ΑΣΚΗΣΕΙΣ ΑΝΑΚΕΦΑΛΑΙΩΣΗΣ

1. Βασικές Πληροφορίες Δικτύου

Παρακάτω εμφανίζεται τμήμα των αποτελεσμάτων που παρέχει μια βασική εντολή του λειτουργικού συστήματος. Η εντολή εμφανίζει πληροφορίες για τους Network Interface Controllers (NIC) ενός υπολογιστή.

```
VirtualBox Host-Only Ethernet Adapter
0A-00-27-00-00-09
No
Yes
fe80::9d91:d60b:d473:5396%9(Preferred)
192.168.56.1(Preferred)
255.255.255.0

587857959
00-01-00-01-23-37-EF-7A-30-9C-23-5F-33-84
fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
Enabled
```

A. Ποια είναι η πλήρης σύνταξη της εντολής που επιστρέφει τις παραπάνω πληροφορίες για όλα τα διαθέσιμα NICs σε λειτουργικό Windows; (1 λεπτό)
B. Ποια είναι η MAC address του συγκεκριμένου NIC; (1 λεπτό)
C. Γράψτε την subnet mask σε μορφή CIDR suffix. (1 λεπτό)
D. Με βάση την απάντηση του C: Πόσοι hosts (ifs) μπορούν να υπάρξουν στο ίδιο υποδίκτυο με το συγκεκριμένο μηχάνημα. (1-2 λεπτό)
E. Με βάση την απάντηση του C: Ποια είναι η IPv4 address του υποδικτύου στο οποίο ανήκει το μηχάνημα. (1-2 λεπτό)

(Εκτιμώμενος χρόνος 5-7 λεπτά)

2. Βασικές Γνώσεις επιπέδων Εφαρμογής – Μεταφοράς – Δικτύου

Παρακάτω εμφανίζονται οι δικτυακές συνδέσεις της διεργασίας Google Drive με Process ID 14640.

Process	PID	Protocol	Local Address	Local P...	Remote Address	Remot...	State
googledrivesync.exe	14640	TCP	192.168.1.24	1040	172.217.16.138	443	CLOSE_WAIT
googledrivesync.exe	14640	TCP	192.168.1.24	1907	172.217.22.10	443	CLOSE_WAIT
googledrivesync.exe	14640	TCP	192.168.1.24	4110	172.217.21.202	443	CLOSE_WAIT
googledrivesync.exe	14640	TCP	192.168.1.24	5475	216.58.210.13	443	CLOSE_WAIT
googledrivesync.exe	14640	TCP	192.168.1.24	26096	172.217.22.106	443	ESTABLISHED

A. Ποια είναι η διεύθυνση IP του μηχανήματος στο οποίο τρέχει η εφαρμογή; (1 λεπτό)
B. Καταγράψτε τα sockets του επιπέδου μεταφοράς για όλους τους servers που επικοινωνεί το Google Drive client για να συγχρονίσει τα αρχεία σας. (2-3 λεπτά)
C. Σε ποια θύρα περιμένουν εισερχόμενα αιτήματα οι servers του Google Cloud; (1 λεπτό)
D. Με βάση την απάντηση του C και κοιτώντας την λίστα που υπάρχει στο https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/ch-ports.html ποιο είναι το πρωτόκολλο επιπέδου εφαρμογής που χρησιμοποιείται; (1-2 λεπτά)
E. Με βάση την απάντηση του D ποια παρατήρηση κάνετε σχετικά με την ασφάλεια της διαδικτυακής επικοινωνίας της εφαρμογής Google Drive. (1-2 λεπτά)

(Εκτιμώμενος χρόνος 5-9 λεπτά)

3. Wireshark (DNS, UDP)

Ανοίξτε το αρχείο καταγραφής Wireshark με την ονομασία **ihu_website.pcapng** που περιλαμβάνει όλη την διαδικτυακή επικοινωνία για την φόρτωση της κεντρικής ιστοσελίδας του Διεθνούς Πανεπιστημίου της Ελλάδας.

