WiCy: Monitoring 802.11AC Networks at Scale

Nishant Sharma
(Proxying for Vivek Ramachandran)
PentesterAcademy.com & AttackDefense.com
Me, **Nishant Sharma**

- R&D Manager and Lead Trainer, Pentester Academy
- Firmware developer, Enterprise WiFi APs and WIPS Sensors
- Masters degree in Infosec
- Published research at Blackhat US/Asia, DEF CON USA and other venues
  - WiDy, IIIDS, Wimonitor, Deceptacon
  - PA-Toolkit
  - BLEMystique
  - VoIPShark

- Proxying for **Vivek Ramachandran**, CEO, Pentester Academy
Talk Outline

• 802.11n/ac basics

• Challenges in the field

• Custom AP based Sniffer

• Conclusion
802.11 a/b/g Monitoring
Monitoring 802.11a/b/g Networks

Single-Input Single-Output

- Wi-Fi card which supports Monitor Mode
- Set same channel as Target
- Antennas generally Omnidirectional

802.11 n/ac  Wave 1 and 2
Channel Bonding

Standard 802.11 channels are effectively 20MHz wide.

Channel bonding combines two adjacent 20MHz channels into a single 40MHz channel providing increased throughput.

Need Compatible Hardware

https://wifiliedi.files.wordpress.com/2009/01/channel-bonding1.jpg
802.11 n/ac MIMO: Multiple-Input Multiple-Output
Spatial Streams

- Pure Diversity – all antennas transmit the same signal
- Spatial Multiplexing (Streams) requires every antenna send a separate signal
- This provides higher throughput at the cost of reliability
- Both transmitted and receiver need to support #streams
- 802.11n: 4 stream maximum
- 802.11ac Wave 2: 8 stream maximum
- 3 x 3 : 2 (Transmitter x Receiver : Streams)

Need Compatible Hardware
SU-MIMO and MU-MIMO

(a) Single-user MIMO
- 802.11n
- 802.11ac Wave 1
- Communicates with a single device at one time
- Hub like behavior

(b) Multi-user MIMO
- 802.11ac Wave 2
- Communicates with multiple devices at the same time
- Switch like behavior

Need Compatible Hardware
Beamforming

Image Source: http://chimera.labs.oreilly.com/books/1234500001778/ch01.htm#sc_product_development_plans
## 802.11n & 802.11ac

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefits</th>
<th>11n</th>
<th>11ac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Width</td>
<td>Quadruple Throughput</td>
<td>20, 40 MHz</td>
<td>20, 40, 80, 80+80, 160 MHz</td>
</tr>
<tr>
<td>QAM Encoding</td>
<td>More Bits/MHz</td>
<td>16, 64 QAM</td>
<td>16, 64, 256 QAM</td>
</tr>
<tr>
<td>Spatial Streams</td>
<td>Double Throughput</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Beamforming</td>
<td>Higher Data Rates &amp; Range</td>
<td>Implicit, Explicit</td>
<td>(Standardized) Explicit</td>
</tr>
<tr>
<td>MIMO</td>
<td>Switch-like Wi-Fi</td>
<td>SU-MIMO</td>
<td>SU-MIMO, MU-MIMO</td>
</tr>
<tr>
<td>Frame Aggregation</td>
<td>Greater Efficiency</td>
<td>A-MSDU size 7,935 Bytes</td>
<td>A-MSDU size 11,426 Bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A-MPDU size 65,535 Bytes</td>
<td>A-MPDU size 1,048,576 Bytes</td>
</tr>
<tr>
<td>Bands Supported</td>
<td>More Channel &amp; Less Cluttered Spectrum</td>
<td>2.4, 5 GHz</td>
<td>5 GHz Only</td>
</tr>
</tbody>
</table>

Source: Airtight Networks
### 802.11n/ac Monitoring Challenges

<table>
<thead>
<tr>
<th>Technology Component</th>
<th>Challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beamforming</td>
<td>Location Matters</td>
</tr>
<tr>
<td>Spatial Stream Count</td>
<td>Capture device supports same number</td>
</tr>
<tr>
<td>High Speed</td>
<td>Need High Throughput Backhaul - USB? Gigabit Ethernet?</td>
</tr>
<tr>
<td>Multi-Channel &amp; Channel Bonding</td>
<td>Multiple capture devices needed</td>
</tr>
</tbody>
</table>
Monitoring 802.11n/ac Networks

• **USB based Adapter**
  – Supports Band
  – Supports maximum streams
  – Speed limitations will remain

• **Access Point Solution**
  – Set to Monitor mode
  – Supports maximum streams
  – Remote capture
AP Based Monitoring: 802.11 a/b/g/n/ac
# Ubiquiti – Unifi AP Series

## Models

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment</td>
<td>Indoor</td>
<td>Indoor</td>
<td>Indoor/Outdoor</td>
<td>Indoor/Outdoor</td>
<td>Indoor</td>
<td>Outdoor</td>
<td>Business</td>
</tr>
<tr>
<td>WiFi Standard</td>
<td>802.11n/ac</td>
<td>802.11n/ac</td>
<td>802.11n/ac</td>
<td>802.11n/ac</td>
<td>802.11n/ac</td>
<td>802.11n/ac</td>
<td>802.11n/ac</td>
</tr>
<tr>
<td>Radios/Antennas</td>
<td>2x2</td>
<td>3x3</td>
<td>3x3</td>
<td>4x4</td>
<td>3x3</td>
<td>2x2</td>
<td>3x3</td>
</tr>
<tr>
<td>2.4GHz</td>
<td>300Mbps</td>
<td>450Mbps</td>
<td>450Mbps</td>
<td>800Mbps</td>
<td>450Mbps</td>
<td>300Mbps</td>
<td>450Mbps</td>
</tr>
<tr>
<td>5GHz</td>
<td>900Mbps</td>
<td>900Mbps</td>
<td>1300Mbps</td>
<td>1733Mbps</td>
<td>1300Mbps</td>
<td>900Mbps</td>
<td>1200Mbps</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>No. Ports</td>
<td>One (1)</td>
<td>One (1)</td>
<td>Two (2)</td>
<td>Two (2)</td>
<td>Two (2)</td>
<td>One (1)</td>
<td>Two (2)</td>
</tr>
<tr>
<td>PoE</td>
<td>-</td>
<td>-</td>
<td>802.3af/802.3at</td>
<td>802.3at</td>
<td>803.2at</td>
<td>802.3af</td>
<td>802.3at</td>
</tr>
<tr>
<td>Wave2 MU-MIMO</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

©PentesterAcademy.com
Ubiquiti UniFi Enterprise WiFi System
AP-Pro (UAP-PRO)
by Ubiquiti Networks

List Price: $229.00
Price: $199.99
You Save: $29.01 (13%)

Free Amazon tech support included
• Ubiquiti UniFi UAP Wireless Access Point/Bridge 11b/g/n enterprise Wi-Fi System
• 23dBm, Wall/Ceiling (Kits included), 48V 5A PoE Adapter included
• It is highly durable and efficient

Used & new (15) from $135.00
UAP-AC-PRO

• OpenWRT based system
• Uses Madwifi-NG drivers for Wi-Fi
• SSH enabled
Wireless Interfaces

```
# Output from ifconfig command

lo    Link encap:Loopback                           inet addr:127.0.0.1  Mask:255.0.0.0  inet6 addr::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436 Metric:1
        RX packets:573 errors:0 dropped:0  overruns:0  frame:0
        TX packets:573 errors:0 dropped:0  overruns:0  carrier:0
        collisions:0 txqueuelen:0
        RX bytes:45242 (44.1 KiB) TX bytes:45242 (44.1 KiB)

wlan0  Link encap:Ethernet  HWaddr F0:0F:C2:33:B1:EA
        inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
        inet6 addr: fe80::200:12ff:fe33:b1ea/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:80 errors:0  dropped:0  overruns:0  frame:0
        TX packets:80 errors:0  dropped:0  overruns:0  carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:12288 (12.0 KiB) TX bytes:12288 (12.0 KiB)
```

© PentesterAcademy.com
Wlanconfig Tool

BZ.v3.7.49# wlanconfig
usage: wlanconfig athX create wlandev wifiX
    wlanmode [sta|adhoc|ap|monitor|wrap|p2pgo|p2pcli|p2pdev]
    [wlanaddr <mac_addr>] [mataddr <mac_addr>] [bssid|-bssid] [nosbeacon]
usage: wlanconfig athX destroy
usage: wlanconfig athX nawds mode (0-4)
usage: wlanconfig athX nawds defcaps CAPS
usage: wlanconfig athX nawds override (0-1)
usage: wlanconfig athX nawds add-repeater MAC (0-1)
usage: wlanconfig athX nawds del-repeater MAC
usage: wlanconfig athX nawds list
usage: wlanconfig athX addssid ssidname per_value(0--100)
usage: wlanconfig athX addsta macaddr(example:112233445566) per_value(0--100)
usage: wlanconfig athX delssid ssidname
usage: wlanconfig athX delsta macaddr
usage: wlanconfig athX showatftable
usage: wlanconfig athX showairtime
usage: wlanconfig athX flushatftable
usage: wlanconfig athX showstastats all
usage: wlanconfig athX showstastats macaddr
usage: wlanconfig athX resetstastats all
usage: wlanconfig athX resetstastats macaddr
usage: wlanconfig athX nf bypass
BZ.v3.7.49#
Create 2.4 Ghz Monitor Mode Interface

BZ.v3.7.49# wlanconfig ath1 create wlan dev wifi0 wlanmode monitor ath1
BZ.v3.7.49# BZ.v3.7.49# BZ.v3.7.49# ifconfig ath1 up
BZ.v3.7.49# iwconfig ath1
ath1 IEEE 802.11b ESSID:"
Mode:Monitor Frequency:2.412 GHz Access Point: Not-Associated
Bit Rate:11 Mb/s Tx-Power:22 dBm
RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=255/94 Signal level=-1 dBm Noise level=109 dBm
Rx invalid mwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0

BZ.v3.7.49# iwconfig ath1 channel 11
BZ.v3.7.49# iwconfig ath1
ath1 IEEE 802.11bg ESSID:"
Mode:Monitor Frequency:2.462 GHz Access Point: Not-Associated
Bit Rate:11 Mb/s Tx-Power:22 dBm
RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=255/94 Signal level=-1 dBm Noise level=96 dBm
Rx invalid mwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0

BZ.v3.7.49#
Create 5Ghz Monitor Mode Interface

```bash
BZ.v3.7.49# wlanconfig ath2 create wlandev wifi1 wlanmode monitor
ath2
BZ.v3.7.49# ifconfig ath2 up
BZ.v3.7.49# iwconfig ath2
ath2     IEEE 802.11a ESSID:"
          Mode:Monitor Frequency:5.18 GHz Access Point: Not-Associated
          Bit Rate:0 kb/s  Tx-Power:22 dBm
          RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94  Signal level=-96 dBm  Noise level=-102 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

BZ.v3.7.49# iwconfig ath2 channel 149
BZ.v3.7.49# iwconfig ath2
ath2     IEEE 802.11ac ESSID:"
          Mode:Monitor Frequency:5.745 GHz Access Point: Not-Associated
          Bit Rate:0 kb/s  Tx-Power:22 dBm
          RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94  Signal level=-96 dBm  Noise level=-104 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

BZ.v3.7.49#
Redirect Packets to Local Wireshark Instance

```
root@kali:~ # ssh admin@192.168.1.20 tcpdump -i ath1 -U -s0 -w - | wireshark -k -i -admin@192.168.1.20's password:
tcpdump: WARNING: ath1: no IPv4 address assigned
tcpdump: listening on ath1, link-type PRISM_HEADER (802.11 plus Prism header), capture size 65535 bytes
```

```
PentesterAcademy# ssh admin@192.168.1.20 tcpdump -i ath2 -U -s0 -w - | wireshark -k -i -admin@192.168.1.20's password:
tcpdump: WARNING: ath2: no IPv4 address assigned
tcpdump: listening on ath2, link-type PRISM_HEADER (802.11 plus Prism header), capture size 65535 bytes
```
Remote Monitoring with Wireshark
Better Alternative

- Cheaper
- Less modification
- Smaller
- External antenna
- Multi purpose
- USB Powered
GL.iNet GL-AR750S-Ext Gigabit Travel AC Router (Slate),
300Mbps(2.4G)+433Mbps(5G) Wi-Fi,
128MB RAM, MicroSD Support,
OpenWrt/LEDE pre-Installed, Cloudflare DNS,
Power Adapter and Cables Included

by GL.iNet

66 customer reviews
| 78 answered questions

Price: $69.99

DUAL BAND AC ROUTER: Simultaneous dual band with wireless speed 300Mbps(2.4G)+433Mbps(5G). Convert a public network(wired/wireless) to a private Wi-Fi for secure surfing.
OPEN SOURCE & PROGRAMMABLE: OpenWrt/LEDE pre-installed, backed by software repository.
VPN CLIENT & SERVER: OpenVPN and WireGuard® pre-installed, compatible with 25+ VPN service providers.
LARGER STORAGE & EXTENSIBILITY: 128MB RAM, 16MB NOR

$69.99
This item ships to India. Learn more
In Stock.

Add to Cart
Buy Now

Sold by GL Technologies and Fulfilled by Amazon.
Gift-wrap available.
Deliver to India
Add to List

©PentesterAcademy.com
Powered by USB, External Antenna
Smaller, Pocket Friendly Shape
Vendor Web UI

No Password by Default
Vendor Web UI

GL.iNet Admin Panel

Cable

- Protocol: DHCP
- IP Address: 192.168.8.174
- Netmask: 255.255.255.0
- Gateway: 192.168.8.1
Authorization Required
Please enter your username and password.

Username: root
Password: 

Login  Reset

Powered by LuCI openwrt-18.06 branch (git-18.196.56128-9112198) / OpenWrt 18.06.1 r7258-5eb055306f
## LuCi

<table>
<thead>
<tr>
<th>Status</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>GL-AR750S</td>
</tr>
<tr>
<td>Model</td>
<td>GL-AR750S</td>
</tr>
<tr>
<td>Architecture</td>
<td>Qualcomm Atheros QCA956X ver 1 rev 0</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>OpenWrt 18.06.1 r7258-5eb055306f / LuCI openwrt-18.06 branch (git-18.196.56128-9112198)</td>
</tr>
<tr>
<td>Kernel Version</td>
<td>4.0.109</td>
</tr>
<tr>
<td>Local Time</td>
<td>Thu May 9 04:10:56 2019</td>
</tr>
<tr>
<td>Uptime</td>
<td>9h 8m 36s</td>
</tr>
<tr>
<td>Load Average</td>
<td>0.49, 0.19, 0.20</td>
</tr>
</tbody>
</table>

## Memory

- **Total Available**: 72464 kB / 124608 kB (58%)
- **Free**: 65840 kB / 124608 kB (52%)
- **Buffered**: 6624 kB / 124608 kB (0%)
BusyBox v1.28.3 () built-in shell (ash)

OpenWrt 18.06.1, r7258-5eb055306f

root@GL-AR750S:~#
Updating Package List

root@GL-AR750S:~# opkg update
Downloading http://download.gl-inet.com/releases/kmod-3.0/ar71xx/nand/Packages.gz
Updated list of available packages in /var/opkg-lists/glinet_core
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/base/Packages.gz
Updated list of available packages in /var/opkg-lists/glinet_base
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/gli_pub/Packages.gz
Updated list of available packages in /var/opkg-lists/glinet_gli_pub
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/packages/Packages.gz
Updated list of available packages in /var/opkg-lists/glinet_packages
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/luci/Packages.gz
Updated list of available packages in /var/opkg-lists/glinet_luci
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/routing/Packages.gz
Updated list of available packages in /var/opkg-lists/glinet_routing
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/telephony/Packages.gz
Updated list of available packages in /var/opkg-lists/glinet_telephony
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/glinet/Packages.gz
Updated list of available packages in /var/opkg-lists/glinet_glinet
root@GL-AR750S:~#
Install Packages

root@GL-AR750S:~# opkg install horst
Installing horst (5.1-2) to root...
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/packages/horst_5.1-2_mips_24kc.ipk
Installing terminfo (6.1-1) to root...
Installing libncurses (6.1-1) to root...
Configuring terminfo.
Configuring libncurses.
Configuring horst.
root@GL-AR750S:~#

root@GL-AR750S:~# opkg install aircrack-ng
Installing aircrack-ng (1.2-rc1-2) to root...
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/packages/aircrack-ng_1.2-rc1-2_mips_24kc.ipk
Installing libnl-core (3.3.0-1) to root...
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/base/libnl-core_3.3.0-1_mips_24kc.ipk
Installing libnl-genl (3.3.0-1) to root...
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/base/libnl-genl_3.3.0-1_mips_24kc.ipk
Configuring libnl-core.
Configuring libnl-genl.
Configuring aircrack-ng.
root@GL-AR750S:~#
Modified /etc/config/wireless

root@GL-AR750S:~# cat /etc/config/wireless
fi-device 'radio0'
  option type 'mac80211'
  option channel '36'
  option hwmode '11a'
  option path 'pci0000:00/0000:00:00.0'
  option htmode 'VHT80'
  option disabled '0'
  option country '00'

config wifi-iface 'default_radio0'
  option device 'radio0'
  option network 'lan'
  option mode 'monitor'

config wifi-device 'radio1'
  option type 'mac80211'
  option channel '11'
  option hwmode '11g'
  option path 'platform/qca953x_wmac'
  option htmode 'HT20'
  option disabled '0'
  option country '00'

config wifi-iface 'default_radio1'
  option device 'radio1'
  option network 'lan'
  option mode 'monitor'

root@GL-AR750S:~#
WiFi Interfaces

```
root@GL-AR750S:~# iw dev
phy#1

    Interface wlan1
          ifindex 5
          wdev 0x100000001
          addr e4:95:6e:45:9c:96
          type monitor
          channel 8 (2447 MHz), width: 20 MHz, center1: 2447 MHz
txpower 23.00 dBm

phy#0

    Interface wlan0
          ifindex 4
          wdev 0x1
          addr e4:95:6e:45:9c:97
          type monitor
          channel 60 (5300 MHz), width: 20 MHz, center1: 5300 MHz
txpower 0.00 dBm
```
Demo
Conclusion

• 11ac monitoring is NOT that hard

• Affordable, Off-the-shelf APs are better alternative

• Massive support from OpenWRT community

• Horizontal scaling to cover more area/spectrum

• Poor man’s Distributed Sniffing/Intrusion Detection System
Q & A

Feel free to reach me at nishant@attackdefense.com
Thanks!!