



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

**Институт информационных технологий (ИИТ)
Кафедра практической и прикладной информатики (ППИ)**

Утверждаю

Заведующий кафедрой ППИ
студент Зуев А.С.
(подпись)
«21» сентября 2023 г.

**ЗАДАНИЕ
на выполнение курсовой работы
по дисциплине «Технологии передачи данных»**

Студент Дерцян Нарек Аренович

Группа ИВБО-06-21

Тема «Проектирование и моделирование сервисной сети передачи данных на примере предприятия, осуществляющего закупку воды в больших емкостях с последующим разливом в мелкую тару без переработки»

Исходные данные:

	Параметр предприятия	Значение
1.	Количество сотрудников в основном здании	90
2.	Количество сотрудников в филиале	0
3.	Количество филиалов	0
4.	Количество точек присутствия	0
5.	Количество сотрудников в точке присутствия	0
6.	Количество сотрудников на складе	30
7.	Количество складов	1
8.	Перечень сетевых служб предприятия:	
8.1.	Служба доменных имен	DNS
8.2.	Служба динамического конфигурирования хостов	DHCP
8.3.	Веб-служба	Apache
8.4.	Служба времени	NTP
8.5.	Файловая служба	NFS
8.6.	Служба управления пользователями	FreeIPA

Исходные данные могут уточняться при разработке разделов курсовой работы и составлении соответствующих спецификаций.

Перечень вопросов, подлежащих разработке, и обязательного графического материала:

1. Выполнить проектирование сервисной сети передачи данных, в том числе:
 - 1.1. Определить структуру предприятия.
 - 1.2. Выполнить расчёт пропускной способности каналов передачи данных.
 - 1.3. Разработать прототип сети передачи данных.
 - 1.4. Выполнить планирование канального уровня сети.
 - 1.5. Выполнить планирование сетевого уровня сети.
 - 1.6. Определить параметры политик фильтрации трафика.
 - 1.7. Определить параметры политик обеспечения качества обслуживания.
 - 1.8. Выполнить планирование службы доменных имен.
 - 1.9. Выполнить планирование внедрения службы динамического конфигурирования хостов.
 - 1.10. Выполнить планирование других сетевых служб, в том числе: файловой службы, службы времени, службы управления пользователями.
 - 1.11. Определить и провести расчет сервисной нагрузки по результатам планирования.
 - 1.12. Разработать топологию сети передачи данных с учетом проведенного планирования.
2. Выполнить моделирование сети с использованием соответствующих средств моделирования и представить артефакты данного процесса.
3. Разработать презентацию с графическими материалами.

Срок представления к защите курсовой работы:

до «15» декабря 2023 г.

Задание на курсовую работу выдал



Подпись руководителя

Зуев А.С.

(ФИО руководителя)

«21» сентября 2023 г.

Задание на курсовую работу получил



Подпись обучающегося

Дерцян Н.А.

(ФИО обучающегося)

«21» сентября 2022 г.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ	6
1 ПЛАНИРОВАНИЕ И ПРОЕКТИРОВАНИЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ	
6	
1.1 Определение структуры предприятия	7
1.2 Расчет пропускной способности каналов передачи данных	8
1.3 Прототипирование сети	13
1.4 Планирование сети уровня 2	18
1.5 Планирование сети уровня 3	23
1.6 Планирование политик фильтрации трафика	28
1.7 Планирование политик обеспечения качества обслуживания	29
1.8 Планирование службы доменных имен	30
1.9 Планирование политик управления пользователями	32
1.10 Планирование внедрения DHCP-сервера	33
1.11 Планирование других сетевых служб	34
1.12 Определение и расчет сервисной нагрузки	36
1.13 Итоговое планирование	44
2 МОДЕЛИРОВАНИЕ СЕТИ	45
2.1 Моделирование сервисов	46
2.2 Моделирование сети передачи данных	53
ЗАКЛЮЧЕНИЕ	60
СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ	61
ПРИЛОЖЕНИЯ	62

ВВЕДЕНИЕ

В современном мире технологии сервисной передачи данных играют значительную роль в повседневной жизни и деятельности организаций. В частности, для предприятий, осуществляющих закупку воды в больших емкостях и последующий разлив в мелкие тары без переработки, эффективная сервисная сеть передачи данных является важным условием успешной и стабильной работы.

Актуальность данной темы обусловлена быстрым ростом объемов передаваемой информации и необходимостью внедрения современных технологий в процессе проектирования сервисных сетей передачи данных. Важность исследования заключается в возможности определения оптимального подхода к проектированию сервисной сети передачи данных для улучшения эффективности работы предприятия.

Объектом исследования является сервисная сеть передачи данных, предметом исследования — особенности проектирования и реализации сервисной сети передачи данных на примере предприятия, занимающегося закупкой и разливом воды. Цель работы состоит в планировании и реализации сервисной сети передачи данных, обеспечивающей эффективное функционирование предприятия.

Для достижения поставленной цели, в рамках работы предполагается решение следующих задач:

1. Проанализировать исходные данные в поставленной задаче;
2. Провести планирование адресации и маршрутизации сети передачи данных, разделение на виртуальные и локальные сети;
3. Провести прототипирование сети передачи данных;
4. Выполнить планирование таких служб, как файловая, служба времени, службы управления пользователями;
5. Провести расчет сервисной нагрузки по результатам планирования;
6. Провести настройку и тестирование сети передачи данных.

Инструментальными средствами исследования выступают программные

инструменты, такие как Cisco Packet Tracer, Apache, которые позволяют моделировать и тестировать сетевые архитектуры.

Основными источниками информации для работы станут научные публикации, учебники и интернет-ресурсы, посвященные технологиям передачи данных, сетевому проектированию и планированию.

Основное содержание работы будет состоять из следующих разделов:

1. Обзор теоретических основ и современных технологий передачи данных, их применение в процессе проектирования сетей для предприятий различных масштабов и отраслей;
2. Изучение специфики деятельности предприятия, анализ требований к сети сервисной передачи данных;
3. Разработка схемы адресации и маршрутизации сети передачи данных с учетом исходных данных и требований предприятия;
4. Проектирование виртуальных и локальных сетей для оптимального разделения и обеспечения безопасности передачи данных;
5. Создание прототипа сети передачи данных с использованием инструментария Cisco Packet Tracer для проверки корректности проектирования и определения возможных узких мест и проблем;
6. Выполнение планирования файловых сетевых, служб времени, служб управления пользователями;
7. Настройка и тестирование сети сервисной передачи данных на предприятии, оценка ее работоспособности и эффективности;
8. Проведение расчетов для определения сервисной нагрузки по результатам планирования;
9. Разработка рекомендаций по улучшению процесса проектирования сетей передачи данных и дальнейшего развития инфраструктуры предприятия.

В результате проведенного исследования, будет предложено оптимальное решение по проектированию сети сервисной передачи данных для предприятия, осуществляющего закупку и разлив воды, что позволит обеспечить стабильную работу в долгосрочной перспективе.

СОКРАЩЕНИЯ

АРМ — Автоматизированное Рабочее Место
VLAN (Virtual Local Area Network) — Виртуальная локальная сеть
STP (Spanning Tree Protocol) — Протокол связующего дерева
RSTP (Rapid Spanning Tree Protocol) — Быстрый протокол связующего дерева
ПК — Персональный Компьютер
ИТ — Информационные технологии
IP (Internet Protocol) — Интернет Протокол
VID (Vlan Identifier) — Идентификатор VLAN
PVID — Port Virtual Local Area Network Identifier
BPDU — Bridge Protocol Data Unit
DNS (Domain Name Server) — Сервер доменных имен
LDAP — Lightweight Directory Access Protocol
NTP — Network Time Protocol
NFS — Network File System
SSH — Secure Shell
GE — Gigabit Ethernet
FE — Fast Ethernet

1 ПЛАНИРОВАНИЕ И ПРОЕКТИРОВАНИЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ

1.1 Определение структуры предприятия

Описываемое предприятие состоит из офиса и одного склада. На рисунке 1.1 в виде диаграммы изображена организационная структура предприятия для точного представления распределения работников предприятия. Так же на диаграмме показаны отделы предприятия, которые в будущем будут разделены на подсети. На рисунках ниже обозначения 2+2 и 3+3 обозначают посменную работу.

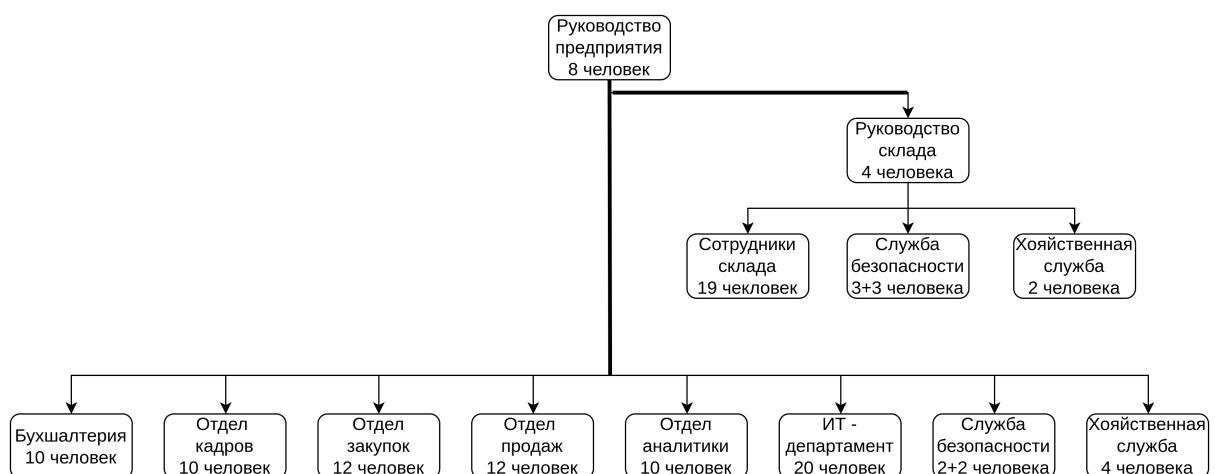


Рисунок 1.1 — Организационная структура предприятия

В основном здании предприятия всего 90 сотрудников, так как а службе охраны и хозяйственной службе в АРМ нуждается не каждый сотрудник и так же с учетом посменной работы, по итоговым расчетом в основном здании достаточно 84 АРМ.

Структура основного здания и склада предприятия по количеству рабочих мест изображена на Рисунках 1.2-1.3.

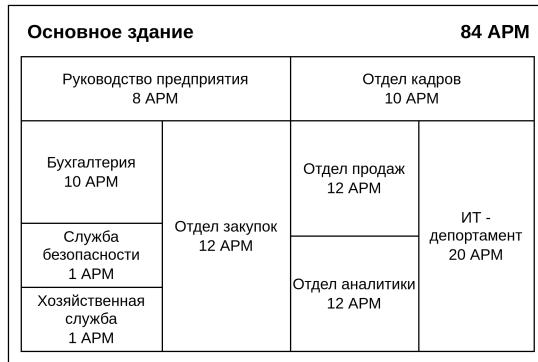


Рисунок 1.2 — Количество рабочих мест в основном здании

На складе всего 30 сотрудников из которых 19 сотрудников это кладовщики, которые не нуждаются в АРМ. Охранной службе достаточно одного АРМ главному по смене сотруднику. Также достаточно одного АРМ для хозяйственной службы для учета выполненной работы.



Рисунок 1.3 — Количество рабочих мест на складе

Для всех отделов, основного здания и склада, количество АРМ совпадает с количеством сотрудников, кроме хозяйственной службы, где только заведующий по хозяйству имеет АРМ и службы охраны, которая работает посменно и рабочее место есть только у 1 сотрудника.

1.2 Расчет пропускной способности каналов передачи данных

В данном пункте будет производится расчет пропускной способности каналов передачи данных с учетом применения трехуровневой архитектуры сети, состоящей из уровня доступа, агрегации ядра.

Расчеты по количеству портов будут выполняться снизу вверх. На уровне доступа количество портов соответствует количеству терминалов с проводным подключением а так же количеству точек доступа, принтеров, IP-телефонов, IP-камер и других устройств[1].

Скоростные требования к портам для обычных конечных пользователей будет 100 Мбит/с и 1 Гбит/с для конечных пользователей с особыми требованиями, таких как начальство. Так же будет требование 1 Гбит/с к портам для сервера. Количество АРМ и требования к каналу передачи данных для основного здания и склада представлены в Таблицах 1.1- 1.2. Обозначение $100 \times 15 + 1000 \times 5$ обозначает, что из общего количества АРМ 15 АРМ требуют канал передачи 100 Мбит/с и 5 АРМ 1000 Мбит/с, так же для склада.

Таблица 1.1 — Требования к каналу передачи данных основного здания

Название отдела	Количество АРМ	Требования к каналу передачи данных, Мбит/с	Конечная нагрузка на отдел, Мбит/с
Руководство предприятия	8	1000	8000
Бухгалтерия	10	100	1000
Отдел кадров	10	100	1000
Отдел закупок	12	100	1200
Отдел продаж	12	100	1200
Отдел аналитики	10	100	1000
ИТ-департамент	20	$100 \times 15 + 1000 \times 5$	6500
Служба безопасности	1	100	100
Хозяйственная служба	1	100	100
Итого:			20100

Таблица 1.2 — Требования к каналу передачи данных склада

Название отдела	Количество АРМ	Требования к каналу передачи данных, Мбит/с	Конечная нагрузка на отдел, Мбит/с
Руководство склада	4	$100 \times 3 + 1000 \times 1$	1300
Служба безопасности	1	100	100
Хозяйственная служба	1	100	100
Итого:			1500

Итоговое количество портов полученное на уровне доступа для

основного здания 102 с учетом точек доступа, принтеров и ip-телефонов. Было определено, что из них 89 портов FastEthernet и 13 портов GigabitEthernet. Для склада на уровне доступа количество портов составляет 19, с учетом устройств требующих проводное подключение. Было определено, что 18 портов FastEthernet и 1 порт GigabitEthernet. Далее с известным количеством карт на уровне доступа рассчитывается количество портов на уровне агрегации.

Для расчета количества портов на уровне агрегации исходя из данных уровня доступа необходимо учесть коэффициент перехода. Данный коэффициент рассчитывается из условия требований для узлов, например, для конечных проводных компьютеров данный коэффициент будет равен 40%, так как узлы не будут постоянно использовать весь канал передачи данных из-за того, что основным сервисом является программное обеспечение 1С: Документооборот, которое не требует особых требований к постоянному широкополосному каналу передачи данных. С другой стороны сервера, подключенные по GigabitEthernet будут тратить более 90% постоянно по причине развертывания на них различных сервисов, в том числе сервера 1С:Документооборот, к которому будут обращаться конечные пользователи при решении своих задач. В данном расчете для серверов будет взят коэффициент 100%, а для конечных узлов 40%.

На основе произведенных выше расчетов и таблиц более полный расчет портов на уровне доступа основного здания и склада будет выглядеть следующим образом (Таблицы 1.3 - 1.5).

Таблица 1.3 — Расчет портов уровня доступа для основного здания

Название отдела	Количество АРМ	Требования к каналу передачи данных, Мбит/с	Суммарные требования на отдел, Мбит/с	Портов GigabitEthernet	Портов FastEthernet
Руководство предприятия	8	1000	8000	8	0
Бухгалтерия	10	100	1000	0	10
Отдел кадров	10	100	1000	0	10
Отдел закупок	12	100	1200	0	12

Таблица 1.4 — Продолжение таблицы 1.3

Название отдела	Количество АРМ	Требования к каналу передачи данных, Мбит/с	Суммарные требования на отдел, Мбит/с	Портов GigabitEthernet	Портов FastEthernet
Отдел продаж	12	100	1200	0	12
Отдел аналитики	10	100	1000	0	10
ИТ-департамент	20	100x15 1000x5	6500	5	15
Служба безопасности	1	100	100	0	1
Хозяйственная служба	1	100	100	0	1
Итого	84	—		13	71

Таблица 1.5 — Расчет портов уровня доступа для склада

Название отдела	Количество АРМ	Требования к каналу передачи данных, Мбит/с	Суммарные требования на отдел, Мбит/с	Портов GigabitEthernet	Портов FastEthernet
Руководство склада	4	3x100 1x1000	1300	1	3
Служба безопасности	1	100	100	0	1
Хозяйственная служба	1	100	100	0	1
Итого	6	—		1	4

Для расчетов подключения конечных устройств будет взят коэффициент 40% для перехода на уровень агрегации по причине того, что будут использоваться приложения не сильно чувствительные к задержкам и потерям. Итого расчеты представлены в Таблице 1.6. Для склада представлены расчеты только для уровня ядра в силу отсутствия уровня агрегации в Таблице 1.8. Следует учитывать, что производится резервирование. Объем трафика при переходе с уровня агрегации на уровень ядра не меняется. Поэтому количество портов на уровне ядра считается по объему трафика на уровне агрегации.

Через знак ‘+’ указываются порты, которые являются резервными и будут использованы для предотвращения проблем при выходе из строя основного порта.

Таблица 1.6 — Расчет портов на уровне агрегации основного здания

Название отдела	Суммарные требования на отдел, Мбит/с	Объем трафика при переходе на уровень агрегации Мбит/с	Количество портов на уровне агрегации, GigabitEthernet
Руководство предприятия	8000	3200	4+1
Бухгалтерия	1000	400	1+1
Отдел кадров	1000	400	1+1
Отдел закупок	1200	480	1+1
Отдел продаж	1200	480	1+1
Отдел аналитики	1000	400	1+1
ИТ-департамент	6500	2600	3+1
Служба безопасности	100	40	1+1
Хозяйственная служба	100	40	1+1
Итого	-	8080	24

Исходя из данных таблицы расчета портов на уровне агрегации, для уровня ядра требуется минимум 9 портов GigabitEthernet в основном здании. Данные по количеству требуемых портов с учетом резервирования представлены в Таблице 1.7.

Таблица 1.7 — Общее количество портов для основного здания

Уровень	Порты GigabitEthernet	порты FastEthernet
Доступ	16	89
Агрегация	24	—
ядро	9	—

Таблица 1.8 — Расчет портов на уровне ядра склада

Название отдела	Суммарные требования на отдел, Мбит/с	Объем трафика на уровне ядра Мбит/с	Количество портов на уровне ядра, GigabitEthernet
Руководство склада	1300	520	1+1

Таблица 1.9 — Продолжение Таблицы 1.8

Название отдела	Суммарные требования на уровне ядра Мбит/с	Объем трафика на уровне ядра Мбит/с	Количество портов на уровне ядра, GigabitEthernet
Служба безопасности	100	40	1+1
Хозяйственная служба	100	40	1+1
Итого	-	600	6

Для склада требуется 19 портов на уровне доступа. Исходя из этого для склада можно опустить уровень агрегации и использовать только устройства уровня ядра. По приведенной выше формуле с учетом коэффициента перехода на уровне ядра для склада требуется пропускная способность в 600 Мбит/с. Для склада на уровне ядра требуется 1 порт GigabitEthernet (Таблица 1.10).

Таблица 1.10 — Общее количество портов для склада

Уровень	Порты GigabitEthernet	порты FastEthernet
Доступ	1	18
Агрегация	—	—
ядро	6	—

Расчеты выведенные в таблицах выше являются предварительными для построения первого чернового прототипа и выбора устройств для использования и не учитывают резервирование линков.

1.3 Прототипирование сети

На данном шаге будет создан прототип сети с учетом предварительного планирования количества портов, политик резервирования, добавления сервера для развертывания программной инфраструктуры предприятия, трехуровневой архитектуры сети, полученных в предыдущем пункте. При формировании прототипа будет использоваться программное обеспечение draw.io и нотации cisco.

В Таблицах 1.13 - 1.11 описаны спецификации промежуточных устройств основного здания. На ней описывается какие порты и устройства

используются. Для сети главного здания используются маршрутизатор 4331, так как имеет 3 порта GigabitEthernet, что является необходимым количеством для соединения с коммутаторами L3, коммутаторы L3 3650 24PS с 24 портами GigabitEthernet для соединения с коммутаторами L2 и коммутаторы 2960 с 24 портами FastEthernet для соединения с конечными устройствами. На скеле же используются коммутаторы 2950T-24 с 24 портами FastEthernet для соединения с конечными устройствами и маршрутизатор 1240. В перечисленных устройствах модули расширения не будут использоваться, кроме маршрутизатора. Считается, что порты 0/0/1 и 0/0/2 маршрутизатора и порты 1/0/2 коммутаторов SW_1-2_L3_DERDZYAN имеют пропускную способность в 10 GigabitEthernet. В качестве конечных узлов в основном здании выступают персональные компьютеры. На Рисунках 1.4 - 1.5 изображена топология сети основного здания на основе Таблиц 1.13 - 1.11. Так как руководству и ИТ-департаменту требуется довольно большая пропускная способность каналов для них между коммутаторами L3 и коммутатором L2 организованы агрегирование каналов[2], которые позволяют увеличить пропускную способность между участниками сети и способствуют отказоустойчивости.

Таблица 1.11 — Спецификации промежуточных устройств прототипа основного здания

Модель устройства	Имя устройства	Общее количество портов	Используемые порты (названия, количество)	Свободные порты (названия, количество)
Маршрутизатор 4331	R_1_DERDZYAN	3 порта GigabitEthernet	0/0/0 - 0/0/2	—
Коммутатор L3 3650 24PS	SW_1_L3_DERDZYAN	24 порта GigabitEthernet	1/0/1 - 1/0/15	1/0/16 - 1/0/24
Коммутатор L3 3650 24PS	SW_2_L3_DERDZYAN	24 порта GigabitEthernet	1/0/1 - 1/0/14	1/0/15 - 1/0/24
Коммутатор L3 3650 24PS	SW_3_L3_DERDZYAN	24 порта GigabitEthernet	1/0/1 - 1/0/4	1/0/5 - 1/0/24
Коммутатор L3 3650 24PS	SW_1_L2_DERDZYAN	24 порта GigabitEthernet	1/0/1 - 1/0/13	1/0/14 - 1/0/24

Таблица 1.12 — Продолжение Таблицы 1.11

Модель устройства	Имя устройства	Общее количество портов	Используемые порты (названия, количество)	Свободные порты (названия, количество)
Коммутатор 2960	SW_2_L2_DERDZYAN	2 порта GigabitEthernet, 24 порта FastEthernet	FastEthernet 0/1 - 0/10, GigabitEthernet 0/1 - 0/2	FastEthernet 0/11 - 0/24
	SW_3_L2_DERDZYAN	2 порта GigabitEthernet, 24 порта FastEthernet	FastEthernet 0/1 - 0/10, GigabitEthernet 0/1 - 0/2	FastEthernet 0/11 - 0/24
	SW_4_L2_DERDZYAN	2 порта GigabitEthernet, 24 порта FastEthernet	FastEthernet 0/1 - 0/12, GigabitEthernet 0/1 - 0/2	FastEthernet 0/13 - 0/24
	SW_5_L2_DERDZYAN	2 порта GigabitEthernet, 24 порта FastEthernet	FastEthernet 0/1 - 0/12, GigabitEthernet 0/1 - 0/2	FastEthernet 0/13 - 0/24
	SW_6_L2_DERDZYAN	2 порта GigabitEthernet, 24 порта FastEthernet	FastEthernet 0/1 - 0/10, GigabitEthernet 0/1 - 0/2	FastEthernet 0/11 - 0/24
Коммутатор L3 3650 24PS	SW_7_L2_DERDZYAN	24 порта GigabitEthernet	GigabitEthernet 1/0/1 - 1/0/24	—
Коммутатор 2960	SW_8_L2_DERDZYAN	2 порта GigabitEthernet, 24 порта FastEthernet	FastEthernet 0/1, GigabitEthernet 0/1 - 0/2	FastEthernet 0/2 - 0/24
	SW_9_L2_DERDZYAN	2 порта GigabitEthernet, 24 порта FastEthernet	FastEthernet 0/1, GigabitEthernet 0/1 - 0/2	FastEthernet 0/2 - 0/24

Таблица 1.13 — Спецификации промежуточных устройств прототипа склада

Модель устройства	Имя устройства	Общее количество портов	Используемые порты (названия, количество)	Свободные порты (названия, количество)
Маршрутизатор 1941	R_1_DERDZYAN	2 порта GigabitEthernet	GigabitEthernet 0/0/1	GigabitEthernet 0/0/2
Коммутатор 2950T-24	SW_1_L3_DERDZYAN	24 порта FastEthernet, 2 порта GigabitEthernet	GigabitEthernet 1/0/1 - 1/0/2, FastEthernet 1/0/1 - 1/0/5	FastEthernet 0/6 - 0/24

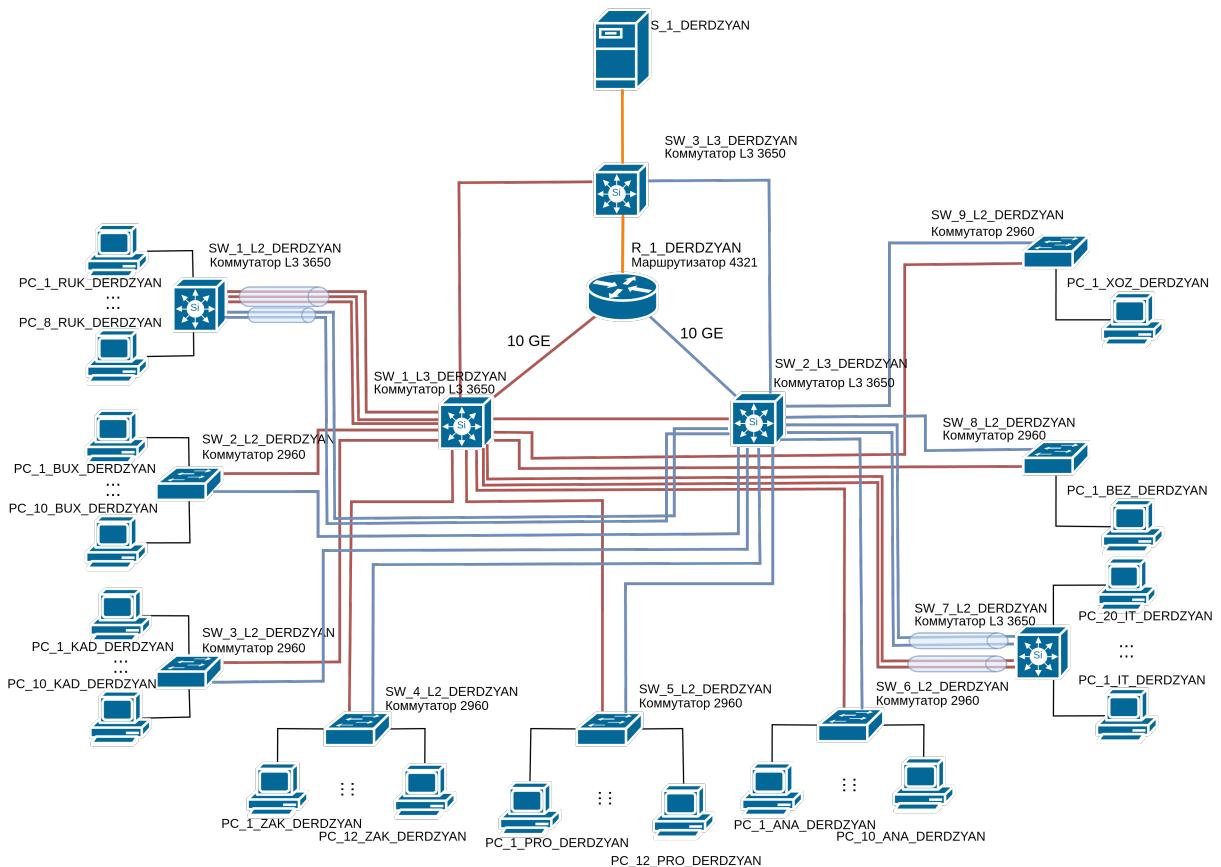


Рисунок 1.4 — Проектирование топологии сети основного здания

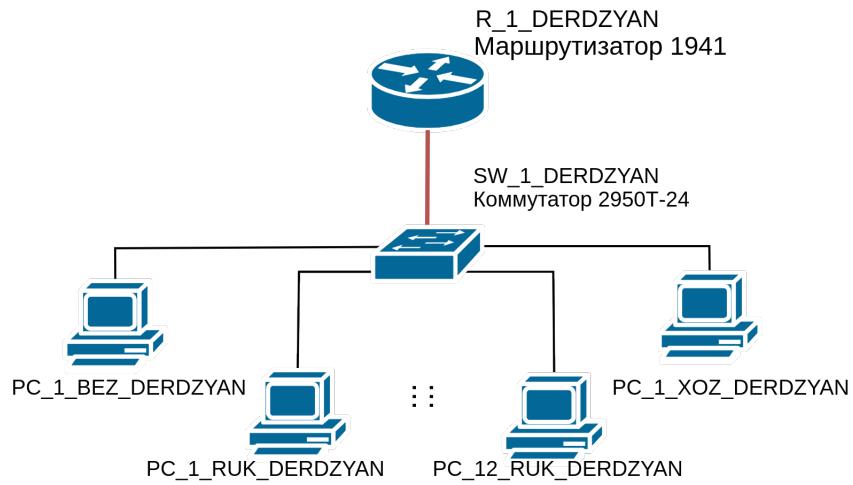


Рисунок 1.5 — Проектирование топологии сети склада

В Таблицах 1.14 - 1.16 представлен план подключения промежуточных устройств в основном здании и складе по портам.

Таблица 1.14 — План подключения оборудования по портам для основного здания

Название устройства	Порт	Описание подключения
R_1_DERDZYAN	GigabitEthernet 0/0/1 - 0/0/3	SW_1-3_L3_DERDZYAN
SW_1_L3_DERDZYAN	GigabitEthernet 1/0/2	R_1_DERDZYAN
	GigabitEthernet 1/0/1, 1/0/3	SW_2-3_L3_DERDZYAN
	GigabitEthernet 1/0/4 - 1/0/15	SW_1-9_L2_DERDZYAN
SW_2_L3_DERDZYAN	GigabitEthernet 1/0/2	R_1_DERDZYAN
	GigabitEthernet 1/0/1, 1/0/3	SW_1, 3_L3_DERDZYAN
	GigabitEthernet 1/0/4 - 1/0/14	SW_1-9_L2_DERDZYAN
SW_3_L3_DERDZYAN	GigabitEthernet 1/0/3	R_1_DERDZYAN
	GigabitEthernet 1/0/2, 1/0/4	SW_1-2_L3_DERDZYAN
	GigabitEthernet 1/0/1	S_1_DERDZYAN
SW_1_L2_DERDZYAN	GigabitEthernet 1/0/1 - 1/0/3	SW_1_L3_DERDZYAN
	GigabitEthernet 1/0/4 - 1/0/6	SW_2_L3_DERDZYAN
	GigabitEthernet 1/0/7 - 1/0/15	PC_1-8_RUK_DERDZYAN
SW_2_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_DERDZYAN
	FastEthernet 0/1 - 0/10	PC_1-10_BUX_DERDZYAN
SW_3_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_DERDZYAN
	FastEthernet 0/1 - 0/10	PC_1-10_KAD_DERDZYAN
SW_4_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_DERDZYAN
	FastEthernet 0/1 - 0/12	PC_1-12_ZAK_DERDZYAN
SW_5_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_DERDZYAN
	FastEthernet 0/1 - 0/10	PC_1-10_PRO_DERDZYAN

Таблица 1.15 — Продолжение Таблицы 1.14

Название устройства	Порт	Описание подключения
SW_6_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_DERDZYAN
	FastEthernet 0/1 - 0/10	PC_1-10_ANA_DERDZYAN
SW_7_L2_DERDZYAN	GigabitEthernet 1/0/1 - 1/0/4	SW_1-2_L3_DERDZYAN
	GigabitEthernet 1/0/5 - 1/0/24	PC_1-20_IT_DERDZYAN
SW_8_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_DERDZYAN
	FastEthernet 0/1	PC_1_BEZ_DERDZYAN
SW_9_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_DERDZYAN
	FastEthernet 0/1	PC_1_XOZ_DERDZYAN

Таблица 1.16 — План подключения оборудования по портам для склада

Название устройства	Порт	Описание подключения
R_1_DERDZYAN	GigabitEthernet 0/0/1	SW_1_DERDZYAN
SW_1_DERDZYAN	FastEthernet 1/0/1	PC_1_BEZ_DERDZYAN
	FastEthernet 1/0/2	PC_1_XOZ_DERDZYAN
	GigabitEthernet 1/0/3	PC_1_RUK_DERDZYAN
	FastEthernet 1/0/4 - 1/0/6	PC_2-4_RUK_DERDZYAN

1.4 Планирование сети уровня 2

Данный этап планирования предназначен для уровня 2 — проектирование виртуальных локальных сетей (VLAN). Виртуальные локальные сети разделены на сервисные VLAN, управляющие VLAN и взаимосвязанные VLAN. VLAN позволяет создавать виртуальные группы устройств, которые могут взаимодействовать друг с другом, независимо от их физического расположения в сети.

Использование технологии VLAN[3] позволяет предприятиям более гибко и эффективно управлять своей сетью, сокращать затраты на физические маршрутизаторы и обеспечивать лучшую изоляцию и безопасность для различных частей сети.

При проектировании сервисной локальной сети учитывается, что она предназначена для обеспечения доступности сервисов для пользователей. Приведенные VLAN назначены на основе логических областей и по типу услуг разных отделов предприятия.

Управляющий VLAN используется для удаленного доступа к устройствам и управления ими. Коммутаторы уровня 2 используют адреса виртуального интерфейса VLAN в качестве адресов управления. Все коммутаторы одной сети уровня 2 используют одну и ту же управляющую VLAN, а их IP-адреса управления находятся в одном сегменте сети. Взаимосвязанные VLAN нужны для соединения устройств при переходе с уровня агрегации на уровень ядра.

1. Управляющая VLAN зарезервирована для устройств уровня 2;
2. Сеть VLAN подразделяется на гостевую VLAN и так же для каждого отдела предприятия отдельный VLAN;
3. Коммутаторы уровня 3 подключены к маршрутизаторам через интерфейс VLANIF используя взаимосвязанный VLAN.

Результат планирования VLAN представлен в Таблице 1.17.

Таблица 1.17 — Результат планирования VLAN для основного здания

Идентификатор VLAN (VID)	Имя VLAN	Описание
2	Management_L2	Управляющая VLAN устройств уровня 2
3	Interconnected_1	Взаимосвязанная VLAN между SW_1_L3_DERDZYAN и R_1_DERDZYAN
4	Interconnected_2	Взаимосвязанная VLAN между SW_2_L3_DERDZYAN и R_1_DERDZYAN
5	Interconnected_3	Взаимосвязанная VLAN между SW_3_L3_DERDZYAN и R_1_DERDZYAN
101	Admin	Руководство предприятия
102	Accaunting	Бухгалтерия
103	HR	Отдел кадров
104	Purchasing	Отдел закупок
105	Sales	Отдел продаж
106	Analytics	Отдел аналитики
107	IT	ИТ — департамент

Таблица 1.18 — Продолжение Таблицы 1.17

Идентификатор VLAN (VID)	Имя VLAN	Описание
108	Security	Служба безопасности
109	Service	Хозяйственная безопасность
111	Server	VLAN для сервера

Ниже представлена таблица с описанием устройств их портов и привязкой к виртуальным локальным сетям (Таблица 1.19). Access port или порт доступа — порт, находящийся в определенном VLAN и передающий не тегированные кадры. Как правило, это порт, смотрящий на пользовательское устройство. Trunk port или магистральный порт — порт, передающий тегированный трафик. Как правило, этот порт поднимается между сетевыми устройствами. Для маршрутизатора в поле access указаны отношения коммутатора и его взаимосвязанный VLAN.

Таблица 1.19 — План виртуальных локальных сетей по портам для основного здания

Название устройства	Порт	Описание подключения	VLAN	
			Access	Trunk
R_1_DERDZYAN	GigabitEthernet 0/0/1 - 0/0/3	SW_1-3_L3_ DERDZYAN	3-5	
SW_1_L3_ DERDZYAN	GigabitEthernet 1/0/2	R_1_ DERDZYAN	3	
	GigabitEthernet 1/0/1, 1/0/3	SW_2-3_L3_ DERDZYAN		101 - 109, 111
	GigabitEthernet 1/0/4 - 1/0/12	SW_1-9_L2_ DERDZYAN		101 - 109, 111
SW_2_L3_ DERDZYAN	GigabitEthernet 1/0/2	R_1_ DERDZYAN	4	
	GigabitEthernet 1/0/1, 1/0/3	SW_1, 3_L3_ DERDZYAN		101 - 109, 111
	GigabitEthernet 1/0/4 - 1/0/12	SW_1-9_L2_ DERDZYAN		101 - 109, 111
SW_3_L3_ DERDZYAN	GigabitEthernet 1/0/3	R_1_ DERDZYAN	5	
	GigabitEthernet 1/0/2, 1/0/4	SW_1-2_L3_ DERDZYAN		101 - 109, 111
	GigabitEthernet 1/0/1	S_1_ DERDZYAN		101 - 109, 111

Таблица 1.20 — Продолжение Таблицы 1.19

Название устройства	Порт	Описание подключения	VLAN	
			Access	Trunk
SW_1_L2_DERDZYAN	GigabitEthernet 1/0/1 - 1/0/3	SW_1_L3_ DERDZYAN		2, 101-109, 111
	GigabitEthernet 1/0/4 - 1/0/5	SW_2_L3_ DERDZYAN		2, 101-109, 111
	GigabitEthernet 1/0/6 - 1/0/13	PC_1-8_RUK_ DERDZYAN	102	
SW_2_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_ DERDZYAN		2, 101 - 109, 111
	FastEthernet 0/1 - 0/10	PC_1-10_BUX_ DERDZYAN	103	
SW_3_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_ DERDZYAN		2, 101 - 109, 111
	FastEthernet 0/1 - 0/10	PC_1-10_KAD_ DERDZYAN	104	
SW_4_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_ DERDZYAN		2, 101 - 109, 111
	FastEthernet 0/1 - 0/12	PC_1-12_ZAK_ DERDZYAN	105	
SW_5_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_ DERDZYAN		2, 101 - 109, 111
	FastEthernet 0/1 - 0/10	PC_1-10_PRO_ DERDZYAN	106	
SW_6_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_ DERDZYAN		2, 101 - 109, 111
	FastEthernet 0/1 - 0/10	PC_1-10_ANA_ DERDZYAN	107	
SW_7_L2_DERDZYAN	GigabitEthernet 1/0/1 - 1/0/4	SW_1-2_L3_ DERDZYAN		2, 101 - 109, 111
	GigabitEthernet 1/0/5 - 1/0/24	PC_1-20_IT_ DERDZYAN	108	
SW_8_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_ DERDZYAN		2, 101 - 109, 111
	FastEthernet 0/1	PC_1_BEZ_ DERDZYAN	109	

Таблица 1.21 — Продолжение Таблицы 1.19

Название устройства	Порт	Описание подключения	VLAN	
			Access	Trunk
SW_9_L2_DERDZYAN	GigabitEthernet 0/1 - 0/2	SW_1-2_L3_DERDZYAN		2, 101 - 109, 111
	FastEthernet 0/1	PC_1_XOZ_DERDZYAN	110	

Для предотвращения петель уровня 2 в основном здании используется протокол связующего дерева[4] (STP), а в частности его модификация под названием RSTP (Rapid Spanning Tree Protocol), который в рамках устройств “Cisco” называется rapid-pvst. RSTP в основном отличается от STP своей ускоренной работой, то на перестройку топологии в случае отказа какого либо порта или коммутатора понадобится меньше времени, так же в RSTP в отличие от STP все свичи шлют BPDU (Bridge Protocol Data Unit).

Принцип работы RSTP - выбирается корневой коммутатор (root switch), затем каждый коммутатор, участвующий в построении дерева, ищет кратчайший маршрут (с учётом пропускной способности канала) к корневому коммутатору через соседние коммутаторы (или напрямую). Линии, не попавшие в маршрут, переводятся в режим ожидания и не используются для передачи данных, пока работают основные линии. В случае выхода из строя основных линий, ожидающие линии используются для построения альтернативной топологии, после чего одна из линий становится активной, а остальные продолжают находиться в режиме ожидания.

В конфигурации RSTP достаточно настроить SW_1_L3_DERDZYAN настроить как корневой мост, а SW_2_L3_DERDZYAN как вторичный и в начале работы RSTP выключит порт соединяющий эти коммутаторы, что и предотвратит появление петель второго уровня. Данный линк сделан для того, чтобы в случае, если какие то порты одного из коммутаторов выйдут из строя другой коммутатор при помощи пакетов BPDU узнал об этом без посредников.

1.5 Планирование сети уровня 3

Для выбора диапазона частных адресов в Таблице 1.22 представлены параметры сети главного здания предприятия. В Таблице используются такие параметры, как количество подсетей, что является значимым фактором в процессе планирования и проектирования сетевой архитектуры. Оно отражает сумму независимых сегментов сети, каждый из которых может быть управляем и конфигурирован независимо. Количество бит для номера подсети определяет уникальный идентификатор, присвоенный каждой подсети в рамках глобальной сети. Количество этих бит может варьироваться в зависимости от требований к сети и выбранной схемы адресации. Максимальное количество узлов относится к максимальному количеству устройств, которые могут быть связаны внутри одной подсети. Этот параметр напрямую зависит от количества бит, выделенных для узловой части IP-адреса. Большее количество бит для узловой части позволяет подключить больше устройств к подсети, в то время как меньшее количество бит может ограничить возможное количество узлов. Минимальное количество бит для узловой части является наименьшим количеством бит, которые могут быть использованы для идентификации узла в подсети. Этот параметр обычно определяется требованиями к сети и выбранной схемой адресации. Минимальное количество бит для узловой части важно для обеспечения эффективного использования адресного пространства и соблюдения требований к сетевой производительности и безопасности.

Так же стоит учесть, что сеть разбита на подсети по принципу изолирования отделов.

Таблица 1.22 — Параметры сети основного здания

Описание	Количество
Количество подсетей	9
Количество бит для номера подсети	3
Максимальное количество узлов	20
Минимальное количество бит для узловой части	7

Исходя из требований для внутренних локальных сетей в основном выбран диапазона частных адресов класса «С» от 192.168.0.0 до

192.168.255.255.

Для IP-адресов используется следующая классификация:

1. Сервисные адреса;
2. Управляющие адреса;
3. Для подключения сетевых устройств.

Результат планирования и распределения IP-адресов представлен в Таблице 1.23.

Таблица 1.23 — Планирование адресации основного здания

Сегмент/маска IP-сети	Адрес шлюза	Описание сегмента сети
192.168.2.0/24	192.168.2.254	Сегмент управляющей сети для устройств уровня 2 со шлюзом, расположенным на коммутаторе уровня агрегации.
192.168.3.0/30	—	Первый сегмент сети между ядром и уровнем агрегации
192.168.4.0/30	—	Второй сегмент сети между ядром и уровнем агрегации
192.168.5.0/30	—	Третий сегмент сети между ядром и уровнем агрегации
192.168.101.0/24	192.168.101.254	Сегмент сети, к которому относится руководство, со шлюзом, расположенным на коммутаторе уровня агрегации.
192.168.102.0/24	192.168.102.254	Сегмент сети, к которому относится бухгалтерия, со шлюзом, расположенным на коммутаторе уровня агрегации.
192.168.103.0/24	192.168.103.254	Сегмент сети, к которому относится отдел кадров, со шлюзом, расположенным на коммутаторе уровня агрегации.

Таблица 1.24 — Продолжение таблицы 1.23

Сегмент/маска IP-сети	Адрес шлюза	Описание сегмента сети
192.168.104.0/24	192.168.104.254	Сегмент сети, к которому относится отдел закупок, со шлюзом, расположенным на коммутаторе уровня агрегации.
192.168.105.0/24	192.168.105.254	Сегмент сети, к которому относится отдел продаж, со шлюзом, расположенным на коммутаторе уровня агрегации.
192.168.106.0/24	192.168.106.254	Сегмент сети, к которому относится отдел аналитики, со шлюзом, расположенным на коммутаторе уровня агрегации.
192.168.107.0/24	192.168.107.254	Сегмент сети, к которому относится IT-отдел, со шлюзом, расположенным на коммутаторе уровня агрегации.
192.168.108.0/24	192.168.108.254	Сегмент сети, к которому относится служба безопасности, со шлюзом, расположенным на коммутаторе уровня агрегации.
192.168.109.0/24	192.168.109.254	Сегмент сети, к которому относится хозяйственная служба, со шлюзом, расположенным на коммутаторе уровня агрегации.
192.168.111.0/24	192.168.111.254	Сегмент сети, предназначенный для сервисов развернутых на сервере, со шлюзом, расположенным на коммутаторе уровня агрегации.

IP-адреса WAN-интерфейсов на выходных шлюзах назначаются оператором связи в статическом режиме. IP-адреса выходных шлюзов заранее получаются у оператора связи. Все терминалы получают IP-адреса по DHCP. Серверам и принтерам назначены фиксированные IP-адреса. IP-адреса всех сетевых устройств (кроме точек доступа) настраиваются динамически (Таблица 1.25).

Таблица 1.25 — Планирование режима распределения IP-адресов для основного здания

Сегмент/Интерфейс IP-сети	Режим распределения	Описание режима распределения
192.168.101.0/24 192.168.102.0/24 192.168.103.0/24 192.168.104.0/24 192.168.105.0/24 192.168.106.0/24 192.168.107.0/24 192.168.108.0/24 192.168.109.0/24	DHCP	Распределяется коммутатором уровня агрегации. Он распределяет динамические IP-адреса на конечные устройства пользователей и фиксированные IP-адреса принтерам и IP-телефонам
192.168.111.0/24	DHCP	Распределяется на уровне агрегации. Он выдает фиксированный IP-адрес для сервера.
192.168.2.0/24	Статический	Статически настроенные IP-адреса управления устройством.
192.168.3.0/30	Статический	Статически настроенный взаимосвязанный IP-адрес
192.168.4.0/30	Статический	Статически настроенный взаимосвязанный IP-адрес
192.168.5.0/30	Статический	Статически настроенный взаимосвязанный IP-адрес
GigabitEthernet 0/4 на коммутаторе уровня ядра	PPPoE	IP-адрес, назначенный оператором связи

Этап проектирование маршрутизации. Схема маршрутизации средней кампусной сети включает в себя проектирование внутренних маршрутов. Проектирование внутренней маршрутизации средней кампусной сети соответствует требованиям к связи устройств и терминалов кампусной

сети и обеспечивать взаимодействие с внешними маршрутами. Поскольку кампусная сеть имеет небольшой размер, структура сети проста. Статические маршруты могут использоваться для удовлетворения требований. Не нужно использовать сложный протокол маршрутизации.

Внутрисетевой сегмент. После выделения IP-адреса по DHCP создается маршрут по умолчанию[5]. Коммутатор уровня агрегации выполняет функции шлюза уровня 3. Межсетевой сегмент. Для соответствия требованиям статические маршруты будут развернуты на всех устройствах, которым пересылают данные уровня 3. На выходе из кампуса настроены статические маршруты по умолчанию (Таблица 1.26).

Таблица 1.26 — Итоги сетевого планирования уровня 3 для основного здания

IP-сеть	Метод назначения адреса; шлюз	Режим маршрутизации	описание сети
192.168.2.0/24	Статические адреса; SW_1-3_L3_DERDZYAN	Маршруты по умолчанию, направленные на SW_1-3_L3_DERDZYAN	Сеть управления устройствами уровня 2
192.168.3.0/30	Статические адреса шлюз не требуется	Включены OSPF и отношения соседства, маршрутизатор анонсирует маршрут по умолчанию	Сеть для организации связи между SW_1_L3_DERDZYAN и R_1_DERDZYAN
192.168.4.0/30			Сеть для организации связи между SW_2_L3_DERDZYAN и R_1_DERDZYAN
192.168.5.0/30			Сеть для организации связи между SW_3_L3_DERDZYAN и R_1_DERDZYAN

Таблица 1.27 — Продолжение таблицы 1.26

IP-сеть	Метод назначения адреса; шлюз	Режим маршрутизации	описание сети
192.168.101.0/24	Назначение выполняет SW_1_L3_DERDZYAN посредством DHCP	Анонсирование в OSPF через шлюзовые устройства	Сеть руководства
192.168.102.0/24			Сеть бухгалтерии
192.168.103.0/24			Сеть отдела кадров
192.168.104.0/24			Сеть отдела закупок
192.168.105.0/24			Сеть отдела продаж
192.168.106.0/24			Сеть отдела аналитики
192.168.107.0/24			Сеть IT-департамента
192.168.108.0/24			Сеть службы безопасности
192.168.109.0/24			Сеть хозяйственной службы
192.168.111.0/24	Статические адреса		Сеть сервера

1.6 Планирование политик фильтрации трафика

Политики фильтрации трафика спланированы и реализованы в формате стандартных списков контроля доступа.

ACL (Access Control List) — список правил, запрещающих или разрешающих использование ресурсов сети: доступа к интернету, телефонии, видеосвязи и т.д. ACL работает с IP-пакетами, но может узнать тип конкретного пакета, проанализировать порты TCP (Transmission Control Protocol) и UDP (User Datagram Protocol).

Все отделы предприятия имеют доступ к сетевым службам для того, чтобы иметь возможность работы с сервером, в остальном отделы не имеют других связей между собой (Рисунок 1.6).

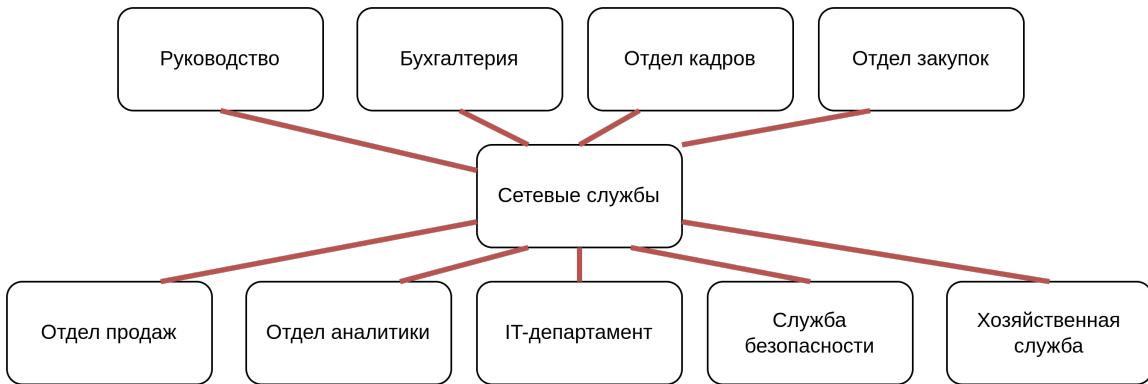


Рисунок 1.6 — Схема доступа

На основе схемы созданы списки контроля доступа (ACL), которые контролируют и фильтруют взаимодействие и передачу данных между отделами. Такое решение обусловлено тем, что требуемое программное обеспечение для работы сотрудников предприятия установлено на сервере. Для обеспечения дополнительной безопасности отделы, не имеют возможности обмениваться данными между собой.

На каждом из коммутаторов второго уровня создан список, фильтрующий трафик, который исходя из IP-адреса отправителя пакета на каждом порту определяет допускать трафик или нет.

1.7 Планирование политик обеспечения качества обслуживания

В системе классификации трафика выделены четыре категории: премиальный, золотой, серебряный и бронзовый. Трафик NFS признается и обрабатывается как премиальный. Категория золотого класса включает в себя трафик службы управления пользователями и веб-службы. Серебряный класс охватывает трафик службы динамического конфигурирования хостов, а бронзовый класс связан с трафиком службы доменных имен. Все остальные виды трафика рассматриваются и обрабатываются в соответствии с моделью Best-effort.

Стандартная пересылка используется для узлов, не маркирующих трафик, или для всего остального трафика в данной топологии. Значение поля

DSCP IP-пакета устанавливается в 000000 для передачи данных по сети, что гарантирует негарантированную доставку пакетов.

Введены четыре класса моделей поведения с гарантированной пересылкой, каждый из которых размещается в соответствующей очереди. Каждому классу присуща вероятность сброса, и при переполнении очереди пакеты с высокой вероятностью будут отброшены раньше остальных. Предусмотрено три уровня приоритета для отбрасывания.

Основной целью ускоренной пересылки EF является помещение пакетов в очередь с минимальной задержкой и потерями. Для этого используется приоритетная очередь, в которой пакеты отправляются раньше других. Однако существует вероятность блокировки других очередей, поэтому применяется ограничение скорости с использованием контроля. Значения DSCP[6] обычно обозначаются как EF, в двоичном виде - 101110, а десятичное значение - 46.

Определенные модели поведения, по которой трафик должен быть обработан и вычисленные значения поля DSCP в Таблице 1.28

Таблица 1.28 — Значения DSCP для классов и типов трафика

Класс трафика	Тип трафика	Модель поведения	Значения DSCP
Премиальный	NFS	EF	46
Золотой	Служба управления пользователями	AF11	10
	Веб-служба	AF12	12
Серебряный	Служба динамического конфигурирования хостов	AF21	18
Бронзовый	Служба доменных имен	AF31	26

1.8 Планирование службы доменных имен

DNS сервер для предприятия развернут в рамках программного обеспечения FreeIPA (Free Identity, Policy, Audit), так как он предоставляет интегрированный DNS-сервер. FreeIPA предлагает несколько преимуществ по сравнению с настройкой DNS изолированно:

1. Централизованное управление идентификацией: FreeIPA предоставляет единую систему для управления идентификацией, политиками и аудитом. Это означает, что вместе с DNS вы также получаете управление пользователями, группами, хостами и другими объектами в единой системе;
2. Интеграция с Kerberos и LDAP: FreeIPA включает в себя Kerberos для аутентификации и LDAP для хранения информации о пользователях и политиках. Это позволяет создавать более безопасную и легко масштабируемую сетевую инфраструктуру;
3. Безопасность: FreeIPA предлагает расширенные функции безопасности, такие как централизованное управление ключами SSH и SSL сертификатами, политики паролей и интеграцию с системами аутентификации многофакторной идентификации;
4. Автоматизация и упрощение администрирования: FreeIPA позволяет автоматизировать и упрощать многие процессы администрирования, которые при изолированной настройке DNS пришлось бы выполнять вручную.

Были определены и установлены ключевые параметры для настройки DNS-сервера, включая зоны, записи и стратегии отказоустойчивости. После анализа было решено внедрить DNS-сервер с использованием программного обеспечения FreeIPA. Этот выбор обеспечивает интегрированное решение для управления пользователями, политиками и аудитом, дополняя основные DNS-сервисы. Преимущества включают централизованное управление, повышенную безопасность и упрощенное администрирование, что делает FreeIPA предпочтительным выбором для современной инфраструктуры предприятия.

Результаты планирования службы доменных имен представлены в Таблице 1.29

Таблица 1.29 — Результаты планирования службы доменных имен

Параметр	Значение параметра
Название зоны	derdzyan.test
Запись в файле зоны	Конфигурируется автоматически программным обеспечением FreeIPA
Название обратной зоны	111.168.192.in-addr.arpa.
Запись в файле зоны	Конфигурируется автоматически программным обеспечением FreeIPA
Список серверов, на которые производится пересылка в случае отсутствия данных на сервере	1.1.1.1, 8.8.8.8

1.9 Планирование политик управления пользователями

В данном пункте осуществляется планирование политик управления пользователями, сфокусированное на развертывании программного обеспечения FreeIPA. План включает в себя выделение ключевых конфигурационных параметров, необходимых для успешного развертывания данного программного продукта.

Основные конфигурационные параметры включают в себя параметры безопасности, параметры централизованного управления и аудита. Преимущества выбора FreeIPA связаны с его интегрированным решением для управления пользователями, политиками и службой доменных имен DNS (Таблица 1.30).

Таблица 1.30 — Основные конфигурационные параметры для FreeIPA

Название параметр	Значение параметра
IP-адрес	192.168.111.4
Обратная зона	111.168.192.in-addr.arpa
Хостнейм сервера	server.derdzyan.test
Имя домена	server.derdzayn.test
Название зоны	derdzyan.test
Сервер пересылки	1.1.1.1, 8.8.8.8
NTP сервер	192.168.111.4
Порт	80

В рамках плана также определены параметры платформы для развертывания программного обеспечения, такие как требуемое количество оперативной памяти, поддерживаемая версия операционной системы, а также необходимые основные параметры и настройки ОС для эффективного функционирования программного обеспечения (Таблица 1.31).

Таблица 1.31 — Основные конфигурационные параметры для FreeIPA

Название параметр	Значение параметра
Оперативная память	2ГБ
Процессор	Двухъядерный
ОС версия	Fedora server 39 (64 bit)
Постоянная память	20ГБ

1.10 Планирование внедрения DHCP-сервера

В данном пункте осуществляется планирование конфигурирования DHCP[7] (Dynamic Host Configuration Protocol), который в автоматическом режиме предоставляет IP-адреса, маски подсетей, шлюзы по умолчанию и другие сетевые параметры в зависимости от конфигураций.

Реализация развертывания сервера осуществлена на сервере предприятия с использованием необходимого пакета – `isc-dhcpd version 4.4.3-P1` и изменения конфигурационного файла, в котором необходимо указать диапазон выдаваемых адресов в соответствии с определенной подсетью, стандартное время аренды IP- адреса в секундах, максимально время аренды, шлюз по умолчанию и адрес DNS-сервера.

Планирование распределения адресов по подсетям представлено в Таблице 1.32

Таблица 1.32 — Результат планирования распределения IP-адресов по отделам

Сегмент сети	Диапазон адресов
192.168.101.0/24	192.168.101.2 - 192.168.101.10
192.168.102.0/24	192.168.102.2 - 192.168.102.12
192.168.103.0/24	192.168.103.2 - 192.168.103.12
192.168.104.0/24	192.168.104.2 - 192.168.104.14
192.168.105.0/24	192.168.105.2 - 192.168.105.14

Таблица 1.33 — Продолжение Таблицы 1.32

Сегмент сети	Диапазон адресов
192.168.106.0/24	192.168.106.2 - 192.168.106.12
192.168.107.0/24	192.168.107.2 - 192.168.107.22
192.168.108.0/24	192.168.108.2 - 192.168.108.3
192.168.109.0/24	192.168.109.2 - 192.168.109.3

Конечный набор параметров и их значения в рамках планирования DHCP-сервера представлены в Таблице 1.34.

Таблица 1.34 — Результат планирования конфигурации DHCP-сервера

Название параметра	Значение параметра
Набор подсетей	192.168.101.0 – 192.168.109.0
Стандартное время аренды	6000 секунд
Максимальное время аренды	7200 секунд
Шлюз по умолчанию	192.168.101.254 – 192.168.109.254
Адрес DNS сервера	109.168.111.4

Стоит также упомянуть, что при разворачивании DHCP отдельно на сервере, требуется настройка DHCP-relay. Этот компонент перенаправляет запросы DHCP от клиентов через сетевые устройства, такие как маршрутизаторы и коммутаторы, к серверу DHCP. DHCP-relay необходим для обеспечения того, чтобы клиенты могли получать IP-конфигурацию в сетевых архитектурах с множественными подсетями, где прямой широковещательный трафик между подсетями ограничен или невозможен из-за разграничений маршрутизации.

1.11 Планирование других сетевых служб

Произведено планирование таких сетевых служб, как NTP (Network Time Protocol), Apache и NFS (Network File System).

Временная служба реализована в составе программного обеспечения chrony, которое состоит из двух компонентов, chronyd - служба, которая в фоновом режиме поддерживает работу времени и chronyc - интерфейс командной строки для chronyd.

Для корректной работы chronyd требуется в первую очередь дополнить конфигурационный файл серверами, которые находятся вблизи локации сервера компании, с которыми будут синхронизироваться часы и указать IP-адреса клиентов, которые могут использовать время на сервере. На клиентской машине в конфигурационном файле задан так же адрес сервера с которым синхронизируются часы клиента.

Apache — веб-сервер, распространяемый бесплатно. Программное обеспечение — кроссплатформенный продукт, то есть работает на разных операционных системах. Основные отличия от конкурентов — надежность и гибкость. Apache[8] работает по принципу модулей. Клиент сначала устанавливает ядро, а потом подключает необходимые модули под свои задачи. В рамках конфигурирования сервера Apache в первую очередь добавляется конфигурационный файл, в котором указывается название сервера, путь по которому находится файл со страницей и при необходимости есть возможность установки порта и IP-адреса на которых разворачивается веб-сервер.

Сетевая файловая система (NFS) обеспечивает хранение файлов в сети. Сетевая файловая система (NFS) - это распределенная файловая система. NFS обеспечивает пользователям доступ к файлам, расположенным на удаленных компьютерах, и позволяет работать с этими файлами точно так же, как и с локальными. Например, с помощью команд операционной системы пользователи могут создавать, удалять, считывать, записывать и изменять атрибуты удаленных файлов и каталогов.

В рамках предприятия было решено создать директории на сервере для каждого отдела в «/root» и разрешить импортирование соответствующим отделам, для этого необходимо каждой новой директории добавить запись в файле конфигурации, задать IP-адрес устройств, которые могут импортировать каталог и дать разрешение на запись и чтение. Так же выделена еще одна директория по пути «/root», которая будет уже доступна для всех отделов. Адреса устройств для доступа к директориям будут заданы, как подсети отделов.

1.12 Определение и расчет сервисной нагрузки

В данном пункте необходимо оценить нагрузку на сервер, сформированную каждым развернутым сервисом. Необходимо определить медианное и пиковое количество запросов к каждой сетевой службе в течение данного промежутка времени (рабочего дня, рабочей смены, а так же в течение секунды, если это является целесообразным).

Из необходимого трафика, от клиента к серверу, на котором запущены все необходимые службы, необходимо определить и вычислить объем данных одной транзакции (одного запроса) для каждого сервиса с учетом спецификации используемого службой протокола.

На Рисунке 1.7 представлена транзакция, состоящая из запроса клиента к серверу.

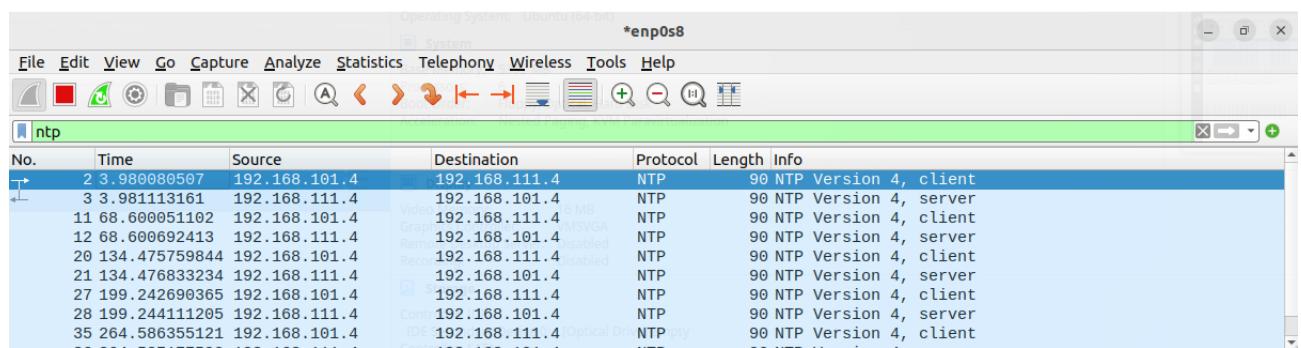


Рисунок 1.7 — Транзакции к NTP

При анализе данной транзакции было определено, что количество пакетов в одной транзакции 2, а максимальный размер пакета 720 бит. Требуется определить объем транзакции, воспользовавшись Формулой 1.1

$$V_{\text{транзакции}} = 720 \times 2 = 1440 = 0.002 \text{ Мбит} \quad (1.1)$$

Количество обращений к службе времени представлено в Таблице 1.35

Таблица 1.35 — Количество обращений к службе времени

Название отдела	Количество АРМ	Количество обращений за рабочий день	Всего пакетов за рабочий день
Руководство предприятия	8	4000	8000

Таблица 1.36 — Продолжение Таблицы 1.35

Название отдела	Количество АРМ	Количество обращений за рабочий день	Всего пакетов за рабочий день
Бухгалтерия	10	5000	10000
Отдел кадров	10	5000	10000
Отдел закупок	12	6000	12000
Отдел продаж	12	6000	12000
Отдел аналитики	10	5000	10000
ИТ-департамент	20	10000	20000
Служба безопасности	1	500	1000
Хозяйственная служба	1	500	1000
Итого	84	42000	84000

В итоге за 9 часов (без вычета обеденного перерыва) формируется примерно 42000 транзакций для файловой службы, то есть около 1.3 транзакции в секунду, что примерно равно 0.0026 Мбит/с. Это значит, что на интерфейс коммутатора только от службы времени будет поступать как минимум 0.0026 Мбит/с трафика или с учетом расчета количества пакетов - 2.6 пакета в секунду.

На Рисунке 1.8 представлены DNS пакеты, которые отправляются от клиента к серверу и обратно.

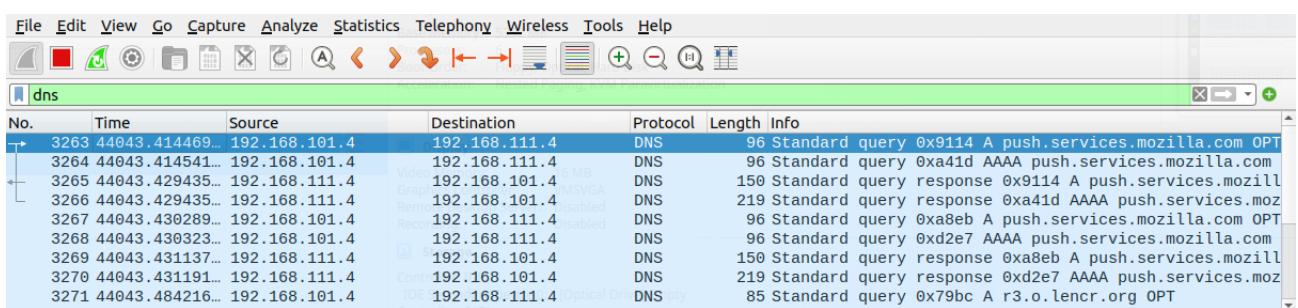


Рисунок 1.8 — Транзакции DNS

При анализе данной транзакции определено, что количество пакетов в одной транзакции — 4, максимальный размер пакета 1632 бита. Объем одной транзакции представлен Формулой 1.2.

$$V_{\text{транзакции}} = 1632 \times 4 = 6528 = 0.006 \text{ Мбит} \quad (1.2)$$

Требуется обратить внимание на то, что количество обращений (транзакций) для каждого из отделов взято на основе логических соображений, а не конкретных подсчетов и анализа трафика. Количество обращений к службе доменных имен представлено в Таблице 1.37

Таблица 1.37 — Количество обращений к службе времени

Название отдела	Количество АРМ	Количество обращений за рабочий день	Всего пакетов за рабочий день
Руководство предприятия	8	16000	64000
Бухгалтерия	10	20000	80000
Отдел кадров	10	20000	80000
Отдел закупок	12	24000	96000
Отдел продаж	12	24000	96000
Отдел аналитики	10	20000	80000
ИТ-департамент	20	40000	160000
Служба безопасности	1	2000	8000
Хозяйственная служба	1	2000	8000
Итого	84	168000	672000

В итоге за 8-часовой рабочий день формируется примерно 168000 транзакций для файловой службы, то есть около 5.8 транзакций в секунду, что примерно 0.348 Мбит/с. Это значит, что на интерфейс коммутатора только от службы доменных имен будет поступать как минимум 0.348 Мбит/с трафика или с учетом количества пакетов - 23.2 пакета в секунду.

На Рисунке 1.9 представлены пакеты, отвечающие за соединение клиента в веб-сервером.

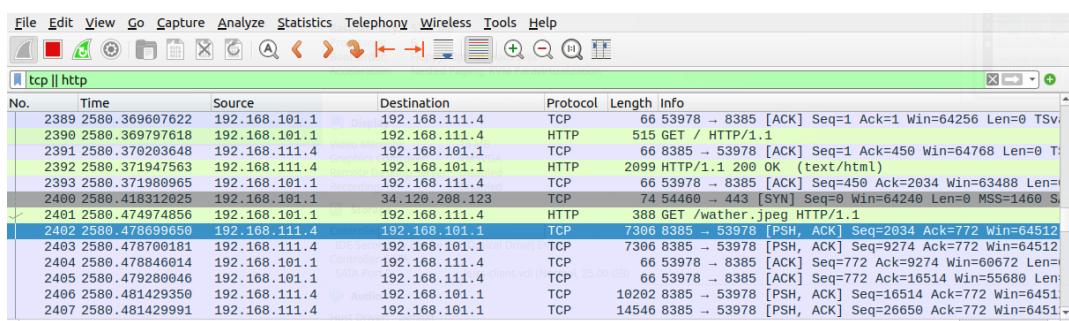


Рисунок 1.9 — Результат соединения клиента и веб-сервера

Соединение состоится на основе применения двух протоколов - TCP и HTTP. При анализе данной транзакции было определено 12 пакетов, максимальный размер пакета 58448 бит. Объем данной транзакции равен (Формула 1.3).

$$V_{\text{транзакции}} = 58448 \times 12 = 701376 = 0.701 \text{ Мбит} \quad (1.3)$$

Количество обращений к веб-серверу представлено в Таблиц 1.38

Таблица 1.38 — Количество обращений к веб-службе

Название отдела	Количество АРМ	Количество обращений за рабочий день	Всего пакетов за рабочий день
Руководство предприятия	8	1600	192000
Бухгалтерия	10	7000	84000
Отдел кадров	10	7000	84000
Отдел закупок	12	7100	85200
Отдел продаж	12	7100	85200
Отдел аналитики	10	7000	84000
ИТ-департамент	20	30000	160000
Служба безопасности	1	10	120
Хозяйственная служба	1	10	120
Итого	84	66820	801840

В итоге за 8-часовой рабочий день формируется примерно 66820 транзакций для веб-службы, то есть около 2.3 транзакций в секунду, что примерно 1.6 Мбит/с. Это значит, что на интерфейс коммутатора только от веб-службы будет поступать как минимум 1.6 Мбит/с трафика или с учетом количества пакетов - 27.6 пакета в секунду.

На Рисунке 1.10 представлены пакеты, отвечающие за NFS трафик. Клиент манипулирует разными pdf, xml файлами размером не больше пяти МБит.

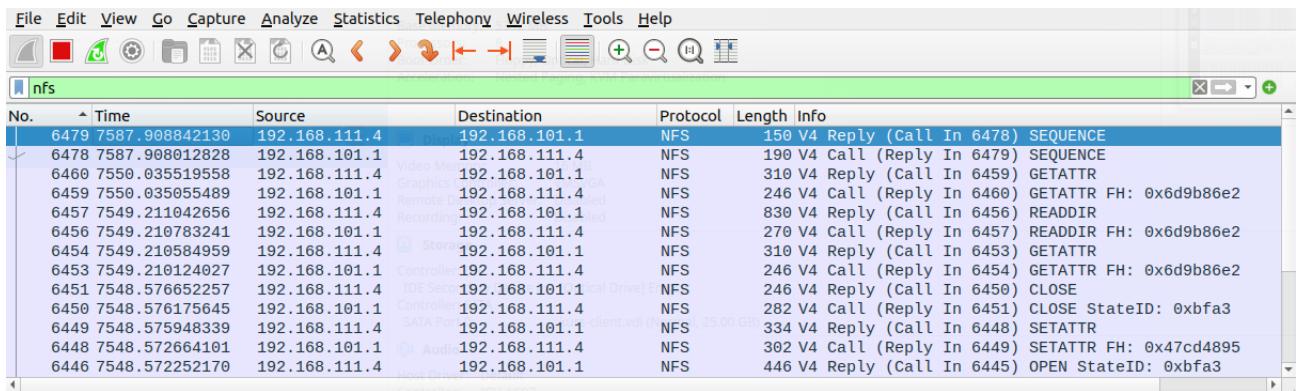


Рисунок 1.10 — Анализ трафика файловой службы

При анализе данной транзакции определено, что количество пакетов в одной транзакции — 540, максимальный размер пакета 2600 бита. Объем одной транзакции представлен Формулой 1.4.

$$V_{\text{транзакции}} = 2600 \times 540 = 1404000 = 1.404 \text{ Мбит} \quad (1.4)$$

Количество обращений к файловой службе представлено в Таблице 1.39

Таблица 1.39 — Количество обращений к файловой службе

Название отдела	Количество АРМ	Количество обращений за рабочий день	Всего пакетов за рабочий день
Руководство предприятия	8	800	43200
Бухгалтерия	10	10000	5400000
Отдел кадров	10	1000	540000
Отдел закупок	12	6000	3240000
Отдел продаж	12	6000	3240000
Отдел аналитики	10	5000	270000
ИТ-департамент	20	8000	4320000
Служба безопасности	1	10	5400
Хозяйственная служба	1	10	5400
Итого	84	36820	19882800

В итоге за 8-часовой рабочий день формируется примерно 36820 транзакций для файловой службы, то есть около 1.3 транзакций в секунду, что примерно 1.82 Мбит/с. Это значит, что на интерфейс коммутатора только от

файловой службы будет поступать как минимум 1.82 Мбит/с трафика или с учетом количества пакетов - 972.8 пакета в секунду.

На Рисунке 1.11 представлены пакеты, относящиеся к службе динамической конфигурации хоста (DHCP).

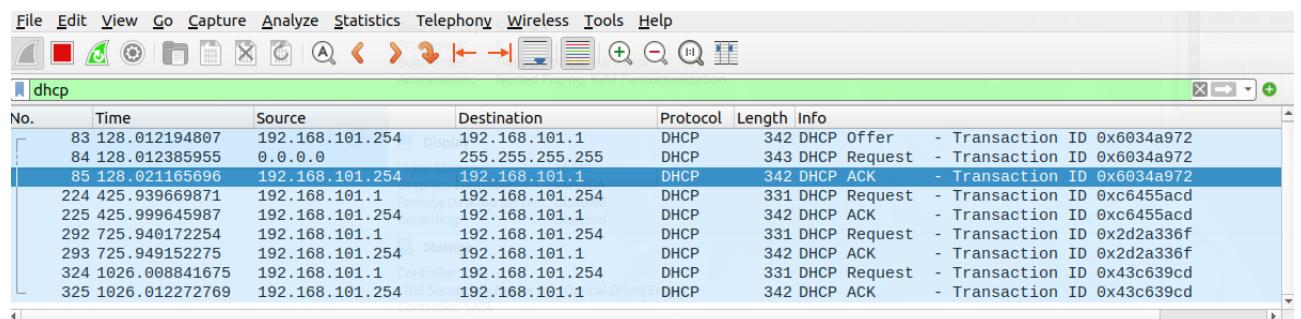


Рисунок 1.11 — Анализ трафика службы DHCP

При анализе данной транзакции определено, что количество пакетов в одной транзакции — 12, максимальный размер пакета 2744 бита. Объем одной транзакции представлен Формулой 1.5.

$$V_{\text{транзакции}} = 2744 \times 12 = 32928 = 0.032 \text{ Мбит} \quad (1.5)$$

Количество обращений к службе управления пользователям представлено в Таблице 1.40

Таблица 1.40 — Количество обращений к службе конфигурирования хостов

Название отдела	Количество АРМ	Количество обращений за рабочий день	Всего пакетов за рабочий день
Руководство предприятия	8	39	468
Бухгалтерия	10	48	576
Отдел кадров	10	48	576
Отдел закупок	12	58	696
Отдел продаж	12	58	696
Отдел аналитики	10	48	576
ИТ-департамент	20	96	1152
Служба безопасности	1	5	60
Хозяйственная служба	1	5	60

Таблица 1.41 — Продолжение Таблицы 1.40

Название отдела	Количество АРМ	Количество обращений за рабочий день	Всего пакетов за рабочий день
Итого	84	405	4860

В итоге за 8-часовой рабочий день формируется примерно 4860 транзакций для службы динамической конфигурации хостов, то есть около 1.17 транзакций в секунду, что примерно 0.04 Мбит/с. Это значит, что на интерфейс коммутатора только от службы DHCP поступает как минимум 0.04 Мбит/с трафика или с учетом количества пакетов - 14 пакета в секунду.

На Рисунке 1.12 представлены пакеты, состоящие из аутентификации пользователя в домене FreeIPA, проверки политик доступа (выполнение команд в привилегированном режиме) и другое.

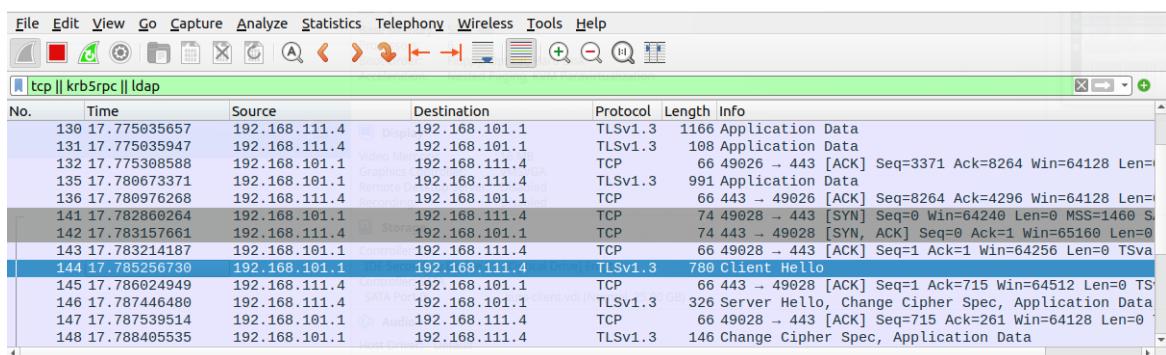


Рисунок 1.12 — Анализ трафика службы управления пользователями

При анализе данной транзакции определено, что количество пакетов в одной транзакции — 210, максимальный размер пакета 7936 бита. Объем одной транзакции представлен Формулой 1.6.

$$V_{\text{транзакции}} = 7936 \times 210 = 1666560 = 1.666 \text{ Мбит} \quad (1.6)$$

Количество обращений к службе управления пользователям представлено в Таблице 1.42

Таблица 1.42 — Количество обращений к службе управления пользователями

Название отдела	Количество АРМ	Количество обращений за рабочий день	Всего пакетов за рабочий день
Руководство предприятия	8	2400	504000
Бухгалтерия	10	3000	630000
Отдел кадров	10	3000	630000
Отдел закупок	12	3600	756000
Отдел продаж	12	3600	756000
Отдел аналитики	10	3000	630000
ИТ-департамент	20	20000	4200000
Служба безопасности	1	200	42000
Хозяйственная служба	1	200	42000
Итого	84	39200	8232000

В итоге за 8-часовой рабочий день формируется примерно 39200 транзакций для службы управления пользователями, то есть около 1.36 транзакций в секунду, что примерно 2.26 Мбит/с. Это значит, что на интерфейс коммутатора только от службы управления пользователями поступает как минимум 2.26 Мбит/с трафика или с учетом количества пакетов - 474.5 пакета в секунду.

На основе полученных данных с использованием и теории очередей М/М/1 произведен расчет минимальной необходимой скорости канала передачи данных между коммутатором L3 и сервером. Исходя из приведенных выше расходов среднее значение максимальных по размеру пакетов равно 15307 сумма всех пакетов передаваемых каждую секунду равна 1489. На основе медианного значения размера пакетов и их количества минимальная скорость канала будет равна 29 Мбит/с (Формула 1.6). Оптимальное значение коэффициента утилизации канала передачи канала взята 80% так как иначе начинается отбрасывания пакетов, что не является предпочтительным сценарием.

$$V_{\text{канала}} \geq \frac{15307 \times 1489}{0.8} \quad (1.7)$$

Сделан вывод, что канала в 1 Гбит/с хватит для поддерживания

необходимой пропускной способности и работы сервисов, как было предложено при предварительном планировании прототипа.

1.13 Итоговое планирование

В результате планирования сервисной сети передачи данных предприятия решено, что предварительный прототип полностью соответствует сети и не требует никаких модификаций. Стоит обратить внимание на то, что в доступных устройствах, с учетом модулей расширения, интерфейс с максимальной пропускной способностью имеет тип GigabitEthernet, чего недостаточно для передачи необходимого количества трафика между коммутаторами SW_1-2_L3_DERDZYAN и маршрутизатором. Для обеспечения требуемой скорости передачи данных следует использовать интерфейс 10GigabitEthernet.

Суммарная стоимость и мощность промежуточных устройств, которые используются в прототипе сети указаны в Таблицах 1.43 — 1.44.

Таблица 1.43 — Стоимость и мощность промежуточных устройств для основного здания

Название устройства	Количество устройств, шт	Стоимость одного устройства, у.е.	Мощность одного устройства, Ватт	Суммарная стоимость, у.е.	Суммарная мощность, Ватт
Маршрутизатор 4331	1	3150	535	3150	535
Коммутатор L3 3650 24PS	5	5100	54	25500	270
Коммутатор 2950T-24	7	550	50	3850	350
Итого:				32500	1155

Таблица 1.44 — Стоимость и мощность промежуточных устройств для склада

Название устройства	Количество устройств, шт	Стоимость одного устройства, у.е.	Мощность одного устройства, Ватт	Суммарная стоимость, у.е.	Суммарная мощность, Ватт
Маршрутизатор 1941	1	650	35	650	35
Коммутатор 1950T-24	1	550	50	550	50
Итого:				1200	85

2 МОДЕЛИРОВАНИЕ СЕТИ

В данном пункте основное внимание уделяется моделированию сетевой инфраструктуры с использованием соответствующих инструментов. Задача заключается в создании и представлении различных артефактов, отражающих ключевые элементы и характеристики сети. Этот процесс разделяется на два взаимосвязанных этапа.

На первом этапе осуществляется моделирование сервисов, где необходимо разработать и описать основные сервисы, предоставляемые сетью. Это включает четкое определение всех необходимых сервисов, планирование их конфигурации, а также описание взаимодействия этих сервисов между собой и с конечными пользователями.

Второй этап фокусируется на моделировании сети передачи данных. Основное внимание уделяется созданию модели физической и логической структуры сети. Важными аспектами являются разработка топологии сети, включая расположение и связи между устройствами, оценка требуемой пропускной способности и производительности, а также интеграция мер безопасности для обеспечения защиты от несанкционированных утечек данных и аварий.

Комбинированный подход этих двух этапов помогает создать комплексную и эффективную модель сети, которая соответствует всем требованиям и спецификациям, необходимым для успешной реализации и поддержки сетевых функций и сервисов.

2.1 Моделирование сервисов

Моделирование сервисов произведено на двух виртуальных машинах с использованием VirtualBox.

В качестве сервера используется виртуальная машина под управлением ОС Fedora server 39 с именем локального пользователя — `server_derdzyan`, а в качестве клиента Ubuntu 22.04.3 LTS с именем локального пользователя `client_derdzyan`. Результат установки представлен на Рисунке 2.1.

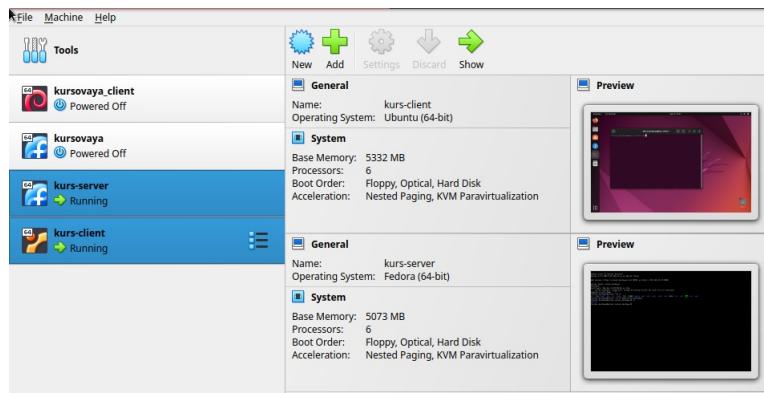


Рисунок 2.1 — Результат установки виртуальных машин

Служба доменных имен развернута в качестве дополнительного пакета программного обеспечения – FreeIPA. Конфигурация сервера DNS, в качестве доменных зон и DNS записей представлена на Рисунках 2.2 - 2.3.

Рисунок 2.2 — DNS зоны

Рисунок 2.3 — DNS записи

Конфигурация клиента представлена на Рисунке 2.4.

```
client_derdzyan@kurs-client:~$ cat /etc/resolv.conf | tail
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 192.168.111.4
options edns0 trust-ad
search .

client_derdzyan@kurs-client:~$
```

Рисунок 2.4 — Конфигурация DNS на клиенте

Тестирование DNS с помощью nslookup представлено на Рисунке 2.5.

```
client_derdzyan@kurs-client:~$ nslookup
> server.derdzyan.test
Server:      192.168.111.4
Address:     192.168.111.4#53

Name:   server.derdzyan.test
Address: 192.168.111.4

> ntp.derdzyan.test
Server:      192.168.111.4
Address:     192.168.111.4#53

Name:   ntp.derdzyan.test
Address: 192.168.111.4

> www.derdzyan.test
Server:      192.168.111.4
Address:     192.168.111.4#53

Name:   www.derdzyan.test
Address: 192.168.111.4

> nfs.derdzyan.test
Server:      192.168.111.4
Address:     192.168.111.4#53

Name:   nfs.derdzyan.test
Address: 192.168.111.4
```

Рисунок 2.5 — Тестирование DNS

Далее представлено развертывание службы динамического конфигурирования хостов (DHCP). Конфигурация сервера представлена на Рисунке 2.6.

```

# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
option domain-name-servers 192.168.111.4;
option domain-name "derdzyan.test";
default-lease-time 600;
max-lease-time 7200;

subnet 192.168.101.0 netmask 255.255.255.0 {
    range 192.168.101.1 192.168.101.10;
    option routers 192.168.101.254;
    option broadcast-address 192.168.101.255;
}
subnet 192.168.102.0 netmask 255.255.255.0 {
    range 192.168.101.1 192.168.101.12;
    option routers 192.168.102.254;
    option broadcast-address 192.168.102.255;
}
subnet 192.168.103.0 netmask 255.255.255.0 {
    range 192.168.101.1 192.168.101.12;
    option routers 192.168.103.254;
    option broadcast-address 192.168.103.255;
}
subnet 192.168.104.0 netmask 255.255.255.0 {
    range 192.168.101.1 192.168.101.14;
    option routers 192.168.104.254;
    option broadcast-address 192.168.104.255;
}

```

Рисунок 2.6 — Конфигурация сервера

Конфигурация клиента представлена на Рисунке 2.7.

```

client_derdzyan@kurs-client:~$ cat /etc/network/interfaces
auto enp0s8
iface enp0s8 inet dhcp
client_derdzyan@kurs-client:~$ 

```

Рисунок 2.7 — Конфигурация клиента

Результат получения клиентом конфигураций представлена на Рисунке 2.8

```

client_derdzyan@kurs-client:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1
    link/ether 08:00:27:74:11:a0 brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1
    link/ether 08:00:27:f4:03:9c brd ff:ff:ff:ff:ff:ff
    inet 192.168.101.1/24 brd 192.168.101.255 scope global dynamic noprefixroute enp0s8
        valid_lft 356sec preferred_lft 356sec
    inet6 fe80::e401:8b5e:aa72:30b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
client_derdzyan@kurs-client:~$ 

```

Рисунок 2.8 — Результат получения клиентом конфигурации

Далее представлены артефакты, иллюстрирующие корректное конфигурирование и работы веб-сервера, а именно Apache. На Рисунке 2.9 представлена конфигурация httpd, в котором и указываются параметры для Apache.

```
bash-5.2$ cat /etc/httpd/conf/httpd.conf | tail
# Load config files in the "/etc/httpd/conf.d/" directory, if any.
IncludeOptional conf.d/*.conf

Listen 8385
<VirtualHost *:8385>
    ServerName www.derdzyan.test
    DocumentRoot "/var/www/web.derdzyan.test"
</VirtualHost>

bash-5.2$
```

Рисунок 2.9 — Основной участок конфигурации сервера

На Рисунке 2.10 показана веб-страница предприятия.

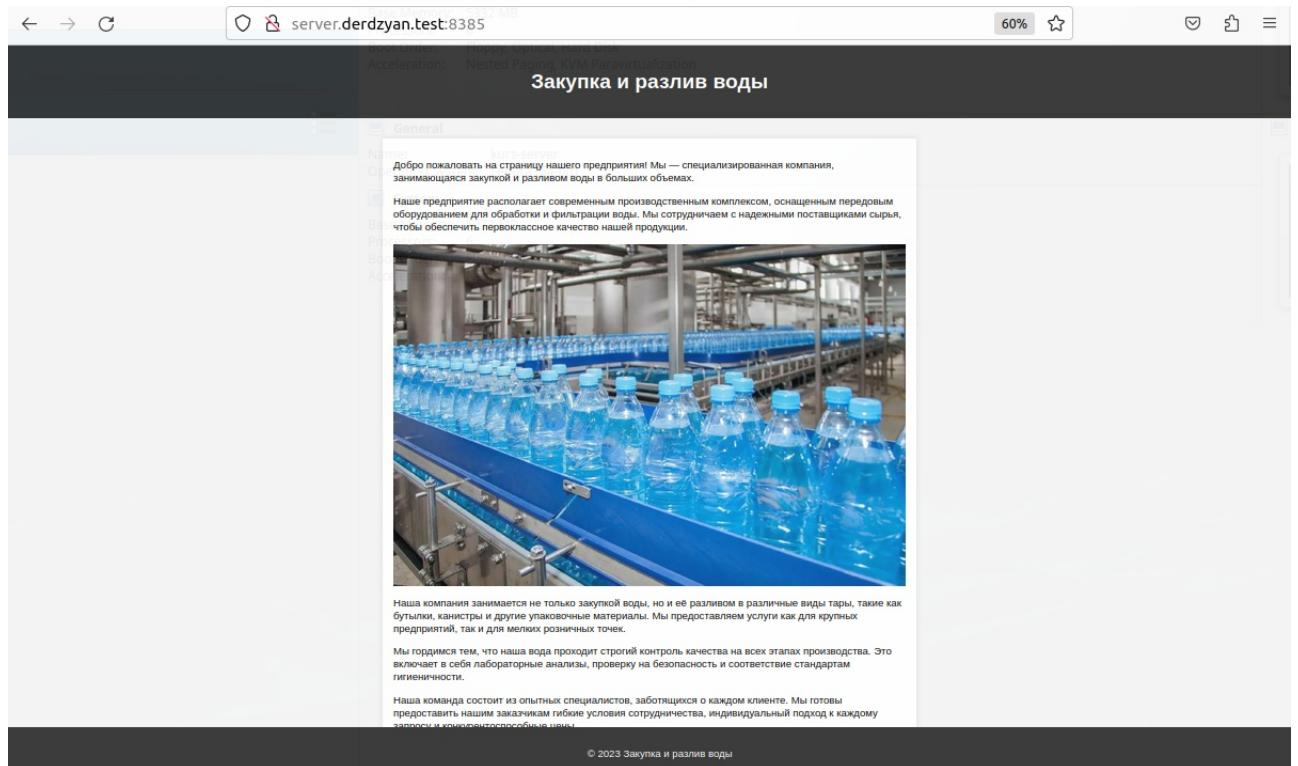


Рисунок 2.10 — Веб-страница

Далее произведено развертывание службы времени — NTP с использованием chrony. На Рисунке 2.11 представлен статус службы на клиенте.

```

client_derdzyan@kurs-client:~$ sudo systemctl status chronyd
[sudo] password for client_derdzyan:
● chrony.service - chrony, an NTP client/server
    Loaded: loaded (/lib/systemd/system/chrony.service; enabled; vendor preset: enabled)
      Active: active (running) since Mon 2023-12-18 18:42:21 MSK; 2h 21min ago
        Docs: man:chronyd(8)
               man:chronyc(1)
               man:chrony.conf(5)
     Process: 715 ExecStart=/usr/lib/systemd/scripts/chronyd-starter.sh $DAEMON_OPTS (code=exited, status=0/SUCCESS)
    Main PID: 746 (chronyd)
       Tasks: 2 (limit: 6050)
      Memory: 2.1M
         CPU: 280ms
      CGroup: /system.slice/chrony.service
              └─746 /usr/sbin/chronyd -F 1
                 ├─752 /usr/sbin/chronyd -F 1

дек 18 20:36:43 kurs-client chronyd[746]: Source 5.78.62.36 online
дек 18 20:36:43 kurs-client chronyd[746]: Source 185.125.190.56 online
дек 18 20:36:43 kurs-client chronyd[746]: Source 91.189.91.157 online
дек 18 20:36:43 kurs-client chronyd[746]: Source 138.236.128.112 online
дек 18 20:36:43 kurs-client chronyd[746]: Source 73.234.118.31 online
дек 18 20:36:43 kurs-client chronyd[746]: Source 69.164.202.202 online
дек 18 20:36:43 kurs-client chronyd[746]: Source 74.6.168.72 online
дек 18 20:36:43 kurs-client chronyd[746]: Source 152.70.159.102 online
дек 18 20:38:26 kurs-client chronyd[746]: Selected source 192.168.111.4
дек 18 20:54:09 kurs-client chronyd[746]: Source 73.234.118.31 replaced with 5.78.89.3 (2.ubuntu.pool.ntp.org)
client_derdzyan@kurs-client:~$ █

```

Рисунок 2.11 — Статус службы chronyd на клиенте

На Рисунке 2.12 представлено текущее время на клиенте.

```

client_derdzyan@kurs-client:~$ chronyc tracking
Reference ID      : C0A86F04 (server.derdzyan.test)
Stratum          : 4
Ref time (UTC)   : Mon Dec 18 18:04:30 2023
System time      : 0.000003302 seconds fast of NTP time
Last offset      : +0.000003350 seconds
RMS offset       : 0.000607096 seconds
Frequency        : 0.329 ppm slow
Residual freq    : -0.000 ppm
Skew             : 0.611 ppm
Root delay       : 0.008931896 seconds
Root dispersion  : 0.027633879 seconds
Update interval  : 65.2 seconds
Leap status      : Normal
client_derdzyan@kurs-client:~$ █

```

Рисунок 2.12 — Текущее время на клиенте

Следующим выполнено разворачивание файловой службы, используется NFS. На Рисунке 2.13 представлена конфигурация NFS на сервере.

```

[server_derdzyan@server home]$ cat /etc/exports
/var/nfs/ruk 192.168.101.0/24(rw,sync,no_subtree_check)
/var/nfs/bux 192.168.102.0/24(rw,sync,no_subtree_check)
/var/nfs/kad 192.168.103.0/24(rw,sync,no_subtree_check)
/var/nfs/zak 192.168.104.0/24(rw,sync,no_subtree_check)
/var/nfs/pro 192.168.105.0/24(rw,sync,no_subtree_check)
/var/nfs/ana 192.168.106.0/24(rw,sync,no_subtree_check)
/var/nfs/it 192.168.107.0/24(rw,sync,no_subtree_check)
/var/nfs/xoz 192.168.108.0/24(rw,sync,no_subtree_check)
/var/nfs/bez 192.168.109.0/24(rw,sync,no_subtree_check)
/var/nfs/all 192.168.0.0/16(rw,sync,no_subtree_check)
[server_derdzyan@server home]$ █

```

Рисунок 2.13 — Конфигурация файловой службы на сервере

Проверка доступности файла отправленного с сервера на клиенте, подключенного к директории NFS (Рисунок 2.14).

```

client_derdzyan@kurs-client:~/nfsruk$ ls
client_derdzyan@kurs-client:~/nfsruk$ ls
msg.txt
client_derdzyan@kurs-client:~/nfsruk$ cat msg.txt
Its a message left by other user on the server
client_derdzyan@kurs-client:~/nfsruk$ ls

```

Рисунок 2.14 — Проверка доступности файлов на клиенте

Также необходимо развернуть службу управления пользователями в качестве ПО – FreeIPA. На Рисунке 2.15 представлен статус службы FreeIPA.

```

[server_derdzyan@server ~]$ systemctl status ipa.service
● ipa.service - Identity, Policy, Audit
   Loaded: loaded (/usr/lib/systemd/system/ipa.service; enabled; preset: disabled)
   Drop-In: /usr/lib/systemd/system/service.d
             └─10-timeout-abort.conf
     Active: active (exited) since Mon 2023-12-18 19:17:46 MSK; 2h 37min ago
       Process: 963 ExecStart=/usr/sbin/ipactl start (code=exited, status=0/SUCCESS)
     Main PID: 963 (code=exited, status=0/SUCCESS)
        CPU: 2.708s

Dec 18 19:17:46 server_derdzyan.test ipactl[963]: Starting Directory Service
Dec 18 19:17:46 server_derdzyan.test ipactl[963]: Starting krb5kdc Service
Dec 18 19:17:46 server_derdzyan.test ipactl[963]: Starting kadmin Service
Dec 18 19:17:46 server_derdzyan.test ipactl[963]: Starting named Service
Dec 18 19:17:46 server_derdzyan.test ipactl[963]: Starting httpd Service
Dec 18 19:17:46 server_derdzyan.test ipactl[963]: Starting ipa-custodia Service
Dec 18 19:17:46 server_derdzyan.test ipactl[963]: Starting pki-tomcatd Service
Dec 18 19:17:46 server_derdzyan.test ipactl[963]: Starting ipa-otp Service
Dec 18 19:17:46 server_derdzyan.test ipactl[963]: Starting ipa-dnskeysyncd Service
Dec 18 19:17:46 server_derdzyan.test systemd[1]: Finished ipa.service - Identity, Policy, Audit.
[server_derdzyan@server ~]$

```

Рисунок 2.15 — Статус службы ipa

На Рисунке 2.16 представлены пользователи домена FreeIPA.

User login	First name	Last name	Status	UID	Email address	Telephone Number	Job Title
admin	System	Administrator	Enabled	450000000			
pc_1_ana_derdzyan	Felix	Postolakyan	Enabled	450000009	pc_1_ana_derdzyan@derdzyan.test		
pc_1_bez_derdzyan	Areg	Derdzyan	Enabled	450000011	pc_1_bez_derdzyan@derdzyan.test		
pc_1_bux_derdzyan	Vazgen	Antinyan	Enabled	450000005	pc_1_bux_derdzyan@derdzyan.test		
pc_1_lt_derdzyan	Aram	Derdzyan	Enabled	450000010	pc_1_lt_derdzyan@derdzyan.test		
pc_1_kad_derdzyan	Arno	Bojukyan	Enabled	450000006	pc_1_kad_derdzyan@derdzyan.test		
pc_1_pro_derdzyan	Hamlet	Postolokyan	Enabled	450000008	pc_1_pro_derdzyan@derdzyan.test		
pc_1_ruk_derdzyan	Ararat	Papyan	Enabled	450000004	pc_1_ruk_derdzyan@derdzyan.test		
pc_1_xoz_derdzyan	Arsine	Derdzyan	Enabled	4500000012	pc_1_xoz_derdzyan@derdzyan.test		
pc_1_zak_derdzyan	Arpine	Abraamyan	Enabled	450000007	pc_1_zak_derdzyan@derdzyan.test		
server_derdzyan	server_derdzyan	server_derdzyan	Enabled	450000003	server_derdzyan@derdzyan.test		

Рисунок 2.16 — Пользователи домена FreeIPA

На Рисунке 2.17 представлено логирование клиента в домен FreeIPA.

```
client_derdzyan@pc1ana_derdzyan:~$ su pc_1_ana_derdzyan
Password:
$ whoami
pc_1_ana_derdzyan
$
```

Рисунок 2.17 — Логирование клиента в домене FreeIPA

2.2 Моделирование сети передачи данных

Моделирование сети передачи данных произведено в стимуляторе сети передачи данных “Cisco Packet Tracer”. Моделирование сети передачи данных произведено только для основного здания предприятия. Топология содержит указанные выше устройства и приближенные к реальности настройки, которые позволяют разным отделам основного здания иметь доступ сетевым службам, в топологии так же реализованы политики качества обслуживания, списки контроля доступа и другое (Рисунок 2.18).

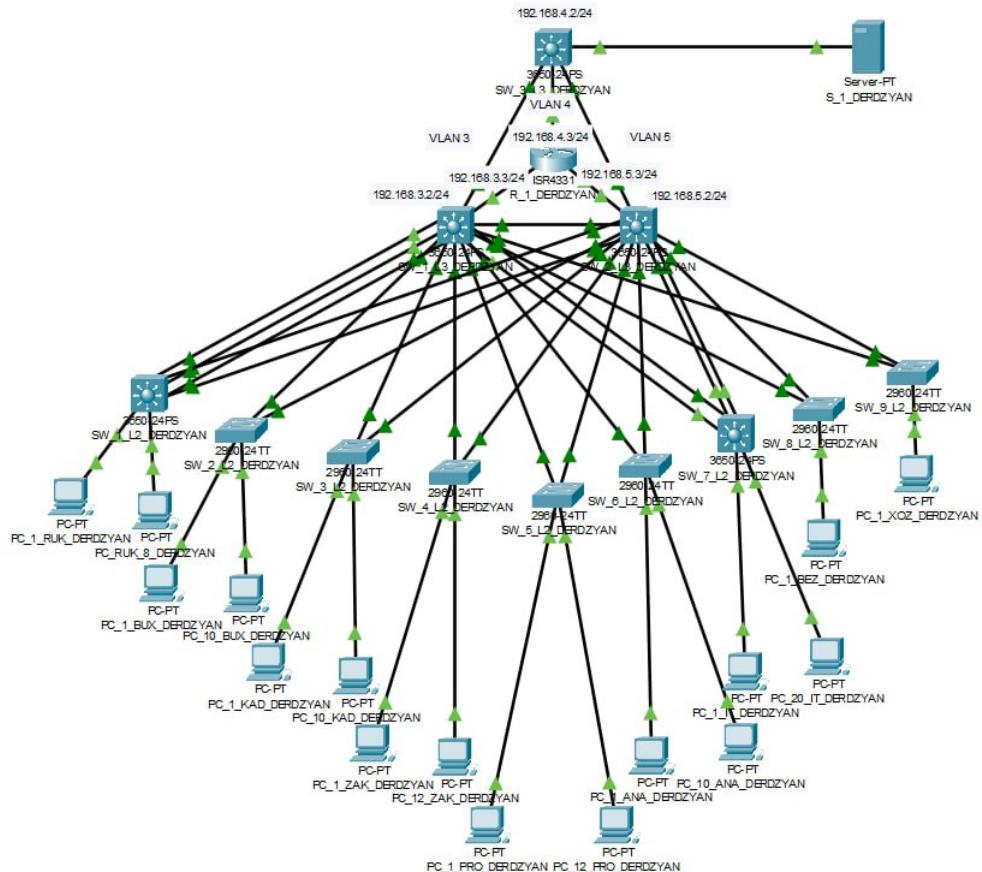


Рисунок 2.18 — Сконфигурированная топология сети передачи данных

Проверка работоспособности смоделированной сети передачи данных представлена на Рисунке 2.19

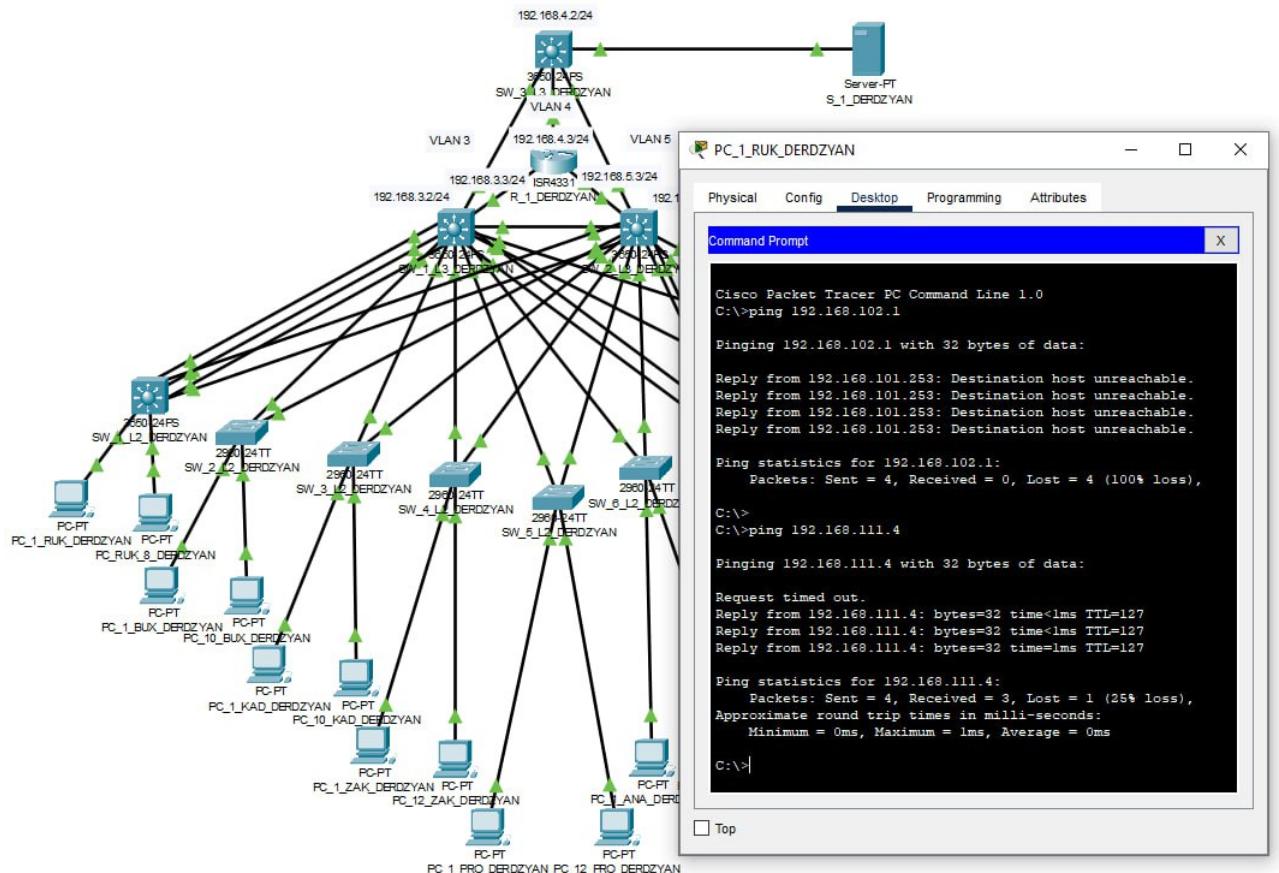


Рисунок 2.19 — Проверка работоспособности смоделированной сети

В Листинге 2.1 представлена конфигурация одного из коммутаторов уровня три, остальная часть конфигураций приведены в Приложении А. В приложении приведены не все конфигурационные файлы, так как большая часть исходит из тех, что приведены за изменением номера порта интерфейса.

Листинг 2.1 — Конфигурация устройства *SW_1_L3_DERDZYAN*

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SW_1_L3_DERDZYAN
!
!
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
```

```
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode rapid-pvst
spanning-tree vlan 3-5,101-109,111 priority 24576
!
!
!
interface Port-channel1
switchport trunk allowed vlan 2-5,101-109,111
switchport mode trunk
!
interface Port-channel2
switchport trunk allowed vlan 2-5,101-109,111
switchport mode trunk
!
interface GigabitEthernet1/0/1
switchport trunk allowed vlan 3-5,101-109,111
switchport mode trunk
!
interface GigabitEthernet1/0/2
switchport access vlan 3
switchport mode access
!
interface GigabitEthernet1/0/3
switchport trunk allowed vlan 2-5,101-109,111
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport trunk allowed vlan 2-5,101-109,111
switchport mode trunk
channel-group 1 mode passive
!
interface GigabitEthernet1/0/5
switchport trunk allowed vlan 2-5,101-109,111
switchport mode trunk
channel-group 1 mode passive
!
```

```
interface GigabitEthernet1/0/6
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
    channel-group 1 mode passive
!
interface GigabitEthernet1/0/7
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
!
interface GigabitEthernet1/0/8
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
!
interface GigabitEthernet1/0/9
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
!
interface GigabitEthernet1/0/10
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
!
interface GigabitEthernet1/0/11
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
!
interface GigabitEthernet1/0/12
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
    channel-group 2 mode passive
!
interface GigabitEthernet1/0/13
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
    channel-group 2 mode passive
!
interface GigabitEthernet1/0/14
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
!
interface GigabitEthernet1/0/15
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
...

```

```

...
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan2
  mac-address 0001.c9a9.6701
  no ip address
!
interface Vlan3
  mac-address 0001.c9a9.6702
  ip address 192.168.3.2 255.255.255.0
!
interface Vlan101
  mac-address 0001.c9a9.6703
  ip address 192.168.101.253 255.255.255.0
  ip access-group 1 out
  standby 101 ip 192.168.101.254
  standby 101 priority 105
  standby 101 preempt
!
interface Vlan102
  mac-address 0001.c9a9.6704
  ip address 192.168.102.253 255.255.255.0
  ip access-group 1 out
  standby 102 ip 192.168.102.254
  standby 102 priority 105
  standby 102 preempt
!
interface Vlan103
  mac-address 0001.c9a9.6705
  ip address 192.168.103.253 255.255.255.0
  ip access-group 1 out
  standby 103 ip 192.168.103.254
  standby 103 priority 105
  standby 103 preempt
!
```

```
interface Vlan104
  mac-address 0001.c9a9.6706
  ip address 192.168.104.253 255.255.255.0
  ip access-group 1 out
  standby 104 ip 192.168.104.254
  standby 104 priority 105
  standby 104 preempt
!
interface Vlan105
  mac-address 0001.c9a9.6707
  ip address 192.168.105.253 255.255.255.0
  ip access-group 1 out
  standby 105 ip 192.168.105.254
  standby 105 priority 105
  standby 105 preempt
!
interface Vlan106
  mac-address 0001.c9a9.6708
  ip address 192.168.106.253 255.255.255.0
  ip access-group 1 out
  standby 106 ip 192.168.106.254
  standby 106 priority 105
  standby 106 preempt
!
interface Vlan107
  mac-address 0001.c9a9.6709
  ip address 192.168.107.253 255.255.255.0
  ip access-group 1 out
  standby 107 ip 192.168.107.254
  standby 107 priority 105
  standby 107 preempt
!
interface Vlan108
  mac-address 0001.c9a9.670b
  ip address 192.168.108.253 255.255.255.0
  ip access-group 1 out
  standby 108 ip 192.168.108.254
  standby 108 priority 105
  standby 108 preempt
!
interface Vlan109
  mac-address 0001.c9a9.670c
  ip address 192.168.109.253 255.255.255.0
  ip access-group 1 out
  standby 109 ip 192.168.109.254
  standby 109 priority 105
  standby 109 preempt
!
```

```
interface Vlan111
  mac-address 0001.c9a9.670d
  ip address 192.168.111.254 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.111.0 0.0.0.255
access-list 1 deny 192.168.101.0 0.0.0.255
access-list 1 deny 192.168.102.0 0.0.0.255
access-list 1 deny 192.168.103.0 0.0.0.255
access-list 1 deny 192.168.104.0 0.0.0.255
access-list 1 deny 192.168.105.0 0.0.0.255
access-list 1 deny 192.168.106.0 0.0.0.255
access-list 1 deny 192.168.107.0 0.0.0.255
access-list 1 deny 192.168.108.0 0.0.0.255
access-list 1 deny 192.168.109.0 0.0.0.255
access-list 1 permit any
!
banner motd #
Authorized users only! #
!
!
line con 0
  password 7 08701E1D
  login
!
line aux 0
!
line vty 0 4
  password 7 08701E1D
  login
line vty 5 15
  password 7 08701E1D
  login
!
!
end
```

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной курсовой работы было проведено планирование и реализация сервисной сети передачи данных для предприятия, занимающегося закупкой воды в больших емкостях и последующим разливом в тару меньшего объема. Целью исследования было создание эффективной и надежной сервисной сети передачи данных, удовлетворяющей специфике и требованиям такого типа бизнеса. Результаты работы позволяют обеспечить стабильную и эффективную работу предприятия в долгосрочной перспективе.

Процесс планирования и проектирования сети передачи данных включал в себя анализ исходных данных, определение структуры предприятия, расчет пропускной способности каналов передачи данных, прототипирование сети, а также планирование адресации, маршрутизации, политик фильтрации трафика, обеспечения качества обслуживания, служб доменных имен, управления пользователями, внедрения DHCP-сервера и других сетевых служб.

Инструменты исследования, такие как Cisco Packet Tracer и Apache, обеспечили возможность моделирования и тестирования сетевых архитектур, что способствовало разработке оптимальных решений.

Основными этапами работы стали обзор теоретических основ и современных технологий передачи данных, изучение специфики деятельности предприятия, разработка схемы адресации и маршрутизации, проектирование виртуальных и локальных сетей, создание прототипа, планирование служб и настройка сети, а также проведение расчетов для определения сервисной нагрузки.

Таким образом, выполнение данной курсовой работы позволило разработать рекомендации по проектированию и реализации системы управления закупками и разливом вина для предприятия, занимающегося данной сферой деятельности. Созданная система управления обеспечивает эффективный контроль и управление процессами закупки и разлива, что способствует повышению производительности предприятия. Итоговое решение предоставит предприятию не только возможность улучшить эффективность своей сервисной сети передачи данных, но и станет основой для развития инфраструктуры в будущем.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Внутренние механизмы TCP, влияющие на скорость загрузки: часть 1. — Режим доступа: <https://habr.com/ru/company/webo/blog/326258/> (Дата обращения: 05/24/2023).
2. Основы компьютерных сетей. Тема №8. Протокол агрегирования каналов: Etherchannel // Хабр URL: <https://habr.com/ru/articles/334778/> (дата обращения 24.12.2023).
3. Жан Вальран, Шьям Парех Коммуникационные сети: краткое введение. - М.: ДМК Пресс, 2023. - 268 с.
4. Сети для самых маленьких. Часть четвертая. STP // Хабр URL: <https://habr.com/ru/articles/143768/> (дата обращения: 24.12.2023).
5. Основы компьютерных сетей. Тема №9. Маршрутизация: статическая и динамическая на примере RIP, OSPF и EIGRP. — Режим доступа: <https://habr.com/ru/articles/335090/> (Дата обращения: 05/24/2023).
6. Приоритет IP и значения DSCP в QoS (Quality of Service) // Блог SEDICOMM URL: <https://blog.sedicomm.com/2021/10/25/prioritet-ip-i-znacheniya-dscp-v-qos-quality-of-service/> (дата обращения: 24.12.2023).
7. Олифер В. Г. Компьютерные сети: принципы, технологии, протоколы. — 2021. — Р. 1050.
8. Apache vs Nginx: практический взгляд // Хабр URL: <https://habr.com/ru/articles/267721/> (дата обращения 24.12.2023).

ПРИЛОЖЕНИЯ

Приложение А — Конфигурация сетевых устройств

Приложение А

Конфигурация сетевых устройств

Листинг A.1 — Конфигурация устройства R_1_DERDZYAN

```
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1_DERDZYAN
!
!
!
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0/0
  ip address 192.168.3.3 255.255.255.0
  duplex auto
```

```

    speed auto
!
interface GigabitEthernet0/0/1
    ip address 192.168.5.3 255.255.255.0
    duplex auto
    speed auto
!
interface GigabitEthernet0/0/2
    ip address 192.168.4.3 255.255.255.0
    duplex auto
    speed auto
!
interface Vlan1
    no ip address
    shutdown
!
ip classless
ip route 192.168.101.0 255.255.255.0 192.168.3.2
ip route 192.168.101.0 255.255.255.0 192.168.5.2 200
ip route 192.168.102.0 255.255.255.0 192.168.3.2
ip route 192.168.102.0 255.255.255.0 192.168.5.2 200
ip route 192.168.103.0 255.255.255.0 192.168.3.2
ip route 192.168.103.0 255.255.255.0 192.168.5.2 200
ip route 192.168.104.0 255.255.255.0 192.168.3.2
ip route 192.168.104.0 255.255.255.0 192.168.5.2 200
ip route 192.168.105.0 255.255.255.0 192.168.3.2
ip route 192.168.105.0 255.255.255.0 192.168.5.2 200
ip route 192.168.106.0 255.255.255.0 192.168.3.2
ip route 192.168.106.0 255.255.255.0 192.168.5.2 200
ip route 192.168.107.0 255.255.255.0 192.168.3.2
ip route 192.168.107.0 255.255.255.0 192.168.5.2 200
ip route 192.168.108.0 255.255.255.0 192.168.3.2
ip route 192.168.108.0 255.255.255.0 192.168.5.2 200
ip route 192.168.109.0 255.255.255.0 192.168.3.2
ip route 192.168.109.0 255.255.255.0 192.168.5.2 200
ip route 192.168.111.0 255.255.255.0 192.168.4.2
!
ip flow-export version 9
!
!
!
!
banner motd #
Authorized users only! #
!
!
!
!
line con 0

```

```
password 7 08701E1D
login
!
line aux 0
!
line vty 0 4
password 7 08701E1D
login
line vty 5 15
password 7 08701E1D
login
!
!
!
end
```

Листинг A.2 — Конфигурация устройства SW_2_L3_DERDZYAN

```
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SW_2_L3_DERDZYAN
!
!
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
!
!
!
!
!
```

```
!
no ip domain-lookup
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface Port-channel1
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface Port-channel2
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface GigabitEthernet1/0/1
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface GigabitEthernet1/0/2
  switchport access vlan 5
  switchport mode access
!
interface GigabitEthernet1/0/3
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface GigabitEthernet1/0/4
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
  channel-group 1 mode passive
!
interface GigabitEthernet1/0/5
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
  channel-group 1 mode passive
!
interface GigabitEthernet1/0/6
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface GigabitEthernet1/0/7
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
```

```
!
interface GigabitEthernet1/0/8
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface GigabitEthernet1/0/9
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface GigabitEthernet1/0/10
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface GigabitEthernet1/0/11
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
  channel-group 2 mode passive
!
interface GigabitEthernet1/0/12
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
  channel-group 2 mode passive
!
interface GigabitEthernet1/0/13
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface GigabitEthernet1/0/14
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
```

```
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan5
  mac-address 0001.428e.0601
  ip address 192.168.5.2 255.255.255.0
!
interface Vlan101
  mac-address 0001.428e.0602
  ip address 192.168.101.252 255.255.255.0
  ip access-group 1 out
  standby 101 ip 192.168.101.254
!
interface Vlan102
  mac-address 0001.428e.0603
  ip address 192.168.102.252 255.255.255.0
  ip access-group 1 out
  standby 102 ip 192.168.102.254
!
interface Vlan103
  mac-address 0001.428e.0604
  ip address 192.168.103.252 255.255.255.0
  ip access-group 1 out
  standby 103 ip 192.168.103.254
!
interface Vlan104
  mac-address 0001.428e.0605
  ip address 192.168.104.252 255.255.255.0
  ip access-group 1 out
  standby 104 ip 192.168.104.254
!
interface Vlan105
  mac-address 0001.428e.0606
  ip address 192.168.105.252 255.255.255.0
  ip access-group 1 out
  standby 105 ip 192.168.105.254
```

```

!
interface Vlan106
  mac-address 0001.428e.0607
  ip address 192.168.106.252 255.255.255.0
  ip access-group 1 out
  standby 106 ip 192.168.106.254
!
interface Vlan107
  mac-address 0001.428e.0608
  ip address 192.168.107.252 255.255.255.0
  ip access-group 1 out
  standby 107 ip 192.168.107.254
!
interface Vlan108
  mac-address 0001.428e.0609
  ip address 192.168.108.252 255.255.255.0
  ip access-group 1 out
  standby 108 ip 192.168.108.254
!
interface Vlan109
  mac-address 0001.428e.060a
  ip address 192.168.109.252 255.255.255.0
  ip access-group 1 out
  standby 109 ip 192.168.109.254
!
interface Vlan111
  mac-address 0001.428e.060b
  ip address 192.168.111.254 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.111.0 0.0.0.255
access-list 1 deny 192.168.101.0 0.0.0.255
access-list 1 deny 192.168.102.0 0.0.0.255
access-list 1 deny 192.168.103.0 0.0.0.255
access-list 1 deny 192.168.104.0 0.0.0.255
access-list 1 deny 192.168.105.0 0.0.0.255
access-list 1 deny 192.168.106.0 0.0.0.255
access-list 1 deny 192.168.107.0 0.0.0.255
access-list 1 deny 192.168.108.0 0.0.0.255
access-list 1 deny 192.168.109.0 0.0.0.255
access-list 1 permit any
!
banner motd #
Authorized users only! #

```

```

!
!
!
!
line con 0
password 7 08701E1D
login
!
line aux 0
!
line vty 0 4
password 7 08701E1D
login
line vty 5 15
password 7 08701E1D
login
!
!
!
!
```

```
end
```

Листинг A.3 — Конфигурация устройства SW_3_L3_DERDZYAN

```

!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SW_3_L3_DERDZYAN
!
!
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
!
```

```
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface GigabitEthernet1/0/1
    switchport access vlan 111
    switchport mode access
!
interface GigabitEthernet1/0/2
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
!
interface GigabitEthernet1/0/3
    switchport access vlan 4
    switchport mode access
!
interface GigabitEthernet1/0/4
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
```

```
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan4
  mac-address 0060.2f51.0401
  ip address 192.168.4.2 255.255.255.0
!
interface Vlan101
  mac-address 0060.2f51.0402
  ip address 192.168.101.251 255.255.255.0
!
interface Vlan102
  mac-address 0060.2f51.0403
  ip address 192.168.102.251 255.255.255.0
```

```
!
interface Vlan103
  mac-address 0060.2f51.0404
  ip address 192.168.103.251 255.255.255.0
!
interface Vlan104
  mac-address 0060.2f51.0405
  ip address 192.168.104.251 255.255.255.0
!
interface Vlan105
  mac-address 0060.2f51.0406
  ip address 192.168.105.251 255.255.255.0
!
interface Vlan106
  mac-address 0060.2f51.0407
  ip address 192.168.106.251 255.255.255.0
!
interface Vlan107
  mac-address 0060.2f51.0408
  ip address 192.168.107.251 255.255.255.0
!
interface Vlan108
  mac-address 0060.2f51.0409
  ip address 192.168.108.251 255.255.255.0
!
interface Vlan109
  mac-address 0060.2f51.040a
  ip address 192.168.109.251 255.255.255.0
!
interface Vlan111
  mac-address 0060.2f51.040b
  ip address 192.168.111.254 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd #
Authorized users only! #
!
!
!
line con 0
password 7 08701E1D
login
```

```

!
line aux 0
!
line vty 0 4
    password 7 08701E1D
    login
line vty 5 15
    password 7 08701E1D
    login
!
!
!
!
end

```

Листинг A.4 — Конфигурация устройства SW_1_L2_DERDZYAN

```

!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SW_1_L2_DERDZYAN
!
!
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
!
!
!
!
!
!
```

```
no ip domain-lookup
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface Port-channel1
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
!
interface Port-channel2
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
!
interface GigabitEthernet1/0/1
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
    channel-group 1 mode active
!
interface GigabitEthernet1/0/2
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
    channel-group 1 mode active
!
interface GigabitEthernet1/0/3
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
    channel-group 1 mode active
!
interface GigabitEthernet1/0/4
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
    channel-group 2 mode active
!
interface GigabitEthernet1/0/5
    switchport trunk allowed vlan 2-5,101-109,111
    switchport mode trunk
    channel-group 2 mode active
!
interface GigabitEthernet1/0/6
    switchport access vlan 101
    switchport mode access
!
interface GigabitEthernet1/0/7
```

```
switchport access vlan 101
switchport mode access
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address
  shutdown
```

```

!
ip classless
!
ip flow-export version 9
!
!
!
!
banner motd #
Authorized users only! #
!
!
!
!
line con 0
password 7 08701E1D
login
!
line aux 0
!
line vty 0 4
password 7 08701E1D
login
line vty 5 15
password 7 08701E1D
login
!
!
!
!
end

```

Листинг A.5 — Конфигурация устройства SW_2_L2_DERDZYAN

```

!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SW_2_L2_DERDZYAN
!
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
!
no ip domain-lookup
!
!
```

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
  switchport access vlan 102
  switchport mode access
!
interface FastEthernet0/2
  switchport access vlan 102
  switchport mode access
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
```

```
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface GigabitEthernet0/2
  switchport trunk allowed vlan 2-5,101-109,111
  switchport mode trunk
!
interface Vlan1
  no ip address
  shutdown
!
banner motd #
Authorized users only! #
!
!
!
line con 0
  password 7 08701E1D
  login
!
line vty 0 4
  password 7 08701E1D
  login
line vty 5 15
  password 7 08701E1D
  login
!
!
!
!
end
```