

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	26.04.2024 г.	Попов И.Д
_____ должность, уч. степень, звание	_____ подпись, дата	_____ инициалы, фамилия

ОТЧЕТ ПО УЧЕБНОЙ ПРАКТИКЕ

В СОСТАВЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ  
ПМ.01 «Выполнение работ по проектированию сетевой инфраструктуры»

Студент группы	С142	26.04.2024 г.	В.М. Строков
	номер группы	_____ подпись, дата	_____ инициалы, фамилия

## Аттестационный лист по учебной практике

Строков Всеволод Михайлович

(фамилия, имя, отчество студента)

обучающийся на 3 курсе в группе С142 по специальности СПО

09.02.06 Сетевое и системное администрирование

код и наименование специальности

успешно прошел учебную практику по профессиональному модулю

ПМ.01 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОЕКТИРОВАНИЮ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

код и наименование профессионального модуля

в объеме 108 часов с «06» апреля 2024 г. по «26» апреля 2024 г.

в организации ФСПО ГУАП, лаб. сетевых технологий, Московский пр., 149-в

наименование организации, структурное подразделение, юридический адрес

### Виды и качество выполнения работ

Виды и объем работ, выполненных обучающимся во время практики	Качество выполнения работ в соответствии с технологией и требованиями организации, в которой проходила практика	
Виды работ	Формы и методы контроля по каждому виду работ	Качество выполненной работы (по пятибалльной шкале)
Проектирование сетевой инфраструктуры	Экспертная оценка результата выполненных работ	
Организация сетевого администрирования	Экспертная оценка результата выполненных работ	
Управление сетевыми сервисами	Экспертная оценка результата выполненных работ	
Модернизация сетевой инфраструктуры	Экспертная оценка результата выполненных работ	
Оформление отчета по выполненной работе	Защита отчета	

Характеристика профессиональной деятельности обучающегося во время учебной практики: получен практический опыт по проектированию архитектуры локальной сети в соответствии с поставленной задачей; установке и настройке сетевых протоколов и сетевого оборудования в соответствии с поставленной задачей; использованию специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей; настройке механизмов фильтрации трафика на базе списков контроля доступа.

Характеристика на обучающегося по освоению общих и профессиональных компетенций в период прохождения практики:

Освоены общие компетенции: ОК 1-5, 9, 10 и профессиональные компетенции:

ПК 1.1. Выполнять проектирование кабельной структуры компьютерной сети;

ПК 1.2. Осуществлять выбор технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности;

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

Дифференцированный зачет по учебной практике «\_\_\_\_\_» \_\_\_\_\_

Дата «26» апреля 2024 г.

## СОДЕРЖАНИЕ

ВВЕДЕНИЕ .....	5
1 Проектирование сетевой инфраструктуры .....	6
1.1 Первичный анализ и создание схем.....	6
1.2 Базовая настройка .....	9
2 Организация сетевого администрирования .....	11
2.1 Настройка сетей провайдера.....	11
2.2 Настройка коммутации .....	14
2.3 Настройка VRRP в главном офисе.....	17
2.4 NAT и portforwarding .....	18
3 Управление сетевыми сервисами .....	21
3.1 Настройка DHCP и DNS серверов .....	21
3.2 Настройка туннелей и OSPF.....	23
3.3 Удаленное администрирование.....	25
4 Модернизация сетевой инфраструктуры .....	27
4.1 Внедрение новых технологий.....	27
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....	30
ПРИЛОЖЕНИЕ А .....	31
ПРИЛОЖЕНИЕ Б.....	32
ПРИЛОЖЕНИЕ В .....	33
ПРИЛОЖЕНИЕ Г.....	34
ПРИЛОЖЕНИЕ Д .....	35

					<b>УП.09.02.06.19Д</b>			
Изм.	Лист	№ докум.	Подп.	Дата				
Разраб.		Строков В. М,			Отчет по учебной практике	Лит.	Лист	Листов
Пров.		Попов И. Д.					4	
						ФСПО ГУАП		
Н. контр.								
УТВ.								

## ВВЕДЕНИЕ

Я, Строков Всеволод Михайлович, студент 3-го курса, проходил учебную практику по дисциплине УП.01 в ФСПО ГУАП, по адресу Санкт-Петербург, Московский проспект, 149ВА. Поставленная задача – проектирование компьютерной сети из курсовой работы для учебной лаборатории программирования, состоящей из двух филиалов и одного главного офиса.

Для успешного выполнения этой задачи необходимо создать сетевую инфраструктуру, способную обеспечить эффективную работу студентов и преподавателей, а также настроить доступ к необходимым ресурсам и сервисам. В контексте учебной лаборатории программирования сетевая инфраструктура играет важную роль в обеспечении доступа к различным программным средствам, обмену данными, надёжности, а также ведению совместной работы над проектами.

Для реализации этой задачи использовались современные технологии сетевого проектирования, включая маршрутизацию, коммутацию, туннелирование, выделенные сервера, а также механизмы отказоустойчивости сетей.

					УП.09.02.06.19Д	Лист
						5
Изм.	Лист	№ докум.	Подп.	Дата		

# 1 Проектирование сетевой инфраструктуры

## 1.1 Первичный анализ и создание схем

Постановка задачи:

Необходимо спроектировать компьютерную сеть учебной лаборатории программирования, которая состоит из 2 филиалов и 1 главного офиса. Филиалы и главный офис подключены к 3-м разным провайдерам, находящихся в разных автономных системах. Создать IP-план. Построить схемы L1, L2, L3. Выбрать оборудование, технологии и протоколы. Разделить исходную сеть 10.19.0.0/16 на требуемое количество подсетей, назначить адреса устройствам для обеспечения IPv4 связности в локальных сетях филиалов и главного офиса. Разделить исходную сеть 200.19.0.0/16 на нужное количество внешних подсетей маршрутизаторов филиалов и главного офиса. Назначить адреса сетевым устройствам.

Таблица 1 – IP-план

Подразделение	Устройство	Интерфейс	IP-адрес
Главный офис	R15	ether2	200.19.128.2
		ether1 (vlan 10)	10.19.176.1
		ether1 (vlan 100)	10.19.224.1
		gre tun 1	10.19.240.1
		gre tun 2	10.19.252.1
		gre tun 3	10.19.254.194
	R16	ether1	200.19.192.2
		ether2 (vlan 10)	10.19.176.2
		ether2 (vlan 100)	10.19.224.2
		gre tun 1	10.19.248.1
		gre tun 2	10.19.254.1
		gre tun 3	10.19.254.130
	S1	vlan 10	10.19.176.4

Продолжение таблицы 1 – IP-план

Подразделение	Устройство	Интерфейс	IP-адрес
	S2	vlan 10	10.19.176.5
	S3	vlan 10	10.19.176.6
	S4	vlan 10	10.19.176.7
	client 1	e0	10.19.224.30
	dns0	ens4	10.19.176.10
	moadm	e0	10.19.176.15
	redosadmin	ens33	10.19.176.70
	proxmox	ens33	10.19.176.100
Филиал 1	R19	ether2	200.19.64.2
		ether1 (vlan 10)	10.19.160.1
		ether1 (vlan 100)	10.19.208.1
		gre tun 1	10.19.240.2
		gre tun 2	10.19.248.2
	S5	vlan 10	10.19.160.2
	S6	vlan 10	10.19.160.3
	pc2admin	e0	10.19.160.50
	client2	e0	10.19.208.250
	client3	e0	10.19.208.249
	dns1	ens33	10.19.160.10
	redos	ens33	10.19.208.248
Филиал 2	R22	ether2	200.19.0.1
		ether1 (vlan 10)	10.19.144.1
		ether1 (vlan 100)	10.19.192.1
		gre tun 1	10.19.252.2
		gre tun 2	10.19.254.2
	pc3adm	e0	10.19.144.40
	dns2	Ens3	10.19.144.10

Продолжение таблицы 1 – IP-план

	S7	vlan 10	10.19.144.2
	S8	vlan 10	10.19.144.3
	redos2	ens33	10.19.192.248
	client4	e0	10.19.192.254
	client5	e0	10.19.192.253
Филиал 3	R23(Huawei)	GE 0/0/0	200.200.19.100
		GE 0/0/1 (vlan 10)	10.19.112.1
		GE 0/0/1 (vlan 100)	10.19.128.1
		gre tun 1	10.19.254.193
		gre tun 2	10.19.254.129
	PC1	Eth 0/0/1	10.19.128.100
	PC2	Eth 0/0/1	10.19.128.200

В качестве маршрутизаторов в филиалах и главном офисе используется CHR MikroTik 14.4.2, в провайдерской сети – Cisco L3. Также, в сетях провайдера и филиалах используются Cisco L2 коммутаторы. Устройства соединены витой парой при помощи технологии Ethernet. В качестве главного сервера предприятия используется Proxmox.

В результате выполнения данного задания была составлена таблица с подсетями, полученными в результате деления на подсети исходных сетей, представленная в приложении Д. Определён выбор используемого оборудования. Созданы следующие схемы:

L1 - Приложение А.

L2 - Приложение Б.

L3 - Приложение В.

Диаграмма маршрутизации – Приложение Г.

А также IP-План, представленный в таблице 1.



## 1.2 Базовая настройка

Постановка задачи:

Провести базовую настройку сетевых устройств.

Базовая настройка включает в себя назначение IP-адреса и имени хоста в соответствии с номером устройства, фамилией и номером по журналу, а также подключение устройств друг с другом в интерфейсы.

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#host
S1(config)#hostname S1_Strokov19
S1_Strokov19(config)#do wr
```

Рисунок 1 – Настройка имени хоста на S1

На остальных коммутаторах выполнены настройки по аналогии

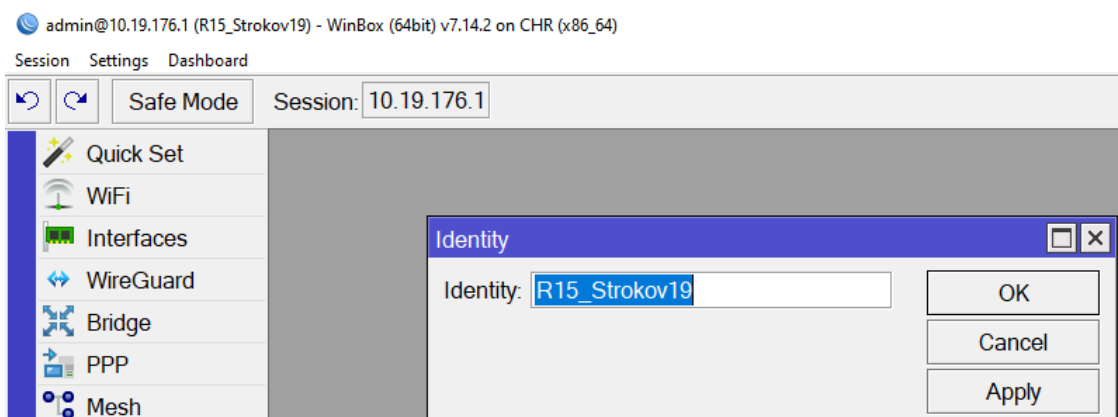


Рисунок 2 – Смена имени хоста на MikroTik (R15)

На остальных маршрутизаторах MikroTik выполнены настройки по аналогии.

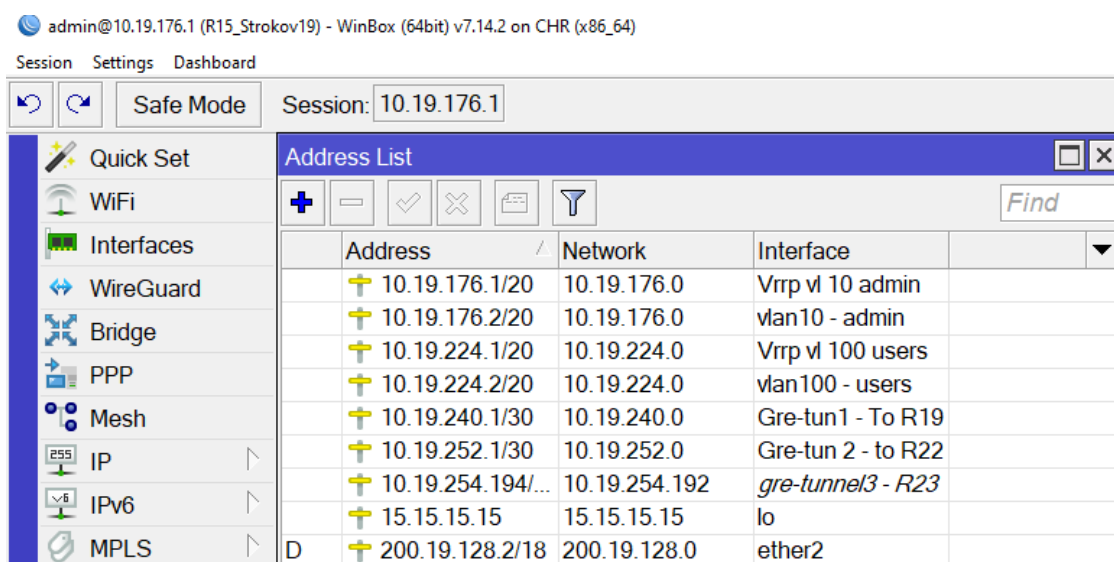


Рисунок 3 – Настройка адресов на маршрутизаторе R15

На других маршрутизаторах и PC выполнена аналогичная настройка.

На остальных коммутаторах выполнены настройки по аналогии. В процессе работы были настроены имена хостов сетевого оборудования: коммутаторы S1 – S9, маршрутизаторы R15, R16, R19, R22, R23. Также, на все устройства назначены IP-адреса. На рисунке 1 представлена настройка имени хоста на коммутаторе S1. На рисунке 2 показана смена хостового имени на маршрутизаторе R15. На рисунке 3 видно, что внешний адрес маршрутизатор получает по DHCP, по заданию.

## 2 Организация сетевого администрирования

### 2.1 Настройка сетей провайдера

Постановка задачи:

Для возможности взаимодействия филиалов и главного офиса, нужно настроить сети провайдера. Необходимо настроить протокол внутренний маршрутизации в сети каждого из провайдеров, а также протокол BGP для взаимодействия автономных систем.

```
R1_Strokov19#sh running-config | section bgp
router bgp 119
  bgp log-neighbor-changes
  neighbor 2.2.2.2 remote-as 119
  neighbor 2.2.2.2 update-source Loopback0
  neighbor 2.2.2.2 next-hop-self
  neighbor 5.5.5.5 remote-as 319
  neighbor 5.5.5.5 ebgp-multihop 2
  neighbor 5.5.5.5 update-source Loopback0
  neighbor 10.10.10.10 remote-as 119
  neighbor 10.10.10.10 update-source Loopback0
  neighbor 10.10.10.10 next-hop-self
  neighbor 11.11.11.11 remote-as 119
  neighbor 11.11.11.11 update-source Loopback0
  neighbor 11.11.11.11 next-hop-self
R1_Strokov19#
```

Рисунок 4 – Настройка BGP на Cisco

На остальных маршрутизаторах выполнены аналогичные настройки.

```
[admin@R12_Strokov19] > ip route/print
Flags: D - DYNAMIC; A - ACTIVE; c - CONNECT, b - BGP, i - IS-IS
Columns: DST-ADDRESS, GATEWAY, DISTANCE
DST-ADDRESS  GATEWAY  DISTANCE
DAb 0.0.0.0/0  19.8.8.8  200
DAi 5.5.5.5/32  30.19.2.1%ether1  115
DAi 6.6.6.6/32  30.19.2.1%ether1  115
DAi 7.7.7.7/32  30.19.2.2%ether1  115
DAi 9.9.9.9/32  30.19.2.2%ether1  115
DAc 12.12.12.12/32  lo  0
DAi 19.8.8.8/32  30.19.2.2%ether1  115
DAi 30.19.1.0/24  30.19.2.1%ether1  115
D i 30.19.2.0/24  30.19.2.1%ether1  115
DAc 30.19.2.0/24  ether1  0
DAi 30.19.3.0/24  30.19.2.2%ether1  115
DAi 30.19.4.0/24  30.19.2.2%ether1  115
DAb 200.19.0.0/18  19.8.8.8  200
DAb 200.19.64.0/18  6.6.6.6  200
DAb 200.19.128.0/18  6.6.6.6  200
DAb 200.19.192.0/18  19.8.8.8  200
DAb 200.200.19.0/24  6.6.6.6  200
[admin@R12_Strokov19] >
```

Рисунок 5 – Просмотр маршрутов на R12, полученных по IS-IS

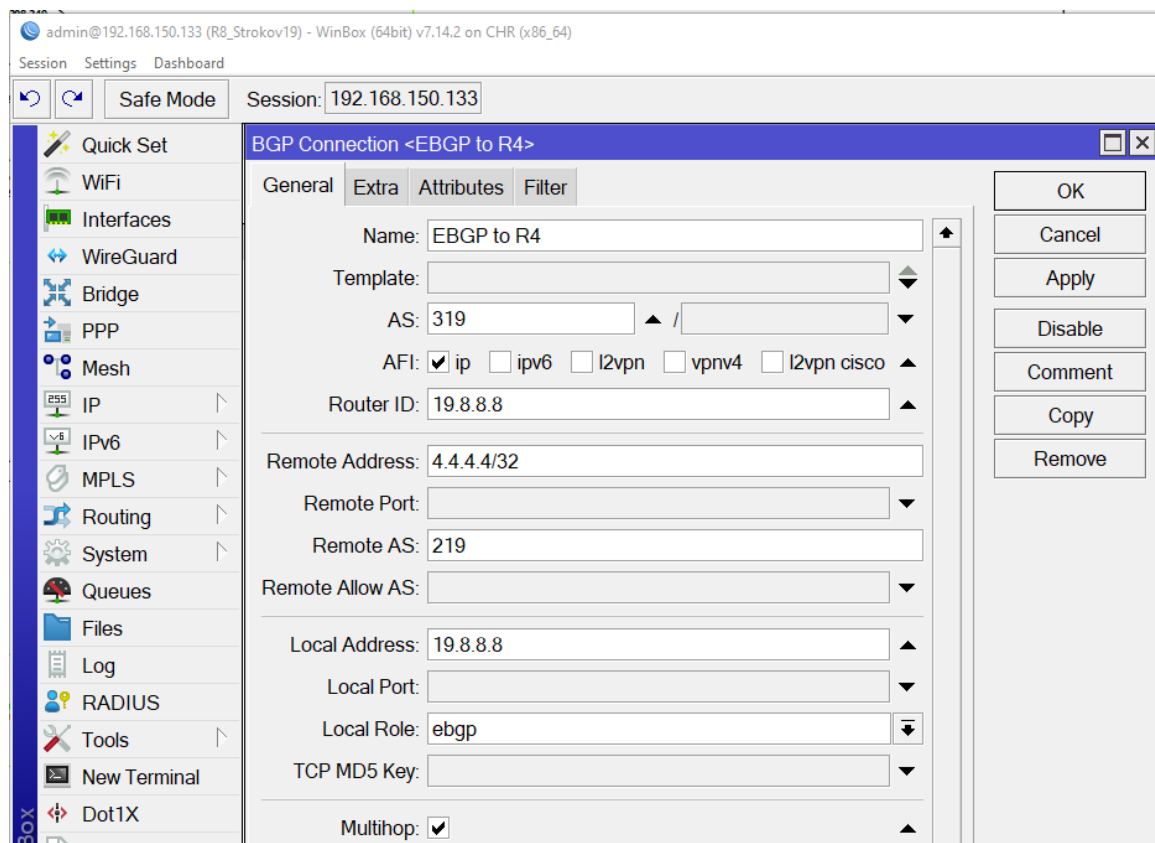


Рисунок 6 – Настройка внешнего соседства BGP на R8

На остальных маршрутизаторах провайдеров выполнены аналогичные настройки.

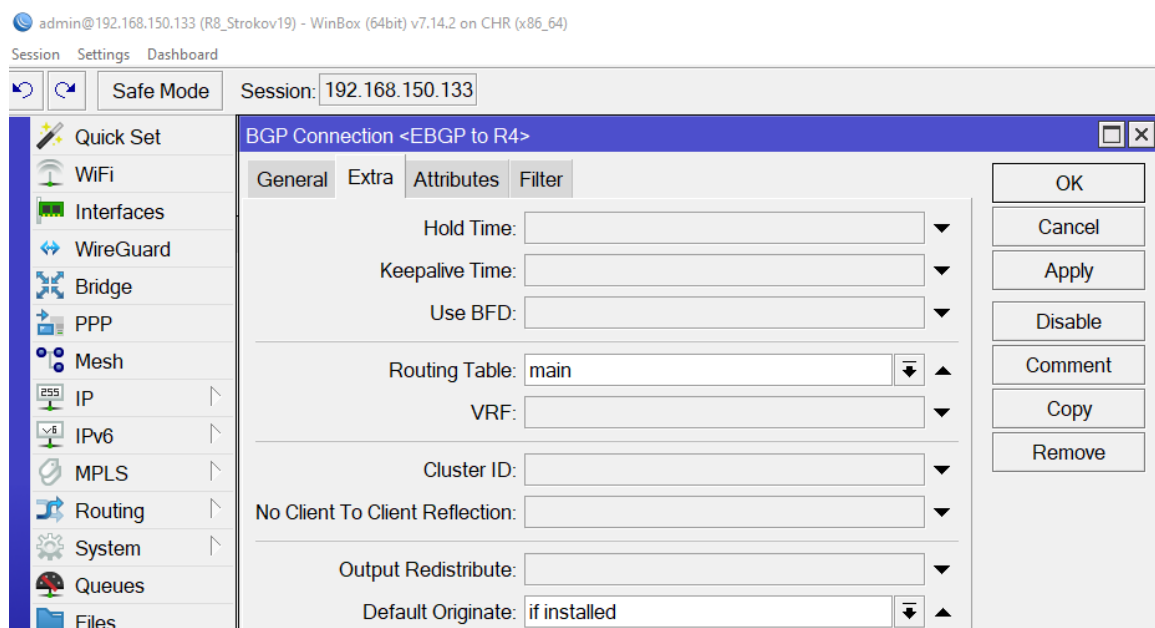


Рисунок 7 – Настройка объявления о маршруте по умолчанию

На остальных маршрутизаторах провайдеров выполнены аналогичные настройки.

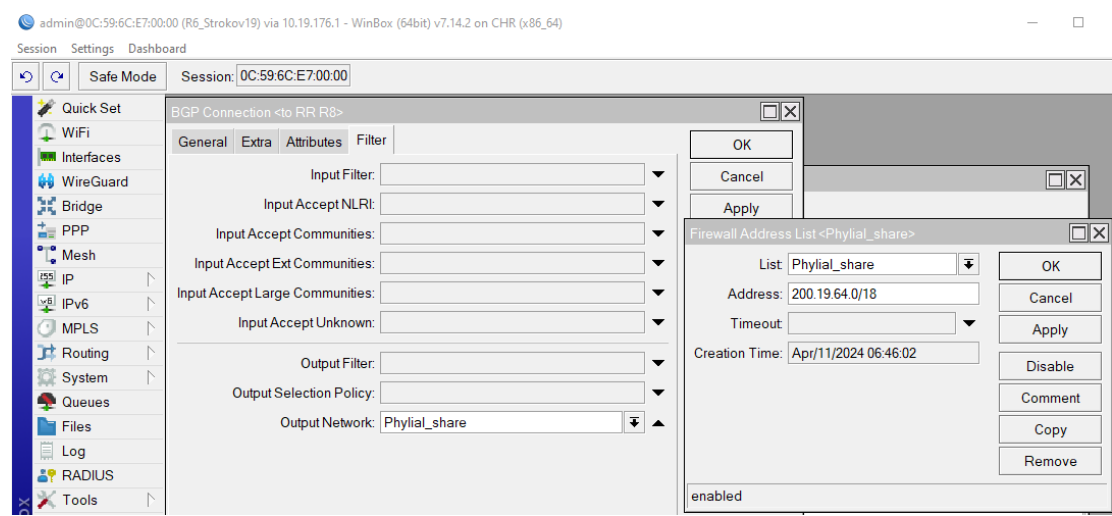


Рисунок 8 – Настройка объявления сетей внешним соседям BGP на R6

На остальных маршрутизаторах провайдеров выполнены аналогичные настройки.

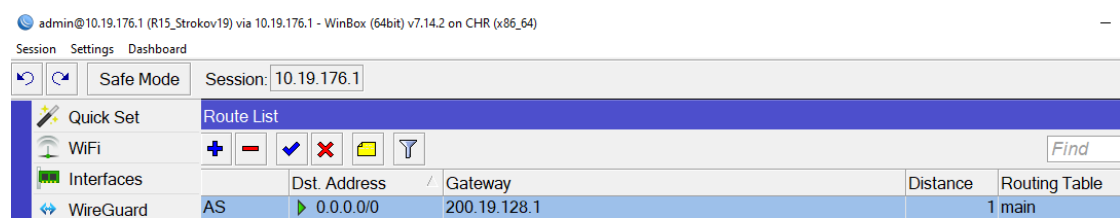


Рисунок 9 – Настройка маршрута по умолчанию

На остальных маршрутизаторах филиалов выполнены аналогичные настройки. На рисунке 4 представлен пример настройки BGP на Cisco R5.

Во всех сетях провайдеров настроен IS-IS. На рисунке 5 видно, что по этому протоколу получены маршруты. На рисунке 6 продемонстрирована конфигурация внешнего соседства BGP на R8. На рисунке 7 можно заметить, что настроено объявление о маршруте по умолчанию, благодаря которому, у устройств будет доступ в интернет.

На рисунке 8 продемонстрировано объявление о внешней сети филиала.

На рисунке 9 продемонстрирован маршрут по умолчанию, отправляющий трафик маршрутизатору провайдера. На рисунке 10 отображена проверка доступности публичного dns сервера.

```
[admin@R15_Strokov19] > ping 8.8.8.8
  SEQ HOST                               SIZE TTL TIME          STATUS
  ---
  0 8.8.8.8                               56 122 20ms83us
  1 8.8.8.8                               56 122 13ms540us
  2 8.8.8.8                               56 122 14ms297us
  3 8.8.8.8                               56 122 15ms278us
sent=4 received=4 packet-loss=0% min-rtt=13ms540us avg-rtt=15ms799us max-rtt=20ms83us
```

Рисунок 10 – Проверка доступности хоста, находящегося в интернете

Благодаря выполненным настройкам, маршрутизаторы филиалов и главного офиса получили доступ в интернет, и могут передавать трафик друг другу.

## 2.2 Настройка коммутации

Постановка задачи:

Создание и настройка vlan для разграничения локальной сети, настройка агрегирования каналов с помощью технологии EtherChannel по протоколу LACP для увеличения надежности сети и увеличения пропускной способности.

```
S4_Strokov19#sh etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)        LACP        Et2/0(P)   Et2/1(P)
2      Po2(SU)        LACP        Et3/0(P)   Et3/1(P)
```

Рисунок 11 – Результат настройки EtherChannel по протоколу LACP на S4

На остальных коммутаторах, участвующих в агрегировании, выполнены аналогичные настройки.

На каждом коммутаторе, создано 2 vlan, 1 для административной сети, и 1 для пользовательской. На рисунке 13 изображён просмотр созданных vlan.

```
S6_Strokov19#sh vl br

VLAN Name                Status    Ports
-----
1    default              active    Et0/2, Et0/3, Et1/0, Et1/1
                                   Et1/2, Et1/3, Et2/0, Et2/1
                                   Et2/2, Et2/3, Et3/0
10   admin                active
100  users                active    Et3/1, Et3/2, Et3/3
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default    act/unsup
1005 trnet-default      act/unsup
S6_Strokov19#
```

Рисунок 12 – Просмотр созданных vlan на S4

На остальных коммутаторах созданы vlan по аналогии.

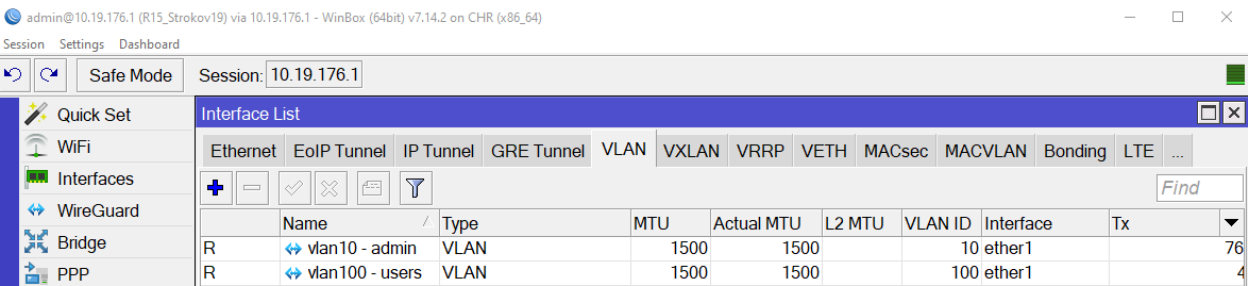


Рисунок 13 – Созданные vlan на R15

На R16 созданы идентичные vlan.

```
S6_Strokov19#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S6_Strokov19(config)#int vlan 10
S6_Strokov19(config-if)#ip address 10.19.160.3 255.255.240.0
S6_Strokov19(config-if)#do wr
```

Рисунок 14 – Настройка IP-адреса на коммутаторе

На других коммутаторах также заданы адреса.

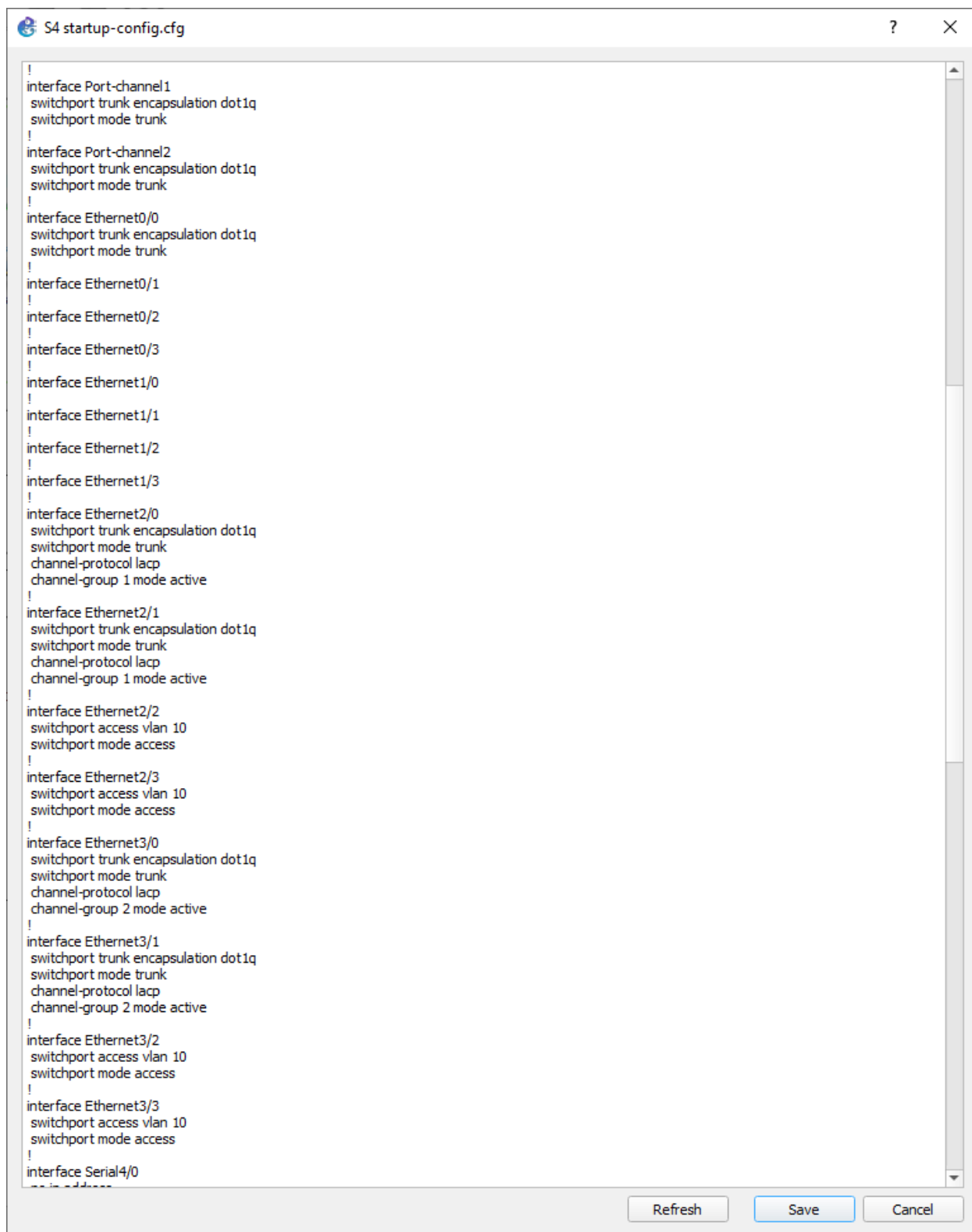


Рисунок 15 – Настройка vlan на интерфейсах S4

На остальных коммутаторах также настроены роли интерфейсов.

При настройке был использован протокол LACP, результат настройки отображён на рисунке 11. На рисунке 12 отображена информация о

					УП.09.02.06.19Д	Лист
						16
Изм.	Лист	№ докум.	Подп.	Дата		



существующих vlan на коммутаторе. На рисунке 13 изображен метод маршрутизации vlan RoAS на MikroTik. Так как в будущем необходимо будет настроить возможность удалённого подключения, в том числе и коммутаторам, им необходимо задать IP-адрес. Эта процедура изображена на рисунке 14.

На основании схемы L2 была выполнена настройка коммутации для сетевых устройств. Etherchannel был настроен на коммутаторах между S1-S4, S2-S4, S5-S6, S7-S8.

2.3 Настройка VRRP в главном офисе

Постановка задачи:

Настроить в главном офисе один из протоколов группы FHRP для обеспечения отказоустойчивости и надёжности.

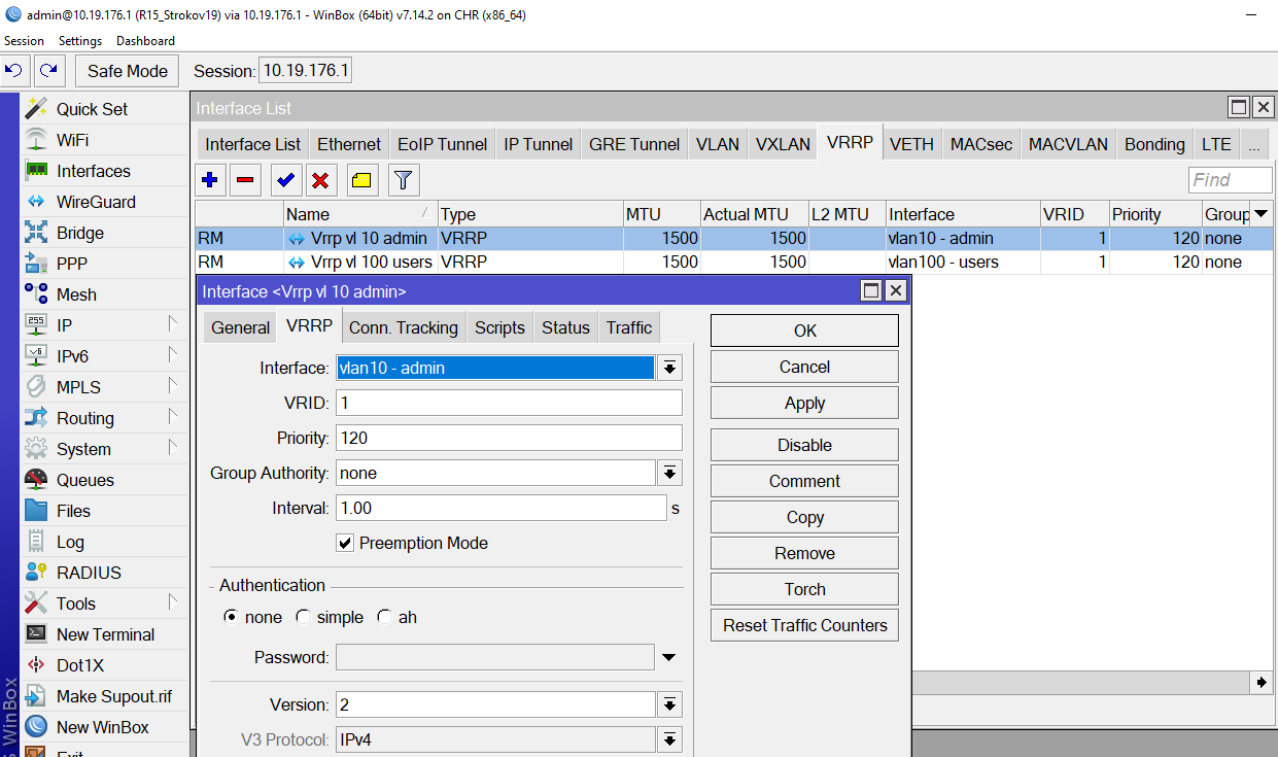


Рисунок 16 – Настройка VRRP на R15

На рисунке 16 изображена процедура настройки VRRP группы на MikroTik. На R16 выполнена идентичная настройка, с приоритетами, установленными в значении "60".

## 2.4 NAT и portforwarding

Поставленная задача:

Обеспечить доступ в интернет устройствам из локальных сетей филиалов и главного офиса. Обеспечить доступ к серверу виртуализации Proxmox из внешних сетей.

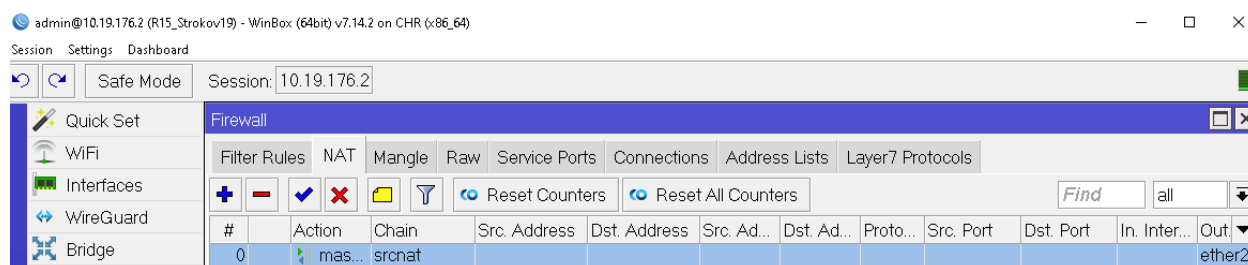


Рисунок 17 – Настройка натирования в сторону внешнего адреса

На маршрутизаторах других филиалов выполнены аналогичные настройки.

```
19_client1> ping 8.8.8.8

84 bytes from 8.8.8.8: icmp_seq=1 ttl=121 time=17.130 ms
84 bytes from 8.8.8.8: icmp_seq=2 ttl=121 time=16.086 ms
84 bytes from 8.8.8.8: icmp_seq=3 ttl=121 time=16.997 ms
84 bytes from 8.8.8.8: icmp_seq=4 ttl=121 time=18.615 ms
84 bytes from 8.8.8.8: icmp_seq=5 ttl=121 time=14.997 ms
```

Рисунок 18 – Проверка доступности адреса из интернета

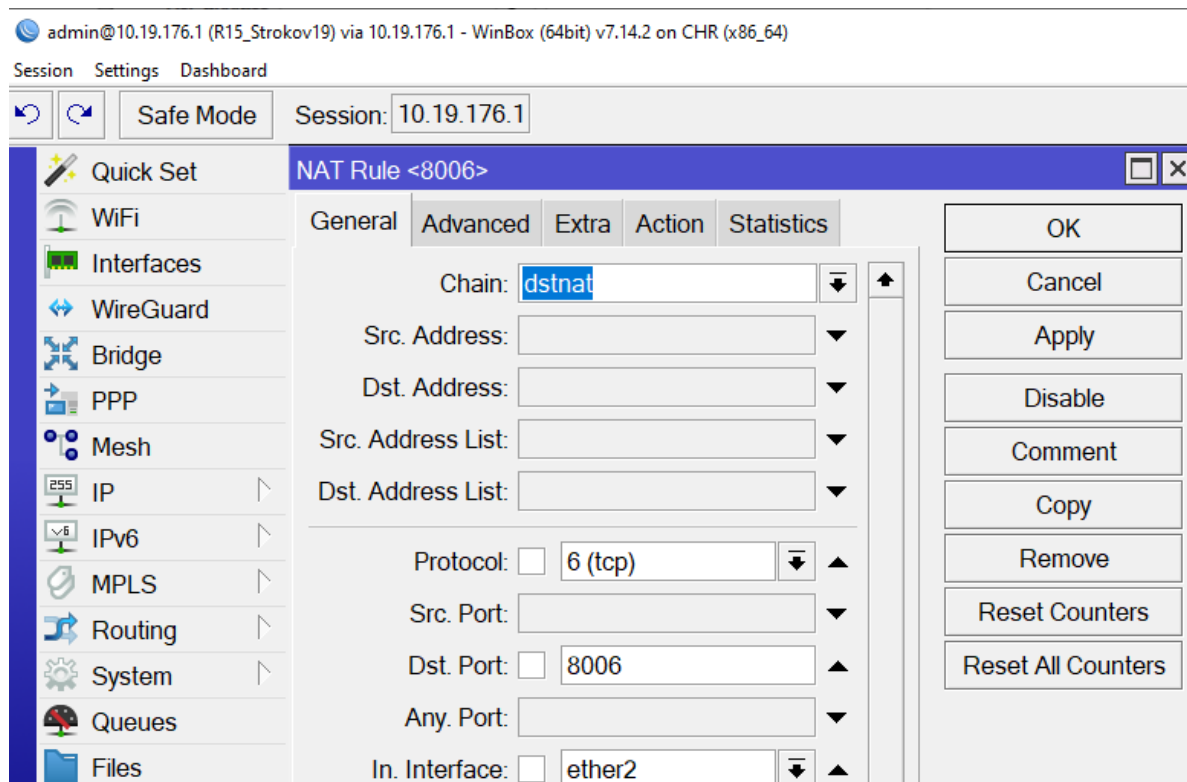


Рисунок 19 – Создание правила проброса порта

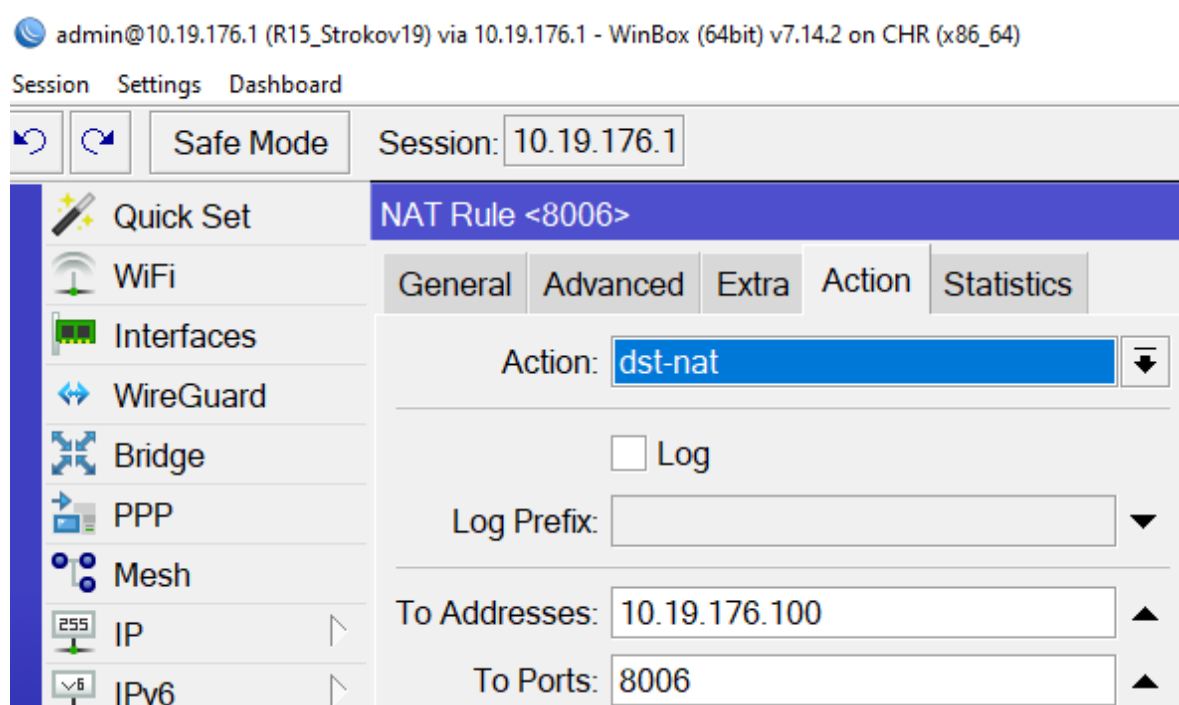


Рисунок 20 – Настройка проброс к серверу Proхтох

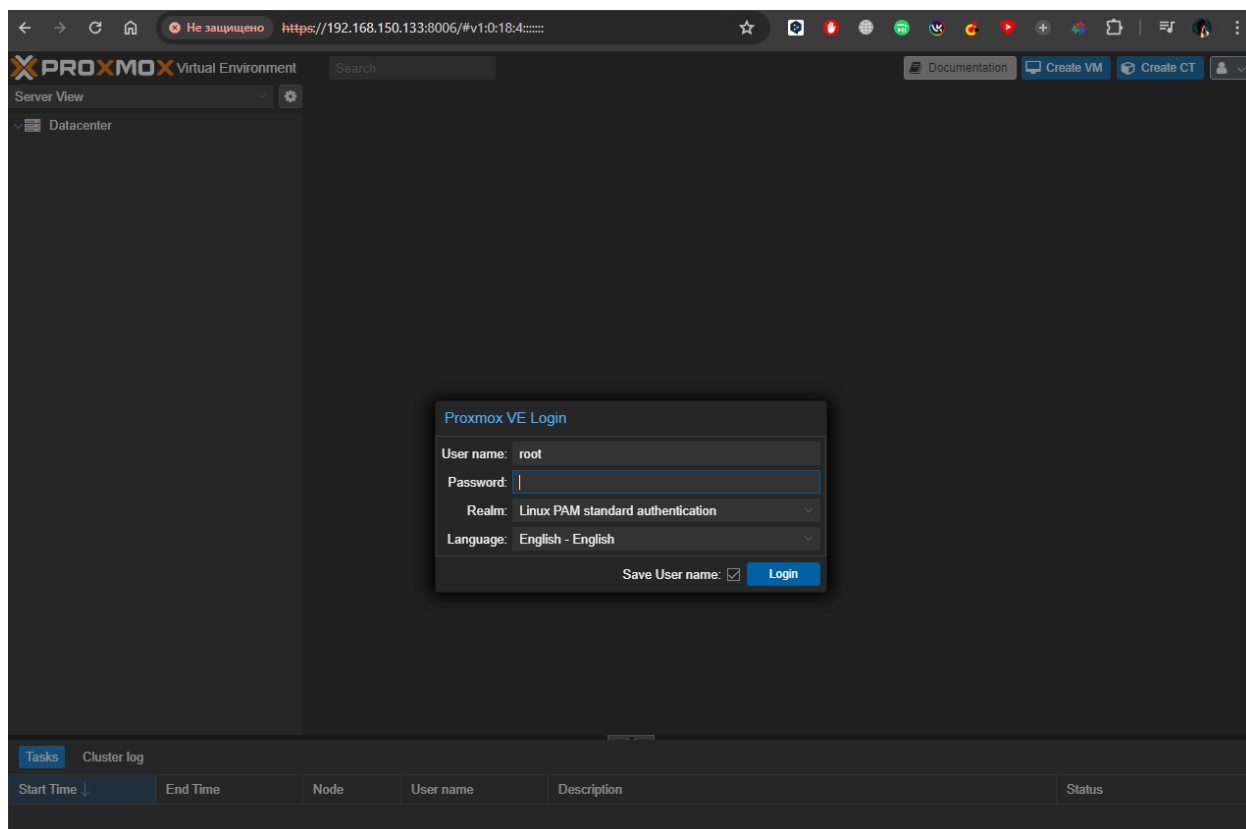


Рисунок 21 – Проверка проброса порта

На рисунке 18 видно, что пакеты успешно доходят то получателя, благодаря чего можно сделать вывод, что натирование работает. На рисунке 19 и 20 показан процесс настройки проброса к серверу. Это необходимо, чтобы к серверу был доступ не только из локальных сетей филиалов, но и из интернета.

### 3 Управление сетевыми сервисами

#### 3.1 Настройка DHCP и DNS серверов

Поставленная задача:

Настроить DHCP сервер на маршрутизаторах, убедиться, что сервер выдаёт адреса. Установить DNS сервер, проверить, что устройства из локальных сетей могут посылать эхо запросы по доменным именам. В качестве доменного имени организации использовать strokov19.up

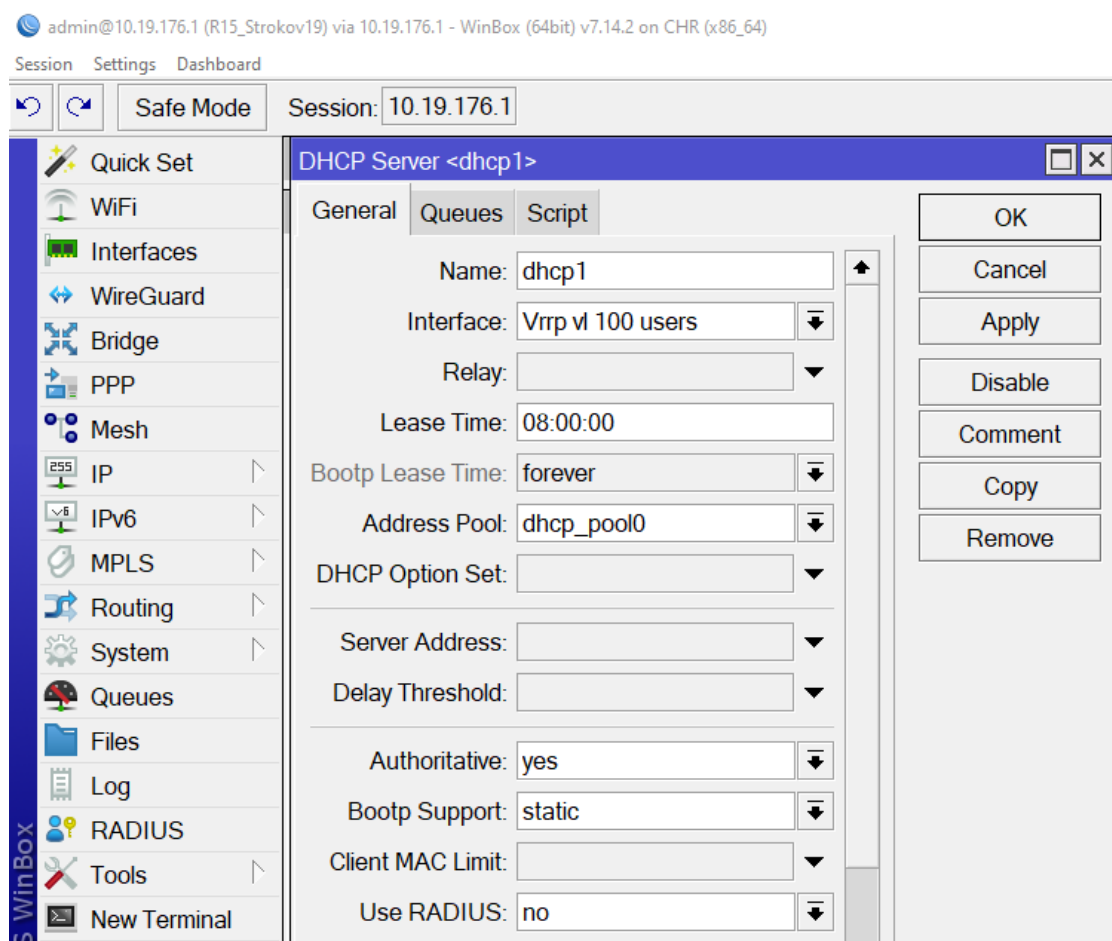


Рисунок 22 – Настройка роли DHCP сервера на маршрутизаторе R15

На остальных маршрутизаторах выполнены настройки по аналогии.

```
19_client1> dhcp
DORA IP 10.19.224.253/20 GW 10.19.224.1
```

Рисунок 23 – Получение адреса по DHCP

В качестве DNS сервера использовался dnsmasq на Debian 11.

```
debian@debian:~$ cat /etc/dnsmasq.conf
domain=strov19.up
expand-hosts
conf-dir=/etc/dnsmasq.d/,*.conf
interface=ens4
bind-interfaces
server=/ph2.strov19.up/10.19.144.10
server=/ph1.strov19.up/10.19.160.10
server=8.8.8.8
debian@debian:~$
```

Рисунок 24 – Настройка сервера пересылки и вторичных зон (филиалы)

```
debian@debian:~$ cat /etc/dnsmasq.d/config.conf
address=/dns0.strov19.up/10.19.176.10
address=/client1.strov19.up/10.19.224.30
address=/proxmox.strov19.up/10.19.176.100
address=/s1.strov19.up/10.19.176.4
address=/s2.strov19.up/10.19.176.5
address=/s3.strov19.up/10.19.176.6
address=/s4.strov19.up/10.19.176.7
address=/moadm.strov19.up/10.19.176.15
address=/client1.strov19.up/10.19.224.30
address=/r15.strov19.up/10.19.176.1
address=/redosadmin.strov19.up/10.19.176.70
debian@debian:~$
```

Рисунок 25 – Созданные А записи на сервере DNS в главном офисе

На других выполнены настройки по аналогии, в качестве адреса пересылки указан DNS сервер главного офиса

```
admStrov19> ping r15.strov19.up
r15.strov19.up resolved to 10.19.176.1

84 bytes from 10.19.176.1 icmp_seq=1 ttl=64 time=2.041 ms
84 bytes from 10.19.176.1 icmp_seq=2 ttl=64 time=1.342 ms
84 bytes from 10.19.176.1 icmp_seq=3 ttl=64 time=2.282 ms
84 bytes from 10.19.176.1 icmp_seq=4 ttl=64 time=1.468 ms
84 bytes from 10.19.176.1 icmp_seq=5 ttl=64 time=1.520 ms
```

Рисунок 26 – Проверка, что работает преобразование доменного имени

					УП.09.02.06.19Д	Лист
						22
Изм.	Лист	№ докум.	Подп.	Дата		

На рисунке 22 представлены настройки DHCP сервера на R15. На рисунке 23 видно, что хост успешно получил адрес по DHCP. На рисунке 24 показаны записи о используемых DNS серверах для получения нужных записей. Записи типа A, о хостах в главном офисе отображены на рисунке 25. Исходя из информации, показанной на рисунке 26, можно сделать вывод, что DNS сервер работает исправно.

### 3.2 Настройка туннелей и OSPF

Постановка задачи:

Для того, чтобы маршрутизаторы филиалов и главного офиса «узнали» про локальные сети друг друга, необходимо настроить туннелирование. Чтобы рассказать о сетях, нужно запустить OSPF, объявив о локальных сетях, и туннеле. Необходимо осуществить контроль трафика филиалов через главный офис, путем объявления маршрута по умолчанию в туннель к главному офису на маршрутизаторах филиалов.

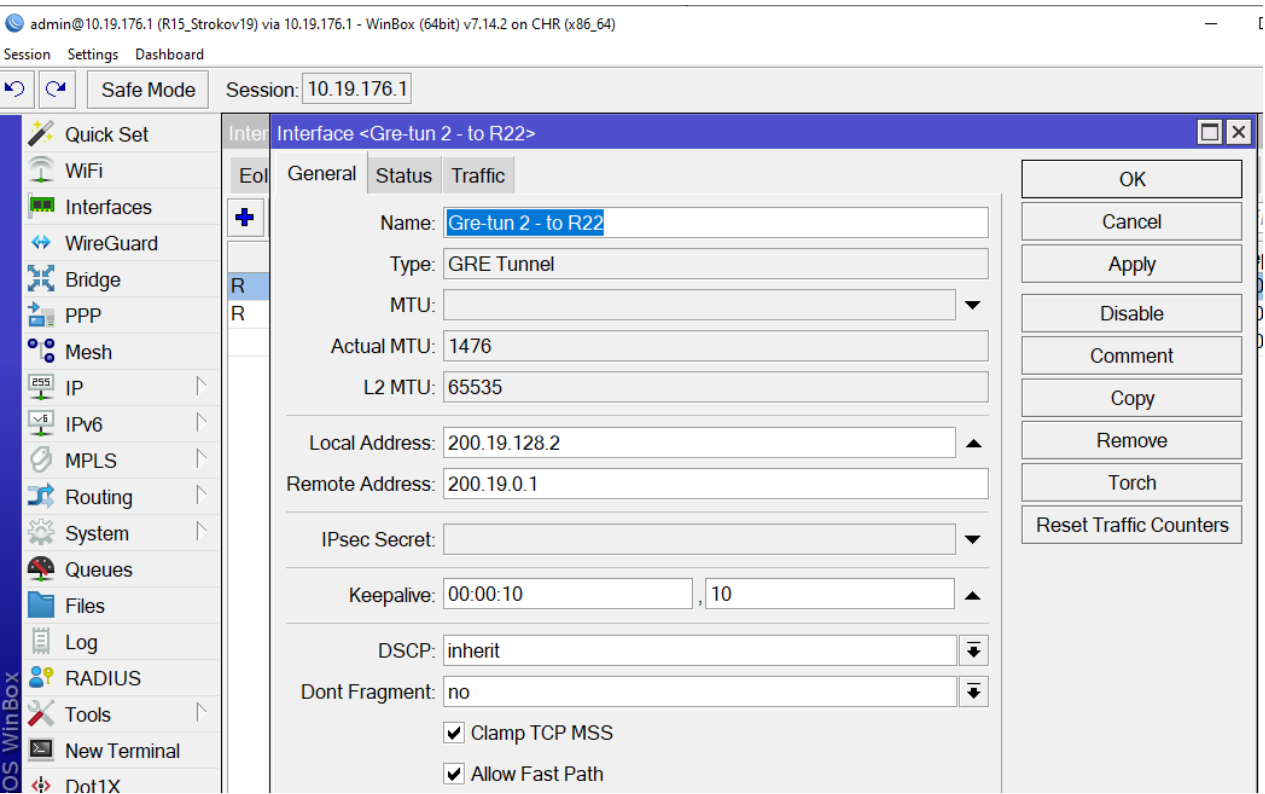


Рисунок 27 – Настройка GRE туннеля к R22

На R22 также настроен туннель к главному офису.

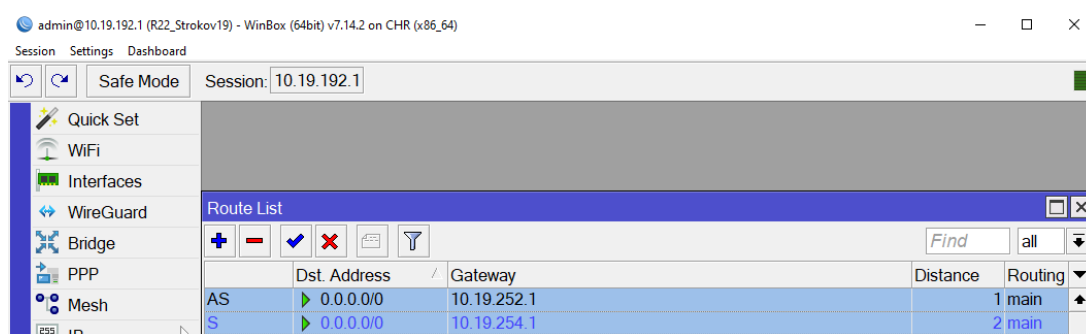


Рисунок 28 – Настройка маршрутов по умолчанию в сторону главного офиса

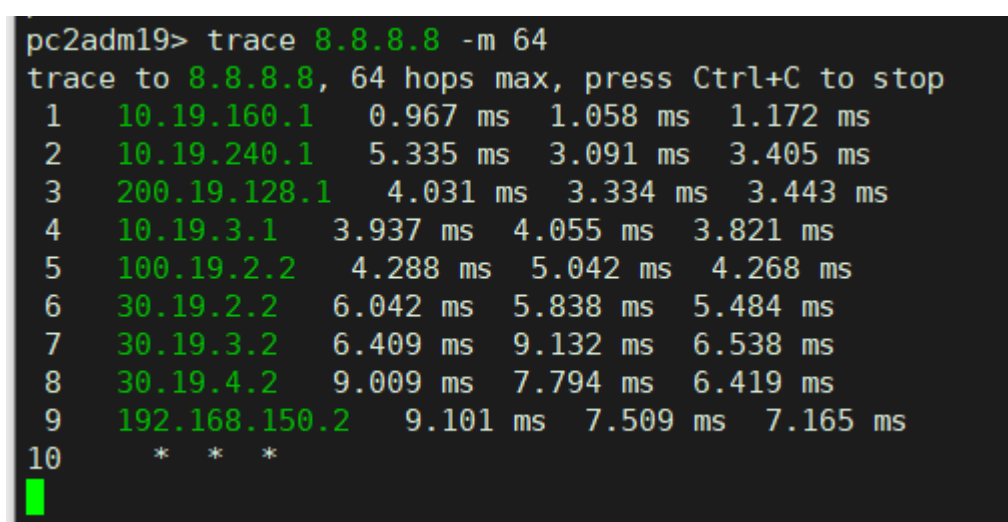


Рисунок 29 – Проверка, что трафик из филиала в интернет, проходит через главный офис предприятия

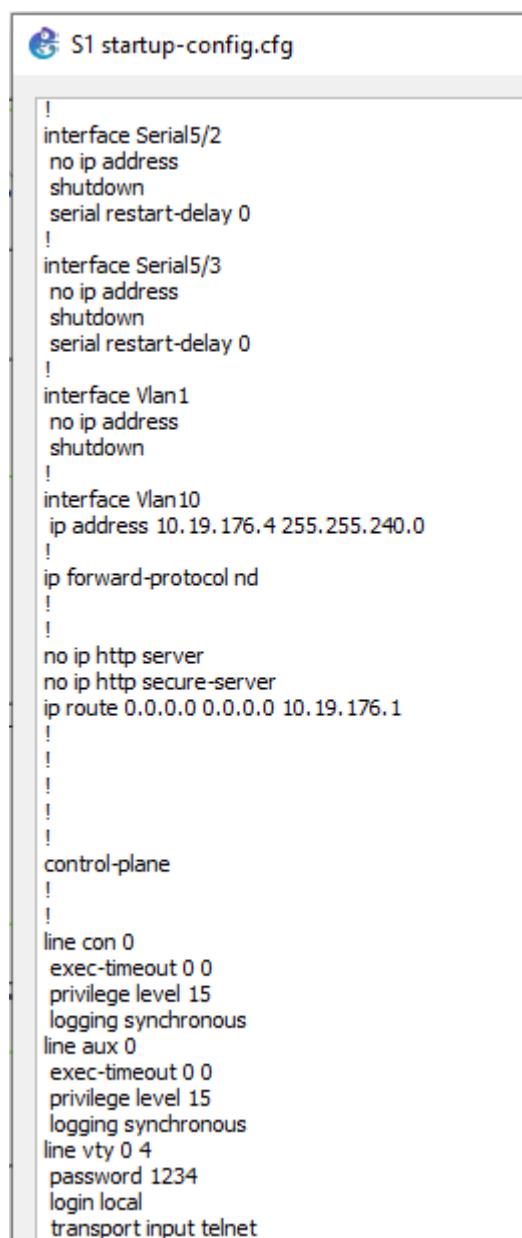
Благодаря настройкам, изображённым на рисунках 27 и 28, трафик из филиала 1 в интернет будет проходить через главный офис. На рисунке 29 можно убедиться, что это действительно так.



### 3.3 Удаленное администрирование

Постановка задачи:

На каждом сервере, коммутаторе и маршрутизаторе настроить возможность удаленного подключения по протоколу SSH или telnet только из главного офиса.



```
!
interface Serial5/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/3
no ip address
shutdown
serial restart-delay 0
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
ip address 10.19.176.4 255.255.240.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.19.176.1
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
password 1234
login local
transport input telnet
```

Рисунок 30 – Настройка S1 для удаленного подключения по telnet

Идентичные настройки выполнены на остальных коммутаторах.

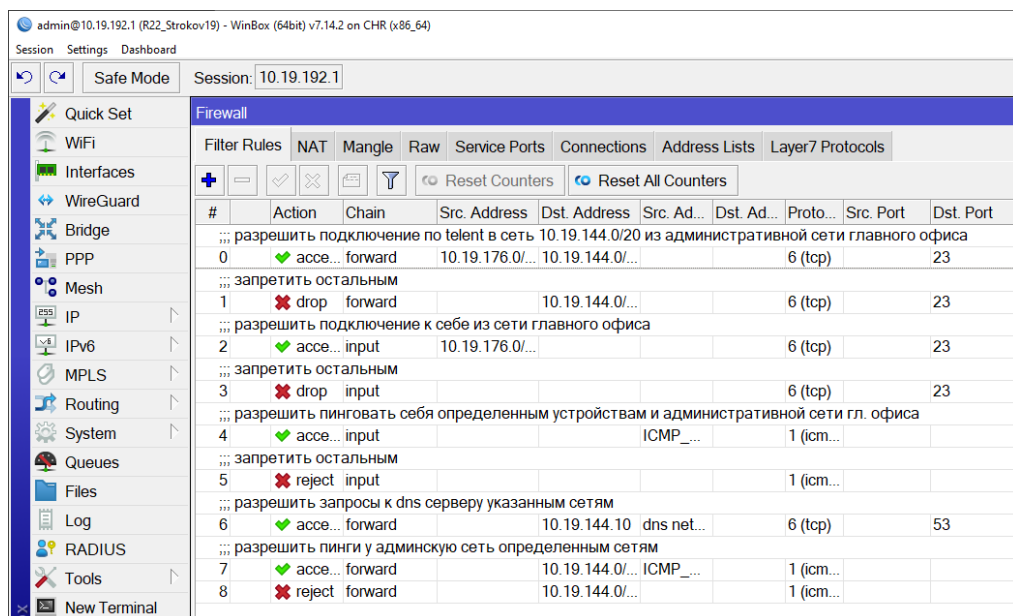


Рисунок 31 – Настройка правил Firewall на маршрутизаторе филиала 2

Идентично сконфигурированы правила файрволла на R19.

```

debian@debian:~$ telnet s5.ph1.strokov19.up
Trying 10.19.160.2...
Connected to s5.ph1.strokov19.up.
Escape character is '^]'.

User Access Verification

Password:
S5_Strokov19>en
Password:
S5_Strokov19#

```

Рисунок 32 – Проверка подключения по telnet с dns0 к S5

```

debian@debian:~$ telnet s5.ph1.strokov19.up
Trying 10.19.160.2...
telnet: Unable to connect to remote host: No route to host
debian@debian:~$

```

Рисунок 33 - Проверка подключения по telnet с dns1 к S5

По рисункам 32 и 33 можно понять, что правила успешно блокируют нежелательный трафик.

## 4 Модернизация сетевой инфраструктуры

### 4.1 Внедрение новых технологий

Постановка задачи:

Внедрить третий филиал, используя в качестве маршрутизатора Huawei, создав при этом простую локальную сеть.

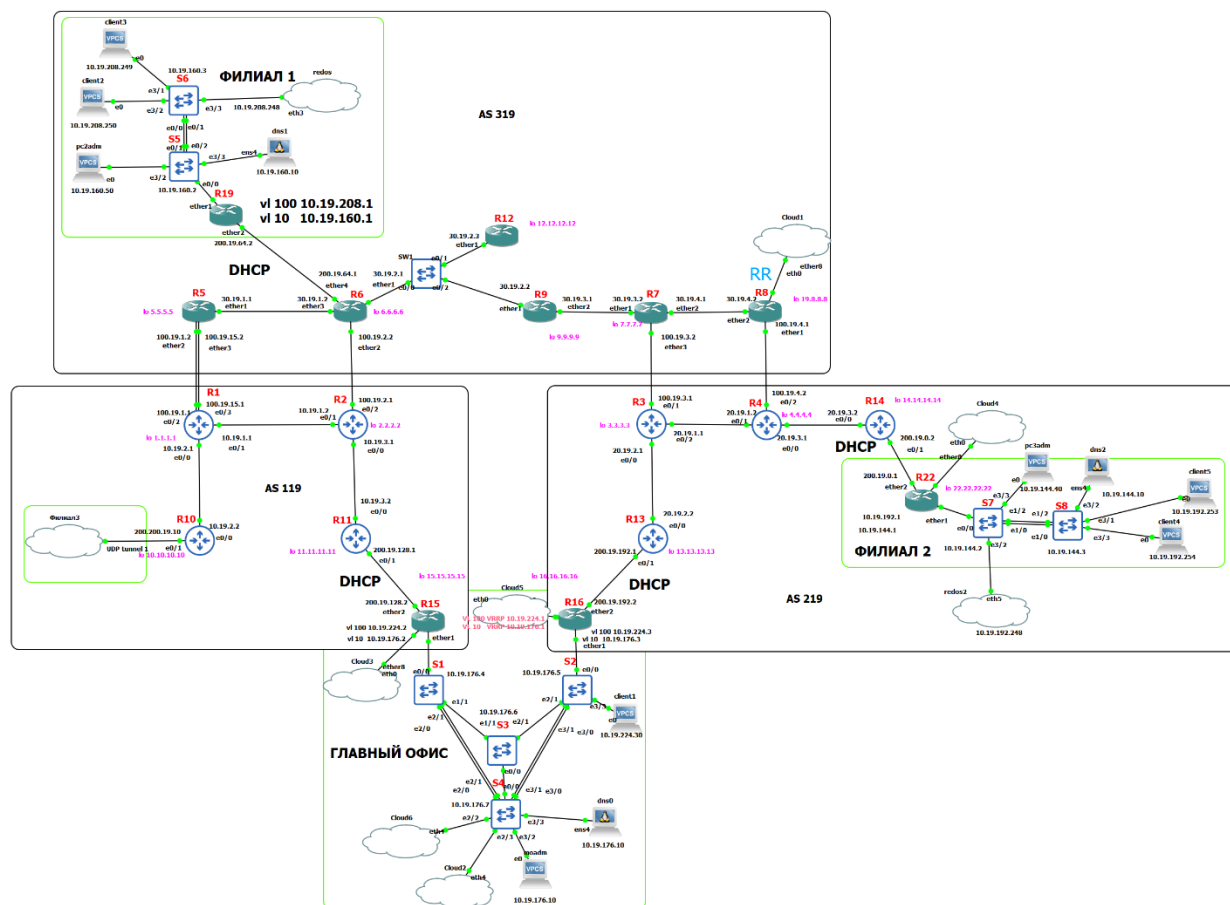


Рисунок 34 – Структура сети с двумя филиалами и главным офисом

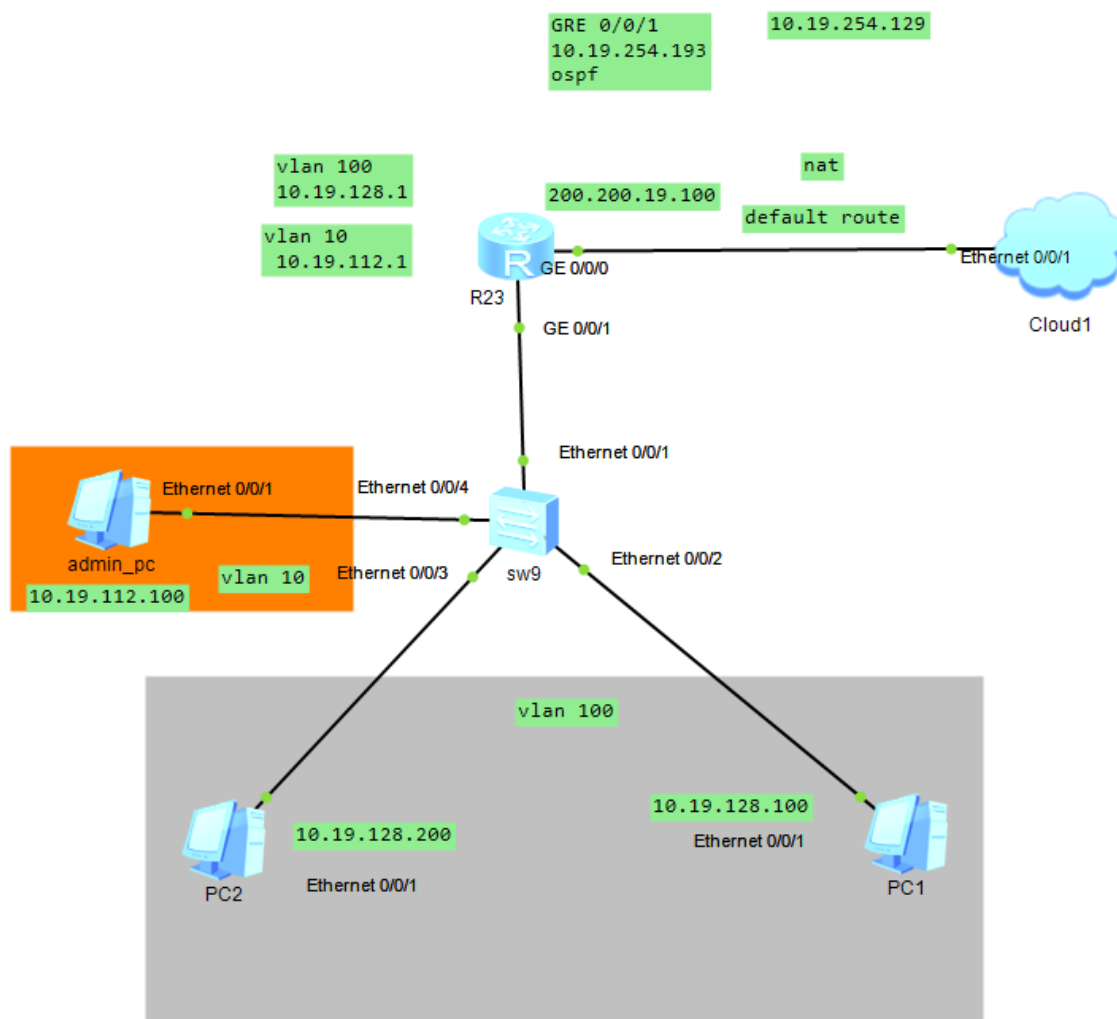


Рисунок 35 – Топология сети филиала с Huawei

```

<R23>display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 7
The number of interface that is DOWN in Physical is 1
The number of interface that is UP in Protocol is 6
The number of interface that is DOWN in Protocol is 2

Interface                               IP Address/Mask      Physical  Protocol
GigabitEthernet0/0/0                    200.200.19.100/24    up        up
GigabitEthernet0/0/1                    unassigned           up        down
GigabitEthernet0/0/1.10                 10.19.112.1/20       up        up
GigabitEthernet0/0/1.100               10.19.128.1/20       up        up
GigabitEthernet0/0/2                    unassigned           down      down
NULL0                                   unassigned           up        up(s)
Tunnel0/0/1                             10.19.254.193/30     up        up
Tunnel0/0/2                             10.19.254.129/30     up        up
<R23>

```

Рисунок 36 – Произведенные настройки Huawei

```

<R23>ping 8.8.8.8
  PING 8.8.8.8: 56 data bytes, press CTRL_C to break
    Reply from 8.8.8.8: bytes=56 Sequence=1 ttl=121 time=30 ms
    Reply from 8.8.8.8: bytes=56 Sequence=2 ttl=121 time=20 ms
    Reply from 8.8.8.8: bytes=56 Sequence=3 ttl=121 time=30 ms
    Reply from 8.8.8.8: bytes=56 Sequence=4 ttl=121 time=20 ms
    Reply from 8.8.8.8: bytes=56 Sequence=5 ttl=121 time=30 ms

--- 8.8.8.8 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 20/26/30 ms

```

Рисунок 37 – Проверка доступности интернета

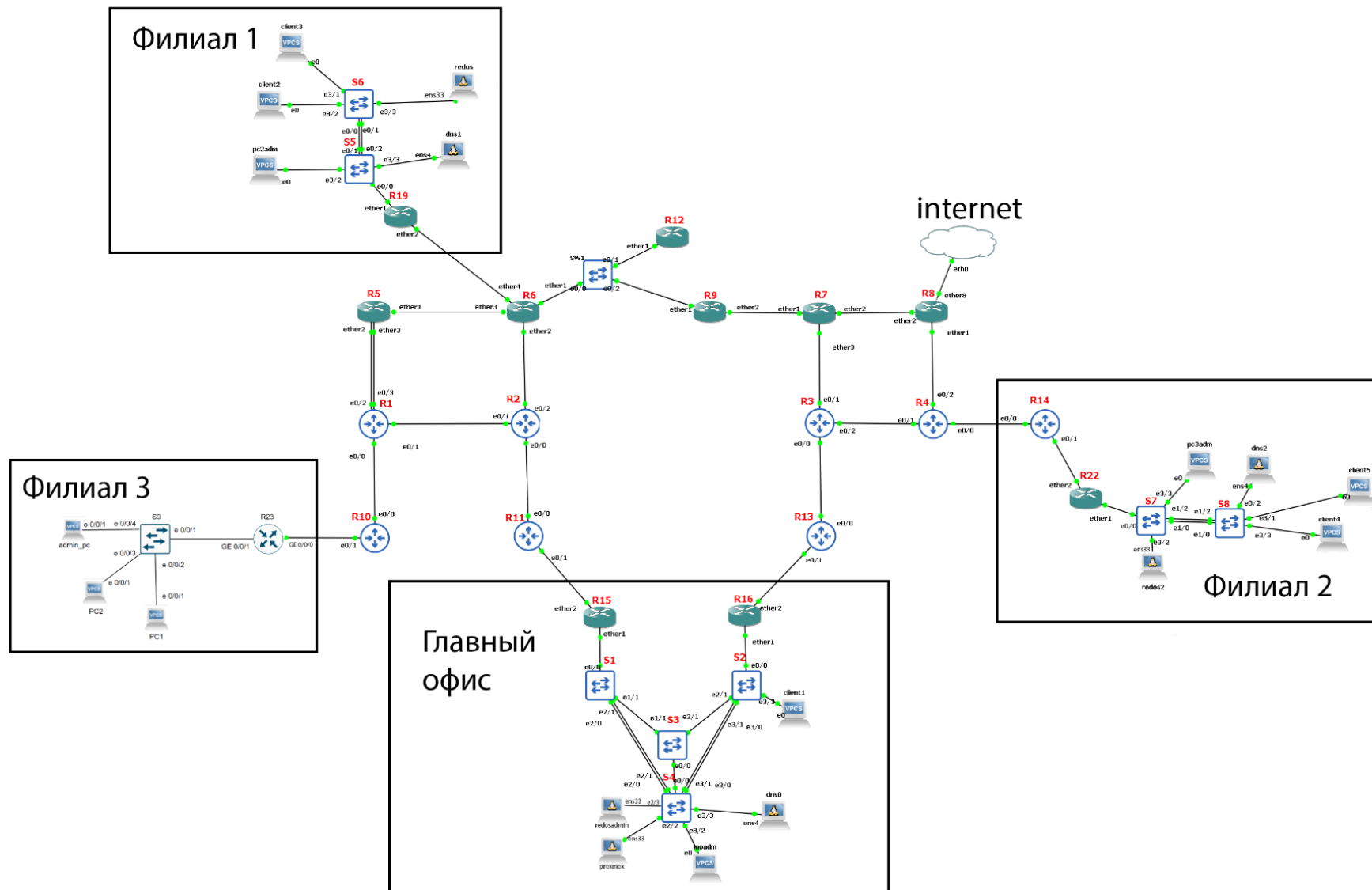
Исходя из рисунков 35-37 можно сделать вывод, об успешной модернизации инфраструктуры.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебное пособие / А. Г. Уймин. – Санкт-Петербург : Лань, 2020. – 480 с.
2. Таненбаум, Э., Уэзеролл, Д. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – 5-е изд. – Санкт-Петербург : Питер, 2013. – 960 с.
3. Дуглас Комер. Межсетевое взаимодействие / Дуглас Комер. – 2-е изд. – Москва : Вильямс, 2005. – 650 с.
4. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Профессиональное образование). — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/453065>
5. Ковган, Н.М. Компьютерные сети : учебное пособие / Н.М. Ковган. - Минск : РИПО, 2019. - 179 с. - ISBN 978-985-503-947-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1056320>

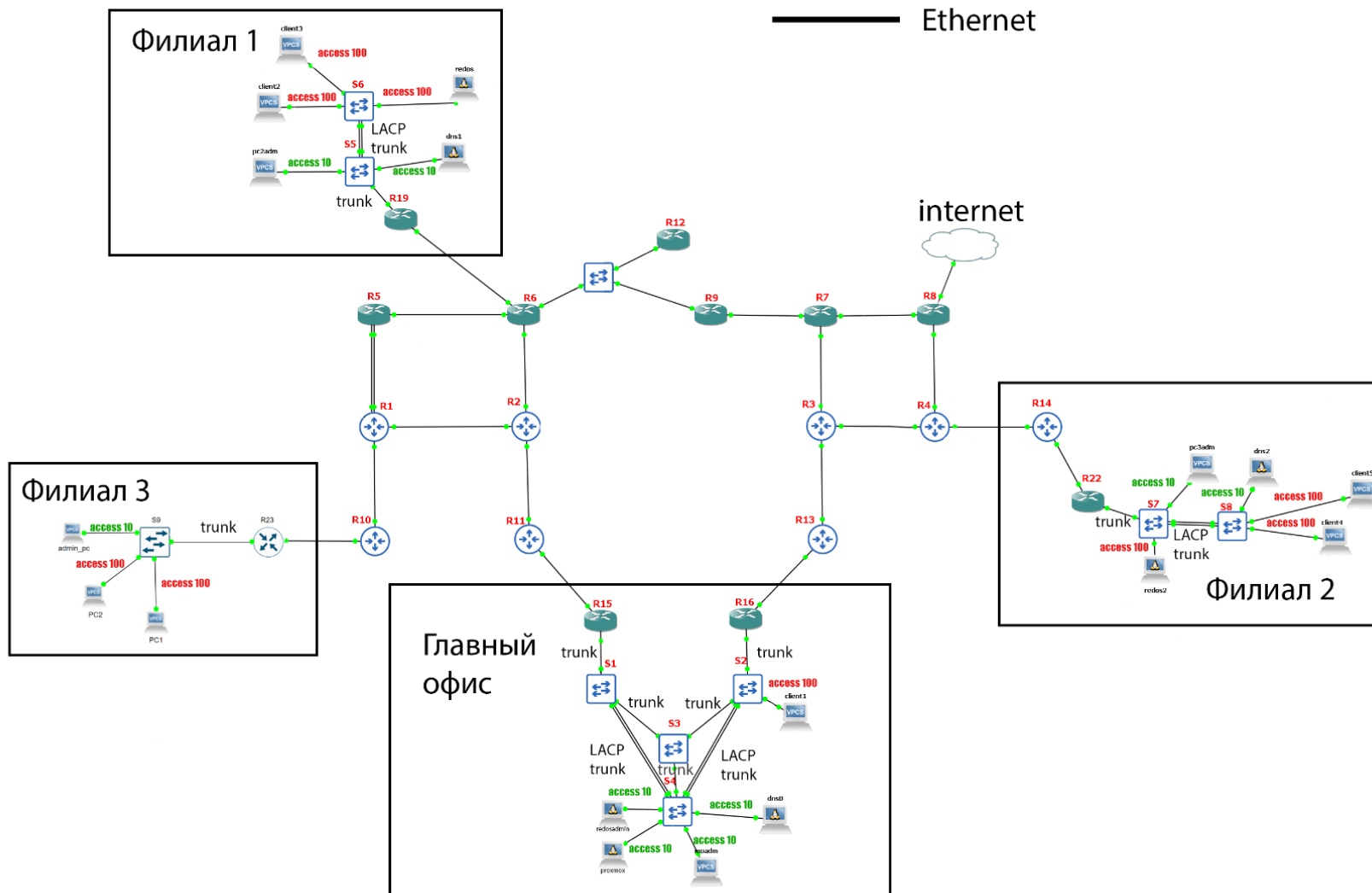
# ПРИЛОЖЕНИЕ А

## Схема L1



## ПРИЛОЖЕНИЕ Б

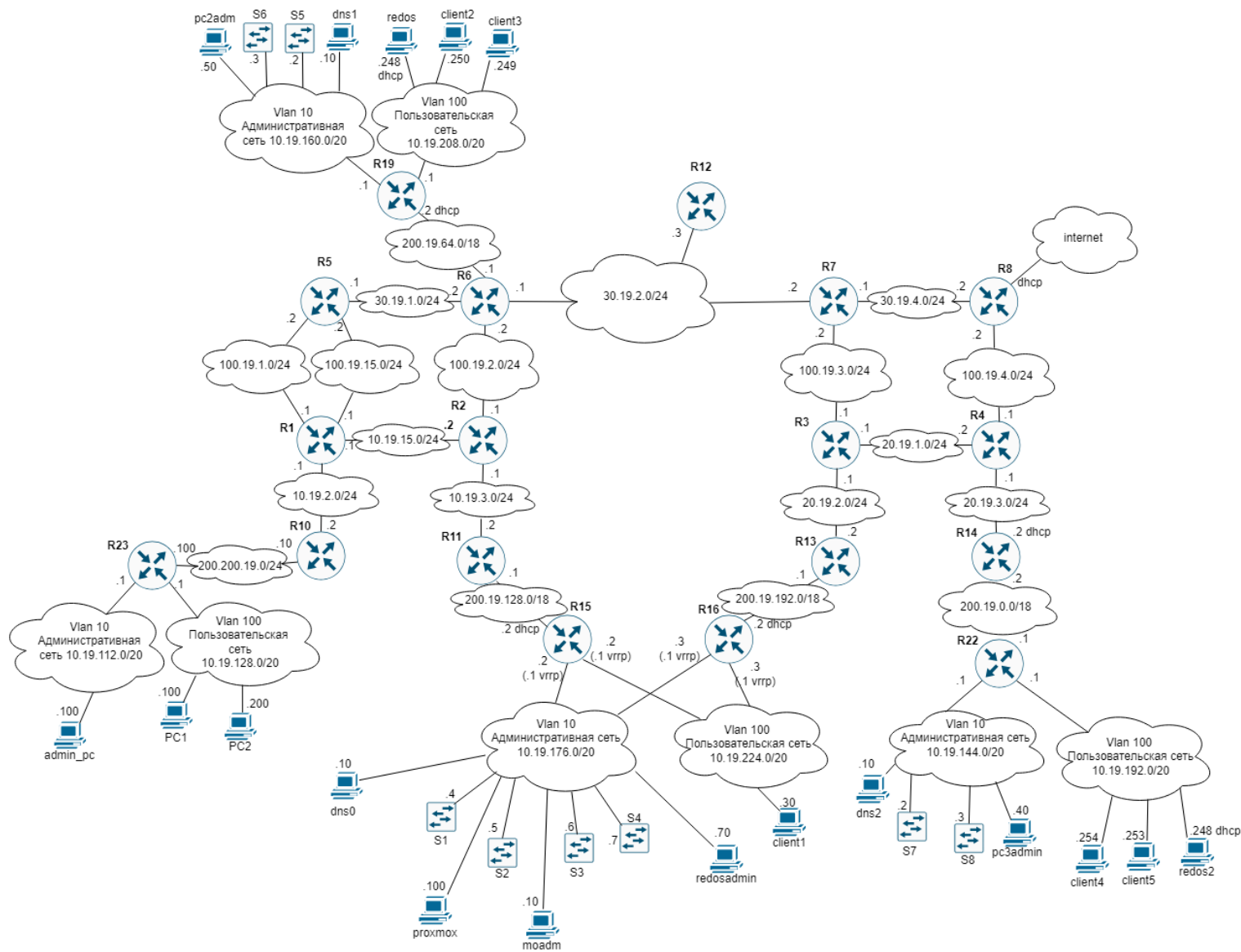
### Схема L2





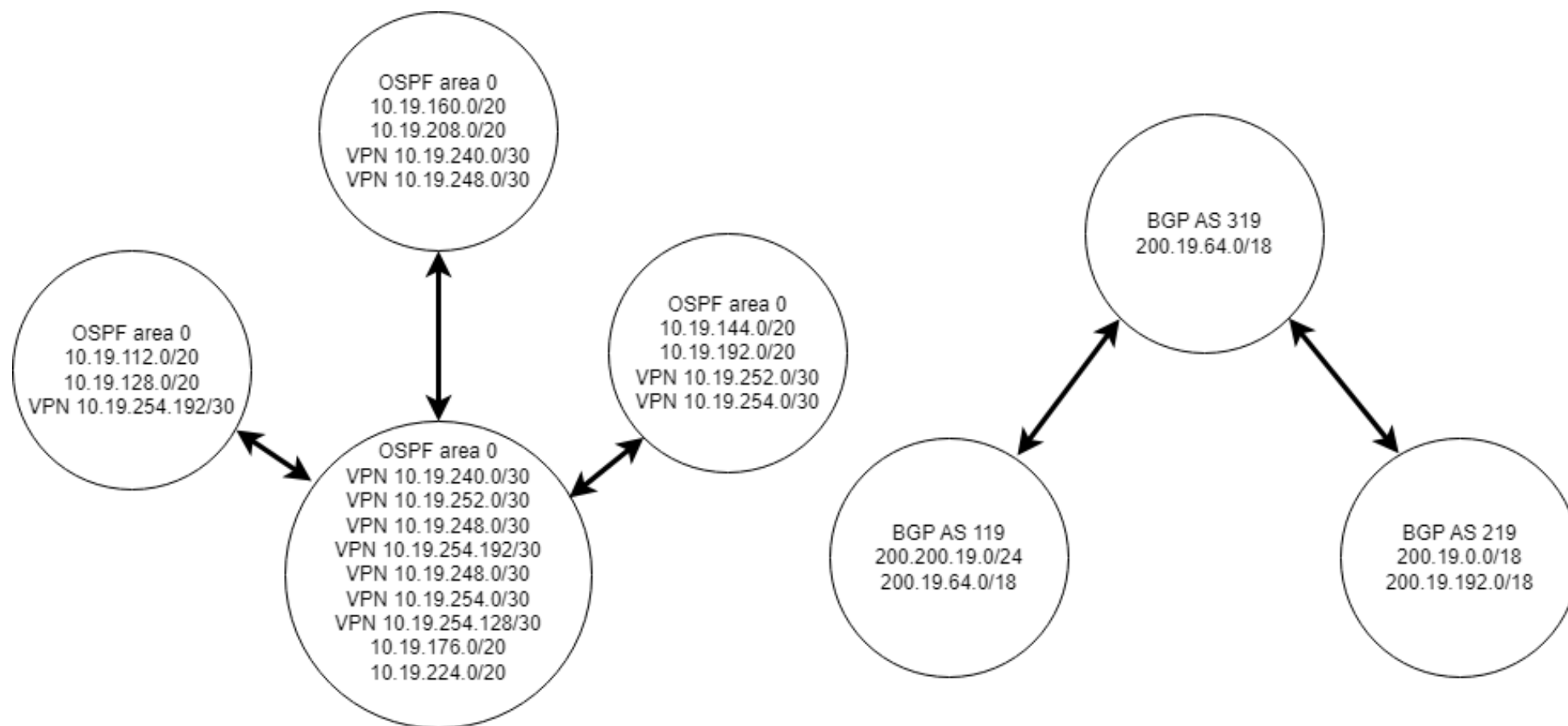
## ПРИЛОЖЕНИЕ В

### Схема L3



## ПРИЛОЖЕНИЕ Г

### Диаграмма маршрутизации



## ПРИЛОЖЕНИЕ Д

### Полученные подсети для использования

Внешние сети:	Исходная сеть	200.19.0.0/16							
1-я		200.19.0.0/18							
2-я		200.19.64.0/18							
3-я		200.19.128.0/18							
4-я		200.19.192.0/18							
сеть Huawei		200.200.19.0/24							
Локальные:	Исходная сеть	10.19.0.0/16							
1-я		10.19.0.0/20	✓	0000					
2-я		10.19.16.0/20	✓	0001					
3-я		10.19.32.0/20	✓	0010					
4-я		10.19.48.0/20	✓	0011					
5-я		10.19.64.0/20	✓	0100					
6-я		10.19.80.0/20	✓	0101					
7-я		10.19.96.0/20	✓	0110					
8-я		10.19.112.0/20	✓	0111	Третий филиал административная сеть	vlan 10			
9-я		10.19.128.0/20		1000	Третий филиал локальная сеть	vlan 10			
10-я		10.19.144.0/20		1001	Второй филиал административная сеть	vlan 10			
11-я		10.19.160.0/20		1010	Первый филиал административная сеть	vlan 10			
12-я		10.19.176.0/20		1011	административная сеть в главном офисе	vlan 10			
13-я		10.19.192.0/20		1100	Второй филиал локальная сеть	vlan 100			
14-я		10.19.208.0/20		1101	Первый филиал локальная сеть	vlan 100			
15-я		10.19.224.0/20		1110	Главный филиал локальная сеть	vlan 100			
16-я		10.19.240.0/20		1111	10.19.240.0/30	Для GRE от R15 от до R19			
					10.19.248.0/30	Для GRE от R16 от до R19			
					10.19.252.0/30	Для GRE от R15 от до R22			
					10.19.254.0/30	Для GRE от R16 от до R22			
					10.19.254.192/30	Для GRE от R23 до R15			
					10.19.254.128/30	Для GRE от R23 до R16			