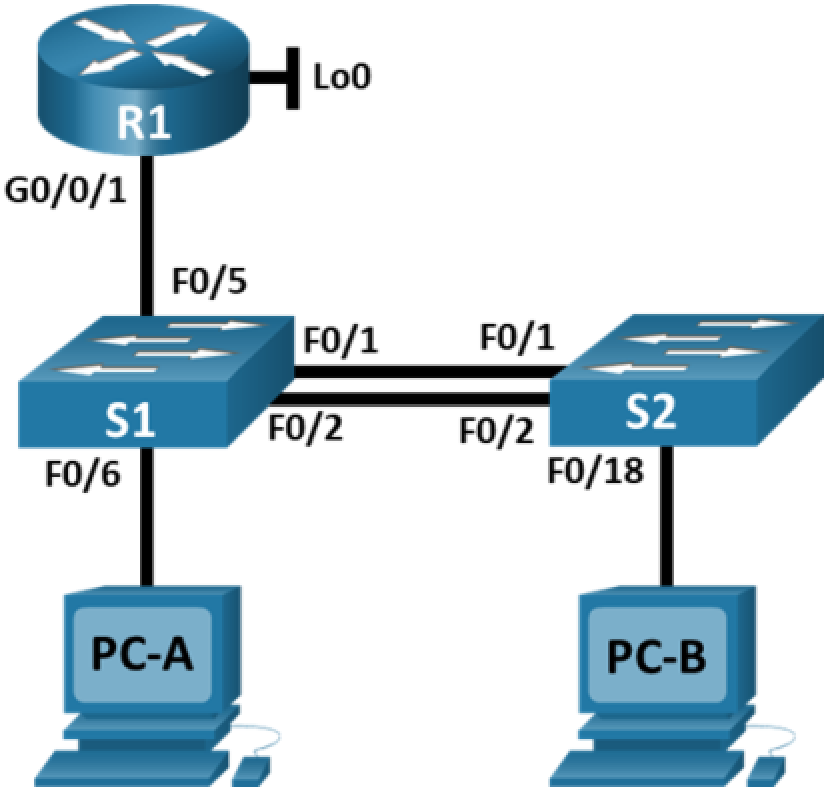
Full answers: ➔ SRWE Final PT Skills Assessment (PTSA)



VLAN Table

VLAN	Router Subinterface	VLAN Name
2	G0/0/1.2	Bikes
3	G0/0/1.3	Trikes
4	G0/0/1.4	Management
5	N/A	Parking
6	G0/0/1.6	Native

Addressing Table

Device / Interface	IP Address/Prefix/Link Local Address	Default Gateway
R1 G0/0/1.2	10.19.8.1 /26	N/A
	2001:db8:acad:a::1 /64	N/A
	fe80::1	N/A
R1 G0/0/1.3	10.19.8.65 /27	N/A
	2001:db8:acad:b::1 /64	N/A
	fe80::1	N/A
R1 G0/0/1.4	10.19.8.97 /29	N/A
	2001:db8:acad:c::1 /64	N/A
	fe80::1	N/A
R1 G0/0/1.6	N/A	N/A
R1 Loopback0	209.165.201.1 /27	N/A
	2001:db8:acad:209::1 /64	N/A
	fe80::1	N/A
S1 VLAN 4 SVI	10.19.8.98 /29	10.19.8.97
S2 VLAN 4 SVI	10.19.8.99 /29	10.19.8.97
PC-A NIC	DHCP for IPv4 address	DHCP for IPv4 default gateway
PC-A NIC	2001:db8:acad:a::50 /64	fe80::1
PC-B NIC	DHCP for IPv4 address	DHCP for IPv4 default gateway
	2001:db8:acad:b::50 /64	fe80::1

Note: There is no interface on the router that supports VLAN 5.

SRWE Final PT Skills Assessment (PTSA)

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.

Assessment Objectives

Part 1: Build the Network

Part 2: Configure Initial Device Settings

Part 3: Configure Network Infrastructure Settings (VLANs, Trunking, EtherChannel)

Part 4: Configure Host Support

Introduction

In this Packet Tracer Skills Assessment (PTSA) you will configure the devices in a small network. You must configure a router, two switches, and two PCs to support both IPv4 and IPv6 connectivity. Your router and switches must also be managed securely. You will configure inter-VLAN routing, DHCP, Etherchannel, and port-security.

All of your tasks will be performed in PT Physical Mode. You will not be able to access the logical topology for this assessment. Network devices must be configured from a direct console connection.

Instructions

Part 1: Build the Network

a. Move the required devices into the equipment rack.

b. Place the PCs on the table.

c. Connect the devices according to the topology diagram.

Part 2: Configure Initial Device Settings

All IOS device configuration must be made through a direct console connections.

Step 1: Configure R1 Basic Settings and Device Hardening

a. Configure basic settings.

1) Prevent the router from attempting to resolve incorrectly entered commands as domain names.
2) Configure the R1 hostname.
3) Configure an appropriate MOTD banner.

b. Configure password security.

1) Configure the console password and enable connections.
2) Configure an enable secret password.
3) Encrypt all clear text passwords.
4) Set the minimum length of newly created passwords to 10 characters.

c. Configure SSH.

1) Create an administrative user in the local user database.
   - Username: **admin**
   - Encrypted Password: **admin1pass**
2) Configure the domain name as **ccna-ptsa.com**
3) Create an RSA crypto key with a modulus of **1024** bits.
4) Ensure that more secure version of SSH will be used.
5) Configure the vty lines to authenticate logins against the local user database.
6) Configure the vty lines to only accept connections over SSH.

Step 2: Configure router interfaces.

a. Configure R1 with a loopback interface. Configure the loopback0 with IPv4 and IPv6 addressing according to the addressing table.

b. Configure Router Subinterfaces

1) Prepare the router to be configured with IPv6 addresses on its interfaces.

2) Use the information in the Addressing Table and VLAN Table to configure subinterfaces on R1:

- Interfaces should be configured with IPv4 and IPv6 addressing.
- All addressed interfaces should use **fe80::1** as the link local address.
- Use the VLAN table to assign VLAN membership to the subinterfaces.

3) Be sure to configure the native VLAN interface.

4) Configure descriptions for **all** interfaces.

Step 3: Configure S1 and S2 with Basic Settings and Device Hardening.

Configuration tasks for the switches S1 and S2 include the following:

a. Â Configure Basic Settings on S1 and S2

1) Prevent the switches from attempting to resolve incorrectly entered commands as domain names.int

2) Configure the S1 or S2 hostname.

3) Configure an appropriate MOTD banner on both switches.

b. Configure Device Hardening on S1 and S2

1) Configure the console password and enable connections.

2) Configure an enable secret password.

3) Encrypt all clear text passwords.

c. Configure SSH on S1 and S2

1) Create an administrative user in the local user database.

- Username: **admin**
- Password: **admin1pass**

2) Configure the domain name as **ccna-ptsa.com**

3) Create an RSA crypto key with a modulus of **1024** bits.

4) Ensure that more secure version of SSH will be used.

5) Configure the vty lines to authenticate logins against the local user database.

6) Configure the vty lines to accept connections over SSH only.

Step 4: Configure SVIs on S1 and S2

Configure the SVI on both switches.

a. Use the information in the Addressing Table to configure SVIs on S1 and S2 for the Management VLAN.

b. Configure the switch so that the SVI can be reached from other networks over the Management VLAN.

Part 3: Configure Network Infrastructure Settings (VLANs, Trunking, EtherChannel)

On S1 and S2, Configure the following.

Step 1: Configure VLANs and Trunking.

a. Create the VLANs according to the VLAN table.

b. Create 802.1Q VLAN trunks on ports **F0/1** and **F0/2.** On **S1**, **F0/5** should also be configured as a trunk. Use **VLAN 6** as the native VLAN.

Step 2: Configure Etherchannel.

Create Layer 2 EtherChannel port group 1 that uses interfaces **F0/1** and **F0/2** on **S1 and S2**. Both ends of the channel should negotiate the LACP link.

Step 3: Configure Switchports.

a. On **S1**, configure the port that is connected to the host with static access mode in **VLAN 2**.

b. On **S2**, configure the port that is connected to the host with static access mode in **VLAN 3**.

c. Configure port security on the S1 and S2 active access ports to accept only three learned MAC addresses.

d. Assign **all** unused switch ports to VLAN 5 on both switches and shut down the ports.

e. Configure a description on the unused ports that is relevant to their status.

Part 4: Configure Host Support

Step 1: Configure Default Routing on R1

a. Configure an IPv4 default route that uses the Lo0 interface as the exit interface.

b. Configure an IPv6 default route that uses the Lo0 interface as the exit interface.

Step 2: Configure IPv4 DHCP for VLAN 2

a. Â On R1, create a DHCP pool called **CCNA-A** that consists of the last 10 host addresses in the **VLAN 2** subnet only.

b. Configure the correct default gateway address in the pool.

c. Configure the domain name of **ccna-a.net**.

Step 3: Configure IPv4 DHCP for VLAN 3

a. On R1, create a DHCP pool called CCNA-B that consists of the last 10 host addresses in the VLAN 3 subnet only.

b. Configure the correct default gateway address in the pool.

c. Configure the domain name of **ccna-b.net**.

Step 4: Configure host computers.

a. Configure the host computers to use DHCP for IPv4 addressing.

b. Statically assign the IPv6 GUA and default gateway addresses using the values in the Addressing Table.

Last Updated: January 2021

Version 1.0

Created in Packet Tracer 8.0 and Marvel 2.0.7