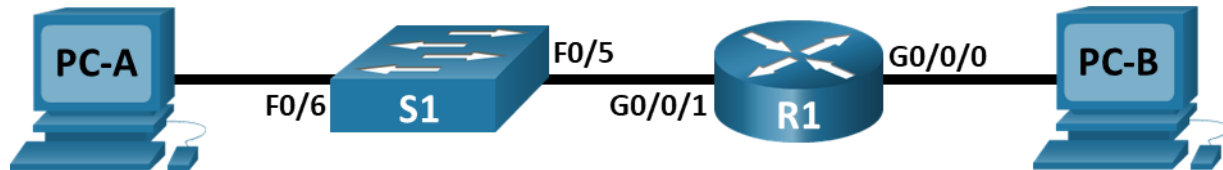


Lab - Configure Basic Router Settings.

Topology



Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0/0	192.168.0.1 /24	N/A
		2001:db8:acad::1 /64	
		fe80::1	
	G0/0/1	192.168.1.1 /24	
		2001:db8:acad:1::1 /64	
		fe80::1	
	Loopback0	10.0.0.1 /24	
		2001:db8:acad:2::1 /64	
		fe80::1	
PC-A	NIC	192.168.1.10 /24	192.168.1.1
		2001:db8:acad:1::10 /64	fe80::1
PC-B	NIC	192.168.0.10 /24	192.168.0.1
		2001:db8:acad::10 /64	fe80::1

Objectives

Part 1: Set Up the Topology and Initialize Devices

- Cable equipment to match the network topology.
- Initialize and restart the router and switch.

Part 2: Configure Devices and Verify Connectivity

- Assign static IPv4 and IPv6 information to the PC interfaces.
- Configure basic router settings.
- Configure the router for SSH.
- Verify network connectivity.

Part 3: Display Router Information

- Retrieve hardware and software information from the router.
- Interpret the output from the startup configuration.
- Interpret the output from the routing table.
- Verify the status of the interfaces.

Background / Scenario

This is a comprehensive lab to review previously covered IOS router commands. In Parts 1 and 2, you will cable the equipment and complete basic configurations and interface settings on the router.

In Part 3, you will use SSH to connect to the router remotely and utilize the IOS commands to retrieve information from the device to answer questions about the router.

For review purposes, this lab provides the commands necessary for specific router configurations.

Note: The routers used with CCNA 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 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 router and switch have been erased and have no startup configurations. Consult with your instructor for the procedure to initialize and reload a router and switch.

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

Note: The Gigabit Ethernet interfaces on Cisco 4221 routers are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Instructions

Part 1: Set Up the Topology and Initialize Devices

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

- Attach the devices as shown in the topology diagram, and cable as necessary.
- Power on all the devices in the topology.

Step 2: Initialize and reload the router and switch.

Part 2: Configure Devices and Verify Connectivity

Step 1: Configure the PC interfaces.

- Configure the IP address, subnet mask, and default gateway settings on PC-A.
- Configure the IP address, subnet mask, and default gateway settings on PC-B.

Step 2: Configure the router.

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

```
router> enable
```

- b. Enter configuration mode.

```
router# config terminal
```

- c. Assign a device name to the router.

```
router(config)# hostname R1
```

- d. Set the router's domain name as ccna-lab.com.

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

- e. 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
```

- f. Encrypt the plaintext passwords.

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

- g. Configure the system to require a minimum 12-character password.

```
R1(config)# security passwords min-length 12
```

- h. Configure the username **SSHadmin** with an encrypted password of **55Hadm!n2020**.

```
R1(config)# username SSHadmin secret 55Hadm!n2020
```

- i. Generate a set of crypto keys with a 1024 bit modulus

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

- j. Assign the privileged EXEC password to **\$cisco!PRIV***

```
R1(config)# enable secret $cisco!PRIV*
```

- k. Assign **\$cisco!!CON*** as the console password, configure sessions to disconnect after four minutes of inactivity, and enable login.

```
R1(config)# line console 0
```

```
R1(config-line)# password $cisco!!CON*
```

```
R1(config-line)# exec-timeout 4 0
```

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

- l. Assign **\$cisco!!VTY*** as the vty password, configure the vty lines to accept SSH connections only, configure sessions to disconnect after four minutes of inactivity, and enable login using the local database.

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

```
R1(config-line)# password $cisco!!VTY*
```

```
R1(config-line)# exec-timeout 4 0
```

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

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

- m. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

```
R1(config)# banner motd $ Authorized Users Only! $
```

- n. Enable IPv6 Routing

```
R1(config)# ipv6 unicast-routing
```

- o. Configure all three interfaces on the router with the IPv4 and IPv6 addressing information from the addressing table above. Configure all three interfaces with descriptions. Activate all three interfaces.

```
R1(config)# interface g0/0/0
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad::1/64
R1(config-if)# description Connection to PC-B
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# description Connection to S1
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface loopback0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# description loopback adapter
R1(config-if)# no shutdown
R1(config-if)# exit
```

- p. The router should not allow vty logins for two minutes if three failed login attempts occur within 60 seconds.

```
R1(config)# login block-for 120 attempts 3 within 60
R1(config)# exit
```

- q. Set the clock on the router.

```
R1# clock set 15:20:00 5 Sept 2019
```

- r. Save the running configuration to the startup configuration file.

```
R1# copy running-config startup-config
```

What would be the result of reloading the router prior to completing the **copy running-config startup-config** command?

The contents of the running configuration in RAM would be erased during reload. As a result, the router would boot up without a startup configuration and the user would be asked if they would like to enter initial configuration dialog.

Step 3: Verify network connectivity.

- a. Using the command line at PC-A, ping the IPv4 and IPv6 addresses for PC-B.

Note: It may be necessary to disable the PCs firewall.

Were the pings successful?

Yes

- b. Remotely access R1 from PC-A using the Tera Term SSH client.

Using Tera Term on PC-A, open an SSH session to the R1 Loopback interface IPv4 address. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router. Log in as **SSHadmin** with the password **55Hadm!n2020**.

Was remote access successful?

Yes

Using Tera Term on PC-A, open an SSH session to the R1 Loopback interface IPv6 address. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router. Log in as **SSHadmin** with the password **55Hadm!n2020**. **Note:** The IPv6 address should be surrounded with square brackets, i.e. [IPv6 address]

Was remote access successful?

Yes

Why is the Telnet protocol considered to be a security risk?

A Telnet session can be seen in plaintext. It is not encrypted. Passwords can easily be seen using a packet sniffer.

Part 3: Display Router Information

In Part 3, you will use **show** commands from an SSH session to retrieve information from the router.

Step 1: Establish an SSH session to R1.

Using Tera Term on PC-B, open an SSH session to the R1 Loopback interface IPv6 address and log in as **SSHadmin** with the password **55Hadm!n2020**.

Step 2: Retrieve important hardware and software information.

- a. Use the **show version** command to answer questions about the router.

```
R1# show version
Cisco IOS XE Software, Version 16.09.04
Cisco IOS Software [Fujil], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9_IAS-M), Version
16.9.4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Wed 20-Mar-19 08:01 by mcpre
```

```
Cisco IOS-XE software, Copyright (c) 2005-2019 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
```

Lab - Configure Basic Router Settings

documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

ROM: IOS-XE ROMMON

R1 uptime is 32 minutes
Uptime for this control processor is 35 minutes
System returned to ROM by PowerOn
System restarted at 14:49:40 UTC Thu Sep 5 2019
System image file is "flash:isr4200-universalk9_ias.16.09.04.SPA.bin"
Last reload reason: PowerOn

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Suite License Information for Module:'esg'

Suite	Suite Current	Type	Suite Next reboot
FoundationSuiteK9 securityk9 appxk9	None	None	None

Technology Package License Information:

Technology	Technology-package Current	Technology-package Type	Technology-package Next reboot
appxk9	None	None	None
securityk9	securityk9	Permanent	securityk9
ipbase	ipbasek9	Permanent	ipbasek9

The current throughput level is 35000 kbps

Smart Licensing Status: Smart Licensing is DISABLED

```
cisco ISR4221/K9 (1RU) processor with 1784656K/6147K bytes of memory.  
Processor board ID FGL221693BV  
2 Gigabit Ethernet interfaces  
2 Serial interfaces  
32768K bytes of non-volatile configuration memory.  
4194304K bytes of physical memory.  
6598655K bytes of flash memory at bootflash:..  
0K bytes of WebUI ODM Files at webui:..
```

Configuration register is 0x2142 (will be 0x2102 at next reload)

What is the name of the IOS image that the router is running?

Image version may vary but in this lab, it is isr4200-universalk9_ias.16.09.04.SPA.bin.

How much non-volatile random-access memory (NVRAM) does the router have?

Answers may vary, but in this lab, it is 32768K bytes of NVRAM.

How much Flash memory does the router have?

Answers may vary but in this lab, it has 6598655K bytes of flash memory.

- b. The **show** commands often provide multiple screens of outputs. Filtering the output allows a user to display certain sections of the output. To enable the filtering command, enter a pipe (|) character after a **show** command, followed by a filtering parameter and a filtering expression. You can match the output to the filtering statement by using the **include** keyword to display all lines from the output that contain the filtering expression. Filter the **show version** command, using **show version | include register** to answer the following question.

```
R1# show version | include register
```

```
Configuration register is 0x2142 (will be 0x2102 at next reload)
```

What is the boot process for the router on the next reload?

Answers may vary. In most cases (0x2102), the router will undergo a normal boot, load the IOS from the Flash memory, and load the startup configuration from the NVRAM if present. If the config register is 0x2142, the router will bypass the startup config and begin at the user-mode command prompt. If the initial boot fails, the router goes into ROMMON mode.

Step 3: Display the startup configuration.

Use the **show startup-config** command on the router to answer the following questions.

```
R1# show start
```

```
Using 1997 out of 33554432 bytes
```

```
!
```

```
! Last configuration change at 15:20:18 UTC Thu Sep 5 2019
```

```
! NVRAM config last updated at 15:25:17 UTC Thu Sep 5 2019
```

```
!
```

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 12
enable secret 5 $1$b2iA$/7Hj3HRmBXTbOESxmlyiG0
!
no aaa new-model
!
no ip domain lookup
ip domain name ccna-lab.com
!
login block-for 120 attempts 3 within 60
login on-success log
!
subscriber templating
!
ipv6 unicast-routing
multilink bundle-name authenticated
!
license udi pid ISR4221/K9 sn FGL221693BV
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
username SSHadmin secret 5 $1$6HtR$T0QPZWbzp6bz3g6iwmZrP1
!
redundancy
mode none
!
interface Loopback0
description loopback adapter
ip address 10.0.0.1 255.255.255.0
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:2::1/64
!
interface GigabitEthernet0/0/0
description Connection to PC-B
ip address 192.168.0.1 255.255.255.0
negotiation auto
```



```
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD::1/64
!
interface GigabitEthernet0/0/1
description Connection to S1
ip address 192.168.1.1 255.255.255.0
negotiation auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:1::1/64
!
interface Serial0/1/0
no ip address
!
interface Serial0/1/1
no ip address
!
ip forward-protocol nd
no ip http server
ip http secure-server
!
control-plane
!
banner motd ^C Authorized Users Only! ^C
!
line con 0
exec-timeout 4 0
password 7 145311021F07256A650B1C1B68
logging synchronous
login
transport input none
stopbits 1
line aux 0
stopbits 1
line vty 0 4
exec-timeout 4 0
password 7 15560805172924656905011B59
login local
transport input ssh
!
end
```

How are passwords presented in the output?

Passwords are encrypted due to the service password-encryption command.

Use the **show startup-config | section vty** command.

```
R1# show startup-config | section vty
line vty 0 4
exec-timeout 4 0
```

```
password 7 15560805172924656905011B59
login local
transport input ssh
```

What is the result of using this command?

A user receives the startup configuration output beginning with the line that includes the first instance of the filtering expression.

Step 4: Display the routing table on the router.

Use the **show ip route** command on the router to answer the following questions.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
```

```
Gateway of last resort is not set
```

```
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/24 is directly connected, Loopback0
L       10.0.0.1/32 is directly connected, Loopback0
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.0.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0/1
```

What code is used in the routing table to indicate a directly connected network?

The C designates a directly connected subnet. An L designates a local interface. Both answers are correct.

How many route entries are coded with a C code in the routing table?

3

Step 5: Display a summary list of the interfaces on the router.

a. Use the **show ip interface brief** command on the router to answer the following question.

```
R1# show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
```

Lab - Configure Basic Router Settings

```
GigabitEthernet0/0/0 192.168.0.1 YES manual up
GigabitEthernet0/0/1 192.168.1.1 YES manual up
Serial0/1/0          unassigned YES unset up
Serial0/1/1          unassigned YES unset up
Loopback0            10.0.0.1   YES manual up
```

What command changed the status of the Gigabit Ethernet ports from administratively down to up?

no shutdown

- b. Use the **show ipv6 int brief** command to verify IPv6 settings on R1.

```
R1# show ipv6 interface brief
```

```
GigabitEthernet0/0/0 [up/up]
    FE80::1
    2001:DB8:ACAD::1
GigabitEthernet0/0/1 [up/up]
    FE80::1
    2001:DB8:ACAD:1::1
Serial0/1/0          [up/up]
    unassigned
Serial0/1/1          [up/up]
    unassigned
Loopback0            [up/up]
    FE80::1
    2001:DB8:ACAD:2::1
```

What is the meaning of the [up/up] part of the output?

The [up/up] status reflects the Layer 1 and Layer 2 status of the interface and does not rely on Layer 3 for status.

- c. On PC-B, change its configuration so that it no longer has a static IPv6 address. You may have to reboot the machine. Then, issue the **ipconfig** command on PC-B to examine the IPv6 configuration.

What is the IPv6 address assigned to PC-B?

Answers will vary. IPv6 address of 2001:db8:acad:a:d428:7de2:997c:b05a

What is the default gateway assigned to PC-B?

fe80::1

Issue a ping from PC-B to the R1 default gateway link local address. Was it successful?

Yes

Issue a ping from PC-B to the R1 IPv6 unicast address 2001:db8:acad::1. Was it successful?

Yes

Reflection Questions

1. In researching a network connectivity issue, a technician suspects that an interface was not enabled. What **show** command could the technician use to troubleshoot this issue?

Answers may vary. However, **show ip interface brief** or **show interfaces** or **show startup-config** would provide the information.

2. In researching a network connectivity issue, a technician suspects that an interface was assigned an incorrect subnet mask. What **show** command could the technician use to troubleshoot this issue?

Answers may vary. **show startup-config** or **show running-config** or **show interfaces** or **show protocols** will provide the information.

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.

Device Configs

Router R1

```
R1# show run
Building configuration...
```

Lab - Configure Basic Router Settings

```
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 12
enable secret 5 $1$b2iA$/7Hj3HRmBXTbOESxmlyiG0
!
no aaa new-model
!
no ip domain lookup
ip domain name ccna-lab.com
!
!
login block-for 120 attempts 3 within 60
login on-success log
!
!
subscriber templating
!
!
ipv6 unicast-routing
multilink bundle-name authenticated
!
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
username SSHadmin secret 5 $1$6HtR$T0QPZWbzp6bz3g6iwmZrP1
!
redundancy
mode none
!
interface Loopback0
description loopback adapter
ip address 10.0.0.1 255.255.255.0
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:2::1/64
!
```

Lab - Configure Basic Router Settings

```
interface GigabitEthernet0/0/0
description Connection to PC-B
ip address 192.168.0.1 255.255.255.0
negotiation auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD::1/64
!
interface GigabitEthernet0/0/1
description Connection to S1
ip address 192.168.1.1 255.255.255.0
negotiation auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:1::1/64
!
interface Serial0/1/0
no ip address
!
interface Serial0/1/1
no ip address
!
ip forward-protocol nd
no ip http server
ip http secure-server
!
control-plane
!
banner motd ^C Authorized Users Only! ^C
!
line con 0
exec-timeout 4 0
password 7 145311021F07256A650B1C1B68
logging synchronous
login
transport input none
stopbits 1
line aux 0
stopbits 1
line vty 0 4
exec-timeout 4 0
password 7 15560805172924656905011B59
login local
transport input ssh
!
end
```