ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

6^{Ο} ΕΡΓΑΣΤΗΡΙΟ

Σεραφείμ Τζελέπης AM:el18849,

Huawei MateBook 14, Windows 10,

Mac Address: 5C-3A-45-DC-95-1D,

Ομάδα : 4

1)

1.1: Το φίλτρο σύλληψης που χρησιμοποιήθηκε είναι το ‘ether host 5c:3a:45:dc:95:1d’

1.2: Το φίλτρο απεικόνισης που χρησιμοποιήθηκε είναι το ‘arp or icmp’

1.3: Καταγράφθηκαν και σκοπός τους ήταν να βρεθεί η MAC Address της διεύθυνσης 192.168.1.1 η οποία είναι η διεύθυνση της προκαθορισμένης πύλης στην οποία κάνουμε ping.

1.4: Protocol : 1 (ICMP)

1.5: Το μήκος της ICMP επικεφαλίδας των ICMP echo requests είναι 8 bytes.

1.6:

- Type: 1 Byte
- Code: 1 Byte
- Checksum: 2 Bytes
- Identifier: 2 Bytes
- Sequence Number: 2 Bytes

4 Bytes

Type	Code	Checksum
Identifier		Sequence Number

1.7: Type: 8 (Echo (ping) request), Code: 0

1.8: Για το πρώτο request έχουμε

- Identifier: 0x0001
- Sequence Number: 0x017e

1.9: Το μήκος των δεδομένων του ICMP echo request είναι 32 Bytes και το περιεχόμενο είναι αύξοντες δεκαεξαδικοί αριθμοί ξεκινώντας από το 61 μέχρι το 77 και στην συνέχεια ξανά αύξοντες δεκαεξαδικοί αριθμοί ξεκινώντας από το 61 μέχρι το 69.

1.10: Το μήκος του είναι 8 Bytes και έχει την ίδια δομή με αυτή του request.

1.11: Type: 0 (Echo (ping) reply), Code: 0

1.12: Το πεδίο Type καθορίζει το είδος του μηνύματος ICMP. Όταν έχει την τιμή 0 έχουμε reply, ενώ όταν έχει την τιμή 1 έχουμε request.

1.13: Για το πρώτο reply έχουμε

- Identifier: 0x0001
- Sequence Number: 0x017e

1.14: Οι τιμές για το request είναι αυτές του ερωτήματος 1.8 και παρατηρούμε ότι είναι ίδιες με αυτές του ερωτήματος 1.13 .

1.15: Ο σκοπός του πεδίου Identifier και του πεδίου Sequence Number είναι η αντιστοίχιση ενός echo request με το reply που αποτελεί απάντηση σε αυτό.

1.16: Το μήκος των δεδομένων του echo reply είναι 32 bytes και το περιεχόμενο είναι αύξοντες δεκαεξαδικοί αριθμοί ξεκινώντας από το 61 μέχρι το 77 και στην συνέχεια ξανά αύξοντες δεκαεξαδικοί αριθμοί ξεκινώντας από το 61 μέχρι το 69..

1.17: Όχι έχουν ακριβώς το ίδιο περιεχόμενο.

1.18: Οι ανταλλαγές ICMP μηνυμάτων είναι απολύτως συνδεδεμένες με τα αποτελέσματα της ping στο παράθυρο εντολών. Πιο συγκεκριμένα κάθε reply που αναγράφεται στο παράθυρο εντολών ως επιτυχές αντιστοιχεί σε μια ανταλλαγή μηνυμάτων ICMP(request + reply).

1.19: ping /n 2 192.168.1.5

1.20: Στάλθηκαν 5 ARP requests.

1.21: Κάθε 1 δευτερόλεπτο.

