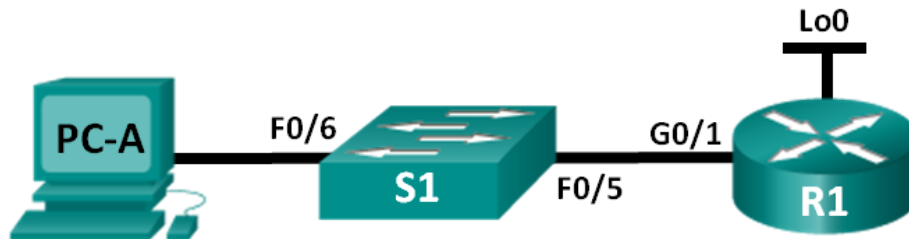


Lab – Using the CLI to Gather Network Device Information

Topology



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

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.

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.

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

Part 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.

Step 1: Cable the network as shown in the topology.

- a. Attach the devices as shown in the topology and cable as necessary.
- b. Power on all devices in the topology.

Step 2: Initialize and reload the router and the switch.

Part 2: 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.

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.

Step 2: Configure the router.

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

- a. Console into the router and enter privileged EXEC mode.
- b. Set the correct time on the router.
- c. Enter global configuration mode.
 - 1) Assign a device name to the router based on the topology and Addressing Table.
 - 2) Disable DNS lookup.

Lab – Using the CLI to Gather Network Device Information

- 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 **512** for the number of bits.
- d. Configure vty line access.
- 1) Use the local database for authentication for SSH.
 - 2) Enable SSH only for login access.
- e. 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.

Step 3: Configure the switch.

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

- a. Console into the switch and enter privileged EXEC mode.
- b. Set the correct time on the switch.
- c. 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 **512** 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.
- d. 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.

Step 4: Verify network connectivity.

- a. 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.
- b. 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.
- c. From the PC-A command prompt, ping the loopback interface on R1. Troubleshoot your physical and logical configurations if the pings were not successful.
- d. 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.

Part 3: 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.

Step 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.

- a. Issue the appropriate command to discover the following information:

Router Model:

IOS Version:

Total RAM:

Total NVRAM:

Total Flash Memory:

IOS Image File:

Configuration Register:

Technology Package:

What command did you issue to gather the information?

- b. 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.

Lab – Using the CLI to Gather Network Device Information

- c. Issue the appropriate command to display the routing table. Write down the command and record your results below.
- d. 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.
- e. 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.
- f. 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

Command:

- g. 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.
- h. 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?

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.

Lab – Using the CLI to Gather Network Device Information

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

Command:

Is the console password encrypted?

Is the SSH password encrypted?

Step 2: 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.

- a. Issue the appropriate command to discover the following information:

Switch Model:

IOS Version:

Total NVRAM:

IOS Image File:

What command did you issue to gather the information?

- b. 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.

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

- d. 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.

- e. 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?

Lab – Using the CLI to Gather Network Device Information

- f. 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

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

Command:

Is the console password encrypted?

Step 3: Gather information on PC-A.

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

- a. From the PC-A command prompt, issue the **ipconfig /all** command and record your answers below.
- What is the PC-A IP address?
- What is the PC-A subnet mask?
- What is the PC-A default gateway address?
- What is the PC-A MAC address?
- b. Issue the appropriate command to test the TCP/IP protocol stack with the NIC. What command did you use?
- c. Ping the loopback interface of R1 from the PC-A command prompt. Was the ping successful?
- d. 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?
- e. 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?

Reflection

Why is it important to document your network devices?

Router Interface Summary Table

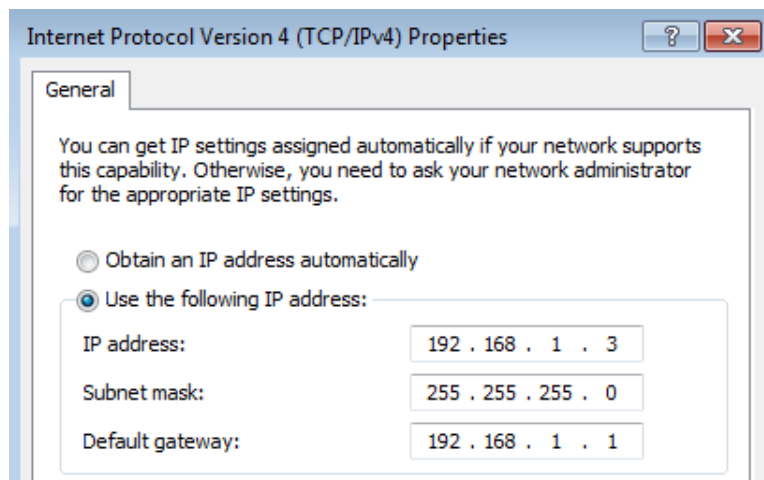
Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	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.

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.

- a. Console into the router and enter privileged EXEC mode.

```
Router> enable
```


Router#

- b. Set the correct time on the router.

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

Router#

- c. 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)#

- 2) Disable DNS lookup.

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

- 3) Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited.

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

- 4) Assign **class** as the privileged EXEC encrypted password.

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

- 5) 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
```

- 6) Encrypt clear text passwords.

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

- 7) Create a domain name of **cisco.com** for SSH access.

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

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

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

- 9) Generate an RSA modulus key. Use **512** for the number of bits.

```
R1(config)# crypto key generate rsa modulus 512
```

- d. Configure vty line access.

- 1) Use the local database for authentication for SSH.

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

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

- 2) Enable SSH only for login access.

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

- e. 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
```

- 2) 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
```

- 3) 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
```

- 4) Save the running configuration file to the startup configuration file.

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

```
R1# copy run start
```

Step 3: Configure the switch.

- a. Console into the switch and enter privileged EXEC mode.

```
Switch> enable
```

```
Switch#
```

- b. Set the correct time on the switch.

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

- c. 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
```

- 2) Disable DNS lookup.

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

- 3) Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited.

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

- 4) Assign **class** as the privileged EXEC encrypted password.

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

- 5) Encrypt the clear text passwords.

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

- 6) Create a domain name of **cisco.com** for SSH access.

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

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

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

- 8) Generate an RSA modulus key. Use **512** for the number of bits.

```
S1(config)# crypto key generate rsa modulus 512
```

- 9) Create and activate an IP address on the switch based on the topology and Addressing Table.

Lab – Using the CLI to Gather Network Device Information

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# no shut
```

10) Set the default gateway on the switch.

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

11) 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
```

d. Configure vty line access.

1) Use local database for authentication for SSH.

```
S1(config-line)# line vty 0 15
S1(config-line)# login local
```

2) Enable SSH only for login access.

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

3) 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
```

4) Save the running configuration file to the startup configuration file.

```
S1(config-if)# end
S1# copy run start
```