Práctica de laboratorio: configuración de los parámetros básicos del router con la CLI del IOS (versión para el instructor - práctica de laboratorio opcional)

**Nota para el instructor:** El color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente. Las actividades opcionales están elaboradas para mejorar la compresión o proporcionar práctica adicional.

1. Topología



1. Tabla de direccionamiento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| El administrador | Interfaces | Dirección IP | Máscara de subred | Gateway predeterminado |
| R1 | G0/0 | 192.168.0.1 | 255.255.255.0 | N/D |
|  | G0/1 | 192.168.1.1 | 255.255.255.0 | N/D |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | 192.168.0.3 | 255.255.255.0 | 192.168.0.1 |

1. Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

* Realizar el cableado de los equipos para que coincidan con la topología de la red.
* Inicializar y reiniciar el router y el switch.

Parte 2: configurar los dispositivos y verificar la conectividad

* Asignar información de IPv4 estática a las interfaces de la computadora.
* Configurar los parámetros básicos del router.
* Verificar la conectividad de la red
* Configurar el router para el acceso por SSH.

Parte 3: Mostrar la información del router

* Recuperar información del hardware y del software del router.
* Interpretar el resultado de la configuración de inicio.
* Interpretar el resultado de la tabla de routing.
* Verificar el estado de las interfaces.

Parte 4: configurar IPv6 y verificar la conectividad

1. Aspectos básicos/situación

Esta es una práctica de laboratorio integral para revisar comandos de router de IOS que se abarcaron anteriormente. En las partes 1 y 2, realizará el cableado de los equipos y completará las configuraciones básicas y las configuraciones de las interfaces IPv4 en el router.

En la parte 3, utilizará SSH para conectarse de manera remota al router y usará comandos de IOS para recuperar la información del dispositivo para responder preguntas sobre el router. En la parte 4, configurará IPv6 en el router de modo que la PC-B pueda adquirir una dirección IP y luego verificará la conectividad.

Para fines de revisión, esta práctica de laboratorio proporciona los comandos necesarios para las configuraciones de router específicas.

**Nota:** Los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960 con IOS de Cisco, versión 15.0(2) (imagen de 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 esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

**Nota:** asegúrese de que el router y el switch se hayan borrado y no tengan configuraciones de inicio. Consulte el apéndice A para conocer los procedimientos para inicializar y volver a cargar los dispositivos.

1. Recursos necesarios

* 1 router (Cisco 1941 con Cisco IOS versión 15.2(4)M3, imagen universal o similar)
* 1 switch (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
* 2 PC (Windows 7, Vista o XP 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

**Nota**: Las interfaces Gigabit Ethernet en los ISR Cisco 1941 poseen detección automática y se puede usar un cable Ethernet directo entre el router y PC-B. Si usa otro modelo de router Cisco, es posible que deba usar un cable Ethernet cruzado.

1. Establecer la topología e inicializar los dispositivos
   1. Realice el cableado de red como se muestra en la topología.
      1. Conecte los dispositivos como se muestra en la topología y realice el cableado necesario.
      2. Encienda todos los dispositivos de la topología.
   2. Inicializar y volver a cargar el router y el switch.

**Nota:** en el apéndice A, se detallan los pasos para inicializar y volver a cargar los dispositivos.

1. Configurar los dispositivos y verificar la conectividad
   1. Configurar las interfaces de la PC.
      1. Configure la dirección IP, la máscara de subred y los parámetros del gateway predeterminado en la PC-A.
      2. Configure la dirección IP, la máscara de subred y los parámetros del gateway predeterminado en la PC-B.
   2. Configurar el router.
      1. Acceda al router mediante el puerto de consola y habilite el modo EXEC privilegiado.

Router> **enable**

Router#

* + 1. Ingrese al modo de configuración global.

Router# **config terminal**

Router(config)#

* + 1. Asigne un nombre de dispositivo al router.

Router(config)# **hostname R1**

* + 1. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos introducidos de manera incorrecta como si fueran nombres de host.

R1(config)# **no ip domain-lookup**

* + 1. Establezca el requisito de que todas las contraseñas tengan como mínimo 10 caracteres.

R1(config)# **security passwords min-length 10**

Además de configurar una longitud mínima, enumere otras formas de aportar seguridad a las contraseñas.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Use letras mayúsculas, números y caracteres especiales en las contraseñas.

