Lab - Configurar CDP, LLDP y NTP **Realizado por Todos**

Topología



# Tabla de asignación de direcciones

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Puerta de enlace predeterminada |
| R1 | Loopback1 | 172.16.1.1 | 255.255.255.0 | N/D |
| R1 | G0/0/1 | 10.22.0.1 | 255.255.255.0 | N/D |
| 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 |

# Objetivos

Parte 1: Armar la red y configurar los ajustes básicos de los dispositivos

Parte 2: Detectar la red con el protocolo CDP

Parte 3: Detectar la red con el protocolo LLDP

Parte 4: Configure y verificar NTP

# Aspectos básicos/situación

Cisco Discovery Protocol (CDP) es un protocolo exclusivo de Cisco para la detección de redes en la capa de enlace de datos. Puede compartir información como nombres de dispositivos y versiones de IOS con otros dispositivos Cisco conectados físicamente. El Protocolo de detección de capa de enlace (LLDP) es un protocolo neutral que utiliza la capa de enlace de datos para la detección de red. Se utiliza principalmente con los dispositivos de red en la red de área local (LAN). Los dispositivos de red anuncian información, como las identidades y funcionalidades a sus vecinos.

El protocolo de tiempo de red (NTP) sincroniza la hora del día entre un conjunto de servidores de hora y clientes distribuidos. NTP usa el protocolo de datagrama de datos (UDP) como protocolo de transporte. Por defecto, las comunicaciones NTP utilizan el Tiempo Universal Coordinado (UTC).

Un servidor NTP generalmente recibe su hora de una fuente horaria autorizada, como un reloj atómico conectado a un servidor horario. Luego distribuye este tiempo a través de la red. NTP es extremadamente eficiente; no es necesario más de un paquete por minuto para sincronizar dos máquinas con una diferencia inferior al milisegundo entre sí.

En esta práctica de laboratorio, debe documentar los puertos conectados a otros switches mediante los protocolos CDP y LLDP. Usted documentará sus conclusiones en un diagrama de topología de la red.

**Nota**: Los routers utilizados con los laboratorios prácticos de CCNA son Cisco 4221 con Cisco IOS XE versión 16.9.4 (universalk9 image). Los switches utilizados en los laboratorios son Cisco Catalyst 2960s con Cisco IOS Release 15.2 (2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

**Nota**: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

# Recursos necesarios

* 1 router (Cisco 4221 con imagen universal Cisco IOS XE versión 16.9.4 o comparable)
* 2 switches (Cisco 2960 con Cisco IOS versión 15.0(2), lanbasek9 image o comparable)
* 1 PC (Windows 7 u 8 con un programa de emulación de terminal, como Tera Term)
* Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
* Cables Ethernet, como se muestra en la topología

## Armar la red y configurar los ajustes básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos del router y el switch.

### Realizar el cableado de red tal como se muestra en la topología

Conecte los dispositivos como se muestra en la topología y realizar el cableado necesario.

### Configure los parámetros básicos para el router.

Abra la ventana de configuración

* + - 1. Asigne un nombre de dispositivo al router.
      2. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.
      3. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
      4. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.
      5. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.
      6. Encripte las contraseñas de texto sin formato.
      7. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
      8. Configure interfaces como se indica en la tabla anterior
      9. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Cierre la ventana de configuración

### Configure los parámetros básicos para cada switch

Abra la ventana de configuración

* + - 1. Asigne un nombre de dispositivo al switch.
      2. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.
      3. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
      4. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.
      5. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.
      6. Encripte las contraseñas de texto sin formato.
      7. Cree un banner que avise a cualquier persona que acceda al dispositivo que vea el mensaje de banner «¡Sólo usuarios autorizados!».
      8. Apague todas las interfaces no utilizadas.
      9. Guarde la configuración en ejecución en el archivo de configuración de inicio

Cierre la ventana de configuración

## Detecte la red con el protocolo CDP

Para los dispositivos Cisco, el CDP está habilitado de manera predeterminada. Utilizará CDP para detectar los puertos conectados actualmente.

Abra la ventana de configuración

* + - 1. En R1, use el comando **show cdp** apropiado para determinar cuántas interfaces están habilitadas CDP, y cuántas están activadas y cuántas están inactivas.

R1# **show cdp interface | include interfaces**

#### unta:

¿Cuántas interfaces participan en el anuncio de CDP? ¿Qué interfaces están activas?

-5 interfaces participan

-Esta activa la G0/0

* + - 1. En R1, utilice el comando **show cdp** apropiado para determinar la versión IOS utilizada en S1.

R1# **show cdp entry S1**

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

Device ID: S1

Entry address(es):

Platform: cisco WS-C2960+24LC-L, Capabilities: Switch IGMP

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

Holdtime : 125 sec

Version :

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.2(4)E8, RELEASE SOFTWARE (fc3)

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

Copyright (c) 1986-2019 by Cisco Systems, Inc.

Compilado vie 15-mar-19 17:28 por prod\_rel\_team

advertisement version: 2

VTP Management Domain: ''

Native VLAN: 1

Duplex: full

#### Pregunta:

¿Qué versión de IOS está usando S1?

Version 12.2(55)

Escriba sus respuestas aquí.

* + - 1. En S1, utilice el comando **show cdp** apropiado para determinar cuántos paquetes CDP se han emitido.

S1# **show cdp traffic**

CDP counters :

Total packets output: 179, Input: 148

Hdr syntax: 0, Chksum error: 0, Encaps failed: 0

No memory: 0, Invalid packet: 0,

CDP version 1 advertisements output: 0, Input: 0

CDP version 2 advertisements output: 179, Input: 148

#### Pregunta:

¿Cuántos paquetes tiene salida CDP desde que se restableció el último contador?

Tiene de salida 486 paquetes

Escriba su

s respuestas aquí.

* + - 1. Configure el SVI para la VLAN 1 en S1 y S2 utilizando las direcciones IP especificadas en la Tabla de direccionamiento anterior. Configure la puerta de enlace predeterminada en cada switch según la tabla de direcciones.
      2. En R1, ejecute el comando **show cdp entry S1** .

#### Pregunta:

¿Qué información adicional está disponible ahora?

Aparece la Vlan 1

Escriba sus respuestas aquí.

R1# **show cdp entry S1**

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

Device ID: S1

Entry address(es):

Ip address: 10.22.0.2

Platform: cisco WS-C2960+24LC-L, Capabilities: Switch IGMP

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

Holdtime : 133 sec

Version :

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.2(4)E8, RELEASE SOFTWARE (fc3)

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

Copyright (c) 1986-2019 by Cisco Systems, Inc.

Compilado vie 15-mar-19 17:28 por prod\_rel\_team

advertisement version: 2

VTP Management Domain: ''

Native VLAN: 1

Duplex: full

Management address(es):

Ip address: 10.22.0.2

* + - 1. Deshabilite CDP globalmente en todos los dispositivos

R1(config)# **no cdp run**

S1(config)# **no cdp run**

S2(config)# **no cdp run**

Cierre la ventana de configuración

## Detecte la red con el protocolo LLDP

En dispositivos de Cisco, LLDP puede estar activado de manera predeterminada. Utilizará LLDP para detectar los puertos conectados actualmente.

Abra la ventana de configuración

* + - 1. Introduzca el comando **lldp** adecuado para habilitar LLDP en todos los dispositivos de la topología

R1(config)# lldp run

S1(config)# lldp run

S2(config)# lldp run

* + - 1. En S1, ejecute el comando **lldp** apropiado para proporcionarle información detallada sobre S2.

S1# **show lldp entry S2**

Capability codes:

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

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

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

Local Intf: Fa0/1

ID del chasis: c025.5cd7.ef00

Port id: Fa0/1

Port Description: FastEthernet0/1

System Name: S2

Descripción del sistema:

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.2(4)E8, RELEASE SOFTWARE (fc3)

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

Copyright (c) 1986-2019 by Cisco Systems, Inc.

Compilado vie 15-mar-19 17:28 por prod\_rel\_team

Time remaining: 109 seconds

System Capabilities: B

Enabled Capabilities: B

Management Addresses:

IP: 10.22.0.3

Auto Negotiation - supported, enabled

Physical media capabilities:

100base-TX(FD)

100base-TX(HD)

10base-T(FD)

10base-T(HD)

Media Attachment Unit type: 16

Vlan ID: 1

Total entries displayed: 1

#### Pregunta:

¿Cuál es el ID del chasis del switch S2?

La ID es 0C27.2461.C500

Escriba sus respuestas aquí.

Cierre la ventana de configuración

* + - 1. ¿Qué comando LLDP debe utilizar para poder dibujar la topología de red física?

Show lldp neighbours

## Configure NTP

En la Parte 4, configurará R1 como el servidor NTP y S1 y S2 como clientes NTP de R1. La sincronización del tiempo es importante para las funciones de syslog y de depuración. Si no se sincroniza el tiempo, es difícil determinar qué evento de red causó el mensaje.

### Muestra la hora actual

Abra la ventana de configuración

Emitir el **comando** show clock detail para mostrar la hora actual en R1. En la siguiente tabla, registre la información relacionada con la hora actual que se muestra.

| Fecha | Tiempo | Zona horaria | Time Source (Fuente horaria) |
| --- | --- | --- | --- |
| 21/04/2022 | 14:32:29.423 | UTC | Hardware Calendar |

### Establezca la hora

Use el comando apropiado (clock set) configure la hora en R1. La hora introducida debe estar en UTC.

### Configure el NTP master.

Configure R1 como NTP master con un nivel de estrato de 4.

R1(config)# **ntp master 4**

### Configure el cliente NTP

* + - 1. Ejecute el comando apropiado en S1 y S2 para ver la hora configurada. Registre la hora actual que se muestra en la siguiente tabla.

| Fecha | Tiempo | Zona horaria |
| --- | --- | --- |
| 01/03/1993 | 03:46:08.203 | UTC |
| 01/03/1993 | 03:49:05.438 | UTC |

* + - 1. Configure S1 y S2 como clientes NTP. Utilice los comandos NTP apropiados para obtener tiempo de la interfaz G0/0/1 de R1, así como para actualizar periódicamente el calendario o el reloj de hardware en el switch.

S1 (config) # **ntp server 10.22.0.1**

S1(config)# **ntp update-calendar**

S2 (config) # **ntp server 10.22.0.1**

S2(config)# **ntp update-calendar**

### Verifique la configuración NTP

* + - 1. Utilice el comando “**show ntp status | include Clock”** para verificar que S1 y S2 estén sincronizados con R1.

**Nota**: Pueden pasar unos minutos antes de que los switches se sincronicen con R1.

Abra la ventana de configuración

# Pregunta de reflexión

Dentro de una red, ¿en qué las interfaces no debe utilizar los protocolos de detección? Explique.

En las de acceso y en las que vayan al exterior, ya que se expondría información sensible sobre la estructura de la red.

Escriba sus respuestas aquí.

# Tabla de resumen de interfaces de router

| Modelo de router | Interfaz Ethernet 1 | Interfaz Ethernet #2 | Interfaz serial 1 | Interfaz serial #2 |
| --- | --- | --- | --- | --- |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 4221 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 4300 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |

Nota: Para conocer la configuración del router, observe las interfaces para identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, aunque puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo de esto. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS para representar la interfaz.

Fin del documento