**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра МО ЭВМ**

отчет

**по лабораторной работе №5**

**по дисциплине «Сети и телекоммуникации»**

Тема: Протоколы TELNET и SNMP

|  |  |  |
| --- | --- | --- |
| Студентка гр. 7383 |  | Левкович Д.В. |
| Преподаватель |  | Фирсов М.А. |

Санкт-Петербург

2019

**Цель работы.**

Изучение уровня приложений стека протоколов TCP/IP на примере протоколов SNMP-DPI и TELNET.

**Порядок выполнения работы.**

1. На компьютере К1 запустить SNMP-агент. (Порт и имя группы выбираются студентом.)
2. С компьютера К2 отправить запросы Get и получить переменные П1, П2, П3. Сравнить полученные значения с реальными.
3. С компьютера К2 отправить запросы GetNext для переменных П1, П2, П3. Объяснить полученные результаты.
4. На компьютере К1 с помощью диалога “Set TCP/IP Properties” изменить IP-адрес, маску подсети и шлюз по умолчанию. С компьютера К2 с помощью запросов Set вернуть К1 в исходное состояние. Проверить результаты посредством SNMP.
5. На компьютере К2 запустить TELNET-сервер. (Порт и пароль выбираются студентом.)
6. С компьютера К3 по протоколу TELNET подключиться к компьютеру К2. Удалить все значения из таблицы маршрутизации и ARP-таблицы. Добавить в таблицу маршрутизации и ARP-таблицу записи необходимые для корректной работы компьютера К2.
7. С помощью команды TELNET-сервера snmp запустить SNMP-агент на К3. С любого компьютера попытаться получить значение произвольной SNMP-переменной по выбору студента.

В отчет необходимо включить схему сети, все вводимые параметры (порт, имя группы доступа и др.), отправленные запросы и полученные ответы. Для протокола TELNET необходимо привести сообщения, выводимые в TELNET-консоль.

**Индивидуальный вариант № 10.**

Файл с вариантом заданий lab1\_var10.jfst.

Обозначения в задании: Компьютеры К1 – PC2; К2 – PC3; К3 – PC4.

SNMP переменные П1 – Counter.OutputUDP; П2 – Counter.ARP; П3 –

Device.AllInterfaces.

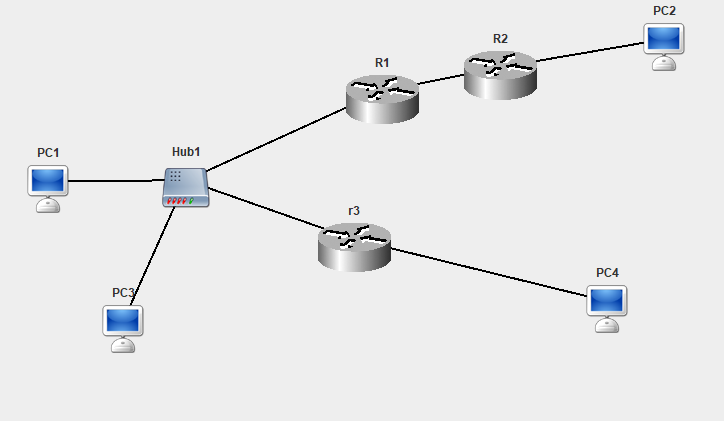


Рисунок 1 – Схема сети для варианта №12

**Ход работы.**

1. Для запуска SNMP-агента на К1 (Manager3) необходимо выбрать пункт контекстного меню «Application» – «Start SNMP Agent» и задать два параметра:

* Порт, на котором SNMP-агент будет ожидать пакеты: 161;
* Имя группы доступа для SNMP-агента: pc2.

В консоль была выведена информация о запуске SNMP-агента:



1. Для выполнения с К2 (PC3) запроса SNMP-агенту на К1 (PC2) нужно выбрать пункт контекстного меню «Application» – «Send SNMP message» со следующими параметрами:

* IP-адрес компьютера, на котором установлен SNMP-агент: 172.168.0.1;
* Порт, на котором SNMP-агент ожидает пакеты: 161;
* SNMP-запрос. Может принимать значение Get;
* SNMP-переменные: Device.AvailableInterfaces; Counter.OutputTCP; Counter.OutputUDP;
* Имя группы доступа: pc1.

