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 Αθήνα, Τηλ: 210-772.2503, Fax: 210-772.1452
e-mail: maglaris@netmode.ntua.gr, URL: http://www.netmode.ntua.gr

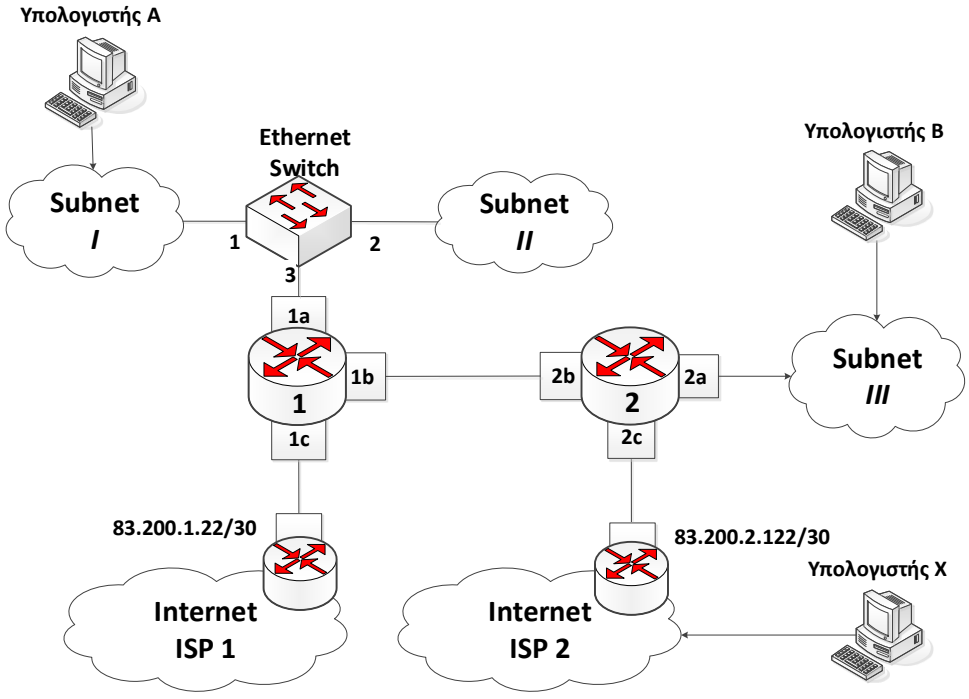
Εξέταση στο Μάθημα:
"ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ - ΕΥΦΥΗ ΔΙΚΤΥΑ"
(9ο Εξάμηνο)
Διδάσκων: Β. Μάγκλαρης
03/02/2020

Ανοικτά Βιβλία & Σημειώσεις. Διάρκεια **2.5 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 δίκτυο του σχήματος, με πρόθεμα (prefix) διευθύνσεων 147.20.0.0/22, το οποίο αποτελείται από τρία διασυνδεόμενα υποδίκτυα.



Τα υποδίκτυα *I*, *II* συνδέονται πάνω στον ίδιο μεταγωγέα (Ethernet Switch) σε 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 83.200.1.22/30. Το υποδίκτυο *III* έχει πρόσβαση στο Internet μέσω του δρομολογητή (Router) 2 και του δρομολογητή (Router) του ISP 2 με IP 83.200.2.122/30.

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

1. Το υποδίκτυο *I* που περιλαμβάνει συνολικά 254 υπολογιστές
2. Το υποδίκτυο *II* που περιλαμβάνει συνολικά 200 υπολογιστές
3. Το υποδίκτυο *III* που περιλαμβάνει συνολικά 120 υπολογιστές.
4. Το υποδίκτυο για τη σύνδεση των δρομολογητών 1, 2 (interfaces 1b, 2b). Η IP του interface 2b είναι 147.20.3.129.

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 Β για όλα τα υποδίκτυα και το Internet στη μορφή:

Destination	Netmask	Gateway

Γ. Ποια διεύθυνση MAC προορισμού πρέπει να έχουν πακέτα που στέλνονται από τον υπολογιστή Α: (1) προς οποιονδήποτε κόμβο εντός του υποδικτύου *I*; (2) προς οποιονδήποτε κόμβο εκτός του υποδικτύου *I*;

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 τα υποδίκτυα *I, II,* βρίσκονται στο ίδιο VLAN;

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 δημιουργήσουμε εικονικό δίκτυο μεταξύ των υπολογιστών Α και Χ οι οποίοι βρίσκονται σε διαφορετικές φυσικές τοποθεσίες. Εξηγείστε συνοπτικά. Επιλέξτε έναν από αυτούς τους μηχανισμούς και δείξτε αποτελέσματα από την εντολή traceroute από τον υπολογιστή Α προς τον υπολογιστή Χ.

ΣΤ. Ο υπολογιστής Α (διεύθυνση MAC 0d:1a:12:34:56:2f) δέχεται Κατανεμημένη Επίθεση Άρνησης Παροχής Υπηρεσίας (Distributed Denial of Service – DDoS) μέσω του ISP1 από υπολογιστές (bots) με διευθύνσεις από τα υποδίκτυα (i) 2.56.255.0/24, (ii) 41.93.128.0/17 και (iii) 186.65.112.0/20. Η επίθεση χρησιμοποιεί DNS απαντήσεις. Θεωρείστε ότι ο μεταγωγέας (Ethernet Switch) υποστηρίζει το πρωτόκολλο OpenFlow.

a) Περιγράψτε αναλυτικά τον τρόπο με τον οποίο θα μπορούσε ο διαχειριστής να αντιληφθεί την εισερχόμενη επίθεση (θεωρείστε αύξηση στον όγκο της κίνησης και στο πλήθος των πακέτων) χρησιμοποιώντας τις δυνατότητες του δρομολογητή). Θεωρείστε ότι το MIB ifIndex είναι ίδιο με τον αριθμό της πόρτας του δρομολογητή στο σχήμα.
b) Αναφέρατε τρόπους προστασίας του υπολογιστή Α από την επίθεση, χρησιμοποιώντας δυνατότητες/λειτουργικότητα του δρομολογητή 1.
c) Περιγράψτε τους κανόνες OpenFlow (με όσο το δυνατόν περισσότερα πεδία) που πρέπει να τοποθετηθούν στον μεταγωγέα ώστε:
    1) Η κίνηση μεταξύ του υπολογιστή Α και του δρομολογητή 1 να προωθείται κανονικά.
    2) Η κακόβουλη κίνηση προς τον υπολογιστή Α να απορρίπτεται. Αναφέρατε τρόπους με τους οποίους οι κανόνες αυτοί θα διαγραφόντουσαν αυτόματα μετά από κάποιο χρονικό διάστημα.

Σημείωση: Η διεύθυνση MAC του interface του δρομολογητή 1 που αντιστοιχεί στο υποδίκτυο *I* είναι 00:40:46:c1:12:34

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

Πιθανές χρήσιμες πληροφορίες:
Ether Type: 0x0800 (IPv4), 0x0806 (ARP), 0x88CC (Link Layer Discovery Protocol)
IP Protocol number: 1 (ICMP), 6 (TCP), 17 (UDP)
Τεκμηριώστε τις απαντήσεις σας.

Θέμα 2 (2.5 μονάδες)

Α) Δίνεται παρακάτω η απάντηση ενός εξυπηρετητή DNS σε αντίστοιχη ερώτηση χρήστη:

```
;; QUESTION SECTION:
;ntua.gr.       IN      SOA

;; ANSWER SECTION:
ntua.gr.        86400   IN      SOA     achilles.noc.ntua.gr.   noc.ntua.gr. (
                2020012001 ; serial             43200   ; refresh (12 hours)
                3600    ; retry (1 hour)
                604800  ; expire (1 week)       86400   ; minimum (1 day)
        )

;; AUTHORITY SECTION:
ntua.gr.                86400   IN      NS      sns1.grnet.gr.
ntua.gr.                86400   IN      NS      sns0.grnet.gr.
ntua.gr.                86400   IN      NS      achilles.noc.ntua.gr.
ntua.gr.                86400   IN      NS      ulysses.noc.ntua.gr.
ntua.gr.                86400   IN      NS      diomedes.noc.ntua.gr.

;; ADDITIONAL SECTION:
ulysses.noc.ntua.gr.    86400   IN      A       147.102.222.230
achilles.noc.ntua.gr.   86400   IN      A       147.102.222.210
diomedes.noc.ntua.gr.   86400   IN      A       147.102.222.220
ulysses.noc.ntua.gr.    86400   IN      AAAA    2001:648:2000:de::230
achilles.noc.ntua.gr.   86400   IN      AAAA    2001:648:2000:de::210
diomedes.noc.ntua.gr.   600     IN      AAAA    2001:648:2000:de::220

;; Query time: 40 msec
;; SERVER: 147.102.222.230#53(147.102.222.230)
```

1) Σε ποιον εξυπηρετητή DNS έγινε η ερώτηση; Ποια ήταν η ερώτηση αυτή;

2) Να περιγράψετε τις πληροφορίες που παρέχονται από τα Resource Records στο ADDITIONAL SECTION της απάντησης.

3) Να εξηγήσετε ποιοι εξυπηρετητές DNS είναι Αρμόδιοι (Authoritative) για τη ζώνη ntua.gr. Από αυτούς, ποιος/ποιοι είναι master/primary και ποιοι slave για τη ζώνη ntua.gr; Να εξηγήσετε την απάντησή σας.

4) Ποιον τύπο ερωτήματος DNS χρησιμοποιούν οι slave εξυπηρετητές για να λάβουν τη ζώνη ntua.gr από τον/τους master εξυπηρετητές σε τακτά χρονικά διαστήματα και τι πρωτόκολλο στρώματος μεταφοράς (UDP, TCP) χρησιμοποιείται; Ποιο πεδίο της εγγραφής SOA συμβουλεύονται οι slave για να μάθουν αν θα ζητήσουν μεταφορά ζώνης ή όχι, δηλαδή αν πραγματοποιήθηκε κάποια αλλαγή στη ζώνη;

Β) Θέλετε να επισκεφθείτε την ιστοσελίδα www.trapeza.gr από έναν υπολογιστή εντός του ΕΜΠ. Για το σκοπό αυτό, πληκτρολογείτε στο browser σας τις παρακάτω διευθύνσεις:

- http://www.trapeza.gr
- https://www.trapeza.gr

1) Θεωρώντας ότι, αρχικά, οι σχετικές caches του υπολογιστή σας δεν έχουν εγγραφές πριν από κάθε ερώτηση, να περιγράψετε και να δικαιολογήσετε τα μηνύματα που θα στείλετε και θα λάβετε τη στιγμή που επισκέπτεστε κάθε μία από τις παραπάνω ιστοσελίδες. Να θεωρήσετε ότι χρησιμοποιείτε ως DNS server τον dolly.netmode.ntua.gr.

2) Σε ποια από τις παραπάνω περιπτώσεις μπορείτε να επιβεβαιώσετε ότι συνδεθήκατε στη σωστή ιστοσελίδα και με ποιο τρόπο;