Προηγμένα Δίκτυα Η/Υ - Ανάλυση Πακέτων Ethernet, IP, ARP

1. Στόχος

Η ανάλυση των IP πακέτων που μεταφέρουν τα μηνύματα που ανταλλάσσονται μεταξύ δύο οντοτήτων που επικοινωνούν όταν χρησιμοποιείται ένα TCP/IP διαδίκτυο. Το πρωτόκολλο IP χρησιμοποιείται στο Network Layer και οι μονάδες δεδομένων (του IP) ονομάζονται datagrams.Στα datagrams ενθυλακώνονται μονάδες δεδομένων των ανωτέρων στρωμάτων του μοντέλου αναφοράς TCP/IP (TCP & Εφαρμογής) τα οποία με τη σειρά τους ενθυλακώνονται σε πλαίσια του Data Link Layer (Ethernet,FDDI,PPP,HDLC κ.λ.π).

Το λογισμικό που θα χρησιμοποιηθεί θα είναι το Wireshark. Βασικά χαρακτηριστικά του IP είναι: (α) αναξιόπιστο επειδή η παράδοση των datagrams στον προορισμό δεν είναι εγγυημένη.Το IP πακέτο μπορεί να χαθεί, να καθυστερήσει, να φθάσει εκτός σειράς, να παραδοθεί δύο φορές (β) παρέχει υπηρεσία χωρίς σύνδεση. Κάθε πακέτο αντιμετωπίζεται ξεχωριστά από τα υπόλοιπα (αυτοδύναμα πακέτα), δεν ακολουθούν όλα κατ' ανάγκη την ίδια διαδρομή για να φθάσουν στον προορισμό τους και πριν την μετάδοση δεν προηγείται μεταξύ πομπού και δέκτη ,κάποια συνεννόηση που θα καθορίζει τις παραμέτρους της επικοινωνίας (γ) best-effort επειδή το IP software καταβάλλει προσπάθεια να παραδώσει τα πακέτα στον προορισμό αλλά αυτό δεν είναι βέβαιο .Δεν περιλαμβάνει μηχανισμούς ανίχνευσης και αντιμετώπισης λαθών ούτε και ενημέρωσης της πηγής και του προορισμού. Το IP ορίζει την μορφή των πακέτων(ποια πεδία περιλαμβάνει η επικεφαλίδα και τη σημασία του καθενός) καθώς επίσης και τον τρόπο με τον οποίο γίνεται η δρομολόγηση των πακέτων από τους routers και τους hosts,πότε τα πακέτα απορρίπτονται, αλλά δημιουργεί και μηνύματα λαθών ανάλογα με το είδος του προβλήματος.

- Πως εκχωρούνται IP διευθύνσεις σε hosts και δρομολογητές
- Η έννοια του Interface σε IP συσκευές

- Κλάσεις IP διευθύνσεων Network & Host IDs. Private και Public IP διευθύνσεις.
- Ειδικές IP διευθύνσεις.

2. Ethernet

Το Ethernet είναι μια τεχνολογία δικτύων τοπικής περιοχής (LAN) που μεταδίδει πληροφορία μεταξύ υπολογιστών με ταχύτητες 10 και 100 εκατομμύρια bit ανά δευτερόλεπτο (Mbps). Αυτήν την περίοδο η ευρύτατα χρησιμοποιημένη έκδοση της τεχνολογίας Ethernet είναι η κατηγορία των 10-Mbps με χρήση καλωδίων ανεστραμμένου ζεύγους (twisted pair).

Οι κατηγορίες μέσου για το 10-Mbps Ethernet περιλαμβάνουν το αρχικό παχύ ομοαξονικό σύστημα, καθώς επίσης και το λεπτό ομοαξονικό, το twisted-pair, και τα συστήματα οπτικών ινών. Τα πιό πρόσφατα Ethernet πρότυπα καθορίζουν το νέο Fast Ethernet 100-Mbps σύστημα το οποίο λειτουργεί πάνω σε twisted-pair μέσα και σε μέσα οπτικών ινών.

Το Ethernet αποτελείται από τρία βασικά στοιχεία: 1. το φυσικό μέσο που χρησιμοποιείται για να μεταφέρει τα σήματα Ethernet μεταξύ των υπολογιστών, 2. ένα σύνολο medium access control κανόνων που ενσωματώνονται σε κάθε διεπαφή Ethernet και επιτρέπουν σε πολλαπλούς υπολογιστές να μοιραστούν δίκαια την πρόσβαση στο κοινό κανάλι Ethernet, και 3. ένα πλαίσιο Ethernet που αποτελείται από ένα τυποποιημένο σύνολο bits τα οποία χρησιμοποιούνται για να μεταφέρουν δεδομένα στο σύστημα.

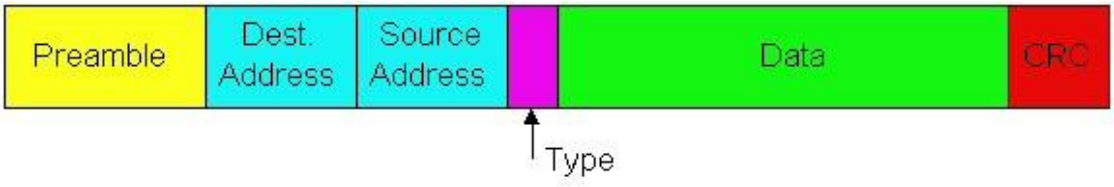
2.1 Λειτουργία Ethernet

Κάθε υπολογιστής εξοπλισμένος με Ethernet, αποκαλούμενος και σταθμός, λειτουργεί ανεξάρτητα από όλους τους άλλους σταθμούς στο δίκτυο: δεν υπάρχει κανένας κεντρικός ελεγκτής. Όλοι οι σταθμοί που προσαρτημένοι σε ένα σύστημα Ethernet, συνδέονται με ένα διαμοιραζόμενο σύστημα σηματοδότησης, γνωστό και ως μέσο. Τα σήματα Ethernet διαβιβάζονται σειριακά, ένα bit κάθε φορά, πάνω στο διαμοιραζόμενο κανάλι σημάτων και προς κάθε συνδεδεμένο σταθμό. Για να στείλει δεδομένα ένας σταθμός "ακούει" αρχικά το κανάλι, και όταν αυτό δεν είναι απασχολημένο, ο σταθμός διαβιβάζει τα δεδομένα του υπό μορφή πλαισίου Ethernet, ή πακέτου.