1.22: Κανένα

1.23: Στο παράθυρο εντολών αναγράφεται ότι και στα δυο replies, ότι host is unreachable

2)

2.1: C:\Windows\system32>arp -a

Interface: 192.168.1.13 --- 0x5

Internet Address	Physical Address	Type
192.168.1.1	d4-60-e3-b9-96-50	dynamic
192.168.1.17	c4-36-6c-64-43-42	dynamic
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.113	01-00-5e-00-00-71	static
239.255.255.250	01-00-5e-7f-ff-fa	static

Interface: 172.18.224.1 --- 0x39

Internet Address	Physical Address	Type
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.113	01-00-5e-00-00-71	static
239.255.255.250	01-00-5e-7f-ff-fa	static

2.2: Source: 5c:3a:45:dc:95:1d, Destination: d4:60:e3:b9:96:50

2.3: Source: 192.168.1.13, Destination: 147.102.1.1

2.4: Η διεύθυνσης MAC πηγής ανήκει στην κάρτα δικτύου του υπολογιστή μου και συνεπώς η IPv4 διεύθυνση στην οποία αντιστοιχεί είναι αυτή του υπολογιστή η 192.168.1.13, και η διεύθυνση προορισμού ανήκει στο ρούτερ του τοπικού δικτύου στο οποίο βρίσκομαι συνδεδεμένος και μπορούμε από τον πίνακα ARP ότι η IPv4 διεύθυνση είναι η 192.168.1.1 .

2.5: Όχι.

2.6: Η εντολή ping είχε προορισμό σε εξωτερικό δίκτυο όποτε έπρεπε να προωθηθεί και να δρομολογηθεί από την default gateway της όποιας η MAC address είναι αποθηκευμένη στο ARP table του υπολογιστή μου για αυτό και δεν υπήρξαν ARP πακέτα.

2.7: Το νέο φίλτρο σύλληψης είναι το 'icmp.type == 0'

2.8: Η τιμή στο πεδίο της επικεφαλίδας TTL ταυτίζεται με αυτή στο παράθυρο εντολών και είναι TTL = 58 και προκύπτει από τον αρχικό TTL με το οποίο στάλθηκε το reply μείον τον αριθμό των ενδιάμεσων κόμβων μέχρι να φτάσει το reply στον υπολογιστή μας.

2.9: Εμφανίζονται μόνο ICMP Echo (ping) requests, Type = 8.

2.10: Στην δεύτερη περίπτωση η διεύθυνση στην οποία κάνουμε ping είναι εξωτερικού δικτύου συνεπώς τα πακέτα στέλνονται στο default gateway του δρομολογητή μας καθώς δεν μπορούμε να γνωρίζουμε αν η IPv4 address αντιστοιχεί σε ενεργό κόμβο, και έτσι παράγονται τα ICMP echo requests, ενώ στην πρώτη περίπτωση που η IPv4 διεύθυνση είναι αντιστοιχεί σε μη ενεργό κόμβο του υποδικτύου μας δεν χρειάστηκε να αποσταλούν τα ICMP πακέτα.

3)

3.1: Το μήκος των δεδομένων είναι 64 Bytes και είναι όλα μηδενικά.

3.2: Στο ερώτημα 1.9 βλέπουμε ότι το μήκος στην περίπτωση της εντολής Ping είναι τα 32 Bytes έναντι των 64. Επίσης στην περίπτωση της ping τα δεδομένα δεν ήταν μηδενικά αλλά ήταν δυο αύξουσες ακολουθίες.

3.3: Time-to-live exceeded (Time to live exceeded in transit).

3.4: Type: 11 (Time-to-live exceeded), Code: 0 (Time to live exceeded in transit).

3.5:

- Checksum: 2 Bytes
- Unused: 3 Bytes
- Length: 1 Byte

3.6: Η επικεφαλίδα έχει μέγεθος 8 Bytes και τα δεδομένα 64 Bytes.

3.7: Το περιεχόμενο του μηνύματος λάθους περιέχει το IPv4 header του ICMP request καθώς και την πρώτη οκτάδα bytes του ICMP request.

4)

4.1: Για να παραχθούν τα πακέτα με το ζητούμενο μέγεθος έπρεπε να υπολογίσουμε ότι το συνολικό μέγεθος του IPv4 πακέτου θα είναι τα δεδομένα του ICMP + ICMP header (8 Bytes) + IP header (20 Bytes), συνεπώς οι τιμές που χρησιμοποιήθηκαν είναι οι εξής: 1472, 1464, 978, 548, 524, 516, 484, 480, 268.

