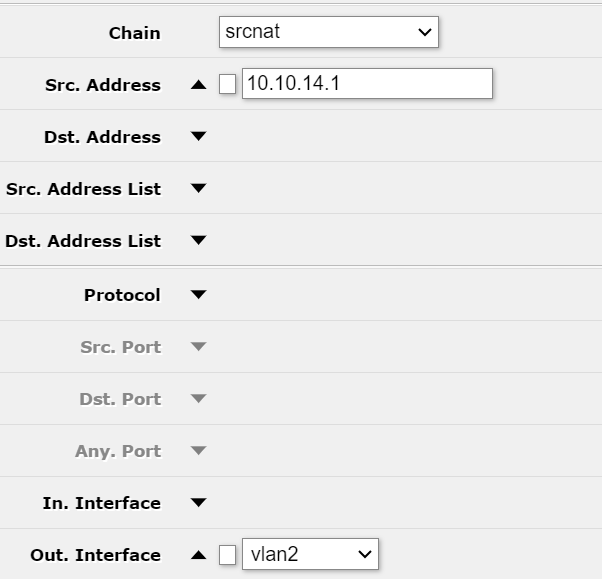


И с хост-машины до астры:



1. На 1 Микротике настраиваем правило трансляции адресов таким образом, чтобы предоставить 1 астре доступ в интернет из нетегируемой сети:

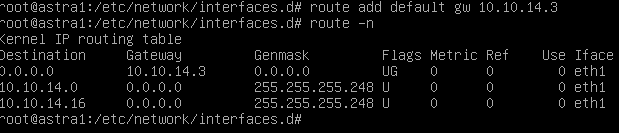
Добавляем адрес 1 астры и VLAN 2, который для доступа в интернет:



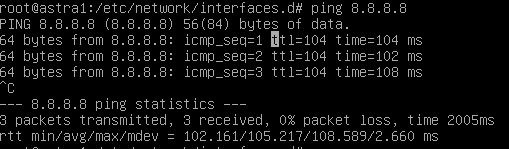


Masquerade, заменяет исходный IP-адрес каждого внутреннего устройства на свой собственный внешний IP-адрес.

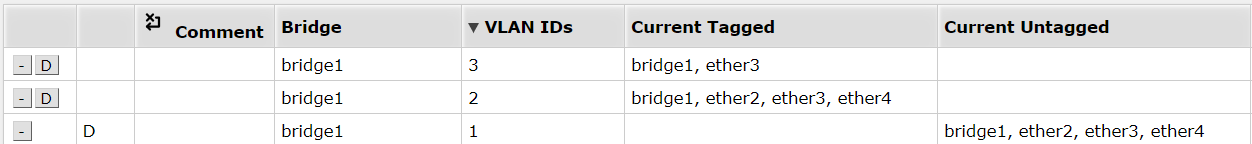
Добавляем в таблицу маршрутизации у астры адрес 1 Микротика:



Предоставили доступ в интернет из нетегируемой сети для 1 астры:



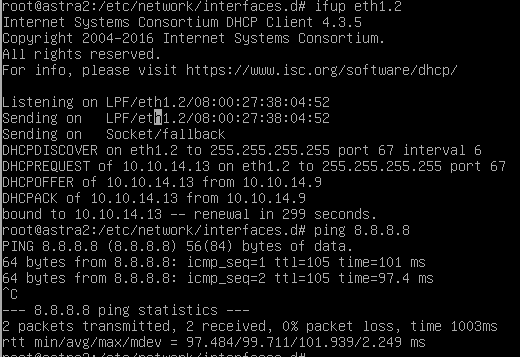
Изменяем конфигурацию 2 Микротика, чтобы обеспечить доступ к тегированной VLAN 2 через интерфейс vboxnet-2, т.е добавляем в VLAN 2 в тегированный трафик ether3, который идет до 2 астры:



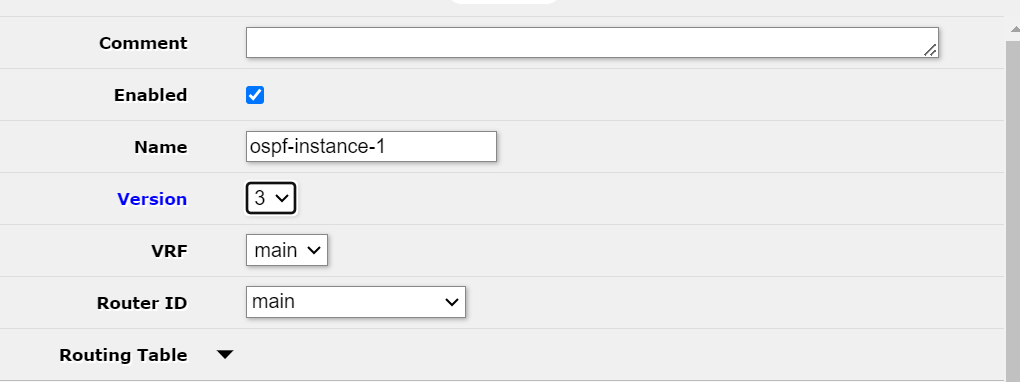
На 2 астре настраиваем виртуальный интерфейс, чтобы он получил автоматическинастройки из сети NAT и доступ в интернет:



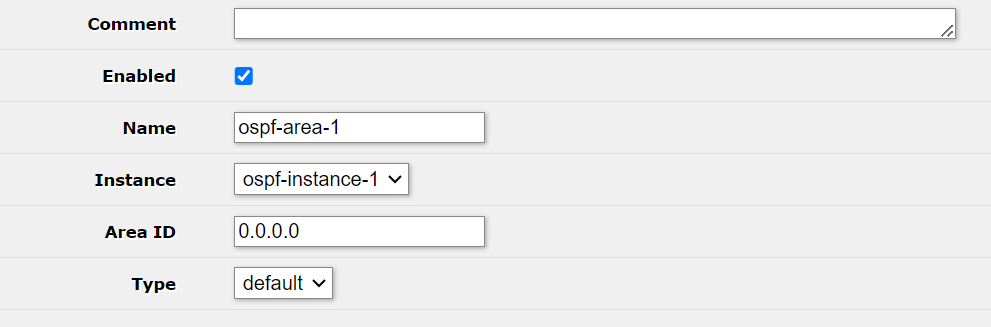
Поднимаем интерфейс и получаем доступ в интернет:



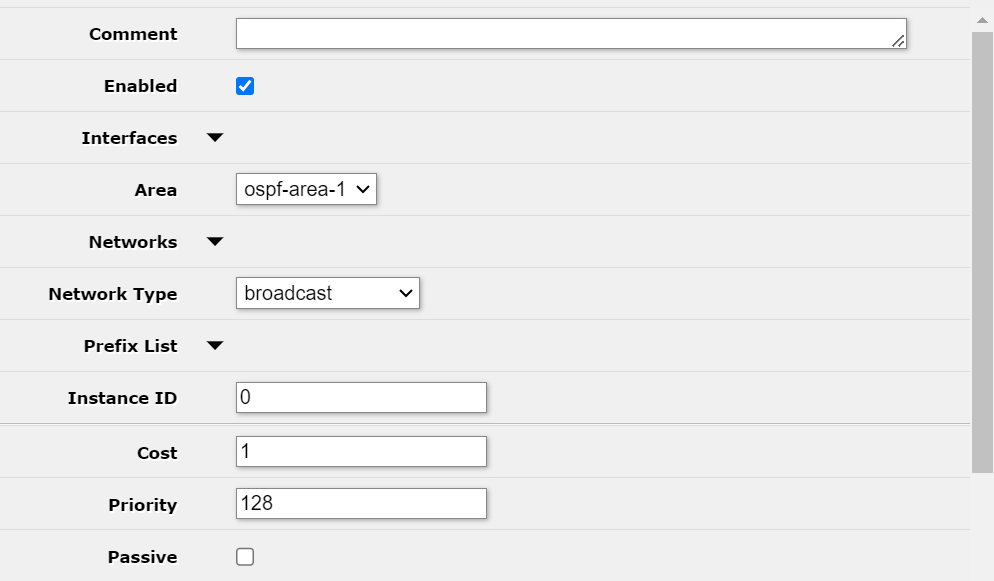
1. Настраиваем на всех микротиках протокол динамической маршрутизации OSPF (протокол динамической маршрутизации класса Link-State, использующий алгоритм Дейкстры для вычисления оптимальных маршрутов внутри автономных систем):



Создаем Areas (зоны для разделения сети на более мелкие логические области):



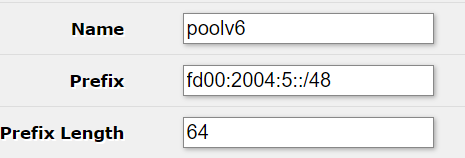
Cоздаем Interface Templates:



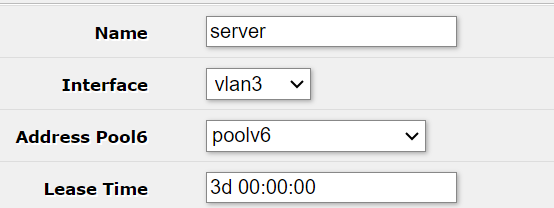
1. Диапазон IPv6-адресов: fd00:2004:5::/48.

На 3 Микротике создаем DHCP-сервер для распределения префиксов IPv6:

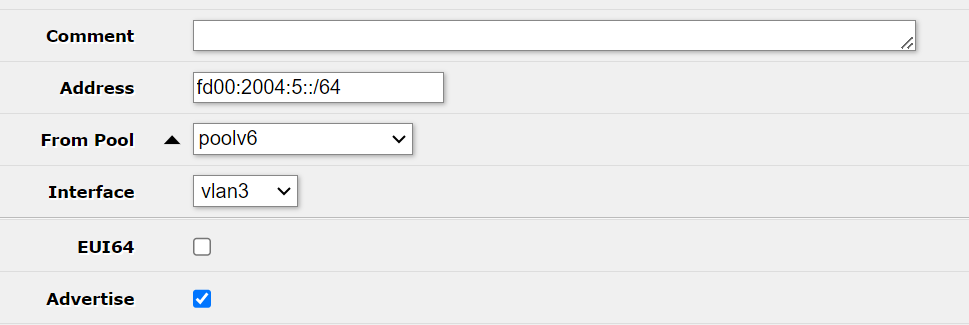
Создаем пул с диапазоном:

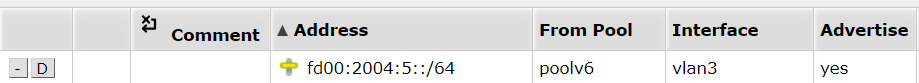


Создаем DHCP-сервер, с созданным пулом и интерфейсом – VLAN3, который будет служит для распределения префиксов:

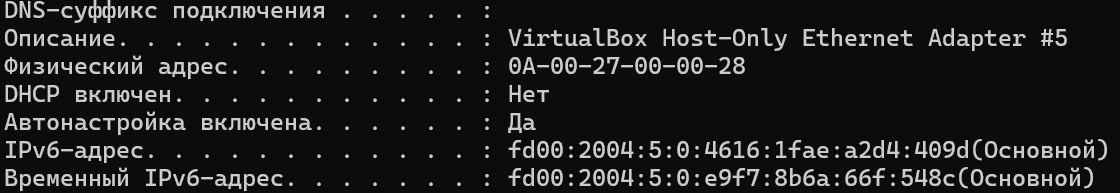


1. На 3 Микротике настраиваем IPv6 адрес на интерфейс VLAN с номером 3, чтобы хост-машина сконфигурировала себе адрес:

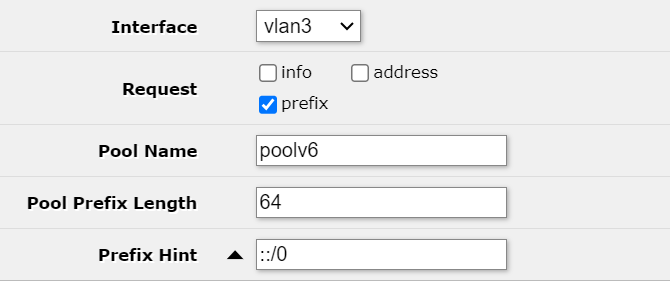




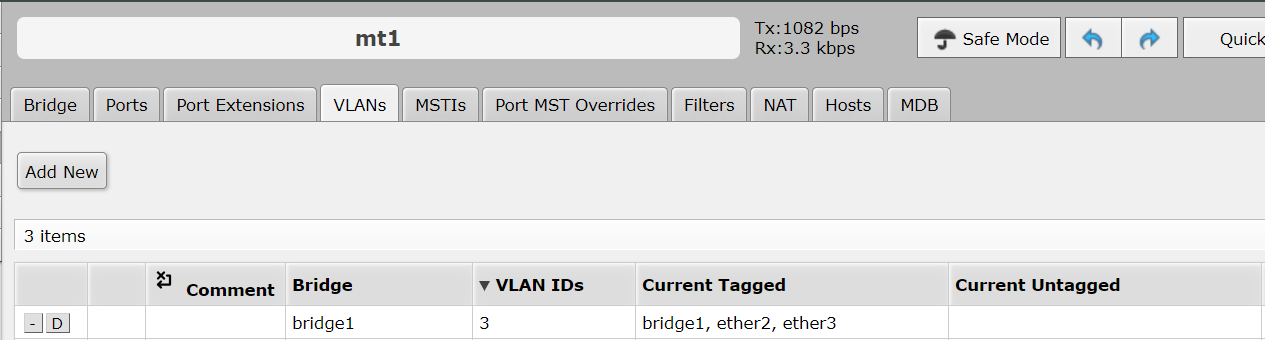
Хост-машина сконфигурировала себе адрес из транслируемого диапазона:

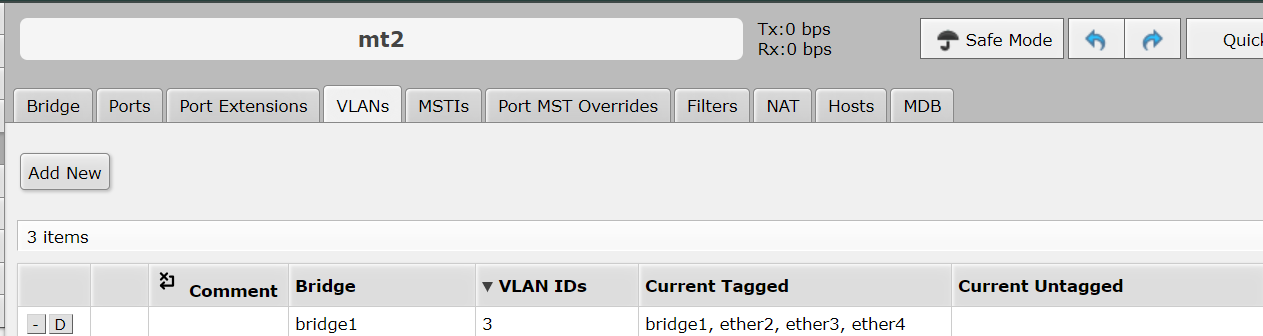


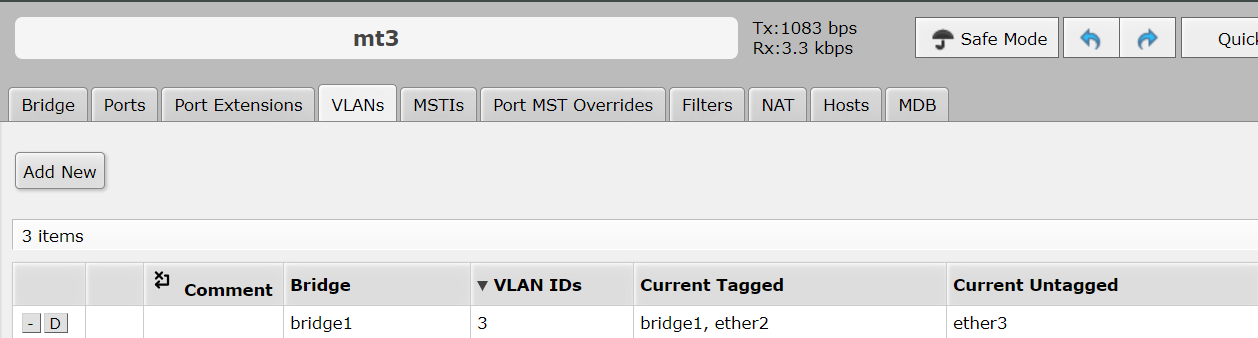
1. На 1 микротике настраиваем DHCP-клиента, чтобы он получил префикс для распределения:

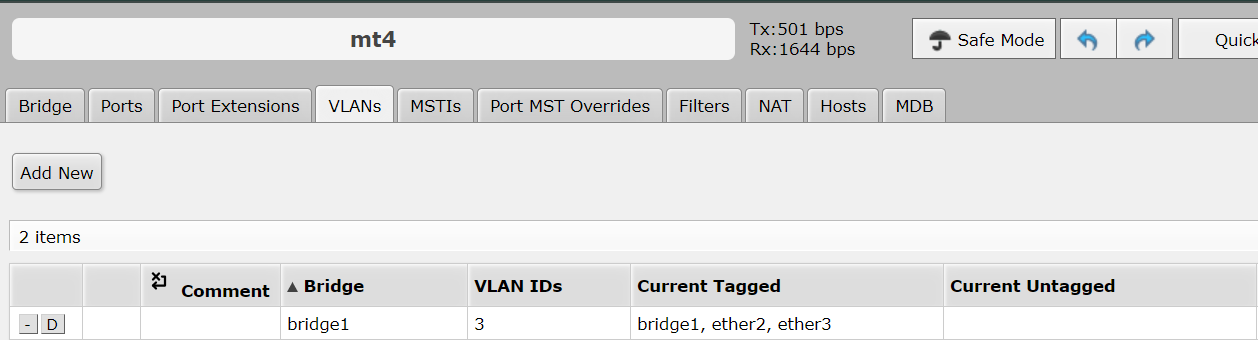


Чтобы 1 микротик смог получить префикс для распределения, то настраиваем маршрутизацию всех VLAN 3 на микротиках, добавляя в тегированный трафик все интерфейсы, которые служат для соединения машин:

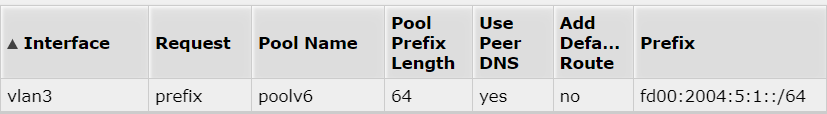




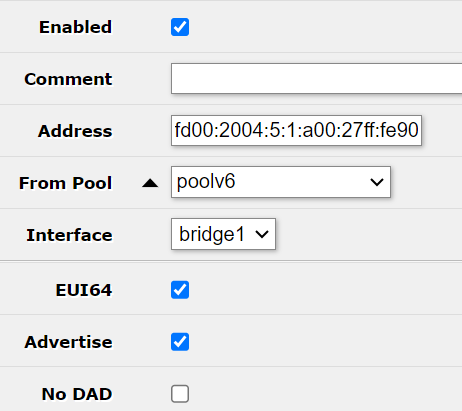




И теперь DHCP-клиент получил префикс для распространения:



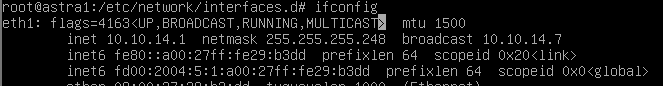
Назначаем из полученного пула IPv6 адресов адрес на интерфейс сетевого моста, включая EUI-64 для получения полного адреса:

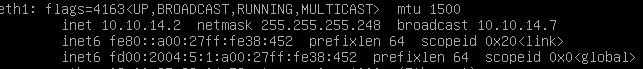


Настраиваем на астралинуксах автоматическую конфигурацию IPv6 адресов:

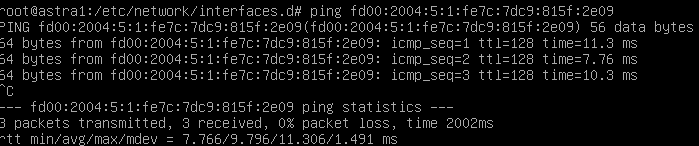


Проверяем, что астры сконфигурировали себе адрес включая префикс:

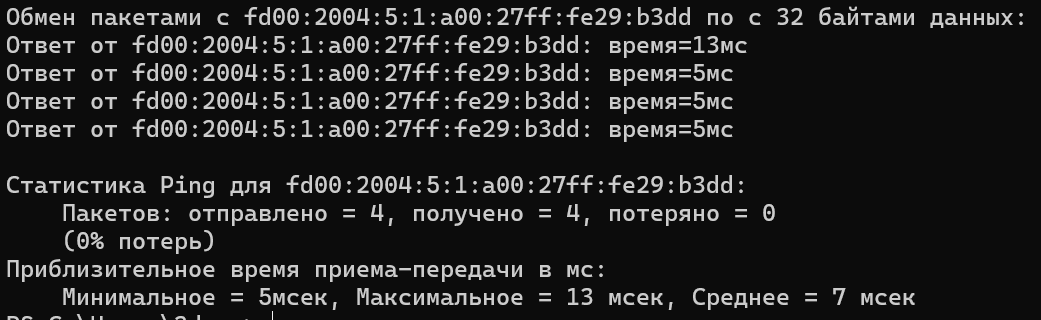




1. Так как в предыдущем пункте уже была правильно настроена маршрутизация VLAN 3, то появляется возможность сразу пинговать хост-машину с астралинуксов:



И наоборот:



1. На 2 астралинуксе проверяем настройки DNS-клиента по пути nano /etc/resolv.conf и меняем значение адреса, чтобы запросы по умолчанию передавались на DNS с адресом 8.8.8.8:

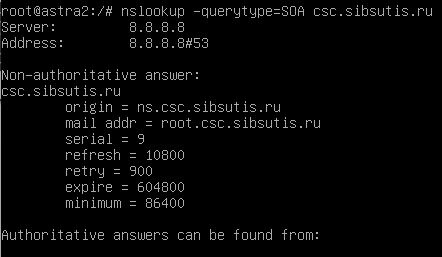


Проверяем, чтобы запросы шли на DNS с адресом 8.8.8.8:

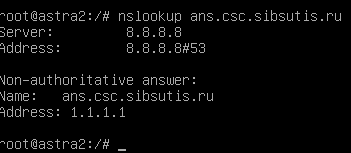


1. Устанавливаем пакет dnsutils для утилиты nslookup::

Информация о DNS-зоне csc.sibsutis.ru:



Информация о IPv4 имени ans.csc.sibsutis.ru



IPv4 адреса для домена mail.ru

