Оглавление

1 Обзор симулятора Cisco Packet Tracer

Cisco Packet Tracer – это многофункциональная программа моделирования сетей, которая позволяет студентам экспериментировать с поведением сети и оценивать возможные сценарии. Packet Tracer предоставляет функции моделирования, визуализации, авторской разработки, аттестации и совместного сотрудничества, а также облегчает преподавание и изучение сложных технологических принципов.

1.1 Загрузка Cisco Packet Tracer

Для загрузки Packet Tracer, выполните следующие действия:

1. Зарегистрируйтесь по ссылке https://www.netacad.com/ru/courses/packet-tracer/introduction-packet-tracer.
2. Запишитесь на курс Introduction to Packet Tracer.
3. Завершите регистрацию в Сетевой академии.
4. Запустите курс Introduction to Packet Tracer.
5. Инструкции по загрузке находятся в материалах курса.

1.2 Интерфейс Cisco Packet Tracer

После запуска Cisco Packet Tracer, по умолчанию открывает главное окно программы. Данное окно содержит следующие области:

1. Главное меню. Данная панель содержит основные команды.
2. Основная панель инструментов. На этой панели отображаются значки ярлыков для наиболее часто используемых команд меню.
3. Панель общих инструментов. Эта панель предоставляет доступ к следующим часто используемым инструментам рабочей области: «Select», «Inspect», «Delete», «Resize Shape», «Place Note», «Drawing Palette», «Add Simple PDU», и «Add Complex PDU».
4. Логическое / физическое рабочее пространство и панель навигации. Позволяет переключаться между Физическим рабочим пространством и Логическим рабочим пространством с помощью вкладок на этой панели.
5. Рабочая область. Отображает созданную сеть, позволяет наблюдать за симуляциями и просматривать различную информацию и статистику.
6. Панель переключения режимов реального времени / симуляции. Позволяет переключаться между режимом реального времени и режимом симуляции с помощью вкладок на этой панели. Кроме того, она содержит часы, которые отображают относительное время в режиме реального времени и режиме моделирования.

7. Панель компонентов сети. В данной панели находятся устройства и соединения предназначенные для размещения в рабочей области. Панель содержит окно выбора типа устройства и окно выбора конкретного устройства.

8. Панель выбора типа устройства. На этой панели содержатся типы устройств и подключений, доступных в Packet Tracer.

9. Панель выбора для конкретного устройства. В этом поле выбираются устройства которые необходимо добавить в сеть и какие подключения установить.

10. Панель созданных пакетов. Эта панель управляет пакетами, которые были помещены в сеть во время сценариев моделирования.

1.3 Работа с объектами сети

Для размещения сетевого объекта на схеме необходимо выбрать в нижней панели инструментов его класс, а затем модель. Выбрав необходимое оборудование его можно перетащить в рабочую область или щелчком мышки указать место в рабочей области, куда следует его поместить.

Для соединения сетевых устройств необходимо выбрать класс «Соединительные кабели», далее выбрать необходимый тип кабеля (или выбрать «автоматическое определение»), указать начальное устройство, выбрать один из его сетевых портов, затем указать конечное устройство и один из его портов. В случае применения объекта «Автоматическое определение типа сетевого кабеля», порт и тип кабеля будут выбираться автоматически (номер порта будет выбираться в порядке возрастания).

Конфигурирование устройства производится по двойному щелчку на нем. В открывшемся окне пользователь может включить/выключить устройство (соответствующим тумблером на его изображении в области «Physical Device View»), изменить аппаратурную конфигурацию добавив или удалить модули, используя область MODULES.

Выбрав вкладку «Config» пользователь может задать некоторые конфигурационные параметры (например, настроить сетевой интерфейс, определить имя устройства и т.п.). На вкладке «CLI» предоставляется доступ к командному интерфейсу устройства (если он предусмотрен).

Для конечных устройств реализованы дополнительные вкладки. На вкладке «Desktop» расположены эмуляторы работы некоторых утилит рабочего стола (командная строка, интернет-браузер и т.п.). «Software/Services» - конфигурирование программного обеспечения, которое должно быть установлено на реально действующем конечном устройстве.

1.4 Пошаговая отладка передачи информации в исследуемой сети

Отладка исследуемой сети может производиться двумя способами: имитируя деятельность администратора с реальным оборудованием (Realtime) и с применением средств моделирования (Simulation).

