Лабораторная работа № 2
Локальные сети на основе коммутаторов

2.1. Цель работы

Лабораторная работа №2 предназначена для изучения технологий и протоколов локальных сетей на основе сетевых коммутаторов и представляет собой три сценария для симулятора Cisco Packet Tracer. Для успешного выполнения лабораторной работы студентам необходимо выполнить задание сценария и подготовить отчет (по своему варианту), а также защитить его в форме собеседования.

2.2. Теоретическая часть

Современные локальные сети строятся по топологии «звезда»: все конечные устройства подключаются к центральному сетевому устройству – концентратору, коммутатору, точке доступа wifi и др.

2.2.1. Концентратор

Концентратор (англ. hub, рис. 2.1) – это сетевое устройство для объединения нескольких других устройств в общий сегмент сети путем повторения электрического сигнала «один во все». Работает на физическом уровне модели OSI, что приводит к созданию на базе концентратора общего домена коллизий, следовательно, снижает эффективность работы сети. К настоящему моменту концентраторы не производятся, т.к. были вытеснены с рынка более функциональными сетевыми коммутаторами.

Рисунок 2.1. Концентратор

2.2.2. Сетевой коммутатор

Коммутатор (англ. switch, рис. 2.2) – это сетевое устройство, предназначенное для объединения сегментов сети в локальную сеть. Иногда называют коммутатор уровня 2 так как он работает на канальном и физическом уровне модели OSI.

Коммутатор уровня 2 осуществляет коммутацию и фильтрацию только на основе MAC-адресов канального уровня и передаёт пакеты данных непосредственно тому абоненту локальной сети, которому они предназначены. Коммутатор создаёт и ведет таблицу MAC-адресов, которую использует для принятия решений о пересылке пакетов.

Рисунок 2.2. Коммутатор Cisco

2.2.3. Таблица MAC-адресов

Таблица MAC-адресов (или таблица коммутации) используется для определения интерфейса, на который необходимо передать входящий кадр. В таблице хранятся пары соответствия MAC-адресов известных устройств и интерфейсов коммутатора, на которых они находятся.

На основе таблицы MAC-адресов коммутатор передаёт данные по сети. При получении кадра данных коммутатор анализирует указанный в кадре MAC-адрес назначения и выполняет поиск по таблице MAC-адресов. Если соответствие найдено, по таблице определяется выходной интерфейс, на который и будет передан кадр. Если соответствие не найдено, коммутатор пересылает этот кадр на все интерфейсы, за исключением того, на который этот кадр изначально поступил. При этом указанный в кадре адрес источника добавляется в таблицу (если его там еще нет) в паре с интерфейсом, на кторый этот кадр поступил.

Таблица хранится в энергозависимой памяти коммутатора, следовательно, данные в ней обнуляются при его перезагрузке.

Для анализа таблицы MAC-адресов используется команда *show mac-address-table*. Вывод этой команды можно фильтровать по интерфейсу, номеру виртуальной сети (см. ниже) и другим параметрам.

2.2.4. MAC-адрес

MAC-адрес (англ. Media Access Control — управление доступом к среде, также Hardware Address) – это уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей. Большинство сетевых протоколов канального уровня используют одно из трёх пространств MAC-адресов, управляемых IEEE: MAC-48, EUI-48 и EUI-64. Адреса в каждом из пространств теоретически должны быть глобально уникальными. Не все протоколы используют MAC-адреса, и не все протоколы, использующие MAC-адреса, нуждаются в подобной уникальности этих адресов.

В широковещательных сетях (таких, как сети на основе Ethernet) MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу. Таким образом, MAC-адреса формируют основу сетей на канальном уровне, которую используют протоколы более высокого (сетевого) уровня. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы (например, ARP и inARP в сетях TCP/IP).

2.2.5. Протокол ARP

ARP (англ. Address Resolution Protocol, протокол определения адреса) – протокол, предназначенный для определения MAC-адреса по известному IP-адресу.

Протокол ARP выполняет две основные функции:

1. сопоставление адресов IPv4 и MAC-адресов (адреса 3 и 2 уровня);
2. сохранение таблицы сопоставлений.

Принцип работы.

Каждый сетевой интерфейс имеет IP-адрес и MAC-адрес. Чтобы продемонстрировать работу протокола ARP представим локальную сеть, состоящую из четырех компьютеров и коммутатора. Пусть в какой-то момент узел H1 направляет пакет узлу H4. Теперь, прежде чем упаковать пакет в кадр Ethernet и направить его коммутатору, необходимо определить соответствующий MAC-адрес. Для решения этой задачи протокол IP обращается к протоколу ARP. Протокол ARP поддерживает на каждом интерфейсе сетевого адаптера или маршрутизатора отдельную ARP-таблицу, в которой в ходе функционирования сети накапливается информация о соответствии между IP-адресами и MAC-адресами других интерфейсов данной сети. Первоначально, при включении компьютера или маршрутизатора в сеть ARP-таблицы пусты.

