LAB-06 (ICMP, ARP)

Ex. 1 | ping in LAN

1.1 |
Capture filter : ether host 7C:2A:31:40:C9:AF

1.2 |
Display filter : arp or icmp

1.3 |
Μετά την εκτέλεση της εντολής ping προς το default gateway, ανταλάσονται πακέτα arp με gateway το οποίο γνωρίζοντας την ip του υπολογιστή μας, ζητά να μάθει και την mac address ωστε να συμπληρώσει το apr table του.

1.4 |
Πεδίο : Protocol → Τιμή : ICMP (01)

1.5 |
Header Length (ICMP) : 8 bytes

1.6 |
(1) Type, (2) Code, (3) Checksum, (4) Identifier, (5) Sequence Number

1.7 |
Type: 8 (Echo (ping) request) → 08 HEX
Code: 0 → 00 HEX

1.8 |
Identifier : 0001 HEX
Sequence Number : 003b HEX

1.9|
Data Length : 32 bytes
Περιεχόμενο : Λατινικοί χαρακτήρες από το a-w και από το a-i

1.10 |
Header Length (ICMP) : 8 bytes. Ναί, είναι ίδιο με αυτό του request

1.11 |
Type: 0 (Echo (ping) reply) → 00 HEX
Code: 0 → 00 HEX

1.12 |
Το πεδίο Type το οποίο είναι το μόνο που αλλάζει

1.13 |
Identifier : 0001 HEX
Sequence Number : 003b HEX

1.14 |
Οι τιμές είναι ίδες με το 1.13 και ταυτίζονται για τα δύο αυτά πακέτα (request και reply)

1.15 |
Χρησιμοποιούνται για γίνεται εφικτή η αντιστοιχηση ενός request πακέτου με το αντίστοιχο reply.

DIRECTORY

1.16 |
Data Length : 32 bytes
Περιεχόμενο : Είναι ίδιο με αυτό του request πακέτου (βλ. 1.9)

1.17 |
Όχι, δεν διαφέρει. Ταυτίζονται.

1.18 |
Οι ανταλαγές γίνονται μεταξύ του υπολογιστή και μίας συγκεκριμένης IP και τα αποτελέσματα της ping αναπαριστούν το χρόνο που έκαναν τα πακέτα για να φτάσουν στην IP αυτή και να επιστρέψουν.

1.19 | ping <address> -n 2

1.20 |
Στάλθηκαν 6 πακέτα ARP request

1.21 |
Στέλνονται κάθε περιπου 1 δευτερόλεπτο

1.22 |
Δεν στάλθηκε κανένα ICMP μήνυμα

1.23 |
Στο παράθυρο εντολών για όλα τα ping requests, στο destination αναγράφει Destination Host Unreachable. Αυτό το καταλαβαίνουμε από το Wireshark καθώς δεν υπάρχουν καθόλου ICMP πακέτα και όλα τα ARP δεν έχουν κάποια απάντηση.

Ex. 2 | ping in WAN

2.1 |
Οι διευθύνσεις έχουν παραμείνει ίδιες με πριν στον ARP table

2.2 |
Destination: 50:78:b3:cd:48:fa
Source: 7c:2a:31:40:c9:af

2.3 |
Source Address: 192.168.1.8
Destination Address: 147.102.1.1

2.4 |
Η MAC του Destination (50:78:b3:cd:48:fa) αντιστοιχεί στην IP 147.102.1.1 και η MAC του Source στην 192.168.1.8

2.5 |
Όχι, δεν παρατήρησα κάποιο

2.6 |
Δεν υπήρξαν γιατί η IP στην οποία έγινε ping ηταν εκτός του τοπικού δικτύου και την MAC address μπορεί να την αναζητήσει μόνο κάποιος άλλος δρομολογητής.

2.7 |
Display filter : arp or icmp.type == 0

2.8 |
Προκύπτει από το πεδίο Time to Live της επικεφαλίδας IPv4 του πακέτου reply

2.9 |
Εμφανίζονται μόνο ICMP requests

2.10 |
Στη προηγούμενη περίπτωση δεν είχαμε μηνύματα ICMP requests, αλλά μόνο ARP. Σε αυτή τη περίπτωση, λόγω του διαφορετικού υποδικτύου, δεν στέλνονται στον υπολογιστή μας πακέτα ARP (αλλά στο router). Επομένως, ο υπολογιστής μας κάπως πρέπει να εντοίσει αν υπάρχει ο υπολογιστής με την IP που ψάχνει και αυτό γίνεται στέλνοντας requests τα οποία κάνουν expire.

