МГТУ им. Н. Э. Баумана

Кафедра «Системы обработки информации и управления»

Методические указания к лабораторной работе 3 по дисциплине

Сети и телекоммуникации

Для студентов 3-го курса кафедры ИУ5

Разработали:

ст. преподаватель Антонов А. И.

Москва 2023 г.

Оглавление

Лабораторная работа №3. «Применение VLAN при проектировании и анализе локальных вычислительных сетей в пакете Cisco Packet Tracer».

1.Цель лабораторной работы.

Изучение и закрепление принципов и правил создания и настройки VLAN внутри локальных вычислительных сетей. Изучение программы Cisco Packet Tracer 8.2., приобретение практических навыков проектирования и моделирования работы сети, а также оценки принятых проектных решений.

2. Теоретическая часть.

2.1. Протокол ARP

Любое устройство, подключенное к локальной сети (Ethernet, FDDI и т.д.), имеет уникальный физический сетевой адрес, заданный аппаратным образом. 6-байтовый Ethernet-адрес выбирает изготовитель сетевого интерфейсного оборудования из выделенного для него по лицензии адресного пространства. Если у машины меняется сетевой адаптер, то меняется и ее MAC-адрес.

4-байтовый IP-адрес задает менеджер сети с учетом положения машины в сети Интернет. Если машина перемещается в другую часть сети Интернет, то ее IP-адрес должен быть изменен. Преобразование IP-адресов в сетевые выполняется с помощью arp-таблицы. Каждая машина сети имеет отдельную ARP-таблицу для каждого своего сетевого адаптера. Не трудно видеть, что существует проблема отображения физического адреса (6 байт для Ethernet) в пространство сетевых IP-адресов (4 байта) и наоборот.

Протокол ARP (address resolution protocol, RFC-826) решает именно эту проблему - преобразует ARP- в MAC-адреса.

Рассмотрим процедуру преобразования адресов при отправлении сообщения. Пусть прикладная программа одной ЭВМ отправляет сообщение другой. Прикладной программе IP-адрес места назначения обычно известен. Для определения Ethernet-адреса просматривается ARP-таблица. Если для требуемого IP-адреса в ней присутствует MAC-адрес, то формируется и посылается соответствующий пакет.

Если же с помощью ARP-таблицы не удается преобразовать адрес, то выполняется следующее:

1. Всем машинам в сети посылается пакет с ARP-запросом (с широковещательным MAC-адресом места назначения).
2. Исходящий IP-пакет ставится в очередь.

Каждая машина, принявшая ARP-запрос, в своем ARP-модуле сравнивает собственный IP-адрес с IP-адресом в запросе. Если IP-адрес совпал, то прямо по MAC-адресу отправителя запроса посылается ответ, содержащий как IP-адрес ответившей машины, так и ее MAC-адрес. После получения ответа на свой ARP-запрос машина имеет требуемую информацию о соответствии IP и MAC-адресов, формирует соответствующий элемент ARP-таблицы и отправляет IP-пакет, ранее поставленный в очередь. Если же в сети нет машины с искомым IP-адресом, то ARP-ответа не будет и не будет записи в ARP-таблицу. Протокол IP будет уничтожать IP-пакеты, предназначенные для отправки по этому адресу.

Протоколы верхнего уровня не могут отличить случай повреждения в среде ethernet от случая отсутствия машины с искомым IP-адресом. Во многих реализациях в случае, если IP-адрес не принадлежит локальной сети, внешний порт сети (gateway) или маршрутизатор откликается, выдавая свой физический адрес (режим прокси-ARP).

Функционально, ARP делится на две части. Одна - определяет физический адрес при посылке пакета, другая отвечает на запросы других машин. ARP-таблицы имеют динамический характер, каждая запись в ней "живет" определенное время после чего удаляется. Менеджер сети может осуществить запись в ARP-таблицу, которая там будет храниться "вечно". ARP-пакеты вкладываются непосредственно в ethernet-кадры. Формат ARP-пакета показан на рис. 1.

Рис. 1. Формат пакета ARP

2.2. Понятие VLAN

VLAN **(**Virtual Local Area Network**)** – это виртуальные локальные компьютерные сети, которые существуют на втором уровне модели OSI. То есть, VLAN можно настроить на коммутаторе второго уровня. Если смотреть на VLAN, абстрагируясь от понятия «виртуальные сети», то можно сказать, что VLAN – это просто метка в кадре, который передается по сети. Метка содержит номер VLAN (его называют VLAN ID или VID), – на который отводится 12 бит, то есть, VLAN может нумероваться от 0 до 4095. Первый и последний номера зарезервированы, их использовать нельзя. Обычно, рабочие станции о VLAN ничего не знают, управление VLAN выполняют коммутаторы. На портах коммутаторов указывается в каком VLAN они находятся. В зависимости от этого весь трафик, который выходит через порт помечается меткой, то есть VLAN. Таким образом каждый порт имеет PVID (*port vlan identifier*). Этот трафик может в дальнейшем проходить через другие порты коммутатора(ов), которые находятся в этом VLAN и не пройдут через все остальные порты. В итоге, создается изолированная среда (подсеть), которая без дополнительного устройства (маршрутизатора) не может взаимодействовать с другими подсетями.

Зачем нужен VLAN ?

- Возможность построения сети, логическая структура которой не зависит от физической. То есть, топология сети на канальном уровне строится независимо от географического расположения составляющих компонентов сети.

- Возможность разбиения одного широковещательного домена на несколько широковещательных доменов. То есть, широковещательный трафик одного домена не проходит в другой домен и наоборот. При этом уменьшается нагрузка на сетевые устройства.
- Возможность обезопасить сеть от несанкционированного доступа. То есть, на канальном уровне кадры с других VLAN будут отсекаться портом коммутатора независимо от того, с каким исходным IP-адресом инкапсулирован пакет в данный кадр.
- Возможность применять политики на группу устройств, которые находятся в одном VLAN.
- Возможность использовать виртуальные интерфейсы для маршрутизации.

Примеры использования VLAN

- *Объединение в единую сеть компьютеров, подключенных к разным коммутаторам*. Допустим, у вас есть компьютеры, которые подключены к разным свитчам, но их нужно объединить в одну сеть. Одни компьютеры мы объединим в виртуальную локальную сеть *VLAN 1*, а другие — в сеть *VLAN 2*. Благодаря функции VLAN компьютеры в каждой виртуальной сети будут работать, словно подключены к одному и тому же свитчу. Компьютеры из разных виртуальных сетей *VLAN 1* и *VLAN 2* будут невидимы друг для друга.

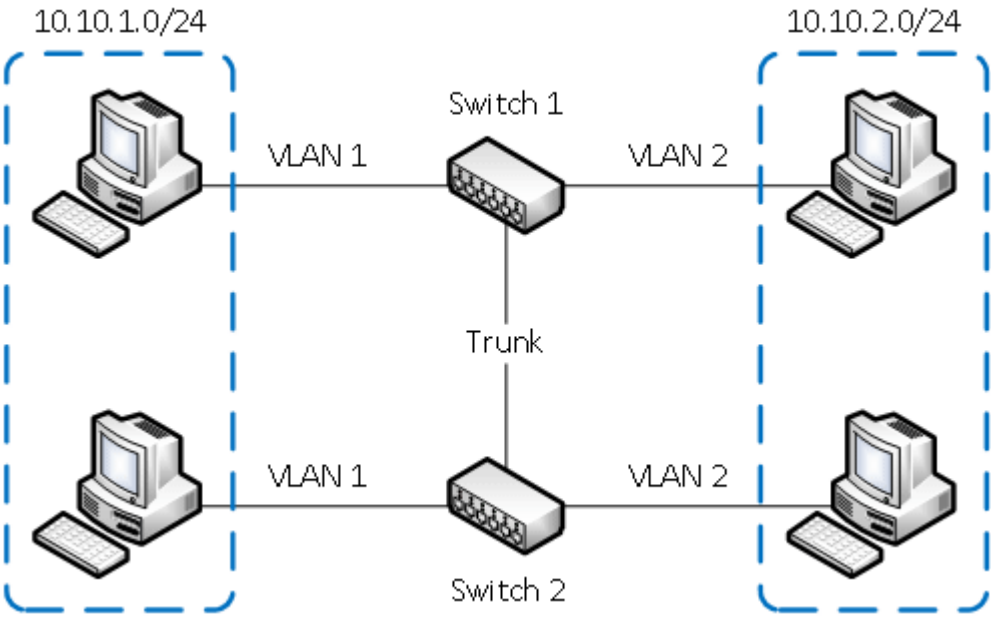

Рис. 2. *Объединение в единую сеть компьютеров, подключенных к разным коммутаторам*

- *Разделение в разные подсети компьютеров, подключенных к одному коммутатору.* На рисунке компьютеры физически подключены к одному свитчу, но разделены в разные виртуальные сети *VLAN 1* и *VLAN 2*. Компьютеры из разных виртуальных подсетей будут невидимы друг для друга.

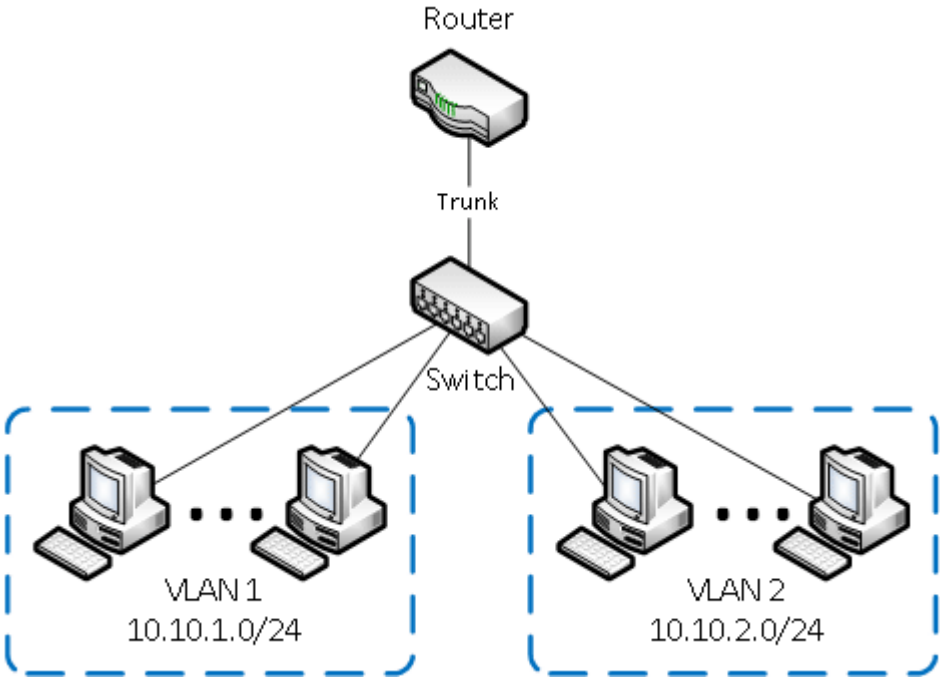

Рис. 3. *Разделение в разные подсети компьютеров, подключенных к одному коммутатору*

- *Разделение гостевой Wi-Fi сети и Wi-Fi сети предприятия.* На рисунке к роутеру подключена физически одна Wi-Fi точка доступа. На точке созданы две виртуальные Wi-Fi точки с названиями HotSpot и Office. К HotSpot будут подключаться по Wi-Fi гостевые ноутбуки для доступа к интернету, а к Office — ноутбуки предприятия. В целях безопасности необходимо, чтобы гостевые ноутбуки не имели доступ к сети предприятия. Для этого компьютеры предприятия и виртуальная Wi-Fi точка Office объединены в виртуальную локальную сеть *VLAN 1*, а гостевые ноутбуки будут находиться в виртуальной сети *VLAN 2*. Гостевые ноутбуки из сети *VLAN 2* не будут иметь доступ к сети предприятия *VLAN 1*.

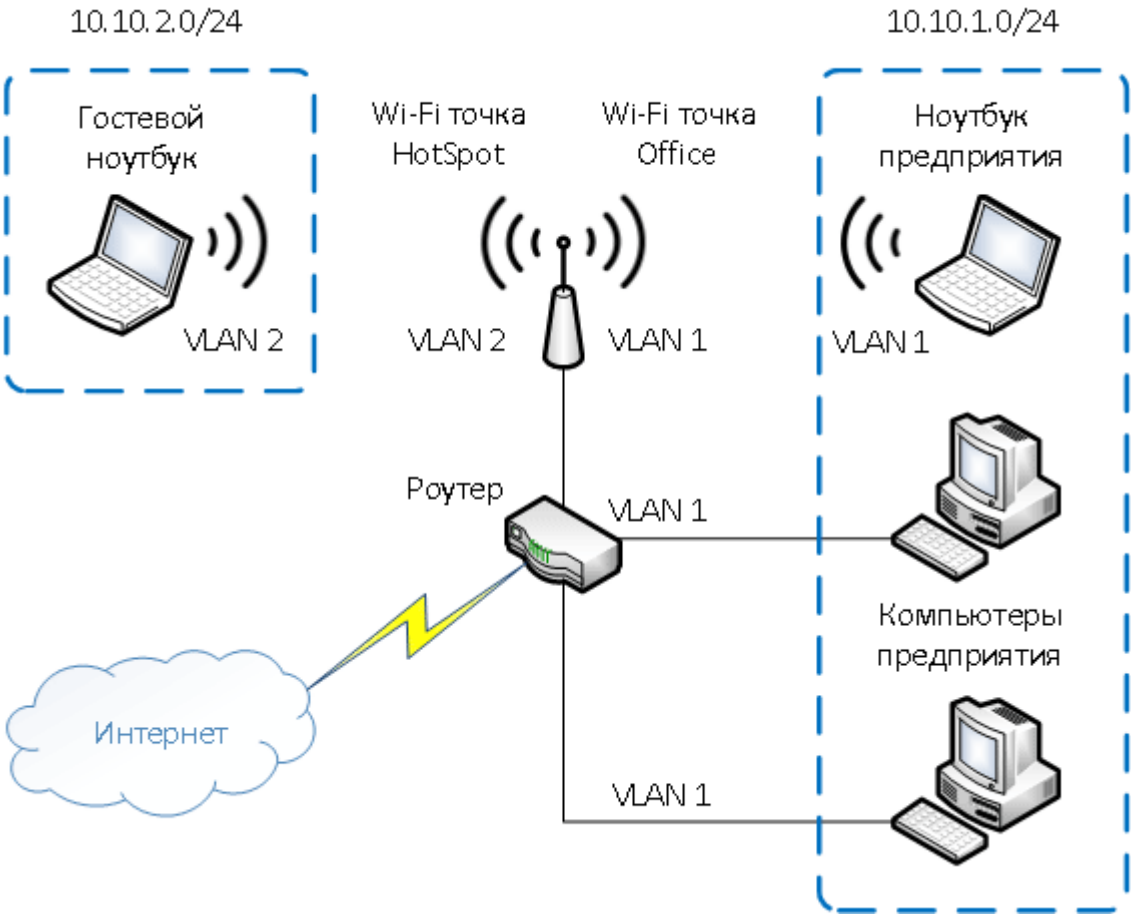

Рис. 4. *Разделение гостевой Wi-Fi сети и Wi-Fi сети предприятия при помощи VLAN*

Достоинства использования VLAN

- Гибкое разделение устройств на группы
- Как правило, одному VLAN соответствует одна подсеть. Компьютеры, находящиеся в разных VLAN, будут изолированы друг от друга. Также можно объединить в одну виртуальную сеть компьютеры, подключенные к разным коммутаторам.
- Уменьшение широковещательного трафика в сети
- Каждый VLAN представляет отдельный широковещательный домен. Широковещательный трафик не будет транслироваться между разными VLAN. Если на разных коммутаторах настроить один и тот же VLAN, то порты разных коммутаторов будут образовывать один широковещательный домен.
- Увеличение безопасности и управляемости сети
- В сети, разбитой на виртуальные подсети, удобно применять политики и правила безопасности для каждого VLAN. Политика будет применена к целой подсети, а не к отдельному устройству.
- Уменьшение количества оборудования и сетевого кабеля
- Для создания новой виртуальной локальной сети не требуется покупка коммутатора и прокладка сетевого кабеля. Однако вы должны использовать более дорогие управляемые коммутаторы с поддержкой VLAN.

Тэгированные и нетэгированные порты

Когда порт должен уметь принимать или отдавать трафик из разных VLAN, то он должен находиться в тэгированном или транковом состоянии, иначе говоря, в trunk режиме. Понятия транкового порта и тэгированного порта одинаковые. Транковый или тэгированный порт может передавать как отдельно указанные VLAN, так и все VLAN по умолчанию, если не указано другое. Если порт нетэгирован, то он может передавать только один VLAN (родной или Native VLAN). Если на порту не указано в каком он VLAN, то подразумевается, что он в нетэгированном состоянии в первом VLAN (VID 1).

Разное оборудование настраивается по-разному в данном случае. Для одного оборудования нужно на физическом интерфейсе указать в каком состоянии находится этот интерфейс, а на другом в определенном VLAN необходимо указать какой порт как позиционируется – с тэгом или без тэга. И если необходимо, чтобы этот порт пропускал через себя несколько VLAN, то в каждом из этих VLAN нужно прописать данный порт с тэгом. На оборудовании

Cisco Systems мы просто указываем какие порты какими VLAN нетэгированы (находятся в режиме *access*) и какие порты находятся в тэгированном состоянии (находятся в режиме *trunk*).

Для настройки портов в режим trunk созданы специальные протоколы. Один из таких имеет стандарт IEEE 802.1Q. Это международный стандарт, который поддерживается всеми производителями и чаще всего используется для настройки виртуальных сетей. Кроме того, разные производители могут иметь свои протоколы передачи данных. Например, Cisco создала для свого оборудования протокол ISL (*Inter Switch Link*).

Межвлановская маршрутизация

Что такое межвлановская маршрутизация? Это обычная маршрутизация подсетей. Разница только в том, что каждой подсети соответствует какой-то VLAN на втором уровне. Что это значит. Допустим у нас есть два VLAN: VID = 10 и VID = 20. На канальном уровне эти VLAN осуществляют разбиение одной сети на две подсети. Хосты, которые находятся в этих подсетях не видят друг друга. То есть, трафик полностью изолирован. Для того, чтобы хосты могли взаимодействовать между собой, необходимо смаршрутизировать трафик этих VLAN. Для этого нам необходимо на сетевом уровне каждому из VLAN присвоить интерфейс, то есть прикрепить к ним IP-адрес. Например, для VID = 10 IP address будет 10.0.10.1/24, а для VID = 20 IP address – 10.0.20.1/24. Эти адреса будет дальше выступать в роли шлюзов для выхода в другие подсети. Таким образом, мы можем трафик хостов с одного VLAN маршрутизировать в другой VLAN. Что дает нам маршрутизация VLAN по сравнению с простой маршрутизацией подсетей без использования VLAN? А вот что:

- Возможность стать членом другой подсети на стороне клиента заблокирована. То есть, если хост находится в определенном VLAN, то даже, если он поменяет себе адресацию с другой подсети, он все равно останется в том VLAN, котором он был. Это значит, что он не получит доступа к другой подсети. А это в свою очередь обезопасит сеть от «плохих» клиентов.
- Мы можем поместить в VLAN несколько физических интерфейсов коммутатора. То есть, у нас есть возможность на коммутаторе третьего уровня сразу настроить маршрутизацию, подключив к нему клиентов сети, без использования внешнего маршрутизатора. Либо мы можем использовать внешний маршрутизатор, подключенный к коммутатору второго уровня, на котором настроены VLAN, и

создать столько вспомогательных интерфейсов (subinterface) на порте маршрутизатора, сколько всего VLAN он должен маршрутизировать.

- Очень удобно между первым и третьим уровнями использовать второй уровень в виде VLAN. Удобно подсети помечать как VLAN с определенными интерфейсами. Удобно настроить один VLAN и поместить в него кучу портов коммутатора. И вообще, много чего удобно делать, когда есть VLAN.

Настройка VLAN

Ниже приведен набор основных команд, необходимых для администрирования VLAN. Пример настройки VLAN можно найти источнике П.13 из списка литературы.

Создание VLAN

```
Switch(config)#vlan 123 - создаем VLAN 123 (VLAN 1 по умолчанию зарезервирован)
```

Задание имени VLAN

```
Switch(config-vlan)#name Dir-ya - попадаем в настройки VLAN и задаем ему имя.
```

Команда для входа в контекст с настройкой VLAN

```
Switch(config)#vlan 123
```

Закрепление VLAN за конкретным портом коммутатора:

```
Switch (config)#interface fastEthernet 0/1 - переходим к настройке 1-ого порта.
Switch (config-if)#switchport mode access - переводим порт в режим access.
Switch (config-if)#switchport access vlan 123 - закрепляем за портом 123-ий VLAN.
```

Настройка шлюзов на маршрутизаторе

Поскольку к роутеру физически подключен только 1 канал, то маршрутизацию необходимо выполнять не на уровне интерфейса, а на уровне виртуальных интерфейсов (англ. subinterface). Пример настройки виртуального интерфейса:

```
Router(config)#interface fastEthernet 0/0.2
Router(config-if)#encapsulation dot1Q 123 – включаем тегирование по протоколу 802.1q
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

Отдельно стоит напомнить, что между коммутаторами должен быть включен режим trunk.

2.3. Протокол VTP

VTP (*VLAN Trunking Protocol*) – проприетарный протокол, разработанный Cisco, который позволяет устройствам автоматически делиться информацией о настроенных на них VLAN и самостоятельно вносить изменения в конфигурацию.

Режимы работы VTP

VTP коммутатор имеет два режима работы:

1. Server

   В этом режиме можно создавать новые и вносить изменения в существующие VLAN’ы.

   Коммутатор будет обновлять свою базу VLAN’ов и сохранять информацию о настройках во Flash памяти. Также в этом режиме генерируются и передаются сообщения как от других коммутаторов, работающих в режиме сервера, так и от клиентов

2. Client

   Коммутатор в этом режиме будет передавать информацию о VLAN полученную от других коммутаторов и синхронизировать свою базу VLAN при получении VTP обновлений. Настройки нельзя будет поменять через командную строку такого устройства.

3. Transparent

   В данном режиме коммутатор будет передавать VTP информацию другим участникам, не синхронизируя свою базу и не генерируя собственные обновления. Настройки VLAN можно поменять лишь для локального коммутатора.

Типы сообщений VTP

В VTP существует три типа сообщений:

1. Advertisement requests

Представляет из себя запрос от клиента к серверу на оповещение SummaryAdvertisement

2. Summary advertisements

   Данное сообщение по умолчанию сервер отправляет каждые 5 минут или сразу же после изменения конфигурации.

3. Subset advertisements

   Отправляется сразу же после изменения конфигурации VLAN, а также после запроса на оповещение.

Стоит отметить, что VTP коммутатор, который получает информацию о новых VLAN'ах, внесет ее в свою конфигурацию только в том случае, если сообщение пришло от коммутатора с большим номером ревизии.

Номер ревизии — это некий идентификатор "свежести" базы VLAN. Коммутатор воспринимает базу с наивысшим номером ревизии как самую "свежую" и вносит изменения в свою конфигурацию.

Для оборудования других производителей существует аналогичный открытый стандарт - GVRP (GARP VLAN Registration Protocol).

Настройка VTP

Ниже приведен набор основных команд, необходимых для настройки STP. Пример настройки можно найти в источнике П.13 из списка литературы

Просмотр режима VTP

```
Switch#show vtp status
```

Настройка режима VTP

```
Switch(config)#vtp mode client – возможные варианты: server, client, transparent
```

Настройка домена VTP

```
Switch  (config)#vtp domain vtp_domain.ru
```

2.4. Протокол STP

Spanning Tree Protocol — сетевой протокол, работающий на втором уровне модели OSI. Основан на одноименном алгоритме, разработчиком которого является Радья Перлман.

Основной задачей STP является приведение сети Ethernet с множественными связями к древовидной топологии, исключающей циклы пакетов. Происходит это путем автоматического блокирования ненужных в данный момент для полной связности портов. Протокол описан в стандарте IEEE 802.1D.

Для того чтобы определить какие порты заблокировать, а какие будут в режиме пересылки, STP выполняет следующее:

1. Выбор корневого моста (Root Bridge)
2. Определение корневых портов (Root Port)
3. Определение выделенных портов (Designated Port)

Выбор корневого моста

Корневым становится коммутатор с наименьшим идентификатором моста (Bridge ID).

Только один коммутатор может быть корневым. Для того чтобы выбрать корневой коммутатор, все коммутаторы отправляют сообщения BPDU, указывая себя в качестве корневого коммутатора. Если коммутатор получает BPDU от коммутатора с меньшим Bridge ID, то он перестает анонсировать информацию о том, что он корневой и начинает передавать BPDU коммутатора с меньшим Bridge ID. В итоге только один коммутатор останется корневым и будет передавать BPDU.

Изначально Bridge ID состоял из двух полей:

- Приоритет — поле, которое позволяет административно влиять на выборы корневого коммутатора. Размер — 2 байта,
- MAC-адрес — используется как уникальный идентификатор, который, в случае совпадения значений приоритетов, позволяет выбрать корневой коммутатор. Так как MAC-адреса уникальны, то и Bridge ID уникален, так что какой-то коммутатор обязательно станет корневым.

Определение корневых портов

Порт коммутатора, который имеет кратчайший путь к корневому коммутатору называется корневым портом. У любого не корневого коммутатора может быть только один корневой порт.

Определение назначенных портов

Коммутатор в сегменте сети, имеющий наименьшее расстояние до корневого коммутатора называется назначенным коммутатором (мостом). Порт этого коммутатора, который подключен к рассматриваемому сегменту сети, называется назначенным портом.

Принцип действия

1. В сети выбирается один корневой мост (Root Bridge).
2. Далее каждый, отличный от корневого, мост просчитывает кратчайший путь к корневому. Соответствующий порт называется корневым портом (Root Port). У любого не корневого коммутатора может быть только один корневой порт.
3. После этого для каждого сегмента сети просчитывается кратчайший путь к корневому порту. Мост, через который проходит этот путь, становится назначенным для этой сети (Designated Bridge). Непосредственно подключенный к сети порт моста — назначенным портом.
4. Далее на всех мостах блокируются все порты, не являющиеся корневыми и назначенными. В итоге получается древовидная структура (математический граф) с вершиной в виде корневого коммутатора.

Алгоритм действия STP

- После включения коммутаторов в сеть, по умолчанию каждый (!) коммутатор считает себя корневым (root).
- Затем коммутатор начинает посылать по всем портам конфигурационные Hello BPDU пакеты раз в 2 секунды.
- Исходя из данных Hello BPDU пакетов, тот или иной коммутатор приобретает статус root, то есть корня.
- После этого все порты кроме root port и designated port блокируются.

Происходит посылка Hello-пакетов раз в 20 секунд либо при пропадании/восстановлении какого-нибудь линка, с целью препятствия появлению петель в сети.

Пример топологии

Изменениями топологии считается изменения ролей DP и RP. Коммутатор, который обнаружил изменения в топологии отправляет Topology Change Notification (TCN) BPDU корневому коммутатору:

- Коммутатор, на котором произошли изменения отправляет TCN BPDU через свой корневой порт. Отправка сообщения повторяется каждый hello interval (2 секунды) до тех пор, пока получение сообщения не будет подтверждено.
- Следующий коммутатор, который получил TCN BPDU отправляет назад подтверждение. Подтверждение отправляется в следующем Hello BPDU, которое будет отправлять коммутатор, выставлением флага Topology Change Acknowledgement (TCA).
- Далее коммутаторы, у которых порт работает в роли DP для сегмента, повторяют первые два шага и отправляют TCN через свой корневой порт и ждут подтверждения.

После того как корневой коммутатор получил TCN BPDU, он отправляет несколько следующих Hello с флагом TCA. Эти сообщения получают все коммутаторы. При получении сообщения hello с флагом TCA, коммутатор использует короткий таймер (Forward Delay time) для того чтобы обновить записи в таблице коммутации. Обновления выполняется из-за того, что после изменений в топологии STP в таблице коммутации могут храниться неправильные записи.

Если порт изменяет состояние с Blocking в Forwarding, то он должен пройти через два промежуточных состояния: Listening и Learning. Переход из Forwarding в Blocking может выполняться сразу.

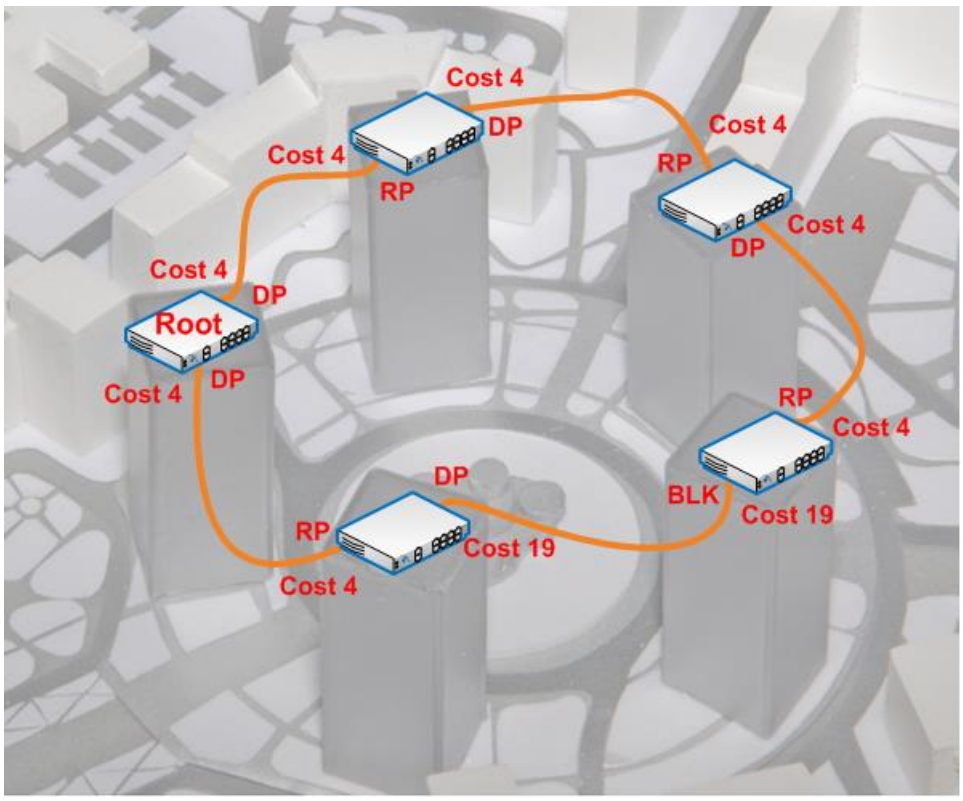

Рис. 5. *Пример сетевой топологии с настроенным STP*

Роли и состояния портов

Роли портов:

- Root Port — корневой порт коммутатора
- Designated Port — назначенный порт сегмента
- Nondesignated Port — неназначенный порт сегмента
- Disabled Port — порт который находится в выключенном состоянии

Состояния портов:

- Blocking — блокирование
- Listening — прослушивание
- Learning — обучение
- Forwarding — пересылка

Настройка STP

Ниже приведен набор основных команд, необходимых для настройки STP. Пример настройки можно найти в источнике П.14 из списка литературы

Просмотр текущих данных STP

```
Switch#show spanning-tree
```

Настройка приоритета VLAN

```
Switch(config)#spanning-tree vlan 3 priority 30000
```

Или

```
Switch(config)# spanning-tree vlan 3 root primary
```

Перевод порта в режим Forwading без выполнения проверок STP

```
Switch(config-if)#spanning-tree portfast  - данная команда должна выполняться только для интерфейсов подключенных к единичному устройству, иначе могут возникнуть циклы.
```

2.5. Протокол EtherChannel

Технология EtherChannel позволяет объединять несколько физических портов на коммутаторах в один логический. Чтобы сразу стало понятно, о чём идёт речь, приведу пример: пусть два коммутатора соединены между собой четырьмя проводами (на каждом используется по 4 порта по 100 Mbit каждый). В случае отсутствия EtherChannel – линки эти будут считаться петлями и протокол Spanning Tree заблокирует три из них. Работать будет только один и скорость обмена данными составит 100 Mbit, зато с тройным резервированием. В случае же объединения их с помощью EtherChannel (на обоих коммутаторах), между коммутаторами будет один виртуальный линк, состоящий из четырёх физических, работающий со скоростью 400 Mbit. Теперь, когда стало более или менее понятно, с чем мы имеем дело перейдём к описанию и настройке.

Технология EtherChanel изначально была предложена компанией Cisco, но в настоящий момент используются и у других производителей. Технология позволяет несколько физических портов в один виртуальный порт, именуемый PortChannel. Возможно создавать несколько отдельных PortChannel-ов на одном коммутаторе. Давайте подумаем, какие преимущества даёт эта технология:

1. Главное преимущество – скорость, нет необходимости покупать новый коммутатор, если на старом только гигабитные порты, а нам надо более быстрый аплинк к следующему коммутатору, мы можем объединить, например, 8 портов и получить 8 гигабит.
2. В плане надёжности Etherchannel отличается от использования протокола Spanning tree тем, что если в STP пропадает какой-то линк, то начинается пересчёт топологии, что занимает какое-то время, после чего, резервный канал вводится в строй, в случае же Etherchannel, топология не меняется, просто скорость канала в предыдущем примере станет не 8, а 7 гигабит. Иными словами, Etherchannel не избавляет от необходимости использовать Spanning Tree, но в случае, если линк пропадает именно на агрегированном участке, избавляет от необходимости пересчёта топологии.
3. Ещё одно небольшое, но всё же преимущество – после создания интерфейса portchannel, большая часть настроек может проводиться на нём – нет необходимости отдельно настраивать входящие в него физические интерфейсы – все параметры будут транслироваться на них автоматически.

Для того, чтобы PortChannel мог существовать, необходимо, чтобы все входящие в него порты имели одинаковые параметры, а именно:

1. Одинаковую скорость (нельзя создать portchannel, куда входили бы, например, FastEthernet0/1 и GigabitEthernet1/1 – либо все 10 Мбит, либо все 100, либо все – гигабит и т.д.)
2. Одинаковые настройки дуплекса
3. Одинаковые настройки VLAN-ов. В случае access портов – все порты должны быть в одном VLAN, в случае trunk портов – список разрешённых VLAN (команда switchport trunk allowed vlan) так же должен совпадать

Когда два коммутатора «договариваются» друг с другом об использовании между ними агрегированного канала, применяется один из двух протоколов: PAgP или LACP. PAgP – разрабатывался изначально cisco, а затем появился аналогичный открытый стандарт LACP, который был оформлен в виде спецификации IEEE и используется как на каталистах, так и на коммутаторах других производителей. Иными словами, в современных реалиях лучше всего использовать LACP, так как он совместим со всеми, в отличие от PAgP. В функциональном же плане протоколы аналогичные. PortChannel может быть настроен в одном из трёх режимов: On, Active и Passive (в LACP) или On, Auto, Desirable (в PAgP соответственно). Для того, чтобы между коммутаторами поднялся и заработал portchannel, необходимо, чтобы обе стороны были настроены в режиме On, либо одна была в режиме Active, а другая – Passive.

Настройка EtherChannel

Для выполнения настройки EtherChannel необходимо изучить источники П.11 и П.12 методических указаний, ниже представлены основные команды необходимые для настройки EtherChannel.

Добавление интерфейсов в channel-group

```
Switch(config)interface range fastEthernet 0/1-2
Switch(config-if -range)#channel-group 1 mode active
```

Просмотр данных Etherchannel

```
Switch#show etherchannel summary
```

2.6. Настройка Event List Filter в Cisco Packet Tracer 8.2

Поскольку в этой ЛР задействуется множество протоколов, работу которых нужно отслеживать, то рекомендуется отключать ненужные протоколы в соответствующем фильтре (см. рис.1)

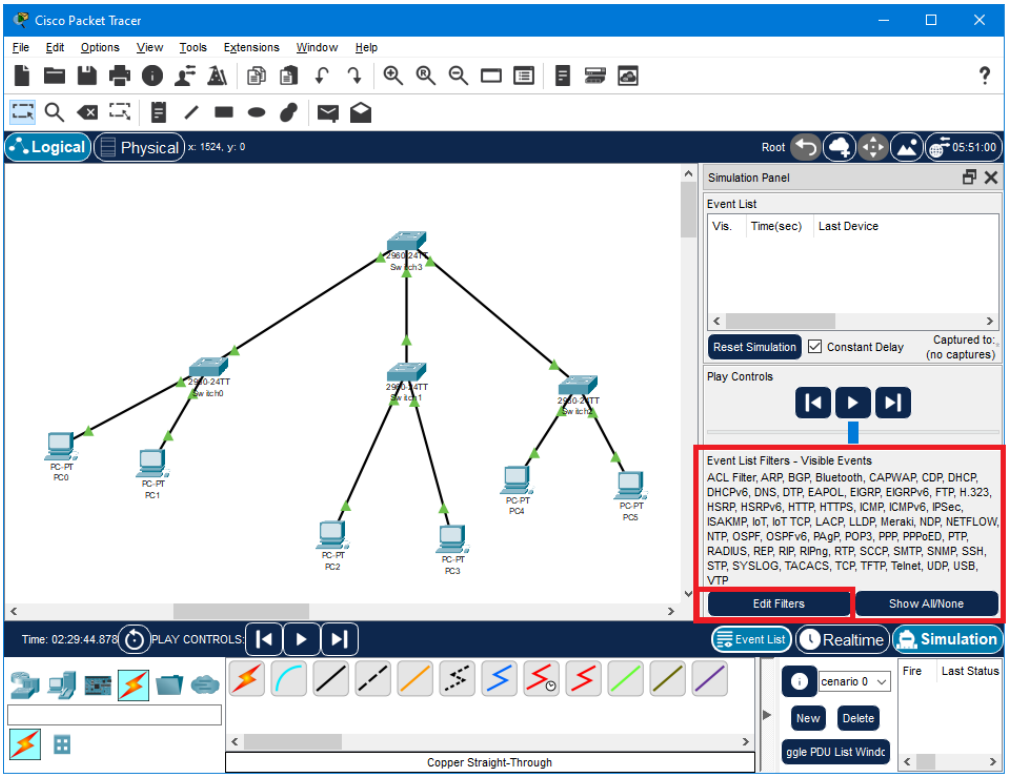

Рис.6. Окно Event List Filters

3. Задание.

Задание: построить локальную сеть, состоящую из 3х сегментов, соединенных через центральный коммутатор (структура изображена на рис.6). В каждом сегменте A, B и C устройств соответственно.

1. Расположить все конечные устройства в одной подсети. Посмотреть и зафиксировать процесс пересылки ARP пакета между узлами сети.
2. Настроить в текущей конфигурации 3 VLAN, при чем как минимум для 1й VLAN устройства должны находиться более чем в 1м сегменте. После этого вновь посмотреть алгоритм отправки ARP пакета.
3. Изменить текущую конфигурацию: настроить 3 разных подсети (каждая подсеть включает в себя устройства одного из VLAN), добавить роутер, подключенный к центральному коммутатору и добиться пересылки пакетов между разными подсетями. Снова посмотреть алгоритм пересылки ARP запроса в сети. Пример описанной топологии изображен на рис.7.

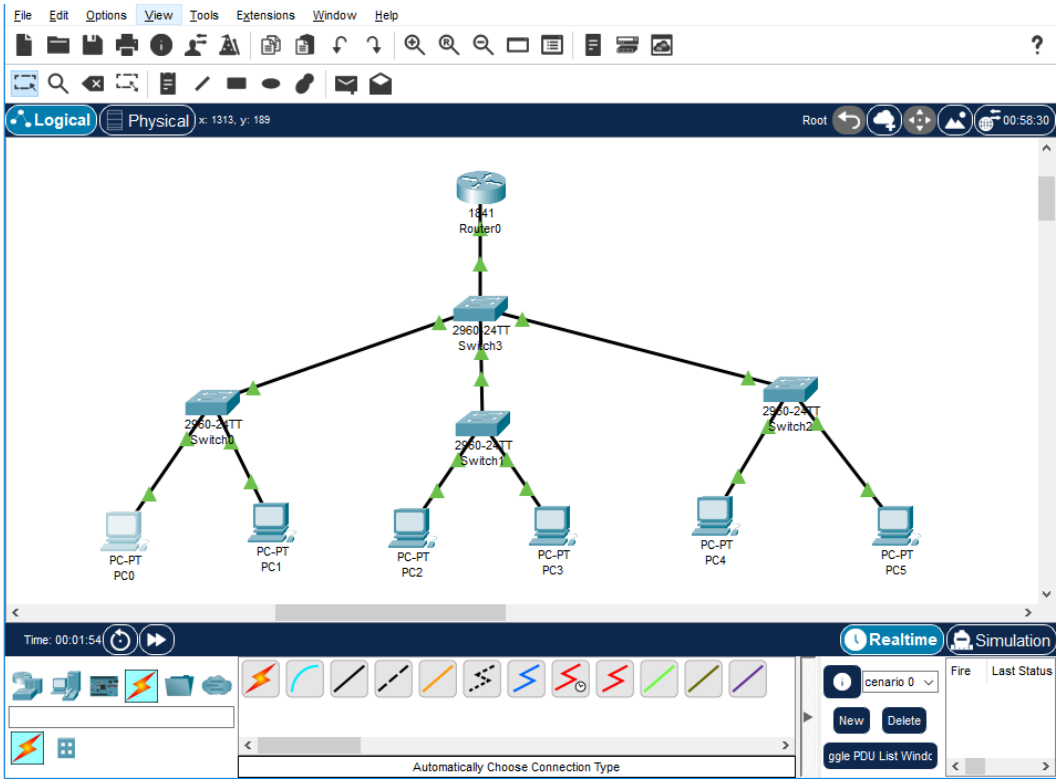

Рис.7. Топология сети для пункта 3 ЛР

Также предлагается выполнить 2 из следующих заданий на выбор:

1. Соединить между собой коммутаторы из разных сегментов. Отследить и

зафиксировать процесс построения spanning tree для полученной архитектуры сети. Сравнить алгоритм построения для сети с аналогичной архитектурой, но без настроенного VLAN.

2. При помощи протокола VTP настроить автоматическую синхронизацию данных VLAN между коммутаторами. Центральный коммутатор должен выступать в роли сервера, остальные – в роли клиентов. Отследить процесс согласования между коммутаторами.
3. Дополнительно соединить центральный коммутатор с остальными коммутаторы по еще 1 каналу. Настроить etherchannel (по протоколу LACP) для агрегации полученных каналов.

4. Контрольные вопросы.

1. Что такое VLAN для чего он предназначен?
2. Для чего предназначен алгоритм ARP?
3. Что такое spanning tree, для чего предназначен этот протокол?
4. Для чего предназначен алгоритм DTP? как выглядит процесс согласования между коммутаторами?
5. Для чего предназначен алгоритм VTP? Какие типы пакетов посылаются этим протоколом? Какова структура этих пакетов?
6. Для чего нужен протокол Etherchannel? Каковы ограничения его применения?
7. Каким образом в Cisco Packet Tracer можно сэмулировать циклическую пересылку пакетов, и какой протокол позволяет этого избежать?
8. Зачем нужно использовать VLAN, если можно просто разбить сеть на подсети на сетевом уровне?
9. Для чего на роутере применялась инкапсуляция протокола 802.1q ? Какие новые поля добавляет этот протокол?

5. Рекомендуемые источники.

1. Галкин В.А., Григорьев Ю.А. Телекоммуникации и сети: Учеб. пособие для вузов. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2003.
2. Олифер В.Г., Олифер Н.А Компьютерные сети. Принципы, технологии, протоколы 3-е издание. Учебное пособие, СПб.:Питер 2007
3. Степанов А.Н. Архитектура вычислительных систем и компьютерных сетей, СПб.: Питер 2007
4. Конфигурирование VLAN: [Электронный ресурс]. URL:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/layer2/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide_Release_5-x_chapter4.html (Дата обращения 25.05.2023)

5. Протокол преобразования адресов ARP: [Электронный ресурс]. URL: https://www.opennet.ru/docs/RUS/inet_book/4/44/arp_446.html (Дата обращения 25.05.2023)
6. IP Addressing: ARP Configuration Guide: [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_arp/configuration/xe-16/arp-xe-16-book.pdf (Дата обращения 25.05.2023)
7. Spanning Tree Protocol: [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/tech/lan-switching/spanning-tree-protocol/index.html (Дата обращения 25.05.2023)
8. Протокол DTP: [Электронный ресурс]. URL: https://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=8 (Дата обращения 25.05.2023)
9. Протокол VTP: [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html (Дата обращения 25.05.2023)
10. Настройка EtherChannel: [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/etherchannel.pdf (Дата обращения 25.05.2023)
11. Агрегация канала EtherChannel: [Электронный ресурс]. URL: http://ciscotips.ru/etherchannel (Дата обращения 25.05.2023)
12. Протокол агрегирования каналов: Etherchannel; [Электронный ресурс]. URL: https://habr.com/ru/articles/334778/ (Дата обращения 23.09.2023)
13. Понятие VLAN, Trunk и протоколы VTP и DTP; [Электронный ресурс]. URL: https://habr.com/ru/articles/319080/ (Дата обращения 23.09.2023)
14. Протокол связующего дерева: STP; [Электронный ресурс]. URL: https://habr.com/ru/articles/321132/ (Дата обращения 23.09.2023)