Lab–Using the CLI to Gather Network Device Information (Answer)

1. Topology



1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
|  | Lo0 | 209.165.200.225 | 255.255.255.224 | N/A |
| 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. Objectives

Part 1: Set Up Topology and Initialize Devices

* Set up equipment to match the network topology.
* Initialize and reload the router and switch.

Part 2: Configure Devices and Verify Connectivity

* Assign a static IP address to PC-A NIC.
* Configure basic settings on R1.
* Configure basic settings on S1.
* Verify network connectivity.

Part 3: Gather Network Device Information

* Gather information on R1 using IOS CLI commands.
* Gather information on S1 using IOS CLI commands.
* Gather information on PC-A using the command prompt CLI.

1. Background / Scenario

Documenting a working network is one of the most important tasks a network professional can perform. Having proper documentation of IP addresses, model numbers, IOS versions, ports used, and testing security, can go a long way in helping to troubleshoot a network.

In this lab, you will build a small network, configure the devices, add some basic security, and then document the configurations by issuing various commands on the router, switch and PC to gather your information.

**Note**: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

**Note**: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

1. Required Resources

* 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
* 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
* 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
* Console cables to configure the Cisco IOS devices via the console ports
* Ethernet cables as shown in the topology

1. Set Up the Topology and Initialize Devices

In Part 1, you will set up the network topology, clear any configurations if necessary, and configure basic settings on the router and switch.

* 1. Cable the network as shown in the topology.
     1. Attach the devices as shown in the topology and cable as necessary.
     2. Power on all devices in the topology.
  2. Initialize and reload the router and the switch.

1. Configure Devices and Verify Connectivity

In Part 2, you will set up the network topology and configure basic settings on the router and switch. Refer to the topology and Addressing Table at the beginning of this lab for device names and address information.

**Note**: Appendix A provides configuration details for the steps in Part 2. You should attempt to complete Part 2 prior to referencing this appendix.

* 1. Configure the IPv4 address for the PC.

Configure the IPv4 address, subnet mask, and default gateway address for PC-A based on the Addressing Table.

* 1. Configure the router.

If you need assistance for Step 2, refer to Appendix A for help.

* + 1. Console into the router and enter privileged EXEC mode.
    2. Set the correct time on the router.
    3. Enter global configuration mode.
       1. Assign a device name to the router based on the topology and Addressing Table.
       2. Disable DNS lookup.
       3. Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited.
       4. Assign **class** as the privileged EXEC encrypted password.
       5. Assign **cisco** as the console password and enable console login access.
       6. Encrypt clear text passwords.
       7. Create a domain name of **cisco.com** for SSH access.
       8. Create a user named **admin** with a secret password of **cisco** for SSH access.
       9. Generate a RSA modulus key. Use **1024** for the number of bits.
    4. Configure vty line access.
       1. Use the local database for authentication for SSH.
       2. Enable SSH only for login access.
    5. Return to global configuration mode.
       1. Create the Loopback 0 interface and assign the IP address based on the Addressing Table.
       2. Configure and activate interface G0/1 on the router.
       3. Configure interface descriptions for G0/1 and L0.
       4. Save the running configuration file to the startup configuration file.
  1. Configure the switch.

If you need assistance for Step 3, refer to Appendix A for help.

* + 1. Console into the switch and enter privileged EXEC mode.
    2. Set the correct time on the switch.
    3. Enter global configuration mode.
       1. Assign a device name on the switch based on the topology and Addressing Table.
       2. Disable DNS lookup.
       3. Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited.
       4. Assign **class** as the privileged EXEC encrypted password.
       5. Encrypt the clear text passwords.
       6. Create a domain name of **cisco.com** for SSH access.
       7. Create a user named **admin** with a secret password of **cisco** for SSH access.
       8. Generate an RSA modulus key. Use **1024** for the number of bits.
       9. Create and activate an IP address on the switch based on the topology and Addressing Table.
       10. Set the default gateway on the switch.
       11. Assign **cisco** as the console password and enable console login access.
    4. Configure vty line access.
       1. Use local database for authentication for SSH.
       2. Enable SSH only for login access.
       3. Enter proper mode to configure interface descriptions for F0/5 and F0/6.
       4. Save the running configuration file to the startup configuration file.
  1. Verify network connectivity.
     1. From a command prompt on PC-A, ping the S1 VLAN 1 IP address. Troubleshoot your physical and logical configurations if the pings were not successful.
     2. From the PC-A command prompt, ping your default gateway IP address on R1. Troubleshoot your physical and logical configurations if the pings were not successful.
     3. From the PC-A command prompt, ping the loopback interface on R1. Troubleshoot your physical and logical configurations if the pings were not successful.
     4. Console back into the switch and ping the G0/1 IP address on R1. Troubleshoot your physical and logical configurations if the pings were not successful.