Рассмотрим более подробно заполнение ARP – таблицы:

На первом шаге ПК H1 проверяет собственную таблицу ARP.

У ПК H1 в таблице ARP отсутствует сопоставлениеIP и MAC адреса компьютера H4. Поэтому ПК H1 формирует ARP – запрос, который рассылается в широковещательном сообщении (Рис 14).

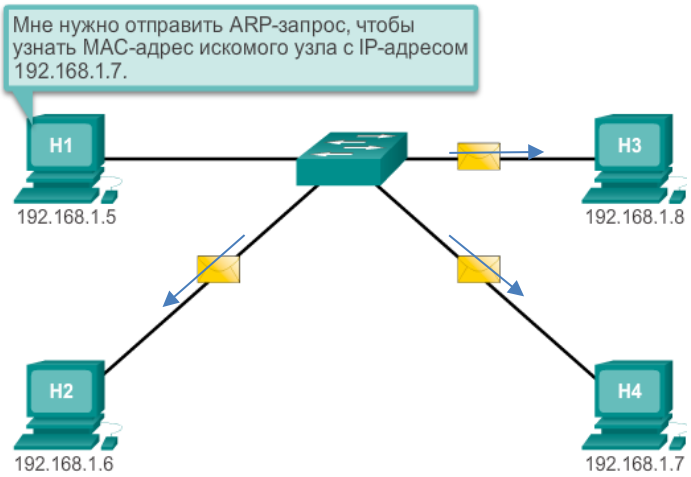

Рисунок 2.3. ARP-запрос

Все узлы сети получают ARP – запрос, и сравнивают свой IP адрес с адресом в сообщении. Узел, у которого совпал IP адрес из ARP-запроса с его собственным, формирует ARP-ответ (Рис 2.4).

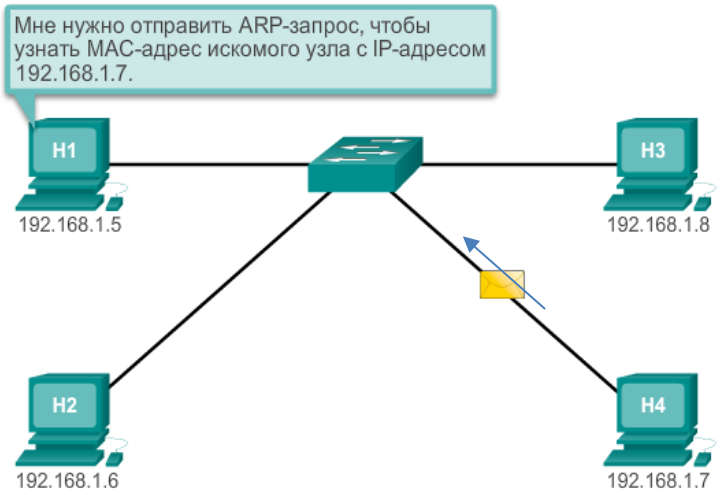

Рисунок 2.4. ARP-ответ

2.2.6. Протокол Spanning Tree (STP)

SpanningTreeProtocol — сетевой протокол, работающий на втором уровне модели OSI. Основан на одноимённом алгоритме, разработчиком которого является Радья Перлман.

Основной задачей STP является приведение сети Ethernet с множественными связями к древовидной топологии, исключающей зацикливание кадров. Происходит это путём автоматического блокирования

избыточных в данный момент связей для полной связности портов. Базовый протокол описан в стандарте IEEE 802.1D, также существует множество версий и вариаций, таких как RSTP, MST, PVST и др., которые не будут рассмотрены в рамках настоящего курса.

Принцип действия протокола STP

1. В сети выбирается один корневой коммутатор – root bridge. Слово bridge (мост) используется, т.к. первоначально протокол создавался для устройств, называвшихся мостами (фактически они представляли собой двухпортовые коммутаторы).

После включения коммутаторов в сеть, по умолчанию каждый (!) коммутатор считает себя корневым. Корневой коммутатор (изначально все) посылает по всем портам служебные кадры BPDU (bridge protocol data unit) каждые 2 секунды. Получив чужой BPDU, коммутатор сравнивает значения bridge ID и, при необходимости, прекращает рассылку собственных BPDU, ретранслирую только те, которые исходят от корневого коммутатора.

Исходя из данных BPDU пакетов, тот или иной коммутатор приобретает статус root, то есть корня, когда в сети не остается иных BPDU. Корневым коммутатором назначается коммутатор с **самым низким** значением bridge ID. Этот числовой идентификатор формируется из приоритета (старшие разряды) и значения MAC-адреса служебного блока коммутатора (младшие разряды), что позволяет управлять процессом выбора путем изменения приоритета (по умолчанию значения приоритета равны и для выбора используются только MAC-адреса).

2. Каждый коммутатор, кроме корневого, просчитывает кратчайший путь к корневому коммутатору. Соответствующий порт, через который это кратчайшее расстояние достигается, называется корневым портом (англ. root port). У любого не-корневого коммутатора всегда ровно один корневой порт.

Для измерения расстояния используется специальная величина STP Cost, связанная с битовой скоростью сегмента обратно пропорциональной зависимостью. Каждый порт коммутатора имеет свою стоимость соединения, установленную либо на заводе-изготовителе (по умолчанию), либо вручную. Из этих стоимостей нарастающим итогом складывается расстояние до корня от любого порта любого коммутатора.

3. Для каждого сегмента сети также просчитывается кратчайший путь к корневому коммутатору. Коммутатор, через который проходит этот путь, становится назначенным для этой сети (англ. designated bridge), а его непосредственно подключенный к этой сети интерфейс – назначенным

портом. В каждом сегменте выбирается ровно один назначенный порт из всех портов всех коммутаторов сегмента.

Отметим, что все порты, к которым подключены конечные устройства (компьютеры и др.) всегда будут назначенными, т.к. они представляют собой единственный порт, принадлежащий коммутатору, в своем сегменте. В других сегментах назначенным всегда будет выбран порт того коммутатора, для которого меньше расстояние до корня на соответствующем корневом порту.

4. В завершение работы протокола на всех коммутаторах блокируются все порты, не являющиеся корневыми или назначенными. В итоге получается древовидная структура (математический граф) с вершиной на корневом коммутаторе. Корневой коммутатор продолжает рассылать кадры BPDU каждые 2 секунды для поддержания древовидной топологии сети в актуальном состоянии.

2.2.7. Виртуальные локальные сети (VLAN)

VLAN (аббр. от англ. virtual local area network) – виртуальная локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к общему широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным узлам группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств.

Идентификатором виртуальной сети является ее номер (десятичное число от 0 до 4095). Этот идентификатор добавляется в специальное поле заголовка кадра (тег), после чего тегированный кадр передается коммутаторами только по транковым портам (см. ниже) и по портам своего VLAN-а.

По умолчанию на каждом порту коммутатора имеется сеть VLAN1 или VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

Способы определения членства в VLAN

1. По порту (англ. port-based, IEEE 802.1Q): порту коммутатора вручную назначается один VLAN. В случае, если одному порту должны соответствовать несколько VLAN (например, если соединение VLAN проходит через несколько свитчей), то этот порт должен быть членом транка.

Свитч будет добавлять метки данной VLAN ко всем принятым кадрам, не имеющим никаких меток. VLAN, построенные на базе портов, имеют некоторые ограничения. Они очень просты в установке, но позволяют поддерживать для каждого порта только один VLAN. Следовательно, такое решение неприемлемо при использовании концентраторов или в сетях с мощными серверами, к которым обращается много пользователей (сервер не удастся включить в разные VLAN). Кроме того, вносить изменения в VLAN на основе портов достаточно сложно, поскольку при каждом изменении требуется физическое переключение устройств. В рамках наятощего курса рассматриваются только port-based VLAN-ы.

2. По MAC-адресу (MAC-based): членство в VLAN основывается на MAC-адресе узла. Для этого необходимо, чтобы в таблице MAC-адресов коммутатора содержалась информация о том, какому VLAN принадлежит тот или иной MAC-адрес. Если сама таблица не поддерживает такое хранение, необходимо обеспечить коммутатору доступ к удаленной таблице соответствия (например, сервер VMPS – VLAN membership policy server).

3. По протоколу (Protocol-based): данные 3-4 уровня в заголовке пакета используются чтобы определить членство в VLAN. Например, IP-машины могут быть переведены в первую VLAN, а AppleTalk-машины во вторую. Основной недостаток этого метода в том, что он нарушает независимость уровней, поэтому, например, переход с IPv4 на IPv6 приведет к нарушению работоспособности сети.

4. Методом аутентификации (Authenticationbased): устройства могут быть автоматически перемещены в VLAN, основываясь на данных аутентификации.

Преимущества использования виртуальных локальных сетей.

1. Облегчается перемещение, добавление устройств и изменение их соединений друг с другом.

2. Достигается большая степень административного контроля вследствие наличия устройства, осуществляющего между сетями VLAN маршрутизацию на третьем уровне.

3. Уменьшается потребление полосы пропускания по сравнению с ситуацией одного широковещательного домена.

4. Сокращается непроизводственное использование CPU за счет сокращения пересылки широковещательных сообщений.

5. Обеспечивается предотвращение широковещательных штормов и предотвращение петель.

2.2.8. Протокол VTP

Протокол VTP — протокол ЛВС, служащий для обмена информацией о VLAN (виртуальных сетях), имеющихся на выбранном транковом порту. Разработан компанией Cisco.

