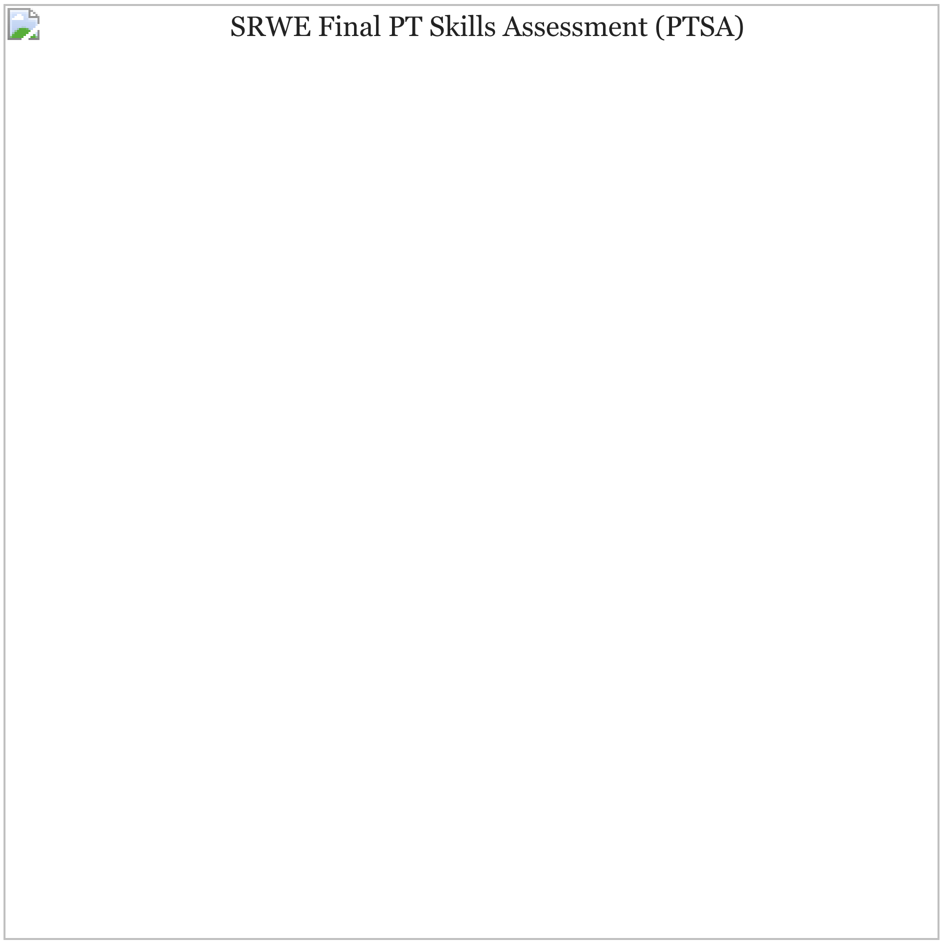
SRWE (Version 7.00) Final PT Skills Assessment Exam (PTSA) Answers

itexamanswers.net/srwe-version-7-00-final-pt-skills-assessment-exam-ptsa-answers.html

December 21, 2019

CCNA 2 SRWE Final PT Skills Assessment (PTSA)

Topology



Topology – 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

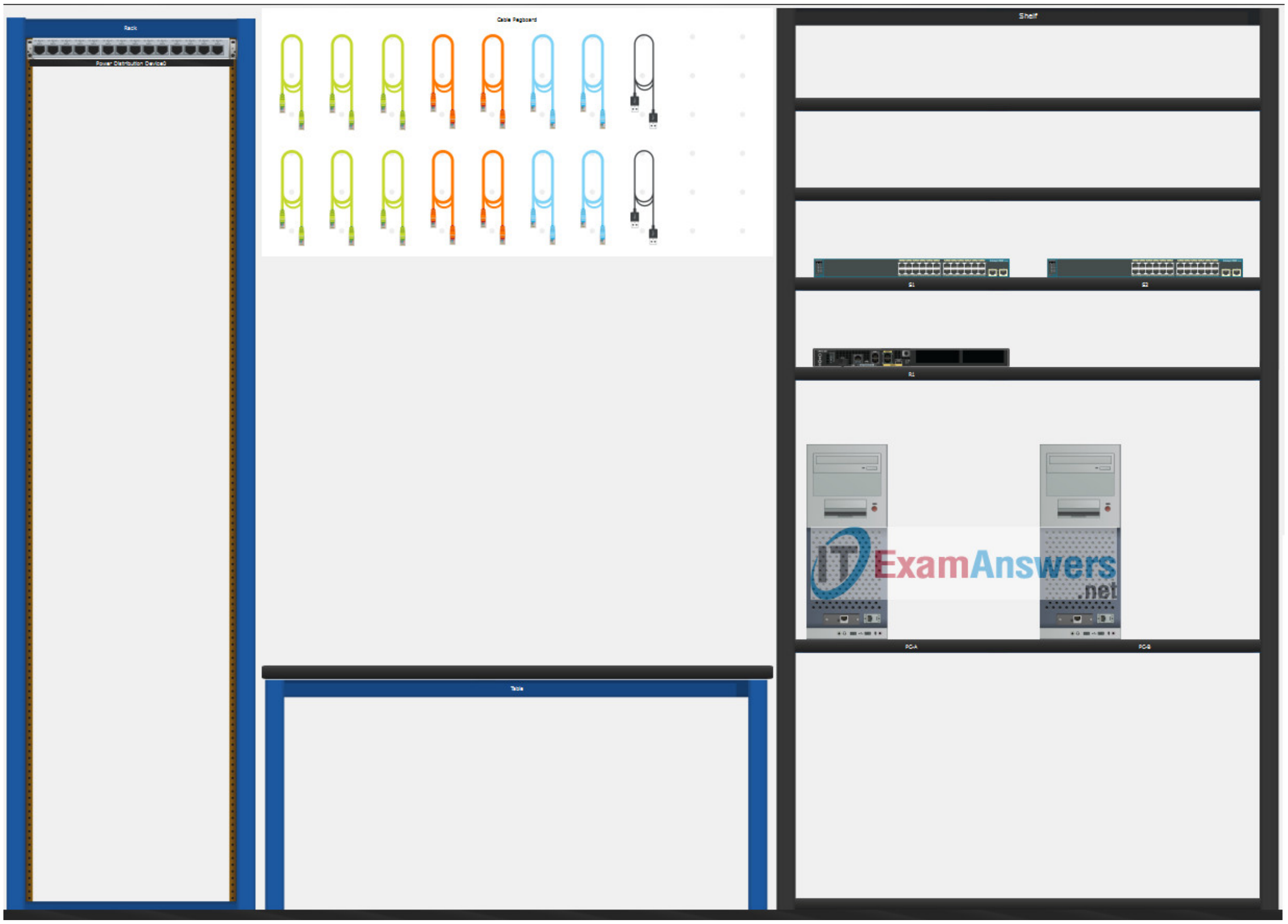
VLAN	Router Subinterface	VLAN Name
5	N/A	Parking
6	G0/0/1.6	Native

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
	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)



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

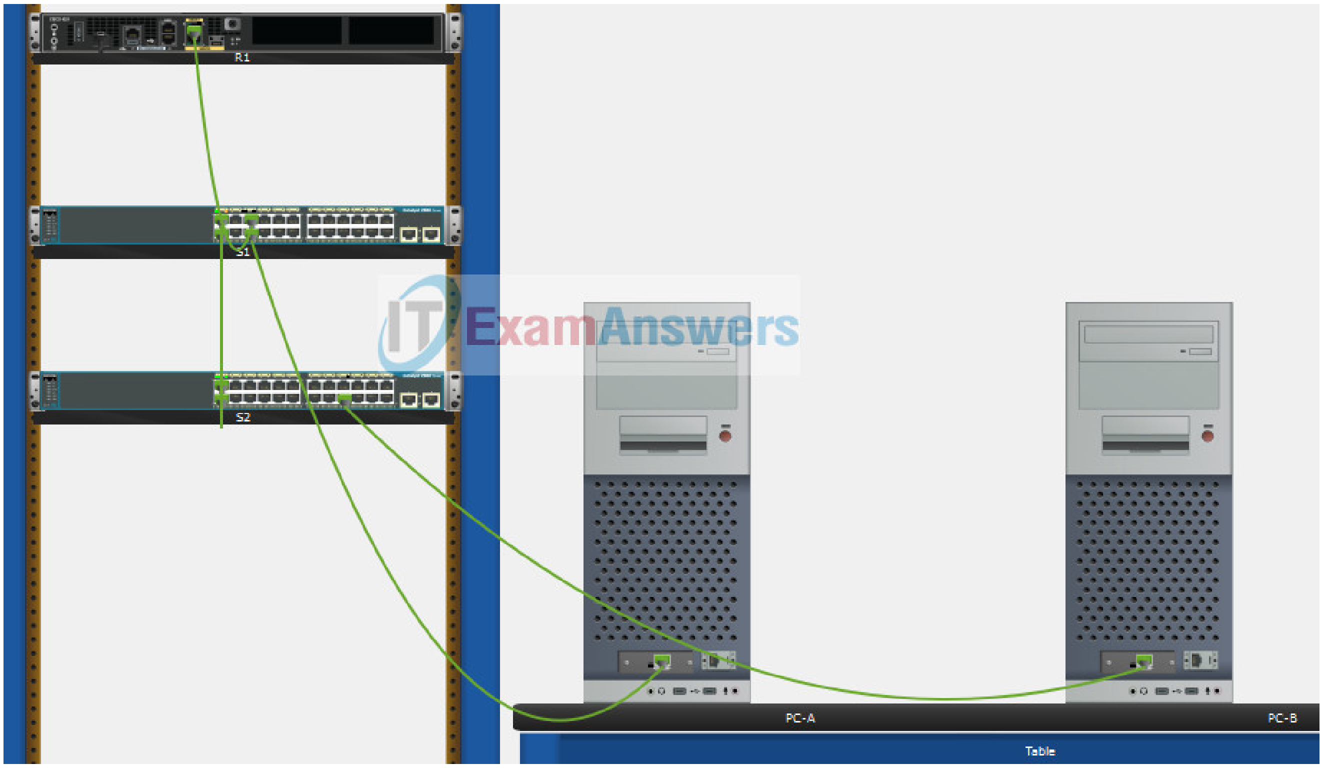
In this Packet Tracer Skills Assessment (PTSA) you will configure the devices in a small network. You must configure a router, two switches, and two PCs to support both IPv4 and IPv6 connectivity. Your router and switches must also be managed securely. You will configure inter-VLAN routing, DHCP, Etherchannel,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

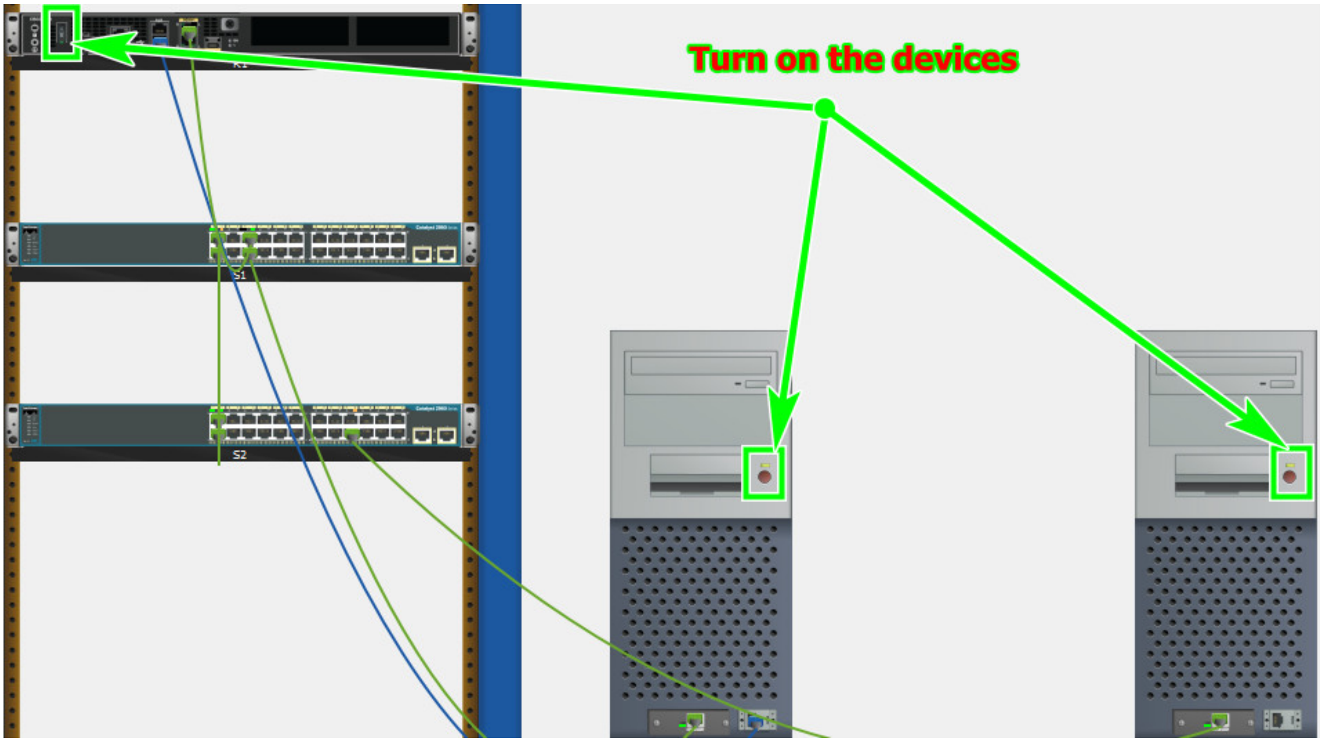
- **Use Copper Straight-Through cable to connect all devices**



IT ExamAnswers

SRWE Final PT Skills Assessment (PTSA)

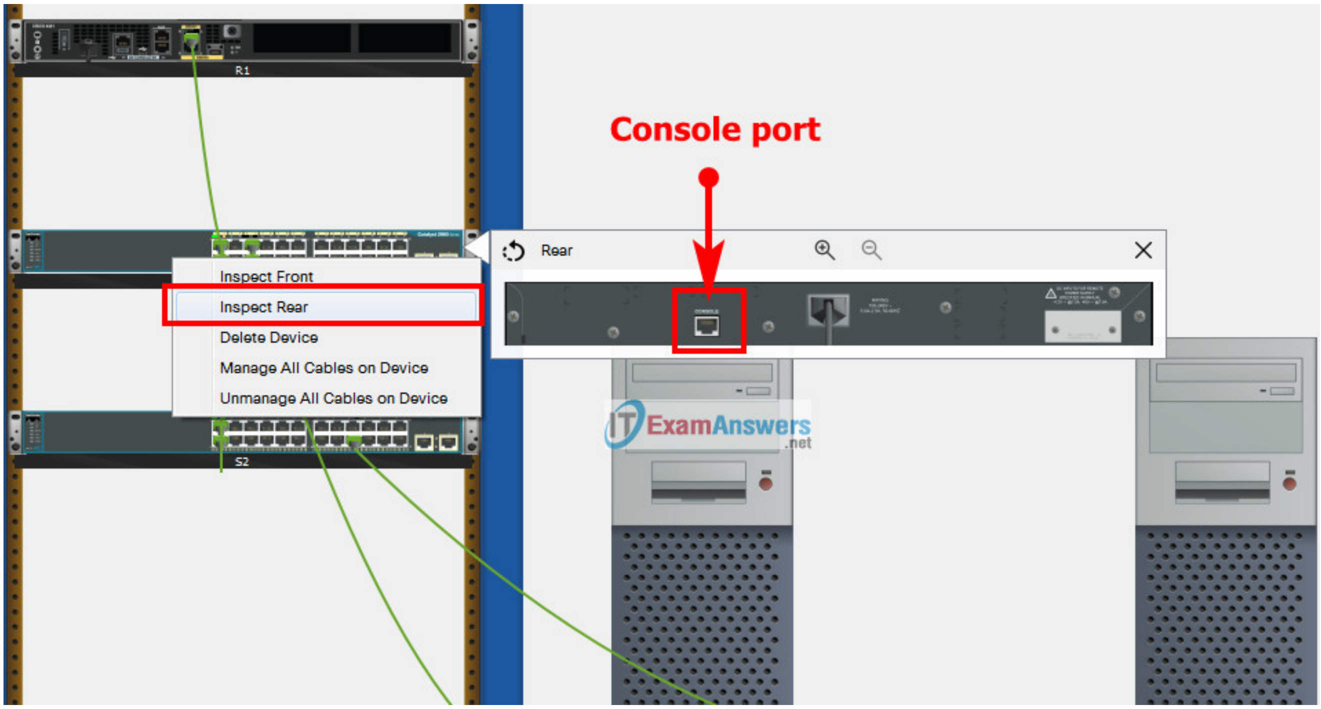
Turn on the devices PCs and Router



Part 2: Configure Initial Device Settings

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

To show Console port on Switch, **Right click** Switch –> **Inspect Rear** –> **Console port**



SRWE Final PT Skills Assessment (PTSA)

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.

```
Router(config)#no ip domain lookup
Router(config)#hostname R1
R1(config)#banner motd #Unauthorized Acess is Prohibited#
```

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.

