# МИНОБРНАУКИ РОССИИ

**САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)**

**Кафедра МОЭВМ**

**ОТЧЕТ**

**по лабораторной работе №5**

**по дисциплине «Сети ЭВМ и телекоммуникации» Тема: Протоколы Telnet и SNMP**

Студент гр. 6304 Виноградов К.А.

Преподаватель Фирсов М.А.

Санкт-Петербург

2018

# Цель работы.

На примере протоколов SNMP-DPI и TELNET ознакомиться с уровнем приложений стека протоколов TCP/IP.

# Задание.

1. На компьютере К1 запустить SNMP агента. Порт и имя группы доступа выбираются студентом;
2. С компьютера К2 отправить запрос(ы) get, и получить переменные П1, П2, П3. Сравнить полученные значения с реальными;
3. С компьютера К2 отправить запрос(ы) getnext для переменных

П1, П2, П3. Объяснить полученные результаты;

1. 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 K1 в исходное состояние. Проверить результаты посредством SNMP;
2. На компьютере K2 запустить TELNET сервер. Порт и пароль выбрать самостоятельно;
3. 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;
4. С помощью команды TELNET-сервера SNMP запустить SNMP агента на К3. Проверить работоспособность SNMP-сервера: с компьютера К2 попытаться получить значение SNMP переменной П2;

**Вариант 2**. Файл со схемой сети lab1\_var2.jfst. Обозначения в задании: К1 – OFFICE1\_PC4; К2 – BIG\_BOSS; К3 – M\_CH\_S; П1 – COUNTER.OUTPUTIP; П2 – IP.SubnetMask\_eth0; П3 – IP.ARPtable.

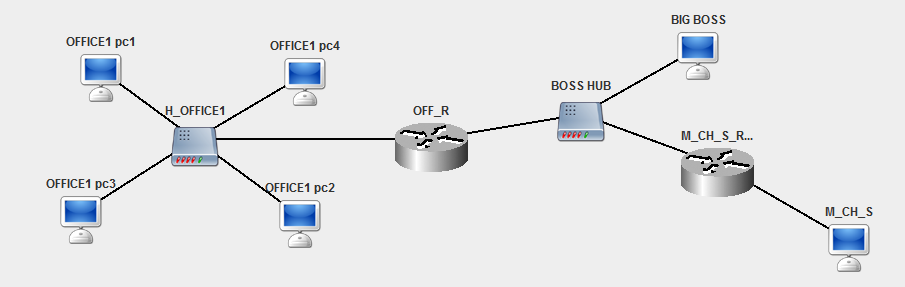


Рисунок 1 – Схема сети

# Основные теоретические положения.

С любой сети функционирует большое количество узлов, маршрутизаторов и имеется широкий набор программных средств. Сеть сохраняет работоспособность благодаря жесткой протокольной регламентации, требующей разработки средств контроля и управления. Функции диагностики сети возложены на ICMP, а функции управления на SNMP (Simple Network Management Protocol – RFC1157). Чаще всего управляющая прикладная программа воздействует на сеть по цепочке: SNMP, UDP, IP, физическая сеть. Управление сетью – это процесс управления отказами, контроля конфигураций, мониторинга производительности, обеспечения защиты и учета деятельности в сети передачи данных. Наиболее важным объектом управления обычно является маршрутизатор. Каждому управляемому объекту присваивается уникальный идентификатор.

Протокол SNMP использует UDP в качестве транспортного протокола и 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.

Приложения управления сетью, называемые менеджерами, общаются с программным обеспечением сетевых устройств, называемым агентами. SNMP – это протокол типа "запрос-отклик", то есть на каждый запрос, поступивший от менеджера, агент должен передать отклик. Под запросом будем понимать передачу информации от менеджера к агенту с целью получения параметров объекта управления. Под откликом будем понимать ответ агента, на запрос менеджера, содержащий требуемые параметры.