* + 1. Asigne **cisco12345** como la contraseña cifrada del modo EXEC privilegiado.

R1(config)# **enable secret cisco12345**

* + 1. Asigne **ciscoconpass** como la contraseña de consola, establezca un tiempo de espera, habilite el inicio de sesión y agregue el comando **logging synchronous**. El comando **logging synchronous** sincroniza la depuración y el resultado del software IOS de Cisco, y evita que estos mensajes interrumpan la entrada del teclado.

R1(config)# **line con 0**

R1(config-line)# **password ciscoconpass**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **login**

R1(config-line)# **logging synchronous**

R1(config-line)# **exit**

R1(config)#

Para el comando **exec-timeout**, ¿qué representan el **5** y el **0**?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

La sesión expirará en 5 minutos y 0 segundos.

* + 1. Asigne **ciscovtypass** como la contraseña de vty, establezca un tiempo de espera, habilite el inicio de sesión y agregue el comando **logging synchronous**.

R1(config)# **line vty 0 4**

R1(config-line)# **password ciscovtypass**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **login**

R1(config-line)# **logging synchronous**

R1(config-line)# **exit**

R1(config)#

* + 1. Cifre las contraseñas de texto no cifrado.

R1(config)# **service password-encryption**

* + 1. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

R1(config)# **banner motd #Prohibido el acceso no autorizado#**

* + 1. Configure una dirección IP y una descripción de interfaz. Active las dos interfaces en el router.

R1(config)# **int g0/0**

R1(config-if)# **description Conexión con PC-B**

R1(config-if)# **ip address 192.168.0.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **int g0/1**

R1(config-if)# **description Conexión con S1**

R1(config-if)# **ip address 192.168.1.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **exit**

R1#

* + 1. Configure el reloj en el router, por ejemplo:

R1# **clock set 17:00:00 18 Feb 2013**

* + 1. Guarde la configuración en ejecución en el archivo de configuración de inicio.

R1# **copy running-config startup-config**

Destination filename [startup-config]?

Building configuration...

[OK]

R1#

¿Qué resultado obtendría al volver a cargar el router antes de completar el comando **copy running-config startup-config**?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Se borraría el contenido de la configuración en ejecución. En esta práctica de laboratorio, el router no tendría una configuración de inicio. Después de un reinicio, se le preguntaría al usuario si desea ingresar al diálogo de configuración inicial.

* 1. Verificar la conectividad de la red
     1. Haga ping a la PC-B en un símbolo del sistema en la PC-A.

**Nota:** quizá sea necesario deshabilitar el firewall de las computadoras.

¿Fueron correctos los pings? \_\_\_\_ Sí

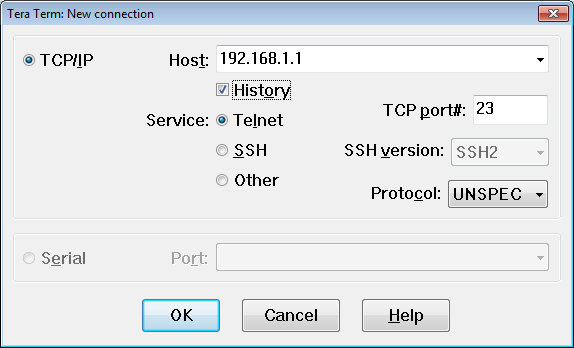
Después de completar esta serie de comandos, ¿qué tipo de acceso remoto podría usarse para acceder al R1?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telnet

* + 1. Acceda de forma remota al R1 desde la PC-A mediante el cliente de Telnet de Tera Term.

Abra Tera Term e ingrese la dirección IP de la interfaz G0/1 de R1 en el campo Host: de la ventana Tera Term: New Connection (Tera Term: Conexión nueva). Asegúrese de que el botón de opción **Telnet** esté seleccionado y después haga clic en **OK** (Aceptar) para conectarse al router.



¿Pudo conectarse remotamente? \_\_\_\_ Sí

¿Por qué el protocolo Telnet es considerado un riesgo de seguridad?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

La sesión de Telnet se puede ver en texto no cifrado. No está cifrada. Las contraseñas pueden verse fácilmente mediante un programa detector de paquetes.

