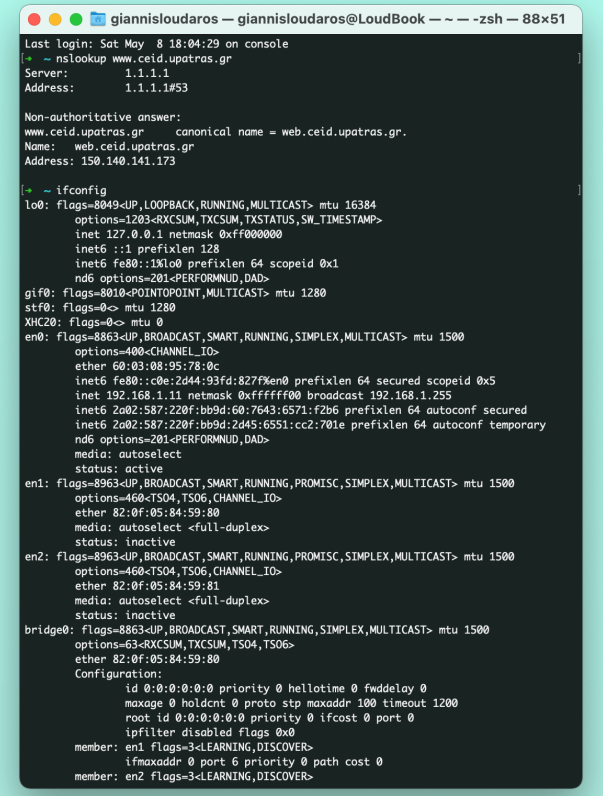
Δίκτυα Υπολογιστών

1η Εργασία για το μάθημα Εργαστήριο Δικτύων

Λουδάρος Ιωάννης (1067400)

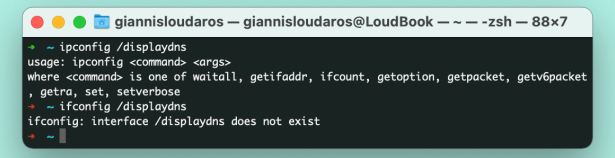
Μπορείτε να δείτε την τελευταία έκδοση του Project εδώ ή σκανάροντας τον κωδικό QR που βρίσκεται στην επικεφαλίδα.

Μέρος Α



Η **nslookup** (Name Server lookup) χρησιμοποιείται για την αναζήτηση πληροφοριών από εξυπηρετητές του συστήματος ονομάτων τομέα (DNS), όπως οι διευθύνσεις ip κάποιου υπολογιστή, οι εγγραφές MX για ένα όνομα domain και οι εξυπηρετητές NS ενός τομέα.

Η **ifconfig** (Interface Configuration) εμφανίζει πληροφορίες σχετικά με τις διεπαφές δικτύου του συστήματος, και με κάποιες παραμέτρους, κάνει ρυθμίσεις σ' αυτές.



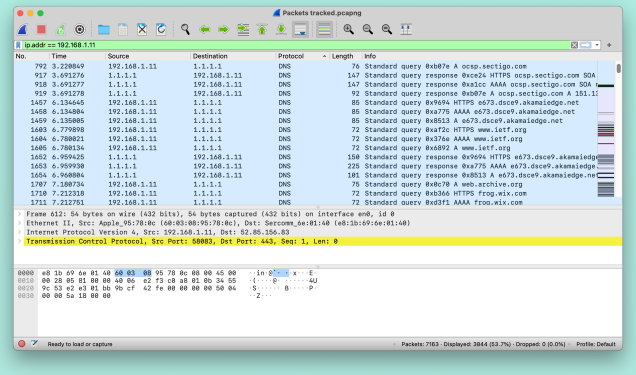
Μπορείτε να δείτε τα αποτελέσματα των ζητούμενων εντολών στα αριστερά. Οι εντολές ipconfig δεν συντάσσονται με τον ίδιο τρόπο στα Unix-like συστήματα και επιστρέφουν error.

Αφού έγινε εκκαθάριση της cache του Safari, έγινε εκκίνηση του Wireshark. Τέθηκε το φίλτρο:

“**ip.addr == 192.168.1.11**”

Δεν χρησιμοποιήθηκε η public IP του συστήματος αφού δεν ζητήθηκε κάτι τέτοιο.

Τότε ξεκίνησε το packet capturing.



Αφού ο browser εμφάνισε την ιστοσελίδα www.ietf.org/, τότε σταμάτησα την καταγραφή. Η παραγόμενη καταγραφή βρίσκεται στον ίδιο κατάλογο με αυτή την αναφορά.

Για την εμφάνιση των πακέτων έχει χρησιμοποιηθεί sorting ανά πρωτόκολλο. Έτσι έχουμε μαζεμένα όλα τα DNS queries μαζί.

Τα πεδία πληροφοριών που εμφανίζονται είναι:

No.	Time	Source	Destination	Protocol	Length	Info

1. Βλέπουμε ότι τα DNS μηνύματα που ανταλλάχθηκαν και είναι σχετικά με το **www.ietf.org/** είναι τα εξής :

No.	Time	Source	Destination	Protocol	Length	Info
1603	6.779898	192.168.1.11	1.1.1.1	DNS	72	Standard query 0xaf2c HTTPS www.ietf.org
1604	6.780021	192.168.1.11	1.1.1.1	DNS	72	Standard query 0x376e AAAA www.ietf.org
1605	6.780134	192.168.1.11	1.1.1.1	DNS	72	Standard query 0x6892 A www.ietf.org
1652	6.959425	1.1.1.1	192.168.1.11	DNS	150	Standard query response 0x9694 HTTPS e673.dsce9.akamaiedge.net SOA n0dsce9.akamaiedge.net
1653	6.959930	1.1.1.1	192.168.1.11	DNS	225	Standard query response 0xa775 AAAA e673.dsce9.akamaiedge.net AAAA 2a02:26f0:118:192::2a1 AAAA 2a02:26f0:118:1a1::2a1 AAAA 2a02:26f0:118:1a4::2a1 AAAA 2a02:26f0:118:1b1::2a1 AAAA 2a02:26f0:118:1bb::2a1

No.	Time	Source	Destination	Protocol	Length	Info
1654	6.960804	1.1.1.1	192.168.1.11	DNS	101	Standard query response 0x8513 A e673.dsce9.akamaiedge.net A 2.20.202.107
1707	7.180734	192.168.1.11	1.1.1.1	DNS	75	Standard query 0x0c70 A web.archive.org
1710	7.212318	192.168.1.11	1.1.1.1	DNS	72	Standard query 0xb366 HTTPS frog.wix.com
1711	7.212751	192.168.1.11	1.1.1.1	DNS	72	Standard query 0xd3f1 AAAA frog.wix.com
1712	7.213126	192.168.1.11	1.1.1.1	DNS	72	Standard query 0x2550 A frog.wix.com
1756	7.456220	1.1.1.1	192.168.1.11	DNS	173	Standard query response 0x376e AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700::6810:2d63 AAAA 2606:4700::6810:2c63
1757	7.457028	192.168.1.11	1.1.1.1	DNS	91	Standard query 0xf87c HTTPS www.ietf.org.cdn.cloudflare.net
1758	7.457287	192.168.1.11	1.1.1.1	DNS	91	Standard query 0x1904 A www.ietf.org.cdn.cloudflare.net

No.	Time	Source	Destination	Protocol	Length	Info
1830	7.739963	1.1.1.1	192.168.1.11	DNS	187	Standard query response 0xaf2c HTTPS www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net HTTPS
1841	7.780592	192.168.1.11	1.1.1.1	DNS	72	Standard query 0x6892 A www.ietf.org

2. Το πρωτόκολλο που χρησιμοποιήθηκε είναι το UDP, όπως μπορούμε να δούμε από την ανάλυση πακέτου

```
> Frame 1603: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0
> Ethernet II, Src: Apple_95:78:0c (60:03:08:95:78:0c), Dst: Sercomm_6e:01:40 (e8:1b:69:6e:01:40)
> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 1.1.1.1
v User Datagram Protocol, Src Port: 54093, Dst Port: 53
    Source Port: 54093
    Destination Port: 53
    Length: 38
    Checksum: 0x96b8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 39]
  > [Timestamps]
    UDP payload (30 bytes)
> Domain Name System (query)
```

3. Όπως βλέπουμε και από την παραπάνω ανάλυση, είναι η θύρα 53
4. Όπως βλέπουμε και από την παραπάνω ανάλυση, είναι η θύρα 54093
5. Το μήνυμα εμφανίζεται στην διεύθυνση 1.1.1.1, την οποία έχω ορίσει εγώ ως διεύθυνση DNS
6. Ο τύπος όπως φαίνεται στο info είναι “Standard query”

```
v Domain Name System (query)
    Transaction ID: 0xaf2c
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
```

7. Περιέχονται 3 απαντήσεις. Τα περιεχόμενα τους φαίνονται καθαρά παρακάτω:

```
Domain Name System (response)
    Transaction ID: 0x376e
  Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
```

```
Answers
  www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1661 (27 minutes, 41 seconds)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700::6810:2d63
      Name: www.ietf.org.cdn.cloudflare.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 161 (2 minutes, 41 seconds)
      Data length: 16
      AAAA Address: 2606:4700::6810:2d63
  www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700::6810:2c63
      Name: www.ietf.org.cdn.cloudflare.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 161 (2 minutes, 41 seconds)
      Data length: 16
      AAAA Address: 2606:4700::6810:2c63
```

8. Το πρώτο TCP SYN στέλνεται σε μία από τις διευθύνσεις του DNS πακέτου μας.

9. Όπως φαίνεται παρακάτω η **θύρα προορισμού είναι η 53** και **η θύρα προέλευσης είναι η 64747**

```
User Datagram Protocol, Src Port: 64747, Dst Port: 53
    Source Port: 64747
    Destination Port: 53
    Length: 45
    Checksum: 0x9e41 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 8]
  > [Timestamps]
    UDP payload (37 bytes)
```

10. Το μήνυμα ερώτησης εμφανίζεται στην προβλεπόμενη διεύθυνση DNS που έχω ορίσει από τα preferences του λειτουργικού συστήματος.

11. Όπως βλέπουμε και παρακάτω είναι “Standard query” που δεν περιλαμβάνει καθόλου απαντήσεις

```
Domain Name System (query)
    Transaction ID: 0x30fe
  Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

12. Όπως είδαμε και προηγούμενα, οι απαντήσεις σχετίζονται με το ερώτημα που έγινε. Περισσότερες πληροφορίες βλέπουμε παρακάτω:

```
Domain Name System (response)
  Transaction ID: 0x30fe
  Flags: 0x8180 Standard query response, No error
    1... .... .... .... = Response: Message is a response
    .000 0... .... .... = Opcode: Standard query (0)
    .... .0.. .... .... = Authoritative: Server is not an authority for domain
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... 1... .... = Recursion available: Server can do recursive queries
    .... .... .0.. .... = Z: reserved (0)
    .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 2
```

```
Answers
  www.ceid.upatras.gr: type CNAME, class IN, cname web.ceid.upatras.gr
      Name: www.ceid.upatras.gr
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 81590 (22 hours, 39 minutes, 50 seconds)
      Data length: 6
      CNAME: web.ceid.upatras.gr
  web.ceid.upatras.gr: type A, class IN, addr 150.140.141.173
      Name: web.ceid.upatras.gr
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 81590 (22 hours, 39 minutes, 50 seconds)
      Data length: 4
      Address: 150.140.141.173
```

Γενικά Ερωτήματα για τον τρόπο λειτουργίας του DNS

13. **Recursive Resolver:** Η πρώτη στάση σε ένα DNS query. Είναι ο μεσάζοντας μεταξύ ενός client και ενός DNS nameserver. Αφού λάβει DNS query από έναν web client, ο recursive resolver είτε θα απαντήσει με δεδομένα που βρίσκονται στην cache (τα δεδομένα στην cache έχουν ληφθεί από authoritative nameservers), είτε θα στείλει requests σε έναν root nameserver, στη συνέχεια σε έναν TLD nameserver και τέλος, σε έναν authoritative nameserver. Όταν λάβει απάντηση από τον τελευταίο, η οποία

περιέχει την IP που ζητήθηκε, τότε ο recursive resolver στέλνει την απάντηση στον client.

Root Nameserver: Υπάρχουν 13 root nameservers. Ο καθένας από αυτούς λαμβάνει queries από έναν recursive resolver, τα οποία περιέχουν ένα domain name. Ο root nameservers κατευθύνει τον recursive resolver σε έναν TLD nameserver.

TLD Nameserver: Περιέχει όλες τις πληροφορίες για όλα τα domain names που μοιράζονται κοινό domain extension. Οι TLD nameservers χωρίζονται σε δύο είδη, στους Generic top-level domains και στους Country code top-level domains.

Authoritative Nameservers: Ένας recursive resolver δέχεται απάντηση από έναν TLD nameserver και η απάντηση αυτή θα οδηγήσει τον resolver σε έναν authoritative nameserver. Συνήθως, είναι η τελευταία στάση ενός resolver. Περιέχει πληροφορίες που είναι συγκεκριμένες για το domain name του.

14. **DNS Header Fields:** Identification, Flags, Number of questions, Number of answers, Number of authority resource records (RRs), Number of additional RRs.

    Identification: Δείχνει ένα ολοκληρωμένο transaction (request και αντίστοιχο response)
    Flags: QR (query/reply), OPCODE (standard query, inverse query, server status request), AA (authoritative answer), TC (truncation), RD (recursion desired), RA (recursion available), Z (zero), RCODE (response code).
    Number of questions: Αριθμός ερωτήσεων σε ένα πακέτο.
    Number of answers: Αριθμός απαντήσεων σε ένα πακέτο.
    Number of authority resource records (RRs): Data records (A, CNAME, SOA, PTR, NS).
    Number of additional RRs: Data records τα οποία ίσως φανούν χρήσιμα στον client.

15. **DNS Standard query 0x0003 A google.com**
    0... .... = Response: Message is a query
    .000 0... .... = Opcode: Standard query (0)
    ....1 .... = Recursion desired: Do query recursively google.com: type A, class IN
    Name: google.com
    Name Length: 10
    Label Count: 2
    Type: A (Host Address) (1) Class: IN (0x0001)

16. **DNS Standard query response 0x0003 A google.com A**
    1... .... = Response: Message is a response
    .000 0... .... = Opcode: Standard query (0)
    .... .0.. .... = Authoritative: Server is not an authority for domain 11 Answers.

Μέρος Β

1. Ανάλυση Πλαισίου

00 A0 92 48 72 45 00 00 0C 05 C3 58 08 00 45 00 00 29 DB FB 40 00 FE 06 7D CB 81 6E 1E 1A 81 6E 02 11 02 03 00 50 6A 86 7B 57 B6 B6 B0 20 50 10 24 00 17 C4 00 00 02 54 41 4D 49 4C D7 87 6C A4

1. 129.110.30.26 → 129.110.2.17
2. Το μήκος του ip είναι 20 bytes (14-33)
3. Το frame είναι 64 bytes on wire (512 bits)
4. Η TCP source port είναι η 515 και η destination port η 80.
5. Το header checksum εντοπίζεται στο 23ο και 24ο byte 0x7dcb

Η τιμή στο frame δεν είναι η σωστή:

- Frame check sequence: 0xd7876ca4 incorrect, should be 0xf07b03a5
  - Expert Info (Error/Checksum): Bad checksum [should be 0xf07b03a5]
  - FCS Status: Bad

2. Πείραμα IP με χρήση Wireshark

Το πείραμα έγινε με χρήση του φίλτρου "*ether host <my_mac_address>*". Η καταγραφή πακέτων άρχισε έπειτα από την εκτέλεση της εντολής tracert -d 83.212.8.210.
(-d: «Do not resolve addresses to hostnames»)
Για την εμφάνιση μόνο πακέτων ICMP, το display filter που χρησιμοποιείται είναι το: *icmp.*

IP address: 192.168.2.8
Εμφανίζεται στο πεδίο "Source" του header, όπως φαίνεται κατά την ανάλυση του πακέτου (Source: 192.168.2.8).

Η τιμή του πεδίου protocol του IP header του μηνύματος ICMP Echo Request είναι: Protocol: ICMP(1)

Τιμή πεδίου: 01

Δεύτερη τετράδα hex αριθμών: **005C** —> 92_{10}. Συνεπώς, το μήκος είναι 92 bytes. Αναλύοντας το hex packet (χρησιμοποιήθηκε η υπηρεσία https://hpd.gasmi.net/) στο πεδίο ICMP data field παρατηρείται πως υπάρχουν 64 bytes.

Ταξινομώντας κατά φθίνουσα σειρά τα IP packets - σύμφωνα με το source address τους - και παρατηρώντας τα μηνύματα ICMP τύπου Echo Request, φαίνεται πως στα IP

addresses μεταβάλλονται τα δύο τελευταία πεδία, δηλαδή το μέρος του host. Ωστόσο, μένει αμετάβλητο το μέρος του network, δηλαδή τα δύο πρώτα πεδία.

Αναλύοντας τα μηνύματα ICMP τύπου Time Extended, προκύπτουν τα εξής συμπεράσματα:
Η κοντινότερή IP address server: 192.168.2.1
Time to Live: 1 για όλα τα πακέτα.

Η τιμή TTL παραμένει σταθερή, γιατί κατά την εκτέλεση της εντολής *tracert -d* 83.212.8.210 δίνονται 30 hops για το trace της διαδρομής.

Μέρος Γ

11. Δίνουμε από το PC0 την εντολή Ping.

I. Στο τοπικό interface του PC0
II. NAI
III. NAI

Μέρος Δ

Μέρος1:

>telnet 10.10.10.2
Εισάγω τον κωδικό για να μπορέσω να ελέγξω το s1: cisco
>enable
Εισάγω ξανά τον κωδικό
>copy running-config startup-config
Εμφανίζεται η ερώτηση Destination filename [startup-config]? Πατάμε enter.
>show running-config
Εμφανίζονται οι κωδικοί.
>conf t
>service password-encryption
>EXIT
>show running-config
Τώρα οι κωδικοί δεν εμφανίζονται, στη θέση τους εμφανίζεται: 0822455D0A16.

Μέρος2:

>conf t
>ip domain-name netacad.pka
>crypto key generate rsa
Εμφανίζεται η ερώτηση How many bits in the modulus [512]: απαντάμε το ζητούμενο 1024.
>user
>username up1067400 secret up1067400
>username diaxeiristis secret cisco
>line vty 0 15
>login local
>transport input ssh
>no password cisco

Μέρος3:

Κάνω exit 3 φορές έως να φτάσω στο pc.
>telnet 10.10.10.2
>ssh
>ssh -l diaxeiristis 10.10.10.2
Δίνω τον κωδικό cisco
>enable
Δίνω τον κωδικό cisco.
>copy running-config startup-config
Enter