Протокол VTP был создан для решения возможных проблем в среде коммутации виртуальных локальных сетей VLAN. Например, рассмотрим домен, в котором имеются несколько связанных друг с другом коммутаторов, которые поддерживают несколько VLAN-сетей. Для создания и поддержания соединений внутри VLAN-сетей каждая из них должна быть сконфигурирована вручную на каждом коммутаторе. По мере роста организации и увеличения количества коммутаторов в сети, каждый новый коммутатор должен быть сконфигурирован вручную с вводом информации о VLAN- сетях. Всего лишь одно неправильное назначение в сети VLAN может вызвать две потенциальные проблемы, такие как:

- перекрестное соединение VLAN-сетей вследствие несогласованности в конфигурации VLAN-сетей.
- согласование и ликвидация противоречивости конфигурации в смешанной среде передачи, например, в среде, включающей в себя сегменты Ethernet и FDDI.

В протоколе VTP согласованность конфигураций VLAN-сетей поддерживается в общем административном домене. Кроме того, протокол VTP уменьшает сложность управления и мониторинга VLAN-сетей. Протокол VTP является протоколом обмена сообщениями, использующим магистральные кадры 2-го уровня для управления добавлением, удалением и переименованием VLAN-сетей в одном домене.

Кроме того, протокол VTP позволяет осуществлять централизованные изменения в сети, о которых сообщается всем другим коммутатором в сети. Сообщения протокола VTP инкапсулируются в кадры протоколов ISL или IEEE 802.1Q и передаются далее по магистральным каналам другим устройствам. К фреймам IEEE 802.1Q в качестве тега добавляется 4-х байтовое поле. В обоих форматах передаются идентификатор ID VLAN-сети.

2.2.9. Trunk port

Магистральный порт или Trunk port — это канал типа «точка-точка» между коммутатором и другим сетевым устройством. Магистральные подключения служат для передачи трафика нескольких VLAN через один канал и обеспечивают им доступ ко всей сети. Магистральные порты

необходимы для передачи трафика нескольких VLAN между устройствами при соединении двух коммутаторов, коммутатора и маршрутизатора или коммутатора и сетевого адаптера узла с поддержкой транкинга 802.1Q.

2.2.10. Архитектура Router-on-a-stick

Сети VLAN используются для сегментации общей сети. На коммутаторах можно настроить более чем четыре тысячи виртуальных сетей. Но возможности коммутатора 2 уровня ограничены, он не может выполнять маршрутизацию.

Сеть VLAN — это домен широковещательной рассылки, поэтому компьютеры в разных сетях VLAN не могут обмениваться данными без помощи устройства маршрутизации. Любое устройство, поддерживающее маршрутизацию 3-го уровня, например, маршрутизатор или многоуровневый коммутатор, можно использовать для выполнения основных функций маршрутизации.

Исторически первым решением для маршрутизации между VLAN стало использование маршрутизаторов с несколькими физическими интерфейсами **(Рис 2.5)**. Каждый интерфейс должен был быть подключён к отдельной сети и настроен с определённой подсетью. При таком устаревшем подходе маршрутизация между VLAN выполняется путём подключения различных физических интерфейсов маршрутизатора к разным физическим портам коммутатора. Порты коммутатора, подключённые к маршрутизатору, переводятся в режим доступа, а каждый физический интерфейс назначается отдельной VLAN.

Метод «**router-on-a-stick**» **(Рис 17)** — это такой тип конфигурации маршрутизатора, при котором один физический интерфейс маршрутизирует трафик между несколькими VLAN. Интерфейс маршрутизатора настраивается для работы в качестве trunk канала и подключается к порту коммутатора, который так же настроен в режиме trunk. Маршрутизатор выполняет маршрутизацию между VLAN, принимая на trunk интерфейсе трафик с меткой VLAN, поступающий от смежного коммутатора, и затем с помощью суб-интерфейсов маршрутизируя его между VLAN. Затем уже маршрутизированный трафик посылается с этого же физического интерфейса с меткой VLAN, соответствующей VLAN назначения.

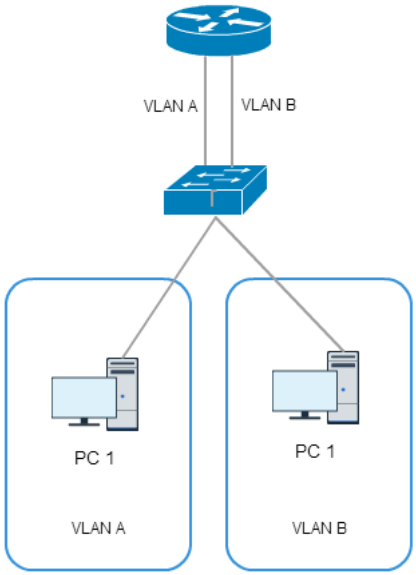

Рисунок 2.5. Устаревший метод

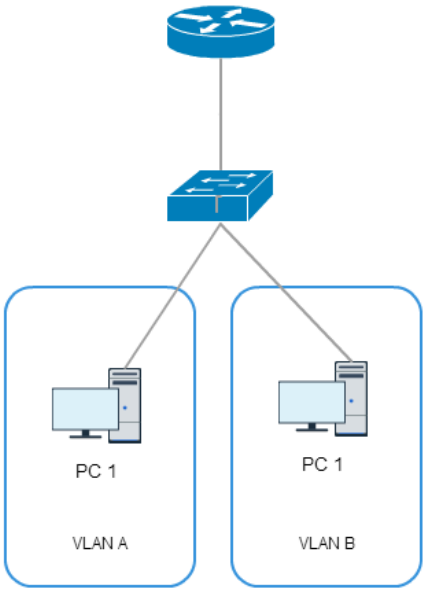

Рисунок 2.6. Router-on-a-stick

Суб-интерфейсы — это программные виртуальные интерфейсы, связанные с одним физическим интерфейсом. Суб-интерфейсы настраиваются в программном обеспечении маршрутизатора, и каждому суб-интерфейсу назначаются IP-адрес и VLAN.

2.2.11. Команды IOS

Рассмотрим список команд IOS, необходимый и достаточный для выполнения лабораторной работы № 2. Для следующих лабораторных работ будут добавлены только новые команды, указанные здесь повторяться не будут. Более простые команды см. в описании лабораторной работы №1.

Команды привилегированного режима // switch#

- **show mac-address table** – выводит таблицу MAC – адресов (допустима фильтрация по интерфейсу, номеру виртуальной сети и др., см. параметры команды во встроенной справке);
- **clear mac address table** – очищает таблицу MAC – адресов;
- **show spanning-tree** – команда без указания дополнительных параметров предоставляет краткие сведения о состоянии STP;
- **show vlan** – выводит таблицу виртуальных сетей, известных коммутатору;
- **show vtp status** – выводит информацию о состоянии протокола vtp на коммутаторе;
- **show vtp password –** выводит пароль vtp;

- **vlan [номер vlan]** – переход в режим конфигурирования виртуальной сети; создает виртуальную локальную сеть с заданным номером, если она не существует;
- **vtp mode [server/client/transparent]** – переводит протокол vtp на текущем коммутаторе в выбранный режим работы;
- **vtp domain [имя домена] –** задает домен для изолированной работы vtp;
- **vtp password [пароль]** – задает пароль для vtp-домена на текущем коммутаторе;

Команды режима глобального конфигурирования // swich(config)#

- **interface [интерфейс].[номер]** – переход в режим конфигурирования суб-интерфейса; создает для указанного интерфейса суб-интерфейс с заданным номером, если он не существует;

Команды режима конфигурирования интерфейса // switch(config-if)#

- **switchport mode [access/trunk]** – переводит порт коммутатора в выбранный режим работы (доступ или транк);
- **switchport access vlan [номер vlan]** – назначает текущему интерфейсу (должен работать в режиме доступа) vlan с указанным номером. Если vlan с таким номером не существует, то он принудительно создаётся;
- **switchport trunk allowed [номера vlan]** – задает список виртуальных сетей, которым разрешён доступ в текущий транк.

Команды режима конфигурирования интерфейса // switch(config-subif)#

- **encapsulation dot1q [номер vlan]** – задает режим инкапсуляции на текущем суб-интерфейсе по стандарту IEEE 802.1q и назначает vlan с указанным номером;

Команды конфигурирования vlan

- **name [текст]** – задать название виртуальной локальной сети.

2.3. Задание на лабораторную работу

Лабораторная работа выполняется в среде Cisco Packet Tracer в предложенных Вам файлах-сценариях формата pka (их три).

Сценарий 2.1

Сценарий 2.1 содержит созданную заранее логическую топологию, из четырех компьютеров, подключенных к общему коммутатору.

ВНИМАНИЕ! Сценарий 2.1 должен быть выполнен на вновь открытом файле сценария. Внесение любых изменений в конфигурацию устройств, а также выполнение любых действий, не указанных в сценарии, может привести к изменению данных в оперативной памяти моделей устройств и к неверным результатам выполнения лабораторной работы.

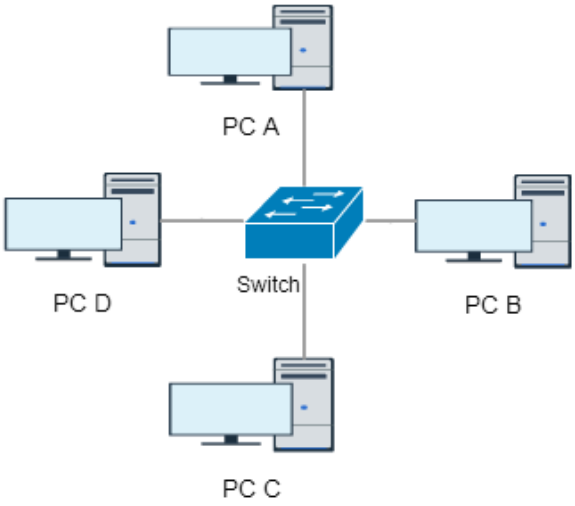

Рисунок 2.7. Топология сети (сценарий 2.1)

Цель сценария 2.1 – изучение принципов формирования и использования таблицы mac-адресов коммутатора.

Задачи:

- Просмотреть таблицу mac-адресов на коммутаторе;
- Перейти в режим simulation
- Создать трафик в локальной сети с помощью echo запроса от компьютера PC D к компьютеру PC A;
- Снова просмотреть на таблицу mac-адресов на коммутаторе;
- Сопоставить mac-адреса из таблицы с компьютерами;
- Сделать выводы.

Сценарий 2.2

Сценарий 2.2 содержит созданную заранее логическую топологию, из трех компьютеров и четырех коммутаторов. Линки между коммутаторами образуют два замкнутых контура.

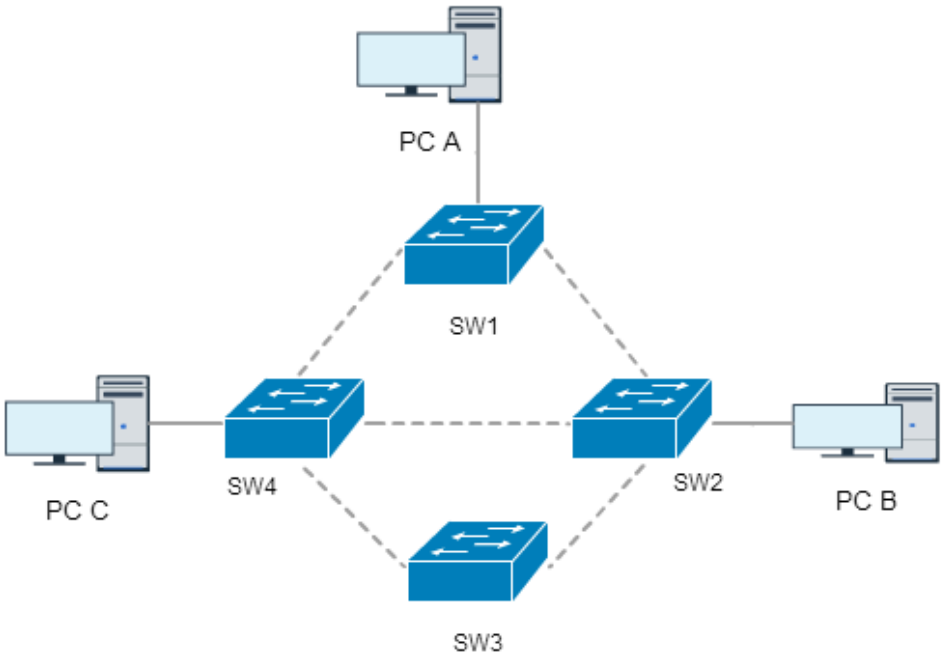

Рис. 2.8. Топология сети (сценарий 2.2)

Цель сценария 2.2 – изучение алгоритма работы протокола STP.

Задачи:

- Проверить роли коммутаторов. Найти root.
- Проверить роли портов.
- Перейти в режим simulation.
- Ввести в терминальной строке на компьютере PCA команду pingc IP адресом компьютера PCB.
- Проследить за прохождением пакета по сети.
- Сделать выводы.

Сценарий 2.3 (основной)

Сценарий 2.3 содержит созданную заранее сложную логическую топологию, включающую несколько компьютеров, несколько коммутаторов и маршрутизатор. Устройства не настроены.

Цель сценария 2.3 – изучение принципов и технологий работы виртуальных локальных сетей, протокола vtp, маршрутизации между виртуальными сетями по архитектуре router-on-a-stick.

Задачи подробно представлены ниже.

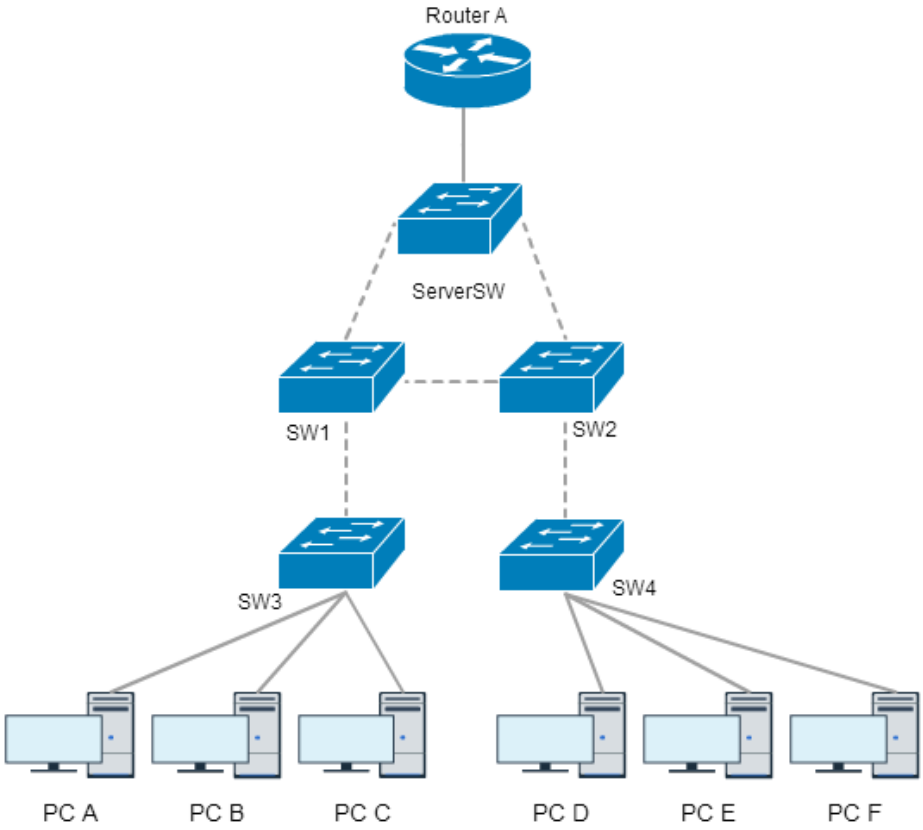

Рис. 2.9. Топология сети (сценарий 2.3)

2.3.1. Расчёт IP-адресов и настройка локальных сетей

Выполнить расчет основных сетевых параметров для сетей VLAN A, VLAN B, VLAN C исходя из известного количества узлов в каждой из них (согласно Вашему варианту), а также известного диапазона адресов для каждой из сетей: (где X – номер Вашего варианта):

- для сети VLAN A – 10.X.0.0/8;
- для сети VLAN B – 172.16.X.0/12;
- для сети VLAN C – 192.168.X.0/16.

Рассчитанные адреса занести в отчет.

Выполнить настройку компьютеров PC_A – PC_F (настроить IP-адрес, маску подсети и шлюз по умолчанию). Задать компьютерам IP-адреса из соответствующих диапазонов:

- PC A, PC D – VLAN A;
- PC B, PC E – VLAN B;
- PC C, PC F – VLAN C.

Как и ранее, использовать для компьютеров **максимальные** IP-адреса из доступных.

2.3.2. Настройка коммутаторов

Выполнить первоначальную настройку коммутаторов (присвоить символьные имена, задать пароли для доступа к консоли и привилегированному режиму, включить шифрование всех паролей и добавить баннер). *Подробнее о первоначальной настройке устройств см. методические рекомендации к лабораторной работе №1.*

Настроить магистральные соединения между всеми коммутаторами и маршрутизатором, переведя соответствующие интерфейсы в режим trunk.

2.3.3. Настройка VLAN и протокола vtp

На коммутаторе ServerSW создать 3 виртуальные сети с номерами:
VLAN A = номер студента по списку + 10,
VLAN B = номер студента по списку + 11,
VLAN C = номер студента по списку + 12.
Название VLAN задать в формате #Фамилия.

Пример: Студент с номером 34 Василий Пупкин создает виртуальные сети 44,45,46 с именами 44pupkin, 45pupkin, 46pupkin.

Выполнить настройку протокола vtp на всех коммутаторах. Пошаговая инструкция по настройке протокола vtp в режиме глобальной конфигурации:

- задать режим работы vtp (клиент, сервер, прозрачный); роль сервера назначить коммутатору ServerSw;
- задать имя домена (использовать ФИО и номер варианта);
- задать пароль (использовать ФИО и номер варианта);
- вернуться в привилегированный режим и убедиться, что протокол настроен корректно (просмотреть сведения о состоянии работы протокола vtp).

Пример. Студент Василий Пупкин имеет вариант 34. Тогда домен и пароль vtp должны иметь вид vpupkin34.

На коммутаторах уровня доступа настроить интерфейсы для компьютеров в режиме access, назначив соответствующие номера VLAN. Необходимые сведения о принадлежности компьютеров к той или иной виртуальной сети указаны в п. 2.3.1.

Убедиться, что интерфейсы настроены верно (просмотреть сведения о конфигурации интерфейсов) и занести конфигурацию в отчет.

2.3.4. Настройка маршрутизатора

Выполнить первоначальную настройку маршрутизатора. *Подробнее о первоначальной настройке устройств см. методические рекомендации к лабораторной работе №1.*

Создать и настроить на интерфейсе Fa0/0 по одному суб-интерфейсу для каждой виртуальной сети. Пошаговая инструкция по настройке суб-интерфейса:

- создать суб-интерфейс;
- назначить ему IP-адрес и маску подсети (для своего VLAN);
- включить инкапсуляцию по стандарту 802.1q и задать соответствующий номер VLAN;
- убедиться, что суб-интерфейс настроен верно (просмотреть сведения о конфигурации интерфейсов) и занести конфигурацию в отчет.