* 1. configurar el router para el acceso por SSH.
     1. Habilite las conexiones SSH y cree un usuario en la base de datos local del router.

R1# **configure terminal**

R1(config)# **ip domain-name CCNA-lab.com**

R1(config)# **username admin privilege 15 secret adminpass1**

R1(config)# **line vty 0 4**

R1(config-line)# **transport input ssh**

R1(config-line)# **login local**

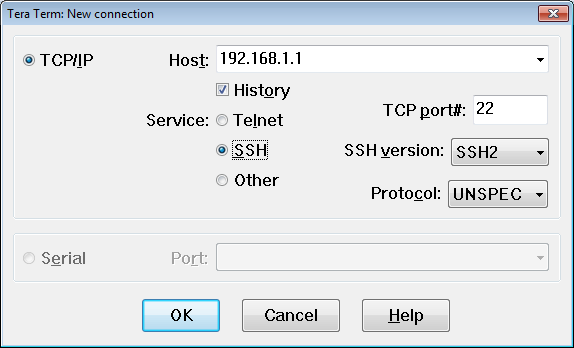
R1(config-line)# **exit**

R1(config)# **crypto key generate rsa modulus 1024**

R1(config)# **exit**

* + 1. Acceda remotamente al R1 desde la PC-A con el cliente SSH de Tera Term.

Abra Tera Term e ingrese la dirección IP de la interfaz G0/1 de R1 en el campo Host: de la ventana Tera Term: New Connection (Tera Term: Conexión nueva). Asegúrese de que el botón de opción **SSH** esté seleccionado y haga clic en **OK** para conectarse al router.



¿Pudo conectarse remotamente? \_\_\_\_ Sí

1. Mostrar la información del router

En la parte 3, utilizará comandos **show** en una sesión SSH para recuperar información del router.

* 1. Establezca una sesión de SSH con R1.

Mediante Tera Term en la PC-B, abra una sesión SSH para el R1 en la dirección IP 192.168.0.1 e inicie sesión como **admin** y use la contraseña **adminpass1**.

* 1. recuperar información importante del hardware y el software.
     1. Use el comando **show version** para responder preguntas sobre el router.

R1# show version

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M3, RELEASE SOFTWARE (fc1)

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

Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Thu 26-Jul-12 19:34 by prod\_rel\_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

El tiempo de funcionamiento de R1 es de 10 minutos.

System returned to ROM by power-on

El archivo de imagen del sistema es "flash0:c1900-universalk9-mz.SPA.152-4.M3.bin"

El tipo de la última recarga: Reinicio normal

Motivo de la última recarga: inicio

This product contains cryptographic features and is subject to United

States and local country laws governing import, export, transfer and

use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for

compliance with U.S. and local country laws. By using this product you

agree to comply with applicable laws and regulations. If you are unable

to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to

export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 446464K/77824K bytes of memory.

Processor board ID FTX0947Z18E

2 interfaces Gigabit Ethernet

2 Serial(sync/async) interfaces

1 líneas de terminales

DRAM configuration is 64 bits wide with parity disabled.

255K bytes de memoria de configuración no volátil

250880K bytes de ATA CompactFlash (Lectura/Escritura)

Información sobre la licencia:

Licencia UDI:

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

SN de Device# PID

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

\*0 CISCO1941/K9 FTX1636848Z

Información sobre la licencia de paquete de tecnología para el Módulo: ‘c1900’

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

Technology-package technology-package de tecnología

Actual Tipo Próximo reinicio

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

ipbasek9 ipbase ipbasek9 permanente

seguridad ninguno ninguno ninguno

datos cualquiera cualquiera cualquiera

Configuration register is 0x2142 (will be 0x2101 at next reload).

¿Cuál es el nombre de la imagen de IOS que el router está ejecutando?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

La versión de la imagen puede variar, pero las respuestas deberían ser algo así como c1900-universalk9-mz.SPA.152-4.M3.bin.

¿Cuánta memoria de acceso aleatorio no volátil (NVRAM) tiene el router?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las respuestas pueden variar, pero el resultado del comando **show version** en el router 1941 es: 255K bytes of non-volatile configuration memory.

¿Cuánta memoria flash tiene el router?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las respuestas pueden variar, pero el resultado predeterminado del comando **show version** en el router 1941 es: 250880K bytes of ATA System CompactFlash 0 (Read/Write).

