Free Questions for 200-301 by dumpssheet

Shared by Klein on 29-01-2024

For More Free Questions and Preparation Resources

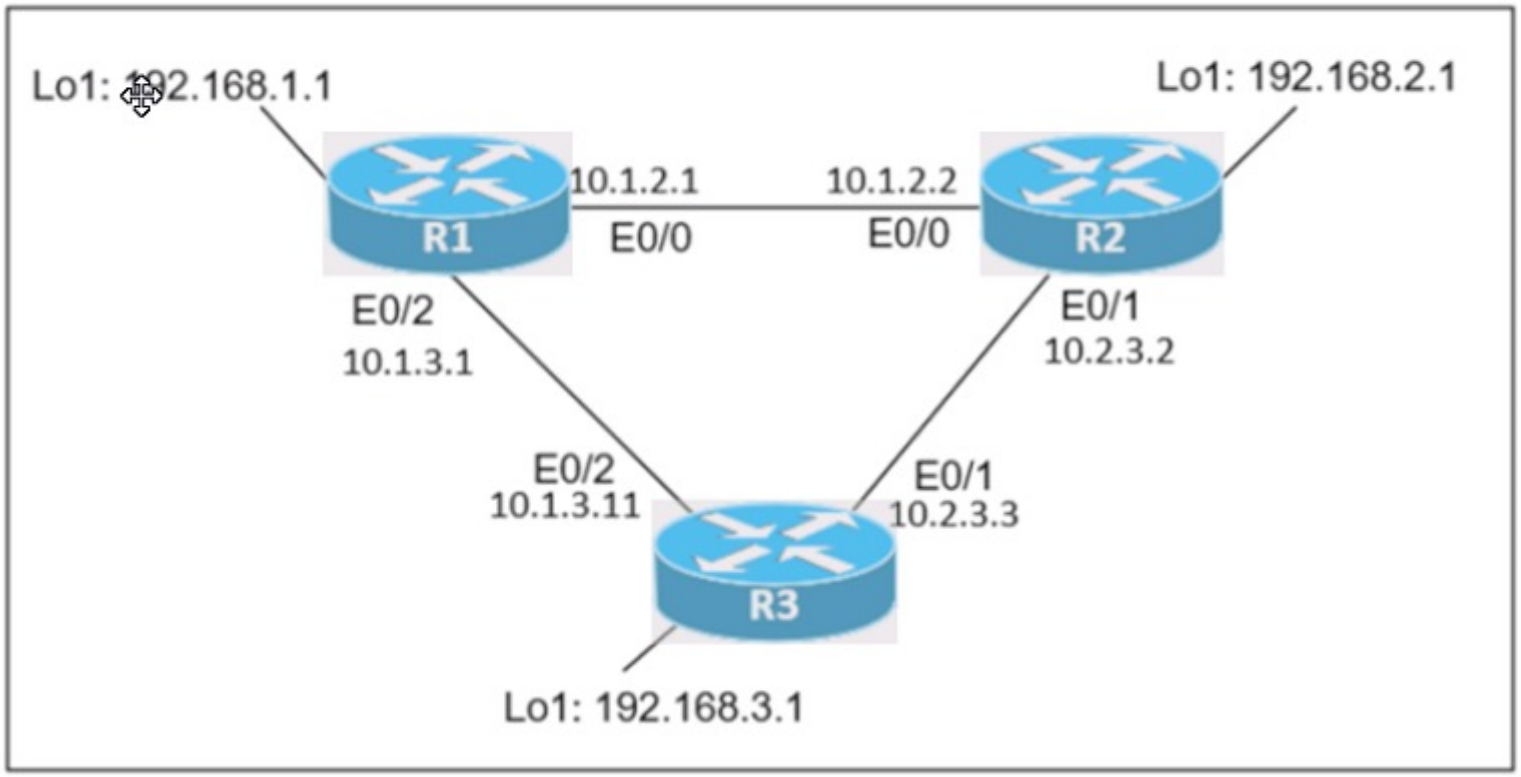
Check the Links on Last Page

Question 1

Question Type: MultipleChoice

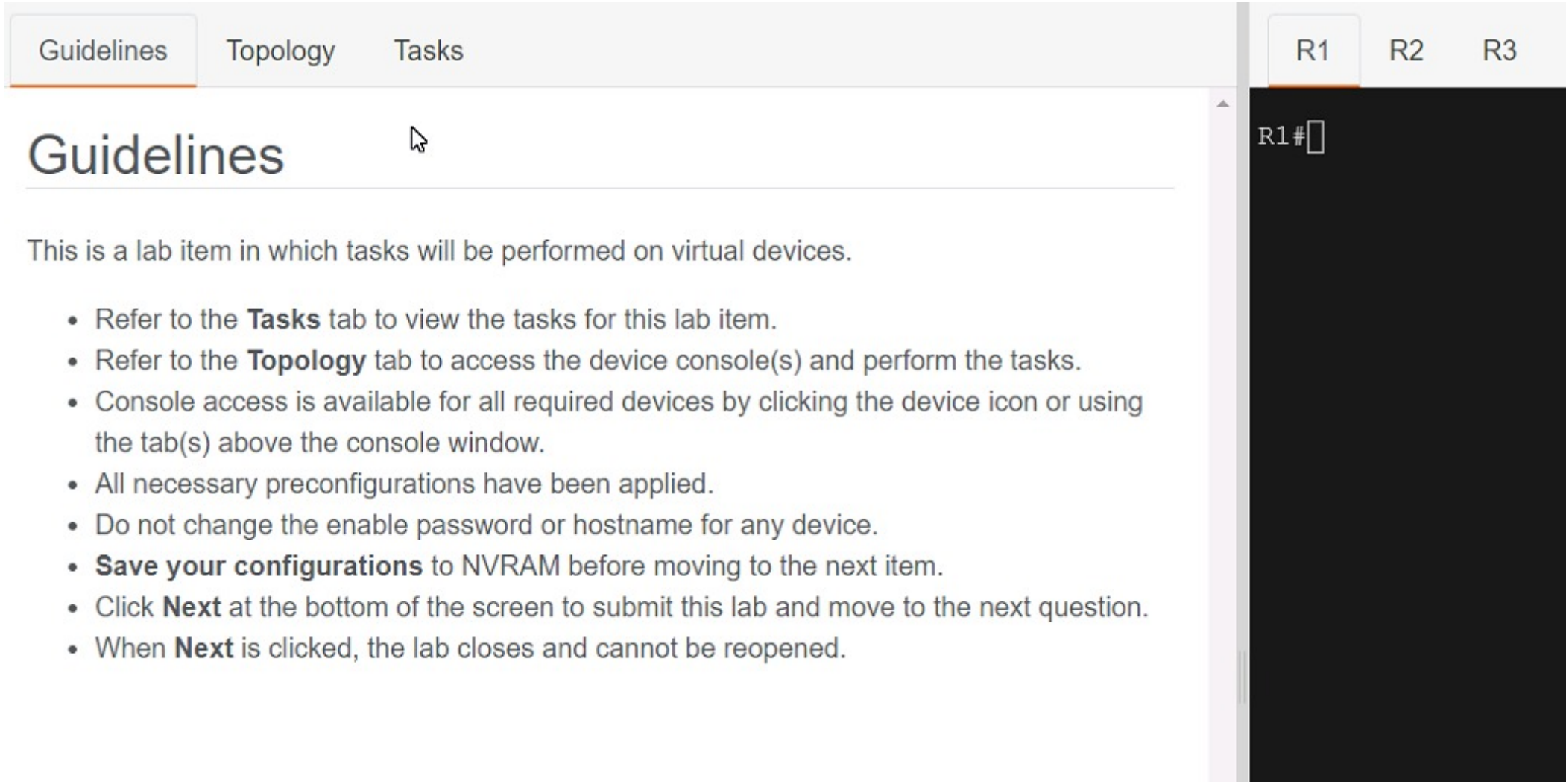
Refer to the exhibit.

Guidelines | Topology | Tasks



R1 | R2 | R3

```
R1#
```



Connectivity between three routers has been established, and IP services must be configured jn the order presented to complete the implementation Tasks assigned include configuration of NAT, NTP, DHCP, and SSH services.

1. All traffic sent from R3 to the R1 Loopback address must be configured for NAT on R2. All source addresses must be translated from R3 to the IP address of Ethernet0/0 on R2, while using only a standard access list named NAT To verify, a ping must be successful to the R1 Loopback address sourced from R3. Do not use NVI NAT configuration.

2. Configure R1 as an NTP server and R2 as a client, not as a peer, using the IP address of the R1 Ethernet0/2 interface. Set the clock on the NTP server for midnight on January 1, 2019.

3. Configure R1 as a DHCP server for the network 10.1.3.0/24 in a pool named TEST. Using a single command, exclude addresses 1-10 from the range. Interface Ethernet0/2 on R3 must be issued the IP address of 10.1.3.11 via DHCP.

4. Configure SSH connectivity from R1 to R3, while excluding access via other remote connection protocols. Access for user root and password Cisco must be set on router R3 using RSA and 1024 bits. Verify connectivity using an SSH session from router R1 using a destination address of 10.1.3.11. Do NOT modify console access or line numbers to accomplish this task.