Для обеспечения удаленного доступа к сетевому устройству с помощью командного интерпретатора используется протокол TELNET (RFC854). Протокол TELNET – это сетевой протокол типа "клиент- сервер". TELNET обеспечивает незащищенное соединение, т.е. все данные передаются в открытой форме в том числе и пароли. TELNET использует TCP в качестве транспортного протокола. Общепринято, что TELNET-сервер ожидает соединения на 23 порту. TELNET позволяет пользователю установить TCP-соединение с сервером и затем передавать коды нажатия клавиш так, как если бы работа проводилась на консоли сервера.

# Ход работы.

1. На компьютере «OFFICE1 pc4» запустим SNMP агента на порту 161 с именем группы «noname».

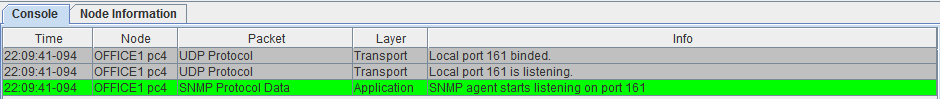


Рисунок 2 – Запуск SNMP агента

1. С компьютера «BIG BOSS» отправим запрос get, и получим переменные П1, П2, П.

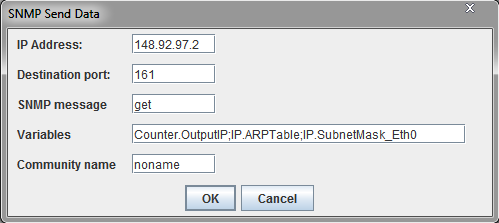


Рисунок 3 – Отправка SNMP запроса

**Результаты:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 22:17:43-440 | BIG BOSS | SNMP Protocol Data | Application | Received getResponse: 'Counter.OutputIP=0' , 'IP.ARPTable=148.92.98.1 7F:5A:AB:89:B4:1B Dynamic' , 'IP.SubnetMask\_Eth0=255.255.0.0' |
| 22:17:43-440 | BIG BOSS | SNMP Protocol Data | Application | SNMP manager closed socket. |

Проверим значения. Результаты на рис.4,5,6.

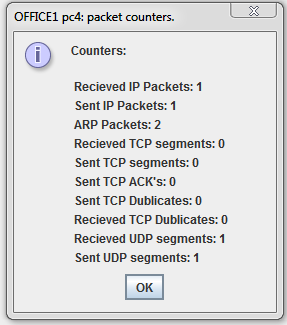


Рисунок 4 – Проверка значения Counter.OutputIP

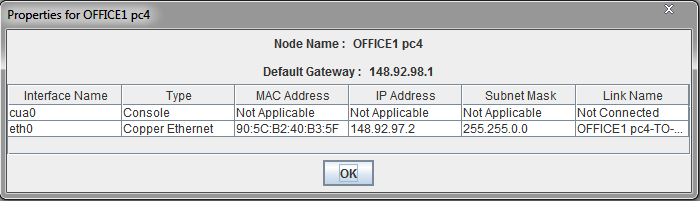


Рисунок 5 – Проверка значения IP.SubnetMask\_Eth0

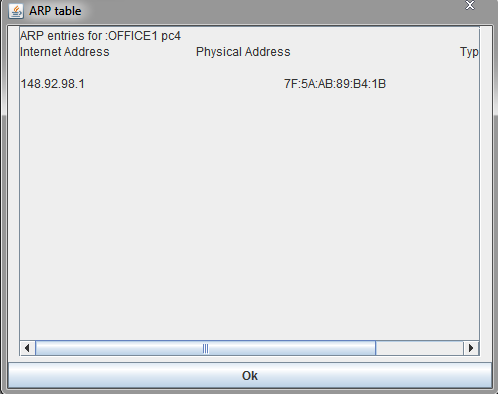


Рисунок 6 – Проверка значения IP.ARPTable

1. С компьютера «BIG BOSS» отправим запрос getnext для переменных П1, П2, П3.

