ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
Τομέας Επικοινωνιών, Ηλεκτρονικής & Συστημάτων Πληροφορικής
Εργαστήριο Διαχείρισης και Βέλτιστου Σχεδιασμού Δικτύων - NETMODE
Ηρώων Πολυτεχνείου 9, Ζωγράφου, 157 80. Τηλ: 210-772.2503, Fax: 210-772.1452
e-mail: *maglaris@netmode.ntua.gr*, URL: *http://www.netmode.ntua.gr*

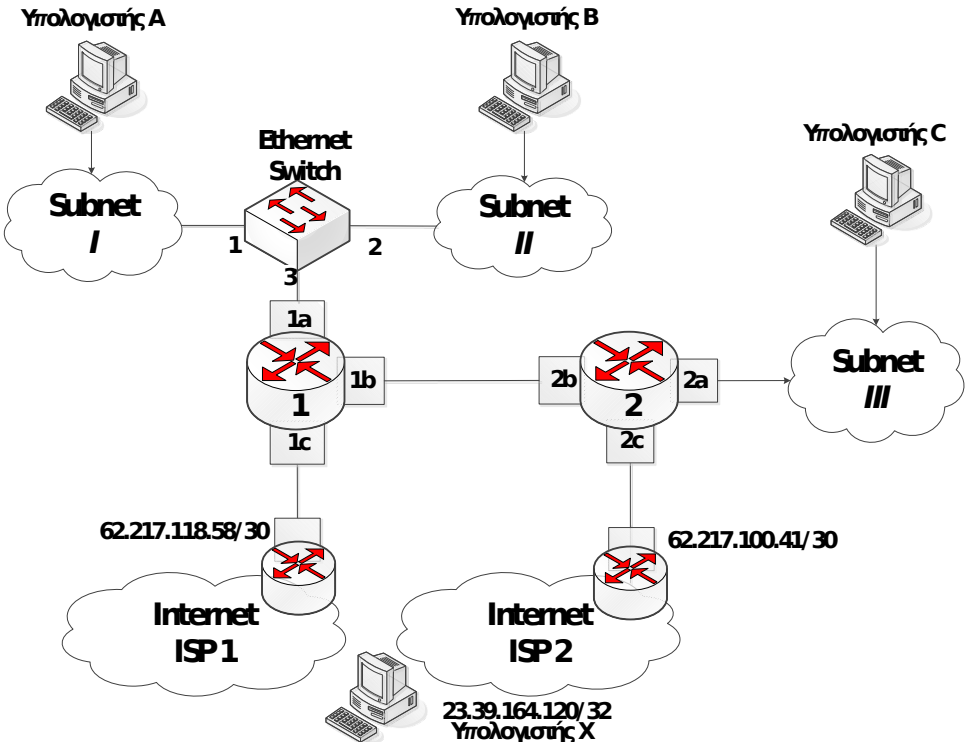
Εξέταση στο Μάθημα:
"ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ - ΕΥΦΥΗ ΔΙΚΤΥΑ"
(9ο Εξάμηνο)
Διδάσκων: Β. Μάγκλαρης
05/02/2018

Ανοικτά Βιβλία & Σημειώσεις. Διάρκεια **3 ώρες**.
Θυμίζουμε ότι οι εργαστηριακές ασκήσεις ήταν υποχρεωτικές και αποτελούν το **30%** της συνολικής βαθμολογίας. **ΚΑΛΗ ΕΠΙΤΥΧΙΑ!**

Οι βαθμοί θα ανακοινωθούν στο URL: *http://www.netmode.ntua.gr*

ΘΕΜΑ 1 (4.5 μονάδες)

Δίνεται το τοπικό δίκτυο του σχήματος, με πρόθεμα (prefix) διευθύνσεων 147.102.111.0/25, το οποίο αποτελείται από τρία διασυνδεόμενα υποδίκτυα.



