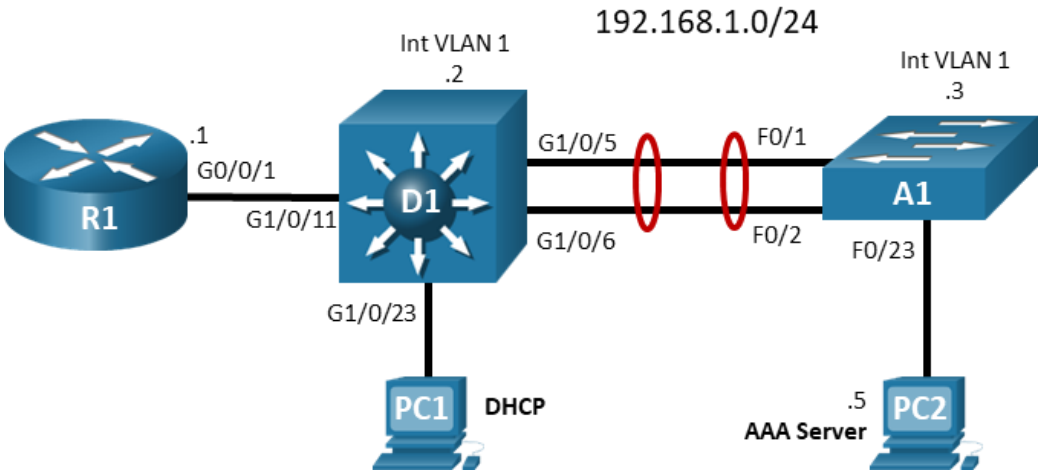
# Lab - Configure Local and Server-Based AAA Authentication

## Topology




## Addressing Table

| Device | Interface | IP Address | Subnet Mask |
|---|---|---|---|
| R1 | G0/0/1 | 192.168.1.1 | 255.255.255.0 |
| D1 | VLAN 1 | 192.168.1.2 | 255.255.255.0 |
| A1 | VLAN 1 | 192.168.1.3 | 255.255.255.0 |
| PC1 | NIC | DHCP | |
| PC2 | NIC | 192.168.1.5 | 255.255.255.0 |

## Objectives

**Part 1: Build the Network and Configure Basic Device Settings and Interface Addressing**

**Part 2: Configure Local AAA**

**Part 3: Configure Server-Based AAA using RADIUS on A1**

**Part 4: Configure Server-Based AAA using TACACS+ on D1**

## Background / Scenario

Using AAA-based services allows for more granular control of access to your devices. In this lab you will configure local AAA users and then server-based AAA leveraging RADIUS and TACACS+. Centralized management of usernames and passwords, as well as privileges and allowed commands, makes overall network access security management much simpler.

**Note:** This lab is an exercise in configuring options available for AAA-based authentication and does not necessarily reflect network troubleshooting best practices.

**Note**: The routers used with CCNP hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 3650s with Cisco IOS XE Release 16.9.4 (universalk9 image) and Cisco Catalyst 2960s with Cisco IOS Release 15.2(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 the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the 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 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 3650 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 1 PC (Choice of operating system with a terminal emulation program installed)
- 1 PC (Choice of operating system with Cisco Networking Academy CCNP VM running in a virtual machine client)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

## Part 1: Build the Network and Configure Basic Device Settings and Interface Addressing

In Part 1, you will set up the network topology and configure basic settings and interface addressing on routers.

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

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

### Step 2: Configure basic settings for each device.

a. Console into each device, enter global configuration mode, and apply the basic settings. The startup configurations for each device are provided below.

**Router R1**

```
hostname R1
no ip domain lookup
enable secret cisco12345cisco
banner motd # R1, Configure AAA-Based Authentication #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
interface g0/0/1
 ip address 192.168.1.1 255.255.255.0
 no shutdown
 exit
ip dhcp excluded-address 192.168.1.1 192.168.1.5
```

```
ip dhcp pool HOST_ADDRESSING
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 exit
```

**Router D1**

```
hostname D1
no ip domain lookup
enable secret cisco12345cisco
banner motd # D1, Configure AAA-Based Authentication #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
interface vlan 1
 ip address 192.168.1.2 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.1
interface g1/0/23
 spanning-tree portfast
 switchport mode access
 no shutdown
 exit
interface g1/0/11
 spanning-tree portfast
 switchport mode access
 no shutdown
 exit
interface range g1/0/5-6
 switchport mode trunk
 channel-group 1 mode active
 no shutdown
 exit
interface range g1/0/1-4, g1/0/7-10, g1/0/12-22, g1/0/24, g1/1/1-4
 shutdown
 exit
```

