

Εργαστηριακή Άσκηση 3

Επικοινωνία στο τοπικό δίκτυο (πλαίσιο Ethernet και πρωτόκολλο ARP)

Ο σκοπός αυτής της εργαστηριακής άσκησης είναι η εξοικείωση με τους βασικούς μηχανισμούς που απαιτούνται ώστε να υπάρξει επικοινωνία μεταξύ υπολογιστών συνδεδεμένων σε τοπικό δίκτυο (LAN). 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, να «νοικιάζεται» από ένα εξυπηρετητή DHCP ή να δημιουργείται αυτόματα. Όμως για την επικοινωνία εντός του τοπικού δικτύου χρησιμοποιούνται οι διευθύνσεις του εκάστοτε φυσικού στρώματος, διευθύνσεις MAC για τη συνήθη περίπτωση του Ethernet. Οπότε απαιτείται ένας μηχανισμός αντιστοίχισης διευθύνσεων, η μελέτη του οποίου είναι το αντικείμενο αυτής της άσκησης για το IPv4.

Το πλαίσιο Ethernet

Το Ethernet πρωτοεμφανίσθηκε περί το 1973 ως κλειστό προϊόν των εταιρειών Digital Equipment Corporation (DEC), Intel και Xerox. Έγινε πρότυπο αρκετά αργότερα, το 1983, γνωστό ως IEEE 802.3. Στο κλασικό ενσύρματο Ethernet και το αρχικό πρότυπο IEEE 802.3 για ταχύτητα 10 Mbps, της μετάδοσης του πλαισίου προηγείται μια σειρά 64 bit, το Preamble (Προοίμιο), που επιτρέπει τον συγχρονισμό του δέκτη με τον αποστολέα σηματοδοτώντας ταυτόχρονα την αρχή του πλαισίου. Τα πρώτα 56 bit του προοιμίου είναι εναλλαγές του 1 και του 0 για να επιτευχθεί συγχρονισμός. Χρησιμοποιούν 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.

Το πλαίσιο Ethernet ξεκινά με την *Επικεφαλίδα (Header)* και ακολουθούν τα *Δεδομένα (Data)*, δηλαδή, η προς μετάδοση πληροφορία. Το πλαίσιο τελειώνει με το πεδίο *CRC (Άθροισμα Ελέγχου)* μήκους 4 byte που ακολουθείται από ένα υποχρεωτικό κενό (*interframe gap*) μήκους 12 byte. Υπάρχουν δύο είδη πλαισίων, το *Ethernet II* και το *IEEE 802.3*. Το πιο συνηθισμένο είναι το Ethernet II, όπου ενθυλακώνονται τα πακέτα IP και τα δεδομένα πολλών άλλων πρωτοκόλλων. Η επικεφαλίδα Ethernet II περιλαμβάνει δύο διευθύνσεις MAC μήκους 6 byte έκαστη, μία για τον προορισμό και μία για την πηγή, καθώς και το πεδίο *Type (Τύπος)*. Ο *Τύπος* δείχνει το πρωτόκολλο ανώτερου στρώματος που ενθυλακώνεται στο πλαίσιο. Στο επόμενο σχήμα φαίνεται παραστατικά ένα πλαίσιο Ethernet II με το προοίμιό του για τρεις χαρακτηριστικές περιπτώσεις ενθυλάκωσης.

Προοίμιο (8 byte)	Διεύθυνση παραλήπτη (6 byte)	Διεύθυνση αποστολέα (6 byte)	Τύπος (2 byte)	Δεδομένα (46 -1500 byte)	CRC (4 byte)
<div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: 80%;"> <div style="display: flex; justify-content: space-between; align-items: center;"> 0x800 Πακέτο IP (46 -1500 byte) </div> </div>					
<div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: 80%;"> <div style="display: flex; justify-content: space-between; align-items: center;"> 0x806 <div style="display: flex; flex-direction: column; align-items: center;"> <div style="display: flex; justify-content: space-between; width: 100%;"> Πακέτο ARP (28 byte) PAD (18 byte) </div> </div> </div> </div>					
<div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: 80%;"> <div style="display: flex; justify-content: space-between; align-items: center;"> 0x86DD Πακέτο IPv6 (46 -1500 byte) </div> </div>					

Στα πλαίσια IEEE 802.3, στη θέση του πεδίου *Τύπος* υπάρχει το πεδίο *Length (Μήκος)*. Το *Μήκος* δηλώνει πόσα byte περιέχονται στο πεδίο δεδομένων, από ένα ελάχιστο 0 μέχρι ένα μέγιστο 1.500 byte. Για να είναι δυνατή η συνύπαρξη πλαισίων Ethernet II και IEEE 802.3 στο ίδιο τοπικό δίκτυο,

οι τιμές του πεδίου *Τύπος* είναι μεγαλύτερες από 1536 (0x0600). Επιπλέον, μετά το *Μήκος* τα πλαίσια IEEE 802.3 περιέχουν μια επικεφαλίδα Logical Link Control (LLC), που καθορίζεται στο πρότυπο IEEE 802.2 (το άνω μέρος του στρώματος ζεύξης δεδομένων), ώστε να προσδιορίζεται το πρωτόκολλο ανωτέρου στρώματος που ενθυλακώνεται.

