

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 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

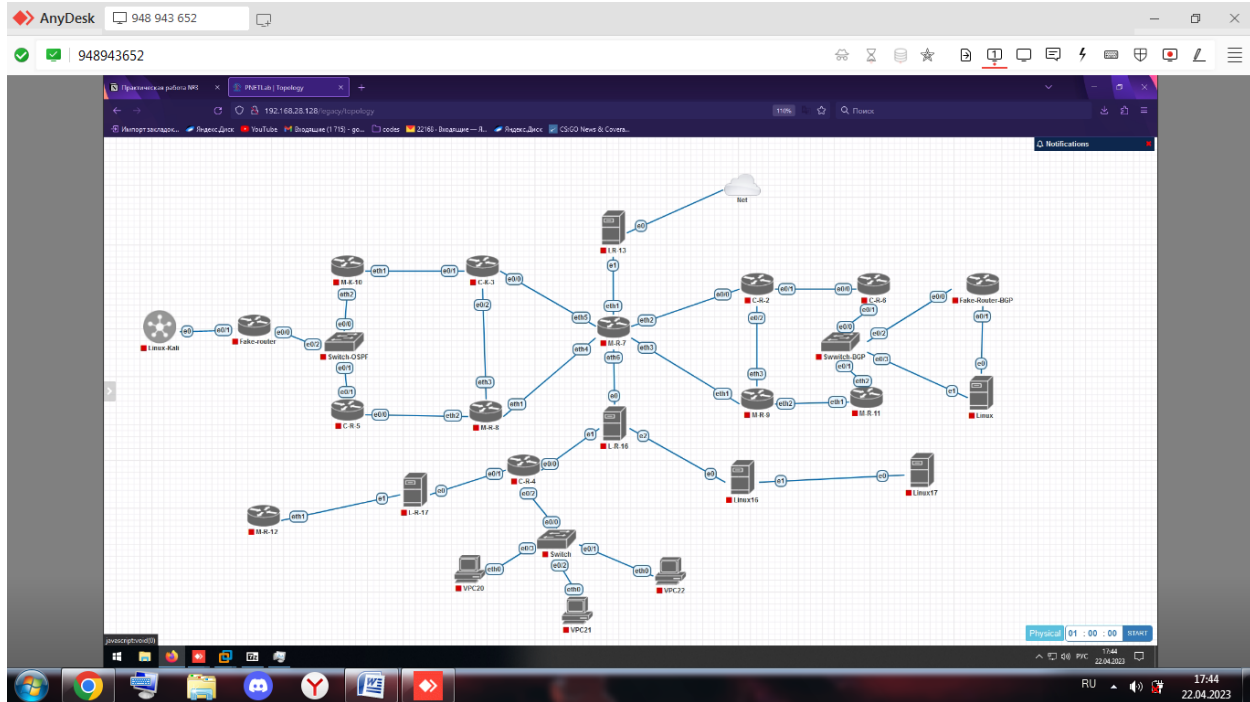


Рис. 1 Исходная схема

```

C-R-2 > configure
Enter configuration commands, one per line. End with CTRL-Z (no newline)
!
0041 0400 00FF FA01 0400 0100 01
ip address 12.0.1.2 255.255.255.0
!
interface Ethernet0/2
ip address 12.0.2.2 255.255.255.0
!
interface Ethernet0/3
no ip address
!
router bgp 100
bgp log-neighbor-changes
redistribute connected
neighbor 12.0.1.6 remote-as 100
neighbor 12.0.2.9 remote-as 100
neighbor 12.0.5.7 remote-as 100
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
--More--
*Apr 22 22:13:22.766: %BGP-5-NBR RESET: Neighbor 12.0.2.9 active reset (BGP Notification sent)
*Apr 22 22:13:22.768: %BGP-5-ADJCHANGE: neighbor 12.0.2.9 active Down BGP Notification sent
*Apr 22 22:13:22.768: %BGP_SESSION-5-ADJCHANGE: neighbor 12.0.2.9 IPv4 Unicast topology base removed from session BGP Notification sent
--More--

```

Рис. 2 Конфигурация C-R-2 (iBGP)

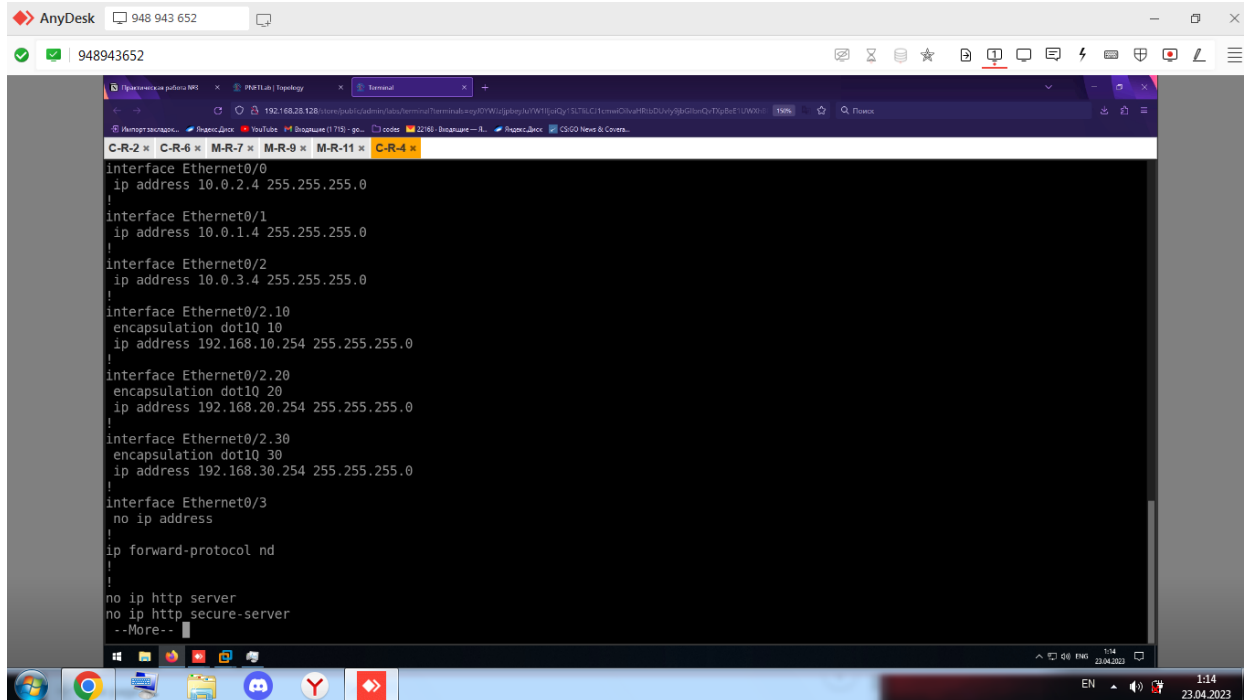


Рис. 3 Конфигурация C-R-4 (Static Routing)

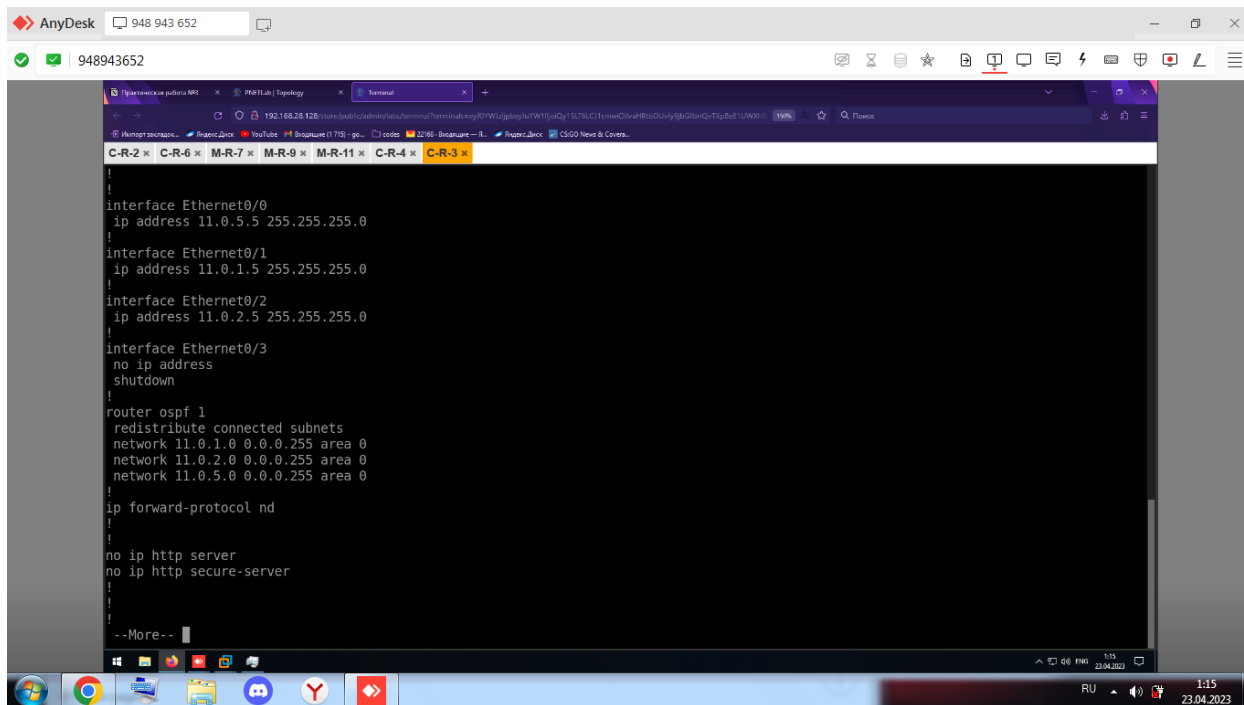


Рис. 4 Конфигурация C-R-3 (OSPF)

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

```

[admin@MikroTik] > ping 10.0.0.12
  SEQ HOST                      SIZE TTL TIME  STATUS
    0 10.0.0.12                  56  63 2ms
    1 10.0.0.12                  56  63 1ms
  sent=2 received=2 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=2ms

[admin@MikroTik] > ping 10.0.5.15
  SEQ HOST                      SIZE TTL TIME  STATUS
    0 10.0.5.15                  56  63 1ms
    1 10.0.5.15                  56  63 1ms
  sent=2 received=2 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms

[admin@MikroTik] > ping 12.0.1.6
  SEQ HOST                      SIZE TTL TIME  STATUS
    0 12.0.1.6                   56 254 1ms
    1 12.0.1.6                   56 254 1ms
    2 12.0.1.6                   56 254 1ms
  sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms

[admin@MikroTik] >
  
```

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

The screenshot shows a terminal window titled "Terminal" within the PNETLab interface. The browser address bar shows "192.168.28.128/store/public/admin/labs/terminal?terminals=eyJ0YWZlZjpbeyJuYW11Ijoi". The terminal tabs are "MR-10", "MR-12", "C-R-6", and "LR-15". The terminal content shows the following commands and results:

```
[admin@MikroTik] > ping 10.0.5.15
  SEQ HOST                                SIZE TTL TIME  STATUS
    0 10.0.5.15                          56  63  1ms
    1 10.0.5.15                          56  63  1ms
  sent=2 received=2 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms

[admin@MikroTik] > ping 11.0.1.10
  SEQ HOST                                SIZE TTL TIME  STATUS
    0 11.0.1.10                          56  63  1ms
    1 11.0.1.10                          56  63  1ms
  sent=2 received=2 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms

[admin@MikroTik] > ping 12.0.1.6
  SEQ HOST                                SIZE TTL TIME  STATUS
    0 12.0.1.6                          56 254  1ms
    1 12.0.1.6                          56 254  1ms
    2 12.0.1.6                          56 254  1ms
  sent=3 received=3 packet-loss=0% min-rtt=1ms avg-rtt=1ms max-rtt=1ms

[admin@MikroTik] >
```

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

The screenshot shows a terminal window titled "Terminal" within the PNETLab interface. The browser address bar shows "192.168.28.128/store/public/admin/labs/terminal?terminals=eyJ0YWZlZjpbeyJuYW11Ijoi". The terminal tabs are "MR-10", "MR-12", "C-R-6", and "LR-15". The terminal content shows the following commands and results:

```
Router#ping 10.0.0.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router#ping 10.0.5.15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.5.15, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router#ping 11.0.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.0.1.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Router#
```

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

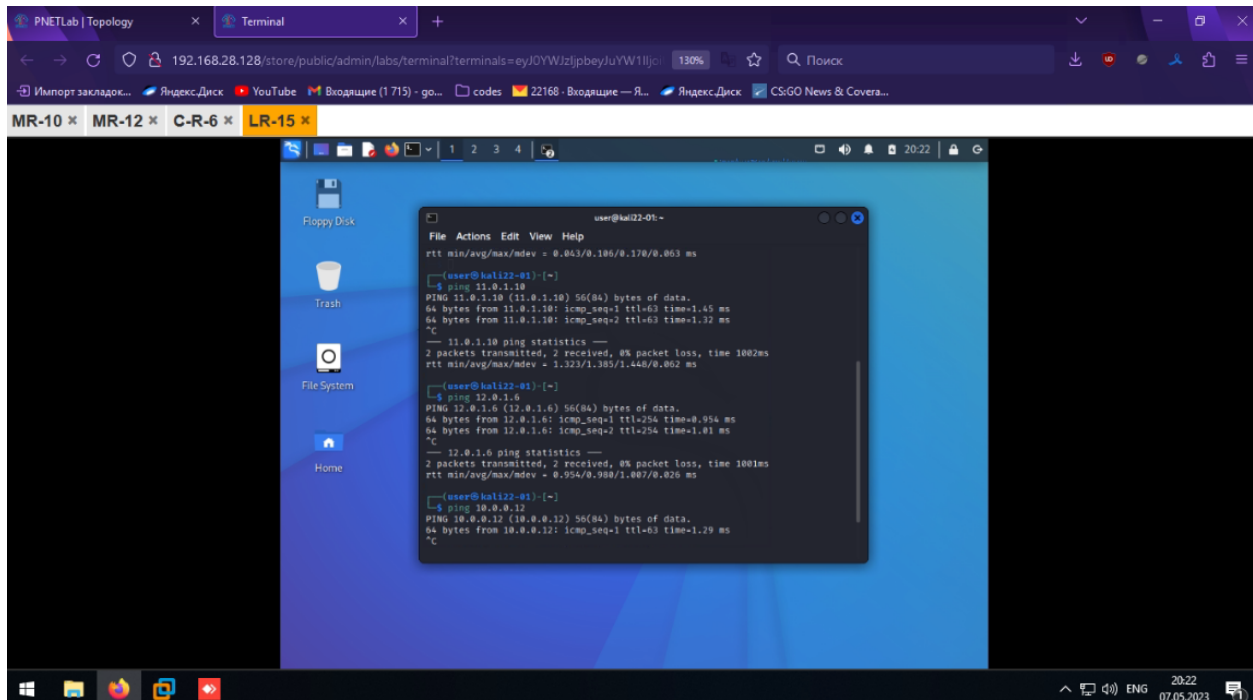
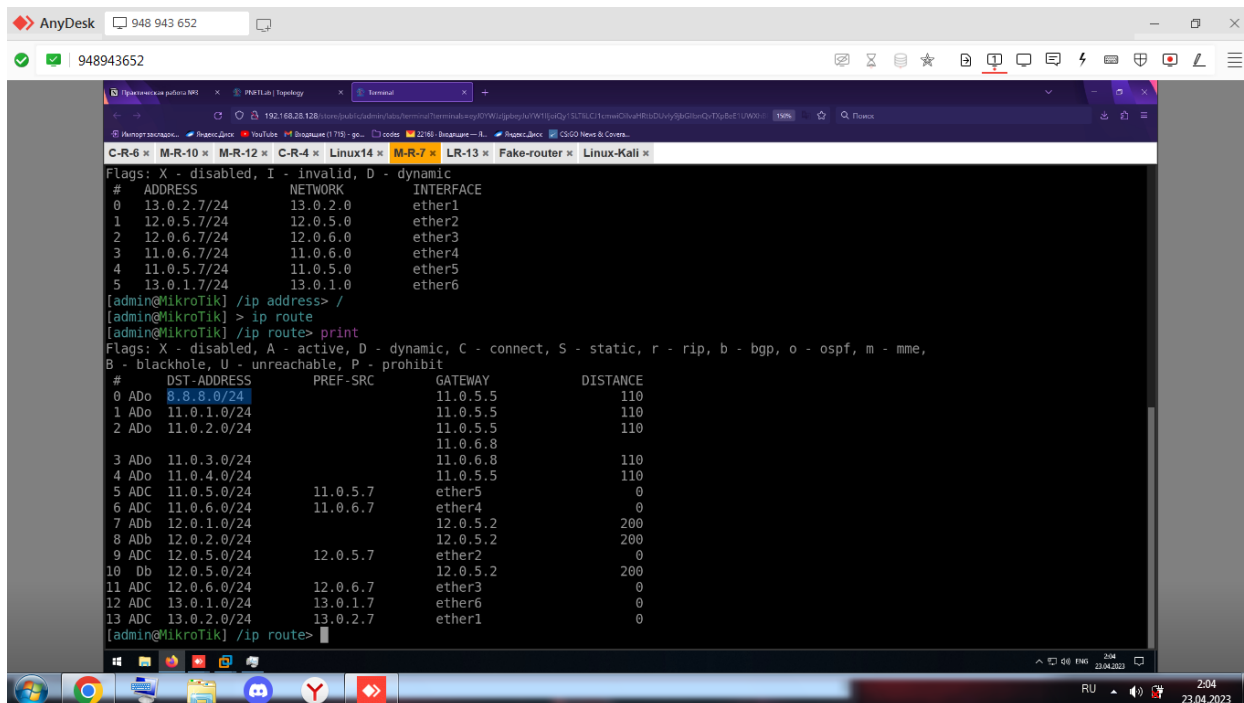


Рис. 8 Пинг с сети 10.0.5.0 на сети 12.0.1.0, 11.0.1.0, 10.0.0.0

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 провели 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 находится (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 находится BGP-роутер. Принадлежность определенного IP к AS и соседи определенной AS могут быть получены различными сервисами, например, тот же ipinfo.io.