В первом случае пользователь среды может выполнять необходимые действия над сетевыми объектами и принимать решения о функциональности собранной им сети. Во втором случае используются встроенные средства среды имитационного моделирования, которые позволяют пошагового наглядно продемонстрировать этапы передачи информации по сети.

Анализируемые задания по передачи данных по сети объединяются в сценарий. В среде допускает создавать несколько сценариев и переключаться между ними для анализа работы сети.

Для создания задания по передаче данных по протоколу ICPM (ping) используется кнопка «Add Simple PDU». Пользователь задает начальный сетевой узел (который будет генерировать данные) и конечный сетевой узел. В результате автоматически создается одно задание в текущем сценарии.

Для формирования передач данных по сети с указанием параметров передаваемой информации (протокол, порт и т.п.) используется кнопка «Add Complex PDU». Нажав на соответствующую кнопку в вертикальной панели пользователь должен указать протокол передачи, источник передаваемой информации и задать дополнительные параметры.

Результаты выполнения заданий по передаче данных отображаются в области сценариев. В режиме реального времени результаты выполнения заданий выводятся сразу же по окончании имитации. В случае, если пользователь попытается при создании простого задания указать устройство (источник или приемник), не имеющего настроенного сетевого интерфейса, то сразу будет выдано сообщение об ошибке.

Переключившись в режим пошагового выполнения пользователь получает возможность наглядно посмотреть каким образом передаются данные по сети. Переход к следующему шагу производится нажатием на кнопку «Next». Перейти к предыдущему шагу можно нажав на клавишу «Back». Нажав на кнопку «Play» запускается автоматический переход к следующему шагу. Кнопка «Reset simulation» – сбрасывает исследуемую сеть в исходное состояние. При выборе пакета в списке открывается окно в котором содержится значения полей PDU всех уровней модели OSI.

2 Конфигурирования устройств Cisco

2.1 Интерфейс командной строки Cisco IOS

Интерфейс командной строки (CLI) Cisco IOS – основной интерфейс, используемый для конфигурирования, мониторинга и обслуживания устройств Cisco. Этот пользовательский интерфейс позволяет непосредственно выполнять команды Cisco IOS с помощью консоли маршрутизатора, терминала или с использованием удаленного доступа.

Чтобы облегчить конфигурирование устройств Cisco, интерфейс командной строки Cisco IOS разделен на отдельные командные режимы. В каждом командном режиме предусмотрен собственный набор команд для конфигурирования, обслуживания и мониторинга работы маршрутизатора и сети. Совокупность доступных в конкретный момент команд зависит от текущего командного режима. Ввод вопросительного знака (?) после системного приглашения позволяет вывести список доступных команд для каждого командного режима.

Применение определенных команд обеспечивает переход от одного командного режима к другому. Стандартный порядок, в котором пользователю следует осуществлять доступ к режимам, таков: пользовательский режим EXEC, привилегированный режим EXEC; режим глобальной конфигурации; режимы специальной конфигурации, подрежимы конфигурации и подрежимы конфигурации 2-го уровня.

Сеанс на маршрутизаторе обычно начинается в пользовательском режиме EXEC, который представляет собой один из двух уровней доступа режима EXEC. В целях безопасности в пользовательском режиме EXEC доступно лишь ограниченное подмножество команд EXEC. Этот уровень доступа предназначен для задач, не изменяющих конфигурацию маршрутизатора, например, определение статуса маршрутизатора.

Для получения доступа ко всем командам необходимо перейти в привилегированный режим EXEC, который обеспечивает второй уровень доступа режима EXEC. Обычно для входа в привилегированный режим EXEC требуется ввести пароль. В привилегированном режиме EXEC можно вводить любую команду EXEC.

Приведенный ниже пример демонстрирует процесс доступа к привилегированному режиму EXEC:

```
Router> enable
Password:<letmein>
Router#
```

Из привилегированного режима EXEC можно перейти в режим глобальной конфигурации. В этом режиме возможен ввод команд, позволяющих конфигурировать общие характеристики системы. Режим глобальной конфигурации может использоваться также для перехода в специфические режимы конфигурирования. Режимы конфигурирования, включая режим глобальной конфигурации, позволяют вносить изменения в текущую конфигурацию. Если конфигурация позднее сохраняется, то эти команды сохраняются после перезагрузки маршрутизатора.