Η μετάδοση των byte για όλα τα πεδία του πλαισίου (και το προοίμιο που δεν αποτελεί μέρος του) γίνεται από αριστερά προς τα δεξιά και για κάθε byte πρώτα μεταδίδεται το λιγότερο σημαντικό bit (LSB) και τελευταίο το περισσότερο σημαντικό bit (MSB). Ο δέκτης εξετάζει το πεδίο ελέγχου του πλαισίου που λαμβάνει και αν ανιχνευθεί σφάλμα το πλαίσιο απορρίπτεται.

Το πρότυπο IEEE 802.3 ορίζει ότι το ελάχιστο μήκος πλαισίου Ethernet είναι 64 byte. Ένα έγκυρο πλαίσιο, από τη διεύθυνση προορισμού μέχρι το άθροισμα ελέγχου, έχει μήκος τουλάχιστον 64 byte, με τα μικρότερου μήκους πλαίσια να είναι συνήθως αποτέλεσμα συγκρούσεων. Εάν το πακέτο που ενθυλακώνεται στο πλαίσιο είναι μικρότερο από 46 byte, τότε θα παραγεμισθεί με μηδενικά (pad) μέχρι το ελάχιστο μήκος των 64 byte. Το ίδιο πρότυπο ορίζει ότι το μέγιστο μήκος πλαισίου Ethernet είναι 1518 byte¹, οπότε τα πολύ μεγάλα πακέτα θα πρέπει να τεμαχιστούν πριν τη μετάδοσή τους ως πλαίσια Ethernet. Προσέξτε ότι το προοίμιο δεν συμπεριλαμβάνεται στη μέτρηση όταν αναφερόμαστε σε μήκος πλαισίου.

Το νεότερο πρότυπο 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). Με τον τρόπο αυτό μπορούν να υποστηριχθούν εικονικά τοπικά δίκτυα (Virtual LANs). Με την εισαγωγή του Gigabit Ethernet, οι κατασκευαστές μεταγωγέων (switches) και καρτών Gigabit Ethernet άρχισαν να υποστηρίζουν τεράστια πλαίσια (jumbo frames) μήκους 9018 byte. Τα τεράστια πλαίσια υποτίθεται ότι βελτιώνουν την επίδοση δικτύων Gigabit Ethernet, όμως απαιτείται να τα υποστηρίξει όλος ο εξοπλισμός από άκρη σε άκρη. Τα τεράστια πλαίσια δεν έχουν υιοθετηθεί ως πρότυπο από το IEEE για λόγους συμβατότητας προς τα πίσω, παλαιότερα πρότυπα για τοπικά δίκτυα τύπου Ethernet (802.3), Token ring (802.4) και Token bus (802.5), και εξ ορισμού δεν είναι ενεργοποιημένα στις κάρτες δικτύωσης και τον λοιπό δικτυακό εξοπλισμό.

Όσον αφορά τις διευθύνσεις, κάθε κάρτα δικτύου διαθέτει μία μοναδική φυσική διεύθυνση, αυτήν του υποστρώματος MAC. Έχει μήκος 48 bit ή 6 byte και η δομή της ορίζεται στο πρότυπο IEEE 802. Το πρώτο bit της διεύθυνσης που μεταδίδεται (το LSB του byte 0) ορίζει το κατά πόσο πρόκειται για Ομαδική (τιμή 1) ή Ατομική (τιμή 0) διεύθυνση. Όταν ένα πλαίσιο στέλνεται σε ομαδική διεύθυνση, το λαμβάνουν όλες οι κάρτες δικτύου της ομάδας. Αυτή η αποστολή ονομάζεται πολλαπλή διανομή (multicast). Το πλαίσιο που περιέχει μόνο 1 στο πεδίο προορισμού (δηλαδή "11...1") υποδηλώνει εκπομπή (broadcast) και λαμβάνεται από όλες τις κάρτες του τοπικού δικτύου. Το δεύτερο bit της διεύθυνσης που μεταδίδεται (το αμέσως προηγούμενο του LSB του byte 0) διαχωρίζει τις τοπικές (τιμή 1) από τις παγκόσμιες (τιμή 0) διευθύνσεις.

Περισσότερες πληροφορίες για το Ethernet και την εξέλιξή του μπορείτε να βρείτε στην ιστοθέση <https://ethernethistory.typepad.com/>, ενώ λεπτομέρειες για τη δομή του πλαισίου (Ethernet II ή IEEE 802.3) θα βρείτε στην ιστοσελίδα https://en.wikipedia.org/wiki/Ethernet_frame.

Το πρωτόκολλο ARP

Η επικοινωνία στο διαδίκτυο βασίζεται στις διευθύνσεις IP και τα πακέτα προωθούνται από τους δρομολογητές προς το προορισμό τους. Όμως, σε επίπεδο τοπικού δικτύου (LAN) δεν παρεμβάλλεται κάποιος δρομολογητής και η επικοινωνία πρέπει να γίνει με τις διευθύνσεις MAC (μήκους 6 byte). Χρειάζεται επομένως ένας μηχανισμός ώστε ο κάθε κόμβος του LAN να μπορεί να μάθει τη διεύθυνση MAC του κόμβου με τον οποίο θέλει να επικοινωνήσει. Στην περίπτωση διευθύνσεων IPv4 η λύση που χρησιμοποιείται είναι να σταλθεί ένα πακέτο εκπομπής (broadcast)

¹ Το CRC περιλαμβάνεται στη μέτρηση του μήκους πλαισίου αν και μερικές φορές παραλείπεται, οπότε αντί 1518 θα δείτε να αναφέρεται 1514.

που να ρωτά ποιος κόμβος έχει τη συγκριμένη διεύθυνση. Το πακέτο θα φτάσει με εκπομπή σε όλες τις συνδεδεμένες στο LAN μηχανές και κάθε μία απ' αυτές θα ελέγξει αν απευθύνεται στη δική της διεύθυνση IPv4. Μόνο η μηχανή με τη σωστή διεύθυνση IPv4 θα αποκριθεί με μονο-εκπομπή (unicast) δίνοντας τη διεύθυνση MAC αυτής. Το πρωτόκολλο που διατυπώνει αυτή την ερώτηση, απαντάει και λαμβάνει την απάντηση, για διευθύνσεις IPv4 είναι το ARP (Address Resolution Protocol) και ορίζεται στο [RFC 826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48 bit Ethernet Address for Transmission on Ethernet Hardware](#). Σε συντομία η λειτουργία του ARP έχει ως εξής:

- ο Οι κόμβοι διατηρούν ένα πίνακα αντιστοιχίσεων φυσικών διευθύνσεων (MAC) με διευθύνσεις IPv4, τον **πίνακα ARP**, που αρχικά είναι άδειος
- ο Ο Α γνωρίζει τη διεύθυνση IPv4_B του Β και θέλει να μάθει τη φυσική του διεύθυνση MAC_B
- ο Ο Α εκπέμπει μια αίτηση ARP (ARP request) που περιέχει τη διεύθυνση IPv4_B του Β, μηδενικά για την MAC_B και το ζεύγος IPv4_A – MAC_A των δικών του διευθύνσεων
- ο Ο Β που βλέπει τη δική του διεύθυνση IPv4_B σε ARP request απαντά με μήνυμα ARP reply συμπληρώνοντας την ελλείπουσα MAC_B και αντιστρέφοντας τα ζεύγη πηγής – προορισμού
 - ο ταυτόχρονα ενημερώνει τον δικό του πίνακα ARP με το ζεύγος IPv4_A – MAC_A ώστε να μη χρειασθεί να προσφύγει σε διαδικασία επίλυσης της διεύθυνσης του Α όταν φτάσει η ώρα να του αποστείλει κάποιο πακέτο IPv4
- ο Ο Α καταχωρεί το ζεύγος IPv4_B – MAC_B στον πίνακα ARP
- ο Οι καταχωρήσεις εκπνέουν χρονικά μετά από μερικά λεπτά και η πληροφορία διαγράφεται
 - ο Όλοι οι κόμβοι του τοπικού δικτύου είναι υποχρεωμένοι να ακούν τα μηνύματα ARP (είτε request ή reply) και να ενημερώνουν τον πίνακα ARP με το ζεύγος IPv4_A – MAC_A, εάν ήδη υπάρχει εγγραφή για την IPv4_A, ανανεώνοντας έτσι τη χρονική διάρκεια της ή τη διεύθυνση MAC_A εάν αυτή έχει αλλάξει

Επισημαίνεται ότι η προαναφερθείσα διαδικασία ισχύει για την επίλυση διευθύνσεων **αποκλειστικά** μέσα στην τοπική περιοχή εκπομπής (broadcast domain), η οποία εν γένει ταυτίζεται με ένα IP υποδίκτυο. **Μεταξύ διαφορετικών υποδικτύων η επικοινωνία γίνεται στο στρώμα δικτύου μέσω δρομολογητών.** Τα πακέτα IP προωθούνται προς τον δρομολογητή που υποδεικνύουν οι πίνακες δρομολόγησης, αυτός με τη σειρά του τα προωθεί στον επόμενο, κοκ μέχρις ότου φτάσουν στο υποδίκτυο προορισμού. Έτσι η ανάγκη επίλυσης διευθύνσεων MAC αφορά τον τοπικό δρομολογητή και όχι τον προορισμό που βρίσκεται έξω από την περιοχή εκπομπής (υποδίκτυο). Για μια πιο λεπτομερή περιγραφή της ανταλλαγής πακέτων ARP και για τις δύο προαναφερθείσες περιπτώσεις (επικοινωνία εντός και εκτός του υποδικτύου) δείτε το διάγραμμα ροής στην ιστοσελίδα <https://eventhelix.com/networking/Arp.pdf>.

Όσον αφορά στις διαδρομές στο διαδίκτυο, δεν υπάρχει μηχανισμός ανάλογος αυτού που περιγράφηκε προηγουμένως. Ο προσδιορισμός των διαδρομών γίνεται καταναμημένα βάσει αλγορίθμων δρομολόγησης. Για κάθε πακέτο το επόμενο βήμα της διαδρομής προκύπτει από τον πίνακα δρομολόγησης του κόμβου στον οποίο βρίσκεται κάθε φορά το πακέτο. 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).**

Συνοπτικά, η διαδικασία επικοινωνίας στο διαδίκτυο έχει ως εξής:

- ο Ο Α γνωρίζει τη διεύθυνση IP του Β ή την μαθαίνει μέσω του DNS.
- ο Μέσω του πίνακα δρομολόγησης του βρίσκει σε ποια από τις διεπαφές του θα πρέπει να προωθήσει το εν λόγω πακέτο.
 - ο Εάν η διεύθυνση IP του Β ανήκει σε υποδίκτυο με το οποίο ο Α είναι άμεσα συνδεδεμένος, τότε ο Α μαθαίνει τη διεύθυνση MAC του Β μέσω του ARP για IPv4 διευθύνσεις. (Σημ. Στην περίπτωση του IPv6 χρησιμοποιείται το πρωτόκολλο Neighbor Discovery Protocol (NDP) που βασίζεται σε ανταλλαγή μηνυμάτων ICMPv6.)

- ο Εάν η διεύθυνση IP του B δεν ανήκει σε υποδίκτυο με το οποίο ο A είναι άμεσα συνδεδεμένος, τότε ο A μαθαίνει μέσω του ARP (ή NDP) τη διεύθυνση MAC του δρομολογητή, που θα προωθήσει το πακέτο στον B.
- ο Ο A στέλνει το πακέτο IP με προορισμό τον B στη διεύθυνση MAC που βρήκε στο προηγούμενο βήμα.

Έτσι, για πακέτα IP που προορίζονται για μηχανές εκτός του τοπικού σας δικτύου, η ως άνω διαδικασία επίλυσης διευθύνσεων MAC γίνεται για να προσδιορισθεί το ζεύγος IP – “φυσική διεύθυνση” της προκαθορισμένης πύλης.

Στην άσκηση αυτή θα μελετήσετε τις λεπτομέρειες της επικοινωνίας σε τοπικό επίπεδο (LAN). Για τη διερεύνηση των παραπάνω, στα Windows και Unix θα χρησιμοποιήσετε την εντολή arp, που έχει διαγνωστικές λειτουργίες σχετικά με την εφαρμογή του πρωτοκόλλου ARP σε έναν υπολογιστή. Σε νεώτερες εκδόσεις του Linux η λειτουργικότητα της arp έχει ενσωματωθεί στην εντολή ip neigh.

Για τις παρακάτω ασκήσεις απαντήστε στο συνοδευτικό φυλλάδιο, το οποίο θα υποβάλλετε ως αρχείο pdf.

Άσκηση 1: Ο Πίνακας ARP

Χρησιμοποιώντας εντολές φλοιού σε παράθυρο γραμμής εντολών του λειτουργικού σας συστήματος βρείτε τις πληροφορίες που ζητούνται παρακάτω.

- 1.1 Με ποια εντολή μπορείτε να δείτε τα περιεχόμενα του πίνακα ARP; **arp**
- 1.2 Με ποια εντολή μπορείτε να διαγράψετε τα περιεχόμενα του πίνακα ARP; **arp -d**
- 1.3 Σημειώστε τις διευθύνσεις IPv4 της προκαθορισμένης πύλης και των εξυπηρετητών DNS του υπολογιστή σας καθώς και την εντολή ή εντολές φλοιού με τις οποίες τις βρήκατε.
- 1.4 Καταγράψτε το περιεχόμενο του πίνακα ARP του υπολογιστή σας.
- 1.5 Ο πίνακας περιέχει τις διευθύνσεις MAC και IPv4 των υπολογιστών με τους οποίους έχει επικοινωνήσει πρόσφατα ο δικός σας. Υπάρχουν οι διευθύνσεις της προκαθορισμένης πύλης και/ή των εξυπηρετητών DNS σε αυτόν; **Υπάρχει η διεύθυνση**
- 1.6 Αδειάστε τον πίνακα ARP και εκτελέστε την εντολή ping <A.B.C.D>, όπου <A.B.C.D> κάποια διεύθυνση IPv4 της ερώτησης 1.4, πλην της προκαθορισμένης πύλης ή εξυπηρετητή DNS. Εάν δεν λάβετε απάντηση, επαναλάβετε με κάποια άλλη διεύθυνση μέχρι να λάβετε απάντηση. Καταγράψτε τη διεύθυνση που χρησιμοποιήσατε.
- 1.7 Δείτε πάλι και καταγράψτε τον πίνακα ARP του υπολογιστή σας. Τι παρατηρείτε;

