Εργαστήριο «Δίκτυα Υπολογιστών Ι»

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

Επιμέλεια: Ιωάννης Ξυδάς, Αντώνης Μπόγρης

Βασικές διαγνωστικές εντολές – Κατανόηση λειτουργίας δρομολόγησης και DNS

Στόχοι της άσκησης:

- Κατανόηση της λειτουργίας δρομολόγησης των κόμβων IP – εξοικείωση με τις εντολές tracert και pathping.
- Κατανόηση της λειτουργίας των εξυπηρετητών DNS

Πληροφορίες:

- Το βιβλίο Δικτύωση Υπολογιστών, Προσέγγιση από πάνω προς τα κάτω
- Το βιβλίο ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ Andrew Tanenbaum.

Βασικές πληροφορίες

Σκοπός αυτού του εργαστηρίου είναι η εξοικείωση με τις εντολές tracert και pathping, οι οποίες αποτελούν χρήσιμα εργαλεία για τη μέτρηση και τον έλεγχο της κίνησης ενός δικτύου. Η άσκηση αυτή δίνει μια καλύτερη εικόνα για τη δομή του Internet και ειδικότερα για τη διασύνδεση των κόμβων ή την τοπολογία, όπως αλλιώς λέγεται, ενός τοπικού ή ευρύτερου δικτύου. Επίσης εξετάζεται η σχέση μεταξύ χρόνου διάδοσης των πακέτων, αριθμού κόμβων και πολυπλοκότητας της δομής των δικτύων. Το εργαστήριο αυτό γίνεται σε περιβάλλον Microsoft Windows 7/10, αλλά παρόμοιες εντολές ισχύουν και σε πλατφόρμα Unix.

Στο Internet δεν υπάρχουν συγκεκριμένες οδοί μεταφοράς των πακέτων, καθώς αυτό απαρτίζεται από πολλά επιμέρους δίκτυα (μικρά ή μεγάλα) που συνδέονται μεταξύ τους μέσω πολλαπλών διαφορετικών διαδρομών (η μεταγωγή είναι σε επίπεδο πακέτου και όχι κυκλώματος). Στα δίκτυα αυτά, συνδέονται εξυπηρετητές και απλοί χρήστες μέσω δικτυακών συσκευών, όπως είναι οι μεταγωγείς (switches). Η διαδρομή ενός μηνύματος από την πηγή μέχρι τον προορισμό του καθορίζεται από τους διάφορους δρομολογητές (routers) που μεσολαβούν και η λήψη των αποφάσεων είναι δυναμική, δηλαδή, αλλάζει ανάλογα με τις τρέχουσες συνθήκες. Η διαδρομή που ακολουθεί ένα πακέτο, μπορεί να ανιχνευθεί με την εντολή tracert. Η tracert στέλνει μηνύματα ICMP τύπου *Echo Request* με μεταβαλλόμενες τιμές του πεδίου Time-To-Live (TTL), του πακέτου IP, προς τον προορισμό. Αρχίζει στέλνοντας ένα ή περισσότερα μηνύματα ICMP τύπου *Echo Request* προς τον προορισμό με την τιμή του πεδίου Time-To-Live (TTL) του πακέτου IP ίση με 1.

Μετά, στέλνει μια παρόμοια σειρά μηνυμάτων στον ίδιο προορισμό με την τιμή του πεδίου TTL του πακέτου IP ίση με 2. Κατόπιν, επαναλαμβάνει την αποστολή των μηνυμάτων στον προορισμό με την τιμή του πεδίου TTL του πακέτου IP ίση με 3, κοκ. Κάθε δρομολογητής κατά μήκος της διαδρομής προς τον προορισμό μειώνει το TTL κατά 1, προτού προωθήσει το πακέτο. Όταν το TTL μηδενισθεί, ο δρομολογητής οφείλει να στείλει μήνυμα ICMP τύπου Time Exceeded στην πηγή. Ως αποτέλεσμα αυτής της διαδικασίας, η αποστολή ενός πακέτου IP με τιμή TTL ίση με 1 (από τον υπολογιστή σας) θα προκαλέσει την αποστολή ενός μηνύματος ICMP τύπου Time Exceeded προς τον υπολογιστή σας από τον δρομολογητή που βρίσκεται ένα βήμα πιο πέρα. Η αποστολή ενός πακέτου IP με τιμή TTL ίση με 2 θα προκαλέσει την αποστολή ενός μηνύματος ICMP τύπου Time Exceeded προς τον υπολογιστή σας από τον δρομολογητή που βρίσκεται δύο βήματα πιο πέρα. Παρόμοια, η αποστολή ενός πακέτου IP με τιμή TTL ίση με 3 θα προκαλέσει την αποστολή ενός μηνύματος ICMP τύπου Time Exceeded προς τον υπολογιστή σας από τον δρομολογητή που βρίσκεται τρία βήματα πιο πέρα., κοκ.

Ο υπολογιστής σας, εκτελώντας την tracert, μπορεί να μάθει τις διευθύνσεις των δρομολογητών μεταξύ αυτού και του εκάστοτε προορισμού. Η διαδρομή βρίσκεται εξετάζοντας τα μηνύματα Time Exceeded που προκαλούνται από διαδοχικά μηνύματα ηχούς με συνεχώς αυξανόμενες τιμές του TTL και καταγράφοντας την εκάστοτε διεύθυνση IP της πηγής που παράγει το μήνυμα ICMP τύπου Time Exceeded.

Η παράμετρος TTL εκφράζει το μέγιστο αριθμό κόμβων από τους οποίους μπορεί να περάσει ένα πακέτο IP μέχρι τον προορισμό του ή τον αριθμό βημάτων (hops) που μπορεί να διανύσει ένα πακέτο IP, άσχετα από τη χρονική διάρκεια του ταξιδιού αυτού. Αντίθετα, η RTT αναφέρεται στο χρόνο. Η tracert στέλνει τρία μηνύματα σε κάθε βήμα, γι' αυτό στα δεδομένα κάθε βήματος φαίνονται τρία αποτελέσματα. Επίσης, η tracert χρησιμοποιεί το DNS για να αντιστοιχίσει ονόματα στις διευθύνσεις IP των κόμβων της διαδρομής.

Η εντολή pathping των Windows είναι ένας συνδυασμός των ping και tracert. Για να χρησιμοποιήσετε τα παραπάνω εργαλεία, ανοίξτε ένα παράθυρο εντολών και πληκτρολογείστε το όνομα της εντολής ακολουθούμενο από τη διεύθυνση ή το όνομα του προορισμού.

Δραστηριότητες – Ασκήσεις

Εντολή Tracert

1. Ανοίξτε τον πλοηγό ιστού και επισκεφτείτε την κεντρική ιστοσελίδα της Cosmote (www.cosmote.gr). Μόλις η σελίδα έχει φορτωθεί πλήρως, χρησιμοποιήστε την εντολή ping με προορισμό πάλι τον εξυπηρετητή ιστού της Cosmote. Τι παράδοξο παρατηρείτε και τι μπορείτε να υποθέσετε για να το εξηγήσετε;

2. Εκτέλεσα από το σπίτι μου την tracert για να επικοινωνήσω με τον εξυπηρετητή ιστού του Παν. Δυτικής Αττικής και έλαβα την ακόλουθη απάντηση:

C:\Users\Yannis>tracert www.uniwa.gr
Tracing route to web-lbmain.noc.teiath.gr [195.130.100.83] over a maximum of 30 hops:

1	**5 ms**	**1 ms**	**5 ms**	**speedport-entry-2i.ote.gr [192.168.1.1]**
2	**34 ms**	**33 ms**	**34 ms**	**80.106.125.100**
3	**39 ms**	**38 ms**	**39 ms**	**nyma-asr99a-klmt-asr9ka.backbone.otenet.net 79.128.241.29]**
4	**39 ms**	**37 ms**	**38 ms**	**grnet.gr-ix.gr [176.126.38.1]**

```
 5    40 ms    39 ms    39 ms  teiath-1.eier.access-link.grnet.gr [62.217.96.117]
 6     *        *        *     Request timed out.
 7     *        *        *     Request timed out.
 8     *        *        *     Request timed out.
 9     *        *        *     Request timed out.
10     *        *        *     Request timed out.
11  ^C
C:\Users\Yannis>
```

Υπενθυμίζουμε ότι εάν παρατηρηθούν διαδοχικά μηνύματα εξάντλησης χρόνου, τότε το πιθανότερο είναι ότι παρεμβάλλεται κάποιο τείχος προστασίας, οπότε διακόψτε την εντολή tracert πιέζοντας τον συνδυασμό πλήκτρων <Ctrl>+c.

3.1 Χρησιμοποιώντας την εντολή tracert προς τον ίδιο προορισμό μπορείτε να συμπεράνετε την πιθανή τοπολογία του δικτύου από τον υπολογιστή σας μέχρι και το www.uniwa.gr. Εκτελέστε την εντολή και προσπαθήστε να σχεδιάσετε την τοπολογία του δικτύου.

3.2 Να σχεδιάσετε τη διαδρομή προς τον δρομολογητή του ΠΑΔΑ από το εργαστήριο δικτύων.

Χρησιμοποιείστε διαδοχικά την εντολή tracert με προορισμούς τους εξυπηρετητές ιστού του Τμήματος Μηχ. Πληροφορικής και Υπολογιστών και του Τμήματος Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών. Το σχεδιάγραμμα που θα κάνετε θα πρέπει να περιλαμβάνει το σταθμό εργασίας σας, τους δρομολογητές και τους εξυπηρετητές ιστού, καταγράφοντας παράλληλα τα ονόματα DNS (αν υπάρχουν), τις διευθύνσεις IP τους, καθώς και την καθυστέρηση.

Στη σελίδα http://www.noc.teiath.gr/?page_id=9 υπάρχει η τοπολογία του δικτύου του ΤΕΙ Αθήνας. Συγκρίνετε το σχεδιάγραμμά σας με αυτό της τοπολογίας του δικτύου του ΤΕΙ και αναγνωρίστε βασικούς κόμβους του δικτύου.

3.3 Ο κόμβος GReek Internet Exchange (https://www.gr-ix.gr/) προσφέρει τοπική διασύνδεση (peering) μεταξύ των εμπορικών δικτύων των εταιρειών παροχής υπηρεσιών Internet (ISP) στη χώρα μας μέσω ενός μεταγωγέα (switch) Ethernet που στεγάζεται σε ειδικό χώρο του δικτύου ΕΔΕΤ. Με τη βοήθεια της εντολής tracert στη γραμμή εντολών, παρατηρήστε τις διαδρομές μέχρι τους εξυπηρετητές ιστού των γνωστών ISPs: Wind, FORTHnet και Vodafone (www.wind.gr, www.forthnet.gr και www.vodafone.gr αντίστοιχα). Σε περίπτωση εκπνοής χρόνου μπορείτε να διακόψετε την εκτέλεση και να προχωρήσετε στον επόμενο ISP.

Βάσει των αποτελεσμάτων της εντολής tracert για τους παραπάνω προορισμούς, σχεδιάστε την τοπολογία του δικτύου από τον υπολογιστή σας μέχρι την κεντρική διεπαφή (interface) που είναι κοινή και στις τρεις διαδρομές.

Ποια είναι η διεύθυνση IP της κοινής διεπαφής που προσδιορίσατε στο ερώτημα και ποια είναι η διεύθυνση του υποδικτύου IP του GR-IX;

Υπηρεσία DNS

Το διαδίκτυο είναι χωρισμένο νοητά σε εκατοντάδες διαφορετικές περιοχές (domains) υψηλού επιπέδου, οι οποίες χωρίζονται με τη σειρά τους σε άλλες υποπεριοχές (subdomains) με πολλούς hosts η καθεμία. Η ιεραρχία των περιοχών μπορεί να παρασταθεί με ένα δέντρο. Το όνομα κάθε host αποτελείται από μια ακολουθία ετικετών (labels) που χωρίζονται με τελείες (π.χ. www.mit.edu). Μια περιοχή είναι ένα υποδέντρο του παγκόσμιου δέντρου ονομάτων. Το όνομα περιοχής (domain name) για ένα host είναι η ακολουθία των ετικετών που οδηγούν από το host (φύλλο στο δέντρο ονομάτων) στην κορυφή (ρίζα) του παγκόσμιου δέντρου ονομάτων.

Σε κάθε περιοχή στο διαδίκτυο (π.χ. uniwa.gr) υπάρχει ένας ή περισσότεροι εξυπηρετητές DNS. Αυτοί περιέχουν μια βάση δεδομένων που αντιστοιχίζει τα ονόματα των κόμβων της συγκεκριμένης περιοχής (π.χ. atlas.central.ntua.gr) σε διευθύνσεις IPv4 και/ή IPv6. Οι εξυπηρετητές DNS απαντούν σε αιτήσεις άλλων εξυπηρετητών DNS καθώς και χρηστών του διαδικτύου για την αντιστοιχία ενός ονόματος σε διεύθυνση IP και το αντίστροφο, ερευνώντας την παγκόσμια ιεραρχία DNS γι' αυτά. Επειδή για την εξυπηρέτηση μιας αίτησης μπορεί να γίνουν διαδοχικές ερωτήσεις σε άλλους εξυπηρετητές, ακολουθώντας την παγκόσμια ιεραρχία DNS, το αποτέλεσμα θα είναι αυξημένη καθυστέρηση. Για την αποφυγή του παραπάνω οι εξυπηρετητές DNS διαθέτουν μια προσωρινή μνήμη (cache) όπου κρατούν τις πιο πρόσφατες αιτήσεις. Η εντολή φλοιού **nslookup (Linux: dig)** μπορεί να χρησιμοποιηθεί για τη λήψη πληροφοριών από ένα εξυπηρετητή DNS. Μέσω της εντολής φλοιού nslookup μπορεί κανείς να ερωτήσει οποιοδήποτε εξυπηρετητή DNS για κάποια εγγραφή DNS. Ο ερωτώμενος εξυπηρετητής DNS μπορεί να είναι ένας εξυπηρετητής κορυφής, ο υπεύθυνος εξυπηρετητής της περιοχής ή οποιοσδήποτε άλλος ενδιάμεσος εξυπηρετητής. Για το σκοπό αυτό η nslookup στέλνει μια ερώτηση στον προσδιοριζόμενο εξυπηρετητή, λαμβάνει την απάντηση από τον εξυπηρετητή αυτό και εμφανίζει το αποτέλεσμα.

Η nslookup μπορεί να κληθεί με ή χωρίς παραμέτρους και έχει δύο τρόπους λειτουργίας. Στο μη διαλογικό τρόπο λειτουργίας (non-interactive mode) ζητείται μια συγκεκριμένη πληροφορία, ενώ στη διαλογική χρήση (interactive mode) αναζητούνται περισσότερες της μίας πληροφορίες. Ακολουθεί παράδειγμα εκτέλεσης της εντολή nslookup σε μη διαλογικό τρόπο λειτουργίας (non-interactive mode)

C:\Users\Yannis>nslookup www.uniwa.gr

Server: hermes.teiath.gr
Address: 195.130.100.19

Name: web-lbmain.noc.teiath.gr
Address: 195.130.100.83
Aliases: www.uniwa.gr

Στην προκειμένη περίπτωση ζητείται η διεύθυνση IP του www.uniwa.gr. Επειδή στα ορίσματα της εντολής δεν ορίστηκε ο εξυπηρετητής DNS που θα ερωτηθεί, χρησιμοποιείται αυτός που έχει οριστεί τοπικά στο σύστημα (στο παράδειγμα είναι ο hermes.teiath.gr). Η έξοδος από την εκτέλεση της εντολής παρέχει δύο πληροφορίες: α) το όνομα και τη διεύθυνση IP του εξυπηρετητή DNS που απάντησε στην ερώτηση (hermes.teiath.gr) και β) την ίδια την απάντηση (195.130.100.83).

Στο επόμενο παράδειγμα χρησιμοποιείται η nslookup ώστε να επιστραφεί η εγγραφή NS (δηλαδή, τα ονόματα των υπεύθυνων εξυπηρετητών) για την περιοχή uniwa.gr.

C:\Users\Yannis>nslookup -type=NS uniwa.gr
DNS request timed out.
timeout was 2 seconds.
Server: UnKnown
Address: 195.130.100.19

uniwa.gr nameserver = scrat.teipir.gr
uniwa.gr nameserver = sns1.grnet.gr
uniwa.gr nameserver = sns0.grnet.gr
uniwa.gr nameserver = hermes.teiath.gr
sns0.grnet.gr internet address = 83.212.5.18
sns1.grnet.gr internet address = 83.212.5.22
scrat.teipir.gr internet address = 195.251.93.78
hermes.teiath.gr internet address = 195.130.100.19
sns0.grnet.gr AAAA IPv6 address = 2001:648:2ffc:111::2
sns1.grnet.gr AAAA IPv6 address = 2001:648:2ffc:112::2

Με τον επόμενο τρόπο κλήσης της nslookup ερωτάται απευθείας ο server athena.teiath.gr, αντί του τοπικού εξυπηρετητή, για την διεύθυνση IP του εξυπηρετητή ιστού www.uniwa.gr.

C:\Users\Yannis>nslookup www.uniwa.gr athena.teiath.gr
DNS request timed out.
timeout was 2 seconds.
Server: UnKnown
Address: 195.130.100.18

Name: web-lbmain.noc.teiath.gr
Address: 195.130.100.83
Aliases: www.uniwa.gr

Άσκηση DNS – Εντολή nslookup

Για τους σκοπούς αυτής της άσκησης θα χρησιμοποιήσετε την εντολή nslookup στο διαλογικό τρόπο λειτουργίας (interactive mode). Ανοίξτε ένα παράθυρο εντολών και πληκτρολογήστε nslookup ακολουθούμενο από <Enter>. Στη συνέχεια πληκτρολογήστε **server hermes.teiath.gr** για να επιλέξετε τον εξυπηρετητή DNS που θα απαντά στη συνέχεια. Χρησιμοποιείστε την υποεντολή **set q=ns**, ώστε οι επόμενες απαντήσεις να περιέχουν εγγραφές σχετικές με τους υπεύθυνους εξυπηρετητές για την περιοχή DNS που θα εξετάζετε.

4.1 Πληκτρολογήστε ‘gr.’. Σε ποια περιοχή ανήκουν οι εξυπηρετητές DNS που εμφανίζονται;
4.2. Καταγράψτε το πλήθος των υπεύθυνων εξυπηρετητών DNS που εμφανίστηκαν καθώς και το όνομα και τη διεύθυνση IP ενός μόνο από αυτούς.
4.3. Πληκτρολογήστε τώρα ‘uniwa.gr’ και ‘teiath.gr’. Τι αποτελέσματα λαμβάνετε;

Χρησιμοποιώντας τώρα την υποεντολή **set q=all** επαναλάβετε τα βήματα 4.1-4.3. Τι παραπάνω πληροφορίες βλέπετε;

Αντί του server hermes.teiath.gr μπορείτε να χρησιμοποιήσετε και ένα τρίτο server εκτός του Πανεπιστημίου, π.χ τον DNS της Google. Οπότε με την υποεντολή **server 8.8.8.8** θα απαντά στη συνέχεια ο DNS server της Google.

Επαναλάβετε τα βήματα 4.1-4.3 με τον DNS server της Google.

Πρωτόκολλο DNS - Wireshark

Στην άσκηση αυτή θα δείτε τη δομή των μηνυμάτων που χρησιμοποιεί το πρωτόκολλο DNS με τη βοήθεια του Wireshark. Θα χρησιμοποιήσετε τη λειτουργία Capture με φίλτρο, ώστε τα πλαίσια που καταγράφονται να περιέχουν κάποια συγκεκριμένα χαρακτηριστικά. Υπενθυμίζεται ότι το φίλτρο απεικόνισης (Display), που επιλέγετε από το μενού Analyze, μπορεί να (απ)ενεργοποιηθεί οποιαδήποτε στιγμή κατά τη διάρκεια της καταγραφής, καθώς επίσης και μετά την ολοκλήρωση αυτής, προκειμένου να αποκρύπτει (αποκαλύπτει) κάποια από τα συλληφθέντα πλαίσια, ενώ το φίλτρο σύλληψης, που επιλέγετε από το μενού Capture, ενεργοποιείται πάντοτε πριν ξεκινήσει η διαδικασία καταγραφής, με αποτέλεσμα να καταγράφεται μόνο ένα μέρος των διερχόμενων πλαισίων.

Προσοχή: η απενεργοποίηση του φίλτρου απεικόνισης γίνεται πιέζοντας το κουμπί Clear (η διαγραφή του φίλτρου στο πεδίο εισαγωγής δεν το ακυρώνει!). Επίσης, αφού ξεκινήσετε το πρόγραμμα Wireshark πηγαίνετε στο Edit, Preferences και στη λίστα επιλογών στα αριστερά διαλέξτε το Name Resolution, βεβαιωθείτε ότι το Enable MAC name resolution και το Enable transport name resolution στα δεξιά είναι επιλεγμένα και πατήστε OK.

Με τη βοήθεια του Wireshark να καταγράψτε την κίνηση ενώ κάνετε χρήση της υπηρεσίας DNS. Εφαρμόστε φίλτρο σύλληψης για να παρατηρείτε μόνο την κίνηση που σχετίζεται με την διεύθυνση IP του υπολογιστή σας και ξεκινήστε την καταγραφή. Ανοίξτε ένα παράθυρο εντολών και καθαρίστε την προσωρινή μνήμη DNS (DNS cache) που διατηρεί ο υπολογιστής χρησιμοποιώντας την εντολή φλοιού ipconfig με την κατάλληλη επιλογή (flushdns). Στη συνέχεια εκτελέστε το πρόγραμμα nslookup ακολουθούμενο από <Enter> ώστε να εισέλθετε στο διαλογικό τρόπο λειτουργίας. Μετά εκτελώντας τις κατάλληλες υπο-εντολές της nslookup βρείτε το όνομα του υπολογιστή 195.134.67.53 έχοντας ως εξυπηρετητή DNS τον υπολογιστή hermes.teiath.gr και τερματίστε την καταγραφή.

5.1 Ποιο είναι το όνομα;

5.2 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε από το DNS (TCP ή UDP);

Μπείτε στη σελίδα www.cs.teiath.gr αφού πρώτα κάνετε capture. Εντοπίστε το πακέτο του πρωτοκόλλου DNS.

5.3 Με βάση αυτό να βρείτε την IP που αντιστοιχεί στο παραπάνω domain name.