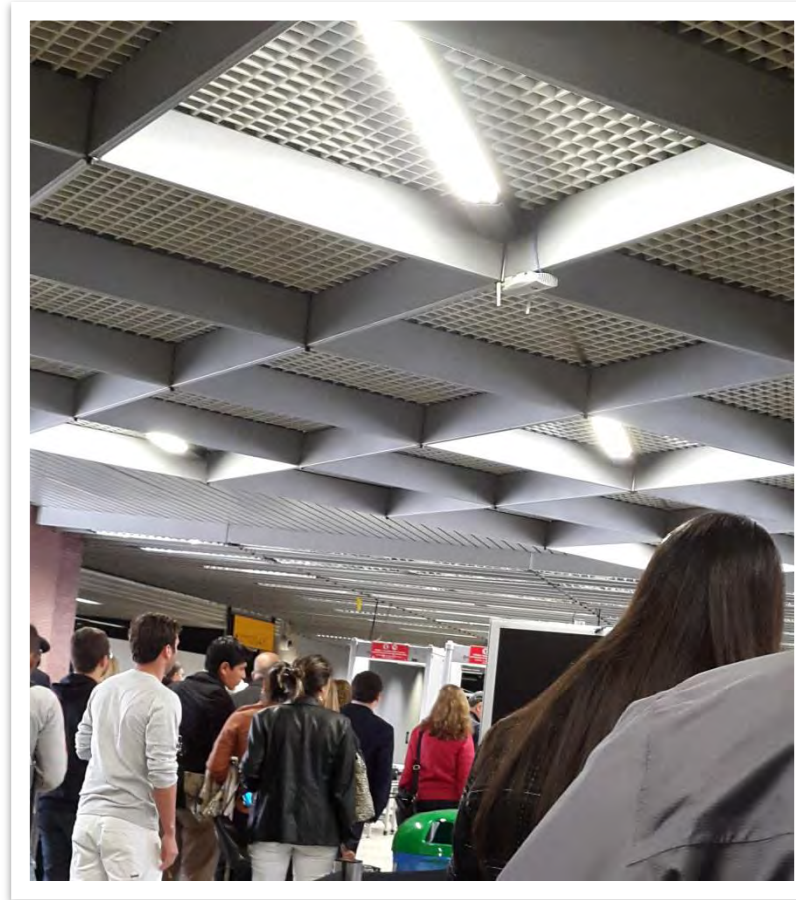


802.11 Massive Monitoring

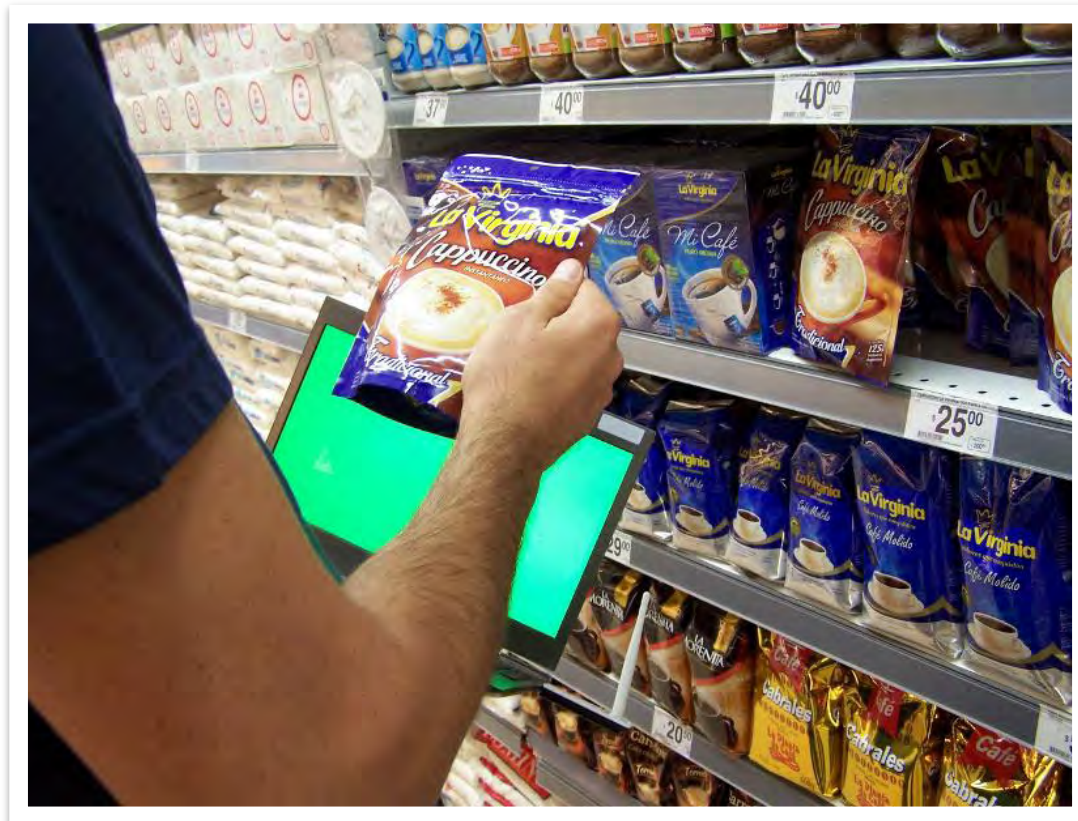
Andrés Blanco - Andrés Gazzoli

- 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?]

```

null@desktop: ~
-3:00:00.000000 8923884210us tsft 24.0 Mb/s 2417 MHz 11g -69dB signal [bit 29] IP
.49146 > .http: Flags [P.], seq 1:150, ack 1, win 229, options [nop,no
p,TS val 15974903 ecr 1269210391], length 149
0x0000: 0000 2400 2f40 00a0 2008 0000 0000 0000 ..$./@.....
0x0010: b2aa e713 0200 0000 1030 7109 c000 bb00 .....0q....
0x0020: 0000 bb00 0801 2c00 0018 f86c 7642 400e .....lvB@.
0x0030: 8576 029f 0015 c561 02e9 d0d5 aaaa 0300 .v.....a.....
0x0040: 0000 0800 4500 00c9 d4b6 4000 4006 cdb0 ....E.....@.
0x0050: bffa 0050 1a77 1542 .....P.w.B
0x0060: 6751 dcaa 8018 00e5 081e 0000 0101 080a gQ.....
0x0070: 00f3 c1f7 4ba6 9d17 4745 5420 2f67 656e ....K...GET./gen
0x0080: 6572 6174 655f 3230 3420 4854 5450 2f31 erate_204.HTTP/1
0x0090: 2e31 0d0a 5573 6572 2d41 6765 6e74 3a20 .1..User-Agent:.
0x00a0: 4461 6c76 696b 2f31 2e36 2e30 2028 4c69 Dalvik/1.6.0.(Li
0x00b0: 6e75 783b 2055 3b20 416e 6472 6f69 6420 nux;.U;.Android.
0x00c0: 342e 333b 2053 4348 2d49 3534 3520 4275 4.3;.SCH-I545.Bu
0x00d0: 696c 642f 4a53 5331 354a 290d 0a48 6f73 ild/JSS15J)..Hos
0x00e0: 743a 2063 6c69 656e 7473 332e 676f 6f67 t:.clients3.goog
0x00f0: 6c65 2e63 6f6d 0d0a 436f 6e6e 6563 7469 le.com..Connecti
0x0100: 6f6e 3a20 636c 6f73 650d 0a0d 0a3c 7536 on:.close....<u6
0x0110: 4d M
-3:00:00.000000 8923900500us tsft 36.0 Mb/s 2417 MHz 11g -69dB signal [bit 29] IP
.http > .49146: Flags [.], ack 150, win 341, options [nop,nop,TS val 1
269210410 ecr 15974903], length 0
0x0000: 0000 2400 2f40 00a0 2008 0000 0000 0000 ..$./@.....
0x0010: 54ea e713 0200 0000 1048 7109 c000 bb00 T.....Hq....
0x0020: 0000 bb00 0802 2c00 400e 8576 029f 0018 .....@.v....
0x0030: f86c 7642 0015 c561 02e9 d0f5 aaaa 0300 .lvB...a.....
0x0040: 0000 0800 4500 0034 4063 0000 3606 ac99 ....E..4@c..6...
0x0050: 0050 bffa 6751 dcaa .....P.gQ..
0x0060: 1a77 15d7 8010 0155 fd4f 0000 0101 080a .w....U.O.....
0x0070: 4ba6 9d2a 00f3 c1f7 71ac 3ba8 K.*....q;.
-3:00:00.000000 8923900731us tsft 36.0 Mb/s 2417 MHz 11g -69dB signal [bit 29] IP
.http > .49146: Flags [P.], seq 1:120, ack 150, win 341, options [nop,
```


Introduction [Who is this talk for?]

The image shows a Wireshark network traffic capture window. The title bar indicates the file is '14cc20bb180e.pcap' and the version is 'Wireshark 1.10.6 (v1.10.6 from master-1.10)'. The main pane displays a list of network packets. Packet 21380 is highlighted in orange, showing an IMAP response: '498 Response: * LIST (\HasNoCh ildren)'. The packet details pane below shows the structure of the captured frame: Radiotap Header, IEEE 802.11 Data, Logical-Link Control, Internet Protocol Version 4, Transmission Control Protocol (Src Port: imap (143), Dst Port: 56440), and Internet Message Access Protocol. The raw data pane shows the hexadecimal and ASCII representation of the packet bytes.

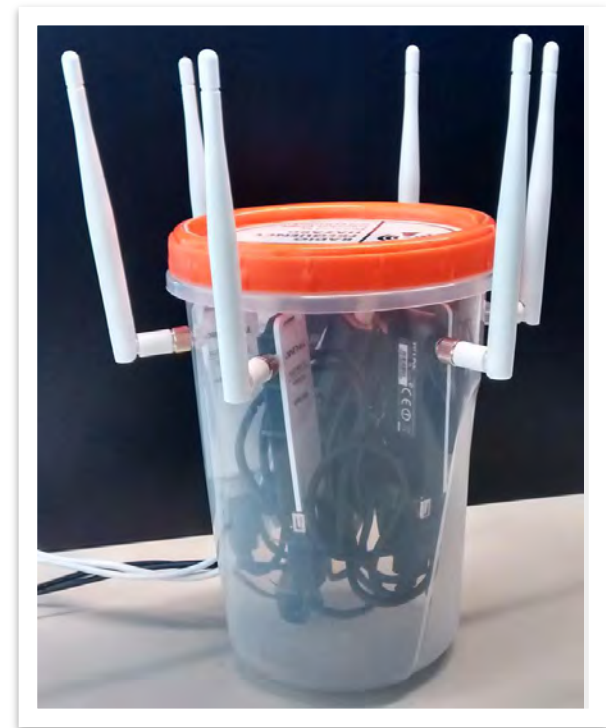
No.	Time	Source	Destination	Protocol	Length	Info
21378	0.000000			IMAP	148	Response: 188 OK NOOP co
21379	0.000000			IMAP	491	Response: * CAPABILITY I
21380	0.000000			IMAP	498	Response: * LIST (\HasNo
21381	0.000000			IMAP	148	Response: 191 OK NOOP co
21382	0.000000			IMAP	461	Response: * FLAGS (\Answ
21383	0.000000			IMAP	461	[TCP Retransmission] Res
21384	0.000000			IMAP	461	[TCP Retransmission] Res
21385	0.000000			IMAP	461	[TCP Retransmission] Res

▶ Frame 21380: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits)
▶ Radiotap Header v0, Length 36
▶ IEEE 802.11 Data, Flags:F.C
▶ Logical-Link Control
▶ Internet Protocol Version 4, Src: ..., Dst: ...
▶ Transmission Control Protocol, Src Port: imap (143), Dst Port: 56440 (56440), Seq: 1174, Ack: 357, Len: 366
▶ Internet Message Access Protocol

```
0000 00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00  ..$./@.. .....
```

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

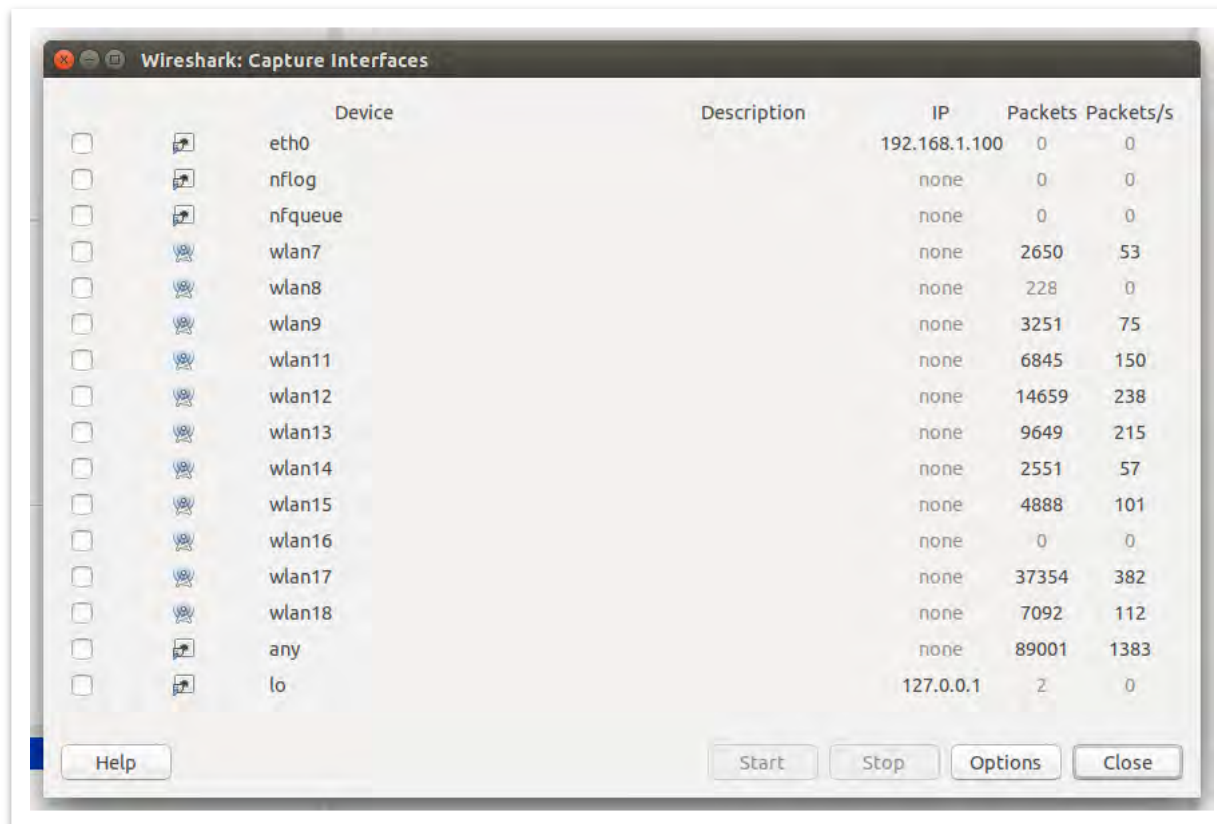
Approaches [first approach]



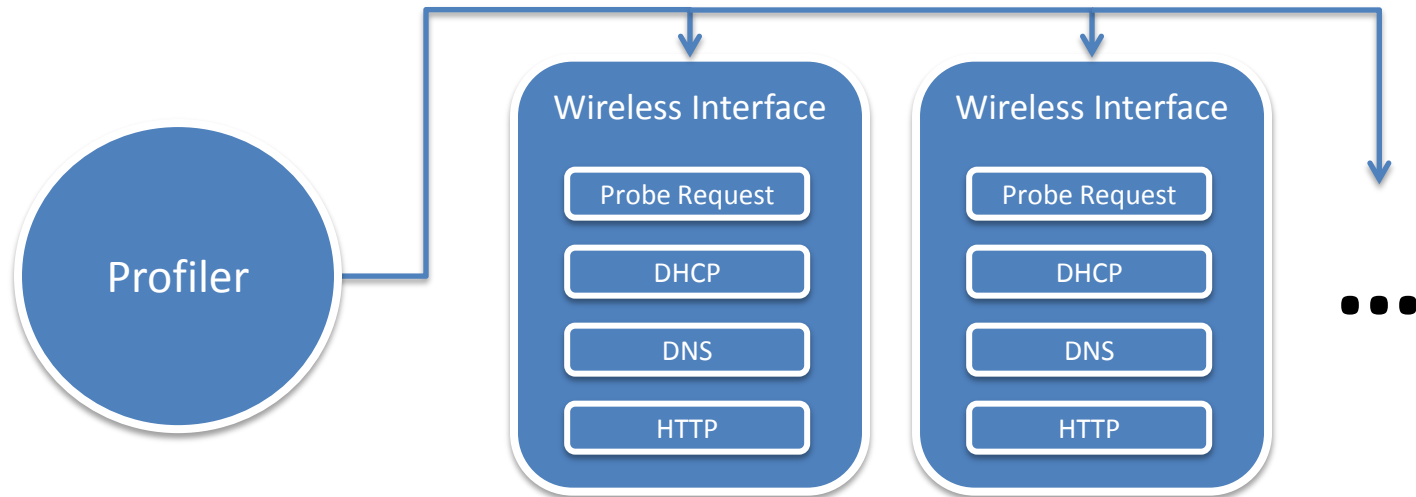
Approaches [second approach]



Approaches [wireshark]



Approaches [station profiler]





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

The USB Dilemma [scalability]



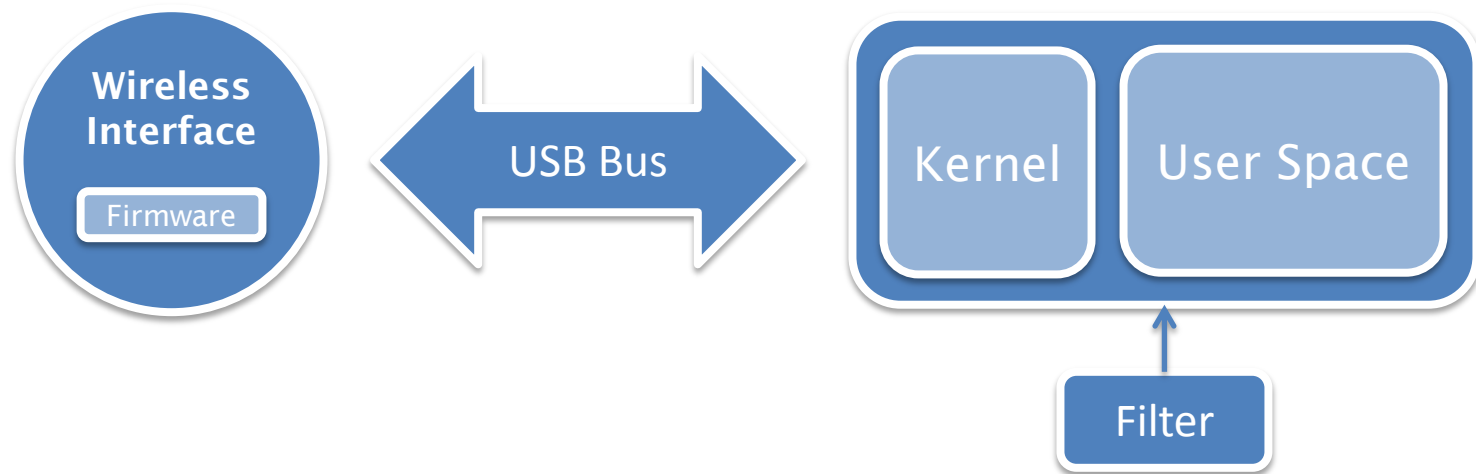
The USB Dilemma [scalability]



The USB Dilemma [bus saturation]

```
null@desktop: ~  
null@desktop:~$ lsusb  
Bus 002 Device 013: ID 0cf3:9271 Atheros Communications, Inc. AR9271 802.11n  
Bus 002 Device 012: ID 0cf3:9271 Atheros Communications, Inc. AR9271 802.11n  
Bus 002 Device 011: ID 0cf3:9271 Atheros Communications, Inc. AR9271 802.11n  
Bus 002 Device 010: ID 0cf3:9271 Atheros Communications, Inc. AR9271 802.11n  
Bus 002 Device 009: ID 05e3:0608 Genesys Logic, Inc. USB-2.0 4-Port HUB  
Bus 002 Device 008: ID 0cf3:9271 Atheros Communications, Inc. AR9271 802.11n  
Bus 002 Device 007: ID 0cf3:9271 Atheros Communications, Inc. AR9271 802.11n  
Bus 002 Device 006: ID 0cf3:9271 Atheros Communications, Inc. AR9271 802.11n  
Bus 002 Device 005: ID 05e3:0608 Genesys Logic, Inc. USB-2.0 4-Port HUB  
Bus 002 Device 004: ID 413c:2003 Dell Computer Corp. Keyboard  
Bus 002 Device 003: ID 0461:4d81 Primax Electronics, Ltd Dell N889 Optical Mouse  
Bus 002 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub  
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub  
Bus 001 Device 008: ID 0cf3:9271 Atheros Communications, Inc. AR9271 802.11n  
Bus 001 Device 007: ID 0cf3:9271 Atheros Communications, Inc. AR9271 802.11n  
Bus 001 Device 006: ID 0cf3:9271 Atheros Communications, Inc. AR9271 802.11n  
Bus 001 Device 005: ID 0cf3:9271 Atheros Communications, Inc. AR9271 802.11n  
Bus 001 Device 004: ID 05e3:0608 Genesys Logic, Inc. USB-2.0 4-Port HUB  
Bus 001 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub  
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub  
null@desktop:~$ lsusb | grep Atheros | wc -l  
11  
null@desktop:~$
```

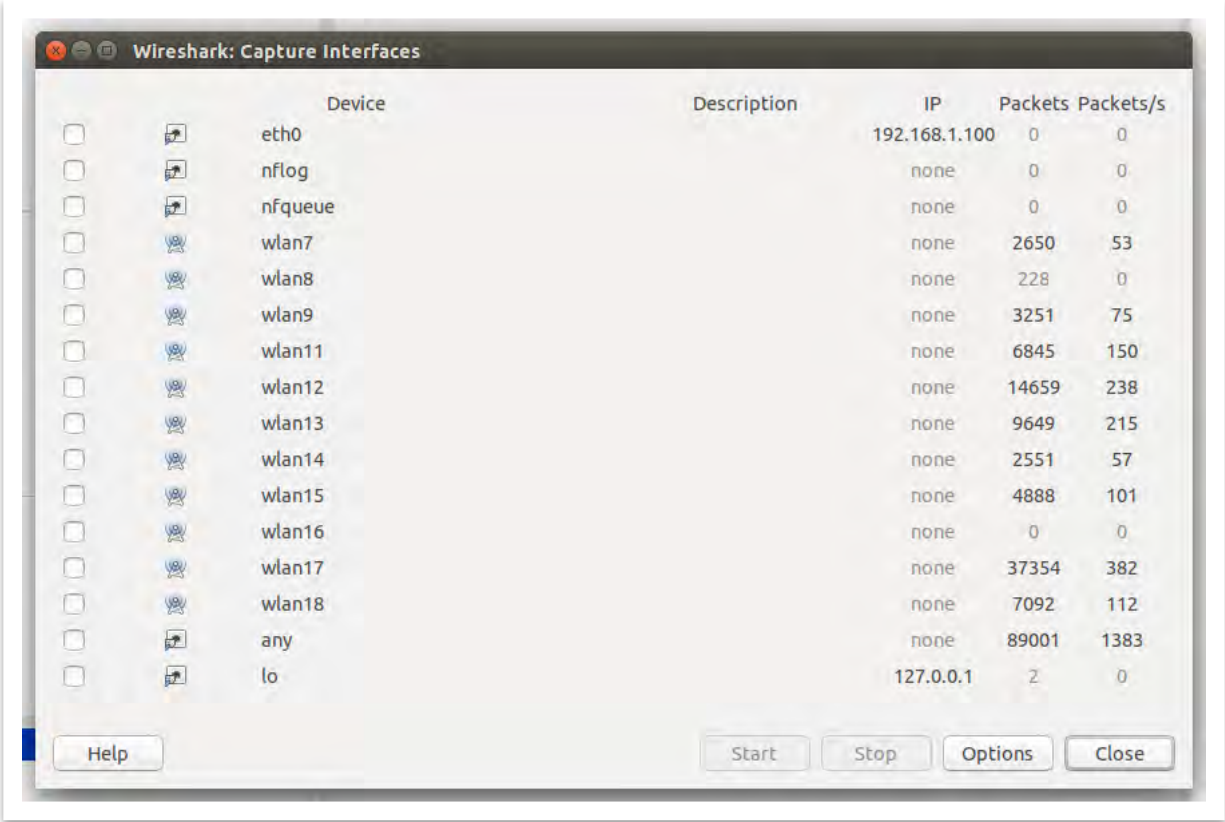
The USB Dilemma [bus saturation]



The USB Dilemma [bus saturation]



The USB Dilemma [bus saturation]



The image shows the 'Wireshark: Capture Interfaces' window. It contains a table of network interfaces. Each row has a checkbox for capture status, an icon, the device name, a description, an IP address, and two columns for traffic statistics: 'Packets' and 'Packets/s'. At the bottom, there are buttons for 'Help', 'Start', 'Stop', 'Options', and 'Close'.

	Device	Description	IP	Packets	Packets/s
<input type="checkbox"/>	eth0		192.168.1.100	0	0
<input type="checkbox"/>	nflog		none	0	0
<input type="checkbox"/>	nfqueue		none	0	0
<input type="checkbox"/>	wlan7		none	2650	53
<input type="checkbox"/>	wlan8		none	228	0
<input type="checkbox"/>	wlan9		none	3251	75
<input type="checkbox"/>	wlan11		none	6845	150
<input type="checkbox"/>	wlan12		none	14659	238
<input type="checkbox"/>	wlan13		none	9649	215
<input type="checkbox"/>	wlan14		none	2551	57
<input type="checkbox"/>	wlan15		none	4888	101
<input type="checkbox"/>	wlan16		none	0	0
<input type="checkbox"/>	wlan17		none	37354	382
<input type="checkbox"/>	wlan18		none	7092	112
<input type="checkbox"/>	any		none	89001	1383
<input type="checkbox"/>	lo		127.0.0.1	2	0

The USB Dilemma [non-removable devices]

```
ubuntu@ubuntu: ~  
ubuntu@ubuntu:~$ lsusb  
Bus 002 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub  
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub  
Bus 001 Device 003: ID 04f2:b307 Chicony Electronics Co., Ltd Webcam  
Bus 001 Device 005: ID 0930:0219 Toshiba Corp. Bluetooth  
Bus 001 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub  
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub  
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub  
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub  
ubuntu@ubuntu:~$
```


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 Chiconi  
Bus 001 Device 005: ID 0930:0219 Toshiba  
Bus 001 Device 007: ID 0cf3:9271 Atheros  
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 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 004: ID 0cf3:9271 Atheros  
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 C  
Bus 002 Device 001: ID 1d6b:0002 Linux F  
Bus 001 Device 003: ID 04f2:b307 Chicony  
Bus 001 Device 005: ID 0930:0219 Toshiba  
Bus 001 Device 002: ID 8087:0024 Intel C  
Bus 001 Device 001: ID 1d6b:0002 Linux F  
Bus 004 Device 001: ID 1d6b:0003 Linux F  
Bus 003 Device 005: ID 0cf3:9271 Athero  
Bus 003 Device 001: ID 1d6b:0002 Linux F  
ubuntu@ubuntu:~$
```

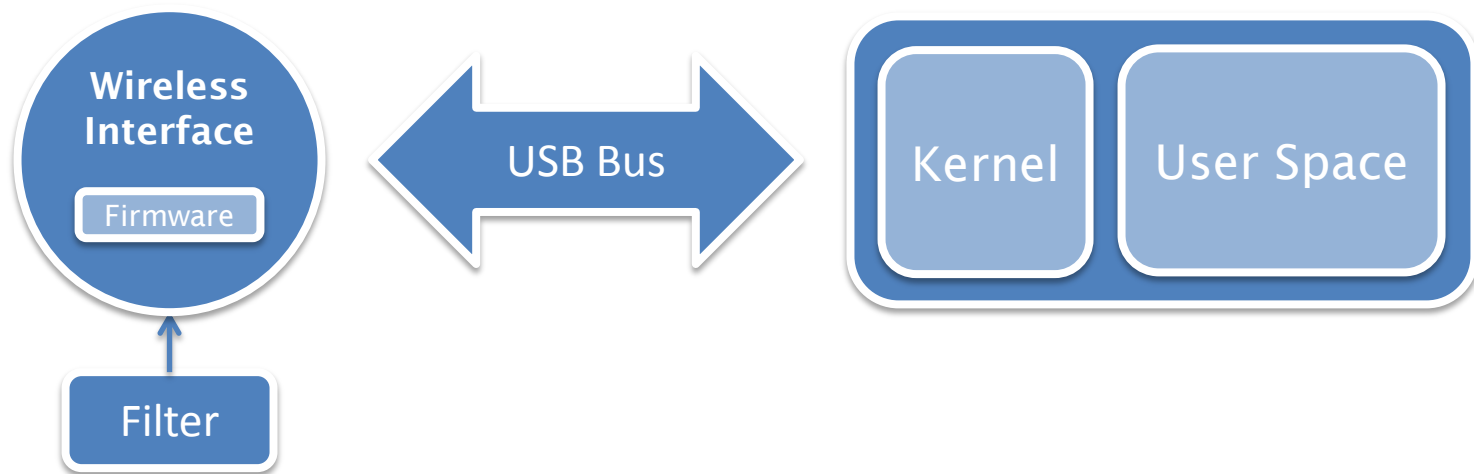
USB Port 3



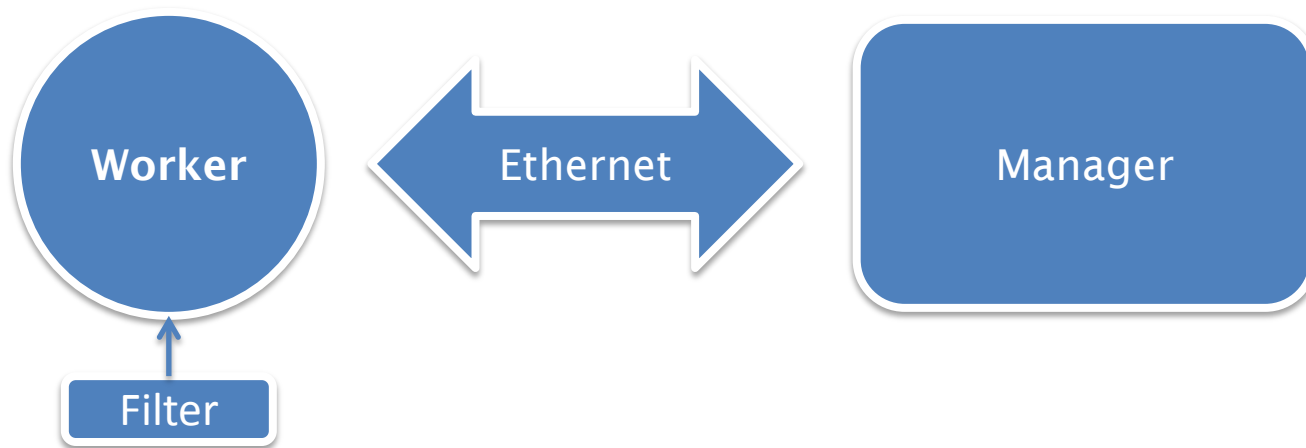
The USB Dilemma [power issues]

```
null@desktop: ~
kernel: [22424.810734] usb 2-1.2.1: device descriptor read/64, error -110
kernel: [22439.998745] usb 2-1.2.1: device descriptor read/64, error -110
kernel: [22450.590695] usb 2-1.2.1: device not accepting address 99, error -110
kernel: [22461.079014] usb 2-1.2.1: device not accepting address 100, error -110
kernel: [22461.583792] usb 2-1.2.4: device descriptor read/64, error -32
kernel: [22461.759882] usb 2-1.2.4: device descriptor read/64, error -32
kernel: [22462.007995] usb 2-1.2.4: device descriptor read/64, error -32
kernel: [22462.184158] usb 2-1.2.4: device descriptor read/64, error -32
kernel: [22462.768354] usb 2-1.2.4: device not accepting address 105, error -32
kernel: [22463.248725] usb 2-1.2.4: device not accepting address 106, error -32
kernel: [22637.222393] usb 2-1.1.1: device descriptor read/64, error -110
kernel: [22652.410460] usb 2-1.1.1: device descriptor read/64, error -110
kernel: [22667.670485] usb 2-1.1.1: device descriptor read/64, error -110
kernel: [22682.858507] usb 2-1.1.1: device descriptor read/64, error -110
kernel: [22693.450461] usb 2-1.1.1: device not accepting address 110, error -110
kernel: [22703.938775] usb 2-1.1.1: device not accepting address 111, error -110
kernel: [22704.443548] usb 2-1.1.4: device descriptor read/64, error -32
kernel: [22704.619687] usb 2-1.1.4: device descriptor read/64, error -32
kernel: [22704.867815] usb 2-1.1.4: device descriptor read/64, error -32
kernel: [22705.043971] usb 2-1.1.4: device descriptor read/64, error -32
kernel: [22705.628109] usb 2-1.1.4: device not accepting address 116, error -32
kernel: [22706.108489] usb 2-1.1.4: device not accepting address 117, error -32
kernel: [22868.204767] usb 2-1.2.1: device descriptor read/64, error -110
kernel: [22883.392808] usb 2-1.2.1: device descriptor read/64, error -110
```

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 is 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



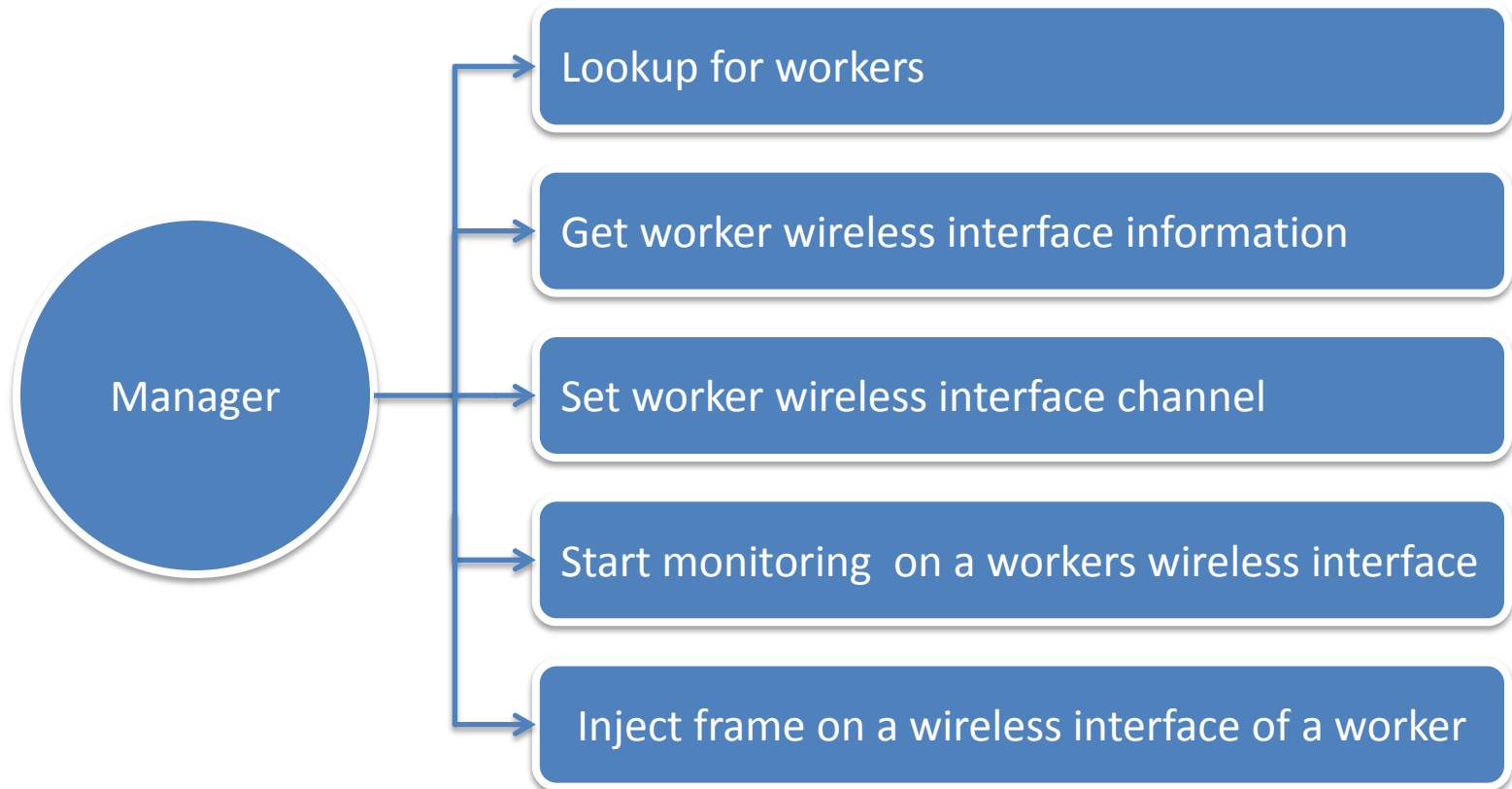
CPU	Atheros AR9344 @ 560 MHz
RAM	128MiB
Flash	8MiB
Network	4 x 1000MBit

TP-Link TL-WDR3600

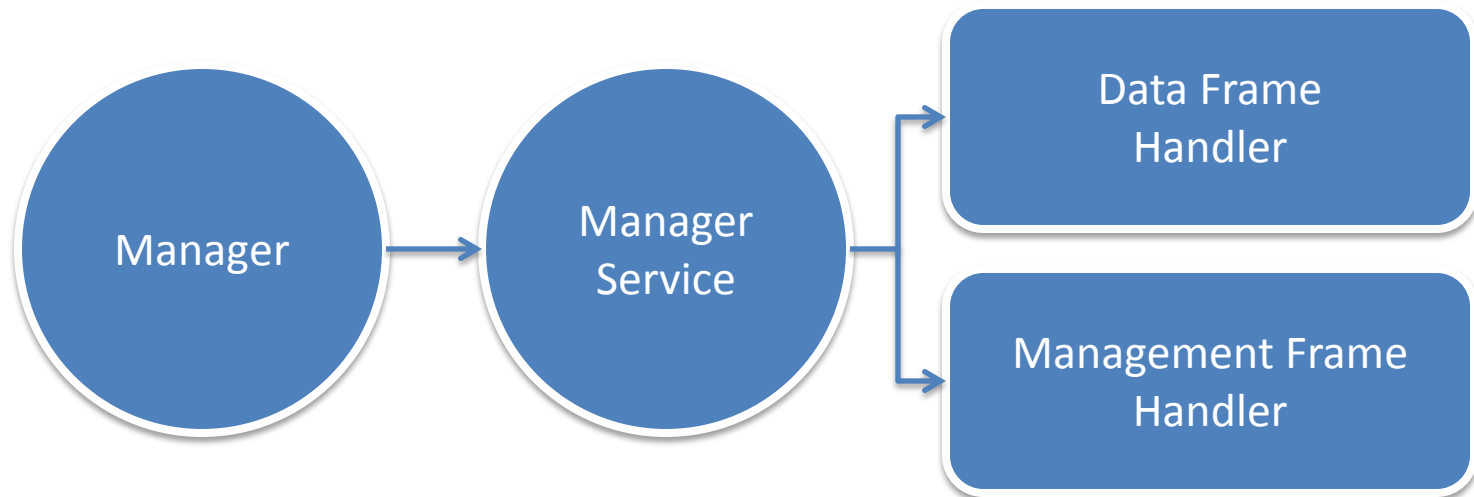


CPU	Atheros AR7240 @ 400MHz
RAM	32MiB
Flash	4MiB
Network	1 x 100MBit

TP-Link TL-MR3040



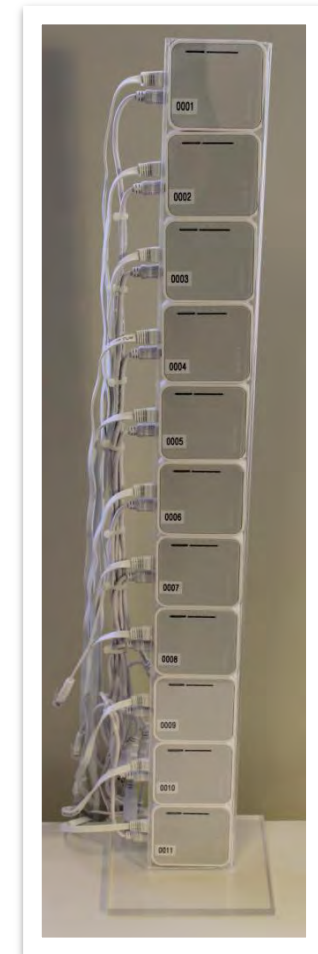
WiWo [manager architecture overview]



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

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

WiWo [hardware PoC]





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

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



<https://github.com/CoreSecurity/wiwo>



ablanco@coresecurity.com



agazzoli@coresecurity.com



<https://twitter.com/6e726d>



<https://twitter.com/rcpota>