Практическая работа №16

БЕЗОПАСНОСТЬ ЛОКАЛЬНЫХ СЕТЕЙ

Цель работы. Изучить способы организации виртуальных локальных сетей для организации разграничения трафика локальной вычислительной сети.

Краткие сведения из теории

Важным свойством коммутатора локальной сети является способность контролировать передачу кадров между сегментами сети. По различным причинам (соблюдение прав доступа, политика безопасности и т. д.) некоторые кадры не следует передавать по адресу назначения. Ограничения такого типа можно реализовать с помощью пользовательских фильтров. Однако пользовательский фильтр может запретить коммутатору передачу кадров только по конкретным адресам, а широковещательный трафик он обязан передать всем сегментам сети. Так требует алгоритм его работы. Поэтому, сети, созданные на основе коммутаторов, иногда называют **плоскими** – из-за отсутствия барьеров на пути широковещательного трафика. Технология виртуальных локальных сетей позволяет преодолеть указанное ограничение.

Виртуальной локальной сетью (**Virtual Local Area Network**, **VLAN**) называется группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов сети.

Это означает, что передача кадров между разными виртуальными сетями на основании адреса канального уровня невозможна независимо от типа адреса (уникального, группового или широковещательного). В то же время внутри виртуальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с адресом назначения кадра. Виртуальные локальные сети могут перекрываться, если один или несколько компьютеров входят в состав более чем одной виртуальной сети. На рисунке 1 сервер электронной почты входит в состав виртуальных сетей 3 и 4. Это означает, что его кадры передаются коммутаторами всем компьютерам, входящим в эти сети. Если же какой-то компьютер входит в состав только виртуальной сети 3, то его кадры до сети 4 доходить не будут, но он может взаимодействовать с компьютерами сети 4 через общий почтовый сервер. Такая схема защищает виртуальные сети друг от друга не полностью, например широковещательный шторм, возникший на сервере электронной почты, затопит и сеть 3, и сеть 4. Говорят, что виртуальная сеть образует

домен широковещательного трафика по аналогии с доменом коллизий, который образуется повторителями сетей Ethernet.

Назначение виртуальных сетей.

С помощью пользовательских фильтров можно вмешиваться в нормальную работу коммутаторов и ограничивать взаимодействие узлов локальной сети в соответствии с требуемыми правилами доступа. Однако механизм пользовательских фильтров коммутаторов имеет несколько недостатков:

– **Приходится задавать отдельные условия для каждого узла сети,** используя при этом громоздкие MAC-адреса. Гораздо проще было бы группировать узлы и описывать условия взаимодействия сразу для групп.

– **Невозможно блокировать широковещательный трафик.** Широковещательный трафик может быть причиной недоступности сети, если какой-то ее узел умышленно или неумышленно с большой интенсивностью генерирует широковещательные кадры.

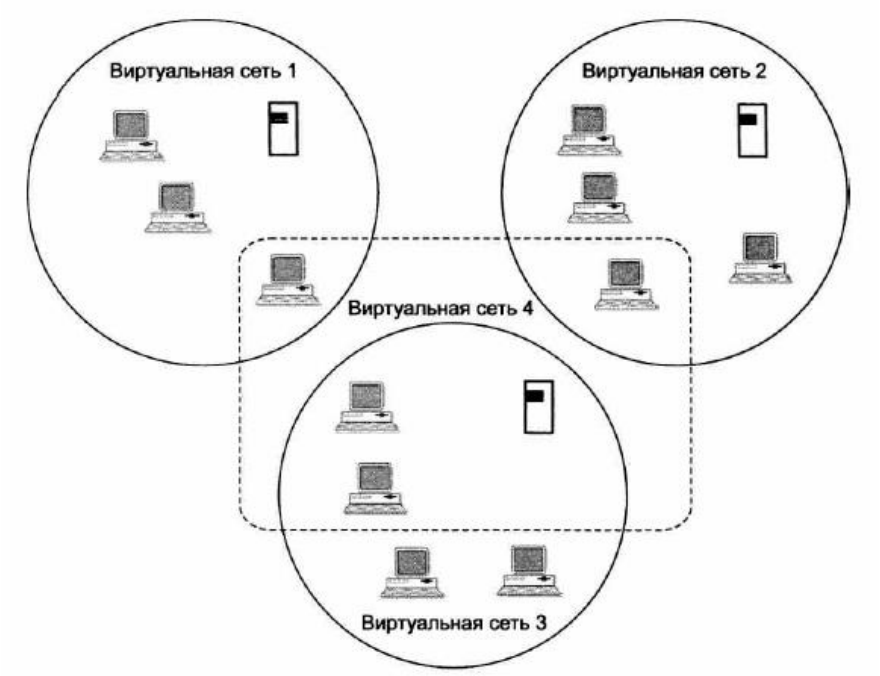

Рисунок 1 – Виртуальные локальные сети

Техника виртуальных локальных сетей решает задачу ограничения взаимодействия узлов сети другим способом. Основное назначение технологии

VLAN состоит в облегчении процесса создания изолированных сетей, которые затем обычно связываются между собой с помощью маршрутизаторов.

Такое построение сети создает мощные барьеры на пути нежелательного трафика из одной сети в другую. Сегодня считается очевидным, что любая крупная сеть должна включать маршрутизаторы, иначе потоки ошибочных кадров, например широковещательных, будут периодически «затапливать» всю сеть через прозрачные для них коммутаторы, приводя ее в неработоспособное состояние.

Достоинством технологии виртуальных сетей является то, что она позволяет создавать полностью изолированные сегменты сети путем логического конфигурирования коммутаторов, не прибегая к изменению физической структуры.

До появления технологии VLAN для создания отдельной сети использовались либо физически изолированные сегменты коаксиального кабеля, либо не связанные между собой сегменты, построенные на повторителях и мостах. Затем эти сети связывались маршрутизаторами в единую составную сеть (рисунок 2).

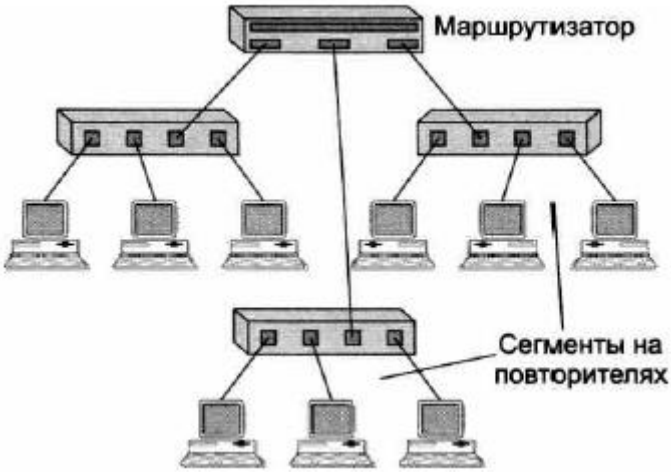

Рисунок 2 – Составная сеть, состоящая из сетей, построенных на основе повторителей

Изменение состава сегментов (переход пользователя в другую сеть, дробление крупных сегментов) при таком подходе подразумевает физическую перекоммутацию разъемов на передних панелях повторителей или на кроссовых панелях, что не очень удобно в больших сетях – много физической работы, к тому же высока вероятность ошибки. Для связывания вирту-

альных сетей в общую сеть требуется привлечение средств сетевого уровня. Он может быть реализован в отдельном маршрутизаторе или в составе программного обеспечения коммутатора, который тогда становится комбинированным устройством – так называемым **коммутатором 3-го уровня.** Технология виртуальных сетей долгое время не стандартизировалась, хотя и была реализована в очень широком спектре моделей коммутаторов разных производителей. Положение изменилось после принятия в 1998 году стандарта IEEE 802.1Q, который определяет базовые правила построения виртуальных локальных сетей, не зависящие от протокола канального уровня, поддерживаемого коммутатором.

Создание виртуальных сетей на базе одного коммутатора.

При создании виртуальных сетей на основе одного коммутатора обычно используется механизм **группирования портов** коммутатора (рисунок 3). При этом каждый порт приписывается той или иной виртуальной сети. Кадр, пришедший от порта, принадлежащего, например, виртуальной сети 1, никогда не будет передан порту, который не принадлежит этой виртуальной сети. Порт можно приписать нескольким виртуальным сетям, хотя на практике так делают редко – пропадает эффект полной изоляции сетей. Создание виртуальных сетей путем группирования портов не требует от администратора большого объема ручной работы – достаточно каждый порт приписать к одной из нескольких заранее поименованных виртуальных сетей. Обычно такая операция выполняется с помощью специальной программы, прилагаемой к коммутатору. Второй способ образования виртуальных сетей основан на **группировании MAC-адресов**. Каждый MAC-адрес, который изучен коммутатором, приписывается той или иной виртуальной сети. При существовании в сети множества узлов этот способ требует от администратора большого объема ручной работы и по этой причине не получил распространения.

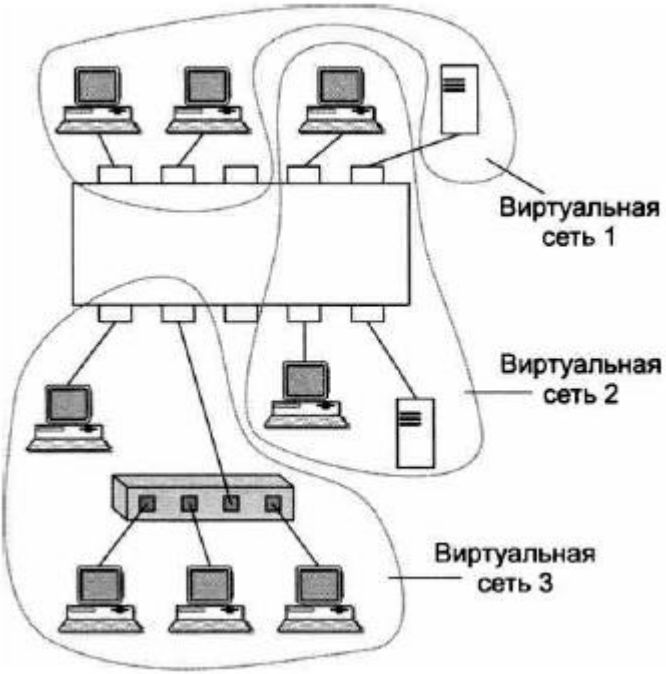

Рисунок 3 – Виртуальные сети, построенные на одном коммутаторе

Создание виртуальных сетей на базе нескольких коммутаторов.

Рисунок 4 иллюстрирует проблему, возникающую при создании виртуальных сетей на основе нескольких коммутаторов, поддерживающих технику **группирования портов**.

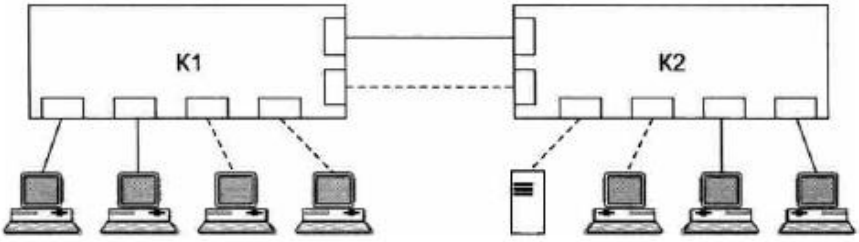

Рисунок 4 – Построение виртуальных сетей на нескольких коммутаторах с группированием портов

Если узлы какой-либо виртуальной сети подключены к разным коммутаторам, то для подключения каждой такой сети на коммутаторах должна

быть выделена специальная пара портов. В противном случае, если коммутаторы будут связаны только одной парой портов, информация о принадлежности кадра той или иной виртуальной сети при передаче из коммутатора в коммутатор будет утеряна. Таким образом, коммутаторы с группированием портов требуют для своего соединения столько портов, сколько виртуальных сетей они поддерживают. Порты и кабели используются в этом случае очень расточительно. Кроме того, при соединении виртуальных сетей через маршрутизатор для каждой виртуальной сети выделяются отдельные кабель и порт маршрутизатора, что также приводит к большим накладным расходам.

Группирование MAC-адресов в виртуальную сеть на каждом коммутаторе избавляет от необходимости связывать их по нескольким портам, поскольку в этом случае MAC-адрес становится меткой виртуальной сети. Однако этот способ требует выполнения большого количества ручных операций по маркировке MAC-адресов на каждом коммутаторе сети. Описанные два подхода основаны только на добавлении дополнительной информации к адресным таблицам коммутатора, и в них отсутствует возможность встраивания в передаваемый кадр информации о принадлежности кадра виртуальной сети. Поэтому широкое распространение получил иной подход, основанный на введении в кадр *дополнительного поля*, которое хранит информацию о принадлежности кадра той или иной виртуальной локальной сети при его перемещениях между коммутаторами сети. При этом нет необходимости помнить в каждом коммутаторе о принадлежности всех MAC-адресов составной сети виртуальным сетям. Дополнительное поле с пометкой о номере виртуальной сети используется только тогда, когда кадр передается от коммутатора к коммутатору, а при передаче кадра конечному узлу оно обычно удаляется. При этом модифицируется протокол взаимодействия «коммутатор-коммутатор», а программное и аппаратное обеспечение конечных узлов остается неизменным. До принятия стандарта IEEE 802.1Q существовало много фирменных протоколов этого типа, но все они имели один недостаток – оборудование различных производителей при образовании VLAN оказывалось несовместимым.Стандарт IEEE 802.1Q вводит в кадре Ethernet дополнительный заголовок, который называется тегом виртуальной локальной сети.

Тег виртуальной локальной сети состоит из поля **TCI** (**Tag Control Information** – управляющая информация тега) размером в 2 байта и предшествующего ему поля **EtherType,** которое является стандартным для кадров Ethernet и также состоит из 2 байт (рисунок 5).

Тег VLAN не является обязательным для кадров Ethernet. Кадр, у которого имеется такой заголовок, называют **помеченным** (**tagged frame**). Коммутаторы могут одновременно работать как с помеченными, так и с непомеченными кадрами. Из-за добавления тега VLAN максимальная длина по-

ля данных уменьшилась на 4 байта. Для того чтобы оборудование локальных сетей могло отличать и понимать помеченные кадры, для них введено специальное значение поля EtherType, равное 0x8100. Это значение говорит о том, что за ним следует поле TCI, а не стандартное поле данных. В помеченном кадре за полями тега VLAN следует другое поле EtherType, указывающее тип протокола, данные которого переносятся полем данных кадра. В поле TCI находится 12-битное поле номера (идентификатора) VLAN, называемого **VID.** Разрядность поля VID позволяет коммутаторам создавать до 4096 виртуальных сетей.

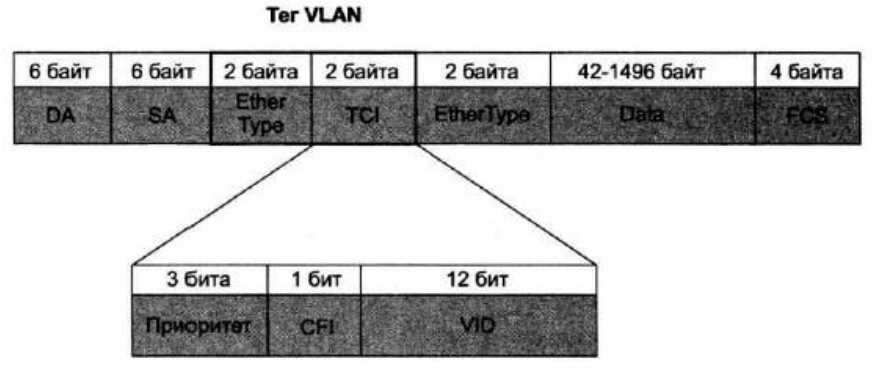

Рисунок 5 – Структура помеченного кадра Ethernet

Помимо этого, в поле TCI помещено 3-битное поле **приоритета** кадра. Однобитное поле **CFI** было введено с целью поддержания специального формата кадра Token Ring, для сетей Ethernet оно должно содержать значение 0. Пользуясь значением VID в помеченных кадрах, коммутаторы сети выполняют групповую фильтрацию трафика, разбивая сеть на виртуальные сегменты, то есть на VLAN. Для поддержки этого режима каждый порт коммутатора приписывается к одной или нескольким виртуальным локальным сетям, то есть выполняется группировка портов. Поле приоритета предназначено для согласованного обеспечения качества обслуживания (QoS) различных классов трафика. Всего может поддерживаться до восьми классов трафика (это определяется тремя битами поля).

Конфигурирование VLAN.

Существуют различные подходы к конфигурированию виртуальных локальных сетей, построенных на нескольких коммутаторах. Наиболее распространенным является подход, основанный на понятиях линии доступа и транка.

Линия доступа связывает порт коммутатора (называемый в этом с конечным узлом (компьютером, мобильным устройством и т. п.), виртуальной

локальной сети. Предполагается, что конечный узел кадрами, то есть структура VLAN для него прозрачна.

Транк – это линия связи, которая соединяет между собой порты двух коммутаторов; в общем случае через транк передается трафик нескольких виртуальных сетей.

Коммутаторы, поддерживающие технику VLAN, без специального конфигурирования по умолчанию работают как стандартные коммутаторы, обеспечивая соединения всех со всеми. В сети, образованной такими коммутаторами, все конечные узлы по умолчанию относятся к условной сети VLAN1 с идентификатором VID, равным 1. Все порты этой сети, к которым подключены конечные узлы, по определению являются портами доступа. Сеть VLAN1 можно отнести к виртуальным локальным сетям лишь условно, так как по ней передаются непомеченные кадры. Условная сеть VLAN также называется сетью VLAN, предлагаемой по умолчанию (default VLAN) или естественной (native VLAN).Для того чтобы образовать в исходной сети виртуальную локальную сеть, нужно в первую очередь выбрать для нее значение идентификатора VID, отличное от 1, а затем, используя команды конфигурирования коммутатора, приписать к этой сети те порты, к которым присоединены включаемые в нее компьютеры. Порт доступа может быть приписан только к одной виртуальной локальной сети. Порты доступа получают от конечных узлов сети непомеченные кадры и помечают их тегом VLAN, содержащим то значение VID, которое назначено этому порту. При передаче же помеченных кадров конечному узлу порт доступа удаляет тег виртуальной локальной сети. Для более наглядного описания вернемся к рассмотренному ранее примеру сети. На рисунке 6 показано, как решается задача избирательного доступа к серверам на основе техники VLAN.

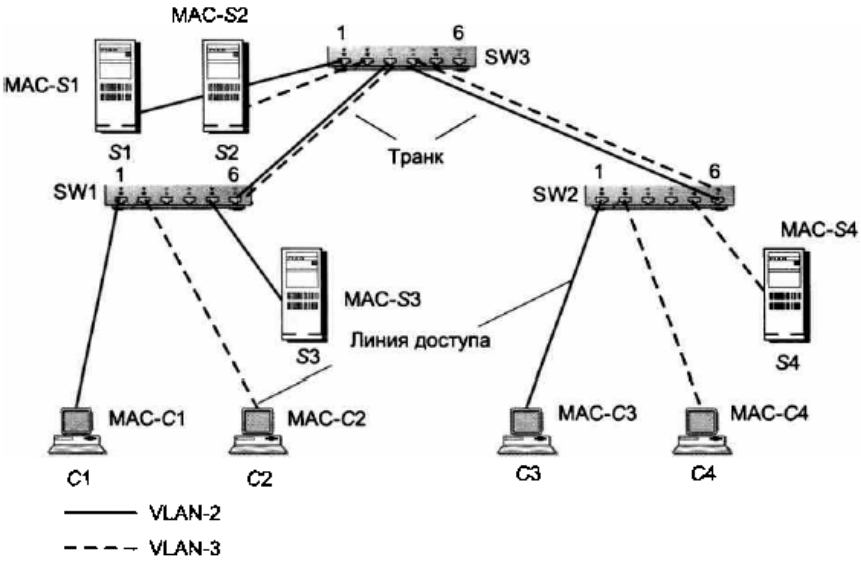

Рисунок 6 – Разбиение сети на две виртуальные локальные сети

Будем считать, что поставлена задача обеспечить доступ компьютеров C1 и C3 к серверам S1 и S3, в то время как компьютеры C2 и C4 должны иметь доступ только к серверам S2 и S4.

Чтобы решить эту задачу, можно организовать две виртуальные локальные сети, VLAN2 и VLAN3 (напомним, что сеть VLAN1 уже существует по умолчанию – это наша исходная сеть), приписав один набор компьютеров и серверов к VLAN2, а другой – к VLAN3. Первым шагом в конфигурировании VLAN2 и VLAN3 является их активизация в каждом из коммутаторов сети. Затем к этим сетям VLAN можно приписать определенные порты, работающие в режиме доступа. Для приписывания конечных узлов к определенной виртуальной локальной сети соответствующие порты объявляются портами доступа этой сети путем назначения им соответствующего идентификатора VID. Например, порт 1 коммутатора SW1 должен быть объявлен портом доступа VLAN2 путем назначения ему идентификатора VID2, то же самое должно быть проделано с портом 5 коммутатора SW1, портом 1 коммутатора SW2 и портом 1 коммутатора SW3. Порты доступа сети VLAN3 должны получить идентификатор VID3. В нашей сети нужно также организовать транки – те линии связи, которые соединяют между собой порты коммутаторов. Порты, подключенные к транкам, не добавляют и не удаляют теги, они просто передают кадры в неизменном виде. В нашем примере такими портами должны быть порты 6 коммутаторов SW1 и SW2, а также

порты 3 и 4 коммутатора SW3. Порты в нашем примере должны поддерживать сети VLAN2 и VLAN3 (и VLAN1, если в сети есть узлы, явно не приписанные ни к одной виртуальной локальной сети). Транк может быть сконфигурирован как в «неразборчивом» режиме, когда он передает кадры с любым номером VLAN, так и в избирательном режиме, когда он передает кадры только определенных номеров VLAN. Коммутаторы, поддерживающие технологию VLAN, осуществляют дополнительную фильтрацию трафика. В том случае если таблица продвижения коммутатора говорит о том, что пришедший кадр нужно передать на некоторый порт, перед передачей коммутатор проверяет, соответствует ли значение VID в теге VLAN кадра той виртуальной локальной сети, которая приписана к этому порту. В случае соответствия кадр передается, несоответствия – отбрасывается. Непомеченные кадры обрабатываются аналогичным образом, но с использованием условной сети VLAN1. MAC-адреса изучаются коммутаторами сети отдельно по каждой виртуальной локальной сети.

Порядок выполнения работы

1 В программе Cisco Packet Tracer собрать локальную сеть, представленную на рисунке 7. Преподавательским и студенческим компьютерам, а также серверу задать IP-адреса в соответствии с данными таблицы 1.

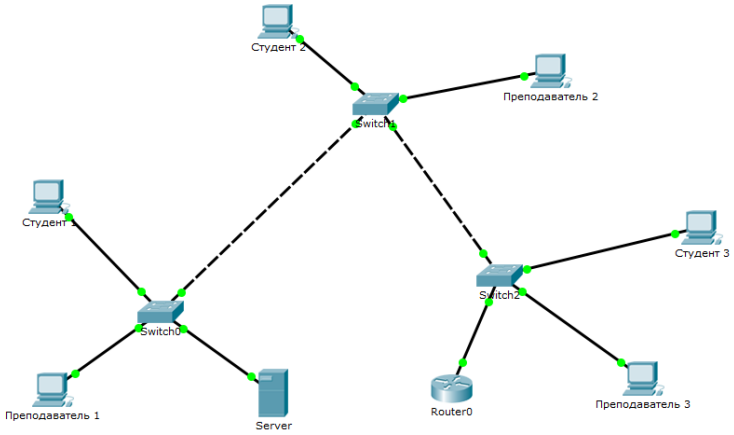

Рисунок 7 – Схема локальной сети

Таблица 1 – **Адреса оконечных устройств локальной сети**

Оконечное устройство	IP-адрес	VLAN
Студент 1	192.168.101.2/24	Student 101
Студент 2	192.168.101.3/24	Student 101
Студент 3	192.168.101.4/24	Student 101

Преподаватель 1	192.168.102.2/24	Professor 102
Преподаватель 2	192.168.102.3/24	Professor 102
Преподаватель 3	192.168.102.4/24	Professor 102
Server	192.168.111.254/24	Other 111

2 На коммутаторах создать виртуальные сети Student (номер 101), Professor (номер 102) и Other (номер 111). Например, для создания VLAN 101 необходимо выполнить следующие команды в командной строке каждого коммутатора (CLI):

Switch>enable
Switch#configure terminal
Switch(config)#vlan 101
Switch(config-vlan)#name Student
Switch(config-vlan)#exit

3 Назначить в созданные VLAN-сети физические порты коммутаторов, для чего перейти в режим конфигурирования каждого интерфейса, перевести его в режим доступа и назначить его в соответствующую VLAN-сеть. Например, для порта FastEthernet 0/1, к которому подключен компьютер с именем Студент 1, с помощью следующих команд назначается VLAN с номером 101:

Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 101
Switch(config-if)#exit

4 Порты Gigabit Ethernet, соединяющие коммутаторы между собой, а также коммутатор с маршрутизатором, являются транковыми, что означает, что через них будут передаваться данные от всех VLAN. Настраиваются эти порты с помощью следующих команд:

Switch(config)#interface GigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 101, 102, 111
Switch(config-if)#exit

5 Всем незадействованным интерфейсам коммутаторов, например, FastEthernet с 4 по 24 необходимо назначить VLAN 111:

Switch(config)#interface range FastEthernet 0/4-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 111
Switch(config-if-range)#exit

6 Необходимо проверить работоспособность виртуальных сетей. Для этого необходимо с использованием утилиты ping проверить доступность компьютера одного студента с компьютера другого студента и доступность компьютера преподавателя с компьютера другого преподавателя. Также необходимо убедиться в недоступности компьютеров преподавателей с компьютеров студентов и наоборот.

7 Для того чтобы маршрутизатор мог передавать трафик из одного VLAN в другой, необходимо выделять под сеть каждого VLAN логический подынтерфейс. Для этого на маршрутизаторе необходимо выполнить следующие команды:

```
Router>enable
Router#configure terminal
Router(config)#interface GigabitEthernet 0/1.1
Router(config-if)#ip address 192.168.101.1 255.255.255.0
Router(config)#interface GigabitEthernet 0/1.2
Router(config-if)#ip address 192.168.102.1 255.255.255.0
Router(config)#interface GigabitEthernet 0/1.11
Router (config-if)#ip address 192.168.111.1 255.255.255.0
Router(config)#interface GigabitEthernet 0/1
Router (config-if)#no shutdown
Router(config-if)#exit
```

IP-адреса 192.168.101.1/24, 192.168.102.1/24 и 192.168.111.1/24 являются адресами шлюзов по умолчанию для VLAN 101, 102 и 111 соответственно.

8 Повторно проверить работоспособность виртуальных сетей с использованием утилиты ping. Необходимо убедиться в доступности компьютеров преподавателей с компьютеров студентов и наоборот, а также доступ к серверу с компьютеров как преподавателей, так и студентов.

Содержание отчета

1 Цель работы.
2 Схема локальной сети с указанием VLAN.
3 Результаты настройки VLAN на каждом из коммутаторов.
4 Результаты настройки логических интерфейсов на маршрутизаторе.
5 Результаты работы утилиты ping.
6 Вывод по работе.

Контрольные вопросы

1 Что такое виртуальная локальная сеть?
2 Назначение VLAN.
3 Создание виртуальных сетей на базе одного коммутатора.
4 Создание виртуальных сетей на базе нескольких коммутаторов.
5 Тег виртуальной локальной сети.

6 Понятие транка.