WiCy: Monitoring 802.11AC Networks at Scale

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

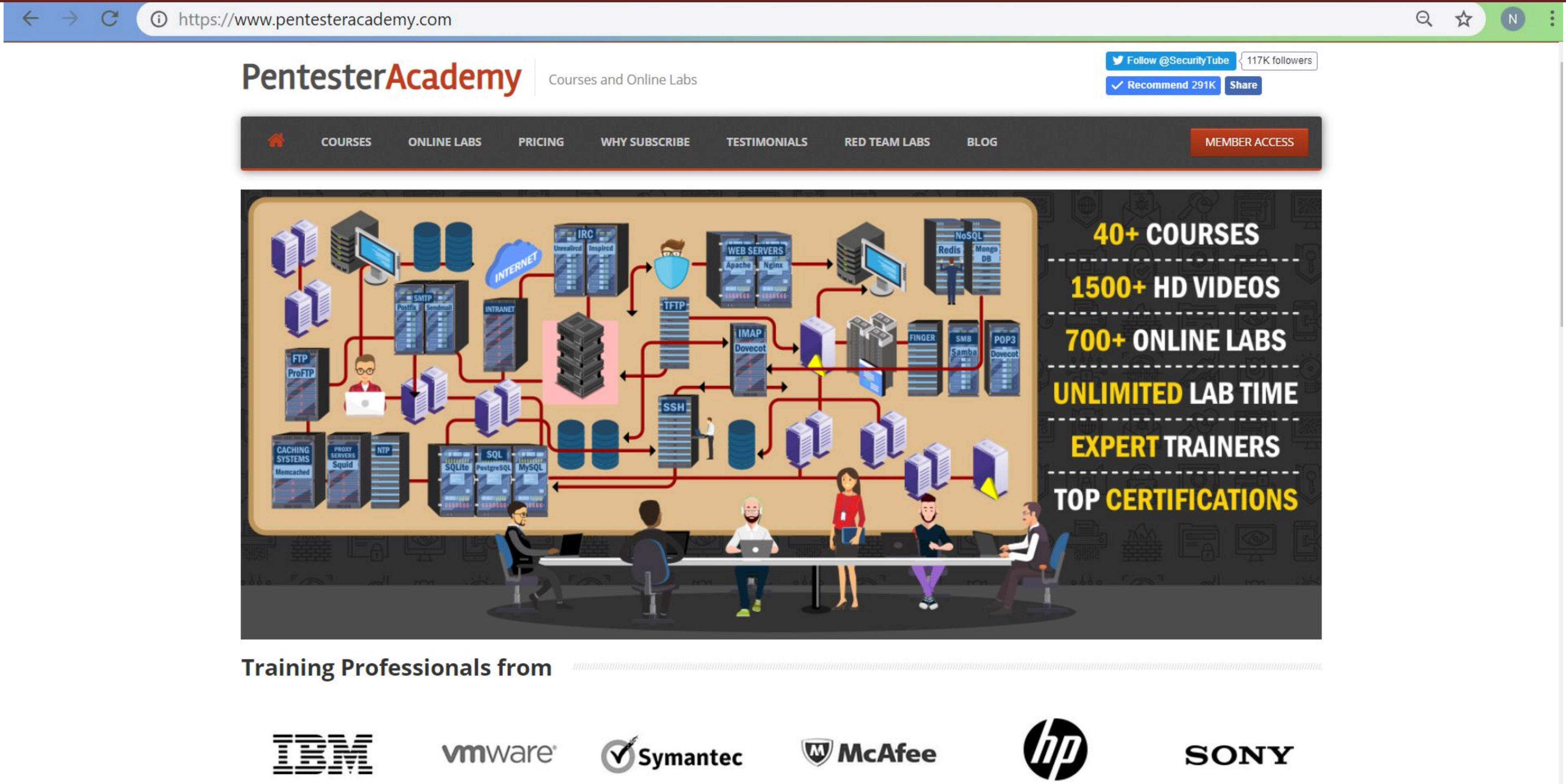
About Me

Me, **Nishant Sharma**

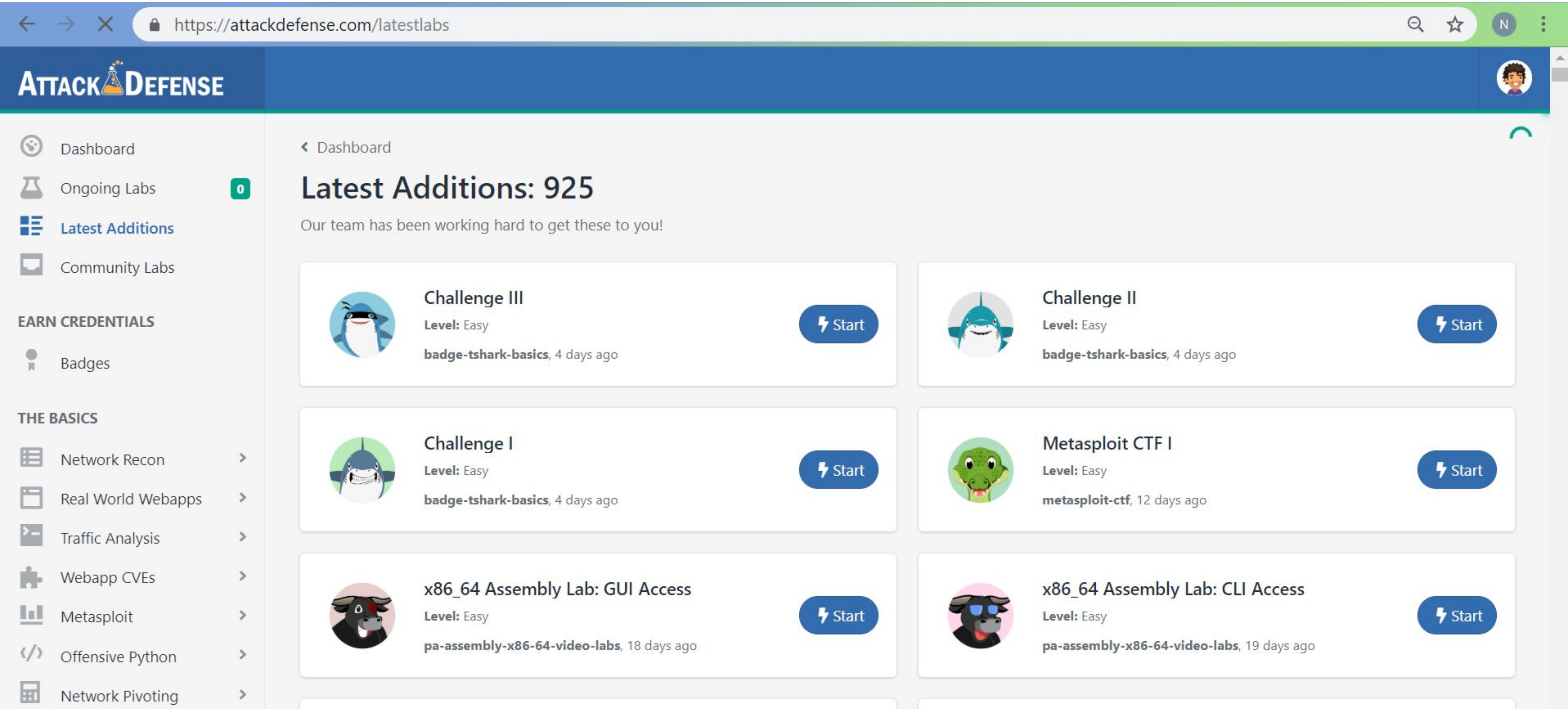
- R&D Manager and Lead Trainer, Pentester Academy
- Firmware developer, Enterprise WiFi APs and WIPS Sensors
- Masters degree in Infosec
- Published research at Blackhat US/Asia, DEF CON USA and other venues
  - WiDy, IIIDS, Wimonitor, Deceptacon
  - PA-Toolkit
  - BLEMystique
  - VoIPShark

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

PentesterAcademy.com



AttackDefense.com



‹ Dashboard

Latest Additions: 925

Our team has been working hard to get these to you!

Challenge III
Level: Easy
badge-tshark-basics, 4 days ago
Start

Challenge II
Level: Easy
badge-tshark-basics, 4 days ago
Start

Challenge I
Level: Easy
badge-tshark-basics, 4 days ago
Start

Metasploit CTF I
Level: Easy
metasploit-ctf, 12 days ago
Start

x86_64 Assembly Lab: GUI Access
Level: Easy
pa-assembly-x86-64-video-labs, 18 days ago
Start

x86_64 Assembly Lab: CLI Access
Level: Easy
pa-assembly-x86-64-video-labs, 19 days ago
Start

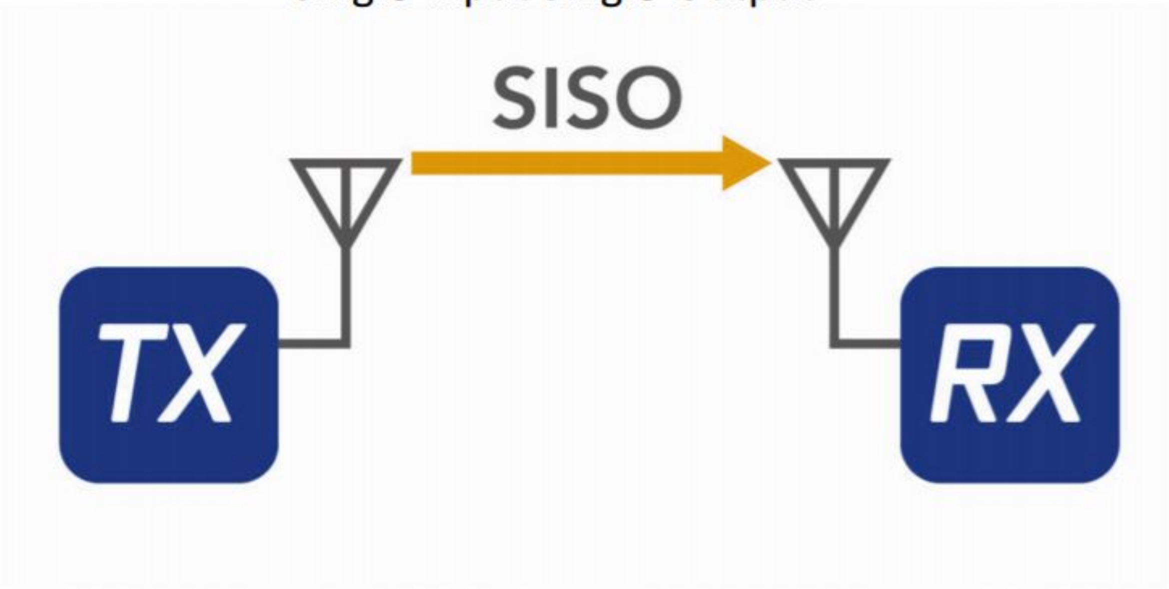
Talk Outline

- 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

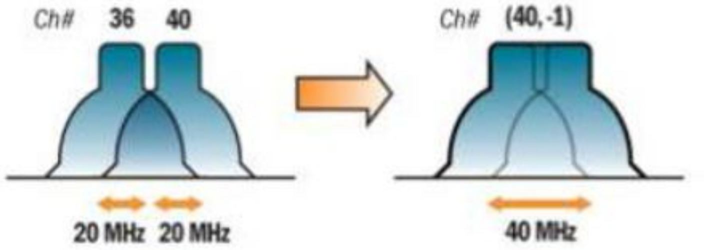


- Wi-Fi card which supports Monitor Mode
- Set same channel as Target
- Antennas generally Omnidirectional

Image Source: http://gearupz.com/wp-content/uploads/2017/03/MIMO-vs-SISO.png

802.11 n/ac Wave 1 and 2

Channel Bonding



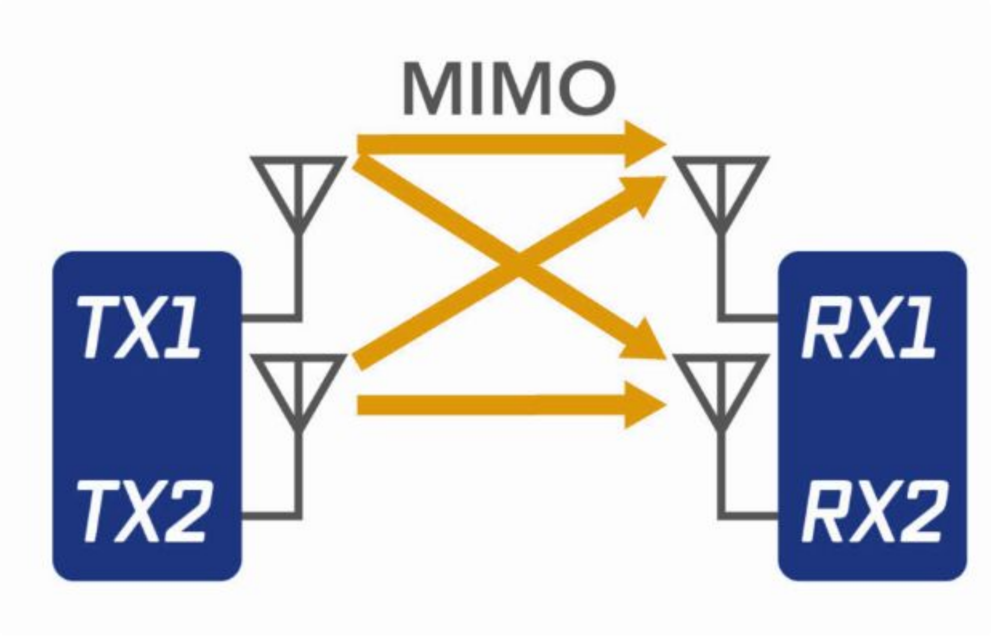
Standard 802.11 channels are effectively 20MHz wide.

