Εργαστηριακή Άσκηση 6
Πρωτόκολλο ICMP

Ο σκοπός αυτής της εργαστηριακής άσκησης είναι η περαιτέρω εξέταση του πρωτοκόλλου ICMP μέσω της καταγραφής και παρατήρησης των περιεχομένων των πακέτων που ανταλλάσσονται κατά τη διάρκεια της χρήσης των εντολών ping και tracert/traceroute. Το πρωτόκολλο IPv4 δεν παρέχει άμεσους τρόπους που να δείχνουν τι έχει συμβεί με τα πακέτα και απαιτείται κάποιος μηχανισμός για ενημέρωση. Το ICMP είναι ένα βοηθητικό (helper) πρωτόκολλο που παρέχει στο IPv4 τη δυνατότητα αναφοράς λαθών (errors) και απλών ερωτημάτων (queries). Τα μηνύματα ICMP όπως ήδη έχετε δει ενθυλακώνονται σε πακέτα IPv4 και στέλνονται πίσω προς την πηγή του πακέτου που δημιούργησε το πρόβλημα ή υπέβαλε το ερώτημα. Τα μηνύματα απλών ερωτημάτων ICMP στέλνονται για διαγνωστικούς λόγους ή παροχή πληροφόρησης. Είναι είτε αίτημα (Request) που αποστέλλεται από υπολογιστή προς δρομολογητή ή άλλο υπολογιστή είτε απάντηση (Reply) που επιστρέφει τη ζητούμενη πληροφορία στον υπολογιστή που έκανε το αίτημα. Τα ICMP μηνύματα λαθών αναφέρουν διάφορες καταστάσεις λάθους και ανάλογα με την περίπτωση εξειδικεύουν το είδος λάθους. Αποστέλλονται προς την πηγή του πακέτου IPv4 όταν για κάποιο λόγο ένας υπολογιστής ή δρομολογητής στη διαδρομή προς τον προορισμό το απορρίπτει. Για περισσότερες λεπτομέρειες σχετικά με το πρωτόκολλο ICMP ανατρέξτε στο σχετικό RFC 792 καθώς και στο RFC 1122 όπου περιγράφονται οι συνθήκες παραγωγής των μηνυμάτων ICMP.

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

1 Εντολή ping στο τοπικό υποδίκτυο

Ξεκινήστε μια καταγραφή με φίλτρο σύλληψης, ώστε να καταγράφονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση MAC του υπολογιστή σας. Καταγράψτε τα διερχόμενα πλαίσια όταν κάνετε ping σε μια διεύθυνση IPv4 υπολογιστή εντός του *τοπικού δικτύου*, π.χ. την προκαθορισμένη πύλη. Αφού τελειώσει η καταγραφή, εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

1.1 Καταγράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε ώστε να συλλαμβάνονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση MAC του υπολογιστή σας.
1.2 Καταγράψτε τη σύνταξη του φίλτρου απεικόνισης ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.
1.3 Εάν καταγράφηκαν, εξηγήστε τον σκοπό των πακέτων πρωτοκόλλου ARP που ανταλλάχθηκαν.
1.4 Βρείτε το πρώτο μήνυμα *Echo request* του πρωτοκόλλου ICMP. Ποιο είναι το όνομα και η τιμή του πεδίου της επικεφαλίδας IPv4 που προσδιορίζει ότι πρόκειται για μήνυμα ICMP;

Η δομή της επικεφαλίδας των μηνυμάτων ICMP εξαρτάται από το είδος τους. Τα πεδία στην πρώτη λέξη 32 bit είναι ταυτόσημα για όλα τα είδη. Μετά, ανάλογα το είδος ακολουθούν λέξεις 32 bit είτε το 0x00000000 (unused) ώστε το ελάχιστο μήκος μηνύματος ICMP να είναι 8 byte.

1.5 Ποιο είναι το μήκος της επικεφαλίδας των μηνυμάτων ICMP *Echo request*;
1.6 Καταγράψτε τα ονόματα και το μήκος σε byte των πεδίων της επικεφαλίδας του μηνύματος ICMP *Echo request* και σημειώστε στο σχήμα τις θέσεις τους.
1.7 Καταγράψτε την τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας των μηνυμάτων ICMP *Echo request*.
1.8 Καταγράψτε τις τιμές των πεδίων ταυτότητας (Identifier) και του αύξοντα αριθμού (Sequence number) της επικεφαλίδας ενός μηνύματος ICMP *Echo request*.
1.9 Ποιο είναι το μήκος και ποιο το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP *Echo request* που παράγει η εντολή ping;

1.10 Βρείτε **ένα** μήνυμα *Echo reply* του πρωτοκόλλου ICMP. Ποιο είναι το μήκος της επικεφαλίδας μηνυμάτων ICMP *Echo reply*; Έχει την ίδια δομή με αυτή του *Echo request*;
1.11 Καταγράψτε την τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας ICMP των μηνυμάτων *Echo reply*.
1.12 Με βάση τις απαντήσεις σας στις ερωτήσεις 0 και 1.11, ποιο από τα πεδία Type και Code καθορίζει το είδους του μηνύματος ICMP;
1.13 Καταγράψτε τις τιμές των πεδίων ταυτότητας (Identifier) και αύξοντα αριθμού (Sequence number) της επικεφαλίδας ICMP **ενός** μηνύματος *Echo reply*.
1.14 Εντοπίστε το μήνυμα ICMP *Echo request* σε απάντηση του οποίου παράχθηκε το προηγούμενο μήνυμα ICMP *Echo reply*. Ποιες είναι οι αντίστοιχες τιμές των πεδίων ταυτότητας και αύξοντα αριθμού. *[Υπόδειξη: κάντε κλικ στη γραμμή Response Frame και θα μεταφερθείτε στο σωστό πλαίσιο.]*
1.15 Ποιος νομίζετε ότι είναι ο ρόλος των πεδίων ταυτότητας και αύξοντα αριθμού στην επικεφαλίδα των μηνυμάτων ICMP *Echo request* και *Echo reply*; *[Υπόδειξη: Συμβουλευθείτε την ιστοσελίδα http://www.networksorcery.com/enp/default0604.htm επιλέγοντας το "IP protocol suite" από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο ICMP στο δεξιό της μέρος. Διαβάστε τις λεπτομέρειες που αφορούν τα μηνύματα ICMP Echo request]*
1.16 Ποιο είναι το μήκος και ποιο το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP *Echo reply*;
1.17 Διαφέρει αυτό το περιεχόμενο από το αντίστοιχο του μηνύματος ICMP *Echo request*;
1.18 Πώς σχετίζονται οι ανταλλαγές των μηνυμάτων ICMP με τα αποτελέσματα της εντολής ping στο παράθυρο εντολών;

Ξεκινήστε πάλι τη διαδικασία καταγραφής των πακέτων με το ίδιο φίλτρο σύλληψης και εκτελέστε την εντολή ping προς μια διεύθυνση IPv4 του υποδικτύου σας που **δεν** αντιστοιχεί σε ενεργό υπολογιστή ζητώντας να παραχθούν **δύο** μηνύματα ICMP *Echo request*. Εν ανάγκη συμβουλευθείτε το διαχειριστικό περιβάλλον του δρομολογητή σας για να δείτε ποιες διευθύνσεις έχουν εκχωρηθεί. Αφού τελειώσει η καταγραφή, εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

1.19 Ποια σύνταξη της εντολής ping χρησιμοποιήσατε ώστε να παραχθούν δύο μηνύματα ICMP;
1.20 Πόσα πακέτα ARP request στάλθηκαν για την ανεύρεση της διεύθυνσης MAC του μη ενεργού υπολογιστή;
1.21 Κάθε πότε στέλνονται; *[Υπόδειξη: Από το μενού View μπορείτε να επιλέξετε Time Display Format → Seconds Since Previous Displayed Packet.]*
1.22 Πόσα μηνύματα ICMP στάλθηκαν;
1.23 Πώς σχετίζονται τα προηγούμενα με τα αποτελέσματα της εντολής ping στο παράθυρο εντολών;

2 Εντολή ping σε άλλο υποδίκτυο

Προτού ξεκινήσετε την άσκηση, παρατηρήστε τον πίνακα arp του υπολογιστή σας. Στη συνέχεια, χρησιμοποιώντας το φίλτρο σύλληψης των προηγούμενων ερωτήσεων, καταγράψτε τα διερχόμενα πλαίσια όταν κάνετε ping σε έναν υπολογιστή εκτός του τοπικού δικτύου σε **μία** από τις ακόλουθες IPv4 διευθύνσεις 147.102.1.1, 147.102.7.1 ή 147.102.40.1. Αφού τελειώσει η καταγραφή εφαρμόστε φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα ARP και ICMP.

2.1 Καταγράψτε τις διευθύνσεις IPv4 που περιέχει ο πίνακας arp μετά την παραπάνω καταγραφή.
2.2 Επιλέξτε ένα μήνυμα ICMP *Echo request*. Καταγράψτε τη διεύθυνση MAC του αποστολέα και του παραλήπτη του αντίστοιχου πλαισίου.
2.3 Καταγράψτε τις διευθύνσεις IPv4 (αποστολέα και παραλήπτη) του πακέτου IPv4 που μεταφέρει το μήνυμα ICMP *Echo request*;
2.4 Οι παραπάνω διευθύνσεις MAC σε ποιες διευθύνσεις IPv4 αντιστοιχούν;

2.5 Παρατηρήσατε πακέτα πρωτοκόλλου ARP κατά την καταγραφή;
2.6 Αν ναι, ποιος ήταν ο σκοπός τους; Εάν όχι, αιτιολογήστε γιατί δεν υπήρξαν.

Αφού απενεργοποιήσετε το προηγούμενο φίλτρο απεικόνισης, εφαρμόστε ένα νέο φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο μηνύματα ICMP *Echo reply*.

2.7 Να καταγραφεί η σύνταξη του. *[Υπόδειξη: Συμβουλευτείτε τις απαντήσεις σας στις ερωτήσεις 1.11 και 1.12]*
2.8 Παρατηρώντας τις τιμές των πεδίων της επικεφαλίδας των πακέτων IPv4 που μεταφέρουν το μήνυμα ICMP *Echo reply*, εξηγήστε πώς προκύπτει η τιμή της παραμέτρου TTL που εμφανίζεται στις απαντήσεις του παραθύρου εντολών.

Ξεκινήστε μια νέα καταγραφή με το προηγούμενο φίλτρο σύλληψης, όταν εκτελείτε την εντολή ping σε έναν υπολογιστή **εκτός του υποδικτύου σας**, που δεν είναι ενεργός (π.χ. στον 147.102.7.45). Όταν τελειώσει η καταγραφή εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

2.9 Ποιοι τύποι μηνυμάτων ICMP εμφανίζονται;
2.10 Σε τι διαφέρει η κίνηση που καταγράψατε σε σχέση με την αντίστοιχη όταν εκτελέσατε την προηγουμένως ping προς μια διεύθυνση IPv4 εντός του υποδικτύου σας, που δεν αντιστοιχεί σε ενεργό υπολογιστή. Αιτιολογήστε τη διαφορά.

3 Εντολή tracert/traceroute

Στην Εργαστηριακή Άσκηση 5 είδατε πώς μπορείτε να βρείτε τη διαδρομή που ακολουθεί ένα πακέτο στο διαδίκτυο με την εντολή tracert ή traceroute. Εδώ θα εξετάσετε με περισσότερη λεπτομέρεια τα ICMP μηνύματα λαθών. Ιστορικά, τα ICMP μηνύματα λάθους επέστρεφαν την επικεφαλίδα IPv4 του πακέτου που τα προκάλεσε μαζί με τα πρώτα 8 byte δεδομένων του. Αργότερα θεσπίστηκαν νέοι κανόνες ώστε να περιλαμβάνεται το περισσότερο δυνατό από το αρχικό πακέτο, χωρίς το μήκος του πακέτου ICMP να ξεπερνά τα 576 byte (το επίσημο μήκος πακέτου στο Internet). Τέλος, στο RFC 4884 προστέθηκε ένα πεδίο 8 bit που δείχνει το μήκος του αρχικού πακέτου σε λέξεις των 32 bit.

Ξεκινήστε μια νέα καταγραφή της δικτυακής κίνησης με φίλτρο σύλληψης ώστε να συλλαμβάνετε μόνο πακέτα IPv4 που περιέχουν την IPv4 διεύθυνση του υπολογιστή σας. Σε παράθυρο εντολών εκτελέστε την εντολή tracert ή traceroute με προορισμό το μηχάνημα με IPv4 διεύθυνση 147.102.40.15. Στην περίπτωση της traceroute χρησιμοποιήστε στην κατάλληλη σύνταξη ώστε να παραχθούν μηνύματα ICMP *Echo request*. Όταν τελειώσει η εκτέλεση της εντολής σταματήστε την καταγραφή και εφαρμόστε φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

3.1 Ποιο είναι το μήκος και το περιεχόμενο του πεδίου δεδομένων των μηνυμάτων ICMP *Echo request* που παράγει η εντολή tracert ή traceroute;
3.2 Συγκρίνετε το παραπάνω μήκος και περιεχόμενο του πεδίου δεδομένων με τα αντίστοιχα στην περίπτωση της εντολής ping (Ερώτηση 1.9);
3.3 Ποιο ICMP μήνυμα λάθους παρατηρείτε στις απαντήσεις των ενδιάμεσων κόμβων (πριν τον 147.102.40.15);
3.4 Ποια είναι η τιμή των πεδίων τύπου (Type) και κωδικού (Code) της επικεφαλίδας ICMP για το προηγούμενο μήνυμα λάθους;
3.5 Ποια άλλα πεδία έχει η επικεφαλίδα του μηνύματος λάθους πριν τα δεδομένα και ποιο το μέγεθός τους;
3.6 Ποιο είναι το μήκος της επικεφαλίδας και ποιο των δεδομένων του ICMP μηνύματος λάθους της ερώτησης 3.3;
3.7 Τι είναι το περιεχόμενο του πεδίου δεδομένων του προηγούμενου ICMP μηνύματος λάθους και ποια η σχέση του με το πακέτο IPv4 εξ αιτίας του οποίου παράχθηκε; *[Υπόδειξη: Συμβουλευθείτε την παράγραφο 4.2 του RFC 4884.]*

4 Ανακάλυψη MTU διαδρομής(Path MTU Discovery)

Ο σκοπός της διαδικασίας ανακάλυψης MTU διαδρομής είναι να αποφευχθεί ο αχρείαστος θρυμματισμός κατά την επικοινωνία δύο κόμβων, ειδικά στην περίπτωση συνδέσεων TCP, όπου υφίσταται ένας παρόμοιος του θρυμματισμού μηχανισμός, γνωστός ως τεμαχισμός (segmentation). Προς τούτο αποστέλλονται πακέτα IPv4 με ενεργοποιημένη τη σημαία μη θρυμματισμού (*Don't fragment flag*), όπως κάνετε στην Εργαστηριακή Άσκηση 4. Αν κάποιος υπολογιστής ή δρομολογητής δεν μπορεί να προωθήσει χωρίς θρυμματισμό ένα τέτοιο πακέτο IPv4, οφείλει να στείλει στην πηγή ένα ICMP μήνυμα λάθους τύπου *Destination Unreachable,* υποπερίπτωση *Fragmentation needed,* δηλώνοντας την τιμή της MTU της απερχόμενης ζεύξης. Ο έλεγχος αυτός γίνεται εύκολα γιατί κάθε πρωτόκολλο στρώματος ζεύξης δεδομένων έχει ένα συγκεκριμένο μέγεθος μέγιστου πλαισίου, π.χ. 1.518 byte για το Ethernet. Έτσι δεν υπάρχει λόγος να γίνει διεξοδικό ψάξιμο, αρκεί να αναζητηθούν τα συνήθη μεγέθη MTU, όπως 1500, 1492, 1006, 576, 552, 544, 512, 508 και 296. Με τον τρόπο αυτό οι υπολογιστές και οι δρομολογητές μπορούν να εντοπίσουν τη **μέγιστη** MTU για την οποία δεν εμφανίζεται θρυμματισμός (ισοδύναμα τη ζεύξη με τη μικρότερη MTU κατά μήκος της διαδρομής).

Θα βρείτε τώρα την MTU της διαδρομής από τον υπολογιστή σας προς τον edu-dy.cn.ntua.gr. Προς τούτο ξεκινήστε μια νέα καταγραφή με φίλτρο σύλληψης ώστε να συλλαμβάνετε μόνο μηνύματα ICMP και μετά εκτελέστε διαδοχικά την εντολή ping στέλνοντας **χωρίς** θρυμματισμό **ένα** μόνο πακέτο για τιμές μεγέθους δεδομένων ICMP σύμφωνες με τις συνήθεις τιμές MTU που δίδονται πιο πάνω, ξεκινώντας από τη μεγαλύτερη προς τη μικρότερη. Σταματήστε τα ping και την καταγραφή όταν λάβετε επιτυχή απάντηση από το 147.102.40.15.

4.1. Ποιες τιμές μήκους δεδομένων ICMP χρησιμοποιήσατε για να παράγετε πακέτα IPv4 με μήκος τις επιθυμητές τιμές MTU;
4.2. Παρατηρήσατε μήνυμα λάθους ICMP *Destination Unreachable*;
4.3. Εάν ναι, ποιος κόμβος της διαδρομής το παρήγαγε;
4.4. Εάν το παρατηρήσατε, καταγράψτε την τιμή των πεδίων Type και Code της επικεφαλίδας του ICMP *Destination Unreachable*. Εάν όχι, χρησιμοποιήστε για αυτή και τις επόμενες δύο ερωτήσεις την καταγραφή στο αρχείο mtu.pcap που θα βρείτε στην ιστοσελίδα του μαθήματος.
4.5. Στο προηγούμενο μήνυμα, ποιο πεδίο δηλώνει ότι το λάθος οφείλεται στην απαίτηση μη θρυμματισμού του πακέτου IPv4 και ποια τιμή έχει η επικεφαλίδα Next-Hop MTU;
4.6. Για το προηγούμενο μήνυμα, τι περιέχει το πεδίο των δεδομένων;
4.7. Ποια είναι 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;
4.8. Για ποιες άλλες τιμές MTU δεν απαντά το 147.102.40.15;
4.9. Ποια είναι η τιμή MTU για την οποία λαμβάνετε απάντηση από το 147.102.40.15;
4.10. Είναι αυτή η MTU της δικτυακής διεπαφής του 147.102.40.15 ή κάποιου άλλου ενδιάμεσου κόμβου; Γιατί; *[Υπόδειξη: Δείτε παράγραφο 4 στο RFC 1191.]*
4.11. Για ποιο λόγο νομίζετε ότι το 147.102.40.15 δεν παράγει ICMP *Destination Unreachable* όταν λαμβάνει πακέτα IPv4 μεγέθους μεγαλύτερου από την MTU της διεπαφής του;

Ξεκινήστε μια νέα καταγραφή και κάντε ping στο 147.102.40.15 στέλνοντας **ένα** μόνο πακέτο ICMP μεγέθους αντίστοιχου της MTU της ερώτησης 4.7 **χωρίς** την απαίτηση μη θρυμματισμού. **Προσοχή**, σε περιβάλλον Linux πρέπει να δηλωθεί ρητά.

4.12. Καταγράψτε το μέγεθος του πρώτου θραύσματος που λαμβάνει ο υπολογιστής σας. Είναι το ίδιο με την MTU που προσδιορίσατε προηγουμένως; Γιατί; *[Υπόδειξη: Αναζητείστε Fragmentation στην ιστοσελίδα https://en.wikipedia.org/wiki/IPv4.]*

5 Απρόσιτη θύρα (Port Unreachable)

Ένα άλλο συνηθισμένο ICMP μήνυμα λάθους είναι το ICMP *Destination Unreachable*, αυτό της απρόσιτης θύρας,. Τυπικά παράγεται όταν ένα πρόγραμμα πελάτης προσπαθεί να επικοινωνήσει με κάποιον εξυπηρετητή, αλλά δεν υπάρχει διεργασία που να ακούει στη συγκεκριμένη θύρα, π.χ. στη θύρα 80 για εξυπηρετητές ιστού ή στη θύρα 53 για εξυπηρετητές DNS.

Ξεκινήστε μια καταγραφή με φίλτρο ώστε να συλλαμβάνετε μόνο πακέτα IPv4 από και προς το μηχάνημα με IPv4 διεύθυνση 147.102.40.15. Στη συνέχεια τρέξτε το πρόγραμμα nslookup σε περιβάλλον Windows, dig σε περιβάλλον Linux ή host σε περιβάλλον Unix, για να ζητήσετε από τον εξυπηρετητή DNS 147.102.40.15 τη διεύθυνση IPv4 του edu-dy.cn.ntua.gr.

5.1 Ποιο φίλτρο σύλληψης χρησιμοποιήσατε;
5.2 Ποια η ακριβής σύνταξη της εντολής nslookup, dig ή host που χρησιμοποιήσατε;
5.3 Λάβατε κάποια απάντηση στο παράθυρο εντολών; Ποιο το νόημά της;
5.4 Παρατηρήσατε μηνύματα DNS στην καταγραφή;
5.5 Ποιο είναι το πρωτόκολλο μεταφοράς και ποια είναι η θύρα προορισμού τους;
5.6 Παρατηρήσατε μηνύματα λάθους ICMP *Destination Unreachable* με πηγή το 147.102.40.15;
5.7 Καταγράψτε την τιμή των πεδίων Type και Code της επικεφαλίδας των.
5.8 Ποιο πεδίο δηλώνει ότι ο λόγος αποτυχίας είναι κάποια απρόσιτη θύρα;
5.9 Πώς προκύπτει ότι πρόκειται για τη θύρα προορισμού των μηνυμάτων DNS;

Στα συστήματα Unix/Linux η εντολή traceroute παράγει εξ ορισμού μηνύματα UDP με θύρες προορισμού στην περιοχή από 33434 έως 33534, αντί μηνυμάτων ICMP.

5.10 Όταν αυτά φτάνουν στον προορισμό τους με ποιο μήνυμα ICMP απαντά αυτός;

6 IPv6 και ICMPv6

Στη χρήση των εντολών ping και tracert/traceroute που κάνατε μέχρι τώρα δόθηκε προσοχή να παράγετε πακέτα IPv4 και να παρατηρείτε ICMP μηνύματα ερωτημάτων ή λαθών. Στα τρέχοντα όμως λειτουργικά συστήματα υποστηρίζεται και η έκδοση 6 του πρωτοκόλλου IP, γνωστή ως IPv6. Στο IPv6 η βασική αλλαγή είναι ότι η επικεφαλίδα του πακέτου IP έχει πλέον σταθερό μήκος και απλούστερη δομή. Ταυτόχρονα το μήκος των αντίστοιχων διευθύνσεων μεγάλωσε από 4 byte σε 16 byte ώστε να αντιμετωπιστεί το πρόβλημα έλλειψης διευθύνσεων IPv4. Παράλληλα, όμως άλλαξε ο τρόπος λειτουργίας του ICMP. Το ICMPv6, το αντίστοιχο με το ICMP πρωτόκολλο, προσφέρει ανάλογες λειτουργίες και αντικαθιστά το ARP όσον αφορά το θέμα της ανεύρεσης γειτόνων. Στο μέρος αυτό της άσκησης θα δείτε τις λεπτομέρειες της επικεφαλίδας του IPv6 και των μηνυμάτων ICMPv6 που παράγονται από τις εντολές ping και tracert/traceroute.

Για τη συνέχεια, εάν ο υπολογιστής σας ή το δίκτυο που χρησιμοποιείτε δεν υποστηρίζει το πρωτόκολλο IPv6, θα χρησιμοποιήσετε την καταγραφή στο αρχείο icmpv6.pcap που θα βρείτε στην ιστοσελίδα του μαθήματος.

Ξεκινήστε μια νέα καταγραφή με φίλτρο ώστε να συλλαμβάνετε μόνο πακέτα IPv6. Στη συνέχεια κάντε ping προς το μηχάνημα με IPv6 διεύθυνση 2001:648:2000:329::101 και μετά tracert ή traceroute στην ίδια διεύθυνση. Στην περίπτωση της traceroute σιγουρευτείτε ότι χρησιμοποιήσατε την κατάλληλη παράμετρο ώστε να παραχθούν πακέτα ICMPv6, αντί UDP. Περιμένετε να ολοκληρωθεί η εκτέλεση των εντολών, σταματήστε την καταγραφή και εφαρμόστε φίλτρο ώστε να παρατηρείτε μόνο μηνύματα ICMPv6.

6.1 Ποια είναι η σύνταξη των ping, tracert ή traceroute που χρησιμοποιήσατε;
6.2 Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε και ποια του φίλτρου απεικόνισης;
6.3 Τι τιμή έχει το πεδίο Type της επικεφαλίδας Ethernet όταν μεταφέρονται πακέτα IPv6;
6.4 Ποιο είναι το μήκος επικεφαλίδας των πακέτων IPv6;

6.5 Καταγράψτε τα ονόματα και το μήκος σε byte των πεδίων της επικεφαλίδας του μηνύματος IPv6 και σημειώστε στο σχήμα τις θέσεις τους.
6.6 Ποια επικεφαλίδα είναι η αντίστοιχη της TTL των πακέτων IPv4;
6.7 Ποια επικεφαλίδα δείχνει το πρωτόκολλο τα δεδομένα του οποίου μεταφέρει το πακέτο IPv6 και ποια η τιμή της για το ICMPv6;
6.8 Εντοπίστε ένα μήνυμα ICMPv6 *Echo request* που να έχει παραχθεί από την εντολή ping. Είναι η δομή της επικεφαλίδας του ίδια με αυτήν που βρήκατε προηγουμένως για το ICMP *Echo request* στην ερώτηση 1.6;
6.9 Ποια η τιμή του πεδίου Type και ποιο το μήκος δεδομένων που μεταφέρει το ICMP *Echo request*;
6.10 Εντοπίστε το μήνυμα ICMPv6 *Echo reply* που παράχθηκε σε απάντηση του προηγούμενου ICMPv6 *Echo request.* Είναι η δομή της επικεφαλίδας του ίδια με αυτήν του ICMPv6 *Echo request*;
6.11 Ποια η τιμή του πεδίου Type και ποιο το μήκος δεδομένων που μεταφέρει το ICMPv6 *Echo reply*;
6.12 Εντοπίστε ένα μήνυμα ICMPv6 *Echo request* που να έχει παραχθεί από την εντολή tracert ή traceroute. Σε τι διαφέρει από το αντίστοιχο που παράγει η εντολή ping;
6.13 Εντοπίστε ένα μήνυμα λάθους ICMPv6 *Time exceeded.* Είναι η δομή της επικεφαλίδας του ίδια με αυτήν που βρήκατε προηγουμένως για το ICMP *Time exceeded* στις ερωτήσεις 3.4 και 3.5;
6.14 Ποια η τιμή του πεδίου Type και ποιο το μήκος δεδομένων που μεταφέρει το ICMPv6 *Time exceeded*;
6.15 Τι περιέχει το πεδίο δεδομένων του;
6.16 Παρατηρήσατε άλλα ICMPv6 μηνύματα; Εάν ναι, τι είδους είναι;
6.17 Ποια η τιμή του πεδίου Type και ποιο το μήκος αυτών των μηνυμάτων ICMPv6;

Ονοματεπώνυμο: Νικόλας Μπέλλος (el18183)		Ομάδα: 3
Όνομα PC/ΛΣ: BELLOS-DELL-G3 / Windows OS		Ημερομηνία: 29 / 11 / 2021
Διεύθυνση IP: 192 . 168 . 1 . 8	Διεύθυνση MAC:	7C - 2A - 31 - 40 - C9 - AF

Εργαστηριακή Άσκηση 6
Πρωτόκολλο ICMP

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

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

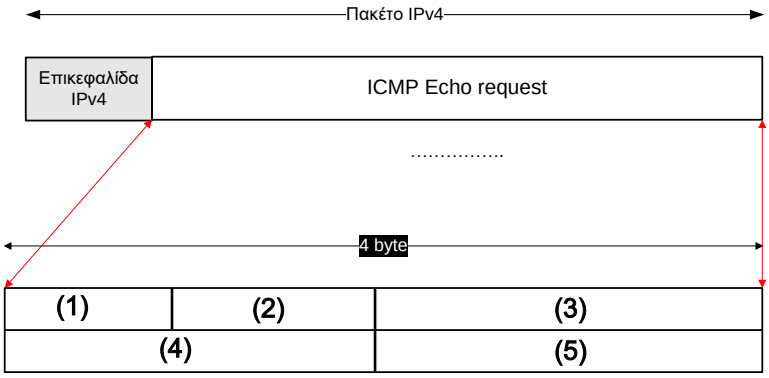
1.2 Display filter : arp or icmp

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 Type: 8 (Echo (ping) request) → 08 HEX

Code: 0 → 00 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.

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.

2

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.

3

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)

4

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.

5

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

6

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

(σημειώστε θέσεις στο σχήμα στην επόμενη σελίδα)

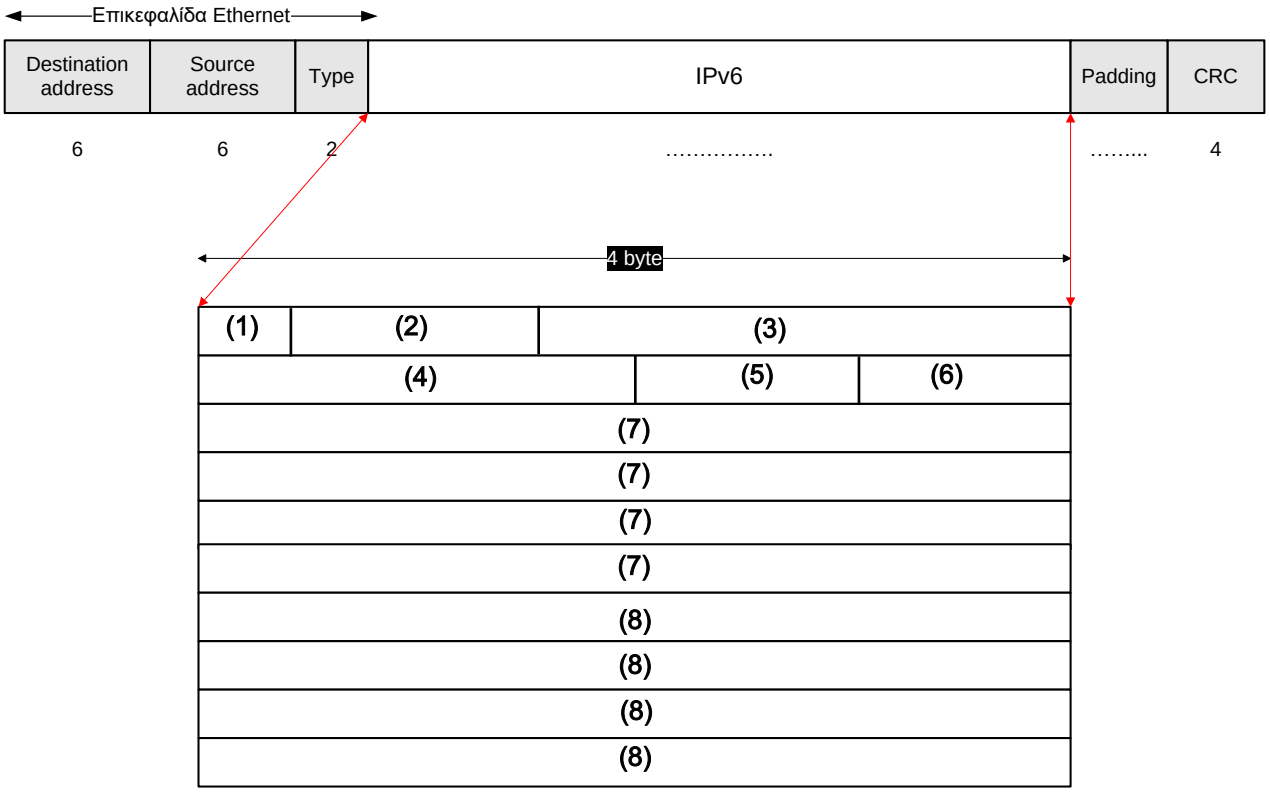
6.6 H Hop Limit

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.