**Router A1**

```
hostname A1
no ip domain lookup
enable secret cisco12345cisco
banner motd # A1, Configure AAA-Based Authentication #
line con 0
 exec-timeout 0 0
 logging synchronous
```

```
 exit
interface vlan 1
 ip address 192.168.1.3 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.1
interface range f0/1-2
 switchport mode trunk
 channel-group 1 mode active
 no shutdown
 exit
interface range f0/3-24, g0/1-2
 shutdown
 exit
interface f0/23
 switchport mode access
 spanning-tree portfast
 no shutdown
 exit
```

b. Set the clock on each device to UTC time.

c. Save the running configuration to startup-config.

d. Verify PC1 receives an address via DHCP.

e. Verify that D1, A1, PC1 and PC2 can ping R1 interface G0/0/1.

### Step 3: Start the CCNP VM on PC2.

**Note**: If you have not completed **Lab - Install the CCNP Virtual Machine**, do so now before continuing with this lab.

The CCNP VM will be the AAA server for this lab.

a. Open VirtualBox. Start the **CCNP VM** virtual machine.

b. Enter the password **StudentPass** to log into the VM if prompted.

c. Open a terminal and determine the network device name. In this example, ens160 is the network device name.

```
student@CCNP:~$ ip address
<output omitted>
2: ens160: <BROADCAST,MUTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether 00:50:56:b3:fa:69 brd ff:ff:ff:ff:ff:ff
```

d. Configure the IP address in the VM.

```
student@CCNP:~$ sudo ip addr add 192.168.1.5/24 dev ens160
```

e. Use the **ip address** command to verify the address has been assigned.

f. Verify that the VM can ping R1 interface G0/0/1, D1 and A1.

## Part 2: Configure Local AAA Authentication

One significant drawback to using local authentication is that it offers no backup capability. Adding AAA services to your device gives you this capability. The basic configurations you loaded do not include any username/password protection on the console or vty lines. In this part of the lab, you will use local AAA to add that functionality.

**Note**: Do not save your configuration beyond this point, just in case you are locked out of the device. This gives you the ability to restart the device and start again at this point versus doing a password recovery and potentially having to reconfigure everything.

### Step 1: Create a local user.

a. Create a local user named **localuser** with a scrypt-encrypted password of **cisco123**.

```
A1(config)# username localuser algorithm-type scrypt secret cisco123
```

b. Verify that the configuration is present in running-config by issuing the command **show run | include username**.

```
A1# show run | include username
username localuser secret 9
$9$FYuVSfDjMKy7hU$SCFRKN.aehfb6f7rguVl6TWTlnpQmNVHqBolXXjRrp.
```

### Step 2: Enable AAA new-model.

Enable AAA on the device with the global configuration command **aaa new-model**.

```
A1(config)# aaa new-model
```

### Step 3: Create and test a default method list.

A single named method list allows you to configure up to four AAA methods for a given operation on the device. These methods will be used in the order they are configured. If any method results in a rejection, then the attempt fails. If the method is unavailable, then the next configured method will be used.

Method lists are named with either a custom name or the name default. A custom-named method list must be configured to intercept the operation of concern. A default method list applies to every instance of a given operation on the device, without any additional configuration.

Operations supported by AAA Authentication include:

```
A1(config)# aaa authentication ?
  arap              Set authentication lists for arap.
  attempts          Set the maximum number of authentication attempts
  banner            Message to use when starting login/authentication.
  dot1x             Set authentication lists for IEEE 802.1x.
  enable            Set authentication list for enable.
  eou               Set authentication lists for EAPoUDP
  fail-message      Message to use for failed login/authentication.
  local-override    Local accounts always get checked first.
  login             Set authentication lists for logins.
  onep              Set authentication lists for ONEP
  password-prompt   Text to use when prompting for a password
  ppp               Set authentication lists for ppp.
  rejected          Set blocking action for failed logins
  sgbp              Set authentication lists for sgbp.
```

```
  suppress         Do not send access request for a specific type of user.
  username-prompt  Text to use when prompting for a username
  webauth          set authentication lists for Webauth
```

Our focus in this lab is the login process. There are many AAA options for the login process:

```
A1(config)# aaa authentication login default ?
  cache          Use Cached-group
  enable         Use enable password for authentication.
  group          Use Server-group
  krb5           Use Kerberos 5 authentication.
  krb5-telnet    Allow logins only if already authenticated via Kerberos V
                 Telnet.
  line           Use line password for authentication.
  local          Use local username authentication.
  local-case     Use case-sensitive local username authentication.
  none           NO authentication.
  passwd-expiry  enable the login list to provide password aging support
  radius         Use RADIUS authentication.
  tacacs+        Use TACACS+ authentication.
```

