Δίκτυα υπολογιστών

Εργαστηριακή άσκηση 6 (Πρωτόκολλο ICMP)

Τσάκωνας Παναγιώτης (03119610) Ομάδα: 2

Ακαδημαϊκό Έτος: 2022-2023

Άσκηση 1: Εντολή ping στο τοπικό υποδίκτυο

1.1) Το φίλτρο σύλληψης που χρησιμοποίησα είναι το εξής: `ether host fc:e2:6c:02:ce:3f`.

1.2) Το φίλτρο απεικόνισης που χρησιμοποίησα είναι: `icmp or arp`.

1.3) Ο λόγος των πακέτων ARP που ανταλλάχθηκαν είναι ότι κατά την εκτέλεση της εντολής ping προς το default gateway, το default gateway γνωρίζοντας το ip του υπολογιστή μου ζητά να μάθει και την Mac Address, έτσι ώστε να μπορέσει να ολοκληρώσει τον πίνακα ARP.

1.4) Είναι το πεδίο Protocol με τιμή ICMP 0x01.

1.5) Το μήκος της επικεφαλίδας των μηνυμάτων ICMP Echo request είναι 8 bytes.

1.6) Τα ονόματα και το μήκος σε byte των πεδίων της επικεφαλίδας του μηνύματος ICMP Echo request είναι τα ακόλουθα: Type (1 byte), Code (1 byte), Checksum (2 bytes), Identifier (2 bytes), Sequence Number (2 bytes).

1.7) Οι τιμές του πεδίου Type είναι 0x08 και του πεδίου Code είναι 0x00 αντίστοιχα.

1.8) Οι τιμές του πεδίου Identifier είναι 0xde64 και του πεδίου Sequence Number είναι 0x0000 αντίστοιχα.

1.9) Το μήκος του πεδίου δεδομένων των μηνυμάτων ICMP Echo request που παράγει η εντολή ping είναι 48 bytes και το περιεχόμενό του είναι: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637.

1.10) το μήκος της επικεφαλίδας μηνυμάτων ICMP Echo reply είναι 8 bytes και ναι είναι το ίδιο με το Echo request.

1.11) Οι τιμές του πεδίου Type είναι 0x00 και του πεδίου Code είναι 0x00 αντίστοιχα.

1.12) Το πεδία Type καθορίζει το είδους του μηνύματος ICMP, καθώς είναι το μόνο που αλλάζει.

1.13) Οι τιμές του πεδίου Identifier είναι 0xde64 και του πεδίου Sequence Number είναι 0x0000 αντίστοιχα.

1.14) Οι τιμές είναι ίδιες με το 1.13 και οι αριθμοί των πεδίων ταυτίζονται για τα δύο πακέτα request και reply.

1.15) Ο ρόλος των πεδίων ταυτότητας και αύξοντα αριθμού στην επικεφαλίδα των μηνυμάτων ICMP Echo request και Echo reply είναι για γίνεται εφικτή η αντιστοίχιση ενός request πακέτου με το αντίστοιχο reply.

1.16) Το μήκος του πεδίου δεδομένων των μηνυμάτων ICMP Echo reply που παράγει η εντολή ping είναι 48 bytes και το περιεχόμενό του είναι: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f20212223242526272829 2a2b2c2d2e2f3031323334353637.

1.17) Όχι δεν διαφέρει, είναι το ίδιο ακριβώς.

1.18) Οι ανταλλαγές των μνημάτων ICMP, γίνονται μεταξύ του υπολογιστή μου και μίας συγκεκριμένης IP. Η εντολή ping χρησιμοποιείται για να μας δείξει πόσο χρόνο έκαναν τα πακέτα για να φτάσουν στην IP αυτή και να επιστρέψουν.

1.19) Η σύνταξη της εντολής ping χρησιμοποίησα, ώστε να παραχθούν δύο μηνύματα ICMP είναι: `ping -c 2 <address>`.

1.20) Στάλθηκαν 5 πακέτα ARP request για την ανεύρεση της διεύθυνσης MAC του μη ενεργού υπολογιστή.

1.21) Στέλνονται περίπου κάθε 1 sec.

1.22) Δεν στάλθηκε κανένα μήνυμα ICMP .

1.23) Στο παράθυρο εντολών για όλα τα ping requests, στο destination αναγράφεται request timeout for icmp_seq. Αυτό γίνεται αντιληπτό και από το Wireshark καθώς δεν εμφανίζονται καθόλου ICMP πακέτα και τα ARP πακέτα που στέλνονται δεν λαμβάνουν κάποια απάντηση.

Άσκηση 2: Εντολή ping σε άλλο υποδίκτυο

2.1) Οι διευθύνσεις έχουν παραμείνει ίδιες με πριν στον πίνακα ARP.

2.2) Destination Address: 08:ec:f5:d0:d9:1d
Source Address: fc:e2:6c:02:ce:3f

2.3) Source Address: 147.102.203.72
Destination Address: 147.102.1.1

2.4) Του Source ανήκει στην διεύθυνση 147.102.203.72 και του Destination ανήκει στην διεύθυνση 147.102.1.1

2.5) Όχι, δεν παρατήρησα κάποιο πακέτο ARP.

2.6) Δεν υπήρξαν, διότι η IP στην οποία έγινε ping ήταν εκτός του τοπικού δικτύου και την MAC Address μπορεί να την αναζητήσει μόνο κάποιος άλλος δρομολογητής.

2.7) Το φίλτρο απεικόνισης που χρησιμοποίησα είναι: `arp or icmp.type==0`.

2.8) Η τιμή της παραμέτρου TTL που εμφανίζεται στις απαντήσεις του παραθύρου εντολών, προκύπτει από το πεδίο Time to Live της επικεφαλίδας IPv4 του πακέτου reply.

2.9) Εμφανίζονται μόνο τα πακέτα ICMP request.

2.10) Η κίνηση που κατέγραψα σε σχέση με την αντίστοιχη όταν εκτέλεσα προηγουμένως την εντολή ping προς μια διεύθυνση IPv4 εντός του υποδικτύου σας είναι ότι δεν στέλνονται στον υπολογιστή μας πακέτα ARP λόγω του διαφορετικού υποδικτύου. Επομένως, ο υπολογιστής μας πρέπει να εντοπίσει αν υπάρχει ο υπολογιστής με την IP που ψάχνει γι' αυτό στέλνει requests τα οποία κάνουν expire, επειδή δεν φτάνουν στον υπολογιστή που κάνουμε ping.

Άσκηση 3: Εντολή tracert/traceroute

3.1) Το μήκος του πεδίου δεδομένων των μηνυμάτων ICMP Echo request που παράγει η εντολή traceroute είναι 44 bytes και το περιεχόμενο του είναι όλα μηδενικά σε δεκαεξαδική αναπαράσταση.

3.2) Το μήκος δεδομένων είναι μιάμιση φορά περισσότερα σε σχέση με το ερώτημα 1.9 και τα δεδομένα είναι κενά.

3.3) Το μήνυμα λάθους που παρατηρώ είναι Time to Live exceeded.

3.4) Οι τιμές του πεδίου Type είναι 0x0b (Time-to-live exceeded) και του πεδίου Code είναι 0x00 (Time-to-live exceeded in transit) αντίστοιχα.

3.5) η επικεφαλίδα του μηνύματος λάθους πριν τα δεδομένα έχει ακόμα τα ακόλουθα πεδία: Checksum (2 bytes), Unused (1 + 2 bytes), Length(1 byte).

3.6) Το μήκος της επικεφαλίδας του ICMP μηνύματος λάθους της ερώτησης 3.3 είναι 8 bytes και των δεδομένων είναι 72 bytes.

3.7) Στο περιεχόμενο του ICMP μηνύματος περιέχονται οι πληροφορίες του πρωτοκόλλου IPv4 εξαιτίας του οποίου παράχθηκε.

Άσκηση 4: Ανακάλυψη MTU διαδρομής(Path MTU Discovery)

4.1) Οι επικεφαλίδες IPv4 και ICMP έχουν μέγεθος 20 + 8 bytes αντίστοιχα. Συνεπώς, από τις τιμές που δίνονται αφαιρούμε 28. Ελέγχουμε, λοιπόν, τις τιμές 1472, 1464, 978, 548.
4.2) Όχι, δεν παρατηρήθηκε μήνυμα λάθους ICMP Destination Unreachable.
4.3) –
4.4) (Χρησιμοποιήθηκε το αρχείο mtu.pcap) Οι τιμές του πεδίου Type είναι 0x03 (Destination unreachable) και του πεδίου Code είναι 0x04 (Fragmentation needed) αντίστοιχα.
4.5) Το πεδίο Code δηλώνει ότι το λάθος οφείλεται στην απαίτηση μη θρυμματισμού του πακέτου IPv4 και η τιμή της επικεφαλίδας MTU of next hop είναι 1492.
4.6) Το πεδίο των δεδομένων περιέχει το περιεχόμενο του IPv4 header του πακέτου που προκάλεσε αυτό το μήνυμα.
4.7) Η MTU για την οποία δεν λαμβάνετε για πρώτη φορά μήνυμα λάθους ICMP Destination Unreachable, άσχετα από το εάν απαντά ή όχι το 147.102.40.15 είναι η 1492.
4.8) Το 147.102.40.15 δεν απαντά για τις τιμές MTU 1500, 1492 και 1006.
4.9) Η τιμή MTU για την οποία λαμβάνετε απάντηση από το 147.102.40.15 είναι 576.
4.10) Είναι η MTU κάποιου ενδιάμεσου κόμβου, γιατί για την αμέσως επόμενη μεγαλύτερη τιμή της MTU είχε υπάρξει σφάλμα σε ενδιάμεσο κόμβο.
4.11) Το 147.102.40.15 δεν παράγει ICMP Destination Unreachable όταν λαμβάνει πακέτα IPv4 μεγέθους μεγαλύτερου από την MTU της διεπαφής του, διότι είναι ο τελικός κόμβος, επομένως δεν χρειάζεται να θρυμματίσει το πακέτο.
4.12) Το μέγεθος του πρώτου θραύσματος που λαμβάνει ο υπολογιστής μου έχει μέγεθος 586 bytes και είναι μικρότερο από την τιμή της ερώτησης 4.7.

Άσκηση 5: Απρόσιτη θύρα (Port Unreachable)

5.1) Το φίλτρο σύλληψης που χρησιμοποίησα είναι: `host 147.102.40.15`
5.2) Η ακριβής σύνταξη της εντολής που χρησιμοποίησα είναι: `host edu-dy.cn.ntua.gr 147.102.40.15`
5.3) Η απάντηση που έλαβα είναι "communications error to 147.102.40.15#53: connection refused", δηλαδή το request δεν είχε αρκετά μεγάλο TTL.
5.4) Ναι, παρατηρήθηκε 1 μήνυμα DNS στην καταγραφή.
5.5) Το πρωτόκολλο μεταφοράς είναι το UDP και Destination Port η 53.
5.6) Ναι, παρατήρησα 1 μήνυμα λάθους ICMP Destination Unreachable με πηγή το 147.102.40.15.
5.7) Οι τιμές του πεδίου Type είναι 0x03 (Destination unreachable) και του πεδίου Code είναι 0x03 (Port unreachable) αντίστοιχα.
5.8) Το πεδίο Code δηλώνει ότι ο λόγος αποτυχίας είναι κάποια απρόσιτη θύρα.
5.9) Προκύπτει από το γεγονός ότι τα μηνύματα DNS έχουν πάντα Destination Port: 53.
5.10) Κανονικά απαντάει με echo reply, αλλά εδώ η απάντηση είναι το Destination unreachable.

Άσκηση 6: IPv6 και ICMPv6

6.1) Η σύνταξη είναι: `ping6 2001:648:2000:329::101` και `traceroute6 -I 2001:648:2000:329::101.`

6.2) Η σύνταξη του φίλτρου σύλληψης που χρησιμοποίησα είναι `ip6` και το φίλτρο απεικόνισης: `icmpv6`.

6.3) Η τιμή που έχει το πεδίο Type της επικεφαλίδας Ethernet είναι 0x86dd.

6.4) Το μήκος επικεφαλίδας των πακέτων IPv6 είναι 40 bytes.

6.5) Τα ονόματα και το μήκος σε byte των πεδίων της επικεφαλίδας του μηνύματος IPv6 είναι: Version (1 byte), Traffic Class (4 bytes), Flow Label (3 bytes), Payload Length (2 bytes), Next Header (1 byte), Hop Limit (1 byte), Source Address (16 bytes) και Destination Address (16 bytes).

6.6) Η αντίστοιχη επικεφαλίδα της TTL των πακέτων IPv4 είναι η επικεφαλίδα Hop Limit.

6.7) Η επικεφαλίδα που δείχνει το πρωτόκολλο τα δεδομένα του οποίου μεταφέρει το πακέτο IPv6 είναι η Next Header και έχει τιμή 58.

6.8) Ναι είναι ίδια.

6.9) Η τιμή του πεδίου Type είναι 80 και το μήκος δεδομένων είναι 8 bytes.

6.10) Ναι είναι ίδια.

6.11) Η τιμή του πεδίου Type είναι 81 και το μήκος δεδομένων είναι 8 bytes.

6.12) Το μόνο που αλλάζει είναι η τιμή του πεδίου Flow Label.

6.13) Όχι δεν είναι η ίδια, έχει προστεθεί το πεδίο Reserved.

6.14) Η τιμή του πεδίου Type είναι 3 και το μήκος δεδομένων είναι 56 bytes.

6.15) Το πεδίο δεδομένων περιέχει τα πακέτα IPv6 και ICMPv6 του echo request που προκάλεσε το Time Exceeded.

6.16) Ναι, παρατήρησα μηνύματα Neighbor Solicitation, Neighbor Advertisement και Router Advertisement.

6.17) Για το μήνυμα Neighbor Solicitation η τιμή του πεδίου Type είναι 135 και το μήκος δεδομένων είναι 32 bytes. Για το μήνυμα Neighbor Advertisement η τιμή του πεδίου Type είναι 136 και το μήκος δεδομένων είναι 24 bytes. Για το μήνυμα Router Advertisement η τιμή του πεδίου Type είναι 134 και το μήκος δεδομένων είναι 48 bytes.