

Μάριος Αλέξανδρος Μορφόπουλος up1058102.

1 Εργασία Δικτύων

1) Μέρος Εργασίας το πρωτόκολλο DNS

Η εντολή nslookup www.ceid.upatras.gr δίνει το ακόλουθο αποτέλεσμα:

**Server: speedport.ip
Address: fe80::1
Non-authoritative answer:
Name: web.cEID.UPAtras.gR
Address: 150.140.141.173
Aliases: www.ceid.upatras.gr**

Εκτελώντας την εντολή ipconfig/all προκύπτει το ακόλουθο αποτέλεσμα:

Windows IP Configuration

**Host Name: pc-PC
Primary Dns Suffix:
Node Type: Hybrid
IP Routing Enabled.....: No
WINS Proxy Enabled.....: No
DNS Suffix Search List.....: home**

Ethernet adapter Bluetooth Network Connection:

**Media State: Media disconnected
Connection-specific DNS Suffix .:
Description: Bluetooth Device (Personal Area Network)
Physical Address.....: 20-16-D8-96-FA-60
DHCP Enabled.....: Yes
Autoconfiguration Enabled: Yes**

Wireless LAN adapter Wireless Network Connection 3:

Media State: Media disconnected

Connection-specific DNS Suffix .:

Description: Microsoft Virtual WiFi Miniport Adapter #2

Physical Address.: 84-3A-4B-4E-28-BD

DHCP Enabled.: Yes

Autoconfiguration Enabled: Yes

Wireless LAN adapter Wireless Network Connection 2:

Media State: Media disconnected

Connection-specific DNS Suffix .:

Description: Microsoft Virtual WiFi Miniport Adapter

Physical Address.: 84-3A-4B-4E-28-BD

DHCP Enabled.: Yes

Autoconfiguration Enabled: Yes

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix .: home

Description: Intel(R) Centrino(R) Advanced-N 6205

Physical Address.: 84-3A-4B-4E-28-BC

DHCP Enabled.: Yes

Autoconfiguration Enabled: Yes

IPv6 Address.: 2a02:587:3b03:e7d7:54a:3124:ebba:cc44(Preferr

Temporary IPv6 Address.: 2a02:587:3b03:e7d7:a4e1:6fa4:f0e9:4f07(Prefer

Link-local IPv6 Address: fe80::54a:3124:ebba:cc44%12(Preferred)

IPv4 Address.: 192.168.1.11(Preferred)

Subnet Mask: 255.255.255.0

Lease Obtained.: ÄåöôÝñá, 13 Áðñéëßïö 2020 9:21:51 ì

Lease Expires: Õñßôç, 14 Áðñéëßïö 2020 9:21:51 ì

Default Gateway: fe80::1%12

192.168.1.1

DHCP Server: 192.168.1.1

DHCPv6 IAID: 310655563

DHCPv6 Client DUID.: 00-01-00-01-23-87-68-70-F0-1F-AF-4E-91-61

DNS Servers: fe80::1%12

192.168.1.1

Ethernet adapter Local Area Connection:

Autoconfiguration Enabled . . . : Yes

Autoconfiguration Enabled . . . : Yes

Windows IP Configuration

[illegible]

Record	Name	:
--------	------	---	---	---	---	---	---

[illegible]

Record Type: 12

Time To Live: 86400

Data Length : 8

Section: Answer

PTR Record: localhost

zkkhimq

Name does not exist.

1.0.0.127.in-addr.arpa

Record Name: 1.0.0.127.in-addr.arpa.

Record Type: 12

Time To Live: 86400

Data Length : 8

Section: Answer

PTR Record: localhost

rsmxsrxcmhpg

Name does not exist.

d.b.a.1.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.0.0.6.8.4.1.0.0.2.ip6.arpa

Name does not exist.

hithwlpbjzthcz

Name does not exist.

wpad

Name does not exist.

e.0.0.2.0.0.0.0.0.0.0.0.0.0.5.1.8.0.1.0.0.4.0.5.4.1.0.0.a.2.ip6.arpa

	Record	Name	:
e.0.0.2.0.0.0.0.0.0.0.0.0.0.5.1.8.0.1.0.0.4.0.5.4.1.0.0.a.2.iP6.ArpA								
Record Type: 12								
Time To Live: 15801								
Data Length: 8								
Section: Answer								
PTR Record: fra15s12-in-x0e.1e100.net								

teredo.ipv6.microsoft.com

Name does not exist.

az416426.vo.msecnd.net

Record Name: az416426.vo.msecnd.net
Record Type: 5
Time To Live: 1609
Data Length: 8
Section: Answer
CNAME Record: cs22.wpc.v0cdn.nEt

diavlfvnnv

Name does not exist.

pyefndtvosawyb

Name does not exist.

0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.b.0.0.a.d.0.5.0.8.5.0.2.0.a.2.ip6.arpa

Name does not exist.

ikzxwhzvtipr

Name does not exist.

fa

Name does not exist.

isatap.home

Name does not exist.

myexternalip.com

Record Name: mYEXTeRNAlIP.coM

Record Type: 1

Time To Live: 179

Data Length: 4
Section: Answer
A (Host) Record ...: 216.239.32.21

Record Name: mYEXTeRNAliP.coM
Record Type: 1
Time To Live: 179
Data Length: 4
Section: Answer
A (Host) Record ...: 216.239.34.21

Record Name: mYEXTeRNAliP.coM
Record Type: 1
Time To Live: 179
Data Length: 4
Section: Answer
A (Host) Record ...: 216.239.38.21

Record Name: mYEXTeRNAliP.coM
Record Type: 1
Time To Live: 179
Data Length: 4
Section: Answer
A (Host) Record ...: 216.239.36.21

localhost

Record Name: localhost
Record Type: 1
Time To Live: 86400
Data Length: 4

Section: Answer

A (Host) Record ...: 127.0.0.1

localhost

Record Name: localhost

Record Type: 28

Time To Live: 86400

Data Length: 16

Section: Answer

AAAA Record: ::1

Εκτελώντας την εντολή ipconfig/flushdns προκύπτει το ακόλουθο αποτέλεσμα:

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

Αρχικά χρησιμοποιώ την εντολή ipconfig

Μετά χρησιμοποιώ την εντολή ipconfig /flushdns

`ip.addr==192.168.1.11`

πηγαίνω στη σελίδα <https://www.ietf.org/>

σταματάω την καταγραφή πακέτων στο Wireshark

Απαντήστε στα παρακάτω ερωτήματα και δώστε screenshots από τα πακέτα.

Απάντηση στην ερώτηση 1

Io.	Time	Source	Destination	Protocol	Length	Info
11	8.395969	fe80::54a:3124:ebba...	fe80::1	DNS	95	Standard query 0x85db A www.gstatic.com
12	8.395974	fe80::54a:3124:ebba...	fe80::1	DNS	95	Standard query 0x85db A www.gstatic.com
13	8.397960	fe80::1	fe80::54a:3124:ebba...	DNS	111	Standard query response 0x85db A www.gstatic.com A 172.217.16.131
14	8.399688	fe80::54a:3124:ebba...	fe80::1	DNS	95	Standard query 0x311b AAAA www.gstatic.com
15	8.399692	fe80::54a:3124:ebba...	fe80::1	DNS	95	Standard query 0x311b AAAA www.gstatic.com
16	8.400332	fe80::54a:3124:ebba...	fe80::1	DNS	109	Standard query 0x66c5 A clientservices.googleapis.com
17	8.400335	fe80::54a:3124:ebba...	fe80::1	DNS	109	Standard query 0x66c5 A clientservices.googleapis.com
18	8.402239	fe80::1	fe80::54a:3124:ebba...	DNS	123	Standard query response 0x311b AAAA www.gstatic.com AAAA 2a00:1450:4001:81d::2003
23	8.419143	fe80::1	fe80::54a:3124:ebba...	DNS	125	Standard query response 0x66c5 A cLiEnTSeRVICes.gOogLeaPis.COM A 216.58.206.3
26	8.428323	fe80::54a:3124:ebba...	fe80::1	DNS	109	Standard query 0x9cf7 AAAA clientservices.googleapis.com

Απάντηση στην ερώτηση 2

Io.	Time	Source	Destination	Protocol	Length	Info
11	8.395969	fe80::54a:3124:ebba...	fe80::1	DNS	95	Standard query 0x85db A www.gstatic.com

11	8.395969	fe80::54a:31...	fe80::1	DNS	95	Standard query 0x85db A www.gstatic.com
12	8.395974	fe80::54a:31...	fe80::1	DNS	95	Standard query 0x85db A www.gstatic.com
13	8.397960	fe80::1	fe80::54a:3...	DNS	111	Standard query response 0x85db A www.gstatic.com A 172.217.16.131
14	8.399688	fe80::54a:31...	fe80::1	DNS	95	Standard query 0x311b AAAA www.gstatic.com
15	8.399692	fe80::54a:31...	fe80::1	DNS	95	Standard query 0x311b AAAA www.gstatic.com
16	8.400332	fe80::54a:31...	fe80::1	DNS	109	Standard query 0x66c5 A clientservices.googleapis.com
17	8.400335	fe80::54a:31...	fe80::1	DNS	109	Standard query 0x66c5 A clientservices.googleapis.com

▶ Frame 11: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
 ▶ Ethernet II, Src: IntelCor_4e:28:bc (84:3a:4b:4e:28:bc), Dst: Sercomm_76:75:30 (d4:60:e3:76:75:30)
 ▶ Internet Protocol Version 6, Src: fe80::54a:3124:ebba:cc44, Dst: fe80::1
 ▶ User Datagram Protocol, Src Port: 56931, Dst Port: 53
 ▶ Domain Name System (query)

Από το screenshot βλέπουμε ότι στο Frame υπάρχει η κεφαλίδα Ethernet, μετά ακολουθεί η κεφαλίδα IP και η κεφαλίδα UDR και τέλος υπάρχει η κεφαλίδα DNS.

Όπως φαίνεται και από το screenshot το πρωτόκολλο UDP χρησιμοποιεί το Port 53

```

  User Datagram Protocol, Src Port: 56931, Dst Port: 53
    Source Port: 56931
    Destination Port: 53
    Length: 41
    Checksum: 0x7944 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
    [Timestamps]
  
```

Μετά ακολουθεί η κεφαλίδα DNS με περιεχόμενο που φαίνεται από το screenshot

```

  Domain Name System (query)
    Transaction ID: 0x85db
    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
      [Response In: 13]
  
```

Η DNS(DNS Header) ξεκινάει με ένα Transaction ID που συσχετίζει ένα DNS request με το αντίστοιχο DNS reply

Μετά έχουμε τα DNS Flags:

Αρχικά πρώτο flag μας δείχνει αν το μήνυμα DNS είναι ερώτηση δηλαδή query ή απάντηση δηλαδή response. Όπως βλέπουμε απο τα προηγούμενα screenshot το δικό μας είναι DNS query. Η **www.ietf.org** είναι το όνομα του name server. Επίσης γνωρίζουμε ότι όλο το DNS message είναι σχεδιασμένο να χωρά σε ένα μόνο UDP message. Τέλος βλέπουμε να φαίνεται ο αριθμός του μηνύματος που είναι η απάντηση στο DNS request μήνυμα.

```
Queries
  www.iEtf.oRg: type A, class IN
    Name: www.iEtf.oRg
    [Name Length: 12]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)

Answers
  www.iEtf.oRg: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
```

Απάντηση στην ερώτηση 3

```
User Datagram Protocol, Src Port: 53, Dst Port: 56931
  Source Port: 53
  Destination Port: 56931
  Length: 57
  Checksum: 0x3725 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
  [Timestamps]
  Domain Name System (response)
```

Η Dst Port(δηλαδή η θύρα προορισμού) είναι το port 53 για το μήνυμα ερώτησης DNS.

Απάντηση στην ερώτηση 4

```
User Datagram Protocol, Src Port: 53, Dst Port: 56931
  Source Port: 53
  Destination Port: 56931
  Length: 57
  Checksum: 0x3725 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
  [Timestamps]
  Domain Name System (response)
```

Η Src Port(δηλαδή η θύρα προέλευσης) είναι το port 53 για το μήνυμα απόκρισης DNS.

Απάντηση στην ερώτηση 5

Όπως φαίνεται από το screenshot το DNS query στέλνεται στο DNS Server

```
Internet Protocol Version 6, Src: fe80::1, Dst: fe80::54a:3124:ebba:cc44
```

Εκτελώ την εντολή ipconfig/all και παίρνω το εξής DNS Server

```
DNS Servers . . . . . : fe80::1%12
                      192.168.1.1
                      192.168.1.1
```

Έτσι έρχομαι στο συμπέρασμα ότι οι 2 διευθύνσεις IP είναι ίδιες δηλαδή η IP του τοπικού μου Server και η IP του Server που στέλνεται το ερώτημα DNS

Απάντηση στην ερώτηση 6

Όπως φαίνεται από το screenshot είναι ένα standard DNS Query ερώτημα και δεν περιέχει απάντηση

```
Flags: 0x8180 Standard query response, No error
1... .... = Response: Message is a response
```

Απάντηση στην ερώτηση 7

```
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: 734 (12 minutes, 14 seconds)
    Data length: 33
    CNAME: www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
```

Όπως φαίνεται και από το screenshot υπάρχει τρεις απαντήσεις που περιέχουν πληροφορίες με το όνομα του host,τον τύπο,την κλάση,το Time to live(δηλαδή το TTL),το μήκος των δεδομένων(Data length) και την διεύθυνση IP,αυτές είναι απαντήσεις που έχω απο εναν DNS Server.

Απάντηση στην ερώτηση 8

```
Frame 52: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: IntelCor_4e:28:bc (84:3a:4b:4e:28:bc), Dst: Sercomm_76:75:30 (d4:60:e3:76:75:30)
  Destination: Sercomm_76:75:30 (d4:60:e3:76:75:30)
  Source: IntelCor_4e:28:bc (84:3a:4b:4e:28:bc)
  Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2a02:587:3b23:ecf:34a8:1040:da84:ce95, Dst: 2a00:1450:4001:81a::2003
  0110 .... = Version: 6
  .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 0000 0000 0000 = Flow Label: 0x0000
  Payload Length: 32
  Next Header: TCP (6)
  Hop Limit: 255
  Source: 2a02:587:3b23:ecf:34a8:1040:da84:ce95
  Destination: 2a00:1450:4001:81a::2003
Transmission Control Protocol, Src Port: 55062, Dst Port: 443, Seq: 0, Len: 0
```

```
0000 d4 60 e3 76 75 30 84 3a 4b 4e 28 bc 86 dd 60 00  ..vu0.: KN( ...
0010 00 00 00 20 06 ff 2a 02 05 87 3b 23 0e cf 34 a8  ..*..;#..4.
0020 10 40 da 84 ce 95 2a 00 14 50 40 01 08 1a 00 00  -@...*..P@....
0030 00 00 00 00 20 03 d7 16 01 bb e8 be 99 18 00 00  .....
0040 00 00 80 02 20 00 e6 96 00 00 02 04 05 98 01 03  .....
0050 03 08 01 01 04 02  .....
```

Βλέπουμε ότι η διεύθυνση IP του Syn πακέτου δεν αντιστοιχεί στην IP διεύθυνση

Εκτελώ την εντολή nslookup www.ceid.upatras.gr

Το 3-4 request και response πακέτο είναι τα εξής.

1318	23.409661	fe80::54a:31...	fe80::1	DNS	99	✓	✓	Standard query 0x0004 A www.ceid.upatras.gr
1319	23.413305	fe80::1	fe80::54a:3...	DNS	148	✓	✓	Standard query response 0x0004 A www.ceid.upatras.gr CNAME web.CEID.UPaTRAS.Gr A 150.140.141.173

Απάντηση στην ερώτηση 9

Το μήνυμα ερώτησης DNS και ο μύνημα απόκρισης DNS είναι τα εξής όπως φαίνεται από τα screenshot

1318	23.409661	fe80::54a:31...	fe80::1	DNS	99	✓	✓	Standard query 0x0004 A www.ceid.upatras.gr
1319	23.413305	fe80::1	fe80::54a:3...	DNS	148	✓	✓	Standard query response 0x0004 A www.ceid.upatras.gr CNAME web.CEID.UPaTRAS.Gr A 150.140.141.173

Όπως φαίνεται και από το screenshot η θύρα προορισμού για το μήνυμα ερώτησης DNS είναι η 53

```
User Datagram Protocol, Src Port: 59294, Dst Port: 53
  Source Port: 59294
  Destination Port: 53
  Length: 51
  Checksum: 0x90b9 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 5]
  ▸ [Timestamps]
  ▸ Domain Name System (query)
```

Όπως φαίνεται και από το screenshot η θύρα προέλευσης του μηνύματος απόκρισης DNS είναι η 53.

```
User Datagram Protocol, Src Port: 53, Dst Port: 59294
  Source Port: 53
  Destination Port: 59294
  Length: 135
  Checksum: 0xb1cc [unverified]
  [Checksum Status: Unverified]
  [Stream index: 5]
  ▸ [Timestamps]
  ▸ Domain Name System (response)
```

Απάντηση στην ερώτηση 10

```
DNS Servers . . . . . : fe80::1%12
                      192.168.1.1
                      192.168.1.1
```

Παρατηρώ ότι η διεύθυνση IP είναι η 192.168.1.1 και είναι ίδια με διεύθυνση IP του προεπιλεγμένου τοπικού διακομιστή DNS επομένως αυτή είναι όντως η διεύθυνση IP του DNS (δηλαδή του default DNS server).

Απάντηση στην ερώτηση 11

Όπως φαίνεται και από το screenshot το μήνυμα ερώτησης DNS είναι τύπου A και δεν έχει απαντήσεις.

```

Queries
  www.ceid.upatras.gr.home: type A, class IN
    Name: www.ceid.upatras.gr.home
    [Name Length: 24]
    [Label Count: 5]
    Type: A (Host Address) (1)
    Class: IN (0x0001)

```

Απάντηση στην ερώτηση 12

Όπως φαίνεται και από το screenshot περιέχει 2 απαντήσεις

```

> www.ceid.upatras.gr: type CNAME, class IN, cname web.cEiD.UPATrAS.GR
> web.cEiD.UPATrAS.GR: type A, class IN, addr 150.140.141.173

```

Κάθε απάντηση περιέχει τον host, τον τύπο διεύθυνση και την κλάση

```

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: 81173 (22 hours, 32 minutes, 53 seconds)
  Data length: 21
  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: 81173 (22 hours, 32 minutes, 53 seconds)
  Data length: 4
  Address: 150.140.141.173

```

Απάντηση στη ερώτηση 13

Ο **Recursive resolver** είναι ένας αναδρομικός αναλυτής όπου στέλνει μια ερώτηση πρώτα στον **root nameserver** που είναι διακομιστής ρίζας (συνεπώς ο root nameserver είναι η πρώτη στάση) η οποία περιέχει ένα domain όνομα (όνομα ιστοσελίδας) στην συνέχεια ο **root nameserver** θα στείλει απάντηση κατευθύνοντας τον recursive resolver στον κατάλληλο TLD nameserver ανάλογα την κατάληξη της ιστοσελίδας (π.χ. .com, .net, .org). Ο TLD nameserver περιέχει πληροφορίες για όλες τις ιστοσελίδες με κοινή επέκταση π.χ.

.com. Έτσι όπου ο **recursive resolver** λάβει απάντηση από τον **root nameserver** απευθύνεται στον αντίστοιχο TLD που του υπέδειξε ο root και του στέλνει ερώτηση. Ο TLD θα στείλει απάντηση στον recursive δείχνοντας του έναν authoritative nameserver (άρα και προτελευταίο βήμα για μια διεύθυνση IP). Ο **authoritative nameservers** περιέχει πληροφορίες για τη συγκεκριμένη ιστοσελίδα που ψάχνουμε π.χ. google και δίνει στον recursive το IP του server που του βρήκε στο DNS.

Απάντηση στην ερώτηση 14

Όλα τα DNS πακέτα έχουν την εξής δομή.Αποτελούνται απο Κεφαλίδα (Header),την Ερώτηση(Question),τις Εγγραφές Απάντησεις(Answer Resource Records),τις Εγγραφές πόρων αρχής(Authority Resource Records),τις Επιπρόσθετες Εγγραφές(Additional Records).

Κεφαλίδα (Header)

Η κεφαλίδα μας δίνει πληροφορίες ταυτοποίησης αλλά και παρέχει περιλήψεις για το περιεχόμενο του μηνύματος.Η κεφαλίδα έχει 6 πεδία συνόλου 16 bits.Το Transaction ID καταλαμβάνει τα πρώτα 16 bits.Στην συνέχεια το επόμενο πεδίο είναι για τα flags (σημαίες) και τα bits τους διαχωρίζονται ως εξής:Το bit 1 είναι QR(δηλαδή για Query/Response flag,το bit 2 εως 5 είναι ο κωδικός λειτουργίας,το bit 6 είναι για το authoritative answer, το bit 7 είναι για το truncated,το bit 8 είναι για το recursion desired,το bit 9 είναι για το recursion available,το bit 10 είναι για το Z,το bit 11 είναι για authentic data,το bit 12 είναι για checking disable και τα bit 13-16 είναι response code.Τέλος το number of questions,answer resource records,authority resource records και additional resource records καταλαμβάνουν τα τέσσερα τελευταία πεδία του header.

Ερώτηση(Question)

Εδώ πρέπει να τονίσω ότι στο πρόγραμμα που χρησιμοποιήσαμε το Wireshark, η ερώτηση αναφέρεται ως Query.Η ερώτηση αποτελείται από 3 μέρη που είναι τα εξής,το όνομα ερωτήματος(Name),τον τύπο ερωτήματος(Type),και τέλος την κλάση ερωτήματος(Class).

Εγγραφές Απάντησεις(Answer Resource Records)

Εδώ τα πεδία διαμορφώνονται ως εξής,A που καταλαμβάνει 4 byte, AAAA που καταλαμβάνει 16 byte,MX καταλαμβάνει δύο πεδία δεδομένων, το ένα αποθηκεύει μια τιμή προτεραιότητας και το ένα αποθηκεύει μια διεύθυνση IP,NS καταλαμβάνει ένα πεδίο δεδομένων που αποθηκεύει το όνομα τομέα του έγκυρου διακομιστή ονομάτων,CNAME καταλαμβάνει ένα πεδίο δεδομένων που αποθηκεύει το όνομα τομέα με το οποίο το πεδίο ερώτησης είναι ψευδώνυμο.

Εγγραφές πόρων αρχής(Authority Resource Records)

Αποτελείται από τα NS αρχεία που είναι διαφορετικά από τα αρχεία A καθώς έχουν ένα όνομα τομέα και στα δύο πεδία RR name και RR.

Σε αντίθεση με την answer section, η authority section μπορεί να έχει μόνο αρχεία NS επίσης να αναφαίρουμε ότι τα αρχεία NS μπορούν να σταλούν σε άλλα τμήματα.

Additional Records (Επιπρόσθετες Εγγραφές)

Επιπρόσθετες εγγραφές βοηθούν στην αποφυγή πρόσθετων ανακλήσεων. Αποτελούνται από A ή AAAA αλλά NS αρχεία.

Απάντηση στην ερώτηση 15

Ethernet Header είναι το 48 F8 B3 26 DF 49 BA BA BA BA BA BA 08 00

IP Header είναι το 00 00 38 66 BD 00 00 80 11 02 0C A8 01 34 08 08 08 08 D5 39 00 35 00 24 44 8F 00 03 01 00 00 01 00 00 00 00 00 00 06 67 6F 6F 67 6C 65 03 63 6F 6D 00

Το Transaction ID έχει περιεχόμενο 00 και 03 διότι καταλαμβάνει τα bytes 43-44

Τα flags έχουν περιεχόμενο 01 00 διότι καταλαμβάνουν τα bytes 45-46. Άρα έχουμε ότι το flag 1 είναι OR και με βάση την τιμή είναι query, το flag 2 είναι το Opcode και με βάση την τιμή του είναι normal query, το flag 6 είναι το AA και με βάση την τιμή του

είναι not authoritative answer, το flag 8 είναι το RD και με βάση την τιμή του είναι iterative query και το flag 9 είναι το RA και με βάση την τιμή του είναι recursion not available not authoritative answer, το flag 8 είναι το RD και με βάση την τιμή του είναι iterative query και το flag 9 είναι το RA και με βάση την τιμή του είναι recursion not available. Συνεπώς καταλήγουμε ότι το DNS πακέτο είναι Request και τα 37 bytes είναι DNS Header.

Απάντηση στην ερώτηση 16

Ethernet Header είναι το 48 F8 B3 26 DF 49 BA BA BA BA BA BA 08 00

IP Header είναι το E8 B2 EF 00 00 37 11 FE 21 08 08 08 08 C0 A8 01 34 00 35 D5 39 00 D4 28 A2 00 03 81 80 00 01 00 0B 00 00 00 00 06 67 6F

Το Transaction ID έχει περιεχόμενο 00 και 03 διότι καταλαμβάνει Τα bytes 43-44

Τα flags έχουν περιεχόμενο 81 80 και καταλαμβάνουν τα bytes 45-46. Άρα έχουμε ότι

Το flag 1 είναι QR και με βάση την τιμή του είναι response, το flag 2 είναι το Op code και με βάση την τιμή του είναι normal response, το flag 6 είναι το AA και με βάση την τιμή του είναι not authoritative answer, το flag 8 είναι το RD και με βάση την τιμή του είναι recursive query και το flag 9 είναι το RA και με βάση την τιμή του είναι recursion not available. Συνεπώς καταλήγουμε ότι το DNS πακέτο είναι Request response και τα 86 bytes είναι το DNS Header.

2) Μέρος Εργασίας Δικτύων το πρωτόκολλο IP

Απαντήσεις στην ανάλυση πλαισίου

Η MAC Address παραλήπτη(δηλαδή Destination MAC Address)έχει bytes 1-6.Συνεπώς τα πεδία που περιέχουν τη Destination MAC Address είναι τα 00 A0 92 48 72 45.

Η MAC Address Αποστολέα(δηλαδή Source MAC Address)έχει bytes 7-12.Συνεπώς τα πεδία που περιέχουν τη Source MAC Address είναι τα 00 00 0C 05 C3 58.

Ο Τύπος Πρωτοκόλλου έχει bytes 13-14.Συνεπώς τα πεδία που περιέχουν τον τύπο πρωτοκόλλου είναι 08 00.Αφού η τιμή είναι 08 00 ακολουθεί η κεφαλίδα IP.

Η Header length έχει byte 15.Συνεπώς το πεδίο είναι 45.

Το Total length έχει byte 17-18.Συνεπώς τα 00 29 περιέχουν το συνολικό μέγεθος του frame

Το Time to Live έχει byte 23.Συνεπώς τα πεδία που περιέχουν το Time to Live(δηλαδή TTL) του frame είναι FE

Ο τύπος Πρωτοκόλλου έχει 24 byte.Συνεπώς προκύπτει ότι το πρωτόκολλο είναι TCP και έχει την τιμή 06.

Το Header Checksum έχει 25-26 byte.Συνεπώς τα πεδία που περιέχουν το checksum της κεφαλίδας του Frame είναι τα 7D CB.

Η Source IP(δηλαδή η IP Αποστολέα) έχει 27-30 byte.Συνεπώς τα πεδία που περιέχουν την διεύθυνση του αποστολέα είναι 81 6E 1E 1A.

Η Destination IP(δηλαδή η IP Παραλήπτη έχει 31-34 byte.Συνεπώς τα πεδία που περιέχουν την IP διεύθυνση του παραλήπτη είναι 81 6E 02 11.

Η Source Port (δηλαδή η TCP Θύρα αποστολέα)έχει 35-36 byte.Συνεπώς τα πεδία που περιέχουν την TCP θύρα αποστολέα είναι 02 03.

Η Destination Port(δηλαδή η θύρα δέκτη)έχει 37-38 byte.Συνεπώς τα πεδία που περιέχουν την TCP θύρα δέκτη είναι 00 50.

Το Checksum περιέχει 41-42 byte.Συνεπώς τα πεδία που περιέχουν το checksum είναι τα 7B 57.

Απαντήσεις στις ερωτήσεις 1,2,3,4,5.

1) Η IP διεύθυνση προορισμού έχει τα 31-34 bytes με αντίστοιχο περιεχόμενο να είναι το 81 6E 02 11 και η IP διεύθυνση αποστολής έχει τα 27-30 bytes και αντιστοίχο περιεχόμενο να είναι το 81 6E 1E 1A.

2)Το μήκος του IP μέρους έχει τα bytes 15-34.

3)Αφού ο τύπος Πρωτοκόλλου έχει την τιμή 06 προκύπτει ότι το πρωτόκολλο είναι TCP.

4)Η TCP θύρα αποστολέα έχει bytes 35-36 με αντίστοιχο περιεχόμενο 02 03 ενώ η TCP θύρα παραλήπτη έχει bytes 37-38 με αντίστοιχο περιεχόμενο 00 50.

5)Το Header Checksum έχει 25-26 bytes συνεπώς το περιεχόμενο του είναι 7D CB.Σε δυαδική μορφή το Header Checksum έχει την μορφή 0111 1101 1100 1011.Πρέπει να

δούμε αν ισούται με το 1111 1111 1111 1111.Βλέπουμε ότι δεν είναι ίδια άρα δεν ανιχνεύτηκε σφάλμα κατά την μετάδοση.

2)Μέρος Εργασίας Δικτύων Πείραμα IP με χρήση Wireshark

Απαντήσεις στις ερωτήσεις 1-2 και ερώτηση 3

Πρώτα θα χρησιμοποιήσουμε την εντολή ipconfig/all

```
Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : home
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6205
Physical Address. . . . . : 84-3A-4B-4E-28-BC
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2a02:587:3b23:ecf:54a:3124:ebba:cc44(Preferred)
Temporary IPv6 Address. . . . . : 2a02:587:3b23:ecf:38f4:8a2d:e8da:1d99(Preferred)
Link-local IPv6 Address . . . . . : fe80::54a:3124:ebba:cc44%12(Preferred)
IPv4 Address. . . . . : 192.168.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Σάββατο, 18 Απριλίου 2020 7:07:03 μμ
Lease Expires . . . . . : Δευτέρα, 20 Απριλίου 2020 12:57:14 πμ
Default Gateway . . . . . : fe80::1%12
                          192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 310655563
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-87-68-70-F0-1F-AF-4E-91-61
DNS Servers . . . . . : fe80::1%12
                          192.168.1.1
                          192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

Η MAC address (physical address) της Wi-Fi σύνδεσης στο συγκεκριμένο Η/Υ είναι E8-24-44-F9-D8-F1

Η MAC Address (δηλαδή η physical address) της Wi-Fi σύνδεσης στον υπολογιστή μου είναι η

84-3A-4B-4E-28-BC

Ανοίγω το Wireshark

Ανοίγω με διπλό κλικ την Wireless Network Connection και γράφω στο παράθυρο του Wireshark

την MAC Address της δικής μου Wi-Fi σύνδεσης. Αυτό είναι το φίλτρο που περιέχει τα πακέτα

της MAC του υπολογιστή μου

```
eth.src==84-3A-4B-4E-28-BC
```

Μετά γράφω στο command line γράφω την εντολή tracert -d 83.212.8.210

Παράλληλα με την εντολή που εκτελείται γράφω στο Wireshark το ακόλουθο φίλτρο σύλληψης πακέτων τύπου icmp

No.	Time	Source	Destination	Protocol	Length	Info
128	38.463113	192.168.1.3	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=129/33024, ttl=4 (no response found!)
131	42.358818	192.168.1.3	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=130/33280, ttl=4 (no response found!)
132	42.358837	192.168.1.3	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=130/33280, ttl=4 (no response found!)
151	46.358404	192.168.1.3	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=131/33536, ttl=4 (no response found!)
152	46.358423	192.168.1.3	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=131/33536, ttl=4 (no response found!)
166	50.359012	192.168.1.3	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=132/33792, ttl=5 (no response found!)
167	50.359031	192.168.1.3	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=132/33792, ttl=5 (no response found!)
176	54.358601	192.168.1.3	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=133/34048, ttl=5 (no response found!)
177	54.358620	192.168.1.3	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=133/34048, ttl=5 (no response found!)
193	58.358367	192.168.1.3	83.212.8.210	ICMP	106	Echo (ping) request id=0x0001, seq=134/34304, ttl=5 (no response found!)

Απάντηση στην ερώτηση 4

- ▷ Frame 90: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
- ▷ Ethernet II, Src: IntelCor_4e:28:bc (84:3a:4b:4e:28:bc), Dst: Sercomm_76:75:30 (d4:60:e3:76:75:30)
- ▲ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 83.212.8.210
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - ▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 92
 - Identification: 0x3628 (13864)
 - ▷ Flags: 0x0000
 - Fragment offset: 0
 - ▷ Time to live: 1
 - Protocol: ICMP (1)
 - Header checksum: 0x6528 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.1.3
 - Destination: 83.212.8.210
- ▷ Internet Control Message Protocol

0010	00 5c 36 28 00 00 01 01	65 28 c0 a8 01 03	53 d4	·\6(.... e(....S·
0020	08 d2 08 00 f7 86 00 01	00 78 00 00 00 00 00 00	·x·	
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	·x·	
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	·x·	
0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	·x·	
0060	00 00 00 00 00 00 00 00	00 00	·x·	

Η IP που έχω στον υπολογιστή μου είναι η εξής 192.168.1.3. Αυτή η IP βρίσκεται στα πεδία 27-30 και είναι c0 a8 01 03.

Απάντηση στην ερώτηση 5

- ▷ Time to live: 1
- Protocol: ICMP (1)
- Header checksum: 0x6528 [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.3
- Destination: 83.212.8.210
- ▷ Internet Control Message Protocol

0010	00 5c 36 28 00 00 01 01	65 28 c0 a8 01 03 53 d4	·\6(··· e(····S·
0020	08 d2 08 00 f7 86 00 01	00 78 00 00 00 00 00 00	·x·
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0060	00 00 00 00 00 00 00 00	00 00	

Το Protocol έχει την τιμή 01 και είναι το 24 byte και ο τύπος του πρωτοκόλλου αυτού είναι ICMP(1).

Απάντηση στην ερώτηση 6

Η IP κεφαλίδα έχει μέγεθος 20 bytes

Απάντηση στην ερώτηση 7

Στο πεδίο δεδομένων το IP πακέτο περιέχει 72 bytes

Απάντηση στην ερώτηση 8

Για να βρούμε το συνολικό μέγεθος του πακέτου κάνουμε αφαίρεση,δηλαδή αφαιρούμε τα 20 bytes της κεφαλίδας και έτσι προκύπτει το μέγεθος των data που είναι $92-20=72$

Απάντηση στην ερώτηση 9

Τα πεδία που αλλάζουν απο πακέτο σε πακέτο είναι τα εξής.Το Identification, το Time to live και τέλος το Header checksum.Αυτό που μένει μοναδικό για κάθε νέο πακέτο είναι το Identification.

Απάντηση στην ερώτηση 10

Τα πεδία που μένουν αμετάβλητα απο πακέτο σε πακέτο είναι τα εξής.Το Version header length διότι η κεφαλίδα έχει το ίδιο μέγεθος,το Differentiated Services διότι όλα χρησιμοποιούν τον ίδιο Service class,το Upper Layer Protocol διότι όλα ενσωματώνονται στο UDP, το source IP διότι προέρχεται από τον ίδιο αποστολέα και τέλος το destination IP διότι όλα προορίζονται στον ίδιο παραλήπτη.

Απάντηση στην ερώτηση 11

Τα πεδία που πρέπει να παραμένουν αμετάβλητα είναι τα εξής. Το Version επειδή χρησιμοποιείται για το IPv4 , το header length διότι όλα είναι πακέτα που περιλαμβάνει είναι τύπου ICMP, το Differentiated Services επειδή όλα αυτά τα πακέτα χρησιμοποιούν τον ίδιο τύπο δηλαδή τον τύπο Service class, το Upper Layer Protocol, το source IP επειδή

όπως αναφέραμε προέρχονται όλα από τον ίδιο αποστολέα και το destination IP διότι προορίζεται για τον ίδιο παραλήπτη.

Απάντηση στην ερώτηση 12

Τα πεδία που πρέπει να αλλάξουν είναι το (TTL) δηλαδή Time to live επειδή σε κάθε νέο πακέτο αυξάνονται τα hops, το Identification αφού τα πακέτα IP έχουν διαφορετικά ids, και τέλος το Header checksum επειδή αλλάζει η κεφαλίδα.

Απάντηση στην ερώτηση 13

Όπως αποδεικνύεται από το screenshot η διεύθυνση του κοντινότερου δρομολογητή είναι 83.212.8.210

Destination: 83.212.8.210

Απάντηση στην ερώτηση 14

Όπως αποδεικνύεται από το screenshot η τιμή για το TTL του 1 πακέτου είναι 1.

▶ Time to live: 1

Απάντηση στην ερώτηση 15

Αυτό που αλλάζει είναι το πεδίο identification για τα responses τύπου ICMP TTL-exceeded.

3) Μέρος Εργασίας Δικτύων Cisco Packet Tracer Υλοποίηση Hub

Παραθέτω screenshot με όλα τα ping από το PC0

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=16ms TTL=128
Reply from 192.168.1.1: bytes=32 time=3ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 4ms
```

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=47ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 47ms, Average = 12ms
```

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

I.(192.168.1.) Σε ποιόν απευθύνεται αυτό το ping;

Στο PC1

Στο PC2

Στο PC3

Στο τοπικό Interface του PC0

Απάντηση

Το ping 192.168.1.1 απευθύνεται στο τοπικό Interface του PC0 επειδή η IP 192.168.1 είναι αυτή που βάλαμε στην Fast Ethernet0 που είναι διεπαφή του PC0

II.(192.168.1.2) Έχουμε απάντηση;

ΝΑΙ

ΌΧΙ

Δικαιολογήστε τις απαντήσεις σας.

Απάντηση

ΝΑΙ και το παρακάτω screenshot το αποδεικνύει

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=47ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 47ms, Average = 12ms
```

III.(192.168.1.3) Έχουμε απάντηση;

ΝΑΙ

ΌΧΙ

Δικαιολογήστε τις απαντήσεις σας.

Απάντηση

ΝΑΙ και το παρακάτω screenshot το αποδεικνύει

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

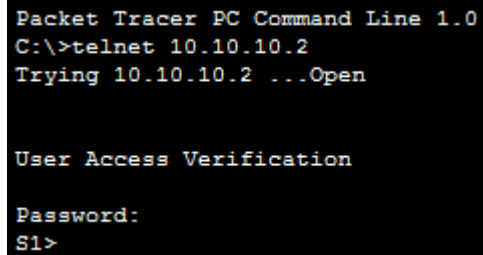
4) Μέρος Εργασίας Δικτύων Packet Tracer Configure SSH

Κομμάτι Πρώτο:Ασφαλείς Κωδικοί Πρόσβασης

Χρησιμοποιώντας τη γραμμή εντολών στο PC1, κάντε Telnet στο S1. Ο κωδικός για τον χρήστη EXEC είναι cisco.

ΕΝΤΟΛΕΣ

C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open
User Access Verification
Password: (εδώ γράψαμε cisco)
S1>



```
Packet Tracer PC Command Line 1.0
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open

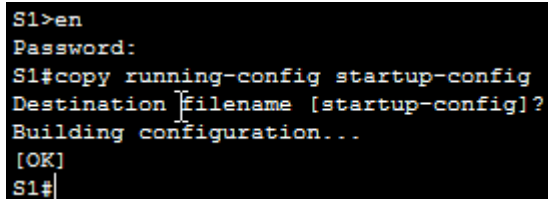
User Access Verification

Password:
S1>
```

Αποθηκεύστε την τρέχουσα διαμόρφωση, έτσι ώστε τυχόν σφάλματα που μπορεί να κάνετε μπορούν να αντιστραφούν με την εναλλαγή της ισχύος για το S1.

ΕΝΤΟΛΕΣ

S1>en
Password: (εδώ γράψαμε cisco)
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#



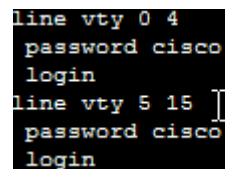
```
S1>en
Password:
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Εμφανίστε την τρέχουσα διαμόρφωση και σημειώστε ότι οι κωδικοί πρόσβασης είναι σε απλό κείμενο.

ΕΝΤΟΛΕΣ

show running-config
το αποτέλεσμα της εκτέλεσης είναι:

line vty 0 4
password cisco
login
line vty 5 15
password ciscologin



```
line vty 0 4
password cisco
login
line vty 5 15
password ciscologin
```

Οι κωδικοί είναι σε απλό κείμενο
Εισαγάγετε την εντολή που κρυπτογραφεί τους κωδικούς πρόσβασης απλού κειμένου: S1(config)# service password-encryption
Βεβαιωθείτε ότι οι κωδικοί πρόσβασης είναι κρυπτογραφημένοι.

ΕΝΤΟΛΕΣ

S1#conf ter

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#service password-encryption

```
S1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)#service password-encryption
```

για να βεβαιωθούμε ότι οι κωδικοί πρόσβασης είναι κρυπτογραφημένοι δίνουμε τις εντολές:

S1(config)#exit

S1#show running-config

```
S1(config)#exit
S1#show running-config
```

και το αποτέλεσμα που λαμβάνουμε είναι το εξής:

line con 0

!

line vty 0 4

password 7 0822455D0A16

login

line vty 5 15

password 7 0822455D0A16

login

```
line con 0
!
line vty 0 4
password 7 0822455D0A16
login
line vty 5 15
password 7 0822455D0A16
login
```

Οι κωδικοί είναι κρυπτογραφημένοι

Κομμάτι Δεύτερο:Κρυπτογράφηση επικοινωνιών

Διαμορφώστε το όνομα τομέα ως netacad.pka.

ΕΝΤΟΛΕΣ

S1# conf ter

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#ip domain-name netacad.pka

S1(config)#

```
S1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip domain-name netacad.pka
S1(config)#
```

**Απαιτούνται κλειδιά ασφαλείας για την κρυπτογράφηση των δεδομένων.
Δημιουργήστε τα κλειδιά RSA χρησιμοποιώντας ένα μήκος 1024.**

ΕΝΤΟΛΕΣ

S1(config)#crypt key generate rsa

The name for the keys will be: S1.netacad.pka

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```
S1(config)#crypt key generate rsa
The name for the keys will be: S1.netacad.pka
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Δημιουργήστε έναν χρήστη SSH και επαναρυθμίστε τις γραμμές VTY για πρόσβαση μόνο SSH.

ΕΝΤΟΛΕΣ

S1(config)#username up1058102 secret up1058102

*Mar 1 9:12:52.981: %SSH-5-ENABLED: SSH 1.99 has been enabled

```
S1(config)#username up1058102 secret up1058102
*Mar 1 9:12:52.981: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Δημιουργήστε έναν χρήστη διαχειριστή με Cisco ως “μυστικό” κωδικό πρόσβασης.

ΕΝΤΟΛΕΣ

S1(config)#username administrator secret Cisco

```
S1(config)#username administrator secret Cisco
```

Ρυθμίστε τις γραμμές VTY για να ελέγξετε την τοπική βάση δεδομένων ονόματος χρήστη για τα διαπιστευτήρια σύνδεσης και για να επιτρέψετε μόνο SSH για απομακρυσμένη πρόσβαση. Καταργήστε τον υπάρχοντα κωδικό πρόσβασης γραμμής vty.

ΕΝΤΟΛΕΣ

S1(config)#line vty 0 15

S1(config-line)#login local

S1(config-line)#transport input ssh

S1(config-line)#no password cisco

```
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#no password cisco
```

Κομμάτι Τρίτο: Επαλήθευση της εφαρμογής SSH

Πραγματοποιήστε έξοδο από την περίοδο λειτουργίας Telnet και προσπαθήστε να συνδεθείτε ξανά χρησιμοποιώντας το Telnet. Η προσπάθεια πρέπει να αποτύχει.

ΕΝΤΟΛΕΣ

```
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open
[Connection to 10.10.10.2 closed by foreign
host]
```

```
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open
[Connection to 10.10.10.2 closed by foreign host]
```

Προσπαθήστε να συνδεθείτε χρησιμοποιώντας SSH. Πληκτρολογήστε ssh και πατήστε Enter χωρίς παραμέτρους για να αποκαλύψετε τις οδηγίες χρήσης εντολών. Συμβουλή: Η επιλογή -l είναι το γράμμα "l", όχι ο αριθμός 1.

ΕΝΤΟΛΕΣ

```
C:\>ssh
Packet Tracer PC SSH
Usage: SSH -l username target
```

```
C:\>ssh
Packet Tracer PC SSH
Usage: SSH -l username target
```

Μετά την επιτυχή σύνδεση, εισαγάγετε την προνομιακή λειτουργία EXEC και αποθηκεύστε τη διαμόρφωση. Αν δεν μπορείτε να έχετε επιτυχή πρόσβαση στο S1, κάντε εναλλαγή της τροφοδοσίας και έναρξη πάλι όπως στο Μέρος 1.

Αν μπούμε με το username up1058102 και password up1058102 τότε θα έχουμε

```
C:\>ssh -l up1058102 10.10.10.2
Password:
S1>
```

```
C:\>ssh -l up1058102 10.10.10.2
Password:
S1>
```

Αν μπούμε με το username administrator και password Cisco τότε θα έχουμε

```
C:\>ssh -l administrator 10.10.10.2
Password:
S1>
Βλέπουμε οτι και οι 2 χρήστες
καταχωρήθηκαν επιτυχώς για ssh
```

```
C:\>ssh -l administrator 10.10.10.2
Password:
S1>
```