# CCNAv7 Introduction to Networks

ITN Practice Skills Assessment – Packet Tracer

**Instructor Version**

Text in red does not appear in the student version of these instructions.

This assessment activity is designed to provide practice in preparation for the final Skills Assessment in this course. This activity uses variables to create variations of this assessment that are presented to the student. The variations consist of changes to the topology layout and labeling and the names of the devices. These device naming variations appear in the instructions as well as the topologies. This means that students will receive different versions of the assessment that combine different names and labels with different topology layouts. There are a number of possible combinations. Each time the student starts the assessment, they will receive a different variation unless they are resuming work on a previously saved assessment.

In the instructions below, values that are contained in double brackets, such as [[Router0Name]], are placeholders for values that will vary for each assessment. Students will not see the double-bracketed terms, instead they will see the device names and labels for their version of the activity.

The variations that students will receive do not affect the difficulty of the assessment activities.

In addition, you will find this assessment activity to be more “open-ended” than some of the activities that the student has experienced in the initial portion of the course. As the course progresses, the instructions become less prescriptive, allowing the student the opportunity to get a better measure of their knowledge and skills. More “open-ended” requirements also allow the instructor the opportunity to target misconceptions or weak areas for students. Students are given the overall requirement to complete or goal to achieve but not the specific details on how to achieve success. This presents a more real-world assessment of their preparedness for the tasks and gives them an opportunity to explore where they may need more study and practice before taking the final Skills Assessment for the course. Depending on the nature of the Skills Assessment you will provide to your students, you may want to provide more or less guidance to optimize the learning experience for your students.

A few things to keep in mind while completing this activity:

1. Do not use the browser Back button or close or reload any exam windows during the exam.

2. Do not close Packet Tracer when you are done. It will close automatically.

3. Click the Submit Assessment button in the browser window to submit your work.

# Introduction

In this assessment, you will configure devices in an IPv4/IPv6 network. For the sake of time, you will not be asked to perform all configurations on all network devices as you may be required to do in a real network or other assessment. Instead, you will use the skills and knowledge that you have learned in the labs in this course to configure the [[Router0Name]] router. In addition, you will address the hosts on two LANs with IPv4 and IPv6 addresses and activate and address the management interface of the [[Switch2Name]].

You will receive one of several topologies.

You are not required to configure the [[Switch1Name]], and you will not be able to access it in this practice skills assessment activity.

All IOS device configurations should be completed from a direct terminal connection to the device console. In addition, many values that are required to complete the configurations have not been given to you. In those cases, create the values that you need to complete the requirements. For values that have been supplied to you, they must be entered exactly as they appear in order for you to get full credit for your configuration.

You will practice and be assessed on the following skills:

* Configuration of initial IOS device settings
* Design and calculation of IPv4 addressing
* Configuration of IOS device interfaces including IPv4 and IPv6 addressing when appropriate
* Addressing of network hosts with IPv4 and IPv6 addresses
* Enhancing device security, including configuration of the secure transport protocol for remote device configuration
* Configuration of a switch management interface

Requirements by device:

[[Router0Name]] router:

* Configuration of initial router settings
* Interface configuration and IPv4 and IPv6 addressing
* Device security enhancement or device hardening
* Secure transport for remote configuration connections as covered in the labs
* Backup of the configuration file to a TFTP server

[[Switch2Name]]:

* Enabling basic remote management by Telnet
* PC and Server hosts:
* IPv4 full addressing
* IPv6 addressing

# Addressing Table

| Device | Interface | IP Address/Mask | Default Gateway |
| --- | --- | --- | --- |
| [[Router0Name]] | G0/0 |  | N/A |
| Router0 | G0/0 | 2001:db8:acad:a::1/64 | N/A |
| Router0 | G0/0 | fe80::1 | N/A |
| Router0 | G0/1 |  | N/A |
| Router0 | G0/1 | 2001:db8:acad:b::1/64 | N/A |
| Router0 | G0/1 | fe80::1 | N/A |
| [[Switch2Name]] | SVI |  |  |
| [[PC1Name]] | NIC |  |  |
| PC1 | NIC | 2001:db8:acad:a::ff/64 |  |
| [[PC2Name]] | NIC |  |  |
| PC2 | NIC | 2001:db8:acad:a::15/64 |  |
| [[PC3Name]] | NIC |  |  |
| PC3 | NIC | 2001:db8:acad:b::ff/64 |  |
| TFTP Server | NIC |  |  |
| TFTP Server | NIC | 2001:db8:acad:b::15/64 |  |

# Instructions

### Determine the IP Addressing Scheme.

Design an IPv4 addressing scheme and complete the Addressing Table based on the following requirements. Use the table to help you organize your work.

| Subnet Number | Beginning Address | Ending Address | Mask | Assignment |
| --- | --- | --- | --- | --- |
| 1 | 192.168.1.0 |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  | [[LAN1Name]] Subnet |
| 5 |  |  |  |  |
| 6 |  |  |  | [[LAN2Name]] Subnet |

* + - 1. Subnet the 192.168.1.0/24 network to provide 30 host addresses per subnet while wasting the fewest addresses.
      2. Assign the fourth subnet to the [[LAN1Name]].
      3. Assign the last network host address (the highest) in this subnet to the G0/0 interface on [[Router0Name]].
      4. Starting with the fifth subnet, subnet the network again so that the new subnets will provide 14 host addresses per subnet while wasting the fewest addresses.
      5. Assign the second of these new 14-host subnets to the [[LAN2Name]].
      6. Assign the last network host address (the highest) in the [[LAN2Name]] subnet to the G0/1 interface of the [[Router0Name]] router.
      7. Assign the second to the last address (the second highest) in this subnet to the VLAN 1 interface of the [[Switch2Name]].
      8. Configure addresses on the hosts using any of the remaining addresses in their respective subnets.

