

АННОТАЦИЯ

В данном документе описан процесс проектирования и моделирования локальной сети предприятия. Определена постановка задачи, требования к проектируемой сети, чертежи здания, а также выбрано оборудование, необходимое для реализации сети. Составлены сценарии настройки активного сетевого оборудования.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 ПОСТАНОВКА ЗАДАЧИ	6
2 ОПРЕДЕЛЕНИЕ КОЛИЧЕСТВА И МЕСТОРАСПОЛОЖЕНИЯ КРОССОВЫХ, СЕРВЕРНЫХ ПОМЕЩЕНИЙ И ТЕЛЕКОММУНИКАЦИОННЫХ РОЗЕТОК СЕТИ	9
3 РАЗРАБОТКА ЛОГИЧЕСКОЙ СТРУКТУРЫ СЕТИ	12
3.1 Выбор и обоснование структуры сети	12
4 ВЫБОР АКТИВНОГО ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ	14
5 НАЗНАЧЕНИЕ СЕТЕВЫХ АДРЕСОВ КОММУНИКАЦИОННОМУ ОБОРУДОВАНИЮ И ПОДСЕТЯМ	19
6 РАЗРАБОТКА ФИЗИЧЕСКОЙ СТРУКТУРЫ СЕТИ	22
6.1 Выбор типов кабелей	22
6.2 Схема размещения компонентов СКС	25
6.3 Расчет величины расхода кабеля	27
6.4. Расчет габаритных размеров декоративного кабельного короба	31
6.5. Выбор пассивного телекоммуникационного оборудования	32
7 РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ПРЕДПРИЯТИЯ	35
7.1 Политика безопасности взаимодействия с Интернет	35
7.2 Инструкция по защите от вирусов	36
7.3 Политика безопасности удаленного доступа	37
7.4 Инструкция по выбору и использованию паролей	37
8 СЦЕНАРИИ КОНФИГУРАЦИИ ОБОРУДОВАНИЯ	38
9 КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ	43
ЗАКЛЮЧЕНИЕ	51
СПИСОК ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ	53
ПРИЛОЖЕНИЕ А	54

ВВЕДЕНИЕ

Современные предприятия и организации повсеместно оборудованы современными информационными системами для решения различных задач вроде регулирования документооборота и электронной переписки. Следовательно, возникает необходимость налаживания сетевого взаимодействия в рамках предприятия между работниками для обмена данными, синхронизации процесса работы и выхода в сеть Интернет. Поэтому использование современных сетевых технологий на предприятии является более чем актуальным.

Цель настоящего курсового проекта – спроектировать локальную сеть средней организации, обеспечивающей информационные услуги ее пользователям с требуемым уровнем безопасности

Для достижения цели курсового проекта должны быть решены следующие задачи:

- определение месторасположения серверных и кроссовых помещений и количества местоположения телекоммуникационных розеток;
- разработка логической структуры сети;
- выбор активного телекоммуникационного оборудования;
- распределения сетевых адресов;
- разработка структурированной кабельной системы и выбор пассивного сетевого оборудования;
- разработка физической структуры сети и схемы электрических соединений;
- разработка политики безопасности, списков доступа к ресурсам сети и сценариев реализации политики безопасности;
- моделирование сети и коррекция схемы сети по результатам моделирования.

Настоящий документ содержит полную информацию по предмету курсового проектирования: текстовое изложение особенностей проектируемой сети, систем телекоммуникационного заземления, администрирования и электропитания. В ней находятся такие разделы, как “Разработка логической структуры сети”, “Обоснование и выбор активного телекоммуникационного оборудования”, “Назначения сетевых адресов подсетям и телекоммуникационному оборудованию”, “Разработка физической структуры сети”, “Политика безопасности в сети”, “Конфигурация коммуникационного оборудования сети”, “Компьютерное моделирование функционирования сети” и “Заключение”.

В разделе “Разработка логической структуры сети” проводится выбор и обоснования структуры проектируемой сети, а также обосновывается деление на независимые виртуальные сети.

В разделе “Выбор активного телекоммуникационного оборудования” приводятся соображения, на основании которых было выбрано активное телекоммуникационное оборудование.

В разделе “Назначение сетевых адресов подсетям и телекоммуникационному оборудованию” необходимо назначить проектируемой сети внешний IP-адрес и сетевую маску, а также присвоить адреса и сетевые маски всем виртуальным сетям и рабочим станциям.

В разделе “Разработка физической структуры сети” осуществляется разработка схемы размещения компонентов структурированной кабельной системы (СКС) сети, построение кабельных трасс, а также проводится обоснование и выбор типов кабелей для горизонтальной и вертикальной систем СКС.

В разделе “Разработка политики информационной безопасности в сети предприятия” должны быть составлены тексты инструкций, в которых излагаются положения специфической политики для заданных техническим

заданием типов сервисов, общие правила доступа пользователей к информационным ресурсам, а также разработаны правила доступа отдельных категорий пользователей к локальным и глобальным сетевым ресурсам.

В разделе “Разработка скриптов конфигурации коммуникационного оборудования сети” изображена логическая схема сети с указанием типа оборудования, адресов виртуальных подсетей, интерфейсов маршрутизаторов и коммутаторов, а также приводятся полные тексты скриптов конфигурации.

В разделе “Компьютерное моделирование функционирования сети” приводится компьютерная модель спроектированной сети и результаты проверки в соответствии с техническим заданием.

1 ПОСТАНОВКА ЗАДАЧИ

Необходимо смоделировать для организации межсетевое взаимодействие в пределах предприятия. Организация располагается 3 этажах здания. На предприятии функционирует 6 внутренних и 3 внешних сервера, подключенных к узлу этажа. Сеть реализована посредством свичей, с делением на подсети. Деление на виртуальные локальные сети не используется. Тип глобальной сети - DSL, классовой способ адресации. Важной чертой сети является ее безопасность. В сети будет представлена политика безопасности удаленного доступа и правил предоставления доступа. Внутренняя безопасность низкая. Применяемый протокол маршрутизации в проектируемой сети OSPF.

В качестве производителя коммуникационного оборудования выбрана фирма Cisco.

Количество потенциальных пользователей сети предприятия N_{π} определяется площадью помещений, занимаемых предприятием:

$$N_{\pi} = \frac{\sum S_i}{5} = \frac{1481}{5} = 296,$$

где S_i — площадь комнат здания. $N_{\pi} = 296$ потенциальных пользователей сети предприятия.

Организация «It Solutions» под руководством Горбенко К.Н. оказывает услуги по разработке веб-ориентированных и мобильных приложений. Используемые сетевые сервисы:

- WWW;
- FTP;

- E-mail;
- Data Base.

Основными информационными технологиями, используемыми сотрудниками будут:

- ОС Windows 10;
- Android Studio;
- JetBrains Webstorm;
- PostMan;
- Adobe Illustrator;
- Adobe Photoshop;
- MS Office;
- 1С Бухгалтерия.

Данные технологии требуют постоянного доступа к сети Интернет, в частности, для координации действий разработчиков, а также для возможности централизованного отслеживания действий в ходе реализации проектов, а также их качества и эффективности.

На предприятии существуют следующие рабочие группы:

- руководители предприятия (1 РГ);
- секретари (2 РГ);
- группа дизайнеров (3 РГ);
- группа тестировщиков (4 РГ);

- группа backend-разработки (5 РГ);
- группа frontend-разработки (6 РГ);
- группа аналитиков (7 РГ);
- группа разработчиков мобильных приложений (8 РГ);
- администраторы сети (9 РГ);

2 ОПРЕДЕЛЕНИЕ КОЛИЧЕСТВА И МЕСТОРАСПОЛОЖЕНИЯ КРОССОВЫХ, СЕРВЕРНЫХ ПОМЕЩЕНИЙ И ТЕЛЕКОММУНИКАЦИОННЫХ РОЗЕТОК СЕТИ

Организация, занимающаяся предоставлением услуг предприятиям и населению располагается в многоэтажном здании и занимает 3 этажа. Общая протяженность коридора, согласно чертежу, равна 48,7 м.

На первом этаже помещение №312 площадью 16,2 кв. м. может быть отведено под расположение серверов и коммутационного оборудования. Также на первом этаже можно выделить помещение №301 площадью 35 кв. м в качестве главного распределительного пункта предприятия.

Таблица 1.1 – Распределение ТР и рабочих групп на первый этаж

№ комнаты	Площадь помещения, м ²	Количество ТР	Количество рабочих групп
301	34.8	2	1
302	17.4	4	1
303	55.2	12	2
304	30	6	1
305	36	8	1
306	17.4	4	1
307	17.4	4	1
308	36	8	1
309	35.4	8	1
310	54	11	2
311	34.2	7	1

312	16.2	4	1
313	54	11	2
314	54	11	1
Итого	492	98	17

На втором этаже помещение №209 площадью 18 кв. м. может быть отведено под расположение серверов и коммутационного оборудования.

Таблица 1.2 – Распределение ТР и рабочих групп на второй этаж

№ комнаты	Площадь помещения, м ²	Количество ТР	Количество рабочих групп
201	53.82	11	2
202	53.82	11	2
203	52.44	11	2
204	38.64	8	1
205	34.5	7	1
206	18	4	1
207	36	8	1
208	36	8	1
209	18	4	1
210	36	8	1
211	36	8	1
212	36	8	1
213	53.82	11	2
Итого	503,04	107	17

На третьем этаже помещение №505 площадью 18 кв. м. может быть отведено под расположение серверов и коммутационного оборудования.

Таблица 1.3 – Распределение ТР и рабочих групп на третий этаж

№ комнаты	Площадь помещения, м ²	Количество ТР	Количество рабочих групп
501	53.82	11	2
502	128.4	26	2
503	53.82	11	2
504	72	15	2
505	18	4	1
506	72	15	2
507	34.5	7	1
508	53.82	11	2
Итого	486,36	96	14

3 РАЗРАБОТКА ЛОГИЧЕСКОЙ СТРУКТУРЫ СЕТИ

3.1 Выбор и обоснование структуры сети

В данном разделе приводятся возможные различные варианты структур локальной сети предприятия, часть из которых рассмотрены в подразделе 2, анализируются их достоинства и недостатки и обосновывается логическая структура проектируемой компьютерной сети, удовлетворяющая поставленным требованиям, в частности, позволяющей масштабирование сети, обеспечивающей повышенную надежность. Здесь же должен быть представлен чертеж логической структуры и его подробное описание (состав и функционирование).

По общим правилам проектирования сеть предприятия необходимо поделить на 3 основных сегмента: локальная сеть, DMZ и выход в Интернет.

Локальная сеть включает в себя подсети трех этажей предприятия, связанных L3-коммутатором на магистральном уровне. Каждый этаж также оборудован L3-коммутатором (уровень распределения). К этому коммутатору подключаются все комнаты этажа, в том числе и серверная. Серверная комната включает в себя DHCP-сервер и сервер 1С. Каждая комната оборудована L2-коммутатором и множеством рабочих мест. Каждый ПК имеет выход в Интернет и доступ к DMZ. Сервера в целях безопасности не имеют доступа в Интернет и к DMZ.

DMZ – демилитаризованная зона, включающая в себя сервера, имеющих обязательный доступ в Интернет. Проектируется в целях улучшения безопасности сети предприятия. В данном случае DMZ включает в себя два веб-сервера и сервер DNS.

Выход в Интернет обеспечивается за счет подключения DSL-модема и эмулируется специальной сетью со статическим IP-адресом. Общая логическая структура локальной сети представлена рисунком 3.1.

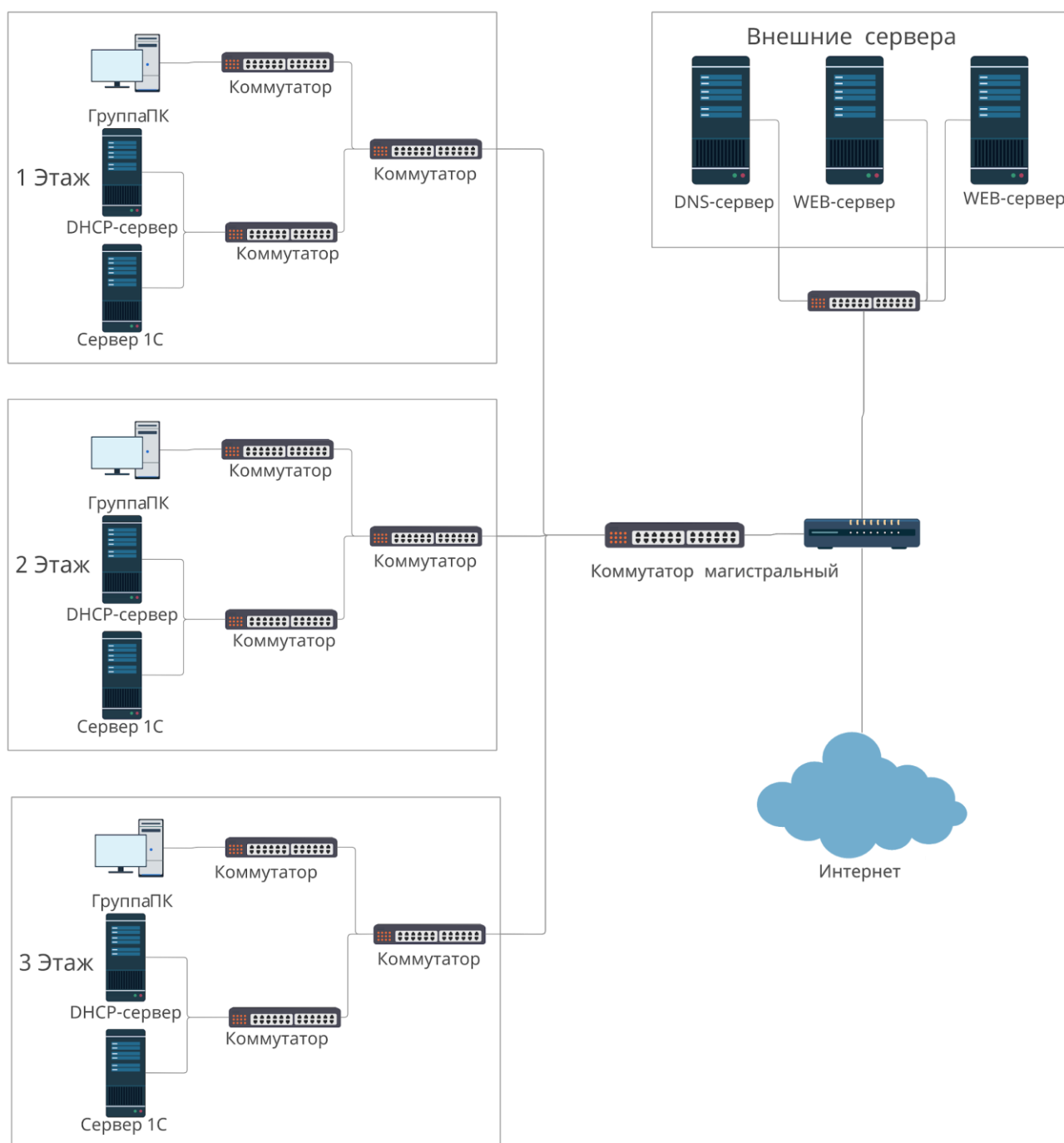


Рисунок 3.1 – Логическая схема проектируемой сети

4 ВЫБОР АКТИВНОГО ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

В локальных компьютерных сетях на уровне доступа пользователей к сети целесообразно использовать коммутаторы фирмы Cisco типа Catalyst 29xx. Коммутаторы этой серии представляют собой полнофункциональную линию коммутаторов 10/100 Ethernet с автоматическим выбором скорости передачи и с поддержкой технологии создания виртуальных сетей. Устройства этой серии обеспечивают наилучшее соотношение цена/производительность среди устройств данного класса. Коммутаторы Catalyst 29XX имеют очень высокую производительность, простоту в эксплуатации и гибкостью в использовании. Эти устройства могут применяться как для создания высокопродуктивных рабочих групп, так и для объединения групп серверов и коммутаторов предыдущего уровня, например, Catalyst 1900/2820. Коммутаторы серии Catalyst 29XX поставляются с пожизненной гарантией, которая предусматривает бесплатный заводской ремонт оборудования в течение всего времени поддержки устройства.

Для проектируемой компьютерной сети для обеспечения подключения на уровне доступа 62-х рабочих станций целесообразно использовать сетевые коммутаторы настольного типа Cisco Catalyst 2950-24. Коммутатор Catalyst 2950C-24 – это 25-х портовый коммутатор уровня доступа, предназначенный для построения малых и средних локальных сетей. Устройство рассчитано на круглосуточную работу и характеризуется высокой производительностью и широкими функциональными возможностями.

Коммутатор автоматически определяет скорость передачи на каждом порту (10/100 Мбит/с), поддерживает протокол качества обслуживания (QoS), предоставляет возможность управления группой коммутаторов и допускает соединения коммутаторов в стек. Основные технические параметры коммутатора типа Catalyst 2950 приведены в таблице 2.1.

Таблица 2.1 — Технические характеристики коммутатора доступа

Параметр	Значение
Тип сети	Fast Ethernet Ethernet
Количество базовых портов	24 (24 макс.)
Буфер памяти (на один порт)	8 МБ
Скорость передачи по UPLINK	100 Мбит/с
Индикаторы	- активное соединение - полнодуплекс / полудуплекс - состояние соединения - уровень загрузки - электропитание
Поддерживаемые стандарты	- IEEE 802.3 (Ethernet) - IEEE 802.3u (Fast Ethernet)
Размер таблицы MAC адресов (L2)	8192
Методы коммутации	store-and-forward
Протоколы удаленного управления	- SNMP - Telnet - Console
Пропускная способность	6,8 Гбит/с
Среда передачи	Ethernet 10/100BaseT - категория 5 НВП - скорость передачи до 100 Мбит/с - длина сегмента до 100 м Ethernet 100baseFX - MMF 62,5 микрон

	- скорость передачи до 100 Мбит/с - длина сегмента до 2 км
Интерфейсы	24 × Ethernet 10/100BaseT • RJ-45 (half / full duplex mode) 2 × Ethernet 100baseFX • MT-RJ (half / full duplex mode)
Электропитание	встроенный блок питания - 200 ...240 В (переменный ток) - потребляемая мощность 30 Вт
Габариты (Высота × Ширина × Глубина), Вес	44,5 × 4,36 × 24,18 мм, 3 кг

В качестве магистрального коммутатора в проектируемой сети целесообразно использовать коммутаторы третьего уровня типа Cisco Catalyst 3500. В состав семейства коммутаторов Catalyst 3500XL входит три модели:

1) **WS-C3512-XL** — содержит 12 универсальных портов 10/100 Mbps Ethernet с автоматическим определением скорости и режима передачи, а также два порта Gigabit Ethernet;

2) **WS-C3524-XL** — содержит 24 универсальных порта 10/100 Mbps Ethernet с автоматическим определением скорости и режима передачи, а также два порта Gigabit Ethernet;

3) **WS-C3508G-XL** — содержит 8 портов Gigabit Ethernet. Коммутаторы семейств 2900XL, 3500XL могут объединяться в стеки (до 16 устройств) при помощи соединений Fast Ethernet, Fast EtherChannel (агрегирование Fast Ethernet по 2 или 4 канала), а также Gigabit Ethernet и Gigabit EtherChannel. Максимальное количество портов, которое может быть установлено в одном стеке равно 380. Такой стек является единым объектом сетевого управления, которое может выполняться как при помощи командного языка CLI с консоли или при помощи

протокола telnet, так и при помощи специализированных систем управления типа CWSI (Cisco Works for Switched Internetworks), так и при помощи WEB-технологии с любой рабочей станции, оснащенной программами просмотра Netscape или Internet Explorer.

Для проектируемой сети, с учетом возможных расширений, достаточно установить 12-портовый маршрутизирующий коммутатор типа WS-C3512-XL. Технические характеристики этого коммутатора приведены в таблице 2.2.

Таблица 2.2 — Технические характеристики коммутатора Catalyst WS-C3512-XL

Параметр	Значение
Тип сети	Fast Ethernet Ethernet
Количество базовых портов	24 (24 макс.)
Производительность	10 Гбит/с
Пропускная способность	7,5 миллионов (64-х байтовых) пакетов в с
Буфер памяти (на один порт)	8 МБ
Скорость передачи по UPLINK	100 Мбит/с
Поддерживаемые стандарты	- IEEE 802.3 (Ethernet) - IEEE 802.3u (Fast Ethernet)
Размер таблицы MAC адресов (L2)	8192
Поддерживаемые стандарты	1) IEEE 802.3x full duplex; 2) IEEE 802.1D Spanning-Tree Protocol; 3) IEEE 802.1Q VLAN; 4) IEEE 802.3z, IEEE 802.3x;

	<p>5) IEEE 802.3u 100BaseTX and 100BaseFX specification;</p> <p>6) IEEE 802.3 10BaseT specification;</p> <p>7) IEEE 802.3z, IEEE 802.3x 1000BaseX specification;</p> <p>8) 1000BaseX (GBIC) — 1000BaseSX, 1000BaseLX/LH, 1000BaseZX.</p>
--	--

5 НАЗНАЧЕНИЕ СЕТЕВЫХ АДРЕСОВ КОММУНИКАЦИОННОМУ ОБОРУДОВАНИЮ И ПОДСЕТЯМ

Внешний IP-адрес и сетевая маска выделяется провайдером Интернет-услуг по запросу предприятия. Пусть согласно варианту предприятию выделен в постоянное пользование один бесклассовый адрес 200.106.32.111.

Известно, что для внутреннего использования в локальных сетях рекомендованы следующие частные адреса (таблица 4).

Таблица 5.1 — Диапазоны частных адресов

Класс	Начальный адрес	Конечный адрес	Число сетей
A	10.0.0.1	10.255.255.25 5	1
B	172.16.0.0.	172.31.255.25 5	16
C	192.168.0.0.	192.168.255.2 5	255

Так как предприятие располагается в несколько этажей, то для удобства администрирования в качестве адреса сети целесообразно выбрать адрес 10.Z.Y.X с сетевым префиксом длиной 24 бита.

Для реализации архитектуры локальной сети предприятия целесообразно использовать деление на подсети. В данном случае достаточно оформить 4 отдельные подсети: 10.2.1.0 (255.255.255.0) – подсеть рабочих станций первого этажа; 10.2.2.0 (255.255.255.0) – подсеть рабочих станций второго этажа; 10.2.3.0 (255.255.255.0) – подсеть рабочих станций третьего этажа; 10.1.0.0 (255.255.0.0) – подсеть внутренних серверов;

Далее необходимо привести таблицу с адресами всех компьютеров, расположенных в помещениях организации, для которой проектируется сеть. В этой таблице целесообразно указать номера коммутаторов/маршрутизаторов и номера портов, к которым подключаются клиентские компьютеры и серверы. Фрагмент таблицы адресов с номерами портов для рассматриваемого примера представлен в таблице 5.1.

Таблица 5.1 – Назначение сетевых адресов коммуникационному оборудованию

№№ ком- нат	Номер/название рабочей группы	Адрес
301	9	10.2.1.1-10.2.1.2
302	1	10.2.1.3-10.2.1.6
303	2,3	10.2.1.7-10.2.1.18
304	3	10.2.1.19-10.2.1.25
305	4	10.2.1.26-10.2.1.35
306	5	10.2.1.36-10.2.1.39
307	5	10.2.1.40-10.2.1.43
308	5	10.2.1.43-10.2.1.50
309	6	10.2.1.51-10.2.1.58
310	6,7	10.2.1.59-10.2.1.60
311	7	10.2.1.61-10.2.1.67
312	9	10.2.1.68-10.2.1.43
313	7,8	10.2.1.44-10.2.1.53
314	8	10.2.1.54-10.2.1.64
201	2	10.2.2.1-10.2.2.11
202	2	10.2.2.12-10.2.2.22
203	3	10.2.2.23-10.2.2.33
204	3	10.2.2.34-10.2.2.41
205	4	10.2.2.42-10.2.2.48
206	4	10.2.2.49-10.2.2.53
207	5	10.2.2.54-10.2.2.61
208	5	10.2.2.62-10.2.2.69
209	9	10.2.2.70-10.2.2.73
210	6	10.2.2.74-10.2.2.81
211	7	10.2.2.82-10.2.2.89
212	8	10.2.2.90-10.2.2.93
213	8	10.2.2.94-10.2.2.101
501	2	10.2.3.1-10.2.3.11
502	3	10.2.3.12-10.2.3.37
503	4	10.2.3.38-10.2.3.48
504	5	10.2.3.49-10.2.3.63

505	9	10.2.3.64-10.2.3.67
506	6	10.2.3.68-10.2.3.82
507	7	10.2.3.83-10.2.3.89
508	8	10.2.3.90-10.2.3.100
312	Сервер внутренний DHCP-1	10.1.1.2
312	Сервер внутренний 1С-1	10.1.1.3
209	Сервер внутренний DHCP-2	10.1.2.2
209	Сервер внутренний 1С-2	10.1.2.3
505	Сервер внутренний DHCP-2	10.1.3.2
505	Сервер внутренний 1С-2	10.1.3.3

6 РАЗРАБОТКА ФИЗИЧЕСКОЙ СТРУКТУРЫ СЕТИ

6.1 Выбор типов кабелей

Наиболее «подвижной» частью любой локальной сети является горизонтальная подсистема. На этом уровне добавление новых пользователей, перемещение рабочих группы происходят гораздо чаще, чем изменения в вертикальных подсистемах между этажами. Поэтому наиболее рациональным вариантом является применение медного неэкранированного кабеля UTP.

С учетом того, что на уровне доступа передача данных выполняется преимущественно со скоростью 100 Мбит/с и с учетом возможности в перспективе увеличения скорости передачи для горизонтальной подсистемы, выбираем кабель типа UTP48-C5-SOLID-INDOOR.

Это кабель 5-й категории типа неэкранированная витая пара (UTP), состоящий из 4 пар одножильных (solid) медных проводников. Кабель соответствует стандарту пожарной безопасности UL 444 и UL 1581 и имеет следующие технические характеристики:

- Диаметр проводника: $0,54 \pm 0,01$ мм (24 AWG);
- Изоляция — полиэтилен повышенной плотности, минимальная толщина 0,18 мм;
- Диаметр провода в изоляции $0,99 \pm 0,02$ мм;
- Цвет витых пар: синий-белый/синий, оранжевый-белый/оранжевый, зеленый-белый/зеленый, коричневый-белый/коричневый;
- 4 витые пары с полиэтиленовым разделителем, покрыты поливинилхлоридной оболочкой (PVC) с минимальной толщиной оболочки 0,4 мм;
- Внешний диаметр кабеля равен $5,3 \pm 0,2$ мм;

- Рабочая температура кабеля от -20°C до $+75^{\circ}\text{C}$;
- Радиус изгиба кабеля: $8\varnothing$ во время инсталляции, $6\varnothing$ при вертикальном кабелировании и $4\varnothing$ диаметра при горизонтальном кабелировании;
- Стандартная упаковка размером $21,5 \times 42 \times 42$ см (Ш× В×Г) — 305 м;
- Вес кабельной бухты без упаковки 12,9 кг.

Кабель характеризуется следующими электрическими параметрами:

- Максимальное сопротивление проводника при температуре 20°C равно $9,38\text{ Ом}/100\text{ м}$;
- Дисбаланс сопротивления не превышает 5%;
- Емкостной дисбаланс пары по отношению к земле равен $330\text{ пф}/100\text{ м}$;
- Сопротивление на частоте от 0,772 до 100 МГц составляет $85\ldots115\text{ Ом}$;
- Максимальная рабочая емкость равна $5,6\text{ нф}/\text{м}$;
- Неравномерность задержки $45\text{ нс}/100\text{ м}$;
- Задержка распространения $<536\text{ нс}/100\text{ м}$.

Частотные характеристики кабеля приведены в таблице 6.1.

Таблица 6.1 – Частотно-зависимые характеристики передачи

Частота МГц	Затухание дБ/100 м	NEXT дБ	ACR дБ/100м	PSNEXT дБ	EL-FEXT дБ/100м	PSEL-FEXT дБ/100м	RL дБ
31,25	11,4	45,9	34,6	42,9	33,9	30,9	23,6
62,5	16,5	41,4	25,8	38,4	27,8	24,8	21,5
100	21,3	38,3	19,0	35,3	23,8	20,8	20,1
155	27,2	35,5	10,8	32,5	19,9	16,9	18,7

Параметры передачи многомодового оптоволоконного кабеля приведены в таблице 6.2, а параметры одномодового в таблице 6.3.

Таблица 6.2 – Оптические параметры многомодового оптоволоконна

Тип Волокна	Длина волны, нм	Затухание (средн/ макс) ,дБ/км	Коэффициент широкополосной оси, МГц·км	Дальность передачи для Ethernet, м		Коэффициент преломления
				1GbE	10 GbE	
62,5/125 OM1	850	3,0/3,2	>200	275	33	1,495
	1300	0,7/0,9	>600	550	–	1,490
50/125 OM2	850	2,6/2,8	>600	550	82	1,481
	1300	0,6/0,9	>1200	550	–	1,476

Таблица 6.3 – Оптические параметры одномодового оптоволоконна ITU-G.652B

Тип волокна	Диаметр, мкм	Длина волны, нм	Затухание (среднее/максимальное), дБ/км	Дисперсия, пс/(нм·км)	PMD, пс/км1/2	Коэфф. преломления
9/125	9,2±0,4	1310	0,35/0,5	< 3,5	–	1,467
	125±0,5	1550	0,21/0,3	< 18	< 0,2	1,467

Параметр PMD (поляризационная-модовая дисперсия) — это дисперсия, вызываемая небольшой асимметричностью поперечного сечения волокна.

Асимметричность приводит к тому, что одна из двух основных ортогональных поляризованных мод передается по оптическому каналу связи быстрее, чем другая. В связи с тем, что приемное устройство принимает комбинацию этих двух мод, то результирующий импульс становится шире входного импульса, поскольку он подвергся дисперсии, т.е. происходит расширение импульса.

Для выполнения силовой проводки используется трехжильный медный кабель типа ВВГ 3×1,5 (Виниловая оболочка, Виниловая изоляция, Гибкий). Сечение кабеля 1,5 мм² выбирается из расчета максимального потребляемого тока 15 А (мощность 3,3 кВт) на одну розетку. Коммутаторы между собой соединены оптическим волокном OM1.

6.2 Схема размещения компонентов СКС

Схема размещения компонентов сети разрабатывается на основе чертежа здания, в котором располагается организация. Во всех помещениях на каждом рабочем месте устанавливаются телекоммуникационные розетки (ТР) с двумя гнездами типа RJ-45 и по три силовых розетки с напряжением 220В.

Телекоммуникационные розетки закрепляются в кабельных коробах на высоте 40 см от уровня пола.

Все телекоммуникационные кабели прокладываются в декоративных пластмассовых кабельных каналах, которые закрепляются на стене помещения. Кабельный канал разделен на две секции. Одна служит для укладки телекоммуникационных кабелей, а вторая — для силовых кабелей. Телекоммуникационные розетки монтируются на корпусе короба, либо на стене. Силовые розетки в количестве 2 шт на каждое рабочее место закрепляются на расстоянии 0,8 м от уровня пола.

Вывод пучка кабелей горизонтальной подсистемы осуществляется через металлический патрубок (конduit) диаметром 80 мм, который пропускается через стену помещения на расстоянии 0,2 м от потолка. В коридоре коммуникационные кабели укладываются в кабельный лоток, который закреплен между потолочным перекрытием и подвесным потолком.

Фрагмент схемы размещения компонентов СКС с указанием типов и параметров кабелей в помещении, в котором располагается рабочая группа организации, показан на рисунке 6.1.

Каждое из кроссовых помещений содержит коммутационный шкаф, в котором находятся коммутаторы и внутренние сервера. Кроме того на каждом этаже помещены внутренние серверы этажа в телекоммуникационный шкаф. Каждое кроссовое помещение также оборудовано рабочим столом, который

необходим инженеру для ремонта вышедшего из строя оборудования. Схема серверного помещения представлена рисунком 6.2.

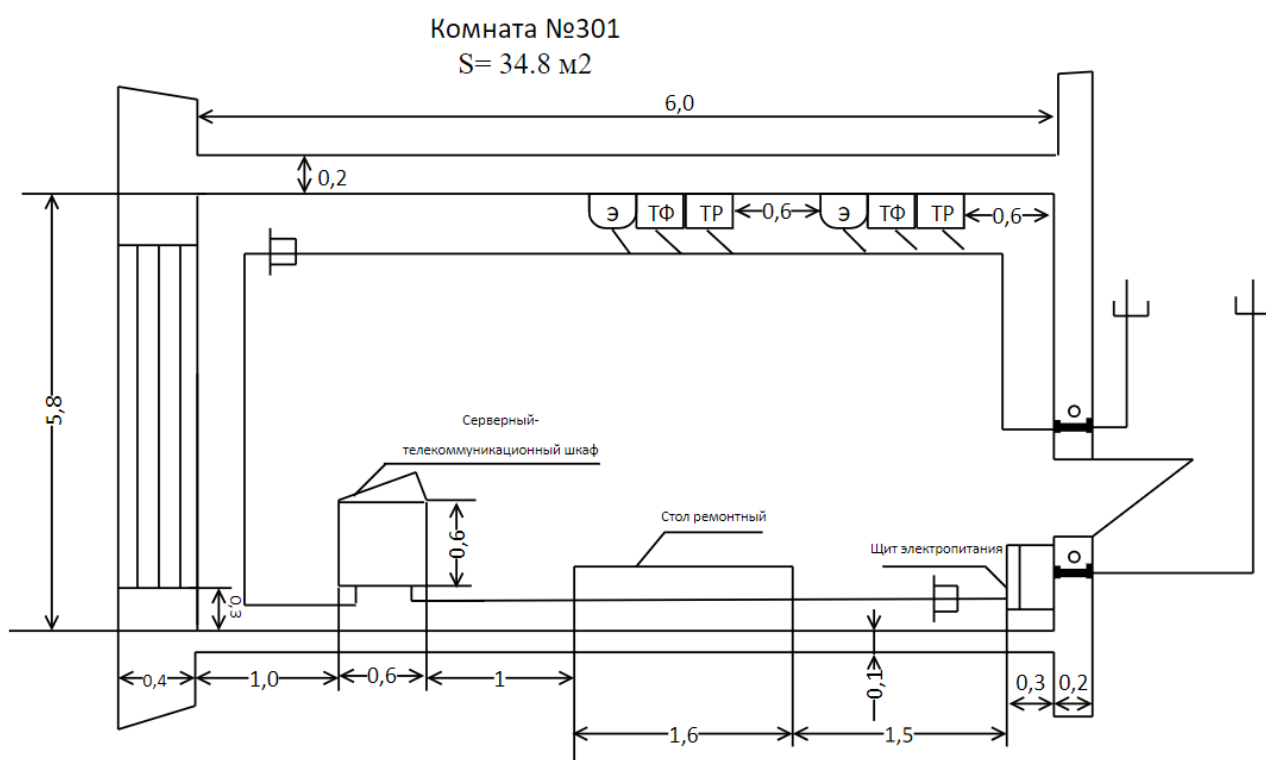


Рисунок 6.1 - Схема размещения компонентов СКС в техническом помещении

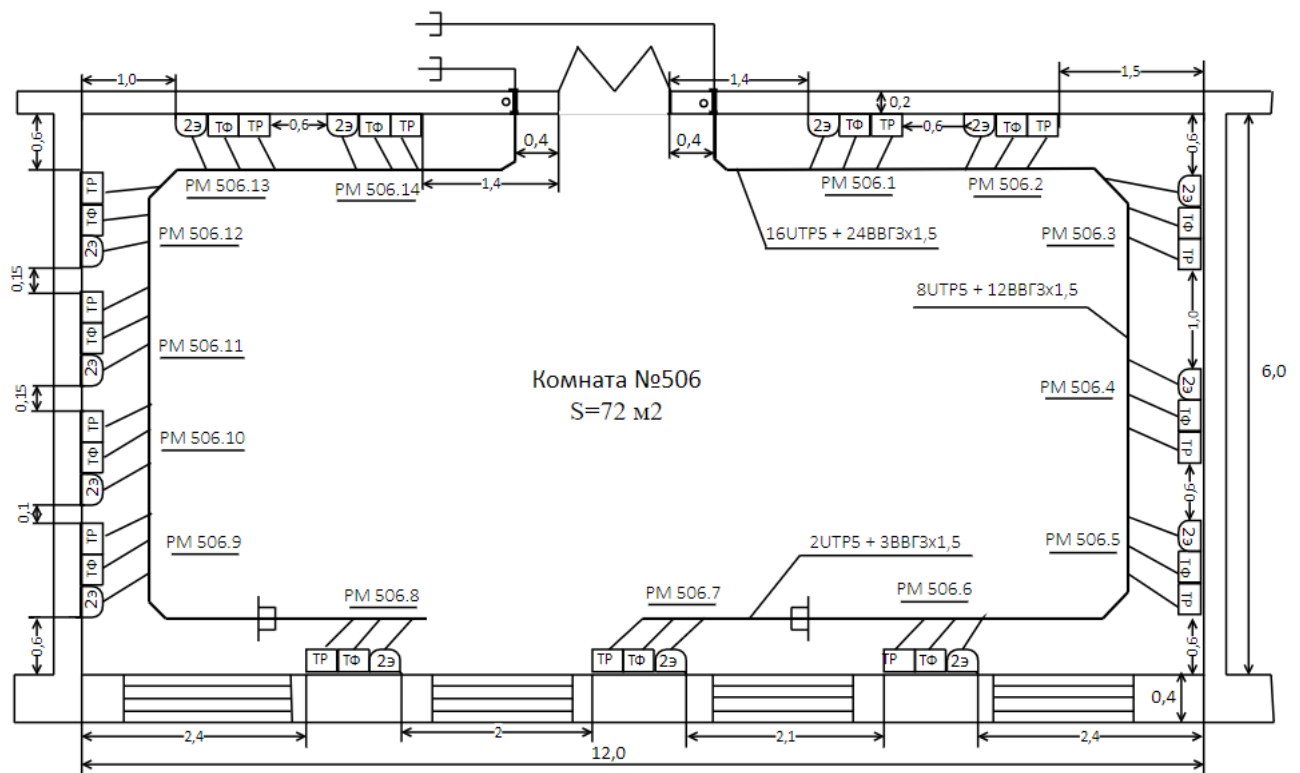


Рисунок 6.2 - Схема помещения размещения рабочей группы

6.3 Расчет величины расхода кабеля

Для определения максимальной и минимальной длины кабелей типа витая пара горизонтальной подсистемы построим профили кабельных трасс на основании планов помещений. Расчет максимальной и минимальной длины кабелей будет выполнен отдельно для каждого этажа.

Для первого этажа:

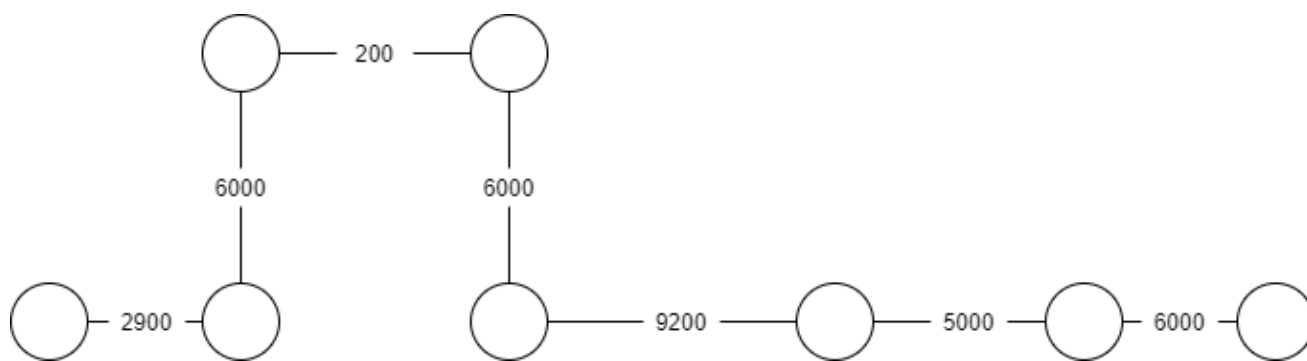


Рисунок 6.3 – Профиль кабельной трассы первого этажа для минимальной длины линии

Для первого этажа – $L_{\min} = 35300$ мм.

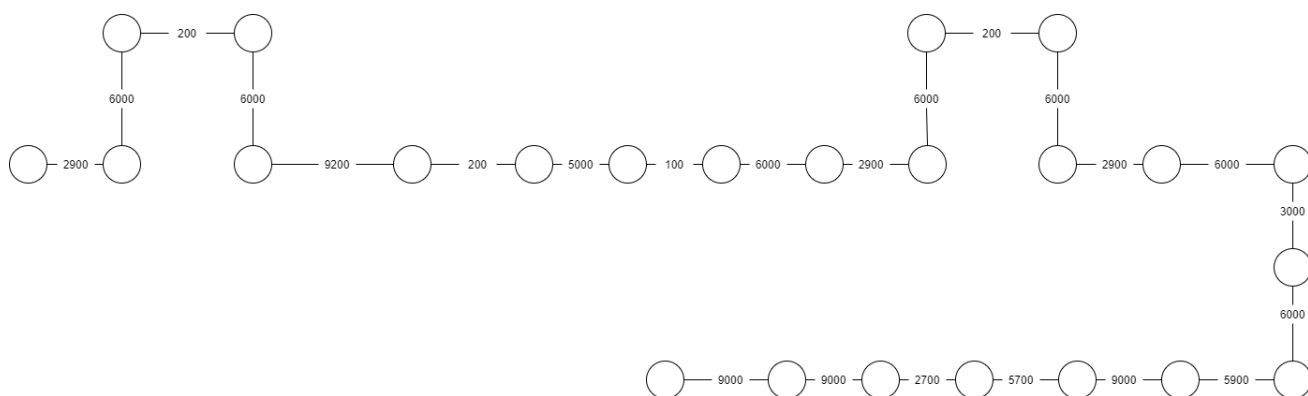


Рисунок 6.4 – Профиль кабельной трассы первого этажа для максимальной длины линии

Для первого этажа – $L_{\max} = 109900$ мм.

$$L_{\text{ср } 1} = (L_{\min} + L_{\max}) / 2 = 72600 \text{ мм.}$$

$$L_1 = 1.1 * L_{\text{ср } 1} * N = 1.1 * 72600 * 105 = 8385300 \text{ мм.}$$

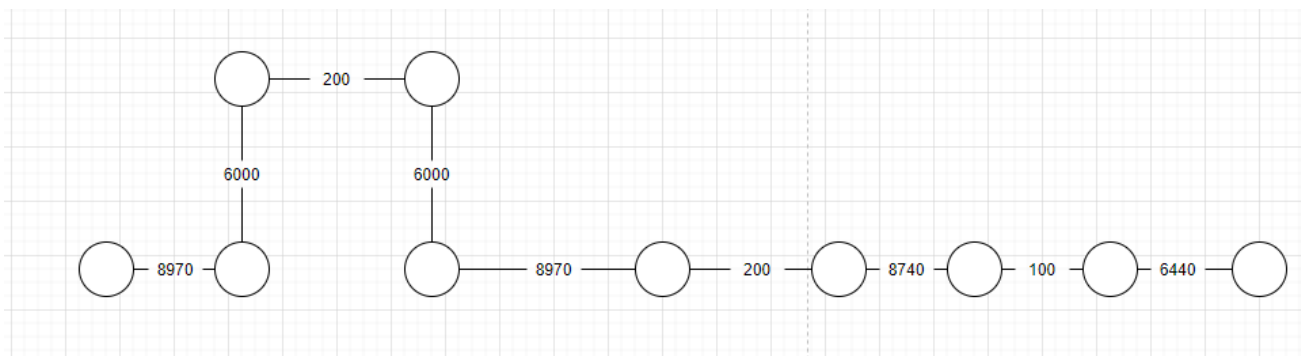


Рисунок 6.5 – Профиль кабельной трассы второго этажа для минимальной длины линии

Для второго этажа – $L_{\min} = 45620$ мм.

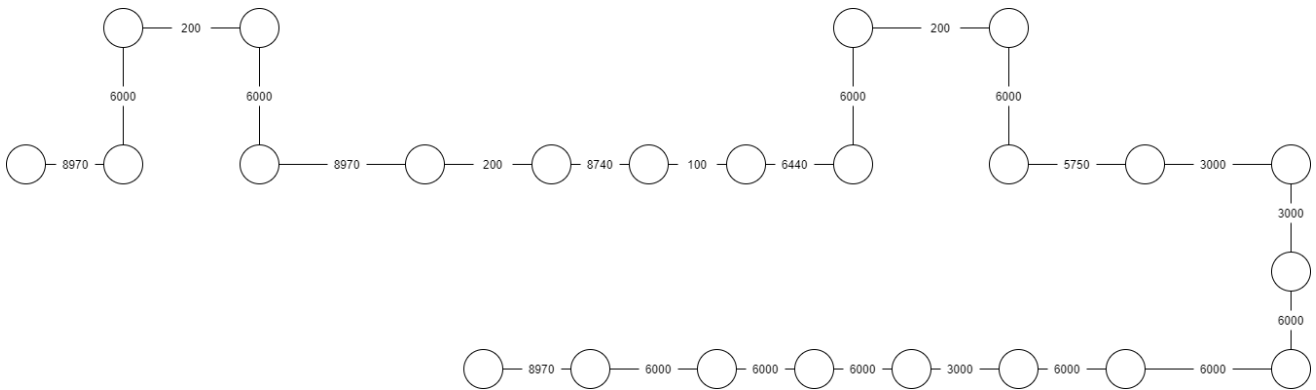


Рисунок 6.6 – Профиль кабельной трассы второго этажа для максимальной длины линии

Для второго этажа – $L_{\max} = 111540$ мм

$$L_{\text{ср } 2} = (L_{\min} + L_{\max}) / 2 = 78580 \text{ мм}$$

$$L_2 = 1.1 * L_{\text{ср } 2} * N = 1.1 * 78580 * 107 = 9248866 \text{ мм}$$

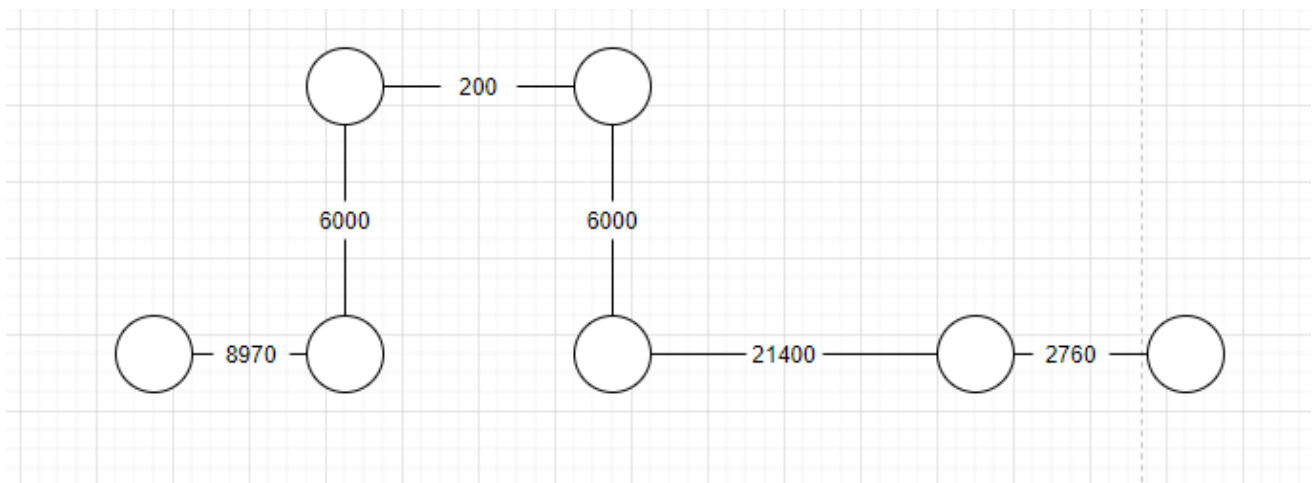


Рисунок 6.7 – Профиль кабельной трассы третьего этажа для минимальной длины линии

Для третьего этажа – $L_{\min} = 45330$ мм.

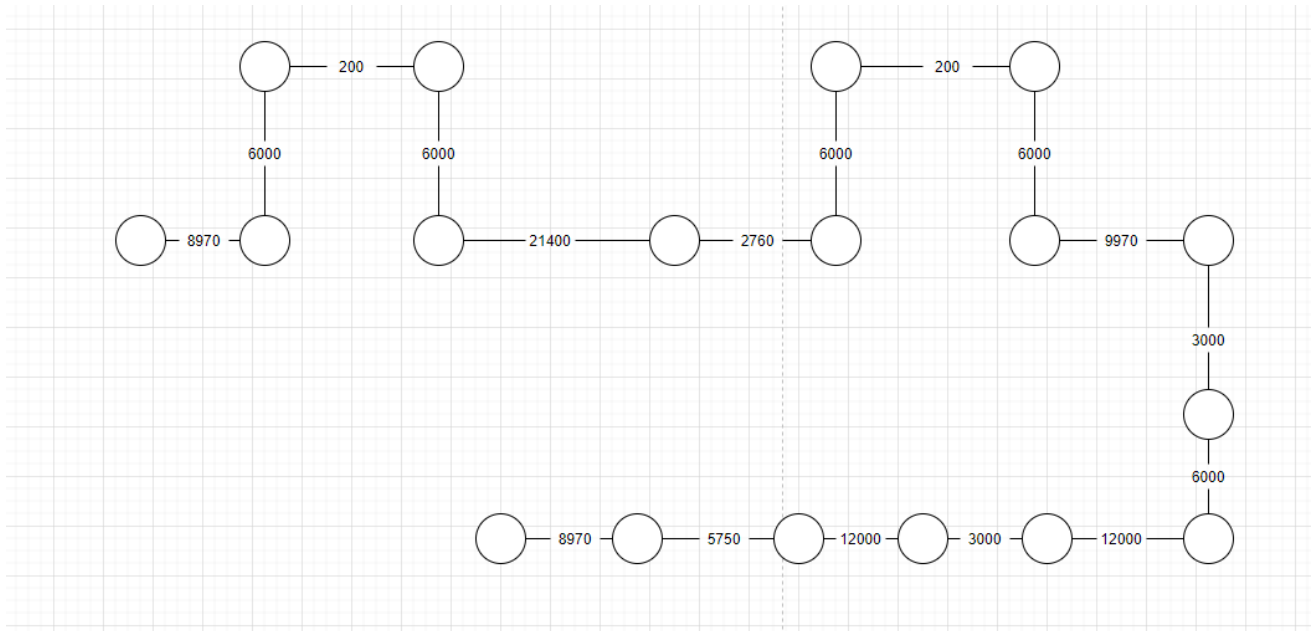


Рисунок 6.8 – Профиль кабельной трассы третьего этажа для максимальной длины линии

Для третьего этажа – $L_{\max} = 118220$ мм

$$L_{\text{ср } 3} = (L_{\min} + L_{\max}) / 2 = 81775 \text{ мм}$$

$$L_3 = 1.1 * L_{\text{ср } 3} * N = 1.1 * 81775 * 100 = 8995250 \text{ мм}$$

Итого:

$$L = L_1 + L_2 + L_3 = 8385300 + 9248866 + 8995250 = 26629416 \text{ мм}$$

Следовательно для реализации сети понадобится около 27 километров витой пары.

6.4. Расчет габаритных размеров декоративного кабельного короба

При расчетах диаметр горизонтального кабеля категории 5е принимается равным 5,2 мм, что соответствует площади поперечного сечения кабеля $S_{\text{Каб}} = 21,2 \text{ мм}^2$. Коэффициент использования площади выбирается равным $k_i = 0,5$, а коэффициент заполнения — $k_z = 0,45$.

С целью уменьшения расхода декоративного короба целесообразно использовать двухсекционный короб, в котором одна секция служит для размещения коммуникационных кабелей, а вторая — для силовых. Для оптоволоконка будем использовать односекционный короб. При этом требуется просчитать необходимые габариты каждой из секций.

Таким образом, требуемое сечение короба определяется по формуле

$$S_{\text{крб}} = (\sum S_{i\text{Ккаб}}) / (k_i k_z) + (\sum S_{j\text{Скаб}}) / (k_i k_z),$$

где $S_{i\text{Ккаб}}$ — сечение i -го коммуникационного кабеля; $S_{j\text{Скаб}}$ — сечение j -го силового кабеля.

Для выбранного кабеля $S_{i\text{Ккаб}} = 9,74 \text{ мм}^2$.

$$S_{\text{крб}} = (116 * 9,74) / (0,5 * 0,45) + (116 * 5,2) / (0,5 * 0,45) = 7703 \text{ мм}^2.$$

(для этажа)

$$S_{\text{крб } 4} = (4 * 9,74) / (0,5 * 0,45) + (4 * 5,2) / (0,5 * 0,45) = 265,6 \text{ мм}^2.$$

$$S_{\text{крб } 5} = (5 * 9,74) / (0,5 * 0,45) + (5 * 5,2) / (0,5 * 0,45) = 308,9 \text{ мм}^2.$$

$$S_{\text{крб } 8} = (8 * 9,74) / (0,5 * 0,45) + (8 * 5,2) / (0,5 * 0,45) = 438,8 \text{ мм}^2.$$

$$S_{\text{крб } 9} = (9 * 9,74) / (0,5 * 0,45) + (9 * 5,2) / (0,5 * 0,45) = 482,1 \text{ мм}^2.$$

$$S_{\text{крб } 12} = (12 * 9,74) / (0,5 * 0,45) + (12 * 5,2) / (0,5 * 0,45) = 612,0 \text{ мм}^2.$$

$$S_{\text{крб } 13} = (13 * 9,74) / (0,5 * 0,45) + (13 * 5,2) / (0,5 * 0,45) = 863,2 \text{ мм}^2.$$

После определения суммарного сечения кабелей выбирается стандартный тип короба с сечением, не меньше рассчитанного.

Результаты расчетов габаритов короба вынесены в таблицу.

Таблица 6.4 — Параметры кабельного короба

Количество обслуживаемых ТР	4	5	8	9	12	13	116
Количество горизонтальных кабелей	8	10	16	18	24	26	232
Требуемая площадь короба, мм ²	265.6	308.9	438.8	482.1	612.0	863.2	7703
Габаритные размеры односекционного короба, мм	40*16	40*16 6	40*16	40*16	40*16	60*16 6	185*50

6.5. Выбор пассивного телекоммуникационного оборудования

При расчетах диаметр горизонтального кабеля категории 5е принимается равным 5,2 мм, что соответствует площади поперечного сечения кабеля $S_{каб} = 21,2 \text{ мм}^2$. Коэффициент использования площади выбирается равным $k_i = 0,5$, а коэффициент заполнения — $k_z = 0,45$.

В качестве коммутационного оборудования для медных кабелей выберем 24-портовые коммутационные патч-панели типа «21-R0-45H024D0-2N1N» категории 5е для разделки кабелей горизонтальной подсистемы. Для подключения кабелей к коммутаторам и маршрутизатору через патч-панели предусмотрены соединительные шнуры (патч-корды) с разъемами «RJ45-RJ45» на обоих концах. Длина соединительных шнуров 1 м.

При монтаже оптоволоконной части подсистемы внутренних магистралей предполагается использовать технологию сварки, которая обеспечивает

минимальные потери в точке сращивания оптических волокон и наибольшую надежность соединения.

Для размещения коммутационного оборудования СКС и активного оборудования ЛВС в здании предусмотрены технические помещения 312, 209, 505. В этих помещениях устанавливается 19-ти дюймовый телекоммуникационный шкаф «CABEUS SH-05C-32U60/60».

Содержимое шкафа:

- 3 патч-панели на 48 портов RJ-45 для терминирования кабелей горизонтальной подсети высотой 2U;
- 3 коммутатора Cisco Catalyst 2960 на 48 портов высотой 2U каждый;
- Два сервера высотой 3U;
- Блок бесперебойного питания высотой 4U;
- Блок электрических розеток высотой 1U;
- Панель вентиляторов потолочная на 2 вентилятора высотой 1U.

В помещении 301, которое служит аппаратной для всего здания, находится 19-ти дюймовый телекоммуникационный шкаф «CABEUS SH-05C-12U60/60» высотой 12U, который в свою очередь снабжен:

- 1 патч-панели на 24 портов RJ-45 для терминирования кабелей вертикальной подсети высотой 1U;
- 1 коммутатор Cisco Catalyst 2960 на 48 портов высотой 2U;
- Маршрутизатор Cisco 4000 высотой 1U;
- Блок бесперебойного питания высотой 4U;
- Блок электрических розеток высотой 1U;
- Панель вентиляторов потолочная на 2 вентилятора высотой 1U.

Перечень пассивного оборудования сети приведен в таблице 6.5.

Таблица 6.5 – Перечень пассивного оборудования сети

№	Наименование компонентов	Ед. изм	Кол- во
1	EuroLAN MiNi настенная информацион- ная розетка RJ45, кат.5е, 2-х портовая	шт	229
2	Кабель UTP 4	м	12958
3	Патч-панель неэкранированная SNR, Cat. 5E, 19", 2U, 24 портов	шт	1
4	Патч-панель неэкранированная SNR, Cat. 5E, 19", 2U, 48 портов	шт	9
5	Модуль вентиляторный потолочный, 380х380 мм, 2 вент	шт	8
6	Шкаф коммутационный напольный 32U «CABEUS SH- 05C-32U60/60»	шт	3
7	Шкаф серверный напольный 12U «CABEUS SH-05C- 12U60/60»	шт	1

7 РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ПРЕДПРИЯТИЯ

Разрабатываемая сеть предоставляет пользователям ряд сервисов, которые не всегда могут быть защищены программным образом. Даже если такие сервисы защищены с помощью шифрования, это не избавляет от возможности утечки данных и взлома. Поэтому компания должна сопровождать ряд политик безопасности. По варианту задания предусмотрено разработать политику безопасности взаимодействия с Интернет, инструкция по защите от вирусов, выбора и использования паролей и удаленного доступа.

7.1 Политика безопасности взаимодействия с Интернет

1. Сотрудники имеет право воспользоваться доступом в глобальную сеть только для выполнения своих обязанностей.
2. Все программы, используемые для доступа к Интернет, должны быть утверждены сетевым администратором и на них должны быть установлены все доработки производителя (patch), связанные с безопасностью.
3. Все загружаемые файлы должны быть проверены антивирусом, заверенным системным администратором.
4. Сотруднику запрещено вносить изменения в конфигурацию компьютера или браузера.
5. Все веб-браузеры должны быть сконфигурированы так, чтобы использовать прокси-сервер для Интернет из состава брандмауэра.
6. При отправке данных на веб-сервер с помощью форм HTML из браузера, удостоверьтесь, что установлен механизм для шифрования сообщения при его отправке (например - SSL (Secure Sockets Layer)).

7.2 Инструкция по защите от вирусов

Регулярно проводимые профилактические работы по выявлению вирусов могут полностью исключить появление и распространение вирусов в ПЭВМ. Поэтому целесообразно включать эти работы в планы работ подразделений. К основным профилактическим работам и мероприятиям относятся:

- 1) ежедневная автоматическая проверка наличия вирусов при включении ПЭВМ;
- 2) регулярная (не реже одного раза в месяц) комплексная проверка наличия вирусов во всех ПЭВМ, даже при отсутствии внешних проявлений вирусов;
- 3) проверка наличия вирусов в ПЭВМ, вернувшихся с ремонта (в том числе гарантийного) в сторонних организациях;
- 4) изучение информации по сообщениям в компьютерных журналах и газетах о новых вирусах;
- 5) создание резервной копии программного продукта сразу же после приобретения;
- 6) системные дискеты и дискеты с наиболее важными программами защищаются от записи на них информации путем установки переключателя на 3-5«-дискетах в положение только чтения - тем самым вирусы не смогут проникнуть на дискеты;
- 7) тщательная проверка всех поступающих и купленных программ и баз данных; проверку необходимо выполнять либо на ПЭВМ без «винчестера», либо на отдельно выделенной ПЭВМ, не входящей в локальную сеть;
- 8) ограничение доступа к ПЭВМ посторонних лиц.

Регулярную комплексную проверку наличия вирусов выполняет администратор. Администратор использует для проверки специальные дискеты с антивирусными программами.

При обнаружении вирусов в ПЭВМ, работающей в локальной сети, проверке подлежат все ПЭВМ, включенные в эту сеть.

Создание резервной копии программного продукта выполняет программист, ответственный за внедрение этого программного продукта.

Проверку всех поступающих и купленных программ выполняет управление информатизации.

7.3 Политика безопасности удаленного доступа

Политика безопасности при удаленном доступе к ресурсам предприятия предусматривает следующее:

1. Удалённый доступ осуществляется только к внешним серверам предприятия, расположенным в DMZ.
2. Любое проникновение из сети интернет во внутреннюю часть сети запрещено.
3. Удалённый доступ к внешним серверам сети может осуществляться только по веб протоколам – http, https.

7.4 Инструкция по выбору и использованию паролей

1. Пароль должен содержать от 8 до 16 символов латинского алфавита, должен содержать прописную литеру и число.
2. Пароль должен содержать случайный набор символов.
3. Запрещено хранить пароль в текстовых файлах на рабочем месте.
4. Запрещено разглашать свой пароль.
5. При возникновении проблем с паролем сотрудник обязан обратиться к системному администратору.

8 СЦЕНАРИИ КОНФИГУРАЦИИ ОБОРУДОВАНИЯ

Из общей структуры локальной сети можно сформулировать основные сценарии конфигурации оборудования. Первым делом необходимо настроить конфигурацию каждого этажа. Первый этаж включает в себя маршрутизатор, что конфигурируется следующим образом:

```
Router>en
Router#conf t
Router(config)#int gigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#
Router(config)#int gigabitEthernet 0/1
Router(config-if)#ip address 10.2.1.1 255.255.255.128
Router(config-if)#no shutdown
Router(config-if)#ip helper-address 10.1.1.2
Router(config-if)#exit
Router(config)#int gigabitEthernet 0/2
Router(config-if)#no sh
Router(config-if)#ip address 10.3.1.2 255.255.255.0
```

Настройка коммутатора включает в себя настройку всех его портов, что будут использованы для соединений. Также настраивается адрес для работы dhcp-сервера и основные шлюзы по умолчанию для рабочих станций.

Аналогичным образом настраивается второй этаж. Настройка маршрутизатора уровня второго этажа:

```
Router>en
Router#conf t
Router(config)#int gigabitEthernet 0/0
Router(config-if)#ip address 10.1.2.1 255.255.0.0
Router(config-if)#exit
Router(config)#int gigabitEthernet 0/1
Router(config-if)#ip address 10.2.2.1 255.255.255.128
Router(config-if)#ip helper-address 10.1.2.2
Router(config-if)#exit
Router(config)#int gigabitEthernet 0/2
Router(config-if)#no shutdown
Router(config-if)#ip address 10.3.2.2 255.255.255.0
```

Аналогичным образом настраивается третий этаж. Настройка маршрутизатора уровня третьего этажа:

```
Router>en
```

```

Router#conf t
Router(config)#int gigabitEthernet 0/0
Router(config-if)#ip address 10.1.3.1 255.255.0.0
Router(config-if)#exit
Router(config)#
Router(config)#int gigabitEthernet 0/1
Router(config-if)#ip address 10.2.3.1 255.255.255.128
Router(config-if)#ip helper-address 10.1.3.2
Router(config-if)#exit
Router(config)#int gigabitEthernet 0/2
Router(config-if)#no shutdown
Router(config-if)#ip address 10.3.3.2 255.255.255.0

```

Далее необходимо настроить маршрутизаторы на уровне здания. Они работают на магистральном уровне и предназначены для маршрутизации трафика между этажами, а также для связи с DMZ и с сетью Интернет. Для настройки необходимо два маршрутизатора, так как необходимо как минимум 4 порта для объединения сети, тогда как на имеющемся оборудовании лишь 3 порта. Ниже приводится формат настройки первого маршрутизатора здания. Он отвечает за маршрутизацию трафика между первым и вторым этажами:

```

Router>en
Router#conf t
Router(config)#int gigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 10.3.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#
Router(config)#int gigabitEthernet 0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 10.3.2.1 255.255.255.0
Router(config-if)#exit
Router(config)#int gigabitEthernet 0/2
Router(config-if)#no shutdown
Router(config-if)#ip address 10.3.4.1 255.255.255.0

```

Второй маршрутизатор на магистральном уровне соединен с первым маршрутизатором и третьим этажом, что дает возможность маршрутизации трафика между 3-мя этажами:

```

Router>en
Router#conf t
Router(config)#int gigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 10.3.4.2 255.255.255.0
Router(config-if)#exit
Router(config)#
Router(config)#int gi
Router(config)#int gigabitEthernet 0/1

```

```

Router(config-if)#
Router(config-if)#no sh
Router(config-if)#no shutdown
Router(config-if)#ip address 10.3.3.1 255.255.255.0
Router(config-if)#exit
Router(config)#int gigabitEthernet 0/2
Router(config-if)#no shutdown
Router(config-if)#ip address 10.3.5.2 255.255.255.0

```

Далее необходимо настроить маршрутизацию трафика по сети. Это позволит различным рабочим группам, располагающимся на разных этажах, взаимодействовать между собой. В качестве используемого протокола берется протокол динамической маршрутизации OSPF. Настройка этажей и уровня ядра представлена ниже.

Настройка первого маршрутизатора на уровне здания:

```

Router(config)#route ospf 1
Router(config-router)#network 10.3.1.0 0.0.0.255 area 1
Router(config-router)#network 10.3.2.0 0.0.0.255 area 1
Router(config-router)#network 10.3.4.0 0.0.0.255 area 1

```

Настройка второго маршрутизатора на уровне здания:

```

Router(config)#route ospf 1
Router(config-router)area 1 range 10.0.0.0 255.0.0.0
Router(config-router)#network 10.3.5.0 0.0.0.255 area 0
Router(config-router)#network 10.3.4.0 0.0.0.255 area 1
Router(config-router)#network 10.3.3.0 0.0.0.255 area 1

```

Настройка маршрутизатора уровня первого этажа:

```

Router(config)#route ospf 1
Router(config-router)#network 10.1.0.0 0.0.255.255 area 1
Router(config-router)#network 10.2.1.0 0.0.255.255 area 1
Router(config-router)#network 10.3.1.0 0.0.255.255 area 1

```

Настройка маршрутизатора уровня второго этажа:

```

Router(config)#route ospf 1
Router(config-router)#
Router(config-router)#net
Router(config-router)#network 10.1.0.0 0.0.255.255 area 1
Router(config-router)#network 10.2.2.0 0.0.0.255 area 1
Router(config-router)#network 10.3.2.0 0.0.0.255 area 1

```

Настройка маршрутизатора уровня третьего этажа:

```

Router(config)#route ospf 1
Router(config-router)#
Router(config-router)#net
Router(config-router)#network 10.1.3.0 0.0.0.255 area 1
Router(config-router)#network 10.2.3.0 0.0.0.255 area 1
Router(config-router)#network 10.3.3.0 0.0.0.255 area 1

```


Далее необходимо оформить DMZ. Для ее оформления нужен дополнительный роутер, который будет играть роль межсетевого экрана. Там также поддерживается маршрутизация протоколом OSPF. Первоначальная настройка роутера выглядит следующим образом:

```
Router(config)#int gigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 10.4.6.1 255.255.255.0
Router(config-if)#exit

Router(config)#int gigabitEthernet 0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 200.200.1.2 255.255.255.0
Router(config-if)#exit

Router(config)#int gigabitEthernet 0/2
Router(config-if)#no shutdown
Router(config-if)#ip address 201.200.1.1 255.255.255.0

Router(config)#route ospf 1
Router(config-router)#network 10.3.5.0 0.0.0.255 area 0
Router(config-router)#network 200.200.1.0 0.0.0.255 area 0
```

Дополнительно к DMZ сразу подключается и сеть Интернет. Подключение к Интернету эмулируется посредством сети из роутера и сервера, подключенной по DSL и использующую «белые» IP-адреса. Конфигурация представлена ниже:

```
Router(config)#int gigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)# ip address 200.200.2.1 255.255.255.0
Router(config-if)#exit

Router(config)#int gigabitEthernet 0/1
Router(config-if)#no shutdown
Router(config-if)# ip address 200.200.1.1 255.255.255.0
Router(config-if)#exit

Router(config)#route ospf 1
Router(config-router)# network 200.200.2.0 0.0.0.255 area 0
Router(config-router)#network 200.200.1.0 0.0.0.255 area 0
```

Согласно политике безопасности, DMZ и сеть Интернет могут обмениваться данными, однако ни DMZ, ни внешние сети не могут получить доступ к внутренней сети предприятия. Для улучшения безопасности внешний

роутер, к которому подключен DMZ, может быть использован как межсетевой экран. Для этого пишутся следующие списки доступа:

```
Router(config)#ip access-list extended FROM-LOCAL
Router(config-ext-nacl)#permit icmp 10.2.1.0 0.0.0.127 any
Router(config-ext-nacl)#permit tcp 10.2.1.0 0.0.0.127 any eq www
Router(config-ext-nacl)#permit icmp 10.2.2.0 0.0.0.127 any
Router(config-ext-nacl)#permit tcp 10.2.2.0 0.0.0.127 any eq www
Router(config-ext-nacl)#permit icmp 10.2.3.0 0.0.0.127 any
Router(config-ext-nacl)#permit icmp 10.2.3.0 0.0.0.127 any
Router(config-ext-nacl)#permit ospf any any
Router(config-ext-nacl)#exit
```

```
Router(config)#ip access-list extended FROM-OUT
Router(config-ext-nacl)#permit icmp any 201.200.1.0 0.0.0.255
Router(config-ext-nacl)#permit tcp any 201.200.1.0 0.0.0.255 eq www
Router(config-ext-nacl)#permit ospf any any
Router(config-ext-nacl)#deny ip any any
```

```
Router(config)#int gigabitEthernet 0/0
Router(config-if)#ip access-group FROM-LOCAL in
```

```
Router(config)#int gigabitEthernet 0/1
Router(config-if)#ip access-group FROM-OUT in
```

Списки доступа работают, однако, при их использовании пользователи локальной сети не смогут пользоваться DMZ и Интернетом. Для решения проблемы используется инспектирование трафика на внешнем роутере:

```
Router(config)#ip inspect name In-Out http
Router(config)#ip inspect name In-Out icmp
Router(config)#ip inspect name In-Out tcp
Router(config)#int fastEthernet 0/0
Router(config-if)#ip inspect In-Out in
```

9 КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

Целью моделирования является проверка функционирования спроектированной компьютерной сети предприятия в соответствии с техническим заданием и корректности разработанных сценариев конфигурирования телекоммуникационного оборудования.

Для моделирования спроектированной сети, использовалась программа Cisco Packet Tracer. Топология сети представлена на рисунках 9.1.

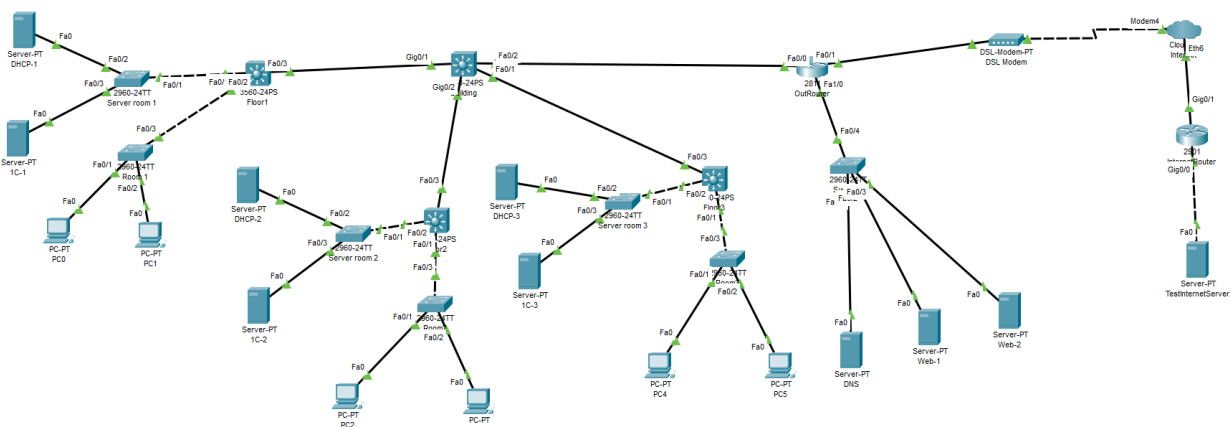


Рисунок 9.1 – Топология сети (внутренняя сеть)

Далее необходимо провести полную отладку модели по всем направлениям. Первым делом необходимо проверить, что работники одной группы могут взаимодействовать между собой. Для этого используется команда ping. Результаты тестирования представлены рисунком 9.2.

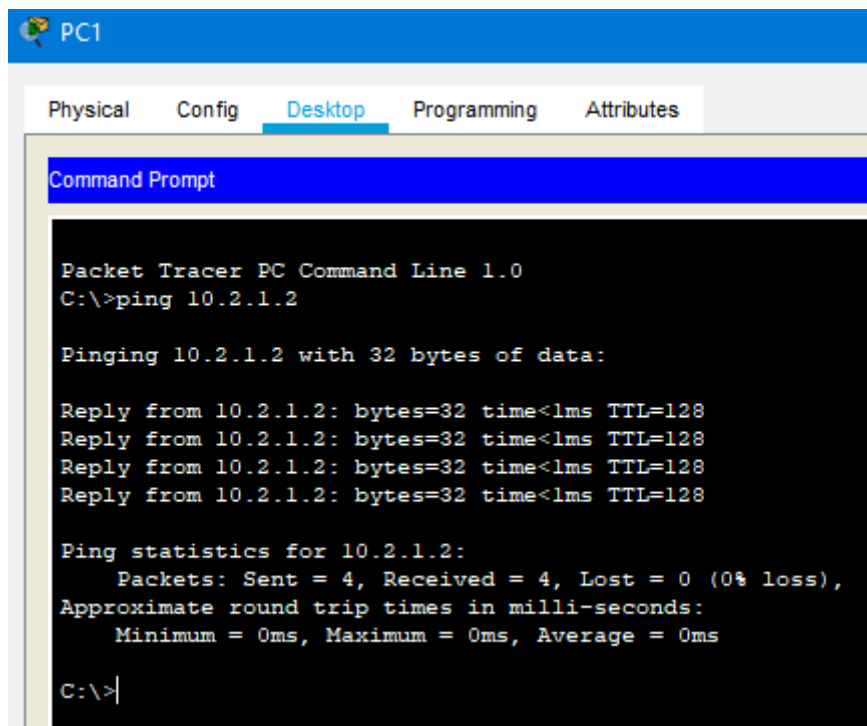


Рисунок 9.2 – Обмен данными между станциями одной группы

Далее проверяется взаимодействие между рабочей станцией и внутренним сервером в пределах одного этажа. В частности, проверяется работа DHCP-сервера. Результаты тестирования представлены рисунком 9.3.

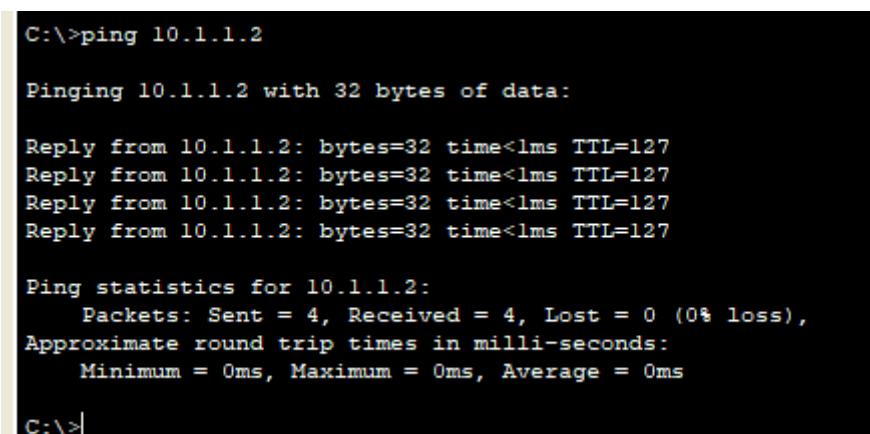
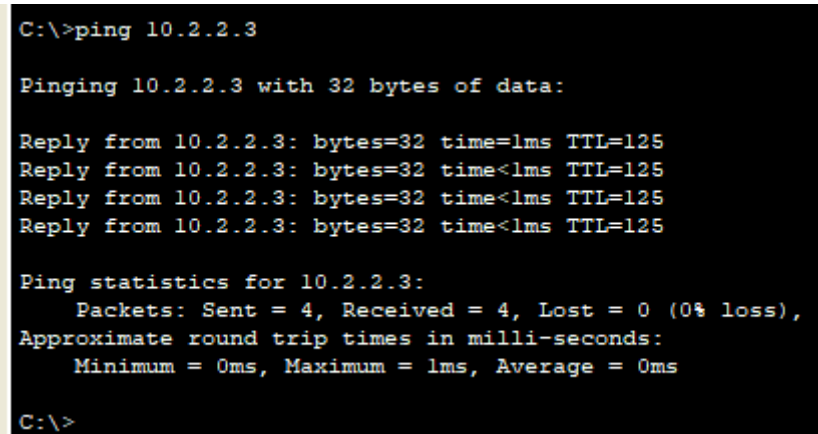


Рисунок 9.3 – Обмен данными между станцией и внутренним сервером

Далее взаимодействие между рабочими станциями, расположенных на разных этажах. В этом тесте проверяется корректность работы маршрутизации и InterVLAN Routing. Результаты тестирования представлены рисунком 9.4.



```
C:\>ping 10.2.2.3

Pinging 10.2.2.3 with 32 bytes of data:

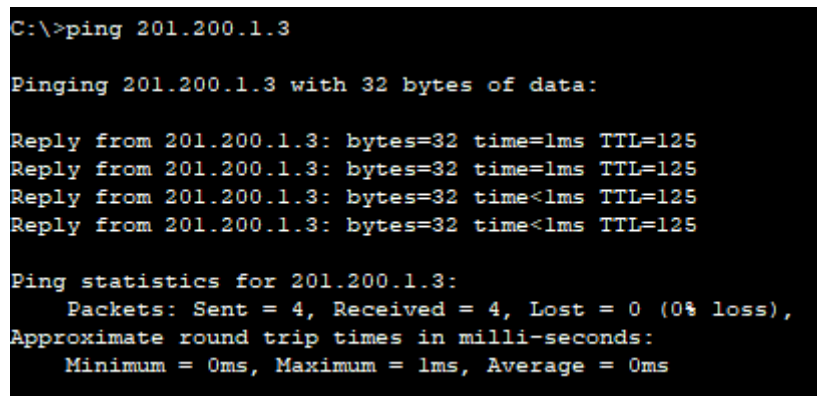
Reply from 10.2.2.3: bytes=32 time=1ms TTL=125
Reply from 10.2.2.3: bytes=32 time<1ms TTL=125
Reply from 10.2.2.3: bytes=32 time<1ms TTL=125
Reply from 10.2.2.3: bytes=32 time<1ms TTL=125

Ping statistics for 10.2.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Рисунок 9.4 – Обмен данными между рабочими станциями на разных этажах

Далее проверяется связь между внутренней сетью и пулом серверов в DMZ. Для этого делается ping от рабочей станции до веб-сервера в DMZ. Также ведется проверка не только по протоколу icmp, но и по протоколу www. Результаты тестирования представлены рисунками 9.5 — 9.6.



```
C:\>ping 201.200.1.3

Pinging 201.200.1.3 with 32 bytes of data:

Reply from 201.200.1.3: bytes=32 time=1ms TTL=125
Reply from 201.200.1.3: bytes=32 time=1ms TTL=125
Reply from 201.200.1.3: bytes=32 time<1ms TTL=125
Reply from 201.200.1.3: bytes=32 time<1ms TTL=125

Ping statistics for 201.200.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Рисунок 9.5 – Обращение рабочей станции к серверу в DMZ



Рисунок 9.6 – Обращение рабочей станции к серверу в DMZ по www

Далее необходимо отметить, может ли DMZ связываться со внутренней сетью. Согласно стандартам безопасности, эту возможность следует исключить. Результаты тестирования представлены рисунком 9.8.

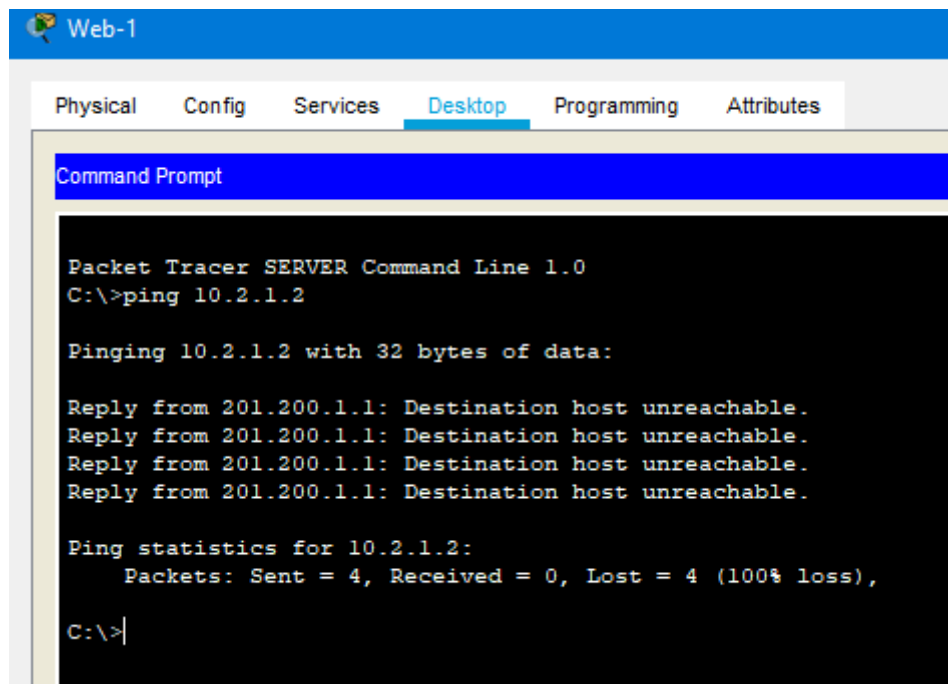


Рисунок 9.7 – Попытка обращения из DMZ во внутреннюю сеть

Далее проверяется выход внутренней сети в Интернет. Проверка делается как по пингу, так и по http-соединению. Результаты тестирования представлены рисунками 9.8 — 9.9.

```

C:\>ping 200.200.2.2

Pinging 200.200.2.2 with 32 bytes of data:

Reply from 200.200.2.2: bytes=32 time=42ms TTL=124
Reply from 200.200.2.2: bytes=32 time=58ms TTL=124
Reply from 200.200.2.2: bytes=32 time=56ms TTL=124
Reply from 200.200.2.2: bytes=32 time=45ms TTL=124

Ping statistics for 200.200.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 42ms, Maximum = 58ms, Average = 50ms

C:\>

```

Рисунок 9.8 – Проверка соединения с Интернетом

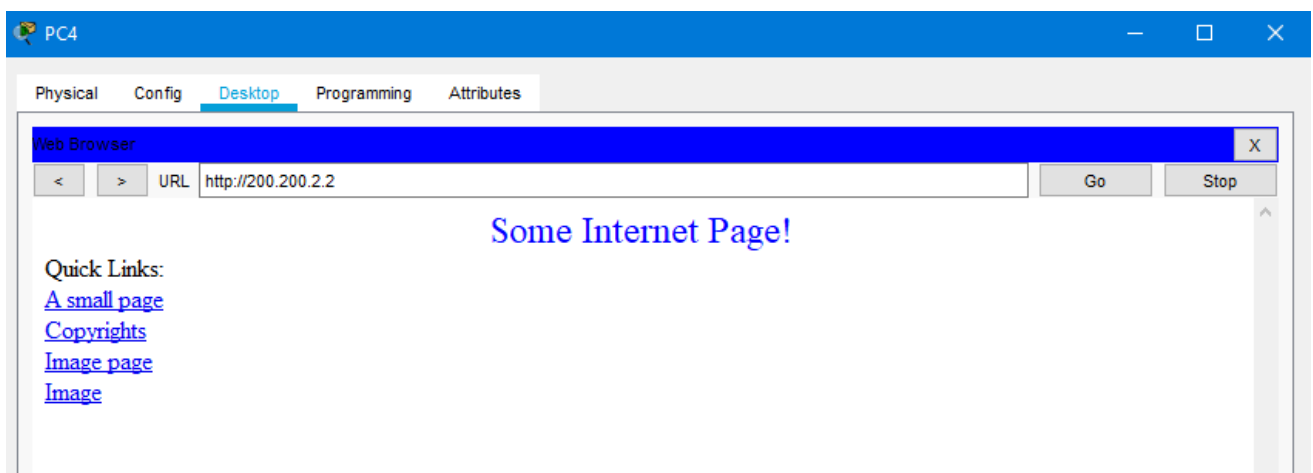


Рисунок 9.9 – Проверка соединения с Интернетом по www

Далее проверяется взаимодействие между DMZ и Интернетом. Результаты тестирования представлены рисунками 9.10-9.11.

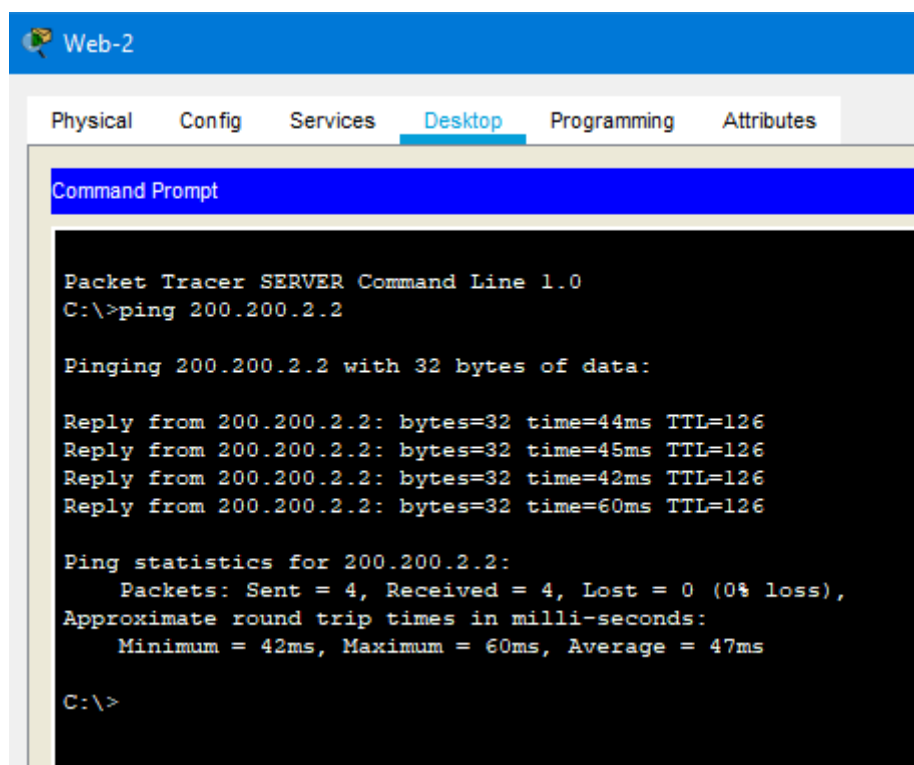


Рисунок 9.10 – Соединение DMZ с Интернетом

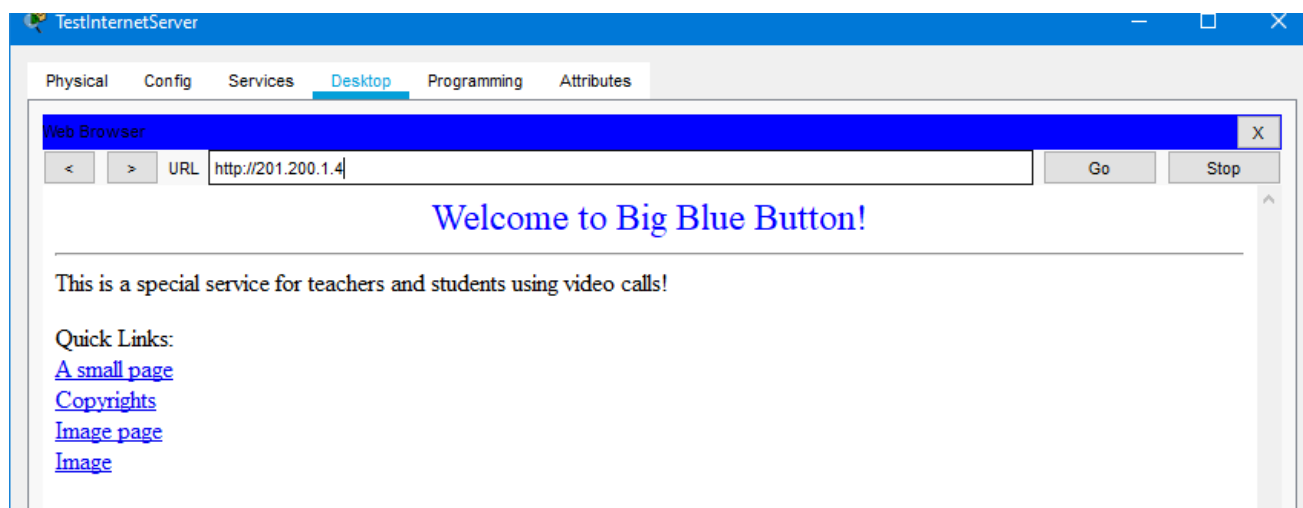


Рисунок 9.11 – Соединение Интернета с DMZ

Далее проверяется работа DHCP-сервером. Эти сервера расположены на каждом этаже и предназначены для раздачи IP-адресов рабочим станциям на этаже. Результаты тестирования представлены рисунками 9.12-9.14.

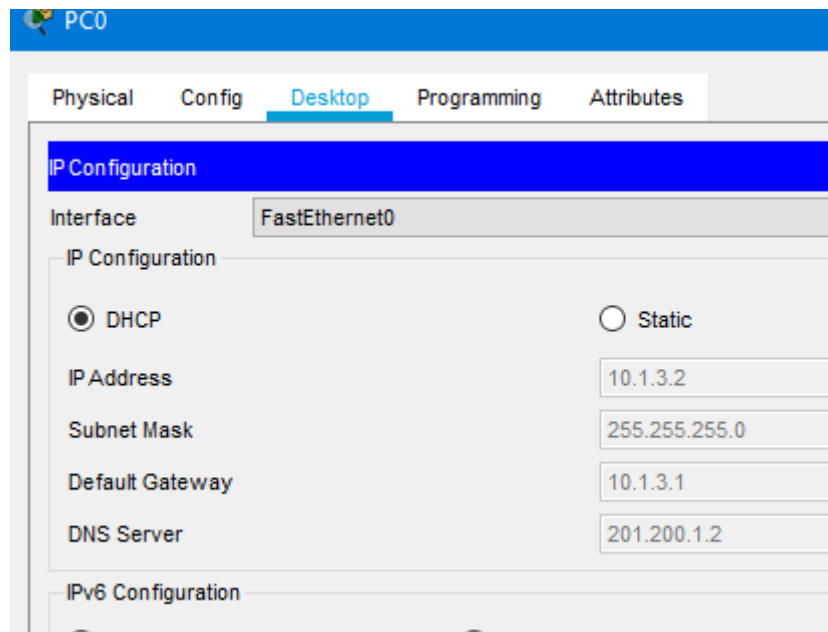


Рисунок 9.12 – DHCP на первом этаже

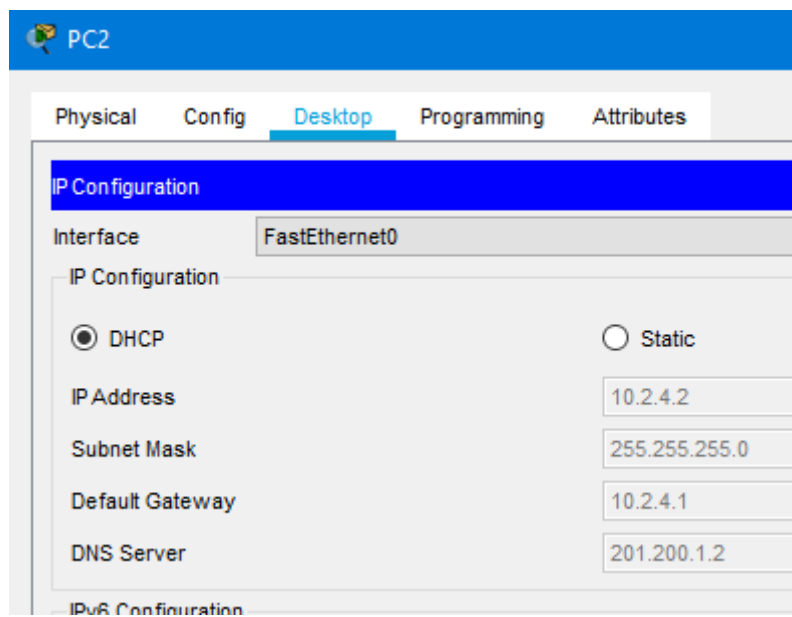


Рисунок 9.13 – DHCP на втором этаже

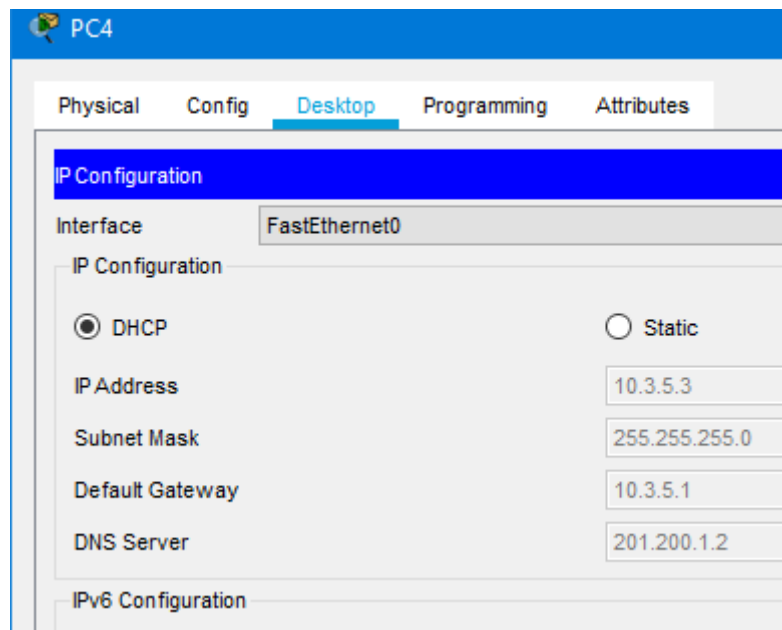


Рисунок 9.14 – DHCP на третьем этаже

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы по дисциплине «Инфокоммуникационные системы и сети» была спроектирована сеть предприятия.

В ходе проектирования решены задачи определения местоположения серверных и кроссовых помещений, определения количества телекоммуникационных розеток, распределения IP-адресов.

Далее была разработана логическая структура сети. Произведён выбор активного и пассивного оборудования сети, а также деление на подсети. Также были построены схемы помещений для предприятия и прописаны политики безопасности. В частности, сеть была разделена на 3 основных сегмента: внутренняя сеть, демилитаризованная зона и внешняя сеть. При этом внутренняя сеть имеет доступ как в зону, так и во внешнюю среду, когда как извне нельзя пробраться во внутреннюю сеть. Внешняя сеть эмулировалась посредством специального сервера с «белым» IP-адресом.

После разработки сети были написаны сценарии настройки активного сетевого оборудования. Была проведена настройка уровней ядра, распределения и доступа. В качестве ядра использовался L3-коммутатор, рассчитанный на маршрутизацию трафика между подсетями. Уровень распределения включал в себя внутренние сервера на каждом этаже и L3-коммутатор. Были прописаны конфигурации коммутаторов, свичей, роутеров. Были приведены в действие протоколы OSPF, VTP, DHCP, DNS.

Для работы с «белыми» IP-адресами был использован DSL-модем.

Для организации соединения с сетью Интернет, а также с DMZ, использовался маршрутизатор, выполняющий роль межсетевого экрана, пропускающие пакеты только от определенных сетей и хостов в определенном

направлении. Таким образом, злоумышленник при попытке взлома сети Интернет или сервера в DMZ не в состоянии получить доступ ко внутренней сети.

На основе написанной конфигурации было произведено моделирование в Cisco Packet Tracer, подтверждающее работоспособность и корректность сети. Написанная сеть проверялась посредством использования команды ping, режимом симуляции программы Cisco Packet Tracer, а также симуляцией работы веб-браузера на устройствах.

Разработанная сеть рассчитана на 312 пользователей и спроектирована с возможностью расширения. Содержит современное телекоммуникационное оборудование, которое позволит эксплуатировать сеть в течение 10-20 лет без существенной модернизации аппаратной части. При проектировании сети использовано оборудование компании Cisco, предусматривающее гарантию.

Таким образом, параметры спроектированной сети полностью соответствуют техническому заданию, результаты моделирования в Cisco Packet Tracer подтверждают её работоспособность.

СПИСОК ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

- 1 Амато В. Основы организации сетей Cisco. Том 1: Пер. с англ./В.Амато.— М.: Изд-во "Вильямс", 2004. — 512 с.
- 2 Амато В. Основы организации сетей Cisco. Том 2. : Пер. с англ. / В.Амато.— М.: Изд-во "Вильямс", 2004. — 464 с.
- 3 Боллапрагада В. Структура операционной системы Cisco IOS: Пер. с англ. / В. Боллапрагада, К.Мэрфи, Р.Уайт: Пер. с англ. — М.: Изд-во "Вильямс", 2002. — 208 с.
- 4 Гук М. Аппаратные средства локальных сетей. Энциклопедия / М.Гук.- СПб.: Изд-во "Питер", 2000. — 576 с.
- 5 Компьютерные сети: Учебное пособие для вузов / В.Чернега, Б. Платтнер - Севастополь: Изд-во СевНТУ, 2006.- 500 с.
- 6 Проектирование локальных компьютерных сетей уровня организаций и предприятий. Методическое пособие по курсовому проектированию / В.С.Чернега. — Севастополь: Изд-во СевНТУ, 2014.— 105 с.

ПРИЛОЖЕНИЕ А

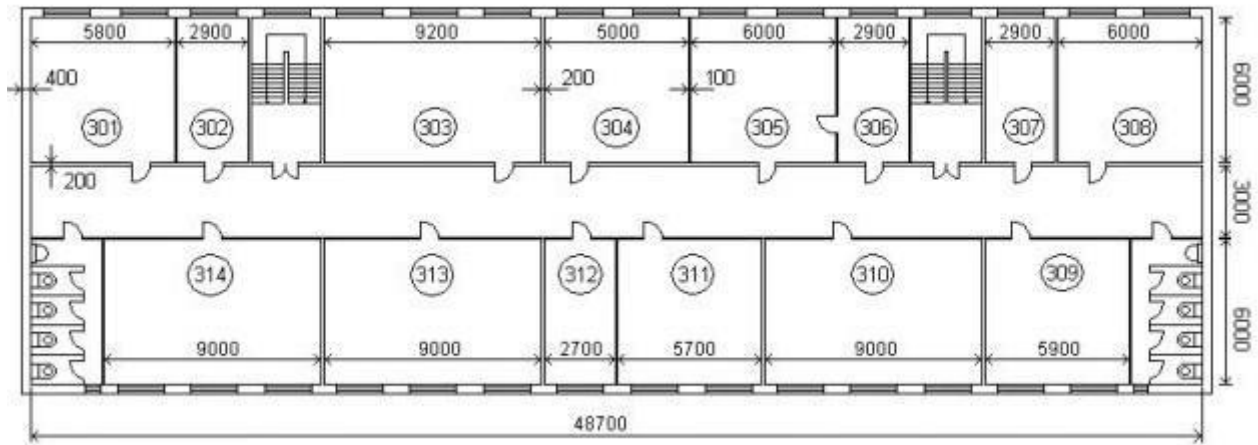


Рисунок А.1 – Схема первого этажа предприятия

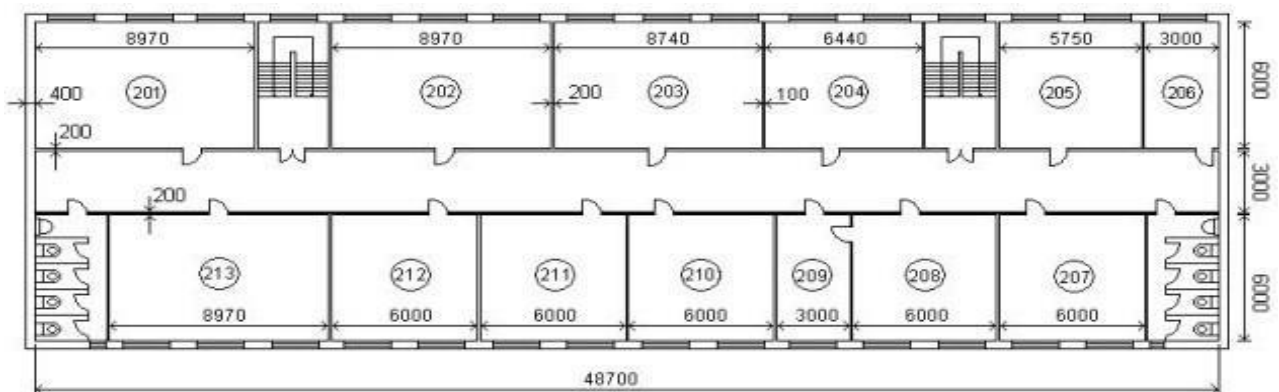


Рисунок А.2 – Схема второго этажа предприятия

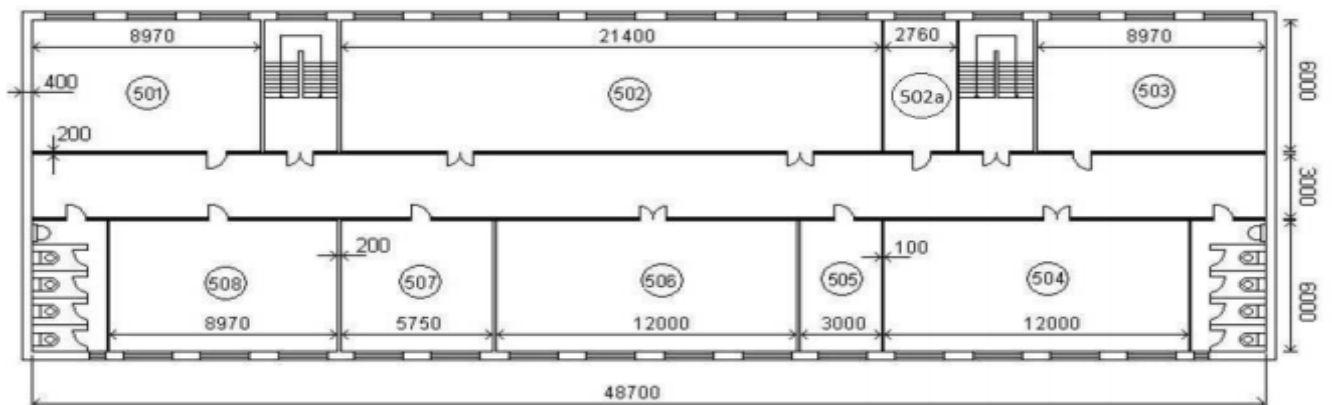


Рисунок А.3 – Схема третьего этажа предприятия