Εργαστηριακή Άσκηση 6
Πρωτόκολλα ARP και ICMP

Ο σκοπός αυτού του εργαστηρίου είναι η περαιτέρω εξέταση των πρωτοκόλλων ARP, IP και ICMP μέσω της καταγραφής και παρατήρησης των περιεχομένων των πακέτων που ανταλλάσσονται κατά τη διάρκεια της χρήσης των εντολών `ping` και `tracert`.

Όπως και στο προηγούμενο εργαστήριο, θα εργαστείτε με το πρόγραμμα Wireshark. Εδώ θα χρησιμοποιήσετε τη λειτουργία *Capture* με φίλτρο, ώστε τα πλαίσια που καταγράφονται να περιέχουν κάποια συγκεκριμένα χαρακτηριστικά. Υπενθυμίζεται ότι το φίλτρο απεικόνισης *(Display)*, που επιλέγετε από το μενού *Analyze,* μπορεί να (απ)ενεργοποιηθεί οποιαδήποτε στιγμή κατά τη διάρκεια της καταγραφής, καθώς επίσης και μετά την ολοκλήρωση αυτής, προκειμένου να αποκρύπτει (αποκαλύπτει) κάποια από τα συλληφθέντα πλαίσια, ενώ το φίλτρο σύλληψης, που επιλέγετε από το μενού *Capture*, ενεργοποιείται πάντοτε **πριν** ξεκινήσει η διαδικασία καταγραφής, με αποτέλεσμα να καταγράφεται μόνο ένα μέρος των διερχόμενων πλαισίων. Πληροφορίες για τη σύνταξη του φίλτρου σύλληψης μπορείτε να βρείτε στην ιστοθέση http://wiki.wireshark.org/CaptureFilters. Για να κάνετε μια καταγραφή με φίλτρο, από το μενού *Capture->Options…* στο παράθυρο που θα εμφανισθεί και στο πεδίο δίπλα από το κουμπί "*Capture Filter*" πληκτρολογήστε μια λογική έκφραση σύμφωνη με τη σύνταξη των φίλτρων καταγραφής και πιέστε *Start* για να αρχίσει η καταγραφή. Για τη δομή των επικεφαλίδων των πρωτοκόλλων της σουίτας TCP/IP συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default0604.htm επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο που σας ενδιαφέρει.

1 Εντολή `ping` στο τοπικό υποδίκτυο

Προτού ξεκινήσετε την άσκηση αδειάστε τον πίνακα arp του υπολογιστή σας εκτελώντας την εντολή `arpclear` σε ένα παράθυρο εντολών (η `arpclear` είναι ισοδύναμη με την `arp -d` την οποία, όμως, ο χρήστης labuser δε μπορεί να εκτελέσει ελλείψει δικαιωμάτων). Στη συνέχεια δημιουργήστε ένα φίλτρο σύλληψης, ώστε να καταγράφονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση MAC του υπολογιστή σας. Καταγράψτε τα διερχόμενα πλαίσια όταν κάνετε `ping` σε υπολογιστή του *τοπικού δικτύου*, π.χ. κάποιον διπλανό σας. Να χρησιμοποιηθεί η εντολή `ping <διεύθυνση IP>`. ***Προσοχή****: Συνεννοηθείτε με διπλανό σας ώστε να μην κάνετε ping ταυτόχρονα ο ένας προς τον άλλο!* Παρατηρείστε τον πίνακα arp μετά από την εκτέλεση της εντολής `ping`. Αφού τελειώσει η καταγραφή, εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

1.1 Καταγράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε ώστε να συλλαμβάνονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση MAC του υπολογιστή σας.

1.2 Καταγράψτε τη σύνταξη της εντολής που χρησιμοποιήσατε για να ελέγξετε τα περιεχόμενα του πίνακα arp του υπολογιστή σας.

1.3 Καταγράψτε τη σύνταξη του φίλτρου απεικόνισης ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

1.4 Με τη βοήθεια του πίνακα arp στο παράθυρο εντολών και της καταγραφής πακέτων που κάνατε παραπάνω, εξηγείστε τον σκοπό των πακέτων πρωτοκόλλου ARP που ανταλλάχθηκαν.

1.5 Πόσα μηνύματα τύπου Echo request του πρωτοκόλλου ICMP παρατηρήσατε;

1.6 Εξετάζοντας την επικεφαλίδα IP των προηγούμενων μηνυμάτων ICMP προσδιορίστε το όνομα του πεδίου της επικεφαλίδας και την τιμή του που προσδιορίζει το πρωτόκολλο ICMP.

1.7 Καταγράψτε την τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας ICMP των μηνυμάτων Echo request.
1.8 Καταγράψτε τις τιμές των πεδίων ταυτότητας (Identifier) και του αύξοντα αριθμού (Sequence number) της επικεφαλίδας ICMP ***ενός*** μηνύματος Echo request.
1.9 Εκτός από τα προηγούμενα πεδία, ποια άλλα πεδία περιλαμβάνει η επικεφαλίδα ICMP;
1.10 Ποιο είναι το μήκος της επικεφαλίδας των μηνυμάτων ICMP τύπου Echo request;
1.11 Ποιο είναι το μήκος και ποιο το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP τύπου Echo request που παράγει η εντολή `ping`;
1.12 Πόσα μηνύματα τύπου Echo reply του πρωτοκόλλου ICMP λάβατε;
1.13 Εξετάζοντας την επικεφαλίδα IP των προηγούμενων μηνυμάτων ICMP προσδιορίστε τον κωδικό που προσδιορίζει το πρωτόκολλο ICMP. Είναι ίδιος με αυτόν της ερώτησης 1.6;
1.14 Καταγράψτε την τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας ICMP των μηνυμάτων Echo reply.
1.15 Με βάση τις απαντήσεις σας στις ερωτήσεις 1.7 και 1.14, ποιο από τα πεδία Type και Code καθορίζει το κατά πόσο πρόκειται για μήνυμα Echo request ή Echo reply;
1.16 Καταγράψτε τις τιμές των πεδίων ταυτότητας (Identifier) και του αύξοντα αριθμού (Sequence number) της επικεφαλίδας ICMP της απάντησης Echo reply στο μήνυμα Echo request που εξετάσατε για την απάντηση της ερώτησης 1.8.
1.17 Ποιος είναι ο ρόλος των πεδίων ταυτότητας και του αύξοντα αριθμού στην επικεφαλίδα ICMP των μηνυμάτων Echo; *[Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default0604.htm επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο ICMP στο δεξιό της μέρος. Διαβάστε τις λεπτομέρειες που αφορούν τα μηνύματα ICMP τύπου Echo request]*
1.18 Ποιο είναι το μήκος της επικεφαλίδας μηνυμάτων ICMP τύπου Echo reply;
1.19 Ποιο είναι το μήκος και ποιο το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP τύπου Echo reply που παράγει η εντολή `ping`;
1.20 Διαφέρει αυτό το περιεχόμενο από το αντίστοιχο του μηνύματος ICMP τύπου Echo request;
1.21 Πώς σχετίζονται οι ανταλλαγές των μηνυμάτων ICMP με τα αποτελέσματα της εντολής ping στο παράθυρο εντολών;

Ξεκινήστε πάλι τη διαδικασία καταγραφής των πακέτων με το ίδιο φίλτρο σύλληψης και εκτελέστε την εντολή `ping` προς μια διεύθυνση IP του υποδικτύου σας που **δεν** αντιστοιχεί σε ενεργό υπολογιστή. Για να βρείτε μια τέτοια διεύθυνση, δοκιμάστε στην τύχη διευθύνσεις IP του υποδικτύου σας. Αφού τελειώσει η καταγραφή, εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

1.22 Πόσα πακέτα ARP request στάλθηκαν για την επίλυση της διεύθυνσης του μη ενεργού υπολογιστή;
1.23 Κάθε πότε στέλνονται; *[Υπόδειξη: Από το μενού View μπορείτε να επιλέξετε Time Display Format → Seconds Since Previous Captured Packet.]*
1.24 Πόσα μηνύματα ICMP στάλθηκαν;
1.25 Πώς σχετίζονται τα προηγούμενα με τα αποτελέσματα της εντολής ping στο παράθυρο εντολών;

2 Εντολή `ping` σε άλλο υποδίκτυο

Προτού ξεκινήσετε την άσκηση, παρατηρείστε τον πίνακα arp του υπολογιστή σας. Στη συνέχεια, χρησιμοποιώντας το φίλτρο σύλληψης των προηγούμενων ερωτήσεων, καταγράψτε τα διερχόμενα πλαίσια όταν κάνετε `ping` σε έναν υπολογιστή εκτός του τοπικού δικτύου. Για το σκοπό αυτό, χρησιμοποιείστε την εντολή `ping` σε **μία** από τις ακόλουθες διευθύνσεις `147.102.1.1` ή `147.102.7.1` ή `147.102.40.1`. Αφού τελειώσει η καταγραφή εφαρμόστε φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

2.1 Επιλέξτε ένα μήνυμα ICMP τύπου Echo request. Καταγράψτε τη διεύθυνση MAC του αποστολέα και του παραλήπτη του αντίστοιχου πλαισίου.
2.2 Καταγράψτε τις διευθύνσεις IP (αποστολέα και παραλήπτη) του πακέτου IP που μεταφέρει το μήνυμα ICMP τύπου Echo request;
2.3 Οι παραπάνω διευθύνσεις MAC σε ποιες διευθύνσεις IP αντιστοιχούν; *[Υπόδειξη: Χρησιμοποιείστε την εντολή* `ipconfig /all` *και τον πίνακα arp]*.
2.4 Παρατηρήσατε πακέτα πρωτοκόλλου ARP κατά την καταγραφή;
2.5 Αν ναι, ποιος ήταν ο σκοπός τους; Εάν όχι, αιτιολογήστε γιατί δεν υπήρξαν.

Αφού απενεργοποιήσετε το προηγούμενο φίλτρο απεικόνισης, εφαρμόστε ένα νέο φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο μηνύματα ICMP τύπου Echo request.

2.6 Να καταγραφεί η σύνταξη του φίλτρου. *[Υπόδειξη: Συμβουλευτείτε τις απαντήσεις σας στις ερωτήσεις 1.7 και 1.15]*
2.7 Κάθε πότε στέλνονται τα μηνύματα Echo request του πρωτοκόλλου ICMP; *[Υπόδειξη: Από το μενού View μπορείτε να επιλέξετε Time Display Format → Seconds Since Previous Captured Packet.*

Αφού απενεργοποιήσετε το προηγούμενο φίλτρο απεικόνισης, εφαρμόστε ένα νέο φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο μηνύματα ICMP τύπου Echo reply.

2.8 Να καταγραφεί η σύνταξη του. *[Υπόδειξη: Συμβουλευτείτε τις απαντήσεις σας στις ερωτήσεις 1.14 και 1.15]*
2.9 Παρατηρώντας την επικεφαλίδα των πακέτων IP που μεταφέρουν το μήνυμα ICMP τύπου Echo reply, εξηγείστε πώς προκύπτει η τιμή της παραμέτρου TTL που εμφανίζεται στις απαντήσεις του παραθύρου εντολών.

Ξεκινήστε μια νέα καταγραφή με το προηγούμενο φίλτρο σύλληψης, όταν εκτελείτε την εντολή `ping` σε έναν υπολογιστή **εκτός του υποδικτύου σας**, που δεν είναι ενεργός (π.χ. στον `147.102.40.20`). Όταν τελειώσει η καταγραφή εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

2.10 Ποιοι τύποι μηνυμάτων ICMP εμφανίζονται;
2.11 Κάθε πότε στέλνονται τα μηνύματα τύπου Echo request του πρωτοκόλλου ICMP;
2.12 Σε τι διαφέρει η κίνηση που καταγράψατε σε σχέση με την αντίστοιχη όταν εκτελέσατε την `ping` προς μια διεύθυνση IP εντός του υποδικτύου σας, που δεν αντιστοιχεί σε ενεργό υπολογιστή (ερώτημα 1). Αιτιολογήστε τη διαφορά.

3 Εντολή `tracert`

Στην εργαστηριακή άσκηση 4 είδατε ότι η διαδρομή που ακολουθεί ένα πακέτο στο διαδίκτυο, μπορεί να ανιχνευθεί με την εντολή `tracert`. Μπορείτε όμως να λάβετε τα ίδια αποτελέσματα και με διαδοχικές εκτελέσεις της εντολής `ping`.

Ξεκινήστε μια νέα καταγραφή της δικτυακής κίνησης χρησιμοποιώντας το προηγούμενο φίλτρο σύλληψης, όταν εκτελείτε την εντολή `ping –n 1 –i X www.edet.gr`. Ξεκινήστε θέτοντας την τιμή της παραμέτρου `X = 1` και αυξήστε τη διαδοχικά κατά 1 μέχρι να παύσει να εμφανίζεται το μήνυμα `TTL expired in transit`. Όταν τελειώσει η καταγραφή εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

3.1 Την τιμή ποιου πεδίου της επικεφαλίδας IP επηρεάζει η τιμή της παραμέτρου `X`;
3.2 Ποια είναι η ελάχιστη τιμή της παραμέτρου `X` για να φτάσει το πακέτο στον εξυπηρετητή ιστού `www.edet.gr`;
3.3 Σχεδιάστε ένα απλό διάγραμμα της διαδρομής μέχρι τον κόμβο `www.edet.gr` όπου να εμφανίζονται οι διευθύνσεις IP των ενδιάμεσων κόμβων. *[Υπόδειξη: Μπορείτε να απαντήσετε με τη βοήθεια του παραθύρου εντολών, παρατηρώντας τη διεύθυνση IP του αποστολέα της*

απάντησης `Reply from <IP address>: ...` *που εμφανίζεται για κάθε διαδοχική εκτέλεση της* `ping`*.]*

3.4 Ποιον άλλο τύπο μηνύματος ICMP παρατηρείτε;

3.5 Ποια είναι η τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας ICMP για το προηγούμενο είδος μηνυμάτων ICMP;

3.6 Ποιο είναι το μήκος και ποιο το περιεχόμενο του πεδίου δεδομένων του προηγούμενου μηνύματος ICMP; *[Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default0604.htm επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο ICMP στο δεξιό της μέρος. Διαβάστε τις λεπτομέρειες που αφορούν τα μηνύματα ICMP τύπου Time exceeded]*

Χρησιμοποιώντας το φίλτρο σύλληψης των προηγούμενων ερωτήσεων, καταγράψτε τη δικτυακή κίνηση όταν εκτελείτε την εντολή `tracert -d www.edet.gr`. Όταν τελειώσει η καταγραφή εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

3.7 Πόσες τριάδες ICMP μηνυμάτων αποστέλλονται και πόσες λαμβάνονται;

3.8 Τι αποτέλεσμα έχει η επιλογή `-d` κατά την κλήση της `tracert`;

3.9 Καταγράψτε την τιμή του πεδίου Protocol της επικεφαλίδας IP ενός μηνύματος ICMP τύπου Echo request που στέλνεται κατά την κλήση της `tracert`.

3.10 Για κάθε τριάδα μηνυμάτων καταγράψτε τη διεύθυνση IP του παραλήπτη του μηνύματος ICMP τύπου Echo Request και τη διεύθυνση IP από όπου έρχεται η απάντηση.

3.11 Καταγράψτε τις τιμές του πεδίου *time to live (TTL)* του πακέτου IP για κάθε τριάδα μηνυμάτων ICMP Echo Request.

3.12 Καταγράψτε τις αντίστοιχες τιμές του πεδίου *time to live (TTL)* για κάθε τριάδα απαντήσεων.