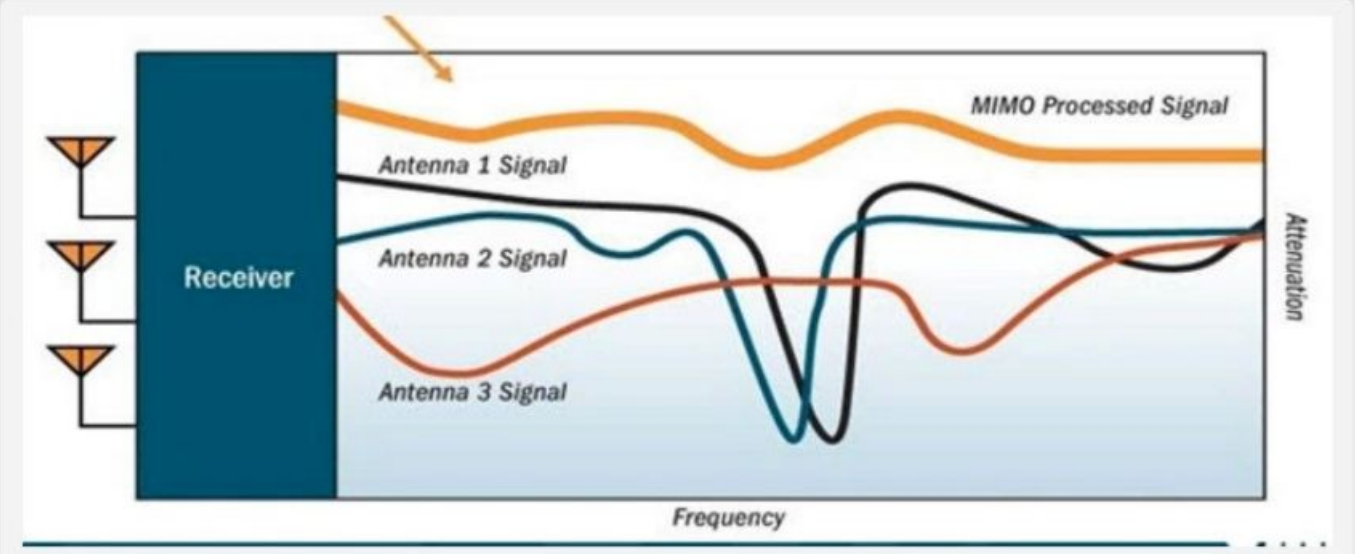
Channel bonding combines two adjacent 20MHz channels into a single 40MHz channel providing increased throughput.

Need Compatible Hardware

https://wifijedi.files.wordpress.com/2009/01/channel-bonding1.jpg

802.11 n/ac MIMO: Multiple-Input Multiple-Output



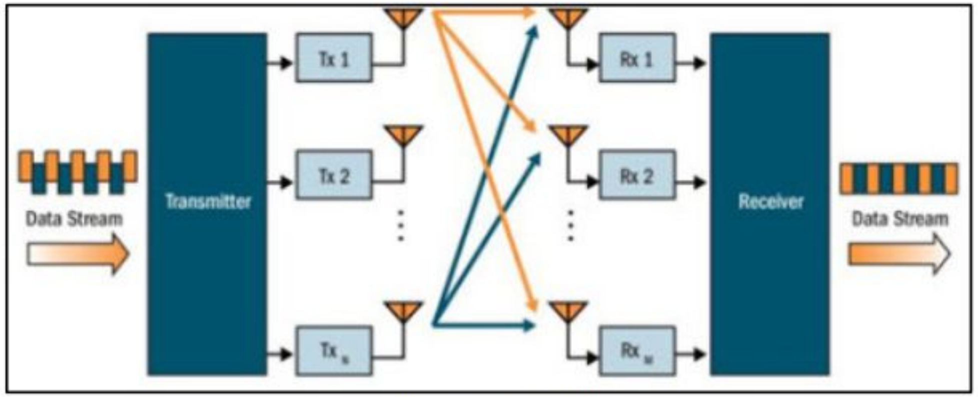


MIMO Signal Processing

Image Source: http://gearupz.com/wp-content/uploads/2017/03/MIMO-vs-SISO.png

Image source: http://internet-access-guide.com/wp-content/uploads/2016/06/MIMO-Signal-Processing.jpg

Spatial Streams

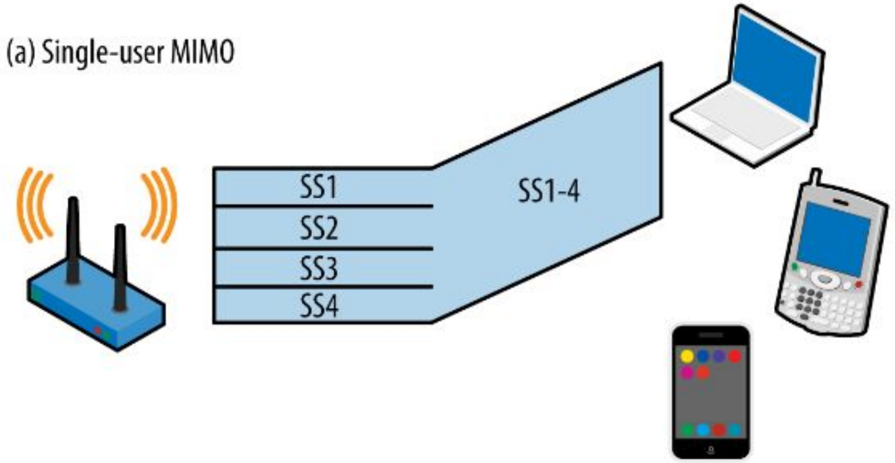


Source: ComputerWorld

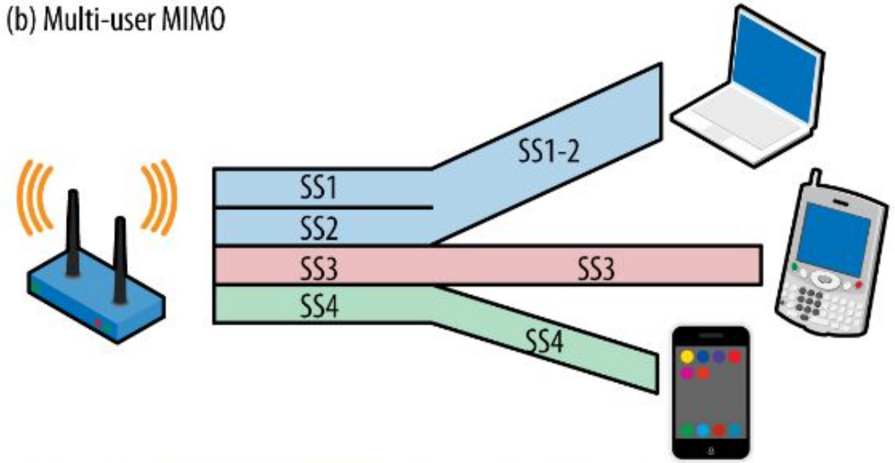
- Pure Diversity – all antennas transmit the same signal
- Spatial Multiplexing (Streams) requires every antenna send a separate signal
- This provides higher throughput at the cost of reliability
- Both transmitted and receiver need to support #streams
- 802.11n: 4 stream maximum
- 802.11ac Wave 2: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

Need Compatible Hardware

SU-MIMO and MU-MIMO



- 802.11n
- 802.11ac Wave 1
- Communicates with a single device at one time
- Hub like behavior

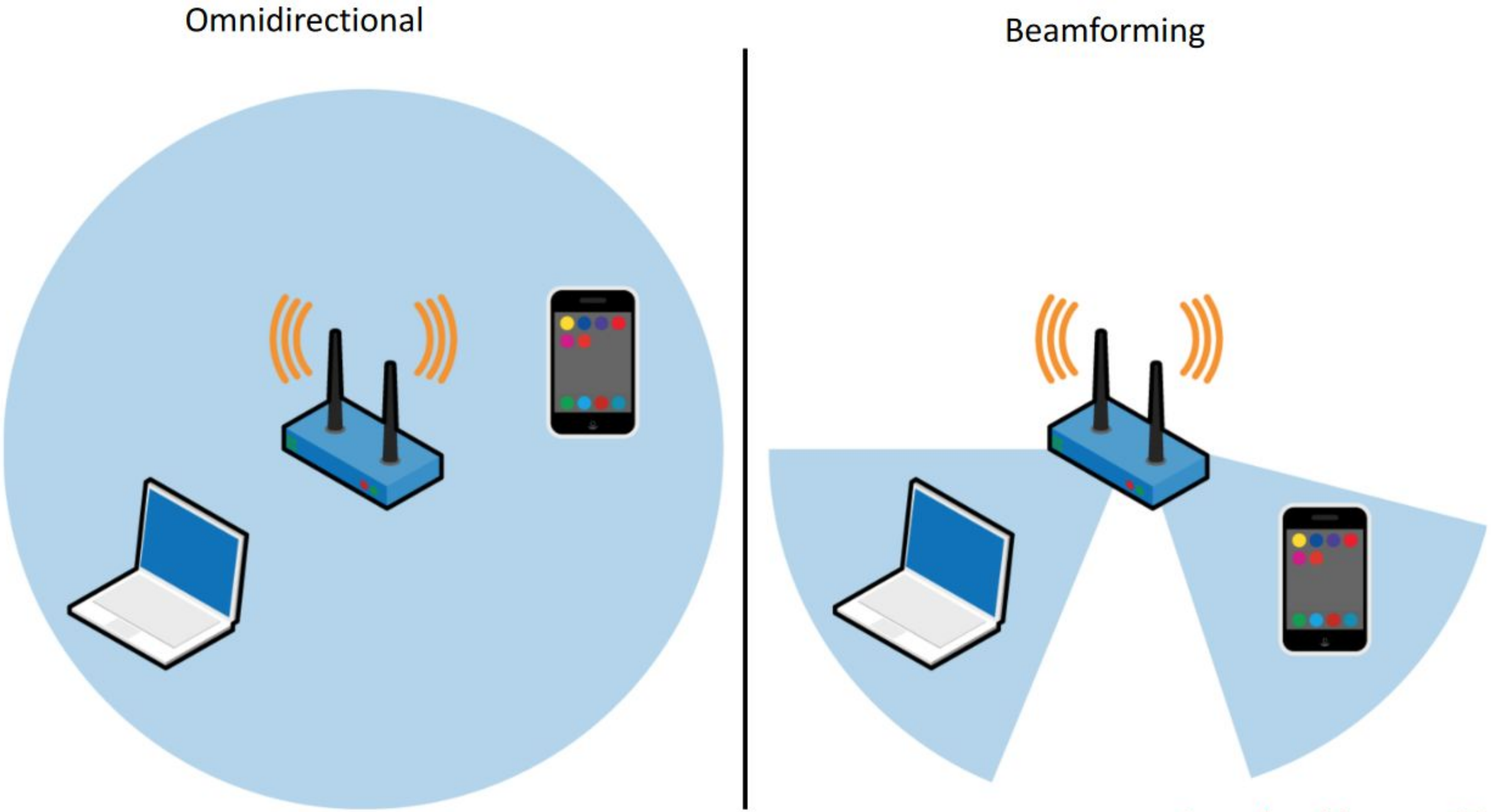


- 802.11ac Wave 2
- Communicates with multiple devices at the same time
- Switch like behavior

Need Compatible Hardware

Image Source: http://chimera.labs.oreilly.com/books/1234000001739/ch01.html#ac_product_development_plans

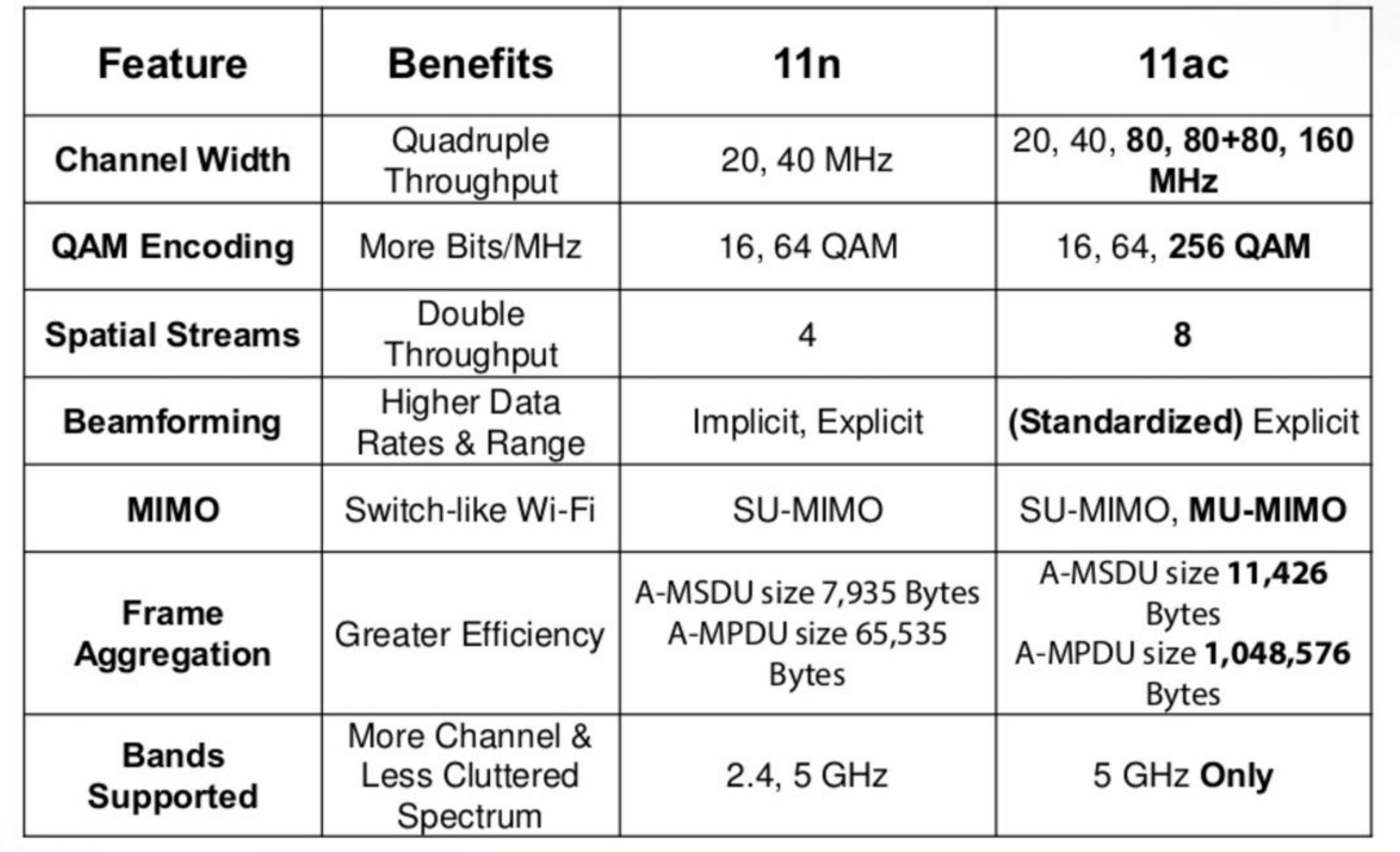
Beamforming



Location Matters, More Sensors

Image Source: http://chimera.labs.oreilly.com/books/1234000001739/ch01.html#ac_product_development_plans

