

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

ОТЧЕТ ПО УЧЕБНОЙ ПРАКТИКЕ

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

ОТЧЕТ ВЫПОЛНИЛ

Студент группы	С142		П.А. Бондарчук
	номер группы	_____ подпись, дата	_____ инициалы, фамилия

Санкт-Петербург 2024

Аттестационный лист по учебной практике

Бондарчук Павел Антонович

(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.

Руководитель практики от факультета СПО _____ Попов И.Д.
подпись

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

на прохождение учебной практики обучающегося по специальности
09.02.06 Сетевое и системное администрирование

код и наименование специальности

1. Фамилия, имя, отчество обучающегося: Иванов Иван Иванович
2. Группа: С142 Сроки проведения практики: с «06» апреля 2024 г. по «26» апреля 2024 г.
3. Тема задания: приобретение первичных профессиональных умений и навыков, начального опыта практической деятельности, овладение необходимыми компетенциями по профессиональному модулю.

ПМ.01 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОЕКТИРОВАНИЮ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

код и наименование профессионального модуля

4. Вопросы, подлежащие изучению:
 - 1) Проектирование сетевой инфраструктуры.
 - 2) Организация сетевого администрирования.
 - 3) Управление сетевыми сервисами.
 - 4) Модернизация сетевой инфраструктуры.
5. Выполнение комплексных работ по проектированию архитектуры локальной сети; установке и настройке сетевых протоколов и сетевого оборудования; использованию специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей; настройке механизмов фильтрации трафика на базе списков контроля доступа.
6. Содержание отчетной документации:
 - 6.1.1. Отчёт, включающий в себя:
 - титульный лист;
 - индивидуальное задание;
 - материалы о выполнении индивидуального задания;
 - список использованных источников.
 - 6.1.2. Аттестационный лист.
7. Срок представления отчета заместителю декана по учебно-производственной работе: «26» апреля 2024 г.

Руководитель практики от факультета СПО

преподаватель

должность, уч. степень, звание



подпись, дата

06.04.2024 г.

И.Д. Попов

инициалы, фамилия

Задание принял к исполнению:

Обучающийся

06.04.2024 г.



подпись

П.А. Бондарчук

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	6
1 Проектирование сетевой инфраструктуры	7
1.1 Изучение предметной области	7
1.2 IP-план и схемы сети	11
2 Организация сетевого администрирования.....	13
2.1 Выполнение настроек VLAN, агрегирования и VRRP в филиалах. ..	14
2.2 Настройка выхода в Интернет с использованием NAT и port forwarding.....	18
2.3 Настройка файлового сервера.....	23
3 Управление сетевыми сервисами.	26
3.1 Настройка DHCP-сервера.	26
3.2 Настройка туннелирования и OSPF между GRE.....	27
3.3 Настройка кеширующих DNS-серверов.	32
3.4 Настройка telnet и файрволла.	34
4 Модернизация сетевой инфраструктуры.	39
Источники	47
ПРИЛОЖЕНИЕ А.....	48
ПРИЛОЖЕНИЕ Б.....	49
ПРИЛОЖЕНИЕ В.....	50
ПРИЛОЖЕНИЕ Г.....	51

					УП.09.02.06.02ПЗ			
Изм.	Лист	№ докум.	Подп.	Дата				
Разраб.		Бондарчук П. А.			Отчет по учебной практике		Лит.	Лист
Пров.		Попов И. Д.						4
							ФСПО ГУАП	
Н. контр.								
Утв.								

ВВЕДЕНИЕ

Я, Бондарчук Павел Антонович, являюсь студентом третьего курса Факультета среднего профессионального образования Государственного университета аэрокосмического приборостроения (ГУАП) и проходил учебную практику по профессиональному модулю ПМ.01 «Выполнение работ по проектированию сетевой инфраструктуры». Целью моего проекта стало создание сетевой инфраструктуры для городской библиотеки, включающей в себя три филиала, включая главный офис, а также провайдерскую сеть с тремя автономными системами.

В современных условиях ключевым требованием к библиотекам является наличие эффективной сетевой инфраструктуры. Библиотеки оперируют большими объемами данных, включая каталоги книг, реестры читателей и операции по выдаче и возврату литературы. Надлежащая сетевая инфраструктура обеспечивает быстрый и точный доступ к этой информации, минимизируя задержки и ошибки, что в свою очередь обеспечивает эффективную работу библиотеки и удовлетворение потребностей посетителей.

При разработке инфраструктуры учтены различные факторы, включая отказоустойчивость и наличие файлового сервера для хранения всей доступной литературы. Также была решена задача обеспечения доступа к глобальной интернет-сети для всех пользователей. В одном из филиалов предусмотрена точка доступа Wi-Fi с использованием технологии HotSpot на оборудовании MikroTik. Это позволяет гостям библиотеки регистрироваться в сети, используя логин и пароль, а также перенаправляться на рекламную страницу учреждения.

					УП.09.02.06.02ПД	Лист
						6
Изм.	Лист	№ докум.	Подп.	Дата		

1 Проектирование сетевой инфраструктуры

Цели и задачи:

- спроектировать отказоустойчивую сеть в организации, состоящей из главного офиса из нескольких филиалов;
- выбрать оборудование, технологии и протоколы;
- объединить удаленные сети с помощью технологии VPN (можно незащищенную);
- построить схемы L1, L2, L3 и IP-план;

Используемое оборудование, инструменты, программное обеспечение:

- Visio/Diagrams.net;
- калькулятор IP;
- редактор таблиц.

Последовательность выполнения и описание действий:

1.1 Изучение предметной области

Предметной областью моего курсового проекта является библиотека.

Определение количества филиалов для библиотеки— это стратегически важный шаг, который должен соответствовать не только текущим потребностям, но и будущим перспективам развития. В данном контексте было принято решение о создании двух филиалов и одного главного офиса по следующим причинам:

Оптимизация распределения ресурсов: имея два филиала и главный офис, мы можем оптимально распределить ресурсы и управлять коллекцией книг и другими материалами. Это позволяет обеспечить максимальную доступность к литературным ресурсам для читателей в разных частях города или района.

Улучшение обслуживания посетителей: распределение библиотечных услуг между филиалами и главным офисом позволяет сократить время ожидания для посетителей и улучшить качество обслуживания. Это особенно актуально для студентов и исследователей, которым может потребоваться

					УП.09.02.06.02ПД	Лист
						7
Изм.	Лист	№ докум.	Подп.	Дата		

доступ к специализированным материалам.

Гибкость и масштабируемость: имея два филиала, мы создаем систему, которая может легко масштабироваться и адаптироваться к изменяющимся потребностям и условиям. Это позволяет быстро реагировать на изменения в библиотечных коллекциях и повышать уровень обслуживания читателей.

Эффективное управление: ограниченное количество филиалов упрощает управление библиотечной системой, позволяя быстрее и эффективнее принимать решения и координировать деятельность между различными частями учреждения.

Экономическая выгода: оптимальное количество филиалов позволяет снизить операционные расходы без ущерба для качества обслуживания. Это особенно важно для муниципальных и региональных библиотек, где финансовые ресурсы могут быть ограничены.

Таким образом, использование двух филиалов и одного главного офиса представляется наиболее эффективным и перспективным решением для организации современной библиотечной системы, обеспечивая высокий уровень доступности, качества обслуживания и управляемости учреждения.

Выбор технологий и протоколов для сетевой инфраструктуры библиотеки основывается на нескольких ключевых принципах, включая надежность, масштабируемость, безопасность и эффективность управления ресурсами. Рассмотрим подробнее примененные решения:

GRE туннели и OSPF протокол:

Надежность и масштабируемость: использование GRE туннелей и OSPF протокола обеспечивает надежное и масштабируемое соединение между филиалами. Это позволяет эффективно управлять трафиком и обеспечивать высокую доступность сетевых ресурсов.

Маршрутизация между VLAN в филиалах:

Безопасность и гибкость: настройка маршрутизации между VLAN позволяет разделять сетевой трафик на клиентскую и административную части, обеспечивая более гибкие возможности по настройке безопасности и

					УП.09.02.06.02ПД	Лист
						8
Изм.	Лист	№ докум.	Подп.	Дата		

контроля доступа в будущем.

DNCP-сервер:

Эффективность и автоматизация: использование DNCP-сервера для выдачи адресов в филиалах упрощает процесс управления сетевыми настройками и обеспечивает автоматическую конфигурацию клиентских устройств.

Двойное подключение к провайдерам и VRRP:

Надежность и высокая доступность: каждый филиал подключен сразу к двум провайдерам и роутеры получают глобальные IPv4 адреса от DNCP-серверов в провайдерской сети. Двойное подключение к провайдерам и использование VRRP адресов обеспечивает высокую доступность интернет-соединения и надежную работу локальной сети в филиалах.

Кеширующие DNS сервера и введение в домен Bondarchuk2.up:

Быстродействие и идентификация: настройка кеширующих DNS серверов позволяет ускорить процесс разрешения доменных имен и интегрировать организацию в доменное имя Bondarchuk2.up, обеспечивая единое идентификационное пространство для всех сотрудников и посетителей.

WI-FI точка доступа на Mikrotik с HotSpot технологией:

Удобство и безопасность: установка WI-FI точки доступа с технологией HotSpot на Mikrotik обеспечивает удобный и безопасный доступ к интернету для посетителей, требуя аутентификации и предоставляя возможность перехода на рекламную страницу библиотеки.

FTP файловый сервер в главном офисе для хранения литературы:

Централизация и удобство доступа: введение FTP файлового сервера для хранения всей литературы библиотеки обеспечивает централизованное и надежное хранение ресурсов. Это упрощает процесс управления и обновлениями коллекции книг, журналов и других материалов, а также обеспечивает удобный доступ к литературным ресурсам для сотрудников и посетителей библиотеки, улучшая эффективность и качество обслуживания

					УП.09.02.06.02ПД	Лист
						9
Изм.	Лист	№ докум.	Подп.	Дата		

пользователей.

Таким образом, выбранные технологии и протоколы обеспечивают комплексное решение для современной библиотечной сети, сочетая в себе высокую надежность, эффективность управления, гибкость настройки безопасности и удобство использования для сотрудников и посетителей.

Примерная схема сети, спроектированная в программе draw.io, изображена на рисунке 1.

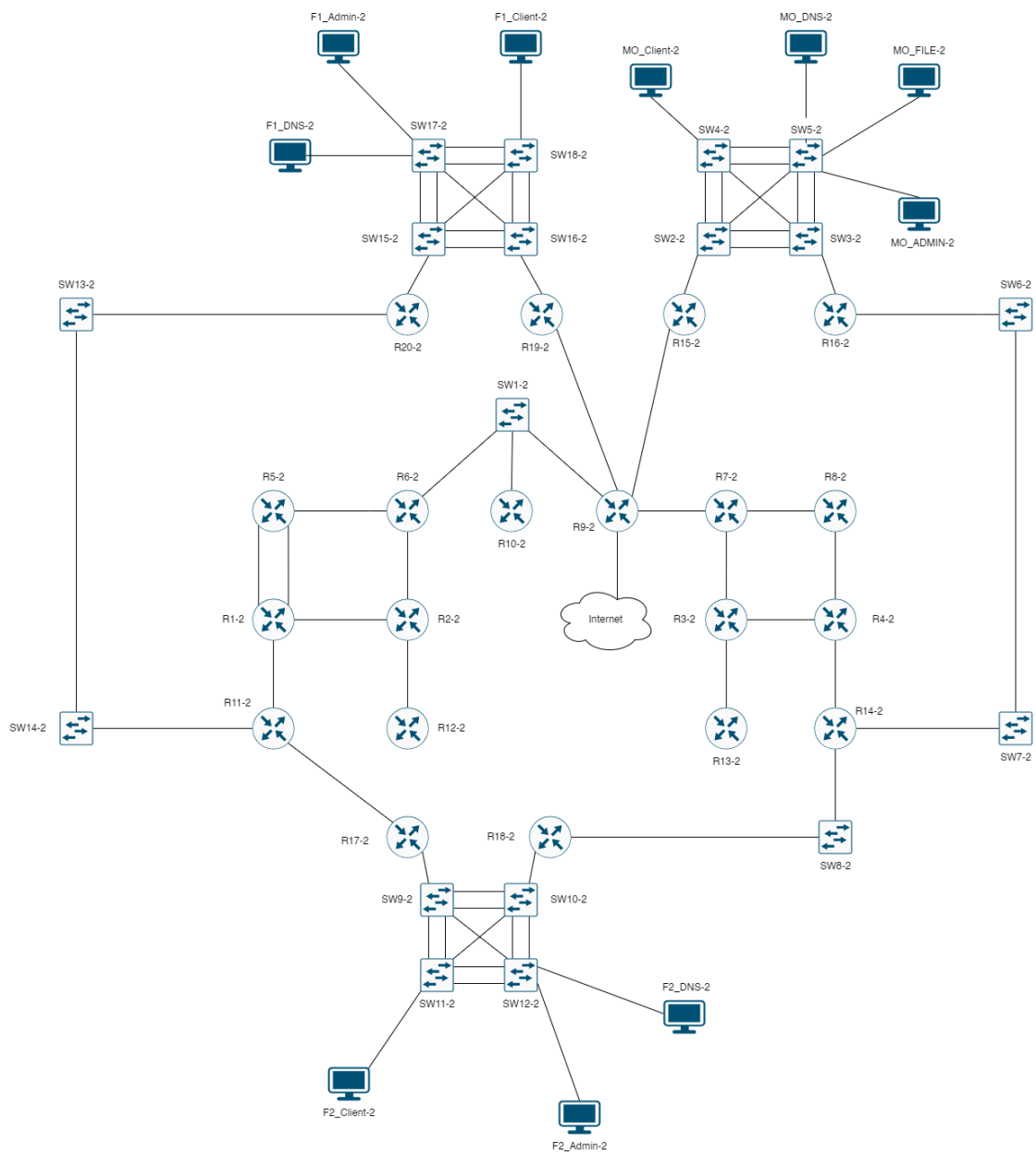


Рисунок 1 – Примерная схема сети

1.2 IP-план и схемы сети

Схема сети L1 показана в приложении А.

Схема сети L2 показана в приложении Б.

Схема сети L3 показана в приложении В.

Диаграмма маршрутизации показана в приложении Г.

Далее приведены IP-планы филиалов:

В таблице 1 показан IP-план главного офиса.

Таблица 1 – IP-план главного офиса

Главный офис			
Оборудование	Интерфейс	IP-адрес	Маска
Mikrotik 7.14.2 (R15-2)	ether0	DHCP (200.2.1.254)	24
	ether1 (vlan 301)	10.2.4.10	24
	ether1 (vlan 302)	10.2.5.2	24
	vrrp301	10.2.4.1	24
	vrrp302	10.2.5.1	24
	lo	2.15.15.15	32
	GRE_to_R17	175.2.175.15	24
	GRE_to_R18	185.2.185.15	24
	GRE_to_R19	195.2.195.15	24
	GRE_to_R20	215.2.215.15	24
Mikrotik 7.14.2 (R16-2)	lo	2.16.16.16	32
	vrrp301	10.2.4.1	24
	ether1 (vlan301)	10.2.4.20	24
	vrrp302	10.2.5.1	24
	ether1 (vlan 302)	10.2.5.3	24
	GRE_to_R17	176.2.176.16	24
	GRE_to_R18	186.2.186.16	24
	GRE_to_R19	196.2.196.16	24
	GRE_to_R20	216.2.216.16	24
	ether0	DHCP (200.2.2.254)	24
MO_Client-2	ens32	DHCP (10.2.5.240)	24
MO_DNS-2	ens4	10.2.4.150	24
MO_File-2	ens32	DHCP (10.2.4.101)	24
MO_Admin-2	ens4	DHCP (10.2.4.102)	24
SW2-2	vlan 301	10.2.4.2	24
SW3-2	vlan 301	10.2.4.3	24
SW4-2	vlan 301	10.2.4.4	24
SW5-2	vlan 301	10.2.4.5	24

В таблице 2 показан IP-план филиала №1.

Таблица 2 – IP-план филиала 1

Филиал 1			
Оборудование	Интерфейс	IP-адрес	Маска
Mikrotik 7.14.2 (R19-2)	ether0	DHCP (200.2.5.254)	24
	ether1 (vlan 101)	10.2.6.3	24
	ether1 (vlan 102)	10.2.7.3	24
	vrrp101	10.2.6.1	24
	vrrp102	10.2.7.1	24
	lo	2.19.19.19	32
	GRE_to_R15	195.2.195.19	24
	GRE_to_R16	196.2.196.19	24
Mikrotik 7.14.2 (R20-2)	ether0	DHCP (200.2.6.254)	24
	ether1 (vlan 101)	10.2.6.2	24
	ether1 (vlan 102)	10.2.7.2	24
	vrrp101	10.2.6.1	24
	vrrp102	10.2.7.1	24
	lo	2.20.20.20	32
	GRE_to_R15	215.2.215.20	24
	GRE_to_R16	216.2.216.20	24
F1_DNS-2	ens4	10.2.6.150	24
F1_Admin-2	ens4	DHCP (10.2.6.100)	24
F1_Client-2	ens32	DHCP (10.2.7.190)	24
SW15-2	vlan 101	10.2.6.15	24
SW16-2	vlan 101	10.2.6.16	24
SW17-2	vlan 101	10.2.6.17	24
SW18-2	vlan 101	10.2.6.18	24

В таблице 3 показан IP-план филиала №2.

Таблица 3 – IP-план филиала 2

Филиал 2			
Оборудование	Интерфейс	IP-адрес	Маска
Mikrotik 7.14.2 (R17-2)	ether0	DHCP (200.2.3.254)	24
	ether1 (vlan 201)	10.2.8.2	24
	ether1 (vlan 202)	10.2.9.2	24
	vrrp201	10.2.8.1	24
	vrrp202	10.2.9.1	24
	lo	2.17.17.17	32
	GRE_to_R15	175.2.175.17	24
	GRE_to_R16	176.2.176.17	24

Продолжение таблицы 3

Mikrotik 7.14.2 (R18-2)	ether0	DHCP (200.2.4.254)	24
	ether1 (vlan 201)	10.2.8.3	24
	ether1 (vlan 202)	10.2.9.3	24
	vrrp201	10.2.8.1	24
	vrrp202	10.2.9.1	24
	lo	2.18.18.18	32
	GRE_to_R15	185.2.185.18	24
	GRE_to_R16	186.2.186.18	24
F2_DNS-2	ens4	10.2.8.150	24
F2_Admin-2	ens4	DHCP (10.2.8.100)	24
F2_Client-2	ens32	DHCP (10.2.9.239)	24
SW9-2	vlan 201	10.2.8.9	24
SW10-2	vlan 201	10.2.8.10	24
SW11-2	vlan 201	10.2.8.11	24
SW12-2	vlan 201	10.2.8.12	24

2 Организация сетевого администрирования.

Цели и задачи:

- настроить коммутацию, резервные каналы, маршрутизацию;
- настроить выход в Интернет;
- настроить механизмы безопасности;
- проверить работоспособность выполненных настроек.

Используемое оборудование, инструменты, программное обеспечение:

- VMware/VirtualBox;
- GNS3/EVE-NG/eNSP;
- образы маршрутизаторов, коммутаторов;
- PuTTY/SuperPuTTY/Xshell/т.п.;
- Debian, Alpine, RedOS в качестве серверов и конечных устройств.

Последовательность выполнения и описание действий:

2.1 Выполнение настроек VLAN, агрегирования и VRRP в филиалах.

В каждом филиале была произведена настройка VLAN. Один VLAN создавался для административной сети и сетевых устройств, другой для клиентской подсети. Маршрутизация между VLAN была произведена с помощью метода Router-on-a-stick. Также коммутаторам тоже были заданы IP-адреса на VLAN-интерфейсы и на них был настроен маршрут по умолчанию на административный адрес VRRP, который делят между собой два роутера. Пример настройки VLAN, агрегирования и VRRP в главном офисе продемонстрирован ниже.

Административный VLAN в главном офисе – 301.

Клиентский VLAN в главном офисе – 302.

На рисунке 2 продемонстрировано объявление VLAN'ов на коммутаторе SW2-2:

```
SW2#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Et1/3, Et2/0, Et2/1, Et2/2
                                Et2/3, Et3/0, Et3/1, Et3/2
                                Et3/3
301  vlan301                 active
302  vlan302                 active    Et1/2
1002 fddi-default            act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup
```

Рисунок 2 – Объявленные VLAN на SW2-2

На рисунке 3 продемонстрирована настройка ip-адреса на vlan-интерфейсе коммутатора SW2-2 и настройка маршрута по умолчанию:

```

!
interface Vlan301
ip address 10.2.4.2 255.255.255.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.2.4.1

```

Рисунок 3 – Назначенный маршрут и IP-адрес

На рисунке 4 продемонстрирована настройка access и trunk портов и выполненное агрегирование с помощью PAGP и LACP на коммутаторе SW2-2.

```

!
interface Port-channel1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Port-channel2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
channel-protocol pagp
channel-group 2 mode desirable
!
interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
channel-protocol pagp
channel-group 2 mode desirable
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode on
!
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode on
!
interface Ethernet1/1
switchport trunk encapsulation dot1q
!
interface Ethernet1/2
switchport access vlan 302
switchport mode access
!

```

Рисунок 4 – Настройка access, trunk портов и агрегирования

					УП.09.02.06.02ПД	Лист
						15
Изм.	Лист	№ докум.	Подп.	Дата		

Настройка VRRP на R15 (RM) для vlan 301 показана на рисунке 5.

Рисунок 5 – Настройка VRRP для VLAN 301 на R15 (RM)

Настройка VRRP на R15 (RM) для vlan 302 показана на рисунке 6.

Рисунок 6 – Настройка VRRP для VLAN 302 на R15 (RM)

Настройка VRRP на R16 (B) для vlan 301 показана на рисунке 7.

Рисунок 7 – Настройка VRRP для VLAN 301 на R16 (B)

Настройка VRRP на R16 (B) для vlan 302 показана на рисунке 8.

Рисунок 8 – Настройка VRRP для VLAN 302 на R16 (B)

На рисунках выше была продемонстрирована примерная настройка VLAN, агрегирования и VRRP в главном филиале. В остальных филиалах настройка производится аналогичным образом. В результате настройки у нас должно получиться так, что для каждого VLAN (административного и клиентского) будет создан VLAN-интерфейс на роутере. На этих интерфейсах будет назначен адрес из сети необходимого VLAN, а на VLAN-интерфейсах будет выполнена настройка VRRP для того, чтобы для каждой сети (клиентской и административной) роутеры делили между собой виртуальный адрес. Позже на VRRP интерфейсы будут установлены DHCP-сервера, чтобы в качестве шлюза по умолчанию устройства из клиентского или административного VLAN, получали соответствующий адрес gateway в виде виртуального адреса VRRP.

Также в результате настройки на каждом коммутаторе в локальной сети должны быть объявлены оба VLAN'а (клиентский и административный), должен быть назначен ip-адрес на интерфейс административного VLAN'а и произведена настройка маршрута по умолчанию на административный VRRP-адрес.

В итоге у нас получается достаточно отказоустойчивая схема локальной сети в каждом филиале. В случае неработоспособности одного из роутеров ему на помощь придёт второй и связность между VLAN'ами никуда не исчезнет.

2.2 Настройка выхода в Интернет с использованием NAT и port forwarding.

В этом отчёте я не буду останавливаться на настройке сети провайдера, но ниже будет продемонстрирована настройка выхода в Интернет с использованием NAT.

На рисунке 9 показано подключение хоста (моего ноутбука) адаптером VMNet8 к схеме для обеспечения доступа в Интернет.

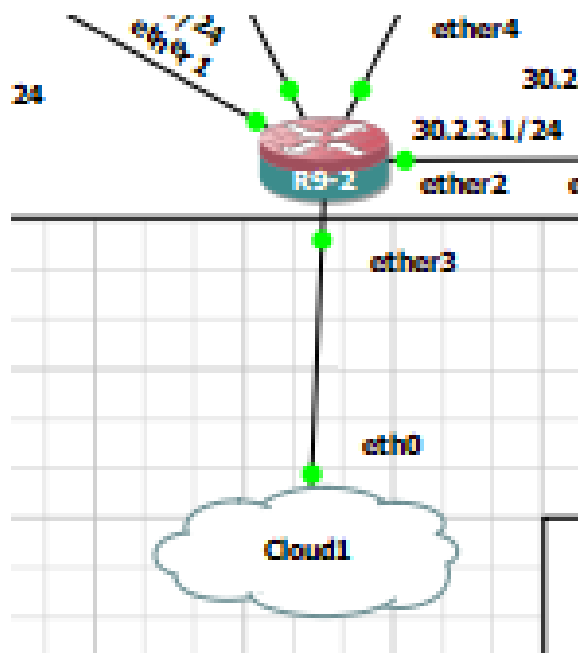


Рисунок 9 – Подключение хоста виртуальным адаптером к сети провайдера для обеспечения доступа в интернет

Теперь необходимо настроить получение адреса и маршрута по умолчанию в Интернет по DHCP на R9-2 маршрутизаторе. Это показано на рисунке 10.

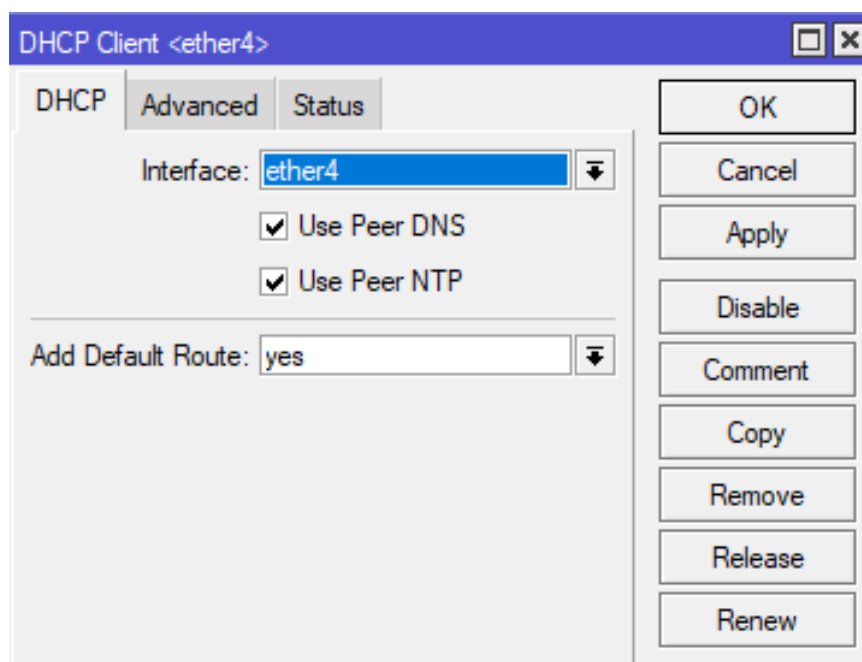


Рисунок 10 – Получение адреса из сети Интернет и маршрута по умолчанию на R9-2

Теперь необходимо настроить распространение маршрута по умолчанию на R9-2 другим маршрутизаторам в провайдерской сети. Делается это в BGP соединении с помощью галочки около пункта – Default Originate Always. Так как R9-2 является Router-Reflector'ом для своей автономной системы, то все маршрутизаторы получают маршрут по умолчанию через него и для того, чтобы был реализован выход в Интернет необходимо настроить NAT на R9-2, чтобы все локальные адреса скрывались за его адресом. Настройка NAT на R9-2 продемонстрирована на рисунках 11-12.

The image shows the 'NAT Rule' configuration window. The 'General' tab is active. The 'Chain' dropdown is set to 'srcnat'. The 'Out. Interface' dropdown is set to 'ether4'. The 'Out. Interface' checkbox is checked. The 'In. Interface' dropdown is empty. The 'In. Interface List' and 'Out. Interface List' dropdowns are empty. The 'Protocol' dropdown is empty. The 'Src. Port', 'Dst. Port', and 'Any. Port' dropdowns are empty. The 'Packet Mark', 'Connection Mark', and 'Routing Mark' dropdowns are empty. The 'Connection Type' dropdown is empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'.

Рисунок 11 – Настройка NAT на R9-2 (General)

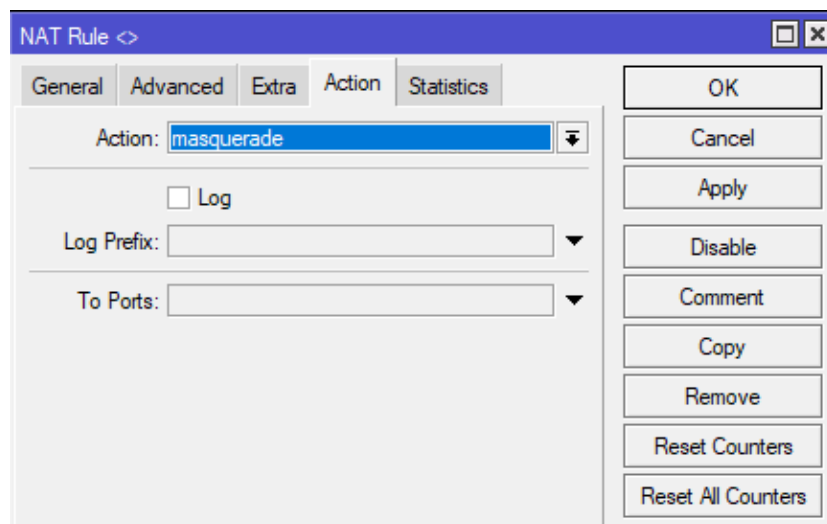


Рисунок 12 – Настройка NAT на R9-2 (Action)

После данной настройки доступ в Интернет был успешно получен, осталось настроить port forwarding, чтобы при обращении хоста к глобальному адресу R9-2 мы попадали на файловый сервер, который находится в локальной сети филиала. Настройка port forwarding продемонстрирована на рисунках 13-16.

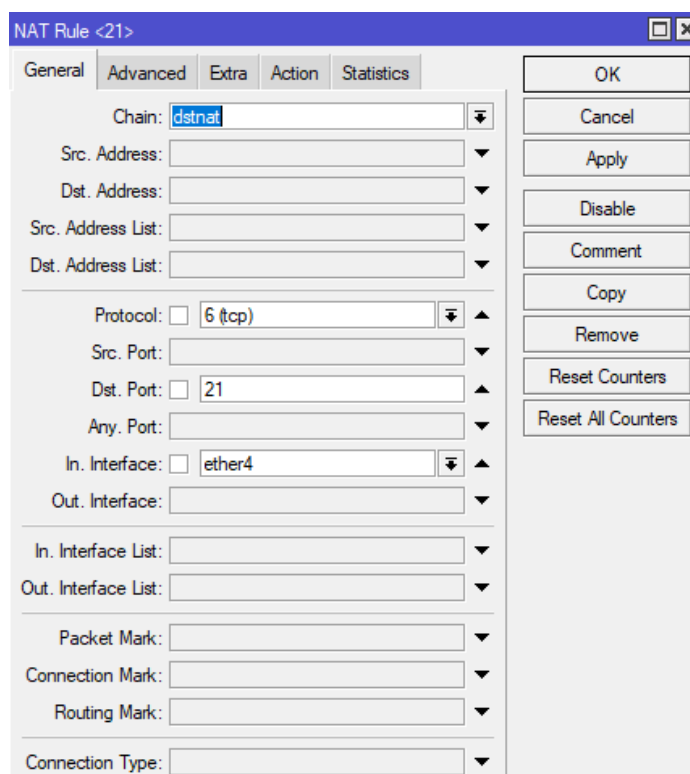


Рисунок 13 – Настройка port forwarding на R9-2 (General)

NAT Rule <21>

General Advanced Extra Action Statistics

Action: **dst-nat**

☐ Log

Log Prefix:

To Addresses: 200.2.1.254

To Ports: 21

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Рисунок 14 – Настройка port forwarding на R9-2 (Action)

NAT Rule <21>

General Advanced Extra Action Statistics

Chain: **dstnat**

Src. Address:

Dst. Address:

Src. Address List:

Dst. Address List:

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port: ☐ 21

Any. Port:

In. Interface: ☐ ether1

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Рисунок 15 – Настройка port forwarding на R15-2 (General)

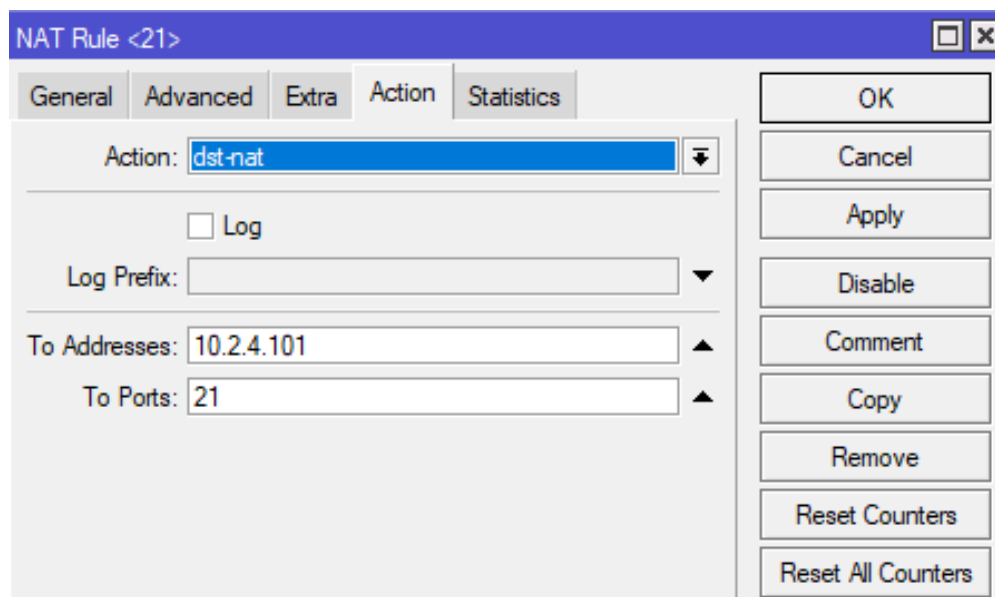


Рисунок 16 – Настройка port forwarding на R15-2 (Action)

В результате настройки при обращении по протоколу ftp к глобальному адресу, который получает R9-2 мы будем попадать на R15-2 и оттуда на файловый сервер.

2.3 Настройка файлового сервера.

Настройка файлового сервера на операционной системе REDOS, который будет находится в главном офисе продемонстрирована ниже:

Для начала необходимо обновить пакеты и установить vsftpd с помощью следующих команд:

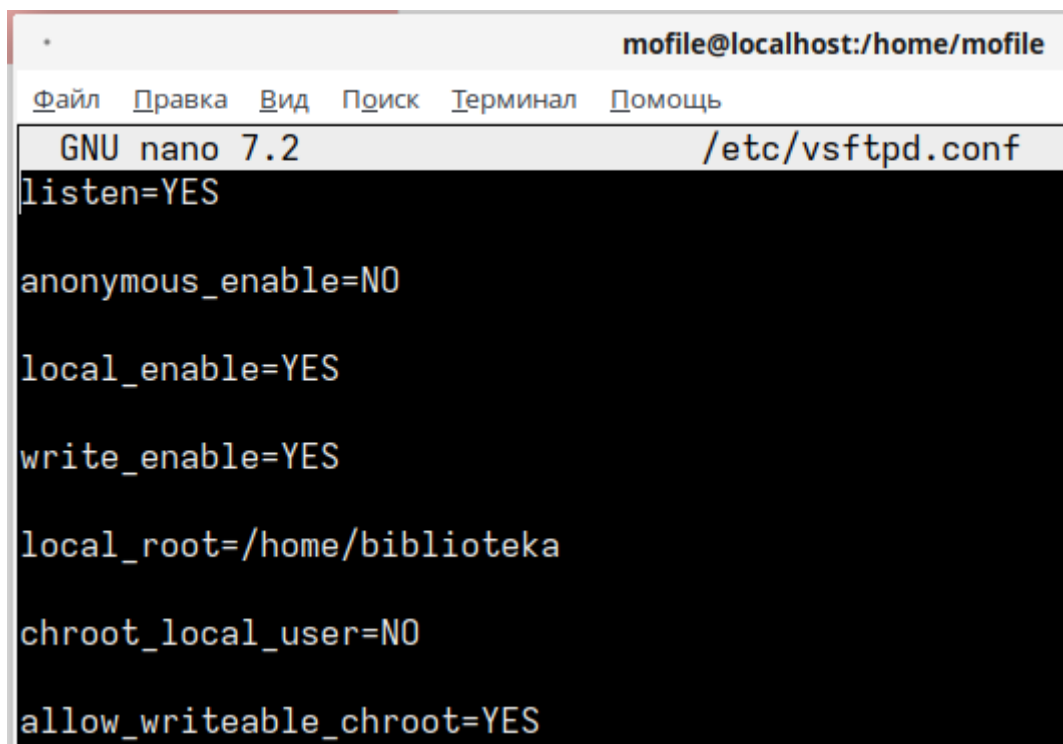
```
sudo apt update
```

```
sudo apt install vsftpd
```

После этого необходимо открыть конфигурационный файл vsftpd с помощью следующей команды для дальнейшего редактирования:

```
sudo nano /etc/vsftpd.conf
```

Добавляем в файл строки, представленные на рисунке 17.



```
mofile@localhost:/home/mofile
Файл  Правка  Вид  Поиск  Терминал  Помощь
GNU nano 7.2 /etc/vsftpd.conf
listen=YES

anonymous_enable=NO

local_enable=YES

write_enable=YES

local_root=/home/biblioteka

chroot_local_user=NO

allow_writeable_chroot=YES
```

Рисунок 17 – Редактирование конфигурационного файла vsftpd.conf

Теперь необходимо создать общую папку и установить права доступа с помощью следующих команд:

```
sudo mkdir /home/biblioteka
sudo chmod 2775 /home/biblioteka
sudo chown root:users /home/biblioteka
```

Далее создаем пользователей для подключения к файловому серверу (админа и клиента) и задаем им пароли с помощью следующих команд:

```
sudo adduser admin
sudo adduser client
sudo passwd admin
sudo passwd client
```

Теперь настраиваем права доступа к общей папке для каждого пользователя. Админ должен иметь полные права, а клиент только на просмотр и исполнение. Настройка продемонстрирована ниже:

sudo setfacl -R -m u:admin:rwX /home/biblioteka

sudo setfacl -R -m u:client:rx /home/biblioteka

Теперь необходимо перезапустить сервис vsftpd с помощью следующей команды и файловый сервер будет успешно настроен:

sudo systemctl restart vsftpd

Проверка правильности настроек:

Установим любой FTP клиент на компьютер (в моем случае выбор пал на FileZilla Client) и подключимся к глобальному адресу R9-2 по протоколу ftp для проверки всех настроек (рисунок 18).

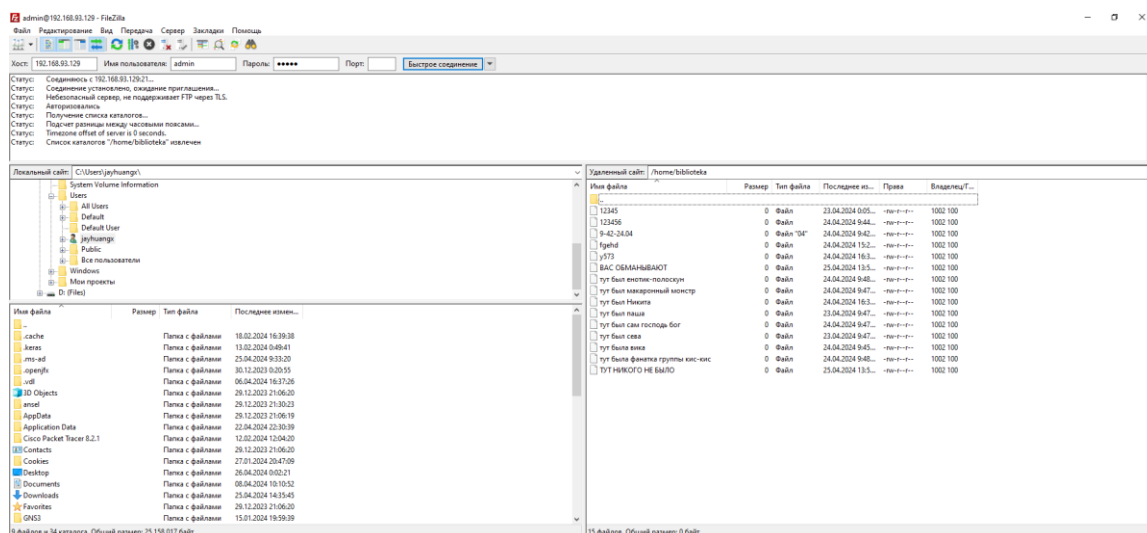


Рисунок 18 – Проверка правильности настроек файлового сервера и port forwarding

3 Управление сетевыми сервисами.

Цели и задачи:

- настроить DHCP и DNS-серверы;
- объединить офисы с помощью технологии VPN;
- настроить удаленный доступ к сетевым устройствам для администратора.

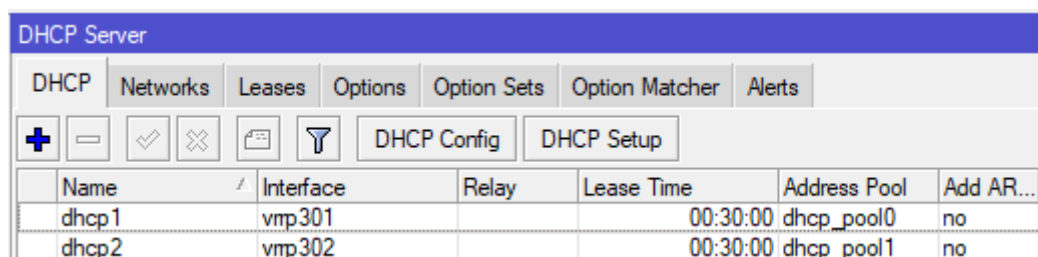
Используемое оборудование, инструменты, программное обеспечение:

- аналогично п.2;
- bind9, dnsmasq, встроенный в сетевое оборудование сервер, прочее;

Последовательность выполнения и описание действий:

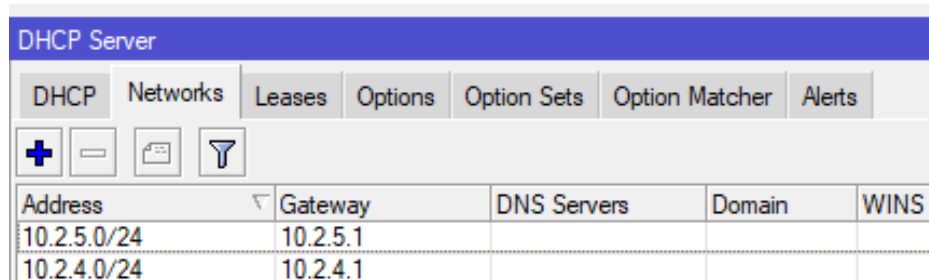
3.1 Настройка DHCP-сервера.

Первым делом необходимо в каждой локальной сети филиалов настроить DHCP-сервер. DHCP сервер будет установлен на VRRP интерфейсы роутеров для каждого из VLAN'ов. Результат настройки DHCP серверов на R15 продемонстрирован на рисунках 19-20.



Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp1	vnp301		00:30:00	dhcp_pool0	no
dhcp2	vnp302		00:30:00	dhcp_pool1	no

Рисунок 19 – DHCP-сервера на R15



Address	Gateway	DNS Servers	Domain	WINS S
10.2.5.0/24	10.2.5.1			
10.2.4.0/24	10.2.4.1			

Рисунок 20 – Сети, которые выдают DHCP сервера

Настройки на остальных маршрутизаторах в филиалах аналогичны тем настройкам, которые представлены на рисунках 19-20.

3.2 Настройка туннелирования и OSPF между GRE.

Для связности филиалов с главным офисом необходимо настроить GRE-туннели. Их настройка на R17 продемонстрирована на рисунках 21-22.

Рисунок 21 – Туннель на R17-2 в сторону главного офиса (R15-2)

Рисунок 22 – Туннель на R17-2 в сторону главного офиса (R16-2)

Аналогичным образом настраиваются GRE туннели на остальных маршрутизаторах в филиалах. В главном офисе в сторону R17-2, R18-2, R19-2, R20-2 и в филиалах в сторону R15-2 и R16-2.

GRE-туннелям необходимо задать IP-адреса и для связности с главным офисом назначить филиалам маршрут по умолчанию на GRE-туннель в сторону главного офиса. Также необходимо указать статичный маршрут к удаленному адресу GRE-туннеля через ближайший к филиалу маршрутизатор, чтобы он знал, как туда добраться.

После необходимых настроек был настроен OSPF между GRE-туннелями для того, чтобы филиалы и главный офис знали про локальные сети друг друга. Пример настройки OSPF между GRE туннелями изображен на рисунках 23 – 25.

Рисунок 23 – Создание ospf instance

OSPF Area <ospf-area-1>

Name:

Instance: ▾

Area ID:

Type: ▾

☐ No Summaries

Default Cost:

NSSA Translator:

☐ Transit Capable

OK

Cancel

Apply

Disable

Comment

Copy

Remove

enabled

transit capable

Рисунок 24 – Создание ospf area

OSPF Interface Template

Interfaces: ▾

▾

▾

▾

▾

Area: ▾

Networks:

Network Type: ▾

Prefix List:

Instance ID:

Cost:

Priority:

☐ Passive

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Рисунок 25 – Включение интерфейсов в OSPF

Аналогичным образом необходимо настроить динамическую маршрутизацию с помощью OSPF между GRE-туннелями на остальных маршрутизаторах в филиалах. После настройки в маршрутах можно увидеть, что все маршрутизаторы в филиалах узнали про локальные сети друг друга. Маршруты, полученные по OSPF между GRE-туннелями представлены на рисунке 26.

DAo	10.2.4.0/24	175.2.175.15%GRE_to_R15
DAo	10.2.5.0/24	175.2.175.15%GRE_to_R15
DAo+	10.2.6.0/24	175.2.175.15%GRE_to_R15
DAo+	10.2.6.0/24	176.2.176.16%GRE_to_R16
DAo+	10.2.7.0/24	175.2.175.15%GRE_to_R15
DAo+	10.2.7.0/24	176.2.176.16%GRE_to_R16
DAC+	10.2.8.0/24	vlan201
DAC+	10.2.8.0/24	vmp201
DAC+	10.2.9.0/24	vlan202
DAC+	10.2.9.0/24	vmp202

Рисунок 26 – Маршруты, полученные по OSPF между GRE-туннелями

Также на выходных физических интерфейсах маршрутизаторов в филиалах необходимо настроить NAT, чтобы локальные адреса филиалов, скрывались за глобальными адресами роутеров. Пример настройки NAT на R17 представлен на рисунках 27-28.

NAT Rule <>

General Advanced Extra Action ...

Chain: srcnat

Src. Address:

Dst. Address:

Src. Address List:

Dst. Address List:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: ☐ ether1

In. Interface List:

Out. Interface List:

Packet Mark:

enabled

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Рисунок 27 – NAT на R17 (General)

NAT Rule <>

Advanced Extra Action Statistics ...

Action: masquerade

☐ Log

Log Prefix:

To Ports:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Рисунок 28 – NAT на R17 (Action)

Выполнение данных настроек на всех маршрутизаторах в филиалах обеспечило связность между локальными сетями филиалов.

3.3 Настройка кеширующих DNS-серверов.

В проектируемой сети библиотеки есть 3 филиала. Для введения устройств в домен и обеспечения name resolving'a было принято решение установить в каждом филиале кеширующие DNS сервера на операционной системе Debian с помощью dnsmasq, так как этот вариант более простой в настройке и ближайший его конкурент bind9 больше подходит для полноценной настройки больших корпораций с трансфером зон между доменами, так что в данной сети его функционал будет излишним. Каждый DNS-сервер будет ответственным исключительно за свою зону. Филиалы, в случае отсутствия записей на локальном DNS сервере должны будут обращаться за помощью к DNS серверу в главном офисе. Доменом главного офиса будет Bondarchuk2.up, а филиалы будут обслуживать зоны в доменах f1.Bondarchuk2.up и f2.Bondarchuk2.up. Кеширующий DNS сервер в главном офисе будет перенаправлять все неизвестные запросы на DNS сервер Google, а запросы, адресованные к первому или второму филиалу на соответствующие DNS сервера. Настройка DNS сервера в главном филиале представлена ниже.

Обновляем пакеты и устанавливаем dnsmasq с помощью следующей команды:

```
apt install dnsmasq
```

После заходим в конфигурационный файл dnsmasq с помощью следующей команды:

```
nano /etc/dnsmasq.conf
```

Записываем в конфигурационный файл следующий набор команд:

```
domain=Bondarchuk2.up
```

```
expand-hosts
```

```
conf-dir=/etc/dnsmasq.d/,*.conf
```

```
interface=ens4
```


bind-interfaces

server=/f2.Bondarchuk2.up/10.2.8.150

server=/f1.Bondarchuk2.up/10.2.6.150

server=8.8.8.8

Далее создаем файл с описанием зоны, за которую ответственен dns сервер в главном офисе и заходим сразу в его редактирование с помощью следующей команды:

```
nano /etc/dnsmasq.d/Bondarchuk2.conf
```

И записываем туда записи о каждом устройстве в данной зоне:

address=/modns.Bondarchuk2.up/10.2.4.150

address=/mocli.Bondarchuk2.up/10.2.5.240

address=/mofile.Bondarchuk2.up/10.2.4.101

address=/moadmin.Bondarchuk2.up/10.2.4.102

address=/r15.Bondarchuk2.up/10.2.4.10

address=/r16.Bondarchuk2.up/10.2.4.20

address=/sw2.Bondarchuk2.up/10.2.4.2

address=/sw3.Bondarchuk2.up/10.2.4.3

address=/sw4.Bondarchuk2.up/10.2.4.4

address=/sw5.Bondarchuk2.up/10.2.4.5

Аналогичным образом настраиваем кеширующие DNS сервера в филиалах, но в файле dnsmasq.conf указываем только один сервер для перенаправления – сервер в главном офисе.

После этого настройка dns серверов будет закончена. Убедимся в этом с помощью выполнения следующей команды, представленной на рисунке 29.

```
root@debian:/home/debian# ping fladmin.fl.Bondarchuk2.up
PING fladmin.fl.Bondarchuk2.up (10.2.6.100) 56(84) bytes of data.
64 bytes from 10.2.6.100 (10.2.6.100): icmp_seq=1 ttl=61 time=28.4 ms
64 bytes from 10.2.6.100 (10.2.6.100): icmp_seq=2 ttl=61 time=19.2 ms
64 bytes from 10.2.6.100 (10.2.6.100): icmp_seq=3 ttl=61 time=47.3 ms
64 bytes from 10.2.6.100 (10.2.6.100): icmp_seq=4 ttl=61 time=69.1 ms
```

Рисунок 29 – Успешный ping по доменному имени со второго на первый филиал

					УП.09.02.06.02ПД	Лист
						33
Изм.	Лист	№ докум.	Подп.	Дата		

Как видно на рисунке 29 перенаправление работает корректно. Давайте также убедимся, что преобразуются у нас не только имена из локального домена, но и из глобальной сети интернет (рисунок 30).

```

root@debian:/home/debian# ping guap.ru
PING guap.ru (194.226.199.248) 56(84) bytes of data.
64 bytes from web1.cit2.guap.ru (194.226.199.248): icmp_seq=1 ttl=125 time=15.8
ms
64 bytes from web1.cit2.guap.ru (194.226.199.248): icmp_seq=2 ttl=125 time=15.3
ms
64 bytes from web1.cit2.guap.ru (194.226.199.248): icmp_seq=3 ttl=125 time=47.2
ms
64 bytes from web1.cit2.guap.ru (194.226.199.248): icmp_seq=4 ttl=125 time=60.7
ms
^C
--- guap.ru ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 15.250/34.750/60.662/19.779 ms

```

Рисунок 30 – Успешный ping guap.ru

Настройка кеширующих DNS серверов для введения компьютеров в домен Bondarchuk2.up прошла успешно.

3.4 Настройка telnet и файрволла.

Для начала нам необходимо обеспечить возможность подключения по telnet ко всем устройствам на схеме. Возможность подключения к Mikrotik по telnet доступна по умолчанию. Необходимо настроить возможность подключения к коммутаторам cisco, серверам на Debian и ReDOS.

Настройка подключения по telnet на cisco коммутаторах выполняется с помощью следующих команд:

```

Conf t
Line vty 0 4
Transport input telnet
Password 1234
Login
Exit
Enable password 1234

```

Настройка подключения по telnet на debian выполняется с помощью установки пакета telnetd.

Настройка подключения по telnet к redos выполняется с помощью установки пакета telnet-server.x86-64

Теперь настроим firewall на маршрутизаторах в филиалах, чтобы только администратор в главном офисе (10.2.4.102) мог подключаться по telnet ко всем сетевым устройствам. Также настроим преобразование адресов с помощью NAT из админской сети в клиентскую, чтобы с помощью правил запретить все новые соединения от клиентов к администраторам.

Настройки Firewall на R15-2 представлены на рисунках 31 – 33.

List	#	Address	Timeout	Creation Time
admin		10.2.4.0/24		Apr/25/2024 07:00...
clients		10.2.5.0/24		Apr/25/2024 07:00...

Рисунок 31 – Address Lists на R15-2

#	Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...
0	mas...	srcnat									ether1
1	dst...	dstnat					6 (tcp)		21	ether1	
2	mas...	srcnat			admin	clients					

Рисунок 32 – NAT на R15-2

#	Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...
0	acc...	forward		10.2.4.150	clients	admin					
1	drop	forward			clients	admin					
2	acc...	forward		10.2.4.102			6 (tcp)	23			
3	drop	forward		10.2.4.102			6 (tcp)	23			

Рисунок 33 – Filter Rules на R15-2

Аналогичным образом настраиваем Firewall на R16-2.

Настройки Firewall на R17-2 представлены на рисунках 34 – 36.

Firewall					
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols					
<div> <div>+</div> <div>–</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> </div>					
List	Address	Timeout	Creation Time		
● admin	10.2.8.0/24		Apr/25/2024 07:1...		
● clients	10.2.9.0/24		Apr/25/2024 07:1...		

Рисунок 34 – Address Lists на R17-2

Firewall												
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols												
<div> <div>+</div> <div>–</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>🔄 Reset Counters</div> <div>🔄 Reset All Counters</div> <div>Find</div> </div>												
#	Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	
0	mas...	srcnat										ether1
1	mas...	srcnat			admin	clients						

Рисунок 35 – NAT на R17-2

Firewall										
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols										
<div> <div>+</div> <div>–</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>🔄 Reset Counters</div> <div>🔄 Reset All Counters</div> </div>										
#	Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	
0	acc...	forward	10.2.4.102				6 (tcp)		23	
1	drop	forward					6 (tcp)		23	
2	drop	forward			clients	admin				

Рисунок 36 – Filter Rules на R17-2

Аналогичным образом настраиваем Firewall на R18-2.

Настройки Firewall на R19-2 представлены на рисунках 37 – 39.

Firewall

Filter Rules

NAT

Mangle

Raw

Service Ports

Connections

Address Lists

Layer7 Protocols

+

−

✓

✗

📄

🔍

Find

List	Address	Timeout	Creation Time
● admin	10.2.6.0/24		Apr/25/2024 07:4...
● client	10.2.7.0/24		Apr/25/2024 07:4...

Рисунок 37 – Filter Rules на R19-2

Firewall

Filter RulesNATMangleRawService PortsConnectionsAddress ListsLayer7 Protocols

</

Рисунок 38 – NAT на R19-2

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Reset Counters

Reset All Counters

Find

all

#	Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	li
0	acc...	forward	10.2.4.102				6 (tcp)		23	
1	drop	forward			client	admin				
2	drop	forward					6 (tcp)		23	

Рисунок 39 – Filter Rules на R19-2

Аналогичным образом настраиваем Firewall на R20-2.

Проверяем работоспособность выполненных настроек на рисунках 40-42.

```

debian@debian:~$ telnet 10.2.8.101
Trying 10.2.8.101...
Connected to 10.2.8.101.
Escape character is '^]'.
Debian GNU/Linux 11
debian login: debian
Password:
Linux debian 5.10.0-28-cloud-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Apr 26 01:01:20 UTC 2024 from 10.2.4.102 on pts/0
debian@debian:~$
telnet> quit
Connection closed.
root@moadmin:/home/debian# telnet 10.2.6.101
Trying 10.2.6.101...
Connected to 10.2.6.101.
Escape character is '^]'.
Debian GNU/Linux 11
debian login: debian
Password:
Linux debian 5.10.0-28-cloud-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Apr 26 01:08:53 UTC 2024 on ttyS0
debian@debian:~$
telnet> quit
Connection closed.
root@moadmin:/home/debian#

```

Рисунок 40 – Успешное подключение по telnet с главного офиса к филиалам

```

root@debian:/home/debian# telnet 10.2.4.150
Trying 10.2.4.150...
^C
root@debian:/home/debian# telnet 10.2.8.101
Trying 10.2.8.101...
^C

```

Рисунок 41 – Безуспешное подключение с 1 филиала к главному офису и 2 филиалу

```

debian@debian:~$ telnet 10.2.6.101
Trying 10.2.6.101...
^C
debian@debian:~$ telnet 10.2.4.150
Trying 10.2.4.150...
^C

```

Рисунок 42 – Безуспешное подключение с 2 филиала к главному офису и 1 филиалу

Проверка показала, что все настройки Firewall'a были выполнены верно.
В сети библиотеки была обеспечена безопасность.

4 Модернизация сетевой инфраструктуры.

Цели и задачи:

- выполнить изменения в сети организации;
- внедрить новые технологии в сети организации;

Используемое оборудование, инструменты, программное обеспечение:

- аналогично п.2;
- беспроводной маршрутизатор MikroTik;
- WinBox;
- eNSP.

Последовательность выполнения и описание действий:

Было получено задание по внедрению в организацию беспроводной сети и беспроводных клиентов, настроив точку доступа Wi-Fi на MikroTik с технологией HotSpot.

Для начала необходимо было подключить реальный физический маршрутизатор MikroTik к хосту (ноутбуку) и через виртуальный адаптер Vmnet0 (Bridge) подключить ноутбук к локальной сети в GNS3 (рисунок 43).

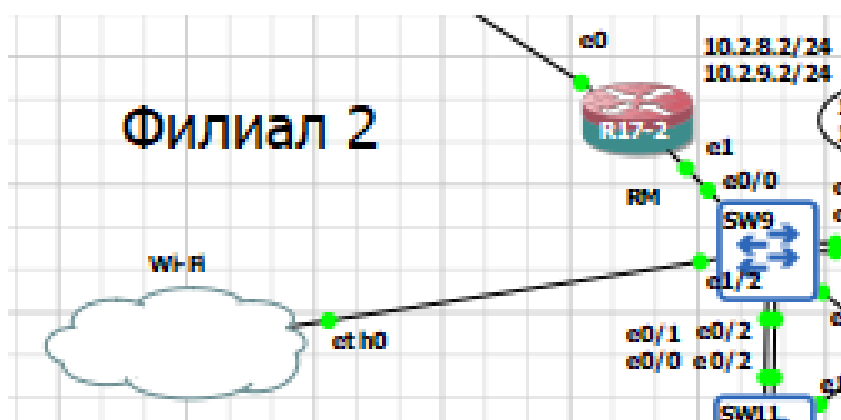


Рисунок 43 – Подключение ноутбука к локальной сети в GNS3 через Bridge адаптер

Теперь необходимо дождаться, когда ноутбук получит IP-адрес по DHCP из локальной сети (рисунок 44) и подключиться к MikroTik для дальнейшей настройки через WinBox.

```
Адаптер Ethernet Ethernet:
DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . : fe80::3059:7e6c:8af6:7079%19
IPv4-адрес. . . . . : 10.2.9.238
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . :
```

Рисунок 44 – Полученный ноутбуком адрес от DHCP сервера

Теперь нужно зайти во вкладку Wireless и отредактировать интерфейс WLAN1 таким образом, как это сделано на рисунке 45.

Рисунок 45 – Настройка интерфейса wlan1

После настройки wlan1 нужно получить адрес на интерфейс MikroTik, который подключен к ноутбуку. В моём случае это ether2 и получение адреса по DHCP на данный интерфейс продемонстрировано на рисунке 46.

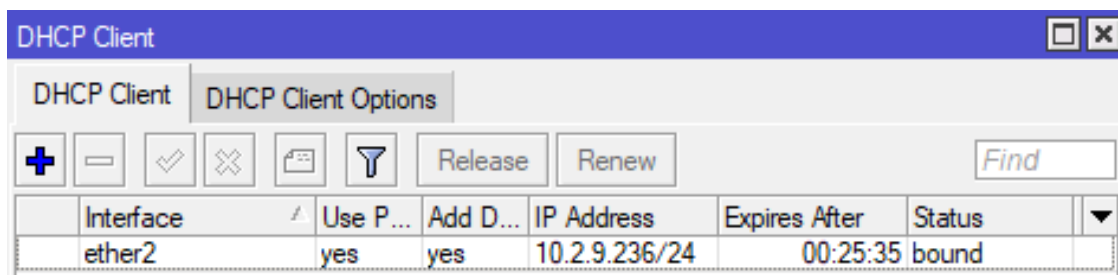


Рисунок 46 – Получение адреса по DHCP на MikroTik

Теперь необходимо выбрать любой незанятый интерфейс на MikroTik и выдать ему адрес из другой сети, адреса из которой будут получать клиенты. В качестве такого интерфейса был выбран ether3, и настройка адреса на нём продемонстрирована на рисунке 47.

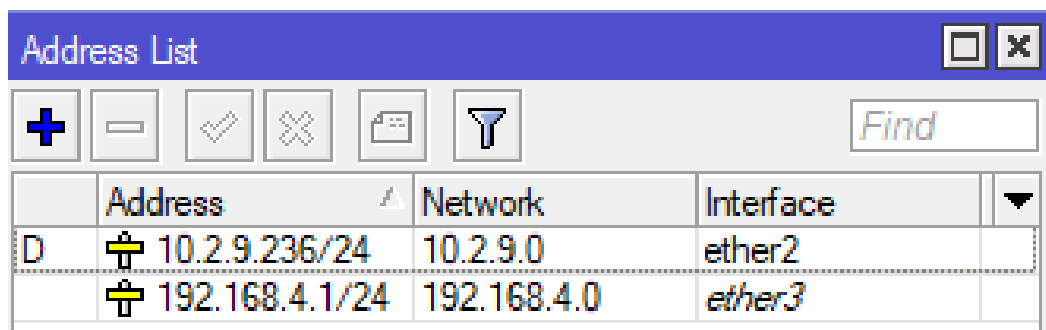


Рисунок 47 – Настройка адреса на ether3

После этого был создан Bridge интерфейс. Его создание продемонстрировано на рисунке 48.

Рисунок 48 – Создание Bridge интерфейса

После создания интерфейса были выбраны порты, которые будут включены в созданный Bridge. Включенные в Bridge порты продемонстрированы на рисунке 49.

#	Interface	Bridge	Horizon	Trusted	Priority (h...	Path Cost	Role
0	wlan1	bridge1		no	80	10	designated port
1	ether3	bridge1		no	80	10	disabled port

Рисунок 49 – Включенные в Bridge порты

После этого был настроен DNS на MikroTik, чтобы подключенные клиенты воспринимали MikroTik как DNS сервер. Настройка DNS продемонстрирована на рисунке 50.

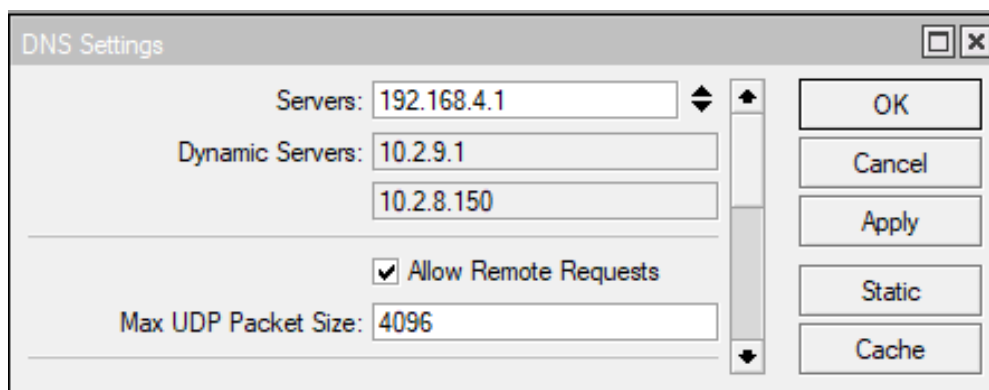


Рисунок 50 – Настройка DNS

После настройки DNS была совершена настройка HotSpot через кнопку HotSpot Setup. В качестве интерфейса был выбран созданный ранее bridge. В качестве гейтвея был выбран адрес из глобальной сети, то есть ether3 (192.168.4.1), все остальные настройки выбирались по умолчанию, а в профиле пользователя был выбран логин guest и пароль 12345678. Результат настроенного HotSpot сервера продемонстрирован на рисунке 51.

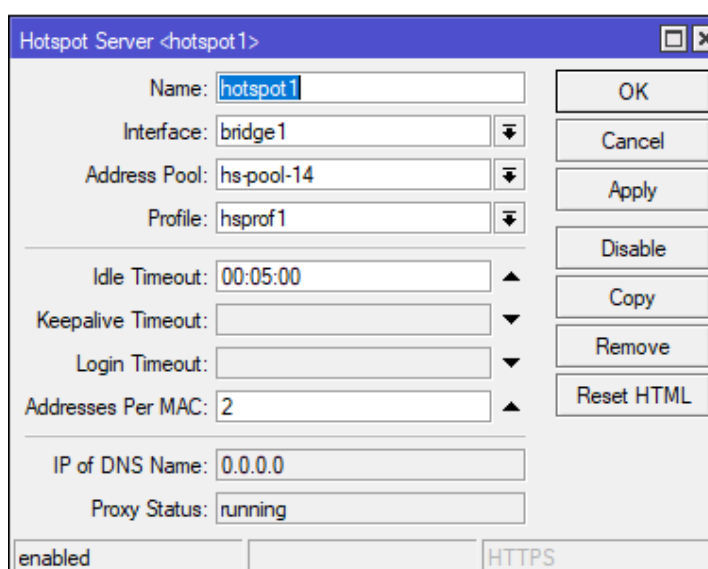


Рисунок 51 – Настроенный hotspot

На рисунках 52 - 54 будет продемонстрирован процесс подключения с телефона к созданной ранее точке доступа.

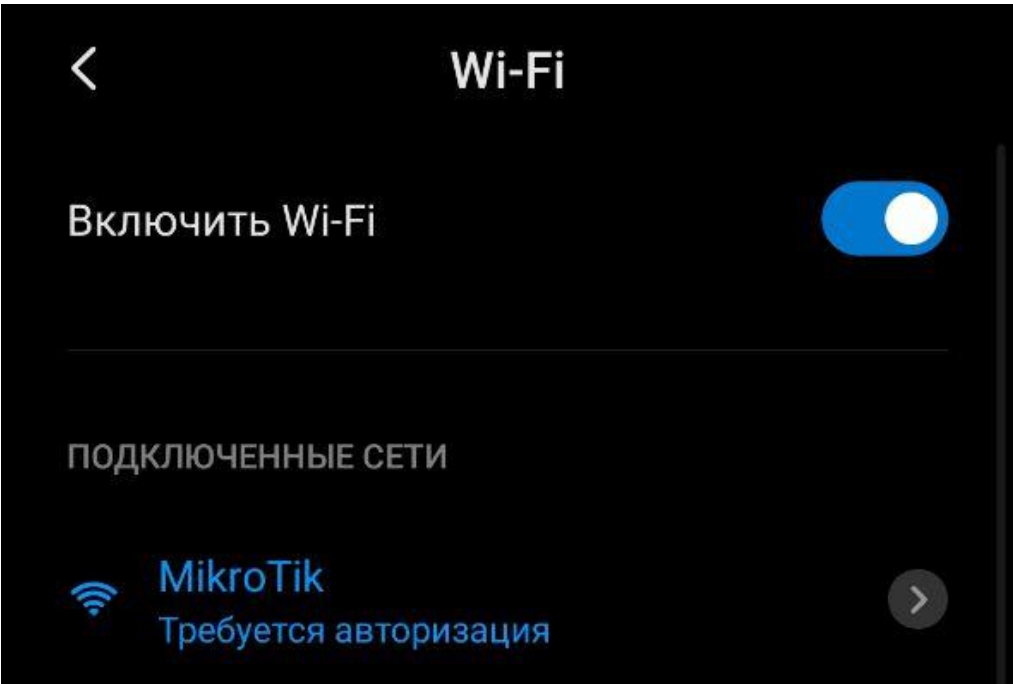


Рисунок 52 – Подключение к Wi-Fi

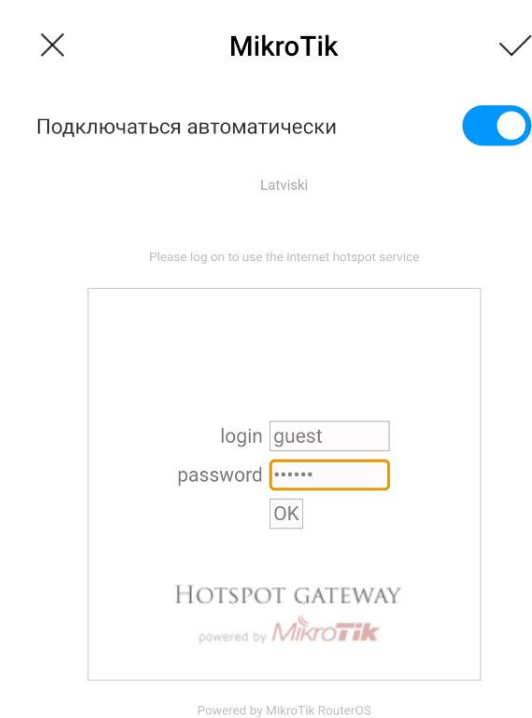


Рисунок 53 – Авторизация в сети через страничку HotSpot

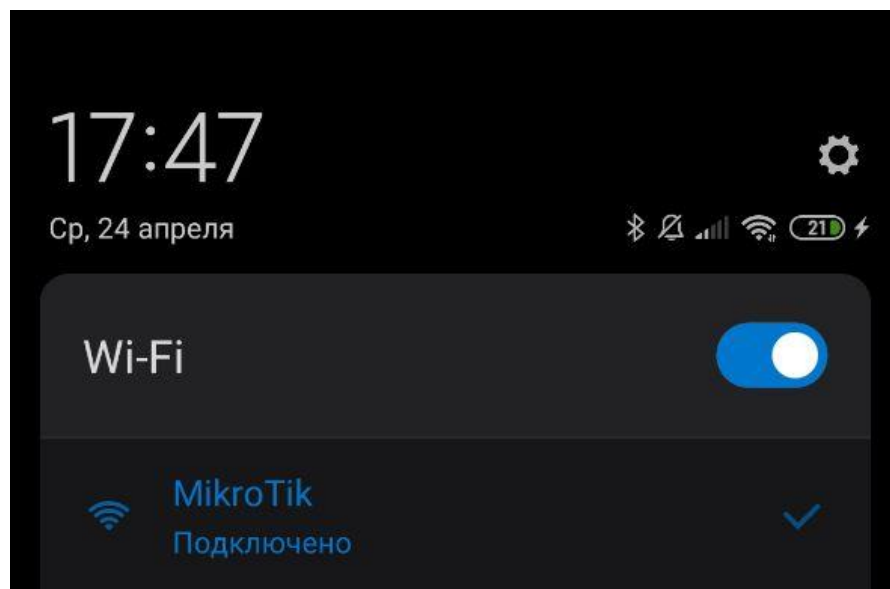


Рисунок 54 – Успешное подключение к сети Wi-Fi

Также было дано задание подключиться к файловому серверу с телефона. В качестве проводника, поддерживающего FTP был выбран СХ проводник. С помощью него было выполнено подключение к файловому серверу по его локальному адресу 10.2.4.101. Результат подключения продемонстрирован на рисунке 55.

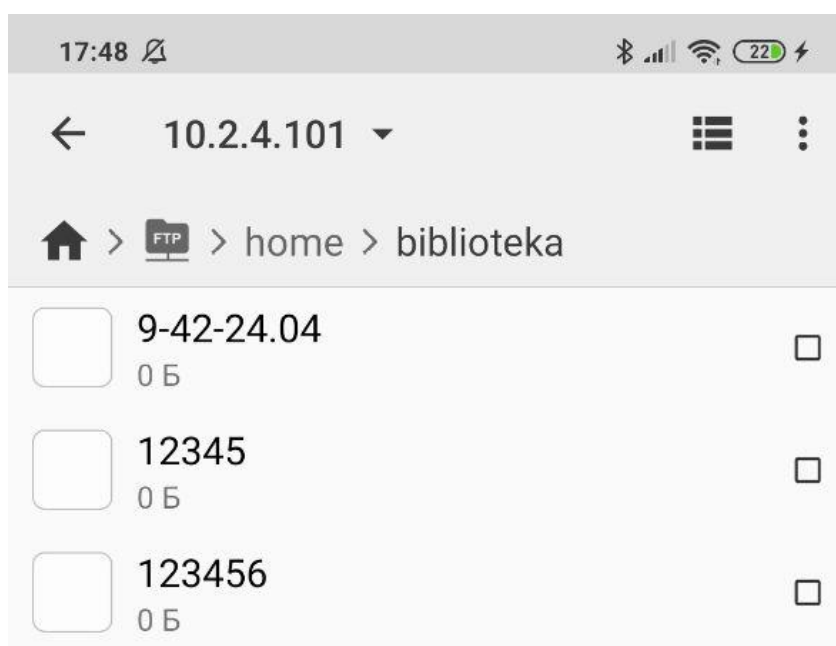


Рисунок 55 – Успешное подключение к файловому серверу

После подключения можно увидеть активную сессию во вкладке Active и временные файлы (Cookies), что говорит о том, что 4 задание было выполнено успешно. Сессия и файлы cookies продемонстрированы на рисунках 56 – 57.

Server	User	Domain	Address	Uptime	Idle Time
hotspot1	guest		192.168.4.250	00:08:07	00:00

Рисунок 56 – Активная сессия HotSpot

User	Domain	MAC Address	Expires In
guest		D8:CE:3A:E7:AE:4D	2d 23:51:35

Рисунок 57 – Cookies HotSpot

Источники

Учебная литература

1. Дибров, М. В. Компьютерные сети и телекоммуникации.

Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Профессиональное образование). — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/452574>

2. Дибров, М. В. Компьютерные сети и телекоммуникации.

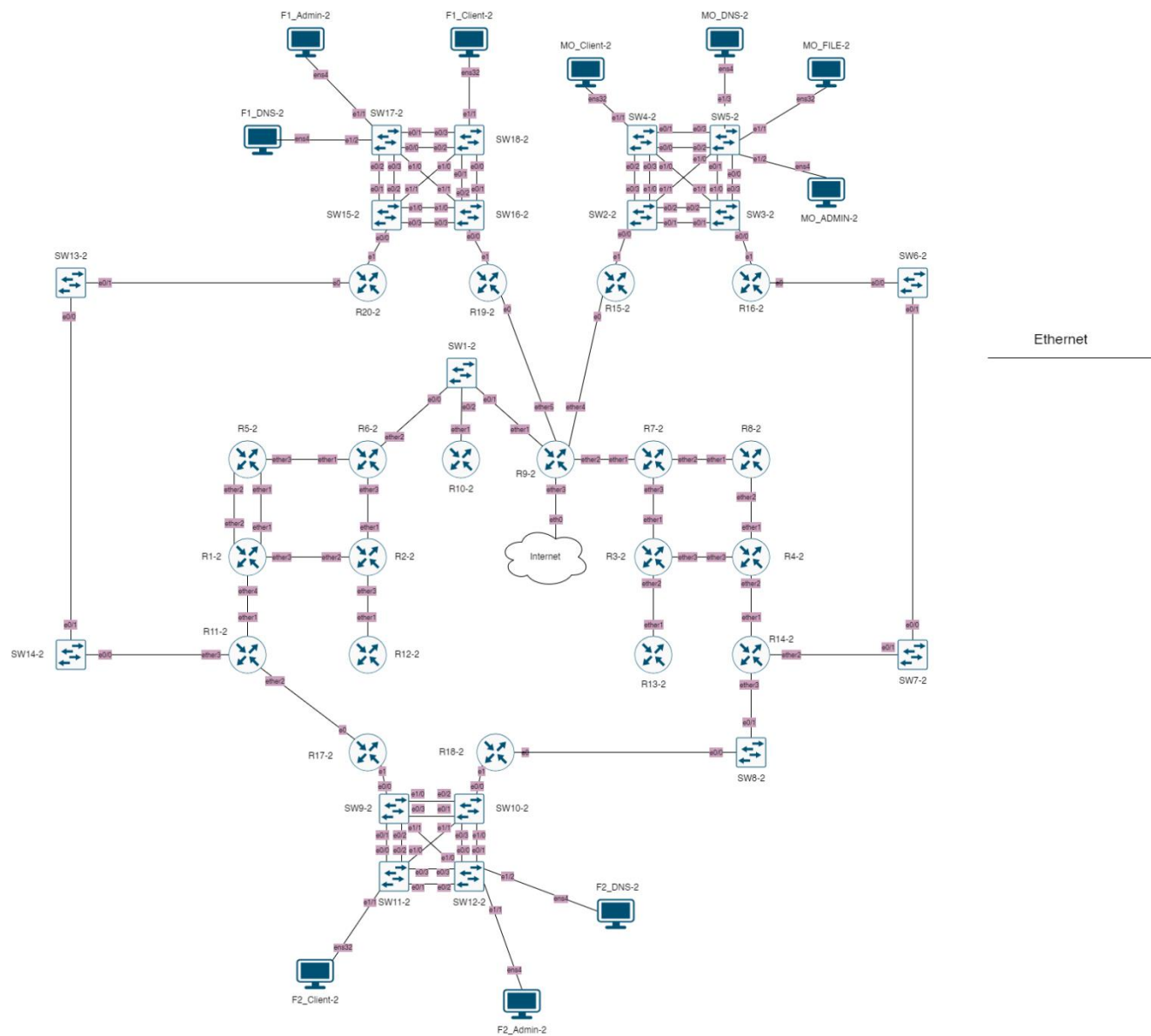
Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Профессиональное образование). — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/453065>

Дополнительные источники информации

3. <https://redos.red-soft.ru/>
4. <https://rus-linux.net/>
5. https://interface31.ru/tech_it/
6. <https://ubuntu.ru/doku.php>
7. <https://www.easycoding.org/>
8. <https://habr.com/>
9. <https://mnorin.com/>
10. <https://mikrotiklab.ru/>
11. <https://mikrotik.wiki/>
12. <https://global-hotspot.ru/nastroyka-hotspot-na-mikrotik/>
13. <https://it-nik.com/articles/nastraivaem-hotspot-na-mikrotik/>

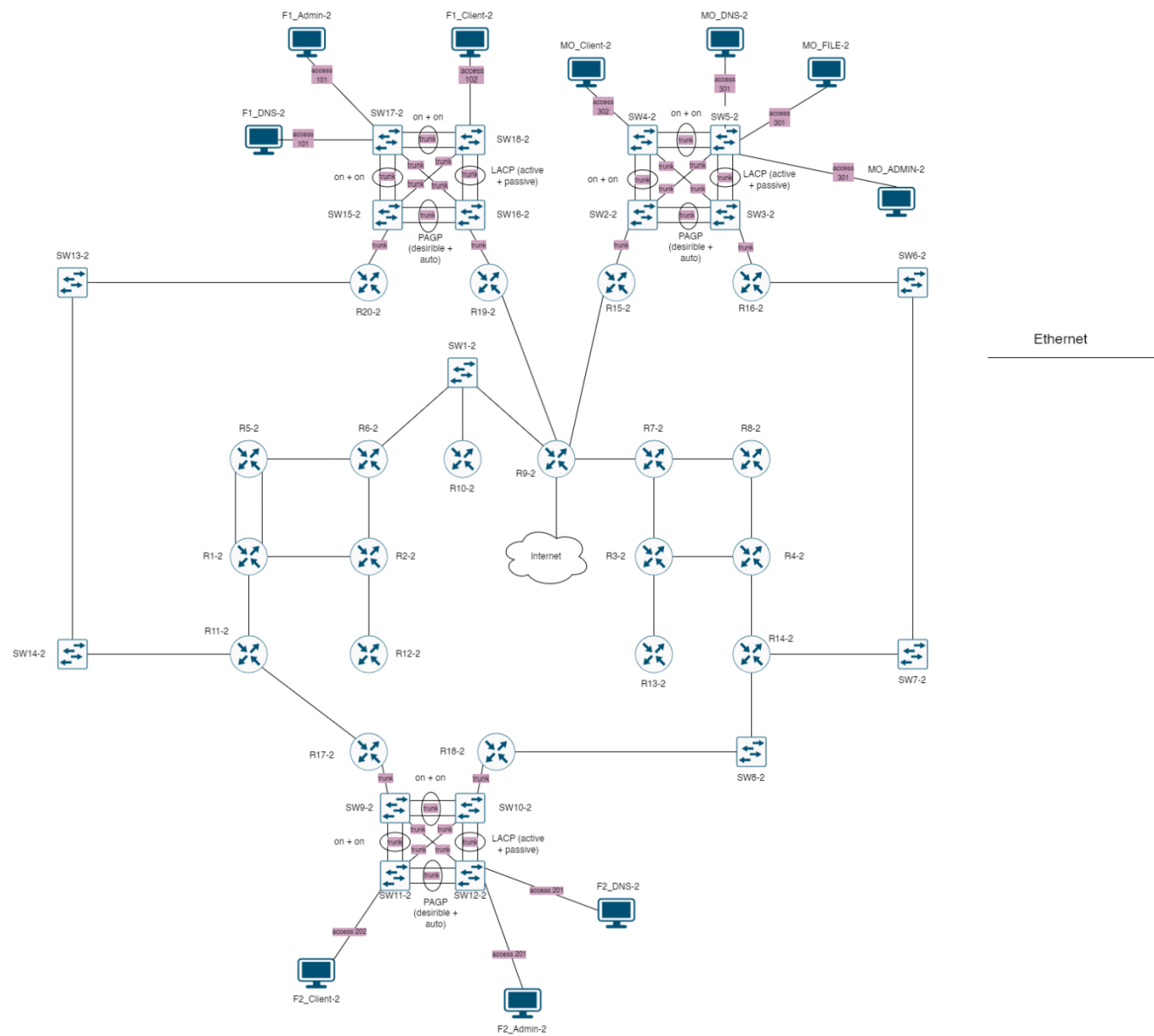
ПРИЛОЖЕНИЕ А

Схема L1



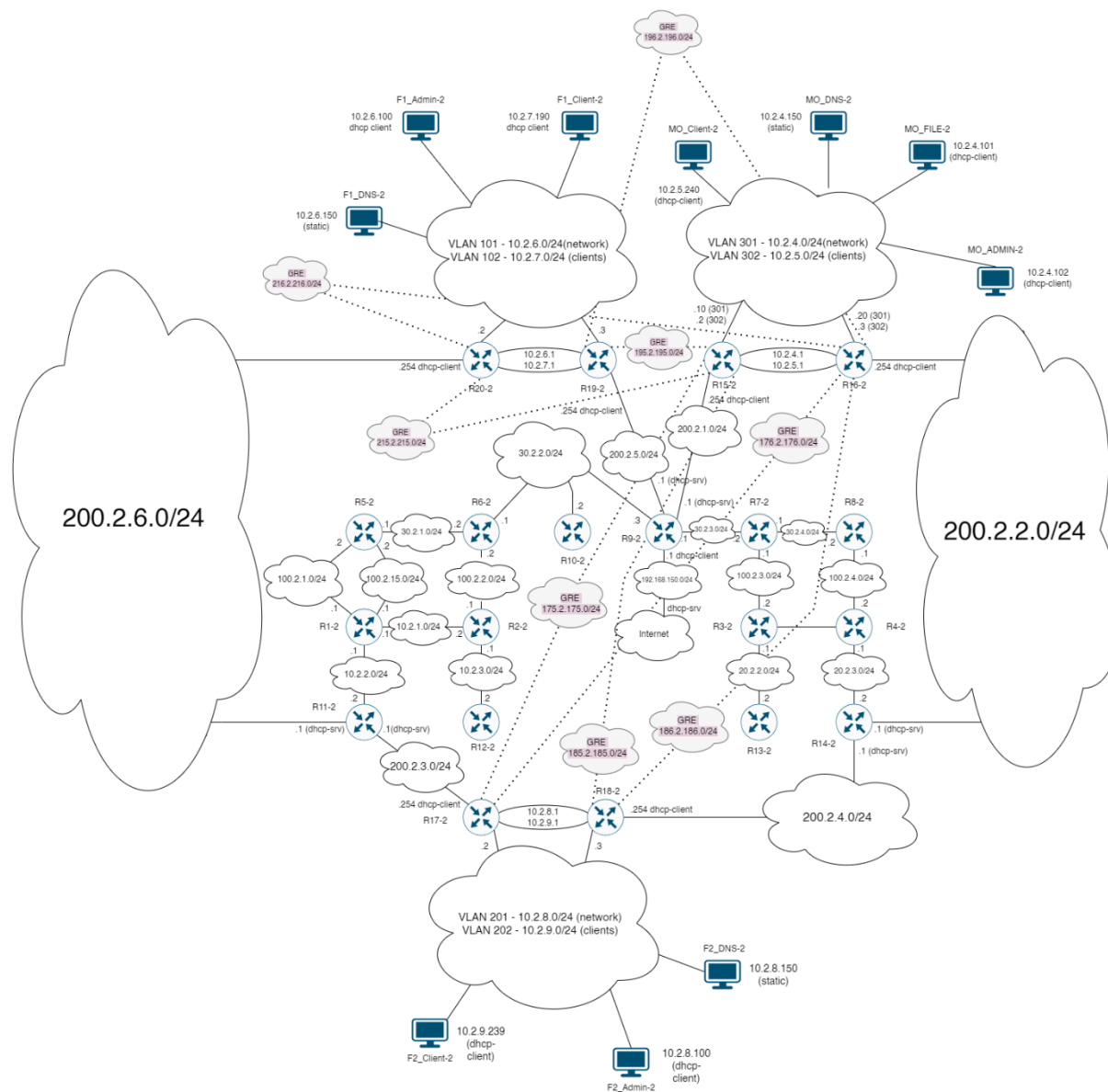
ПРИЛОЖЕНИЕ Б

Схема L2



ПРИЛОЖЕНИЕ В

Схема L3



Loopback адреса:

R1-2 = 2.1.1.1/32
R2-2 = 2.2.2.2/32
R3-2 = 2.3.3.3/32
R4-2 = 2.4.4.4/32
R5-2 = 2.5.5.5/32
R6-2 = 2.6.6.6/32
R7-2 = 2.7.7.7/32
R8-2 = 2.8.8.8/32
R9-2 = 2.9.9.9/32
R10-2 = 2.10.10.10/32
R11-2 = 2.11.11.11/32
R12-2 = 2.12.12.12/32
R13-2 = 2.13.13.13/32
R14-2 = 2.14.14.14/32
R15-2 = 2.15.15.15/32
R16-2 = 2.16.16.16/32
R17-2 = 2.17.17.17/32
R18-2 = 2.18.18.18/32
R19-2 = 2.19.19.19/32
R20-2 = 2.20.20.20/32

Router ID = Loopback

ПРИЛОЖЕНИЕ Г

Диаграмма маршрутизации