3.13 Γιατί οι πρώτοι κόμβοι της διαδρομής απαντούν με μήνυμα ICMP τύπου Time Exceeded, ενώ ο τελευταίος με ICMP τύπου Echo Reply;

3.14 Ποιο είναι το μήκος και το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP τύπου Echo request που παράγει η εντολή `tracert`;

3.15 Συγκρίνετε το παραπάνω μήκος και περιεχόμενο του πεδίου δεδομένων με τα αντίστοιχα στην περίπτωση της εντολής `ping` (Ερώτηση 1.11);

Η παροχή τέτοιας λεπτομερούς πληροφόρησης σχετικά με τη διαδρομή των πακέτων ήταν αποδεκτή στις αρχικές ημέρες του διαδικτύου. Αργότερα όμως άρχισε να θεωρείται προβληματική για λόγους ασφαλείας. Η πληροφόρηση που μπορεί να λάβει κανείς μέσω της εντολής `ping` χρησιμοποιήθηκε από ιούς και σκουλήκια για να εντοπίσουν πιθανούς στόχους για την εξάπλωσή τους. Επίσης, η `tracert` χρησιμοποιήθηκε συχνά από χάκερς για να αποκτήσουν γνώση σε σχέση με την αρχιτεκτονική (εταιρικών) δικτύων και στη συνέχεια να εκμεταλλευθούν πιθανές τρωτότητες κόμβων ή υπολογιστών. Γι' αυτό αρκετά δίκτυα άρχισαν να φιλτράρουν στα όρια τους τα μηνύματα ICMP τύπου *Echo Request*. Έτσι, εν γένει, μπορεί κάποιος να βρει τη διαδρομή μέχρι την άκρη ενός (εταιρικού) δικτύου, αλλά όχι τη διαδρομή στο εσωτερικό του.

Αντίστοιχα, σε λειτουργικά συστήματα όπως τα Windows XP SP2 η προκαθορισμένη επιλογή είναι φιλτράρουν τα μηνύματα ICMP τύπου Echo Request, παρότι το πρότυπο RFC 1122 ορίζει ότι κάθε υπολογιστής (host) πρέπει να δέχεται τα μηνύματα ICMP τύπου *Echo Request* και να απαντά με ICMP τύπου *Echo Reply*. Παρόλα αυτά αμφότερες οι εντολές είναι χρήσιμα διαγνωστικά εργαλεία και βοηθούν αρκετές φορές στην επίλυση προβλημάτων (δρομολόγησης) ή στην εύρεση των πλησιέστερων κόμβων π.χ. για το κατέβασμα δημοφιλών αρχείων.

Είναι σημαντικό όμως να γίνει κατανοητό ότι η βάση λειτουργίας της εντολής `tracert` δεν είναι η απάντηση στο μήνυμα ICMP τύπου *Echo Request*, αλλά η παραγωγή της ένδειξης σφάλματος (TTL expired in transit) που σχετίζεται με την επικεφαλίδα του πακέτου IP. Έτσι η αντίστοιχη υλοποίηση της εντολής `tracert` των Windows, στα λειτουργικά συστήματα Unix/Linux, που ονομάζεται `traceroute`, παρουσιάζει την εξής διαφορά: αντί να στέλνει μια σειρά από

μηνύματα ICMP τύπου *Echo request* στον προορισμό, όπως συμβαίνει στα Windows, χρησιμοποιεί δεδομενογράμματα UDP με θύρα προορισμού στην περιοχή από 33434 έως 33534. Και στις δύο υλοποιήσεις, η τιμή της παραμέτρου Time-to-live (TTL) κάθε πακέτου αρχίζει από την τιμή 1 και αυξάνεται κατά 1 για κάθε διαδοχική αποστολή. Κάθε δρομολογητής κατά μήκος της διαδρομής προς τον προορισμό, μειώνει το TTL κατά 1, προτού προωθήσει το πακέτο. Όταν το TTL μηδενισθεί, ο δρομολογητής οφείλει να στείλει μήνυμα ICMP τύπου *Time Exceeded* στην πηγή. Η διαδρομή βρίσκεται εξετάζοντας τα μηνύματα *Time Exceeded*. Αξίζει να τονιστεί ότι η παράμετρος TTL, άσχετα με ό,τι υποδηλώνει το όνομα της, δεν έχει καμία σχέση με χρονική διάρκεια. Εκφράζει απλά το μέγιστο αριθμό κόμβων από τους οποίους μπορεί να περάσει ένα πακέτο IP μέχρι τον προορισμό του, άσχετα από τη χρονική διάρκεια του ταξιδιού αυτού. Ας σημειωθεί ότι στο Unix/Linux, η εντολή `traceroute` μπορεί επίσης να χρησιμοποιήσει το πρωτόκολλο ICMP αν κληθεί με την επιλογή `-I`, ενώ οι πιο πρόσφατες υλοποιήσεις της μπορούν να χρησιμοποιήσουν και το πρωτόκολλο TCP με την επιλογή –T. Με τη χρήση TCP σε αρκετές περιπτώσεις είναι δυνατό να διαπεραστούν τα τείχη πυρασφάλειας (firewalls) μέσω θυρών που είναι ανοικτές για τους υπολογιστές που βρίσκονται πίσω τους, στέλνοντας τεμάχια TCP SYN, αντί δεδομενογράμματα UDP ή μηνύματα ICMP τύπου *Echo Request*.

3.16 Ποια θα ήταν η τιμή του πεδίου Protocol του αντίστοιχου πακέτου IP, εάν αντί της εντολής `tracert` είχε χρησιμοποιηθεί η `traceroute` (από Unix/Linux);

3.17 Γιατί τα μηνύματα ICMP δεν περιλαμβάνουν αριθμό θύρας πηγής και προορισμού;

4 IP options

Πληροφορίες για τη διαδρομή στο δίκτυο μπορεί να λάβει κανείς και μέσω της επικεφαλίδας των πακέτων IP! Η πλειονότητα των πακέτων IP περιλαμβάνουν τη συνήθη επικεφαλίδα των 20 byte με τα πεδία που είδατε στις προηγούμενες ασκήσεις. Οι δημιουργοί του IPv4 όμως προέβλεψαν τη δυνατότητα μετά το σταθερό μέρος (20 byte) της επικεφαλίδας να ακολουθούν προαιρετικές επιλογές (options). Όλοι οι δρομολογητές απαιτείται να τις διαβάζουν και να ενεργούν κατάλληλα. Το πεδίο μήκους της επικεφαλίδας IP μπορεί να λάβει τη μέγιστη τιμή 60, που σημαίνει ότι 40 byte είναι διαθέσιμα για προαιρετικές επιλογές. Οι πιο συνήθεις εξ αυτών σχετίζονται με τη δρομολόγηση πηγής (Source Routing), την καταγραφή διαδρομών (Record Route) και την καταγραφή χρόνων (Time stamp). Στην περίπτωση της καταγραφής διαδρομών, όταν ο δρομολογητής λάβει ένα πακέτο με την προαιρετική επιλογή της καταγραφής διαδρομής ενεργοποιημένη, εισάγει την IP διεύθυνσή του στη θέση της επικεφαλίδας που ορίζει ο σχετικός δείκτης, αυξάνει τον δείκτη κατά 4 και προωθεί το πακέτο. Εάν η επικεφαλίδα γεμίσει, το πακέτο προωθείται χωρίς την καταγραφή της διεύθυνσης IP.

Μπορείτε εύκολα να παράγετε πακέτα IP με επικεφαλίδες που περιέχουν προαιρετικές επιλογές χρησιμοποιώντας την εντολή `ping`. Π.χ., η επιλογή `-r` στην εντολή `ping` ενεργοποιεί την *καταγραφή (recording)* των διευθύνσεων IP κατά μήκος της διαδρομής. [Για περισσότερες πληροφορίες σχετικές με τη σύνταξη της εντολής `ping` πηγαίνετε στο *Start* → *Help and Support*, στο πλαίσιο *Search* πληκτρολογήστε "TCP/IP utilities" και τέλος επιλέξτε την εντολή `ping`.]

Ωστόσο, λόγω περιορισμών που εισάγει το τείχος πυρασφάλειας (firewall) του διατμηματικού ΕΠΥ[1], η εκτέλεση της εντολής `ping` με την επιλογή `-r` από τον υπολογιστή σας θα αποτύχει! Γι' αυτό, στη συνέχεια αυτή θα χρησιμοποιήσετε τα στοιχεία των παραδειγμάτων που παρατίθενται. Η εκτέλεση της εντολής `tracert` από τον υπολογιστή `147.102.40.164` με προορισμό τον υπολογιστή `www.grnet2.gr`, έχει την ακόλουθη έξοδο:

[1] Στο ΕΠΥ του νέου κτιρίου της Σχολής δεν υπάρχει ο αντίστοιχος περιορισμός.

```
C:\>tracert www.grnet2.gr

Tracing route to nic.grnet.gr [194.177.210.210]
over a maximum of 30 hops:

  1     2 ms    <1 ms    <1 ms  router.cn.ece.ntua.gr [147.102.40.200]
  2    <1 ms    <1 ms    <1 ms  backboneRouter.ntua.ilissos.athensMAN.grnet.gr [195.251.24.70]
  3     1 ms     1 ms    <1 ms  athens3-to-ilissos1.backbone.grnet.gr [195.251.24.226]
  4     1 ms     1 ms    <1 ms  nic.grnet.gr [194.177.210.210]

Trace complete.

C:\>
```

4.1 Να καταγράψετε στο σχήμα που παρατίθεται στο φυλλάδιο των απαντήσεων τις διευθύνσεις IP των κόμβων της διαδρομής. (**Σημείωση**: Οι διευθύνσεις IP που εμφανίζονται αντιστοιχούν στις διεπαφές των κόμβων κατά μήκος της διαδρομής που βρίσκονται **προς την πλευρά του υπολογιστή** `147.102.40.164`).

Η έξοδος από την εκτέλεση της `ping -n 1 -r 1 www.grnet2.gr` (με ενεργοποιημένη την καταγραφή διευθύνσεων και αφετηρία πάλι τον υπολογιστή `147.102.40.164`) είναι:

```
C:\>ping -n 1 -r 1 www.grnet2.gr

Pinging nic.grnet.gr [194.177.210.210] with 32 bytes of data:

Reply from 194.177.210.210: bytes=32 time=14ms TTL=252
    Route: 195.251.24.69

Ping statistics for 194.177.210.210:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 14ms, Average = 14ms

C:\>
```

ενώ πληκτρολογώντας `ping -n 1 -r 3 www.grnet2.gr` σε ένα παράθυρο εντολών του ίδιου υπολογιστή, για την *καταγραφή (recording)* τριών διευθύνσεων κατά μήκος της διαδρομής, λαμβάνουμε την ακόλουθη έξοδο:

```
C:\>ping -n 1 -r 3 www.grnet2.gr

Pinging nic.grnet.gr [194.177.210.210] with 32 bytes of data:

Reply from 194.177.210.210: bytes=32 time=9ms TTL=252
    Route: 195.251.24.69 ->
           195.251.24.225 ->
           194.177.210.200

Ping statistics for 194.177.210.210:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 9ms, Average = 9ms

C:\>
```

Οι διευθύνσεις IP που καταγράφονται αντιστοιχούν στις διεπαφές των κόμβων κατά μήκος της διαδρομής που βρίσκονται **προς την πλευρά του παραλήπτη** (`www.grnet2.gr`).

4.2 Συμπληρώστε, βάσει της εξόδου της εντολής `ping` που σας δόθηκε, το σχήμα στο φύλλο των απαντήσεων με την τοπολογία της διαδρομής από τον υπολογιστή `147.102.40.164` μέχρι τον υπολογιστή `www.grnet2.gr`, σημειώνοντας τις διευθύνσεις IP **όλων** των διεπαφών που μεσολαβούν.

4.3 Ποια είναι η διεύθυνση του προκαθορισμένου δρομολογητή (default gateway) για το υποδίκτυο που ανήκει ο `147.102.40.164`; *[Υπόδειξη: Η διεύθυνση του υποδικτύου είναι `147.102.40.0/24`]*

4.4 Ποια είναι η διεύθυνση του προκαθορισμένου δρομολογητή (default gateway) για το υποδίκτυο που ανήκει ο προορισμός, δηλαδή ο `www.grnet2.gr`; *[Υπόδειξη: Η διεύθυνση του υποδικτύου είναι `194.177.210.0/24`]*

Για την πραγματοποίηση του τελευταίου μέρους της άσκησης, θα αναλύσετε την κίνηση ICMP που παράγεται κατά την εκτέλεση της εντολής `ping -n 1 -r X www.ucla.edu` από τον υπολογιστή `147.102.40.164`, όπου η παράμετρος '*X*' παίρνει διαδοχικά τις τιμές από 1 μέχρι τη μέγιστη τιμή της που είναι 9. Η κίνηση έχει ήδη καταγραφεί στο αρχείο `lab5.cap` που βρίσκεται στον υπολογιστή `edu-dy.cn.ntua.gr`. Για να κατεβάσετε το αρχείο αυτό στον υπολογιστή σας, πληκτρολογήστε `ftp edu-dy.cn.ntua.gr` σε ένα παράθυρο εντολών. Στην προτροπή `User:` πληκτρολογήστε `anonymous` ακολουθούμενο από `<Enter>`, ενώ στην προτροπή `Password:` πληκτρολογήστε το e-mail σας ακολουθούμενο από `<Enter>`. Στη συνέχεια, πληκτρολογήστε `lcd desktop`, ώστε να μεταφερθεί ο τοπικός κατάλογος στο Desktop του υπολογιστή σας, έπειτα δώστε την εντολή `bin`, ώστε η μεταφορά αρχείων να γίνει σε δυαδική μορφή και τέλος `hash` για να βλέπετε την πρόοδο της μεταφοράς του αρχείου. Προκειμένου να κατεβάσετε το `lab5.cap` πληκτρολογήστε την εντολή `get lab5.cap` *[Προσοχή στα μικρά και κεφαλαία γράμματα]*. Τέλος πληκτρολογήστε `bye` για να τερματίσετε την εφαρμογή `ftp` και αρχίστε την ανάλυση της καταγεγραμμένης κίνησης ανοίγοντας το `lab5.cap` από το Wireshark (*File* → *Open*... και επιλέξτε το `lab5.cap`).

4.5 Ποιο είναι το μήκος της επικεφαλίδας IP για κάθε ζεύγος μηνυμάτων *Echo* και *Echo reply* που προέκυψε από τις διαδοχικές εκτελέσεις της εντολής `ping`;

4.6 Τι παρατηρείτε για το μέγεθος της επικεφαλίδας σε σχέση με την τιμή της παραμέτρου `-r X`;

4.7 Σε ποιο πεδίο του πακέτου IP καταγράφονται οι διευθύνσεις IP των διεπαφών της διαδρομής;

4.8 Πόσες διευθύνσεις IP χωρούν στο παραπάνω πεδίο;

Ονοματεπώνυμο:	**Αρ. PC:**
Ομάδα:	**Ημερομηνία:**
Διεύθυνση IP: . . .	**Διεύθυνση MAC: - - - - -**

Εργαστηριακή Άσκηση 6
Πρωτόκολλα ARP και ICMP

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 .....

1.2 .....

1.3 .....

1.4 .....

.....

.....

1.5 .....

1.6 .....

1.7 .....

1.8 .....

1.9 .....

.....

1.10 .....

1.11 .....

.....

1.12 .....

1.13 .....

1.14 .....

1.15 .....

1.16 .....

1.17 .....

.....

1.18 .....

1.19 .....

.....

1.20 .....

1.21 .....

.....

4