Некоммерческое
Акционерное
общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА

Кафедра
телекоммуникаций и
инновационных технологий

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ 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 современных транспортных сетей связи. Методические указания по выполнению лабораторных работ для магистрантов ОП 7М06201 – Радиотехника, электроника и телекоммуникации. – Алматы: АУЭС, 2021 – 49 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 программной среде GNS-3.

Методические указания предназначены для магистрантов, обучающихся по ОП 7М06201 – Радиотехника, электроника и телекоммуникации.

Ил. 33, 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.

Введение

Методические указания к выполнению лабораторных работ по курсу «Исследование современных транспортных сетей связи» для магистрантов, обучающихся по образовательной программе 7М06201 – «Радиотехника, электроника и телекоммуникации». В настоящий сборник включены 10 лабораторных работ, целью которых является изучение и анализ функционирования современных транспортных сетей связи. В первых пяти работах предлагаются работы по настройке сети на действующем стенде. Во второй части комплекса приведены работы по моделированию транспортных сетей с использованием эмулятора транспортных сетей связи GNS-3.

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 фирм 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.

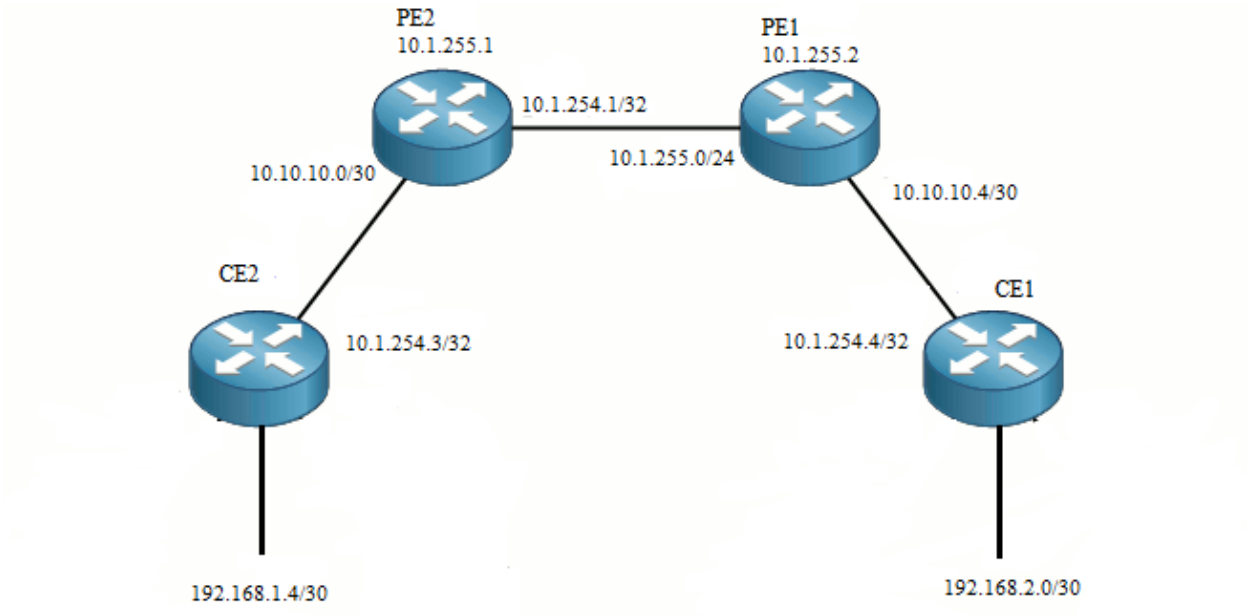

Рисунок 1 – Схема сети MPLS

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 компьютером. 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 (рисунок 3) берем параметр COM1.

Рисунок 3 – Окно Connect To

2.2.4. Отмечаем параметры как рисунке 4:

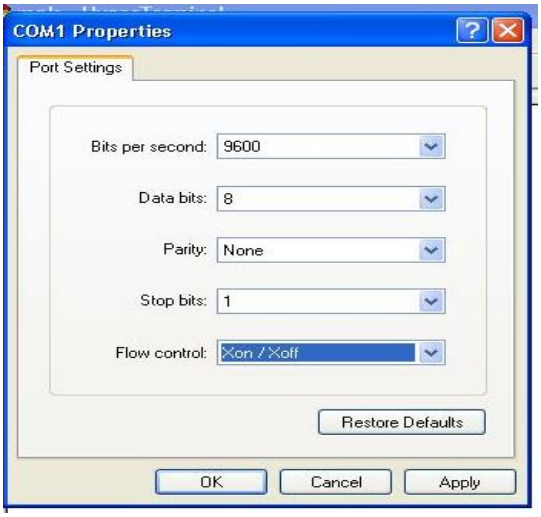

Рисунок 4 – Окно COM1

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

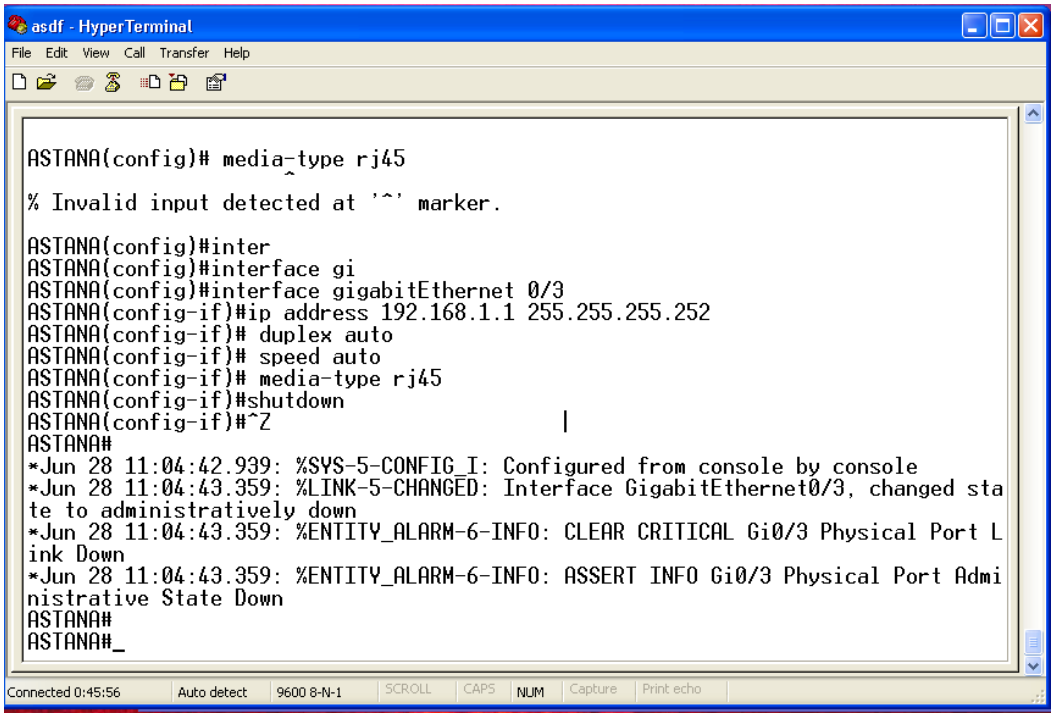

Рисунок 5 – Интерфейсы CISCO 7204

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 подключаемся к Almaty (PE2). Назначаем адреса на интерфейсах устройств.

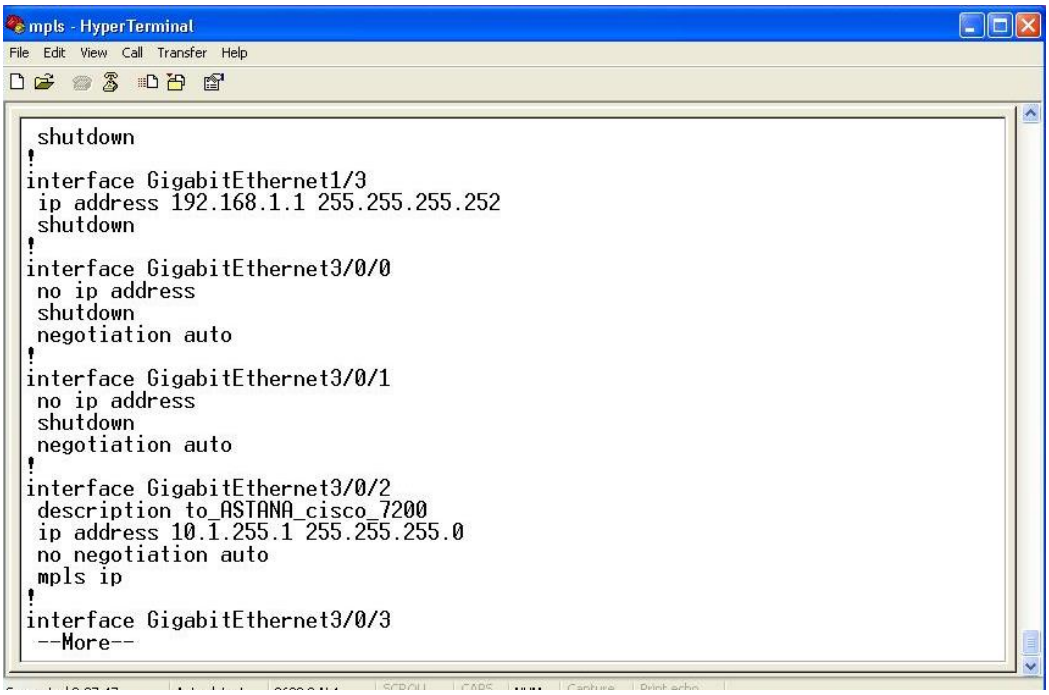

Рисунок 6 – Интерфейсы CISCO 7604

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.

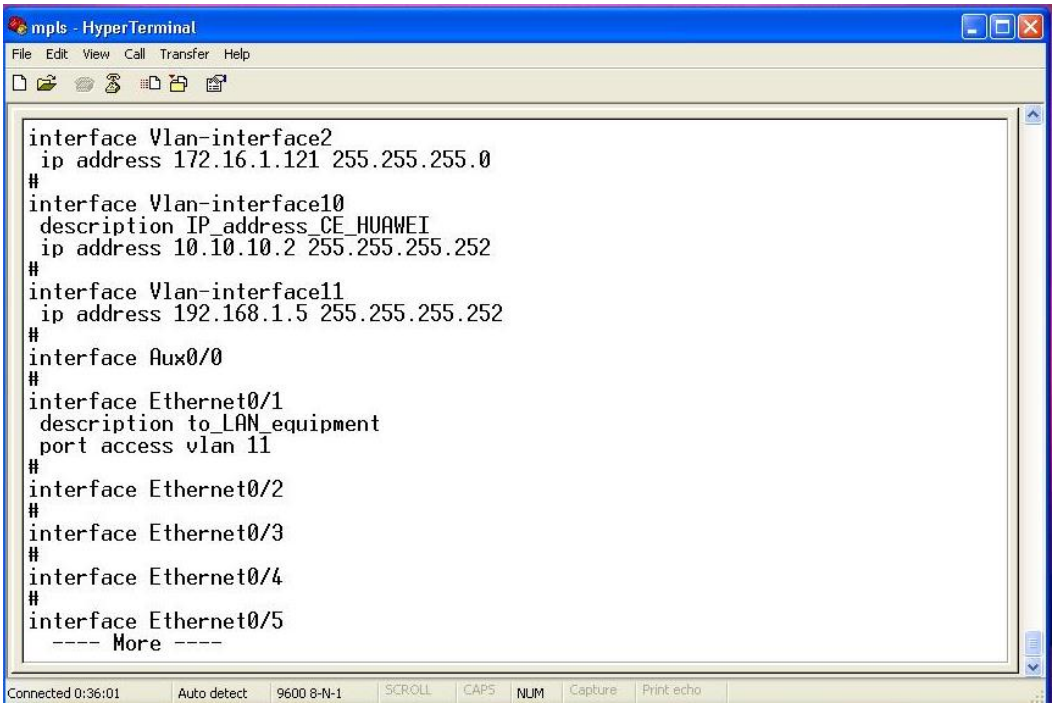

Рисунок 7 – Интерфейсы Quidway

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.

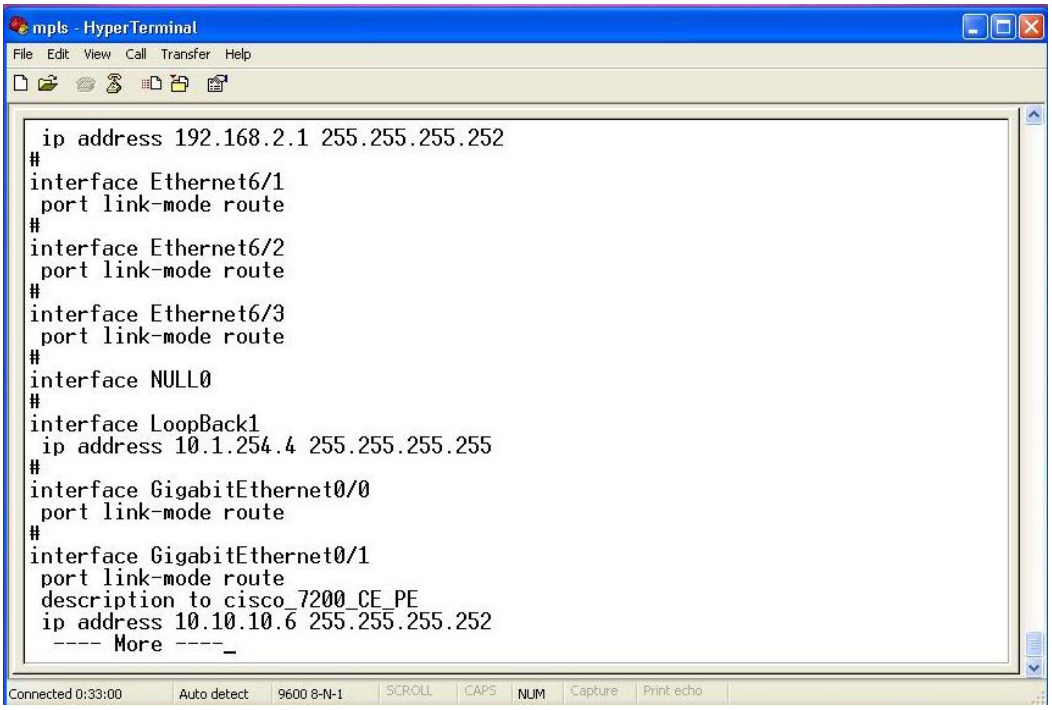

Рисунок 8 – Адресные планы интерфейсов H3C

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:

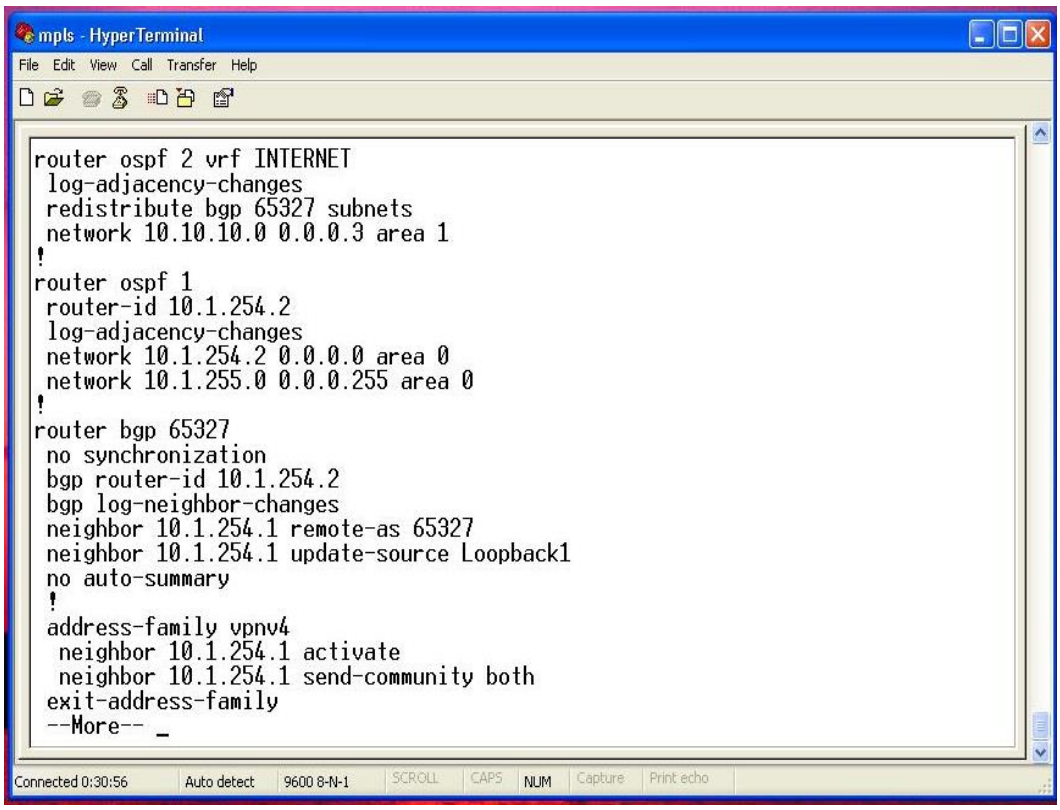

Рисунок 9 – Протоколы CISCO 7204

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:

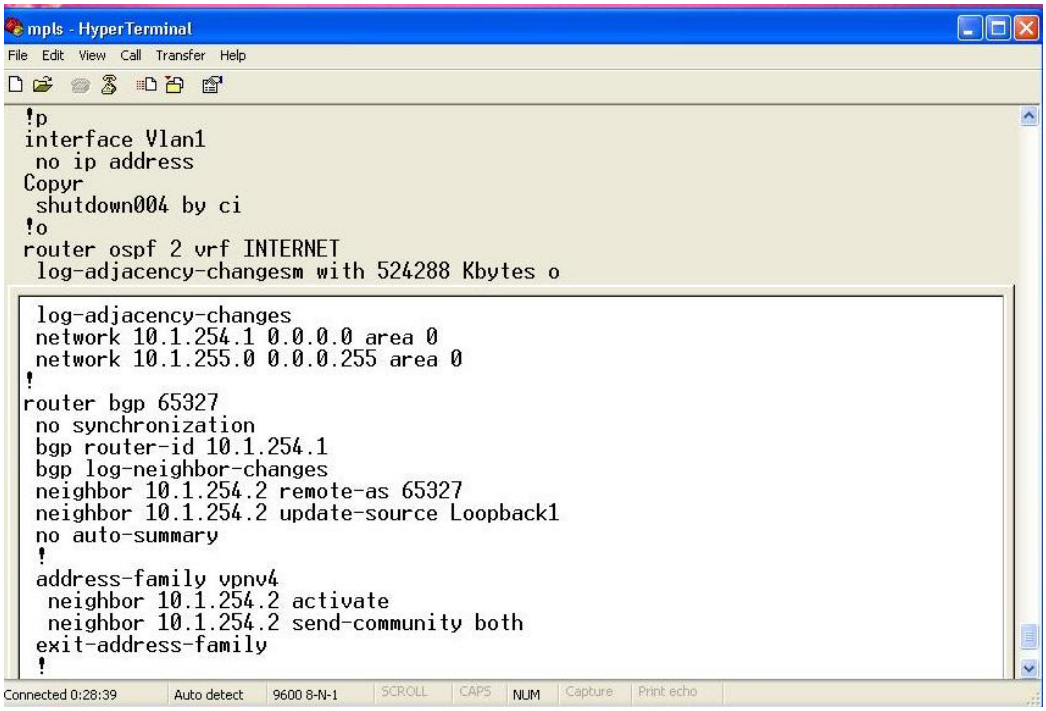

Рисунок 10 – Окно протоколов CISCO 7604

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:

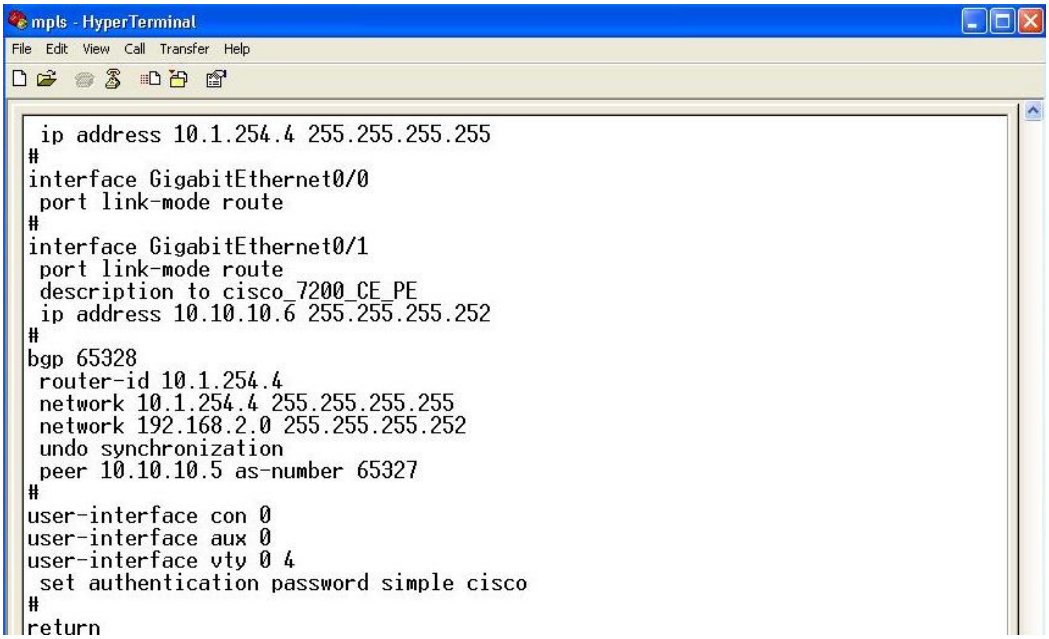

Рисунок 11 – Протоколы Quidway

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 и прописать протоколы:

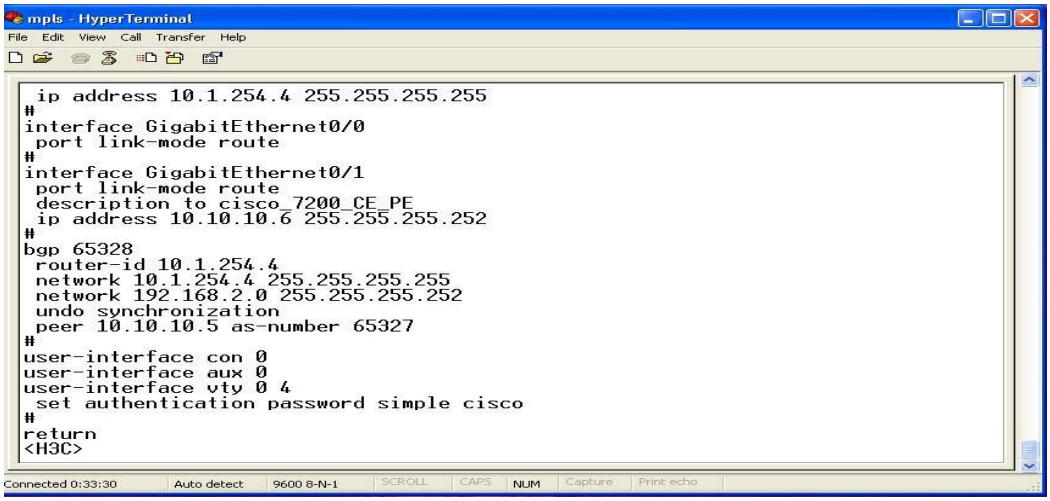

Рисунок 12 – Протоколы H3C

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: создания 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. Повторить пункты 2.2.1, 2.2.2, 2.2.3, 2.2.4 лабораторной работы № 2.

4.2.2. С помощью UTP кабеля соединяемся с PE1, прописываем конфигурацияю.

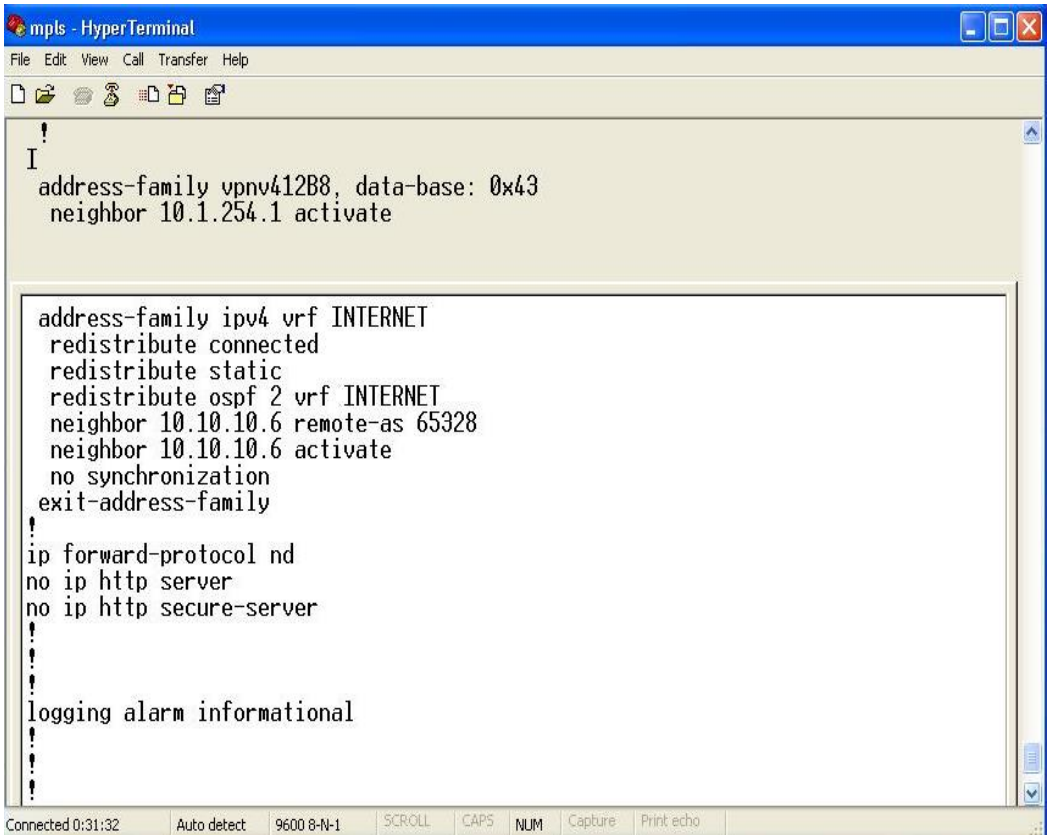

Рисунок 13 – Конфигурация VPN в CISCO 7204

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 соединяемся с PE2 и прописываем в конфигурацию.

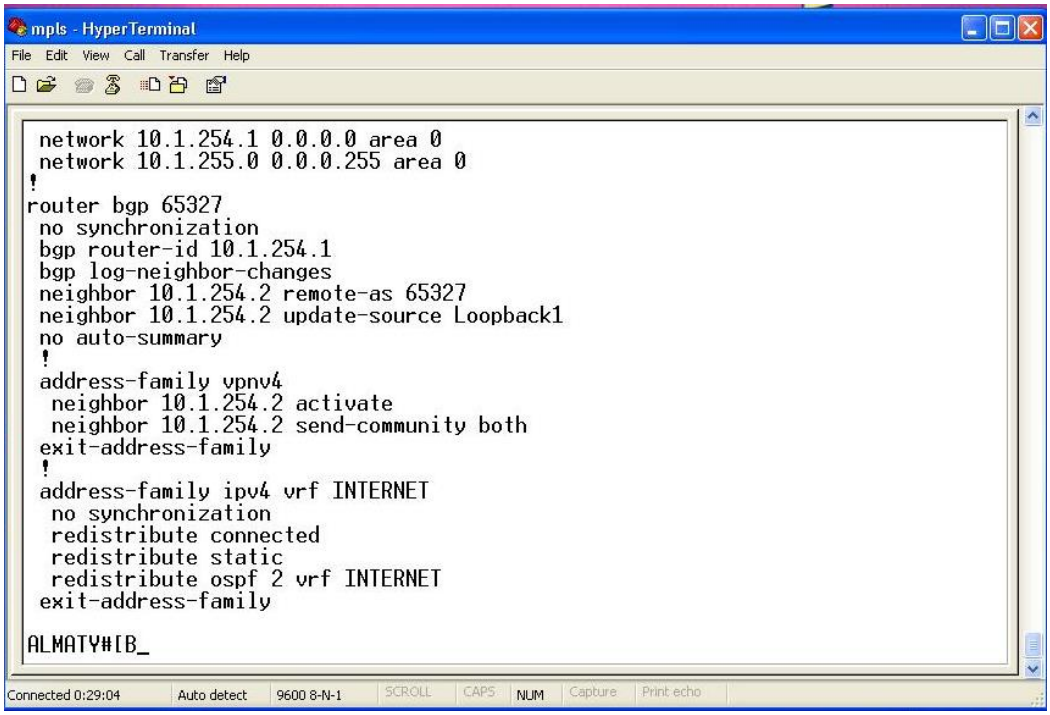

Рисунок 14 – Конфигурации VPN в CISCO 7604

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. Повторить пункты 2.2.1, 2.2.2, 2.2.3, 2.2.4 лабораторной работы № 2.

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

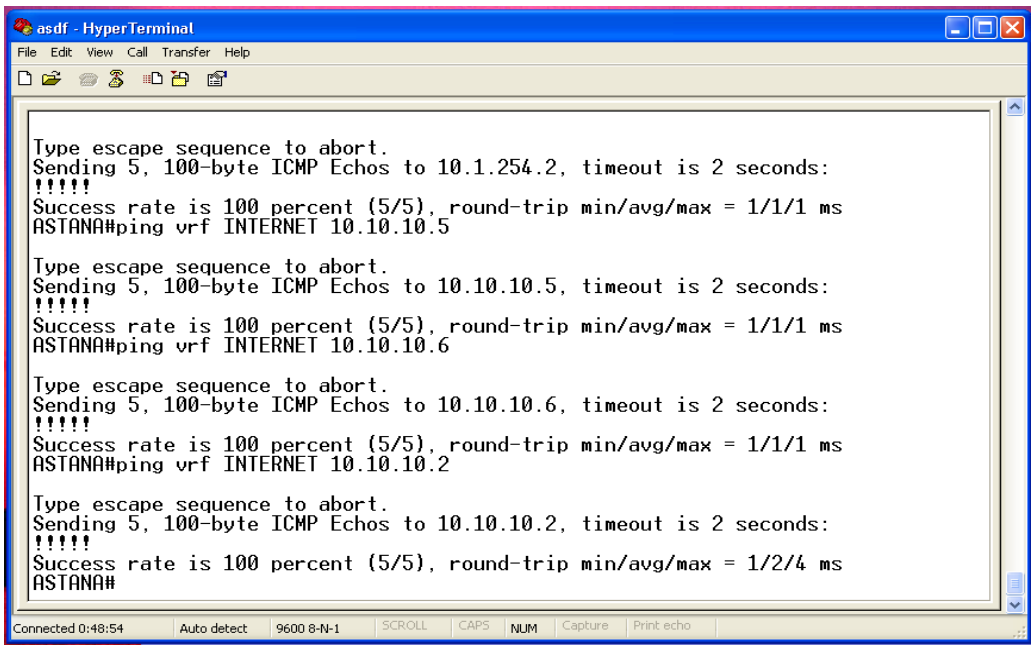

Рисунок 15 – Проверка соединения

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

5.1.4 Подсоединившись с CE1, проверяем PING VRF INTERNET IP адреса на интерфейсах:

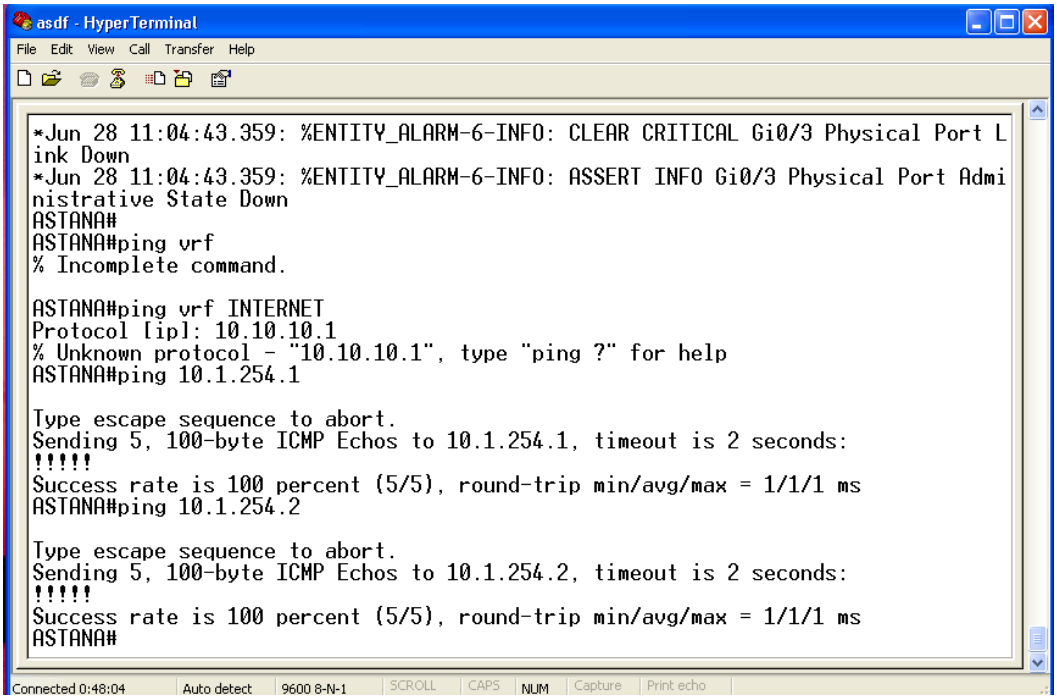

Рисунок 16 – Проверка VRF соединения

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. Моделирование транспортной сети технологии OSPF/BGP с использованием пакета GNS-3

Цель работы: построить модель сети средствами пакета GNS-3 для установки, собранной в лабораторной № 1.

6.1. Рабочее задание

6.1.1. Собрать схему из трех роутеров (рисунок 17). Проверить работоспособность сети.

6.2. Методические указания

6.2.1. Описание сети:

CR1 и CR2 – Customer Edge (CE) роутеры, к которым подключены клиентские сети;

R1 и R3 – роутеры на границе OSPF домена;

R2 – роутер, находящийся внутри домена OSPF.

Протокол маршрутизации OSPF используется для организации сетевой доступности внутри домена.

Необходимо проложить путь из сети 50.1.128.0/24 в сеть 50.1.130.0/24. По маршруту пакет с R1 дойдет до R2, который по протоколу BGP переправит его на R3. По протоколу OSPF роутер R2 знает своих соседей R1 и R3.

6.3. Порядок выполнения работы

Необходимо на каждом роутере добавить слоты с 2 портами.

Собрать схему (рисунок 16) с использованием образов операционной системы IOS роутеров CISCO 7200.

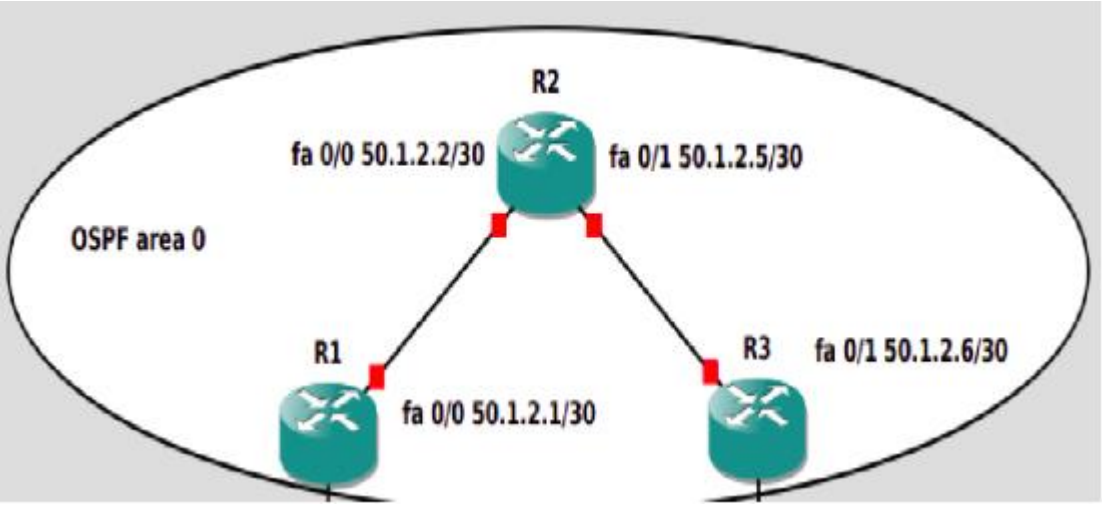

Рисунок 16 – Схема сети

6.3.1 Запуск протокола OSPF
R1:
R1>en
R1#configure terminal##
R1(config)#int loopback 0#
R1(config-if)#ip address 50.1.1.1 255.255.255.255#
R1(config-if)#exit#
Нужно проверить интерфейс, который подключен к R2. Здесь это fa 0/0.
R1(config)#int fa 0/0#
R1(config-if)#ip address 50.1.2.1 255.255.255.252#
R1(config-if)#no shutdown#
R1(config-if)#exit#
Настроить протокол OSPF#
R1(config)#router ospf 1#
R1(config-router)#log-adjacency-changes#
R1(config-router)#redistribute connected subnets#
R1(config-router)#redistribute static subnets#
R1(config-router)#network 50.1.1.0 0.0.0.255 area 0#
R1(config-router)#network 50.1.2.0 0.0.0.255 area 0#
R1(config-router)#exit#
R1(config)#exit#
R1# write#

R2:#
R2>en#
R2#configure terminal#
R2(config)#int loopback 0#
R2(config-if)#ip address 50.1.1.2 255.255.255.255#
R2(config-if)#exit#
Проверить интерфейс подключенный к R1 -fa 0/0

R2(config)#int fa 0/0#
R2(config-if)#ip address 50.1.2.2 255.255.255.252#
R2(config-if)#no shutdown#
R2(config-if)#exit#
Проверить интерфейс на R3 - fa 0/1.
R2(config)#int fa 0/1#
R2(config-if)#ip address 50.1.2.5 255.255.255.252#
R2(config-if)#no shutdown#
R2(config-if)#exit#
Настройка протокола внутренней маршрутизации OSPF.
R2(config)#router ospf 1#
R2(config-router)#log-adjacency-changes#
R2(config-router)#redistribute connected subnets#
R2(config-router)#redistribute static subnets#
R2(config-router)#network 50.1.1.0 0.0.0.255 area 0#
R2(config-router)#network 50.1.2.0 0.0.0.255 area 0#
R2(config-router)#exit#
R2(config)#exit
R2#write#
R3:#
R3>en#
R3#configure terminal#
R3(config)#int loopback 0#
R3(config-if)#ip address 50.1.1.3 255.255.255.255#
R3(config-if)#exit#
Проверить интерфейс к роутеру R2 -fa 0/1.
R3(config)#int fa 0/1#
R3(config-if)#ip address 50.1.2.6 255.255.255.252#
R3(config-if)#no shutdown#
R3(config-if)#exit#
Настройка OSPF
R3(config)#router ospf 1#
R3(config-router)#log-adjacency-changes#
R3(config-router)#redistribute connected subnets#
R3(config-router)#redistribute static subnets#
R3(config-router)#network 50.1.1.0 0.0.0.255 area 0#
R3(config-router)#network 50.1.2.0 0.0.0.255 area 0#
R3(config-router)#exit#
R3(config)#exit#
R3#write#
R1#show ip route#
В результате получаем таблицу маршрутизации
R1#ping 50.1.2.6#

Проверка работоспособности сети.

6.3.2. Настройка протокола внешней маршрутизации BGP на пограничных роутерах.

R1:#
R1#configure terminal#
R1(config)#router bgp 64512#
R1(config-router)# bgp log-neighbor-changes#
R1(config-router)# no bgp default ipv4-unicast#
R1(config-router)# neighbor 50.1.1.2 remote-as 64512#
R1(config-router)# neighbor 50.1.1.2 update-source Loopback0#

R1(config-router)#address-family ipv4#
R1(config-router-af)# redistribute connected#
R1(config-router-af)# redistribute static##
R1(config-router-af)# redistribute ospf 1##
R1(config-router-af)# neighbor 50.1.1.2 activate#
R1(config-router-af)# neighbor 50.1.1.2 send-community extended#
R1(config-router-af)# exit-address-familyy#

R1(config-router)# address-family vpnv4#
R1(config-router-af)# neighbor 50.1.1.2 activate#
R1(config-router-af)# neighbor 50.1.1.2 send-community extended#
R1(config-router-af)# exit-address-family#
R1(config-router)# exit#
R1(config)# exit#
R1# write#

R3:
R3#configure terminal#
R3(config)#router bgp 64512#
R3(config-router)# bgp log-neighbor-changes#
R3(config-router)# no bgp default ipv4-unicast#
R3(config-router)# neighbor 50.1.1.2 remote-as 64512#
R3(config-router)# neighbor 50.1.1.2 update-source Loopback0#

R3(config-router)#address-family ipv4#
R3(config-router-af)# redistribute connected#
R3(config-router-af)# redistribute static#
R3(config-router-af)# redistribute ospf 1#
R3(config-router-af)# neighbor 50.1.1.2 activate#
R3(config-router-af)# neighbor 50.1.1.2 send-community extended#
R3(config-router-af)# exit-address-family#

R3(config-router)# address-family vpnv4#
R3(config-router-af)# neighbor 50.1.1.2 activate#
R3(config-router-af)# neighbor 50.1.1.2 send-community extended#
R3(config-router-af)# exit-address-family#
R3(config-router)# exit#
R3(config)# exit#
R3# write#
6.3.3 Настройка протокола BGP на роутере провайдера.
R2(config)#router bgp 64512#
R2(config-router)# bgp cluster-id 100#
R2(config-router)# bgp log-neighbor-changes#
R2(config-router)# no bgp default ipv4-unicast#
R2(config-router)# neighbor 50.1.1.1 remote-as 64512#
R2(config-router)# neighbor 50.1.1.1 update-source Loopback0#
R2(config-router)# neighbor 50.1.1.3 remote-as 64512#
R2(config-router)# neighbor 50.1.1.3 update-source Loopback0#

R2(config-router)# address-family ipv4
R2(config-router-af)# neighbor 50.1.1.1 #activate#
R2(config-router-af)# neighbor 50.1.1.1 send-community extended#
R2(config-router-af)# neighbor 50.1.1.1 route-reflector-client#
R2(config-router-af)# neighbor 50.1.1.3 activate#
R2(config-router-af)# neighbor 50.1.1.3 send-community extended#
R2(config-router-af)# neighbor 50.1.1.3 route-reflector-client#
R2(config-router-af)# exit-address-family#
R2(config-router)##

R2(config-router)# address-family vpnv4#
R2(config-router-af)# neighbor 50.1.1.1 activate#
R2(config-router-af)# neighbor 50.1.1.1 send-community extended#
R2(config-router-af)# neighbor 50.1.1.1 route-reflector-client#
R2(config-router-af)# neighbor 50.1.1.3 activate##
R2(config-router-af)# neighbor 50.1.1.3 send-community extended##
R2(config-router-af)# neighbor 50.1.1.3 route-reflector-client##
R2(config-router-af)# exit-address-family##
R2(config-router)# exit##
R2(config)# exit##
R2# write##
Записать команду просмотра протокола внешней маршрутизации BGP
R2#show ip bgp summary#
Проверяем работу сети командой
R1#ping 50.1.2.6#

6.4. Контрольные вопросы

1. Что такое Эмулятор GNS-3?
2. Каковы особенности протокола OSPF?
3. Каковы особенности протокола BGP?
4. Что такое рефлекторный роутер провайдера?
5. Какие еще динамические протоколы маршрутизации вы знаете?
6. Чем отличаются динамические и статические маршруты?
7. Что такое база данных смежности в протоколе OSPF?
8. Что находится в таблице маршрутизации, полученной после команды show ip route.

7. Лабораторная работа № 7. Моделирование транспортной сети MPLS с использованием пакета GNS-3

Цель работы: построить модель сети средствами пакета GNS-3 для установки, собранной в лабораторной № 4.

7.1. Рабочее задание

7.1.1. Использовать собранную модель по схеме в лабораторной работе № 6 для 3 трех роутеров.

7.1.2. Подключить двух клиентов к сети и проверить работоспособность полной сети из 5 роутеров.

7.2. Методические указания

7.2.1. Настройка локального подключения.

Добавьте новые элементы в уже существующую схему.

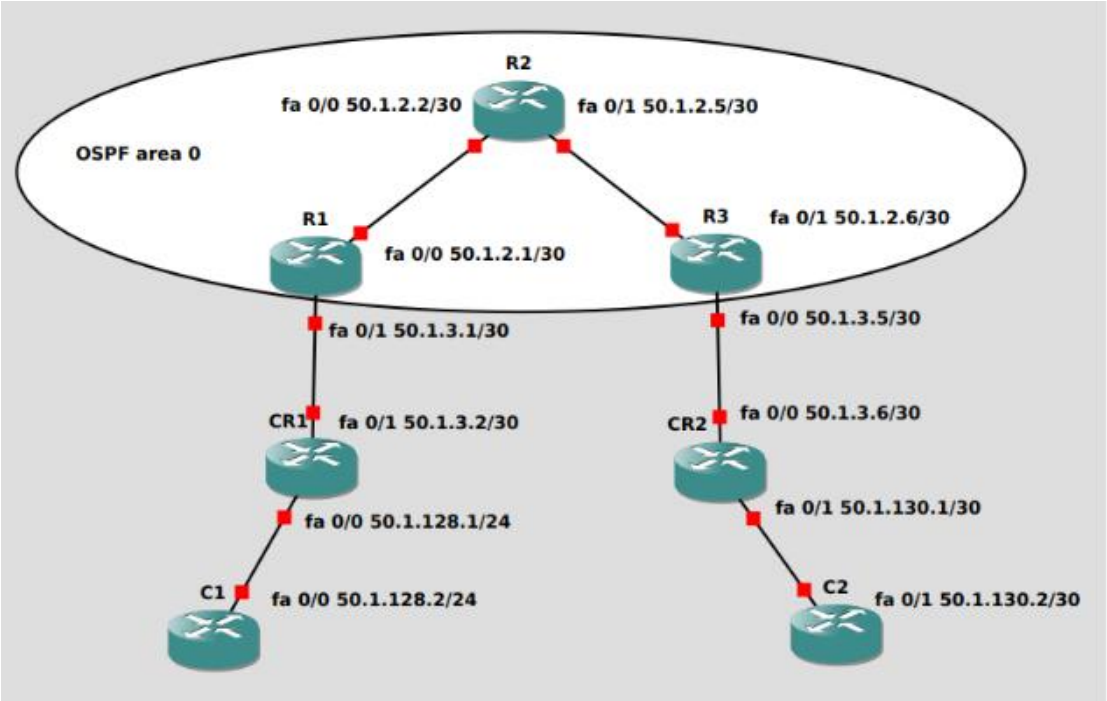

Рисунок 18 – Модель сети

Настроить роутеры клиентов:
CR1:#
CR1>en#
CR1#configure terminal#
Проверить интерфейс к C1. Здесь номер этого интерфейса – fa 0/0.
CR1(config)#intfa 0/0#
CR1(config-if)#ip address 50.1.128.1 255.255.255.0#
CR1(config-if)#no shutdown#
CR1(config-if)#exit#
CR1(config)#exit#
CR1#write#

C1:#
C1>en#
C1#configure terminal#
Проверить интерфейс к CR1. Здесь номер этого интерфейса – fa 0/0.
C1(config)#intfa 0/0#
C1(config-if)#ip address 50.1.128.2 255.255.255.0#
C1(config-if)#no shutdown#
C1(config-if)#exit#
C1(config)#ip route 0.0.0.0 0.0.0.0 50.1.128.1#
C1(config)#exit##
C1#write##
CR2:##
CR2>en#

CR2#configure terminal##
Проверить интерфейс к C2. Здесь номер этого интерфейса – fa 0/1.
CR2(config)#intfa 0/1#
CR2(config-if)#ip address 50.1.130.1255.255.255.0##
CR2(config-if)#noshutdown#
CR2(config-if)#exit#
CR2(config)#exit#
CR2#write##

C2:#
C2>en#
C2#configure terminal
Проверить интерфейс к CR2. Здесь номер этого интерфейса – fa 0/1.
C2(config)#intfa 0/1#
C2(config-if)#ip address 50.1.130.2 255.255.255.0#
C2(config-if)#no shutdown#
C2(config-if)#exit#
C2(config)#ip route 0.0.0.0 0.0.0.0 50.1.130.1#
C2(config)#exit#
C2#write#
Проверка всех локальных соединений
C2# ping 50.1130.1#
C1# ping 50.1.128.1#
7.2.2 Подключение к маршрутизаторам провайдера.
R1:#
R1>en##
R1#configure terminal##
Проверка номера интерфейса к CR1. Это интерфейс fa 0/1.
R1(config)#intfa 0/1#
R1(config-if)#ip address 50.1.3.1255.255.255.252#
R1(config-if)#noshutdown##
R1(config-if)#exit#
R1(config)#ip route 50.1.1280 255.255.255.0 50.1.3.2#
R1(config)#exit##
R1#write##

CR1:
CR1>en
CR1#configureterminal
Проверка номеров интерфейсов к R1. Здесь номер fa 0/1.
CR1(config)#intfa0/1
CR1(config-if)#ipaddress 50.1.3.2 255.255.255.252#
CR1(config-if)#noshutdown#

CR1(configif)#exit#
CR1(config)#ip route 0.0.0.0 0.0.0.0 50.1.3.1#
CR1(config)#exit#
CR1#write#
R3:#
R3>en#
R3#configure terminal##
Проверка номеров интерфейсов к CR1. Здесь номер fa 0/0
R3(config)#intfa 0/0#
R3(config-if)#ip address 50.1.35 255.255.255.252#
R3(config-if)#noshutdown#
R3(config-if)#exit#
R3(config)#ip route 50.1130.0 255.255.255.0 50.1.3.6#
R3(config)#exit#
R3#write#

CR2:#
CR2#>en#
CR2#configure terminal#
Проверка номеров интерфейсов к R1. Здесь номер fa 0/0
CR2(config)#intfa 0/0#
CR2(config-if)#ipaddress 50.1.3.6 255.255.255.252##
CR2(config-if)#noshutdown##
CR2(config-if)#exit#
CR2(config)#ip route 0.0.0.0 0.00.0 50.1.3.5##
CR2(config)#exit#
CR2#write#

С целью проверки работоспособности сети поставить команду ping.
C1#ping 50.1.1302#
Для проверки протокола OSPF добавить команды в R1 или R3.
ip ospfneighbor#
ipospf database#
show ip route#

7.3. Контрольные вопросы

1. Какие можно отметить особенности технология BGP/MPLS VPN (RFC 2547)?
2. Что такое MPLS Traffic Engineering (TE)?
3. На какой уровень модели OSI\ISO можно поместить технологию MPLS?
4. Какие можно назвать элементы сети MPLS?
5. Что такое метки и способы маркировки в MPLS.?
6. Что такое протокол LDP?

7. Что такое VPN L3 MPLS?
8. Что такое класс эквивалентности FEC в MPLS?

8. Лабораторная работа № 8. Моделирование транспортной сети MPLS L3VPN с использованием пакета GNS-3

Цель работы: построить модель сети средствами пакета GNS-3 для установки, собранной в лабораторной № 5 для технологии MPLS L3VPN.

8.1. Рабочее задание

8.1.1. Собрать схему (рисунок 19).

8.2. Методические указания

Для выполнения данной лабораторной работы необходимо построить схему на платформе GNS3. Рекомендуется использовать образ маршрутизатора “c7200-adventerprisek9-mz.152-4.S6”.

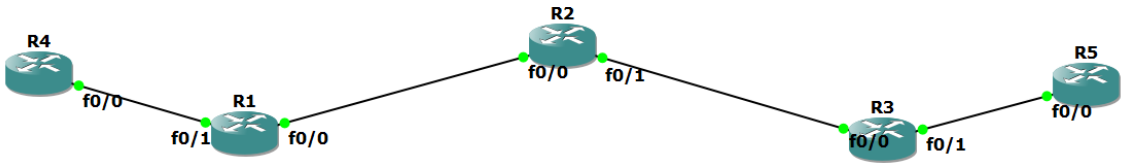

Рисунок 19 – Модель сети на GNS3

Далее необходимо настроить каждый маршрутизатор.
Настройка маршрутизатора R1:
conf t#
hostname R1#
int lo0#
ipaddress 1.1.1.1 255.255.255.255#
ipospf 1 area 0#
exit##
intfa0/0#
ip address 10.0.0.1 255.255.255.0#
noshut#
ip ospf 1 area 0#
exit##
router ospf1#
mpls ldp autoconfig#
exit#

router bgp 1#
neighbor 3.3.3.3 remote-as 1#
neighbor 3.3.3.3 update-source Loopback0#
no auto-summary#
address-family vpnv4#
neighbor 3.3.3.3 activate#
exit##
exit##
intf0/1
noshut#
ip address 192.168.1.1 255255.255.0#
exit#
ip vrf RED#
rd 4:4#
route-target both 4:4#
exit#
intf0/1#
ip vrf forwarding RED
exit#
int f0/1#
ip add 192.168.1.1 255.255.255.0#
exit#
intf0/1
ip ospf 2 area 2#
exit#
router bgp 1
address-family ipv4 vrf RED#
redistribute ospf 2#
exit#
router ospf2#
redistribute bgp1subnets#
exit#
end#
wr- mem#

Настройка маршрутизатора R2:
Conft#
hostnameR2#
intlo0
ip address 2.2.2.2 255255.255.255#
ip ospf 1 area0#
exit#
intfa0/0

ip address 10.0.0.2 255255.255.0#
noshut#
ip ospf1area0#
exit#
intfa0/1#
ip address 10.0.1.2 255.255.255.0#
noshut#
ip ospf1 area0#
exit
router ospf1#
mpls ldpautoconfig#
exit#
end
wrmem#

Настройка маршрутизатора R3:
conft
hostname R3#
intlo0
ip address 3.3.3.3 255255.255.255#
ip ospf1 area0#
exit#
intfa0/0#
ip address 10.0.13 255.255.255.0#
noshut
ip ospf1 area0#
exit#
router ospf1#
mpls ldpautoconfig#
exit#
router bgp1
neighbor 1.1.1.1. remoteas1#
neighbor 1.1.1.1 update-sourceLoopback0#
no autosummary#
address-family vpnv4
neighbor 1.1.1.1activate#
exit#
exit#
intf0/1
noshut
ipadd 192.168.2.3 255255.255.0#
exit#
ip vrfRED#

rd 4:4#
route-targetboth 4:4#
exit#
intf0/1
ip vrfforwarding RED#
exit#
intf0/1
ip add 192.168.2.1255.255.255.0#
ipospf 2 area 2#
exit#
router bgp1#
address-familyipv4 vrfRED#
redistributeospf2#
exit#
router ospf2#
redistribute bgp1subnets#
exit#
end
wrmem#

Настройка маршрутизатора R4:
conft#
intlo0#
ipadd 4.4.4.4 255255.255.255#
ipospf2 area2#
intf0/0#
ip add192.168.1.4 255255.255.0#
ip ospf2 area2#
no shut#
exit#
end#
wrmem
Настройка маршрутизатора R5:
Conft#
int lo0#
ip add 6.6.6.6 255.255.255255#
ipospf2 area2#
int f0/0#
ip add 192.168.2.6 255.255.2550#
ip ospf 2 area 2#
noshut
exit#
end#
wrmem#

Проверка сети с R1командой “ping 3.3.3.3 source Lo0”.

Можно посмотреть метки с маршрутизатора R1 “trace 3.3.3.3”.

Проверим связь между маршрутизаторами R4 и R5 командами “trace 6.6.6.6 и ping 192.168.2.6”.

8.3. Контрольные вопросы

1. Какова особенность протоколов: RSVP; LDP; BGP?

2. Что такое независимые таблицы маршрутизации и продвижения VRF (VPN Routing and Forwarding)?

3. Что такое VPN L2 MPLS?

4. Какие отличия пограничного маршрутизатора LER от LSR?

5. Что такое виртуальный путь LSP?

6. Как маршрутизатор, коммутирующий по меткам, определяет, какая метка из стека меток считается верхней, нижней или средней?

7. Каков диапазон значений метки? Что означают полученные значения?

8. Какой протокол и номер порта позволяют использовать протоколы LDP и TDP для распределения меток в узлах LDP/TDP?

. Лабораторная работа № 9. Анализ построенной сети при помощи Wireshark

Цель работы: настроить сеть средствами пакета GNS-3 и произвести анализ пакетов при помощи Wireshark.

9.1. Рабочее задание

9.1.1. Необходимо собрать схему (рисунок 20) и настроить оборудование. Для удобства можно расписать все подсети и IP адреса интерфейсов. После прописки IP адреса портов надо настроить протокол OSPF на каждом роутере.

9.1.2. Провести анализ с помощью пакета Wireshark.

9.2. Методические указания

Пакет программ «Wireshark» известен как хороший инструмент для анализа и захвата трафика и является условно стандартом как для образования, так и для практики.

Wireshark нужен для исследования сетевых протоколов и приложений. С его помощью можно находить проблемы в работе сети и выяснять причины этих проблем.

Собираем модель сети на GNS-3.

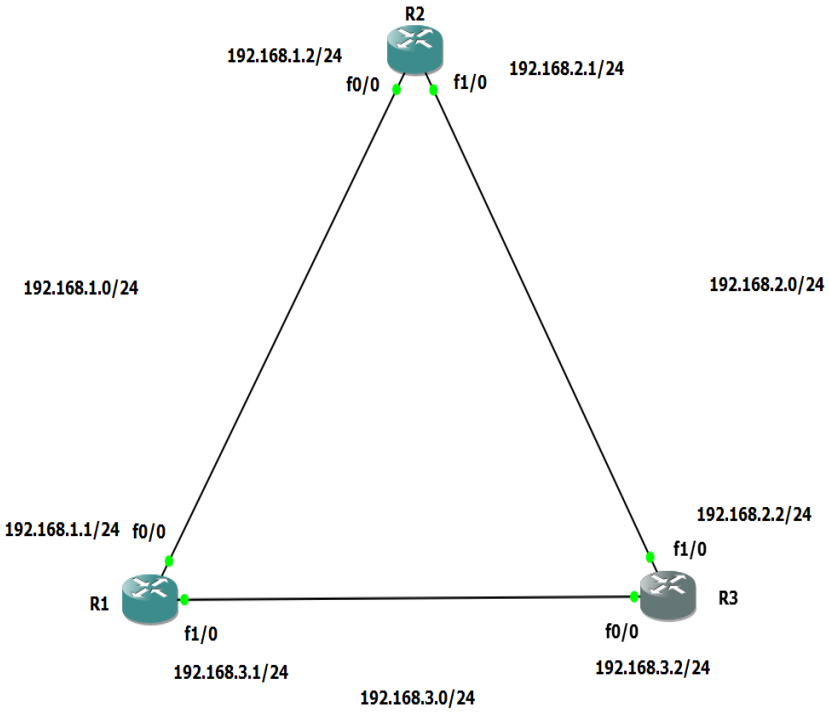

Рисунок 20 – Схема сети

Далее нажимаем ПКМ на линк между роутерами R1 и R3. И выбираем “Start capture”. Появится окно “Packet capture”, далее нажимаем “ok”.

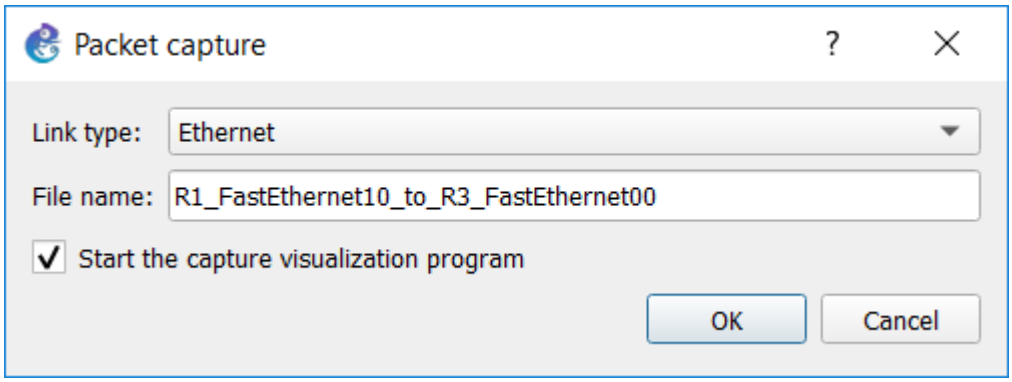

Рисунок 21 – Окно Packet capture

Должно всплыть окно “wireshark”.

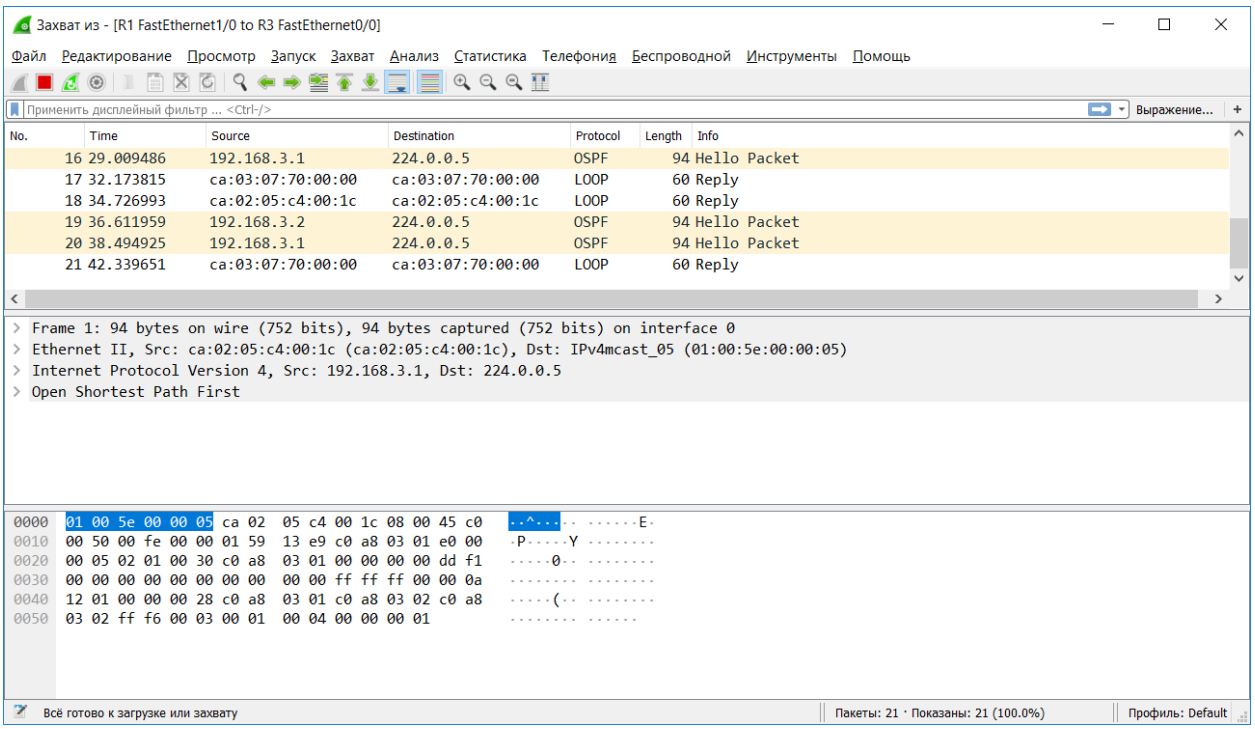

Рисунок 22 – Окно wireshark

Все пакеты в сети видны в окне захвата.

С помощью выражения к дисплейному фильтру есть возможность отфильтровки необходимых пакетов и просмотра их. При этом другие данные сети не будут нам мешать.

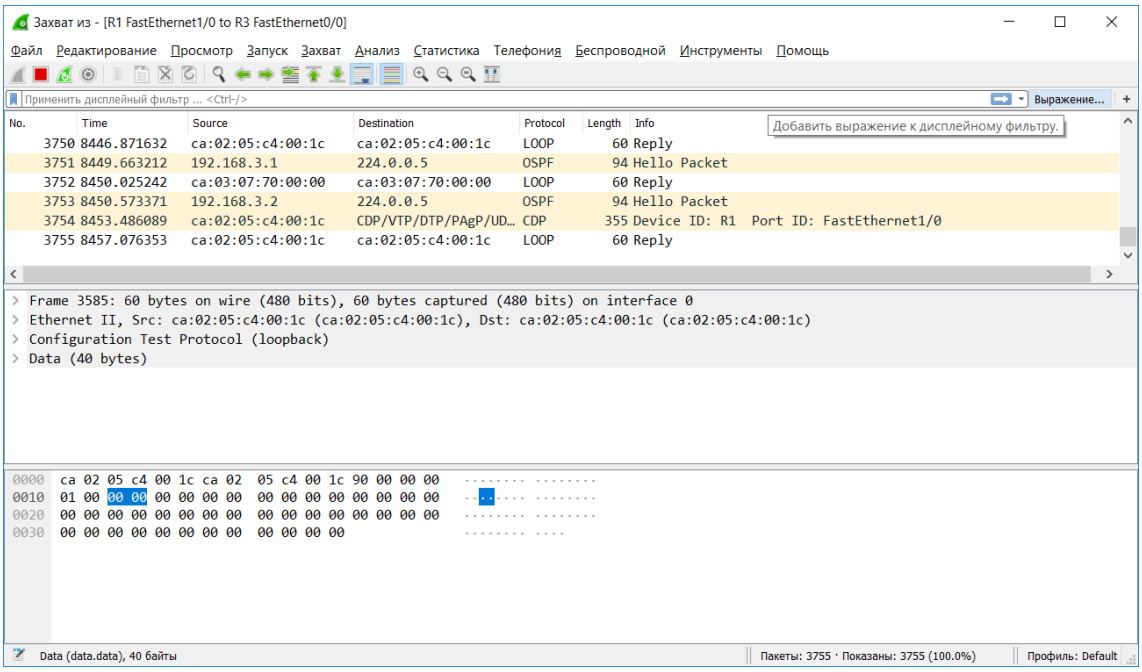

Рисунок 23 – Фильтрование

Ввести имя протокола в поле фильтра. Тогда можно контролировать движение пакета в сети.

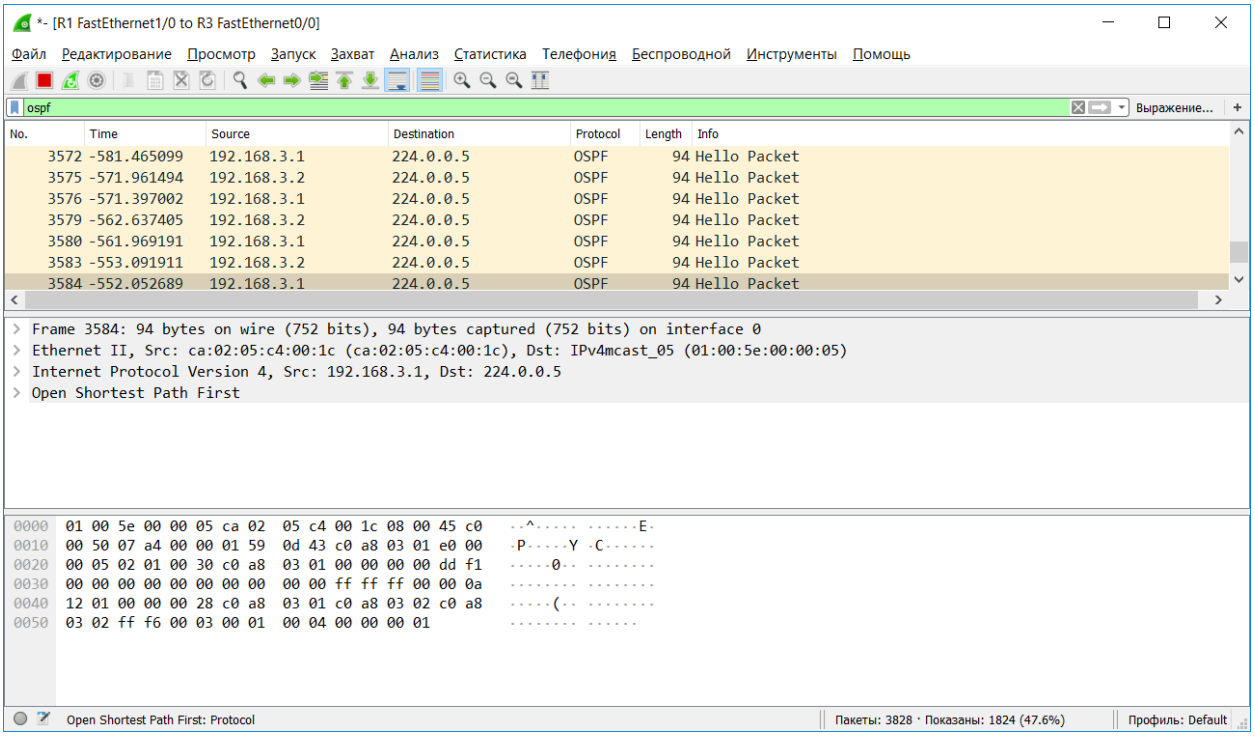

Рисунок 24 – Процесс фильтрования-2

Но есть и недостатки у программы Wireshark.

Если имеется подключение через Telnet, то, используя пакет Wireshark, злоумышленники имеют возможность раскрыть логин и пароль роутера. А затем осуществить переадресацию ваших данных.

Можно просмотреть этот процесс.

Для этого необходимо настроить доступ telnet на одном из наших роутеров и затем сделать подключение к нему с другого роутера. В лабораторной работе используем роутер R2.

router>enable#

router # configureterminal#

router (config)# enable secretaues#

enable secret aues #– сдесь устанавливается пароль на команду enable. Соответственно, aues это и есть наш пароль.

router r (config)#username admin_aues privilege 15 secret aues#

router r (config)#line vty 0 4#

router r (config-line)#login local#

router (config-line)#end#

router #write#

Далее необходимо включить сбор трафика на интерфейсе R2.

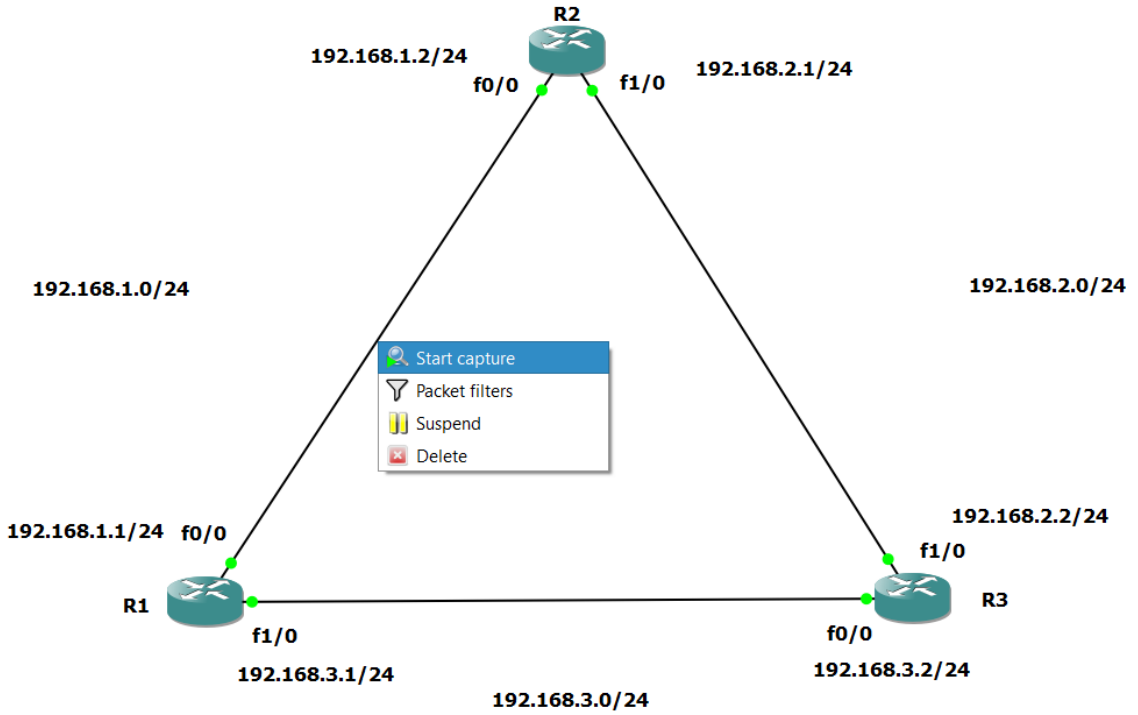

Рисунок 25 – Модель с Wireshark

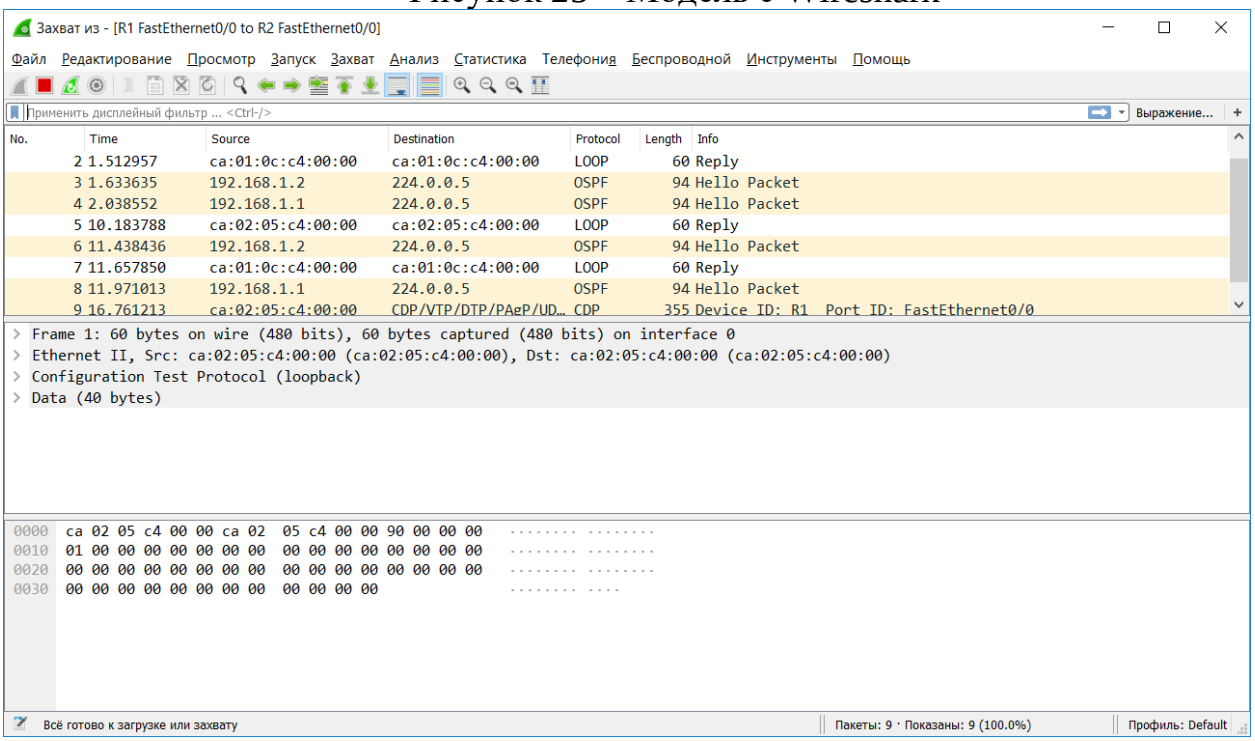

Рисунок 26 – Сбор трафика на интерфейсе R2

Команда подключения через Telnet к R2 с R1.
R1#telnet 192.168.1.2#

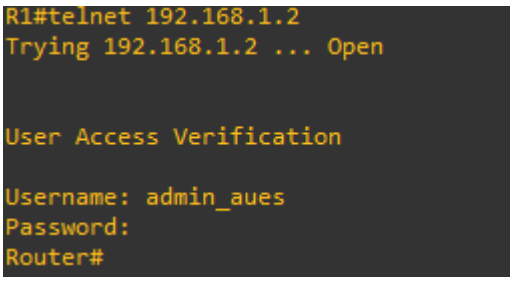

Рисунок 27 – Окно пароля

Username: admin_aues#
Password: aues#

После подключения к R2 через telnet с роутора R1 необходимо ввести команду “show run”. Можно видеть в wireshark пакеты через Telnet.

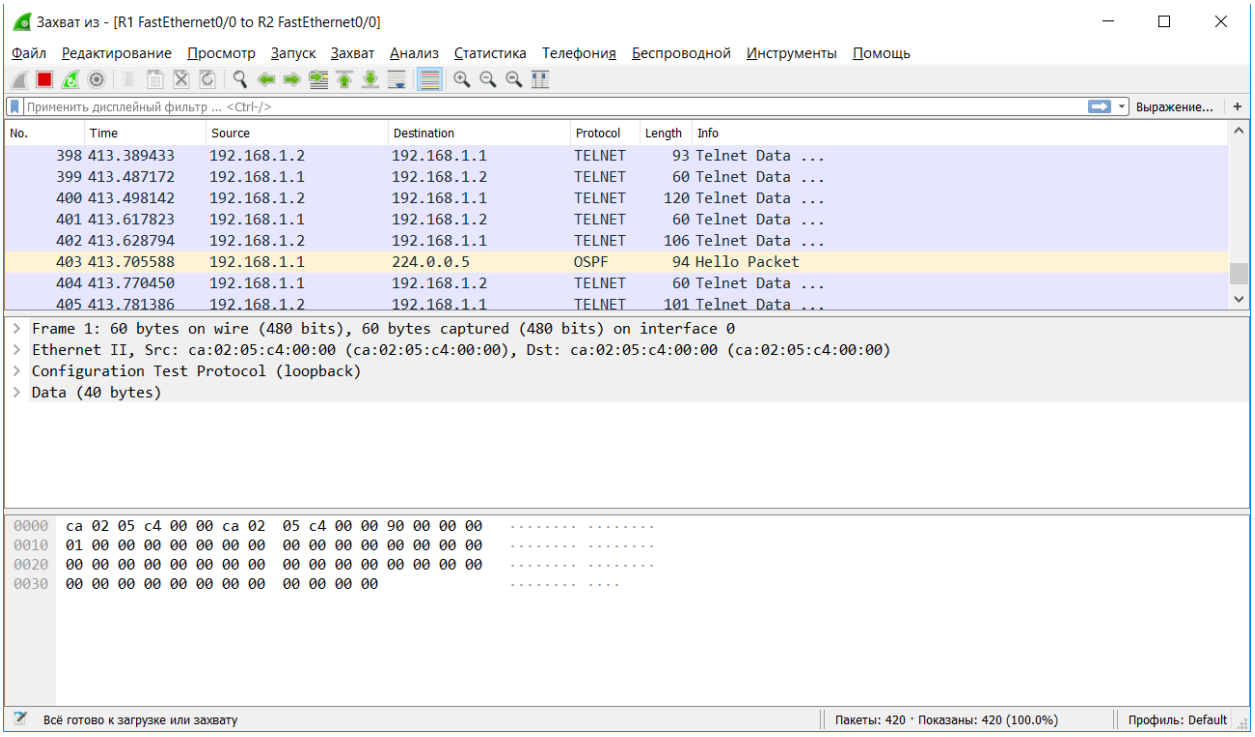

Рисунок 28 – Окно Telnet

После выбора одного пакета Telnet нажать ПКМ.

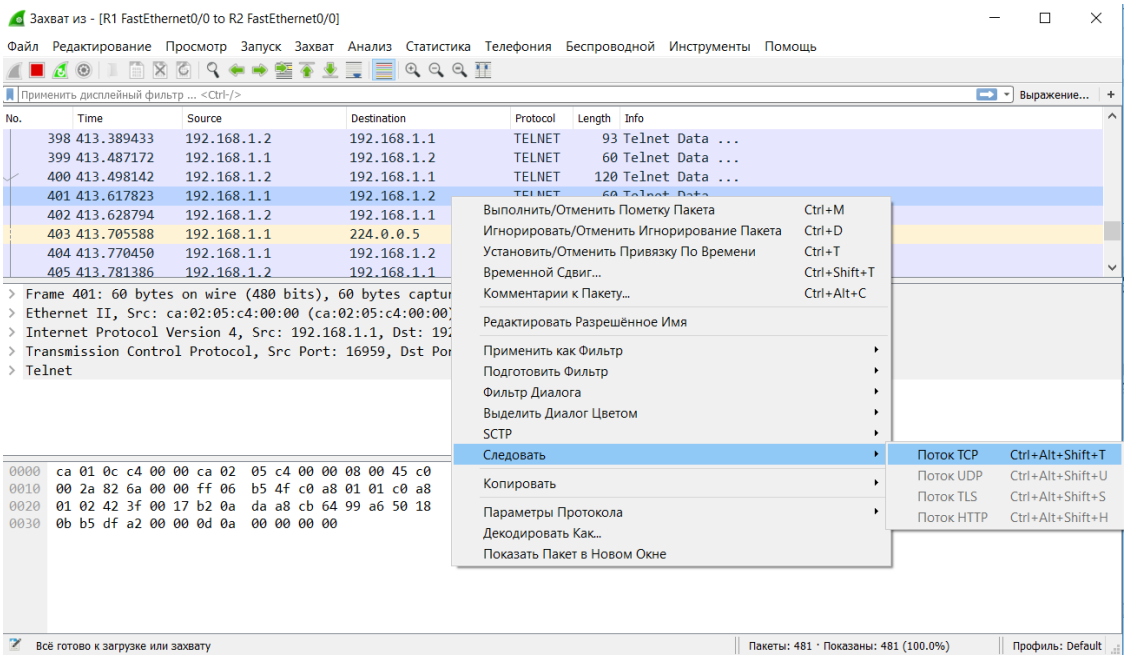

Рисунок 29 – Окно программы Telnet-2

В следующем окне видно username и password, и даже то, что делал администратор. Это объясняется тем, что программа Telnet не имеет шифрования.

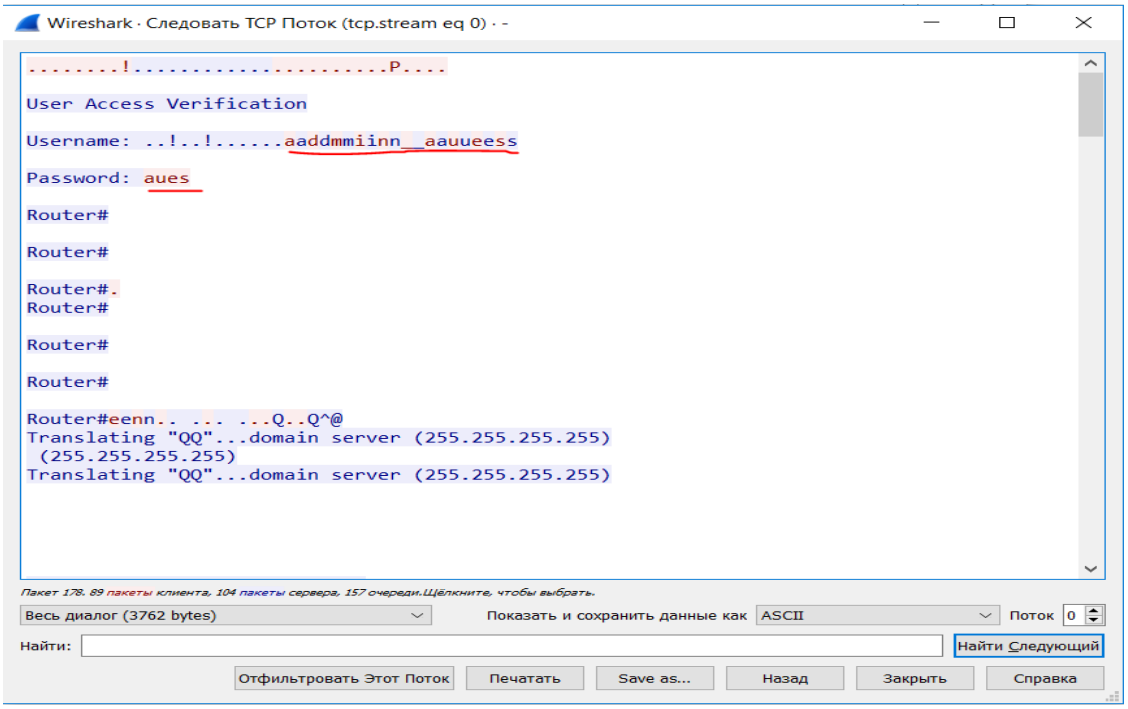

Рисунок 30 – Окно пароля

Для закрытия наших данных нам нужно запустить протокол шифрования SSH.

Заходим в роутер R2.

router#configureterminal#

router (config)#hostname R2#
R2(config)#ip domainname r2.aues.ret#
R2(config)#crypto key generate rsa general-keys modulus 1024#
Настроили SSH на R2
Подключаемся к R2 через R1 по SSH
R1#ssh -l admin_aues192.168.12#
Пароль: aues#
R2#show run#
В программе Wireshark видны пакеты SSH.

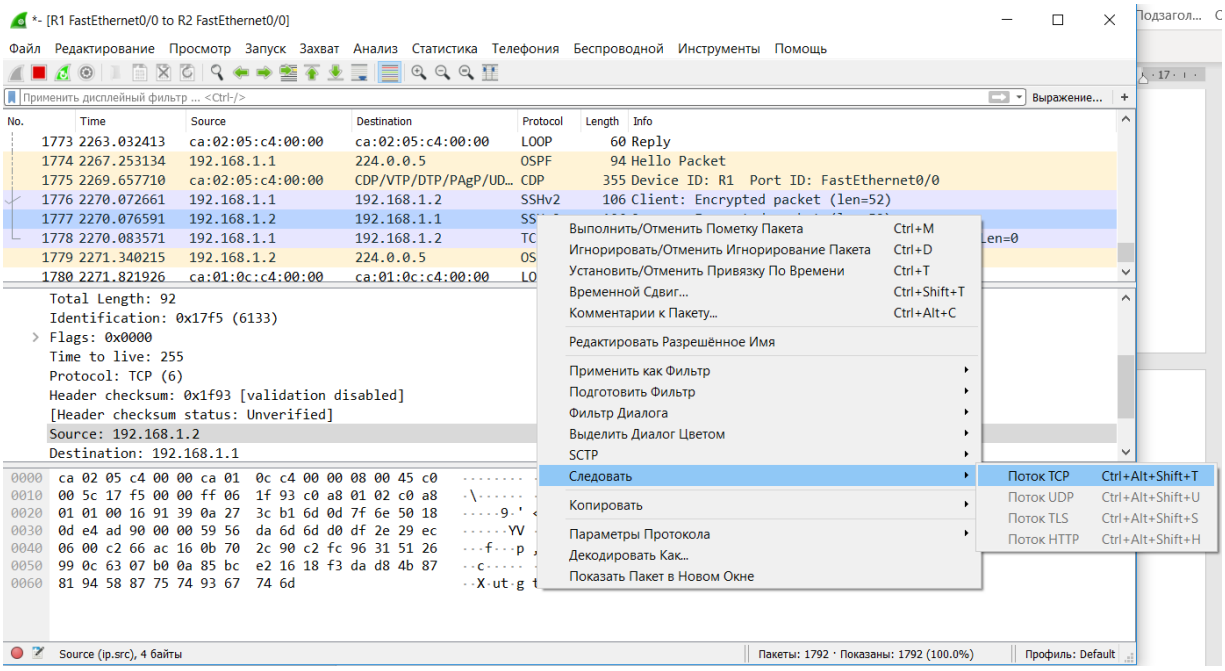

Рисунок 31 – Пакеты протокола SSH

В появившемся окне видно, что все данные представлены в зашифрованном виде.

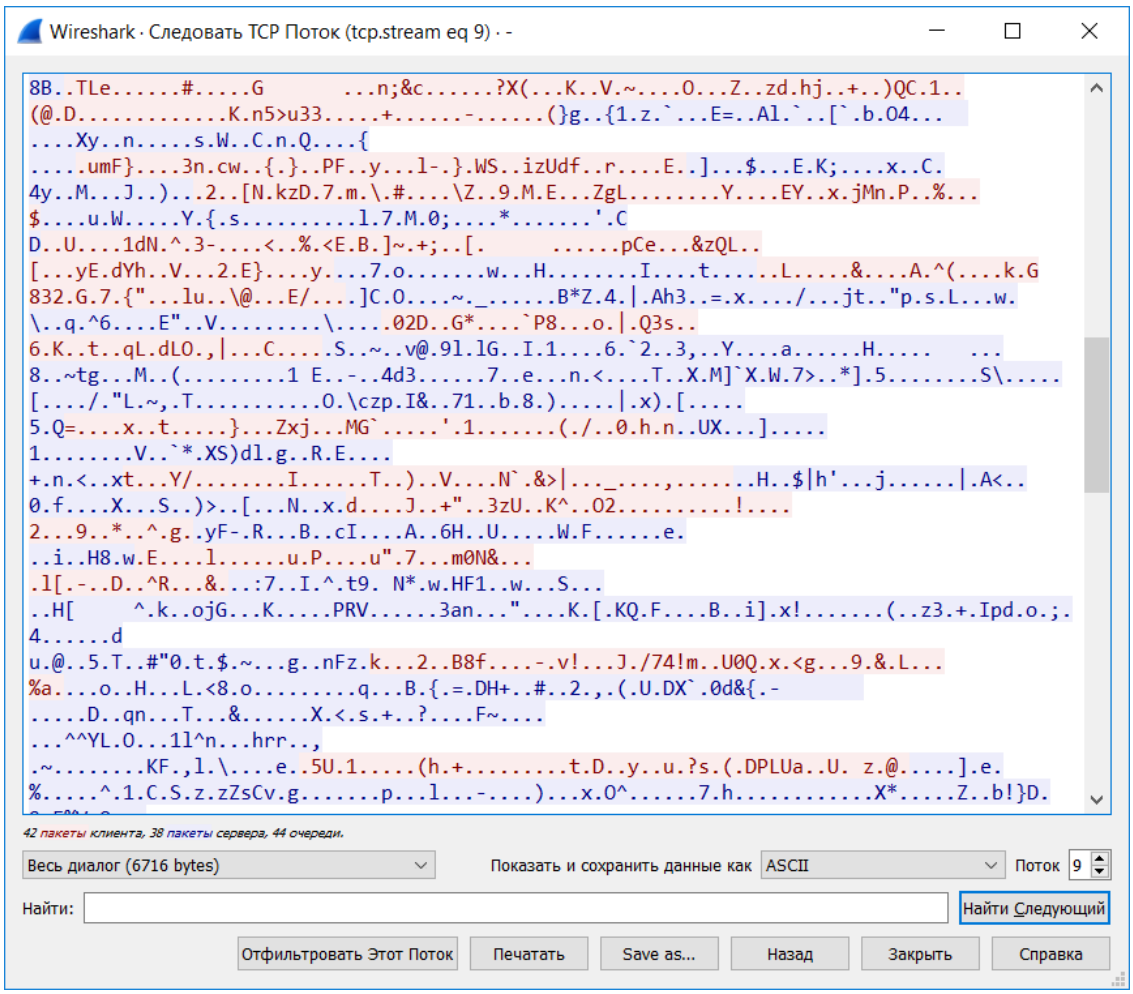

Рисунок 32 – Шифрование данных

Далее можно отключить один из интерфесов нашей схемы, используя команду “shutdown”.

Проследить, каким образом будут передаваться пакеты до и после отключения интерфейса на схеме. Так можно понять принцип работы протокола OSPF.

9.3. Контрольные вопросы

1. Для чего нужен wireshark?
2. Какой главный минус программы wireshark?
3. Что такое telnet?
4. Какие протоколы защиты на канальном уровне есть в модели OSI?
5. Какие протоколы защиты протоколы защиты есть на сетевом уровне модели OSI?
6. Какие протоколы защиты протоколы защиты есть на транспортном уровне модели OSI.
7. На каком уровне модели OSI работает протокол защиты IPSec?
8. Что такое протокол защиты SSH?

10. Лабораторная работа № 10. Построение шифрованной сети на базе технологии IPSec

Цель работы: настроить IPSec туннель средствами пакета GNS-3 и произвести анализ пакетов при помощи Wireshark.

10.1. Рабочее задание

10.1.1. Необходимо собрать схему (рисунок 33) и настроить оборудование. Расписать все подсети и IP адреса интерфейсов. После прописки IP адреса портов необходимо настроить протокол IPSec на каждом роутере.

10.1.2. Провести анализ с помощью пакета Wireshark.

10.2. Методические указания

IPsec – это комплекс протоколов, которые используются для обеспечения аутентификации и сервисов закрытия данных. Это протоколы обмена ключами (IKE) и защиты информации (AH, ESP).

В IPsec используются однонаправленные сессии Secure associations (SA) между участниками соединений для установления безопасных соединений в Интернет. Эти SA определяют операции, применяемые к пакету. Здесь определяются: методы аутентификации, алгоритмы шифрования и ключи, время ключа шифрования, время существования SA и номер последовательности (sequence number).

SA могут быть установлены вручную или автоматически с помощью IKE.

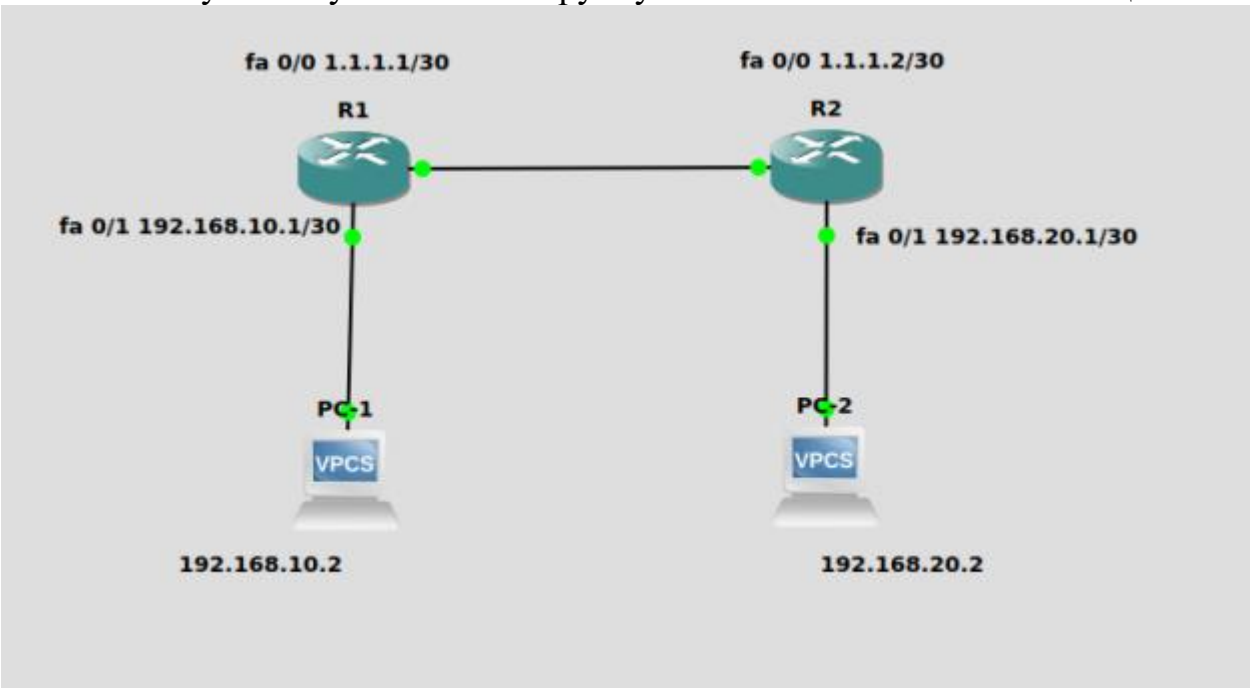

Рисунок 33 – Схема сети

Настройка IPSec Phase1.

R1(config)#crypto isakmppolicy 5#

R1(config-isakmp)#hash sha#

R1(config-isakmp)#authentication preshare#
R1(config-isakmp)#group2#
R1(config-isakmp)#lifetime86400#
R1(config-isakmp)#encryption3des#
R1(config-isakmp)#exit#
R1(config)#crypto isakmp key aues-key address 1.1.1.2#
Настройка IPSec Phase2#
R1(config)#crypto ipsec transform-set MY-SET espaes 128 espmd5-hmac#
R1(cfg-crypto-trans)#crypto ipsec securityassociation lifetime seconds3600

Настройка расширенных ACL политик

R1(config)#ip access-list ext## Настройка расширенных ACL политик ended VPN-TRAFFIC#
R1(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 192168.20.0 0.0.0.255#
Настройка Crypto Map#
R1(config)#crypto map IPSEC-SITE-TO-SITE-VPN 10 ipsec-isakmp#
R1(config-crypto-map)#match addressVPN-TRAFFIC#
R1(config-crypto-map)#set peer 1.1.1.2#
R1(config-crypto-map)#set transform-set MY-SET#
Настройка Crypto Map для исходящего интерфейса на R1#
R1(config)#int fa0/0
R1(config-if)#crypto mapIPSEC-SITE-TO-SITE-VPN#
Настройка исключений трафика в NAT
R1(config)#ip accesslist extended10#
R1(config-ext-nacl)#deny ip 192.168.0.0 0.0.0.255 192.168.20.0 0.0.0.255#
R1(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R1(config-ext-nacl)#exit#
R1(config)#ip nat inside source list 101 interfaceFastEthernet0/0 overload#
Настройка маршрутизации #
R1(config)# iproute 192.168.200 255.255.255.0 1.1.1.2#

Повторить все то же самое для R2
Настройка IPSec Phase1#
R2(config)#crypto isakmp policy 5#
R2(config-isakmp)#hash sha#
R2(config-isakmp)#authentication pre-share#
R2(config-isakmp)#group 2#
R2(config-isakmp)#lifetime 86400#
R2(config-isakmp)#encryption 3des#
R2(config-isakmp)#exit#
R2(config)#crypto isakmp key aues-key address 1.1.1.1#

Настройка IPSec Phase2

R2(config)#crypto ipsec transform-set MY-SET esp-aes 128 esp-md5-hmac#
R2(cfg-crypto-trans)#crypto ipsec securityassociation lifetime seconds 3600#

Настройка расширенных ACL политик
R2(config)#ip access-list extended VPN-TRAFFIC#
R2(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 192.168.100 0.0.0.255#

Настройка Crypto Map#
R2(config)#crypto map IPSEC-SITE-TO-SITE-VPN 10 ipsec-isakmp#
R2(config-crypto-map)#match address VPN-TRAFFIC#
R2(config-cryptomap)#set peer 1.1.1.1#
R2(config-crypto-map)#set transformset MY-SET#
Настройка Crypto Map для исходящего интерфейса на R2#
R2(config)#int fa0/0#
R2(config-if)#crypto mapIPSEC-SITE-TO-SITE-VPN#
Настройка исключений трафика в NAT
R2(config)#ip access-list extended 101#
R2(config-ext-nacl)#deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255#
R2(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 any#
R2(config-ext-nacl)#exit#
R2(config)#ip nat inside source list 101 interface FastEthernet0/0 overload#
Настройка маршрутизации
R2(config)# ip route 192.168.10.0 255.255.255.0 1.1.1.1

Тестирование
1) PC1# ping 192.168.20.2
2) Включите Wireshark между R1 и R2 и убедитесь, что трафик шифруется. В Wireshark видны зашифрованные пакеты ESP.

10.3. Контрольные вопросы

1. Для чего нужен IPSec?
2. Для чего нужен wireshark?
3. Смысл фазы 1 в протоколе IPSec?
4. Понятие фазы 2 в протоколе IPSec?
5. Что такое технология NAT?
6. На каком уровне модели OSI работает протокол IPSec?
7. Из каких основных блоков состоит IPSec?
8. Каковы особенности протоколов защиты передаваемых данных (AH, ESP)?

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

Дополнительный план 2021 г.поз.8

Байкенов Алимжан Сергеевич

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ 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 Формат 60×84 1/16
Тираж 50 экз. Бумага типографская № 1
Объём 3,0 уч.-изд. л. Заказ___Цена 1500 тенге

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