Лабораторная работа - Настройка протоколов CDP, LLDP и NTP

# Топология



# Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
| R1 | Loopback1 | 172.16.1.1 | 255.255.255.0 | — |
| R1 | G0/0/1 | 10.22.0.1 | 255.255.255.0 | — |
| S1 | SVI VLAN 1 | 10.22.0.2 | 255.255.255.0 | 10.22.0.1 |
| S2 | SVI VLAN 1 | 10.22.0.3 | 255.255.255.0 | 10.22.0.1 |

# Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Обнаружение сетевых ресурсов с помощью протокола CDP

Часть 3. Обнаружение сетевых ресурсов с помощью протокола LLDP

Часть 4. Настройка и проверка NTP

# Общие сведения/сценарий

Протокол Cisco Discovery Protocol (CDP) — собственный протокол Cisco для обнаружения сетевых ресурсов, функционирующий на канальном уровне. Он служит для обмена информацией, например именами устройств и версиями ПО IOS, с другими физически подключенными устройствами Cisco. Протокол Link Layer Discovery Protocol (LLDP) — это не зависящий от производителя протокол для обнаружения сетевых ресурсов, функционирующий на канальном уровне. В основном он используется сетевыми устройствами в локальной сети (LAN). Сетевые устройства сообщают соседям такие данные о себе, как идентификаторы и сведения о функциональных возможностях.

Протокол сетевого времени (NTP) служит для синхронизации времени между распределенными серверами времени и клиентами. В качестве транспортного протокола NTP использует протокол UDP. Все операции обмена данными по протоколу NTP выполняются по времени в формате UTC.

Сервер NTP обычно получает данные о времени из достоверного источника, такого как атомные часы, к которым подключен сервер. Затем он распределяет это время по сети. Протокол NTP чрезвычайно эффективен; для синхронизации времени на двух компьютерах с временной разницей в пределах миллисекунды требуется отправлять не более одного пакета в минуту.

В этой лабораторной работе вам предстоит задокументировать порты, которые используются для подключения к другим коммутаторам по протоколам CDP и LLDP. Полученные результаты следует указать в диаграмме сетевой топологии.

**Примечание**: Маршрутизаторы, используемые в практических лабораторных работах CCNA, - это Cisco 4221 с Cisco IOS XE Release 16.9.4 (образ universalk9). В лабораторных работах используются коммутаторы Cisco Catalyst 2960 с Cisco IOS версии 15.2(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

**Примечание.** Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены в этом, обратитесь к инструктору.

# Необходимые ресурсы

* 1 Маршрутизатор (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.4 или аналогичным)
* 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.2(2) (образ lanbasek9) или аналогичная модель)
* 1 ПК (под управлением Windows с программой эмуляции терминала, например, Tera Term)
* Консольные кабели для настройки устройств Cisco IOS через консольные порты.
* Кабели Ethernet, расположенные в соответствии с топологией.

## Создание сети и настройка основных параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры для маршрутизатора и коммутаторов.

### Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

### Настройте базовые параметры для маршрутизатора.

Откройте окно конфигурации

* + - 1. Назначьте маршрутизатору имя устройства.
      2. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
      3. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
      4. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
      5. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
      6. Зашифруйте открытые пароли.
      7. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
      8. Настройка интерфейсов, перечисленных в таблице выше
      9. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Закройте окно настройки.

### Настройте базовые параметры каждого коммутатора.

Откройте окно конфигурации

* + - 1. Присвойте коммутатору имя устройства.
      2. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
      3. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
      4. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
      5. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
      6. Зашифруйте открытые пароли.
      7. Создайте баннер, который предупреждает всех, кто обращается к устройству, видит баннерное сообщение «Только авторизованные пользователи!».
      8. Отключите неиспользуемые интерфейсы
      9. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Закройте окно настройки.

## Обнаружение сетевых ресурсов с помощью протокола CDP

На устройствах Cisco протокол CDP включен по умолчанию. Воспользуйтесь CDP, чтобы обнаружить порты, к которым подключены кабели.

Откройте окно конфигурации

* + - 1. На R1 используйте соответствующую команду **show cdp**, чтобы определить, сколько интерфейсов включено CDP, сколько из них включено и сколько отключено.

#### Вопрос:

Сколько интерфейсов участвует в объявлениях CDP? Какие из них активны?

R1#show cdp interface

Vlan1 is administratively down, line protocol is down

Sending CDP packets every 60 seconds

Holdtime is 180 seconds

GigabitEthernet0/0/0 is up, line protocol is down

Sending CDP packets every 60 seconds

Holdtime is 180 seconds

GigabitEthernet0/0/1 is up, line protocol is up

Sending CDP packets every 60 seconds

Holdtime is 180 seconds

GigabitEthernet0/0/2 is up, line protocol is down

Sending CDP packets every 60 seconds

Holdtime is 180 seconds

* + - 1. На R1 используйте соответствующую команду **show cdp**, чтобы определить версию IOS, используемую на S1.

# §

* + - 1. На S1 используйте соответствующую команду **show cdp**, чтобы определить, сколько пакетов CDP было выданных.

S1#show cdp traffic

^

% Invalid input detected at '^' marker.

S1#show cdp ?

entry Information for specific neighbor entry

interface CDP interface status and configuration

neighbors CDP neighbor entries

<cr>

* + - 1. Настройте SVI для VLAN 1 на S1 и S2, используя IP-адреса, указанные в таблице адресации выше. Настройте шлюз по умолчанию для каждого коммутатора на основе таблицы адресов.

Настроено

* + - 1. На R1 выполните команду **show cdp entry S1** .

#### Вопрос:

Какие дополнительные сведения доступны теперь?

R1#show cdp entry S1

Device ID: S1

Entry address(es):

IP address : 10.22.0.2

Platform: cisco 2960, Capabilities: Switch

Interface: GigabitEthernet0/0/1, Port ID (outgoing port): FastEthernet0/5

Holdtime: 134

Version :

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2013 by Cisco Systems, Inc.

Compiled Wed 26-Jun-13 02:49 by mnguyen

advertisement version: 2

Duplex: full

* + - 1. Отключить CDP глобально на всех устройствах.

R1(config)#no cdp run

Закройте окно настройки.

## Обнаружение сетевых ресурсов с помощью протокола LLDP

На устройствах Cisco протокол LLDP может быть включен по умолчанию. Воспользуйтесь LLDP, чтобы обнаружить порты, к которым подключены кабели.

Откройте окно конфигурации

* + - 1. Введите соответствующую команду **lldp**, чтобы включить LLDP на всех устройствах в топологии.

R1(config)#lldp run

* + - 1. На S1 выполните соответствующую команду **lldp**, чтобы предоставить подробную информацию о S2.

# S1#show lldp entry S2

# ^

# % Invalid input detected at '^' marker.

S1#show lldp neighbors detail

------------------------------------------------

Chassis id: 0005.5E21.E601

Port id: Fa0/1

Port Description: FastEthernet0/1

System Name: S2

System Description:

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2013 by Cisco Systems, Inc.

Compiled Wed 26-Jun-13 02:49 by mnguyen

Time remaining: 90 seconds

System Capabilities: B

Enabled Capabilities: B

Management Addresses - not advertised

Auto Negotiation - supported, enabled

Physical media capabilities:

100baseT(FD)

100baseT(HD)

1000baseT(HD)

Media Attachment Unit type: 10

Vlan ID: 1

------------------------------------------------

Chassis id: 0006.2A61.0E02

Port id: Gig0/0/1

Port Description: GigabitEthernet0/0/1

System Name: R1

System Description:

Cisco IOS XE Software, Version 03.13.04.S - Extended Support Release

Cisco IOS Software, ISR Software (X86\_64\_LINUX\_IOSD-UNIVERSALK9-M), Version 15.5(3)S5, RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2017 by Cisco Systems, Inc.

Compiled Mon 05-Oct-15 11:24 by mcpre

Time remaining: 90 seconds

System Capabilities: R

Enabled Capabilities: R

Management Addresses - not advertised

Auto Negotiation - supported, enabled

Physical media capabilities:

1000baseT(HD)

100baseT(FD)

Media Attachment Unit type: 10

Vlan ID: 1

Total entries displayed: 2

#### Вопрос:

Что такое chassis ID для коммутатора S2?