**Note**: Do not save your configuration until you have tested the default method list and verified that it works.

a. Create a default method list for login that uses the enable password.

```
A1(config)# aaa authentication login default enable
```

b. Because this method list is a default for the login process, it is now in effect for every possible login vector, without any additional configuration. Issue the **show run | section line con** command and note that the login command is not present in any form.

```
A1# show run | section line con
line con 0
 exec-timeout 0 0
 logging synchronous
```

c. Completely log out of the console session, and then try to log back in. You should be prompted for a password only. Enter the enable secret password, which is configured as **cisco12345cisco**.

```
A1 con0 is now available

Press RETURN to get started.

 A1, Configure AAA-Based Authentication

User Access Verification

Password: <enter cisco12345cisco>

A1>
```

### Step 4: Create and test a named method list.

a. Create another method list for login, but this time name the list **VTY-AUTH**. This method list should use the local database only.

```
A1(config)# aaa authentication login VTY-AUTH local
```

b. Apply the VTY-AUTH method list to the vty lines.

```
A1(config)# line vty 0 4
A1(config-line)# login authentication VTY-AUTH
A1(config-line)# exit
```

c. Now use Telnet from a PC to A1. You are now prompted for a username and then a password. Use the username **localuser** and password **cisco123** and see if you can log in.

```
A1, Configure AAA-Based Authentication


User Access Verification


Username: localuser
Password: <entered correct password, cisco123>
```

## Part 3: Configure Server-Based AAA using RADIUS on A1

The main drawback to local authentication of any sort is that it cannot be centrally managed. To change a password for a particular user, you must configure each device in the network that person accesses. Obviously, this is not very efficient, and could consume a lot of time. Using a centralized authentication server is much more efficient.

There are two main authentication protocols, RADIUS and TACACS+. In this part, we will focus on RADIUS.

It is important that you know the RADIUS server ports. The standard ports are UDP/1812 for authentication and authorization and UDP/1813 for accounting. Cisco IOS defaults to RADIUS to using UDP ports 1645 for authentication and authorization and 1646 for accounting. In our lab, we are using a RADIUS server listening on the standard ports. Therefore, the port numbers must be set as a part of the configuration.

### Step 1: Configure a radius server.

Create an individual server object for each RADIUS server that is serving your network.

a. Create the server using the command **radius server** *name*.

```
A1(config)# radius server RADIUS
A1(config-radius-server)#
```

b. Configure the address and the port numbers used for this RADIUS server.

```
A1(config-radius-server)# address ipv4 192.168.1.5 ?
  acct-port  UDP port for RADIUS accounting server (default is 1646)
  alias      1-8 aliases for this server (max. 8)
  auth-port  UDP port for RADIUS authentication server (default is 1645)
  <cr>
A1(config-radius-server)# address ipv4 192.168.1.5 auth-port 1812 acct-port 1813
```

c. Configure the shared secret for this RADIUS server. The RADIUS server we are using has a shared secret set to **$trongPass**.

```
A1(config-radius-server)# key $trongPass
A1(config-radius-server)# exit
```

**Note**: The example configuration is being deployed on a 2960 switch. On an IOS-XE based device, after entering the key, you will receive a warning that in the future you must use an encrypted key.

```
WARNING: Command has been added to the configuration using a type 0 password. However,
type 0 passwords will soon be deprecated. Migrate to a supported password type
```

d. Verify the radius server creation with the command **show radius server all.** As you can see from the output below, the radius server is automatically put into a server group called radius.

```
A1# show radius server all
Server group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
    Server(192.168.1.5:1812,1813) Transactions:
    Authen: 0   Author: 0       Acct: 0
    Server_auto_test_enabled: FALSE
     Keywrap enabled: FALSE
```

## Step 2: Configure a method list to use the AAA server group RADIUS.

a. Create a method list that utilizes the AAA server group radius as its primary authentication server and the local database as the backup authentication method.

```
A1(config)# aaa authentication login RAD-AUTH group radius local
```

b. Apply the newly created method list to the vty lines.

```
A1(config)# line vty 0 4
A1(config-line)# login authentication RAD-AUTH
A1(config-line)# exit
```

c. Test the configuration by using Telnet from your PC to A1. You should be prompted for a username and password. In this case, the username on our RADIUS server is **raduser** and the password is **upass123**.

d. Disconnect the Telnet session.

