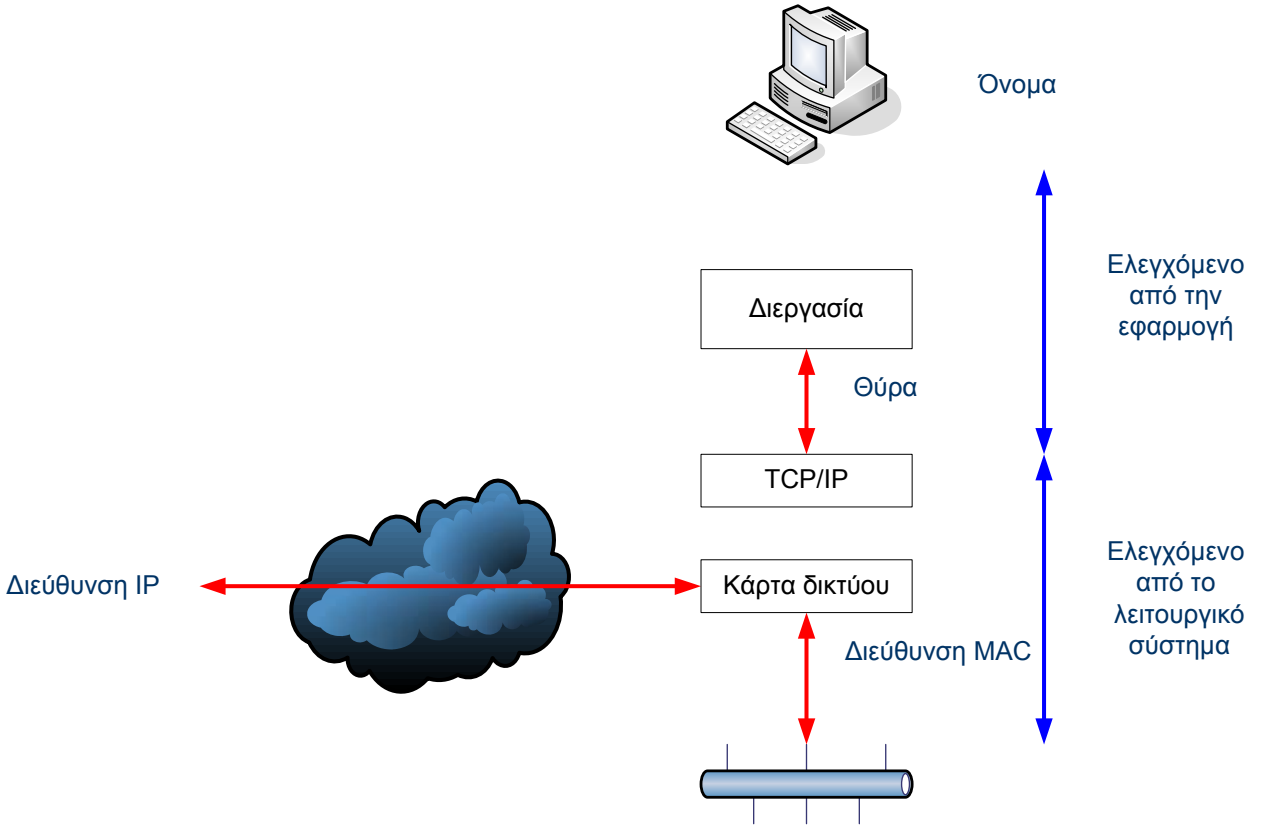
Εργαστηριακή Άσκηση 2
Επικοινωνία στο τοπικό δίκτυο
(πλαίσιο Ethernet και πρωτόκολλο ARP)

Ο σκοπός αυτού του εργαστηρίου είναι η εξοικείωση με τους βασικούς μηχανισμούς που απαιτούνται ώστε να υπάρξει επικοινωνία μεταξύ υπολογιστών συνδεδεμένων σε τοπικό δίκτυο (LAN). Δηλαδή, θα έχετε μια πρώτη επαφή με το θέμα της αριθμοδότησης και διευθυνσιοδότησης. Για να είναι εφικτή οποιαδήποτε επικοινωνία μεταξύ δύο οντοτήτων πρέπει προηγουμένως να έχουν προσδιορισθεί τρία θεμελιώδη χαρακτηριστικά τους: το όνομα (δηλαδή, ποιος επικοινωνεί), η διεύθυνση (πού βρίσκεται) και η διαδρομή (πώς φτάνουμε εκεί). Οποιοδήποτε από τα προηγούμενα χαρακτηριστικά μπορεί να θεωρηθεί ως ένα είδος ταυτότητας (identifier) ή αριθμού (numbering). Ανάλογα με τι ακριβώς υποδηλώνει η ταυτότητα, χρησιμοποιούνται ειδικότερες λέξεις, όπως, Όνομα (name), Διεύθυνση (Address), Διαδρομή (Route).

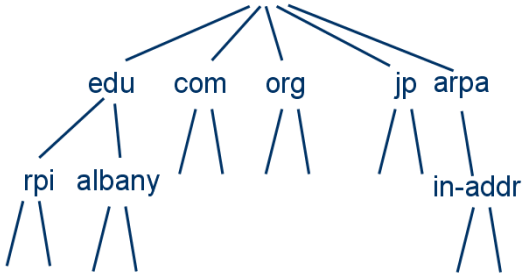
Στην περίπτωση ενός υπολογιστή στο διαδίκτυο, οι οντότητες που χρήζουν ονομάτων ή διευθύνσεων είναι: ο ίδιος ο υπολογιστής (όνομα), οι διεργασίες (θύρα TCP/UDP), οι διεπαφές (διεύθυνση IP) και οι κάρτες δικτύου (διεύθυνση Medium Access Control – MAC). Το Σχήμα 1 δείχνει τη μεταξύ τους σχέση, αλλά κρύβει την πολυπλοκότητα της ανάθεσης και διαχείρισής τους. Στο διαδίκτυο υπάρχουν μηχανισμοί και αντίστοιχα πρωτόκολλα για τη μετάφραση του ονόματος ενός κόμβου στη διεύθυνσή IP αυτού, την απόδοση διεύθυνσης IP σε ένα υπολογιστή και τελικά τη μετάφραση της διεύθυνσης IP σε διεύθυνση MAC. Για τις παραπάνω λειτουργίες χρησιμοποιούνται οι εξυπηρετητές του συστήματος δυναμικής διάρθρωσης κόμβου DHCP (Dynamic Host Configuration Protocol) και του συστήματος ονομασίας περιοχών DNS (Domain Name System) καθώς και το Πρωτόκολλο Επίλυσης Διευθύνσεων ARP (Address Resolution Protocol).



Σχήμα 1: Ονόματα, διευθύνσεις και θύρες στο διαδίκτυο

Όσον αφορά τα ονόματα, το διαδίκτυο είναι χωρισμένο νοητά σε εκατοντάδες διαφορετικές **περιοχές** (domains) υψηλού επιπέδου, οι οποίες χωρίζονται με τη σειρά τους σε άλλες υποπεριοχές

(subdomains) με πολλούς host (υπολογιστές ή κόμβους) η καθεμία. Η ιεραρχία των περιοχών μπορεί να παρασταθεί με ένα δέντρο (Σχήμα 2). Το όνομα κάθε host αποτελείται από μια ακολουθία *ετικετών* (labels) που χωρίζονται με τελείες (π.χ. www.mit.edu). Κάθε ετικέτα μπορεί να έχει μέχρι 63 χαρακτήρες, ενώ το όνομα του host συνολικά, μπορεί να έχει το πολύ 255 χαρακτήρες. Μια περιοχή είναι ένα υποδέντρο του παγκόσμιου δέντρου ονομάτων και ως εκ τούτου, το όνομα περιοχής (domain name) για ένα host είναι η ακολουθία των ετικετών που οδηγούν από το host (φύλλο στο δέντρο ονομάτων) στην κορυφή του παγκόσμιου δέντρου ονομάτων.



Σχήμα 2: Ιεραρχία DNS

Όσον αφορά τις διευθύνσεις, το διαδίκτυο βασίζεται στη χρήση της στοίβας πρωτοκόλλων TCP/IP, οπότε οι διευθύνσεις είναι αυτές που ορίζει το πρωτόκολλο IP. Όπως θα δείτε σε λίγο, μία διεύθυνση IP αντιστοιχεί σε μία διεπαφή του host, δηλαδή, όχι στον ίδιο τον υπολογιστή (ή τον κόμβο). Για να είναι εύκολος ο εντοπισμός των διευθύνσεων, σε κάθε περιοχή στο διαδίκτυο (π.χ. ntua.gr) υπάρχει ένας ή περισσότεροι εξυπηρετητές DNS. Αυτοί περιέχουν μια βάση δεδομένων που αντιστοιχίζει τα ονόματα των κόμβων της συγκεκριμένης περιοχής (π.χ. atlas.central.ntua.gr) σε διευθύνσεις **IPv4** και/ή **IPv6**. Οι πρώτες έχουν μήκος 4 byte ή 32 bit (π.χ. `147.102.240.1`), ενώ οι δεύτερες 16 byte ή 128 bit (π.χ. `CEDF:BP76:3245:4464:FACE:2E50:3025:DF12`). Επίσης μπορεί να περιέχει πληροφορίες για τις διευθύνσεις άλλων εξυπηρετητών DNS «υπεύθυνων» για την περιοχή (name servers – NS), διευθύνσεις εξυπηρετητών ηλεκτρονικού ταχυδρομείου (mail exchangers – MX), επίσημα ονόματα υπολογιστών (canonical names – CNAME), κλπ. Οι εξυπηρετητές DNS απαντούν σε αιτήσεις άλλων εξυπηρετητών DNS, καθώς και χρηστών του διαδικτύου για την αντιστοιχία ενός ονόματος σε διεύθυνση IP και το αντίστροφο, ερευνώντας την παγκόσμια ιεραρχία DNS γι' αυτά.

Στην Εργαστηριακή Άσκηση 1, αναφέρθηκε ότι για τη λειτουργία της στοίβας πρωτοκόλλων TCP/IP, κάθε υπολογιστής ή κόμβος υποχρεούται να διαθέτει μία τουλάχιστον διεύθυνση IP για κάθε διεπαφή που διαθέτει, ανεξαρτήτως του τύπου της (Ethernet, LAN, WAN, virtual κτλ), αρκεί να είναι μοναδική στο υποδίκτυο (subnet) όπου ανήκει. Η διεύθυνση αυτή μπορεί να τίθεται στατικά στον ίδιο τον υπολογιστή ή, εναλλακτικά, να «νοικιάζεται» δυναμικά από ένα εξυπηρετητή DHCP. Υπενθυμίζεται ότι μπορούμε να λάβουμε πληροφορίες σχετικά με τις ρυθμίσεις του DHCP (διεύθυνση που αποδόθηκε στο host, διεύθυνση εξυπηρετητή DHCP, διάρκεια μίσθωσης) με τη βοήθεια της εντολής `ipconfig` των Windows.

Όμως, τα τοπικά δίκτυα (LAN) λειτουργούν τυπικά με διευθύνσεις MAC (μήκους 6 byte) και δεν γνωρίζουν τίποτε περί διευθύνσεων IP. Για να είναι εφικτή η επικοινωνία δύο υπολογιστών, πρέπει ο καθένας να γνωρίζει τη διεύθυνση MAC του άλλου. Η λύση που χρησιμοποιείται, λοιπόν, είναι να σταλθεί ένα πακέτο εκπομπής που ρωτά: «Σε ποιον ανήκει η διεύθυνση IP 147.102.240.1;» Το πακέτο θα φτάσει με εκπομπή (broadcast) σε κάθε μηχανή του υποδικτύου 147.102.240.0 (εάν η μάσκα είναι 255.255.255.0) και κάθε μία απ' αυτές θα ελέγξει αν απευθύνεται στη δική της διεύθυνση IP. Μόνο η μηχανή με τη σωστή διεύθυνση IP θα αποκριθεί με μονο-εκπομπή (unicast) δίνοντας τη διεύθυνση MAC αυτής. Το πρωτόκολλο που διατυπώνει αυτή την ερώτηση, απαντάει και λαμβάνει την απάντηση, είναι το ARP.

Σε συντομία η λειτουργία του ARP έχει ως εξής:

- Ο Α γνωρίζει την διεύθυνση IP του Β και θέλει να μάθει τη φυσική του διεύθυνση (MAC)
- Ο Α εκπέμπει μια αίτηση ARP που περιέχει τη διεύθυνση IP του Β
- Όλοι είναι υποχρεωμένοι να ακούν για ερωτήσεις ARP και να απαντούν
- Ο Β λαμβάνει το πακέτο ARP και απαντά με τη φυσική του διεύθυνσή του
- Ο Α καταχωρεί το ζεύγος IP-"φυσική διεύθυνση" σε προσωρινή μνήμη[1]
- Οι καταχωρήσεις εκπνέουν χρονικά μετά από μερικά λεπτά και η πληροφορία διαγράφεται

Σημειώνεται ότι η προαναφερθείσα διαδικασία, που σχετίζεται με τις διευθύνσεις MAC καθώς και με το πρωτόκολλο ARP, ισχύει για την επίλυση διευθύνσεων *αποκλειστικά* μέσα στην τοπική περιοχή εκπομπής (broadcast domain)[2]. Μεταξύ διαφορετικών τοπικών περιοχών εφαρμόζονται αλγόριθμοι δρομολόγησης και γίνεται επικοινωνία στο στρώμα δικτύου (IP). Το πακέτο IP δρομολογείται προς την πύλη (gateway) που υποδεικνύουν οι πίνακες δρομολόγησης, την οποία (πύλη) αφορά και η ανάγκη επίλυσης διευθύνσεων. Δηλαδή, αφού τα πακέτα IP που προορίζονται για μηχανές εκτός του τοπικού υποδικτύου (147.102.38.0/24 για την περίπτωση του ΕΠΥ της Σχολής) αποστέλλονται στην πύλη, η ως άνω διαδικασία επίλυσης διευθύνσεων γίνεται για να προσδιορισθεί το ζεύγος IP-"φυσική διεύθυνση" της πύλης.

Όσον αφορά τις διαδρομές στο διαδίκτυο, δεν υπάρχει μηχανισμός για την αντιστοίχιση αυτών σε διευθύνσεις IP, ανάλογος των μηχανισμών που περιγράφθηκαν προηγουμένως για τα ονόματα και τις διευθύνσεις MAC. Παρότι, μια διαδρομή μεταξύ υποδικτύων μπορεί να ορισθεί ως μια σειρά από διευθύνσεις IP μέσω των οποίων θα διέλθει το πακέτο IP, ο προσδιορισμός των συγκεκριμένων διαδρομών γίνεται κατανεμημένα βάσει των αλγορίθμων δρομολόγησης. Για κάθε πακέτο το επόμενο βήμα της διαδρομής προκύπτει από τον πίνακα δρομολόγησης. Επιπλέον, ένα πακέτο IP. ανάλογα με το υποδίκτυο προορισμού του, προωθείται προς την κατάλληλη διεπαφή εξόδου και μέσω αυτής στον επόμενο κόμβο. Ελλείψει ειδικότερης πληροφόρησης, το πακέτο προωθείται στην προκαθορισμένη πύλη (default gateway).

Απομένει να περιγραφθεί το πιο ουσιαστικό μέρος της όλης διαδικασίας, δηλαδή, η επικοινωνία μεταξύ δύο υπολογιστών. Αυτή γίνεται όταν ο ένας εξ αυτών (πελάτης – client) ζητά μια υπηρεσία από τον άλλο (εξυπηρετητής – server). Βεβαίως ένας υπολογιστής μπορεί να είναι ταυτόχρονα πελάτης και εξυπηρετητής. Για να δοθούν υπηρεσίες προς άγνωστους καλούντες (πελάτες), ορίζεται μια **θύρα** (port) ως σημείο πρώτης επαφής, όπου η εφαρμογή ή ο εξυπηρετητής «ακούει». Πρόκειται για έναν αριθμό μήκους 16 bit, επομένως ορίζονται συνολικά 65536 θύρες (0 έως 65535). Οι πρώτες 1024 θύρες (0 έως 1023) θεωρούνται πασίγνωστες (well known ports) και αντιστοιχούν σε γνωστές εφαρμογές. Οι θύρες 1024 έως 49151 χρησιμοποιούνται από διάφορες εφαρμογές, αλλά προηγείται δέσμευσή τους μέσω διαδικασίας εγγραφής (Registered Ports), ενώ οι θύρες 49152 έως 65535 χρησιμοποιούνται ελεύθερα (Dynamic ή Private Ports).

Για παράδειγμα, οι εξυπηρετητές ιστού ακούνε συνήθως στη θύρα 80. Έτσι για την επίσκεψη σε μια ιστοσελίδα θα πρέπει να γίνει μια πρώτη επαφή με τον εξυπηρετητή ιστού στη θύρα 80 και να ζητηθεί η συγκεκριμένη σελίδα με το όνομά της. Όμως εάν η διεύθυνση IP του εξυπηρετητή ιστού δεν είναι γνωστή, θα πρέπει να προηγηθεί μια αίτηση στον τοπικό εξυπηρετητή DNS (που ακούει στη θύρα 53) για την αντιστοίχηση του ονόματος της ιστοθέσης (web site) σε διεύθυνση IP. Για την εξυπηρέτηση της αίτησης μπορεί να γίνουν διαδοχικές ερωτήσεις σε άλλους εξυπηρετητές, ακολουθώντας την παγκόσμια ιεραρχία DNS, με αποτέλεσμα αυξημένη καθυστέρηση. Για την αποφυγή του παραπάνω οι εξυπηρετητές DNS διαθέτουν μια προσωρινή μνήμη (cache) όπου

[1] Ο αποστολέας (Α) συμπεριλαμβάνει την IP διεύθυνσή του στο πακέτο ARP που στέλνει. Έτσι ο Β, με τη λήψη της αίτησης ARP, ενημερώνει και αυτός τον δικό του πίνακα ARP ώστε να μη χρειασθεί να προσφύγει σε διαδικασία επίλυσης της διεύθυνσής του Α όταν φτάσει η ώρα να του αποστείλει κάποιο πακέτο IP.

[2] Στο ΕΠΥ της Σχολής όλοι οι υπολογιστές του υποδικτύου 147.102.38.0/24 βρίσκονται εντός της ίδιας περιοχής εκπομπής.

κρατούν τις απαντήσεις στις πιο πρόσφατες αιτήσεις. Τελικά, το λογισμικό του χρήστη μαθαίνει τη διεύθυνση IP της ιστοθέσης (την οποία συνήθως τοποθετεί σε τοπική προσωρινή μνήμη για την περίπτωση που θα τη χρειαστεί και πάλι σύντομα). Για να μεταδώσει πακέτα IP προς τα εκεί, πρέπει να τα περάσει στο στρώμα ζεύξης δεδομένων (data link) της κάρτας δικτύου του, όπου θα ενθυλακωθούν σε πλαίσια προτού μεταδοθούν.

Στην άσκηση αυτή θα μελετήσετε τις λεπτομέρειες της δικτυακής επικοινωνίας σε τοπικό επίπεδο (LAN). Για τη διερεύνηση των παραπάνω, στα Windows XP θα χρησιμοποιηθεί η εντολή `arp`. Η εντολή `arp` έχει διαγνωστικές λειτουργίες σχετικά με την εφαρμογή του πρωτοκόλλου ARP σε έναν υπολογιστή. Για βοήθεια πηγαίνετε στο *Start* → *Help and Support* και στο πλαίσιο *Search* πληκτρολογήστε "TCP/IP utilities", οπότε εμφανίζονται όλες οι σχετικές εντολές. Περισσότερες πληροφορίες για το πρωτόκολλο ARP μπορείτε να βρείτε στην ιστοσελίδα του σχετικού προτύπου RFC 826 http://www.faqs.org/rfcs/rfc826.html.

Άσκηση 1 – Ο Πίνακας ARP

1.1. Δείτε και καταγράψτε τον πίνακα ARP του υπολογιστή σας πληκτρολογώντας `arp -a` ή `arp -g` σε ένα παράθυρο εντολών. Ο πίνακας αυτός περιέχει τις διευθύνσεις MAC και IP των υπολογιστών με τους οποίους έχει επικοινωνήσει πρόσφατα ο δικός σας.

1.2. Σε ένα παράθυρο εντολών εκτελέστε την εντολή `ping <διεύθυνση IP>`, όπου `<διεύθυνση IP>` η διεύθυνση IP του διπλανού σας υπολογιστή. Δείτε πάλι και καταγράψτε τον πίνακα ARP του υπολογιστή σας. Τι παρατηρείτε;

1.3. Σημειώστε τις διευθύνσεις IP της προκαθορισμένης πύλης και των εξυπηρετητών DNS του υπολογιστή σας. [*Υπόδειξη: Για την εύρεση του default gateway και των εξυπηρετητών DNS μπορείτε να χρησιμοποιήσετε την εντολή* `ipconfig /all`.]

1.4. Υπάρχουν οι διευθύνσεις αυτές στον πίνακα ARP του υπολογιστή σας;

Σε ένα παράθυρο εντολών εκτελέστε την εντολή `arpclear` ώστε να αδειάσει ο πίνακας ARP[3] του υπολογιστή σας καθώς και `ipconfig /flushdns` για να διαγραφούν οι γνωστές αντιστοιχήσεις ονομάτων σε διευθύνσεις IP. Στη συνέχεια επισκεφτείτε την κεντρική σελίδα του Πολυτεχνείου www.ntua.gr χρησιμοποιώντας κάποιον πλοηγό ιστού. Μιας και η διεύθυνση IP του εξυπηρετητή ιστού του ΕΜΠ δεν είναι γνωστή στον πλοηγό ιστού (ακόμη και εάν ήταν μόλις τη διαγράψατε), θα προηγηθεί επικοινωνία με τον εξυπηρετητή DNS ώστε να προσδιορισθεί. Κατόπιν θα ακολουθήσει η ανταλλαγή μηνυμάτων μεταξύ του πλοηγού ιστού (πελάτης) και του εξυπηρετητή.

1.5. Ποιες από τις διευθύνσεις IP που προσδιορίσατε στο ερώτημα 1.3 έχουν τώρα καταχωρηθεί στον πίνακα ARP και γιατί; [*Υπόδειξη: Εάν πελάτης και εξυπηρετητής βρίσκονται σε διαφορετικά υποδίκτυα, η επικοινωνία στο στρώμα IP γίνεται μέσω της πύλης που υποδεικνύει ο πίνακας δρομολόγησης.*]

1.6. Ποιες από τις διευθύνσεις IP που προσδιορίσατε στο ερώτημα 1.3 δεν καταχωρήθηκαν στον πίνακα ARP και γιατί;

Άσκηση 2 – Το πλαίσιο Ethernet

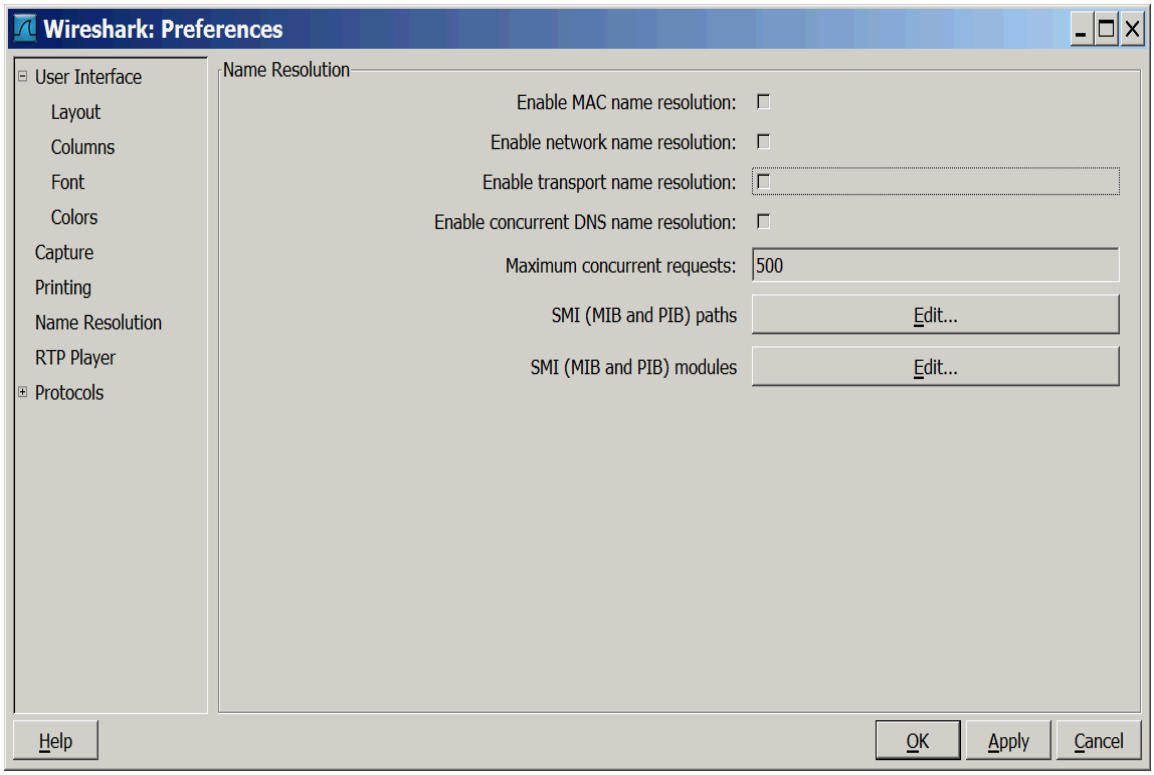
Σε αυτή την άσκηση θα καταγραφούν τα πλαίσια του Ethernet που παράγονται κατά την επίσκεψη μιας ιστοσελίδας. Οι απαντήσεις, στις ερωτήσεις αυτής και της επόμενης άσκησης, προϋποθέτουν

[3] Η εντολή αυτή ισοδυναμεί με την `arp -d`, την οποία ο χρήστης labuser του ΕΠΥ δεν μπορεί να εκτελέσει ελλείψει κατάλληλων δικαιωμάτων.

γνώση της θεωρίας που παρουσιάσθηκε στην Εργαστηριακή Άσκηση 1 και ειδικά της δομής των πλαισίων Ethernet. Περισσότερες πληροφορίες για το Ethernet και την εξέλιξή του μπορείτε να βρείτε στην ιστοθέση http://www.techfest.com/networking/lan/ethernet.htm, ενώ λεπτομέρειες για τη δομή του πλαισίου Ethernet και τα πεδία του θα βρείτε στην ιστοσελίδα http://www.techfest.com/networking/lan/ethernet2.htm. Υπενθυμίζεται ότι το αρχικό πρότυπο για ταχύτητα 10 Mbps ορίζει ότι το ελάχιστο μήκος πλαισίου Ethernet είναι 64 byte[4]. Εάν το πακέτο που ενθυλακώνεται στο πλαίσιο έχει πολύ μικρό μήκος, τότε θα παραγεμισθεί με μηδενικά ώστε το μεταδιδόμενο πλαίσιο να αποκτήσει το ελάχιστο μήκος 64 byte. Το ίδιο πρότυπο ορίζει ότι το μέγιστο μήκος πλαισίου Ethernet είναι 1.518 byte, οπότε τα πολύ μεγάλα πακέτα θα πρέπει να τεμαχιστούν πριν τη μετάδοσή τους[5].

Προτού αρχίσετε την καταγραφή φροντίστε να αδειάσετε την προσωρινή μνήμη (cache) του πλοηγού. Στον Internet Explorer επιλέξτε *Tools→Internet Options*, στην πινακίδα (tab) *General* πιέστε το κουμπί *Delete Files*, επιβεβαιώστε την πρόθεσή σας, περιμένετε να ολοκληρωθεί η διαγραφή και κλείστε το παράθυρο διαλόγου. Στον Mozilla Firefox επιλέξτε *Tools → Clear Private Data*, επιλέξτε το cache στον πίνακα που θα εμφανισθεί, επιβεβαιώστε την πρόθεσή σας, περιμένετε να ολοκληρωθεί η διαγραφή και κλείστε το παράθυρο διαλόγου.

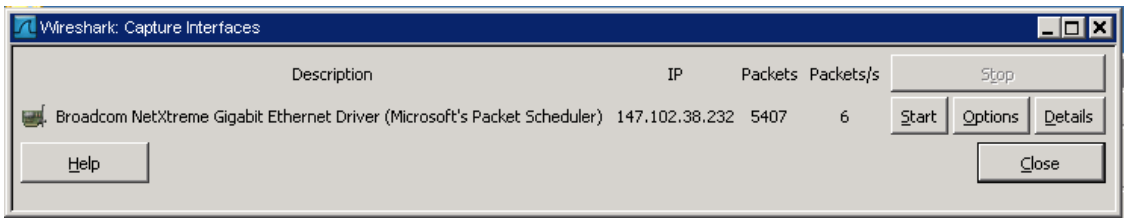
Αφού ξεκινήσετε το Wireshark, ακολουθήστε από το μενού του κεντρικού παραθύρου, τη διαδρομή *Edit → Preferences…* και από τη λίστα επιλογών στα αριστερά διαλέγετε το *Name Resolution*. Βεβαιωθείτε ότι κανένα από τα τετραγωνάκια στα δεξιά δεν είναι επιλεγμένο και πατήστε *OK*.



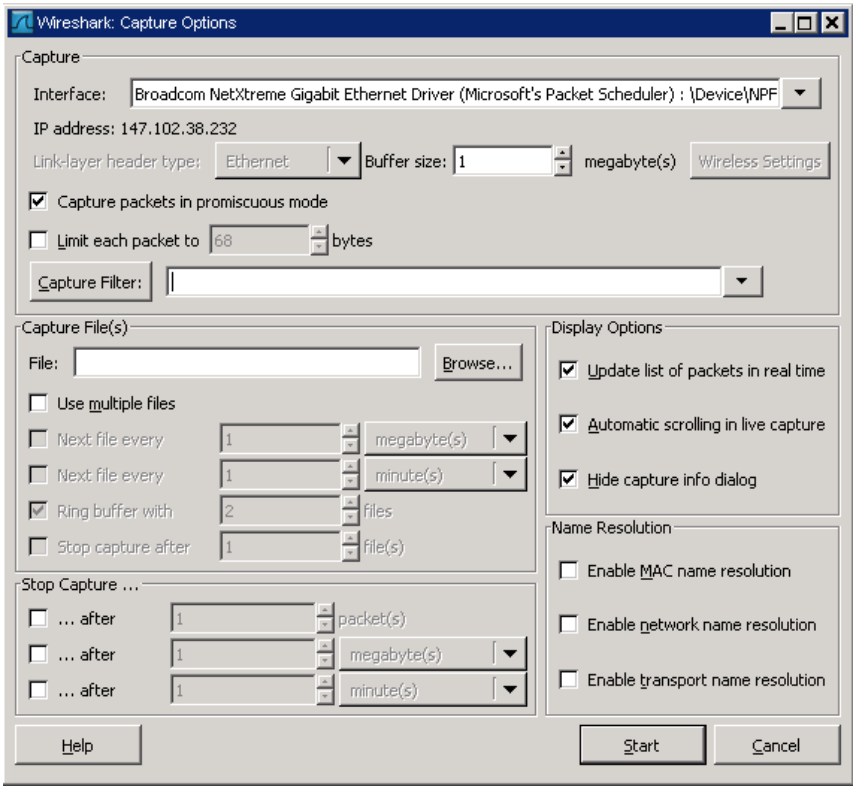
[4] Το προοίμιο δε συμπεριλαμβάνεται στη μέτρηση όταν αναφερόμαστε σε μήκος πλαισίου (ενώ το CRC περιλαμβάνεται). Τα πρώτα 56 bit του προοιμίου είναι εναλλαγές του 1 και του 0 για να επιτευχθεί συγχρονισμός. Χρησιμεύουν ώστε τα ηλεκτρονικά στοιχεία να προλάβουν να ανιχνεύσουν την ύπαρξη σήματος και να αρχίσουν να "διαβάζουν" προτού αρχίσει η μετάδοση του πλαισίου. Τα επόμενα 8 bit είναι 10101011 και υποδεικνύουν την αρχή του πλαισίου. Παρατηρείστε ότι μόνο το τελευταίο bit αποτελεί παραβίαση του κανόνα εναλλαγής και αυτό είναι που πραγματικά δείχνει την αρχή.

[5] Το νεότερο πρότυποThe IEEE 802.3ac του 1998 επέκτεινε το μέγιστο επιτρεπόμενο μήκος πλαισίου στα 1522 byte ώστε να υπάρξει χώρος για την εισαγωγή ετικετών "VLAN tag" μήκους 4 byte στο πλαίσιο Ethernet (αμέσως μετά τις διευθύνσεις MAC και πριν το πεδίο Τύπος/Μήκος).

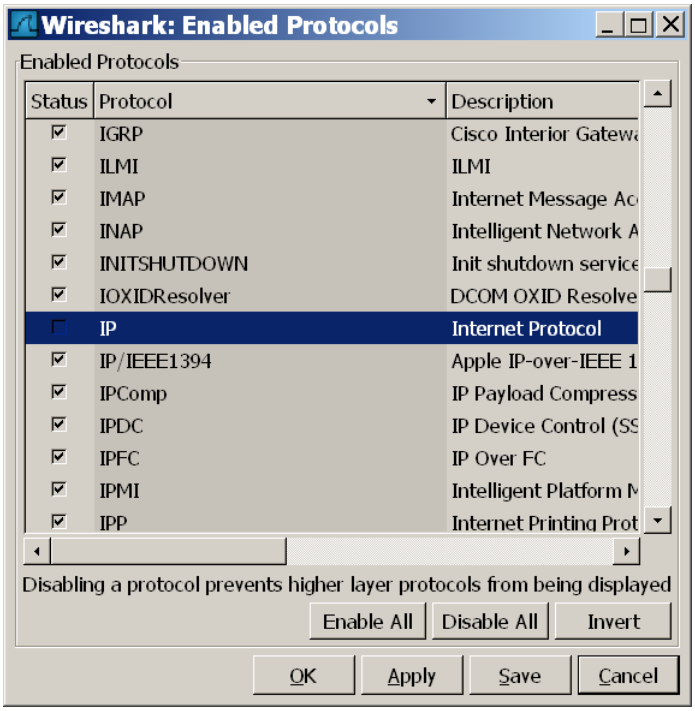
Για τη διαδικασία της καταγραφής ακολουθούμε από το μενού επιλογών τη διαδρομή *Capture* → *Interfaces…* Στο παράθυρο που εμφανίζεται θα δείτε όλες τις διαθέσιμες κάρτες δικτύου του υπολογιστή σας, την IP διεύθυνση τους και μια ένδειξη για το πλήθος και ρυθμό πακέτων (εφόσον υπάρχει τηλεπικοινωνιακή κίνηση). Επιλέξτε την κάρτα δικτύου του υπολογιστή σας μέσω της οποίας θα γίνει η σύλληψη των πακέτων και πιέστε το κουμπί *Options* που της αντιστοιχεί.



Στο επόμενο παράθυρο που εμφανίζεται, μπορείτε να ορίσετε επιλογές σχετικές με τη διαδικασία σύλληψης, όπως, φίλτρα, διάρκεια σύλληψης, και τον τρόπο εμφάνισης των αποτελεσμάτων σύλληψης, όπως, εμφάνιση σε πραγματικό χρόνο. Βεβαιωθείτε ότι καμιά από τις επιλογές της κατηγορίας *Name Resolution* δεν είναι ενεργοποιημένη. Πατώντας το κουμπί *Start* αρχίζει η καταγραφή!



Στη συνέχεια επισκεφτείτε την ιστοσελίδα http://www.cn.ntua.gr/ που φιλοξενείται στον υπολογιστή με διεύθυνση IP 147.102.40.1. Μόλις φορτωθεί πλήρως η σελίδα πατήστε το *Stop* για να σταματήσει η καταγραφή. Επειδή στην άσκηση αυτή δεν θα ασχοληθείτε με το IP και πρωτόκολλα ανωτέρων στρωμάτων, θα αλλάξετε την εμφάνιση του παραθύρου λίστας καταγεγραμμένων πακέτων, ώστε να μη δείχνει πληροφορία για πρωτόκολλα πάνω από το IP. Πηγαίνετε *Analyze* → *Enabled protocols* και, αφού βρείτε τη γραμμή για το IP με κλικ στο αντίστοιχο τετράγωνο, απενεργοποιείστε την ανάλυση του πρωτοκόλλου IP.



Θα βασίσετε τις απαντήσεις σας για τις επόμενες ερωτήσεις στα στοιχεία της καταγραφής και ειδικότερα στις πληροφορίες που αποτυπώνονται στα παράθυρα με τις λεπτομέρειες της επικεφαλίδας και το περιεχόμενο των πλαισίων. Υπενθυμίζουμε ότι τα πακέτα IP και ARP ενθυλακώνονται σε πλαίσια Ethernet.

2.1. Βρείτε και επιλέξτε το πλαίσιο Ethernet που περιέχει το πρώτο μήνυμα HTTP GET και προσδιορίστε τη διεύθυνση MAC του υπολογιστή σας. *[Υπόδειξη: Ακολουθήστε τη διαδρομή Edit → Find Packet… και στο παράθυρο που θα εμφανιστεί επιλέξτε String. Στο πλαίσιο Filter: πληκτρολογήστε "GET", χωρίς τα εισαγωγικά, και πατήστε το κουμπί Find. Εν ανάγκη συνεχίστε την αναζήτηση από την αρχή της καταγραφής].*

2.2. Ποια είναι η διεύθυνση MAC του προορισμού του πλαισίου;

2.3. Είναι η παραπάνω διεύθυνση MAC αυτή του www.cn.ntua.gr; *[Υπόδειξη: Ελέγξετε εάν ο www.cn.ntua.gr βρίσκεται στο ίδιο υπο-δίκτυο με τον υπολογιστή σας].*

2.4. Εάν όχι, σε ποια συσκευή ανήκει και γιατί; *[Υπόδειξη: Αναζητήστε μεταξύ των συσκευών που προσδιορίσατε στο ερώτημα 1.3].*

2.5. Ποια είναι η δεκαεξαδική τιμή του πεδίου *Τύπος* (Type) του παραπάνω πλαισίου και ποιο πρωτόκολλο υποδεικνύει; *[Υπόδειξη: αναπτύξτε την επικεφαλίδα του πλαισίου Ethernet κάνοντας κλικ στο σύμβολο + ώστε να εμφανισθούν όλα τα πεδία που την απαρτίζουν].*

2.6. Ποιο είναι το μήκος του πλαισίου σε byte;

2.7. Πόσα byte του πλαισίου Ethernet προηγούνται του χαρακτήρα ASCII "G" της λέξης GET; *[Υπόδειξη: επιλέξτε το πεδίο δεδομένων του προηγούμενου αναπτύγματος ώστε να εμφανισθούν στο παράθυρο με τα περιεχόμενα τα αντίστοιχα byte δεδομένων].*

Στη συνέχεια βρείτε και επιλέξτε το πλαίσιο Ethernet που περιέχει την απάντηση στο προηγούμενο μήνυμα HTTP [*Υπόδειξη: Ακολουθώντας την υπόδειξη του ερωτήματος 2.1, αναζητείστε την ακολουθία "200 OK", χωρίς τα εισαγωγικά, στο περιεχόμενο των αμέσως επόμενων πλαισίων της λίστας καταγεγραμμένων πακέτων.*]

2.8. Ποια είναι η διεύθυνση MAC του αποστολέα;

2.9. Είναι η παραπάνω διεύθυνση MAC αυτή του www.cn.ntua.gr;

2.10. Σε ποια συσκευή ανήκει η διεύθυνση αυτή;.

2.11. Ποια είναι η διεύθυνση MAC του παραλήπτη;

2.12. Σε ποιον υπολογιστή ανήκει;

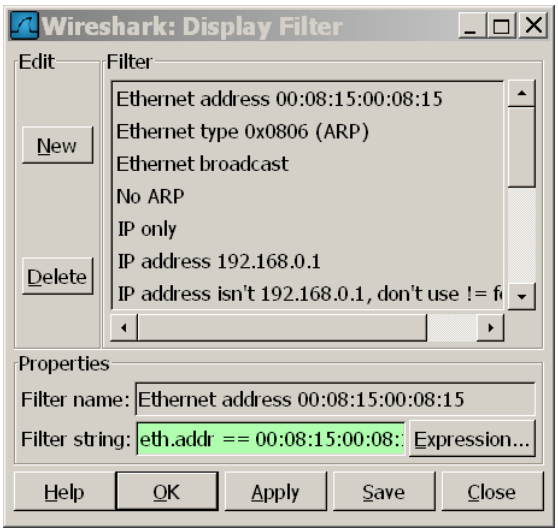
2.13. Ποια είναι η δεκαεξαδική τιμή του πεδίου Τύπος του παραπάνω πλαισίου;
2.14. Ποιο είναι το μήκος του πλαισίου σε byte;
2.15. Πόσα byte του πλαισίου Ethernet προηγούνται του χαρακτήρα ASCII "O" της λέξης OK;
2.16. Ποια από τα πεδία του πλαισίου Ethernet καταγράφει το Wireshark; [*Υπόδειξη: συμβουλευθείτε την http://www.techfest.com/networking/lan/ethernet2.htm#2.1 για να δείτε τα πεδία του πλαισίου Ethernet και τα ονόματά τους.*]
2.17. Τι συμβαίνει με το CRC; [*Υπόδειξη: δείτε http://www.wireshark.org/faq.html#q7.10.*]

Άσκηση 3 – Περισσότερα για τα πακέτα ARP

Σε αυτή την άσκηση θα καταγραφούν τα πακέτα που ανταλλάσσονται στο πρωτόκολλο ARP, με τη βοήθεια του Wireshark. Υπενθυμίζουμε ότι ο χρήστης μπορεί να ορίσει κατάλληλα φίλτρα καταγραφής/ανάλυσης τα οποία περιορίζουν την κίνηση που καταγράφεται/αναλύεται σύμφωνα με τα κριτήριά του. Έτσι, σύμφωνα με την ορολογία του Wireshark, διακρίνουμε τα *capture* και τα *display filters* αντίστοιχα, τα οποία θα αναλυθούν στις επόμενες σειρές ασκήσεων. Υπενθυμίζεται ότι πληροφορίες σχετικά με το Wireshark μπορείτε να βρείτε στο http://www.wireshark.org/docs/.

Ξεκινήσετε μια νέα καταγραφή με το Wireshark όπως στην άσκηση 2. Στη συνέχεια ανοίξτε τη γραμμή εντολών και πληκτρολογείστε την εντολή `arp -a` ώστε να βεβαιωθείτε ότι η διεύθυνση IP του διπλανού σας υπολογιστή δεν περιέχεται στον πίνακα ARP. Αν περιέχεται τότε πληκτρολογήστε από το παράθυρο εντολών την εντολή `arpclear`. Στη συνέχεια, εκτελέστε την εντολή `ping <IP διεύθυνση>`, όπου `<IP διεύθυνση>` η διεύθυνση IP του διπλανού σας υπολογιστή, και μόλις ολοκληρωθεί η εκτέλεση της εντολής πατήστε το *Stop* για να σταματήσει η καταγραφή. Επαναλάβετε τον έλεγχο του πίνακα arp μετά από την εκτέλεση της εντολής ping. Προσοχή: Συνεννοηθείτε με το διπλανό σας ώστε να μην κάνετε ping *ταυτόχρονα* ο ένας προς τον άλλο!

Στο κύριο παράθυρο του Wireshark, όπου φαίνεται η καταγεγραμμένη δικτυακή κίνηση, μπορεί ενδεχομένως να παρατηρήσετε κίνηση που δε σχετίζεται με την παραπάνω εντολή. Η ζητούμενη κίνηση μπορεί να απομονωθεί με την εφαρμογή φίλτρου παρατήρησης ως εξής: πηγαίνετε *Analyze → Display Filters…* και στο παράθυρο *Filter* επιλέξτε τη γραμμή Ethernet address 00:08:15:00:08:15. Στη συνέχεια στο πεδίο *Filter string* διορθώστε τη διεύθυνση ώστε να είναι ίση με τη διεύθυνση MAC της κάρτας δικτύου του υπολογιστή σας. **Η σύνταξη του φίλτρου είναι σωστή όταν το πεδίο "Filter string" έχει πράσινο χρώμα**. Το φίλτρο ενεργοποιείται με το πάτημα του *Apply*, ενώ το παράθυρο διαλόγου κλείνει με *OK*.



3.1 Τι αποτέλεσμα έχει η εφαρμογή αυτού του φίλτρου;

Στη συνέχεια κάντε κλικ στο τέλος της έκφρασης στο πράσινο πεδίο που περιέχει το προηγούμενο φίλτρο, προσθέστε την έκφραση `and arp` και πιέστε το *Apply*.

3.2 Τι αποτέλεσμα έχει η εφαρμογή του δεύτερου φίλτρου;
3.3 Πόσα πακέτα ARP ανταλλάχθηκαν κατά την εκτέλεση της εντολής ping;
3.4 Τι αποτέλεσμα έχει η χρήση του or αντί για το and στο προηγούμενο φίλτρο;

Επιλέξτε το πλαίσιο που περιέχει την ερώτηση για το ποιος έχει τη διεύθυνση IP του διπλανού σας υπολογιστή (δηλαδή, ποια είναι η διεύθυνση MAC αυτού) με βάση την πληροφορία στη στήλη Info του παραθύρου με τη λίστα καταγεγραμμένων πακέτων. Για να δείτε την πληροφορία που σχετίζεται με το στρώμα ζεύξης δεδομένων, πιέστε το + στη γραμμή με τίτλο Ethernet II στο παράθυρο με τις λεπτομέρειες επικεφαλίδας.

3.5 Σε ποιον υπολογιστή ανήκει η διεύθυνση MAC του αποστολέα και σε ποιον του παραλήπτη;
3.6 Ποια είναι η δεκαεξαδική τιμή του πεδίου *Τύπος* του παραπάνω πλαισίου και ποιο πρωτόκολλο υποδεικνύει;

Στο Ethernet, η μετάδοση των byte γίνεται έτσι ώστε το πλέον σημαντικό byte να μεταδίδεται πρώτο. Αντίθετα, όσον αφορά τη μετάδοση των bit ενός byte, το λιγότερο σημαντικό bit μεταδίδεται πρώτο. Στην Εργαστηριακή Άσκηση 1 είδατε ότι το υψηλότερης τάξης bit (47^o) της διεύθυνσης δείχνει το κατά πόσο η διεύθυνση είναι ομαδική ή ατομική, ενώ το bit που ακολουθεί (46^o) δείχνει τα κατά πόσο πρόκειται για τοπική ή μοναδική διεύθυνση.

3.7 Τι είδους διεύθυνση (ομαδική ή ατομική, τοπική ή μοναδική) είναι κάθε μία από τις προηγούμενες διευθύνσεις; *[Υπόδειξη: Αναπτύξτε τα περιεχόμενα των πεδίων διεύθυνσης πηγής και προορισμού του πλαισίου Ethernet]*.
3.8 Σε ποια θέση του πρώτου byte εμφανίζεται το bit υψηλότερης τάξης της διεύθυνσης MAC και σε ποια το επόμενό του;

Για να δείτε όλη την πληροφορία που σχετίζεται με το πρωτόκολλο ARP, πιέστε το + στη γραμμή Address Resolution Protocol στο παράθυρο με τις λεπτομέρειες επικεφαλίδας. Αφού μελετήσετε τις με προσοχή τα πεδία που αποτελούν το πακέτο ARP απαντήστε τις επόμενες ερωτήσεις:

3.9 Καταγράψτε τα ονόματα και το μήκος σε byte των πεδίων του πακέτου ARP χρησιμοποιώντας ως υπόδειγμα το σχήμα στο τέλος του φυλλαδίου των απαντήσεων.
3.10 Πόσα byte του πλαισίου Ethernet προηγούνται του πεδίου ARP opcode;
3.11 Πόσα byte είναι το συνολικό μέγεθος του πακέτου ARP request;
3.12 Ποια η τιμή του πεδίου ARP opcode;
3.13 Το πακέτο ARP μεταφέρει τη διεύθυνση MAC του αποστολέα;
3.14 Το πακέτο ARP μεταφέρει τη διεύθυνση IP του αποστολέα;
3.15 Σε ποιο πεδίο του πακέτου ARP περιέχεται η ερώτηση, δηλαδή, η διεύθυνση IP του υπολογιστή του οποίου αναζητείται η διεύθυνση MAC;

Εντοπίστε το πρώτο πακέτο ARP reply που αποτελεί την απόκριση στο παραπάνω πακέτο ARP request.

3.16 Ποια είναι η δεκαεξαδική τιμή του πεδίου *Τύπος* του παραπάνω πλαισίου και ποιο πρωτόκολλο υποδεικνύει;
3.17 Σε ποιον υπολογιστή ανήκει η διεύθυνση MAC του αποστολέα και σε ποιον του παραλήπτη;
3.18 Πόσα byte του πλαισίου Ethernet προηγούνται του πεδίου ARP opcode;
3.19 Ποια η τιμή του πεδίου ARP opcode;
3.20 Το πακέτο ARP μεταφέρει τη διεύθυνση IP του αποστολέα;
3.21 Το πακέτο ARP μεταφέρει τη διεύθυνση IP του παραλήπτη;

3.22 Σε ποιο πεδίο του πακέτου ARP περιέχεται η απάντηση, δηλαδή, η διεύθυνση MAC του υπολογιστή που έχει τη διεύθυνση IP για την οποία έγινε η ερώτηση;
3.23 Πόσα byte είναι το συνολικό μέγεθος του πακέτου ARP reply;
3.24 Είναι το προηγούμενο μήκος ίδιο με αυτό που προσδιορίσατε στην ερώτηση 3.11;
3.25 Δοθέντος του μήκους των πεδίων των πακέτων ARP request/reply που προσδιορίσατε πριν, πώς εξηγείτε το διαφορετικό μήκος πλαισίων Ethernet για πακέτα ARP reply και ARP request; *[Υπόδειξη: Η βιβλιοθήκη WinPcap που χρησιμοποιεί το Wireshark, όπως φαίνεται και στο σχετικό σχήμα της Εργαστηριακής Άσκησης 1, συλλαμβάνει τα απερχόμενα πλαίσια προτού μεταδοθούν στο τοπικό δίκτυο]*.

Από τα προηγούμενα είναι προφανές ότι τα πακέτα του πρωτοκόλλου ARP δεν είναι πακέτα IP.

3.26 Ποιο πεδίο του πλαισίου Ethernet τα διαφοροποιεί;
3.27 Ποιο πεδίο υποδεικνύει το κατά πόσον πρόκειται για πακέτο ARP request ήARP reply;.
3.28 Γιατί η πληροφορία που μεταφέρουν τα πακέτα του πρωτοκόλλου ARP δεν μπορεί να μεταφερθεί με πακέτα IP;

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

Εργαστηριακή Άσκηση 2
Επικοινωνία στο τοπικό δίκτυο
(πλαίσιο Ethernet και πρωτόκολλο ARP)

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

Άσκηση 1

1.1 .....

.....

1.2 .....

.....

1.3 .....

.....

1.4 .....

1.5 .....

.....

.....

1.6 .....

.....

.....

Άσκηση 2

2.1 .....

2.2 .....

2.3 .....

2.4 .....

.....

.....

2.5 .....

2.6 .....

2.7 .....

2.8 .....

2.9 .....

2.10 .....

2.11 .....

2.12 .....

.....

Άσκηση 3