Για τη συνέχεια, εάν χρησιμοποιείτε Windows, σε ένα παράθυρο εντολών εκτελέστε την εντολή ipconfig /flushdns για να διαγραφούν οι αντιστοιχίσεις ονομάτων DNS σε διευθύνσεις IP. Σε Ubuntu εκτελέστε την εντολή sudo systemd-resolve --flush-caches. Σε συστήματα Unix/Linux, εάν έχετε ενεργοποιήσει την προσωρινή αποθήκευση για την επίλυση ονομάτων, διαγράψτε τα περιεχόμενά της επανεκκινώντας την αντίστοιχη υπηρεσία. Κατόπιν αδειάστε τον πίνακα ARP του υπολογιστή σας και αμέσως μετά επισκεφτείτε την ιστοσελίδα <http://edu-dy.cn.ntua.gr/lab3> χρησιμοποιώντας κάποιον πλοηγό ιστού. Μιας και η διεύθυνση IPv4 του εξυπηρετητή ιστού 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.

- 1.8 Ποιες από τις διευθύνσεις IPv4 που προσδιορίσατε στο ερώτημα 1.3 έχουν τώρα καταχωρηθεί στον πίνακα ARP και γιατί; [Υπενθύμιση: Εάν πελάτης και εξυπηρετητής βρίσκονται σε διαφορετικά υποδίκτυα, η επικοινωνία στο στρώμα IP γίνεται μέσω της πύλης που υποδεικνύει ο πίνακας δρομολόγησης.] **μόνο του gateway**
- 1.9 Έχει καταχωρηθεί η διεύθυνση IPv4 του edu-dy.cn.ntua.gr στον πίνακα ARP και γιατί;

όχι, μέσω του

Άσκηση 2: Το πλαίσιο Ethernet

Σε αυτή την άσκηση θα επαναλάβετε την επίσκεψη την ιστοσελίδα <http://edu-dy.cn.ntua.gr/lab3> καταγράφοντας παράλληλα την κίνηση που παράγεται. Επειδή έχετε προηγουμένως επισκεφτεί την ιστοσελίδα αυτή, φροντίστε να αδειάσετε την προσωρινή μνήμη (cache) του πλοηγού. Στον Mozilla Firefox από τη διαδρομή *History* → *Clear Recent History* επιλέξτε το cache στον πίνακα που θα εμφανισθεί, επιβεβαιώστε με OK την πρόθεσή σας, περιμένετε να ολοκληρωθεί η διαγραφή και κλείστε το παράθυρο διαλόγου. Αντίστοιχα, σε Google Chrome στο *History* επιλέξτε *Clear browsing data*, κλπ. Για την καταγραφή από το μενού *Capture* → *Options...* επιλέξτε την κάρτα δικτύου του υπολογιστή σας μέσω της οποίας συνδέεστε στο τοπικό δίκτυο και πατήστε το κουμπί *Start*. Κατόπιν αδειάστε τον πίνακα ARP του υπολογιστή σας και αμέσως μετά επισκεφτείτε την ιστοσελίδα <http://edu-dy.cn.ntua.gr/lab3> που φιλοξενείται στον υπολογιστή με IPv4 διεύθυνση 147.102.40.15. Μόλις φορτωθεί η σελίδα, πατήστε το *Stop* για να σταματήσει η καταγραφή. Από το μενού *View* → *Name Resolution* απενεργοποιήστε την επιλογή *Resolve Physical Addresses*. Τέλος, εφαρμόστε φίλτρο απεικόνισης *ip or ipn6 or arp*.

Θα βασίσετε τις απαντήσεις σας για τις επόμενες ερωτήσεις στα στοιχεία της καταγραφής και ειδικότερα στις πληροφορίες που αποτυπώνονται στα παράθυρα με τις λεπτομέρειες και το περιεχόμενο των πλαισίων Ethernet.

Destination, Source.

2.1 Ποια από τα πεδία του πλαισίου Ethernet καταγράφει το Wireshark; [Υπόδειξη: συμβουλευθείτε την ιστοσελίδα https://en.wikipedia.org/wiki/Ethernet_frame για να δείτε τα πεδία του πλαισίου Ethernet και τα ονόματά τους.]

2.2 Έχει καταγραφεί το προοίμιο; Γιατί; **Όχι δεν έχει καταγραφεί διότι το**

2.3 Τι συμβαίνει με το CRC; [Υπόδειξη: Αναζητήστε *FCS – Frame Check Sequence* στην ιστοσελίδα <https://www.wireshark.org/faq.html>.] **δεν καταγράφεται**

2.4 Ποια είναι η τιμή του πεδίου Type της επικεφαλίδας Ethernet για πακέτα IPv4; **0x0800**

2.5 Ποια είναι η τιμή του πεδίου Type για πακέτα ARP; **0x0806**

2.6 Εάν καταγράφηκαν, ποια είναι η τιμή του πεδίου Type για πακέτα IPv6; **δεν καταγράφηκαν αλλά σύμφωνα με το διαδίκτυο 0x86DD**

Βρείτε και επιλέξτε το πλαίσιο Ethernet που περιέχει το πρώτο μήνυμα HTTP GET προς το edu-dy.cn.ntua.gr. [Υπόδειξη: Ακολουθήστε τη διαδρομή *Edit* → *Find Packet...* και στη γραμμή που θα εμφανιστεί επιλέξτε **String** (ώστε να αναζητήσετε συρμό χαρακτήρων), **Packet bytes** (ώστε η αναζήτηση να γίνει εντός των δεδομένων των πακέτων), στο ροζ πλαίσιο πληκτρολογήστε “GET”, χωρίς τα εισαγωγικά, και πατήστε το κουμπί *Find*. Ξεκινήστε την αναζήτηση από την **αρχή** της καταγραφής!].

2.7 Ποια είναι η διεύθυνση MAC πηγής του πλαισίου; **90:78:41:15:16:66**

2.8 Ποια είναι η διεύθυνση MAC προορισμού του πλαισίου; **08:ec:f5:d0:d9:1d**

2.9 Είναι η παραπάνω διεύθυνση MAC αυτή του edu-dy.cn.ntua.gr; **όχι**

2.10 Εάν όχι, σε ποια συσκευή ανήκει και γιατί; [Υπόδειξη: Αναζητήστε μεταξύ των συσκευών που προσδιορίσατε στο ερώτημα 1.3] **ανήκει στον δρομολογητή (default gateway)**

2.11 Ποιο είναι το μήκος του πλαισίου σε byte; **153**

2.12 Πόσα byte του πλαισίου Ethernet προηγούνται του χαρακτήρα ASCII “G” της λέξης GET; [Υπόδειξη: επιλέξτε το πεδίο δεδομένων του προηγούμενου αναπτύγματος ώστε να υπογραμμιστούν στο παράθυρο με τα περιεχόμενα τα αντίστοιχα byte δεδομένων.] **66**

Στη συνέχεια βρείτε και επιλέξτε το πλαίσιο Ethernet που περιέχει την απάντηση στο προηγούμενο μήνυμα HTTP [Υπόδειξη: Αναζητήστε την ακολουθία “200 OK”, χωρίς τα εισαγωγικά, στο περιεχόμενο των αμέσως επόμενων πλαισίων της λίστας πακέτων.]

2.13 Ποια είναι η διεύθυνση MAC του αποστολέα; **ec:be:5f:86:e9:4**

2.14 Είναι η παραπάνω διεύθυνση MAC αυτή του edu-dy.cn.ntua.gr;

2.15 Σε ποια συσκευή ανήκει η διεύθυνση αυτή;

2.16 Ποια είναι η διεύθυνση MAC του παραλήπτη;

2.17 Σε ποιον υπολογιστή ανήκει;

- 2.18 Ποιο είναι το μήκος του πλαισίου σε byte;
2.19 Πόσα byte του πλαισίου Ethernet προηγούνται του χαρακτήρα ASCII “Ο” της λέξης OK;

Άσκηση 3: Περισσότερα για τα πλαίσια Ethernet

Ξεκινήστε μια νέα καταγραφή με το Wireshark και φίλτρο σύλληψης *ether multicast* ώστε να καταγράφονται μόνο πλαίσια που απευθύνονται σε πολλαπλούς προορισμούς. Επισκεφτείτε την ιστοθέση <http://edu-dy.cn.ntua.gr/lab3.pcap> και κατεβάστε στον υπολογιστή σας το αρχείο lab3.pcap που περιέχει μια αντίστοιχη καταγραφή στο περιβάλλον του PC Lab της Σχολής. Περιμένετε λίγα δευτερόλεπτα ακόμη και σταματήστε την καταγραφή. Εάν δεν καταγράψετε κανένα πλαίσιο ή δεν βρίσκετε την πληροφορία που ζητείται παρακάτω χρησιμοποιήστε το αρχείο που μόλις κατεβάσατε.

- 3.1 Τι είδους (ομαδικές ή ατομικές, τοπικές ή μοναδικές) είναι οι διευθύνσεις MAC πηγής των πλαισίων Ethernet που καταγράψατε; [Υπόδειξη: Αναπτύξτε το περιεχόμενο του πεδίου διεύθυνσης πηγής των πλαισίων].
3.2 Τι είδους (ομαδικές ή ατομικές, τοπικές ή μοναδικές) είναι διευθύνσεις MAC προορισμού των πλαισίων Ethernet που παρατηρείτε στην καταγραφή;
3.3 Σε ποια θέση στο πρώτο byte εμφανίζεται το πρώτο bit της διεύθυνσης MAC και σε ποια το επόμενο του;
3.4 Ποια είναι η διεύθυνση MAC για τα πλαίσια εκπομπής (broadcast);
3.5 Εφαρμόστε φίλτρο απεικόνισης *llc*. Τι είδους πλαίσια παραμένουν;
3.6 Τι δηλώνει το πεδίο μετά τις διευθύνσεις MAC στα πλαίσια IEEE 802.3;
3.7 Πώς ξεχωρίζουν τα πλαίσια IEEE 802.3 από τα Ethernet II;
3.8 Τι μέγεθος έχει και ποια πεδία περιλαμβάνει η επικεφαλίδα LLC στα πλαίσια IEEE 802.3;
3.9 Δεδομένα ποιου πρωτοκόλλου μεταφέρουν τα πλαίσια IEEE 802.3 που παρατηρήσατε και τι μέγεθος έχουν αυτά;
3.10 Τι μέγεθος έχει το παραγέμισμα (padding) και γιατί υπάρχει;

Άσκηση 4: Περισσότερα για τα πακέτα ARP

Σε αυτή την άσκηση θα καταγραφούν με τη βοήθεια του Wireshark τα πακέτα ARP που ανταλλάσσονται κατά τη διαδικασία ανεύρεσης μιας διεύθυνσης MAC. Ξεκινήστε μια νέα καταγραφή με το Wireshark χωρίς φίλτρο σύλληψης. Στη συνέχεια σε παράθυρο γραμμής εντολών, ως *διαχειριστής* του υπολογιστή, δώστε την κατάλληλη εντολή² ώστε να αδειάσετε τον πίνακα ARP. Αμέσως, εκτελέστε την εντολή `ping <A.B.C.D>`, όπου `<A.B.C.D>` η διεύθυνση IPv4 της προκαθορισμένης πύλης που προσδιορίσατε στο ερώτημα 1.3 ή του μηχανήματος που απάντησε στο ερώτημα 1.6. Μόλις ολοκληρωθεί η εκτέλεση της εντολής πατήστε το κόκκινο *Stop* για να σταματήσει η καταγραφή. Ελέγξτε τον πίνακα ARP και βεβαιωθείτε ότι η διεύθυνση όπου κάνατε `ping` έχει προστεθεί, αλλιώς επαναλάβετε τη διαδικασία.

Κατόπιν εφαρμόστε φίλτρο απεικόνισης κάνοντας κλικ στο γαλάζιο σύμβολο (bookmark) πλάι από το πεδίο ορισμού φίλτρων απεικόνισης. Θα εμφανισθεί μια λίστα χρήσιμων προτύπων για φίλτρα απεικόνισης. Διαλέξτε τη γραμμή Ethernet address `00:00:5e:00:53:00` και αυτόματα θα συμπληρωθεί ένα συντακτικά σωστό φίλτρο απεικόνισης για τη MAC διεύθυνση `00:00:5e:00:53:00`. Μετά διορθώστε τη διεύθυνση MAC ώστε να είναι ίση με τη διεύθυνση MAC της κάρτας δικτύου του υπολογιστή σας. Η σύνταξη του φίλτρου είναι σωστή όταν το πεδίο έχει πράσινο χρώμα και ενεργοποιείται πατώντας το `<Enter>`.

- 4.1 Τι αποτέλεσμα έχει η εφαρμογή αυτού του φίλτρου;
4.2 Κάντε κλικ στο τέλος του προηγούμενου φίλτρου, προσθέστε την έκφραση `and arp` και πατήστε το `<Enter>`. Τι αποτέλεσμα έχει η εφαρμογή του δεύτερου φίλτρου;
4.3 Πόσα πακέτα ARP ανταλλάχθηκαν κατά την εκτέλεση της εντολής `ping`;

² Προς τούτο σε μηχανήματα Windows XP του PC Lab εκτελέστε την εντολή `arpclear`.

4.4 Τα πακέτα ARP δεν είναι πακέτα IPv4. Ποιο πεδίο του πλαισίου Ethernet τα διαφοροποιεί;

Επιλέξτε ένα πακέτο ARP και, για να δείτε την πληροφορία που μεταφέρει, στο παράθυρο με τις λεπτομέρειες πιάστε το σύμβολο '>' στη γραμμή Address Resolution Protocol. Αφού μελετήσετε με προσοχή τα πεδία που αποτελούν το πακέτο ARP απαντήστε τις επόμενες ερωτήσεις:

4.5 Καταγράψτε τα ονόματα και το μήκος σε byte των πεδίων του πακέτου ARP χρησιμοποιώντας ως υπόδειγμα το σχήμα στο τέλος του φυλλαδίου των απαντήσεων.

4.6 Ποια είναι η τιμή του πεδίου Hardware type και τι είδος υλικού κάρτας δικτύου υποδεικνύει;

4.7 Ποια είναι η τιμή του πεδίου Protocol type και ποιο πρωτόκολλο υποδεικνύει;

4.8 Πώς σχετίζεται η τιμή του πεδίου Protocol type με τα Ethertypes του Ethernet II;

4.9 Εξηγήστε γιατί η τιμή του πεδίου Protocol size έχει την τιμή 4. [Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα <http://www.networksorcery.com/enp/default.htm> επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο ARP στο δεξιό της μέρος. **Εάν η ιστοσελίδα δεν ανταποκρίνεται αναζητήστε την στο [Internet Archive](#).**]

4.10 Εξηγήστε γιατί η τιμή του πεδίου Hardware size έχει την τιμή 6.

Με βάση την πληροφορία στη στήλη Info του παραθύρου με τη λίστα πακέτων επιλέξτε το πακέτο ARP request που περιέχει την ερώτηση για το ποιος έχει τη διεύθυνση IPv4 όπου κάνατε ping.

4.11 Σε ποιον υπολογιστή ανήκει η διεύθυνση MAC αποστολέα του πλαισίου Ethernet που μεταφέρει το ARP request;

4.12 Ποια είναι η διεύθυνση MAC παραλήπτη του πλαισίου αυτού;

4.13 Ποιο είναι το συνολικό μέγεθος σε byte του πακέτου ARP request και ποιο του πλαισίου Ethernet που το μεταφέρει;

4.14 Πόσα byte του πλαισίου Ethernet προηγούνται του πεδίου opcode στο ARP request;

4.15 Ποια η τιμή του πεδίου opcode στο ARP request;

4.16 Σε ποιο πεδίο του πακέτου ARP request περιέχεται η διεύθυνση MAC του αποστολέα;

4.17 Σε ποιο πεδίο του πακέτου ARP request περιέχεται η διεύθυνση IPv4 του αποστολέα;

4.18 Σε ποιο πεδίο του πακέτου ARP request περιέχεται η ερώτηση, δηλαδή, η διεύθυνση IPv4 του υπολογιστή του οποίου αναζητείται η διεύθυνση MAC;

4.19 Υπάρχει στο πακέτο ARP request πεδίο για τη ζητούμενη διεύθυνση MAC και ποια τιμή περιέχει;

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

4.20 Σε ποιον υπολογιστή ανήκει η διεύθυνση MAC του αποστολέα και σε ποιον του παραλήπτη του πλαισίου Ethernet που μεταφέρει το ARP reply;

4.21 Ποια η τιμή του πεδίου opcode στο ARP reply;

4.22 Σε ποιο πεδίο του πακέτου ARP reply περιέχεται η διεύθυνση IPv4 του αποστολέα;

4.23 Σε ποιο πεδίο του πακέτου ARP reply περιέχεται η διεύθυνση MAC του αποστολέα;

4.24 Σε ποιο πεδίο του πακέτου ARP reply περιέχεται η διεύθυνση IPv4 του παραλήπτη;

4.25 Σε ποιο πεδίο του πακέτου ARP reply περιέχεται η απάντηση, δηλαδή, η διεύθυνση MAC του υπολογιστή που έχει τη διεύθυνση IPv4 για την οποία έγινε η ερώτηση;

4.26 Ποιο είναι το συνολικό μέγεθος σε byte του πακέτου ARP reply και ποιο του πλαισίου Ethernet που το μεταφέρει;

4.27 Είναι ίδια με αυτά που προσδιορίσατε στην ερώτηση 4.13;

4.28 Όπως θα έχετε ήδη παρατηρήσει ότι η δομή των πακέτων ARP request/reply είναι η ίδια. Ποιο πεδίο υποδεικνύει το κατά πόσον πρόκειται για πακέτο ARP request ή ARP reply;

4.29 Πώς εξηγείτε το διαφορετικό μήκος πλαισίων Ethernet για πακέτα ARP reply και ARP request; [Υπόδειξη: Η βιβλιοθήκη nrcap που χρησιμοποιεί το Wireshark, όπως φαίνεται και στο σχετικό σχήμα της Εργαστηριακής Άσκησης 1, συλλαμβάνει τα απερχόμενα πλαίσια προτού μεταδοθούν.]

Απερχόμενος == που φεύγει

4.30 Που αλλού διαφέρουν τα πλαίσια για πακέτα ARP request και ARP reply;

4.31 Τι θα συνέβαινε εάν ένας κακόβουλος υπολογιστής στο τοπικό δίκτυο απαντούσε σε όλα τα ARP request δίνοντας τη δική του διεύθυνση MAC;

Όνοματεπώνυμο:			Ομάδα:		
Όνομα PC/ΛΣ:			Ημερομηνία: / /		
Διεύθυνση IP: . . .		Διεύθυνση MAC: - - - - -			

Εργαστηριακή Άσκηση 3 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
1.7
.....
.....
1.8
.....
.....
1.9
.....

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.....
2.13.....
2.14.....
2.15.....
2.16.....
2.17.....
2.18.....
2.19.....

Άσκηση 3

- 3.1
.....
3.2
.....
3.3
.....
3.4
3.5
3.6
3.7
.....
3.8
.....
.....
3.9
.....
3.10.....
.....

Άσκηση 4

- 4.1
4.2
.....

- 4.3
4.4
4.5 (χρησιμοποιήσετε το σχήμα στο τέλος)
4.6
4.7
4.8
4.9
.....
4.10
.....
4.11
4.12
4.13
.....
4.14
4.15
4.16
4.17
4.18
4.19
4.20
.....
4.21
4.22
4.23
4.24
4.25
4.26
.....
4.27
4.28
.....
.....
4.29
4.30
4.31
.....
.....
.....

