Некоммерческое
Акционерное
общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА

Кафедра
телекоммуникаций и
инновационных технологий

ИССЛЕДОВАНИЕ ТЕХНОЛОГИЙ ТРАНСПОРТНЫХ СЕТЕЙ СВЯЗИ

Методические указания к лабораторным работам
для магистрантов образовательной программы
7М06201 – Радиотехника, электроника и телекоммуникации
(Магистратура научного и педагогического направления)

Алматы 2021

СОСТАВИТЕЛЬ: А.С. Байкенов. Исследование технологий транспортных сетей связи. Методические указания по выполнению лабораторных работ для магистрантов ОП 7М06201 – Радиотехника, электроника и телекоммуникации. – Алматы: АУЭС, 2021 – 46 с.

Методические указания содержат материал к лабораторным работам по дисциплине «Исследование современных транспортных сетей связи», описание выполнения 10 лабораторных работ, перечень рекомендуемой литературы и контрольные вопросы к защите лабораторных работ. Лабораторные работы реализованы на стенде и эмуляторе транспортных сетей Mininet.

Методические указания предназначены для магистрантов, обучающихся по образовательной программе 7М06201 – «Радиотехника, электроника и телекоммуникации».

Ил. 48, библиогр. – 12 назв.

Рецензент: доцент каф. ЭТ А.С. Баймаганов

Печатается по дополнительному плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи имени Гумарбека Даукеева» на 2021 г.

НАО «Алматинский университет энергетики и связи имени Гумарбека Даукеева», 2021 г.

Введение

Методические указания к выполнению лабораторных работ по курсу «Исследование технологий транспортных сетей связи» для магистрантов, обучающихся по образовательной программе 7М06201 – «Радиотехника, электроника и телекоммуникации». В настоящий сборник включены работы, целью которых является изучение и анализ функционирования технологий транспортных сетей связи. В первой части предлагаются работы по настройке сети на действующем стенде. Во второй части комплекса приведены работы по моделированию транспортных сетей с использованием эмулятора NetLab.

1. Лабораторная работа № 1. Ознакомление и запуск оборудования

Цель работы: изучение лабораторного стенда, его функциональных возможностей. Подготовка к запуску системы.

1.1. Описание лабораторной установки

- оборудование CISCO 7200, 7600 типа провайдерского класса для передачи трафика со скоростью до 2 млн. пакетов в секунду. Маршрутизаторы имеют базовые модули для реализации различных конфигураций сети. Главными особенностями является большой набор различных вариантов конфигурирования, большая скорость маршрутизации, VPN шифрование с аппаратной поддержкой, наличие большого числа интерфейсов, а также Fast Ethernet, Gigabit Ethernet, Packet Over SONET, отказоустойчивость, избыточность оборудования;

- оборудование фирмы Huawei Quidway s3500, H3C MSR 30-40 – это коммутаторы FastEthernet со скоростным соединением третьего уровня коробчатого типа с агрегацией 10/100M в центрах обработки информации операторов, кластере серверов и городских сетях связи.

1.2. Методические указания

1.2.1. Нужно собрать сеть, представленную на рисунке 1.

Предлагается сеть, состоящая из филиалов одной фирмы. Филиалы размещены условно в городах Алматы и Астана.

В каждый город устанавливается пограничный CE-маршрутизатор (Customer Edge router), соединенный по физическому каналу с одним из периферийных PE-маршрутизаторов (Provider Edge router) сети провайдера. При этом на физическом канале, соединяющем CE и PE маршрутизаторы, может быть поднят из протоколов канального уровня (PPP, Ethernet, FDDI, FR, ATM и т.д.).

Стендовая схема сети MPLS- Service показана на рисунке 1.

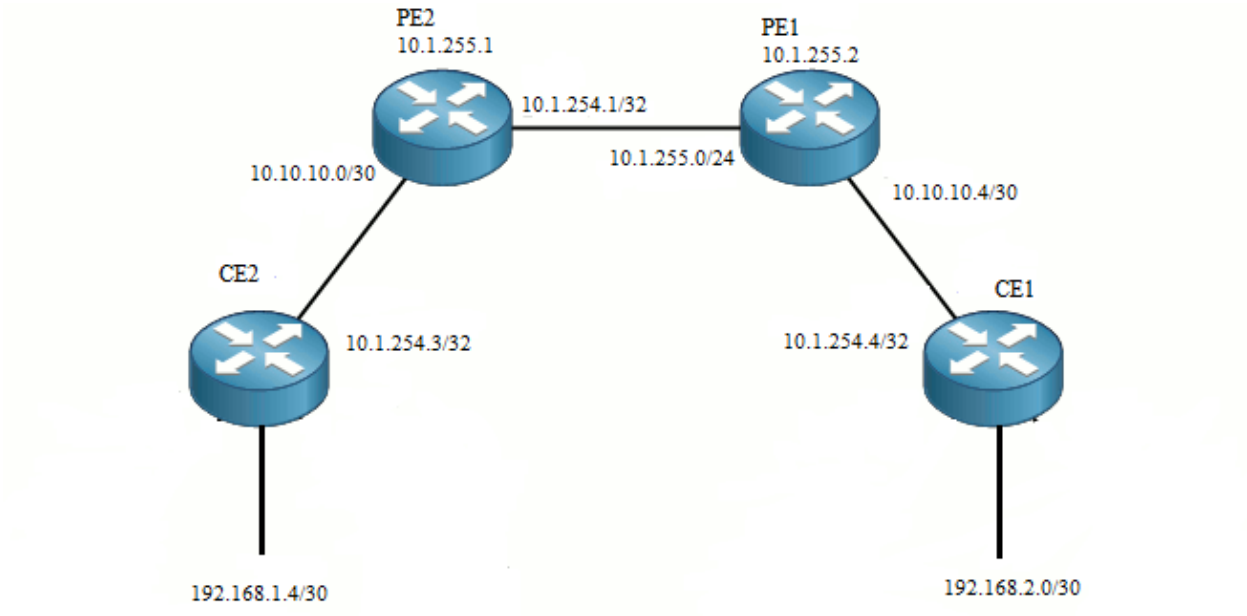


Рисунок 1 – Схема сети MPLS

На структурной схеме:

- CE2 – Huawei Quidway s3528g CE1-H3C MSR 30-40 – пограничные коммутаторы;
- PE1 – Cisco 7204, PE2 – Cisco 7604 – переферийные маршрутизаторы.

Протоколы, используемые на сети:

- PE1 – CE1 OSPF;
- PE1 – PE2 MP-BGP;
- PE2 – CE2 OSPF.

1.3. Контрольные вопросы

1. Каковы технические характеристики маршрутизатора CISCO 7200?
2. Каковы технические характеристики аппаратуры Huawei Quidway s3500?
3. Каковы технические характеристики коммутатора H3C MSR 30-40?
4. Какие основные особенности протокола OSPF?
5. Какие основные особенности протокола протокола MP-BGP?
6. Каковы технические характеристики маршрутизатора 7600?
7. Какие основные особенности технологии BGP/MPLS VPN?
8. Какие протоколы сетевого уровня?

2. Лабораторная работа № 2. Адресные планы PE1, PE2, CE1, CE2

Цель работы: произвести настройку оборудования с присвоением адресов на интерфесах.

2.1. Рабочее задание

2.1.1. Выполнить физическое соединение;
2.1.2. Осуществить запуск системы;

2.1.3. Присвоить IP адреса на PE1;
2.1.4. Присвоить IP адрес на PE2;
2.1.5. Присвоить IP адрес на CE1;
2.1.6. Присвоить IP адрес на CE2.

2.2. Методические указания

2.2.1. Проверить соединения и подключение всех устройств к блоку питания и запустить систему;

2.2.2. Запустить Hyper Terminal – терминальную программу, осуществляющую доступ к компьютерам. В раскладке Name даем имя MPLS и нажимаем OK. Окно Connection Description приведено на рисунке 2.

Рисунок 2 – Окно Connection Description

2.2.3. В данном окне рисунка 3 выбираем параметр COM1.

Рисунок 3 – Окно Connect To

2.2.4. Отмечаем параметры как рисунке 4.

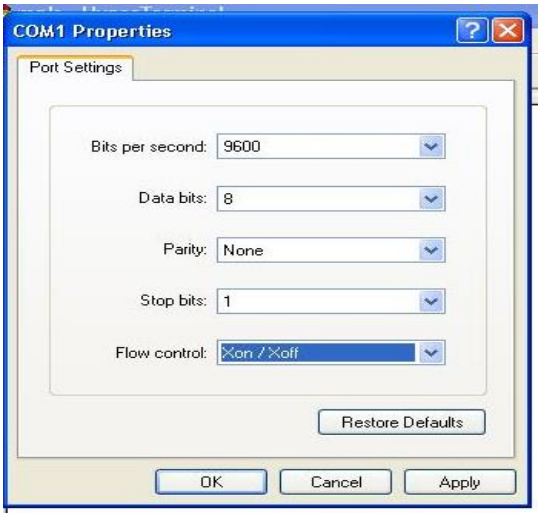


Рисунок 4 – Окно COM1

2.2.5. Подсоединяемся к Astana (PE1), используя кабель UTP. Далее устанавливаем адреса на интерфейсах.

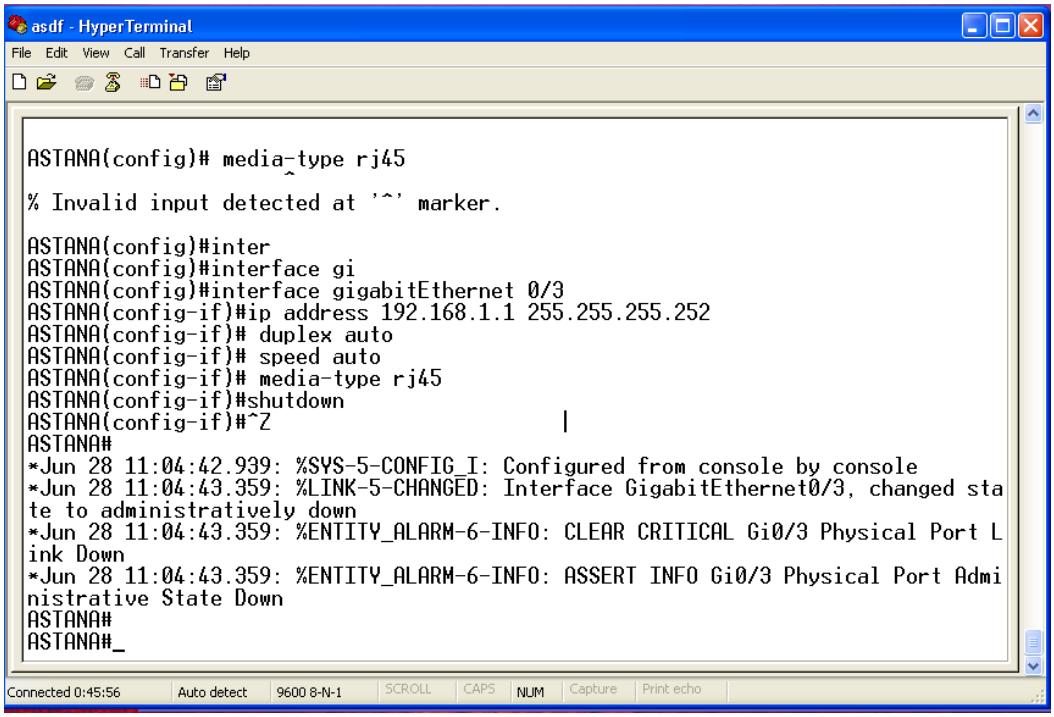


Рисунок 5 – Интерфейсы CISCO 7204

Программа для остальных интерфейсов:

interface GigabitEthernet0/1#
description TO_CISCO_7604##
ip address 10.1.255.2 255.255.255.0#
duplex auto#

speed 1000#
media-type gbic#
no negotiation auto#
mpls ip#
interface GigabitEthernet0/2#
 description TO_CE_H3C#
 ip vrf forwarding INTERNET#
 ip address 10.10.10.5 255.255.255.252#
 duplex auto#
 speed auto#
 media-type rj45#
 no negotiation auto
interface GigabitEthernet0/3#
 ip address 192.168.1.1 255.255.255.252#
 duplex auto#
 speed auto#
 media-type rj45#
shutdown#

2.2.6. С помощью кабеля UTP к Almaty (PE2) назначаем адреса на интерфейсах устройств.

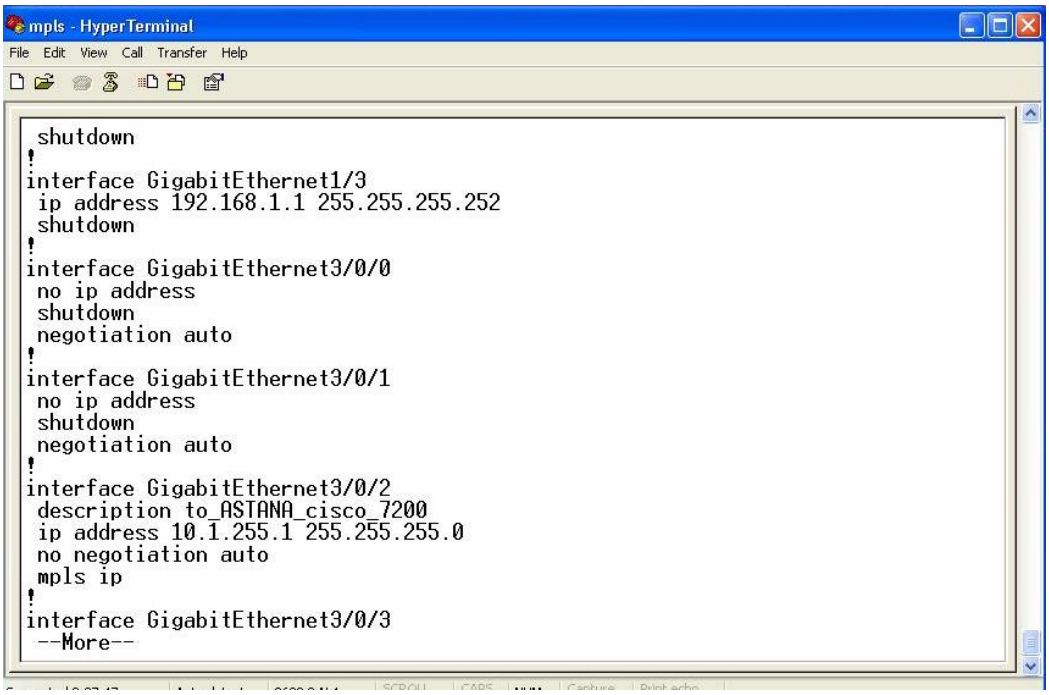


Рисунок 6 – Интерфейсы CISCO 7604

Программа для других интерфейсов:

interface Loopback1#
 ip address 10.1.254.1 255.255.255.255#
interface GigabitEthernet3/0/2#
 description to_ASTANA_cisco_7200#
 ip address 10.1.255.1 255.255.255.0#
 no negotiation auto#
 mpls ip#
interface GigabitEthernet3/1/4#
 description TO_CE_HUAWEI_S3500#
 ip vrf forwarding INTERNET#
 ip address 10.10.10.1 255.255.255.252#
 negotiation auto#
interface Vlan#
 no ip address##
 shutdown##

2.2.7. С помощью кабеля UTP присоединяемся к Quidway (CE2). Назначаем адреса на интерфейсы устройства.

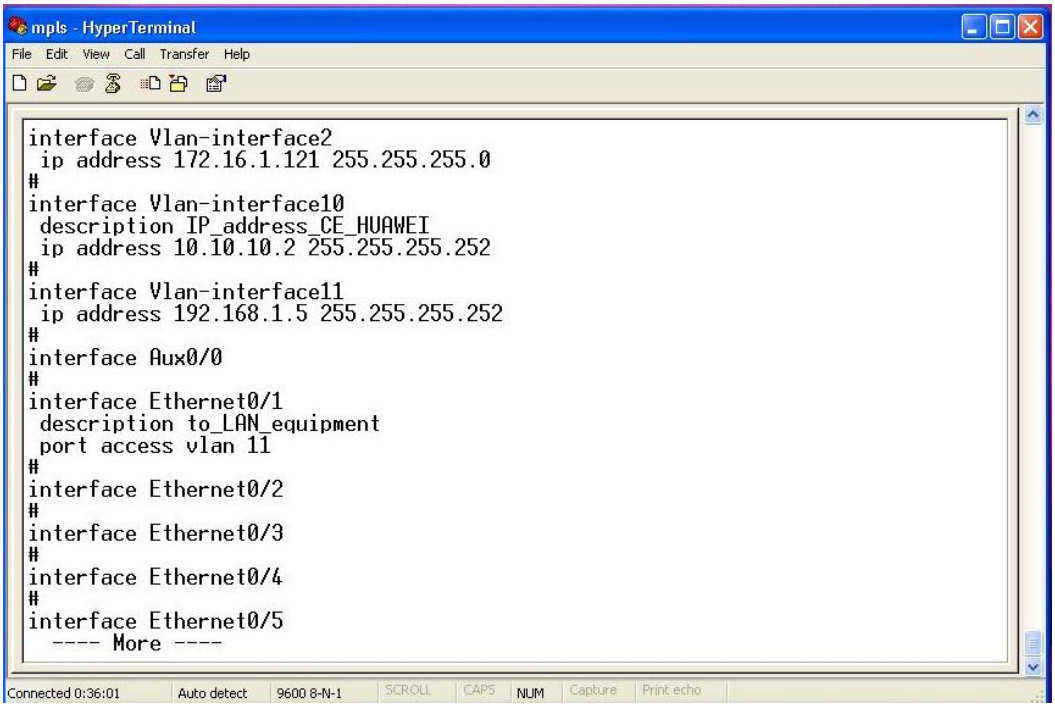


Рисунок 7 – Интерфейсы Quidway

Программа для других интерфейсов:

```
Vlan1#
vlan2#
 description MGM#
 nameMGM#
vlan10#
 description CE_PE_MPLS#
vlan11#
 description CE_FROM_CE_SDH#
interface Vlan-interface2#
 ip address 172.16.1.121 255255.255.0#
interface Vlan-interface10#
 ip address 10.10.10.2 255255.255.252#
interface Vlan-interface11
 ip address 192.168.1.5255.255.255.252#
interface Aux0/0#
interface Ethernet0/1#
 description to_LAN_equipment#
 port access vlan 11
interface Ethernet0/21#
 port access vlan2#
interface GigabitEthernet1/1#
 description from_CE_toPE#
 port access vlan10#
interface LoopBack1#
 ip address 10.1.254.3 255.255255.255#
```

2.2.8. С помощью кабеля UTP подсоединяемся к H3C (CE2). Назначаем адреса на интерфейсы.

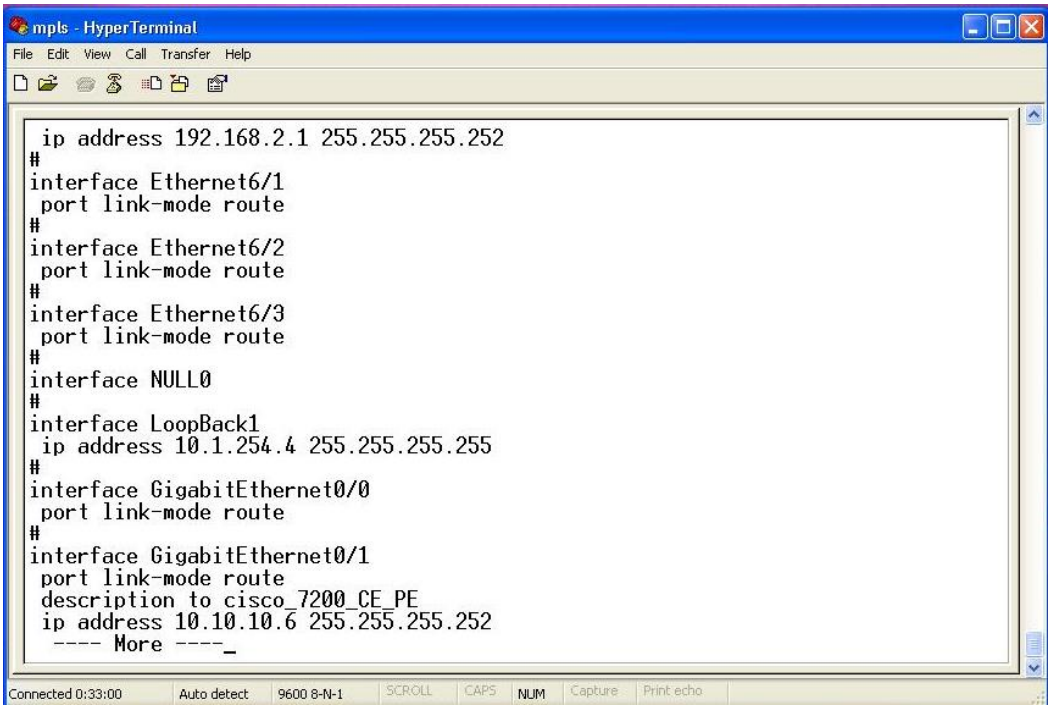


Рисунок 8 – Адресные планы интерфейсов H3C

Листинг для остальных интерфейсов:

interface Aux0#
async mode flow#
link-protocol ppp
interface Ethernet6/0#
port link-mode route#
ip address 192.168.21 255.255.255.252#
interface Ethernet6/1#
port link-mode route#
interface Ethernet6/2#
port link-mode route#
interface Ethernet6/3#
port link-mode route#
interface NULL0#
interfaceLoopBack1#
ip address 10.1.254.4 255255.255.255
interface GigabitEthernet0/0#
port linkmode route#
interface GigabitEthernet0/1#
port link-mode route#
description to cisco_7200_CE_PE#
ip address 10.10.10.6 255.255255.252#

2.3. Контрольные вопросы

1. Каково назначение программы Hyper Terminal.?
2. Каково назначение IP адресов?
3. Какие основные особенности технологии FastEthernet?
4. Какие основные особенности технологии GigabitEthernet?
5. Что означает команда address 10.10.10.6 255.255.255.252?
6. Что означает interface LoopBack1?
7. Каково назначение технологии vlan?
8. Какие основные особенности технологии 10 GigabitEthernet.

3. Лабораторная работа № 3. Настройка протоколов для маршрутизации PE1↔ PE2, CE1↔ PE1, CE2↔ PE2

Цель работы: настройка конфигурации протоколов между устройствами сети.

3.1. Рабочее задание

3.1.1. Выбрать нужный протокол маршрутизации между PE1↔ PE2, CE1↔ PE1, CE2↔ PE2.

3.1.2. Написать программу.

3.2. Методические указания

3.2.1. Выполнить пункты 2.2.1, 2.2.2, 2.2.3, 2.2.4 лабораторной работы № 2.

3.2.2. Соединиться с PE1 с помощью UTP и поднять протоколы.

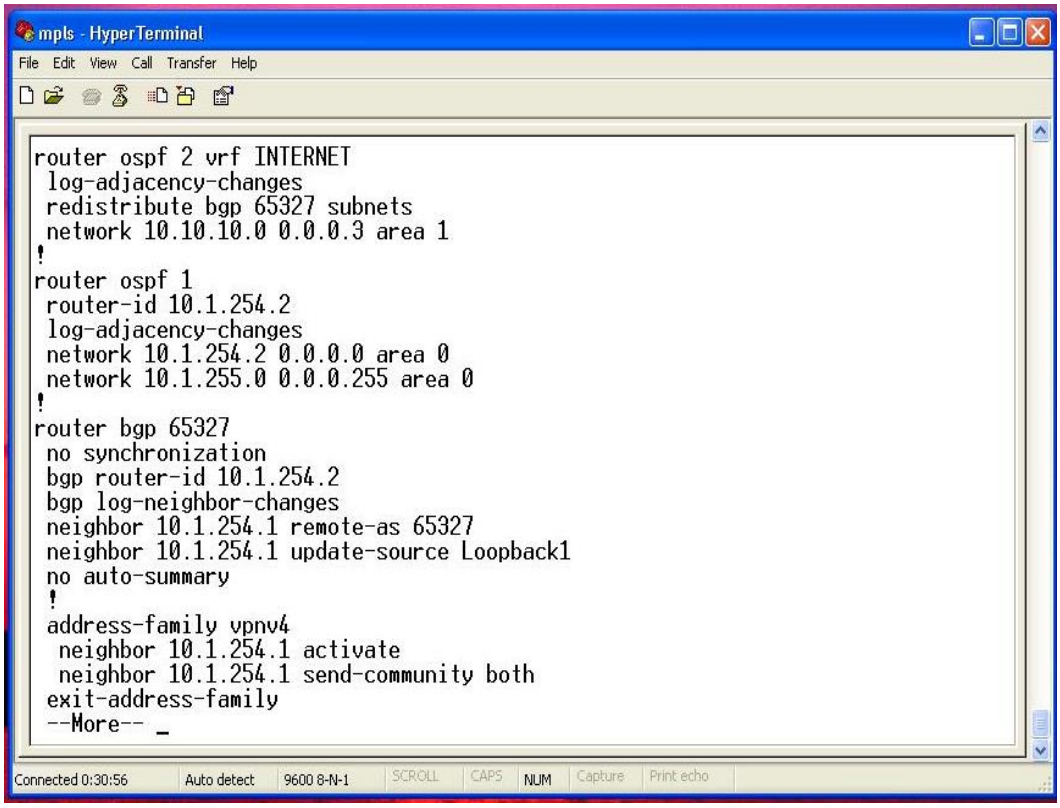


Рисунок 9 – Протоколы CISCO 7204

Программа:

router ospf1#
router-id 10.1.254.2#
log-adjacencychanges#
network 10.1.254.2 00.0.0 area 0#
network 10.1.255.0 00.0.255 area0#
router bgp 65327##
nosynchronization#
bgp router-id 10.1.254.2#
bgp log-neighborchanges#
neighbor 10.1.254.1 remoteas 65327#
neighbor 10.1.254.1 update-sourceLoopback1#
no autosummary#

3.2.3. С помощью UTP соединиться с PE2 и поднять протоколы.

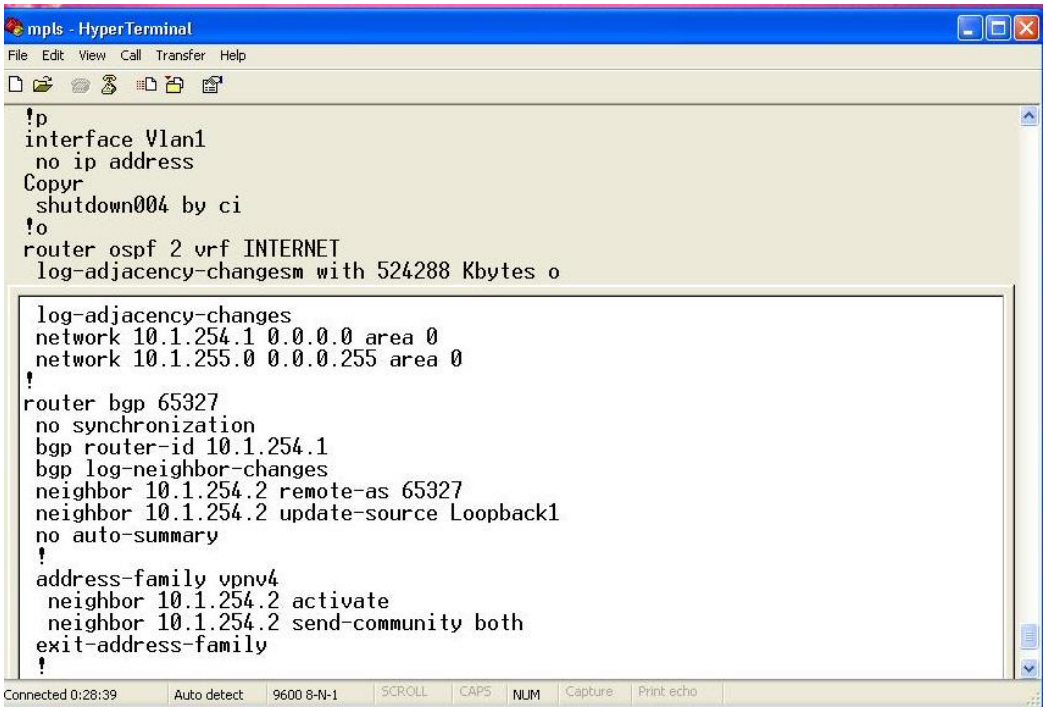


Рисунок 10 – Окно протоколов CISCO 7604

Программа:

router ospf1#
router-id 10.1254.1#
log-adjacency-changes#
network 10.1.254.1 00.0.0 area 0#
network 10.1.255.0 0.0.0.255 area 0#
router bgp 65327#
no synchronization#
bgp router-id 10.1.254.1#
bgp log-neighborchanges#
neighbor 10.1.254.2 remoteas 65327#
neighbor 10.1.254.2 update-sourceLoopback1#

3.2.4. С помощью UTP соединиться с CE1 и поднять протоколы.

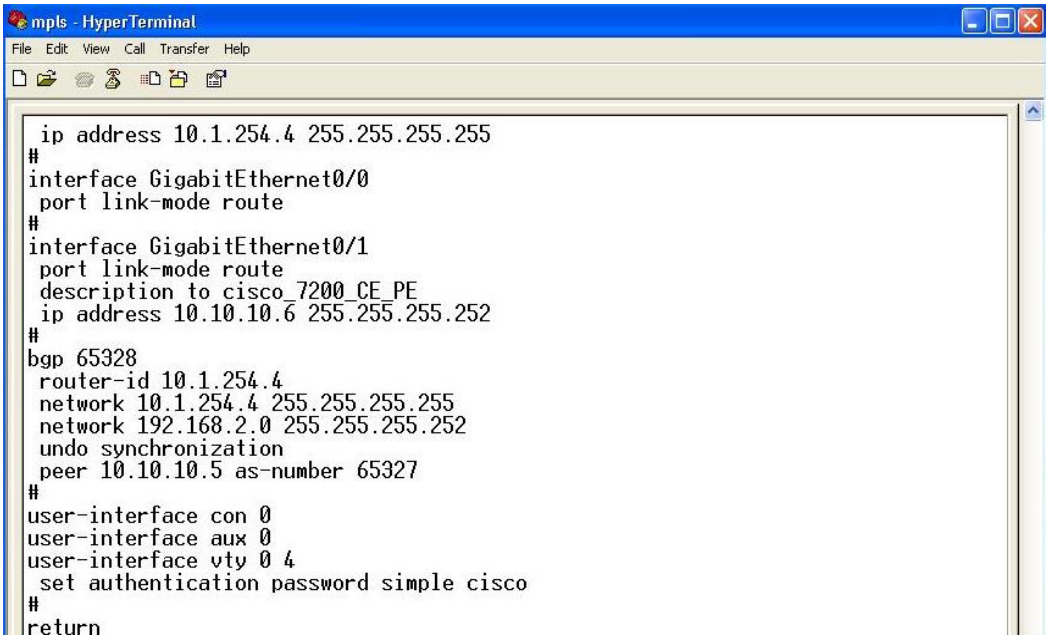


Рисунок 11 – Протоколы Quidway

Программа:
bgp 65328#
routerid 10.1.2544#
network 10.1.254.4 255.255.255255#
network 192.168.2.0 255.255.255.252#
undo- synchronization#
peer- 10.10.10.5 asnumber 65327#
user-interfacecon 0#
user-interfaceaux 0#
user-interface vty 0 4#

3.2.5. С помощью UTP соединиться CE2 с прописать протоколы.

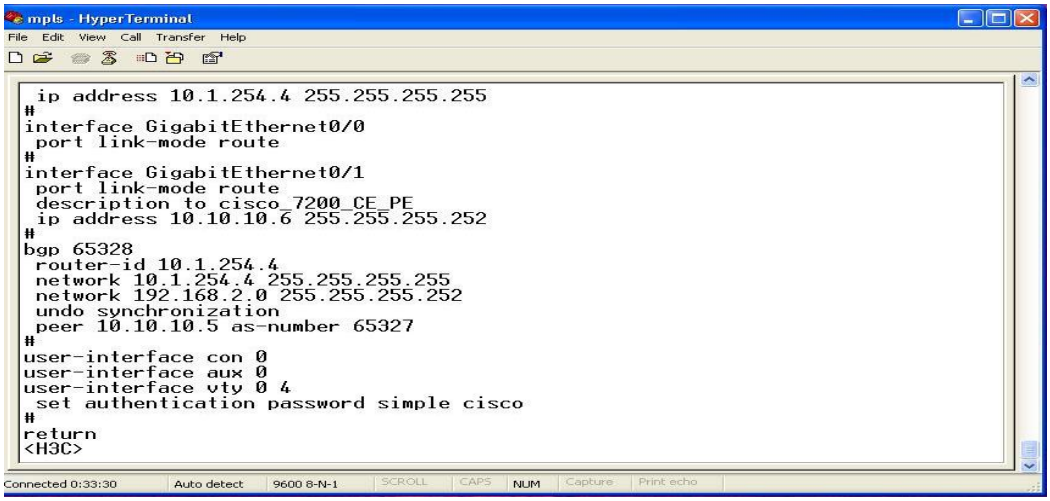


Рисунок 12 – Протоколы H3C

Программа:
ospf#
area 0.00.#1
network 10.1.254.30.0.0.0#
network 10.1010.0 0.0.0.3#
network 192.168.14 0.0.0.3#
user-interface aux 0#
user-interface vty0 4#
set authentication passwordsimple cisco#

3.3. Контрольные вопросы

1. Какие особенности имеет порт в маршрутизаторе?
2. Какие особенности протокола OSPF вы можете назвать?
3. Какие особенности протокола BGP отличают от его от других протоколов?
4. Что означает команда router-id 10.1.254.1?
5. Что означает команда area 0.0.0.1?
6. Какие еще динамические протоколы маршрутизации вы знаете?
7 . Чем отличаются динамические и статические маршруты?
8. Какой протокол OSPF или BGP потребляет больше вычислительных ресурсов?

4. Лабораторная работа № 4. Настройка L3 VPN MPLS модели

Цель работы: создать VRF(VPN) и установить защищенное соединение.

4.1. Рабочее задание

4.1.1. Реализовать L3 VPN MPLS на PE1.

4.1.2. Реализовать L3 VPN MPLS на PE2.

4.2. Методические указания

4.2.1. Выполнить пункты 2.2.1, 2.2.2, 2.2.3, 2.2.4 лабораторной работы № 2.

4.2.2. С помощью UTP кабеля соединиться с PE1, прописать конфигурацияю.

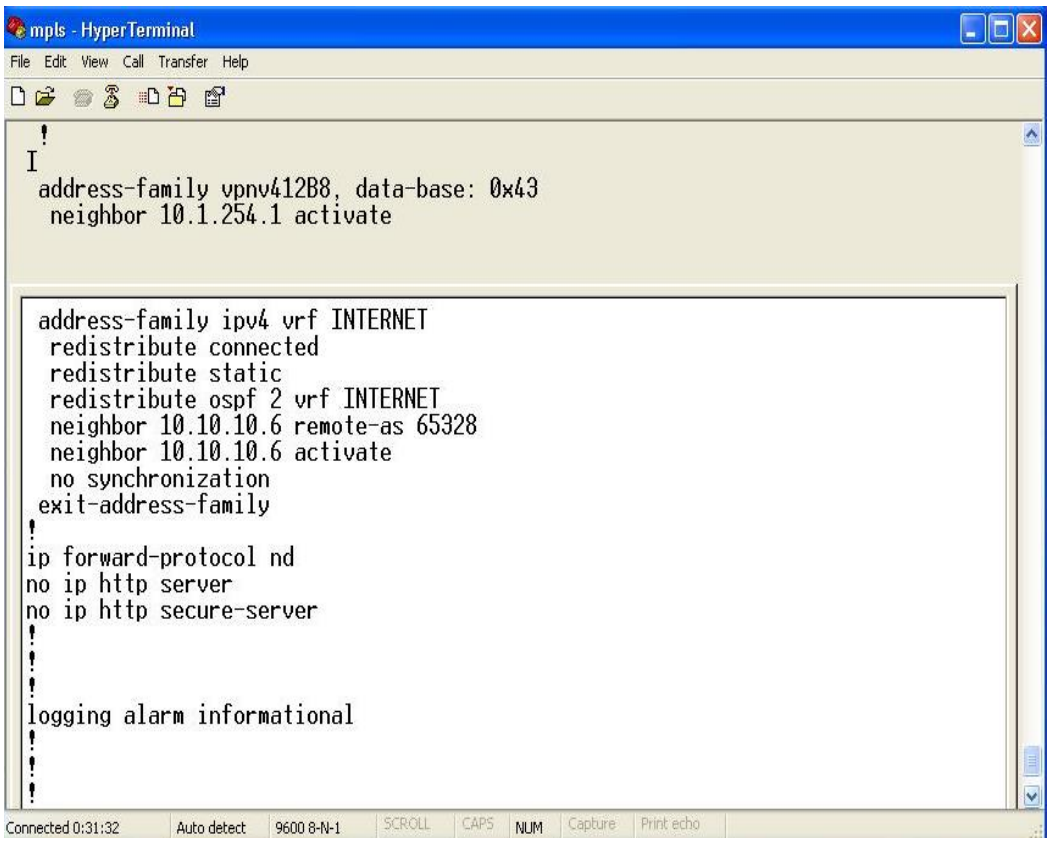


Рисунок 13 – Конфигурация VPN в CISCO 7204

Программы:
ip vrfINTERNET#
rd 65327:1##
route-target export 65327:1##
route-target import 65327:1##
!interface Loopback11#
ip address 10.1255.2 255.255.255.0#
router ospf 2 vrfINTERNET#
logadjacency-changes#
redistribute bgp 65327 subnets#
network 10.10.10.0 0.0.0.3 area 1#
address-family vpnv4##

neighbor 10.1254.1activate#
neighbor 10.1.2541 send-communityboth#
exitaddress-family#
address-familyipv4 vrf INTERNET@
redistribute connected
redistribute static
redistribute ospf 2 vrf INTERNET
neighbor 10.10.10.6 remote-as 65328
neighbor 10.10.10.6 activate#
no synchronization#
exit-addressfamily#

4.2.3. С помощью UTP кабеля соединиться с PE2 и прописать в конфигурацию.

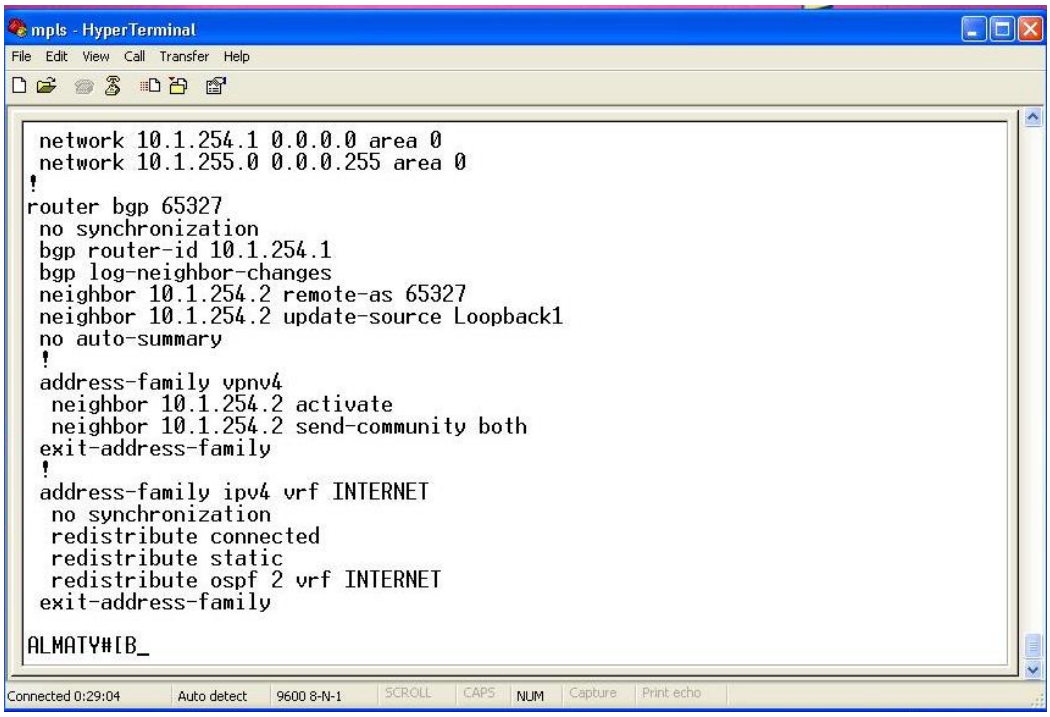


Рисунок 14 – Конфигурации VPN в CISCO 7604

Программа:
router ospf 2vrf INTERNET#
log-adjacency-changes#
redistribute bgp 65327 subnets#
network 10.10.100 0.0.0.3 area1#
address-familyvpnv4#
neighbor 10.1.254.2 activate1#
neighbor 10.1.2542 send-community both#
exit-address-family
address-familyipv4 vrf INTERNET#
no synchronization##
redistributeconnected##
redistribute static##
redistribute ospf 2 vrfINTERNET#
exit-addressfamily#

4.3. Контрольные вопросы

1. Что такое VPN?
2. Какие имеются способы реализации VPN?
3. Что такое VRF?
4. Что означает команда interface Loopback1?
5. Что означает команда redistribute bgp 65327 subnets 1?
6. Что означает команда address-family ipv4 vrf INTERNET?
7. Что такое нисходящий маршрутизатор, коммутирующий по меткам?
8. Какие протоколы можно отнести к протоколам с внутренней маршрутизацией?

5. Лабораторная работа № 5. Проверка связи между CE1 и CE2 по VPN

Цель работы: проверка соединения и получение конфигурации устройств.

5.1. Методические указания

5.1.1. Выполнить пункты 2.2.1, 2.2.2, 2.2.3, 2.2.4 лабораторной работы № 2.

5.1.2. С помощью кабеля UTP соединиться с PE1. Проверить IP адреса PE2 – 10.1.255.1, CE1 – 10.1.254.4, CE2 – 10.1.254.3., используя функцию PING.

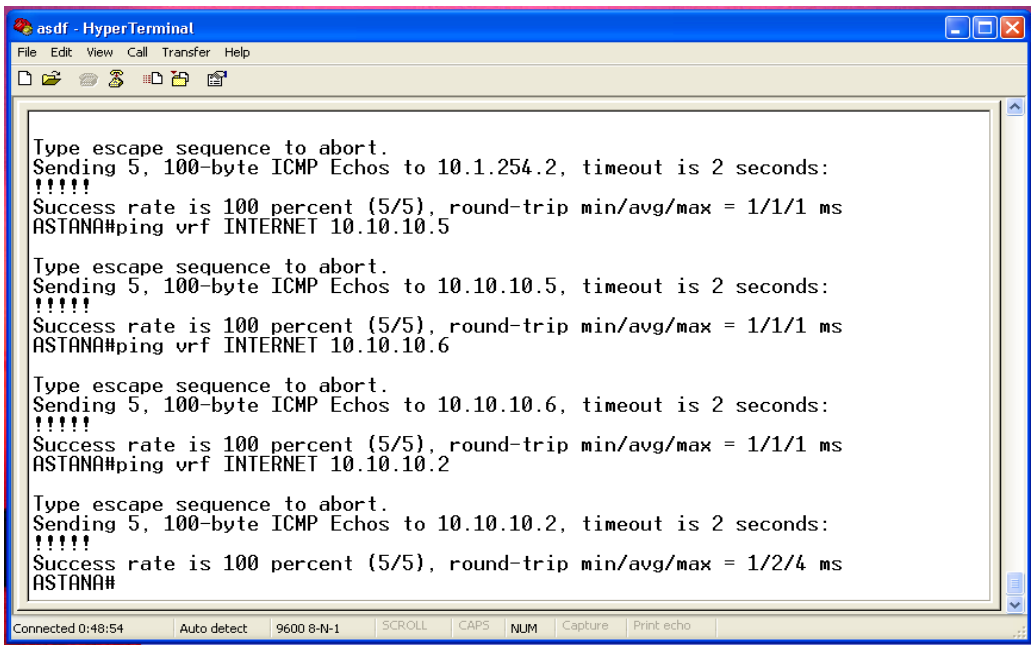


Рисунок 15 – Проверка соединения

5.1.3. Также проверить IP адреса от PE2, CE1, CE2 (IP адрес PE1 – 10.1.255.2).

5.1.4. Подсоединившись к CE1, проверить PING VRF INTERNET IP адреса на интерфейсах.

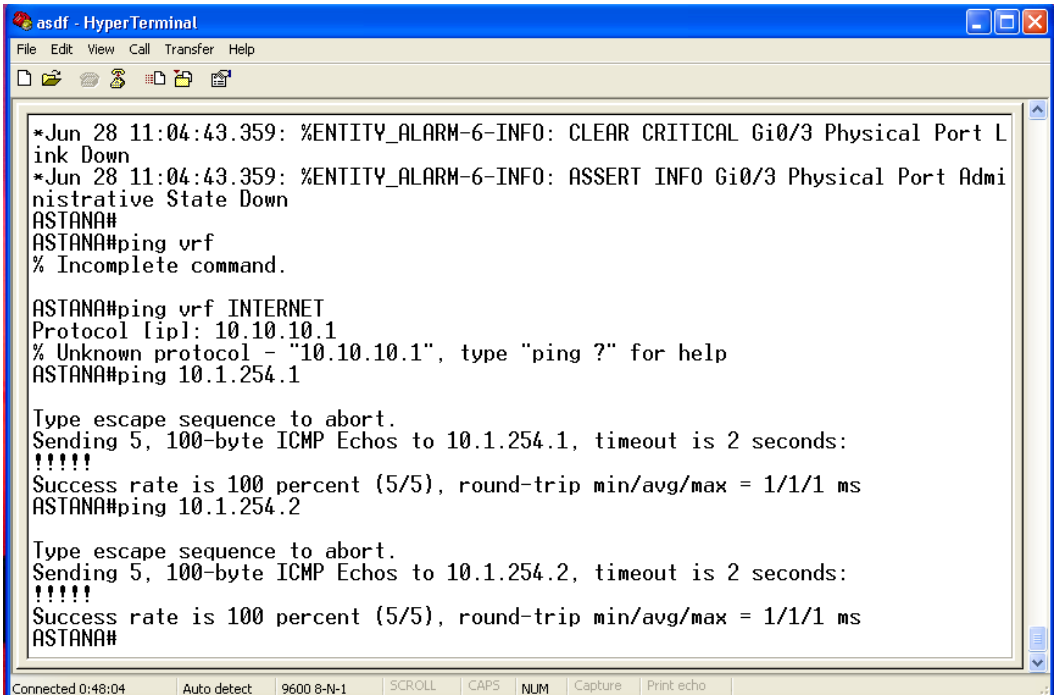


Рисунок 16 – Проверка VRF соединения

5.2. Контрольные вопросы

1. Что такое стек протоколов TCP/IP?
2. Что такое VRF?
3. Какой ping считается нормальным?
4. Протокол ICMP.
5. Что такое VPN?
6. Какие протоколы можно отнести к канальному уровню?
7. Что такое класс эквивалентной переадресации (FEC)?
8. Что такое восходящий маршрутизатор, коммутирующий по меткам (LSR)?

6. Лабораторная работа № 6. Запуск Mininet

Цель работы: запуск эмулятора компьютерной сети Mininet с использованием программы VirtualBox.

6.1. Рабочее задание

6.1.1. Создание виртуальной машины.
6.1.2. Запуск виртуальной машины.
6.1.3. Организация доступа к виртуальной машине через SSH.
6.1.4. Корректность настройки.

6.2. Методические указания

Сначала нужно установить VirtualBox из свободного доступа в интернете. На рисунке 17 показан первичный интерфейс программы.

Пакет программ Mininet используется для эмуляции транспортной сети. Транспортная сеть SDN рассматривается с использованием OpenFlow-контроллеров. На одной из виртуальной машин ВМ есть возможность строить сети из коммутаторов, контроллеров в различных топологиях.

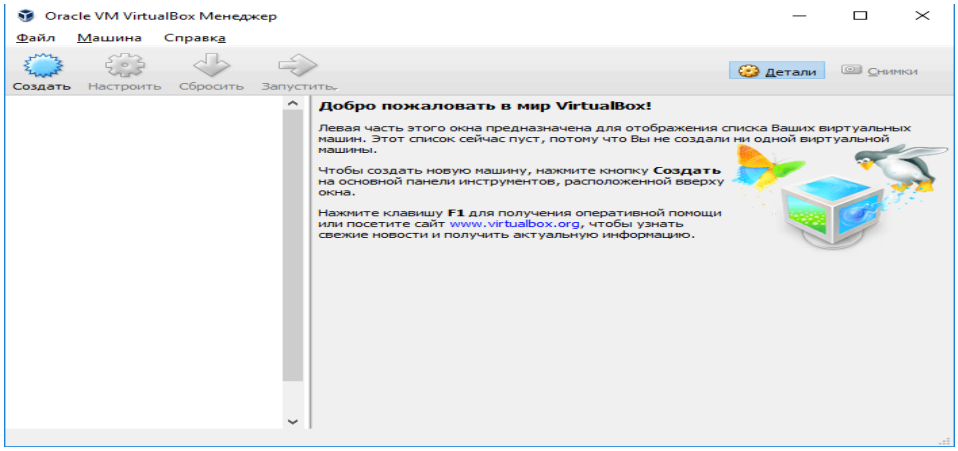


Рисунок 17 – Стартовая страница VirtualBox

Устанавливаем виртуальную машину (рисунок 18).

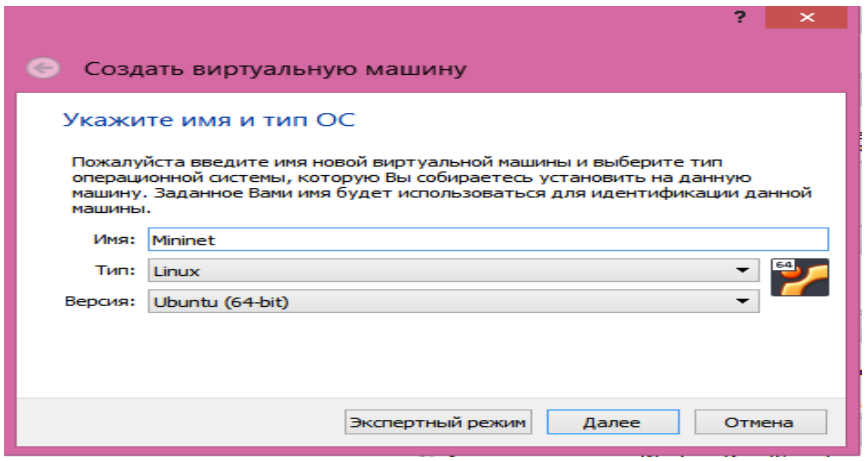


Рисунок 18 – Окно Mininet

Даем имя виртуальной машине – «Mininet» и далее указываем операционную систему Ubuntu (64-bit).

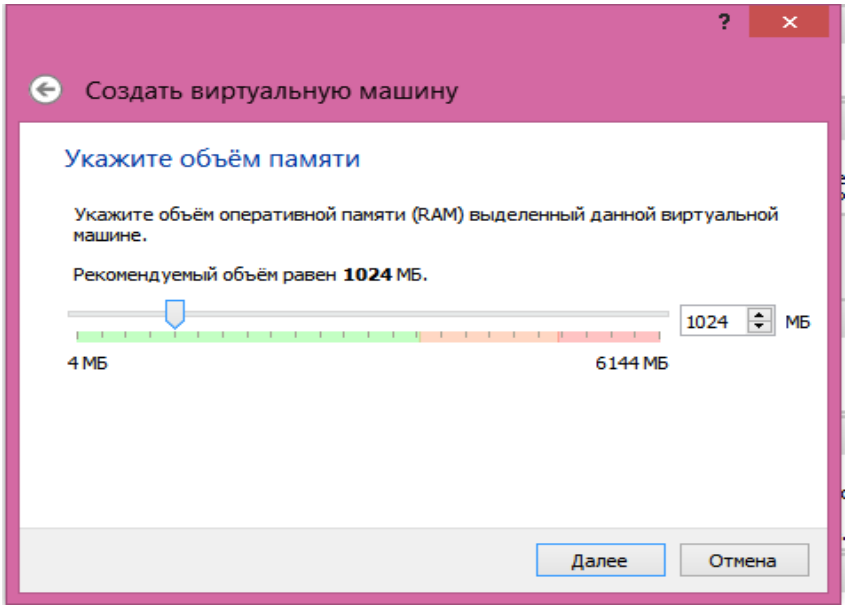


Рисунок 19 – Задание ОЗУ для Mininet

К виртуальной машине можно подключить жесткий диск (рисунок 20).

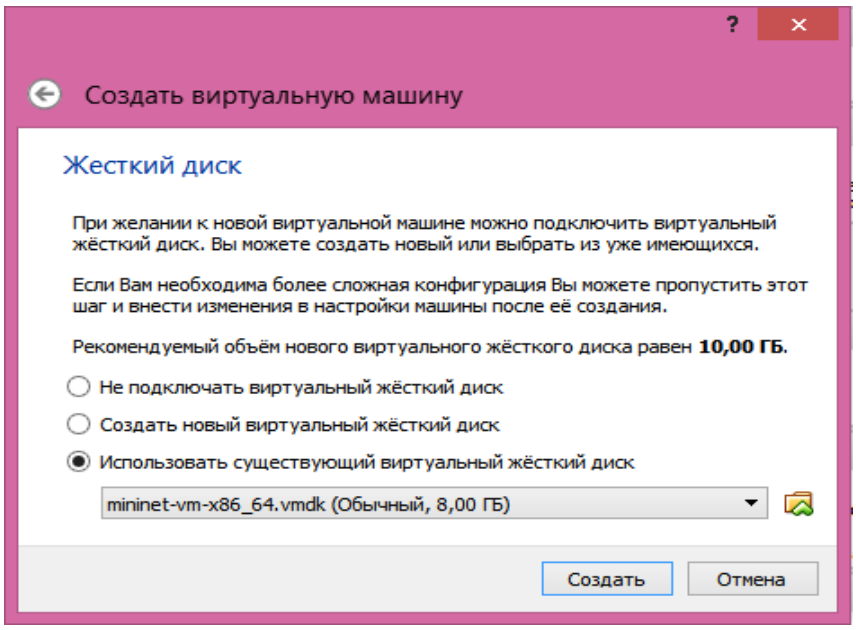


Рисунок 20 – Подключение жесткого диска

При создании виртуальной машины появляется имя Mininet в левом окошке программы ВМ.

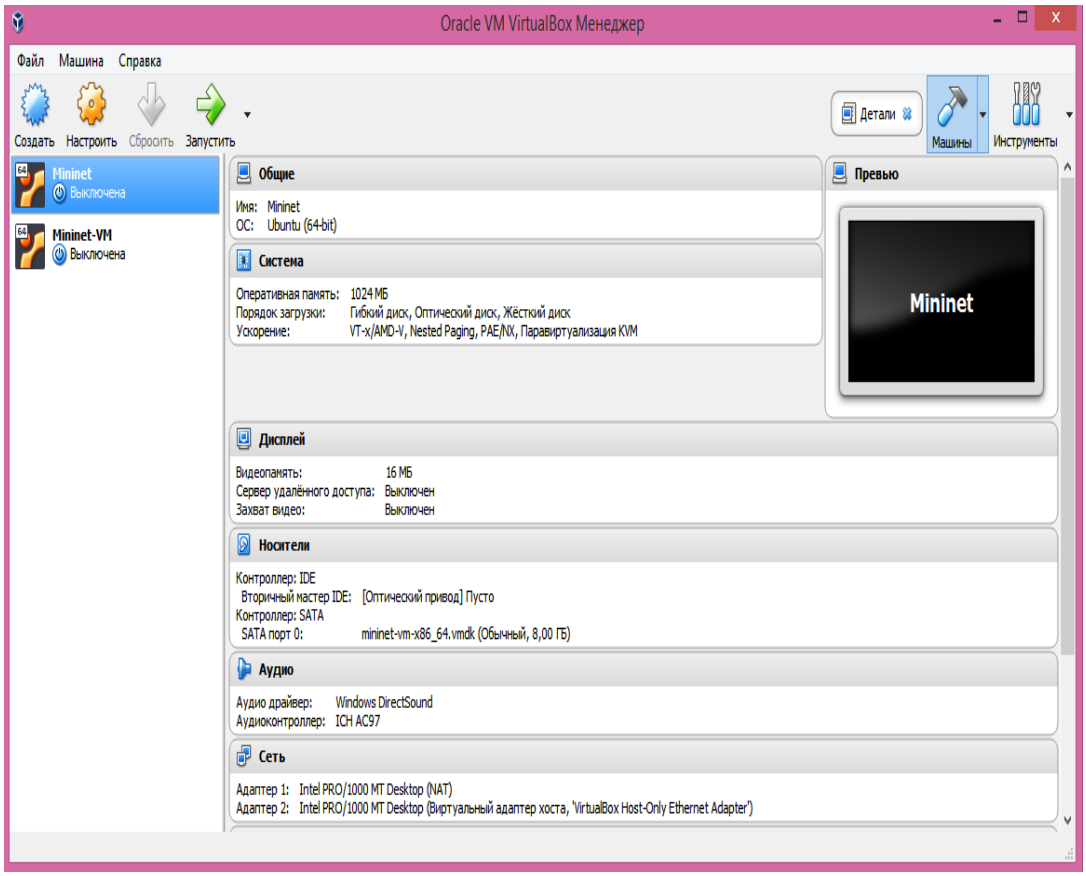


Рисунок 21 – Созданная ВМ

Нажимаем «Запустить», и должна выйти строка Mininet. Для входа в систему ВМ необходимо ввести имя и пароль: mininet-ВМ.

Login: mininet#

Password: mininet#

Здесь можно убедиться в возможности подключиться к гостевой виртуальной машине (Mininet) через SSH с главного компьютера.

Появляются 3 интерфейса (eth0, eth1, lo) eth1, имеющие IP-адреса (рисунок 22).

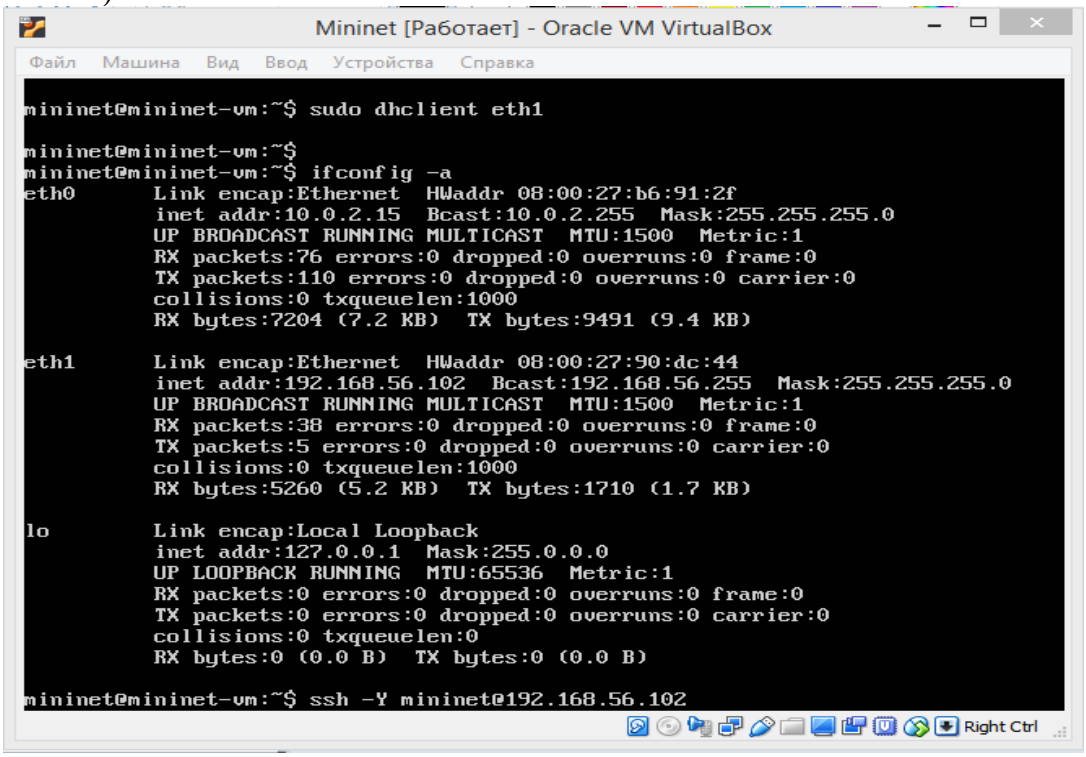


Рисунок 22 – Окно полученных интерфейсов

Затем нужно поставить команду для установки соединения с программой PuTTY.

mininet@mininet-vm:˜$ssh –Y mininet@192.168.56.102#

«192.168.56.102» является полученным интерфейсом eth11

Следом необходимо запустить программу PuTTY, используемую в качестве приложения GUI. Для подключения указываем IP-адрес: 192.168.56.102 своей ВМ и делаем пересылку X11.

На сервере Xming должны быть включены приложения xterm и wirehark. Далее нужно включить SSH-соединение с пересылкой X11.

Для включения пересылки X11 из графического интерфейса PuTTY нужно нажать PuTTY → SSH → X11и потом перенаправление → «Enable X11 forwarding» (рисунок 23).

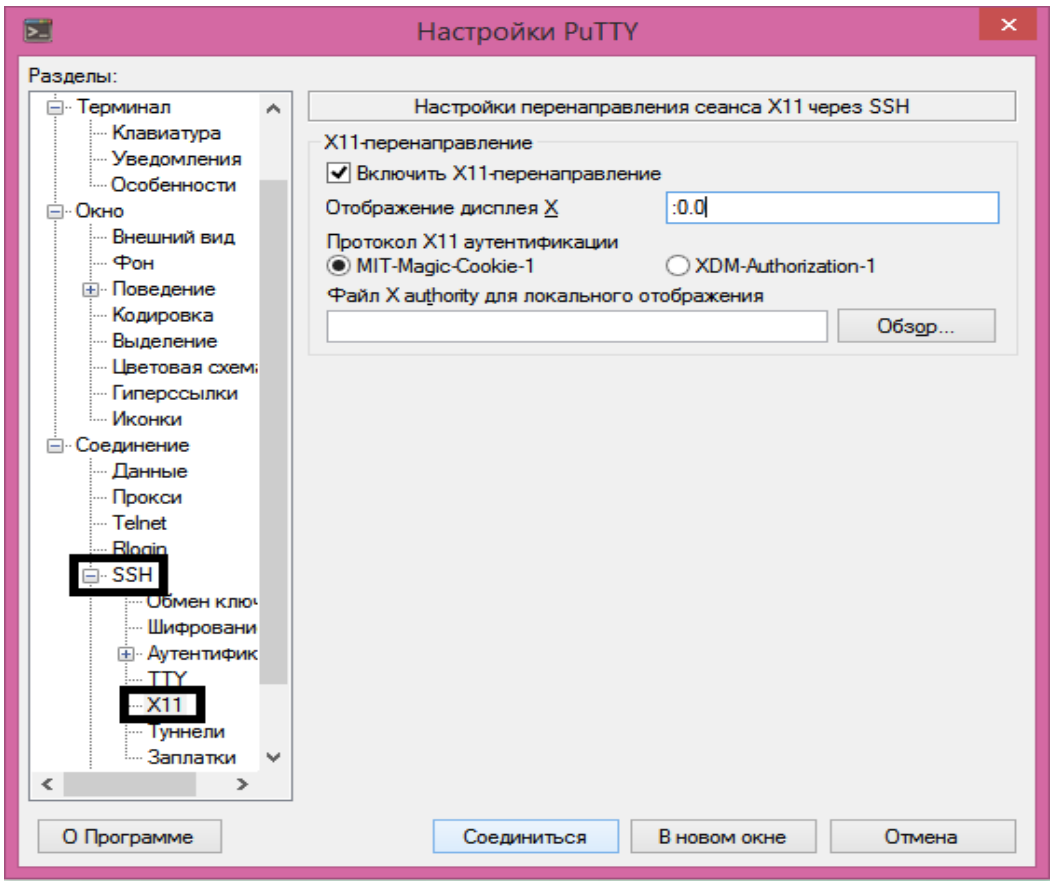


Рисунок 23 – Окно конфигурации

Для входа используется следующие имя и пароль: mininet.

Введем команду:

mininet@mininet:~$ sudo wireshark &@#

Создается минимальная сеть, состоящая из коммутатора (s1), двух хостов (h1, h2) и контроллера (c0). Программа mn будет в режиме команд интерпретации.

Появится CLI Mininet. В CLI нужно ввести:

Mininet#> h1 pingc 1 h2#

Ping есть, и идет передача пакетов без потерь.

Это можно подтвердить, используя программу Wireshark.

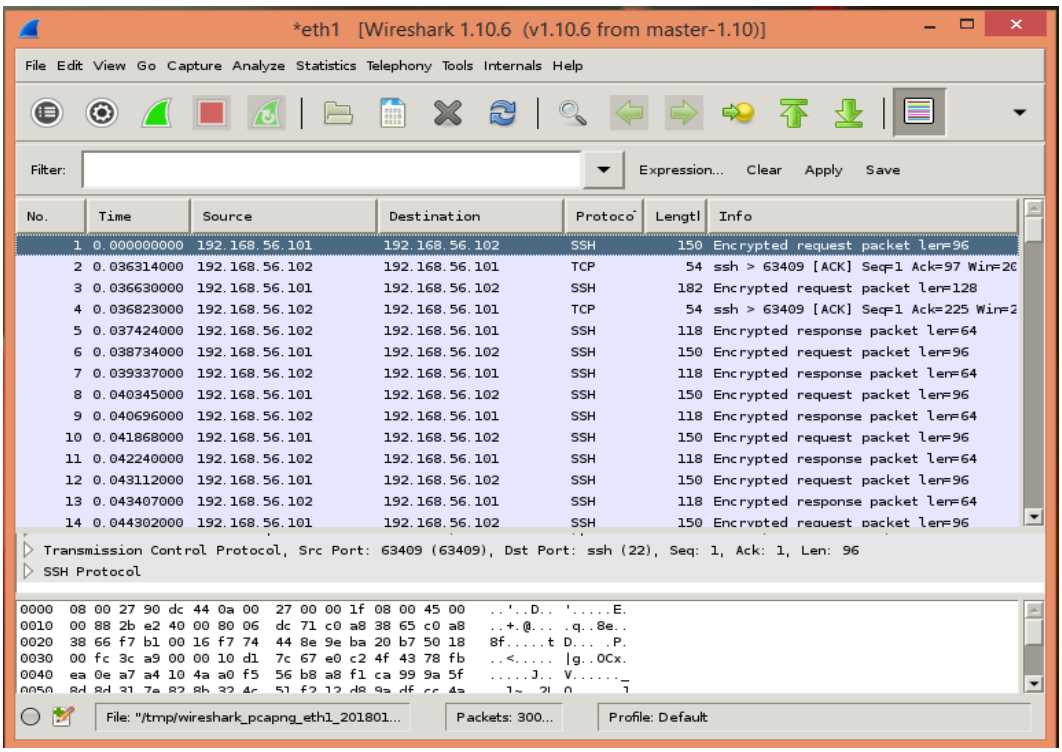


Рисунок 24 – Программа-анализатор трафика Wireshark

Эмулятор Mininet успешно установлен.

6.3. Контрольные вопросы

1. Что такое виртуальная машина?
2. Что такое Mininet?
3. Для чего предназначен протокол SSH?
4. Каково назначение программы Wireshark.
5. Чем отличаются симуляторы и эмуляторы?
6. Какие вы еще знаете эмуляторы сетей?
7. . Какие вы еще знаете симуляторы сетей?
8. Какие есть протоколы защиты на канальном и сетевом уровнях модели OSI?

7. Лабораторная работа № 7. Настройка сетевой топологии SDN

Цель работы: разработка сетевой топологии SDN с помощью графического интерфейса MiniEdit.

7.1. Рабочее задание

7.1.1. Запустить ВМ Mininet, как в лабораторной работе № 6.
7.1.2. Организовать запуск графического редактора MiniEdit.
7.1.3. Создать топологию из двух хостов, коммутатора и контроллера.
7.1.4. Провести проверку работоспособности.

7.2. Методические указания

7.2.1. Запустить ВМ. Использовать следующие имя и пароль:

Login: mininet#

Password: mininet#

На консоли виртуальной машины вводим:

$ sudo dhclienteth1#

$ ifconfig a#

Появятся интерфейсы (eth0, eth1, lo). eth1 с назначенными IP-адресами, как в предыдущей лабораторной работе.

Далее нужно ввести команду для соединения с PuTTy:

$ ssh –Y mininet@«IP-адрес eth1»#

7.2.2. Используем программу PuTTY, указывая IP-адрес:

«IP-адрес eth1» #созданной ВМ, включив пересылку X11.

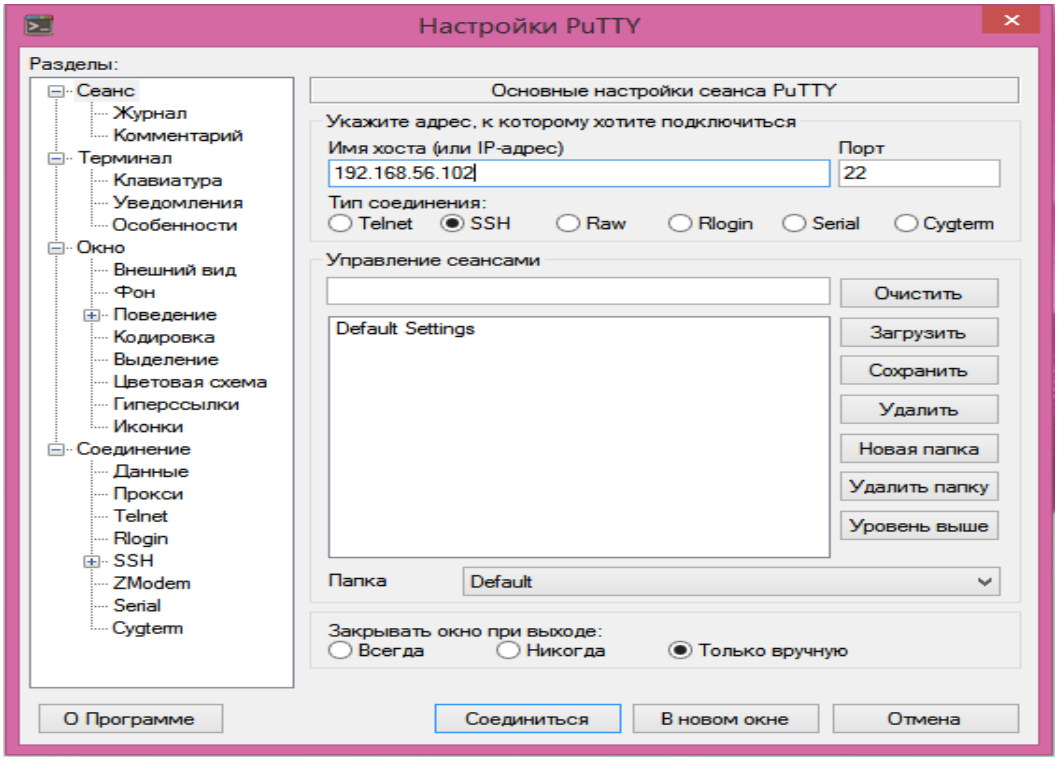


Рисунок 25 – Настройки PuTTY

Здесь также используем пароль и имя mininet. Для запуска MiniEdit, введем команду:

mininet@mininet:~$ sudo python ./mininet/examp1es/miniedit.py##

Для запуска Mininet привилегиями root запускаем MiniEdit, используя команду sudo.

В MiniEdit есть Host с инструментами с левой стороны в меню (рисунок 26).

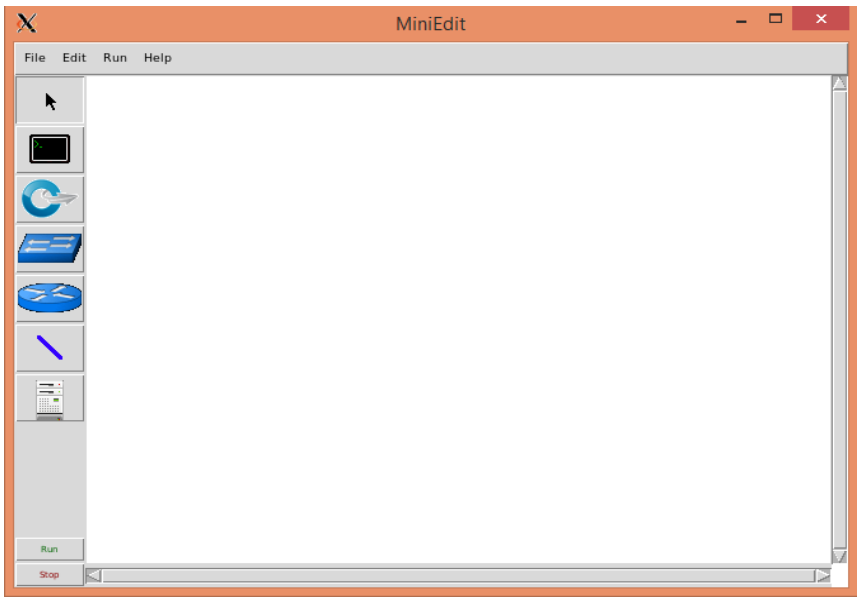


Рисунок 26 – Окно MiniEdit

7.2.3. Добавляем два хоста в настройку. Нажимая на значок «Host» перемещаем указатель на местоположение в окне MiniEdit. В окне должен появится значок Host.

При активности «Host» есть возможность добавлять еще хосты. Здесь было добавлено 2 хоста.

Нажимая на «Switch», добавим коммутатор и на «Controller» получим контроллер.

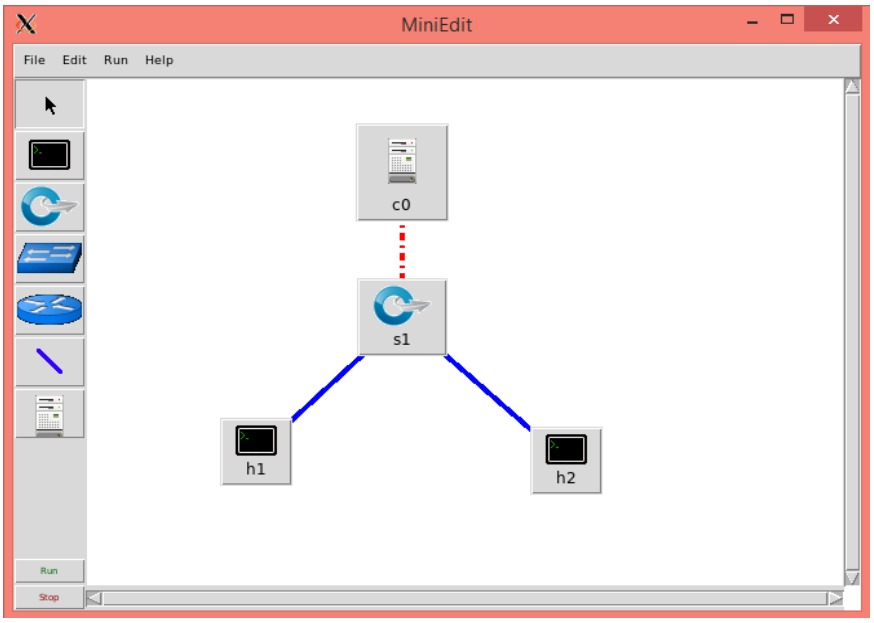


Рисунок 27 – Окно с примером топологии сети

Для настройки возможностей MiniEdit можно применить команду MiniEdit, Edit → Preferences. Для использования CLI Mininet при его запуске нужно установить флажок «START CLI». Нажимаем «ОК».

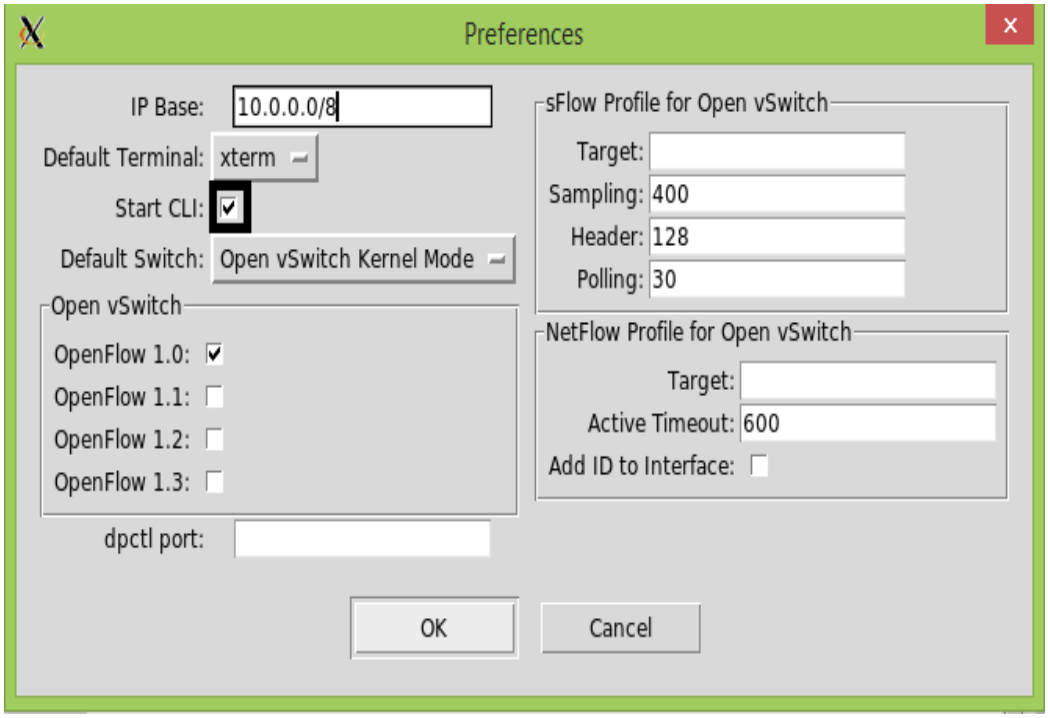


Рисунок 28 – Окно Preferences

Нажимаем кнопку «Выполнить» в MiniEdit(me). В окне запуска me появятся сообщения, которые отображают показывающие запуск моделирования и приглашение Starting CLI.

7.2.4 В сценарии устанавливается топология сети с приглашением (mininet>#).

С консоли me запускаем команду ping. Проверяем работоспособность сети.

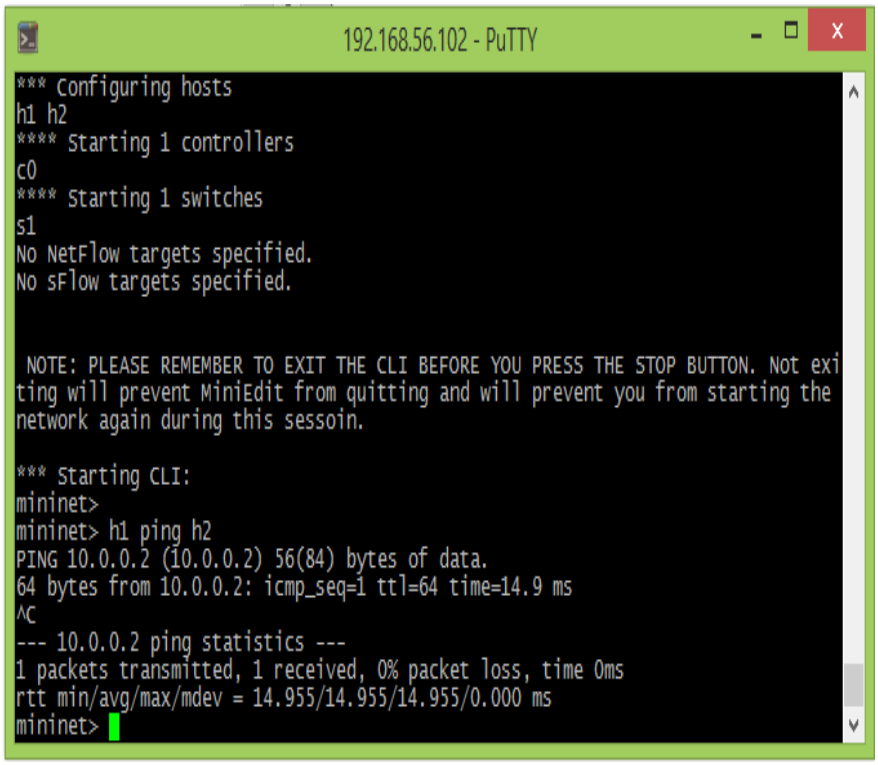


Рисунок 29 – Окно р команды ping

7.3. Контрольные вопросы

1. Каково назначение программа PuTTy?
2. Что такое программа Mininet?
3. Каково назначение программы MiniEdit?
4 Каково назначение программы Wireshark?
5. Какие еще эмуляторы транспортных сетей вы знаете?
6. Каково быстродействиево графического редактора MiniEdit?
7. Какие симуляторы транспортных сетей вы ещезнаете?
8. Что входит в состав сетевой топологии SDN?

8. Лабораторная работа № 8. Создание виртуальной лаборатории SDN

Цель работы: создание виртуальной лаборатории SDN на основе Mininet.

8.1. Рабочее задание

8.1.1. Запустить графический интерфейс MiniEdit(me).

8.1.2. Создать топологию транспортной сети из 4 хостов, 2 коммутаторов и одного контроллера.

8.1.3. Проверить работоспособность сети, используя пакет Wireshark.

8.2. Методические указания

8.2.1. Виртуальной лаборатория SDN будет состоять из коммутаторов OpenFlow и хостов Linux. Здесь используются пакеты программ MiniEdit и графический интерфейс Mininet.

Для запуска MiniEdit (me) ставим команду:

$ sudo ~/mininet/examp1es/miniedit.py#

Далее должно появиться полотно MiniEdit.

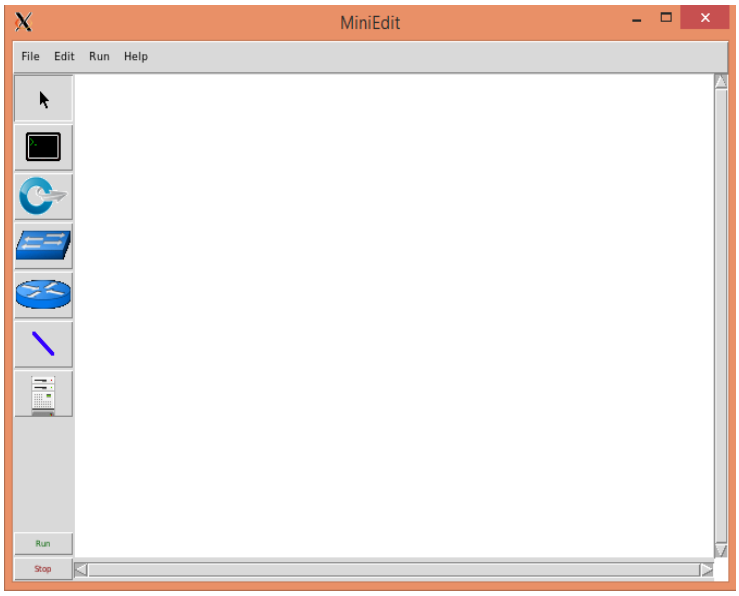


Рисунок 30 – Полотно me

8.2.2 Создаем сеть, имеющую в своем составе 2 коммутатора, 4 хоста и один контроллер. Каждый коммутатор соединен с двумя хостами. Контроллер подключается к коммутаторам (рисунок 31).

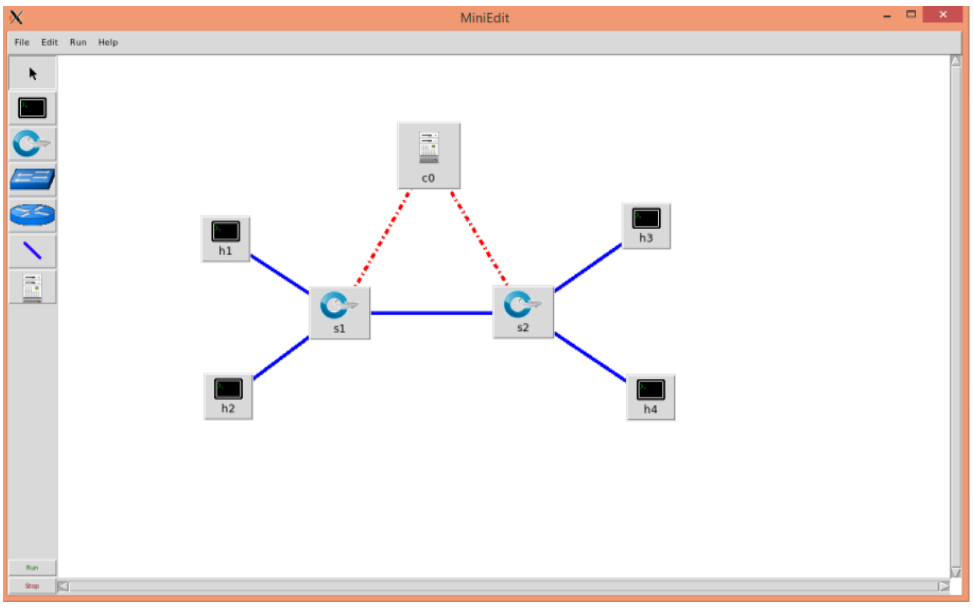


Рисунок 31 – Окно транспортной сети

Нажимаем «Начать CLI» в окне настроек me.

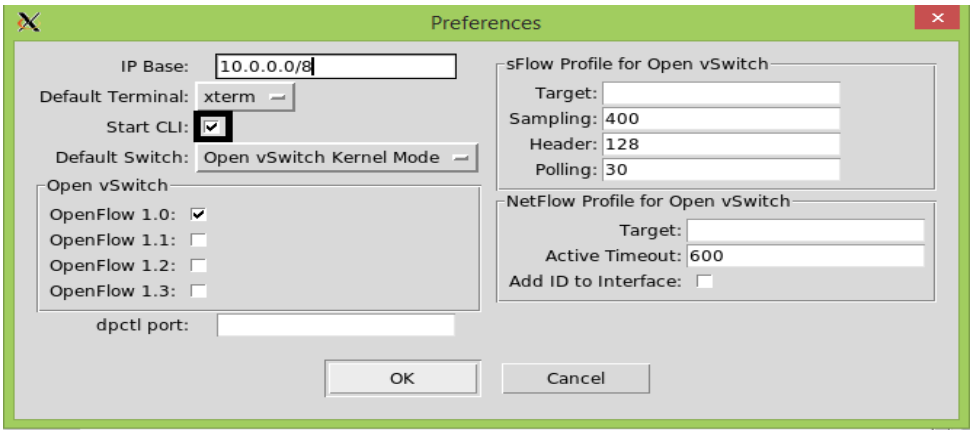


Рисунок 32 – Включение CLI в окне настроек me

Для настройки контролера необходимо щелчком правой кнопки мыши на контроллере выбрать «Свойства». Далее выбрать Remote Controller.

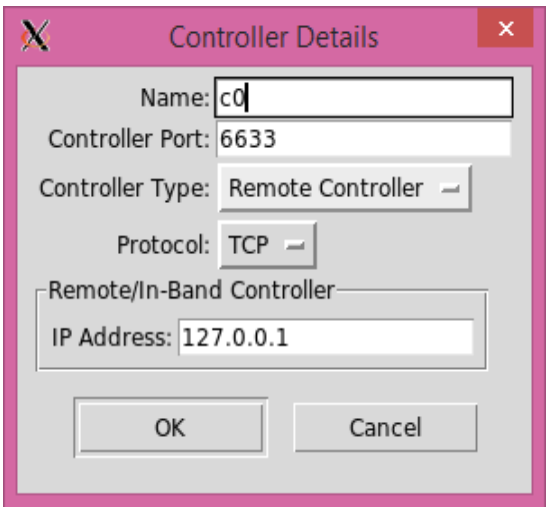


Рисунок 33 – Свойства контроллера

При настройке хостов даем им IP-адреса от 10.0.0.1 до 10.0.0.4.

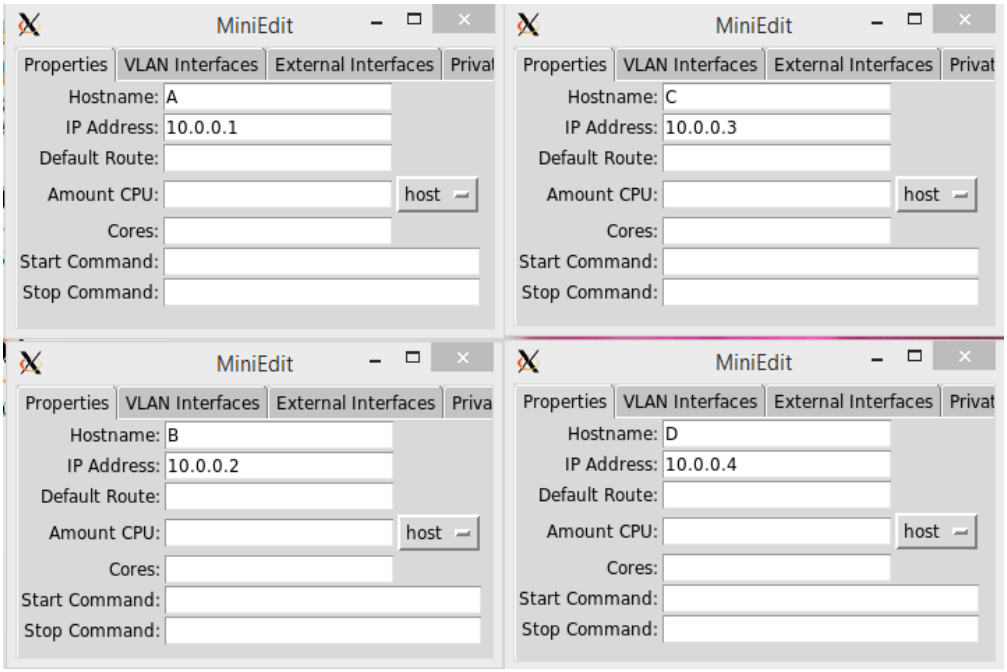


Рисунок 34 – Назначение адресов

Сохранить эту сборку mn.

8.2.3. Открыть окно xterm1 на всех 4 хостах. Щелкнув правой кнопкой мыши в me, выбрать «Терминал».

Далее для мониторинга трафика в окне h1 xterm нужно запустить Wireshark, используя команду «wireshark &». В окне h4 xterm запустить команду «tcpdump» для трассировки пакета.

Для второй проверки работоспособности между хостами h1 и h4 запустить команду ping. Вводим с консоли mn команду:

Mininet#> h1 ping h4#

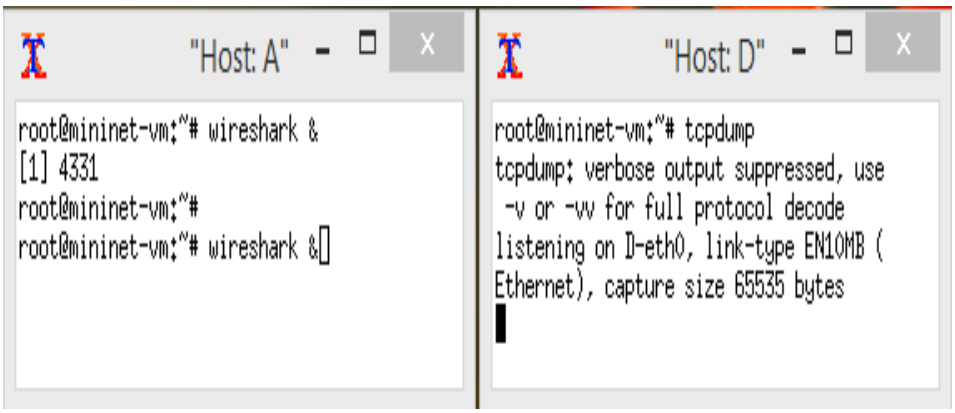


Рисунок 35 – Команда xterm

В консоли me появятся результаты команды ping. В программе Wireshark будут видны ICMP пакеты с ответами.

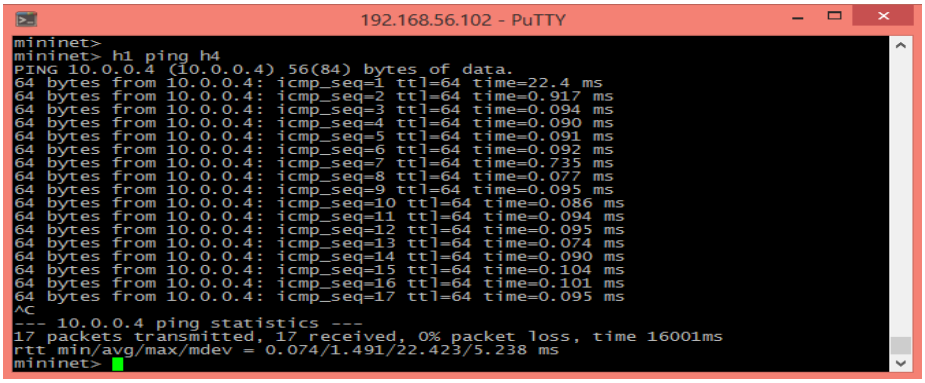


Рисунок 36 – Окно результатов команды ping

8.3. Контрольные вопросы

1. Что такое программно-определяемая сеть SDN?
2. Каково назначение протокола OpenFlow?
3. Какой программой проверяется роботоспособность сети?
4. С какими протоками защиты работает программа Wireshark?
5. Чем отличается технология SDN от классических транспортных сетей связи?
6. Какие основные компоненты технологии сетей SDN?
7. Каковы основные задачи контроллера SDN?
8. Для чего реализовано в SDN разделение функций передачи трафика от функций управления?

9. Лабораторная работа № 9. Использование контроллера OpenDaylight SDN

Цель работы: изучение работы контроллера OpenDaylight SDN с эмулятором сети Mininet.

9.1. Рабочее задание

9.1.1. Подключить к ВМ OpenDaylight, используя протокол SSH.
9.1.2. Подключить к ВМ Mininet, используя протокол SSH.
9.1.3. Осуществить захват сообщений OpenFlow.
9.1.4. Проанализировать работоспособность в Wireshark.

9.2. Методические указания

9.2.1. Дать ВМ имя OpenDaylight. Необходимо его настроить с использованием двух процессоров и двух ГБ оперативной памяти. Далее необходимо добавить адаптер сети хоста в ВМ.

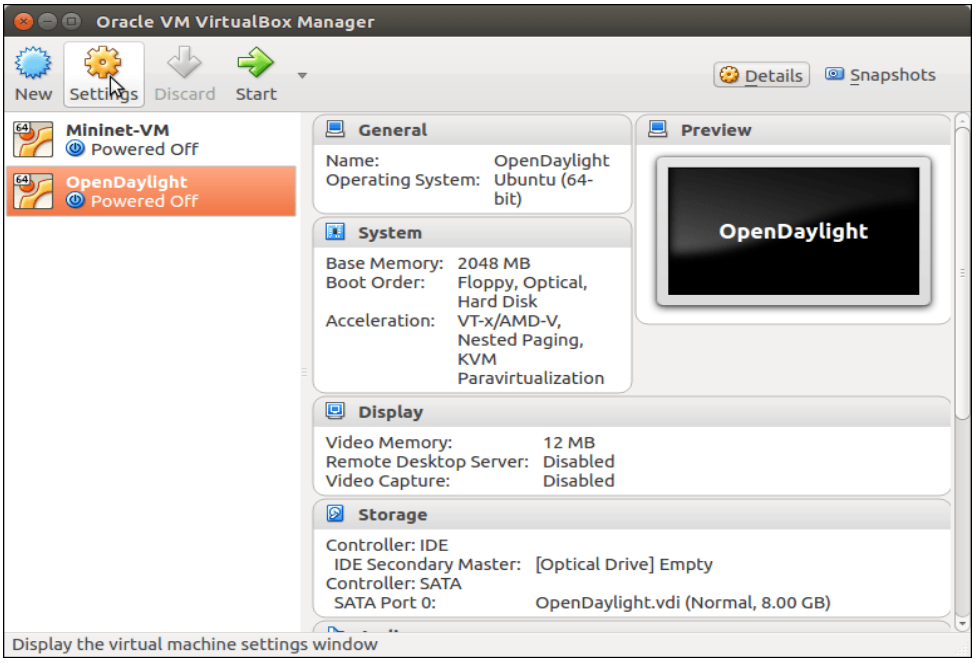


Рисунок 37 – Виртуальная машина OpenDaylight

В ВМ включить 2 сетевых интерфейса. К интерфейсу NAT нужно подключить первый сетевой адаптер, а 2-й сетевой адаптер подключить к сети для хоста VirtualBox Host-Only Eth Adapter.

Видно в окне, что интерфейс enp0s8 не имеет IP-адреса. Это относится ко второму сетевому адаптеру, подключенному к Vbox Host-Only Eth Adapter. Пакет программ VirtualBox имеет возможность назначать IP-адрес этого интерфейса, используя протокол DHCP при запросе от своего клиента.

Запустить команду настройки интерфейса enp0s8:

brian@odl:~$ sudo dhclient enp0s8#

Проверив IP-адрес, присвоенный enp0s8, увидим, что DHCP-сервер VirtualBox дал этому IP-адрес 192.168.56.101#.

9.2.2. Открыть терминал на главном компьютере и войти в систему с помощью протокола SSH:

brian@T420:~$ ssh -X brian@192.168.56.10/1#

Сейчас есть подключение к ВМ OpenDaylight. Можно видеть, что имя стало odl.

Для запуска OpenDaylight используем команду karaf, которая находится в папке для распространения пакетов:

brian@odl:~$ cd distribution-karaf0.4.0-Beryllium#

brian@odl:~$ ./bin/karaf#

9.2.3. Запустить ВМ Mininet в VirtualBox Manager. В данный момент уже созданы две ВМ: OpenDaylight VM и Mininet VM. При запуске виртуальной машины OpenDaylight видно, что у нее IP-адрес 192.168.56.101, а ВМ Mininet получила 2-й IP-адрес для хоста – 192,168.56.102#.

Далее нужно открыть окно программы PuTTy на хосте и протокол SSH в VM Mininet. Включить X forwarding.

В открытом браузере вводим URL-адрес пользовательского интерфейса OpenDaylight (интерфейс DLUX), который определен на ВМ OpenDaylight, с IP-адресом 192.168.56.102 и портом 8181:

http://192.168.56.101:8181/index.html#

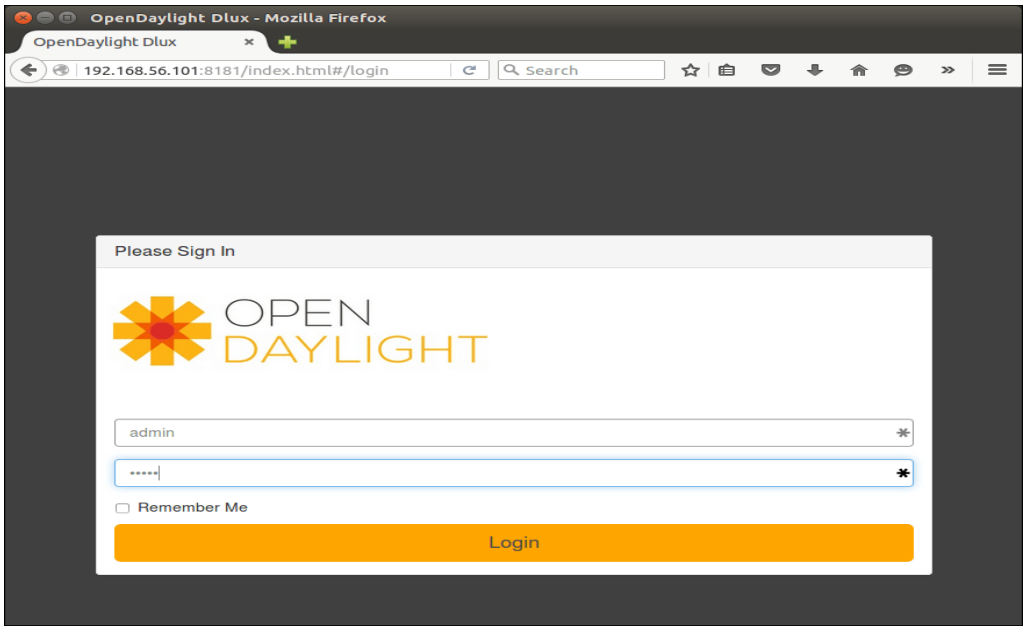


Рисунок 38 – Окно контроллера OpenDaylight

Можно увидеть топологию сети на рисунке 39.

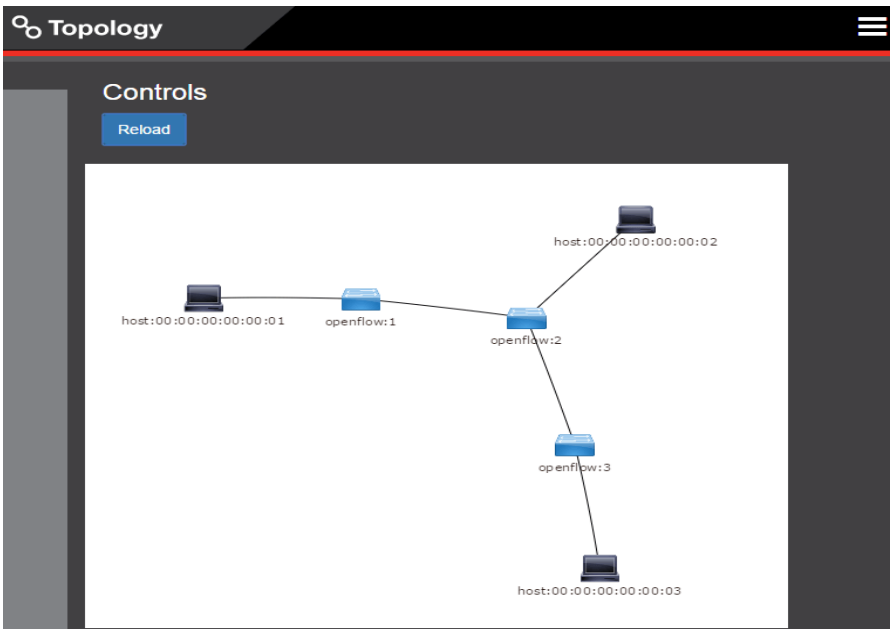
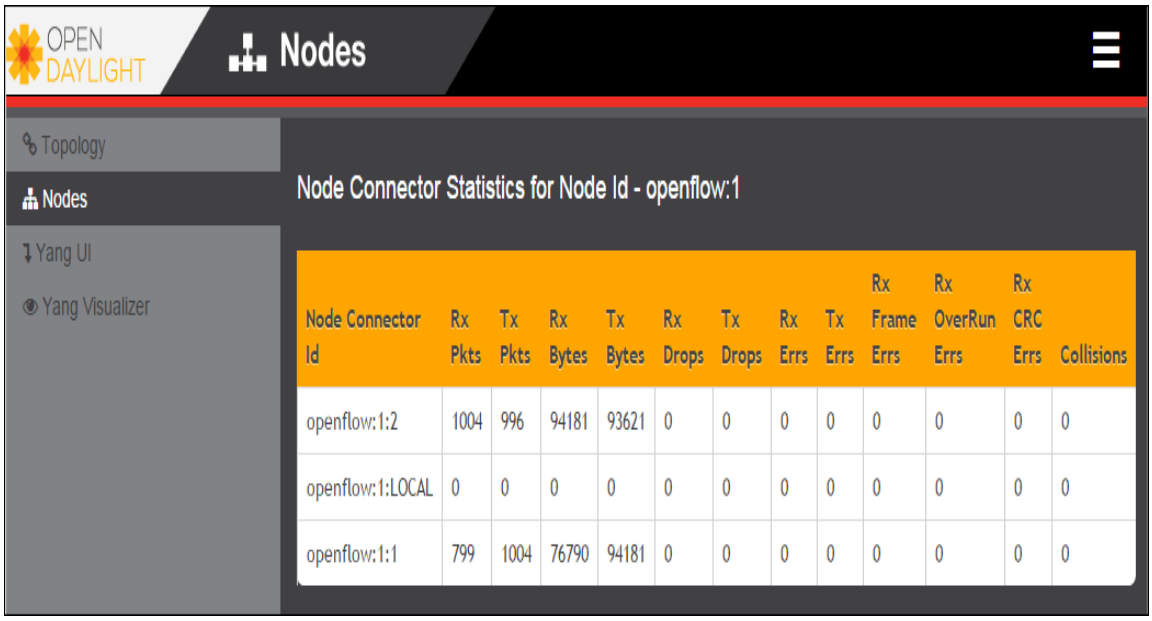


Рисунок 39 – Окно топологии сети Mininet

Для просмотра информации о портах коммутатора нужно нажать на ссылку Node Connectors (рисунок 40).



Node Connector Id	Rx Pkts	Tx Pkts	Rx Bytes	Tx Bytes	Rx Drops	Tx Drops	Rx Errs	Tx Errs	Rx Frame Errs	Rx OverRun Errs	Rx CRC Errs	Collisions
openflow:1:2	1004	996	94181	93621	0	0	0	0	0	0	0	0
openflow:1:LOCAL	0	0	0	0	0	0	0	0	0	0	0	0
openflow:1:1	799	1004	76790	94181	0	0	0	0	0	0	0	0

Рисунок 40 – Интерфейсы коммутатора

9.2.4. Для более основательного изучения работы контроллера SDN и коммутатора можно посмотреть сообщения OpenFlow между контроллером и коммутаторами в сети.

Для этого нужно запустить Wireshark на ВМ Mininet и захватить данные на интерфейсе eth1 хоста.

Создать фильтр отображения для сообщений OpenFlow. Ввести текст ofb окне «Фильтр» и нажать « Применить» .

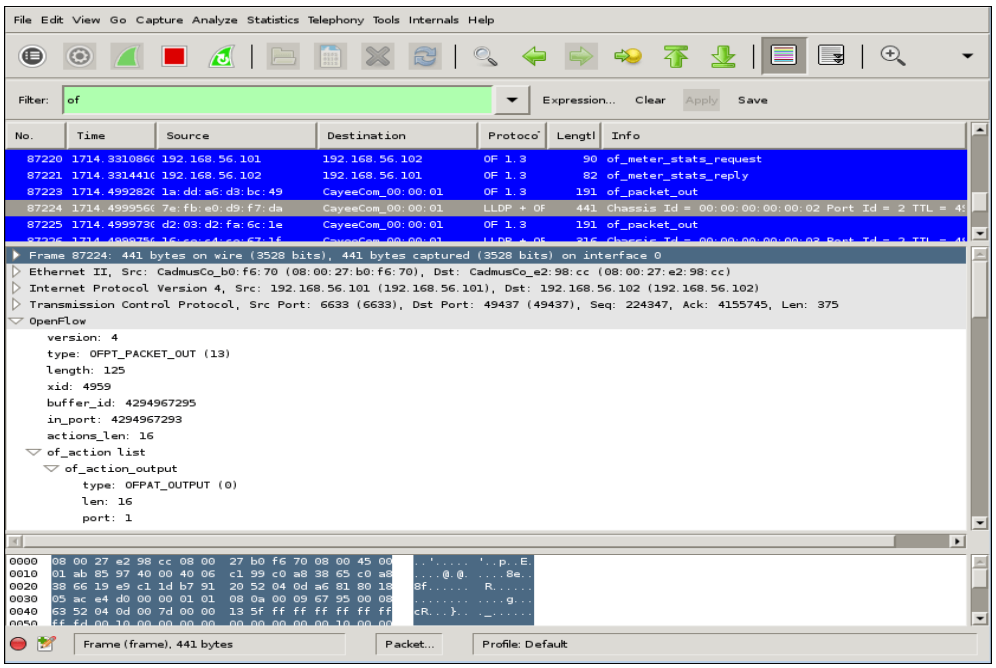


Рисунок 41 – Сообщения OpenFlow в Wireshark

9.3. Контрольные вопросы

1. Какие приемущества есть у технологии SDN?
2. Как выглядит логическая модель сетевых устройств SDN?
3. Каково назначение контроллера OpenDaylight SDN?
4. Каков состав коммутатора OpenFlow?
5. Для чего применяется технология NAT?
6. Что означает команда brian@odl:~$ cd distribution-karaf-0.4.0-Beryllium?
7. Что означает команда brian@T420:~$ ssh -X brian@192.168.56.101?
8. Каково назначение OpenFlow портов.

10. Лабораторная работа № 10. Создание пользовательской сетевой топологии SDN

Цель работы: создание и настройка сетевой топологии в SDN.

10.1. Рабочее задание

10.1.1. Запустить MiniEdit.
10.1.2. Получить и настроить пользовательскую топологию.
10.1.3. Провести эксперименты с сетью.
10.1.4. Организовать имитацию не работающей ссылки.

10.2. Методические указания

10.2.1. Если mn находится в своей ОС, то me будет запускаться при запуске команды python miniedit.py
$ sudo ~ / mininet / examp1es / miniedit.py#

Рисунок 42 – Полотно me

Затем нужно добавить в интерфейс 10 хостов (Рисунок 43)

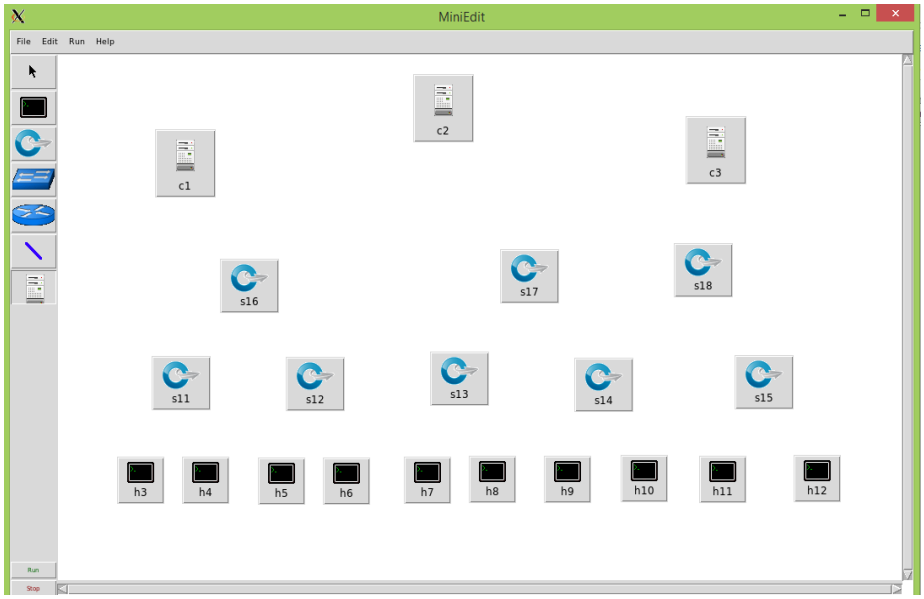


Рисунок 43 – Хосты коммутаторов и контроллеров

Далее нужно добавить ссылки между узлами на полотне. Для этого нужно нажать на инструмент NetLink и затем, щелкнув узел, перетащить ссылку на другой узел.

Завершенная сеть представлена на рисунке 44.

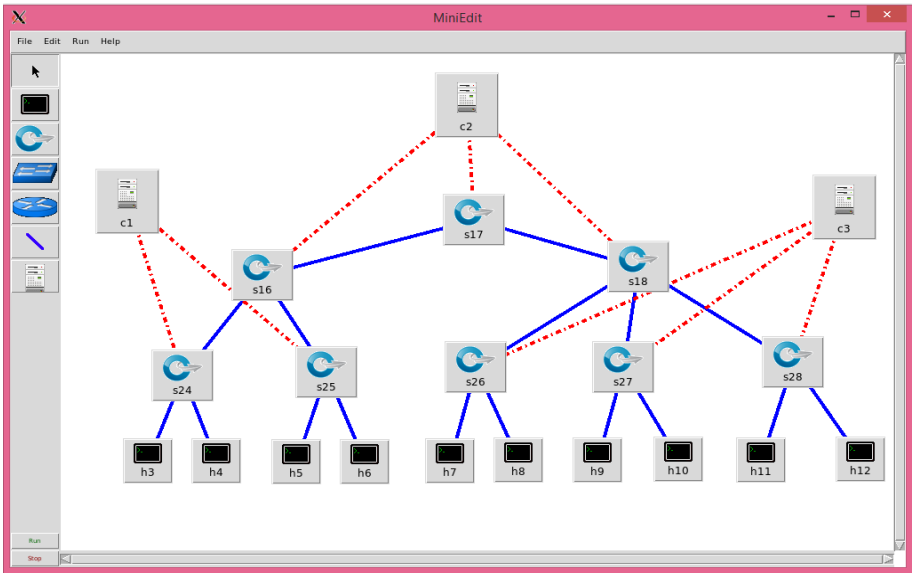


Рисунок 44 – Окно сети

При настройке трех контроллеров необходимо установить опцию Start CLI и запустить сетевой сценарий.

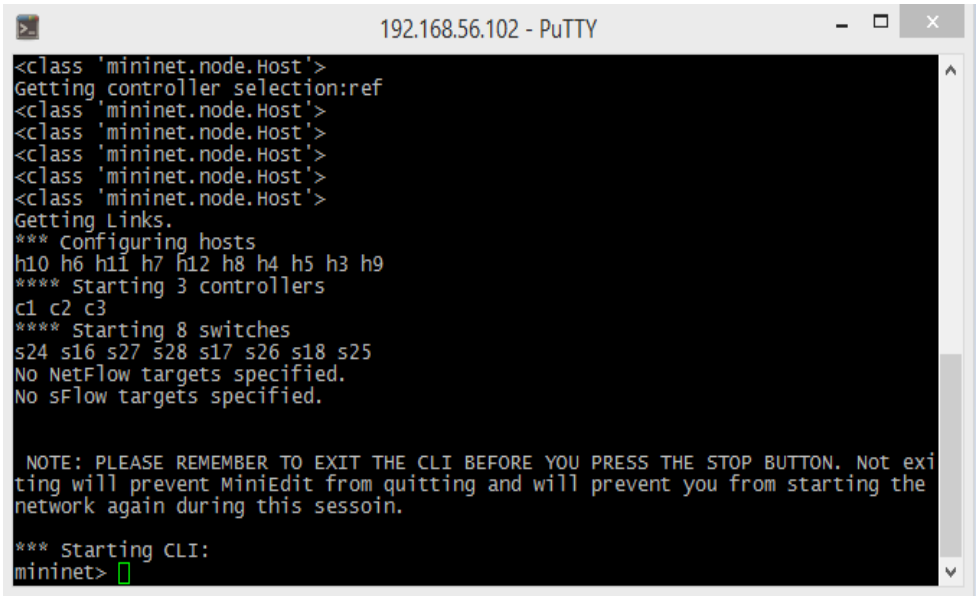


Рисунок 45 – Приглашение Mininet в консоле MiniEdit

Необходимо обратить внимание на предупреждение. Здесь нужно перед остановкой моделирования ввести команду exit в Mininet строке в окне mn в консоли.

10.2.2. Для того, чтобы смоделировать сетевые сбои, необходимо открыть окна терминала. Далее запустить сетевой трафик, запустить программы на моделируемых хостах. В меню MiniEdit запустить «Показать сводку OVS», для просмотра списка конфигураций коммутатора (Рисунок 46).

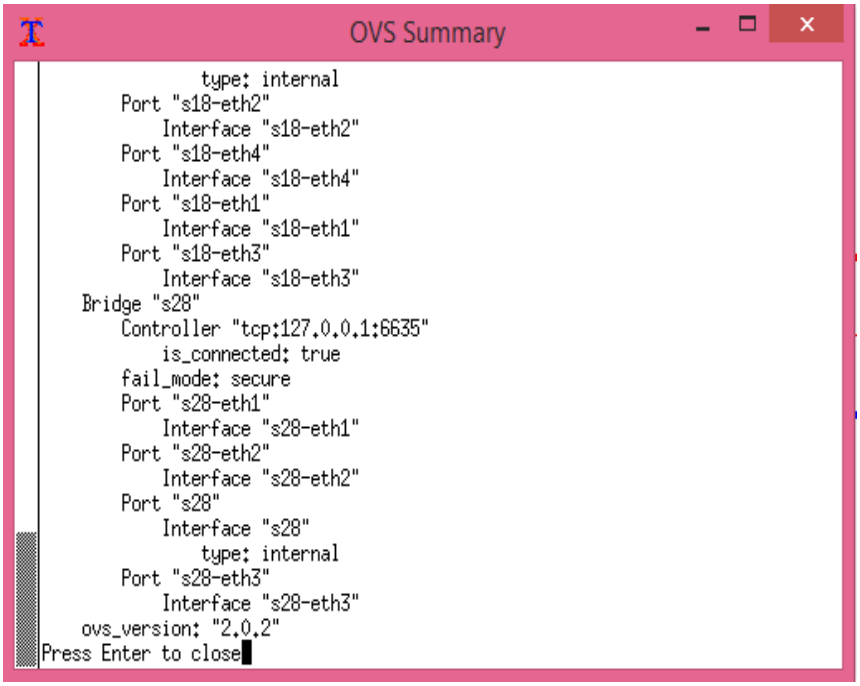


Рисунок 46 – Сводки OVS

Открыть окно xterm на хостах h3 и h8. Выбрать «Терминал» в появившемся меню, щелкнув правой кнопкой мыши на каждый узел в графическом me. Запустить Wireshark в окне h3 xterm &#. Там же с помощью команды tcpdump# запустить трассировку, как в предыдущей работе, для демонстрации двух разных методов мониторинга трафика на виртуальных портах.

Далее ввести в окне консоли MiniEdit команду ping для отправки трафика между хостами h3 и h8:

mininet> h3 ping h8#

Результат контроля трафика показан на рисунке 47.

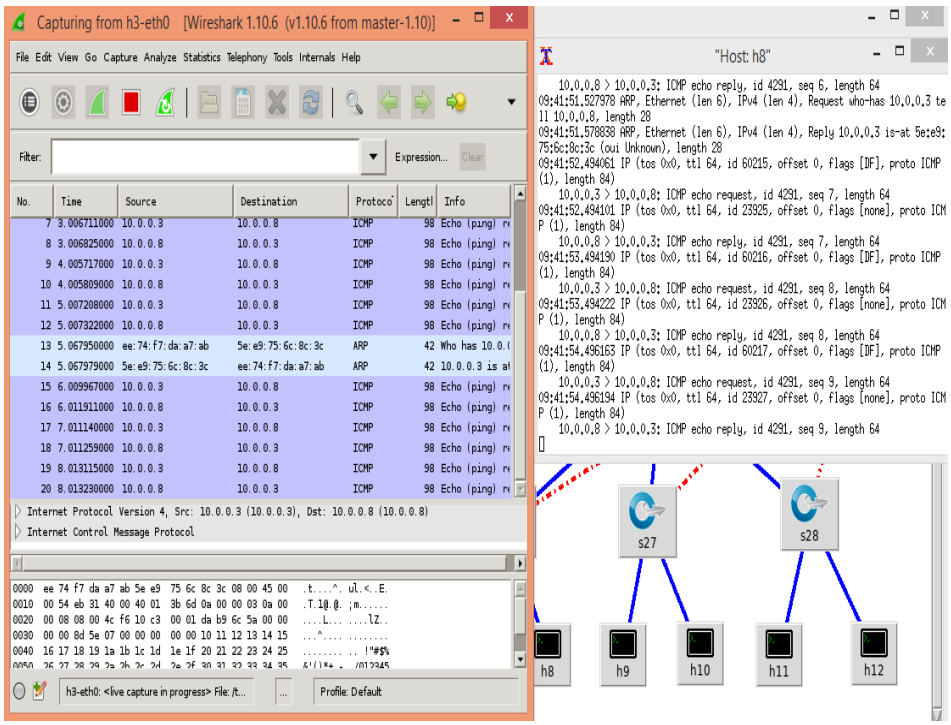


Рисунок 47 – Результат контроля трафика командой ping

Статистика отправленных пакетов показана на рисунке 48.

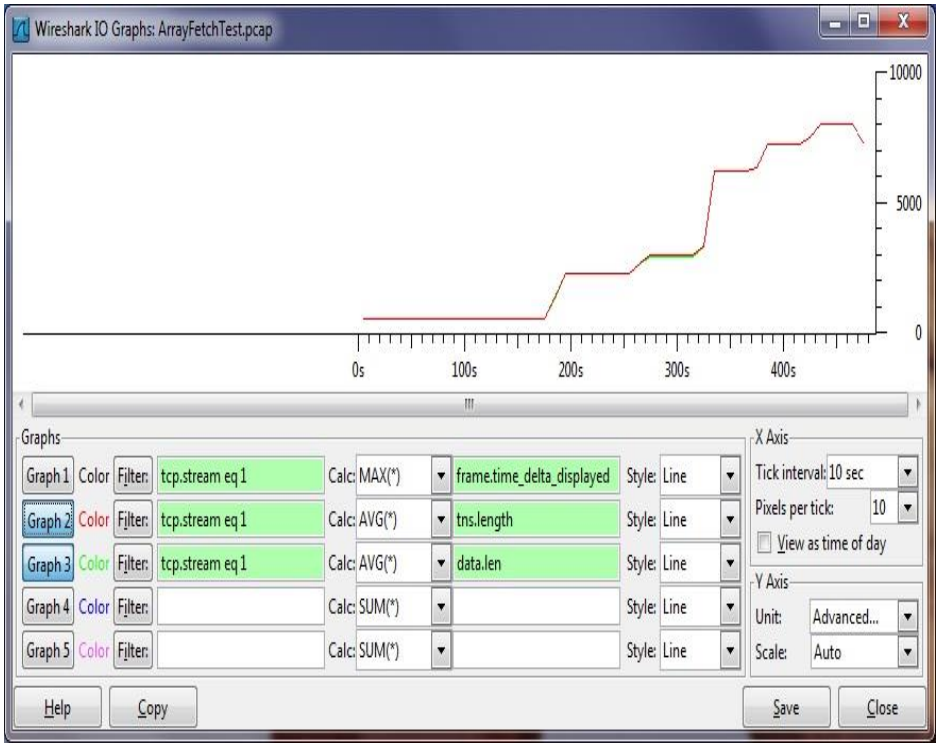


Рисунок 48 – Результаты статистики Wireshark

10.3. Контрольные вопросы

1. Как происходит виртуализация физических ресурсов сети в технология SDN?

2. Какие преимущества и недостатки архитектуры программно-определяемой сети?

3. Какова структура контроллеров технологии SDN?

4. Каковы недостатки технология NAT?

5. Что означает команда mininet> h3 ping h8?

6. Какова архитектура управление SDN?

7. Какова общая концепция технологии SDN/NFV?

8. Каковы преимущества и недостатки контроллера POX SDN?

Список литературы

1. Э. Таненбаум, Д. Уэзеролл. Компьютерные сети. Пятое издание: Энциклопедия пользователя: Пер. с англ./Марк А. Спартак и др. – К.: Изд-во «Питер», 2012. – 432 с.

2. Создание эмуляторов EVE-ng, Cisco VIRL и GNS3. http://www.ciscolab.ru/labs/43-sravnenie-emulyatorov-eveng-cisco-virl-i-gns.html (дата обращения 07.02.2018).

3. Cooper. J. Архитектура корпоративных сетей. Краткое руководство Ver 1.0: http://blog.netskills.ru/p/blog-page.html (дата обращения 15.01.2018).

4. Руководство по SDN и NFV. https://shalaginov.com/2018/01/16/руководство-по-sdn-и-nfv-1/

5. Хабрахабр.ру. Эмулятор EVE-ng – прыжок модернизации: http://habrahabr.ru/post/262027/ (дата обращения 2.02.2018).

6. Фокин В.Г. Компоненты, технологии и услуги корпоративных сетей. Учебное пособие. – Новосибирск, СибГУТИ, 2001. –142 с.

7. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. — СПб.: Питер, 2006. — 958 с: ил.

8. Росляков А.В. Зарубежные и отечественные платформы сетей NGN [Текст]: Учеб. пособие для вузов / А.В. Росляков. – М.: Горячая линия-Телеком, 2014. – 258 с.

9. Хабрахабр.ру. Эмулятор UNetLab – революционный прыжок: http://habrahabr.ru/post/262027/ (дата обращения 2.02.2016).

10. Сравнение эмуляторов UNetLab, Cisco VIRL и GNS3. http://www.ciscolab.ru/labs/43-sravnenie-emulyatorov-unetlab-cisco-virl-i-gns.html (дата обращения 17.01.2016).

11. Маршутизатор Cisco 7604. https://www.cisco.com/c/ru_ru/support/routers/7604-router/model.html

12. Маршрутизаторы Cisco серии 7200. http://www.univers-spb.ru/

Содержание

Введение 3
1. Лабораторная работа № 1. Ознакомление и запуск оборудования 4
1.1. Описание лабораторной установки 4
1.2. Методические указания 4
1.3. Контрольные вопросы 5
2. Лабораторная работа № 2. Адресные планы PE1, PE2, CE1, CE2 5
2.1. Рабочее задание 5
2.2. Методические указания 6
2.3. Контрольные вопросы 12
3. Лабораторная работа № 3. Настройка протоколов для маршрутизации PE1↔ PE2, CE1↔ PE1, CE2↔ PE2 12
3.1. Рабочее задание 12
3.2. Методические указания 12
3.3. Контрольные вопросы 16
4. Лабораторная работа № 4. Настройка L3 VPN MPLS модели 16
4.1. Рабочее задание 16
4.2. Методические указания 17
4.3. Контрольные вопросы 19
5. Лабораторная работа № 5. Проверка связи между CE1 и CE2 по VPN 19
5.1. Методические указания 19
5.2. Контрольные вопросы 21
6. Лабораторная работа № 6. Запуск Mininet 21
6.1. Рабочее задание 21
6.2. Методические указания 21
6.3. Контрольные вопросы 26
7. Лабораторная работа № 7. Настройка сетевой топологии SDN 26
7.1. Рабочее задание 26
7.2. Методические указания 26
7.3. Контрольные вопросы 30
8. Лабораторная работа № 8. Создание виртуальной лаборатории SDN 30
8.1. Рабочее задание 30
8.2. Методические указания 31
8.3. Контрольные вопросы 34
9. Лабораторная работа № 9. Использование контроллера OpenDaylight SDN 35
9.1. Рабочее задание 35
9.2. Методические указания 35
9.3. Контрольные вопросы 38
10. Лабораторная работа № 10. Создание пользовательской сетевой топологии SDN 38
10.1. Рабочее задание 38
10.2. Методические указания 38
10.3. Контрольные вопросы 42
Список литературы 44

Дополнительный план 2021 г., поз. 9

Байкенов Алимжан Сергеевич

ИССЛЕДОВАНИЕ ТЕХНОЛОГИЙ ТРАНСПОРТНЫХ СЕТЕЙ СВЯЗИ

Методические указания к лабораторным работам
для магистрантов образовательной программы
7М06201 – «Радиотехника, электроника и телекоммуникации»
(Магистратура научного и педагогического направления)

Редактор: Е.Б. Жанабаева
Специалист по стандартизации: Ж.А. Ануарбек

Подписано в печать
Тираж 50 экз.
Объём 2,8 уч.-изд. л.

Формат 60×84 1/16
Бумага типографская № 1
Заказ___Цена 1400 тенге

Копировально-множительное бюро
некоммерческого акционерного общества
«Алматинский университет энергетики и связи имени Гумарбека Даукеева»
050013, Алматы, ул. Байтурсынова, 126/1