Packet Tracer – Сравнение управления через CLI и SDN Controller

Таблица адресации

Примечание. Все маски подсети — /24 (255.255.255.0).

Устройство	Интерфейс	Айпи адрес
R1	G0/0/0	192.168.101.1
	S0/1/0	192.168.1.2
R2	G0/0/0	192.168.102.1
	S0/1/1	192.168.2.2
R3	G0/0/0	10.0.1.1
	G0/0/1	10.0.2.1
	S0/1/0	192.168.1.1
	S0/1/1	192.168.2.1
SWL1	VLAN 1	192.168.101.2
SWL2	VLAN 1	192.168.102.2
SWR1	VLAN 1	10.0.1.2
SWR2	VLAN 1	10.0.1.3
SWR3	VLAN 1	10.0.1.4
SWR4	VLAN 1	10.0.1.5
Admin	сетевая карта	10.0.1.129
PC1	сетевая карта	10.0.1.130
PC2	сетевая карта	10.0.2.129
PC3	сетевая карта	10.0.2.130
PC4	сетевая карта	192.168.102.3
Example Server	сетевая карта	192.168.101.100
PT-Controller*	сетевая карта	192.168.101.254

* В части 3 вы добавите и настроите PT-Controller0.

Цели

Часть 1. Изучение топологии сети

Часть 2. Использование интерфейса командной строки для сбора информации

Часть 3. Настройка контроллера SDN

Часть 4. Использование контроллера SDN для обнаружения топологии

Часть 5. Использование контроллера SDN для сбора информации

Часть 6. Использование контроллера SDN для настройки параметров сети

Предыстория/сценарий

В этом упражнении Packet Tracer вы сравните различия между управлением сетью из интерфейса командной строки (CLI) и использованием контроллера программно-определяемой сети (SDN) для управления сетью.

Инструкции

Часть 1: Изучите топологию сети

В этой части вы познакомитесь с топологией, которую будете использовать для действий по программированию сети.

Шаг 1: Просмотрите документацию по конфигурации сети.

Сеть настроена следующим образом:

- Маршрутизаторы работают под управлением OSPFv2.
- SSH включен на всех устройствах с пользователем **cisco** и паролем **cisco123!**
- R1 не имеет хостов.
- R2 LAN IPv4 настроен статически.
- R3 — сервер DHCPv4 для LAN1 и LAN2.
- Коммутаторы относятся к уровню 2 (без VLAN).
- Все коммутаторы **SWR#** принадлежат LAN1.

Шаг 2: Убедитесь, что все устройства могут пинговать друг друга.

Либо используйте командную строку на каждом устройстве, либо используйте инструмент **Add Simple PDU (P)** , чтобы убедиться, что все устройства могут пинговать друг друга.

Часть 2: Используйте CLI для сбора информации

В этой части вы вручную получаете доступ к каждому устройству для сбора информации о версии программного обеспечения.

Шаг 1: С ПК администратора получите безопасный доступ к коммутатору SWR3.

a. Нажмите **Admin > Desktop > Command Prompt**.

b. Введите команду **ssh -l cisco 10.0.1.4** . Опция -l — это буква «L», а не цифра один.

c. При появлении запроса введите **cisco123!** как пароль. Теперь вы вошли в SWR3.

Шаг 2: Соберите информацию о программном обеспечении на SWR3.

a. Введите следующую команду, чтобы отфильтровать выходные данные команды **show version** для просмотра только ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ RELEASE, установленного на устройстве. Обратите внимание, что SWR3 работает под управлением IOS 16.3.2 и загрузчика 4.2.6.

```
SWR3# show version | include RELEASE
```

```
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Version 16.3.2, RELEASE SOFTWARE (fc4)
BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.26, RELEASE SOFTWARE (P)
SWR3#
```

b. Скопируйте информацию в буфер обмена

c. Откройте редактор текстовых файлов и вставьте информацию в текстовый файл.

d. Сохраните файл как **software-versions.txt** .

Шаг 3: Соберите информацию о программном обеспечении для остальных сетевых устройств.

a. Из **Command Prompt** на SWR3 получите безопасный доступ к другому сетевому устройству и повторите шаг 2 выше.

b. Продолжайте документировать версии программного обеспечения, пока не закончите работу со всеми девятью сетевыми устройствами: SWL1, SWL2, SWR1, SWR2, SWR3, SWR4, R1, R2 и R3.

c. Выйдите из всех ваших сеансов SSH.

Часть 3: Настройка PT-контроллера

В течение многих лет сетевые администраторы использовали ранние инструменты автоматизации, такие как сценарии bash или программное обеспечение с поддержкой SNMP, для выполнения процесса, аналогичного тому, что вы делали на предыдущем шаге. Однако с введением SDN этот процесс значительно улучшился. Packet Tracer предоставляет простой PT-контроллер для имитации контроллера SDN. В этой части вы подключите и настроите PT-контроллер.

Примечание . Чтобы узнать больше о реализации сетевого контроллера в Packet Tracer, щелкните меню **Help**, затем **Contents**. В указателе слева, примерно посередине, вы найдете заголовок **Configuring Devices**. Под этим заголовком найдите **Network Controllers**. Здесь вы найдете огромное количество информации, большую часть которой вы изучите в ходе занятий этого курса.

Шаг 1: Добавьте сетевой контроллер в топологию.

a. В левом нижнем углу интерфейса Packet Tracer щелкните **End Devices > Network Controller**.

b. Добавьте сетевой контроллер в пустое место слева от коммутатора **SWL1**. Имя уже должно быть **PT-Controller0.** Если нет, щелкните имя и измените его.

c. Внизу снова щелкните молнию для **Connections**. Нажмите на сплошной черный кабель **Copper Straight-Through**.

d. Нажмите **PT-Controller0** и выберите **GigabitEthernet0**. Затем нажмите **SWL1** и выберите первый доступный интерфейс Gigabit Ethernet.

Шаг 2: Настройте подключение для PT-Controller0.

a. Нажмите **PT-Controller0 > Config**.

b. Для **Gateway/DNS IPv4** введите 192.168.101.1 в качестве адреса **шлюза (Gateway).**

c. Слева в разделе **INTERFACE** щелкните **GigabitEthernet0** .

d. Для **IP Configuration** введите **IP-адрес** 192.168.101.254 и **маску подсети** 255.255.255.0.

e. Слева в разделе **REAL WORLD** нажмите **Controller**. Если **Server Status - Stopped**, перейдите к следующему шагу . Если **Server Status - Disabled in Preferences**, вам нужно будет включить внешний доступ, следуя этим инструкциям:

1) Выберите **Options > Preferences** в меню Packet Tracer.

2) Щелкните **Miscellaneous**.

3) В разделе **External Network Access** щелкните **Enable External Access for Network Controller REST API**.

4) Закройте **Preferences** и нажмите **PT-Controller0 > Config** , если это необходимо.

5) Слева в разделе **REAL WORLD** щелкните **Controller**.

f. **Server Status** теперь должен быть **Stopped**. Щелкните **Access Enabled**, чтобы включить его. **Server Status** изменится на **Listening on port 58000**. Если порт имеет другое значение, измените его на **58000** . Это номер порта в сценариях Python.

Шаг 3: Под администратором проверьте подключение к PT-Controller0.

Убедитесь, что администратор может выполнить эхо-запрос PT-Controller0. Если вы не можете выполнить эхо-запрос, убедитесь, что ваша конфигурация соответствует спецификациям, указанным на предыдущем шаге.

Шаг 4: Зарегистрируйте нового пользователя и войдите в PT-Controller0.

a. Нажмите **Admin > Desktop > Web Browser**.

b. Введите IPv4-адрес 192.168.101.254, чтобы получить доступ к **User Setup** для **PT-Controller0** .

c. Введите **cisco** в поле **Username** и **cisco123!** в полях **Password** и **Confirm Password**, а затем нажмите **SETUP**.

Примечание. Здесь вы можете использовать любое имя пользователя и пароль. Для простоты мы рекомендуем использовать общие учетные данные, используемые в остальной части действия.

d. На экране **User Login** введите свои учетные данные и нажмите **LOG IN**.

e. Теперь вы вошли в панель управления для **PT-Controller0** . На этом этапе может быть полезно развернуть окно, чтобы вы могли видеть весь интерфейс.

Часть 4: Использование контроллера SDN для обнаружения топологии

В этой части вы настроите PT-Controller0 для использования протокола обнаружения Cisco (CDP) для автоматического обнаружения девяти сетевых устройств в вашей топологии. PT-Controller0 также обнаружит все пять хост-устройств, подключенных к сети.

