

εργασία για το μάθημα
Διαχείρισης Δικτύων



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικό και Καποδιστριακό
Πανεπιστήμιο Αθηνών

Τσαούσης Λεωνίδας
Α.Μ.: 1115201200184
Εαρινό εξάμηνο 2015-'16



ΤΜΗΜΑ
ΠΛΗΡΟΦΟΡΙΚΗΣ &
ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Αντικείμενο της εργασίας

- **Εκτέλεση** εργαλείων παρακολούθησης δικτύων και ανίχνευσης πακέτων (sniffers).
- **Καταγραφή** δεδομένων για την ύπαρξη και χρήση ασύρματων δικτύων αλλά και των υπολογιστών/εφαρμογών που είναι συνδεδεμένοι στα τοπικά αυτά δίκτυα.
Παρακολούθηση:
 - της χρήσης καναλιών, ισχύς σήματος, κάλυψης κτλ. των ασύρματων δικτύων
 - πρωτόκολλα που χρησιμοποιήθηκαν για την πρόσβαση στον ιστό, υπηρεσίες και στατιστικά
 - συσκευές που συνδέθηκαν, user agents
- Δημιουργία **βάσης δεδομένων** και εισαγωγή των παραπάνω καταγεγραμμένων στοιχείων σ'αυτην.
- **Σχεδιασμός εφαρμογής** για την παρουσίαση, επεξεργασία και λήψη αποφάσεων.
- Συσχέτιση των δράσεων αυτών/ευθυγράμμιση τους με το **θεωρητικό υπόβαθρο** (π. χ. μοντέλο *FCAPS*) της διαχείρισης δικτύων

Καταγραφή δεδομένων



Με το λογισμικό
Wireshark

Ενεργοποίηση του monitor mode/promiscuous mode στις κάρτες δικτύου

Start Stop Restart Options Open Save Close Reload Find Packet... Previous Packet Next Packet Go to Packet... First Packet Last Packet Auto Scroll

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info
25	19:51:20.6932	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TLSv1.2	Application Data
26	19:51:20.8803	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TCP	[TCP ACKed unseen segment] 443 → 51249 [ACK] Seq=1 Ack=214 Win=1641 Len=0 TSV=1910461639
27	19:51:20.8125	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TCP	443 → 51249 [ACK] Seq=1 Ack=1012 Win=1035 Len=0 TSV=1910461639 TSecr=2803024
28	19:51:20.8125	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TLSv1.2	Application Data
29	19:51:20.8284	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TCP	443 → 51249 [ACK] Seq=39 Ack=3028 Win=1641 Len=0 TSV=1910461655 TSecr=2803024
30	19:51:20.8502	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TCP	51249 → 443 [ACK] Seq=3028 Ack=39 Win=11297 Len=0 TSV=1910461639 TSecr=1910461639
31	19:51:21.1862	192.168.1.3	192.241.189.82	TCP	39861 → 443 [ACK] Seq=1 Ack=1 Win=319 Len=0 TSV=1910461639 TSecr=3598454239
32	19:51:21.3335	192.241.189.82	192.168.1.3	TCP	[TCP ACKed unseen segment] 443 → 39861 [ACK] Seq=1 Ack=2 Win=12 Len=0 TSV=1910461639 TSecr=3598454239
33	19:51:21.4687	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TLSv1.2	Application Data
34	19:51:21.4687	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TCP	51249 → 443 [ACK] Seq=3028 Ack=97 Win=11297 Len=0 TSV=1910462295 TSecr=1910462295
35	19:51:21.4688	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TLSv1.2	Application Data
36	19:51:21.4688	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TCP	51249 → 443 [ACK] Seq=3028 Ack=127 Win=11297 Len=0 TSV=1910462295 TSecr=1910462295
37	19:51:21.4688	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TLSv1.2	Application Data
38	19:51:21.4688	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TCP	51249 → 443 [ACK] Seq=3028 Ack=165 Win=11297 Len=0 TSV=1910462295 TSecr=1910462295
39	19:51:21.4700	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TLSv1.2	Application Data
40	19:51:21.6212	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TCP	443 → 51249 [ACK] Seq=165 Ack=3066 Win=1641 Len=0 TSV=1910462447 TSecr=2803218
41	19:51:26.4051	192.168.1.3	54.186.17.145	TCP	48606 → 80 [FIN, ACK] Seq=1 Ack=1 Win=237 Len=0 TSV=1910462447 TSecr=1910462447
42	19:51:26.4052	192.168.1.3	52.6.238.110	TCP	38712 → 80 [FIN, ACK] Seq=1 Ack=1 Win=248 Len=0 TSV=1910462447 TSecr=1910462447
43	19:51:26.4056	fe80::222:faf::fe80::1	fe80::1	DNS	Standard query 0xa0df A api.ipinfodb.com
44	19:51:26.4056	fe80::222:faf::fe80::1	fe80::1	DNS	Standard query response 0xa0df A api.ipinfodb.com
45	19:51:26.4117	fe80::1	fe80::222:faf::fe80::1	DNS	Standard query response 0xa0df A api.ipinfodb.com
46	19:51:26.4117	fe80::1	fe80::222:faf::fe80::1	DNS	Standard query response 0xa0df A api.ipinfodb.com
47	19:51:26.4137	192.168.1.3	104.238.195.60	TCP	42027 → 80 [SYN] Seq=0 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSV=1910462447 TSecr=1910462447
48	19:51:26.4737	2a02:587:dea::2a00:1450:4017:803::2004	2a02:587:dea::2a00:1450:4017:803::2004	HTTP	GET /search?client=navclient-auto&lench=64148744987&ie=UTF-8&oe=UTF-8&features=Rank&q=info: http://filehippo.com HTTP/1.1\r\n
49	19:51:26.5660	52.6.238.110	192.168.1.3	TCP	80 → 38712 [ACK] Seq=1 Ack=2 Win=75 Len=0 TSV=191511695 TSecr=2804452
50	19:51:26.5877	2a02:587:dea::2a00:1450:4017:802::200e	2a02:587:dea::2a00:1450:4017:802::200e	TCP	80 → 38590 [ACK] Seq=1 Ack=820 Win=950 Len=0 TSV=1918641494 TSecr=2804460
51	19:51:26.6286	104.238.195.60	192.168.1.3	TCP	80 → 42027 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
52	19:51:26.6286	104.238.195.60	192.168.1.3	TCP	42027 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0
53	19:51:26.6289	104.238.195.60	192.168.1.3	HTTP	GET /v2/ip_query.php?key=dc76799dd2e27326bbdbd952307d129f7a217ae44ee84bde24bc3e2f013c\r\n
54	19:51:26.6309	54.186.17.145	192.168.1.3	TCP	80 → 48606 [ACK] Seq=1 Ack=2 Win=75 Len=0 TSV=191761118 TSecr=2804452
55	19:51:26.8525	104.238.195.60	192.168.1.3	TCP	80 → 42027 [ACK] Seq=1 Ack=421 Win=15744 Len=0
56	19:51:26.8525	104.238.195.60	192.168.1.3	TCP	80 → 42027 [FIN, ACK] Seq=1 Ack=421 Win=15744 Len=0
57	19:51:26.8541	192.168.1.3	104.238.195.60	TCP	42027 → 80 [ACK] Seq=421 Ack=2 Win=29312 Len=0

Frame 48: 905 bytes on wire (7240 bits), 905 bytes captured (7240 bits) on interface 0

Ethernet II, Src: 08:00:27:14:0b:06, Dst: 08:00:27:14:0b:06

Internet Protocol Version 6, Src: 2a02:587:dea::2a00:1450:4017:803::2004

Transmission Control Protocol, Src Port: 38590 (38590), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 819

Hypertext Transfer Protocol

GET /search?client=navclient-auto&lench=64148744987&ie=UTF-8&oe=UTF-8&features=Rank&q=info: http://filehippo.com HTTP/1.1\r\n

Host: toolbarqueries.google.com\r\n

Connection: keep-alive\r\n

User-Agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/51.0.2704.79 Chrome/51.0.2704.79 Safari/537.36\r\n

Accept: */*\r\n

Accept-Encoding: gzip, deflate, sdch\r\n

Accept-Language: el,en;q=0.8\r\n

wireshark.pcapng_wlan0_20160807195113_jd56W4

Packets: 3073 · Display

ΑΠΟ ΤΟ ΟΙΚΙΑΚΟ ΔΙΤΚΥΟ...

- view/capture filters, configuration profiles για 802.11 κίνηση

<https://wiki.wireshark.org/CaptureSetup/WLAN>

Wireshark interface showing a capture of 802.11 WLAN traffic. The packet list displays various frames, including 802.11 Probe Response, Authentication, Association Request, and EAPOL (Extensible Authentication Protocol) frames. The packet details pane shows the structure of an IEEE 802.11 QoS Data frame, including the Type/Subtype (QoS Data), Frame Control Field, and various addresses (Receiver, Destination, Transmitter, Source).

No.	Source	Destination	Protocol	Length	Channel	Info
270	a4:7e:39:da:fd:a8	ac:0d:1b:e6:86:4c	802.11	291	11	Probe Response, SN=1577, FN=0, Flags=.....C, BI=100, SSID=...
272	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	63	11	Authentication, SN=476, FN=0, Flags=.....C
274	a4:7e:39:da:fd:a8	ac:0d:1b:e6:86:4c	802.11	52	11	Authentication, SN=1580, FN=0, Flags=.....C
276	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	101	11	Association Request, SN=477, FN=0, Flags=.....C, SSID=...
278	a4:7e:39:da:fd:a8	ac:0d:1b:e6:86:4c	802.11	231	11	Association Response, SN=1581, FN=0, Flags=.....C
280	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	46	11	Null function (No data), SN=476, FN=0, Flags=.....TC
282	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	46	11	Null function (No data), SN=479, FN=0, Flags=.....TC
295	a4:7e:39:da:fd:a8	ac:0d:1b:e6:86:4c	EAPOL	155	11	Key (Message 1 of 4)
297	a4:7e:39:da:fd:a8	ac:0d:1b:e6:86:4c	802.11	55	11	Action, SN=1582, FN=0, Flags=.....C
299	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	55	11	Action, SN=480, FN=0, Flags=.....C
303	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	55	11	Action, SN=481, FN=0, Flags=.....C
305	a4:7e:39:da:fd:a8	ac:0d:1b:e6:86:4c	802.11	55	11	Action, SN=1584, FN=0, Flags=.....C
307	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	EAPOL	179	11	Key (Message 2 of 4)
311	a4:7e:39:da:fd:a8	ac:0d:1b:e6:86:4c	EAPOL	183	11	Key (Message 3 of 4)
313	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	EAPOL	155	11	Key (Message 4 of 4)
315	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	46	11	Null function (No data), SN=482, FN=0, Flags=.....TC
317	a4:7e:39:da:fd:a8	ac:0d:1b:e6:86:4c	EAPOL	211	11	Key (Group Message 1 of 2)
319	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	46	11	Null function (No data), SN=483, FN=0, Flags=.....TC
321	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	EAPOL	171	11	Key (Group Message 2 of 2)
323	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	46	11	Null function (No data), SN=484, FN=0, Flags=.....TC
351	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	46	11	Null function (No data), SN=485, FN=0, Flags=.....P...TC
379	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	46	11	Null function (No data), SN=486, FN=0, Flags=.....TC
384	192.168.1.1	192.168.1.4	DHCP	648	11	DHCP ACK - Transaction ID 0x521a94f5
390	a4:7e:39:da:fd:a8	ac:0d:1b:e6:86:4c	ARP	100	11	192.168.1.1 is at a4:7e:39:da:fd:a8
392	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	55	11	Action, SN=487, FN=0, Flags=.....C
394	192.168.1.4	192.168.1.1	ICMP	651	11	Destination unreachable (Port unreachable)
396	a4:7e:39:da:fd:a8	ac:0d:1b:e6:86:4c	802.11	55	11	Action, SN=1586, FN=0, Flags=.....C
413	ac:0d:1b:e6:86:4c	a4:7e:39:da:fd:a8	802.11	46	11	Null function (No data), SN=488, FN=0, Flags=.....P...TC
418	192.168.1.4	192.168.1.1	DNS	151	11	Standard query 0xc5e2 A clients3.google.com

Frame 321: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface 0
▶ Radiotap Header v0, Length 18
▶ 802.11 radio information
▼ IEEE 802.11 QoS Data, Flags: .p....TC
Type/Subtype: QoS Data (0x0028)
▶ Frame Control Field: 0x0041
...0001 0011 1010 = Duration: 314 microseconds
Receiver address: a4:7e:39:da:fd:a8
Destination address: a4:7e:39:da:fd:a8
Transmitter address: ac:0d:1b:e6:86:4c
Source address: ac:0d:1b:e6:86:4c

...αλλα και απο γειτονικά

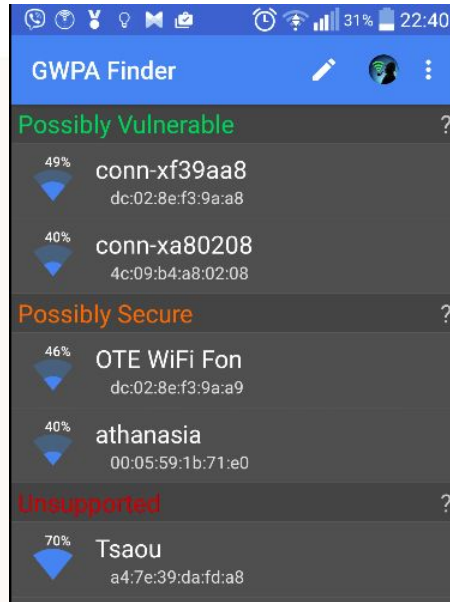
- Channel Hopping

```
1 #!/bin/bash
2
3 IFACE=wlan0
4 SEC=0.5
5
6 IEEE80211bg="1 2 3 4 5 6 7 8 9 10 11"
7 IEEE80211bg_intl="$IEEE80211bg 12 13 14"
8 IEEE80211bg_eu="$IEEE80211bg 12 13"
9
10 IEEE80211a="36 40 44 48 52 56 60 64 149 153 157 161"
11 IEEE80211bga="$IEEE80211bg $IEEE80211a"
12 IEEE80211bga_intl="$IEEE80211bg_intl $IEEE80211a"
13
14 ifconfig $IFACE down
15 iwconfig $IFACE mode monitor
16 ifconfig $IFACE up
17
18 while true ; do
19     for CHAN in $IEEE80211bg_eu ; do
20         echo "Switching to channel $CHAN"
21         iwconfig $IFACE channel $CHAN
22         sleep $SEC
23     done
24 done
```

~/chanho2.sh [sh] enH row:17/24 col:001 [+]
-- INSERT --



- WiFi keys



Βάση δεδομένων

MySQL server / client



MySQL Workbench για τον σχεδιασμό του μοντέλου

```
root@ip-10-43-142: ~
mysql> select name, alias, passwd from users where name='zabbix';
+-----+-----+-----+
| name | alias | passwd |
+-----+-----+-----+
| Zabbix | Admin | berkshire |
+-----+-----+-----+
1 row in set (0.00 sec)

mysql>

Broadcast Message from root@ip-1
(somewhere) at 10:06 ...

You have about 10 minutes before instance termination

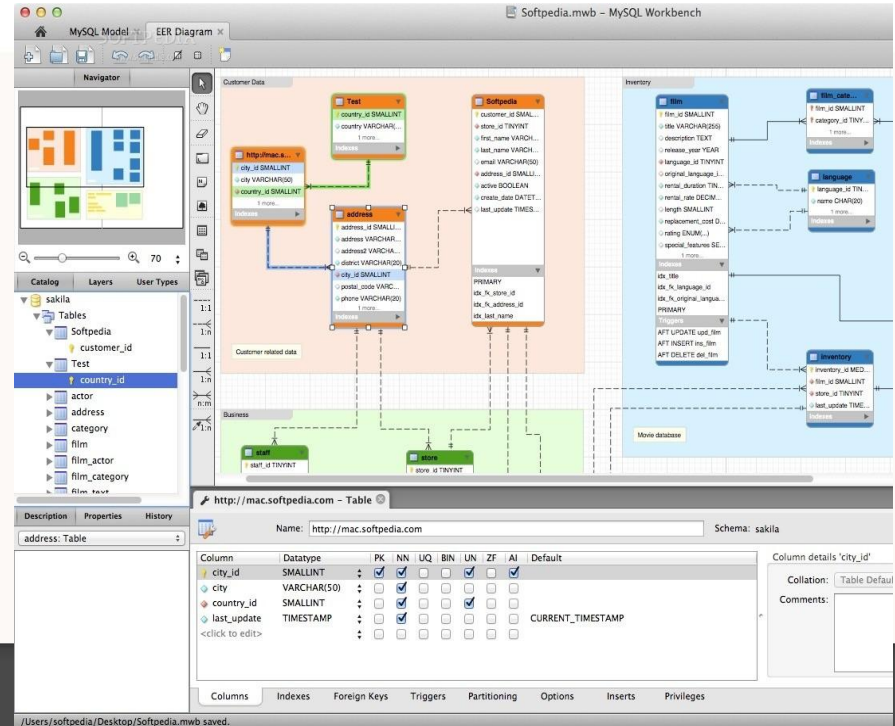
% 'zabbix';
ERROR 1054 (42S22): Unknown column 'MD' in 'where clause'
mysql>
mysql> update users set passwd='berkshire' where name=MD5('zabbix');
Query OK, 0 rows affected (0.00 sec)
Rows matched: 0 Changed: 0 Warnings: 0

mysql> select name, alias, passwd from users where name='zabbix';
+-----+-----+-----+
| name | alias | passwd |
+-----+-----+-----+
| Zabbix | Admin | berkshire |
+-----+-----+-----+
1 row in set (0.00 sec)

mysql> update users set passwd=MD5('berkshire') where name='Zabbix';
Query OK, 1 row affected (0.00 sec)
Rows matched: 1 Changed: 1 Warnings: 0

mysql> select name, alias, passwd from users where name='zabbix';
+-----+-----+-----+
| name | alias | passwd |
+-----+-----+-----+
| Zabbix | Admin | 4695d8d2b959dabb53cf9650201a53a8 |
+-----+-----+-----+
1 row in set (0.00 sec)

mysql>
```



Management Console



Linux



Apache



MySQL



PHP

- LAMP server
- Automates DB population
- Some DB operations (e.g. 'Empty')
- Visualizes information
- Ease-of-use

Management Console

FCAPS model WiFi Analysis Captured Data

Fault

Configuration

Accounting

Performance

Security

FCAPS reference model

According to wikipedia:

^ The five areas of function of the model

The OSI network management model categorizes five areas of function, sometimes referred to as the "FCAPS model." FCAPS can be seen as the predecessor of the newer FAB model defined in the [Business Process Framework \(eTOM\)](#). FAB is short for fulfillment, assurance, billing. As guideline, you can map the two models as follows:

FCAPS	FAB
Fault	Assurance
Configuration	Fulfillment
Accounting	Billing
Performance	Assurance
Security	Fulfillment

The FCAPS model can be seen as bottom-up or network-centric. The FAB model looks at the processes more from top-down, is customer/business-centric. The two

Live Demo

1. Open MySQL Workbench > `quick_queries.sql` + `mib.mwb`
2. Open Management Console (look around > Index)
3. FCAPS > Fault > Analyze
 - Tsaou
 - tasoswaterski
4. Empty DB
5. Show .xml, Populate DB (ether.xml)
6. FCAPS > Conf > Analyze
 - Tsaou
 - Vergis
- ...
7. Show Code (PHP + CSS + HTML + SQL)
8. Take a closer look!



Συλλογή δεδομένων

Εκτέλεση Wireshark (λάπτοπ = “router”) σε

- διάφορα δίκτυα
 - a. σπιτιού μου
 - b. σπίτια φίλων
 - c. δίκτυο καφετέριας
- τρέχοντας στο λάπτοπ μου διάφορες διεργασίες
 - a. browsing
 - b. torrents
 - c. streaming (internet radio)
 - d. χρήση εκτυπωτών
 - e. pings
- κάνοντας σε άλλες συνδεδεμένες συσκευές (smartphones) διάφορες διεργασίες

Capturing configurations: 2 είδη

1. στην wlan0 με monitor mode και link-layer header: *802.11+radiotap*
2. στην wlan0 χωρίς monitor mode και link-layer header: ethernet (pseudo)

Αλλαζοντας το channel κάθε 5 λεπτά μεχρι να τα καλύψω ολα

Για να πιάσω 802.11 Headers με info οπως:

- ❖ signal strength
- ❖ SSIDs
- ❖ data rates
- ❖ encryption types