

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΑΡΙΝΟ ΕΞΑΜΗΝΟ 2020-2021

ΜΑΘΗΜΑ «ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ»

ΔΙΔΑΣΚΩΝ: ΓΕΩΡΓΙΟΣ Δ. ΣΤΑΜΟΥΛΗΣ, ΚΑΘΗΓΗΤΗΣ

ΒΟΗΘΟΙ: ΔΙΟΝΥΣΙΟΣ ΔΑΜΑΣΙΩΤΗΣ, ΙΑΚΩΒΟΣ ΠΙΤΤΑΡΑΣ

Σειρά Εργαστηριακών Ασκήσεων 2

Παράδοση: 20/4/2021

Σκοπός

Εξοικείωση με το Wireshark και εφαρμογή του για την άντληση πληροφοριών για τα πρωτόκολλα DHCP και IP. Επίσης, μελέτη θεωρητικών ασκήσεων σε δρομολόγηση.

Γενικές πληροφορίες

Η εργασία θα πρέπει να εκπονηθεί σε ομάδες των τριών (3) ατόμων. Για την παράδοση της εργασίας θα ετοιμάσετε σύντομη αναφορά με τις απαντήσεις σας και με τεκμηρίωση (screen shots), την οποία θα υποβάλλετε ηλεκτρονικά μέσω **e-class**. Για απορίες απευθυνθείτε στον κ. Δαμασιώτη στο email: diondam@gmail.com

1. Πρωτόκολλο DHCP

Το Dynamic Host Control Protocol (DHCP) είναι ένα τυποποιημένο πρωτόκολλο <http://tools.ietf.org/html/rfc2131> που δημιουργήθηκε από την ανάγκη απλοποίησης της διαχείρισης δικτύων βασισμένων στο πρωτόκολλο IP (και γενικά στην στοίβα πρωτοκόλλων του Internet). Παλαιότερα τα περισσότερα τοπικά δίκτυα είχαν περιορισμένο αριθμό σταθερών υπολογιστών κάτι που επέτρεπε τη στατική ανάθεση διευθύνσεων IP. Αυτό προϋπέθετε τη δια χειρός αλλαγή και ρύθμιση των διευθύνσεων οι οποίες αποθηκεύονταν στο δίσκο του υπολογιστή. Αν χρειαζόταν ένας υπολογιστής να αλλάξει διεύθυνση τότε αυτό γινόταν από το τερματικό του και συνήθως απαιτούσε επανεκκίνηση. Σχετικά σύντομα, και καθώς άρχισαν να δημιουργούνται όλο και πιο σύνθετα δίκτυα, υπήρξε η ανάγκη για κεντρική διαχείριση των διευθύνσεων IP. Αυτό έγινε γιατί άρχισαν να χρησιμοποιούνται κατά κόρον σταθμοί εργασίας (και αργότερα προσωπικοί υπολογιστές). Ένα ειδικό πρωτόκολλο, το Reverse Address Resolution Protocol (RARP), δημιουργήθηκε για τέτοιες περιπτώσεις ([RFC 903](http://tools.ietf.org/html/rfc903)). Επέτρεπε σε ένα μηχάνημα να «μάθει» την IP διεύθυνσή του και μετά να ξεκινήσει την κανονική λειτουργία του IP.

Ένα άλλο πρωτόκολλο, το BOOTstrap Protocol (BOOTP), αναπτύχθηκε για να επιτρέψει σε φθηνούς σταθμούς εργασίας που δεν διέθεταν χώρο μόνιμης αποθήκευσης (σκληρό δίσκο) να λαμβάνουν την IP διεύθυνσή τους και την εικόνα του λειτουργικού τους συστήματος κατά την εκκίνηση ([RFC951](http://tools.ietf.org/html/rfc951)). Το BOOTP στη συνέχεια εμπλουτίστηκε με ένα μηχανισμό επέκτασης (BOOTP extension mechanism) που επέτρεπε αποστολή επιπλέον δεδομένων και επιλογές μηνυμάτων. Αυτή η έκδοση του BOOTP ήταν ο πρόγονος του DHCP. Υπάρχουν δύο κύριες διαφορές μεταξύ των πρωτοκόλλων BOOTP και DHCP. Το DHCP ορίζει μηχανισμούς δυναμικής εκχώρησης διευθύνσεων IP στους σταθμούς εργασίας προσωρινά και για καθορισμένο χρονικό διάστημα. Έτσι επιτυγχάνεται η επαναχρησιμοποίηση ενός αριθμού διευθύνσεων IP από πολλούς σταθμούς εργασίας. Επιπλέον, το DHCP παρέχει το μηχανισμό με τον οποίο ο σταθμός εργασίας μπορεί μόνος του να αποκτήσει και τις υπόλοιπες πληροφορίες που απαιτούνται προκειμένου να λειτουργήσει στο δίκτυο.