Шаг 1: Добавьте учетные данные для доступа ко всем сетевым устройствам в топологии.

a. В графическом интерфейсе **Network Controller** нажмите кнопку меню слева от логотипа Cisco.

b. Выберите **Provisioning**. Отсюда вы можете вручную добавить сетевые устройства. Однако вы будете использовать CDP для автоматического обнаружения устройств.

c. Щелкните **CREDENTIALS ,** а затем нажмите **+ CREDENTIAL** , чтобы добавить **New Credential**.

d. В поле **Username** введите **cisco**, а в поле **Password** введите **cisco123!** . Оставьте поле **Enable Password** пустым. В поле **Description** введите **admin credentials** и нажмите **OKAY**.

e. Новые учетные данные CLI теперь хранятся на PT-Controller0 для использования в задачах автоматизации.

Шаг 2: Используйте CDP для обнаружения всех устройств в сети.

a. Щелкните **DISCOVERY** и щелкните **+ DISCOVERY** , чтобы добавить **New Discovery**.

b. В поле **Name** введите **SWL1** . В качестве **IP-адреса** введите **192.168.101.2**. Для **CLI Credential List** раскройте список и выберите **cisco - admin credentials**.

c. Нажмите **ADD**.

d. Теперь вы должны увидеть **Status** - **In Progress**. Вы можете подождать, пока Packet Tracer закончит моделирование этого процесса. Или вы можете нажать кнопку **Fast Forward Time** в главном окне Topology, чтобы ускорить процесс.

Часть 5: Используйте контроллер SDN для сбора информации

В этой части вы будете использовать графический интерфейс PT-Controller0 для просмотра информации о сетевых устройствах и хост-устройствах в топологии. Вы просмотрите топологию, созданную контроллером, а затем выполните трассировку пути по сети.

Шаг 1: Просмотрите список обнаруженных сетевых устройств.

a. Щелкните **NETWORK DEVICE**. Теперь вы должны увидеть все девять перечисленных сетевых устройств.

b. Щелкните значок шестеренки рядом с именем хоста любого устройства, чтобы просмотреть информацию, собранную в процессе обнаружения. Обратите внимание, что указана **Software Version**, а также другая подробная информация об устройстве.

Шаг 2: Просмотрите список всех обнаруженных хост-устройств.

a. Вернитесь на панель инструментов. Нажмите меню рядом с логотипом Cisco, затем нажмите **Dashboard**. (Вы также можете просто щелкнуть баннер **Network Controller**, чтобы вернуться на **Dashboard** из любого места.)

b. На панели инструментов вы увидите диаграммы с количеством хостов, до которых можно добраться с помощью ping, и количеством управляемых сетевых устройств. Оба должны быть 100%.

c. Вы также должны увидеть плитки для **QoS** , **Network Device** и **Host**. Щелкните значок шестеренки для **хоста** . Вы перейдете на вкладку **HOSTS** для **ASSURANCE** .

d. На этой странице вы можете просмотреть всю информацию о подключении уровней 2 и 3 для каждого хоста, а также сетевых устройств, к которым они подключены.

e. Щелкните значок шестеренки рядом с любым хостом, чтобы просмотреть более подробную информацию.

Шаг 3: Просмотрите топологию, созданную PT-Controller0.

a. Откройте вкладку **TOPOLOGY**. Обратите внимание, что PT-контроллер динамически создал ту же топологию, которую вы видите в главном окне Packet Tracer.

b. В этом представлении вы можете щелкнуть любое сетевое устройство, чтобы просмотреть сведения о нем.

c. Вы также можете щелкнуть и перетащить значки устройств, чтобы изменить топологию. Однако ваши изменения не будут сохранены, когда вы покинете рабочее пространство **TOPOLOGY**.

Шаг 4: Проследите путь от одного устройства к другому устройству.

a. Перейдите на вкладку **PATH TRACE**.

b. Щелкните **+ PATH**, чтобы добавить **New Path**.

c. Проследите путь от одного конца сети до другого. Например, вы можете ввести IP-адреса для компьютеров с PC1 по PC4. Затем нажмите **OKAY**.

d. Щелкните новый путь, который был добавлен, чтобы инициировать трассировку пути.

Вы получите отчет о **маршруте**, в котором показаны все переходы от источника к месту назначения. Обратите внимание, что указана информация только об устройстве уровня 3.

Коммутаторы отображаются как **UNKNOWN** (НЕИЗВЕСТНОЕ) устройство. Это потому, что все они работают только на уровне 2.