2.3.5. Анализ пакета в режиме симуляции

Сети настроены. Посмотрим, как передаются пакеты между узлами одной виртуальной сети, а также из одной виртуальной сети в другую.

Перейти в режим simulation.

Послать echo запрос с компьютера PCA на PCD.

Для этого ввести в терминальной строке (приложение command prompt) на компьютере – источнике запроса команду **ping** с IP-адресом компьютера – получателя запроса и проследить за прохождением пакета по сети, изменением адресов в заголовках сетевого и канального уровней.

Повторить анализ для пакета, отправленного с PCA на PCE.

Полученные данные и выводы занесите в отчет.

2.4. Контрольные вопросы

1. Какие задачи решает канальный уровень модели OSI?
2. Какие устройства относятся к канальному уровню OSI? Чем они отличаются друг от друга?
3. Что такое коммутатор?
4. Что собой представляет MAC-адрес? Как он используется?
5. Как и для чего используется таблица MAC-адресов? Какие сведения в ней хранятся? Как она заполняется и очищается? Как просмотреть ее содержимое?
6. Для чего используется протокол STP? Каков алгоритм его работы?
7. В каких трех основных состояниях могут находиться порты коммутаторов с точки зрения протокола STP?

8. Как выбирается корневой коммутатор? Какова его роль в сети?
9. Где и как выбираются корневые порты?
10. Где и как выбираются назначенные порты?
11. Что такое виртуальная локальная сеть (VLAN)?
12. Для чего используются VLAN-ы?
13. Какой стандарт описывает инкапсуляцию Ethernet-кадров для работы в среде с VLAN? Как и где осуществляется эта инкапсуляция?
14. Как передать трафик из одного VLAN в другой?
15. Что такое суб-интерфейс? Какие параметры являются ключевыми при конфигурировании суб-интерфейсов?
16. Что собой представляет топология router-on-a-stick? В чем ее преимущества перед ранее использованными схемами?
17. Опишите трехуровневую иерархическую модель сети. Определите назначения уровней ядра, распределения, доступа.

2.5. Варианты индивидуальных заданий

Номер варианта	**Количество узлов в сети**		
	LAN A	**LAN B**	**LAN C**
1	1024	464	7
2	255	178	65
3	1987	56	13
4	756	167	78
5	267	263	36
6	978	512	24
7	1654	189	15
8	367	134	5
9	145	98	198
10	826	129	98
11	1100	624	9
12	752	63	28
13	314	289	130
14	1456	604	29
15	1358	230	55

2.6. Форма отчета

Отчет о выполнении лабораторной работы оформляется строго в соответствии с индивидуальным вариантом задания и является обязательным требованием для допуска к защите наряду с правильно настроенными сценариями работы в программе Packet Tracer.

Отчет должен включать титульный лист схему сети, а также заполненные таблицы, приведенные ниже.

Сценарий 1 – Сведения о конфигурации устройств

Устройство	Интерфейс	IP-адрес	MAC-адрес
PC A	NIC		
PC B	NIC		
PC C	NIC		
PC D	NIC		

Сценарий 1 – Таблица MAC-адресов

Изначальная	После отправки пакета PCD-PCA

Сценарий 2 – STP – Роли коммутаторов и состояния портов

Устройство	Роль	Интерфейс	Состояние порта
SW1	Отметьте корневой коммутатор в столбце слева		
SW2			
SW3			
SW4			

Сценарий 3 – Расчет адресов сетей

Параметр	VLAN A	VLAN B	VLAN C
Количество узлов			
Ближайшая сверху степень двойки			
Маска (префиксная)			
Маска (десятичная)			
SUBNET			
HOSTMIN (router)			
HOSTMAX (host)			
BROADCAST			

Сценарий 3 – Сведения о конфигурации L3 устройств

Устройство	Интерфейс	IP-адрес	Маска подсети	Основной шлюз
PC A	NIC			
PC B	NIC			
PC C	NIC			
PC D	NIC			
PC E	NIC			
PC F	NIC			
Router	Fa0/0.____			
	Fa0/0.____			
	Fa0/0.____			
	Fa0/0			

Сценарий 3 – Сведения о конфигурации L2 устройств

Устройство	VTP Домен VTP Пароль VTP-Роль	Интерфейс	VLAN или trunk
SW1			
SW2			
SW3			
SW4			
ServerSw			

Сценарий 3 – Анализ маршрута и заголовков пакета PC A – PC D

На устройстве	IP-адрес		MAC-адрес	
	Source	Destination	Source	Destination

Сценарий 3 – Анализ маршрута и заголовков пакета PC A – PC E

На устройстве	IP-адрес		MAC-адрес	
	Source	Destination	Source	Destination