802.11n & 802.11ac



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

Source: Airtight Networks

802.11n/ac Monitoring Challenges

Technology Component	Challenge
Beamforming	Location Matters
Spatial Stream Count	Capture device supports same number
High Speed	Need High Throughput Backhaul - USB? Gigabit Ethernet?
Multi-Channel & Channel Bonding	Multiple capture devices needed

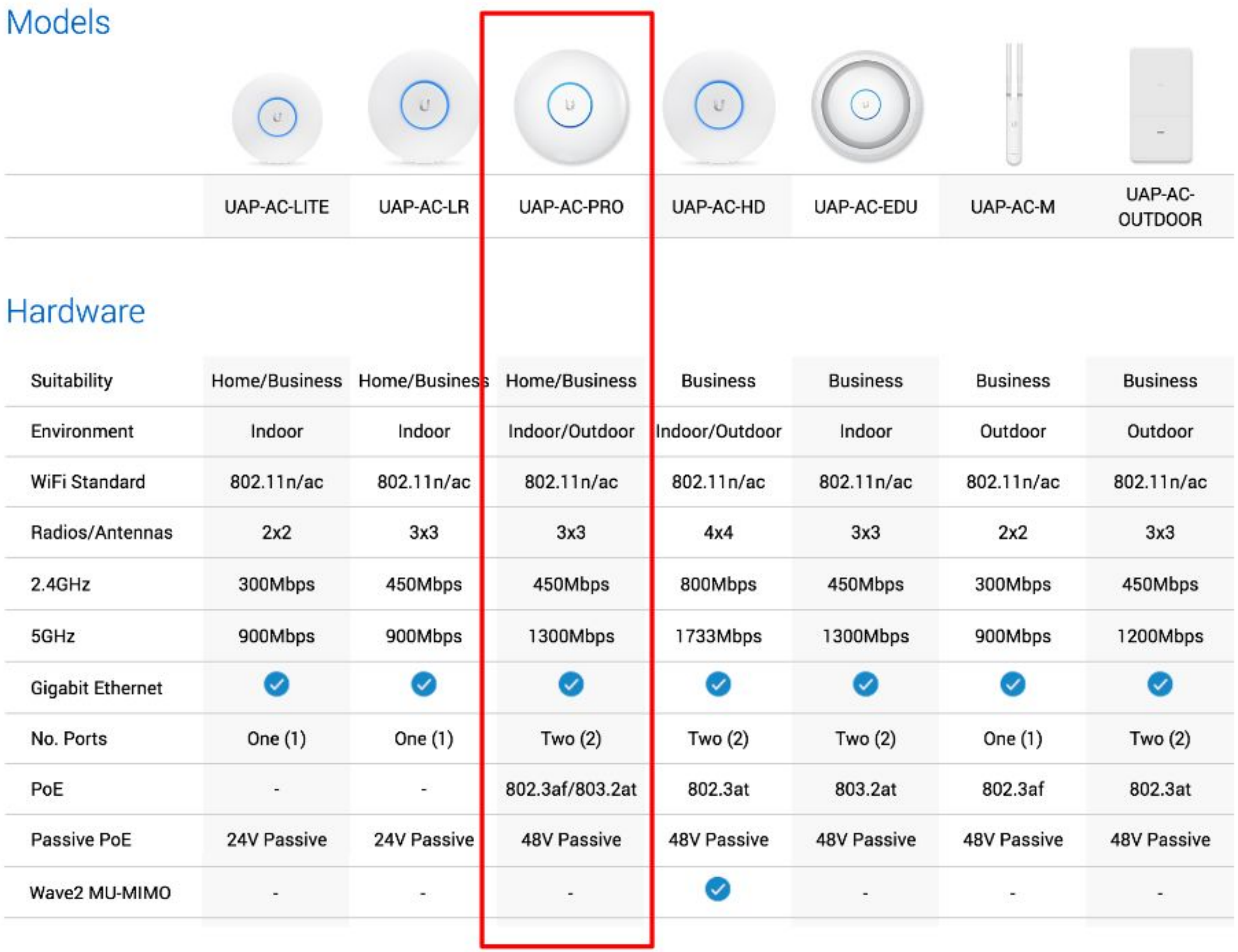
Monitoring 802.11n/ac Networks

- **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



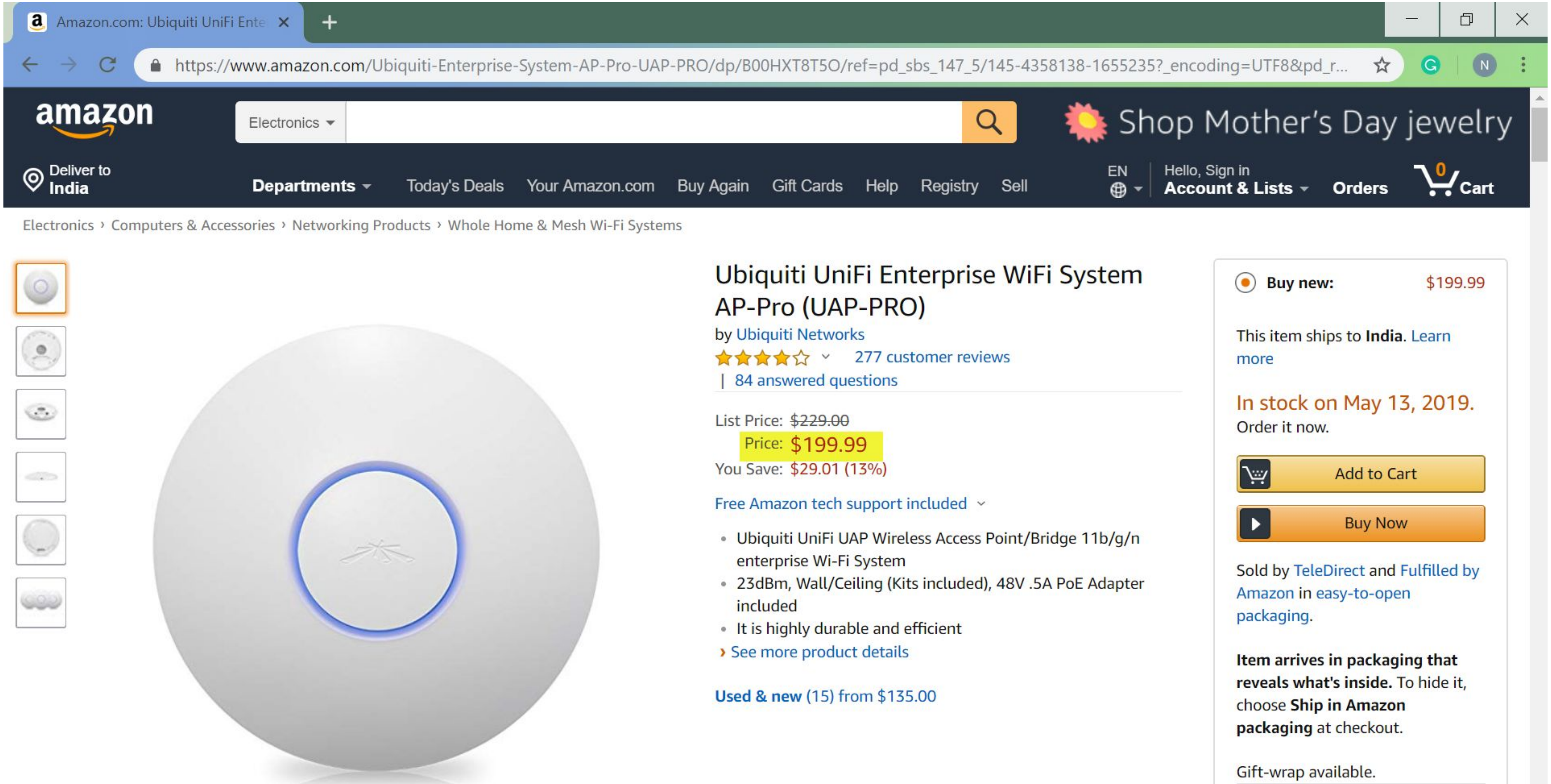
Models

	UAP-AC-LITE	UAP-AC-LR	UAP-AC-PRO	UAP-AC-HD	UAP-AC-EDU	UAP-AC-M	UAP-AC-OUTDOOR

Hardware

Suitability	Home/Business	Home/Business	Home/Business	Business	Business	Business	Business
Environment	Indoor	Indoor	Indoor/Outdoor	Indoor/Outdoor	Indoor	Outdoor	Outdoor
WiFi Standard	802.11n/ac	802.11n/ac	802.11n/ac	802.11n/ac	802.11n/ac	802.11n/ac	802.11n/ac
Radios/Antennas	2x2	3x3	3x3	4x4	3x3	2x2	3x3
2.4GHz	300Mbps	450Mbps	450Mbps	800Mbps	450Mbps	300Mbps	450Mbps
5GHz	900Mbps	900Mbps	1300Mbps	1733Mbps	1300Mbps	900Mbps	1200Mbps
Gigabit Ethernet	✓	✓	✓	✓	✓	✓	✓
No. Ports	One (1)	One (1)	Two (2)	Two (2)	Two (2)	One (1)	Two (2)
PoE	-	-	802.3af/803.2at	802.3at	803.2at	802.3af	802.3at
Passive PoE	24V Passive	24V Passive	48V Passive	48V Passive	48V Passive	48V Passive	48V Passive
Wave2 MU-MIMO	-	-	-	✓	-	-	-

UAP-AC-PRO



Amazon.com: Ubiquiti UniFi Ente
https://www.amazon.com/Ubiquiti-Enterprise-System-AP-Pro-UAP-PRO/dp/B00HXT8T5O/ref=pd_sbs_147_5/145-4358138-1655235?_encoding=UTF8&pd_r...
amazon
Electronics
Shop Mother's Day jewelry
Deliver to India
Departments
Today's Deals
Your Amazon.com
Buy Again
Gift Cards
Help
Registry
Sell
EN
Hello, Sign in
Account & Lists
Orders
0
Cart

Electronics › Computers & Accessories › Networking Products › Whole Home & Mesh Wi-Fi Systems

Ubiquiti UniFi Enterprise WiFi System AP-Pro (UAP-PRO)

by Ubiquiti Networks

277 customer reviews | 84 answered questions

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

› See more product details

Used & new (15) from $135.00

● Buy new: $199.99

This item ships to India. Learn more

In stock on May 13, 2019.
Order it now.

Sold by TeleDirect and Fulfilled by Amazon in easy-to-open packaging.

Item arrives in packaging that reveals what's inside. To hide it, choose **Ship in Amazon packaging** at checkout.

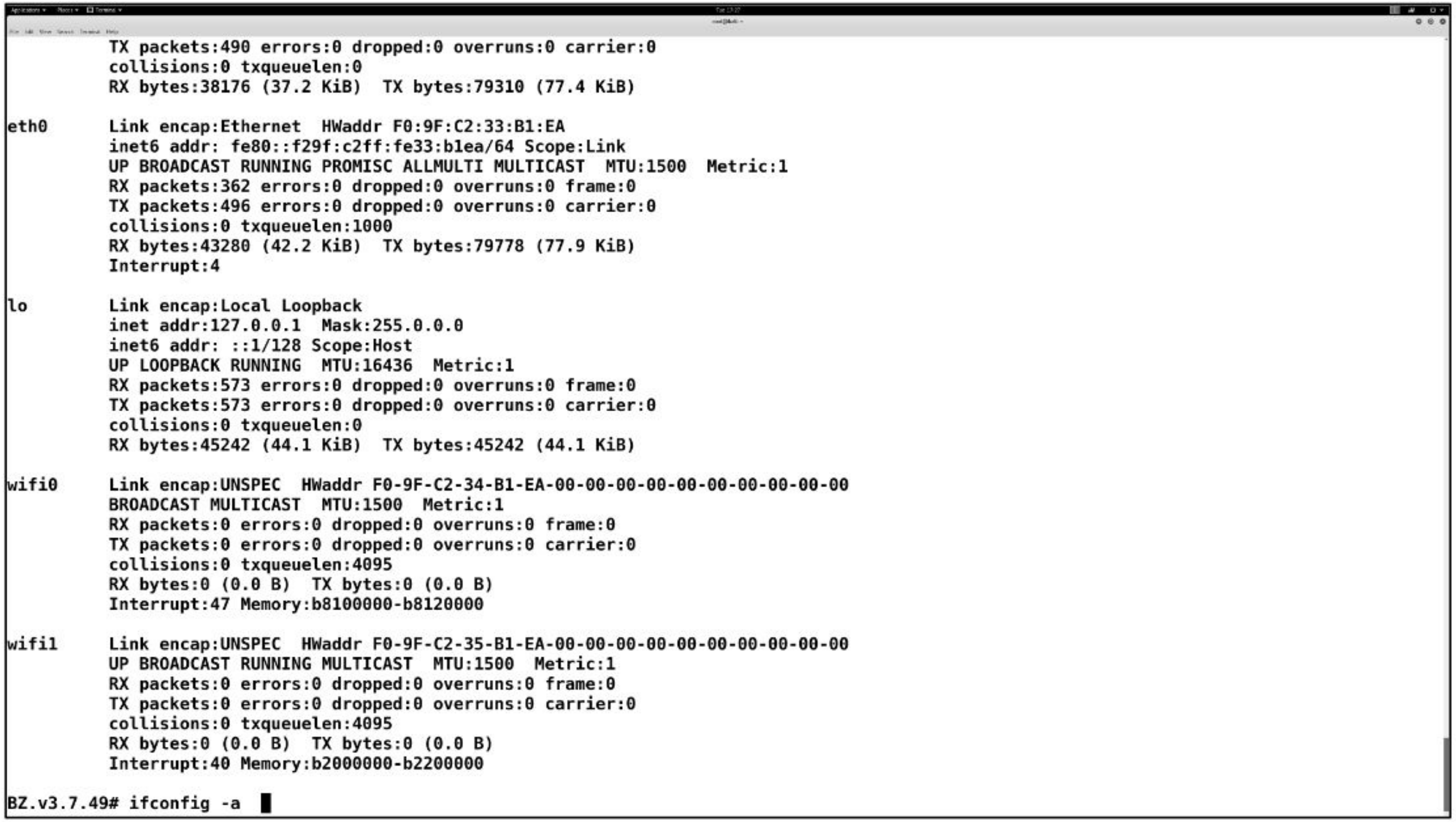
Gift-wrap available.

©PentesterAcademy.com

UAP-AC-PRO

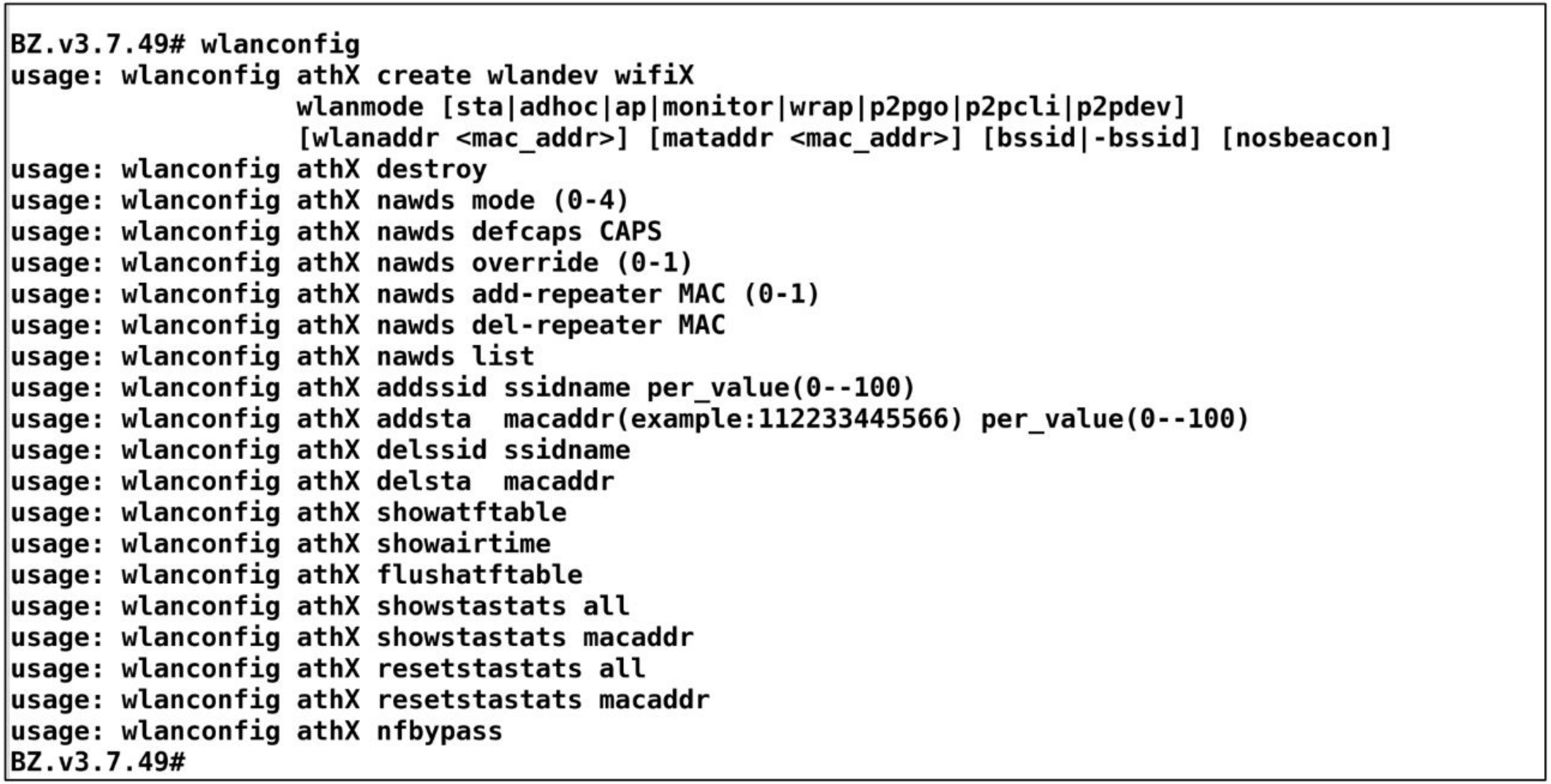
- OpenWRT based system
- Uses Madwifi-NG drivers for Wi-Fi
- SSH enabled

Wireless Interfaces



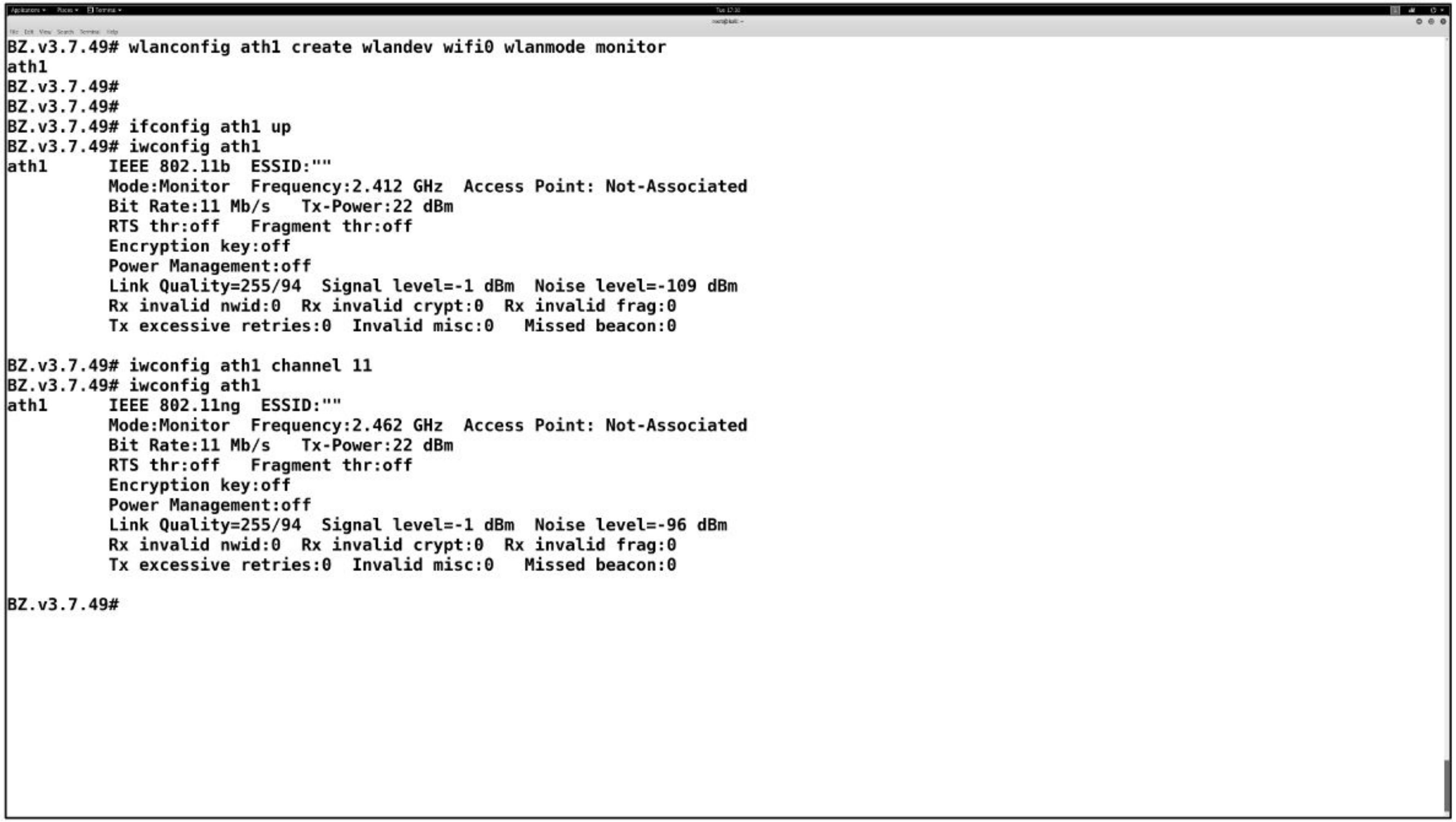
```
          TX packets:490 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:38176 (37.2 KiB)  TX bytes:79310 (77.4 KiB)

eth0      Link encap:Ethernet  HWaddr F0:9F:C2:33:B1:EA
          inet6 addr: fe80::f29f:c2ff:fe33:b1ea/64 Scope:Link
          UP BROADCAST RUNNING PROMISC ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:362 errors:0 dropped:0 overruns:0 frame:0
          TX packets:496 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:43280 (42.2 KiB)  TX bytes:79778 (77.9 KiB)
          Interrupt:4

lo        Link encap:Local 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)

wifi0     Link encap:UNSPEC  HWaddr F0-9F-C2-34-B1-EA-00-00-00-00-00-00-00-00-00-00
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:4095
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:47 Memory:b8100000-b8120000

wifi1     Link encap:UNSPEC  HWaddr F0-9F-C2-35-B1-EA-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:4095
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:40 Memory:b2000000-b2200000

BZ.v3.7.49# ifconfig -a
```

Wlanconfig Tool



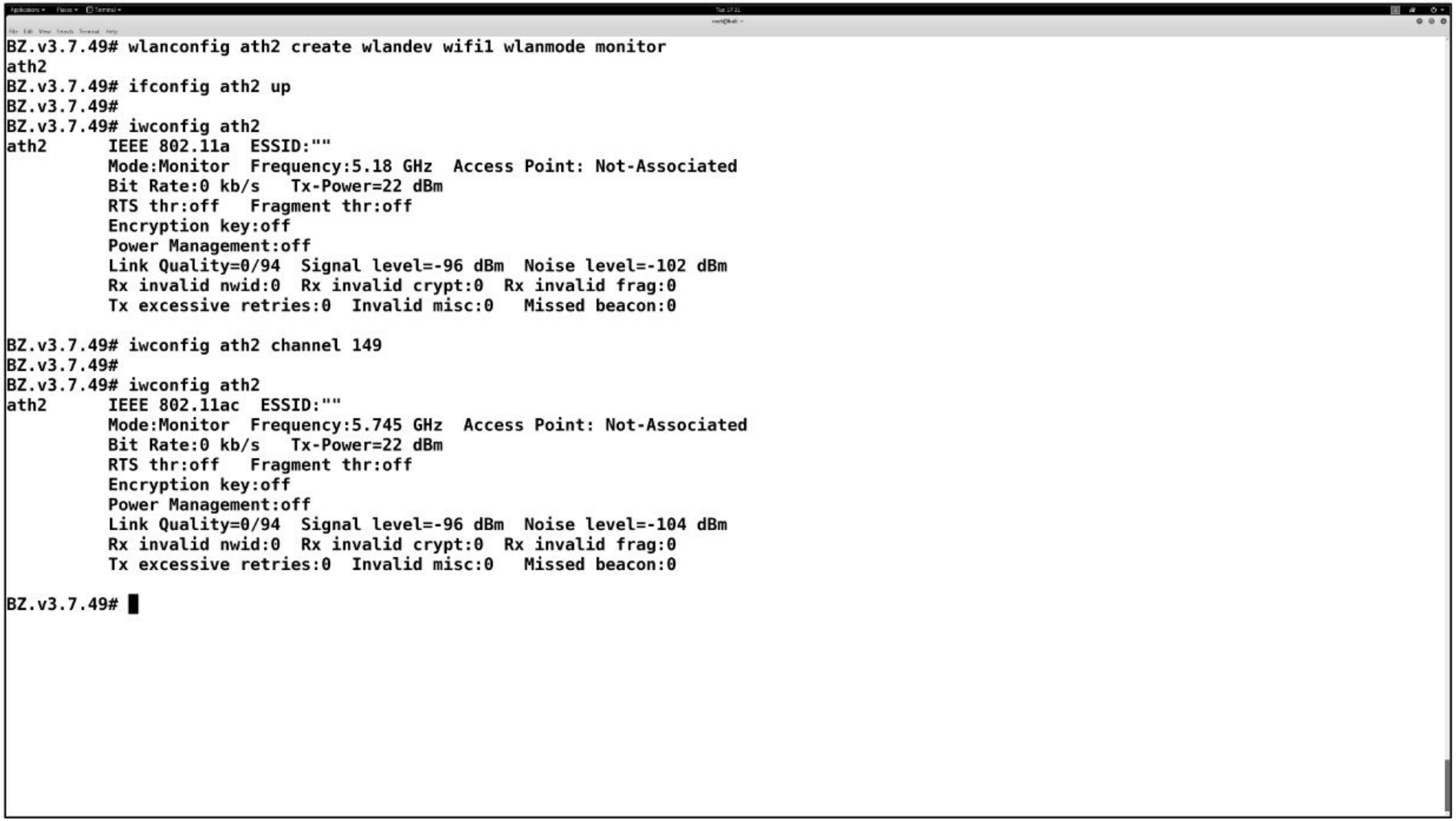
```
BZ.v3.7.49# wlanconfig
usage: wlanconfig athX create wlandev wifiX
                  wlanmode [sta|adhoc|ap|monitor|wrap|p2pgo|p2pcli|p2pdev]
                  [wlanaddr <mac_addr>] [mataddr <mac_addr>] [bssid|-bssid] [nosbeacon]
usage: wlanconfig athX destroy
usage: wlanconfig athX nawds mode (0-4)
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 nfbypass
BZ.v3.7.49#
```

Create 2.4 Ghz Monitor Mode Interface



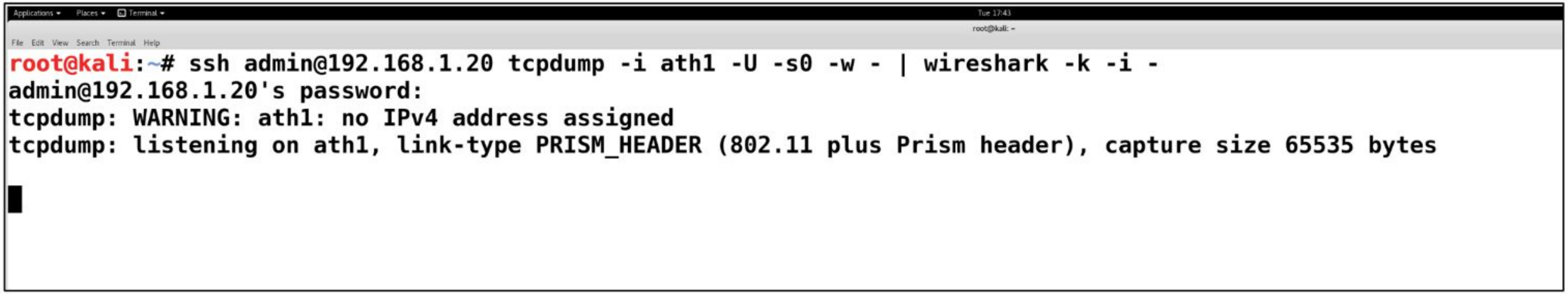
```
BZ.v3.7.49# wlanconfig ath1 create wlandev wifi0 wlanmode monitor
ath1
BZ.v3.7.49#
BZ.v3.7.49#
BZ.v3.7.49# ifconfig ath1 up
BZ.v3.7.49# iwconfig ath1
ath1      IEEE 802.11b  ESSID:""
          Mode:Monitor  Frequency:2.412 GHz  Access Point: Not-Associated
          Bit Rate:11 Mb/s   Tx-Power:22 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 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 ath1 channel 11
BZ.v3.7.49# iwconfig ath1
ath1      IEEE 802.11ng  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 nwid: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

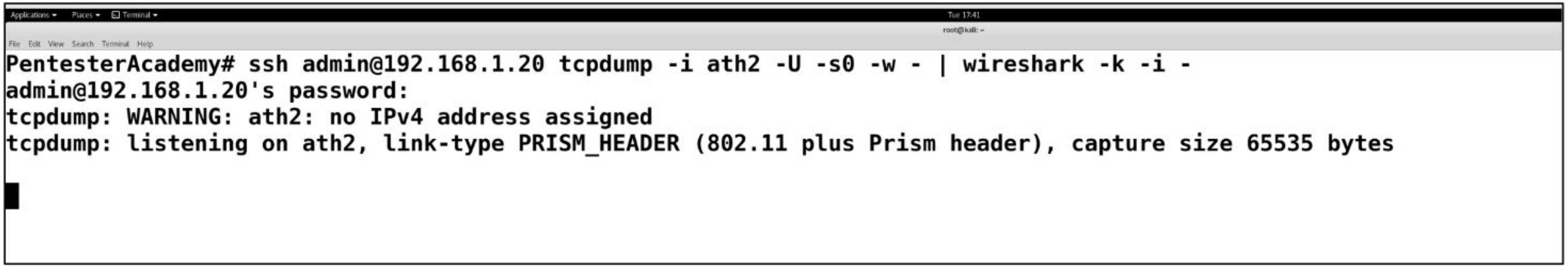


```
BZ.v3.7.49# wlanconfig ath2 create wlandev wifi1 wlanmode monitor
ath2
BZ.v3.7.49# ifconfig ath2 up
BZ.v3.7.49#
BZ.v3.7.49# iwconfig ath2
ath2      IEEE 802.11a  ESSID:""
          Mode:Monitor  Frequency:5.18 GHz  Access Point: Not-Associated
          Bit Rate:0 kb/s   Tx-Power=22 dBm
          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#
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

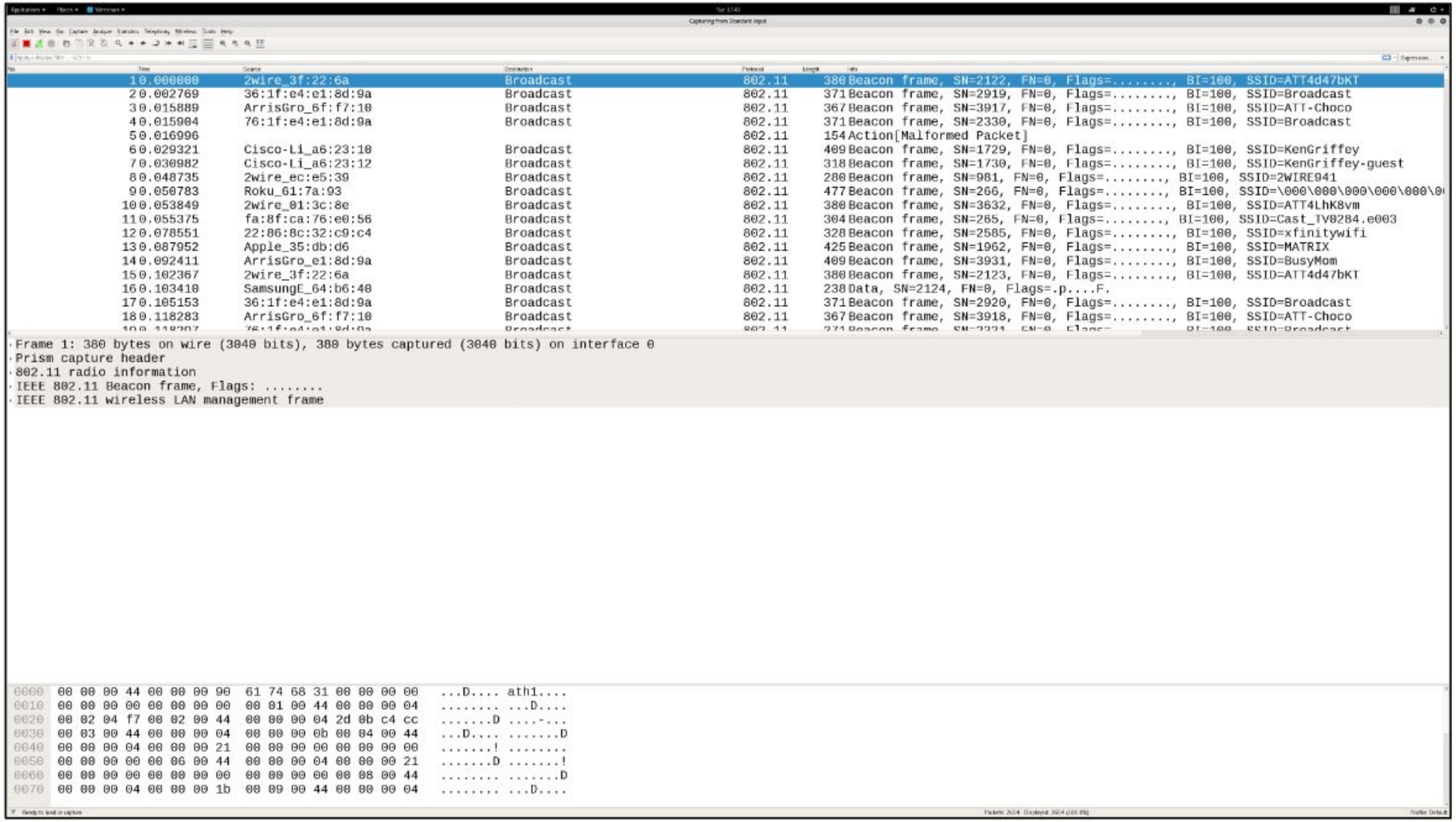


```
root@kali:~# ssh admin@192.168.1.20 tcpdump -i ath1 -U -s0 -w - | wireshark -k -i -
admin@192.168.1.20's password:
tcpdump: WARNING: ath1: no IPv4 address assigned
tcpdump: listening on ath1, link-type PRISM_HEADER (802.11 plus Prism header), capture size 65535 bytes
```



```
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


Applications ▾
Places ▾
Wireshark ▾
Capturing from Standard input
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

```
No.  Time        Source              Destination  Protocol  Length Info
   1 0.000000    2wire_3f:22:6a      Broadcast    802.11    380 Beacon frame, SN=2122, FN=0, Flags=........, BI=100, SSID=ATT4d47bKT
   2 0.002769    36:1f:e4:e1:8d:9a   Broadcast    802.11    371 Beacon frame, SN=2919, FN=0, Flags=........, BI=100, SSID=Broadcast
   3 0.015889    ArrisGro_6f:f7:10   Broadcast    802.11    367 Beacon frame, SN=3917, FN=0, Flags=........, BI=100, SSID=ATT-Choco
   4 0.015904    76:1f:e4:e1:8d:9a   Broadcast    802.11    371 Beacon frame, SN=2330, FN=0, Flags=........, BI=100, SSID=Broadcast
   5 0.016996                                     802.11    154 Action[Malformed Packet]
   6 0.029321    Cisco-Li_a6:23:10   Broadcast    802.11    409 Beacon frame, SN=1729, FN=0, Flags=........, BI=100, SSID=KenGriffey
   7 0.030982    Cisco-Li_a6:23:12   Broadcast    802.11    318 Beacon frame, SN=1730, FN=0, Flags=........, BI=100, SSID=KenGriffey-guest
   8 0.048735    2wire_ec:e5:39      Broadcast    802.11    280 Beacon frame, SN=981, FN=0, Flags=........, BI=100, SSID=2WIRE941
   9 0.050783    Roku_61:7a:93       Broadcast    802.11    477 Beacon frame, SN=266, FN=0, Flags=........, BI=100, SSID=\000\000\000\000\000\0
  10 0.053849    2wire_01:3c:8e      Broadcast    802.11    380 Beacon frame, SN=3632, FN=0, Flags=........, BI=100, SSID=ATT4LhK8vm
  11 0.055375    fa:8f:ca:76:e0:56   Broadcast    802.11    304 Beacon frame, SN=265, FN=0, Flags=........, BI=100, SSID=Cast_TV0284.e003
  12 0.078551    22:86:8c:32:c9:c4   Broadcast    802.11    328 Beacon frame, SN=2585, FN=0, Flags=........, BI=100, SSID=xfinitywifi
  13 0.087952    Apple_35:db:d6      Broadcast    802.11    425 Beacon frame, SN=1962, FN=0, Flags=........, BI=100, SSID=MATRIX
  14 0.092411    ArrisGro_e1:8d:9a   Broadcast    802.11    409 Beacon frame, SN=3931, FN=0, Flags=........, BI=100, SSID=BusyMom
  15 0.102367    2wire_3f:22:6a      Broadcast    802.11    380 Beacon frame, SN=2123, FN=0, Flags=........, BI=100, SSID=ATT4d47bKT
  16 0.103410    SamsungE_64:b6:40   Broadcast    802.11    238 Data, SN=2124, FN=0, Flags=.p....F.
  17 0.105153    36:1f:e4:e1:8d:9a   Broadcast    802.11    371 Beacon frame, SN=2920, FN=0, Flags=........, BI=100, SSID=Broadcast
  18 0.118283    ArrisGro_6f:f7:10   Broadcast    802.11    367 Beacon frame, SN=3918, FN=0, Flags=........, BI=100, SSID=ATT-Choco
```

```
› Frame 1: 380 bytes on wire (3040 bits), 380 bytes captured (3040 bits) on interface 0
› Prism capture header
› 802.11 radio information
› IEEE 802.11 Beacon frame, Flags: ........
› IEEE 802.11 wireless LAN management frame
```

```
0000  00 00 00 44 00 00 00 90  61 74 68 31 00 00 00 00   ...D.... ath1....
0010  00 00 00 00 00 00 00 00  00 01 00 44 00 00 00 04   ........ ...D....
0020  00 02 04 f7 00 02 00 44  00 00 00 04 2d 0b c4 cc   .......D ....-...
0030  00 03 00 44 00 00 00 04  00 00 00 0b 00 04 00 44   ...D.... .......D
0040  00 00 00 04 00 00 00 21  00 00 00 00 00 00 00 00   .......! ........
0050  00 00 00 00 00 06 00 44  00 00 00 04 00 00 00 21   .......D .......!
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 08 00 44   ........ .......D
0070  00 00 00 04 00 00 00 1b  00 09 00 44 00 00 00 04   ........ ...D....
```

Ready to load or capture

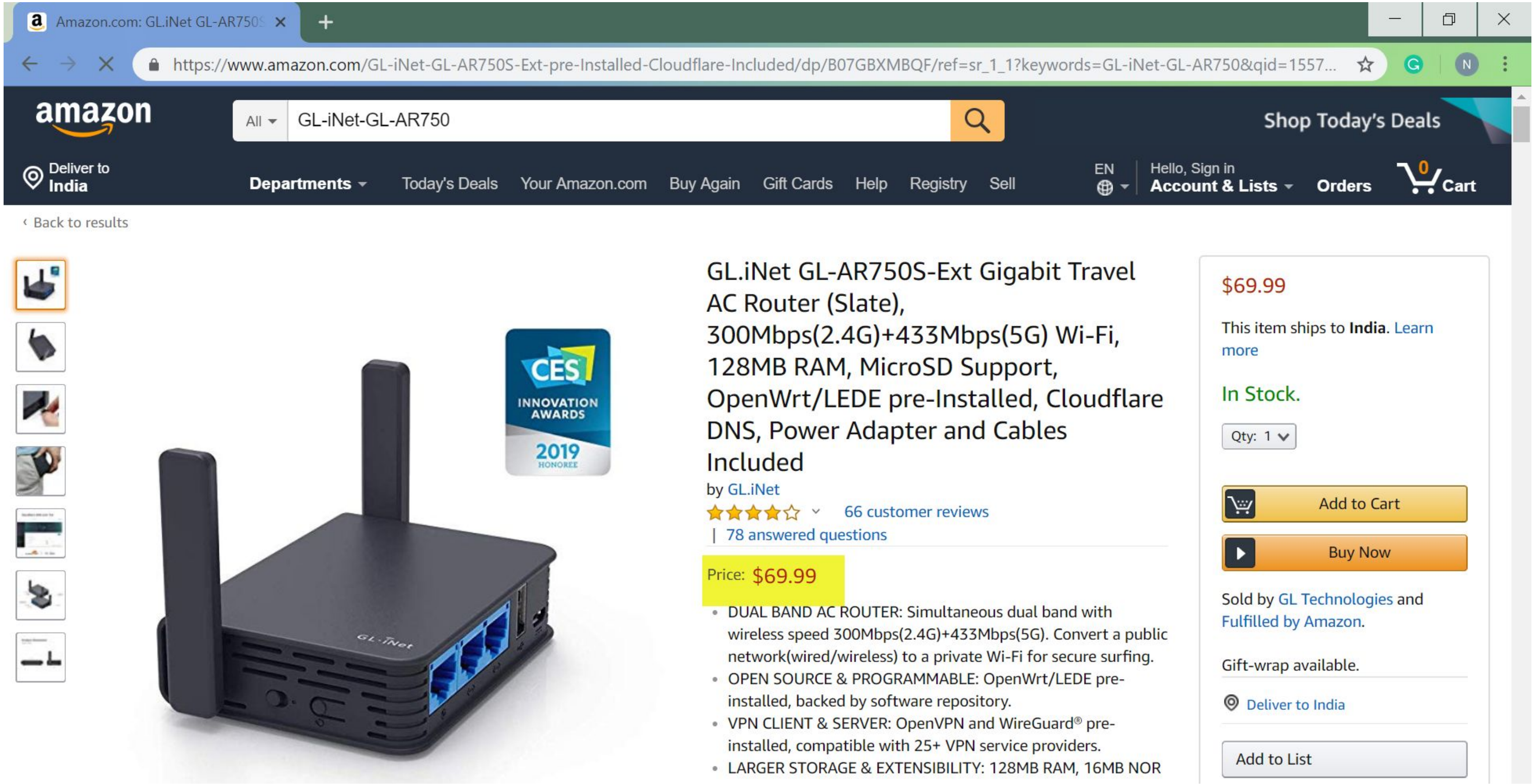
Packets: 2614 · Displayed: 2614 (100.0%)

Profile: Default

Better Alternative

- Cheaper
- Less modification
- Smaller
- External antenna
- Multi purpose
- USB Powered

GL.iNet GL-AR750S



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

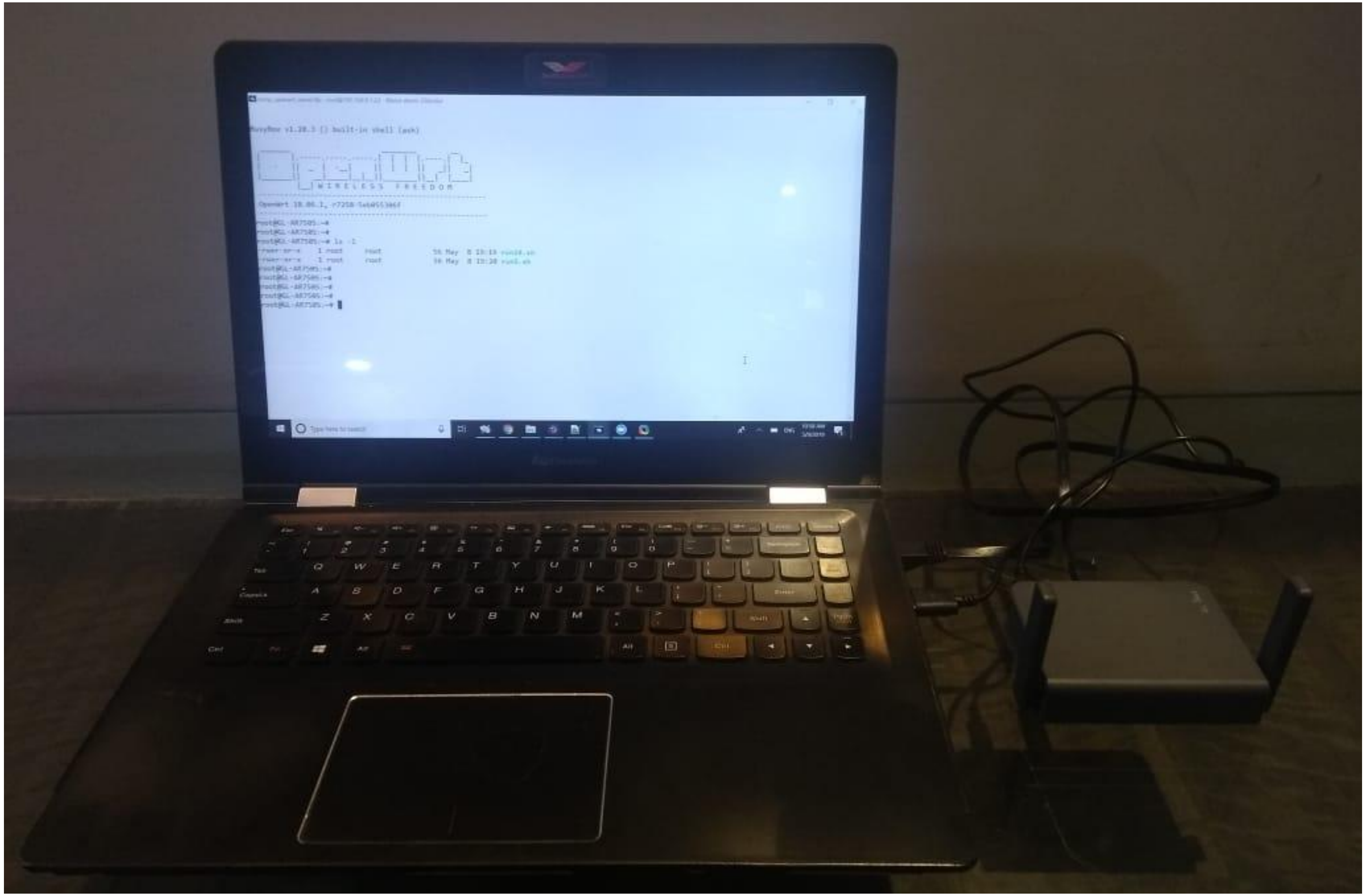
In Stock.

Qty: 1

Sold by GL Technologies and Fulfilled by Amazon.

Gift-wrap available.

Powered by USB, External Antenna

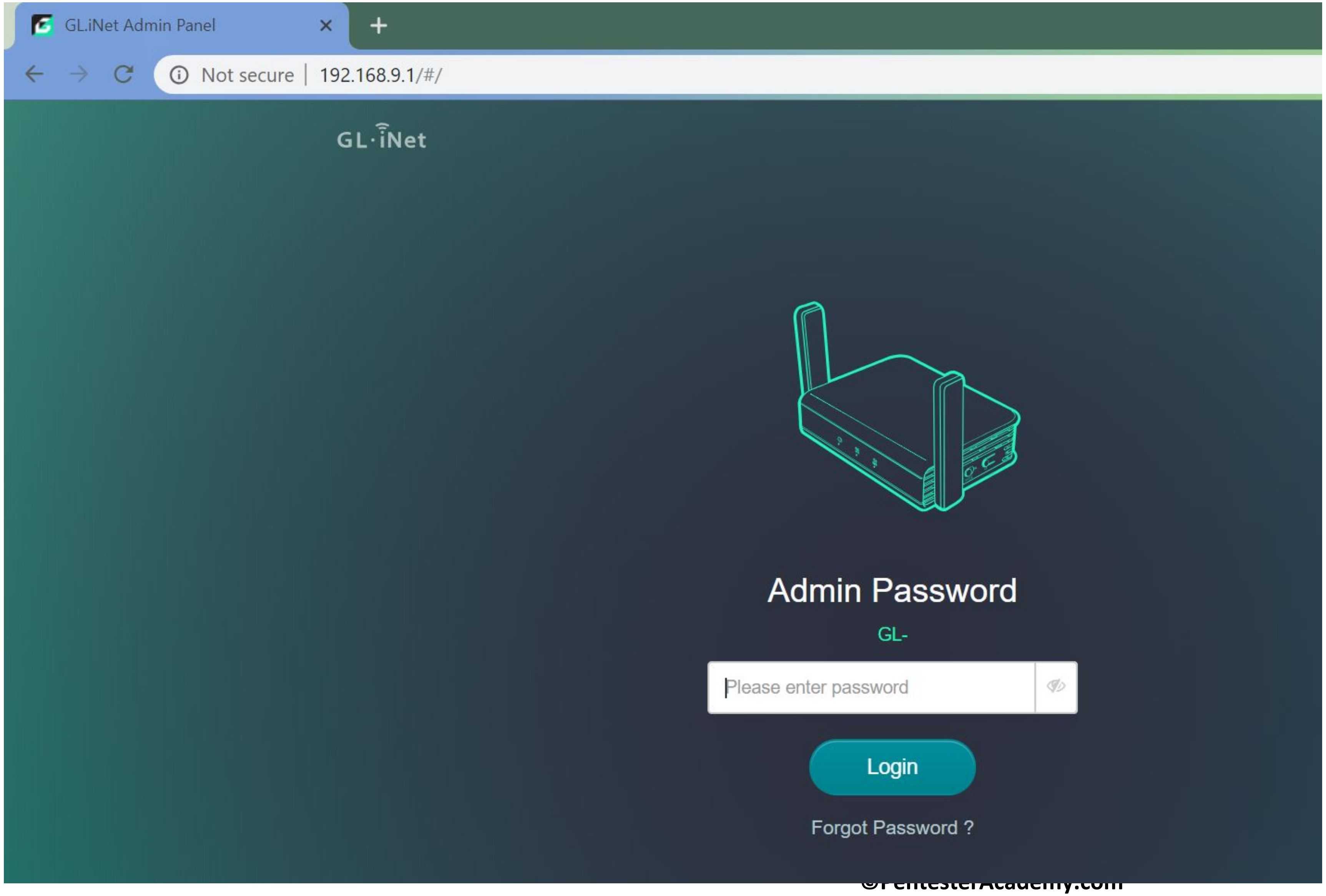


```
BusyBox v1.28.3 () built-in shell (ash)

                   W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 OpenWrt 18.06.1, r7258-5eb055306f
 -----------------------------------------------------
root@GL-AR750S:~#
root@GL-AR750S:~#
root@GL-AR750S:~# ls -l
-rwxr-xr-x    1 root     root            56 May  8 19:19 run10.sh
-rwxr-xr-x    1 root     root            36 May  8 19:20 run1.sh
root@GL-AR750S:~#
root@GL-AR750S:~#
root@GL-AR750S:~#
root@GL-AR750S:~#
root@GL-AR750S:~#
```

©PentesterAcademy.com

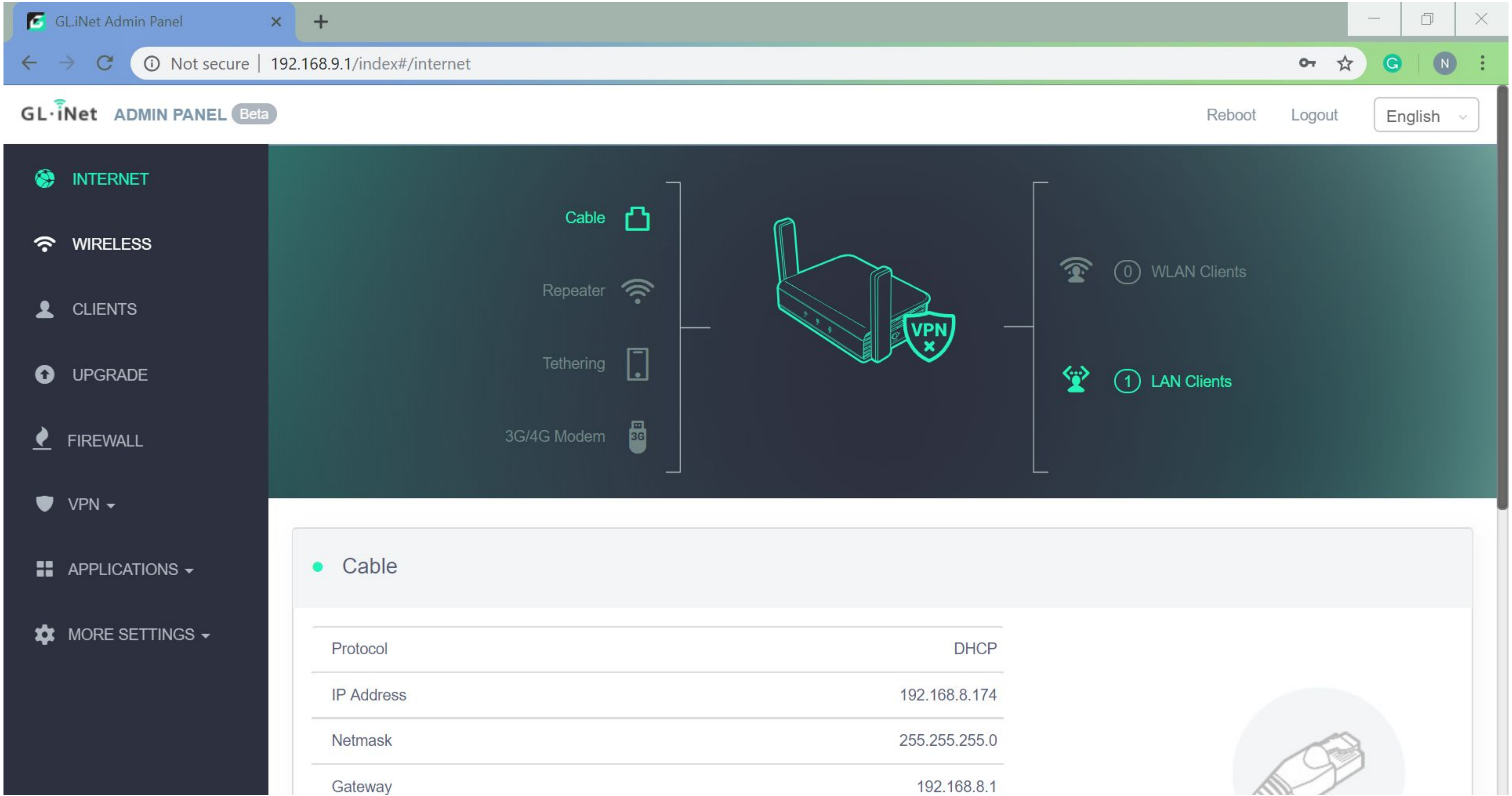
Smaller, Pocket Friendly Shape

Vendor Web UI



No Password by Default

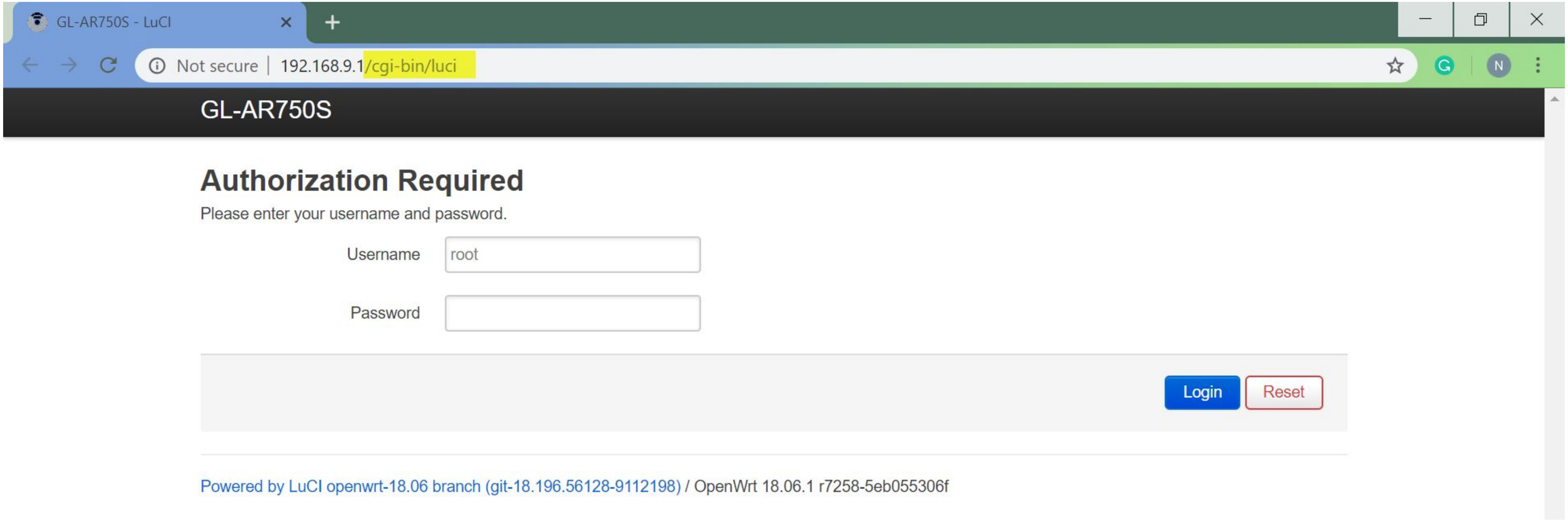
Vendor Web UI



● Cable

Protocol	DHCP
IP Address	192.168.8.174
Netmask	255.255.255.0
Gateway	192.168.8.1

LuCI



192.168.9.1/cgi-bin/luci

GL-AR750S

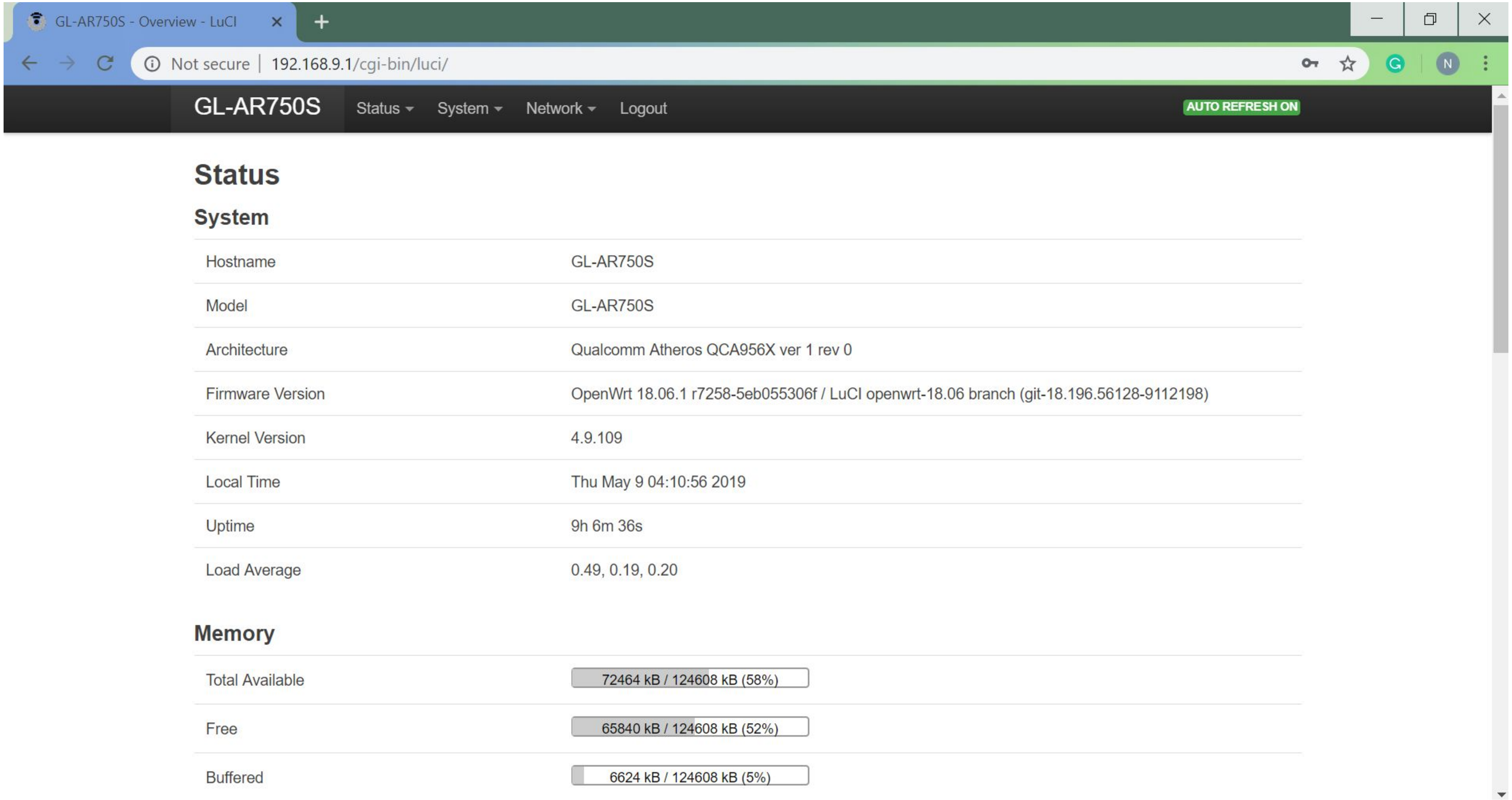
Authorization Required

Please enter your username and password.

Username	root
Password	

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

LuCI



GL-AR750S - Overview - LuCI
Not secure | 192.168.9.1/cgi-bin/luci/
GL-AR750S
Status
System
Network
Logout
AUTO REFRESH ON

Status

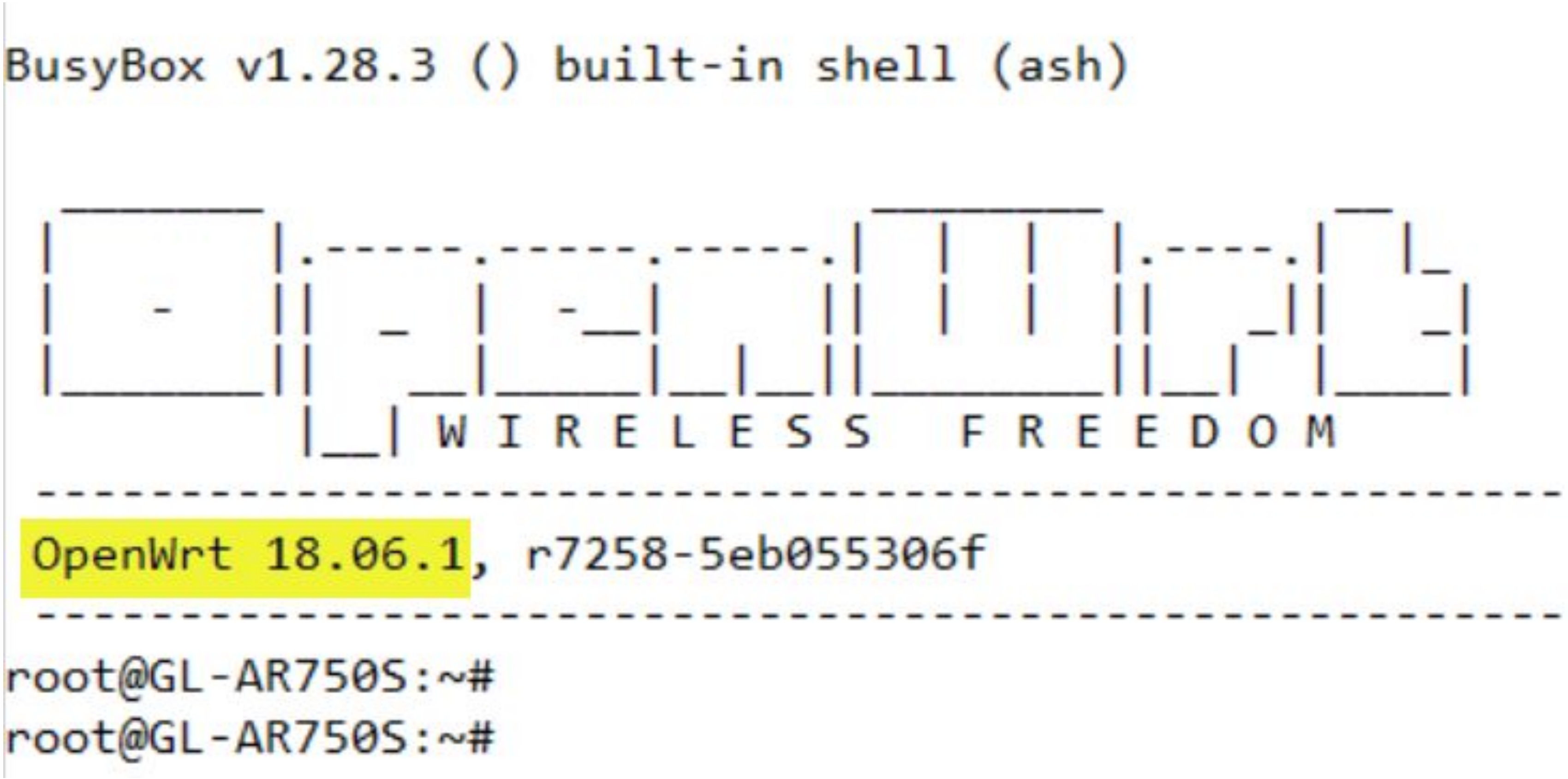
System

Hostname	GL-AR750S
Model	GL-AR750S
Architecture	Qualcomm Atheros QCA956X ver 1 rev 0
Firmware Version	OpenWrt 18.06.1 r7258-5eb055306f / LuCI openwrt-18.06 branch (git-18.196.56128-9112198)
Kernel Version	4.9.109
Local Time	Thu May 9 04:10:56 2019
Uptime	9h 6m 36s
Load Average	0.49, 0.19, 0.20

Memory

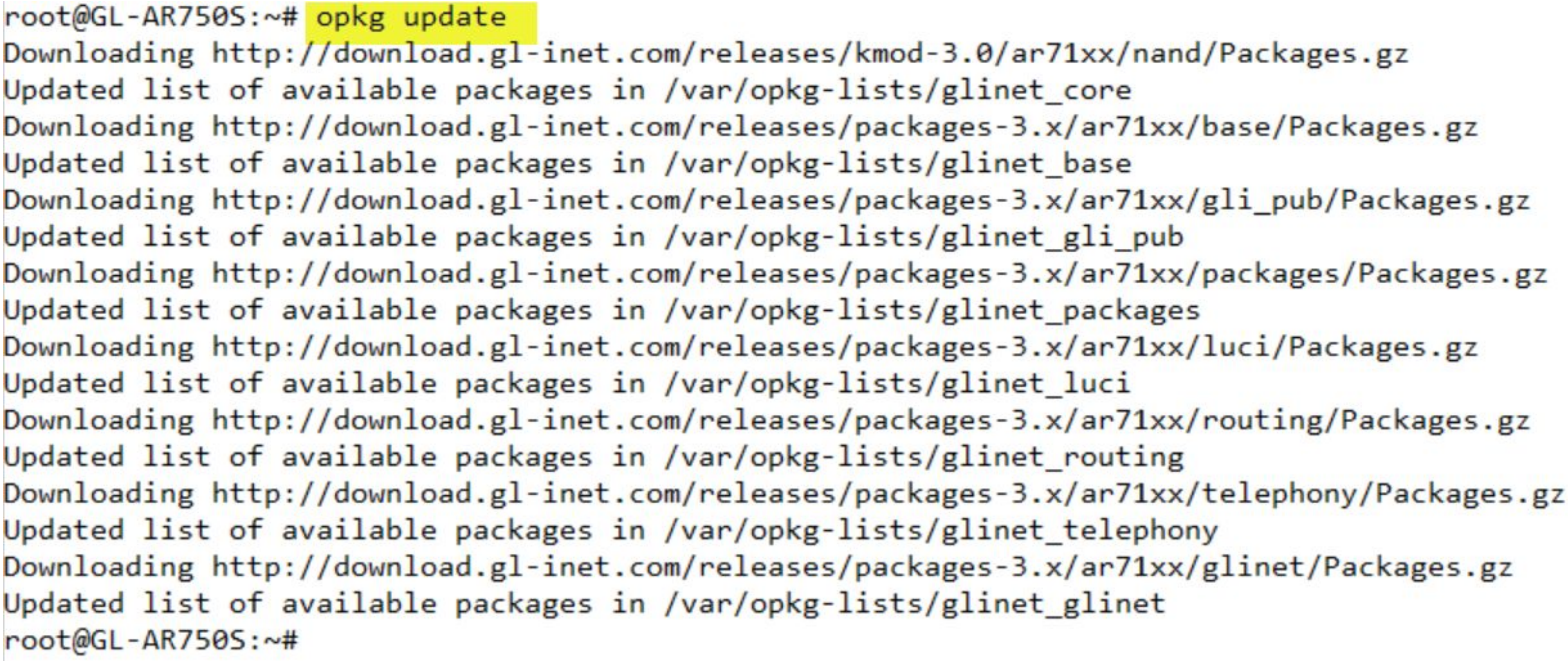
Total Available	72464 kB / 124608 kB (58%)
Free	65840 kB / 124608 kB (52%)
Buffered	6624 kB / 124608 kB (5%)

SSH



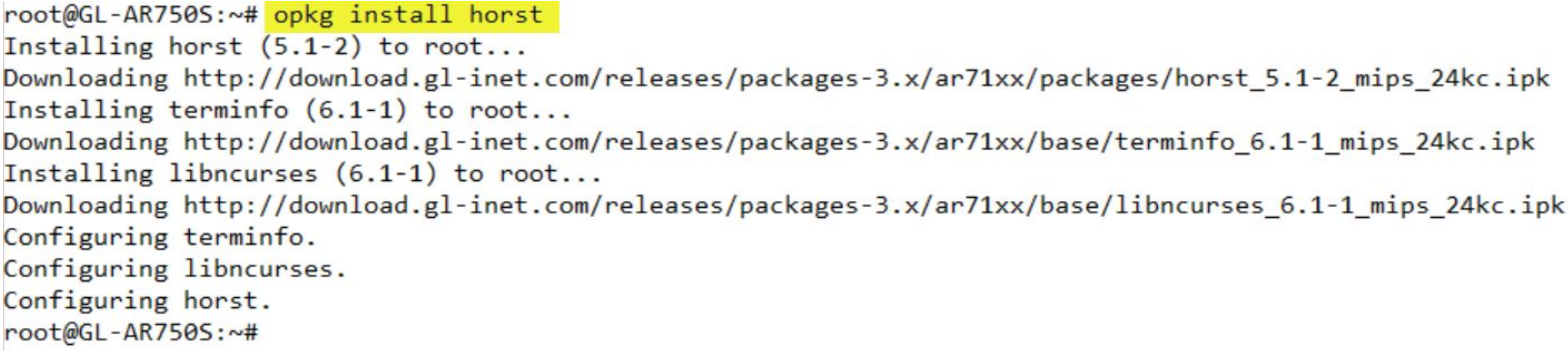
```
BusyBox v1.28.3 () built-in shell (ash)

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 OpenWrt 18.06.1, r7258-5eb055306f
 -----------------------------------------------------
root@GL-AR750S:~#
root@GL-AR750S:~#
```

Updating Package List

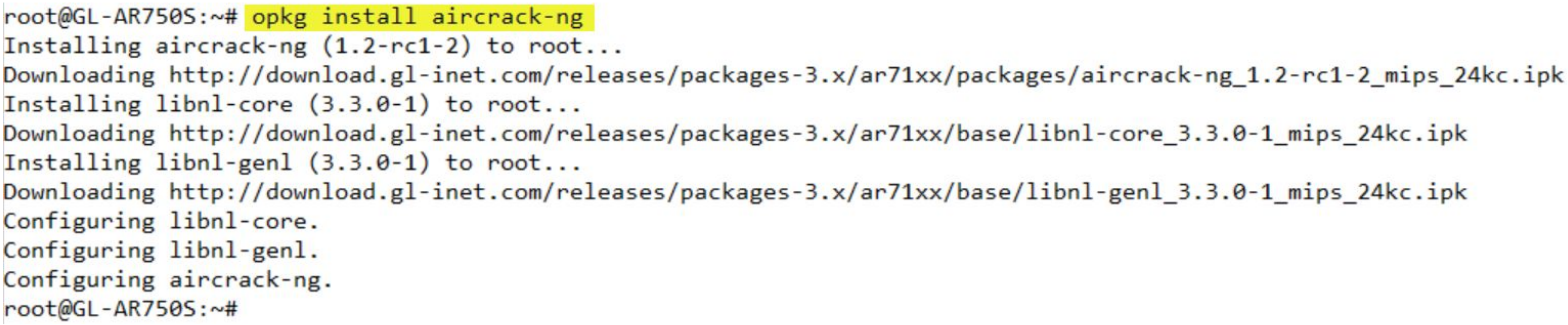


```
root@GL-AR750S:~# opkg update
Downloading http://download.gl-inet.com/releases/kmod-3.0/ar71xx/nand/Packages.gz
Updated list of available packages in /var/opkg-lists/glinet_core
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/base/Packages.gz
Updated list of available packages 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

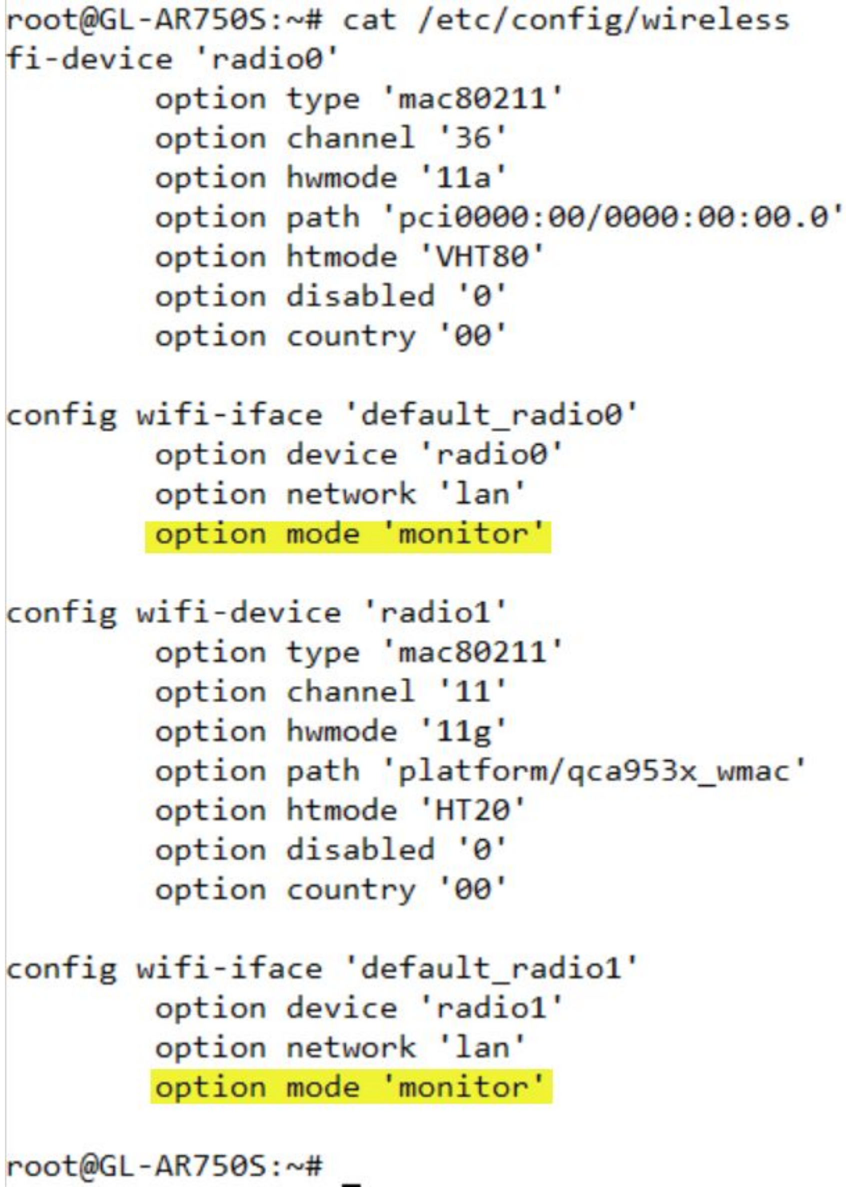


```
root@GL-AR750S:~# opkg install horst
Installing horst (5.1-2) to root...
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/packages/horst_5.1-2_mips_24kc.ipk
Installing terminfo (6.1-1) to root...
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/base/terminfo_6.1-1_mips_24kc.ipk
Installing libncurses (6.1-1) to root...
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/base/libncurses_6.1-1_mips_24kc.ipk
Configuring terminfo.
Configuring libncurses.
Configuring horst.
root@GL-AR750S:~#
```



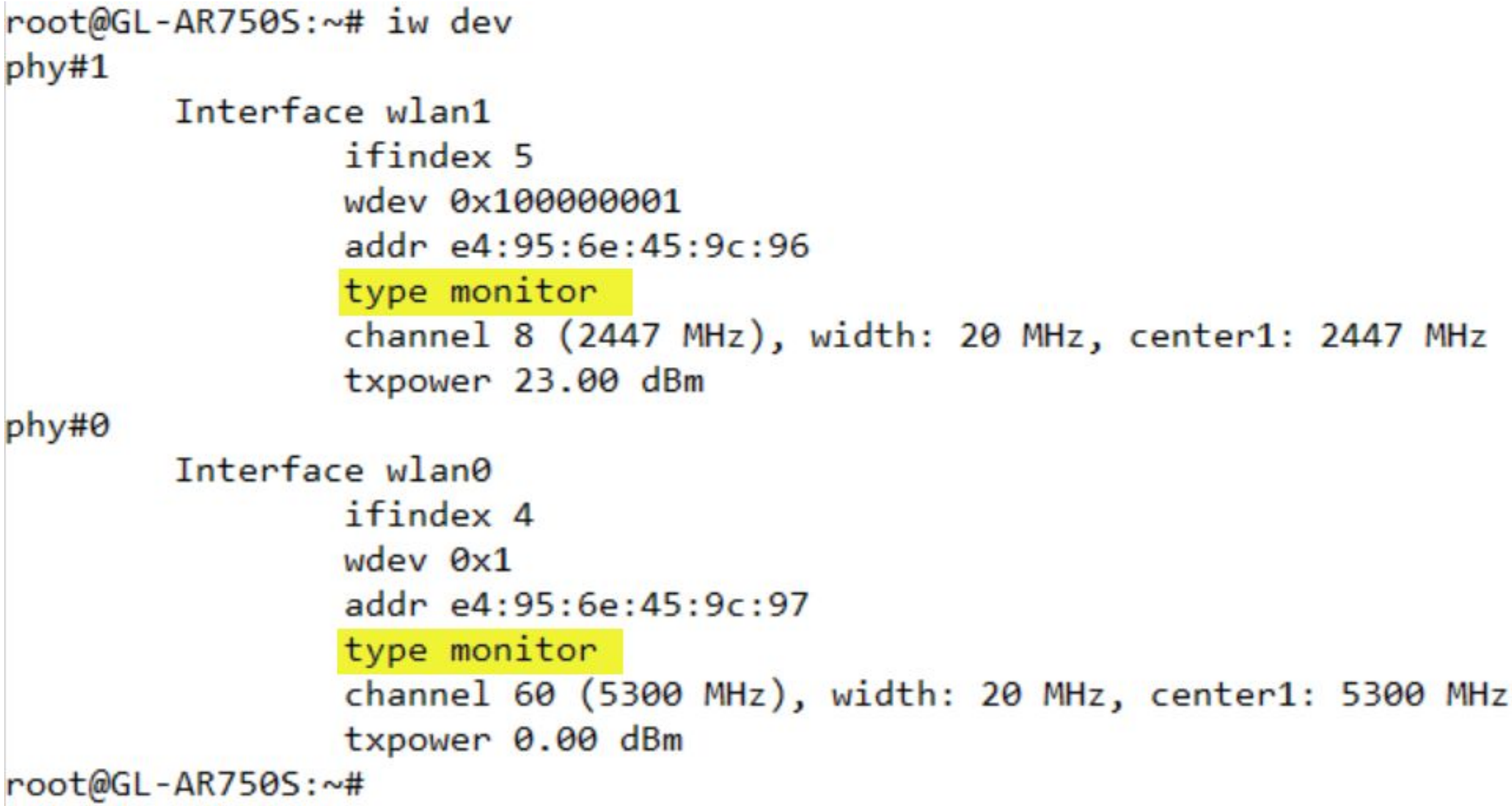
```
root@GL-AR750S:~# opkg install aircrack-ng
Installing aircrack-ng (1.2-rc1-2) to root...
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/packages/aircrack-ng_1.2-rc1-2_mips_24kc.ipk
Installing libnl-core (3.3.0-1) to root...
Downloading http://download.gl-inet.com/releases/packages-3.x/ar71xx/base/libnl-core_3.3.0-1_mips_24kc.ipk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

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!!