4.2: Ναι.

4.3: Το παρήγαγε το router με διεύθυνση 192.168.1.1 (Default Gateway).

4.4: Type: 3 (Destination unreachable), Code: 4 (Fragmentation needed)

4.5: Το πεδίο Code και η τιμή του πεδίου είναι MTU of next hop: 1492 .

4.6: Στο πεδίο των ICMP δεδομένων έχουμε 520 Bytes τα οποία είναι επαναλαμβανόμενη αύξοντες αριθμοί ξεκινώντας από το 61 μέχρι το 77, η τελευταία ακολουθία φτάνει μέχρι το 6e.

4.7: Για την τιμή 1492.

4.8: Για τις τιμές 1500,1492,1006.

4.9: 576

4.10: Το ICMP Destination unreachable μήνυμα παράγεται όταν ένας κόμβος αδυνατεί να προωθήσει ένα πακέτο καθώς υπερβαίνει το MTU του επόμενου hop, συνεπώς εξ ορισμού αυτό το μήνυμα μπορεί να προέλθει μόνο από ενδιάμεσο κόμβο.

4.11: Διότι παρόλο που η δικτυακή επαφή του προορισμού δεν λαμβάνει πακέτα τέτοιου μεγέθους, οι ενδιάμεσοι κόμβοι μπορούσαν να προωθήσουν χωρίς θρυμματισμό αυτά τα πακέτα και συνεπώς δεν παρήγαγαν κάποιο ICMP Destination unreachable μήνυμα.

4.12: Δεν παρατηρείται θρυμματισμός.

5)

5.1: host 157.102.40.15

5.2: nslookup edu-dy.cn.ntua.gr

5.3: Non-authoritative answer

5.4: Ναι

5.5: UDP και η θύρα προορισμού είναι το port 53.

5.6: Ναι

5.7: Type: 3(0x03), Code: 3(0x03).

5.8: Το πεδίο code.

5.9: Η θύρα η οποία είναι προκαθορισμένη για τα DNS Queries είναι η port 53.

5.10: Το λειτουργικό μου σύστημα είναι Windows.

6)

6.1: ping /6 2001:648:2000:329::101 και tracert /6 2001:648:2000:329::101 .

6.2: Το φίλτρο σύλληψης είναι το “ip6” ενώ το φίλτρο απεικόνισης το “icmpv6” .

6.3: Type: 0x86dd(IPv6).

6.4: 40 Bytes.

6.5:

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Source Address			
Source Address			
Source Address			
Destination Address			
Destination Address			
Destination Address			
Destination Address			

6.6: Hop Limit.

6.7: Next Header και στην συγκεκριμένη περίπτωση είναι Next Header: ICMPv6 (58) δηλαδή 0x3a.

6.8: Είναι ίδια απλώς το Sequence Number εδώ αναγράφεται ως Sequence.

6.9: Type: 128(Echo Ping Request) και τα δεδομένα έχουν μήκος 32 Bytes.

6.10: Ναι είναι ίδια.

6.11: Type: 129(Echo Ping Reply) και τα δεδομένα έχουν μήκος 32 Bytes.

6.12: Τα πεδία Type, Code, Identifier παραμένουν ίδια ενώ το Checksum, το Sequence και το μήκος των δεδομένων αλλάζουν

6.13: Η μόνη διαφορά στη δομή είναι ότι σε αυτή την περίπτωση έχουμε το πεδίο reserved αντί του unused και του Length που είχαμε στο 3.4, 3.5 .

6.14: Type: 3 και το μήκος των δεδομένων είναι 64 Bytes

6.15: Μηδενικά

6.16: Neighbor Advertisement, Neighbor Solicitation, Router Advertisement

6.17:

- Neighbor Advertisement: Type: 136, Length: 32 Bytes.
- Neighbor Solicitation: Type: 135, Length: 32 Bytes.
- Router Advertisement: Type: 134, Length: 56 Bytes.