* + 1. Con frecuencia, los comandos **show** proporcionan varias pantallas de resultados. Filtrar el resultado permite que un usuario visualice determinadas secciones del resultado. Para habilitar el comando de filtrado, introduzca una barra vertical (**|**) después de un comando **show**, seguido de un parámetro de filtrado y una expresión de filtrado. Para que el resultado coincida con la instrucción de filtrado, puede usar la palabra clave **include** para ver todas las líneas del resultado que contienen la expresión de filtrado. Filtre el comando **show version** mediante **show version | include register** para responder la siguiente pregunta.

R1# show version - include register

El registro de configuración es 0x2142

¿Cuál es el proceso de arranque para el router en la siguiente recarga?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las respuestas pueden variar. En la mayoría de los casos (0x2102), el router experimenta un arranque normal, carga el IOS desde la memoria flash y carga la configuración de inicio desde la NVRAM, en caso de existir. Si el registro de configuración es 0x2142, el router omite la configuración de inicio y comienza en el símbolo del sistema del modo usuario. Si el arranque inicial falla, el router ingresa al modo ROMMON.

* 1. mostrar la configuración de inicio.

Use el comando **show startup-config** en el router para responder las siguientes preguntas.

R1# show version

Using 1674 out of 262136 bytes

!

versión 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

!

security passwords min-length 10

enable secret 4 3mxoP2KRPf3sFHYl6Vm6.ssJJi9tOJqqb6DMG/YH5No

!

no aaa new-model

!

no ipv6 cef

ip source-route

!

no ip domain lookup

ip domain name CCNA-lab.com

ip cef

multilink bundle-name authenticated

!

!

!

license udi pid CISCO2911/K9 sn FTX1636848Z

!

!

username admin privilege 15 secret 7 1304131f020214B383779

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

description Connection to PC-B

ip address 192.168.0.1 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/1

description Connection to S1

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 200 0000

!

interface Serial0/0/1

no ip address

shutdown

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

control-plane

!

!

banner motd ^CUnauthorized access prohibited!^C

!

línea con 0

exec-timeout 5 0

password 7 060506324F410A160B0713181F

logging synchronous

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

exec-timeout 5 0

password 7 060506324F411F0D1C0713181F

logging synchronous

login local

transport input ssh

!

scheduler allocate 20000 1000

end

¿De qué forma figuran las contraseñas en el resultado?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las contraseñas están cifradas debido al comando service password-encryption. Las contraseña line con de ciscoconpass está cifrada como 060506324F410A160B0713181F. La contraseña de line vty de ciscovtypass está cifrada como 060506324F411F0D1C0713181F.

Use el comando **show startup-config | begin vty**.

line vty 0 4

exec-timeout 5 0

password 7 060506324F411F0D1C0713181F

login local

transport input ssh

!

scheduler allocate 20000 1000

end

¿Qué resultado se obtiene al usar este comando?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Un usuario recibe el resultado de la configuración de inicio que empieza con la línea que incluye la primera instancia de la expresión de filtrado.

* 1. Mostrar la tabla de routing en el router.

Utilice el comando **show ip route** en el router para responder las preguntas siguientes:

R1# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is not set

192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.0.0/24 is directly connected, GigabitEthernet0/0

L 192.168.0.1/32 is directly connected, GigabitEthernet0/0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0/1

L 192.168.1.1/32 is directly connected, GigabitEthernet0/1

¿Qué código se utiliza en la tabla de routing para indicar una red conectada directamente?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

La C designa una subred conectada directamente. Una L designa una interfaz local. Las dos respuestas son correctas.

¿Cuántas entradas de ruta están codificadas con un código C en la tabla de routing? \_\_\_\_\_ 2

* 1. mostrar una lista de resumen de las interfaces del router.

Use el comando **show ip interface brief** en el router para responder la siguiente pregunta.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 192.168.0.1 YES manual up up

GigabitEthernet0/1 192.168.1.1 YES manual up up

Serial0/0/0 unassigned YES unset administratively down down

Serial0/0/1 unassigned YES unset administratively down down

R1#

¿Qué comando cambió el estado de los puertos Gigabit Ethernet de administrativamente inactivo a activo?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**no shutdown**

1. configurar IPv6 y verificar la conectividad
   1. asignar direcciones IPv6 a la G0/0 del R1 y habilitar el routing IPv6.

**Nota:** la asignación de una dirección IPv6, además de una dirección IPv4, en una interfaz se conoce como “dual stacking”, debido a que las pilas de protocolos IPv4 e IPv6 están activas. Al habilitar el routing de unidifusión IPv6 en el R1, la PC-B recibe el prefijo de red IPv6 de G0/0 del R1 y puede configurar automáticamente la dirección IPv6 y el gateway predeterminado.

* + 1. Asigne una dirección de unidifusión global IPv6 a la interfaz G0/0; asigne la dirección link-local en la interfaz, además de la dirección de unidifusión; y habilite el routing IPv6.

R1# **configure terminal**

R1(config)# **interface g0/0**

R1(config-if)# **ipv6 address 2001:db8:acad:a::1/64**

R1(config-if)# **ipv6 address fe80::1 link-local**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **ipv6 unicast-routing**

R1(config)# **exit**

* + 1. Use el comando **show ipv6 int brief** para verificar la configuración de IPv6 en el R1.

R1#**show ipv6 int brief**

Em0/0 [administratively down/down]

no asignado

GigabitEthernet0/0 [up/up]

FE80::1

2001:DB8:ACAD:A::1

GigabitEthernet0/1 [up/up]

no asignado

Serial0/0/0 [administratively down/down]

no asignado

Serial0/0/1 [administratively down/down]

No asignado

Si no se asignó una dirección IPv6 a la G0/1, ¿por qué se indica como [up/up]?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

El estado [up/up] refleja el estado de la capa 1 y la capa 2 de la interfaz y no depende de la capa 3.

* + 1. Emita el comando **ipconfig** en la PC-B para examinar la configuración de IPv6.

¿Cuál es la dirección IPv6 asignada a la PC-B?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las respuestas varían. Dirección IPv6 de 2001:db8:acad:a:d428:7de2:997c:b05a

¿Cuál es el gateway predeterminado asignado a la PC-B? \_\_\_\_\_\_\_\_\_\_\_\_ fe80::1

En la PC-B, haga ping a la dirección link-local del gateway predeterminado del R1. ¿Tuvo éxito? \_\_\_\_\_\_\_\_ Sí

En la PC-B, haga ping a la dirección IPv6 de unidifusión del R1 2001:db8:acad:a::1. ¿Tuvo éxito? \_\_\_\_\_\_\_\_ Sí

1. Reflexión
   1. Durante la investigación de un problema de conectividad de red, un técnico sospecha que no se habilitó una interfaz. ¿Qué comando **show** podría usar el técnico para resolver este problema?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las respuestas pueden variar. Sin embargo, los comandos **show ip interface brief** o **show startup-config** proporcionarían la información.

* 1. Durante la investigación de un problema de conectividad de red, un técnico sospecha que se asignó una máscara de subred incorrecta a una interfaz. ¿Qué comando **show** podría usar el técnico para resolver este problema?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**show startup-config** or **show running-config**

* 1. Después de configurar IPv6 en la LAN de la PC-B en la interfaz G0/0 del R1, si hiciera ping de la PC-A a la dirección IPv6 de la PC-B, ¿el ping sería correcto? ¿Por qué o por qué no?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

El ping fallaría, porque la interfaz G0/1 del R1 no se configuró con IPv6 y la PC-A solo tiene una dirección IPv4.

1. Tabla de resumen de interfaces de router

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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) |
| **Nota**: Para conocer la configuración del router, observe las interfaces a fin de 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, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS para representar la interfaz. | | | | |

1. Apéndice A: inicialización y recarga de un router y un switch
   1. Inicie y vuelva a cargar el router.
      1. Acceda al router mediante el puerto de consola y habilite el modo EXEC privilegiado.

Router> **enable**

Router#

* + 1. Escriba el comando **erase startup-config** para eliminar el archivo de configuración de inicio de la NVRAM.

Router# **erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Router#

* + 1. Emita el comando **reload** para eliminar una configuración antigua de la memoria. Cuando reciba el mensaje **Proceed with reload** (Continuar con la recarga), presione Enter para confirmar. (Si presiona cualquier otra tecla, se cancela la recarga).

Router# **reload**

Proceed with reload? [confirm]

\*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

**Nota:** es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el router. Escriba **no** y presione Intro.

System configuration has been modified. Save? [yes/no]: **no**

* + 1. Una vez que se vuelve a cargar el router, se le solicita introducir el diálogo de configuración inicial. Escriba **no** y presione Enter.

Would you like to enter the initial configuration dialog? [yes/no]: **no**

* + 1. Se le solicita finalizar la instalación automática. Escriba **yes** (sí) y, luego, presione Enter.

Would you like to terminate autoinstall? [yes]: **yes**

* 1. inicializar y volver a cargar el switch.
     1. Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.

Switch> **enable**

Switch#

* + 1. Utilice el comando **show flash** para determinar si se crearon VLAN en el switch.

Switch# **show flash**

Directory of flash:/

2 -rwx 1919 Mar 1 1993 00:06:33 +00:00 private-config.text

3 -rwx 1632 Mar 1 1993 0:06:33 +00:00 config.text

4 -rwx 13336 Mar 1 1993 0:06:33 +00:00 multiple-fs

5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin

6 -rwx 616 Mar 1 1993 00:07:13 +00:00 vlan.dat

32514048 bytes totales (20886528 bytes libres)

Switch#

* + 1. Si se encontró el archivo **vlan.dat** en la memoria flash, elimínelo.

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

* + 1. Se le solicitará que verifique el nombre de archivo. En este momento, puede cambiar el nombre de archivo o, simplemente, presionar Enter si introdujo el nombre de manera correcta.
    2. Se le solicitará que confirme que desea eliminar este archivo. Presione Enter para confirmar la eliminación. (Si se presiona cualquier otra tecla, se anula la eliminación).

Delete flash:/vlan.dat? [confirm]

Switch#

* + 1. Utilice el comando **erase startup-config** para eliminar el archivo de configuración de inicio de la NVRAM. Se le solicitará que confirme la eliminación del archivo de configuración. Presione Enter para confirmar que desea borrar este archivo. (Al pulsar cualquier otra tecla, se cancela la operación).

Switch# **erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Switch#

* + 1. Vuelva a cargar el switch para eliminar toda información de configuración antigua de la memoria. Se le solicitará que confirme la recarga del switch. Presione Enter para seguir con la recarga. (Si presiona cualquier otra tecla, se cancela la recarga).

Switch# **reload**

Proceed with reload? [confirm]

**Nota:** es posible que reciba un mensaje para guardar la configuración en ejecución antes de volver a cargar el switch. Escriba **no** y presione Intro.

System configuration has been modified. Save? [yes/no]: **no**

* + 1. Una vez que se vuelve a cargar el switch, se le solicita introducir el diálogo de configuración inicial. Escriba **no** y presione Intro.

Would you like to enter the initial configuration dialog? [yes/no]: **no**

Switch>

1. Configuraciones de dispositivos
2. Router R1

R1#show run

Building configuration...

Current configuration : 1742 bytes

!

versión 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

!

security passwords min-length 10

enable secret 4 3mxoP2KRPf3sFHYl6Vm6.ssJJi9tOJqqb6DMG/YH5No

!

no aaa new-model

!

!

!

!

!

!

!

no ip domain lookup

ip domain name CCNA-lab.com

ip cef

ipv6 unicast-routing

ipv6 cef

multilink bundle-name authenticated

!

!

!

license udi pid CISCO1941/K9 sn FTX1636848Z

license accept end user agreement

!

!

username admin privilege 15 password 7 1304131F0202142B383779

!

!

!

!

!

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

description Connection to PC-B

ip address 192.168.0.1 255.255.255.0

duplex auto

speed auto

ipv6 address FE80::1 link-local

ipv6 address 2001:DB8:ACAD:A::1/64

!

interface GigabitEthernet0/1

description Connection to S1

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

!

interface Serial0/0/1

no ip address

shutdown

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

!

!

!

!

control-plane

!

!

banner motd ^CUnauthorized access prohibited!^C

!

línea con 0

exec-timeout 5 0

password 7 03075218050022434019181604

logging synchronous

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

exec-timeout 5 0

password 7 14141B180F0B3C3F3D38322631

logging synchronous

login local

transport input ssh

!

scheduler allocate 20000 1000

!

end