e. At the console of A1, issue the command **debug radius authentication**. Then, return to your PC and connect to A1 via Telnet. This time, use the localuser account you created at the beginning of the lab. It will not work. After the login attempt fails, go back to the console of your device and look at the debug output. You should see an “ACCESS-REJECT” message.

```
Feb 14 20:27:42.025: RADIUS/ENCODE(00000010): ask "Username: "
Feb 14 20:27:42.025: RADIUS/ENCODE(00000010): send packet; GET_USER
A1#
Feb 14 20:27:46.227: RADIUS/ENCODE(00000010): ask "Password: "
Feb 14 20:27:46.236: RADIUS/ENCODE(00000010): send packet; GET_PASSWORD
A1#
Feb 14 20:27:48.450: RADIUS/ENCODE(00000010):Orig. component type = Exec
Feb 14 20:27:48.450: RADIUS/ENCODE(00000010): dropping service type, "radius-server
attribute 6 on-for-login-auth" is off
Feb 14 20:27:48.450: RADIUS(00000010): Config NAS IP: 0.0.0.0
Feb 14 20:27:48.450: RADIUS(00000010): Config NAS IPv6: ::
Feb 14 20:27:48.450: RADIUS/ENCODE(00000010): acct_session_id: 5
Feb 14 20:27:48.450: RADIUS(00000010): sending
Feb 14 20:27:48.450: RADIUS/ENCODE: Best Local IP-Address 192.168.1.3 for R
A1#adius-Server 192.168.1.5
Feb 14 20:27:48.450: RADIUS(00000010): Send Access-Request to 192.168.1.5:1812
onvrf(0) id 1645/8, len 73
```

```
Feb 14 20:27:48.450: RADIUS:  authenticator CD DA 11 0D 3A AC E1 B0 - D5 F7 A0 81 00
B7 FB 7E
Feb 14 20:27:48.450: RADIUS:  User-Name           [1]   11  "localuser"
Feb 14 20:27:48.450: RADIUS:  User-Password       [2]   18  *
Feb 14 20:27:48.450: RADIUS:  NAS-Port            [5]   6   1
Feb 14 20:27:48.450: RADIUS:  NAS-Port-Id         [87]  6
A1# "tty1"
Feb 14 20:27:48.450: RADIUS:  NAS-Port-Type       [61]  6   Virtual      [5]
Feb 14 20:27:48.450: RADIUS:  NAS-IP-Address      [4]   6   192.168.1.3
Feb 14 20:27:48.450: RADIUS(00000010): Sending a IPv4 Radius Packet
Feb 14 20:27:48.450: RADIUS(00000010): Started 5 sec timeout
Feb 14 20:27:49.457: RADIUS: Received from id 1645/8 192.168.1.5:1812, Access-Reject,
len 20
Feb 14 20:27:49.457: RADIUS:  authenticator 83 77 D4 F5 4F F8 95 76 - ED 7F 37 1D 6A
85 B9 F8
Feb
A1# 14 20:27:49.457: RADIUS(00000010): Received from id 1645/8
A1#
Feb 14 20:27:53.467: RADIUS/ENCODE(00000010): ask "Username: "
Feb 14 20:27:53.467: RADIUS/ENCODE(00000010): send packet; GET_USER
```

f. Disconnect the Telnet session, then shutdown the port connecting your RADIUS server to the switch and use Telnet to access A1 again. Provide the localuser name and password once again. You will see that the device falls back to the second option, which is the local user database.

## Part 4: Configure Server-Based AAA using TACACS+ on D1

TACACS+ was developed by Cisco and released as an open standard beginning in 1993. It is an incompatible derivation of the original TACACS protocol, handling authentication, authorization, and accounting services. TACACS+ works differently than RADIUS by separating the authentication and authorization components. This allows TACACS+ to provide granular control of what an authenticated user is allowed to do. Other differences include operating over TCP (TCP port 49) instead of UDP, and encrypting the entire TACACS+ packet. RADIUS only encrypts passwords. In this part of the lab, you will configure a TACACS+ server and method list for use on the vty lines.

### Step 1: Enable AAA new-model.

Enable AAA on the device with the global configuration command **aaa new-model**.

```
D1(config)# aaa new-model
```

### Step 2: Create a local user.

Create a local user named **localuser** with a scrypt-encrypted password of **cisco123**.

```
D1(config)# username localuser algorithm-type scrypt secret cisco123
```

### Step 3: Configure a TACACS+ server.

a. Create the server using the command **tacacs server [name]**.

```
D1(config)# tacacs server TACACS
```

b. Configure the address used for this TACACS server.

```
D1(config-server-tacacs)# address ipv4 192.168.1.5
```

c. Configure the shared secret for this TACACS server. If your AAA server is the Cisco Networking Academy-provided Ubuntu server, the shared secret is set to **$trongPass**.

```
D1(config-server-tacacs)# key $trongPass
```

**Note**: The example configuration is being deployed on a 3650 switch. On an IOS-XE based device, after entering the key, you will receive a warning that in the future you must use an encrypted key.

```
WARNING: Command has been added to the configuration using a type 0 password. However,
type 0 passwords will soon be deprecated. Migrate to a supported password type
```

d. Configure the single-connection option, which causes the device to maintain the TCP connection to the TACACS+ server. This cuts down on connections to the AAA server and can help to speed up the AAA process between the device and the server.

```
D1(config-server-tacacs)# single-connection
D1(config-server-tacacs)# exit
```

e. Create a group for the TACACS servers, and identify the servers belonging to the group. The servers are queried in the order they are added to the group.

```
D1(config)# aaa group server tacacs+ TACACS-GP
D1(config-sg-tacacs+)# server name TACACS
D1(config-sg-tacacs+)# exit
D1(config)# end
```

f. Verify the TACACS server creation with the command **show tacacs**.

```
D1# show tacacs

Tacacs+ Server -  public  :
               Server name: TACACS
            Server address: 192.168.1.5
               Server port: 49
             Socket opens:          0
            Socket closes:          0
            Socket aborts:          0
            Socket errors:          0
         Socket Timeouts:           0
   Failed Connect Attempts:         0
        Total Packets Sent:         0
        Total Packets Recv:         0
          Expected Replies:         0
```

### Step 4: Configure an authentication method list to use the AAA server group TACACS-GP.

Getting started, first establish TACACS as the authentication server and login with a privileged account.

a. Create a default authentication method list for the login process. Reference the TACACS server group first and then the local database.

```
D1(config)# aaa authentication login default group TACACS-GP local
```

b. Create a default authorization method list for the EXEC process, referencing the TACACS server group first and then the none method.

```
D1(config)# aaa authorization exec default group TACACS-GP none
```

**Note**: The none method should never be used in a production environment.

c. Log out of the console and log back in. If your AAA server is the Cisco Networking Academy CCNP VM, use the username **tacadmin** and password **tacpass1**. Issue the enable command and provide the configured enable secret **cisco12345cisco**. This should work and you should be in privileged EXEC mode.

d. Issue the command show privilege and you should be advised that you are operating at privilege level 15.

```
D1# show privilege
Current privilege level is 15
```

### Step 5: Configure method lists to use AAA server group TACACS-GP.

To fully utilize TACACS+, several method lists must be configured.

a. Create three authorization default methods lists, one for privilege 0, one for privilege 1, and one for privilege 15. In each list, reference the TACACS server group first and then the none method.

```
D1(config)# aaa authorization commands 0 default group TACACS-GP none
D1(config)# aaa authorization commands 1 default group TACACS-GP none
D1(config)# aaa authorization commands 15 default group TACACS-GP none
```

b. Create a default accounting method list for the exec process using start-stop accounting and reference the TACACS server group only.

```
D1(config)# aaa accounting exec default start-stop group TACACS-GP
```

c. Create a default accounting method list for commands at level 15 using start-stop accounting and reference the TACACS server group only.

```
D1(config)# aaa accounting commands 15 default start-stop group TACACS-GP
```

d. Configure AAA authorization for config-commands.

```
D1(config)# aaa authorization config-commands
```

e. Configure AAA authorization for the console.

```
D1(config)# aaa authorization console
```

f. Logout of the device.

### Step 6: Verify AAA using TACACS.

a. From PC1, use Telnet to access D1. If your AAA server is the Cisco Networking Academy CCNP VM, use the username **tacreader** and password **tacpass2**. You should be logged in successfully at user EXEC.

b. Attempt to enter privileged EXEC mode and you will be denied. Attempt to issue the **show ip interface brief** command and you will be allowed. Log out.

c. From PC1, use Telnet to access D1. If your AAA server is the Cisco Networking Academy CCNP VM, use the username **tacadmin** and password **tacpass1**.

d. Login should be successful. You should be able to enter global configuration mode. Attempt to make a trivial change to the device, such as changing the motd banner. You should be allowed to do so. Log out.

e. If you have access to the TACACS+ server, examine the accounting file located at **/var/log/tac_plus.acct**. You should see a record of your activity as **tacreader** and **tacadmin**.

f. As a challenge, you can configure server-based AAA using RADIUS or TACACS+ server on R1.

## Router Interface Summary Table

| 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) |
| 4221 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 4300 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |

**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.