|  |  |
| --- | --- |
|  | **Министерство науки и высшего образования Российской Федерации Мытищинский филиал**  **Федерального государственного бюджетного образовательного учреждение**  **высшего образования**  **«Московский государственный технический университет**  **имени Н.Э. Баумана**  **(национальный исследовательский университет)»**  **(МФ МГТУ им. Н.Э. Баумана)** |

ФАКУЛЬТЕТ \_\_\_\_\_\_космический\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

КАФЕДРА \_\_\_\_\_\_\_\_К-3\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**отчет**

***К ЛАБОРАТОРНОЙ РАБОТЕ***

***№3.9***

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

# *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* по ДИСЦИПЛИНЕ

**«Сети эвм и телекоммуникации»**

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

Студент \_\_\_\_К3-73Б\_\_\_\_\_ **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_**Ю.А. Цветков**\_\_\_\_\_\_**

(Группа) (Подпись, дата) (И.О.Фамилия)

Преподаватель **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_**И.И. Гизбрехт**\_\_\_\_\_\_**

(Подпись, дата) (И.О.Фамилия)

*2021 г.*

**Выполнение лабораторной работы**

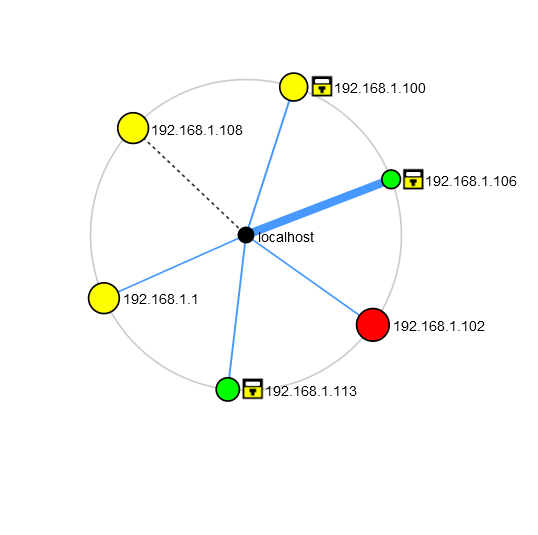
Выполним стандартное сканирование сети с помощью утилиты nmap, используя следующую команду:

nmap -T4 -A -v 192.168.1.1/24

Аргумент -A используется для агрессивного сканирования, он включает определение ОС, определение версий, использование стандартных скриптов для сканирования и трассировку. Аргумент -T4 используется для более быстрого выполнения, -v для более подробного вывода. Так как вывод довольно длинный, то можно воспользоваться графическим интерфейсом Zenmap и посмотреть результаты в графическом виде:

Изображение выглядит как текст

Автоматически созданное описание



Изображение выглядит как текст

Автоматически созданное описание

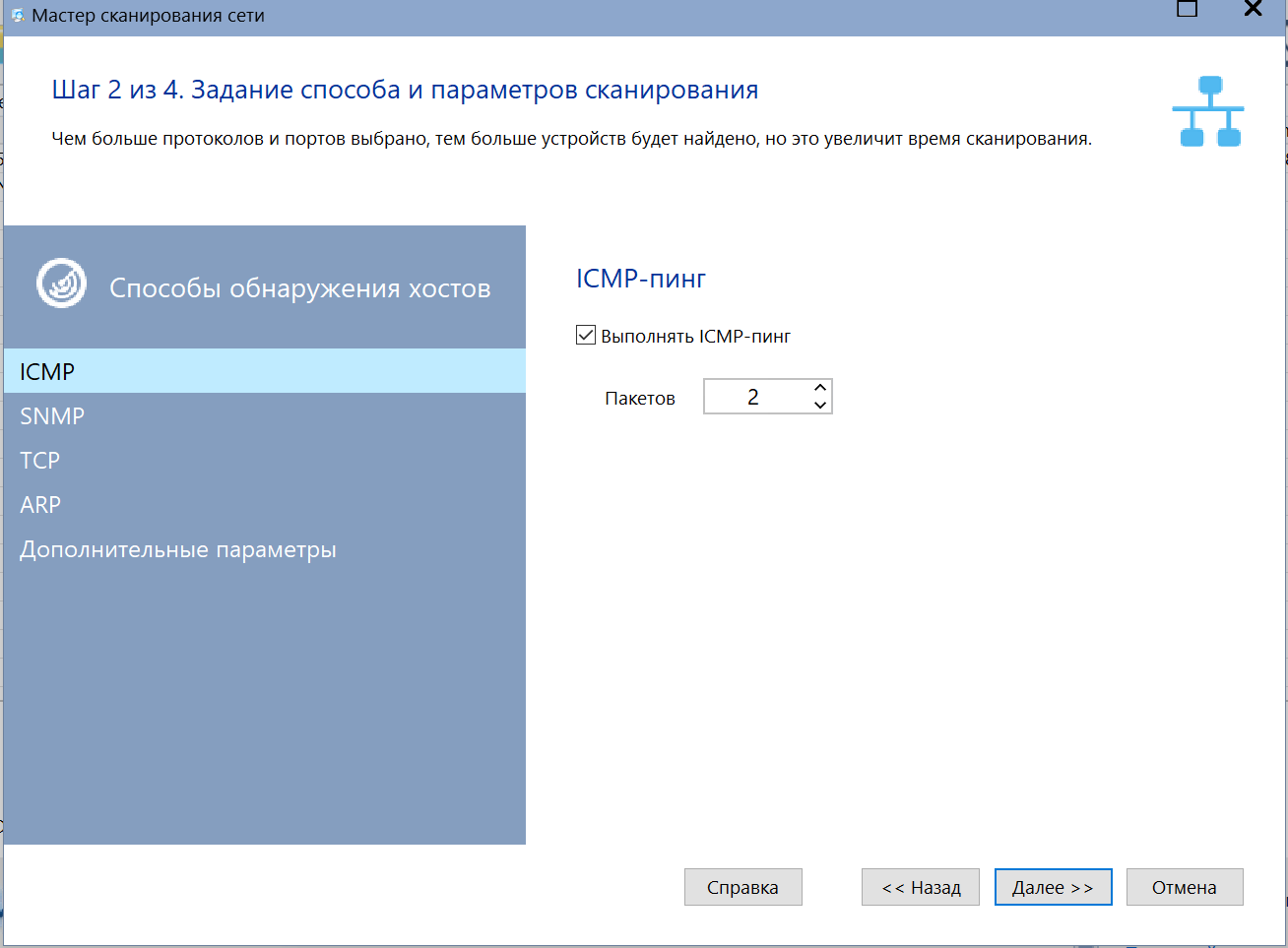
Как видно из рисунков, была получена подробная информация об узлах в сети: информация о портах и сервисах, информация об ОС, топология сети.

Утилита nmap имеет много опций, с помощью которых можно указать способ сканирования (TCP SYN, TCP connect, TCP ACK, UDP и проч.), параметры сканирования, параметры обнаружения сервисов, версий, ОС. Также nmap имеет мощный движок скриптов (NSE), который позволяет запускать различные скрипты, в т. ч. пользовательские.

Выполним сканирование с помощью программы «10-Страйк: Сканирование сети», при этом будем использовать все доступные способы обнаружения хостов (ICMP, SNMP, популярные порты TCP, ARP):

Изображение выглядит как текст

Автоматически созданное описание



В результате были найдены все узлы сети и некоторая дополнительная информация о них:

