|  |  |
| --- | --- |
|  | **ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ**ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝΤομέας Επικοινωνιών, Ηλεκτρονικής & Συστημάτων ΠληροφορικήςΕργαστήριο Διαχείρισης και Βέλτιστου Σχεδιασμού Δικτύων - NETMODE Ηρώων Πολυτεχνείου 9, Ζωγράφου, 157 80 Αθήνα, Τηλ: 210-772.2503, Fax: 210-772.1452e-mail: maglaris@netmode.ntua.gr, URL: http://www.netmode.ntua.gr  |

Εξέταση στο Μάθημα:

 "ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ - ΕΥΦΥΗ ΔΙΚΤΥΑ"

(9ο Εξάμηνο)

Διδάσκων: Β. Μάγκλαρης

**01/02/2019**

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 τοπικό δίκτυο του σχήματος, με πρόθεμα (prefix) διευθύνσεων 83.212.16.0/23, 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 53.217.118.66/30. Το υποδίκτυο *ΙΙΙ* έχει πρόσβαση στο Internet μέσω του δρομολογητή (Router) 2 και του δρομολογητή (Router) του ISP 2 με IP 53.217.100.14/30.

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

1. Το υποδίκτυο *I* που περιλαμβάνει συνολικά 126 υπολογιστές
2. Το υποδίκτυο *II* που περιλαμβάνει συνολικά 100 υπολογιστές
3. Το υποδίκτυο *III* που περιλαμβάνει συνολικά 31 υπολογιστές.
4. Το υποδίκτυο για τη σύνδεση των δρομολογητών 1, 2 (interfaces 1b, 2b). Η IP του interface 2b είναι 83.212.17.193.

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 A και C 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 A: (1) Προς τον υπολογιστή B; (2) Προς τον υπολογιστή C; (3) Προς τον υπολογιστή D;

Έστω πως ο υπολογιστής A 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 *Ι*, *ΙΙ* 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 *ΙΙΙ* 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.

ΣΤ. Δείξτε τα αποτελέσματα από την εκτέλεση των εντολών traceroute: (i) από τον υπολογιστή B 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 A προς τον υπολογιστή Χ θεωρώντας ότι συνδέονται εικονικά σε επίπεδο 2.

(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 υπολογιστής Α (διεύθυνση MAC 00:1e:09:45:22:c4) δέχεται Κατανεμημένη Επίθεση Άρνησης Παροχής Υπηρεσίας (Distributed Denial of Service – DDoS) μέσω του ISP1 από υπολογιστές (bots) από τα υποδίκτυα (i) 27.112.32.0/19 , (ii) 31.11.43.0/24 και (iii) 45.170.228.0/22. Θεωρείστε ότι ο μεταγωγέας (Ethernet Switch) υποστηρίζει το πρωτόκολλο OpenFlow.

1. Καταγράψτε τη διαδικασία μέσω SNMP με την οποία ο διαχειριστής μπορεί να ανακτήσει την τιμή των bits/sec και packets/sec που διέρχονται από τον μεταγωγέα (Ethernet Switch). Θεωρείστε ότι το ifIndex είναι ίδιο με τον αριθμό της πόρτας στο σχήμα.
2. Αναφέρατε τρόπους προστασίας του υπολογιστή Α από την επίθεση, χρησιμοποιώντας δυνατότητες/λειτουργικότητα του δρομολογητή 1.
3. Περιγράψτε τους κανόνες OpenFlow (με όσο το δυνατόν περισσότερα πεδία) που πρέπει να τοποθετηθούν στον μεταγωγέα ώστε:
4. Η κίνηση μεταξύ του υπολογιστή Α και του δρομολογητή 1 να προωθείται κανονικά (Να χρησιμοποιηθεί το Action NORMAL).
5. Η κακόβουλη κίνηση να απορρίπτεται.

Σημείωση: Η διεύθυνση MAC του interface του δρομολογητή 1 που αντιστοιχεί στο υποδίκτυο *I* είναι 00:50:56:c0:00:08

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:
;noc.ntua.gr.              IN     MX

;; ANSWER SECTION:
noc.ntua.gr.      86400      IN      MX      10 achilles.noc.ntua.gr.
noc.ntua.gr.       86400      IN      MX      10 ulysses.noc.ntua.gr.
noc.ntua.gr.       86400      IN      MX      10 diomedes.noc.ntua.gr.

;; AUTHORITY SECTION:
noc.ntua.gr.       2358      IN      NS      diomedes.noc.ntua.gr.
noc.ntua.gr.       2358      IN      NS      achilles.noc.ntua.gr.
noc.ntua.gr.       2358      IN      NS      ulysses.noc.ntua.gr.

;; ADDITIONAL SECTION:
achilles.noc.ntua.gr.       818      IN      A      147.102.222.210
achilles.noc.ntua.gr. 85126      IN      AAAA      2001:648:2000:de::210
ulysses.noc.ntua.gr. 22     IN     A     147.102.222.230
ulysses.noc.ntua.gr.     85126     IN     AAAA  2001:648:2000:de::230
diomedes.noc.ntua.gr.     2358     IN     A     147.102.222.220
diomedes.noc.ntua.gr.     303     IN     AAAA  2001:648:2000:de::220

;; Query time: 3 msec
;; SERVER: 147.102.13.10#53(147.102.13.10)

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

2) Να ερμηνεύσετε όλες τις πληροφορίες που παρέχονται από τα *Resource Records* στα sections του μηνύματος που επιστράφηκε ως απάντηση.

3) Μετά από 5 δευτερόλεπτα, ο χρήστης επαναλαμβάνει την ίδια ερώτηση. Τι διαφορές θα παρατηρήσετε ανάμεσα στις δύο απαντήσεις; Να δικαιολογήσετε την απάντησή σας.

Β) Να θεωρήσετε το σενάριο του παρακάτω σχήματος:



Σε αυτό το σενάριο, ο χρήστης *User* θέλει να μάθει τη διεύθυνση IP του *Web Server* που φιλοξενεί την ιστοσελίδα *www.trapeza.gr*. Ο χρήστης *User* γνωρίζει ότι ο καθ’ ύλην αρμόδιος (authoritative) εξυπηρετητής DNS της ζώνης *trapeza.gr* είναι ο *ns.trapeza.gr*. Επίσης, γνωρίζει τη διεύθυνση IP του αναδρομικού (recursive) εξυπηρετητή DNS *dolly.netmode.ece.ntua.gr*, τον οποίο χρησιμοποιεί για να διατυπώνει αναδρομικά ερωτήματα DNS.

Για να μάθει τη διεύθυνση IP του *Web Server* που φιλοξενεί την ιστοσελίδα *www.trapeza.gr*, ο χρήστης *User* διατυπώνει το παρακάτω ερώτημα:

**dig A www.trapeza.gr. @ns.trapeza.gr.**

1) Θεωρώντας ότι, αρχικά, οι σχετικές caches του χρήστη *User* είναι άδειες, να περιγράψετε και να δικαιολογήσετε τα μηνύματα που θα στείλει και θα λάβει ο *User* από τη στιγμή που διατυπώνει το παραπάνω ερώτημα DNS μέχρι να μάθει τη διεύθυνση IP του *Web Server* που φιλοξενεί την ιστοσελίδα *www.trapeza.gr*.

2) Περιγράψτε συνοπτικά τη διαδικασία με την οποία μπορεί να επιβεβαιώσει ο χρήστης *User* ότι έχει πράγματι συνδεθεί στην ιστοσελίδα της τράπεζάς του και όχι σε κάποια άλλη κακόβουλη ιστοσελίδα;