Ex. 3 | tracert/traceroute

3.1 |
Data Length : 64 bytes, Περιεχόμενο : Όλα μηδενικά (00 HEX)

3.2 |
Το μήκος δεδομένων είναι διπλάσια σε σχέση με το ερώτημα 1.9 και τα δεδομένα είναι κενά

3.3 |
Time-to-live exceeded

3.4 |
Type: 11 (Time-to-live exceeded) → 0b HEX
Code: 0 (Time to live exceeded in transit) → 00 HEX

3.5 |
Checksum (2 bytes), Unsused (1+2 bytes), Length(1 byte)

3.6 |
Επικεφαλίδα : 8 bytes
Data : 20+8+64 bytes = 92 bytes

3.7 |
Στο περιεχόμενο του ICMP μηνήματος περιέχονται οι πληροφορίες του πρωτοκόλλου IPv4 εξαιτίας του οποίου παράχθηκε (Identification κλπ)

Ex. 4 | Path MTU Discovery

4.1 |
Θα πρέπει Data + Headers = MTU. Άρα σε όλες τις τιμές της MTU που αναγράφονται για να ορίσουμε το length του πακέτου αφαιρούμε το IPv4 header (20 bytes) και το ICMP header (8 bytes). Άρα πχ χρησιμοποιούμε την 1500-28 = 1472

4.2 |
Όχι, δεν παρατηρήθηκε

4.3 |
Δεν το παρήγαγε κάποιος κόμβος της διαδρομής

4.4 |
(Χρησιμοποιήθηκε το αρχείο mtu.pcap)
Type: 3 (Destination unreachable) → 03 HEX
Code: 4 (Fragmentation needed) → 04 HEX

4.5 |
Το πεδίο Code. MTU of next hop: 1492

4.6 |
Περιέχει το περιεχόμενο του IPv4 header του πακέτου που προκάλεσε αυτό το μήνημα.

4.7 |
Για τη τιμή MTU = 1492

4.8 |
Για τιμές MTU = {1492, 1006}

4.9 |
Για τη τιμή MTU = 576

4.10 |
Είναι η MTU κάποιου ενδιάμεσου κόμβου, γιατί για την αμέσως επόμενη μεγαλύτερη τιμή της MTU είχε υπάρξει σφάλμα σε ενδοιάμεσο κόμβο.

4.11 |
Γιατί είναι ο τελικός κόμβος, επομένως δεν χρειάζεται να θρυματίσει το πακέτο.

4.12 |
Έχει μέγεθος 1464 bytes το οποίο είναι ακέραιο πολλαπλάσιο του 8 bytes.

Ex. 5 | Port Unreachable

5.1 |
Capture filter : ip host 147.102.40.15

5.2 |
nslookup edu-dy.cn.ntua.gr 147.102.40.15

5.3 |
Έλαβα απάντηση "DNS request timed out", δηλαδή το request δεν είχε αρκετά μεγάλο TTL.

5.4 |
Ναι, παρατηρήθηκαν 5 μηνήματα DNS

5.5 |
Πρωτόκολλο μεταφοράς είναι το UDP και Destination Port η 53

5.6 |
Ναι, παρατήρησα 5 τέτοια ICMP μηνήματα

5.7 |
Type: 3 (Destination unreachable) → 03 HEX
Code: 3 (Port unreachable) → 03 HEX

5.8 |
Το πεδίο Code

5.9 |
Τα μηνήματα DNS έχουν πάντα Destination Port : 53

5.10 |
Δεν έχω linux

Ex. 6 | IPv6 and ICMPv6

6.1 |
ping -6 2001:648:2000:329::101
tracert -6 2001:648:2000:329::101

6.2 |
Capture filter : ip6
Display filter : icmpv6

6.3 |
Type: IPv6 (0x86dd)

6.4 |
IPv6 Header : 40 bytes

6.5 |
(1) Version, (2) Traffic Class, (3) Flow Label, (4) Payload Length, (5) Next Header, (6) Hop Limit, (7) Source Address, (8) Destination Address

6.6 |

H Hop Limit

6.7 |
Το πεδίο Next Header το οποίο έχει τιμή 58 → 3α HEX

6.8 |
Ναί, είναι ίδια

6.9 |
Type: Echo (ping) request (128) → 80 HEX
Data Length : 32 bytes

6.10 |
Ναι, είναι ίδια

6.11 |
Type: Echo (ping) reply (129) → 81 HEX
Data Length : 32 bytes

6.12 |
Έχει διπλάσιο μήκος δεδομένων (64 bytes)

6.13 |
Όχι, έχει προστεθεί το πεδίο Reserved

6.14 |
Type: Time Exceeded (3) → 03 HEX
Data Length : 64 bytes

6.15 |
Περιέχει μόνο μηδενικά

6.16 |
Παρατήρησα μηνήματα ICMPv6 τύπου Neighbor Solicitation και Neighbor Advertisement

6.17 |
Έχουν Type: Neighbor Solicitation (135) και Type: Neighbor Advertisement (136) αντίστοιχα και μέγεθος πακέτου ίσο με 86 bytes συνολικά.