A. Ποια η διεύθυνση IPv4 του DNS server στον οποίο στέλνει ερωτήματα (queries) ο υπολογιστής στον οποίον έτρεξε η καταγραφή (εφαρμόστε κατάλληλο φίλτρο); (2-3 λεπτά)
B. Βρείτε την επικοινωνία κατά την οποία επιστρέφεται η IPv4 address της ιστοσελίδας του ΔΙΠΑΕ. Συγκεκριμένα αυτήν που ξεκινάει με query 0x8091 και ακολουθεί η αντίστοιχη response. Ποια είναι η port στην οποία αποστέλλεται το αίτημα και από την οποία έρχεται η απάντηση; (2-3 λεπτά).
C. Πάνω στις γραμμές που εντοπίσατε στο B: Ποιο είναι το άθροισμα ελέγχου checksum για το UDP segment της response (η απάντηση είναι στο δεκαεξαδικό σύστημα). (1 λεπτό)
D. Πάνω στις γραμμές που εντοπίσατε στο B: Πόσος χρόνος σε msecs χρειάστηκε για να φτάσει το τμήμα UDP της απόκρισης στο ερώτημα 0x8091; (1 λεπτό)
E. Παρατηρήστε ένα ερώτημα τύπου AAAA για το **gstaticadssl.l.google.com**. Τι είδους διεύθυνση σε επίπεδο δικτύου L3 επιστρέφεται στην απόκριση; (1 λεπτό)

(Εκτιμώμενος χρόνος 7-9 λεπτά)

4. Wireshark (WWW, TCP)

Ανοίξτε το αρχείο καταγραφής Wireshark με την ονομασία **ihu_website.pcapng** που περιλαμβάνει όλη την διαδικτυακή επικοινωνία για την φόρτωση της κεντρικής ιστοσελίδας του Διεθνούς Πανεπιστημίου της Ελλάδας.

A. Ποιο είναι το κατάλληλο φίλτρο ώστε να εμφανιστεί η επικοινωνία από και προς την διεύθυνση IPv4 του web server (η οποία είναι 83.212.10.28) για οποιαδήποτε πρωτόκολλο; (1 λεπτό)
B. Βρείτε την γραμμή της επικοινωνίας στην οποία ο client προσπαθεί να κατεβάσει την αρχική σελίδα από τον web server. Υπενθυμίζεται ότι η κεντρική σελίδα αναπαρίσταται ως */*. Ποιο είναι το πρωτόκολλο εφαρμογής (L5) που χρησιμοποιείται (2-3 λεπτά)

C. Στην ίδια γραμμή που βρήκατε για το B: Ποιο είναι το μέγεθος σε bytes του TCP segment; (1 λεπτό)

D. Βρείτε την γραμμή της επικοινωνίας στην οποία ο server απαντάει στον client με χαιρετισμό, δηλώνοντας τον έτσι ότι υποστηρίζει πρωτόκολλο TLSv1.2. Ποιο είναι το sequence number του επόμενου TCP segment; (1 λεπτό)

E. Μπορείτε να καταλάβετε σε ποιο σημείο της επικοινωνίας κατεβαίνει το logo του πανεπιστημίου μας; Γιατί; (3-4 λεπτά)

(Εκτιμώμενος χρόνος 7-10 λεπτά)

5. DNS - Ping

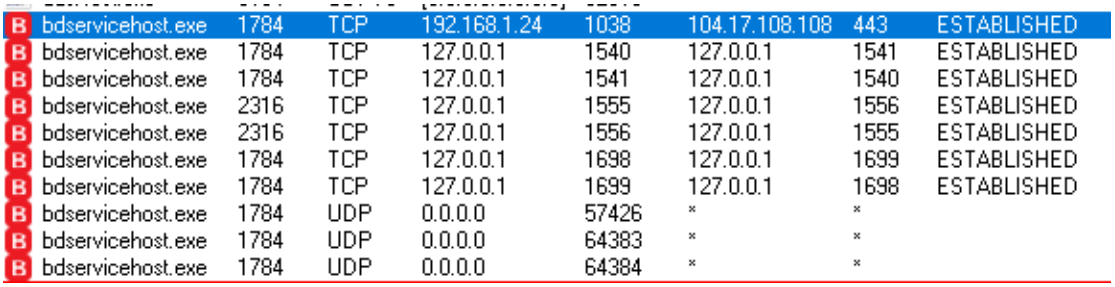
Παρακάτω εμφανίζονται τα αποτελέσματα μιας εντολής που εκτελεί ερωτήματα στο πρωτόκολλο DNS.

```
; <<>> DiG 9.14.8 <<>> ns teithe.gr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14570
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;teithe.gr.                     IN      NS

;; ANSWER SECTION:
teithe.gr.              13297   IN      NS      aetos.it.teithe.gr.
teithe.gr.              13297   IN      NS      alpha.it.teithe.gr.
teithe.gr.              13297   IN      NS      ns0.grnet.gr.
teithe.gr.              13297   IN      NS      ns1.grnet.gr.

;; Query time: 37 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Dec 15 16:18:48 GTB Standard Time 2019
;; MSG SIZE  rcvd: 123
```

A. Ποια είναι η πλήρης σύνταξη της εντολής που επιστρέφει το συγκεκριμένο είδος εγγραφών DNS για το domain **teithe.gr** (1 λεπτό)
B. Εκτελέστε την ίδια εντολή και βρείτε τους DNS servers του **ΑΠΘ (auth).** (2-3 λεπτά)
C. Αν αλλάξετε το όρισμα της εντολής που χρησιμοποιήσατε στο Β σε **mx** ποια πληροφορία θα επιστραφεί στα αποτελέσματα; (1 λεπτό)
D. Από τα αποτελέσματα των εντολών Α και Β,C που τρέξατε: Ποια η διεύθυνση IPv4 του DNS server στον οποίο στέλνει ερωτήματα (queries) ο υπολογιστής μας; (1 λεπτό)
E. Με χρήση της εντολής των ερωτημάτων A,B,C ή της εντολής **ping** βρείτε την IPv4 διεύθυνση του ιστότοπου του **ΕΜΠ (ntua).** (1 λεπτό)
(Εκτιμώμενος χρόνος 6-7 λεπτά)

6. Subnet Mask

Παρακάτω η διαδικτυακή επικοινωνία του Bitdefender Antivirus.



bdservicehost.exe	1784	TCP	192.168.1.24	1038	104.17.108.108	443	ESTABLISHED
bdservicehost.exe	1784	TCP	127.0.0.1	1540	127.0.0.1	1541	ESTABLISHED
bdservicehost.exe	1784	TCP	127.0.0.1	1541	127.0.0.1	1540	ESTABLISHED
bdservicehost.exe	2316	TCP	127.0.0.1	1555	127.0.0.1	1556	ESTABLISHED
bdservicehost.exe	2316	TCP	127.0.0.1	1556	127.0.0.1	1555	ESTABLISHED
bdservicehost.exe	1784	TCP	127.0.0.1	1698	127.0.0.1	1699	ESTABLISHED
bdservicehost.exe	1784	TCP	127.0.0.1	1699	127.0.0.1	1698	ESTABLISHED
bdservicehost.exe	1784	UDP	0.0.0.0	57426	*	*	
bdservicehost.exe	1784	UDP	0.0.0.0	64383	*	*	
bdservicehost.exe	1784	UDP	0.0.0.0	64384	*	*	

A. Ποια είναι η IPv4 του server από τον οποίον κατεβάζει updates το antivirus; (1 λεπτό)
B. Με βάση την απάντηση 1: Μπορούμε να ξέρουμε σε ποιο υποδίκτυο ανήκει έχοντας μόνο την IPv4 διεύθυνση; (1 λεπτό)
C. Με βάση την απάντηση 1: Αν ο server βρίσκεται σε ένα υποδίκτυο με άλλους 29 υπολογιστές, ποια η subnet mask και ποια η IPv4 διεύθυνση του υποδικτύου; Μπορείτε να χρησιμοποιήσετε το βοήθημα https://www.calculator.net/ip-subnet-calculator.html (1 λεπτό)
D. Με βάση την απάντηση C: Ποια είναι η IPv4 διεύθυνση για αποστολή ενός πακέτου και στους 30 υπολογιστές; (1 λεπτό)
E. Με βάση την απάντηση C: Αν χρησιμοποιούσαμε την πρώτη έγκυρη διεύθυνση IPv4 για τον router του δικτύου, ποια θα ήταν αυτή; (1 λεπτό)

(Εκτιμώμενος χρόνος 5 λεπτά)

7. Subnetting

7.1 Optimal Subnetting

Δίδεται το εύρος διευθύνσεων 193.92.224.0/22 και οι εξής ανάγκες για τα υποδίκτυα Δ1-Δ7 σε hosts (ifs): 41, 16, 29, 120, 14, 38, 80. Το πρώτο βήμα είναι να ταξινομήσουμε τις ανάγκες από το μεγαλύτερο πλήθος προς το μικρότερο.

Κωδικός	Απαίτηση σε hosts	Χωρητικότητα Υποδικτύου (hosts)	CIDR Υποδικτύου	Εύρος έγκυρων διευθύνσεων IPv4
Δ4	120			
Δ7	80			
Δ1	41			
Δ6	38			
Δ3	29			
Δ2	16			
Δ5	14			

A. Πόσους hosts χωράει το δοθέν εύρος διευθύνσεων;
B. Ποιες είναι οι αντίστοιχες χωρητικότητες που καλύπτουν με βέλτιστο τρόπο τις απαιτήσεις σε hosts που προκύπτουν από τις διαφορετικές subnet mask; Συμπληρώστε την 3η στήλη.
C. Βασιστείτε στην απάντηση B και χρησιμοποιήστε το online εργαλείο για υποδικτύωση http://www.davidc.net/sites/default/subnets/subnets.html, ξεκινώντας την ανάθεση από τις μικρότερες IP διευθύνσεις προς τις μεγαλύτερες.
D. Βασιστείτε στην εργασία που κάνατε για το C: Καταγράψτε τα CIDR των υποδικτύων.
E. Βασιστείτε στην εργασία που κάνατε για το C: Καταγράψτε τα εύρη έγκυρων διευθύνσεων IPv4.

(Εκτιμώμενος χρόνος 8-10 λεπτά)

7.2 Optimal Subnetting

Δίδεται το εύρος διευθύνσεων 192.168.128.0/21 και οι εξής ανάγκες για τα υποδίκτυα Δ1-Δ8 σε hosts (ifs): 450, 320, 100, 50, 32, 10, 7, 4

A. Πόσους hosts χωράει το συνολικό δοθέν εύρος διευθύνσεων;
B. Γράψτε τον υπολογισμό που οδηγεί στην απάντηση 1.
C. Ποιες είναι οι αντίστοιχες χωρητικότητες που καλύπτουν με βέλτιστο τρόπο τις απαιτήσεις σε hosts που προκύπτουν από τις διαφορετικές subnet mask; Συμπληρώστε την 3η στήλη.
D. Βασιστείτε στην απάντηση C και χρησιμοποιήστε το online εργαλείο για υποδικτύωση http://www.davidc.net/sites/default/subnets/subnets.html, ξεκινώντας την ανάθεση από τις μικρότερες IP διευθύνσεις προς τις μεγαλύτερες.
E. Βασιστείτε στην εργασία που κάνατε για το D: Καταγράψτε τα CIDR των υποδικτύων.

(Εκτιμώμενος χρόνος 10-12 λεπτά)

7.3 Professional Subnetting (Προαιρετικό)

Ένας πάροχος hosting ζητάει από εσάς να οργανώσετε τις διαθέσιμες IPv4 για μια μικρή web farm. Ο οργανισμός IANA του έχει δώσει το εύρος διευθύνσεων από 176.128.128.1 μέχρι και 176.128.129.254. Τα προϊόντα που διαθέτει είναι

- **DS** = 16-Core Dedicated Server hosting με 5 IP διευθύνσεις ανά blade server.
- **VPS** = Quad-Core Virtual Private Server hosting με 1 IP διεύθυνση, έχοντας 4 VPS σε κάθε blade server.

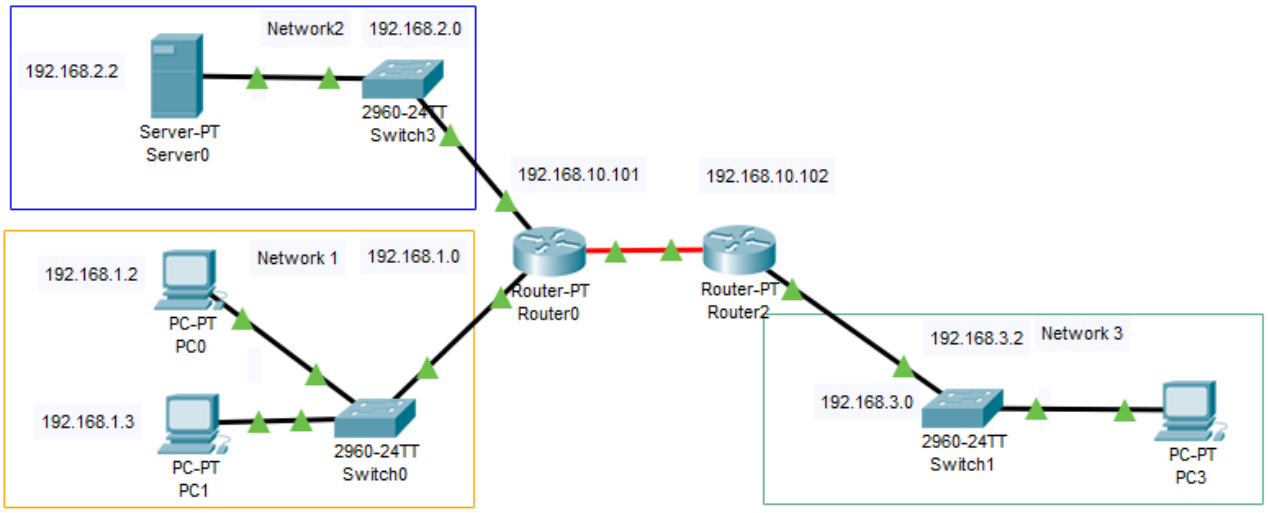
A. Πόσους hosts χωράει το συνολικό δοθέν εύρος διευθύνσεων;
B. Από τις διαθέσιμες subnet masks υποδικτύωσης: Ποια είναι η βέλτιστη χωρητικότητα για το υποδίκτυο που θα περιλαμβάνει τα προϊόντα DS, ώστε:

   a. Να κρατηθεί μια διεύθυνση IP για έναν router.
   b. Να μην σπαταληθεί ούτε μια διεύθυνση IP.
   c. Να χωρούν οι blade servers του υποδικτύου των DS σε περίβλημα blade enclosure 32 θέσεων.

C. Με βάση την επιλογή που κάνατε στο 2: Γεμίστε τις υπόλοιπες θέσεις του blade enclosure με προϊόντα VPS ώστε να κρατηθεί μια διεύθυνση IP για έναν router και να παραμείνει μία κενή. Πόσες διευθύνσεις IP αντιστοιχούν στα προϊόντα VPS και ποια η αντίστοιχη subnet mask για το υποδίκτυο των VPS;
D. Πόσα επιπλέον blade enclosures 32 θέσεων με υποδίκτυο DS και υποδίκτυο VPS μπορούν να δημιουργηθούν;
E. Με βάση τον σχεδιασμό στα B,C,D: Ποιο είναι το πλήθος των διαθέσιμο προϊόντων DS και VPS;
F. Πόσες IP παραμένουν διαθέσιμες για μελλοντική χρήση από τον πάροχο hosting.

8. Routing

Στο αρχείο SimpleNet.pkt υπάρχει ένα έτοιμο δίκτυο σε Cisco Packet Tracer ανοίξτε το και ακολουθήστε τις οδηγίες ώστε να απαντήσετε στα ερωτήματα.



A. Ρυθμίστε ανάλογα με τις IP διευθύνσεις που είναι σημειωμένες πάνω από τους Routers το δίκτυο μεταξύ των routers. Ποιες εγγραφές static route πρέπει να δημιουργήσετε στον Router0 και στον Router2 ώστε το 192.168.3.1 (PC3) να μπορεί να κάνει ping τον 192.168.2.2 (Server); Υπενθυμίζεται ότι το ping τρέχει από την καρτέλα Desktop ανοίγοντας το Command Prompt. (Εκτιμώμενος χρόνος 3-4 λεπτά)

B. Σε συνέχεια του A τρέξτε την εντολή tracert 192.168.2.2 στο Command Prompt για να δείτε την σειρά δρομολόγησης από το 192.168.3.1 (PC3) προς το 192.168.2.2 (Server). Καταγράψτε τα IP address με αύξουσα σειρά 1 ως 3. (Εκτιμώμενος χρόνος 1 λεπτό)

C. Αν τρέξετε την tracert 192.168.2.2 στο Command Prompt του 192.168.1.3 (PC1) με ποιες εγγραφές στον Router0 υλοποιείται η απευθείας δρομολόγηση που βλέπετε; (Εκτιμώμενος χρόνος 1-2 λεπτά)

(Εκτιμώμενος χρόνος 5-6 λεπτά)

9. Frame Analysis

9.1 Broadcast frame

Το αρχείο Frame1.txt περιέχει τα bytes ενός πλαισίου Ethernet σε δεκαεξαδική μορφή. Χρησιμοποιήστε το εργαλείο ανάλυσης πλαισίου https://hpd.gasmi.net/ για να απαντήσετε στα ερωτήματα.

A. Ποιος είναι ο δεκαεξαδικός κωδικός Ethertype για αυτό το πλαίσιο; (1-2 λεπτά)
B. Τα πρωτόκολλα που αντιστοιχούν στις τιμές του Ethertype και υπάρχουν στην λίστα https://en.wikipedia.org/wiki/EtherType#Examples σε ποιο επίπεδο αντιστοιχούν; (1 λεπτό)
C. Αν το πεδίο περιείχε τον κωδικό 0x86DD ποιο θα ήταν το εγκιβωτισμένο πρωτόκολλο; (1-2 λεπτά)
D. Ποια είναι η MAC address του αποστολέα του πλαισίου. (1 λεπτό)
E. Ποια είναι η IP address του παραλήπτη του πακέτου (σε διαμόρφωση decimal-dotted); (2-3 λεπτά)

(Εκτιμώμενος χρόνος 5-9 λεπτά)

9.2 Encrypted frame

Το αρχείο Frame2.txt περιέχει τα bytes ενός πλαισίου Ethernet σε δεκαεξαδική μορφή. Χρησιμοποιήστε το εργαλείο ανάλυσης πλαισίου https://hpd.gasmi.net/ για να απαντήσετε στα ερωτήματα.

A. Τι ποσοστό του πλαισίου καταλαμβάνουν τα κρυπτογραφημένα δεδομένα επιπέδου παρουσίασης L5; (1-2 λεπτά)
B. Ποιο είναι το TCP sequence number του εγκιβωτισμένου segment (στο δεκαδικό σύστημα); (1-2 λεπτά)

(Εκτιμώμενος χρόνος 2-4 λεπτά)

9.1 Broadcast frame

Το αρχείο Frame3.txt περιέχει τα bytes ενός πλαισίου Ethernet σε δεκαεξαδική μορφή. Χρησιμοποιήστε το εργαλείο ανάλυσης πλαισίου https://hpd.gasmi.net/ για να απαντήσετε στα ερωτήματα.

A. Ποιος είναι ο κωδικός αριθμός του πρωτοκόλλου μεταφοράς L4 που υπάρχει στο πεδίο protocol της κεφαλίδας του πακέτου IPv4 που είναι είναι εγκιβωτισμένο στο πλαίσιο; (1 -2 λεπτά)
B. Αν ο κωδικός του protocol ήταν 0x11 με βάση την λίστα https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers ποιο θα ήταν το πρωτόκολλο μεταφοράς L4; (1 – 2 λεπτά)

(Εκτιμώμενος χρόνος 2-4 λεπτά)