1. Gather Network Device Information

In Part 3, you will use a variety of commands to gather information about the devices on your network, as well as some performance characteristics. Network documentation is a very important component of managing your network. Documentation of both physical and logical topologies is important, as is verifying platform models and IOS versions of your network devices. Having knowledge of the proper commands to gather this information is essential for a network professional.

* 1. Gather information on R1 using IOS commands.

One of the most basic steps is to gather information on the physical device, as well as information on the operating system.

* + 1. Issue the appropriate command to discover the following information:

**Note**: Your answers for all of step 1 will vary based on router model and IOS. Note that the answer for Technology Package only applies to routers running IOS 15.0 and greater.

Router Model: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Cisco 1941 Router

IOS Version: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

15.2(4)M3

Total RAM: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

512MB

Total NVRAM: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

255K bytes

Total Flash Memory: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

250880K bytes

IOS Image File: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Configuration Register: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

0x2102

Technology Package: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ipbasek9

What command did you issue to gather the information?

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

The **show version** command can be used from either the user EXEC or privileged EXEC prompt.

* + 1. Issue the appropriate command to display a summary of important information about the router interfaces. Write down the command and record your results below.

**Note**: Only record interfaces that have IP addresses.

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

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

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

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

The **show ip interface brief** command can be used from either the user EXEC or privileged EXEC prompt.

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. Issue the appropriate command to display the routing table. Write down the command and record your results below.

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

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

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

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

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

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

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

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

The **show ip route** command can be used from either the user EXEC or privileged EXEC prompt.

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. What command would you use to display the Layer 2 to Layer 3 mapping of addresses on the router? Write down the command and record your results below.

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

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

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

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

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

The **show arp** command can be used from either the user EXEC or privileged EXEC prompt.

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. What command would you use to see detailed information about all the interfaces on the router or about a specific interface? Write down the command below.

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

The **show interfaces** command can be used from either the user EXEC or privileged EXEC prompt.

* + 1. Cisco has a very powerful protocol that operates at Layer 2 of the OSI model. This protocol can help you map out how Cisco devices are connected physically, as well as determining model numbers and even IOS versions and IP addressing. What command or commands would you use on router R1 to find out information about switch S1 to help you complete the table below?

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Device ID | Local Interface | Capability | Model # | Remote Port ID | IP Address | IOS Version |
| S1.cisco.com | G 0/1 | Switch | WS-2960-24TT-L | F 0/5 | 192.168.1.11 | 15.0(2)SE1 |

The **show cdp neighbors detail** command can be used from either the user EXEC or privileged EXEC prompt.

* + 1. A very elementary test of your network devices is to see if you can telnet into them. Remember, Telnet is not a secure protocol. It should not be enabled in most cases. Using a Telnet client, such as Tera Term or PuTTY, try to telnet to R1 using the default gateway IP address. Record your results below.

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

Tera Term Output: Connection refused.

* + 1. From PC-A, test to ensure that SSH is working properly. Using an SSH client, such as Tera Term or PuTTY, SSH into R1 from PC-A. If you get a warning message regarding a different key, click **Continue**. Log in with the appropriate username and password you created in Part 2. Were you successful?

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

Yes.

The various passwords configured on your router should be as strong and protected as possible.

**Note**: The passwords used for our lab (**cisco** and **class**) do not follow the best practices needed for strong passwords. These passwords are used merely for the convenience of performing the labs. By default, the console password and any vty passwords configured would display in clear text in your configuration file.

* + 1. Verify that all of your passwords in the configuration file are encrypted. Write down the command and record your results below.

Command: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The **show running-config** or **show run** command can be used from the privileged EXEC prompt.

Is the console password encrypted? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Yes

Is the SSH password encrypted? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Yes

* 1. Gather information on S1 using IOS commands.

Many of the commands that you used on R1 can also be used with the switch. However, there are some differences with some of the commands.

**Note**: Answers for all of Step 2 will vary based on Switch model, ports used, and MAC addresses.

* + 1. Issue the appropriate command to discover the following information:

Switch Model: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ WS-C2960-24TT-L

IOS Version: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 15.0(2)SE1

Total NVRAM: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 64K

IOS Image File: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ c2960-lanbasek9-mz.150-2.SE1.bin

What command did you issue to gather the information?

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

The **show version** command can be used from either the user EXEC or privileged EXEC prompt.

* + 1. Issue the appropriate command to display a summary of key information about the switch interfaces. Write down the command and record your results below.

**Note**: Only record active interfaces.

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

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

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

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

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

The **show ip interface brief** command can be used from either the user EXEC or privileged EXEC prompt.

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. Issue the appropriate command to display the switch MAC address table. Record the dynamic type MAC addresses only in the space below.

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

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

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

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

The **show mac address-table** command can be used from either the user EXEC or privileged EXEC prompt.

Mac Address Table

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

Vlan Mac Address Type Ports

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

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

1 c80a.a9fa.de0d DYNAMIC Fa0/6

* + 1. Verify that Telnet VTY access is disabled on S1. Using a Telnet client, such as Tera Term or PuTTY, try to telnet to S1 using the 192.168.1.11 address. Record your results below.

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

Tera Term Output: Connection refused.

* + 1. From PC-A, test to ensure that SSH is working properly. Using an SSH client, such as Tera Term or PuTTY, SSH into S1 from PC-A. If you get a warning message regarding a different key, click **Continue**. Log in with an appropriate username and password. Were you successful?

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

Yes.

* + 1. Complete the table below with information about router R1 using the appropriate command or commands necessary on S1.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Device Id | Local Interface | Capability | Model # | Remote Port ID | IP Address | IOS Version |
| R1.cisco.com | F 0/5 | Router | CISCO1941/K9 | G 0/1 | 192.168.1.1 | 15.2(4)M3 |

The **show cdp neighbors detail** command can be used from either the user EXEC or privileged EXEC prompt.

* + 1. Verify that all of your passwords in the configuration file are encrypted. Write down the command and record your results below.

Command: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The **show running-config** or **show run** command can be used from the privileged EXEC prompt.

Is the console password encrypted? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Yes

* 1. Gather information on PC-A.

Using various Windows utility commands, you will gather information on PC-A.

* + 1. From the PC-A command prompt, issue the **ipconfig /all** command and record your answers below.

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

<output omitted>

What is the PC-A IP address?

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

192.168.1.3

What is the PC-A subnet mask?

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

255.255.255.0

What is the PC-A default gateway address?

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

192.168.1.1

What is the PC-A MAC address?

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

Answers will vary.

* + 1. Issue the appropriate command to test the TCP/IP protocol stack with the NIC. What command did you use?

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

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. Ping the loopback interface of R1 from the PC-A command prompt. Was the ping successful?

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

Yes.

* + 1. Issue the appropriate command on PC-A to trace the list of router hops for packets originating from PC-A to the loopback interface on R1. Record the command and output below. What command did you use?

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

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

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. Issue the appropriate command on PC-A to find the Layer 2 to Layer 3 address mappings held on your NIC. Record your answers below. Only record answers for the 192.168.1.0/24 network. What command did you use?

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

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

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

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

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. Reflection

Why is it important to document your network devices?

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

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

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

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

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

Having the proper information including: IP addresses, physical port connections, IOS versions, copies of configuration files, and the amount of memory storage, can greatly aid you when troubleshooting and performing network baseline tests. Having good documentation can also help you recover from network outages and replacing equipment when necessary.

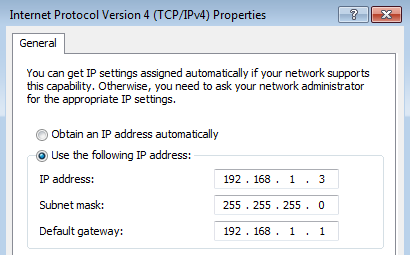
1. Router Interface Summary Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Router Interface Summary | | | | |
| Router Model | Ethernet Interface #1 | Ethernet Interface #2 | Serial Interface #1 | Serial Interface #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) |
| **Note**: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface. | | | | |

1. Appendix A: Configuration Details for Steps in Part 2

Step 1: Configure the IPv4 address for the PC.

Configure the IPv4 address, subnet mask, and default gateway address for PC-A based on the Addressing Table at the beginning of this lab.



Step 2: Configure the router.

* + 1. Console into the router and enter privileged EXEC mode.

Router> **enable**

Router#

* + 1. Set the correct time on the router.

Router# **clock set 10:40:30 6 February 2013**

Router#

* + 1. Enter global configuration mode.

Router# **config t**

Router(config)#

* + - 1. Assign a hostname to the router. Use the topology and Addressing Table as guidelines.

Router(config)# **hostname R1**

R1(config)#

* + - 1. Disable DNS lookup.

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

* + - 1. Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited.

R1(config)# **banner motd #Warning! Unauthorized Access is prohibited.#**

* + - 1. Assign **class** as the privileged EXEC encrypted password.

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

* + - 1. Assign **cisco** as the console password and enable console login access.

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

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

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

* + - 1. Encrypt clear text passwords.

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

* + - 1. Create a domain name of **cisco.com** for SSH access.

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

* + - 1. Create a user named **admin** with a secret password of **cisco** for SSH access.

R1(config)# **username admin secret cisco**

* + - 1. Generate an RSA modulus key. Use **1024** for the number of bits.

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

* + 1. Configure vty line access.
       1. Use the local database for authentication for SSH.

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

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

* + - 1. Enable SSH only for login access.

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

* + 1. Return to global configuration mode.

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

* + - 1. Create the Loopback 0 interface and assign the IP address based on the Address Table.

R1(config)# **interface loopback 0**

R1(config-if)# **ip address 209.165.200.225 255.255.255.224**

* + - 1. Configure and activate interface G0/1 on the router.

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

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

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

* + - 1. Configure interface descriptions for G0/1 and L0.

R1(config-if)# **description Connected to LAN**

R1(config-if)# **int lo0**

R1(config-if)# **description Emulate ISP Connection**

* + - 1. Save the running configuration file to the startup configuration file.

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

R1# **copy run start**

Step 3: Configure the switch.

* + 1. Console into the switch and enter privileged EXEC mode.

Switch> **enable**

Switch#

* + 1. Set the correct time on the switch.

Switch# **clock set 10:52:30 6 February 2013**

* + 1. Enter global configuration mode.

Switch# **config t**

* + - 1. Assign a hostname on the switch based on the topology and Addressing Table.

Switch(config)# **hostname S1**

* + - 1. Disable DNS lookup.

S1(config)# **no ip domain-lookup**

* + - 1. Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited.

S1(config)# **banner motd #Warning! Unauthorized access is prohibited.#**

* + - 1. Assign **class** as the privileged EXEC encrypted password.

S1(config)# **enable secret class**

* + - 1. Encrypt the clear text passwords.

S1(config)# **service password-encryption**

* + - 1. Create a domain name of **cisco.com** for SSH access.

S1(config)# **ip domain-name cisco.com**

* + - 1. Create a user named **admin** with a secret password of **cisco** for SSH access.

S1(config)# **username admin secret cisco**

* + - 1. Generate an RSA modulus key. Use **1024** for the number of bits.

S1(config)# **crypto key generate rsa modulus 1024**

* + - 1. Create and activate an IP address on the switch based on the topology and Addressing Table.

S1(config)# **interface vlan 1**

S1(config-if)# **ip address 192.168.1.11 255.255.255.0**

S1(config-if)# **no shut**

* + - 1. Set the default gateway on the switch.

S1(config)# **ip default-gateway 192.168.1.1**

* + - 1. Assign **cisco** as the console password and enable console login access.

S1(config-if)# **line con 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

* + 1. Configure vty line access.
       1. Use local database for authentication for SSH.

S1(config-line)# **line vty 0 15**

S1(config-line)# **login local**

* + - 1. Enable SSH only for login access.

S1(config-line)# **transport input ssh**

* + - 1. Enter the appropriate configuration mode to configure interface descriptions for F0/5 and F0/6.

S1(config-line)# **int f0/5**

S1(config-if)# **description Connected to R1**

S1(config-if)# **int f0/6**

S1(config-if)# **description Connected to PC-A**

* + - 1. Save the running configuration file to the startup configuration file.

S1(config-if)# **end**

S1# **copy run start**

1. Device Configs
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