В приведенном ниже примере показан процесс перехода в режим глобальной конфигурации из привилегированного режима EXEC:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Команды, вводимые в режиме глобальной конфигурации, при вводе изменяют текущую конфигурацию. Иными словами, изменения конфигурации вступают в силу при каждом нажатии клавиши Enter или Return после ввода правильной команды. Тем не менее эти изменения не сохраняются в файле конфигурации запуска, пока не будет введена команда режима EXEC:

```
Router# copy running-config startup-config
```

Из режима глобальной конфигурации можно перейти во множество режимов конфигурации, специфических для конкретного протокола или функции. В следующем примере пользователь входит в режим конфигурирования интерфейса FastEthernet0/0. Новое приглашение hostname(config-if)#, указывает на режим конфигурирования интерфейса.

```
Router(config)# interface FastEthernet0/0
Router(config-if)#
```

Из режима конфигурирования интерфейса можно перейти в режим конфигурирования субинтерфейса. В режиме конфигурирования субинтерфейса можно задавать параметры множества виртуальных интерфейсов (они называются субинтерфейсами) на единственном физическом интерфейсе.

В следующем примере задаются параметры субинтерфейса. Субинтерфейс получает обозначение "0.1", указывающее на то, что это субинтерфейс 0 линии 2. Приглашение hostname(config-subif)#, указывает на конфигурирование субинтерфейса.

```
Router(config)# interface FastEthernet0/0
Router(config-if)# interface FastEthernet0/0.1
Router(config-subif)#
```

2.2 Дополнение частичного имени команд

Если не удается запомнить полное имя команды или хотелось бы сократить количество вводимых символов, можно вводить первые несколько букв команды и затем нажать клавишу Tab. Синтаксический анализатор командной строки дополнит команду, если введенная строка уникальна для данного командного режима.

Интерфейс командной строки распознает команду в том случае, если введено достаточно символов, чтобы сделать команду уникальной. Например, при вводе conf в привилегированном режиме EXEC интерфейс командной строки сможет ассоциировать введенные символы с командой configure, так как только команда configure начинается с conf. В следующем примере CLI распознаёт уникальную для привилегированного режима EXEC строку conf при нажатии клавиши Tab:

```
Router# conf<Tab>
Router# configure
```

При использовании функции дополнения команды интерфейс командной строки отображает полное имя команды. Команда не выполняется, пока не будет нажата клавиша Enter или Return. Благодаря этому есть возможность изменить команду, если полная команда – это не то, что требовалось ввести с помощью сокращения. Если введена совокупность символов, которые могут обозначать более одной команды, система выдает сообщение, указывающий на то, что строка не уникальна.

Если CLI не может дополнить команду, можно ввести вопросительный знак (?), чтобы получить список команд, начинающихся с этой совокупности символов. Не оставляйте пробел между последней введенной буквой и вопросительным знаком (?).

Например, при вводе co? будет выведен список всех команд, доступных в текущем командном режиме:

```
Router# co?
configure connect copy
Router# co
```

Обратите внимание на то, что символы, введенные до вопросительного знака, отображаются на экране, чтобы дать возможность закончить ввод команды.

2.3 VLAN

В терминологии Cisco определяется два типа VLAN портов:

1. access – порт принадлежащий одному VLAN и передающий нетегированный трафик

2. trunk – порт передающий тегированный трафик одного или нескольких VLAN.

Dynamic Trunk Protocol (DTP) — проприетарный протокол Cisco, который позволяет коммутаторам динамически распознавать настроен ли соседний коммутатор для поднятия транка и какой протокол использовать (802.1Q или ISL). Включен по умолчанию.

Создание VLAN с идентификатором 2 и задание имени для него:

```
Switch(config)# vlan 2
Switch(config-vlan)# name test
```

Удаление VLAN с идентификатором 2:

```
Switch(config)# no vlan 2
```

Настройка access портов

Задание access порта:

```
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
```

Просмотр информации о VLAN'ax:

```
Switch# show vlan brief
```

Настройка trunk портов

Задание trunk порта:

```
Switch(config)# interface fa0/22
Switch(config-if)# switchport mode trunk
```

Настройка разрешенных VLAN

По умолчанию в транке разрешены все VLAN. Можно ограничить перечень VLAN, которые могут передаваться через конкретный транк.

