МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

федеральное государственное автономное образовательное учреждение высшего образования

«Санкт-Петербургский государственный университет аэрокосмического приборостроения»

ФАКУЛЬТЕТ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ОТЧЕТ О ПРАКТИКЕ

ЗАЩИЩЕН С ОЦЕНКОЙ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

РУКОВОДИТЕЛЬ

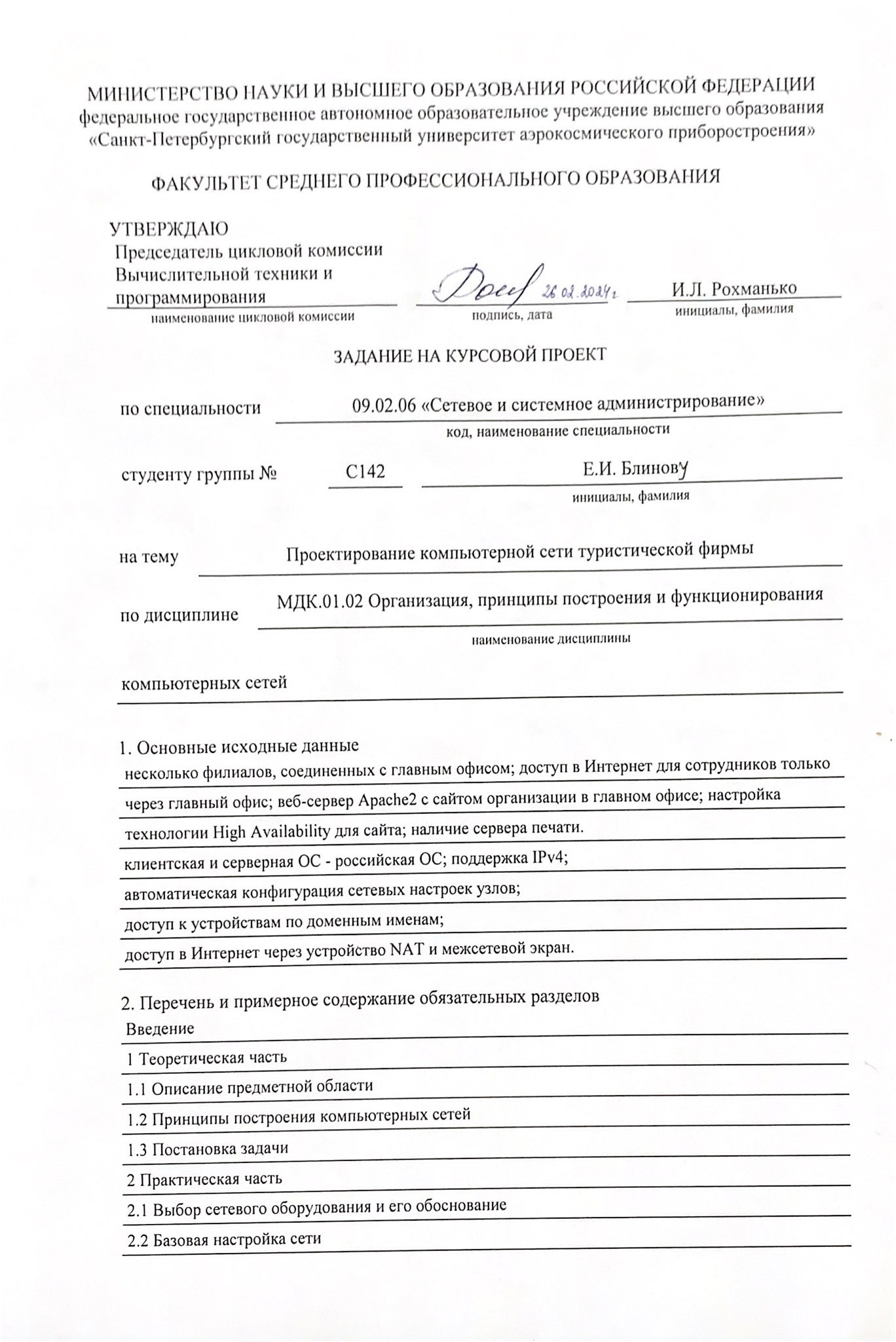
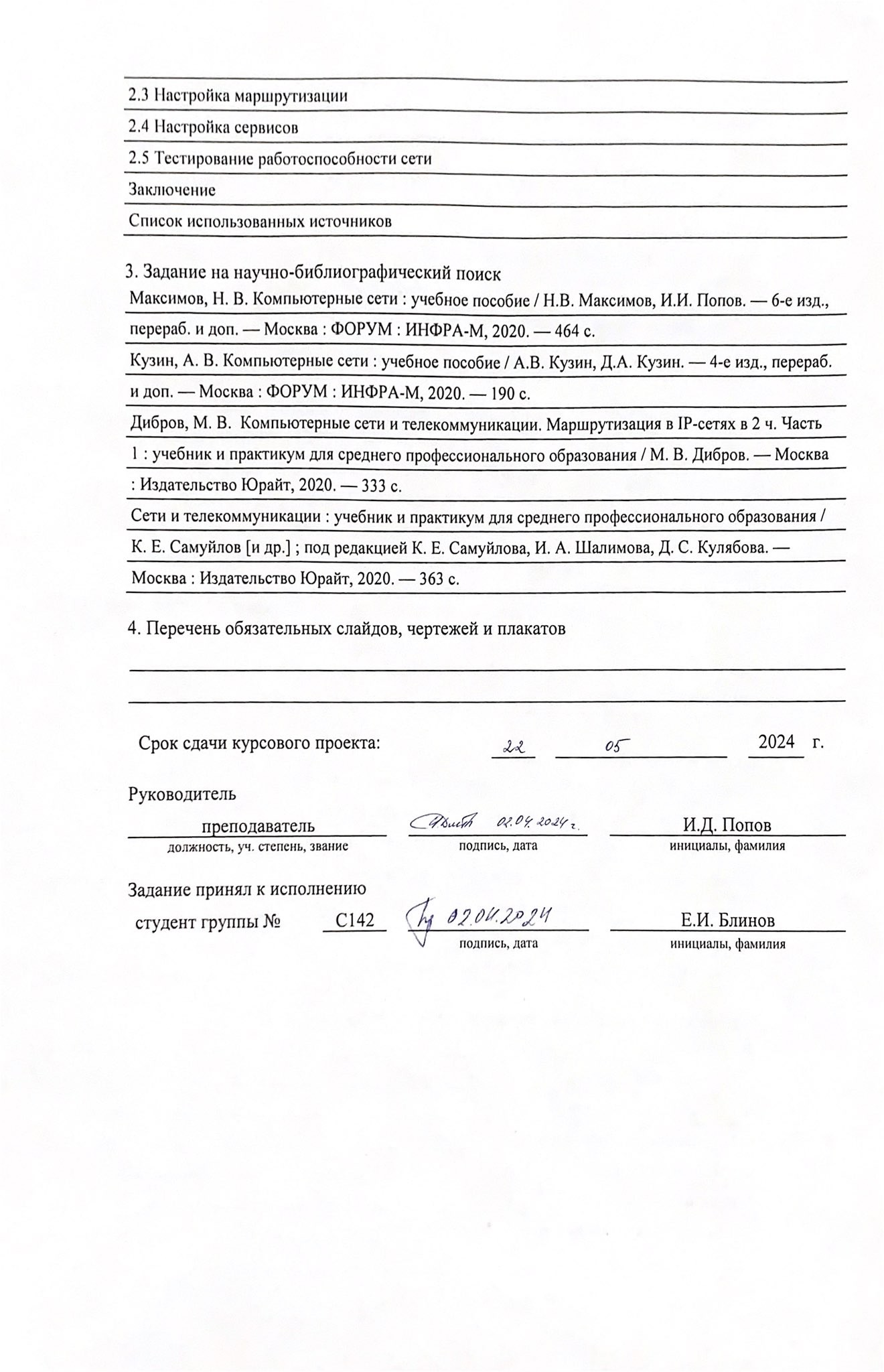
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| преподаватель |  |  |  | Попов И.Д. |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К КУРСОВОЙ РАБОТЕ |
| В СОСТАВЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ |
| ПМ.01 «Выполнение работ по проектированию сетевой инфраструктуры» |
|  |

ОТЧЕТ ВЫПОЛНИЛ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Студент группы | С142 |  |  |  | Е.И. Блинов |
|  | номер группы |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2024

Изм.

Лист

№ докум.

Подп.

Дата

Лист

4

КП.09.02.06.01ПЗ

Разраб.

Блинов Е. И.

Пров.

Попов И. Д.

Н. контр.

Утв.

Проектирование компьютерной сети туристической фирмы

Лит.

Листов

ФСПО ГУАП

**СОДЕРЖАНИЕ**

[**ВВЕДЕНИЕ** 6](#_Toc166608158)

[**1 Теоретическая часть** 7](#_Toc166608159)

[**1.1 Описание предметной области** 7](#_Toc166608160)

[**1.2 Принципы построения компьютерных сетей** 8](#_Toc166608161)

[**1.3 Постановка задачи** 10](#_Toc166608162)

[**2 Практическая часть** 11](#_Toc166608163)

[**2.1 Выбор сетевого оборудования и его обоснование** 11](#_Toc166608164)

[**2.2 Базовая настройка сети** 11](#_Toc166608165)

[**2.3 Настройка** **маршрутизации** 16](#_Toc166608166)

[**2.4 Настройка сервисов** 20](#_Toc166608167)

## **ВВЕДЕНИЕ**

В настоящее время тяжело представить себе туристическую фирму без сетевой инфраструктуры из-за нескольких факторов, приведенных далее.

Управление информацией: туристические компании работают с большим объемом информации, включая бронирование отелей, билетов, транспорта и других услуг. Эффективная сетевая инфраструктура позволяет управлять этой информацией без задержек и с минимальными ошибками.

Работа в реальном времени: клиенты ожидают моментальных ответов и оперативного обновления информации. Хорошо спроектированная сетевая инфраструктура обеспечивает возможность работать в реальном времени, что позволяет операторам быстро реагировать на запросы клиентов и изменения на рынке.

Безопасность данных: туристические компании обрабатывают конфиденциальные данные клиентов, такие как данные паспортов, кредитные карты и информация о бронировании. Надежная сетевая инфраструктура с соответствующими мерами безопасности защищает эти данные от утечек и несанкционированного доступа.

Связь с поставщиками услуг: туристические фирмы часто работают с различными поставщиками услуг, такими как авиакомпании, отели, транспортные компании и туристические агентства.

Масштабируемость и гибкость: туристический бизнес может быть подвержен сезонным колебаниям спроса. Надежная сетевая инфраструктура должна быть способна масштабироваться в зависимости от изменяющихся потребностей бизнеса и гибко адаптироваться к новым технологиям и требованиям рынка.

Исходя из всего вышеперечисленного можно понять то, что любая туристическая фирма в наше время обязана иметь сетевую инфраструктуру для успешного выполнения работы.

## **1 Теоретическая часть**

### **1.1 Описание предметной области**

Туристическая фирма состоит из 4 филиалов включая главный офис. Каждый из филиалов должен иметь выход в интернет, при этом весь трафик необходимо маршрутизировать через главный офис. В главном офисе стоит web-сервер, необходимо повысить его отказоустойчивость, также к серверу необходимо иметь доступ из вне. Также в каждом филиале необходимо расположить сервер печати для печати филиалов и повышенной удобности администрирования. Во всех филиалах необходимо настроить динамическую маршрутизация для удобства пользователей и облегчения администрирования сети. Также один из филиалов делит помещения с другой фирмой и необходимо разграничить трафик двух компаний. В одном из филиалов есть беспроводная точка доступа для работников необходимо настроить её и позволить им обращаться к web-серверу при помощи телефонов. Также для повышения безопасности в филиалах будет настроен удаленный доступ ко всему управляемому оборудованию из главного офиса, филиалы в свою очередь не сможет получить удаленный доступ к управляемому оборудованию. В филиалах необходимо по два маршрутизатора объединённых в один виртуальный для повышения отказоустойчивости, за исключением филиала с беспроводной точкой доступа. Для всех филиалов необходимо настроить доступ из одной подсети в другую при помощи VPN, также между этими сетями должно быть динамическое обновление маршрутов для лучшей маршрутизации и повышенной отказоустойчивости.

Примерная схема сети изображена на рисунке 1.

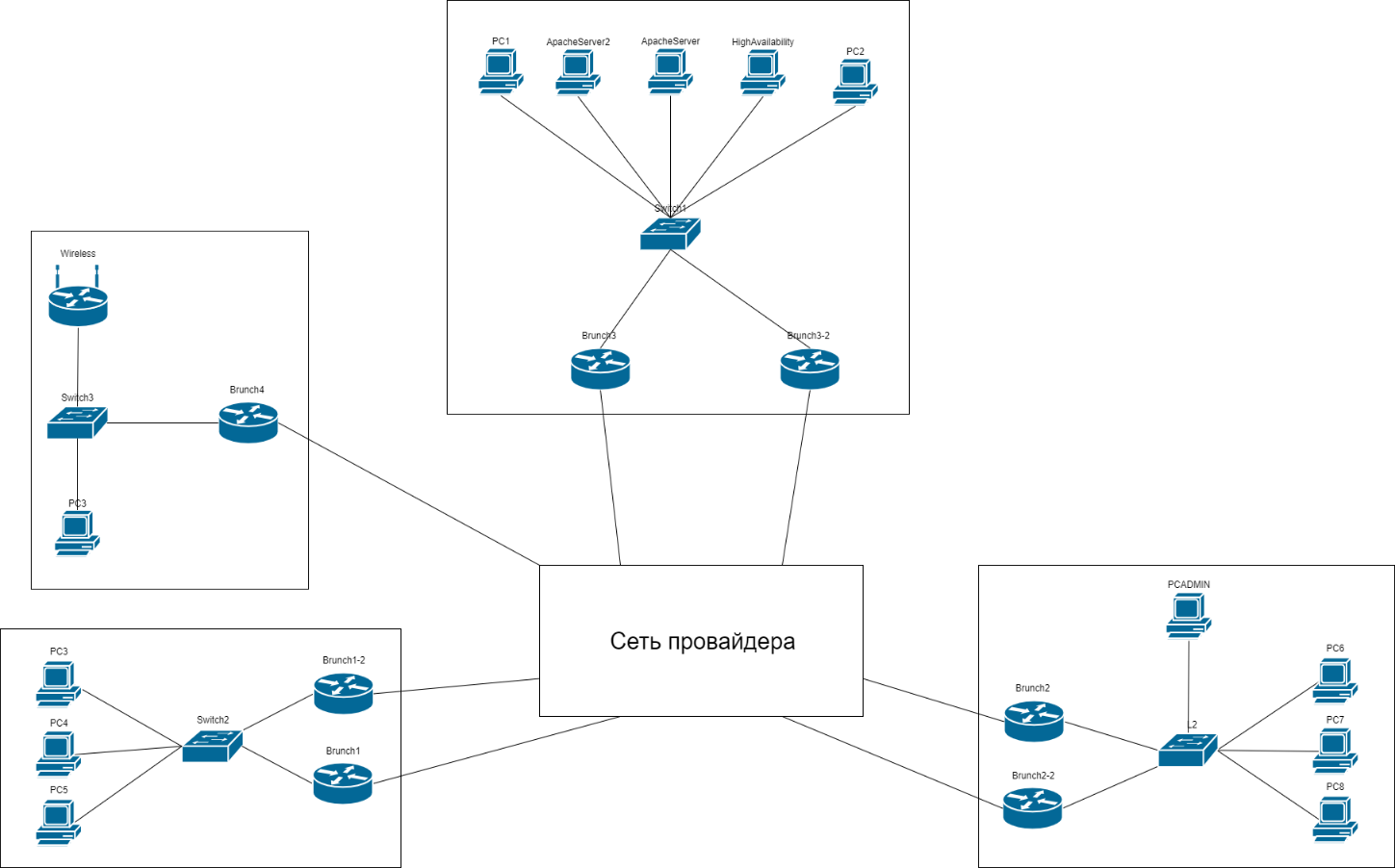


Рисунок 1 – Примерная схема сети

### **1.2 Принципы построения компьютерных сетей**

Поскольку в сети филиалов необходим интернет необходимо настроить преобразование адресов локальной сети в белые адреса. Помимо этого, необходимо настроить разрешение доменных имен в компании, для этого можно реализовать кэширующие DNS, которые будут разрешать имена.

В филиалах есть по две точки выхода в интернет для их объединения в виртуальный маршрутизатор используется протокол VRRP, позволяющий создать виртуальный интерфейс с одинаковым адресом у двух маршрутизаторов и объединить их в один виртуальный маршрутизатор.

Между филиалами необходима VPN связность, которую можно реализовать при помощи L2VPN, к примеру протокол VxLAN, или L3VPN, к примеру протоколы GRE-туннелирование или WireGuard.

Между филиалами, благодаря технологии VPN можно организовать маршрутизацию. Маршрутизация бывает статической и динамической. Статическая маршрутизация использует один маршрут и в случае неисправности соседа ничего не делает, поскольку в сети компании много филиалов и много точек выхода рекомендуется динамическая маршрутизация. Её отличия от статической в том, что маршруты обновляются динамически в зависимости от доступности соседа. Примеров протоколов динамической маршрутизации могут послужить RIP, OSPF, ISIS. RIP сильно отличается от OSPF и ISIS и почти не используется в текущее время.

В филиалах помимо маршрутизаторов есть клиенты в виде ПК, которые с ростом компании будут увеличиваться, для их нормальной работы необходимо настроить на маршрутизаторе DHCP-сервер для динамической выдачи адресов компьютерам и устройствам. Также адреса можно задать статически, но при изменениях в сети, каждое устройство придется менять вручную.

В Компании необходимо поднять Web-сервер для этого можно использовать средства виртуализации и на машине основанной на Linux поднять Web-сервер. На Linux машинах имеется два наиболее распространённых программных обеспечения под названием Apache2 и Nginx. Помимо Web-сервера также необходимо повысить его отказоустойчивость что можно сделать, реализовав технологию High Availability. High Availability – это технология перераспределяющая нагрузку на сервер между несколькими серверами, при отключении одного из серверов нагрузка приходящая на этот сервер перераспределяется на другие сервера.

В компании настроен Web-сервер к которому необходимо иметь доступ из интернета, на маршрутизаторе в таком случае необходимо настроить проброс портов.

В одном из филиалов необходимо разграничить сеть для этого в нем можно реализовать технологию VLAN, позволяющую использовать один и тот же порт маршрутизатора для локальной сети, добавлением метки VLAN.

Также в компании в каждом филиале есть сервер печати, который необходимо настроить для возможности клиентов добавлять сетевые принтеры.

### **1.3 Постановка задачи**

Для выполнения поставленной задачи необходимо:

* Настроить базовую адресацию маршрутизаторов
* Настроить DHCP-сервер
* Настроить кэширующий DNS
* Настроить преобразование адресов
* Настроить GRE-туннелирование
* Настроить динамическую маршрутизацию
* Настроить Web-сервера
* Настроить High Availability
* Настроить проброс портов на High Availability
* Настроить беспроводной маршрутизатор
* Настроить VLAN в филиале
* Настроить Firewall в компании
* Настроить VRRP на маршрутизаторах

## **2 Практическая часть**

### **2.1 Выбор сетевого оборудования и его обоснование**

### **2.2 Базовая настройка сети**

Схема сети L1 показана в приложении А.

Схема сети L2 показана в приложении Б.

Схема сети L3 показана в приложении В.

Схема диаграммы маршрутизации показана в приложении Г.

#### 2.2.1 Настройка адресации

Для начала настройки маршрутизаторам в сети были выдан локальный адрес, адрес через который филиалы общаются выдается им провайдером. На рисунке 2 и 3 показано как они получали адреса

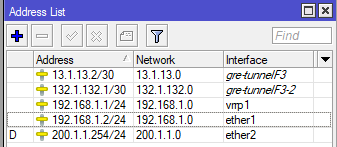


Рисунок 2 – Статический адрес на Brunch1

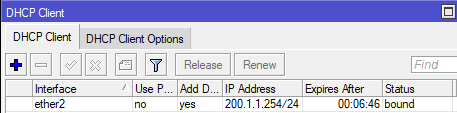


Рисунок 3 – Динамический адрес на Brunch1

Аналогично были настроены другие маршрутизаторы Mikrotik.

Для настройки ESR мы подключили два интерфейса и создали две зоны настройки показаны ниже

config

security zone trust

security zone untrust

security zone-pair trust self

rule 1

action permit

match protocol icmp

match icmp echo

exit

exit

security zone-pair untrust self

rule 1

action permit

match protocol icmp

enable

После настройки зон безопасности заходим на сами интерфейсы и настраиваем их.

config

int gi1/0/8

ip add dhcp

security-zone untrust

int gi1/0/4

ip add 192.168.4.1/24

security-zone trust

#### 2.2.2 Настройка VRRP в филиалах

Во всех филиалах, кроме 4, настроен VRRP протокол для повышения отказоустойчивости сети. Создаем интерфейс VRRP, задаем на нем адрес и меняем на интерфейсе, также на Backup маршрутизаторах настраиваем no preemption mode, и уменьшаем приоритет. Сама настройка показана на рисунках 4 и 5.

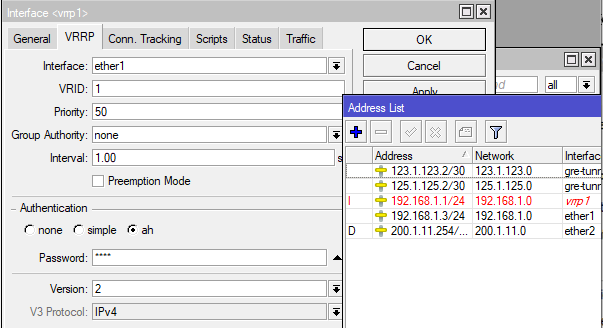


Рисунок 4 – Настройка Backup vrrp на Brunch1-2

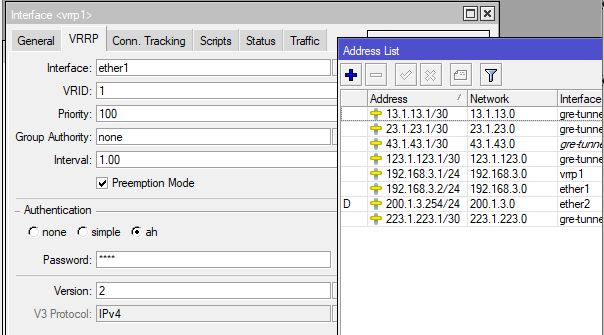


Рисунок 5 – Настройка Master vrrp на Brunch3

Аналогично настроены маршрутизаторы в первом и третьем филиале.