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit

R1(config)#enable secret ciscoenpass

R1(config)#service password-encryption

R1(config)#security passwords min-length 10
```

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.

```
R1(config)#username admin secret admin1pass

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

R1(config)#crypto key generate rsa
1024

R1(config)#ip ssh version 2

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

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.

```
R1(config-subif)#interface Loopback 0
R1(config-subif)#description Loopback
R1(config-subif)#ip address 209.165.201.1 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:209::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
```

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.

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

R1(config)#interface g0/0/1.2
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#description Bikes
R1(config-subif)#ip address 10.19.8.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local

R1(config-subif)#interface g0/0/1.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#description Trikes
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local

R1(config-subif)#interface g0/0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#description Management
R1(config-subif)#ip address 10.19.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local

R1(config-subif)#interface g0/0/1.6
R1(config-subif)#encapsulation dot1Q 6 native
R1(config-subif)#description Native

R1(config)#interface g0/0/1
R1(config-if)#no shutdown
```

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

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

```
Switch1(config)#no ip domain lookup
Switch1(config)#hostname S1
S1(config)#banner motd #Unauthorized Access is Prohibitted!#

Switch2(config)#no ip domain lookup
Switch2(config)#hostname S2
S2(config)#banner motd #Unauthorized Access is Prohibitted!#
```

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.

```
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit

S1(config)#enable secret ciscoenpass

S1(config)#service password-encryption

S2(config)#line console 0
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit

S2(config)#enable secret ciscoenpass

S2(config)#service password-encryption
```

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.

```
S1(config)#username admin secret admin1pass

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

S1(config)#crypto key generate rsa
1024

S1(config)#ip ssh version 2

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

S2(config)#username admin secret admin1pass

S2(config)#ip domain name ccna-ptsa.com

S2(config)#crypto key generate rsa
1024

S2(config)#ip ssh version 2

S2(config)#line vty 0 15
S2(config-line)#login local
S2(config-line)#transport input ssh
S2(config-line)#exit
```

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.

```
S1(config)#interface vlan 4
S1(config-if)#ip address 10.19.8.98 255.255.255.248
S1(config-if)#description Management Interface
S1(config-if)#no shutdown
S1(config-if)#exit

S1(config)#ip default-gateway 10.19.8.97

S2(config)#interface vlan 4
S2(config-if)#ip address 10.19.8.99 255.255.255.248
S2(config-if)#description Management Interface
S2(config-if)#no shutdown
S2(config-if)#exit

S2(config)#ip default-gateway 10.19.8.97
```

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.

```
S1(config)#vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native

S1(config)#interface range f0/1-2
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 6
S1(config-if-range)#switchport trunk allowed vlan 2, 3, 4, 5, 6
S1(config-if-range)#exit

S1(config)#interface f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2, 3, 4, 5, 6
S1(config-if)#exit

S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#vlan 4
S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native

S2(config)#interface range f0/1-2
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 6
S2(config-if-range)#switchport trunk allowed vlan 2, 3, 4, 5, 6
S2(config-if-range)#exit
```

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.

```
S1(config)#interface range f0/1-2
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#interface port-channel 1
S1(config-if-range)#exit
```

```
S2(config)#interface range f0/1-2
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#interface port-channel 1
S2(config-if-range)#exit
```

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.

```
S1(config)#interface f0/6
S1(config-if)#description host
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3

S1(config)#interface range f0/3-4, f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Unused Interfaces
S1(config-if-range)#shutdown

S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport port-security
S2(config-if)#switchport access vlan 3
S2(config-if)#switchport port-security maximum 3

S2(config)#interface range f0/3-17, f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Unused Interfaces
S2(config-if-range)#shutdown
```

Part 4: Configure Host Support

Step 1: Configure Default Routing on R1

Use Console cable to re-conntect PC and Router, enter password **ciscoconpass** and **ciscoenpass** to login router

- 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.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
R1(config)#ipv6 route ::/0 loopback 0
```

Step 2: Configure IPv4 DHCP for VLAN 2

- a. 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.

```
R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#ip dhcp pool CCNA-A
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#exit
```

Step 3: Configure IPv4 DHCP for VLAN 3

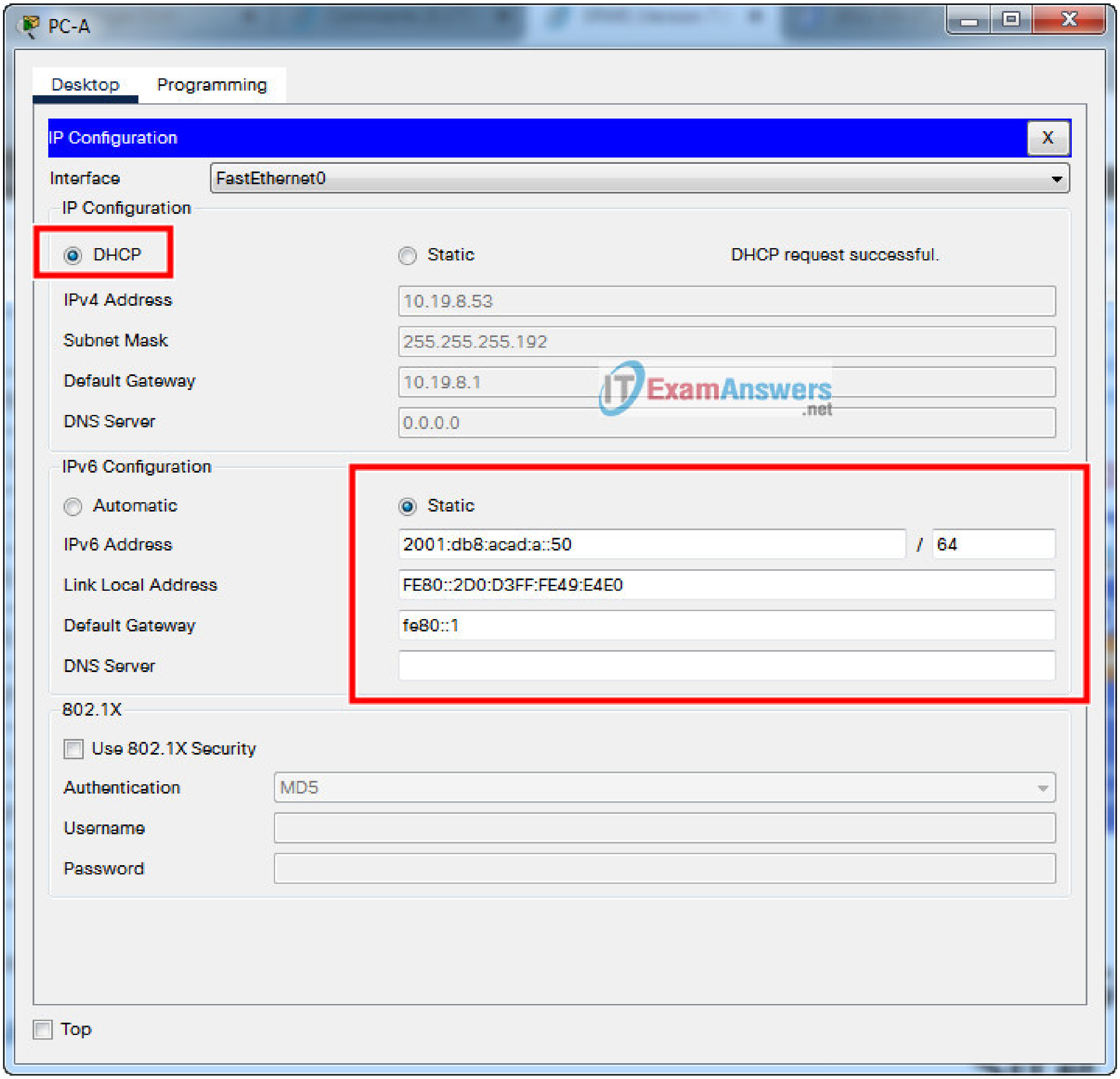
- a. On R1, create a DHCP pool called **CCNA-B** that consists of the last 10 host addresses in the VLAN 3 subnet only.
- b. Configure the correct default gateway address in the pool.
- c. Configure the domain name of ccna-b.net.

```
R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
R1(config)#ip dhcp pool CCNA-B
R1(dhcp-config)#network 10.19.8.64 255.255.255.224
R1(dhcp-config)#default-router 10.19.8.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#exit
```

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.

- PC-A
- PC-B



IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 10.19.8.53

Subnet Mask: 255.255.255.192

Default Gateway: 10.19.8.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: 2001:db8:acad:a::50 / 64

Link Local Address: FE80::2D0:D3FF:FE49:E4E0

Default Gateway: fe80::1

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

ITExamAnswers.net

Configure host computer A

Script answers key:

Router R1

```
enable
configure terminal

no ip domain lookup
hostname R1
banner motd #Unauthorized Acess is Prohibited#

line console 0
password ciscoconpass
login
exit

enable secret ciscoenpass
service password-encryption
security passwords min-length 10

username admin secret admin1pass
ip domain name ccna-ptsa.com
crypto key generate rsa
1024

ip ssh version 2

line vty 0 15
login local
transport input ssh
exit

interface Loopback 0
description Loopback
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:db8:acad:209::1/64
ipv6 address fe80::1 link-local
exit

ipv6 unicast-routing
interface g0/0/1.2
encapsulation dot1Q 2
description Bikes
ip address 10.19.8.1 255.255.255.192
ipv6 address 2001:db8:acad:a::1/64
ipv6 address fe80::1 link-local

interface g0/0/1.3
encapsulation dot1Q 3
description Trikes
ip address 10.19.8.65 255.255.255.224
ipv6 address 2001:db8:acad:b::1/64
ipv6 address fe80::1 link-local

interface g0/0/1.4
encapsulation dot1Q 4
```

```
description Management
ip address 10.19.8.97 255.255.255.248
ipv6 address 2001:db8:acad:c::1/64
ipv6 address fe80::1 link-local

interface g0/0/1.6
encapsulation dot1Q 6 native
description Native

interface g0/0/1
no shutdown
exit

ip route 0.0.0.0 0.0.0.0 loopback 0

ipv6 route ::/0 loopback 0

ip dhcp excluded-address 10.19.8.1 10.19.8.52
ip dhcp pool CCNA-A
network 10.19.8.0 255.255.255.192
default-router 10.19.8.1
domain-name ccna-a.net
exit

ip dhcp excluded-address 10.19.8.65 10.19.8.84
ip dhcp pool CCNA-B
network 10.19.8.64 255.255.255.224
default-router 10.19.8.65
domain-name ccna-b.net
exit
```

Switch S1

```
enable
configure terminal

no ip domain lookup
hostname S1
banner motd #Unauthorized Access is Prohibitted!#
line console 0
password ciscoconpass
login
exit
enable secret ciscoenpass
service password-encryption
username admin secret admin1pass
ip domain name ccna-ptsa.com
crypto key generate rsa
1024

ip ssh version 2

line vty 0 15
login local
transport input ssh
exit

interface vlan 4
ip address 10.19.8.98 255.255.255.248
description Management Interface
no shutdown
exit
ip default-gateway 10.19.8.97

vlan 2
name Bikes
vlan 3
name Trikes
vlan 4

name Management
vlan 5
name Parking
vlan 6
name Native

interface range f0/1-2
switchport mode trunk
switchport trunk native vlan 6
switchport trunk allowed vlan 2, 3, 4, 5, 6
exit

interface f0/5
switchport mode trunk
switchport trunk native vlan 6
switchport trunk allowed vlan 2, 3, 4, 5, 6
exit
interface range f0/1-2
channel-group 1 mode active
interface port-channel 1
exit

interface f0/6
description host
switchport mode access
switchport access vlan 2
switchport port-security
switchport port-security maximum 3

interface range f0/3-4, f0/7-24, g0/1-2
switchport mode access
switchport access vlan 5
description Unused Interfaces
shutdown
```

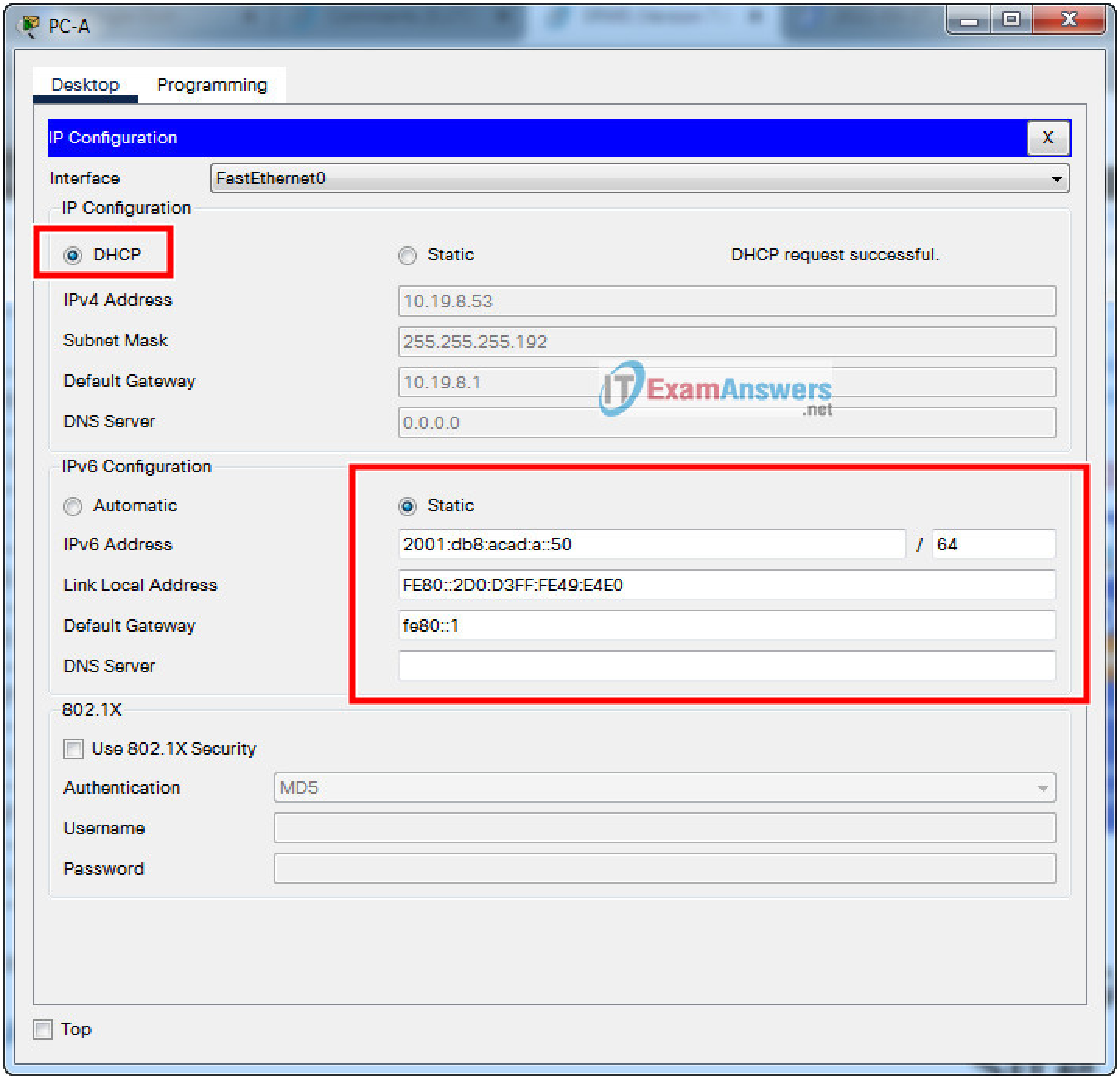
Switch S2:

```
enable
configure terminal
no ip domain lookup
hostname S2
banner motd #Unauthorized Access is Prohibitted!#

line console 0
password ciscoconpass
login
exit

enable secret ciscoenpass
service password-encryption

username admin secret admin1pass
ip domain name ccna-ptsa.com
crypto key generate rsa
1024
ip ssh version 2
line vty 0 15
login local
transport input ssh
exit
interface vlan 4

ip address 10.19.8.99 255.255.255.248
description Management Interface
no shutdown
exit
ip default-gateway 10.19.8.97

vlan 2
name Bikes
vlan 3
name Trikes
vlan 4
name Management
vlan 5
name Parking
vlan 6
name Native

interface range f0/1-2
switchport mode trunk
switchport trunk native vlan 6
switchport trunk allowed vlan 2, 3, 4, 5, 6
exit
interface range f0/1-2
channel-group 1 mode active
interface port-channel 1
exit
interface f0/18
```

```
switchport mode access
switchport access vlan 3
switchport port-security
switchport port-security maximum 3
interface range f0/3-17, f0/19-24, g0/1-2
switchport mode access
switchport access vlan 5
description Unused Interfaces
shutdown
```

Configure PC-A & PC-B

- PC-A
- PC-B



IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 10.19.8.53

Subnet Mask: 255.255.255.192

Default Gateway: 10.19.8.1

DNS Server: 0.0.0.0

IT ExamAnswers .net

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: 2001:db8:acad:a::50 / 64

Link Local Address: FE80::2D0:D3FF:FE49:E4E0

Default Gateway: fe80::1

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

□ Top

Configure host computer A

Download PDF + Packet Tracer files

[sociallocker id=”57850″]

SRWE Final PT Skills Assessment .PDF file 189.17 KB 9444 downloads

…

Download

[/sociallocker]