СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Проектирование сети

СПбГЭТУ «ЛЭТИ», 2021 г.

1. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ СЕТЕЙ. ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННОЙ КОМПЬЮТЕРНОЙ СЕТИ

Цель работы: изучение теоретического материала необходимого для построения сетевой инфраструктуры, получение практических навыков настройки сетей, основанных на технологии виртуальных сетей с использованием коммутаторов Cisco.

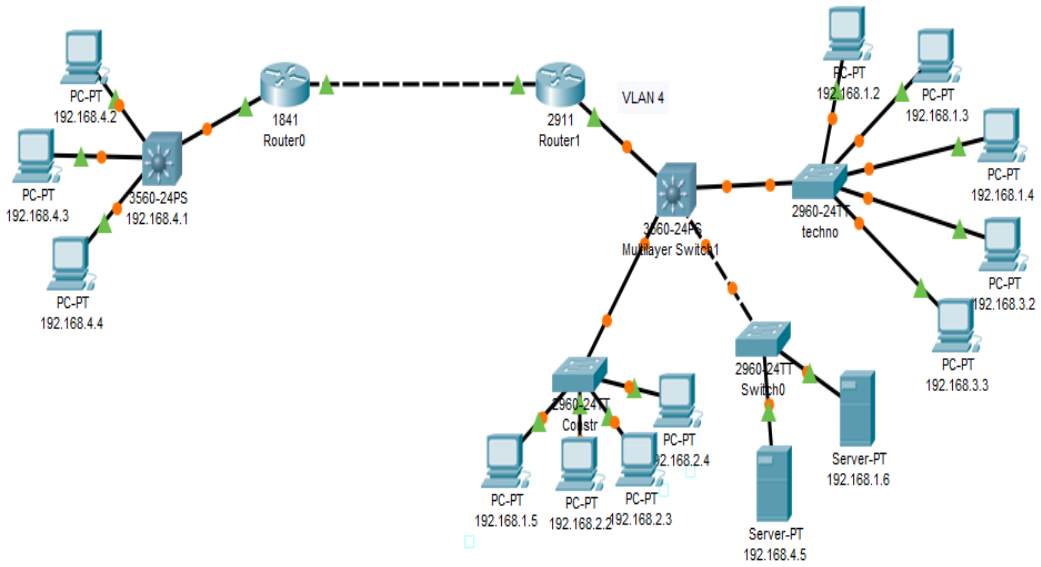
1.1 Общие сведения

Сетевая инфраструктура включает в себя три категории компонентов сети (рис. 1.1.):

-устройства (хосты);

-средства подключения (сетевые платы, кабель);

-сервисы (предоставляемые услуги);



- Рис. 1.1

• *Сетевая интерфейсная плата* (Network Interface Card, NIC) — интерфейсная плата или адаптер сети LAN, который обеспечивает физическое подключение к сети на настольном компьютере или другом устройстве. Средство подключения, соединяющее компьютер с сетевым устройством, подключается непосредственно к сетевой плате.

• *Физический порт* — разъем на сетевом устройстве, через который кабели подключены к компьютеру или другому сетевому устройству.

• *Интерфейс* — специализированные порты в сетевом устройстве, которые подключаются к отдельным сетям. Поскольку маршрутизаторы используются для связывания сетей, порты маршрутизатора называются сетевыми интерфейсами.

Термины «порт» и «интерфейс» часто взаимозаменяемы. Для объединения устройств в сетевую инфраструктуру используют три основных вида устройств:

Концентратор – устройство для объединения конечных физических узлов сети в единую разделяемую среду в соответствии с принятым в данной сети протоколом:

- позволяет осуществлять разделение сети на подсети;
- не осуществляет фильтрацию трафика;
- использует первые уровни модели OSI (L1, L2) отправляет пакеты во все порты, кроме порта источника;

Использование концентраторов дает следующие преимущества:

- при разрыве кабеля в сети, подключенного к концентратору, нарушается работа только данного сегмента. Остальные сегменты остаются работоспособными;
- простота масштабирования сети при подключении новых компьютеров или концентраторов;

Коммутатор- устройство, соединяющее 2 и более сети, с одним и тем же протоколом и обрабатывающий кадры параллельно. Каждый из портов коммутатора обслуживается собственным процессором, системным модулем, имеющим общую адресную таблицу и коммутационной матрицей.

Применяет второй уровень модели OSI (L2) отправляет пакет только в определенный порт за счет использования таблицы MAC – адресов.

Общая схема работы коммутатора выглядит следующим образом:

1. Прием первых байт кадра процессором входного порта.
2. Просмотр адресной таблицы процесса для определения порта передачи. В случае отсутствия записи обращение к таблице системного модуля, обслуживающего запросы всех процессоров коммутатора.
3. Обращение к коммутационной матрицы и соединение своего порта с портом, через который следует маршрут адреса назначения.

4. Получение доступа к среде передачи процессором выходного порта и передача кадров в сеть.

Для передачи кадров между портами коммутатора в качестве базовой производители коммутаторов используют одну из 3 схем:

- ***коммутационная матрица*** -входной блок процессора порта на основании просмотра адресной таблицы определяет по адресу назначения номер выходного порта. Эта информация добавляется к исходному кадру в виде ярлыка, на основании которого коммутационная матрица, состоящая из переключателей, соединяет входной порт с выходным портом.;
- ***коммутаторы с общей шиной***- входной блок процессора порта помещает в кадр номер порта назначения. Каждый выходной блок процессора содержит фильтр, выбирающий кадры, предназначенные данному порту;
- ***коммутаторы с разделяемой памятью***. Входной блок процессора порта соединяется с выходным через разделяемую память, в которой организована очередь. Входные порты записывают данные в очередь разделяемой памяти порта, соответствующего адресу назначения. По мере заполнения очереди производится поочередное подключение выхода разделяемой памяти к выходным портам.

Маршрутизатор–устройство, использующее одну и более метрик для определения оптимального пути передачи сетевого трафика на основе информации, полученной из заголовков сетевого уровня.

На все три категории распространяются различные сетевые атаки, в том числе:

1. Недостаточная идентификация объектов и субъектов сети или «слабые» алгоритмы аутентификации.

2. Взаимодействие объектов без установления виртуального канала связи или отсутствия контроля над пакетами, передающимися в сети.

3. Отсутствие возможности контроля за маршрутом сообщений.

4. Отсутствие полной информации о ее объектах.

5. Отсутствие криптозащиты сообщений.

Для устранения данных причин необходимо на стадии проектирования рассмотреть весь возможный набор угроз и уязвимостей сетевой

инфраструктуры и сформировать модель угроз, с учетом которой осуществить проектирование сети [1].

Этапы проектирования сетевой инфраструктуры:

1. ***Определение зон подключения*** и периметра удаленности сетей друг от друга с необходимостью обеспечения доступа к серверам, а также сетям провайдера.
2. ***Определение групп пользователей и их ролей при использовании сетевой инфраструктур*** позволяет сформировать перечень возможных угроз со стороны внутренних пользователей, оценить риски и возможные механизмы для предотвращения атак. Например, имеется четыре группы пользователей: бухгалтерия, финансово-экономический отдел, кадров, объединенных в одну группу, находящиеся на одной площадке и производственно-технический отдел, технологический и технологический отдел, находящиеся на другой площадке. Все группы разграничены и не имеют прямого доступа друг к другу.
3. ***Определение необходимого оборудования***, каналов связи, интерфейсов для организации доступа к сетевой инфраструктуре. и связано с оценкой категорией информации, которую необходимо передать по сети и учетом модели угроз [1-15]. Например, необходимо передать сведения содержащие персональные данные, в этом случае необходимо выяснить к какой категории будет относится информация и какое оборудование, а также программно-аппаратные средства необходимы для передачи информации по сети и подключению к абонентному каналу связи [1-15].

При определении сетевой инфраструктуры следует:

- придерживаться иерархической модели сети, которая имеет много достоинств по сравнению с “плоской сетью”;
- оценить модульность и возможность масштабируемости сетевой инфраструктуры;
- предусмотреть отказоустойчивость за счет дублирования устройств и/или соединений и/или реконфигурации;
- сформировать распределение функций по обеспечению работоспособности сети по различным устройствам и резервированию.

Произвести предварительную оценку

- стоимости;
- скорости и типов подключаемых портов;
- функции и сервисы операционной системы;
- возможную IP-адресацию планируемой сетевой инфраструктуры.

4. ***Согласование проекта сетевой инфраструктуры***. Согласование может быть как на уровне предприятия, так и на более высоком уровне.
5. ***Разработка политики безопасности при передаче информации***. При этом если передача осуществляется на удаленные площадки, то возникает необходимость гармонизации политик безопасности, так как нарушение в одной подсети может привести к лавинообразному нарушений все сети организации.
6. ***Разработка документации на сеть***. Вся сеть должна быть строго документирована: от принципиальной схемы, до имени интерфейса. При этом целесообразно сформировать проект сети, содержащий:
   6.1 Титульный лист;
   6.2 Оглавление;
   6.3 Пояснительная записка;
   6.4 Схема прокладки кабельных трасс (ЛВС, ВОЛС);
   6.5 Схем расположения и состава рабочих мест;
   6.6 Схема расположения оборудования и проводок;
   6.7 Таблица кабельных соединений (Кабельный журнал);
   6.8 Схема монтажа и размещения оборудования в коммутационных шкафах и помещениях;
   6.9 Структурная схема СКС, отражающая коммутацию портов и кроссового оборудования;
   6.10 Протокол тестирования СКС (по требованию заказчика, для проведения сертификации СКС);
   6.11 Руководство по эксплуатации СКС. (по требованию заказчика, содержит рекомендации по поддержанию работоспособного состояния СКС, перечень и сроки гарантийного и сервисного обслуживания).
   6.12 Политика безопасности;

6.13 Другие документы, предусматривающие аттестацию объекта [1-15].

1.2 Задание

Подготовить структурную схему сети и назначить IP-адреса всем устройствам сети:

- дать понятные названия всем устройствам сети;
- составить таблицу статических и динамических VLAN;
- составить план IP адресации выделив диапазон адресов для каждого из VLAN;
- составить таблицу портов подключенного оборудования.

1.3 Порядок выполнения работы

Выполнить первоначальное проектирование сети согласно исходным данным проектируемой сети, используя данные в таблице 1.

Таблица 1

Параметр	*Значение*
Тип организации сети	клиент-сервер
Адресация IP	по классу С
Количество VLAN	8
Минимальное количество узлов в каждой VLAN	2
Начальный IP адрес	192.168.0.0/16
Маска для проектируемой сети	255.255.0.0

1.3.1. Разработка *структурной схемы сети*

Техническое задание состоит из проектировки, разработки и настройки сети организации. Проект здания содержит:

1. Количество корпусов:1
2. Количество комнат:12
3. Количество конечных устройств:40
4. Количество промежуточных устройств:12

В помещении, предназначенном для размещения серверного оборудования, находится два сервера и маршрутизатор. Один сервер отвечает за работу административных служб, а другой сервер отвечает за работу диспетчерской и охранной систем.

В автоматизированной сети (АС) имеется 24 узла выполняющих функции рабочих станций. Рабочие станции распределены по кабинетам. Коммутаторы обеспечивают связь между отделами. Маршрутизатор обеспечивает связь к серверам.

На представленной схеме (рис.1.2) ядром информационной сети (Core) будет маршрутизатор Router 3, а коммутатор Multilayer Switch0 относится к уровню распространения (Distribution), поскольку на нём агрегируются все VLAN в общий транкинг. Коммутаторы Cisco 2960 будут устройствами доступа (Access). К ним будут подключаться конечные пользователи, офисная техника, сервера.

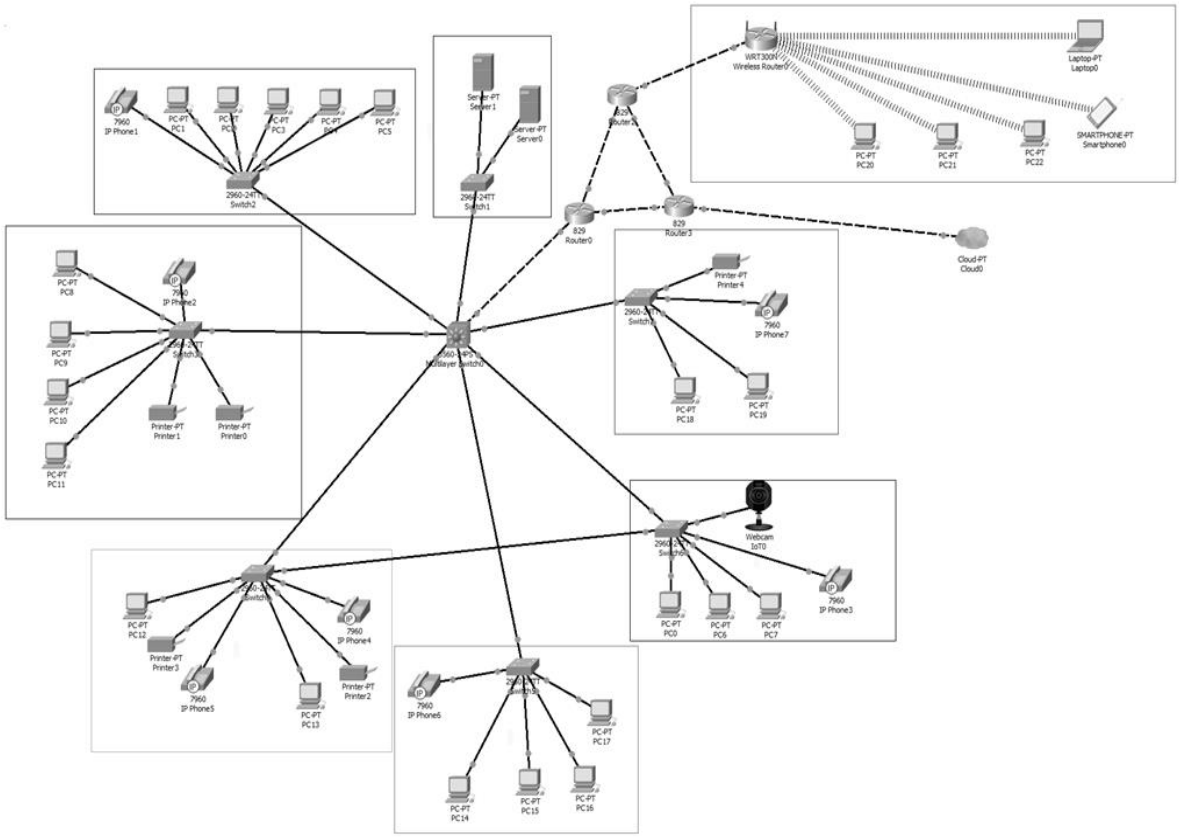


Рис. 2.2 Структурная схема проектируемой сети уровня L-1, L-2, L-3

На схеме, отражающей подключения на канальном уровне L1 указать физические устройства сети с номерами портов и подключением к ним.

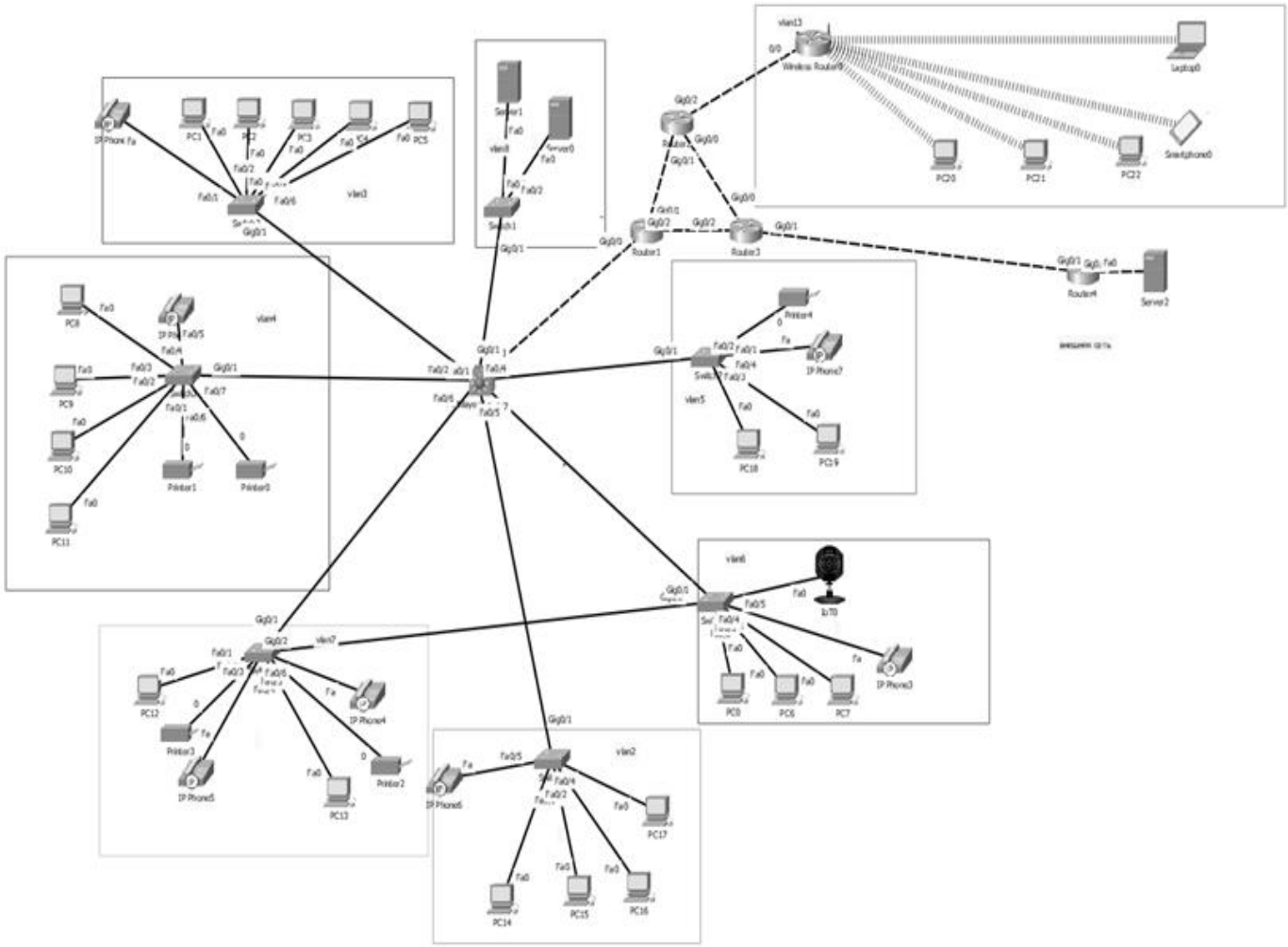


Рис. 3. 3 Схема уровня L1

На схеме, отражающей подключения на канальном уровне L2 указать VLAN-ы, подключенные к сети.

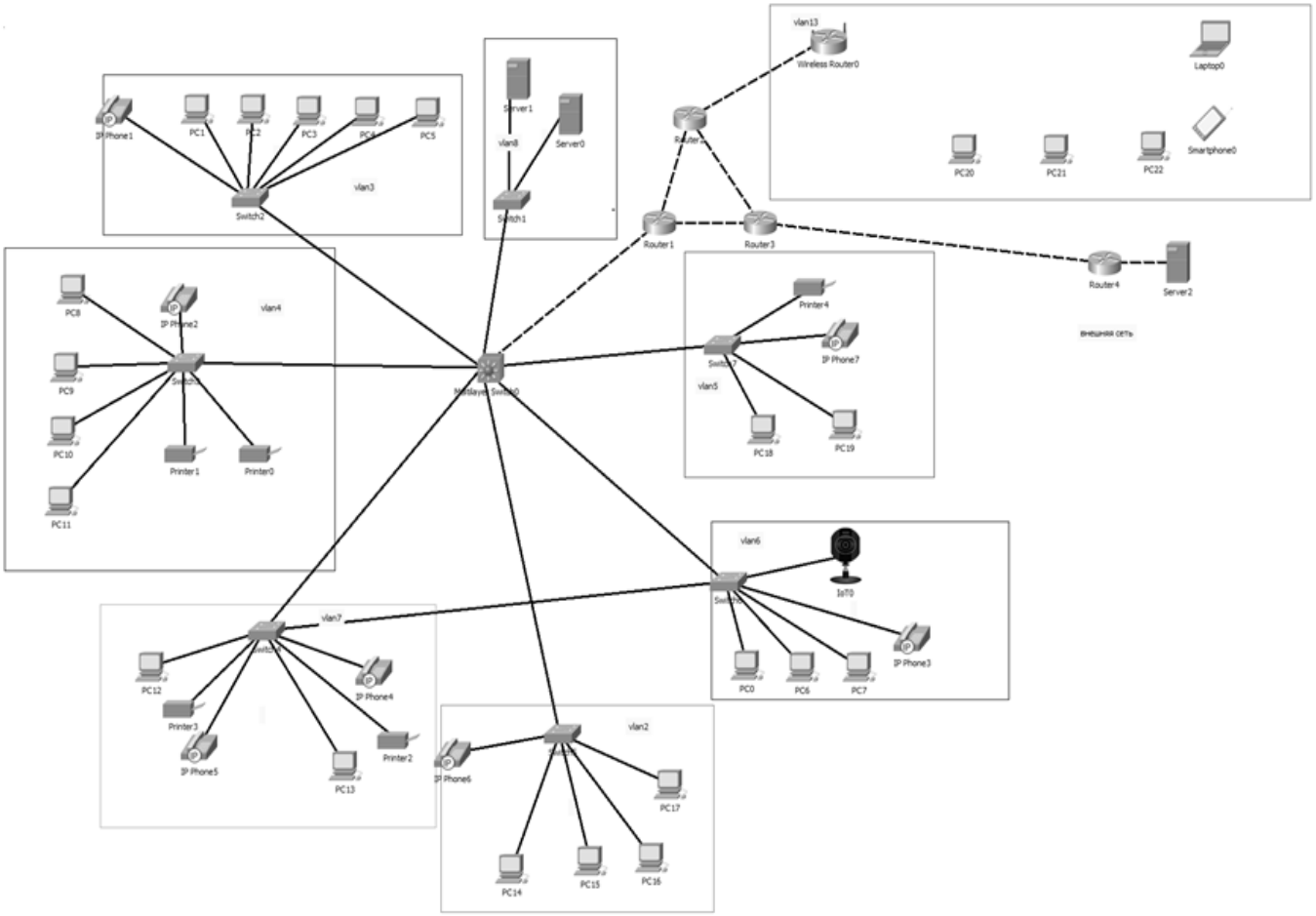


Рис. 1.4. Схема уровня L2

На схеме, отражающей подключения на сетевом уровне L3-схемы отразить следующую информацию:

- подсети (VLAN ID, названия VLAN, сетевые адреса и маски);
- L3-устройства.

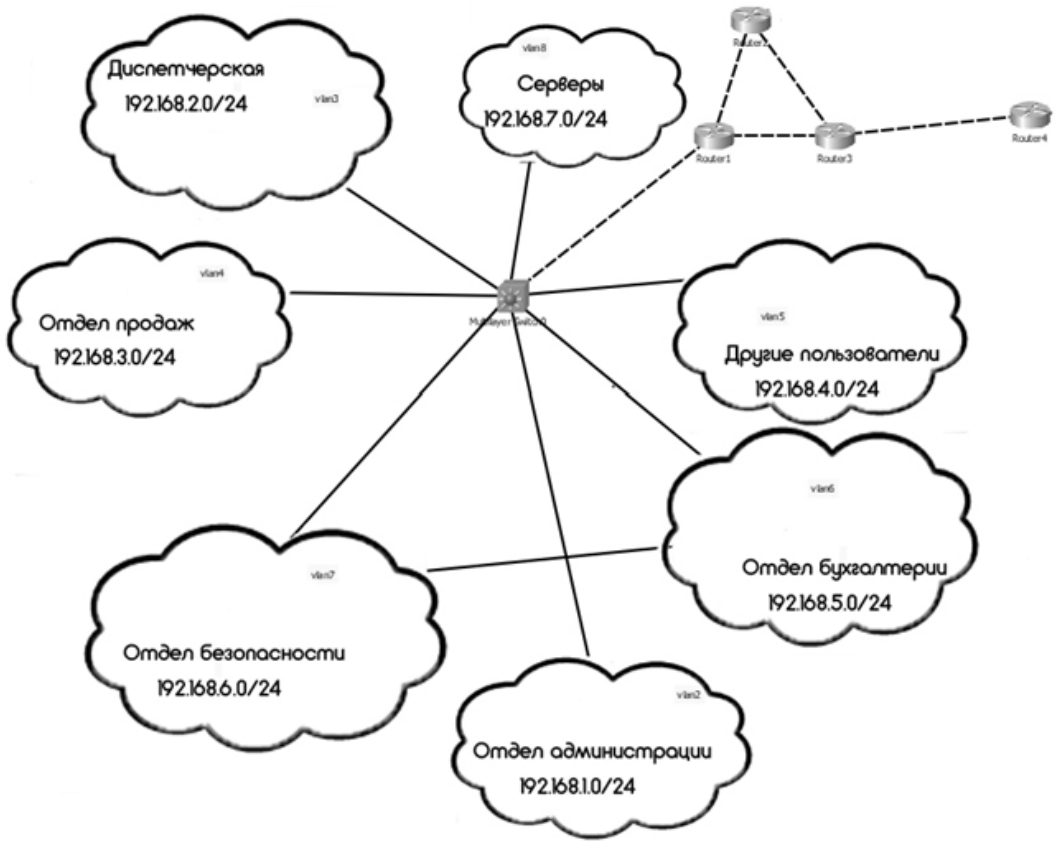


Рис. 1.5. Схема уровня L3

1.3.2. Разработка плана подключения оборудования

Составить список VLAN (табл.1).

