IEs, we Scan!

Using proprietary beacon extensions
to facilitate wireless community link building

Claudio Pisa
clauz@ninux.org
@cl4u2

sponsored by

Internet Society

INESCTEC

ispa Internet Service Providers Austria

netidee

Unwired Networks

freewave

BATTLEMESH v10

JUNE 05-11, 2017

#WBM10

Network Bogotá

netCommons

endorsed by

freifunk.net

AWMN Athens Wireless Metropolitan Network

wlanslovenija

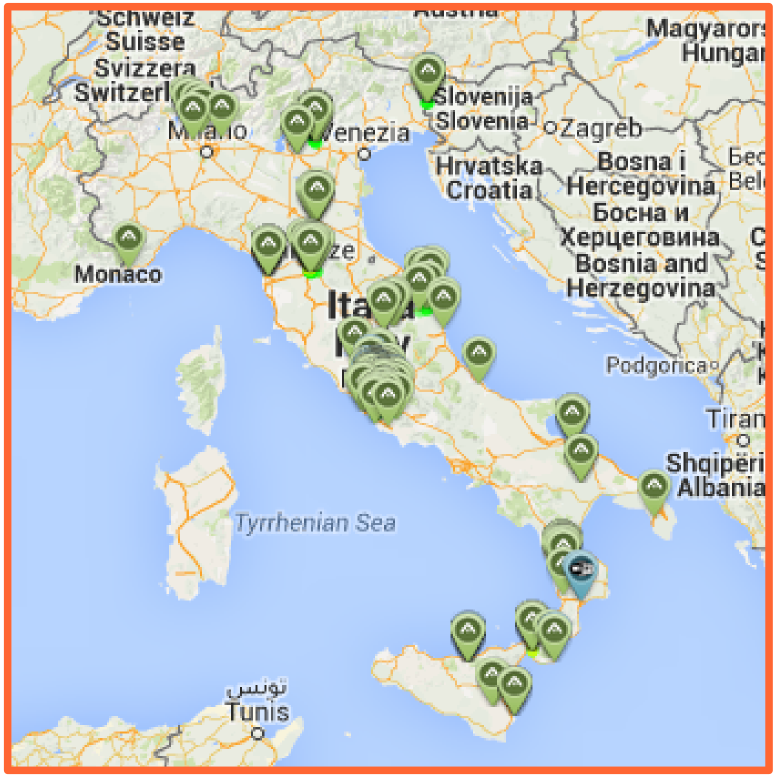
ninux.org wireless community network

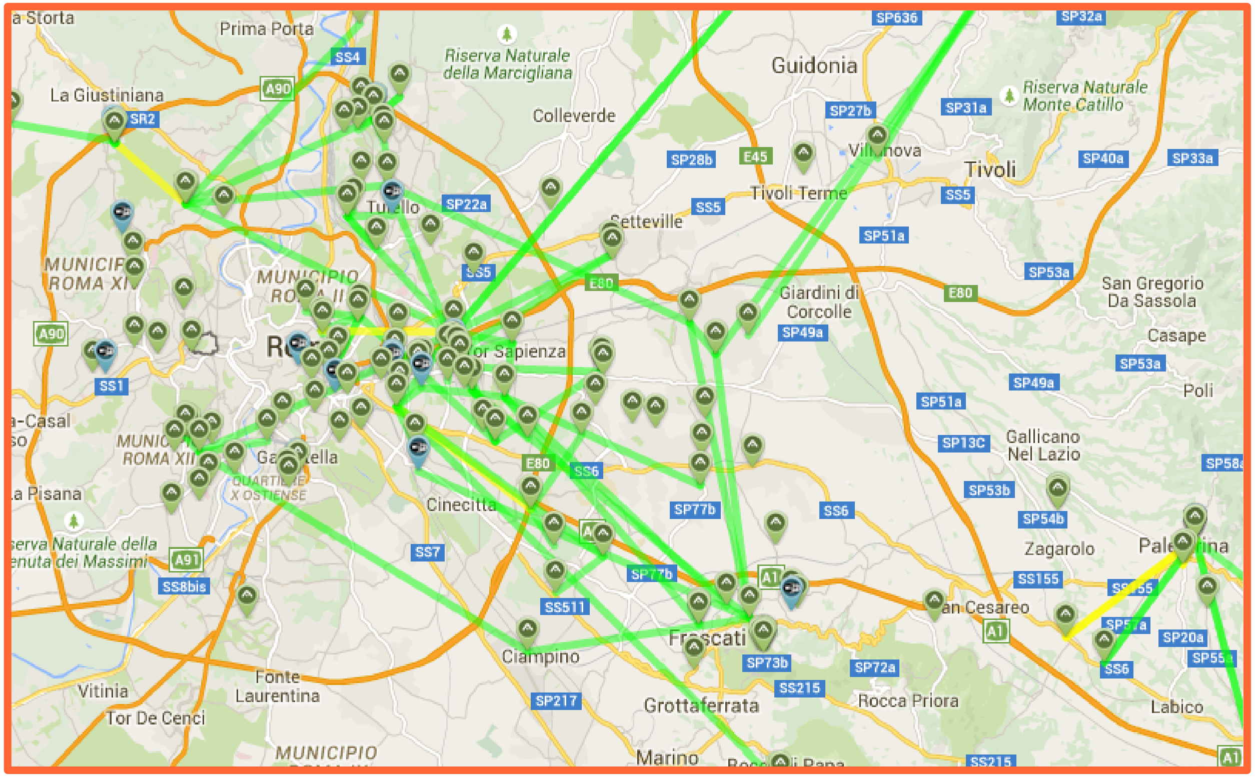
guifi·net

ninux.org

- Community network in Italy
- Islands
  - each island is in a geographical region
  - each island uses a different routing protocol

ninux.org


Schweiz
Suisse
Svizzera
Switzerl
Austria
Magyarors
Hungar
Slovenija
Slovenia
Zagreb
Milano
Venezia
Hrvatska
Croatia
Bosna i
Hercegovina
Босна и
Херцеговина
Bosnia and
Herzegovina
Monaco
Italia
Podgorica
Tiran
Shqipëri
Albania
Tyrrhenian Sea
تونس
Tunis


La Storta
Prima Porta
Riserva Naturale della Marcigliana
Guidonia
Riserva Naturale Monte Catillo
La Giustiniana
Colleverde
Villanova
Tivoli
Tivoli Terme
Settecamini
Setteville
Tufello
MUNICIPIO ROMA XIV
MUNICIPIO ROMA II
Roma
Tor Sapienza
Giardini di Corcolle
San Gregorio Da Sassola
Casape
Poli
Casal
La Pisana
MUNICIPIO ROMA XII
Garbatella
QUARTIERE X OSTIENSE
Cinecittà
Gallicano Nel Lazio
Zagarolo
Palestrina
Riserva Naturale della Tenuta dei Massimi
San Cesareo
Ciampino
Frascati
Vitinia
Fonte Laurentina
Tor De Cenci
Grottaferrata
Rocca Priora
Labico
MUNICIPIO
Marino
Rocca di Papa
A90
A1
E80
E45
SS4
SR2
SS1
SS5
SS6
SS7
SS8bis
SS511
SS155
SS215
SP22a
SP28b
SP27b
SP31a
SP32a
SP636
SP40a
SP33a
SP51a
SP53a
SP49a
SP13C
SP53b
SP54b
SP77b
SP73b
SP72a
SP217
SP20a
SP58a
SP55a

ninux.org
WIRELESS COMMUNITY NETWORK

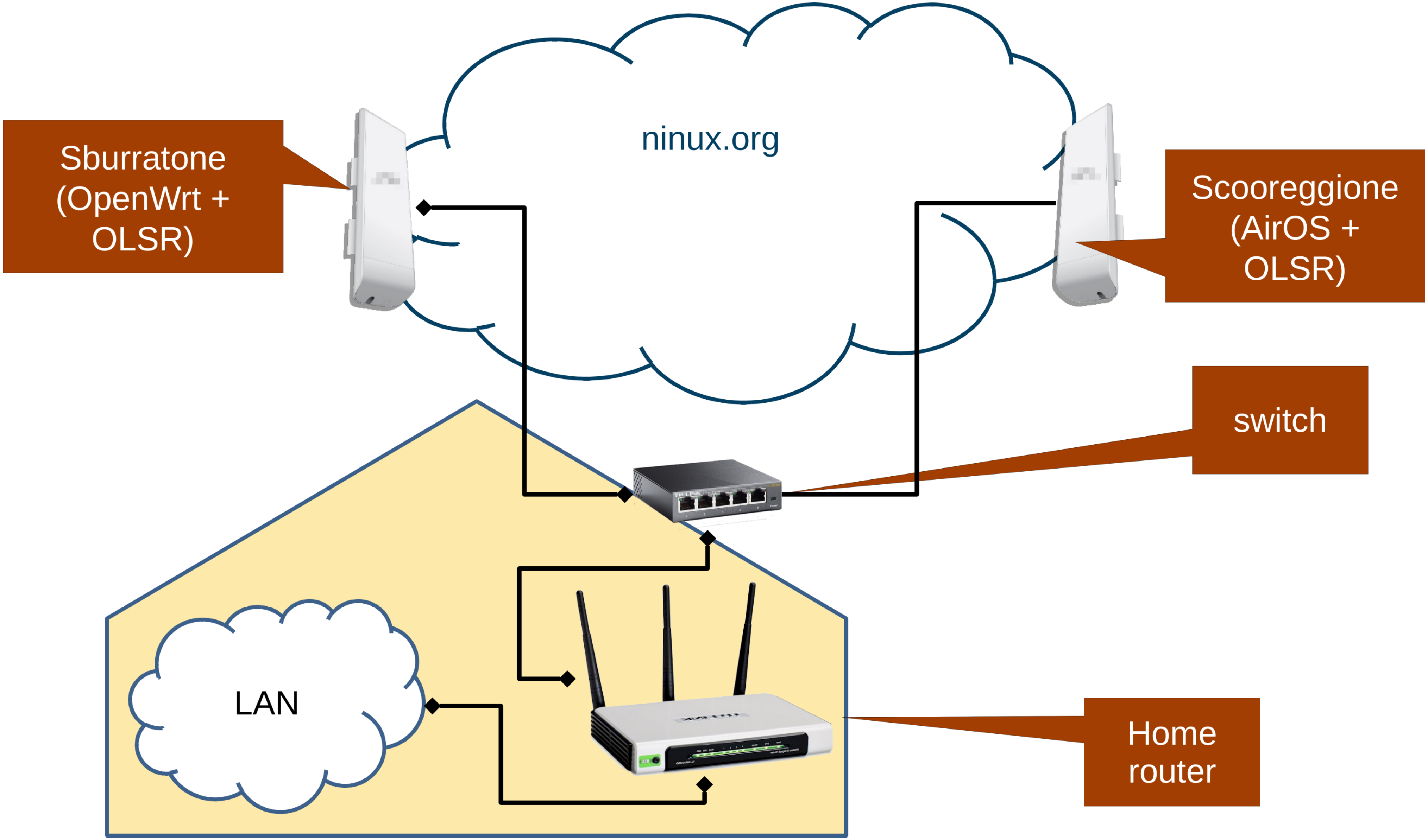
Ninux Rome

- OLSR (v1)
- IPv4 + IPv6 network
  - Uplinks:
    - BGP peerings (both IPv6 and IPv4)
    - DSLs (IPv4 only)
- Experimentation-oriented

Ninux Firmwares

- **Scooreggione**
  - customized OpenWrt with OLSR (v1)
- **Sburratone**
  - customized Ubiquiti AirOS with OLSR
    - Reversed firmware image at first, then Ubiquiti released the AirOS SDK
  - Why? Very active people joined but they wanted to use proprietary firmware. Their claims:
    - driver performance
      - and use of wireless proprietary extensions (e.g. AirMax)
    - user interfaces
    - firmware features
      - site survey (more about this later)
      - performance tests
      - ...

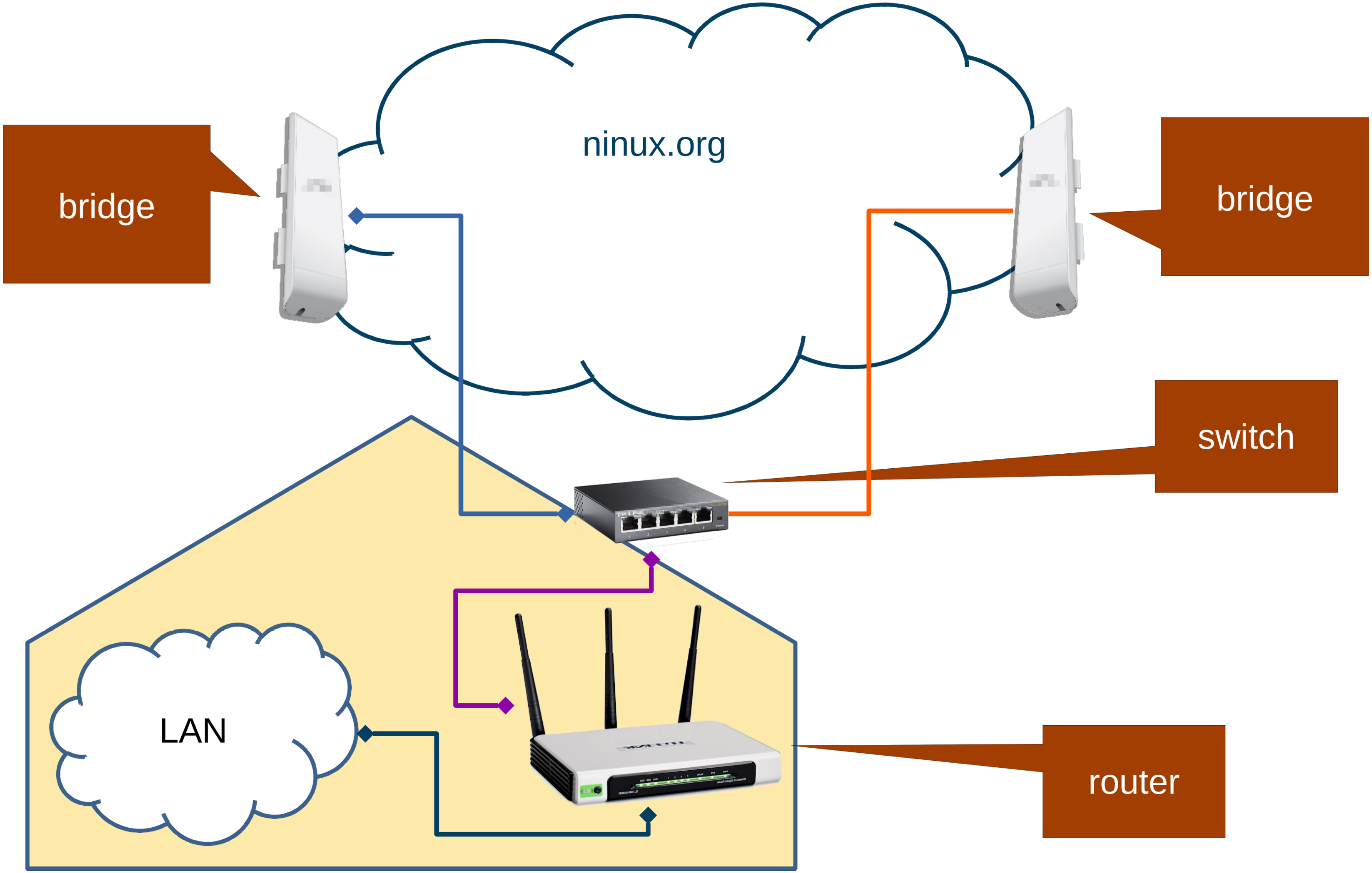
Ninux Roma node - routing on the roof



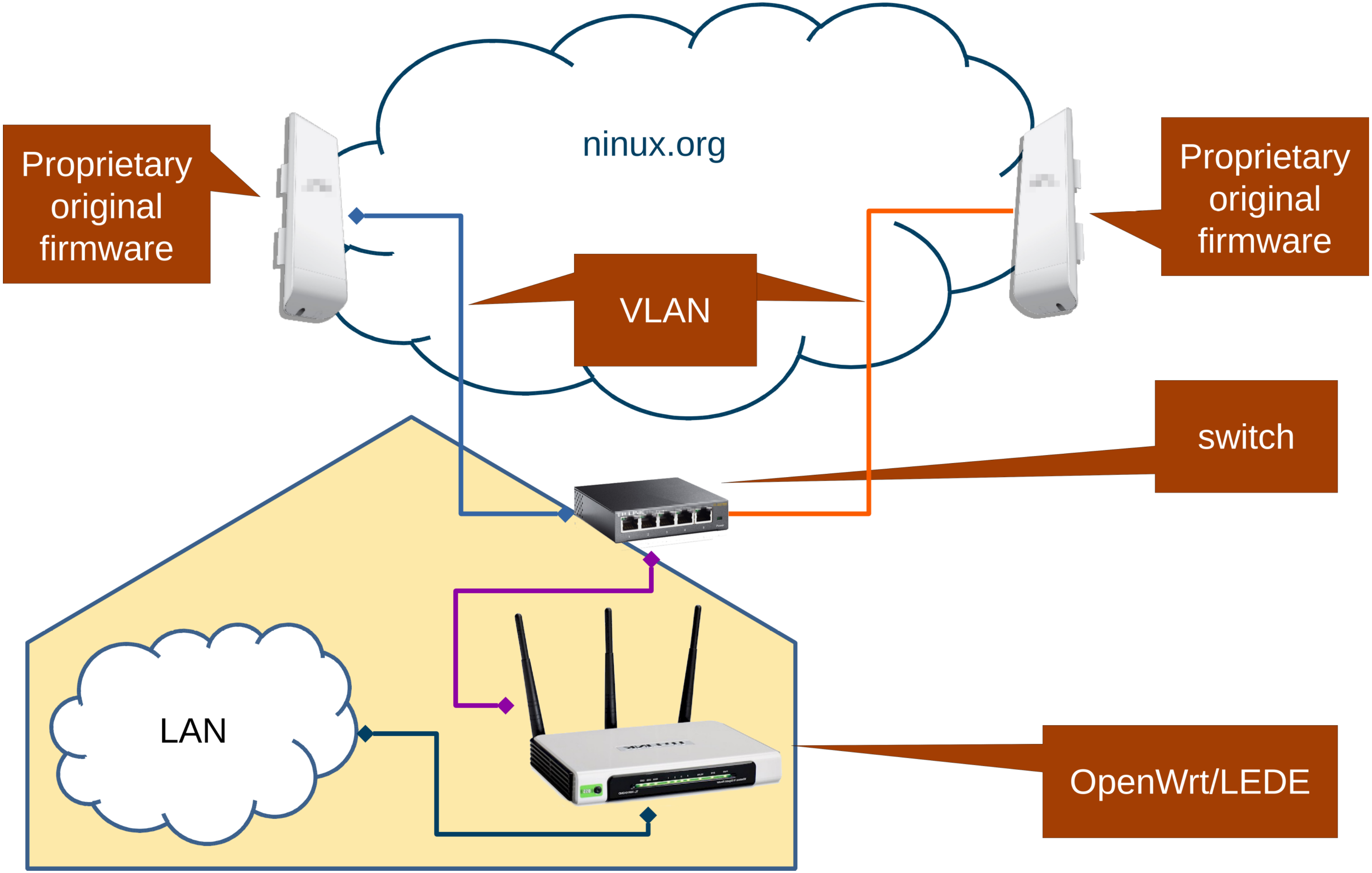
No more SDK!

- Ubiquiti decided to close its AirOS SDK in 2013
- Proposal by some: let's use the proprietary original firmware on the CPEs and move the routing to another device

ninux Roma node - ground routing



ninux Roma node - ground routing



Proprietary original firmware

Proprietary original firmware

VLAN

switch

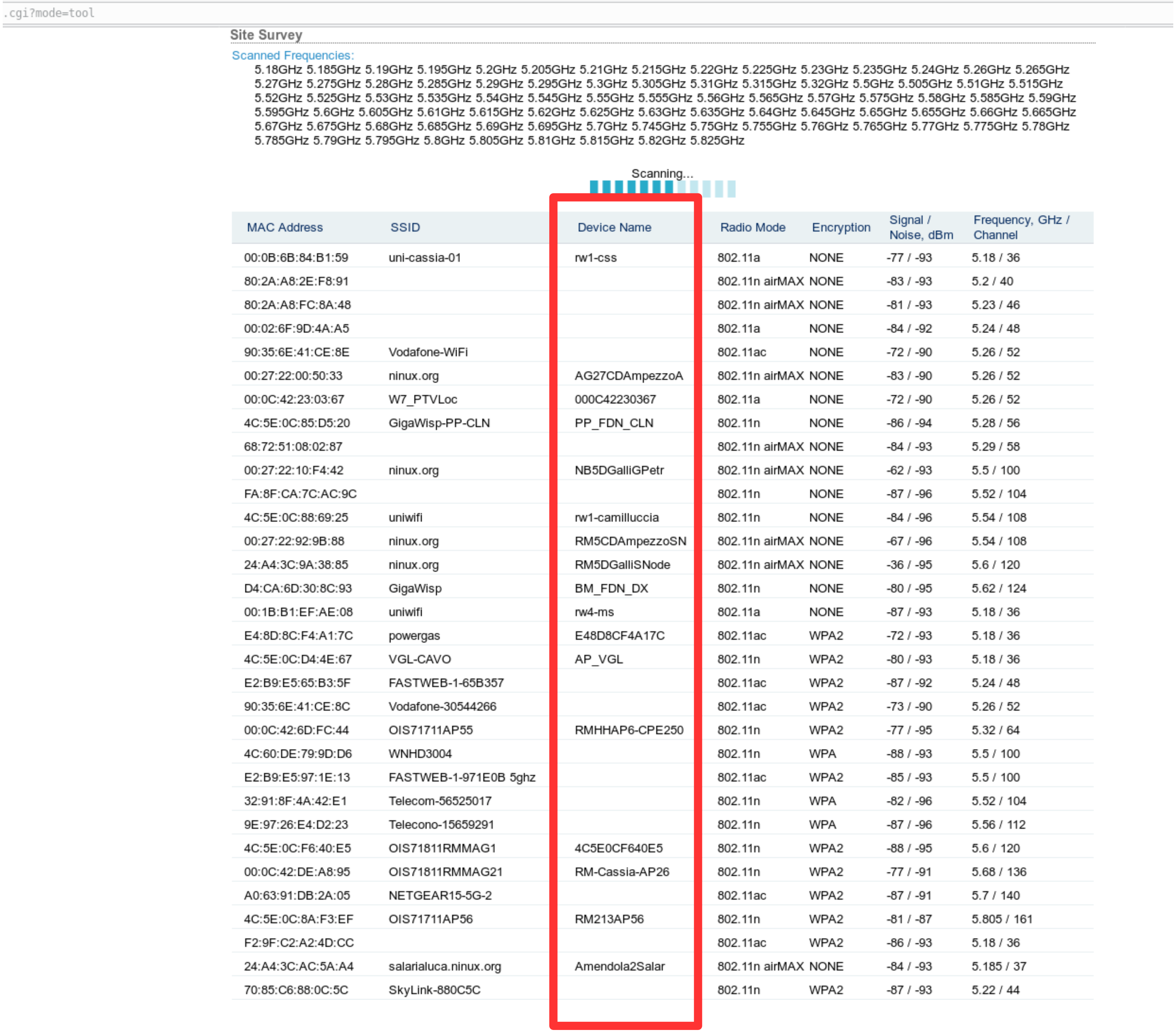
OpenWrt/LEDE

So...

- Result: we have a lot of different firmwares and node setups in the network
  - Sburratone
  - Scooreggione
  - Proprietary firmwares
  - Vanilla OpenWrt
  - Vanilla LEDE
  - Libremesh
  - ...

Site Survey

- One of the features missing in OpenWrt/LEDE according to proprietary firmware supporters is the “site survey” functionality
  - To understand what you are scanning when you are on the roof you can either:
    - use a unique SSID on each AP
    - maintain a database of MAC addresses
    - rely on the hostname as broadcast by the proprietary extensions



.cgi?mode=tool

Site Survey

Scanned Frequencies:

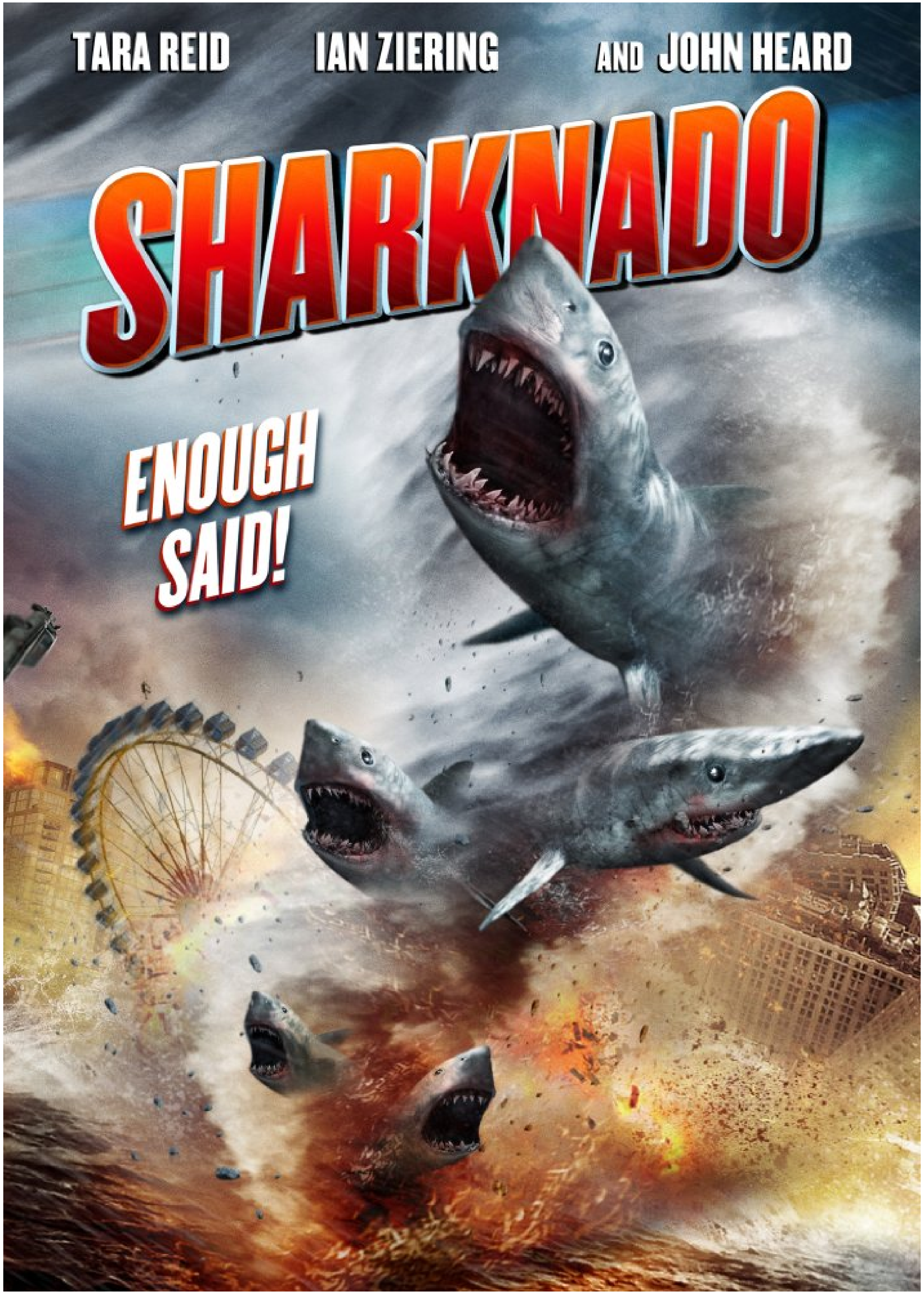
5.18GHz 5.185GHz 5.19GHz 5.195GHz 5.2GHz 5.205GHz 5.21GHz 5.215GHz 5.22GHz 5.225GHz 5.23GHz 5.235GHz 5.24GHz 5.26GHz 5.265GHz
5.27GHz 5.275GHz 5.28GHz 5.285GHz 5.29GHz 5.295GHz 5.3GHz 5.305GHz 5.31GHz 5.315GHz 5.32GHz 5.5GHz 5.505GHz 5.51GHz 5.515GHz
5.52GHz 5.525GHz 5.53GHz 5.535GHz 5.54GHz 5.545GHz 5.55GHz 5.555GHz 5.56GHz 5.565GHz 5.57GHz 5.575GHz 5.58GHz 5.585GHz 5.59GHz
5.595GHz 5.6GHz 5.605GHz 5.61GHz 5.615GHz 5.62GHz 5.625GHz 5.63GHz 5.635GHz 5.64GHz 5.645GHz 5.65GHz 5.655GHz 5.66GHz 5.665GHz
5.67GHz 5.675GHz 5.68GHz 5.685GHz 5.69GHz 5.695GHz 5.7GHz 5.745GHz 5.75GHz 5.755GHz 5.76GHz 5.765GHz 5.77GHz 5.775GHz 5.78GHz
5.785GHz 5.79GHz 5.795GHz 5.8GHz 5.805GHz 5.81GHz 5.815GHz 5.82GHz 5.825GHz

Scanning...

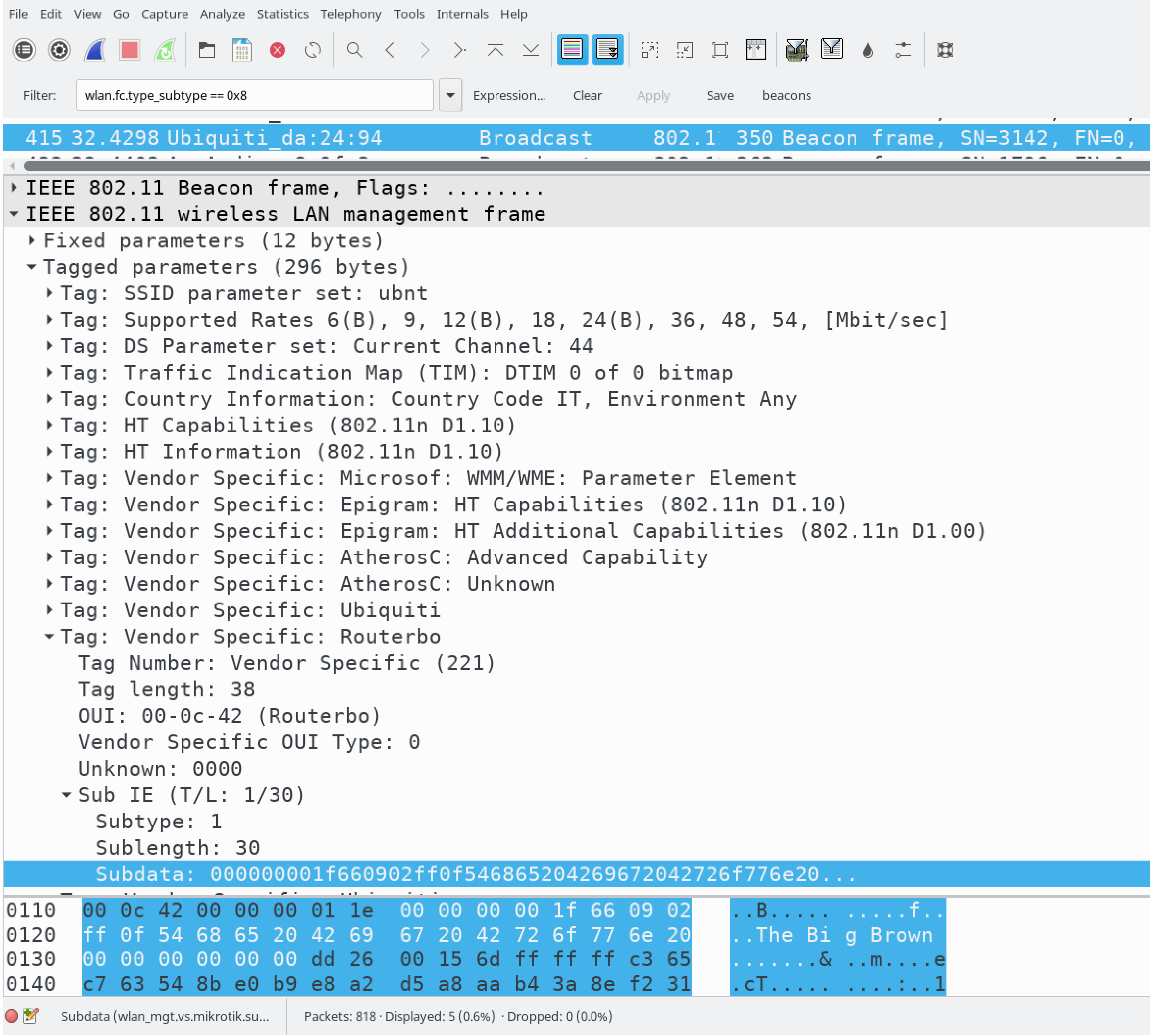
MAC Address	SSID	Device Name	Radio Mode	Encryption	Signal / Noise, dBm	Frequency, GHz / Channel
00:0B:6B:84:B1:59	uni-cassia-01	rw1-css	802.11a	NONE	-77 / -93	5.18 / 36
80:2A:A8:2E:F8:91			802.11n airMAX	NONE	-83 / -93	5.2 / 40
80:2A:A8:FC:8A:48			802.11n airMAX	NONE	-81 / -93	5.23 / 46
00:02:6F:9D:4A:A5			802.11a	NONE	-84 / -92	5.24 / 48
90:35:6E:41:CE:8E	Vodafone-WiFi		802.11ac	NONE	-72 / -90	5.26 / 52
00:27:22:00:50:33	ninux.org	AG27CDAmpezzoA	802.11n airMAX	NONE	-83 / -90	5.26 / 52
00:0C:42:23:03:67	W7_PTVLoc	000C42230367	802.11a	NONE	-72 / -90	5.26 / 52
4C:5E:0C:85:D5:20	GigaWisp-PP-CLN	PP_FDN_CLN	802.11n	NONE	-86 / -94	5.28 / 56
68:72:51:08:02:87			802.11n airMAX	NONE	-84 / -93	5.29 / 58
00:27:22:10:F4:42	ninux.org	NB5DGalliGPetr	802.11n airMAX	NONE	-62 / -93	5.5 / 100
FA:8F:CA:7C:AC:9C			802.11n	NONE	-87 / -96	5.52 / 104
4C:5E:0C:88:69:25	uniwifi	rw1-camilluccia	802.11n	NONE	-84 / -96	5.54 / 108
00:27:22:92:9B:88	ninux.org	RM5CDAmpezzoSN	802.11n airMAX	NONE	-67 / -96	5.54 / 108
24:A4:3C:9A:38:85	ninux.org	RM5DGalliSNode	802.11n airMAX	NONE	-36 / -95	5.6 / 120
D4:CA:6D:30:8C:93	GigaWisp	BM_FDN_DX	802.11n	NONE	-80 / -95	5.62 / 124
00:1B:B1:EF:AE:08	uniwifi	rw4-ms	802.11a	NONE	-87 / -93	5.18 / 36
E4:8D:8C:F4:A1:7C	powergas	E48D8CF4A17C	802.11ac	WPA2	-72 / -93	5.18 / 36
4C:5E:0C:D4:4E:67	VGL-CAVO	AP_VGL	802.11n	WPA2	-80 / -93	5.18 / 36
E2:B9:E5:65:B3:5F	FASTWEB-1-65B357		802.11ac	WPA2	-87 / -92	5.24 / 48
90:35:6E:41:CE:8C	Vodafone-30544266		802.11ac	WPA2	-73 / -90	5.26 / 52
00:0C:42:6D:FC:44	OIS71711AP55	RMHHAP6-CPE250	802.11n	WPA2	-77 / -95	5.32 / 64
4C:60:DE:79:9D:D6	WNHD3004		802.11n	WPA	-88 / -93	5.5 / 100
E2:B9:E5:97:1E:13	FASTWEB-1-971E0B 5ghz		802.11ac	WPA2	-85 / -93	5.5 / 100
32:91:8F:4A:42:E1	Telecom-56525017		802.11n	WPA	-82 / -96	5.52 / 104
9E:97:26:E4:D2:23	Telecono-15659291		802.11n	WPA	-87 / -96	5.56 / 112
4C:5E:0C:F6:40:E5	OIS71811RMMAG1	4C5E0CF640E5	802.11n	WPA2	-88 / -95	5.6 / 120
00:0C:42:DE:A8:95	OIS71811RMMAG21	RM-Cassia-AP26	802.11n	WPA2	-77 / -91	5.68 / 136
A0:63:91:DB:2A:05	NETGEAR15-5G-2		802.11ac	WPA2	-87 / -91	5.7 / 140
4C:5E:0C:8A:F3:EF	OIS71711AP56	RM213AP56	802.11n	WPA2	-81 / -87	5.805 / 161
F2:9F:C2:A2:4D:CC			802.11ac	WPA2	-86 / -93	5.18 / 36
24:A4:3C:AC:5A:A4	salarialuca.ninux.org	Amendola2Salar	802.11n airMAX	NONE	-84 / -93	5.185 / 37
70:85:C6:88:0C:5C	SkyLink-880C5C		802.11n	WPA2	-87 / -93	5.22 / 44

Site Survey

- How is this done?
- Proprietary extensions to the IEEE 802.11 beacons



TARA REID
IAN ZIERING
AND JOHN HEARD
SHARKNADO
ENOUGH SAID!



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save
beacons

Filter: wlan.fc.type_subtype == 0x8

```
415 32.4298 Ubiquiti_da:24:94      Broadcast      802.1  350 Beacon frame, SN=3142, FN=0,
```

```
▸ IEEE 802.11 Beacon frame, Flags: ........
▾ IEEE 802.11 wireless LAN management frame
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (296 bytes)
    ▸ Tag: SSID parameter set: ubnt
    ▸ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 44
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: Country Information: Country Code IT, Environment Any
    ▸ Tag: HT Capabilities (802.11n D1.10)
    ▸ Tag: HT Information (802.11n D1.10)
    ▸ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    ▸ Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
    ▸ Tag: Vendor Specific: Epigram: HT Additional Capabilities (802.11n D1.00)
    ▸ Tag: Vendor Specific: AtherosC: Advanced Capability
    ▸ Tag: Vendor Specific: AtherosC: Unknown
    ▸ Tag: Vendor Specific: Ubiquiti
    ▾ Tag: Vendor Specific: Routerbo
        Tag Number: Vendor Specific (221)
        Tag length: 38
        OUI: 00-0c-42 (Routerbo)
        Vendor Specific OUI Type: 0
        Unknown: 0000
      ▾ Sub IE (T/L: 1/30)
          Subtype: 1
          Sublength: 30
          Subdata: 000000001f660902ff0f54686520426967204272 6f776e20...
```

```
0110  00 0c 42 00 00 00 01 1e  00 00 00 00 1f 66 09 02   ..B..... .....f..
0120  ff 0f 54 68 65 20 42 69  67 20 42 72 6f 77 6e 20   ..The Bi g Brown 
0130  00 00 00 00 00 00 dd 26  00 15 6d ff ff ff c3 65   .......& ..m....e
0140  c7 63 54 8b e0 b9 e8 a2  d5 a8 aa b4 3a 8e f2 31   .cT..... ....:..1
```

Subdata (wlan_mgt.vs.mikrotik.su... Packets: 818 · Displayed: 5 (0.6%) · Dropped: 0 (0.0%)

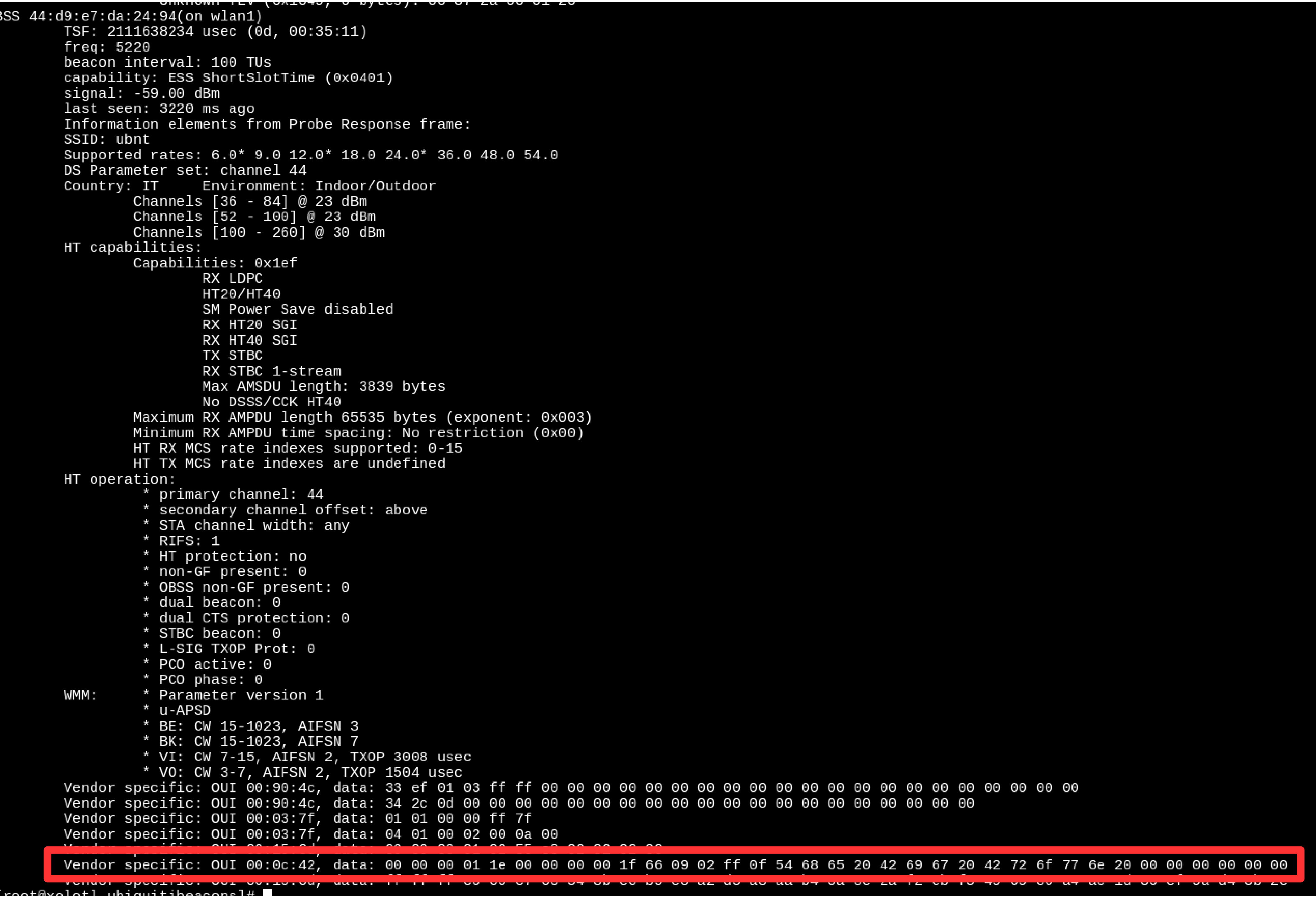
Information Elements (IEs)

- IEEE 802.11 management frames may contain groups of fields called Information Elements (in a way similar to TLVs)
  - The Beacon frames may contain Vendor-Specific IEs
    - The Vendor Specific IE is used to carry information not defined in the standard

Element ID	Length	OUI	Vendor-specific content
1	1	3	n-3 (octects)

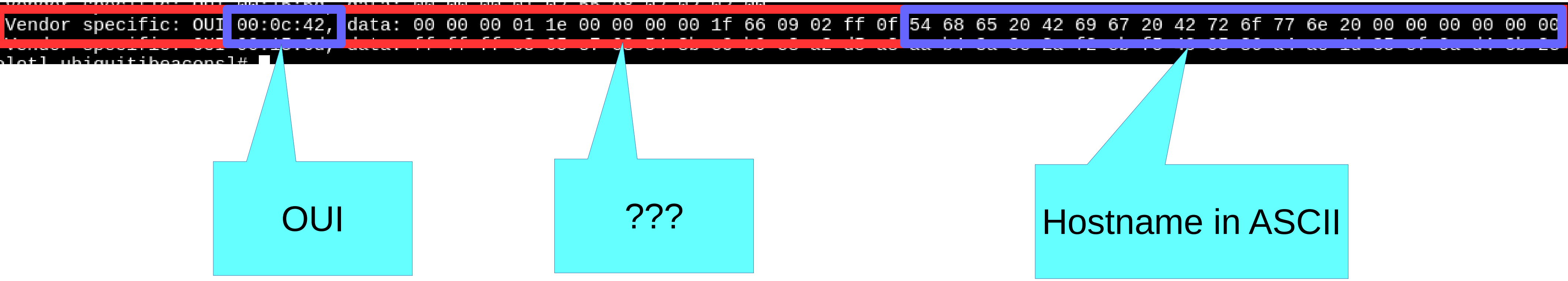
- The OUI field shall be a public OUI assigned by the IEEE
  - In our case 00:0c:42 (assigned to Routerboard.com - Mikrotik)

iw dev wlan0 scan -u

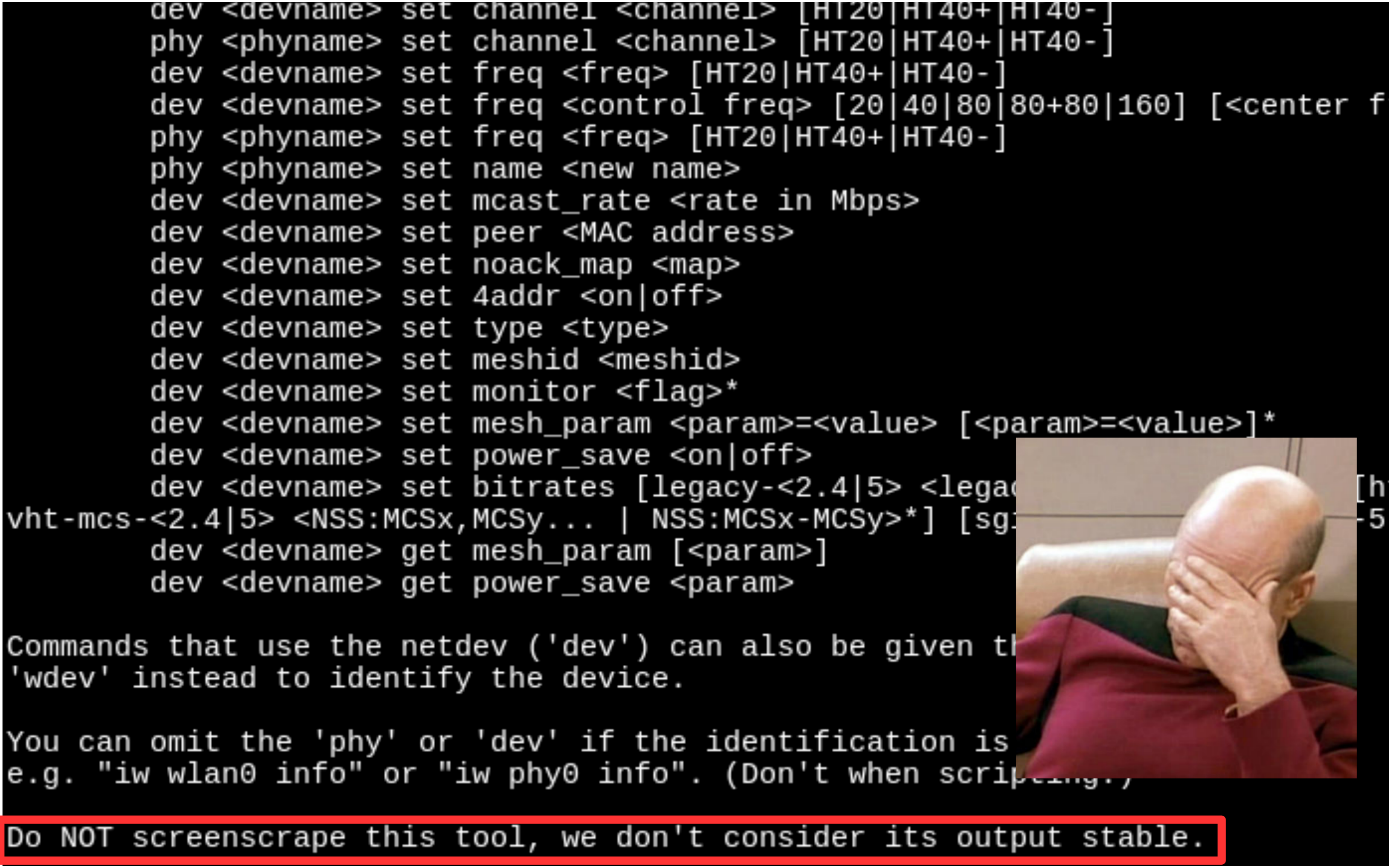


```
                Unknown TLV (0x1049, 6 bytes): 00 37 2a 00 01 20
BSS 44:d9:e7:da:24:94(on wlan1)
        TSF: 2111638234 usec (0d, 00:35:11)
        freq: 5220
        beacon interval: 100 TUs
        capability: ESS ShortSlotTime (0x0401)
        signal: -59.00 dBm
        last seen: 3220 ms ago
        Information elements from Probe Response frame:
        SSID: ubnt
        Supported rates: 6.0* 9.0 12.0* 18.0 24.0* 36.0 48.0 54.0
        DS Parameter set: channel 44
        Country: IT     Environment: Indoor/Outdoor
                Channels [36 - 84] @ 23 dBm
                Channels [52 - 100] @ 23 dBm
                Channels [100 - 260] @ 30 dBm
        HT capabilities:
                Capabilities: 0x1ef
                        RX LDPC
                        HT20/HT40
                        SM Power Save disabled
                        RX HT20 SGI
                        RX HT40 SGI
                        TX STBC
                        RX STBC 1-stream
                        Max AMSDU length: 3839 bytes
                        No DSSS/CCK HT40
                Maximum RX AMPDU length 65535 bytes (exponent: 0x003)
                Minimum RX AMPDU time spacing: No restriction (0x00)
                HT RX MCS rate indexes supported: 0-15
                HT TX MCS rate indexes are undefined
        HT operation:
                 * primary channel: 44
                 * secondary channel offset: above
                 * STA channel width: any
                 * RIFS: 1
                 * HT protection: no
                 * non-GF present: 0
                 * OBSS non-GF present: 0
                 * dual beacon: 0
                 * dual CTS protection: 0
                 * STBC beacon: 0
                 * L-SIG TXOP Prot: 0
                 * PCO active: 0
                 * PCO phase: 0
        WMM:     * Parameter version 1
                 * u-APSD
                 * BE: CW 15-1023, AIFSN 3
                 * BK: CW 15-1023, AIFSN 7
                 * VI: CW 7-15, AIFSN 2, TXOP 3008 usec
                 * VO: CW 3-7, AIFSN 2, TXOP 1504 usec
        Vendor specific: OUI 00:90:4c, data: 33 ef 01 03 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        Vendor specific: OUI 00:90:4c, data: 34 2c 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        Vendor specific: OUI 00:03:7f, data: 01 01 00 00 ff 7f
        Vendor specific: OUI 00:03:7f, data: 04 01 00 02 00 0a 00
        Vendor specific: OUI 00:15:6d, data: 00 00 00 01 00 55 c8 08 00 00 00
        Vendor specific: OUI 00:0c:42, data: 00 00 00 01 1e 00 00 00 00 1f 66 09 02 ff 0f 54 68 65 20 42 69 67 20 42 72 6f 77 6e 20 00 00 00 00 00 00
        Vendor specific: OUI 00:15:6d, data: [illegible]
[root@xolotl ubiquitibeacons]#
```

Hostname IEs format



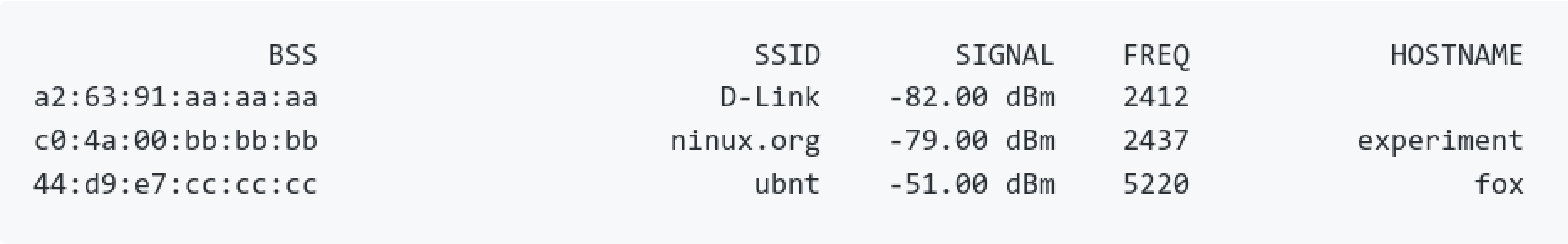
```
Vendor specific: OUI 00:0c:42, data: 00 00 00 01 1e 00 00 00 00 1f 66 09 02 ff 0f 54 68 65 20 42 69 67 20 42 72 6f 77 6e 20 00 00 00 00 00 00
```



```
        dev <devname> set channel <channel> [HT20|HT40+|HT40-]
        phy <phyname> set channel <channel> [HT20|HT40+|HT40-]
        dev <devname> set freq <freq> [HT20|HT40+|HT40-]
        dev <devname> set freq <control freq> [20|40|80|80+80|160] [<center f
        phy <phyname> set freq <freq> [HT20|HT40+|HT40-]
        phy <phyname> set name <new name>
        dev <devname> set mcast_rate <rate in Mbps>
        dev <devname> set peer <MAC address>
        dev <devname> set noack_map <map>
        dev <devname> set 4addr <on|off>
        dev <devname> set type <type>
        dev <devname> set meshid <meshid>
        dev <devname> set monitor <flag>*
        dev <devname> set mesh_param <param>=<value> [<param>=<value>]*
        dev <devname> set power_save <on|off>
        dev <devname> set bitrates [legacy-<2.4|5> <legac                   [h
vht-mcs-<2.4|5> <NSS:MCSx,MCSy... | NSS:MCSx-MCSy>*] [sg                    -5
        dev <devname> get mesh_param [<param>]
        dev <devname> get power_save <param>

Commands that use the netdev ('dev') can also be given th
'wdev' instead to identify the device.

You can omit the 'phy' or 'dev' if the identification is
e.g. "iw wlan0 info" or "iw phy0 info". (Don't when scripting.)

Do NOT screenscrape this tool, we don't consider its output stable.
```

sitesurvey script

- busybox-friendly shell script
- Takes the output of the vendor elements from iw -u and performs a translation to ASCII



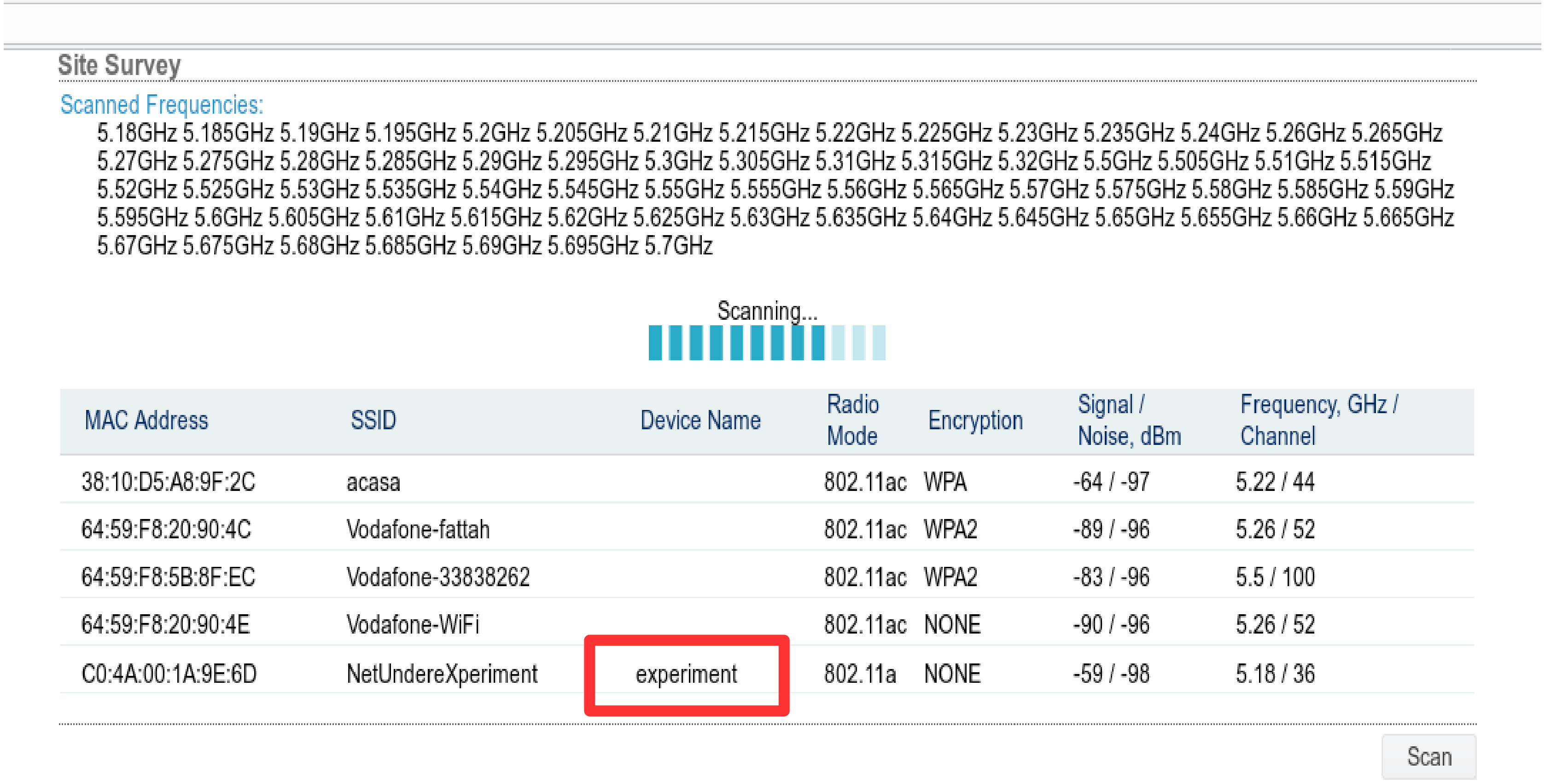
```
              BSS                          SSID        SIGNAL    FREQ            HOSTNAME
a2:63:91:aa:aa:aa                        D-Link    -82.00 dBm    2412
c0:4a:00:bb:bb:bb                     ninux.org    -79.00 dBm    2437          experiment
44:d9:e7:cc:cc:cc                          ubnt    -51.00 dBm    5220                 fox
```

And on the AP side?

- vendor_elements in hostapd.conf
- generatevendorelements script

generatevendorelements script

```
echo vendor_elements=$(./generatevendorelements experiment) >> hostapd.conf

hostapd hostapd.conf
```



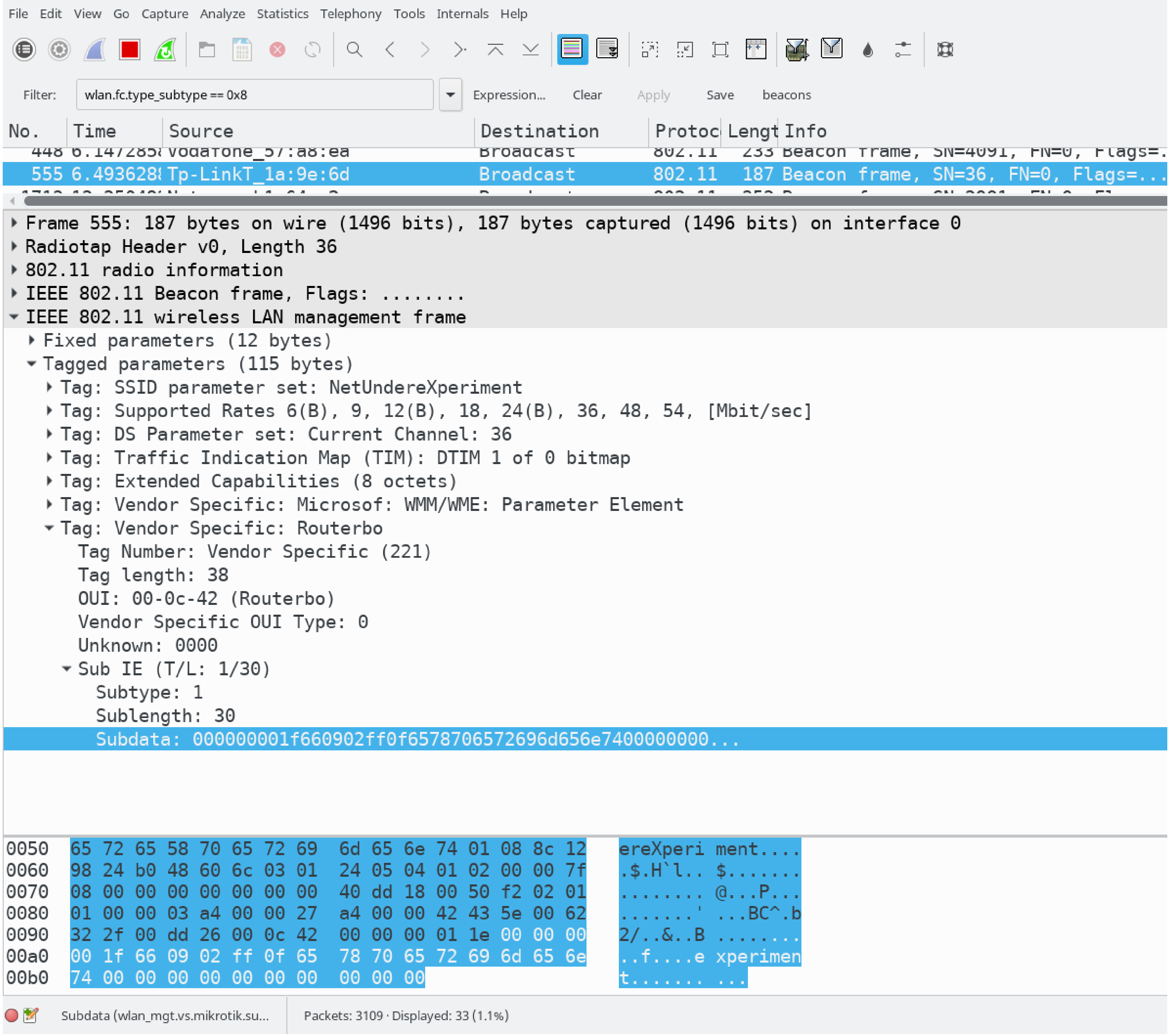
Site Survey

Scanned Frequencies:

5.18GHz 5.185GHz 5.19GHz 5.195GHz 5.2GHz 5.205GHz 5.21GHz 5.215GHz 5.22GHz 5.225GHz 5.23GHz 5.235GHz 5.24GHz 5.26GHz 5.265GHz 5.27GHz 5.275GHz 5.28GHz 5.285GHz 5.29GHz 5.295GHz 5.3GHz 5.305GHz 5.31GHz 5.315GHz 5.32GHz 5.5GHz 5.505GHz 5.51GHz 5.515GHz 5.52GHz 5.525GHz 5.53GHz 5.535GHz 5.54GHz 5.545GHz 5.55GHz 5.555GHz 5.56GHz 5.565GHz 5.57GHz 5.575GHz 5.58GHz 5.585GHz 5.59GHz 5.595GHz 5.6GHz 5.605GHz 5.61GHz 5.615GHz 5.62GHz 5.625GHz 5.63GHz 5.635GHz 5.64GHz 5.645GHz 5.65GHz 5.655GHz 5.66GHz 5.665GHz 5.67GHz 5.675GHz 5.68GHz 5.685GHz 5.69GHz 5.695GHz 5.7GHz

MAC Address	SSID	Device Name	Radio Mode	Encryption	Signal / Noise, dBm	Frequency, GHz / Channel
38:10:D5:A8:9F:2C	acasa		802.11ac	WPA	-64 / -97	5.22 / 44
64:59:F8:20:90:4C	Vodafone-fattah		802.11ac	WPA2	-89 / -96	5.26 / 52
64:59:F8:5B:8F:EC	Vodafone-33838262		802.11ac	WPA2	-83 / -96	5.5 / 100
64:59:F8:20:90:4E	Vodafone-WiFi		802.11ac	NONE	-90 / -96	5.26 / 52
C0:4A:00:1A:9E:6D	NetUndereXperiment	experiment	802.11a	NONE	-59 / -98	5.18 / 36

SHARKNADO 2
THE SECOND ONE
SHARK HAPPENS!
Syfy
Imagine Greater



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.fc.type_subtype == 0x8

Expression... Clear Apply Save beacons

```
No.  Time       Source              Destination   Protoc Lengt Info
 448 6.147285   Vodafone_57:a8:ea   Broadcast     802.11  233 Beacon frame, SN=4091, FN=0, Flags=.
 555 6.493628   Tp-LinkT_1a:9e:6d   Broadcast     802.11  187 Beacon frame, SN=36, FN=0, Flags=...
```

```
▸ Frame 555: 187 bytes on wire (1496 bits), 187 bytes captured (1496 bits) on interface 0
▸ Radiotap Header v0, Length 36
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........
▾ IEEE 802.11 wireless LAN management frame
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (115 bytes)
    ▸ Tag: SSID parameter set: NetUndereXperiment
    ▸ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 36
    ▸ Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
    ▸ Tag: Extended Capabilities (8 octets)
    ▸ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    ▾ Tag: Vendor Specific: Routerbo
        Tag Number: Vendor Specific (221)
        Tag length: 38
        OUI: 00-0c-42 (Routerbo)
        Vendor Specific OUI Type: 0
        Unknown: 0000
      ▾ Sub IE (T/L: 1/30)
          Subtype: 1
          Sublength: 30
          Subdata: 000000001f660902ff0f6578706572696d656e7400000000...
```

```
0050  65 72 65 58 70 65 72 69  6d 65 6e 74 01 08 8c 12   ereXperi ment....
0060  98 24 b0 48 60 6c 03 01  24 05 04 01 02 00 00 7f   .$.H`l.. $.......
0070  08 00 00 00 00 00 00 00  40 dd 18 00 50 f2 02 01   ........ @...P...
0080  01 00 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62   .......' ...BC^.b
0090  32 2f 00 dd 26 00 0c 42  00 00 00 01 1e 00 00 00   2/..&..B ........
00a0  00 1f 66 09 02 ff 0f 65  78 70 65 72 69 6d 65 6e   ..f....e xperimen
00b0  74 00 00 00 00 00 00 00  00 00 00                  t....... ...
```

Subdata (wlan_mgt.vs.mikrotik.su... Packets: 3109 · Displayed: 33 (1.1%)

Support in OpenWrt/LEDE

- iw scan -u is not working
  - in both OpenWrt and LEDE
  - a patch disables the -u option
  - works on old OpenWrt versions
    - tried on Attitude Adjustment
- hostapd vendor_elements
  - ubus support in LEDE 17.01 and OpenWRT 15.05

200-reduce-size.patch

```
@@ -1835,6 +1838,7 @@ void print_ies(unsigned char *ie, int ie
                    ieprinters[ie[0]].name &&
                    ieprinters[ie[0]].flags & BIT(ptype)) {
                        print_ie(&ieprinters[ie[0]], ie[0], ie[1], ie + 2);
+#if 0
                } else if (ie[0] == 221 /* vendor */) {
                        print_vendor(ie[1], ie + 2, unknown, ptype);
                } else if (unknown) {
@@ -1844,6 +1848,7 @@ void print_ies(unsigned char *ie, int ie
                        for (i=0; i<ie[1]; i++)
                                printf(" %.2x", ie[2+i]);
                        printf("\n");
+#endif
                }
                ielen -= ie[1] + 2;
                ie += ie[1] + 2;
```

iw binary: 75049 bytes
iw binary without the above hunks: 79869 bytes
Delta = 4820 bytes

vendor_elements support in OpenWrt/LEDE

```
ubus -v list hostapd.wlan0
```

```
ubus call hostapd.wlan0 set_vendor_elements
'{"vendor_elements":
"dd26000c42000000011e000000001f660902ff0f6578706572696d656e
7400000000000000000000"}'
```

```
ubus call hostapd.wlan0 update_beacon
```

Notes

- scraping iw is bad
  - a parsable (JSON?) output option for iw would be nice to have :)
- How to bring back iw scan -u?
  - remove the hunk from patch 200?
  - submit a new patch?
  - create a new “iw-full” package?

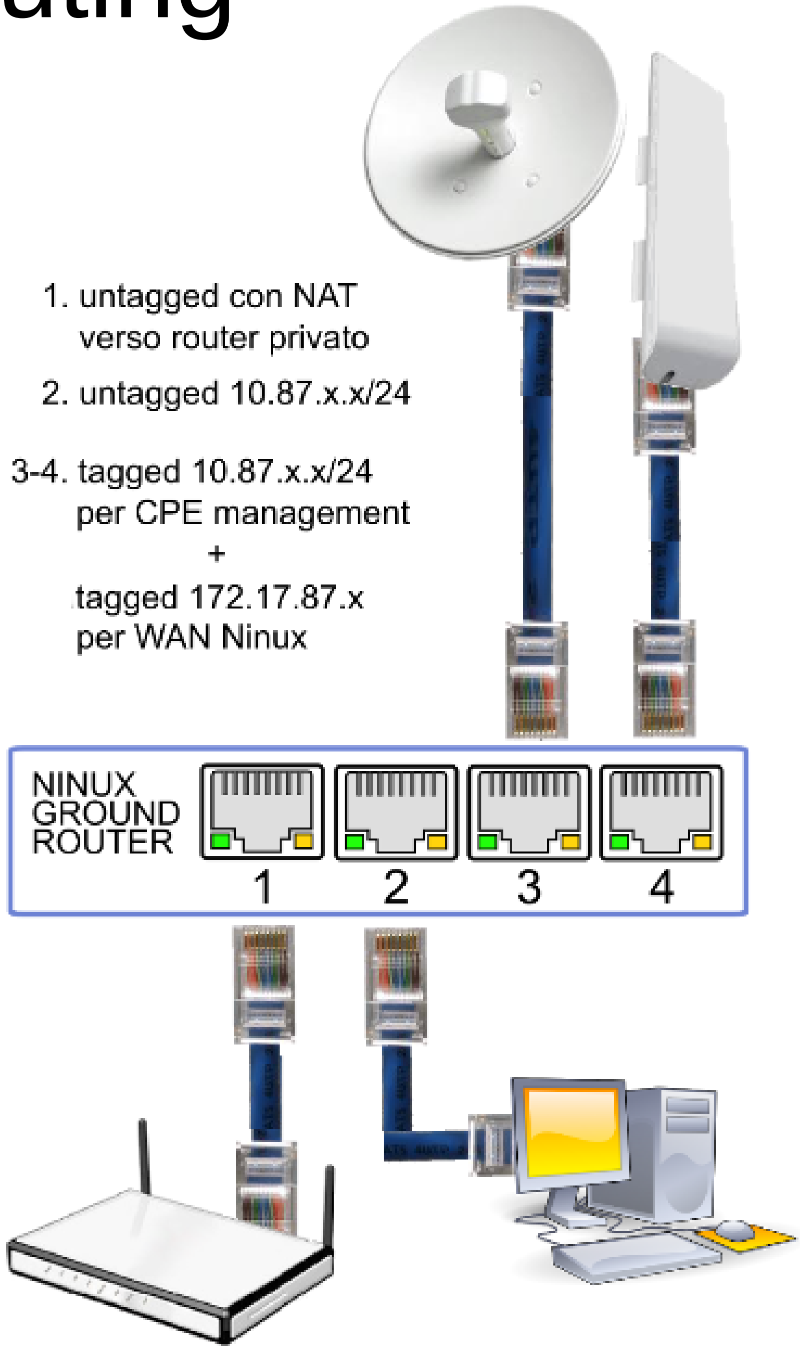
References

- https://github.com/cl4u2/ieswescan
- No More AirOS SDK
  https://community.ubnt.com/t5/airOS-SDK-Custom-Development/No-more-SDK/td-p/440237

Thank you!

Ground Routing

- Several outdoor routers:
  - In bridge mode
  - Each one on a different VLAN
- A single router:
  - usually indoor, on the ground
  - runs olsrd (over OpenWrt)
    - Routing logic


1. untagged con NAT
verso router privato
2. untagged 10.87.x.x/24
3-4. tagged 10.87.x.x/24
per CPE management
+
tagged 172.17.87.x
per WAN Ninux
NINUX
GROUND
ROUTER
1
2
3
4