

Лабораторная работа №3 Виртуальные локальные сети

Цель: изучить принципы организации и настройки виртуальных локальных сетей на базе коммутаторов Cisco.

1. Теоретические сведения

Виртуальная локальная сеть (Virtual Local Area Network, VLAN) представляет собой коммутируемый сегмент сети, который логически выделен по выполняемым функциям, рабочим группам или приложениям, вне зависимости от физического расположения пользователей. Виртуальные локальные сети имеют все свойства физических локальных сетей, но рабочие станции можно группировать, даже если они физически расположены не в одном сегменте, т.к. любой порт коммутатора можно настроить на принадлежность определенной VLAN. При этом одноадресный, многоадресный и широковещательный трафик будет передаваться только между рабочими станциями, принадлежащими одной VLAN. Каждая VLAN рассматривается как логическая сеть, т.е. кадры, предназначенные станциям, которые не принадлежат данной VLAN, должны передаваться через маршрутизирующее устройство (маршрутизатор или коммутатор 3-го уровня). Таким образом, с помощью виртуальных локальных сетей решается проблема ограничения области передачи широковещательных кадров и вызываемых ими последствий, которые существенно снижают производительность сети, вызывают широковещательные штормы.

Типы VLAN:

- **VLAN на основе портов (Port-based VLAN)** — каждый порт коммутатора назначается в определенную VLAN и любое сетевое устройство, подключенное в данный порт, будет находиться в назначенной виртуальной сети;
- **VLAN на основе MAC-адресов (MAC-based VLAN)** — членство в VLAN основывается на MAC-адресе рабочей станции. В этом случае на коммутаторе необходимо создать привязку MAC-адресов всех устройств к VLAN;
- **VLAN на основе портов и протоколов IEEE 802.1v** — тип протокола используется для определения членства в VLAN;
- **VLAN на основе стандарта IEEE 802.1Q** — поле принадлежности VLAN, интегрируется в структуру кадра Ethernet, что позволяет передавать данную информацию по сети. Преимуществом является гибкость настройки, использование не только на одном коммутаторе, но и в пределах всей коммутируемой сети; возможность использования оборудования разных производителей при организации сети. Данный тип VLAN используется чаще остальных.

Существуют два метода назначения порта в определенную VLAN:

- **статическое назначение** — когда принадлежность порта VLAN задается администратором в процессе настройки;
- **динамическое назначение** — когда принадлежность порта VLAN определяется в ходе работы коммутатора с помощью процедур, описанных в специальных стандартах, таких, например, как IEEE 802.1X. При использовании IEEE 802.1X для получения доступа к порту коммутатора пользователь проходит аутентификацию на сервере RADIUS. По результатам аутентификации порт коммутатора помещается в ту или иную VLAN.

Коммутаторы Cisco поддерживают стандарт IEEE 802.1Q, используя при этом два типа портов:

- **Access Port** применяется для подключения конечных устройств (компьютеры, ноутбуки, IP-телефон или видеокамера). Во **входящих Access-портах** в кадры внедряется тег с идентификатором VLAN, к которой принадлежит данный порт. В **исходящих Access-портах** осуществляется сравнение идентификатора VLAN порта и идентификатора, содержащегося в теге кадра. Если они не совпадают от кадр фильтруется (отбрасывается коммутатором). Если совпадают, то из кадра извлекается тег, после чего кадр продвигается на конечное устройство;
- **Trunk Port** (магистральный порт) применяется для соединений между коммутаторами. Trunk-порты коммутатора работают с тегированными кадрами, сверяя идентификатор VLAN в теге кадра со списком разрешенных VLAN, который прикреплен к порту. Если идентификатор в теге не обнаруживается в списке, то такой пакет фильтруется. В противном случае, входящий Trunk-порт впускает пакет в коммутатор, а исходящий Trunk-порт выпускает наружу.

Реализация VLAN в коммутаторах позволяет структурировать сеть, обеспечить безопасность сети, объединить разрозненные физические сегменты сети, уменьшить размер домена коллизий и вероятность широковещательных штормов.

2. Задание

2.1. Обучающая часть

Настройка VLANs на основе одного коммутатора. Настройка сети с несколькими VLAN и одним коммутатором заключается в определении идентификаторов VLAN на коммутаторе и присоединении портов в обозначенным VLAN.

1. В СРТ на основе коммутатора 2960 постройте сеть с физической топологией, показанной на рисунке 1.

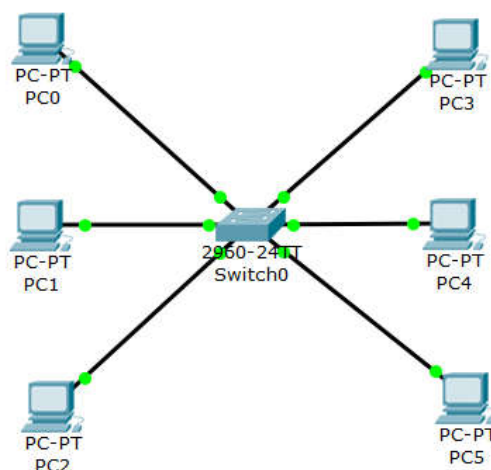


Рис. 1. Физическая топология локальной сети

2. С помощью VLAN разделим сеть на три сегмента, которые входят в разные домены коллизий и не могут обмениваться друг с другом трафиком на канальном уровне модели OSI (рис. 2).

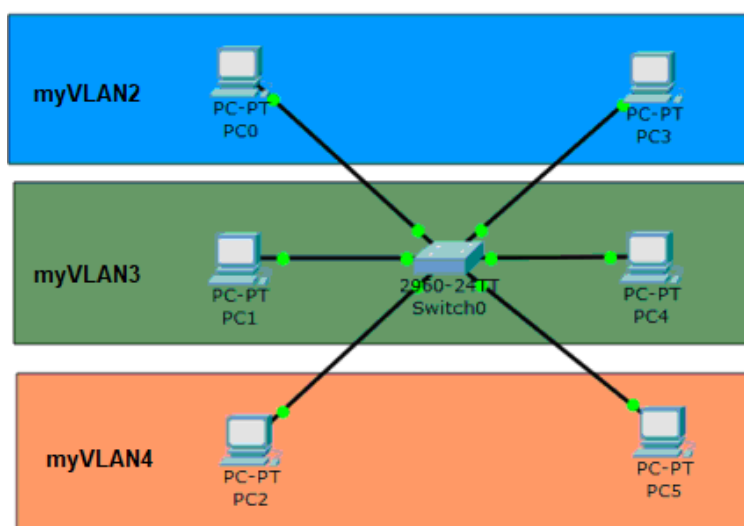


Рис. 2. Логическая топология локальной сети

3. Щелкните по коммутатору и в диалоговом окне выберите вкладку CLI (command line interface).
4. Войдите в режим глобального конфигурирования. По умолчанию все порты коммутатора принадлежат VLAN с VID=1.
5. Сначала определим новые VLAN, задав их VID. С помощью команды **vlan 2** создайте VLAN с идентификатором 2.
6. Подсказка командной строки станет такой: **Switch(config-vlan)#**
7. Задайте имя VLAN с помощью команды **name myVLAN2**. Выйдите из режима конфигурирования VLAN, выполнив команду **exit**.
8. Аналогичным образом создайте VLAN с идентификаторами 3 и 4, и именами myVLAN3, myVLAN4 соответственно.

9. Войдите в привилегированный режим и с помощью команды **show vlan brief** получите сведения об имеющихся на коммутаторе VLAN с распределением портов между ними.
10. Назначьте порты коммутатора во VLAN в соответствии с логической топологией (рис. 2). К myVLAN2 с идентификатором 2 нужно отнести порты fa0/1 и fa0/4, заданные физической топологией сети для компьютеров PC0 и PC3. Войдите в режим конфигурирования интерфейса с помощью команды: **interface fastEthernet 0/1**. Подсказка примет вид:
Switch(config-if)#
11. Далее выполните конфигурирование интерфейса fa0/1. Назначьте тип порта текущего интерфейса с помощью команды: **switchport mode access**. Данная команда задает тип порта access для интерфейса fa0/1.
12. С помощью команды **switchport access vlan 2** прикрепите порт интерфейса fa0/1 к VLAN с идентификатором 2. Выйдите из режима настройки интерфейса fa0/1 с помощью команды **exit**.
13. Повторите действия, описанные в п.10-12, чтобы назначить порту интерфейса fa0/4 тип access и прикрепить его к VLAN с VID=2.
14. В привилегированном режиме выполните команду **show vlan brief**. Какие интерфейсы (порты) сопоставлены с myVLAN2?
15. Выполните аналогичные действия, чтобы отнести интерфейсы fa0/2 и fa0/5 к myVLAN3, а fa0/3 и fa0/6 к myVLAN4.
16. Статически назначьте IP-адреса компьютеров так, чтобы они все принадлежали одной сети.
17. С помощью утилиты **ping** проверьте прохождение пакетов между конечными устройствами сети. В каких случаях продвижение пакетов не происходит и ping дает отрицательный результат?
18. В привилегированном режиме с помощью команды **show mac-address-table** отследите процесс формирования таблицы коммутации. Примечание: новые записи в таблице коммутации формируются динамически, по мере передачи пакетов с разных компьютеров.
19. Сохраните проект CPT в файле, имя которого удовлетворяет шаблону:
LabNet-3(Фамилия_группа)-task-1-1.pkt.
20. Работоспособность Вашего проекта продемонстрируйте преподавателю.
21. Загрузите проект на качестве отчета о выполнении первой обучающей части задания на сайт eluniver.ugrasu.ru.

Настройка VLANs на основе нескольких коммутаторов

22. Создайте новый проект CPT и на основе двух коммутаторов 2960 постройте сеть с показанную на рисунке 3. Коммутаторы могут быть физически расположены на разных этажах. Использование так называемых trunk-портов позволяет передавать трафик между конечными устройствами, входящими в одну VLAN, без дополнительных физических соединений. Как правило, используется одна высокоскоростная линия связи, порты которой имеют тип trunk.

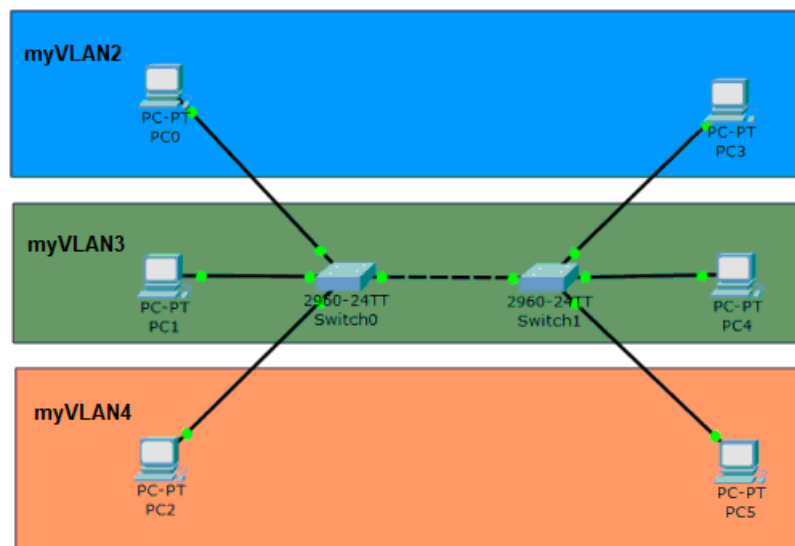


Рис. 3. Организация локальной сети на основе двух коммутаторов

- 23.С помощью настройки коммутаторов организуйте в сети три логических сегмента VLAN: myVLAN2, myVLAN3, myVLAN4.
- 24.Используйте порт GigabitEthernet на обоих коммутаторах, чтобы организовать линию связи между ними. В СРТ принято соединять устройства, работающие на одном уровне модели OSI кросс-кабелем. Поэтому выполните соединение коммутаторов кросс-кабелем, используя порты Gig0/1.
- 25.Для настройки trunk-порта выполните следующую настройку с помощью закладки CLI. Войдите в режим глобального конфигурирования, а затем с помощью команды **interface gigabitEthernet 0/1** в режим конфигурирования интерфейса Gig0/1.
- 26.Установите тип порта trunk с помощью команды **switchport mode trunk**.
- 27.Разрешите передавать через trunk-порт трафик всех Ваших VLAN с помощью команды: **switchport trunk allowed vlan 2,3,4**
- 28.Войдите в привилегированный режим и с помощью **show running-config** посмотрите настройки порта Gig0/1.
- 29.Действия п.4-7 выполните для настройки trunk-порта второго коммутатора.
- 30.В соответствии с топологией, показанной на рисунке 3, на обоих коммутаторах настройте access-порты.
- 31.Статически назначьте IP-адреса компьютеров так, чтобы они все принадлежали одной сети.
- 32.С помощью утилиты **ping** проверьте прохождение пакетов между конечными устройствами сети. В каких случаях продвижение пакетов не происходит и ping дает отрицательный результат?
- 33.На одном из коммутаторов перенастройте trunk-порт так, чтобы он мог передавать трафик только одной VLAN. Как изменилось прохождение пакетов между узлами?
- 34.Сохраните проект СРТ в файле, имя которого удовлетворяет шаблону:
LabNet-3(Фамилия_группа)-task-1-2.pkt.
- 35.Работоспособность Вашего проекта продемонстрируйте преподавателю.

36. Загрузите проект на качестве отчета о выполнении второй обучающей части задания на сайт eluniver.ugrasu.ru.

2.2. Самостоятельная работа

Построение локальной сети предприятия. Компьютерная сеть предприятия должна находиться на трех этажах здания. На каждом этаже нужно использовать отдельный коммутатор. Дайте название коммутаторам в соответствии с шаблоном:

<Фамилия студента>-Sw<номер коммутатора>.

На первом этаже расположен операционный зал для обслуживания клиентов. На втором и третьем этажах находятся две службы: «служба 1» находится в левом крыле, а «служба 2» - в правом. На основе VLAN разделите сеть на три сегмента: операционный зал (operating room - **OR**), «служба1» (**service-1**), «служба 2» (**service-2**). Для VLAN «службы 1» на коммутаторах назначьте IP-адрес и на основе протокола SSH организуйте их удаленное управление. Убедитесь, что из других VLAN управление коммутаторами невозможно. Для именования VLAN используйте шаблон:

ФИО (аббревиатура на латинице)-<одно из значений: OR, service-1, service-2>.

При настройке trunk-портов коммутаторов обратите внимание, что трафик рабочих станций операционного зала не должен покидать первого этажа, а трафик сетевых устройств «службы 2» не должен проникать на первый этаж.

1. Сохраните проект CPT в файле, имя которого удовлетворяет шаблону:
LabNet-3(Фамилия_группа)-task-2.pkt.
2. Работоспособность Вашего проекта продемонстрируйте преподавателю.
3. Загрузите проект на качестве отчета о выполнении **Самостоятельной работы** на сайт eluniver.ugrasu.ru.

3. Подготовка отчета, представление и оценка работы

Структура отчета

В качестве отчета по каждой части задания необходимо предоставить готовый проект Cisco Packet Tracer. В рабочей области проекта нужно текстовыми метками указать логины и пароли, которые были задействованы при настройке или требуются для использования какого-либо устройства или сетевой службы. В отчете (проекте Cisco Packet Tracer) оценивается точность названий, для которых в задании определен шаблон или уникальное значение, параметры настройки сетевого оборудования.

Загрузку проектов на сайт Eluniver следует выполнять после демонстрации всех частей задания преподавателю. Желательно загружать все проекты одновременно либо отдельными файлами, либо общим архивом.

Представление и защита работы

Представлением работы является ее демонстрация преподавателю. Каждый проект может быть представлен отдельно от других частей задания. В ходе представления преподаватель может задать вопрос по любому пункту

соответствующей части задания или попросить выполнить какие-либо построения на основе навыков, полученных при разработке проекта. Оценка за представление задания выставляется на основе работоспособности проекта, правильности ответа студента на вопросы по проекту и готовности выполнить дополнительное задание без использования методического материала.

Защита работы заключается в ответе на два контрольных вопроса, выбранных произвольно преподавателем из списка контрольных вопросов (п.4). Оценивается детальность и точность ответа. Во время ответа пользоваться методическим материалом нельзя. Возможность ответа на контрольные вопросы дается студенту после представления всех частей задания.

Структура оценки практической работы

№	Вид оценки	Максимальный балл
1.	Проект «Обучающая часть» (два проекта)	10+15
2.	Проект «Самостоятельная работа»	25
3.	Отчет «Обучающая часть» (два проекта)	5+5
4.	Отчет «Самостоятельная работа»	10
5.	Контрольный вопрос 1	15
6.	Контрольный вопрос 2	15
Итого:		100

4. Контрольные вопросы

1. Дайте определение виртуальной локальной сети.
2. На каком уровне модели OSI определено понятие VLAN?
3. Какие типы VLAN Вам известны?
4. Каким образом информация о VLAN передается по сети?
5. Что представляет собой тег стандарта 802.1Q?
6. Дайте определение входного порта коммутатора.
7. Дайте определение выходного порта коммутатора?
8. Что представляет собой операция по извлечению тега? Когда она выполняется?
9. Какие типа портов коммутатора можно определить при настройке коммутатора?
10. Какие команды коммутаторов Cisco позволяют создать несколько VLAN в сети?
11. Можно ли назначить VLAN IP-адрес?
12. Как подключиться в коммутатору по протоколу telnet когда в сети определено несколько VLAN?
13. Как настроить trunk-порт коммутатора?
14. Чем отличается работа trunk-порта от порта типа access?
15. Каким типом кабеля соединяются trunk- и access-порты в СРТ? Почему?
16. В разработке...