### Configure the [[Router0Name]] Router.

* + - 1. Configure the [[Router0Name]] router with all initial configurations that you have learned in the course so far:
* Configure the router hostname: **Middle**
* Protect device configurations from unauthorized access with the encrypted privileged exec password.
* Secure all access lines into the router using methods covered in the course and labs.
* Require newly-entered passwords must have a minimum length of 10 characters.
* Prevent all passwords from being viewed in clear text in device configuration files.
* Configure the router to only accept in-band management connections over the protocol that is more secure than Telnet, as was done in the labs.  Use the value **1024** for encryption key strength.
* Configure local user authentication for in-band management connections. Create a user with the name **netadmin** and a secret password of **Cisco\_CCNA5.** Give the user the highest administrative privileges. Your answer must match these values exactly.
  + - 1. Configure the two Gigabit Ethernet interfaces using the IPv4 addressing values you calculated and the IPv6 values provided in the addressing table.
* Reconfigure the link local addresses to the value shown in the table.
* Document the interfaces in the configuration file.

### **Configure the [[Switch2Name]].**

Configure [[Switch2Name]] for remote management over Telnet.

* + - 1. Use the IPv4 addressing from Step 1 and the IPv6 addressing values provided in the addressing table to configure all host PCs with the correct addressing.
      2. Use the router interface link-local address as the IPv6 default gateways on the hosts.
      3. Complete the configuration of the TFTP server using the IPv4 addressing values from Step 1 and the values in the addressing table.

Last Updated: December, 2019

ID:[[indexTopos]][[indexNames]]

***Version 1.0***

***Created in Packet Tracer 7.2.2 and Marvel 2.0.6  
All contents are Copyright © 2019 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.***

Example answer configurations:

Router0: possible labels: Town Hall, Building 1, CS Department

======================================

ena

config t

service password-encryption

!

hostname Middle

!

enable secret PT\_ccna5

!

ipv6 unicast-routing

!

username netadmin privilege 15 secret Cisco\_CCNA5

!

ip domain-name any\_domain\_name

!

interface GigabitEthernet0/0

description enter any text

ip address 192.168.1.126 255.255.255.224

ipv6 address FE80::1 link-local

ipv6 address 2001:DB8:ACAD:A::1/64

no shutdown

!

interface GigabitEthernet0/1

description enter any text

ip address 192.168.1.158 255.255.255.240

ipv6 address FE80::1 link-local

ipv6 address 2001:DB8:ACAD:B::1/64

no shutdown

!

banner motd ^C

Any banner text^C

!

line con 0

exec-timeout 5 0

login

password PT\_ccna5

!

line vty 0 4

exec-timeout 5 0

login local

transport input ssh

password PT\_ccna5

exit

security passwords min-length 10

!

-------------

Configure crypto key generate rsa with a modulus of 1024

Switch 2: Possible labels: Administration Switch, Second Floor Switch, LAB 214-A Switch

==========================================

ena

config t

interface Vlan1

ip address 192.168.1.157 255.255.255.240

no shutdown

!

ip default-gateway 192.168.1.158

!

line vty 0

password PT\_ccna5

login

Host addressing configuration:

===================================

PC1: possible labels in topology: Reception Host, Host 1, 124-1

-Click PC1, click Desktop tab, click IP Configuration, choose Static

-Enter the following:

IPv4 Address = 192.168.1.97 - 192.168.1.125 (PT will prevent the student from entering the same IP address as PC2)

IPv4 Subnet Mask = 255.255.255.224

IPv4 Default Gateway = 192.168.1.126

IPv6 Address = 2001:DB8:ACAD:A::FF

IPv6 Prefix = 64

IPv6 Default Gateway = FE80::1

PC2: possible labels in topology: Operator Host, Host 2, 124-5

-Click PC2, click Desktop tab, click IP Configuration, choose Static

-Enter the following:

IPv4 Address = 192.168.1.97 - 192.168.1.125 (PT will prevent the student from entering the same IP address as PC2)

IPv4 Subnet Mask = 255.255.255.224

IPv4 Default Gateway = 192.168.1.126

IPv6 Address = 2001:DB8:ACAD:A::15

IPv6 Prefix = 64

IPv6 Default Gateway = FE80::1

PC3: possible labels in topology: IT Host, Host 3, 214-1

-Click PC3, click Desktop tab, click IP Configuration, choose Static

-Enter the following:

IPv4 Address = 192.168.1.145 - 192.168.1.156 (PT will prevent the student from entering the same IP address as PC2)

IPv4 Subnet Mask = 255.255.255.240

IPv4 Default Gateway = 192.168.1.158

IPv6 Address = 2001:DB8:ACAD:B::FF

IPv6 Prefix = 64

IPv6 Default Gateway = FE80::1

TFTP Server: label does not vary

-Click TFTP Server, click Desktop tab, click IP Configuration, choose Static

-Enter the following:

IPv4 Address = 192.168.1.145 - 192.168.1.156 (PT will prevent the student from entering the same IP address as PC2)

IPv4 Subnet Mask = 255.255.255.240

IPv4 Default Gateway = 192.168.1.158

IPv6 Address = 2001:DB8:ACAD:B::15

IPv6 Prefix = 64

IPv6 Default Gateway = FE80::1