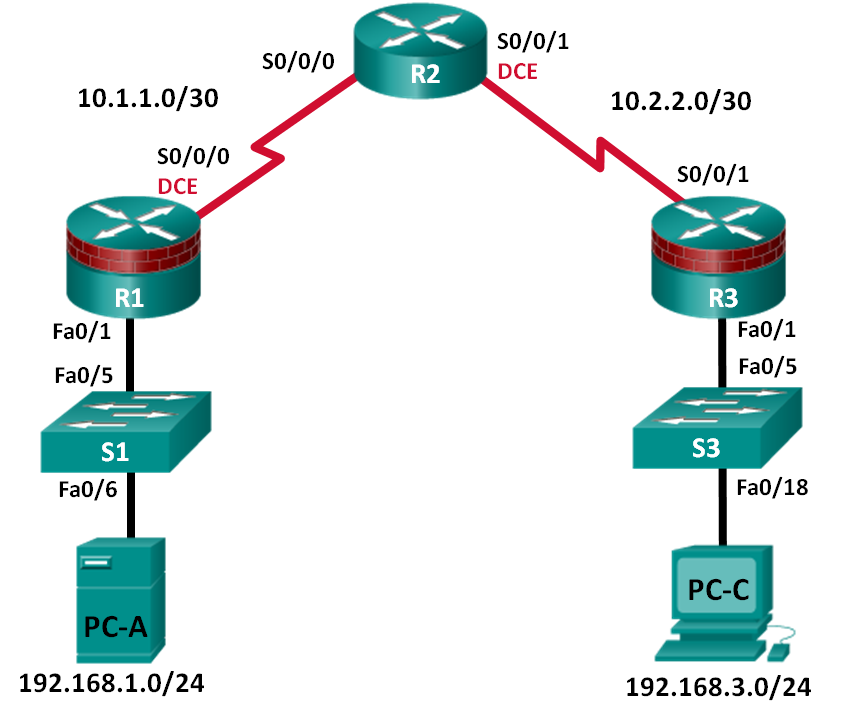
1. CCNA Security

Lab - Configuring Devices for Use with Cisco Configuration Professional (CCP) 2.5

1. Topology



**Note**: ISR G2 devices use GigabitEthernet interfaces instead of FastEthernet Interfaces.

1. IP Addressing Table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway | Switch Port |
| R1 | Fa0/1 | 192.168.1.1 | 255.255.255.0 | N/A | S1 Fa0/5 |
| S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A | N/A |
| R2 | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A | N/A |
| S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/A | N/A |
| R3 | Fa0/1 | 192.168.3.1 | 255.255.255.0 | N/A | S3 Fa0/5 |
| S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A | N/A |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | S1 Fa0/6 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 | S3 Fa0/18 |

1. Objectives

Part 1: Initialize and Reload Network Devices

* Initialize the router and reload
* Initialize the switch and reload

Part 2: Basic Network Device Configuration

* Cable the network as shown in the topology
* Initialize network devices
* Configure basic IP addressing for routers and PCs
* Configure routing
* Verify connectivity between hosts and routers

Part 3: Configure CCP Access for Routers

* Enable a secure HTTP server
* Create a user account with privilege level 15
* Configure SSH and Telnet access for local login

Part 4: Basic CCP Configuration

* Install CCP
* Manage communities
* Discover router devices

1. Background / Scenario

Cisco Configuration Professional (CCP) is a Windows-based device management tool for Integrated Service Routers (ISRs). CCP simplifies router configurations through easy-to-use wizards. The objective of this lab is to verify that the routers and PCs are configured properly for use with CCP.

**Note**: The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 15.1(4)M8 (Advanced IP Services image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

**Note**: Make sure that the routers and switches have been erased and have no startup configurations.

1. Required Resources

* 3 Routers (Cisco 1841 with Cisco IOS Release 15.1(4)M8 advanced IP services image or comparable)
* 2 Switches (Cisco 2960 or comparable)
* 2 PCs (Windows Vista or Windows 7 with CCP 2.5, latest version of Java, Internet Explorer, and Flash Player)
* Serial and Ethernet cables, as shown in the topology
* Console cables to configure Cisco networking devices

**CCP Notes**:

* If the PC on which CCP is installed is running Windows Vista or Windows 7, it may be necessary to right-click on the CCP icon or menu item, and choose **Run as administrator**.
* In order to run CCP, it may be necessary to temporarily disable antivirus programs and O/S firewalls. Make sure that all pop-up blockers are turned off in the browser.

1. CCP Related Hardware and Software Information using Academy Bundled Equipment

IOS Images:

For the latest compatible IOS images, search for **NetAcad Maintenance – Image & Hardware Spport.xls** in the NetAcad Maintenance under Equipment Information on NetSpace.

Interface Cards:

|  |  |
| --- | --- |
| Interfaces | Part Numbers |
| WAN Interface Cards (WICs) | WIC-1T, WIC-2A/S, WIC-2T |
| High-speed WICs (HWICs) | HWIC-4ESW-POE, HWIC-2A/S, HWIC-2T, HWIC-4ESW |

The following table summarizes the minimum PC requirement to run CCP:

|  |  |
| --- | --- |
| PC operating systems | Windows 7  Windows Vista: Business Edition and Ultimate Edition  Mac OSX 10.5.6 running Windows XP using VMWare 2.0 |
| Other software | Sun JRE 1.5.0\_11 up to 1.6.0\_16  Adobe Flash Player Version 10.0.12.36 and later |
| PC hardware | Minimum 2-GHz processor  1-GB DRAM minimum; 2 GB recommended  Screen Resolution: 1024 x 768  Free disk space of 400 MB |
| Browser requirements | Microsoft IE 6.0 or later |

The following JRE settings are needed for Cisco CP to function properly:

* + - * 1. Go to **Start** > **Control Panel** > **Java**.
        2. Click **View** under Java Applet Runtime Settings.
        3. Select your JRE in use.

In addition, if JRE is upgraded to versions 1.6.0\_11 or above, following settings are needed after Cisco CP installation.

* + - * 1. Go to **Start** > **Control Panel** > **Java** > **Advanced** tab.
        2. Click **Java Plug-in** tree.
        3. Uncheck the check box for **Enable Next-generation Java Plug-in**.
        4. Restart Cisco CP.

Link to release notes for CCP:

CCP version 2.5:

<http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/v2_5/rlsnts/ccp_rel_notes.html>

CCP version 2.6:

<http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_configuration_professional/v2_6/rlsnts/ccp_rel_notes.html>

CCP version 2.7:

<http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_configuration_professional/v2_7/rlsnts/ccp_v27_rel_notes.html>

1. Initialize and Reload Network Devices
   1. Initialize the Router and Reload.
      1. Connect to the router.

Console into the router and enter privileged EXEC mode using the **enable** command.

Router> **enable**

Router#

* + 1. Erase the startup configuration file from NVRAM.

Type the **erase startup-config** command to remove the startup configuration from NVRAM.

Router# **erase startup-config**

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

[OK]

Erase of nvram: complete

Router#

* + 1. Reload the router.

Issue the **reload** command to remove old configurations from memory. When prompted to Proceed with reload, press Enter to confirm the reload. Pressing any other key will abort the reload.

Router# **reload**

Proceed with reload? [confirm]

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

You may receive a prompt to save the running configuration prior to reloading the router. Respond by typing **no** and press **Enter**.

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

* + 1. Bypass the initial configuration dialog.

After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press **Enter**.

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

* + 1. Terminate the autoinstall program.

You will be prompted to terminate the autoinstall program. Respond **yes** and then press **Enter**.

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

Router>

* 1. Initialize the Switch and Reload.
     1. Connect to the switch.

Console into the switch and enter privileged EXEC mode.

Switch> **enable**

Switch#

* + 1. Determine if there have been any virtual LANs (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

Switch# **show flash**

Directory of flash:/

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

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

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

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

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

32514048 bytes total (20886528 bytes free)

Switch#

* + 1. Delete the VLAN file.
       1. If the **vlan.dat** file was found in flash, then delete this file.

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

You will be prompted to verify the file name. At this point, you can change the file name or press **Enter** if you have entered the name correctly.

* + - 1. When you are prompted to delete this file, press **Enter** to confirm the deletion. Pressing any other key will abort the deletion.

Delete flash:/vlan.dat? [confirm]

Switch#

* + 1. Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When prompted to remove the configuration file, press **Enter** to confirm the erase. (Pressing any other key will abort the operation.)

Switch# **erase startup-config**

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

[OK]

Erase of nvram: complete

Switch#

* + 1. Reload the switch.

Reload the switch to remove old configurations information from memory. When prompted to reload the switch, press **Enter** to proceed with the reload. Pressing any other key will abort the reload.

Switch# **reload**

Proceed with reload? [confirm]

**Note**: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press **Enter**.

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

* + 1. Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press **Enter**.

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

Switch>

1. Basic Network Device Configuration

In Part 2 of this lab, you will set up the network topology and configure basic settings such as interface IP addresses and routing.

* + 1. Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

* + 1. Configure basic settings for each router.
       1. Configure host names as shown in the topology.
       2. Configure the interface IP addresses as shown in the IP addressing table.
       3. Configure a clock rate for the routers with a DCE serial cable attached to their serial interface.

R1(config)# **interface S0/0/0**

R1(config-if)# **clock rate 64000**

* + - 1. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

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

* + 1. Configure routing on the routers.

Static and dynamic routing protocols are used in different chapter labs. Please refer to the chapter instructions to determine which routing protocol is used in each chapter lab.

* + 1. Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C, as shown in the IP addressing table.

* + 1. Verify connectivity between PC-A and R3.
       1. Ping from R1 to R3.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

* + - 1. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

**Note**: If you can ping from PC-A to PC-C, you have demonstrated that static routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to help identify routing protocol-related problems.

1. Router Access for CCP

In Part 3 of this lab, you will set up a router for use with CCP by enabling a secure HTTP server, creating a privileged user account, and configuring a SSH and Telnet access.

* + 1. Connect to your router through Telnet or SSH or the console.

Enter the global configuration mode using the command:

Router> **enable**

Router# **configure terminal**

* + 1. Enable the router as a HTTP server.
       1. Enable HTTP server.

Router(config)# **ip http server**

* + - 1. For a secure connection, enable the secure HTTP server.

Router(config)# **ip http secure-server**

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 3 seconds)

R1(config)#

\*Jan 1 17:23:44.103: %SSH-5-ENABLED: SSH 1.99 has been enabled

\*Jan 1 17:23:44.215: %PKI-4-NOAUTOSAVE: Configuration was modified. Issue "write memory" to save new certificate

**Note**: A secure HTTP server can only be enabled for cryptography-enabled Cisco IOS Software images. It is also possible to connect using an unsecure connection if the command **ip http server** is configured; however, this is an unsecure connection and not recommended for production environments.

* + - 1. Configure authentication for HTTP access using the local authentication.

Router(config)# **ip http authentication local**

* + 1. Create a user with privilege level 15.

Router(config)# **username admin privilege 15 password cisco12345**

* + 1. Configure SSH and Telnet for local login.

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

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

Router(config-line)# **transport input telnet**

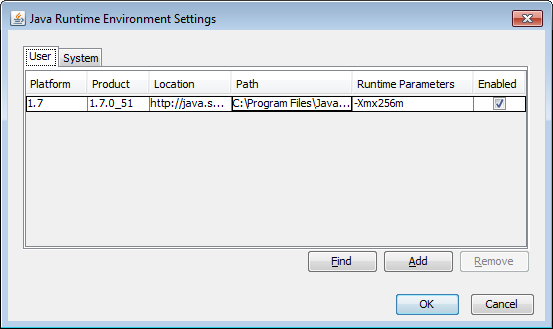
Router(config-line)# **transport input telnet ssh**

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

1. Java Settings on PCs

The next-generation Java Plug-in must be enabled, and the Security setting must be set to Medium for the CCP configuration of IPS. To support CCP configuration of IPS, PC should be running Java JRE version 6 or newer to set the Java heap to 256 MB. This is done using the runtime parameter –Xmx256m. The latest JRE for Windows can be downloaded from Oracle Corporation at <http://www.oracle.com/>.

* + 1. Enable next-generation Java Plug-in.
       1. Open the **Control Panel**, select **Java** to access the Java Control Panel.
       2. In the Java Control Panel, click the **Advanced** tab.
       3. Locate the heading Java Plug-in. Select the checkbox to **Enable the next-generation Plug-in**, which requires browser restart.
       4. Click **Apply**.
       5. Click **Yes** to allow the changes. Then click **OK** to acknowledge the changes.
    2. Change the Java security settings.
       1. Click the **Security** tab.
       2. Change the Security Level to **Medium** by moving the slider.
       3. Click **Apply**.
    3. Change the Java Applet Runtime settings.
       1. Click the **Java** tab and click the **View** button to change the Java Applet Runtime Settings.
       2. Double-click the **Runtime Parameters** box. Type **–Xmx256m** in the box.
       3. Click **OK**. Click **OK** again to exit the Java Control Panel.



* + 1. Restart all web browsers, including CCP if opened, for the changes to take effect.

1. CCP Installation and Initial Setup
   * 1. Install CCP.

**Note**: This section can be skipped if CCP is already installed on your PC.

* + - 1. Download CCP 2.5 from Cisco’s website:

<http://www.cisco.com/cisco/software/release.html?mdfid=281795035&softwareid=282159854&release=2.5&rellifecycle=&relind=AVAILABLE&reltype=all>

**Note**: Be sure to select the correct CCP file and not CCP Express. If there is a more current release of CCP, you may choose to download it. However, the labs in this course are based on CCP 2.5.

* + - 1. Choose the file **cisco-config-pro-k9-pkg-2\_5-en.zip**.

**Note**: Choose the PC-based version, not the Express version.

* + - 1. Agree to the terms and conditions. Download and save the file to the desired location.
      2. Open the zip file and run the CCP executable.
      3. Follow the on-screen instructions to install CCP 2.5 on your PC.
    1. Run CCP as Administrator.

If CCP is installed on a PC that uses the Microsoft Windows Vista operating system or the Microsoft Windows 7 operating system, CCP may fail to launch. Two possible solutions are listed below:

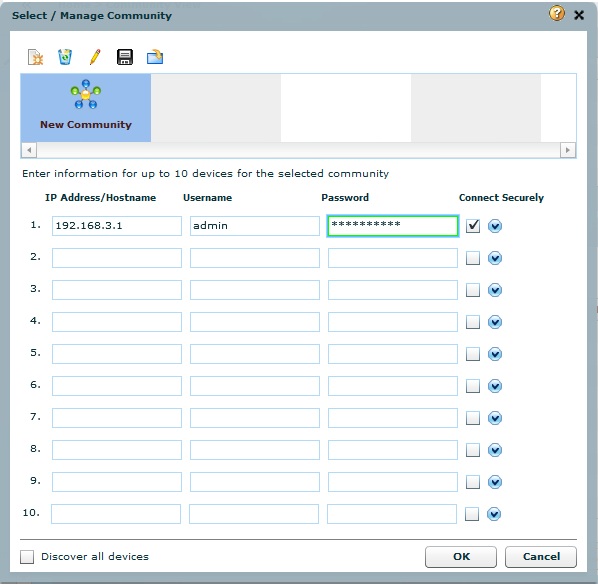
* + - 1. Option 1: Run as Administrator settings:
         1. Right click on the CCP icon or menu item and select **Properties**.
         2. While in the **Properties** dialog box, select the **Compatibility** tab. In this tab, select the checkbox for **Run this program as administrator** in Privilege Level section.
         3. Click **OK**.
      2. Option 2: Run as Administrator for each launch:
         1. Right click on the CCP icon or menu item and select **Run as Administrator**.
         2. For more information, please refer to the [Cisco CP Quick Start Guide](http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/guides/CiscoCPqsg.html) or search for “run as administrator” for your operating system on the Internet.

**Note**: It may be necessary to temporarily disable antivirus programs and O/S firewalls in order to run CCP.

* + 1. Create / Manage Communities.

CCP 2.5 can discover up to 10 devices in a community. If desired, the information for both R1 and R3 can be included in one community, if the PC has network connectivity to the routers. Only R3 is discovered on PC-C in this section.

