Práctica de laboratorio: Uso de la CLI para recopilar información sobre dispositivos de red (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 | IP Address (Dirección IP) | Subnet Mask (Máscara de subred) | Gateway predeterminado |
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | N/D |
| Lo0 | 209.165.200.225 | 255.255.255.224 | N/D |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 | 192.168.1.1 |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |

1. Objetivos

Parte 1: Establecer la topología e inicializar los dispositivos

Parte 2: configurar los dispositivos y verificar la conectividad

Parte 3: Recopilar información sobre los dispositivos de red

1. Aspectos básicos/situación

La documentación de una red en funcionamiento es una de las tareas más importantes que puede realizar un profesional de red. Tener la documentación correspondiente de las direcciones IP, los números de modelo, las versiones del IOS y los puertos utilizados, así como probar la seguridad, puede resultar muy útil para resolver los problemas de una red.

En esta práctica de laboratorio, armará una red pequeña, configurará los dispositivos, implementará seguridad básica y documentará las configuraciones mediante la emisión de diversos comandos en el router, el switch y la PC para recopilar la información.

**Nota**: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s 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 que se encuentra al final de esta 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.

**Nota para el instructor**: Consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

1. Recursos necesarios

* 1 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
* 1 switch (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 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

1. establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red, borrará cualquier configuración, de ser necesario, y configurará los parámetros básicos del router y el switch.

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

1. Configurar dispositivos y verificar la conectividad

En la parte 2, establecerá la topología de la red y configurará los parámetros básicos del router y el switch. Consulte la topología y la tabla de direccionamiento que se encuentran al principio de esta práctica de laboratorio para obtener información sobre nombres de dispositivos y direcciones.

* 1. Configurar la dirección IPv4 para la PC

Configure la dirección IPv4, la máscara de subred y la dirección de gateway predeterminado para la PC-A según la tabla de direccionamiento.

* 1. Configurar el router.
     1. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.
     2. Configure la hora correcta en el router.
     3. Ingrese al modo de configuración global.
        1. Asigne un nombre de dispositivo al router según la topología y la tabla de direccionamiento.
        2. Desactive la búsqueda del DNS.
        3. Cree un mensaje MOTD que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
        4. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
        5. Asigne **cisco** como la contraseña de consola y habilite el acceso de inicio de sesión a la consola.
        6. Cifre las contraseñas de texto no cifrado.
        7. Cree un nombre de dominio **cisco.com** para el acceso por SSH.
        8. Cree un usuario denominado **admin** con la contraseña secreta **cisco** para el acceso por SSH.
        9. Genere una clave de módulo RSA. Use **1024** para la cantidad de bits.
     4. Configure el acceso a las líneas VTY.
        1. Use la base de datos local para la autenticación de SSH.
        2. Habilite SSH solo para el acceso de inicio de sesión.
     5. Vuelva al modo de configuración global.
        1. Cree la interfaz Loopback 0 y asigne la dirección IP según la tabla de direccionamiento.
        2. Configure y habilite la interfaz G0/1 en el router.
        3. Configure las descripciones de interfaz para G0/1 y L0.
        4. Guarde el archivo de configuración en ejecución en el archivo de configuración de inicio.
  2. Configure el switch.
     1. Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.
     2. Configure la hora correcta en el switch.
     3. Ingrese al modo de configuración global.
        1. Asigne un nombre de dispositivo al switch según la topología y la tabla de direccionamiento.
        2. Desactive la búsqueda del DNS.
        3. Cree un mensaje MOTD que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
        4. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
        5. Cifre las contraseñas de texto no cifrado.
        6. Cree un nombre de dominio **cisco.com** para el acceso por SSH.
        7. Cree un usuario denominado **admin** con la contraseña secreta **cisco** para el acceso por SSH.
        8. Genere una clave RSA. Use **1024** para la cantidad de bits.
        9. Cree y active una dirección IP en el switch según la topología y la tabla de direccionamiento.
        10. Configure el gateway predeterminado en el switch.
        11. Asigne **cisco** como la contraseña de consola y habilite el acceso de inicio de sesión a la consola.
     4. Configure el acceso a las líneas VTY.
        1. Use la base de datos local para la autenticación de SSH.
        2. Habilite SSH solo para el acceso de inicio de sesión.
        3. Guarde el archivo de configuración en ejecución en el archivo de configuración de inicio.
     5. Ingrese al modo correspondiente para configurar las descripciones de interfaz de F0/5 y F0/6.
  3. Verificar la conectividad de la red
     1. Desde el símbolo del sistema en la PC-A, haga ping a la dirección IP de la VLAN 1 del S1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.
     2. En el símbolo del sistema de la PC-A, haga ping a la dirección IP del gateway predeterminado en el R1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.
     3. En el símbolo del sistema de la PC-A, haga ping a la interfaz loopback en R1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.
     4. Vuelva a acceder al switch mediante la consola y haga ping a la dirección IP de G0/1 en el R1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.

