Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерного проектирования

Кафедра проектирования информационно-компьютерных систем

Е. Н. Шнейдеров, А. А. Фещенко, С. М. Боровиков

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве пособия для специальности 1-39 03 02 «Программируемые мобильные системы»

Минск БГУИР 2022

УДК 004.738(076)
ББК 32.971.35я73
Ш76

Р е ц е н з е н т ы:

кафедра моделирования и проектирования учреждения образования «Белорусский государственный аграрный технический университет» (протокол №7 от 11.02.2019);

заведующий кафедрой программного обеспечения сетей телекоммуникаций учреждения образования «Белорусская государственная академия связи» кандидат технических наук, доцент В. А. Рыбак

Шнейдеров, Е. Н.

Ш76 Организация информационно-компьютерных систем и сетей. Курсовое проектирование : пособие / Е. Н. Шнейдеров, А. А. Фещенко, С. М. Боровиков. – Минск : БГУИР, 2022. – 68 с. : ил.

ISBN 978-985-543-552-6.

Содержит описание требований к курсовому проекту, целью которого является приобретение навыков разработки современной компьютерной сети малого и среднего предприятия.

Может быть использовано для подготовки отдельных тем сертификационных экзаменов CCNA Routing and Switching.

УДК 004.738(076)
ББК 32.971.35я73

ISBN 978-985-543-552-6

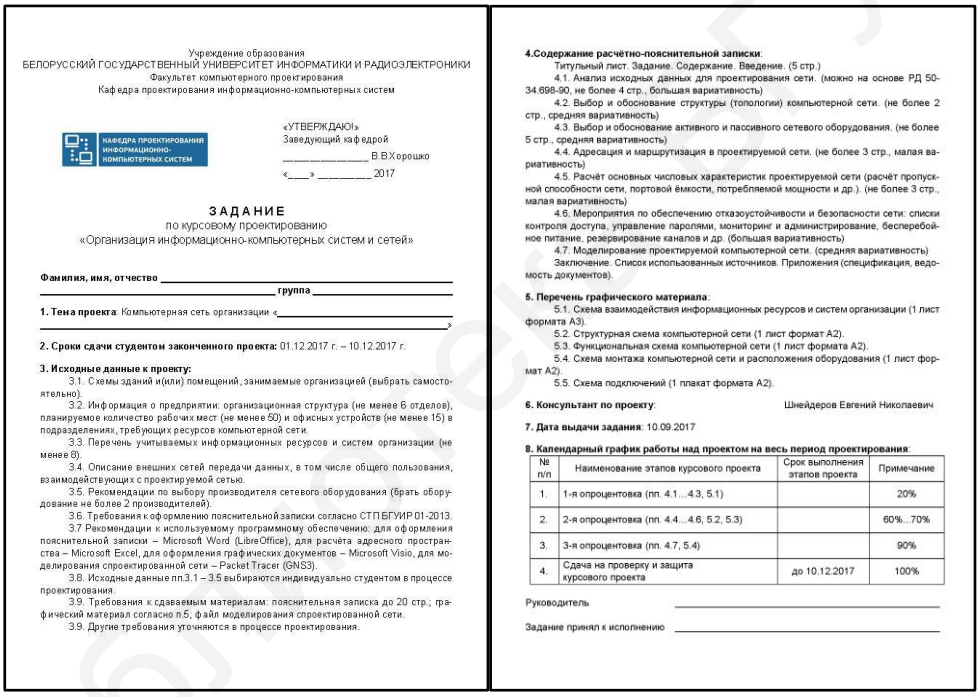
СОДЕРЖАНИЕ

1 ЗАДАНИЕ НА КУРСОВОЙ ПРОЕКТ

1.1 Общая информация

Задание на курсовой проект по дисциплине «Организация информационно-компьютерных систем и сетей» оформляется в соответствии с требованиями СТП БГУИР 01–2017 и включает в себя четыре основных раздела, определяющих содержательную часть работы: тема, исходные данные, содержание расчётно-пояснительной записки и перечень графического материала. Трудоёмкость курсового проекта составляет около 40 часов.

Традиционно тема курсового проекта называется «Компьютерная сеть организации с информационной инфраструктурой», где вместо слова «организация» фигурирует её наименование. Например, «Компьютерная сеть БГУИР с информационной инфраструктурой». Пример бланка задания представлен на рисунке 1.



Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ
Факультет компьютерного проектирования
Кафедра проектирования информационно-компьютерных систем

КАФЕДРА ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ СИСТЕМ

«УТВЕРЖДАЮ»
Заведующий кафедрой
_____ В.В.Хорошко
«____» _____ 2017

ЗАДАНИЕ
по курсовому проектированию
«Организация информационно-компьютерных систем и сетей»

Фамилия, имя, отчество _____
_____ **группа** _____

1. Тема проекта: Компьютерная сеть организации «_____»

2. Сроки сдачи студентом законченного проекта: 01.12.2017 г. – 10.12.2017 г.

3. Исходные данные к проекту:
3.1. Схемы зданий и(или) помещений, занимаемые организацией (выбрать самостоятельно).
3.2. Информация о предприятии: организационная структура (не менее 6 отделов), планируемое количество рабочих мест (не менее 50) и офисных устройств (не менее 15) в подразделениях, требующих ресурсов компьютерной сети.
3.3. Перечень учитываемых информационных ресурсов и систем организации (не менее 8).
3.4. Описание внешних сетей передачи данных, в том числе общего пользования, взаимодействующих с проектируемой сетью.
3.5. Рекомендации по выбору производителя сетевого оборудования (брать оборудование не более 2 производителей).
3.6. Требования к оформлению пояснительной записки согласно СТП БГУИР 01-2013.
3.7 Рекомендации к используемому программному обеспечению: для оформления пояснительной записки – Microsoft Word (LibreOffice), для расчёта адресного пространства – Microsoft Excel, для оформления графических документов – Microsoft Visio, для моделирования спроектированной сети – Packet Tracer (GNS3).
3.8. Исходные данные пп.3.1 – 3.5 выбираются индивидуально студентом в процессе проектирования.
3.9. Требования к сдаваемым материалам: пояснительная записка до 20 стр.; графический материал согласно п.5; файл моделирования спроектированной сети.
3.9. Другие требования уточняются в процессе проектирования.

4.Содержание расчётно-пояснительной записки:
Титульный лист. Задание. Содержание. Введение. (5 стр.)
4.1. Анализ исходных данных для проектирования сети. (можно на основе РД 50-34.698-90, не более 4 стр., большая вариативность)
4.2. Выбор и обоснование структуры (топологии) компьютерной сети. (не более 2 стр., средняя вариативность)
4.3. Выбор и обоснование активного и пассивного сетевого оборудования. (не более 5 стр., средняя вариативность)
4.4. Адресация и маршрутизация в проектируемой сети. (не более 3 стр., малая вариативность)
4.5. Расчёт основных числовых характеристик проектируемой сети (расчёт пропускной способности сети, портовой ёмкости, потребляемой мощности и др.). (не более 3 стр., малая вариативность)
4.6. Мероприятия по обеспечению отказоустойчивости и безопасности сети: списки контроля доступа, управление паролями, мониторинг и администрирование, бесперебойное питание, резервирование каналов и др. (большая вариативность)
4.7. Моделирование проектируемой компьютерной сети. (средняя вариативность)
Заключение. Список использованных источников. Приложения (спецификация, ведомость документов).

5. Перечень графического материала:
5.1. Схема взаимодействия информационных ресурсов и систем организации (1 лист формата А3).
5.2. Структурная схема компьютерной сети (1 лист формат А2).
5.3. Функциональная схема компьютерной сети (1 лист формата А2).
5.4. Схема монтажа компьютерной сети и расположения оборудования (1 лист формат А2).
5.5. Схема подключений (1 плакат формата А2).

6. Консультант по проекту: Шнейдеров Евгений Николаевич

7. Дата выдачи задания: 10.09.2017

8. Календарный график работы над проектом на весь период проектирования:

№ п/п	Наименование этапов курсового проекта	Срок выполнения этапов проекта	Примечание
1.	1-я опроцентовка (пп. 4.1…4.3, 5.1)		20%
2.	2-я опроцентовка (пп. 4.4…4.6, 5.2, 5.3)		60%...70%
3.	3-я опроцентовка (пп. 4.7, 5.4)		90%
4.	Сдача на проверку и защита курсового проекта	до 10.12.2017	100%

Руководитель _____

Задание принял к исполнению _____

Рисунок 1 – Бланк задания на курсовой проект по дисциплине ОИКСиС

1.2 Исходные данные к курсовому проекту

Исходные данные к курсовому проекту определяют следующие аспекты:

1 **Схема зданий и(или) помещений, занимаемых организацией**. Схема может выбираться либо на основании реальных данных об организации, либо случайным образом. На схеме должны быть указаны размеры помещений. Рекомендуется для фокусировки работы при выборе схемы делать акцент на одну из следующих особенностей проекта:

– кабельную систему магистральной зоны (несколько одно- или двухкомнатных отдельно стоящих зданий – филиалов организации);

– кабельную систему здания (один или два схожих этажа здания, имеющих множество помещений);

– беспроводную сеть (один или два схожих этажа здания, имеющих большое общее неразделённое пространство: холлы, переговорные кабинеты и т. п.).

Ограничения на схему зданий и(или) помещений:

– общая площадь помещений составляет не менее 350 м^2;

– общее количество помещений, задействованных в компьютерной сети, не менее 10 шт.

2 **Информация об организации**, включающая организационную структуру (не менее семи отделов), планируемое количество рабочих мест (рекомендуется не менее 50) и офисных устройств (рекомендуется не менее 15), требующих подключения к компьютерной сети.

3 **Перечень проектируемых информационных ресурсов и систем организации** (рекомендуется не менее восьми). Часто в качестве основных информационных ресурсов выбирают сервер данных, веб-сервер, почтовый сервер и подключение к глобальной сети. В качестве дополнительных ресурсов – серверы лицензий, файловые хранилища данных (в том числе систем контроля версий), серверы резервного копирования, видеосерверы, серверы для ПО бухгалтерии и отдела кадров, фермы виртуальных машин и многие другие.

4 **Описание внешних сетей передачи данных**. Как правило, этот пункт представлен стандартом сети (для определения интерфейса подключения и допустимой пропускной способности) и выделенным сетевым адресом (для настройки в ПО в целях моделирования сетей).

5 **Рекомендации по выбору производителя сетевого оборудования**. Для адаптации курсового проекта к рынку страны выбор осуществляется из следующих вендоров сетевого оборудования: *D-Link, Huawei, Cisco, MikroTik, Juniper* и др., реже – *TP-Link, ZTE, Zyxel* и др. Этот пункт может использоваться преподавателем как дополнительный для усложнения курсового проекта.

6 **Рекомендации к используемому программному обеспечению**. Для оформления пояснительной записки используется *Microsoft Word* (альтернативы – *LibreOffice Writer, Google Documents*), для инженерных расчётов – *Microsoft Excel* (альтернативы – *LibreOffice Calc, Google Sheets*), для оформления графических документов – *Microsoft Visio* (альтернативы – *Dia* и множество веб-сервисов для создания схем и диаграмм), для моделирования сети – *Cisco Packet Tracer* (альтернативы – *GNS3* и множество других приложений для моделирования сети). Стоит отметить, что наибольшую сложность для моделирования сети представляет поиск ПО, которое в основном поставляется только на платной основе. Однако в рамках курсового проекта на моделирование сети отводится не более 10 часов, что позволяет использовать почти любую программу в течение пробного бесплатного периода.

7 **Требования к предоставляемым материалам по итогам курсового проектирования**. Обычно это графический материал, пояснительная записка

объёмом до 25 страниц (оформленная согласно СТП БГУИР 01–2017) и файл моделирования спроектированной сети.

Процесс формирования индивидуального задания определяется руководителем (консультантом) проекта. Используется следующий алгоритм. На первом практическом занятии по дисциплине студентам выдаётся задача по поиску плана здания и(или) помещений (удовлетворяющего условиям пункта 1) и самостоятельной разработки организационной структуры предприятия (по пункту 2), а также информационной инфраструктуры (по пункту 3). Студент распечатывает разработанную структуру и согласовывает с преподавателем. **Этот лист прилагается к заданию по курсовому проектированию в качестве обязательного приложения.** Такой алгоритм в некотором роде мотивирует студента, так как он сам принимает участие в формировании задания.

Приложение
(обязательное)
к заданию на курсовой проект по дисциплине
Организация информационно-компьютерных систем и сетей
студента гр.XXXXXX Иванова И.И.

Организационная структура
– ген. директор, секретарь – 2 РМ + 4 устройства;
– исполн. директор, секретарь – 2 РМ + 4 устройства;
– гл. бухгалтер, бухгалтерия – 4 РМ + 2 устройства;
– нач. отдела кадров, отдел кадров – 3 РМ + 2 устройства;
– юридический отдел – 2 РМ + 1 устройство;
– отдел снабжения – 4 РМ + 1 устройство;
– отдел продаж и работы с клиентами – 5 РМ + 3 устройства;
– отдел АСУ – 3 РМ + 3 устройства;
– отдел маркетинга – 3 РМ + 2 устройства;
– отдел разработки – 15 РМ + 3 устройства.

Итого – 68 подключений

Рисунок 2 – Приложение к заданию на дипломный проект

1.3 Содержание расчётно-пояснительной записки

Основные разделы расчётно-пояснительной записки (содержательная часть разделов носит рекомендательный характер и может быть определена преподавателем индивидуально для студента):

1 **Титульный лист. Реферат. Задание на курсовой проект (включая приложение к заданию). Содержание. Введение**.

Рекомендуемый общий объём текущих разделов – 6-7 страниц. Малая вариативность информации. Введение чаще всего включает в себя описание

задач, которые решаются в курсовом проекте, и отвечает на вопрос, что может найти читатель в данном проекте.

2 **Анализ исходных данных к курсовому проекту**.

Рекомендуемый объём раздела – 3-4 страницы. Большая вариативность информации. В данном разделе студент выполняет следующие виды работ:

– определение рабочих мест структурных подразделений организации в помещениях объекта с учётом норм на минимальную площадь рабочего места;

– определение и обоснование мест размещения коммуникационных шкафов;

– определение и обоснование назначения, размещения и способа реализации информационных ресурсов организации;

– расчёт необходимой портовой ёмкости компьютерной сети.

Рекомендуемая форма представления ключевой информации в разделе:

– изображение плана объекта с указанием рабочих мест (и их номеров), а также мест размещения шкафов, серверов, офисного оборудования и др.;

– таблица информационных ресурсов, содержащая столбцы: «Наименование ресурса», «Назначение», «Способ реализации», «Используемое ПО».

3 **Выбор и обоснование структуры компьютерной сети**.

Рекомендуемый объём раздела – 2 страницы. Большая вариативность информации. В данном разделе студент выполняет по следующие виды работ:

– проектирование топологии и выбор используемых стандартов компьютерной сети с учётом структурных подразделений организации;

– обоснование сегментации с использованием виртуальных сетей организации.

Рекомендуемая форма представления ключевой информации в разделе:

– изображение топологии объекта с указанием структурных подразделений, конечных сетей и активного сетевого оборудования;

– таблица виртуальных сетей с указанием относящихся к ним рабочих мест и структурных подразделений.

4 **Выбор и обоснование активного и пассивного сетевого оборудования**.

Рекомендуемый объём раздела – не более 5 страниц. Средняя вариативность информации. Рекомендуемая форма представления ключевой информации в разделе:

– таблица активного сетевого оборудования с указанием обозначения оборудования (согласно структурной схеме), количества, моделей оборудования, основных характеристик (по которым была выбрана именно эта модель), дополнительных характеристик и его изображения;

– таблица пассивного сетевого оборудования с указанием компонентов, их назначения, количества и характеристик.

5 **Адресация и маршрутизация в проектируемой сети**.

Рекомендуемый объём раздела – 3 страницы. Средняя вариативность информации. Рекомендуемая форма представления ключевой информации в

разделе: таблица адресации с указанием названий виртуальных сетей, их адресных пулов, шлюзов, широковещательных, групповых, зарезервированных, выданных и свободных адресов и т. п. Основные маршруты, используемые в сети, также рекомендуется представлять в табличном виде. Данный раздел отвечает на вопрос, как выполняется адресация и маршрутизация в любом сегменте сети.

6 **Расчёт характеристик проектируемой сети**.

Рекомендуемый объём раздела – 2 страницы. Малая вариативность информации. Рекомендуемые расчёты, которые могут быть выполнены в курсовом проекте:

– оценка пропускной способности сети (маршрута);

– оценка портовой ёмкости сети (сегмента);

– расчёт потребляемой мощности активным оборудованием;

– расчёт времени двойного оборота сигнала и др.

Автором обычно определён расчёт пропускной способности самого длинного маршрута сети и расчёт мощности, потребляемой системой. Пример расчётов приведён в соответствующих разделах пособия.

7 **Обеспечение отказоустойчивости и безопасности сети**.

Рекомендуемый объём раздела – 3 страницы. Большая вариативность информации. В данном разделе студентом описываются мероприятия, которые необходимо реализовать для обеспечения отказоустойчивости и безопасности. Эти мероприятия могут включать в себя описание списков контроля доступа, настройки брандмауэров, политики управления паролями, подходы к мониторингу и администрированию сети (включая соответствующие протоколы), организацию системы бесперебойного питания, описание резервирования каналов и др. Данный раздел является наиболее творческим в курсовом проекте.

8 **Моделирование компьютерной сети**.

Рекомендуемый объём раздела – 2 страницы. Малая вариативность информации. В данном разделе должно содержаться:

– краткое описание программного средства для моделирования спроектированной сети;

– изображение окна программного средства с разработанной топологией (включая графические и текстовые пометки студента, поясняющие эту топологию);

– перечень технологий и протоколов, которые были реализованы при моделировании сети и которые были упразднены;

– численные результаты моделирования (временные характеристики отдельных сегментов, значения пропускной способности, графики нагрузки сетевых каналов и др.).

Данный раздел является в большей степени, чем другие, практико-направленным.

9 **Заключение. Список используемых источников**.

Рекомендуемый объём раздела – 2-3 страницы. Средняя вариативность информации. Заключение чаще всего включает в себя описание выполненных в

курсовом проекте задач, а также отвечает на вопрос, какой этап проекта был самым сложным для понимания, трудоёмким и т. п.

10 **Приложения. Ведомость документов**.

Приложения к пояснительной записке не ограничены объёмом. В них могут быть вынесены вспомогательные таблицы, расчёты и изображения, которые по объёму не включены в основную часть записки. Рекомендуется привести в приложениях листинги *runtime*-настроек активного сетевого оборудования с комментариями.

1.4 Перечень графического материала

Перечень графического материала включает в себя следующие позиции:

1 **Структурная схема компьютерной сети** (1 лист формата А2). Назначение этой схемы – дать общее представление о топологии спроектированной сети с учётом формирования адресного пространства, используемого активного оборудования, а также о стандартах сетей.

2 **Схема монтажа компьютерной сети и размещения оборудования** (1 или 2 листа формата А2). Назначение этой схемы – дать представление о территориальном размещении компонентов сети на объекте, проверить оптимальность проектирования СКС, оценить длину кабельных трасс и количество другого пассивного оборудования, радиусы действия беспроводных точек доступа и др.

3 **Схема коммуникационных шкафов** (1 лист формата А2). Назначение этой схемы – дать визуальное представление о размещении активного оборудования в коммуникационных шкафах, точках ввода в шкафы, маркировке и др.

4 **Схема информационных ресурсов** (1 лист формата А3). Назначение этой схемы – изобразить информационное взаимодействие между структурными подразделениями и информационными ресурсами организации, методы контроля доступа и информационной безопасности ресурсов, базовые настройки программного обеспечения.

Более подробно правила оформления графического материала представлены в соответствующих разделах пособия.

2 РЕКОМЕНДОВАННЫЙ ПОРЯДОК ВЫПОЛНЕНИЯ КУРСОВОГО ПРОЕКТА И ЕГО ЗАЩИТА

Данный практико-ориентированный курсовой проект предполагает стандартный порядок выполнения: сначала описание практической части в виде пояснительной записки, затем выполняется моделирование сети с помощью специализированного программного обеспечения.

Для последовательного выполнения работы предлагается следующий алгоритм, представленный на рисунке 3.