2.2 Πλαίσιο Ethernet

Η καρδιά του συστήματος Ethernet είναι το πλαίσιο Ethernet, το οποίο χρησιμοποιείται για να αποστείλει δεδομένα μεταξύ των υπολογιστών. Το πλαίσιο αποτελείται από ένα σύνολο bits που οργανώνονται σε διάφορα πεδία.

Αυτά τα πεδία περιλαμβάνουν: πεδία διευθύνσεων, ένα μεταβλητού μεγέθους πεδίο δεδομένων, που συγκρατεί από 46 έως 1.500 bytes δεδομένων, και ένα πεδίο ελέγχου λαθών το οποίο ελέγχει την ακεραιότητα των bits στο πλαίσιο για να εξασφαλίσει ότι το πλαίσιο έχει φθάσει άθικτο.
Η μορφή του Ethernet πλαισίου έχει ως εξής:



Εικόνα 1: Δομή Πλαισίου Ethernet

Preamble:**8** Bytes.Χρησιμοποιείται για το συγχρονισμό του δέκτη
Destination & Source Address: **6** Bytes η κάθε μία. Οι MAC διευθύνσεις παραλήπτη και αποστολέα
Type:**2** Bytes. Δείχνει σε ποιο πρωτόκολλο θα παραδοθούν τα Data του πλαισίου.(IP=0X800,X25=0X805,ARP=0X806)
Data: Μέχρι **1500** Bytes. Τα δεδομένα που παρελήφθησαν από τα ανώτερα στρώματα.(Πχ IP datagram)
CRC: **4** Bytes. Χρησιμοποιείται για τον έλεγχο της ορθότητας του πλαισίου. Αν το πλαίσιο είναι λανθασμένο απλώς απορρίπτεται. Ο αποστολέας δεν ενημερώνεται. Για το λόγο αυτό λέμε ότι το Ethernet παρέχει connectionless υπηρεσίες.

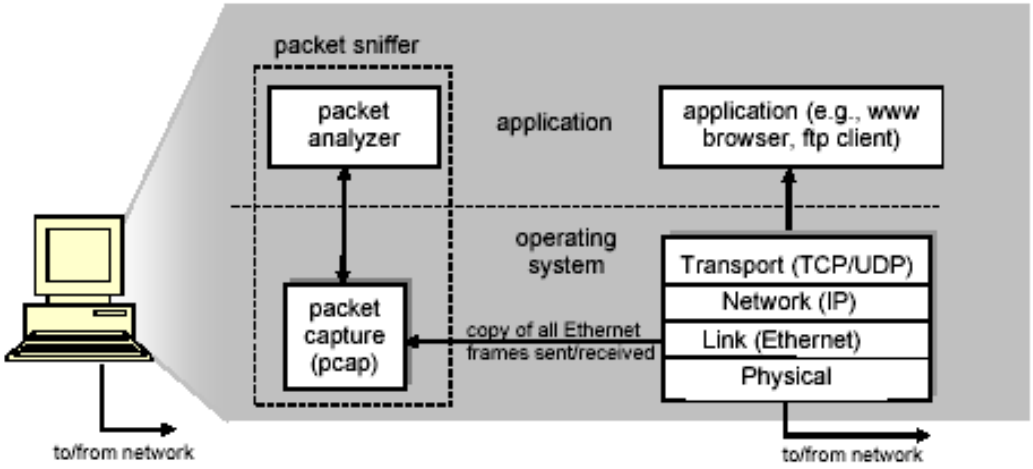
2.3 Η διεύθυνση MAC (Media Access Control)

Η MAC address ή Ethernet address ή Φυσική διεύθυνση είναι μία 48μπιτη διεύθυνση που αναπαρίσταται με 12 δεκαεξαδικά ψηφία (π.χ.
00:A0:CC:DF:48:9C). Τα πρώτα 6 δεκαεξαδικά ψηφία της διεύθυνσης MAC
περιέχουν έναν κωδικό αναγνώρισης του κατασκευαστή ή του προμηθευτή. Τα τελευταία 6 δεκαδικά ψηφία χορηγούνται από τον εκάστοτε προμηθευτή και συχνά αντιπροσωπεύουν τον αύξοντα αριθμό της σύνδεσης.

3. Wireshark – Packet Sniffer

Το βασικό λογισμικό που θα χρησιμοποιηθεί για τις παρατηρήσεις είναι ένας packet sniffer. Όπως προκύπτει και από το όνομα, το λογισμικό αυτό συλλαμβάνει κάθε πακέτο που μεταδίδεται στο δίκτυο. Ένας packet sniffer δεν στέλνει ο ίδιος πακέτα στο δίκτυο αλλά αντιγράφει κάθε πακέτο που στέλνει ο Η/Υ στο δίκτυο. Ομοίως κανένα πακέτο δεν στέλνεται στον sniffer αλλά αντιγράφεται καθώς εισέρχεται στην NIC του Η/Υ (στον οποίο τρέχει ο sniffer).

Παρακάτω φαίνεται η δομή ενός sniffer:



Εικόνα 2: Δομή Packet sniffer

Στη δεξιά πλευρά της εικόνας φαίνονται οι εφαρμογές που τρέχουν στον Η/Υ (διάφοροι Internet clients) και αριστερά τα τμήματα του sniffer. Το ένα τμήμα αντιγράφει κάθε πλαίσιο του data link layer που στέλνεται ή λαμβάνεται από τον Η/Υ καθώς μηνύματα ανταλλάσσονται μεταξύ πρωτοκόλλων υψηλότερων επιπέδων (HTTP,FTP,DNS,TCP,UDP,IP).

Το άλλο τμήμα είναι ο packet analyzer που αναλύει τα πεδία των πλαισίων σε επίπεδο bit εμφανίζοντας τα περιεχόμενα τους και μια σύντομη περιγραφή της σημασίας των. Αντιλαμβάνεται τη μορφή του Ethernet πλαισίου, τη δομή του IP datagram στο payload του πλαισίου, τη δομή του TCP segment στο payload του datagram και τελικά το μήνυμα της εφαρμογής(π.χ Telnet) που μεταφέρει το datagram.

Το λογισμικό που θα χρησιμοποιήσουμε είναι το Wireshark (www.wireshark.org) το οποίο είναι ελεύθερης τρέχει σε συστήματα Windows,Mac,Unix,Linux, βρίσκεται σε ευρεία χρήση και είναι αρκετά σταθερό. Το Wireshark αναγνωρίζει πολλά πρωτόκολλα (περίπου 500) και παρέχει γραφικό περιβάλλον διασύνδεσης με το χρήστη. Παρακάτω

εμφανίζεται το βασικό περιβάλλον στο οποίο εκτός από το menu διακρίνουμε τα εξής συστατικά:

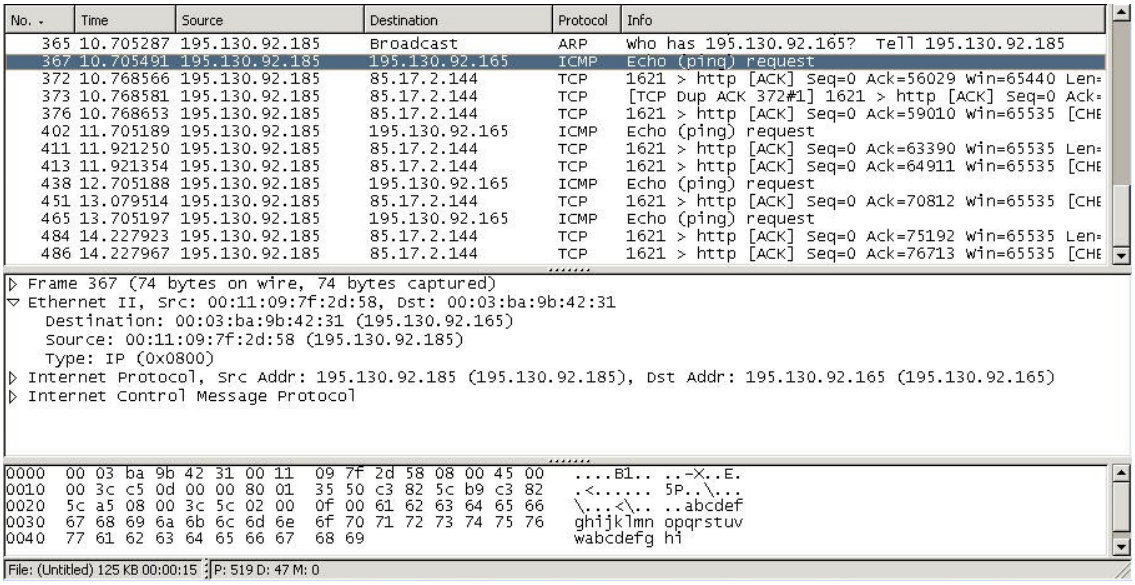
- **Λίστα πακέτων που καταγράφηκαν:**

Όπου φαίνονται οι χρόνοι καταγραφής κάθε πακέτου, οι διευθύνσεις αποστολής και προορισμού, το πρωτόκολλο πληροφορίες του οποίου μεταφέρει το πακέτο και πληροφορίες ειδικά για κάθε πρωτόκολλο. Το πρωτόκολλο είναι αυτό του υψηλοτέρου επιπέδου.

- **Headers των πακέτων:** Εμφανίζονται τα περιεχόμενα των πεδίων των επικεφαλίδων κάθε πρωτοκόλλου (Ethernet,ip,tcp,udp)

- **Περιεχόμενα του πακέτου:** Εμφανίζονται τα περιεχόμενα του πακέτου σε ASCII και δεκαεξαδική μορφή.

Θα χρησιμοποιήσουμε την εντολή ping (λειτουργεί και σε UNIX) για να παρατηρήσουμε την επικοινωνία μεταξύ δύο Η/Υ στο ίδιο φυσικό δίκτυο. Η εντολή ping επιτρέπει τον έλεγχο της επικοινωνίας μεταξύ δύο hosts. Η εντολή , στον αποστολέα, δημιουργεί πακέτα τα στέλνει στον παραλήπτη, ο οποίος αν είναι σε λειτουργία, το αντίστοιχο πρόγραμμα σε αυτόν απαντάει στέλνοντας πίσω αντίστοιχα πακέτα. Και στις δύο κατευθύνσεις τα μηνύματα που ανταλλάσσονται ορίζονται από το πρωτόκολλο ICMP (Internet Control Message Protocol).



Εικόνα 3: Wireshark Διεπαφή Χρήστη

4. Διευθύνσεις IP

Κάθε interface ενός TCP/IP host προσδιορίζεται από μια (λογική) IP διεύθυνση. Η διεύθυνση αυτή είναι μοναδική σε ολόκληρο το IP δίκτυο. Οι IP διευθύνσεις αποτελούνται από 32 bits και προσδιορίζουν τη θέση ενός host σε ένα δίκτυο.(Με τον ίδιο τρόπο που η διεύθυνση ενός κτιρίου προσδιορίζει τη θέση του στο δρόμο)

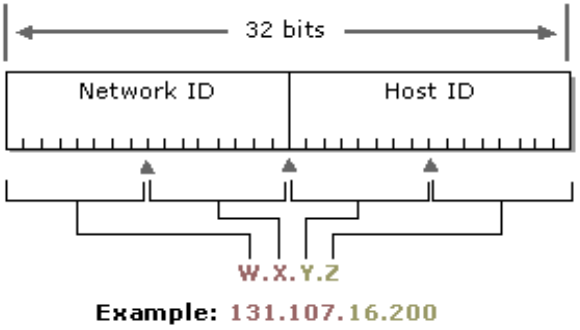
Όπως η διεύθυνση του κτιρίου αποτελείται από δύο τμήματα(δρόμος ,αριθμός σπιτιού) κάθε IP διεύθυνση αποτελείται (και ερμηνεύεται εσωτερικά από τα συστήματα) από δύο τμήματα:

- το τμήμα που προσδιορίζει το δίκτυο (Network ID) και το τμήμα που προσδιορίζει τον host(Host ID).Η διεύθυνση δικτύου προσδιορίζει το υποδίκτυο ,σε ένα ευρύτερο IP διαδίκτυο(δίκτυο αποτελούμενο από δίκτυα).Όλα τα συστήματα τα οποία είναι συνδεδεμένα στο ίδιο υποδίκτυο έχουν το ίδιο Network ID στις IP διευθύνσεις τους. Το Network ID πρέπει επίσης να είναι μοναδικό στο IP διαδίκτυο.
- Το host ID είναι το τμήμα της IP διεύθυνσης που προσδιορίζει τον host ή οποιονδήποτε TCP/IP κόμβο(σταθμός εργασίας, δρομολογητής,server) και είναι μοναδικό μέσα στο υποδίκτυο.

Μια IP διεύθυνση είναι η 10000011 01101011 00010000 11001000 .Αποτελείται από 4 τμήματα των 8 bits τα οποία για λόγους ευκολίας τα μετατρέπουμε σε 4 αριθμούς γραμμένους στο δεκαδικό σύστημα αρίθμησης χωρισμένους μεταξύ τους με μία τελεία. Έτσι η παραπάνω IP διεύθυνση μετατρέπεται στην 131.107.16.200

Χρησιμοποιείστε τον πίνακα παρακάτω για να δοκιμάστε τη μετατροπή

Octet	**1st bit**	**2nd bit**	**3rd bit**	**4th bit**	**5th bit**	**6th bit**	**7th bit**	**8th bit**
Δύναμη 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Δεκαδικός αριθμός	128	64	32	16	8	4	2	1



Στην παραπάνω διεύθυνση η διεύθυνση υποδικτύου είναι 131.107 και η διεύθυνση του Host είναι 16.200

Σημείωση: Αν μία συσκευή έχει περισσότερα από ένα interfaces(ένας server με δύο κάρτες δικτύου ή ένας δρομολογητής συνδεδεμένος σε πολλά δίκτυα) τότε κάθε interface έχει τη δική του IP διεύθυνση.

4.1 Κλάσεις IP διευθύνσεων

Στο Internet ορίζονται 5 κλάσεις, συμβολικά οι A,B,C,D,E εκ των οποίων οι τρεις πρώτες χρησιμοποιούνται για τη διευθυνσιοδότηση των hosts.Οι κλάσεις ορίζουν ποια bits χρησιμοποιούνται για το τμήμα δικτύου και ποια για το τμήμα host.Ορίζουν επίσης πόσα υποδίκτυα και hosts υπάρχουν σε κάθε δίκτυο. Ο παρακάτω πίνακας χρησιμοποιεί τη διεύθυνση w.x.y.z και δείχνει:

- Πως η τιμή του w προσδιορίζει σε ποια κλάση ανήκει μια διεύθυνση
- Ποιο τμήμα της διεύθυνσης προσδιορίζει το δίκτυο και ποιο τον host
- Πόσα δίκτυα υπάρχουν και πόσοι hosts μπορούν να ανήκουν σε κάθε δίκτυο

Class	**Value of *w***	**Network ID**	**Host ID**	**Number of networks**	**Number of hosts per network**
A	1–126	*w*	*x.y.z*	126	16.777.214
B	128–191	*w.x*	*y.z*	16.384	65.534
C	192–223	*w.x.y*	*z*	2.097.152	254

4.2 Δομή IP πακέτου

Η μορφή της επικεφαλίδας ενός IP datagram έχει ως εξής:

4 bits	4 bits	4 bits	4 bits	4 bits	4 bits	4 bits	bits
VERS	HLEN	TYPE OF SERVICE		ΣΥΝΟΛΙΚΟ ΜΗΚΟΣ			
	IDENTIFICATION			FLAGS	FRAGMENT OFFSET		
TTL		PROTOCOL		HEADER		CHECK	
IP ADDRESS ΠΗΓΗΣ							
IP ADDRESS ΠΡΟΟΡΙΣΜΟΥ							
IP OPTIONS (ΠΡΟΑΙΡΕΤΙΚΑ)						PAD	
Δεδομένα Ανωτέρων Επιπέδων							

Περιγραφή των πεδίων της επικεφαλίδας ενός IP datagram:

VERS: Έκδοση (Version): Μήκος 4 bits και καθορίζει τη έκδοση του IP. Σήμερα υπάρχει η έκδοση 6 (IPV6) αλλά τα περισσότερα συστήματα λειτουργούν με την έκδοση 4 (IPv4).Έτσι το πεδίο αυτό έχει τιμή 0100.

HLEN: Μήκος επικεφαλίδα (Header Length): Μήκος 4 bits.Καθορίζει το μήκος της επικεφαλίδας του πακέτου (συμπεριλαμβάνεται το πεδίο option) σε λέξεις των 32 bits. Αν δεν υπάρχει πεδίο option η τιμή του πεδίου αυτού είναι 5 (5X32bits=160 bits=20 bytes που είναι και το ελάχιστο μήκος της IP επικεφαλίδας)

Type of Service: Μήκος 8 bits. Η τιμή αυτού του πεδίου(και ειδικότερα τα 3 πρώτα bits) καθορίζει τον τρόπο με τον οποίο θα μεταχειριστεί το δίκτυο το πακέτο, σε σχέση με τα άλλα ,υλοποιώντας με αυτό τον τρόπο πολιτικές QoS (Quality of Service).

Συνολικό Μήκος: Μήκος 16 bits προσδιορίζει το μήκος του πακέτου(μετρούμενο σε bytes) συμπεριλαμβανομένης και της επικεφαλίδας. Το μήκος του IP πακέτου δεν είναι σταθερό (εξαιτίας των IP Options) και έχει μέγιστη τιμή 2^{16} =65536 bytes και ελάχιστη 20 bytes.

IDENTIFICATION: Αριθμός Αναγνώρισης:Μήκος 16 bits Ένα IP πακέτο συνήθως διέρχεται από διαφορετικού τύπου δίκτυα μέχρι να φθάσει στον προορισμό του. Είναι πιθανό λοιπόν ένα IP πακέτο να έχει μέγεθος μεγαλύτερο από αυτό που επιτρέπει να ένα δίκτυο, που συναντά στη διαδρομή του .Σε μια τέτοια περίπτωση το πακέτο χωρίζεται σε περισσότερα κομμάτια μικρότερου μεγέθους τα οποία ονομάζονται fragments .Κάθε κομμάτι αποκτά ένα αριθμό Αναγνώρισης που είναι ίδιος για όλα τα τμήματα του ίδιου πακέτου. Αυτός χρησιμεύει ώστε ο κόμβος παραλήπτης να επανασυναρμολογήσει το αρχικό πακέτο από τα τμήματα του .

FLAGS:

DF(Don't Fragment): Όταν έχει τιμή 0 ο αποστολέας ζητάει από το δίκτυο να μην τεμαχιστεί το πακέτο ενώ όταν έχει τιμή 1 επιτρέπεται ο τεμαχισμός.

MF(More Fragment):Έχει την τιμή 1 όταν δεν είναι το τελευταίο τμήμα ενός κατατμημένου πακέτου (υπάρχουν δηλαδή και άλλα τμήματα του ίδιου πακέτου) και τιμή 0 όταν είναι το τελευταίο.

FRAGMENT OFFSET: θέση τμήματος:Μία τιμή που προσδιορίζει ποιο τμήμα είναι από το αρχικό IP πακέτο

Χρόνος ζωής Time to live TTL: Η αρχική τιμή του πεδίου αυτού ,όταν το πακέτο ξεκινάει από τον αποστολέα, προσδιορίζεται από τα πρωτόκολλα των υψηλότερων επιπέδων αλλά η μέγιστη τιμή έναρξης είναι 255.Κάθε φορά που το πακέτο περνάει από ένα router του δικτύου, η τιμή του πεδίου αυτού μειώνεται κατά 1 .Όταν ένας κόμβος διαπιστώσει ότι ένα πακέτο έχει τιμή TTL=0 τότε απορρίπτει το πακέτο. Στην πράξη το πεδίο αυτό είναι ένας μετρητής hops. Η χρήση του πεδίου αυτού είναι να καθορίζει ένα μέγιστο χρόνο ζωής του πακέτου μέσα στο δίκτυο καθώς και την αποφυγή της κατάστασης να βρεθεί ένα πακέτο σε ατέρμονα βρόχο.(από λάθη δρομολόγησης συνήθως)

PROTOCOL: Πρωτόκολλο:Η τιμή του πεδίου καθορίζει ποιο είναι το πρωτόκολλο του υψηλότερου επιπέδου, δεδομένα του οποίου μεταφέρει το IP πακέτο. Παραδείγματα τέτοιων τιμών είναι TCP=6,UDP=17,ICMP=1,IGMP=2

HEADER CHECK: Αθροισμα ελέγχου επικεφαλίδας:Χρησιμοποιείται για τον έλεγχο της ορθής μετάδοσης της επικεφαλίδας κάθε πακέτου. Ο έλεγχος αυτός είναι επιβεβλημένος, γιατί, καθώς το αυτοδύναμο πακέτο περνά από δρομολογητή σε δρομολογητή, η επικεφαλίδα του συνεχώς τροποποιείται, με αποτέλεσμα να αυξάνεται η πιθανότητα να συμβεί κάποιο σφάλμα. Δεν λαμβάνονται υπόψη στον υπολογισμό τα δεδομένα. Η τιμή του πεδίου αυτού υπολογίζεται σε κάθε κόμβο του δικτύου και αν κάποιος (κόμβος) δεν βρει την αναμενόμενη τιμή ,τότε το πακέτο απορρίπτεται.

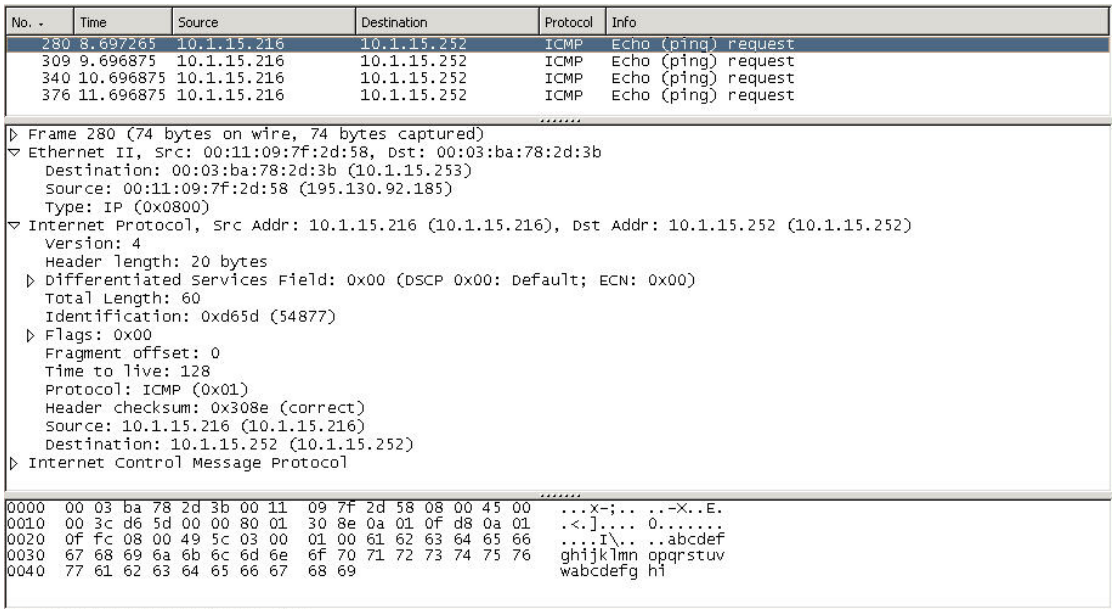
IP ADDRESSES: Διεύθυνση αποστολέα και παραλήπτη:Οι IP διευθύνσεις αποστολέα και παραλήπτη που φέρει κάθε IP πακέτο. Με βάση τη διεύθυνση παραλήπτη γίνεται η δρομολόγηση κάθε πακέτου στον προορισμό του.

Options: Το πεδίο αυτό χρησιμοποιείται για να μεταφέρει πληροφορίες ελέγχου, διαχείρισης και μετρήσεων επίδοσης του δικτύου. Πρόκειται για πεδίο που δεν είναι υποχρεωτικό και χρησιμοποιείται σε λίγες υλοποιήσεις του IP.

4.2.1 Τι θα κάνετε:

Τα αποτελέσματα στο Wireshark που εμφανίζονται στο φυλλάδιο αυτό ,είναι μεταξύ δύο hosts σε δύο Wireshark που συνδέονται με ένα router, με IP διευθύνσεις 10.1.15.216 και 10.1.15.252

- Τρέξτε το Wireshark και ξεκινήστε τη σύλληψη πακέτων.
- Πραγματοποιείστε ping σε κάποιο γειτονικό σας Η/Υ. Στην συνέχεια σταματήστε την καταγραφή. Πιθανόν να χρειαστεί να εισάγετε φίλτρο εμφάνισης πακέτων ώστε να εμφανίζονται μόνον τα πακέτα που ανταλλάσσονται μεταξύ του δικού σας Η/Υ και του Η/Υ στον οποίο κάνατε ping (ip.src=10.1.15.216 && ip.dst=10.1.15.252) .Τα αποτελέσματα μοιάζουν με τα παρακάτω:



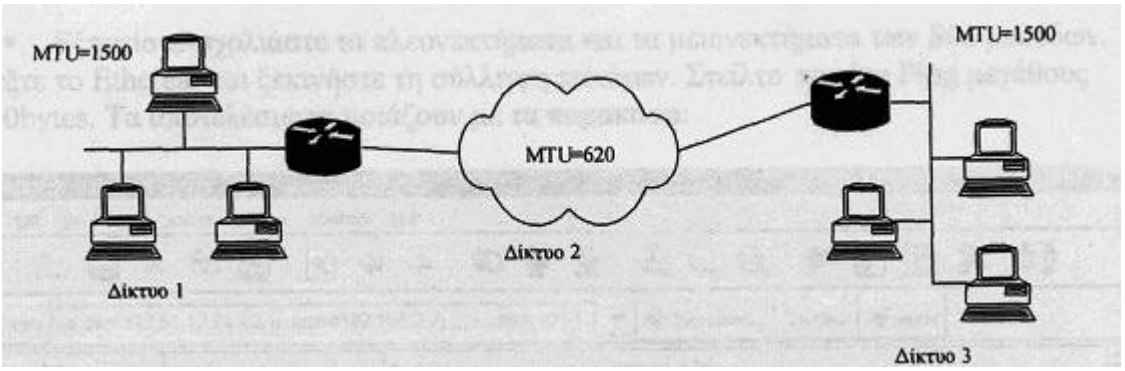
A.

- Διακρίνετε τα πακέτα IP μέσα στα ICMP
- Ποια είναι η IP διεύθυνση του Η/Υ σας
- Ποια είναι η τιμή του πεδίου PROTOCOL και τι καθορίζει;
- Ποιο είναι το μήκος του Header του IP datagram και ποιο το μήκος της περιοχής δεδομένων του datagram(payload);

Εξηγείστε πως προκύπτει το μήκος του payload του IP datagram.(Θυμηθείτε ότι το ping έστειλε 32 bytes δεδομένων με κάθε πακέτο που δημιούργησε)

Β.

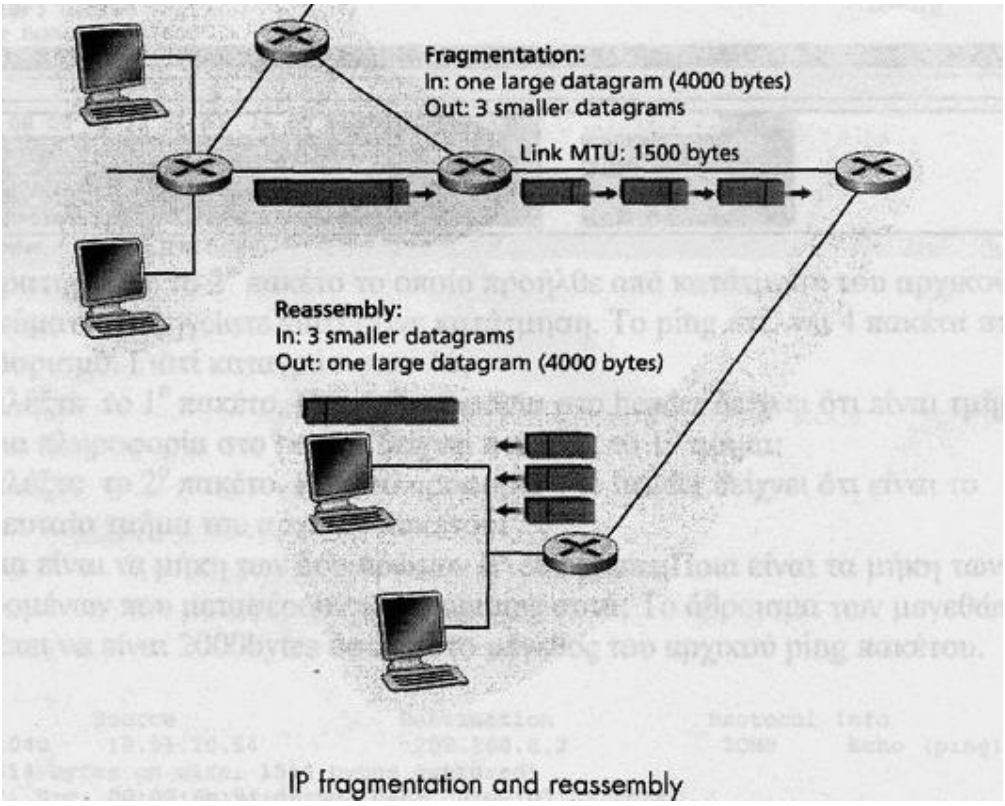
θεωρείστε το παρακάτω δίκτυο:



Τι είναι το MTU;Εξηγείστε αν τα IP πακέτα από το δίκτυο 1 που προορίζονται για το δίκτυο 3 θα πρέπει να διασπασθούν σε fragments.Πόσα νέα datagrams θα προκύψουν;

- Επιλέξτε ένα οποιοδήποτε πακέτο από αυτά που καταγράφηκαν προηγουμένως και διαπιστώστε αν έχουν προέλθει από fragmentation.Εντοπίστε στην επικεφαλίδα του IP πακέτου το κατάλληλο bit.

Για την επανασυναρμολόγηση των τμημάτων ο προορισμός χρησιμοποιεί τα πεδία IDENTIFICATION, FRAGMENT OFFSET και το bit MF.



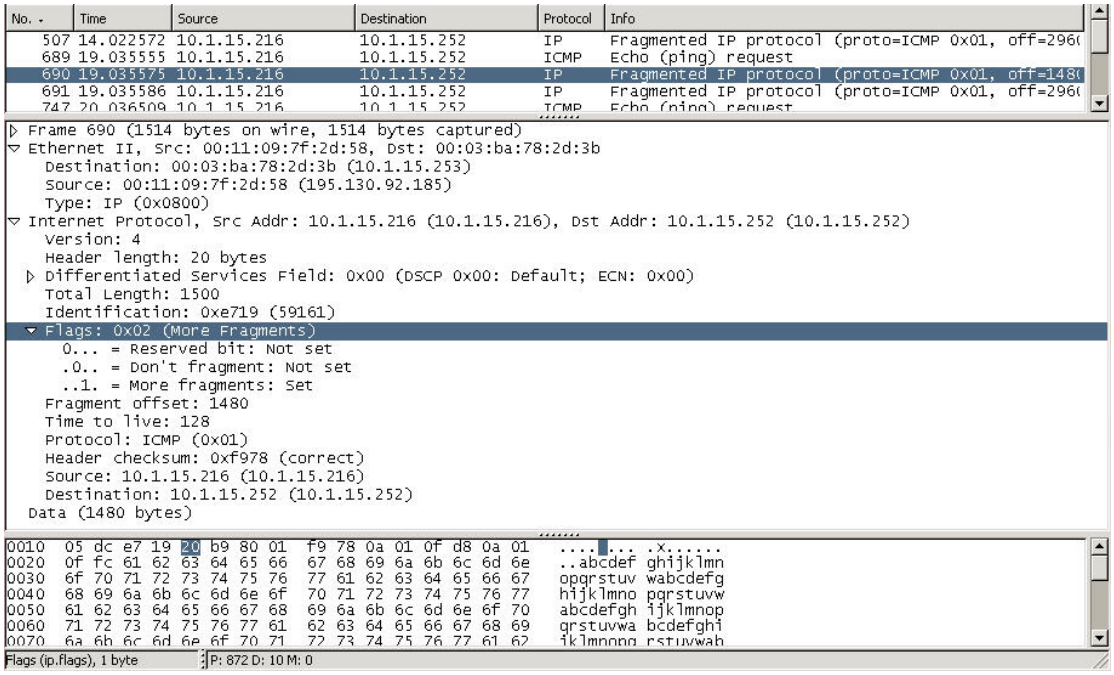
IP fragmentation and reassembly

4.2.2 Πως λειτουργεί το fragmentation

Για το παραπάνω δίκτυο ποιες είναι οι τιμές του πεδίου offset ,του πεδίου συνολικό μήκος και του MF bit σε κάθε fragment;

Τα τμήματα που προήλθαν από τη διάσπαση κάποιου πακέτου IP θα πρέπει κάποια στιγμή, να επανασυναρμολογηθούν ώστε ο παραλήπτης να λάβει το αρχικό πακέτο. Αυτή διαδικασία γίνεται από το IP software του παραλήπτη όταν φθάσουν όλα τα fragments. Ένας άλλος τρόπος θα ήταν κάθε ενδιάμεσος router ,αν το φυσικό δίκτυο στο οποίο είναι συνδεδεμένος και βρίσκεται στην κατεύθυνση του προορισμού έχει κατάλληλο MTU, να επανασυναρμολογεί τα τμήματα και να δημιουργεί το αρχικό πακέτο.(αυτό δεν γίνεται στο TCP/IP).

- Εξηγείστε-σχολιάστε τα πλεονεκτήματα και τα μειονεκτήματα των δύο μεθόδων.
- Τρέξτε το Wireshark και ξεκινήστε τη σύλληψη πακέτων. Στείλτε πακέτα Ping μεγέθους 3000 bytes. Τα αποτελέσματα μοιάζουν με τα παρακάτω:



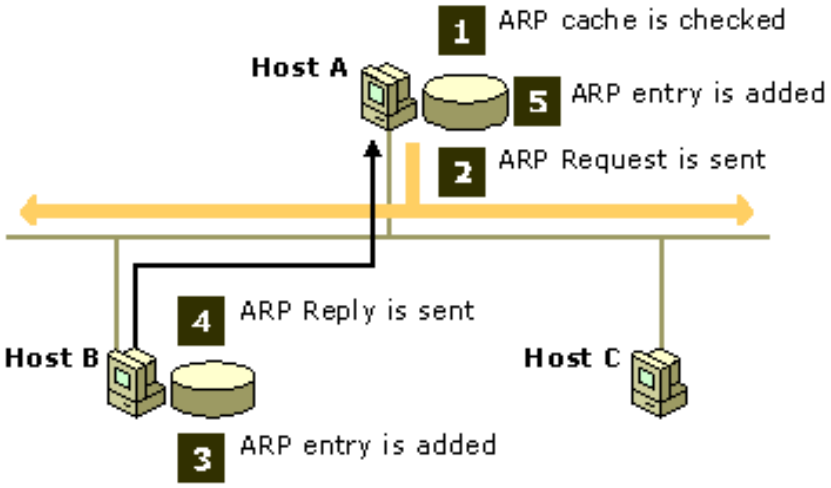
- Παρατηρείστε το 2ο πακέτο το οποίο προήλθε από κατάτμηση του αρχικού μηνύματος. Εξηγείστε γιατί έγινε κατάτμηση. Το ping στέλνει 4 πακέτα στον προορισμό .Γιατί καταγράφηκαν 16;
- Επιλέξτε το 1ο πακέτο. Ποια πληροφορία στο header δείχνει ότι είναι το 1ο τμήμα
- Επιλέξτε το 2ο πακέτο. Ποια πληροφορία στο header δείχνει ότι είναι το τελευταίο τμήμα του αρχικού πακέτου.
- Ποια είναι τα μήκη των δύο πρώτων IP datagrams; Ποια είναι τα μήκη των δεδομένων που μεταφέρουν τα datagrams αυτά;Το άθροισμα των μεγεθών αυτών πρέπει να είναι 2000 bytes όσο δηλαδή και το μέγεθος του αρχικού ping πακέτου.

5. Δομή ARP πακέτου

Υπάρχουν τουλάχιστον δύο ειδών διευθύνσεις οι φυσικές(Hardware) ή MAC και οι λογικές (διευθύνσεις επιπέδου δικτύου π.χ IP διευθύνσεις) θα πρέπει να υπάρχει μια αντιστοιχία μεταξύ των. Και αυτό διότι για να στείλει ένα πακέτο (IP για παράδειγμα) ο Χ στον Υ θα πρέπει να το ενθυλακώσει σε ένα πλαίσιο κατάλληλο για το φυσικό δίκτυο που πρέπει να χρησιμοποιηθεί για τη διαδρομή προς τον Υ(Ethernet για παράδειγμα).Αν υποθέσουμε (για ευκολία) ότι Χ,Υ βρίσκονται στο ίδιο δίκτυο το πλαίσιο αυτό θα έχει διευθύνσεις προορισμού και αποστολής τις φυσικές διευθύνσεις των Χ,Υ. Ο Χ που δημιουργεί το πλαίσιο, πρέπει να «ανακαλύψει» την φυσική διεύθυνση του Υ , με δεδομένο την λογική του διεύθυνση ,αφού αυτή (τη λογική) γνωρίζουν οι εφαρμογές που τρέχουν στον Χ. Το πρωτόκολλο ARP (Address Resolution Protocol) επιτελεί αυτό το έργο. Προκειμένου ο Χ να μην επαναλαμβάνει τη διαδικασία για κάθε πακέτο που στέλνει κατά τη διάρκεια ενός session με τον Υ, κάθε φορά που μαθαίνει την αντιστοίχιση μιας λογικής διεύθυνσης με μια MAC , αποθηκεύει την πληροφορία σε μια Arp Cache μνήμη ,ώστε την επόμενη φορά η αναζήτηση να είναι ταχύτερη. Τα μηνύματα Arp έχουν την παρακάτω μορφή:

<table>
<tr><td>8 bits</td><td>8 bits</td><td>8 bits</td><td>8 bits</td></tr>
<tr><td colspan="2">Hardaware Type</td><td colspan="2">Protocol Type</td></tr>
<tr><td>Hlen</td><td>Plen</td><td colspan="2">Operation</td></tr>
<tr><td colspan="4">Sender Hardware Address</td></tr>
<tr><td colspan="2">Sender Hardware Address</td><td colspan="2">Sender IP Address</td></tr>
<tr><td colspan="2">Sender IP Address</td><td colspan="2">Target Hardware Address</td></tr>
<tr><td colspan="4">Target Hardware Address</td></tr>
<tr><td colspan="4">Target IP Address</td></tr>
</table>

Το πρωτόκολλο ARP σχεδιάστηκε να λειτουργεί με διάφορες δικτυακές τεχνολογίες και έτσι είναι αρκετά γενικό. Η σημασία των πεδίων είναι:
Hardware Type:Ανάλογα με το είδος του φυσικού δικτύου. 1 για το Ethernet
Protocol Type:Ανάλογα με το πρωτόκολλο επιπέδου δικτύου. 0x800 για το IP
Operation:1=Arp Request, 2=Arp Response, 3=Rarp Request, 4=Rarp Response
Hlen: Μήκος των φυσικών (Hardware)διευθύνσεων.
Plen: Μήκος λογικών διευθύνσεων.
Η ανταλλαγή Arp μηνυμάτων φαίνεται στο σχήμα που ακολουθεί:



Οι καταχωρίσεις στην Arp μνήμη έχουν συγκεκριμένη διάρκεια η οποία μόλις εκπνεύσει η αντίστοιχη καταχώρηση διαγράφεται.(**Γιατί**;)

Για τις ανάγκες του εργαστηρίου, θα στείλετε με την εντολή ping πακέτα σε κάποιον Η/Υ , αφού ενεργοποιείστε την καταγραφή πακέτων από το Wireshark. Τα αποτελέσματα μοιάζουν με τα παρακάτω: