



[Home](#) [★ CCNA »](#) [Security »](#) [CyberOps »](#) [Linux »](#)

[IT Questions Bank](#) [CCNA »](#) [CCNA Security v2.0 »](#) [Cybersecurity »](#) [Linux »](#) [Networking Essentials](#) [IoT »](#)

[IOS Commands Help](#) [IP Subnet Calculators »](#) [Donation](#) [Contact](#)

## 1.6.2 Packet Tracer – Configure Basic Router Settings – Physical Mode Answers

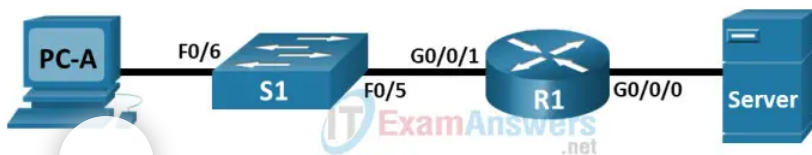
Jan 15, 2022 | Last Updated: Jan 17, 2022 | CCNA v7 Course #2 | No Comments

Share Tweet Share Pin it

**Contents**

### 1.6.2 Packet Tracer – Configure Basic Router Settings – Physical Mode Answers

#### Topology



#### Addressing Table

Device	
R1	(

Device	Interface	IP Address / Prefix	Default Gateway
R1		2001:db8:acad::1 /64	
		fe80::1	
	G0/0/1	192.168.1.1 /24	N/A
		2001:db8:acad:1::1 /64	
		fe80::1	
	Loopback0	10.0.0.1 /24	N/A
		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
Server	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**
- **Part 2: Configure Devices and Verify Connectivity**
- **Part 3: Display Router Information**

CCNA v7.0 Exam Answers

[CCNA 1 - v7](#)

[CCNA 2 - v7](#)

[CCNA 3 - v7](#)

## Background / Scenario

This is a comprehensive Packet Tracer Physical Mode (PTPM) activity 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 use the IOS commands to retrieve information from the device to answer questions about the router.

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

## Instructions

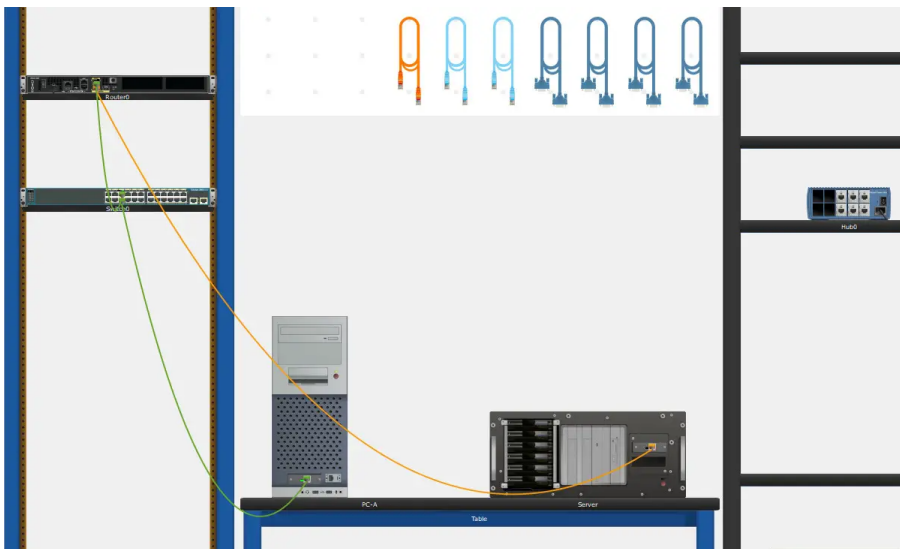
### Part 1: Set Up the Topology and Initialize Devices

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

- Click and drag the **Cisco 4321 ISR**, the **Cisco 2960 Switch**, and the **Server** from the **Shelf** to the **Rack**.
- Click and drag the **PC** from the **Shelf** to the **Table**.



- c. Cable the devices as specified in the topology diagram. Use **Copper Straight-through** cables for network connections.
- d. From the **PC**, connect a **Console Cable** to the **Cisco 4321 ISR**.
- e. Power on the **Cisco 4321 ISR**, **PC-A**, and **Server**. The power button for **Server** is on the bottom right. The 2960 switch should power on automatically.

[System Test Exam](#)[Modules 1 - 3: Basic Network Connectivity and Communications Exam Answers](#)[Modules 4 - 7: Ethernet Concepts Exam Answers](#)[Modules 8 - 10: Communicating Between Networks Exam Answers](#)[Modules 11 - 13: IP Addressing Exam Answers](#)[Modules 14 - 15: Network Application Communications Exam Answers](#)[Modules 16 - 17: Building and Securing a Small Network Exam Answers](#)[\[PT Skills\] Practice PT Skills Assessment \(PTSA\)](#)[\[Final Skills\] ITN Final Skills Exam \(PTSA\)](#)[ITNv7 Practice Final Exam](#)[CCNA 1 v7 FINAL Exam Answers](#)

## Part 2: Con

### Step 1: Conf

- a. Configure th

PC-A

Physical Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: 2001:db8:acad:1::10 / 64

Link Local Address: FE80::203:E4FF:FE71:4258

Default Gateway: fe80::1

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

## Related Posts

[13.3.12 Packet Tracer – Configure a WPA2 Enterprise WLAN on the WLC – Instructions Answer](#)

[6.2.4 Packet Tracer – Configure EtherChannel \(Instructions Answer\)](#)

[3.6.1 Packet Tracer – Implement VLANs and Trunking \(Instructions Answer\)](#)

[CCNA 2 \(Version 7.00\) SRWE Practice Final Exam Answers](#)

[CCNA 3 v7 Modules 6 – 8: WAN Concepts Test Online](#)

[9.3.4 Packet Tracer – Data Center Exploration – Physical Mode Answers](#)

[CCNA 2 v7 Modules 7 – 9: Available and Reliable Networks Test Online](#)

[12.1.7 Check Your Understanding – Introduction to Wireless Answers](#)

[7.1.5 Check Your Understanding – DHCPv4 Concepts Answers](#)

[14.3.5 Packet Tracer – Basic Router Configuration Review – Instructions Answer](#)

## Recent Comments

[I PT Skills  
wers](#)

[jre Basic Router](#)

b. Configure the IP address, subnet mask, and default gateway settings on **Server**.

Server

Physical Services Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.0.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server:

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: 2001:db8:acad::10 / 64

Link Local Address: FE80::207:ECFF:FEA5:6286

Default Gateway: fe80::1

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

[Settings \(Answers\)](#)

Humberto Santos on [IT Essentials \(ITE v6.0 + v7.0\) Chapter 3 Test Online](#)

IT Administrator on [ITN \(Version 7.00\) Final PT Skills Assessment \(PTSA\) Exam Answers](#)

Help on [ITN \(Version 7.00\) Final PT Skills Assessment \(PTSA\) Exam Answers](#)

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. Encrypt the plaintext passwords.

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

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

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

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

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

h. Generate a :



[report this ad](#)

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

i. Assign **\$cisco!PRIV\*** as the privileged EXEC password.

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

j. 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
```

k. 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
```

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



```
R1(config)#
```

m. Enable IPv6 routing.

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

n. 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 Server
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
```

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
```

o. Set the clock on the router.



```
R1# clock set 15:20:00 12 Nov 2020
```

p. Save the configuration.

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 **Server**.

Were the pings successful? **Yes**

b. From **PC-A**, remotely access **R1** using the Telnet / SSH client.

Using the Telnet / SSH client on PC-A, open an SSH session to the R1 Loopback interface IPv4 address. Ensure that the Connection Type is set to **SSH** and use **SSHadmin** as the username. When prompted, enter the password **55Hadm!n2020**.

Was remote access successful? **Yes**

c. Using the Telnet / SSH client on **PC-A**, open an SSH session to the R1 Loopback interface IPv6 address. Ensure that the Connection Type is set to **SSH** and use **SSHadmin** as the username. When prompted, enter the password **55Hadm!n2020**.

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 Telnet /  
interface IPv6 :  
**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 03.16.05.S - Extended Support Release  
Cisco IOS Software, ISR Software (X86\_64\_LINUX\_IOSD-UNIVERSALK9-M)  
Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2017 by Cisco Systems, Inc.

Compiled Thu 19-Jan-17 11:24 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2017 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  
software code licensed under GPL Version 2.0 is free software that  
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  
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

Router uptime is 1 days, 23 hours, 24 minutes, 3 seconds

Uptime for this control processor is 1 days, 23 hours, 24 minutes,  
System returned to ROM by power-on

System image file is "bootflash:/isr4300-universalk9.03.16.05.S.1!"

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 a  
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](mailto:export@cisco.com).

Suite License Information for Module:'esg'

---

Suite	CurrentType	Suite	Next	reboot
FoundationSuiteK9	None	None	None	None
securityk9				
appxk9				
AdvUCSuiteK9	None	None	None	None
uck9				
cme - srst				
cube				

---

FoundationSuiteK9

securityk9

appxk9

AdvUCSuiteK9

uck9

cme - srst

cube

Technology Package License Information:

---

Technology	Technology-package	Technology-package
CurrentType	Next	reboot

---

appxk9

uck9

securityk9:

ipbaseipba:

securityser

ipbaseipba:

```
cisco ISR4321/K9 (1RU) processor with 1687137K/6147K bytes of mem  
Processor board ID FLM2041W2HD  
2 Gigabit Ethernet interfaces  
32768K bytes of non-volatile configuration memory.  
4194304K bytes of physical memory.  
3223551K bytes of flash memory at bootflash:..  
Configuration register is 0x2102
```

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

**Image version may vary but in this PTLC, it is isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin.**

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

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

How much Flash memory does the router have?

**Answers may vary but in this PTLC, it has 3223551K bytes of flash memory.**

b. The **show** commands often provide multiple screens of outputs. Filtering the output lets you 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 0x2102
```

What would be the boot process for the router on the next reload if the configuration register was 0x2142?

**In most cases the configuration register will have a value of 0x2102 signifying that 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.

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

```
R1# show start  
Using 1520 bytes  
!  
version 15  
no service  
no service
```

```
service password-encryption
security passwords min-length 12
!
hostname R1
!
login block-for 120 attempts 3 within 60
!
!
enable secret 5 $1$mERr$2q6B19eTeuK92k7m8BhgZ/
!
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
username SSHadmin secret 5 $1$mERr$fuFUX0tVJZMfnQ0coB7vt/
!
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
!
spanning-tree mode pvst
!
!
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 Server
ip address 192.168.0.1 255.255.255.0
duplex auto
speed 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
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:1::1/64
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
ip access-
```

```

deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
!
banner motd ^C Authorized Users Only! ^C
!
!
line con 0
exec-timeout 4 0
password 7 08654F471A1A0A565328232A60
login
!
line aux 0
!
line vty 0 4
exec-timeout 4 0
password 7 08654F471A1A0A56533D383D60
login local
transport input ssh
!
!
end
!

```

How are passwords presented in the output?

**Passwords are encrypted because of the service password-encryption command.**

b. Use the **show running-config | section vty** command.

```

R1# show running-config | section vty
line vty 0 4
exec-timeout 4 0
password 7 08654F471A1A0A56533D383D60
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,
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 specific
+ - replicated
Gateway of
10.0.0.0/8

```

```
C10.0.0.0/24 is directly connected, Loopback0
L10.0.0.1/32 is directly connected, Loopback0
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C192.168.0.0/24 is directly connected, GigabitEthernet0/0/0
L192.168.0.1/32 is directly connected, GigabitEthernet0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C192.168.1.0/24 is directly connected, GigabitEthernet0/0/1
L192.168.1.1/32 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.

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

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
Loopback0 [up/up]
FE80::1
2001:DB8:ACAD:2::1
Vlan1 [administratively down/down]
unassigned
```

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 **Server**, change its configuration so that it no longer has a static IPv6 address. Then, issue the **ipconfig** command on **Server** to examine the IPv6 configuration.

What is the IPv6 address assigned to Server?

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

What is the default gateway assigned to **Server**?

**fe80::1**

From **PC-B**, issue a ping to the **R1** default gateway link local address. Was it successful?

**Yes**

From **Server**, issue a ping 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.**

## Download 1.6.2 Packet Tracer & PDF – Configure Basic Router Settings – Physical Mode



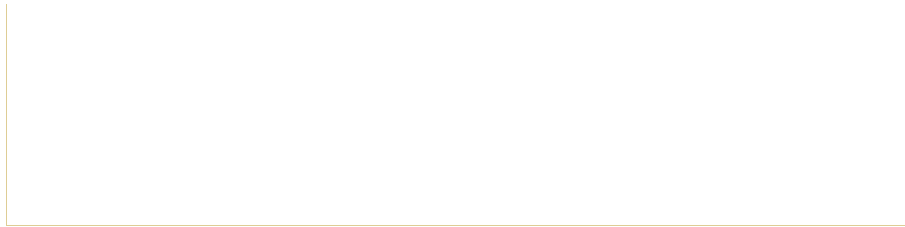
[1.6.2 Packet Tracer - Configure Basic Router Settings - Physical Mode](#)

2 file(s) 508.10 KB

Download



1.6.1 Pack  
S

[← Previous Article](#)[1.1.7 Packet Tracer – Basic Switch Configuration – Physical Mode Answers](#)[Next Article →](#)[3.4.6 Packet Tracer – Configure VLANs and Trunking – Physical Mode Answers](#)[report this ad](#)

*Be the First to Comment!*

**B** *I* U



**0 COMMENTS**

