



ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΕΡΓΑΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΩΝ

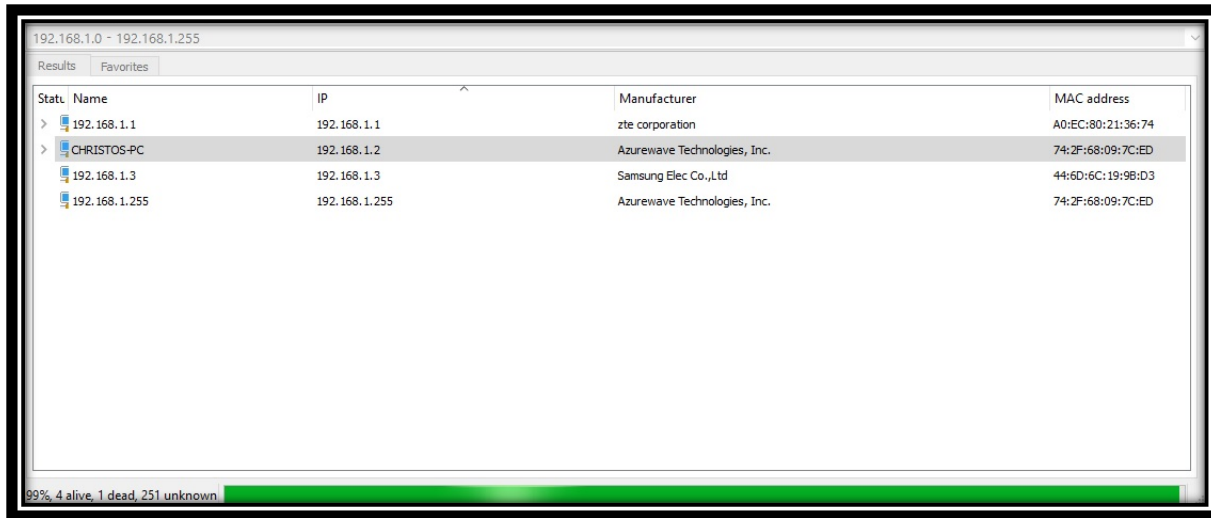
ΓΑΛΑΝΗ ANNA-ΜΑΡΙΑ
ΠΑΤΣΟΥΡΑΣ ΧΡΗΣΤΟΣ

1115201300231
1115201100132

ΔΙΔΑΣΚΟΥΣΑ: ΝΑΝΣΥ ΑΛΩΝΙΣΤΙΩΤΗ

ΕΡΓΑΛΕΙΑ ΜΕΤΡΗΣΕΩΝ (1/4)

Advanced IP Scanner



Statu	Name	IP	Manufacturer	MAC address
>	192.168.1.1	192.168.1.1	zte corporation	A0:EC:80:21:36:74
>	CHRISTOS-PC	192.168.1.2	Azurewave Technologies, Inc.	74:2F:68:09:7C:ED
	192.168.1.3	192.168.1.3	Samsung Elec Co.,Ltd	44:6D:6C:19:9B:D3
	192.168.1.255	192.168.1.255	Azurewave Technologies, Inc.	74:2F:68:09:7C:ED

99% 4 alive, 1 dead, 251 unknown



Program



XML output

```
<?xml version="1.0" encoding="UTF-8"?>
<Advanced_IP_scanner>
  <row status="unknown" name="192.168.1.0" ip="192.168.1.0" mac="00:00:00:00:00:00" has_http="0" is_http8080="0" has_https="0" has_ftp="0" has_rdp="0">
  </row>
  <row status="alive" name="192.168.1.1" ip="192.168.1.1" manufacturer="zte corporation" mac="A0:EC:80:21:36:74" has_http="1" is_http8080="0" http_title="Prot
  </row>
  <row status="alive" name="CHRISTOS-PC" ip="192.168.1.2" manufacturer="Azurewave Technologies, Inc." mac="74:2F:68:09:7C:ED" has_http="0" is_http8080="0" has
  <share name="Users"/>
  </row>
  <row status="alive" name="192.168.1.3" ip="192.168.1.3" manufacturer="Samsung Elec Co.,Ltd" mac="44:6D:6C:19:9B:D3" has_http="0" is_http8080="0" has_https="
  </row>
  <row status="unknown" name="192.168.1.4" ip="192.168.1.4" mac="00:00:00:00:00:00" has_http="0" is_http8080="0" has_https="0" has_ftp="0" has_rdp="0">
  </row>
  <row status="unknown" name="192.168.1.5" ip="192.168.1.5" mac="00:00:00:00:00:00" has_http="0" is_http8080="0" has_https="0" has_ftp="0" has_rdp="0">
  </row>
  <row status="alive" name="CHRISTOS-PC" ip="192.168.1.6" manufacturer="LEXMARK INTERNATIONAL, INC." mac="00:20:00:AD:2A:2F" has_http="1" is_http8080="0" http
  </row>
  <row status="unknown" name="192.168.1.7" ip="192.168.1.7" mac="00:00:00:00:00:00" has_http="0" is_http8080="0" has_https="0" has_ftp="0" has_rdp="0">
  </row>
  <row status="unknown" name="192.168.1.8" ip="192.168.1.8" mac="00:00:00:00:00:00" has_http="0" is_http8080="0" has_https="0" has_ftp="0" has_rdp="0">
  </row>
  <row status="unknown" name="192.168.1.9" ip="192.168.1.9" mac="00:00:00:00:00:00" has_http="0" is_http8080="0" has_https="0" has_ftp="0" has_rdp="0">
  </row>
  <row status="unknown" name="192.168.1.10" ip="192.168.1.10" mac="00:00:00:00:00:00" has_http="0" is_http8080="0" has_https="0" has_ftp="0" has_rdp="0">
  </row>
</Advanced_IP_scanner>
```

ΕΡΓΑΛΕΙΑ ΜΕΤΡΗΣΕΩΝ (2/4)

Wireshark

Time	Source	Src Port	Destination	Info	Dst Port	Length	Protocol
2016-06-27 13:53:51.4...	192.168.1.1		224.0.0.12	Membership Report group 224.0.0.12		60	IGMPv2
2016-06-27 13:53:51.4...	192.168.1.3	5353	224.0.0.251	Standard query 0x0000 PTR_805741C9_sub_googlecast_tcp.local, "QM" questi...	5353	119	MDNS
2016-06-27 13:53:51.8...	62.1.38.49	80	192.168.1.2	80 > 63629 [ACK] Seq=1 Ack=1 Win=980 Len=0	63629	60	TCP
2016-06-27 13:53:51.8...	192.168.1.2	63629	62.1.38.49	[TCP ZeroWindow] [TCP ACKed unseen segment] 63629 > 80 [ACK] Seq=1 Ack=2 Win=...	80	54	TCP
2016-06-27 13:53:53.2...	2a03:2880:f01c:20e:face:b00c:0:2	443	2a02:214d:8117:f00...	Application Data	63672	176	TLSv1
2016-06-27 13:53:53.2...	2a02:214d:8117:f00:789e:6030:366d:7455	63672	2a03:2880:f01c:20e:...	63672 > 443 [ACK] Seq=1 Ack=103 Win=255 Len=0	443	74	TCP
2016-06-27 13:53:53.4...	192.168.1.2	64111	204.79.197.200	64111 > 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1	443	66	TCP
2016-06-27 13:53:53.4...	192.168.1.2	64112	204.79.197.200	64112 > 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1	443	66	TCP
2016-06-27 13:53:53.5...	204.79.197.200	443	192.168.1.2	443 > 64111 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1	64111	66	TCP
2016-06-27 13:53:53.5...	192.168.1.2	64111	204.79.197.200	64111 > 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0	443	54	TCP
2016-06-27 13:53:53.5...	192.168.1.2	64111	204.79.197.200	Client Hello	443	303	TLSv1
2016-06-27 13:53:53.5...	192.168.1.3		224.0.0.2	Leave Group 224.0.0.251		46	IGMPv2
2016-06-27 13:53:53.5...	204.79.197.200	443	192.168.1.2	443 > 64112 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1	64112	66	TCP
2016-06-27 13:53:53.5...	192.168.1.2	64112	204.79.197.200	64112 > 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0	443	54	TCP
2016-06-27 13:53:53.5...	192.168.1.2	64112	204.79.197.200	Client Hello	443	303	TLSv1

> Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: ZteCorpo_21:36:74 (a0:ec:80:21:36:74), Dst: Azurewav_09:7c:ed (74:2f:68:09:7c:ed)
> Internet Protocol Version 4, Src: 204.79.197.200, Dst: 192.168.1.2
> Transmission Control Protocol, Src Port: 443 (443), Dst Port: 64111 (64111), Seq: 0, Ack: 1, Len: 0

Program

1	Time	Source	Src Port	Destination	Info
2	2016-06-27 13:53:51.1862	192.168.1.1		224.0.0.12	Membership Report group 224.0.0.12
3	2016-06-27 13:53:51.4892	192.168.1.3	5353	224.0.0.251	Standard query 0x0000 PTR_805741C9_sub_googlecast_tcp.local, "QM" question PTR_233637DE_sub_googlecast_tcp.local, "QM" question PTR
4	2016-06-27 13:53:51.8627	192.168.1.2	80	192.168.1.2	80 > 63629 [ACK] Seq=1 Ack=1 Win=980 Len=0
5	2016-06-27 13:53:51.8627	192.168.1.2	63629	62.1.38.49	[TCP ZeroWindow] [TCP ACKed unseen segment] 63629 > 80 [ACK] Seq=1 Ack=2 Win=0 Len=0
6	2016-06-27 13:53:53.2067	2a03:2880:f01c:20e:face:b00c:0:2	443	2a02:214d:8117:f00:789e:6030:366d:7455	Application Data
7	2016-06-27 13:53:53.2411	2a02:214d:8117:f00:789e:6030:366d:7455	63672	2a03:2880:f01c:20e:face:b00c:0:2	63672 > 443 [ACK] Seq=1 Ack=103 Win=255 Len=0
8	2016-06-27 13:53:53.4418	192.168.1.2	64111	204.79.197.200	64111 > 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	2016-06-27 13:53:53.4831	192.168.1.2	64112	204.79.197.200	64112 > 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	2016-06-27 13:53:53.5132	204.79.197.200	443	192.168.1.2	443 > 64111 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1
11	2016-06-27 13:53:53.5136	192.168.1.2	64111	204.79.197.200	64111 > 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
12	2016-06-27 13:53:53.5136	192.168.1.2	64111	204.79.197.200	Client Hello
13	2016-06-27 13:53:53.5434	192.168.1.3		224.0.0.2	Leave Group 224.0.0.251
14	2016-06-27 13:53:53.5539	204.79.197.200	443	192.168.1.2	443 > 64112 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1
15	2016-06-27 13:53:53.5540	192.168.1.2	64112	204.79.197.200	64112 > 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
16	2016-06-27 13:53:53.5543	192.168.1.2	64112	204.79.197.200	Client Hello
17	2016-06-27 13:53:53.5869	204.79.197.200	443	192.168.1.2	443 > 64111 [ACK] Seq=1 Ack=250 Win=131584 Len=0
18	2016-06-27 13:53:53.5899	204.79.197.200	443	192.168.1.2	[TCP segment of a reassembled PDU]
19	2016-06-27 13:53:53.5899	192.168.1.2	64111	204.79.197.200	64111 > 443 [ACK] Seq=250 Ack=1401 Win=262144 Len=0
20	2016-06-27 13:53:53.5911	204.79.197.200	443	192.168.1.2	[TCP segment of a reassembled PDU]
21	2016-06-27 13:53:53.5911	192.168.1.2	64111	204.79.197.200	64111 > 443 [ACK] Seq=250 Ack=2801 Win=262144 Len=0
22	2016-06-27 13:53:53.5925	204.79.197.200	443	192.168.1.2	[TCP segment of a reassembled PDU]
23	2016-06-27 13:53:53.5926	192.168.1.2	64111	204.79.197.200	64111 > 443 [ACK] Seq=250 Ack=4201 Win=262144 Len=0
24	2016-06-27 13:53:53.5938	204.79.197.200	443	192.168.1.2	[TCP segment of a reassembled PDU]
25	2016-06-27 13:53:53.5938	192.168.1.2	64111	204.79.197.200	64111 > 443 [ACK] Seq=250 Ack=5601 Win=262144 Len=0
26	2016-06-27 13:53:53.5940	204.79.197.200	443	192.168.1.2	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
27	2016-06-27 13:53:53.5940	192.168.1.2	64111	204.79.197.200	64111 > 443 [ACK] Seq=250 Ack=5919 Win=261632 Len=0
28	2016-06-27 13:53:53.6075	192.168.1.2	64111	204.79.197.200	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
29	2016-06-27 13:53:53.6084	192.168.1.2	64111	204.79.197.200	[TCP segment of a reassembled PDU]
30	2016-06-27 13:53:53.6084	192.168.1.2	64111	204.79.197.200	[TCP segment of a reassembled PDU]
31	2016-06-27 13:53:53.6085	192.168.1.2	64111	204.79.197.200	[TCP segment of a reassembled PDU]
32	2016-06-27 13:53:53.6290	204.79.197.200	443	192.168.1.2	Application Data
33	2016-06-27 13:53:53.6354	204.79.197.200	443	192.168.1.2	443 > 64112 [ACK] Seq=1 Ack=250 Win=131584 Len=0
34	2016-06-27 13:53:53.6356	192.168.1.2	64112	204.79.197.200	[TCP segment of a reassembled PDU]
35	2016-06-27 13:53:53.6359	204.79.197.200	443	192.168.1.2	64112 > 443 [ACK] Seq=250 Ack=1401 Win=262144 Len=0
36	2016-06-27 13:53:53.6360	192.168.1.2	64112	204.79.197.200	[TCP segment of a reassembled PDU]
37	2016-06-27 13:53:53.6363	204.79.197.200	443	192.168.1.2	64112 > 443 [ACK] Seq=250 Ack=2801 Win=262144 Len=0
38	2016-06-27 13:53:53.6364	192.168.1.2	64112	204.79.197.200	[TCP segment of a reassembled PDU]
39	2016-06-27 13:53:53.6368	204.79.197.200	443	192.168.1.2	64112 > 443 [ACK] Seq=250 Ack=4201 Win=262144 Len=0

CSV output

ΕΡΓΑΛΕΙΑ ΜΕΤΡΗΣΕΩΝ (3/4)

Wireless Net View

SSID	Last Signal	Average Sig...	Detection Counter	% Detection	Security Enabled	Connectable	Authentication	Cipher	PHY Types	First Detected On	Last Detect
TSOUTSOU...PROUTSOU	81%	68%	6	100.0%	Yes	Yes	RSNA-PSK	CCMP	802.11n	31-Jul-16 2:15:33 PM	31-Jul-16 2:15:33 PM
Wind WiFi 6Hxfs	49%	50%	5	83.3%	Yes	Yes	RSNA-PSK	CCMP	802.11n	31-Jul-16 2:15:33 PM	31-Jul-16 2:15:33 PM
ThomsonC2FD01	49%	49%	6	100.0%	Yes	Yes	RSNA-PSK	CCMP	802.11g	31-Jul-16 2:15:33 PM	31-Jul-16 2:15:33 PM
Cosmic Zone	49%	49%	2	33.3%	Yes	Yes	RSNA-PSK	CCMP	802.11n	31-Jul-16 2:15:33 PM	31-Jul-16 2:15:33 PM
Forthnet-158F9A	49%	49%	6	100.0%	Yes	Yes	WPA-PSK	TKIP	802.11g	31-Jul-16 2:15:33 PM	31-Jul-16 2:15:33 PM
vodafone 2016	48%	48%	3	50.0%	Yes	Yes	WPA-PSK	CCMP	802.11n	31-Jul-16 2:15:33 PM	31-Jul-16 2:15:33 PM
OTEFb08a0	49%	47%	5	100.0%	Yes	Yes	WPA-PSK	CCMP	802.11n	31-Jul-16 2:15:43 PM	31-Jul-16 2:15:43 PM
COSMOTE-409B16	44%	45%	3	50.0%	Yes	Yes	RSNA-PSK	CCMP	802.11n	31-Jul-16 2:15:33 PM	31-Jul-16 2:15:33 PM
Carmen	44%	44%	1	16.7%	Yes	Yes	RSNA-PSK	CCMP	802.11n	31-Jul-16 2:15:33 PM	31-Jul-16 2:15:33 PM

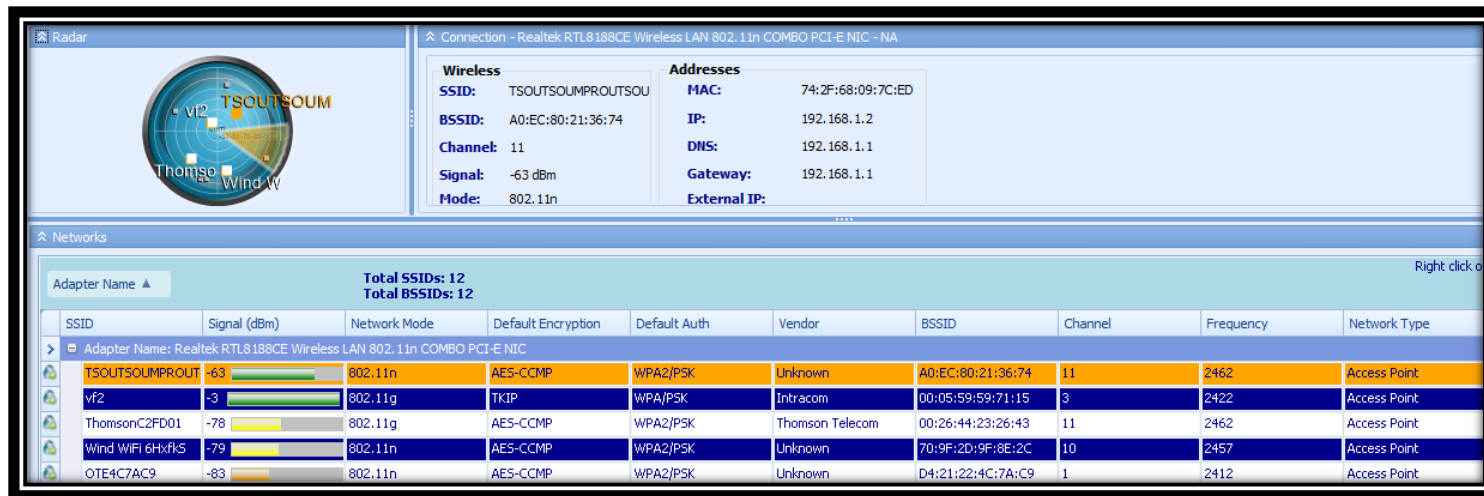


TSOUTSOU...PROUTSOU	80%	79%	9	100.0%	Yes	Yes	RSNA-PSK	CCMP	802.11n	27-Jun-16 2:29:40 PM	27-Jun-16 2:31:00 PM	A0:EC:80:21:36:74	-56	2.462	11	72 Mbps	Infrastructure	Yes
Forthnet-158F9A	52%	52%	8	88.9%	Yes	Yes	WPA-PSK	TKIP	802.11g	27-Jun-16 2:29:40 PM	27-Jun-16 2:31:00 PM	18:17:25:15:8F:9A	-83	2.417	2	54 Mbps	Infrastructure	No
Wind WiFi 6Hxfs	48%	49%	7	77.8%	Yes	Yes	RSNA-PSK	CCMP	802.11n	27-Jun-16 2:29:40 PM	27-Jun-16 2:31:00 PM	70:9F:2D:9F:8E:2C	-85	2.437	6	130 Mbps	Infrastructure	No
ThomsonC2FD01	50%	49%	9	100.0%	Yes	Yes	RSNA-PSK	CCMP	802.11g	27-Jun-16 2:29:40 PM	27-Jun-16 2:31:00 PM	00:26:44:23:26:43	-82	2.462	11	54 Mbps	Infrastructure	No
Cosmic Zone	46%	47%	7	87.5%	Yes	Yes	RSNA-PSK	CCMP	802.11n	27-Jun-16 2:29:50 PM	27-Jun-16 2:31:00 PM	14:CC:20:0D:72:10	-89	2.412	1	150 Mbps	Infrastructure	No
OTEFb08a0	45%	46%	6	75.0%	Yes	Yes	WPA-PSK	CCMP	802.11n	27-Jun-16 2:29:50 PM	27-Jun-16 2:31:00 PM	A4:7E:39:FB:08:A0	-85	2.452	9	150 Mbps	Infrastructure	No
PANAGIOTIS	42%	46%	2	25.0%	Yes	Yes	RSNA-PSK	CCMP	802.11g	27-Jun-16 2:29:50 PM	27-Jun-16 2:30:40 PM	00:13:33:87:48:B3	-94	2.437	6	54 Mbps	Infrastructure	No
OTE4C7AC9	46%	45%	3	33.3%	Yes	Yes	RSNA-PSK	CCMP	802.11n	27-Jun-16 2:29:40 PM	27-Jun-16 2:31:00 PM	D4:21:22:4C:7A:C9	-88	2.412	1	144 Mbps	Infrastructure	No
v2	36%	39%	8	88.9%	Yes	Yes	WPA-PSK	TKIP	802.11g	27-Jun-16 2:29:40 PM	27-Jun-16 2:31:00 PM	00:05:59:59:71:15	-96	2.422	3	54 Mbps	Infrastructure	No
Viki	42%	39%	2	66.7%	Yes	Yes	WPA-PSK	CCMP	802.11n	27-Jun-16 2:30:40 PM	27-Jun-16 2:31:00 PM	14:60:80:D7:5E:88	-94	2.452	9	150 Mbps	Infrastructure	No
OTE-Rob	36%	38%	3	33.3%	Yes	Yes	RSNA-PSK	CCMP	802.11n	27-Jun-16 2:29:40 PM	27-Jun-16 2:30:00 PM	D4:21:22:1F:11:89	-96	2.462	11	144 Mbps	Infrastructure	No
OTE WiFi Fon	36%	36%	1	16.7%	No	Yes	802.11 Open	None	802.11n	27-Jun-16 2:30:10 PM	27-Jun-16 2:30:10 PM	14:60:80:D7:5E:89	-96	2.452	9	150 Mbps	Infrastructure	No
OTE WiFi Fon	36%	36%	1	33.3%	No	Yes	802.11 Open	None	802.11n	27-Jun-16 2:30:40 PM	27-Jun-16 2:30:40 PM	6A:A7:B7:39:39:41	-96	2.412	1	270 Mbps	Infrastructure	No
OTEE7b6ea	0%	31%	9	100.0%	Yes	Yes	WPA-PSK	TKIP	802.11g	27-Jun-16 2:29:40 PM	27-Jun-16 2:31:00 PM	38:46:08:E7:B6:EA	-99	2.462	11	54 Mbps	Infrastructure	No
OTEB0EB38	0%	0%	1	20.0%	Yes	Yes	RSNA-PSK	CCMP	802.11n	27-Jun-16 2:30:20 PM	27-Jun-16 2:30:20 PM	00:26:44:B0:EB:38	-102	2.452	9	65 Mbps	Infrastructure	No



ΕΡΓΑΛΕΙΑ ΜΕΤΡΗΣΕΩΝ (4/4)

Xirrus Wifi Inspector

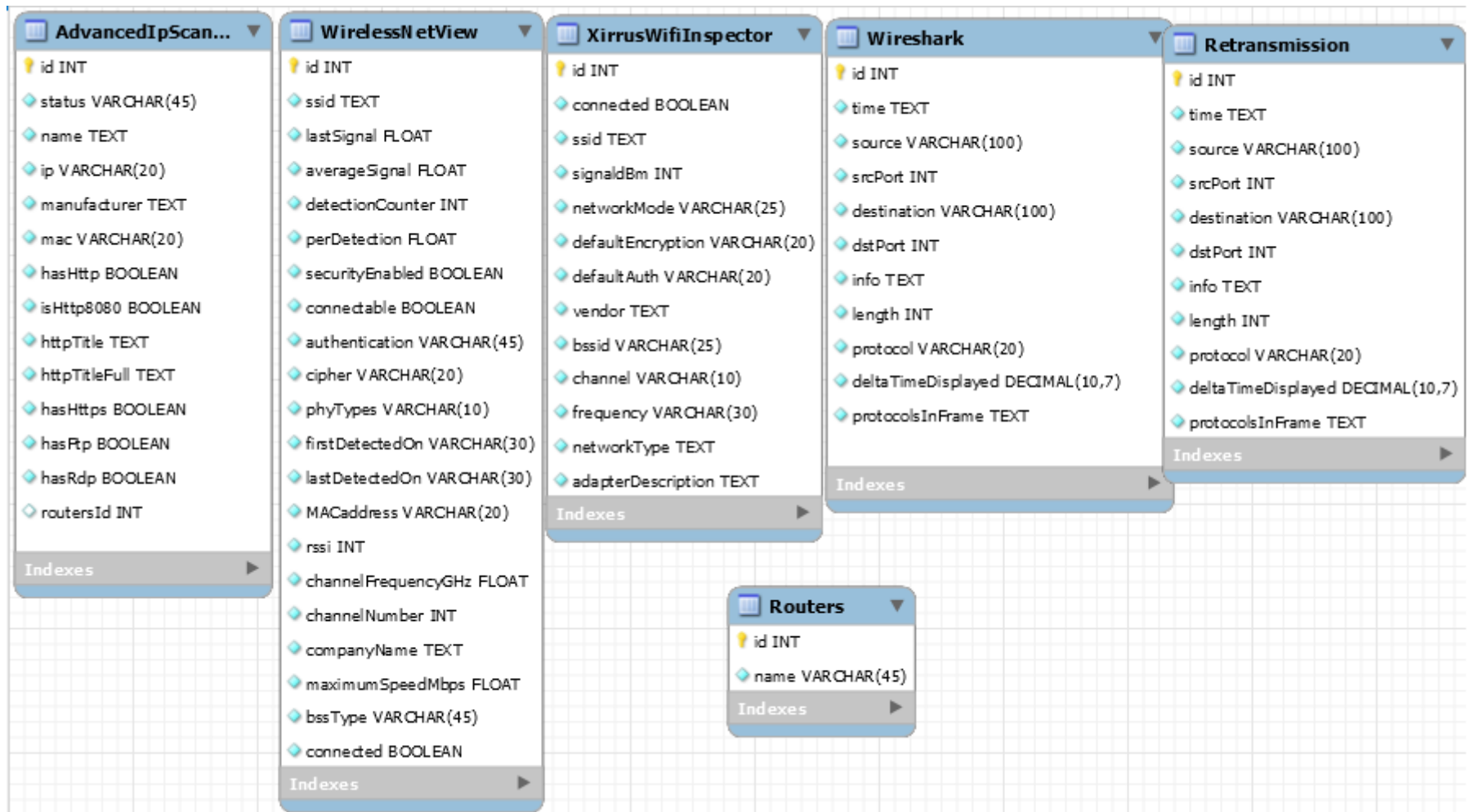


Program

Connected	SSID	Signal(dBm)	Network Mode	Default Encryption	Default Auth	Vendor	BSSID	Channel	Frequency	Network Type	Adapter Description
True	TSOUTSOUMPROUTSOU	-56	802.11n	AES-CCMP	WPA2/PSK	Unknown	A0:EC:80:21:36:74	11	2462	Access Point	Realtek RTL8188CE Wireless LAN 802.11n COMBO PCI-E NIC
False	ThomsonC2FD01	-82	802.11g	AES-CCMP	WPA2/PSK	Thomson Telecom	00:26:44:23:26:43	11	2462	Access Point	Realtek RTL8188CE Wireless LAN 802.11n COMBO PCI-E NIC
False	Fortinet-158F9A	-86	802.11g	TKIP	WPA/PSK	Unknown	18:17:25:15:8F:9A	2	2417	Access Point	Realtek RTL8188CE Wireless LAN 802.11n COMBO PCI-E NIC
False	Wind WiFi 6HxrkS	-86	802.11n	AES-CCMP	WPA2/PSK	Unknown	70:9F:2D:9F:8E:2C	6	2437	Access Point	Realtek RTL8188CE Wireless LAN 802.11n COMBO PCI-E NIC
False	OTE4C7AC9	-86	802.11n	AES-CCMP	WPA2/PSK	Unknown	D4:21:22:4C:7A:C9	1	2412	Access Point	Realtek RTL8188CE Wireless LAN 802.11n COMBO PCI-E NIC
False	vf2	-94	802.11g	TKIP	WPA/PSK	Intracom	00:05:59:59:71:15	3	2422	Access Point	Realtek RTL8188CE Wireless LAN 802.11n COMBO PCI-E NIC
False	OTEe7b6ea	-94	802.11g	TKIP	WPA/PSK	ZTE	38:46:08:E7:B6:EA	11	2462	Access Point	Realtek RTL8188CE Wireless LAN 802.11n COMBO PCI-E NIC
False	OTE-Rob	-96	802.11n	AES-CCMP	WPA2/PSK	Unknown	D4:21:22:1F:11:B9	11	2462	Access Point	Realtek RTL8188CE Wireless LAN 802.11n COMBO PCI-E NIC

CSV output

ΒΑΣΗ ΔΕΔΟΜΕΝΩΝ (1/2)



ΒΑΣΗ ΔΕΔΟΜΕΝΩΝ (2/2)

- Οι πίνακες AdvancedIpScanner, WirelessNetView, XirrusWifiInspector και Wireshark αφορούν τα δεδομένα που προέρχονται από τα αντίστοιχα προγράμματα συλλογής δεδομένων.
- Ο πίνακας Routers αναφέρεται στα Access Points στα οποία συνδεθήκαμε και συσχετίζεται με τον πίνακα AdvancedIpScanner, ώστε να βρούμε ποιες συσκευές είναι συνδεδεμένες σε καθένα από αυτά.
- Ο πίνακας Retransmission περιέχει τα ίδια πεδία με τον πίνακα Wireshark. Προέρχεται από το ίδιο πρόγραμμα με χρήση τού φίλτρου tcp.analysis.retransmission, ώστε να βρίσκουμε τις αναμεταδόσεις των TCP πακέτων.

FCAPS

Η εργασία βασίστηκε στο μοντέλο διαχείρισης δικτύων FCAPS, το οποίο περιλαμβάνει τις εξής ενότητες :

- ✓ Fault Management
- ✓ Configuration Management
- ✓ Accounting Management
- ✓ Performance Management
- ✓ Security Management

F	C	A	P	S
Fault detection	Resource initialization	Track service / resource usage	Utilization & error rates	Selective resource access
Fault correction	Network provisioning	Cost for services	Consistent performance level	Enable NE functions
Fault isolation	Auto-discovery	Accounting limit	Performance data collection	Access logs
Network recovery	Backup and restore	Combine costs for multiple resources	Performance report generation	Security alarm / event reporting
Alarm handling	Resource shut down	Set quotas for usage	Performance data analysis	Data privacy
Alarm filtering	Change management	Audits	Problem reporting	User access rights checking
Alarm generation	Pre-provisioning	Fraud reporting	Capacity planning	Take care of security breaches & attempts
Clear correlation	Inventory/asset management	Support for different modes of accounting	Performance data & statistics collection	Security audit trail log
Diagnostic test	Copy configuration		Maintaining & examining historical logs	Security related information distributions
Error logging	Remote configuration			
Error handling	Job initiation, tracking & execution			
Error statistics	Automated software distribution			

Fault Management

- ❖ Εύρεση και διόρθωση προβλημάτων διαδικτύου
- ❖ Αναγνώριση, πρόβλεψη και αποφυγή πιθανών σφαλμάτων
- ❖ Αποφυγή διακοπής λειτουργίας του δικτύου
- ❖ Πάντα διαθέσιμο δίκτυο
- ❖ Σύστημα παρακολουθεί και ειδοποιεί διαχειριστές και χρήστες με διαφορετικά σήματα
- ❖ Αναπτύσσονται εφαρμογές για να τα αντιμετωπίζουν αυτόματα



Configuration Management

- ❖ Παρακολουθείται και ελέγχεται η λειτουργία του δικτύου
- ❖ Συγκέντρωση και αποθήκευση ρυθμίσεων των συσκευών δικτύου
- ❖ Ενημέρωση και αναβάθμιση υλικού και λογισμικού
- ❖ Προσθήκη νέου εξοπλισμού, ανάπτυξη νέων προγραμμάτων



Accounting Management

- ❖ Υπεύθυνο για τη σωστή χρέωση των πελατών
- ❖ Προσδιορισμός κόστους στον πάροχο υπηρεσιών
- ❖ Κατανομή πόρων κατά βέλτιστο τρόπο μεταξύ των χρηστών
- ❖ Αποτελεσματική χρήση πόρων με το ελάχιστο κόστος λειτουργίας
- ❖ Συγκέντρωση στατιστικών στοιχείων χρήσης

*We don't want
your money!*



*We can take some from
poor people if we need it.*

Performance Management

- ❖ Εξασφάλιση αποδεκτής απόδοσης του δικτύου
- ❖ Προσδιορισμός αποτελεσματικότητας υφιστάμενου δικτύου, προετοιμασία για το μέλλον
- ❖ Εύρεση μεθόδων που θα δώσουν τη μεγαλύτερη συνολική βελτίωση των επιδόσεων
- ❖ Ζητήματα: Μεγιστοποίηση throughput, αποφυγή bottlenecks, ελαχιστοποίηση χρόνων απόκρισης, μείωση απωλειών και σφαλμάτων, βελτιώσεις στη χρήση τής ζεύξης



"Just measuring your job performance..."

Security Management

- ❖ Προστασία δεδομένων από μη εξουσιοδοτημένους χρήστες
- ❖ Έλεγχος πρόσβασης, διασφάλιση εμπιστευτικότητας
- ❖ Επιτυγχάνεται με κρυπτογράφηση και έλεγχο ταυτότητας
- ❖ Συγκέντρωση πληροφοριών που αφορούν την ασφάλεια
- ❖ Άλλες κοινές εργασίες περιλαμβάνουν τη διαμόρφωση και τη διαχείριση των firewalls, συστήματα ανίχνευσης κινήσεων και πολιτικών ασφάλειας



Σχεδιασμός δικτύου

- ❑ Συνδεθήκαμε σε 4 διαφορετικά access points, καταγράψαμε κίνηση και συλλέξαμε δεδομένα
- ❑ Ενώσαμε τα 4 δίκτυα σε ένα μεγάλο το οποίο θεωρούμε ότι διαχειριζόμαστε
- ❑ Με βάση το μοντέλο FCAPS καταγράψαμε κάποια βασικά προβλήματα
- ❑ Το σχήμα του δικτύου ακολουθεί στην επόμενη διαφάνεια
- ❑ Θεωρούμε ότι κάθε access point έχει γείτονες το προηγούμενο του και το επόμενο του στο επόμενο σχήμα

Wireless Router Network Diagram



Κώδικας

- Φτιάξαμε ένα παράθυρο από όπου μπορούμε να κάνουμε browse το αρχείο και να διαλέξουμε πίνακα στον οποίο θα εισάγουμε τα δεδομένα
- Στη συνέχεια οδηγούμαστε σε ένα menu προβλημάτων. Μπορούμε να επιλέξει ένα από αυτά και να ελέγχουμε κατά πόσο υπάρχει στο δίκτυο
- Τα προβλήματα σχετίζονται με το μοντέλο FCAPS
- Θα παρουσιάσουμε όλα τα προβλήματα και το σχετικό γραφικό κομμάτι στις επόμενες διαφάνειες



Real programmers code in binary.

Import window

The screenshot shows a window titled "Import data" with a close button. The main text inside says "Browse the file you want to insert" and "From which program did you select data?". There are four main interactive elements highlighted with colored ovals and arrows pointing to Greek text boxes below: 1. A "Browse file:" label next to a text input field containing the path "/home/christos/Desktop/data/christos/wireshark1". The "Browse" button to its right is circled in yellow. 2. A "Select Program:" label next to a list box containing "Wireshark", "Advanced Ip Scanner", "Wireless NetView", "Xirrus Wifi Inspector", and "Wireshark" (selected). The "Submit" button below is circled in red. 3. A "Clear" button below the list box, circled in green. 4. A "Continue" button at the bottom right, circled in blue. A yellow arrow also points from the "Continue" button area towards the "Browse" button.

Υποβολή στοιχείων
για εισαγωγή στη
βάση

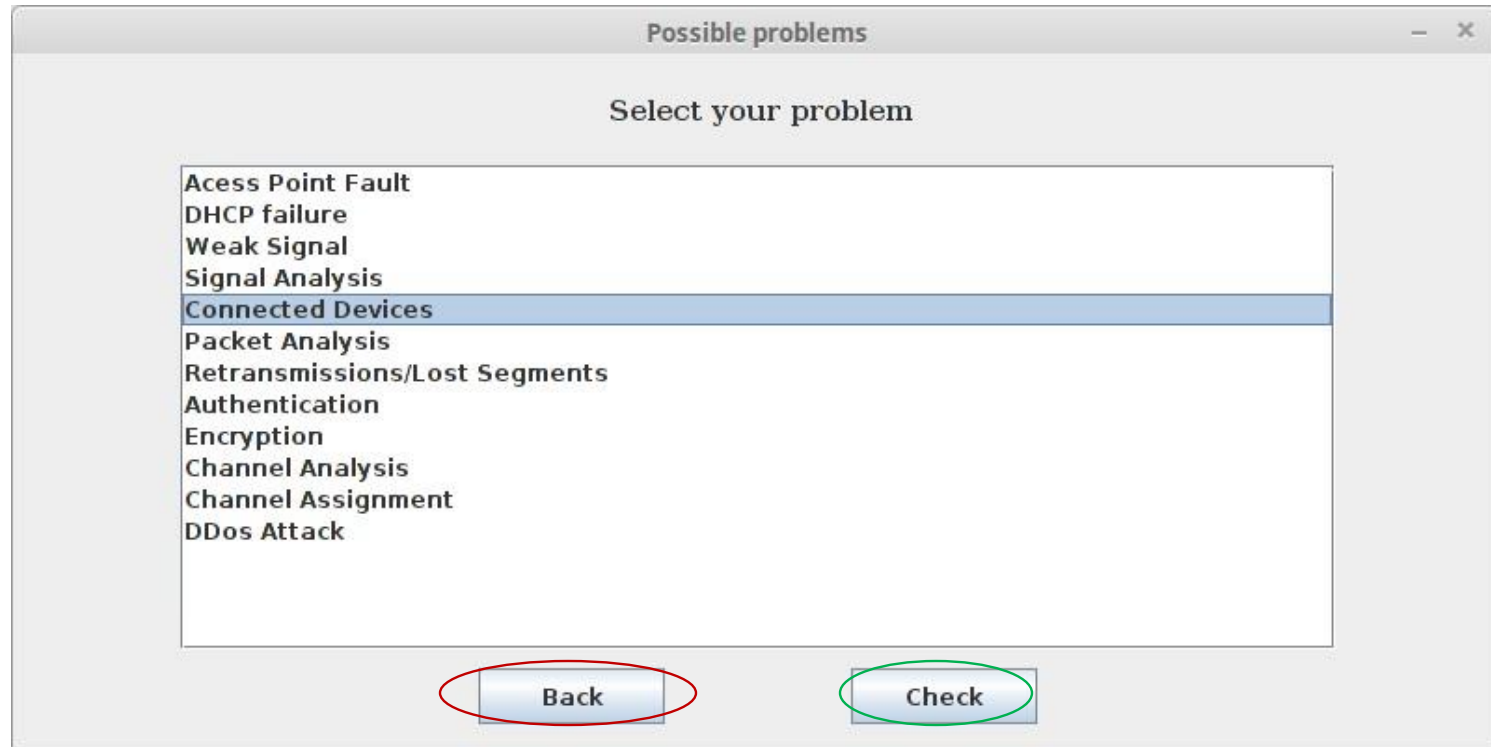
Καθαρισμός όλων
των δεδομένων της
φόρμας

Οδηγεί στο μενού με
τα προβλήματα

Για φόρτωση του
path του αρχείου
με τα δεδομένα

Problems' menu

Το μενού με τα πιθανά προβλήματα. Ο χρήστης μπορεί να επιλέξει ένα από τα προβλήματα και να πατήσει Check ώστε να οδηγηθεί στο σχετικό παράθυρο είτε να πατήσει back και να οδηγηθεί στο Import Window που αναλύσαμε

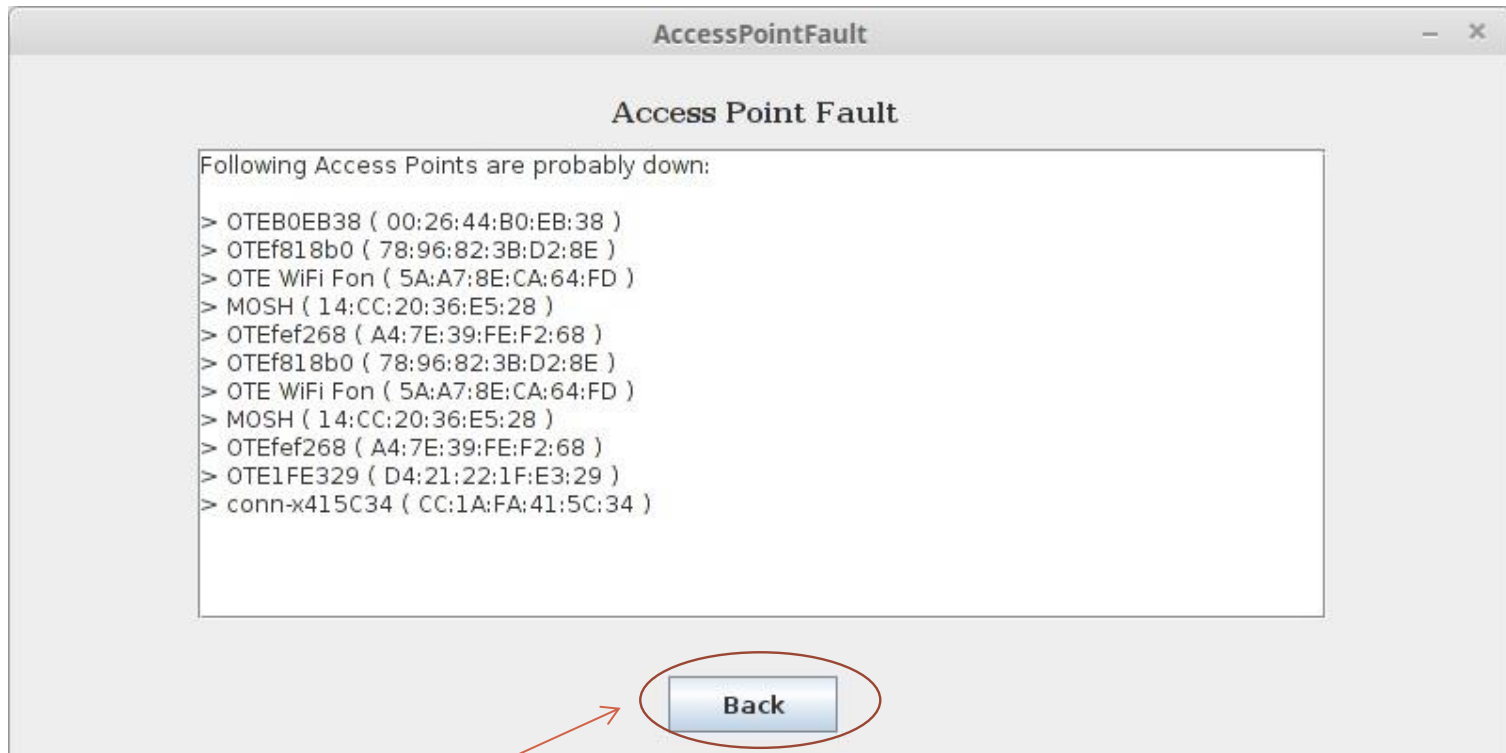


Πίσω στο
Import window

Οδηγεί στο γραφικό
του σχετικού
προβλήματος

Access Point Fault

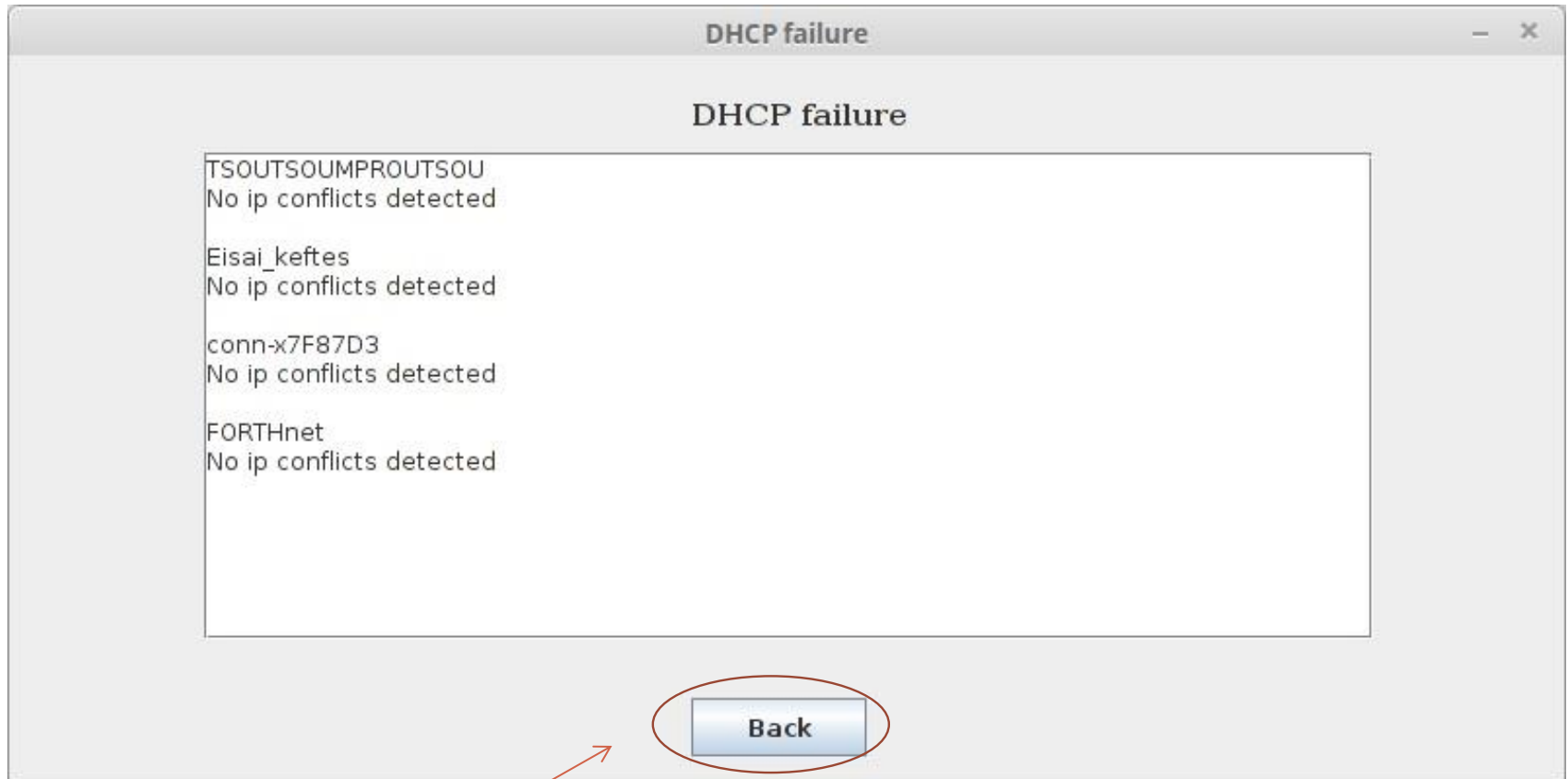
Καταγράφει τα access points που δε λειτουργούν
Πρόκειται για αυτά που έχουν μηδενικό last και average signal



Πίσω στο μενού
προβλημάτων

DHCP failure

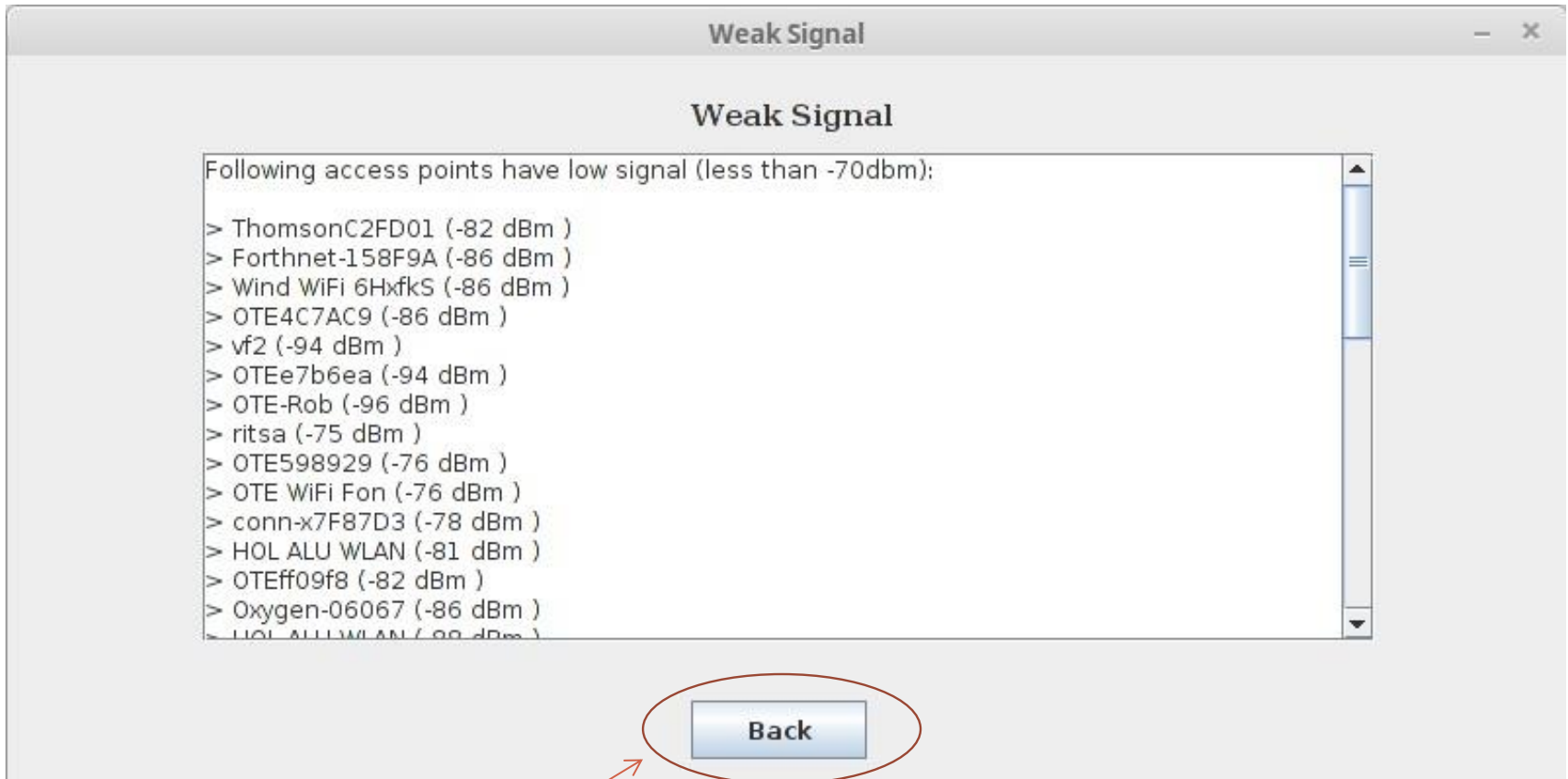
Ψάχνει για ip conflicts, δηλαδή αν έχει δοθεί η ίδια ip διεύθυνση σε παραπάνω από μία συνδεδεμένες συσκευές στο ίδιο access point



Πίσω στο μενού
προβλημάτων

Weak signal

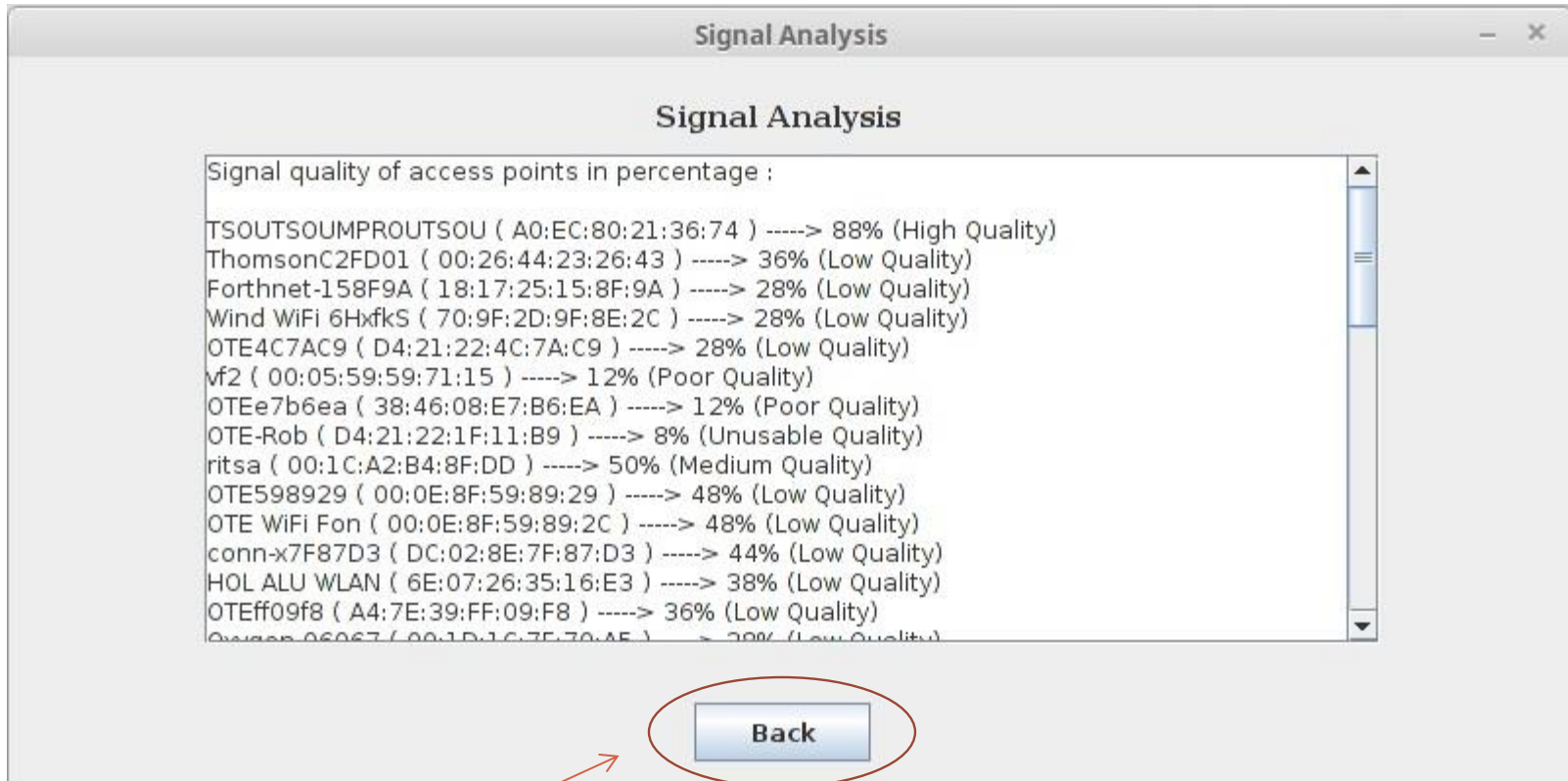
Εμφανίζει τα access points που έχουν χαμηλό σήμα και η σύνδεση σε αυτά δε θα είναι καλή



Πίσω στο μενού
προβλημάτων

Signal Analysis

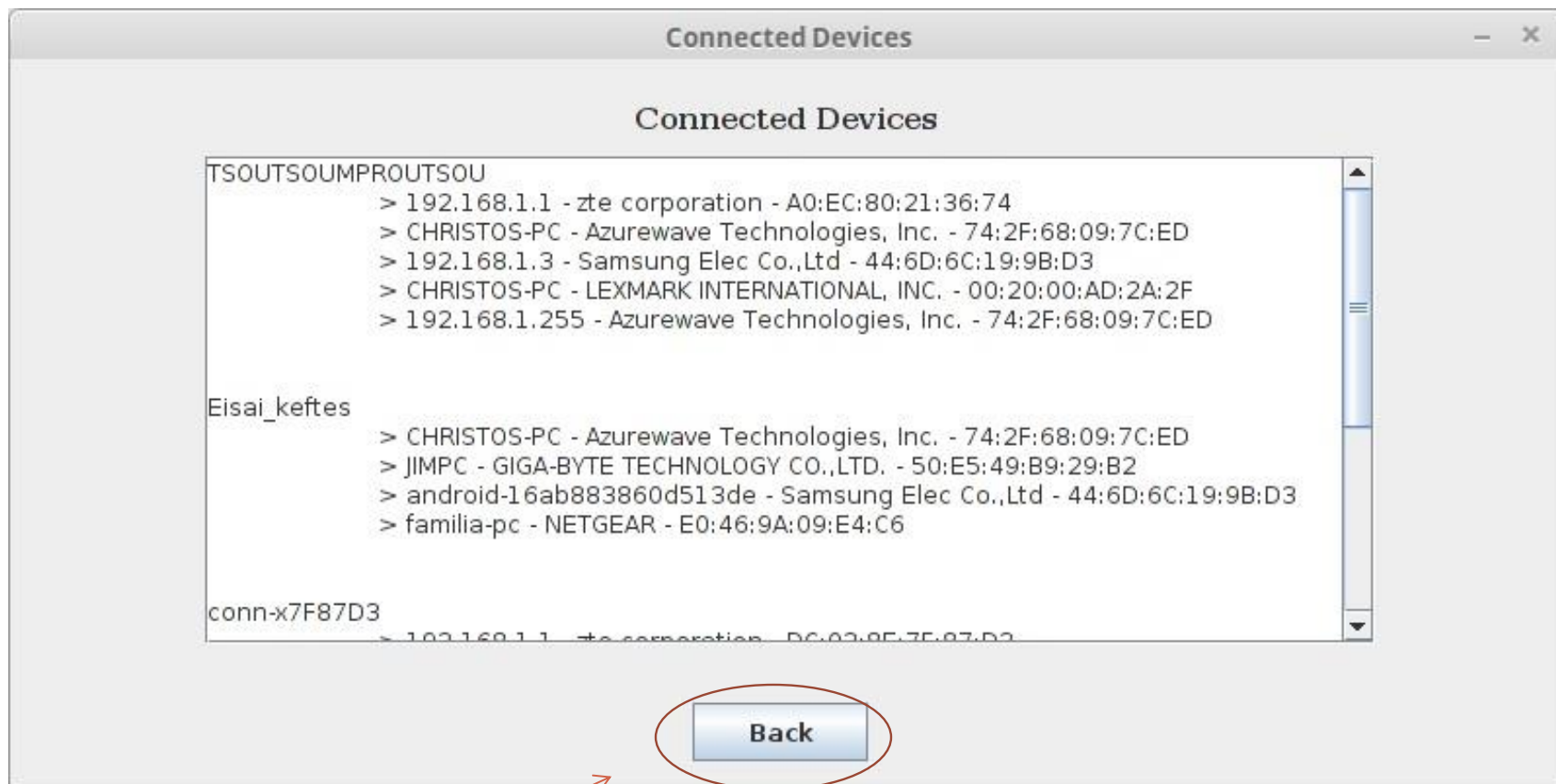
Αναλύουμε την ποιότητα του σήματος των access points παίρνοντας την ισχύ σε dBm και βρίσκοντας ποσοστιαία την ισχύ με χρήση του τύπου: $2 * (100 + \text{rssi})$



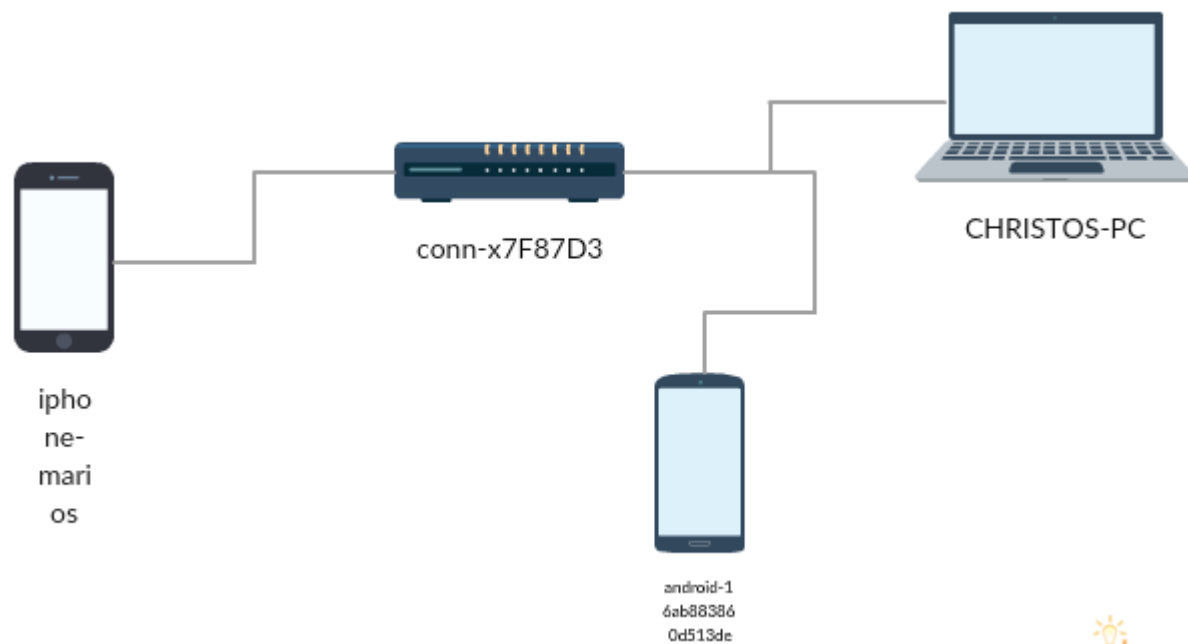
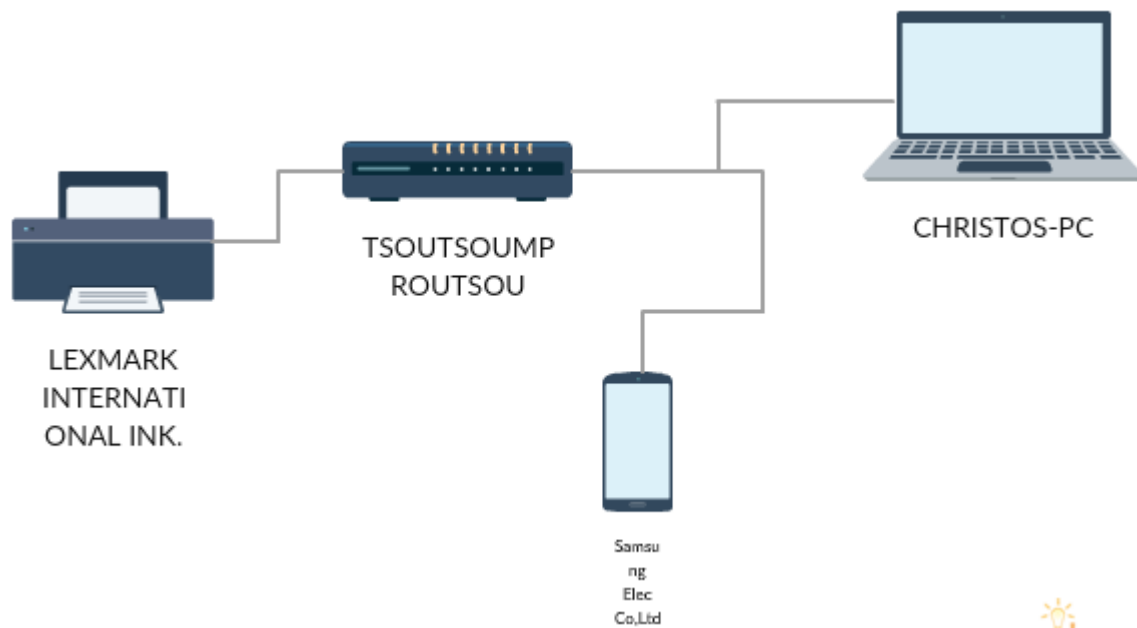
Πίσω στο μενού
προβλημάτων

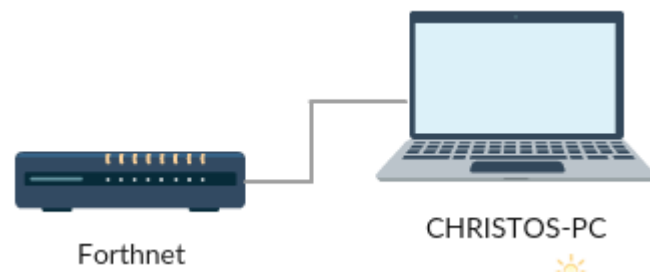
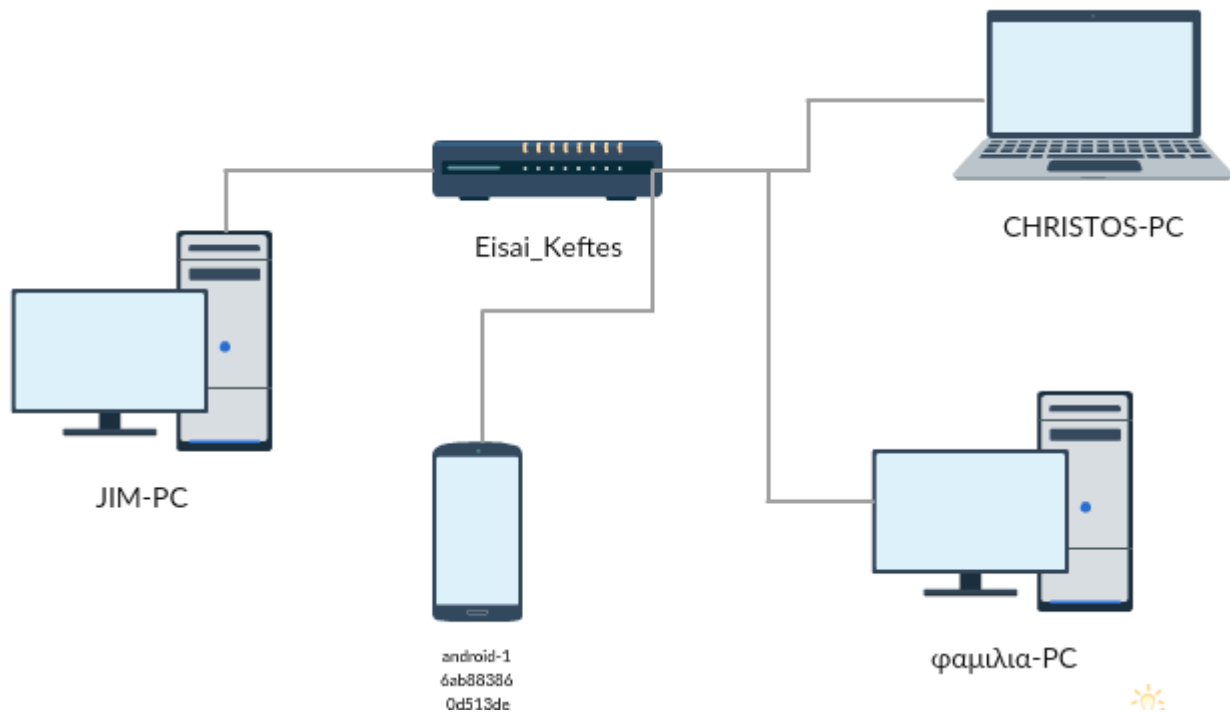
Connected devices

Παρουσιάζονται οι συσκευές που είναι συνδεδεμένες στα access points από τα οποία συλλέξαμε δεδομένα. Ακολουθούν σχετικά γραφήματα.



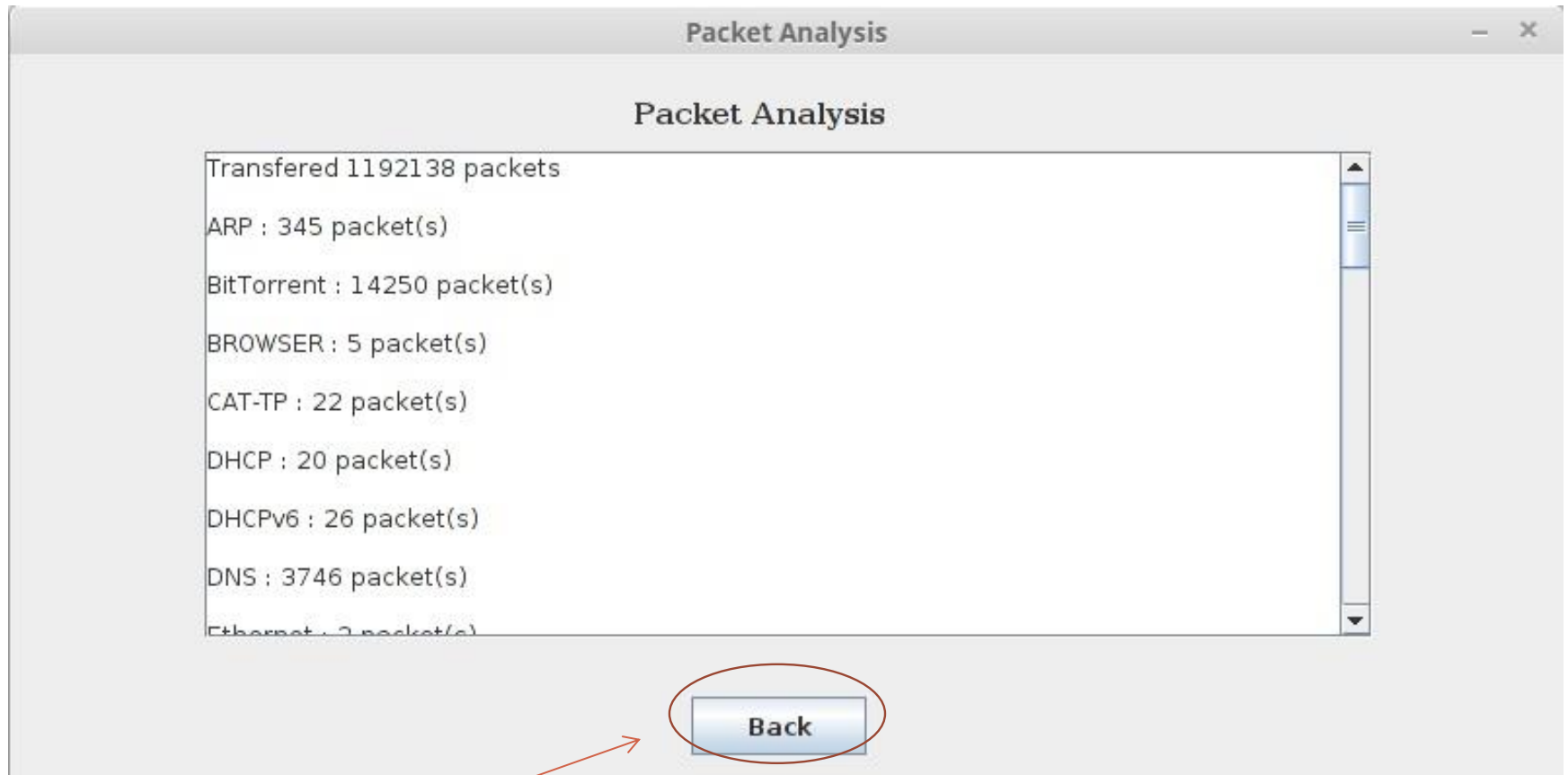
Πίσω στο μενού
προβλημάτων





Packet analysis

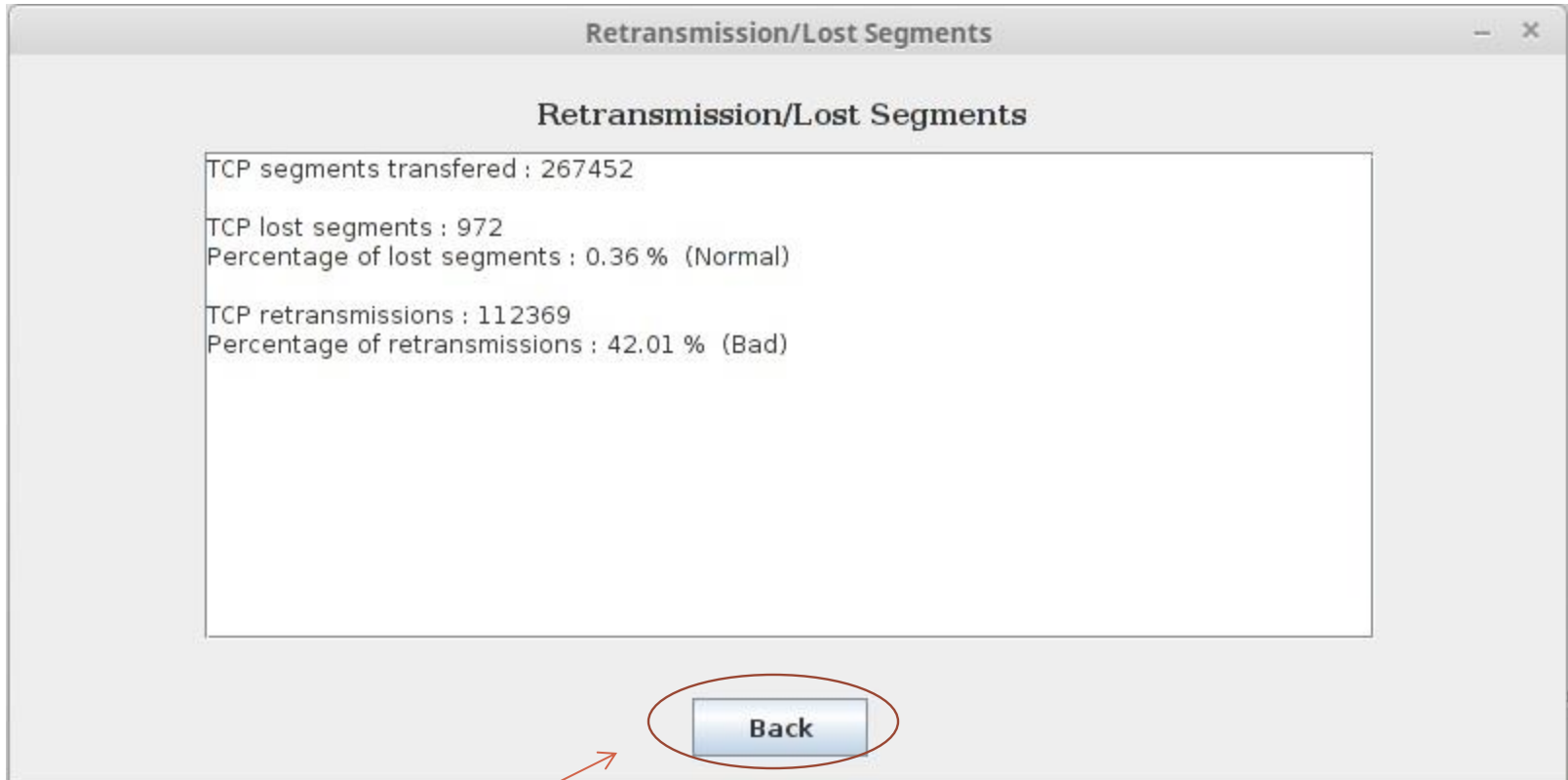
Καταγραφή του πλήθους και της φύσης των πακέτων που διακινούνται στο δίκτυο.



Πίσω στο μενού
προβλημάτων

Retransmissions/Lost segments

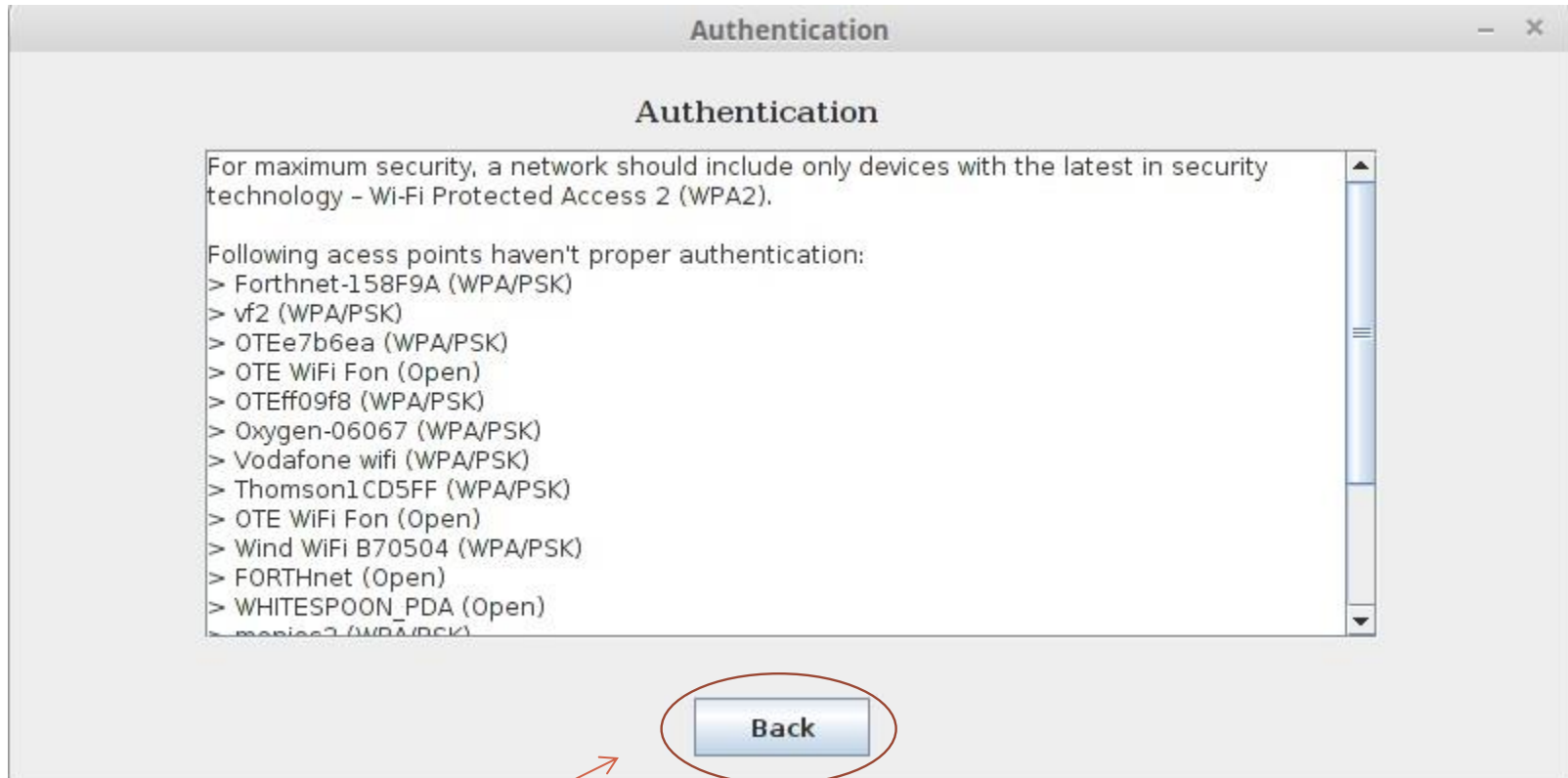
Επαναμεταδόσεις και χαμένα TCP πακέτα στο δίκτυο που εξετάζουμε



Πίσω στο μενού
προβλημάτων

Authentication

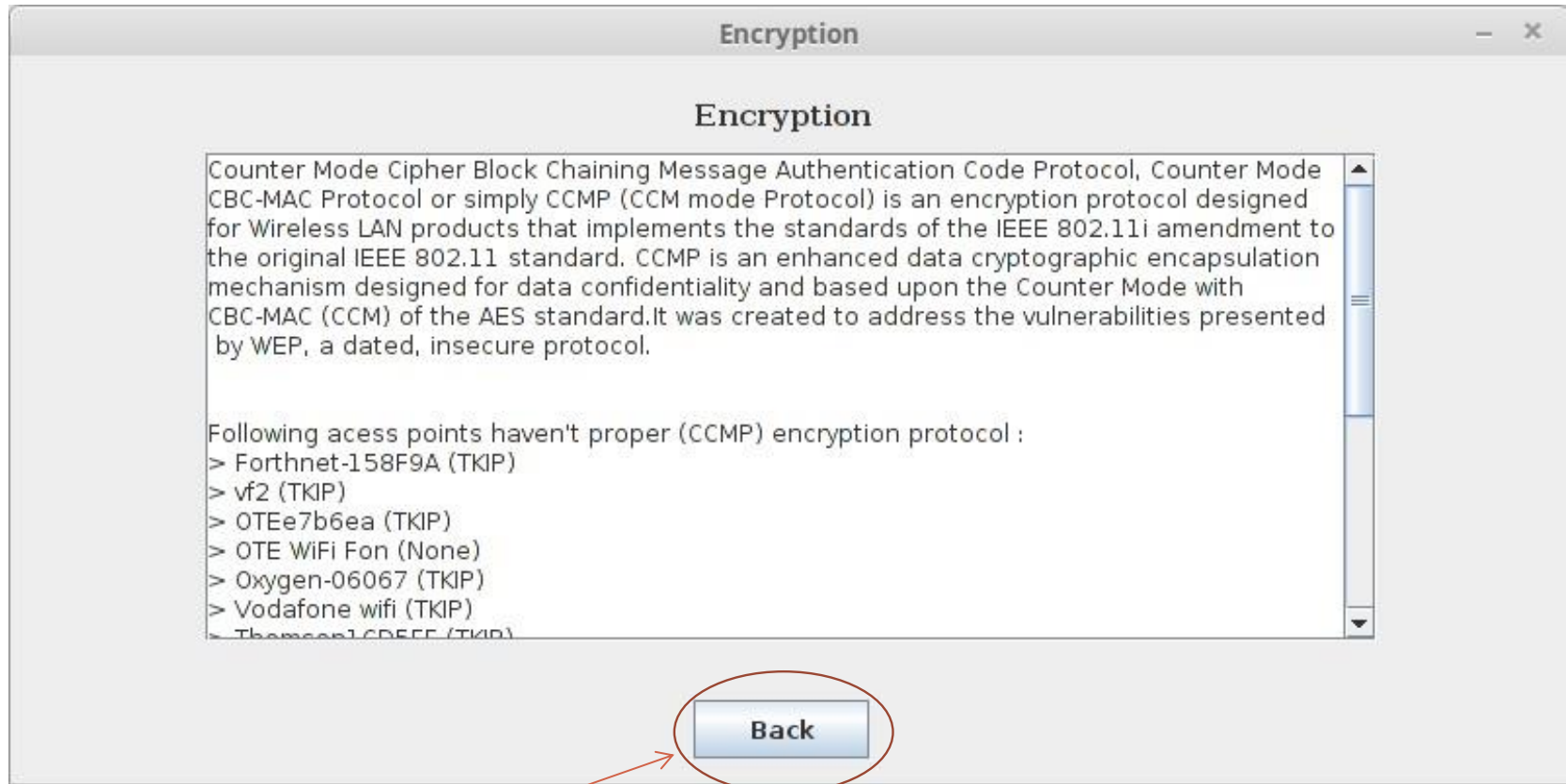
Κατάλληλο authentication το WPA2



Πίσω στο μενού
προβλημάτων

Encryption

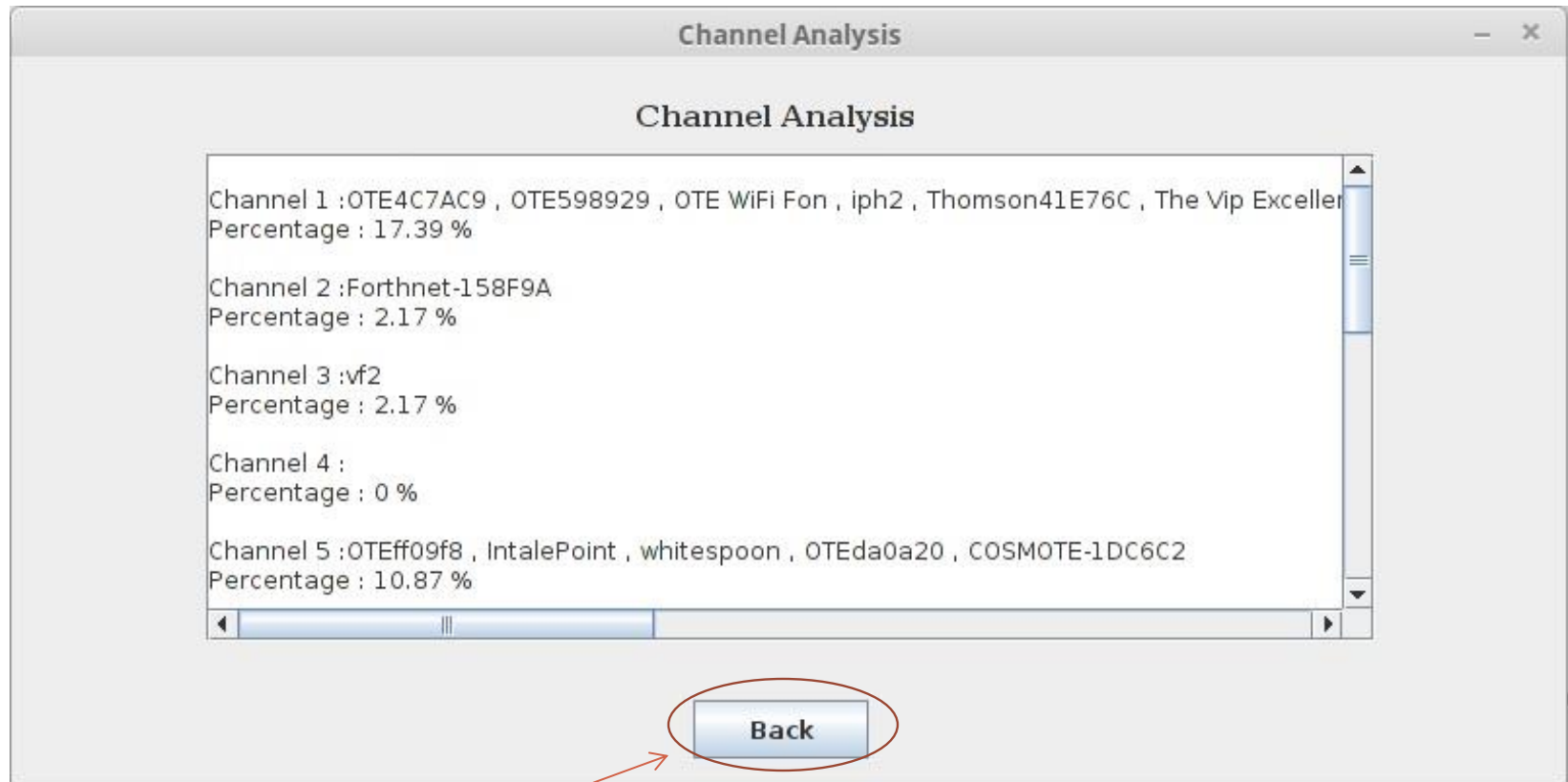
Το πιο σύγχρονο πρωτόκολλο encryption είναι το CCMP. Τα υπόλοιπα τα έχουμε σημειώσει ως μη αποδεκτά.



Πίσω στο μενού
προβλημάτων

Channel analysis

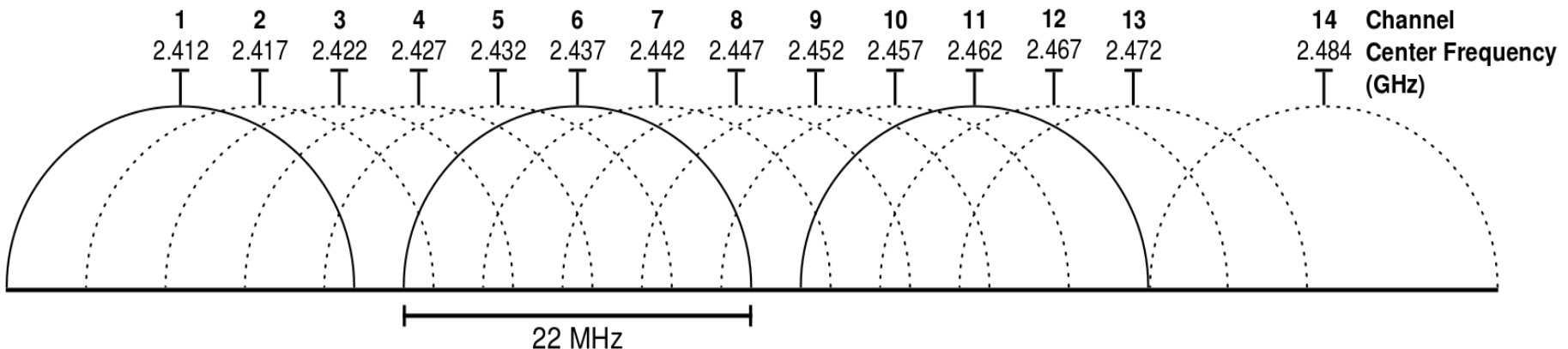
Μελέτη της κατανομής των access points στα κανάλια 1 έως 13



Πίσω στο μενού
προβλημάτων

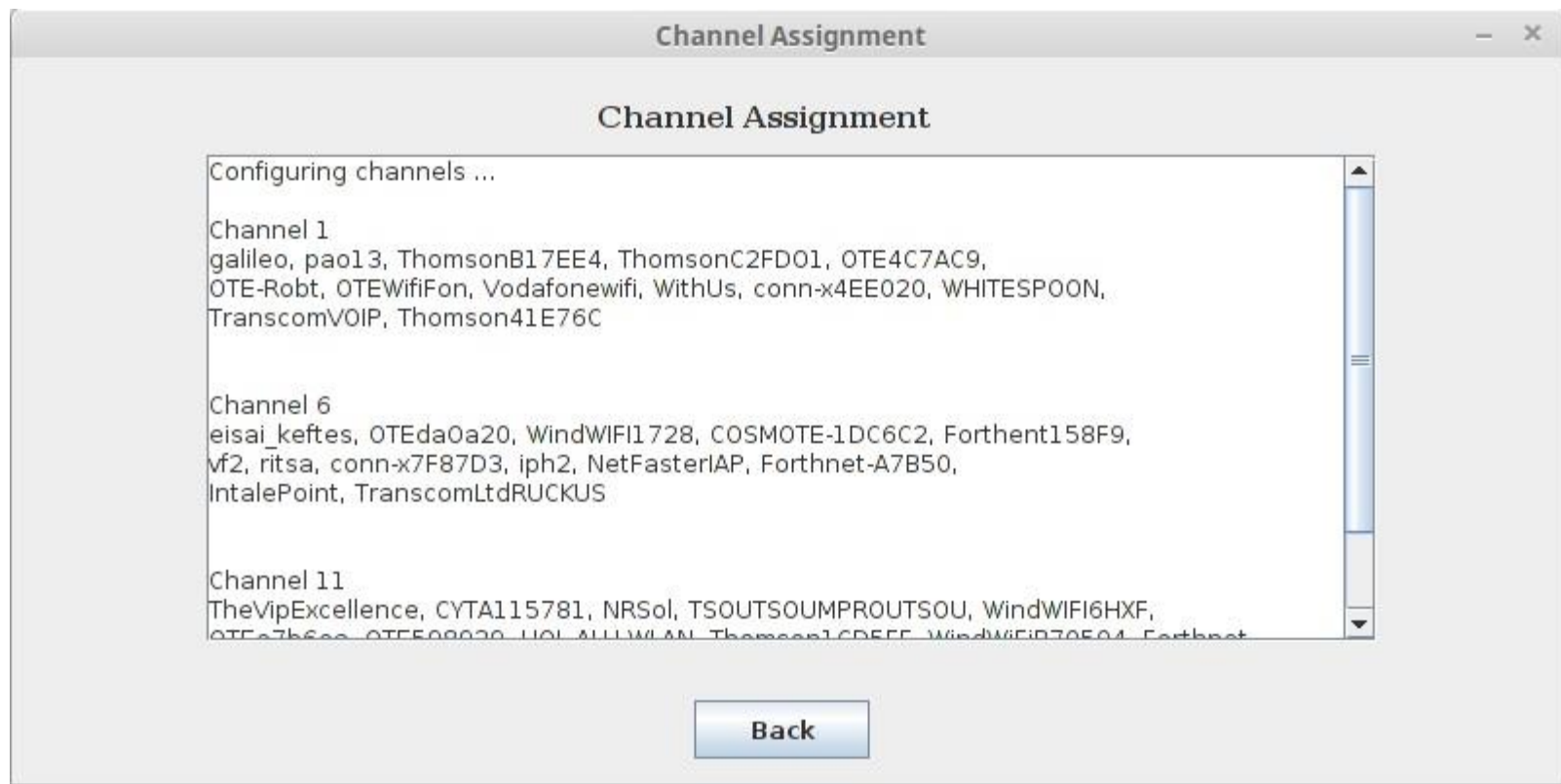
Channel assignment (1/2)

- Οι συχνότητες ανάμεσα στα 2400MHz και τα 2500 MHz σε 13 κανάλια
- Οι κεντρικές συχνότητες των καναλιών φαίνονται στο σχήμα παρακάτω
- Κάθε κανάλι έχει ένα εύρος συχνοτήτων στο οποίο μπορεί να εκπέμψει
- Βλέπουμε ότι ορισμένες συχνότητες ανήκουν σε περισσότερα από ένα κανάλια
- Για παράδειγμα στη συχνότητα 2416 MHz μπορούν να εκπέμψουν τα κανάλια 1,2 και 3



Channel assignment (2/2)

- Κάθε access point θεωρούμε ότι άλλα 2 γειτονικά
- Βλέπουμε ότι τα κανάλια 1,6 και 11 είναι μη επικαλυπτόμενα μεταξύ τους
- Σε κάθε μέλος της τριάδας θα δίνουμε ένα εκ των καναλιών 1,6 και 11 ώστε να έχουν διαφορετικά κανάλια μεταξύ τους



DDos attack

Τα δεδομένα έχουν συλλεχθεί σε διαφορετικά χρονικά διαστήματα και ενώ ήμασταν συνδεδεμένοι σε διαφορετικά δίκτυα. Για αυτό το λόγο, θεωρούμε ότι υπάρχει επίθεση όταν υπάρχουν 80 ή περισσότερα πακέτα του ίδιου πρωτοκόλλου που στέλνονται στην ίδια IP διεύθυνση και στο ίδιο port



That's all Folks!