Η λειτουργία του DHCP είναι περιληπτικά η ακόλουθη. Μόλις ο υπολογιστής εκκινήσει εκπέμπει ένα μήνυμα αναζήτησης (*DHCP Discover*) εξυπηρετητή DHCP. Οι εξυπηρετητές DHCP που λαμβάνουν αυτό το μήνυμα, απαντούν με μήνυμα προσφοράς (*DHCP Offer*), το οποίο ορίζει διαθέσιμες διευθύνσεις IP. Ο υπολογιστής επιλέγει μία από τις προσφορές αυτές και εκπέμπει αίτηση (*DHCP Request*) προς τον

εξυπηρετητή ζητώντας τη συγκεκριμένη διεύθυνση IP. Όλοι οι άλλοι εξυπηρετητές δεν απαντούν και ο εξυπηρετητής που επιλέχθηκε η προσφορά του στέλνει επιβεβαίωση (DHCP ACK) για την εκχωρούμενη διεύθυνση IP. Η διεύθυνση IP παραχωρείται προσωρινά και για συγκεκριμένο χρονικό διάστημα (lease time). Προτού λήξει το διάστημα αυτό, ο υπολογιστής πρέπει να ανανεώσει τον «δανεισμό» της διεύθυνσης IP αυτής. Όταν ο υπολογιστής τελειώσει, στέλνει μήνυμα απελευθέρωσης (DHCP Release) της διεύθυνσης.

Ουσιαστικά, το DHCP αναλαμβάνει να ορίσει αυτόματα, χωρίς την παρουσία διαχειριστή δικτύου, τις αναγκαίες παραμέτρους για την διασύνδεση ενός υπολογιστή στο Internet, περιλαμβανομένης και της διεύθυνσης IP.

Προκειμένου να δείτε τις τρέχουσες ρυθμίσεις δικτύου IP του υπολογιστή σας, πρέπει να ανοίξετε ένα παράθυρο εντολών και να εκτελέσετε την εντολή `ipconfig /all`.

1. Να καταγράψετε τη διεύθυνση IP, τη μάσκα υποδικτύου του υπολογιστή σας καθώς και τη διεύθυνση IP του εξυπηρετητή DHCP που απέστειλε τις παραμέτρους αυτές.

Στη συνέχεια με τη βοήθεια του Wireshark να ξεκινήσετε μια νέα καταγραφή της κίνησης (χωρίς φίλτρο σύλληψης) προκειμένου να μελετήσετε τα μηνύματα DHCP που ανταλλάσσονται κατά την εκχώρηση/αποδέσμευση των ρυθμίσεων δικτύου του υπολογιστή σας.

Κατόπιν να εκτελέσετε την εντολή `iprelease`¹ που θα προκαλέσει την αποδέσμευση των ρυθμίσεων δικτύου του υπολογιστή σας. Έπειτα να εκτελέσετε την εντολή `iprenew`² προκειμένου να εκχωρηθούν νέες δικτυακές ρυθμίσεις στον υπολογιστή σας. Να περιμένετε έως ότου ολοκληρωθεί η εκχώρηση και να εκτελέσετε πάλι την εντολή `iprenew` ώστε να ανανεώσετε τις ρυθμίσεις. Όταν ολοκληρωθεί και η εκτέλεση της δεύτερης `iprenew`, να σταματήσετε την καταγραφή μηνυμάτων από το Wireshark.

2. Να εφαρμόσετε κατάλληλο φίλτρο απεικόνισης ώστε να εμφανίζονται μόνο μηνύματα DHCP. Ποια είναι η σύνταξη του φίλτρου αυτού; [Υπόδειξη: Υπενθυμίζεται ότι το πρωτόκολλο DHCP αποτελεί επέκταση του BOOTP.]
3. Ποιο πρωτόκολλο επιπέδου μεταφοράς χρησιμοποιεί το DHCP;
4. Ποια είδη μηνυμάτων DHCP παρήχθησαν από την αλληλουχία εντολών απελευθέρωσης (`iprelease`), εκχώρησης και ανανέωσης (`iprenew`) δικτυακών ρυθμίσεων; [Υπόδειξη: Ο τύπος μηνύματος DHCP αναφέρεται και στο πεδίο *Info* του παράθυρου με τη λίστα καταγεγραμμένων πακέτων του Wireshark.]
5. Ποιος είναι ο σκοπός του πρώτου μηνύματος DHCP που παρατηρείτε;
6. Ποιες είναι οι διευθύνσεις IP του αποστολέα και του παραλήπτη του παραπάνω μηνύματος;
7. Παρατηρώντας το περιεχόμενο των πεδίων της επικεφαλίδας όλων των μηνυμάτων DHCP, να καταγραφούν: η αριθμητική ετικέτα (tag) και το μήκος (length) της επιλογής (option) που καθορίζει τον τύπο του εκάστοτε μηνύματος (DHCP Message Type). [Υπόδειξη: Το Wireshark εμφανίζει την ετικέτα και το μήκος ($t=x, l=y$) στην πρώτη γραμμή δίπλα από κάθε επιλογή που περιλαμβάνεται στις επικεφαλίδες των μηνυμάτων DHCP]
8. Ποια είναι η τιμή (value) που αντιστοιχεί στην αριθμητική ετικέτα που καταγράψατε στην ερώτηση 7 για κάθε είδος μηνύματος DHCP που καταγράψατε; [Υπόδειξη: Στο παράθυρο λεπτομερειών πακέτου του Wireshark, να αναπτύξετε όλες τις γραμμές που αντιστοιχούν στην επιλογή DHCP με τη συγκεκριμένη αριθμητική ετικέτα.]

Όπως προαναφέρθηκε, η διεύθυνση IP που εκχωρείται στον υπολογιστή σας, επιβεβαιώνεται στο τέλος της ανταλλαγής των μηνυμάτων DHCP Discover/Offer/Request/ACK μεταξύ του υπολογιστή σας και του εξυπηρετητή DHCP.

9. Να καταγράψετε τις θύρες πηγής και προορισμού που χρησιμοποιήθηκαν κατά την ανταλλαγή των μηνυμάτων DHCP Discover/Offer/Request/ACK μεταξύ του υπολογιστή σας και του εξυπηρετητή DHCP.
10. Ποιες από τις παραπάνω θύρες αντιστοιχούν στις συνήθεις (γνωστές) θύρες (well-known ports) της υπηρεσίας DHCP; [Υπόδειξη: Να συμβουλευτείτε έναν κατάλογο στο Internet με τις διαθέσιμες well-known ports]

¹ Ταυτόσημη με την `ipconfig /release`.

² Ισοδυναμεί με την εντολή `ipconfig /renew`.

11. Ποιες είναι οι διευθύνσεις IP αποστολέα και παραλήπτη των παραπάνω τεσσάρων μηνυμάτων;
12. Ποια είναι η διεύθυνση IP του παραλήπτη του μηνύματος DHCP Discover;
13. Ποια διεύθυνση IP αποδίδεται τελικά στον υπολογιστή σας;
14. Για πόσο χρόνο διαρκεί η εκχώρηση της διεύθυνσης IP αυτής; [Υπόδειξη: Να αναζητήσετε την τιμή του *lease time* στο DHCP μήνυμα ACK.]
15. Συμπίπτει η διεύθυνση IP που εκχωρήθηκε με αυτή που είχατε καταγράψει αρχικά στο ερώτημα 1; Να αιτιολογήσετε την απάντησή σας.

Εκτός από την διεύθυνση IP, ο υπολογιστής σας χρησιμοποιεί το πρωτόκολλο DHCP για να λάβει και άλλες δικτυακές παραμέτρους αναγκαίες για τη δικτυακή λειτουργία του. Παρατηρώντας τα περιεχόμενα του μηνύματος DHCP Discover του υπολογιστή σας, θα βρείτε την επιλογή (option) Parameter Request List που περιλαμβάνει τη λίστα των δικτυακών παραμέτρων που μπορεί να ζητηθούν.

16. Να καταγραφούν οι κωδικοί, τα ονόματα, καθώς και η σημασία τριών παραμέτρων που ζητά ο υπολογιστής σας [Υπόδειξη: Να συμβουλευτείτε την ιστοσελίδα <http://www.iana.org/assignments/bootp-dhcp-parameters>]
17. Πόσες από τις παραμέτρους που ζήτησε ο υπολογιστής σας προσδιορίζει τελικά ο εξυπηρετητής DHCP στο μήνυμα *DCHP Offer*;

Μετά τη λήψη της προσφοράς για διεύθυνση IP, ο υπολογιστής σας βεβαιώνεται ότι αυτή είναι πραγματικά διαθέσιμη (δεν χρησιμοποιείται από άλλον) και αμέσως μετά ζητά την δέσμευσή της.