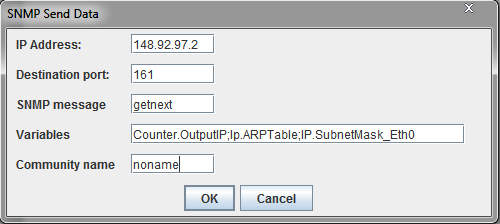


Рисунок 7 – Отправка SNMP запроса

**Результаты:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 22:42:41-314 | BIG BOSS | SNMP Protocol Data | Application | Received getResponse: 'Counter.ARP=2' , 'IP.DefaultGateway=148.92.98.1' , 'SNMP.CommunityName=noname' |
| 22:42:41-314 | BIG BOSS | SNMP Protocol Data | Application | SNMP manager closed socket. |

Соответственно получили значения следующих в лексикографическом порядке по дереву MIB переменных для переменных в запросе.

1. На компьютере «OFFICE1 pc4» с помощью диалога "Set TCP/IP Properties" изменим IP адрес, маску подсети и шлюз по умолчанию. С компьютера «BIG BOSS» с помощью запроса set вернём «OFFICE1 pc4» в исходное состояние. Проверим результаты посредством SNMP запроса get.

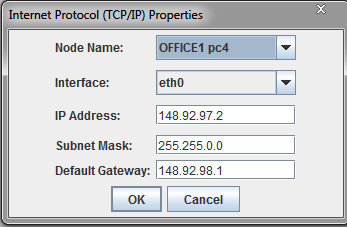


Рисунок 7 – Начальные параметры «OFFICE1 pc4»

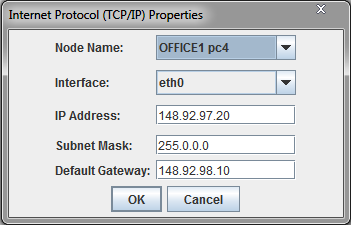


Рисунок 8 – Параметры «OFFICE1 pc4» после изменения

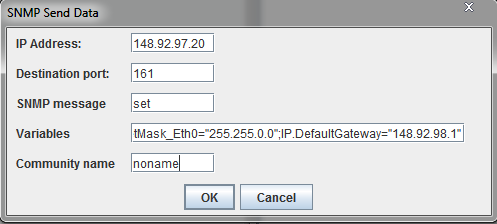


Рисунок 9 – Возвращение «OFFICE1 pc4» в исходное состояние

**Тело запроса:**

IP.Address\_eth0="148.92.97.2";IP.SubnetMask\_eth0="255.255.0.0";

IP.DefaultGateway="148.92.98.1"

**Результаты:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23:32:33-646 | BIG BOSS | SNMP Protocol Data | Application | Received getResponse: 'IP.Address\_Eth0=148.92.97.2' , 'IP.SubnetMask\_Eth0=255.255.0.0' , 'IP.DefaultGateway=148.92.98.1' |
| 23:32:33-646 | BIG BOSS | SNMP Protocol Data | Application | SNMP manager closed socket. |

Проверим с помощью get запроса.

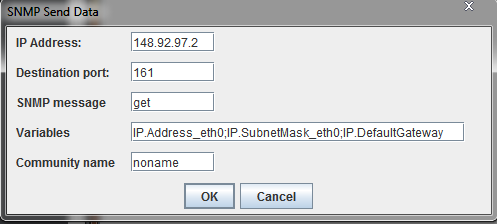


Рисунок 10 – Отправка SNMP запроса на «OFFICE1 pc4»

**Тело запроса:**

IP.Address\_eth0;IP.SubnetMask\_eth0;IP.DefaultGateway

**Результаты:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23:42:55-807 | BIG BOSS | SNMP Protocol Data | Application | Received getResponse: 'IP.Address\_Eth0=148.92.97.2' , 'IP.SubnetMask\_Eth0=255.255.0.0' , 'IP.DefaultGateway=148.92.98.1' |
| 23:42:55-807 | BIG BOSS | SNMP Protocol Data | Application | SNMP manager closed socket. |

1. На компьютере «BIG BOSS» запустим TELNET сервер на порте 23 с паролем 666.