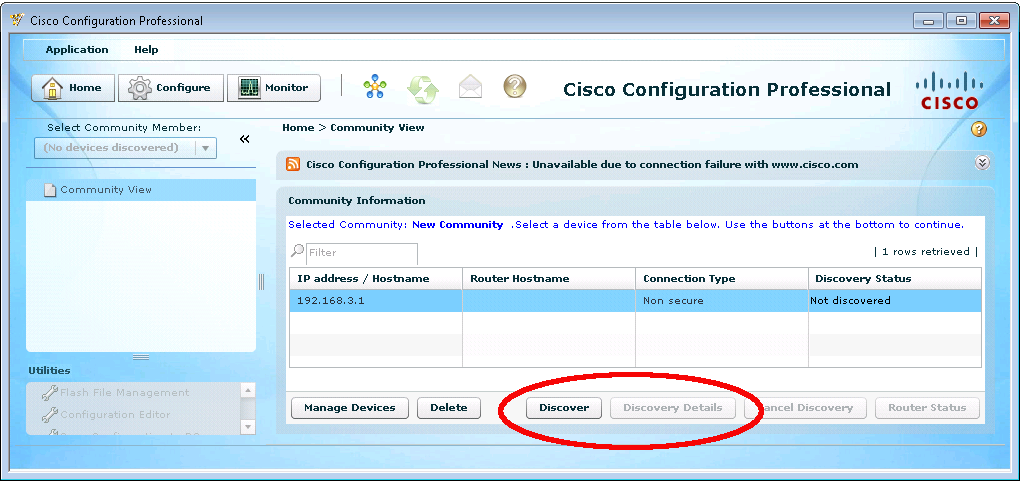
* + - 1. On PC-C, start CCP: **Start** > **Cisco Configuration Professional**.
      2. In the Select / Manage Community window, input into the appropriate fields the R3 IP address 192.168.3.1, the username **admin**, and the password **cisco12345**. The checkbox **Connect Securely** can be selected for a more secure connection to the device. This requires the configuration of the command **ip http secure-server**.
      3. Click **OK** to continue.



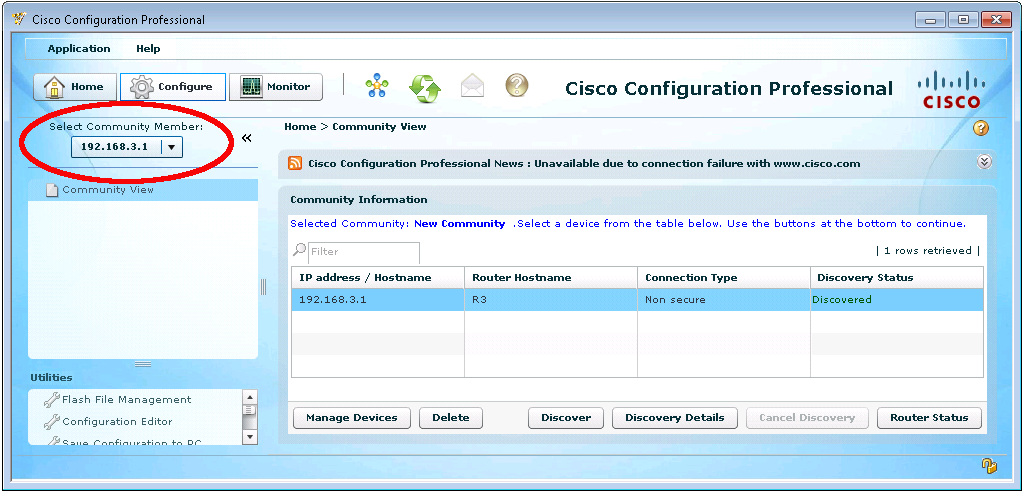
* + 1. Discovery Router Devices.
       1. Click **Discover** on the Dashboard to discover and connect to R3. If discovery fails, click the **Discovery Details** button to determine the problem so that you can resolve the issue.

When connecting securely, you must accept the certificate when the Security Certificate Alert window displays, to establish a connection to the device. CCP uses the Internet Explorer (IE) browser. Be sure IE settings are set to allow popup windows.

**Note**: If you experience problems with accepting the security certificate, you can connect using an unsecure connection. The command **ip http server** must be configured on the router and the checkbox **Connect Securely** (from step 2 above) must be unchecked. Keep in mind, this is an unsecure connection and not recommended in a production environment.



* + - 1. After the router has been discovered by CCP, you are ready to configure your Select Community Member. In this example, the Select Community Member is 192.168.3.1.



* + - 1. After the successful discovery of the device, configure the device as directed in the respective labs.

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 (Fa0/0) | Fast Ethernet 0/1 (Fa0/1) | 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 (Fa0/0) | Fast Ethernet 0/1 (Fa0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (Fa0/0) | Fast Ethernet 0/1 (Fa0/1) | 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. | | | | |