CCNAv7 ITN Skills Assessment – ITN Final Skills Exam (Equipment)

Your exam may be different

Topology

CCNAv7 ITN Skills Assessment

Assessment Objectives

- **Part 1: Develop an IP Addressing Scheme** (20 points, 25 minutes)
- **Part 2: Initialize and Reload Devices** (10 points, 20 minutes)
- **Part 3: Configure Device IP address and Security Settings** (45 points, 35 minutes)
- **Part 4: Test and Verify IPv4 and IPv6 End-to-End Connectivity** (15 points, 20 minutes)
- **Part 5: Use the IOS CLI to Gather Device Information** (10 points, 10 minutes)

Scenario

In this Skills Assessment (SA) you will configure the devices in a small network. You must configure a router, switch and PCs to support both IPv4 and IPv6 connectivity. You will configure security, including SSH, on the router. In addition, you will test and document the network using common CLI commands.

Required Resources

- 1 Router (Cisco 4221 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)
- 2 PCs (Windows with a 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

Instructions

Part 1: Develop an IP Addressing Scheme

- **Total points: 20**
- **Time: 25 minutes**

a. Your instructor will assign one of the IPv4 networks from the table below. You will subnet it to provide IP addresses to two subnets that will support the required number of hosts. No subnet calculators may be used. All work must be shown using the IP Addressing worksheet below.

Network	Number of Hosts in Subnet A	Number of Hosts in Subnet B
192.168.10.0/24	100	50
172.16.1.0/25	60	20
209.165.201.0/27	12	5

IP Addressing Worksheet

- Type 1
- Type 2
- Type 3

Specification	Subnet A	Subnet B
Number of bits in the subnet	**25**	**26**
IP mask (binary)	11111111.11111111.11111111.10000000	11111111.11111111.11111111.11000000
New IP mask (decimal)	**255.255.255.128**	**255.255.255.192**
Maximum number of usable subnets (including the 0th subnet)	**2**	**4**
Number of usable hosts per subnet	**126**	**62**
IP Subnet	**192.168.10.0**	**192.168.10.128**
First IP Host address	**192.168.10.1**	**192.168.10.129**
Last IP Host address	**192.168.10.126**	**192.168.10.190**

b. Record your subnet assignment in the table below.

- 1) Assign the first IPv4 address of each subnet to a router interface
  - (i) subnet A is hosted on R1 G0/0/1
  - (ii) subnet B is hosted on R1 G0/0/0
- 2) Assign the last IPv4 address of each subnet to the PC NIC
- 3) Assign the second IPv4 address of subnet A to S1
- 4) List the maximum number of useable hosts per subnet

Description	Subnet A	Subnet B
First IP address	**192.168.10.1**	**192.168.10.129**
Last IP address	**192.168.10.126**	**192.168.10.190**
Maximum number of hosts	**126**	**62**

c. Record the IP address information for each device:

Device	IP address	Subnet Mask	Gateway	Points
PC-A	**192.168.10.126**	**255.255.255.128**	**192.168.10.1**	2 points
R1-G0/0/0	**192.168.10.129**	**255.255.255.192**	N/A	2 points
R1-G0/0/1	**192.168.10.1**	**255.255.255.128**	N/A	2 points
S1	**192.168.10.2**	**192.168.10.1**	**255.255.255.128**	2 points
PC-B	**192.168.10.190**	**255.255.255.192**	**192.168.10.129**	2 points

d. Use the IPv6 address 2001:db8:acad::/48 and create two subnets for use in this network. Record the IPv6 addresses in the table.

Assigned to Interface	IPv6 Subnet Address	Prefix Length
G0/0/1	**2001:db8:acad:a::/64**	**64**
G0/0/0	**2001:db8:acad:b::/64**	**64**

e. Record the IPv6 address information for each device.

Note: Use **FE80::1** as the link-local address on both router interfaces.

Device	IPv6 address	Prefix Length	Gateway	Points
R1-G0/0/0	**2001:db8:acad:b::1**	**64**	N/A	3 pts

Device	IPv6 address	Prefix Length	Gateway	Points
R1-G0/0/1	**2001:db8:acad:a::1**	**64**	N/A	3 pts
S1	**2001:db8:acad:a::2**	**64**	**2001:db8:acad:a::1**	4 pts

Before proceeding, verify your IP addressing scheme with the instructor.

Instructor Sign-off Part 1:

Instructor Sign-off

Total Points for Part 1 (20 points):

Enter score here.

Part 2: Initialize and Reload Devices

- **Total points: 10**
- **Time: 20 minutes**
- Erase the startup configurations and VLANs from the router and switch and reload the devices.

On Switch

```
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete vlan.dat
Switch#reload
Proceed with reload? [confirm]
```

On Router

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
Initializing Hardware ...
```

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

- After the switch is reloaded, change the SDM template to one that supports IPv6 as necessary, and reload the switch again.
  On Switch:

```
Switch>

Switch>enable

Switch#configure terminal


Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#exit

Switch#reload
```

Before proceeding, ask your instructor verify device initializations.

Instructor Sign-off Part 2:

Instructor Sign-off

Total points (10 points):

Enter score here.

Part 3: Configure Device IP Address and Security Settings

- **Total points: 45**
- **Time: 35 minutes**

Step 1: Configure R1.

Configuration tasks for R1 include the following:

Task	Specification	Points
Disable DNS lookup		
Router name	R1	1 point
Domain name	ccna-lab.com	1 point

Task	Specification	Points
Encrypted privileged EXEC password	ciscoenpass	1 point
Console access password	ciscoconpass	1 point
Set the minimum length for passwords	10 characters	2 points
Create an administrative user in the local database	Username: **admin** Password: **admin1pass**	2 points
Set login on vty lines to use local database		1 point
Set vty lines to accept SSH connections only		1 point
Encrypt the clear text passwords		1 point
Configure an MOTD Banner		1 point
Enable IPv6 Routing		1 point
Configure Interface G0/0/0	Set the description Set the Layer 3 IPv4 address Set the IPv6 Link Local Address as **FE80::1** Set the Layer 3 IPv6 address Activate Interface	6 points
Configure Interface G0/0/1	Set the description Set the Layer 3 IPv4 address Set the IPv6 Link Local Address as **FE80::1** Set the Layer 3 IPv6 address Activate Interface	6 points
Generate an RSA crypto key	1024 bits modulus	2 points

On Router

```
Router>enable
Router#configure terminal

Router(config)#no ip domain lookup

Router(config)#hostname R1

R1(config)#ip domain-name ccna-lab.com

R1(config)#enable secret ciscoenpass

R1(config)#line console 0

R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit

R1(config)#security passwords min-length 10

R1(config)#username admin secret admin1pass

R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
```

```
R1(config-line)#exit

R1(config)#service password-encryption

R1(config)#banner motd #Unauthorized Access is Prohibited!#

R1(config)# ipv6 unicast-routing

R1(config)#interface g0/0/0
R1(config-if)#description Connect to Subnet B
R1(config-if)#ip address 192.168.10.129 255.255.255.192
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#ipv6 address 2001:db8:acad:b::1/64
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#interface g0/0/1
R1(config-if)#description Connect to Subnet A
R1(config-if)#ip address 192.168.10.1 255.255.255.128
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#ipv6 address 2001:db8:acad:a::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
```

```
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to
2048 for your
  General Purpose Keys. Choosing a key modulus greater than
512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]
```

Step 2: Configure S1.

Configuration tasks for S1 include the following:

Task	Specification	Points
Disable DNS lookup		1 point
Switch name	S1	1 point
Domain name	ccna-lab.com	1 point
Encrypted privileged EXEC password	ciscoenpass	1 point
Console access password	ciscoconpass	1 point
Shutdown all unused interfaces	F0/1-4, F0/7-24, G0/1-2	1 point
Create an administrative user in the local database	Username: **admin** Password: **admin1pass**	1 point
Set login on vty lines to use local database		1 point
Set vty lines to accept SSH connections only		1 point
Encrypt the clear text passwords		1 point

Task	Specification	Points
Configure an MOTD Banner		1 point
Generate an RSA crypto key	1024 bits modulus	2 points
Configure Management Interface (SVI) on VLAN1	Set the description Set the Layer 3 IPv4 address Set the IPv6 Link Local Address as **FE80::2** Set the Layer 3 IPv6 address	2 points

```
Switch>enable

Switch#configure terminal


Switch(config)#no ip domain lookup


Switch(config)#hostname S1


S1(config)#ip domain-name ccna-lab.com


S1(config)#enable secret ciscoenpass


S1(config)#line console 0

S1(config-line)#password ciscoconpass

S1(config-line)#login

S1(config-line)#exit
```

```
S1(config)#interface range f0/1-4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown


S1(config)#username admin secret admin1pass


S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit


S1(config)#service password-encryption


S1(config)#banner motd #Unauthorized Access is Prohibited!#


S1(config)#crypto key generate rsa
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to
2048 for your
  General Purpose Keys. Choosing a key modulus greater than
512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]

S1(config)#interface vlan 1
S1(config-if)#description Switch Subnet A
S1(config-if)#ip address 192.168.10.2 255.255.255.128
S1(config-if)#ipv6 address FE80::2 link-local
S1(config-if)#ipv6 address 2001:db8:acad:a::2/64
```

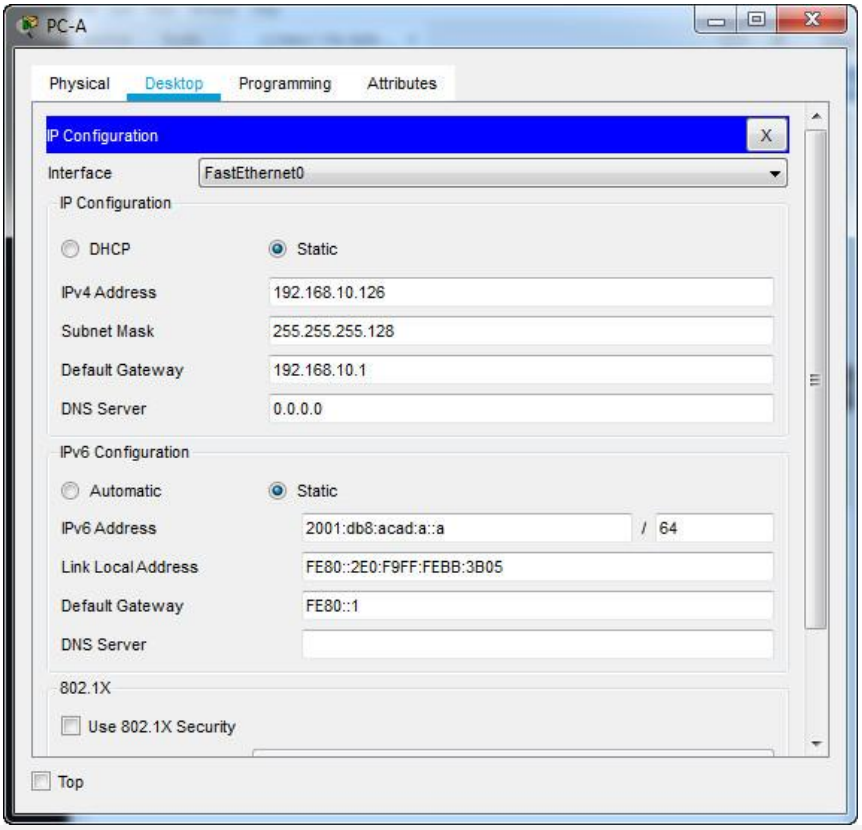
```
S1(config-if)#no shutdown
S1(config-if)#exit

S1(config)#ip default-gateway 192.168.10.1
```

Step 3: Configure host computers.

After configuring each host computer, record the host network settings with the `ipconfig /all` command. (2 points)

PC-A Network Configuration (1 point)	
Description	
Physical Address	**00E0.F9BB.3B05**
IPv4 Address	**192.168.10.126**
Subnet Mask	**255.255.255.128**
IPv4 Default Gateway	**192.168.10.1**
IPv6 Address	**2001:DB8:ACAD:A::A**
IPv6 Default Gateway	**FE80::1**

PC-A

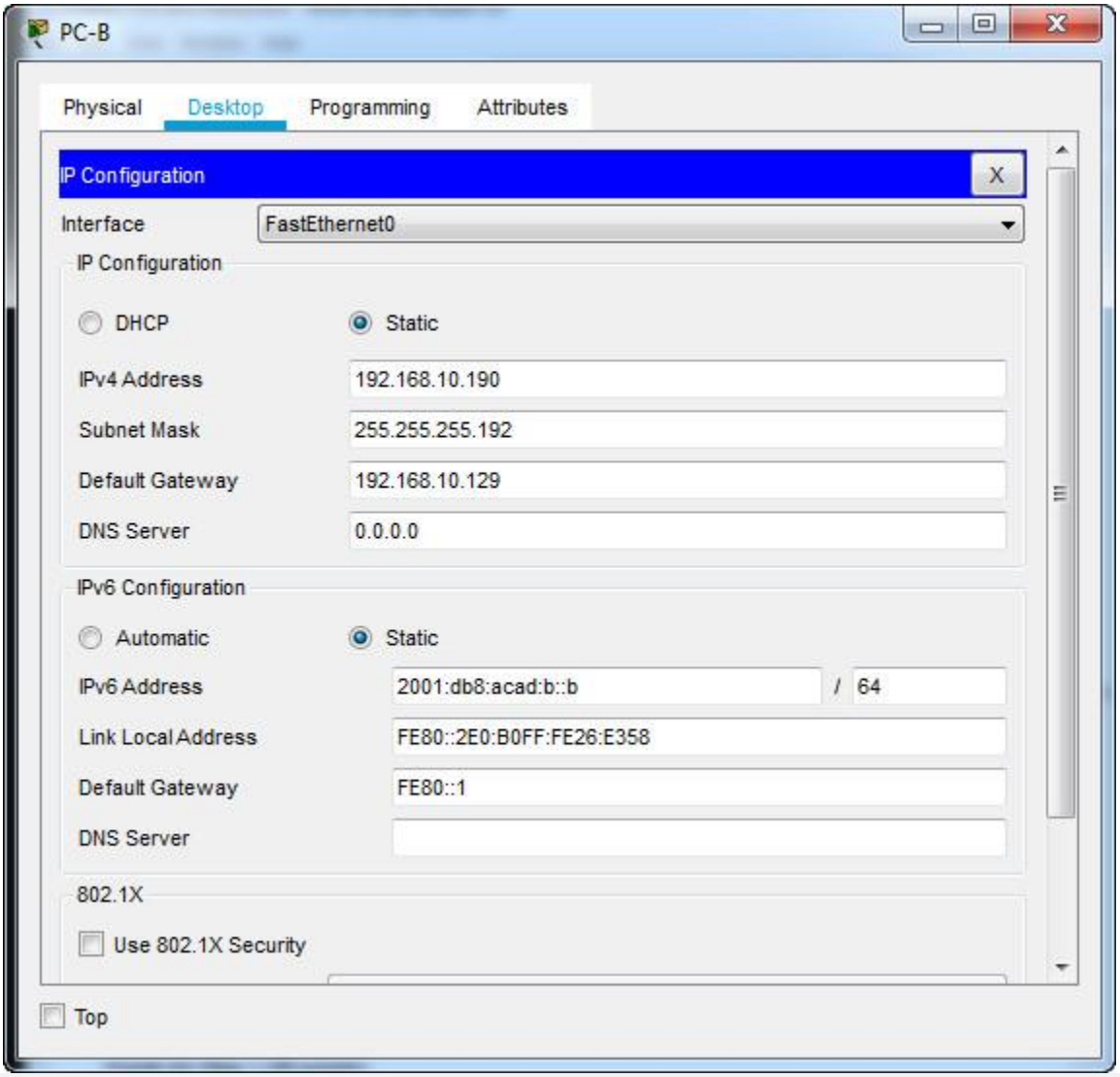



```
C:\>ipconfig /all


FastEthernet0 Connection:(default port)


   Connection-specific DNS Suffix..:

   Physical Address.................: 00E0.F9BB.3B05

   Link-local IPv6 Address.........:
FE80::2E0:F9FF:FEBB:3B05

   IPv6 Address....................: 2001:DB8:ACAD:A::A

   IPv4 Address....................: 192.168.10.126
```

```
   Subnet Mask.....................: 255.255.255.128

   Default Gateway.................: FE80::1

                                     192.168.10.1

   DHCP Servers....................: 0.0.0.0

   DHCPv6 IAID.....................:

   DHCPv6 Client DUID..............: 00-01-00-01-32-43-85-
90-00-E0-F9-BB-3B-05

   DNS Servers.....................: ::

                                     0.0.0.0
```

PC-B Network Configuration (1 point)	
Description	
Physical Address	**00E0.B026.E358**
IPv4 Address	**192.168.10.190**
Subnet Mask	**255.255.255.192**
IPv4 Default Gateway	**192.168.10.129**
IPv6 Address	**2001:DB8:ACAD:B::B**
IPv6 Default Gateway	**FE80::1**

PC-B




```
C:\>ipconfig /all


FastEthernet0 Connection:(default port)


   Connection-specific DNS Suffix..:

   Physical Address.................: 00E0.B026.E358

   Link-local IPv6 Address.........:
FE80::2E0:B0FF:FE26:E358
```

```
   IPv6 Address....................: 2001:DB8:ACAD:B::B

   IPv4 Address....................: 192.168.10.190

   Subnet Mask.....................: 255.255.255.192

   Default Gateway.................: FE80::1

                                     192.168.10.129

   DHCP Servers....................: 0.0.0.0

   DHCPv6 IAID.....................:

   DHCPv6 Client DUID..............: 00-01-00-01-A3-07-96-
75-00-E0-B0-26-E3-58

   DNS Servers.....................: ::

                                     0.0.0.0
```

Points for Step 1 (28 points):
Enter score here.
Points for Step 2 (15 points):
Enter score here.
Points for Step 3 (2 points):
Enter score here.
Instructor Sign-off Part 4:
Instructor Sign-off
Total Points for Part 3 (45 points)
Enter score here.

Part 4: Test and Verify End-to-End Connectivity

- **Total points: 15**
- **Time: 10 minutes**

Use the ping command to test IPv4 and IPv6 connectivity between all network devices.
Note: If pings to host computers fail, temporarily disable the computer firewall and retest.
Use the following table to methodically verify connectivity with each network device. Take corrective action to establish connectivity if a test fails:

From	To	Protocol	IP Address	Ping Results	Points
PC-A	R1 G0/0/0	IPv4	192.168.10.129	success	1 point
		IPv6	2001:DB8:ACAD:B::1	success	1 point
	R1 G0/0/1	IPv4	192.168.10.1	success	1 point
		IPv6	2001:DB8:ACAD:A::1	success	1 point
	S1 VLAN 1	IPv4	192.168.10.2	success	1 point
		IPv6	2001:db8:acad:a::2	success	1 point
	PC-B	IPv4	192.168.10.190	success	1 point
		IPv6	2001:DB8:ACAD:B::B	success	1 point
PC-B	R1 G0/0/0	IPv4	192.168.10.129	success	1 point
		IPv6	2001:DB8:ACAD:B::1	success	1 point
	R1 G0/0/1	IPv4	192.168.10.1	success	1 point
		IPv6	2001:DB8:ACAD:A::1	success	1 point
	S1 VLAN 1	IPv4	192.168.10.2	success	1 point
		IPv6	2001:db8:acad:a::2	success	1 point

In addition to the ping command, what other command is useful in displaying network delay and breaks in the path to the destination? (1 point)
tracert or traceroute

Instructor Sign-off Part 4:
Instructor Sign-off

Total points for Part 4 (15 points):
Enter score here.

Part 5: Use the IOS CLI to Gather Device Information

- **Total points: 10**
- **Time: 10 minutes**

Step 1: Issue the appropriate command to discover the following information: `show version`

Description	Command	Points
Router Model	blank	1/3 point
IOS Image File	blank	1/3 point
Total RAM	blank	1/3 point
Total Flash Memory	blank	1/3 point
Configuration Register	blank	1/3 point
CLI Command Used	blank	1/3 point

Step 2: Enter the appropriate CLI command needed to display the following on R1:

Command Description	Command	Points
Display a summary of important information about the IPv4 interfaces on R1.	blank	1 point
Display the IPv4 routing table.	blank	1 point
Display the Layer 2 to Layer 3 mapping of addresses on R1.	blank	1 point
Display detailed IPv4 information about interface G0/0/0 on R1.	blank	1 point
Display the IPv6 routing table.	blank	1 point

Command Description	Command	Points
Display a summary of IPv6 interface addresses and status.	blank	1 point
Display information about the devices connected to R1. Information should include Device ID, Local Interface, Hold time, Capability, Platform, and Port ID.	blank	1 point
Save the current configuration so it will be used the next time the router is started.	blank	1 point

Instructor Sign-off Part 5:
Instructor Sign-off
Total points for Part 5 (10 points):
Enter score here.

Part 6: Cleanup

NOTE: DO NOT PROCEED WITH CLEANUP UNTIL YOUR INSTRUCTOR HAS GRADED YOUR SKILLS EXAM AND HAS INFORMED YOU THAT YOU MAY BEGIN CLEANUP.
Unless directed otherwise by the instructor, restore host computer network connectivity, and then turn off power to the host computers.

Before turning off power to the router and switch, remove the NVRAM configuration files (if saved) from both devices.

Disconnect and neatly put away all LAN cables that were used in the Final.

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)

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
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.