1. Recopilar información sobre los dispositivos de red

En la parte 3, utilizará una variedad de comandos para recopilar información sobre los dispositivos en la red, así como algunas características de rendimiento. La documentación de la red es un componente muy importante de la administración de una red. La documentación de la topología física y lógica es importante, al igual que la verificación de los modelos de plataforma y las versiones del IOS de los dispositivos de red. Tener conocimientos de los comandos adecuados para recopilar esta información es fundamental para los profesionales de red.

* 1. Recopilar información sobre el R1 mediante los comandos del IOS.

Uno de los pasos más básicos consiste en recopilar información sobre el dispositivo físico, así como la información del sistema operativo.

* + 1. Emita el comando adecuado para obtener la siguiente información:

**Nota para el instructor**: las respuestas para todo el paso 1 varían según el modelo de router y el IOS. Tenga en cuenta que la respuesta para el paquete de tecnología se aplica solo a los routers que ejecutan el IOS 15.0 y posterior.

Modelo de router: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Router Cisco 1941

Versión del IOS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

15.2(4)M3

RAM total: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

512MB

NVRAM total: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

255K

Memoria flash total: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

250880 KB

Archivo de imagen de IOS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

c1900-universalk9-mz.SPA.152-4.M3.bin

Registro de configuración: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

0x2102

Paquete de tecnología: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ipbasek9

¿Qué comando emitió para recopilar la información?

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

Se puede usar el comando **show version** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

* + 1. Emita el comando adecuado para mostrar un resumen de la información importante sobre las interfaces del router. Escriba el comando y registre sus resultados a continuación.

**Nota**: registre solo las interfaces que tengan direcciones IP.

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

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

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

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

Se puede usar el comando **show ip interface brief** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/1 192.168.1.1 YES NVRAM up up

Loopback0 209.165.200.225 YES NVRAM up up

<some output omitted>

* + 1. Emita el comando adecuado para mostrar la tabla de enrutamiento. Escriba el comando y registre sus resultados a continuación.

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

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

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

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

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

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

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

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

Se puede usar el comando **show ip route** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

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

209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.200.224/27 is directly connected, Loopback0

L 209.165.200.225/32 is directly connected, Loopback0

* + 1. ¿Qué comando usaría para mostrar la asignación de direcciones de capa 2 y capa 3 en el router? Escriba el comando y registre sus resultados a continuación.

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

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

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

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

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

Se puede usar el comando **show arp** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.168.1.1 - 30f7.0da3.1821 ARPA GigabitEthernet0/1

Internet 192.168.1.3 0 c80a.a9fa.de0d ARPA GigabitEthernet0/1

Internet 192.168.1.11 2 0cd9.96d2.34c0 ARPA GigabitEthernet0/1

* + 1. ¿Qué comando usaría para ver información detallada sobre todas las interfaces en el router o sobre una interfaz específica? Escriba el comando a continuación.

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

Se puede usar el comando **show interfaces** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

* + 1. Cisco tiene un protocolo muy eficaz que funciona en la capa 2 del modelo OSI. Este protocolo puede ayudarlo a delinear la forma en que se conectan físicamente los dispositivos Cisco, así como a determinar los números de modelo e incluso el direccionamiento IP y las versiones del IOS. ¿Qué comandos usaría en el router R1 para obtener información sobre el switch S1 que le ayude a completar la siguiente tabla?

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Identificador del dispositivo | Interfaz local | Capacidad | N.º de modelo | ID del puerto remoto | IP Address (Dirección IP) | Versión del IOS |
| S1.cisco.com | G 0/1 | Switch | WS-2960-24TT-L | F 0/5 | 192.168.1.11 | 15.0(2)SE1 |

Se puede usar el comando show **cdp neighbors detail** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

* + 1. Una prueba muy simple de los dispositivos de red consiste en ver si se puede acceder a estos mediante Telnet. No obstante, tenga en cuenta que Telnet no es un protocolo seguro. No se debe habilitar en la mayoría de los casos. Con un cliente Telnet, como Tera Term o PuTTY, intente acceder al R1 mediante Telnet con la dirección IP del gateway predeterminado. Registre sus resultados a continuación.

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

Tera Term Output: Connection refused.

* + 1. En la PC-A, realice pruebas para asegurar que SSH funcione correctamente. Con un cliente SSH, como Tera Term o PuTTY, acceda al R1 mediante SSH desde la PC-A. Si aparece un mensaje de advertencia en relación con una clave diferente, haga clic en **Continue** (Continuar). Inicie sesión con el nombre de usuario y la contraseña correspondientes que creó en la parte 2. ¿Tuvo éxito?

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

Sí.

Las distintas contraseñas configuradas en el router deben ser tan seguras y protegidas como sea posible.

**Nota**: las contraseñas utilizadas para la práctica de laboratorio (**cisco** y **class**) no cumplen con las prácticas recomendadas para las contraseñas seguras. Estas contraseñas se usan simplemente por cuestiones de practicidad para realizar las prácticas de laboratorio. De manera predeterminada, la contraseña de consola y todas las contraseñas de vty configuradas se muestran como texto no cifrado en el archivo de configuración.

* + 1. Verifique que todas las contraseñas en el archivo de configuración estén cifradas. Escriba el comando y registre sus resultados a continuación.

Comando: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Se puede usar el comando **show running-config** o **show run** en la petición de entrada de EXEC privilegiado.

¿Está cifrada la contraseña de consola? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sí

¿Está cifrada la contraseña de SSH? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sí

* 1. Recopilar información sobre el S1 mediante los comandos del IOS.

Muchos de los comandos que usó en R1 se pueden utilizar con el switch. Sin embargo, existen algunas diferencias con algunos de los comandos.

**Nota para el instructor**: las respuestas para todo el paso 2 varían según el modelo de switch, los puertos utilizados y las direcciones MAC.

* + 1. Emita el comando adecuado para obtener la siguiente información:

Modelo de switch: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ WS-C2960-24TT-L

Versión del IOS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 15.0(2)SE1

NVRAM total: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 64K

Archivo de imagen de IOS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ c2960-lanbasek9-mz.150-2.SE1.bin

¿Qué comando emitió para recopilar la información?

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

Se puede usar el comando **show version** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

* + 1. Emita el comando adecuado para mostrar un resumen de la información de estado sobre las interfaces del switch. Escriba el comando y registre sus resultados a continuación.

**Nota**: registre solo las interfaces activas.

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

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

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

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

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

Se puede usar el comando **show ip interface brief** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

Interface IP-Address OK? Method Status Protocol

Vlan1 192.168.1.11 YES NVRAM up up

FastEthernet0/5 unassigned YES unset up up

FastEthernet0/6 unassigned YES unset up up

<some output omitted>

* + 1. Emita el comando adecuado para mostrar la tabla de direcciones MAC del switch. Registre solo las direcciones MAC dinámicas en el siguiente espacio.

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

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

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

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

Se puede usar el comando **show mac address-table** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

Mac Address Table

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

Vlan Mac Address Type Ports

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

1 30f7.0da3.1821 DYNAMIC Fa0/5

1 c80a.a9fa.de0d DYNAMIC Fa0/6

* + 1. Verifique que el acceso a VTY por Telnet esté deshabilitado en el S1. Con un cliente Telnet, como Tera Term o PuTTY, intente acceder al S1 mediante Telnet con la dirección 192.168.1.11. Registre sus resultados a continuación.

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

Tera Term Output: Connection refused.

* + 1. En la PC-A, realice pruebas para asegurar que SSH funcione correctamente. Con un cliente SSH, como Tera Term o PuTTY, acceda al S1 mediante SSH desde la PC-A. Si aparece un mensaje de advertencia en relación con una clave diferente, haga clic en **Continue** (Continuar). Inicie sesión con un nombre de usuario y una contraseña adecuados. ¿Tuvo éxito?

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

Sí.

* + 1. Complete la siguiente tabla con información sobre el router R1 utilizando los comandos adecuados en el S1.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Id. del dispositivo | Interfaz local | Capacidad | N.º de modelo | ID del puerto remoto | IP Address (Dirección IP) | Versión del IOS |
| R1.cisco.com | F 0/5 | Router | CISCO1941/K9 | G 0/1 | 192.168.1.1 | 15.2(4)M3 |

Se puede usar el comando show **cdp neighbors detail** en la petición de entrada de EXEC del usuario o de EXEC privilegiado.

* + 1. Verifique que todas las contraseñas en el archivo de configuración estén cifradas. Escriba el comando y registre sus resultados a continuación.

Comando: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Se puede usar el comando **show running-config** o **show run** en la petición de entrada de EXEC privilegiado.

¿Está cifrada la contraseña de consola? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sí

* 1. Recopilar información sobre la PC-A.

Mediante diversos comandos de utilidades de Windows, recopilará información sobre la PC-A.

* + 1. En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all** y registre sus respuestas a continuación.

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller

Physical Address. . . . . . . . . : C8-0A-A9-FA-DE-0D

DHCP Enabled. . . . . . . . . . . : No

Autoconfiguration Enabled . . . . : Yes

IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.1.1

<resultado omitido>

¿Cuál es la dirección IP de la PC-A?

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

192.168.1.3

¿Cuál es la máscara de subred de la PC-A?

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

255.255.255.0

¿Cuál es la dirección de gateway predeterminado de la PC-A?

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

192.168.1.1

¿Cuál es la dirección MAC de la PC-A?

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

Las respuestas varían.

* + 1. Emita el comando adecuado para probar el stack de protocolos TCP/IP con la NIC. ¿Qué comando utilizó?

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

C:\> **ping 127.0.0.1**

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

* + 1. Haga ping a la interfaz loopback del R1 desde el símbolo del sistema de la PC-A. ¿El ping se realizó correctamente?

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

Sí.

* + 1. Emita el comando adecuado en la PC-A para rastrear la lista de saltos de router para los paquetes provenientes de la PC-A a la interfaz loopback en R1. Registre el comando y el resultado a continuación. ¿Qué comando utilizó?

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

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

C:\> **tracert 209.165.200.225**

Tracing route to 209.165.200.225 over a maximum of 30 hops

1 1 ms 1 ms 1 ms 209.165.200.225

Trace complete.

* + 1. Emita el comando adecuado en la PC-A para buscar las asignaciones de direcciones de capa 2 y capa 3 que se realizaron en la NIC. Registre sus respuestas a continuación. Registre solo las respuestas para la red 192.168.1.0/24. ¿Qué comando utilizó?

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

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

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

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

C:\> **arp –a**

Interface: 192.168.1.3 --- 0xb

Internet Address Physical Address Type

192.168.1.1 30-f7-0d-a3-18-21 dynamic

192.168.1.11 0c-d9-96-d2-34-c0 dynamic

192.168.1.255 ff-ff-ff-ff-ff-ff static

1. Reflexión

¿Por qué es importante registrar los dispositivos de red?

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

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

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

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

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

Tener la información adecuada, incluidas las direcciones IP, las conexiones de puertos físicos, las versiones del IOS, las copias de los archivos de configuración y la cantidad de almacenamiento de memoria, puede ayudarlo en gran medida al realizar la resolución de problemas y las pruebas de línea de base de red. Tener una buena documentación también le permite recuperarse de las interrupciones de la red y reemplazar equipos cuando sea necesario.

1. Tabla de resumen de interfaces de router

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resumen de la interfaz del 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 Cisco para representar la interfaz. | | | | |

1. Configuraciones de dispositivos
2. Router R1

R1#sh run

Building configuration...

Current configuration : 1545 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

no ip domain lookup

ip domain name cisco.com

ip cef

no ipv6 cef

multilink bundle-name authenticated

!

!

username admin secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

!

!

ip ssh version 1

!

interface Loopback0

description Emulate ISP Connection

ip address 209.165.200.225 255.255.255.224

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

description Connected to LAN

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

clock rate 2000000

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

!

control-plane

!

!

banner motd ^CWarning! Unauthorized access is prohibited.^C

!

line con 0

password 7 060506324F41

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

login local

transport input ssh

!

scheduler allocate 20000 1000

!

End

1. Switch S1

S1#sh run

Building configuration...

Current configuration : 1752 bytes

!

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

username admin secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

no aaa new-model

system mtu routing 1500

!

!

no ip domain-lookup

ip domain-name cisco.com

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

ip ssh version 1

!

interface FastEthernet0/1

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

description Connected to R1

!

interface FastEthernet0/6

description Connected to PC-A

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

ip address 192.168.1.11 255.255.255.0

!

ip default-gateway 192.168.1.1

ip http server

ip http secure-server

!

banner motd ^CWarning! Unauthorized access is prohibited.^C

!

line con 0

password 7 00071A150754

login

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

!

end