Options:

A- See the Explanation below

Answer:

A

Explanation:

Answer as below configuration:

conf t

R1(config)#ntp master 1

R2(config)#ntp server 10.1.2.1

Exit

Router#clock set 00:00:00 jan 1 2019

ip dhcp pool TEST

network 10.1.3.0 255.255.255.0

ip dhcp exluded-address 10.1.3.1 10.1.3.10

R3(config)#int e0/3

R3(config)#int e0/2

ip address dhcp

no shut

crypto key generate RSA

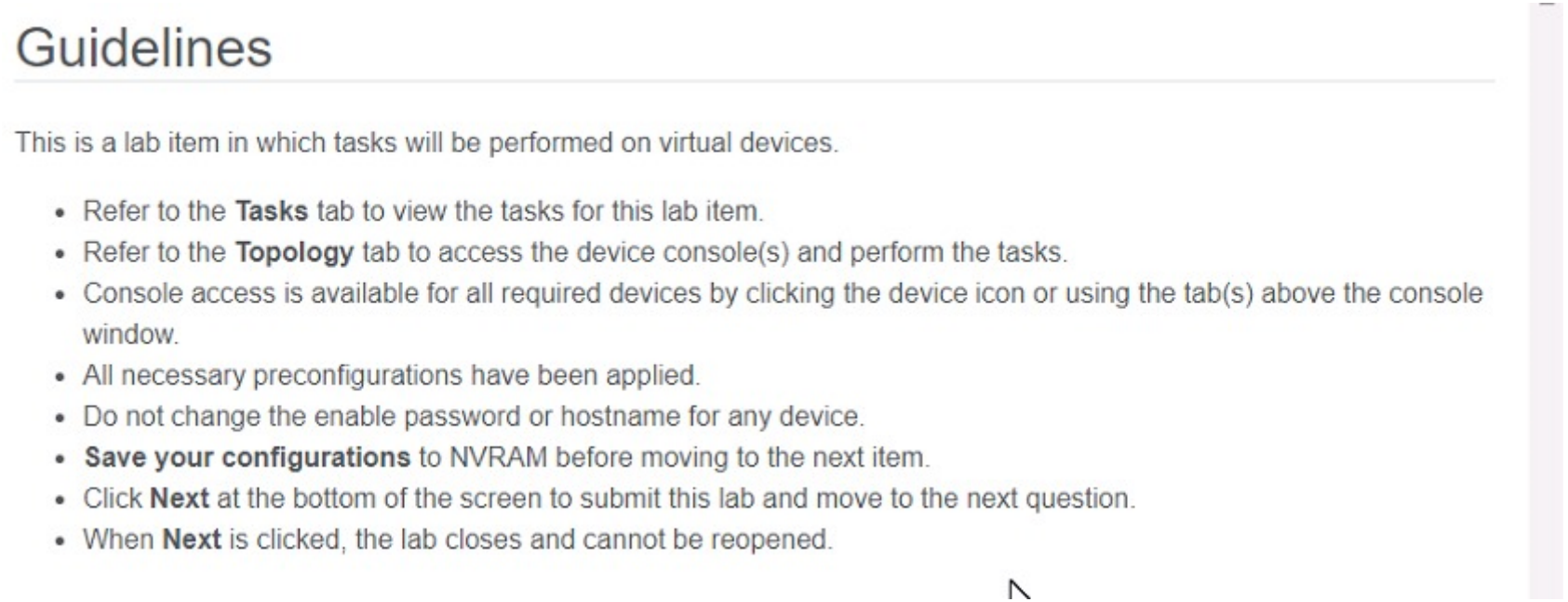
1024

Copy run start

Question 2

Question Type: **MultipleChoice**

Refer to the exhibit.



Three switches must be configured for Layer 2 connectivity. The company requires only the designated VLANs to be configured on their respective switches and permitted accross any links between switches for security purposes. Do not modify or delete VTP configurations.

The network needs two user-defined VLANs configured:

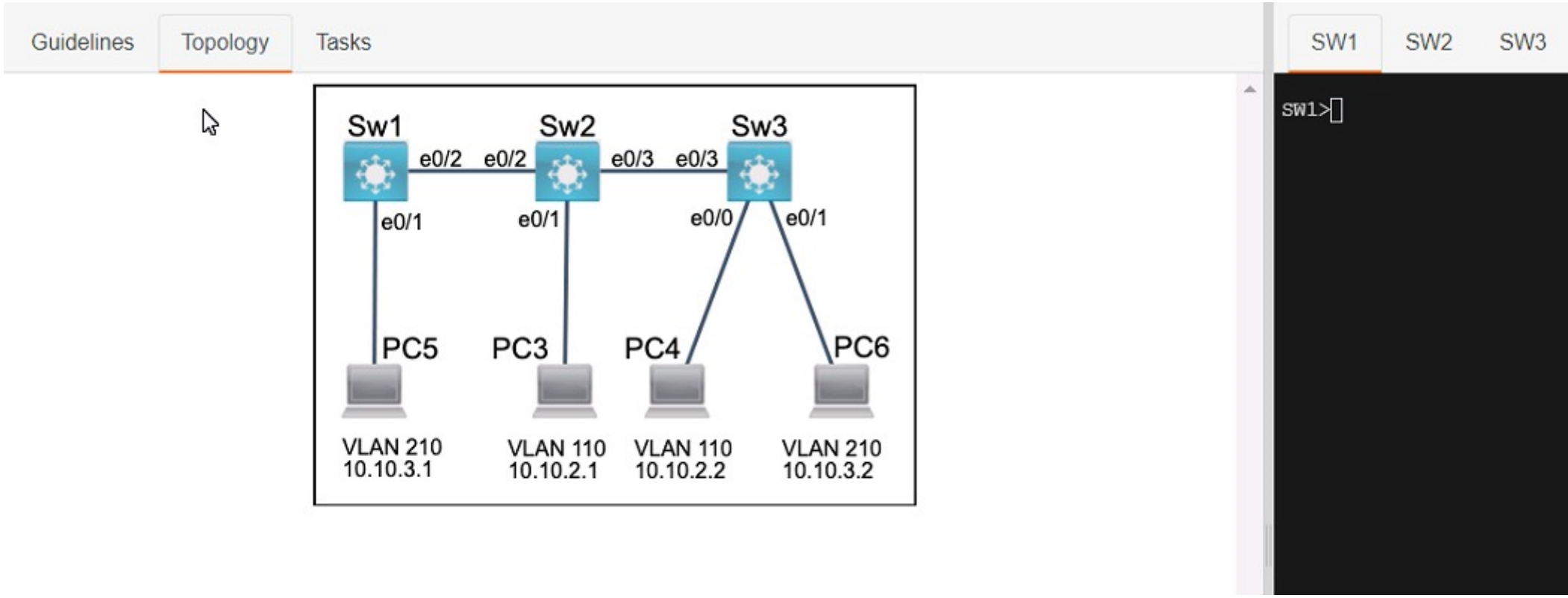
VLAN 110: MARKETING

VLAN 210: FINANCE

1. Configure the VLANs on the designated switches and assign them as access ports to the interfaces connected to the PCs.

2. Configure the e0/2 interfaces on Sw1 and Sw2 as 802.1q trunks with only the required VLANs permitted.

3. Configure the e0/3 interfaces on Sw2 and Sw3 as 802.1q trunks with only the required VLANs permitted.



Options:

A- See the Explanation below

Answer:

A

Explanation:

Answer as below configuration:

Sw1

enbale

config t

Vlan 210

Name FINANCE

Inter e0/1

Switchport access vlan 210

do wr

Sw2

Enable

config t

Vlan 110

Name MARKITING

Int e0/1

Switchport acees vlan 110

do wr

Sw3

Enable

config t

Vlan 110

Name MARKITING

Vlan 210

Name FINANCE

Int e0/0

Switchport access vlan 110

Int e0/1

Switchport access vlan 210

Sw1

Int e0/1

Switchport allowed vlan 210

Sw2

Int e0/2

Switchport trunk allowed vlan 210

Sw3

Int e0/3

Switchport trunk allowed vlan 210

Switchport trunk allowed vlan 210,110

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit.

Guidelines

This is a lab item in which tasks will be performed on virtual devices.

- Refer to the **Tasks** tab to view the tasks for this lab item.
- Refer to the **Topology** tab to access the device console(s) and perform the tasks.
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
- All necessary preconfigurations have been applied.
- Do not change the enable password or hostname for any device.
- **Save your configurations** to NVRAM before moving to the next item.
- Click **Next** at the bottom of the screen to submit this lab and move to the next question.
- When **Next** is clicked, the lab closes and cannot be reopened.

All physical cabling between the two switches is installed. Configure the network connectivity between the switches using the designated VLANs and interfaces.

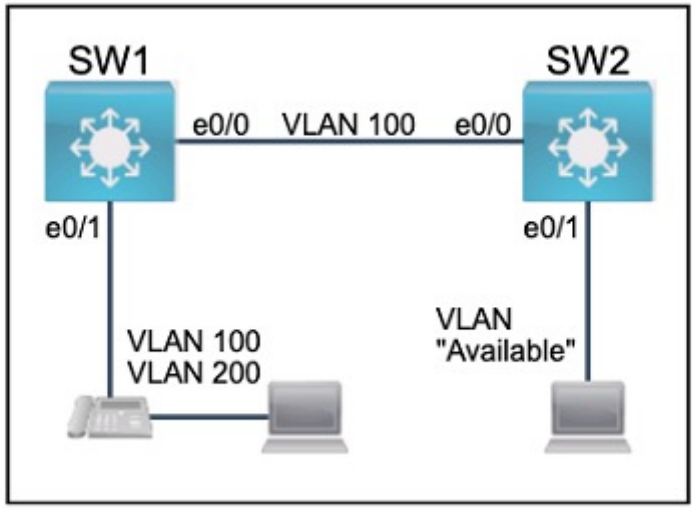
1. Configure VLAN 100 named Compute and VLAN 200 named Telephony where required for each task.

2. Configure Ethernet0/1 on SW2 to use the existing VLAN named Available.

3. Configure the connection between the switches using access ports.

4. Configure Ethernet0/1 on SW1 using data and voice VLANs.

5. Configure Ethemet0/1 on SW2 so that the Cisco proprietary neighbor discovery protocol is turned off for the designated interface only.



Options:

A- See the Explanation below

Answer:

A

Explanation:

Answer as below configuration:

on sw1

enable

conf t

vlan 100

name Compute

vlan 200

name Telephony

int e0/1

switchport voice vlan 200

switchport access vlan 100

int e0/0

switchport mode access

do wr

on sw2

Vlan 99

Name Available

Int e0/1

Switchport access vlan 99

do wr

Question 4

Question Type: **MultipleChoice**

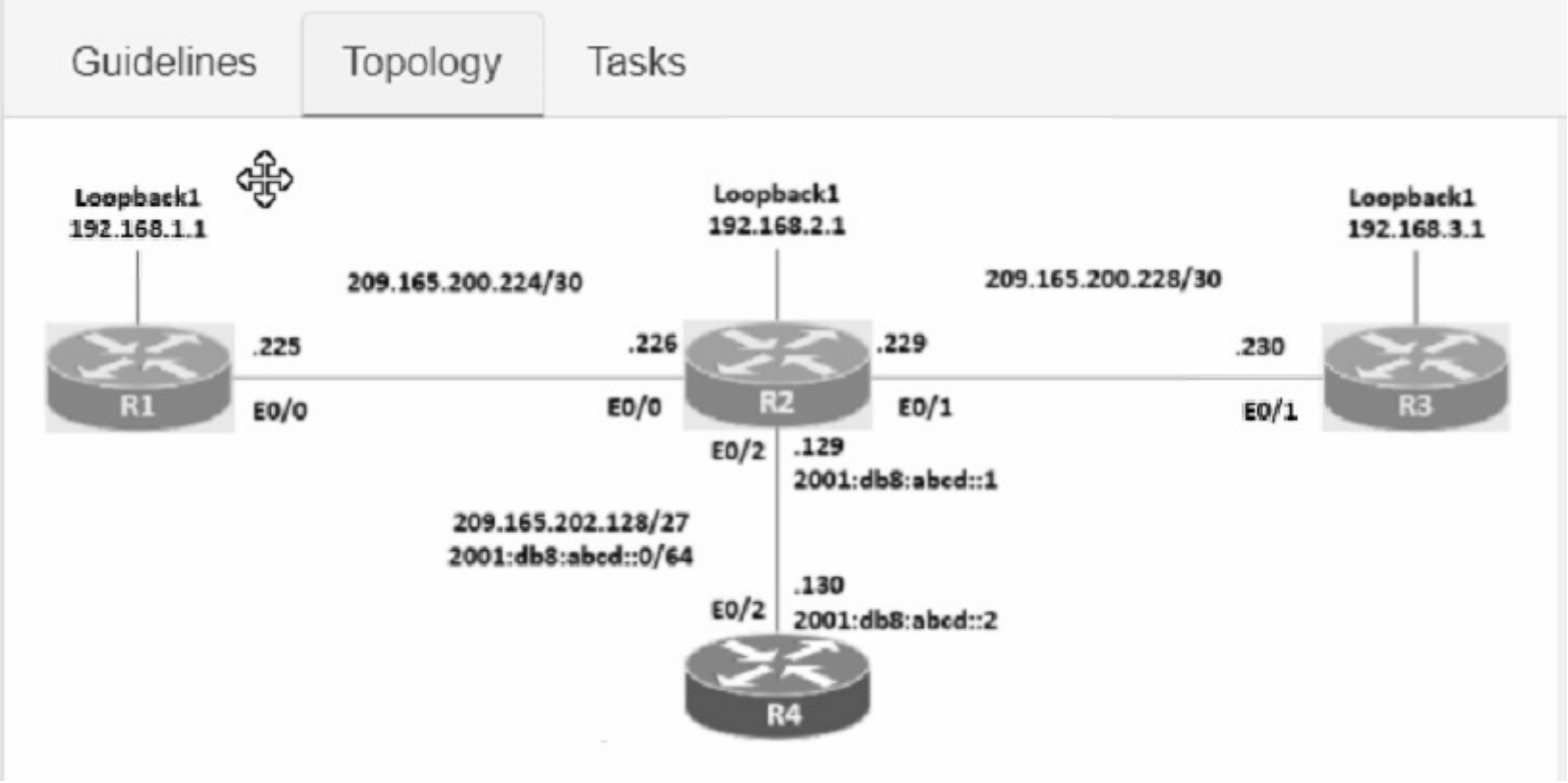
Refer to the exhibit.

Connectivity between four routers has been established. IP connectivity must be configured in the order presented to complete the implementation. No dynamic routing protocols are included.

1. Configure static routing using host routes to establish connectivity from router R3 to the router R1 Loopback address using the source IP of 209.165.200.230.

2. Configure an IPv4 default route on router R2 destined for router R4.

3. Configure an IPv6 default router on router R2 destined for router R4.



Options:

A- See the Explanation below

Answer:

A

Explanation:

Answer as below configuration:

1.- on R3

config terminal

ip route 192.168.1.1 255.255.255.255 209.165.200.229

end

copy running start

2.- on R2

config terminal

ip route 0.0.0.0 0.0.0.0 209.165.202.130

end

copy running start

3.- on R2

config terminal

ipv6 route ::/0 2001:db8:abcd::2

end

copy running start

Question 5

Question Type: **MultipleChoice**

Refer to the exhibit.

Configure IPv4 and IPv6 connectivity between two routers. For IPv4, use a /28 network from the 192.168.1.0/24 private range. For IPv6, use the first /64 subnet from the 2001:0db8:aaaa::/48 subnet.

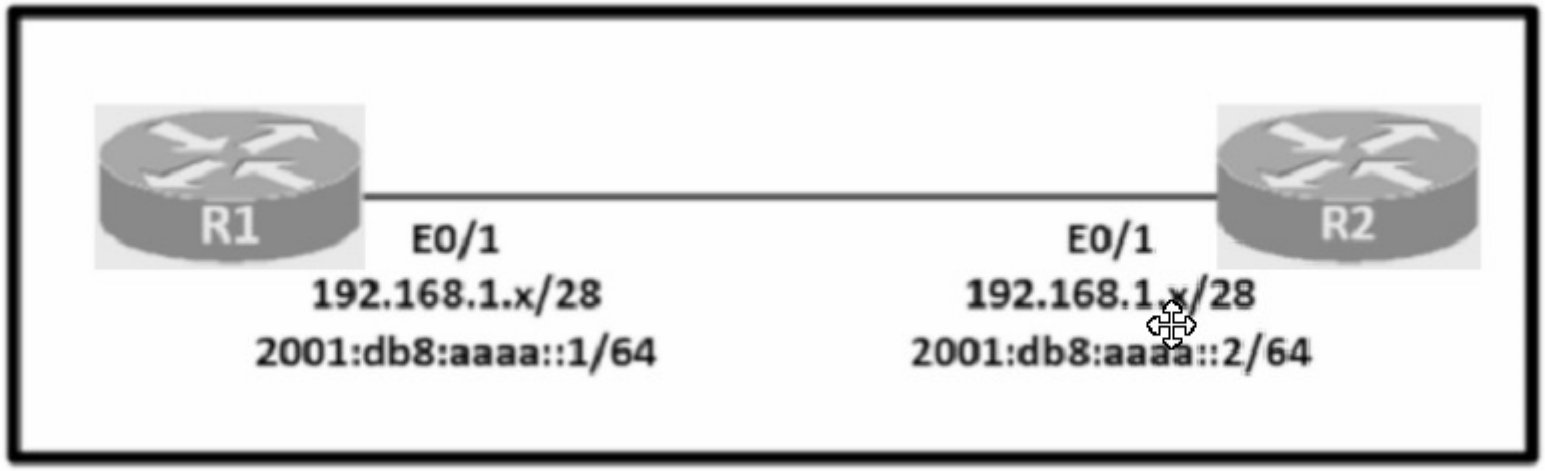
1. Using Ethernet0/1 on routers R1 and R2, configure the next usable/28 from the 192.168.1.0/24 range. The network 192.168.1.0/28 is unavailable.

2. For the IPv4 /28 subnet, router R1 must be configured with the first usable host address.

3. For the IPv4 /28 subnet, router R2 must be configured with the last usable host address.

4. For the IPv6 /64 subnet, configure the routers with the IP addressing provided from the topology.

5. A ping must work between the routers on the IPv4 and IPv6 address ranges.



Options:

A- See the Explanation below

Answer:

A

Explanation:

Answer as below configuration:

on R1

config terminal

ipv6 unicast-routing

inter eth0/1

ip addre 192.168.1.1 255.255.255.240

ipv6 addre 2001:db8:aaaa::1/64

not shut

end

copy running start

on R2

config terminal

ipv6 unicast-routing

inter eth0/1

ip address 192.168.1.14 255.255.255.240

ipv6 address 2001:db8:aaaa::2/64

not shut

end

copy running start

---

for test from R1

ping ipv6 2001:db8:aaaa::1

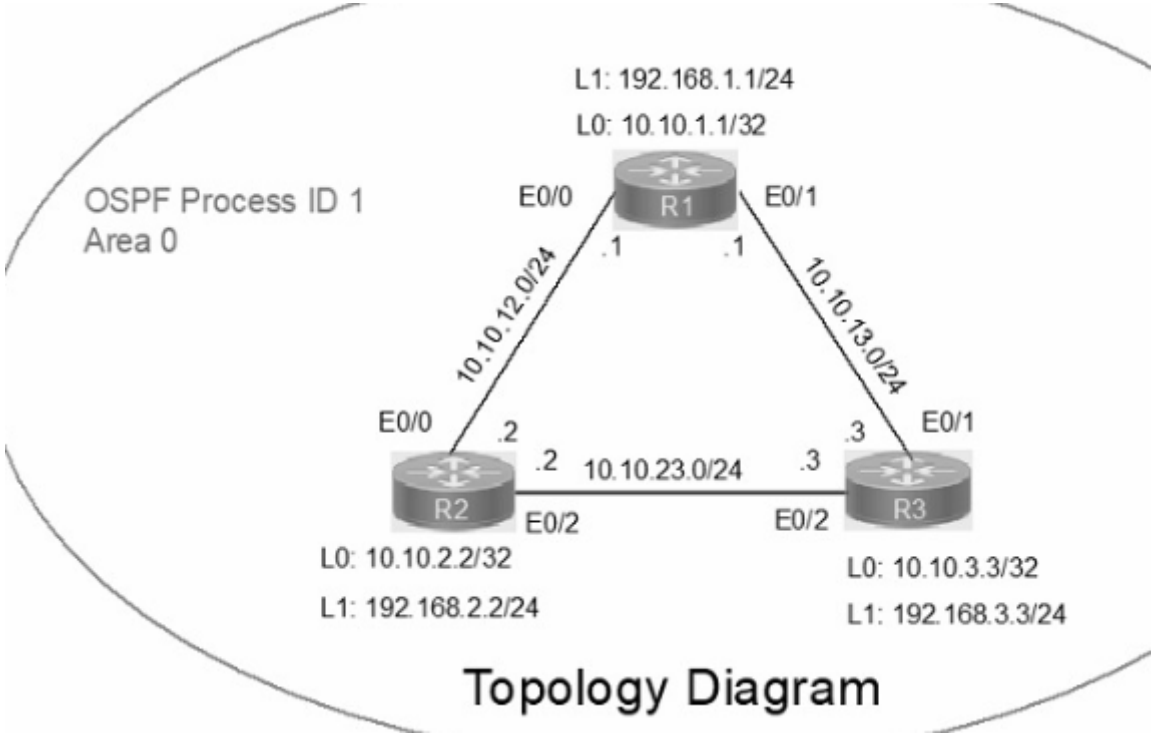
for test from R2

ping ipv6 2001:db8:aaaa::2

Question 6

Question Type: **MultipleChoice**

Refer to the exhibit.


L1: 192.168.1.1/24
L0: 10.10.1.1/32
OSPF Process ID 1
Area 0
E0/0
R1
E0/1
.1
.1
10.10.12.0/24
10.10.13.0/24
E0/0
.2
E0/1
.3
.2
10.10.23.0/24
.3
R2
E0/2
E0/2
R3
L0: 10.10.2.2/32
L1: 192.168.2.2/24
L0: 10.10.3.3/32
L1: 192.168.3.3/24
Topology Diagram

Guidelines

This is a lab item in which tasks will be performed on virtual devices.

- Refer to the **Tasks** tab to view the tasks for this lab item.
- Refer to the **Topology** tab to access the device console(s) and perform the tasks.
- Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
- All necessary preconfigurations have been applied.
- Do not change the enable password or hostname for any device.
- **Save your configurations** to NVRAM before moving to the next item.
- Click **Next** at the bottom of the screen to submit this lab and move to the next question.
- When **Next** is clicked, the lab closes and cannot be reopened.

IP connectivity between the three routers is configured. OSPF adjacencies must be established.

1. Configure R1 and R2 Router IDs using the interface IP addresses from the link that is shared between them.

2. Configure the R2 links with a max value facing R1 and R3. R2 must become the DR. R1 and R3 links facing R2 must remain with the default OSPF configuration for DR election. Verify the configuration after clearing the OSPF process.

3. Using a host wildcard mask, configure all three routers to advertise their respective Loopback1 networks.

4. Configure the link between R1 and R3 to disable their ability to add other OSPF routers.

Options:

A- See the Explanation below

Answer:

A

Explanation:

Answer as below configuration:

on R1

conf terminal

interface Loopback0

ip address 10.10.1.1 255.255.255.255

!

interface Loopback1

ip address 192.168.1.1 255.255.255.0

!

```
interface Ethernet0/0
no shut
ip address 10.10.12.1 255.255.255.0
ip ospf 1 area 0
duplex auto
!
interface Ethernet0/1
no shut
ip address 10.10.13.1 255.255.255.0
ip ospf 1 area 0
duplex auto
!
router ospf 1
router-id 10.10.12.1
network 10.10.1.1 0.0.0.0 area 0
```

network 192.168.1.0 0.0.0.255 area 0

!

copy run star

On R2

conf terminal

interface Loopback0

ip address 10.10.2.2 255.255.255.255

!

interface Loopback1

ip address 192.168.2.2 255.255.255.0

!

interface Ethernet0/0

no shut

ip address 10.10.12.2 255.255.255.0

```
ip ospf priority 255
ip ospf 1 area 0
duplex auto
!
interface Ethernet0/2
no shut
ip address 10.10.23.2 255.255.255.0
ip ospf priority 255
ip ospf 1 area 0
duplex auto
!
router ospf 1
network 10.10.2.2 0.0.0.0 area 0
network 192.168.2.0 0.0.0.255 area 0
!
```

copy runs start

On R3

conf ter

interface Loopback0

ip address 10.10.3.3 255.255.255.255

!

interface Loopback1

ip address 192.168.3.3 255.255.255.0

!

interface Ethernet0/1

no shut

ip address 10.10.13.3 255.255.255.0

ip ospf 1 area 0

duplex auto

```
!
interface Ethernet0/2
no shut
ip address 10.10.23.3 255.255.255.0
ip ospf 1 area 0
duplex auto
!
router ospf 1
network 10.10.3.3 0.0.0.0 area 0
network 192.168.3.0 0.0.0.255 area 0
!
copy run start
!
```

Question 7

Question Type: MultipleChoice

An on-site service desk technician must verify the IP address and DNS server information on a users Windows computer. Which command must the technician enter at the command prompt on the user's computer?

Options:

A- ipconfig /all

B- ifconfig -a

C- show interface

D- netstat -r

Answer:

A

Explanation:

The ipconfig /all command displays the configuration information of all the network adapters on a Windows computer, including the IP address, subnet mask, default gateway, and DNS server information12. This command can help troubleshoot network connectivity and DNS resolution issues.

Topic 5, Simulations / Lab

Question 8

Question Type: MultipleChoice

What is the operating mode and role of a backup port on a shared LAN segment in Rapid PVST+?

Options:

A- forwarding mode and provides the lowest-cost path to the root bridge for each VLAN

B- learning mode and provides the shortest path toward the root bridge handling traffic away from the LAN

C- blocking mode and provides an alternate path toward the designated bridge

D- listening mode and provides an alternate path toward the root bridge

Answer:

C

Question 9

Question Type: MultipleChoice

What does WPA3 provide in wireless networking?

Options:

A- safeguards against brute force attacks with SAE

B- optional Protected Management Frame negotiation

C- backward compatibility with WPAand WPA2

D- increased security and requirement of a complex configuration

Answer:

A

Explanation:

https://www.swascan.com/wi-fi-security/

Question 10

Question Type: MultipleChoice

It work security team noticed that an increasing number of employees are becoming victims of phishing attacks. Which security program should be implemented to mitigate the problem?

Options:

A- email system patches

B- physical access control

C- software firewall enabled on all PCs

D- user awareness training

Answer:

D

Question 11

Question Type: MultipleChoice

What are two functions of DHCP servers? (Choose two.)

Options:

A- prevent users from assigning their own IP addresses to hosts

B- assign dynamic IP configurations to hosts in a network

C- support centralized IP management

D- issue DHCPDISCOVER messages when added to the network

E- respond to client DHCPOFFER requests by issuing an IP address

Answer:

B, C

Question 12

Question Type: **MultipleChoice**

How does IPsec provide secure networking for applications within an organization?

Options:

A- It takes advantage of FTP to secure file transfers between nodes on the network.

B- It provides GRE tunnels to transmit traffic securely between network nodes.

C- It enables sets of security associations between peers.

D- It leverages TFTP providing secure file transfers among peers on the network.

Answer:

C

Explanation:

IPsec (Internet Protocol Security) is a protocol suite that provides secure communication over Internet Protocol (IP) networks. It achieves this by authenticating and encrypting each IP packet within a communication session. One of the key concepts in IPsec is the establishment of security associations (SAs) between peers. Security associations are the combination of algorithms and keys used to secure communication between two devices. They define the security parameters for the communication, including the encryption algorithm, integrity algorithm, and keying information. By establishing these security associations, IPsec ensures confidentiality, integrity, and authenticity of the data being transmitted between network nodes.