МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

ОТЧЕТ

по лабораторной работе №2

по дисциплине

«Сети и телекоммуникации»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_ Гай. В.Е\_\_

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_ Папанов Р.В

(подпись) (фамилия, и.,о.)

\_\_\_\_\_\_19-В-1\_\_\_\_\_\_\_\_

(шифр группы)

Работа защищена «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

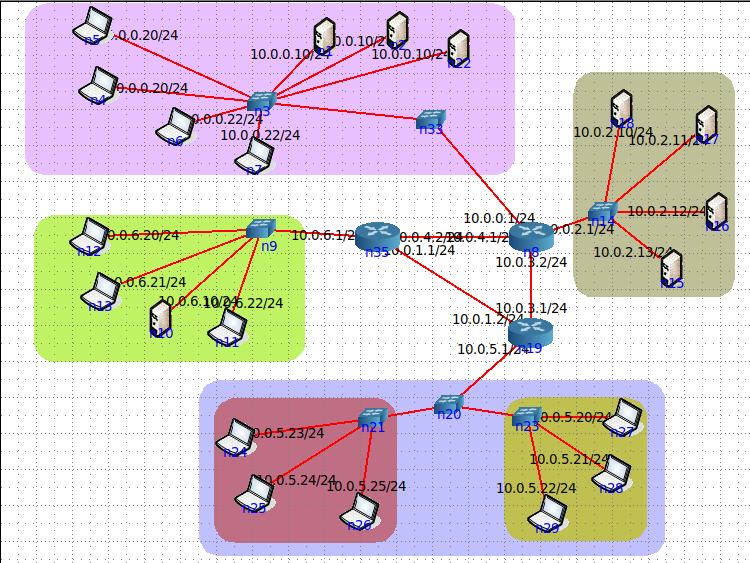
Нижний Новгород 2022

**Задание на лабораторную работу**

1. На выданной в качестве варианта схеме найти и устранить некорректные адреса сетей. Привести в отчёте доказательства наличия некорректных IP-адресов и особенности работы сети при их наличии. Привести в отчёте схему, полученную в результате устранения неисправностей, доказать, что в результате их устранения сеть работает в нормальном режиме. Привести в отчёте команды, с помощью которых можно исправить ошибки в настройках сети.
2. На выданной в качестве варианта схеме найти компьютеры, IP-адреса которых выходят за пределы диапазона допустимых IP-адресов заданной маски. На основании полученных результатов вычислить допустимую для подсети маску. Привести в отчёте доказательства наличия неисправности. Привести в отчёте результат правильного выбора маски и доказать, что в результате устранения неисправности сеть работает в нормальном режиме. Привести в отчёте команды, с помощью которых можно исправить ошибки в настройках сети.
3. На выданной в качестве варианта схеме найти и устранить ошибку в настройке сетевого адаптера машины. Привести в отчёте доказательства наличия ошибки и особенности работы сети при её наличии. Привести в отчёте исправленные настройки сетевого адаптера и схему, полученную в результате исправления настроек. Доказать, что в результате устранения ошибки сеть работает в нормальном режиме. Привести в отчёте команды, с помощью которых можно исправить ошибки в настройках сети.
4. На выданной в качестве варианта схеме найти компьютеры с конфликтом IP-адресов. На основании полученных результатов изменить IP-адрес на допустимый. Привести в отчёте доказательства наличия неисправности. Привести в отчёте результат верного выбора IP- адресов (с учётом маски сети) и доказать, что в результате устранения неисправности сеть работает в нормальном режиме. Привести в отчёте команды, с помощью которых можно исправить ошибки в настройках сети.

**6qo0kp6k – конфликт IP-адресов**

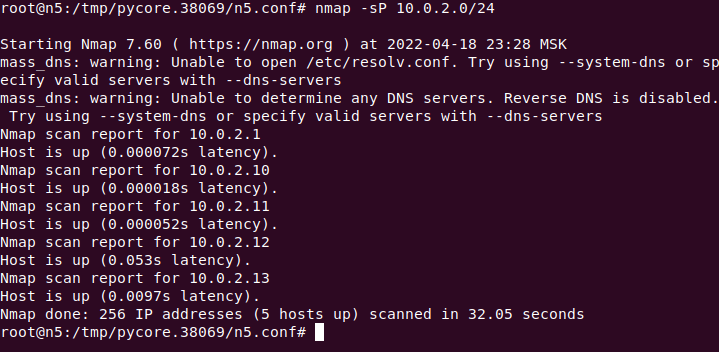
Схема сети:



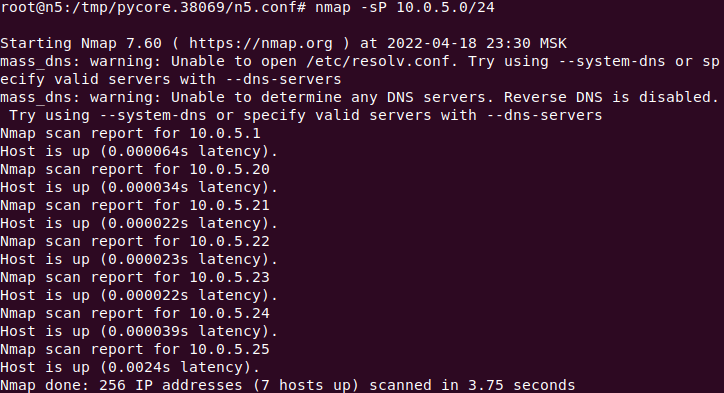
Для поиска неисправностей будет использоваться сканер портов nmap. С опцией -sP можно провести пинг сканирование целой сети.

Сканировать будем с узла 10.0.0.20/24.

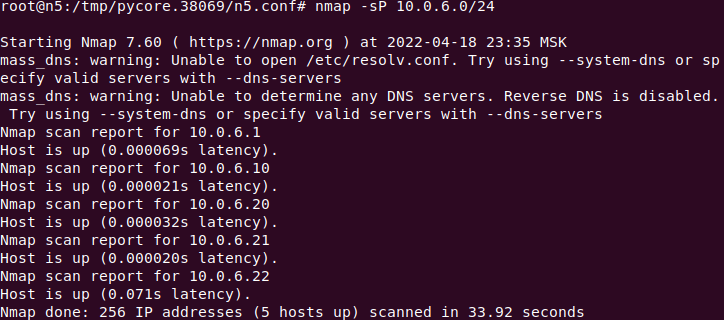
Сеть 10.0.2.0/24 — на схеме 5 узлов, обнаружено 5 узлов:



Сеть 10.0.5.0/24 — на схеме 7 узлов, обнаружено 7:



Сеть 10.0.6.0/24 — на схеме 5 узлов, обнаружено 5:



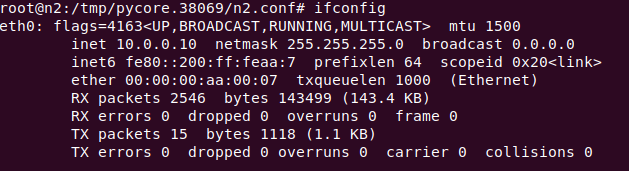
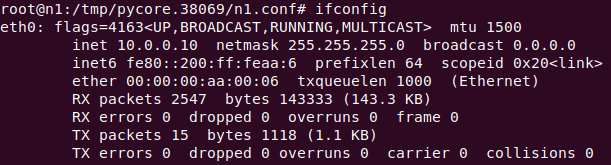
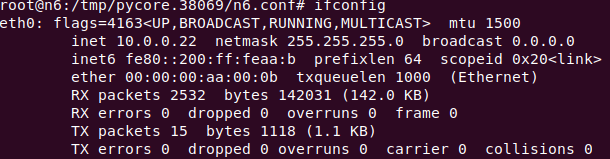
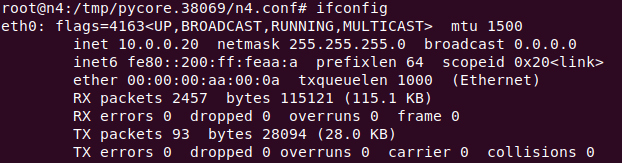
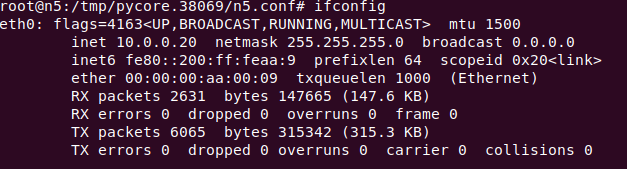
Теперь осталось проверить последнюю сеть 10.0.0.0/24 с исправного компьютера из другой сети, например 10.0.6.20/24:

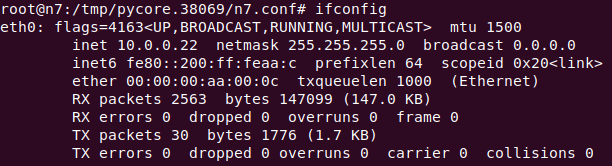
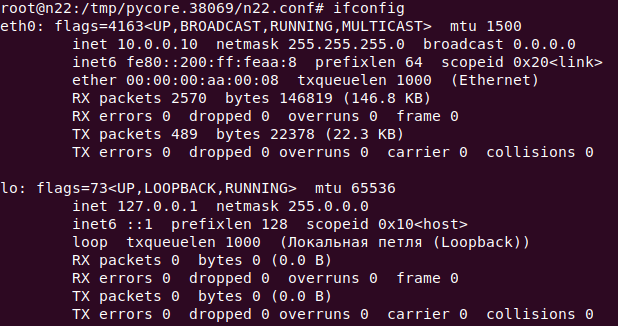
Сеть 10.0.0.0/24 – на схеме 8 узлов, обнаружено 4 – имеются проблемы:



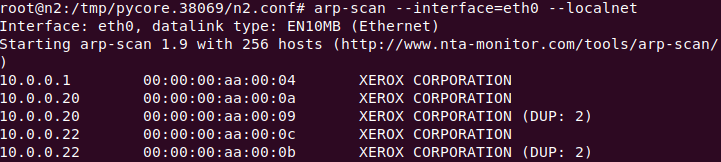
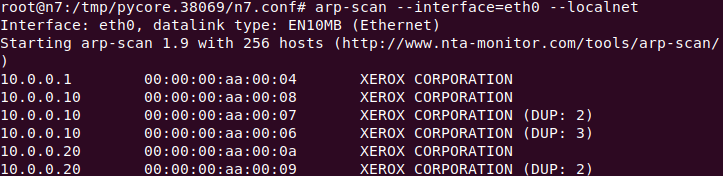
Проблема имеется в сети 10.0.0.0/24

С помощью утилиты ifconfig узнаем IP каждого компьютера и составим таблицу соответствий





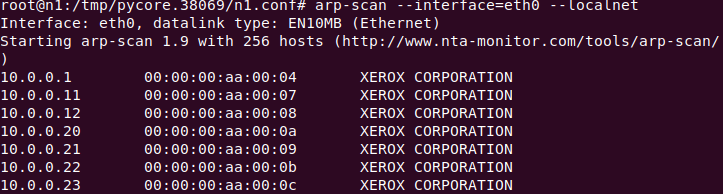
|  |  |
| --- | --- |
| ***Компьютер*** | ***IP адрес/маска*** |
| n1 | 10.0.0.10/24 |
| n2 | **10.0.0.10/24** |
| n4 | 10.0.0.20/24 |
| n5 | **10.0.0.20/24** |
| n6 | 10.0.0.22/24 |
| n7 | **10.0.0.22/24** |
| n22 | **10.0.0.10/24** |

Как можем заметить, повторяющие IP-адреса имеют компьютеры: n1 совпадает с n2 и n22, n4 - n5 и n6 -n7. 

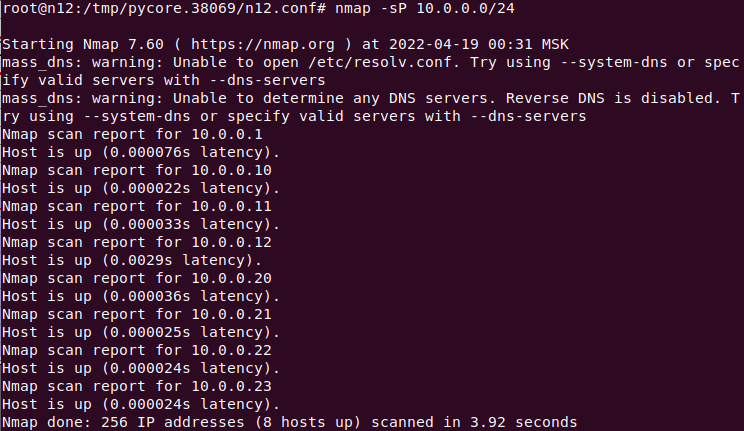
Так как маска подсети 24, то можно выбрать любой адрес из диапазона 10.0.0.1-10.0.0.254 (10.0.0.0 — сеть, 10.0.0.255 — широковещательный, 10.0.0.10, 10.0.0.20,10.0.0.22 уже заняты). Установим адреса: 10.0.0.11/24 для n2, 10.0.0.12/24 для n22, 10.0.0.21/24 для n5, 10.0.0.23/24 для n7:

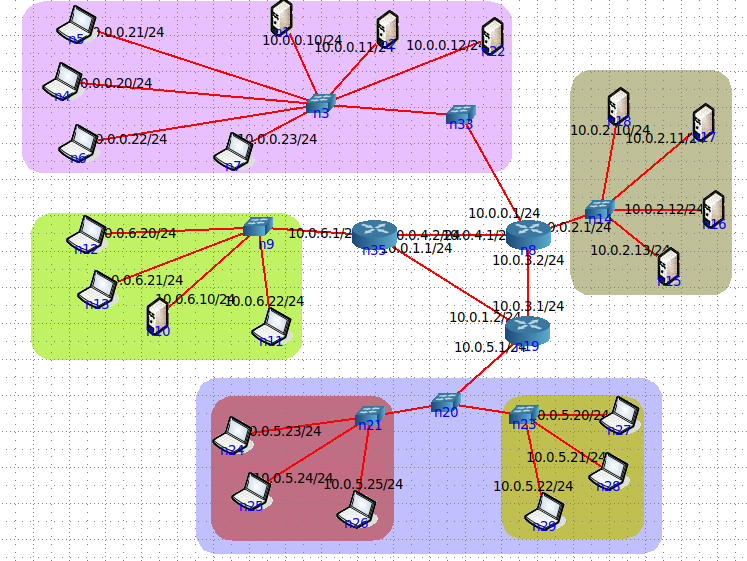


Конфликт IP-адресов пропал:



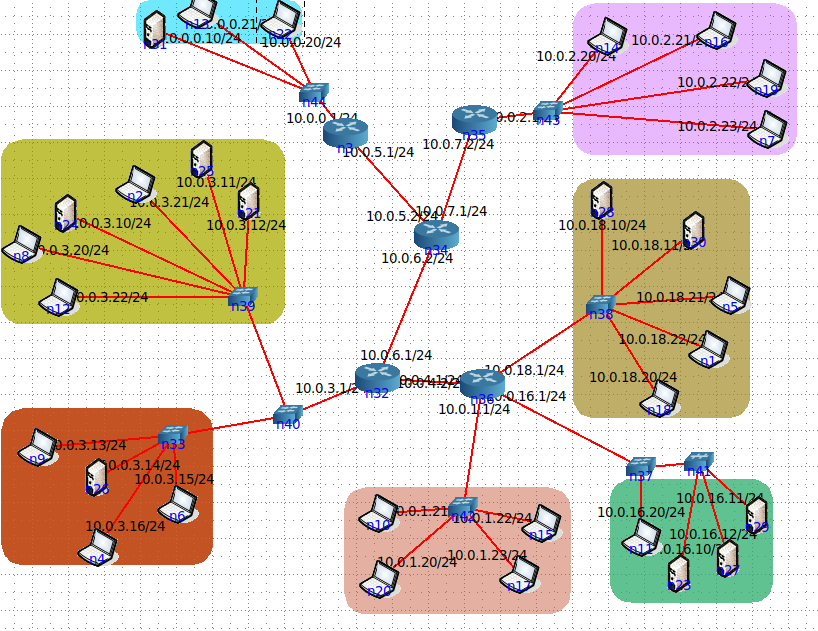
Теперь при использовании утилиты nmap отображаются все 8 узлов:





**076nkk1g - не настроен шлюз по умолчанию**

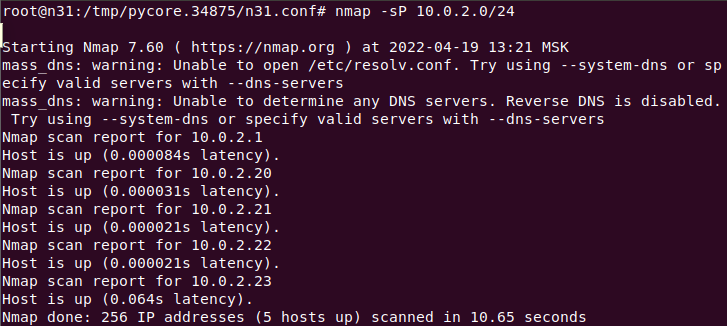
Схема сети:



С помощью утили nmap найдет проблемные компьютеры.

Начнем сканировать с узла 10.0.0.10/24:

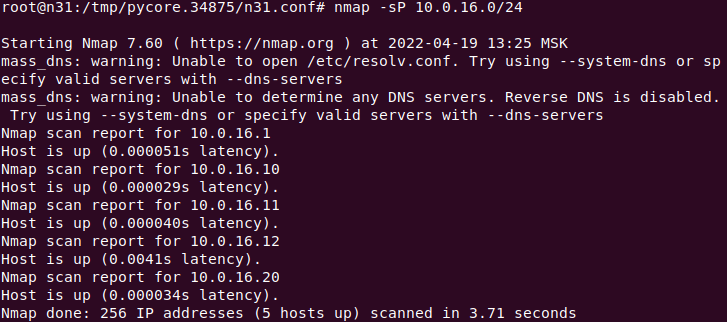
Сеть 10.0.2.0/24 – на схеме 5 узлов, обнаружено - 5:



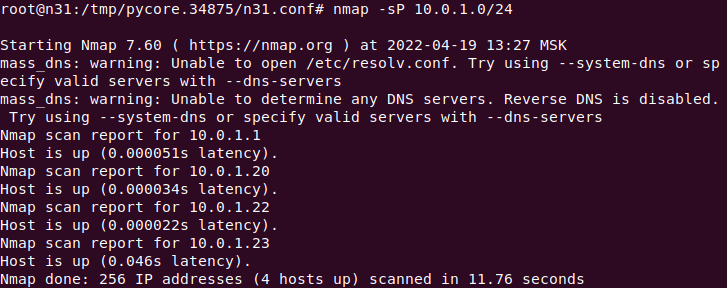
Сеть 10.0.18.0/24 – на схеме 6 узлов, обнаружено - 6:



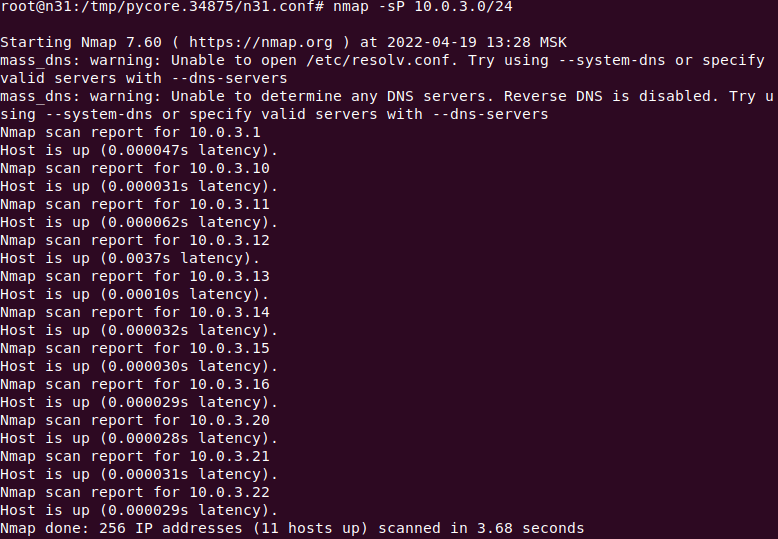
Сеть 10.0.16.0/24 – на схеме 5 узлов, обнаружено - 5:



Сеть 10.0.1.0/24 – на схеме 5 узлов, обнаружено – 4 – имеются проблемы:

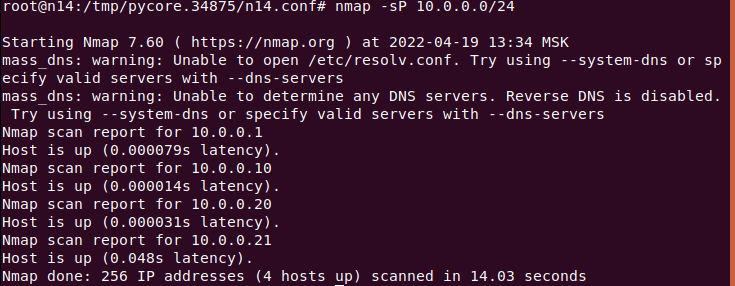


Сеть 10.0.3.0/24 – на схеме 11 узлов, обнаружено – 11:



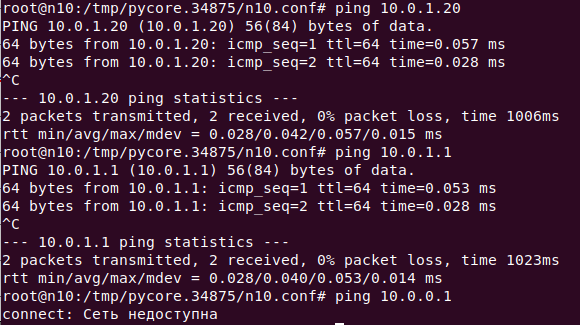
Теперь проверим сеть 10.0.0.0/24 с компьютера 10.0.2.20/24:

Сеть 10.0.0.0/24 – на схеме 4 узла, обнаружено – 4:



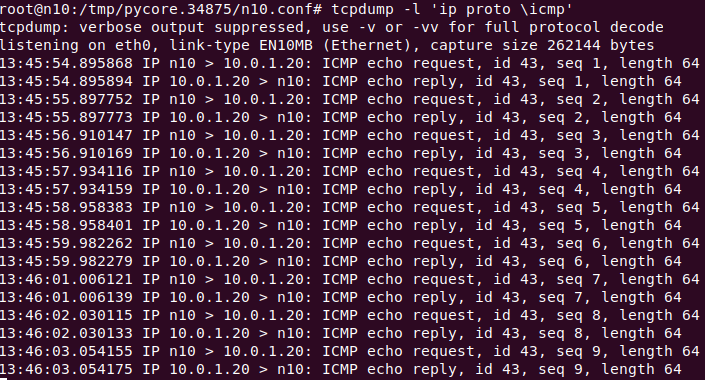
Проблемы имеются у компьютера 10.0.1.21/24.

Пинг проходит от 10.0.1.21/24 к компьютерам внутри сети, но ко внешним нет, так как «сеть недоступна».



Аналогично, если из другой сети пинговать этот компьютер.

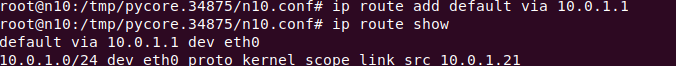
Если использовать анализатор пакетов, например, tcpdump, то видно, что проблемный компьютер не может ответить на ICMP реквест, если он идет из другой сети, однако, если пинг идет из локальной сети, то компьютер отвечает на реквесты:



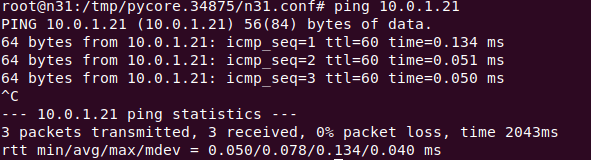
При помощи команды ip route show можно обнаружить, что не настроен шлюз по умолчанию:



Настроем его:

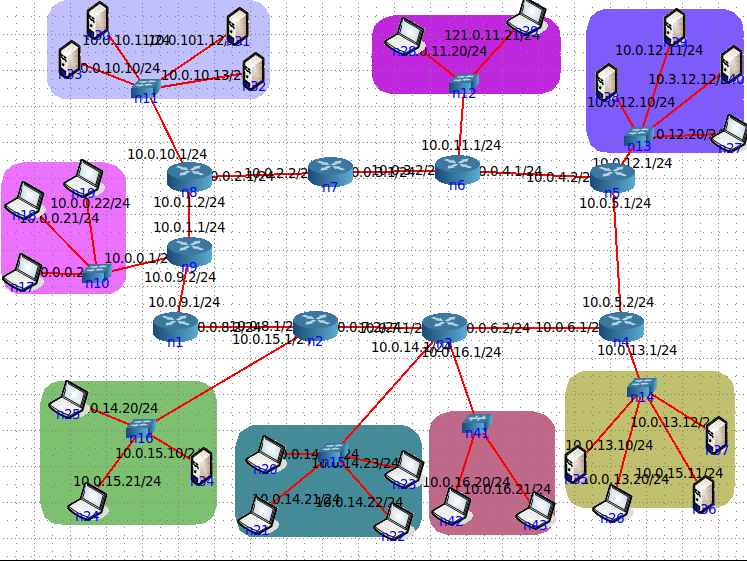


Теперь пинг из внешнего компьютера 10.0.0.10/24 проходит к 10.0.1.21



**85q1k3x3 – некорректные адреса сетей**

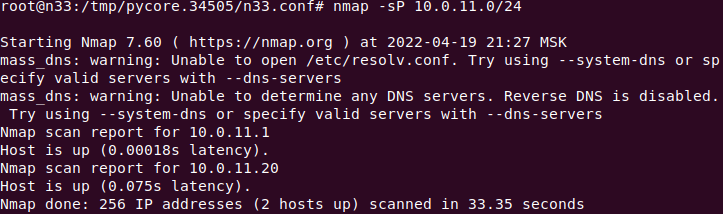
Схема сети:



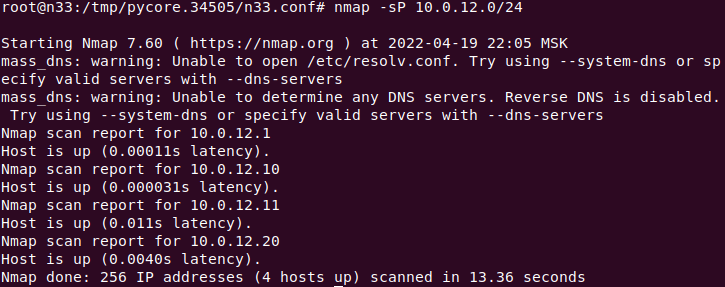
С помощью утили nmap найдет проблемные компьютеры.

Начнем сканировать с узла 10.0.10.10/24.

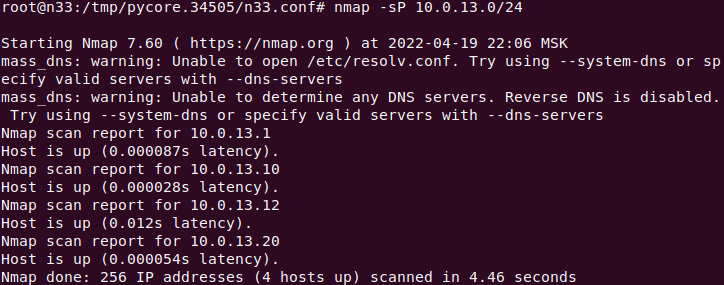
Сеть 10.0.11.0 – на схеме 3 узла, обнаружено – 2:



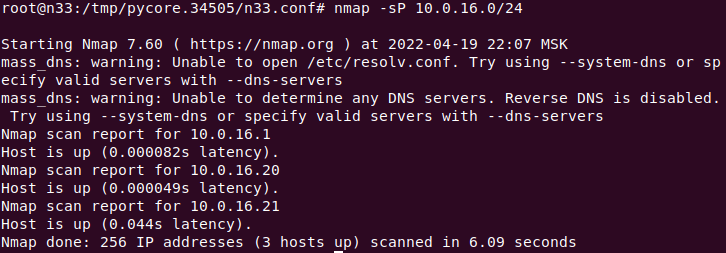
Сеть 10.0.12.0 – на схеме 5 узлов, обнаружено – 4:



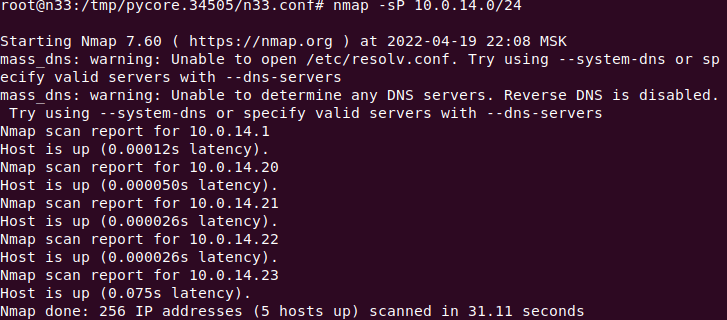
Сеть 10.0.13.0 – на схеме 5 узлов, обнаружено – 4:



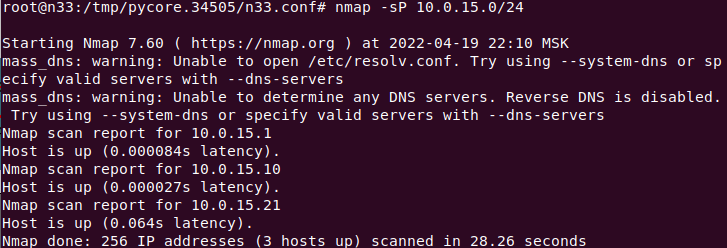
Сеть 10.0.16.0 – на схеме 3 узла, обнаружено – 3:



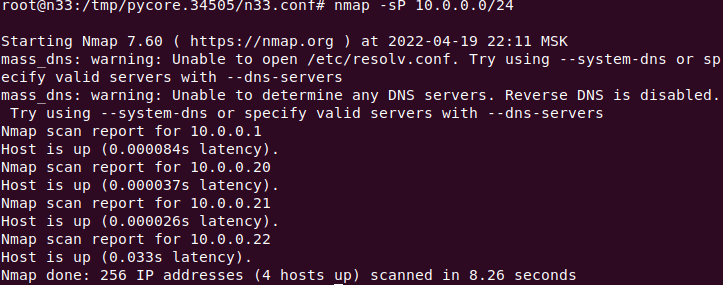
Сеть 10.0.14.0 – на схеме 5 узлов, обнаружено – 5:

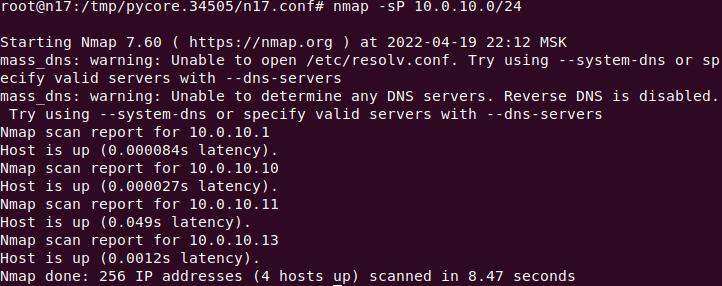


Сеть 10.0.15.0 – на схеме 4 узла, обнаружено – 3:



Сеть 10.0.0.0 – на схеме 4 узла, обнаружено – 4:



Проверим сеть 10.0.10.0 с узла 10.0.0.20/24 – на схеме 5 узлов, обнаружено – 4: 

Имеются проблемы в следующих сетях:

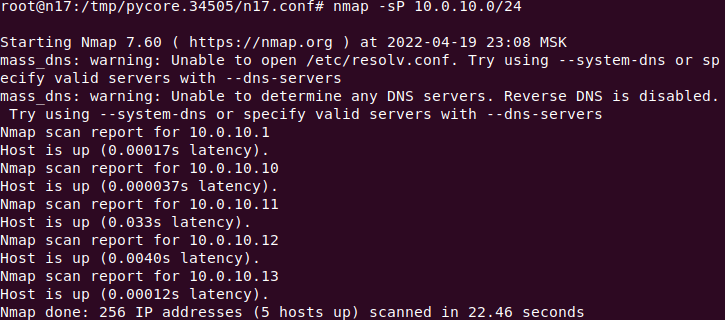
* 10.0.10.0
* 10.0.15.0
* 10.0.13.0
* 10.0.12.0
* 10.0.11.0

Составим таблицу IP адресов, масок подсетей и то, какие адреса и маски нужно изменить:

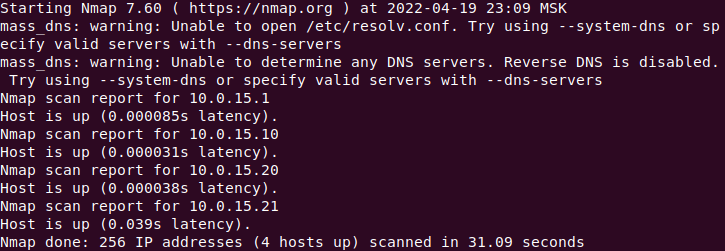
|  |  |
| --- | --- |
| n30 | 10.0.10.11/24 |
| n31 | 10.0.101.12/24 →10.0.10.12/24 |
| n32 | 10.0.10.13/24 |
| n33 | 10.0.10.10/24 |
| n28 | 10.0.11.20/24 |
| n29 | 121.0.11.21/24 → 10.0.11.21/24 |
| n38 | 10.0.12.10/24 |
| n39 | 10.0.12.11/24 |
| n40 | 10.3.12.12/24 → 10.0.12.12/24 |
| n27 | 10.0.12.20/24 |
| n35 | 10.0.13.10/24 |
| n36 | 10.0.15.11/24 → 10.0.13.11/24 |
| n37 | 10.0.13.12/24 |
| n26 | 10.0.13.20/24 |
| n24 | 10.0.14.20/24 → 10.0.15.20/24 |
| n25 | 10.0.15.10/24 |
| n34 | 10.0.15.21/24 |

Повторим проверку сетей у которых раннее наблюдались проблемы с узла 10.0.0.20/24:

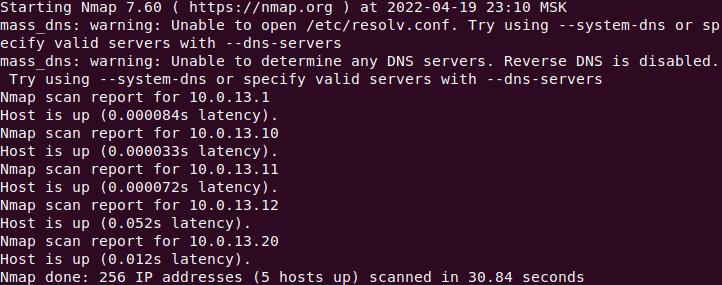
Сеть 10.0.10.0 – на схеме 5 узлов, обнаружено – 5:



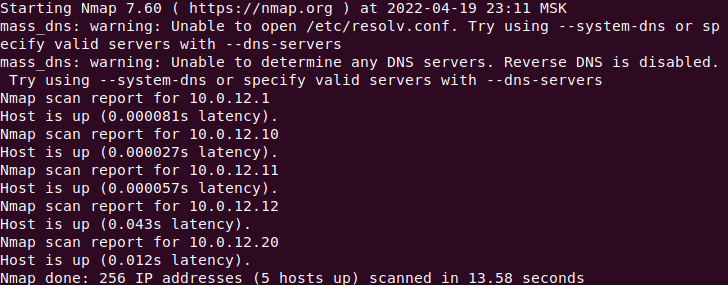
Сеть 10.0.15.0 – на схеме 4 узла, обнаружено – 4:



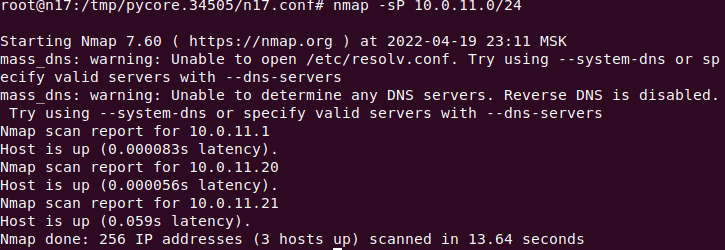
Сеть 10.0.13.0 – на схеме 5 узлов, обнаружено – 5:



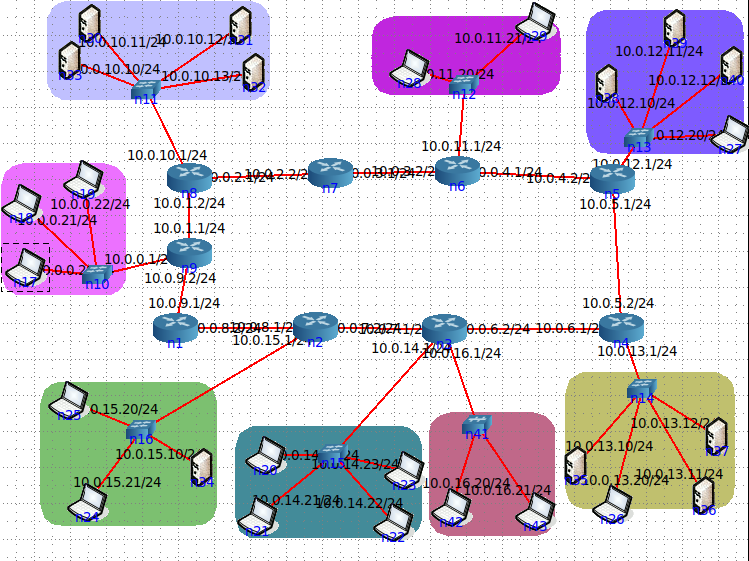
Сеть 10.0.12.0 – на схеме 5 узлов, обнаружено – 5:



Сеть 10.0.11.0 – на схеме 3 узла, обнаружено – 3:

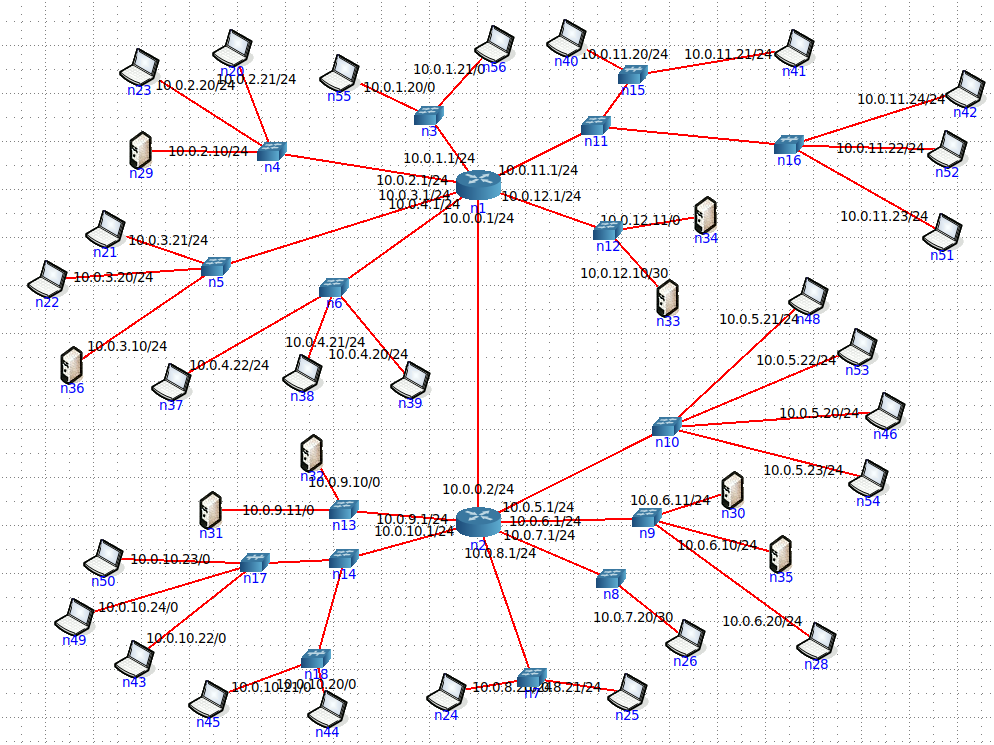


Ранее не обнаруженные компьютеры, теперь видны при использование утилиты nmap.

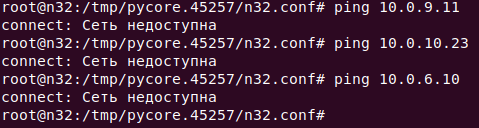


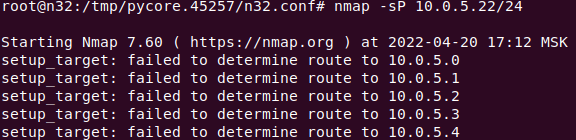
**ynaco3vo- неверно указаная маска подсети**

Схема сети:



Проверим от узла 10.0.9.10/0 к компьютерам в своей сети и в чужой, в обоих случаях получаем ответ «сеть недоступна»:



С помощью утилиты nmap, не получается обнаружить компьютеры: 

С помощью команды ifconfig узнаем IP адрес и маску подсети каждого компьютера и роутера. Для удобства приведем данные в таблице:

|  |  |
| --- | --- |
| n20 | 10.0.2.21/24 |
| n23 | 10.0.2.20/24 |
| n29 | 10.0.2.10/24 |
| n1 | 10.0.2.1/24 |
| n55 | 10.0.1.20/0 |
| n56 | 10.0.1.21/0 |
| n1 | 10.0.1.1/24 |
| n40 | 10.0.11.20/24 |
| n41 | 10.0.11.21/24 |
| n42 | 10.0.11.24/24 |
| n52 | 10.0.11.22/24 |
| n51 | 10.0.11.23/24 |
| n1 | 10.0.11.1/24 |
| n21 | 10.0.3.21/24 |
| n22 | 10.0.3.20/24 |
| n36 | 10.0.3.10/24 |
| n1 | 10.0.3.1/24 |
| n37 | 10.0.4.22/24 |
| n38 | 10.0.4.21/24 |
| n39 | 10.0.4.20/24 |
| n1 | 10.0.4.1/24 |
| n34 | 10.0.12.11/0 |
| n33 | 10.0.12.10/30 |
| n1 | 10.0.12.1/24 |
| n1 | 10.0.0.1/24 |
| n2 | 10.0.0.2/24 |
| n32 | 10.0.9.10/0 |
| n31 | 10.0.9.11/0 |
| n2 | 10.0.9.1/24 |
| n50 | 10.0.10.23/0 |
| n49 | 10.0.10.24/0 |
| n43 | 10.0.10.22/0 |
| n45 | 10.0.10.21/0 |
| n44 | 10.0.10.20/0 |
| n2 | 10.0.10.1/24 |
| n24 | 10.0.8.20/24 |
| n25 | 10.0.8.21/24 |
| n2 | 10.0.8.1/24 |
| n26 | 10.0.7.20/30 |
| n2 | 10.0.7.1/24 |
| n30 | 10.0.6.11/24 |
| n35 | 10.0.6.10/24 |
| n28 | 10.0.6.20/24 |
| n2 | 10.0.6.1/24 |
| n48 | 10.0.5.21/24 |
| n53 | 10.0.5.22/24 |
| n46 | 10.0.5.20/24 |
| n54 | 10.0.5.23/24 |
| n2 | 10.0.5.1/24 |

Самое максимальное число, которое встречается в 4 октете — 24, значит под маску подсети можно оставить 32 — 8 = 24, где 2^5 = 32, наиболее близкое к 24 число.

00001010.00000000.00000100.000 **11011**

00001010.00000000.00000011.000 \*\*\*\*\*

00001010.00000000.00000010.000 \*\*\*\*\*

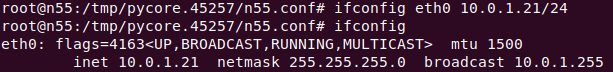
00001010.00000000.00000001.000 \*\*\*\*\*

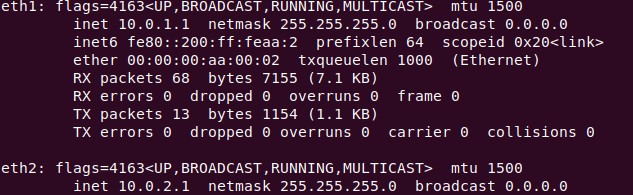
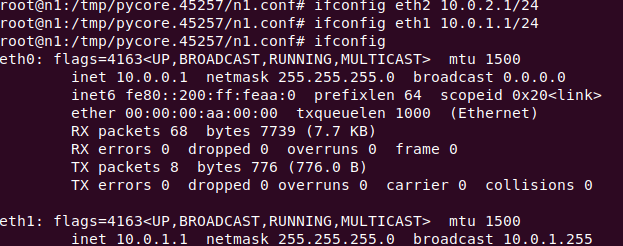
00001010.00000000.00000000.000 \*\*\*\*\*

где левая часть отвечает за сеть, а правая — за узлы внутри этой подсети.

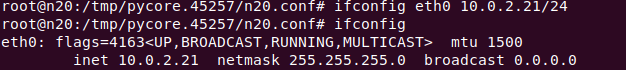
Поменяем маску подсети у n20 и n55 (находятся в разных подсетях) и у роутера n1 и посмотрим на доступность компьютеров:

Компьютер n55:

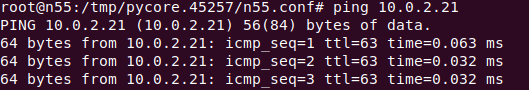


Роутер n1: 

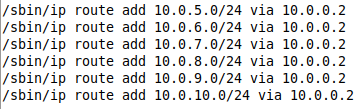
Компьютер n20:



Пинг проходит:

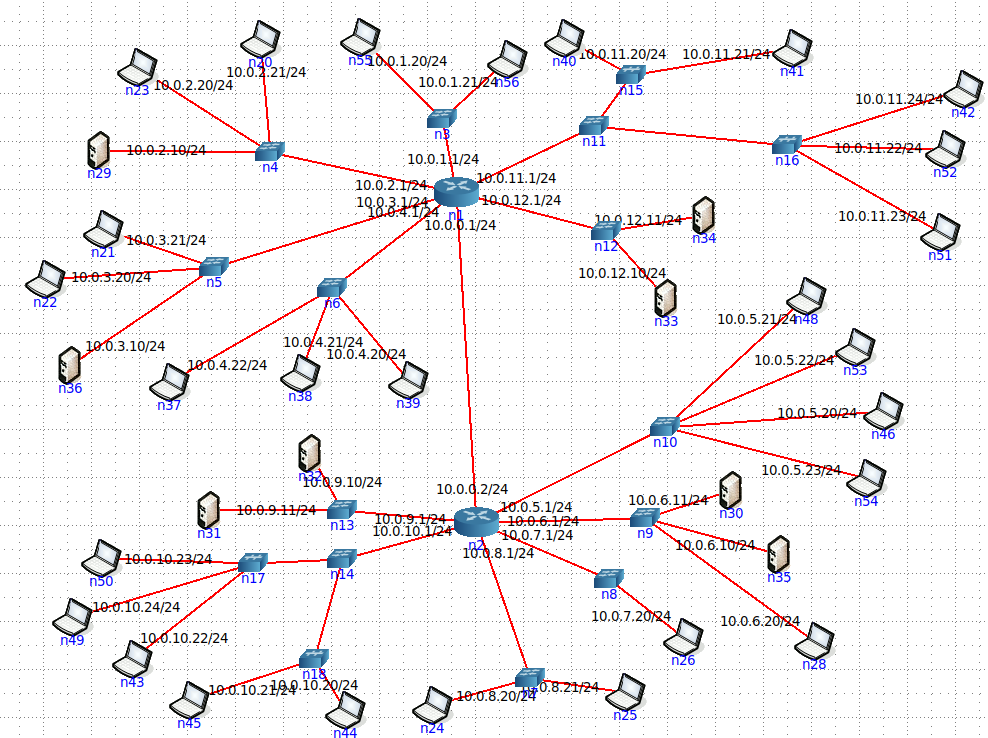


Однако при создании сети, подразумевалось, что маска подсети везде равна 24 (именно такая маска подсети в статичных маршрутах у роутеров):



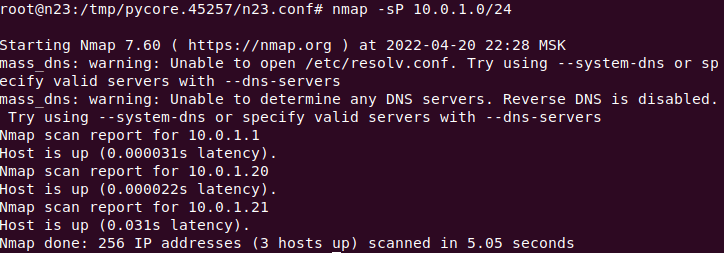
Поэтому сделаем маску подсети везде 24.

Измененные маски подсети:

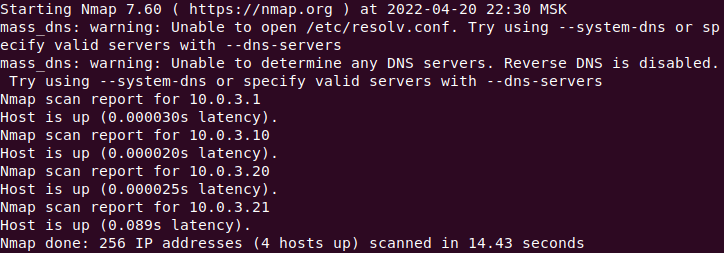


Проверяем сеть с помощью утилиты nmap, с узла 10.0.2.20/24:

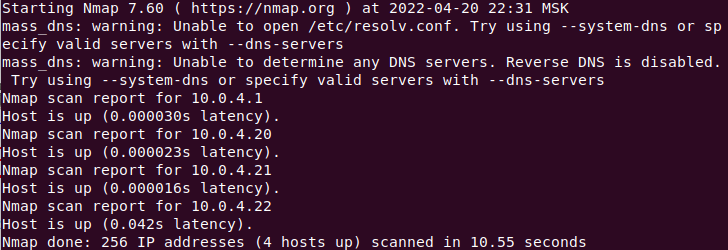
Сеть 10.0.1.0/24 – на схеме 3 узла, обнаружено – 3:



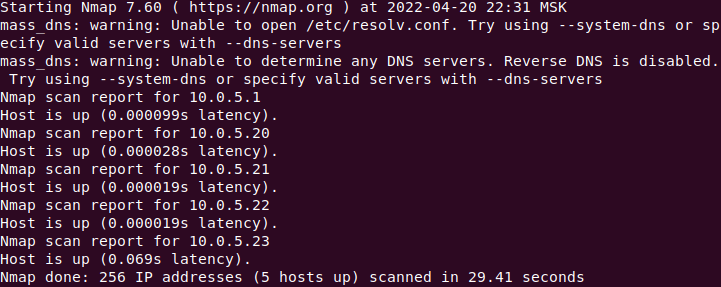
Сеть 10.0.3.0/24 – на схеме 4 узла, обнаружено – 4:



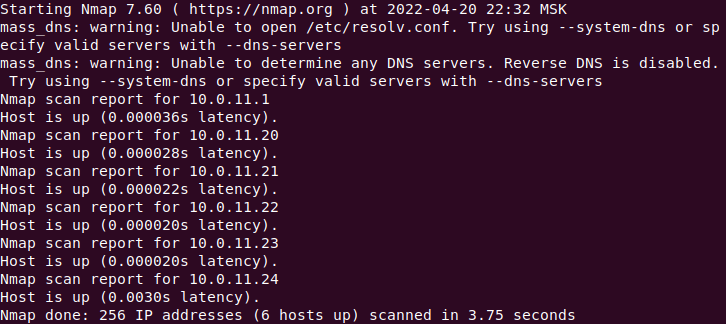
Сеть 10.0.4.0/24 – на схеме 4 узла, обнаружено – 4:



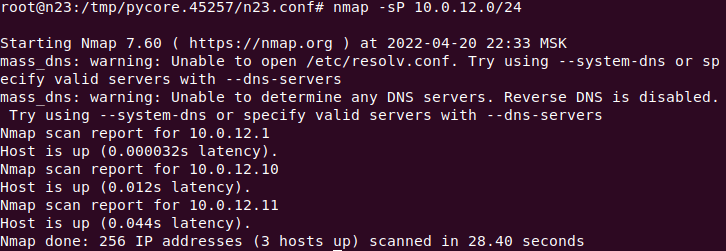
Сеть 10.0.5.0/24 – на схеме 5 узлов, обнаружено – 5:



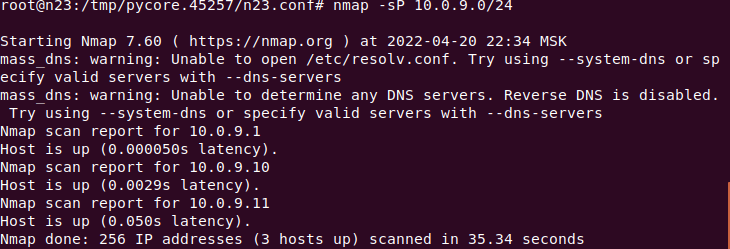
Сеть 10.0.11.0/24 – на схеме 6 узлов, обнаружено – 6:



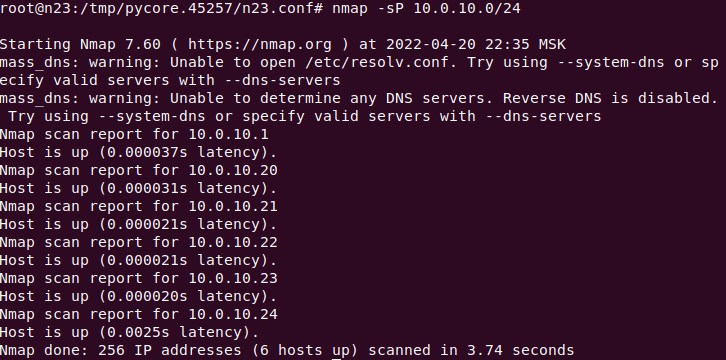
Сеть 10.0.12.0/24 – на схеме 3 узла, обнаружено – 3:



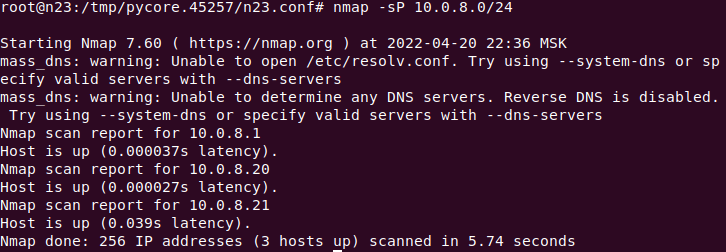
Сеть 10.0.9.0/24 – на схеме 3 узла, обнаружено – 3:



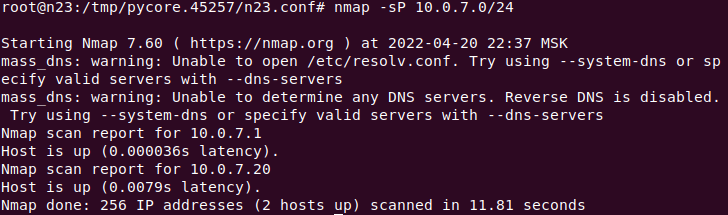
Сеть 10.0.10.0/24 – на схеме 6 узлов, обнаружено – 6:



Сеть 10.0.8.0/24 – на схеме 3 узла, обнаружено – 3:



Сеть 10.0.7.0/24 – на схеме 2 узла, обнаружено – 2:



Сеть 10.0.6.0/24 – на схеме 4 узла, обнаружено – 4:

