

**Магистральная подсистема.**

Центральный коммутатор первого корпуса и центральный коммутатор второго корпуса, а также линии, соединяющие их с комутаторами этажей. Скорость передачи данных в магистральной подсистеме 1 Гб/с.

Оборудование магистральной подсистемы находится в напольных монтажных шкафах. Также в этих шкафайж находятся кроссовые панели, в которые приходят кабели.

В качестве кабелей магистральной подсистемы внутри зданий используется витая пара категории 5е, так как данная категория может передавать данные на скорости 1Гб/с. Снаружи зданий используется оптическое волокно, так как оно менее чувствительно к электромагнитным помехам и разрешено использованию снаружи зданий согласно ГОСТ Р 53246-2008. Для подключения оптического волокна к коммутаторам используются SFP модули.

**Горизонтальная подсистема**

В неё входят те коммутаторы, к которым подключены компьютеры пользователей. Коммутаторы этой подсистемы имеют как порты работающие на скорости 1Гб/c, так и порты, работающие нас скорости 100 Мб/с. Через первые они соединяются с магистральной подсистемой, через вторые — с компьютерами пользователей. Согласно ГОСТ Р 53246-2008 на одном этаже находится один коммутатор. Коммутаторы находятся в настенных монтажных шкафах. Также в этих шкафах находятся кроссовые панели, в которые приходят кабели от магистральной подсистемы и компьютеров пользователей.

Коммутаторы горизонтальной подсистемы не требуют настройки.

**Настройка VLAN**

На коммутаторах магистральной подсистемы настроены VLAN стандарта IEEE-802.1Q. Порты, соединяющие их с коммутаторами этажей имеют тип Access, порты, соединяющие их друг с другом и с маршрутизатором имеют тип Trunk. Благодаря этому пользователя, находящиеся на разных этажах не могут передавать друг другу пакеты, минуя маршрутизатор. В результате серверный сегмент сети будет доступен всем узлам сети и администратор может контролировать передачу пакетов между этажами путём настройки фаервола на маршрутизаторе.

В сети настроены 5 VLAN, они имеют идентификаторы от 2 до 6. VLAN с идентификатором 1 не используется, это является особенностью дляоборудования Cisco. Компьютеры распределены по VLAN следующим образом.

|  |  |  |
| --- | --- | --- |
| **Идентификатор VLAN** | **Номер корпуса** | **Номер этажа** |
| 2 | 1 | 1 |
| 3 | 1 | 2 |
| 4 | 2 | 1 |
| 5 | 2 | 2 |

В VLAN с идентификатором 6 входит один лишь сервер резервных копий. То, что этот сервер входит в отдельный VLAN даёт ему дополнительную защиту от несанкционированного доступа.

Связующим звеном между VLAN является внутренний маршрутизатор. На его внутреннем сетевом интерфейсе настроены 5 виртуальных интерфейсов, каждый из которых входит в один VLAN.

**Настройка IP подсетей.**

Каждому VLAN будет соответствовать IP подсеть. Это даст возможность сделать серверный сегмент доступным для всех узлов сети. Подсети, в которые входят компьютеры пользователей настроены следующим образом.

|  |  |  |  |
| --- | --- | --- | --- |
| **Идентификатор VLAN** | **Адрес подсети** | **Маска подсети** | **Основной шлюз** |
| 2 | 192.168.2.0 | 255.255.255.0 | 192.168.2.1 |
| 3 | 192.168.3.0 | 255.255.255.0 | 192.168.3.1 |
| 4 | 192.168.4.0 | 255.255.255.0 | 192.168.4.1 |
| 5 | 192.168.5.0 | 255.255.255.0 | 192.168.5.1 |

Сервер резервных копий выделен в отдельную подсеть для повышения его безопасности со следующими настройками.

|  |  |  |  |
| --- | --- | --- | --- |
| **Идентификатор VLAN** | **Адрес подсети** | **Маска подсети** | **Основной шлюз** |
| 6 | 192.168.6.0 | 255.255.255.0 | 192.168.6.1 |

IP адреса основных шлюзов — это адреса виртуальных интерфейсов, настроенных на внутреннем роутере.

Сетевые настройки компьютеры пользователей получают по протоколу DHCP. В качестве DHCP сервера выступает внутренний роутер. Сервер резервных копий имеет постоянный IP адрес 192.168.6.2.

Кроме перечисленных подсетей имеется также подсеть серверного сегмента со следующими параметрами.

|  |  |  |
| --- | --- | --- |
| **Адрес подсети** | **Маска подсети** | **Основной шлюз** |
| 10.0.0.0 | 255.255.255.0 | 10.0.0.1 |

IP адрес основного шлюза — это адрес внешнего интерфейса внутреннего роутера. Сетевые настройки узлов серверного сегмента задаются администратором вручную, так как IP адреса серверов должны быть постоянными. VLAN в серверном сегменте не настраивается, так как серверы должны быть доступны друг для друга.

В результате серверный сегмент отделён роутерами как от компьютеров пользователей, так и от сети провайдера. Такой способ организации серверного сегмента носит название Демилитаризованная зона.

**Настройка фаервола**

Фаервол настраивается на внутреннемроутере. Он запрещает передачу пакетов из любой подсети, в которых находятся компьютеры пользователей в любую из этих подсетей. Но разрешает передачу остальных пакетов. В результате подсети пользователей могут взаимодействовать с серверным сегментом, но не могут взаимодействовать друг с другом, что повышает безопасность сети.

**Настройка порганичного маршрутизатора**

Порганичный маршрутизатор соединяет сеть предприятия с сетью провайдера, а через него с интернетом. Для организации выхода в интернет на пограничном роутере настроена трансляция адресов (NAT - Network Address Translation). Эта технология позволяет, используя один IP адрес, полученный от провайдера обеспечить выход в интернет для всех компьютеров организации. Кроме этого технология NAT защищает внутреннюю подсеть от кибер-атак извне, так как иницииатором сетевого соединения между узлами сети предприятия и интернетом может выступать лишь компьютер сети предприятия, но не узел интернета.