Занятие 3. Модель OSI. Сетевой уровень - L3

Задание:

- Настроить сетевое оборудование в зоне статической маршрутизации
- Настроить статические маршруты на устройствах в зоне статической маршрутизации
- Настроить сетевое оборудование в зоне OSPF
- Настроить динамическую маршрутизацию в зоне OSPF
- Настроить сетевое оборудование в зоне BGP
- Настроить динамическую маршрутизацию в зоне BGP
- Провести атаку с подменой маршрута в зоне OSPF
- Провести атаку с подменой маршрута в зоне BGP*

В отчете отразить:

- Конфигурацию любого одно маршрутизатора в каждой из зон маршрутизации (должно получиться 3 конфигурации роутеров)
- Скрин работы утилиты ping между каждыми крайними маршрутизаторами (MR-12, MR-10, CR-6, LR-15)
- Скрин успешной атаки на OSPF (получен fake маршрут)
- Скрин успешной атаки на BGP (если у вас получилось реализовать атаку), а также идею реализации атаки

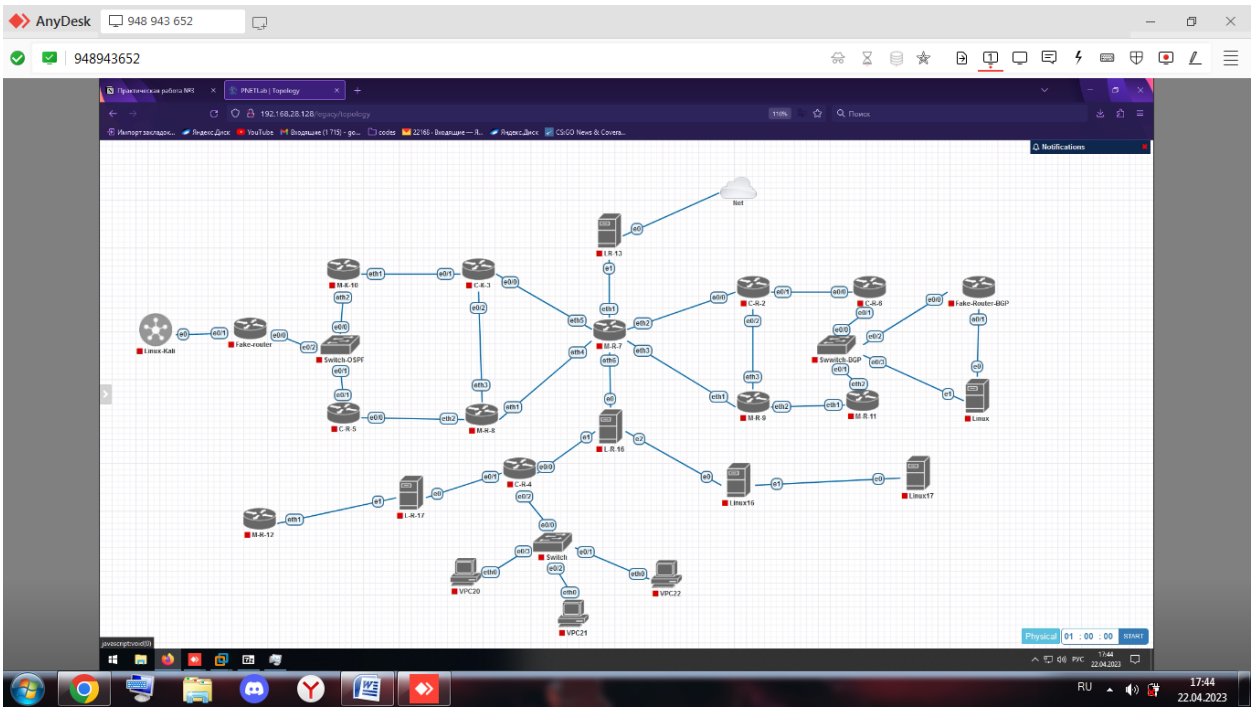


Рис. 1 Исходная схема

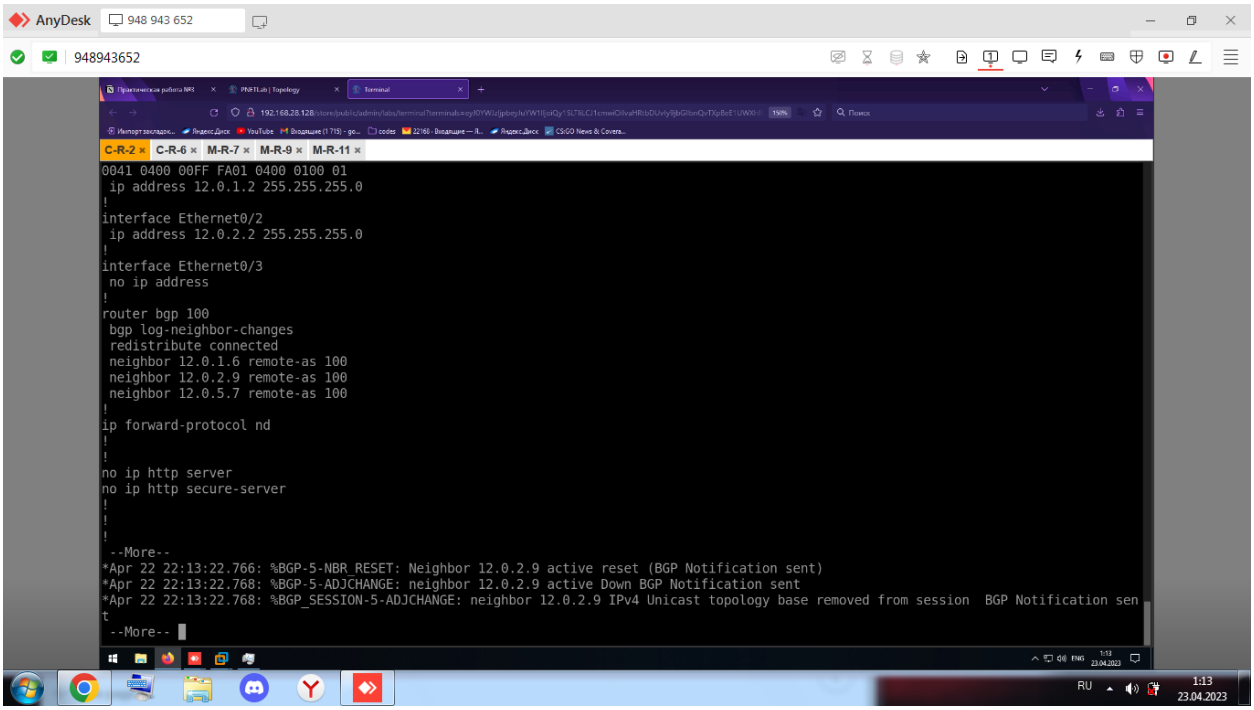


Рис. 2 Конфигурация C-R-2 (iBGP)

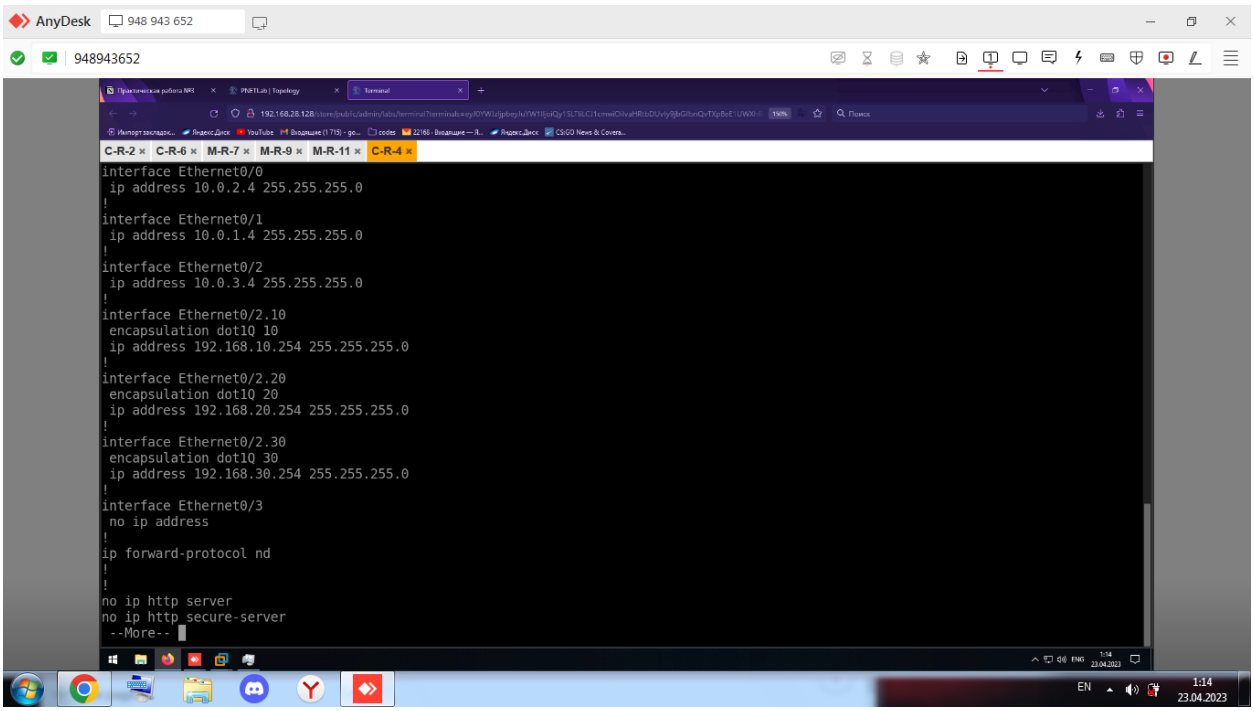


Рис. 3 Конфигурация C-R-4 (Static Routing)

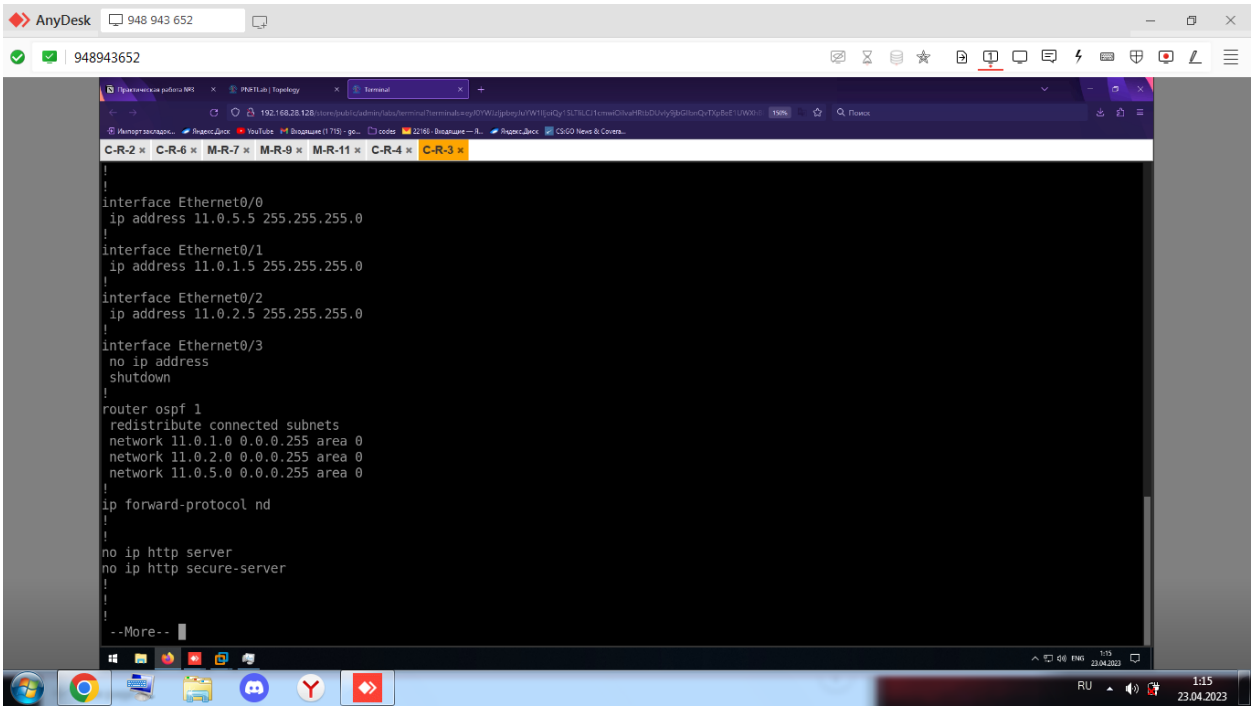


Рис. 4 Конфигурация C-R-3 (OSPF)

- Скрин работы утилиты ping между каждыми крайними маршрутизаторами (MR-12, MR-10, CR-6, LR-15)

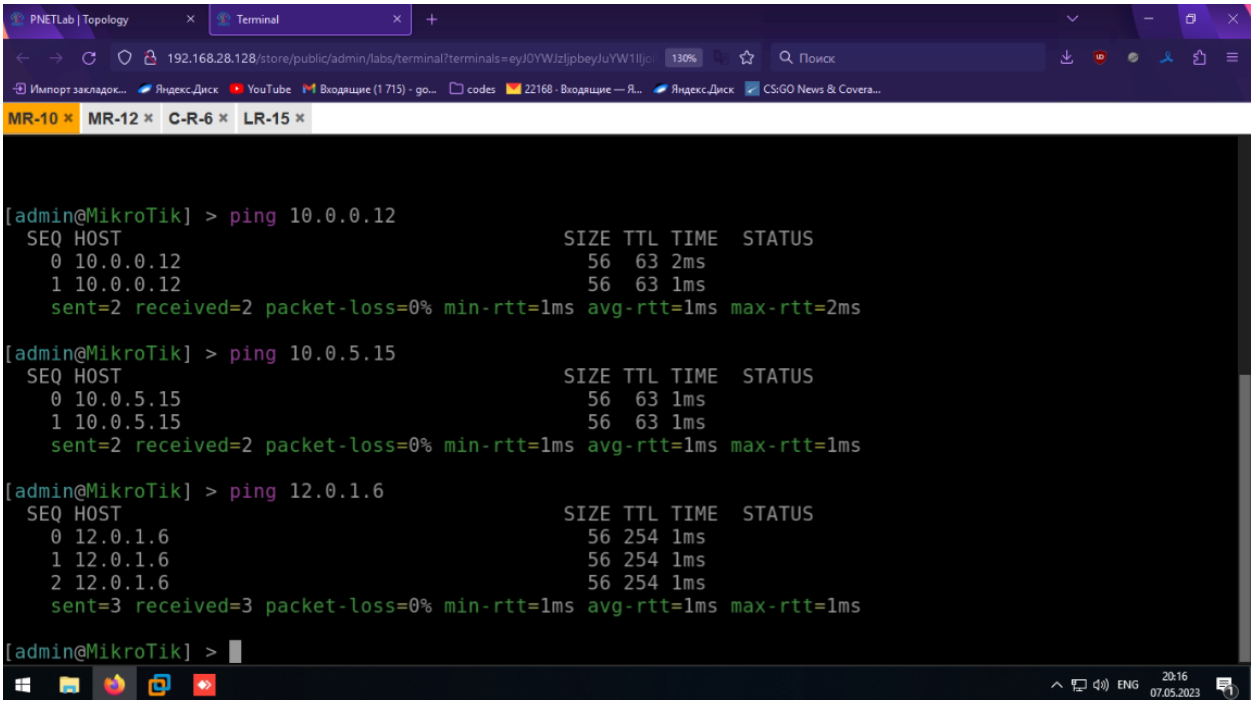


Рис. 5 Пинг с сети 11.0.1.0 на сети 10.0.5.0, 10.0.0.0, 12.0.1.0

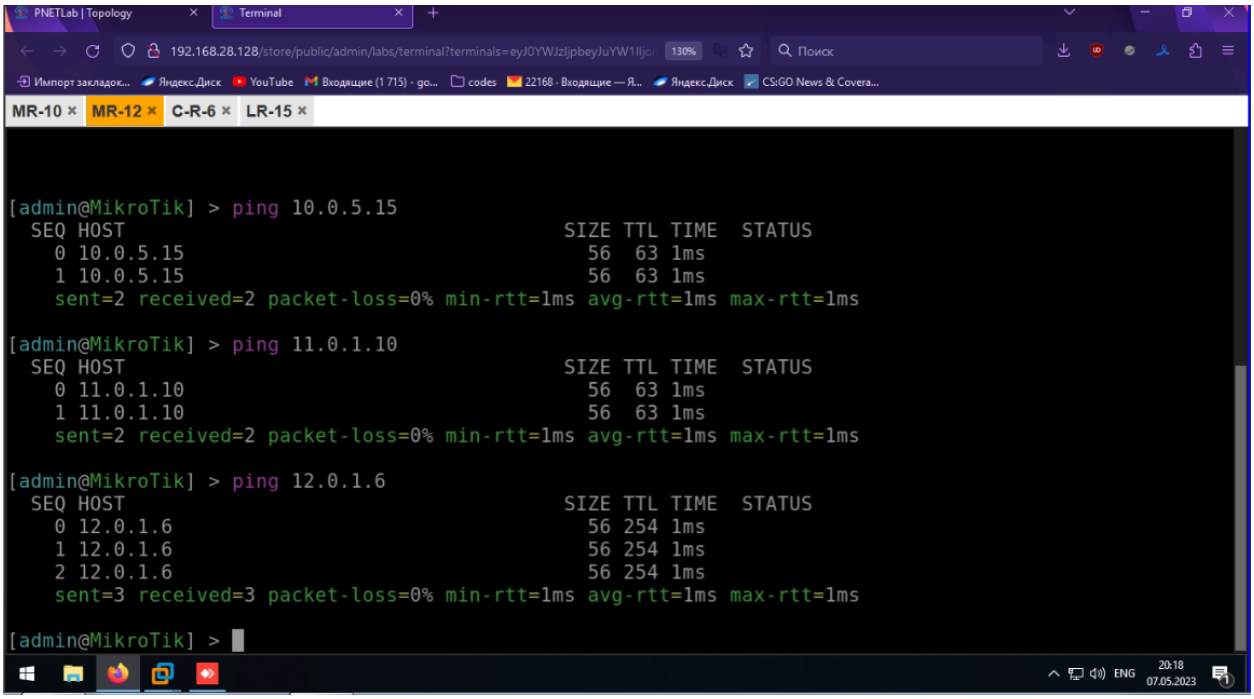


Рис. 6 Пинг с сети 10.0.0.0 на сети 10.0.5.0, 11.0.1.0, 12.0.1.0

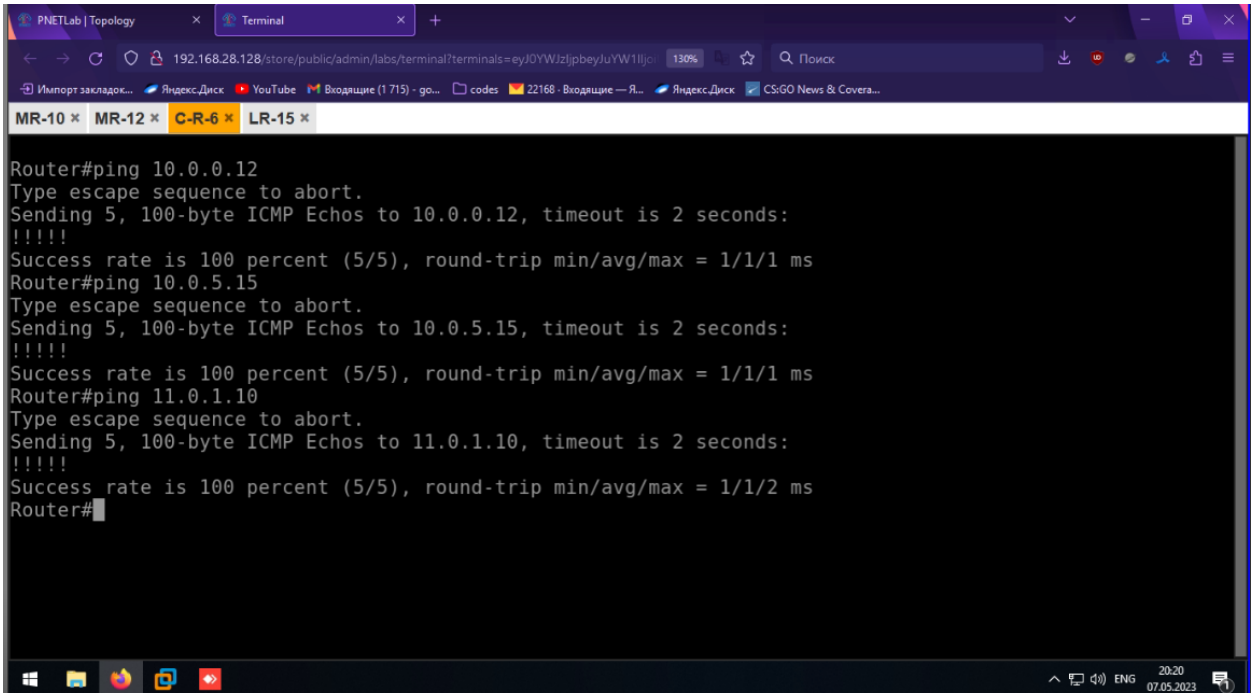


Рис. 7 Пинг с сети 12.0.1.0 на сети 10.0.5.0, 11.0.1.0, 10.0.0.0

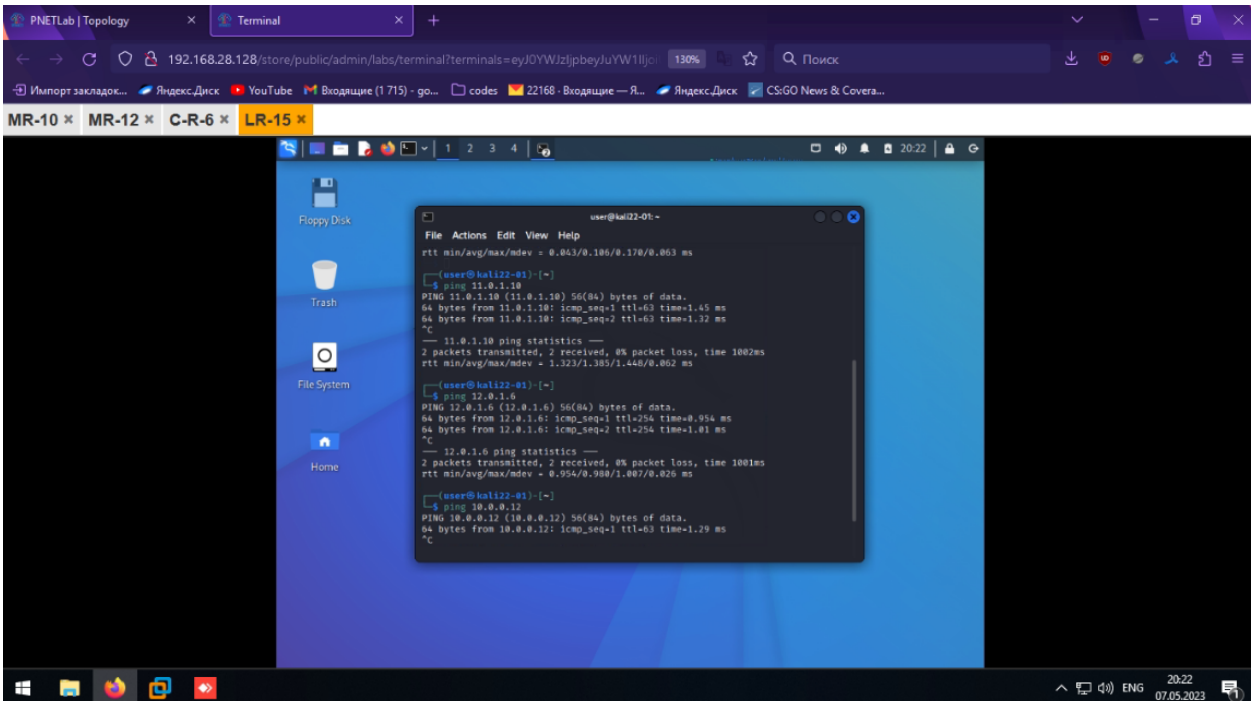


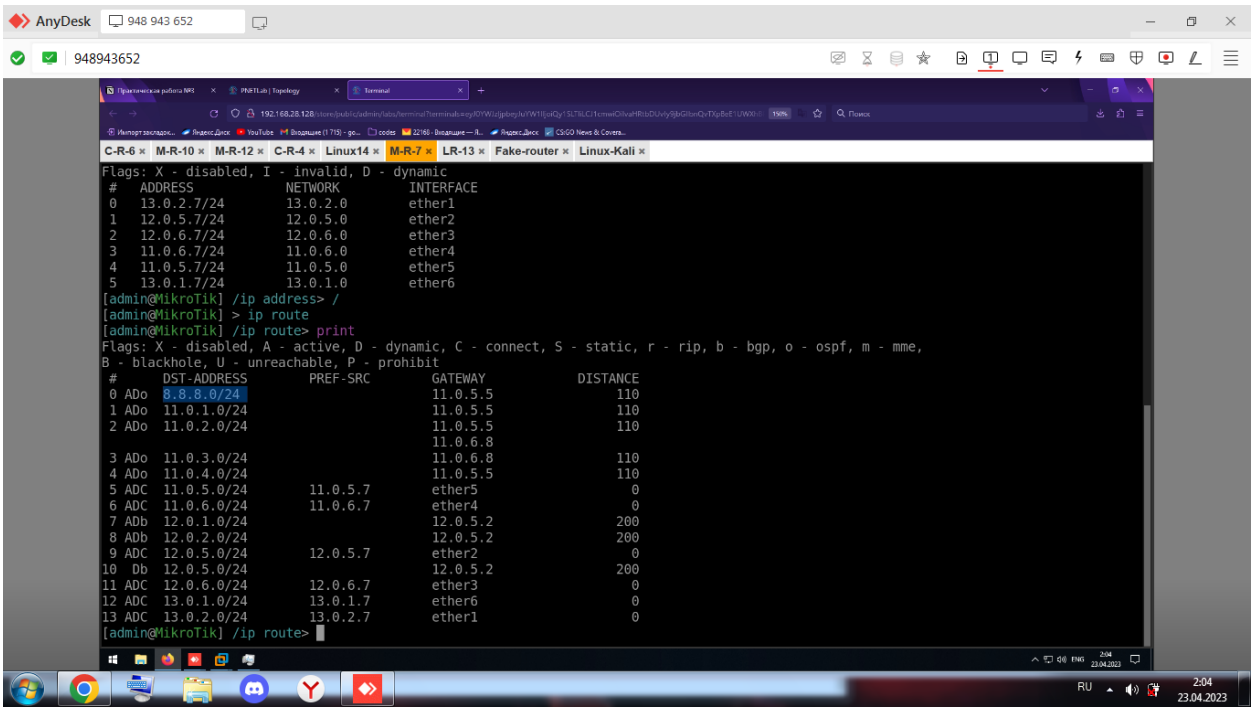
Рис. 8 Пинг с сети 10.0.5.0 на сети 12.0.1.0, 11.0.1.0, 10.0.0.0

Оптимальный вариант для атаки на домен OSPF — это получение контроля над легитимным маршрутизатором в сети.

Поэтому мы создали «mitm» роутер и подключились к домену, перед этим првоели анализ мультикастовых пакетов OSPF и изучили следующие параметры в пакете:

- OSPF Hello Interval;
- OSPF Dead Interval;
- наличие аутентификации.

- Скрин успешной атаки на OSPF (получен fake маршрут)



В контексте атаки на OSPF была рассмотрена инъекция маршрута с перехватом трафика.

Мы включали редистрибуцию статических маршрутов с наименьшей метрикой, чтобы у внедрённого маршрута была самая низкая стоимость.

- Провести атаку с подменой маршрута в зоне BGP*

Встраивание в уже созданную BGP сессию.

Можно использовать обычные IP Spoofing + TCP hijacking атаки для того, чтобы попробовать направить всё общение между двумя роутерами через роутер MITM.

Для начала нужно определить цели, точнее нам известен ip-адрес какого-то BGP роутера, который очевидно общается с другими, так что возникает вопрос, как можно узнать его соседей. Это возможно сделать с помощью

Public Route Servers, где можно найти записи о том, от какого роутера к какому идёт трафик.

После того, как был получен доступ к роутеру всё будет зависеть от настроек его соседей. Есть вероятность, что этому роутеру доверяют все его соседи, а им — их соседи и т.п., так можно несанкционированно поменять пути из целых сетевых сегментов и манипулировать огромными объемами трафика. А возможно, что через этот роутер можно будет изменить пути только в сети, в которой он находиться (или в автономной системе этого роутера).

Для начала надо определить, из каких AS у нас наиболее вероятен перехват трафика, а это, как правило, соседние AS относительно той, в которой находиться BGP-роутер. Принадлежность определенного IP к AS и соседи определенной AS могут быть получены различными сервисами, например, тот же ipinfo.io.