Указать перечень разрешенных VLAN для транкового порта fa0/22:

```
Switch(config)# interface fa0/22
Switch(config-if)# switchport trunk allowed vlan 1-2,10,15
```

Добавление ещё одного разрешенного VLAN:

```
Switch(config)# interface fa0/22
Switch(config-if)# switchport trunk allowed vlan add 160
```

Удаление VLAN из списка разрешенных:

```
Switch(config)# interface fa0/22
Switch(config-if)# switchport trunk allowed vlan remove 160
```

Native VLAN

В стандарте 802.1Q существует понятие native VLAN. Трафик этого VLAN передается нетегированным. По умолчанию это VLAN 1. Однако можно изменить это и указать другой VLAN как native.

Настройка VLAN 5 как native:

```
Switch(config-if)# switchport trunk native vlan 5
```

2.4 Лабораторная работа №1. Базовая настройка коммутатора

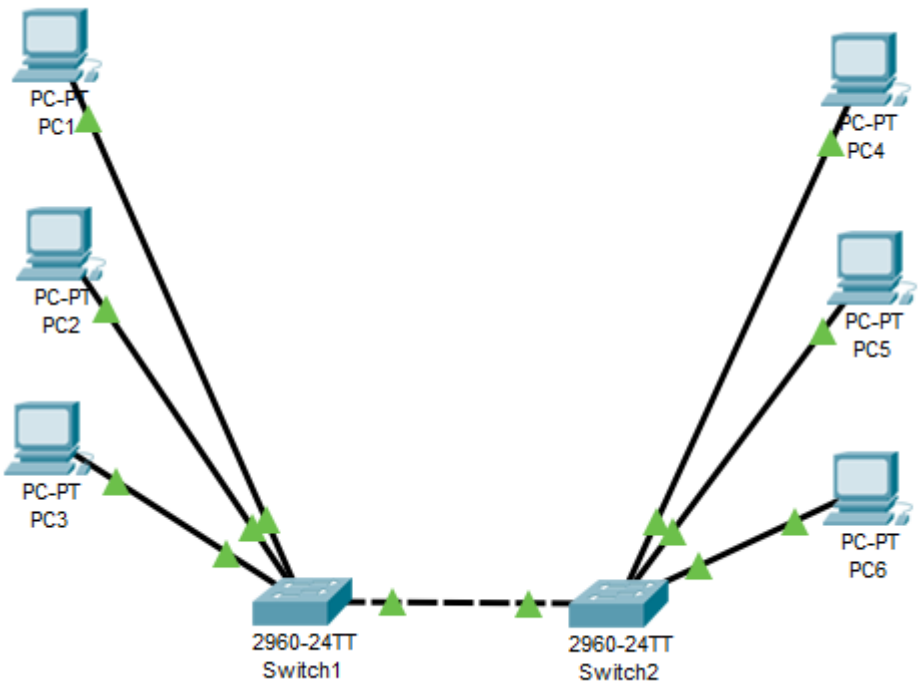

Рисунок 1 – Схема сети

Изначально мы попадаем в пользовательский режим. Он имеет ограниченные возможности. Этот режим выглядит таким образом:

Switch>

1. Задание имени и домена коммутатора

Для этого нужно переключить в привилегированный режим командой:

Switch>enable

Далее переключаемся в режим глобальной конфигурации:

Switch#configure terminal (Switch#conf t)

Задаем имя коммутатора

Switch(config)#hostname sw1

Задаем имя домена
sw1 (config)#ip domain-name sw1.sw

2. Создание пользователя для доступа к коммутатору

Создадим пользователя admin с максимальными правами доступа 15 с паролем 123abc
sw1(config)#username admin privilege 15 secret 123abc

3. Задание пароля на привилегированный режим:

sw1 (config)#enable secret 123abc

4. Запрет нежелательного поиска в DNS:

sw1 (config)#no ip domain-lookup

5. Настройка IP-адреса на Switch Virtual Interface (SVI) коммутатора

Для удаленного управления коммутаторов настроим IP-адрес на vlan1
sw1(config)#interface vlan1

Далее присвоим ip-адрес и маску подсети выбранному vlan1
sw1 (config-if)#ip address 192.168.1.2 255.255.255.0