Часть 6: Использование контроллера SDN для настройки параметров сети

Основным преимуществом автоматизации сети с использованием контроллера является возможность настроить глобальные сетевые параметры и политики для всех устройств, а затем применить эту конфигурацию одним нажатием кнопки. В этой части вы настроите **PT-Controller0** с сетевыми настройками для DNS, NTP и Syslog. Затем вы передадите эту конфигурацию на поддерживаемые сетевые устройства. Наконец, вы проверите и протестируете политику.

Шаг 1: Изучите конфигурацию Example server.

a. Нажмите **Example Server > Services**.

b. В разделе **SERVICES** щелкните **DNS**. Обратите внимание, что служба DNS включена и имеется одна запись для www.example.com.

c. В разделе **SERVICES** щелкните **SYSLOG**. Обратите внимание, что служба системного журнала включена.

d. В разделе **SERVICES** щелкните **NTP**. Обратите внимание, что служба NTP включена.

Шаг 2: Настройте глобальную политику для DNS, SYSLOG и NTP.

a. Щелкните **Admin**. Если вы закрыли **Admin** , вам нужно будет открыть приложение **Web Browser** и повторно пройти аутентификацию с помощью **PT-Controller0** .

b. Щелкните меню слева от логотипа Cisco.

c. Щелкните **Policy**.

d. на вкладке **QOS** есть параметры для настройки **Scope** и **Policy** . В этом упражнении вы настроите **NETWORK SETTINGS**.

e. Нажмите **NETWORK SETTINGS**.

f. Щелкните **DNS** . Введите **example.com** в качестве **Domain Name** и **192.168.101.100** в качестве **IP-адреса**.

g. Нажмите **Save**.

h. Щелкните **NTP** .

i. Введите **192.168.101.100** в качестве **IP-адреса** .

j. Нажмите **Save**.

k. Щелкните **SYSLOG**.

l. Введите **192.168.101.100** в качестве **IP-адреса** .

m. Нажмите **Save**.

n. Нажмите **DNS** , **NTP** и **SYSLOG** еще раз, чтобы проверить правильность информации. Если нет, исправьте каждый раз сохранение информации.

o. Щелкните **PUSH CONFIG**.

p. Откроется диалоговое окно **Push All Network Settings.** Проверьте свои настройки и нажмите **OKAY**. На короткое время появится сообщение «Успешно сохранено».

Шаг 3: Проверьте и протестируйте параметры сети, переданные на устройства.

В нижней части окна **NETWORK SETTINGS** находится следующее:

Примечание. Эта функция поддерживается только на устройствах с ОС IOS-XE и Switch 2960-24TT.

Это означает, что для этой версии Packet Tracer ваши глобальные настройки применялись только к маршрутизаторам.

a. Щелкните любой из трех маршрутизаторов. **R1** показан в следующем выводе.

b. Щелкните **CLI**.

c. Щелкните внутри окна и нажмите **Enter** , чтобы получить командную строку.

d. Войдите в привилегированный режим EXEC и проверьте настройки DNS.

```
R1> enable
R1# show run | begin ip domain
ip domain-name example.com
ip name-server 192.168.101.100
!
<output omitted>
R1#
```

e. Введите следующие команды, чтобы проверить настройки NTP. Время на R1 должно совпадать с вашим текущим временем. Packet Tracer может занять некоторое время для распространения сообщений NTP. Вы можете нажать кнопку **Fast Forward Time** , чтобы ускорить процесс.

```
R1# show ntp associations

address         ref clock       st   when     poll    reach  delay          offset
disp
*~192.168.101.100127.127.1.1     1    12       16      377    0.00           0.00
0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1# show clock
15:30:54.268 UTC Thu Jun 11 2020
R1#
```

f. Введите следующую команду, чтобы убедиться, что ведение журнала настроено.

```
R1# show run | include logging
logging 192.168.101.100
R1#
```

g. Чтобы проверить ведение журнала, выключите интерфейс Serial0/1/0, а затем повторно активируйте его.

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface s0/1/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
15:36:37: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/1/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
15:36:53: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/1/0 from LOADING to
FULL, Loading Done
```

```
R1(config-if)# end
R1#
```

h. Щелкните **Example Server > Services > SYSLOG**. Вы должны увидеть, что те же сообщения системного журнала, которые вы видели в CLI, также регистрируются на сервере. Дважды щелкните любую из записей, чтобы просмотреть сообщения.