

AIW FAQ

How to Verify the WiFi LAR (Location Aware Regulatory) Feature on AIW-170

Category	AIW	Date	2026/6/17
Keyword	AIW-170 (Qualcomm WCN6855 / ath11k driver), LAR (Location Aware Regulatory), Regulatory Domain, Country Code, 5GHz No-IR		

Contents:

1. What Is WiFi LAR and Why Does It Affect the 5GHz Band?	2
2. Why Doesn't "iw reg set <country>" Work?	2
3. Test Prerequisites.....	3
4. Step-by-Step Verification Procedure	3
5. How to Judge Pass / Fail.....	5
6. Frequently Asked Questions	6
Appendix: Full Command List	7

1. What Is WiFi LAR?

LAR (Location Aware Regulatory) is a WiFi mechanism built into some of WiFi chipsets such as the Qualcomm WCN6855. When the module boots and has not yet scanned any AP, it cannot determine its current region and therefore starts up using the global default regulatory domain (country 00 / phy#0 “na: DFS-UNSET”).

Once the module performs a WiFi scan and receives a Country Information Element (Country IE) carried in the beacon of a nearby AP, the driver (cfg80211 / ath11k) automatically switches the regulatory domain according to the detected country code.

This is the core behavior of LAR: the module “listens” to the country codes broadcast by nearby APs and dynamically adjusts its own regulatory region, instead of relying on a manual software setting.

2. Why Doesn't “iw reg set <country>” Work?

On the Qualcomm ath11k platform, the regulatory domain is mainly controlled by the firmware (FW). Even if you run the following in userspace:

```
# sudo iw reg set TW
# iw reg get
```

the global country value will indeed show “TW”, but phy#0 (self-managed) will still be overridden back by the FW to its original value (e.g. it remains US). In other words, the userspace setting does not actually take effect.

➔ Therefore, to verify whether the module truly supports regional regulatory domains, you cannot simply check whether “iw reg set” succeeds. Instead, you must verify the actual LAR behavior – i.e. automatically switching the regulatory domain after scanning nearby APs – which is the method described in this document.

3. Test Prerequisites

Item	Description
Test platform	A host with AIW-170 (WCN6855 / ath11k) installed, running Ubuntu 22.04.3 LTS
Signal source AP	Any WiFi AP that broadcasts a Country IE in its beacon (e.g. a smartphone personal hotspot placed close to the DUT)
Environment	A shielding box/chamber is recommended.

Tip: If the surrounding environment has no AP broadcasting a correct Country IE, enable a personal hotspot on a smartphone and place it as close as possible to the DUT’s antenna connectors. Most smartphones broadcast a Country IE in their Beacon that corresponds to the local telecom regulations (e.g. TW).

4. Step-by-Step Verification Procedure

Step 1: Stop Services That May Interfere with the Wireless Interface

```
# systemctl status NetworkManager
```

```
# systemctl status ModemManager
```

Confirm that both services are “inactive (dead)”, so that they do not automatically manage the wireless interface and interfere with the scan results.

Step 2: Check the Initial Regulatory Domain (Before Any Scan)

Expected result: the “phy#0 (self-managed)” section shows “country na: DFS-UNSET”. At this point all 5GHz channels (Band 2 / Band 4) are marked “(no IR)”, for example:

```
# iw reg get

phy#0 (self-managed)
country na: DFS-UNSET
        (2402 - 2472 @ 40), (N/A, 20), (N/A)
        (5170 - 5330 @ 160), (N/A, 20), (N/A), AUTO-BW, PASSIVE-SCAN
...
```

→ This is the initial state before any regulatory domain has been applied, and serves as the “Before” baseline for later comparison.

Step 3: Bring Up the Wireless Interface

```
# ifconfig wlp2s0 up
```

(“wlp2s0” is the wireless network interface corresponding to AIW-170; confirm the actual interface name with “ifconfig -a”.)

Step 4: Run a Scan to Trigger LAR Detection

This step lets the module actively scan the surrounding environment and receive the Beacon / Probe Response frames of nearby APs. If an AP carries a Country IE, the driver will update the regulatory domain accordingly.

```
# iw dev wlp2s0 scan
```

Tip: If there is a smartphone hotspot nearby, place the DUT as close as possible to it before running the scan to increase the chance of receiving its Country IE.

Step 5: Check the Regulatory Domain Again to Confirm It Has Changed

If LAR is working correctly, the country value of “phy#0 (self-managed)” should change from “na: DFS-UNSET” to the country code broadcast by the scanned AP. In this test, it changed to “country TW: DFS-FCC”:

```
# iw reg get

phy#0 (self-managed)
country TW: DFS-FCC
        (2402 - 2472 @ 40), (6, 30), (N/A)
        (5170 - 5250 @ 80), (6, 24), (N/A), NO-OUTDOOR, AUTO-BW
        (5250 - 5330 @ 80), (6, 24), (0 ms), DFS, AUTO-BW
        (5490 - 5730 @ 160), (6, 24), (0 ms), DFS, AUTO-BW
        (5735 - 5835 @ 80), (6, 30), (N/A), AUTO-BW
```

✓ If the country code changes from “na” / “00” / “US” to the country code matching the test environment (e.g. TW), this indicates that the LAR mechanism is working correctly.

Step 6: Cross-Check the Country IE in the Scan Results

```
# iw dev wlp2s0 scan | grep -E "SSID:|Country:" -i
```

Example output:

```
SSID: Klee
Country: TW      Environment: Indoor/Outdoor
SSID: AIWiFi6
Country: TW      Environment: bogus
SSID: RF_5G
Country: US      Environment: Indoor/Outdoor
```

➔ Several APs in the surrounding environment broadcast “Country: TW”, which is the basis for phy#0’s regulatory domain becoming “TW” in Step 5.

Note: To confirm which specific AP (e.g. an iPhone hotspot) triggered the change, you can turn off other APs in the environment before scanning, or record the SSID with the strongest signal (closest to 0 dBm) together with its Country IE.

Step 7: Compare the 5GHz Channel List and Tx Power Before / After (Final Verification)

```
# iw list | grep -E "MHZ|Band" -i
```

Before switching (country na, 5GHz is “(no IR)” – cannot transmit):

```
Band 2:
* 5180 MHz [36] (20.0 dBm) (no IR)
* 5200 MHz [40] (20.0 dBm) (no IR)
...
* 5825 MHz [165] (20.0 dBm) (no IR)
```

After switching (country TW, 5GHz is now transmittable, with channel limits applied per local regulations):

```
Band 2:
* 5180 MHz [36] (24.0 dBm)
* 5200 MHz [40] (24.0 dBm)
* 5260 MHz [52] (24.0 dBm) (radar detection)
...
* 5745 MHz [149] (30.0 dBm)
* 5825 MHz [165] (30.0 dBm)
* 5845 MHz [169] (disabled)
* 5865 MHz [173] (disabled)
* 5885 MHz [177] (disabled)
```

Key verification points:

- The “(no IR)” marker disappears, meaning the channel can now actively transmit (e.g. start an AP / hotspot).
- Each channel now shows the actual Tx power (24.0 / 30.0 dBm) and “(radar detection)” for DFS channels, and some channels become “(disabled)” – all of these reflect the regulatory limits for TW.
- This confirms that the regulatory domain has truly been switched and applied – not just that the displayed text changed.

5. How to Judge Pass / Fail

Check Item	Pass	Fail
phy#0 country in “iw reg get”	Changes from “na” / “00” to the country code matching the scan environment	Stays at “na: DFS-UNSET”, or is fixed at “US” regardless of environment
5GHz channels in “iw list”	“(no IR)” marker disappears; normal Tx power is shown	5GHz channels remain entirely “(no IR)”
Country IE from “iw dev scan”	Nearby APs broadcast the expected Country IE (e.g. TW)	No nearby AP broadcasts any Country IE

If items 1–3 are consistent (e.g. all nearby APs are TW, phy#0 also becomes TW, and the 5GHz “no IR” restriction is lifted), the module can be considered to support LAR and is working correctly.

6. Frequently Asked Questions

Q: Why must we actually scan an AP – can't we just switch the country code with a command?

A: On Qualcomm platforms the regulatory domain is managed by the firmware. “iw reg set <country>” will be overridden back by the FW at the phy layer (it stays at the original value, e.g. US), so it cannot be treated as a valid regulatory switch. LAR is a native chipset mechanism that is only triggered by actually scanning and receiving a Country IE – this is the only way to demonstrate that the module truly supports multi-region regulatory domains.

Q: What if the test environment has no AP other than US nearby?

A: Enable a personal hotspot on a smartphone (most phones broadcast a Country IE corresponding to their local telecom regulations) and place the DUT as close as possible to the hotspot before scanning, to increase the chance of receiving that Country IE.

Q: After power-on the country always shows “00” or “na” – does this mean the module is faulty?

A: This is the normal initial state (no scan has been performed yet, so the region cannot be determined). It is expected that 5GHz is “(no IR)” at this point. What matters is whether the country code switches correctly after scanning – not the value immediately after power-on.

Q: What is the difference between “country 00” (global) and “phy#0 country” (self-managed)?

A: “global” is the default value of the cfg80211 subsystem and generally does not change. The value that truly reflects the chip's actual regulatory state is the “phy#0 (self-managed)” line – this is the value affected by the LAR switch.

Q: Can this method be used to verify any specific country (e.g. CN, JP)?

A: Yes. The principle is the same – as long as the DUT can scan an AP that broadcasts a Country IE for that country, phy#0's country should switch to the corresponding code and the 5GHz channel table (allowed channels, max power, DFS radar-detection channels, etc.) will be adjusted according to that country's regulations. Prepare an AP / hotspot broadcasting the target country's Country IE to perform the corresponding verification.

Appendix: Full Command List (Run in Order)

```
# 1. Make sure background services do not interfere
systemctl status NetworkManager
systemctl status ModemManager

# 2. Record the initial regulatory domain (Before)
iw reg get
iw list | grep -E "MHZ|Band" -i

# 3. Bring up the wireless interface
ifconfig wlp2s0 up

# 4. Scan the surrounding environment to trigger LAR
iw dev wlp2s0 scan

# 5. Check whether the regulatory domain has changed (After)
iw reg get

# 6. Check the Country IE of scanned APs
iw dev wlp2s0 scan | grep -E "SSID:|Country:" -i

# 7. Compare the 5GHz channel/power table before and after
iw list | grep -E "MHZ|Band" -i
```

This document is based on the actual bring-up / test log of the BSCI-AIW-170BQ case (2026/5/26). Platform: AIW-170 (WCN6855 / ath11k), OS: Ubuntu 22.04.3 LTS, Kernel 6.5.0-44-generic.