Chassis ID для коммутатора S2 - это уникальный идентификатор, который используется для идентификации данного коммутатора в сети.

Закройте окно настройки.

* + - 1. Соединитесь через консоль на всех устройствах и используйте команды LLDP, необходимые для отображения топологии физической сети только из выходных данных команды show.

# R1#sh lldp neighbors

# Capability codes:

# (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device

# (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

# Device ID Local Intf Hold-time Capability Port ID

# S1 Gig0/0/1 120 B Fa0/5

# Total entries displayed: 1

# S1#sh lldp neighbors

# Capability codes:

# (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device

# (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

# Device ID Local Intf Hold-time Capability Port ID

# S2 Fa0/1 120 B Fa0/1

# R1 Fa0/5 120 R Gig0/0/1

# Total entries displayed: 2

# S2#sh lldp neighbors

# Capability codes:

# (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device

# (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

# Device ID Local Intf Hold-time Capability Port ID

# S1 Fa0/1 120 B Fa0/1

# Total entries displayed: 1

## Настройка NTP

В части 4 необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента NTP маршрутизатора R1. Необходимо выполнить синхронизацию времени для Syslog и отладочных функций. Если время не синхронизировано, сложно определить, какое сетевое событие стало причиной данного сообщения.

### Выведите на экран текущее время.

R1#show clock detail

\*1:5:29.263 UTC Mon Mar 1 1993

Time source is hardware calendar

### Установите время.

С помощью команды clock set установите время на маршрутизаторе R1. Введенное время должно быть в формате UTC.

R1#clock set 23:53:00 5 july 2024

R1#sh clock

23:53:17.886 UTC Fri Jul 5 2024

### Настройте главный сервер NTP.

Настройте R1 в качестве хозяина NTP с уровнем слоя 4.

R1(config)#ntp master 4

### Настройте клиент NTP.

* + - 1. Выполните соответствующую команду на S1 и S2, чтобы просмотреть настроенное время. Запишите текущее время, в следующей таблице.

# S1#show clock detail

# \*1:9:58.418 UTC Mon Mar 1 1993

# Time source is hardware calendar

S2#show clock detail

\*1:9:52.35 UTC Mon Mar 1 1993

Time source is hardware calendar

* + - 1. Настройте S1 и S2 в качестве клиентов NTP. Используйте соответствующие команды NTP для получения времени от интерфейса G0/0/1 R1, а также для периодического обновления календаря или аппаратных часов коммутатора.

S1(config)#ntp server 10.22.0.1

S2(config)#ntp server 10.22.0.1

### Проверьте настройку NTP.

* + - 1. Используйте соответствующую команду **show** , чтобы убедиться, что S1 и S2 синхронизированы с R1.

# S1#show ntp associations

# address ref clock st when poll reach delay offset disp

# ~10.22.0.1 127.127.1.1 4 10 16 37 0.00 989275585724.00 0.12

# \* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

# S1#show ntp status

# Clock is unsynchronized, stratum 16, no reference clock

# nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2\*\*24

# reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1990)

# clock offset is 0.00 msec, root delay is 0.00 msec

# root dispersion is 0.00 msec, peer dispersion is 0.00 msec.

# loopfilter state is 'FSET' (Drift set from file), drift is - 0.000001193 s/s system poll interval is 4, never updated.

* + - 1. Выполните соответствующую команду на S1 и S2, чтобы просмотреть настроенное время и сравнить ранее записанное время.

# S2#show clock

# 0:1:7.89 UTC Sat Jul 6 2024

Откройте окно конфигурации

# Вопрос для повторения

Для каких интерфейсов в пределах сети не следует использовать протоколы обнаружения сетевых ресурсов? Поясните ответ.

Не рекомендуется использовать протоколы обнаружения сетевых ресурсов на интерфейсах, которые подключены к ненадежным или неподконтрольным сегментам сети, так как это может представлять угрозу для безопасности сети.