Free Questions for 200-301 by braindumpscollection

Shared by Grimes on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Physical connectivity is implemented between the two Layer 2 switches,

and the network connectivity between them must be configured.

I . Configure an LACP EtherChanneI and number it as 44; configure it

between switches SWI and SW2 using interfaces EthernetO/O and

Ethernet0/1 on both sides. The LACP mode must match on both ends.

2. Configure the EtherChanneI as a trunk link.

3. Configure the trunk link with 802. Iq tags.

4. Configure VLAN 'MONITORING' as the untagged VLAN of the

EtherChannel.

==========

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.

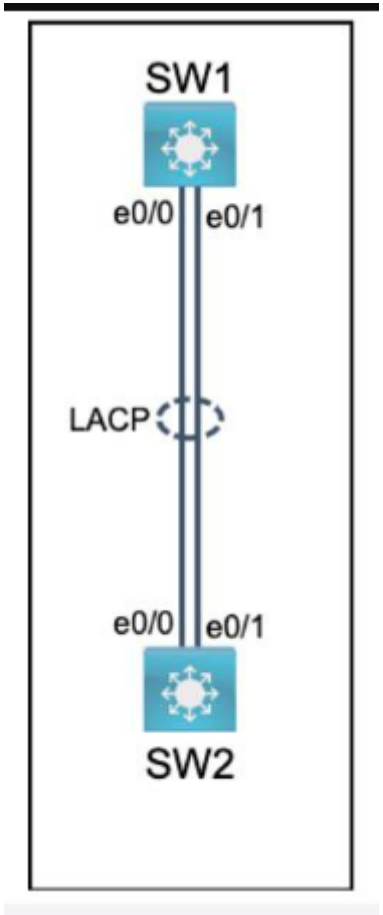
* All necessary preconfigurations have been applied.

* 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.



Options:

A- Solution is given below explanation

Answer:

A

Explanation:

To configure an LACP EtherChannel and number it as 44, configure it between switches SW1 and SW2 using interfaces Ethernet0/0 and Ethernet0/1 on both sides, configure the EtherChannel as a trunk link, configure the trunk link with 802.1q tags, and configure VLAN 'MONITORING' as the untagged VLAN of the EtherChannel, you need to follow these steps:

On both SW1 and SW2, enter the global configuration mode by using the configure terminal command.

On both SW1 and SW2, select the two interfaces that will form the EtherChannel by using the interface range ethernet 0/0 - 1 command. This will enter the interface range configuration mode.

On both SW1 and SW2, set the protocol to LACP by using the channel-protocol lacp command.

On both SW1 and SW2, assign the interfaces to an EtherChannel group number 44 by using the channel-group 44 mode active command. This will create a logical interface named Port-channel44 and set the LACP mode to active on both ends. The LACP mode must match on both ends for the EtherChannel to form.

On both SW1 and SW2, exit the interface range configuration mode by using the exit command.

On both SW1 and SW2, enter the Port-channel interface configuration mode by using the interface port-channel 44 command.

On both SW1 and SW2, configure the Port-channel interface as a trunk link by using the switchport mode trunk command.

On both SW1 and SW2, configure the Port-channel interface to use 802.1q tags for VLAN identification by using the switchport trunk encapsulation dot1q command.

On both SW1 and SW2, configure VLAN 'MONITORING' as the untagged VLAN of the Port-channel interface by using the switchport trunk native vlan MONITORING command.

On both SW1 and SW2, exit the Port-channel interface configuration mode by using the exit command.

On both SW1 and SW2, save the configuration to NVRAM by using the copy running-config startup-config command.

Question 2

Question Type: **MultipleChoice**

All physical cabling is in place. Router R4 and PCI are fully configured and

inaccessible. R4's WAN interfaces use .4 in the last octet for each subnet.

Configurations should ensure that connectivity is established end-to-end.

1 . Configure static routing to ensure RI prefers the path through R2 to

reach only PCI on R4's LAN

2. Configure static routing that ensures traffic sourced from RI will take

an alternate path through R3 to PCI in the event of an outage along

the primary path

3. Configure default routes on RI and R3 to the Internet using the least number of hops

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.

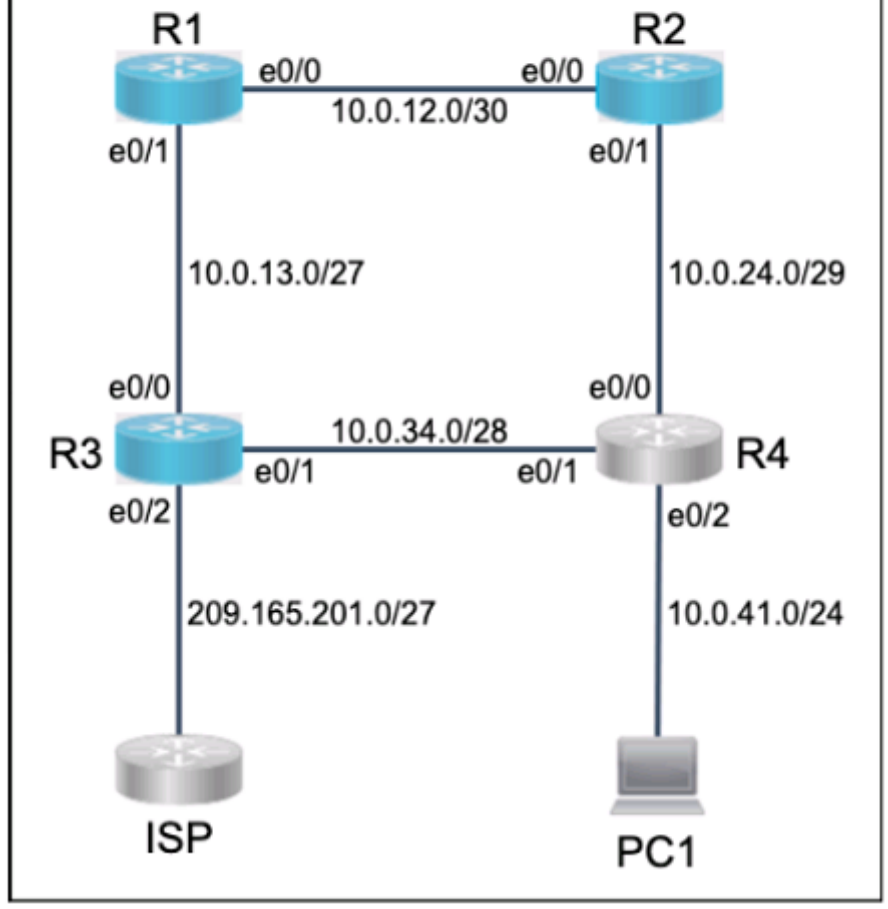
* Do not change the enable password or hostname for any device.

* 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.

Device	Interface	IP Address
R3	e0/2	209.165.201.3
ISP	e0/0	209.165.201.1
PC1	e0/0	10.0.41.10



Options:

A- See the solution below in Explanation

Answer:

A

Explanation:

To configure static routing on R1 to ensure that it prefers the path through R2 to reach only PC1 on R4's LAN, you need to create a static route for the host 10.0.0.100/8 with a next-hop address of 20.0.0.2, which is the IP address of R2's interface connected to R1. You also need to assign a lower administrative distance (AD) to this route than the default AD of 1 for static routes, so that it has a higher preference over other possible routes. For example, you can use an AD of 10 for this route. To create this static route, you need to enter the following commands on R1's console:

R1#configure terminal R1(config)#ip route 10.0.0.100 255.0.0.0 20.0.0.2 10 R1(config)#end

To configure static routing on R1 that ensures that traffic sourced from R1 will take an alternate path through R3 to PC1 in the event of an outage along the primary path, you need to create another static route for the host 10.0.0.100/8 with a next-hop address of 40.0.0.2, which is the IP address of R3's interface connected to R1. You also need to assign a higher AD to this route than the AD of the primary route, so that it has a lower preference and acts as a backup route. For example, you can use an AD of 20 for this route. This type of static route is also known as a floating static route. To create this static route, you need to enter the following commands on R1's console:

R1#configure terminal R1(config)#ip route 10.0.0.100 255.0.0.0 40.0.0.2 20 R1(config)#end

To configure default routes on R1 and R3 to the Internet using the least number of hops, you need to create a static route for the network 0.0.0.0/0 with a next-hop address of the ISP's interface connected to each router respectively. A default route is a special type of static route that matches any destination address and is used when no other specific route is available. The ISP's interface connected to R1 has an IP address of 10.0.0.4, and the ISP's interface connected to R3 has an IP address of 50.0.0.4. To create these default routes, you need to enter the following commands on each router's console:

On R1: R1#configure terminal R1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.4 R1(config)#end

On R3: R3#configure terminal R3(config)#ip route 0.0.0.0 0.0.0.0 50.0.0.4 R3(config)#end

Question 3

Question Type: **MultipleChoice**

All physical cabling is in place. A company plans to deploy 32 new sites.

The sites will utilize both IPv4 and IPv6 networks.

1 . Subnet 172.25.0.0/16 to meet the subnet requirements and maximize

the number of hosts

Using the second subnet

* Assign the first usable IP address to e0/0 on Sw1O1

* Assign the last usable IP address to e0/0 on Sw102

2. Subnet to meet the subnet requirements and maximize

the number of hosts

c Using the second subnet

* Assign an IPv6 GUA using a unique 64-Bit interface identifier

on e0/0 on Sw101

* Assign an IPv6 GUA using a unique 64-Bit interface identifier

on eO/O on swi02

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.

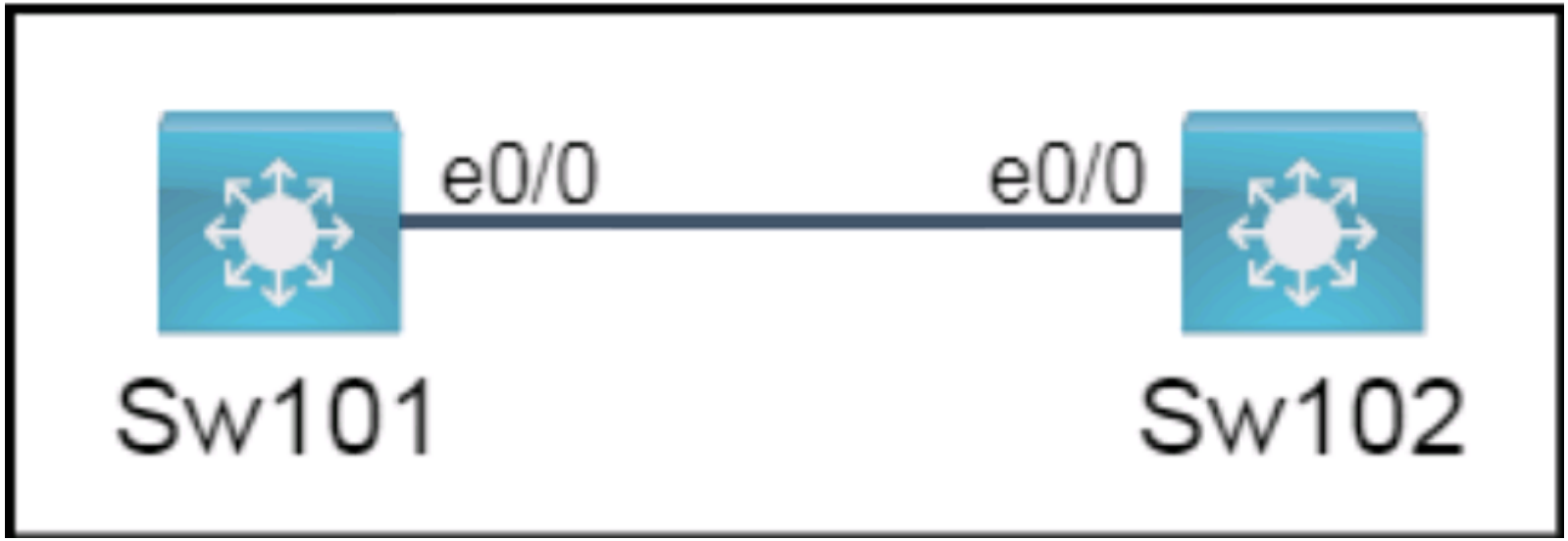
* All necessary preconfigurations have been applied.

* 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.



Options:

A- See the Explanation for the solution

Answer:

A

Explanation:

To subnet 172.25.0.0/16 to meet the subnet requirements and maximize the number of hosts, you need to determine how many bits you need to borrow from the host portion of the address to create enough subnets for 32 sites. Since 32 is 2^5, you need to borrow 5 bits, which means your new subnet mask will be /21 or 255.255.248.0. To find the second subnet, you need to add the value of the fifth bit (32) to the third octet of the network address (0), which gives you 172.25.32.0/21 as the second subnet. The first usable IP address in this subnet is 172.25.32.1, and the last usable IP address is 172.25.39.254.

To assign the first usable IP address to e0/0 on Sw101, you need to enter the following commands on the device console:

Sw101#configure terminal Sw101(config)#interface e0/0 Sw101(config-if)#ip address 172.25.32.1 255.255.248.0 Sw101(config-if)#no shutdown Sw101(config-if)#end

To assign the last usable IP address to e0/0 on Sw102, you need to enter the following commands on the device console:

Sw102#configure terminal Sw102(config)#interface e0/0 Sw102(config-if)#ip address 172.25.39.254 255.255.248.0 Sw102(config-if)#no shutdown Sw102(config-if)#end

To subnet an IPv6 GUA to meet the subnet requirements and maximize the number of hosts, you need to determine how many bits you need to borrow from the interface identifier portion of the address to create enough subnets for 32 sites. Since 32 is 2^5, you need to

borrow 5 bits, which means your new prefix length will be /69 or ffff:ffff:ffff:fff8::/69 (assuming that your IPv6 GUA has a /64 prefix by default). To find the second subnet, you need to add the value of the fifth bit (32) to the fourth hextet of the network address (0000), which gives you xxxx:xxxx:xxxx:0020::/69 as the second subnet (where xxxx:xxxx:xxxx is your IPv6 GUA prefix). The first and last IPv6 addresses in this subnet are xxxx:xxxx:xxxx:0020::1 and xxxx:xxxx:xxxx:0027:ffff:ffff:ffff:fffe respectively.

To assign an IPv6 GUA using a unique 64-bit interface identifier on e0/0 on Sw101, you need to enter the following commands on the device console (assuming that your IPv6 GUA prefix is 2001:db8::/64):

Sw101#configure terminal Sw101(config)#interface e0/0 Sw101(config-if)#ipv6 address 2001:db8::20::1/69 Sw101(config-if)#no shutdown Sw101(config-if)#end

To assign an IPv6 GUA using a unique 64-bit interface identifier on e0/0 on Sw102, you need to enter the following commands on the device console (assuming that your IPv6 GUA prefix is 2001:db8::/64):

Sw102#configure terminal Sw102(config)#interface e0/0 Sw102(config-if)#ipv6 address 2001:db8::27::fffe/69 Sw102(config-if)#no shutdown Sw102(config-if)#end

Question 4

Question Type: **MultipleChoice**

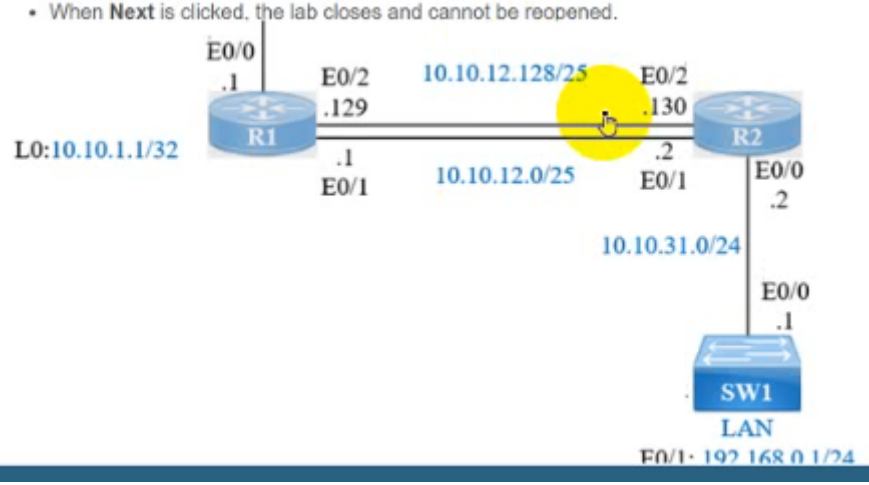
Refer to exhibit.

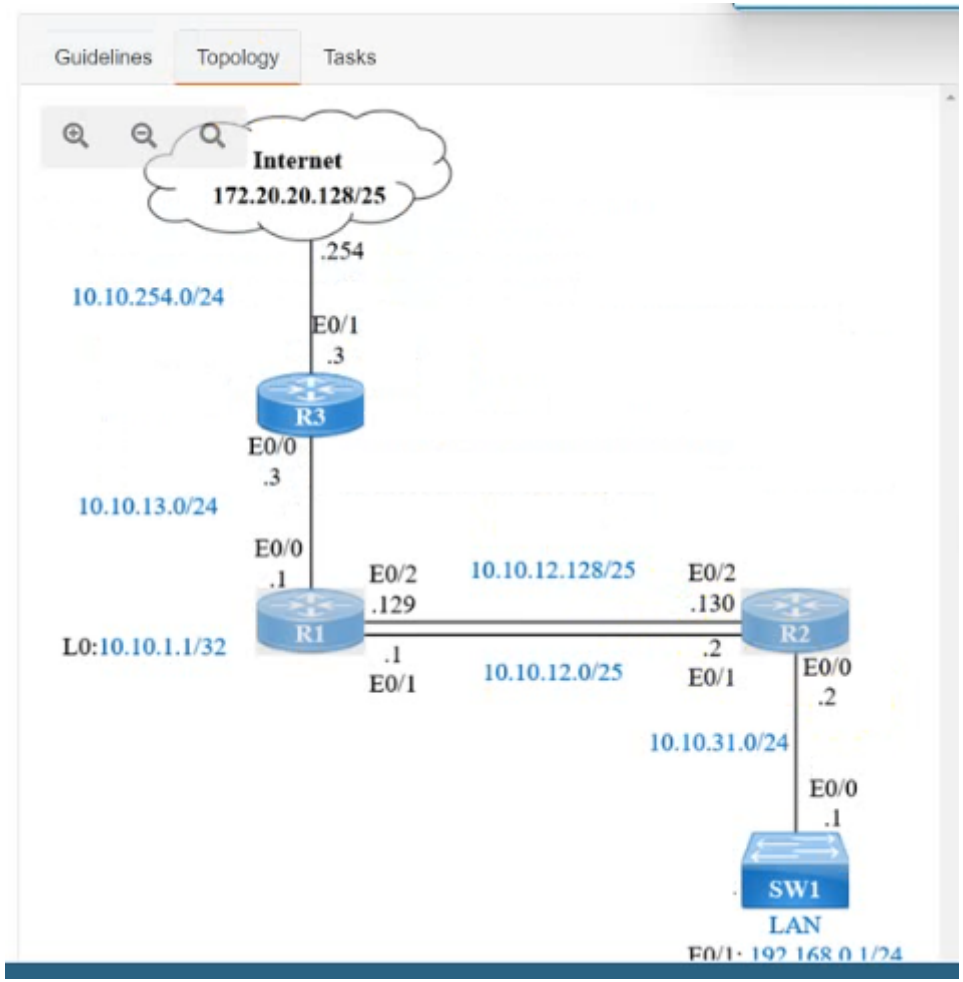
Guidelines | Topology | Tasks

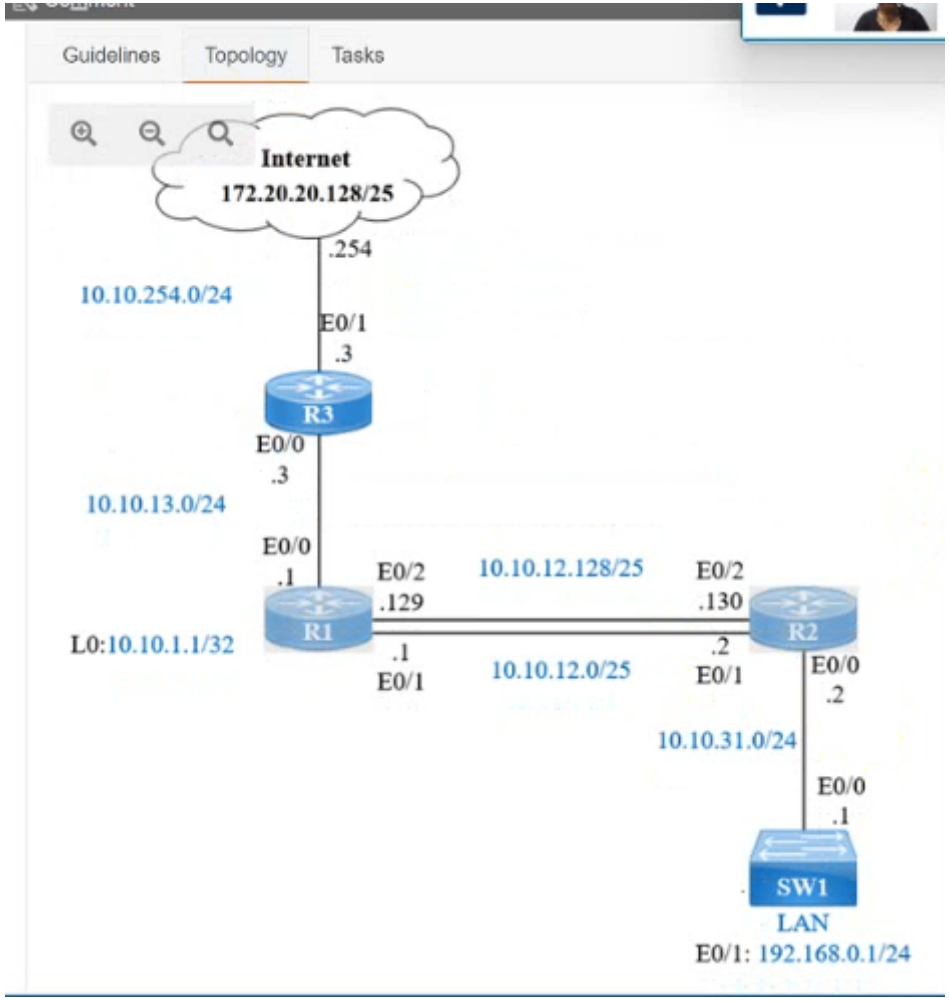
Guidelines

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.




Guidelines
Topology
Tasks
Internet
172.20.20.128/25
.254
10.10.254.0/24
E0/1
.3
R3
E0/0
.3
10.10.13.0/24
E0/0
.1
E0/2
.129
10.10.12.128/25
E0/2
.130
R1
R2
L0:10.10.1.1/32
.1
E0/1
10.10.12.0/25
.2
E0/1
E0/0
.2
10.10.31.0/24
E0/0
.1
SW1
LAN
E0/1: 192.168.0.1/24



IP connectivity and OSPF are preconfigured on all devices where necessary. Do not make any changes to the IP addressing or OSPF. The company policy uses connected interfaces and next hops when configuring static routes except for load balancing or redundancy without floating static. Connectivity must be established between subnet 172.20.20.128/25 on the Internet and the LAN at 192.168.0.0/24 connected to SW1:

1. Configure reachability to the switch SW1 LAN subnet in router R2.

2. Configure default reachability to the Internet subnet in router R1.

3. Configure a single static route in router R2 to reach to the Internet subnet considering both redundant links between routers R1 and R2. A default route is NOT allowed in router R2.

4. Configure a static route in router R1 toward the switch SW1 LAN subnet where the primary link must be through Ethernet0/1. and the backup link must be through Ethernet0/2 using a floating route. Use the minimal administrative distance value when required.

Options:

A- See the Explanation below

Answer:

A

Explanation:

Answer as below configuration:

On R2:

Enable

Conf t

Ip route 192.168.1.0 255.255.255.0 10.10.31.1

On R1:

Enable

Conf t

Ip route 0.0.0.0 0.0.0.0 10.10.13.3

On R2

Ip route 172.20.20.128 255.255.255.128 e0/2

Ip route 172.20.20.128 255.255.255.128 e0/1

On R1

Ip route 192.168.0.0 255.255.255.0 e0/1

Ip route 192.168.0.0 255.255.255.0 10.10.12.2 3

Save all configurations after every router from anyone of these command

Do wr

Or

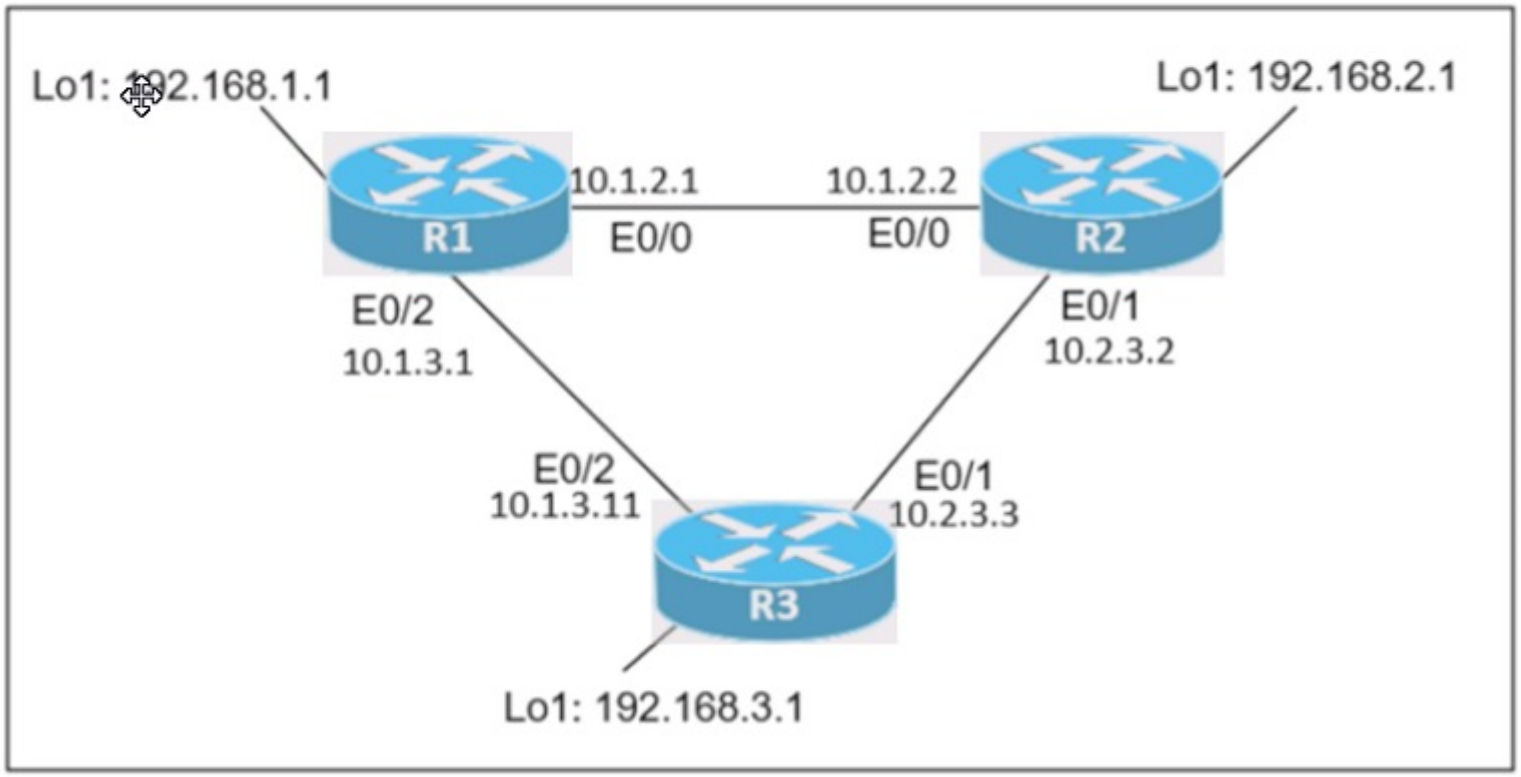
Copy run start

Question 5

Question Type: **MultipleChoice**

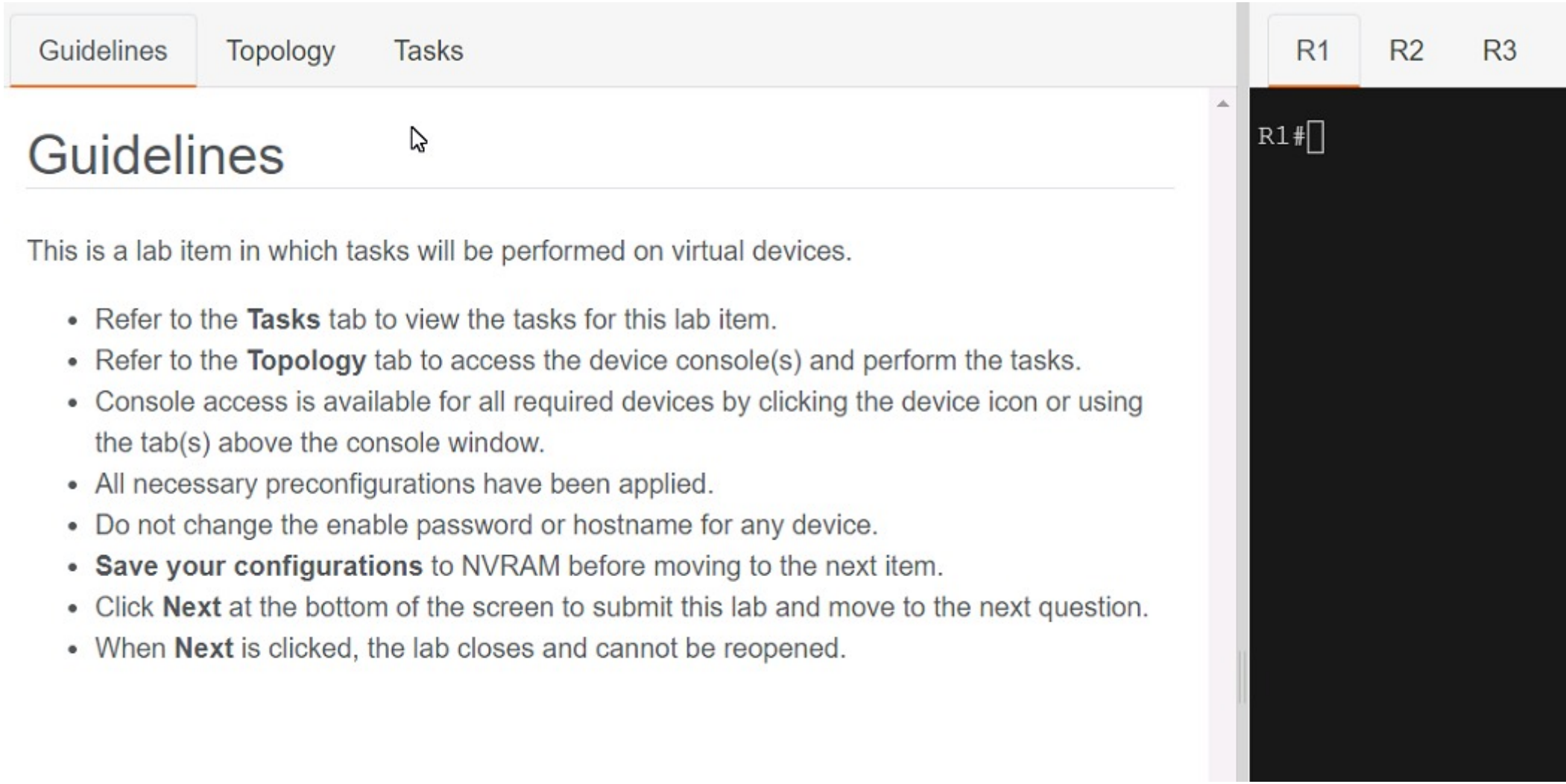
Refer to exhibit.

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

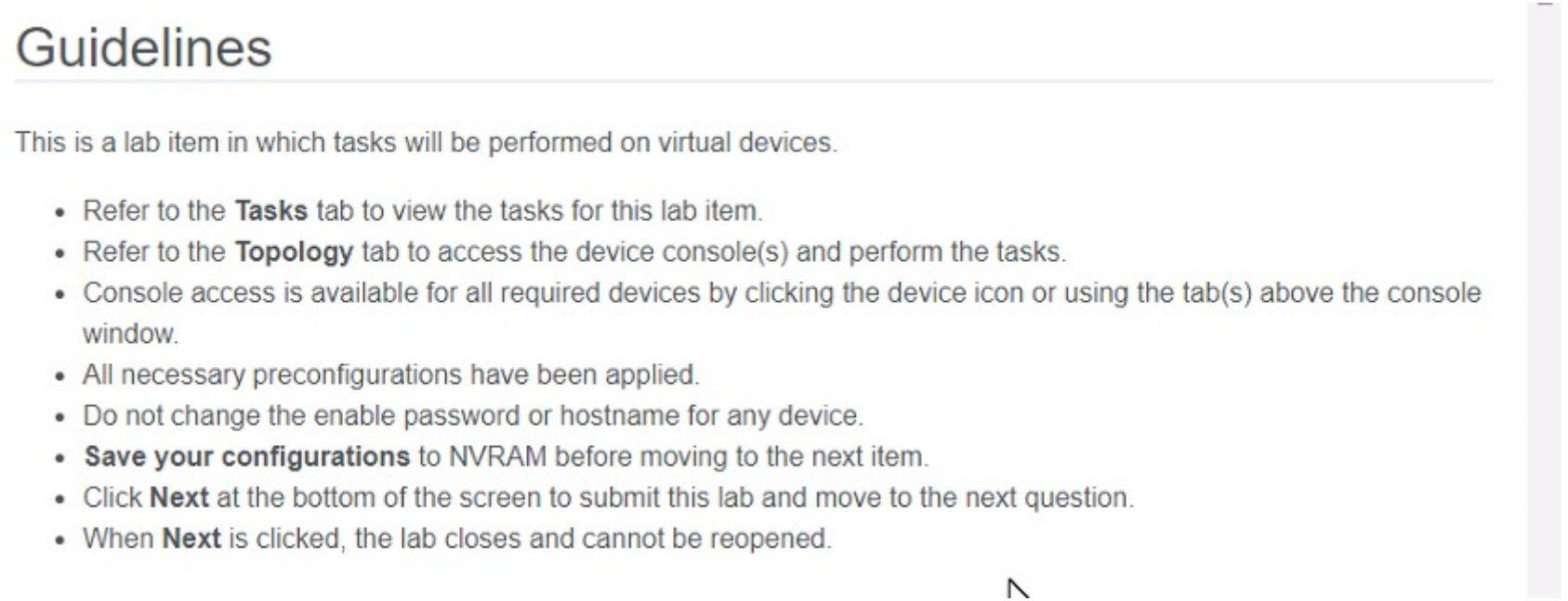
1024

Copy run start

Question 6

Question Type: MultipleChoice

Refer to 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:

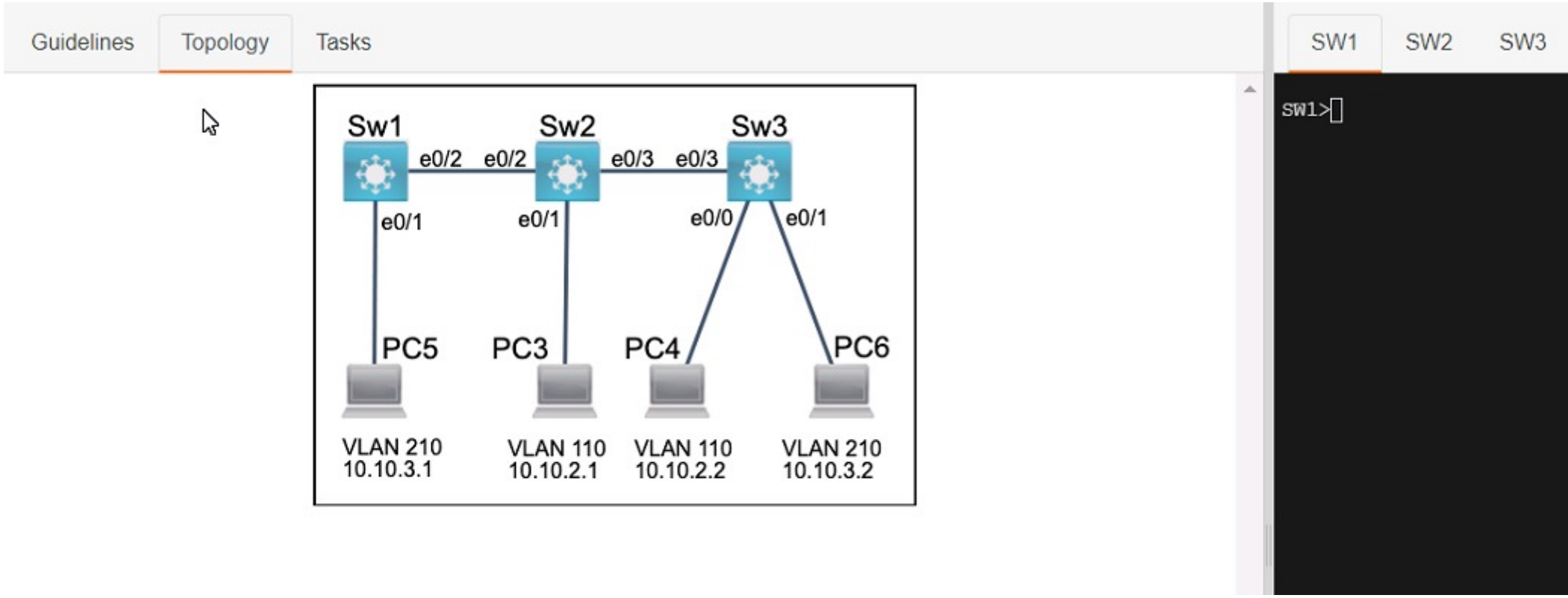
VLAN 110: MARKETING

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 7

Question Type: **MultipleChoice**

Refer to 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.

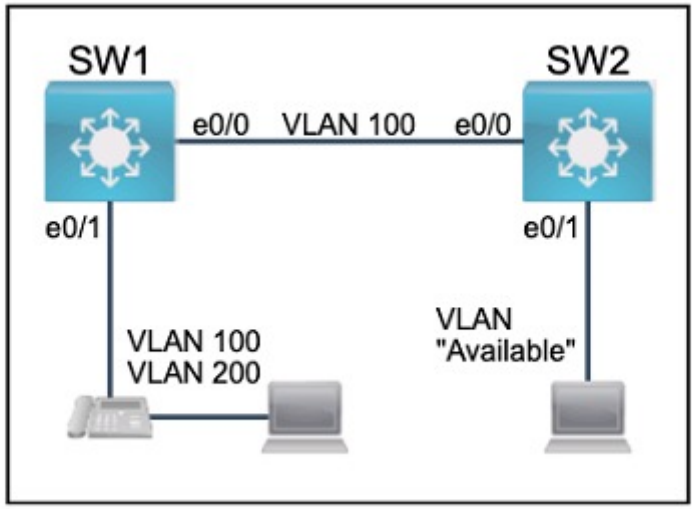
1. Configure VLAN 100 named Compute and VLAN 200 named Telephony where required for each task.

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 8

Question Type: **MultipleChoice**

Physical connectivity is implemented between the two Layer 2 switches, and the network connectivity between them must be configured

1. Configure an LACP EtherChannel and number it as 1; configure it between switches SW1 and SVV2 using interfaces Ethernet0/0 and Ethernet0/1 on both sides. The LACP mode must match on both ends

2 Configure the EtherChannel as a trunk link.

3. Configure the trunk link with 802.1 q tags.

4. Configure the native VLAN of the EtherChannel as VLAN 15.

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.

Options:

A- See the Explanation below

Answer:

A

Explanation:

Answer as below configuration:

On SW1:

conf terminal

vlan 15

exit

interface range eth0/0 - 1

channel-group 1 mode active

exit

interface port-channel 1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk native vlan 15

end

copy run start

on SW2:

conf terminal

vlan 15

exit

interface range eth0/0 - 1

channel-group 1 mode active

exit

interface port-channel 1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk native vlan 15

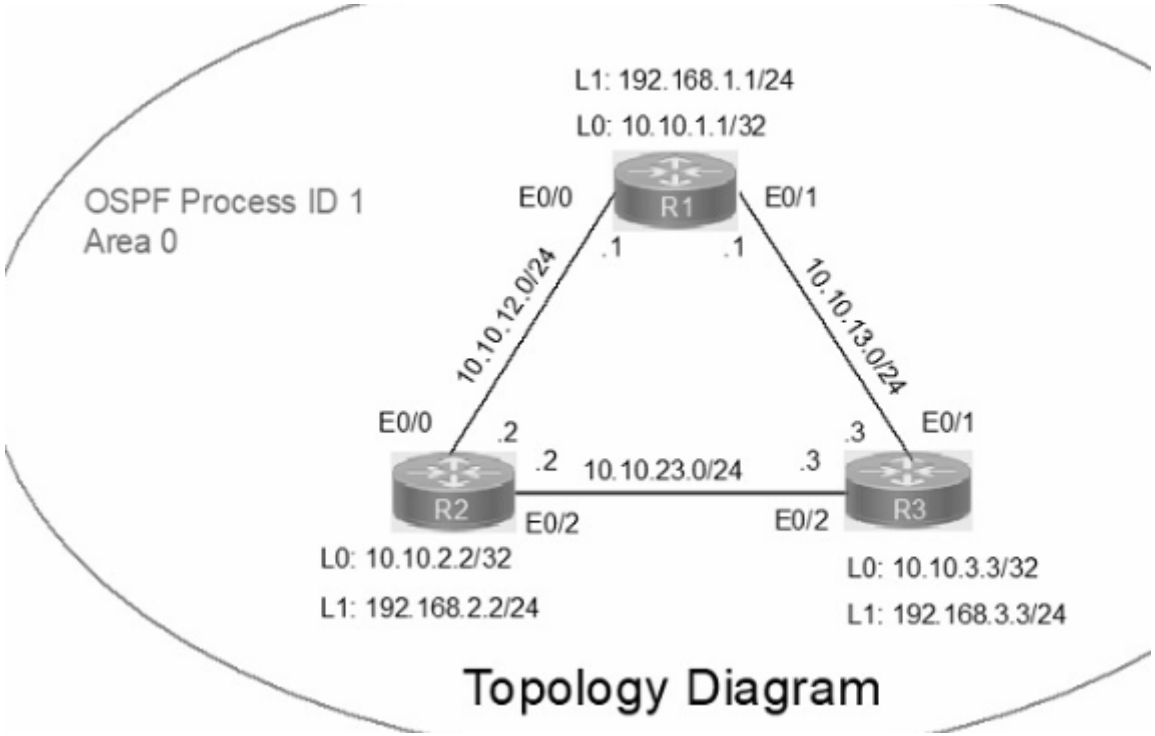
end

copy run start

Question 9

Question Type: MultipleChoice

Refer to 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.

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 10

Question Type: MultipleChoice

Which two capabilities of Cisco DNA Center make it more extensible as compared to traditional campus device management? (Choose two.)

Options:

A- REST APIs that allow for external applications to interact natively

B- adapters that support all families of Cisco IOS software

C- SDKs that support interaction with third-party network equipment

D- customized versions for small, medium, and large enterprises

E- modular design that is upgradable as needed

Answer:

A, C

Explanation:

Topic 5, Simulations / Lab

Question 11

Question Type: MultipleChoice

Which type of encryption does WPA1 use for data protection?

Options:

A- AES

B- TKIP

C- PEAP

D- EAP

Answer:

B

Question 12

Question Type: MultipleChoice

What is used to identify spurious DHCP servers?

Options:

A- DHCPREQUEST

B- DHCPDISCOVER

C- DHCPACK

D- DHCPOFFER

Answer:

D

Explanation:

DHCPOFFER is used to identify spurious DHCP servers. A spurious DHCP server is any device that is configured to act as a DHCP server without the network administrator's knowledge or permission. A spurious DHCP server can cause network problems by assigning incorrect or duplicate IP addresses to clients, or by redirecting traffic to malicious gateways.To prevent such attacks, the DHCP snooping feature can be enabled on switches to filter out invalid or unauthorized DHCP messages from untrusted sources1.

DHCP snooping works by intercepting and validating DHCP messages on a per-VLAN basis.The switch maintains a DHCP snooping binding database that contains information about the trusted hosts with leased IP addresses, such as MAC address, IP address, lease

time, binding type, VLAN number, and interface information2. The switch also classifies its ports as trusted or untrusted. Trusted ports are those that connect to authorized DHCP servers or other trusted switches. Untrusted ports are those that connect to untrusted hosts or devices.The switch only allows DHCP messages from trusted ports, and drops any DHCP messages from untrusted ports that do not match the information in the binding database3.

The switch uses DHCPOFFER messages to identify spurious DHCP servers. A DHCPOFFER message is a response from a DHCP server to a client's request for an IP address.The message contains the offered IP address, subnet mask, default gateway, and other configuration parameters for the client4. When the switch receives a DHCPOFFER message from an untrusted port, it compares the source MAC address and the offered IP address with the binding database. If there is no match, the switch considers the message as coming from a spurious DHCP server and drops it.The switch also logs an error message and increments a counter for the number of dropped messages5.

1: Configuring DHCP Snooping - Cisco

2: Catalyst 6500 Release 12.2SX Software Configuration Guide - DHCP Snooping Binding Database

3: What is DHCP Snooping? - IONOS

4: Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) Parameters

5: Configuring DHCP Snooping - Cisco