Τα υποδίκτυα *I*, *II* συνδέονται πάνω στον ίδιο μεταγωγέα (Ethernet Switch) σαν δύο διαφορετικά VLAN, ένα για κάθε υποδίκτυο. Η πρόσβαση στο Internet για τα δίκτυα αυτά γίνεται μέσω του δρομολογητή (Router) 1 και του δρομολογητή (Router) του ISP 1 με IP 62.217.118.58/30. Το υποδίκτυο *III* έχει πρόσβαση στο Internet μέσω του δρομολογητή (Router) 2 και του δρομολογητή (Router) του ISP 2 με IP 62.217.100.41/30. Θεωρείστε Υπολογιστή Χ με IP 23.39.164.120, ο οποίος είναι προσβάσιμος και από τα 3 υποδίκτυα μέσω των αντιστοίχων ISPs.

Α. Ζητείται να προσδιοριστούν τα παρακάτω 4 υποδίκτυα (subnets) με την μέγιστη οικονομία διευθύνσεων:

1. Το υποδίκτυο *I* που περιλαμβάνει συνολικά 13 υπολογιστές. Ο υπολογιστής Α έχει IP 147.102.111.37.
2. Το υποδίκτυο *II* που περιλαμβάνει συνολικά 61 υπολογιστές. Ο υπολογιστής Β έχει IP 147.102.111.86.
3. Το υποδίκτυο *III* που περιλαμβάνει συνολικά 7 υπολογιστές. Ο υπολογιστής C έχει IP 147.102.111.22.
4. Το υποδίκτυο για τη σύνδεση των δρομολογητών 1, 2 (interfaces 1b, 2b). Η IP του interface 2b είναι 147.102.111.1.

Σημείωση: Η διαχειριστική IP του μεταγωγέα ανήκει στο πεδίο IP του υποδικτύου *I*

Β. Αποδώστε διευθύνσεις IP στα interfaces 1a, 1b, 1c, 2a, 2c, των δρομολογητών 1 και 2. Περιγράψτε τους πίνακες δρομολόγησης του δρομολογητή 1 και των υπολογιστών Α και C για όλα τα υποδίκτυα και το Internet στη μορφή:

Destination	Netmask	Gateway

Γ. Ποια διεύθυνση MAC προορισμού πρέπει να ενθυλακωθεί σε πακέτα που στέλνονται από τον υπολογιστή Α: (1) Προς τον υπολογιστή Β; (2) Προς τον υπολογιστή C; (3) Προς τον υπολογιστή D (όπου D τυχαίος υπολογιστής στο υποδίκτυο *I*); (4) Προς τον υπολογιστή Χ;

Έστω πως ο υπολογιστής Α στέλνει ένα ARP ερώτημα για να μάθει την διεύθυνση MAC του interface 1a του δρομολογητή 1. Θα φτάσει αυτό το ερώτημα σε κόμβο εκτός του υποδικτύου *I*; Αλλάζει κάτι στην υποθετική περίπτωση που το Ethernet Switch **δεν** υποστηρίζει VLANs;

Δ. Τι διαχειριστικές αλλαγές απαιτούνται ώστε να υπάρχει η δυνατότητα υπολογιστών που ανήκουν στα υποδίκτυα *I*, *II* να έχουν εναλλακτική δρομολόγηση από και προς το Internet μέσω του ISP 2; Τι απαιτείται ώστε να υπάρχει η δυνατότητα υπολογιστών που ανήκουν στο υποδίκτυο *III* να έχουν εναλλακτική δρομολόγηση από και προς το Internet μέσω του ISP 1;

Ε. Με ποιους μηχανισμούς μπορούμε να συνδέσουμε τους υπολογιστές Α και Χ σαν να βρίσκονται στο ίδιο υποδίκτυο;

ΣΤ. Δείξτε τα αποτελέσματα από την εκτέλεση των εντολών traceroute: (i) από τον υπολογιστή Β προς τον κόμβο nero.grnet.gr (194.177.210.54) και (ii) από τον υπολογιστή C προς τον κόμβο nero.grnet.gr (194.177.210.54). Επίσης (iii) από τον υπολογιστή Α προς τον υπολογιστή Χ θεωρώντας ότι έχει υλοποιηθεί η σύνδεση του (Ε).

(iv) Έστω ότι η σύνδεση μεταξύ των δρομολογητών 1 και 2 τίθεται προσωρινά εκτός λειτουργίας. Τι παρατηρείτε χρησιμοποιώντας την εντολή traceroute από τον υπολογιστή C προς τον υπολογιστή Α. Εξηγείστε συνοπτικά.

Σημείωση: Οι διευθύνσεις IP στις απαντήσεις δεν θα αφορούν hops στο εσωτερικό του ISP και το γενικότερο Internet.

Ζ. Ο κόμβος Α (διεύθυνση MAC 00:1e:09:45:22:c4) δέχεται Κατανεμημένη επίθεση Άρνησης Παροχής Υπηρεσίας (Distributed Denial of Service – DDoS) μέσω του ISP1. Έστω ότι οι επιτιθέμενοι βρίσκονται στο υποδίκτυο και ότι ο μεταγωγέας (Ethernet Switch) υποστηρίζει το πρωτόκολλο OpenFlow.

a) Αναφέρατε τρόπους προστασίας του κόμβου Α από την επίθεση, χρησιμοποιώντας δυνατότητες/λειτουργικότητα του δρομολογητή 1 (διεύθυνση MAC 00:08:7c:63: e4:00).
b) Περιγράψτε τους κανόνες OpenFlow (με όσο το δυνατόν περισσότερα πεδία) που πρέπει να τοποθετηθούν στον μεταγωγέα ώστε:
    1) Η φυσιολογική κίνηση να προωθείται κανονικά.
    2) Η κακόβουλη κίνηση να απορρίπτεται.

Οι κανόνες πρέπει να είναι στην μορφή:

In port	MAC src	MAC dst	Ether type	VLAN PCP	VLAN ID	IP src	IP dst	IP protocol	IP ToS	Port src	Port dst	Priority	Action

Τα πεδία Ether Type και IP Protocol μπορούν να πάρουν τις εξής τιμές:

Ether Type: 0x0800 για IPv4, 0x0806 για ARP, 0x88CC για Link Layer Discovery Protocol
IP Protocol: 1 για ICMP, 6 για TCP, 17 για UDP
Τεκμηριώστε τις απαντήσεις σας.

ΘΕΜΑ 2 (2.5 μονάδες)

Α) Δίνεται η απάντηση του DNS server dolly.netmode.ntua.gr σε σχετική ερώτηση:

```
;; QUESTION SECTION:
;karate.netmode.ntua.gr.              IN      A

;; ANSWER SECTION:
karate.netmode.ntua.gr.      86400   IN      CNAME   karate.netmode.ece.ntua.gr.
karate.netmode.ece.ntua.gr.  86400   IN      A       147.102.13.86

;; AUTHORITY SECTION:
netmode.ece.ntua.gr.         86400   IN      NS      ulysses.noc.ntua.gr.
netmode.ece.ntua.gr.         86400   IN      NS      dolly.netmode.ece.ntua.gr.

;; ADDITIONAL SECTION:
dolly.netmode.ece.ntua.gr.   86400   IN      A       147.102.13.10
ulysses.noc.ntua.gr.         83177   IN      A       147.102.222.230
ulysses.noc.ntua.gr.         74719   IN      AAAA    2001:648:2000:de::230
```

1) Τι ερώτηση έγινε προς τον server; Να ερμηνεύσετε όλες τις πληροφορίες που παρέχονται από τα Resource Records στα sections του μηνύματος που επιστρέφεται ως απάντηση από το server.

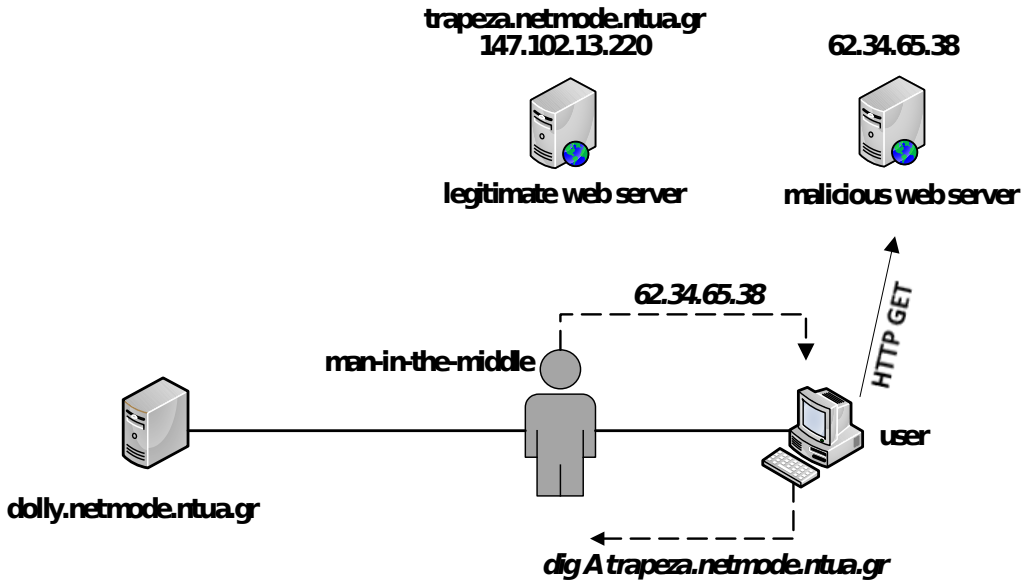
2) Μετά από κάποιο χρονικό διάστημα, η απάντηση στην ίδια ερώτηση είναι η εξής:

```
;; QUESTION SECTION:
;karate.netmode.ntua.gr.              IN      A

;; ANSWER SECTION:
karate.netmode.ntua.gr.      86400   IN      CNAME   karate.netmode.ece.ntua.gr.
karate.netmode.ece.ntua.gr.  86400   IN      A       147.102.13.86

;; AUTHORITY SECTION:
netmode.ece.ntua.gr.         86400   IN      NS      ulysses.noc.ntua.gr.
netmode.ece.ntua.gr.         86400   IN      NS      dolly.netmode.ece.ntua.gr.

;; ADDITIONAL SECTION:
dolly.netmode.ece.ntua.gr.   86400   IN      A       147.102.13.10
ulysses.noc.ntua.gr.         83127   IN      A       147.102.222.230
ulysses.noc.ntua.gr.         74669   IN      AAAA    2001:648:2000:de::230
```

Με βάση το παραπάνω, για ποιες από τις παραπάνω πληροφορίες πιστεύετε ότι ο DNS server dolly.netmode.ntua.gr είναι ο καθ' ύλην αρμόδιος (Authoritative); Να αιτιολογήσετε την απάντησή σας.

3) Ο διαχειριστής της ζώνης noc.ntua.gr αλλάζει τη διεύθυνση IP του server ulysses.noc.ntua.gr σε 147.102.222.240. Τι απάντηση θα λάβει κάποιος χρήστης εάν ρωτήσει το server dolly.netmode.ntua.gr για την IP του ulysses.noc.ntua.gr; Να αιτιολογήσετε την απάντησή σας.

B) Θεωρείστε το σενάριο που φαίνεται στο παρακάτω σχήμα. Ο χρήστης (user) θέλει να διατυπώσει ένα ερώτημα στο server dolly.netmode.ntua.gr για να λάβει τη διεύθυνση IP του trapeza.netmode.ntua.gr. Μία τρίτη κακόβουλη οντότητα παρεμβάλλεται ανάμεσα στον user και τον server. Ο σκοπός της είναι να απαντήσει στο user, προσποιούμενος τον DNS server, παραποιώντας τις απαντήσεις. Η διεύθυνση αυτή, αντί να οδηγεί τον user στο σωστό εξυπηρετητή με διεύθυνση IP 147.102.13.220 (legitimate web server), θα τον οδηγεί σε έναν κακόβουλο εξυπηρετητή (malicious web server) με διεύθυνση IP 62.34.65.38. Να απαντήσετε στις παρακάτω ερωτήσεις:



1) Υπάρχει δυνατότητα να καταλάβει ο χρήστης ότι η απάντηση προέρχεται από τον επιτιθέμενο και όχι από το server dolly.netmode.ntua.gr;

2) Με ποια διαδικασία μπορεί να διαπιστώσει ο χρήστης πως έχει συνδεθεί σε κακόβουλο web server ώστε να μην προβεί σε εισαγωγή εμπιστευτικών στοιχείων;