18. Να τροποποιήσετε το φίλτρο απεικόνισης ώστε εκτός των μηνυμάτων DHCP να εμφανίζονται και πλαίσια με τα μηνύματα του πρωτοκόλλου ARP. Ποια είναι η νέα σύνταξη του φίλτρου απεικόνισης;
19. Παρατηρείτε την αποστολή πλαισίων ARP αμέσως μετά το μήνυμα DHCP ACK;
20. Εάν ναι, ποιος υπολογιστής τα παράγει και ποιου υπολογιστή τη διεύθυνση MAC αναζητεί;
21. Να εξηγήσετε τη χρησιμότητα αυτών των πλαισίων ARP [Υπόδειξη: Να αναζητήσετε πληροφορίες για το “*gratuitous ARP*” .];

Με την δεύτερη εκτέλεση της εντολής *iprenew*, ο υπολογιστής σας ζητά την ανανέωση της διεύθυνσης IP που του εκχωρήθηκε προηγουμένως (κατά την πρώτη εκτέλεση της εντολής *iprenew*).

22. Ποια είδη μηνυμάτων DHCP παρήχθησαν μετά τη δεύτερη εκτέλεση της εντολής *iprenew*;
23. Ποια είναι η βασική διαφορά του μηνύματος DHCP Request της δεύτερης εκτέλεσης της εντολής *iprenew*, σε σχέση με το DHCP Request της πρώτης εκτέλεσης της εντολής; [Υπόδειξη: Να περιορισθείτε στις βασικές παραμέτρους που εμφανίζονται στο παράθυρο με τη λίστα των καταγεγραμμένων πακέτων του *Wireshark*.]

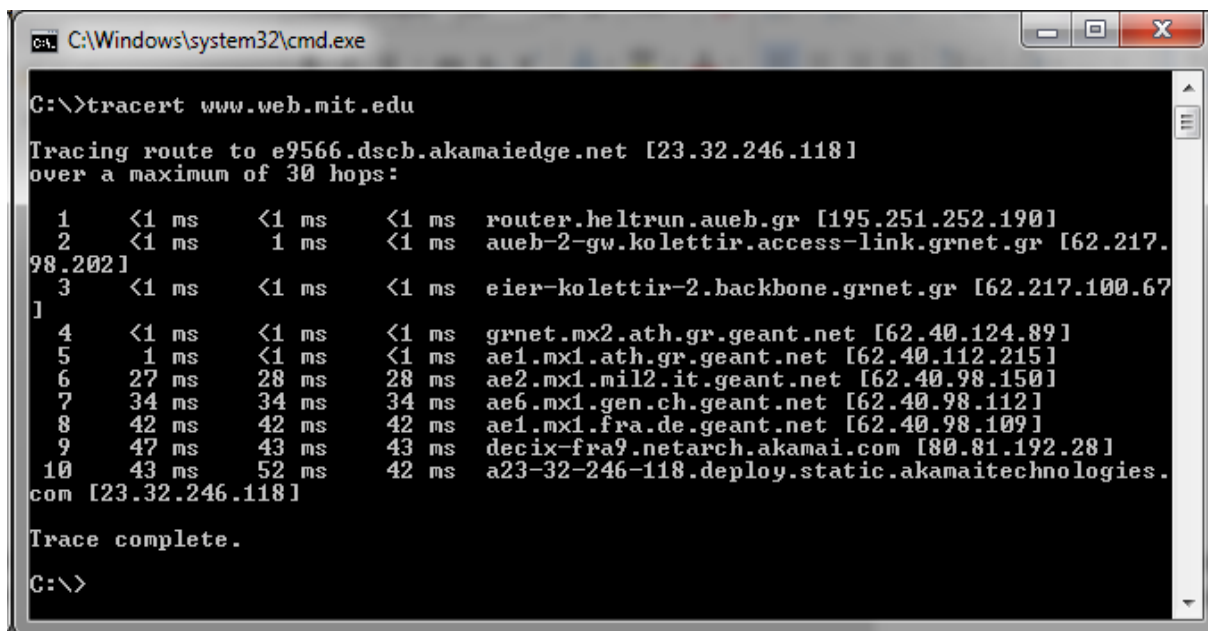
2. Πρωτόκολλο IP

Το πρωτόκολλο IP ανήκει στο επίπεδο δικτύου και χρησιμοποιείται για την επικοινωνία στο Διαδίκτυο. Στην άσκηση αυτή θα μελετήσετε την χρήση του πρωτοκόλλου IPv4. Το ίχνος (trace) που πρέπει να καταγραφεί είναι αυτό μίας απλής άντλησης μέσω web (web-fetch) από έναν απομακρυσμένο διακομιστή, η οποία θα έχει ως αποτέλεσμα ο υπολογιστής σας να στέλνει και να λαμβάνει πακέτα IP. Στη συνέχεια θα εκτελέσετε την εντολή *tracert* για τον απομακρυσμένο διακομιστή για να ανακαλύψετε το μονοπάτι (διαδρομή) που χρησιμοποιείται πάνω από το Διαδίκτυο.

Πρέπει επίσης να κατεβάσετε και να εγκαταστήσετε το *wget*, που είναι πρόγραμμα ελεύθερου λογισμικού (<http://gnuwin32.sourceforge.net/packages/wget.htm>), το οποίο χρησιμοποιείται για την άντληση περιεχομένου διαδικτύου.

- 1) Να ανοίξετε ένα παράθυρο εντολών και να μεταβείτε στην τοποθεσία *C:\Program Files (x86)\GnuWin32\bin*, όπου ευρίσκεται το εκτελέσιμο αρχείο του παραπάνω προγράμματος. Στη συνέχεια, να πληκτρολογήσετε την εντολή “*wget http://www.mit.edu/*”, προκειμένου να ελέγξετε αν μπορείτε να αντλήσετε τα περιεχόμενα της παραπάνω ιστοσελίδας. Με τη χρήση της εντολής “*wget*” πρέπει να λάβετε απάντηση με status code “200 OK”.

- 2) Να εκτελέσετε την εντολή `tracert` προς τον ίδιο απομακρυσμένο διακομιστή. Για Windows να πληκτρολογήσετε την εντολή "`tracert www.mit.edu`". Η εντολή αυτή θα σας δώσει πληροφορίες για το μονοπάτι που ακολουθείται στο διαδίκτυο (Εικόνα 1). Σημειωτέο ότι το `tracert` μπορεί να απαιτήσει έως και 1 min για να τρέξει. Κάθε γραμμή δίνει πληροφορίες σχετικά με το επόμενο IP hop από τον υπολογιστή που εκτελεί το `tracert` προς τον προορισμό. Οι γραμμές με "*" δείχνουν ότι δεν υπήρξε απάντηση από το δίκτυο για να αναγνωριστεί το συγκεκριμένο τμήμα της διαδρομής στο Διαδίκτυο. Μερικά τέτοια τμήματα διαδρομής θα πρέπει να αναμένεται ότι θα εμφανιστούν. Ωστόσο, εάν το `tracert` δεν λειτουργεί σωστά τότε σχεδόν όλη η διαδρομή θα είναι "*". Σε αυτή την περίπτωση, μπορείτε να δοκιμάσετε ένα διαφορετικό απομακρυσμένο διακομιστή.



```
C:\Windows\system32\cmd.exe

C:\>tracert www.web.mit.edu

Tracing route to e9566.dsch.akamaiedge.net [23.32.246.118]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    router.heltrun.aueb.gr [195.251.252.190]
  1  <1 ms     1 ms     <1 ms    aueb-2-gw.kolettir.access-link.grnet.gr [62.217.98.202]
  2  <1 ms     <1 ms    <1 ms    eier-kolettir-2.backbone.grnet.gr [62.217.100.67]
  3  <1 ms     <1 ms    <1 ms    grnet.mx2.ath.gr.geant.net [62.40.124.89]
  4  1 ms      <1 ms    <1 ms    ae1.mx1.ath.gr.geant.net [62.40.112.215]
  5  27 ms     28 ms    28 ms    ae2.mx1.mil2.it.geant.net [62.40.98.150]
  6  34 ms     34 ms    34 ms    ae6.mx1.gen.ch.geant.net [62.40.98.112]
  7  42 ms     42 ms    42 ms    ae1.mx1.fra.de.geant.net [62.40.98.109]
  8  47 ms     43 ms    43 ms    decix-fra9.netarch.akamai.com [80.81.192.28]
  9  43 ms     52 ms    42 ms    a23-32-246-118.deploy.static.akamaitechnologies.com [23.32.246.118]

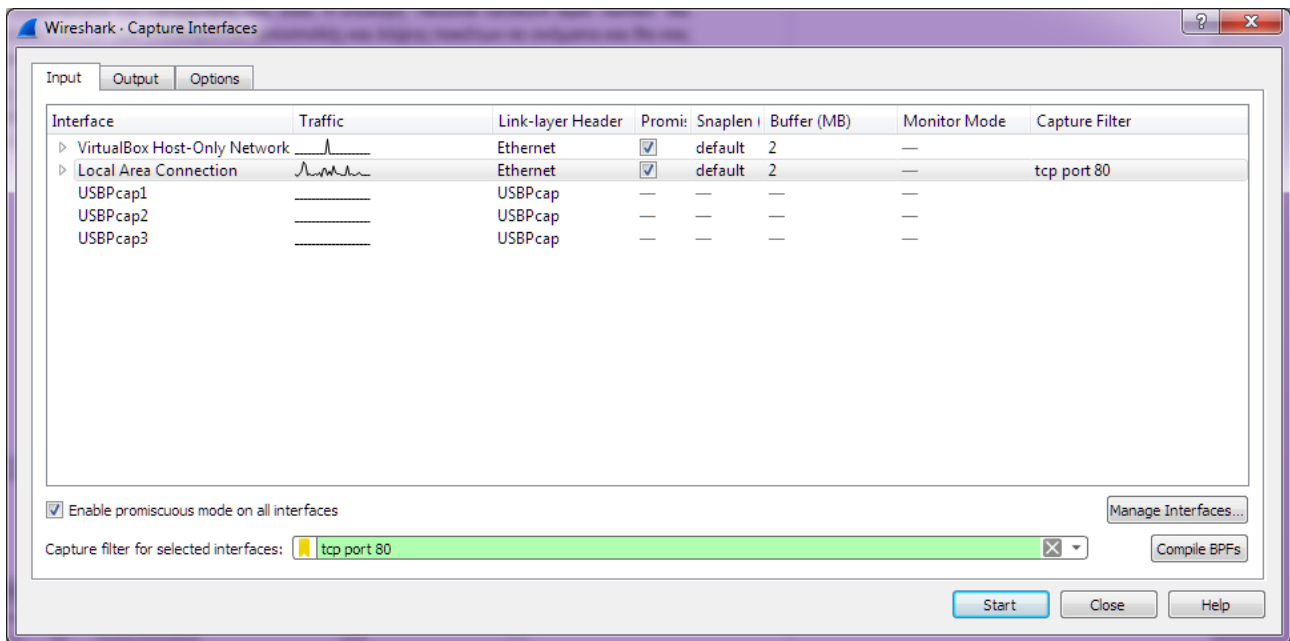
Trace complete.

C:\>
```

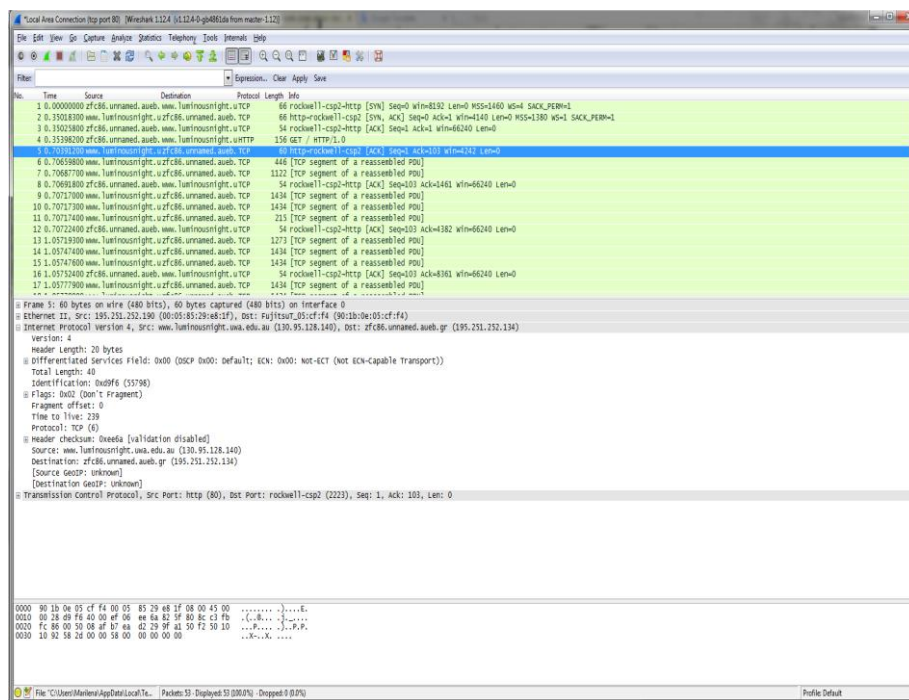
Εικόνα 1. Εκτέλεση της εντολής `tracert` στα Windows (`tracert`)

Με βάση τα στοιχεία της καταγραφής σας:

- Πόσα hops χρειάστηκαν μέχρι τον προορισμό;
 - Να εκτελέσετε την εντολή "`tracert www.ntua.gr`". Πόσα hops χρειάστηκαν στην περίπτωση αυτή;
 - Να εκτελέσετε την εντολή "`tracert www.cs.aueb.gr`". Πόσα hops χρειάστηκαν στην περίπτωση αυτή; Τι παρατηρείτε σε σχέση με τα προηγούμενα ερωτήματα και τον αριθμό των hops;
- 3) Να ξεκινήσετε μία νέα καταγραφή στο Wireshark με φίλτρο "`tcp port 80`". Να βεβαιωθείτε ότι είναι ενεργοποιημένη η επιλογή "`Resolve network layer names`". Να χρησιμοποιήσετε αυτό το φίλτρο για να καταγραφεί μόνο κυκλοφορία της εφαρμογής του web. Η επιλογή "`Resolve network layer names`" θα μεταφράσει τις διευθύνσεις IP των υπολογιστών αποστολής και λήψης πακέτων σε ονόματα και θα σας βοηθήσει να αναγνωρίσετε αν τα πακέτα αποστέλλονται προς ή από τον υπολογιστή σας.
- 4) Αφού ξεκινήσει η καταγραφή, να εκτελέσετε ξανά την εντολή "`wget http://www.mit.edu`". Μόλις ολοκληρωθεί η εντολή, να σταματήσετε την καταγραφή στο Wireshark. Το παράθυρο λήψης σας πρέπει να είναι παρόμοιο με εκείνο που απεικονίζεται παρακάτω στην Εικόνα 3.



Εικόνα 2. Καθορισμός επιλογών φίλτρου σύλληψης



Εικόνα 3. Ίχνος της κίνησης από την εκτέλεση της εντολής wget

- 5) Να επιλέξετε οποιοδήποτε πακέτο στο ίχνος και να διευρύνετε τα πεδία κεφαλίδας IP (χρησιμοποιώντας το "+" επέκτασης ή το εικονίδιο) για να δείτε τις λεπτομέρειες. Μπορείτε απλά να κάνετε κλικ σε ένα πακέτο για να το επιλέξετε (στην κορυφή του πίνακα). Θα παρατηρήσετε τις λεπτομέρειες της δομής του (στο μεσαίο panel) και τα bytes που συνθέτουν το πακέτο (στον κάτω πίνακα). Το ενδιαφέρον μας είναι στην κεφαλίδα IP, οπότε μπορείτε να αγνοήσετε τα υπόλοιπα πρωτόκολλα υψηλότερου και χαμηλότερου επιπέδου. Όταν κάνετε κλικ σε πεδία της Κεφαλίδας IP, θα δείτε στο κάτω μέρος του πίνακα τα bytes που αντιστοιχούν στο κάθε πεδίο το οποίο τονίζεται. Στην **Εικόνα 3** απεικονίζεται επικεφαλίδα IP με όλα τα πεδία της.

Με βάση τα στοιχεία της καταγραφής σας, να απαντήσετε στις επόμενες ερωτήσεις:

1. Ποιες είναι οι διευθύνσεις IP του υπολογιστή σας και του απομακρυσμένου διακομιστή;
2. Ποιο είναι το μήκος της κεφαλίδας IP και πώς αυτό κωδικοποιείται στο πεδίο μήκους κεφαλίδας; Υπόδειξη: Να παρατηρήσετε ότι μόνο 4 bits χρησιμοποιούνται για αυτό το πεδίο.
3. Το πεδίο Total Length περιλαμβάνει το μήκος της κεφαλίδας IP συν το μήκος του ωφέλιμου φορτίου του πακέτου (IP payload), ή απλά συν το μήκος του ωφέλιμου φορτίου; Αν όντως περιλαμβάνει και το μήκος της κεφαλίδας IP, πώς μπορεί να υπολογισθεί το μήκος του ωφέλιμου φορτίου;
4. Ποια είναι η αρχική τιμή του πεδίου TTL για τα πακέτα που αποστέλλονται από τον υπολογιστή σας; Είναι ίδια με την τιμή του πεδίου TTL των πακέτων που λαμβάνονται από τον παραλήπτη; Είναι η μέγιστη δυνατή τιμή, ή κάποια χαμηλότερη τιμή και γιατί;
5. Τις περισσότερες φορές τα πακέτα IP σε κανονική λειτουργία δεν είναι κατακερματισμένα. Πώς μπορείτε να ανιχνεύσετε αν ένα πακέτο έχει κατακερματιστεί;
6. Τι ισχύει ως προς τον κατακερματισμό για τα πακέτα που παρατηρείτε;
7. Να μελετήσετε αν αλλάζει η τιμή του Identification field και πώς ή αν παραμένει ίδια για διαφορετικά πακέτα. Για παράδειγμα, να παρατηρήσετε αν η τιμή αλλάζει σε κάθε πακέτο ή παραμένει ίδια για ορισμένα πακέτα της ίδιας σύνδεσης TCP. Είναι τα πακέτα αυτά διαδοχικά; Ισχύει το ίδιο και στις δύο κατευθύνσεις; Τι παρατηρείτε στην περίπτωση που αλλάζει η τιμή και τι στην περίπτωση που δεν αλλάξει ως προς άλλα πεδία;

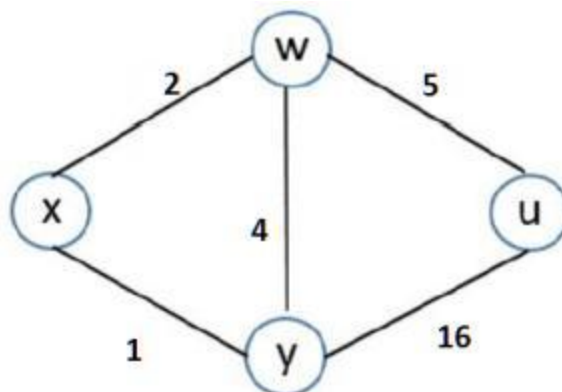
Να ξεκινήσετε μία νέα καταγραφή στο Wireshark με φίλτρο `"tcp port 80"`. Αφού ξεκινήσει η καταγραφή να εκτελέσετε ξανά την εντολή `wget http://grad.cs.aueb.gr/`. Μόλις ολοκληρωθεί η εντολή, να σταματήσετε την καταγραφή στο Wireshark.

8. Να απαντήσετε στα ερωτήματα 6 και 7 με βάση αυτή τη νέα καταγραφή. Τι παρατηρείτε σε σχέση με τα προηγούμενα αποτελέσματα των ερωτημάτων 6 και 7.

Ασκήσεις σε δρομολόγηση

Άσκηση 3

Να θεωρήσετε το δίκτυο που φαίνεται στο παρακάτω σχήμα και αποτελείται από τους δρομολογητές x, y, w και u. Επίσης να θεωρήσετε ότι ο αλγόριθμος δρομολόγησης που εκτελείται είναι ο αλγόριθμος διανυσμάτων απόστασης (distance vector). Αρχικά να παρουσιάσετε τους πίνακες δρομολόγησης καθενός κόμβου, οι οποίοι πρέπει να περιλαμβάνουν το Next Hop για κάθε προορισμό και την απόσταση προς αυτόν μέσω της αντίστοιχης διαδρομής. Στην συνέχεια να υποθέσετε ότι συμβαίνει μία σημαντική αύξηση (συγκεκριμένα από 2 σε 30) στο κόστος της ζεύξης $x \rightarrow y$ (και μόνο σε αυτή την κατεύθυνση). Να περιγράψετε τα βήματα σύμφωνα με τα οποία ο κόμβος x θα ενημερώσει τους γείτονες του για μια νέα διαδρομή ελάχιστου κόστους προς τον u.



Άσκηση 4

Να θεωρήσετε το δίκτυο που απεικονίζεται στο παρακάτω σχήμα. Να υπολογίσετε τις διαδρομές ελάχιστου κόστους από τον κόμβο u προς όλους τους άλλους κόμβους, εκτελώντας τον αλγόριθμο κατάστασης συνδέσμων (αλγόριθμος του Dijkstra). Για την εκτέλεση του αλγορίθμου και την παρουσίαση των αποτελεσμάτων κάθε βήματος να χρησιμοποιήσετε κατάλληλο πίνακα. Αφού εκτελέσετε τον αλγόριθμο, να κατασκευάσετε τον πίνακα δρομολόγησης του κόμβου u προς κάθε πιθανό προορισμό.