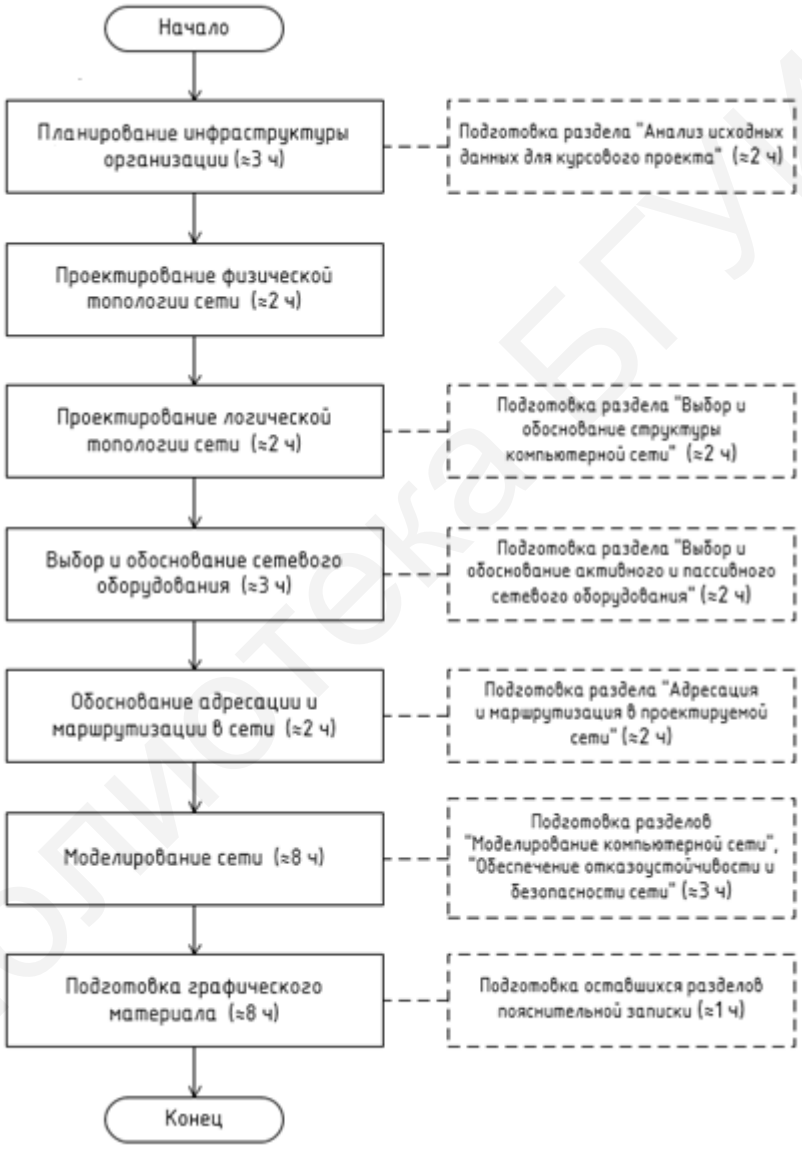


Рисунок 3 – Алгоритм выполнения курсовой работы

Примерное время, затрачиваемое на выполнение этапов курсового проекта, указано в скобках. Этапы, на которых можно уменьшить затрачиваемое время, – проектирование физической и логической топологий, а также обоснование адресации и маршрутизации. Этапы, выполнение которых может

превысить указанное в скобках время, – моделирование сети и подготовка графического материала. Время выполнения этих этапов указано с учётом того, что студент разбирается в программном обеспечении, с помощью которого он их выполняет.

Защита курсового проекта предполагает представление комиссии пояснительной записки, графического материала и работоспособной модели сети как практико-ориентированного результата выполнения. Стоит отметить, что модель сети должна полностью реализовывать логическую топологию, адресацию (в том числе и динамическую) и маршрутизацию, частично реализовывать информационную инфраструктуру и методы защиты в спроектированной сети.

3 ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА ОРГАНИЗАЦИИ

3.1 Организация корпоративных сервисов

Клиент-серверная система – программная или аппаратно-программная система, в которой несколько программных средств имеют различные роли (чаще всего роль поставщика информационных услуг – сервера – и роль потребителя услуг – клиента) и взаимодействуют друг с другом посредством компьютерной сети.

Веб-система (веб-сервис) – клиент-серверная система, в которой в качестве клиента выступает веб-браузер.

Чаще всего в качестве корпоративных выступают следующие сервисы:

1 **Веб-сайт и другие веб-системы управления бизнес-процессами** (*CRM*, системы управления проектами, документооборотом и проч.). Организация простого локально размещаемого веб-сайта может быть реализована с использованием одного сервера (рисунок 4).

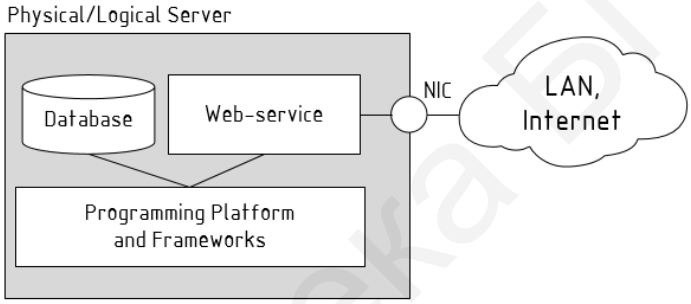


Рисунок 4 – Реализация веб-системы с использованием одного сервера

При такой реализации веб-сайта нет разделения между данными (базой данных) и их представлением клиенту (логическим веб-сервером). В связи с этим по соображениям отказоустойчивости базу данных часто переносят на другой сервер (рисунок 5). Такое разделение позволяет хранить все данные на одном сервере, а доступ к ним осуществлять с нескольких веб-сервисов:

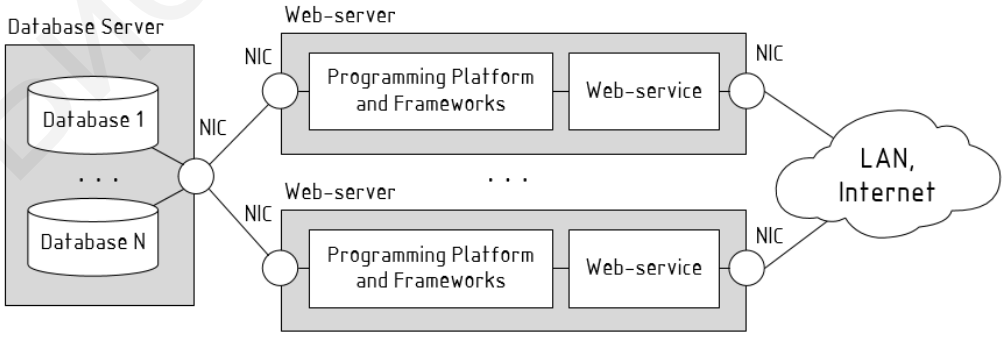


Рисунок 5 – Реализация нескольких веб-систем с отделением слоя данных

При больших нагрузках на сервер он масштабируется и используется совместно с балансировщиком нагрузки. Размещение баз данных на одном сервере тоже снижает отказоустойчивость системы, поэтому часто используются различные виды репликаций данных. Пример приведён на рисунке 6.

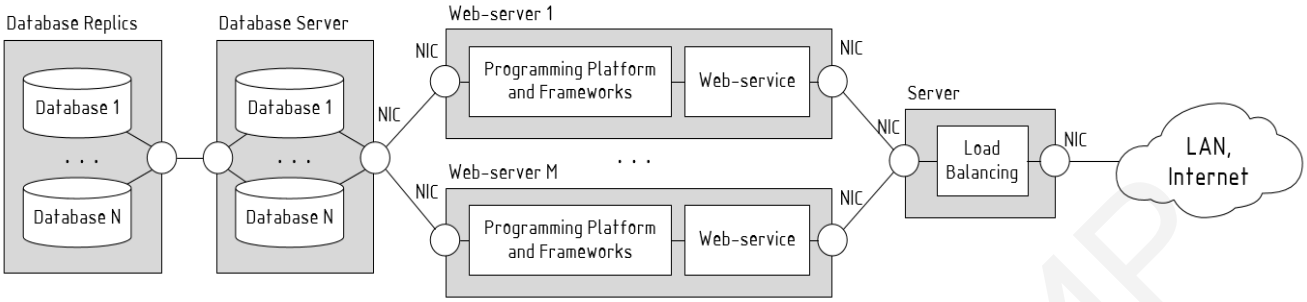


Рисунок 6 – Реализация высоконагруженных веб-систем с резервированием слоя данных

Все перечисленные способы организации веб-систем описаны поверхностно, так как цель их описания – демонстрация. Для реализации даже одного корпоративного веб-сервиса может быть задействовано от одного до десятков физических или виртуальных серверов, по схожему принципу могут быть реализованы и клиент-серверные системы (1С, системы видео-конференц-связи и др.). Описание рекомендуемой архитектуры конкретных веб-систем должно рассматриваться студентом индивидуально в соответствии с рекомендациями разработчиков.

2 **Служба каталогов** (*Directory Service*) – программная система, позволяющая централизованно хранить данные об информационных объектах организации, а также реализовывать групповые политики в их отношении. Под информационными объектами организации понимают учётные записи пользователей, хосты, серверы, общие ресурсы и др. Пример использования службы каталогов – централизованная авторизация пользователей.

Служба каталогов – частный случай клиент-серверной системы. Для её реализации необходим выделенный сервер, называемый контроллером, который хранит всю информацию. В сетях, управляемых службами каталогов *Active Directory*, его называют контроллером домена (*Domain Controller*). Для обеспечения отказоустойчивости всей информационной инфраструктуры в сети обязательно должен быть предусмотрен резервный контроллер.

3 **Сервис доставки программного окружения** (терминальный сервер, *RDP* (*Remote Desktop Protocol)*-сервер). Терминальная система – частный случай клиент-серверной системы, в которой «тонкие» клиенты получают программное обеспечение от терминального сервера. Для её реализации необходим выделенный сервер с обеспечением отказоустойчивости (резервирования).

4 **Сервис разрешения доменных имён** (*DNS*-сервер (*Domain Name System*)). Локальный *DNS*-сервер в основном используется для поддержки службы каталогов и разрешает имена внутри домена, чего не могут сделать

серверы провайдера, не обладая информацией о локальной информационной инфраструктуре. В других случаях локальный *DNS*-сервер может ещё выполнять и другие функции, как, например, кэширование. Для обеспечения отказоустойчивости службы в сети всегда должна поддерживаться резервная копия *DNS*-сервера.

5 **Сервис обмена файлов** (файл-сервер). Наиболее простым способом реализации сервиса обмена файлов является *FTP*-сервер (*File Transfer Protocol*) или *TFTP*-сервер с авторизированным доступом к файлам и каталогам. Для обеспечения отказоустойчивости файл-сервера всегда должна поддерживаться его резервная копия.

6 **Сервис электронной почты** (почтовый сервер). Почтовый сервер – программная система, используемая в целях передачи электронных сообщений между пользователями. Для хранения информации о сообщениях почтовый сервер использует базу данных, поэтому его архитектура во многом будет напоминать архитектуру веб-сайта.

7 **Служба многопользовательской печати** (принт-сервер). Принт-сервер обычно используется в небольших организациях, где отсутствуют службы каталогов. Принт-сервер – это программное средство физического или виртуального сервера, позволяющее централизованно для множества пользователей управлять очередями печати на принтерах. Обычно его не резервируют, однако в организациях, где печать является основным видом деятельности, рекомендуется использование резервного принт-сервера.

Большинство современных компаний при планировании инфраструктуры выбирает аутсорсинг поддержки корпоративных сервисов, размещая их на сторонних хостингах. Тем самым достигается экономическая выгода, связанная с уменьшением площадей для размещения серверного оборудования, сокращение энергозатрат и расходов на обслуживание. Соответственно имеет место уменьшение численности штата вспомогательного технического персонала. При аутсорсе информационных услуг работа, связанная с развитием сервисов, также передаётся подрядчикам. При такой организации различают различные модели использования услуг:

– *Software-as-a-Service (SaaS)* – модель, в которой поставщик услуг предоставляет к использованию масштабируемые и обслуживаемые им программные средства (доступ к ним осуществляется обычно посредством веб-браузера);

– *Platform-as-a-Service (PaaS)* – модель, в которой поставщик услуг предоставляет к использованию программные платформы и связанные с ними вычислительные ресурсы (обычно это операционные системы, СУБД, средства разработки и тестирования с возможностью доступа к ним на уровне администратора);

– *Infrastructure-as-a-Service (IaaS)* – модель, в которой поставщик услуг предоставляет к использованию вычислительные ресурсы (чаще всего это виртуальные машины с конкретной вычислительной мощностью) и не контролирует программное обеспечение потребителя;

– *Desktop-as-a-Service (DaaS)* – модель, в которой поставщик услуг предоставляет к использованию программное окружение рабочего места сотрудника организации, включая всю инфраструктуру (фактически сотрудники организации используют компьютеры как терминалы для подключения к удалённой информационной инфраструктуре организации).

При аутсорсе информационных сервисов важнейшую роль в процессе планирования компьютерной сети играют вопросы организации надёжного и скоростного канала связи между предприятием и поставщиком услуг, вопросы безопасности, а также организации удалённого доступа к ресурсам.

3.2 *IP*-телефония

IP-телефония (*VoIP* (*Voice over IP*)) – совокупность технологий, предназначенных для организации телефонных переговоров и другого интерактивного обмена мультимедийным трафиком по *IP*-сетям. *IP*-телефония включает в себя следующие компоненты:

– пользовательское оборудование (*VoIP*-телефоны, смартфоны и т. д.) и(или) программное обеспечение (для звонков с ПК);

– серверное оборудование и программное обеспечение, управляющее звонками и выполняющее интеграцию с *PSTN* (*Public Switched Telephone Network*), *GSM* (*Groupe Special Mobile*) и др.;

– протоколы (сигнальные – *H*.323, *SIP* (*Session Initiation Protocol*) и др., передачи данных – *RTP* (*Real-time Transport Protocol*), *SRTP* (*Secure Real-time Transport Protocol*) и др.);

– транспортные сети и поддержка ими *QoS*.

С точки зрения выполнения курсового проекта важно понимать, что реализация IP-телефонии не предполагает монтажа новой компьютерной сети, а может быть выполнена на базе уже существующей. Для этого необходимо изначально располагать топологией и сетевым оборудованием, позволяющим адаптировать существующую сеть для подключения необходимого оборудования. Упрощённая топология локально размещённой сети с поддержкой *IP*-телефонии приведена на рисунке 7.

Особенности:

– для подключения *VoIP*-телефонов коммутатор должен поддерживать технологию *PoE* (*Power over Ethernet*) для их питания;

– для интеграции обычных телефонов в *VoIP*-домен необходимо использовать *VoIP*-адаптер;

– для обеспечения достаточного качества передачи телефонного трафика сетевое оборудование в *VoIP*-домене должно поддерживать технологию *QoS*;

– для управления потоками данных в *VoIP*-домене должен быть настроен VoIP-сервер;

– для автоматической настройки оборудования в *VoIP*-домене должен быть настроен *DHCP*-сервер;

– для синхронизации времени в телефонной сети в *VoIP*-домене должен быть настроен *NTP*-сервер;

– для интеграции с *GSM*-сетями необходимо подключение *GSM-VoIP* шлюза.

В том случае, если коммутатор уровня доступа не поддерживает технологию *PoE*, необходимую для питания *VoIP*-телефонов, питание обеспечивается за счёт инжекторов *PoE*.

Сейчас существует ряд поставщиков услуг IP-телефонии, которые предоставляют удалённо администрируемые серверы. В таком случае упрощённая топология будет иметь вид, представленный на рисунке 8.

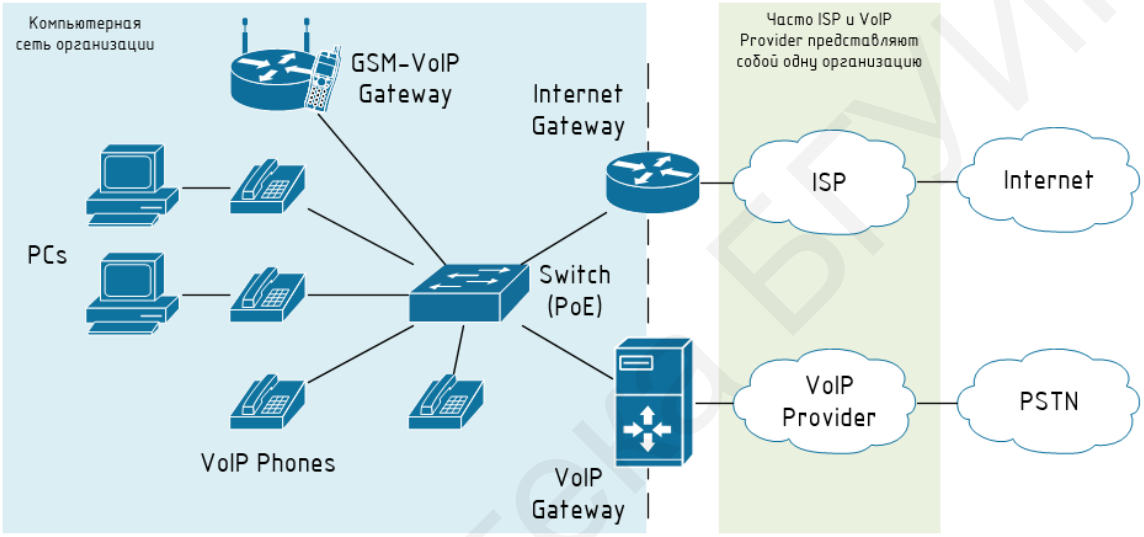


Рисунок 7 – Упрощённая топология локально размещённой *VoIP*-сети

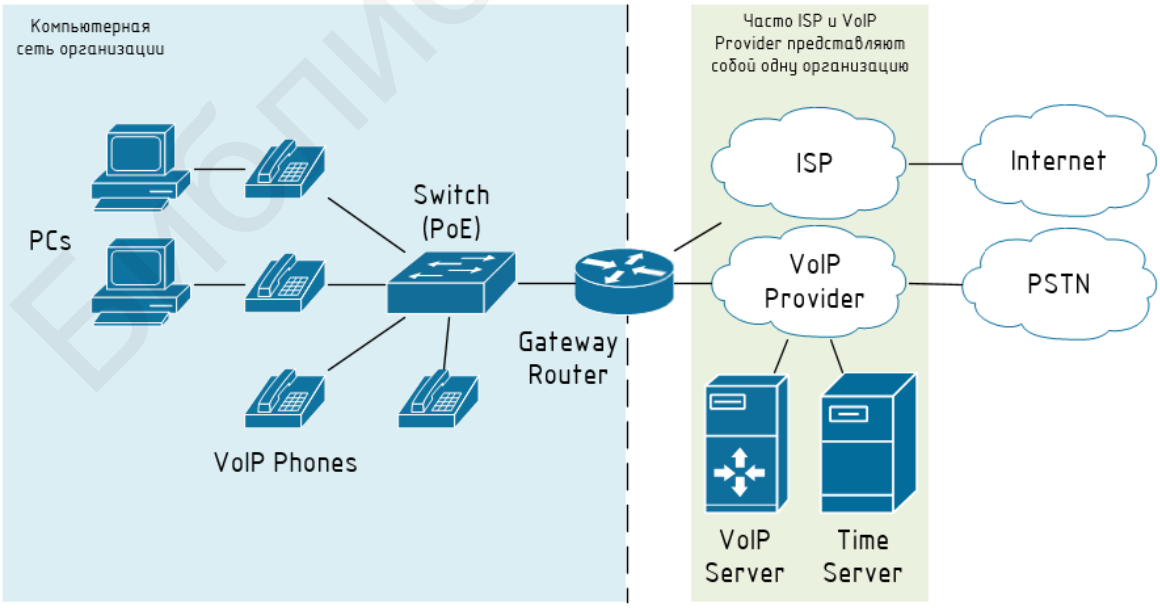


Рисунок 8 – Упрощённая топология *VoIP*-сети при услугах провайдера

При оценке объёма трафика, генерируемого за счёт работы *IP*-телефонии, следует учитывать, что видео- и аудиозвонки отличаются по объёму сообщений. Кроме этого, на пропускную способность оказывает влияние используемый протокол передачи данных, кодек для сжатия данных, тип подключения (точка – точка или многоточечный тип), программное и аппаратное средства для захвата информации и др. В среднем голосовой звонок занимает полосу пропускания до 100 кбит/с, а полоса пропускания видеозвонка зависит от разрешающей способности *IP*-камеры.

3.3 *IP*-видеонаблюдение

IP-видеонаблюдение – совокупность технологий, предназначенных для передачи данных системы охранного видеонаблюдения по *IP*-сетям. *IP*-телефония включает в себя следующие компоненты:

– сетевое оборудование для захвата видеоизображения (*IP*-видеокамеры);

– сетевой видеорекордер для сжатия данных (*NVR* (*Network Video Recorder*) или сервер видеонаблюдения);

– хранилище данных (в большинстве случаев интегрировано с *NVR*);

– программное обеспечение для управления системой *IP*-видеонаблюдения;

– транспортные сети и поддержка ими *QoS* (*Quality of Service*) (рисунок 9).

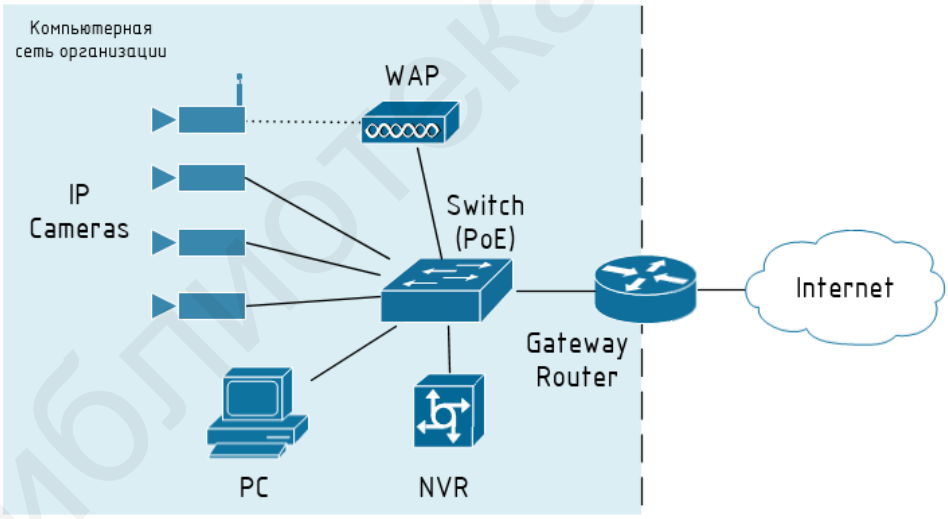


Рисунок 9 – Упрощённая топология системы *IP*-видеонаблюдения

Наиболее важным моментом для проектирования систем *IP*-видеонаблюдения с точки зрения компьютерной сети является планирование используемых стандартов каналов связи, которые определяют их пропускную способность. Планирование пропускной способности зависит от настроек видеокамер (разрешающей способности, кодеков, частоты кадров и др.). В том случае, если *IP*-видеонаблюдение проектируется на основе общей компьютерной сети передачи данных, необходимо предварительно оценить наиболее «узкие»

места с точки зрения пропускной способности и оптимизировать сеть, добавляя резервные каналы и агрегируя их.

Особенности:

– для подключения *IP*-видеокамер коммутатор должен поддерживать технологию *PoE* для их питания;

– для обеспечения достаточного качества передачи видеотрафика в режиме реального времени сетевое оборудование в домене должно поддерживать технологию *QoS*.

4 ПРОЕКТИРОВАНИЕ КОМПЬЮТЕРНОЙ СЕТИ ОРГАНИЗАЦИИ

4.1 Общие требования к компьютерной сети организации

Независимо от размера и требований к компьютерной сети, работа над проектом выполняется согласно следующим принципам структурного проектирования:

1 Иерархическая структура. В рамках этого принципа сложная система разбивается на меньшие.

2 Модульность. Разделение различных функций по отдельным модулям облегчает проектирование сети.

3 Отказоустойчивость. Резервирование каналов и маршрутов.

4 Гибкость. Возможность изменять участки сети, добавлять новые сервисы или увеличивать пропускную способность без полной модернизации основного оборудования (то есть без замены аппаратных устройств).

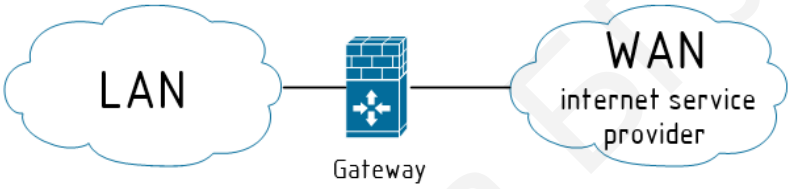


Рисунок 10 – Укрупнённая структура компьютерной сети

Стоит отметить, что начинающий проектировщик сети редко задаётся следующими вопросами:

1 Как гарантировать изоляцию трафика на *L*3 (*path-isolation*)?

2 Как безопасно предоставить доступ в *Internet* гостевым устройствам (*guest security*)?

3 Как создать сеть для временных работников и внешних аудиторов (*temporary network*)?

4 Как контролировать действия гостей, аудиторов и контрактников в локальной сети (*network monitoring*)?

5 Как уменьшить время простоя при пересчете *STP*?

6 Как сделать проводную сеть такой же безопасной, как и беспроводная (*networking security*)?

7 Как уменьшить затраты на закупку и поддержку оборудования?

Это только часть вопросов, которые определяют удобство работы и исправления неполадок в спроектированной сети.

Сеть с иерархической структурой делится на несколько отдельных уровней. Каждый уровень в иерархии обеспечивает конкретные функции, которые определяют его роль в сети. В итоге реализуется топология типа «звезда». Это позволяет проектировщику и архитектору сети оптимизировать решение и выбрать соответствующее сетевое оборудование, программное

обеспечение и функции для выполнения конкретных ролей на этом сетевом уровне.

4.2 Проектирование компьютерной сети отдела

Компьютерная сеть небольшой организации или отдела, насчитывающего 2–7 рабочих мест, не может содержать много отдельных сетевых устройств по причине трудоёмкости их раздельного администрирования и высокой суммарной стоимости. Как правило, такая сеть представляет собой один коммутационный домен, объединённый *SOHO*-устройством (низко- или среднепроизводительным *L*3-шлюзом, решающим задачи коммутации, маршрутизации, фильтрации трафика и даже конечного *VPN*-устройства) и поэтому называется плоской сетью. На рисунке 11 приведена упрощённая схема описанной сети отдела.

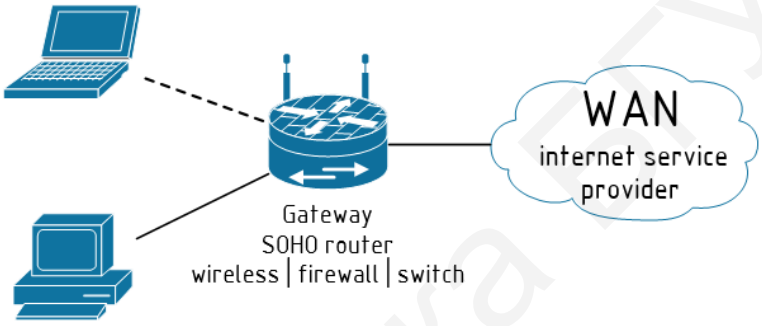


Рисунок 11 – Схема компьютерной сети отдела

Представленная на рисунке структура сети обычно реализуется провайдерами в квартирах абонентов. Пропускная способность каналов такой сети редко превышает 1 Гбит/с.

При увеличении количества конечных устройств производительности и портовой ёмкости такого шлюза начинает не хватать. При увеличении числа рабочих мест до 12–25 функции *SOHO*-устройства делятся между различным оборудованием. В частности, выделяют уровень доступа и шлюз. Такая одноуровневая схема сети приведена на рисунке 12. Уровень доступа (*access layer*) включает в себя *L*2-коммутаторы и другие *L*2-устройства с устоявшимся на практике стандартом подключения конечных устройств *Gigabit Ethernet*. Подключение к сети провайдера выполняет *L*3-шлюз (обычно маршрутизатор) с устоявшимся на практике стандартом подключения 10 *Gigabit Ethernet*.

В такой схеме сети шлюз является самым высоконагруженным и уязвимым звеном. Особенно при наличии нескольких *L*2-устройств выход шлюза из строя делит сеть на автономные физические сегменты без доступа к *WAN* (фактически является единой точкой отказа сети). Это может быть особо критично для организаций с развитой информационной инфраструктурой.

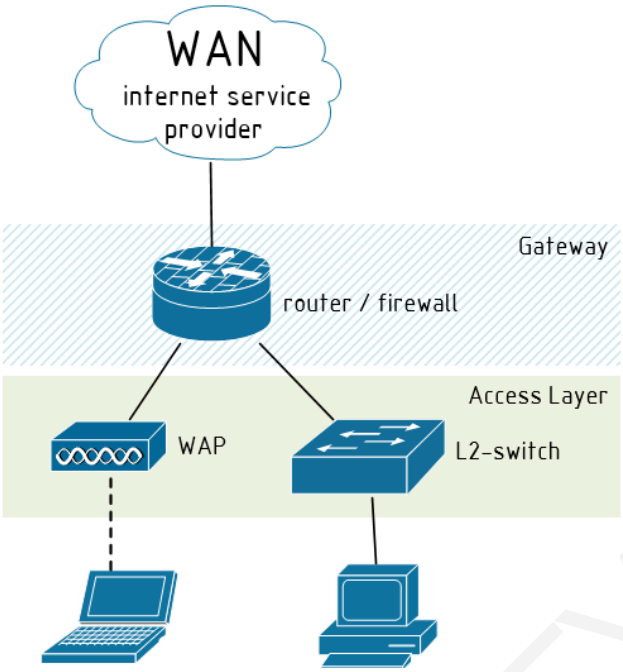


Рисунок 12 – Схема одноуровневой компьютерной сети небольшой организации

Для проектирования компьютерной сети с количеством рабочих мест более 50 обычно используется другой подход, в том числе применяющийся при проектировании компьютерной сети здания или группы рядом стоящих зданий, называемых кампусом.

4.3 Проектирование компьютерной сети кампуса

Компьютерную сеть кампуса называют *CAN* (*Campus Area Network*). Классически *CAN* реализована двух- или трёхуровневой иерархической архитектурой, где каждый уровень выполняет определенные функции. Такое разделение упрощает проектирование, развертывание и администрирование сети.

Первым шагом к разделению сети на функциональные уровни стала двухуровневая иерархическая архитектура (см. рисунок 4), состоящая из уровня доступа, уровня вырожденного ядра (*collapsed layer*) и шлюза.

Уровень доступа, как и в рассмотренной ранее структурной схеме, предоставляет конечным устройствам и пользователям подключение к компьютерной сети и выполняет следующие функции: *L2*-коммутация, *VLAN*, *ARP*, *STP*, безопасность интерфейсов, *QoS*-маркировка кадров и определение границ доверия, *VACL*, *PoE* и др. Появившийся уровень вырожденного ядра решает задачи, связанные с надёжным функционированием компьютерной сети. Обычно этот уровень включает в себя основные и резервные *L3*-устройства, а также избыточное количество каналов между ними, которые исключают единую точку отказа и позволяют при выходе из строя любого промежуточного узла обеспечить связь между конечными пользователями (рисунок 13).

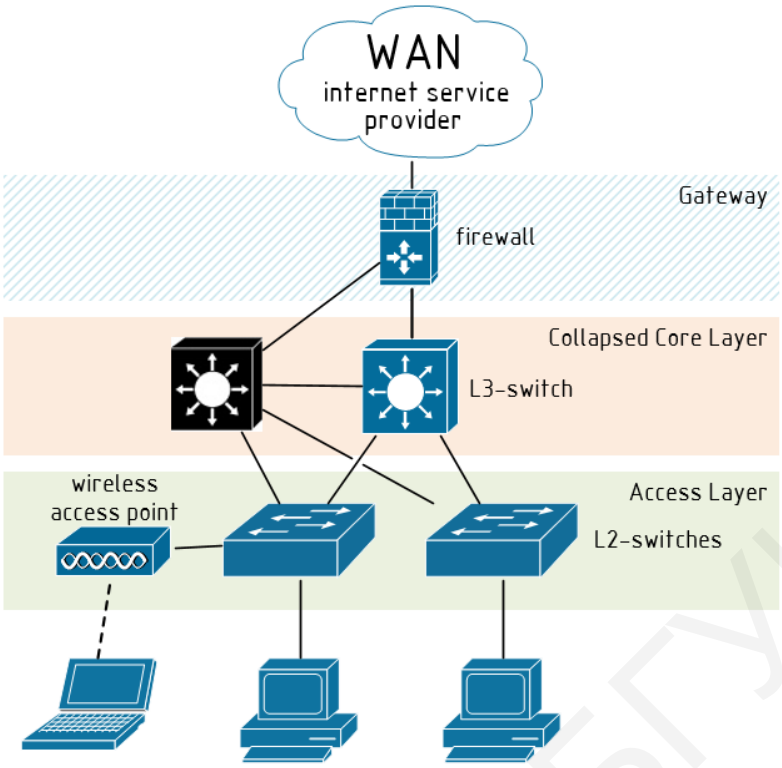


Рисунок 13 – Схема двухуровневой компьютерной сети

Классически же *CAN* реализована трёхуровневой иерархической архитектурой (рисунок 14), состоящей из уровня доступа, уровня распределения, уровня ядра и шлюзов.

Уровень распределения решает задачи агрегирования каналов и данных, внутренней фильтрации трафика, маршрутизации между подсетями и *VLAN*, балансировки нагрузки, управления широковещательными доменами и др. Устройства уровня распределения являются центральной точкой в коммутационных шкафах.

Уровень ядра называют также сетевой магистралью. Уровень ядра состоит из высокоскоростных сетевых устройств, предназначенных для более быстрой коммутации пакетов (часто в разнородных сетях) и связи нескольких компонентов внутри комплекса зданий, например модулей распределения, сервисных модулей, центров обработки данных и границы *WAN*.

Следует также учитывать следующие соображения относительно уровня ядра:

– обеспечение высокоскоростной коммутации (то есть быстрой передачи данных);

– обеспечение надёжности и устойчивости к сбоям;

– масштабирование за счёт использования более быстродействующего оборудования, а не за счёт увеличения числа устройств;

– устранение операций с пакетами, требующих большой загрузки ЦП (центрального процессора), которые порождаются процессами обеспечения безопасности, классификации *QoS* или иными процессами.

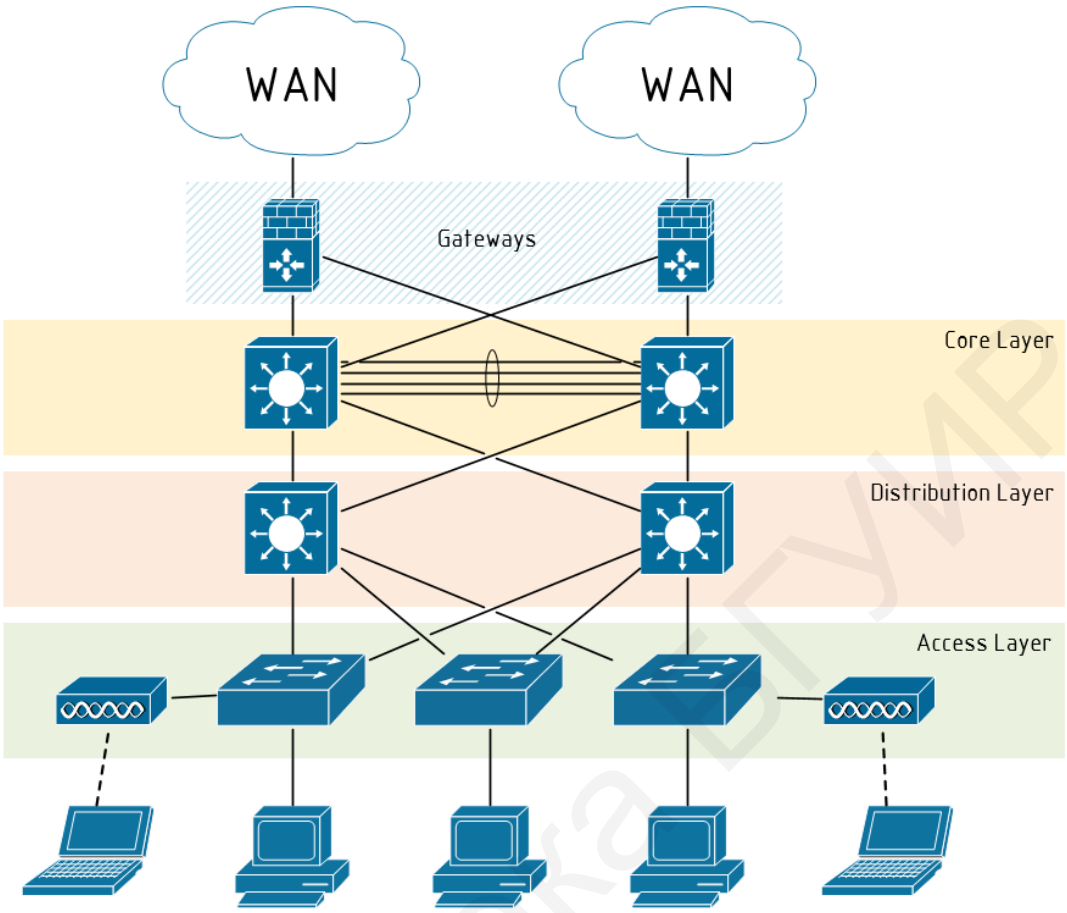


Рисунок 14 – Схема трёхуровневой компьютерной сети

В последнее время в связи с увеличением объёма трафика, активным использованием ресурсов сети для передачи медиа-трафика (аудио и видео) возникла необходимость отделять серверы компании от обычных компьютеров, подключать их через выделенные коммутаторы с целью более гибкого управления пропускной способностью каналов.

Серверная ферма представляет собой группу коммутаторов, являющуюся ключевой компонентой ЛВС (локальной вычислительной системой) предприятия, обеспечивающей подключение к ней серверов. Важное требование, предъявляемое к серверной ферме, заключается в высокой производительности и надежности. Простои серверной фермы приводят к простоям работы информационных систем, а следовательно, к потерям дохода организации.

Таким образом, многоуровневая архитектура сети позволяет индивидуально решать задачи организации, сокращать время простоя сети и информационных систем и минимизировать потери рабочего времени, а также создает возможность внедрения дополнительных приложений и сервисов.

4.4 Планирование компьютерной сети группы зданий

Классическая иерархическая *LAN* для комплекса зданий (филиалов организации) содержит следующие три уровня:

1 Уровень доступа обеспечивает доступ к сети рабочей группе или отдельному пользователю.

2 Уровень распределения обеспечивает маршрутизацию и фильтрацию трафика различных сетей и контролирует границу между уровнями доступа и ядра.

3 Уровень ядра обеспечивает быструю передачу данных между коммутаторами-распределителями в рамках комплекса зданий предприятия.

4.5 Проектирование информационной инфраструктуры организации

Рассмотренный в пособии подход к проектированию сети называется проектированием на основе многоуровневой модели. Его преимуществами являются:

– понятный и задокументированный типовой дизайн с многолетней историей успешных внедрений;

– использование индустриальных стандартов протоколов;

– возможность использования оборудования различных производителей и ценовой категории.

Недостатками такого подхода являются:

– трудоёмкая конфигурация для достижения быстрой конвергенции сети;

– дополнительная сложность в эксплуатации при добавлении *VLAN*- или *VRF*-сегментации;

– индивидуальное управление всем сетевым оборудованием.

4.6 Подключение к глобальной сети

В настоящий момент в стране доступ к сети *Internet* для организаций предоставляется с помощью следующих технологий:

1 *xDSL* (*Digital Subscriber Line*) – технология широкополосного доступа к сети Internet по абонентскому каналу телефонной линии общего назначения. Часто данную технологию называют технологией «последней мили»: она несложная в установке, не требует дорогого оборудования, однако ограничена в максимальной пропускной способности (преимущественно до 10 Мбит/с). К основным типам *xDSL* относятся *ADSL*, *HDSL*, *RADSL*, *SDSL* и *VDSL*. Для реализации такого подключения необходим модем (сплиттер), представляющий собой фильтр низких частот и предназначенный для разделения низкочастотного сигнала обычной телефонной связи и высокочастотного сигнала *DSL*.

2 *Ethernet* по «витой паре». Это классическая устоявшаяся технология подключения абонентов, которая нецелесообразна при большой удалённости абонента от телекоммуникационных узлов провайдера из-за высокой стоимости кабеля и необходимости установки повторителей электрического сигнала.

3 Подключение по сети *3G/4G* – технология доступа к сети *Internet* посредством мобильной сети. Для реализации такого подключения необходим *3G/4G*-модем, подключённый к прокси-серверу или шлюзу сети. Данная технология требует развитой инфраструктуры поставщика услуг, а подключение зависит от множества внешних факторов.

4 *xPON* (*Passive Optical Network*) – технология доступа к сети *Internet* по оптическим каналам связи. Пассивной такая сеть называется потому, что в её древовидной структуре не содержится активных устройств с оптико-электрическим преобразованием сигналов. Вместо этого для передачи данных в системах *xPON* используются пассивные оптоволоконные смесители или разветвители. Для реализации такого подключения используются оптические терминалы (*PON*-модемы).

5 ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ В КОМПЬЮТЕРНЫХ СЕТЯХ

5.1 Сегментация компьютерной сети

Для уменьшения широковещательных доменов и повышения безопасности сети повсеместное применение получила технология виртуальных компьютерных сетей (*VLANs – Virtual Local Area Networks*). Технология *VLAN* – механизм для создания логической топологии сети, не зависящей от её физической топологии.

VLAN – логическая группа хостов, трафик которой (в том числе и широковещательный) на канальном уровне полностью изолирован от других узлов сети (рисунок 15). Это означает, что передача кадров между разными *VLANs* на основании *MAC*-адреса невозможна независимо от типа адреса. В то же время внутри *VLAN* кадры передаются по правилам коммутации, то есть только на тот интерфейс, который связан с адресом назначения кадра.

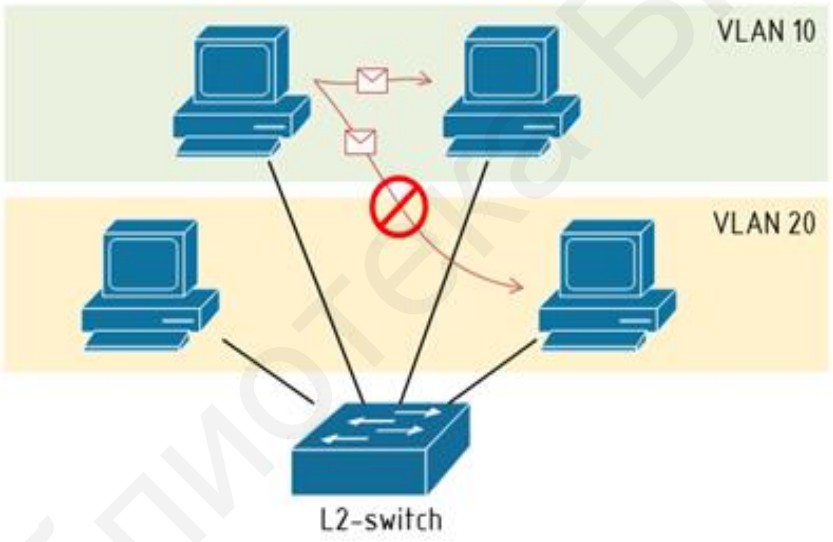


Рисунок 15 – Схема разделения физической сети на две виртуальные: *VLAN* 10 и *VLAN* 20

Технология *VLAN* реализована в программном обеспечении сетевого оборудования и поддерживается не всеми устройствами.

Основные функции технологии *VLAN* и преимущества её использования:

– гибкое разделение устройств на группы (оптимизация применения групповых, а не локальных политик);

– сокращение широковещательного трафика в сети (увеличение пропускной способности сети);

– возможность применения политик взаимодействия хостов различных *VLANs* (повышение безопасности и управляемости сети).

В коммутаторах могут быть реализованы следующие наиболее распространённые типы *VLAN*:

1 *VLAN* на основе интерфейсов (*port-based VLAN*).

При использовании *port-based VLAN* на основе портов каждый интерфейс назначается для одной определённой *VLAN*, независимо от того, какой пользователь или хост подключён к этому интерфейсу. Это означает, что все хосты, подключённые к этому порту, будут членами одной *VLAN*. Конфигурация интерфейсов статическая и может быть изменена только вручную. Данный тип *VLAN* рекомендуется использовать в сети, содержащей один коммутатор.

Достоинствами *port-based VLAN* являются простота настройки и возможность лёгкой реорганизации логической сети. Основным недостатком такого решения является то, что при маршрутизации один порт каждой VLAN необходимо подключать к маршрутизатору. Это приводит к дополнительным расходам на покупку кабелей и маршрутизаторов, а также порты коммутатора используются неэкономно.

2 *VLAN* на основе стандарта *IEEE 802.1Q*.

IEEE 802.1*Q* – стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к *VLAN*. Коммутатор, поддерживающий *IEEE* 802.1*Q*, помещает внутрь кадра тег, который содержит информацию о принадлежности трафика к определённой *VLAN*. Согласно этому стандарту заголовок кадра не изменяется, поэтому сетевые устройства, которые не поддерживают этот стандарт, могут передавать трафик без учёта его принадлежности к *VLAN*.

3 *VLAN* на основе *MAC*-адресов. В этом случае принадлежность пакета к *VLAN* определяется *MAC*-адресом источника или приёмника. Каждый коммутатор поддерживает таблицу *MAC*-адресов и их соотношение с *VLAN*. Ключевое преимущество этого метода состоит в том, что не требуется переконфигурация коммутатора при переподключении пользователей к различным портам. Однако присвоение *MAC*-адресов *VLAN* может потребовать значительных временных затрат, а также присвоение отдельных *MAC*-адресов нескольким *VLAN* может быть непростой задачей и существенным ограничением для совместного использования ресурсов сервера между несколькими *VLAN*.

Наиболее часто используемым стандартом для конфигурации *VLAN* является *IEEE* 802.1*Q*

Каждая виртуальная сеть имеет индивидуальный номер, который варьируется.

Порты коммутатора, поддерживающего *VLAN*, можно разделить на два множества (рисунок 16):

1) транковые порты (*trunk*-порты);

2) порты доступа (*access*-порты).

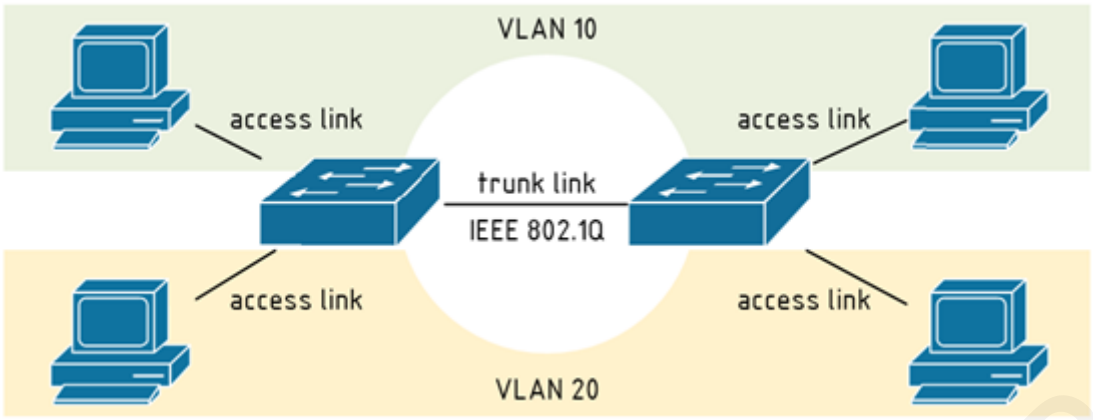


Рисунок 16 – Использование магистральных каналов в технологии *VLAN*

Транковые порты нужны для того, чтобы через один порт была возможность передать несколько *VLAN* и, соответственно, получать трафик нескольких *VLAN* на один порт. Информация о принадлежности трафика *VLAN*, как было сказано, указывается в специальном теге. Без тега коммутатор не сможет различить трафик разных *VLAN*. Если порт является портом доступа в каком-то *VLAN*, то его трафик передаётся без тега. Порт доступа может быть только в одной виртуальной локальной сети. Если порт является транковым, то в этом случае весь нетегированный трафик будет приниматься специальным *VLAN* (*native VLAN*). Проще всего это понять, если «забыть» всю внутреннюю структуру коммутатора и отталкиваться только от портов. Допустим, есть *VLAN* с номером 111, есть два порта, которые принадлежат к *VLAN* 111. Они общаются только между собой: с *access*-порта выходит нетегированный трафик; с *trunk*-порта выходит трафик, тегированный в *VLAN* 111. Все необходимые преобразования прозрачно внутри себя делает коммутатор. Обычно по умолчанию все порты коммутатора считаются портами доступа и принадлежат *VLAN* 1. В процессе настройки или работы коммутатора они могут перемещаться в другие *VLAN*.

Существуют два подхода к назначению порта в определённый *VLAN*:

• статическое назначение – когда принадлежность порта к определённому *VLAN* задаётся администратором в процессе настройки;

• динамическое назначение – когда принадлежность порта к определённому *VLAN* определяется в ходе работы коммутатора с помощью процедур, описанных в специальных стандартах, таких, например, как 802.1*X*. При использовании 802.1*X* для того, чтобы получить доступ к порту коммутатора, пользователь проходит аутентификацию на *RADIUS*-сервере. По результатам аутентификации порт коммутатора размещается в том или ином *VLAN*.

VTP – VLAN trunking protocol. Без автоматизированного метода управления корпоративной сетью с сотнями *VLAN* потребовалась бы ручная настройка каждой *VLAN* на каждом коммутаторе. Любое изменение структуры

VLAN требует дополнительной ручной настройки. Один неверно набранный номер может стать причиной неустойчивости соединений по всей сети.

Чтобы решить эту проблему, был создан протокол *VTP*, который автоматизирует многие задачи конфигурации *VLAN*. *VTP* гарантирует согласованное обслуживание конфигурации *VLAN* по всей сети и уменьшает необходимость в управлении и мониторинге *VLAN*.

VTP – это протокол обмена сообщениями с архитектурой «клиент – сервер», который добавляет, удаляет и переименовывает *VLAN* в одном домене *VTP*. Все коммутаторы под общим управлением являются частью домена. У каждого домена есть уникальное имя. Коммутаторы *VTP* обмениваются сообщениями *VTP* только с другими коммутаторами в домене.

VTP использует три режима: серверный, клиентский и прозрачный. По умолчанию все коммутаторы являются серверами. Рекомендуется настроить хотя бы два коммутатора в сети в качестве серверов, чтобы обеспечить резервирование.

5.2 Агрегация каналов

Агрегирование каналов – технология, которая позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность и надёжность канала. Агрегирование каналов может быть настроено между двумя коммутаторами, коммутатором и маршрутизатором (рисунок 17).

Агрегирование каналов позволяет решить две задачи:

1) повысить пропускную способность канала;

2) обеспечить резерв на случай выхода из строя одного из каналов.

Большинство технологий по агрегированию позволяют объединять только параллельные каналы, то есть такие, которые начинаются на одном и том же устройстве и заканчиваются на другом.

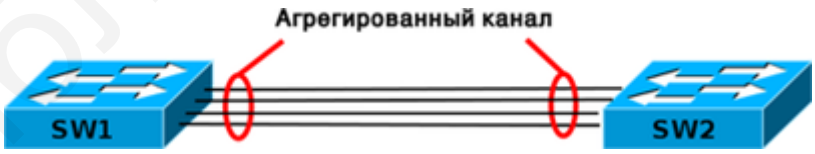


Рисунок 17 – Агрегированный канал

Если рассматривать избыточные соединения между коммутаторами, то без использования специальных технологий для агрегирования каналов передаваться данные будут только через один интерфейс, который не заблокирован *STP* (рисунок 18). Такой вариант позволяет обеспечить резервирование каналов, но не даёт возможности увеличить пропускную способность.

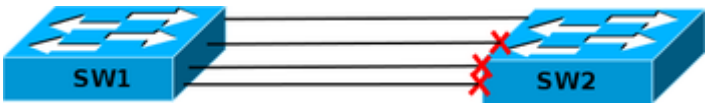


Рисунок 18 – Блокировка интерфейсов протокола *STP* при избыточности соединений

Технологии по агрегированию каналов позволяют использовать все интерфейсы одновременно. При этом устройства контролируют распространение широковещательных фреймов (а также *multicast* и *unknown unicast*), чтобы они не зацикливались. Для этого коммутатор при получении широковещательного фрейма через обычный интерфейс отправляет его в агрегированный канал только через один интерфейс, а при получении широковещательного фрейма из агрегированного канала не отправляет его назад.

Для агрегирования каналов может быть использован один из трёх вариантов:

– *LACP* (*Link Aggregation Control Protocol*) стандартный протокол;

– *PAgP* (*Port Aggregation Protocol*) проприетарный протокол *Cisco*;

– статическое агрегирование без использования протоколов.

Так как *LACP* и *PAgP* решают одни и те же задачи (с небольшими отличиями по возможностям), то лучше использовать стандартный протокол. Фактически остается выбор между *LACP* и статическим агрегированием.

Статическое агрегирование

Преимущество: не вносит дополнительную задержку при поднятии агрегированного канала или изменении его настроек.

Недостатки:

– нет согласования настроек с удалённой стороной;

– ошибки в настройке могут привести к образованию петель.

Агрегирование с помощью LACP

Преимущества:

– согласование настроек с удаленной стороной позволяет избежать ошибок и петель в сети;

– поддержка *standby*-интерфейсов позволяет агрегировать до 16 портов, восемь из которых будут активными, а остальные – в режиме *standby*.

Недостаток: вносит дополнительную задержку при поднятии агрегированного канала или изменении его настроек.

При настройке агрегирования каналов на оборудовании используется несколько терминов:

– *etherChannel* – технология агрегирования каналов;

– *port-channel* – логический интерфейс, который объединяет физические интерфейсы;

– *channel-group* – команда, которая указывает, какому логическому интерфейсу принадлежит физический интерфейс и какой режим используется для агрегирования.

5.3 Избыточность каналов связи

Для обеспечения высокой отказоустойчивости компьютерной сети в неё нередко включают избыточные каналы связи. Это исключает единую точку отказа – и сеть может функционировать в случае выхода из строя основного канала связи или физического интерфейса. Также избыточные каналы связи можно использовать для снижения нагрузки на основные, увеличивая пропускную способность.

Избыточность физических каналов связи имеет следующие недостатки: нестабильность таблицы *MAC*-адресов (кадры с одинаковым *MAC*-адресом источника могут быть получены на разных интерфейсах), широковещательные штормы при наличии петель в сети, а также возникновение копий кадров даже *unicast*-рассылки. Для устранения этих недостатков используются протоколы канального уровня типа *STP* (*Spanning-Tree Protocol*, *IEEE* 802.1*d*): *RSTP* (*Rapid Spanning-Tree Protocol*), *MSTP* (*Multiple Spanning-Tree Protocol*) и др. Они обеспечивают только один логический путь между всеми хостами в сети путём намеренного блокирования резервных путей, которые могли бы образовать петлю.

Суть работы *STP*-протоколов заключается в том, что поддерживающие их коммутаторы обмениваются друг с другом *BPDUs* (*Bridge Protocol Data units*). На основании содержащегося в них *BID* (*Bridge ID*) один из коммутаторов назначается корневым мостом (*root bridge*), после чего все остальные коммутаторы по алгоритму *STA* (*Spanning-Tree Algorithm*) выбирают для работы интерфейсы, называемые *root ports* и соединённые с корневым мостом кратчайшим путём (учитывается количество посредников и пропускная способность каналов). Все прочие интерфейсы, ведущие к корневому мосту, блокируются. Таким образом образуется несвязное дерево с корнем в назначенном коммутаторе.

BID содержит значение приоритета, *MAC*-адрес отправляющего коммутатора и дополнительный расширенный идентификатор системы. Самое низкое значение *BID* определяется комбинацией значений в этих трёх полях.

У любого некорневого коммутатора может быть только один корневой порт. Порт считается заблокированным, когда заблокированы отправка и приём данных на этот порт.

5.4 Технология *VPN*

VPN (*Virtual Private Network*) – обобщённое название группы технологий, позволяющих реализовать одну логическую топологию сети поверх другой (например, *LAN* поверх *Internet*). В зависимости от применяемых протоколов и назначения *VPN* может обеспечивать соединения трёх видов: узел – узел, узел – сеть и сеть – сеть.

Примеры *VPN*:

– *IPSec* (*IP Security*) – часто используется поверх *IPv*4;

– *PPTP* (*Point-to-Point Tunneling Protocol*) – разрабатывался совместными усилиями нескольких компаний, включая *Microsoft*;

– *PPPoE* (*PPP* (*Point-to-Point Protocol*) *over Ethernet*);

– *L2TP* (*Layer* 2 *Tunnelling Protocol*) – используется в продуктах компаний *Microsoft* и *Cisco*;

– *L2TPv*3 (*Layer* 2 *Tunnelling Protocol version* 3);

– *Open VPN SSL VPN* с открытым исходным кодом, поддерживает режимы *PPP*, *bridge*, *point-to-point*, *multi-client server*;

– *freelan SSL P2P VPN* с открытым исходным кодом;

– *Hamachi* – программа для создания одноранговой *VPN*-сети.

5.5 Безопасность в компьютерной сети *ACL* (фильтрация трафика)

Одним из наиболее распространённых способов фильтрации трафика является использование списков контроля доступа (*ACL*-списков). *ACL*-списки можно применять для управления входящим и существующим трафиком в сети и его фильтрации (рисунок 19).

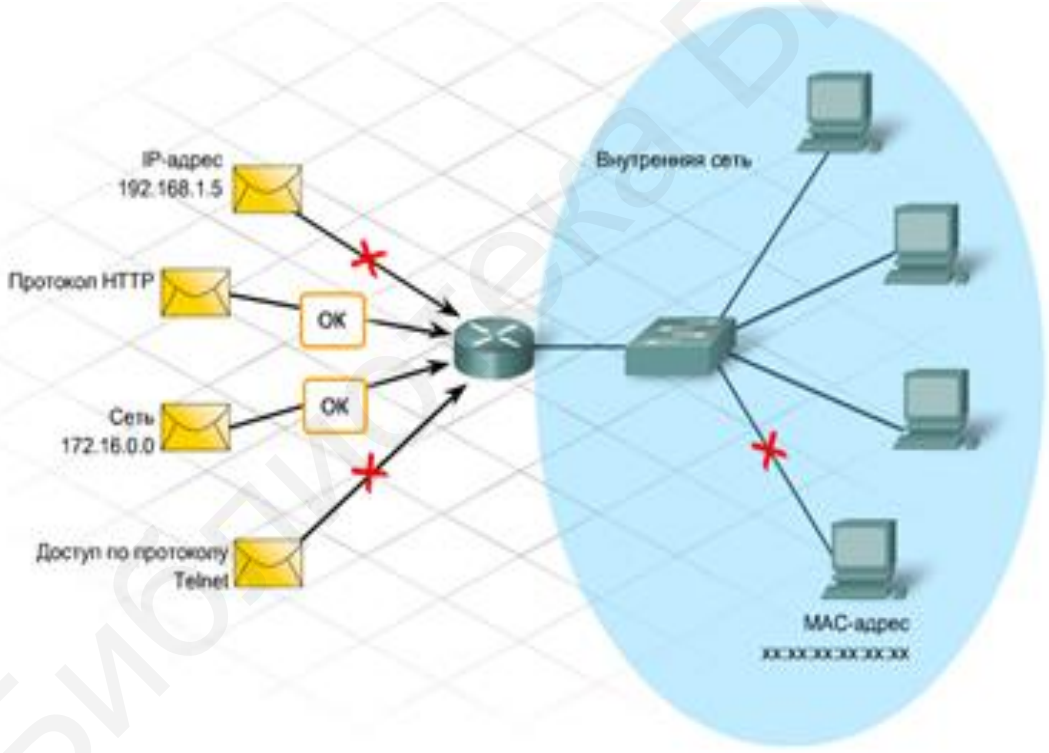


Рисунок 19 – Фильтрация трафика

Существует три типа *ACL*-списков:

1 Стандартный *ACL*-список является самым простым из трёх типов. При создании такого списка для *IP*-протокола фильтрация по *ACL*-спискам осуществляется на основе исходного *IP*-адреса пакета. Стандартные *ACL*-списки определяют разрешения пакетов на основе всего протокола, такого как

IP-протокол. Таким образом, при запрете узлового устройства стандартным *ACL*-списком запрещаются все службы этого узла.

2 Расширенные *ACL*-списки используются для фильтрации не только по исходному *IP*-адресу, но и по конечному *IP*-адресу, протоколу и номерам портов. Такие списки используются чаще стандартных, поскольку они являются более определёнными и обеспечивают более высокий уровень контроля. Расширенным *ACL*-спискам присваиваются номера из диапазона от 100 до 199 и от 2 000 до 2 699.

3 Именованные *ACL*-списки (*NACL*-списки) имеют формат стандартного или расширенного списка и обозначаются описательным именем, а не номером. При настройке именованных *ACL*-списков маршрутизатор *IOS* использует режим подкоманды *NACL*.

Размер *ACL*-списка может варьироваться от одной инструкции, по которой разрешается или блокируется трафик от одного источника, до сотни инструкций, разрешающих или запрещающих пакеты с нескольких источников. В основном *ACL*-списки используются для определения типов принимаемых или отклоняемых пакетов.

Администратору доступно несколько вариантов создания списков контроля доступа. Сложность требований к структуре определяет тип необходимого *ACL*-списка (рисунок 20).

Типы списков доступа IOS

Тип ACL-списка	Пример команды/инструкции ACL-списка	Назначение инструкции
Стандартный	`Router(config)#access-list 1 permit host 172.16.2.88`	• Разрешает конкретный IP-адрес
Расширенный	`Router(config)#access-list 100 deny tcp 172.16.2.0 0.0.0.255 any eq telnet`	• Запрещает доступ из подсети 172.16.2.0/24 к любому другому узлу с помощью telnet
Именованный	`Router(config)#ip access-list standard permit-ip` `Router(config-ext-nacl)#permit host 192.168.5.47`	• Создает стандартный список доступа с именем permit-ip • Разрешает доступ с IP-адреса 192.168.5.47 • Первая команда переводит маршрутизатор в режим подкоманд NACL-списка.

Рисунок 20 – Типы *ACL*-списков

5.6 Протокол *PPP*

Протокол «точка – точка» (*PPP*) является инкапсуляцией канального уровня для последовательных каналов. Он использует многоуровневую архитектуру для инкапсулирования и передачи датаграмм нескольких протоколов по прямому каналу. Так как протокол *PPP* является стандартизированным, он позволяет подключать оборудование разных производителей.

Стандарт *PPP* содержит два подпротокола:

1 Протокол управления каналом. *PPP* использует протокол управления каналом (*LCP*) для установления, поддержки, тестирования и завершения передачи данных по прямому соединению. Дополнительно протокол управления каналом согласовывает и настраивает параметры канала сети *WAN* (рисунок 21). Протокол *LCP* выполняет согласование следующих параметров: аутентификация, сжатие, обнаружение ошибок, группа каналов, обратный *PPP*-вызов.

Также протокол *LCP* обрабатывает различные размеры пакетов, обнаруживает общие ошибки настроек, определяет нормальную и сбойную работу канала.

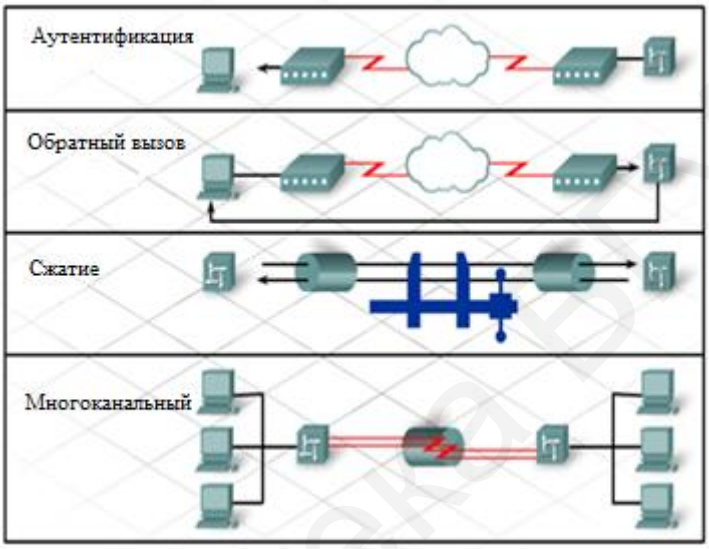


Рисунок 21 – Согласование параметров

2 Протокол управления сетью. Протокол *PPP* использует компонент протокола управления сетью (*NCP*) для инкапсулирования нескольких протоколов сетевого уровня, чтобы они могли выполняться в тех же каналах связи.

Для каждого протокола сетевого уровня, передаваемого по каналу *PPP*, требуется отдельный протокол управления сетью. Например, протокол *IP* использует управляющий межсетевой протокол (*IPCP*), а протокол *IPX* – протокол управления межсетевым обменом пакетами (*IPXCP*). Протоколы управления сетью включают поля с кодами, которые определяют протокол сетевого уровня.

Выполнение сеансов *PPP* проходит через три этапа:

1 Этап установления соединения. *PPP* отправляет кадры по протоколу *LCP* для настройки и тестирования канала передачи данных. Кадры *LCP* содержат поле параметров настройки, которое выполняет согласование таких параметров, как максимальный размер передаваемого блока данных (*MTU*), сжатие и аутентификация соединения. Если какой-либо параметр настройки отсутствует, предполагается, что он имеет значение по умолчанию. На этапе аутентификации

соединения и определения качества канала проверяются параметры этапа установки соединения. Проверка определения качества соединения устанавливает, имеет ли соединение достаточное качество для поддержки протоколов сетевого уровня. Необязательные параметры могут быть указаны перед получением кадра с подтверждением настроек. Получением кадра с подтверждением настроек завершается этап установки соединения.

2 Этап аутентификации (необязательно). На данном этапе включается защита с помощью паролей для идентификации маршрутизаторов соединения. Аутентификация происходит после того, как два маршрутизатора выполнят согласование по настройке параметров, но до того, как может начаться этап согласования протокола управления сетью.

3 Этап согласования протокола управления сетью. *PPP* отправляет пакеты по протоколу управления сетью для выбора настройки одного или нескольких протоколов сетевого уровня, таких как *IP* или *IPX*. Если протокол управления каналом закрывает соединение, информацию об этом получают протоколы сетевого уровня, поэтому они могут выполнить соответствующие действия. Команда *show interfaces* отображает состояния протоколов *LCP* и *NCP*.

После установки соединения канал *PPP* остается активным, пока кадры протокола *LCP* или *NCP* не закроют канал или не истечёт время активности соединения. Также завершить соединение может пользователь.

5.7 Организация *DMZ*

Рассмотрим модели организации доступа к информационной инфраструктуре предприятия из сети *Internet*:

1 *Модель плоской сети* (рисунок 22). В данном варианте все хосты корпоративной сети содержатся в одной, общей для всех сети, в рамках которой коммуникации между ними не ограничиваются. Сеть подключена к *Internet* через пограничный маршрутизатор (межсетевой экран).

Достоинства:

– минимальные требования к функциональным возможностям пограничного маршрутизатора (можно реализовать даже на *SOHO*-маршрутизаторе);

– минимальные требования к знаниям специалиста, осуществляющего реализацию.

Недостаток: минимальный уровень безопасности (в случае взлома, при котором нарушитель получит контроль над одним из серверов, ему для дальнейшей атаки становятся доступны все остальные хосты и каналы связи сети).

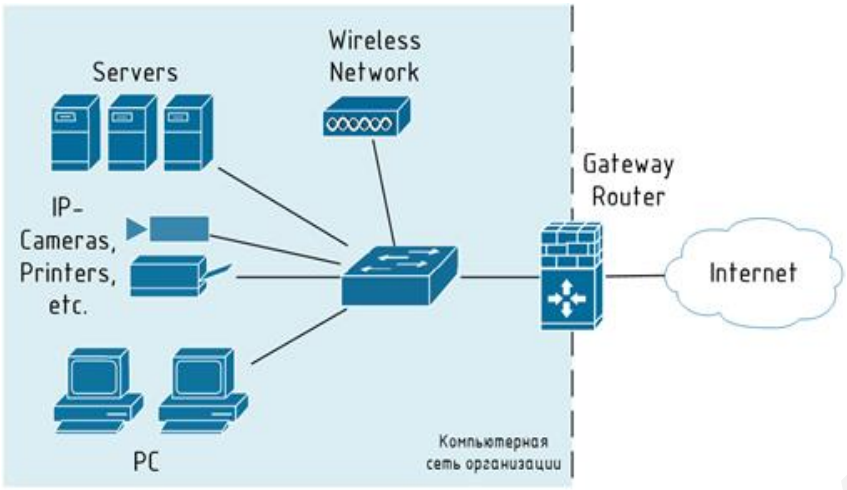


Рисунок 22 – Топология модели плоской сети

2 *Модель DMZ*. Для устранения недостатка модели плоской сети узлы, доступные из *Internet*, размещают в специально выделенный сегмент – демилитаризованную зону (*DMZ*). *DMZ* организуется с помощью межсетевых экранов, отделяющих её как от сети *Internet* (*IFW*), так и от внутренней сети (*DFW*) (рисунок 23).

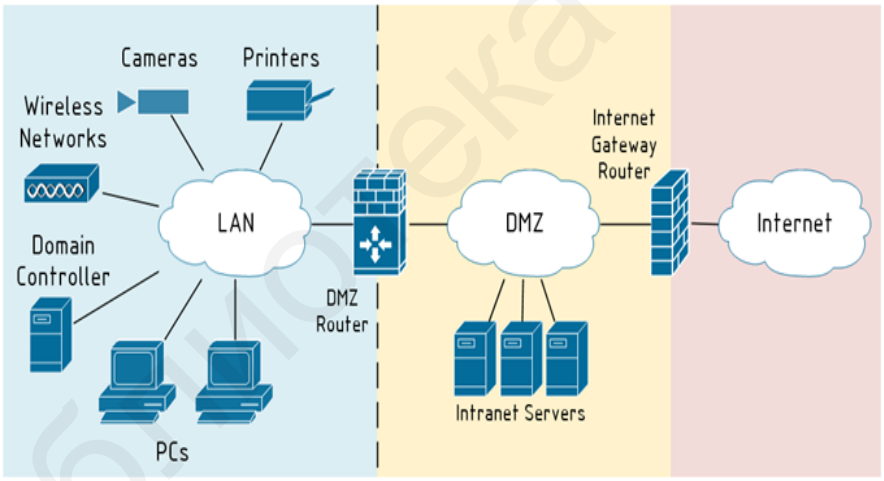


Рисунок 23 – Модель *DMZ* с межсетевым экраном

При этом правила фильтрации межсетевых экранов выглядят следующим образом:

– из внутренней сети можно инициировать соединения в *DMZ* и *WAN*;

– из *DMZ* можно инициировать соединения в *WAN*;

– из *WAN* можно инициировать соединения в *DMZ*;

– инициация соединений из *WAN* и *DMZ* ко внутренней сети запрещена.

Достоинство: повышенная защищённость сети от взломов отдельных сервисов (даже если один из серверов будет взломан, нарушитель не сможет получить доступ к ресурсам, находящимся во внутренней сети (например, сетевым принтерам, системам видеонаблюдения и т. д.)).

Недостатки:

– сам по себе вынос серверов в *DMZ* не повышает их защищённость;

– необходим дополнительный межсетевой экран для отделения *DMZ* от внутренней сети (рисунок 24).

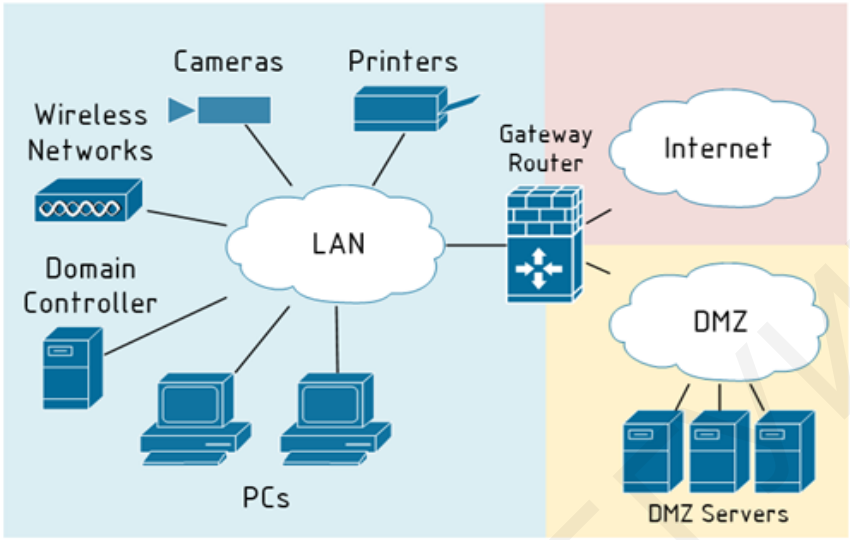


Рисунок 24 – *DMZ Servers*

3 *Модель разделения сервисов на front-end и back-end.* Одним из вариантов исправления ситуации безопасности самого сервиса является разделение функционала сервиса на две части: *front-end* и *back-end*. При этом каждая часть располагается на отдельном сервере, между которыми организуется сетевое взаимодействие. Серверы *front-end*, реализующие функционал взаимодействия с клиентами, находящимися в Internet, размещают в *DMZ*, а серверы *back-end*, реализующие остальной функционал, оставляют во внутренней сети. Для взаимодействия между ними на межсетевых экранах создают правила, разрешающие инициацию подключений от *front-end* к *back-end* (рисунок 25).

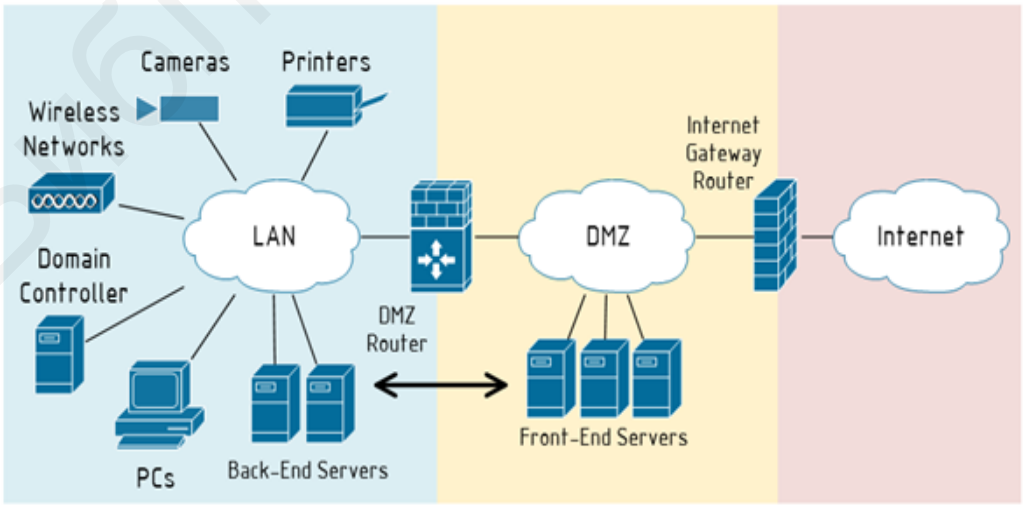


Рисунок 25 – Инициация соединений от *front-end* и *back-end*

В качестве примера рассмотрим корпоративный почтовый сервис, обслуживающий клиентов как в локальной сети, так и из *Internet*. Клиенты изнутри используют *POP*3/*SMTP*/*IMAP*, а клиенты из *Internet* работают через веб-интерфейс. Обычно на этапе внедрения компании выбирают наиболее простой способ развёртывания сервиса и ставят все его компоненты на один сервер. Затем, по мере осознания необходимости обеспечения информационной безопасности, функционал сервиса разделяют на части, и та часть, что отвечает за обслуживание клиентов из I*nternet* (*front-end*), выносится на отдельный сервер, который по сети взаимодействует с сервером, реализующим оставшийся функционал (*back-end*). При этом *front-end* размещают в *DMZ*, а *back-end* остаётся во внутреннем сегменте. Для связи между *front-end* и *back-end* на межсетевых экранах создают правило, разрешающее инициацию соединений от *front-end* к *back-end*.

Достоинства:

– в общем случае атаки, направленные против защищаемого сервиса, могут «споткнуться» о *front-end*, что позволит нейтрализовать или существенно снизить возможный ущерб, например, атаки типа *TCP SYN Flood* или *slow http read*, направленные на сервис, приведут к тому, что *front-end* сервер может оказаться недоступен, в то время как *back-end* будет продолжать нормально функционировать и обслуживать пользователей;

– на *back-end* сервере может не быть доступа в *Internet*, что в случае его взлома (например, локально запущенным вредоносным кодом) затруднит удалённое управление им из *Internet*;

– *front-end* хорошо подходит для размещения на нем межсетевого экрана уровня приложений (например, *Web application firewall*) или системы предотвращения вторжений (*IPS*, например *snort*).

Недостатки:

– для связи между *front-end* и *back-end* на межсетевом экране создаётся правило, разрешающее инициацию соединения из *DMZ* во внутреннюю сеть, что порождает угрозы, связанные с использованием данного правила со стороны других узлов в *DMZ* (например, за счет реализации атак *IP spoofing*, *ARP* poisoning и т. д.);

– не все сервисы могут быть разделены на *front-end* и *back-end*;

– в организации должны быть реализованы бизнес-процессы актуализации правил межсетевого экранирования;

– в компании должны быть реализованы механизмы защиты от атак со стороны нарушителей, получивших доступ к серверу в *DMZ*.

Примечания

1 В реальной жизни даже без разделения серверов на *front-end* и *back-end* серверам из *DMZ* очень часто необходимо обращаться к серверам, находящимся во внутренней сети, поэтому указанные минусы данного варианта будут также справедливы и для предыдущего рассмотренного варианта.

2 Если рассматривать защиту приложений, работающих через веб-интерфейс, то даже если сервер не поддерживает разнесение функций на

front-end и *back-end*, применение *http reverse proxy* сервера (например, *nginx*) в качестве *front-end* позволит минимизировать риски, связанные с атаками на отказ в обслуживании. Например, атаки типа *SYN flood* могут сделать *http reverse proxy* недоступным, в то время как *back-end* будет продолжать работать.

5.8 Управление компьютерной сетью (*SNMP*)

SNMP – это стандартный протокол для управления устройствами в *IP*-сетях. С его помощью серверы могут обмениваться информацией о своем текущем состоянии, а администратор может изменять предварительно определённые значения. Сам протокол очень простой, однако структура основанных на нём программ может оказаться сложной.

Существует много различных версий протокола *SNMP*. Кроме того, протокол частично реализуется некоторыми сетевыми аппаратными устройствами. Наиболее распространённой является версия *SNMPv1*, но она имеет много уязвимостей; основными причинами её популярности являются её вездесущность и долгое время существования. Вместо неё рекомендуется использовать более безопасную версию *SNMPv3*.

Сеть на основе *SNMP* в основном состоит из *SNMP*-агентов. Агент – это программа, которая собирает информацию об аппаратном устройстве, систематизирует её в предварительно определённые записи, а также отвечает на запросы с помощью протокола *SNMP*.

Компонент, который запрашивает данные у агентов, называется менеджером *SNMP*. S*NMP*-менеджеры получают данные о всех управляемых устройствах и могут выдавать запросы для сбора информации и устанавливать некоторые свойства.

Менеджер *SNMP* – это машина, которая запрашивает информацию, собранную агентами *SNMP*. Такая машина гораздо проще устроена, чем клиенты, поскольку она просто запрашивает данные.

Менеджером может быть любая машина, имеющая возможность отправлять запросы агентам *SNMP*, предоставляя валидные учётные данные (например, сервер мониторинга); иногда задачи менеджера выполняет сам администратор с помощью простых утилит для быстрого запроса данных.

Агенты *SNMP* выполняют основную работу. Они отвечают за сбор данных о локальной системе, их хранение в удобном для запросов формате, обновление БД *Management Information Base* (*MIB*).

MIB – это иерархическая, предварительно определенная структура, хранящая информацию, которую можно запросить или добавить. Она доступна для запросов *SNMP*, исходящих от хоста, предоставившего правильные учётные данные (то есть менеджера *SNMP*).

Агент определяет, какие менеджеры могут получить доступ к данным. Также агент может выступать в качестве посредника и передавать информацию на устройства, не настроенные для *SNMP*-трафика.

Отчасти протокол *SNMP* популярен благодаря простым командам. Он выполняет всего несколько операций, но они достаточно гибки.

Следующие блоки данных протокола описывают точные типы сообщений, которые поддерживает протокол:

1 *Get*: это сообщение менеджер отправляет агенту, чтобы запросить значение определённого *OID*. В ответ этот запрос получает сообщение Response, содержащее все необходимые данные.

2 *GetNext*: это сообщение позволяет менеджеру запрашивать следующий последовательный объект в *MIB*. Так можно пересечь структуру *MIB*, не используя в запросах *OID*.

3 *Set*: это сообщение менеджер отправляет агенту для того, чтобы изменить значение переменной. С помощью *Set* можно управлять информацией о конфигурации или иным образом изменять состояние удалённых хостов. Это единственная операция записи, которую поддерживает протокол.

4 *GetBulk*: этот запрос работает как несколько запросов *GetNext*. Менеджер получит в качестве ответа максимальный объём данных (учитывая ограничения запроса).

5 *Response*: агент отправляет это сообщение менеджеру, чтобы передать ему запрашиваемые данные. Если запрашиваемые данные нельзя передать, *Response* будет содержать ошибку с дополнительной информацией. Сообщение *Response* отправляется на любой из вышеперечисленных запросов, а также на сообщение *Inform*.

6 *Trap*: это сообщение обычно отправляется агентом менеджеру, чтобы предоставить информацию о событиях, которые происходят на управляемых устройствах.

7 *Inform*: такое сообщение менеджер отправляет агенту в ответ на *trap*. Если агент не получит такого сообщения, он будет повторно отправлять сообщения *trap*.

5.9 Системы хранения данных

Сегодня все системы хранения данных (СХД) можно разделить на три типа:

– устройства с прямым подключением (*DAS – Direct-Attached Storage*);

– сетевые хранилища (*NAS – Network Attached Storage*);

– сети хранения данных (*SAN – Storage Area Network*).

Чаще всего под *DAS* понимают связку «сервер – накопитель», где «накопитель» – любое запоминающее устройство от *USB* до дискового хранилища. На сегодняшний день чаще всего для связи сервера с накопителем используются интерфейсы *SAS* (*Serial Attached SCSI*) и *eSATA*. Схема такой связки представлена на рисунке 26. Использование такой СХД рационально в организациях с 1–3 внутренними серверами.

Рисунок 26 – Классическая схема *DAS*

Строго говоря, под понятие *DAS* подходит не только классическая комбинация сервера с подключённым накопителем. Например, хранилище *SAN*, подключённое одним единственным кабелем к соответствующему серверному интерфейсу, по сути, представляет собой *DAS*-систему, несмотря на то, что для взаимодействия используется протокол *Fibre Channel*.

Достоинствами использования *DAS* являются низкая стоимость решения, простота организации, сетевая безопасность и высокая скорость передачи данных (более 10 Гбит/с в случае), недостатками – сложность масштабирования, отсутствие консолидации, ограничение отказоустойчивости, сложность разделения ресурсов и сложность управления.

Система *NAS* представляет собой хост в компьютерной сети, единственной функцией которого часто является хранение данных, полученных от других хостов (системам *NAS* предшествовали классические файловые серверы). По сути, *NAS* представляет собой сочетание системы хранения данных и программно-аппаратной платформы, позволяющей подключить эту систему в компьютерную сеть. Явным отличием *NAS* от *DAS* является развитый стек протоколов и наличие сетевой файловой системы совместного доступа. От классических файловых серверов *NAS* могут отличаться проприетарной операционной системой, отсутствием возможности подключения монитора и клавиатуры, ограниченностью установки дополнительного ПО и др.

Схема подключения *NAS*-накопителя представлена на рисунке 27. Использование такой СХД рационально в небольших организациях, имеющих 3–10 низко- или средненагруженных серверов. Часто *NAS* используется в качестве системы резервного копирования инфраструктуры и файлов пользователей.

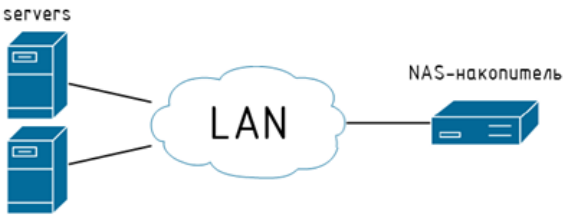


Рисунок 27 – Классическая схема *NAS*

Достоинствами *NAS* являются относительно низкая стоимость, простота управления и разделения ресурсов, недостатками – невысокая скорость передачи данных (при использовании классических подходов), высокие накладные расходы и ограниченность внедрения новых алгоритмов.

Система *SAN* представляет собой самодостаточную систему передачи и хранения данных, не зависящую от компьютерной сети (по сути является отдельной, второй сетью). Основная цель разработки *SAN* – устранение недостатков *DAS* и *NAS*. Наиболее простая схема построения *SAN* для двух серверов приведена на рисунке 28. Использование такой СХД рационально при наличии развитой сетевой инфраструктуры (10 и более серверов) или повышенных требований к доступности данных.

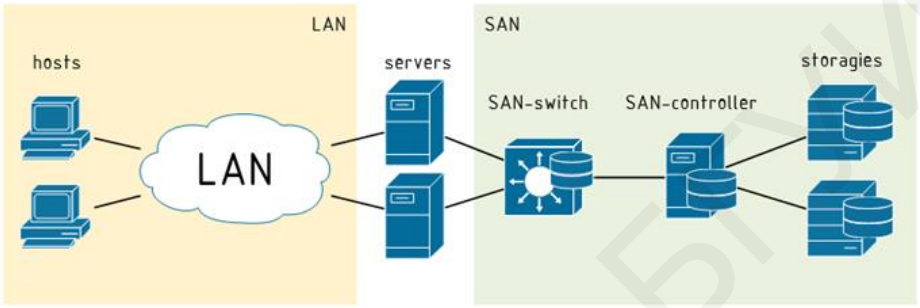


Рисунок 28 – Схема *SAN* с одним *SAN*-коммутатором и *SAN*-контроллером

В зависимости от требований к надёжности системы, размеров и бюджета СХД подключение серверов к *SAN* может быть выполнено через дублирующие коммутаторы и контроллеры. В SAN используются протоколы на базе *FC* (*Fibre Channel*) для обеспечения высокой пропускной способности: *FCP* (*FC Protocol*), *FCIP* (*FC over IP*), *FCoE* (*FC over Ethernet*) и др.

Достоинствами SAN являются практически все устранённые недостатки *NAS* и *DAS*, недостатками – высокая стоимость системы и сложность в настройке оборудования.

Существуют также гибридные решения СХД, проектирование которых индивидуально для поставленных задач организации и не может быть рассмотрено в пособии в силу своей специфики.

6 ПРОЕКТИРОВАНИЕ СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

Структурированная кабельная система (СКС) – это физическая основа инфраструктуры сети здания, позволяющая свести в единую систему множество сетевых информационных сервисов разного назначения: локальные вычислительные сети, телефонные сети, системы безопасности, видеонаблюдения и др.

Сам термин «структурированная» предполагает то, что данная система поддерживает телекоммуникационные приложения, поставляемые различными производителями, используя при этом несколько типов передающих сред. Все компоненты системы, к которым относятся телекоммуникационные розетки, коммутаторы, маршрутизаторы, патч-панели, связаны между собой кабелем, поэтому такая система и называется кабельной. Таким образом, структурированная кабельная система представляет собой иерархическую кабельную сеть, с помощью которой все элементы телекоммуникаций объединяются в единое целое и эксплуатируются в соответствии с утверждёнными стандартами (рисунок 29).

Рисунок 29 – Структурированная кабельная система

При проектировании структурированной кабельной системы в здании формируется единый коммутационный центр, который с помощью вертикальной проводки соединён с находящимися на этажах коммутационными узлами. Эти узлы представляют собой стойки или специальные шкафы, содержащие необходимое коммутационное оборудование, основой которого служат патч-панели. Коммутационные узлы позволяют производить администрирование, то есть изменение и дополнение параметров конфигурации системы для всего этажа в целом. От коммутационного узла кабельные линии горизонтально разводятся непосредственно к рабочим местам.

Требования при проектировании СКС:

– должна быть спроектирована с избыточностью по количеству подключений;

– должна быть выполнена в соответствии с международными стандартами (например, *ANSI*/*EIA*/*TIA* 568, *ANSI*/*EIA*/*TIA* 569);

– рабочее место должно иметь как минимум один разъём для подключения к сети и один разъём для подключения к телефонной сети;

– максимальное расстояние горизонтальной сети не должно превышать 90 м;

– каждая линия связи кабельной системы от точки подключения оконечного оборудования до точки подключения к коммутационной панели должна пройти тестирование на принадлежность как минимум к пятой категории;

– должна обеспечивать быструю перекоммутацию линий горизонтальной проводки и магистрали здания;

– монтаж кабелей в коридорах должен осуществляться за фальшпотолком, если таковой имеется, а при его отсутствии – в специализированных кабель-каналах (коробах) или в существующих закладных; в рабочих помещениях подвод кабеля к рабочим местам производится в кабель-каналах.

Готовая структурированная кабельная система должна не только гарантировать функциональность всех устройств, подключенных к ней, но и предоставлять возможность качественного управления ими.

Использование структурированной кабельной системы вместо хаотически проложенных кабелей обеспечивает много преимуществ:

1 Универсальность. СКС при продуманной организации может стать единой средой для передачи компьютерных данных в локальной вычислительной сети, организации локальной телефонной сети, передачи видеоинформации и даже передачи сигналов от датчиков пожарной безопасности или охранных систем. Это позволяет автоматизировать многие процессы контроля, мониторинга и управления хозяйственными службами и системами жизнеобеспечения предприятия.

2 Увеличение срока службы. Срок морального старения хорошо структурированной кабельной системы может составлять до 15 лет.

3 Уменьшение стоимости добавления новых пользователей и изменение их мест размещения. Известно, что стоимость кабельной системы значительна и определяется в основном не стоимостью кабеля, а стоимостью работ по его прокладке. Поэтому более выгодно провести однократную работу по прокладке кабеля, возможно, с большим запасом по длине, чем несколько раз выполнять прокладку, наращивая длину кабеля. При таком подходе все работы по добавлению или перемещению пользователя сводятся к подключению компьютера к уже имеющейся розетке.

4 Возможность лёгкого расширения сети. Структурированная кабельная система является модульной, поэтому ее легко расширять. Например, к магистрали можно добавить новую подсеть, не оказывая никакого влияния на существующие подсети. Можно заменить в отдельной подсети тип кабеля

независимо от остальной части сети. Структурированная кабельная система является основой для деления сети на легко управляемые логические сегменты, так как она сама уже разделена на физические сегменты.

5 Обеспечение более эффективного обслуживания. Структурированная кабельная система облегчает обслуживание и поиск неисправностей по сравнению с шинной кабельной системой. При шинной организации кабельной системы отказ одного из устройств или соединительных элементов приводит к трудно локализуемому отказу всей сети. В структурированных кабельных системах отказ одного сегмента не действует на другие, так как объединение сегментов осуществляется с помощью концентраторов. Концентраторы диагностируют и локализуют неисправный участок.

6 Надёжность. Структурированная кабельная система имеет повышенную надёжность, поскольку производитель такой системы гарантирует не только качество её отдельных компонентов, но и их совместимость.

Проект СКС объединяет в себе две подсистемы: горизонтальную и вертикальную (магистральную) кабельную систему. Вертикальная КС подразумевает организацию обмена информацией между распределительными пунктами, которые могут базироваться на разных этажах офиса. В горизонтальную подсистему обычно объединены все абоненты, имеющие доступ к магистральным ресурсам.

6.1 Проектирование горизонтальной кабельной системы

Горизонтальная кабельная система начинается телекоммуникационной розеткой на рабочем месте и заканчивается в телекоммуникационном шкафу этажа (рисунок 30). Она включает в себя розетку, горизонтальный кабель, точки терминирования и патч-корды.

Большинство проектировщиков начинает разработку структурированной кабельной системы с горизонтальных подсистем, так как именно к ним подключаются конечные пользователи. При этом линия связи может быть экранированной витой парой, неэкранированной витой парой, коаксиальным кабелем или беспроводной связью.

Горизонтальная подсистема характеризуется очень большим количеством ответвлений кабеля, так как его нужно провести к каждой пользовательской розетке, причем и в тех комнатах, где пока компьютеры в сеть не объединены. Поэтому к кабелю, используемому в горизонтальной проводке, предъявляются повышенные требования к удобству выполнения ответвлений, а также удобству его прокладки в помещениях. На этаже обычно устанавливается патч-панель, которая позволяет с помощью коротких отрезков кабеля, оснащённого разъёмами, провести перекоммутацию соединений между пользовательским оборудованием и коммутаторами.

Рисунок 30 – Горизонтальная подсистема

При выборе кабеля принимаются во внимание следующие характеристики: полоса пропускания, расстояние, физическая защищённость, электромагнитная помехозащищённость, стоимость. Кроме того, при выборе кабеля нужно учитывать, какая кабельная система уже установлена на предприятии, а также какие тенденции и перспективы существуют на рынке в данный момент (рисунок 31).

В горизонтальной кабельной подсистеме используются кабели следующих типов:

1 Медный провод, в частности, неэкранированная витая пара, является предпочтительной средой для горизонтальной кабельной подсистемы, хотя, если пользователям нужна очень высокая пропускная способность или кабельная система прокладывается в агрессивной среде, для неё подойдёт и волоконно-оптический кабель.

2 Коаксиальный кабель – это устаревшая технология, которую следует избегать, если только она уже широко не используется на предприятии.

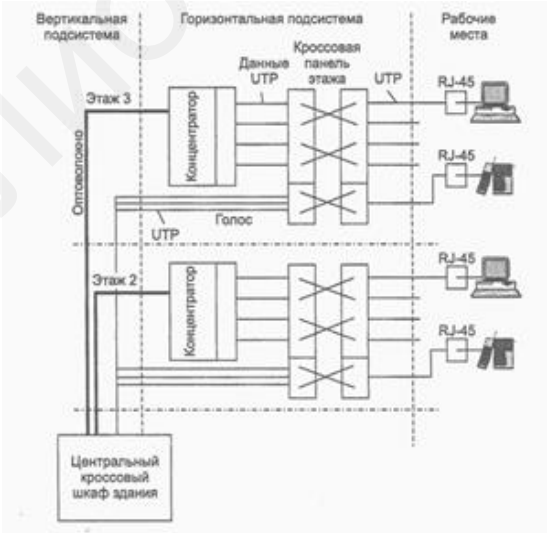


Рисунок 31 – Кабельная система здания

Беспроводная связь является новой и многообещающей технологией, однако из-за сравнительной новизны и низкой помехоустойчивости лучше ограничить масштабы её использования неответственными областями.

Основные области применения оптоволоконного кабеля – вертикальная подсистема и подсистемы кампусов. Однако, если нужна высокая степень защищённости данных, высокая пропускная способность или устойчивость к электромагнитным помехам, волоконно-оптический кабель может использоваться и в горизонтальных подсистемах. Стоимость установки сетей на оптоволоконном кабеле для горизонтальной подсистемы оказывается достаточно высокой. Эта стоимость складывается из стоимости сетевых адаптеров и стоимости монтажных работ, которая в случае оптоволокна гораздо выше, чем при работе с другими видами кабеля.

Преобладающим видом кабеля для горизонтальной подсистемы является неэкранированная витая пара категории 5.

6.2 Проектирование вертикальной кабельной системы

Все кабельные соединения между телекоммуникационными помещениями считаются вертикальными. Во многих случаях вертикальная кабельная структура будет находиться между коммуникационными шкафами в пределах одного этажа здания, но классический случай применения этой системы отображён на рисунке 32, когда вертикальная кабельная система находится между этажами.

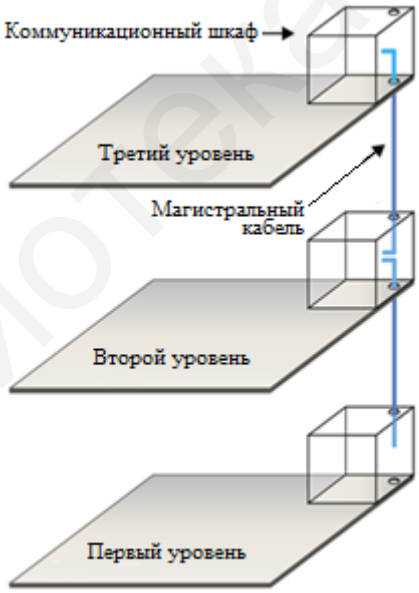


Рисунок 32 – Вертикальная кабельная система

Вертикальная кабельная структура должна быть соединена по тем же принципам, что и горизонтальная. Вертикальный кабель должен принадлежать категории и типу, которые соответствуют требованиям работоспособности системы. Если система требует использования горизонтального кабеля категории 5*e*, можно использовать кабель этой категории для создания вертикальной кабельной структуры, но целесообразнее использовать кабель

более высокой категории, чем нужно, например, категории 6. Если необходимо использовать кабельную систему со многими приложениями, удвойте или утройте каждый канал вертикальной кабельной системы, чтобы повысить возможности её развития для соответствия любым новым требованиям.

При выборе конфигурации и проектировании вертикальной кабельной подсистемы следует принимать во внимание следующие факторы:

– срок службы вертикальной кабельной подсистемы рассчитывается на период от 3 до 10 лет, который значительно меньше срока службы всей кабельной системы (несколько десятилетий);

– к началу планируемого периода кабельная подсистема должна быть спроектирована в максимальном размере, который может потребоваться в течение всего периода планирования; все изменения и расширения кабельной подсистемы в течение этого периода должны проходить без добавления дополнительных кабельных линий;

– затруднён или ограничен доступ к магистральным линиям кабельной системы, что следует учитывать при выборе периода проектирования и монтажа кабельной системы, который будет более продолжительным;

– вертикальные линии кабельной системы должны содержать набор всех типов сред передачи данных, которые могут потребоваться для планируемых приложений;

– при проектировании следует избегать мест возможного расположения источников электромагнитного излучения.

Для использования в вертикальных кабельных подсистемах рекомендуются следующие типы линии связи:

– четырёхпарные кабели на основе неэкранированной витой пары проводников с волновым сопротивлением 100 Ом и рабочими характеристиками категорий 5*e* и 6;

– четырёхпарные кабели на основе экранированной витой пары проводников (*FTP*/*ScTP*/*SFTP*) с волновым сопротивлением 100 Ом и рабочими характеристиками передачи категорий 5*e* и 6;

– многопарные кабели на основе неэкранированной витой пары проводников с волновым сопротивлением 100 Ом и рабочими характеристиками передачи категорий 3 и 5;

– многопарные кабели на основе экранированной витой пары проводников (*FTP*/*ScTP*/*SFTP*) с волновым сопротивлением 100 Ом и рабочими характеристиками передачи категорий 3 и 5;

– многомодовые волоконно-оптические кабели с размерами сердечника/ оболочки 50/125 мкм;

– многомодовые волоконно-оптические кабели с размерами сердечника/ оболочки 62,5/125 мкм;

– одномодовые волоконно-оптические кабели с размерами сердечника/ оболочки 9/125 мкм.

Многопарные кабели на основе витой пары проводников с рабочими характеристиками передачи категорий 3 и 5 предназначены для передачи

сигналов низкоскоростных приложений, таких как аналоговая и цифровая телефония.

Применение волоконно-оптического кабеля в вертикальной подсистеме имеет ряд преимуществ. Он передаёт данные на значительно большие расстояния без необходимости регенерации сигнала. Он имеет сердечник меньшего диаметра, поэтому может быть проложен в более узких местах. Так как передаваемые по нему сигналы являются световыми, а не электрическими, оптоволоконный кабель нечувствителен к электромагнитным и радиочастотным помехам, в отличие от медного коаксиального кабеля. Это делает оптоволоконный кабель идеальной средой передачи данных для промышленных сетей. Оптоволоконный кабель устойчив к воздействию молнии, поэтому он хорош для внешней прокладки. Он обеспечивает более высокую степень защиты от несанкционированного доступа, так как ответвление гораздо легче обнаружить, чем в случае медного кабеля (при ответвлении резко уменьшается интенсивность света).

Оптоволоконный кабель имеет и недостатки. Он дороже, чем медный, дороже стоит и его прокладка. Оптоволоконный кабель менее прочный, чем коаксиальный. Инструменты, применяемые при прокладке и тестировании оптоволоконного кабеля, имеют высокую стоимость и сложны в работе. Присоединение коннекторов к оптоволоконному кабелю требует большого профессионализма и времени, а следовательно, и финансовых затрат.

Телекоммуникационные системы заземления и уравнивания потенциалов, экранирования, защиты от электромагнитных помех (EMI), электромагнитной совместимости (EMC), пиковых напряжений и паразитных токов должны быть спроектированы и установлены в полном соответствии с требованиями нормативных документов.

6.3 Проектирование коммутационных шкафов

В настоящее время организации имеют в своем распоряжении и используют большое количество телекоммуникационного оборудования, которое необходимо где-то разместить и обеспечить определённые условия его функционирования. Для нормальной работы электронного оборудования приходится выделять отдельное телекоммуникационное помещение (рисунок 33).

Телекоммуникационный шкаф – основа для организации коммутационных узлов, объединяющих слаботочную инфраструктуру, активное оборудование и силовую сеть.

Телекоммуникационный шкаф выполняет следующие функции:

– размещения максимального количества пассивного и активного оборудования на минимальной площади;

– распределения в телекоммуникационном помещении большого количества слаботочных кабельных линий, прокладываемых от телекоммуникационных розеток;

– обеспечения защиты оборудования и кабелей от различных внешних воздействий;

– защиты работающего персонала от электромагнитного излучения работающих телекоммуникационных систем.

Рисунок 33 – Серверная

Для осуществления названных функций одним из отраслевых стандартов определено использование 19-дюймовых телекоммуникационных шкафов (рисунок 34). Шкафы стали изначально применяться для установки различного пассивного оборудования (патч-панелей, оптических распределительных панелей, кабельных организаторов), а затем стали использоваться и для монтажа активного оборудования (коммутаторов, маршрутизаторов, источников бесперебойного электропитания, переключателей), серверов, систем хранения данных, системы распределения электроснабжения (*PDU*-блоки, блоки электрических розеток) и другого электронного оборудования.

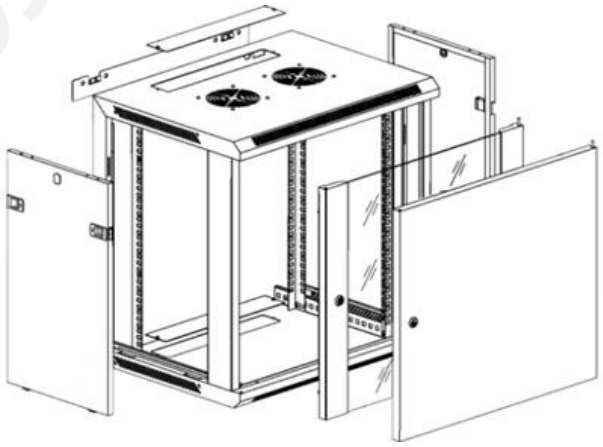


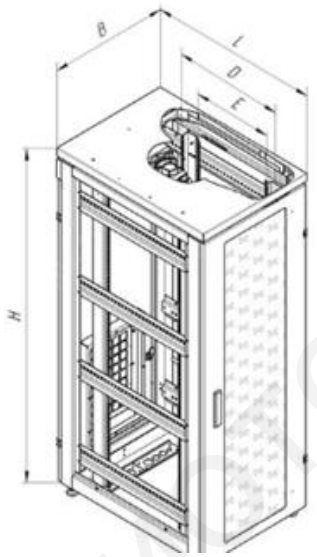
Рисунок 34 – Телекоммуникационный шкаф

19 дюймов (19") – это расстояние между парами направляющих (экструдерами, монтажными рельсами), к которым крепится активное и пассивное оборудование, имеющее стандартное 19-дюймовое крепление.

Телекоммуникационные шкафы значительно упрощают процесс монтажа и установки телекоммуникационного оборудования – один человек может за несколько минут выполнить установку телекоммуникационного оборудования в шкафу 19 дюймов, а при необходимости – демонтаж оборудования. И при этом нет необходимости покупать специальный инструмент и что-то подгонять.

Телекоммуникационный шкаф позволяет защитить устройства от влаги и электромагнитного излучения, а также от проникновения пыли и грязи. Защиту от электромагнитного излучения обеспечивает установка металлической двери и устройство защитного заземления шкафа.

При проектировании и выборе шкафов важно учитывать габаритные размеры: высоту, ширину и глубину (рисунок 35).



Обозначение	B	L	H	D_{max}	E_{max}
NT PROFI plus IP55 42-610	600	1050	2033	870	720
NT PROFI plus IP55 42-68	600	850	2033	670	520
NT PROFI plus IP55 42-66	600	650	2033	470	320
NT PROFI plus IP55 33-610	600	1050	1633	870	720
NT PROFI plus IP55 33-68	600	850	1633	670	520
NT PROFI plus IP55 33-66	600	650	1633	470	320
NT PROFI plus IP55 24-610	600	1050	1233	870	720
NT PROFI plus IP55 24-68	600	850	1233	670	520
NT PROFI plus IP55 24-66	600	650	1233	470	320

Рисунок 35 – Габаритные размеры

По ширине напольные телекоммуникационные шкафы могут быть от 600 до 800 мм.

Для определения высоты шкафов и оборудования, монтируемого в шкафы, используется термин юнит. Ю́нит (обозначение *U*, от англ. – *unit*) – это единица измерения, которая указывает на высоту шкафа и высоту оборудования. Один юнит равен 4,445 см или 1,75 дюйма. Если шкаф имеет высоту 42*u*, то это значит, что в данном монтажном шкафу можно разместить максимально 42 единицы оборудования высотой в 1 юнит или можно установить 21 устройство высотой 2*u*. Чем больше показатель высоты в юнитах, тем больше единиц оборудования можно разместить в монтажном конструктиве.

Еще один важный параметр, используемый для обозначения габаритных размеров, – это глубина шкафа, которая указывается в миллиметрах и варьируется от 450 до 1200 мм.

Зная высоту шкафа, резерв свободного пространства в шкафу и высоту всего монтируемого оборудования в юнитах, путем несложных математических расчетов можно рассчитать количество шкафов, которые потребуется разместить. Для расчета используется следующая формула:

Количество шкафов = ОКРВВЕРХ (суммарное количество юнитов устанавливаемого оборудования / (высота шкафа в юнитах – резерв юнитов)).

Например, если требуется установить оборудование общей высотой 100 юнитов и проектировщик выбирает в качестве решения шкафы высотой 42u, то с учётом резерва 10 юнитов свободного места в каждом шкафу на объекте потребуется четыре телекоммуникационных шкафа:

Количество шкафов = ОКРВВЕРХ (100 / (42 – 10)) = 4.

На стадии проектирования следует определиться и с глубиной шкафа. Глубина шкафа должна быть достаточной для установки оборудования и прокладки кабелей. Кроме того, она должна быть на 150 мм больше глубины монтируемого оборудования, что отмечено в стандарте *TIA*/*EIA*-942. При проектировании необходимо учитывать тот факт, что монтажные рельсы не вплотную примыкают к двери, а монтируются на определённом расстоянии.

Также рекомендуется оставить как минимум 20 %, а желательно не менее 30 % свободного пространства для монтажа дополнительного оборудования, которое потребуется установить в телекоммуникационный шкаф в будущем.

Еще один из вопросов, который возникает перед проектировщиками: как правильно разместить пассивное и активное оборудование в телекоммуникационном шкафу? Большинство структурированных кабельных сетей инсталлируется на одном этаже с использованием в телекоммуникационном помещении одного монтажного шкафа. Поэтому необходимо рассмотреть, как следует установить активное и пассивное оборудование в один телекоммуникационный шкаф или телекоммуникационную стойку.

В верхней части монтажного конструктива устанавливается оборудование с оптическими портами. Так как даже небольшая частица пыли, которая может попасть на поверхность оптоволоконного адаптера, модуля или коннектора, может привести к ухудшению технических параметров кабельной линии и даже к потере соединения, необходимо очень тщательно следить за чистотой волоконно-оптических коннекторов и адаптеров и каждый раз при коммутации не забывать чистить поверхность оптики специальным раствором и специальными салфетками. При установке оборудования с оптоволоконными соединениями сверху уменьшается вероятность запыления оптических модулей. Также уменьшается вероятность повреждения оборудования вследствие падения на них предметов. Поэтому установка оборудования с оптическими портами сверху безопаснее.

Оборудование, используемое в основном для коммутации и подачи телефонных сервисов по многопарному кабелю «витая пара», лучше устанавливать на уровне глаз или чуть пониже, чтобы монтажникам было удобно осуществить расключение витых пар в *IDC*-блоки кроссов, а обслуживающему персоналу – коммутацию витой пары на кроссовом поле.

Патч-панели с портами *RJ*-45, к которым с тыльной стороны подводятся горизонтальные кабели «витая пара», устанавливаются в шкафу обычно в середине.

Телекоммуникационные шкафы рассчитаны на монтаж и установку не только пассивного, но и активного оборудования. Активное оборудование, используемое для организации компьютерной сети, обычно располагается в шкафу ниже патч-панелей.

Желательно не забывать про установку горизонтальных и вертикальных организаторов, размещаемых равномерно между патч-панелями, кроссами и активным оборудованием. Обычно устанавливается как минимум по одному организатору через каждые 2*U* активного и пассивного оборудования, чтобы избежать сильных перегибов патч-кордов (коммутационных шнуров).

Внизу шкафа обычно монтируются источники бесперебойного электропитания (ИБП). Так как это оборудование имеет большой вес, то для придания устойчивости всей собранной конструкции лучше разместить тяжелое оборудование внизу. Чуть повыше ИБП монтируется блок с электрическими розетками, через который обеспечивается распределение электропитания и подключается активное оборудование (рисунок 36).

Рисунок 36 – Телекоммутационный шкаф с установленным оборудованием

Ввод слаботочных и электрических кабелей в телекоммуникационный шкаф можно осуществить сверху или снизу. Гораздо реже ввод кабелей осуществляется сбоку шкафа, однако и этот способ возможен, если использовать для этих целей цоколь.

Наиболее часто используемый на практике способ ввода кабелей осуществляется через крышу. Кабели подводятся сверху, обычно в лотке или коробе, и затем вводятся внутрь шкафа. При этом способе к кабелям нет доступа, и они физически хорошо защищены.

Если в серверном помещении есть фальшполы, то ввод кабелей чаще всего осуществляется снизу.

Гораздо реже на объектах встречается ввод кабелей сбоку и сзади телекоммуникационного шкафа, когда подводится короб и ввод кабелей в шкаф осуществляется через одну из боковых панелей цоколя.

Учитывая требования группы нормативных документов «Правила устройства электроустановок» и североамериканского стандарта *ANSI*/*TIA*/*EIA*-607 «Требования по заземлению и электрическим соединениям телекоммуникационных систем коммерческих зданий» телекоммуникационные шкафы подлежат заземлению как металлические конструкции, которые при пробое изоляции токоведущих частей могут оказаться под напряжением.

Степень защищённости оборудования от пыли и влаги указывается в маркировке телекоммуникационного шкафа в виде кода: *IP***, где буквенное обозначение указывает на то, что защита шкафа от влияния внешней среды существует, а ** – это численное значение, соответствующее определённому уровню защиты.

Чем выше значение *IP*, тем лучше защищённость. Например, для открытых площадок и на улицах необходимо использовать телекоммуникационные шкафы с уровнем защиты не менее *IP*65, а для помещений, в том числе и серверных, вполне достаточно уровня защиты *IP*20.

Современное телекоммуникационное оборудование – серверы, системы хранения данных, коммутаторы – выделяют большое количество тепла. Чтобы обеспечить эффективную систему охлаждения, требуется организовать принудительную систему вентиляции в шкафу. Для организации принудительной вентиляции и большего потока холодного воздуха внутри шкафа с целью охлаждения активного оборудования, а также фильтрации подаваемого в шкаф воздуха, необходимо использовать 19-дюймовые полки (панели) с вентиляторами и потолочные вентиляторные блоки, устанавливаемые сверху под крышей шкафа.

Вентиляторные полки комплектуются вентиляторами и могут устанавливаться на любой высоте при помощи стандартного 19-дюймового крепежа. Существуют полки с различным количеством вентиляторов, в зависимости от необходимой мощности создаваемого внутри шкафа потока воздуха.

7 МОДЕЛИРОВАНИЕ КОМПЬЮТЕРНОЙ СЕТИ

В данном разделе приведены основные команды и сценарии настройки оборудования *Cisco* для программного средства моделирования сети *Cisco Packet Tracer*. В пособии рассмотрено программное средство версии 7.3.

7.1 Базовые команды *IOS*

Рассмотрим базовые команды *IOS*:

Device> enable – вход в привилегированный режим *EXEC*;

Device> ping *{address or domain name}* – отправка эхо-пакета хосту;

Device> traceroute *{address or domain name}* – трассировка маршрута к целевому хосту;

Device# disable – выход из привилегированного режима *EXEC*;

Device# show running-config – просмотр текущих настроек устройства;

Device# show startup-config – просмотр загрузочных настроек устройства;

Device# copy running-config startup-config – сохранение текущих настроек устройства;

Device# write – альтернативная команда сохранения текущих настроек устройства;

Device# configure terminal – вход в режим настройки устройства;

Device(config)# end – выход из режима настройки устройства;

Device(config)# exit – выход из текущего режима устройства;

Device(config)# do *{privileged mode command}* – запуск команды привилегированного режима в режиме настройки устройства.

7.2 Настройка аутентификации *IOS* и отображения сообщения

Для обеспечения безопасного доступа к привилегированному режиму обычно на ввод команды **enable** устанавливается пароль. Для этого в режиме настройки устройства необходимо ввести следующую команду:

Device(config)# enable password *{password}*

В том случае, когда необходимо хранить пароль в настройках в зашифрованном виде, используют команду

Device(config)# enable secret *{password}*

Для обеспечения безопасного доступа к консольному подключению также устанавливают парольное подключение. Для этого необходимо ввести следующие команды:

Device(config)# line console 0
Device(config-line)# password *{password}*
Device(config-line)# login

Шифрование пароля доступа к консольному подключению выполняется командой

Device(config)# service password-encryption

На каждом сетевом устройстве должно быть настроено сообщение, предупреждающее неавторизованных пользователей о том, что доступ запрещен. Его также можно использовать для того, чтобы оставить сообщение сетевым инженерам (например, о запланированном отключении системы или к кому обращаться за получением доступа). Это сообщение называется баннер *MOTD* (*message of the day*) и настраивается следующей командой:

Device(config)# banner motd "Authorized Access Only!"

7.3 Настройка *IPv*4

Для настройки статического *IPv*4-адреса на интерфейсе необходимо прописать следующие команды:

Device(config)# interface gigabitEthernet 0/0 // выбор интерфейса, на котором будет настраиваться *IPv*4 адрес

Device(config-line)# ip address 192.168.1.1 255.255.255.0 // назначение *IPv*4-адреса и маски подсети на выбранный интерфейс

Device(config-line)# exit

В *Cisco Packet Tracer* рядом с обозначенными интерфейсами указываются их адреса (рисунок 37).

Рисунок 37 – Назначение *IPv*4-адреса на оконечном устройстве

Для конфигурации интерфейсов компьютеров необходимо выбрать вкладку *IP Configuration* на *PC*1 и в поле *IP Configuration* прописать *IP Address* и *Default Gateway*. Аналогично настроить *PC*2.

7.4 Настройка *IPv*6

Настройки статического *IPv*6-адреса на интерфейсе производится аналогично *IPv*4-адреса. Рядом с обозначенными интерфейсами указаны их адреса (рисунок 38).

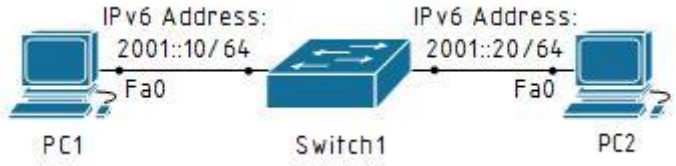


Рисунок 38 – Назначение *IPv*6-адреса на оконечном устройстве

Для конфигурации интерфейсов компьютеров необходимо выбрать вкладку *IP Configuration* на *PC*1 и в поле *IPv*6 *Configuration* прописать *IPv*6 *Address* и *IPv*6 *Gateway*. Аналогично настроить *PC*2.

7.5 Настройка *VLAN*

Рассмотрим настройку виртуальных локальных сетей на примере сети, схема которой приведена на рисунке 39.

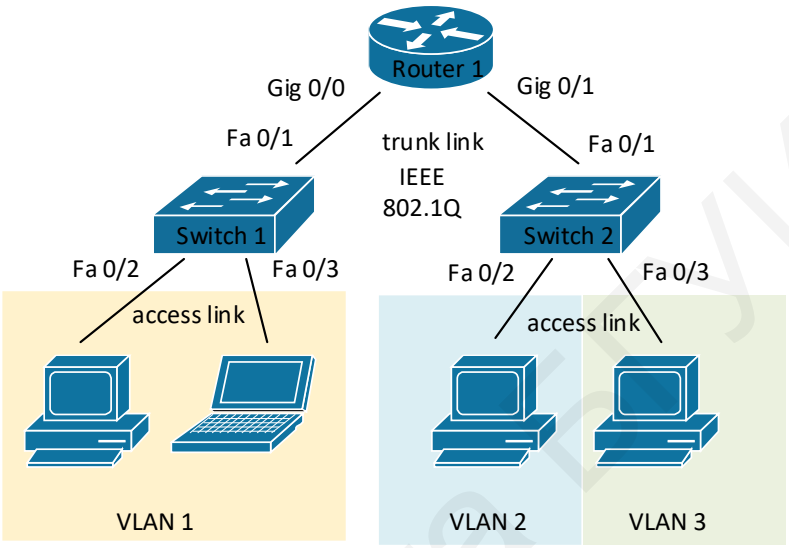


Рисунок 39 – Создание *VLAN* на сетевом оборудовании

Для реализации данной компьютерной сети с технологией виртуальных локальных сетей необходимо прописать на S*witch*1 следующие команды:

S1(config)# interface range fastEthernet 0/2-3 // настройка диапазона интерфейсов
Switch(config-if-range)# switchport mode access // переключение вышеуказанных интерфейсов в режим доступа
Switch(config-if-range)#switchport access vlan 1 // приписывание интерфейсов к *VLAN*1
Switch(config-if-range)#exit
Switch(config)#interface fastEthernet 0/1 // настройка интерфейса
Switch(config-if)#switchport mode trunk // переключение вышеуказанного интерфейса в режим магистрали
Switch(config-if)#exit

На *Switch*2 прописать следующие команды:

Switch>enable
Switch#vlan database // добавление *VLAN*
Switch(vlan)#vlan 2
Switch(vlan)#vlan 3
Switch(vlan)#exit
Switch#configure terminal
Switch(config)#interface fastEthernet 0/1 // настройка интерфейса
Switch(config-if)#switchport mode trunk // переключение в режим магистрали
Switch(config-if)#exit

Switch(config)#interface fastEthernet 0/2 // настройка интерфейса
Switch(config-if-range)#switchport mode access // переключение в режим доступа
Switch(config-if-range)#switchport access vlan 2 // приписывание интерфейса к *VLAN*2
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/3 // настройка интерфейса
Switch(config-if-range)#switchport mode access // переключение в режим доступа
Switch(config-if-range)#switchport access vlan 3 // приписывание интерфейса к *VLAN*3
Switch(config-if)#exit

На *Router*1 выполнить следующие команды:

Router>enable
Router#vlan database // добавление *VLANs*
Router(vlan)#vlan 1
Router(vlan)#vlan 2
Router(vlan)#vlan 3
Router(vlan)#exit
Router#configure terminal
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#no shutdown // включение интерфейса
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#no shutdown // включение интерфейса
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/0.1 // разбиение на подынтерфейсы
Router(config-subif)#encapsulation dot1Q 1
Router(config-subif)#ip address 192.168.1.10 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/1.2 // разбиение на подынтерфейсы
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 192.168.2.10 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gigabitEthernet 0/1.3 // разбиение на подынтерфейсы
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 192.168.3.10 255.255.255.0
Router(config-subif)#exit
Router(config)#router rip // динамическая маршрутизация
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0

7.6 Настройка *VTP*

Настроим протокол *VTP* на коммутаторах. Режимы работы протокола указаны в скобках под изображениями коммутаторов (рисунок 40).

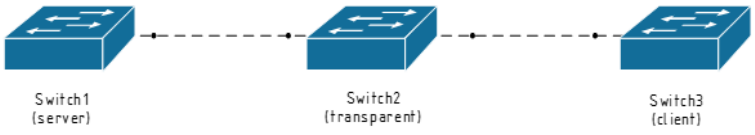


Рисунок 40 – Настройка *VTP*-протокола

Сначала переведём порты, соединяющие коммутаторы, в режим *trunk.* Для этого необходимо на каждом коммутаторе выполнить следующие команды:

Switch>enable
Switch# configure terminal
Switch(config)# interface gigabitEthernet 0/N // *N* **–** номер интерфейса
Switch(config-if)#switchport mode trunk

Теперь настроим *VTP* на коммутаторах. Первые строки настройки будут одинаковы для всех коммутаторов:

Switch>enable
Switch# configure terminal
Switch(config)#vtp version 2 // включаем протокол *VTP*

Дальнейшая настройка будет зависеть от режима работы, который необходимо настроить. Для режима *Server* это будет выглядеть следующим образом:

Switch(config)#vtp mode server
Switch(config)#vtp domain main // создаём домен
Switch(config)#password main // устанавливаем пароль
Для режима transparent:
Switch(config)#vtp mode transparent
Switch(config)#vtp domain main
Switch(config)#password main

Для режима *client*:

Switch(config)#vtp mode client
Switch(config)#vtp domain main
Switch(config)#password main

Теперь создаём *VLAN* на первом и втором коммутаторах:
Switch 1:

Switch(config)#vlan 3
Switch(config-vlan)#name vlan3

Switch 2:

Switch(config)#vlan 2
Switch(config-vlan)#name vlan2

Теперь можем проверить настроенные *VLAN* на коммутаторах через команду *show vlan*. На коммутаторах 1 и 3 будет *VLAN*2, а на коммутаторе 2 – *VLAN*3.

7.7 Настройка *EtherChannel*

Рассмотрим пример объединения нескольких физических интерфейсов в один логический на примере схемы, представленной на рисунке 41.

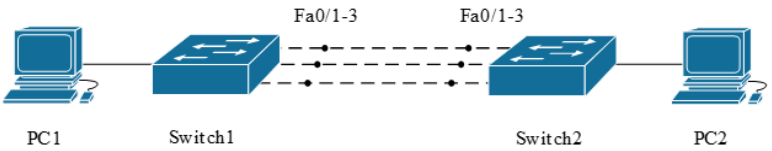


Рисунок 41 – Объединения нескольких физических интерфейсов в один логический

Для этого необходимо привести конфигурацию *Switch*1 и *Switch*2. Команды на каждом *Switch* в *CLI* будут одинаковыми:

```
Router>enable
Router#configure terminal
Switch(config)#interface range fastEthernet 0/1-3
Switch(config-if-range)#shutdown
Switch(config-if-range)#channel-group 1 mode on
```

Этими командами назначается диапазон интерфейсов, начиная с *fastEthernet* 0/1 до *fastEthernet* 0/3 *в port-channel* с номером 1.

7.8 Настройка *STP*

Настраивать коммутаторы в пределах одной *VLAN* необходимо таким образом, чтобы избежать образования петель (рисунок 42).

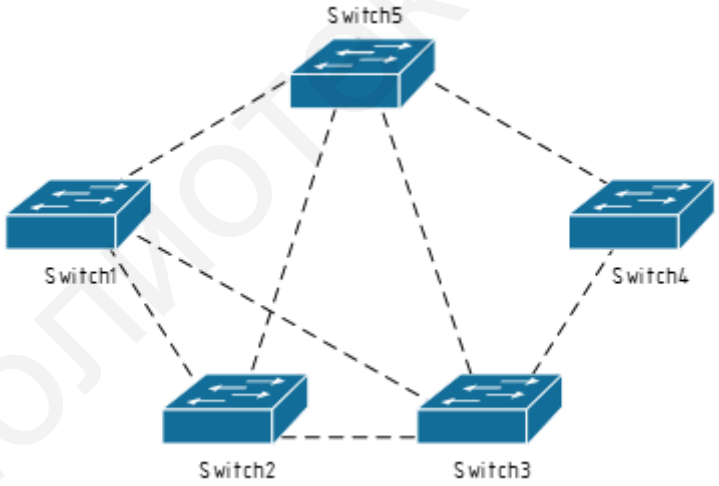


Рисунок 42 – Работа протокола *STP*

Для этого необходимо задать приоритет коммутатора. Этот параметр определяет выбор *root bridge*. Приоритет может принимать значение от 0 до 61 440 с шагом 4096. Значение по умолчанию 32 768. Настройка приоритета может иметь вид

```
Switch(config)#spanning-tree vlan 1 priority 24576
```

Также можно напрямую назначить коммутатор на роль основного или вторичного *root bridge*. При этом значение *priority* будет выставлено меньшим, чем у нынешнего *root bridge*.

Настройка основного *root bridge*:

Switch(config)#spanning-tree vlan 1 root primary

Настройка вторичного *root bridge*:

Switch(config)#spanning-tree vlan 1 root secondary

Приоритет интерфейса необходим для определения кратчайшего пути к *root bridge*. Можно настроить приоритет использования линий связи. Приоритет интерфейса может принимать значение от 0 до 240 с шагом 16. Значение по умолчанию 128. Настройка может иметь вид

Switch(config-if)#spanning-tree vlan 1 port-priority 240

7.9 Настройка *RSTP*

Начальные настройки *STP* осуществляются согласно подразделу 7.8. После на коммутаторе *root bridge* включить *RSTP*:

Switch>enable
Switch#configure terminal
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#exit

Данный протокол нужен для того, чтобы при выходе из строя кабеля, находящегося между роутерами, сходимость сети происходила почти мгновенно (потеря пакетов при передаче была минимальной).

7.10 Настройка *Telnet*

Рассмотрим настройку удалённого доступа по протоколу *Telnet* на примере сети, схема которой изображена на рисунке 43.

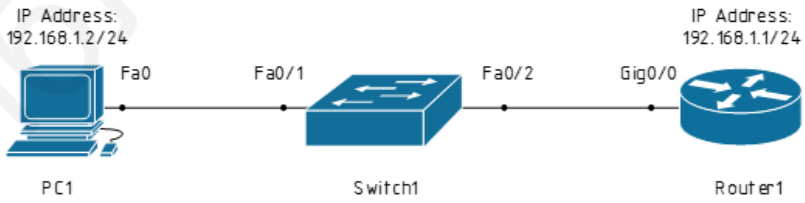


Рисунок 43 – Настройка уделённого доступа по протоколу *Telnet*

Рядом с интерфейсами указаны их *IP*-адреса. Интерфейсы сконфигурировать самостоятельно (см. подраздел 7.3).

Затем прописываются следующие команды на *Router*1:

Router>enable
Router#configure terminal

Router(config)#line vty 0 14 // диапазон значений, присваиваемых каждой активной сессии

Router(config-line)#login local
Router(config-line)#password telnet12
Router(config-line)#privilege level 15 // уровень полномочий
Router(config-line)#exit
Router(config)#username cisco privilege 15 password cisco12
Router(config)#end

7.11 Настройка *SSH*-доступа

Для безопасного управления удалёнными подключениями рекомендуется заменить протокол *Telnet* на протокол *SSH*, который обеспечивает защиту удалённых подключений, предоставляя надёжное шифрование данных аутентификации устройства (имя пользователя и пароль). Для настройки протокола удалённого доступа *SSH* используется следующая последовательность команд:

Router>enable
Router#configure terminal
Router(config)#hostname router
Router(config)#ip domain name bsuir.by // имя домена
Router(config)#crypto key generate rsa // генерирование *RSA*-ключа
Router(config)#service password-encryption // шифрование паролей в конфигурационном файле
Router(config)#username student privilege 15 password student // создание пользователя с именем s*tudent*, паролем *student* и уровнем привилегий 15
Router(config)#aaa new-model // активация протокола *AAA*
Router(config)#line vty 0 4 // вход в режим конфигурирования терминальных линий с 0 по 4
Router(config-line)#transport input ssh // указывается среда доступа через сеть по умолчанию *SSH*
Router(config-line)#logging synchronous // активация автоматического поднятия строки после ответа системы на проделанные изменения
Router(config-line)#exec-timeout 60 0 // указываетя время тайм-аута до автоматического закрытия *SSH*-сессии в 60 минут
Router(config-line)#exit
Router(config)# exit

7.12 Настройка статической маршрутизации *IPv*4

Настройка статической *IPv*4 маршрутизации будет рассмотрена на примере сети, схема которой изображена на рисунке 44.

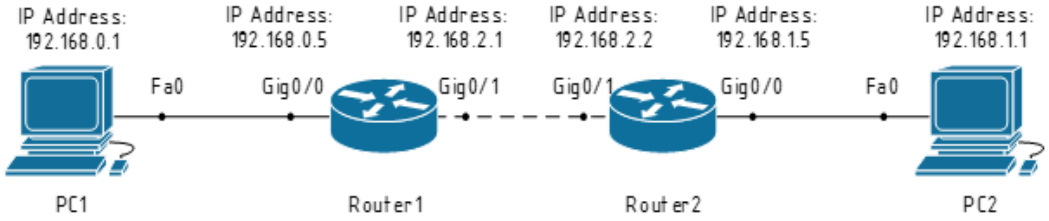


Рисунок 44 – Настройка статической маршрутизации для протокола *IPv*4

Рядом с интерфейсами указаны их *IP*-адреса. Интерфейсы необходимо сконфигурировать самостоятельно (см. подраздел 7.3).

Для настройки статического маршрута между сетями следует на каждом роутере указать *IP*-адрес интерфейса, на который необходимо пересылать пакеты данной сети. Для *Router*1 эти строки будут выглядеть следующим образом:

```
Router>enable
Router#configure terminal
Router(config)#ip route 192.168.0.0 255.255.255.0 192.168.2.2
Router(config)#exit
```

Аналогично, пользуясь рисунком, можно сконфигурировать *Router*2.

7.13 Настройка статической маршрутизации *IPv*6

Настройка статической *IPv*6 маршрутизации будет рассмотрена на примере сети, схема которой изображена на рисунке 45.

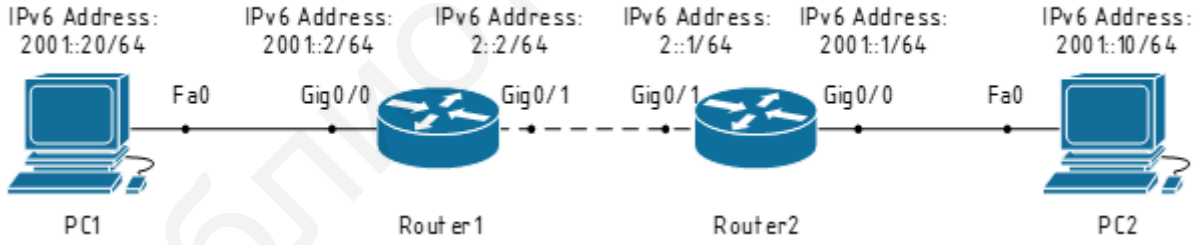


Рисунок 45 – Настройка статической маршрутизации для протокола *IPv*6

Рядом с интерфейсами указаны их *IP*-адреса. Интерфейсы необходимо сконфигурировать самостоятельно (см. подраздел 7.4).

Перед выбором интерфейса роутера и его последующего конфигурирования необходимо включить протокол *IPv*6:

```
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing // включение протокола IPv6
```

Для настройки статического маршрута между сетями следует на каждом роутере указать *IP*-адрес интерфейса, на который необходимо пересылать пакеты данной сети.

Для *Router*1 эти настройки будут выглядеть так:

```
Router>enable
Router#configure terminal
Router(config)#ipv6 route 2001::0/64 2::1
Router(config)#exit
```

Аналогично, пользуясь рисунком, можно сконфигурировать *Router*2.

7.14 Настройка стандартных и расширенных *ACL*

Настройка *access-list* будет рассмотрена на примере простейшей сети, схема которой изображена на рисунке 46.

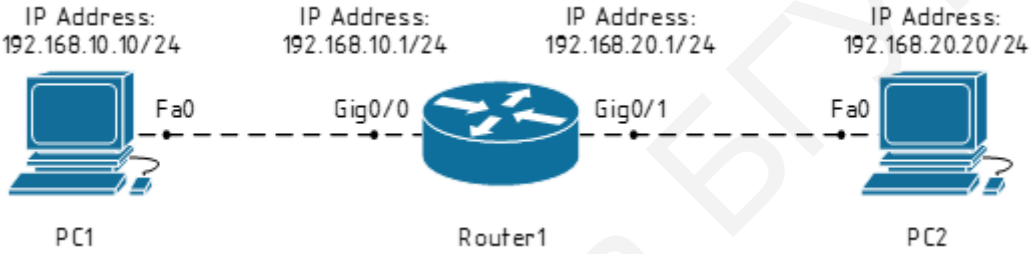


Рисунок 46 – Настройка *access-list*

Базовая настройка интерфейсов роутера и компьютеров была рассмотрена в подразделе 7.3. Для настройки стандартного *access-lista* используется следующая последовательность команд:

```
Router>enable
Router#configure terminal
```

Router(config)#access-list 1 deny host 192.168.10.10 // инструкция, запрещающая пересылку трафика от ПК с адресом 192.168.10.10\24

Router# interface gigabitEthernet 0/0 access-group 1 in // назначение инструкции на входящий интерфейс *Router*1

```
Router(config)#exit
```

Аналогичным образом создаются инструкции для расширенных *ACL*-списков, разница только в том, что для создания стандартного *ACL*-списка используются номера инструкций от 1 до 99, для расширенных – от 100 до 199. С технической стороны разница между стандартными и расширенными *ACL*-списками заключается в следующем: стандартные *ACL* фильтруют трафик только по *IP*-адресу отправителя, расширенные *ACL* фильтруют трафик по четырём параметрам (*IP*-адрес отправителя/получателя, протокол и номер порта). Пример создания расширенного списка представлен ниже.

```
Router>enable
Router#configure terminal
```

Router(config)#access-list 100 deny tcp 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 eq 80 // инструкция, запрещающая пересылку/перенаправление трафика по протоколу *tcp* от сети 192.168.20.0 255.255.255.0 к 192.168.10.0 255.255.255.0 и номеру порта, равному 80

Router# interface gigabitEthernet 0/1 access-group 1 in // назначение инструкции на входящий интерфейс *Router*2

Router(config)#exit

7.15 Настройка *DHCP*

Настройка *DHCP* будет рассмотрена на примере простейшей сети, схема которой расположена на рисунке 47.

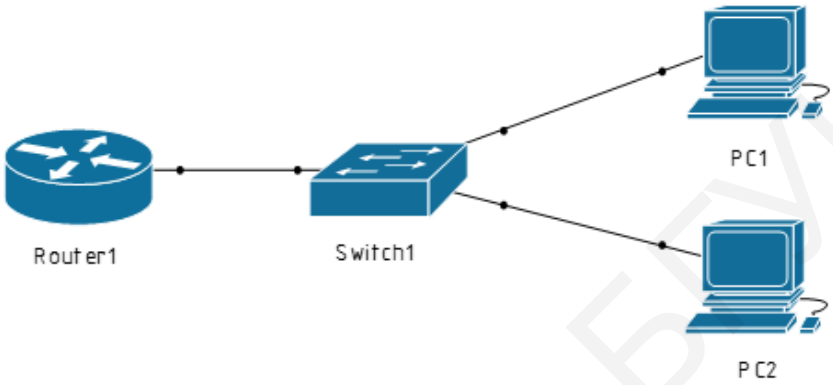


Рисунок 47 – Настройка *DHCP*

Базовая настройка интерфейсов роутера и компьютеров была рассмотрена в подразделе 7.3. Для настройки *DHCP* необходимо прописать на *Router*1 следующие команды:

Router>enable

Router#configure terminal

Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10 // исключаем указанный диапазон адресов из пула

Router(config)#ip dhcp pool MY-POOL

Router(dhcp-config)#network 192.168.1.0 255.255.255.0 // указываем сеть, адреса которой будут выдаваться (кроме исключённых ранее)

Router(dhcp-config)#default-router 192.168.1.1 // в качестве шлюза указываем роутер

7.16 Настройка статического *NAT*

Рассмотрим реализацию статического *NAT* на примере сети, схема которой изображена на рисунке 48. Настроим *Router*1 таким образом, чтобы пакеты, исходящие от *PC*1, приходили на *PC*2 с *IP*-адресом, отличным от *IP*-адреса *PC*1.

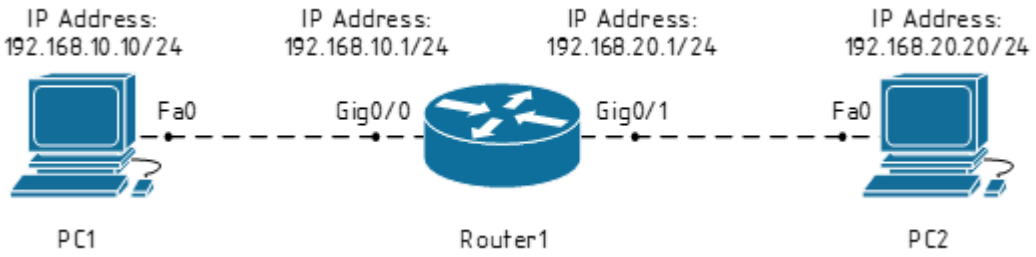


Рисунок 48 – Схема для настройки *NAT*

Рядом с интерфейсами указаны их *IP*-адреса. Конфигурацию интерфейсов необходимо выполнить самостоятельно (см. подраздел 7.3). Базовая настройка интерфейсов роутера и компьютеров была рассмотрена в подразделах 7.3 и 7.12. Для настройки статического *NAT* необходимо прописать на *Router*1 следующие команды:

Router>enable
Router#configure terminal
Router(config) #interface gigabitEthernet 0/0 // выбор интерфейса
Router(config-if) #ip nat inside // назначение его внутренним интерфейсом
Router(config-if) #interface gigabitEthernet 0/1 // выбор интерфейса
Router(config-if) #ip nat outside // назначение его внешним интерфейсом
Router(config-if) #ip nat inside source static 192.168.10.10 100.100.100.100 // настройка статического *NAT*
Router(config) #exit

При настройке статического *NAT* необходимо указать *IP*-адрес пакетов, который будет преобразован, и новый *IP*-адрес для этих пакетов. Второй вариант настройки статического *NAT* предполагает, что необходимо указать *IP*-адреса интерфейса, исходящие пакеты которого будут транслироваться с изменённым *IP*-адресом, и новый *IP*-адрес для этих пакетов.

7.17 Настройка *Port Security*

Рассмотрим пример реализации фильтрации по *MAC*-адресам при помощи функции *Port Security* на примере сети, схема которой представлена на рисунке 49.

Рисунок 49 – Схема для настройки *NAT*

Для начала рассмотрим пример реализации фильтрации по количеству. Для этого необходимо прописать на *Switch*1 следующие команды:

Switch>enable
Switch#configure terminal
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport mode access
Switch(config-if)#switchport voice vlan 2
Switch(config-if)#switchport port-security // включение *Port Security* на интерфейсе
Switch(config-if)#switchport port-security maximum 2 // ограничение количества *MAC*-адресов для одновременного подключения к интерфейсу
Router(config-if)#switchport port-security violation restrict

Последняя строка указывает режим реагирования на нарушение. Если на данном интерфейсе одновременно «засветится» третий (неизвестный) *MAC*-адрес, то все пакеты с этого адреса будут отбрасываться.

Существует три команды реагирования на нарушение безопасности:

switchport port-security violation restrict
switchport port-security violation shutdown
switchport port-security violation protect

Команда **switchport port-security violation restrict** описана выше.

Вторая команда – **switchport port-security violation shutdown** – при выявлении нарушений переводит интерфейс в состояние *error-disabled* и выключает его. При этом отправляется оповещение *SNMP trap*, сообщение *syslog* и увеличивается счётчик нарушений (*violation counter*).

Если же на интерфейсе введена команда **switchport port-security violation protect**, то при нарушениях от неизвестного *MAC*-адреса пакеты отбрасываются, но при этом никакие сообщения об ошибках не генерируются.

Также можно реализовать фильтрацию по *MAC*-адресам, введя их статически. Для этого на *Switch*1 нужно прописать команды, рассмотренные выше, а затем добавить:

Switch(config-if)#switchport port-security mac-address 0003.E40E.A002
Switch(config-if)#switchport port-security mac-address 00E0.F75B.C101

Теперь только от этих двух указанных *MAC*-адресов на данный интерфейс будут разрешены входящие пакеты.

Фильтрацию по *MAC*-адресам можно настроить с использованием *Sticky MAC*. Для этого вместо предыдущих команд нужно добавить следующие:

Switch(config-if)#switchport port-security mac-address 0003.E40E.A002
Switch(config-if)#switchport port-security mac-address sticky

Также отличительной строкой станет

Switch(config-if)#switchport port-security maximum

В этом случае был сконфигурирован один *MAC*-адрес статически (**switchport port-security mac-address 0003.E40E.A002**), а все остальные *MAC*-адреса (в нашем случае ещё один) будут выучены динамически, после записаны в память коммутатора (**switchport port-security mac-address sticky**).

Св. план 2019, поз. 3

Учебное издание

Шнейдеров Евгений Николаевич
Фещенко Артём Александрович
Боровиков Сергей Максимович

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

ПОСОБИЕ

Редактор *М. А. Зайцева*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *В. М. Задоля*

Подписано в печать 20.06.2022. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 4,19. Уч.-изд. л. 4,5. Тираж 50 экз. Заказ 375.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск