

ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΑΘΛΗΤΙΣΜΟΥ ΚΑΙ ΝΕΟΛΑΙΑΣ  
ΔΙΕΥΘΥΝΣΗ ΜΕΣΗΣ ΓΕΝΙΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ

ΕΝΙΑΙΕΣ ΤΕΛΙΚΕΣ ΑΠΟΛΥΤΗΡΙΕΣ ΓΡΑΠΤΕΣ ΕΞΕΤΑΣΕΙΣ 2023-2024

Γ΄ ΤΑΞΗΣ ΛΥΚΕΙΟΥ

ΗΜΕΡΟΜΗΝΙΑ: ΔΕΥΤΕΡΑ 20 ΜΑΪΟΥ 2024

ΕΞΕΤΑΖΟΜΕΝΟ ΜΑΘΗΜΑ: ΔΙΚΤΥΑ - CISCO

Α΄ ΣΕΙΡΑ

ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ: Γ060

ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ

ΣΥΝΟΛΙΚΗ ΔΙΑΡΚΕΙΑ ΓΡΑΠΤΗΣ ΕΞΕΤΑΣΗΣ : 90 λεπτά

ΤΟ ΕΞΕΤΑΣΤΙΚΟ ΔΟΚΙΜΙΟ ΑΠΟΤΕΛΕΙΤΑΙ ΑΠΟ ΔΕΚΑΤΡΕΙΣ (13) ΣΕΛΙΔΕΣ

---

ΟΔΗΓΙΕΣ (για τους εξεταζομένους)

1. Στο εξώφυλλο του τετραδίου απαντήσεων να συμπληρώσετε όλα τα κενά με τα στοιχεία που ζητούνται.
2. **Να απαντήσετε ΟΛΑ τα ερωτήματα.**
3. **Να μην αντιγράψετε τα θέματα** στο τετράδιο απαντήσεων.
4. Να μη γράψετε πουθενά στις απαντήσεις σας το όνομά σας.
5. Να απαντήσετε στο τετράδιό σας σε όλα τα θέματα **μόνο με μπλε πένα ανεξίτηλης μελάνης**. Μολύβι επιτρέπεται, μόνο αν το ζητάει η εκφώνηση, και μόνο για σχήματα, πίνακες, διαγράμματα κ.λπ.
6. Απαγορεύεται η χρήση διορθωτικού υγρού ή διορθωτικής ταινίας.
7. Επιτρέπεται η χρήση μη προγραμματιζόμενης υπολογιστικής μηχανής που φέρει τη σφραγίδα του σχολείου.

**ΜΕΡΟΣ Α (30 μονάδες)**

Να απαντήσετε και στις είκοσι (20) ερωτήσεις πολλαπλής επιλογής. Υπάρχει μόνο μια σωστή απάντηση σε κάθε ερώτηση. Η κάθε ερώτηση βαθμολογείται με 1½ μονάδα.

**Ερώτηση 1. (ch1. 2024) A**

What is the primary purpose of assigning an IP address to a switch?

- (a) To enable the switch to route between different VLANs.
- (b) **To prepare the switch for remote management access.**
- (c) To increase the switch processing power.
- (d) To enable the switch to generate logs.

**Ερώτηση 2. (ch1. 2024) A**

Which feature allows a switch port to detect the required cable type and configure itself accordingly?

- (a) Duplex mode
- (b) Speed setting
- (c) **Auto-MDIX**
- (d) VLAN assignment

**Ερώτηση 3. (ch3. 2024) A**

On a switch that is configured with multiple VLANs, which command will remove only VLAN 10?

- (a) **Switch(config)# no vlan 10**
- (b) Switch# **delete flash:vlan.dat**
- (c) Switch(config-if)# **no switchport access vlan 10**
- (d) Switch(config-if)# **no switchport trunk allowed vlan 10**

**Ερώτηση 4. (ch3. 2024) A**

In a multi-switched environment, what is the function of a trunk link?

- (a) **To carry multiple VLANs across a single physical link**
- (b) To restrict traffic to a single VLAN
- (c) To connect different networks
- (d) To provide backup links in case of a primary link failure

**Ερώτηση 5. (ch4. 2024) A**

What is the purpose of subinterfaces in Router-on-a-Stick Inter-VLAN routing?

- (a) To enable different encryption levels
- (b) **To allow a single router interface to route multiple VLANs**
- (c) To increase the number of physical interfaces on the router
- (d) To configure additional physical connections to the router

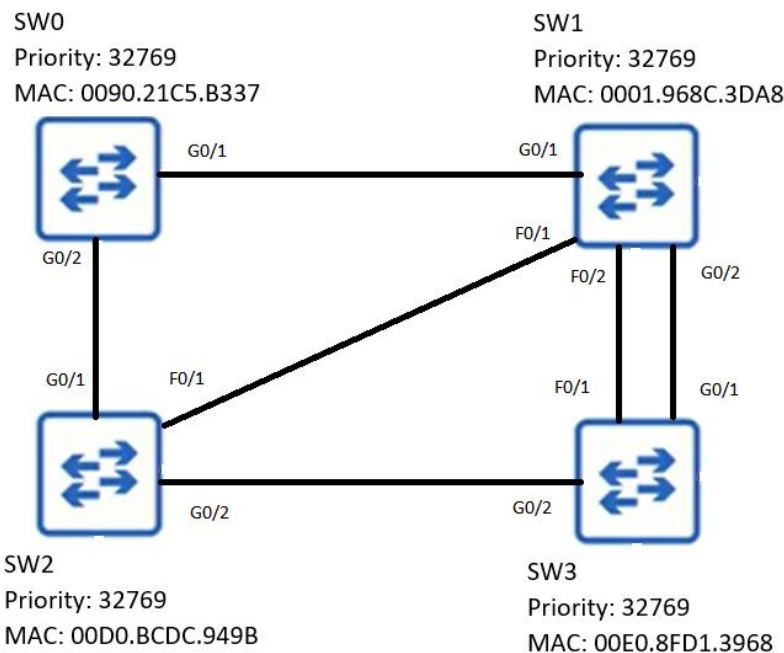
**Ερώτηση 6. (ch5. 2024) A**

What is the function of STP in a scalable network?

- (a) It spreads traffic across multiple physical WAN links.
- (b) It enables traffic from multiple VLANs to travel over a single Layer 2 link.
- (c) It disables redundant paths to eliminate Layer 2 loops.
- (d) It combines multiple switch trunk links to act as one logical link for increased bandwidth

**Ερώτηση 7. (ch5. 2024) A**

Which switch will be elected as the root bridge if STP is running on the switches?



- (a) SW0
- (b) SW1
- (c) SW2
- (d) SW3

**Ερώτηση 8. (ch6. 2024) A**

What is the primary purpose of EtherChannel technology in network configurations?

- (a) To decrease the number of physical connections between devices.
- (b) To increase bandwidth by combining multiple Ethernet links into a single logical link.
- (c) To enable faster packet delivery by reducing latency and overhead.
- (d) To eliminate switching loop.

**Ερώτηση 9. (ch6. 2024) A**

What must be consistent across all ports in an EtherChannel group?

- (a) The speed, duplex settings, and VLAN information must be the same.
- (b) The ports must be on different VLANs for proper load balancing.
- (c) Each port must have a unique IP address for identification.
- (d) All configuration tasks must be done on the individual ports.

**Ερώτηση 10. (ch7. 2024) A**

Which of the following describes the DHCP Discover message?

- (a) It is sent from the server to offer an IP address to the client.
- (b) It is sent from the client to accept an IP address received from the server.
- (c) It is sent from the client to initiate contact with DHCP servers.
- (d) It is a final acknowledgment from the client to accept the offered IP address.

**Ερώτηση 11. (ch7. 2024) A**

What is one indication that a Windows computer did not receive an IPv4 address from a DHCP server?

- (a) The computer cannot ping 127.0.0.0
- (b) The computer cannot ping 127.0.0.1
- (c) Windows displays a DHCP timeout message
- (d) The computer receives an IP address that starts with 169.254

**Ερώτηση 12. (ch14. 2024) A**

How does a router handle a packet when there is no valid route in the routing table?

- (a) The packet is forwarded to the next available router for processing.
- (b) The packet is stored until a route becomes available.
- (c) The packet is dropped.
- (d) The packet is sent to the management console for further inspection.

**Ερώτηση 13. (ch14. 2024) A**

Which of these routes would have the highest administrative distance?

- (a) a static route.
- (b) a directly connected network.
- (c) a route received through the OSPF routing protocol.
- (d) a route received through the EIGRP routing protocol.

**Ερώτηση 14. (ch10. 2024) A**

What does AAA stand for in network security?

- (a) Authentication, Authorization, and Accounting
- (b) Automatic, Assisted, and Administered
- (c) Analyze, Act, and Audit
- (d) Access, Allocate, and Audit

**Ερώτηση 15. (ch10. 2024) A**

What is the most appropriate mitigation technique for MAC address table flooding attacks?

- (a) Implementing port security to limit the number of MAC addresses on a port.
- (b) Using stronger encryption methods for data packets.
- (c) Increasing the size of the MAC address table.
- (d) Configure DHCP snooping.

**Ερώτηση 16. (ch.14 2024) A**

What is the correct syntax of a floating (backup) static route?

- (a) `ip route 209.165.200.228 255.255.255.248 serial 0/0/0`
- (b) `ip route 209.165.200.228 255.255.255.248 10.0.0.1 120`
- (c) `ip route 0.0.0.0 0.0.0.0 serial 0/0/0`
- (d) `ip route 172.16.0.0 255.248.0.0 10.0.0.1`

**Ερώτηση 17. (CCNA3 – Ch1 - Dynamic Routing OSPF 2024) A**

What type of routing protocol is OSPF?

- (a) Distance vector
- (b) Path vector
- (c) Link-state
- (d) Hybrid

**Ερώτηση 18. (CCNA3 – Ch1 - Dynamic Routing OSPF 2024) A**

A network technician issues the following commands when configuring a router RR:

```
RR(config)# router ospf 100
RR(config-router)# network 172.16.1.0 0.0.0.255 area 0
```

What does the number 100 represent?

- (a) the cost of the link to RR.
- (b) the OSPF process ID on RR.
- (c) the autonomous system (AS) number to which RR belongs.
- (d) the area number where RR is located.

**Ερώτηση 19. (CCNA 3 ch.4 2024) A**

What is the primary purpose of Access Control Lists (ACLs) in network routers?

- (a) To define routes for data packets.
- (b) To filter packets based on rules to enhance security.
- (c) To assign IP addresses to devices.
- (d) To manage bandwidth allocation on the network.

**Ερώτηση 20. (CCNA3-ch. 4 2024) A**

What is the main difference between inbound and outbound ACLs when applied to a router interface?

- (a) Inbound ACLs filter traffic after it has been routed; outbound ACLs filter before routing.
- (b) Inbound ACLs filter traffic before it has been routed; outbound ACLs filter after routing.
- (c) Inbound ACLs apply only to TCP traffic; outbound ACLs apply to both TCP and UDP.
- (d) There is no difference; both perform filtering at the same stage.

**Μέρος Β (30 μονάδες)**

Να απαντήσετε σε όλες τις ερωτήσεις. Η κάθε ερώτηση βαθμολογείται με έξι (6) μονάδες.

**Ερώτηση 1. (ccna 3 ch1 ) 2024 A**

For each network specify the corresponding subnet mask and wildcard mask.

| Network           | Decimal Subnet Mask | Wildcard Mask |
|-------------------|---------------------|---------------|
| (a) 10.10.0.0 /9  | 255.128.0.0         | 0.127.255.255 |
| (b) 10.20.0.0 /20 | 255.255.240.0       | 0.0.15.255    |
| (c) 10.30.0.0 /27 | 255.255.255.224     | 0.0.0.31      |

**Ερώτηση 2. (Chapter 14) 2024 A**

A network administrator has issued the command **show ip route** on a router. Based on the following output fill in the blanks:

Gateway of last resort is not set

192.168.0.0/16 is subnetted, 2 subnets

O 192.168.10.0/24 [110/85] via 10.1.2.2, 00:10:46, Serial0/1/0

O 192.168.20.0/24 [110/85] via 10.1.2.2, 00:10:33, Serial0/1/0

10.1.0.0/16 is variably subnetted, 5 subnets, 2 masks

C 10.1.1.0/24 is directly connected, GigabitEthernet1/0

C 10.1.2.0/24 is directly connected, Serial0/1/0

C 10.1.3.0/24 is directly connected, Serial0/1/1

R 10.2.1.0/24 [120/1] via 10.1.3.2, 00:00:30, Serial0/1/1

S 10.2.2.0/24 [1/0] via 10.1.3.2

- (a) The C in the 10.1.1.0/24 network indicates a (directly) connected route
- (b) The value of administrative distance (AD) for 10.1.3.0/24 route is 0.
- (c) The next hop IP address for network 192.168.10.0/24 is 10.1.2.2
- (d) The 192.168.20.0/24 network has been learned dynamically from another router using the protocol OSPF
- (e) The value of the metric for 192.168.20.0/24 route is 85.
- (f) The exit interface for packets going to network 10.2.1.0/24 is Serial 0/1/1

**Ερώτηση 3. (CCNA3 - ACL 2024) A**

For each access entry, determine the action that will be taken (permit or deny) when applied to the comparison address provided.

|     | Access List Entry (ACE)                      | Comparison Address | Permit or Deny |
|-----|--|--------------------|----------------|
| (a) | Access-list 10 permit 192.168.1.0 0.0.0.255  | 192.168.1.11       | Permit         |
| (b) | Access-list 10 permit 172.16.0.0 0.0.255.255 | 172.17.5.11        | Deny           |
| (c) | Access-list 10 permit 10.0.0.0 0.255.255.255 | 10.16.31.34        | Permit         |
| (d) | Access-list 10 permit 172.16.1.16 0.0.0.7    | 172.16.1.27        | Deny           |
| (e) | Access-list 10 permit 192.168.128.0.0.31.255 | 192.168.170.21     | Deny           |
| (f) | Access-list 10 permit 10.32.0.0 0.15.255.255 | 10.60.10.34        | Deny           |

**Ερώτηση 4. (CCNA2 - Chapter 11) 2024 A**

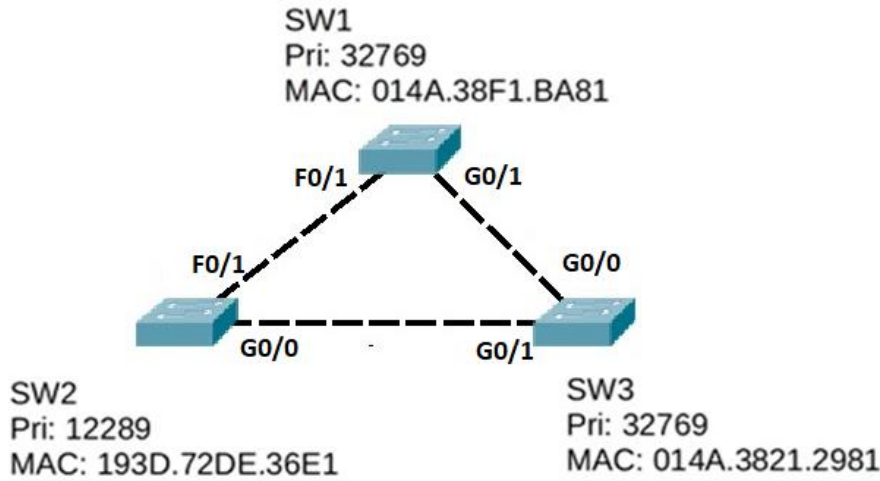
Relate each command in the left column with its corresponding function in the right column. Not all functions are used.

| Command/Term   |   | Function/Value   |
|--|---|--|
| (a) S2(config-if)# <b>switchport port-security mac-address sticky</b>                    | 6 | 1. Sets a maximum number of secure MAC addresses allowed on a switch port.                               |
| (b) S2(config)# <b>interface range fa0/17-20</b><br>S1(config-if-range)# <b>shutdown</b> | 3 | 2. Relates manually a MAC address with a switch port.  |
| (c) S2(config-if)# <b>switchport port-security mac-address 2024.2024.2024</b>            | 2 | 3. Used as a security measure to disable all unused ports.   |
| (d) S2(config-if)# <b>switchport port-security maximum 2</b>                             | 1 | 4. Blocks a switch port for maximum time of two minutes when a violation occurs.                         |
|  |   | 5. Enables port security on a port of a switch.  |
|  |   | 6. Enables the switch to dynamically learn MAC addresses and add them in the running configuration file. |

(a)-6 (b)-3 (c)-2 (d)-1

**Ερώτηση 5. (Chapter 5) 2024 A**

Consider the following network. The network has three switches (SW1, SW2, SW3) connected with each other. STP is running on all of the switches. The priority and mac address are shown to on the following exhibit.



SW2 has been elected as root bridge. Write the state of each interface (**Root port**, **Designated** or **Alternate – Blocked**).

| Switch | Interface | State      |
|--------|-----------|------------|
| SW1    | (a) F0/1  | Blocked    |
|        | (b) G0/1  | Root Port  |
| SW2    | (c) F0/1  | Designated |
|        | (d) G0/0  | Designated |
| SW3    | (e) G0/0  | Designated |
|        | (f) G0/1  | Root port  |

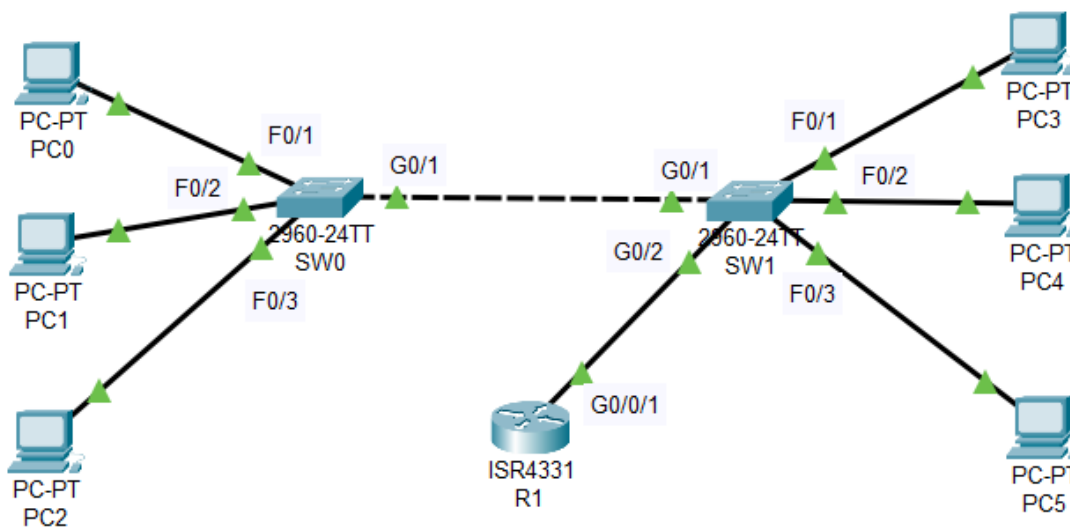


**ΜΕΡΟΣ Γ (40 Μονάδες)**

Να απαντήσετε σε όλες τις ερωτήσεις. Η κάθε ερώτηση βαθμολογείται με είκοσι (20) μονάδες.

**Ερώτηση 1. (Chapter 3, 4, 11) 2024**

The network topology and addressing table are given below. Follow the instructions provided.

**Network Topology****Addressing Table**

| Device | Interface  | IPv4 Address | Subnet Mask   | Default Gateway | VLAN |
|--------|------------|--------------|---------------|-----------------|------|
| PC0    | F0/1 / SW0 | 192.168.1.10 | 255.255.255.0 | 192.168.1.1     | 10   |
| PC1    | F0/2 / SW0 | 192.168.1.11 | 255.255.255.0 | 192.168.1.1     | 10   |
| PC2    | F0/3 / SW0 | 192.168.2.12 | 255.255.255.0 | 192.168.2.1     | 20   |
| PC3    | F0/1 / SW1 | 192.168.1.13 | 255.255.255.0 | 192.168.1.1     | 10   |
| PC4    | F0/2 / SW1 | 192.168.2.14 | 255.255.255.0 | 192.168.2.1     | 20   |
| PC5    | F0/3 / SW1 | 192.168.2.15 | 255.255.255.0 | 192.168.2.1     | 20   |

(a) Create VLAN 10 and VLAN 20 on switches SW0 and SW1.

(1 pt)

```
SW0(config)# vlan 10
SW0(config-vlan)#vlan 20
SW1(config)# vlan 10
SW1(config-vlan)#vlan 20
```

- (b) Assign the appropriate interfaces to the VLAN 10 and VLAN 20, for both switches SW0 and SW1. (7pts)

```
SW0(config)# int range f0/1-2
SW0(config-if-range)#switchport mode access
SW0(config-if-range)#switchport access vlan 10
SW0(config-if-range)#exit
SW0(config)#int f0/3
SW0(config-if)#switchport mode access
SW0(config-if)#switchport access vlan 20
SW1(config)# int f0/1
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#exit
SW1(config)#int range f0/2-3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
```

- (c) Configure G0/1 interface on each switch as trunk. (2 pts)

```
SW0(config)# int g0/1
SW0(config-if)#switchport mode trunk
```

```
SW1(config)# int g0/1
SW1(config-if)#switchport mode trunk
```

- (d) Disable the unused interfaces f0/4-24 on switch SW0. (1 pt)

```
SW0(config)# int range f0/4-24
SW0(config-if-range)#shut
```

- (e) Write the command on switch SW0 in order to verify the vlans and the ports on each vlan. The result of the command must be as follows. (1 pt)

| VLAN | Name               | Status | Ports  |
|------|--------------------|--------|--|
| 1    | default            | active | Fa0/4, Fa0/5, Fa0/6, Fa0/7<br>Fa0/8, Fa0/9, Fa0/10, Fa0/11<br>Fa0/12, Fa0/13, Fa0/14, Fa0/15<br>Fa0/16, Fa0/17, Fa0/18, Fa0/19<br>Fa0/20, Fa0/21, Fa0/22, Fa0/23<br>Fa0/24, Gig0/1, Gig0/2 |
| 10   | VLAN0010           | active | Fa0/1, Fa0/2   |
| 20   | VLAN0020           | active | Fa0/3  |
| 1002 | fddi-default       | active |  |
| 1003 | token-ring-default | active |  |
| 1004 | fddinet-default    | active |  |
| 1005 | trnet-default      | active |  |

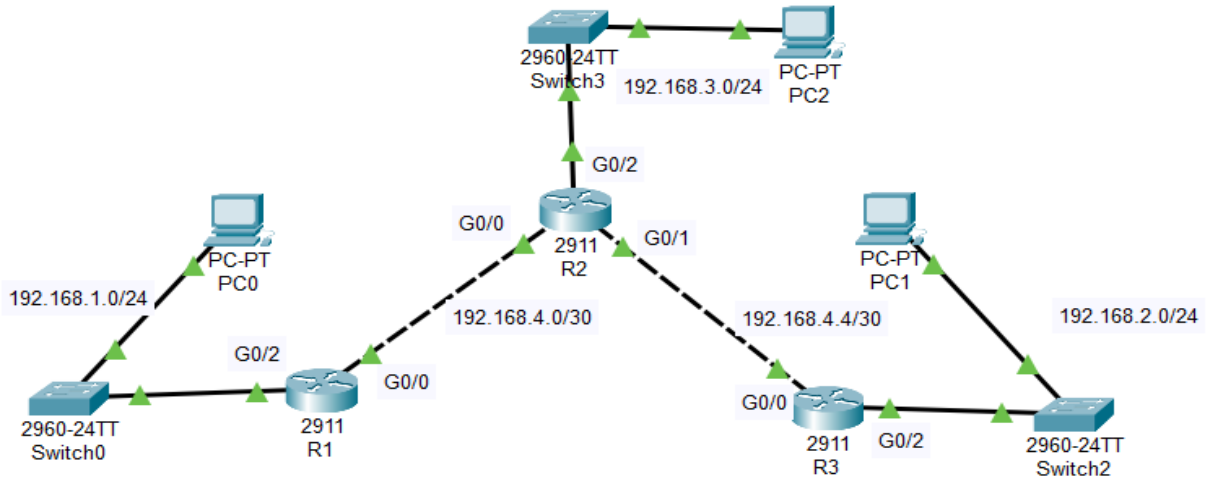
SW0# show vlan brief

- (f) Configure sub-interfaces on R1 using the 802.1Q encapsulation to achieve communication between VLAN10 and VLAN20. Activate the interfaces as needed. R1 is connected with SW1 using interface G0/0/1. (8 pts)

```
R1(config)# int g0/0/1.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.1.1 255.255.255.0
R1(config-subif)#int g0/0/1.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.2.1 255.255.255.0
R1(config-subif)#int g0/0/1
R1(config-if)#no shutdown
```

**Ερώτηση 2. (CCNA 3 ch2..4 CCNA 2 ch. 7, CCNA 2 ch 15) 2024 A**

The network topology and addressing table are given below. Follow the instructions provided.



**Addressing Table**

| Device | Interface | IP Address  | Prefix Notation |
|--------|-----------|-------------|-----------------|
| R1     | G0/0      | 192.168.4.1 | /30             |
|        | G0/2      | 192.168.1.1 | /24             |
| R2     | G0/0      | 192.168.4.2 | /30             |
|        | G0/1      | 192.168.4.6 | /30             |
|        | G0/2      | 192.168.3.1 | /24             |
| R3     | G0/0      | 192.168.4.5 | /30             |
|        | G0/2      | 192.168.2.1 | /24             |

(a) Configure R1 to act as DHCPv4 Server for 192.168.1.0/24 network. (4 pts)

- i. Exclude the first 10 addresses of 192.168.1.0/24 network
- ii. Define the pool name as LAN1
- iii. Specify the network that DHCP is supporting.
- iv. Configure the default gateway address

```
R1(config)#> ip dhcp excluded-address 192.168.1.1 192.168.1.10
R1(config)#ip dhcp pool LAN1
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
```

(b) Use the following requirements to configure OSPFv2 dynamic routing on router R1:

- i. Process ID 10
- ii. Router ID 1.1.1.1
- iii. Area 0
- iv. Network address and appropriate network wildcard mask for each interface
- v. LAN interface set to passive (5 pts)

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 192.168.4.0 0.0.0.3 area 0
R1(config-router)# passive-interface G0/2
```

(c) Configure the fully specified routes on R2 for every remote network. (2 pts)

```
R2(config)# ip route 192.168.1.0 255.255.255.0 g0/0 192.168.4.1
R2(config)# ip route 192.168.2.0 255.255.255.0 g0/1 192.168.4.5
```

(d) Configure the recursive (next-hop) static routes on R3 for every remote network.

(3 pts)

```
R3(config)# ip route 192.168.1.0 255.255.255.0 192.168.4.6
R3(config)# ip route 192.168.3.0 255.255.255.0 192.168.4.6
R3(config)# ip route 192.168.4.0 255.255.255.252 192.168.4.6
```

(e) Configure a static default route on R1.

(1 pt)

```
R1(config)# ip route 0.0.0.0 0.0.0.0 G0/0
```

(f) Configure and apply the numbered standard ACL 1.

(3 pts)

The ACL should block all traffic from network 192.168.1.0/24 to network 192.168.2.0/24. It must also block traffic from both hosts 192.168.3.11 and 192.168.3.12. All other traffic to 192.168.2.0 network should be allowed. Place the ACL on router R3. Choose the appropriate interface and direction.

```
R3(config)# access-list 1 deny 192.168.1.0 0.0.0.255
R3(config)# access-list 1 deny host 192.168.3.11
R3(config)# access-list 1 deny host 192.168.3.12
R3(config)# access-list 1 permit any
R3(config)# interface G0/2
R3(config-if)# ip access-group 1 out
or
R3(config)# interface G0/0
R3(config-if)# ip access-group 1 in
```

(g) Configure and apply the numbered standard ACL 2 (2 pts)

The ACL should block host 192.168.1.100 from accessing any other network except from 192.168.1.0/24. Place ACL on router R1. Choose the appropriate interface and direction.

```
R1(config)# access-list 2 deny host 192.168.1.100
R1(config)# access-list 2 permit any
R1(config)# interface GigabitEthernet0/2
R1(config-if)# ip access-group 2 in
or
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip access-group 2 out
```

**ΤΕΛΟΣ ΕΞΕΤΑΣΤΙΚΟΥ ΔΟΚΙΜΙΟΥ**  
**ΣΑΣ ΕΥΧΟΜΑΣΤΕ ΚΑΛΗ ΕΠΙΤΥΧΙΑ**