**Результаты:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23:57:17-628 | BIG BOSS | TCP Protocol | Transport | Local port 23 binded. |
| 23:57:17-628 | BIG BOSS | TCP Protocol | Transport | Local port 23 is listening. |

1. C компьютера «M\_CH\_S» по протоколу TELNET подключимся к компьютеру «BIG BOSS». Удалим все значения из таблицы маршрутизации и ARP таблицы. Добавим в таблицу маршрутизации и ARP таблицу записи необходимые для корректной работы компьютера «BIG BOSS».

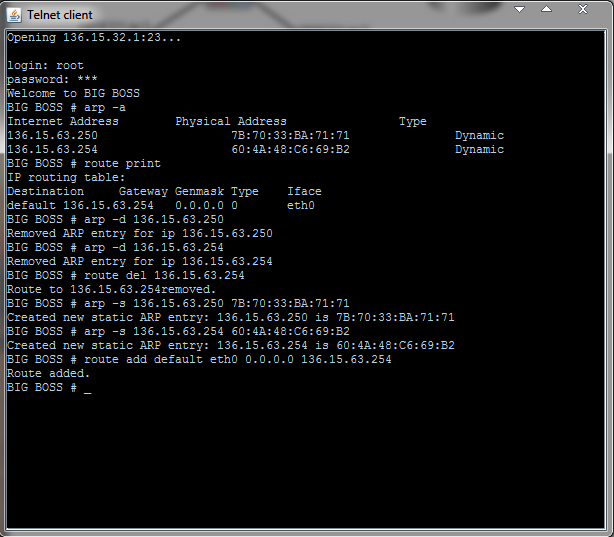


Рисунок 11 – Работа с «BIG BOSS» по TELNET

1. С помощью команды TELNET-сервера SNMP запустим SNMP агента на «BIG BOSS». Проверим работоспособность SNMP-сервера: с компьютера «M\_CH\_S». Для этого попытаемся получить значение SNMP переменной П2.

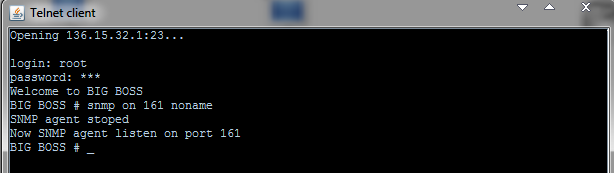


Рисунок 12 – Запуск SNMP агента на «BIG BOSS» по TELNET

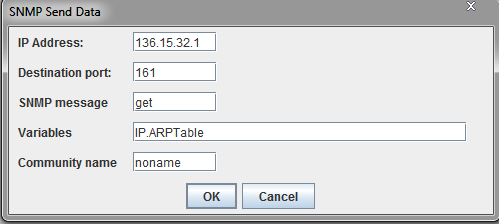


Рисунок 13 – SNMP запрос к К2

**Результаты:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 00:31:40-540 | M\_CH\_S | SNMP Protocol Data | Application | Received getResponse: 'IP.ARPTable=136.15.63.254 60:4A:48:C6:69:B2 Static, 136.15.63.250 7B:70:33:BA:71:71 Dynamic' |
| 00:31:40-540 | M\_CH\_S | SNMP Protocol Data | Application | SNMP manager closed socket. |

# Вывод.

Протокол SNMP предоставляет широкий набор функций для управления сетью, а протокол TELNET доступ к удалённым устройствам с помощью командного интерпретатора. Оба протокола работают на уровне приложений модели TCP/IP, что позволяет взаимодействовать с ними непосредственно в прикладной программе.