

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИССЛЕДОВАНИЕ СЕТЕВОГО КОММУТАТОРА ВТОРОГО УРОВНЯ

Учебно-методическое пособие

по выполнению лабораторной работы по дисциплине

«Телекоммуникационные системы»

для студентов очной и заочной форм обучения

направлений подготовки 11.03.01 «Радиотехника»,

11.03.02 «Инфокоммуникационные технологии и системы связи»

и специальности 11.05.01 «Радиоэлектронные системы и комплексы»

Севастополь
СевГУ
2020

УДК 621.396 + 621.391
И88

Р е ц е н з е н т:

С.Р. Зиборов - кандидат технических наук, доцент,
доцент кафедры «Радиоэлектроника и телекоммуникации»

Ответственный за выпуск:

И.Л. Афонин - заведующий кафедрой «Радиоэлектроника
и телекоммуникации», д.т.н., профессор

Составитель: А.А. Савочкин

И88 Исследование сетевого коммутатора второго уровня : учебно-методическое пособие по выполнению лабораторной работы по дисциплине «Телекоммуникационные системы» для студентов очной и заочной форм обучения направлений подготовки 11.03.01 «Радиотехника», 11.03.02 «Инфокоммуникационные технологии и системы связи» и специальности 11.05.01 «Радиоэлектронные системы и комплексы» / Сост. А.А. Савочкин ; Министерство науки и высшего образования РФ, Севастопольский государственный университет, Институт радиоэлектроники и информационной безопасности, кафедра «Радиоэлектроника и телекоммуникации». - Севастополь: СевГУ, 2020. - 24 с. - Текст : электронный.

Целью учебно-методического пособия является оказание помощи студентам при выполнении лабораторной работы по дисциплине «Телекоммуникационные системы», а также в получении ими теоретических знаний и практических навыков работы с коммутаторами второго уровня *Cisco Catalyst 2924 XL*.

УДК 621.396 + 621.391

Утверждено на заседании кафедры «Радиоэлектроника и телекоммуникации», протокол № 12 от 09 июня 2020 г.

Рассмотрено и рекомендовано к изданию на заседании Ученого совета Института радиоэлектроники и информационной безопасности, протокол № 12 от 10 июня 2020 г.

СОДЕРЖАНИЕ

1. Цель лабораторной работы	4
2. Теоретическая часть.....	4
2.1. Принципы реализации коммутации в локальных сетях	4
2.2. Основные функции коммутации второго уровня	5
2.3. Режимы работы коммутаторов локальных сетей	8
2.4. Виртуальные локальные сети	9
2.5. Особенности работы портов коммутаторов	13
2.6. Особенности настройки коммутаторов <i>Cisco</i>	14
3. Описание лабораторной установки	16
3.1. Состав лабораторной установки.....	16
4. Порядок выполнения лабораторной работы	17
4.1. Подключение к коммутатору и определение характери- стик его функционирования.....	17
4.2. Создание виртуальных локальных компьютерных сетей на коммутаторе <i>A</i>	19
4.3. Создание виртуальных локальных компьютерных сетей на коммутаторе <i>B</i>	21
5. Содержание отчета по лабораторной работе	22
6. Контрольные вопросы	23
6.1. Вопросы для допуска к выполнению лабораторной работы.....	23
6.2. Вопросы для защиты лабораторной работы.....	23
Библиографический список.....	24

1. ЦЕЛЬ ЛАБОРАТОРНОЙ РАБОТЫ

Целью лабораторной работы является изучение особенностей работы сетевых коммутаторов и особенностей программирования сетевого коммутатора на втором уровне модели открытых систем *OSI*.

2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

2.1. Принципы реализации коммутации в локальных сетях

Сетевой коммутатор или свитч предназначен для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю, исключение составляет широковещательный трафик (на *MAC*-адрес *FF:FF:FF:FF:FF:FF*) всем узлам сети. Такой режим повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Коммутатор работает на втором (канальном) уровне модели *OSI* и потому в общем случае может только объединять узлы одной сети по их *MAC*-адресам. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты.

Коммутация это термин, используемый в основном для описания сетевых устройств второго уровня, которые переправляют фреймы, основываясь на *MAC*-адресе получателя.

Сетевая коммутация на втором уровне реализуется аппаратно, т. е. коммутатор для сетевой фильтрации использует *MAC*-адреса удаленных сетевых устройств. В коммутаторах используются специализированные интегральные микросхемы (*Application-Specific Integrated Circuits — ASIC*), которые формируют и обслуживают таблицы фильтрации. Коммутаторы второго уровня работают достаточно быстро, поскольку не используют информацию из заголовков сетевого уровня, а анализируют аппаратные адреса в кадре для решения о перенаправлении или об отбросе пакета.

Коммутация на втором уровне используется для обеспечения связей между рабочими группами и для сегментации сети (деление на домены конфликтов). Процесс коммутации второго уровня позволяет реализовывать сетевые проекты с гораздо большим числом сегментов, чем в сетях на концентраторах.

Коммутация второго уровня увеличивает пропускную способность для каждого пользователя при малом запаздывании, поскольку каждая связь с коммутатором образует собственный домен конфликтов.

Недостатки коммутации второго уровня обусловлены тем, что

коммутация на втором уровне аналогична работе мостов. Мосты эффективны только при правильном проектировании сети, т. е. при правильном делении на домены конфликтов. Правильным считается такой проект сети с мостами, в котором трафик пользователей не менее 80 % своего времени передается внутри собственных локальных сегментов. Мосты делят сеть на домены конфликтов, но вся сеть остается одним большим доменом ширококвещательных рассылок.

Коммутаторы второго уровня (мосты) не способны разделить домен ширококвещательных рассылок, поскольку возникнут проблемы с производительностью и проявятся ограничения на размер сети. Ширококвещательные и многоадресные рассылки совместно с малым временем конвергенции алгоритма покрывающего дерева могут привести к серьезным проблемам при увеличении размера сети. Учитывая эти проблемы, нельзя считать, что переключатели второго уровня способны заменить маршрутизаторы (устройства третьего уровня) в сложных сетях.

Перечислим **основные отличия работы коммутаторов второго уровня от работы мостов** с большим числом портов:

- а) мосты реализуются программно, а коммутаторы — аппаратно, поскольку переключатели могут использовать *ASIC* для принятия решений о фильтрации данных;
- б) мосты способны обслужить только один экземпляр покрывающего дерева на устройство, а коммутаторы — несколько покрывающих деревьев;
- в) мосты содержат не более 16 портов, а коммутаторы могут иметь сотни портов.

2.2. Основные функции коммутации второго уровня

В процессе коммутации второго уровня выполняются три основные функции: изучение адресов; решение о пересылке или фильтрации; исключение заикливания.

Изучение адресов. Коммутаторы второго уровня и мосты запоминают аппаратный адрес источника каждого полученного интерфейсом кадра и сохраняют эту информацию в своей базе данных *MAC*-адресов.

После включения питания коммутатора его таблица фильтрации *MAC*-адресов пуста. Когда устройство передает, а интерфейс получает кадр, коммутатор помещает адрес источника в таблицу фильтрации *MAC*-адресов вместе с номером интерфейса. Коммутатор не выполняет самостоятельных решений о перенаправлении кадров, поскольку не знает местонахождение устройства назначения. Если устройство отвечает и посылает кадр обратно, то коммутатор извлекает адрес источника из возвращенного кадра и помещает его *MAC*-адрес в свою базу данных, причем связывает этот адрес с интерфейсом, получившим кадр. После этого коммутатор содержит в таблице фильтрации два *MAC*-адреса и может устано-

вить соединение «точка-точка», в результате чего кадры будут перемещаться только между двумя известными переключателю устройствами. Именно поэтому коммутатор второго уровня работает эффективнее концентратора [1].

На рис. 2.1 показана процедура построения базы данных *MAC*-адресов на примере четырех станций, подключенных к коммутатору.

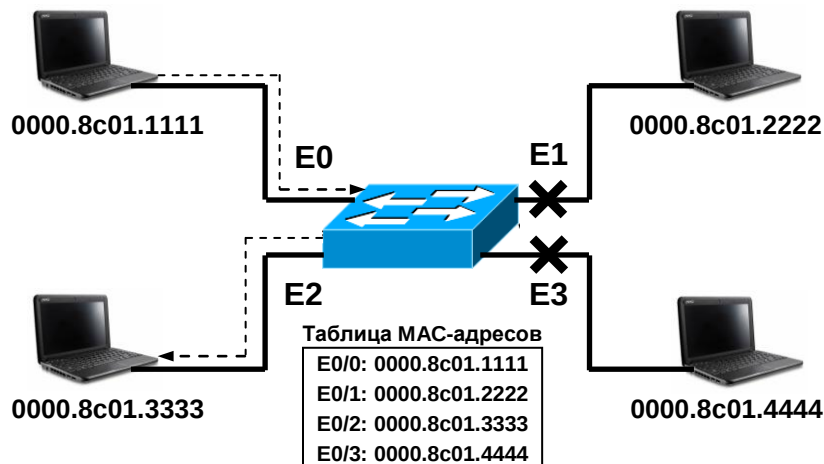


Рис. 2.1 — Процедура построения базы данных *MAC*-адресов

После включения питания коммутатора выполняются следующие операции:

1) Станция 1 посылает кадр Станции 3. Предположим, что *MAC*-адрес первой станции равен 0000.8c01.1111, а *MAC*-адрес третьей станции — 0000.8c01.3333.

2) Коммутатор принимает кадр по интерфейсу E0 и помещает в таблицу *MAC*-адресов адрес источника.

3) В базе данных *MAC*-адресов нет адреса назначения, поэтому кадр передается во все интерфейсы.

4) Станция 3 получает кадр и откликается на вызов Станции 1. Коммутатор принимает этот ответный кадр по интерфейсу E2 и помещает аппаратный адрес источника второго кадра в базу данных *MAC*-адресов.

5) Станции 1 и 3 могут установить соединение «точка-точка», причем кадры будут пересылаться только между этими двумя устройствами. Станции 2 и 4 не будут «видеть» подобные кадры.

6) Если в течение определенного времени два устройства не будут откликаться во время передачи кадров через коммутатор, то коммутатор очистит соответствующие записи в своей базе данных, чтобы поддержать корректность таблицы адресов.

Решение о пересылке или фильтрации. Когда интерфейс получает кадр, коммутатор анализирует аппаратный адрес назначения и осуществляет поиск в своей базе данных *MAC*-адресов требуемый интерфейс.

Если аппаратный адрес назначения известен и присутствует в базе

данных, то кадр направляется только в один выходной интерфейс, предписанный в таблице базы данных. Коммутатор не транслирует кадр во все остальные интерфейсы, за исключением интерфейса, ведущего к точке назначения. Это уменьшает загрузку других сетевых сегментов, а сам процесс называется рамочной фильтрацией кадров (*frame filtering*).

Если же аппаратный адрес назначения не указан в базе данных MAC-адресов, то кадр отсылается в широковещательной рассылке по всем активным интерфейсам, за исключением интерфейса, по которому этот кадр был получен. Если одно из устройств откликается на широковещательную рассылку, происходит обновление базы данных MAC-адресов за счет добавления местоположения устройства (интерфейса) назначения.

Исключение заикливания. Если между коммутаторами для повышения надежности сети создано несколько путей, то могут появиться замкнутые пути передачи информации. Протокол покрывающего дерева (*Spanning-Tree Protocol, STP*) позволяет исключить заикливание пакетов в сети при сохранении избыточности в сети.

Избыточные соединения между коммутаторами полезны, поскольку помогают предотвратить отказ сети при выходе из строя отдельной связи. Однако, несмотря на полезность избыточных соединений, они создают большие сложности. Поскольку кадры одновременно передаются в широковещательных рассылках по всем дублирующим соединениям, то могут возникать заикливания, а также другие проблемы. Рассмотрим наиболее серьезные негативные последствия.

а) Если не реализована схема исключения заикливания, то коммутатор переполнит бесконечными широковещательными рассылками объединенную сеть. Такой режим работы называется штормом широковещательных рассылок (*broadcast storm*). В этом случае кадры на физическом уровне объединенной сети будут пересылаться бесконечно в широковещательных рассылках.

б) Сетевое устройство может получить несколько копий одного кадра, поскольку кадры одновременно поступают из разных сегментов сети. На рис. 2.2 показан одновременный прием нескольких кадров из разных сегментов.

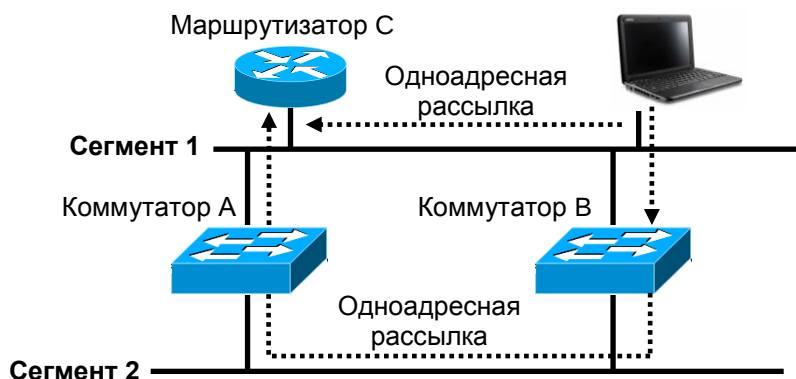


Рис. 2.2 — Схема формирования копий кадра в многосегментной сети

в) Таблица фильтрации MAC-адресов не может быть заполнена корректно, поскольку коммутатор получает ответы от одного устройства по нескольким связям. Вполне возможно, что коммутатор не сможет переслать кадр, поскольку будет постоянно обновлять таблицу фильтрации MAC-адресов на основе постоянно изменяющихся сведений о местоположении аппаратного адреса источника. Этот процесс называется «хлопаньем» (*thrashing*) таблицы MAC-адресов.

г) Наиболее опасной проблемой является генерирование нескольких зацикленных путей в объединенной сети. Зацикливание одного пути порождает зацикливание в других путях по сети, а шторм широковещательных рассылок будет усиливаться до такой степени, что произойдет полная остановка работы сети. Избежать проблем с зацикливанием помогает протокол покрывающего дерева *STP*.

Протокол *STP* позволяет найти все связи в сети и выделить среди них избыточные, чтобы отключить их и, тем самым, устранить любые зацикливания в сети. Для этого выполняется выбор корневого моста (*root bridge*), который будет следить за сетевой топологией. В любой сети может быть только один корневой мост.

В случае использования нескольких коммутаторов с одинаковым приоритетом, корневой мост назначается для коммутатора с наименьшим MAC-адресом.

2.3. Режимы работы коммутаторов локальных сетей

Задержка коммутации пакетов в коммутаторе зависит от выбранного режима работы. Существуют три режима работы коммутаторов: ***Store and forward*** (сохранить и передать); ***Cut-through*** (сквозной); ***FragmentFree*** (без фрагментации).

Режим «сохранить и передать». В таком режиме коммутатор локальной сети полностью копирует кадр в собственный встроенный буфер и проверяет контрольную сумму — *Cyclic redundancy check (CRC)*. Поскольку в этом режиме копируется весь кадр, задержка коммутации зависит от длины кадра. При ошибке *CRC* кадр отбрасывается, а также отбрасываются слишком короткие (менее 64 байтов, включая *CRC*) или слишком длинные (более 1518 байтов, включая *CRC*) кадры. Если в кадре не обнаружено ошибок, переключатель локальной сети выполняет поиск по аппаратному адресу назначения в своей таблице коммутации или перенаправления и выявляет выходной интерфейс для кадра. Затем кадр отправляется через выбранный интерфейс в точку назначения. Этот режим используется в переключателях серии *Catalyst 5000* и обычно не может быть изменен в устройстве.

Сквозной режим (реальное время). В этом режиме коммутатор копирует в собственный встроенный буфер только адрес назначения (первые

шесть байтов после преамбулы). Затем определяет аппаратный адрес назначения в MAC-таблице коммутатора, чтобы определить выходной интерфейс и направить в него кадр. Сквозной режим работы коммутатора обеспечивают низкую задержку, поскольку в этом случае обеспечивает пересылку кадра сразу после чтения адреса назначения и выявления выходного интерфейса. Некоторые коммутаторы могут настраиваться на сквозной режим для каждого отдельного порта. Причем этот режим действует до превышения установленной пользователем границы ошибок. Затем устройство автоматически переходит в режим «сохранить и передать», чтобы предотвратить дальнейшее распространение ошибок. Если же уровень ошибок для порта возвращается в установленные пределы, коммутатор возвращается в сквозной режим.

Режим без фрагментации является модифицированной версией сквозного режима, в котором коммутатор ожидает заполнения окна конфликтов (64 байта) до выполнения перенаправления. Если обнаруживается ошибка в принятом пакете, то она всегда проявляется в первых 64 байтах. Этот режим обеспечивает лучшую проверку на ошибки по сравнению со сквозным режимом (в частности, за счет того, что не происходит увеличения задержки на длинных кадрах). Этот режим используется по умолчанию для коммутаторов серии *Catalyst 1900*.

2.4. Виртуальные локальные сети

Виртуальная локальная компьютерная сеть или *Virtual Local Area Network (VLAN)* отличается от физической LAN лишь тем, что организуется разделение пакетов в единой локальной сети так, как если бы это были бы разные подсети. Таким образом, с помощью VLAN можно организовать деление локальной сети на отдельные участки.

Существует четыре основных способа организации виртуальных локальных сетей [2, 3].

VLAN на базе портов. При использовании VLAN на базе портов, каждый порт коммутатора назначается в определенную VLAN, независимо от того, какой пользователь или компьютер подключен к этому порту. Это означает, что все пользователи, подключенные к этому порту, будут членами одной VLAN. Конфигурация портов статическая и может быть изменена только вручную. Пример структуры порт ориентированной VLAN изображен на рис. 2.3.

VLAN на базе MAC адресов. При существовании в сети большого числа узлов этот способ требует выполнения большого числа ручных операций по настройке. Однако при построении виртуальных сетей на основе нескольких коммутаторов он оказывается более гибким, чем способ группировки портов. Широковещательные домены на базе MAC-адресов, обеспечивают физическое перемещение станции (подключение к любому пор-

ту коммутатора), позволяя оставаться ей в одном и том же широковещательном домене без каких-либо изменений в настройках конфигурации.

Это означает, что если из-за перепланировки нового назначения или реорганизации рабочая станция физически перемещается с одного порта на другой, то коммутатор автоматически отслеживает данное перемещение. Коммутатор распознает, что шестнадцатеричный адрес платы адаптера локальной сети теперь ассоциируется с другим портом. Такое распознавание происходит при передаче адаптером кадра и считывании коммутатором адреса его отправителя. Поскольку соответствие в этом случае устанавливается на основании *MAC*-адресов, а не портов, подобный метод создания виртуальной локальной сети позволяет также соотносить отдельные рабочие станции на одном и том же порту с разными виртуальными локальными сетями [3].



Рис. 2.3 — Пример структуры порт ориентированной VLAN

VLAN на основе меток в дополнительном поле кадра. Метод основан на использовании возможностей стандарта *IEEE 802.1Q*. Описанные выше два способа основаны только на добавлении дополнительной информации к адресным таблицам коммутатора и не используют возможности встраивания информации о принадлежности кадра к виртуальной сети в передаваемый кадр. Метод организации VLAN на основе меток — тэгов, использует дополнительные поля кадра для хранения информации о принадлежности кадра при его перемещениях между коммутаторами сети. Пример структуры VLAN на основе меток изображен на рис. 2.4.

Протокол *IEEE 802.1Q* использует вставку (тег) в оригинальный заголовок фрейма, длиной 4 байта, таким образом, максимальный размер фрейма может быть 1522 байта, т. е. 1518 байт для максимального пакета *Ethernet* плюс 4 байта заголовка. Минимальный размер тегированного фрейма может составлять 68 байт для технологии *Ethernet*. При работе по

протоколу 802.1Q изменяется непосредственно оригинальный фрейм: вставляется дополнительное поле и пересчитывается контрольная сумма.

Теги *ID* в такой *VLAN* могут быть добавлены явно или неявно. Если на устройствах сети используются сетевые карты с поддержкой *IEEE 802.1Q*, и на этих картах включен соответствующий режим, то исходящие кадры *Ethernet* от этих карт будут содержать теги *VLAN* идентификации. Данные теги идентификации *VLAN* добавлены явно. Коммутаторы, поддерживающие *IEEE 802.1Q*, идентифицируют членство в *VLAN*, проверяя теги *ID* в кадрах *Ethernet* [4].

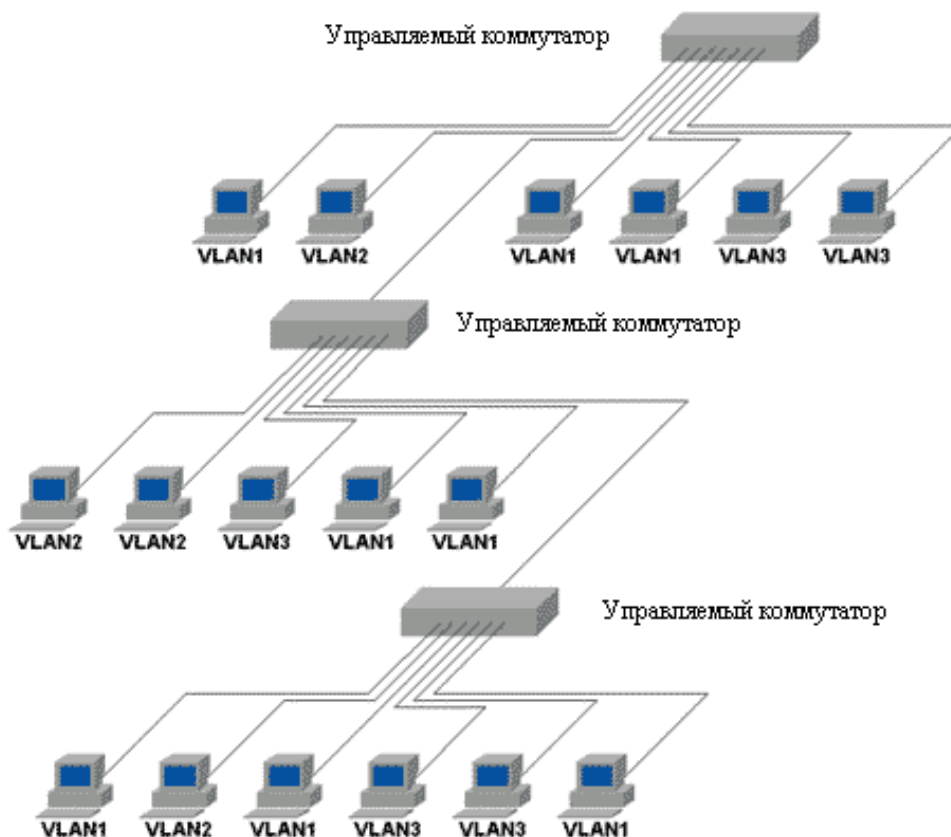


Рис. 2.4 — Структура *VLAN* на основе меток

Если сетевые адаптеры (подключенные к этой сети) не поддерживают протокол *IEEE 802.1Q*, то добавление тегов *VLAN* может быть все же выполнено на основе группировки по портам. Коммутатор с поддержкой *IEEE 802.1Q* будет добавлять тег *ID* к входящим на этот порт кадрам *Ethernet* с соответствующим *ID VLAN*. Но эти теги будут удалены коммутатором из исходящих кадров.

Если идентификация *VLAN* тегами протокола *IEEE 802.1Q* была осуществлена обоими способами — явно и неявно, входящие кадры к портам коммутатора могут состоять из обоих (с тегами и без тегов) типов кадров. В этой ситуации к неотмеченным входящим кадрам будут добавляться теги *ID VLAN*, описанные методом группировки по портам. В то время как

маркированные кадры уже поддерживают членство *VLAN* определенное явно. Например, если порт был сгруппирован неявно под *VLAN1*, то входящие к порту кадры с отметками *ID* сети *VLAN2* сохраняют их членство в *VLAN2* даже при том условии, что порт был сгруппирован под *VLAN1*.

Создание виртуальных локальных сетей на третьем уровне. Организуемые на третьем уровне сети *VLAN* используют информацию, содержащуюся в заголовках пакетов сетевого уровня. Таким образом, реализация данного метода построения виртуальных локальных сетей возможна только при применении маршрутизаторов и коммутаторов, поддерживающих маршрутизацию на третьем уровне. Критерии, в соответствии с которыми создаются подобные *VLAN*, напоминают принципы работы маршрутизатора, иными словами, они позволяют использовать в качестве критерия построения виртуальной локальной сети подсети *IP* и сетевые адреса *IPX*, домены *AppleTalk* и протоколы третьего (сетевого) уровня.

Например, возможно реализовать две *VLAN* в соответствии с сетевыми адресами *IP*. В данном примере первая виртуальная локальная сеть может соотноситься с ширококестельным доменом, образованным подсетью 198.78.55.0, которая, в свою очередь, представляет *IP*-адрес класса *C*. А вторая виртуальная локальная сеть может соотноситься с подсетью 198.78.42.0, представляющей другой *IP*-адрес класса *C* [3]. Пример структуры *VLAN* организованной на третьем уровне изображен на рис. 2.5.

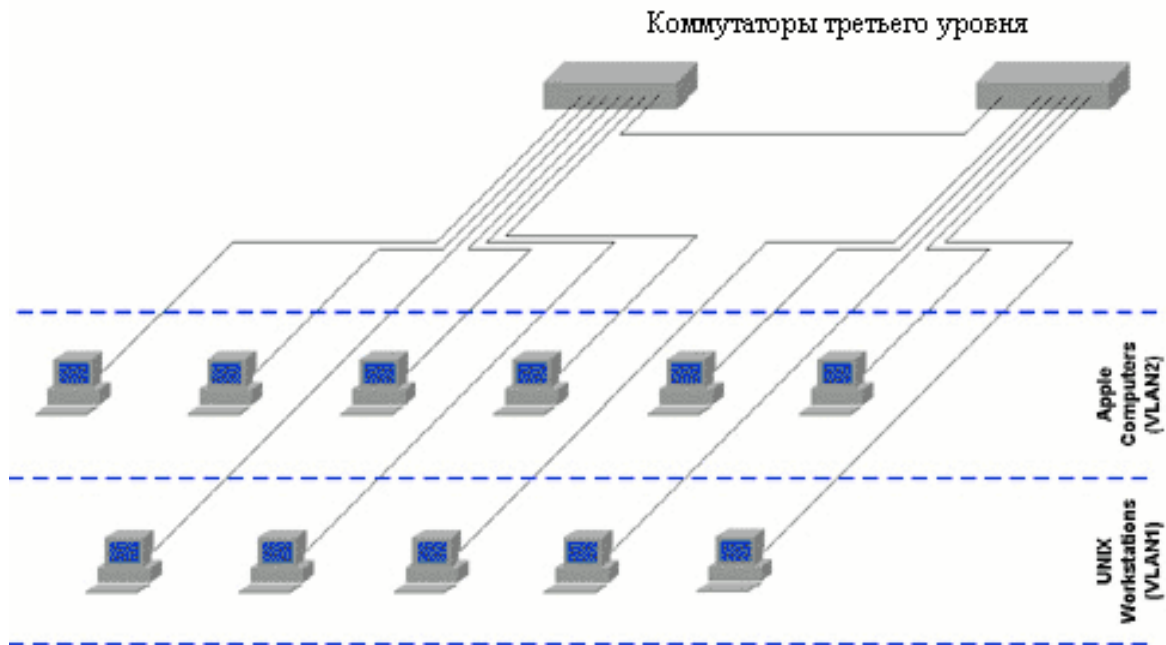


Рис. 2.5 — Структура виртуальной локальной сети организованной на третьем уровне

Использование виртуальных локальных сетей третьего уровня дает три основных преимущества: гибкость, простоту конфигурации и под-

держку взаимодействия между VLAN. Что касается гибкости, при перемещении пользователя в другой сегмент той же подсети многие коммутаторы, поддерживающие создание виртуальных локальных сетей на третьем уровне, отслеживают подобные изменения и не требуют изменения конфигурации коммутатора. Конфигурация VLAN уровня 3 может происходить автоматически, поскольку коммутатор анализирует IP-адреса сетевых станций, соотносимых с каждой VLAN. Таким образом, поддержка VLAN третьего уровня обходится дешевле и требует существенно меньших усилий, чем поддержка других типов сетей.

Еще одно преимущество виртуальных локальных сетей третьего уровня состоит в том, что они поддерживают маршрутизацию. Это означает встроенную поддержку взаимодействия между VLAN. Если коммутатор предусматривает средства транкинга, то его можно подключить к маршрутизатору через один глобальный порт. Если виртуальные локальные сети третьего уровня создаются на базе подсетей IP, то маршрутизатор будет соотносить с каждой подсетью уникальный MAC-адрес отправителя. Это действие позволяет переадресовать трафик с маршрутизатора обратно на коммутатор, но с указанием другого MAC-адреса отправителя (в зависимости от адреса подсети). В результате трафик направляется через коммутатор на его порты, соотносимые с другой VLAN. Такой метод позволяет обойтись одним соединением между маршрутизатором (манипулирующим MAC-адресами) и коммутатором, так как с точки зрения коммутатора оно выглядит как несколько соединений. Между тем, поскольку обычный маршрутизатор не может поддерживать несколько подсетей IP на один порт, он не обеспечивает маршрутизацию через один глобальный путь.

2.5. Особенности работы портов коммутаторов

Каждый порт коммутатора Cisco является либо портом доступа к сети (*access port*), либо магистральным портом (*trunk port*).

Порты доступа принадлежат одной VLAN-сети и не обеспечивают какого-либо идентификационного маркирования фреймов, которые передаются между коммутаторами. Порт доступа также транспортирует трафик, следующий только от той VLAN-сети, которая назначена данному порту. Порты доступа коммутатора второго уровня предназначены для подключения рабочих станций или других неуправляемых коммутаторов.

Магистральные порты предназначены для организации транк-магистралей между двумя коммутаторами. Магистральные порты стандартно являются участниками всех VLAN-сетей, существующих на коммутаторе, и транспортируют трафик для всех этих сетей между коммутаторами. Чтобы различать потоки трафика, магистральный порт с помощью специальных меток (*tags*) маркирует фреймы по мере того, как они передаются между коммутаторами.

Транкинг (*trunking*) — функция, которую необходимо включать на обоих концах канала. Например, если два коммутатора соединены вместе, их порты должны быть сконфигурированы для транкинга, и оба коммутатора необходимо настроить на один и тот же механизм маркирования фреймов (например, *ISL* или *802.1Q*).

Так, например, на рис. 2.6 для связи между двумя коммутаторами показан магистральный канал (транк-магистраль) по которому передаются данные всех виртуальных локальных сетей.

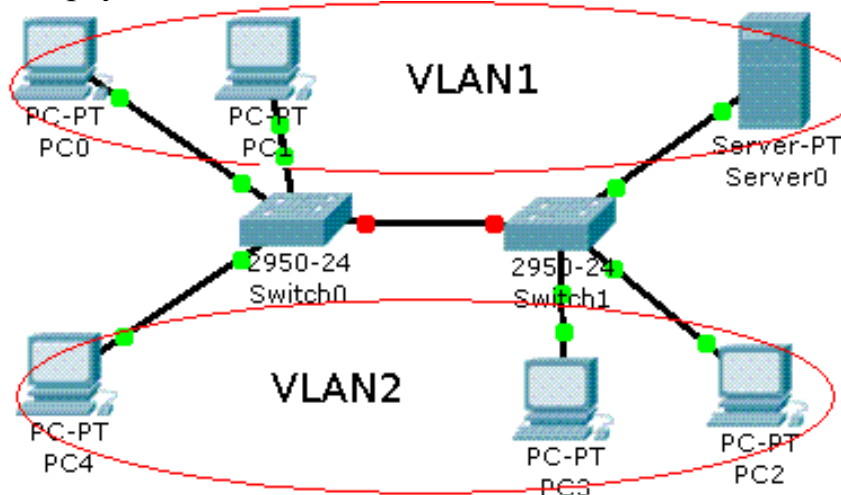


Рис. 2.6 — Структура локальной сети с транк магистралью

2.6. Особенности настройки коммутаторов *Cisco*

При выполнении лабораторной работы студенты выполняют исследование работы аппаратуры сетевой коммутации. Исследование проводится путем настройки структуры локальной сети, построенной на основе коммутаторов второго уровня *Cisco Catalyst 2924 XL*.

2.6.1. Настройка виртуальных локальных сетей по умолчанию

Коммутаторы *Cisco Catalyst* имеют несколько *VLAN*, объявленных по умолчанию. Сеть *VLAN 1* объявлена всегда, и все активные порты сгруппированы в нее по умолчанию. Дополнительно объявлены сети *VLAN 1002...1005* для *FDDI* и *Token Ring*. Эти сети являются частью конфигурации по умолчанию.

2.6.2. Создания виртуальных локальных сетей

Для создания виртуальных локальных сетей на оборудовании *Cisco* следует использовать далее описанную последовательность команд. Рассмотрим порядок команд на примере создания *VLAN 10* путем объединения портов коммутатора с номерами от 17 до 19.

```
#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
(config)#interface VLAN 10
(config-subif)#description student_vlan_10
(config-subif)#exit
(config)#interface fastEthernet 0/17
(config-if)#switchport access vlan 10
(config-if)#exit
(config)#interface fastEthernet 0/18
(config-if)#switchport access vlan 10
(config-if)#exit
(config)#interface fastEthernet 0/19
(config-if)#switchport access vlan 10
(config-if)#exit
(config)#exit
#
```

2.6.3. Создания виртуальных локальных сетей в режиме MULTI

Режим *MULTI VLAN* позволяет сконфигурировать порты, входящие в несколько виртуальных локальных сетей. Рассмотрим порядок команд на примере создания *VLAN 20* и *VLAN 30*, и разрешение порту с номером 15 работать с указанными *VLAN*.

```
#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
(config)#interface VLAN 20
(config-subif)#description student_vlan_20
(config-subif)#exit
(config)#interface VLAN 30
(config-subif)#description student_vlan_30
(config-subif)#exit
(config)#interface fastEthernet 0/15
(config-if)#switchport multi vlan 20,30
(config-if)#switchport mode multi
(config-if)#exit
#
```

3. ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

3.1. Состав лабораторной установки

Лабораторная работа выполняется на коммутаторах второго уровня типа «Cisco 2924 XL» размещенных в одной монтажной стойке типоразмера 19". Упрощенная структурная схема лабораторного стенда изображена на рис. 3.1. Расположение персональных компьютер (сетевых станций) на схеме примерно соответствует их размещению в учебной лаборатории. Коммутаторы *Cisco Catalyst 2924 XL* расположены в средней части стойки. Выше в стойке установлен коммутатор А, а ниже — коммутатор В).

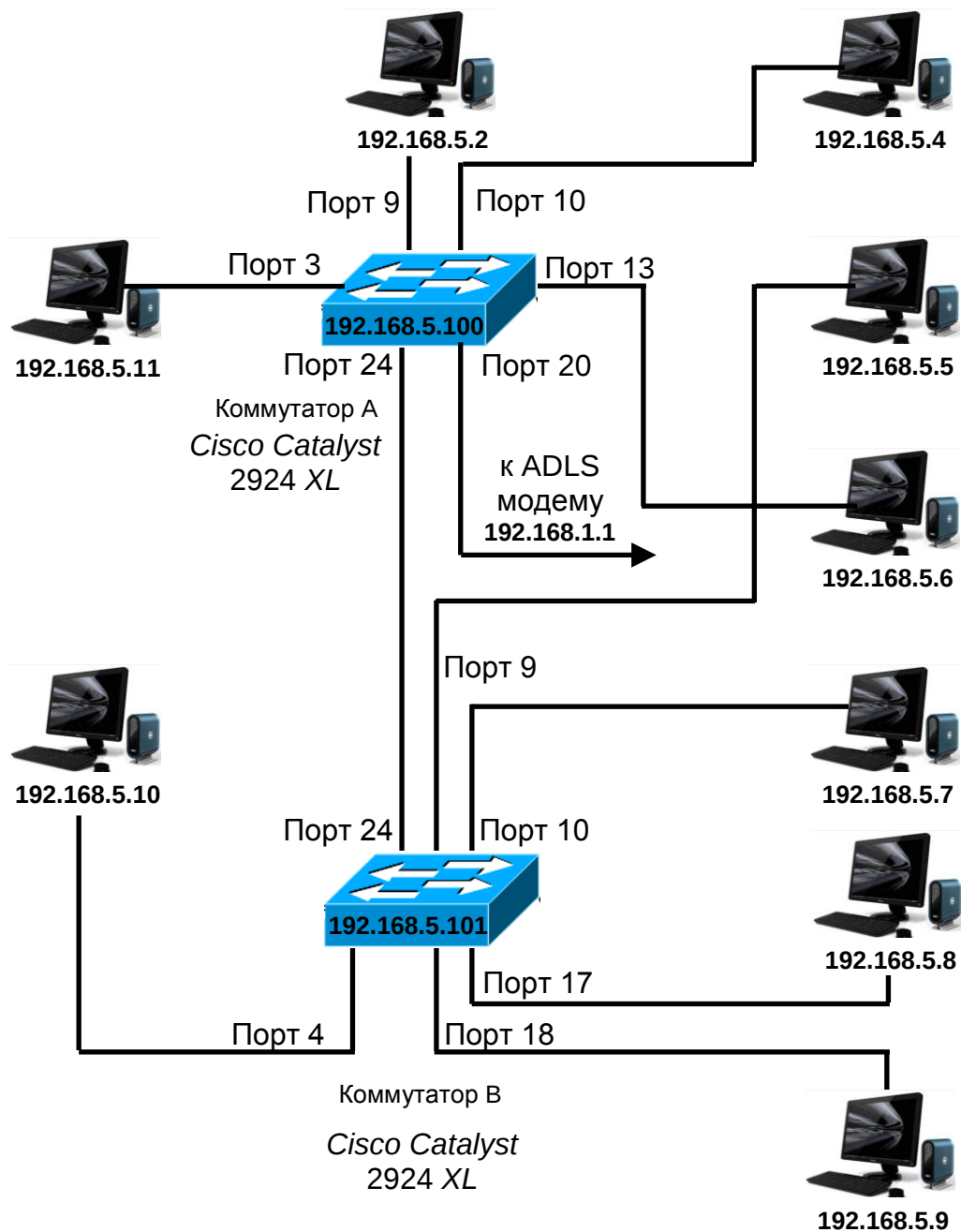


Рис. 3.1 — Структурная схема лабораторного оборудования

4. ПОРЯДОК ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ

1 занятие

4.1. Подключение к коммутатору и определение характеристик его функционирования

1) Конфигурирование коммутатора производится с компьютера, подключенного к любому порту коммутатора сетевым кабелем с помощью утилиты **telnet** операционной системы.

Примечание 1. Все успешные операции по выполнению настройки и определению параметров работы коммутатора следует сохранять в электронном протоколе по выполнению лабораторной работы. Электронный протокол сохраняется в виде файла *MS Word*. Для копирования информации в консольном окне *Windows* в буфер обмена следует нажать правую кнопку мыши на области терминального окна и выбрать команду «**Поместить**», а затем выделить необходимую область мышью или клавишами управления курсором (при нажатой клавише **Shift**) и завершить копирования текстовой области нажатием клавиши **Enter**.

Произвести запуск командной консоли *Windows*. Для этого нажать «**Пуск**» — «**Выполнить**», и в поле ввода команды набрать *CMD*, завершив ввод нажатием кнопки **ОК**.

После чего в командной строке консоли набрать команду запуска **telnet** с указанием *IP*-адреса устройства. В данном случае *IP*-адрес коммутатора 192.168.5.100. После соединения с устройством по протоколу **telnet** следует ввести пароль **123456** и завершить ввод нажатием клавиши **Enter**.

2) Набрать символ **?** в командной строке для того, чтобы вывести на экран список команд управления коммутатором.

3) Определить статуса интерфейсов по портам коммутатора

show interfaces status

Занести в протокол по лабораторной работе сведения о режим дуплекса, скорость подключения и тип физического подключения для всех активных портов коммутатора.

4) Определить *MAC* адреса оборудования подключенного к портам коммутатора

show mac-address-table

Занести в протокол по лабораторной работе таблицу соответствия *MAC* адресов оборудования и портов коммутатора, к которым подключено оборудование.

5) Войти в привилегированный режим администратора, для выполнения настройки устройства. Для этого использовать команду **enable**. На запрос пароля ввести комбинацию символов **123456** и завершить ввод нажатием клавиши **Enter**.

Выход из привилегированного режима при необходимости можно выполнить командой **disable**.

Признак работы коммутатора в привилегированном режиме — наличие символа **#** в подсказке командной строки.

6) Просмотреть текущий рабочий файл конфигурации коммутатора, и сохранить результаты в протокол, используя команду **#show running-config**

Примечание 2. Для просмотра текущего рабочего файла конфигурации, возможно, использовать сокращенный вариант команды **sh ru**, или использовать режим автодополнения, который активируется клавишей **TAB**. Наберите начало команды, например, **show ru** и нажмите клавишу **TAB**, в результате чего набранный текст расширится в **show running-config**.

7) Установить на портах 9...11 коммутатора скорость передачи информации равную 10 Мбит/с.

Для этого войти в режим настройки устройства с помощью команды **#configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.

Подсказка команды показывает, что можно завершить работу в этом режиме по нажатию клавиш **CNTL/Z**.

Далее следует ознакомиться с Примечанием 3 и Примечанием 4, и далее выполнить последовательность команд:

```
(config)#interface fastEthernet 0/9
(config-if)#speed 10
(config-if)#exit
(config)#interface fastEthernet 0/10
(config-if)#speed 10
(config-if)#exit
(config)#interface fastEthernet 0/11
(config-if)#speed 10
(config-if)#exit
(config)#exit
```

Примечание 3. Следует учесть, что после изменения на порту скорости передачи, сетевому адаптеру персонального компьютера может потребоваться принудительное обновление режима работы. Для чего следует в

окне «Сетевые подключения» операционной системы нажать правой кнопкой мыши на требуемом сетевом подключении и выбрать команду «Исправить». После выполнения операции следует закрыть окно исправления соединения.

Если изменение скорости производилось для порта, через который выполнялось управление сетевым коммутатором, то возможно потеря управления после изменения скорости. После выдачи команды «Исправить» на сетевом подключении операционной системы работа сеанса управления восстановится.

Примечание 4. Для повтора ранее набранных команд можно использовать память буфера консоли. Для этого использовать клавиши клавиатуры «стрелка вверх» и «стрелка вниз».

8) После выполнения настройки портов просмотреть полученную конфигурацию портов с помощью команды
#show interfaces status

Кроме того, непосредственно на рабочих станциях, для которых было выполнено изменение режима, следует проверить скорость работы сетевого интерфейса. Для этого в окне «Сетевые подключения» нажать правой кнопкой мыши на значке «Подключение по локальной сети» и выбрать команду «Состояние». В открывшейся панели в закладке «Общие» будет показан режим работы сетевого интерфейса по скорости. Сделать копию закладки «Общие» и сохранить ее для включения в электронном протоколе.

9) Просмотреть MAC-адреса подключенного к коммутатору оборудования. Для этого использовать команду
#show mac-address-table

Результаты работы команд занести в электронный протокол.

4.2. Создание виртуальных локальных компьютерных сетей на коммутаторе А

1) Определить на коммутаторе А наличие настроенных VLAN, для этого использовать команду

#show vlan

2) Выполнить создание виртуальных локальных сетей в соответствии с конфигурацией, заданной в таблице 4.1. Для создания сетей следует использовать последовательность команд (см. п. п. 2.6.2.).

Таблица 4.1 — Конфигурация виртуальных локальных сетей

Коммутатор	A
Наименование <i>VLAN</i>	<i>VLAN 2</i>
Описание <i>VLAN</i>	Ф.И.О. студента. Например, <i>Ivanov S.D.</i>
Номера портов	9...12, 16

3) Проверить правильность создания *VLAN* с помощью команды **#show vlan**.

4) Проверить наличие связи между отдельными компьютерами, входящими в различные *VLAN* с помощью команды *ping*. Связь между компьютерами в пределах одной *VLAN* должна существовать.

5) Результаты тестирования оформить в виде таблицы 4.2.

Таблица 4.2 — Результаты тестирования конфигурации локальной сети

Команда	Адрес источника	Адрес назначения	Результат		Примечание
			Доступность узла да/нет	Среднее время отклика, мс	

6) Определить *MAC*-адреса подключенного к коммутатору **A** оборудования. Для этого использовать команду

#show mac-address-table

7) Определить наличие оборудования, подключенного к коммутатору **A**, и не показанного на схеме рис. 3.1. Сохранить в протокол *MAC*-адрес этого оборудования.

8) Сохранить электронный протокол всех выполненных действий для дальнейшего анализа.

2 занятие

4.3. Создание виртуальных локальных компьютерных сетей на коммутаторе **B**

1) Выполнить подключение к коммутатору **B** с помощью *telnet* протокола (коммутатору **B** имеет IP-адрес 192.168.5.101). На запрос пароля ввести комбинацию символов **123456** и завершить ввод нажатием клавиши **Enter**.

2) Войти в привилегированный режим администратора, для выполнения настройки устройства. Для этого использовать команду **enable**. На запрос пароля ввести комбинацию символов **123456** и завершить ввод нажатием клавиши **Enter**.

3) Определить на коммутаторе **B** наличие настроенных *VLAN*, для этого использовать команду

#show vlan

4) Выполнить создание виртуальных локальных сетей в соответствии с конфигурацией, заданной в табл. 4.3.

При этом следует учитывать, что по умолчанию на коммутаторе существует виртуальная локальная сеть «*VLAN 1*», которая объединяет все активные порты коммутатора.

На первом этапе создать конфигурацию «*Multi VLAN*» для порта, к которому подключен компьютер и с которого производится настройка коммутатора **B**, а затем выполнить конфигурирование остальных портов *VLAN*. Для конфигурирования «*Multi VLAN*» следует использовать последовательность команд (см. п. п. 2.6.3.).

Таблица 4.3 — Конфигурация виртуальных локальных сетей

Коммутатор	B		
Наименование <i>VLAN</i>	<i>VLAN 1, VLAN 2, VLAN 3</i>	<i>VLAN 2</i>	<i>VLAN 3</i>
Описание <i>VLAN</i>	<i>Multi VLAN</i>	Ф.И.О. студента. Например, <i>Ivanov S.D.</i>	Дата выполнения настройки. Например, 2013.03.24
Номера портов	Порт, к которому подключен компьютер с которого производится настройка коммутатора	4, 9...12	17...20

5) Проверить правильность создания *VLAN* с помощью команды **#show vlan**.

6) Проверить наличие связи между отдельными компьютерами, входящими в различные *VLAN* с помощью команды *ping*. Связь между компьютерами в пределах одной *VLAN* должна существовать.

7) Результаты тестирования оформить в виде таблицы 4.2.

8) Просмотреть MAC-адреса подключенного к коммутатору В оборудования. Для этого использовать команду **#show mac-address-table**

9) Сохранить электронный протокол всех выполненных действий для дальнейшего анализа.

5. СОДЕРЖАНИЕ ОТЧЕТА ПО ЛАБОРАТОРНОЙ РАБОТЕ

1) Сформулировать цель лабораторной работы, в которой указать подробно какие зависимости и параметры исследуются в лабораторной работе.

2) В отчете привести отредактированные варианты электронных протоколов, отдельно для коммутаторов **A** и **B**, удалив из протокола явно ошибочные команды.

3) Включить в отчет результаты тестирования локальной сети (см. табл. 4.2) в соответствии с п.п. 4.2. и 4.3.

4) Изобразить структурную схему для созданных при выполнении работы *VLAN*.

5) Используя источники [2], [3], [5] выполнить запись команд настройки транк-магистрали между коммутаторами второго уровня *Cisco Catalyst* в предположении, что магистраль соединяет 24-е порты коммутаторов.

6) Сформулировать выводы по работе, в которых привести подробный анализ экспериментальных данных, и выполнить подробное обсуждение результатов.

6. КОНТРОЛЬНЫЕ ВОПРОСЫ

6.1. Вопросы для допуска к выполнению лабораторной работы

- 1) Охарактеризуйте назначение коммутатора второго уровня.
- 2) Запишите последовательность команд в *telnet* сеансе для создания VLAN.
- 3) Запишите последовательность команд в *telnet* сеансе для определения статуса интерфейсов портов.
- 4) Охарактеризуйте последовательность действий для изменения скорости работы интерфейса с заданным номером.
- 5) Охарактеризуйте особенности лабораторного оборудования на структурном уровне.
- 6) Охарактеризуйте принцип управления коммутатором на примере какой-либо команды для *telnet* подключения.
- 7) Запишите последовательность команд для подключения коммутатору по *telnet* протоколу.
- 8) Запишите и охарактеризуйте команды, которые необходимо использовать для входа в привилегированный режим администратора.
- 9) Охарактеризуйте первый и второй уровни модели взаимодействия открытых систем.
- 10) Поясните особенности размещения портов и элементов управления на корпусе устройства.

6.2. Вопросы для защиты лабораторной работы

- 1) Охарактеризуйте принципы реализации коммутации в локальных сетях.
- 2) Охарактеризуйте основные функции коммутации второго уровня.
- 3) Охарактеризуйте основные уровни модели открытых систем OSI.
- 4) Охарактеризуйте режимы работы коммутаторов локальных сетей.
- 5) Сформулируйте основное назначение виртуальных локальных сетей.
- 6) Охарактеризуйте принципы работы VLAN на базе портов.
- 7) Охарактеризуйте принципы работы VLAN на основе меток в дополнительном поле кадра.
- 8) Охарактеризуйте принципы создания виртуальных локальных сетей на третьем уровне.
- 9) Охарактеризуйте назначение и принципы организации транк-магистралей.
- 10) Разработайте алгоритм конфигурирования порта в режиме «*Multi VLAN*» для доступа к VLAN 10, 11 и 12. Алгоритм составить в текстовом виде.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Чернега, В.С. Компьютерные сети / В.С. Чернега, Б. Платтнер. — Севастополь: Изд-во СевНТУ, 2006. — 500 с.
2. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. — СПб.: Питер, 2006. — 945 с.
3. Воплощение в реальность / Гилберт Хелд. — Режим доступа: <http://www.osp.ru/lan/1998/06/133532/> (дата обращения: 24.12.2018).
4. Виртуальные локальные сети VLAN - описание, принцип работы и настройка // Easy-Network — Режим доступа: <https://easy-network.ru/27-urok-17.html> (дата обращения: 02.02.2020)
5. Установка и настройка коммутаторов CISCO CATALYST серий 2900XL и 3500 (Часть 2). — Режим доступа: http://network.xsp.ru/4_4.php (дата обращения: 02.02.2020).

ИССЛЕДОВАНИЕ СЕТЕВОГО КОММУТАТОРА ВТОРОГО УРОВНЯ

*Учебно-методическое пособие
по выполнению лабораторной работы*

Составитель: Савочкин Александр Анатольевич

Редактор: к. т. н., доцент В. Г. Слёзкин

Изд. № 194/2020. Объем 1,5 п.л.

РИИЦМ ФГАОУ ВО «Севастопольский государственный университет»