Включаем vlan1
sw1(config-if)#no shutdown

6. Ограничение доступа к консольному порту

sw1(config)#line console 0

sw1(config-line)#password 123abc

sw1(config-line)#login local

7. Настроим линии Virtual Teletype (VTY) для коммутатора, чтобы разрешить удаленный доступ по протоколу SSH

Генерация RSA ключа:
sw1 (config)# crypto key generate rsa

Настроим линии Virtual Teletype (VTY):
sw1(config)#line vty 0 4

sw1(config-line)#transport input ssh

sw1(config-line)#login local

Также можно активировать шифрование паролей командой:
sw1(config)# service password-encryption

8. Настроим для используемых интерфейсов duplex-режим и скорость

Данной командой выбираем нужные интерфейсы:
sw1(config)#int range fa0/1-0/4

Настройка duplex-режима
sw1(config-if-range)#duplex full

Настройка скорости
sw1(config-if-range)#speed 100

9. Сохранение настроек коммутатора

sw1#write memory

2.5. Агрегирование каналов

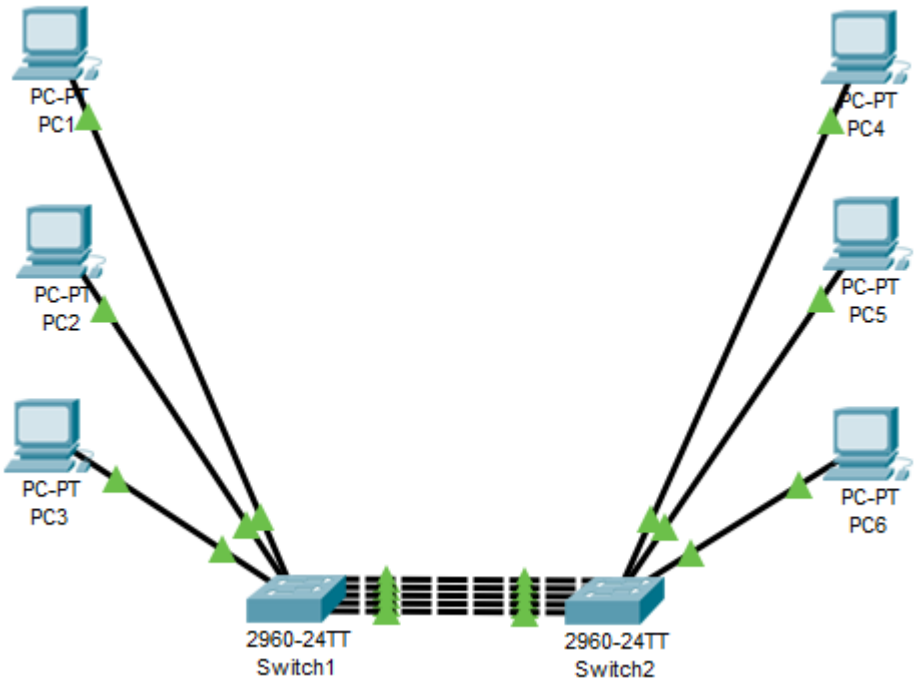

Рисунок 2 – Схема агрегирования каналов

3.2.1 Описание хода настройки коммутатора
Существует 3 вида агрегирования каналов:

a) LACP (Link Aggregation Control Protocol) стандартный протокол
b) PAgP (Port Aggregation Protocol) проприетарный протокол Cisco
c) Статическое агрегирование без использования протоколов

Рассмотрим настройку агрегированного канала:

a) Настройка с помощью LACP

Настраиваем 1 коммутатор:

1. Выбираем группу интерфейсов для агрегированного канала

sw1(config)#int range fa0/4-0/8

2. Выключаем их
sw1(config-if)#shutdown

3. Создаем интерфейс port-channel 1 (это и будет виртуальный интерфейс агрегированного канала) и переводим его в режим active.

sw1(config-if)#channel-group 1 mode active

4. Включаем интерфейсы
sw1(config-if)#no shutdown

Настраиваем 2 коммутатор:

1. Выбираем группу интерфейсов для агрегированного канала
sw1(config)#int range fa0/4-0/8

2. Выключаем их
sw1(config-if)#shutdown

3. Создаем port-channel 1 и переводим в режим passive (включится, когда получит LACP-сообщение)
sw1(config-if-range)#channel-group 1 mode passive

