Εργαστήριο «Δίκτυα Υπολογιστών Ι»

Άσκηση 2η
Τμήμα Μηχ. Πληροφορικής & Υπολογιστών
Παν. Δυτικής Αττικής
Ημερομηνία έκδοσης: 3/10/2018

Επιμέλεια: Αντώνης Μπόγρης, Ιωάννης Ξυδάς

Μελέτη βασικών στοιχείων Ethernet - IP

Στόχοι της άσκησης:

- Η μελέτη των ιδιοτήτων των στοιχείων ενός δικτύου βασισμένου σε τεχνολογία TCP/IP με Ethernet.
- Ανάλυση της λειτουργίας του με τη βοήθεια του λογισμικού Wireshark και εντολών από τη γραμμή εντολής.

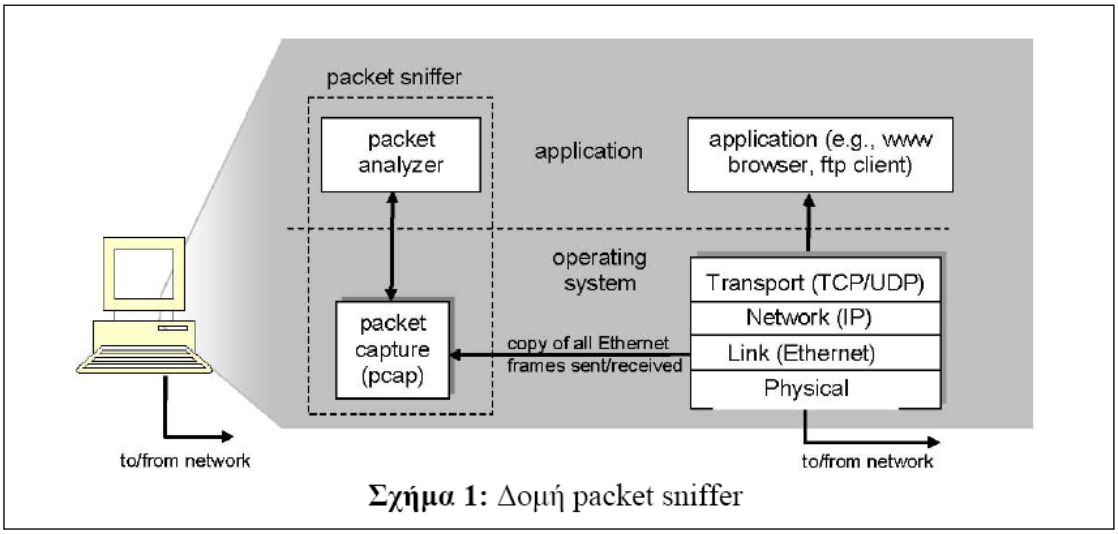
Διαθέσιμα:

- Σταθμοί δικτύου - οι υπολογιστές του εργαστηρίου.
- Καλώδια δικτύου UTP.
- Το λογισμικό Wireshark

Γενικά στοιχεία για το Wireshark

Το βασικό εργαλείο για την παρατήρηση των μηνυμάτων που ανταλλάσσονται μεταξύ των εκτελούμενων οντοτήτων πρωτοκόλλων καλείται packet sniffer. Όπως υπονοεί και το όνομα, ο packet sniffer συλλαμβάνει (“sniffs”) τα μηνύματα τα οποία στέλνονται ή λαμβάνονται από τον υπολογιστή. Επίσης, ο packet sniffer συνήθως αποθηκεύει και απεικονίζει τα περιεχόμενα διαφόρων πεδίων πρωτοκόλλων που περιέχονται στα μηνύματα που συλλαμβάνονται. Ο ίδιος ο packet sniffer είναι παθητικός. Παρατηρεί τα μηνύματα που στέλνονται και λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που εκτελούνται στον υπολογιστή αλλά ο ίδιος δεν στέλνει ποτέ πακέτα. Παρόμοια, τα λαμβανόμενα πακέτα δεν απευθύνονται ποτέ με ρητό τρόπο στον packet sniffer. Αντίθετα, ο packet sniffer λαμβάνει ένα αντίγραφο των πακέτων που στέλνονται ή λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που εκτελούνται στον υπολογιστή.

Στο Σχήμα 1 φαίνεται η δομή ενός packet sniffer.



Σχήμα 1: Δομή packet sniffer

Στο δεξί μέρος του Σχήματος 1 φαίνονται τα πρωτόκολλα (στην προκειμένη περίπτωση τα πρωτόκολλα του Διαδικτύου) και οι εφαρμογές (όπως ένας web browser ή ένας ftp client) που τρέχουν κανονικά στον υπολογιστή. Ο packet sniffer, ο οποίος φαίνεται μέσα στο παραλληλόγραμμο διακεκομμένων γραμμών του Σχήματος 1, είναι μία προσθήκη στο σύνηθες λογισμικό του υπολογιστή και αποτελείται από δύο μέρη. Η βιβλιοθήκη σύλληψης πακέτων (packet capture library) λαμβάνει ένα αντίγραφο κάθε πλαισίου επιπέδου ζεύξης που στέλνεται ή λαμβάνεται από τον υπολογιστή σας. Υπενθυμίζεται ότι τα μηνύματα που ανταλλάσσονται από τα πρωτόκολλα ανώτερων επιπέδων, όπως το HTTP, FTP, TCP, UDP ή το IP, τελικά ενθυλακώνονται όλα μέσα σε πλαίσια επιπέδου ζεύξης τα οποία μεταδίδονται μέσω φυσικών μέσων όπως ένα καλώδιο Ethernet. Επομένως, η σύλληψη όλων των πλαισίων επιπέδου ζεύξης σας παρέχει όλα τα μηνύματα που στέλνονται και λαμβάνονται από όλα τα πρωτόκολλα και όλες τις εφαρμογές που εκτελούνται στον υπολογιστή σας.

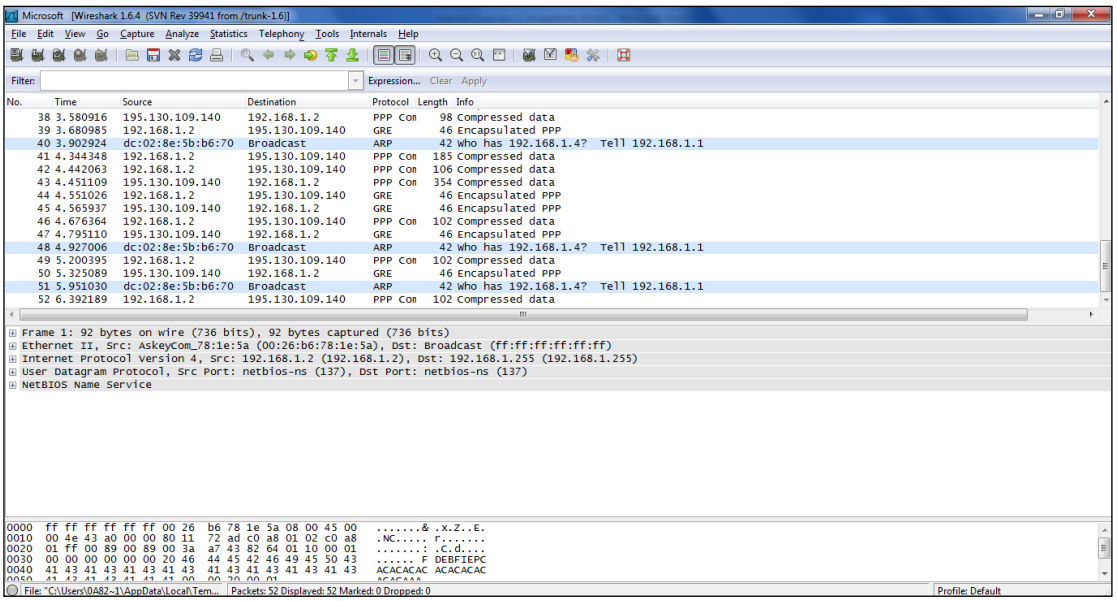
Το δεύτερο συστατικό στοιχείο ενός packet sniffer είναι ο αναλυτής πακέτων (packet analyzer), ο οποίος απεικονίζει το περιεχόμενο όλων των πεδίων στο μήνυμα ενός πρωτοκόλλου. Για να το πετύχει αυτό, ο αναλυτής πακέτων πρέπει να "καταλαβαίνει" τη δομή όλων των μηνυμάτων που ανταλλάσσονται από τα πρωτόκολλα. Για παράδειγμα, έστω ότι ενδιαφερόμαστε να απεικονίσουμε τα διάφορα πεδία των μηνυμάτων που ανταλλάσσονται από το πρωτόκολλο HTTP στο Σχήμα 1. Ο αναλυτής πακέτων καταλαβαίνει τη μορφή των πλαισίων Ethernet και επομένως μπορεί να αναγνωρίσει ένα αυτοδύναμο πακέτο IP (IP datagram) μέσα σε ένα πλαίσιο Ethernet. Επίσης, καταλαβαίνει τη μορφή ενός IP datagram, ώστε να είναι σε θέση να εξάγει ένα TCP segment που περιέχεται μέσα σε ένα IP datagram. Επιπλέον, καταλαβαίνει τη δομή ενός TCP segment οπότε μπορεί να εξάγει το μήνυμα HTTP που περιέχεται στο TCP segment. Τέλος, καταλαβαίνει το πρωτόκολλο HTTP και έτσι, για παράδειγμα, γνωρίζει ότι τα πρώτα bytes ενός μηνύματος HTTP θα περιέχουν τις ακολουθίες χαρακτήρων "GET", "POST" ή "HEAD".

Στα εργαστήρια αυτά θα χρησιμοποιήσουμε τον packet sniffer Wireshark http://www.wireshark.org), ο οποίος θα μας δώσει τη δυνατότητα να απεικονίσουμε τα περιεχόμενα των μηνυμάτων που στέλνονται ή λαμβάνονται από τα πρωτόκολλα σε διαφορετικά επίπεδα της στοίβας πρωτοκόλλων. (Σε τεχνική γλώσσα, το Wireshark είναι ένας αναλυτής πακέτων που χρησιμοποιεί μία βιβλιοθήκη σύλληψης πακέτων στον υπολογιστή σας.) Το Wireshark λειτουργεί σε υπολογιστές που για τη διασύνδεση τους με το διαδίκτυο χρησιμοποιούν το πρωτόκολλο Ethernet, καθώς επίσης σε υπολογιστές που

χρησιμοποιούν τα λεγόμενα πρωτόκολλα σημείου-προς-σημείο όπως το PPP (π.χ. xDSL τεχνολογίες).

Εκτέλεση του Wireshark

Κατά την εκτέλεση του προγράμματος Wireshark εμφανίζεται στην οθόνη η γραφική διεπαφή χρήστη (graphical user interface, GUI) του Wireshark που φαίνεται στο Σχήμα 2. Αρχικά, τα διάφορα παράθυρα δεν περιέχουν δεδομένα. Η διεπαφή του Wireshark περιλαμβάνει πέντε κύρια συστατικά στοιχεία:



Σχήμα 2: Γραφική Διεπαφή Χρήστη (Graphical User Interface) του Wireshark

- Τα μενού των εντολών (command menus) είναι συνηθισμένα μενού που βρίσκονται στο επάνω μέρος του παραθύρου. Προς το παρόν μας ενδιαφέρουν τα μενού File και Capture. Το μενού File επιτρέπει την αποθήκευση δεδομένων για πακέτα που έχουν συλληφθεί ή το άνοιγμα ενός αρχείου που περιέχει δεδομένα πακέτων που είχαν συλληφθεί προηγουμένως και την έξοδο από το Wireshark. Το μενού Capture επιτρέπει να ξεκινήσετε τη σύλληψη πακέτων. Για ευκολία ο συνδυασμός CTRL-E αρχίζει/σταματά την καταγραφή της κίνησης.
- Το πάνω παράθυρο καταλόγου πακέτων (packet-listing window) παρουσιάζει μία περίληψη της μιας γραμμής για κάθε πακέτο που συλλαμβάνεται η οποία περιλαμβάνει τον αριθμό πακέτου (πρόκειται για αριθμό που απονέμεται από το Wireshark και όχι για έναν αριθμό πακέτου που περιέχεται στην επικεφαλίδα οποιουδήποτε πρωτοκόλλου), τον χρόνο σύλληψης του πακέτου, τις διευθύνσεις πηγής και προορισμού του πακέτου, το είδος του πρωτοκόλλου και πληροφορία σχετική με το πρωτόκολλο η οποία περιέχεται στο πακέτο. Ο κατάλογος των πακέτων μπορεί να ταξινομηθεί σύμφωνα με οποιαδήποτε από αυτές τις κατηγορίες κάνοντας κλικ στο όνομα της αντίστοιχης στήλης. Στο πεδίο είδος πρωτοκόλλου (protocol type) αναφέρεται το ανωτάτου επιπέδου πρωτόκολλο το οποίο έστειλε ή έλαβε ένα πακέτο, δηλαδή, το πρωτόκολλο που είναι η πηγή ή ο τελικός αποδέκτης αυτού του πακέτου.

- Το μεσαίο παράθυρο λεπτομερειών επικεφαλίδας πακέτου (packet-header details window) παρέχει λεπτομέρειες σχετικά με το επιλεγμένο στο παράθυρο packet-listing πακέτο. (Για να επιλέξετε ένα από τα πακέτα του παραθύρου packet-listing, τοποθετείστε τον cursor πάνω από την μιας-γραμμής περίληψη του πακέτου στο παράθυρο packet-listing και κάντε αριστερό κλικ). Οι λεπτομέρειες αυτές περιλαμβάνουν πληροφορίες σχετικά με το πλαίσιο Ethernet και το IP datagram που περιέχουν αυτό το πακέτο. Το ποσό των λεπτομερειών που παρουσιάζεται για το Ethernet και το επίπεδο IP μπορεί να επεκταθεί ή να ελαχιστοποιηθεί κάνοντας κλικ στο βέλος που δείχνει δεξιά ή προς τα κάτω και βρίσκεται στα αριστερά της γραμμής του πλαισίου Ethernet ή του IP datagram στο παράθυρο packetheader details. Εάν το πακέτο έχει μεταφερθεί με TCP ή UDP, θα παρουσιαστούν και οι λεπτομέρειες που αφορούν το TCP ή το UDP, οι οποίες μπορούν να επεκταθούν ή να ελαχιστοποιηθούν με παρόμοιο τρόπο. Τέλος, λεπτομέρειες παρέχονται επίσης για το ανωτάτου επιπέδου πρωτόκολλο το οποίο έστειλε ή έλαβε αυτό το πακέτο.
- Το κάτω παράθυρο περιεχομένων πακέτου (packet-contents window) παρουσιάζει ολόκληρο το περιεχόμενο ενός συλλαμβανόμενου πλαισίου και σε μορφή ASCII και σε δεκαεξαδική μορφή.
- Προς το επάνω μέρος της διεπαφής Wireshark βρίσκεται το πεδίο του φίλτρου παρουσίασης πακέτων (packet display filter field) στο οποίο μπορούμε να εισάγουμε την IP διεύθυνση του Η/Υ μας ή το όνομα ενός πρωτοκόλλου ή άλλη πληροφορία έτσι ώστε να φιλτράρουμε την πληροφορία που παρουσιάζεται στο παράθυρο packet-listing (και επομένως στα παράθυρα packetheader και packet-contents). Στο παράδειγμα που ακολουθεί θα χρησιμοποιήσουμε το πεδίο packet display filter ώστε να κάνουμε το Wireshark να κρύψει (να μην παρουσιάσει) όλα τα πακέτα εκτός από εκείνα που αντιστοιχούν σε μηνύματα HTTP.

Δραστηριότητες- Ασκήσεις

Βήμα 1^{ο}: Εύρεση στοιχείων κάρτας δικτύου

Χρησιμοποιώντας τις ρυθμίσεις δικτύου στον πίνακα ελέγχου βρείτε και καταγράψτε:

1. Την ονομασία της κάρτας δικτύωσης (network adapter)
2. Την ταχύτητα σύνδεσης.
3. Τη διεύθυνση υποστρώματος MAC σε δεκαεξαδική μορφή.
4. Τον κατασκευαστή της κάρτας δικτύου.

Βήμα 2^{ο}: Διαγνωστικές εντολές δικτύου (πρωτόκολλο TCP/IP)

Στη συνέχεια να αναζητήσετε διάφορα στοιχεία σχετικά με τις παραμέτρους δικτύωσης του υπολογιστή σας μέσω εντολών φλοιού. Χρήσιμες τέτοιες εντολές φλοιού είναι οι hostname, ipconfig, net, netstat και route (ανατρέξτε στο συνοδευτικό φυλλάδιο **Net_Commands.pdf** που περιέχει τις εντολές και τη χρήση τους). Για την εκτέλεσή τους ανοίξτε ένα παράθυρο εντολών (command prompt), πηγαίνετε στο *Start, Run* και αφού γράψετε την εντολή cmd, πιέστε το πλήκτρο *Enter*. Για να βρείτε πληροφορίες σχετικά με αυτές γράψτε την εντολή ακολουθούμενη από /? ή -? και πιέστε το πλήκτρο *Enter*.

Εάν το κείμενο δεν χωρά στην οθόνη προσθέστε το | more είτε μετακινήσετε τη δεξιά μπάρα (ή χρησιμοποιήστε τον τροχό του ποντικιού) για να εμφανισθεί το μέρος του παραθύρου που δεν είναι ορατό. Αφού μελετήσετε το help για τις εντολές ipconfig, ping, pathping, tracert, hostname, route, arp, getmac, netstat, net, δίνοντας έμφαση στις επιλογές view και config της τελευταίας, να απαντήσετε στα ακόλουθα ερωτήματα και να καταγράψετε μαζί με την απάντηση την ακριβή σύνταξη της εντολής που χρησιμοποιήθηκε:

1. Το όνομα του υπολογιστή σας.
2. Την περιοχή (Workstation domain) που ανήκει ο υπολογιστής σας.
3. Τη διεύθυνση IP του υπολογιστή σας.
4. Τη φυσική διεύθυνση MAC.
5. Τη μάσκα του υποδικτύου.
6. Τη διεύθυνση IP της προκαθορισμένης πύλης (default gateway).
7. Τη διεύθυνση IP του εξυπηρετητή DHCP και τη διάρκεια της περιόδου απονομής (lease).

Βήμα 3^{ο}: Εξάσκηση με το wireshark

Επισκεφτείτε με τον Internet Explorer την ακόλουθη ιστοσελίδα: http://www.uniwa.gr/ και μόλις φορτωθεί πλήρως η σελίδα σταματήστε την καταγραφή. Στο κύριο παράθυρο του Wireshark, όπου φαίνεται η καταγεγραμμένη δικτυακή κίνηση, μπορεί ενδεχομένως να παρατηρήσετε κίνηση που δε σχετίζεται με την επίσκεψη της ιστοσελίδας. Η ζητούμενη κίνηση μπορεί να απομονωθεί με την εφαρμογή φίλτρου παρατήρησης ως εξής: πηγαίνετε *Analyze, Display Filters…* και πατήστε το πλήκτρο *Expression*. Από το πεδίο *Field name* βρείτε την επιλογή IP, πατήστε το +, διαλέγετε την επιλογή *ip.addr*, από το πεδίο *Relation* διαλέξτε το ==, στο πεδίο *Value (IPv4 address)* πληκτρολογήστε την IP διεύθυνση του www.uniwa.gr και πατήστε *OK*. Το φίλτρο ενεργοποιείται με το πάτημα του *Apply*.

Κλείνοντας το παράθυρο διαλόγου (με OK) θα διαπιστώσετε ότι η κίνηση είναι ενδεχομένως περιορισμένη σε σχέση με την παρατήρηση χωρίς φίλτρο. Στη λίστα των καταγεγραμμένων πακέτων, και κάτω από την επικεφαλίδα Protocol, εμφανίζεται το εκάστοτε πρωτόκολλο υψηλότερου επιπέδου που περιέχει το πλαίσιο. Εντοπίστε το πρώτο μήνυμα HTTP GET που έστειλε ο υπολογιστής σας για να κατεβάσει τη σελίδα και την αντίστοιχη απόκριση HTTP του εξυπηρετητή. Με βάση τα στοιχεία της καταγραφής σας απαντήστε τις επόμενες ερωτήσεις.

1. Ποια είναι η διεύθυνση IP του www.uniwa.gr;
2. Ποια είναι η διεύθυνση IP του υπολογιστή σας;
3. Ποια είναι η διεύθυνση MAC του υπολογιστή σας σε δεκαεξαδική μορφή;
4. Ποιος είναι ο κατασκευαστής της κάρτας δικτύου;
5. Να καταγράψετε τα πρωτόκολλα που παρατηρείτε ότι χρησιμοποιούνται για την επικοινωνία με την ιστοσελίδα.

Για τα 3 και 4 ελέγξτε αν οι απαντήσεις συμπίπτουν με αυτές προηγούμενων ερωτημάτων.

Βήμα 4^{ο} : Αποσαφήνιση των εννοιών τοπικού δικτύου – εξωτερικού δικτύου και του ρόλου της δικτυακής πύλης

Η εντολή ping έχει χαρακτήρα ελεγκτικό και εξετάζει αν υφίσταται επικοινωνία μεταξύ δύο διεπαφών δικτύου. Η εντολή ping ελέγχει βασικά εάν κάποιος κόμβος (ή ακριβέστερα η διεπαφή (interface) του κόμβου) ενός δικτύου IP είναι ενεργός (alive ή up). Το ping χρησιμοποιεί το πρωτόκολλο ICMP (Internet Control Message Protocol) για να στείλει ένα μήνυμα Αίτησης Ηχούς (Echo Request), έτσι ώστε να λάβει μια Απάντηση Ηχούς (Echo Reply) από τον συγκεκριμένο κόμβο. Για τη μεταφορά του πάνω από το δίκτυο, το μήνυμα ICMP ενθυλακώνεται μέσα στο πακέτο IP. Η συνολική χρονική διάρκεια ταξιδιού RTT (Round-Trip Time) των μηνυμάτων Echo Request και Echo Reply μέσα στο δίκτυο δίνει μια ένδειξη για τη φόρτιση του δικτύου. Ειδικά στα Windows, το ping στέλνει τέσσερα διαδοχικά πακέτα Αίτησης Ηχούς (Echo Request), γι' αυτό βλέπετε τέσσερα αποτελέσματα. Τα αποτελέσματα του ping δεν μπορεί να θεωρηθούν σε καμία περίπτωση πλήρως αξιόπιστα, όσον αφορά τη σωστή επικοινωνία και δρομολόγηση πακέτων. Για παράδειγμα, αν με τη βοήθεια της εντολής αυτής, βρεθεί ένας κόμβος ανενεργός, δεν εξυπακούεται ότι πράγματι είναι. Πιο συγκεκριμένα, αν δε ληφθεί Echo Reply από τον κόμβο προορισμού, υπάρχει πιθανότητα ο ίδιος ο κόμβος ή κάποιο τείχος προστασίας (firewall), που παρεμβάλλεται στη διαδρομή, να μπλοκάρει τα μηνύματα του πρωτοκόλλου ICMP και να μας οδηγεί εσφαλμένα στο συμπέρασμα ότι ο κόμβος είναι μη ενεργός (down ή unreachable). Επίσης είναι δυνατό ο κόμβος προορισμού ή κάποια ενδιάμεση συσκευή να μην είναι επαρκώς πληροφορημένη για το δίκτυο του αποστολέα και έτσι να μην είναι δυνατή η σωστή επιστροφή της απάντησης.

1. Εκτελέστε την εντολή ping από την γραμμή εντολών ώστε να επικοινωνήσετε με το διπλανό σας υπολογιστή.
2. Καταγράψτε τη διεύθυνση MAC της κάρτας δικτύου του με τη βοήθεια του wireshark (υπόδειξη: Ψάξτε να βρείτε πρωτόκολλο ICMP)
3. Δοκιμάστε να επικοινωνήσετε μέσω του ping με το www.google.com. Βρείτε την IP διεύθυνση που αντιστοιχεί στο www.google.com μέσω του wireshark και καταγράψτε την αντίστοιχη διεύθυνση MAC του πλαισίου Ethernet. Σε ποια διεπαφή ανήκει αυτή η MAC διεύθυνση και γιατί;