CORE SECURITY
Thinking Ahead.

DEF CON 23

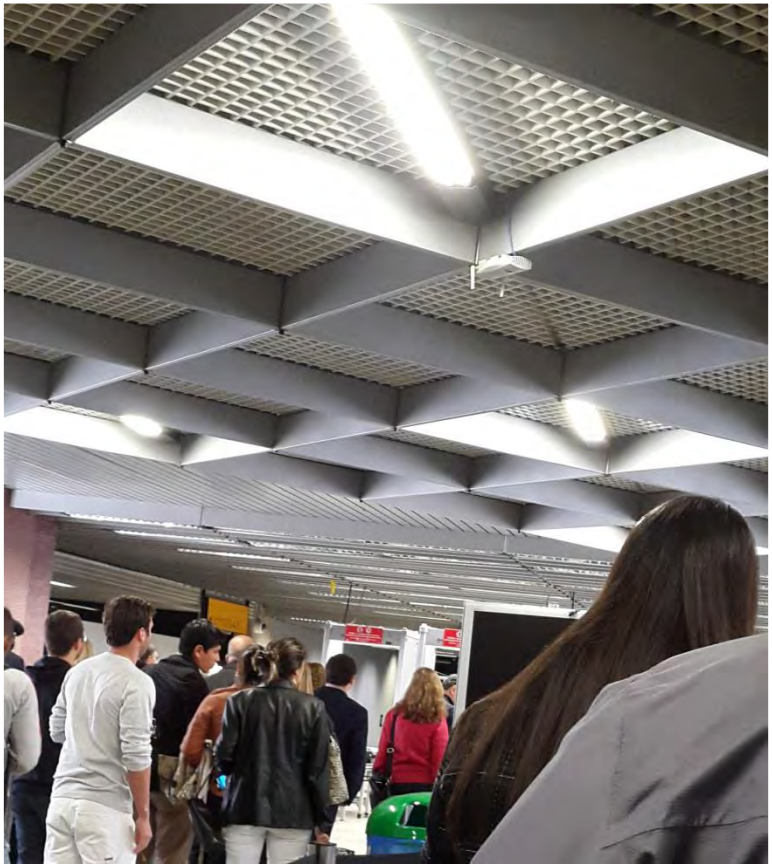
802.11 Massive Monitoring

Andrés Blanco - Andrés Gazzoli

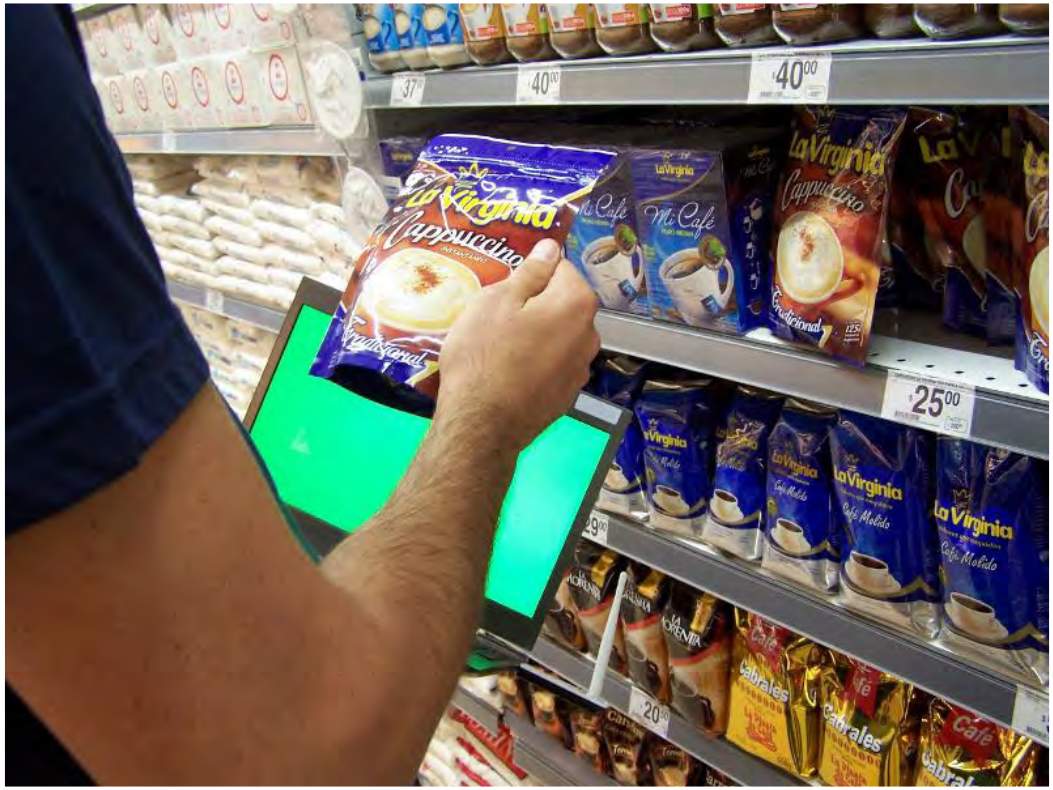
Outline

- Introduction
- Approaches
- The USB Dilemma
- Distributed System
- WiWo
- Questions

Introduction [Who is this talk for? **]**



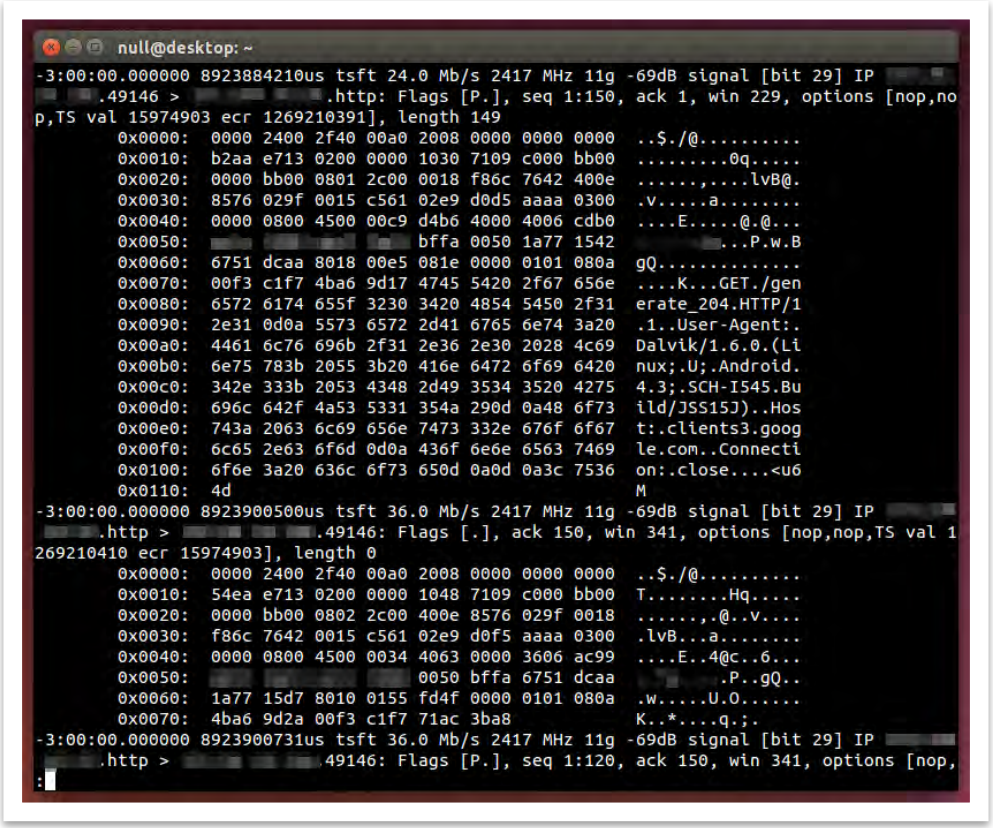
Introduction [Who is this talk for? **]**



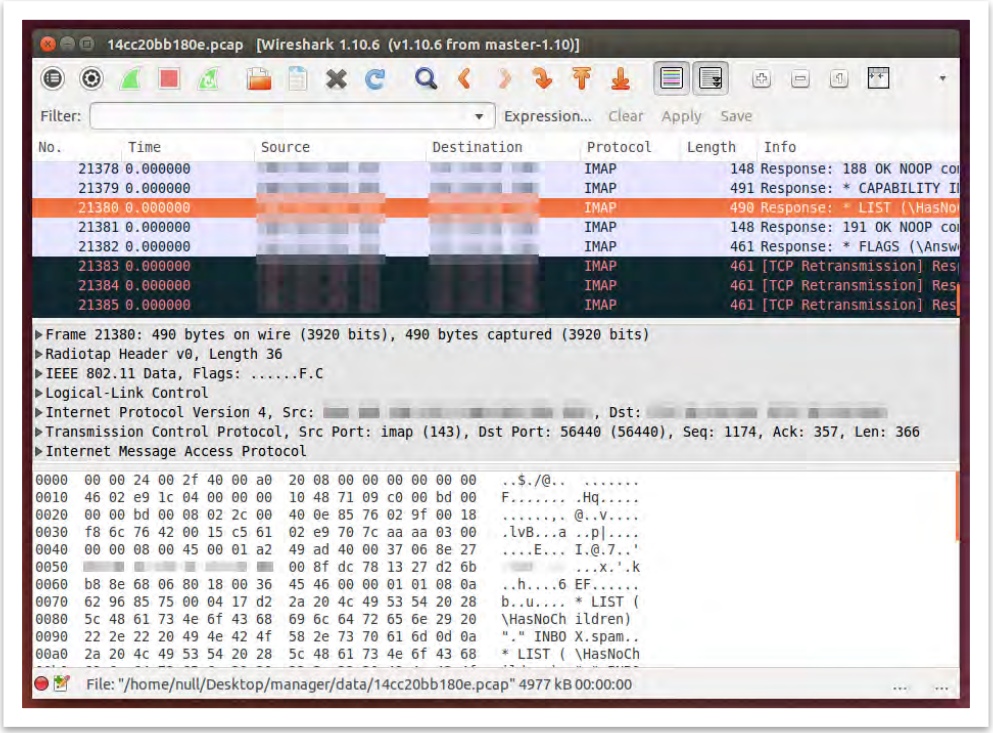
Introduction [Who is this talk for? **]**



Introduction [Who is this talk for? **]**



Introduction [Who is this talk for? **]**



- Monitor
  - Channel hopping traffic (such as WiFi-Direct)
  - Access Points with auto channel selection
  - Multiple Access Points on different channels
  - Stations
  - Multiple locations at the same time
- Inject frames on multiple channels

Introduction [802.11 channels **]**

2.4 GHz (802.11b/g/n)

Channel	Frequency
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

3.6 GHz (802.11y)

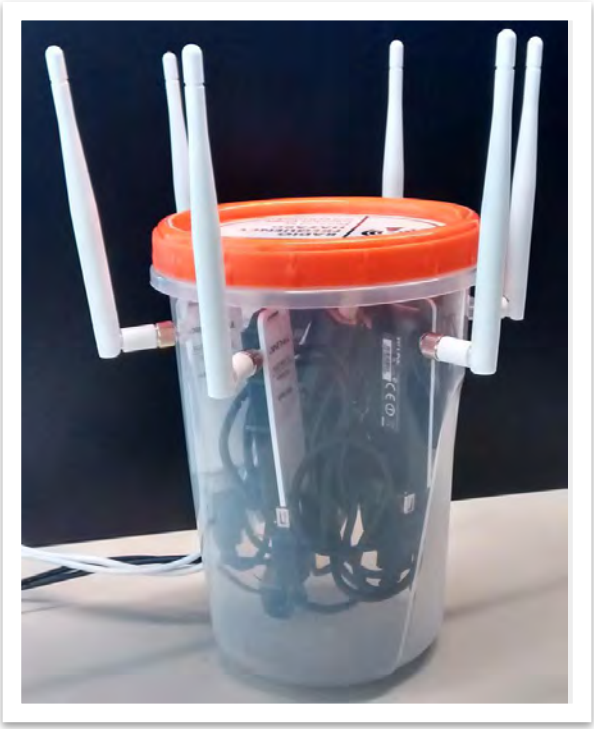
Channel	Frequency
131	3657.5
132	3660.0 - 3662.5
133	3665.0 - 3667.5
134	3670.0 - 3672.5
135	3675.0 - 3677.5
136	3680.0 - 3682.5
137	3685.0 - 3687.5
138	3690.0 - 3692.5

5 GHz (802.11a/h/j/n/ac)

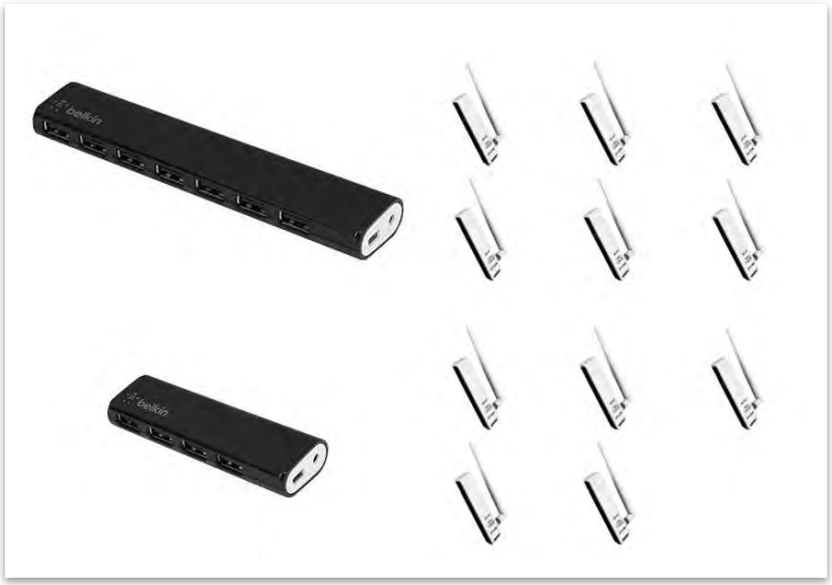
Channel	Frequency	Channel	Frequency
36	5180	116	5580
40	5200	120	5600
44	5220	124	5620
48	5240	128	5640
52	5260	132	5660
56	5280	136	5680
60	5300	140	5700
64	5320	149	5745
100	5500	153	5765
104	5520	157	5785
108	5540	161	5805
112	5560	165	5825

Approaches [first approach **]**



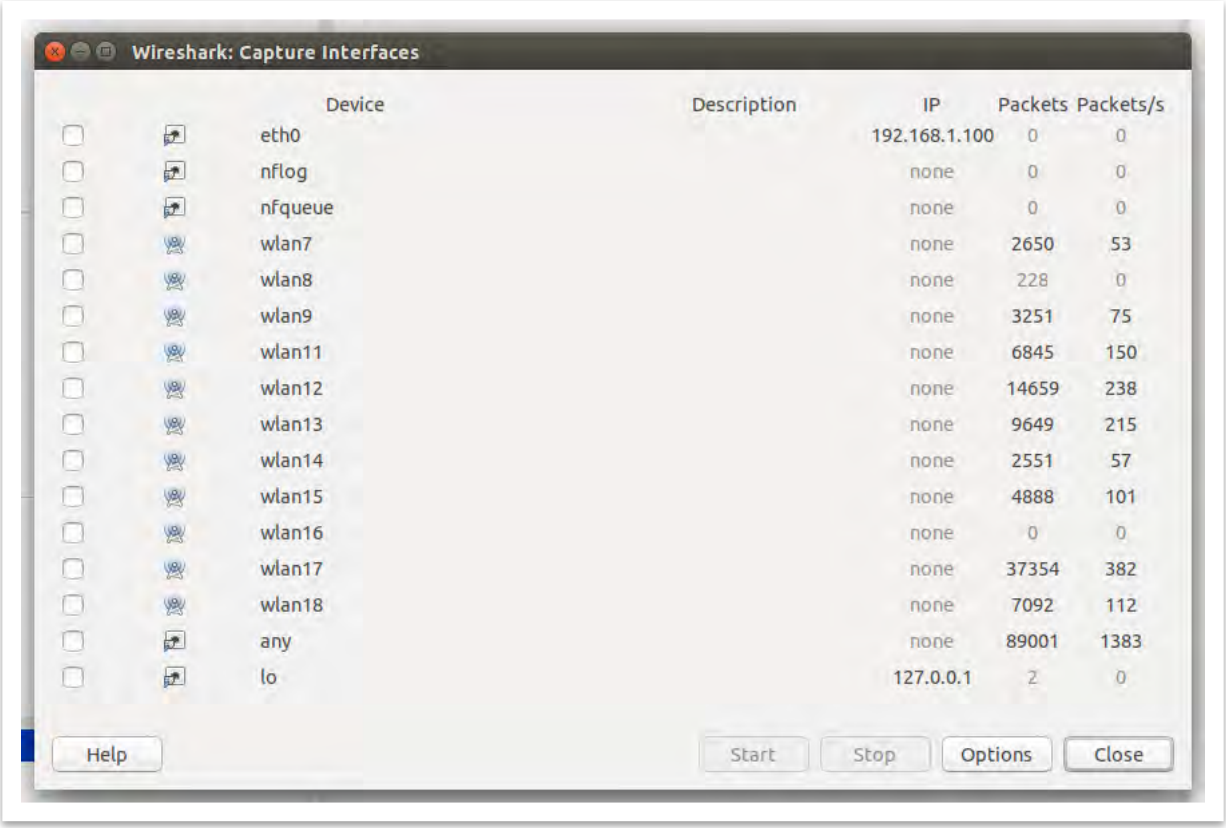


Approaches [second approach **]**

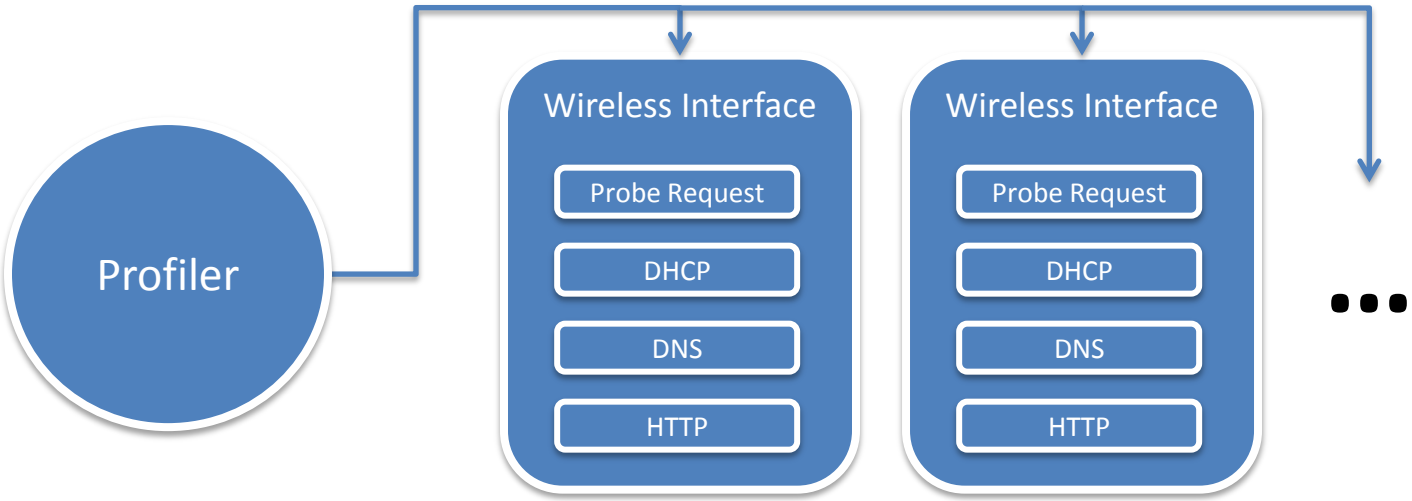




Approaches [wireshark **]**



Approaches [station profiler **]**



Demo [second approach **]**



Wireless Network Traffic could be displayed during the demo.
Please disable Wi-Fi if you don’t want to be part of it.

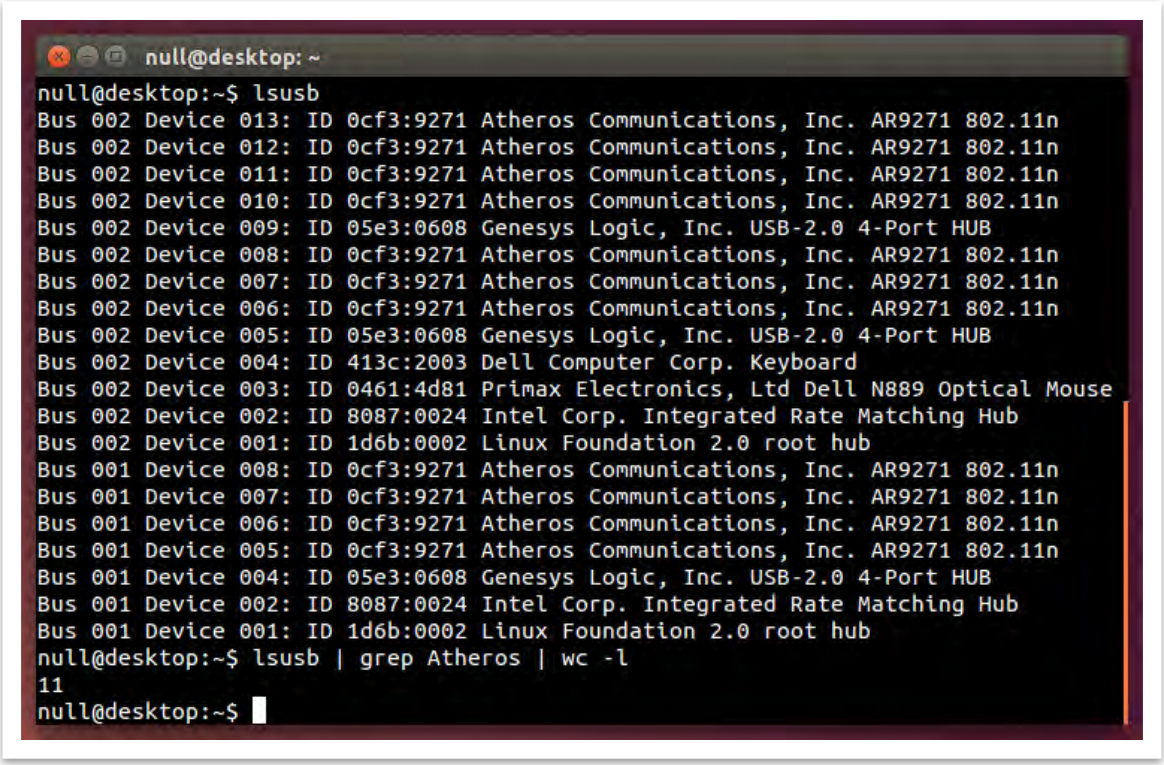
The USB Dilemma [scalability **]**



The USB Dilemma [scalability]



The USB Dilemma [bus saturation **]**

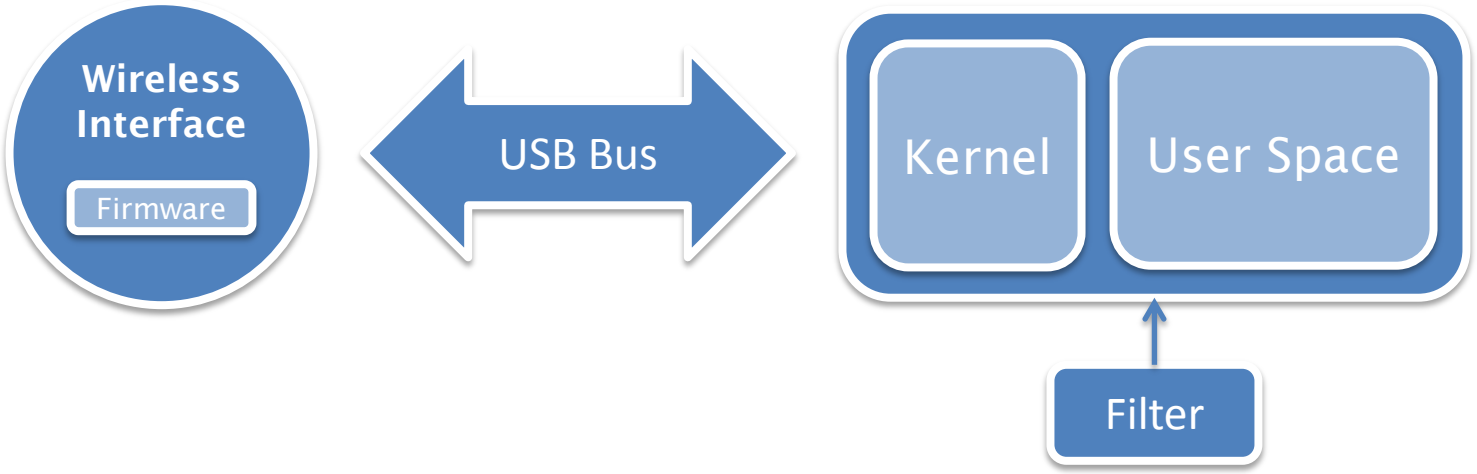


Demo [bus saturation **]**



Wireless Network Traffic could be displayed during the demo.
Please disable Wi-Fi if you don’t want to be part of it.

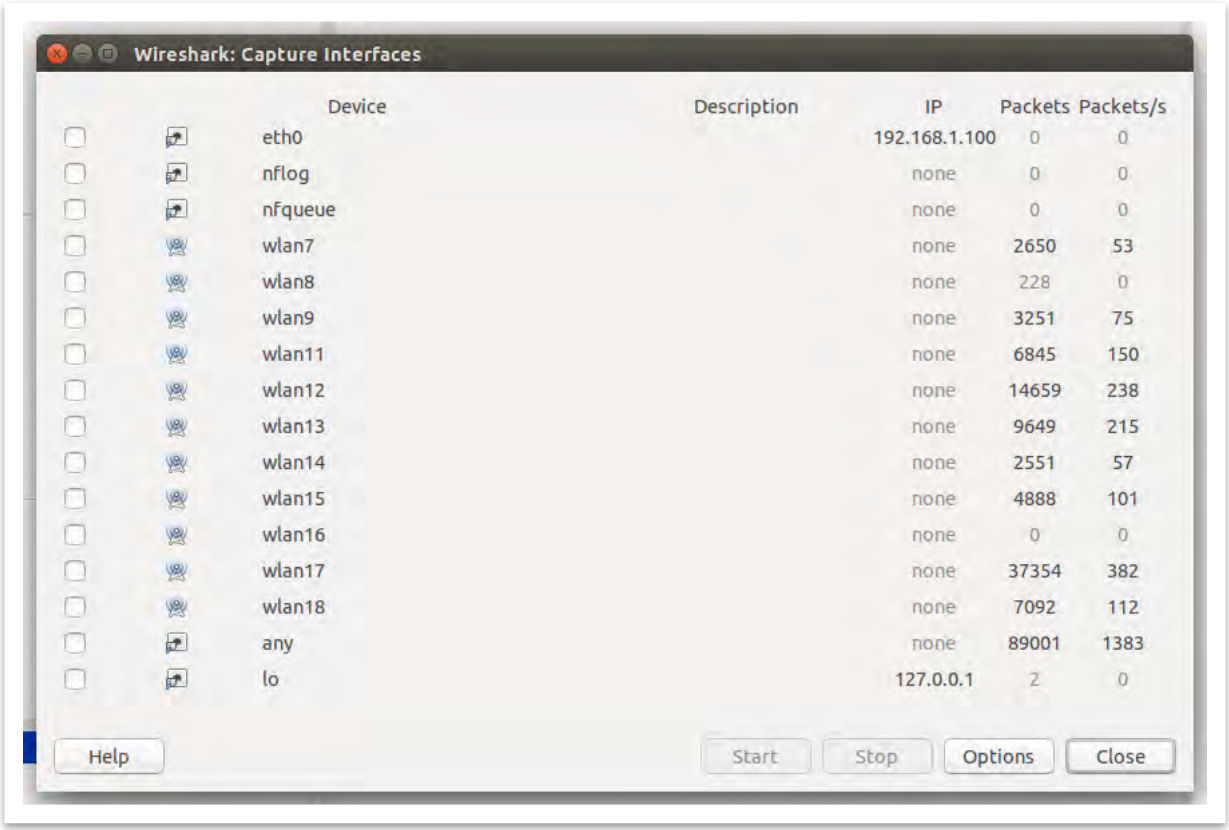
The USB Dilemma [bus saturation **]**



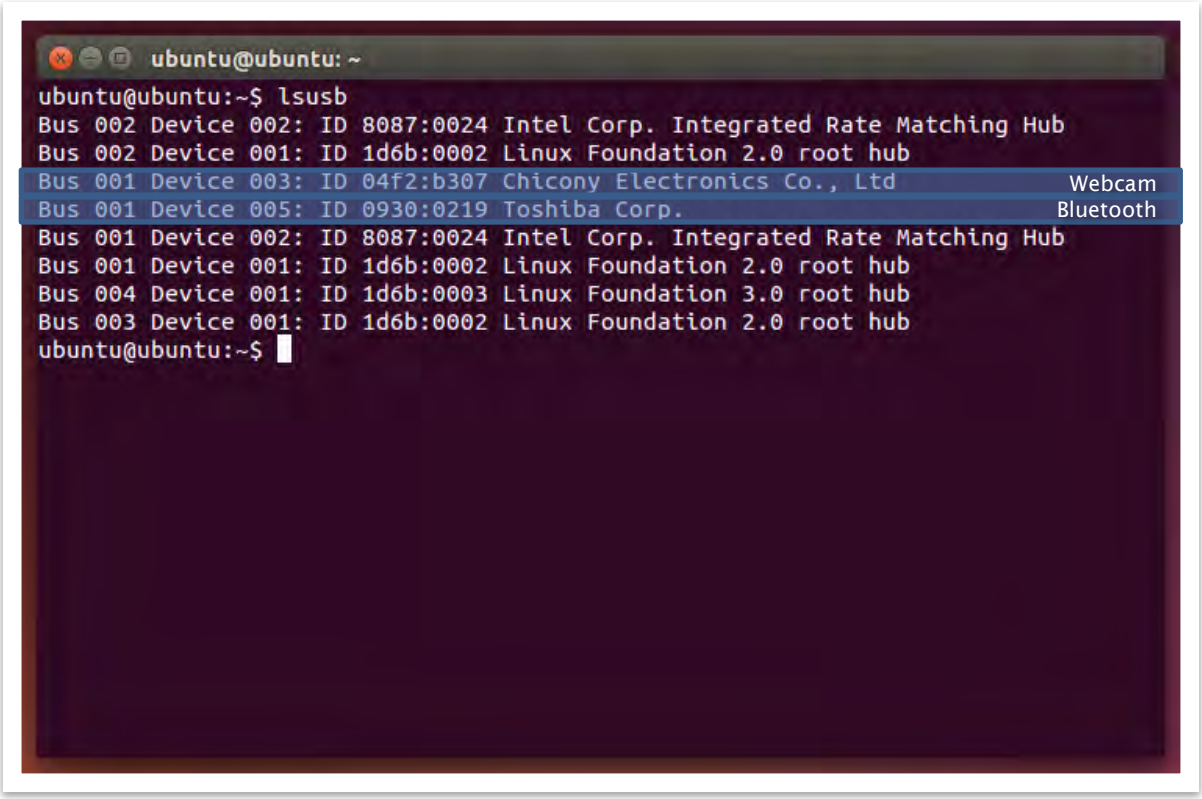
The USB Dilemma [bus saturation **]**



The USB Dilemma [bus saturation **]**



The USB Dilemma [non-removable devices **]**



The USB Dilemma [non-removable devices **]**



The USB Dilemma [available buses]

```
ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ lsusb
Bus 002 Device 002: ID 8087:0024 Intel
Bus 002 Device 001: ID 1d6b:0002 Linux
Bus 001 Device 003: ID 04f2:b307 Chicon
Bus 001 Device 005: ID 0930:0219 Toshib
Bus 001 Device 007: ID 0cf3:9271 Atherc
Bus 001 Device 002: ID 8087:0024 Intel
Bus 001 Device 001: ID 1d6b:0002 Linux
Bus 004 Device 001: ID 1d6b:0003 Linux
Bus 003 Device 001: ID 1d6b:0002 Linux
ubuntu@ubuntu:~$
```



USB Port 1

The USB Dilemma [available buses]

```
ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ lsusb
Bus 002 Device 002: ID 8087:0024 Intel
Bus 002 Device 001: ID 1d6b:0002 Linux
Bus 001 Device 003: ID 04f2:b307 Chicon
Bus 001 Device 005: ID 0930:0219 Toshib
Bus 001 Device 002: ID 8087:0024 Intel
Bus 001 Device 001: ID 1d6b:0002 Linux
Bus 004 Device 001: ID 1d6b:0003 Linux
Bus 003 Device 004: ID 0cf3:9271 Athero
Bus 003 Device 001: ID 1d6b:0002 Linux
ubuntu@ubuntu:~$
```





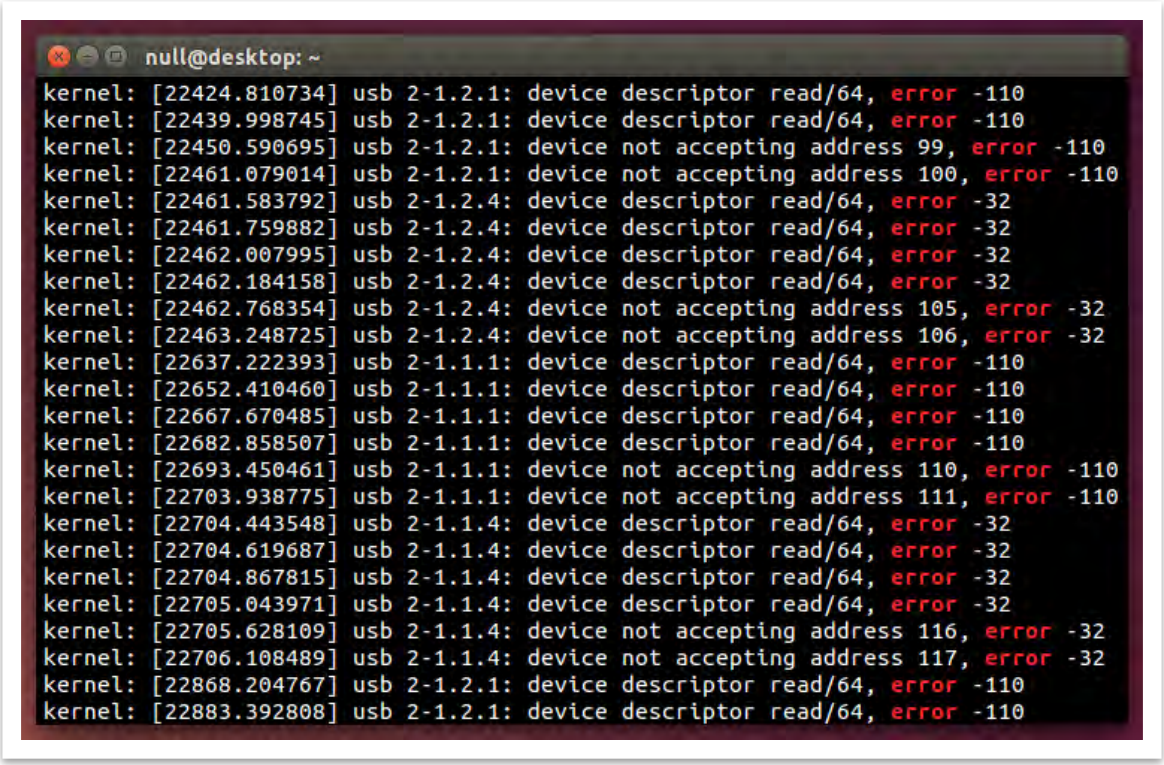
USB Port 2

The USB Dilemma [available buses]

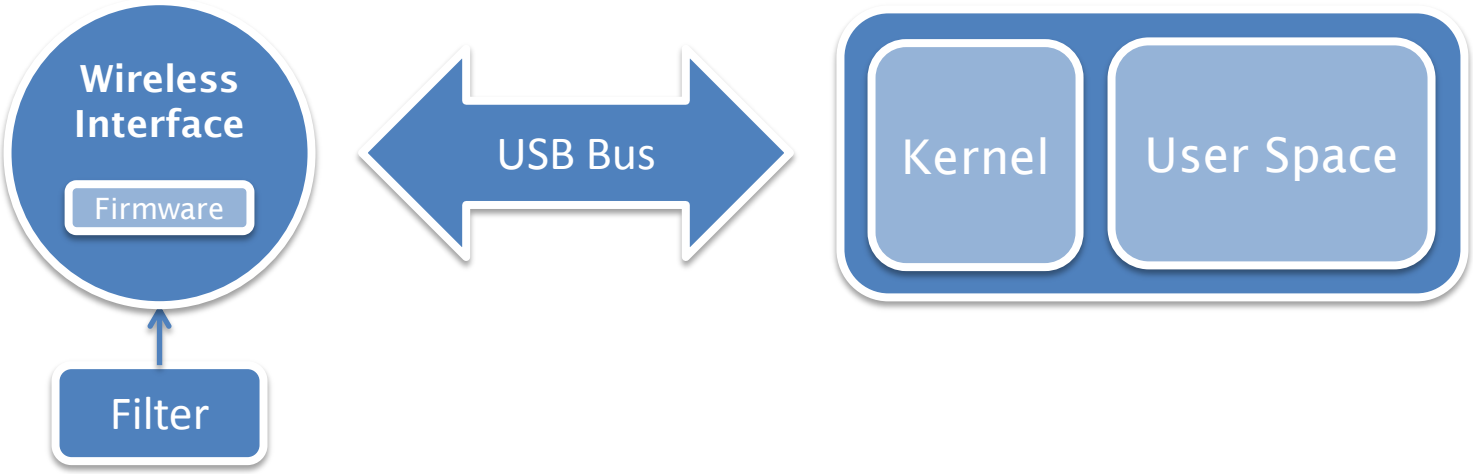
```
ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ lsusb
Bus 002 Device 002: ID 8087:0024 Intel
Bus 002 Device 001: ID 1d6b:0002 Linux
Bus 001 Device 003: ID 04f2:b307 Chicony
Bus 001 Device 005: ID 0930:0219 Toshiba
Bus 001 Device 002: ID 8087:0024 Intel
Bus 001 Device 001: ID 1d6b:0002 Linux
Bus 004 Device 001: ID 1d6b:0003 Linux
Bus 003 Device 005: ID 0cf3:9271 Athero
Bus 003 Device 001: ID 1d6b:0002 Linux
ubuntu@ubuntu:~$
```



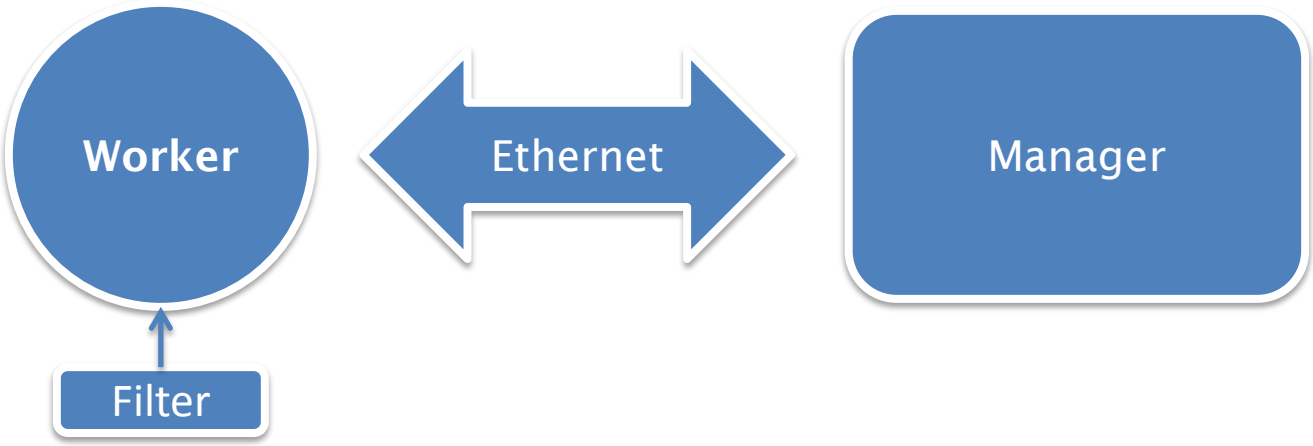
The USB Dilemma [power issues]



The USB Dilemma [the option? **]**



Distributed System [scalability]



Distributed System [scalability **]**



Distributed System [scalability **]**











WiWo is a distributed 802.11 monitoring and injecting system that was designed to be simple and scalable, in which all workers (nodes) can be managed by a Python framework.



CPU	Atheros AR7240@400MHz
RAM	32MiB
Flash	4MiB
Network	1 x 100MBit

TP-Link TL-MR3020



CPU	Atheros AR9344 @ 560 MHz
RAM	128MiB
Flash	8MiB
Network	4 x 1000MBit

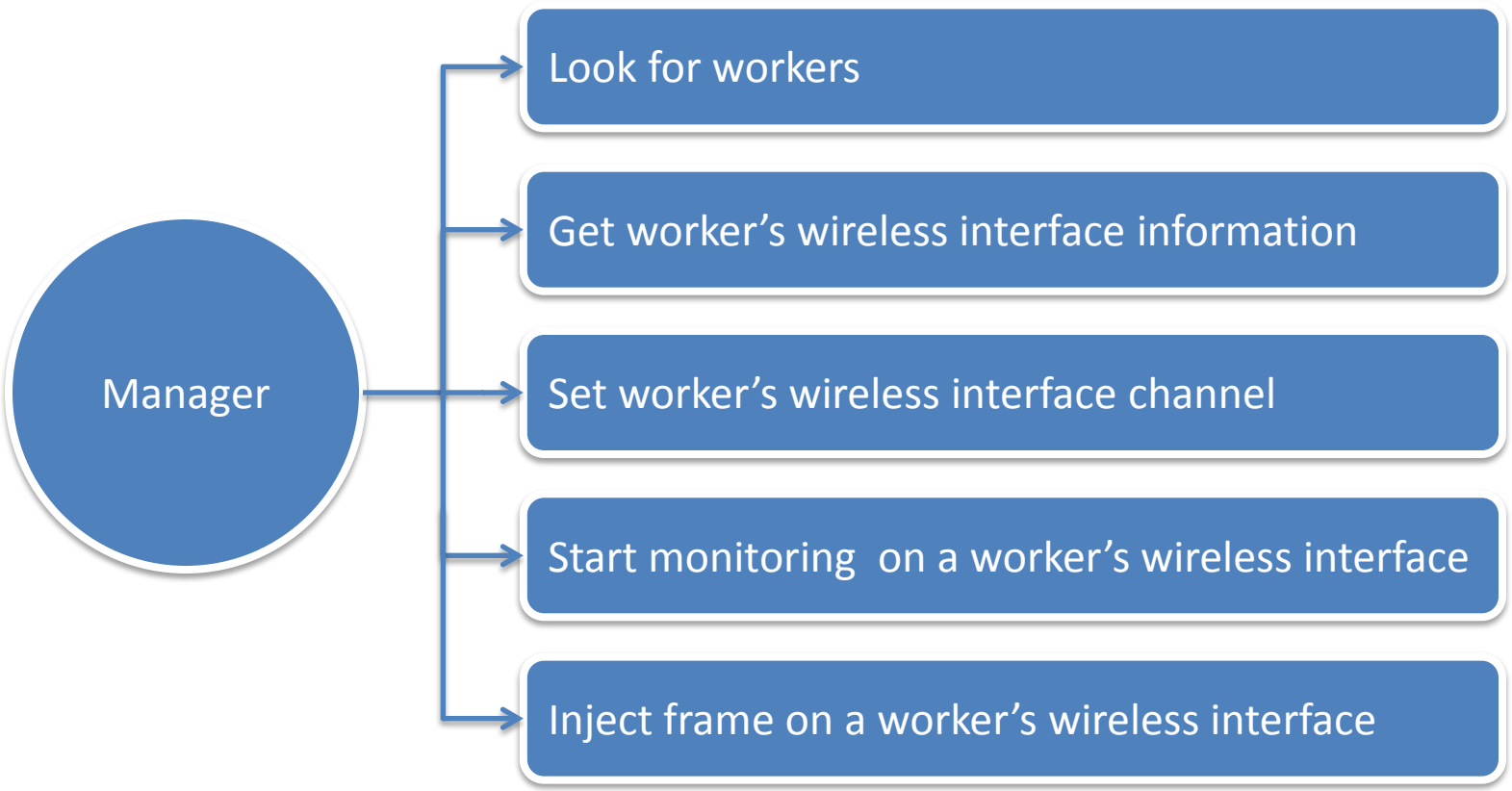
TP-Link TL-WDR3600



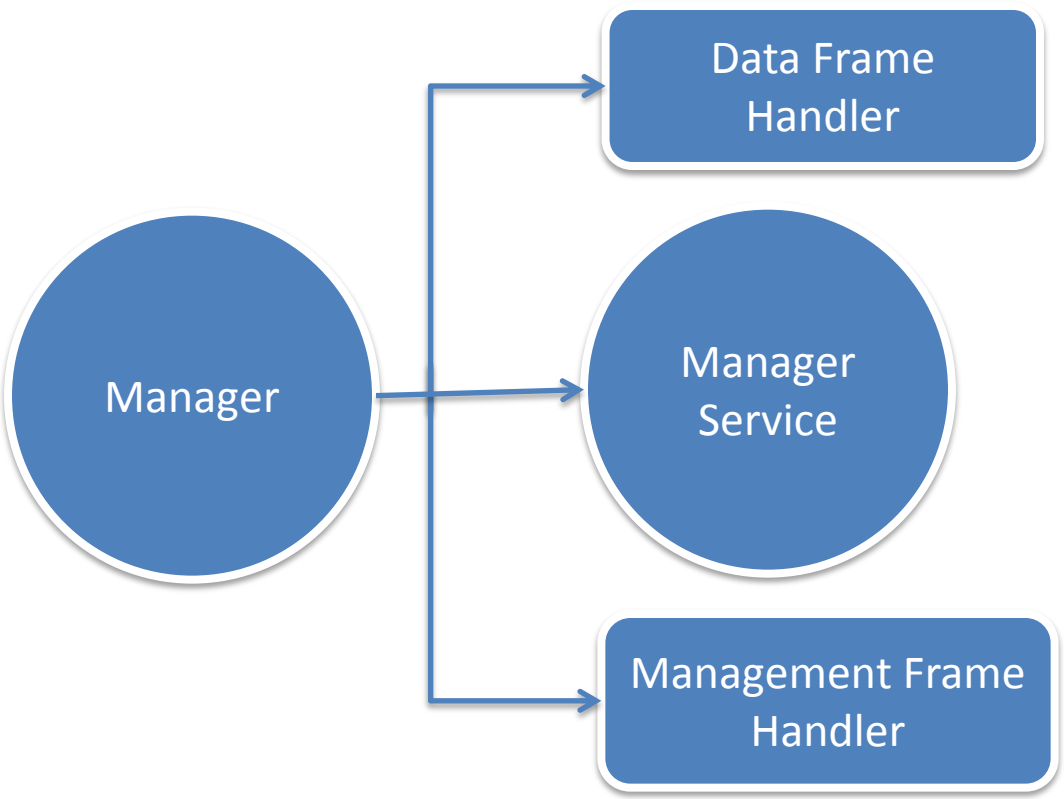
CPU	Atheros AR7240 @ 400MHz
RAM	32MiB
Flash	4MiB
Network	1 x 100MBit

TP-Link TL-MR3040

WiWo [features]



WiWo [manager architecture overview **]**



- Plug n’ Play
- Silence on the wire
- Avoid overhead to keep fragmentation low

WiWo [scalable **]**





WiWo [scalable **]**



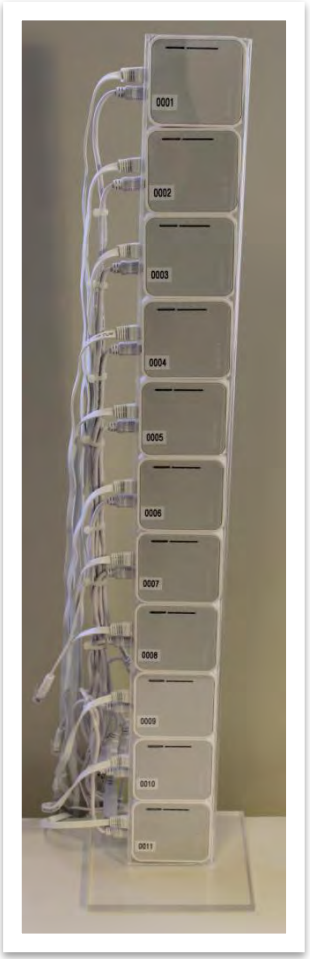




- IDS/IPS
- Traffic analysis
- Device Tracking
- Protocol analysis

WiWo [hardware PoC **]**







Wireless Network Traffic could be displayed during the demo.
Please disable Wi-Fi if you don’t want to be part of it.

Future Work

- IP support
- Build more OpenWRT firmware’s
- Code more examples
- Interaction with other tools

Questions?



https://github.com/CoreSecurity/wiwo



ablanco@coresecurity.com



agazzoli@coresecurity.com



https://twitter.com/6e726d



https://twitter.com/rcpota