4. Включаем интерфейсы
sw1(config-if)#no shutdown

b) Настройка с помощью PAgP

Настраиваем 1 коммутатор:

1. Выбираем группу интерфейсов для агрегированного канала
sw1(config)#int range fa0/4-0/8

2. Выключаем их
sw1(config-if)#shutdown

3. Создаем port-channel и переключаем его в режим desirable (то есть включить)
sw1(config-if-range)#channel-group 1 mode desirable

4. Включаем интерфейсы
sw1(config-if)#no shutdown

Настраиваем 2 коммутатор:

1. Выбираем группу интерфейсов для агрегированного канала
sw1(config)#int range fa0/4-0/8

2. Выключаем их
sw1(config-if)#shutdown

3. Создаем port-channel и переводим в auto (включиться, если получит PAgP-сообщение)
sw1(config-if-range)# channel-group 1 mode auto

4. Включаем интерфейсы
sw1(config-if)#no shutdown

c) Статическое агрегирование без использования протоколов
Настройка для первого и второго коммутаторов:
1. Выбираем группу интерфейсов для агрегированного канала
sw1(config)#int range fa0/4-0/8

2. Выключаем их
sw1(config-if)#shutdown

3. Выполняем команду агрегирования каналов
sw1(config-if)# channel-group 1 mode on

4. Включаем интерфейсы
sw1(config-if)#no shutdown

2.6.Настройка VLAN при помощи access портов

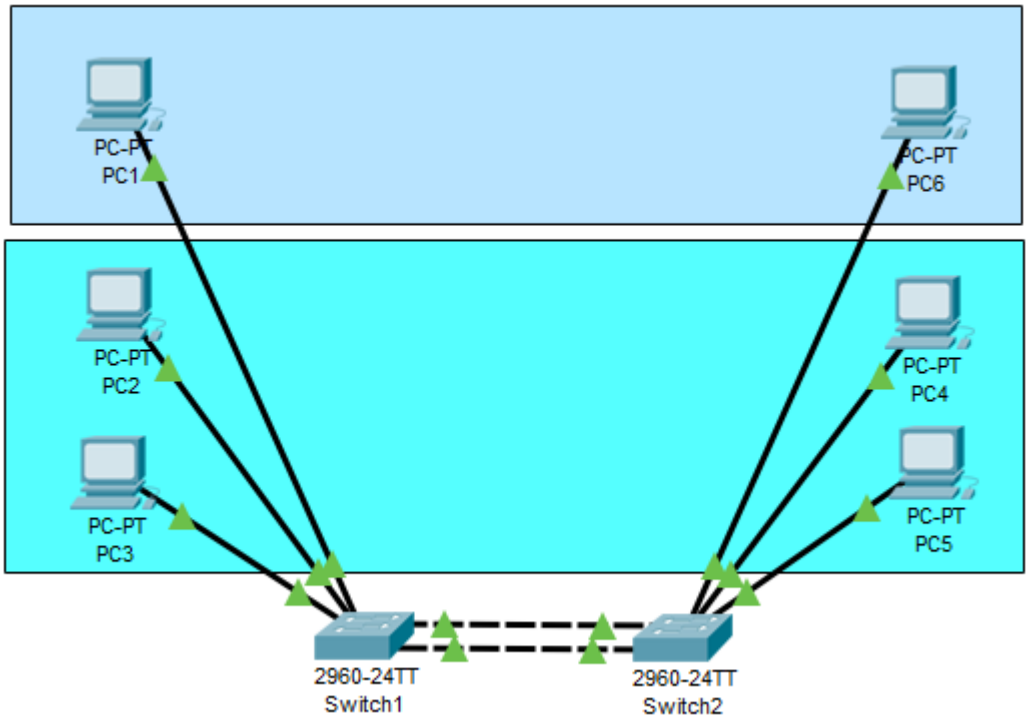

Рисунок 3 – Настройка VLAN с access-портами

Настройка Vlan одинакова на обоих коммутаторах.

Приведем пример настройки для одного коммутатора

1. Создадим vlan2 и vlan3 и добавим названия:
sw1(config)# vlan 2

sw1(config-vlan)# name group1

sw1(config)# vlan 3

sw1(config-vlan)# name group2

2. Настроим access порты для компьютеров и присвоим определенному vlan
sw1(config)# interface range fa0/1-2

sw1(config-if)# switchport mode access

sw1(config-if)# switchport access vlan 2

sw1(config)# interface fa0/3

sw1(config-if)# switchport mode access

sw1(config-if)# switchport access vlan 3

3. Настроим access порты между коммутаторами и присвоим определенному vlan
sw1(config)# interface fa0/4

sw1(config-if)# switchport mode access

sw1(config-if)# switchport access vlan 2

sw1(config)# interface fa0/5

sw1(config-if)# switchport mode access

sw1(config-if)# switchport access vlan 3

2.7. Настройка VLAN с помощью trunk-портов

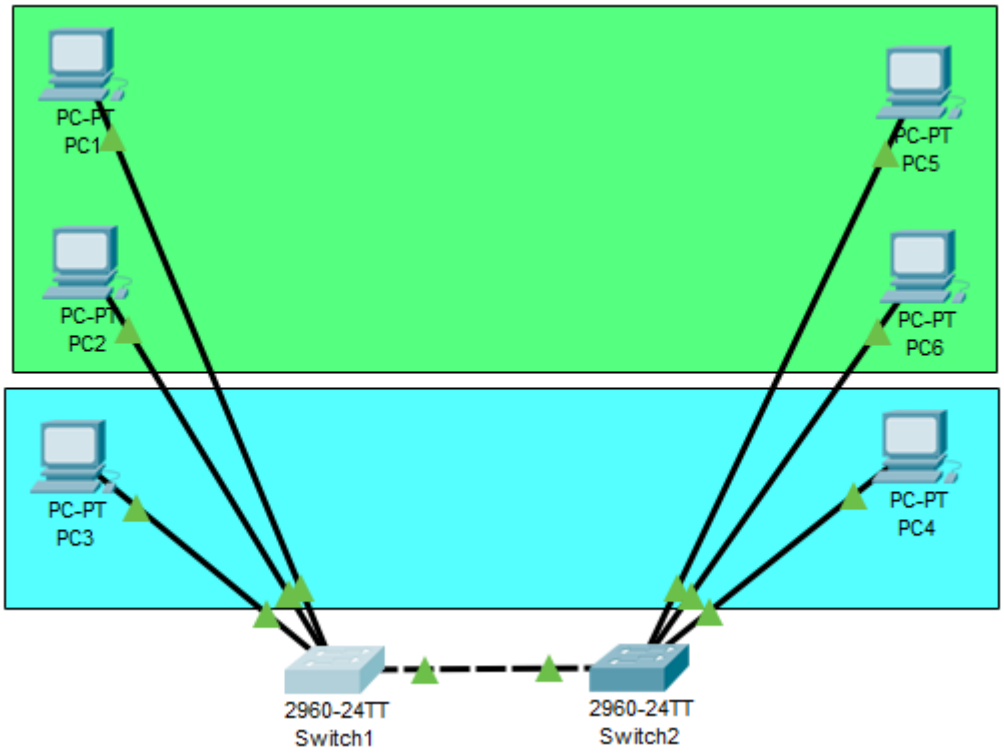

Рисунок 4 – Настройка VLAN с trunk-портами

Настройка Vlan одинакова на обоих коммутаторах.

Приведем пример настройки для одного коммутатора

1. Создадим vlan2 и vlan3 и добавим названия:
sw1(config)# vlan 2

sw1(config-vlan)# name group1

sw1(config)# vlan 3

sw1(config-vlan)# name group2

2. Настроим access порты для компьютеров и присвоим определенному vlan

sw1(config)# interface range fa0/1-2

sw1(config-if)# switchport mode access

sw1(config-if)# switchport access vlan 2

sw1(config)# interface fa0/3

sw1(config-if)# switchport mode access

sw1(config-if)# switchport access vlan 3

3. Настроим trunk порты между коммутаторами и присвоим определенному vlan
sw1(config)# interface fa0/4

sw1(config-if)# switchport mode trunk

По умолчанию в транке разрешены все VLAN. Можно ограничить перечень VLAN, которые могут передаваться через конкретный транк.
Указать перечень разрешенных VLAN для транкового порта fa0/4:
sw1(config-if)# switchport trunk allowed vlan 2,3

2.8. Настройка VLAN с помощью trank-channel

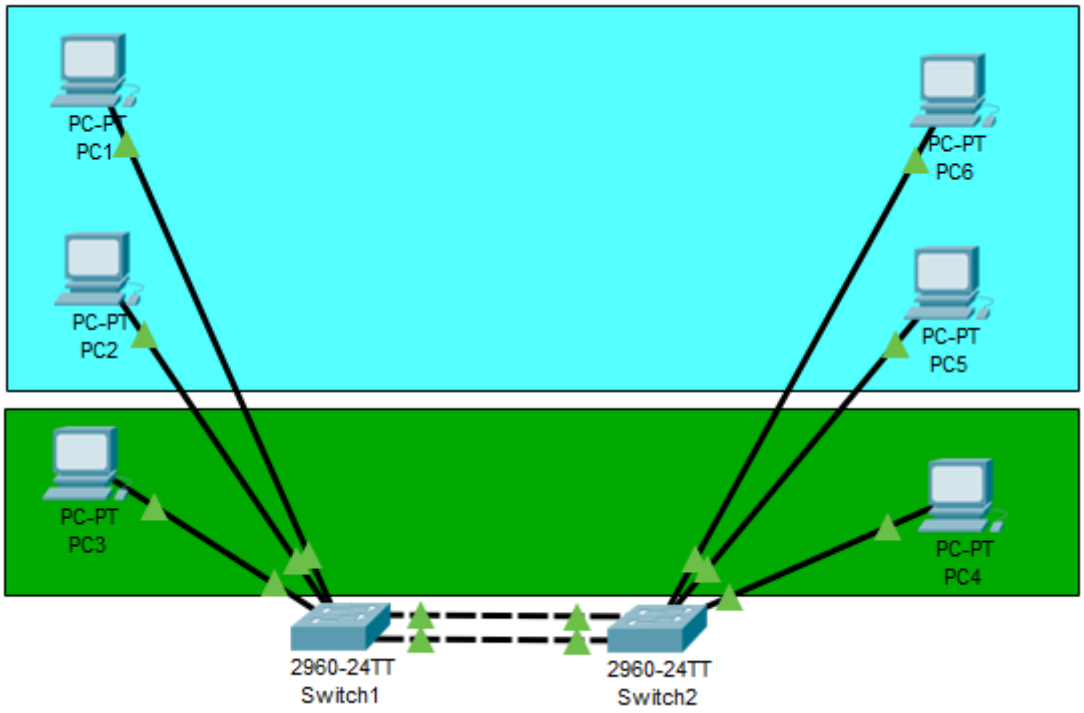

Рисунок 5 – Настройка VLAN с trunk-channel

Приведем пример настройки для одного коммутатора
1. Создадим vlan2 и vlan3 и добавим названия:
sw1(config)# vlan 2

sw1(config-vlan)# name group1

sw1(config)# vlan 3

sw1(config-vlan)# name group2

2. Настроим access порты для компьютеров и присвоим определенному vlan
sw1(config)# interface range fa0/1-2

sw1(config-if)# switchport mode access

sw1(config-if)# switchport access vlan 2

sw1(config)# interface fa0/3

sw1(config-if)# switchport mode access

sw1(config-if)# switchport access vlan 3

3. Проведем агрегирование каналов между коммутаторами
sw1(config)#int range fa0/4-0/5

sw1(config-if)#shutdown

sw1(config-if)# channel-group 1 mode on

sw1(config-if)#no shutdown

4. Создаем trunk-канал
sw1(config)# interface fa0/4

sw1(config-if)# switchport mode trunk

Список литературы

1. Служба поддержки Cisco [Электронный ресурс] – URL: https://www.cisco.com/c/ru_ru/support

2. Сборник статей по сетевым технологиям [Электронный ресурс] – URL:http://xgu.ru

3. Jesin A.Packet Tracer NetworkSimulator. Birmingham: Packt Publishing, 2014 — 134c.

4. Odom W. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-105: маршрутизация и коммутация. Москва: Вильямс, 2019 — 1452c.

5. Bonnie J. Cisco IOS in a Nutshell, 2nd Edition. Sebastopol: O'Reilly Media, 2009. — 800 c

6. Andrew S. Tanenbaum, David J. Wetherall. Компьютерные сети. СПб.: Питер, 2012. — 960 c