Таблица 2.1

№ VLAN	*VLAN name*	*Примечания*
1	default	Не используется
2	Office1	Отдел администрации
3	Users1	Диспетчерская
4	Users2	Отдел продаж
5	Users3	Другие пользователи
6	Managers	Отдел бухгалтерии
7	Security	Отдел безопасности
8	Servers	Серверы

Каждому устройству в каждой локальной сети задать IP-адрес и маску подсети. IP address - IP-адрес, или Internet-адрес- 32-разрядный адрес, присваиваемый хостам с помощью протокола TCP/IP. IP-адрес относится к одному из пяти классов (A, B, C, D или E) и записывается в виде 4 октетов, разделенных точками (в десятичном формате). Каждый адрес состоит из сетевого номера, дополнительного номера подсети и номера хоста. Номера сети и подсети используются для маршрутизации, а номер хоста — для адресации отдельного хоста этой сети или подсети. Маска подсети используется для извлечения информации о сети и подсети из IP-адреса. Маска – это используемое совместно с IP-адресом четырехбайтовое число, двоичная запись которого содержит единицы в разрядах, соответствующих в адресе номеру сети, и нули в разрядах, соответствующих номеру узла. Единицы в маске начинаются в первом разряде адреса и не могут чередоваться с нулями.

Для вычисления номера сети по заданному IP-адресу и маске необходимо применить побитовую операцию “И” к адресу и маске. Такая операция называется наложением маски на адрес.

.

1-ый операнд	*2-ой операнд*	*Значение «И»*
0	0	0
1	0	0
0	1	0
1	1	1

Для вычисления номера узла по заданному IP-адресу и маске необходимо применить побитовую операцию “И” к адресу и результату применения побитовой операции “НЕ” к маске.

Ниже представлено табличное определение унарной операции побитового отрицания “НЕ”.

Операнд	*Значение «НЕ»*
1	0
0	1

Пример:

Дано: адрес 215.17.125.177 и маска 255.255.255.240. Необходимо вычислить номер сети и номер узла.

IP-адрес: 215.17.125.177 (11010111.00010001.01111101.10110001)

Маска: 255.255.255.240 (11111111.11111111.11111111.11110000)

В этом случае номер сети (Н.с.) и номер узла (Н.у.) будут следующими:

Н.с.: 215.17.125.176 (11010111.00010001.01111101.10110000)

Н.у.: 0.0.0.1 (00000000.00000000.00000000.00000001)

Составить IP-план, который будет включать в себя название устройства, его адрес, номер подсети и принадлежность к VLAN (табл. 1.2).

Таблица 3.2

P-адрес	*Примечание*	*VLAN*
192.168.0.0/16		
192.168.1.0/24	**Отдел администрации**	**2**
192.168.1.1	Шлюз	
192.168.1.2	PC14	
192.168.1.3	PC15	
192.168.1.4	PC16	
192.168.1.5	PC17	
192.168.1.6	IP Phone6	
192.168.1.7-192.168.1.254	Зарезервировано	
192.168.2.0/24	**Диспетчерская**	**3**
192.168.2.1	Шлюз	
192.168.2.2	PC1	
192.168.2.3	PC2	
192.168.2.4	PC3	
192.168.2.5	PC4	
192.168.2.6	PC5	
192.168.2.7	IP Phone1	
192.168.2.8-192.168.2.254	Зарезервировано	
192.168.3.0/24	**Отдел продаж**	**4**
192.168.3.1	Шлюз	
192.168.3.2	PC8	
192.168.3.3	PC9	
192.168.3.4	PC10	
192.168.3.5	PC11	
192.168.3.6	IP Phone2	
192.168.3.7	Printer0	
192.168.3.8	Printer1	
192.168.3.9-192.168.3.254	Зарезервировано	
192.168.4.0/24	**Другие пользователи**	**5**
192.168.4.1	Шлюз	

Таблица 3.2

P-адрес	*Примечание*	*VLAN*
192.168.4.2	PC18	
192.168.4.3	PC19	
192.168.4.4	IP Phone7	
192.168.4.5	Printer4	
192.168.4.6- 192.168.4.254	Зарезервировано	
192.168.5.0/24	**Отдел бухгалтерии**	**6**
192.168.5.1	Шлюз	
192.168.5.2	PC0	
192.168.5.3	PC6	
192.168.5.4	PC7	
192.168.5.5	IP Phone3	
192.168.5.6	Webcam IoT0	
192.168.5.7- 192.168.5.254	Зарезервировано	
192.168.6.0/24	**Отдел безопасности**	**7**
192.168.6.1	Шлюз	
192.168.6.2	PC12	
192.168.6.3	PC13	
192.168.6.4	IP Phone4	
192.168.6.5	IP Phone5	
192.168.6.6	Printer2	
192.168.6.7	Printer3	
192.168.6.8- 192.168.6.254	Зарезервировано	
192.168.7.0/24	**Серверы**	**8**
192.168.7.1	Шлюз	
192.168.7.2	Server0	
192.168.7.3	Server1	
192.168.7.4-192.168.7.254	Зарезервировано	

Составить таблицу подключения оборудования по портам (табл.1.3).

Таблица 4.3

Имя	*Название*	*FE*	*Gigabit*	*Access*	*Trunk*
Router3	Router0		2		
	Router2		3		
	Cloud		1		
Router0	Multilayer Switch0		2		
	Router2		1		
	Router3		3		
Router2	Router0		2		
	Router3		3		
	Wireless router0		1		
Multilayer Switch0	Router0		0/1		9
	Switch1	0/3			8

Таблица 4.3

Имя	Название	FE	Gigabit	Access	Trunk
	Switch2	0/2			2-3
	Switch3	0/1			4
	Switch4	0/6			7
	Switch5	0/7			2-3
	Switch6	0/5			6
	Switch7	0/4			5
Switch1	Multilayer Switch0		0/1		8
	Server0	0/8		8	
	Server1	0/7		8	
Switch2	Multilayer Switch0	0/1			2-3
	PC1	0/2		3	
	PC2	0/3		3	
	PC3	0/4		3	
	PC4	0/5		3	
	PC5	0/6		3	
	IP Phone1	0/1		3	
Switch3	Multilayer Switch0		0/1		4
	PC8	0/4		4	
	PC9	0/3		4	
	PC10	0/2		4	
	PC11	0/1		4	
	IP Phone2	0/5		4	
	Printer0	0/7		4	
	Printer1	0/6		4	
Switch4	Multilayer Switch0		0/1		7
	PC12	0/1		7	
	PC13	0/4		7	
	IP Phone4	0/6		7	
	IP Phone5	0/3		7	
	Printer2	0/5		7	
	Printer3	0/2		7	
Switch5	Multilayer Switch0		0/1		2-3
	PC14	0/3		2	
	PC15	0/1		2	
	PC16	0/2		2	
	PC17	0/4		2	
	IP Phone6	0/5		2	
Switch6	Multilayer Switch0		0/1		6
	PC0	0/1		6	
	PC6	0/2		6	
	PC7	0/3		6	
	IP Phone3	0/4		6	
	Webcam IoT0	0/5		6	
Switch7	Multilayer Switch0		0/1		5

Таблица 4.3

Имя	*Название*	*FE*	*Gigabit*	*Access*	*Trunk*
	PC18	0/3		5	
	PC19	0/4		5	
	IP Phone7	0/2		5	
	Printer4	0/1		5	

1.4 Контрольные вопросы

1. Какое нормативноправовое обеспечение необходимо учитывать при при построении защищённой сети?
2. Какие виды документов разрабатываются при построении сети?
3. 3. Как формируется модель угроз и модель нарушителя информационной безопасности при построении компьютерной сети?
4. Какие основные типы оборудования входят в сетевую инфраструктуру?
5. Как осуществляется IP адресация в сети?
6. Перечислите основные элементы многоуровневой системы обеспечения защиты при передаче информации по каналам связи.

СПИСОК ЛИТЕРАТУРЫ

1. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
4. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно телекоммуникационных сетей международного информационного обмена».
6. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
7. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
8. Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 09.08.2018) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
9. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования»

10. Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ»

11. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности.

12. ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт российской федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. https://fstec.ru/en/rss-lenta/113-tekhnicheskaya-zashchita-informatsii/dokumenty/gosudarstvennye-standarty/377-gosudarstvennye-standarty

13. ГОСТ Р ИСО/МЭК 27033-3-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.

14. ГОСТ Р ИСО/МЭК 27033-4-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности" утвержден приказом Росстандарта от 19 мая 2021 года N 391-ст.

15. ГОСТ Р 56045-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по оценке мер обеспечения информационной безопасности" утвержден приказом Росстандарта от 20 мая 2021 года N 421-ст.