Настройка во втором филиале не сильно отличается за исключением того, что там два VRRP интерфейса, и они поставлены на vlan интерфейсы. Настройка показана на рисунках 6 и 7.

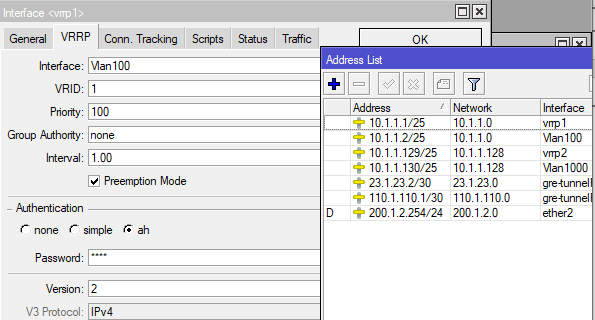


Рисунок 6 – Настройка vrrp1 на Brunch2

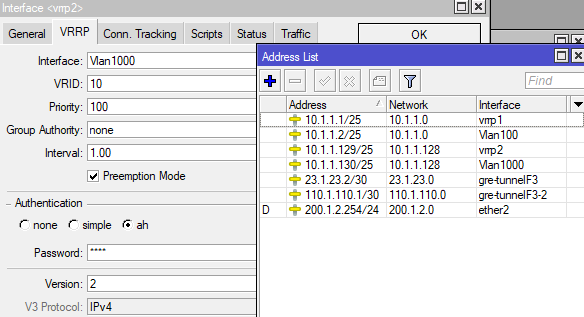


Рисунок 7 – Настройка vrrp2 на Brunch2

Аналогично настроен маршрутизатор Brunch2-2

#### 2.2.3 Настройка беспроводного маршрутизатора

Для начала необходимо объединить в bridge порт порты WLAN и ether2. Это показано на рисунке 8.

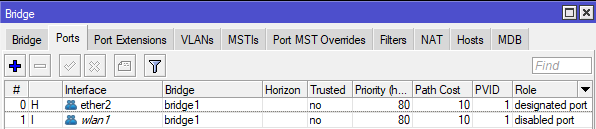


Рисунок 8 – Объединение портов в bridge

После объединения портов необходимо задать адрес для bridge интерфейса, так как маршрутизатор находится в локальной сети он получает адрес по DHCP. Затем мы резервируем этот адрес на ESR.

Теперь прейдем к настройке wlan интерфейса, этот процесс изображен на рисунках 9 и 10.

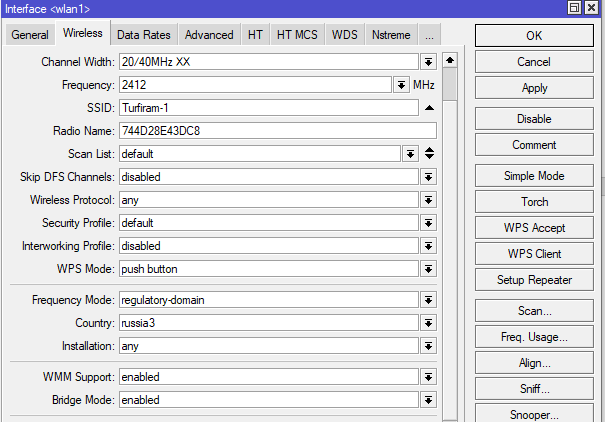


Рисунок 9 – Настройка wlan на Wireless

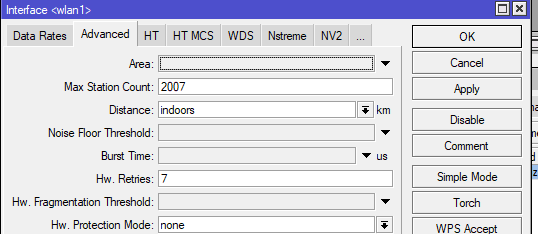


Рисунок 10 – Настройка wlan на Wireless

После данной настройки необходимо задать пароль для WI-FI, в security profiles настраиваем профиль по умолчанию, пароль задаем 34127856, это показано на рисунке 11.

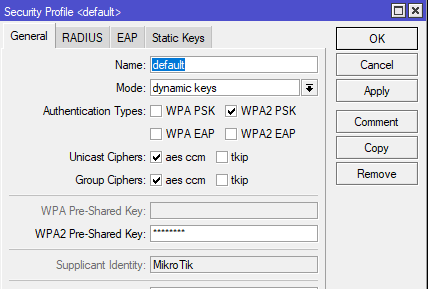


Рисунок 11 – Настройка Security profile

После настройки включаем интерфейс и подключаемся с телефона пользователя.

### **2.3 Настройка** **маршрутизации**

#### 2.3.1 Настройка GRE туннелирования

Весь трафик должен проходить через главный офис, для этого реализуется GRE-туннелирование и настраивается доступ в Интернет, все маршруты проходят через главный офис. Настройка GRE-туннелирования показана на рисунках 12 и 13.

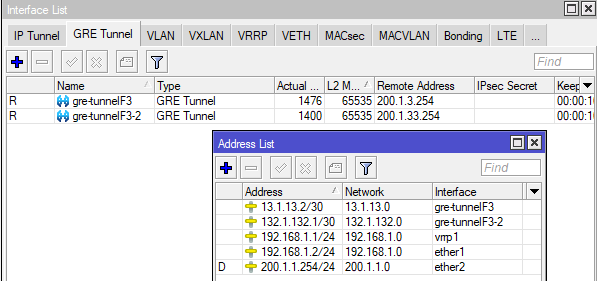


Рисунок 12 – Настройка GRE на Brunch1

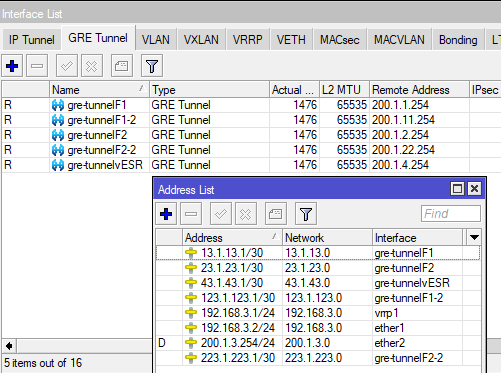


Рисунок 13 – Настройка GRE на Brunch3

Аналогично настроено на других маршрутизаторах в сети, за исключением ESR, его конфигурация показана далее:

config

security zone-pair untrust self

rule 5

//Для дальнейшей настройки OSPF

action permit

match protocol ospf

enable

exit

exit

//Добавляем возможность эхо запроса в другие области

security zone-pair trust untrust

rule 1

action permit

match protocol icmp

enable

exit

rule 2

action permit

match protocol ospf

enable

exit

exit

tunnel gre 3

security-zone untrust

local address 200.1.4.254

remote address 200.1.3.254

ip address 43.1.43.2/30

enable

#### 2.3.2 Настройка OSPF

После настройки GRE туннелей, локальные сети должны иметь доступ друг к другу, для этого настраивается OSPF внутри GRE-туннелей. Настройка OSPF показана на рисунках 14-16.

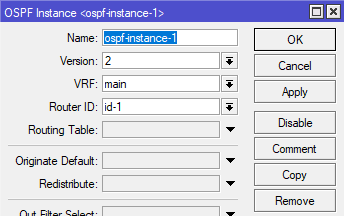


Рисунок 14 – Настройка OSPF instance на Brunch3

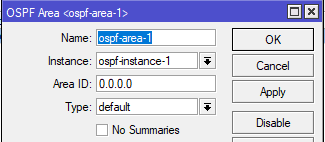


Рисунок 15 – Настройка OSPF area на Brunch3

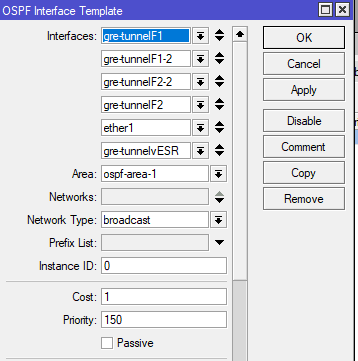


Рисунок 16 – Настройка OSPF interfaces на Brunch3

Аналогично OSPF настроен на других маршрутизаторах Mikrotik, настройка на ESR показана далее:

Router

Router ospf 1

router-id 4.4.4.4

area 0.0.0.0

network 192.168.4.0/24

network 43.1.43.0/30

enable

exit

enable

exit

tunnel gre 3

ip ospf instances 1

ip ospf priority 100

ip ospf

mtu 1476

ttl 250

### **2.4 Настройка сервисов**

#### 2.4.1 Настройка DHCP в филиалах

Во всех филиалах настроена динамическая выдача адресов.

На Mikrotik маршрутизаторах все DHCP сервера находятся на VRRP интерфейсах, это показано на рисунке 17, на рисунке 18 показан пул адресов для этого DHCP сервера.

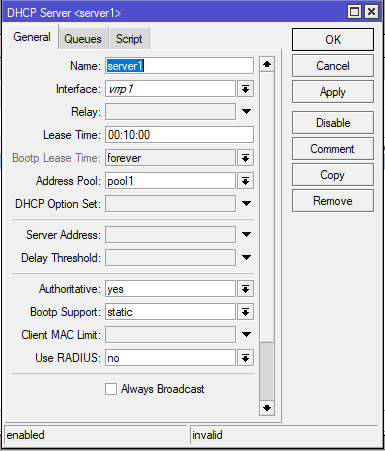


Рисунок 17 – Настройка DHCP сервера на Brunch3-2

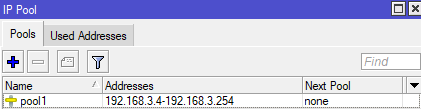


Рисунок 18 – Pool на Brunch3-2

Аналогично настроены другие Mikrotik маршрутизаторы, за исключением второго филиала в котором 2 DHCP сервера, а не один, и в 3 филиале. Настройка ESR показана далее:

config

object-group service dhcp\_server

port-range 67

exit

security zone-pair trust self

rule 2

action permit

match protocol udp

match destination-port dhcp\_server

enable

exit

exit

ip dhcp-server

ip dhcp-server pool pool1

network 192.168.4.0/24

domain-name blinov1.up

default-lease-time 0:0:30

address-range 192.168.4.2-192.168.4.128

dns-server 192.168.4.1

#### 2.4.2 Настройка DNS в филиалах

После настройки доступа клиентов друг с другом необходимо настроить выход в интернет для клиентов. Интернет выдает провайдер, необходимо просто настроить кэширующие DNS сервера. Настройка кэширующего DNS показана на рисунках 19 и 20.

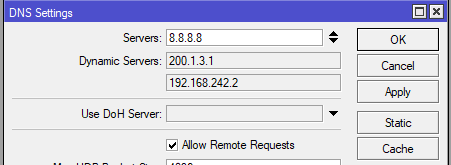


Рисунок 19 – Настройка кэширующего DNS на Brunch3

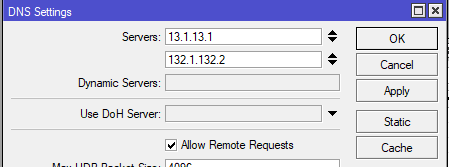


Рисунок 20 – Настройка кэширующего DNS на Brunch1

Как видно на рисунке 18 указывается 2 DNS сервера, так как доступ в Интернет имеют сразу 2 маршрутизатора в главном офисе, при отключении одного, трафик будет идти через другой. Аналогично настроены и другие маршрутизаторы Mikrotik, настройка ESR показана ниже.

domain lookup enable

domain name-server 43.1.43.1 //Адрес GRE туннеля

#### 2.4.3 Настройка Web-сервера

В качестве Web-сервера выбрана операционная система REDOS будет настроен Apache2 сервер. На рисунке 21 показана настройка установка Apache сервера.



Рисунок 21 – Установка Apache2

После установки Apache2 сервера необходимо поменять начальную страницу сайта расположенную в /usr/share/httpd/noindex/index.html. На рисунке 22 показано как был изменен файл.

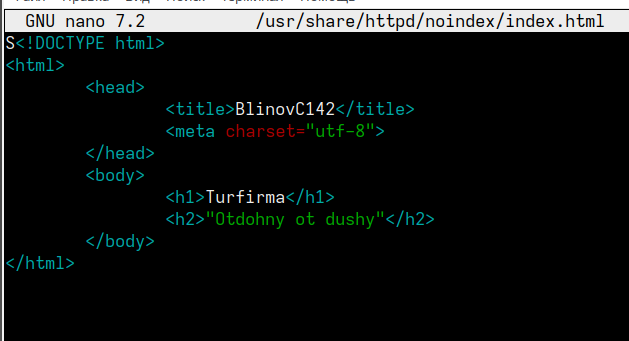


Рисунок 22 – Файл веб страницы

После редактирования этого файла необходимо включить и добавить в автозагрузку, это можно сделать при помощи следующей команды

systemctl enable httpd && systemctl start httpd

Аналогично был настроены другие сервера

#### 2.4.4 Настройка HAProxy

HAProxy установлен на Debian 12 и дальнейшие настройки будут показаны на нем. После настройки всех Web-серверов необходимо объединить их и распределить нагрузку. Ниже приведены команды по установке и настройке HAProxy

apt install haproxy -y

nano /etc/default/haproxy

//В файле добавляем строку ENABLED=1

//После этого мы сможем запустить haproxy

//Далее редактируем файл haproxy

nano /etc/haproxy/haproxy.cfg

//В конец файла вставляем следующую информацию

frontend Local\_Server

bind 192.168.3.249:5000

mode http

default\_backend webserver

backend webserver

mode http

balance roundrobin

option forwardfor

http-request set-header X-Forwarded-Port %[dst\_port]

http-request add-header X-Forwarded-Proto https if { ssl\_fc }

option httpchk HEAD / HTTP/1.1rnHost:localhost

server web1 192.168.3.251:80

server web2 192.168.3.252:80

//Сохраняем файл и настройка завершена теперь необходимо его запустить, это можно сделать следующей командой

service haproxy start

После его запуска необходимо на маршрутизаторе настроить проброс портов на HAProxy, это показано на рисунке 23

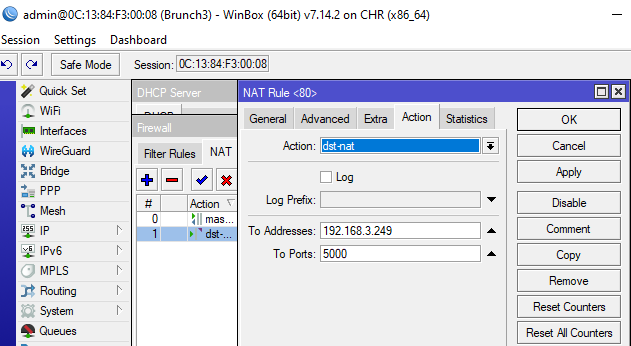


Рисунок 23 – Проброс портов на Brunch3 и Brunch3-2

#### 2.4.5localhost:631 Настройка сервера печати

Для сервера печати выбран cups. Настройка и установка cups показана далее. cups уже установлен на REDOS.

Заходим в браузер переходим по адресу http://localhost:631 и попадаем в меню настройки cups, затем добавляем принтер и разрешаем ему совместный доступ. Процесс добавления принтера в cups показан на рисунках

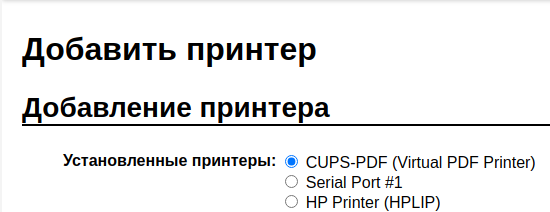


Рисунок 24 – Выбор типа принтера

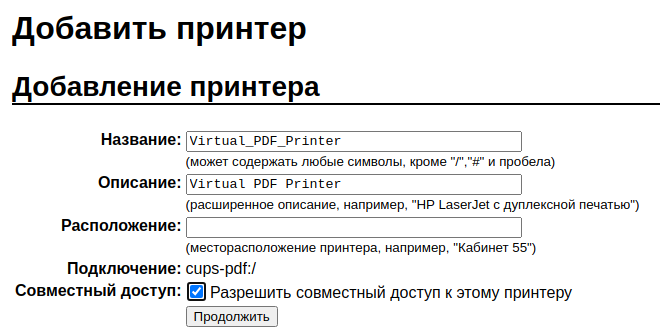


Рисунок 25 – Название принтера

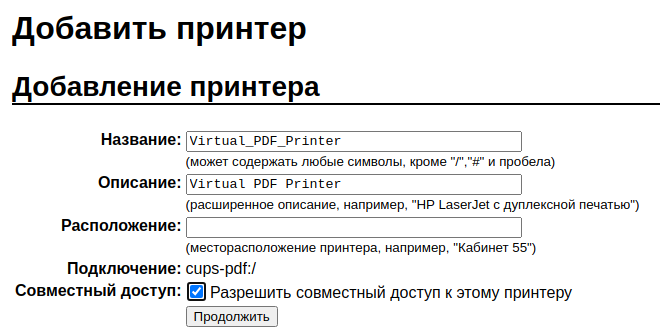


Рисунок 26 – Выбор драйвера принтера

После добавления принтера к нему уже может спокойно обратиться с клиентом в одной подсети.

### **2.5 Тестирование работоспособности сети**

На рисунках 27-29 показана доступность клиентов внутри сети

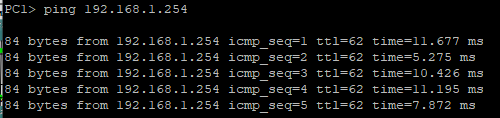


Рисунок 27 – Ping c PC1 PC3

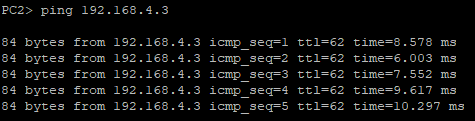


Рисунок 28 – Ping c PC2 PC9

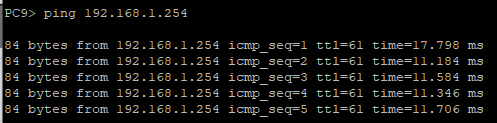


Рисунок 29 – Ping c PC9 PC3

На рисунке 30 показано что весь трафик идет через главный офис, адрес этого GRE-туннеля 13.1.13.1. Также на этом рисунке показано что маршрутизатор разрешает доменное имя ya.ru.

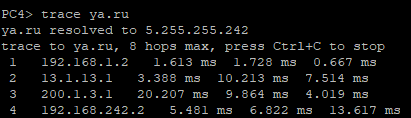


Рисунок 30 – Trace c PC4 ya.ru

На рисунке 31 показана таблица маршрутизации Brunch1, на ней видны маршруты полученные по OSPF.

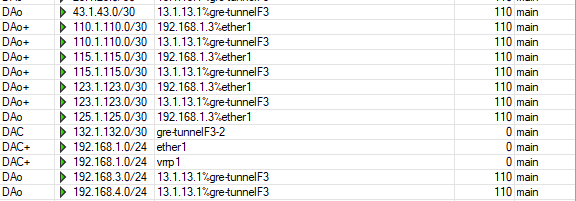


Рисунок 31 – Таблица маршрутизации Brunch1

На рисунке 32 и 33 показан доступ к Web-серверу из локальной сети и из вне.

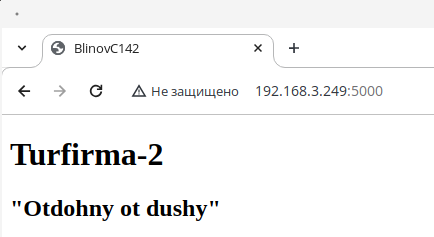


Рисунок 32 – Доступ из локальной сети

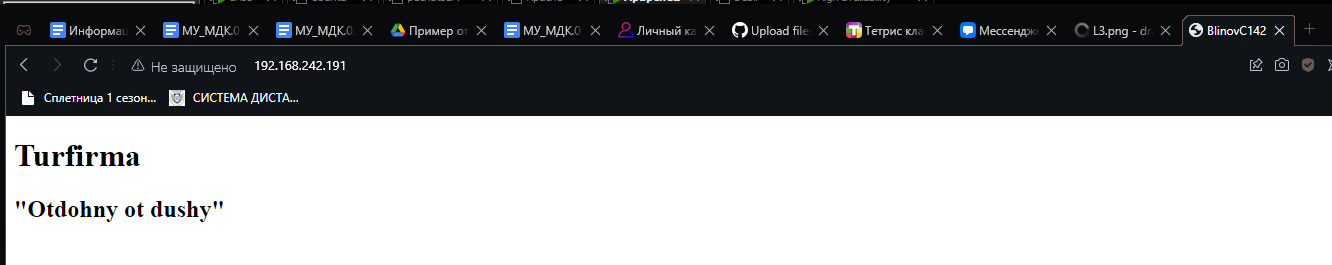


Рисунок 33 – Доступ к Web-серверу из вне

На рисунке 34 и 35 показана работа сервера печати.

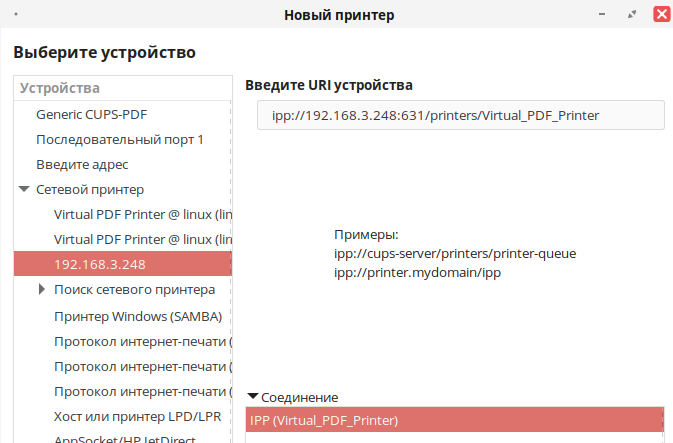


Рисунок 34 – Принтер на клиенте

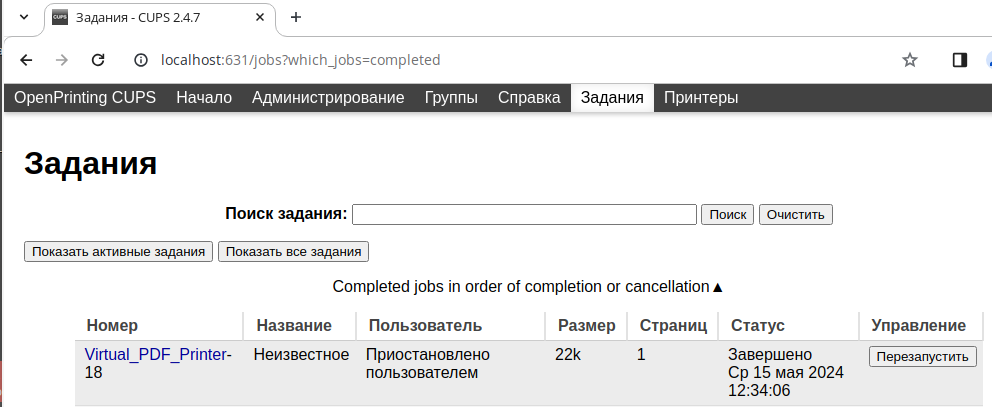


Рисунок 35 – Задание на сервере

На рисунке 36 и 37 показано, что при выключенном маршрутизаторе работает протокол VRRP

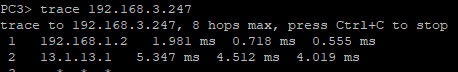


Рисунок 36 – Trace c PC3 PC1, когда мастер Brunch1

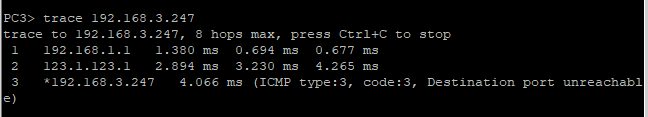
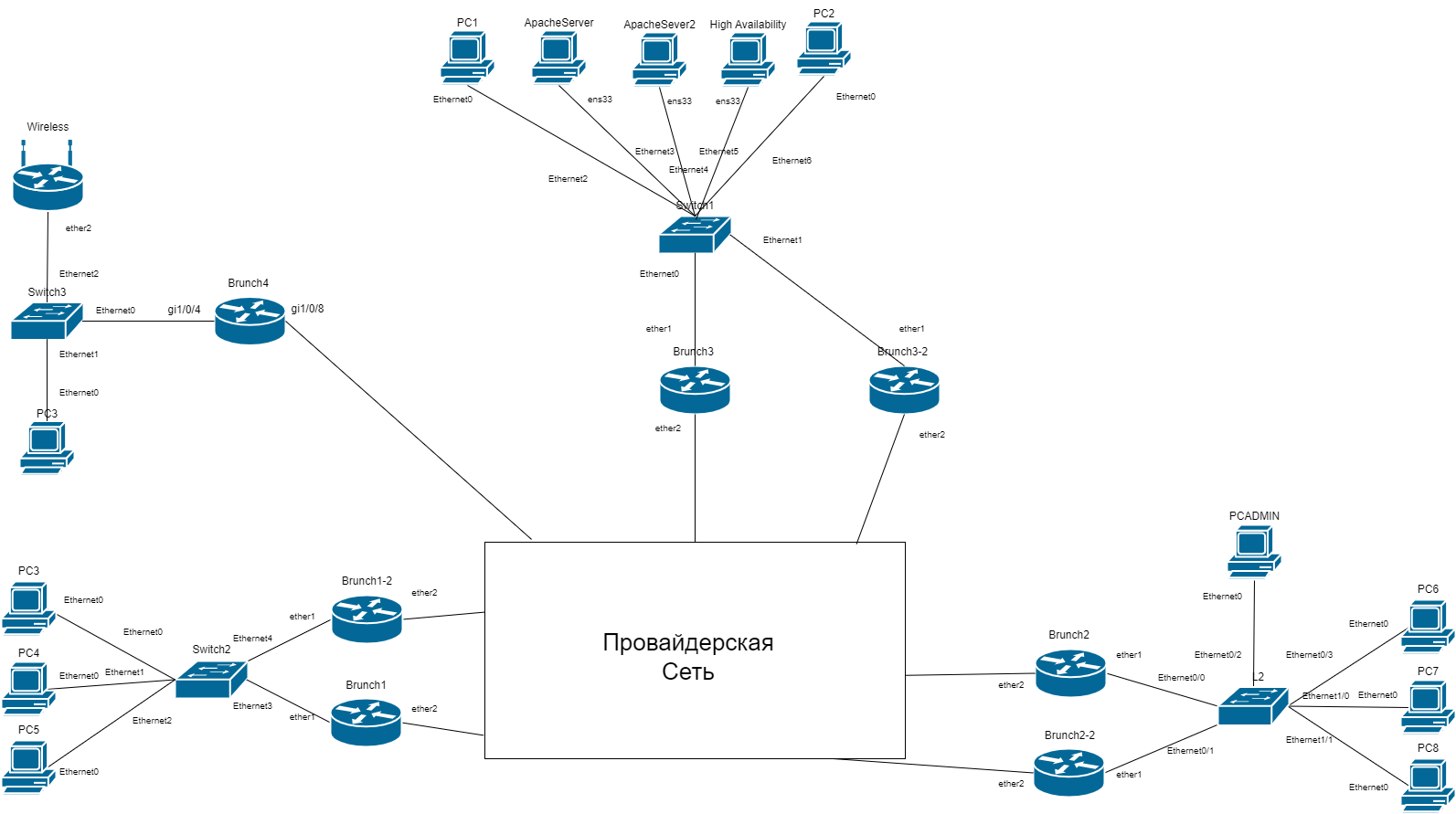


Рисунок 36 – Trace c PC3 PC1, при выключенном Brunch1

## **ЗАКЛЮЧЕНИЕ**

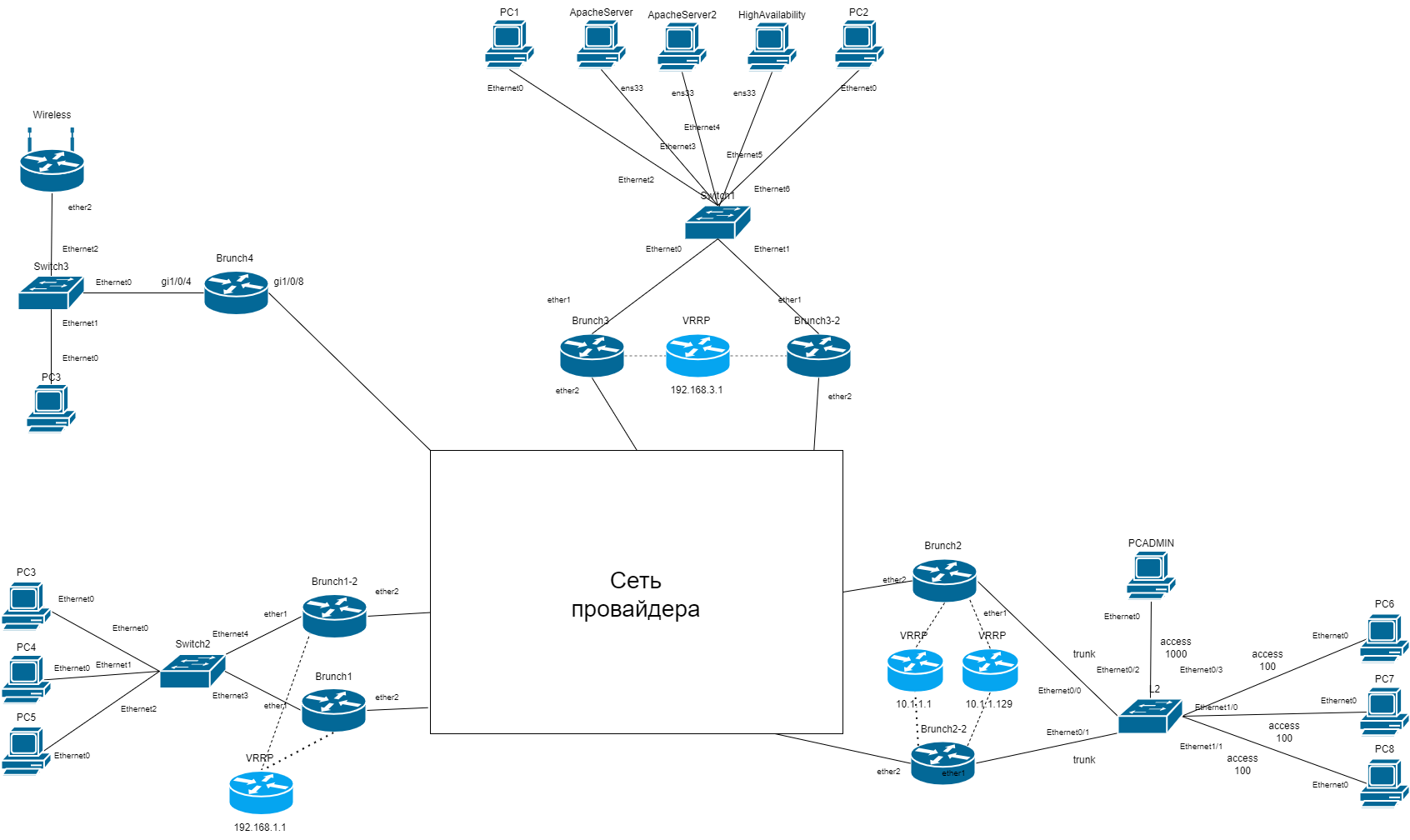
## **ПРИЛОЖЕНИЕ А**

**Схема сети L1**

****

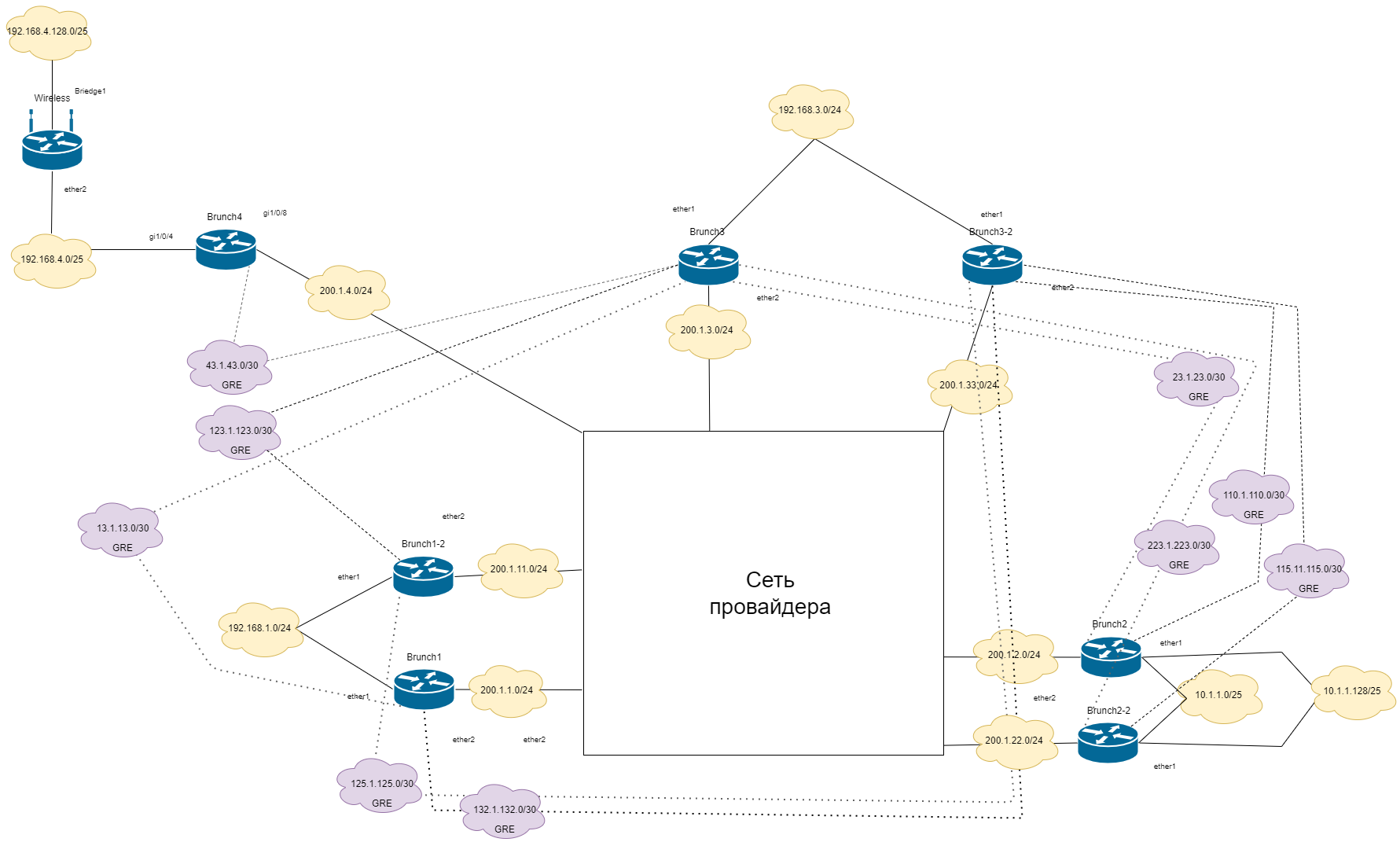
## **ПРИЛОЖЕНИЕ Б**

**Схема сети L2**

****

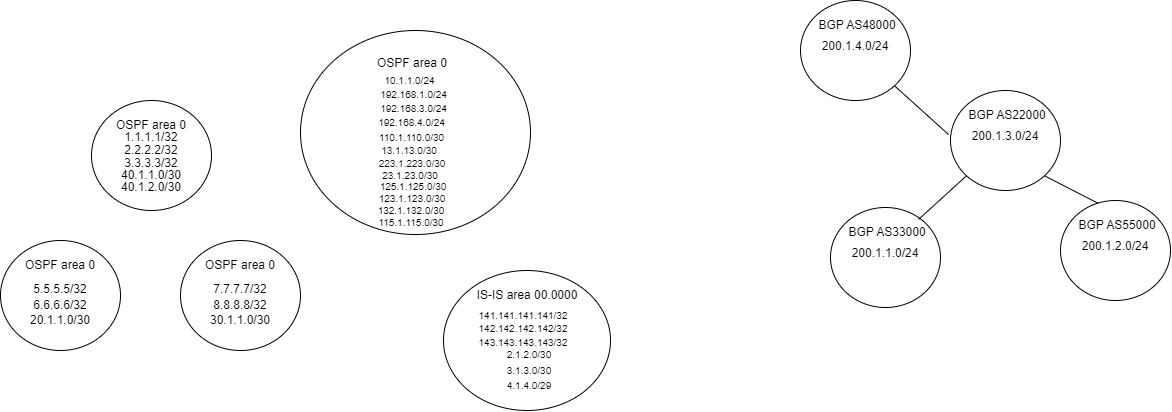
## **ПРИЛОЖЕНИЕ В**

**Схема сети L3**

****

## **ПРИЛОЖЕНИЕ Г**

**ДИАГРАММА МАРШРУТИЗАЦИИ**

****