Окно запроса представлено на рис. 2.

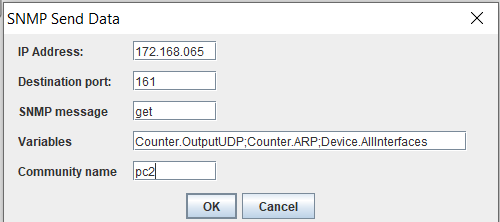


Рисунок 2 – Окно SNMP запроса.

Результаты запроса были выведены на консоль:



Полученные переменные соответствуют реальным данным, что представлены на рис. 3-4.

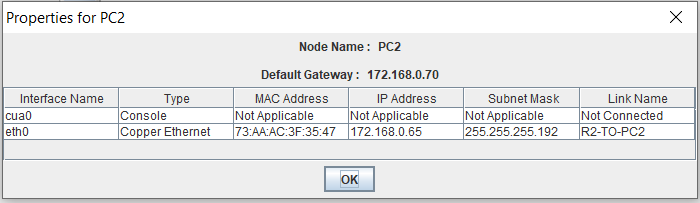


Рисунок 3 – Список всех доступных интерфейсов у Manager3.

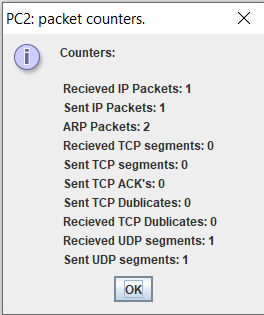


Рисунок 4 – Данные о количестве отправленных TCP и UDP пакетов у Manager3.

1. С К2 (Service) отправили запросы GetNext для переменных П1, П2 и П3.

Окно запроса представлено на рис. 5.

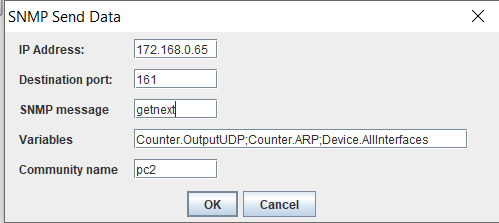


Рисунок 5 – Окно запроса GetNext

В консоль выведена информация:



Полученные переменные – это те переменные, которые следуют после указанных в запросе.

1. На компьютере К1 (Manager3) с помощью диалога “Set TCP/IP Properties” изменили IP-адрес, маску подсети и шлюз по умолчанию.

На рис. 6 показано начальное состояние Manager3, а на рис. 7 – после изменений.

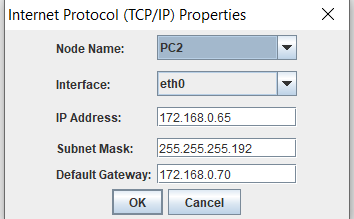


Рисунок 6 – Исходные значения.

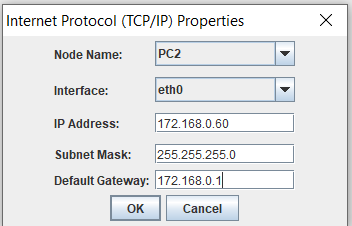


Рисунок 7 – Данные после изменения.

С компьютера К2 (Service) с помощью запроса Set вернули К1 (Manager3) в исходное состояние. Вид запроса представлен на рис. 8.

Параметры:

П1 – ip.address\_eth0="172.168.0.65";

П2 – ip.defaultgateway="172.168.0.70";

П3 – ip.subnetmask\_eth0=" 255.255.255.192".

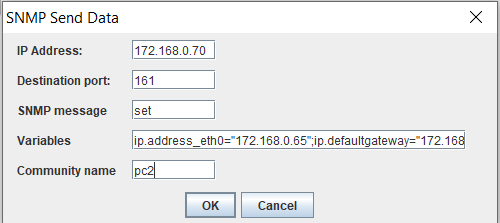


Рисунок 7 – Set запрос.

Получили результат:



Проверили результаты посредством SNMP, отправив Get запрос, показанный на рис. 8.

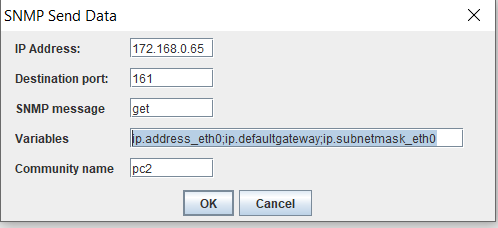


Рисунок 8 – Get запрос.

Полученный ответ от K1:



1. На компьютере К2 (Service) запустили TELNET-сервер «Application» – «Start telnet server to listen» со следующими параметрами:

* Порт, на котором TELNET-сервер будет ожидать пакеты: 21;
* Пароль для доступа к TELNET: 123.

Результат:



1. С компьютера К3 (Chief) по протоколу TELNET подключились к компьютеру К2 (Service).

С помощью команд «arp –a» посмотрели ARP-таблицу Service, с помощью команды «arp –d [ip]» 172.168.0.4 удалили одну строку из этой таблицы. Результаты работы показаны на рис. 9-10.

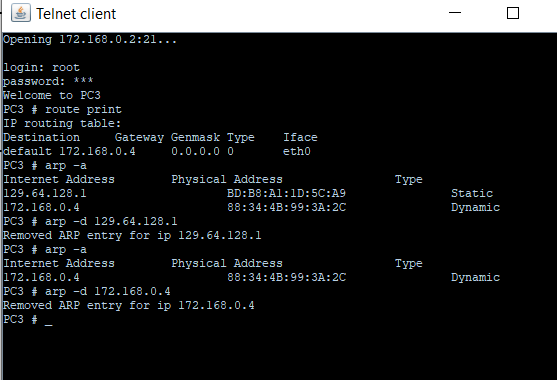


Рисунок 9 – Telnet client.

Затем командой «route del default» удалили все данные из таблицы маршрутизации Service, что видно на рис. 11-12.

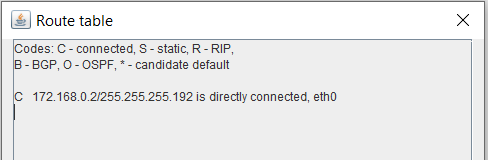


Рисунок 11 – Route table после удаления всех записей.

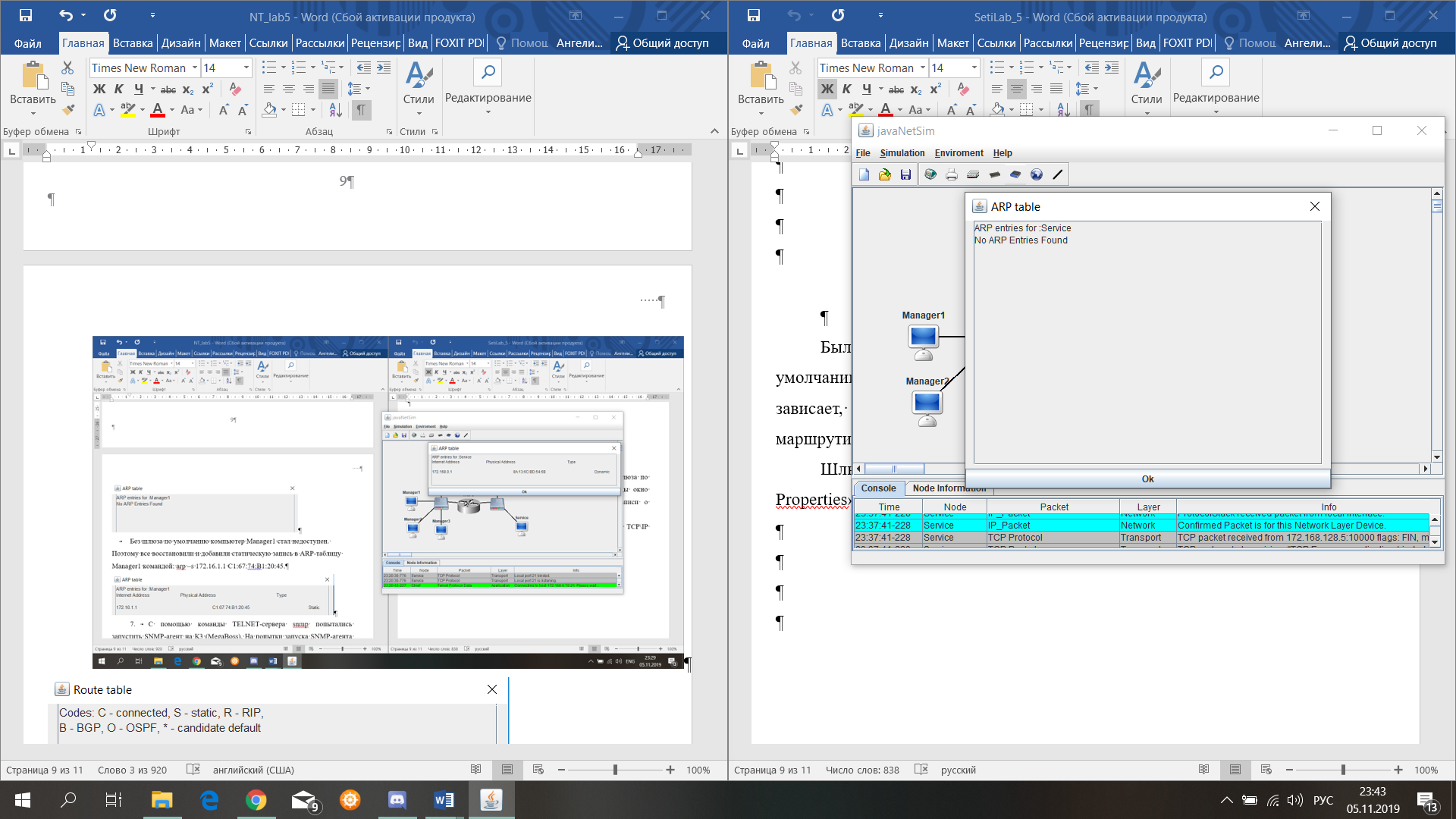


Рисунок 12 – ARP таблица после удаления всех записей.

Без шлюза по умолчанию компьютер Service стал недоступен, а окно ввода зависло. Вероятно, это связано с тем, что после удаления записи о маршрутизаторе по умолчанию сеть не может работать корректно.

Поэтому все восстановили и добавили статическую запись в ARP-таблицу Service командой «arp –s», окно ввода представлено на рис. 13.

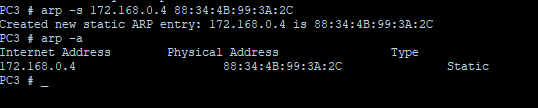


Рисунок 13 – Telnet client.

ARP-таблица после внесённых изменения показана на рис. 14.

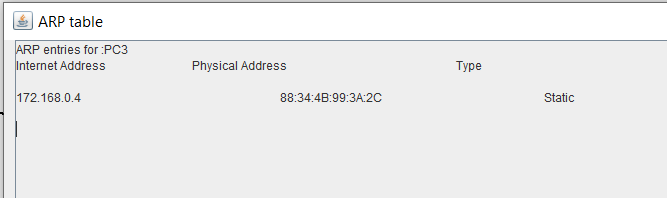


Рисунок 14 – Добавление статической записи.

1. С помощью команды TELNET-сервера snmp попытались запустить SNMP-агент на К3 (Chief). На попытки запуска SNMP-агента программа отреагировала следующим сообщением, которое представлено на рис. 15.

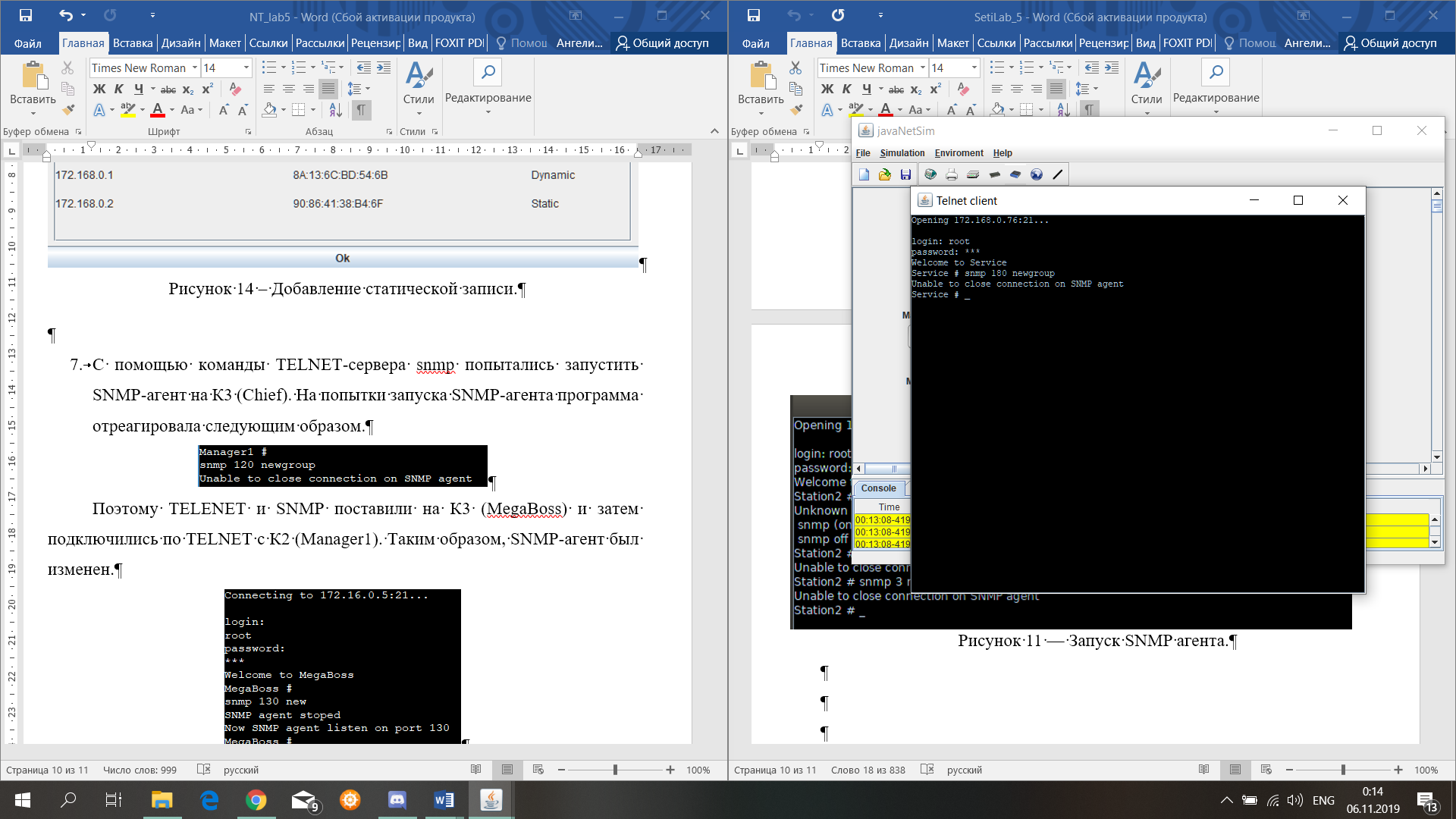


Рисунок 15 – Вывод сообщения.

Поэтому TELNET и SNMP поставили на К3 (Chief) и затем подключились по TELNET с К2 (Service). Таким образом, SNMP-агент был изменен. Результат продемонстрирован на рис. 16.

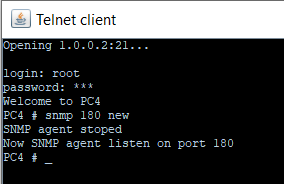


Рисунок 16 – Запуск SNMP агента.

Затем с К2 отправили запрос на получение значения переменной Device.Hostname. Запрос показан на рис. 17.

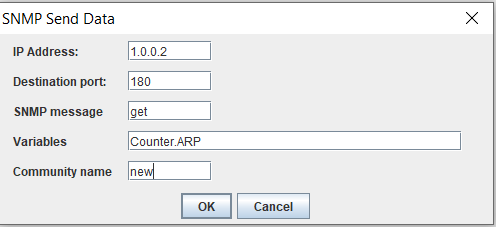


Рисунок 17 – Get запрос.

В консоль был выведен ответ на запрос. Все верно.



**Вывод.**

В ходе выполнения работы изучили уровень приложений стека протоколов TCP/IP на примере протоколов SNMP-DPI и TELNET.

**Ответы на контрольные вопросы.**

1. **Для чего предназначен протокол SNMP?**

SNMP (Simple Network Management Protocol) протокол предназначен для использования сетевыми управляющими станциями. Он позволяет управляющим станциям собирать информацию о положении в сети. Протокол определяет формат данных, а их обработка и интерпретация остаются на усмотрение управляющих станций или менеджера сети.

1. **Если на SNMP запрос пришел отклик с установленным флагом ошибки, то какие переменные будут содержаться в этом отклике? Если в set запросе часть переменных имеет корректные значения, а часть некорректные то какие переменные объекта управления изменятся?**

Get-response обеспечивает передачу отклика на команды Get-request, GetNext-request или Set от агента SNMP менеджеру. Get-response возвращает значения запрошенных объектов, только в случае успешного выполнения команд Get, GetNext или Set, следовательно если при SNMP запросе пришел ответ с установленным флагом ошибки, то переменные возвращены не будут.

Если запросом Set устанавливаются значения сразу нескольких переменных, то в случае ошибки они все останутся без изменений.

1. **Как обеспечивается защита в протоколе SNMP? Как вы думаете насколько безопасно применения протокола SNMP для управления реальной сетью? Что надо сделать для увеличения безопасности?**

Сообщения SNMP имеют достаточно простую структуру. Это упрощает реализацию протокола, но ведет к тому, что имя группы доступа, предназначенное для ограничения доступа к SNMP-агенту, никак не шифруется и передается по сети в открытой форме. Из этого следует что применение данного протокола для управления реальной сетью не является безопасным.

Для увеличения безопасности необходимо разработать возможность аунтификации и шифрования. В современной версии протокола SNMPv3 смогли решить часть проблем, связанных с безопасностью, но продолжают работать над расширениями и улучшениями.

1. **Для чего предназначен протокол TELNET?**

Протокол Telnet предназначен для обеспечения удаленного доступа к сетевому устройству с помощью командного интерпретатора. Telnet позволяет пользователю установить TCP-соединение с сервером и затем передавать коды нажатия клавиш так, как если бы работа проводилась на консоли сервера.

1. **Как работает протокол TELNET? Как обеспечивается безопасность при вводе пароля?**

В упрощенном варианте протокол Telnet работает следующим образом:

* Между клиентом и сервером устанавливается TCP соединение.
* Клиент посылает серверу символ перевода строки для того, чтобы сервер знал, что это клиент хочет соединится по Telnet.
* В ответ сервер посылает приглашение ввода имени (например: login) и ждет ввода имени пользователя. После ввода сервер посылает приглашение ввода пароля (например: password) и ждет ввода пароля.
* Если введенные имя и пароль корректны, то Telnet-сервер переходит в режим ввода.
* В этом режиме любой введенный текст пересылается удаленному сетевому устройству. Ввод может производиться посимвольно или построчно. При посимвольном режиме каждый введенный символ пересылается немедленно, при построчном режиме отклик на каждое нажатие клавиши производится локально, а пересылка выполняется лишь при нажатии клавиши <Enter>.

Telnet обеспечивает незащищенное соединение, т.е. все данные передаются в открытой форме, в том числе и пароли.